servicenow

ワシントンDCプラットフォームのセキュリティ

最終更新日: **2025**年**12**月**17**日

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

これらの資料は、翻訳ソフトウェアを使用してお客様の便宜のために翻訳されています。正確な翻訳をご提供できるよう相当な努力を払っておりますが、いかなる自動翻訳も人間の翻訳者に代わることはなく、そのようなことは意図されておりません。翻訳は「現状のまま」提供されています。他言語への翻訳の的確性、信頼性または正確性については、明示または黙示を問わず、いかなる保証も行われません。翻訳ソフトには限界があるため、一部のコンテンツが正確に翻訳されていない場合があります。これらの資料の公用言語は英語です。翻訳の際に生じる相違または不一致は、コンプライアンスまたは履行の目的に関しては拘束力を有さず、法的効力はないものとします。

ここで示したいくつかの例と図は、説明の目的でのみ提供されています。ServiceNow 製品またはサービスへの実際の関連付けやつながりは意図されておらず、推測されるものではありません。

ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは米国および/またはその他の国における ServiceNow, Inc. の商標または登録商標です。その他の会社名および製品名は、それぞれの所有者の商標です。

下記の ServiceNow ウェブサイト利用規約をお読みください。 www.servicenow.com/terms-of-use.html

自動翻訳

本社
2225 Lawson Lane
Santa Clara, CA 95054
United States
(408) 501-8550

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

servicenow

目次

インスタンスの保護 9
プラットフォームセキュリティ 17
証明書 19
証明書の概要 20
LDAP クライアント証明書の生成 21
インスタンスへの証明書のアップロード 23
コード署名 24
コード署名の概要 28
コード署名の構成 30
コード署名の使用 46
コード署名の参照 62
セキュリティロール 67
明示的なロール 67
昇格された権限ロール 75
Security Center 77
ホームページ 78
セキュリティの強化 79
セキュリティスキャナー 86
セキュリティ測定基準 88
重大な更新 93
セキュリティ学習 96
Instance Security Center 96
Instance Security Center から ServiceNow Security Center への移行 106
セキュリティイベントの監視 109
日次コンプライアンススコアの確認とセキュリティプロパティの設定 114
誤ったセキュリティ定義のスキャン 123
インスタンス測定基準の監視 124
ISC 仮想エージェントインターフェイスのアクティブ化 136
その他の設定とセキュリティリソース 137
インスタンスセキュリティ強化設定 139
ハードニング設定 244
ハードニング設定のベースライン 246
アクセス制御 260
API と Web サービス 303
アーキテクチャ、設計、および脅威のモデル化 318
認証 328
ビジネスロジック 354
通信 357
設定 362

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

データ保護 372
エラー処理とログ記録 375
ファイルとリソース 382
悪意のあるコード 389
セッション管理 391
保存された暗号化 403
検証、サニタイズ、およびエンコーディング 404
暗号化とキー管理 436
キー管理フレームワークの詳細 438
[store-future: BEGIN review]
[End]
暗号化とキー管理のサブスクリプションバンドル 439
キー管理フレームワークの理解 441
キー管理アクション 470
Web サービスからキーをインポートする 473
キー管理フレームワークの健全性 476
GlideEncrypter の廃止に向けたインスタンスの準備 478
password2 フィールドの GlideEncrypter を廃止 479
キー管理フレームワークリソース交換 482
Column Level Encryption 489
Column Level Encryption Enterprise 497
Infrastructure Security 531
Key Management Framework (KMF) による Password2 暗号化 533
キー管理を使用したクラウド暗号化 535
データベース暗号化 555
フルディスク暗号化 560
Edge Encryption 560
ログ 694
システムログ 696
ログエクスポートサービス (ルス) 710
ログ記録、監査、およびエラー 722
シークレット管理 722
シークレット管理の詳細 723
クライアントのアクセス可能なシークレットの構成 727
シークレット管理ダッシュボード 740
ServiceNow Vault 751
プラットフォームプライバシー 754
アクセス制御リストのルール 755
アクセス制御リストの概要 757
ACL ルールの構成 772
コンテキスト依存セキュリティマネージャー 775
ACL の詳細設定 780

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

セキュリティ属性ホームページ ... 791
セキュリティ属性の基礎 ... 792
セキュリティ属性を作成 ... 792
セキュリティ属性 スコープ ... 795
データ分類 ... 795
データ分類の概要 ... 797
データ分類 プラグインのデモデータをインストールする ... 798
データ分類の作成 ... 799
辞書エントリへのデータ分類の割り当て ... 800
概要ダッシュボードを使用したデータ分類の分析 ... 801
ドメイン分離と データ分類 ... 803
データフィルタリング ... 804
データフィルタリングの概要 ... 805
データフィルタリングの有効化 ... 807
データフィルタリングルールの作成 ... 807
対象基準の作成 ... 810
データフィルタリングのデバッグ ... 813
Data Privacy ... 815
Data Privacy の概要 ... 816
Domain Separation と Data Privacy ... 817
匿名化でサポートされているフィールドタイプ ... 817
Data Privacy ロール ... 819
Data Privacy (Classic) ... 821
Data Privacy ... 831
データディスカバリー ... 846
データディスカバリー の概要 ... 848
データディスカバリー のアクティブ化 ... 850
データディスカバリー の結果ページでデータを分類する ... 851
データディスカバリー ジョブ ... 851
データディスカバリー ロール ... 856
データディスカバリー のジョブ結果 ... 857
サービスプロバイダーの Domain Separation ... 858
Domain Separation の概要 ... 860
アプリケーションでのドメイン分離のサポート ... 878
サービスプロバイダー向けのドメイン分離の推奨プラクティス ... 887
Domain Separation のヘルプ ... 927
Domain Separation のセットアップと管理 ... 928
Domain Separation センター ... 962
ID ... 970
アクセスアナライザー ... 971
Access Analyzer の概要 ... 972
Access Analyzer の使用 ... 973

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

権限の評価 992
よく寄せられる質問 994
Global Identity 999
フェデレーション ID の探索 1001
フェデレーション ID 基準へのアクセス 1002
ID フィールドの更新 1002
ID とアクセスの監査 1004
ID およびアクセス監査の詳細 1005
監査結果 1006
セキュリティ監査可能フィールド 1010
ID アクセスと監査でサポートされているフィールドとサポートされていないフィールド 1013
ID センター 1015
ID センターの概要 1016
ID センターのアクティブ化 1016
ユーザー向け ID センター 1017
管理者の ID 測定基準 1020
クロスドメイン ID 管理システム (SCIM) 1020
SCIM プロバイダー 1021
SCIM クライアント 1040
アクセス管理 1059
認証 1060
適応認証 1063
API 認証 1119
API アクセスポリシー 1130
証明書ベースの認証 1157
インスタンスへのカスタム URL の関連付け 1165
LDAP 統合 1172
同時セッションの制限 1236
マルチファクター認証 (MFA) 1240
複数プロバイダーの Single sign-on (SSO) 1286
OAuth 受信および送信認証 1383
パスワードの複雑さの要件 1420
ServiceNow インスタンスへの自己登録 1432
トークンベースの認証 (ユーザーログイン) 1443
Zero Trust アクセス 1456
接続と資格情報 1470
資格情報、接続、およびエイリアスの概要 1472
接続を開始 1486
認証情報の開始 1497
認証アルゴリズム 1565
ログインと認証のセキュリティ 1575

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ログインと認証のセキュリティの詳細 1577
ログアウト確認プロンプトの構成 1578
ログインシナリオの定義 1578
参照例：デフォルトのセルフサービス パスワードリセット プロセス 1582
Web サービスセキュリティ 1594
Web サービスセキュリティの詳細 1596
相互認証の構成 1597
参照：WS-Security 1600
一般的なプラットフォームのセキュリティ設定 1602
アンチウイルススキャン 1604
Antivirus Scanning の詳細 1605
アンチウイルススキャン の構成 1607
隔離されたファイルの確認 1607
アンチウイルススキャン の辞書属性について 1608
監査 1609
監査の詳細 1610
テーブルの監査の構成 1613
システム監査テーブルおよびリレーションシップ変更の監査テーブルの表示 1615
履歴セットについて 1616
高セキュリティ設定 1626
高セキュリティ設定の詳細 1627
スクリプトサンドボックスプロパティの構成 1638
高セキュリティ設定の有効化 1639
HTML サニタイザー 1642
HTML サニタイザーの詳細 1643
HTML サニタイザーの構成 1646
HTML サニタイザーの有効化 1647
その他の設定とセキュリティリソース 1648
[store-future: BEGIN review]
セキュリティ設定プロパティ 1649
MID Server の安全な展開ガイド 1654
元に戻せる動作 1658
廃止されたセキュリティプロパティ 1659
JavaScript コンテンツアクセス制御の使用 1660
その他のセキュリティ強化リソース 1662
[End]
ServiceNow® アクセス制御 1662
ServiceNow® アクセス制御の詳細 1663
ServiceNow® アクセス制御の有効化 1666
ServiceNow® アクセス制御の構成 1668
監査ログ 1669
仮想プライベートネットワーク (VPN) 1669

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

仮想プライベートネットワーク (VPN) の詳細.....1670
VPN サービスのアクティブ化..... 1673
VPN 通信用のアドレスの構成..... 1673

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

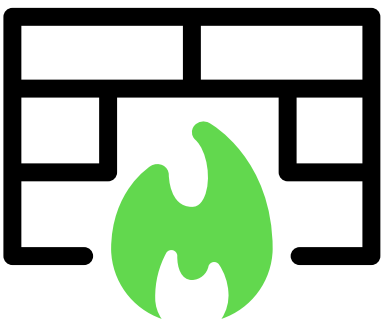
インスタンスの保護

Now Platform® のセキュリティにより、インスタンスの保護、データの暗号化、ID の確認、ユーザーの認証、およびアプリケーションセキュリティ標準に基づく現在のコンプライアンスレベルの表示が可能になります。

セキュリティは Now Platform のすべてのレベルに組み込まれています。失敗したログインの管理や暗号化されたパスワード保護から、アクセス制御ルールや監査ログまで、組織に適したセキュリティ機能が実装されています。

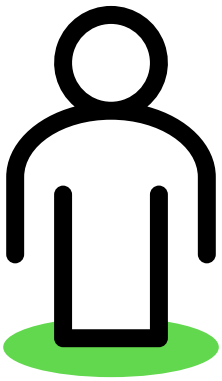
いずれかのタイルを選択して開始します。

プラットフォームセキュリティ



ServiceNow® の Platform Security アプリケーションには、セキュリティ侵入からインスタンスを保護し、データを安全に保つ一連の機能があります。

プラットフォームプライバシー



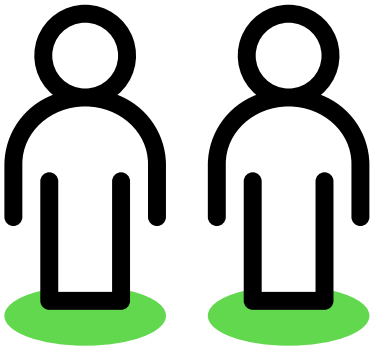
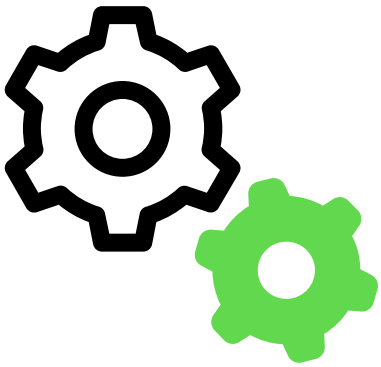
Platform Privacy を使用して、機密データを分類し、本番インスタンスのユーザーデータから個人識別可能情報 (PII) を削除して、非本番インスタンスのデータを匿名化できます。匿名化されると、ユーザーデータは規制対象の個人情報と見なされなくなります。

ID

ServiceNow® の Platform Identity アプリケーションには、インスタンス全体の ID を認識するための一連の機能があります。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

アクセス管理	一般的なプラットフォームのセキュリティ設定	
		
ServiceNow® の Access Management では、インスタンスにアクセスするユーザーを認証し、ユーザーのロールまたは職務に一致する機能に対してユーザーを許可できます。	一般的なプラットフォームセキュリティ設定の詳細を確認します。	

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

インスタンスの保護

セキュリティは Now Platform のすべてのレベルに組み込まれています。失敗したログインの管理や暗号化されたパスワード保護から、アクセス制御ルールや監査ログまで、組織に適したセキュリティ機能が実装されています。

ServiceNow Vault

ライフサイクル全体に渡って機密情報を不正なアクセス、破損、または盗難から保護するデータセキュリティツールの ServiceNow Vault 製品セットを使用します。機密情報の編集と監査のために、暗号化、シークレット管理、データプライバシーなどの保護を適用します。ServiceNow Vault ホームページは、ServiceNow Vault データセキュリティ製品を見つけてそこに移動するための単一の表示可能な場所を提供します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

機密データへのリスクを軽減する

アプリケーションレベルでのフィールドの暗号化のためのキー保護とキーライフサイクル管理を行う Key Management Framework および 列レベル暗号化エンタープライズを使用してプラットフォームのデータを暗号化します。

転送中のデータを暗号化する

データセンターと ServiceNow クラウド間を移動する機密データを暗号化および復号化するネットワーク内のサーバーを使用してデータを暗号化します。

インスタンスへ安全にアクセスする

インスタンスにアクセスするユーザーの ID を検証し、ユーザーのロールや職務に一致する機能に対してユーザーを許可します。

個人識別可能情報 (PII) を匿名化する

すべてのユーザーまたは一部のユーザーの情報をすべて匿名化するかどうかを定義します。匿名化すると、選択したユーザーレコードのデータが、ランダムな値または定義した値に置き換えられます。値を置き換える際は、さまざまな手法でデータ構造を保持できます。データ構造を保持すると、メールアドレスや物理アドレスなどのデータが、同様の形式で匿名化されたバージョンに置き換えられます。

リスクに迅速に対応する

リアルタイムで作業可能なダッシュボード、推奨事項のカスタマイズ、およびセキュリティの欠陥を迅速に修正するためのガイド付き手順により、セキュリティの可視性が向上します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Column Level Encryption を使用して機密データに対するリスクを軽減する

列レベル暗号化エンタープライズ が Key Management Framework を使用することで、インスタンス上での暗号化および復号化に関する詳細な仕様をカスタマイズして管理するためのキーライフサイクル管理のベストプラクティスが可能になります。列レベル暗号化エンタープライズ はサブスクリプションを購入する必要がありますが、Key Management Framework はすべてのインスタンスでデフォルトで使用できます。

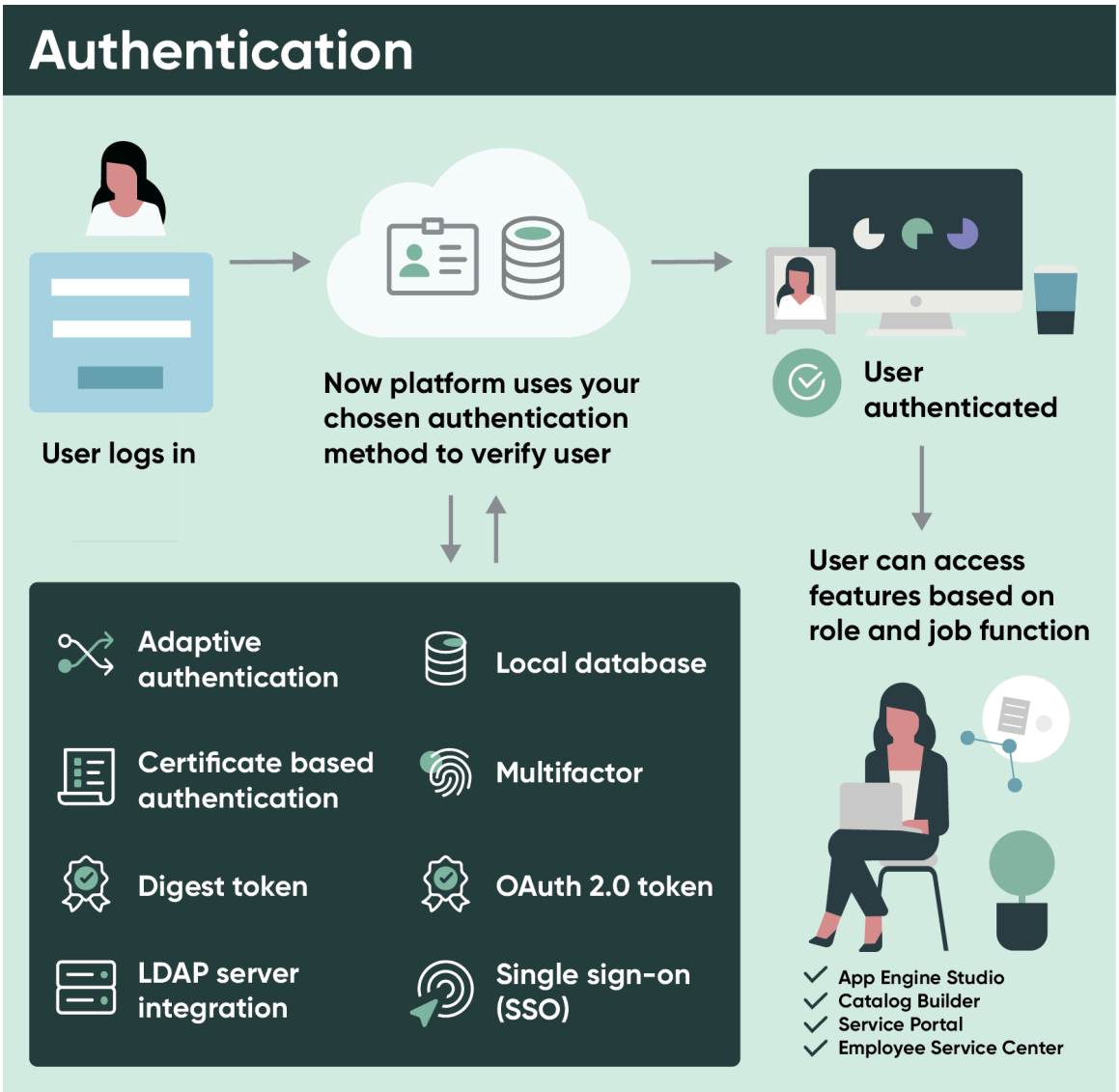
Edge Encryption を使用した転送データの暗号化

エッジ暗号化 は、社内の機密データを暗号化してから (送信中に暗号化) インターネット経由でインスタンスに送信します。インスタンスでは保存時もデータは暗号化されたままです。「クライアント側」暗号化とも呼ばれる Edge は、インフラストラクチャ上で維持されているプロキシを通過するために、すべての双方向ユーザートラフィックを必要とします。キーはインフラストラクチャ上のプロキシ内に保存されるため、キー管理を完全に制御できます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

インスタンスへ安全にアクセスする

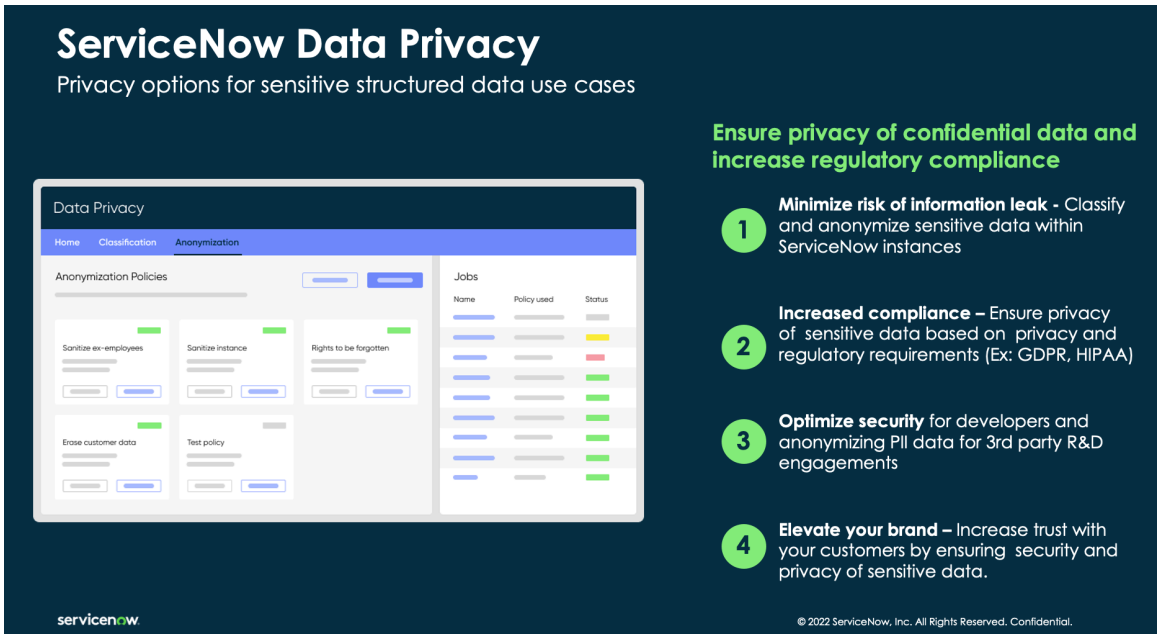


会社のニーズを満たす認証のタイプを選択します。ユーザーの認証、シングルサインオンの有効化、Web クライアントによるインスタンスへのアクセスの承認などを行うことができます。

自動翻訳

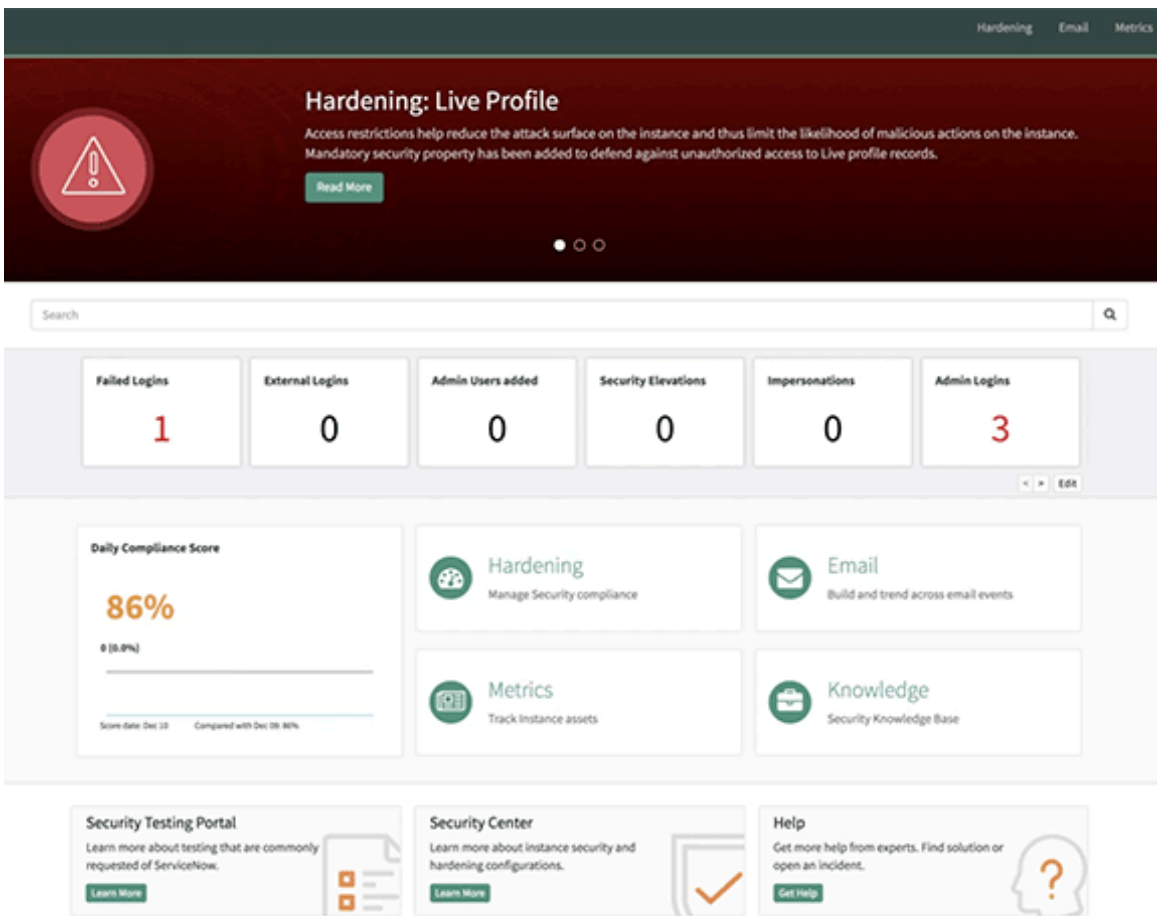
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

個人識別可能情報 **(PII)** を匿名化する



Data Privacy を使用して、本番インスタンスのユーザーデータから個人識別可能情報 (PII) を削除し、非本番インスタンスのデータを匿名化します。ユーザーデータが規制対象の個人情報と見なされなくなっていることを確認します。

リスクに迅速に対応する



自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

インスタンスセキュリティコントロールのコンプライアンスレベルの監視、セキュリティイベントモニタリング測定基準の表示、インスタンスセキュリティ設定の構成と維持はすべて、Instance Security Center 内から行います。Instance Security Center は、複数の主要なセキュリティコンポーネントを単一のコントロールコンソールに統合し、インスタンスベースのセキュリティイベントの検出、保護、応答を支援します。

製品

- アクセス制御リストのルール
- Antivirus Scanning
- 監査
- 認証
- 証明書
- 接続および資格情報
- データ分類
- データフィルタリング
- Data Privacy
- サービスプロバイダーの Domain Separation
- 暗号化とキー管理
- Explicit Roles
- ID
- Instance Security Center
- インスタンスセキュリティ強化設定
- ボールト
- 仮想プライベートネットワーク (VPN)

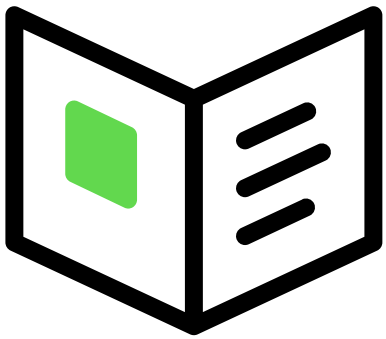
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

プラットフォームセキュリティ

プラットフォームセキュリティは、インスタンスを保護する機能を提供します。

証明書



証明書を使用してセキュア接続を確立し、署名を検証します。

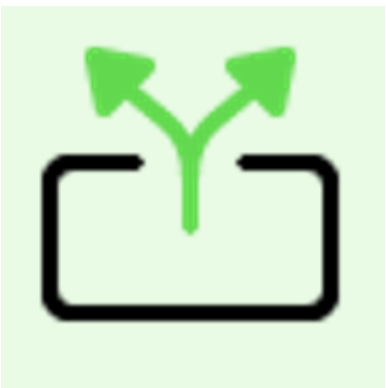
コード署名

コード署名は、データの信頼性と整合性を確認するために後でチェックされるデータのデジタル署名を作成します。

セキュリティロール

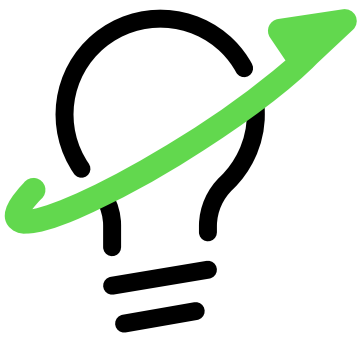
セキュリティロールによりセキュリティを強化するためには、ユーザー全員に少なくとも 1 つのロールを割り当てて、インスタンスが内部ユーザーと外部ユーザーを区別できるようにする必要があります。

ログ



ログモジュールは、インスタンス内で発生するトランザクションやイベントのトラブルシューティングとデバッグに使用できるさまざまなログを提供します。

ServiceNow Vault



ライフサイクル全体に渡って機密情報を不正なアクセス、破損、または盗難から保護するデータセキュリティツールの ServiceNow Vault 製品セットを使用します。

セキュリティセンター

管理者は最高レベルのセキュリティ体制を継続的に維持し、安全でないイベントや動作を簡単に監視できます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

暗号化とキー管理	シークレット管理	
暗号化は、プレーンテキストを暗号テキストに変換して情報の公開を制御する暗号化手順です。	ServiceNow シークレット管理を使用し、ビジネスニーズに合わせてパスワードへのアクセスを詳細に管理します。	

証明書

証明書は、LDAP、送信 Web サービス相互認証、Web セキュリティサービス、MID Server などの機能で、安全な接続を確立して署名を検証するために使用されます。

コード署名

コード署名を使用して、機密性の高いアプリケーション構成データとスクリプトを使用する前に検証できるので、セキュリティの強化に役立ちます。コード署名は、データの信頼性と整合性を確認するために後でチェックされるデータのデジタル署名を作成します。コード署名は、ServiceNow Vault のコンポーネントとしてライセンスされるモジュールです。

セキュリティロール

セキュリティロールによりセキュリティを強化するためには、ユーザー全員に少なくとも 1 つのロールを割り当てて、インスタンスが内部ユーザーと外部ユーザーを区別できるようにする必要があります。

暗号化とキー管理

暗号化は、プレーンテキストを暗号テキストに変換して情報の公開を制御する暗号化手順です。

セキュリティセンター

セキュリティセンターを使用すると、管理者は最高レベルのセキュリティ体制を継続的に維持し、安全でないイベントや動作を簡単に監視できます。

ログ

ログモジュールは、インスタンス内で発生するトランザクションやイベントのトラブルシューティングとデバッグに使用できるさまざまなログを提供します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

シークレット管理

ServiceNowシークレット管理では、ビジネスニーズに合わせてパスワードへのアクセスを詳細に管理します。

ServiceNow Vault

ServiceNow Vault 製品はライフサイクル全体に渡って機密情報を不正なアクセス、破損、または盗難から保護するデータセキュリティツールの設定に役立ちます。機密情報の編集と監査のために、暗号化、シークレット管理、データプライバシーなどの保護を適用します。

証明書

インスタンスには、セキュア接続を確立して署名を検証するための証明書が必要です。

探索	構成
証明書の主な機能とビジネス価値について学びます。	コア構成を計画します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

アップロード

アプリケーションを計画して設定します。

証明書の概要

インスタンスには、セキュア接続を確立して署名を検証するための証明書が必要です。

証明書は次のような機能に使用されます。

- LDAPS
- Outbound web service mutual authentication
- Web サービスセキュリティ
- MID Server

証明書を使用するには、セキュリティ保護されたサーバーまたはクライアントの証明書を生成または購入し、インスタンスにアップロードする必要があります。

LDAP 証明書

インスタンスが LDAP サーバーとの LDAP over SSL (LDAPS プロトコル) 接続を確立するには、SSL 証明書が必要です。

インスタンスは、次の 2 つのタイプの LDAP 証明書を受け入れます。

証明書	タイプ	必須
LDAP サーバー証明書	サポートされている任意のタイプ	すべての LDAP 構成
LDAP クライアント証明書	Java キーストアタイプ	相互認証

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

複数のサーバー証明書がある場合、LDAP サーバーが接続を許可するまで、インスタンスは各サーバー証明書を順番に試行します。複数の LDAP サーバーを使用する場合は、LDAP サーバーごとに SSL 証明書を含めてください。

相互認証では、サーバーに加えてクライアントが証明書を提示する必要があります。LDAP サーバーが相互認証を必要とする場合は、LDAP サーバーのクライアント証明書を Java キーストアタイプの証明書で指定する必要があります。

証明書の条件

有効な証明書は次の条件を満たす必要があります。

- 証明書のキーサイズは最大 2048 ビットです。
- 証明書には、次のいずれかのファイル拡張子が必要です。

拡張	説明
DER	*Distinguished Encoding Rules* 形式は、バイナリメッセージ転送構文です。この形式は、.CER および .CRT ファイル拡張子もサポートしています。
CER	Distinguished Encoding Rules 形式を使用する証明書の証明書ファイル拡張子。
CRT	Distinguished Encoding Rules 形式を使用する証明書の証明書ファイル拡張子。
PEM	*Privacy Enhanced Mail* 形式は、「-----BEGIN CERTIFICATE-----」と「-----END CERTIFICATE-----」のテキスト文字列で囲まれた、base-64 でエンコードされた DER 証明書です。

証明書の信頼

デフォルトでは、インスタンスは、Java 仮想マシン (JVM) で認識される認証局 (CA) からの証明書のみを信頼します。自己署名証明書およびエンタープライズ署名証明書は信頼されません。

注:
証明書の使用に影響するプロパティの詳細については、「インスタンスセキュリティ強化設定」の「安全な通信」を参照してください。

LDAP クライアント証明書の生成

OpenSSL を使用して相互認証用の LDAP クライアント証明書を生成します。最終的な出力は、Java キーストア内に格納される PKCS#12 証明書です。

始める前に
必要なロール：管理者

このタスクについて
証明書の生成の詳細については、OpenSSL のドキュメント を参照してください。これらの手順では、OpenSSL にアクセスできることを前提としています。

コマンドラインインターフェイスで次のコマンドを入力します。

手順

1. 自己署名クライアント証明書を生成します。

   Example
   たとえば、このコマンドは、test1-key.key 秘密キーに基づいてクライアント証明書 test1-cert.crt を作成します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

```
openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout test1-key.key -out
 test1-cert.crt
```

2. 証明書ファイルと秘密キーの両方を PKCS#12 (.pfx または .p12 拡張子のファイル) に変換します。

   Example
   たとえば、このコマンドは、クライアント証明書と秘密キーを test1-certificate.pfx と呼ばれる PKCS#12 証明書に変換します。

   ```
   openssl pkcs12 -export -out test1-certificate.pfx -inkey test1-key.key -in test1-cert.crt
   ```

3. Java キーストアを生成し、pkcs12 ファイルをインポートします。

   Example
   たとえば、このコマンドは、証明書を test1.jks Java キーストアにインポートします。

   ```
   keytool -importkeystore -srckeystore test1-certificate.pfx -srcstoretype PKCS12
    -destkeystore test1.jks
   ```

4. Java キーストアファイル (test1.jks) の証明書をインスタンスにアップロードします。

   注:

   .jks 拡張子の証明書を使用してオンプレミスのインスタンスにアップロードしているときに、「アプリケーションのアップロードを処理するための有効な証明書が見つかりません」というメッセージが表示された場合は、.pfx 拡張子の証明書を代わりに使用してください。

次のタスク
インスタンスへの証明書のアップロード

サーバー証明書の生成

keytool を使用して、新しい Java キーストアファイルを生成し、証明書署名要求 (CSR) を作成してから、秘密キー、公開証明書のペア、および署名済み証明書をキーストアにインポートすることができます。

始める前に
必要なロール：管理者

このタスクについて
キーと CSR の生成の詳細については、Java keytool のドキュメント を参照してください。

コマンドラインインターフェイスで次のコマンドを入力します。

手順

1. Java キーストアとキーペアを生成します。

   Example
   たとえば、このコマンドは my.keystore と呼ばれるキーストアを作成し、キーストア内に mydomain と呼ばれる秘密キーを生成します。

   ```
   keytool -genkey -alias mydomain -keyalg RSA -keystore my.keystore
   ```

2. 既存の Java キーストアの CSR を生成します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Example
たとえば、このコマンドは mydomain.csr または mydomain キーと呼ばれる CSR を生成します。

```
keytool -certreq -alias mydomain -keystore my.keystore -file mydomain.csr
```

3. ルートまたは中間認証局 (CA) 証明書を Java キーストアにインポートします。

Example
たとえば、このコマンドは Thawte の CA 証明書をインポートします。このコマンドでは、Thwate が CSR に署名した CA であると仮定しています。

```
keytool -import -trustcacerts -alias root -file Thawte.crt -keystore my.keystore
```

4. 署名済みプライマリ証明書を Java キーストアにインポートします。

Example
たとえば、このコマンドは署名された証明書 mydomain.crt をキーストアにコピーします。

```
keytool -import -trustcacerts -alias mydomain -file mydomain.crt -keystore my.keystore
```

5. Java キーストアファイル (my.keystore) の証明書をインスタンスにアップロードします。

次のタスク
インスタンスへの証明書のアップロード

インスタンスへの証明書のアップロード

[証明書] モジュールからインスタンスに証明書を追加します。

始める前に
必要なロール：管理者

このタスクについて
ADFS サーバーで証明書が更新されている場合は、更新された証明書へのインスタンスもアップロードする必要があります。

手順

1. 移動先 すべて > システム定義 > 証明書.
2. [新規] をクリックします。
3. フォームのフィールドに入力します。
4. [送信] をクリックします。

   アップロード中に、モジュールは証明書の読み取り専用プロパティを抽出して次のフィールドに表示します。

   - 有効開始日
   - 有効期限

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- Issuer
- 証明書の件名

5. [ストア/証明書を検証] をクリックして、証明書が正しいかどうかを確認します。インスタンスで証明書またはキーストアに関するエラーが発生した場合は、エラーメッセージが表示されます。

信頼できるサーバー証明書のアップロード

サービスプロバイダーの信頼できるサーバー証明書をアップロードすることで、インスタンスにより、接続しているサービスの有効性と安全性を確保できます。

始める前に
必要なロール：管理者

このタスクについて
インスタンスは、サービスプロバイダーによって提供される証明書を使用して、送信 Web サービス呼び出しを検証します。

手順

1. 信頼ストア証明書タイプの新しい証明書レコードを作成します。
2. 次のいずれかのアクションを実行します。
   - サービスプロバイダーの DER 形式の証明書を添付します。
   - サービスプロバイダーの PEM 形式の証明書を **[PEM** 証明書] フィールドにコピーして貼り付けます。

コード署名

コード署名は、データの信頼性と整合性を確認するために後でチェックされるデータのデジタル署名を作成します。コード署名は、ServiceNow Vault のコンポーネントとしてライセンスされるモジュールです。

コード署名と信頼のサークル

(COT) は信頼のサークル、信頼できるインスタンスと本番インスタンス間の安全な通信を作成して、承認されたユーザーのみがコード署名機能にアクセスできるようにするコード署名の前提条件です。

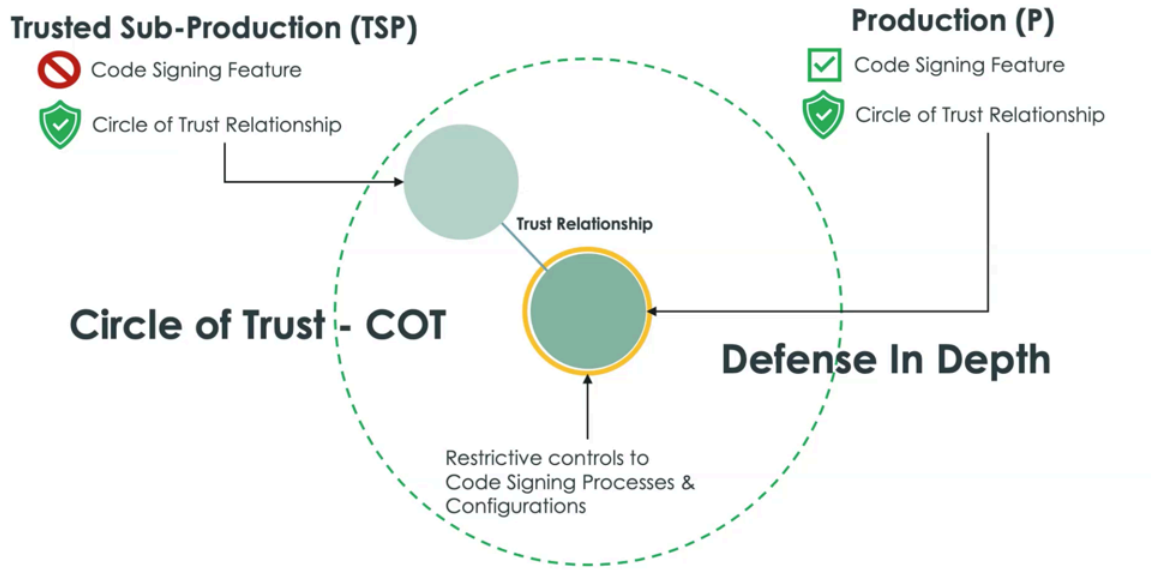
複数のセキュリティ対策があると、本番インスタンスが侵害された場合に、悪意のある攻撃者がコード署名を無効にしたり悪用したりするのを防ぐことができます。多層防御戦略の一環として、COT は次のコンポーネントを使用します。

- コード署名のプロセスと構成を保護するために、最も強力な管理者アカウントさえも制限するコントロールが本番インスタンスに確立されます。
- 信頼できる (TSP) インスタンスは、本番インスタンスと連携して関係を確立する 信頼のサークルために必要です。少なくとも 1 つのトラステッド・インスタンスが必要ですが、複数の TSP インスタンスを本番インスタンスと連携するように構成できます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

信頼のサークルの概要

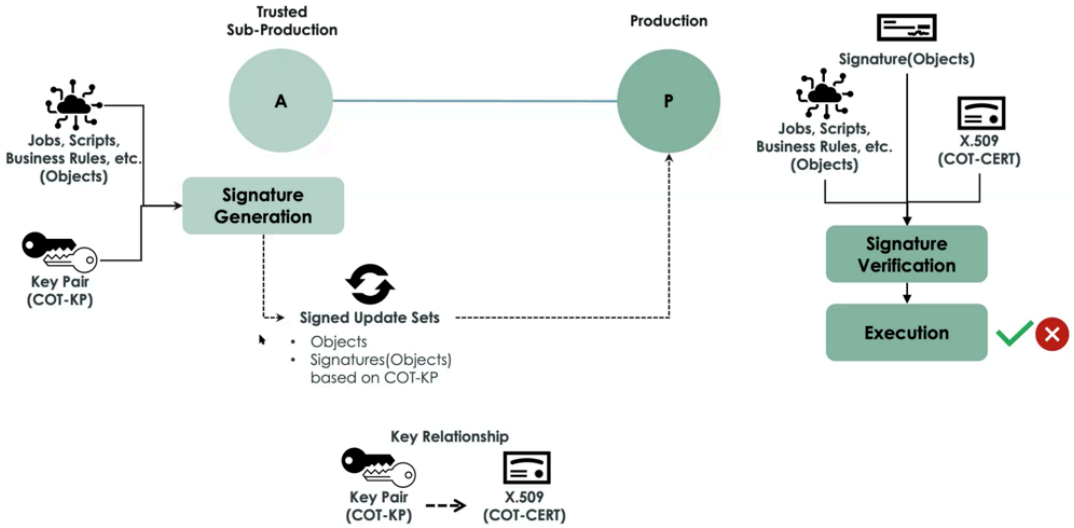


信頼のサークルは、キーペアとともにジョブ、スクリプト、およびビジネスルールを使用して、本番インスタンスへの更新セットに署名するための署名を生成します。ジョブが呼び出されると、本番インスタンスの更新を実行するために、信頼できる証明書とともに署名が検証されます。

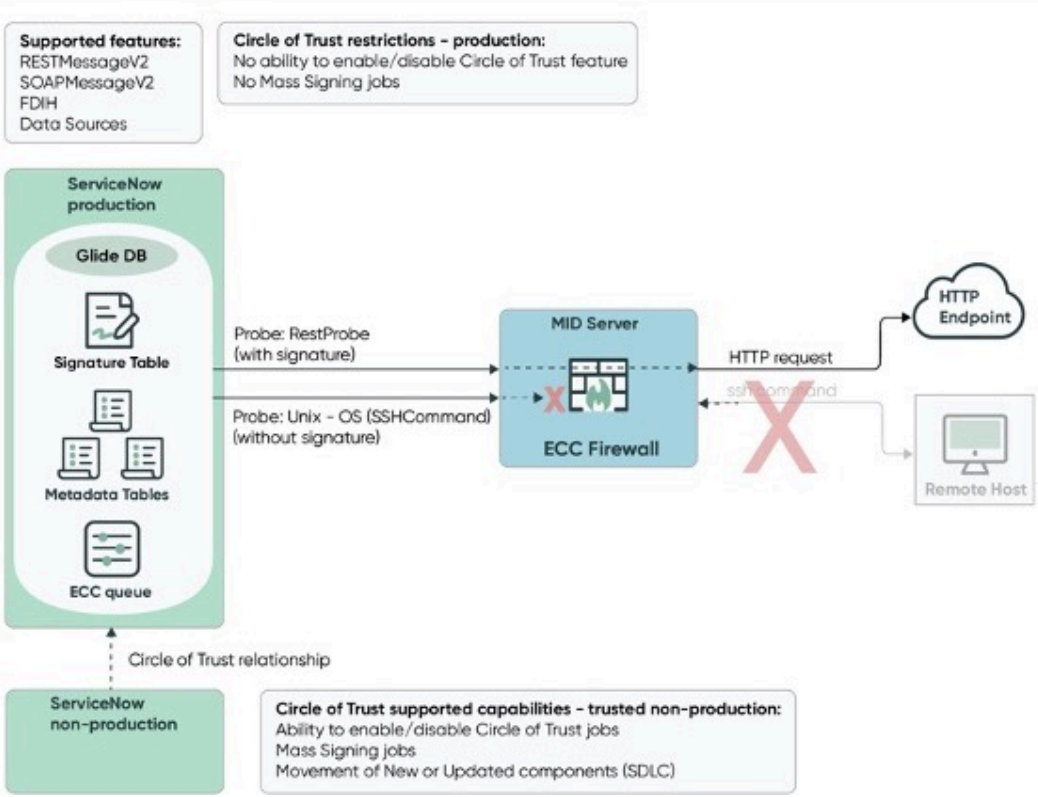
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

信頼できる更新セットのプロセス



コード署名フロー

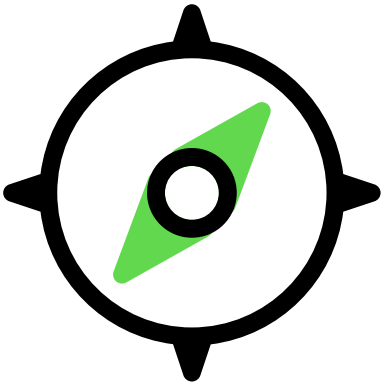
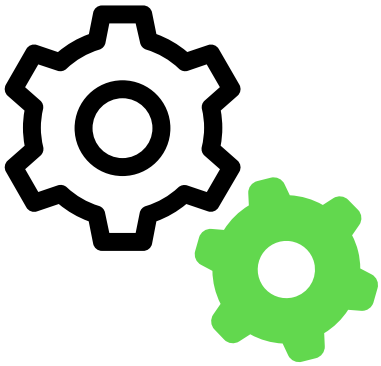
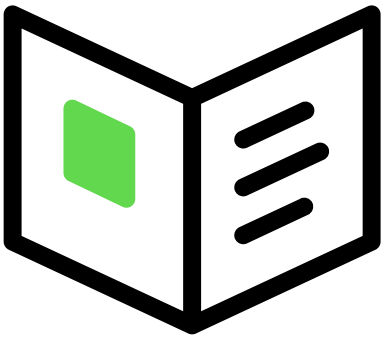


これには 信頼のサークル 、信頼できるインスタンスと本番インスタンス間に最初の信頼関係が必要であり、これにより、任意の認証レベルを持つ権限のないユーザーが未承認のアクティビティにアクセスできないようになります。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

開始するには

探索	構成	参照
		
コード署名の主な機能とビジネス価値について学びます。	コード署名をアクティブ化して構成します。	プロパティとトラブルシューティングの詳細を取得する

使用方法
コード署名を使用してデータの信頼性と整合性を検証する方法について説明します。

自動翻訳

トラブルシューティングとヘルプ

- https://www.servicenow.com/community/secops/ct-p/security-operations
- Known Error Portal で既知のエラー記事を検索
- 担当者 カスタマーサービス & サポート

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

コード署名の概要

コード署名は、機密性の高いアプリケーション構成データとスクリプトを使用する前の検証に使用できるため、セキュリティの強化に役立ちます。

コード署名は、データの信頼性と整合性を確認するために後でチェックされるデータのデジタル署名を作成します。コード署名は、ServiceNow Vault のコンポーネントとしてライセンスされるモジュールです。

注:
カスタマーサービス & サポートチームはコード署名へのアクセスを許可する必要があります。

コード署名は、実行されている操作の背後にある意図を宣言し、リソースまたはレコードを、意図した目的で使用できるかどうかを検証します。コード署名を容易にするために、Key Management Framework (KMF) は、デジタル署名のためにデジタル証明書と業界標準の非対称暗号化を使用します。

プラットフォームとインフラストラクチャ側で内部的にコード署名を使用します。コード署名は、特定のテーブルのコンテンツまたは特定のメタデータテーブル内のレコードのサブセットに署名する方法を提供します。

コード署名では、信頼できるインスタンスと本番インスタンスの間で安全な 信頼のサークル (COT) を使用して、承認された安全な信頼できるインスタンスのみがコード署名機能にアクセスできるようにします。

ユースケース

コード署名は、MID サーバー および 統合ハブ を使用する操作に使用できます。認証とは、コード署名を使用して、MID Server 操作および Integration Hub 操作で使用される ECC キューレコードのデジタル署名を作成することです。

たとえば、実行時に ECC キューレコードを作成するために によって ServiceNow 書き込まれたスクリプトインクルードは、「ベースシステムのコンテンツ」として署名されます。検証も署名もされていないバックグラウンドスクリプトやその他の作成元から ECC キューに挿入されるのではなく、「インスタンスによって ServiceNow 適切に発行された」ものとして署名されます。

統合ハブ は、コード署名を使用して、プラットフォームで生成された動的コンテンツに署名し、アプリケーションデータの重要な部分を検証できます。

ヒント:

タイムスタンプにより、証明書の有効期限が切れる前にレコードが署名されている限り、証明書の有効期限が切れても署名済みレコードが期限切れにならないようになります。証明書の有効期間の周りに 4 時間の猶予期間があり、サーバー間の時間差によって証明書が意図的に無効にならないようにします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

コード署名の検証とジョブ

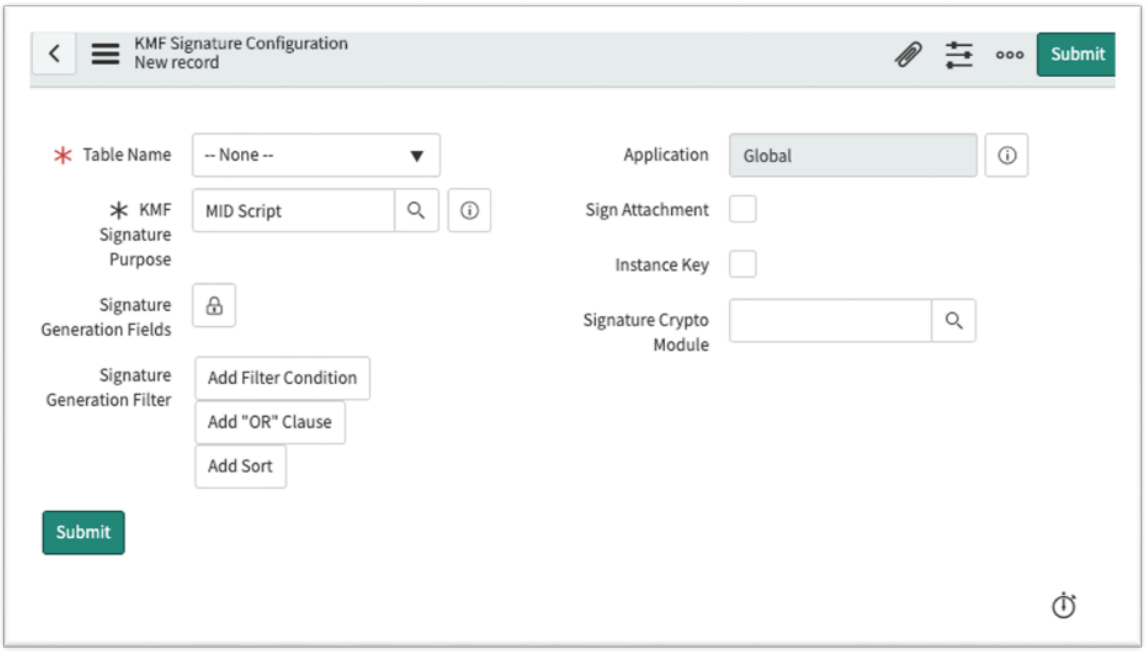
有効な構成を持つすべてのメタデータテーブルは、コード署名メタデータプラグイン (*com.glide.code_signing*) を使用してビルド時に署名されます。テーブルに署名することを選択した場合、セキュリティ管理者ロールを持つ管理者ユーザーは、コード署名暗号化ジョブにアクセスできます。

- 更新セットに署名する。
- レコードに一括署名する。
- 添付ファイルに一括署名する。

更新セットに署名する。

このジョブでは、更新セット内の署名構成に一致するレコードに署名します。このジョブでは、すべての新しい署名レコードと検証証明書も更新セットに追加します。

更新セットの **KMF** 署名レコード



レコードに一括署名する

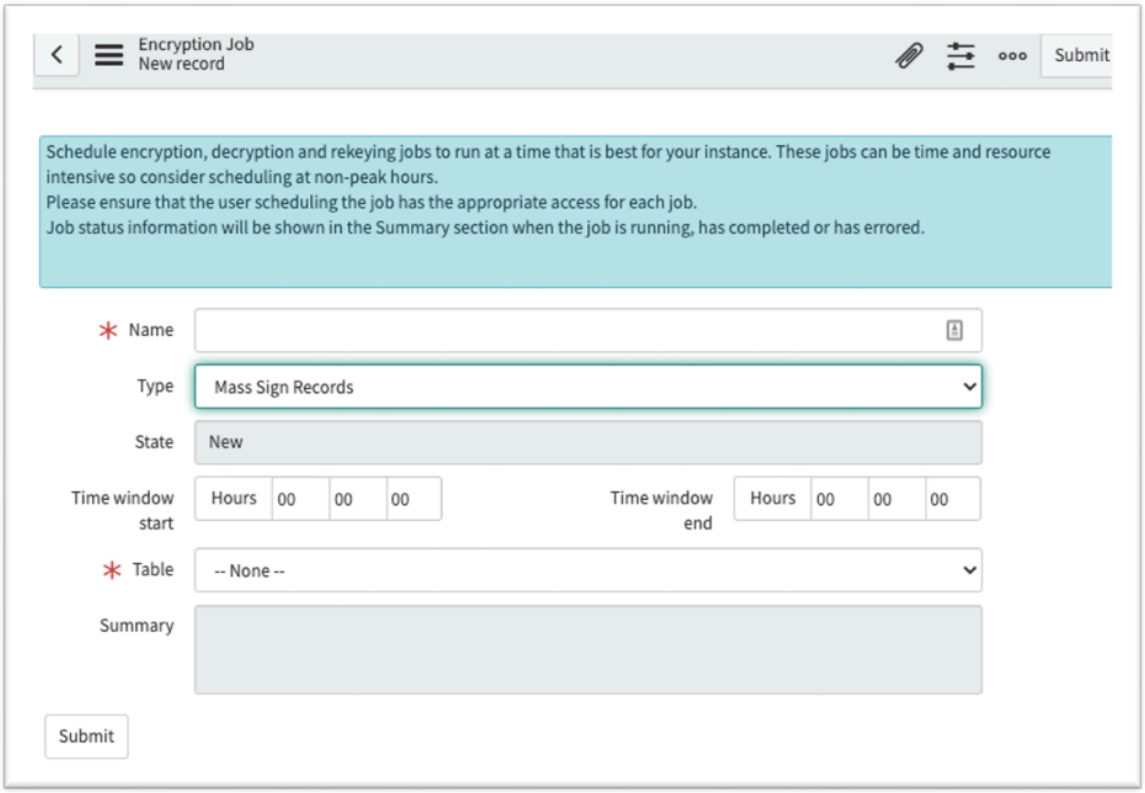
このジョブでは、特定のメタデータテーブルに適用される署名構成に一致するすべてのレコードに署名します。

添付ファイルに一括署名する

このジョブでは、指定された署名構成に一致するテーブルに添付されているすべての添付ファイルレコードに署名します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

レコードに一括署名する暗号化ジョブ



コード署名の構成

データの信頼性と完全性を確保するために、コード署名を有効にして構成します。

構成の概要

コード署名では、信頼されたインスタンスと本番インスタンス間の最初の信頼関係が必要であり、これにより、任意の認証レベルを持つ権限のないユーザーが未承認のアクティビティにアクセスするのを防ぐことができます。

コード署名で信頼のサークルを確立するための構成手順を実行するには、各トピックを参照してください。

- コード署名の有効化

  本番インスタンスにリンクする信頼できるインスタンスを識別するには、信頼できるインスタンスでコード署名を有効にします。

- コード署名キーペアと証明書を作成する

  署名付き証明書に 2 つのキーペアを作成して、本番インスタンスと信頼済みインスタンス間の信頼を確立します。

- コード署名に必要なキーペアと証明書をロードします

  コード署名を使用して、 信頼のサークル 指定された信頼できるインスタンスで関係を確立します。この最初のステップでは、暗号化キーを非本番環境にロードして、本番インスタンスの更新用の信頼できるソースを確立します。

- 信頼のサークル証明書の準備

  信頼できるインスタンスに更新セットを作成して、信頼できる証明書を本番環境にエクスポートします。

- 信頼のサークルの証明書のインポートとインストール

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

更新セットが信頼できる環境からエクスポートされた後、本番環境で更新セットを取得して、2 つのインスタンス間に信頼関係を確立します。信頼できるインスタンスで信頼を表すために作成された証明書が、本番インスタンスに受け入れられる必要があります。

ECC ファイアウォールでのカスタムルールの指定

で MID サーバー 外部通信チャネル (ECC) ファイアウォールを設定して、受信メッセージを選択的に許可または拒否するカスタムルールを作成し、コード署名設定を上書きします。

コード署名の有効化

信頼できる非本番インスタンスでコード署名をオンにして、本番インスタンスにリンクする信頼できるインスタンスを特定します。

始める前に

必要なロール：admin、security_admin

コード署名を有効にする前に、カスタマーサービス & サポートチームに連絡して Code Signing Framework [com.glide.code_signing] プラグインを有効にする必要があります。

このタスクについて

署名済み更新セットを含むコード署名ジョブは、コード署名機能を有効または無効にするために使用されます。この機能を使用するための他の方法はありません。このプロセスには以下が含まれます。

- 信頼済みで 2 つのコード署名ジョブを作成します。1 つはコード署名をオンにし、もう 1 つはコード署名をオフにします。
  - [オンにする] ジョブスケジュールは、署名済みコードの MID Server 検証プロセスを開始します。
  - [オフにする] ジョブスケジュールは、署名済みコードの MID Server 検証を停止します。

  注:
  コード署名をオフにすると、システムプロパティが **false** にマークされますが、コード署名の信頼できる友人リストは引き続き使用できます。

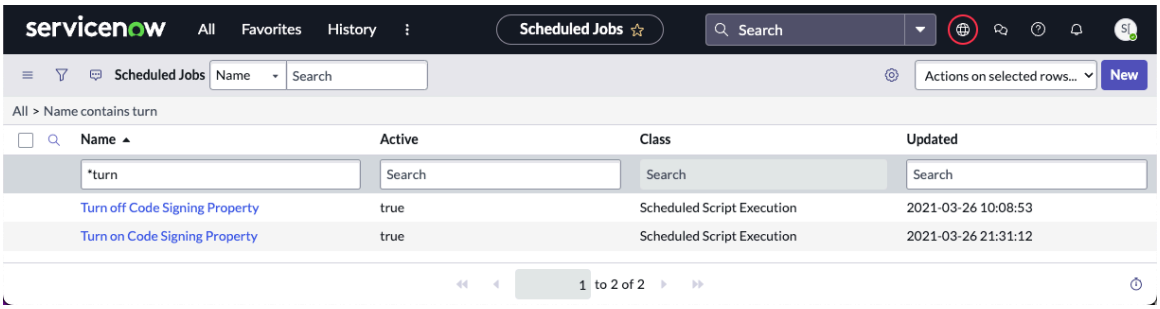
- [コード署名プロパティをオンにする **(Turn on Code Signing Property)]** ジョブを更新セットに配置します。
- ジョブを本番環境に移行します。
- 署名が信頼できる信頼できるインスタンスからのものであることが検証された場合は、本番環境で [コード署名プロパティをオンにする **(Turn on Code Signing Property**)] ジョブを使用します。

手順

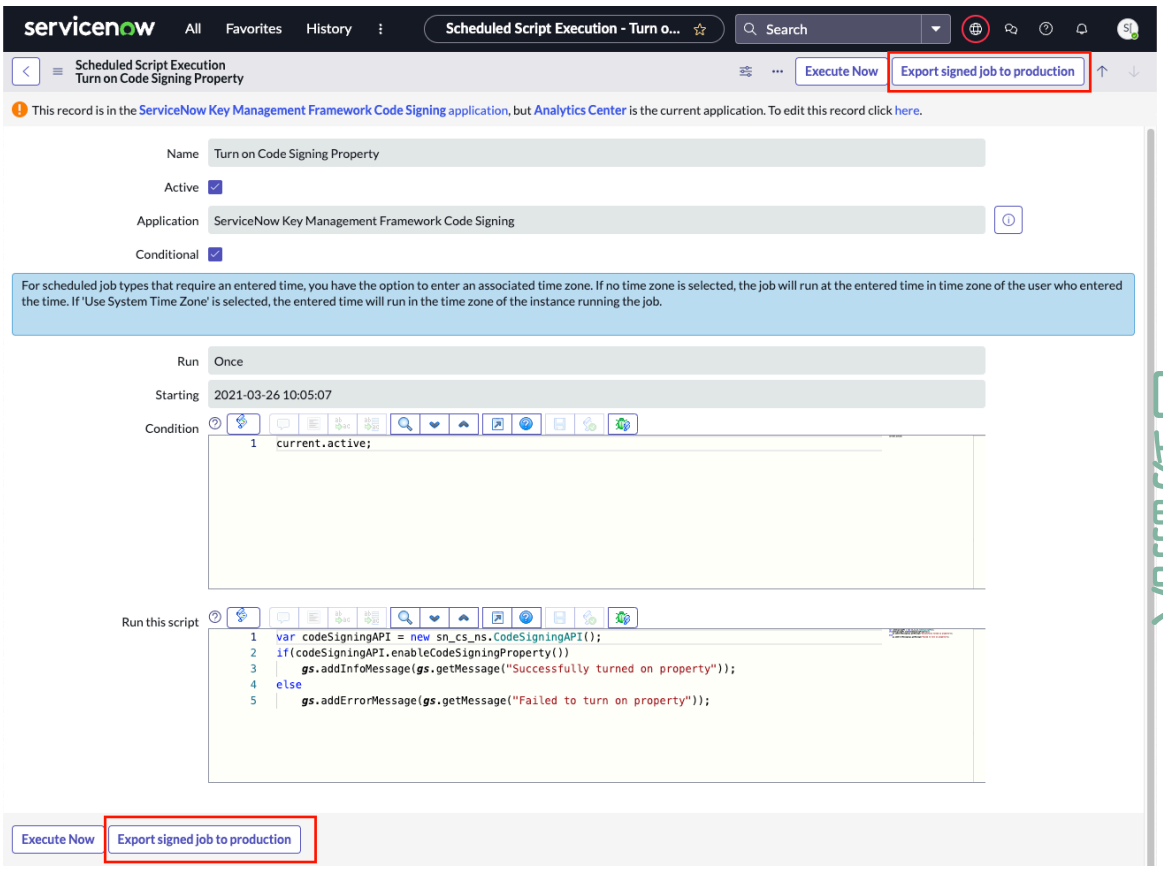
1. 信頼できるインスタンスで、次の場所に移動します。 すべて > システム定義 > スケジュール済みジョブ.
2. 名前フィールドで「*Turn」を検索します。
3. [コード署名プロパティをオンにする **(Turn on Code Signing Property)]** を選択します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



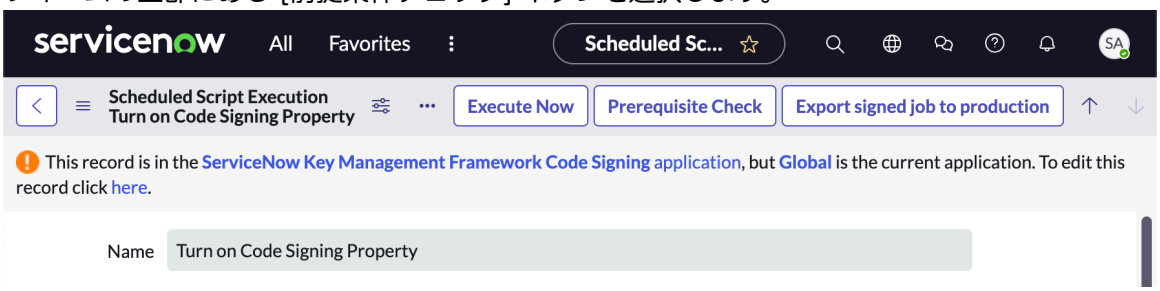
[スクリプトの実行を予定] フォームがロードされます。このフォームには [コード署名] プロパティを有効にするための情報が含まれます。ジョブは、ジョブとコード署名プロセスを介した検証済みの署名を含む更新セットを作成します。



4. スクリプトをすぐに実行するには、証明書に署名し、更新セットを作成して、[署名済みジョブを本番環境にエクスポートします] を選択します。
   指定されたスケジュールで実行するようにスクリプトを構成することもできます。
5. 移動先 システムアップデートセット > ローカル更新セット.
6. 各コード署名プロパティの更新セットを開き、**[XML** にエクスポート **(Export to XML)]** を選択します。
7. 本番インスタンスにログインします。
8. 移動先 システムアップデートセット > 取得済み **Update Sets**.
9. **[XML** から更新セットをインポート] ボタンを選択し、コード署名プロパティ更新セットを選択します。
10. [ファイルを選択] を選択し、更新セットをアップロードしてコミットします。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

11. 次に移動して、ジョブスケジュールのリストに戻ります。 すべて > システム定義 > スケジュール済みジョブ.
12. [コード署名プロパティをオンにする **(Turn on Code Signing Property)]** ジョブレコードを開きます。
13. フォームの上部にある [前提条件チェック] ボタンを選択します。



14. 前提条件の確認が完了したら、[今すぐ実行] ボタンを選択します。
[コード署名プロパティをオンにする **(Turn on Code Signing Property)]** ジョブスケジュールは、署名済みコードの MID Server 検証プロセスを開始します。
15. ナビゲーターで、「sn_kmf_record_signature.list」と入力して、**[KMF** 署名レコード] リストを開き、**[KMF** 署名の目的] が [信頼のサークル (Circle of Trust)] になっているレコードをフィルタリングします。
信頼関係によってジョブが移動され、ジョブが使用されると署名検証プロセスが実行されます。ジョブ、署名、および証明書がすべて信頼のサークルの一部である場合、 信頼のサークルを含むコード署名を有効にできます。
16. ナビゲーターで、「sys_properties.list」と入力して、システムプロパティリストを開きます。
17. *com_snc_kmf_signature.validation.flag* を検索し、値が **true** に設定されていることを確認します。
18. 新しいプロパティ *com_snc_kmf_signature.validation.certificate* がテーブルに表示されていることを確認します。

システムプロパティ

com.snc.kmf.signature.validation.certifi...	{"trust_map": {"025b4ed53d332010f877c0bf6...	string	ServiceNow Key Management Framework
com.snc.kmf.signature.validation.flag	true	true | false	Global

本番環境で信頼のサークルジョブを使用して、信頼関係を確認します。コードに署名しようとする直接ジョブは本番環境では実行できません。設定オプションについては、「」を参照してください。

コード署名をオフにする

信頼できる非本番インスタンスでコード署名をオフにして、本番インスタンスにリンクする信頼できるインスタンスを特定します。

始める前に
必要なロール：admin、security_admin

このタスクについて
署名済み更新セットを含むコード署名ジョブは、コード署名機能のオンとオフを切り替えるために使用されます。この機能を使用するための他の方法はありません。このプロセスには以下が含まれます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- 信頼できるインスタンスに 2 つのコード署名ジョブを作成します。1 つはコード署名をオンにし、もう 1 つはコード署名をオフにします。

  注:
  コード署名をオフにすると、システムプロパティは **false** に設定されますが、コード署名の信頼できる友人リストは引き続き使用できます。

- [コード署名プロパティをオフにする **(Turn off Code Signing Property)**] ジョブを更新セットに配置します。
- ジョブを本番環境に移行します。
- 署名が信頼できるインスタンスからのものであることが検証された場合は、本番環境でこのジョブを使用します。

手順

1. 移動先 すべて > システム定義 > スケジュール済みジョブ.
2. 名前フィールドで「*Turn」を検索します。

   重要:
   [コード署名プロパティをオンにする **(Turn on Code Signing Property)**] と [コード署名プロパティをオフにする **(Turn off Code Signing Property)**] の 2 つのジョブがテーブルにリストされています。これらの各ジョブでこの手順を実行します。

3. [コード署名プロパティをオフにする] を選択します。
   [スクリプトの実行を予定] フォームがロードされ、これには [コード署名] プロパティをオフにするための情報が含まれます。ジョブは、ジョブとコード署名プロセスを介した検証済みの署名を含む更新セットを作成します。
4. スクリプトをすぐに実行するには、証明書に署名し、更新セットを作成して、[署名済みジョブを本番環境にエクスポートします] を選択します。
   指定されたスケジュールで実行するようにスクリプトを構成することもできます。
5. 移動先 システムアップデートセット > ローカル更新セット.
6. 各コード署名プロパティの更新セットを開き、**[XML** にエクスポート **(Export to XML)]** を選択します。
7. 本番インスタンスにログインします。
8. 移動先 システムアップデートセット > 取得済み **Update Sets**.
9. [**XML** から更新セットをインポート] を選択し、[コード署名] プロパティの更新セットを選択します。
10. [ファイルを選択] を選択し、更新セットをアップロードしてコミットします。
11. 各更新セットを選択し、[今すぐ実行] を選択します。
12. 移動先 **KMF** 署名レコード > すべて をクリックし、 KMF の署名の目的 信頼のサークルを検索します。
    信頼関係によってジョブが移動され、ジョブが使用されると署名検証プロセスが実行されます。ジョブ、署名、および証明書がすべて 信頼のサークルの一部である場合は、コード署名をオフにする 信頼のサークル ことができます。
13. 移動先 システムプロパティ > すべての。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

14. *com_snc_kmf_signature.validation.flag* を検索し、値が **true** に設定されていることを確認します。
15. 新しいプロパティ *com_snc_kmf_signature.validation.certificate* がテーブルに表示されていることを確認します。

コード署名キーペアと証明書を作成する

署名付き証明書に 2 つのキーペアを作成して、本番インスタンスと信頼済みインスタンス間の信頼を確立します。

インスタンス間の信頼を確立するには、 cm_code_attest および cm_code_signing の各暗号化モジュールのキーペアと証明書を作成する必要があります。

キーペアと証明書の作成は、OpenSSL ツールなどのローカルデバイスにインストールされている暗号化ツールを使用して行われます。このツールの詳細については、次のリンクを参照してください https://www.openssl.org 。組織で LibreSSL や GnuTLS などの他の暗号化ツールを使用している場合は、それらの製品のドキュメントで類似した手順について参照してください。

キーペアの仕様

作成するキーペアは、これらの要件を満たしている必要があります。

タイプ	RSA
キー長	4096
署名アルゴリズム	RSASSA_PKCS1_V1_5_SHA_512

証明書の仕様

証明書は、パブリック認証局によって署名されている必要があります。

コード署名に必要なキーペアと証明書をロードします

コード署名を使用して、指定された非本番インスタンスで関係を確立します。この最初のステップでは、2 つの暗号化キーを非本番環境にロードして、本番インスタンスの更新用の信頼できるソースを確立します。

始める前に

必要なロール：sn_kmf.admin or sn_kmf.cryptographic_manager

このタスクについて

関係を確立する最初のステップは、コード署名を使用して、指定された非本番インスタンスで信頼基盤を確立することです。このタスクを実行するには、以下が必要です。

- コード署名暗号化モジュールにロードするには、2 つの 4096 ビット RSA 公開鍵/秘密鍵のペアが必要です。
  - cm_code_signing暗号化モジュール用の 1 つのペア
  - cm_code_attest暗号化モジュール用の 1 つのペア

  これらのキーの詳細については、次のリンクを参照してください コード署名キーペアと証明書を作成する。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

> **重要:**
> これらのキーペアは、パブリック認証局によって署名されているか、組織の内部認証局によって署名されている必要があります。証明書を自己署名することはできません。

- 配布証明書を含む公開鍵暗号化標準 #12 (.p12) ファイル

手順

1. キーストアからキーをインポートします。
   a. 移動先 すべて > キー管理 > 暗号化モジュール > すべて.
   b. cm_code_signing という名前の暗号化モジュールを見つけて開きます。
   c. [暗号化仕様] リストで、暗号化仕様の名前を選択して開きます。
   d. [キーストアからキーをインポート] 画面で、[キーのインポート] を選択します。
2. 最初のステップを繰り返して、cm_code_attest という名前の暗号化モジュールをインポートします。
3. [キーストアパスワードを入力してください] フィールドに、RSA 証明書の生成時に作成したチャレンジパスワードを入力します。

   > **注:**
   > 作成したチャレンジパスワードは、ここではキーストアパスワードと呼ばれます。プロセスの他の部分では、これはインポートパスワードまたはエクスポートパスワードと呼ばれる場合があります。どの場合でも、このパスワードは前の手順で作成したチャレンジパスワードと同じです。

4. [キーストア/証明書のインポート] の横にある [参照] ボタンを選択します。
5. p12 ファイル (このドキュメントの上部にある「開始する前に」セクションで説明) を選択し、[すべてダウンロード] を選択します。
6. **[OK]** を選択します。

> **重要:**
> 独自の内部認証局を使用している場合は、ステップ 5 ～ 6 のプロセスを使用して、内部認証局の中間証明書をアップロードする必要があります。

キーと証明書のインポートが成功すると、確認メッセージが表示されます。

キーと証明書が X.509 証明書 [sys_certificate] テーブルのインスタンスに存在することを検証できます。これらのレコードのタイプは [信頼ストア証明書]です。

[暗号化モジュール] [sys_kmf_crypto_module] テーブルでキーを検証できます。

次のタスク
証明書を本番環境にエクスポートします。詳細については、「」を参照してください。

信頼のサークル証明書の準備

信頼できる環境で更新セットを作成して、信頼できる証明書を本番環境にエクスポートします。

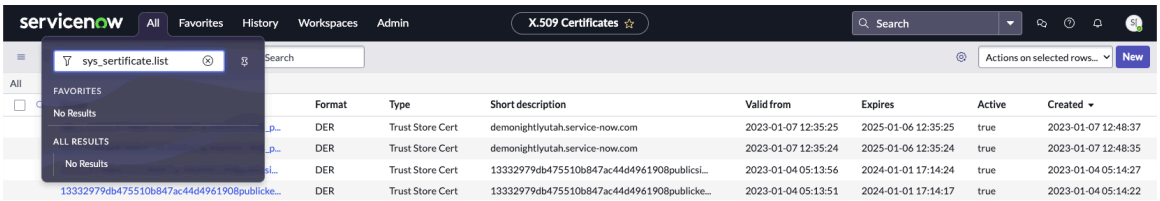
始める前に
必要なロール：admin、security_admin

自動翻訳

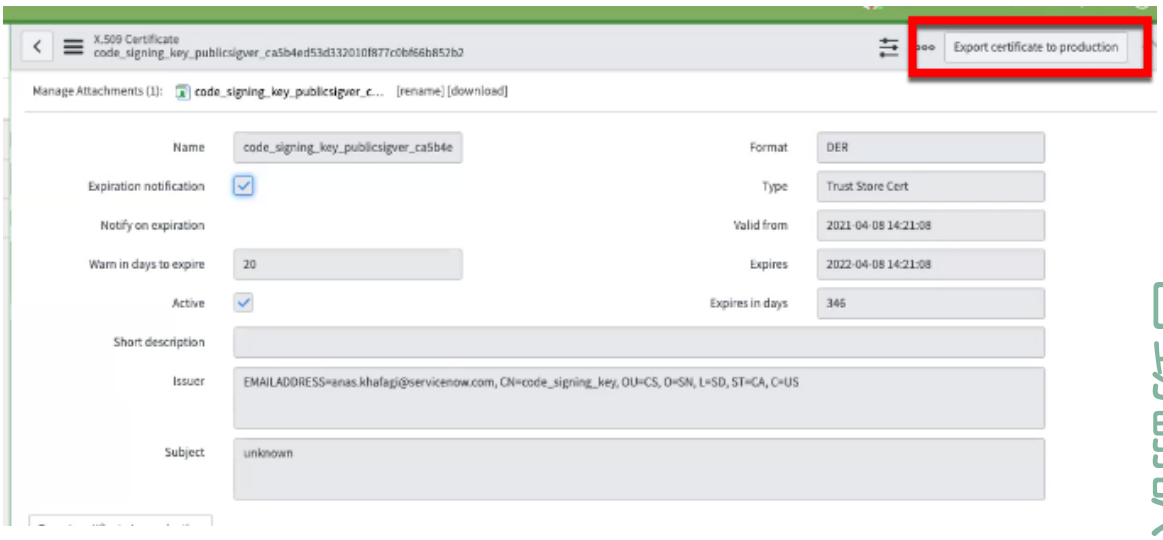
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. 信頼できる環境で、次の場所に移動します。 **sys_certificate.**リスト.



2. [信頼ストア証明書]タイプで生成された、最後に作成された X.509 証明書を開きます。
   最新のレコードを見つけるために、[作成日時] フィールドをリストに追加する必要がある場合があります。「パーソナルリスト」を参照してください。
3. [証明書を運用環境にエクスポートする] を選択します。



   証明書とともに署名が作成されます。
4. 移動先 システムアップデートセット > ローカル更新セット.
5. コード署名の更新を見つけて開きます。

   この更新は、テキスト code_signing_key_publicsigverで始まります。

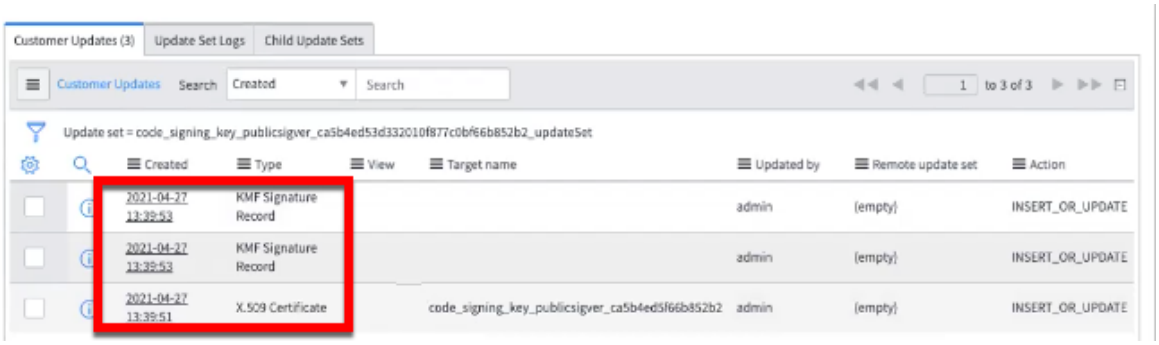
   前のステップによって、新しいコード署名更新セットレコードが作成されました。このレコードを見つけるには、[作成者] フィールドを使用してリストをソートし、[名前] フィールドでレコードを検索します。

6. 関連する署名レコードと X.509 証明書を表示します。

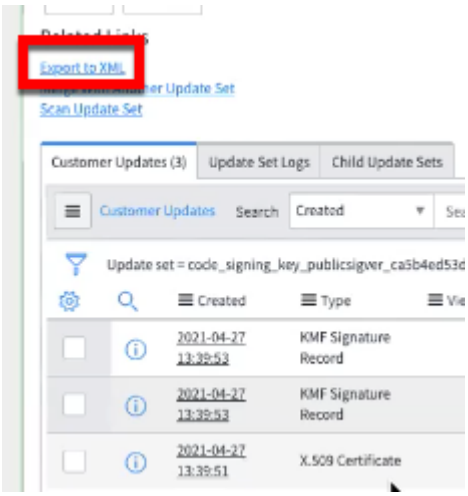
   更新セットには、署名レコードの添付ファイル、テーブル内の署名のエントリ、および証明書が含まれています。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



7. **[XML** へのエクスポート] 関連リンクを選択します。



8. 本番環境で更新セットを取得します。
詳細は、「Retrieve an update set」を参照してください。

> **重要:**
> 2 番目のキーペアに対してこれらの手順を繰り返します。cm_code_attest 暗号化モジュールと cm_code_signing 暗号化モジュールの両方にキーがあることに注意してください。

信頼のサークルの証明書のインポートとインストール

本番環境で更新セットを取得して、2 つのインスタンス間の信頼関係を確立します。信頼できるインスタンスで信頼を表すために作成された証明書が、本番インスタンスに受け入れられる必要があります。

始める前に

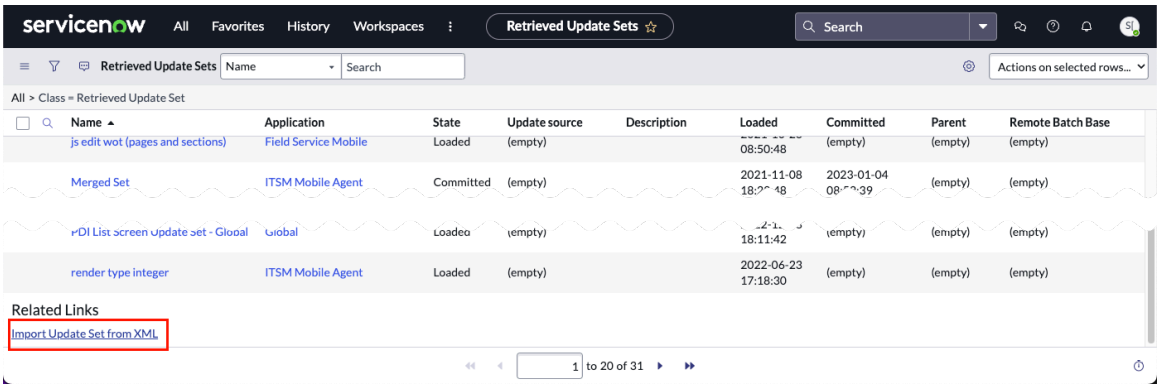
必要なロール：admin、security_admin

手順

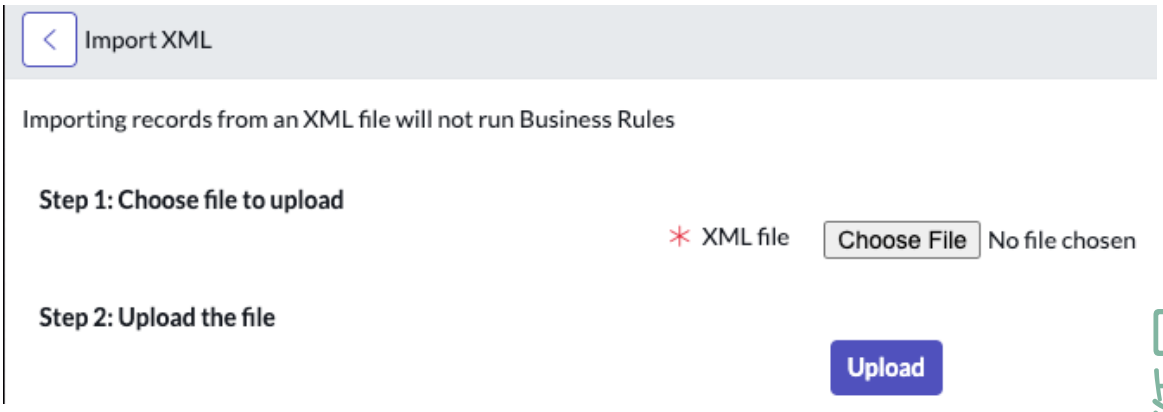
1. 本番インスタンスで、次の場所に移動します。 システムアップデートセット > 取得済み **Update Sets**.
2. 画面の左下隅にある [**XML** から更新セットをインポート] ボタンを選択します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

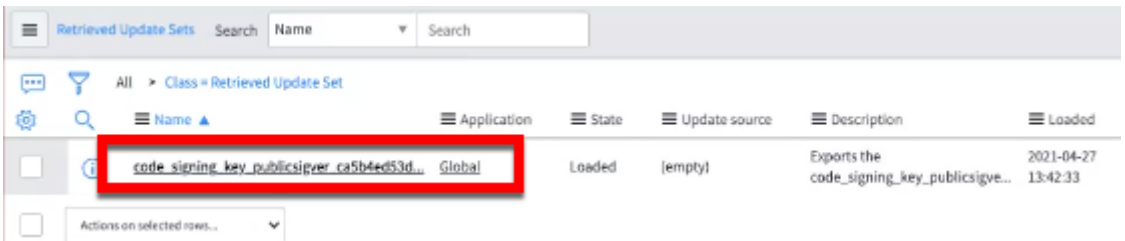
自動翻訳



3. [ファイルの選択] を選択し、 でエクスポート 信頼のサークル証明書の準備した XML ファイルを参照して選択します。



4. [Upload] を選択します。
コード署名更新セットが [取得済み更新セット] テーブルに追加されます。



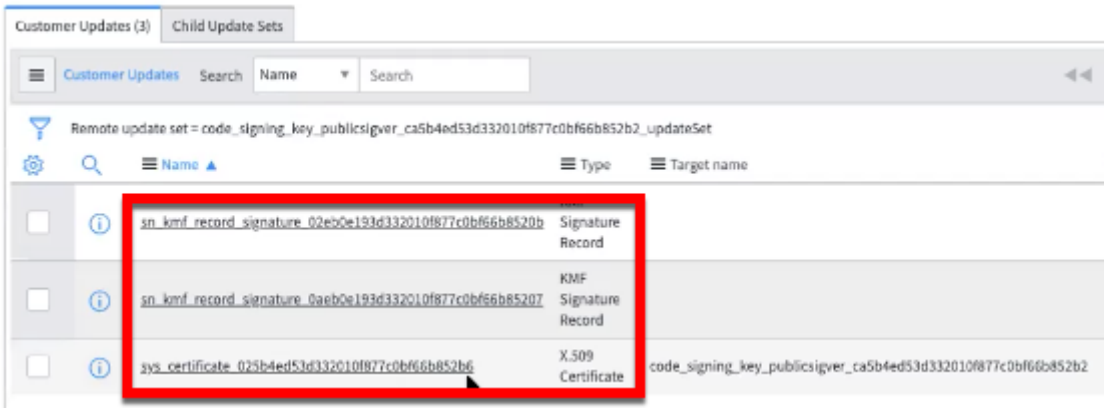
注:
更新セットが表示されない場合は、ロード済みステータスのレコードのリストをフィルタリングし、[ロード済み] フィールドでリストをソートします。

5. 更新セットレコードを開き、顧客アップデートテーブルに次の 3 つのレコードが含まれていることを確認します。

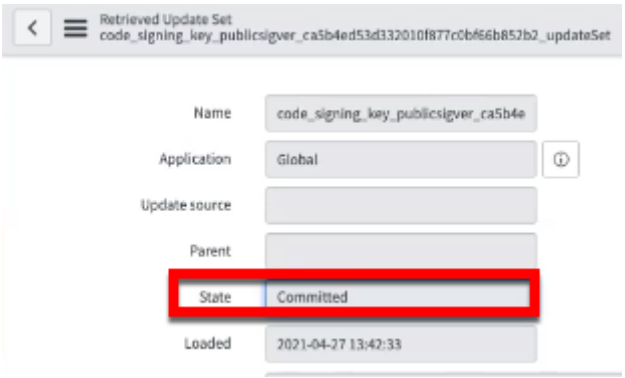
- 2 つの KMF 署名レコード
- X.509 証明書

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



6. [更新セットのプレビュー] を選択します。
7. [**Commit Update Set**] を選択します。

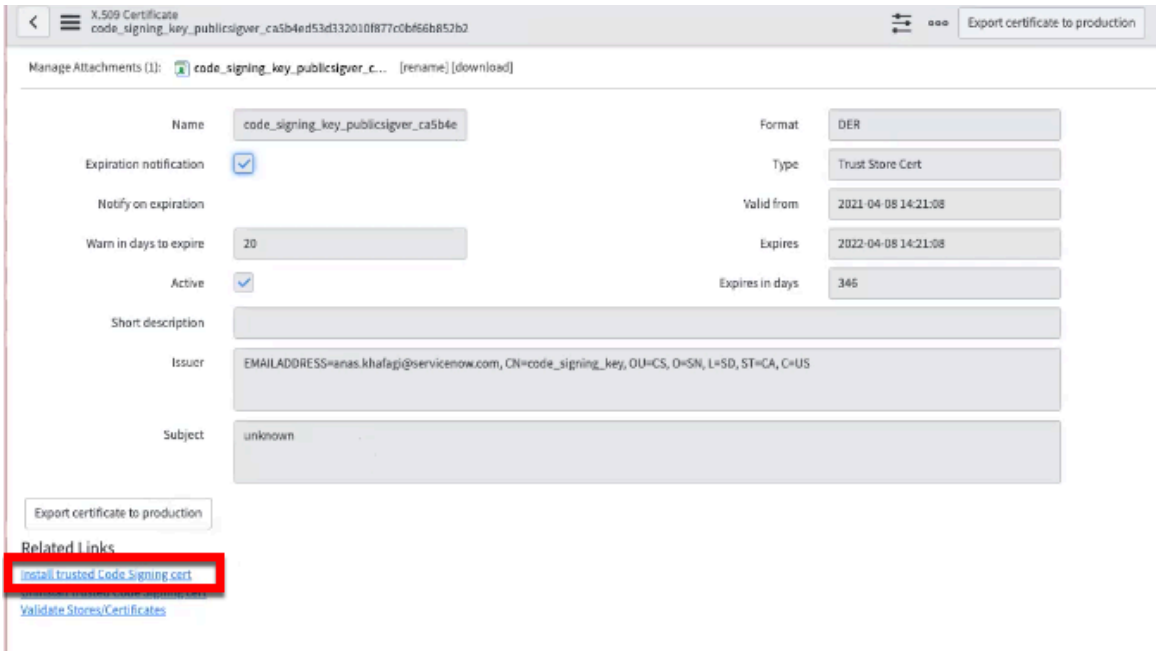


取得済み更新セットの [ステータス] が [コミット済み] に更新されます。

8. ナビゲーターで、 「sn_kmf_record_signature.list」と入力して **[KMF** 署名レコード] リストを開きます。
9. 2 つの KMF 署名レコードを見つけます。
これらのレコードは、最近作成されたレコードであり、[**KMF** 署名の目的] フィールドの値が [信頼のサークル] です。[作成済み] フィールドをリストに追加するか、現在の日付で作成されたレコードをフィルタリングする必要がある場合があります。
10. ナビゲーターで「sys_certificate.list」と入力し、[簡単な説明] の値が *[code_signing_key]* で、 [タイプ] の値が [トラストストア証明書] になっているレコードを開きます。
11. [信頼できるコード署名証明書のインストール] を選択します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



証明書タイプが [信頼できる *CodeSigning* 証明書] に更新されます。

> **重要:**
> 2 番目の証明書に対してこれらの手順を繰り返します。cm_code_attest と cm_code_signing の両方の暗号化モジュールに証明書があることに注意してください。

タスクの結果
信頼関係は、信頼できるインスタンスと本番インスタンスの間に確立されます。コード署名を有効にする準備ができました。「コード署名の有効化」を参照して手順を実行します。

ECC ファイアウォールでのカスタムルールの指定

受信メッセージを選択的に許可または拒否し、コード署名設定を上書きするカスタムルールを指定して、外部通信チャネル (ECC) ファイアウォール MID サーバー を構成します。

セキュリティ管理者は、ECC ファイアウォールタグを使用してコード署名の構成をオーバーライドし、MID サーバー に対する特定の操作を許可または拒否することができます。これらのカスタムルールは、agent/boot-config.yaml にある の YAML ファイルで指定する必要があります。

これらのタグはプロトコルに固有です。親タグに指定された構成が、子タグに適用されます。たとえば、HTTP プロトコルが許可されている場合は、REST プロトコルと SOAP プロトコルも許可されます。次の表に、使用可能な親タグと子タグを示します。

親タグ	子タグ
DNS	
HTTP	• REST • SOAP
DIRECTORY_SERVICES	LDAP
SNMP	

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

親タグ	子タグ
SSH	• SCP • SFTP
SYSLOG	
WINDOWS	• CIM • POWERSHELL • WMI • WINRM
JAVASCRIPT	
GROOVY	
VCS	GIT
DATABASES	JDBC
DATA_SOURCES	
INTEGRATION_HUB	
ITOM	• CLOUD_PROVISIONING_GOVERNANCE • DISCOVERY • EVENT_MANAGEMENT • Health_LOG_ANALYTICS • SERVICE_MAPPING
ORCHESTRATION	

自動翻訳

カスタムルールを設定するには、次のようにします。

1. MID サーバー で、boot-config-sample.yaml ファイルを見つけます。
2. YAML ファイルの名前を boot-config.yaml に変更し、そのファイルを agent/boot-config.yaml の場所に移動します。
3. YAML ファイルで、カスタムルールを指定して変更を保存します。YAML ファイルの例：

```
security:
  eccFirewall:
    mode: enforcing
    rules:
      - tags: [rest]
        action: accept
      - tags: [soap]
        action: accept
      - tags: [jdbc]
        action: reject
```

4. MID サーバー を再起動します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

信頼のルート構成の変更

信頼のルート (ROT) を使用するように変更することで、ビルド証明書 (既定) に依存する ServiceNow 代わりに、独自の証明書を信頼して使用します。 ServiceNow スクリプト インクルード、ビジネス ルールなどのコンポーネントは、ビルド時にビルド時キーを使用して ServiceNow 署名されます (検証証明書はビルド証明書です ServiceNow)。

信頼のルートを変える

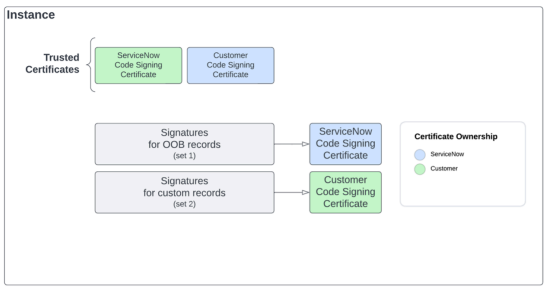
これらのレコードの署名の信頼のルートを変更するには、信頼のルートの変更プロセスに従う必要があります。

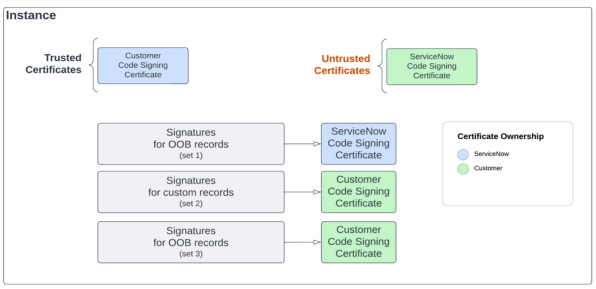
- 提供された証明書を使用して、提供されたすべてのコンポーネントの新しい署名セットを生成して移行します。
- スケジュール設定済みジョブを使用して信頼のルートプロパティを無効にします。

これらのステップの詳細については、「」およびServiceNow Root of Trust の無効化を参照してください顧客証明書を使用するための署名の移行。

署名の生成と検証プロセスへの影響

既定では、コード署名ビルド証明書は署名検証プロセス中に信頼されます。この変更を行うと、インスタンスは独自のコード署名証明書からの署名のみを受け入れます。





FALSE に設定された **ROT** プロパティ (デフォルト)	**ROT** プロパティを **true** に設定
• 検証時には、ビルド証明書を含む署名が信頼されます。 • 署名時にキーを指定しない場合、インスタンス署名キーがバックアップキーとして使用されます。 • 署名 REST エンドポイント *api/sn_kmf/signature/certificates* は、インスタンスに存在する他の証明書とともにコード署名ビルド証明書を返します ServiceNow 。	• 検証時に、ビルド証明書を含む署名は信頼されません。 • 署名時にキーを指定しないと、署名は実行されません。 • 署名 REST エンドポイント *api/sn_kmf/signature/certificates* では ServiceNow 、ビルド証明書 (San Diego、Vancouver PKI、W PKI) は除外されます。

MID Server への影響

ROT プロパティが false に設定されている場合

ROT プロパティをデフォルト値 (false) のままにすることを選択した場合、MID Server に影響はありません。

コード署名が有効で、ROT プロパティが true に設定されている場合

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- `isTrusted()` API は、ビルド証明書を含む署名に対して false を返します。
- `isTrusted()` API は、証明書を使用した署名に対して true を返します。
- 証明書の REST API 呼び出しでは、ビルド証明書は除外されます。
- 署名検証失敗メッセージなど、MID Server の問題がログに表示される場合があります。

顧客証明書を使用するための署名の移行

署名ジョブを実行して、署名を顧客の信頼のルート (ROT) に移行します。

始める前に

必要なロール:admin、security_admin、および sn_kmf.cryptographic_manager

コード署名は、本番インスタンスと信頼できるインスタンスで有効にする必要があります。**com.snc.kmf.signature.validation.flag** システムプロパティが true に設定されていることを確認することで確認できます。

この手順は、インスタンスの顧客の信頼のルート (ROT) を変更する一連の手順の一部です。このプロセスの概要については、「信頼のルート構成の変更」を参照してください。

手順

1. 本番インスタンスにログインします。
2. 移動先 すべて > システム定義 > スケジュール済みジョブ.
3. [**ROT -** 顧客証明書スケジュールを使用して署名を移行するためのレコードの更新セットを生成 **(Generate Update set of records to migrate signature using customer certificate)]** ジョブスケジュールを見つけて開きます。
4. フォームの下部にある [今すぐ実行] を選択します。
5. 移動先 すべて > システムセキュリティ > セキュリティジョブ > 新規作成.
6. プロンプトで、[署名ジョブ] を選択します。
7. [署名ジョブ] フォームで、必要に応じてフィールドに入力します。

フィールド	値
名前	ジョブの一意の名前を作成します。
タイプ	[更新セットに署名する **(Sign Update Set)]** を選択します。
テーブル	これまでのステップで作成した更新セットを選択します。更新セットの名前は change_root_of_trust_updateSet で始まります。

8. フォーム ヘッダーを右クリックし、[保存] を選択してこのレコードを保存します。
9. フォームヘッダーを右クリックし、 エクスポート > **XML** (このレコード) をクリックして、このレコードを XML ファイルとしてエクスポートします。
10. 信頼できるインスタンスにログインします。
11. 移動先 すべて > システムセキュリティ > セキュリティジョブ > すべて.
12. リストヘッダーを右クリックし、[**XML** のインポート] を選択します。
13. [XML のインポート] フォームで、[ファイルの選択] を選択し、前の手順でダウンロードした XML ファイル を選択します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

14. [アップロード] を選択します。
15. リストから、インポートされたセキュリティジョブを開きます。
16. [コード署名ジョブを本番環境にエクスポート] を選択します。
    このアクションにより、ジョブが署名され、本番インスタンスにインポートできる新しい更新セットに配置されます。

    重要:
    ジョブに署名した後、10 分以内に次の手順を実行する必要があります。この期間を超えた場合は、これらの手順を使用してジョブに再署名すると、別の署名済み更新セットが作成されます。

17. 移動先 すべて > システムアップデートセット > ローカル更新セット.
18. これまでの手順で作成した更新セットを見つけます。
    名前は SIGN_UPDATE_SET_updateSet で始まります。
19. [XML のエクスポート] を選択して、更新セットを XML ファイルとして エクスポート します。
20. 本番インスタンスにログインします。
21. 移動先 すべて > システムアップデートセット > 取得済み **Update Sets**.
22. リストの一番下で、[**XML** から更新セットをインポート] を選択します。
23. [XML のインポート] フォームで、[ファイルの選択] を選択し、前の手順でダウンロードした XML ファイル を選択します。
24. [アップロード] を選択します。
25. 移動先 すべて > システムアップデートセット > 取得済み **Update Sets**をクリックし、SIGN_UPDATE_SET_updateSetで始まる更新セットを開きます。
26. [更新セットのプレビュー] を選択します。
27. プレビューが完了したら、[更新セットのコミット] を選択します。
28. 移動先 すべて > システムセキュリティ > セキュリティジョブ > すべて.
29. インポートされたセキュリティジョブを開きます。
30. [開始] を選択してセキュリティ ジョブを実行します。

    セキュリティ ジョブが完了すると、ジョブのステータスに関する情報が [サマリー] フィールドに表示されます。

    ジョブが [完了] ステータスの場合、更新セットレコードのすべての署名で、顧客が提供した証明書を検証証明書として使用する必要があります。これは、KMF 署名レコード [sn_kmf_record_signature] テーブルで確認できます。

次のタスク
信頼のルートの構成プロセスを続行するには、「」を参照してください ServiceNow Root of Trust の無効化。

ServiceNow Root of Trust の無効化

信頼された非本番インスタンスでスケジュール設定済みジョブを実行して、信頼のルートを無効にします。

始める前に
必要なロール:admin、security_admin、および sn_kmf.cryptographic_manager

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

コード署名は、本番インスタンスと信頼できるインスタンスで有効にする必要があります。**com.snc.kmf.signature.validation.flag** システムプロパティが true に設定されていることを確認することで確認できます。

この手順は、インスタンスの顧客の信頼のルート (ROT) に変更する一連の手順の一部です。このプロセスの概要については、「信頼のルート構成の変更」を参照してください。

手順

1. 信頼できるインスタンスにログインします。
2. 移動先 すべて > システム定義 > スケジュール済みジョブ.
3. **[ServiceNow Root of Trust** の無効化 **(Disable ServiceNow Root of Trust)]** スケジュール設定済みジョブを開きます。
4. [署名済みジョブを本番環境にエクスポート] を選択します。
5. 移動先 すべて > システムアップデートセット > ローカル更新セット.
6. **[ServiceNow Root of Trust** の無効化 **(Disable ServiceNow Root of Trust)]** 更新セットを見つけて開きます。
7. [XML のエクスポート] を選択して、更新セットを XML ファイルとして エクスポート します。
8. 本番インスタンスにログインします。
9. 移動先 すべて > システムアップデートセット > 取得済み **Update Sets**.
10. リストの一番下で、[**XML** から更新セットをインポート] を選択します。
11. [XML のインポート] フォームで、[ファイルの選択] を選択し、前の手順でダウンロードした XML ファイル を選択します。
12. [アップロード] を選択します。
13. 移動先 すべて > システムアップデートセット > 取得済み **Update Sets**をクリックし、[**ServiceNow Root of Trust** の無効化 **(Disable ServiceNow Root of Trust)]** 更新セットを開きます。
14. [更新セットのプレビュー] を選択します。
15. プレビューが完了したら、[更新セットのコミット] を選択します。
16. 移動先 すべて > システム定義 > スケジュール済みジョブ.
17. 更新セットにインポートされたスケジュール設定済みジョブを開きます。
18. [今すぐ実行] ボタンを選択してジョブを実行します。

タスクの結果
スケジュール設定済みジョブを実行すると、ROT プロパティが true に設定されます。インスタンスは、顧客の信頼のルートを使用するように構成されています。

コード署名の使用

レコード、メッセージ、および添付ファイルに署名して、データの信頼性と整合性を検証する方法について説明します。

本番インスタンスで JDBC データソースレコードに署名する

本番インスタンスおよび信頼できるインスタンスでコード署名を有効にすることで、更新セットを使用して JDBC データソースに署名して検証します。

本番インスタンスで REST および SOAP メッセージに署名する

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

本番インスタンスおよび信頼できるインスタンスでコード署名を有効にすることで、更新セットを使用して REST および SOAP メッセージに署名して検証します。

本番インスタンスでフロー、サブフロー、およびアクションに署名する

本番インスタンスおよび信頼できるインスタンスでコード署名を有効にすることで、更新セットを使用してフロー、サブフロー、およびアクションに署名して検証します。

特定のレコードまたは添付ファイルへの署名

テーブル上のすべてのレコードまたは添付ファイルではなく、特定のレコードまたは添付ファイルに署名するセキュリティジョブを作成します。

スタンドアロン署名ツール

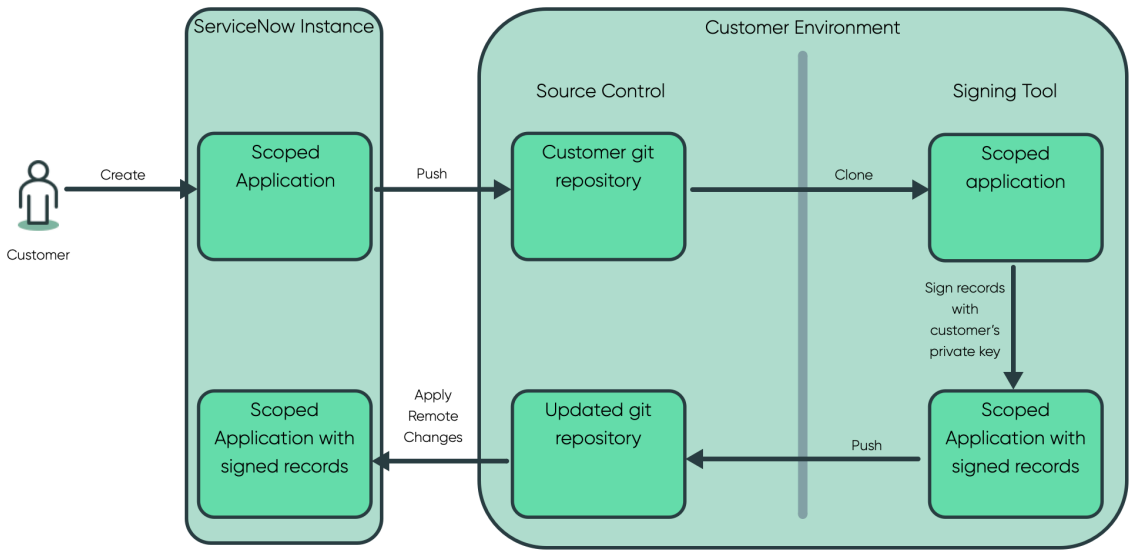
スタンドアロン署名ツールを使用して、独自の秘密鍵を使用して ServiceNow アプリケーションでサポートされているレコードに署名します。

スタンドアロン署名ツール

スタンドアロン署名ツールを使用して、独自の秘密鍵を使用して ServiceNow アプリケーションでサポートされているレコードに署名します。

署名ツールを使用して、ServiceNow アプリのレコードに署名します。このツールでは、独自の秘密鍵を使用してローカル環境のレコードの署名が生成されます。

署名ツールのワークフロー



1. ビジネスルールやスクリプトインクルードなど、署名するレコードを含む既存の ServiceNow アプリケーションを作成または選択します。
2. 環境に存在する Git リポジトリにアプリケーションをプッシュします。

   注:
   ソースコントロール統合を使用して、Git リポジトリとインスタンス間でアプリケーションを同期できます。この統合の構成と使用の詳細については、「Source Control integration」を参照してください。

3. ローカル環境でアプリケーションのクローンを作成します。
4. (同様にローカル環境で) 署名ツールを使用し、秘密鍵を使用してクローンされた ServiceNow アプリケーションからサポートされているレコードに署名します。署名ツールにより署名レコードと

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

X.509 証明書 [sys_certificate] レコードが作成されます。署名ツールの使用の詳細については、「署名ツールの使用」を参照してください。

5. 更新されたアプリケーションを Git リポジトリにプッシュします。
6. インスタンスで、リモート変更を適用することにより、更新されたアプリケーションをインポートします。

署名ツールの使用

署名ツールを使用して ServiceNow アプリケーションでサポートされているレコードに署名する方法について説明します。

始める前に

必要なロール：admin

これらのステップを実行するには、以下が必要です。

- 署名するレコードを含む ServiceNow アプリケーション
- レコードに署名するための秘密鍵
- 実行権限があるローカル環境の *signRecords.sh* スクリプト

> **重要:**
> *signRecords.sh* スクリプトは、署名ツール jar ファイルの一部として含まれます。このファイルは、次の場所から要求する必要があります ServiceNow カスタマーサポート.

手順

1. ローカル環境で *signRecords.sh* スクリプトを含むディレクトリに移動します。
2. レコードに署名するには、次のコマンド形式を使用します。

```
./signRecords.sh -d [Path to the root directory of the ServiceNow Application to Sign] -f [Path to the Keystore file]
```

例：

```
./signRecords.sh -d /users/abc/ServiceNow-App-1 -f /users/abc/codesigning.p12
```

3. プロンプトが表示されたら、キーストアのパスワードを入力します。
パスワードがない場合は Enter キーを押します。
4. 出力をレビューして、署名が成功したことを確認します。

```
Sep 26, 2022 2:41:09 PM com.snc.java.commands.ACommand start
INFO: CODESIGN: executing codesigning...
Sep 26, 2022 2:41:09 PM com.snc.core.codesigning.CodeSignerSupplier get
INFO: CODESIGN: signing record for documentId: 65e811327702111057416efe7c5a994f
Sep 26, 2022 2:41:11 PM com.snc.java.commands.ACommand start
INFO: CODESIGN: codesigning successfully completed!
```

前の出力例では、署名ツールは提供されたキーストアファイルを使用してレコードに署名しました。以下についても確認できます。

- スクリプトによりサポートされているレコード 65e811327702111057416efe7c5a994f が検出され、署名されています。
- ServiceNow-App-1 ディレクトリに、sys_certificate.xml と sn_kmf_record_signature.xml という 2 つのレコードが作成されています。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

5. スタジオ でリモート変更を適用することにより、更新されたアプリケーションをインスタンスにインポートして戻します。
   詳細については、「Apply remote changes」を参照してください。

署名ツールの引数

署名ツールで利用可能な引数について説明します。

コマンドラインの引数

引数	必須	説明
-d	はい	署名するプロジェクトのルートディレクトリ。プロジェクトディレクトリ (ランダムな 32 文字の英数字)、sn_source_control.properties ファイル、および <project_name>.iml ファイルが含まれている必要があります。
-f	はい	キーストアのファイルパス。
-a	いいえ	キーストア内の特定のエントリにアクセスするために使用されるエイリアス。
-c	いいえ	レコード署名を 1 つのファイルに連結します。
-k	いいえ	キーストア内に格納されているキーにアクセスするためのパスワード。引数内ではなく、プロンプトが表示されたときにこのパスワードを入力することもできます。
-o	いいえ	既存の sys_cert ファイルの代わりに新しい証明書を使用して署名します。
-p	いいえ	キーストアにアクセスするためのパスワード (パスワードがある場合)。引数内ではなく、プロンプトが表示されたときにこのパスワードを入力することもできます。
-w	いいえ	既存のすべての署名レコードファイルをワイプします。
-h	いいえ	このヘルプメッセージを表示して終了します。

本番インスタンスで JDBC データソースレコードに署名する

本番インスタンスおよび信頼された非本番インスタンスでコード署名を有効にすることで、更新セットを使用して JDBC データソースに署名して検証します。

始める前に

- 本番インスタンスと信頼されるインスタンスの間で確立します 信頼のサークル 。
- 必要なロール：security_admin

このタスクについて

注:

- MID サーバー はファイルデータソースを処理しないため、これらのデータソースはコード署名されていません。
- LDAP データソースはコード署名できません。

JDBC タイプの既存のデータソースに署名する

更新セットを使用して、一括署名ジョブを本番インスタンスに移動します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

手順

1. 信頼できるインスタンスで、データソースに署名するように KMF 署名ジョブを設定します。

   a. 移動先 システムセキュリティ > セキュリティジョブ > すべて.

   b. [新規] をクリックします。

   c. フォームに、これらの値を入力します。

フィールド	説明
名前	レコードを識別する名前。
タイプ	暗号化ジョブのタイプ。[レコードに一括署名する**(Mass Sign Records)**] を選択します。
テーブル	レコードの署名元のテーブル。[データソース] を選択します。

   d. [コード署名ジョブを本番環境にエクスポートする **(Export Code Signing job to production)**] をクリックします。
   更新セットが署名されたことを示す確認メッセージが表示されます。

   e. 生成された更新セットを XML ファイルにエクスポートします。

2. 本番インスタンスで、更新セットをインポートしてコミットし、信頼できるインスタンスから一括署名ジョブを取得します。

   a. 移動先 システムセキュリティ > セキュリティジョブ > すべて.

   b. 信頼できるインスタンスからエクスポートされた更新セットを開きます。

   c. [開始] をクリックします。
   レコードが署名されたことを示す確認メッセージが表示されます。

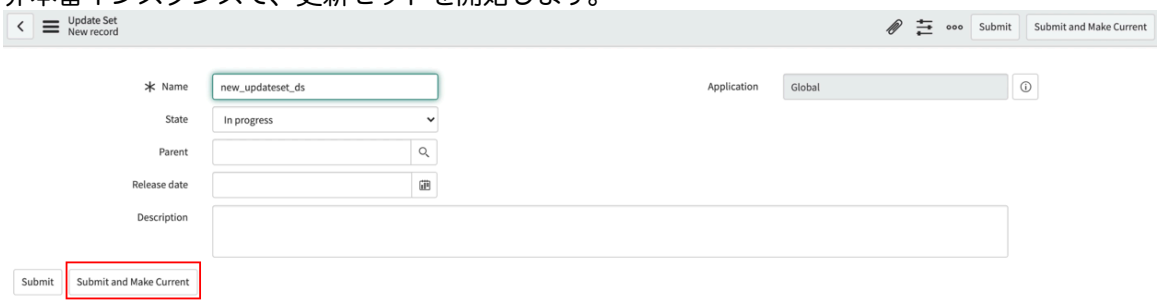
JDBC タイプの新しいデータソースに署名する

更新セットを使用して、署名済みの更新セットを本番インスタンスに移動します。

始める前に
必要なロール：sn_kmf.cryptographic_manager

手順

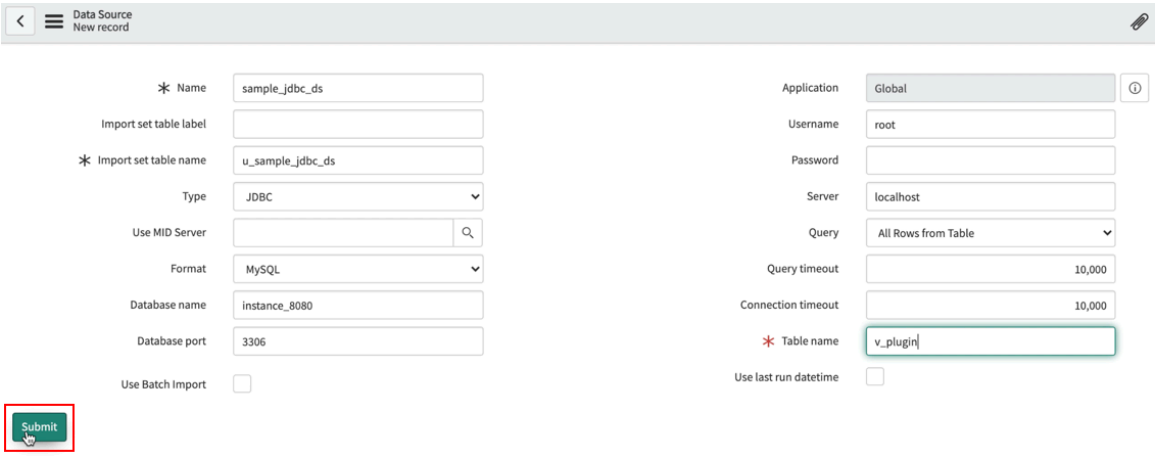
1. 非本番インスタンスで、更新セットを開始します。



© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

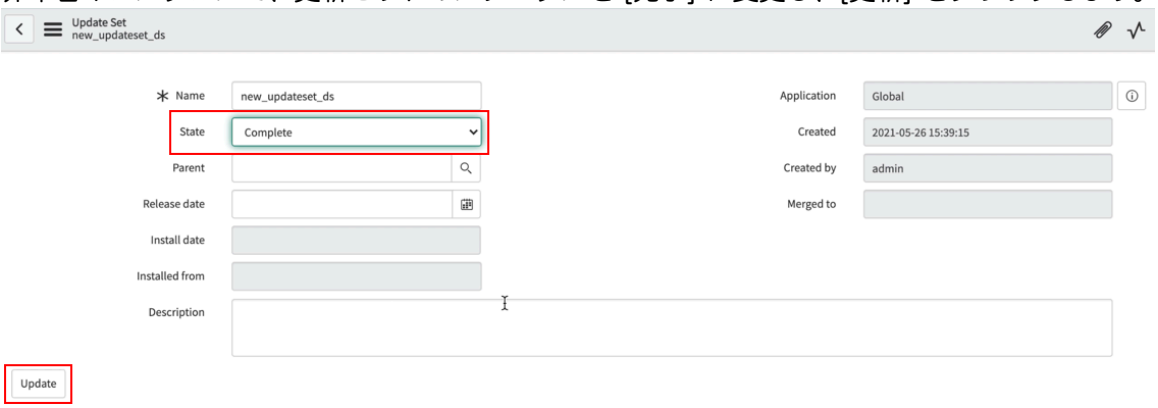
自動翻訳

2. 非本番インスタンスで、必要なデータソースを作成します。



データソースが更新セットに追加されます。

3. 非本番インスタンスで、更新セットのステータスを [完了] に変更し、[更新] をクリックします。



4. 非本番インスタンスで、暗号化ジョブを作成して更新セットに署名します。

   a. 移動先 システムセキュリティ > セキュリティジョブ > すべて.

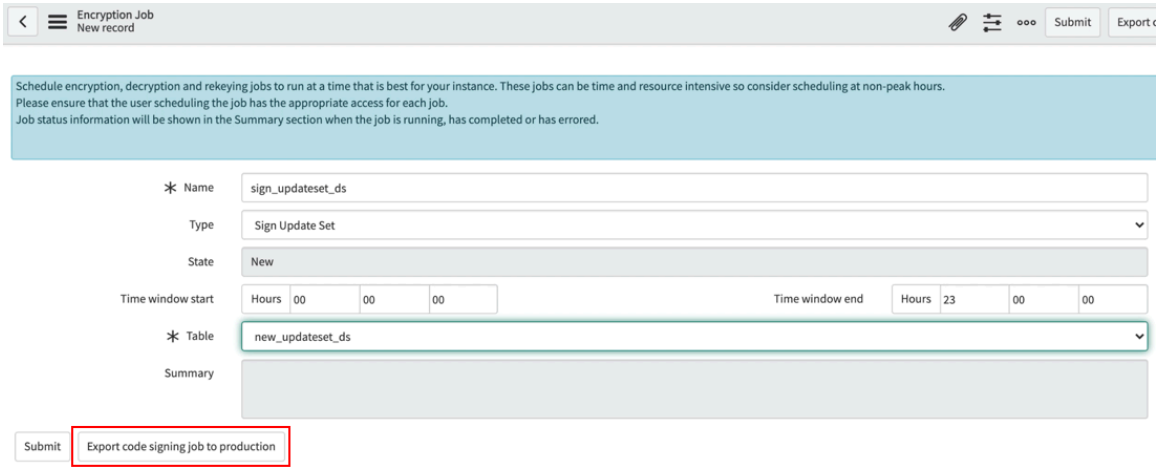
   b. [新規] をクリックします。

   c. フォームに、これらの値を入力します。

フィールド	説明
名前	レコードを識別する名前。
タイプ	暗号化ジョブのタイプ。[更新セットに署名する **(Sign Update Set)**] を選択します。
テーブル	レコードの署名元の更新セット。

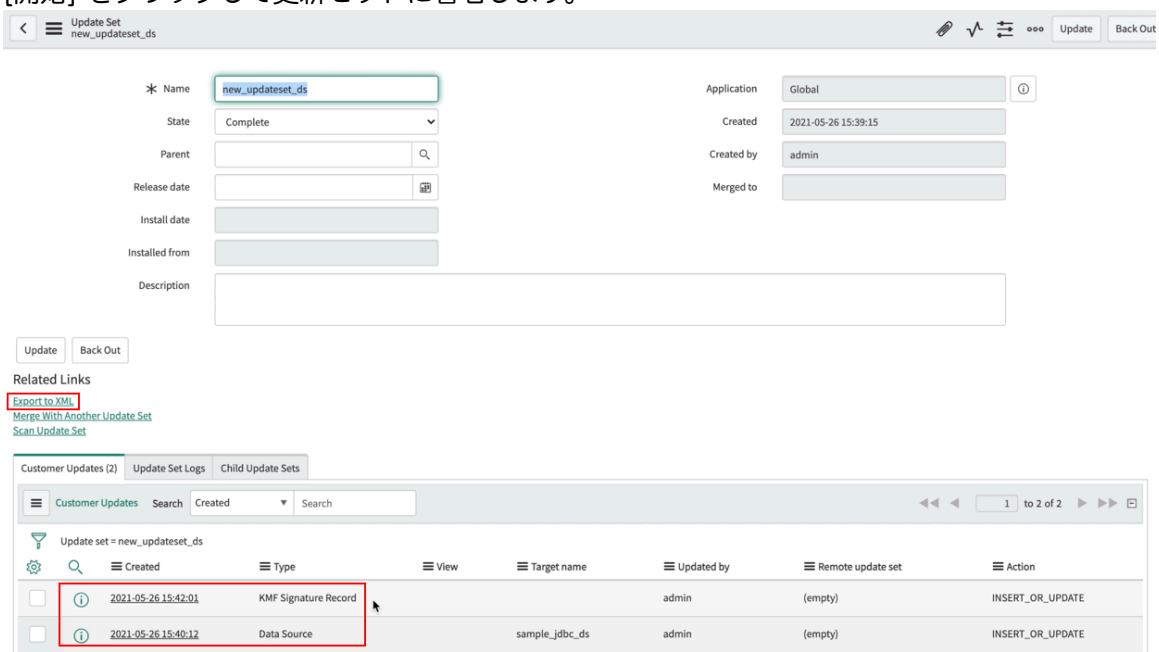
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



d. [送信] をクリックします。

e. [開始] をクリックして更新セットに署名します。



- サマリーが更新され、レコードが署名されます。
- 更新セットが更新され、署名が付加されます。

5. 非本番インスタンスで、署名付き更新セットレコードを開き、XML にエクスポートします。

6. 本番インスタンスで、更新セットをインポートして署名します。

a. 移動先 システムアップデートセット > 取得済み更新セット.

b. [XML から更新セットをインポート] 関連リンクをクリックして、信頼できるインスタンスからエクスポートされた 更新セットをインポート します。
詳細については、「クイックスタート更新セットのインポートとコミット」を参照してください。
更新セットが正常にコミットされます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

本番インスタンスで REST および SOAP メッセージに署名する

本番インスタンスおよび非本番インスタンスでコード署名を有効にすることで、更新セットを使用して REST および SOAP メッセージに署名して検証します。

始める前に

- 非本番インスタンスと本番インスタンス間に信頼のサークルを確立します。
- 必要なロール：security_admin

既存の REST および SOAP メッセージに署名する

本番インスタンスおよび信頼できる非本番インスタンスでコード署名を有効にすることで、既存の REST および SOAP メッセージに署名して検証します。

始める前に

必要なロール：sn_kmf.cryptographic_manager

手順

1. 信頼できるインスタンスで、UI アクションに署名するように KMF 署名ジョブを設定します。

a. [KMF 署名構成] に移動します。

b. フォームに、これらの値を入力します。

[KMF 署名構成] フォーム

フィールド	説明
テーブル名	Glide テーブル名。たとえば、**[UI アクション] [sys_ui_action]** を選択します。
KMF 署名の目的	レコードに署名する目的。**[ECC キュー]** を選択します。
署名生成フィールド	署名するデータソースのフィールド。これらのフィールドの 1 つ以上の値が変更されると、以前に生成された署名が無効になります。[名前] と [スクリプト] を選択します。
署名生成フィルター	レコードに署名するために満たす必要があるフィルター基準。
添付ファイルに署名	Glide レコードの添付ファイルに署名するオプション。
インスタンスキー	インスタンスキーを使用するオプション。

c. フォームヘッダーを右クリックし、[保存] をクリックします。

2. トラステッドインスタンスで、必要なレコードに署名します。

a. 移動先 システムセキュリティ > セキュリティジョブ > すべて.

b. [新規] をクリックします。

c. フォームに、これらの値を入力します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
名前	レコードを識別する名前。
タイプ	暗号化ジョブのタイプ。[レコードに一括署名する**(Mass Sign Records)**] を選択します。
テーブル	レコードの署名元のテーブル。**[UI** アクション] を選択します。

d. [コード署名ジョブを本番環境にエクスポートする **(Export Code Signing job to production)**] をクリックします。
2 つのローカルで署名された更新セットが作成されます。

- UI アクション構成用の 1 つの更新セット。
- コード署名ジョブをエクスポートするための暗号化ジョブからの別の更新セット。

3. 信頼できるインスタンスで、ローカル更新セットを XML ファイルにエクスポートします。

a. 移動先 システムアップデートセット > ローカル更新セット.

b. レコードへの一括署名用に作成した更新セットを開きます。

c. [XML へのエクスポート] 関連リンクをクリックし、XML ファイルを保存します。

4. 本番インスタンスで、更新セットをインポートします。

a. 移動先 システムアップデートセット > 取得済み **Update Sets**.

b. [XML から更新セットをインポート] 関連リンクをクリックして、信頼できるインスタンスからエクスポートされた 更新セットをインポート します。
詳細については、「クイックスタート更新セットのインポートとコミット」を参照してください。
更新セットが正常にコミットされます。

5. 本番インスタンスで、以前にトラステッドインスタンスで作成した暗号化ジョブを [開始] を選択して実行します。
レコードが署名されたことを示す確認メッセージが表示されます。

新しい **REST** および **SOAP** メッセージに署名する

本番インスタンスおよび信頼できるインスタンスでコード署名を有効にすることで、信頼できるインスタンスからの新しい REST および SOAP メッセージに署名して検証します。

手順

1. 非本番インスタンスで、更新セットを開始します。

2. 非本番インスタンスで、必要な REST または SOAP メッセージを作成します。
メッセージが更新セットに追加されます。

3. 非本番インスタンスで、更新セットのステータスを [完了] に変更し、[更新] をクリックします。

4. 非本番インスタンスで、暗号化ジョブを作成して更新セットに署名します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

a. 移動先 システムセキュリティ > セキュリティジョブ > すべて.

b. [新規] をクリックします。

c. フォームに、これらの値を入力します。

フィールド	説明
名前	レコードを識別する名前。
タイプ	暗号化ジョブのタイプ。[更新セットに署名する **(Sign Update Set)]** を選択します。
テーブル	レコードの署名元の更新セット。[新しい **Rest V2** 更新セット-1 に署名する **(Sign new Rest V2 update set-1)]** を選択します。

d. [送信] をクリックします。

e. [開始] をクリックして更新セットに署名します。

- サマリーが更新され、レコードが署名されます。
- 更新セットが更新され、署名が付加されます。

5. 非本番インスタンスで、署名付き更新セットレコードを開き、XML にエクスポートします。

6. 本番インスタンスで、更新セットをインポートします。

a. 移動先 システムアップデートセット > 取得済み **Update Sets**.

b. [XML から更新セットをインポート] 関連リンクをクリックして、信頼できるインスタンスからエクスポートされた 更新セットをインポート します。詳細については、「クイックスタート更新セットのインポートとコミット」を参照してください。
更新セットが正常にコミットされます。

本番インスタンスでフロー、サブフロー、およびアクションに署名する

本番インスタンスおよび信頼できるインスタンスでコード署名を有効にすることで、更新セットを使用してフロー、サブフロー、およびアクションに署名して検証します。

始める前に

- 本番インスタンスと信頼されるインスタンスの間で確立します 信頼のサークル 。
- 必要なロール：security_admin

既存のフロー、サブフロー、およびアクションに署名する

本番インスタンスおよび信頼できる非本番インスタンスでコード署名を有効にすることで、既存のフロー、サブフロー、およびアクションに署名して検証します。

始める前に

必要なロール：sn_kmf.cryptographic_manager

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

手順

1. トラステッドインスタンスで、ステップインスタンステーブルのレコードに署名します。

   a. 移動先 システムセキュリティ > セキュリティジョブ > すべて.

   b. [新規] をクリックします。

   c. フォームに、これらの値を入力します。

フィールド	説明
名前	レコードを識別する名前。
タイプ	暗号化ジョブのタイプ。[レコードに一括署名する**(Mass Sign Records)**] を選択します。
テーブル	レコードの署名元のテーブル。[ステップインスタンス] を選択します。

   d. [コード署名ジョブを本番環境にエクスポートする **(Export Code Signing job to production)**] をクリックします。
   2 つのローカルで署名された更新セットが作成されます。
   - KMF 署名の 1 つの更新セット。
   - コード署名ジョブをエクスポートするための暗号化ジョブからの別の更新セット。

2. 信頼できるインスタンスで、ローカル更新セットを XML ファイルにエクスポートします。
   a. 移動先 システムアップデートセット > ローカル更新セット.
   b. レコードへの一括署名用に作成した更新セットを開きます。
   c. **[XML** へのエクスポート] 関連リンクをクリックし、XML ファイルを保存します。
3. 本番インスタンスで、XML ファイルをインポートします。

   a. 移動先 システムアップデートセット > 取得済み **Update Sets**.

   b. [XML から更新セットをインポート] 関連リンクをクリックして、信頼できるインスタンスからエクスポートされた 更新セットをインポート します。
   詳細については、「クイックスタート更新セットのインポートとコミット」を参照してください。
   更新セットが正常にコミットされます。

4. 本番インスタンスで、以前にトラステッドインスタンスで作成した暗号化ジョブを実行します。
   a. 移動先 システムセキュリティ > セキュリティジョブ > すべて.
   b. 以前に信頼できるインスタンスで作成した暗号化ジョブを開きます。
   c. [開始] をクリックしてジョブを開始します。
   レコードが署名されたことを示す確認メッセージが表示されます。

新しいフロー、サブフロー、およびアクションに署名する

本番インスタンスおよび信頼できる非本番インスタンスでコード署名を有効にすることで、新しいフロー、サブフロー、およびアクションに署名して検証します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

始める前に
必要なロール：sn_kmf.cryptographic_manager

手順

1. 信頼されたインスタンスで、更新セットを開始します。
2. 信頼できるインスタンスで、必要なフロー、サブフロー、またはアクションを作成して公開します。
   フロー、サブフロー、またはアクションが更新セットに追加されます。
3. 信頼されたインスタンスで、更新セットのステータスを [完了] に変更し、[更新] をクリックします。
4. トラステッドインスタンスで、暗号化ジョブを作成して更新セットに署名します。

   a. 移動先 システムセキュリティ > セキュリティジョブ > すべて.

   b. [新規] をクリックします。

   c. フォームに、これらの値を入力します。

フィールド	説明
名前	レコードを識別する名前。
タイプ	暗号化ジョブのタイプ。[更新セットに署名する **(Sign Update Set)]** を選択します。
テーブル	レコードの署名元の更新セット。

   d. [送信] をクリックします。

   e. [開始] をクリックして更新セットに署名します。
      - サマリーが更新され、レコードが署名されます。
      - 更新セットが更新され、署名が付加されます。

5. 信頼できるインスタンスで、署名付き更新セットレコードを開き、XML にエクスポートします。
6. 本番インスタンスで、更新セットをインポートして署名します。

   a. 移動先 システムアップデートセット > 取得済み更新セット.

   b. 信頼できるインスタンスからエクスポートされた更新セットをインポートするには、[**XML** から更新セットをインポート] 関連リンクを選択します。
   詳細については、「クイックスタート更新セットのインポートとコミット」を参照してください。
   更新セットが正常にコミットされます。

特定のレコードまたは添付ファイルへの署名

テーブル上のすべてのレコードまたは添付ファイルではなく、特定のレコードまたは添付ファイルに署名するセキュリティジョブを作成します。

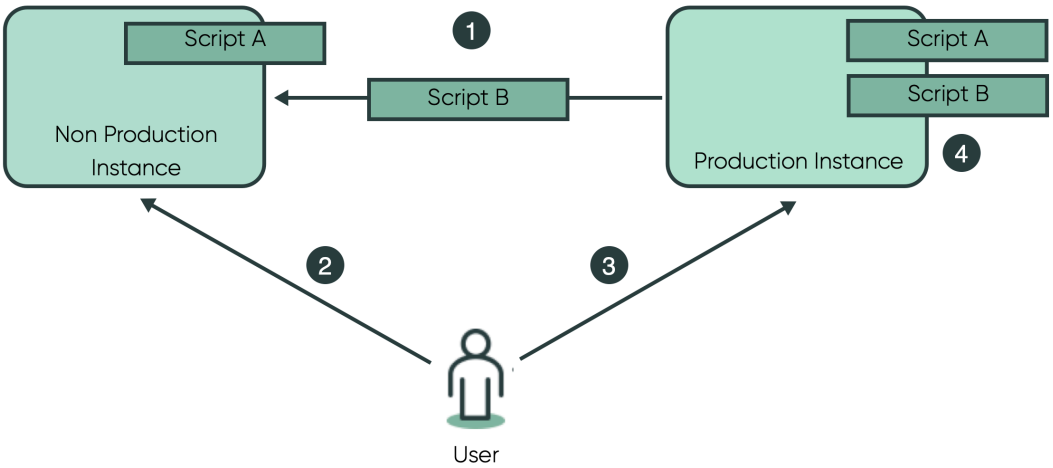
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

Vancouver リリース以降、セキュリティ管理者はセキュリティジョブを使用して、テーブルのすべてのレコードではなく、テーブルの特定のレコードに署名できます。レビュー前のコードに誤って署名しないように、特定のレコードに署名します。

これらのジョブには、署名ジョブの最後に生成される添付ログファイルが含まれています。このログファイルには、署名されたレコードと使用された署名構成に関する情報が含まれています。

署名プロセス



この図は、署名プロセスの使用例を示しています。この例では、 Script B というラベルの付いたスクリプトは本番インスタンスにのみ存在し、信頼できるインスタンスにインポートして署名する必要があります。Script A は両方のインスタンスに既に存在し、署名する必要はありません。既にレビューおよび署名されているか、まだレビューされておらず署名すべきではありません。

1. 信頼できる環境にレコードをインポートします。
2. 信頼できるインスタンスで、レコードに署名するための署名ジョブを作成します。このプロセスの詳細については、「信頼できるインスタンスで特定のレコードまたは添付ファイルに署名するジョブを作成する」を参照してください。
3. 更新セットを使用して、署名された署名ジョブを本番インスタンスにインポートします。
4. 本番インスタンスで、インポートされた署名ジョブを実行します。

信頼できるインスタンスで特定のレコードまたは添付ファイルに署名するジョブを作成する

信頼できる非本番インスタンスで定義した特定のレコードまたはレコードグループに署名します。

始める前に

必要なロール：security_admin または sn_kmf.cryptographic_manager

手順

1. 移動先 すべて > システムセキュリティ > セキュリティジョブ > 新規作成.
2. [作成するセキュリティジョブのタイプは？] プロンプトで、[署名ジョブ **(Signing Job)]** を選択します。
   新しい [署名ジョブ **(Signing Job)]** レコードが表示されます。
3. 必要に応じて、フォームのフィールドに入力します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

[署名ジョブ **(Signing Job)**] フィールド

フィールド	説明
名前	このジョブの内容を端的に表す名前。
タイプ	セキュリティジョブのタイプ。特定のレコードに署名するには、[特定のレコードに署名] オプションを選択します。特定の添付ファイルに署名するには、[特定の添付ファイルに署名] を選択します。
ステータス	このジョブのステータス。このフィールドは、[新規] という値で始まります。このフィールドは読み取り専用です。
テーブル	署名するレコードまたは添付ファイルを含むテーブル。 添付ファイルに署名する場合は、添付ファイル [sys_attachment] テーブルではなく、添付ファイルが関連付けられているレコードを含むテーブルを選択します。 ヒント: Key Management Framework (KMF) 署名レコード [sn_kmf_record_signature] テーブルをチェックして、選択したテーブルの署名がまだないことを確認します。
レコードのフィルタリング	[署名するレコードを選択 **(Select records for signing)**] テーブルに表示するレコードを制限するために使用するフィルター条件。
署名するレコードを選択	[テーブル] フィールドで選択されたテーブルのレコードリスト。[レコードのフィルタリング] フィールドで作成されたフィルターによって制限されます。 レコードを [利用可能] ウィンドウから [選択済み] ウィンドウに移動して、署名ジョブに含めます。
期間開始	このジョブを実行する期間の開始時間。ジョブは、このフィールドに入力された時間の後に実行されます。 有効な時間値は、24 時間表記に基づく世界標準時です。
期間終了	このジョブを実行する期間の終了時間。ジョブは、このフィールドに入力された時間まで実行されます。ジョブがまだ完了していない場合、ジョブは一時停止し、次の期間の開始時に再開されます。終了時間は開始時間よりも後でなければなりません 有効な時間値は、24 時間表記に基づく世界標準時です。
サマリ	このジョブの実行のサマリ。このフィールドは読み取り専用です。

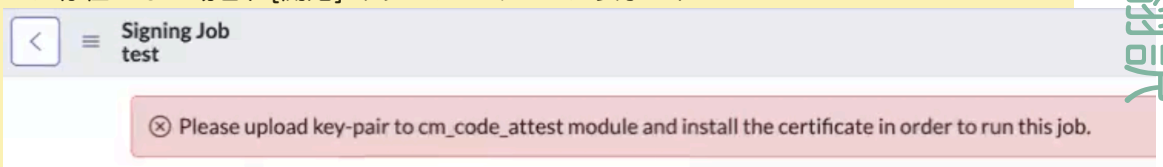
4. フォームヘッダーを右クリックし、[保存] を選択します。
5. フォームの下部で、[コード署名ジョブを本番環境にエクスポートします] を選択します。
このアクションにより、署名ジョブが署名され、エクスポートの準備が整います。
6. 移動先 すべて > システムアップデートセット > ローカル更新セット

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

7. 署名ジョブの更新セットを見つけて開きます。
   [顧客アップデート] タブで、この更新セットに署名ジョブと署名レコードが含まれていることを確認できます。
8. **[XML** にエクスポート **(Export to XML)]** を選択します。
   このアクションにより、ローカルデバイスで更新セットを含む XML ファイルが作成されます。
9. 本番インスタンスで、次に移動します。 すべて > システムアップデートセット > 取得済み **Update Sets** > **.**
10. ページの下部で、**[XML** から更新セットをインポート] を選択します。
11. [ファイルを選択] ボタンを選択し、前のステップで作成した XML ファイルを選択します。
12. [アップロード] を選択します。
    更新セットがロードされ、[取得済み更新セット] リストに表示されます。
13. [取得済み更新セット] リストで、インポートされた更新セットのレコードを開きます。
14. [更新セットのプレビュー] ボタンを選択します。
    プレビューが正常に完了すると、[更新セットのコミット] ボタンが表示されます。
15. [**Commit Update Set**] を選択します。
16. すべて > システムセキュリティ > セキュリティジョブ > すべて.
17. 署名ジョブを開きます。
18. [開始] を選択して署名ジョブを実行します。

⚠ 警告:
キーペアが本番インスタンスにアップロードされていない場合は、レコードフォームの上部に警告が表示されます。このキーペアがインスタンスに存在しない場合、[開始] ボタンはフォームに表示されません。



次のタスク
完了すると、[サマリ] フィールドにジョブの結果が表示されます。「Mass_Sign_Records-<sys_id>」という名前の署名ジョブレコードに添付されたログファイルもあります。ジョブの詳細については、このレコードと、各署名済みレコードの sys_id のリストを確認してください。

本番インスタンスで特定のレコードまたは添付ファイルに署名する

本番インスタンスで定義した特定のレコードまたはレコードグループに署名します。

始める前に
必要なロール：security_admin または sn_kmf.cryptographic_manager

このタスクについて
本番インスタンスと信頼できるインスタンスの間に信頼関係が設定されていない場合は、次のステップを使用して、本番インスタンスでレコードまたは添付ファイルに直接署名できます。インスタンス間にこの関係を作成する場合は、「コード署名に必要なキーペアと証明書をロードします」を参照してください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. 移動先 すべて > システムセキュリティ > セキュリティジョブ > 新規作成.
2. [作成するセキュリティジョブのタイプは？] プロンプトで、[署名ジョブ **(Signing Job)]** を選択します。
   新しい [署名ジョブ **(Signing Job)]** レコードが表示されます。
3. 必要に応じて、フォームのフィールドに入力します。

[署名ジョブ **(Signing Job)]** フィールド

フィールド	説明
名前	このジョブの内容を端的に表す名前。
タイプ	セキュリティジョブのタイプ。特定のレコードに署名するには、[特定のレコードに署名] オプションを選択します。特定の添付ファイルに署名するには、[特定の添付ファイルに署名] を選択します。
ステータス	このジョブのステータス。このフィールドは、[新規] という値で始まります。このフィールドは読み取り専用です。
テーブル	署名するレコードまたは添付ファイルを含むテーブル。 添付ファイルに署名する場合は、添付ファイル [sys_attachment] テーブルではなく、添付ファイルが関連付けられているレコードを含むテーブルを選択します。 ヒント: Key Management Framework (KMF) 署名レコード [sn_kmf_record_signature] テーブルをチェックして、選択したテーブルの署名がまだないことを確認します。
レコードのフィルタリング	[署名するレコードを選択 **(Select records for signing)]** テーブルに表示するレコードを制限するために使用するフィルター条件。
署名するレコードを選択	[テーブル] フィールドで選択されたテーブルのレコードリスト。[レコードのフィルタリング **(Filter Records)]** フィールドで作成されたフィルターによって制限されます。 レコードを [利用可能] ウィンドウから [選択済み] ウィンドウに移動して、署名ジョブに含めます。
期間開始	このジョブを実行する期間の開始時間。ジョブは、このフィールドに入力された時間の後に実行されます。 有効な時間値は、24 時間表記に基づく世界標準時です。
期間終了	このジョブを実行する期間の終了時間。ジョブは、このフィールドに入力された時間まで実行されます。ジョブがまだ完了していない場合、ジョブは一時停止し、次の期間の開始時に再開されます。終了時間は開始時間よりも後でなければなりません 有効な時間値は、24 時間表記に基づく世界標準時です。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
サマリ	このジョブの実行のサマリ。このフィールドは読み取り専用です。

4. [送信] を選択します。

次のタスク
セキュリティジョブは、[期間開始] と [期間終了] フィールドで指定した時間の間に実行されるか、[実行] ボタンを選択すると実行されます。完了すると、[サマリ] フィールドにジョブの結果が表示されます。「Mass_Sign_Records-<sys_id>」という名前の署名ジョブレコードに添付されたログファイルもあります。ジョブの詳細については、このレコードと、各署名済みレコードの sys_id のリストを確認してください。

コード署名の参照

参照トピックには、コード署名を管理およびトラブルシューティングするための追加情報が記載されています。

- コード署名とともにインストールされるプロパティ

  コード署名は、次のプロパティを追加します。

- トラブルシューティングとログへのアクセス

  さまざまなログにアクセスしてトラブルシューティングを行い、失敗の理由を特定します。

コード署名とともにインストールされるプロパティ

コード署名は、次のプロパティを追加します。

プロパティ	タイプ	説明
com.glide.codesigning.expanded.tracking.enabled	true|false	true の場合、**com.glide.codesigning.expanded_tracking.topic.list** プロパティにリストされている ecc_queueトピックのメタスタックの検証の長さが増加します。 **重要:** このプロパティを変更するには、昇格されたセキュリティが必要です。
com.glide.codesigning.expanded.tracking.length	整数	コード署名が有効になっている場合に発生するコード署名検証のレベル。デフォルト値は 3 です。 **重要:** このプロパティを変更するには、昇格されたセキュリティが必要です。
com.glide.codesigning.expanded_tracking.topic.list	文字列	改善されたメタスタックトラッキングの対象となるトピックのリスト (カンマ区切り)。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

プロパティ	タイプ	説明
		重要: このプロパティを変更するには、昇格されたセキュリティが必要です。
com.glide.codesigning.tracking.agent.validation.exclusion_list	文字列	コード署名をスキップする必要があるecc_queueエージェントのカンマ区切りリスト
com.glide.codesigning.tracking.debug	true | false	true の場合、コード署名トラッカーのデバッグログが有効になります。
com.glide.codesigning.tracking.enabled	true | false	true の場合、コード署名申請者追跡が有効になります。 **重要:** このプロパティを変更するには、昇格されたセキュリティが必要です。
com.glide.codesigning.tracking.logging.enabled	true | false	true の場合、コード署名追跡のログ記録を有効にします。
com.glide.codesigning.tracking.unsupported_script_tracking.enabled	true | false	true の場合、サポートされていないスクリプトを介して挿入されたecc_queueレコード (検出された場合) は認証されません。 **重要:** このプロパティを変更するには、昇格されたセキュリティが必要です。
com.glide.codesigning.tracking.validation.fail_fast	true | false	true の場合、すべてのスクリプトを検証するのではなく、最初のスクリプト検証エラーでコード署名の検証が失敗します。 **重要:** このプロパティを変更するには、昇格されたセキュリティが必要です。
com.glide.event_handler.code_signing.tracking	文字列	コード署名を新たに有効にする顧客が可能な限り安全になるように設定するためのイベントハンドラーを定義します。 **重要:** このプロパティを変更するには、昇格されたセキュリティが必要です。
com.glide.web_service_outbound.impl.code_signing.tracking	true | false	true の場合、SOAPMessageV2 コード署名追跡を有効にします **重要:** このプロパティを変更するには、昇格されたセキュリティが必要です。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

プロパティ	タイプ	説明
com.snc.csf.servicenow_root_of_trust.disabled	true | false	信頼のルート機能がアクティブかどうか。既定値は false で、ビルド証明書が信頼されていることを意味します ServiceNow 。 **重要:** このプロパティは、管理者、セキュリティ管理者、および KMF マネージャーのロールを持つユーザーからの署名済みジョブスケジュールを使用してのみ変更できます。信頼のルートの変更の詳細については、「」を参照してください 信頼のルート構成の変更。
com.snc.kmf.signature.validation.optin	true | false	true の場合、インスタンスでコード署名が有効になります。 **重要:** このプロパティは、への カスタマーサービス & サポート要求によってのみ変更できます。詳細については、「KB1205749」を参照してください
glide.jdbcprobeloader.tracking	true | false	JDBC データソースのコード署名のオンとオフを切り替えます。 **重要:** このプロパティを変更するには、昇格されたセキュリティが必要です。
glide.rest.codesigning.tracking	true | false	true の場合、RESTMessageV2 コード署名の追跡が有効になります。 **重要:** このプロパティを変更するには、昇格されたセキュリティが必要です。

トラブルシューティングとログへのアクセス

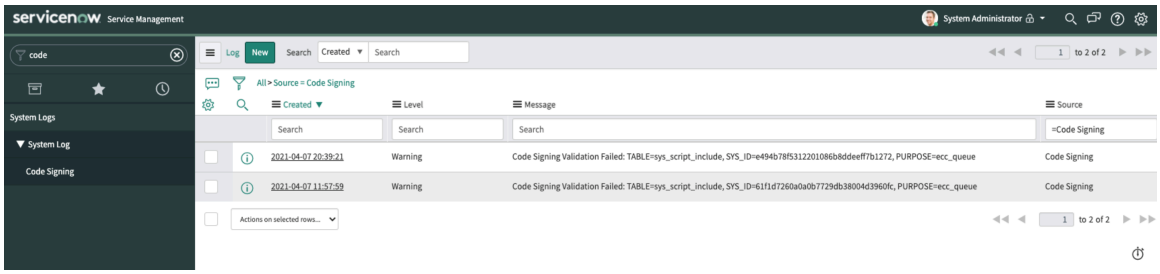
さまざまなログにアクセスしてトラブルシューティングを行い、失敗の理由を特定します。

コード署名ログ

ECC キューレコードのいずれかがコード署名トラッカー API によって署名されていない場合、署名されていないメッセージと必要な詳細がコード署名モジュールに表示されます。移動先 システムログ > システムログ > コード署名 をクリックして、信頼されていないレコードリストにアクセスします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

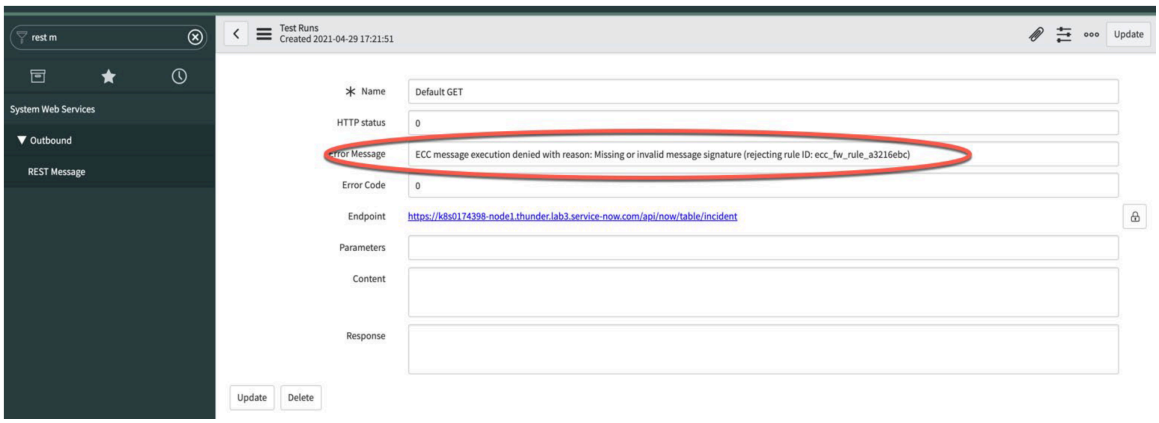


追加のデバッグノードログを表示するには、*com.glide.codesigning.tracking.debug* を有効にし、その値を true に設定します。

MID サーバー での REST メッセージ署名の検証の失敗

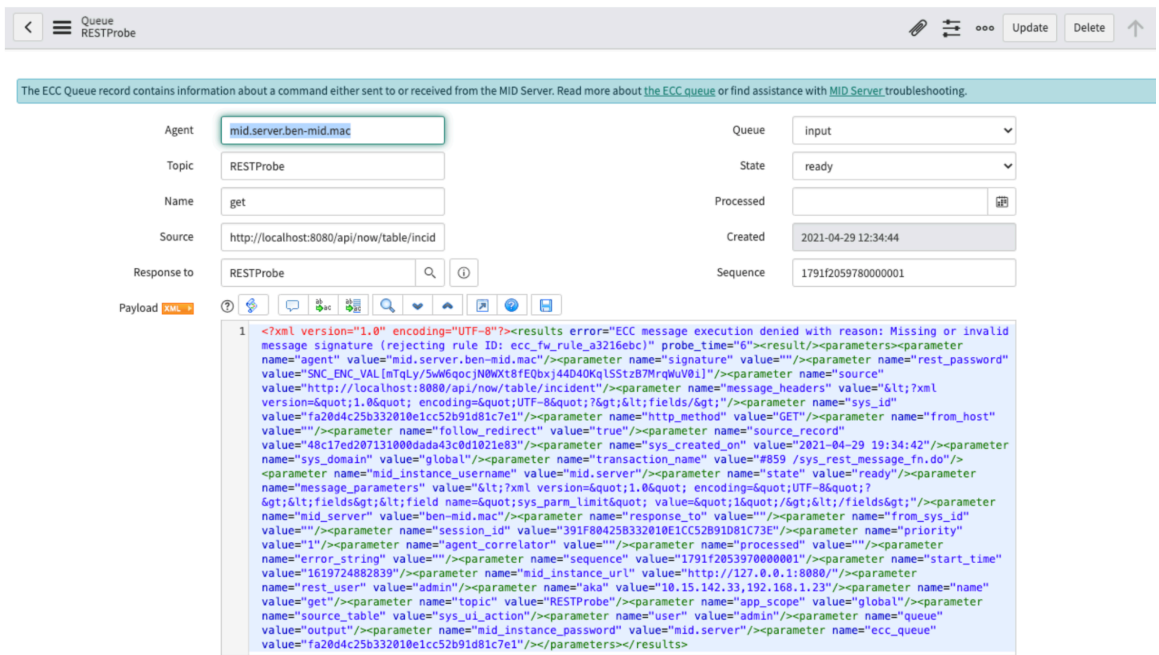
署名検証の失敗に関するエラーメッセージにアクセスするには、 次に移動します。 システム **Web** サービス > 送信 > **REST** メッセージ 必要な REST メッセージレコードを開きます。

MID サーバー での署名検証の失敗



注:
ECC ファイアウォール拒否に関連するエラーメッセージは、最初が「ECC メッセージの実行が拒否されました (ECC message execution denied)」です。

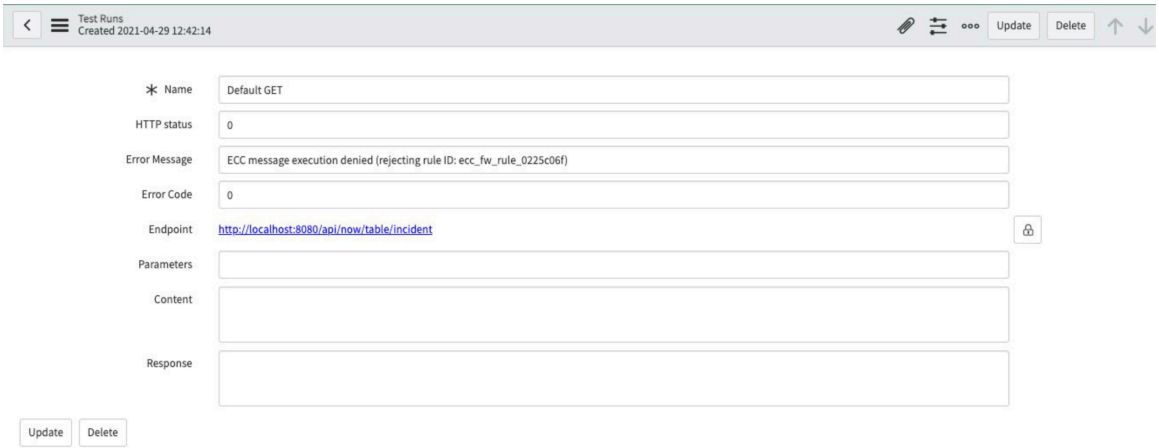
MID サーバー で署名検証に失敗した場合の ECC キュー



自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

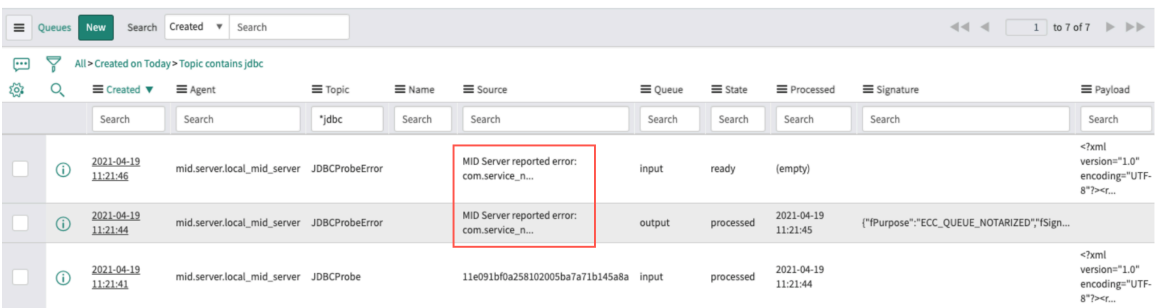
ユーザールールによって **ECC** メッセージがブロックされた場合のエラーメッセージ



JDBC プローブ

署名が無効または欠落している JDBC データソースが MID サーバー で実行された場合、必要な詳細を含むエラーメッセージが表示されます。

ソースには、エラーメッセージの詳細も表示されます。



MID サーバー ログ

詳細な ECC ファイアウォールログ記録を有効にするには、MID Server 構成パラメーター *mid.log.level* の値を TRACEに設定します。詳細ログは、次の情報を提供します。

- MID サーバー がブート構成ファイルからロードしたルール。
- ルールの詳細な実行トレース。
- ECC メッセージが承認または却下された原因となった特定のルール。

注:
boot-config.xml が無効な場合、MID サーバー は起動に失敗し、失敗の詳細が MID エージェントログに記録されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

セキュリティロール

セキュリティロールによりセキュリティを強化するためには、ユーザー全員に少なくとも 1 つのロールを割り当てて、インスタンスが内部ユーザーと外部ユーザーを区別できるようにする必要があります。

明示的なロールの詳細

明示的なロールの主な機能とビジネス価値について学びます。

昇格された特権の詳細

昇格された権限ロールでセッションベースの権限を有効にする方法について説明します。

自動翻訳

明示的なロール

内部ユーザーと外部ユーザーの両方に、インスタンスへのアクセス権を与えることができます。ただし、両方のタイプのユーザーに同レベルのアクセス権を持たせない方が良い場合もあります。セキュリティを追加するためには、ユーザー全員に少なくとも 1 つのロールを割り当てて、インスタンスが内部ユーザーと外部ユーザーを区別できるようにする必要があります。

Parisリリース時点では、ユーザーは、明示的なロール (snc_internal および snc_external) をともに持つことはできません。グループとロールには、そのようなグループまたはロールにアサインされたグループメンバーまたはユーザーが両方のロールを自動的に持つようになるため、両方のロールを包有することはできません。Now Platform では、このようなシナリオを作成する操作はすべて中断されます。

外部ユーザーは、少なくとも snc_external ロールを取得する必要があります。snc_external ロールは、ユーザーが組織の外部にいることを示します。こうしたユーザーは、リソースへのアクセス権を持つことはできません。ただし、ACL を通じて snc_external ロールか、または snc_external ロールを継承する追加ロールに対して明示的に許可された場合は例外です。 デフォルトでは、snc_external ロールを持つユーザーは次のものにアクセスできません。

- 外部とマークされていない Scripted REST APIs リソース。
- snc_external ロールまたは公開ロールを継承するロールがないテーブル。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- snc_external ロールまたは snc_external ロールを継承するロールへのアクセスの許可がないプロセッサーや UI ページなど、レコードタイプ以外のリソース。
- Now Intelligence ダッシュボード

snc_internal ロールを昇格したロールとしてマークしないでください。内部ユーザーがインスタンスにアクセスできなくなります。

明示的ロールプラグイン

明示的ロールプラグインが有効になっている場合：

- すべての ユーザーは、内部リソースにアクセスするための snc_internal ロール、または外部リソースにアクセスするための snc_external ロールを持つ必要があります。いずれの明示的もロールを持たないユーザーは、公開リソースにのみアクセスできます。
- 既存のユーザー全員に、snc_internal ロールが自動的にアサインされます。このロールでは、既存のアクセスレベルやシステムの動作は変更されません。その代わり、内部ユーザーと外部ユーザーを区別するためのカテゴリが提供されます。内部ユーザーは全員、プラグインが有効化される前と同レベルのアクセスを維持します。

  ヒント:
  ユーザーの既存の機能を変更しないようにするために、明示的なロールプラグインが有効になると、インスタンス内の既存ユーザー全員に snc_internal ユーザーロールがアサインされます。既存ユーザーには、明示的なロールプラグインが有効になる前に追加された外部ユーザーも含まれます。明示的ロールプラグインが有効になった後、明示的ロールプラグインの有効化以前に追加されたすべての外部ユーザーに対して、以下を実行します。
  - snc_internal ロールを削除します。
  - snc_external ロールを追加します。

  これにより、明示的なロールプラグインを有効化する前に追加されていた外部ユーザーは、内部ユーザーのみが使用できる内部リソースにはアクセスできなくなります。

- 新しく作成されたユーザーは、最初にインスタンスにログインしようとした時点で snc_internal ロールが自動的にアサインされますが、snc_external ロールが明示的にアサインされている場合は例外です。新しいユーザーがインスタンスに最初にログインする前に snc_external ロールを追加すると、外部ユーザー権限を提供することができます。

  重要:

  メインテナンス期間中またはログインしているユーザーが少ないときに、このプラグインを有効にします。プラグインが有効化されているときに現在ログインしているユーザーには、snc_internal ロールは動的にアサインされません。むしろ、ユーザーは snc_internal ロールをアサインするために、ログアウトして再度ログインする必要があります。プラグインが有効化されると、snc_internal および snc_external ロールをいつでも追加または削除して、ユーザーの権限を変更できます。

  プラグインが有効になると、ユーザーがログインするたびに、アカウントに snc_internal ロールが付与され (ない場合)、snc_external ロールが付与されます。これには、代理操作を介してログインしたユーザーが含まれます。

- ロール要件を持たないすべての既存の ACL に、snc_internal ロールが自動的にアサインされます。既存の ACL とユーザーの両方に snc_internal ロールがアサインされているため、既存のアクセスレベルは変更されません。
- ロール要件を持たない新規作成 ACL には、snc_internal ロールが自動的にアサインされます。このロールは、新規作成 ACL にロールがアサインされている場合にはアサインされません。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- **Type=script** のすべての既存のプロセッサー [sys_processor] レコードまたは新しく作成されたプロセッサー [sys_processor] レコードについては、フィールドが空の場合、snc_internal ロールが [ロール] フィールドに自動的に追加されます。
- UI ページへのアクセスを内部ユーザーに制限する場合、プラグインによって **ui_page** タイプの* ACL に snc_internal ロールが自動的に割り当てられます。
- プロセッサーへのアクセスを内部ユーザーに制限する場合、プラグインによって **ui_page** タイプの* ACL に snc_internal ロールが自動的に割り当てられます。
- 外部ユーザーがインスタンスにアクセスするためには、少なくとも snc_external ロールを取得する必要があります。このロールは、外部ユーザーに手動で付与する必要があります。レコードへのアクセスは、ACL を通じて付与されます。

明示的なロールプラグインが有効であるかどうかにかかわらず、システム更新セットをインスタンス間で移動しないでください。詳細については、「System Update Sets」を参照してください。

注:
このプラグインには、Contextual Security Manager プラグインも必要です。

外部ユーザーへのテーブルアクセスの提供

snc_external ロールを継承するロールをテーブルに追加することで、外部ユーザーにテーブルへのアクセス権を付与できます。詳細については、「Provide external users access to a table」を参照してください。

hasRoles() メソッド

hasroles() メソッドはまだ利用できますが、 Geneva リリースでは廃止されます。代わりに hasRole(ロール名) メソッドを使用します。

hasRoles() メソッドを使用する場合は、次のような変更に注意してください。

- この方法では、ロールをチェックする際にデフォルトの snc_internal ロールが自動的に除外されます。これは、ユーザーが snc_internal ロールしか持っていない場合でも、hasRoles() メソッドが **false** を返すことを意味します。
- ユーザーが snc_external ロールを持っている場合、インスタンスは外部ユーザーがロールを持たないと判断するため、このメソッドは **false** を返します。

相互除外：**snc_external** 対 **snc_internal**

Now Platform では、snc_external ロールと snc_internal ロールの両方をユーザーに付与することはできません。Now Platform では、 システム内のすべての場所でこの相互除外が適用され、エラーメッセージが各競合のログに書き込まれます。

注:
ACL リソースにすべてのユーザーがアクセスできるようにするには、ACL に両方のロールを含めます。

例：ユーザーに明示的なロールの両方を追加 (直接衝突)：

1. ユーザー Abel Tuter に snc_internal ロールをアサインします。
2. ユーザー Abel Tuter に snc_external ロールをアサインします。

結果：Abel Tuter は snc_internal ロールを持つため、snc_external ロールの追加に失敗しました。

例：グループに両方の明示的なロールを追加 (直接衝突)：

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

1. 現在グループに割り当てられている明示的なロールがないテストグループと呼ばれるグループを検討してください。
2. テストグループにアベル、担当 tuter を追加します。
3. テストグループに snc_external ロールを追加します。

結果：Abel Tuter はすでに snc_internal ロールを持っており、両方のロールを持つことはできないため、snc_external ロールの追加に失敗しました。

例：グループメンバーが競合する明示的なロールを持つグループに明示的なロールを追加します (間接衝突) ：

1. ユーザー Abel Tuter に snc_internal ロールをアサインします。
2. 現在グループに割り当てられている明示的なロールがないテストグループと呼ばれるグループを検討してください。
3. テストグループにアベル、担当 tuter を追加します。
4. snc_external ロールをテストグループに追加します。

結果：Abel Tuter はグループメンバーシップを通じて snc_external ロールを継承するため、グループに snc_external ロールを追加することはできません。両方の明示的なロールが同じユーザーに割り当てられます。これは許可されていません。

その他の例については、次のテーブルを参照してください。

ロール	試行したアクション	結果
直接衝突		
ユーザーは snc_internal ロールを持っています。	snc_external ロールを追加します。	アクションが中断されました。
ユーザーは snc_external ロールを持っています。	snc_internal ロールを追加します。	アクションが中断されました。
ユーザーに明示的なロールがありません。	snc_external と snc_internal の各ロールを追加します。	ロールが追加されました。
ユーザーは、両方の明示的なロールを持ちます (衝突が存在します) 。	ロールを持たないグループにユーザーを追加してください。	アクションが中断されました。
どのユーザーにも関連付けられていないロールに、snc_internal ロールが含まれています。	snc_external ロールを追加します。	アクションが中断されました。
どのユーザーにも関連付けられていないロールには、snc_external ロールが含まれています。	snc_internal ロールを追加します。	アクションが中断されました。
ロールには、明示的なロールが含まれています (衝突が存在します) 。	ロールをユーザー、ロール、またはグループに追加します。	アクションが中断されました。
メンバーを含まないグループに snc_internal	snc_external ロールを追加します。	アクションが中断されました。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ロール	試行したアクション	結果
ロールが割り当てられています。		
メンバーを含まないグループに snc_external ロールが割り当てられています。	snc_internal ロールを追加します。	アクションが中断されました。
メンバーを含まないグループにはロールはありません。	snc_external と snc_internal の各ロールを追加します。	ロールが追加されました。
間接衝突		
衝突を包有するロール	1. snc_internal ロールを持つユーザーに Test ロールと呼ばれるロールを付与します。 2. snc_external ロールの Test ロールを追加します。	アクションが中断されました。
衝突を包有しないロール	1. ロールを持たないユーザーに Test ロールと呼ばれるロールを付与します。 2. snc_external ロールに Test ロールを追加します。	このロールは、ユーザーと Test ロールの両方に追加されます。
衝突を包有するグループ	1. snc_internal ロールを持つユーザーを、Test Group 2 (Test Group 1 の子) というグループに追加します。 2. snc_external ロールを Test Group 2 に追加します。 3. snc_external ロールを Test Group 1 (Test Group 2 の親) という親グループに追加します。	アクションが中断されました。
衝突を包有しないグループ	1. ロールを持たないユーザーを、Test Group 2 (Test Group 1 の子) というグループに追加します。 2. snc_external ロールまたは snc_internal ロールを Test Group 1 (Test Group 2 の親) に追加します。	ロールが親グループ、子グループ、およびユーザーに追加されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ロール	試行したアクション	結果
グループとロールに衝突が包有されています	Test Group 1 (Test Group 2 の親) に contains_external を追加します。	Test Group 1 と Test Group 2 はともに contains_external を取得しますが、snc_external ロールを明示的に取得することはできません。
	Test Group 1 の子である Test Group 2 に snc_internal ロールを追加します。	アクションが中断されました。
グループの親の変更とグループの包有	1. Test Group 2 の親として Test Group 1 を削除します。 2. snc_internal ロールを Test Group 1 に追加します。 3. snc_external ロールを Test Group 2 に追加します。 4. Test Group 2 では、Test Group 1を親グループとして設定して保存します。	アクションが中断されました。 同じ想定で、既にネストされたグループに対して手順を繰り返します。

アクションの中断の原因がエラーメッセージに表示され、別の試行が成功する前に対応する必要があります。

個々のユーザーに明示的ロールを追加するなど、直接的なケースでは、ユーザーがどの明示的ロールを持つ必要があるかを確認します。ユーザーが不適切な明示的なロールを持つ場合は、まず削除し、次に正しい明示的なロールを追加する必要があります。

グループに明示的なロールを追加するなど、間接ケースでは (グループメンバーに両方の明示的なロールがアサインされるようにするために)、ユーザーをグループに含める必要があるかどうかを評価します。グループ階層とロールの包含を通じた継承を含め、グループに明示的なロールを指定する必要があるかどうかも決定します。

Now Platform では、最初に発生した衝突の可能性のみがレポートされることに注意してください。修正後も繰り返し試行が失敗し、毎回新しい根本原因が発生する場合は、関連するユーザー/グループ/ロールの相互依存関係をより広範に再評価してください。グループとロールの包有がどのように構成されているかを再考することをお勧めします。

明示的なロールを要求する

Now Support Service Catalog から明示的なロールプラグイン (com.glide.explicit_roles) を要求して明示的なロールをアクティブ化します。

始める前に
必要なロール：admin

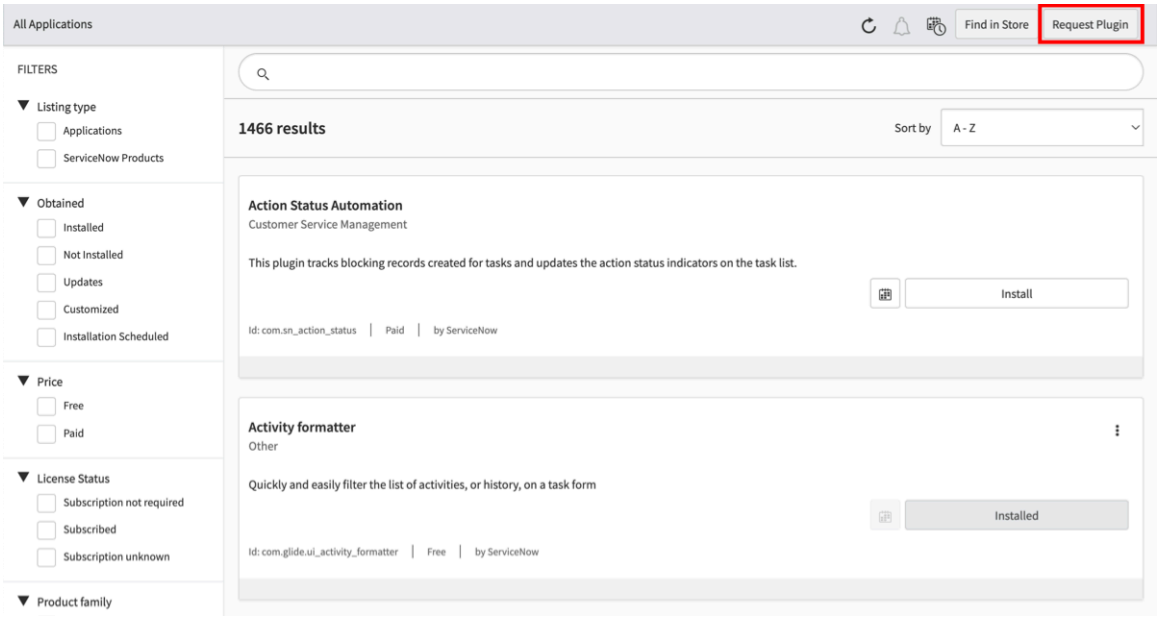
重要:
メインテナンス期間中またはログインしているユーザーが少ないときに、このプラグインを有効にします。プラグインが有効化されているときに現在ログインしているユーザーには、snc_internal ロールは動的にアサインされません。むしろ、ユーザーは snc_internal ロールをアサインするために、ログアウトして再度ログインする必要があります。プラグインが有効化されると、snc_internal および snc_external ロールをいつでも追加または削除して、ユーザーの権限を変更できます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

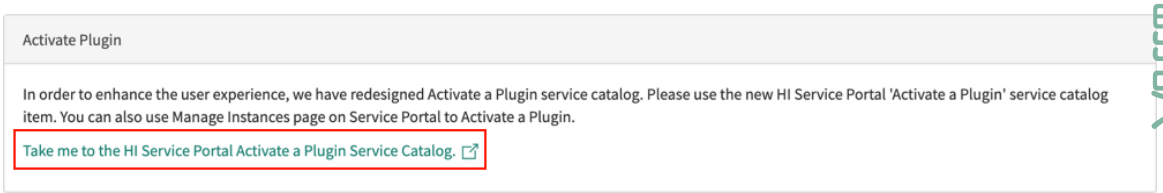
自動翻訳

手順

1. 移動先 すべて > システムアプリケーション > 利用可能なすべてのアプリケーション > すべて。
2. [すべてのアプリケーション] ページで [プラグインの要求] をクリックして、Now Support で [プラグインをアクティブ化] フォームを開きます。



3. Now Support で、Now Support サービスポータル サービスカタログ にアクセスするリンクを選択します。



4. インスタンスを選択します。
5. [アクション] > [プラグインのアクティブ化] を選択します。
6. [プラグインのアクティブ化] フォームで、次の情報を入力します。

[プラグインのアクティブ化] フォーム

フィールド	説明
ターゲットインスタンスは何ですか	プラグインをアクティブ化するインスタンス。
どのプラグインをアクティブ化しますか	アクティブ化するプラグインの名前です。

自動翻訳

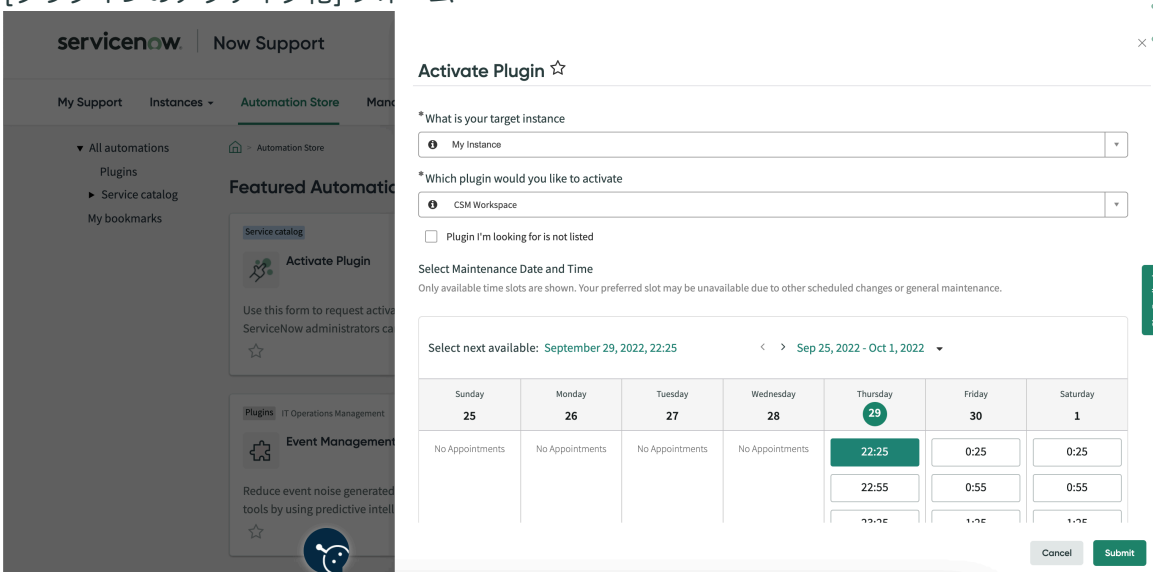
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	注: 必要なプラグインが表示されない場合、または OEM またはオンプレミスのインスタンスでプラグインをアクティブ化している場合は、[探しているプラグインが表示されていません **(Plugin I'm looking for is not listed)]** チェックボックスをオンにして、プラグインの名前を入力します。
メンテナンスの日時を選択 (Select Maintenance Date and Time)	プラグインをアクティブ化する日時。 注: プラグインは、米国太平洋標準時で、毎営業日の朝と夕方の 2 回のバッチでアクティブ化されます。特定の時刻にプラグインをアクティブ化する必要がある場合は、[理由/コメント **(Reason/ Comments)]** フィールドに要求を入力します。

Example

たとえば、 [自分のインスタンス (My Instance)] という名前のインスタンスで CSM Workspace プラグインをアクティブ化するには、次のフォームを参照してください。

[プラグインのアクティブ化] フォーム



7. [送信] を選択します。
プラグインの要求の詳細については、次を参照してください。 の Service Catalog [KB0751715] 記事からのプラグインの要求 Now Support ナレッジベース。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

昇格された権限ロール

昇格された権限ロールでは、ロールの機能にアクセスする前に、そのロールを使用する責任を手動で受け入れる必要があります。

デフォルトでは、ログイン時に昇格された権限のロールはありません。ロールの権限に手動で昇格させる必要があります。昇格された権限のロールは、ユーザーセッションの間のみ有効です。セッションタイムアウトまたはログアウトでこのロールは削除されます。

任意のロールを昇格された権限のロールとして指定し、そのロールを 1 人以上のユーザーに割り当てることができます。これは、ログイン直後にロールが提供する権限にユーザーがアクセスできないようにする場合に実行します。ロールフォームで権限ロールを指定できます。手順については「ロールの作成」を参照してください。

昇格したロールを使用するには、次の条件を満たす必要があります。

- 昇格したロールを割り当てる必要があります。
- 最初に昇格したロールを含む 2 番目に昇格したロールに既に昇格している場合でも、その権限を取得するには、特定の昇格したロールに手動で昇格させる必要があります。

  たとえば、昇格したロール A に昇格したロール B が含まれている場合、ロール A に昇格しても、その権限を取得するにはロール B に昇格する必要があります。

admin ロール

ユーザーに admin ロールを付与するには、付与するユーザーも admin ロールが必要です。たとえば、user_admin ロールのみを持つユーザーは、他のユーザーに admin ロールを付与することはできません。

- 非管理者ユーザーは admin ロールが含まれるグループにユーザーを追加できません。
- ユーザーに security_admin ロールを付与するには、そのユーザーも admin ロールを持っている必要があり、他のユーザーに security_admin ロールを付与する前に、security_admin ロールに昇格する必要があります。admin ロールのみを持つユーザーは、他のユーザーに security_admin ロールを付与することはできません。
- security_admin ロールのないユーザーは、security_admin ロールが含まれるグループにユーザーを追加できません。

警告:
admin ロールで昇格した権限の使用はサポートされておらず、予期しない動作が生じる可能性があります。管理者を手動で昇格させるように要求するには、「管理者に手動での昇格を強制する」を参照してください。

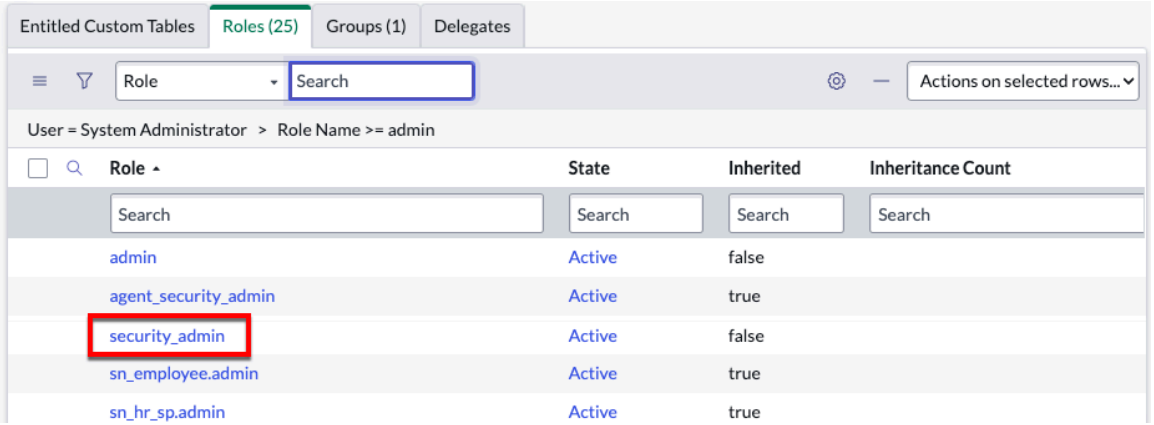
security_admin ロール

ベースシステムでは、security_admin ロールのみが昇格された権限を持ちます。このロールは、デフォルトのシステム管理者 (admin) ユーザーに自動的に割り当てられます。ACL および 高セキュリティ設定へのアクセスを提供します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

システム管理者 **(admin)** ユーザーに割り当てられたロール



注:
このロールを表示するには、まず security_admin ロールに昇格する必要があります。システム管理者 (admin) ユーザーとしてのみログインしている場合、ロールのリストに security_admin レコードは表示されません。

security_admin ロール

security_admin ロールは、ユーザーがアクセス制御の作成や変更を行ったり、高セキュリティ設定を変更したりできる、高セキュリティ設定で提供される昇格された権限ロールです。

ベースシステムでは、デフォルトのシステム管理者 (admin) ユーザーのみが security_admin ロールを持っています。昇格する権限が必要なため、管理者ユーザーはログイン時にこのロールを持っていません。権限を昇格した後、管理者ユーザーはユーザーセッションの間、security_admin ロールを持ちます。詳細については、「特権ロールへの昇格」を参照してください。

高いセキュリティを維持するために、security_admin ロールには昇格する権限が必要です。このロールを割り当てるユーザーとグループを制限します。

特権ロールへの昇格

ベースシステム管理者は、高セキュリティ設定の機能にアクセスするために、特権ロールに昇格できます。

始める前に

必要なロール：管理者

注:
追加のユーザーに admin ロールを付与した場合、そのユーザーは特権ロールに昇格できません。ベースシステム管理者のみが昇格できます。

手順

1. バナーフレームで画像をクリックします。画像をアップロードしていない場合は、自分のイニシャルをクリックします。
2. [ロールを昇格] を選択します。
   昇格に利用可能なロールを含むダイアログボックスが表示されます。
3. アサインする昇格済みロールを選択し、**[OK]** をクリックします。
   このロールは、残りのセッションでこのロールによって制御されるすべてのリソースに対する昇格された権限をユーザーに付与します。ユーザーがログアウトすると、昇格した権限はセッションで終了しますが、次回のログイン時に再確立できます。
4. 手順 2 のダイアログボックスに戻り、ロールの選択を解除して、ロールの昇格を終了します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

管理者に手動での昇格を強制する

管理者ロールを持つすべてのユーザーに、昇格するロールを手動で選択させるプロパティがあります。

始める前に

必要なロール：security_admin

手順

1. 管理者としてログインします。
2. ロールを security_admin に昇格させます。
3. **sys_properties.list** に移動します。
4. *glide.security.strict_elevate_privilege* プロパティを検索して選択します。
5. [値] フィールドを **true** に設定し、[送信] をクリックします。

タスクの結果

ユーザーがログインすると、昇格できるロールを選択するダイアログウィンドウが表示されます。

Security Center

ServiceNow Security Center は、組織が ServiceNow 展開のセキュリティを管理するのを支援するように設計された一連のツールで構成されるアプリケーションです。Security Center を使用して、シームレスなユーザーエクスペリエンスでセキュリティ体制を改善し、コンプライアンスレベルを強化できます。

Security Center は、システム管理者が ServiceNow Store からダウンロードできる無料アプリケーションです。Vancouver リリースからはデフォルトでインストールされます。

> **注:**
> Instance Security Center (ISC) は、2024 年 9 月までに販売が終了します。SSC が、今後推奨されるソリューションです。詳細については、「Instance Security Center から ServiceNow Security Center への移行」を参照してください。

ホームページ	セキュリティの強化	セキュリティスキャナー
	ハードニング構成が ServiceNow のセキュリティ推奨事項にどのように準拠しているかを確認する	一連のセキュリティチェックをスキャンして、設定ミスや安全でない動作を特定します

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ハードニングコンプライアンススコアをパーセンテージで表示し、修正が必要な上位の非準拠ハードニング設定を分析し、セキュリティスキャンの結果を確認します。		
セキュリティ測定基準	アンチウイルス	セキュリティ学習
潜在的なセキュリティ上の脅威を特定するのに役立つ 50 を超えるさまざまなメトリックを監視します。	感染した可能性があるファイルでイベントが発生したときの傾向を表示します。	ServiceNow のセキュリティおよびコンプライアンスドキュメントへのアクセスを提供する、セキュリティリソースの集中管理リポジトリ。

自動翻訳

開始するには

- Security Center は、Vancouver 以降のすべてのファミリーリリースに含まれています。
- 製品ドキュメントは、まず「ホームページ」からお読みください。

ホームページ

ホームページでインスタンスのセキュリティ体制の概要をすばやく把握できます。ハードニングコンプライアンススコアをパーセンテージで表示し、コンプライアンススコアのトレンドをグラフ形式で検出し、修正が必要な上位の非準拠ハードニング設定を分析し、セキュリティスキャンの結果を確認します。

ハードニングコンプライアンススコアは、セキュリティ設定が推奨設定にどの程度近いかを示すパーセンテージです。ハードニングコンプライアンススコアサマリには、このパーセンテージと最近のスコア変更に関連するデータが表示されます。ハードニングコンプライアンススコアのトレンドチャートを使用して、一定期間にわたるコンプライアンススコアの変化を確認します。

上位の非準拠ハードニング設定を使用して、コンプライアンススコアを改善します。このリストには、ハードニングコンプライアンススコアに最も悪影響を及ぼしている 10 のセキュリティ強化設定が表示されます。この表示は、修正するハードニング設定の優先順位付けに役立ちます。

[セキュリティスキャンの概要 (security scan summary)] セクションには、各セキュリティスキャンの経時的な検出結果の数を反映する棒グラフが表示されます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

1. ホームページから、または次に移動して、ハードニングコンプライアンススコアのトレンドチャートにアクセスします ハードニング > スコアの傾向.
2. [スコアトレンドを確認 **(Review score trend)]** を選択して期間をカスタマイズし、分析するトレンドラインのポイントを選択します。
3. [セキュリティスキャンサマリー] セクションで、棒を選択してそのスキャンスイートのスキャン結果ページに移動します。

セキュリティの強化

Security Center の強化ツールを使用して、ハードニングコンプライアンススコアを確認し、以前のスコアと比較し、設定を変更してコンプライアンススコアとセキュリティ体制を改善します。

ハードニング設定は、NOW Platform のセキュリティ関連プロパティとプラグインの推奨値を指定します。この強化ツールは、ハードニング設定のコンプライアンススコアをパーセンテージで計算します。この数値は、インスタンスが Security Center のハードニング設定にどの程度準拠しているかを示します。

ハードニングコンプライアンススコアの計算式：

- 各ハードニング設定のリスクスコアは 0 ～ 10 です。
- スコアは、すべての準拠リスクスコアの合計をすべてのリスクスコアの合計で割った値と等しくなります。

たとえば、すべての準拠リスクスコアの合計が 25.4 で、すべてのリスクスコアの合計が 34.9 の場合、コンプライアンススコアは (25.4 /34.9) x 100 = 72.7 になります。この小数は最も近い整数に切り上げられるため、73 になります。

ハードニングスコアの比較

ハードニング設定の健全性を可視化し、このデータを使用してインスタンスのセキュリティ体制を改善します。

ハードニングスコア比較ページには、最初の日付と 2 番目の日付の間のコンプライアンスステータスの変更を含むハードニング設定と、それらがハードニングコンプライアンススコアにどのように影響したかが表示されます。たとえば、設定が準拠から非準拠に変更された場合、スコアは低下します。

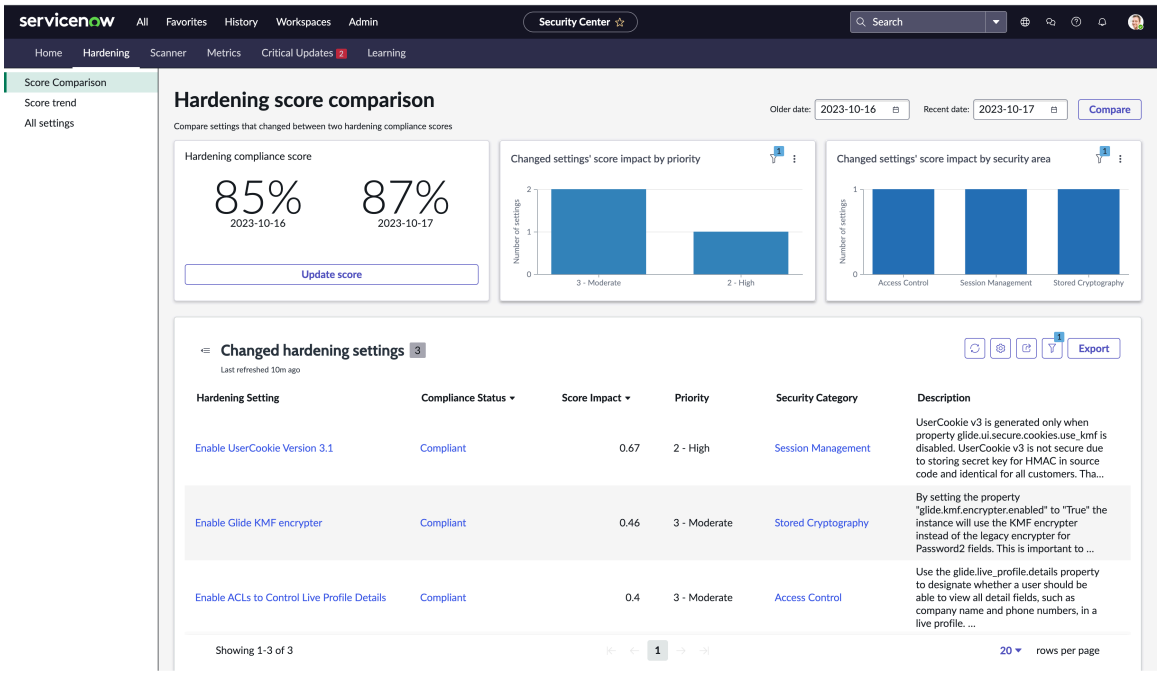
これらの変更の結果を表示するには、ページの右上にある日付ピッカーに 古い日付 と 最近の日付 を入力し、比較 を選択します。以下は、各カードの説明です。

- ハードニングコンプライアンススコア:選択した 1 日目と 2 日目のインスタンスのコンプライアンススコアをパーセンテージで表示します。
- 優先度別の変更された設定のスコアへの影響度:2 つの日付の間にコンプライアンスステータスを変更したハードニング設定の数を優先度値別に表示します。
- セキュリティ領域別の変更された設定のスコアへの影響: 2 つの日付の間にコンプライアンスステータスを変更したハードニング設定の数をセキュリティ領域別に表示します。
- 変更されたハードニング設定:2 つの日付の間にコンプライアンス スタチューを変更したハードニング設定のリストを表示します。非準拠になり、ハードニング比較スコアを低下させた設定を確認して、それらを準拠させてスコアを上げる機会を得ることができます。ハードニングコンプライアンススコアの増加 を参照してください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

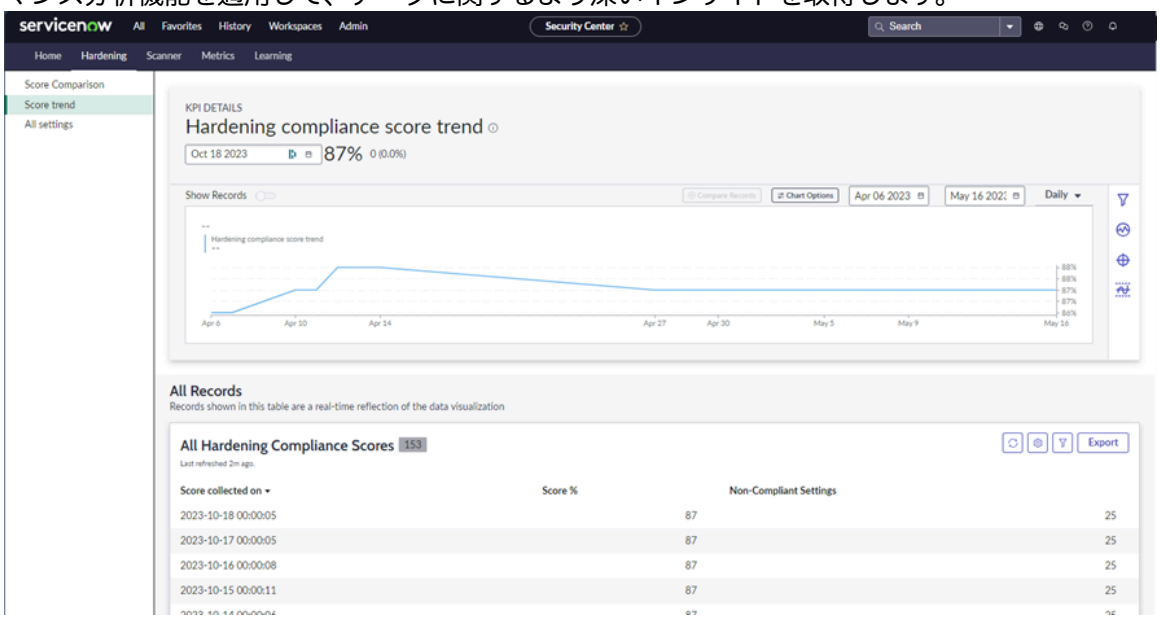
たとえば、次のスクリーンショットでは、コンプライアンススコアが増加しています。これは、この期間中にセキュリティ体制が改善されたことを示しています。



ハードニングコンプライアンススコアのトレンド

一定期間にわたるハードニングコンプライアンススコアのトレンドをチャートまたはテーブルで表示します。

一定期間にわたるコンプライアンススコアのトレンドを確認します。日付ピッカーを使用して分析する期間を選択し、ターゲット、しきい値、KPI などのパフォーマンス分析機能を適用して、データに関するより深いインサイトを取得します。



チャートオプション：分析を実行し、時系列を表示し、いくつかのチャートタイプでデータを表示するには、[チャートオプション] を選択します。

分析

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- ターゲット：組織が達成したい目標です。「Performance Analytics targets」を参照してください。
- しきい値：インジケーターの通常のスコアの範囲を定義し、特定のイベントが発生したときに警告します。「Performance Analytics thresholds」を参照してください。
- 予測：過去の動作に基づいて将来のスコアを予測する機能について説明します。「Performance Analytics scores forecasts」を参照してください。
- トレンド：1 つ以上のアイテムの値が時間の経過とともにどのように変化するかを示します。
- コメント：個々のデータポイントの注釈を表示します。
- ラベル：ビジュアル化に関連するスコアを表示します。
- 統計情報：コンプライアンススコアに関連する統計情報を表示します。

時系列

- スコア：KPI のスコア
- 変更：このインジケーターのスコアの変更
- 変更割合：スコアの変更割合

グラフのタイプ：「Time series visualization type use cases」を参照してください。

すべてのレコードテーブル

[すべてのレコード] テーブルには、コンプライアンススコアが収集された日付、スコアの割合、および非準拠設定の数が表示されます。このテーブルを別のオプションとして使用して、 時間の経過に伴うインスタンスのセキュリティ体制を分析できます。

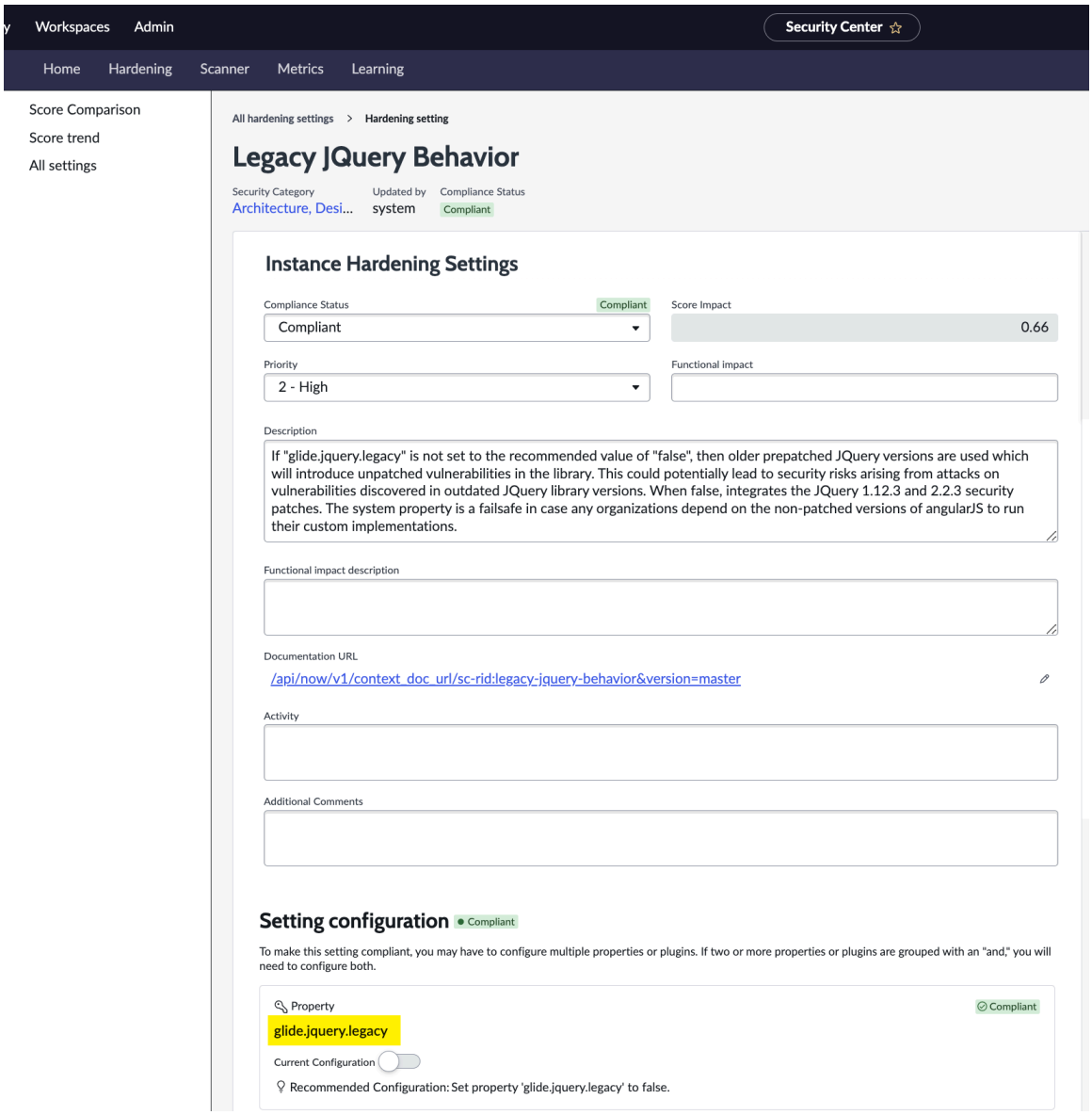
ハードニング構成の詳細

Security Center アプリ内のリンクを選択して、ハードニング設定の詳細を分析します。

移動先 ハードニング > すべての設定をクリックし、ハードニング設定を選択して、セキュリティ関連情報を表示するハードニング設定ツール内のページにリダイレクトされます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



ハードニング設定構成の詳細

構成属性	説明
コンプライアンスのステータス	ハードニング設定が準拠しているかどうかを示します。
スコアへの影響	このハードニング設定がセキュリティ体制にどの程度影響するかを示すパーセンテージ。
優先度	1 ～ 4 の範囲内の数値。1 が最も高い重み付けで、このハードニング設定がセキュリティ体制に与える影響の強さを示します。
機能への影響度	このハードニング設定がインスタンスの操作に与える影響。
説明	ハードニング設定に関する一般的な概要。
ドキュメント URL	ハードニング設定のドキュメントへのリンク。
アクティビティ	ハードニング設定に関連する更新の通知。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ハードニング設定構成の詳細 (続く)

構成属性	説明
設定構成	ハードニング設定のコンプライアンスステータスに関連する詳細と、それらを準拠させる方法の手順。 **注:** 一部のハードニング設定では、それらを準拠させるために複数のプロパティとプラグインの構成が必要になる場合があります。

ハードニングコンプライアンススコアの増加

ハードニング設定がシステムの推奨事項に準拠していることを確認し、ハードニングコンプライアンススコアを増加します。

始める前に

必要なロール：admin

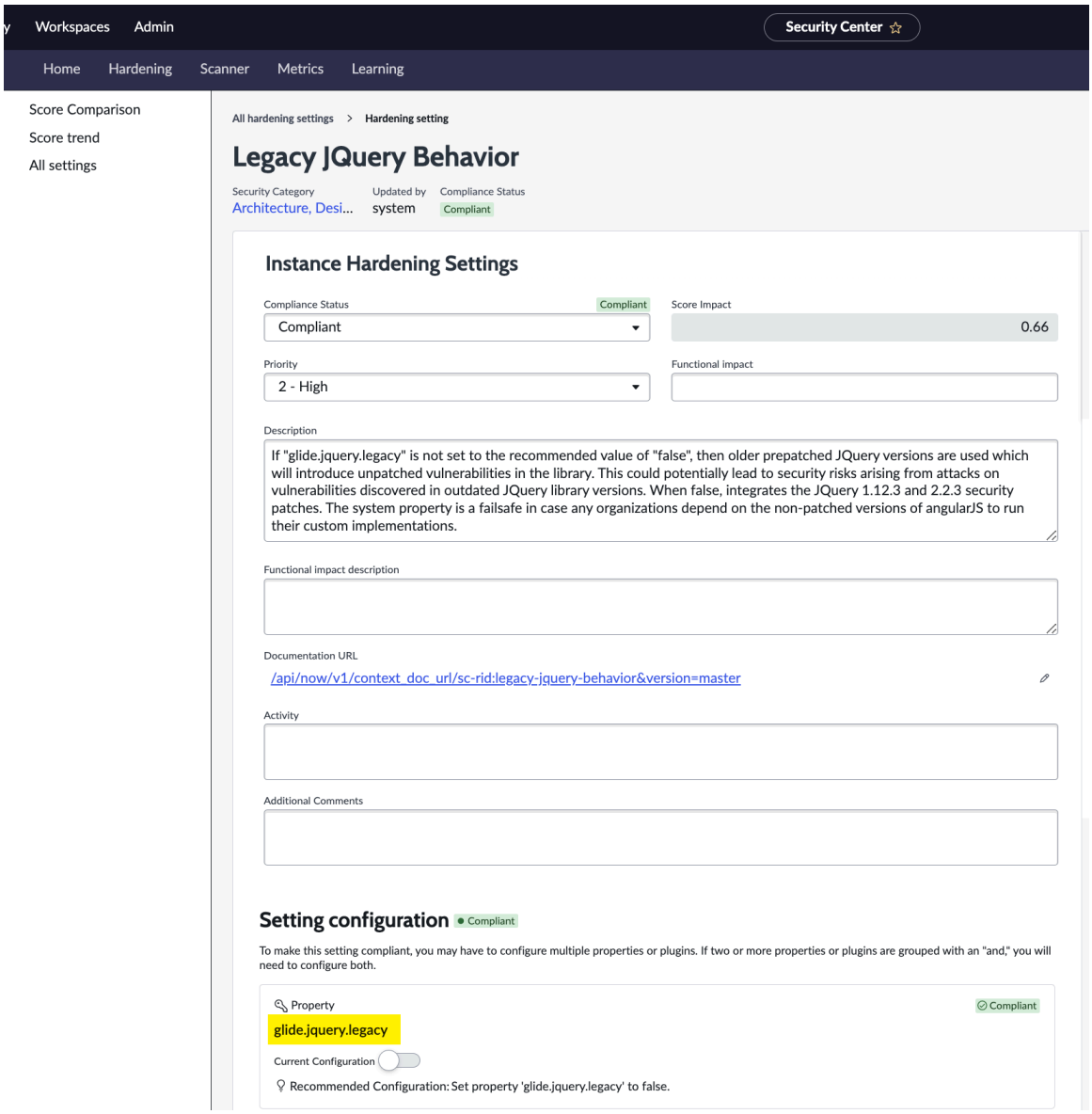
インスタンスでスコアへの影響が最も高い非準拠のハードニング設定を特定します。それらをレビューして、全体的なコンプライアンススコアを上げることができるように、システムの推奨事項に準拠できるかどうかを確認します。

手順

1. 移動先 ハードニング > すべての設定.
2. [コンプライアンスステータス] 列をフィルタリングして、非準拠のハードニング設定のみを表示します。
3. [スコアへの影響度] を選択して、最大から最小にソートします。
4. 設定を選択し、設定の詳細を確認して、推奨事項に準拠するかどうかを決定します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



5. ハードニング設定を準拠させます。

6. 非準拠のハードニングスコアを更新して準拠させる場合は、ホームページに移動し、[スコアを更新] を選択して最新のスコアを表示します。
ハードニングスコアは切り上げられます。86.75% のスコアは 87 に切り上げられます。

すべての設定

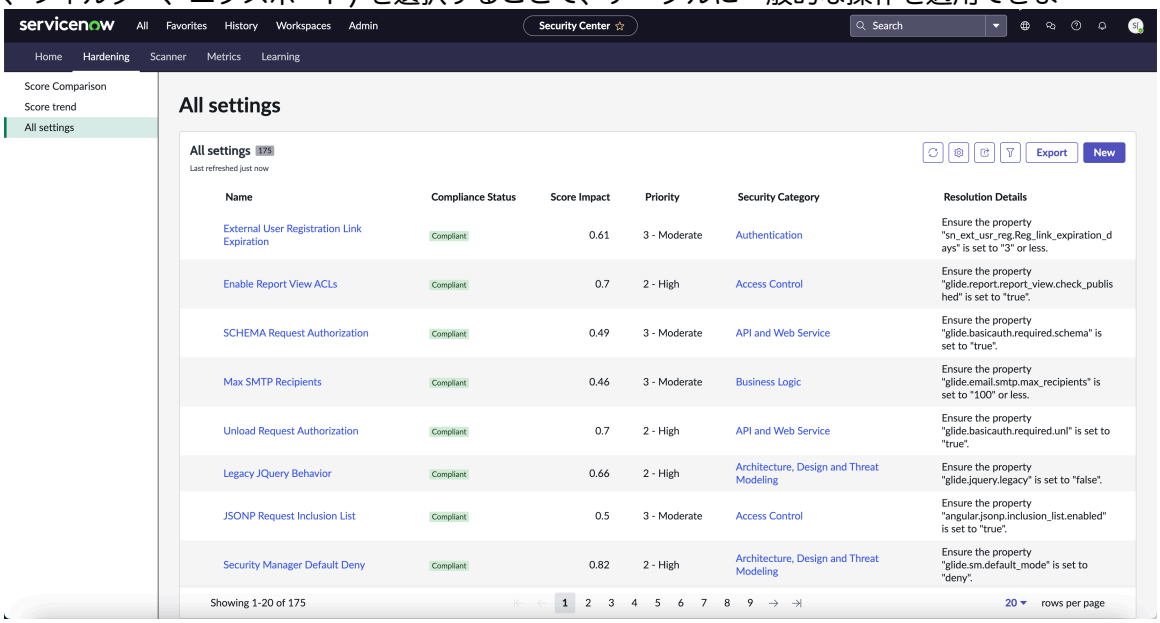
インスタンスで利用可能なすべてのハードニング設定を 1 ページに表示します。

インスタンスで利用可能なすべてのハードニング設定を表示するテーブル。テーブルの右上にあるアイコン (リストのリフレッシュ、リストアクション、すべての設定の URL のコ

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ピー、フィルター、エクスポート) を選択することで、テーブルに一般的な操作を適用できま



す。

- 名前：ハードニング設定プロパティの名前。
- コンプライアンスステータス：[準拠] は、ハードニング設定が適切に構成されていることを示します。[非準拠] は、ハードニング設定プロパティがシステムの推奨に従って構成されていないことを示します。
- スコアへの影響 **(Score Impact)**：このハードニング設定がセキュリティ体制に与える影響のパーセンテージ値。すべてのスコアへの影響の合計は 100% になります。
- 優先度：設定の重要度を表す値 (重大、高、中、および低)。スコアへの影響と優先度の関係は、スコアへの影響が高いほど重要度が高いことを示します。
- セキュリティカテゴリ **(Security category)**：プロパティのセキュリティカテゴリ。
- 解決の詳細：ハードニング設定のセキュリティ脆弱性を修正するために実行する必要がある手順。

ハードニング設定プロパティの構成方法については、「ハードニングコンプライアンススコアの増加」を参照してください。

ハードニング設定のベースライン

ハードニング設定の個別のベースラインバージョンが、さまざまなファミリーおよびストアリリースにどのように対応しているかについて説明します。

Security Center は、インスタンスからシステムプロパティのサブセットを取り込み、その構成の詳細と、アプリ内での非準拠のセキュリティへの影響を表示することで機能します。ベースラインは、Security Center アプリの各リリースで取り込まれるシステムプロパティの参照ポイントとして機能します。

ハードニング設定ベースラインの概要

Security Center のバージョン	ハードニング設定のベースラインバージョン	サポートされているファミリー	ストアリリース日	デフォルトでインストールされる内容
SSC v1.1	ベースライン v1.0	Utah、Vancouver	2023 年 5 月	Vancouver ファミリー
SSC v1.2	ベースライン v1.0	Utah、Vancouver	2023 年 8 月	ストアのみ

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

ハードニング設定ベースラインの概要 (続く)

Security Center のバージョン	ハードニング設定のベースラインバージョン	サポートされているファミリー	ストアリリース日	デフォルトでインストールされる内容
SSC v1.3	ベースライン v2.0	Vancouver、Washington	2023 年 11 月	Washington ファミリー

セキュリティスキャナー

スキャナーツールを使用して、一連のセキュリティチェックに対してインスタンスをスキャンし、設定ミスを特定します。このツールを使用すると、さまざまなユースケースに対して異なるチェックスイートを作成するプロセスが簡素化されるため、結果を経時的に分析できます。

セキュリティスキャンは、インスタンスについてセキュリティの健全性の問題を示す構成を調べる方法です。これにより、組織のセキュリティ推奨事項を実装する機会を特定できます。

スキャナーツールにアクセスする場合、スイートの少なくとも 2 つのスキャン結果と比較するスイートを選択するまで、比較することはできません。デフォルトのスイートとチェックを使用することも、独自のカスタムチェックとスイートを作成することもできます。

ハードニングスコアの比較

ハードニング設定の健全性を可視化し、このデータを使用してセキュリティの脅威を修正し、インスタンスのセキュリティ体制を改善します。

ハードニングスコアの比較ページには、最初の日付と 2 番目の日付の間でハードニング設定 のセキュリティ変更が表示されます。これらの変更を表示するには、ページの右上にある日付ピッカーに [古い日付 **(Older date)]** と [最近の日付 **(Recent date)]** を入力し、[比較] をクリックします。各カードの説明は次のとおりです。

- ハードニングコンプライアンススコア **(Hardening compliance score)**：インスタンスのコンプライアンススコアを最初の日付と 2 番目の日付のパーセンテージで表示します。
- 優先度ごとの変更された設定のスコアへの影響 **(Changed settings' score impact by priority)**：優先度が変更された設定の数を表示します。
- セキュリティエリアごとの変更された設定のスコアへの影響 **(Changed settings' score impact by security area)**：カテゴリが変更された設定の数を表示します。たとえば、[アクセス制御] から [データ保護 **(Data Protection)]** に移行します。
- 変更されたハードニング設定 **(Changed hardening settings)**： 関連するセキュリティデータとともに、変更された設定の統合ビューがリストに表示されます。さらに、リフレッシュ、リスト UI アクション、URL のコピー、フィルター、エクスポートなど、リストに関連付けられた一般的な機能を適用できます。

たとえば、次のスクリーンショットでは、コンプライアンススコアが 71% から 73% に変更されており、これはその期間内にセキュリティ体制が強化されたことを示しています。

優先度が変更された設定の数は、高が 2 つ、中が 2 つの合計 4 つです。また、セキュリティが変更された設定の数は、アクセス制御が 2 つ、認証が 1 つ、ビジネスロジックが 1 つの合計 4 つです。これらの 4 つの設定に関するセキュリティの詳細は、[変更されたハードニング設定 (Changed hardening settings)] リストにも表示されます。非準拠の設定を表示して修正すると、ハードニングコンプライアンススコアが再計算されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

スキャンチェック

チェックは、セキュリティプラクティスに準拠しない構成またはアクティビティを指定するルールです。チェックは、テーブル、レコード、またはメタデータに対して実行できます。

作成できるチェックのタイプは次のとおりです。

- テーブルチェック
- 列タイプチェック
- スクリプトのみのチェック
- リンターチェック

チェックの詳細については、「Getting started with checks」を参照してください。

チェックを作成する準備ができたら、[新規] をクリックします。

新しいスイートの作成

組織に対するインスタンスのセキュリティを分析できるように、カスタムスイートを作成してスケジュールします。

始める前に

必要なロール：admin

スイートは、スキャンに使用できるチェックのコレクションです。次に移動して、インスタンス内で利用可能なスキャンスイートのリストをテーブルに整理して表示します。 スキャナー > スイート. 独自のスイートを作成することも、デフォルトのスイートである監査ツールを使用することもできます。監査ツールは、セキュリティのベストプラクティスのチェックを含む、すぐに利用可能なデフォルトのスイートです。これらのチェックは、インスタンスのセキュリティ体制に影響を与える可能性があるシステムプロパティ、プラグイン、およびテーブルで構成されています。次の手順では、スイートを作成する方法を、その設定に使用できるいくつかのオプションとともに示します。

手順

1. 移動先 スイート > 新規.
2. スイートの [名前] と [説明] を入力し、[保存] を選択します。
3. チェック
   ここで、スイートにチェックを追加します。
   a. [編集] を選択します。
   b. 追加するチェックを選択し、[追加] (**>**) を選択してスイートに配置します。
   c. [保存] を選択します。
4. 子スイート
   ここで子スイート (親スイートの下に配置されるスイート) を追加します。
   a. [編集] を選択します。
   b. 追加する子スイートを選択し、[追加] (**>**) を選択して子スイートに配置します。
   c. [保存] を選択します。
5. 親スイート
   ここで親スイートを追加します。スキャンで親スイートが使用されると、すべての子スイートが実行されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

a. [編集] を選択します。

b. 追加する子スイートを選択し、[追加] (**>**) を選択して親スイートに配置します。

c. [保存] を選択します。

6. スケジュール
スイートの実行時間を設定します。

a. [新規] を選択します。

b. スケジュールスキャンの詳細を入力します。
時間フィールドの形式は、時:分:秒です。

c. [保存] を選択します。

スキャン検出結果

検出結果は、インスタンスでチェックのルールに違反したレコードへの参照です。ソースレコードと、レコードが特定のチェックのルールをトリガーした回数がわかります。

[結果] に移動して、インスタンスのスキャン結果のリストを表示します。[作成済み] 列のリンクを選択してドリルダウンし、結果に関連する詳細を表示します。

- チェック：スキャンに関連付けられたチェックのリスト
- カテゴリ：スキャンに関連付けられたセキュリティカテゴリたとえば、アクセス制御や悪意のあるコードなどです。
- カウント：レコードがチェックルールに違反した回数
- 優先度：セキュリティリスクの重大度。最高の優先度が 1、最低が 4 です。
- 結果：スキャンのステータスとタイプ
- チェックバージョン：チェックの変更バージョン
- ソーステーブル：チェックのルールに違反したレコード
- ミュートの理由：結果をミュートする理由
- ソース：結果が作成された日付
- タスク：レコードの結果からタスクを容易にアサインするために使用されます。
- ドメイン：アクセスできるものとできないものを定義します。
- 簡単な説明：スキャンの簡単な説明
- 解決の詳細：スキャンの問題を解決する方法に関する指示

セキュリティ測定基準

測定基準ツールを使用して 50 を超えるさまざまなセキュリティ測定基準を監視し、潜在的なセキュリティの脅威や安全でない動作を特定します。メール通知のしきい値を設定し、さまざまな方法でデータを可視化および分析し、データをエクスポートすることも、組織に最も重要である測定基準を使用してダッシュボードを作成することもできます。

測定基準は、しきい値を超えたときのメールアラートの送信、ターゲットのビジュアル化、基礎となるイベントの表示とフィルタリングなど、豊富な機能セットを使用可能にする分析ハブのビジュアル化として実装されます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

自分のセキュリティ測定基準ダッシュボード

単一のダッシュボードでインスタンスのセキュリティ測定基準を表示します。

[測定基準] ページに移動するには、[自分の測定基準 **(My metrics)]** を選択します。このページにはデフォルトのダッシュボードが表示されますが、[編集] を選択して独自のダッシュボードを作成することもできます。

ビジュアル化、フィルター、見出し、画像、リッチテキスト、およびリストを追加して、独自のダッシュボードをカスタマイズできます。ダッシュボードをカスタマイズするさまざまな方法については、「Platform Analytics dashboards」を参照してください。

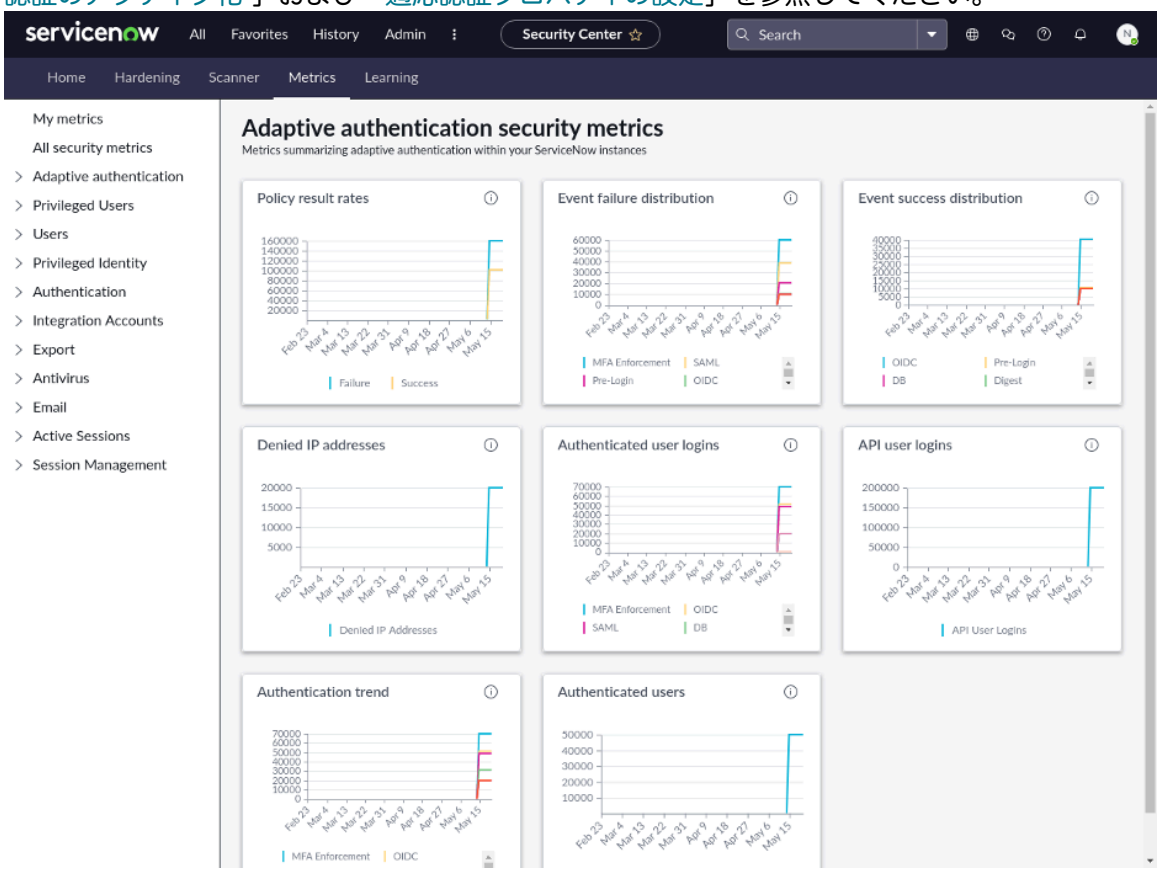
すべてのセキュリティ測定基準

[すべてのセキュリティ測定基準] に移動して、インスタンスのセキュリティ測定基準に関連するデータを含むテーブルを表示します。

適応認証セキュリティ測定基準

認証ポリシーを使用して認証要求を評価し、指定されたポリシー条件に基づいてインスタンスへのアクセスを拒否または許可します。

適応認証測定基準では、インスタンスでの適応認証の使用状況を監視できます。適応認証のすべての測定基準のサマリを表示することも、ポリシー結果評価や拒否された IP アドレスなどの個々の測定基準を掘り下げて表示することもできます。このページでは、適応認証用の Adaptive Authentication (`com.snc.adaptive_authentication`) プラグインをインスタンスで使用できるようにする必要があります。測定基準を表示するには、認証ポリシーを有効にする必要もあります。詳細については、「適応認証のアクティブ化」および「適応認証プロパティの設定」を参照してください。



注:
この機能はバージョン 1.2 でリリースされました。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

- ポリシー結果評価：成功および失敗したすべての適応認証イベント
- イベント失敗の分布：イベントタイプごとの失敗したすべてのイベント
- イベント成功の分布：イベントタイプごとに関連付けられた成功イベント
- 拒否された IP アドレス：インスタンスによってブロックされた IP アドレスの数とその関連データ
- 認証済みのユーザーログイン：イベントタイプごとにカウントされたイベントの数 (ログイン前のイベントを除く)
- API ユーザーログイン：イベントタイプごとの API 認証ポリシーに関連付けられたイベントの数
- 認証傾向：記録されたイベントの合計数
- 認証ユーザー：イベントタイプごとにカウントされたユーザーの数 (ログイン前のイベントを除く)

特権ユーザー

Now Platform での特権ユーザー (アクティブおよび非アクティブ) とそのアクティビティのトレンドラインを表示します。

[特権ユーザー概要 (Privileged users overview)] セクションに、Now Platform での特権ユーザー (アクティブおよび非アクティブ) とそのアクティビティのトレンドラインが表示されます。特権ユーザーは、高セキュリティ設定、インポート、ポータルユーザーなどの機能にアクセスするために、管理者によって追加のロールがアサインされたユーザーです。

特権ユーザーの説明は次のとおりです。

- 合計ユーザー：インスタンスのユーザーの合計数
- アクティブユーザー：インスタンスでセッションを開始したユーザーの合計数
- 非アクティブなユーザー：最近インスタンスにログインしていないユーザー
- ロックアウトされていない非アクティブなユーザー (Inactive users who are not locked out)：最近ログインしていないが、まだ自分のアカウントにアクセスできるユーザー
- ロックアウトされたユーザー：アカウントへの認証が許可されていないユーザー
- 新規ユーザー：インスタンスに最近追加されたユーザー
- 成功したログイン (Successful logins)：正常にログインしたユーザー
- 失敗したログイン：失敗したログイン試行
- MFA で保護されていないローカルログイン (Local logins not protected by MFA)：MFA なしでログインしたユーザー
- ログインしていないユーザー (Users never logged in)：インスタンスにログインしたことのないユーザー
- 先月からログインしていないユーザー (Users not logged in since last month)：過去 30 日間ログインしていないユーザー
- 6 か月前からログインしていないユーザー (Users not logged in since the last 6 months)：過去 6 か月間ログインしていないユーザー
- 1 年前からログインしていないユーザー (Users not logged in since the last 1 year)：過去 1 年間ログインしていないユーザー
- パスワードのリセットが必要 (Need to reset password)：パスワードをリセットする必要があるユーザー
- ユーザーのパスワードリセットの失敗 (Password reset failures of the users：ユーザーあたりのパスワードの失敗数

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ユーザー

Now Platform で合計ユーザー (アクティブおよび非アクティブ) とそのアクティビティのトレンドラインを表示します。

[ユーザー概要 (Users overview)] セクションに、Now Platform での合計ユーザー (アクティブおよび非アクティブ) とそのアクティビティのトレンドラインが表示されます。

ユーザーのタイプの説明は次のとおりです。

- 合計ユーザー：インスタンスのユーザーの合計数
- アクティブユーザー：インスタンスでセッションを開始したユーザーの合計数
- 非アクティブなユーザー：最近インスタンスにログインしていないユーザー
- ロックアウトされていない非アクティブなユーザー (Inactive users who are not locked out)：最近ログインしていないが、まだ自分のアカウントにアクセスできるユーザー
- 新規ユーザー：インスタンスに最近追加されたユーザー
- 成功したログイン (Successful logins)：正常にログインしたユーザー
- 失敗したログイン：失敗したログイン試行
- 外部ログイン：サードパーティを使用する認証
- MFA で保護されていないローカルログイン (Local logins not protected by MFA)：MFA を使用しないログイン
- 先月からログインしていないユーザー (Users not logged in since last month)：過去 30 日間ログインしていないユーザー
- 6 か月前からログインしていないユーザー (Users not logged in since the last 6 months)：過去 6 か月間ログインしていないユーザー
- 1 年前からログインしていないユーザー (Users not logged in since the last 1 year)：過去 1 年間ログインしていないユーザー
- パスワードのリセットが必要 (Need to reset password)：パスワードをリセットする必要があるユーザー
- ユーザーのパスワードリセットの失敗 (Password reset failures of the users：ユーザーあたりのパスワードの失敗数

特権 ID

特権 ID を持つユーザーの測定基準に関連するデータを分析します。

このダッシュボードには、特権 ID ユーザーとそのインスタンスでのアクティビティに関連するデータが表示されます。

- 管理ログイン：admin ロールのユーザーによるログインの合計数
- 代理操作：impersonator ロールを持つユーザーにより行われた代理操作の合計数
- 昇格 (Elevation)：security_admin ロールを持つユーザーにより行われたセキュリティ昇格の合計数
- ServiceNow ログイン：ServiceNow 従業員によるログインの合計数
- 追加された管理者ユーザー：admin ロールを付与されたユーザーの合計数

認証測定基準

ダッシュボードからインスタンスの認証に関連する測定基準を表示します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

MFA の使用状況、Web サービスアカウント、生体認証スキャナーの使用状況など、認証スキームに関連する測定基準のデータを表示します。

- MFA に登録されているユーザー：MFA の使用に登録されているユーザーの合計数
- MFA バイパスを使用しているユーザー (Users using MFA bypass)：マルチファクター認証を回避しているユーザーの合計数
- 高権限非 MFA ユーザー (High privileged non-mfa user)：MFA を使用していない高権限ユーザーの合計数
- アクティブな MFA ユーザー：インスタンスでアクティブな MFA ユーザーの合計数
- ロックアウトされた MFA ユーザー：インスタンスでロックアウトされた MFA ユーザーの合計数
- Web サービスアカウントユーザー(Web service account user)：Web サービスアカウントのみを持つユーザーの合計数
- 期限が切れる X509 証明書 (X509 certificates expiring)：30 日後に期限が切れる X509 証明書の合計数

統合アカウント

Now Platform で作成された統合アカウントに関する傾向を表示します。

統合アカウントのダッシュボードには、Now Platform で作成された統合アカウントに関する傾向が表示されます。

以下は、統合アカウントの測定基準の説明です。

- 合計統合アカウント (Total integration accounts)：インスタンスの統合アカウントに関連する傾向
- アクティブ統合アカウント (Active integration accounts)：インスタンスの統合アカウントに関連する傾向
- 非アクティブ統合アカウント (Inactive integration accounts)：インスタンスで非アクティブな統合アカウントの合計数の傾向

エクスポート

一般的にエクスポートされるデータと、エクスポートを実行するユーザーを検出します。

- 合計エクスポート数 (Total exports)：ユーザーによってエクスポートされたテーブルレコードの合計数
- 分類されたエクスポート (Classified exports)：アサインされたデータ分類別に要約されている、エクスポートされたテーブルレコードの合計数

ウィルス対策

感染した可能性があるファイルでイベントが発生したときの傾向を表示します。検出、隔離、復元、または削除がいつ行われたかを確認します。

- 隔離されたファイル：マルウェアが含まれている可能性があるファイルの数
- ダウンロードされたファイル (Downloaded files)：ダウンロードされたファイルの数
- 復元されたファイル (Restored files)：復元されたファイルの数
- 削除されたファイル：削除されたファイルの数

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

メール

外部で受信されているスパムメールに関連するデータを表示します。

[スパムメール **(Spam emails)**] は 1 日あたりに受信した迷惑メールの数を表します。

アクティブセッション

Now Platform のアクティブユーザーのトレンドラインを表示します。

次の測定基準のトレンドラインを表示できます。

- ユーザーセッション：インスタンスのアクティブなユーザーセッションに関連する測定基準
- 特権ユーザーセッション (Privileged user sessions)：特権ユーザーまたは追加のロールがアサインされたユーザーに関連する測定基準

セッション管理

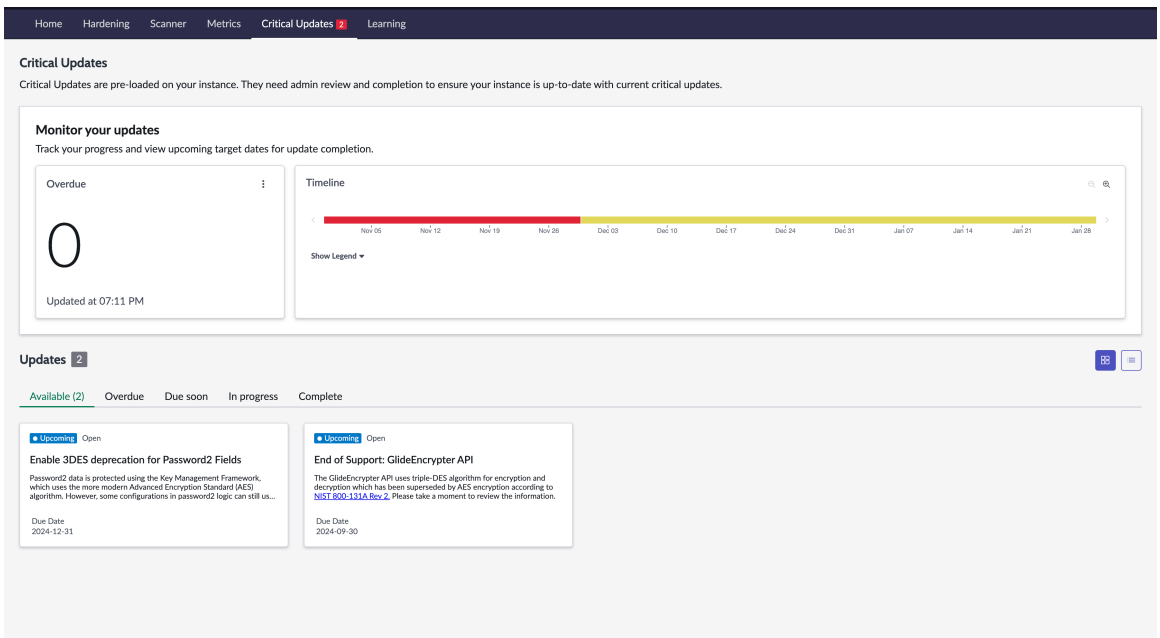
ユーザーセッションに関連する測定基準とセッションのロックアウトの頻度を表示します。

重大な更新

システムが推奨する重要な更新が予定どおりに実装されるようにすることで、インスタンスのセキュリティ体制を強化します。

重要な更新は、管理者がインスタンスとプラグインの構成に基づいて重要なセキュリティ更新プログラムを実装するのに役立つツールです。重要な更新は、セキュリティ関連の変更の重要性の理解を助けることに重点を置いた、インスタンスで推奨される変更です。重要な更新は、インスタンスでセキュリティ更新プログラムをスキャン、更新、およびテストする手順の実装を支援します。重要な更新を実装して、インスタンスのカスタマイズが妨げられるのを防ぎます。手動で実装された重要な更新は、インスタンスでレンダリングされる、ファミリーリリースやパッチを使用した ServiceNow コードや機能への自動更新とは異なります。

重要な更新プログラムのホームページでは、重要な更新プログラムのタイムラインを表示できるため、手順を実装するタイミングに優先順位を付けることができます。スクリーンショットのタイムラインには、期限切れの重要な更新プログラムとまもなく期限切れの更新プログラムが表示されます。さらに、[更新プログラム] ラベルで重要な更新プログラムの進行状況を追跡できます。利用可能な、期限切れ、期限が近い、進行中、または完了していることを確認するためのタブを選択します。



自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

はじめに:

- このツールにアクセスするには、セキュリティ センター内の [重要な更新プログラム] に移動します。
- 重要な更新プログラムは、ワシントン DC から始まるセキュリティ センター アプリに含まれています。

重要な更新プログラムの手順を実装する

インスタンスに重要な更新を実装してセキュリティ体制を強化する方法について説明します。

始める前に

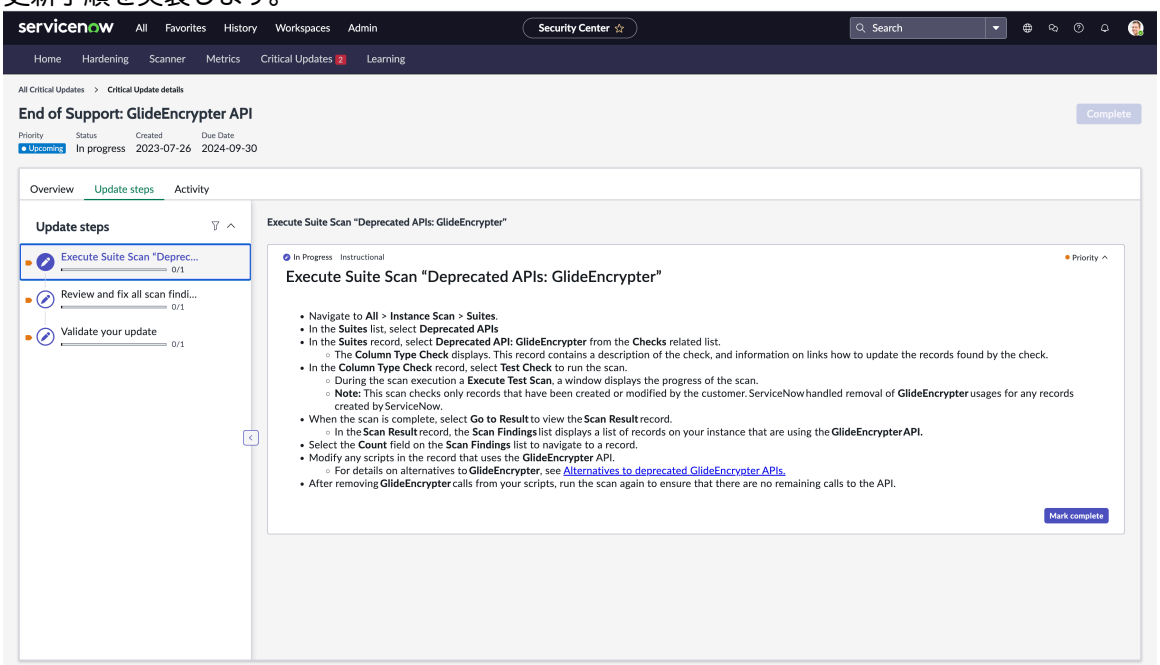
必要なロール：admin

このタスクについて

重要な更新 (CU) では、インスタンスに変更を実装してセキュリティ体制を強化する方法について、順を追って説明します。CU は、実装プロセスの各ステップをガイドするために、製品ドキュメントから関連コンテンツを取得します。以下の手順に従って、重要な更新プログラムを実装する方法を確認してください。

手順

1. 重要な更新プログラム アプリに移動します。
2. 実装する重要な更新をクリックします。
   [更新] セクションの [利用可能] タブには、インスタンスのすべての重要な更新が一覧表示されます。このタブの下にある重要な更新をクリックすると、手順が表示されます。
3. 概要を読んで、重要な更新プログラムが必要な理由を確認し、手順を実装する準備をします。
   [**Go to next step**] をクリックして、実装の詳細に進みます。
4. 更新手順を実装します。



   a. 指示の各グループを読み、インスタンス内で実装します。
   b. 一連の指示を完了したら、[完了としてマーク] をクリックします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

c. すべての更新手順を完了するまで、手順 a から b を繰り返します。

d. [完了] をクリックします。
重要な更新プログラムは、[重要な更新プログラム] ホームページの [更新プログラム] セクションで利用 できなくなります。

重要な更新のアクティビティの表示

重要な更新に関連するすべてのアクティビティの詳細を表示します。

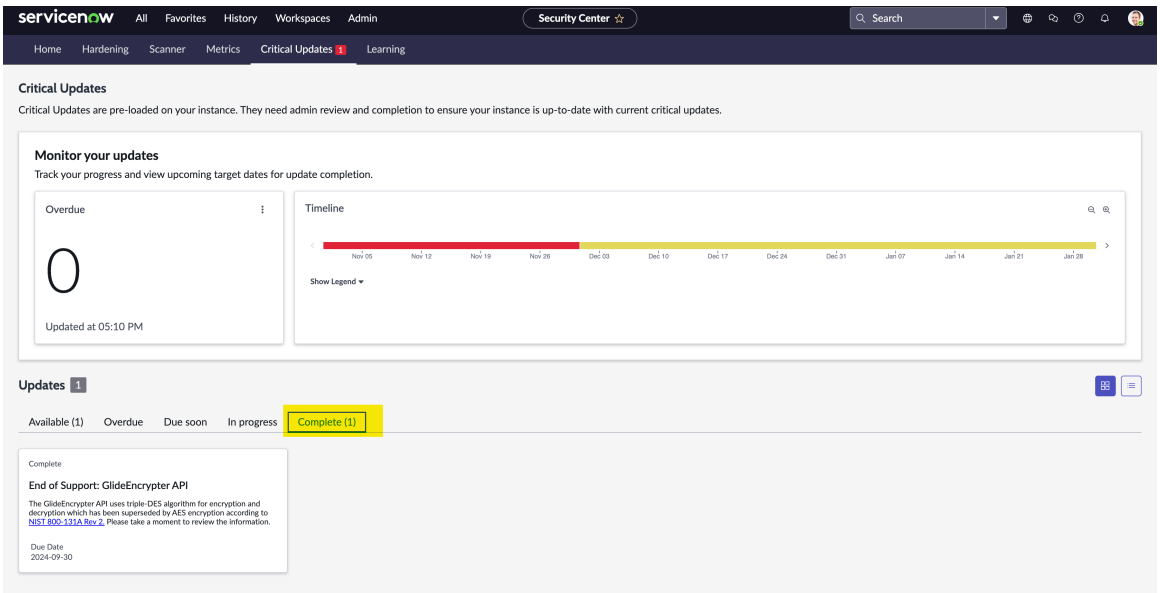
始める前に
必要なロール：admin

このタスクについて
アクティビティは新しいものから古いものの順にリストされるため、最新のアクティビティを最初に分析できます。アクティビティに対する各更新にはタイムスタンプが付き、検索とフィルターを使用して特定の情報をクエリできます。

手順

1. セキュリティセンター内の 重要な更新 アプリに移動します。
2. [重要な更新プログラム] の [更新プログラム] ラベル に移動します。
3. 状態をクリックし、その状態から重要な更新プログラムを選択します。

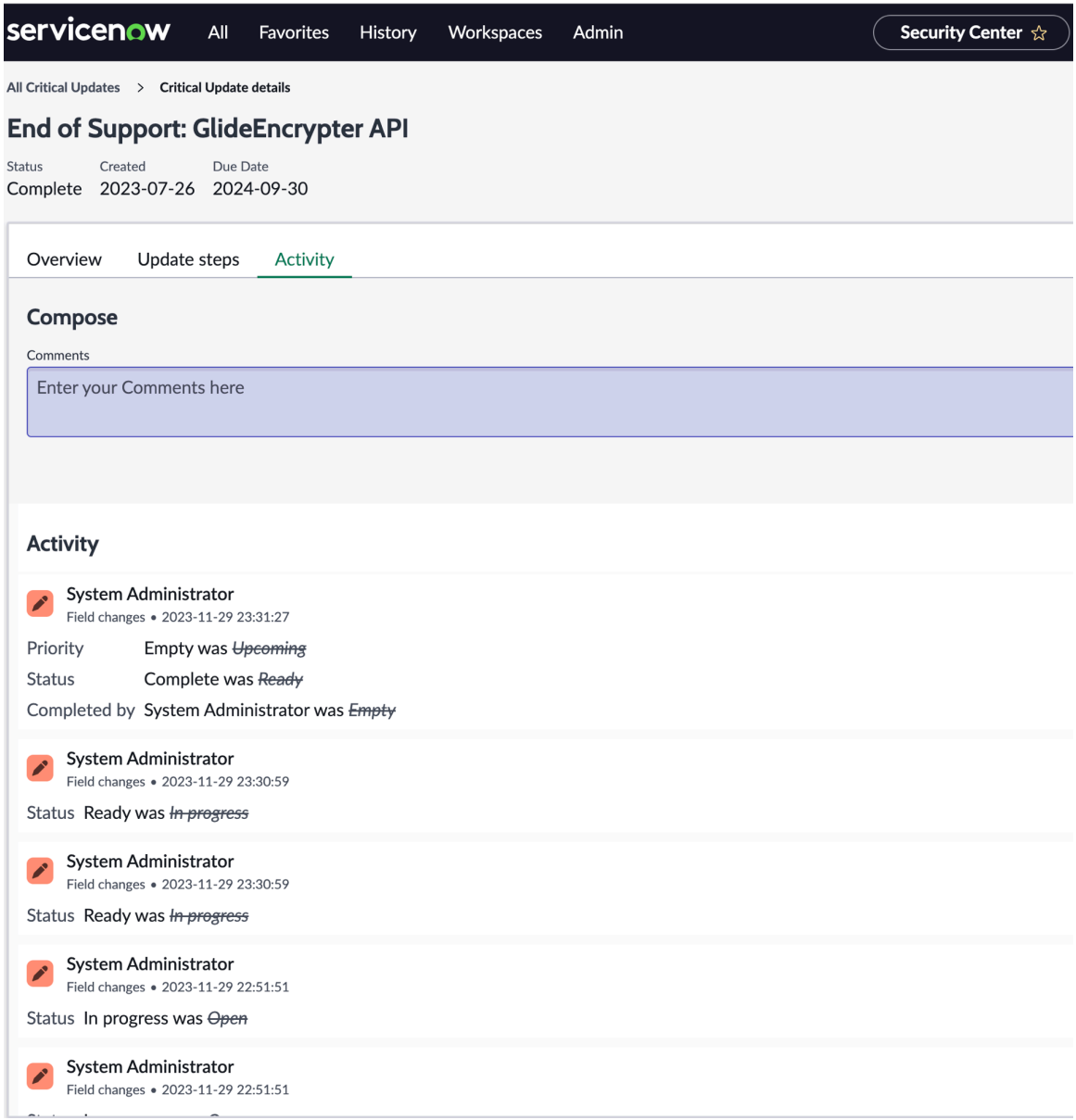
   以下の例では、[完了] ステータスが選択され、[サポート終了:GlideEncrypter **API**] の重要な更新が選択されています。



4. 重要な更新のアクティビティを表示します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



重要な更新に関連するすべてのアクティビティが自動的に記録されます。また、アクティビティにコメントを追加することもできます。

セキュリティ学習

単一のページからセキュリティ学習教材にアクセスします。

[学習] に移動して、セキュリティホワイトペーパー、電子書籍、ナレッジベース (KB) 記事、製品ドキュメント、およびコミュニティディスカッションを統合ビューから参照します。コンテンツは、見出しと内容を端的に表す UI カード別に整理されているため、正しいリソースをすばやく特定できます。

Instance Security Center

インスタンスセキュリティコントロールのコンプライアンスレベルの監視、セキュリティイベントモニタリング測定基準の表示、インスタンスセキュリティ設定の構成と維持はすべて、Instance Security Center 内から行います。Instance Security Center は、複数の主要なセキュリティコンポーネントを単一のコントロールコンソールに統合し、インスタンスベースのセキュリティイベントの検出、保護、応答を支援します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注:

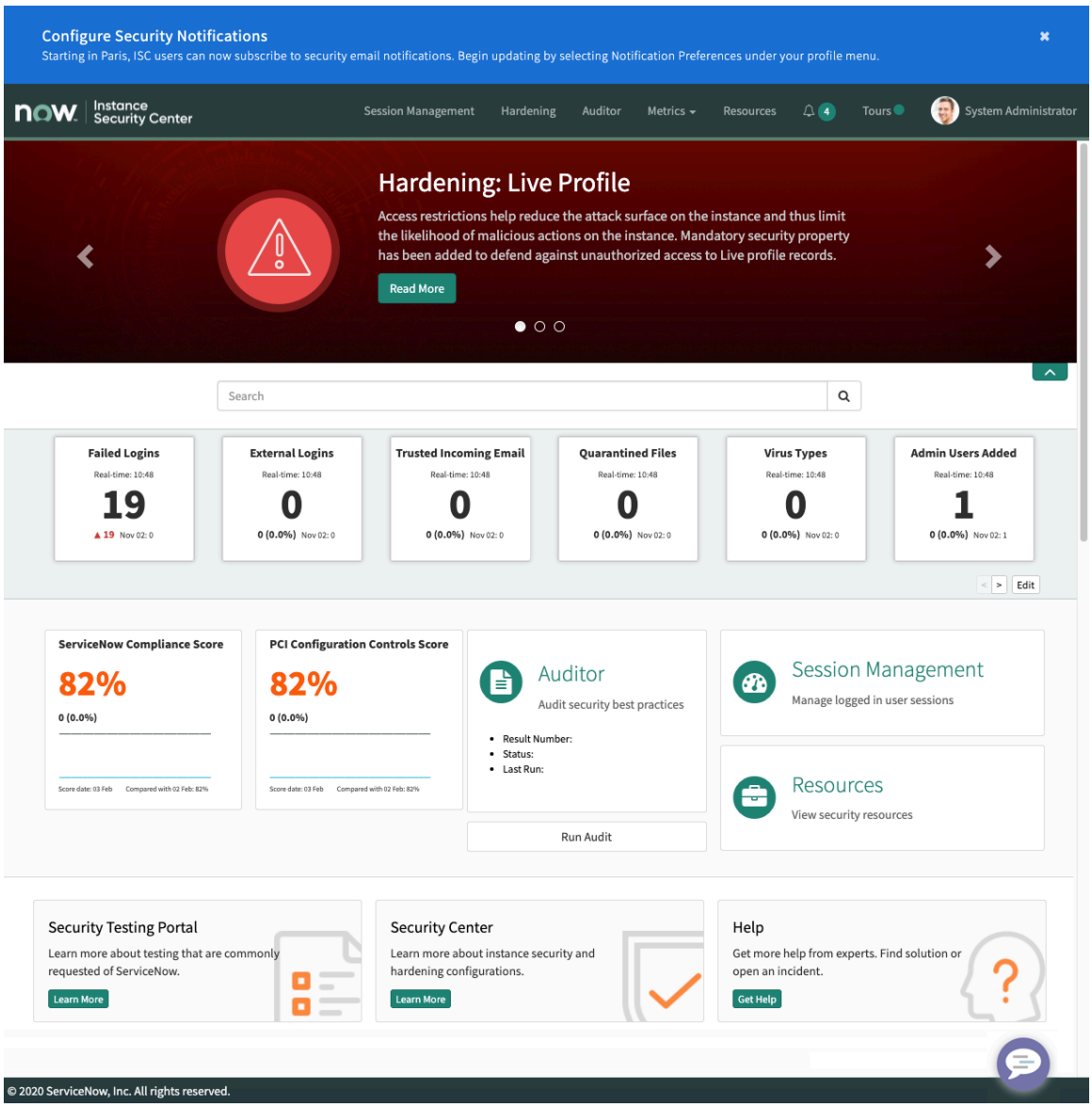
Instance Security Center は今後廃止される予定です。これは非表示になり、新しいインスタンスではアクティブ化されなくなりますが、引き続きサポートされます。この機能の最新のエクスペリエンスは ServiceNow Security Center で提供されます。

詳細については、Now Support ナレッジベースの廃止プロセスに関する記事 を参照してください。

Instance Security Center の概要

Instance Security Center のコンポーネント

Instance Security Center にアクセスするには、次の場所に移動します。 システムセキュリティ > インスタンスセキュリティセンター または システム管理ホームページがあります



Instance Security Center のホームページには、次のようなセキュリティコンポーネントが含まれています。

- 管理者メッセージ
- ローテーションセキュリティバナー

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- 検索
- セキュリティイベントリボン
- 日次コンプライアンススコア
- PCI 構成コントロールスコア
- セッション管理
- ハードニング
- 監査ツール
- 測定基準 (ユーザー、メール、ウイルス対策)
- リソース
- セキュリティ通知
- ツアー
- セキュリティテストポータル
- セキュリティセンター
- ヘルプ
- 仮想エージェントアクセス

Instance Security Center のホームページから、インスタンスのセキュリティコンプライアンススコアを表示し、全体的なセキュリティ健全性を監視できます。その後、インスタンスのセキュリティに関連するシステムプロパティを構成または更新して、セキュリティ要件に準拠させることができます。

注:
Instance Security Center はドメイン分離をサポートしていません。

ユーザーロール

Instance Security Center を使用するには、admin または security_dashboard_user ロールが必要です。

ユーザーごとのサブスクリプションの管理の詳細については、アカウント担当者に問い合わせ Managing per-user subscriptions in Subscription Management てください。

ロール

必要なロール	ユーザー	メリット
admin	管理者はアクセス制御リスト (ACL) ルールをオーバーライドし、すべてのロールチェックに合格できるため、このロールはすべてのシステム機能性、機能、データにアクセスできます。より対象が絞られたロールを使用できる場合は、このロールをユーザーに割り当てないでください。	ツールを活用して Security Center インスタンスのセキュリティ体制を改善し、セキュリティ関連の動作を監視します。
sn_vsc.security_center_viewer	このロールでは、管理者以外のユーザーがツール内の Security	インスタンスのセキュリティ体制を監視し、セキュリティ動

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ロール (続く)

必要なロール	ユーザー	メリット
	Center 情報を表示できますが、 Security Center ツールを変更したり、ツールを使用してインスタンス構成を変更したり Security Center することはできません。 たとえば、プラットフォームオーナー、セキュリティ運用アナリスト、またはコンプライアンスの利害関係者は、 で利用可能な Security Centerセキュリティ KPI、セキュリティインサイト、およびセキュリティ学習教材の一部を表示する必要があるかもしれません。	作を監視するツールを可視化 Security Center します。

⚠ 警告:
アップグレードのたびに Instance Security Center が最新のセキュリティ情報を受信するようにするには、このモジュールをカスタマイズしないでください。インスタンスのセキュリティ設定を変更する場合は、まず非本番環境でテストしてください。

管理者メッセージ

主に管理者向けのメッセージとリマインダーが、ローテーションするセキュリティバナーの上に表示されます。

たとえば、[セキュリティ通知の設定 (Configure Security Notifications)] というメッセージが表示され、管理者がセキュリティ通知の設定を行っていない場合は設定するように促されます。また、そのための適切なページを示します。

注:
管理者メッセージバナーは、管理者以外のユーザーの場合、または管理者ユーザーにアクション可能なアイテムがない場合は表示されません。

ローテーションセキュリティバナー

インスタンスのセキュリティ健全性の監視を支援するために、重要なインスタンスのセキュリティメッセージがローテーションバナーに表示されます。

- 通常、2 ～ 3 件のセキュリティメッセージが定期的にローテーションされます。
- バナーの下部にあるドットは、現在のセキュリティメッセージの合計数を示しています。
- メッセージ間を移動するには、ドットを選択するか、メッセージの両側に表示される矢印を選択します。

バナーの背景色は、メッセージの相対的な重大度を示します。

色	説明
赤	タイムリーな対応、または重大なセキュリティイベントの保護または対応方法に関する推奨事項が必要な、重大なセキュリティ状況

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

色	説明
ダークグレー	重大でない警告メッセージ
青	一般情報メッセージ。

バナーのテキストコンテンツを折りたたむ (最小化する) には、 を選択します。テキストコンテンツを最大化するには、もう一度選択します。

- Instance Security Center を再度使用すると、テキストコンテンツは前のセッションでの使用方法に応じて、折りたたまれるか展開されて表示されます。
- テキストコンテンツ自体が変更されると、すべてのユーザーに対して最大化されて表示されます。

検索

検索バーを使用して、Instance Security Center 全体を対象に、セキュリティ問題の理解と解決に役立つセキュリティリソースを検索します。次のセキュリティ関連リソースを検索できます。

- Now Support ナレッジベース の記事
- Instance Security Center のページ
- 外部 Now Support リンク
- 日次コンプライアンススコアや外部受信メールなど、PA セキュリティウィジェット
- バナーコンテンツ

イベントリボン

イベントリボンを使用して、現在のインスタンスの主要なセキュリティイベントモニタリング測定基準を表示します。

- 測定基準を手動でスクロールするには、左右の矢印キーを選択します。
- イベントリボンを設定するには、[編集] を選択します。

イベントリボンとその設定方法については、「セキュリティイベントの監視」および「セキュリティイベントリボンの構成」を参照してください。

日次コンプライアンススコア

[日次コンプライアンススコア] セクションには、[日次コンプライアンススコア]、[セッション管理]、[ハードニング]、[監査ツール **(Auditor)]**、および [リソース] というタイルが含まれています。

日次コンプライアンススコアを使用して、セキュリティの観点からインスタンスの健全性を評価します。

日次コンプライアンススコアは、パーセンテージスコアです。これは、インスタンスのセキュリティプロパティの現在の設定が、インスタンスセキュリティ強化設定 で公開されているコンプライアンス値にどの程度準拠しているかに基づいています。

- 日次コンプライアンススコアの計算と強化設定の影響の詳細については、「日次コンプライアンススコアの確認とセキュリティプロパティの設定」を参照してください。
- [更新] ボタンを使用すると、管理者は日次コンプライアンススコアをただちに再計算できます。詳細については、「日次コンプライアンススコア、傾向、およびグラフデータの更新方法 」を参照してください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ハードニング

このプロセスを使用して、日次コンプライアンススコアに影響する特定のセキュリティ設定プロパティを調整します。

1. [コンプライアンス構成の強化 (Hardening Compliance Configurations)] ページにアクセスしてインスタンスセキュリティの強化を実行するには、[日次コンプライアンススコア] タイルまたは [ハードニング] リンクを選択します。
2. すべてのセキュリティコントロールを表示するか、推奨されるセキュリティコントロールのみを表示するかを指定します。次に、作業するカテゴリを選択します。
3. 選択したカテゴリで、セキュリティ構成プロパティをそれぞれ設定します。[その他の情報] をクリックすると、プロパティの詳細情報が表示されます。

コンプライアンスをさらに強化するためのセキュリティ構成プロパティの強化と最適化の詳細については、「 インスタンスのセキュリティ設定調整によるコンプライアンスの強化」を参照してください。

傾向データとグラフデータの更新方法の詳細については、「日次コンプライアンススコア、傾向、およびグラフデータの更新方法」を参照してください。

監査ツール

監査ツールを実行してインスタンスをスキャンし、誤ったセキュリティ定義を見つけます。 インスタンスのセキュリティ体制を改善するために修正できる結果を提供します。

[監査人] ページにアクセスするには、[監査人] タイルまたは [監査人] リンクを選択します。詳細については、「誤ったセキュリティ定義のスキャン」を参照してください。

セッション管理

Session Management を使用して次のことを行います。

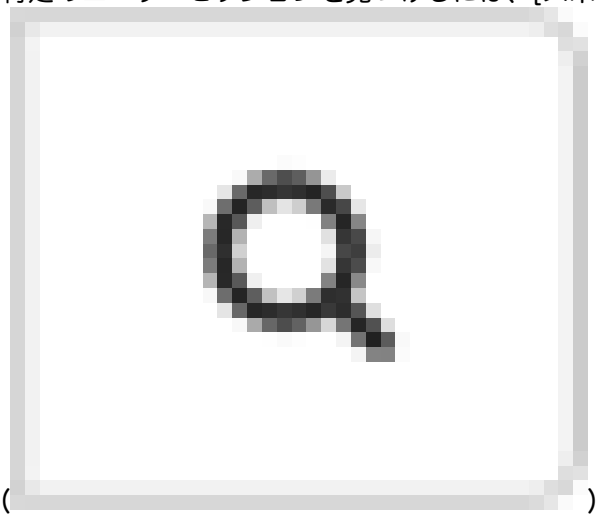
- ユーザーログインセッションを表示および管理します。
- 接続している現在のノードのユーザーログインセッションを確認します。
- ユーザー名や IP アドレスなど、各セッションの詳細情報を表示します。
- セキュリティ上のリスクを引き起こす特定のユーザーセッションを隔離してロックアウトします。

[Session Management] ページにアクセスするには、**[Session Management]** タイルまたはリンクを選択します。

フィールド	説明
ユーザー	このログインセッションに関連付けられたユーザーの名前。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	• 特定のユーザーセッションを見つけるには、[スポットライト検索] アイコン  ( ) を選択して、ユーザー、ユーザーエージェントキーワード、または IP アドレスで検索します。 たとえば、特定タイプのブラウザからの現在のログインをすべて検索する場合は、ブラウザ名をキーワードとして [ユーザーエージェント] フィールドに入力します。 • ユーザー名をクリックして、ユーザープロファイルレコードにアクセスします。ユーザープロファイルを変更できるのは、admin ロールが割り当てられている場合のみです。 **注:** ユーザープロファイルの詳細については、「ユーザーの作成」を参照してください。
MFA	ログインしているユーザーに対してマルチファクター認証 (MFA) が有効になっているかどうかを示すチェックボックス。MFA の詳細については、「マルチファクター認証 (MFA)」を参照してください。
アクティブ	ログインしているユーザーがアクティブか非アクティブかを示すチェックボックス
ユーザーエージェント	ユーザーログインセッションのブラウザのタイプとデバイスのオペレーティングシステム
IP アドレス	ログインしているユーザーの IP アドレス。
前回アクセス	このユーザーセッションが最後にインスタンスにアクセスした日時。 **注:** 特定のログインセッションの詳細情報を表示するか、またはセッション自体をロックアウトするには、[ユーザーエージェント]、**[IP** アドレス]、または [前回アクセス] フィールドを選択します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

測定基準

次のタイプの測定基準の詳細を表示します。

測定基準のタイプ	説明
ユーザー	インスタンス内のユーザーアクティビティに関連付けられているセキュリティ測定基準。 [ユーザー測定基準] ページにアクセスするには、[測定基準] リンクを選択し、[ユーザー測定基準] を選択します。
エクスポート	インスタンスからエクスポートされるデータに関連付けられているセキュリティ測定基準。 [測定基準をエクスポート] ページにアクセスするには、[測定基準] リンクを選択し、[測定基準をエクスポート] を選択します。
認証	使用頻度の低い IP アドレス、失敗したログイン、ユーザーが使用する認証スキームのタイプなど、認証に関連するセキュリティ測定基準。 [測定基準をエクスポート] ページにアクセスするには、[測定基準] リンクを選択し、[認証測定基準] を選択します。
メール	インスタンスの受信メールに関連する例外動作に関連付けられたセキュリティ測定基準。 [メール測定基準 (Email Metrics)] ページにアクセスするには、[測定基準] リンクを選択し、[メール測定基準 **(Email Metrics)]** を選択します。
ウィルス対策	インスタンス内のウイルス対策イベントアクティビティに関連付けられているセキュリティ測定基準。 [ウイルス対策測定基準 (Antivirus Metrics)] ページにアクセスするには、[ウイルス対策] タイルを選択するか、[測定基準] リンクを選択して、[ウイルス対策] を選択します。

注:
各タイプの測定基準の監視の詳細については、「インスタンス測定基準の監視」を参照してください。

リソース

インスタンスセキュリティに関連する Now Support ナレッジベース 記事、リソース、およびブログにアクセスします。これらのリソースには、セキュリティ設定、コーディング、コンプライアンス、修正、および関連トピックが含まれます。[リソース] ページにアクセスするには、以下の手順を実行します。

1. [リソース] タイルまたはリンクをクリックします。
2. [リソース] ページで、カテゴリを選択します。

カテゴリ	説明
推奨ガイドライン	インスタンスセキュリティ強化設定 およびセキュアコーディングガイド [KB0623354] に関する記事など、推奨されるセキュリティガイドラインへのアクセス

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

カテゴリ	説明
セキュリティリソース	ナレッジベース内の、以下のようなセキュリティ関連リソースへのアクセス ○ カスタマーインスタンスのセキュリティテスト ○ クラウドセキュリティ、信頼、およびコンプライアンスセンターに関するナレッジベース記事

セキュリティ通知

Instance Security Center に、通知ベルアイコン ( ) が未読のセキュリティ通知の合計数とともに表示されます。通知は、既読としてマークするまで保持され、未読としてカウントされます。

1. ベルアイコンをクリックすると、未読のセキュリティ通知の最初の 5 件が表示されます。

   管理ログイン、管理者ロック解除 **(Admin Unlocked)**、失敗したログイン、高権限ロール **(High Privilege Role)**、代理操作、セキュリティ昇格、および週次ダイジェスト **(Weekly Digest)** のイベントがインスタンスで発生すると、通知が表示されます。これらのセキュリティイベントの詳細については、「セキュリティイベントの監視」を参照してください。

2. 特定のセキュリティイベントの詳細情報を表示するには、[通知] を選択します。

   たとえば、高権限ロールの通知をクリックすると、ロール (sys_user_role) テーブルを表示できます。このテーブルを使用して、暦日に特権ロールが割り当てられたユーザーを確認します。この履歴を使用すると、ロールが適切に割り当てられているかどうかを判断できます。

3. 未読の通知が 5 件より多い場合は、[すべての通知を表示] を選択すると、すべての未読通知が一覧表示される [すべての通知] ページにアクセスできます。
   - 特定のセキュリティイベントの詳細情報を表示するには、[通知] を選択します。
   - リストされているすべての通知を既読にするには、[すべて既読としてマーク] を選択します。

注:
管理者は、セキュリティイベントのタイプごとに特定のタイプの通知を送信するように設定することもできます。詳細については、「セキュリティイベント通知の設定 」を参照してください。

ツアー

[ツアー] リンクをクリックして、Instance Security Center のビジュアルガイドツアーを表示します。

- チュートリアルには、 ホームページにリストされているセキュリティモニタリング機能のみが含まれています。
- ホームページのタイルまたはリンクを選択したときにアクセスするセキュリティ機能は含まれません。

セキュリティテストポータル、セキュリティセンター、およびヘルプ

Now Support サービスポータル は、インスタンス、タスク、およびアカウントを管理するために使用する中心的なリソースです。インスタンスのセキュリティおよび技術的な問題を診断して解決するために利用できる有用なリソースにもアクセスできます。

これらのリソースにアクセスするには、次のタイルで [詳細] または [ヘルプ] を選択します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

タイル	説明
セキュリティテストポータル	Now Support セキュリティテストポータルのセキュリティダッシュボードにアクセスします。
セキュリティセンター	Now Support セキュリティポータルのセキュリティコンプライアンスにアクセスします。
ヘルプ	Now Support セキュリティポータルの、次のヘルプリソースにアクセスします。 • エキスパートに一般的な質問に対する回答を見つけてもらうことができます。 • ケースをオープンして、ServiceNow グローバルテクニカルサポートに問題または機能停止を報告します。 • 以下ののようなセルフサービスサポートリソース ◦ ビデオ ◦ ドキュメント ◦ ServiceNow Community ◦ ナレッジベース ◦ 既知のエラーポータル ◦ セキュリティ RFX データベース • 使用が推奨される ServiceNow Community の質問

仮想エージェントアクセス

仮想エージェント は、メッセージングインターフェイス内の会話を通じてユーザーサポートを提供するためのプラットフォームです。

関連プラグインがインストールされている場合、管理者は [仮想エージェント] アイコンをクリックして仮想エージェントおよび 自然言語理解 (NLU) (NLU) の機能にアクセスできます。

次のタスクを実行できます。

- セキュリティ関連の質問をして、簡単な要約回答と詳細への参照リンクを取得する
- 次のようなプロセスに関連する回答を取得する
  - Instance Security Center
  - プラットフォームセキュリティ
  - ServiceNow セキュリティポリシー
  - 信頼、ガバナンス、リスク
- Now Support Security ポータルでナレッジベースのトピックなどのセキュリティ関連リソースを検索する

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注:
仮想エージェントを使用およびアクティブ化する方法の詳細については、以下を参照してください。

- 仮想エージェント
- ISC 仮想エージェントインターフェイスのアクティブ化

Instance Security Center から ServiceNow Security Center への移行

Instance Security Center (ISC) から ServiceNow Security Center (SSC) に移行する際の主な違いについて説明します。

ServiceNow Security Center (SSC) は、組織が ServiceNow 展開のセキュリティを管理するのを支援するように設計された一連の専用ツールで構成される新しいセキュリティアプリケーションです。Security Center を使用すると、組織はシームレスなユーザーエクスペリエンスを使用して、セキュリティ体制を改善し、コンプライアンスレベルを強化できます。インスタンス セキュリティ センター (ISC) は従来の製品です。ServiceNow は、2024 年 9 月に予定されている Now Platform Xanadu リリースをもって、ISC のサポートを終了します。その結果、SSCは今後採用する推奨ソリューションです。

SSC のハードニング設定の更新

ServiceNow Security Center (SSC) のハードニング設定に加えられた更新について説明します。

機能拡張	ISC と SSC
拡張セキュリティ強化設定	SSC には、以前のバージョンの ISC と比較してはるかに多くの強化設定が含まれています。今後の SSC バージョンでは、引き続き設定の数が拡張されます。

強化設定の簡素化されたスコアリング	• ISC は、高、中、低の設定に対して特定の割合の影響度を確認する計算式を使用します。
	• SSC は別の計算式を使用します。
	  ○ 設定ごとに独自のスコアの重み付けがあります。
	  ○ ハードニングコンプライアンススコアは、分子 (すべての準拠設定の合計) を分母 (すべての設定の影響度の重み付けの合計) で除算することによって計算されます。

データを評価するためのユーザーエクスペリエンスの向上	• 2 つの異なる日付のコンプライアンススコアを比較します。 • コンプライアンススコアを線グラフで可視化し、分析ハブを使用してデータを分析します。

SSC での一般的なセキュリティハードニングタスクの実行

以下は、SSC で一般的なセキュリティハードニングタスクを実行するための手順です。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

最新スコアを確認する	次のいずれかに移動します。 • ホーム ホームページ を参照してください。 • ハードニング>スコア ハードニングコンプライアンススコアのトレンド を参照してください。
最新スコアを更新する	SSC ホームページで、[スコアを更新] を選択します。
設定構成を変更する	次のいずれかのページで設定名を選択して [設定] 詳細ページを表示します。そこで、構成の変更、以前のアクティビティの確認、メモの追加を行うことができます。 • ホーム • [ハードニング] > [すべての設定] • ハードニング>スコアの比較 「ハードニングコンプライアンススコアの増加」を参照してください。
コンプライアンススコアの再計算のスケジュールを設定する	システムがコンプライアンススコアの更新をトリガーするタイミングをスケジュールします。 • sysauto_script テーブルで、SC - Calculate Compliance Monthly でフィルタリングします。 • 希望するスケジュールを反映するようにレコードを変更します。

SSC のセキュリティ KPI と測定基準の更新

ServiceNow Security Center (SSC) のセキュリティ KPI と測定基準に加えられた更新について説明します。

機能拡張	ISC と SSC
KPI の機能拡張	SSC では以下を実行できます。 • 経時的なスコアの傾向を確認します。 • 同じインターフェイスと分析機能を使用して、すべての KPI と測定基準を監視します。
測定基準の機能拡張	SSC で次の機能拡張が行われました。 • 50 を超える新しい測定基準が追加されています。 • 同じユーザーインターフェイスから KPI と測定基準を監視および分析できます。 • 測定基準のターゲットとしきい値を作成できます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

SSC のセキュリティ KPI とアクセスの測定基準

次のいずれかの操作を行います。

- 移動先 ホーム > 測定基準をクリックし、左側のナビゲーション メニューから [メトリック] を選択します。
- 移動先 ホーム > すべての測定基準をクリックし、テーブルから [メトリック] を選択します。

SSC でのセキュリティスキャナーの更新

ServiceNow Security Center (SSC) のセキュリティスキャナーに加えられた更新について説明します。

機能拡張	ISC と SSC
新機能	SSC には、次の新機能が含まれています。 • スキャンを手動で実行するか、特定の時間に実行するようにスケジュールします。 • 独自のスキャンチェックを作成します。 • 独自のスキャンスイートを作成します。 • 2 つのスキャンの結果を比較します。
拡張されたメール機能	インスタンスで新しいセキュリティイベントが発生したときにアラートを受け取るように、メール通知を設定します。

SSC での一般的なセキュリティスキャナータスクの実行

以下は、SSC で一般的なセキュリティスキャナータスクを実行するための手順です。

監査ツールスイートスキャンの実行	**1.** 移動先 スキャナー > スイート. **2.** リストから監査人スイートを選択します。 **3.** [セキュリティ スキャンの実行] を選択します。
スイートスキャン結果の表示	移動先 スキャナー > 結果.

SSC の新しいセキュリティ機能

ServiceNow Security Center (SSC) に導入された新しいセキュリティ機能について説明します。

ServiceNow Security Center に次の新機能が追加されました。

- セッションの監視: 新しいメトリック ツールを使用して、時間の経過に伴うセッション アクティビティを視覚化できます。
- リソースの検索：すべてのセキュリティ学習リソースが 1 つのページにグループ化されるようになりました。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

セッションアクティビティの監視	**1.** [測定基準] に移動します。 **2.** 左側のナビゲーションの [セッション管理] で、[アクティブ セッション] を選択します。
学習リソースへのアクセス	[学習] に移動します。

セキュリティイベントの監視

潜在的なセキュリティイベントを特定して防止できるように、インスタンスのイベント測定基準を分析します。

[インスタンスセキュリティ (Instance Security)] ホームページにあるイベントリボンでは、これらの測定基準とそれに付随する詳細を分析して、インスタンス内の潜在的なセキュリティイベントを特定できます。

- イベント測定基準ごとにリアルタイムの単一スコア数が表示されます。この数値は、このインスタンスで 1 日にイベントが発生した回数を示しています。これらの単一スコアレポートは、対応するイベントが発生すると自動的に更新されます。
- 各イベント測定基準には、日付範囲内のコンプライアンスの傾向とグラフ情報も含まれています。パフォーマンス分析ジョブを実行する場合、この情報は毎日更新されます。詳細については、「イベント傾向の詳細分析」セクションを参照してください。

イベントタイプ

次のタイプのイベントのうち、少なくとも 6 件のイベントを監視できます。イベントが 6 件を超える場合は、イベントリボンの下にある左右の矢印を使用してスクロールします。イベントリボンの設定方法については、「セキュリティイベントリボンの構成」を参照してください。

通知設定	説明
管理ログイン	admin ロールを割り当てられたユーザーが、暦日の間にこのインスタンスにログインしようとした回数。
管理者ユーザーが追加されました	暦日の間にこのインスタンスに追加された admin ロールを持つユーザーの数。たとえば、カウントが 10 であるが、admin ロールを割り当てられたユーザーが 4 名の場合は、セキュリティ上の問題がある可能性があります。
外部の受信メール	詳細については、「メール測定基準 」を参照してください。
外部ログイン	暦日の間にこのインスタンスにログインした、snc_external ロールを持つユーザーの数 通常、これらのログインは、メンテナンス、サポート、コンサルティング、または監査の目的で発生します。この測定基準を監視することで、外部ログイン試行が正規のものであり、潜在的なセキュリティ上の問題ではないことを確認できます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

通知設定	説明
	外部ユーザーロールの割り当ての詳細については、「明示的なロール」を参照してください。
失敗したログイン	暦日の間にこのインスタンスで失敗したログインの数 この測定基準は、ログインが試行され、インスタンスのセキュリティが侵害されていることを示している可能性があります。
代理操作	暦日の間にこのインスタンスで代理操作されたログインの数。ユーザーの代理操作の詳細については、「ユーザーの代理操作を行う」を参照してください。
隔離されたファイル	暦日の間にこのインスタンスで アンチウイルススキャン を実行したときに隔離されたファイルの数。隔離されたファイルと アンチウイルススキャン の詳細については、「ウイルス対策測定基準」および「アンチウイルススキャン」を参照してください。
セキュリティ昇格	暦日の間に、セキュリティ管理者が標準ユーザーに対して、割り当てられたユーザーロールを高い権限のセキュリティロールに変更することによって、セキュリティ権限を強化した回数。このような高権限のセキュリティ ロールには、oauth_admin、admin、security_admin、および impersonator が含まれます。 • この測定基準は、誰かが無許可のユーザーのセキュリティを昇格しようとした可能性があることを示しています。特定のセキュリティ侵害を検出するために、この測定基準を単独で使用しないでください。代わりに、この測定基準は、セキュリティ侵害の発生を確認するために別の測定基準をチェックする必要があることを示す指標として扱ってください。 • ユーザーセキュリティの昇格の詳細については、「特権ロールへの昇格」および「昇格された権限ロール」を参照してください。
SNC ログイン	暦日の間にハイホッピング技術を使用してこのインスタンスにログインしたカスタマーサービス & サポート担当者の数。通常、これらのログインは、メンテナンス、サポート、コンサルティング、または監査の目的で発生します。 ServiceNow 社員のアクセスを制御する方法については、「ServiceNow アクセス制御」を参照してください。
スパム	詳細については、「メール測定基準 」を参照してください。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

通知設定	説明
信頼できる受信メール	詳細については、「メール測定基準 」を参照してください。
信頼できない受信メール	詳細については、「メール測定基準 」を参照してください。
ウイルスタイプ	暦日の間にこのインスタンスで発生したさまざまなタイプのウイルス対策イベントの数。ウイルス対策イベントタイプの詳細については、「ウイルス対策測定基準」を参照してください。

イベント傾向の詳細分析

イベント測定基準の傾向の詳細を表示するには、イベント数をクリックして [分析ハブ] ページにアクセスします。インスタンスに表示される詳細は、測定基準のタイプによって異なります。

たとえば、[セキュリティダッシュボードイベントログ] ページに試行の失敗を一覧表示するには、次の操作を実行します。

- [失敗したログイン] 測定基準を選択します。
- [アナリティクスハブ] ページで、[レコードを表示] をクリックします。
- 失敗したログイン試行の 1 つをクリックします。
- 詳細には、ログインを試行したユーザーの名前、ユーザーの IP アドレス、およびユーザーがアクセスしようとしたテーブル名が含まれます。

アナリティクスハブ でイベントしきい値トリガーを設定して、インジケーターのスコアの範囲内で特定のイベントが発生したときにアラートを提供できます。希望のスコアとイベントの実際のスコアとの差異を視覚化できるターゲットを設定することもできます。

たとえば、[失敗したログイン] の測定基準のしきい値を 10 に設定できます。1 日に 10 回以上ログイン試行が失敗すると、特定のセキュリティ担当者にアラートが送信されます。同様のターゲットを設定して、1 日に 10 回ログインに失敗したときに、[アナリティクスハブ] で視覚的にハイライト表示させることもできます。

[イベント] リボンタイルと [アナリティクスハブ] に表示される傾向データとグラフは、パフォーマンス分析ジョブが現地時間の 02:00 に実行された後に更新されます。詳細については、「日次コンプライアンススコア、傾向、およびグラフデータの更新方法 」を参照してください。

関連情報

Instance Security Center

Now Intelligence

分析ハブ

Performance Analytics のターゲットとしきい値

セキュリティイベントリボンの構成

Instance Security Center ホームページのセキュリティイベントリボンを構成して、運用内でインスタンスセキュリティの追跡に関連するイベントのみを含めるようにします。リボンに表示されるセキュリティイベントタイルの順序を変更することもできます。

始める前に

必要なロール：security_dashboard_user または管理者

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

このタスクについて
セキュリティイベントリボンには、当初、標準セキュリティイベントの完全なセットが入力されています。自身の組織に関連しないイベントを削除してリボンをカスタマイズできます。

- たとえば、セキュリティ上の問題が内部担当者のアクションに起因していると思われる場合は、[管理ログイン]、[追加された管理者ユーザー]、および [セキュリティ昇格] のイベントインジケーターを含めます。
- これらのインジケーターは、管理者ロールを持つユーザーがログインを試行した回数、また管理者ユーザーが追加された場合は、セキュリティロールを昇格させるために何が試行されたかを監視します。

注:
イベントリボンに表示されるセキュリティイベントのタイプについては、「セキュリティイベントの監視」を参照してください。

手順

1. 移動先 すべて > システムセキュリティ > インスタンスセキュリティセンター.
2. イベントリボンで、[編集] (< > Edit) をクリックします。
   [イベントを編集] フォームの [選択済み] 列には、既にリストされているイベントが含まれています。
3. イベントリボンにセキュリティイベントを追加するには、セキュリティイベントを [利用可能] 列から [選択済み] 列に移動します。
   リボンに表示されるイベントの順序を変更するには、イベントを選択し、上向きと下向きの矢印をクリックして正しい位置に移動します。
   - Instance Security Center のイベントリボンに表示される順序でイベントを配置します。
   - [利用可能] 列の上部に配置したイベントは、Instance Security Center のイベントリボンの左側に順番に表示されます。列の下部に配置されたイベントは、イベントリボンの右側に表示されます。
4. イベントリボンからセキュリティイベントを削除するには、次の操作を実行します。
   - [選択済み] 列で、イベントリボンから削除するセキュリティイベントを選択します。
   - イベントを [選択済み] 列から [利用可能] 列に移動します。
5. [保存] をクリックします。

関連情報

Instance Security Center

セキュリティイベント通知の設定

特定のセキュリティイベントが発生したときに受信する通知のタイプを設定します。タイプごとに、メール、Now Mobile のプッシュ通知、または Slack や Microsoft Teams などのサードパーティのメッセージングアプリケーションで通知を受信するかどうかを指定します。

始める前に
サードパーティのメッセージングアプリケーションでセキュリティイベント通知を送信できるようにするには、Messaging Notification (com.glide.notification.messaging) プラグインをアクティブ化する必要があります。個々のユーザーが独自に設定する必要があります。詳細については、「メッセージングアプリケーションでの通知」を参照してください。

必要なロール：admin。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

手順

1. Instance Security Center のホームページでプロファイルメニューをクリックし、[通知設定] をクリックします。

通知設定

通知設定	説明
管理ログイン	管理者ロールを割り当てられた他のユーザーが別の IP アドレスからこのインスタンスにログインするたびに、選択したタイプの通知を送信します。
管理者によるロック解除 (Admin Unlock)	高い権限を持つユーザーのアカウントのロックが解除されるたびに、選択したタイプの通知を送信します。
失敗したログイン	他のユーザーが *glide.user.max_unlock_attempts* プロパティで定義された試行回数よりも少ない回数でこのインスタンスへのログインに失敗するたびに、選択したタイプの通知を送信します。このプロパティを設定しない場合、デフォルト値は 5 です。 このプロパティの詳細については、「失敗したログイン試行のロックアウトを指定する」を参照してください。
追加された HP ロール (HP Role Added)	高い権限のセキュリティロール (oauth_admin、admin、security_admin、および impersonator ロールなど) が別のユーザーに付与されるたびに、選択したタイプの通知を送信します。 ユーザーセキュリティの昇格の詳細については、「特権ロールへの昇格」および「昇格された権限ロール」を参照してください。
代理操作	他のユーザーが代理操作を行うたびに、選択したタイプの通知を送信します。 ユーザーの代理操作の詳細については、「ユーザーの代理操作を行う」を参照してください。
セキュリティ昇格	他のユーザーがこのインスタンスでセキュリティ管理者ロールに昇格するたびに、選択したタイプの通知を送信します。
週次ダイジェスト	選択したタイプの通知について週次ダイジェストを送信します。含まれる内容： ○ 1 週間にこのインスタンスで行われたすべてのセキュリティアクティビティのサマリー ○ インスタンスの現在の日次コンプライアンススコア

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

2. セキュリティイベントのタイプごとに、適切なチェックボックスをオンにして送信する通知のタイプを指定します。
   それぞれに複数の通知方法を選択できます。

3. [保存] をクリックします。

日次コンプライアンススコアの確認とセキュリティプロパティの設定

日次コンプライアンススコアの測定基準とセキュリティ構成プロパティを確認して、提案されたセキュリティ要件にインスタンスが準拠しているかどうかを確認します。[コンプライアンス構成の強化 (Hardening Compliance Configurations)] ページで非準拠のセキュリティプロパティを更新すると、日次のコンプライアンススコアに影響を与えることがあります。

日次コンプライアンススコアは、パーセンテージスコアです。これは、インスタンスのセキュリティプロパティの現在の設定が、インスタンスセキュリティ強化設定 で公開されているコンプライアンス値にどの程度準拠しているかに基づいています。

インスタンスの日次コンプライアンススコアを定期的に確認します。日次コンプライアンススコアを評価するときは、次のガイドラインに従ってください。

- 90 % 以上は、インスタンスが重要なセキュリティコントロールに準拠していることを示します。
- 50 % 以上 90 % 未満の場合は、セキュリティコンプライアンスのレベルが中程度であることを示します。
- 50 % 未満は、セキュリティコンプライアンスのレベルが低いことを示します。

インスタンスのセキュリティ設定調整によるコンプライアンスの強化

[コンプライアンス構成の強化 (Hardening Compliance Configurations)] ページを使用して、インスタンスの日次コンプライアンススコアに影響する非準拠セキュリティプロパティを強化して最適化します。これを使用することで、インスタンスは公開されたセキュリティ強化基準に確実に準拠し、同時に会社のセキュリティ要件を満たせるようになります。

始める前に
必要なロール：security_dashboard_user または admin

詳細な説明、コンプライアンス値、Now Platform のセキュリティ関連システムプロパティおよびプラグインについては、「インスタンスセキュリティ強化設定」の内容を参照してください。

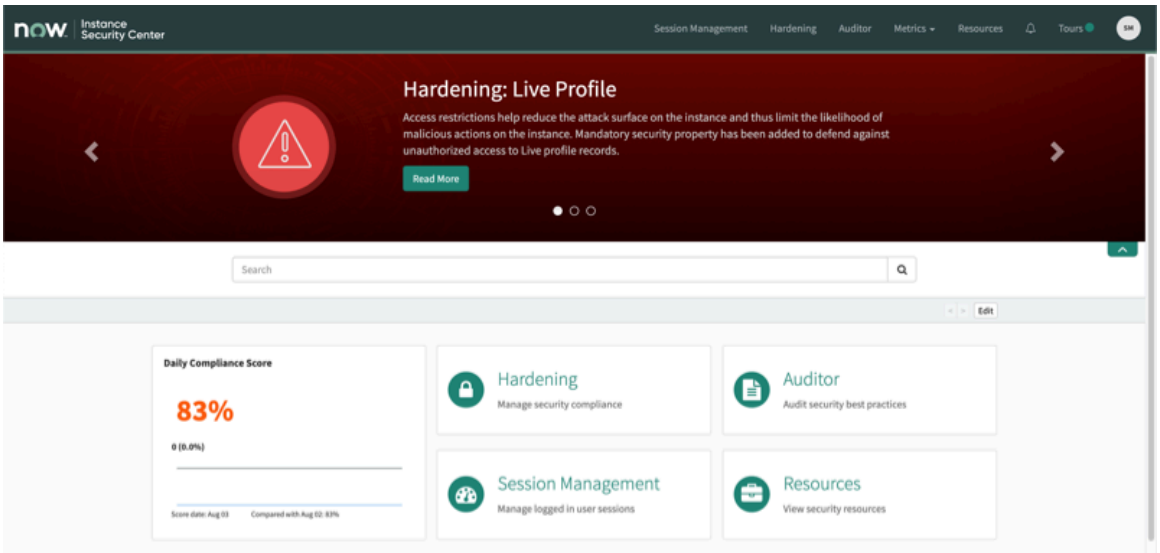
- 一部のコンプライアンス値がインスタンスに適していない場合でも、セキュリティ関連のプロパティを設定または更新するときは、必ずインスタンスセキュリティ強化設定を参照してください。
- これらのプロパティを更新するときは、インスタンスが引き続き期待どおりに動作することを確認してください。セキュリティへの影響を判断するには、専門知識を持つ適切な内部担当者に相談してください。

> **注:**
> admin ロールを持っている場合は、セキュリティコントロールを表示して編集できます。security_dashboard_user ロールを持っている場合は、セキュリティコントロールを表示できますが、編集することはできません。

手順

1. 移動先 すべて > システムセキュリティ > インスタンスセキュリティセンター.
2. [日次コンプライアンススコア] タイルまたは [ハードニング] リンクをクリックして、[コンプライアンス構成の強化 (Hardening Compliance Configurations)] ページにアクセスします。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

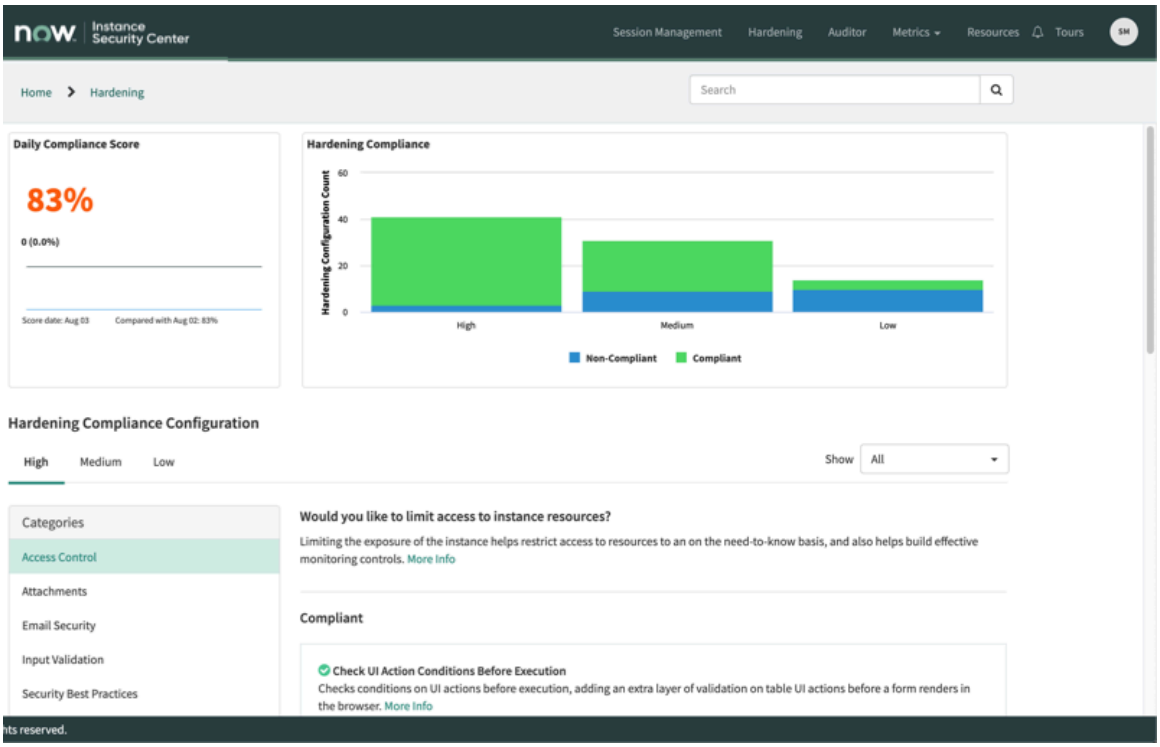


3. [コンプライアンスの強化] チャートで、準拠および非準拠のセキュリティ構成プロパティの統計情報を表示します。

オプション	説明
準拠	インスタンスセキュリティ強化設定のコンプライアンス値に準拠するセキュリティ構成プロパティの数 **注:** [コンプライアンス構成の強化 (Hardening Compliance Configurations)] では、準拠するセキュリティプロパティの設定を変更することはできません。変更する場合は、[システムのプロパティ] で更新する必要があります。詳細については、「システムプロパティを追加する」を参照してください。
非準拠	インスタンスセキュリティ強化設定のコンプライアンス値に準拠しないセキュリティ構成プロパティの数。非準拠プロパティの設定を更新できます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



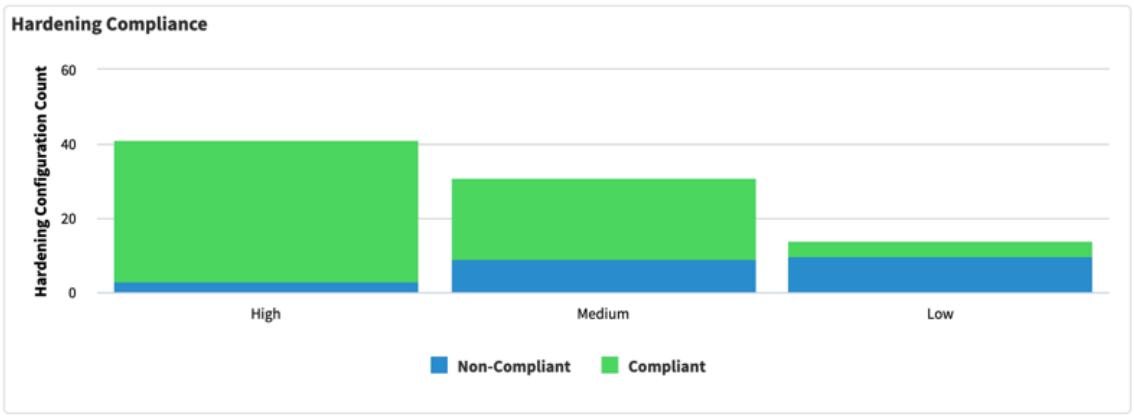
注:
日付範囲内の準拠または非準拠のセキュリティスコアの数を表示するには、[日次コンプライアンススコア] の下のスライダーにある青いドットを移動します。

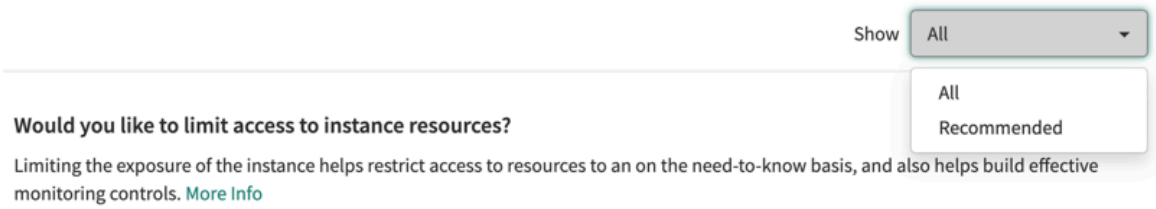
4. チャートの下にある [表示] リストで、すべてのセキュリティ構成プロパティにアクセスするのか、推奨されるプロパティのみにアクセスするのかを指定します。

オプション	説明
すべて	(デフォルト) 選択した各カテゴリのすべての準拠および非準拠のセキュリティ構成プロパティ
推奨	選択した各カテゴリには、推奨されるセキュリティ構成プロパティのみが表示されます。これらのセキュリティ構成プロパティは、Now Platform を保護するために使用される最も重要なプロパティを選択したサブセットです。 これらのセキュリティ構成プロパティは、Now Platform を保護するために設定する必要がある最低限の設定数であると考えてください。 **注:** インスタンスを完全に保護するには、[すべて] オプションを使用します。これには、推奨されるすべてのセキュリティ構成プロパティも含まれます。

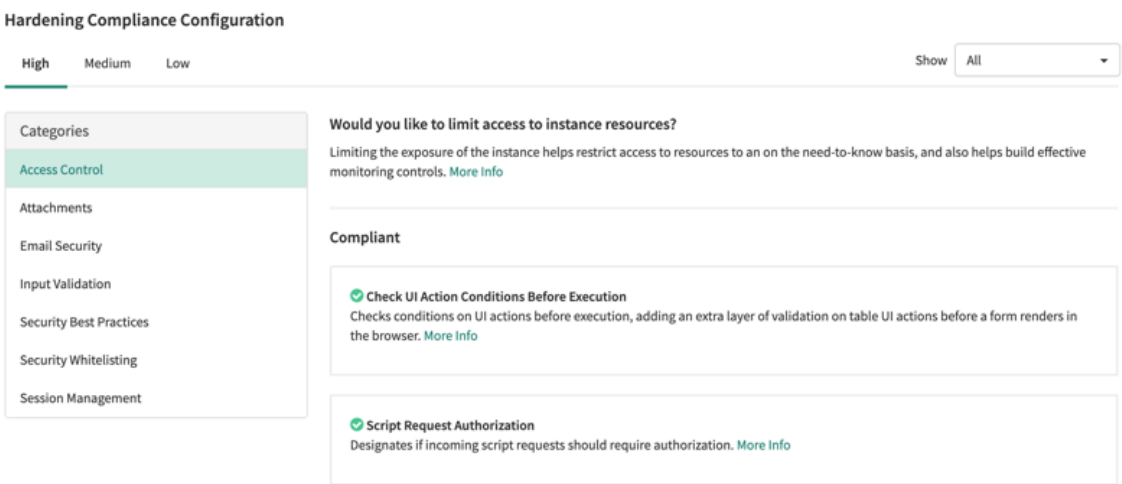
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。





5. [カテゴリ] で、アクセスしたいセキュリティ構成プロパティを含むカテゴリを選択します。



オプション	説明
アクセス制御	アクセス制御は、特定のリソースの使用をどのユーザーが許可されているかに基づいて、特定のリソースへのユーザーアクセスを許可するか拒否するかを決定します。詳細については、「インスタンスセキュリティ強化設定」の「アクセス制御」を参照してください。
添付ファイル	添付ファイルのセキュリティコントロールを使用すると、受信した添付ファイルを検証して、攻撃者から送信された悪意のあるファイルからインスタンスを保護できます。詳細については、「インスタンスセキュリティ強化設定」の「添付ファイル」を参照してください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

オプション	説明
メールセキュリティ	メールセキュリティには、すべての受信メールに対応する適切なセキュリティポリシーを確実に実施するために管理者が構成できる、セキュリティ構成プロパティが含まれます。詳細については、「インスタンスセキュリティ強化設定」の「メールセキュリティ (インスタンスセキュリティ強化)」を参照してください。
入力の検証	入力検証には、ソースに関係なく管理者が不正な形式のデータの入力を最小限に抑えるために構成できる、セキュリティ関連プロパティが含まれています。詳細については、「インスタンスセキュリティ強化設定」の「入力の検証」を参照してください。
安全な通信	セキュア通信プロパティは、HTTP トラフィックの転送を保護するために管理者が構成できるプロパティです。詳細については、「インスタンスセキュリティ強化設定」の「安全な通信」を参照してください。
セキュリティベストプラクティス	セキュリティのベストプラクティスには、管理者が一定の時間間隔内に定期的に実行する必要があるセキュリティタスクが含まれており、関連する構成プロパティが含まれています。 詳細については、「インスタンスセキュリティ強化設定」を参照してください セキュリティベストプラクティス 。
セキュリティ包含リスト	セキュリティ包含リストには、動作を既知の包含リストに制限するように管理者が構成できる、セキュリティ関連プロパティが含まれています。詳細については、「インスタンスセキュリティ強化設定」の「セキュリティ包含リスト」を参照してください。
セッション管理	Session Management には、管理者が Now Platform で安全なセッション管理を確保するために構成できる、セキュリティ関連プロパティが含まれています。詳細については、「インスタンスセキュリティ強化設定」の「セッション管理」を参照してください。

6. 選択したカテゴリの非準拠セキュリティプロパティを設定します。
   - 特に指定しないかぎり、スイッチをオンにスライドするとセキュリティプロパティが推奨設定に設定されます。たとえば、ほとんどのコントロールは true または false に設定しますが、中には値の入力 (カンマ区切りの値リストなど) が必要なものがあります。
   - セキュリティコントロールのための専用のインスタンスセキュリティ強化設定トピックにアクセスして詳細を確認するには、[その他の情報] をクリックします。

タスクの結果

日次コンプライアンススコアは、非準拠のセキュリティコントロール設定に対して行われた変更に応じて増減します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

関連情報

Instance Security Center

日次コンプライアンススコア、傾向、およびグラフデータの更新方法

Instance Security Center の傾向およびグラフデータは、パフォーマンス分析ジョブがローカル時間の 02:00 に実行された後に更新されます。これは [日次コンプライアンススコア] タイル、イベントリボンのタイル、さらにイベントタイルの 1 つをクリックした場合には [アナリティクスハブ] ページの詳細に表示されます。

[AppSec] 日次データ管理ジョブは、夜間に次のタスクを実行する定期スケジュールジョブです。

1. 最初にスケジュール設定した時点で、[AppSec] 日次データ管理ジョブと [PA AppSec] 日次データ収集ジョブに、有効なユーザーがアサインされているかどうかが確認されます。
   - [実行方法] フィールドに有効なユーザーを入力した場合、ジョブは処理を続行します。有効なユーザーとは、インスタンスからロックアウトされておらず、admin ロールが割り当てられているユーザーのことです。
   - 無効なユーザーを入力した場合、Instance Security Center のローテーションセキュリティバナーの上にエラーメッセージが表示されます。

     注:
     ジョブスケジュールの実行時にアサインされたユーザーを更新する方法の詳細については、「データコレクションジョブの作成またはスケジュール」を参照してください。

2. ビジネスロジックを実行して、[コンプライアンス構成の強化 (Hardening Compliance Configurations)] ページで構成したセキュリティプロパティのコンプライアンスステータスを設定します。詳細については、「日次コンプライアンススコアの確認とセキュリティプロパティの設定」を参照してください。
3. [PA AppSec] 日次データ収集パフォーマンス分析ジョブを実行して、コンプライアンスデータを収集し、日次コンプライアンススコアを更新します。

日次コンプライアンススコアの手動更新

admin ロールが割り当てられている場合は、[リフレッシュ] をクリックして、いつでも日次コンプライアンススコアを更新して再計算することができます。

注:
[リフレッシュ] ボタンは、security_dashboard_user ロールが割り当てられているユーザーには表示されません。

- リフレッシュ機能は、日次データ収集パフォーマンス分析ジョブと同じタスクを実行しますが、バッチ処理ではなくリアルタイムで実行します。
- 通常は、日次コンプライアンススコアを更新して、インスタンスセキュリティアクティビティの影響をすぐに表示する場合に使用します。
- 更新されたスコアが表示されるまでに少し時間がかかる場合があります。

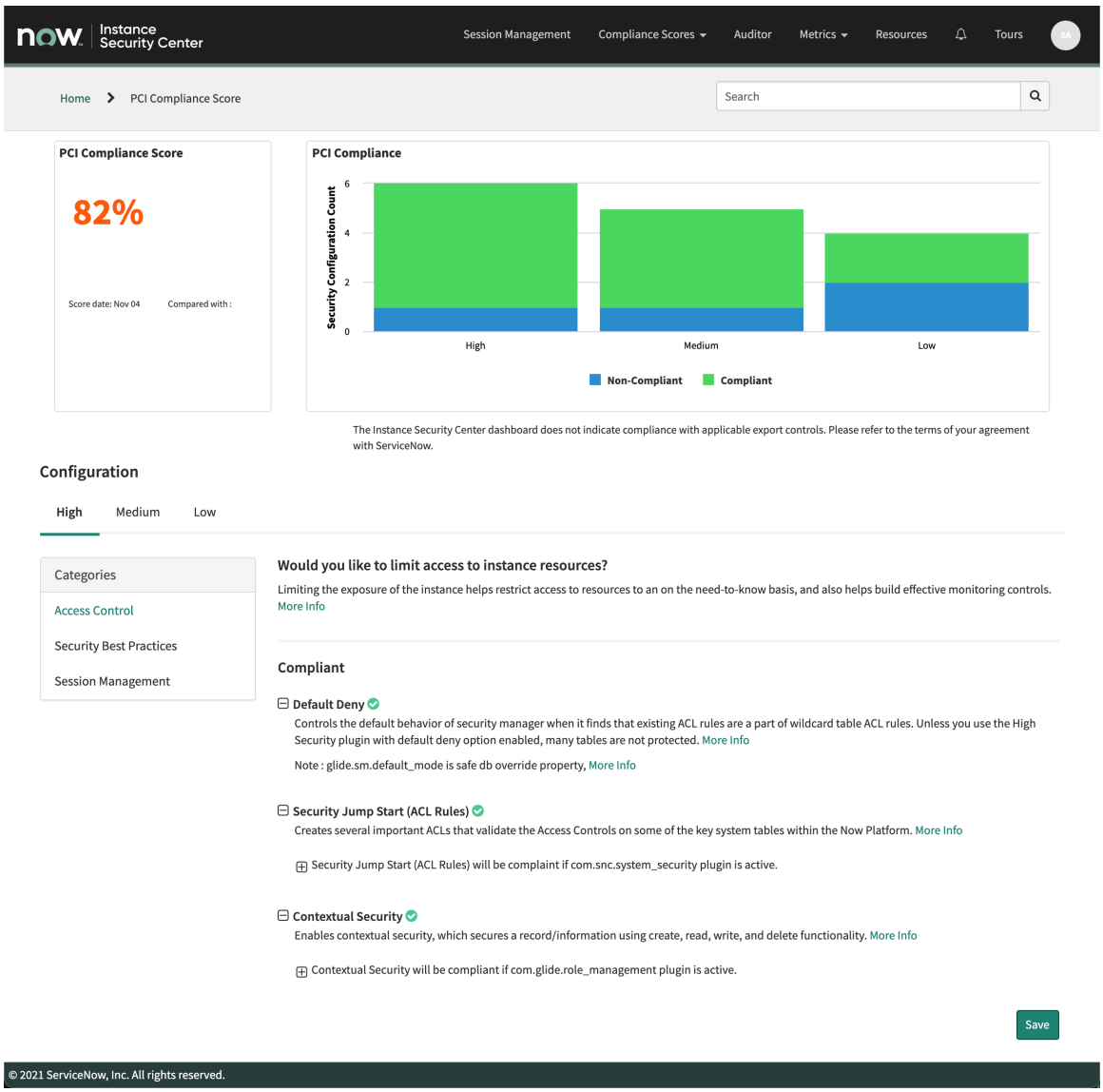
注:
アップグレードを実行すると (London から Washington DC へなど)、Instance Security Center (ISC) プラグインが自動的にアクティブ化されます。提供される修正スクリプトによって、ロールが割り当てられていないカスタムユーザーが自動的に割り当てられます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

PCI コンプライアンススコアダッシュボード

PCI コンプライアンススコアダッシュボードは、インスタンスがペイメントカード業界 (PCI) のセキュリティ標準にどの程度準拠しているかを示します。ダッシュボードを使用してコンプライアンススコアを表示し、構成を変更してセキュリティを向上します。



必要な Now Platform ロール

PCI コンプライアンススコアダッシュボードを表示するには、security_dashboard_user または admin が必要です。

PCI コンプライアンススコアダッシュボードへのアクセス

ダッシュボードを開くには、次の場所に移動します。 システムセキュリティ > インスタンスセキュリティセンター. Instance Security Center から、ヘッダーの [コンプライアンススコア] をクリックし、次に **[PCI** コンプライアンススコア] を選択します。

ユースケース

組織内のさまざまなユーザーがこのダッシュボードをどのように使用するかの例については、次のユースケースを参照してください。

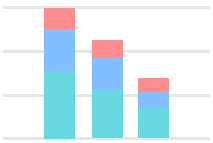
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ユーザー	ダッシュボードの使用法
セキュリティダッシュボードユーザー (security_dashboard_user)	インスタンスセキュリティコンプライアンスを継続的に監視および管理します。
管理者 (admin)	インスタンスセキュリティコンプライアンスを継続的に監視し、セキュリティ脅威を検出して対応します。

インジケーター

インジケーター	説明
PCI コンプライアンススコア	インスタンスのコンプライアンススコアをパーセンテージで表示します。この割合は、コンプライアンス標準を満たすインスタンスのセキュリティ構成の割合を表します。このインジケーターには、コンプライアンススコアが計算された日付と、以前に計算されたスコアとの比較も表示されます。

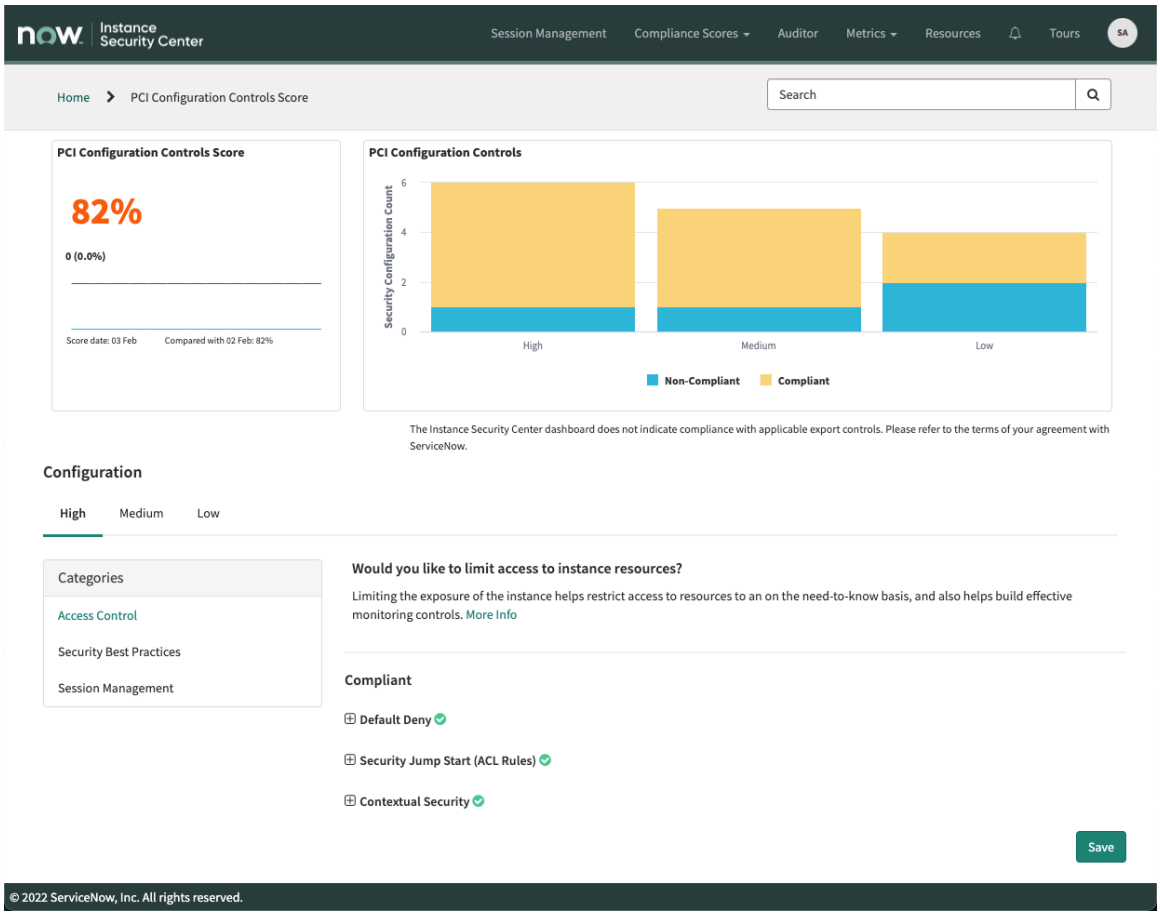
データの表示方法

タイトル	タイプ	ソーステーブル	説明
PCI コンプライアンス	 積み重ね式の棒グラフ	セキュリティ構成 [isc_security_configuration]	高、中、低のカテゴリで準拠と非準拠のセキュリティ構成を表示します。レポートの領域をクリックすると、一致するセキュリティ構成が表示されます。

PCI 構成コントロールスコアのダッシュボード

PCI 構成コントロールスコアのダッシュボードを使用して、PCI 構成を確認し、非準拠のセキュリティチェックを特定します。非準拠のセキュリティチェックの構成は、Instance Security Center から変更できます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



必要な **Now Platform** ロール

PCI コンプライアンススコアダッシュボードを表示するには、security_dashboard_user または admin ロールが必要です。

PCI 構成コントロールスコアのダッシュボードへのアクセス

ダッシュボードを開くには、次の場所に移動します。 システムセキュリティ > インスタンスセキュリティセンター. Instance Security Center から、ヘッダーの [コンプライアンススコア] をクリックし、次に **[PCI** 構成コントロールスコア] を選択します。

ユースケース

組織内のさまざまなユーザーがこのダッシュボードをどのように使用するかの例については、次のユースケースを参照してください。

ユーザー	ダッシュボードの使用法
セキュリティダッシュボードユーザー (security_dashboard_user)	インスタンスの PCI 構成コントロールのコンプライアンスを継続的に監視および管理します。PCI 構成を変更してコンプライアンスを確保し、インスタンスのセキュリティを向上します。
管理者 (admin)	PCI 構成コントロールコンプライアンスを継続的に監視し、潜在的なセキュリティ脅威を検出して対応します。

自動翻訳

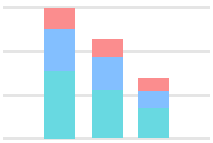
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

インジケーター

PCI 構成コントロールスコア

インスタンスの PCI 構成コントロールスコアをパーセンテージで表示します。このパーセンテージは、コンプライアンス標準を満たすインスタンスのセキュリティ PCI コントロール構成の割合を表します。このインジケーターには、コンプライアンススコアが計算された日付と、以前に計算されたスコアとの比較も表示されます。

データの表示方法

タイトル	タイプ	ソーステーブル	説明
PCI 構成コントロール	 積み重ね式の棒グラフ	セキュリティ構成 [isc_security_configuration]	高、中、低のカテゴリで準拠と非準拠の PCI コントロール構成を表示します。レポートの領域をクリックすると、一致するセキュリティ構成が表示されます。

誤ったセキュリティ定義のスキャン

監査ツールを実行してインスタンスをスキャンし、誤ったセキュリティ定義を見つけます。 インスタンスのセキュリティ体制を改善するために修正できる結果を提供します。

監査ツールは、システム構成を分析するインスタンスの健全性の「総合」アセスメントを実行します。セキュリティスキャンでは、現在のセキュリティ構成がベストプラクティスの定義、およびセキュリティプロパティのコンプライアンス値と比較されます。

インスタンスのセキュリティの観点から、継続して実行すべきことや改善できる可能性がある箇所についてのインサイトと推奨事項を提供します。 これらのインサイトと推奨事項は、次の質問に答えるために役立ちます。

- 適切なセキュリティ関連プロパティが設定されていますか？
- High Security プラグインが有効になっていますか？
- 適切なアクセス制御ルールが存在しますか？

監査ツールの実行とスキャン結果の分析

1. 監査ツールを実行するには、Instance Security Center のホームページで [監査] をクリックします。
2. 完了したら、[スキャン結果] を開いてセキュリティ検出結果を確認および分析します。
3. 特定のスキャン結果の詳細を確認するには、結果番号をダブルクリックします。この情報には、ステータス、スキャンタイプ、実行時間、およびエラーメッセージが含まれています。
4. 監査ツールの各検出結果には、解決策の詳細と、それに対処する方法に関する製品コンテンツの URL が含まれています。文書化されたガイドラインに従って、各検出結果の問題を解決します。

関連情報

- インスタンスセキュリティ強化設定
- 高セキュリティプラグイン
- アクセス制御リストのルール

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

インスタンス測定基準の監視

インスタンスのユーザー、エクスポート、認証、メール、およびウイルス対策の測定基準を監視します。たとえば、インスタンスの信頼できないドメインと信頼できるドメインからのスパム、外部メール、受信メールの測定基準をチェックすることで、メールのセキュリティを監視できます。これらの測定基準を分析して、インスタンスで実行されているアクティビティに関連した例外的なセキュリティ動作を探します。

ユーザー測定基準

ユーザー測定基準を分析して、インスタンスで特定のタイプのユーザーアクティビティに関連した例外動作を探します。

先月/過去 6 か月間/去年のログインなし

先月、過去 6 か月以内、および昨年の暦年に、インスタンスにログインしていないユーザーの数を示します。特定の測定基準のユーザー詳細を表示するには、次の操作を実行します。

- 測定基準をクリックすると、指定された期間中にインスタンスにログインしていないユーザーのリストが表示されます。
- ユーザー名をクリックすると、そのユーザーの詳細が表示されます。

高権限のロールを持つユーザー

次のような高い権限のロールタイプを持つユーザーの数を示します。

ユーザーロール	説明
admin	セキュリティ上の制約に関係なく、システムの機能とデータすべてに対してアクセスを提供するプライマリ管理者ロール
ais_high_security_admin	ユーザーが AI 検索 の高セキュリティ設定にアクセスできるようにするための、昇格された権限ロール。詳細については、以下を参照してください。 へのロールのアサイン AI 検索 管理者とユーザー.
password_reset_admin	パスワードリセットアクティビティのステータスを表示し、潜在的なセキュリティ上の脅威を特定し、パスワードセキュリティポリシーに準拠しているかどうかを監視できるようにする管理者ロール。詳細については、以下を参照してください。 パスワードリセット およびパスワード変更のレポートとログ.
script_include_admin	スクリプトインクルードにもアクセスできる管理者ロール
security_admin	ユーザーがアクセス制御と高セキュリティ設定を作成および変更できるようにするための、昇格された権限ロール。詳細については、「security_admin ロール」を参照してください。
user_admin	ユーザー、ロール、ユーザーグループ、ロール、および部門のアサインも管理できる管理者ロール。

注:
これらの管理ロールタイプの詳細については、「特別管理ロール」を参照してください。

特定のユーザーロール測定基準のユーザー詳細を表示するには、次の操作を実行します。

- ユーザー数ロール測定基準をクリックすると、その高い権限のロールタイプを持つユーザーのリストが表示されます。
- ユーザー名をクリックすると、そのユーザーの詳細が表示されます。その後、これらのセキュリティ上重要なロールが適切な担当者に割り当てられているかどうか判断できます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ユーザーの傾向

次のタイプのユーザーについて、一定期間のカウント傾向情報を表示します。

カウントタイプ	説明
アクティブユーザー	インスタンスでアクティブとしてマークされているユーザーの数
非アクティブなユーザー	インスタンスで非アクティブとしてマークされているユーザーの数
ロックアウト	インスタンスからロックアウトされているユーザーの数

特定のユーザー数のユーザー詳細 (ロックアウトされたユーザーなど) を表示するには、次の操作を実行します。

- [ロックアウトされたユーザー] 測定基準をクリックします。
- [アナリティクスハブ] ページで、[レコードを表示] をクリックします。
- ユーザー名をクリックすると、そのユーザーの詳細が表示されます。その後、このユーザーがロックアウトされた理由があるかどうかを判断して、その状況を解決できます。

イベントの傾向

次のタイプのイベントについて、一定期間のカウント傾向情報を表示します。

イベントタイプ	説明
管理ログイン	特定の日にログインした、権限の高い管理者ユーザーロールを持つユーザーの数
外部ログイン	暦日の間にこのインスタンスにログインした、snc_external ロールを持つユーザーの数通常、これらのログインは、メンテナンス、サポート、コンサルティング、または監査の目的で発生します。この測定基準を監視することで、外部ログイン試行が正規のものであり、潜在的なセキュリティ上の問題ではないことを確認できます。
失敗したログイン	特定の日に失敗したログイン試行回数
代理操作	特定の日に他のユーザーの代理操作でログインしているユーザーの数
セキュリティ昇格	暦日の間に、セキュリティ管理者が標準ユーザーに対して、割り当てられたユーザーロールを高い権限のセキュリティロールに変更することによって、セキュリティ権限を強化した回数。このような高権限のセキュリティ ロールには、oauth_admin、admin、security_admin、および impersonator が含まれます。
SNC ログイン	特定の日にハイホッピング技術を使用してこのインスタンスにログインしたカスタマーサービス & サポートの数

特定のイベント数のユーザー詳細 (代理操作など) を表示するには、次の操作を実行します。

- ユーザー数の測定基準をクリックします。[セキュリティダッシュボードイベントログ] ページには、そのタイプのイベントのイベントログが一覧表示されます。
- ユーザー名をクリックすると、そのイベントの詳細が表示されます。

関連情報

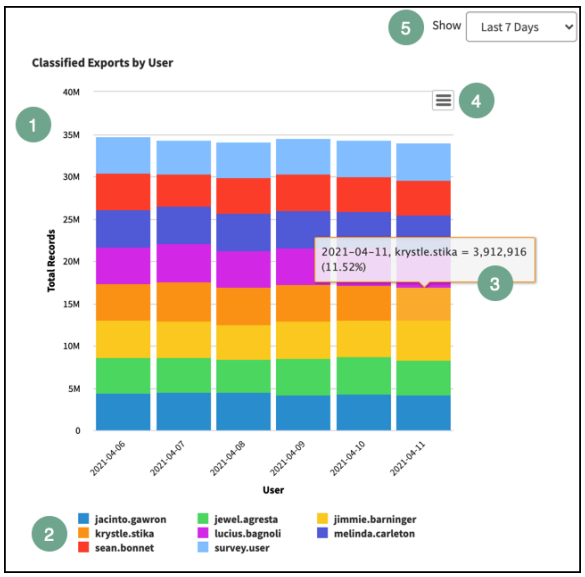
分析ハブ

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

エクスポート測定基準

エクスポート測定基準を分析して、最もよくエクスポートされるデータと、最も多くのデータをエクスポートするユーザーを確認します。



1. エクスポートチャート

   各レポートでは、色分けされたキーを使用して、エクスポートを実行したユーザーを示すエクスポートイベントの数が表示されます。列のカラー部分をクリックすると、そのエントリに一致するエクスポートイベント [isc_export_event] レコードリストが表示されます。

2. レポートキー

   レポートの下部にあるキーは、どの色でどのユーザーやテーブルを特定しているのかを示します。

3. プレビューポップアップ

   チャート内のエントリをポイントすると、ポップアッププレビューが表示されます。このプレビューには、ユーザーまたはテーブルの名前、エクスポートの数、およびその列の合計に対する割合が表示されます。

4. 画像のエクスポート

   レポートを画像として保存するには、アイコンをクリックします。レポートは PNG または JPEG 形式で保存できます。

5. レポート日付範囲

   [表示] リストを使用して、過去 24 時間または過去 7 日以内のエクスポートを表示します。

エクスポート測定基準レポート

エクスポート測定基準のページには 4 つのレポートが表示されます。

ユーザー別のエクスポート

[ユーザー別のエクスポート] レポートを使用すると、最も多くのデータをエクスポートしているユーザーを確認できます。

ユーザー別に分類されたエクスポート

[ユーザー別に分類されたエクスポート] レポートを使用すると、機密情報、制限付き情報、個人情報などの分類に一致するデータを最も多くエクスポートしているユーザーを確認できます。管理者は、このレポートで使用する分類を [設定] タブで定義できます。

テーブル別のエクスポート

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

[テーブル別のエクスポート] レポートを使用すると、最も頻繁にエクスポート元になるテーブルを確認できます。

テーブル別に分類されたエクスポート

[テーブル別に分類されたエクスポート] レポートを使用すると、機密情報、制限付き情報、個人情報などの分類に一致し、最も頻繁にエクスポート元になるテーブルを確認できます。管理者は、このレポートで使用する分類を [設定] タブで定義できます。

注:
測定基準レポートをエクスポートすると、エクスポートイベントのみが追跡されます。REST API やワークフローなどの他のソースからのエクスポートは、この機能の一部として追跡されることはありません。

エクスポート測定基準の設定

[設定] タブの設定オプションを使用して、レポート結果を絞り込みます。

[設定] タブをクリックして、エクスポート測定基準の設定にアクセスします。

設定構成フィールド

エクスポート測定基準の構成

設定	説明
測定基準の分類	このフィールドで分類の追加または削除を行い、[ユーザー別に分類されたエクスポート] および [テーブル別に分類されたエクスポート] レポートに組み込むエクスポートを決定します。これらのレポートは、次の分類をサポートしています。 • 個人識別可能情報 • 機密 • 制限付き • 内部 • 公開 データ分類の詳細については、「データ分類」を参照してください。
アラートの分類	このフィールドで分類の追加または削除を行い、インスタンスセキュリティ通知をトリガーするエクスポートを決定します。[測定基準の分類] フィールドでサポートされている分類がここでサポートされます。これらのアラートの詳細については、[Instance Security Center] ページのセキュリティ通知に関するセクションを参照してください。[レコードのしきい値] フィールドは、インスタンスがトリガーされてアラートが発生する前にエクスポートされるレコードの数を定義します。
レコードのしきい値	アラートをトリガーするためにエクスポートする必要があるレコードの数。アラートをトリガーするには、これらのレコードが [アラートの

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

エクスポート測定基準の構成 (続く)

設定	説明
	分類] フィールドにリストされている分類とも一致する必要があります。

[保存 (⌘ + s)] ボタンを使用して設定を保存します。

認証測定基準

認証測定基準を分析して、使用頻度の低い IP アドレス、失敗したログイン、ユーザーが使用している認証スキームのタイプなど、認証に関連する情報を表示します。

[認証測定基準] ページを使用して、認証構成に関連するレポートを表示します。このタブには次のレポートが表示されます。

注:
[認証測定基準] ページには、**REST API Access Policy** プラグイン (com.glide.rest.policy) が必要です。この機能の詳細については、「REST API アクセスポリシー」を参照してください。

認証ポリシーのない API

アクセスポリシーのないすべての API のリアルタイム数を表示します。

強化：アカウント復旧フロー

強化：ロールベースの MFA 機能関連の設定

Web サービスアクセスのみのアカウント

User [sys_user] テーブルで Web サービスアクセスオプションが有効になっているすべてのユーザーレコードの数を表示します。

30 日後に期限が切れる X509 証明書

X.509 Certificates [sys_certificate] テーブルで、30 日以内に期限が切れる X.509 証明書の総数を表示します。

適応認証測定基準

適応認証測定基準を分析して、インスタンスでの適応認証の使用状況を監視し、インサイトを追加します。

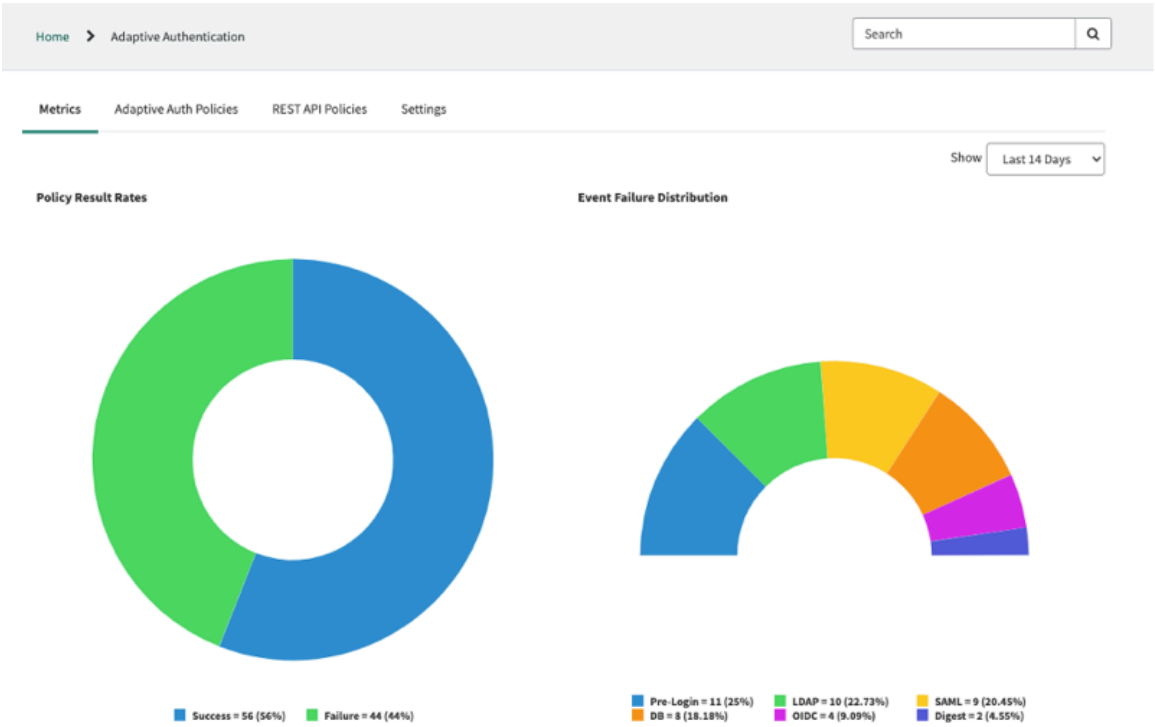
適応認証測定基準ページを使用して、1 つの場所で適応認証に関連付けられたレポート、設定、およびポリシーを表示します。セキュリティ管理者は、レポートを使用して適応認証ポリシーの結果を監視できます。このデータを使用して、インサイトを得てポリシーを調整し、パフォーマンスを向上します。

注:
適応認証測定基準ページでは、**Adaptive Authentication** (com.snc.adaptive_authentication) プラグインが必要です。この機能の詳細については、「適応認証」を参照してください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

測定基準



[測定基準] タブを使用して、適応認証構成に関連するレポートを表示します。このタブには次のレポートが表示されます。

- ポリシー結果評価
- イベント失敗の分布
- イベント成功の分布
- 拒否された IP アドレス
- 認証ユーザーログイン
- API ユーザーログイン
- 認証傾向

[表示] リストを使用して、表示するレポートの期間を選択します。

適応認証ポリシー

[適応認証ポリシー **(Adaptive Auth Policies)**] タブを使用して、インスタンスの適応認証ポリシーとポリシーコンテキストを表示します。これらのリストのエントリをクリックすると、関連するレコードが表示されます。これらのレコードの詳細については、「適応認証」を参照してください。

設定

[設定] タブを使用して、適応認証システムのプロパティを表示および設定します。これらのプロパティの詳細については、「適応認証プロパティの設定」を参照してください。

メール測定基準

メール測定基準を分析して、インスタンスに配信される受信メールに関連した例外動作を探します。たとえば、測定基準が特定のドメインからのスパムメールのスパイクを示している場合は、インスタンスへの配信を防ぐ受信アクションを定義できます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

各メール測定基準について、暦日の間に配信または送信されたメールのタイプごとにカウント数が表示されます。

通知設定	説明
外部の受信メール	該当の暦日に外部メールドメインからインスタンスに配信された受信メールの数 注: 外部メールドメインとは、*security.list.internal.domains* システムプロパティにリストされていないドメインです。このプロパティは内部のメールドメインのみを追跡するからです。このプロパティの詳細については、「利用可能なシステムプロパティ」を参照してください。
スパム	該当の暦日にインスタンスに配信され、スパムとしてマークされた受信メールの数件数が過去の傾向と一致しない場合、インスタンスのセキュリティを侵害しようとする試みが行われたことを示している可能性があります。
信頼できる受信メール	該当の暦日に信頼できると指定されたメールドメインからインスタンスに配信された受信メールの数
信頼できない受信メール	該当の暦日に信頼できないと指定されたメールドメインからインスタンスに配信された受信メールの数。 [信頼できない/信頼できるドメイン] フォームで信頼できないメールドメインまたは信頼できるメールドメインを指定して、それらのドメインから送信された受信メールを追跡できるようにすることができます。信頼できないメールドメインまたは信頼できるメールドメインを指定する方法については、「信頼できないメールドメインと信頼できるメールドメインの指定」を参照してください。

メール測定基準をクリックした後、次のいずれかをクリックすることで、インスタンスで発生する可能性があるメール セキュリティの問題を調べることができます。

コマンド	説明
チャート	選択したメールタイプ (スパム、外部受信、信頼できない、または信頼できる) の受信メール数と数の傾向
レコード	選択したメールタイプの日次カウントを侵害する個々のメールレコード
詳細情報	選択したメールタイプの追加情報

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注:
メール測定基準は、インスタンスに配信される受信メールにのみ適用されます。測定基準は、全社的なメールサーバーを介して処理される通常のトラフィックには適用されません。受信アクションの定義と受信メールの処理への影響については、「受信メールアクション」を参照してください。

信頼できないメールドメインと信頼できるメールドメインの指定

特定のメールドメインを、信頼できないドメインまたは信頼できるドメインに指定して、インスタンス内のこれらのソースからの受信メールの測定基準を監視できるようにします。

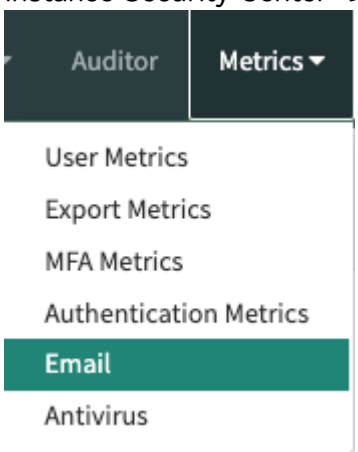
始める前に
必要なロール：security_dashboard_user または管理者

このタスクについて
信頼できないドメインまたは信頼できるドメインがインスタンスにメールを送信すると、その日次カウントが [メール] ページの [信頼できない受信メール] または [信頼できる受信メール] 測定基準に表示されます。これらのドメインからのメールアクティビティを追跡し、メールログを使用して特定の受信メールを表示できます。また、信頼できないドメインまたは信頼できるドメインからアクティビティが発生するたびに通知するユーザー (通常はマネージャーまたはセキュリティアナリスト) を指定することもできます。

注:
メールドメインを信頼できないと指定する場合、これはセキュリティトラッキングのみを目的としています。管理者は、信頼できないドメインからのメールを無視するようにシステムアドレスフィルターを設定することもできます。メールをフィルタリングして配信をブロックする方法については、「システムアドレスフィルター」を参照してください。

手順

1. 移動先 すべて > システムセキュリティ > インスタンスセキュリティセンター.
2. Instance Security Center のホームページで、[測定基準] メニューから [メール] を選択します。



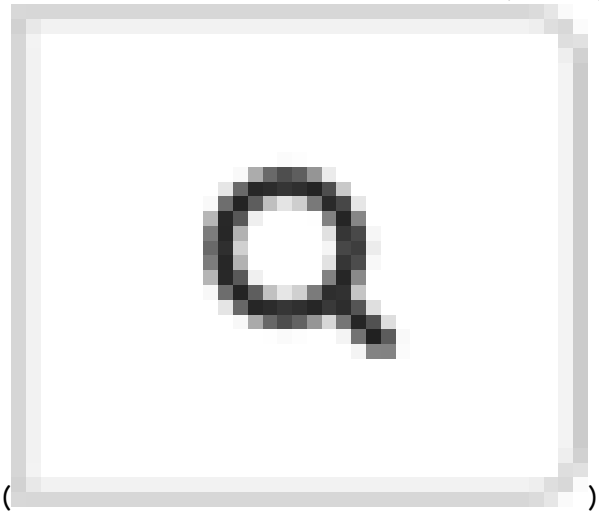
3. [メール] ページの [信頼できない/信頼できるドメイン] セクションで、[新規] をクリックします。
4. フォームのフィールドに入力します。

[信頼できない/信頼できるドメイン] フォーム

フィールド	説明
ドメイン	信頼できないまたは信頼できるという指定を行うメールドメイン名。たとえば、ServiceNow の従業員がインスタンスに信頼できるメールを送信できるようにするには、「servicenow.com」と入力します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

フィールド	説明
カテゴリ	メールドメインが信頼できないか信頼できるかを示すカテゴリ： 信頼できない メールドメインを信頼できないものとして指定します。これを使用して、インスタンスに不審なメールや潜在的なセキュリティ上の脅威をもたらすメールを送信するドメインを特定します。 信頼できる メールドメインを信頼できるものとして指定します。ドメインからの受信メールにセキュリティ上の脅威がないことが測定基準で示されている場合に、これを使用してそのドメインを識別します。信頼できるドメインに指定すると、受信メールアクティビティを経時的に追跡できます。
アクティブ	指定されたメールドメインに対して、信頼できない/信頼できるステータスを有効または無効にするためのチェックボックス
Notify	信頼できないドメインまたは信頼できるドメインでアクティビティが発生したときにメールで通知するユーザーの名前。スポットライト検索アイコン  ( ) をクリックして、ユーザーの名前を検索します。通知を送信しない場合、[通知 **(Notify)]** フィールドは空白のままにします。

5. [保存] を選択します。

タスクの結果

信頼できない/信頼できるメールドメインの情報は、[メール] ページの [信頼できない/信頼できるドメイン] リストにも追加されます。

関連情報

Instance Security Center

メール測定基準

ウイルス対策測定基準

アンチウイルススキャン プラグインが有効になっている場合は、インスタンスでアンチウイルススキャンが実行され、添付ファイルからのウイルス感染からインスタンスを保護します。

次の測定基準はアクティビティの最後 60 日間表示され、アンチウイルススキャン機能の有効性を評価できます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

ウイルス対策イベント

ウイルス対策イベントは、インスタンス内のウイルス対策イベントの数を日付別に示します。ウイルス対策イベントにアクセスするには、次の場所に移動します。 システムセキュリティ > インスタンスセキュリティセンター をクリックし、[メトリック] タブを選択します。色分けされたグラフの線は、次のタイプのウイルス対策イベントを表しています。

色	説明
青	指定された日付にこのインスタンスでアンチウイルススキャンによって隔離されたファイルの数
緑	インスタンスにダウンロードされ、指定された期間隔離された感染ファイルの数。これらのファイルは主に、ウイルスまたは不正なコードを含むメールの添付ファイルです。
黄	指定された日付にこのインスタンスで削除された隔離ファイルの数
オレンジ	指定された日付にこのインスタンスで復元された隔離ファイルの数 **注:** アンチウイルススキャンが実行されて誤検出が見つかった場合、隔離ファイルを復元してインスタンスでアクセスできるようにすることができます。

- [アナリティクスハブ] ページにアクセスして、特定の日付の詳細なスコアカードと分析情報を表示するには、[ウイルス対策イベント] グラフで色付きの線をクリックします。たとえば、青色のグラフィックラインをクリックすると、特定の日付に隔離されたファイルの分析情報が表示されます。
- [アナリティクスハブ] ページで次のブレークダウンを表示するには、をクリックし、次の項目をクリックします。

ブレークダウン	説明
AppSec - ウイルス対策イベントソース	ウイルス対策イベントのソース ○ アップロード時：感染したファイル (通常は添付ファイル) のアップロードが原因で発生しました。 ○ 隔離から：感染したファイル (通常は添付ファイル) の隔離によって発生しました。 ○ ダウンロード時：感染したファイル (通常は添付ファイル) のダウンロードが原因で発生しました。 ○ レコードから： テーブル内の感染したレコードが原因で発生しました。
AppSec - ウイルス対策イベントタイプ	ウイルス対策イベントのタイプ ○ 隔離：ファイル (通常は添付ファイル) の隔離が原因で発生しました。 ○ ダウンロード済み：ファイル (通常は添付ファイル) のダウンロードが原因で発生しました。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ブレークダウン	説明
	○ 復元済み：隔離されたファイルの復元が原因で発生しました。 ○ 削除済み：隔離されたファイルの削除が原因で発生しました。
AppSec - ウイルス対策アップローダー	アンチウイルススキャン アプリケーションによって検出されたウイルスの感染源のファイルをアップロードしたログインユーザーの名前。

隔離されたファイル

アンチウイルススキャンによって隔離されたインスタンス内の感染ファイルのリスト：

フィールド	説明
ファイル名	感染ファイルの名前
コンテンツタイプ	ファイル内の感染したコンテンツのタイプ。たとえば、**application/x-dosexec** は感染したアプリケーションまたは DOS の実行可能ファイルですが、**text/plain** は感染した .txt ファイルです。
テーブル	感染ファイルを含むテーブルの名前。たとえば、インシデントファイルレコードの場合は [インシデント] が表示されます。
ウィルス	アンチウイルススキャンによって隔離されたファイルの名前
検出	感染ファイルが検出された日時
作成者	感染ファイルを隔離したユーザーの名前
作成日時	隔離ファイルレコードが作成された日時
テーブル Sys ID	隔離ファイルレコードに割り当てられたテーブルシステム識別子

注:
[隔離されたファイル] タイルと [ウイルスタイプ] タイルを [イベント] リボンに追加することもできます。詳細については、「セキュリティイベントの監視」と「セキュリティイベントリボンの構成」を参照してください。

関連情報

- アンチウイルススキャン
- アンチウイルススキャン の構成
- 隔離されたファイルの確認
- ウイルス対策アクティビティの確認
- 分析ハブ
- Performance Analytics のブレークダウン
- Analytics, Intelligence, and Reporting

MFA 測定基準ダッシュボード

MFA 測定基準ダッシュボードには、インスタンスのマルチファクター認証構成に関する情報が表示されます。ダッシュボードを使用して、MFA 構成がセキュリティ標準を満たしていることを確認します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

必要な Now Platform ロール

PCI コンプライアンススコアダッシュボードを表示するには、security_dashboard_user または admin が必要です。

MFA 測定基準ダッシュボードへのアクセス

ダッシュボードを開くには、次の場所に移動します。 システムセキュリティ > インスタンスセキュリティセンター. Instance Security Center からヘッダーの [測定基準] をクリックし、**[MFA** 測定基準] を選択します。

ユースケース

組織内のさまざまなユーザーがこのダッシュボードをどのように使用するかの例については、次のユースケースを参照してください。

ユーザー	ダッシュボードの使用法
セキュリティダッシュボードユーザー (security_dashboard_user)	インスタンスセキュリティコンプライアンスを継続的に監視および管理します。
管理者 (admin)	インスタンスセキュリティコンプライアンスを継続的に監視し、セキュリティ脅威を検出して対応します。

インジケーター

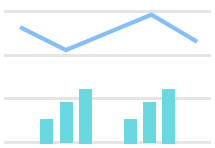
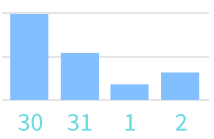
MFA に登録されているユーザー

MFA に登録されているインスタンスのユーザーの合計数を表示します。クリックして分析ハブを開き、詳細を表示します。

MFA バイパスを使用しているユーザー

MFA バイパスを使用しているユーザーの合計数を表示します。クリックして分析ハブを開き、詳細を表示します。

データの可視化

タイトル	タイプ	ソーステーブル	説明
高権限 MFA ユーザー	 棒		
MFA ユーザーの傾向	 傾向図		

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ISC 仮想エージェントインターフェイスのアクティブ化

admin ロールを持っている場合は、ISC 仮想エージェント会話プラグイン (com.glide.isc_virtualagent) をアクティブ化できます。このプラグインをアクティブ化すると、仮想エージェントおよび 自然言語理解 (NLU) (NLU) コンテンツパックがインストールされ、Instance Security Center から仮想エージェントにアクセスできるようになります。

始める前に

Instance Security Center の仮想エージェントインターフェイスを利用できるのは、有料の仮想エージェントサブスクリプションに登録し、Glide 仮想エージェント (com.glide.cs.chatbot) プラグインをアクティブ化しているユーザーに限られます。詳細については、「仮想エージェントの有効化」を参照してください。

必要なロール：admin。

このタスクについて

ISC 仮想エージェントインターフェイスを使用すると、次のタスクを実行できます。

- セキュリティ関連の質問をして、簡単な要約回答と詳細への参照リンクを取得する
- Instance Security Center、プラットフォームセキュリティ、ServiceNow セキュリティポリシー、信頼、ガバナンス、リスク、およびその他のプロセスに関連する回答を取得する
- Now Support Security ポータルでナレッジベースのトピックなどのセキュリティ関連リソースを検索する

ISC 仮想エージェントのプラグイン

プラグイン	説明
ISC 仮想エージェント会話 [com.glide.isc_virtualagent]	Instance Security Center 用の ISC 仮想エージェント会話コンテンツパックをアクティブ化します。
仮想エージェント会話用の ISC NLU モデル [com.glide.isc_nlu]	Instance Security Center の 自然言語理解 (NLU) (NLU) コンテンツパックを有効にします。

注:
com.glide.isc_virtualagent プラグインを有効にすると、 com.glide.isc_nlu が自動的にアクティブ化されます。ただし、初めて com.glide.isc_nlu プラグインをアクティブ化する場合は、 com.glide.isc_virtualagent も手動でアクティブ化する必要があります。

手順

1. 移動先 すべて > システムアプリケーション > 利用可能なすべてのアプリケーション > すべて.
2. フィルター基準と検索バーを使用してプラグインを検索します。

   名前または ID でプラグインを検索できます。プラグインが見つからない場合は、ServiceNow 担当者から要求する必要があります。

自動翻訳

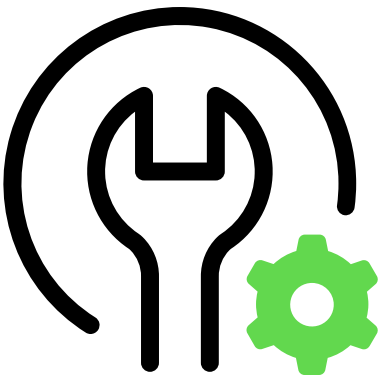
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

3. [インストール] を選択して、[プラグインをアクティブにする] ダイアログボックスで、[アクティブ化] をクリックします。

> **注:**
> ドメイン分離と代理管理者がインスタンスで有効になっている場合、管理ユーザーはグローバルドメインに含まれている必要があります。それ以外の場合、次のエラーが表示されます： 別の操作が実行されているため、アプリケーションのインストールは利用できません：<プラグイン名> のプラグインの有効化。

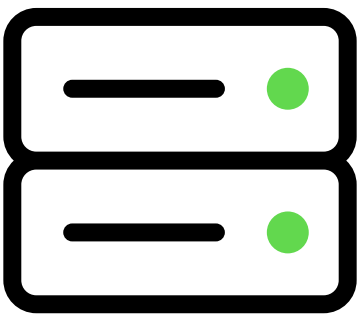
その他の設定とセキュリティリソース

このセクションでは、Instance Security Center の外部で設定するセキュリティプロパティについて説明します。また、その他のセキュリティ関連のリソースについても説明します。



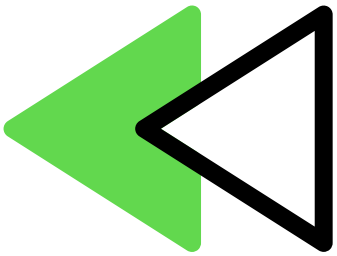
セキュリティシステムプロパティ

セキュリティ設定には、インスタンスのセキュリティレベルを制御するプロパティがいくつかあります。



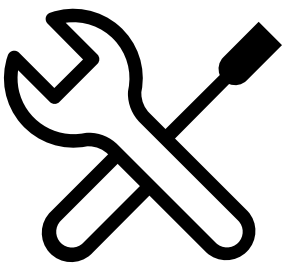
MID Server 展開ガイド

ServiceNow Management, Integration, and Discovery (MID) サーバーは、仮想マシンを含む標準ハードウェア上で Windows サービスまたは UNIX デーモンとして動作する軽量の Java アプリケーションです。

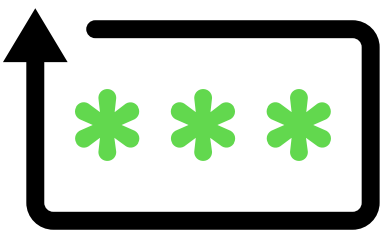


元に戻せる動作

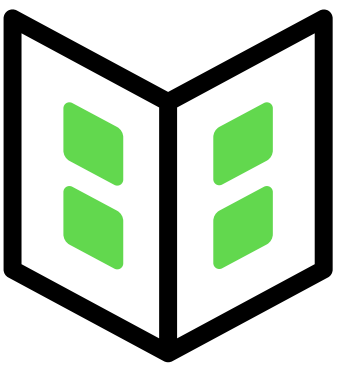
「safe_overrides」または「no_db_override」のいずれかに分類されるシステムプロパティがあります。



減価償却済みセキュリティプロパティ



Javascript コンテンツアクセス制御の使用



その他のセキュリティ強化リソース

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

これらのセキュリティプロパティは、以前のリリースで廃止されました。	JavaScript コンテンツアクセス制御を使用して、インスタンス内でブロックされたサードパーティの JavaScript URL のリストを変更できます。	Now Platform に関連する、セキュリティコントロールの強化に関するその他の情報源。

ログ記録、監査、およびエラー (インスタンスセキュリティ強化)

ログ記録と監査戦略を適用して、不審なアクティビティを適切なタイミングで特定して対処できるようにします。

インスタンスのログ記録の詳細については、「システムログ」を参照してください。を使用して、ログインや失敗したログインなどのシステムイベントを監視するスケジュールがあることを確認するシステムログ > イベント.

SQL エラーメッセージの無効化 (インスタンスセキュリティ強化)

glide.db.loguser プロパティを使用して、SQL エラーメッセージがブラウザーでレンダリングされないようにします。

詳細情報

属性	説明
プロパティ名	glide.db.loguser
構成タイプ	システムプロパティ (/sys_properties_list.do)
Instance Security Center で構成可能	いいえ
目的	ブラウザー内での SQL エラーメッセージの表示を無効にすること
タイプ	true | false
推奨値	false
機能への影響度	(低) この修正により、SQL エラーメッセージをレンダリングできなくなります。機能への影響はありません。
セキュリティリスク	(中) 攻撃者に役立つ可能性のある機密の SQL 情報は、Web ページのエラーメッセージに含まれて表示されることはありません。

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

その他のセキュリティ強化リソース

Now Platform に関連するセキュリティコントロールの強化に関しては、他にも次のような情報源があります。

リソース	説明
セキュリティテストポータル	HI のセキュリティサービスポートフォリオ
KB0538598	顧客アプリケーションのペネトレーションテスト | ポリシーおよび手順

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

リソース	説明
KB0546756	公開コンテンツ管理システム (CMS) アクセスの無効化
KB0550071	ServiceNow, Inc. インスタンスアクセス制御のレビュー
KB0550613	IP アドレス制限の識別と有効化
KB0550828	GlideAjax トランザクションの監査とレビュー
KB0550837	スクリプトサンドボックスの修復
KB0551031	パスワードリセット UI のセキュリティ修正
KB0552835	デモユーザーアカウントの修正
KB0529232	ServiceNow, Inc. Monitoring - 概要とインサイト
KB0564232	外部認証による ServiceNow, Inc. モバイルアプリの使用
セキュリティとリスク	ServiceNow, Inc. コミュニティ

インスタンスセキュリティ強化設定

インスタンスセキュリティの強化設定コンテンツには、Now Platform のセキュリティ関連のシステムプロパティとプラグインの詳細な説明とコンプライアンス値が含まれています。Instance Security Center の [ハードニングコンプライアンス構成] ページで、これらのプロパティの大半を設定できます。

概要と目的

Instance Security Center は、パーセンテージで表される日次コンプライアンススコアを計算します。これは、現在のインスタンスセキュリティ設定が [インスタンスセキュリティ強化設定] のコンプライアンス値にどの程度準拠しているかに基づいています。

[ハードニングコンプライアンス構成] ページを使用すると、インスタンスのスコアに影響を与える可能性のある特定のセキュリティ構成設定を管理できます。インスタンスが強化要件を満たしていることを確認する方法の詳細については、以下を参照してください。

- Instance Security Center
- インスタンスのセキュリティ設定調整によるコンプライアンスの強化

一部のコンプライアンス値がインスタンスに適していない場合でも、セキュリティ関連のプロパティを設定または更新するときは、必ずインスタンスセキュリティ強化設定を参照してください。 これらのプロパティを更新するときは、インスタンスが引き続き期待どおりに動作することを確認してください。セキュリティへの影響を判断するには、専門知識を持つ適切な内部担当者に相談してください。

その他のリソース

ユーザーの参照用に、Now Platform には製品ドキュメントの広範な構成機能情報が含まれています。インスタンスの保護 にあるリンクを使用すると、セキュリティコンテンツの大半にアクセスできます。また、以下も参照してください。

- 利用可能なシステムプロパティ
- セキュリティ設定プロパティ
- 高セキュリティ設定

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

インスタンスセキュリティ強化テーブル

セキュリティ構成テーブル

セキュリティ構成 [isc_security_configurations] テーブルのレコードには、セキュリティ構成の詳細が含まれています。レコードには、構成の説明、そのコンプライアンスステータス、その他の重要な詳細が格納されています。

セキュリティ構成レコードを使用すると、構成を準拠させるために設定する必要があるすべてのプロパティと依存関係を 1 か所で確認できます。

セキュリティ構成レコード内では、この構成に関連付けられた関連セキュリティ依存関係および依存関係グループレコードが表示されます。

セキュリティ依存関係テーブル

セキュリティ依存関係 [isc_security_dependencies] テーブルのレコードは、受信基準と送信基準、および推奨タイプを定義します。このタイプは、Instance Security Center での依存関係の表示方法を定義します。

依存関係グループテーブル

依存関係グループ [isc_dependency_groups] テーブルのレコードを使用して、複数の依存関係をグループ化します。グループが準拠していると見なされるには、グループ内のすべての依存関係が準拠している必要があります。

アクセス制御 (インスタンスセキュリティ強化)

アクセス制御は、特定のリソースへのアクセスを許可するか拒否するかを決定します。リソースの使用が許可されているユーザーのみに、そのリソースへのアクセスが許可されます。

「承認」と「認証」の用語とその定義はよく混同されますが、この 2 つは等価な動作ではありません。

- 認証は、ID の提供および検証です。
- 承認には、ユーザー (またはプリンシパル) がアクセスできる機能とデータを決定する実行ルールが含まれており、認証が成功した後にアクセス権が確実かつ適切に割り当てられるようにします。

承認は、認証が成功した後に行われるプロセスです。明確に定義されたロールと権限のセットに関連付けられた有効な資格情報をユーザーが保持していることを判断した後に、リソースを承認できるかどうかを指定するセキュリティプロパティを設定できます。

Now Platform 内の機密エンティティへの不正アクセスを制限するために管理者が設定できるセキュリティコントロールは次のとおりです。

- アクセス制御リストのルール
- ACL ルールの構成
- ServiceNow アクセス制御

GlideSystemUserSession スクリプト可能 **API** へのアクセス

クライアントコール可能な GlideSystemUserSessionSandbox スクリプト可能 API は、GlideSystemUserSession の addErrorMessageNoSainitization メソッドと addInfoMessageNoSainitization メソッドを javascript サンドボックスに公開しています。これにより、すべてのユーザーがスクリプトを介してこのメソッドをコールできます。

true に設定すると、サンドボックス化されたユーザーセッションで、サニタイズなしで情報メッセージやエラーメッセージをコールすることができます。メッセージが呼び出されると、警告がログに記録されます。 **false** に設定すると、コールは許可されません。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

詳細情報

属性	説明
プロパティ名	*glide.sandbox.usersession.allow_unsanitized_messages*
構成タイプ	システムプロパティ (/sys_properties_list.do)
Instance Security Center で構成可能	あり
目的	このプロパティにより、サンドボックス化されたユーザーセッションでの、サニタイズされていない情報メッセージまたはエラーメッセージのコールが制限されます。
タイプ	true | false boolean
推奨値	false
セキュリティ依存関係	このプロパティの値は安全な上書きであり、いったん変更したら変えることはできません。
機能への影響度	(高) プロパティの値を false に設定すると、これらの関数が呼び出された場合にメッセージが作成されず、ログも記録されません。
セキュリティリスク	(高) 適切にサニタイズされないと、危険性のあるコンテンツにアクセスする可能性があり、サニタイズされていないエラー関数がスクリプトで使用可能になります。
参照	アクセス制御 安全な上書き

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

スクリプト実行の許可

glide.script_processor.authorized_script_module_role プロパティを使用して、*sys_app_module* テーブルからの実行中のスクリプトの使用を、プロパティ内で定義されたロールに制限します。

このプロパティでは、プロパティ内で指定されたロールを持っていない限り、sys_app_module からスクリプトを実行するすべてのシステムユーザーを制限します。glide.script_processor.authorized_script_module_role プロパティを使用して、スクリプトを実行できるロールを指定します。

詳細情報

属性	説明
プロパティ名	*glide.script_processor.authorized_script_module_role*
構成タイプ	システムプロパティ (/sys_properties_list.do)
Instance Security Center での構成	あり
目的	*sys_app_module*からのスクリプト実行のために指定されたロールを要求するため。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

属性	説明
推奨値	ロールのカンマ区切りリストを含む TextBox
機能への影響度	(中) この修正では、定義されたロールによる承認の形式で認証が適用されます。 • インスタンスでスクリプト要求を処理する際に、この認証を実行します。 • 現在このデータにアクセスしているゲストユーザーを制限します。必要であれば、このコンテンツへのアクセスを必要とするユーザーのために、必要なアクセス制御権限を持つ新しいアカウントを作成する場合があります。
セキュリティリスク	(高) スクリプト要求で適切な承認が構成されていない場合、無許可のユーザーがインスタンスの機密コンテンツ/データにアクセスする可能性があります。
参照	アクセス制御

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

基本認証：**JSONv2** 要求 (インスタンスセキュリティ強化)

glide.basicauth.required.jsonv2 プロパティを使用して、受信 JSONv2 要求で基本承認を要求するかどうかを指定します。

詳細情報

属性	説明
プロパティ名	glide.basicauth.required.jsonv2
構成タイプ	システムプロパティ (/sys_properties_list.do)
Instance Security Center での構成	あり
目的	JSONv2 要求承認の適用
推奨値	true
機能への影響度	(中) この修正では、基本認証とシステムレベルのアクセス制御の形で、認証方法の組み合わせが適用されます。 • インスタンス上で JSON データの形式でテーブル/ページからデータを取得する際に、この認証を実行します。 • 現在このデータにアクセスしているゲストユーザーを制限します。 • このコンテンツへのアクセスを必要とするユーザーのために、必要なアクセス制御権限を持つアカウントを作成します。 詳細については、「JSONv2 Web サービス JSONv2 Web サービス」を参照してください。
セキュリティリスク	(高) データソースの JSON 要求で適切な承認が構成されていない場合、無許可のユーザーがターゲットインスタン

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

属性	説明
	スの機密コンテンツ/データにアクセスする可能性があります。
参照	認証 着信 JSONv2 要求に対する基本認証の要求

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

基本認証：**SOAP** 要求 (インスタンスセキュリティ強化)

glide.basicauth.required.soap プロパティを使用して、受信 SOAP 要求で基本承認を要求するかどうかを指定します。

詳細情報

属性	説明
プロパティ名	glide.basicauth.required.soap
構成タイプ	システムプロパティ (/sys_properties_list.do)
Instance Security Center での構成	あり
目的	SOAP 要求承認の適用
推奨値	true
機能への影響度	(中) この修正では、基本認証とシステムレベルのアクセス制御の形で、認証方法の組み合わせが適用されます。 • インスタンス上で SOAP データの形式でテーブル/ページからデータを取得する際に、この認証を実行します。 • 現在このデータにアクセスしているゲストユーザーを制限します。 • このコンテンツへのアクセスを必要とするユーザーのために、必要なアクセス制御権限を持つアカウントを作成します。 詳細については、「SOAP Web サービス」および「MID Server 認証資格情報と SOAP 要求」を参照してください。
セキュリティリスク	(中) データソースの SOAP 要求で適切な承認が構成されていない場合、無許可のユーザーがターゲットインスタンスの機密コンテンツ/データにアクセスする可能性があります。
参照	認証

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

委任開発者に対するアクセスのブロック

この設定は、スクリプトを使用してユーザーロールを更新する委任開発者のアクセスに影響します。設定が準拠している場合、開発者は user_admin ロールなしでテーブル *sys_user_has_role* のレコードを更新したり挿入したりすることはできません。

このプロパティの値は、インスタンス内の機能への予期しないアクセスを委任開発者が許可できるかどうかに影響します。プロパティにロールが含まれている場合は、そのロールのみがスクリプトのモジュールを実行できます。

詳細情報

属性	説明
プロパティ名	*com.glide.sys.security.delegateddev.block_grant_roles*
構成タイプ	システムプロパティ (/sys_properties_list.do)
Instance Security Center での構成	あり
目的	このプロパティの値は、インスタンス内の機能への予期しないアクセスを委任開発者が許可できるかどうかに影響します。
タイプ	切り替えスイッチ
推奨値	true
セキュリティ依存関係	none
機能への影響度	(高) delegated_developer ロールを持つユーザーが sys_user_has_role のレコードを変更しようとすると、その操作に対する追加のセキュリティチェックがこのプロパティによって有効になります。ユーザーが sys_user_has_role を作成または更新しようとしている場合、user_admin ロールがそのユーザーに付与されていることが追加のセキュリティチェックによって検証されます。ユーザーに user_admin ロールがない場合、アクセスは拒否されます。プロパティが false の場合、これらの追加チェックは検証されません。
セキュリティリスク	(高) 適切な承認がないと、無許可のユーザーがインスタンスの機密コンテンツ/データにアクセスする可能性があります。
参照	アクセス制御

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

UI アクション条件の実行前確認 (インスタンスセキュリティ強化)

glide.security.strict.actions プロパティを使用して、実行前にフォームおよびリスト内の UI アクションの条件を確認できるようにします。このプロパティを **true** に設定すると、実行前にテーブル UI アクションに検証レイヤーが追加されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

詳細情報

属性	説明
プロパティ名	glide.security.strict.actions
構成タイプ	システムプロパティ (/sys_properties_list.do)
Instance Security Center での構成	あり
目的	実行前にテーブル UI アクションに検証レイヤーをさらに追加すること
推奨値	true
機能への影響度	(低) この修正では、インスタンスのターゲットテーブル/ページで UI アクションをチェックするための検証レイヤーが追加されるだけです。アクセス制御が顧客インスタンスで適切に設定されているかぎり、ここに影響はありません。
セキュリティリスク	(中) 2 つのゾーンの間でトランザクションが発生した場合は常に、アクセス要求がチェックされます。この操作により、エンドユーザーに対してフォームがレンダリングされる前に UI アクションが検証されます。
参照	高セキュリティプラグイン

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

コンテキスト依存セキュリティ：**Role Management** プラグイン (インスタンスセキュリティ強化)

コンテキストセキュリティのアクティブ化： (*com.glide.role_management*) プラグインによりコンテキストセキュリティが有効になり、作成、読み取り、書き込み、および削除機能を使用してレコード/情報が保護されます。

インストールしてアクティブ化すると、(簡易セキュリティマネージャーによって作成された) dictionary ロールはテストされなくなります。代わりに、Now Platform はフィールドとテーブルの ACL ルールを検索します。また、シンプルなセキュリティマネージャーによって実装される従来のロールベースの辞書ルールではなく、ACL ルールを使用してデータを保護します。辞書フォームを設定して辞書エントリにロールを追加しても、権限は変更されません。

詳細情報

属性	説明
プラグイン ID	com.glide.role_management
構成タイプ	[システム定義] > [プラグイン]
Instance Security Center での構成	あり
目的	シンプルなセキュリティマネージャーとは異なり、コンテキストセキュリティマネージャーはシステムテーブル階層を認識しています。階層内の表示場所に基づいて、1 つのフィールドに複数の異なるセキュリティルールを設定できます。
推奨値	アクティブ (デフォルトでアクティブ化されたプラグイン)

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

属性	説明
機能への影響度	(中) この修正では、アクセス制御の機能レベルが適用されます。これにより、アプリケーションは ACL テーブルのみに基づいてアクセス制限を決定できます。
セキュリティリスク	(高) CRUD 操作を実行する前に、サーバー側から機能レベルのアクセス制御を適用し、インスタンスユーザーに適切なレベルのアクセスを確保する必要があります。
参照	コンテキスト依存セキュリティマネージャー

プラグインのアクティブ化の詳細については、「Activate a plugin」を参照してください。

CSV 要求承認 (インスタンスセキュリティ強化)

glide.basicauth.required.csv プロパティを使用して、受信 CSV (カンマ区切り値) 要求で基本認証を要求するかどうかを指定します。

詳細情報

属性	説明
プロパティ名	glide.basicauth.required.csv
構成タイプ	システムプロパティ (/sys_properties_list.do)
Instance Security Center での構成	あり
目的	CSV 要求に対して基本認証を適用すること
推奨値	true
機能への影響度	(低) この修正では、基本認証とシステムレベルのアクセス制御の形で、認証方法の組み合わせが適用されます。 • インスタンス上の CSV データの形式でテーブル/ページからデータを取得する際に、この認証を実行します。 • 現在このデータにアクセスしているゲストユーザーを制限します。必要であれば、このコンテンツへのアクセスを必要とするユーザーのために、必要なアクセス制御権限を持つ新しいアカウントを作成する場合があります。 詳細については、「CSV 形式のファイルからのデータの取得」を参照してください。
セキュリティリスク	(中) 受信 CSV 要求で適切な承認が構成されていない場合、無許可のユーザーがターゲットインスタンスの機密コンテンツ/データにアクセスする可能性があります。
参照	Web サービスセキュリティ

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

デフォルトで拒否 (インスタンスセキュリティ強化)

glide.sm.default_mode プロパティを使用して、既存の ACL ルールがワイルドカードテーブルの ACL ルールの一部であることが判明した場合の、セキュリティマネージャーのデフォルトの動作を制御します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

初期インスタンスのインストール中に High Security Settings (*com.glide.high_security*) プラグインがアクティブ化されると、このプロパティが作成され、ワイルドカード ACL ルールが作成されます。システムテーブルへのロールベースのアクセスを提供するために、これらのルールは多数の ACL と最も一般的なレコードベースの操作を制御します。

- 読み取り
- 書き込み
- 作成
- 削除

デフォルトの拒否オプションを有効にして High Security プラグインを使用しないかぎり、多くのテーブルは保護されません。Now Platform では、管理者以外のユーザーは一致する ACL ルールを満たさないかぎりオブジェクトにアクセスできないという、デフォルトの拒否セキュリティモデルを使用します。このモデルを使用して、安全でないスクリプトなどの多くの攻撃ベクトルを削除します。

詳細情報

属性	説明
プロパティ名	glide.sm.default_mode
構成タイプ	システムプロパティ (/sys_properties_list.do)
Instance Security Center での構成	あり
目的	セキュリティ上のベストプラクティスは、無許可のユーザーによるテーブルへのアクセスを制限することです。 • テーブルに ACL ルールがない場合、このプロパティは、テーブル/フィールドで実行される CRUD 操作に対して少なくともワイルドカード ACL が検証されるようにします。 • これらのルールでは、ユーザーが admin ロールを所有しているか、別のテーブル ACL ルールの要件を満たしている場合を除き、読み取り、書き込み、作成、削除の操作をすべてのテーブルで制限します。
推奨値	拒否
機能への影響度	(高) このプロパティを [許可] に設定すると、ワイルドカードテーブル ACL ルールは、そのような操作を制限する特定のテーブル ACL ルールが存在する場合を除き、CRUD 操作をすべてのテーブルで許可します。 **注:** このプラグインは、本番環境で既に使用されているテーブルへのセキュリティアクセスを変更する可能性があるため、既存のインスタンスを対象としていません。
セキュリティリスク	(高) 管理者以外のユーザーは、ワイルドカードテーブル ACL ルールに一致するオブジェクトにアクセスできます。
参照	デフォルトの拒否プロパティ

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

受信トランザクションのダブルチェック (インスタンスセキュリティ強化)

glide.security.strict.updates プロパティはフォーム送信時に受信トランザクションのセキュリティのダブルチェックを有効にし、ブラウザでフォームが表示される前のテーブル検証のレイヤーを追加します。このプロパティはデフォルトで **true** に設定されています。

詳細情報

注:
Vancouver 以降のリリースでは、このプロパティはデフォルトで **true** に設定されており、管理者が変更することはできません。プロパティを変更する必要があるユースケースについては、カスタマーサポートにお問い合わせください。

属性	説明
プロパティ名	glide.security.strict.updates
構成タイプ	システムプロパティ (/sys_properties_list.do)
Instance Security Center での構成	あり
目的	ブラウザーでフォームを表示する前に、ユーザー権限の検証レイヤーを確実に追加すること
推奨値	true
機能への影響度	(低) この修正では、インスタンスのターゲットテーブル/ページでユーザー権限をチェックするための検証レイヤーが追加されます。アクセス制御が顧客インスタンスで適切に設定されているかぎり、影響はありません。
セキュリティリスク	(高) 2 つのゾーンの間でトランザクションが発生した場合は常に、アクセス要求をチェックする必要があります。この操作では、フォームが要求されたとき、およびフォームがレンダリングされる前に、権限がチェックされます。
参照	セキュリティ設定プロパティ

ACL を有効にしてライブプロファイルの詳細を制御する (インスタンスセキュリティ強化)

glide.live_profile.details プロパティを使用して、ユーザーがライブプロファイルのすべての詳細フィールド (会社名や電話番号など) を表示できるようにするかどうかを指定します。

glide.live_profile.details プロパティの設定に応じて、以下が発生します。

- 値が [表示] に設定されている場合、ユーザープロファイルに対して作成された ACL に関係なく、ライブプロファイル情報へのアクセスが許可されます。
- 値が **[ACL]** に設定されている場合、ユーザープロファイルに対して作成された ACL に応じて、ライブプロファイル情報へのアクセスが制限されます。
- 値が [非表示] に設定されている場合、ユーザープロファイルに対して作成された ACL に関係なく、ライブプロファイル情報へのアクセスが制限されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

詳細情報

属性	説明
プロパティ名	glide.live_profile.details
構成タイプ	システムプロパティ (/sys_properties_list.do)
Instance Security Center での構成	あり
目的	目的は、許可されたユーザーのみがライブプロファイルの詳細 (会社名、電話番号など) にアクセスできるようにすることです。
推奨値	ACL
機能への影響度	(中) プロパティが有効になっていない場合、無許可のユーザーが他のすべてのユーザーのライブプロファイルの詳細にアクセスできます。
セキュリティリスク	(中) API 要求は常にテーブル ACL を優先する必要があります。無許可のユーザーがライブプロファイルの詳細にアクセスするのを防ぐために、制限を適用する必要があります。

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

AJAXGlideRecord ACL チェックの有効化 (インスタンスセキュリティ強化)

glide.script.secure.ajaxgliderecord プロパティを使用して、クライアントスクリプト内で GlideAjax API を使用してサーバー側のレコード (テーブルなど) にアクセスする場合にアクセス制御リスト (ACL) ルール検証を実行します。

クライアントスクリプトから、AJAXGlideRecord (GlideAjax -クライアント) API。サーバー側の Glide レコードなどの構文を使用します。多くの展開で、これは強力で便利なツールです。

アクセス制御リスト (ACL) を GlideAjax API 呼び出しに適用することを選択すると、現在接続しているユーザーがアクセスできるデータのみをクエリーできます。たとえば、cmn_location テーブルを読み取る権限のない ESS ユーザーがログインすると、そのテーブルに対する GlideAjax API 呼び出しは失敗します。

Now Platform が GlideAjax ACL 呼び出しのチェックなしで実行されている場合、API は、現在ログインしているユーザーが他の方法ではアクセスできない情報を返す可能性があります。

詳細情報

属性	説明
プロパティ名	glide.script.secure.ajaxgliderecord
構成タイプ	システムプロパティ (/sys_properties_list.do)
Instance Security Center での構成	あり
目的	クライアント側 API を介してレコードにアクセスする場合でも、セキュリティ ACL が確実にチェックおよび検証されるようすること
推奨値	true

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

属性	説明
機能への影響度	(高) この修正では、AJAXGlideRecord API 呼び出しを使用して要求が行われた場合に、サーバー側レコードとの ACL 関係が適用されます。ACL 構成が適切に設定されていない場合、影響を受ける可能性があります。影響度とその識別方法の詳細については、「クライアント側 GlideRecord (AJAXGlideRecord) トランザクションの監査とレビューに関する記事 [KB0550828] (HI ナレッジベース で入手可能)」を参照してください。
セキュリティリスク	(高) クライアントスクリプトを使用すると、GlideAjax API を介してサーバーから任意のデータをクエリーできます。サーバー側のリソースには適切な承認なしでアクセスできるため、ACL 検証を使用すると、アプリケーションで設定された承認に基づいて要求を検証するのに役立ちます。
ワークアラウンド	GlideAjax (AJAXGlideRecord) API で使用されるスクリプトインクルード、プロセッサー、およびその他のエンティティに対して適切な ACL が作成され、適切な承認の下で実行されるようにします。 canRead ()、canWrite ()、canCreate ()、canDelete () などのメソッドを実装して、GlideRecord を使用してテーブルレコードにアクセスする前に、ユーザーの承認を実行します。 もう 1 つの方法は、GlideRecordSecure を使用することです。このクラスは GlideRecord サーバーから継承され、GlideRecord と同じ関数を実行し、ACL も適用します。
参照	ACL を AJAXGlideRecord (クライアント側の Glide レコード) に追加 このプロパティは、クライアントからのスクリプトの実行を保護および制限するプロパティと同じファミリーに属します。 • `glide.script.use.sandbox`：「クライアント生成スクリプトサンドボックス」を参照 • `glide.script.allow.ajaxevaluate`：「AJAXEvaluate を有効にする」を参照

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

Excel 要求承認 (インスタンスセキュリティ強化)

`glide.basicauth.required.excel` プロパティを使用して、受信 Excel 要求で基本認証を要求するかどうかを指定します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

詳細情報

属性	説明
プロパティ名	glide.basicauth.required.excel
構成タイプ	システムプロパティ (/sys_properties_list.do)
Instance Security Center での構成	あり
目的	Excel 要求に対して基本認証を適用すること
推奨値	true
機能への影響度	(低) この修正では、基本認証とシステムレベルのアクセス制御の形で、認証方法の組み合わせが適用されます。 • インスタンス上で Excel データの形式でテーブル/ページからデータを取得する際に、この認証を実行します。 • 現在このデータにアクセスしているゲストユーザーを制限します。必要であれば、このコンテンツへのアクセスを必要とするユーザーのために、必要なアクセス制御権限を持つ新しいアカウントを作成する場合があります。
セキュリティリスク	(中) 受信 Excel 要求で適切な承認が構成されていない場合、無許可のユーザーがターゲットインスタンスの機密コンテンツ/データにアクセスする可能性があります。

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

Explicit Role プラグイン (インスタンスセキュリティ強化)

Explicit Role (*com.glide.explicit_roles*) プラグインをアクティブ化して、B2B および B2C アプリケーション用の新しい snc_internal および snc_external ロールをインスタンスに提供し、外部ユーザーが内部データにアクセスできないようにします。エンタープライズユーザー (従業員) には内部ロールが必要ですが、非エンタープライズユーザー (非従業員) には外部ロールが必要です。

Explicit Role プラグインをインストールする場合：

- 既存のすべてのユーザーに新しい snc_internal ロールを割り当てます。また、ロールのないすべてのテーブルに snc_internal ロールを割り当てます。
- Explicit Role プラグインをアクティブ化した後にユーザーまたはテーブルを作成すると、Now Platform がユーザーまたはテーブルに snc_internal ロールをアサインします。
- Now Platform では、snc_external ロールが明示的にアサインされていないテーブルに snc_external ロールを持つユーザーがアクセスすることを禁止します。
- public ロールがアサインされたテーブルには、内部ユーザーと外部ユーザーの両方がアクセスできます。
- 一部のサービスポータルウィジェットではログインが必要ですが、特定のユーザーロールは必要ありません。Explicit Roles プラグインをインストールすると、外部ユーザーはこれらのポータルにアクセスできなくなります。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- ○ 外部ユーザーのアクセスを許可するには、ウィジェットを編集して必要なロールを空白から **snc_internal, snc_external** に変更します。
  - ○ この問題の一例として、ケースマネジメントアプリケーションを使用しており、かつ外部ユーザーが自分のケースレコードにファイルを添付できることを必要とする顧客が挙げられます。説明のとおりに **Encryption-context-picker** ウィジェットの構成を変更すると、外部ユーザーが想定どおりに添付できるようになります。
  - ○ ウィジェットの構成の詳細については、「ウィジェットインスタンスオプションの設定」を参照してください。

注:
明示的なロールプラグインが有効であるかどうかにかかわらず、System Update Sets をインスタンス間で移動しないでください。詳細については、「System Update Sets」を参照してください。

ロールの概要

snc_internal

このロールは、すべての内部ユーザー (従業員または組織の内部) に割り当てられます。追加された新しいユーザーは、snc_external ロールがまだ割り当てられていない場合、初回のログイン/代理操作中にもこのロールを取得します。ロールのないすべての既存のアクセス制御ルール (ACL) には、「snc_internal」ロールが適用されます。新しい ACL の場合、ACL がロールなしで保存されると、Now Platform によってこのロールが自動的に追加されます。

snc_external

このロールは、ユーザーが組織の外部にあり、次の場合を除きリソースにアクセスできないことを示します。

- snc_external ロールに対して ACL によるアクセスを明示的に許可している場合、または
- 追加のロールを明示的に付与した場合。

デフォルトでは、snc_external ロールを持つユーザーは、プロセッサーや UI ページなどの非レコードタイプのリソースにもアクセスできません。

公開

公開ロールがアサインされたエンティティには、snc_internal と snc_external の両方のユーザーがアクセスできます。

明示的なロールプラグインを使用する場合：

1. 公開ロールを含むテーブルに、非認証の公開ユーザーなどの外部ユーザーに対する機密レコードが含まれていないことを確認し、検証します。
2. 公開ロールを持つテーブルに機密データが含まれており、外部ユーザーから機密レコードを制限したい場合は、次のいずれかを行います。
   - ○ テーブルから公開ロールを削除します。または
   - ○ スクリプト化された ACL をテーブルに追加します。
3. Scripted REST APIs などのすべてのエンドポイントが、*`GlideRecordSecure`* を使用している、または `canRead()`、`canWrite()`、`canUpdate()`、および `canDelete()` を使用して、明示的にロールをチェックしているかを確認および検証します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

詳細情報

属性	説明
プラグイン名	com.glide.explicit_roles
構成タイプ	[システム定義] > [プラグイン]
Instance Security Center での構成	なし
目的	外部ユーザーが内部データにアクセスできないようにすること
推奨値	有効
機能への影響度	(低) snc_internal ロールはプラグインによって自動的にテーブルにアサインされるため、既存の内部ユーザーは引き続き必要なアクセスを行えるため、大きな影響はありません。
セキュリティリスク	(高) 外部ユーザー (非従業員) は、ロールが割り当てられていない Now Platform 内の多くの機密テーブルにアクセスできます。これらは、内部ユーザー (従業員) のみにアクセスを限定する必要があります。
参照	明示的なロール

設定手順

明示的なロールを持つ機能またはアプリケーションを作成する場合：

1. 新しい機能またはアプリケーションの snc_external ロールを継承するロールを作成します。
2. 外部ユーザーを作成する場合は、snc_internal ロールを削除し、snc_external ロールを継承する新たに作成したロールを追加します。
3. snc_external ロールを継承する新規ロールを既存のテーブルに追加する場合は、テーブルに機密レコードが含まれていないことを確認および検証してください。
4. テーブルを作成する場合は、が承認された内部および外部ユーザーロールのみがテーブルにアクセスできることを検証します。
5. スクリプト化された REST API などのエンドポイントを作成する場合は、GlideRecordSecure を使用するか、canRead()、canWrite()、canUpdate()、および canDelete() を使用して明示的にロールをチェックします。

公開ロールでテーブルを作成する場合は、そのテーブルに、非認証の公開ユーザーなどの外部ユーザーに対する機密レコードが含まれないようにしてください。

インポート要求承認 (インスタンスセキュリティ強化)

glide.basicauth.required.importprocessor プロパティを使用して、受信インポート要求で基本認証を要求するかどうかを指定します。

詳細情報

属性	説明
プロパティ名	glide.basicauth.required.importprocessor
構成タイプ	システムプロパティ (/sys_properties_list.do)

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

属性	説明
Instance Security Center での構成	あり
目的	インポート要求に基本認証を適用すること
推奨値	true
機能への影響度	(低) この修正では、基本認証とシステムレベルのアクセス制御の形で、認証方法の組み合わせが適用されます。 • データソースをインスタンステーブル/ページにインポートするときに、この認証を実行します。 • 現在このデータにアクセスしているゲストユーザーを制限します。必要であれば、このコンテンツへのアクセスを必要とするユーザーのために、必要なアクセス制御権限を持つ新しいアカウントを作成する場合があります。 詳細については、「CSV 形式のファイルからのデータの取得」を参照してください。
セキュリティリスク	(中) データソースインポート要求で適切な承認が構成されていない場合、無許可のユーザーがターゲットインスタンスの機密コンテンツ/データにアクセスする可能性があります。
参照	SOAP Web Services のセキュリティ SOAP Web サービス

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

PDF 要求承認 (インスタンスセキュリティ強化)

glide.basicauth.required.pdf プロパティを使用して、受信 PDF 要求で基本認証を要求するかどうかを指定します。

詳細情報

属性	説明
プロパティ名	glide.basicauth.required.pdf
構成タイプ	システムプロパティ (/sys_properties_list.do)
Instance Security Center での構成	あり
目的	PDF 要求に対して基本認証を適用すること
推奨値	true
機能への影響度	(低) この修正では、基本認証とシステムレベルのアクセス制御の形で、認証方法の組み合わせが適用されます。 • インスタンス上で PDF データの形式でテーブル/ページからデータを取得する際に、この認証を実行します。 • 現在このデータにアクセスしているゲストユーザーを制限します。必要であれば、このコンテンツへのアクセスを必要とするユーザーのために、必要なアクセス制御権限を持つ新しいアカウントを作成する場合があります。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

属性	説明
	詳細については、「Web サービスインポートセット」を参照してください。
セキュリティリスク	(中) 受信 PDF 要求で適切な承認が構成されていない場合、無許可のユーザーがターゲットインスタンスの機密コンテンツ/データにアクセスする可能性があります。

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

パフォーマンス監視 **(ACL)** (インスタンスセキュリティ強化)

glide.security.diag_txns_acl プロパティを使用して、認証されていない接続からの stats.do、threads.do、thread_pool_stats および replication.do アクセスを制御します。

このプロパティを **true**に設定すると、*glide.security.diag_txns_acl* プロパティは管理者アカウントによる以下へのアクセスのみを許可します。

- https://<instancename>.servicenow.com/stats.do
- https://<instancename>.servicenow.com/threads.do
- https://<instancename>.servicenow.com/replication.do
- https://<instancename>.servicenow.com/thread_pool_stats.do

この設定を有効にしない場合、認証されていない接続からこれらのリソースに引き続きアクセスできます。

詳細情報

属性	説明
プロパティ名	glide.security.diag_txns_acl
構成タイプ	システムプロパティ (/sys_properties_list.do)
Instance Security Center での構成	あり
目的	設定ページへのアクセスを管理者アカウントのみに制限すること
推奨値	true
機能への影響度	(低) この修正では、ログ記録とトラブルシューティングの目的で、管理者アカウントのみがアプリケーションの機密データにアクセスできるようにします。
セキュリティリスク	(低) サーバーの詳細、スレッド、サーバーで実行されるプロセスなどの機密データは、適切な権限のないエンドユーザーが表示したりアクセスしたりすることはできません。

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

パフォーマンス監視 **IP** 制限 (インスタンスセキュリティ強化)

glide.custom.ip.authenticate.allow プロパティを使用して、stats.do、threads.do および replication.do pages ページへのアクセスを、指定されたカンマ区切りリストまたは IP アドレス範囲のみに限定します。このプロパティが有効になっていない場合は、どの IP アドレスからでもこれらのタイプのページにアクセスできます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注:
直近の変更に基づいて、すべての IP 制限に IP アドレスアクセス制御を使用する必要があります。「特定の IP 範囲へのアクセスを制限する」の「設定手順」の項を参照してください。

詳細情報

属性	説明
プロパティ名	glide.custom.ip.authenticate.allow
構成タイプ	システムプロパティ (/sys_properties_list.do)
Instance Security Center での構成	なし
目的	構成ページへのアクセスを包含リストの IP アドレスに制限すること
推奨値	IP アドレスのカンマ区切りリスト
機能への影響度	(低) 信頼できない IP アドレスからでも機密情報ページにアクセスできます。
セキュリティリスク	(低) IP アクセス制御機能を使用して、インターネット上のターゲットインスタンスへの不必要な開示を制限する必要があります。
参照	利用可能なシステムプロパティ

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

クライアント呼び出し可能スクリプトインクルードのプライバシー (インスタンスセキュリティ強化)

デフォルトでは、明示的に可視性を設定していないクライアント呼び出し可能スクリプトインクルードは、公開状態になります。必要に応じて *glide.script.ccsi.ispublic* プロパティを追加すると、公開ページからアクセスされるクライアント呼び出し可能スクリプトインクルード全体に対してプライバシーコントロールができるようになります。

このプロパティを追加する場合は、値を **false** に設定する必要があります。これは、クライアント呼び出し可能スクリプトインクルードがすべて非公開であり、公開ページで可視性を変更するという指定になります。

注:
値が **true** のプロパティを追加したり、値を **false** から **true** に変更したりすることはできません。これを実行しようとすると、エラーメッセージが表示されます。

必要に応じて、isPublic() 関数を追加することにより、クライアント呼び出し可能スクリプトインクルードのプライバシー設定を個別に変更できます。

- isPublic() 設定は *glide.script.ccsi.ispublic* プロパティよりも優先されます。
- たとえば、個別のスクリプトで isPublic() を **true** に設定すると、このスクリプトが公開状態になります。これは、他のクライアント呼び出し可能スクリプトインクルードをすべて非公開にする *glide.script.ccsi.ispublic* プロパティを上書きします

詳細情報

属性	説明
プロパティ名	glide.script.ccsi.ispublic

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

属性	説明
構成タイプ	システムプロパティ (/sys_properties_list.do)
Instance Security Center での構成	あり
目的	クライアント呼び出し可能スクリプトインクルードを非公開にすると、公開ページにアクセスするゲストはクライアント呼び出し可能スクリプトインクルードにアクセスできないということになります。ログインしていないユーザーは、非公開スクリプトを実行できません。
推奨値	false
機能への影響度	(高) クライアント呼び出し可能スクリプトインクルードが公開として指定されている場合 (つまり、このプロパティがない場合)、非認証ユーザーはクライアントスクリプトを実行できます。ログインしていないユーザーによるスクリプトの実行を制限するプロパティを追加します。
セキュリティリスク	(高) このプロパティを追加しない場合、クライアント側スクリプトインクルードが ACL を回避し、その結果意図せずに機能が公開される可能性があります。クライアントスクリプトに機密情報がある場合は、有害なセキュリティリスクが発生するおそれがあります。
ワークアラウンド	*glide.script.ccsi.ispublic* プロパティを **false** に設定すると、すべてのクライアント呼び出し可能スクリプトインクルードが非公開になります。 isPublic() 関数を追加することにより、クライアント呼び出し可能スクリプトインクルードのプライバシー設定を個別に変更できます。isPublic() 関数は *glide.script.ccsi.ispublic* プロパティよりも優先されます。スクリプトインクルードに次の構文を追加します。 isPublic:function(){return[true/false];},

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

お気に入りへの公開アクセス

glide.ui.magellan.favorites.allow_public を使用して、認証されていないユーザーがナビゲーターで [お気に入り] を表示できるようにするかどうかを指定します。

glide.ui.magellan.favorites.allow_public が **false** に設定されている場合、お気に入りへの公開アクセスは準拠します。

詳細情報

属性	説明
プロパティ名	*glide.ui.magellan.favorites.allow_public*
構成タイプ	システムプロパティ (/sys_properties_list.do)
Instance Security Center での構成	あり

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

属性	説明
目的	認証されていないユーザーがナビゲーターで [お気に入り] を表示できるようにするかどうかを制御します。
タイプ	True/False
推奨値	*false*
セキュリティ依存関係	*glide.ui.magellan.favorites.allow_public* を **false** に設定します。
機能への影響度	(中) このプロパティを有効にすると、権限のないユーザーから保護するレイヤーとして機能します。
セキュリティリスク	(中) このプロパティを有効にしないと、機密データに不正にアクセスされるリスクがあります。
参照	お気に入りの作成または表示

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

特定の IP 範囲にアクセスを制限する (インスタンスセキュリティ強化)

com.snc.ipauthenticator プロパティを使用して、特定の IP 範囲にアクセスを制限します。インスタンスに対するパブリック アクセスが意図されている場合を除き、管理者は割り当てられた IP ネットブロックにアクセスを制限する必要があります。

必須条件

このプロパティを設定する前に、IP Range Based Authentication *com.snc.ipauthenticator* プラグインをアクティブ化する必要があります。詳細については、「IP 範囲ベースの認証」および「設定手順」の項 (下記) を参照してください。

詳細情報

属性	説明
プラグイン名	com.snc.ipauthenticator
構成タイプ	[System Security] > [IP アドレスアクセス制御]
Instance Security Center での構成	あり
目的	インスタンスにアクセスできるまたはアクセスできない IP アドレスの範囲を、信頼できるドメインと信頼できないドメインのリストに追加すること
推奨値	有効
機能への影響度	(低) 顧客が拒否した IP 範囲がこの修正アイテムに使用されます。顧客がターゲットリストを定義するため、影響はありません。
セキュリティリスク	(低) IP アクセス制御機能を使用して、インターネット上のターゲットインスタンスへの不必要な開示を制限する必要があります。
参照	IP 範囲ベースの認証

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

設定手順

1. com.snc.ipauthenticator プラグインがアクティブであることを確認します。
2. 移動先 システムセキュリティ > **IP** アドレスアクセス制御.
3. [新規] をクリックして、IP アドレスの除外リスト (拒否) または包含リスト (許可) を作成します。
4. [送信] をクリックします。

RSS 要求承認 (インスタンスセキュリティ強化)

glide.basicauth.required.rss プロパティを使用して、受信 RSS 要求で基本認証を要求するかどうかを指定します。

詳細情報

属性	説明
プロパティ名	glide.basicauth.required.rss
構成タイプ	システムプロパティ (/sys_properties_list.do)
Instance Security Center での構成	あり
目的	RSS 要求に対して基本認証を適用すること
推奨値	true
機能への影響度	(低) この修正では、基本認証とシステムレベルのアクセス制御の形で、認証方法の組み合わせが適用されます。 • インスタンスで RSS 要求を処理する際に、この認証を実行します。 • 現在このデータにアクセスしているゲストユーザーを制限します。必要であれば、このコンテンツへのアクセスを必要とするユーザーのために、必要なアクセス制御権限を持つ新しいアカウントを作成する場合があります。 詳細については、「RSS フィードジェネレーター」を参照してください。
セキュリティリスク	(中) 受信 RSS 要求で適切な承認が構成されていない場合、無許可のユーザーがターゲットインスタンスの機密コンテンツ/データにアクセスする可能性があります。
参照	RSS 基本認証

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

SAML 2.0 Web ブラウザ **SSO** プロファイル (インスタンスセキュリティ強化)

com.snc.integration.sso.saml20.update1 プラグインは、SAML 2.0 Single Sign-On プラグインのステータスがアクティブであることを確認します。

セキュリティアサーションマークアップ言語 (SAML) は、セキュリティドメイン間で認証および承認データを交換するための XML ベースの規格です。SAML は、ID プロバイダー (アサーションのプロデューサー) とサービスプロバイダー (アサーションのコンシューマー) の間でセキュリティ情報を交換します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

com.snc.integration.sso.saml20.update1 プラグインは必須のプラグインですが、手動でアクティブ化する必要はありません。*sso.multi.installer* は、必要なすべての SAML 関連プラグインをインストールします。また、応答検証のオプションを提供する saml2 実装スクリプトも含まれています。詳細については、「詳細情報」の「参照」トピックを参照してください。

詳細情報

属性	説明
プラグイン名	com.snc.integration.sso.saml20.update1 (新規)
構成タイプ	[システム定義] > [プラグイン]
Instance Security Center での構成	あり
目的	クロスサイトスクリプティング攻撃を防止すること
推奨値	有効
必要なロール	管理者はプラグインをアクティブ化できません。昇格されたセキュリティ権限を持つユーザーに、インスタンスでのアクティブ化を要求します。
参照	SAML による認証 SAML 統合 既存の SAML 2.0 統合の更新

プラグインのアクティブ化の詳細については、「Activate a plugin」を参照してください。

スクリプト要求承認 (インスタンスセキュリティ強化)

glide.basicauth.required.scriptedprocessor プロパティを使用して、受信スクリプト要求で基本認証を要求するかどうかを指定します。

詳細情報

属性	説明
プロパティ名	glide.basicauth.required.scriptedprocessor
構成タイプ	システムプロパティ (/sys_properties_list.do)
Instance Security Center での構成	あり
目的	スクリプト要求に対して基本認証を適用すること
推奨値	true
機能への影響度	(中) この修正では、基本承認の形式で認証が適用されます。 • インスタンスでスクリプト要求を処理する際に、この認証を実行します。 • 現在このデータにアクセスしているゲストユーザーを制限します。必要であれば、このコンテンツへのアクセスを必要とするユーザーのために、必要なアクセス制御権限を持つ新しいアカウントを作成する場合があります。
セキュリティリスク	(高) 受信スクリプト要求で適切な承認が構成されていない場合、無許可のユーザーがターゲットインスタンスの機密コンテンツ/データにアクセスします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

属性	説明
参照	認証

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

セキュリティジャンプスタート (ACL ルール) (インスタンスセキュリティ強化)

Security Jump Start (ACL Rules) (*com.snc.system_security*) プラグインをアクティブ化して、Now Platform 内の主要なシステムテーブルの一部でアクセス制御を検証する重要な ACL を複数作成します。

これらのルールは、多くのシステムテーブルを保護するためのジャンプスタートを提供し、組織がより簡単にインスタンスを本番環境に移行できるようにします。Security Jump Start (ACL ルール) プラグインは、すべての新しいインスタンスに自動的にインストールされます。

詳細情報

属性	説明
プラグイン ID	com.snc.system_security
構成タイプ	[システム定義] > [プラグイン]
Instance Security Center での構成	あり
目的	Security Jump Start (ACL Rules) プラグインをアクティブ化して、適切なセキュリティコンプライアンスを実現します。 これは、最初にシステムテーブルを保護する基本的な ACL をいくつか提供します。インスタンスのデフォルトのプロビジョニングに付属する各システムテーブルに対して手動で作成するのではありません。これらの ACL は、新しく作成されたインスタンスを迅速に本番環境に移行する必要がある場合に役立ちます。
推奨値	有効
機能への影響度	(中) インスタンスの既存の ACL を監査せずにこのプラグインをインストールすると、機能に大きな影響があります。修正を行う前に、顧客への働きかけと定義が必要です。
セキュリティリスク	(高) アクセス制御を適用して、インスタンスへの意図しないアクセスをロックする必要があります。ACL ジャンプスタートルールは、多くのシステムテーブルを保護するための開始点を提供し、組織が迅速に本番環境に移行できるようにするために作成されました。
参照	Security Jump Start - ACL ルール

設定手順

インスタンスでこのプラグインがアクティブ化されていない場合は、ServiceNow サポートにお問い合わせください。この時点でプラグインをアクティブ化すると、本番環境で既に使用されているテーブルへのセキュリティアクセスが変更される可能性があります。プラグインから提供される新しい ACL ルールに管理者が注目している場合は、必要に応じて既存のインスタンスに 1 つ以上の ACL ルールを手動で作成できます。この ACL のリストは、その場合の指針として使用できます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

プラグインのアクティブ化の詳細については、「Activate a plugin」を参照してください。

SNC Access Control プラグイン (インスタンスセキュリティ強化)

SNC Access Control (*com.snc.snc_access_control*) プラグインをアクティブ化して、カスタマーサービス & サポート担当者によるインスタンスへのアクセスを制御します。

Now Platform のデフォルト構成では、短期的なサポート資格情報を作成する内部プロセスを介してカスタマーサービスとサポートがインスタンスにアクセスできます。すべてのアクセスが監査されますが、このアクセスを制御することを希望する顧客もいます。

このプラグインを使用すると、顧客管理者は、カスタマーサービス & サポート の従業員がインスタンスにアクセスできないようにすることができます。サポートアクティビティを開始する前に Now Platform アクセスを有効にする必要があるため、この決定はサポート SLA に影響します。詳細については、「ServiceNow アクセス制御 」を参照してください。

詳細情報

属性	説明
プラグイン名	com.snc.snc_access_control
構成タイプ	[システム定義] > [プラグイン]
Instance Security Center での構成	あり
目的	カスタマーサービス & サポートの従業員によるインスタンスへのアクセスの禁止
推奨値	有効
必要なロール	顧客管理者はプラグインをアクティブ化できません。プラグインをアクティブ化するには昇格された権限が必要なため、明示的に要求する必要があります。
機能への影響度	(低) このプラグインが非アクティブの場合、カスタマーサービス & サポートのすべての従業員は顧客のインスタンスにアクセスできます。プラグインを有効にすると、顧客は承認されたカスタマーサービス & サポートの従業員のみにアクセスを制限できます。
セキュリティリスク	(低) より幅広いユーザーグループに対してインスタンスアクセスが不必要に公開されます。
参照	ServiceNow アクセス制御

設定手順

1. プラグインを要求するには、「ServiceNow アクセス制御の有効化」の手順に従います。顧客は HI から SNC Access Control プラグイン (com.snc.snc_access_control) を要求する必要があります。
2. SNC アクセス制御を有効にするには、「ServiceNow アクセス制御の構成」の手順に従います。アクセス制御レコードを設定して、インスタンスにログインする権限を持つカスタマーサービス & サポートの従業員を 1 人以上指定します。

SOAP コンテンツタイプのチェック (インスタンスセキュリティ強化)

glide.soap.require_content_type_xml プロパティを使用して、テキスト/xml のコンテンツタイプの検証を有効にし、無効な SOAP 要求から保護します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

- **true** に設定すると、Now Platform はテキスト/xml のコンテンツタイプを検証して無効な SOAP 要求から保護します。
- **false** に設定すると、すべてのコンテンツタイプの値が許可されます。

詳細情報

属性	説明
プロパティ名	glide.soap.require_content_type_xml
構成タイプ	システムプロパティ (/sys_properties_list.do)
Instance Security Center での構成	あり
目的	無効な SOAP 要求から保護すること
推奨値	true
機能への影響度	(低) この修正により、すべての受信 SOAP 要求に対して SOAP コンテンツタイプを検証できるようになります。 • 受信要求に text/xml 以外のコンテンツタイプを使用している場合は、SOAP トランザクションが失敗する可能性があります。 • 正しい MIME タイプを使用していない場合、サードパーティの統合が中断される可能性があります。
セキュリティリスク	(高) 受信 SOAP 要求を受け入れる場合、適切な検証が実行され、関連するコンテンツタイプが要求の一部として定義されていることが確認されます。これにより、セキュリティリスクと見なされる可能性のある無効な SOAP 応答が制限されます。
参照	コンテンツタイプ

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

厳格な IP 制限 (インスタンスセキュリティ強化)

glide.ip.authenticate.strict プロパティを使用して、DC やセキュア VPN などの厳格な IP アドレスのセットがこのインスタンスにアクセスできるようにします。

詳細情報

属性	説明
プロパティ名	glide.ip.authenticate.strict
構成タイプ	システムプロパティ (/sys_properties_list.do)
Instance Security Center での構成	あり
目的	ServiceNow の従業員が、保護された IP 範囲を介してのみインスタンスにアクセスできるようにすること
推奨値	true

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

属性	説明
機能への影響度	(低) このプロパティが有効になっていない場合、ServiceNow の従業員はすべての IP 範囲を介して顧客のインスタンスにアクセスできます。このプロパティを有効にすると、アクセスが保護された IP 範囲 (セキュア VPN、DC) セットに制限されます。 **注:** このプロパティを true に設定すると、Now Platform は、インスタンスにアクセスできる IP 範囲セットに対して、パフォーマンス監視 IP 制限 (*glide.ip.authenticate.allow.secured*) プロパティの代わりに、より制限の強い *glide.ip.authenticate.allow.secured* プロパティを使用します。
セキュリティリスク	(低) より幅広いユーザーグループに対してインスタンスアクセスが不必要に公開されます。
参照	IP 範囲ベースの認証

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

注: IP アクセス制御に追加されていない IP からのアクセスをすべて制限するには、「すべて拒否」ルールを IP アクセス制御に追加する必要があります。その後、必要な許可された IP をすべて IP アクセス制御に追加する必要があります。

アンロード要求承認 (インスタンスセキュリティ強化)

glide.basicauth.required.unl (useUnloadFormat) プロパティを使用して、受信アンロード要求で基本認証を要求するかどうかを指定します。

詳細情報

属性	説明
プロパティ名	glide.basicauth.required.unl
構成タイプ	システムプロパティ (/sys_properties_list.do)
Instance Security Center での構成	あり
目的	アンロード要求に対して基本認証を適用すること
推奨値	true
機能への影響度	(中) この修正では、基本認証とシステムレベルのアクセス制御の形で、認証方法の組み合わせが適用されます。インスタンス上でアンロードデータの形式でテーブル/ページからデータを取得する際に、この認証を実行します。
セキュリティリスク	(高) データソースのアンロード要求で適切な承認が構成されていない場合、無許可のユーザーがターゲットインスタンスの機密コンテンツ/データにアクセスする可能性があります。
参照	認証

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

WSDL 要求承認 (インスタンスセキュリティ強化)

glide.basicauth.required.wsdl プロパティを使用して、受信 WSDL (Web Services Description Language) 要求で基本認証を要求するかどうかを指定します。

注:
受信 WSDL 要求に基本認証を要求しないという選択をする場合は、アクセス制御 (ACL) ルールを変更してゲストユーザーが WSDL コンテンツにアクセスできるようにする必要があります。

詳細情報

属性	説明
プロパティ名	glide.basicauth.required.wsdl
構成タイプ	システムプロパティ (/sys_properties_list.do)
Instance Security Center での構成	あり
目的	WSDL 要求に対して基本認証を適用すること
推奨値	true
機能への影響度	(低) この修正では、基本認証とシステムレベルのアクセス制御の形で、認証方法の組み合わせが適用されます。 • インスタンス上で WSDL データの形式でテーブル/ページからデータを取得する際に、この認証を実行します。 • 現在このデータにアクセスしているゲストユーザーを制限します。必要であれば、このコンテンツへのアクセスを必要とするユーザーのために、必要なアクセス制御権限を持つ新しいアカウントを作成する場合があります。
セキュリティリスク	(中) WSDL Web サービスで適切な承認が構成されていない場合、無許可のユーザーがターゲットインスタンスの機密 WSDL コンテンツ/データにアクセスする可能性があります。
参照	Web サービスセキュリティ

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

XML 要求承認 (インスタンスセキュリティ強化)

glide.basicauth.required.xml プロパティを使用して、受信 XML 要求で基本認証を要求するかどうかを指定します。

詳細情報

属性	説明
プロパティ名	glide.basicauth.required.xml
構成タイプ	システムプロパティ (/sys_properties_list.do)

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

属性	説明
Instance Security Center での構成	あり
目的	XML 要求に対して基本認証を適用すること
推奨値	true
機能への影響度	(低) この修正では、基本認証とシステムレベルのアクセス制御の形で、認証方法の組み合わせが適用されます。 • インスタンス上で XML データの形式でテーブル/ページからデータを取得する際に、この認証を実行します。 • 現在このデータにアクセスしているゲストユーザーを制限します。必要であれば、このコンテンツへのアクセスを必要とするユーザーのために、必要なアクセス制御権限を持つ新しいアカウントを作成する場合があります。 詳細については、「XML パーサーステップ」を参照してください。
セキュリティリスク	(中) 受信 XML 要求で適切な承認が構成されていない場合、無許可のユーザーがターゲットインスタンスの機密コンテンツ/データにアクセスする可能性があります。
参照	認証

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

XSD 要求承認 (インスタンスセキュリティ強化)

glide.basicauth.required.xsd プロパティを使用して、受信 XSD (XML Schema Definition) 要求で基本認証を要求するかどうかを指定します。

詳細情報

属性	説明
プロパティ名	glide.basicauth.required.xsd
構成タイプ	システムプロパティ (/sys_properties_list.do)
Instance Security Center での構成	あり
目的	XSD 要求に対して基本認証を適用すること
推奨値	true
機能への影響度	(低) この修正では、基本認証とシステムレベルのアクセス制御の形で、認証方法の組み合わせが適用されます。 • インスタンス上で XSD データの形式でテーブル/ページからデータを取得する際に、この認証を実行します。 • 現在このデータにアクセスしているゲストユーザーを制限します。必要であれば、このコンテンツへのアクセスを必要とするユーザーのために、必要なアクセス制御権限を持つ新しいアカウントを作成する場合があります。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

属性	説明
	詳細については、「非インタラクティブセッション」を参照してください。
セキュリティリスク	(中) 受信 XSD 要求で適切な承認が構成されていない場合、無許可のユーザーがターゲットインスタンスの機密コンテンツ/データにアクセスする可能性があります。
参照	認証

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

添付ファイル (インスタンスセキュリティ強化)

Now Platform ビジネスプロセスの多くでは、データ/情報のアップロードが可能です。テキストの有効性とセキュリティは定期的にチェックされますが、これらのファイルを受け入れるとさらにリスクが生じます。

リスクを軽減するには、悪意のあるファイルを検証して、これらのファイルを送信する攻撃者から Now Platform が正しく保護できるようにする必要があります。これらのファイルを処理するには、アップロードプロセス中にファイルをスキャンし、悪意があると認められるファイルを却下するビジネスロジックを含めます。

内部参照

- 添付ファイルの管理
- 添付ファイルのシステムプロパティの構成

ダウンロード可能な **MIME** タイプ (インスタンスセキュリティ強化)

glide.ui.attachment.download_mime_types プロパティを使用して、添付ファイルの MIME タイプをカンマ区切りリストに指定します。MIME タイプはダウンロードする必要があるものの、ブラウザーにインラインでレンダリングされません。

既存の MIME タイプのリストを表示するには、「/sys_attachment_icon_rule_list.do」と入力します。これらの MIME タイプのいずれかを有効にして、Now Platform 内のセキュリティコンプライアンス要件を満たすことができます。

> **注:**
> **[MIME** タイプのダウンロードを強制する] プロパティを **true** に設定すると、これは [ダウンロード可能な **MIME** タイプ] プロパティ (ダウンロード可能な MIME タイプをカンマで区切ったリスト) より優先されます。詳細については、「MIME タイプのダウンロードを強制する」を参照してください。

詳細情報

属性	説明
プロパティ名	glide.ui.attachment.download_mime_types
構成タイプ	システムプロパティ (/sys_properties_list.do)
Instance Security Center での構成	あり
目的	ファイルタイプがブラウザーでレンダリングされないように制限し、悪意のあるスクリプトの実行を回避すること

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

属性	説明
推奨値	いくつかの定義されたファイルタイプ (text/html、text/csv など)。
機能への影響度	(低) この修正では、Now Platform アプリケーションで添付ファイルをクリックしたときに、アクションを実行する前に検証チェックを適用します。潜在的な影響はありませんが、ユーザーエクスペリエンスが変わります。
セキュリティリスク	(中) クライアント側のスクリプティング攻撃ベクトルにはさまざまな種類があり、MIME タイプの添付ファイルの悪用も例外ではありません。 攻撃者は MIME タイプを悪用し、意図しないスクリプトコンテンツを被害者側の添付ファイルに配置して機密情報を取得することができます。現在のコンテキストでは、添付ファイル MIME タイプの中でブラウザーでインラインレンダリングしてはいけないものを、カンマ区切りのリストの形式でプロパティに入力します。 例：text/html

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

添付ファイルの拒否リストの有効化 (インスタンスセキュリティ強化)

glide.security.attachment_type.use_blacklist プロパティを使用して、Now Platform が指定された除外リストに対して添付ファイルを検証するかどうかを指定します。

> **注:**
> *glide.attachment.blacklisted.extensions* および *glide.attachment.blacklisted.types* プロパティを設定するまで、*glide.security.attachment_type.use_blacklist* プロパティを true に設定しないでください。詳細については、「拒否される拡張を指定する」と「拒否されるファイルタイプを指定する」を参照してください。

詳細情報

属性	説明
プロパティ名	glide.security.attachment_type.use_blacklist
構成タイプ	システムプロパティ (/sys_properties_list.do)
Instance Security Center での構成	あり
目的	疑わしいファイル拡張子とファイルタイプ (exe、dll、jar、text/html など) を持つ添付ファイルに対して、アップロード (挿入/書き込み/更新) 操作を制限すること
推奨値	true
機能への影響度	(低) 除外リストのプロパティ (*glide.attachment.blacklisted.extensions* および *glide.attachment.blacklisted.types*) で指定されたファイル拡張子やファイルタイプをアップロードしようとしないかぎり、機能への影響はありません。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

属性	説明
セキュリティリスク	(中) 悪意のあるユーザーは、一般的な実行可能ファイルの拡張子やタイプを使用して、マルウェアに感染した添付ファイルをアップロードできます。
ワークアラウンド	ベースシステムでは、除外リストではなく包含リストを使用して、同じ問題に対処するプロパティを使用できます。詳細については、以下を参照してください。 • ファイル拡張子を制限する • MIME タイプ制限をアップロードする

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

ファイルのダウンロード制限の有効化 (インスタンスセキュリティ強化)

glide.ui.strict_customer_uploaded_static_content プロパティを使用して、ファイルのアップロード機能でアップロードされた場合にダウンロード可能になるファイルタイプを制限できるようにします。

このプロパティを *glide.ui.strict_customer_uploaded_content_types* プロパティとともに使用すると、制限付きダウンロード可能ファイルタイプのカンマ区切りリストが作成されます。詳細については、「ダウンロード可能なファイルタイプ」を参照してください。

詳細情報

属性	説明
プロパティ名	glide.ui.strict_customer_uploaded_static_content
構成タイプ	システムプロパティ (/sys_properties_list.do)
Instance Security Center での構成	なし
目的	アプリケーションからダウンロードできるファイルタイプを確実に安全なものにすること
推奨値	true
機能への影響度	(低) この修正では、*glide.ui.strict_customer_uploaded_content_types* プロパティで指定された値に基づいてファイルのダウンロード制限が適用されます。詳細については、「ダウンロード可能なファイルタイプ」を参照してください。
セキュリティリスク	(中) ファイルのダウンロード制限は、信頼できないユーザー入力ソースに適用する必要があります。

厳格なユーザー画像アップロードの適用 (インスタンスセキュリティ強化)

glide.security.strict.user_image_upload プロパティを使用して、ユーザーレコードでプロファイル画像のアップロード/更新を実行する際のアクセス制御を有効にします。

この設定では、無許可のユーザーが別のユーザーのプロファイルに画像をアップロードする可能性が生じます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- このプロパティを **true** に設定すると、写真をアップロードするときにテーブル ACL が適用され、許可されたユーザーのみが画像をアップロードできるようになります。
- **false** に設定すると、[写真] フィールドへの画像アップロードに ACL は適用されません。

詳細情報

属性	説明
プロパティ名	glide.security.strict.user_image_upload
構成タイプ	システムプロパティ (/sys_properties_list.do)
Instance Security Center での構成	あり
目的	ユーザー画像のアップロードを許可されたユーザーのみに制限すること
推奨値	true
機能への影響度	(低) 承認されたユーザーは引き続きユーザープロファイルに画像をアップロードできるため、機能への影響はありません。
セキュリティリスク	(中) このプロパティを **false** に設定すると、認証されたユーザーは別のユーザーのアカウントに承認なしで画像をアップロードできます。

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

MIME タイプの強制ダウンロード (インスタンスセキュリティ強化)

glide.ui.attachment.force_download_all_mime_types プロパティを使用して、すべての MIME タイプの添付ファイルを強制的にダウンロードします。

> **注:**
> **[MIME** タイプのダウンロードを強制する] プロパティを **true** に設定すると、これは [ダウンロード可能な **MIME** タイプ] プロパティ (ダウンロード可能な MIME タイプをカンマで区切ったリスト) より優先されます。詳細については、「ダウンロード可能な MIME タイプ」を参照してください。

詳細情報

属性	説明
プロパティ名	glide.ui.attachment.force_download_all_mime_types
構成タイプ	システムプロパティ (/sys_properties_list.do)
Instance Security Center での構成	なし
目的	すべての添付ファイルを、ブラウザーで実行せず強制的にダウンロードすること
推奨値	true
機能への影響度	(中) この修正では、すべての添付ファイルのダウンロードが強制されます。機能に影響はありませんが、ユーザーエクスペリエンスが変わります。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

属性	説明
セキュリティリスク	(高) クライアント側のスクリプティング攻撃を減らすには、添付ファイルをブラウザーコンテキストでレンダリングするのではなく、強制的にダウンロードする必要があります。
参照	利用可能なシステムプロパティ

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

ファイル拡張子の制限 (インスタンス セキュリティ強化)

glide.attachment.extensions システムプロパティを使用して、インスタンスにアップロードできるファイルタイプを定義します。このプロパティは、許可されたファイル拡張子タイプのカンマ区切りリストを使用します。指定されたファイル拡張子タイプのみが添付ファイルとしてアップロードされます。

インスタンスで *glide.attachment.extensions* プロパティを使用すると、次のようなメリットがあります。

セキュリティの強化

このプロパティを使用すると、ユーザーがウイルスなどの有害なファイルを添付ファイルとしてアップロードできないようにして、セキュリティを強化できます。通常は実行可能プログラムやスクリプトで使用されるタイプをブロックすることで、インスタンスを保護します。

互換性のないファイルタイプを避ける

このプロパティを使用して、ユーザーが互換性のないファイルをアップロードしないようにします。たとえば、ブラウザーの中には PNG 形式のアイコンをサポートしないものがあります。png ファイル拡張子を除外すると、ユーザーは PNG ファイルをアップロードできなくなります。

重要:
このプロパティは、実際のファイルタイプ (MIME タイプ) に基づいてファイルを制限するのではなく、拡張子に基づいてのみファイルを制限します。MIME タイプに基づいてアップロードを制限するには、*glide.attachment.extensions* プロパティの設定が完了した後に *glide.security.file.mime_type.validation* プロパティを設定します。*glide.security.file.mime_type.validation* の設定の詳細については、「MIME タイプのアップロード制限」を参照してください。

設定手順

1. インスタンスのフィルターナビゲーターで「sys_properties.list」と入力し、Enter キーを押します。
2. *glide.attachment.extensions* プロパティを検索して開きます。
3. [値] フィールドに、添付ファイルとしてアップロードを許可するファイル拡張子を入力します。フィールド内の複数のエントリはカンマで区切ります。複数のエントリの値の例は *doc,docx,xls,xlxs,pdf,jpeg,jpg,png,ico* です。

   注:
   [値] フィールドにファイルタイプが指定されていない場合は、どのファイルタイプでも添付ファイルとしてアップロードできます。

4. [更新] をクリックして変更を保存します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

詳細情報

属性	説明
プロパティ名	glide.attachment.extensions
構成タイプ	システムプロパティ (/sys_properties_list.do)
Instance Security Center で構成可能	なし
目的	ファイル添付時に許容可能なファイル拡張子のみがアップロードされるようにすること悪意がある可能性がある拡張子のアップロードをブロックします。
推奨値	定義されたファイル拡張子 (doc、docx、pdf、xls、xlsx など)
機能への影響度	(中) この修正により、包含リスト内の拡張子を除くすべてのファイル拡張子が制限されます。組織で許容される拡張子以外のファイルをアップロードしようとする場合を除き、機能への影響はありません。
セキュリティリスク	(中) MIME タイプの検証はこのプロパティに依存するため、悪意のあるファイルのアップロードに関連する脆弱性を軽減することをお勧めします。

添付ファイルへの非認証アクセスの制限 (インスタンスセキュリティ強化)

glide.image_provider.security_enabled プロパティを使用して画像のセキュリティ設定を制御します。**true** に設定すると、認証および承認されたユーザーにのみ画像が表示されます。**false** に設定すると、添付ファイルへの URL を持つすべてのユーザーに画像が表示されます。

詳細情報

属性	説明
プロパティ名	glide.image_provider.security_enabled
構成タイプ	システムプロパティ (/sys_properties_list.do)
Instance Security Center での構成	あり
目的	.iix 形式を使用してレンダリングされた添付ファイルへの非認証アクセスを防止すること
推奨値	true
機能への影響度	(低) 機能に大きな影響はありません。以前に .iix に直接アクセスしていたユーザーは認証を受ける必要があるため、ユーザーエクスペリエンスに多少影響する可能性があります。
セキュリティリスク	(高) 一部の添付ファイルに機密情報が含まれている可能性があるため、非認証ユーザーには制限を適用する必要があります。
参照	添付ファイルの管理 利用可能なシステムプロパティ

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

除外する添付ファイルの拡張子の指定 (インスタンスセキュリティ強化)

Now Platform で除外リストの検証を有効にする場合は、*glide.attachment.blacklisted.extensions* プロパティを使用して、アップロード可能なファイル拡張子のタイプを制限するカンマ区切りリストを作成します。指定されたファイル拡張子のタイプのアップロードは制限されます。

必須条件

glide.security.attachment_type.use_blacklist プロパティを true に設定する前に、このプロパティを設定します。詳細については、「添付ファイルのブラックリストを有効にする」を参照してください。

詳細情報

属性	説明
プロパティ名	glide.attachment.blacklisted.extensions
構成タイプ	システムプロパティ (/sys_properties_list.do)
Instance Security Center での構成	あり
目的	疑わしいファイル拡張子を持つ添付ファイルに対して、アップロード (挿入/書き込み/更新) 操作を制限すること
タイプ	文字列
推奨値	ユーザー指定のファイル拡張子。一般的な例としては、ex、dll、xslx などがあります。
機能への影響度	(低) このプロパティで指定された拡張子のファイルをアップロードしようとしないかぎり、機能への影響はありません。
セキュリティリスク	(中) 悪意のあるユーザーは、一般的な実行可能ファイルの拡張子を使用して、マルウェアに感染した添付ファイルをアップロードできます。
ワークアラウンド	除外リストではなく包含リストで同じ問題に対処するベースシステム機能で、プロパティを使用できます。詳細については、以下を参照してください。 • ファイル拡張子を制限する • MIME タイプのアップロード制限

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

除外する添付ファイルのタイプの指定 (インスタンスセキュリティ強化)

Now Platform で除外リストの検証を有効にする場合は、*glide.attachment.blacklisted.types* プロパティを使用して、アップロード可能なファイルタイプを制限するカンマ区切りリストを作成します。指定されたファイルタイプのアップロードは制限されます。

必須条件

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

glide.security.attachment_type.use_blacklist プロパティを true に設定する前に、このプロパティを設定します。詳細については、「添付ファイルのブラックリストを有効にする」を参照してください。

詳細情報

属性	説明
プロパティ名	glide.attachment.blacklisted.types
構成タイプ	システムプロパティ (/sys_properties_list.do)
Instance Security Center での構成	あり
目的	疑わしいファイルタイプの添付ファイルに対して、アップロード (挿入/書き込み/更新) 操作を制限すること。例：text/html。
推奨値	いくつかの定義されたファイルタイプ (text/html、text/csv など)。
機能への影響度	(低) このプロパティで指定されたタイプのファイルをアップロードしようとしないかぎり、機能への影響はありません。
セキュリティリスク	(中) 悪意のあるユーザーは、一般的な実行可能ファイルタイプを使用して、マルウェアに感染した添付ファイルをアップロードできます。
ワークアラウンド	除外リストではなく包含リストで同じ問題に対処するベースシステム機能で、プロパティを使用できます。詳細については、以下を参照してください。 • ファイル拡張子を制限する • MIME タイプのアップロード制限

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

ダウンロード可能なファイルタイプ (インスタンスセキュリティ強化)

glide.ui.strict_customer_uploaded_content_types プロパティを使用して、制限付きダウンロード可能ファイルタイプのカンマ区切りリストを作成します。インスタンスから静的コンテンツとしてダウンロードできるのは、指定されたファイルタイプに限られます。

詳細情報

属性	説明
プロパティ名	glide.ui.strict_customer_uploaded_content_types
構成タイプ	システムプロパティ (/sys_properties_list.do)
Instance Security Center での構成	あり
目的	ダウンロードできるファイルタイプを、確実に包含リスト内のファイルタイプに限定すること
推奨値	ユーザー指定 (共通：doc、docx、xls、xlsx、pdf など)

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

属性	説明
機能への影響度	(中) 包含リストにあるファイルのみダウンロード可能です。これは組織のポリシーに影響を与える可能性があります。カンマ区切りの包含リストを、許容できるダウンロード可能なファイルタイプに関する組織のポリシーに準拠するように変更する必要があります。
セキュリティリスク	(低) ファイルのダウンロード制限は、信頼できないユーザー入力ソースに適用する必要があります。
参照	セキュリティ設定プロパティ コンテンツタイプ

設定手順

1. 移動先 **/sys_properties_list.do**.
2. *glide.ui.strict_customer_uploaded_content_types* プロパティを検索します。
3. 許容できるダウンロード可能なファイルタイプを、次のようにカンマ区切りリストで指定し、[更新] をクリックします。リストの正しい形式の値の例は *ico,gif,png,jpg,jpeg,bmp,ogg,mp3,doc,docx,xls,pdf* です。

MIME タイプのアップロード制限 (インスタンス セキュリティ強化)

glide.security.file.mime_type.validation プロパティを使用して、アップロードする MIME タイプのチェックをアクティブ化します。添付ファイルの MIME タイプ検証を有効 (プロパティを **true** に設定) または無効 (**false** に設定) にすることができます。

必須条件

このプロパティを設定する前に *glide.attachment.extensions* プロパティを設定してください。*glide.attachment.extensions* で指定された拡張子のみがアップロード時に MIME タイプをチェックされます。詳細については、「ファイル拡張子の制限」を参照してください。

詳細情報

属性	説明
プロパティ名	glide.security.file.mime_type.validation
構成タイプ	システムプロパティ (/sys_properties_list.do)
Instance Security Center での構成	あり
目的	ファイルのアップロード中に MIME タイプ/マジックバイトのチェックを適用すること。
推奨値	true
機能への影響度	(中) この修正により、アプリケーションに対して添付ファイルの MIME タイプの検証が有効になります。この検証は MIME タイプとデータ間の不一致をチェックするだけであるため、ファイルのアップロードに悪意がある場合を除き、機能への影響はありません。
セキュリティリスク	(中) ファイルの包含や悪意があるファイルのアップロードなどの脆弱性を低減するには、MIME タイプ検証を有効にする必要があります。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

属性	説明
参照	添付ファイルの管理

強化のためのプロパティの設定の詳細については、「インスタンスセキュリティ強化設定」を参照してください。

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

メールセキュリティ (インスタンスセキュリティ強化)

このセクションでは、すべての受信メールに対応する適切なセキュリティポリシーを確実に実施するために管理者が構成できるセキュリティコントロールについて解説します。

受信メール **HTML** の変換 (インスタンスセキュリティ強化)

glide.email.inbound.convert_html_inline_attachment_references プロパティを使用して、メール画像がメール HTML 本文のプレビューに表示されるように受信メール HTML を変換するかどうかを指定します。

glide.email.inbound.convert_html_inline_attachment_reference システムプロパティが false に設定されている場合は、次のように動作します。

- Now Platform で、受信した画像の代わりに破損した cid (コンテンツ ID) リンクが表示されます。メール画像の表示形式は、現在のプロパティ設定ではなく、メールを受信した時点でのプロパティ設定によって異なります。
- 添付ファイルで受信した「悪意のある」コンテンツがメールの HTML で参照されません。添付ファイル自体は [sys_attachment] テーブルに保存されます。
- 受信メール処理で、sys_attachment テーブル内の添付ファイルの保存場所を反映してメールの HTML データが更新されません。その結果、次のように動作します。
  - インライン画像がアクティビティフォーマッターのメールに表示されない。

    注:
    アクティビティフォーマッターを使用してこの問題を解決するには、最初にセキュリティ上の懸念がないかどうかを確認してください。次に、*glide.email.inbound.convert_html_inline_attachment_reference* システムプロパティを **true** に設定して、今後受信するメールに、画像の参照に必要な HTML URL を含めるようにしてください。このプロパティを変更しても、既に受信したメールは更新されません。新しい値はプロパティの変更後に受信した受信メールにのみ影響します。

  - メールの HTML プレビューでメールを表示するとインライン画像が表示されない。
  - コードタグ間の受信アクションで email.body_htm を追加すると、画像が欠落する。

必須条件

このプロパティを設定する前に、*glide.email.read.active* プロパティを true に設定します。詳細については、「独自の POP3 サーバーの使用を有効にする」を参照してください。

詳細情報

属性	説明
プロパティ名	glide.email.inbound.convert_html_inline_attachment_references

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

属性	説明
構成タイプ	システムプロパティ (/sys_properties_list.do)
Instance Security Center での構成	あり
目的	HTML 本文のプレビューでの画像のレンダリングを制限すること
推奨値	false
機能への影響度	(中) このプロパティが設定されると、ユーザーはメール本文の画像プレビューを表示できません。
セキュリティリスク	(中) このプロパティが有効になっていない場合、攻撃者はマルウェアを含む悪意のある画像を送信する可能性があります。
参照	メールプロパティ 受信メール設定

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

スパムメールのスコアリングとフィルタリング (インスタンスセキュリティ強化)

Email Filter (*com.glide.email_filter*) プラグインをインストールして、インスタンス内にメールフィルタリングをインストールします。このフィルタリングでは、既存のヘッダーを識別し、関連するヘッダーに基づいてメールの処理方法を決定できます。

Now Platform メールサーバーを介して送信されるメッセージはすべて、スパムメールの可能性について評価されます。

注:
インスタンスがプライベートメールサーバーを使用している場合は、このトピックは適用できません。詳細については、「スパムメールのスコアリングとフィルタリング」を参照してください。

必須条件

このプロパティを設定する前に、次の手順を実行してください。

- *glide.email.read.active* プロパティを true に設定します。詳細については、「独自の POP3 サーバーの使用を有効にする」を参照してください。
- このフィルターは *glide.pop3.ignore_headers* プロパティを上書きします。詳細については、「利用可能なシステムプロパティ」を参照してください。

詳細情報

属性	説明
プラグイン名	com.glide.email_filter
構成タイプ	[システム定義] > [プラグイン]
Instance Security Center での構成	あり
目的	フィルタリングを適用してメールのスパム送信を回避すること

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

属性	説明
推奨値	有効
機能への影響度	(低) スパムスコアリングの一環として、インスタンスからメールがフィルタリング、ブロック、または隔離されることがなくなります。スコアリングのみが行われた後、インスタンスに送信されます。フィルタリングはすべて、Email Filters プラグインを使用して インスタンス内で行われます。
セキュリティリスク	(中) メールフィルターを使用すると、管理者は条件ビルダーまたは条件付きスクリプトを使用して、既知/不明の送信者からの悪意のある受信メールを無視するタイミングを指定できます。
参照	メールフィルター https://support.servicenow.com/kb_view.do?sysparm_article=KB0549426

プラグインのアクティブ化の詳細については、「Activate a plugin」を参照してください。

ターゲットテーブルが空のメールへのアクセスを制限する (インスタンスセキュリティ強化)

glide.email.email_with_no_target_visible_to_all プロパティをアクティブ化して、ユーザーからメールへのアクセスを制限します (メール送信元のユーザーであるか、管理者ロールを持つ場合を除く)。

許可されていないユーザーは、ターゲットレコードのないメール [sys_email] テーブル内のメールにアクセスできます。このプロパティは、メールエントリに ACL を適用するのではなく、メール送信者と admin ロールを持つユーザーのみにアクセスを制限します。

注:
インスタンスによって送受信されたメールは、メール [sys_email] テーブルに表示されます。ただし、[エラー] および [無視] ステータスがマークされた受信メールにかぎり、空のターゲットテーブルを設定する必要があります。

詳細情報

属性	説明
プロパティ名	glide.email.email_with_no_target_visible_to_all
構成タイプ	システムのプロパティ [sys_properties]
Instance Security Center での構成	あり
目的	ユーザーがアクセスを許可しない場合に、メールクライアントでメールが表示されないようにすること
推奨値	false
機能への影響度	(低) ユーザーは、管理者またはメールの送信元でないかぎり、ターゲットテーブルが空のメールを表示できなくなります。
セキュリティリスク	(中) プロパティが有効でない場合、許可されていないユーザーは [target_table] フィールドが空であるメールにアクセスできます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

属性	説明
参照	詳細なメールプロパティ https://support.servicenow.com/kb_view.do?sysparm_article=KB0690043

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

ユーザー作成のためにドメイン別にメールを制限する (インスタンスセキュリティ強化)

glide.user.trusted_domain プロパティを使用して、受信メールからユーザーを作成する際に信頼できるドメインのカンマ区切りリストを指定します。

デフォルトでは、アスタリスク (*) を使用してすべてのドメインを信頼します。すべてのドメインからのメールを許可する必要がない場合は、特定のドメインを指定する必要があります。インスタンスは、既存のユーザーのアドレスからのものでないかぎり、他のドメインからの受信メールを無視します。インスタンスは、信頼できないドメインのメールからゲストユーザーを作成することはありません。

必須条件

このプロパティを設定する前に、次の手順を実行してください。

- *glide.email.read.active* プロパティを true に設定します。詳細については、「独自の POP3 サーバーの使用を有効にする」を参照してください。
- *glide.pop3readerjob.create_caller* プロパティを true に設定します。詳細については、「ユーザーの自動作成の有効化」を参照してください。

> **注:**
> *glide.pop3readerjob.create_caller* プロパティが **false** に設定されている場合は、*glide.user.default_password* プロパティをスキップします。

詳細情報

属性	説明
プロパティ名	glide.user.trusted_domain
構成タイプ	システムプロパティ (/sys_properties_list.do)
Instance Security Center での構成	あり
推奨値	信頼できるドメインのカンマ区切りリスト [例：servicenow.com (特定のドメイン名)]
機能への影響度	(中) このプロパティが設定されると、インスタンスは信頼できるドメインからのメールのみ受け入れます。信頼できるリストにドメインを含めない場合、アカウントが自動的に作成されるため、ゲストユーザーに影響があります。
セキュリティリスク	(中) このプロパティが有効になっていない場合、攻撃者がなりすまし/スパムキャンペーンを使用して複数のメールを送信した結果、不要なゲストユーザーをさらに作成する可能性があります。
参照	メールプロパティ

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

属性	説明
	受信メール設定

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

入力検証 (インスタンスセキュリティ強化)

Now Platform は、誤ったデータの入力によって発生する問題を防ぐために、入力検証を実行します。

ここでは、Now Platform 内部のセキュリティコントロールについて説明します。管理者はこのセキュリティコントロールを設定して、ソースに関係なく不正な形式のデータの入力を最小限に抑えることができます。これらのソースには、ユーザーによる手動入力、またはインフラストラクチャ、外部エンティティ、データベースシステムからの入力があります。

埋め込み **HTML** コードの許可 (インスタンスセキュリティ強化)

glide.ui.security.allow_codetag プロパティを使用して、[code] タグを使用して作成された HTML コードの埋め込みサポートを無効にします。

Now Platform は、エスケープおよびエンコード技術を実装することで、多くのインジェクション攻撃とクロスサイト攻撃を軽減します。その結果、ユーザーはジャーナルフィールドに対して HTML 形式の入力の書き込みや送信ができなくなります。しかしジャーナルフィールドでは、コードタグで囲まれたテキストを HTML としてレンダリングできます。

- ただし、関連するセキュリティリスクがあります。true に設定すると、悪意のあるユーザーは、ジャーナルフィールドをレンダリングした後に、別のクライアントブラウザーで実行できる有害な HTML JS コードを書き込むことができます。
- このプロパティを false に設定すると、[code] タグのサポートを無効にすることで、ジャーナルフィールドで HTML コードがレンダリングされないようにすることができます。

詳細情報

属性	説明
プロパティ名	glide.ui.security.allow_codetag
構成タイプ	システムプロパティ (/sys_properties_list.do)
Instance Security Center での構成	あり
目的	クロスサイトスクリプティングと悪意のあるスクリプトの実行からの保護
推奨値	false
機能への影響度	(中) この修正では、UI で強制的に HTML エンコードが行われ、エンコードされた結果がユーザーに対してレンダリングされます。 このプロパティはデフォルトで [true] に設定されています。このステータスでは、インスタンスはジャーナルフィールドとフォームにレンダリングされた HTML を表示します。 このプロパティを falseに設定すると、HTML が正しくレンダリングされず、フォームのジャーナルフィールドに HTML タグが表示される場合があります。これは、機能に

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

属性	説明
	悪影響を及ぼし、結果のデータを用いたユーザーインタラクションに悪影響を与える可能性があります。
セキュリティリスク	(中) クロスサイトスクリプティング攻撃から防御するために、アプリケーションで入力検証を行う必要があります。これらの攻撃により、ログインしているブラウザーのコンテキストで、ユーザーセッションで外部スクリプトが実行される可能性があります。攻撃者はこれを使用してセッション情報と機密データを盗むことができます。
参照	ジャーナルフィールドの CODE タグを制限する ジャーナルフィールドエントリを HTML としてレンダリングする 高セキュリティ設定

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

埋め込み **HTML** での **JavaScript** タグの許可 (インスタンスセキュリティ強化)

`glide.ui.security.codetag.allow_script` プロパティは、[code] タグを使用して作成された HTML JavaScript コードの埋め込みサポートを無効にします。

> **注:**
> Vancouver 以降のリリースでは、このプロパティはデフォルトで **true** に設定されており、管理者が変更することはできません。プロパティを変更する必要があるユースケースについては、カスタマーサポートにお問い合わせください。

Now Platform は、エスケープおよびエンコード技術を実装することで、多くのインジェクション攻撃とクロスサイト攻撃を軽減します。その結果、ユーザーはジャーナルフィールドに対して HTML 形式の入力を書き込んで送信することができなくなります。しかしジャーナルフィールドでは、コードタグで囲まれたテキストを HTML としてレンダリングできます。

- ただし、関連するセキュリティリスクがあります。**true** に設定すると、悪意のあるユーザーは、ジャーナルフィールドをレンダリングした後に、別のクライアントブラウザーで実行できる有害な HTML JavaScript コードを書き込むことができます。
- このプロパティを **false** に設定すると、`[code]` タグのサポートを無効にすることで、ジャーナルフィールドで HTML JavaScript コードがレンダリングされないようにすることができます。

詳細情報

属性	説明
プロパティ名	glide.ui.security.codetag.allow_script
構成タイプ	システムプロパティ (/sys_properties_list.do)
Instance Security Center での構成	あり
目的	クロスサイトスクリプティングと悪意のあるスクリプトの実行からの保護
推奨値	false

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

属性	説明
機能への影響度	(中) この修正では、UI で強制的に JavaScript エスケープが行われ、エンコードされた結果がユーザーに対してレンダリングされます。これは、結果のデータを用いたインスタンスのユーザーインタラクションに基づいて、機能に影響を与える可能性があります。
セキュリティリスク	(高) クロスサイトスクリプティング攻撃から防御するために、アプリケーションで入力検証を行う必要があります。これらの攻撃により、ログインしているブラウザーのコンテキストで、ユーザーセッションで外部スクリプトが実行される可能性があります。攻撃者はこれを使用してセッション情報と機密データを盗むことができます。
参照	ジャーナルフィールドの CODE タグを制限する ジャーナルフィールドエントリを HTML としてレンダリングする 高セキュリティ設定

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

サニタイズされていない **HTML** の確認 (インスタンスセキュリティ強化)

com.glide.security.check_unsanitized_html プロパティを使用して、フィールドアサインのためにグローバルレベルで translated_html フィールドのサニタイズ動作を適用します。

HTML は、辞書フィールドに割り当てることができるタイプの一種です。HTML フィールドを任意のフィールドタイプに割り当てると、HTML タグ (<p>、<a href>、<b>、<font>、<img> など) を使用してコンテンツをフォーマットできるようになります。悪意のあるアクティビティを防ぐために、ブロックリストを使用して特定の HTML タグを禁止することができます。このプロパティは、インスタンスの translated_html フィールドで禁止タグが使用されないようにします。

- このプロパティを **enforce** に設定すると、translated_html フィールドのサニタイズ動作が適用されます。
- プロパティを **disable** に設定すると、html のサニタイズがオフになり、translated_html フィールドでブロックされた html タグが許可されます。

詳細情報

属性	説明
プロパティ名	com.glide.security.check_unsanitized_html
構成タイプ	システムプロパティ (/sys_properties_list.do)
Instance Security Center での構成	あり
目的	クロスサイトスクリプティングなどの攻撃から保護するために、安全でない HTML タグの使用を防止すること
タイプ	文字列
推奨値	*enforce*
機能への影響度	(中) この修正では、UI で強制的に HTML サニタイズが行われ、翻訳された html フィールドがユーザーに対してレ

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

属性	説明
	ンダリングされます。読みやすさと書式設定に影響を与える可能性があります。
セキュリティリスク	(高) クロスサイトスクリプティング攻撃から防御するために、アプリケーションで入力検証を行う必要があります。これらの攻撃により、ログインしているブラウザーのコンテキストで、ユーザーセッションで外部スクリプトが実行される可能性があります。攻撃者はこれを使用してセッション情報と機密データを盗むことができます。
参照	HTML サニタイザー

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

クライアント生成スクリプトサンドボックス (インスタンスセキュリティ強化)

glide.script.use.sandbox プロパティを使用して、スクリプトサンドボックスを有効にします。

Now Platform には、クライアントが評価のためにサーバーにスクリプトを送信できるケースが 2 つあります。

フィルターまたはクエリー

: assigned_to=JavaScript:getMyGroups() などのフィルターをサーバーに送信することは合法です。

システム API

: API 呼び出しにより、クライアントはサーバー上で任意のスクリプトを実行して、応答を受信することができます。

スクリプトサンドボックスを有効にすると、これらの 2 つのエントリポイントのいずれかで評価されるスクリプトが、次の特性を持つ権限の低いサンドボックス内で実行されます。

- サンドボックス内では、クライアントコール可能とマークされたビジネスルールのみを使用できます。
- サンドボックス内では、クライアントコール可能とマークされたスクリプトインクルードのみ使用できます。
- 特定の API 呼び出し (直接 DB アクセスを扱うものに概ね限定) は許可されていません。
- サンドボックス内部からデータを挿入、更新、または削除することはできません。たとえば、current.update() の呼び出しはすべて無視されます。スクリプトサンドボックスを有効にせずに Now Platform を実行する場合、これらの制限は適用されません。

詳細情報

属性	説明
プロパティ名	glide.script.use.sandbox
構成タイプ	システムプロパティ (/sys_properties_list.do)
Instance Security Center での構成	あり
目的	プラットフォームに対して起動されるクライアント側 JavaScript クエリーの検証を適用すること
推奨値	true

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

属性	説明
機能への影響度	(高) この修正では、Now Platform に対して起動されるクライアント側 JavaScript クエリーの検証が適用されます。顧客が CRUD 操作を実行するためにハードコードされた JavaScript クエリーを組み込んだカスタマイズを行っている場合、潜在的な影響があります。
セキュリティリスク	(高) Now Platform は JavaScript クエリーを介してさまざまな機能を提供します。ただし、適切な承認と検証がないと、攻撃者がプラットフォームに対して不正な操作を実行する可能性があります。
参照	スクリプトサンドボックスプロパティの構成 *glide.script.use.sandbox* は、クライアントからのスクリプトの実行を保護および制限するプロパティと同じファミリーに属します。 • *glide.script.allow.ajaxevaluate*：「AJAXEvaluate を有効にする」を参照 • *glide.script.secure.ajaxgliderecord*：「AJAXGlideRecord ACL チェックの有効化」を参照

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

AJAXEvaluate の有効化 (インスタンスセキュリティ強化)

glide.script.allow.ajaxevaluate プロパティを使用して、サーバー側のシステム API による任意のクライアントスクリプトの実行を制限します。

Now Platform には、クライアントが評価のためにサーバーにスクリプトを送信できるケースが 2 つあります。

フィルター および/またはクエリー

assigned_to=javascript:getMyGroups() などのフィルターをサーバーに送信することは合法です。

システム API

AJAXEvaluate API 呼び出しにより、クライアントはサーバー上で任意のスクリプトを実行して、応答を受信することができます。

このプロパティを **false** に設定すると、Now Platform ではクライアントスクリプトからの AJAXEvaluate API 呼び出しを使用できません。

詳細情報

属性	説明
プロパティ名	glide.script.allow.ajaxevaluate
構成タイプ	システムプロパティ (/sys_properties_list.do)
Instance Security Center での構成	あり
目的	サーバー側のシステム API を使用して、任意のクライアントスクリプトの実行を制限すること
推奨値	false

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

属性	説明
機能への影響度	(中) この修正では、AJAEvaluate プロセッサーが強制的にオフになります。カスタマイズされたスクリプトの一部として AJAX 評価プロセッサーを明示的に使用している場合は、機能に影響を与える可能性があります。 詳細については、「GlideAjax」を参照してください。
セキュリティリスク	(高) AJAXEvaluate は、サーバー側のオブジェクトを適用することで、クライアントブラウザーで任意の JavaScript コードを実行できるようにします。
参照	スクリプトサンドボックスプロパティの構成 GlideAjax *glide.script.allow.ajaxevaluate* は、クライアントからのスクリプトの実行を保護および制限するプロパティと同じファミリーに属します。 • *glide.script.use.sandbox*：「クライアント生成スクリプトサンドボックス」を参照 • *glide.script.secure.ajaxgliderecord*：「AJAXGlideRecord ACL チェックの有効化」を参照

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

Excel 式のエスケープ (インスタンスセキュリティ強化)

glide.export.escape_formulas プロパティを使用して、Excel のインジェクション (式のインジェクションとも呼ばれる) を防止します。

Excel インジェクションは、Web サイトが Excel ファイル内に信頼できないエントリを埋め込むときに発生します。Microsoft Excel や LibreOffice Call などのスプレッドシートアプリケーションを使用してファイルを開くと、+、-、=、または @ で始まるセルは式として解釈されます。*glide.export.escape_formulas* プロパティを **true** に設定すると、CSV、XLS、または XLSX ファイルにエクスポートする際に、+、-、=、または @ で始まる文字列の値には、先頭にアポストロフィが 1 つ追加されます。

詳細情報

属性	説明
プロパティ名	glide.export.escape_formulas
構成タイプ	システムプロパティ (/sys_properties_list.do)
Instance Security Center での構成	あり
目的	アプリケーションで Excel インジェクションまたは式のインジェクションを防止すること
推奨値	true
機能への影響度	(低) 悪意で細工された式を使用すると、スプレッドシートソフトウェアの脆弱性を利用してユーザーのコンピューターをハイジャックすることができます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

属性	説明
セキュリティリスク	(中) 悪意のある式は、閲覧者のコンピューターの侵害に使用される可能性があるため、埋め込みスプレッドシートに機密情報が含まれていない場合であってもリスクを引き起こします。
ワークアラウンド	代替手段として、可能な場合はすべての末尾の空白を削除し、クライアントが提供するすべてのデータを英数字のみに制限することを検討してください。
参照	利用可能なシステムプロパティ

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

HTML のエスケープ (インスタンスセキュリティ強化)

glide.ui.escape_html_list_field プロパティを使用して、リストビューの HTML フィールドで強制的に HTML をエスケープします。

HTML は、辞書フィールドに割り当てることができるタイプの一種です。HTML フィールドを任意のフィールドタイプに割り当てると、HTML コード (<p>、<a href>、<b>、<font>、<img> など) を使用してコンテンツをフォーマットできるようになります。悪意のあるユーザーは、フォームフィールド内に HTML コードを挿入して、さまざまなクライアント/ユーザーセッションで不要なスクリプトを実行できます。

- このプロパティを **true** に設定すると、テーブルがリストビューとして表示されるときに、レコード/フィールドがブラウザーでレンダリングされる前に HTML エスケープが実行されます。
- **false** に設定し、テーブルまたはレコードリストを表示しているときにリストビューでその列を選択すると、これらの HTML 形式のフィールドが表示される場合があります。

詳細情報

属性	説明
プロパティ名	glide.ui.escape_html_list_field
構成タイプ	システムプロパティ (/sys_properties_list.do)
Instance Security Center での構成	あり
目的	アプリケーションでクロスサイトスクリプティング攻撃を防ぐこと
推奨値	true
機能への影響度	(中) この修正では、UI で強制的に HTML パーサーレベルの HTML エンコードが行われ、エンコードされた結果がユーザーに対してレンダリングされます。これは、結果のデータを用いたインスタンスのユーザーインタラクションに基づいて、機能に影響を与える可能性があります。
セキュリティリスク	(高) クロスサイトスクリプティング攻撃から防御するために、アプリケーションで入力検証を行う必要があります。これらの攻撃により、ログインしているブラウザーのコンテキストで、ユーザーセッションで外部スクリプトが実行される可能性があります。攻撃者はこれを使用してセッション情報と機密データを盗むことができます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

属性	説明
参照	高セキュリティ設定

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

JavaScript のエスケープ (インスタンスセキュリティ強化)

glide.html.escape_script プロパティを使用して、リストビュー中に HTML フィールドの JavaScript (<script></script>) タグからのエスケープを適用します。

HTML は、辞書フィールドに割り当てることができるタイプの一種です。HTML フィールドを任意のフィールドタイプに割り当てると、ユーザーは HTML コード (<p>、<a href>、<b>、<font>、<img> など) を使用してコンテンツをフォーマットできるようになります。*glide.html.escape_script* を **false** に設定すると、テーブルまたはレコードリストを表示しているときにリストビューでその列を選択すると、(<script></script>) タグが表示される場合があります。

悪意のある攻撃者は、(<script></script>) タグ内に JavaScript コードを埋め込んで挿入できます。攻撃者は、ユーザーがテーブルレコードを開いたときに実行される可能性のある高度な JS ベクトルを挿入して利用することができます。

詳細情報

属性	説明
プロパティ名	glide.html.escape_script
構成タイプ	システムプロパティ (/sys_properties_list.do)
Instance Security Center での構成	あり
目的	アプリケーションに対するクロスサイトスクリプティング攻撃を防ぐこと
推奨値	true
機能への影響度	(中) この修正では、UI で強制的に JavaScript エスケープが行われ、エンコードされた結果がユーザーに対してレンダリングされます。これは、結果のデータを用いたインスタンスのユーザーインタラクションに基づいて、機能に影響を与える可能性があります。
セキュリティリスク	(高) クロスサイトスクリプティング攻撃から防御するために、アプリケーションで入力検証を行う必要があります。これらの攻撃により、ログインしているブラウザーのコンテキストで、ユーザーセッションで外部スクリプトが実行される可能性があります。攻撃者はこれを使用してセッション情報と機密データを盗むことができます。
参照	利用可能なシステムプロパティ 高セキュリティ設定

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Jelly のエスケープ (インスタンスセキュリティ強化)

glide.ui.escape_all_script プロパティを使用して、Jelly に挿入されたすべてのスクリプトを強制的にエスケープします。

これは、<j:jelly> ... </j:jelly> に含まれるすべての JS および HTML 文字列を、出力ストリームに書き込まれる前にエスケープして、いくつかの XSS 問題が発生しないようにします。

詳細情報

属性	説明
プロパティ名	glide.ui.escape_all_script
構成タイプ	システムプロパティ (/sys_properties_list.do)
Instance Security Center での構成	あり
目的	プロパティが **true** に設定されていない場合、開発者は XSS の問題を防ぐために、各カスタム Jelly スクリプトでいくつかの手順を実行する必要があります。これらの手順には、Web ページにレンダリングするために出力ストリームに送信される Jelly 変数の特定と、次の各タグのエスケープが含まれます。 $â {JS:expression} $â {HTML:expression} OR $â {JS,HTML:expression}
推奨値	true
機能への影響度	(中) この修正では、パーサーレベルで Jelly エスケープが適用されます。結果のデータを用いたユーザーインタラクションに機能的な影響を与える可能性があります。
セキュリティリスク	(高) アプリケーションで入力されるすべてのユーザー入力で入力検証を行う必要があります。これにより、プラットフォームに対するインジェクション攻撃を防御および保護できます。
ワークアラウンド	Web ページでのレンダリング用に設計された一部のスクリプトと HTML タグが破損したように見えるため、UI が影響を受ける可能性があります。この修正では、出力エンコードされたページをブラウザーに送信してレンダリングします。 たとえば、<u> タグが適切にエスケープされると、「my string here」ではなく「<u> my string here</u>」と表示されます。この場合、エスケープを防ぐには、NOESC プリフィックスを Jelly 式に追加して JS エスケープを防止します。例： • 変更前：($[jvar_context_menus]); • 変更後：($[NOESC:jvar_context_menus]);

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

属性	説明
	• 変更前：$[jvar_ui_policy_scripts] • 変更後：$[NOESC:jvar_ui_policy_scripts]
参照	高セキュリティ設定 Jelly のタグ

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

XML のエスケープ (インスタンスセキュリティ強化)

glide.ui.escape_text プロパティは、パーサーレベルで XML 値を強制的にエスケープしてから、クライアントのブラウザに送信します。

> **注:**
> Vancouver 以降のリリースでは、このプロパティはデフォルトで **true** に設定されており、管理者が変更することはできません。プロパティを変更する必要があるユースケースについては、カスタマーサポートにお問い合わせください。

クロスサイトスクリプティングは、攻撃者が悪意のある JavaScript をエントリポイントに挿入するときに発生します。プラットフォーム/アプリケーションは、被害者のブラウザに送信して実行する前に悪意のある JavaScript をエスケープすることができません。このコンテキストでのエスケープとは、次のことを意味します。

- **&** --> &
- **<** --> <
- **>** --> >
- **"** --> "
- **'** --> '
- **/** --> /

例:<![CDATA[<script>alert('XSS Attack');]]>

エスケープ：<script>alert('XSS Attack');</script>

詳細情報

属性	説明
プロパティ名	glide.ui.escape_text
構成タイプ	システムプロパティ (/sys_properties_list.do)
Instance Security Center での構成	あり
目的	XML をエスケープすることで、信頼できないデータに埋め込まれた悪意のある JavaScript をブラウザが解析して JavaScript として実行することを確実になくします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

属性	説明
	• 悪意のあるユーザーが XSS 攻撃を試みて、他のユーザーのセッションをハイジャックするか、ユーザーを悪意のある Web サイトにリダイレクトする可能性があります。 • Now Platform には cookie を保護するためのコードが含まれていますが、それをエスケープするにはこのプロパティが **true** に設定されている必要があります。
推奨値	true
機能への影響度	(中) この修正では、UI で XML パーサーレベルの XML エンコードが適用されます。これにより、エンコードされた結果がユーザーに対してレンダリングされるので、結果のデータを用いたインスタンスのユーザーインタラクションに基づいて、機能に影響を与える可能性があります。
セキュリティリスク	(高) クロスサイトスクリプティング攻撃から防御するために、アプリケーションで入力検証を行う必要があります。これらの攻撃により、ログインしているブラウザのコンテキストで、ユーザーセッションで外部スクリプトが実行される可能性があります。攻撃者はこれを使用してセッション情報と機密データを盗むことができます。

ワークアラウンド	このプロパティを **true** に設定すると、カタログアイテムの説明またはカタログアイテム変数のヘルプテキストの HTML タグでレンダリングが停止します。フィールドによっては、HTML 形式を使用できない場合があります。
	
	ただし、*glide.ui.escape_text* プロパティをオフにすると、出力エンコーダーにより、すべての JEXL 式にプリフィックスが付加されます。
	
	`${JS:expression}`
	
	`${HTML:expression}`
	
	または
	
	`${JS,HTML:expression}`

参照	高セキュリティ設定

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

HTML サニタイザー (インスタンスセキュリティ強化)

glide.html.sanitize_all_fields プロパティを使用して、HTMLSainitizer スクリプトインクルードを有効にし、スクリプトで構成された除外リストおよび包含リストの属性に基づいて HTML 入力をサニタイズします。

辞書/フィールドで利用可能なフィールドタイプには、HTML や翻訳された HTML などがあります。これらの HTML 入力フィールドを使用すると、次のような HTML 形式の入力を記述できます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

<h1>Test</h1>)、<img>、<a href …>、<iframe> などの最も基本的な HTML タグを使用

これにより、悪意のある攻撃者が次のような HTML タグを使用して悪意のあるベクトルを挿入する可能性があります。

[<IMG SRC=" &#14; JavaScript:alert('XSS');">][<IMG onmouseover="alert('xss')">],[a href="" onclick=alert(/xss/)]

詳細情報

属性	説明
プロパティ名	niglide.html.sanitize_all_fields
構成タイプ	システムプロパティ (/sys_properties_list.do)
Instance Security Center での構成	あり
目的	アプリケーションでクロスサイトスクリプティング攻撃および HTML インジェクション攻撃を防ぐこと
推奨値	true
機能への影響度	(高) この修正では、ユーザーデータがユーザーにレンダリングされる前に、HTML 出力エンコードメカニズムが適用されます。顧客が HTML 属性またはコンテンツデータのレンダリングを伴うカスタマイズを行っている場合は、機能に影響があります。
セキュリティリスク	(高) データがアプリケーションに格納および処理されるときに、ユーザー入力を安全に処理する必要があります。これにより、データの出力エンコードによるクライアント側のクロスサイトスクリプティング攻撃が低減されます。
ワークアラウンド	このプロパティは、システム内のすべての HTML フィールドをサニタイズします。個々のフィールドで HTML のサニタイズを有効にする必要がある場合は、「個々のフィールドでサニタイズを有効にする」を参照してください。 包含リストまたは除外リストを設定して、組織のポリシーに従って HTML タグと属性をサニタイズすることもできます。
参照	HTML サニタイザーの有効化 HTML サニタイザー

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

Jelly/JS 補間 (インスタンスセキュリティ強化)

glide.ui.jelly.js_interpolation.protect プロパティを使用して、Jelly ページで実行しようとしているすべての JavaScript が Jelly 補間を使用したインジェクションから確実に保護されるようにします。

プロパティを **true** に設定すると、アプリケーションは (ネストされた) Jelly スクリプトツリーを経由します。潜在的に危険な Jelly 式は、次を実行するフィルターでラップされます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

- 結果をエスケープして安全にします。または、
- 安全性を保証できない場合は SecurityException を生成します。これは、評価される予定の式がセキュリティ上の問題を示している可能性があるためです。

詳細情報

属性	説明
プロパティ名	glide.ui.jelly.js_interpolation.protect
構成タイプ	システムプロパティ (/sys_properties_list.do)
Instance Security Center での構成	あり
目的	Jelly インジェクションを使用すると発生する可能性がある、悪意のあるコードの実行攻撃を軽減すること
推奨値	true
機能への影響度	(高) このプロパティは、式が引用符で囲まれているかどうかについて最適な推測を行います。正当な式に誤って引用符を付ける可能性があります。その場合、手動で式に安全とマークする必要がある場合があります。
セキュリティリスク	(中) JEXL インジェクションは、Now Platform に固有の入力インジェクションの形式です。これにより、クロスサイト要求の偽造とコード実行の両方が発生する可能性があります。保護を完全にオフにすると、多くの P1 セキュリティ脆弱性がオープンになるおそれがあります。
ワークアラウンド	手動で式に安全とマークするには、SAFE というプリフィックスを Jelly 式に追加します。 ${SAFE:sysparm_input}; すべての式に機械的に SAFE を追加するという方法は、セキュリティの脆弱性をオープンにするおそれがあるため、問題へのアプローチとしては不適切です。 • 式に SAFE を追加するのは、式にクライアントからの入力が含まれていないことが保証できる場合に限ってください。 • 含まれている場合、悪意のあるクライアントによって特権 JavaScript が評価される可能性があります。
参照	Jelly のタグ 高セキュリティ設定

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

SOAP 要求の厳格なセキュリティ (インスタンスセキュリティ強化)

glide.soap.strict_security プロパティを使用して、Web サービスのセキュリティを適用します。

このプロパティでは、次の組み合わせを使用します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

- HTTP プロトコルを介した基本認証のチャレンジ/応答、および
- Contextual Security: Role Management プラグインのシステムレベルのアクセス制御。

このプロパティを **true** に設定すると、次のアクションが実行されます。

- ユーザーが操作を実行するための適切なロールを持っている場合は、受信 SOAP 要求に検証するロール承認がないかチェックします。これは、作成、読み取り、更新、または削除操作を実行するときに、Now Platform テーブルに対して行われる SOAP Web サービスの呼び出し/要求中に発生します。
- テーブルのデータを SOAP データの形式で取得するときに、システムレベルの ACL をチェックします。
- フィールドレベルの ACL で、テーブルのフィールドに対して実行された CRUD 操作がないかチェックします。

詳細情報

属性	説明
プロパティ名	glide.soap.strict_security
構成タイプ	システムプロパティ (/sys_properties_list.do)
Instance Security Center での構成	あり
目的	SOAP 呼び出しを介してレコードにアクセスする場合でも、セキュリティ ACL が確実にチェックおよび検証されるようにすること
推奨値	true
機能への影響度	(高) この修正では、インスタンスでテーブル/ページからデータを SOAP データの形式で取得する際に、システムレベルのアクセス制御が適用されます。現在このデータにアクセスしているユーザーがいる場合、ACL ルールに基づいてデータへのアクセスが制限/許可されます。 SOAP データにアクセスできるデフォルトのロールについては、「SOAP のロール」を参照してください。
セキュリティリスク	(高) 受信 SOAP 要求で適切な承認が構成されていない場合、無許可のユーザーがターゲットインスタンスの機密コンテンツ/データにアクセスする可能性があります。
参照	受信 SOAP の厳格なセキュリティの適用 SOAP Web サービス

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

セキュアな通信 (インスタンスセキュリティ強化)

セキュアな通信プロパティは、HTTP トラフィックの転送のセキュリティに関連しています。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

証明書の信頼 (インスタンスセキュリティ強化)

デフォルトでは、*com.glide.communications.trustmanager_trust_all* プロパティは **false** に設定されています。Now Platform は、JVM 証明書ストアに対して検証できる証明書のみを信頼します。自己署名証明書およびエンタープライズ署名証明書は信頼されません。

> **注:**
> これらのプロパティの値は 安全なオーバーライド であるため、一度変更すると変えることができなくなります (元に戻すことはできません)。セキュリティ上の理由から、このプロパティ値は変更しないでください。さらに質問がある場合は、カスタマーサービス & サポートにお問い合わせください。

詳細情報

属性	説明
プロパティ名	com.glide.communications.trustmanager_trust_all
構成タイプ	システムプロパティ (/sys_properties_list.do)
Instance Security Center での構成	あり
目的	送信要求の証明書の検証を適用すること
推奨値	false
機能への影響度	(中) この修正では、証明書の CA (認証局) フィールドに厳格な検証が適用されます。信頼できるエンティティ (CA) が証明書を発行した場合、インスタンスはそれを受け入れてその後使用します。
セキュリティリスク	(中) 機密性と完全性の理由から、アプリケーションはどのトランザクション操作に対しても、証明書を使用する前に証明書の CA を検証する必要があります。
参照	証明書 HTTP クライアントホスト名の検証

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

SSLv2/SSLv3 の無効化 (インスタンスセキュリティ強化)

glide.outbound.sslv3.disabled プロパティを設定して、REST 要求や SOAP 要求などの送信接続を行うときに、MID Server が強制的に TLS を使用するようにします。通常は、インスタンスからの送信接続で SSL の代わりに TLS が使用されます。

詳細情報

属性	説明
プロパティ名	glide.outbound.sslv3.disabled
構成タイプ	システムプロパティ (/sys_properties_list.do)
Instance Security Center での構成	あり
目的	ServiceNow インスタンスからのすべての送信接続で TLS の使用を強制すること

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

属性	説明
推奨値	true
機能への影響度	(中) この修正では、HTTPS で通信するときに TLS プロトコルバージョンの使用が強制されます。インスタンスの顧客/ユーザーが TLS 通信をサポートしていないデバイスを使用している場合は、機能停止する可能性があります。
セキュリティリスク	(中) SSL の従来のバージョンは、HTTP セキュアシェル実装に使用した場合、BEAST や SSL ハートブリードなどのクライアント側の攻撃のためにセキュアでないことが確認されています。

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

HTTP クライアントホスト名の検証

com.glide.communications.httpclient.verify_hostname を使用して、リモート SSL ホストによって提示されたホスト名と証明書チェーンを確認します。

com.glide.communications.httpclient.verify_hostname を **true** に設定すると、2 者間の通信がインターセプトされる MitM (中間者) 攻撃から保護されます。このプロパティを設定すると *com.glide.communications.trustmanager_trust_all* プロパティが上書きされます。

詳細情報

属性	説明
プロパティ名	*com.glide.communications.httpclient.verify_hostname*
構成タイプ	システムプロパティ (/sys_properties_list.do)
Instance Security Center での構成	あり
目的	取り消しステータスの確認によって証明書チェーン内のすべての証明書を評価する認定確認プロセスを無効にする。
タイプ	True | False
推奨値	true
機能への影響度	(中) 検証されていない証明書が安全でないホストとして接続できるようになります。
セキュリティリスク	(中) 悪影響を与える可能性のあるホスト名への http クライアントの接続を、例外なく許可または防止します。
参照	証明書 証明書の信頼

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

失効した証明書の検証

このプロパティを使用して、取り消しステータスの確認によって証明書チェーン内のすべての証明書を評価する認定確認プロセスを無効にします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

高セキュリティのプラグインを使用する API 呼び出しで、このプロパティを設定できます。完全な認定チェーンがインスタンスの信頼ストアで定義されていない場合、または使用されている証明書が OCSP (オンライン証明書ステータスプロトコル) の失効チェックと互換性がない場合は、API 呼び出しにエラーが返される可能性があります。

証明書の失効チェックは、プロパティ *com.glide.communications.httpclient.verify_revoked_certificate* を **false** に設定することでオフにできます。

チェックを実行できないことに関連するエラーは、NPE、SSLPeerUnverifiedException、CertPathValidatorException です。これらのエラーは HttpException にラップされている可能性があります。チェックを正常に実行する機能に影響する可能性のある要因としては、次のようなものがあります。

- URI はインスタンスにアクセス可能である必要があります。元の OCSP の実装ではプロキシ接続にアクセスできない可能性があります。
- チェックを行う際は、参照元の OCSP サービスがオンラインである必要があります。

注:
これらのプロパティの値は 安全なオーバーライド であるため、一度変更すると変えることができなくなります (元に戻すことはできません)。さらに質問がある場合は、カスタマーサービス & サポートにお問い合わせください。

詳細情報

属性	説明
プロパティ名	*com.glide.communications.httpclient.verify_revoked_certif*
構成タイプ	システムプロパティ (/sys_properties_list.do)
Instance Security Center での構成	あり
目的	取り消しステータスの確認によって証明書チェーン内のすべての証明書を評価する証明書確認プロセスを無効にする。インスタンスの信頼ストアには自己署名済みサーバー証明書のみをロードする必要があります。
タイプ	True | False
デフォルト値	true
推奨値	true
機能への影響度	(中)
セキュリティリスク	(中) High Security プラグインを使用する API 呼び出しが、インスタンスの信頼ストアでの OCSP 失効チェックで検証されなくなる。
参照	証明書

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

セキュリティのベストプラクティス (インスタンスセキュリティ強化)

セキュリティ構成に加えて、Now Platform アプリケーションの日常的なセキュリティ保護を強化するために、いくつかの手動作業が必要です。このセクションでは、管理者が一定の間隔で定期的に実行する必要があるセキュリティタスクを説明しています。

コンテンツタイプのオプションの自動設定

X-Content-Type-Options 応答 HTTP ヘッダーは、Content-Type ヘッダーで公示される MIME (多目的インターネットメール拡張) タイプに従う必要があることを示すために使用されます。

このヘッダーを設定すると、ブラウザーがファイルを HTTP ヘッダーのコンテンツタイプによって宣言されたもの以外のものとして解釈するのを防ぐことができます。このヘッダーは、MIME 混同攻撃を軽減するのに役立ちます。

glide.security.header.auto_set_x_content_type_options が **true** に設定されていれば、自動設定コンテンツタイプオプションは準拠しています。

詳細情報

属性	説明
プロパティ名	*glide.security.header.auto_set_x_content_type_options*
構成タイプ	システムプロパティ (/sys_properties_list.do)
Instance Security Center での構成	あり
目的	ブラウザーがファイルを HTTP ヘッダーのコンテンツタイプによって宣言されたもの以外のものとして解釈するのを防ぐ。
タイプ	True | False
推奨値	**true**
機能への影響度	(高) このヘッダーは、MIME 混同攻撃を軽減するのに役立ちます。
セキュリティリスク	(高) このプロパティが有効でないと、ブラウザーが HTTP ヘッダーのコンテンツタイプを誤って解釈する可能性があります。
参照	ダウンロード可能な MIME タイプ

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

キャッシュ制御 **HTTP** ヘッダー値 (インスタンスセキュリティ強化)

glide.http.cache_control プロパティを使用して、ページの静的コンテンツデータを要求するときに Now Platform から送信される HTTP 応答ヘッダーのデフォルトのキャッシュ制御値を設定します。静的コンテンツには、たとえばページで内部からレンダリングされる画像、CSS、および JavaScript などがあります。

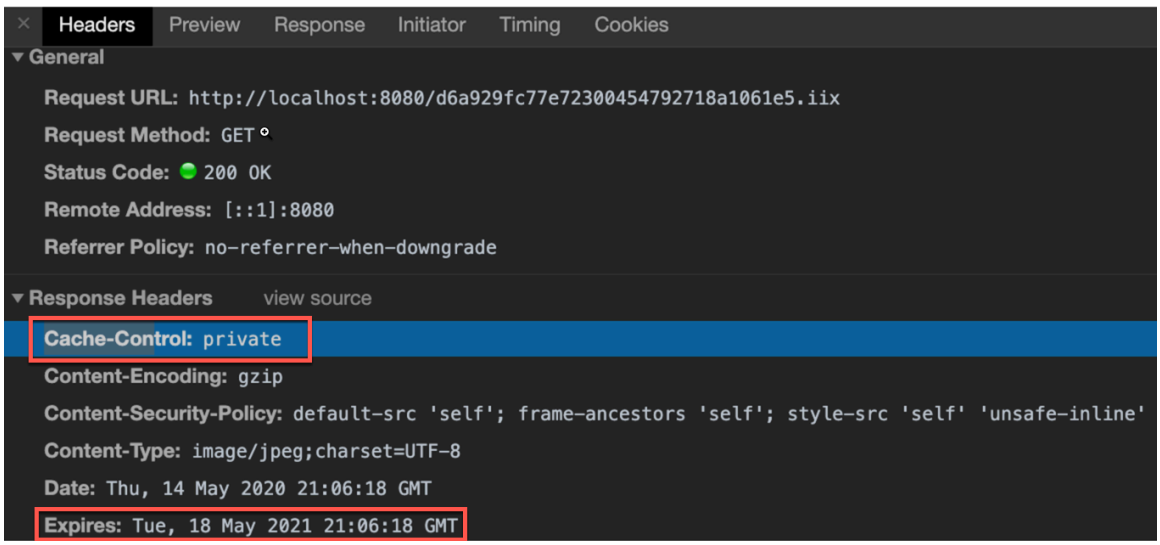
glide.http.cache_control プロパティは、HTTP 応答ヘッダーのデフォルトのキャッシュ制御値を **private** または **public** に設定します。デフォルトは **private** です。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

値	説明
private	静的コンテンツはブラウザー (クライアント) レベルでキャッシュできますが、プロキシサーバーレベルではキャッシュできません。
公開	静的コンテンツはブラウザー (クライアント) レベルでキャッシュでき、またプロキシサーバーレベルでもキャッシュできます。

HTTP 応答ヘッダーの Expires の値は、静的コンテンツの有効期限を制御します。デフォルト値は 369 日です。デフォルト値を手動で上書きするには、*glide.http.expire.days* プロパティを使用します。



注:
glide.http.cache プロパティを使用して、HTTP 応答ヘッダーの Cache-Control と Expires の値の設定を有効にするか無効にするかを指定できます。デフォルトは **true** で、以下の項目を設定できます。

- *glide.http.cache_control* プロパティを使用してデフォルトの Cache-Control (キャッシュ制御) 値を設定可能
- *glide.http.expire.days* プロパティを使用してデフォルトの Expires (有効期限) 値を設定可能

詳細情報

属性	説明
プロパティ名	glide.http.cache_control
構成タイプ	システムプロパティ (/sys_properties_list.do)
Instance Security Center での構成	あり
目的	静的コンテンツのキャッシュ制御 HTTP 応答ヘッダー値を設定すること
推奨値	private

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

属性	説明
機能への影響度	(中) HTTP 応答ヘッダーのデフォルトのキャッシュ制御値を設定します。
セキュリティリスク	(高) このプロパティを **public** に設定すると、CDN/プロキシを備えたインスタンスが静的コンテンツをキャッシュし、認証なしでレンダリングする場合があります。 • **private** は、CDN/プロキシセットアップを使用するインスタンスに適した設定です。 • インスタンスに CDN/プロキシが設定されていない場合は、どちらの値でもかまいません。

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

レポートにセキュリティを強制 (Enforce Security On Reports)

ユーザーがレポートを公開したりアクセスしたりできないようにするには、このプロパティを無効にします。このプロパティによって、レポートの公開レポート機能が無効になります。

glide.report.published_reports.enabled を **true** に設定してレポートの公開を有効にします。

glide.report.published_reports.enabled が **false**に設定されていれば、 レポートへのにセキュリティの強制は準拠しています。

詳細情報

属性	説明
プロパティ名	*glide.report.published_reports.enabled*
構成タイプ	システムプロパティ (/sys_properties_list.do)
Instance Security Center での構成	あり
目的	レポートの公開レポート機能を無効化する。
タイプ	True | False
推奨値	**false**
機能への影響度	(中) ユーザーはレポートを公開できません。
セキュリティリスク	(中) このプロパティが有効でないと、ユーザーがレポートにアクセスしたり公開したりして機密データが公開される可能性があります。レポートを公開して、ユーザー以外の人を含め、誰でもレポートにアクセスできる URL を作成します。誰かがその URL に移動すると、インスタンスから現在のデータでレポートが生成されます。
参照	レポートの公開

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

High Security プラグイン (インスタンスセキュリティ強化)

High Security プラグインをアクティブ化すると、インスタンスのセキュリティレベルを制御する数百もの異なる構成が作成または更新されます。これらの構成は、厳格なアクセス制御、入力検証、および出力エンコーディングを有効にすることで、上位の OWASP 攻撃の多くを軽減します。

これらの設定には次のような内容が含まれます。

- アクセス制御
- ビジネスルール
- システムプロパティ
- UI ポリシーアクション
- スクリプトアクション
- スクリプトインクルード

例

次のプロパティの例を参照してください。

プロパティ	トピック
glide.ui.escape_all_script	Jelly をエスケープする
glide.security.strict.actions	実行前に UI アクションをチェックする
glide.security.csrf_previous.allow	CSRF 対策トークン
glide.security.csrf.strict.validation.mode	CSRF 厳格検証

詳細情報

属性	説明
プラグイン名	com.glide.high_security
構成タイプ	[システム定義] > [プラグイン - 開発]
目的	このプラグインをアクティブ化する必要があります。これにより、インスタンスのセキュリティレベルが向上し、CSRF、XSS、セッション Cookie のセキュリティ保護、ファイルのアップロードなどの owasp 上位 10 件の攻撃が軽減されることで、攻撃対象領域が縮小します。
推奨値	有効
機能への影響度	(高) このプラグインは、UI と機能に影響を与える可能性があるシステムセキュリティ構成をいくつか有効にします。
セキュリティリスク	(高) 多くのセキュリティ設定が意図せずオープンのままになるため、一部の重大な脆弱性が無防備になる可能性があります。
参照	高セキュリティ設定の有効化 高セキュリティ設定

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

プラグインのアクティブ化の詳細については、「Activate a plugin」を参照してください。

個々のログイン ID (インスタンスセキュリティ強化)

すべてのユーザーに個別のユーザー ID があることを確認します。これにより、すべてのユーザーアクティビティの監査が可能になります。

注:
使用されていないローカルユーザーアカウントでは、[アクティブ **(Active)]** フラグを false に設定する必要があります。

- [アクティブ **(Active)]** フラグを **false** に設定すると、[ロックアウト] フラグが自動的に **true** に設定されます。[ロックアウト] フラグが **true** に設定されている場合、そのユーザーアカウントではインスタンスに対する認証が許可されません。
- [アクティブ **(Active)]** フラグを **false** に設定しても、Now Platform からユーザーは削除されませんが、管理者以外のアカウントには表示されなくなります。
- [アクティブ **(Active)]** フラグが **false** に設定され、[ロックアウト] フラグも **false** に設定されている場合でも、ユーザーはこのアカウントにログインできます。

ユーザーアカウントの詳細については、「ユーザー管理」を参照してください。

モバイル UI の難読化 (インスタンスセキュリティ強化)

glide.ui.m.blur_ui_when_backgrounded プロパティを使用して、バックグラウンド処理中に画像を保存する際に、スナップショットのすべてのフィールドを難読化します。

Android デバイスでは、アプリケーションがバックグラウンドに送信されるときに、Android オペレーティングシステムによって最新のタスクメニューで使用されるスクリーンショットが取得されます。ユーザーは、アプリケーションのスクリーンショットを手動で撮影し、公開状態でデバイスに保存することもできます。

iOS デバイスでは、iOS オペレーティングシステムによってアプリケーションで画像ファイルを保存できるようにすることもできます。このファイルは、アプリケーションがバックグラウンドに送信されたときにユーザーが最後に表示した画面です。ユーザーエクスペリエンスを向上させることが目的ですが、画像が PNG 画像ファイルとして保存されるため、セキュリティ上のリスクも生じます。

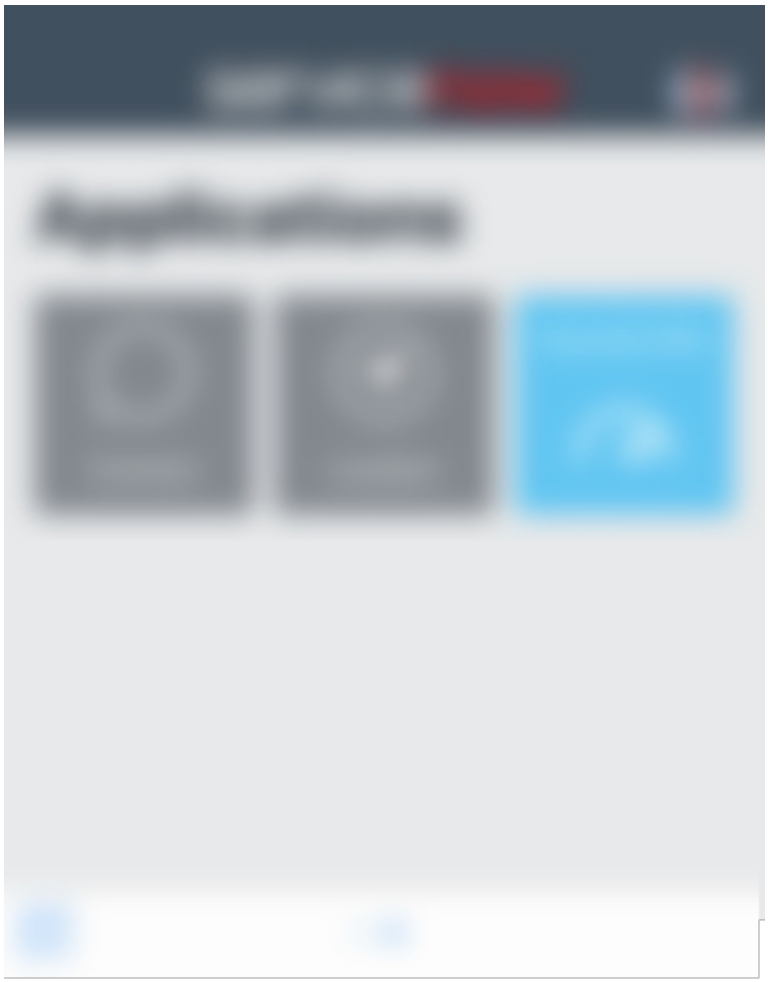
注:
この設定や構成はインスタンス単位で行われるため、ユーザーは プロパティを設定してインスタンスに接続する必要があります。

ServiceNow Classic アプリのスナップショットのフィールドをすべて難読化するには、「セキュリティ向上のためのアプリをぼかすオプションの設定」を参照してください。

例

このプロパティを **true** に設定すると、バックグラウンドアプリケーションは、iOS デバイスでは難読化され、Android iOS デバイスではブラックアウトされます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



詳細情報

属性	説明
プロパティ/プラグイン名	glide.ui.m.blur_ui_when_backgrounded
構成タイプ	システムプロパティ (/sys_properties_list.do)
Instance Security Center で構成可能	いいえ
目的	バックグラウンド処理中に画像を保存する際に、スナップショットのすべてのフィールドを難読化すること
推奨値	true
機能への影響度	(低) *glide.ui.m.blur_ui_when_backgrounded* プロパティが **true** に設定されている場合、ネイティブアプリは、アプリがバックグラウンドに入った時点でサーバーで定義されたパラメーターを使用して画面をぼかします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

属性	説明
	• アプリがバックグラウンドに入ると、iOS と Android で撮影されたスクリーンショットがぼやけて表示されます。 • アプリがバックグラウンドに送信されるとコンテンツが表示されなくなるため、ユーザーエクスペリエンスに悪影響を与える可能性があります。
セキュリティリスク	(中) 侵害された (ジェイルブレイクされた) デバイスは、ファイルシステムへのフルアクセス権を持ち、機密情報が埋め込まれたファイル/スナップショットにアクセスできます。

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

パッチと更新 (インスタンスセキュリティ強化)

インスタンスが最新のパッチレベルを実行していることを確認します。Now Platform のセキュリティ修正は、製品機能の更新に伴う多くのパッチとホットフィックス内で定期的にリリースされます。新しいパッチやホットフィックスが利用可能になったときにアップグレードすると、潜在的な脆弱性のリスクが軽減されます。

Now Platform では、平均で週に 2 回のペネトレーションテストが実施されます。

- これらのテストの大半は重大な脆弱性につながることはありませんが、定期的に脆弱性が発見され、修正されます。
- Now Platform リリース、パッチ、およびホットフィックスに関する情報は、製品ドキュメントの「リリースノート」セクションにあります。詳細については、「アップグレードのリリースノート」を参照してください。

デモデータの削除 (インスタンスセキュリティ強化)

デモデータ (特にデモアカウント) は、通常、インスタンスの作成時点で組み込まれます。その場合は、非本番環境または本番環境でインスタンスを使用する前に、すべてのデモデータを削除する必要があります。

HI で要求を開きます。要求を送信する前に、必ず管理アカウントを作成してください。

本番インスタンスの最新のクローンである準本番インスタンスで、本番環境でのデモデータの削除を正常に検証することを強くお勧めします。

内部リソース

https://support.servicenow.com/kb_view.do?sysparm_article=KB0550107

https://community.servicenow.com/community?id=community_blog&sys_id=786eaeaddbd0dbc01dcaf3231f961959

Service Catalog を使用したデモデータの削除

一部のユーザーは、要求をインシデントとして送信しなくても、Service Catalog を使用してインスタンス上のデモデータの削除を要求することが可能です。このようなユーザーには、内部ユーザーと、customer_admin または partner_admin ロールを持つユーザーが含まれます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

1. https://support.servicenow.com/now に移動します。
2. デモデータを削除するインスタンスを指定します。

   インスタンスを見つけるのが難しい場合は、インスタンス名の先頭に * を付けて、包含クエリーを実行します。
3. クリック セルフサービス > デモデータの削除 > .
4. 選択したインスタンスからデモデータを削除する日時を指定します。

   日付と時刻は、現在の時刻よりも少なくとも 4 時間遅くする必要があります。
5. [送信] をクリックします。

新しい変更要求が作成され、自動的に表示されます。[終了予定日] は、[開始予定日] に基づいて 5 時間 (プロセスにかかる時間) を加算して自動計算されます。変更要求で、ウォッチリストを使用して、変更要求ステータスを知らせる必要がある他のチームメンバーを追加します。

セキュリティ包含リスト (インスタンスセキュリティ強化)

「ポジティブな」セキュリティモデル (「包含リスト」とも呼ばれる) は、何が許可されるかを定義し、それ以外はすべて拒否します。このセクションには、管理者が既知の包含リストに動作を制限するように設定できるセキュリティコントロールが含まれています。

注:
更新セットは構成を昇格させずにエラーを返すため、セキュリティ包含リストのプロパティはインスタンスごとに手動で設定する必要があります。

許可リストのメンバーコールの確認 (インスタンスセキュリティ強化)

必要に応じて、[sys_whitelist_member] テーブルから包含リストのメンバーコールエントリを確認し、削除します。

メンバーコールエントリは、サーバー側の Java リソースにアクセスして、適切な検証なしでアプリケーションベースの操作を実行できます。顧客データの不正な開示や改ざんを引き起こす可能性があるため、これはセキュリティ上の重大な問題になります。

詳細情報

属性	説明
テーブル名	sys_whitelist_member **注:** 最近のリリースでは、ServiceNow の従業員のみがこのテーブルにアクセスできます。管理者でもアクセスできません。
構成タイプ	テーブル
Instance Security Center での構成	あり
目的	このテーブルのエントリを確認して削除すること。
推奨値	テーブルにはレコードが存在しないようにしてください (リストは空である必要があります)。
機能への影響度	(低) パッケージコール削除ツールの実行時に生成された結果を確認および承認しているかぎり、影響はありません。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

属性	説明
	インスタンスが確実に正しく機能するようにするには、本番環境に展開する前に非本番環境でテストします。詳細は、「パッケージコール削除ツール」を参照してください。
セキュリティリスク	(高) サーバー上のデータ取得またはオブジェクトアクセスという結果になるクライアント側 API 呼び出しは、セキュリティの観点から危険であると見なされます。機密オブジェクトへのアクセスを許可および制限するために、これらのアイテムを検証してください。

設定手順

注:
以下に示す手順は、次の「設定手順」セクションで説明されている手順と類似しています。

- パッケージコール削除ツール
- チェック許可リストパッケージコール

既に完了している場合は、これらの手順をスキップできます。

1. パッケージ コール削除ツールプラグインをアクティブにします。詳細は、「パッケージコール削除ツール」を参照してください。
2. フィルターナビゲーターを使用して、[パッケージコール削除ユーティリティ] に移動します。
3. (1) ～ (4) の各スクリプトをクリックします。出力を待ってから、次の出力に進みます。
4. スクリプト (4) を実行すると、影響を受けるフィールドのリストが [パッケージコールアイテム] ページに表示されます。
5. [提案済み] および [エラー] セクションのすべてのアイテムを解決します。

   注:
   このツールは、`sa_mapping_ext_commands` および `sa_custom_operation` で使用されるいくつかのパッケージコールを報告する場合があります。これらのパッケージコールは MID Server に属します。クラスがないため、コードは MID Server で実行されます。[エラー] セクションで次のメンバーコールを見つけた場合は、[却下] (無視) としてマークします。このツールでは、そのメンバーコールを再度報告しません。

   - `Packages.com.snc.sw.util.JSONUtil.toJSONPlain(file_content);`
   - `Packages.com.snc.sw.util.JSONUtil.toJSONPlain(file_name);`
   - `Packages.com.snc.sw.commands.HttpCallHandler;`
   - `Packages.com.snc.sw.dto.ProviderType.SSH`

6. 詳細な修正については、ServiceNow サポートにお問い合わせください。

許可リストのパッケージコールの確認 (インスタンスセキュリティ強化)

必要に応じて、[sys_whitelist_package] テーブルから包含リストのパッケージコールエントリを確認し、削除します。

パッケージコールエントリは、サーバー側の Java リソースにアクセスして、適切な検証なしでアプリケーションベースの操作を実行できます。顧客データの不正な開示や改ざんを引き起こす可能性があるため、これはセキュリティ上の重大な問題になります。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

詳細情報

属性	説明
テーブル名	sys_whitelist_package **注:** 最近のリリースでは、カスタマーサービス & サポート のみがこのテーブルにアクセスできます。管理者でもアクセスできません。
構成タイプ	テーブル
Instance Security Center での構成	あり
目的	このテーブルのエントリを確認して削除すること。
推奨値	テーブルにはレコードが存在しないようにしてください (リストは空である必要があります)。
機能への影響度	(低) パッケージコール削除ツールの実行結果を確認および承認しているかぎり、影響はありません。 インスタンスが確実に正しく機能するようにするには、本番環境に展開する前に非本番環境でテストします。詳細については、「パッケージコール削除ツール 」を参照してください。
セキュリティリスク	(高) サーバー上のデータ取得またはオブジェクトアクセスという結果になるクライアント側 API 呼び出しは、セキュリティの観点から危険であると見なされます。機密オブジェクトへのアクセスを許可および制限するために、これらのアイテムを検証してください。
ワークアラウンド	ServiceNow サポートにお問い合わせください。

設定手順

1. パッケージ コール削除ツールプラグインをアクティブにします。詳細は、「パッケージコール削除ツール」を参照してください。
2. フィルターナビゲーターを使用して、[パッケージコール削除ユーティリティ] に移動します。
3. (1) ～ (4) の各スクリプトをクリックします。出力を待ってから、次の出力に進みます。
4. スクリプト (4) を実行すると、影響を受けるフィールドのリストが [パッケージコールアイテム] ページに表示されます。
5. [提案済み] および [エラー] セクションのすべてのアイテムを解決します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注:
このツールは、sa_mapping_ext_commands および sa_custom_operation で使用されるいくつかのパッケージコールを報告する場合があります。これらのパッケージコールは MID Server に属します。クラスがないため、コードは MID Server で実行されます。[エラー] セクションで次のパッケージコールを見つけた場合は、[却下] (無視) としてマークします。ツールは、そのパッケージコールを再度報告しません。

- Packages.com.snc.sw.util.JSONUtil.toJSONPlain(file_content);
- Packages.com.snc.sw.util.JSONUtil.toJSONPlain(file_name);
- Packages.com.snc.sw.commands.HttpCallHandler;
- Packages.com.snc.sw.dto.ProviderType.SSH

6. 詳細な修正については、ServiceNow サポートにお問い合わせください。

クロスオリジン **iframe** 通信の **URL** 許可リストを有効にする (インスタンスセキュリティ強化)

glide.ui.concourse.onmessage_enforce_same_origin プロパティを使用して、iframe 間のクロスオリジン通信を有効にします。

Openframe は、*glide.ui.concourse.onmessage_enforce_same_origin_whitelist* プロパティで指定された信頼できるドメインからのメッセージのみ処理できます。詳細については、「Specify UTL allow list for cross-origin iframe communication (クロスオリジン iframe 通信の UTL 許可リストを指定する)」を参照してください。

詳細情報

属性	説明
プロパティ名	glide.ui.concourse.onmessage_enforce_same_origin
構成タイプ	システムプロパティ (/sys_properties_list.do)
Instance Security Center での構成	あり
目的	信頼できるドメインの包含リストを有効にし、OpenFrame の iframe 間で通信できるようにすること
推奨値	true
機能への影響度	(中) 意図したドメインを包含リストに含めない場合、Now Platform インスタンス内に他のページを埋め込む機能が制限されることがあります。
セキュリティリスク	(高) Web ページに適切な作成元検証を実行しないイベントハンドラーが含まれている場合、任意の作成元からの Web ページまたはスクリプトは、その Web ページと通信できます。また、イベントハンドラーによって実行される機能を開始することもできます。
参照	OpenFrame の概要

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

相対リンクの適用 (インスタンスセキュリティ強化)

glide.cms.catalog_uri_relative プロパティを使用して、/ess/catalog.do の URL パラメーターからの相対リンクを適用します。

- **true** に設定されている場合、*uri* パラメーターを使用して、/ess/catalog.do ページから相対 URL のみが許可されます。
- **false** に設定すると、すべての URL が許可され、外部の未承認コンテンツへのリンクが許可される可能性があります。

詳細情報

属性	説明
プロパティ名	glide.cms.catalog_uri_relative
構成タイプ	システムプロパティ (/sys_properties_list.do)
Instance Security Center での構成	あり
目的	外部の未承認コンテンツへのリンクを制限すること
推奨値	true
機能への影響度	(低) この修正では、相対 URL のみが許可されるようにカタログページの検証が適用されます。外部 Web アプリケーションへの既存のリンクが切断されます。
セキュリティリスク	(高) 絶対 URL をパラメーターまたはフィールド値の一部として使用すると、セキュリティリスクが生じる可能性があるため、ソースページは攻撃者が制御する Web サイトにリダイレクトされます。

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

パッケージコール削除ツール (インスタンスセキュリティ強化)

Packages Call Removal Tool (*com.glide.script.packages_call_removal*) プラグインをアクティブ化して実行し、提案されたそれぞれの変更を完了するか却下するかを検討します。

Packages Call Removal Tool は、次のようなプラグインです。

- Now Platform Java クラスに対するパッケージコールのスクリプトをスキャンします。
- 優先する GlideScriptable 名に置き換える変更を提案します。
- スクリプトを容易に変更できるようにします。

注:
このレコードがベースシステムレコードの場合、ツールからの推奨事項を使用すると、アイテムは customer_update としてマークされます。そのスクリプトは今後更新されない可能性があります。それ以降のリリースでは、sys_whtelist_xxx テーブルが空であることが想定されています。ただし、このツールを使用すると、Packages,xxx のコールにフラグが設定されるので今もなお便利です。

このパッケージコール削除ツールは、sa_mapping_ext_commands および sa_custom_operation で使用されるいくつかのパッケージコールを報告する場合があります。これらのパッケージコールは MID Server に属します。クラスがないため、コードは MID Server で実行されます。[エラー] セク

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ションで次に列記するパッケージコールを見つけた場合は、[却下] (無視) としてマークします。ツールは、そのパッケージコールを再度報告しません。

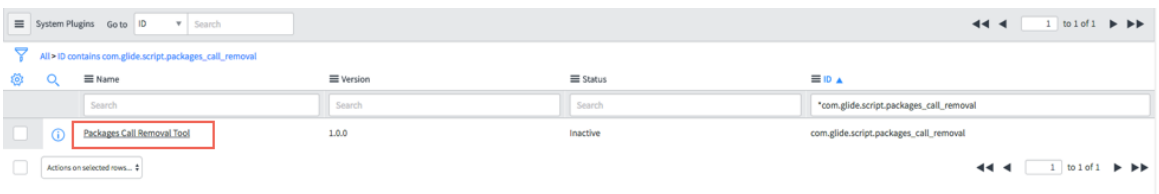
- Packages.com.snc.sw.util.JSONUtil.toJSONPlain(file_content);
- Packages.com.snc.sw.util.JSONUtil.toJSONPlain(file_name);
- Packages.com.snc.sw.commands.HttpCallHandler;
- Packages.com.snc.sw.dto.ProviderType.SSH

詳細情報

属性	説明
プラグイン名	com.glide.script.packages_call_removal
構成タイプ	[システム定義] > [プラグイン]
Instance Security Center での構成	あり
目的	承認されたデータアクセスのみを許可する Glide 許容 (GlideScriptable) 名の未承認パッケージ/メンバーコールを削除すること
推奨値	有効
機能への影響度	(低) この修正により、パッケージ呼び出しが `GlideScriptable` API に置き換えられ、パッケージコールを含むカスタマイズに影響を与える可能性があります。このツールは、実際にはパッケージコールを自動的に置き換えるわけではありません。代わりに、packages_call_item テーブルに保存される提案が提供されます。その後、管理者は提案された変更を承認するか却下するかを決定できます。
セキュリティリスク	(中) サーバー上でのデータ取得またはオブジェクトアクセスという結果をもたらすクライアント側 API 呼び出しは、セキュリティの観点から危険であると見なされます。機密オブジェクトへのアクセスを許可および制限するために、検証が必要になります。

設定手順

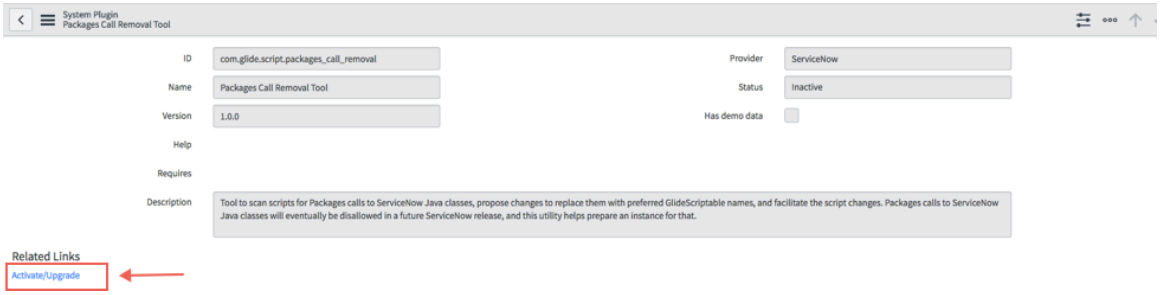
1. 移動先 システム定義 > プラグイン



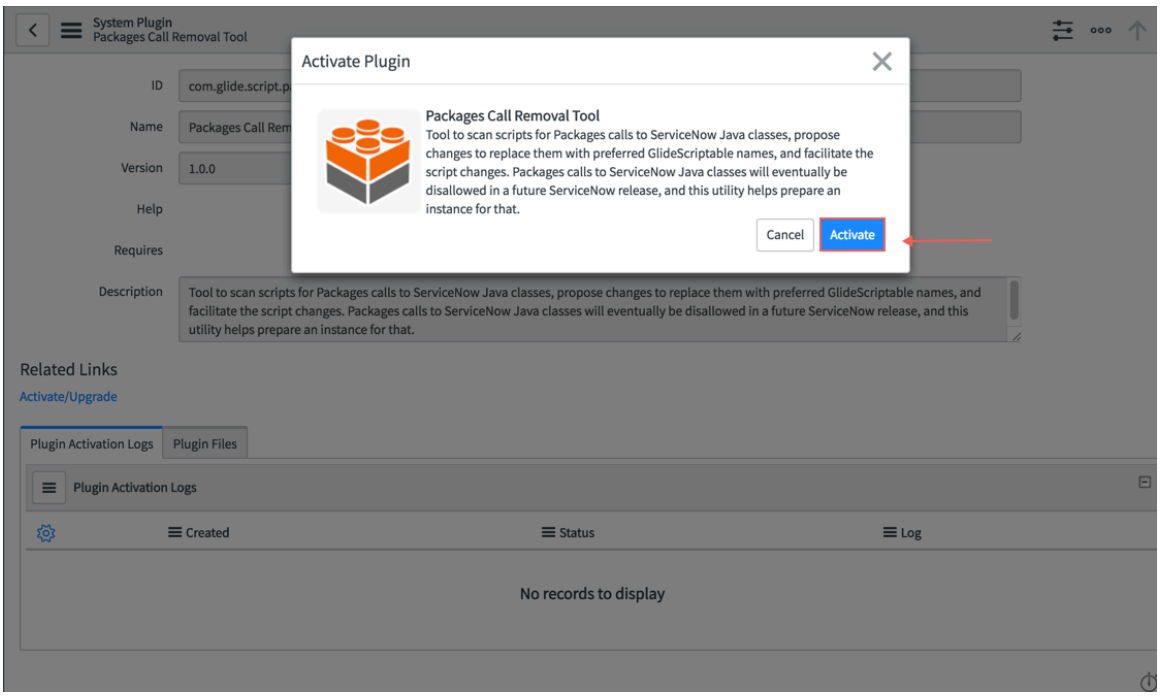
2. プラグイン ID = `com.glide.script.packages_call_removal` を検索します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



3. [アクティブ化/アップグレード **(Activate/Upgrade)]** をクリックしてプラグインをアクティブ化します。



4. 包含リストパッケージコールと包含リストメンバーコールを確認するには、次のトピックの「構成手順」セクションで説明されている手順を完了してください。
   - チェック許可リストメンバーコール
   - チェック許可リストパッケージコール

クロスオリジン **iframe** 通信の **URL** 許可リストを指定する (インスタンスセキュリティ強化)

glide.ui.concourse.onmessage_enforce_same_origin_whitelist プロパティを使用して、包含リストで指定した信頼ドメインから iframe 間のクロスオリジン通信を有効にします。

詳細情報

属性	説明
プロパティ名	glide.ui.concourse.onmessage_enforce_same_origin_whitelist
構成タイプ	システムプロパティ (/sys_properties_list.do)
Instance Security Center での構成	なし

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

属性	説明
目的	信頼できるドメインの包含リストを有効にし、OpenFrame の iframe 間で通信できるようにすること
要件	必須
機能への影響度	(中) 意図したドメインをリストに含めない場合、Now Platform インスタンス内に他のページを埋め込む機能が制限されることがあります。
セキュリティリスク	(高) Web ページに適切な作成元検証を実行しないイベントハンドラーが含まれている場合、任意の作成元からの Web ページまたはスクリプトは、その Web ページと通信できます。また、イベントハンドラーによって実行される機能を開始することもできます。他のドメインからの iframe との通信はセキュリティ上のリスクです。

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

ログアウトリダイレクトの **URL** 許可リスト (インスタンスセキュリティ強化)

glide.security.url.whitelist プロパティを使用して、導入された外部 URL を包含リストの URL に含めるかどうかを確認するために、検証レイヤーを追加します。

オープンリダイレクトは、脆弱な Web ページのリダイレクト先が、ユーザーを危険にさらす可能性がある、信頼できない悪意のあるページである場合に発生します。オープンリダイレクト攻撃にはフィッシング攻撃が伴います。これは、変更された脆弱なリンクが元のサイトと同じであることから、フィッシング攻撃が成功する可能性が高くなるためです。

このプロパティは、次の場合に適用されます。

- /logout.do?sysparm_goto_url={External URL}
- /cms_login_redirect.do?sysparm_goto_url={External URL}

ユーザーがインスタンスからログアウトすると、外部の信頼できるサイトに誘導されます。

- /logout_redirect.do?sysparm_url={External URL}
- /saml_redirector.do?sysparm_uri={External URL}

SAML を有効にすると、ID プロバイダー (IDP) のログアウト URL が呼び出されます。

詳細情報

属性	説明
プロパティ名	glide.security.url.whitelist
構成タイプ	システムプロパティ (/sys_properties_list.do)
Instance Security Center での構成	あり
目的	ログイン、ログアウト、またはその他のリダイレクト時に安全な URL リダイレクトを実装すること。このプロパティは、「未検証のリダイレクトと転送」と呼ばれる OWASP 上位 10 件の攻撃の 1 つを軽減します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

属性	説明
タイプ	カンマとスペースで区切られた文字列。例：https://example.com, https://wiki.example.com。
値	組織の承認済み URL [何らかの定義された FQDN (完全修飾ドメイン名) 例：http://www.servicenow.com]
機能への影響度	(中) この修正では、ログアウトページで検証が適用されます。SSO/SAML 構成のインスタンスのユーザーに機能的な影響を与える可能性があります。
セキュリティリスク	(高) クライアント側のオープンリダイレクトにより、攻撃者は、攻撃者が制御する Web サイトに被害者/ユーザーをリダイレクトできるようになります。これはセキュリティリスクと見なされます。
参照	マルチ SSO (SAML 2.0) のエラーと修正

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

仮想エージェント埋め込みクライアントコンテンツのセキュリティポリシー (インスタンスセキュリティ強化)

com.glide.cs.embed.csp_frame_ancestors プロパティを使用して、frame-ancestors ポリシーの構成を、https://<インスタンス>.service-now.com/sn_va_web_client_app_embed.do ページに対してのみ有効にします。

仮想エージェントプラグインを使用すると、外部 Web ページにクライアントを埋め込むことができます。Web ページにクライアントページを埋め込めるようにするには、コンテンツセキュリティポリシーによって外部ページが親フレームとして許可されている必要があります。

注:
コンテンツセキュリティポリシーを「*」のみで指定しないでください。この指定ではすべてのドメインが有効になり、アプリケーションがクリックジャッキングに対して脆弱な状態になる可能性があります。

詳細情報

属性	説明
プロパティ名	com.glide.cs.embed.csp_frame_ancestors
構成タイプ	システムプロパティ (/sys_properties_list.do)
Instance Security Center での構成	なし
目的	埋め込み可能な仮想エージェントページ用にカスタマイズされたコンテンツセキュリティポリシーを作成できるようにすること
推奨値	信頼できるドメインに設定
機能への影響度	(高) 仮想エージェントの埋め込み可能クライアントは、それ自体を外部サイトに埋め込むことを許可していませんが、コンテンツセキュリティポリシーが適切に設定されている場合は例外です。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

属性	説明
セキュリティリスク	(中) 設定が不適切な場合 (すべての親フレームを許可)、埋め込み可能なクライアントページがクリックジャッキングに対して脆弱な状態になる可能性があります。
参照	仮想エージェント Web クライアントを外部 Web ページに埋め込む frame-ancestors のコンテンツセキュリティポリシーの作成の詳細については、こちら を参照してください。

設定手順

1. 移動先 **/sys_properties_list.do**.
2. *com.glide.cs.embed.csp_frame_ancestors* プロパティを検索します。
3. 許容可能なコンテンツセキュリティポリシーを割り当て (会社またはその他の承認済みドメインのみを許可)、[更新] をクリックします。

仮想エージェント埋め込みクライアント **X-Frame-Options** (インスタンスセキュリティ強化)

com.glide.cs.embed.xframe_options プロパティを使用して、X-Frame ヘッダーの構成を、https://<インスタンス>.service-now.com/sn_va_web_client_app_embed.do ページに対してのみ有効にします。

仮想エージェントプラグインを使用すると、外部 Web ページにクライアントを埋め込むことができます。クライアントページを Web ページに埋め込めるようにするには、X-Frame-Options ヘッダーで iframe を親フレームに組み込むことができるようにする必要があります。

注:
X-Frame-Options ヘッダーの値を allow-from * に指定しないでください。この指定ではすべてのドメインが有効になり、アプリケーションがクリックジャッキングに対して脆弱な状態になる可能性があります。

詳細情報

属性	説明
プロパティ名	com.glide.cs.embed.xframe_options
構成タイプ	システムプロパティ (/sys_properties_list.do)
Instance Security Center での構成	なし
目的	埋め込み可能な仮想エージェントページの X-Frame-Options ヘッダーのディレクティブ指定を有効にすること
推奨値	sameorigin
機能への影響	(高) 仮想エージェントの埋め込み可能クライアントは、それ自体を外部サイトに埋め込むことはできませんが、 X-Frame-Options ヘッダーが適切に設定されている場合は例外です。
セキュリティリスク	(中) 設定が不適切な場合 (すべての親フレームを許可)、埋め込み可能なクライアントページがクリックジャッキングに対して脆弱な状態になる可能性があります。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

属性	説明
参照	仮想エージェント Web クライアントを外部 Web ページに埋め込む

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

X-Frame-Options: SAMEORIGIN (インスタンスセキュリティ強化)

glide.set_x_frame_options プロパティを使用して、すべての UI ページの SAMEORIGIN に対して X-Frame-Options 応答ヘッダーを設定します。

X-Frame-Options HTTP 応答ヘッダーは、<frame> または <iframe> 内のページをブラウザーでレンダリングできるかどうかを示すために使用されます。サイトでは、この機能を使用して、そのコンテンツがその他のサイトに組み込まれることがないようにすることで、クリックジャッキング攻撃を回避することができます。攻撃者は、お客様のページを自分のページに埋め込み、ページ要素が悪意を持って実行されるようにする可能性があります。エンドユーザーは、ページが自分のページに似ているため、そのページが正当だと考えるかもしれません。エンドユーザーが通常どおりに要素をクリックするだけで、悪意のあるスクリプトまたは要素が実行される可能性があります。

詳細情報

属性	説明
プロパティ名	glide.set_x_frame_options
構成タイプ	システムプロパティ (/sys_properties_list.do)
Instance Security Center での構成	あり
目的	クリックジャッキング攻撃の軽減
推奨値	true
機能への影響度	(低) この修正では、サードパーティアプリケーション内で Now Platform アプリケーションを iframe の形式でレンダリングする際に制限が適用されます。このような統合がある場合、アプリケーションはカスタマイズされたサードパーティアプリにはレンダリングされません。
セキュリティリスク	(中) 同一生成元ポリシーを使用すると、ドメインが別のドメインからスクリプトやリソースを取得できないようにすることができます。最新のブラウザーはすべてこの機能をサポートしています。 このポリシーは、プロトコル、ポート、およびホストに基づいて接続を検証します。CORS (クロスオリジン要求) は同一生成元ポリシーを修正したものであり、ヘッダー値の一部として明示的に指定されている場合に、別のドメインのリソース/スクリプトにアクセスできるようにします。 • この場合、**X-Frame-Options** ヘッダーは、Now Platform アプリケーションをサードパーティの Web サイトでレンダリングできるかどうかを制御します。 • プロパティ値を **SAMEORIGIN** に設定するとレンダリングが行われないため、機密情報が公開されることが減少します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

属性	説明
参照	利用可能なシステムプロパティ iFrame の設定

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

XML 外部エンティティ処理の検証

これらのプロパティは、XML DOCTYPE 参照の一部として含まれている場合、エンティティの拡張を可能にし、外部エンティティ (URL など) を制限します。DTD は基本的に XML スキーマです。XXE (外部エンティティ) の可能性があるエンティティ宣言のソリューションを探している場合は、システムプロパティを使用して XXE に対する包含リストの防御を有効にします。

XMLDocument および XMLUtil 解析の場合

カスタマイズで XMLDocument または XMLUtil を使用する場合は、次のシステムプロパティを設定します。エンティティの拡張を制御し、外部エンティティの検証を有効にします。これにより、包含リストにあるエンティティのみが処理されます。

エンティティ拡張しきい値の設定 (インスタンスセキュリティ強化)

glide.xmlutil.max_entity_expansion プロパティを使用して、エンティティ拡張の上限を小さい数値に変更します。

Now Platform は、このプロパティで指定された許容制限を超えるエンティティ拡張を処理しません。

> **注:**
> Now Platform によって設定されるデフォルトの最小値は 3,000 で、これは安全なしきい値と見なされています。したがって、入力した整数値が 3,000 未満の場合、プラットフォームではこのデフォルトの最小値が考慮されます。

詳細情報

属性	説明
プロパティ名	glide.xmlutil.max_entity_expansion
構成タイプ	システムプロパティ (/sys_properties_list.do)
Instance Security Center での構成	あり
目的	この修復コントロールは、XML エンティティ拡張/Billion Laugh 攻撃から防御するために有効にする必要があります。
推奨値	3,000
機能への影響度	(低) カスタマイズで大規模なエンティティ拡張を使用している場合、Now Platform が以降の処理をブロックする可能性があります。
セキュリティリスク	(高) 攻撃者はこの脆弱性を利用してデータを指数関数的に拡張し、すべてのシステムリソースを短時間で消費する可能性があります。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

許可リストを使用した **XMLdoc/XMLUtil** エンティティ検証 (インスタンスセキュリティ強化)

glide.xml.entity.whitelist.enabled プロパティを使用すると外部エンティティの検証が有効になり、包含リストに含まれているもののみを処理できます。

- このプロパティを **true** に設定すると、包含リストに記載されたエンティティの処理のみが許可されます (推奨設定)。
- このプロパティを **false** に設定すると、すべての外部エンティティの処理が許可されます。

必須条件

このプロパティを設定する前に、*glide.xml.entity.whitelist* プロパティでカンマ区切りの FQDN リストを定義してください。XML エンティティ処理を使用してアクセスできるのは、これらの URL のみになります。詳細については、XML 外部エンティティ処理 - 許可リスト を参照してください。

詳細情報

属性	説明
プロパティ名	*glide.xml.entity.whitelist.enabled*
構成タイプ	システムプロパティ (/sys_properties_list.do)
Instance Security Center での構成	あり
目的	この修復コントロールは、XXE 攻撃から防御するために有効にする必要があります。
推奨値	true
機能への影響度	(低) カスタマイズで *glide.xml.entity.whitelist* プロパティの包含リストではなく外部エンティティを使用している場合、Now Platform が以降の処理をブロックする可能性があります。詳細については、XML 外部エンティティ処理 - 許可リスト を参照してください。
セキュリティリスク	(高) 攻撃者は DTD を使用して、サーバーが実行する可能性のある任意の HTTP 要求を含めることができます。この場合、サーバーと他のエンティティとの信頼関係を利用する他の攻撃につながる可能性があります。
ワークアラウンド	外部エンティティ拡張を使用していない場合は、無効にします。詳細については、「エンティティ拡張の無効化」を参照してください。

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

XMLDocument2 パーサーの場合

カスタマイズで XMLDocument2 パーサーを使用する場合は、次のシステムプロパティを使用して外部エンティティの検証を有効にします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

エンティティ拡張の無効化 (インスタンスセキュリティ強化)

カスタマイズでエンティティの拡張が必要ない場合は、*glide.stax.allow_entity_resolution* プロパティを使用して外部エンティティの拡張を完全に無効化します。XML は解析を完了しますが、内部または外部エンティティは含まれません。

- このプロパティを **true** に設定すると、*glide.stax.whitelist_enabled* プロパティの設定に従って、すべての外部エンティティが対象エンティティを解決または拡張しようとします。
- このプロパティを **false** に設定すると、すべてのエンティティの解決と拡張がブロックされます。詳細については、許可リストを使用した XMLdoc2 エンティティ検証 を参照してください。

必須条件

このプロパティを設定する前に、次の手順を実行してください。

- *glide.xml.entity.whitelist.enabled* および *glide.stax.whitelist_enabled* プロパティを true に設定します。詳細については、「許可リストを使用した XMLdoc/XMLUtil エンティティ検証」と「許可リストを使用した XMLdoc2 エンティティ検証」を参照してください。
- *glide.xml.entity.whitelist* プロパティでカンマ区切りの FQDN リストを定義してください。XML エンティティ処理を使用してアクセスできるのは、これらの URL のみになります。詳細については、XML 外部エンティティ処理 - 許可リスト を参照してください。

詳細情報

属性	説明
プロパティ名	glide.stax.allow_entity_resolution
構成タイプ	システムプロパティ (/sys_properties_list.do)
Instance Security Center での構成	あり
目的	この修復コントロールは、XML エンティティ拡張/Billion Laugh 攻撃から防御するために有効にする必要があります。
推奨値	false
機能への影響度	(低) カスタマイズでエンティティ拡張を使用している場合、Now Platform が以降の処理をブロックする可能性があります。
セキュリティリスク	(高) 攻撃者はこの脆弱性を利用してデータを指数関数的に拡張し、すべてのシステムリソースを短時間で消費する可能性があります。
ワークアラウンド	カスタマイズでエンティティ拡張が必要な場合は、このプロパティを true に設定し、「許可リストを使用した XMLdoc2 エンティティ検証」に記載されている手順を実行してください。

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

OWASp リソースの詳細については、「OWASp」を参照してください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

許可リストを使用した **XMLdoc2** エンティティ検証 (インスタンスセキュリティ強化)

プロパティを使用して、包含リストに含まれている、 XMLDocument2 を使用した外部エンティティの処理を有効にします。

必須条件

このプロパティを設定する前に、次の手順を実行してください。

- *glide.xml.entity.whitelist.enabled* プロパティを true に設定します。詳細については、許可リストを使用した XMLdoc/XMLUtil エンティティ検証 を参照してください。
- *glide.xml.entity.whitelist* プロパティでカンマ区切りの FQDN リストを定義してください。XML エンティティ処理を使用してアクセスできるのは、これらの URL のみになります。詳細については、XML 外部エンティティ処理 - 許可リスト を参照してください。

詳細情報

属性	説明
プロパティ名	glide.stax.whitelist_enabled
構成タイプ	システムプロパティ (/sys_properties_list.do)
Instance Security Center での構成	あり
目的	この修復コントロールは、XML 外部エンティティ攻撃から防御するために有効にする必要があります。
推奨値	true
機能への影響度	(低) カスタマイズで包含リストではなく外部のエンティティを使用している場合、Now Platform が以降の処理をブロックする可能性があります。詳細については、「XML 外部エンティティ処理 - 許可リスト」を参照してください。
セキュリティリスク	(高) 攻撃者は DTD を使用して、サーバーが実行する可能性のある任意の HTTP 要求を含めることができます。サーバーと他のエンティティとの信頼関係を利用した他の攻撃につながる可能性があります。

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

XML 外部エンティティ処理 - 許可リスト (インスタンスセキュリティ強化)

必要に応じて、*glide.xml.entity.whitelist* プロパティを使用して、FQDN のカンマ区切りリストにアクセスできるようにします。XML エンティティ処理を使用してアクセスできるのは、これらの URL のみになります。

必須条件

このプロパティを設定する前に、*glide.xml.entity.whitelist.enabled* プロパティを設定します。これにより、外部エンティティの検証が有効になり、*glide.xml.entity.whitelist* プロパティで指定した包含リストの処理のみが許可されます。詳細については、「ホワイトリストによる XMLdoc/XMLUtil エンティティ検証」を参照してください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

詳細情報

属性	説明
プロパティ名	glide.xml.entity.whitelist
構成タイプ	システムプロパティ (/sys_properties_list.do)
Instance Security Center での構成	あり
目的	XML エンティティ処理がアクセスできる URL の包含リストを作成すること
推奨値	ユーザー指定 (例：https://google.com)
機能への影響度	(低) 包含リストに記載されていない場合、外部エンティティ処理がブロックされる可能性があります。包含リストを有効にすると、外部エンティティ定義の PUBLIC フォームが必要になります。
セキュリティリスク	(高) 攻撃者は DTD を使用して、サーバーが実行する可能性のある任意の HTTP 要求を含めることができます。この場合、サーバーと他のエンティティとの信頼関係を利用する他の攻撃につながる可能性があります。

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

セッション管理 (インスタンスセキュリティ強化)

セッション管理は、特定のユーザーに属するトラフィックを適切に識別するために役立ちます。信頼関係を悪用されないように注意してください。

Web アプリケーションは、最初のユーザー要求の後に匿名ユーザーを追跡するセッションを作成できます。たとえば、ユーザーの言語設定を維持して、次の事項を確認します。

- 後に続く要求でのユーザーの識別
- セキュリティアクセス制御の適用
- ユーザーのプライベートデータへのアクセスの承認
- アプリケーションのユーザビリティの向上

このようにして、現在の Web アプリケーションは、事前認証と事後認証の両方でセッション機能を提供できます。

認証とセッション管理

認証は、個人、エンティティ、または Web サイトが本物であることを確認するプロセスです。

認証は、通信の送信者のデジタル ID を確認しようとします。認証スキーマをテストすることは、認証プロセスがどのように機能するかを理解し、その情報を使用して認証メカニズムを回避することを意味します。一般的な例に、ログインプロセスがあります。ユーザー名、ユーザー ID、およびユーザーのみが知っている 1 件以上の個人情報を送信した後に、認証が行われます。

セッション管理にはセキュリティ関連プロパティが含まれています。管理者はこのプロパティを構成して、Now Platform で安全なセッション管理メカニズムが確立されていることを確認できます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

絶対セッションタイムアウト (インスタンスセキュリティ強化)

glide.ui.user_cookie.max_life_span_in_days プロパティを使用して、ユーザーが [記憶する] チェックボックスを選択してログインしたときに作成される Cookie の最大有効期間を設定します。Cookie の有効期間が切れると、[記憶する] チェックボックスを選択したユーザーはインスタンスへの再認証を強制されます。

これによりユーザー Cookie の有効期間は、Cookie が最初に発行されてからの指定の日数になります。デフォルト値は 30 日で、上限は 365 日です。

注:
任意のアクティブユーザーセッションに対して最大セッション時間を適用する場合は、「Configure a maximum active time for user sessions」を参照してください。

詳細情報

属性	説明
プロパティ名	*glide.ui.user_cookie.max_life_span_in_days*
構成タイプ	システムプロパティ (/sys_properties_list.do)
Instance Security Center での構成	あり
目的	特定の日数後に、[記憶する] チェックボックスを選択したユーザーに再認証を強制します。
機能への影響度	(中) このプロパティは、指定された期間が経過した後、すべての種類の Cookie ローテーションを回避することによって再ログインを強制します。
セキュリティリスク	(中) ユーザーの Cookie が無期限にアクティブになるとセキュリティリスクが発生するため、時間ベースの構成で期限が切れるようにする必要があります。
参照	利用可能なシステムプロパティ [記憶する] チェックボックスと cookie の設定を変更する

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

CSRF 対策トークン (インスタンスセキュリティ強化)

glide.security.use_csrf_token プロパティを使用して、受信要求の識別および検証に保護トークンが使用されるようにします。このトークンは、これらの攻撃を防止するために使用されます。

クロスサイト要求偽造 (CSRF) は、エンドユーザーが現在認証されている Web アプリケーションで不要なアクションを実行するように強制する攻撃です。CSRF 攻撃は、データの盗難ではなく、ステータス変更の要求を明確にターゲットにしています。これは、攻撃者に偽造要求に対する応答を確認する方法がないからです。

次のプロパティを有効にすると、CSRF トークンを制御できます。

- *glide.security.csrf_previous.time_limit*
- *glide.security.csrf_previous.allow*
- *glide.security.csrf.strict.validation.mode*

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

詳細情報

属性	説明
プロパティ名	glide.security.use_csrf_token
構成タイプ	システムプロパティ (/sys_properties_list.do)
Instance Security Center での構成	あり
目的	CSRF 攻撃の可能性からアプリケーションを保護すること
推奨値	true
機能への影響度	(低) この修正により、インスタンスユーザーがインスタンスへの書き込み要求を送信する前に、追加の検証手順が有効になります。すべての書き込み要求には、CSRF トークン (つまりユーザーセッションに関連付けられた検証/CSRF ID) が含まれています。ユーザーセッションが期限切れになると、セキュアトークンも期限切れになります。
セキュリティリスク	(高) クロスサイト要求偽造は、インスタンスデータの完全性を侵害する重大なセキュリティリスクです。攻撃者は、インスタンスユーザーの信頼を悪用して CSRF 攻撃を開始することができます。ソーシャルエンジニアリング攻撃を利用して、ユーザーがインスタンスで攻撃者の代わりに誤った要求を送信する可能性があります。

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

デフォルトの資格情報の変更 (インスタンスセキュリティ強化)

[ユーザーとグループ] の [パスワードのリセットが必要] チェックボックスを使用して、不正なユーザーがデフォルトのデータを利用できないようにします。

Now Platform には、インスタンスが zboot されるとき、または新しいインスタンスをプロビジョニングするときのデフォルトデータがいくつか含まれています。デフォルト管理者、ITIL、従業員などのデモユーザーアカウントが含まれている場合があります。プロパティを設定すると、アプリケーションにログインするときにデフォルトの管理者、ITIL、および従業員の資格情報を変更する必要が生じます。

設定手順

1. ユーザー名 **admin** とパスワード **admin** でログインします。
2. 移動先 システムセキュリティ > ユーザー > ユーザーとグループ。
3. ユーザー ID **admin** と名前「管理者 **(administrator)**」でユーザーを検索します。**[admin]** ユーザー ID をクリックして、ユーザーの設定を変更します。
4. 該当のユーザーの有効なメールアドレスを反映するように [メール] フィールドを変更します。
5. [パスワードのリセットを強制] チェックボックスをオンにします。
6. [更新] をクリックします。
7. ログアウトします。
8. 再度ログインすると、新しいパスワードの設定が求められます。
9. ITIL および従業員アカウントについて、手順 3 ～ 7 を繰り返します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

Cookie の HTTPOnly (インスタンスセキュリティ強化)

glide.cookies.http_only プロパティを使用して、機密性の高い Cookie の HTTPOnly 属性を有効にします。

HTTPOnly 属性は、JavaScript などのクライアント側スクリプトを使用した Cookie へのアクセスを許可しないため、クロスサイトスクリプティングなどの攻撃を防止するために使用します。クロスサイトスクリプティングのリスクは排除されませんが、一部の悪用ベクトルは排除されます。

詳細情報

属性	説明
プロパティ名	glide.cookies.http_only
構成タイプ	システムプロパティ (/sys_properties_list.do)
Instance Security Center での構成	あり
目的	クライアント側スクリプトが保護された Cookie にアクセスするリスクを軽減すること
推奨値	true
機能への影響度	(低) この修正では、セッション Cookie に HTTPOnly フラグが追加されるため、Cookie の盗難を防ぎます。 • ユーザーの Cookie にアクセスするために JavaScript を必要とするカスタム機能がある場合、その機能は損なわれます。通常の状況では発生しないはずです。 • Now Platform がセッション管理を処理するため、カスタムスクリプトがユーザーの Cookie にアクセスする理由はありません。
セキュリティリスク	(中) アプリケーションのセッション Cookie はエンドユーザーを認証し、アプリケーションに対する暗黙的なアクセス権限を付与します。つまり、セッション Cookie の盗難やエクスポートの防止が必要になります。HTTP Only フラグは、JavaScript インジェクションまたはクロスサイトスクリプティングの脆弱性による盗難からセッション Cookie を保護します。
参照	利用可能なシステムプロパティ

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

CSRF の厳格検証 (インスタンスセキュリティ強化)

glide.security.csrf.strict.validation.mode プロパティを使用して、CSRF トークンの厳格検証を有効にします。CSRF トークンが一致しない場合、要求は再送信されません。

詳細情報

属性	説明
プロパティ名	glide.security.csrf.strict.validation.mode
構成タイプ	システムプロパティ (/sys_properties_list.do)

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

属性	説明
Instance Security Center での構成	あり
目的	CSRF トークンの厳格検証を適用し、再利用を防止すること
推奨値	true
機能への影響度	(中) この修正により、インスタンスユーザーがインスタンスへの書き込み要求を送信する前に、追加の検証手順が有効になります。現在の CSRF トークンが以前に使用されたかどうかをチェックします。[はい] の場合、以降の書き込み要求は送信されません。
セキュリティリスク	(中) クロスサイト要求偽造は、インスタンスデータの完全性を侵害する重大なセキュリティリスクです。攻撃者は、インスタンスユーザーの信頼を悪用して、どのインスタンスユーザーにでも CSRF 攻撃を開始することができます。ソーシャルエンジニアリング攻撃を利用して、ユーザーが攻撃者の代わりにインスタンスに対して誤った要求を送信する可能性があります。

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

パスワードなし認証の無効化 (インスタンスセキュリティ強化)

glide.login.no_blank_password プロパティを使用すると、ユーザーが空白のパスワードで Now Platform にログインしたり、 [パスワード] フィールドを空のままにしたりできなくなります。

管理者が意図的に空の値または空白のパスワードをユーザーレコードに割り当てた場合でも、ユーザーは [パスワード] フィールドに値を指定しなければログインできなくなります。

詳細情報

属性	説明
プロパティ名	glide.login.no_blank_password
構成タイプ	システムプロパティ (/sys_properties_list.do)
Instance Security Center での構成	あり
目的	組織内ではユーザー名が簡単に推測できることがあるため、強力な認証を確実に実現すること
推奨値	true
機能への影響度	(低) 空白のパスワードは重大なセキュリティリスクと見なされるため、使用するべきではありません。ただし、このような使用法に有効なケースがある場合は、機能停止する可能性があります。パスワードが空白のユーザーは、インスタンスにログインできません。
セキュリティリスク	(高) 攻撃者は、デフォルトのユーザー名を使用して、またはパスワードのない特定の個人/グループ (通常は firstname.lastname) を使用してインスタンスにログインできます。この操作は、公開ユーザーがインスタンスデー

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

属性	説明
	タの機密性と完全性を侵害する可能性があるため、重大なセキュリティリスクと見なされます。

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

マルチファクター認証 **(MFA)** の有効化 (インスタンスセキュリティ強化)

glide.authenticate.multifactor プロパティを使用して、インスタンスでマルチファクター認証 (MFA) を有効にします。MFA は、インスタンスに対して認証するために、ユーザーに複数セットの資格情報の入力を要求するセキュリティ要件です。

詳細情報

属性	説明
プロパティ名	glide.authenticate.multifactor
構成タイプ	システムプロパティ (/sys_properties_list.do)
Instance Security Center での構成	あり
目的	インタラクティブなユーザーログインにマルチファクター認証を導入することで、インスタンスのセキュリティを強化すること
推奨値	true
機能への影響度	(中) このプロパティを有効にすると、ユーザーのエクスペリエンスが向上します。これは、侵害された資格情報に対する保護およびセキュリティの追加レイヤーとして機能します。
セキュリティリスク	(中) このプロパティを有効にしないと、機密データに不正にアクセスされるリスクがあります。
参照	Multifactor Authentication システムプロパティ

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

ロールベースのマルチファクター認証の基準を設定する

glide.authenticate.multifactor プロパティを使用して、特定のロールに割り当てられたすべてのユーザーにロールベースのマルチファクター認証 (MFA) を適用します。

マルチファクター認証は、ユーザーに割り当てられたロールに基づいて適用します。マルチファクターロールリストで「admin」、「security_admin」または「user_admin」のロールがユーザーに割り当てられている場合は、MFA が適用されます。

- 特定のロールに割り当てられたすべてのユーザーに対してロールベースのマルチファクター認証を適用するには、このプロパティを **true** に設定します。
- 特定のロールに割り当てられたすべてのユーザーに対してロールベースのマルチファクター認証を無効にするには、このプロパティを **false** に設定します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

詳細情報

属性	説明
プロパティ名	*glide.authenticate.multifactor*
構成タイプ	システムプロパティ (/sys_properties_list.do)
Instance Security Center での構成	あり
目的	特定のロールに割り当てられたすべてのユーザーに対してロールベースのマルチファクター認証を適用する。
タイプ	True/False
推奨値	*true*
セキュリティ依存関係	[マルチファクター基準] テーブルで、[ロールベースのマルチファクター認証 **(Role-based multi-factor authentication)]** をアクティブ化します。
機能への影響度	(中) このプロパティを有効にすると、ユーザーのエクスペリエンスが向上します。これは、侵害された資格情報に対する保護およびセキュリティの追加レイヤーとして機能します。
セキュリティリスク	(中) このプロパティを有効にしないと、機密データに不正にアクセスされるリスクがあります。
参照	ロールベースのマルチファクター基準の設定

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

パスワードリセットポリシーチェックの有効化 (インスタンスセキュリティ強化)

glide.enable.password_policy プロパティを使用して、ユーザーがユーザーインターフェイスを使用してパスワードを変更するたびに、パスワードポリシーのチェックを有効にします。

このプロパティを有効にした後に使用するパスワードポリシーを定義するには、「インスタンスでのパスワードポリシーの有効化」を参照してください。

> **注:**
> **glide.enable.password_policy** は、管理者がパスワードを変更する場合や、スクリプトを使用してユーザーを追加する場合には適用されません。

詳細情報

属性	説明
プロパティ名	glide.enable.password_policy
Instance Security Center での構成	あり
構成タイプ	システムプロパティ (/sys_properties_list.do)
目的	パスワード変更時にパスワードポリシーを適用すること
推奨値	true (より強力なパスワードの場合)

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

属性	説明
機能への影響度	(中) プロパティを true に設定すると、ユーザーがパスワードをリセットするときにパスワードポリシーチェックがオンになります。
セキュリティリスク	(中) パスワードポリシーがない場合、ユーザーが脆弱なパスワードを作成するため、攻撃者がインスタンスにアクセスする可能性が高くなります。

設定手順

Instance Security Center の [ハードニングコンプライアンス構成] ページでこの設定を構成する場合は、次の手順を実行します。

1. [中] で、**[Session Management]** を選択します。
2. [パスワードリセットポリシーチェックの有効化 **(Enable Password Reset Policy Checks)]** 設定で、パスワードの強度を中程度にする場合は [中] を、より強力なパスワードにする場合は [強 **(strong)]** を選択します。これらのオプションのいずれかを選択すると、**glide.enable.password_policy** プロパティが true に設定され、パスワードポリシーを自動的に更新するワークフローが開始されます。

さらに、*glide.apply.password_policy.on_login* システムプロパティを設定して、ログイン時のパスワードポリシーチェックを有効にすることもできます。

失敗したログイン試行の管理 (インスタンスセキュリティ強化)

ユーザーがパスワードの入力を何度間違えると Now Platform からロックアウトされるかをサイト管理者が管理できるようにするために、2 つのスクリプトアクションが用意されています。これらのスクリプトアクションのいずれかを有効にして、ログイン試行の失敗を管理できます。

詳細情報

属性	説明
プロパティ/プラグイン名	適用外
構成タイプ	[システムポリシー] > [スクリプトアクション]
Instance Security Center での構成	あり
目的	ログイン試行の失敗に対して厳格なポリシーを適用し、資格情報に対する総当たり攻撃を防止すること
推奨値	有効
機能への影響度	(低) この修正により、インスタンスの管理者は悪意のあるユーザーアクセスを監視および報告できるようになります。機能への影響はなく、ユーザーエクスペリエンスのみが変わります。
セキュリティリスク	(中) 定義されたログ記録と監査戦略を適用して、不審なアクティビティを適切なタイミングで特定して対処できるようにします。
参照	

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

設定手順

1. 移動先 システムポリシー > スクリプトアクション。
2. 名前「*SNC User*」を検索します。
3. 失敗したログイン試行を管理できるようにするには、*SNC User Lockout Check with Auto Unlock* または *SNC User Lockout Check* スクリプトアクションのいずれかの [アクティブ] ステータスを **false** から **true** に変更します。
4. ログイン成功後にログイン失敗回数のカウンターをリセットするには、*SNC User Clear* スクリプトアクションをアクティブ化します。

パスワードフィールドのオートコンプリート (インスタンスセキュリティ強化)

glide.login.autocomplete を使用して、ブラウザーがログインフォームのパスワードフィールドでオートコンプリート機能を使用できるようにします。

詳細情報

属性	説明
プロパティ名	glide.login.autocomplete
構成タイプ	システムプロパティ (/sys_properties_list.do)
Instance Security Center での構成	あり
目的	ブラウザーのパスワードフィールドのオートコンプリートを無効にすること
推奨値	false
機能への影響度	(低) この修正により、[パスワードフィールドのオートコンプリート **(Password field autocomplete)]** フラグがオフになり、ブラウザーによるパスワード履歴キャッシュがフィールドに表示されなくなります。機能への影響はありません。
セキュリティリスク	(低) ユーザー認証フィールドを検証する必要があり、クライアント側でのキャッシュは絶対に許可しないでください。
参照	https://support.servicenow.com/kb_view.do?sysparm_article=KB0563953

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

ようこそページからの資格情報の削除 (インスタンスセキュリティ強化)

ようこそページのデフォルトコンテンツを変更し、デフォルトの資格情報を削除します。

注:
2 つの [ログイン方法 (How to Login)] レコードは、CMS プラグインのデモ データの一部です。インスタンスのデモデータをインストールしない場合、これらのレコードは存在しません。その場合、推奨されるセキュリティプラクティスに従って、構成はセキュリティ準拠と見なされます。詳細については、「セキュリティベストプラクティス」を参照してください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

設定手順

1. 移動先 システム **UI** > 初期 (ようこそ) ページのコンテンツ > **.**
2. ログイン方法の簡単な説明が記載されている 2 つのセクションを見つけます。
3. それぞれの [アクティブ (Active)] ステータスを **true** から **false** に変更します。

[記憶する] の削除 (インスタンスセキュリティ強化)

glide.ui.forgetme プロパティを使用して、ログインページから [記憶する] チェックボックスを削除して、ログイン情報がキャッシュされないようにします。

詳細情報

属性	説明
プロパティ名	glide.ui.forgetme
構成タイプ	システムプロパティ (/sys_properties_list.do)
Instance Security Center での構成	あり
目的	認証情報がキャッシュされないようにすること。
推奨値	true
機能への影響度	(低) この修正では、セッションが期限切れになるとインスタンスから自動的にログアウトされるため、ユーザーエクスペリエンスが変わります。セッションの有効期限は、「ユーザーセッションの管理」で詳述されているように、システムプロパティに設定された値にのみ依存します。
セキュリティリスク	(中) [記憶する] チェックボックスをログイン時にオンにした場合、ユーザーのコンピューターに追加の Cookie が保存されます。 • その目的は、ログイン中のユーザーが再度アクセスした場合にセッションを自動的に再確立することです。 • ユーザーが意図的にログアウトするまでユーザーセッションはアクティブにできるため、セキュリティ上のリスクがあります。エンドユーザーがブラウザーをそのままにして席を離れた場合、または別の攻撃によって侵害された場合、このシナリオでの攻撃の可能性が高くなります。
参照	[記憶する] チェックボックスを削除する

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

HTTP セッション識別子のローテーション (インスタンスセキュリティ強化)

glide.ui.rotate_sessions プロパティを使用して HTTP セッション識別子のローテーションを有効にし、セキュリティの脆弱性を軽減します。

認証後に非認証ユーザーのセッション ID が変更されない場合、Web アプリケーションはセッション固定化攻撃 に対して脆弱になります。悪意のあるユーザーが非認証セッションを開始し、関連するセッション ID を被害者に提供する可能性があります。被害者が認証されると、悪意のあるユーザーがその認証済みセッションを共有するようになります。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

詳細情報

属性	説明
プロパティ名	glide.ui.rotate_session
構成タイプ	システムプロパティ (/sys_properties_list.do)
Instance Security Center での構成	あり
目的	より安全なセッション認証を実現すること
推奨値	true
機能への影響度	(中) この修正では、ユーザーが非認証ページから認証済みページに移動したときに SessionID が変更されました。 • ユーザーの初回ログイン時に、または何らかの目的でプロキシを使用したり、SessionID をハードコーディングしたりすると、機能に影響を与える可能性があります。 • Single Sign-on 認証に SAML 2.0 プラグインを使用している場合、インスタンスと ID プロバイダーの間で行われるセッション情報の共有が妨げられる可能性があります。そのような場合、このプロパティを false に設定できます。
セキュリティリスク	(遅延) SessionID は、ブラウザーでセッションステータスを維持することによって、インスタンスユーザーを処理および認証するために使用されます。したがって、SessionID は機密データと見なされ、デフォルトで安全である必要があります。セッションローテーションは、ユーザーが非認証ページから認証ページへ移動するたびに SessionID の変更を適用するセキュリティコントロールです。
参照	SAML による認証

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

セキュアセッションの **Cookie** (インスタンスセキュリティ強化中)

glide.ui.secure_cookies プロパティを使用して、適切にフォーマットされた Cookie を要求します。

プロパティが true に設定されていると、関連付けられた Cookie が想定される形式でない場合、インスタンスはセッションを拒否します。

詳細情報

属性	説明
プロパティ名	glide.ui.secure_cookies
構成タイプ	システムプロパティ (/sys_properties_list.do)
Instance Security Center での構成	あり

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

属性	説明
目的	より安全なセッション認証を実現すること
推奨値	true
機能への影響度	(低) プロパティが true に設定されている場合、不適切な形式の Cookie は却下されます。このような Cookie が却下された場合、ユーザーは再度ログインする必要があります。

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

セキュリティ照会ポリシー (インスタンスセキュリティ強化)

com.glide.security.referrerpolicy プロパティを使用して、Now Platform ページがデータの要求を送信するときに HTTP 応答ヘッダーで送信する参照元データを制御します。HTTP ヘッダーの Referer-Policy 値は、データ要求に含める参照元情報を制御します。

セキュリティ照会ポリシーの値

com.glide.security.referrerpolicy プロパティは、以下のプロパティ値のいずれかを設定します。

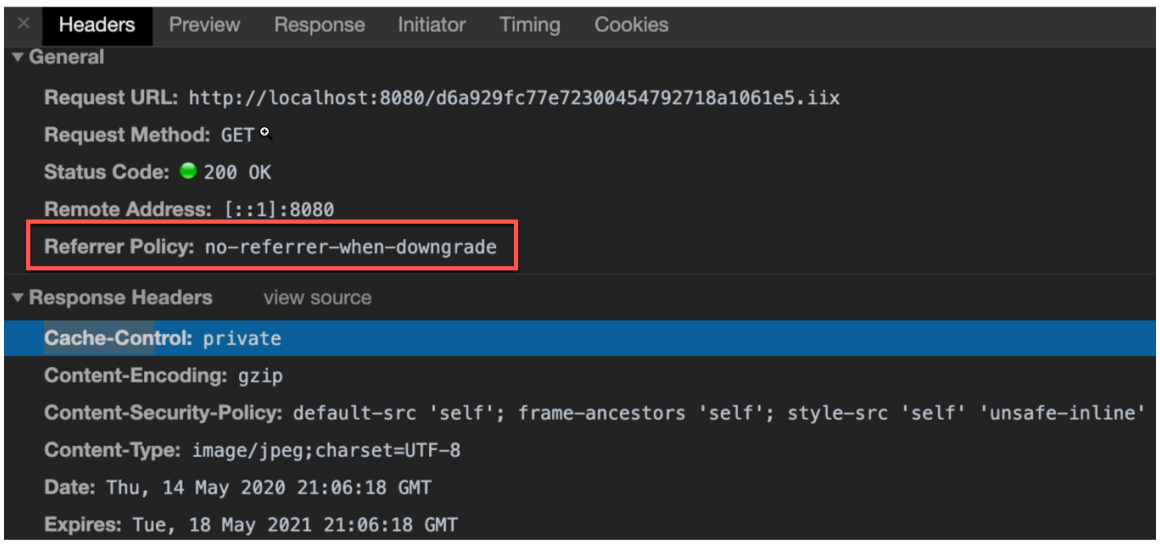
値	説明
default	Now Platform インスタンスは、特定の Now Platform ページ要求に適した参照元ヘッダーで送信される情報のレベルを管理します。
same-origin	Now Platform ページは、インスタンスおよび同じドメイン内部には完全な参照元 URL を送信し、外部の作成元には参照元ヘッダーを送信しません。 この設定により、適切なレベルのインスタンスセキュリティが確保されます。
origin	Now Platform ページは、インスタンスおよび同じドメイン内部に参照元ヘッダーのベース URL を送信し、また外部にも送信します。 この設定により、適切なレベルのインスタンスセキュリティが確保されます。
origin-when-cross-origin	Now Platform ページは、インスタンスおよび同じドメイン内部で参照元ヘッダーの URL 全体を送信し、外部にはベース URL のみを送信します。 この設定により、適切なレベルのインスタンスセキュリティが確保されます。
no-referrer-when-downgrade	セキュリティプロトコルにダウングレードがないかぎり、Now Platform ページは URL の作成元、パス、およびクエリー文字列を送信します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

値	説明
	注: この設定は、Now Platform で適切なレベルのインスタンスセキュリティが確保されないため、使用しないでください。

参照元ポリシーの例と値の概要



詳細情報

属性	説明
プロパティ名	com.glide.security.referrerpolicy
構成タイプ	システムプロパティ (/sys_properties_list.do)
Instance Security Center での構成	なし
目的	Now Platform ページがデータの要求を送信するときに、「referrer」ヘッダーを介して送信される受信データの量を制御すること
推奨値	default
機能への影響度	(低)「default」に設定すると、Now Platform インスタンスが referrer ヘッダーで送信される情報のレベルを管理します。
セキュリティリスク	(高) このプロパティ値を「no-referrer-when-downgrade」に設定しても、インスタンスに対して適切なレベルのセキュリティは保証されません。
参照	https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referrer-Policy

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

属性	説明
	https://developer.mozilla.org/en-US/docs/Glossary/origin

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

セッションアクティビティタイムアウト (インスタンスセキュリティ強化)

glide.ui.session_timeout プロパティを使用して、アクティビティのタイムアウト値を分単位で指定します。

このプロパティを設定すると、機能にいくつかの影響が生じます。

- 指定されたセッションタイムアウトが長いほど、セッションの処理中に使用されるメモリ量が多くなります。ベースシステムでは、デフォルトの Apache Tomcat タイムアウト時間の 30 分を使用します。
- Now Platform は [記憶する] によってもユーザーをログアウトします。アプリケーションで 30 分間操作がなかった場合、ログインページの [記憶する] チェックボックスがオンになっていないかぎり、プラットフォームはユーザーを自動的にログアウトします。違いは、再度ログインして続行することがないことです。
- ユーザーのホームページに自動的に更新されるゲージまたはコンテンツがある場合は、このタイムアウト値に一度も達しない可能性があります。

詳細情報

属性	説明
プロパティ名	glide.ui.session_timeout
構成タイプ	システムプロパティ (/sys_properties_list.do)
Instance Security Center での構成	あり
目的	セッションタイムアウトを適用すること
推奨値	ユーザー指定のタイムアウト (分)。推奨値は 30 分ですが、この値は機能とセキュリティ要件によって異なる場合があります。この値の設定は 1 日を超えないようにしてください。
機能への影響度	(中) この修正では、ユーザーアカウントのタイムリーな有効期限が適用されます。機能への影響はありませんが、ユーザーエクスペリエンスは変わります。
セキュリティリスク	(中) 無期限にアクティブであるユーザーセッションはセキュリティリスクです。時間ベースの設定で期限切れにする必要があります。
参照	ユーザーセッションの管理

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

セッションウィンドウのタイムアウト (インスタンスセキュリティ強化)

glide.ui.user_cookie.life_span_in_days プロパティを使用して、「記憶する」Cookie の有効期限を設定します。デフォルト値は 15 日で、上限は 30 日です。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

詳細情報

属性	説明
プロパティ名	glide.ui.user_cookie.life_span_in_days
構成タイプ	システムプロパティ (/sys_properties_list.do)
Instance Security Center での構成	あり
目的	「記憶する」Cookie のデフォルトの有効期限を有効にすること
推奨値	ユーザー定義の整数値 (日数) [例：15]
機能への影響度	(中) エンドユーザーがログインページから [記憶する] チェックボックスをオンにして Now Platform にログインすると、このプロパティが有効になります。
セキュリティリスク	(中) ユーザーの Cookie が無期限にアクティブになるとセキュリティリスクが発生するため、時間ベースの構成で期限が切れるようにする必要があります。
参照	利用可能なシステムプロパティ [記憶する] チェックボックスと cookie の設定を変更する

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

自動作成されたユーザーアカウントのパスワード設定

システムプロパティ *glide.email.inbound.use_default_password* および *glide.user.default_password* を使用して、受信メールから作成された新しいユーザーのパスワード作成方法を定義します。

このドキュメントで説明されているシステムプロパティは、受信メールから生成されたユーザーアカウントのパスワードをインスタンスが処理する方法を定義します。インスタンスは、メールを受信し、自動的にユーザーを作成できるように設定する必要があります。これらの構成の詳細については、以下のセクションを参照してください。

アカウントを自動作成できるようにインスタンスを設定した後は、プロパティを使用して、デフォルトのパスワードを使用するかどうかを決定し、必要に応じてパスワードを定義できます。

必須条件

これらのプロパティを使用するには、新しいユーザーアカウントを自動的に作成するようにインスタンスを構成する必要があります。

- 独自の POP3 サーバーを設定して、インスタンスのメールを格納および受信する必要があります。次に、*glide.email.read.active* システムプロパティを true に設定する必要があります。インスタンスでの POP3 サーバー設定についての詳細は、「独自の POP3 サーバーの使用を有効にする」を参照してください。
- *glide.pop3readerjob.create_caller* プロパティを true に設定します。このプロパティの変更により、インスタンスは受信メールから自動的にユーザーを作成できます。詳細については、「ユーザーの自動作成の有効化」を参照してください。

> **注:**
> *glide.pop3readerjob.create_caller* プロパティが **false** に設定されている場合は、*glide.user.default_password* プロパティをスキップします。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

インスタンスでのパスワードの定義方法

Quebec およびそれ以前のリリースの ServiceNow では、*glide.user.default_password* システムプロパティで定義された複雑なパスワードを使用して、インスタンスが受信メールから新しいユーザーアカウントを作成します。ユーザーは初回のログインでこのパスワードを使用し、その後インスタンスからユーザーに対して新しいパスワードの入力が求められます。インスタンスを Rome 以降のリリースにアップグレードした場合、このプロセスは変更されません。管理者は、以下で説明する新しい方法を使用するようにインスタンスを更新できます。

Rome リリース以降の新しいインスタンスでは、受信メールから作成されたユーザーアカウントにはパスワードがありません。ユーザーが新しいアカウントでインスタンスに初めてアクセスするときに、ユーザー名を入力して [パスワードを忘れた場合] ボタンをクリックし、初期パスワードを作成する必要があります。

Rome 以降のリリースでは、*glide.email.inbound.use_default_password* システムプロパティの値を設定することで、インスタンスがどのプロセスに従うか選択できます。上記のデフォルトの動作を変更するには、次の情報を使用してこのシステムプロパティを作成します。

システムプロパティのフィールド	値
名前	glide.email.inbound.use_default_password
タイプ	true | false
値	目的の動作に基づいて値を選択します。 true 新しいアカウントは、*glide.user.default_password* システムプロパティで定義されたデフォルトのパスワードを使用します。 false 新しいアカウントにはデフォルトのパスワードがありません。このセクションで前述したように、ユーザーはパスワードを定義する必要があります。

システムプロパティの作成の詳細については、「システムプロパティを追加する」を参照してください。

デフォルトパスワードの定義

インスタンスがデフォルトのパスワードを使用するように設定されている場合は、*glide.user.default_password* システムプロパティを使用してそのパスワードを定義する必要があります。次の情報を使用してこのプロパティを作成します。

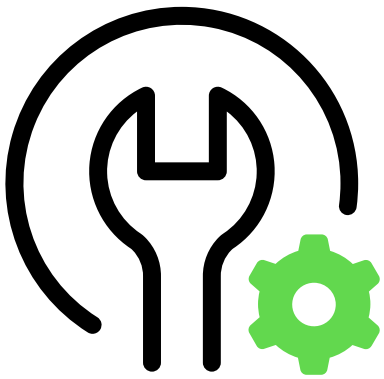
システムプロパティのフィールド	値
名前	glide.user.default_password
タイプ	password2
値	デフォルトとして使用する一意のパスワードを入力します。パスワードの複雑さを強力にして、インスタンスのセキュリティを確保するようにしてください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

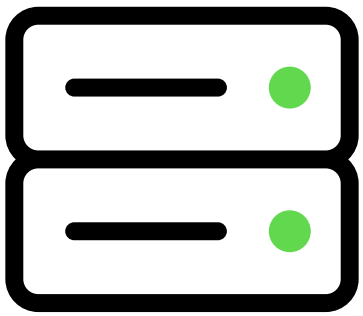
その他の設定とセキュリティリソース

このセクションでは、Instance Security Center の外部で設定するセキュリティプロパティについて説明します。また、その他のセキュリティ関連のリソースについても説明します。



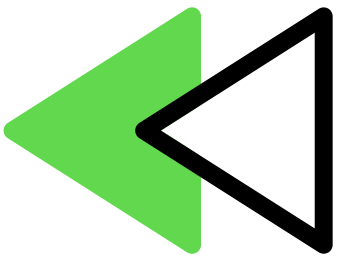
セキュリティシステムプロパティ

セキュリティ設定には、インスタンスのセキュリティレベルを制御するプロパティがいくつかあります。



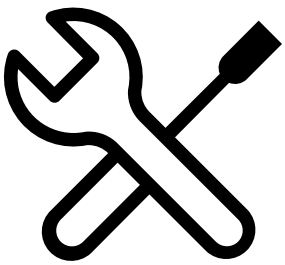
MID Server 展開ガイド

ServiceNow Management, Integration, and Discovery (MID) サーバーは、仮想マシンを含む標準ハードウェア上で Windows サービスまたは UNIX デーモンとして動作する軽量の Java アプリケーションです。



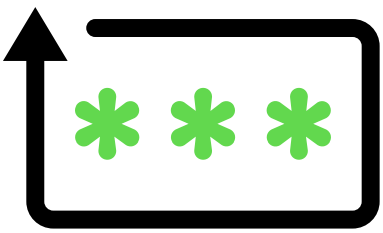
元に戻せる動作

「safe_overrides」または「no_db_override」のいずれかに分類されるシステムプロパティがあります。



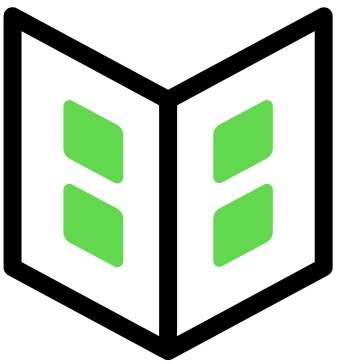
減価償却済みセキュリティプロパティ

これらのセキュリティプロパティは、以前のリリースで廃止されました。



Javascript コンテンツアクセス制御の使用

JavaScript コンテンツアクセス制御を使用して、インスタンス内でブロックされたサードパーティの JavaScript URL のリストを変更できます。



その他のセキュリティ強化リソース

Now Platform に関連する、セキュリティコントロールの強化に関するその他の情報源。

ログ記録、監査、およびエラー (インスタンスセキュリティ強化)

ログ記録と監査戦略を適用して、不審なアクティビティを適切なタイミングで特定して対処できるようにします。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

インスタンスのログ記録の詳細については、「システムログ」を参照してください。を使用して、ログインや失敗したログインなどのシステムイベントを監視するスケジュールがあることを確認するシステムログ > イベント.

SQL エラーメッセージの無効化 (インスタンスセキュリティ強化)

glide.db.loguser プロパティを使用して、SQL エラーメッセージがブラウザーでレンダリングされないようにします。

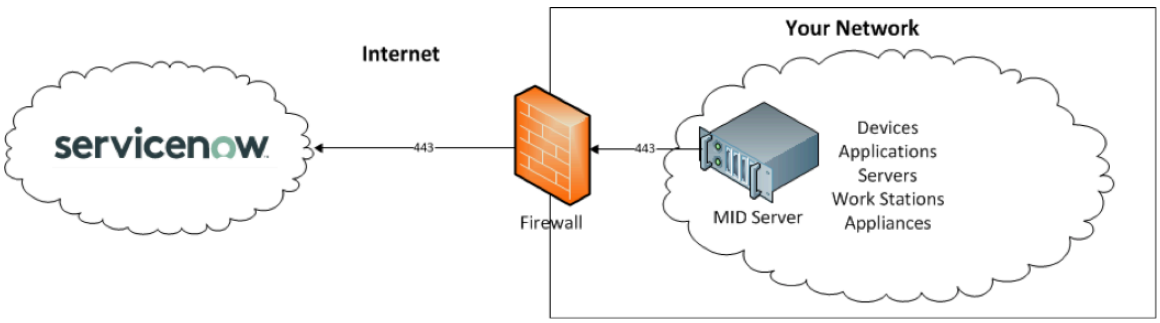
詳細情報

属性	説明
プロパティ名	glide.db.loguser
構成タイプ	システムプロパティ (/sys_properties_list.do)
Instance Security Center で構成可能	いいえ
目的	ブラウザー内での SQL エラーメッセージの表示を無効にすること
タイプ	true | false
推奨値	false
機能への影響度	(低) この修正により、SQL エラーメッセージをレンダリングできなくなります。機能への影響はありません。
セキュリティリスク	(中) 攻撃者に役立つ可能性のある機密の SQL 情報は、Web ページのエラーメッセージに含まれて表示されることはありません。

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

MID Server の安全な展開ガイド (インスタンスセキュリティ強化)

ServiceNow の管理、統合、検出サーバー (MID Server) は、仮想マシンを含む標準ハードウェア上で Windows サービスまたは UNIX デーモンとして動作する軽量の Java アプリケーションです。



独自のログイン資格情報を使用して ServiceNow クラウド内のインスタンスに対して安全に認証し、アプリケーション、データソース、およびサービスによるデータ送信を容易にします。複数の MID Server をさまざまなネットワークセグメントに展開して、スケーラビリティを向上させることができます。

MID Server のセキュリティに関して、次の要素を考慮してください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

物理セキュリティ

MID Server、または仮想化された MID Server のハイパーバイザーをホストする物理ハードウェアを保護します。

- 不正アクセスからハードウェアを保護する安全な場所にハードウェアを配置します。
- 電子カードリーダーと CCTV 監視を使用して、この場所へのアクセスを保護します。
- 物理的なハードウェアを、ロックされたゲージまたは物理キーのアクセス制御を備えたラックに入れます。

仮想インフラストラクチャのセキュリティ

仮想化を柔軟に使用して、仮想化されたオペレーティングシステムに複数の MID Server をインストールし、共有の物理ハードウェアにネットワークをインストールします。

仮想化された MID Server の不正なクローン作成を防ぐために、ハイパーバイザーおよび仮想インフラストラクチャ管理コンソールへのアクセスを保護する必要があります。

- 信頼できる少数の管理者によるハイパーバイザーおよび仮想インフラストラクチャ管理コンソールへのアクセスを制限します。
- ESX サーバーや VirtualCenter などの管理コンソールに対しては、内部の信頼できるネットワークのみ接続を許可します。
- VLAN を使用してネットワーク攻撃を防止します。
- ベンダーの仮想化強化ガイドで公開されているセキュリティガイドラインに従ってください。

オペレーティングシステムのセキュリティ

インスタンスに対する安全な認証のために、config.xml という名前の構成ファイルに記載された Now Platform ユーザー名とパスワードがどのように MID Server に格納されるかを学習します。

資格情報を不正アクセスから保護するために、セキュアで強化されたオペレーティングシステムに MID Server を展開する必要があります。

- オペレーティングシステムへのアクセスを、数人の信頼できる管理者に制限します。
- オペレーティングシステムのログを監視して、不正なアクセス、特に config.xml ファイルへのアクセスを検出します。このファイルには重要な MID Server 構成情報が含まれているからです。
- オペレーティングシステムのセキュリティパッチを最新のアンチウイルスソフトウェアで定期的にインストールし、アンチウイルス定義を定期的に更新します。
- MID Server を実行するには、最新の Java フレームワークが必要です。Java を定期的に更新します。
- 不要なサービスやアプリケーションを削除または無効化します。
- OS ファイアウォールをインストールして、許可されていないポートへのアクセスを制限します。
- ベンダーのオペレーティングシステム強化ガイドで公開されているセキュリティガイドラインに従ってください。

ネットワークセキュリティ

MID Server は SSL を使用してポート 443 でインスタンスと通信します。受信接続は必要ありません。

ネットワーク内の MID Server を適切に保護するには、次の手順を実行します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- 企業ファイアウォールの背後にある保護されたサーバーに MID Server をインストールして、インターネットから不正アクセスされないようにします。
- オペレーティングシステムとハードウェアの企業管理に必要な受信接続以外は受け入れないように、MID Server のファイアウォールを設定します。
- MID Server をホストするシステムが **install.servicenow.com** で ServiceNow ダウンロードサイトにアクセスできる必要があります。

  注:
  この URL は ServiceNow ダウンロードサイトを示しており、このトピックからはアクセスできません。

  MID Server のホストマシンは、そのサイトにアクセスしてインストーラーパッケージをダウンロードできる必要があります。60 分ごとに **install.servicenow.com** にアクセスして新しいバージョンが利用可能かどうかを確認し、利用可能な場合は自動アップグレードを実行します。MID Server のアップグレードは、インスタンスをアップグレードするときにも行われます。

ファイアウォール

MID Server からインスタンスや自動アップグレードサーバーへの送信ネットワークトラフィックを許可するようにファイアウォールを設定します。

ファイアウォールを設定するには、次の構文例を使用します。

- `<source IP> TO <instance_name>.service-now.com ON PORT 443`
- `<source IP> TO install.service-now.com ON PORT 443`

管理とマネージメント

このセクションでは、お使いの環境で MID Server を管理するためのセキュリティプラクティスとガイドラインについて説明します。

mid_server ロールを持つアカウントの作成

mid_server ロールを含むインスタンスにユーザーアカウントを作成します。

ユーザーアカウントを作成するときは、次のガイドラインに従ってください。

- MID Server のインスタンスで管理アカウントを使用しないでください。
- MID Server アカウントに対して、十分に長く複雑なパスワードを使用します。
- パスワードは、大文字、小文字、数字、および特殊文字を含めて 12 文字以上にする必要があります。
- インスタンス内の異なる MID Server に対して、一意のパスワードを持つ異なる MID Server アカウントを使用します。
- で有効にすることで、厳格な SOAP セキュリティ機能を使用して、すべてのテーブルをアクセス制御リスト (ACL) で保護 *`Enforce strict security on incoming SOAP requests`* します。 システムプロパティ > **Web** サービス.
- 組織のパスワードポリシーを満たす頻度で MID Server のパスワードを変更します。

注:
詳細については、「MID Server ユーザーの作成とロールの付与」を参照してください。

Windows ホストでの **MID Server** の設定

Windows ホストに MID Server をインストールすると、Windows サービスが作成されます。デフォルトでは、このサービスはローカル Windows システムアカウントとして実行されます。インス

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

トールが完了したら、新しく作成された Windows サービスを、Windows ホストで MID Server を実行するために必要な最小限の権限を持つアカウントに変更します。

1. 移動先 コンピュータ管理 > サービスとアプリケーション > サービス.
2. **[ServiceNow MID Server]** を右クリックし、[プロパティ] をクリックします。
3. ポップアップウィンドウで [ログオン] タブをクリックします。
4. [このアカウント **(This account)]** の横にあるラジオボタンをクリックします。
5. サービスを実行するアカウントのユーザー名とパスワードを適宜入力します。
6. **[OK]** をクリックします。
7. [サービス] ウィンドウで、**[ServiceNow MID Server]** を右クリックし、[再起動] をクリックします。
8. MID Server が正常に再起動し、インスタンスに接続できることを確認します。

Windows Discovery と **Orchestration** の資格情報

ターゲットシステムで、必要な最小限の権限を備えたローカルの Windows または Active Directory アカウントを設定します。ドメイン管理者の資格情報は、使用する必要がない場合があります。

次の製品ドキュメントのページには、使用が必要なアカウントのタイプと必要な権限に関するガイダンスが記載されています。

- Windows 資格情報
- Windows プローブと権限
- Discovery 用 Microsoft Just Enough Administration (JEA)

Linux Discovery と **Orchestration** の資格情報

検出とオーケストレーションを実行するときは、ターゲット Linux システムで制限付きの sudo 権限を持つ非ルートアカウントを使用します。

次のガイドラインを使用してください。

- Linux アカウントに対して、十分に長く複雑なパスワードを使用します。パスワードは、大文字、小文字、数字、および特殊文字を含めて 12 文字以上にする必要があります。
- sudo 権限を設定する場合、実行している Linux ディストリビューションによっては、実行可能なバイナリファイルへのローカルパスが異なる場合があります。「MID Server 特権コマンド」を参照してください。

MID Server ログイン資格情報の暗号化

デフォルトで、MID Server のログイン資格情報は、config.xml ファイル内で暗号化されます。

config.xml ファイルを編集してパスワードを指定するときは、次の構文を使用して、`encrypt="true"` 属性を確保してください。

```
<parameter name="MID.instance.username" value="MIDsrvadmin" />
```

```
<parameter name="MID.instance.password" encrypt="true" value="$ECUREpassw0rd"/>
```

注:
MID Server のログイン資格情報の暗号化は、物理セキュリティおよびネットワークセキュリティが不十分である危険なサーバーホストを置き換えるものではありません。config.xml ファイルに格納されているパスワードは、MID Server の初回起動時、または既存の MID Server の場合は再起動時に暗号化されます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

DH グループの最小サイズを 2048 ビットに設定

米国国立標準技術研究所 (NIST) は、2013 年以降、Diffie-Hellman (DH) 1024 ビットキーの使用を禁止しています。代わりに、DH グループの最小サイズを 2048 ビットに設定します。

1. インスタンスで、次の場所に移動します。 **MID** サーバー > サーバー.
2. この機能を無効にする MID Server の名前をクリックします。
3. MID Server 構成で、[構成パラメーター] の横にある [新規] ボタンをクリックします。
4. [MID Server 構成パラメーター] で、次のパラメーター設定を構成します。
   - パラメーター名 `mid.ssh.dh_group_length_min`
   - 値 `2048`

送信 SSL の無効化

Now Platform で SSLv2 および SSLv3 を無効にすることができます。このプロパティを設定すると、REST 要求や SOAP 要求などの送信接続を行うときに、MID Server は TLS を使用して強化されたセキュリティを利用します。

1. インスタンスで、次の場所に移動します。 **MID** サーバー > プロパティ.
2. 設定パラメーターを追加し、値を次のように設定します。
   - 名前 `glide.outbound.sslv3.disabled`
   - 値 `true`

弱いアルゴリズムの無効化

弱いアルゴリズムを無効にして、以前は機能していた、TLS 1.2 に準拠していない HTTP サーバーへの要求が失敗するようにすることができます。

次の構文を使用して、agent フォルダーの jre/lib/security/java.security ファイルを編集します。

`jdk.tls.disabledAlgorithms=SSLv3, TLSv1, TLSv1.1, [その他の弱いアルゴリズム…]`

注:
このファイルはアップグレード時に上書きされるため、アップグレードするたびにこのファイルを再更新するプロセスを実行する必要があります。

Powershell ユーザーは、Windows 管理者に問い合わせて、古いバージョンの TLS を無効にする必要があります。Powershell で使用されている TLS のバージョンの詳細については、`[enum]::GetNames([Net.SecurityProtocolType])` コマンドを使用してください。

元に戻せる動作

「safe_overrides」または「no_db_override」のいずれかに分類されるシステムプロパティがあります。

安全なオーバーライド

これらのプロパティの値は、一度変更すると変えることができなくなります (元に戻すことはできません)。

注:
管理者は、安全なオーバーライドプロパティの名前を変更したり、削除したりすることはできません。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

属性	カテゴリ
デフォルトの拒否	アクセス制御
AJAXGlideRecord ACL チェックの有効化	アクセス制御
クライアント呼び出し可能スクリプトインクルードのプライバシー	アクセス制御
クライアント生成スクリプトサンドボックス	入力の検証
コレクションモードのオーバーライド (使用廃止)	セキュリティ包含リスト

DB オーバーライドなし

これらのプロパティの既存の値を変更またはオーバーライドすることはできません。

属性	カテゴリ
ファイルのダウンロード制限を有効にする	添付ファイル

廃止されたセキュリティプロパティ

これらのセキュリティプロパティは、以前のリリースで廃止されました。

コレクションモードのオーバーライド (使用廃止)

glide.whitelist.manager.collection_mode.override プロパティは、高度にカスタマイズされたインスタンスに下位互換性を提供するように設計されています。このプロパティでは、Calgary より前のバージョンで作成されたパッケージコールを使用していましたが、それ以降は廃止されました。

詳細情報

属性	説明
プロパティ名	glide.whitelist.manager.collection_mode.override
構成タイプ	システムプロパティ (/sys_properties_list.do)
Instance Security Center での構成	なし
目的	[コレクションモード (Collection Mode)] プロパティを無効にして、Java パッケージコールをインスタンスにインポートする場合のセキュリティギャップを解消します。
推奨値	false
機能への影響度	(低) セクション 10.6 の結果を確認して承認しているかぎり、影響はありません。インスタンスが確実に正しく機能するようにするには、本番環境に展開する前に非本番環境でテストします。
セキュリティリスク	(高) サーバー上のデータ取得またはオブジェクトアクセスという結果になるクライアント側 API 呼び出しは、セキュリティの観点から危険であると見なされます。機密オブジェクトへのアクセスを許可および制限するために検証してください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

属性	説明
参照	https://support.servicenow.com/kb_view.do?sysparm_article=KB0621483

SMTP 認証 (使用廃止)

glide.smtp.auth プロパティは、SMTP サーバーがユーザー名とパスワードの認証エントリを必要とするかどうかを指定していました。

詳細情報

属性	説明
プロパティ名	glide.smtp.auth
構成タイプ	システムプロパティ (/sys_properties_list.do)
Instance Security Center での構成	なし
目的	SMTP 認証の適用
推奨値	true
機能への影響度	(高) この修正では、コンテンツがメールの形式で配信される前に、外部メール サーバーへの認証が適用されます。自動化でメールコンテンツを配信するように設定されている場合は、プロパティを設定し、該当するユーザー名/パスワードを入力してメールサーバーにアクセスするまでは、影響が生じる可能性があります。
セキュリティリスク	(低) コンテンツを外部メールサーバーに送信する前に SMTP 認証を有効にします。認証は、常に、インスタンスとの間でトランザクションが発生する前に行う必要があります。
参照	メールプロパティ

JavaScript コンテンツアクセス制御の使用

アップグレードしたお客様は、JavaScript コンテンツアクセス制御を使用することで、インスタンス内のブロックされたサードパーティの JavaScript URL のリストを変更できます。

始める前に

アップグレードしたお客様には、テーブルへの読み取りおよび書き込みアクセス権があります。

新規のお客様ではすべてのレコードが非表示になります。 ServiceNow® サポートにお問い合わせください。

必要なロール：admin

手順

1. アプリケーションナビゲーターで、 sys_js_content_provider_rule.listを検索します。
2. [新規] をクリックします。
3. フォームのフィールドに入力します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

JavaScript コンテンツプロバイダールール

フィールド	説明
アクティブ	選択するとルールがアクティブになるオプション。オフにすると、一致する他のルールがない場合に、[パス] の URL が許可されます。
パス	JavaScript ファイルへの絶対 URL。 **注:** すべてのパスに 4 つのバリエーションがあります。たとえば、/scripts/lib/jquery/jquery-1.8.2.min.js というパスは次の URL をブロックします。 ○ /scripts/lib/jquery/jquery-1.8.2.min.js ○ /scripts/lib/jquery/jquery-1.8.2.min.jsx ○ /lib/jquery/jquery-1.8.2.min.js ○ /lib/jquery/jquery-1.8.2.min.js
アクション	次の操作を行うオプション。 ○ 拒否：[パス] の URL またはそのバリエーションに対して、サーバーが **404 Not Found** 応答を返します。 ○ 許可：サーバーが、[パス] の URL またはそのバリエーションのファイルのコンテンツを返します。 ○ リダイレクト：サーバーが、[リダイレクトパス] フィールドで指定された代替ファイルの内容を返します。
アプリケーション	ルールのスコープを指定するオプション。デフォルトは [グローバル] です。 **注:** この機能は、スコープやアプリケーション、またはドメインに依存しません。
リダイレクトパス	リダイレクト先のパスを明確にするフィールド。 [アクション] を [リダイレクト]に設定すると、[パス] の URL への要求に対して、この URL の内容が代わりに提供されます。

4. [送信] をクリックします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

その他のセキュリティ強化リソース

Now Platform に関連するセキュリティコントロールの強化に関しては、他にも次のような情報源があります。

リソース	説明
セキュリティテストポータル	HI のセキュリティサービスポートフォリオ
KB0538598	顧客アプリケーションのペネトレーションテスト | ポリシーおよび手順
KB0546756	公開コンテンツ管理システム (CMS) アクセスの無効化
KB0550071	ServiceNow, Inc. インスタンスアクセス制御のレビュー
KB0550613	IP アドレス制限の識別と有効化
KB0550828	GlideAjax トランザクションの監査とレビュー
KB0550837	スクリプトサンドボックスの修復
KB0551031	パスワードリセット UI のセキュリティ修正
KB0552835	デモユーザーアカウントの修正
KB0529232	ServiceNow, Inc. Monitoring - 概要とインサイト
KB0564232	外部認証による ServiceNow, Inc. モバイルアプリの使用
セキュリティとリスク	ServiceNow, Inc. コミュニティ

ハードニング設定

ServiceNow, Inc. セキュリティセンターのハードニング設定コンテンツには、Now Platform のセキュリティ関連のシステムプロパティとプラグインの詳細な説明とコンプライアンス値が含まれています。セキュリティセンターのハードニング設定アプリを使用して、これらのプロパティを設定できます。

概要と目的

セキュリティセンターは、現在のインスタンスセキュリティ設定がセキュリティセンターのハードニング設定のコンプライアンス値にどの程度準拠しているかに基づいて、毎日のコンプライアンススコアを計算し、パーセンテージで表します。

インスタンスのスコアに影響を与える可能性がある特定のセキュリティ設定を、セキュリティセンターから直接管理できます。

ハードニング設定の構成について、テーブルに示す属性を使用して説明します。

ハードニング設定構成の詳細

構成属性	説明
概要	推奨事項の概要を提供します。
構成名	プロパティまたはプラグイン名。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ハードニング設定構成の詳細 (続く)

構成属性	説明
構成タイプ	システムプロパティ (*sys_properties_list.do*) など、セキュリティセンターの外部でプロパティを構成できる場所について説明します。
データタイプ	構成に必要な値のタイプを説明します。例としては、true/false ブーリアン、インストール、プラグイン、文字列などがあります。
推奨値	インスタンスのセキュリティコンプライアンスを強化するためにセキュリティセンターによって推奨される値。
デフォルト値	ベースシステムで構成が設定されている値。
カテゴリ	ハードニング設定のカテゴリの名前とリンク。
セキュリティリスク	重大度スコア：スコアは、脆弱性が悪用される可能性に応じて、インスタンスに対する潜在的なセキュリティリスクを示します。セキュリティ脆弱性は、**0.0** ～ **10.0** のスケールで CVSS (共通の脆弱性採点システム) スコアを使用して個別に考慮され、採点されます。詳細については、「https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator」を参照してください。
	CVSS スコアに応じた重大度： • 重大：9.0 ～ 10.0 • 高：7.0 ～ 8.9 • 中：4.0 ～ 6.9 • 低：0.01 ～ 3.9 • なし：0.0
	セキュリティリスクの詳細：設定構成の重要性と、推奨構成を利用しない場合のリスクについて説明します。
依存関係と前提条件	ハードニング構成の前、またはそれともに必要な関連設定または構成。
機能への影響	このハードニング設定がインスタンスの操作に与える影響。
参照	構成ドキュメントまたはその他の役立つ情報へのリンク。

注:
一部の構成は カスタマーサービス & サポート によってのみ完了でき、そのように示されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

インスタンスが強化要件を満たしていることを確認する方法の詳細については、「セキュリティの強化」を参照してください。

その他のリソース

ユーザーの参照用に、Now Platform には製品ドキュメントの広範な構成機能情報が含まれています。インスタンスの保護 にあるリンクを使用すると、セキュリティコンテンツの大半にアクセスできます。また、以下も参照してください。

- 利用可能なシステムプロパティ
- 一般的なセキュリティ設定のプロパティ
- 高セキュリティ設定

ハードニング設定のベースライン

ハードニング設定の個別のベースラインバージョンが、さまざまなファミリーおよびストアリリースにどのように対応しているかについて説明します。

Security Center は、インスタンスからシステムプロパティのサブセットを取り込み、その構成の詳細と、アプリ内での非準拠のセキュリティへの影響を表示することで機能します。ベースラインは、Security Center アプリの各リリースで取り込まれるシステムプロパティの参照ポイントとして機能します。

ハードニング設定ベースラインの概要

Security Center のバージョン	ハードニング設定のベースラインバージョン	サポートされているファミリー	ストアリリース日	デフォルトでインストールされる内容
SSC v1.1	ベースライン v1.0	Utah、Vancouver	2023 年 5 月	Vancouver ファミリー
SSC v1.2	ベースライン v1.0	Utah、Vancouver	2023 年 8 月	ストアのみ
SSC v1.3	ベースライン v2.0	Vancouver、Washington	2023 年 11 月	Washington ファミリー

新しいハードニング設定

以下は、バージョン 2.0 ベースラインで Security Center リリースされたすべての新しいハードニング設定のリストです。

- 資格情報エイリアスの使用を強制
- ネットワークエラーの OCSP チェックを強制する
- 証明書チェーンとホスト名の確認
- 証明書の失効の確認
- SVG ファイルの安全なコンテンツセキュリティポリシーの設定
- インポートセット API 内での安全な複数挿入操作の使用
- Protected Tables プラグインの有効化
- 安全なリファラーポリシーの適用
- アクティブセッションタイムアウト例外ロールの定義

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- 非アクティブなセッションのプロアクティブな無効化
- AttachmentCreator SOAP Web Service のファイル MIME タイプの検証
- 証明書ベースの認証の適用
- セッション監査イベントのログ記録
- イベント管理 HTTP プロセッサーで認証を必須とする
- 共有ダッシュボードへのセキュリティルールの適用
- ターゲットクローン作成の禁止
- Public Sector Digital Services のスコープセキュリティの適用
- 情報要求 Playbook のスコープ付き ACL アクセスを強制する
- ゲストのアクティブなセッションの有効期間の制限
- HTTP 応答本文のサイズを制限する
- 統合のアクティブセッションの有効期間の制限
- ナレッジベースへのアクセス制限
- 記事のユーザーコメントの非表示
- OAuth パラメーターの POST 投稿への制限
- トレーニングフローと予測フローでの添付ファイルサイズの制限
- ダッシュボードの作成/削除でのアクセスチェック
- GlideRecord スコープフェンシングのレガシー動作の有効化
- アプリケーションスコープ制限の適用
- Service Catalog アイテム追加ページにアクセスするための書き込みアクセス権
- CSRF 対策トークンの検証時間
- アーカイブテーブル ACL のチェック
- 強化された Java セキュリティマネージャーの有効化
- 厳格な特権昇格の適用
- モバイルアプリケーションをバックグラウンドで実行する場合のペーストボードのクリア
- デバイスの暗号化とパスコードの要件の適用
- UI のアクティブセッションの有効期間の制限
- MID 監査ログを有効にする
- 必要な JMS 接続ファクトリー
- Customer Service アプリケーションでのゲストウォークアップエクスペリエンスに CAPTCHA を必須にする
- 人事アプリで ACL 評価の代理操作を確認する
- 個人メールからの人事ケースの更新を制限する

ハードニング設定の更新

このリストには、ベースラインバージョン 2.0 で Security Center 更新されたハードニング設定が含まれています。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ドキュメント	更新
JSONP 要求を信頼できる URL に制限する	• 新しい簡単な説明:JSONP 要求を信頼できる URL に制限する (Restrict JSONP Requests to Trusted TURLS) • 以前の簡単な説明:JSONP 要求包含リスト
許可される添付ファイルサイズを最小化	• 新しい簡単な説明: 許可された添付ファイルサイズを最小化 • 以前の簡単な説明:添付ファイルの最大許容サイズ
証明書の信頼を強制する	• 新しい簡単な説明:証明書の信頼を強制する • 以前の簡単な説明:証明書の信頼
Xframe オプションを設定してサードパーティの Web サイトが埋め込まれないようにする	• 新しい簡単な説明: サードパーティの Web サイトが埋め込まれないように Xframe オプションを設定する • 以前の簡単な説明:Xframe オプション
仮想エージェント内で HTML サニタイザーを有効化する	• 新しい簡単な説明: 仮想エージェント内で HTML サニタイザーを有効にする • 古い簡単な説明:HTML サニタイザーを有効にする
委任開発者の読み取りアクセスを制限する	• 新しい簡単な説明:委任開発者の読み取りアクセスを制限する • 以前の簡単な説明:委任開発者の読み取りアクセス許可リスト (Delegated developers Read Access Allowlist)
スパムメールのスコアリングとフィルタリングを有効にする	• 新しい簡単な説明: スパムメールのスコアリングとフィルタリングを有効にする • 古い短い説明: スパムメールのスコアリングとフィルタリング
High Security プラグイン	• 新しい簡単な説明: High Security プラグインを有効にする • 古い簡単な説明:High Security プラグイン

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ドキュメント	更新
Contextual Security プラグインの有効化	• 新しい簡単な説明: Contextual Security プラグインの有効化 • 以前の簡単な説明:Contextual Security プラグイン
HTML サニタイゼーションを強制する	• 新しい簡単な説明:HTML のサニタイズを強制する • 古い簡単な説明:サニタイズされていない HTML を確認
SOAP 要求のゲストユーザーの設定	• 新しい簡単な説明: SOAP 要求のゲストユーザーの設定 • 以前の簡単な説明:SOAP 要求のゲストユーザー
SNC アクセス制御プラグインを有効にする	• 新しい簡単な説明: SNC アクセス制御プラグインを有効にする • 以前の簡単な説明:SNC アクセス制御プラグイン
セキュリティジャンプスタートプラグイン (ACL ルール) を有効にする	• 新しい簡単な説明: セキュリティのジャンプスタートプラグインを有効にする • 以前の簡単な説明:Security Jump Start プラグイン (ACL ルール)
従来の AngularJS の動作を無効にする	• 新しい簡単な説明:レガシー AngularJS の動作を無効にする • 以前の簡単な説明:レガシー AngularJS の動作
同時インタラクティブセッションの制限	• 新しい簡単な説明:同時インタラクティブセッションの制限 • 以前の簡単な説明:Glide 認証による同時インタラクティブセッションの制限
すべてのノードにまたがる同時セッションを制限する	• 新しい簡単な説明:すべてのノードで同時セッションを制限する • 以前の簡単な説明:Glide 認証で全ノードでの同時セッションを制限

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ドキュメント	更新
同時インタラクティブセッション数の最小化	• 新しい簡単な説明:同時インタラクティブセッション量の最小化 • 以前の簡単な説明:Glide 認証の最大同時インタラクティブセッション数
ロールベースのマルチファクター認証のアクティブ化	• 新しい簡単な説明:ロールベースのマルチファクター認証のアクティブ化 • 以前の簡単な説明:ロールベースのマルチファクター認証
マルチ SSO プラグインの更新バージョンを有効にする	• 新しい簡単な説明:マルチ SSO プラグインの更新バージョンを有効にする (Enable Updated Version of Multi SSO Plugin) • 以前の簡単な説明:更新されたバージョンのマルチ SSO プラグインが有効になっています
SAML notBefore または notOnOrAfter 制約期間の最小化	• 新しい簡単な説明:SAML の「notBefore」または「notOnOrAfter」制約期間の最小化 • 古い簡単な説明:SAML「notBefore」または「notOnOrAfter」制約
API 要求に認証を要求する	• 新しい簡単な説明:API 要求に認証を要求 • 以前の簡単な説明:API 要求認証
csv 要求に認証を要求する	• 新しい簡単な説明:CSV 要求に認証を要求 • 以前の簡単な説明:CSV 要求認証
データブローカー REST API の認証を要求	• 新しい簡単な説明:データブローカー Rest API の認証を要求 • 以前の簡単な説明:データブローカー Rest API 認証
Excel 要求に認証を要求	• 新しい簡単な説明:Excel 要求に認証を要求 • 以前の簡単な説明:Excel 要求認証
インポート要求に認証を要求する	• 新しい簡単な説明: インポート要求に認証を要求 • 以前の簡単な説明:インポート要求認証

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ドキュメント	更新
JSONv2 要求に認証を要求	• 新しい簡単な説明:JSONv2 要求の認証を要求 • 以前の簡単な説明:JSONv2 要求認証
PDF 要求に認証を要求	• 新しい簡単な説明: PDF 要求に認証を要求 • 以前の簡単な説明:PDF 要求認証
RSS 要求に認証を要求する	• 新しい簡単な説明: RSS 要求に認証を要求する • 以前の簡単な説明:RSS 要求認証
SCHEMA 要求に認証を要求する	• 新しい簡単な説明:SCHEMA 要求に認証を要求する • 以前の簡単な説明:SCHEMA 要求認証
SOAP 要求に認証を要求する	• 新しい簡単な説明:SOAP 要求に認証を要求する • 以前の簡単な説明:SOAP 要求認証
アンロード要求に認証を要求する	• 新しい簡単な説明: アンロード要求に認証を要求 • 以前の簡単な説明:要求認証をアンロード
WSDL 要求に認証を要求する	• 新しい簡単な説明: WSDL 要求に認証を要求 • 以前の簡単な説明:WSDL 要求認証
XML 要求に認証を要求する	• 新しい簡単な説明: XML 要求に認証を要求する • 古い簡単な説明:XML 要求認証
XML 出力依頼に権限を要求する	• 新しい簡単な説明: XML 出力要求に認証を要求する • 古い簡単な説明: XML 出力認証
XSD 要求に対する認証を必須とする	• 新しい簡単な説明: • 以前の簡単な説明:

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ドキュメント	更新
HTTP のみの Cookie フラグを有効にする	• 新しい簡単な説明:HTTP のみの Cookie フラグを有効にする • 以前の簡単な説明:HTTP のみの Cookie フラグ
生データベースクエリの実行を無効にする	• 新しい簡単な説明:生のデータベースクエリの実行を無効にする • 以前の簡単な説明: 操作レベルのアクセス制御要件
SQL エラーメッセージを無効にする	• 新しい簡単な説明: SQL エラーメッセージを無効にする • 古い簡単な説明: SQL エラーメッセージの無効化
受信メールの画像を添付ファイルに変換	• 新しい簡単な説明:受信メール画像を添付ファイルに変換 • 以前の簡単な説明:Inbound Email HTML の変換
SMTP 受信者の数量を最小化する	• 新しい簡単な説明: SMTP 受信者数の最小化 • 以前の簡単な説明:最大 SMTP 受信者数
Excel 式をエスケープ	• 新しい簡単な説明:Excel の数式をエスケープする • 以前の簡単な説明:Excel 式をエスケープ
HTML サニタイザーを有効にする	• 新しい簡単な説明:HTML サニタイザーを有効にする • 古い簡単な説明:HTML サニタイザー
HTTP ヘッダー値のキャッシュコントロール	• 新しい簡単な説明: キャッシュ制御 HTTP ヘッダー値 • 古い簡単な説明:キャッシュ制御 HTTP ヘッダー値
本番インスタンスの動作を強制	• 新しい簡単な説明:本番インスタンスの動作を強制 • 以前の簡単な説明:本番インスタンスの動作

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ドキュメント	更新
許可された ServiceNow 内部 IP アドレスを定義する	• 新しい簡単な説明:許可された ServiceNow 内部 IP アドレスの定義 (Define Allowed ServiceNow Internal IP Addresses) • 以前の簡単な説明:IP アドレスのアクセス許可リスト (IP Addresses Access Allowlist)
従来の JQuery の動作を無効にする	• 新しい簡単な説明:レガシー JQuery の動作を無効にする • 以前の簡単な説明:レガシー JQuery の動作
LDAP 初期識別名の設定解除	• 新しい簡単な説明: LDAP 初期識別名の設定解除 • 以前の簡単な説明:LDAP 最初の識別名
カスタムジャーナルエントリへのアクセスを制限する	• 新しい簡単な説明:カスタムジャーナルエントリへのアクセスを制限する • 以前の簡単な説明:安全なカスタムジャーナルエントリー
1 回限りの帯域外検証ツールの有効期間の最小化	• 新しい簡単な説明: 1 回限りの Out of Band 検証ツールの有効期間を最小限に抑える • 以前の簡単な説明:短い 1 回限りの Out of Band 検証ツールの有効期間
送信 SSLv2/SSLv3 接続の無効化	• 新しい簡単な説明:送信 SSLv2/SSLv3 接続を無効にする • 古い簡単な説明:SSLv2/SSLv3 の無効化
受信メールからのユーザーの作成を無効にする	• 新しい簡単な説明:受信メールからのユーザーの作成を無効にする • 古い簡単な説明:ドメインでメールを制限する
GlideSystemUserSession スクリプト可能 API へのアクセスを制限する	• 新しい簡単な説明:クライアント呼び出し可能スクリプトインクルードにデフォルトで認証を要求する • 以前の簡単な説明:クライアントコール可能スクリプトインクルードのプライバシー

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ドキュメント	更新
クライアント呼び出し可能スクリプトインクルードにデフォルトで認証を要求する	• 新しい簡単な説明:クライアント呼び出し可能スクリプトインクルードにデフォルトで認証を要求する • 以前の簡単な説明:クライアントコール可能スクリプトインクルードのプライバシー
AJAXGlideRecord ACL チェックが必要	• 新しい簡単な説明:AJAXGlideRecord ACL チェックが必要 • 以前の簡単な説明:AJAXGlideRecord ACL チェックの有効化
クライアント生成スクリプトサンドボックスを強制	• 新しい簡単な説明:クライアント生成スクリプトサンドボックスを強制 • 以前の簡単な説明:クライアント生成スクリプトサンドボックス
CSRF トークンの厳格な検証を強制する	• 新しい簡単な説明:CSRF トークンの厳格な検証を実施する • 以前の簡単な説明:CSRF の厳格検証
アップロードされた MIME タイプを制限する	• 新しい簡単な説明:アップロードされた MIME タイプの制限* 簡単な説明 • 古い簡単な説明:MIME タイプの制限をアップロードする、デフォルト値が TRUE から FALSE に変更されました
スコープ指定された管理者アプリケーション ACL の有効化	• 新しい簡単な説明:Enable Scoped Admin Application ACL • 以前の簡単な説明:Administer Scoped Admin Application ACL
CSRF 対策トークンの有効化	• 新しい簡単な説明:CSRF 対策トークンを有効にする • 古い簡単な説明:Anti-CSRF トークン
x-frame-options: SAMEORIGIN セキュリティヘッダーの実装	• 新しい簡単な説明: Implement the X-Frame-Options: SAMEORIGIN Security ヘッダー • 古い短い説明: X-Frame-Options: SAMEORIGIN

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ドキュメント	更新
モバイルアプリ UI の難読化を必須にする	• 新しい簡単な説明:モバイルアプリ UI の難読化を必須にする • 以前の簡単な説明:モバイルアプリ UI 難読化
空の ACL でデフォルトで拒否	• 新しい簡単な説明:空の ACL でデフォルトで拒否 • 以前の簡単な説明:セキュリティマネージャーのデフォルト拒否
SOAP コンテンツタイプの検証	• 新しい簡単な説明:SOAP コンテンツタイプの検証 • 古い簡単な説明:SOAP コンテンツタイプのチェック
SOAP 要求の厳格なセキュリティの適用	• 新しい簡単な説明:Enforce SOAP Request Strict Security • 以前の簡単な説明:SOAP 要求の厳格なセキュリティ
アカウント復旧の有効化	• 新しい簡単な説明: アカウント復旧の有効化 • 古い簡単な説明:アカウント復旧
allowlistDisable エンティティ拡張による XMLdoc2 エンティティ検証の要求	• 新しい簡単な説明:allowlistDisable エンティティ拡張を使用した XMLdoc2 エンティティ検証の要求 • 古い簡単な説明: allowlistDisable エンティティ拡張を使用した XMLdoc2 エンティティ検証
ドット連結フィールドにドメイン分離を適用する	• 新しい簡単な説明:ドット連結フィールドにドメイン分離を適用する • 以前の簡単な説明:ドメイン分離の適用
ダウンロード可能な MIME タイプを制限する	• 新しい簡単な説明: ダウンロード可能な MIME タイプの制限 • 古い簡単な説明:ダウンロード可能な MIME タイプの拒否リスト

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ドキュメント	更新
制限付きダウンロード可能な MIME タイプを定義する	• 新しい簡単な説明: 制限付きダウンロード可能 MIME タイプの定義 • 古い短い説明: ダウンロード可能な MIME タイプ
Jelly スクリプトをエスケープ	• 新しい簡単な説明:Jelly スクリプトをエスケープ • 古い簡単な説明:Jelly をエスケープする
リストビューで HTML をエスケープする	• 新しい簡単な説明:リストビューで HTML をエスケープ • 以前の簡単な説明:HTML をエスケープ
スクラッチパッド内のスクリプトのエスケープ	• 新しい簡単な説明:スクラッチパッドのエスケープスクリプト • 以前の簡単な説明:Escape Scratchpad
XML マークアップをエスケープする	• 新しい簡単な説明: XML マークアップをエスケープする • 古い簡単な説明:XML のエスケープ
クラシックモバイルアプリ UI の難読化の要求	• 新しい簡単な説明:クラシックモバイルアプリ UI の難読化の要求 • 以前の簡単な説明:クラシックモバイルアプリ UI 難読化
お気に入りへの公開アクセス	• 新しい簡単な説明:お気に入りへのパブリックアクセスを無効にする • 以前の簡単な説明:お気に入りへのパブリックアクセス
セッション Cookie の厳格なセキュリティを適用する	• 新しい簡単な説明: セッション Cookie の厳格なセキュリティを適用する • 古い簡単な説明:セキュアセッションクッキー
埋め込み HTML コードを無効にする	• 新しい簡単な説明:埋め込み HTML コードの無効化 • 以前の簡単な説明:埋め込み HTML コード

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ドキュメント	更新
埋め込み HTML で JavaScript タグを無効にする	• 新しい簡単な説明:埋め込み HTML で JavaScript タグを無効にする • 古い簡単な説明:埋め込み HTML で Javascript タグを許可する
セッションアクティビティのタイムアウト期間を最小化する	• 新しい簡単な説明:セッションアクティビティのタイムアウト期間の最小化 • 以前の簡単な説明:セッションアクティビティのタイムアウト
静的コンテンツでダウンロード可能なファイルタイプを制限する	• 新しい簡単な説明:静的コンテンツでダウンロード可能なファイルタイプを制限する • 古い簡単な説明: 静的コンテンツからのファイルタイプのダウンロード制限
セッションウィンドウのタイムアウト期間の最小化	• 新しい簡単な説明:セッションウィンドウのタイムアウト期間の最小化 • 以前の簡単な説明:セッションウィンドウのタイムアウト
絶対セッションタイムアウト期間の最小化	• 新しい簡単な説明:絶対セッションタイムアウト期間の最小化 • 以前の簡単な説明:絶対セッションタイムアウト
失敗したログインロック解除のタイムアウト期間を最大化	• 新しい簡単な説明:失敗したログインロック解除タイムアウト期間の最大化 • 以前の簡単な説明: ログイン失敗後のロック解除タイムアウトの管理
XML 外部エンティティの制限	• 新しい簡単な説明: XML 外部エンティティの制限 • 以前の簡単な説明:XML エンティティ検証 URL 許可リスト (XML Entity Validation URL Allowlist)
エンティティ拡張しきい値の最小化	• 新しい簡単な説明: エンティティ拡張しきい値の最小化 • 以前の簡単な説明: エンティティ拡張しきい値の設定

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ドキュメント	更新
パスワードリセット要求の有効期限の最小化	• 新しい簡単な説明:パスワードリセット要求の有効期限を最小限に抑える • 以前の簡単な説明:パスワードリセット要求の有効期限
パスワードリセット要求の最大試行許容量を最小化	• 新しい簡単な説明: パスワードリセット要求の最大試行許容量を最小限に抑える • 以前の簡単な説明:パスワードリセット要求の最大試行回数
パスワードリセット要求の最大試行回数ウィンドウ期間を最小化	• 新しい簡単な説明: パスワードリセット要求の最小化 最大試行回数ウィンドウ期間 • 以前の簡単な説明:パスワードリセット要求の最大試行回数ウィンドウ
パスワードリセット要求の再試行期間の最大化	• 新しい簡単な説明: パスワードリセット要求再試行期間の最大化 • 以前の簡単な説明:パスワードリセット要求再試行ウィンドウ
パスワードリセット要求の成功期間を最小化	• 新しい簡単な説明: パスワードリセット要求の成功期間を最小化 • 以前の簡単な説明:パスワードリセット要求の成功ウィンドウ
パスワードリセット要求ロック解除期間の最大化	• 新しい簡単な説明:パスワードリセット要求ロック解除期間の最大化 • 以前の簡単な説明:[パスワードリセット要求のロック解除] ウィンドウ
パスワードリセット SMS の複雑さの最大化	• 新しい簡単な説明:パスワードリセット SMS の複雑さの最大化 • 以前の簡単な説明:パスワードリセット SMS の複雑さ
パスワードリセット SMS の有効期限を最小限に抑える	• 新しい簡単な説明:パスワードリセット SMS の有効期限を最小限に抑える • 以前の簡単な説明:パスワードリセット SMS の有効期限

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ドキュメント	更新
パスワードリセットの 1 日あたりの最大 SMS を最小化	• 新しい簡単な説明:パスワードリセットの 1 日あたりの最大 SMS の最小化 • 以前の簡単な説明:1 日あたりのパスワードリセット SMS の最大数
パスワードリセットの SMS 一時停止期間の最大化	• 新しい簡単な説明:パスワードリセット SMS の一時停止ウィンドウ期間の最大化 • 以前の簡単な説明:パスワードリセット SMS の一時停止ウィンドウ
登録と検証の SMS コード通知を有効にする	• 新しい簡単な説明: 登録と検証の SMS コード通知を有効にする • 以前の簡単な説明:登録と検証の SMS コード通知
パスワードリセット検証の遅延時間の最大化	• 新しい簡単な説明:パスワードリセット検証遅延期間の最大化 • 以前の簡単な説明:パスワードリセットの検証遅延
パスワードのリセット/変更プロセス中にユーザーに通知	• 新しい簡単な説明:パスワードのリセット/変更プロセス中にユーザーに通知 • 以前の簡単な説明:Password Reset/変更通知プロセス
外部ユーザー登録のメールドメインを制限する	• 新しい簡単な説明:外部ユーザー登録用のメールドメインの制限 • 以前の簡単な説明:外部ユーザー登録メールドメインの許可リスト
外部ユーザー登録リンクの有効期限を最小限に抑える	• 新しい簡単な説明:外部ユーザー登録リンクの有効期限の最小化 • 以前の簡単な説明:外部ユーザー登録リンクの有効期限
許可された Java パッケージの制限	• 新しい簡単な説明:許可されたJavaパッケージの制限 • 古い簡単な説明:Java パッケージ許可リスト (Allow list)

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

削除されたハードニング設定

このリストには、ベースラインバージョン 2.0 で Security Center 削除されたハードニング設定が含まれています。

- アプリケーション構成データとスクリプトのコード署名を有効にする
- Glide KMF エンクリプターを有効にする
- インスタンスレベルのエンクリプターの使用を無効にする
- あらゆるアウトバウンド HTTP 要求フィールドをログ記録

アクセス制御

アクセス制御カテゴリは、権限モデルに基づいて要求を許可および拒否することで、権限のないアクセスからリソースを保護するプロセスを監査します。これには、リソースにアクセスするエンティティがそれを行うための有効な資格情報を保持していることの確認、明確に定義されたロールまたは権限のセットの作成および保護、ロールまたは権限のコントロールが再現や改ざんから保護されていることの確認が含まれます。

アクセス制御は、特定のリソースへのアクセスを許可するか拒否するかを決定します。リソースの使用が許可されているユーザーのみに、そのリソースへのアクセスが許可されます。

CSRF 対策トークンの検証時間

glide.security.csrf_previous.time_limit プロパティは、保護トークンが期限切れになるまでの時間 (秒) を指定します。

ユーザーセッションの有効期限が切れると、[期限切れトークンの再利用を許可することを許可する] プロパティが有効になっていない限り、セキュアトークンも期限切れになり、このプロパティで指定された期間内になります。このトークンはクロスサイトリクエストフォージェリ攻撃を防ぐために使用されます。

詳細情報

属性	説明
構成名	*glide.security.csrf_previous.time_limit*
構成タイプ	システムプロパティ (/sys_properties_list.do)
データタイプ	整数
推奨値	
デフォルト値	86,400 秒または 1 日
カテゴリ	アクセス制御
セキュリティリスク	• 重大度スコア：5.3 • CVSS スコア：中 • セキュリティリスクの詳細：このプロパティを推奨値に設定しないと、クロスサイトリクエストフォージェリ攻撃を防ぐために使用されるトークン検証が無効になります。
依存関係と前提条件	なし

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

属性	説明
機能への影響度	このプロパティは、保護トークンが有効な期間を秒単位で決定します。[期限切れトークンの再利用を許可] プロパティが有効になっていて、トークンがこのプロパティで指定された期間内にない限り、ユーザーセッションが期限切れになると、セキュアトークンは期限切れになります。このトークンは、クロスサイトリクエストフォージェリ攻撃を防ぎます。デフォルト値は 86400 秒または 1 日です。

ドット連結フィールドにドメイン分離を適用する

glide.sys.domain.include_domain_condition_on_join プロパティは、ドット連結フィールドのドメイン分離機能を確実に適用するために、結合クエリにドメイン分離条件を指定するかどうかを制御します。

このプロパティ *glide.sys.domain.include_domain_condition_on_join* は、ドット連結フィールドのドメイン分離機能を確実に適用するために、結合クエリにドメイン分離条件を指定するかどうかを制御します。*glide.sys.domain.include_domain_condition_on_join*がドメイン分離を使用するインスタンスで推奨値の true に設定されていない場合、特定のドメインと共有されない機密情報が開示される可能性があります。

注:
Domain Separation プラグインがインストールされるときに、このプロパティの sys_properties レコードがインストールされ、その値は **true** (デフォルト値ではない) に設定されます。それ以外の場合は、Domain Separation がインストールされていないベースシステムにプロパティレコードが存在せず、デフォルト以外の値に設定されます。

警告:
これはセーフハーバープロパティです。つまり、いったん変更したら変えることはできません。元に戻すことはできません。

詳細情報

属性	説明
プロパティ名	*glide.sys.domain.include_domain_condition_on_join*
構成タイプ	システムプロパティ (/sys_properties_list.do)
カテゴリ	アクセス制御
目的	ドット連結フィールドのドメイン分離機能を確実に適用するために、結合クエリにドメイン分離条件を指定するかどうかを制御します。
推奨値	Domain Separation がインストールされている場合は true。それ以外の場合、このプロパティは存在しません。
構成タイプ	ブーリアン
セキュリティリスク	(中) *glide.sys.domain.include_domain_condition_on_join* が推奨値である **true** に設定されていない場合、特定のドメインと共有されない機密情報が公開される可能性があります。
参照	サービスプロバイダーの Domain Separation

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

スコープ指定された管理者アプリケーション ACL の有効化

glide.security.scoped_administration.honor_global_acl は、アプリケーション管理アプリがグローバルアクセス制御リスト (ACL) ルールを継承できるかどうかを決定します。

このプロパティは、スコープ対象の管理アプリケーション ACL がレコードスコープに対して定義されていない場合に特に役立ちます。

アプリケーションへの権限を持つ低い特権のユーザーが機密レコードにアクセスすることを防ぐには、*glide.security.scoped_administration.honor_global_acl* を true に設定します 。

詳細情報

属性	説明
プロパティ名	*glide.security.scoped_administration.honor_global_acl*
構成タイプ	システムプロパティ (/sys_properties_list.do)
カテゴリ	アクセス制御
目的	スコープ対象の管理アプリケーションで ACL アクセスルールを制御します。
推奨値	True (デフォルト)
構成タイプ	ブーリアン
セキュリティリスク	(低) プロパティ値が true で、レコードスコープにスコープ対象の管理アプリケーション ACL が定義されていない場合は、グローバル ACL が優先されます。false に設定すると、レコードスコープにスコープ対象の管理アプリケーション ACL が定義されていない場合、ACL チェックは無視されます。
セキュリティリスク評価	3.8
参照	acl-access-checksAccess control rules in application administration apps

プラグインのアクティブ化の詳細については、「Activate a plugin」を参照してください。

委任開発者に対するアクセスのブロック

この設定は、スクリプトを使用してユーザーロールを更新する委任開発者のアクセスに影響します。設定が準拠している場合、開発者は user_admin ロールなしで sys_user_has_role テーブルのレコードを更新したり挿入したりすることはできません。

このプロパティの値は、インスタンス内の機能への予期しないアクセスを委任開発者が許可できるかどうかに影響します。プロパティにロールが含まれている場合は、そのロールのみがスクリプトのモジュールを実行できます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

詳細情報

属性	説明
プロパティ名	*com.glide.sys.security.delegateddev.block_grant_roles*
構成タイプ	システムプロパティ (/sys_properties_list.do)
カテゴリ	アクセス制御
目的	このプロパティの値は、インスタンス内の機能への予期しないアクセスを委任開発者が許可できるかどうかに影響します。
タイプ	切り替えスイッチ
推奨値	true
セキュリティ依存関係	なし
セキュリティリスク評価	6.7
機能への影響度	(高) delegated_developer ロールを持つユーザーが sys_user_has_role テーブルのレコードを変更しようとすると、その操作に対する追加のセキュリティチェックがこのプロパティによって有効になります。ユーザーが sys_user_has_role テーブルを作成または更新しようとしている場合、user_admin ロールがそのユーザーに付与されていることが追加のセキュリティチェックによって検証されます。ユーザーに user_admin ロールがない場合、アクセスは拒否されます。プロパティが false の場合、これらの追加チェックは検証されません。
セキュリティリスク	(中) 適切な承認がないと、無許可のユーザーがインスタンスの機密コンテンツ/データにアクセスする可能性があります。
参照	アクセス制御

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

期限切れ CSRF トークンのブロック

クロスサイトリクエストフォージェリ攻撃を防ぐために期限切れの CSRF トークンをブロックします。

概要

クロスサイトリクエストフォージェリは、認証されたユーザーに代わって不正なコマンドを実行する悪意のあるエクスプロイトの一種です。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

構成詳細

属性	説明
概要	期限切れのセキュアトークンの使用をコントロールして、受信要求を識別して検証します。以前に期限切れになったトークンを使用して受信要求を検証しないようにするには、**false** に設定します。
構成名	*glide.security.csrf_previous.allow*
構成タイプ	Glide プロパティ：*sys_properties_list.do*
データタイプ	true/false ブーリアン
推奨値	**false**
デフォルト値	**true**
カテゴリ	アクセス制御
セキュリティリスク	重大度スコア：6.5
	CVSS スコアに応じた重大度：中
	セキュリティリスクの詳細：認証された機能を保護するために強力な CSRF 対策メカニズムを適用し、効果的な自動化対策または CSRF 対策で認証されていない機能を保護します。
依存関係と前提条件	なし
参照	CSRF 対策トークンの有効化、 クロスサイトリクエストフォージェリ 。

実行前の UI アクションの条件のチェック

glide.security.strict.actions プロパティを使用して、実行前にフォームおよびリスト内の UI アクションの条件を確認できるようにします。このプロパティを true に設定すると、実行前にテーブル UI アクションに検証レイヤーが追加されます。

詳細情報

属性	説明
プロパティ名	*glide.security.strict.actions*
構成タイプ	システムプロパティ (/sys_properties_list.do)
カテゴリ	アクセス制御
目的	実行前にテーブル UI アクションに検証レイヤーをさらに追加すること
推奨値	true
セキュリティリスク評価	3.3

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

属性	説明
機能への影響度	(低) この修正では、インスタンスのターゲットテーブル/ページで UI アクションをチェックするための検証レイヤーが追加されるだけです。アクセス制御が顧客インスタンスで適切に設定されているかぎり、ここに影響はありません。
セキュリティリスク	(低) 2 つのゾーンの間でトランザクションが発生した場合は常に、アクセス要求がチェックされます。この操作により、エンドユーザーに対してフォームがレンダリングされる前に UI アクションが検証されます。
参照	高セキュリティプラグイン

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

明示的な外部ロールへの内部アクセスを拒否する

複数のプロパティが組み合わされて、明示的なロールの内部拒否リストの有効化の強化設定が構成されます。*glide.security.explicit_roles.enable_internal_user_blacklist* プロパティは、外部ユーザーに snc_internal ロールがアサインされないようにします。snc_external ロールをアサインするには、*glide.security.explicit_roles.internal_user_blacklist* プロパティを有効にします。

Glide.security.explicit_roles.enable_internal_user_blacklist

内部ユーザーと外部ユーザーの両方に、インスタンスへのアクセス権を与えることができます。セキュリティを強化するためには、すべてのユーザーに少なくとも 1 つのロールをアサインして、インスタンスが内部ユーザーと外部ユーザーを区別できるようにする必要があります。

snc_external ロールを割り当てる機能を有効にするには、*glide.security.explicit_roles.enable_internal_user_blacklist* プロパティを推奨値である **true** に設定します。

snc_external ロールを割り当てる機能を無効にするには、値を **false** に設定します。すべてのユーザーにデフォルトで snc_internal ロールが割り当てられます。

注:
明示的なロールがインストールされていないインスタンスは影響を受けません。Paris リリース以降、明示的なロールの新規インストールでは、プロパティにはデフォルト値 true が指定されます。

詳細情報

属性	説明
プロパティ名	*glide.security.explicit_roles.enable_internal_user_blacklist*
構成タイプ	システムプロパティ (/sys_properties_list.do)
カテゴリ	アクセス制御
目的	snc_internal ロールの代わりに、指定されたユーザークラスを snc_external ロールに割り当てることができます。
推奨値	True (デフォルト)。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

属性	説明
構成タイプ	ブーリアン。
セキュリティリスク	(中) プロパティを無効にすると、不適切なデフォルトのロールが割り当てられる可能性があります。
セキュリティリスク評価	5.4
参照	CSM 内の明示的なロール、

Glide.security.explicit_roles.internal_user_blacklist

glide.security.explicit_roles.internal_user_blacklist 値は、snc_internal ロールの代わりに snc_external ロールを割り当てる必要があるユーザークラス (sys_user を拡張するテーブル) を決定します。デフォルト値 csm_consumer_user,customer_contact は、Customer Service Management プラグインのユースケースに合わせて定義されています。

snc_internal ロールではなく、デフォルトで snc_external ロールをアサインする必要がある追加のまたは異なるユーザークラスがある場合にのみ、このプロパティ値を変更する必要があります。これらの値を変更するには、サポートにお問い合わせください。

属性	説明
プロパティ名	*glide.security.explicit_roles.internal_user_blacklist*
構成タイプ	システムプロパティ (/sys_properties_list.do)
カテゴリ	アクセス制御
目的	snc_internal ロールの代わりに、デフォルトでアサインされる snc_external ロールのアサインを許可します。
推奨値	*csm_consumer_user*、*customer_contact*
構成タイプ	文字列
機能への影響度	
セキュリティリスク	(中) プロパティを無効にすると、不適切なデフォルトのロールが割り当てられる可能性があります。
セキュリティリスク評価	5.4
参照	明示的なロール、外部ユーザーのロールのアサインの修正

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

要求アイテムへの不正アクセスの拒否

glide.sc.req_for.roles.default プロパティは、*retrieveAddress* API のデフォルトの動作を定義します。

このプロパティは、*glide.sc.req_for.roles* に値がない場合にのみ機能します。*glide.sc.req_for.roles* に値がある場合、このプロパティは重要ではなく、定義されたロールのみを持つユーザーに API へのアクセス権が付与されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

詳細情報

属性	説明
プロパティ名	*glide.sc.req_for.roles.default*
構成タイプ	システムプロパティ (/sys_properties_list.do)
カテゴリ	アクセス制御
目的	プロパティでロールが指定されていない場合、特権のないログインユーザーが、クライアントコール可能スクリプトインクルード *ScriptServiceCatalogGetLocation* を呼び出して、システム内の他のユーザーのアドレスを取得できます。このプロパティは、この API が特権のないユーザーに公開されるのを防ぎます。
推奨値	拒否 (デフォルト)
構成タイプ	選択リスト (許可 | 拒否)
セキュリティリスク	(中) *glide.sc.req_for.roles.default* が推奨値 **deny** (許可) に設定されておらず、*glide.sc.req_for.roles* の値が空の場合、どのユーザーも他のユーザーのアイテムを要求できるようになり、不正なリソースアクセスが許可されます。
参照	クライアントコール可能スクリプトインクルード

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

CSRF 対策トークンの有効化

glide.security.use_csrf_token プロパティを使用して、受信要求の識別および検証に保護トークンが使用されるようにします。このトークンは、これらの攻撃を防止するために使用されます。

クロスサイト要求偽造 (CSRF) は、エンドユーザーが現在認証されている Web アプリケーションで不要なアクションを実行するように強制する攻撃です。CSRF 攻撃は、データの盗難ではなく、ステータス変更の要求を明確にターゲットにしています。これは、攻撃者に偽造要求に対する応答を確認する方法がないからです。

次のプロパティを有効にすると、CSRF トークンを制御できます。

- *glide.security.csrf_previous.time_limit*
- *glide.security.csrf_previous.allow*
- *glide.security.csrf.strict.validation.mode*

詳細情報

属性	説明
プロパティ名	*glide.security.use_csrf_token*
構成タイプ	システムプロパティ (/sys_properties_list.do)
カテゴリ	アクセス制御

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

属性	説明
目的	CSRF 攻撃の可能性からアプリケーションを保護すること
セキュリティリスク評価	8.1
推奨値	true
機能への影響度	(低) この修正により、インスタンスユーザーがインスタンスへの書き込み要求を送信する前に、追加の検証手順が有効になります。すべての書き込み要求には、CSRF トークン (つまりユーザーセッションに関連付けられた検証/CSRF ID) が含まれています。ユーザーセッションが期限切れになると、セキュアトークンも期限切れになります。
セキュリティリスク	(高) クロスサイト要求偽造は、インスタンスデータの完全性を侵害する重大なセキュリティリスクです。攻撃者は、インスタンスユーザーの信頼を悪用して CSRF 攻撃を開始することができます。ソーシャルエンジニアリング攻撃を利用して、ユーザーがインスタンスで攻撃者の代わりに誤った要求を送信する可能性があります。

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

アーカイブテーブル **ACL** のチェック

このプロパティは *glide.security.enable_archive_table_acls* 、元のテーブル (アーカイブテーブルの作成元のテーブル) のアクセス制御リスト (ACL) を false と評価するかどうかを制御します。

*glide.security.enable_archive_table_acls*元のテーブルの ACL はその値に関係なく評価されるため、このプロパティを false に設定しないでください。アーカイブテーブルの追加の ACL は、追加しないことで回避できます。

詳細情報

属性	説明
構成名	*glide.security.enable_archive_table_acls*
構成タイプ	システムプロパティ (/sys_properties_list.do)
データタイプ	ブーリアン
推奨値	true
デフォルト値	true
カテゴリ	アクセス制御
セキュリティリスク	• 重大度スコア：3 • CVSS スコア：低 • セキュリティリスクの詳細:プロパティが false に設定されている場合、アーカイブされたテーブルに追加された ACL は無視されます。これは直感に反するアクションであるため、認証バイパスにつながる可能性があります。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

属性	説明
依存関係と前提条件	なし
機能への影響	このプロパティが true に設定されている場合、アーカイブテーブルのアクティブな読み取り ACL がすべて受け入れられます。アクティブな読み込み ACL が存在しないか、プロパティが false に設定されている場合、元のテーブル (データのアーカイブ元のテーブル) がアーカイブテーブルに適用されます。 **注:** アーカイブテーブルでは読み取り ACL のみがサポートされます。アーカイブテーブルに対するその他の操作は、アクセスハンドラーによって内部的に制御されます。

Contextual Security プラグインの有効化

Contextual Security プラグイン (*com.glide.role_management*) のアクティブ化によりコンテキストセキュリティが有効になり、作成、読み取り、書き込み、および削除機能を使用してレコード/情報が保護されます。

インストールしてアクティブ化すると、(簡易セキュリティマネージャーによって作成された) dictionary ロールはテストされなくなります。代わりに、Now Platform はフィールドとテーブルの ACL ルールを検索します。また、シンプルなセキュリティマネージャーによって実装される従来のロールベースの辞書ルールではなく、ACL ルールを使用してデータを保護します。辞書フォームを設定して辞書エントリにロールを追加しても、権限は変更されません。

詳細情報

属性	説明
プラグイン ID	*com.glide.role_management*
構成タイプ	[システム定義] > [プラグイン]
カテゴリ	アクセス制御
目的	シンプルなセキュリティマネージャーとは異なり、コンテキストセキュリティマネージャーはシステムテーブル階層を認識しています。階層内の表示場所に基づいて、1 つのフィールドに複数の異なるセキュリティルールを設定できます。
推奨値	アクティブ (デフォルトでアクティブ化されたプラグイン)
セキュリティリスク評価	8.1
機能への影響度	(中) この修正では、アクセス制御の機能レベルが適用されます。これにより、アプリケーションは ACL テーブルのみに基づいてアクセス制限を決定できます。
セキュリティリスク	(高) CRUD 操作を実行する前に、サーバー側から機能レベルのアクセス制御を適用し、インスタンスユーザーに適切なレベルのアクセスを確保する必要があります。
参照	コンテキスト依存セキュリティマネージャー

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

プラグインのアクティブ化の詳細については、「Activate a plugin」を参照してください。

AJAXGlideRecord ACL チェックの有効化 (インスタンスセキュリティ強化)

glide.script.secure.ajaxgliderecord プロパティを使用して、クライアントスクリプト内で GlideAjax API を使用してサーバー側のレコード (テーブルなど) にアクセスする場合にアクセス制御リスト (ACL) ルール検証を実行します。

クライアントスクリプトから、AJAXGlideRecord (GlideAjax -クライアント) API。サーバー側の Glide レコードなどの構文を使用します。多くの展開で、これは強力で便利なツールです。

アクセス制御リスト (ACL) を GlideAjax API 呼び出しに適用することを選択すると、現在接続しているユーザーがアクセスできるデータのみをクエリーできます。たとえば、cmn_location テーブルを読み取る権限のない ESS ユーザーがログインすると、そのテーブルに対する GlideAjax API 呼び出しは失敗します。

Now Platform が GlideAjax ACL 呼び出しのチェックなしで実行されている場合、API は、現在ログインしているユーザーが他の方法ではアクセスできない情報を返す可能性があります。

詳細情報

属性	説明
プロパティ名	glide.script.secure.ajaxgliderecord
構成タイプ	システムプロパティ (/sys_properties_list.do)
Instance Security Center での構成	あり
目的	クライアント側 API を介してレコードにアクセスする場合でも、セキュリティ ACL が確実にチェックおよび検証されるようすること
推奨値	true
機能への影響度	(高) この修正では、AJAXGlideRecord API 呼び出しを使用して要求が行われた場合に、サーバー側レコードとの ACL 関係が適用されます。ACL 構成が適切に設定されていない場合、影響を受ける可能性があります。影響度とその識別方法の詳細については、「クライアント側 GlideRecord (AJAXGlideRecord) トランザクションの監査とレビューに関する記事 [KB0550828] (HI ナレッジベース で入手可能)」を参照してください。
セキュリティリスク	(高) クライアントスクリプトを使用すると、GlideAjax API を介してサーバーから任意のデータをクエリーできます。サーバー側のリソースには適切な承認なしでアクセスできるため、ACL 検証を使用すると、アプリケーションで設定された承認に基づいて要求を検証するのに役立ちます。
ワークアラウンド	GlideAjax (AJAXGlideRecord) API で使用されるスクリプトインクルード、プロセッサー、およびその他のエンティティに対して適切な ACL が作成され、適切な承認の下で実行されるようにします。 canRead ()、canWrite ()、canCreate ()、canDelete () などのメソッドを実装して、GlideRecord を使用してテーブ

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

属性	説明
	ルレコードにアクセスする前に、ユーザーの承認を実行します。 もう 1 つの方法は、GlideRecordSecure を使用することです。このクラスは GlideRecord サーバーから継承され、GlideRecord と同じ関数を実行し、ACL も適用します。
参照	ACL を AJAXGlideRecord (クライアント側の Glide レコード) に追加 このプロパティは、クライアントからのスクリプトの実行を保護および制限するプロパティと同じファミリーに属します。 • *glide.script.use.sandbox*：「クライアント生成スクリプトサンドボックス」を参照 • *glide.script.allow.ajaxevaluate*：「AJAXEvaluate を有効にする」を参照

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

CSRF トークンの厳格な検証を強制する

glide.security.csrf.strict.validation.mode プロパティを使用して、CSRF トークンの厳格検証を有効にします。CSRF トークンが一致しない場合、要求は再送信されません。

このプロパティは *glide.security.csrf.strict.validation.mode* 、CSRF トークンの再利用を防止する CSRF トークンの厳格な検証を有効にします。このプロパティが推奨値の true に設定されていない場合、CSRF トークンが再利用され、CSRF 攻撃への扉が開かれる可能性があります。

詳細情報

属性	説明
プロパティ名	*glide.security.csrf.strict.validation.mode*
構成タイプ	システムプロパティ (/sys_properties_list.do)
カテゴリ	アクセス制御
目的	CSRF トークンの厳格検証を適用し、再利用を防止すること
推奨値	true
セキュリティリスク評価	(中) クロスサイト要求偽造は、インスタンスデータの完全性を侵害する重大なセキュリティリスクです。攻撃者は、インスタンスユーザーの信頼を悪用して、どのインスタンスユーザーにでも CSRF 攻撃を開始することができます。ソーシャルエンジニアリング攻撃を利用して、ユーザーが攻撃者の代わりにインスタンスに対して誤った要求を送信する可能性があります。
機能への影響度	(中) この修正により、インスタンスユーザーがインスタンスへの書き込み要求を送信する前に、追加の検証手順が有

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

属性	説明
	効になります。現在の CSRF トークンが以前に使用されたかどうかをチェックします。[はい] の場合、以降の書き込み要求は送信されません。
セキュリティリスク	(中) クロスサイト要求偽造は、インスタンスデータの完全性を侵害する重大なセキュリティリスクです。攻撃者は、インスタンスユーザーの信頼を悪用して、どのインスタンスユーザーにでも CSRF 攻撃を開始することができます。ソーシャルエンジニアリング攻撃を利用して、ユーザーが攻撃者の代わりにインスタンスに対して誤った要求を送信する可能性があります。

ラップされたキーをアップロードするには 顧客指定のキーの設定とアップロード に戻ります。

委任開発者の読み取りアクセスを制限する

com.glide.dd_allow_global_access_tables に wf_activity、wf_activity_definition、wf_workflow、wf_workflow_version、sp_portal、sp_widget、sp_page の推奨値が含まれていない場合、これらのテーブルは委任開発者によって読み取られる可能性があります。これにより、機密情報への委任開発者の読み取りアクセスが提供される可能性があります。

詳細情報

属性	説明
プロパティ名	*com.glide.dd_allow_global_access_tables*
構成タイプ	システムプロパティ (/sys_properties_list.do)
データタイプ	文字列
カテゴリ	アクセス制御
推奨値	wf_activity、wf_activity_definition、wf_workflow、wf_workflow_versio

自動翻訳

ロックアウトされたユーザーの受信メールを無効にする

glide.pop3.process_locked_out プロパティを使用して、ロックアウトされたアクティブなユーザーの受信メールアクションを制御します。

ロックアウトされたユーザーの受信メールを無効にするには、このプロパティを **false** に設定します。

> **注:**
> 信頼できないドメインのユーザーからのメールによる受信メールアクションのトリガーを許可する前に、それらのユーザーを許可する場合のセキュリティへの影響とユーザーがロックアウトされている理由を検討してください。

詳細情報

属性	説明
プロパティ名	*glide.pop3.process_locked_out*
構成タイプ	システムプロパティ (/sys_properties_list.do)

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

属性	説明
カテゴリ	アクセス制御
目的	このプロパティは、ロックアウトされているユーザーの受信メールアクションを制御します。
推奨値	False
構成タイプ	ブーリアン
セキュリティリスク	(高) このプロパティを **true** に設定した場合、ロックされたアカウントを持つユーザーが受信メールを受信するため、情報が公開される可能性があります。
セキュリティリスク評価	7.5

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

受信トランザクションを再確認する

glide.security.strict.updates プロパティを使用して、フォームの送信時に受信トランザクションのセキュリティのダブルチェックを有効にします。このプロパティを **true** に設定すると、フォームがブラウザーでレンダリングされる前に、テーブル検証レイヤーがさらに追加されます。

詳細情報

警告:
これはセーフハーバープロパティです。つまり、いったん変更したら変えることはできません。元に戻すことはできません。

属性	説明
プロパティ名	*glide.security.strict.updates*
構成タイプ	システムプロパティ (/sys_properties_list.do)
カテゴリ	アクセス制御
目的	ブラウザーでフォームを表示する前に、ユーザー権限の検証レイヤーを確実に追加すること
推奨値	true
セキュリティリスク評価	8.1
機能への影響度	(低) この修正では、インスタンスのターゲットテーブル/ページでユーザー権限をチェックするための検証レイヤーが追加されます。アクセス制御が顧客インスタンスで適切に設定されているかぎり、影響はありません。
セキュリティリスク	(高) 2 つのゾーンの間でトランザクションが発生した場合は常に、アクセス要求をチェックする必要があります。この操作では、フォームが要求されたとき、およびフォームがレンダリングされる前に、権限がチェックされます。
参照	セキュリティ設定プロパティ

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ACL を有効にしてライブプロファイルの詳細を制御する

glide.live_profile.details プロパティを使用して、ユーザーがライブプロファイルのすべての詳細フィールド (会社名や電話番号など) を表示できるようにするかどうかを指定します。

glide.live_profile.details プロパティの設定に応じて、以下が発生します。

- 値が [表示] に設定されている場合、ユーザープロファイルに対して作成された ACL に関係なく、ライブプロファイル情報へのアクセスが許可されます。
- 値が [ACL] に設定されている場合、ユーザープロファイルに対して作成された ACL に応じて、ライブプロファイル情報へのアクセスが制限されます。
- 値が [非表示] に設定されている場合、ユーザープロファイルに対して作成された ACL に関係なく、ライブプロファイル情報へのアクセスが制限されます。

詳細情報

属性	説明
プロパティ名	*glide.live_profile.details*
構成タイプ	システムプロパティ (/sys_properties_list.do)
カテゴリ	アクセス制御
目的	目的は、許可されたユーザーのみがライブプロファイルの詳細 (会社名、電話番号など) にアクセスできるようにすることです。
推奨値	ACL
セキュリティリスク評価	4.3
機能への影響度	(中) プロパティが有効になっていない場合、無許可のユーザーが他のすべてのユーザーのライブプロファイルの詳細にアクセスできます。
セキュリティリスク	(中) API 要求は常にテーブル ACL を優先する必要があります。無許可のユーザーがライブプロファイルの詳細にアクセスするのを防ぐために、制限を適用する必要があります。

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

レポートビュー ACL の有効化

公開されたレポートの report_view ACL のチェックを管理します。

glide.report.report_view.check_published プロパティを使用して、公開されたレポートの report_view ACL のチェックを管理します。このプロパティが推奨値の **true** に設定されていない場合、公開されたレポートの report_view ACL のチェックはオフになります。

警告:
これはセーフハーバープロパティです。つまり、いったん変更したら変えることはできません。元に戻すことはできません。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

詳細情報

属性	説明
構成名	*glide.report.report_view.check_published*
構成タイプ	システムプロパティ (/sys_properties_list.do)
データタイプ	ブーリアン
推奨値	true
デフォルト値	true
カテゴリ	アクセス制御
セキュリティリスク	• 重大度スコア：高 • CVSS スコア：7.5 • セキュリティリスクの詳細：このプロパティが推奨値の **true** に設定されている場合、公開されたレポートの report_view ACL のチェックはオフになります。
依存関係と前提条件	なし

クロスオリジン **iFrame** 通信の **URL** 許可リストを有効にする

glide.ui.concourse.onmessage_enforce_same_origin プロパティを使用して、iframe 間のクロスオリジン通信を有効にします。

Openframe は、*glide.ui.concourse.onmessage_enforce_same_origin_whitelist* プロパティで指定された信頼できるドメインからのメッセージのみ処理できます。詳細については、「Specify UTL allow list for cross-origin iframe communication (クロスオリジン iframe 通信の UTL 許可リストを指定する)」を参照してください。

詳細情報

属性	説明
プロパティ名	*glide.ui.concourse.onmessage_enforce_same_origin*
構成タイプ	システムプロパティ (/sys_properties_list.do)
カテゴリ	アクセス制御
目的	信頼できるドメインの包含リストを有効にし、OpenFrame の iframe 間で通信できるようにすること
推奨値	true
セキュリティリスク評価	4.2
機能への影響度	(中) 意図したドメインを包含リストに含めない場合、Now Platform インスタンス内に他のページを埋め込む機能が制限されることがあります。
セキュリティリスク	(高) Web ページに適切な作成元検証を実行しないイベントハンドラーが含まれている場合、任意の作成元からの Web ページまたはスクリプトは、その Web ページと通信

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

属性	説明
	できます。また、イベントハンドラーによって実行される機能を開始することもできます。
参照	OpenFrame の概要

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

ロールレス ACL の認証の適用

*glide.security.enforce_auth_roleless_acl*このプロパティを使用して、認証されたユーザーのみが空の ACL のチェックに合格するようにします。

glide.security.enforce_auth_roleless_acl プロパティが true に設定されていない場合、GlideRecordSecure は、データを保護する基になるアクセス制御リスト (ACL) にロールや条件がない場合に、未認証ユーザーにアクセス権を付与します。

多くの場合、ACL は、インスタンス上のすべての認証済みユーザーにアクセス権を付与することを意図している開発者によって空白のままになります。これは、すべてのユーザーが空の ACL のチェックに合格することを意味します。このプロパティにより、認証されたユーザーのみが空の ACL のチェックに合格するようになります。未認証ユーザーにアクセスを許可するには、公開ロールを明示的に使用する必要があります。

詳細情報

属性	説明
構成名	*glide.security.enforce_auth_roleless_acl*
構成タイプ	システムプロパティ (/sys_properties_list.do)
データタイプ	ブーリアン
推奨値	true
デフォルト値	false
カテゴリ	アクセス制御
セキュリティリスク	• 重大度スコア：7.5 • CVSS スコア：高 • セキュリティリスクの詳細：このプロパティが true に設定されていない場合、機密性に影響を与える未認証のデータ漏洩が発生する可能性があります。
依存関係と前提条件	なし

アプリケーションスコープ制限の適用

glide.record.legacy_cross_scope_access_policy_in_script プロパティを使用して、スコープ対象アプリの権限をコントロールします。

glide.record.legacy_cross_scope_access_policy_in_script プロパティが true に設定されている場合、スコープ対象アプリは、グローバルアプリのみが使用できるはずの API を呼び出すことができます。このプロパティは、これらのスコープ対象アプリの開発者を作成および更新するための意図されたアクセス制御をバイパスします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

詳細情報

属性	説明
構成名	*glide.record.legacy_cross_scope_access_policy_in_script*
構成タイプ	システムプロパティ (/sys_properties_list.do)
データタイプ	ブーリアン
推奨値	true
デフォルト値	false
カテゴリ	アクセス制御
セキュリティリスク	• 重大度スコア：3.5 • CVSS スコア：低 • セキュリティリスクの詳細：このプロパティが推奨値に設定されていない場合、スコープ対象アプリとそれらのスコープ対象アプリの委任開発者は、インシデントなどのグローバルテーブルのレコードを作成および更新できます。
依存関係と前提条件	なし

共有ダッシュボードへのセキュリティルールの適用

*glide.cms.dashboards.sharing_with_secure_search*このプロパティを使用して、ユーザーがダッシュボードを共有できるかどうかを制御します。

プロパティが *glide.cms.dashboards.sharing_with_secure_search***true** に設定されていない場合、ユーザーはアクセス権のないダッシュボード グループとロールを共有できます。このプロパティを有効にすると、ダッシュボード共有プロセス中にsys_user、sys_user_role、およびsys_user_groupテーブルを検索するときにアクセス制御リスト (ACL) が適用されます。ダッシュボードを過度に共有すると、ユーザー、グループ、またはロールが、表示する権限を持たないデータにアクセスし、機密情報が侵害される可能性があります。したがって、*glide.cms.dashboards.sharing_with_secure_search* を true に設定して、適切な権限を持つユーザーとのみダッシュボードが共有されるようにすることをお勧めします。

詳細情報

属性	説明
構成名	*glide.cms.dashboards.sharing_with_secure_search*
構成タイプ	システムプロパティ (/sys_properties_list.do)
データタイプ	ブーリアン
推奨値	true
デフォルト値	false
カテゴリ	アクセス制御

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

属性	説明
セキュリティリスク	• 重大度スコア：3.5 • CVSS スコア：低 • セキュリティリスクの詳細：このプロパティを推奨値の true に設定しないと、sys_user、sys_user_role、および sys_user_group テーブルの検索時にアクセス制御リストは適用されません。これにより、ダッシュボードが許可されていないユーザーと共有され、機密情報が公開される可能性があります。
依存関係と前提条件	なし
参照	Access control
機能への影響度	このプロパティは、ダッシュボードを共有すると表示されるユーザーのリスト、ユーザーグループ、およびロールにセキュリティルールを適用します。

Public Sector Digital Services のスコープセキュリティの適用

*glide.enforce_security_scope.sn_gsm*このプロパティを使用して、Public Sector Digital Services アプリケーションからのアプリケーションデータへのアクセス方法を制御します。

この ServiceNow 公共機関デジタルサービス アプリケーションを使用すると、構成員、ビジネス、および機関にデジタルサービスを提供する公共部門アプリケーションを開発できます。

が *glide.enforce_security_scope.sn_gsm* false に設定されている場合、Public Sector Digital Services アプリのグローバルテーブル内のアプリケーションデータへのアクセスは、それらのグローバルテーブルのアクセス制御リスト (ACL) に基づいてアクセス可能です。このプロパティが true に設定されている場合、グローバルテーブルに存在するデータへのアクセスは、Public Sector Digital Services アプリで直接出荷される ACL に基づいてのみ評価されます。このプロパティを false に設定すると、過度に寛容な ACL から情報が開示される可能性があります。

このセキュリティリスクを修復するには、*glide.enforce_security_scope.sn_gsm* を true に設定します。

詳細情報

属性	説明
構成名	*glide.enforce_security_scope.sn_gsm*
構成タイプ	システムプロパティ (/sys_properties_list.do)
データタイプ	ブーリアン
推奨値	true
デフォルト値	true
カテゴリ	アクセス制御

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

属性	説明
セキュリティリスク	• 重大度スコア：4.2 • CVSS スコア：中 • セキュリティリスクの詳細：このプロパティを推奨値に設定しないと、過剰な許容度の ACL により情報が開示される可能性があります。
依存関係と前提条件	なし
参照	

情報要求 **Playbook** のスコープ付き **ACL** アクセスを強制する

glide.enforce_security_scope.sn_gsm_info_req プロパティを使用して、Information Request Playbook 機能の Playbook データへのアクセスを制御します。

このアプリケーションを使用すると、公共部門のエンドユーザーは Information Request Playbook 、公開記録要求を送信および追跡できます。さらに、これらの要求を処理および解決するための事前定義されたプロセスを政府機関に提供します。true *glide.enforce_security_scope.sn_gsm_info_req* に設定されていない場合、情報要求 Playbook アプリケーションの Playbook データに予期しないアクセスが許可される可能性があります。アクセスを許可するときに sn_gsm_info_req スコープからの ACL のみを考慮するには、このプロパティを true に設定します。

詳細情報

属性	説明
構成名	*glide.enforce_security_scope.sn_gsm_info_req*
構成タイプ	システムプロパティ (/sys_properties_list.do)
データタイプ	ブーリアン
推奨値	true
デフォルト値	true
カテゴリ	アクセス制御
セキュリティリスク	• 重大度スコア：7.3 • CVSS スコア：中 • セキュリティリスクの詳細:このプロパティが false に設定されている場合、スコープマスターテーブルの Playbook データへのアクセスを許可するときに、すべてのスコープの ACL が考慮されます。これにより、Information Request Playbook データが公開されます。
依存関係と前提条件	なし

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

属性	説明
参照	• Using Information Request Playbook • Configure Information Requests service channel

厳格な特権昇格の適用

*glide.security.strict_elevate_privilege*このプロパティを使用して、ユーザーにロールの機能を付与するために、特権としてマークされたロールを手動で昇格する必要があるかどうかを制御します。

特権ユーザーがロールを昇格させたときにセキュリティ検証のレイヤーを追加するには、このプロパティを true に設定します。

詳細情報

属性	説明
構成名	*glide.security.strict_elevate_privilege*
構成タイプ	システムプロパティ (/sys_properties_list.do)
データタイプ	ブーリアン
推奨値	true
デフォルト値	true
カテゴリ	アクセス制御
セキュリティリスク	• 重大度スコア：6.7 • CVSS スコア：中 • セキュリティリスクの詳細: *glide.security.strict_elevate_privilege* false に設定すると、特権としてマークされたロールは、管理者ユーザーの新しいセッション時に自動的に昇格され、手動で昇格する必要はありません (security_adminを除く)。
依存関係と前提条件	なし
機能への影響度	このプロパティでは、必要に応じて権限を昇格するには、必ず「admin」ロールユーザーである必要があります。

AJAXGlideRecord ACL チェックが必要

glide.script.secure.ajaxgliderecord プロパティを使用して、クライアントスクリプト内で GlideAjax API を使用してサーバー側のレコード (テーブルなど) にアクセスする場合にアクセス制御リスト (ACL) ルール検証を実行します。

クライアントスクリプトから、AJAXGlideRecord (GlideAjax -クライアント) API。サーバー側の Glide レコードなどの構文を使用します。多くの展開で、これは強力で便利なツールです。

アクセス制御リスト (ACL) を GlideAjax API 呼び出しに適用することを選択すると、現在接続しているユーザーがアクセスできるデータのみをクエリーできます。たとえば、cmn_location テーブル

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

を読み取る権限のない ESS ユーザーがログインすると、そのテーブルに対する GlideAjax API 呼び出しは失敗します。

Now Platform が GlideAjax ACL 呼び出しのチェックなしで実行されている場合、API は、現在ログインしているユーザーが他の方法ではアクセスできない情報を返す可能性があります。

⚠ 警告:
これはセーフハーバープロパティです。つまり、いったん変更したら変えることはできません。元に戻すことはできません。

詳細情報

属性	説明
プロパティ名	*glide.script.secure.ajaxgliderecord*
構成タイプ	システムプロパティ (/sys_properties_list.do)
カテゴリ	アクセス制御
目的	クライアント側 API を介してレコードにアクセスする場合でも、セキュリティ ACL が確実にチェックおよび検証されるようすること
推奨値	true
セキュリティリスク評価	8.1
機能への影響度	(高) この修正では、AJAXGlideRecord API 呼び出しを使用して要求が行われた場合に、サーバー側レコードとの ACL 関係が適用されます。ACL 構成が適切に設定されていない場合、影響を受ける可能性があります。影響度とその識別方法の詳細については、「クライアント側 GlideRecord (AJAXGlideRecord) トランザクションの監査とレビューに関する記事 [KB0550828] (HI ナレッジベース で入手可能)」を参照してください。
セキュリティリスク	(高) クライアントスクリプトを使用すると、GlideAjax API を介してサーバーから任意のデータをクエリーできます。サーバー側のリソースには適切な承認なしでアクセスできるため、ACL 検証を使用すると、アプリケーションで設定された承認に基づいて要求を検証するのに役立ちます。
ワークアラウンド	GlideAjax (AJAXGlideRecord) API で使用されるスクリプトインクルード、プロセッサー、およびその他のエンティティに対して適切な ACL が作成され、適切な承認の下で実行されるようにします。 canRead ()、canWrite ()、canCreate ()、canDelete () などのメソッドを実装して、GlideRecord を使用してテーブルレコードにアクセスする前に、ユーザーの承認を実行します。 もう 1 つの方法は、GlideRecordSecure を使用することです。このクラスは GlideRecord サーバーから継承され、GlideRecord と同じ関数を実行し、ACL も適用します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

属性	説明
参照	ACL を AJAXGlideRecord (クライアント側の Glide レコード) に追加 このプロパティは、クライアントからのスクリプトの実行を保護および制限するプロパティと同じファミリーに属します。 • *glide.script.use.sandbox*：「クライアント生成スクリプトサンドボックス」を参照 • *glide.script.allow.ajaxevaluate*：「AJAXEvaluate を有効にする」を参照

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

GlideRecordSandbox でのフィールドレベル ACL の適用

インスタンスの GlideRecordSandbox でフィールドレベルの ACL を管理します。

glide.sandbox.fields.check_acl プロパティを使用して、GlideRecordSandbox でフィールドレベルの ACL を適用します。このプロパティが適用される例としては、*sysparm_query* のようにユーザーがスクリプトを提供できる場合が挙げられます。このプロパティが推奨値の **true** に設定されていない場合、ACL 制限がバイパスされ、権限のないユーザーによって、*sys_user.user_password* などの機密データが侵害される可能性があります。

警告:
このプロパティの値は、DB なしのオーバーライドです。変更またはオーバーライドすることはできません。

詳細情報

属性	説明
構成名	*glide.sandbox.fields.check_acl*
構成タイプ	システムプロパティ (/sys_properties_list.do)
データタイプ	ブーリアン
推奨値	true
デフォルト値	true
カテゴリ	アクセス制御
セキュリティリスク	• 重大度スコア：7.5 • CVSS スコア：高 • セキュリティリスクの詳細：このプロパティを **false** に設定すると、ACL 制限がバイパスされ、機密データが公開される可能性があります。
依存関係と前提条件	なし

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

資格情報エイリアスの使用を強制

MID Server のプロパティを設定して資格情報を不正使用から保護する方法について説明します。

管理、計測、検出 (MID) サーバーは、ローカルネットワーク上で Windows のサービスまたは UNIX のデーモンとして動作する Java アプリケーションです。MID Server のプロパティは [ecc_agent_property] テーブルにリストされます。インスタンスでそれらにアクセスするには、次の場所に移動します。 **MID** サーバー > プロパティ. 資格情報エイリアスを使用すると、管理者は検出スケジュールで特定の資格情報を使用できます。資格情報エイリアスを使用すると、Discovery テーブルで使用できる資格情報をより詳細に制御できます。このセキュリティの脆弱性を修復するには、厳格な設定を設定して、 *alias_filtering_behavior* 昇格された権限を持つ資格情報が不必要に公開されないようにします。詳細は、「MID Server properties」を参照してください。

詳細情報

属性	説明
構成名	*alias_filtering_behavior*
構成タイプ	システムプロパティ (/sys_properties_list.do)
データタイプ	文字列
推奨値	strict
デフォルト値	緩い
カテゴリ	アクセス制御
セキュリティリスク	• 重大度スコア: 2 • CVSS スコア：低 • セキュリティリスクの詳細：このハードニング設定が「厳格 (strict)」に設定されていない場合、Discovery テーブルのエイリアスに関係なくすべての資格情報が使用されるため、不正アクセスの可能性が高まります。
依存関係と前提条件	なし
参照	• MID Server • Discovery の資格情報エイリアス

GroupBy ACL の適用

groupby 列の ACL チェックを実施するようにインスタンスを構成します。

このプロパティを使用して、groupby 列の ACL チェックを実施するようにインスタンスを構成します。このプロパティが推奨値の **true** に設定されている場合、テーブルの *groupby_acl_check* 属性は groupby ACL を優先するように設定されます。プロパティが **false** に設定されている場合、テーブルの groupby 列に対する ACL チェックが行われず、情報漏洩につながる可能性があります。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

詳細情報

属性	説明
構成名	*glide.security.groupby_acl_check*
構成タイプ	システムプロパティ (/sys_properties_list.do)
データタイプ	ブーリアン
推奨値	true
デフォルト値	true
カテゴリ	アクセス制御
セキュリティリスク	• 重大度スコア：3.7 • CVSS スコア：低 • セキュリティリスクの詳細：このプロパティを **false** に設定すると、groupby 列の ACL チェックが無効になり、情報漏洩につながる可能性があります。
依存関係と前提条件	なし

ダッシュボードの作成/削除でのアクセスチェック

このプロパティは *glide.processors.check_access_before_process* 、ユーザーのログイン時にダッシュボードを作成または削除するためのアクセス制御リスト (ACL) の適用を有効にします。このプロパティは常に true に設定する必要があります。

詳細情報

属性	説明
構成名	*glide.processors.check_access_before_process*
構成タイプ	システムプロパティ (/sys_properties_list.do)
データタイプ	ブーリアン
推奨値	true
デフォルト値	false
カテゴリ	アクセス制御
セキュリティリスク	• 重大度スコア：6.3 • CVSS スコア：中 • セキュリティリスクの詳細: このプロパティを false に設定して無効にすると、ダッシュボードで ACL バイパスが有効になります。これにより、低い権限を持つすべての認証済みユーザーがダッシュボードを削除および追加できます。
依存関係と前提条件	なし

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

属性	説明
機能への影響度	このプロパティは、ユーザーに必要なアクセス権がない場合に、新しい sys_dashboards を作成したり、既存のダッシュボードを削除したりする機能を制御します。値が false に設定されている場合、不適切なロールを持つユーザーは、sys_dashboardエントリを追加および削除できます (ただし、GlideRecord レイヤーは既存の ACL を再チェックする必要があります)。値 true を指定すると、必要なアクセス権を持たないユーザーの追加または削除操作が制限されます。

OAuth ステータスパラメーター検証の適用

クロスサイトリクエストフォージェリ (CSRF) 攻撃からインスタンスを保護するように *glide.oauth.state.parameter.required* プロパティを設定します。

glide.oauth.state.parameter.required プロパティを使用すると、認証コードフローの OAuth 要求でステータスパラメーターを要求できます。ステータスパラメーターは文字列値であり、特殊文字を含めたり、空白にしたりすることはできません。このプロパティを **true** に設定すると、攻撃者は認証中にクロスサイトリクエストフォージェリ (CSRF) 攻撃を実行できなくなります。これにより、代理操作されたユーザーからの攻撃からインスタンスが保護されます。

詳細情報

属性	説明
構成名	*glide.oauth.state.parameter.required*
構成タイプ	システムプロパティ (/sys_properties_list.do)
データタイプ	ブーリアン
推奨値	true
デフォルト値	true
カテゴリ	アクセス制御
セキュリティリスク	• 重大度スコア：4.2 • CVSS スコア：中 • セキュリティリスクの詳細：CSRF 攻撃を確実に防止するには、このプロパティを **true** に設定します。
依存関係と前提条件	なし

厳格なユーザー画像アップロードを強制する

glide.security.strict.user_image_upload プロパティを使用して、ユーザーレコードでプロファイル画像のアップロード/更新を実行する際のアクセス制御を有効にします。

この設定では、無許可のユーザーが別のユーザーのプロファイルに画像をアップロードする可能性が生じます。

- このプロパティを **true** に設定すると、写真をアップロードするときにテーブル ACL が適用され、許可されたユーザーのみが画像をアップロードできるようになります。
- **false** に設定すると、[写真] フィールドへの画像アップロードに ACL は適用されません。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

詳細情報

属性	説明
プロパティ名	*glide.security.strict.user_image_upload*
構成タイプ	システムプロパティ (/sys_properties_list.do)
カテゴリ	アクセス制御
目的	ユーザー画像のアップロードを許可されたユーザーのみに制限すること
推奨値	true
セキュリティリスク評価	3.7
機能への影響度	(低) 承認されたユーザーは引き続きユーザープロファイルに画像をアップロードできるため、機能への影響はありません。
セキュリティリスク	(例) このプロパティを **false** に設定すると、認証されたユーザーは別のユーザーのアカウントに承認なしで画像をアップロードできます。

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

外部ユーザー登録のメールドメインを制限する

sn_ext_usr_reg.allowed_email_domains プロパティを使用して、許容可能な外部メールドメインを一覧表示します。

詳細情報

属性	説明
プロパティ名	*sn_ext_usr_reg.allowed_email_domains*
構成タイプ	システムのプロパティ (/sys_properties_list.do)、Communities プロパティ
カテゴリ	アクセス制御
目的	ユーザーのメールの登録を許可するためにメールドメインを一覧表示します。
推奨値	空の値として設定します (デフォルト)。
構成タイプ	文字列
セキュリティリスク	(高) 悪意のあるアクターが、不要なドメインからのメールアドレスを使用して登録を実行する可能性があります。が *sn_ext_usr_reg.allowed_email_domains* 空の値に設定されていないことを確認します。
セキュリティリスク評価	7.5
参照	Communities

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

記事のユーザーコメントの非表示

*glide.knowman.show_user_feedback*このプロパティを使用して、フィードバックコメントを表示するかどうかを制御します。

glide.knowman.show_user_feedback[なし] に設定されていない場合、フィードバックコメントは Glide プロパティ *glide.knowman.show_user_feedback.roles*で定義されたロールを持つユーザーに対して、ナレッジベース (KB) 記事に表示されます。フィードバックコメントには機密情報が含まれている可能性があるため、フィードバックを表示したくない場合があります。このプロパティが never に設定されていない場合、機密情報がフィードバックで開示された場合に機密性に影響を与える可能性があります。

詳細情報

属性	説明
構成名	*glide.knowman.show_user_feedback*
構成タイプ	システムプロパティ (/sys_properties_list.do)
データタイプ	選択リスト
推奨値	まったくない
デフォルト値	onLoad
カテゴリ	アクセス制御
セキュリティリスク	• 重大度スコア：3.5 • CVSS スコア：低 • セキュリティリスクの詳細：このプロパティを never に設定しないと、機密情報がフィードバックコメントで公開される可能性があります。
依存関係と前提条件	なし
機能への影響度	構成で言及されている選択肢に基づいて、KB 記事にユーザーコメントを表示します。

High Security プラグイン

High Security プラグインをアクティブ化すると、インスタンスのセキュリティレベルを制御する数百もの異なる構成が作成または更新されます。これらの構成は、厳格なアクセス制御、入力検証、および出力エンコーディングを有効にすることで、上位の OWASP 攻撃の多くを軽減します。

これらの設定には次のような内容が含まれます。

- アクセス制御
- ビジネスルール
- システムプロパティ
- UI ポリシーアクション
- スクリプトアクション
- スクリプトインクルード

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

例

次のプロパティの例を参照してください。

プロパティ	トピック
glide.ui.escape_all_script	Jelly をエスケープする
glide.security.strict.actions	実行前に UI アクションをチェックする
glide.security.csrf_previous.allow	CSRF 対策トークン
glide.security.csrf.strict.validation.mode	CSRF 厳格検証

詳細情報

属性	説明
プラグイン名	com.glide.high_security
構成タイプ	[システム定義] > [プラグイン - 開発]
カテゴリ	アクセス制御
目的	このプラグインをアクティブ化する必要があります。これにより、インスタンスのセキュリティレベルが向上し、CSRF、XSS、セッション Cookie のセキュリティ保護、ファイルのアップロードなどの owasp 上位 10 件の攻撃が軽減されることで、攻撃対象領域が縮小します。
推奨値	有効
セキュリティリスク評価	9.8
機能への影響度	(高) このプラグインは、UI と機能に影響を与える可能性があるシステムセキュリティ構成をいくつか有効にします。
セキュリティリスク	(高) 多くのセキュリティ設定が意図せずオープンのままになるため、一部の重大な脆弱性が無防備になる可能性があります。
参照	高セキュリティ設定の有効化 高セキュリティ設定

プラグインのアクティブ化の詳細については、「Activate a plugin」を参照してください。

管理者優先 ACL

glide.security.admin.override.accessterm プロパティは、上書きが有効になっている場合でも、管理者が ACL 評価を上書きできないように制御します。

詳細情報

属性	説明
プロパティ名	*glide.security.admin.override.accessterm*

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

属性	説明
構成タイプ	システムプロパティ (/sys_properties_list.do)
カテゴリ	アクセス制御
目的	管理者が ACL 評価を上書きできないように制御します。
推奨値	True (デフォルト)
構成タイプ	ブーリアン
セキュリティリスク	(低) ACL は累積的に評価されます。指定されたフィールドに多数の ACL があり、そのうちの 1 つで管理者優先オプションが false (未選択) の場合、すべての ACL の有効な管理者優先は falseと見なされます。
セキュリティリスク評価	3.8
参照	アクセス制御リストのルール

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

JSONP 要求を信頼できる URL に制限する

AngularJS $http サービスの信頼できる URL を指定して、JSONP 要求を許可または拒否します。

このプロパティは *angular.jsonp.inclusion_list.enabled* 、JSONP 要求を許可または拒否するために angularJS $http サービスの信頼できる URL を指定します。このプロパティが必要なのは、これにより顧客の変更が破棄される可能性があるため、信頼できる URL を追加する方法が必要になるためです。このプロパティが推奨値の true に設定されていない場合、JSONP 要求は任意の URL に対して許可されます。

詳細情報

属性	説明
構成名	*angular.jsonp.inclusion_list.enabled*
構成タイプ	システムプロパティ (/sys_properties_list.do)
データタイプ	ブーリアン
推奨値	true
デフォルト値	true
カテゴリ	アクセス制御
セキュリティリスク	• 重大度スコア：中 • CVSS スコア：5.4 • セキュリティリスクの詳細：このプロパティを **false** に設定すると、任意の URL への JSONP 要求が可能になります。
依存関係と前提条件	なし

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

生データベースクエリの実行を無効にする

ユーザーがデータベースに対して生の SQL クエリを実行できるかどうかを制御します。

glide.db.allow_unsafe_dbi_execute_sql プロパティを使用すると、ユーザーは生の SQL クエリをデータベースで実行できます。これにより、GlideRecord の制限外のテーブルとデータにアクセスできます。このプロパティが推奨値の *false* に設定されていない場合、悪意のある SQL ステートメントの実行につながる可能性がある Glide Scriptable から *dbi.executeStatement()* を呼び出すことができるようになります。

警告:
このプロパティは安全であり、db オーバーライドはありません。

詳細情報

属性	説明
構成名	*glide.db.allow_unsafe_dbi_execute_sql*
構成タイプ	システムプロパティ (/sys_properties_list.do)
データタイプ	ブーリアン
推奨値	false
デフォルト値	false
カテゴリ	アクセス制御
セキュリティリスク	• 重大度スコア：7.2 • CVSS スコア：高 • セキュリティリスクの詳細：このプロパティを **false** に設定しないと、Glide Scriptable からの *dbi.executeStatement()* 呼び出しが可能になります。
依存関係と前提条件	なし
参照	アクセス制御リストのルール

SOAP 要求のゲストユーザーの設定

このプロパティを構成して、非認証 SOAP 要求のアクセスレベルを制御します。

このプロパティは、非認証 SOAP 要求のアクセスレベルを制御します。このプロパティが推奨値 *soap.guest* に設定されていない場合、または権限が制限されたユーザーに設定されている場合は、SOAP 要求がそのユーザーの代わりに実行されます。このプロパティが空白の場合、管理者レベルまたはメンテナンスレベルの操作への認証されていないアクセスが可能になり、インスタンス内のすべてのセキュリティ制御が無効になります。

詳細情報

属性	説明
構成名	*com.glide.soap.guest_user*
構成タイプ	システムプロパティ (/sys_properties_list.do)

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

属性	説明
データタイプ	文字列
推奨値	soap.guest
デフォルト値	soap.guest
カテゴリ	アクセス制御
セキュリティリスク	• 重大度スコア：8.1 • CVSS スコア：高 • セキュリティリスクの詳細：このプロパティを空白に設定すると、管理者またはメンテナンスレベルの操作への認証されていないアクセスが可能になります。
依存関係と前提条件	なし

クライアント呼び出し可能スクリプトインクルードにデフォルトで認証を要求する

デフォルトでは、明示的に可視性を設定していないクライアント呼び出し可能スクリプトインクルードは、公開状態になります。必要に応じて *glide.script.ccsi.ispublic* プロパティを追加すると、公開ページからアクセスされるクライアント呼び出し可能スクリプトインクルード全体に対してプライバシーコントロールができるようになります。

このプロパティを追加する場合は、値を **false** に設定する必要があります。これは、クライアント呼び出し可能スクリプトインクルードがすべて非公開であり、公開ページで可視性を変更するという指定になります。

注:
値が **true** のプロパティを追加したり、値を **false** から **true** に変更したりすることはできません。これを実行しようとすると、エラーメッセージが表示されます。

必要に応じて、isPublic() 関数を追加することにより、クライアント呼び出し可能スクリプトインクルードのプライバシー設定を個別に変更できます。

- isPublic() 設定は *glide.script.ccsi.ispublic* プロパティよりも優先されます。
- たとえば、個別のスクリプトで isPublic() を **true** に設定すると、このスクリプトが公開状態になります。これは、他のクライアント呼び出し可能スクリプトインクルードをすべて非公開にする *glide.script.ccsi.ispublic* プロパティを上書きします

警告:
これはセーフハーバープロパティです。つまり、いったん変更したら変えることはできません。元に戻すことはできません。

詳細情報

属性	説明
プロパティ名	*glide.script.ccsi.ispublic*
構成タイプ	システムプロパティ (/sys_properties_list.do)
カテゴリ	アクセス制御
目的	クライアント呼び出し可能スクリプトインクルードを非公開にすると、公開ページにアクセスするゲストはクライア

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

属性	説明
	ント呼び出し可能スクリプトインクルードにアクセスできないということになります。ログインしていないユーザーは、非公開スクリプトを実行できません。
推奨値	false
セキュリティリスク評価	7.5
機能への影響度	(高) クライアント呼び出し可能スクリプトインクルードが公開として指定されている場合 (つまり、このプロパティがない場合)、非認証ユーザーはクライアントスクリプトを実行できます。ログインしていないユーザーによるスクリプトの実行を制限するプロパティを追加します。
セキュリティリスク	(高) このプロパティを追加しない場合、クライアント側スクリプトインクルードが ACL を回避し、その結果意図せずに機能が公開される可能性があります。クライアントスクリプトに機密情報がある場合は、有害なセキュリティリスクが発生するおそれがあります。
ワークアラウンド	*glide.script.ccsi.ispublic* プロパティを **false** に設定すると、すべてのクライアント呼び出し可能スクリプトインクルードが非公開になります。 isPublic() 関数を追加することにより、クライアント呼び出し可能スクリプトインクルードのプライバシー設定を個別に変更できます。isPublic() 関数は *glide.script.ccsi.ispublic* プロパティよりも優先されます。スクリプトインクルードに次の構文を追加します。 isPublic:function(){return[true/false];},

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

本番インスタンスの動作を強制

インスタンスを本番インスタンスのように処理するか非本番インスタンスのように処理するかを設定します。

glide.installation.production プロパティが推奨値の **true** に設定されていない場合、インスタンスは本番インスタンスとして扱われないため、zboot やその他の危険性のあるスクリプトの実行が許可されます。本番インスタンスを非本番インスタンスとして評価できるようにすると、情報漏えいやサービス拒否 (DoS) 攻撃につながる可能性があります。

詳細情報

属性	説明
構成名	*glide.installation.production*
構成タイプ	システムプロパティ (/sys_properties_list.do)
データタイプ	ブーリアン
推奨値	true

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

属性	説明
デフォルト値	true
カテゴリ	アクセス制御
セキュリティリスク	• 重大度スコア：6.3 • CVSS スコア：中 • セキュリティリスクの詳細：このプロパティ値を **false** に設定すると、インスタンスが非本番インスタンスとして扱われ、zboot やその他の危険性のあるスクリプトを実行できるようになります。
依存関係と前提条件	なし

バックグラウンドスクリプトへのアクセス制限

glide.script_processor.admin プロパティを構成して、Script Background モジュールへのアクセスに必要なロールを設定します。

glide.script_processor.admin プロパティは、Script Background モジュールへのアクセスに必要なロールを保持します。このプロパティが推奨値の **admin** に設定されていない場合、ロールに関係なく、すべてのユーザーがインスタンスでバックグラウンドスクリプトを実行できます。これにより、攻撃者が ACL システムをバイパスして、テーブルへのフルアクセスを取得できます。

⚠ 警告:
これはセーフハーバープロパティです。つまり、いったん変更したら変えることはできません。元に戻すことはできません。

詳細情報

属性	説明
構成名	*glide.script_processor.admin*
構成タイプ	システムプロパティ (/sys_properties_list.do)
データタイプ	文字列
推奨値	admin
デフォルト値	admin
カテゴリ	アクセス制御
セキュリティリスク	• 重大度スコア：8.8 • CVSS スコア：高 • セキュリティリスクの詳細：このプロパティを推奨値の **admin** に設定しないと、すべてのユーザーがインスタンスでバックグラウンドスクリプトを実行できます。
依存関係と前提条件	なし

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ターゲットテーブルが空のメールへのアクセスを制限する

glide.email.email_with_no_target_visible_to_all プロパティをアクティブ化して、ユーザーからメールへのアクセスを制限します (メール送信元のユーザーであるか、管理者ロールを持つ場合を除く)。

許可されていないユーザーは、ターゲットレコードのない [sys_email_list] テーブル内のメールにアクセスできます。このプロパティは、メールエントリに ACL を適用するのではなく、メール送信者と admin ロールを持つユーザーのみにアクセスを制限します。

注:
インスタンスによって送受信されたメールは、[sys_email_list] テーブルに表示されます。ただし、[エラー] および [無視] ステータスがマークされた受信メールにかぎり、空のターゲットテーブルを設定する必要があります。

詳細情報

属性	説明
プロパティ名	*glide.email.email_with_no_target_visible_to_all*
構成タイプ	システムプロパティ (/sys_properties_list.do)
構成	アクセス制御
目的	ユーザーがアクセスを許可しない場合に、メールクライアントでメールが表示されないようにすること
推奨値	false
セキュリティリスク評価	5.4
機能への影響度	(低) ユーザーは、管理者またはメールの送信元でないかぎり、ターゲットテーブルが空のメールを表示できなくなります。
セキュリティリスク	(中) プロパティが有効でない場合、許可されていないユーザーは [target_table] フィールドが空であるメールにアクセスできます。
参照	詳細なメールプロパティ https://support.servicenow.com/kb_view.do?sysparm_article=KB0690043

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

特定の IP 範囲プラグインへのアクセス制限

com.snc.ipauthenticator プラグインを使用して、特定の IP 範囲にアクセスを制限します。インスタンスに対するパブリック アクセスが意図されている場合を除き、管理者は割り当てられた IP ネットブロックにアクセスを制限する必要があります。

必須条件

このプロパティを設定する前に、IP Range Based Authentication (com.snc.ipauthenticator)*com.snc.ipauthenticator* プラグインをアクティブ化する必要があ

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

ります。詳細については、「IP 範囲ベースの認証」および「設定手順」の項 (下記) を参照してください。

詳細情報

属性	説明
プラグイン名	*com.snc.ipauthenticator*
構成タイプ	[System Security] > [IP アドレスアクセス制御]
カテゴリ	アクセス制御
目的	インスタンスにアクセスできるまたはアクセスできない IP アドレスの範囲を、信頼できるドメインと信頼できないドメインのリストに追加すること
推奨値	有効
セキュリティリスク評価	5.3
機能への影響度	(低) 顧客が拒否した IP 範囲がこの修正アイテムに使用されます。顧客がターゲットリストを定義するため、影響はありません。
セキュリティリスク	(低) IP アクセス制御機能を使用して、インターネット上のターゲットインスタンスへの不必要な開示を制限する必要があります。
参照	IP 範囲ベースの認証

設定手順

1. com.snc.ipauthenticator プラグインがアクティブであることを確認します。
2. 移動先 システムセキュリティ > **IP** アドレスアクセス制御.
3. [新規] をクリックして、IP アドレスの除外リスト (拒否) または包含リスト (許可) を作成します。
4. [送信] をクリックします。

ナレッジベースへのアクセス制限

*glide.knowman.block_access_with_no_user_criteria*このプロパティは、ナレッジベース記事に対するユーザーの読み取り/書き込みアクセスを制御するために使用されます。

詳細情報

属性	説明
構成名	*glide.knowman.block_access_with_no_user_criteria*
構成タイプ	システムプロパティ (/sys_properties_list.do)
データタイプ	ブーリアン
推奨値	true
デフォルト値	false
カテゴリ	アクセス制御

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

属性	説明
セキュリティリスク	• 重大度スコア：9.1 • CVSS スコア：重大 • セキュリティリスクの詳細:このプロパティが推奨値の true に設定されていない場合、すべてのユーザーが KB を読み取り、KB に寄稿できます。
依存関係と前提条件	なし
機能への影響	[読込可能] と [寄稿可能] のいずれかが指定されていない場合、ナレッジベースへのアクセスを拒否します。

CMDB モデルの権限を制限する

csm_cmdb_model.customer_visible_flag システムプロパティを使用し、CMDB モデルへの追加のアクセス制御として、製品モデルテーブルのデータへの顧客のアクセスを制限します。

csm_cmdb_model.customer_visible_flag プロパティを **true** に設定して、以下にリストされているテーブルの [顧客に表示] フィールドを有効にします。

- 製品モデルテーブル [cmdb_model]
- ソフトウェアモデルテーブル [cmdb_software_product_model]
- アプリケーションモデルテーブル [cmdb_application_product_model]
- 消耗品モデルテーブル [cmdb_consumable_product_model]
- 施設モデルテーブル [cmdb_facility_product_model]
- ハードウェアモデルテーブル [cmdb_hardware_product_model]

このプロパティを **true** に設定すると、すべての cmdb_model 値がデフォルトで非表示になります。

cmdb_model テーブルの customer_visible 列/属性を考慮せずに、sn_esm_user がアクセスできるベース cmdb_model ACL に依存するには、このプロパティを **false** に設定します。

詳細情報

属性	説明
プロパティ名	*csm_cmdb_model.customer_visible_flag*
構成タイプ	システムプロパティ (/sys_properties_list.do)
カテゴリ	アクセス制御
目的	**true** に設定すると、[顧客に表示] フィールドの設定を使用して、Customer Service Portal の製品モデルデータへのアクセスが決定されます。
推奨値	true (デフォルトは false)。
構成タイプ	ブーリアン
セキュリティリスク	(中) sn_esm_user ロールと初期設定の ACL を持つすべてのユーザーが、CMDB モデルに対する権限を持つ可能性があります。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

属性	説明
	注: このロールは、外部ユーザーに付与される傾向があります。外部ユーザーに望まない CMDB モデルへの権限が付与される可能性があります。
参照	Customer Service Portal で製品モデルデータへのアクセスを制限します

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

添付ファイルへの非認証アクセスを制限する

glide.image_provider.security_enabled プロパティを使用して画像のセキュリティ設定を制御します。**true** に設定すると、認証および承認されたユーザーにのみ画像が表示されます。**false** に設定すると、添付ファイルへの URL を持つすべてのユーザーに画像が表示されます。

詳細情報

属性	説明
プロパティ名	*glide.image_provider.security_enabled*
構成タイプ	システムプロパティ (/sys_properties_list.do)
カテゴリ	アクセス制御
目的	*.iix* 形式を使用してレンダリングされた添付ファイルへの非認証アクセスを防止します。
推奨値	True (デフォルト)
機能への影響度	(低) 機能に大きな影響はありません。以前に .iix に直接アクセスしていたユーザーは認証を受ける必要があるため、ユーザーエクスペリエンスに多少影響する可能性があります。
セキュリティリスク	(高) 一部の添付ファイルに機密情報が含まれている可能性があるため、非認証ユーザーには制限を適用する必要があります。
参照	添付ファイルの管理 利用可能なシステムプロパティ

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

カスタムジャーナルエントリへのアクセスを制限する

glide.live_feed.custom_journal.acl_check_enabled プロパティを使用して、カスタムジャーナルフィールドの ACL を優先します。

*glide.live_feed.custom_journal.acl_check_enabled*推奨値の true に設定されていない場合、すべてのユーザーはライフフィード機能内のすべてのジャーナルエントリーを表示できます。プロパティを true に設定すると、推奨機能であるカスタムジャーナルフィールドの ACL が優先されます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

詳細情報

属性	説明
プロパティ名	*glide.live_feed.custom_journal.acl_check_enabled*
構成タイプ	システムプロパティ (/sys_properties_list.do)
カテゴリ	アクセス制御
目的	ACL に基づいてどのユーザーにどのジャーナルエントリーを表示するかを制御します。
推奨値	true
構成タイプ	ブーリアン。
セキュリティリスク	(中) true に設定すると、ACL に合格するカスタムジャーナルエントリーのみがライブフィードに表示されます。それ以外の場合、すべてのユーザーがすべてのジャーナルエントリーを表示できます。

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

セキュリティジャンプスタートプラグイン (ACL ルール) を有効にする

Security Jump Start (ACL Rules) (com.snc.system_security*com.snc.system_security*) プラグインをアクティブ化して、Now Platform 内の主要なシステムテーブルの一部でアクセス制御を検証する重要な ACL を複数作成します。

これらのルールは、多くのシステムテーブルを保護するためのジャンプスタートを提供し、組織がより簡単にインスタンスを本番環境に移行できるようにします。Security Jump Start (ACL ルール) プラグインは、すべての新しいインスタンスに自動的にインストールされます。

詳細情報

属性	説明
プラグイン ID	*com.snc.system_security*
構成タイプ	[システム定義] > [プラグイン]
カテゴリ	アクセス制御
目的	Security Jump Start (ACL Rules) プラグインをアクティブ化して、適切なセキュリティコンプライアンスを実現します。 これは、最初にシステムテーブルを保護する基本的な ACL をいくつか提供します。インスタンスのデフォルトのプロビジョニングに付属する各システムテーブルに対して手動で作成するのではありません。これらの ACL は、新しく作成されたインスタンスを迅速に本番環境に移行する必要がある場合に役立ちます。
推奨値	有効
セキュリティリスク評価	8.1

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

属性	説明
機能への影響度	(中) インスタンスの既存の ACL を監査せずにこのプラグインをインストールすると、機能に大きな影響があります。修正を行う前に、顧客への働きかけと定義が必要です。
セキュリティリスク	(高) アクセス制御を適用して、インスタンスへの意図しないアクセスをロックする必要があります。ACL ジャンプスタートルールは、多くのシステムテーブルを保護するための開始点を提供し、組織が迅速に本番環境に移行できるようにするために作成されました。
参照	Security Jump Start - ACL ルール

設定手順

インスタンスでこのプラグインがアクティブ化されていない場合は、ServiceNow サポートにお問い合わせください。この時点でプラグインをアクティブ化すると、本番環境で既に使用されているテーブルへのセキュリティアクセスが変更される可能性があります。プラグインから提供される新しい ACL ルールに管理者が注目している場合は、必要に応じて既存のインスタンスに 1 つ以上の ACL ルールを手動で作成できます。この ACL のリストは、その場合の指針として使用できます。

プラグインのアクティブ化の詳細については、「Activate a plugin」を参照してください。

インポートセット **API** 内での安全な複数挿入操作の使用

*com.glide.import_set_api.insert_multiple_optimize*このプロパティを使用して、インポートセット API 内の複数挿入操作に *GlideRecordSecure* または *GlideRecord* を使用するかどうかを制御します。

推奨 *com.glide.import_set_api.insert_multiple_optimize* 値の false に設定すると、*GlideRecordSecure* を使用してレコードが挿入され、テーブルレベルのアクセス制御リスト (ACL) が評価されます。このプロパティが true に設定されている場合、 *GlideRecord* はレコードの挿入に使用され、テーブルレベルの ACL は評価されません。さらに、インポートセット API での複数の REST エンドポイント挿入 ACL (sys_id:3101b770ff2211105cf343d0653bf182) が有効であること、およびユーザーがロール import_transformer を持っていることを確認する必要があります。

詳細情報

属性	説明
構成名	*com.glide.import_set_api.insert_multiple_optimize*
構成タイプ	システムプロパティ (/sys_properties_list.do)
データタイプ	ブーリアン
推奨値	true
デフォルト値	false
カテゴリ	アクセス制御
セキュリティリスク	• 重大度スコア：6.5 • CVSS スコア：中

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

属性	説明
	• セキュリティリスクの詳細：このプロパティが false に設定されていない場合、特権の低いユーザーが自分の特権ロールのスコープ外のテーブルにデータを挿入できる可能性があります。
元に戻せる動作	安全なデータベース上書きとデータベース上書きなしの両方。
依存関係と前提条件	なし
機能への影響度	このプロパティは、GlideRecord を使用してデータを保存することで、インポートセット API のパフォーマンスを最適化します。パラメーターが設定されている場合、API にアクセスするには、統合ユーザーが import_transformer ロールを持っている必要があります。
参照	https://developer.servicenow.com/blog.do?p=/post/gliderecord-vs-gliderecordsecure

SOAP 要求の厳格なセキュリティの適用

glide.soap.strict_security プロパティを使用して、Web サービスのセキュリティを適用します。

このプロパティでは、次の組み合わせを使用します。

- HTTP プロトコルを介した基本認証のチャレンジ/応答、および
- コンテキスト依存セキュリティ：ロール管理プラグイン のシステムレベルのアクセス制御。

このプロパティを **true** に設定すると、次のアクションが実行されます。

- ユーザーが操作を実行するための適切なロールを持っている場合は、受信 SOAP 要求に検証するロール承認がないかチェックします。これは、作成、読み取り、更新、または削除操作を実行するときに、Now Platform テーブルに対して行われる SOAP Web サービスの呼び出し/要求中に発生します。
- テーブルのデータを SOAP データの形式で取得するときに、システムレベルの ACL をチェックします。
- フィールドレベルの ACL で、テーブルのフィールドに対して実行された CRUD 操作がないかチェックします。

詳細情報

属性	説明
プロパティ名	*glide.soap.strict_security*
構成タイプ	システムプロパティ (/sys_properties_list.do)
カテゴリ	アクセス制御
目的	SOAP 呼び出しを介してレコードにアクセスする場合でも、セキュリティ ACL が確実にチェックおよび検証されるようにすること
推奨値	true

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

属性	説明
機能への影響度	(高) この修正では、インスタンスでテーブル/ページからデータを SOAP データの形式で取得する際に、システムレベルのアクセス制御が適用されます。現在このデータにアクセスしているユーザーがいる場合、ACL ルールに基づいてデータへのアクセスが制限/許可されます。 SOAP データにアクセスできるデフォルトのロールについては、「SOAP web service」を参照してください。
セキュリティリスク	(中) 受信 SOAP 要求で適切な承認が構成されていない場合、無許可のユーザーがターゲットインスタンスの機密コンテンツ/データにアクセスする可能性があります。
参照	Enforce strict security for inbound SOAP SOAP web service

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

必要な JMS 接続ファクトリー

mid.property.jms.command.allowed_factory_names プロパティは 、MID Server が使用できる Java Messaging Service (JMS) 接続ファクトリを制御します。

これは、JMS アクティビティまたはアクション用のプラグインに必要な一部のファクトリを対象としています。追加のファクトリを含めることは、許可されたファクトリで攻撃者が利用できる機能に依存する JDNI 挿入など、脆弱性に対する一連の攻撃のステップになる可能性があります。脆弱性が利用される可能性を防ぐために、必要なデフォルト以外のファクトリを含めないでください。

このセキュリティリスクを修正するには、mid プロパティ *mid.property.jms.command.allowed_factory_names* に指定された名前のリストを確認します。デフォルトの connectionFactory、queueConnectionFactory、および topicConnectionFactory 以外の追加の Java ファクトリ名が必要であるかを確認してください。

詳細情報

属性	説明
構成名	*mid.property.jms.command.allowed_factory_names*
構成タイプ	システムプロパティ (/sys_properties_list.do)
データタイプ	文字列
デフォルト値	*connectionFactory*、*queueConnectionFactory*、*topicConnectio*
カテゴリ	アクセス制御
セキュリティリスク	• 重大度スコア：4.1 • CVSS スコア：中 • セキュリティリスクの詳細：
依存関係と前提条件	なし

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

SOAP 要求のゲストユーザーの設定

このプロパティを構成して、非認証 SOAP 要求のアクセスレベルを制御します。

このプロパティは、非認証 SOAP 要求のアクセスレベルを制御します。このプロパティが推奨値 *soap.guest* に設定されていない場合、または権限が制限されたユーザーに設定されている場合は、SOAP 要求がそのユーザーの代わりに実行されます。このプロパティが空白の場合、管理者レベルまたはメンテナンスレベルの操作への認証されていないアクセスが可能になり、インスタンス内のすべてのセキュリティ制御が無効になります。

詳細情報

属性	説明
構成名	*com.glide.soap.guest_user*
構成タイプ	システムプロパティ (/sys_properties_list.do)
データタイプ	文字列
推奨値	soap.guest
デフォルト値	soap.guest
カテゴリ	アクセス制御
セキュリティリスク	• 重大度スコア：8.1 • CVSS スコア：高 • セキュリティリスクの詳細：このプロパティを空白に設定すると、管理者またはメンテナンスレベルの操作への認証されていないアクセスが可能になります。
依存関係と前提条件	なし

SNC アクセス制御プラグインを有効にする

SNC Access Control (com.snc.snc_access_control*com.snc.snc_access_control*) プラグインをアクティブ化して、カスタマーサービス & サポート担当者によるインスタンスへのアクセスを制御します。

Now Platform のデフォルト構成では、短期的なサポート資格情報を作成する内部プロセスを介してカスタマーサービス & サポートがインスタンスにアクセスできます。すべてのアクセスが監査されますが、このアクセスを制御することを希望する顧客もいます。

このプラグインを使用すると、カスタマーサービスとサポートでカスタマーサービス & サポートの従業員がインスタンスにアクセスできないようにすることができます。サポートアクティビティを開始する前に Now Platform アクセスを有効にする必要があるため、この決定はサポート SLA に影響します。詳細については、「ServiceNow アクセス制御 」を参照してください。

詳細情報

属性	説明
プラグイン名	*com.snc.snc_access_control*
構成タイプ	[システム定義] > [プラグイン]

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

属性	説明
カテゴリ	アクセス制御
目的	カスタマーサービス & サポートの従業員によるインスタンスへのアクセスの禁止
推奨値	有効
必要なロール	顧客管理者はプラグインをアクティブ化できません。プラグインをアクティブ化するには昇格された権限が必要なため、明示的に要求する必要があります。
セキュリティリスク評価	8.2
機能への影響度	(低) このプラグインが非アクティブの場合、カスタマーサービス & サポートのすべての従業員は顧客のインスタンスにアクセスできます。プラグインを有効にすると、顧客は承認されたカスタマーサービス & サポートの従業員のみにアクセスを制限できます。
セキュリティリスク	(高) より幅広いユーザーグループに対してインスタンスアクセスが不必要に公開されます。
参照	ServiceNow アクセス制御

設定手順

1. プラグインを要求するには、「ServiceNow アクセス制御の有効化」の手順に従います。顧客は HI から SNC Access Control プラグイン (com.snc.snc_access_control) を要求する必要があります。
2. SNC アクセス制御を有効にするには、「ServiceNow アクセス制御の構成」の手順に従います。アクセス制御レコードを設定して、インスタンスにログインする権限を持つカスタマーサービス & サポートの従業員を 1 人以上指定します。

API と Web サービス

API および Web サービスカテゴリでは、アプリケーションに適切な認証、承認、およびセッション管理があることを確認し、信頼境界を横切るすべての入力を検証します。またそのカテゴリにはすべての API タイプのセキュリティコントロールが含まれています。

このカテゴリの特定のコントロールは、SOAP Web サービスの XDS スキーマ検証や graphQL API のサービス拒否保護など、サービスタイプ別の入力検証に対応します。

SOAP コンテンツタイプの検証

glide.soap.require_content_type_xml プロパティを使用して、テキスト/xml のコンテンツタイプの検証を有効にし、無効な SOAP 要求から保護します。

- **true** に設定すると、Now Platform はテキスト/xml のコンテンツタイプを検証して無効な SOAP 要求から保護します。
- **false** に設定すると、すべてのコンテンツタイプの値が許可されます。

> ⚠ 警告:
> これはセーフハーバープロパティです。つまり、いったん変更したら変えることはできません。元に戻すことはできません。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

詳細情報

属性	説明
プロパティ名	*glide.soap.require_content_type_xml*
構成タイプ	システムプロパティ (/sys_properties_list.do)
カテゴリ	API と Web サービス
目的	無効な SOAP 要求から保護すること
推奨値	true
セキュリティリスク評価	8.8
機能への影響度	(低) この修正により、すべての受信 SOAP 要求に対して SOAP コンテンツタイプを検証できるようになります。 • 受信要求に text/xml 以外のコンテンツタイプを使用している場合は、SOAP トランザクションが失敗する可能性があります。 • 正しい MIME タイプを使用していない場合、サードパーティの統合が中断される可能性があります。
セキュリティリスク	(中) 受信 SOAP 要求を受け入れる場合、適切な検証が実行され、関連するコンテンツタイプが要求の一部として定義されていることが確認されます。これにより、セキュリティリスクと見なされる可能性のある無効な SOAP 応答が制限されます。
参照	コンテンツタイプ

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

PDF 要求に認証を要求

glide.basicauth.required.pdf プロパティを使用して、受信 PDF 要求で基本認証を要求するかどうかを指定します。

詳細情報

警告:
これはセーフハーバープロパティです。つまり、いったん変更したら変えることはできません。元に戻すことはできません。

属性	説明
プロパティ名	*glide.basicauth.required.pdf*
構成タイプ	システムプロパティ (/sys_properties_list.do)
カテゴリ	API と Web サービス
目的	PDF 要求に対して基本認証を適用すること
推奨値	true

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

属性	説明
セキュリティリスク評価	7.5
機能への影響度	(低) この修正では、基本認証とシステムレベルのアクセス制御の形で、認証方法の組み合わせが適用されます。 • インスタンス上で PDF データの形式でテーブル/ページからデータを取得する際に、この認証を実行します。 • 現在このデータにアクセスしているゲストユーザーを制限します。必要であれば、このコンテンツへのアクセスを必要とするユーザーのために、必要なアクセス制御権限を持つ新しいアカウントを作成する場合があります。 詳細については、「Web サービスインポートセット」を参照してください。
セキュリティリスク	(高) 受信 PDF 要求で適切な承認が構成されていない場合、無許可のユーザーがターゲットインスタンスの機密コンテンツ/データにアクセスする可能性があります。

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

Cookie 認証要求に認証プロファイルチェックを要求する

このプロパティを使用して、Cookie 認証要求の認証プロファイルチェックを実施します。

プロパティが *glide.authenticate.cookie.auth.check* 推奨値の **true** に設定されていない場合、前の要求で Cookie 認証を使用して要求されたリソースに対して認証プロファイルのチェックは必要ありません。これは、認証セキュリティ制御のバイパスにつながる可能性のあるセキュリティの脆弱性です。

このリスクを修復するには、プロパティを **true** に設定します*glide.authenticate.cookie.auth.check*。

詳細情報

属性	説明
構成名	*glide.authenticate.cookie.auth.check*
構成タイプ	システムプロパティ (/sys_properties_list.do)
データタイプ	ブーリアン
推奨値	true
デフォルト値	true
カテゴリ	API と Web サービス
セキュリティリスク	• 重大度スコア：7.4 • CVSS スコア：高 • セキュリティリスクの詳細：

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

属性	説明
元に戻せる動作	安全なデータベース上書きとデータベース上書きなしの両方。
依存関係と前提条件	なし

イベント管理 HTTP プロセッサーで認証を必須とする

Event Management プラグイン () が有効になっている場合に、受信 Amazon Simple Notification Service (*com.glideapp.itom.snac*SNS) 要求に対して安全な基本認証を確立する方法について説明します。

プロパティが *glide.basicauth.required.evtmgmthttpprocessor* 推奨値の **true** に設定されておらず、Event Management プラグイン () がアクティブな場合、すべての受信 Amazon Simple Notification Service (*com.glideapp.itom.snac*SNS) 要求に基本認証は必要ありません。これにより、インスタンスデータへの非認証アクセスが発生する可能性があります。

このセキュリティリスクを修復するには、*glide.basicauth.required.evtmgmthttpprocessor* が **true** に設定され、*com.glideapp.itom.snac* がアクティブになっていることを確認してください。

詳細情報

属性	説明
構成名	*glide.basicauth.required.evtmgmthttpprocessor*
構成タイプ	システムプロパティ (/sys_properties_list.do)
データタイプ	ブーリアン
推奨値	true
デフォルト値	true
カテゴリ	API と Web サービス
セキュリティリスク	• 重大度スコア：7 • CVSS スコア：高 • セキュリティリスクの詳細：*glide.basicauth.required.evtmgmthttpprocessor* が推奨値の true に設定されておらず、*com.glideapp.itom.snac* プラグインをアクティブにしていない場合、インバウンド SNS 要求に対して基本認証が有効になりません。これにより、インスタンスデータへの非認証アクセスが発生する可能性があります。
依存関係と前提条件	なし
参照	• https://docs.aws.amazon.com/sns/latest/dg/welcome.html • Access control

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

属性	説明
機能への影響度	*glide.basicauth.required.evtmgmthttpprocessor* が推奨値の true に設定されておらず、Event Management プラグイン (com.glideapp.itom.snac) がアクティブな場合、すべてのインバウンド Amazon Simple Notification Service (SNS) 要求に対して基本認証は必要ありません。これにより、インスタンスデータへの非認証アクセスが発生する可能性があります。

SOAP 要求に認証を要求する

glide.basicauth.required.soap プロパティを使用して、受信 SOAP 要求で基本承認を要求するかどうかを指定します。

詳細情報

警告:
これはセーフハーバープロパティです。つまり、いったん変更したら変えることはできません。元に戻すことはできません。

属性	説明
プロパティ名	*glide.basicauth.required.soap*
構成タイプ	システムプロパティ (/sys_properties_list.do)
カテゴリ	API と Web サービス
目的	SOAP 要求承認の適用
推奨値	true
セキュリティリスク評価	8.1
機能への影響度	(中) この修正では、基本認証とシステムレベルのアクセス制御の形で、認証方法の組み合わせが適用されます。 • インスタンス上で SOAP データの形式でテーブル/ページからデータを取得する際に、この認証を実行します。 • 現在このデータにアクセスしているゲストユーザーを制限します。 • このコンテンツへのアクセスを必要とするユーザーのために、必要なアクセス制御権限を持つアカウントを作成します。 詳細については、「SOAP Web サービス」および「MID Server 認証資格情報と SOAP 要求」を参照してください。
セキュリティリスク	(中) データソースの SOAP 要求で適切な承認が構成されていない場合、無許可のユーザーがターゲットインスタンスの機密コンテンツ/データにアクセスする可能性があります。
参照	認証

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

アンロード要求に認証を要求する

glide.basicauth.required.unl (useUnloadFormat) プロパティを使用して、受信アンロード要求で基本認証を要求するかどうかを指定します。

詳細情報

属性	説明
プロパティ名	*glide.basicauth.required.unl*
構成タイプ	システムプロパティ (/sys_properties_list.do)
カテゴリ	API と Web サービス
目的	アンロード要求に対して基本認証を適用すること
推奨値	true
セキュリティリスク評価	7.5
機能への影響度	(中) この修正では、基本認証とシステムレベルのアクセス制御の形で、認証方法の組み合わせが適用されます。インスタンス上でアンロードデータの形式でテーブル/ページからデータを取得する際に、この認証を実行します。
セキュリティリスク	(高) データソースのアンロード要求で適切な承認が構成されていない場合、無許可のユーザーがターゲットインスタンスの機密コンテンツ/データにアクセスする可能性があります。が *glide.basicauth.required.unl* sys_properties_table内に存在し、true に設定されていることを確認します。
参照	認証

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

csv 要求に認証を要求する

glide.basicauth.required.csv プロパティを使用して、受信 CSV (カンマ区切り値) 要求で基本認証を要求するかどうかを指定します。

詳細情報

警告:
これはセーフハーバープロパティです。つまり、いったん変更したら変えることはできません。元に戻すことはできません。

属性	説明
プロパティ名	*glide.basicauth.required.csv*
構成タイプ	システムプロパティ (/sys_properties_list.do)
カテゴリ	API と Web サービス
目的	CSV 要求に対して基本認証を適用すること
推奨値	true

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

属性	説明
セキュリティリスク評価	7.5
機能への影響度	(低) この修正では、基本認証とシステムレベルのアクセス制御の形で、認証方法の組み合わせが適用されます。 • インスタンス上の CSV データの形式でテーブル/ページからデータを取得する際に、この認証を実行します。 • 現在このデータにアクセスしているゲストユーザーを制限します。必要であれば、このコンテンツへのアクセスを必要とするユーザーのために、必要なアクセス制御権限を持つ新しいアカウントを作成する場合があります。 詳細については、「CSV 形式のファイルからのデータの取得」を参照してください。
セキュリティリスク	(高)受信 CSV 要求で適切な承認が構成されていない場合、無許可のユーザーがターゲットインスタンスの機密コンテンツや機密データにアクセスする可能性があります。が *glide.basicauth.required.csv* sys_properties テーブルに存在し、true に設定されていることを確認します。
参照	Web サービスセキュリティ

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

Excel 要求に認証を要求

glide.basicauth.required.excel プロパティを使用して、受信 Excel 要求で基本認証を要求するかどうかを指定します。

詳細情報

警告:
これはセーフハーバープロパティです。つまり、いったん変更したら変えることはできません。元に戻すことはできません。

属性	説明
プロパティ名	*glide.basicauth.required.excel*
構成タイプ	システムプロパティ (/sys_properties_list.do)
カテゴリ	API と Web サービス
目的	Excel 要求に対して基本認証を適用すること
推奨値	true
セキュリティリスク評価	7.5
機能への影響度	(低) この修正では、基本認証とシステムレベルのアクセス制御の形で、認証方法の組み合わせが適用されます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

属性	説明
	• インスタンス上で Excel データの形式でテーブル/ページからデータを取得する際に、この認証を実行します。 • 現在このデータにアクセスしているゲストユーザーを制限します。必要であれば、このコンテンツへのアクセスを必要とするユーザーのために、必要なアクセス制御権限を持つ新しいアカウントを作成する場合があります。
セキュリティリスク	(高) 受信 Excel 要求で適切な承認が構成されていない場合、無許可のユーザーがターゲットインスタンスの機密コンテンツ/データにアクセスする可能性があります。

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

インポート要求に認証を要求する

glide.basicauth.required.importprocessor プロパティを使用して、受信インポート要求で基本認証を要求するかどうかを指定します。

詳細情報

警告:
これはセーフハーバープロパティです。つまり、いったん変更したら変えることはできません。元に戻すことはできません。

属性	説明
プロパティ名	*glide.basicauth.required.importprocessor*
構成タイプ	システムプロパティ (/sys_properties_list.do)
カテゴリ	API と Web サービス
目的	インポート要求に基本認証を適用すること
推奨値	true
セキュリティリスク評価	5.3
機能への影響度	(低) この修正では、基本認証とシステムレベルのアクセス制御の形で、認証方法の組み合わせが適用されます。 • データソースをインスタンステーブル/ページにインポートするときに、この認証を実行します。 • 現在このデータにアクセスしているゲストユーザーを制限します。必要であれば、このコンテンツへのアクセスを必要とするユーザーのために、必要なアクセス制御権限を持つ新しいアカウントを作成する場合があります。 詳細については、「CSV 形式のファイルからのデータの取得」を参照してください。
セキュリティリスク	(中) データソースインポート要求で適切な承認が構成されていない場合、無許可のユーザーがターゲットインスタンスの機密コンテンツ/データにアクセスする可能性があります。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

属性	説明
参照	SOAP Web Services のセキュリティ SOAP Web サービス

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

JSONv2 要求に認証を要求

glide.basicauth.required.jsonv2 プロパティを使用して、受信 JSONv2 要求で基本承認を要求するかどうかを指定します。

詳細情報

警告:
これはセーフハーバープロパティです。つまり、いったん変更したら変えることはできません。元に戻すことはできません。

属性	説明
プロパティ名	*glide.basicauth.required.jsonv2*
構成タイプ	システムプロパティ (/sys_properties_list.do)
カテゴリ	API と Web サービス
目的	JSONv2 要求承認の適用
セキュリティリスク評価	7.5
推奨値	true
機能への影響度	(中) この修正では、基本認証とシステムレベルのアクセス制御の形で、認証方法の組み合わせが適用されます。 • インスタンス上で JSON データの形式でテーブル/ページからデータを取得する際に、この認証を実行します。 • 現在このデータにアクセスしているゲストユーザーを制限します。 • このコンテンツへのアクセスを必要とするユーザーのために、必要なアクセス制御権限を持つアカウントを作成します。 詳細については、「JSONv2 Web サービス JSONv2 Web サービス」を参照してください。
セキュリティリスク	(高) データソースの JSON 要求で適切な承認が構成されていない場合、無許可のユーザーがターゲットインスタンスの機密コンテンツ/データにアクセスする可能性があります。
参照	認証 着信 JSONv2 要求に対する基本認証の要求

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

WSDL 要求に認証を要求する

glide.basicauth.required.wsdl プロパティを使用して、受信 WSDL (Web Services Description Language) 要求で基本認証を要求するかどうかを指定します。

注:
受信 WSDL 要求に基本認証を要求しないという選択をする場合は、アクセス制御 (ACL) ルールを変更してゲストユーザーが WSDL コンテンツにアクセスできるようにする必要があります。

詳細情報

警告:
これはセーフハーバープロパティです。つまり、いったん変更したら変えることはできません。元に戻すことはできません。

属性	説明
プロパティ名	*glide.basicauth.required.wsdl*
構成タイプ	システムプロパティ (/sys_properties_list.do)
カテゴリ	API と Web サービス
目的	WSDL 要求に対して基本認証を適用すること
推奨値	true
セキュリティリスク評価	4.3
機能への影響度	(低) この修正では、基本認証とシステムレベルのアクセス制御の形で、認証方法の組み合わせが適用されます。 • インスタンス上で WSDL データの形式でテーブル/ページからデータを取得する際に、この認証を実行します。 • 現在このデータにアクセスしているゲストユーザーを制限します。必要であれば、このコンテンツへのアクセスを必要とするユーザーのために、必要なアクセス制御権限を持つ新しいアカウントを作成する場合があります。
セキュリティリスク	(中) WSDL Web サービスで適切な承認が構成されていない場合、無許可のユーザーがターゲットインスタンスの機密 WSDL コンテンツ/データにアクセスする可能性があります。
参照	Web サービスセキュリティ

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

XML 要求に認証を要求する

glide.basicauth.required.xml プロパティを使用して、受信 XML 要求で基本認証を要求するかどうかを指定します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

詳細情報

⚠ 警告:
これはセーフハーバープロパティです。つまり、いったん変更したら変えることはできません。元に戻すことはできません。

属性	説明
プロパティ名	*glide.basicauth.required.xml*
構成タイプ	システムプロパティ (/sys_properties_list.do)
カテゴリ	API と Web サービス
目的	XML 要求に対して基本認証を適用すること
セキュリティリスク評価	7.5
推奨値	true
機能への影響度	(低) この修正では、基本認証とシステムレベルのアクセス制御の形で、認証方法の組み合わせが適用されます。 • インスタンス上で XML データの形式でテーブル/ページからデータを取得する際に、この認証を実行します。 • 現在このデータにアクセスしているゲストユーザーを制限します。必要であれば、このコンテンツへのアクセスを必要とするユーザーのために、必要なアクセス制御権限を持つ新しいアカウントを作成する場合があります。 詳細については、「XML パーサーステップ」を参照してください。
セキュリティリスク	(高) 受信 XML 要求で適切な承認が構成されていない場合、無許可のユーザーがターゲットインスタンスの機密コンテンツ/データにアクセスする可能性があります。
参照	認証

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

XML 出力依頼に権限を要求する

すべての受信 XMLOutputProcessor 要求に対して基本認証が必要となるように、このプロパティを構成します。

glide.basicauth.required.xmloutputprocessor プロパティが推奨値の **true** に設定されていない場合、受信 XMLOutputProcessor 要求に基本認証は必要ありません。これにより、インスタンスから情報が非認証で開示される可能性があります。

⚠ 警告:
これはセーフハーバープロパティです。つまり、いったん変更したら変えることはできません。元に戻すことはできません。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

詳細情報

属性	説明
構成名	*glide.basicauth.required.xmloutputprocessor*
構成タイプ	システムプロパティ (/sys_properties_list.do)
データタイプ	ブーリアン
推奨値	true
デフォルト値	true
カテゴリ	API と Web サービス
セキュリティリスク	• 重大度スコア：7.5 • CVSS スコア：高 • セキュリティリスクの詳細：プロパティを推奨値の **true** に設定しないと、機密情報がインスタンスから漏洩する可能性があります。
依存関係と前提条件	なし

XSD 要求に対する認証を必須とする

glide.basicauth.required.xsd プロパティを使用して、受信 XSD (XML Schema Definition) 要求で基本認証を要求するかどうかを指定します。

詳細情報

⚠ 警告:
これはセーフハーバープロパティです。つまり、いったん変更したら変えることはできません。元に戻すことはできません。

属性	説明
プロパティ名	glide.basicauth.required.xsd*glide.basicauth.required.xsd*
構成タイプ	システムプロパティ (/sys_properties_list.do)
カテゴリ	API と Web サービス
目的	XSD 要求に対して基本認証を適用すること
推奨値	true
セキュリティリスク評価	5.3
機能への影響度	(低) この修正では、基本認証とシステムレベルのアクセス制御の形で、認証方法の組み合わせが適用されます。 • インスタンス上で XSD データの形式でテーブル/ページからデータを取得する際に、この認証を実行します。 • 現在このデータにアクセスしているゲストユーザーを制限します。必要であれば、このコンテンツへのアクセスを必要とするユーザーのために、必要なアクセス制御権限を持つ新しいアカウントを作成する場合があります。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

属性	説明
	詳細については、「非インタラクティブセッション」を参照してください。
セキュリティリスク	(中) 受信 XSD 要求で適切な承認が構成されていない場合、無許可のユーザーがターゲットインスタンスの機密コンテンツ/データにアクセスする可能性があります。
参照	認証

スクリプト要求に認証を要求する

glide.basicauth.required.scriptedprocessor プロパティを使用して、受信スクリプト要求で基本認証を要求するかどうかを指定します。

詳細情報

警告:
これはセーフハーバープロパティです。つまり、いったん変更したら変えることはできません。元に戻すことはできません。

属性	説明
プロパティ名	*glide.basicauth.required.scriptedprocessor*
構成タイプ	システムプロパティ (/sys_properties_list.do)
カテゴリ	API と Web サービス
目的	スクリプト要求に対して基本認証を適用すること
推奨値	true
セキュリティリスク評価	7.2
機能への影響度	(中) この修正では、基本承認の形式で認証が適用されます。 • インスタンスでスクリプト要求を処理する際に、この認証を実行します。 • 現在このデータにアクセスしているゲストユーザーを制限します。必要であれば、このコンテンツへのアクセスを必要とするユーザーのために、必要なアクセス制御権限を持つ新しいアカウントを作成する場合があります。
セキュリティリスク	(高) 受信スクリプト要求で適切な承認が構成されていない場合、無許可のユーザーがターゲットインスタンスの機密コンテンツ/データにアクセスします。
参照	認証

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

SCHEMA 要求に認証を要求する

glide.basicauth.required.schema プロパティを使用して、すべての受信 Table Schema Processor 要求に対して基本認証を要求します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

受信 Table Schema Processor は、プラットフォームに対する受信スキーマ要求を処理します。

すべての受信 Table Schema Processor 要求に対して基本認証を要求するには、*glide.basicauth.required.schema* を推奨値の **true** に設定します。すべての受信 Table Schema Processor 要求に対して基本認証を要求しないようにするには、この値を **false** に設定します。

⚠ 警告:
これはセーフハーバープロパティです。つまり、いったん変更したら変えることはできません。元に戻すことはできません。

詳細情報

属性	説明
プロパティ名	*glide.basicauth.required.schema*
構成タイプ	システムプロパティ (/sys_properties_list.do)
カテゴリ	API と Web サービス
目的	すべての受信 Table Schema Processor 要求に対して基本認証を要求します。
推奨値	True (デフォルト値)。
構成タイプ	ブーリアン
セキュリティリスク	(中) このプロセッサーからの認証を省略すると、インスタンスデータへの不正なアクセスが発生します。

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

RSS 要求に認証を要求する

glide.basicauth.required.rss プロパティを使用して、受信 RSS 要求で基本認証を要求するかどうかを指定します。

詳細情報

⚠ 警告:
これはセーフハーバープロパティです。つまり、いったん変更したら変えることはできません。元に戻すことはできません。

属性	説明
プロパティ名	*glide.basicauth.required.rss*
構成タイプ	システムプロパティ (/sys_properties_list.do)
カテゴリ	API と Web サービス
目的	RSS 要求に対して基本認証を適用すること
推奨値	true
セキュリティリスク評価	7.5
機能への影響度	(低) この修正では、基本認証とシステムレベルのアクセス制御の形で、認証方法の組み合わせが適用されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

属性	説明
	• インスタンスで RSS 要求を処理する際に、この認証を実行します。 • 現在このデータにアクセスしているゲストユーザーを制限します。必要であれば、このコンテンツへのアクセスを必要とするユーザーのために、必要なアクセス制御権限を持つ新しいアカウントを作成する場合があります。 詳細については、「RSS フィードジェネレーター」を参照してください。
セキュリティリスク	(高) 受信 RSS 要求で適切な承認が構成されていない場合、無許可のユーザーがターゲットインスタンスの機密コンテンツ/データにアクセスする可能性があります。
参照	RSS 基本認証

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

API 要求に認証を要求する

glide.basicauth.required.api プロパティを使用して、着信 REST 要求の基本認証のセキュリティを強化します。

すべての REST 要求に対して認証を要求するには、*glide.basicauth.required.api* プロパティを **true** に設定します。すべての REST 要求に対して認証をバイパスするには、プロパティを **false** に設定します。

警告:
これはセーフハーバープロパティです。つまり、いったん変更したら変えることはできません。元に戻すことはできません。

詳細情報

属性	説明
プロパティ名	*glide.basicauth.required.api*
構成タイプ	システムプロパティ (/sys_properties_list.do)
カテゴリ	API と Web サービス
目的	着信 RSS 要求の基本認証
推奨値	True (デフォルト)
構成タイプ	文字列
セキュリティリスク	(高) 「glide.basicauth.required.api」が推奨値の「true」に設定されていない場合、API 要求で基本認証が無効になり、インスタンスデータへの非認証アクセスが発生します。
セキュリティリスク評価	8.6

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

アンロード要求に認証を要求する

glide.basicauth.required.unl (useUnloadFormat) プロパティを使用して、受信アンロード要求で基本認証を要求するかどうかを指定します。

詳細情報

属性	説明
プロパティ名	*glide.basicauth.required.unl*
構成タイプ	システムプロパティ (/sys_properties_list.do)
カテゴリ	API と Web サービス
目的	アンロード要求に対して基本認証を適用すること
推奨値	true
セキュリティリスク評価	7.5
機能への影響度	(中) この修正では、基本認証とシステムレベルのアクセス制御の形で、認証方法の組み合わせが適用されます。インスタンス上でアンロードデータの形式でテーブル/ページからデータを取得する際に、この認証を実行します。
セキュリティリスク	(高) データソースのアンロード要求で適切な承認が構成されていない場合、無許可のユーザーがターゲットインスタンスの機密コンテンツ/データにアクセスする可能性があります。
参照	認証

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

アーキテクチャ、設計、および脅威のモデル化

この幅広いコントロールは、安全なアプリケーションを実装するための高レベルの設計上の考慮事項と重要な要素に対応しています。これには、可用性、機密性処理の整合性、否認防止、およびプライバシーが含まれます。さらに、安全なソフトウェア開発ライフサイクルの要素が含まれています。

証明書ベースの認証の適用

glide.authenticate.mutual.enabled プロパティは、証明書ベースの認証を有効にします。これは、Now Platform の REST および SOAP API への受信 REST 接続に対する相互認証の一種です。

相互認証では、セキュアソケットレイヤー (SSL) 証明書を交換して信頼できる認証局で証明書を検証することにより、サーバーとクライアント間の信頼を確立します。これにより、信頼できるソースが Now Platform に接続していることを検証できます。このインスタンスが推奨値の true に設定されていない場合、インスタンスは中間者攻撃 (MitM) に対して脆弱になる可能性があります。

セキュリティ上の脅威を緩和するために、受信 Web サービスの相互認証を有効にします。証明書ベースの認証プラグイン*com.glide.auth.mutual)*Now Platform証明書ベースの認証の設定を初めてインストールする場合は、指示に従ってください。さらに、プラグインをアクティブ化するに

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

は、*glide.authenticate.mutual.enabled* プロパティが true に設定されていることを確認してください。

詳細情報

属性	説明
構成名	*glide.authenticate.mutual.enabled*
構成タイプ	システムプロパティ (/sys_properties_list.do)
データタイプ	ブーリアン
推奨値	true
デフォルト値	true
カテゴリ	アーキテクチャ、設計、および脅威のモデル化
セキュリティリスク	• 重大度スコア：5.3 • CVSS スコア：中 • セキュリティリスクの詳細:このプロパティが推奨値の true に設定されていない場合、証明書ベースの認証は信頼できる認証局で証明書を検証しません。これにより、攻撃者が MitM 攻撃を使用してインスタンスを攻撃する可能性が高まります。
依存関係と前提条件	なし
参照	• https://csrc.nist.gov/glossary/term/man_in_the_middle_attack • 証明書ベースの認証 • 相互認証の構成

人事アプリで **ACL** 評価の代理操作を確認する

sn_hr_core.impersonateCheck プロパティを使用して、ユーザーが別のユーザーの代理操作を行って自身の HR 情報にアクセスすることを防止します。

安全な設定にすると、管理者は代理操作の使用中に他のユーザーの人事情報を表示できなくなります。このプロパティを安全でない設定にすると、管理者がユーザーの代理操作を行い、代理操作されたユーザーのアクセス権でアンケート結果や監査レコードなどの HR データにアクセスできるようになります。メールなどのユーザー自身だけが利用できる情報など、このタイプのデータの性質上、これはお勧めしません。*sn_hr_core.impersonateCheck* を true に設定すると 、ユーザーが他のユーザーの代理操作を行っていない場合にのみ、HR 情報へのアクセスが許可されます。

詳細情報

属性	説明
構成名	*sn_hr_core.impersonateCheck*
構成タイプ	システムプロパティ (/sys_properties_list.do)

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

属性	説明
データタイプ	ブーリアン
推奨値	true
デフォルト値	false
カテゴリ	アーキテクチャ、設計、および脅威のモデル化
セキュリティリスク	• 重大度スコア：2.7 • CVSS スコア：低 • セキュリティリスクの詳細：このプロパティを安全でない設定にすると、管理者がユーザーの代理操作を行い、代理操作されたユーザーのアクセス権でアンケート結果や監査レコードなどの HR データにアクセスできるようになります。
依存関係と前提条件	なし
機能への影響度	このプロパティを true に設定すると、管理者は代理操作の使用中に他のユーザーの HR 情報を表示できなくなります。false に設定すると、管理者はユーザーの代理操作を行い、代理操作されたたユーザーのアクセス権でアンケート結果や監査レコードなどの HR データにアクセスできるようになります。メールなどのユーザー自身だけが利用できる情報など、このタイプのデータの性質上、これはお勧めしません。sn_hr_core.impersonateCheck を true に設定すると 、ユーザーが他のユーザーの代理操作を行っていない場合にのみ、HR 情報へのアクセスが許可されます。

未認証の公開レポートを無効にする

ユーザーがレポートを公開したりアクセスしたりできないようにするには、このプロパティを無効にします。このプロパティによって、レポートの公開レポート機能が無効になります。

glide.report.published_reports.enabled を **true** に設定してレポートの公開を有効にします。

glide.report.published_reports.enabled が **false**に設定されていれば、 レポートへのにセキュリティの強制は準拠しています。

詳細情報

属性	説明
プロパティ名	*glide.report.published_reports.enabled*
構成タイプ	システムプロパティ (/sys_properties_list.do)
カテゴリ	アーキテクチャ、設計、および脅威のモデル化
目的	レポートの公開レポート機能を無効化する。
タイプ	True | False
推奨値	**false**

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

属性	説明
セキュリティリスク評価	6.5
機能への影響度	(中) ユーザーはレポートを公開できません。
セキュリティリスク	(中) このプロパティが有効でないと、ユーザーがレポートにアクセスしたり公開したりして機密データが公開される可能性があります。レポートを公開して、ユーザー以外の人を含め、誰でもレポートにアクセスできる URL を作成します。誰かがその URL に移動すると、インスタンスから現在のデータでレポートが生成されます。
参照	レポートの公開

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

インバウンドクエリ要求でのフィールド **ACL** の強制

インスタンスでの受信クエリの検証方法を管理します。

glide.report.report_view.check_published プロパティを使用して、インスタンスでの受信クエリの検証方法を確認します。このプロパティが推奨値の **true** に設定されている場合、フィールド ACL は受信クエリと比較して確認され、ユーザーに権限がない場合は却下されます。プロパティが **false** に設定されている場合、ACL は受信クエリと比較して確認されずに実行が継続されるため、権限のない当事者に情報が開示される可能性があります。

詳細情報

属性	説明
構成名	*glide.report.report_view.check_published*
構成タイプ	システムプロパティ (/sys_properties_list.do)
データタイプ	ブーリアン
推奨値	true
デフォルト値	true
カテゴリ	アーキテクチャ、設計、および脅威のモデル化
セキュリティリスク	• 重大度スコア：4.4 • CVSS スコア：中 • セキュリティリスクの詳細：このプロパティが **false** に設定されている場合、ACL は受信クエリと比較して確認されないため、情報が開示される可能性があります。
依存関係と前提条件	なし

レポートビューでの読み取り **ACL** の適用

読み取り ACL をインスタンスに適用する方法を管理します。

テーブルまたはフィールドにレポートビュー ACL がない場合に、*glide.report.report_view.read_acl* プロパティを使用してレポート機能の読み取り

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ACL (テーブルレベル) を適用します。このプロパティが **enforce** に設定されていない場合、ACL がバイパスされ、機密情報が漏洩する可能性があります。

詳細情報

属性	説明
構成名	*glide.report.report_view.read_acl*
構成タイプ	システムプロパティ (/sys_properties_list.do)
データタイプ	文字列
推奨値	enforce
デフォルト値	enforce
カテゴリ	アーキテクチャ、設計、および脅威のモデル化
セキュリティリスク	• 重大度スコア：7.1 • CVSS スコア：高 • セキュリティリスクの詳細：このプロパティを **enforce** に設定しないと、ACL がバイパスされる可能性があります。
依存関係と前提条件	なし

許可された **ServiceNow** 内部 **IP** アドレスを定義する

glide.ip.authenticate.strict プロパティを使用して、インスタンスで受信接続を行うことができる IP 範囲を指定します。

glide.ip.authenticate.strict が true に設定されている場合、*glide.ip.authenticate.allow.secured* で指定された IP 範囲のみがインスタンスで受信接続を行うことができます。このプロパティには、必須の ServiceNow 内部 IP 範囲 (セキュア VPN、DC) のみのリストが含まれています。

glide.ip.authenticate.allow.secured が推奨値の「10.0.0.0/8、37.98.232.0/21、103.23.64.0/22、149.96.0.0/17、149.96.0.0/16、199.91.136.0/21、148.139.0.0/16、127.0.0.1、0:0:0:0:0:0:0:1」に設定されていない場合、ServiceNow DataCenter およびセキュアな VPN の外部の信頼できないソースがインスタンスの機密性の高い監視エンドポイントにアクセスできる可能性があります。

⚠ **警告:**
このプロパティの値は、DB なしのオーバーライドです。変更またはオーバーライドすることはできません。

詳細情報

属性	説明
プロパティ名	*glide.ip.authenticate.strict*
構成タイプ	システムプロパティ (/sys_properties_list.do)
カテゴリ	アーキテクチャ、設計、および脅威のモデル化

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

属性	説明
目的	ServiceNow の従業員が、保護された IP 範囲を介してのみインスタンスにアクセスできるようにすること
推奨値	true
セキュリティリスク評価	4.3
機能への影響度	(低) このプロパティが有効になっていない場合、ServiceNow の従業員はすべての IP 範囲を介して顧客のインスタンスにアクセスできます。このプロパティを有効にすると、アクセスが保護された IP 範囲 (セキュア VPN、DC) セットに制限されます。 **注:** このプロパティを `true` に設定すると、Now Platform は、インスタンスにアクセスできる IP 範囲セットに対して、パフォーマンス監視 IP 制限 (*`glide.ip.authenticate.allow.secured`*) プロパティの代わりに、より制限の強い *`glide.ip.authenticate.allow.secured`* プロパティを使用します。
セキュリティリスク	(低) より幅広いユーザーグループに対してインスタンスアクセスが不必要に公開されます。
参照	IP 範囲ベースの認証

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

注: IP アクセス制御に追加されていない IP からのアクセスをすべて制限するには、「すべて拒否」ルールを IP アクセス制御に追加する必要があります。その後、必要な許可された IP をすべて IP アクセス制御に追加する必要があります。

従来の **JQuery** の動作を無効にする

`glide.jquery.legacy` は、古いパッチが事前に適用されたバージョンの JQuery が使用され、ライブラリにパッチ未適用の脆弱性が生じるのを防ぐために使用されます。

古いパッチが事前に適用されたバージョンの JQuery が使用され、ライブラリにパッチ未適用の脆弱性が生じるのを防ぐには、*`glide.jquery.legacy`* を **false** に設定します。パッチが事前に適用されたバージョンの JQuery を許可するには、値を **true** に設定します。

詳細情報

属性	説明
プロパティ名	*`glide.jquery.legacy`*
構成タイプ	システムプロパティ (/sys_properties_list.do)
カテゴリ	アーキテクチャ、設計、および脅威のモデル化
目的	古いバージョンの AngularJS ライブラリで発見された脆弱性に対する攻撃から発生する潜在的なセキュリティリスクを防止します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

属性	説明
推奨値	False
構成タイプ	ブーリアン
セキュリティリスク	(高) ライブラリにパッチ未適用の脆弱性が生じる、古いパッチが事前に適用された JQuery バージョンの使用を防止します。システムプロパティは、パッチ適用されていないバージョンの angularJS に依存してカスタム実装を実行する場合はフェイルセーフです。
セキュリティリスク評価	7.1

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

GlideRecord スコープフェンシングのレガシー動作の有効化

このプロパティは *glide.record.legacy_cross_scope_access_policy_in_script* 、スコープフェンシングを無効にし、スコープ対象アプリがグローバルスクリプトインターフェイスにアクセスできるようにします。これは、GlideRecord のクロススコープアクセスに対するパッチとして作成されました。

GlideRecord は、そのレベルのアクセスで構成されていないテーブルへのクロススコープ作成および更新アクセス権を提供します。このスコープ指定のアクセス動作にパッチを適用したときに、顧客のアプリケーションが壊れないようにするために、*glide.record.legacy_cross_scope_access_policy_in_script* プロパティが作成されました。このプロパティを true に設定すると、クロススコープアクセスは従来の動作にフォールバックしますが、これは安全ではありません。

詳細情報

属性	説明
構成名	*glide.record.legacy_cross_scope_access_policy_in_script*
構成タイプ	システムプロパティ (/sys_properties_list.do)
データタイプ	ブーリアン
推奨値	true
デフォルト値	false
カテゴリ	アーキテクチャ、設計、および脅威のモデル化
セキュリティリスク	• 重大度スコア：5 • CVSS スコア：中 • セキュリティリスクの詳細：スコーピングにより、アプリケーションは、明示的なアクセス権を持つリソースにのみ、または最小特権の原則に従ってスコープ内でのみアクセスできます。この機能を無効にすると、機密性、可用性、および整合性に影響を与える可能性があります。
依存関係と前提条件	なし

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

従来の **AngularJS** の動作を無効にする

glide.angular.legacy プロパティを使用して、古いバージョンの AngularJS ライブラリで発見された脆弱性に対する攻撃から発生する潜在的なセキュリティリスクから保護します。

glide.angular.legacy を推奨値の **false** に設定すると、古いパッチが事前に適用されたバージョンの angularJS が使用されなくなります。古いパッチが事前に適用されたバージョンの angularJS を使用するには、 プロパティを **true** に設定します。

詳細情報

属性	説明
プロパティ名	*glide.angular.legacy*
構成タイプ	システムプロパティ (/sys_properties_list.do)
カテゴリ	アーキテクチャ、設計、および脅威のモデル化
目的	システムプロパティは、パッチ適用されていないバージョンの angularJS に依存してカスタム実装を実行する場合はフェイルセーフです。
推奨値	False
構成タイプ	ブーリアン
セキュリティリスク	(高) 古いバージョンの angularJS を使用すると、古いバージョンの AngularJS ライブラリで発見された脆弱性に対する攻撃から発生する潜在的なセキュリティリスクが生じる可能性があります。
セキュリティリスク評価	7.1

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

お気に入りへの公開アクセス

glide.ui.magellan.favorites.allow_public を使用して、認証されていないユーザーがナビゲーターで [お気に入り] を表示できるようにするかどうかを指定します。

glide.ui.magellan.favorites.allow_public が **false** に設定されている場合、お気に入りへの公開アクセスは準拠します。

詳細情報

属性	説明
プロパティ名	*glide.ui.magellan.favorites.allow_public*
構成タイプ	システムプロパティ (/sys_properties_list.do)
Instance Security Center での構成	あり
目的	認証されていないユーザーがナビゲーターで [お気に入り] を表示できるようにするかどうかを制御します。
タイプ	True/False
推奨値	*false*

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

属性	説明
セキュリティ依存関係	*glide.ui.magellan.favorites.allow_public* を **false** に設定します。
機能への影響度	(中) このプロパティを有効にすると、権限のないユーザーから保護するレイヤーとして機能します。
セキュリティリスク	(中) このプロパティを有効にしないと、機密データに不正にアクセスされるリスクがあります。
参照	お気に入りの作成または表示

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

データブローカー **REST API** の認証を要求

glide.basicauth.required.databrokerrestapiprocessor プロパティを使用して、すべての受信 Data Broker Rest API 要求に対して基本認証を要求します。

このプロパティが **true** に設定されている場合、認証が適用されます。**false** に設定されている場合は、認証が使用されないため、機密情報がインスタンスから漏洩する可能性があります。

> ⚠ 警告:
> これはセーフハーバープロパティです。つまり、いったん変更したら変えることはできません。元に戻すことはできません。

詳細情報

属性	説明
構成名	*glide.basicauth.required.databrokerrestapiprocessor*
構成タイプ	システムプロパティ (/sys_properties_list.do)
データタイプ	ブーリアン
推奨値	true
デフォルト値	true
カテゴリ	アーキテクチャ、設計、および脅威のモデル化
セキュリティリスク	• 重大度スコア：8.6 • CVSS スコア：高 • セキュリティリスクの詳細：プロパティが **false** に設定されている場合、API 認証は適用されず、攻撃者が機密データにアクセスできるようになります。
依存関係と前提条件	なし

空の **ACL** でデフォルトで拒否

glide.sm.default_mode プロパティを使用して、既存の ACL ルールがワイルドカードテーブルの ACL ルールの一部であることが判明した場合の、セキュリティマネージャーのデフォルトの動作を制御します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

初期インスタンスのインストール中に High Security Settings (com.glide.high_security) プラグインがアクティブ化されると、このプロパティが作成され、ワイルドカード ACL ルールが作成されます。システムテーブルへのロールベースのアクセスを提供するために、これらのルールは多数の ACL と最も一般的なレコードベースの操作を制御します。

- 読み取り
- 書き込み
- 作成
- 削除

デフォルトの拒否オプションを有効にして High Security プラグインを使用しないかぎり、多くのテーブルは保護されません。Now Platform では、管理者以外のユーザーは一致する ACL ルールを満たさないかぎりオブジェクトにアクセスできないという、デフォルトの拒否セキュリティモデルを使用します。このモデルを使用して、安全でないスクリプトなどの多くの攻撃ベクトルを削除します。

警告:
これはセーフハーバープロパティです。つまり、いったん変更したら変えることはできません。元に戻すことはできません。

詳細情報

属性	説明
プロパティ名	*glide.sm.default_mode*
構成タイプ	システムプロパティ (/sys_properties_list.do)
カテゴリ	アーキテクチャ、設計、および脅威のモデル化
目的	セキュリティ上のベストプラクティスは、無許可のユーザーによるテーブルへのアクセスを制限することです。 • テーブルに ACL ルールがない場合、このプロパティは、テーブル/フィールドで実行される CRUD 操作に対して少なくともワイルドカード ACL が検証されるようにします。 • これらのルールでは、ユーザーが admin ロールを所有しているか、別のテーブル ACL ルールの要件を満たしている場合を除き、読み取り、書き込み、作成、削除の操作をすべてのテーブルで制限します。
推奨値	拒否
機能への影響度	(高) このプロパティを [許可] に設定すると、ワイルドカードテーブル ACL ルールは、そのような操作を制限する特定のテーブル ACL ルールが存在する場合を除き、CRUD 操作をすべてのテーブルで許可します。 **注:** このプラグインは、本番環境で既に使用されているテーブルへのセキュリティアクセスを変更する可能性があるため、既存のインスタンスを対象としていません。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

属性	説明
セキュリティリスク	8.8
参照	デフォルトの拒否プロパティ

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

認証

認証カテゴリは、エンティティとその主張が本物で正確であり、偽装を防止し、パスワードの傍受を防止していることを確認するための最新の認証の主要な要素をカバーしています。

ASVS 標準は、このセクションの NIST 800-63b (https://pages.nist.gov/800-63-3/sp800-63b.html) 仕様に基づいて構築されています。

認証には、パスワードポリシー、コントロールとストレージ、認証システムの適切な実装、帯域外または 1 回限りの検証機能の適切な実装が含まれます。

ロールベースのマルチファクター認証の有効化

glide.authenticate.multifactor プロパティを使用して、特定のロールに割り当てられたすべてのユーザーにロールベースのマルチファクター認証 (MFA) を適用します。

マルチファクター認証は、ユーザーに割り当てられたロールに基づいて適用します。マルチファクターロールリストで「admin」、「security_admin」または「user_admin」のロールがユーザーに割り当てられている場合は、MFA が適用されます。

- 特定のロールに割り当てられたすべてのユーザーに対してロールベースのマルチファクター認証を適用するには、このプロパティを **true** に設定します。
- 特定のロールに割り当てられたすべてのユーザーに対してロールベースのマルチファクター認証を無効にするには、このプロパティを **false** に設定します。

詳細情報

属性	説明
プロパティ名	*glide.authenticate.multifactor*
構成タイプ	システムプロパティ (/sys_properties_list.do)
カテゴリ	認証
目的	特定のロールに割り当てられたすべてのユーザーに対してロールベースのマルチファクター認証を適用する。
タイプ	True/False
推奨値	*true*
セキュリティ依存関係	[マルチファクター基準] テーブルで、[ロールベースのマルチファクター認証 **(Role-based multi-factor authentication)**] をアクティブ化します。
セキュリティリスク評価	7.2
機能への影響度	(中) このプロパティを有効にすると、ユーザーのエクスペリエンスが向上します。これは、侵害された資格情報に対

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

属性	説明
	する保護およびセキュリティの追加レイヤーとして機能します。
セキュリティリスク	(中) このプロパティを有効にしないと、機密データに不正にアクセスされるリスクがあります。
参照	ロールベースのマルチファクター基準の設定

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

アカウント復旧の有効化

glide.sso.acr.enabled プロパティは、アカウント復旧機能を制御します。

glide.sso.acr.enabled を推奨値 **true** に設定すると、ユーザー ID によるアカウント復旧が可能になります。ユーザー ID によるアカウント復旧を禁止するには、値を **false** に設定します。

詳細情報

属性	説明
プロパティ名	*glide.sso.acr.enabled*
構成タイプ	システムプロパティ (/sys_properties_list.do)
カテゴリ	認証
目的	ユーザー ID 機能によってアカウント復旧機能を制御します。
推奨値	True (デフォルト)
構成タイプ	ブーリアン
セキュリティリスク	重大 (このプロパティを有効にしないと、ユーザーはユーザー ID でアカウントを復旧できません)。
セキュリティリスク評価	9.1
参照	詳細については、「アカウント復旧 (ACR)」を参照してください。

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

クラシックモバイルアプリ **UI** の難読化の要求

glide.ui.m.blur_ui_when_backgrounded プロパティを使用して、バックグラウンド処理中に画像を保存する際に、スナップショットのすべてのフィールドを難読化します。

Android デバイスでは、アプリケーションがバックグラウンドに送信されるときに、Android オペレーティングシステムによって最新のタスクメニューで使用されるスクリーンショットが取得されます。ユーザーは、アプリケーションのスクリーンショットを手動で撮影し、公開状態でデバイスに保存することもできます。

iOS デバイスでは、iOS オペレーティングシステムによってアプリケーションで画像ファイルを保存できるようにすることもできます。このファイルは、アプリケーションがバックグラウンドに送信されたときにユーザーが最後に表示した画面です。ユーザーエクスペリエンスを向上させることが目的ですが、画像が PNG 画像ファイルとして保存されるため、セキュリティ上のリスクも生じます。

自動翻訳

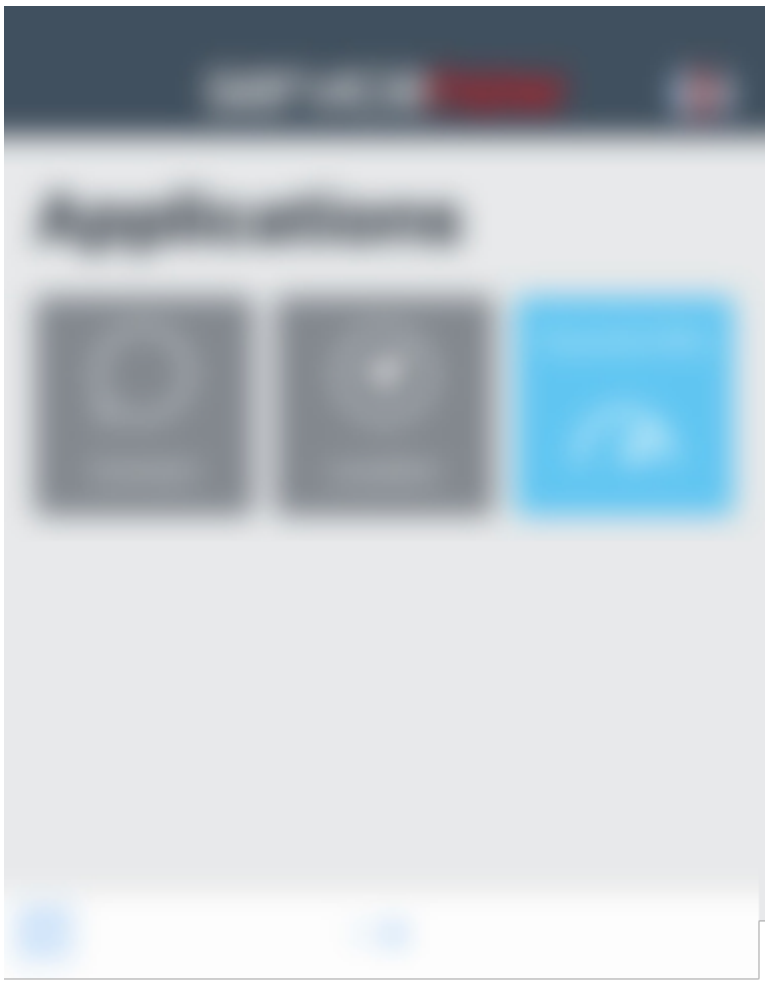
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注:
この設定や構成はインスタンス単位で行われるため、ユーザーは プロパティを設定してインスタンスに接続する必要があります。

ServiceNow Classic アプリのスナップショットのフィールドをすべて難読化するには、「セキュリティ向上のためのアプリをぼかすオプションの設定」を参照してください。

例

このプロパティを true に設定すると、バックグラウンドアプリケーションは、iOS デバイスでは難読化され、Android iOS デバイスではブラックアウトされます。



詳細情報

属性	説明
プロパティ/プラグイン名	*glide.ui.m.blur_ui_when_backgrounded*
構成タイプ	システムプロパティ (/sys_properties_list.do)
カテゴリ	認証
目的	バックグラウンド処理中に画像を保存する際に、スナップショットのすべてのフィールドを難読化すること
推奨値	true
セキュリティリスク評価	2.4

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

属性	説明
機能への影響度	(低) *glide.ui.m.blur_ui_when_backgrounded* プロパティが true に設定されている場合、ネイティブアプリは、アプリがバックグラウンドに入った時点でサーバーで定義されたパラメーターを使用して画面をぼかします。 • アプリがバックグラウンドに入ると、iOS と Android で撮影されたスクリーンショットがぼやけて表示されます。 • アプリがバックグラウンドに送信されるとコンテンツが表示されなくなるため、ユーザーエクスペリエンスに悪影響を与える可能性があります。
セキュリティリスク	(中) 侵害された (ジェイルブレイクされた) デバイスは、ファイルシステムへのフルアクセス権を持ち、機密情報が埋め込まれたファイル/スナップショットにアクセスできます。

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

パスワードなしの認証の無効化

glide.login.no_blank_password プロパティを使用すると、ユーザーが NOW プラットフォームに空白のパスワードでログインしたり、 [パスワード] フィールドを空のままにしたりできなくなります。

管理者が意図的に空の値または空白のパスワードをユーザーレコードに割り当てた場合でも、ユーザーは [パスワード] フィールドに値を指定しなければログインできなくなります。

詳細情報

属性	説明
プロパティ名	*glide.login.no_blank_password*
構成タイプ	システムプロパティ (/sys_properties_list.do)
Instance Security Center での構成	あり
目的	組織内ではユーザー名が簡単に推測できることがあるため、強力な認証を確実に実現すること
推奨値	true
機能への影響度	(低) 空白のパスワードは重大なセキュリティリスクと見なされるため、使用するべきではありません。ただし、このような使用法に有効なケースがある場合は、機能停止する可能性があります。パスワードが空白のユーザーは、インスタンスにログインできません。
セキュリティリスク	(高) 攻撃者は、デフォルトのユーザー名を使用して、またはパスワードのない特定の個人/グループ (通常は firstname.lastname) を使用してインスタンスにログインできます。この操作は、公開ユーザーがインスタンスデータの機密性と完全性を侵害する可能性があるため、重大なセキュリティリスクと見なされます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ログイン時にパスワードポリシーを適用しない

インスタンスでパスワードの複雑さの処理方法を管理します。

glide.apply.password_policy.on_login プロパティを使用して、パスワードの複雑さを管理します。このプロパティが **false** に設定されている場合、ログイン時にパスワードの複雑さが強制されません。**true** に設定されている場合、パスワードの複雑さが強制され、組織のポリシーコンプライアンスの問題が発生する可能性があります。 アプリケーション セキュリティ検証標準 (ASVS) では、パスワードの複雑さを強制する代わりに、パスワードの長さに 12 文字以上を適用することが提案されています。

詳細情報

属性	説明
構成名	*glide.apply.password_policy.on_login*
構成タイプ	システムプロパティ (/sys_properties_list.do)
データタイプ	ブーリアン
推奨値	false
デフォルト値	false
カテゴリ	認証
セキュリティリスク	• 重大度スコア：4.4 • CVSS スコア：中 • セキュリティリスクの詳細：このプロパティを **true** に設定すると、パスワードの複雑さが強制され、組織のコンプライアンスの問題が発生する可能性があります。
依存関係と前提条件	なし

ブラックリストに含まれているパスワードの検証チェックの有効化

[除外されたパスワード] テーブルでブラックリストに含まれているパスワードを管理します。

glide.enable.blacklist_password プロパティを使用して、ブラックリストに含まれているパスワードを監視します。プロパティが **True** に設定されている場合、ユーザーのパスワードはブラックリストに含まれたパスワードのリストと照合され、侵害されたパスワードのセットからのパスワードを使用できないようになります。管理者は、[除外されたパスワード] テーブルにパスワードを挿入することでリストを管理できます。

詳細情報

属性	説明
構成名	*glide.enable.blacklist_password*
構成タイプ	システムプロパティ (/sys_properties_list.do)
データタイプ	ブーリアン
推奨値	true
デフォルト値	false

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

属性	説明
カテゴリ	認証
依存関係と前提条件	なし
参照	インスタンスのパスワードポリシーによるパスワードの除外

外部ユーザー登録用に CAPTCHA を有効にする

sn_ext_usr_reg.captchaEnabled は、外部ユーザー登録のために CAPTCHA を検証するかどうかを制御します。

sn_ext_usr_reg.captchaEnabled を推奨値の **true** に設定すると、外部ユーザー登録で CAPTCHA を要求することで自動アカウント作成攻撃を防ぐことができます。外部ユーザー登録に CAPTCHA を要求しない場合は、値を **false** に設定します。

詳細情報

属性	説明
プロパティ名	*sn_ext_usr_reg.captchaEnabled*
構成タイプ	システムプロパティ (/sys_properties_list.do)
カテゴリ	認証
目的	このプロパティは、CSP、Community などのポータルで外部ユーザー登録を実行するときに CAPTCHA 検証を有効または無効にするために使用されます。これは、VAM や CSM Guest Walkup などのストアアプリでも CAPTCHA を有効または無効にするために使用されます。
推奨値	true
構成タイプ	ブーリアン
セキュリティリスク	(低) このプロパティは、外部ユーザー登録での CAPTCHA の有効化を制御します。理想的でない値を指定すると、セキュリティの脆弱性をもたらす可能性があります。
セキュリティリスク評価	3.7

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

パスワードリセットで CAPTCHA を有効にする

password_reset.captcha.ignore プロパティを使用して、ユーザーがパスワードをリセットするときに CAPTCHA チャレンジの要求を有効または無効にします。

ユーザーがパスワードをリセットする際に CAPTCHA チャレンジを要求するには、*password_reset.captcha.ignore* を推奨値の **false** に設定します。パスワードリセットの CAPTCHA オプションを無視するには、値を **true** に設定します。

CAPTCHA は、自動化されたシステムでは簡単に回答できないチャレンジ応答をユーザーに表示することで、自動化攻撃を防止するために役立ちます。CAPTCHA を無効にすると、パスワードリセット機能に対する自動攻撃が成功する可能性が高くなります。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

注:
このプロパティは、パスワードリセットの自動化にのみ使用されます。

詳細情報

属性	説明
プロパティ名	*password_reset.captcha.ignore*
構成タイプ	システムプロパティ (/sys_properties_list.do)
カテゴリ	認証
目的	このプロパティは、パスワードリセット時の CAPTCHA 検証を有効または無効にするために使用されます。
推奨値	false
構成タイプ	ブーリアン
セキュリティリスク	(中) 理想的でない値を指定すると、セキュリティの脆弱性をもたらす可能性があります。
セキュリティリスク評価	5.5

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

マルチファクター認証のメール **OTP** の有効化

インスタンスで 2 要素認証の適用方法を管理します。

glide.authenticate.multifactor.email.otp.enabled プロパティを使用して、2 要素認証のトークンをメールを使用して送信するかどうかを制御します。メールは脆弱な MFA 要素と見なされており、MFA をバイパスするために攻撃者がアクセス権を取得する可能性があります。このプロパティを **false** に設定すると、攻撃者がユーザーのパスワードを侵害したときに MFA をバイパスするリスクが軽減されます。

詳細情報

属性	説明
構成名	*glide.authenticate.multifactor.email.otp.enabled*
構成タイプ	システムプロパティ (/sys_properties_list.do)
データタイプ	ブーリアン
推奨値	false
デフォルト値	true
カテゴリ	認証

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

属性	説明
セキュリティリスク	• 重大度スコア：3.1 • CVSS スコア：低 • セキュリティリスクの詳細：このプロパティを **false** に設定すると、攻撃者が 2 要素認証をバイパスするリスクが軽減されます。
依存関係と前提条件	なし
参照	メールを使用したマルチファクター認証

パスワードリセットポリシーチェックを有効にする

glide.enable.password_policy プロパティを使用して、ユーザーがユーザーインターフェイスを使用してパスワードを変更するたびに、パスワードポリシーのチェックを有効にします。

このプロパティを有効にした後に使用するパスワードポリシーを定義するには、「インスタンスでのパスワードポリシーの有効化」を参照してください。

注:
glide.enable.password_policy は、管理者がパスワードを変更する場合や、スクリプトを使用してユーザーを追加する場合には適用されません。

警告:
これはセーフハーバープロパティです。つまり、いったん変更したら変えることはできません。元に戻すことはできません。

詳細情報

属性	説明
プロパティ名	*glide.enable.password_policy*
構成タイプ	システムプロパティ (/sys_properties_list.do)
カテゴリ	認証
目的	パスワード変更時にパスワードポリシーを適用すること
推奨値	true (より強力なパスワードの場合)
セキュリティリスク評価	7.4
機能への影響度	(中) プロパティを true に設定すると、ユーザーがパスワードをリセットするときにパスワードポリシーチェックがオンになります。
セキュリティリスク	(中) パスワードポリシーがない場合、ユーザーが脆弱なパスワードを作成するため、攻撃者がインスタンスにアクセスする可能性が高くなります。

設定手順

Instance Security Center の [ハードニングコンプライアンス構成] ページでこの設定を構成する場合は、次の手順を実行します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

1. [中] で、**[Session Management]** を選択します。
2. [パスワードリセットポリシーチェックの有効化 **(Enable Password Reset Policy Checks)**] 設定で、パスワードの強度を中程度にする場合は [中] を、より強力なパスワードにする場合は [強 **(strong)**] を選択します。これらのオプションのいずれかを選択すると、**glide.enable.password_policy** プロパティが true に設定され、パスワードポリシーを自動的に更新するワークフローが開始されます。

さらに、*glide.apply.password_policy.on_login* システムプロパティを設定して、ログイン時のパスワードポリシーチェックを有効にすることもできます。

LDAP Authentication での SSL の有効化

インスタンスで LDAP 認証要求の暗号化を管理します。

glide.ldap.use.ssl プロパティを使用して、ネットワーク経由で送信される LDAP Authentication 要求の TLS 暗号化を有効または無効にします。このプロパティが推奨値の **true** に設定されていない場合、LDAP Authentication は中間者攻撃の影響を受けやすくなります。

詳細情報

属性	説明
構成名	*glide.ldap.use.ssl*
構成タイプ	システムプロパティ (/sys_properties_list.do)
データタイプ	ブーリアン
推奨値	true
デフォルト値	true
カテゴリ	認証
セキュリティリスク	• 重大度スコア：8.1 • CVSS スコア：高 • セキュリティリスクの詳細：このプロパティを **false** に設定すると、LDAP Authentication は中間者攻撃に対して脆弱になります。
依存関係と前提条件	なし
参照	LDAP Authentication での SSL の有効化

外部ユーザー登録リンクの有効期限を最小限に抑える

登録リンクにアクセスできる日数を管理します。

sn_ext_usr_reg.Reg_link_expiration_days プロパティを使用して、登録リンクにアクセスできるユーザーを管理します。リンクが推奨値の **3** に設定されている場合、目的のユーザー以外のユーザーが後で登録リンクを見つけたときに、その登録リンクが使用される可能性があります。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

詳細情報

属性	説明
構成名	*sn_ext_usr_reg.Reg_link_expiration_days*
構成タイプ	システムプロパティ (/sys_properties_list.do)
データタイプ	整数
推奨値	3
デフォルト値	3
カテゴリ	認証
セキュリティリスク	• 重大度スコア：中 • CVSS スコア：6.6 • セキュリティリスクの詳細：このプロパティを整数 3 に設定しないと、意図しないユーザーによって登録リンクが使用される可能性があります。
依存関係と前提条件	なし

失敗したログイン試行の管理

ユーザーがパスワードの入力を何度間違えると Now Platform からロックアウトされるかをサイト管理者が管理できるようにするために、2 つのスクリプトアクションが用意されています。これらのスクリプトアクションのいずれかを有効にして、ログイン試行の失敗を管理できます。

詳細情報

属性	説明
プロパティ/プラグイン名	適用外
構成タイプ	[システムポリシー] > [スクリプトアクション]
カテゴリ	認証
目的	ログイン試行の失敗に対して厳格なポリシーを適用し、資格情報に対する総当たり攻撃を防止すること
推奨値	有効
セキュリティリスク評価	7.3
機能への影響度	(低) この修正により、インスタンスの管理者は悪意のあるユーザーアクセスを監視および報告できるようになります。機能への影響はなく、ユーザーエクスペリエンスのみが変わります。
セキュリティリスク	(中) 定義されたログ記録と監査戦略を適用して、不審なアクティビティを適切なタイミングで特定して対処できるようにします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

設定手順

1. 移動先 システムポリシー > スクリプトアクション。
2. 名前「*SNC User*」を検索します。
3. 失敗したログイン試行を管理できるようにするには、*SNC User Lockout Check with Auto Unlock* または *SNC User Lockout Check* スクリプトアクションのいずれかの [アクティブ] ステータスを **false** から **true** に変更します。
4. ログイン成功後にログイン失敗回数のカウンターをリセットするには、*SNC User Clear* スクリプトアクションをアクティブ化します。

失敗したログインロック解除のタイムアウト期間を最大化

ユーザーがパスワードの入力を何度間違えると Now Platform からロックアウトされるかをサイト管理者が管理できるようにするために、2 つのスクリプトアクションが用意されています。これらのスクリプトアクションのいずれかを有効にして、ログイン試行の失敗を管理できます。

詳細情報

属性	説明
プロパティ名	*glide.user.unlock_timeout_in_mins*
構成タイプ	[システムポリシー] > [スクリプトアクション]
カテゴリ	認証
目的	ログイン試行の失敗に対して厳格なポリシーを適用し、資格情報に対する総当たり攻撃を防止すること
推奨値	有効
機能への影響度	(低) この修正により、インスタンスの管理者は悪意のあるユーザーアクセスを監視および報告できるようになります。機能への影響はなく、ユーザーエクスペリエンスのみが変わります。
セキュリティリスク	(中) 定義されたログ記録と監査戦略を適用して、不審なアクティビティを適切なタイミングで特定して対処できるようにします。

設定手順

1. 移動先 システムポリシー > スクリプトアクション。
2. 名前「*SNC User*」を検索します。
3. 失敗したログイン試行を管理できるようにするには、*SNC User Lockout Check with Auto Unlock* または *SNC User Lockout Check* スクリプトアクションのいずれかの [アクティブ] ステータスを **false** から **true** に変更します。
4. ログイン成功後にログイン失敗回数のカウンターをリセットするには、*SNC User Clear* スクリプトアクションをアクティブ化します。

モバイルアプリ **UI** の難読化を必須にする

アプリがバックグラウンドで実行されているときにアプリの UI がぼやけるように、*glide.sg.blur_ui_when_backgrounded* プロパティを設定します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

このプロパティが推奨値の **true** に設定されていない場合、アプリスイッチャーから表示するとモバイルアプリのユーザーインターフェイスが表示されます。UI は、アプリがバックグラウンドで実行されている場合でも表示され、エンドユーザーに低レベルのセキュリティと機密性を提供します。

詳細情報

属性	説明
構成名	*glide.sg.blur_ui_when_backgrounded*
構成タイプ	システムプロパティ (/sys_properties_list.do)
データタイプ	ブーリアン
推奨値	true
デフォルト値	false
カテゴリ	ファイルとリソース
セキュリティリスク	• 重大度スコア：2.4 • CVSS スコア (CVSS score)：低 • セキュリティリスクの詳細 (Security risk details)：値を **true** に設定すると、アプリがバックグラウンドで実行されているときに UI がぼやけて表示されるため、ローカルデバイスの機密性とプライバシーが向上します。
依存関係と前提条件	なし
参照	モバイル UI の難読化

パスワードのリセット/変更プロセス中にユーザーに通知

このアプリケーションを使用して、エンドユーザーを有効にし、セルフサービスプロセスを使用して、パスワードをリセットまたは変更します。

このアプリケーションを使用すると、エンドユーザーはセルフサービスプロセスを使用してパスワードをリセットまたは変更できます。または、エンドユーザーのパスワードをリセットするためにサービスデスク担当者を必要とするプロセスを組織で実装することもできます。

詳細情報

属性	説明
構成名	*pwd_process.change, pwd_process.reset*
構成タイプ	システムプロパティ (/sys_properties_list.do)
データタイプ	ブーリアン
推奨値	true
デフォルト値	true
カテゴリ	認証

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

属性	説明
セキュリティリスク	• 重大度スコア：8.1 • CVSS スコア：高 • セキュリティリスクの詳細：パスワードの変更やリセットプロセスでパスワードの更新についてユーザーに通知されない場合、知らないうちに攻撃者がユーザーをアカウントからロックアウトできる可能性があります。これにより、攻撃者が悪意のあるアクティビティを実行する時間が長くなります。パスワードの変更またはリセットの際に、パスワードリセットプロセスがユーザーに通知することを確認します。
依存関係と前提条件	なし

ようこそページからの資格情報の削除

ようこそページのデフォルトコンテンツを変更し、デフォルトの資格情報を削除します。

2 つの [ログイン方法 **(How to Login)]** レコードは、CMS プラグインのデモデータの一部としてインストールされます。

注:
インスタンスのデモデータをインストールしない場合、これらのレコードは存在しません。その場合、推奨されるセキュリティプラクティスに従って、構成はセキュリティ準拠と見なされます。

詳細情報

属性	説明
名前	*How to login*
構成タイプ	テーブル：sys_home
カテゴリ	認証
目的	デモデータとともに追加されたデフォルトの資格情報をようこそページから削除する。
推奨値	デモデータが利用されなかった場合は False または null。
構成タイプ	ブーリアン
セキュリティリスク	(中) デモデータは CMS プラグイン用に提供されています。これには、ようこそページに含まれる 2 つのデフォルトパスワードが含まれています。これが削除されない場合、権限のない攻撃者がインスタンスにアクセスできる可能性があります。
参照	https://support.servicenow.com/kb_view.do?sysparm_article=KB0550107 Welcome pages

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

パスワードリセットの1日あたりの最大SMSを最小化

検証目的で送信される 1 日あたりの SMS コードの最大数を管理します。

password_reset.sms.max_per_day プロパティは、ユーザーが検証のために送信できる 1 日あたりの SMS コードの最大数を表します。

詳細情報

属性	説明
構成名	*password_reset.sms.max_per_day*
構成タイプ	システムプロパティ (/sys_properties_list.do)
データタイプ	整数
推奨値	10
デフォルト値	10
カテゴリ	認証
セキュリティリスク	• 重大度スコア：5.9 • CVSS スコア：中 • セキュリティリスクの詳細：このプロパティが推奨値の **10** 以下に設定されていない場合は、SMS コードの総当たり攻撃が容易になります。
依存関係と前提条件	なし

パスワードリセット要求の有効期限の最小化

password_reset.request.expiry は、ユーザーがパスワードリセットプロセスを実行する必要がある期間 (分単位)を指定します。

注:
password_reset.request.expiry プロパティの設定は、デフォルトで 12 時間に設定される *glide.pwd_reset.onetime.token.validity* プロパティの設定よりも優先されます。

詳細情報

属性	説明
プロパティ名	*password_reset.request.expiry*
構成タイプ	システムプロパティ (/sys_properties_list.do)
カテゴリ	認証
目的	ユーザーがパスワードリセットプロセスを実行する必要がある期間 (分単位) を指定します。
推奨値	**10** 以下の整数に設定します。デフォルト値は 10 です。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

属性	説明
構成タイプ	整数値
セキュリティリスク	(中) プロパティが 10 以下の推奨値に設定されていない場合、他のユーザーがその要求を推測して使用し、パスワードのリセットを試行する可能性が高くなります。
セキュリティリスク評価	4.2
参照	Password Reset プロパティの設定

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

パスワードリセット要求の最大試行許容量を最小化

password_reset.request.max_attempt は、指定された期間ロックアウトされるまでにユーザーが実行できるパスワードのリセットまたは変更の最大試行失敗回数を制御するために使用されます。

詳細情報

属性	説明
プロパティ名	*password_reset.request.max_attempt*
構成タイプ	システムプロパティ (/sys_properties_list.do)
カテゴリ	認証
目的	ユーザーがパスワードリセットプロセスからロックアウトされるまでに実行できる、パスワードリセットの最大試行失敗回数を示します。ロックアウト期間は *password_reset.request.max_attempt_window* の値によって決まります。
推奨値	3 未満の正の整数値に設定します。デフォルト値は **[3]** です。プロパティの上限を決定するときは、ユーザーが実行しているタスクを考慮してください。
構成タイプ	正の整数値
セキュリティリスク	(高) プロパティが推奨値の「**3**」またはその他の妥当な小さい値に設定されていない場合、パスワードリセットプロセスに対して総当たり攻撃が行われる可能性があります。
セキュリティリスク評価	7.5
参照	Password Reset プロパティの設定

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

パスワードリセット要求の最大試行回数ウィンドウ期間を最小化

password_reset.request.max_attempt_window プロパティは、*password_reset.request.max_attempt* プロパティで設定された最大試行失敗回数を超えた場合に、ユーザーがパスワードのリセットまたは変更を待機する必要がある時間 (分数) を制御します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

詳細情報

属性	説明
プロパティ名	*password_reset.request.max_attempt_window*
構成タイプ	システムプロパティ (/sys_properties_list.do)
カテゴリ	認証
目的	パスワードリセットの最大試行失敗回数に達した後のロックアウト期間 (分数) を示します。
推奨値	**1440** 以下の正の整数値に設定します。デフォルト値は **1440** 分です。
構成タイプ	正の整数値
機能への影響度	
セキュリティリスク	(高) プロパティが 1440 以下の推奨値に設定されていない場合、誤った認証試行の最大回数に達してもアカウントがロックされないため、アカウントの総当たりを実行できる可能性があります。
セキュリティリスク評価	7.5
参照	Password Reset プロパティの設定

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

パスワードリセット要求の再試行期間の最大化

password_reset.request.retry_window プロパティは、パスワードリセットの試行回数が更新されるまでの時間 (分数) を制御します。

詳細情報

属性	説明
プロパティ名	*password_reset.request.retry_window*
構成タイプ	システムプロパティ (/sys_properties_list.do)
カテゴリ	認証
目的	再試行回数が 0 にリセットされるまでの、最後の要求からのパスワード試行回数の更新までの時間 (分数) を示します。
推奨値	**1440** 以上の正の整数値に設定します。デフォルト値は **1440** 分です。
構成タイプ	正の整数値
セキュリティリスク	(高) プロパティが推奨値の 1440 以上に設定されていない場合、パスワードリセットプロセスに対してアカウントの総当たり攻撃が行われる可能性があります。
セキュリティリスク評価	7.5

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

属性	説明
参照	Password Reset プロパティの設定

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

パスワードリセット要求の成功期間を最小化

password_reset.request.success_window プロパティは、パスワードが正常にリセットされた後で、ユーザーがパスワードのリセットまたは変更を待機する必要がある時間 (分数) を制御します。指定された期間、ユーザーはパスワードを再度リセットすることができません。

詳細情報

属性	説明
プロパティ名	*password_reset.request.success_window*
構成タイプ	システムプロパティ (/sys_properties_list.do)
カテゴリ	認証
目的	パスワードを正常にリセットした後で、ユーザーがパスワードを再度リセットするために待機しなければならない時間 (分数) を示します。
推奨値	**1440** 以下の正の整数値に設定します。デフォルト値は **1440** 分です。
構成タイプ	正の整数値
セキュリティリスク	(高) プロパティが 1440 以下の推奨値に設定されていない場合、他の誰かがパスワードリセット機能を悪用してユーザーアカウントに不正にアクセスする可能性が高くなります。
セキュリティリスク評価	4.9
参照	Password Reset プロパティの設定

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

パスワードリセット要求ロック解除期間の最大化

password_reset.request.unlock_window プロパティは、最後にアカウントのロック解除アクションに成功した後でユーザーがリセット要求を開始するために待機しなければならない時間 (分数) を制御します。

詳細情報

属性	説明
プロパティ名	*password_reset.request.unlock_window*
構成タイプ	システムプロパティ (/sys_properties_list.do)
カテゴリ	認証

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

属性	説明
目的	パスワードを正常にリセットした後で、ユーザーがパスワードを再度リセットするために待機しなければならない時間 (分数) を示します。
推奨値	**1440** 以上の正の整数値に設定します。デフォルト値は **1440** 分です。
構成タイプ	正の整数値
セキュリティリスク	(高) プロパティが 1440 以上の推奨値に設定されていない場合、悪意のある攻撃者が自動ツールを使用してパスワードの総当たり攻撃を行う機会が増えます。
セキュリティリスク評価	5.9
参照	Password Reset プロパティの設定

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

パスワードリセット **SMS** の複雑さの最大化

password_reset.sms.default_complexity プロパティは、パスワードのリセット時に必要な SMS コード検証の最小サイズを制御します。

詳細情報

属性	説明
プロパティ名	*password_reset.sms.default_complexity*
構成タイプ	システムプロパティ (/sys_properties_list.do)
カテゴリ	認証
目的	パスワードのリセット時に必要な SMS コード検証サイズを制御します。
推奨値	**4** 以上の整数に設定します。デフォルト値は 4 です。
構成タイプ	ゼロより大きい整数値
セキュリティリスク	(低) プロパティが推奨値に設定されていない場合、弱い SMS 検証トークンが使用されます。これにより、アカウントの乗っ取りにつながる可能性があるトークン推測の可能性が高まります。
セキュリティリスク評価	3.8

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

パスワードリセット **SMS** の有効期限を最小限に抑える

SMS コードの有効期限が切れるまでの時間 (分) をコントロールします。

password_reset.sms.expiry プロパティは、SMS コードの有効期限が切れるまでの時間 (分) を表します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

詳細情報

属性	説明
構成名	*password_reset.sms.expiry*
構成タイプ	システムプロパティ (/sys_properties_list.do)
データタイプ	整数
推奨値	5
デフォルト値	5
カテゴリ	認証
セキュリティリスク	• 重大度スコア：5.6 • CVSS スコア：中 • セキュリティリスクの詳細：このプロパティが推奨値の **5** 以下に設定されていない場合、攻撃者が SMS コードを推測して使用し、パスワードをリセットする可能性が高くなります。
依存関係と前提条件	なし

パスワードリセットの **SMS** 一時停止期間の最大化

ユーザーが新しいパスワードリセットコードを要求するまでに待機しなければならない時間を分単位で管理します。

このプロパティが推奨値の **2** 分以上に設定されていない場合、悪意のあるユーザーが短い時間に多くのパスワードリセットコードを開始する可能性があります。これにより、攻撃者が SMS リセットコードを予測できる可能性が高くなります。

詳細情報

属性	説明
構成名	*password_reset.sms.pause_window*
構成タイプ	システムプロパティ (/sys_properties_list.do)
データタイプ	整数
推奨値	2
デフォルト値	2
カテゴリ	認証
セキュリティリスク	• 重大度スコア：4.8 • CVSS スコア：中 • セキュリティリスクの詳細:2 *password_reset.sms.pause_window* 以上の値に設定されていることを確認します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

属性	説明
依存関係と前提条件	なし

パスワードリセット検証の遅延時間の最大化

新しいパスワードリセット要求を送信する前にユーザーが待機する必要がある遅延をミリ秒単位で設定します。

攻撃者は、 Bot などの自動化ツールを使用して、ログイン資格情報の総当たり攻撃を試みる可能性があります。[パスワードリセット検証遅延 **(Reset Password Verification Delay)]** プロパティはこの防御に役立ちます。このプロパティ値は、ユーザーがパスワードリセット要求を行うまでに待機しなければならない遅延をミリ秒単位で表します。このプロパティが推奨値の **1000** 以上に設定されていない場合、ログインは総当たり攻撃に対してより脆弱になります。

詳細情報

属性	説明
構成名	*password_reset.verification.delay*
構成タイプ	システムプロパティ (/sys_properties_list.do)
データタイプ	文字列
推奨値	1000
デフォルト値	1000
カテゴリ	認証
セキュリティリスク	• 重大度スコア：5.9 • CVSS スコア：中 • セキュリティリスクの詳細：プロパティ値を 1000 未満に設定すると、ログインが総当たり攻撃に対してより脆弱になります。
依存関係と前提条件	なし
参照	ユーザーのパスワードの構成

SAML notBefore または notOnOrAfter 制約期間の最小化

このプロパティを構成し、SAML 要求と応答が有効であると見なされる猶予期間を追加します。

このプロパティは、SAML 要求と応答が有効であると見なされる猶予期間を追加します。このプロパティ値は、ID プロバイダー (IdP) クロックとサービスプロバイダー (SP) クロックの時間差を考慮して、 *NotBefore* および *NotOnOrAfter* の制約に追加する秒数を表します。これらの制約は、指定された期間内に行われない要求を拒否することによって、リプレイ攻撃を防止します。IdP クロックと SP クロックが大幅に異なる場合、ネットワーク遅延により SAML 要求が認可されないことがあります。

詳細情報

属性	説明
構成名	*glide.authenticate.sso.saml2.clockskew*

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

属性	説明
構成タイプ	システムプロパティ (/sys_properties_list.do)
データタイプ	文字列
推奨値	60
デフォルト値	180
カテゴリ	認証
セキュリティリスク	• 重大度スコア：7.5 • CVSS スコア：高 • セキュリティリスクの詳細：プロパティ値を 60 以上に設定すると、制約によるリプレイ攻撃の防御ができなくなる可能性があります。
依存関係と前提条件	なし

受信メールからのユーザーの作成を無効にする

glide.user.trusted_domain プロパティを使用して、受信メールからユーザーを作成する際に信頼できるドメインのカンマ区切りリストを指定します。

管理者は、受信メールからユーザーを自動的に作成するようにメール プロパティを設定できます。このプロパティを安全でない値に設定すると、インスタンスは受信メールから自動的にユーザーを作成します。作成された各ユーザーは、同じハードコードされたデフォルトのパスワードを持つため、ブルートフォースによる認証のバイパスが容易になります。

詳細情報

属性	説明
プロパティ名	*glide.user.trusted_domain*
構成タイプ	システムプロパティ (/sys_properties_list.do)
カテゴリ	認証
推奨値	信頼できるドメインのカンマ区切りリスト [例：servicenow.com (特定のドメイン名)]
セキュリティリスク評価	7.4
機能への影響度	(中) このプロパティが設定されると、インスタンスは信頼できるドメインからのメールのみ受け入れます。信頼できるリストにドメインを含めない場合、アカウントが自動的に作成されるため、ゲストユーザーに影響があります。
セキュリティリスク	(中) このプロパティが有効になっていない場合、攻撃者がなりすまし/スパムキャンペーンを使用して複数のメールを送信した結果、不要なゲストユーザーをさらに作成する可能性があります。
参照	受信メール設定

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

ロールベースのマルチファクター認証のアクティブ化

glide.authenticate.multifactor プロパティを使用して、特定のロールに割り当てられたすべてのユーザーにロールベースのマルチファクター認証 (MFA) を適用します。

マルチファクター認証は、ユーザーに割り当てられたロールに基づいて適用します。マルチファクターロールリストで「admin」、「security_admin」または「user_admin」のロールがユーザーに割り当てられている場合は、MFA が適用されます。

- 特定のロールに割り当てられたすべてのユーザーに対してロールベースのマルチファクター認証を適用するには、このプロパティを **true** に設定します。
- 特定のロールに割り当てられたすべてのユーザーに対してロールベースのマルチファクター認証を無効にするには、このプロパティを **false** に設定します。

詳細情報

属性	説明
プロパティ名	*glide.authenticate.multifactor*
構成タイプ	システムプロパティ (/sys_properties_list.do)
カテゴリ	認証
目的	特定のロールに割り当てられたすべてのユーザーに対してロールベースのマルチファクター認証を適用する。
タイプ	True/False
推奨値	*true*
セキュリティ依存関係	[マルチファクター基準] テーブルで、[ロールベースのマルチファクター認証 **(Role-based multi-factor authentication)**] をアクティブ化します。
セキュリティリスク評価	7.2
機能への影響度	(中) このプロパティを有効にすると、ユーザーのエクスペリエンスが向上します。これは、侵害された資格情報に対する保護およびセキュリティの追加レイヤーとして機能します。
セキュリティリスク	(中) このプロパティを有効にしないと、機密データに不正にアクセスされるリスクがあります。
参照	ロールベースのマルチファクター基準の設定

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

パスワードの最小長の設定

インスタンスのユーザーパスワードの最小長を設定します。

set.password.length プロパティは、パスワードに必要な最小長を定義し、現在のパスワードポリシーに対するコンプライアンスを評価するために使用されます。プロパティ値は整数で、最小推奨

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

値は **12** です。長さを短くすると、推奨される規制に対するコンプライアンス違反になる可能性があります。

詳細情報

属性	説明
構成名	*set.password.length*
構成タイプ	システムプロパティ (/sys_properties_list.do)
データタイプ	整数
推奨値	12
デフォルト値	12
カテゴリ	認証
セキュリティリスク	• 重大度スコア：5.9 • CVSS スコア：中 • セキュリティリスクの詳細：プロパティの値を 12 未満に設定すると、コンプライアンスの問題が発生し、攻撃者がパスワードの総当たり攻撃に成功するリスクが高まる可能性があります。
依存関係と前提条件	なし

Password Reset の **OTP** 期限を **12** 時間以下に設定

Password Reset メールのリンクの期限を制御します。

このプロパティにより、プロパティで指定された時間が経過すると、Password Reset メール内のリンクが期限切れになります。Password Reset トークンの有効期間は、通常のユーザーエクスペリエンスを妨げない程度に、できるだけ短くする必要があります。

詳細情報

属性	説明
構成名	*glide.pwd_reset.onetime.token.validity*
構成タイプ	システムプロパティ (/sys_properties_list.do)
データタイプ	整数
推奨値	12
デフォルト値	12
カテゴリ	認証

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

属性	説明
セキュリティリスク	• 重大度スコア：5.6 • CVSS スコア：中 • セキュリティリスクの詳細：Password Reset トークンの有効期間が長いと、攻撃者がアカウントの乗っ取りを実行する可能性が高くなります。
依存関係と前提条件	なし

1 回限りの帯域外検証ツールの有効期間の最小化

帯域外検証ツールの期限を管理します。

帯域外検証ツールは、1 回限りのコードでの代替配信方法です。たとえば、マルチファクタートークンのリセットなどです。マルチファクター認証 (MFA) プラグインで管理者がこのメソッドを有効にしている場合、ワンタイムコードがメールで配信されます。1 回限りの帯域外検証ツールを 10 分後に期限切れになるように設定して、有効期間を制限します。有効期間が長いほど、フィッシング、ソーシャルエンジニアリング、ショルダーサーフィン攻撃などの不正な手段によってコードが侵害される可能性が高くなります。

詳細情報

属性	説明
構成名	*glide.multifactor.onetime.code.validity*
構成タイプ	システムプロパティ (/sys_properties_list.do)
データタイプ	整数
推奨値	10
デフォルト値	10
カテゴリ	認証
セキュリティリスク	• 重大度スコア：3.9 • CVSS スコア：低 • セキュリティリスクの詳細：1 回限りの帯域外検証ツールを 10 分後に期限切れになるように設定します。時間が長くなると、攻撃者によってコードが侵害されるリスクが高まります。
依存関係と前提条件	マルチファクター認証 (MFA)
参照	MFA プラグインのアクティブ化

デバイスの暗号化とパスコードの要件の適用

このプロパティは *glide.sg.device_encryption_enabled* 、連邦情報処理標準 (FIPS 140-2) 暗号化を適用します。モバイルデバイスの暗号化とパスコードにより、デバイスが物理的に取得された場合でも、権限のないユーザーがデバイスのコンテンツにアクセスできなくなります。

*glide.sg.device_encryption_enabled*が true に設定されている場合、ServiceNow モバイルアプリは、デバイスの暗号化とデバイスのパスコードが有効になっていることを確認します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

詳細情報

属性	説明
構成名	*glide.sg.device_encryption_enabled*
構成タイプ	システムプロパティ (/sys_properties_list.do)
データタイプ	ブーリアン
推奨値	true
デフォルト値	false
カテゴリ	認証
セキュリティリスク	• 重大度スコア：4.2 • CVSS スコア：中 • セキュリティリスクの詳細: 暗号化またはパスコードが有効になっていない場合、ユーザーはモバイルでインスタンスにログインできません
依存関係と前提条件	なし
機能への影響	このプロパティが true に設定されている場合、モバイルアプリはデバイスの暗号化が有効になっているかどうかを確認します。暗号化が有効になっていない場合、ユーザーはモバイルで現在のインスタンスにログインできません。

XML 出力依頼に権限を要求する

glide.basicauth.required.xml プロパティを使用して、受信 XML 要求で基本認証を要求するかどうかを指定します。

詳細情報

警告:
これはセーフハーバープロパティです。つまり、いったん変更したら変えることはできません。元に戻すことはできません。

属性	説明
プロパティ名	*glide.basicauth.required.xml*
構成タイプ	システムプロパティ (/sys_properties_list.do)
カテゴリ	API と Web サービス
目的	XML 要求に対して基本認証を適用すること
セキュリティリスク評価	7.5
推奨値	true
機能への影響度	(低) この修正では、基本認証とシステムレベルのアクセス制御の形で、認証方法の組み合わせが適用されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

属性	説明
	• インスタンス上で XML データの形式でテーブル/ページからデータを取得する際に、この認証を実行します。 • 現在このデータにアクセスしているゲストユーザーを制限します。必要であれば、このコンテンツへのアクセスを必要とするユーザーのために、必要なアクセス制御権限を持つ新しいアカウントを作成する場合があります。 詳細については、「XML パーサーステップ」を参照してください。
セキュリティリスク	(高)受信 XML 要求で適切な承認が構成されていない場合、無許可のユーザーがターゲットインスタンスの機密コンテンツや機密データにアクセスする可能性があります。が `glide.basicauth.required.xml` sys_properties テーブルに存在し、true に設定されていることを確認します。
参照	認証

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

Customer Service アプリケーションでのゲストウォークアップエクスペリエンスに CAPTCHA を必須にする

ゲスト Walk-up Experience 用のキャプチャは、ユーザーにキャプチャ検証の完了を要求することで、認証されていないゲストユーザーが予約を作成するのを防ぎます。

詳細情報

属性	説明
構成名	`sn_guest_walkup_cs.captcha.enabled`
構成タイプ	システムプロパティ (/sys_properties_list.do)
データタイプ	ブーリアン
推奨値	true
デフォルト値	true
カテゴリ	認証
セキュリティリスク	• 重大度スコア：3.7 • CVSS スコア：低 • セキュリティリスクの詳細：キャプチャが有効になっていない場合、スパム予約が自動的に作成されてシステムが過負荷状態になったり、利用可能なすべての予約スポットがいっぱいになったりするサービス拒否 (DoS) 攻撃が発生する可能性があります。
依存関係と前提条件	なし

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

属性	説明
機能への影響	このプロパティは、「CSM ゲストウォークアップチェックイン」ウィジェットのキャプチャを有効または無効にします。デフォルトでは true に設定されています。

登録と検証の **SMS** コード通知を有効にする

password_reset.sms.use_notify プロパティは、パスワードリセット用の SMS コード通知の使用を制御します。

password_reset.sms.use_notify プロパティが推奨値の **true** に設定されている場合、SMS 検証とメールよりも安全な新しいデバイス登録を使用して、パスワードをリセットするようにユーザーに通知されます。

詳細情報

属性	説明
構成名	*password_reset.sms.use_notify*
構成タイプ	システムプロパティ (/sys_properties_list.do)
データタイプ	ブーリアン
推奨値	true
デフォルト値	true
カテゴリ	認証
セキュリティリスク	• 重大度スコア：3.7 • CVSS スコア：低 • セキュリティリスクの詳細：このプロパティを **false** に設定すると、SMS よりも安全性が低いメールがパスワード回復のデフォルト方法となります。
依存関係と前提条件	なし

ビジネスロジック

このカテゴリでは、一般的な安全原則に基づいて各アプリケーションに固有のロジックとフローを確認します。具体的には、ビジネスロジックフローの意図された順序がバイパスできないこと、自動攻撃を検出して防止するための制限が存在すること、およびなりすまし、改ざん、情報開示、および権限昇格攻撃に対する保護が存在することを確認します。

Now Platform 内の機密エンティティへの不正アクセスを制限するために管理者が設定できるセキュリティコントロールは、次のとおりです。

1 日あたりのユーザー **1** 人あたりのコメント最大数の制限

1 日あたりの QA コメントの数を制限するように *sn_kb_social_qa.max_comments_per_user_daily* プロパティを設定します。

このプロパティが、推奨値の **500** 以下に設定されていない場合、1 日あたりの QA コメント数に制限がなくなり、これはリソースの枯渇につながる可能性があります。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

詳細情報

属性	説明
構成名	*sn_kb_social_qa.max_comments_per_user_daily*
構成タイプ	システムプロパティ (/sys_properties_list.do)
データタイプ	整数
推奨値	500
デフォルト値	500
カテゴリ	ビジネスロジック
セキュリティリスク	• 重大度スコア：3.7 • CVSS スコア：低 • セキュリティリスクの詳細：このプロパティが、推奨値の 500 以下に設定されていない場合、1 日あたりの QA コメント数に制限がなくなり、リソースの枯渇につながる可能性があります。
依存関係と前提条件	なし

1 日あたりのユーザー 1 人あたりのサブスクリプション最大数の制限

この *sn_kb_social_qa.max_subscriptions_per_user_daily* プロパティを構成して、ユーザーが 1 日に登録できるサブスクリプションの最大数を制限します。

このプロパティが推奨値の **500** 以下に設定されていない場合、ユーザーが 1 日に登録できる Q&A 質問の最大数に制限はありません。この制限がないとリソースが枯渇し、ご自分のインスタンスの可用性に影響を与える可能性があります。

詳細情報

属性	説明
構成名	*sn_kb_social_qa.max_subscriptions_per_user_daily*
構成タイプ	システムプロパティ (/sys_properties_list.do)
データタイプ	整数
推奨値	500
デフォルト値	500
カテゴリ	ビジネスロジック
セキュリティリスク	• 重大度スコア：3.7 • CVSS スコア：低 • セキュリティリスクの詳細：リソースの枯渇を防ぐには、このプロパティの値を 500 以下に設定します。
依存関係と前提条件	なし

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

SMTP 受信者の数量を最小化する

glide.email.smtp.max_recipients は、1 件のメール通知でインスタンスが **To:** の行に一覧表示できる受信者の最大数を指定します。

glide.email.smtp.max_recipients を **100** 以下の推奨値に設定します。この制限を超える通知については、代わりに受信者リストの一部に宛てた複製メール通知を作成します。各メール通知には同じ最大数の受信者が指定されています。

詳細情報

属性	説明
プロパティ名	*glide.email.smtp.max_recipients*
構成タイプ	システムプロパティ (/sys_properties_list.do)
カテゴリ	ビジネスロジック
目的	このプロパティがデフォルト値の 100 を超える安全でない値に設定されている場合、インスタンスでサービス拒否が発生する可能性があります。
推奨値	100 以下の整数に設定します。デフォルト値は 100 です。
構成タイプ	整数
機能への影響度	
セキュリティリスク	(中) この制限を超える通知については、代わりに受信者リストの一部に宛てた複製メール通知を作成します。
セキュリティリスク評価	4.9

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

リモートホストの検証

攻撃者がネットワークで内部ポートスキャンを使用するのを防ぐには、このプロパティを true に設定します。

glide.update_set.remote.check_host プロパティが 推奨値の **true** に設定されていない場合、Team Development リモートインスタンステスト機能では、悪意のある攻撃者がネットワークの脆弱性を発見するために使用できる方法である内部ポートスキャンが許可されます。その後、特定のホストで開いているすべてのポートを列挙し、場合によっては応答データを抽出して、情報漏えいや不正なデータアクセスにつながる可能性があります。

⚠ 警告:
これはセーフハーバープロパティです。つまり、いったん変更したら変えることはできません。元に戻すことはできません。

詳細情報

属性	説明
構成名	*glide.update_set.remote.check_host*
構成タイプ	システムプロパティ (/sys_properties_list.do)

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

属性	説明
データタイプ	ブーリアン
推奨値	true
デフォルト値	true
カテゴリ	ビジネスロジック
セキュリティリスク	• 重大度スコア：6.3 • CVSS スコア：中 • セキュリティリスクの詳細：このプロパティを推奨値の **true** に設定しないと、攻撃者が内部ポートスキャンを使用して許可されていないデータにアクセスできる可能性があります。
依存関係と前提条件	なし
参照	https://support.servicenow.com/kb?id=kb_article_view&sysparm_article=KB0755132 Define a remote instance

通信

このコントロールにより、強力なアルゴリズムと暗号を使用して適切な暗号化が行われます。これには、クライアント接続での推奨されるバージョンの TLS の使用、強力な暗号スイートの使用、信頼できる署名付き証明書の使用の確認、およびコンポーネント間での接続の暗号化と接続エラーのログ記録の確認が含まれます。

証明書の信頼を強制する

デフォルトでは、*com.glide.communications.trustmanager_trust_all* プロパティは **false** に設定されています。Now Platform は、JVM 証明書ストアに対して検証できる証明書のみを信頼します。自己署名証明書およびエンタープライズ署名証明書は信頼されません。

注:
これらのプロパティの値は 安全なオーバーライド であるため、一度変更すると変えることができなくなります (元に戻すことはできません)。セキュリティ上の理由から、このプロパティ値は変更しないでください。さらに質問がある場合は、カスタマーサービス & サポートにお問い合わせください。

詳細情報

属性	説明
プロパティ名	*com.glide.communications.trustmanager_trust_all*
構成タイプ	システムプロパティ (/sys_properties_list.do)
カテゴリ	通信
目的	送信要求の証明書の検証を適用すること
推奨値	false

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

属性	説明
セキュリティリスク評価	6.6
機能への影響度	(中) この修正では、証明書の CA (認証局) フィールドに厳格な検証が適用されます。信頼できるエンティティ (CA) が証明書を発行した場合、インスタンスはそれを受け入れてその後使用します。
セキュリティリスク	(中) 機密性と完全性の理由から、アプリケーションはどのトランザクション操作に対しても、証明書を使用する前に証明書の CA を検証する必要があります。
参照	証明書 HTTP クライアントホスト名の検証

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

送信 SSLv2/SSLv3 接続の無効化

glide.outbound.sslv3.disabled プロパティを設定して、REST 要求や SOAP 要求などの送信接続を行うときに、MID Server が強制的に TLS を使用するようにします。通常は、インスタンスからの送信接続で SSL の代わりに TLS が使用されます。

詳細情報

属性	説明
プロパティ名	*glide.outbound.sslv3.disabled*
構成タイプ	システムプロパティ (/sys_properties_list.do)
カテゴリ	通信
目的	ServiceNow インスタンスからのすべての送信接続で TLS の使用を強制すること
推奨値	true
セキュリティリスク評価	6.5
機能への影響度	(中) この修正では、HTTPS で通信するときに TLS プロトコルバージョンの使用が強制されます。インスタンスの顧客/ユーザーが TLS 通信をサポートしていないデバイスを使用している場合は、機能停止する可能性があります。
セキュリティリスク	(中) SSL の従来のバージョンは、HTTP セキュアシェル実装に使用した場合、BEAST や SSL ハートブリードなどのクライアント側の攻撃のためにセキュアでないことが確認されています。

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

アクティブな SAML 構成にデモ証明書を使用しない

本番 SAML 構成でデモ証明書を使用するかどうかを制御します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ServiceNow によって提供されるデモ証明書は、既知のパスフレーズを持つすべてのインスタンスに共通するものであるため、本番 SAML 構成では使用しないでください。証明書キーストアを使用する SAML プロパティのいずれかがアクティブ (*require_signed_authnrequest*、*require_signed_logoutrequest*、または *encrypt_assertion*) の場合は、デモデータを使用しないでください。デモデータはすべてのインスタンスで共有されるため、共有証明書で署名された要求の整合性は保証されません。したがって、IDP によって暗号化されたメッセージが、インターセプトされた場合、攻撃者によって復号化される可能性があります。

詳細情報

属性	説明
構成名	*glide.authenticate.sso.saml2.keystore*
構成タイプ	システムプロパティ (/sys_properties_list.do)
データタイプ	文字列
推奨値	カスタムキーストアの sys_id
デフォルト値	空白文字列
カテゴリ	通信
セキュリティリスク	• 重大度スコア：3.9 • CVSS スコア：低
依存関係と前提条件	なし

ネットワークエラーの **OCSP** チェックを強制する

攻撃者がオンライン証明書ステータスプロトコル (OCSP) チェックをバイパスしないように *com.glide.communications.httpclient.ocsp_allow_network_error* プロパティを設定する方法について説明します。

*com.glide.communications.httpclient.ocsp_allow_network_error*が推奨値の false に設定されていない場合、オンライン証明書状態プロトコル (OCSP) チェックでネットワーク エラー (タイムアウトや失効情報の取得に関する問題など) が発生した場合、OCSP セキュリティ チェックはバイパスされ、成功したと見なされます。これにより、失効した証明書を持つ攻撃者が、Web の基盤となる公開キー基盤 (PKI) およびデジタル証明書の信頼を破る可能性があります。失効した証明書の使用は、サーバーが同期していない限り、多くの場合、悪意のあるアクティビティの指標となります。

詳細情報

属性	説明
構成名	*com.glide.communications.httpclient.ocsp_allow_network_er*
構成タイプ	システムプロパティ (/sys_properties_list.do)
データタイプ	ブーリアン
推奨値	false
デフォルト値	true

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

属性	説明
カテゴリ	通信
セキュリティリスク	• 重大度スコア：5.9 • CVSS スコア：中 • セキュリティリスクの詳細：このプロパティを false に設定しないと、攻撃者が OCSP セキュリティチェックをバイパスできる可能性があります。
依存関係と前提条件	なし
機能への影響	このプロパティは、接続エラーまたはタイムアウト エラーが発生した場合に、機関情報アクセス (AIA) オンライン証明書状態プロトコル (OCSP) URI に対する要求が合格または失敗の結果になるかどうかを決定します。false に設定すると、提示されたサーバー証明書の失効状態を検証できず、そのエンドポイントとの通信エラーが発生します。プロパティがデフォルト値の true に設定されているときにネットワークエラーが発生した場合、証明書は失効の観点から有効として扱われます。

証明書チェーンとホスト名の確認

com.glide.communications.httpclient.verify_hostname プロパティを構成して、証明書検証プロセスが確実に実行されるようにすることで、中間者攻撃を防ぎます。

が **true** に設定されていない場合*com.glide.communications.httpclient.verify_hostname*、2 者間の通信が傍受される中間者攻撃が可能になる可能性があります。このプロパティを false に設定すると、証明書の検証プロセスが無効になります。このセキュリティ上の脅威を修復するには、*com.glide.communications.httpclient.verify_hostname* を **true** に設定し、害を及ぼす可能性のあるホスト名に http クライアントが接続しないようにします。

詳細情報

属性	説明
構成名	*com.glide.communications.httpclient.verify_hostname*
構成タイプ	システムプロパティ (/sys_properties_list.do)
データタイプ	ブーリアン
推奨値	true
デフォルト値	false
カテゴリ	通信
セキュリティリスク	• 重大度スコア：高 • CVSS スコア：7.4

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

属性	説明
	• セキュリティリスクの詳細:推奨値の true に設定 *com.glide.communications.httpclient.verify_hostname* しないと、インスタンスが中間者攻撃に対して脆弱になる可能性があります。
依存関係と前提条件	なし
機能への影響	リモート SSL (Secure Socket Layer) ホストによって提示されたホスト名と証明書チェーンを検証します。このプロパティを true に設定し、中間者 (MITM) 攻撃から保護します。 **注:** このプロパティは *com.glide.communications.trustmanager_trust_all* プロパティを上書きします。

証明書の失効の確認

com.glide.communications.httpclient.verify_revoked_certificate プロパティは 、トランスポートレイヤーセキュリティ (TLS) ハンドシェイク中に証明書の失効をチェックし、セキュリティチェックがバイパスされていないことを確認します。

*com.glide.communications.httpclient.verify_revoked_certificate*が推奨値の **true** に設定されていない場合、TLS ハンドシェイク中に証明書の失効はチェックされません。TLS は、インターネット経由で送信されるデータを暗号化して、悪意のある人物がパスワードやクレジットカード番号などの機密情報を表示できないようにします。TLS ハンドシェイクをバイパスすると、失効した証明書を持つ攻撃者が有効な証明書の提供を怠り、公開キー基盤 (PKI) とデジタル証明書の信頼を破る可能性があるため、セキュリティ上のリスクがあります。

詳細情報

属性	説明
構成名	*com.glide.communications.httpclient.verify_revoked_certif*
構成タイプ	システムプロパティ (/sys_properties_list.do)
データタイプ	ブーリアン
推奨値	true
デフォルト値	true
カテゴリ	通信
セキュリティリスク	• 重大度スコア：6.5 • CVSS スコア：中 • セキュリティリスクの詳細：*com.glide.communications.httpclient.verify_revoked_c* を推奨値の true に設定しないと、TLS ハンドシェイク中に証明書の失効がチェックされません。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

属性	説明
依存関係と前提条件	なし
機能への影響	トランスポートレイヤーセキュリティ (TLS) セッションが本物のエンドポイントで開始されるようにするには、このプロパティを true に設定する必要があります。このプロパティが false に設定されている場合、証明書はチェックされず、インスタンスのセキュリティが侵害される可能性があります。

設定

構成カテゴリは、アプリケーションにセキュアなビルド環境と強化されたサードパーティのライブラリーコンポーネントがあることを確認します。具体的には、ビルドと展開のパイプラインが繰り返し可能で自動テストが含まれていることを確認し、既知のセキュリティの問題が展開されないようにします。これには、依存関係を最新の状態に保ち、既知の脆弱性を排除することが含まれます。

HTTP ヘッダー値のキャッシュコントロール

glide.http.cache_control プロパティを使用して、ページの静的コンテンツデータを要求するときに Now Platform から送信される HTTP 応答ヘッダーのデフォルトのキャッシュ制御値を設定します。静的コンテンツには、たとえばページで内部からレンダリングされる画像、CSS、および JavaScript などがあります。

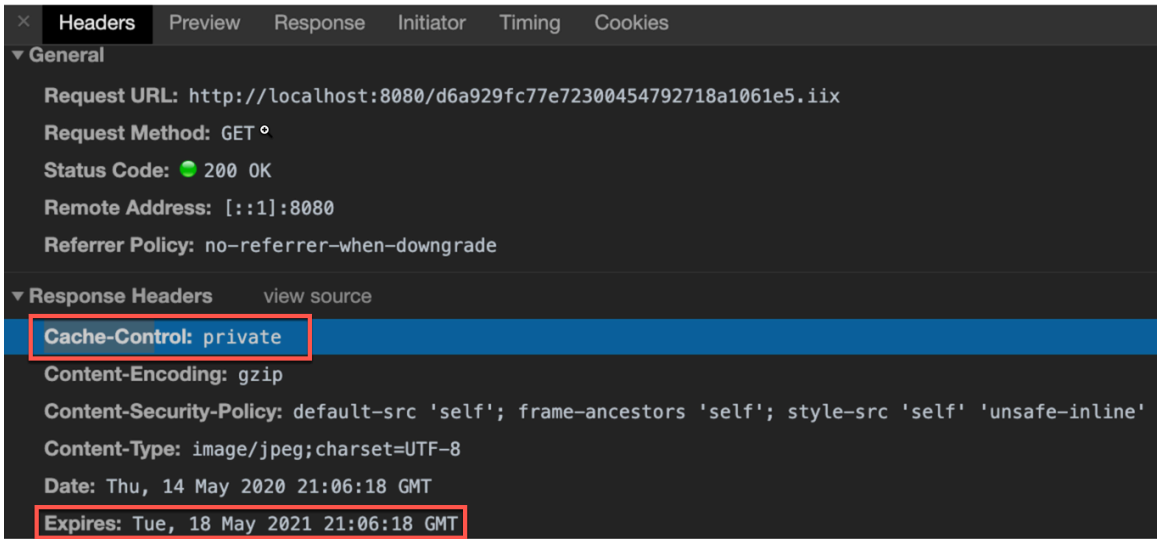
glide.http.cache_control プロパティは、HTTP 応答ヘッダーのデフォルトのキャッシュ制御値を **private** または **public** に設定します。デフォルトは **private** です。

値	説明
private	静的コンテンツはブラウザー (クライアント) レベルでキャッシュできますが、プロキシサーバーレベルではキャッシュできません。
公開	静的コンテンツはブラウザー (クライアント) レベルでキャッシュでき、またプロキシサーバーレベルでもキャッシュできます。

HTTP 応答ヘッダーの Expires の値は、静的コンテンツの有効期限を制御します。デフォルト値は 369 日です。デフォルト値を手動で上書きするには、*glide.http.expire.days* プロパティを使用します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



注:
glide.http.cache プロパティを使用して、HTTP 応答ヘッダーの Cache-Control と Expires の値の設定を有効にするか無効にするかを指定できます。デフォルトは **true** で、以下の項目を設定できます。

- *glide.http.cache_control* プロパティを使用してデフォルトの Cache-Control (キャッシュ制御) 値を設定可能
- *glide.http.expire.days* プロパティを使用してデフォルトの Expires (有効期限) 値を設定可能

詳細情報

属性	説明
プロパティ名	*glide.http.cache_control*
構成タイプ	システムプロパティ (/sys_properties_list.do)
カテゴリ	設定
目的	静的コンテンツのキャッシュ制御 HTTP 応答ヘッダー値を設定すること
推奨値	private
セキュリティリスク評価	4.3
機能への影響度	(中) HTTP 応答ヘッダーのデフォルトのキャッシュ制御値を設定します。
セキュリティリスク	(高) このプロパティを **public** に設定すると、CDN/プロキシを備えたインスタンスが静的コンテンツをキャッシュし、認証なしでレンダリングする場合があります。 • **private** は、CDN/プロキシセットアップを使用するインスタンスに適した設定です。 • インスタンスに CDN/プロキシが設定されていない場合は、どちらの値でもかまいません。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

チャットサーバーのデバッグの無効化

このプロパティを設定して、インスタンスのシステムログを有効または無効にします。

glide.cs.debug プロパティを使用して、インスタンスでのシステムログの処理方法を管理します。プロパティが推奨値の **false** に設定されている場合、システムログは有効になりません。**true** に設定されている場合、システムログが有効になります。トラブルシューティングが必要な場合にのみこのプロパティを **true** に設定し、完了したら無効にします。システムログを有効にすると、多くのメッセージが生成され、システムログが過負荷になる可能性があります。また、ログメッセージによって機密情報が誤って公開される可能性があります。

詳細情報

属性	説明
構成名	*glide.cs.debug*
構成タイプ	システムプロパティ (/sys_properties_list.do)
データタイプ	ブーリアン
推奨値	false
デフォルト値	false
カテゴリ	設定
セキュリティリスク	• 重大度スコア：2.3 • CVSS スコア：低 • セキュリティリスクの詳細：システムログを有効にすると、多くのメッセージが生成され、ログメッセージでシステムが過負荷になり、ログメッセージから機密情報が誤って公開される可能性があります。
依存関係と前提条件	なし

ロックされたフォーム要素のデバッグを無効にする

glide.security.explain.write.locks の説明です。

ロックされたフォーム要素の説明を表示しないようにするには、*glide.security.explain.write.locks* を推奨値の **false** に設定します。ロックされたフォーム要素の説明を表示するには、値を **true** に設定します。

詳細情報

属性	説明
プロパティ名	*glide.security.explain.write.locks*
構成タイプ	システムプロパティ (/sys_properties_list.do)
カテゴリ	設定

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

属性	説明
目的	他のプロパティに依存しない SecurityDebugger の表示動作を制限します。
推奨値	False
構成タイプ	ブーリアン
セキュリティリスク	(低) ロックされたフォーム要素に説明が表示されないようにします。これにより、セキュリティデバッガーによって提供される情報が少なくなるため、アプリケーションの安全性がわずかに向上します。
セキュリティリスク評価	3.5

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

マルチッソデバッグを無効にする

glide.authenticate.multisso.debug プロパティは、マルチ SSO のデバッグログ記録を制御します。

詳細情報

属性	説明
プロパティ名	*glide.authenticate.multisso.debug*
構成タイプ	システムプロパティ (/sys_properties_list.do)
カテゴリ	設定
目的	マルチ SSO デバッグを無効にします。
推奨値	False
構成タイプ	ブーリアン
セキュリティリスク	(高) プロパティを推奨値の「False」に設定します。そのようにしないと、MultiSSO デバッグが有効になり、意図しない機密情報の漏洩が発生する可能性があります。
セキュリティリスク評価	4.0
参照	複数プロバイダー SSO のプロパティ、テーブル、およびスクリプト

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

ターゲットクローン作成の禁止

インスタンスがクローンターゲットとして使用されないように *glide.db.clone.allow_clone_target* プロパティを設定します。

glide.db.clone.allow_clone_target が推奨値の false に設定されていない場合 、インスタンスはクローンターゲットとして、またはクローン作成に使用されるインスタンス URL と資格情報を指定するレコードとして使用できます。システムクローンは、データベース内のすべてのものを、あるインスタンスから別のインスタンスにコピーします。クローン作成プロセスでインスタンスデータベースが上書きされて、データが失われたり、データの完全性が失われたりする可能性があるた

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

め、これはセキュリティ上のリスクです。修正として、*glide.db.clone.allow_clone_target* が false に設定されていることを確認します。

詳細情報

属性	説明
構成名	*glide.db.clone.allow_clone_target*
構成タイプ	システムプロパティ (/sys_properties_list.do)
データタイプ	ブーリアン
推奨値	false
デフォルト値	true
カテゴリ	設定
セキュリティリスク	• 重大度スコア：5.9 • CVSS スコア：中 • セキュリティリスクの詳細：このプロパティを推奨値の false に設定しないと、インスタンスをクローンターゲットとして使用できるようになります。クローン作成プロセスでインスタンスデータベースが上書きされる可能性があるため、これはセキュリティ上のリスクです。
依存関係と前提条件	なし
参照	• System clone • Clone Target Registration and Authentication
機能への影響度	このプロパティは、本番インスタンスがクローンされないようにする追加の安全策を提供します。デフォルト値は、本番インスタンスの場合は false、dev や qa などの準本番インスタンスの場合は true です。インスタンスをクローンターゲットとして使用できるようにするには、このプロパティを true に設定します。

SOAP フォールトスタックトレースディスプレイの無効化

スタックトレースをインスタンスに表示する方法を管理します。

glide.soapfault.display_stack_trace プロパティを使用して、インスタンスのスタックトレースを管理します。このプロパティが **false** に設定されている場合、機密情報が漏洩する可能性があります。これが **true** に設定されている場合、スタックトレースは表示されません。

詳細情報

属性	説明
構成名	*glide.soapfault.display_stack_trace*
構成タイプ	システムプロパティ (/sys_properties_list.do)

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

属性	説明
データタイプ	ブーリアン
推奨値	false
デフォルト値	false
カテゴリ	設定
セキュリティリスク	• 重大度スコア：7.3 • CVSS スコア (CVSS score)：中 • セキュリティリスクの詳細 (Security risk details)：このプロパティを **false** に設定すると、スタックトレースから機密情報が公開される可能性があります。
依存関係と前提条件	なし

パフォーマンス監視アクセスの制限

glide.security.diag_txns_acl プロパティを使用して、認証されていない接続からの stats.do、threads.do、thread_pool_stats および replication.do アクセスを制御します。

このプロパティを **true**に設定すると、*glide.security.diag_txns_acl* プロパティは管理者アカウントによる以下へのアクセスのみを許可します。

- https://<instancename>.servicenow.com/stats.do
- https://<instancename>.servicenow.com/threads.do
- https://<instancename>.servicenow.com/replication.do
- https://<instancename>.servicenow.com/thread_pool_stats.do

この設定を有効にしない場合、認証されていない接続からこれらのリソースに引き続きアクセスできます。

詳細情報

属性	説明
プロパティ名	*glide.security.diag_txns_acl*
構成タイプ	システムプロパティ (/sys_properties_list.do)
カテゴリ	設定
目的	設定ページへのアクセスを管理者アカウントのみに制限すること
推奨値	true
セキュリティリスク評価	5.3
機能への影響度	(低) この修正では、ログ記録とトラブルシューティングの目的で、管理者アカウントのみがアプリケーションの機密データにアクセスできるようにします。
セキュリティリスク	(中) サーバーの詳細、スレッド、サーバーで実行されるプロセスなどの機密データは、適切な権限のないエンドユーザーが表示したりアクセスしたりすることはできません。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

マルチ SSO プラグインの更新バージョンを有効にする

セキュリティの脆弱性を軽減するには、Multi SSO プラグインの v2 を使用していて、true に設定されていることを確認します。

インスタンスで Multi SSO プラグインが有効になっている場合、バージョンは v2 で、値を **true** に設定する必要があります。SAML 1.1 および SAML 2.0 を含む MultiSSOv2 より前のバージョンは、既知の共通脆弱性識別子 (CVE) がある OpenSAML ライブラリバージョンを使用しているため、セキュリティ標準に準拠していません。既知の CVE が古い OpenSAML ライブラリのセキュリティ脅威だった場合、悪意のある攻撃者がメッセージを偽造し、XML 署名ラッピング攻撃により認証をバイパスし、エンティティの代理操作、または中間者攻撃者によりインスタンスへの不正アクセスを得る可能性があります。

詳細情報

属性	説明
構成名	*glide.authenticate.multissov2_feature.enabled*
構成タイプ	システムプロパティ (/sys_properties_list.do)
データタイプ	ブーリアン
推奨値	true
デフォルト値	true
カテゴリ	設定
セキュリティリスク	• 重大度スコア：5 • CVSS スコア：中 • セキュリティリスクの詳細：プロパティ値を **false** に設定するということは、セキュリティの脆弱性がある OpenSAML ライブラリを使用する以前のバージョンの MultiSSOv2 を使用していることを意味します。これにより、攻撃者がメッセージを偽造できる可能性があります。
依存関係と前提条件	なし
参照	https://support.servicenow.com/kb?id=kb_article_view&sysparm_article=KB0756504

安全なリファラーポリシーの適用

*com.glide.security.referrerpolicy*このプロパティを使用して、データ漏洩を防ぐために、参照元ポリシーの HTTP ヘッダーが各ServiceNow ページに適切なレベルのデータを送信するようにします。

プロパティを *com.glide.security.referrerpolicy* default に設定すると、Referrer-Policy HTTP ヘッダーは、特に要求ページに合わせて Now Platform 調整された、適切なレベルの送信された情報で管理されます。これにより、パスやクエリ文字列など、完全な URL の他の部分からアクセスできる不正なデータ漏洩を防ぐことができます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

詳細情報

属性	説明
構成名	*com.glide.security.referrerpolicy*
構成タイプ	システムプロパティ (/sys_properties_list.do)
データタイプ	文字列
推奨値	デフォルト
デフォルト値	default
カテゴリ	設定
セキュリティリスク	• 重大度スコア：7.3 • CVSS スコア：中 • セキュリティリスクの詳細：不正なデータの漏洩を防ぐために、*com.glide.security.referrerpolicy* プロパティが default に設定されていることを確認してください。
依存関係と前提条件	なし
参照	Referrer-Policy
機能への影響	このプロパティは、ページから要求が送信されたときに、参照元ヘッダーを介して送信される情報の量を制御します。 • デフォルト:インスタンスが参照元ヘッダーを処理します • same-origin:インスタンス/同じドメイン内で完全な参照元 URL を送信し、外部の作成元には送信しません • origin: オリジンのみをリファラーとして、オリジンの内側と外側に送信します • origin-when-cross-origin:インスタンス/同一ドメイン内で完全な参照元URLを送信し、オリジン外のオリジンのみを送信します

x-frame-options: SAMEORIGIN セキュリティヘッダーの実装

glide.set_x_frame_options プロパティを使用して、すべての UI ページの SAMEORIGIN に対して X-Frame-Options 応答ヘッダーを設定します。

X-Frame-Options HTTP 応答ヘッダーは、<frame> または <iframe> 内のページをブラウザーでレンダリングできるかどうかを示すために使用されます。サイトでは、この機能を使用して、そのコンテンツがその他のサイトに組み込まれることがないようにすることで、クリックジャッキング攻撃を回避することができます。攻撃者は、お客様のページを自分のページに埋め込み、ページ要素が悪意を持って実行されるようにする可能性があります。エンドユーザーは、ページが自分のページに似ているため、そのページが正当だと考えるかもしれません。エンドユーザーが通常どおりに要素をクリックするだけで、悪意のあるスクリプトまたは要素が実行される可能性があります。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

詳細情報

属性	説明
プロパティ名	*glide.set_x_frame_options*
構成タイプ	システムプロパティ (/sys_properties_list.do)
カテゴリ	設定
目的	クリックジャッキング攻撃の軽減
推奨値	true
セキュリティリスク評価	7.1
機能への影響度	(低) この修正では、サードパーティアプリケーション内で Now Platform アプリケーションを iframe の形式でレンダリングする際に制限が適用されます。このような統合がある場合、アプリケーションはカスタマイズされたサードパーティアプリにはレンダリングされません。
セキュリティリスク	(中) 同一生成元ポリシーを使用すると、ドメインが別のドメインからスクリプトやリソースを取得できないようにすることができます。最新のブラウザーはすべてこの機能をサポートしています。 このポリシーは、プロトコル、ポート、およびホストに基づいて接続を検証します。CORS (クロスオリジン要求) は同一生成元ポリシーを修正したものであり、ヘッダー値の一部として明示的に指定されている場合に、別のドメインのリソース/スクリプトにアクセスできるようにします。 • この場合、X-Frame-Options ヘッダーは、Now Platform アプリケーションをサードパーティの Web サイトでレンダリングできるかどうかを制御します。 • プロパティ値を **SAMEORIGIN** に設定するとレンダリングが行われないため、機密情報が公開されることが減少します。
参照	利用可能なシステムプロパティ iFrame の設定

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

Service Catalog アイテム追加ページにアクセスするための書き込みアクセス権

glide.sc.request.add_item_write_access プロパティを使用して、カタログアイテムに対して不正な操作が実行されないようにします。

詳細情報

属性	説明
構成名	*glide.sc.request.add_item_write_access*

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

属性	説明
構成タイプ	システムプロパティ (/sys_properties_list.do)
データタイプ	ブーリアン
推奨値	true
デフォルト値	false
カテゴリ	設定
セキュリティリスク	• 重大度スコア：7.3 • CVSS スコア：中 • セキュリティリスクの詳細:プロパティが *glide.sc.request.add_item_write_access* false に設定されている場合、ログインしているユーザーは誰でも [カタログアイテムの追加] UI ページにアクセスできます。これにより、カタログアイテムに対して不正な操作が実行される可能性があります。このセキュリティリスクを修復するには、このプロパティを true に設定します。
依存関係と前提条件	なし
機能への影響	プロパティが true の場合、ユーザーは UI ページのコンテキストでレコードへの書き込みアクセス権を持っている必要があります。

Xframe オプションを設定してサードパーティの Web サイトが埋め込まれないようにする

Web アプリケーションのコンテンツがサードパーティのサイトに埋め込まれないようにするには、このプロパティを構成します。

このプロパティが推奨値の **DENY** または **SAMEORIGIN** に設定されていない場合、Web アプリケーションのコンテンツは **ALLOW-FROM** URI を使用してサードパーティサイトに埋め込まれる可能性があります。信頼できないサードパーティサイトを許可すると、クリックジャッキングなどの攻撃が可能になる可能性があります。

詳細情報

属性	説明
構成名	*com.glide.cs.embed.xframe_options*
構成タイプ	システムプロパティ (/sys_properties_list.do)
データタイプ	文字列
推奨値	sameorigin
デフォルト値	sameorigin
カテゴリ	設定
セキュリティリスク	• 重大度スコア：3.1 • CVSS スコア：低

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

属性	説明
	• セキュリティリスクの詳細：このプロパティを推奨値に設定しないと、Web アプリケーションのコンテンツがサードパーティのサイトに埋め込まれ、クリックジャッキングなどの攻撃が可能になる可能性があります。
依存関係と前提条件	なし

データ保護

データ保護カテゴリは、データの機密性、完全性、および可用性 (CIA) の要素を対象としています。

CIA コンポーネントは次のとおりです。

- 機密性：データは転送中および停止中に不正アクセスから保護されます。
- 完全性：データは不正な作成、削除、変更から保護されます。
- 可用性：必要に応じてデータにアクセスできます。

[記憶する] の削除

glide.ui.forgetme プロパティを使用して、ログインページから [記憶する] チェックボックスを削除して、ログイン情報がキャッシュされないようにします。

詳細情報

属性	説明
プロパティ名	*glide.ui.forgetme*
構成タイプ	システムプロパティ (/sys_properties_list.do)
カテゴリ	データ保護
目的	認証情報がキャッシュされないようにすること。
セキュリティリスク評価	3.5
推奨値	true
機能への影響度	(低) この修正では、セッションが期限切れになるとインスタンスから自動的にログアウトされるため、ユーザーエクスペリエンスが変わります。セッションの有効期限は、「Managing user sessions」で詳述されているようにシステムプロパティに設定された値にのみ依存します。
セキュリティリスク	(低) [記憶する] チェックボックスをログイン時にオンにした場合、ユーザーのコンピューターに追加の Cookie が保存されます。 • その目的は、ログイン中のユーザーが再度アクセスした場合にセッションを自動的に再確立することです。 • ユーザーが意図的にログアウトするまでユーザーセッションはアクティブにできるため、セキュリティ上のリスクがあります。エンドユーザーがブラウザーをそのま

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

属性	説明
	まにして席を離れた場合、または別の攻撃によって侵害された場合、このシナリオでの攻撃の可能性が高くなります。
参照	[記憶する] チェックボックスを削除する

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

モバイルアプリケーションをバックグラウンドで実行する場合のペーストボードのクリア

このプロパティは *glide.sg.clear_pasteboard_when_backgrounded* 、ServiceNow モバイルアプリからコピーされたテキストを、アプリがバックグラウンドモードになった後もクリッパーとペーストボードに保持するかどうかを制御します。

詳細情報

属性	説明
構成名	*glide.sg.clear_pasteboard_when_backgrounded*
構成タイプ	システムプロパティ (/sys_properties_list.do)
データタイプ	ブーリアン
推奨値	true
デフォルト値	false
カテゴリ	データ保護
セキュリティリスク	• 重大度スコア：3.5 • CVSS スコア：低 • セキュリティリスクの詳細：このプロパティが推奨値の true に設定されていない場合、機密情報が Android または iOS のクリップボードに開示され、デバイス上の他のアプリケーションに開示される可能性があります。
依存関係と前提条件	なし
機能への影響	このプロパティは、ServiceNow アプリがバックグラウンドに入ったときにコピーおよび貼り付けクリップボードをクリアします。

個人メールからの人事ケースの更新を制限する

sn_hr_core.restrict_guest_email プロパティを使用して、ユーザーが個人メールで HR ケースに返信できるかどうかを制御します。

sn_hr_core.restrict_guest_email プロパティが true に設定されていない場合、ユーザーは、作業メモに含める HR ケースを参照するメールを個人アカウントから送信できます。これにより、個人のメールが侵害された場合や安全でない通信が行われた場合に、機密性や整合性に関する軽微な問題が発生する可能性があります。管理者は、どのユーザーが個人メールアカウントにアクセス

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

しているか確かでないため、ユーザーが個人メールから HR ケースに応答する機能を制限することができます。

詳細情報

属性	説明
構成名	*sn_hr_core.restrict_guest_email*
構成タイプ	システムプロパティ (/sys_properties_list.do)
データタイプ	ブーリアン
推奨値	true
デフォルト値	false
カテゴリ	データ保護
セキュリティリスク	• 重大度スコア：3.5 • CVSS スコア：低 • セキュリティリスクの詳細：このプロパティを true に設定しないと、個人のメールが侵害された場合や安全でない通信が行われた場合に、機密性や整合性に関する軽微な問題が発生する可能性があります。
依存関係と前提条件	なし
機能への影響	このプロパティは、個人メールアドレスからの返信で HR ケースを更新するかどうかを制御します。true に設定すると、個人用メールからの返信はすべてケースノートに追加されます。false の場合、ケースとメモは更新されません。

OAuth パラメーターの POST 投稿への制限

glide.oauth.allow.parameters.in.post.body.only プロパティは、インバウンド OAuth 認証によるアクセストークンの受け入れを制御します。アクセストークンは機密性が高く、POST 要求本文内にある場合にのみ受け入れるようにする必要があります。

詳細情報

属性	説明
構成名	*glide.oauth.allow.parameters.in.post.body.only*
構成タイプ	システムプロパティ (/sys_properties_list.do)
データタイプ	ブーリアン
推奨値	true
デフォルト値	true
カテゴリ	データ保護
セキュリティリスク	• 重大度スコア：7.4 • CVSS スコア：高

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

属性	説明
	• セキュリティ リスクの詳細: *glide.oauth.allow.parameters.in.post.body.only* 推奨値の true に設定されていない場合、アクセス トークンは GET 要求パラメーターに含まれる可能性があり、クライアント インフラストラクチャ ログに残り、それらのログが漏洩した場合にアカウントの乗っ取りにつながる可能性があります。
依存関係と前提条件	なし
参照	• OAuth 2.0 • OAuth トークンの管理
機能への影響度	oauth_token.do プロセッサが、サポートされているすべての権限許可タイプに対する入力として POST 本文パラメーターのみを受け付けることを確認します。

エラー処理とログ記録

エラー処理とログ記録のカテゴリは、ステークホルダーに公開されるログ情報の品質と詳細度に対応します。

これには、ログとエラーメッセージが機密情報を収集せず、分類に従ってデータを正しく保護し、適切な有効期間を設定していることの確認が含まれます。また、このカテゴリは、適切なエラー処理に関連し、さらにセキュリティに影響を与える未処理の例外の詳細なスタックトレースなどの機密性の高いエラーをエンドユーザーに公開しないことに関連しています。

スクリプトサンドボックスで権限の低いユーザーに対してロガーを無効にする

サンドボックス環境で実行されているスクリプトをログ記録する Glide システムの機能を管理します。

glide.security.sandbox_no_logging プロパティを使用して、サンドボックス環境で実行されているスクリプトをログ記録する Glide システムの機能を制御します。*glide.security.sandbox_no_logging* が **false** に設定されている場合、サンドボックススクリプトを使用して、権限の低いユーザーがログ記録を利用できます。権限の低いユーザーがログを挿入して、攻撃者が攻撃を難読化できる可能性があるため、これは潜在的なセキュリティの脆弱性です。サンドボックススクリプトを使用している権限の低いユーザーがログ記録機能を使用しないようにするには、プロパティを **true** に設定します。

詳細情報

属性	説明
構成名	*glide.security.sandbox_no_logging*
構成タイプ	システムプロパティ (/sys_properties_list.do)
データタイプ	ブーリアン
推奨値	true
デフォルト値	true

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

属性	説明
カテゴリ	エラー処理とログ記録
セキュリティリスク	• 重大度スコア：2.2 • CVSS スコア：低 • セキュリティリスクの詳細：このプロパティを **false** に設定すると、権限の低いユーザーのログ記録が有効になり、攻撃者が攻撃を難読化する可能性があります。
依存関係と前提条件	なし

安全な **Cookie** のデバッグの無効化

インスタンス内の Cookie に関連するログメッセージを管理します。

glide.secure_cookie.debug プロパティを使用して、Cookie に関連するログメッセージを管理します。このプロパティを **false** に設定すると、ログメッセージは表示されません。**true** に設定すると、SecureUserCookie クラスおよび Cookie クラスのメッセージがログに記録されます。これにより、機密情報がインスタンスで公開される可能性があります。

詳細情報

属性	説明
構成名	*glide.secure_cookie.debug*
構成タイプ	システムプロパティ (/sys_properties_list.do)
データタイプ	ブーリアン
推奨値	false
デフォルト値	false
カテゴリ	エラー処理とログ記録
セキュリティリスク	• 重大度スコア：4.2 • CVSS スコア：中 • セキュリティリスクの詳細：このプロパティを **true** に設定すると、機密情報が公開される可能性があります。
依存関係と前提条件	なし

SQL エラーメッセージを無効にする

glide.db.loguser プロパティを使用して、SQL エラーメッセージがブラウザーでレンダリングされないようにします。

詳細情報

属性	説明
プロパティ名	*glide.db.loguser*

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

属性	説明
構成タイプ	システムプロパティ (/sys_properties_list.do)
カテゴリ	エラー処理とログ記録
目的	ブラウザー内での SQL エラーメッセージの表示を無効にすること
タイプ	true | false
推奨値	false
セキュリティリスク評価	3.1
機能への影響度	(低) この修正により、SQL エラーメッセージをレンダリングできなくなります。機能への影響はありません。
セキュリティリスク	(中) 攻撃者に役立つ可能性のある機密の SQL 情報は、Web ページのエラーメッセージに含まれて表示されることはありません。

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

MID 監査ログを有効にする

MID Server コマンド監査ログには、コマンド名、コマンドハッシュ、使用された資格情報の名前、実行ステータスなどの詳細が記録されます。

有効にすると、ecc_agent_command_audit_logテーブルでagent_security_adminロールを持つユーザーが、または次の場所に移動して監査ログを表示できます **MID** サーバー > コマンド監査ログ.

MID Server によって実行されるコマンドの監査をオンにするには、ecc_agent_property テーブルで *`mid.log.command_audit.enable`* を true に設定します。

詳細情報

属性	説明
構成名	*`mid.log.command_audit.enable`*
構成タイプ	システムプロパティ (/sys_properties_list.do)
データタイプ	ブーリアン
推奨値	true
デフォルト値	false
カテゴリ	エラー処理とログ記録
セキュリティリスク	• 重大度スコア：2.2 • CVSS スコア：低 • セキュリティリスクの詳細：セキュリティ調査の際に、インシデント対応チームはこのテーブルを使用して、MID Server で実行されるコマンドを監査できます。このログがないと、アカウントの不正使用などの状況に対応するための十分な詳細情報がない可能性があります。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

属性	説明
依存関係と前提条件	なし

Protected Tables プラグインの有効化

com.glide.security.protected_table.enabled プロパティを使用して、権限の高いユーザーによってログテーブルが改ざんされることを防ぎます。

com.glide.security.protected_table.enabled プロパティが **true** に設定されている場合、Protected Tables プラグインを使用して、権限の高いユーザーによってインスタンスでログテーブルが改ざんされることを防ぎます。このプロパティが **true** に設定されている場合、次のログテーブルには特別な保護が適用されます。

- syslog (データベース上書きなし)
- syslog_transaction
- sys_outbound_http_log
- sysevent
- sys_audit
- sys_push_notification
- protected_table_configuration (データベース上書きなし)

ログの完全性は、顧客管理者がインスタンスで悪意のあるアクティビティを判断するために重要です。

詳細情報

属性	説明
構成名	*com.glide.security.protected_table.enabled*
構成タイプ	システムプロパティ (/sys_properties_list.do)
データタイプ	ブーリアン
推奨値	true
デフォルト値	false
カテゴリ	エラー処理とログ記録
セキュリティリスク	• 重大度スコア：4.5 • CVSS スコア：中 • セキュリティリスクの詳細：*com.glide.security.protected_table.enabled* を推奨値の true に設定しないと、高い権限を持つユーザーによってインスタンスでログテーブルが改ざんされる可能性があります。
依存関係と前提条件	なし
参照	システムログ

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

すべての送信 **http** 要求フィールドをログに記録する **[Security Center v1.3.2** で削除]

glide.outbound_http.security.log.allow.all.fields プロパティを false に設定し、機密性の高い送信 HTTP フィールドがプレーンテキストでログに記録されないようにします。

このプロパティが推奨値の **false** に設定されていない場合、機密性の高い送信 HTTP フィールドがプレーンテキストでログに記録される可能性があります。これにより、機密データや資格情報を含む送信要求が暗号化されていないプレーンテキストでログに記録され、特権の低いユーザーが表示できるため、企業ネットワークのセキュリティ体制が低下する可能性があります。

詳細情報

属性	説明
構成名	*glide.outbound_http.security.log.allow.all.fields*
構成タイプ	システムプロパティ (/sys_properties_list.do)
データタイプ	整数
推奨値	30
デフォルト値	30
カテゴリ	エラー処理とログ記録
セキュリティリスク	• 重大度スコア：6.8 • CVSS スコア：中 • セキュリティリスクの詳細：このプロパティを **false** に設定しないと、機密性の高い送信フィールドがプレーンテキストでログに記録される可能性が高くなり、セキュリティリスクを生じます。
依存関係と前提条件	なし

HTML サニタイゼーションのログ記録

glide.html_sanitize.discarded_log.enable プロパティを設定して、HTML サニタイゼーションイベントをインスタンスに記録するかどうかを決定します。

このプロパティが推奨値の **true** に設定されていない場合、HTML サニタイゼーションイベントは *sys_log* テーブルに記録されません。ログ記録がないと、インスタンスの自動セキュリティ検出および調査機能に悪影響を与える可能性があります。

詳細情報

属性	説明
構成名	*glide.html_sanitize.discarded_log.enable*
構成タイプ	システムプロパティ (/sys_properties_list.do)
データタイプ	ブーリアン
推奨値	true

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

属性	説明
デフォルト値	true
カテゴリ	エラー処理とログ記録
セキュリティリスク	• 重大度スコア：2.4 • CVSS スコア (CVSS score)：低 • セキュリティリスクの詳細 (Security risk details)：このプロパティが推奨値の **true** に設定されていない場合、HTML サニタイゼーションイベントは *sys_log* テーブルに記録されず、自動セキュリティ検出および調査機能に影響を与える可能性があります。
依存関係と前提条件	なし
参照	HTML サニタイザーの有効化

セッション監査イベントのログ記録

glide.authenticate.session_access.log_audit_event プロパティを **true** に設定すると、セッション監査イベントが *sys_session_access_audit* テーブルに作成されます。

セッションアクセスに関する情報のログ記録は、サイバーセキュリティ攻撃の分析に役立ちます。ログに記録される情報には、ユーザー、セッション ID (機密ではない)、IP アドレス、ロール、およびポリシーが含まれます。

詳細情報

属性	説明
構成名	*glide.authenticate.session_access.log_audit_event*
構成タイプ	システムプロパティ (/sys_properties_list.do)
データタイプ	ブーリアン
推奨値	true
デフォルト値	true
カテゴリ	エラー処理とログ記録
セキュリティリスク	• 重大度スコア：6.3 • CVSS スコア：中 • セキュリティリスクの詳細: このプロパティを推奨値の true に設定しないと、イベントがログに記録されなくなります。これにより、サイバー攻撃が発生した場合に攻撃者を見つけられなくなる可能性があります。
依存関係と前提条件	なし

ユーザー代理操作のログ記録

glide.sys.log_impersonation を構成して、ユーザー代理操作イベントをインスタンスのログに記録するかどうかを制御します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

このプロパティが推奨値の **true** に設定されていない場合、ユーザー代理操作イベントがログに記録されなくなります。ログ記録がないと、インスタンスの自動セキュリティ検出および調査機能に影響を与える可能性があります。

詳細情報

属性	説明
構成名	*glide.sys.log_impersonation*
構成タイプ	システムプロパティ (/sys_properties_list.do)
データタイプ	ブーリアン
推奨値	true
デフォルト値	true
カテゴリ	エラー処理とログ記録
セキュリティリスク	• 重大度スコア：6.4 • CVSS スコア：中 • セキュリティリスクの詳細：このプロパティが **true** に設定されていない場合、ユーザー代理操作イベントがログに記録されなくなり、インスタンスのセキュリティ検出および調査機能に影響を与える可能性があります。
依存関係と前提条件	なし
参照	Impersonating users

インポートプロセッサーでの詳細な **SQL** エラーメッセージの無効化

このプロパティを構成して、詳細な SQL エラーメッセージを表示するかどうかを制御します。

このプロパティが **false** に設定されている場合は、機密情報が漏洩する可能性がある詳細な SQL エラーメッセージが表示されます。これを回避するには、プロパティを **true** に設定して汎用メッセージを表示します。

詳細情報

属性	説明
構成名	*glide.import.error_message.generic*
構成タイプ	システムプロパティ (/sys_properties_list.do)
データタイプ	ブーリアン
推奨値	true
デフォルト値	true
カテゴリ	エラー処理とログ記録

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

属性	説明
セキュリティリスク	• 重大度スコア：3.1 • CVSS スコア：低 • セキュリティリスクの詳細：このプロパティを **false** に設定すると、情報漏えいにつながる可能性がある詳細な SQL メッセージが有効になります。
依存関係と前提条件	なし

ファイルとリソース

ファイルとリソースカテゴリにより、アプリケーションが信頼できないファイルデータを安全に処理し、権限が制限された信頼できないソースからの信頼できないデータを適切な場所に保存できるようになります。

これには、サイズが大きいファイルまたは予期しないファイルタイプによるサービス拒否の回避、ファイルタイプの検証、パストラバースの防止などのコントロールが含まれます。

感染したファイルのダウンロードを許可しない

このプロパティを管理して、スタックトレースをインスタンスに表示するかどうかを制御します。

*com.glide.snap.infected_download_allowed*推奨値の false に設定されていない場合、スキャンされていない悪意のあるファイルをダウンロードして、ユーザーのデスクトップに感染する可能性があります。

詳細情報

属性	説明
構成名	*com.glide.snap.infected_download_allowed*
構成タイプ	システムプロパティ (/sys_properties_list.do)
データタイプ	ブーリアン
推奨値	true
デフォルト値	true
カテゴリ	ファイルとリソース
セキュリティリスク	• 重大度スコア：6.7 • CVSS スコア：中 • セキュリティリスクの詳細:このプロパティを推奨値の false に設定しないと、インスタンスが悪意のあるファイルのダウンロードにさらされる可能性があります。
依存関係と前提条件	なし

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

スパムメールのスコアリングとフィルタリングを有効にする

Email Filter (*com.glide.email_filter*) プラグインをインストールして、インスタンス内にメールフィルタリングをインストールします。このフィルタリングでは、既存のヘッダーを識別し、関連するヘッダーに基づいてメールの処理方法を決定できます。

Now Platform メールサーバーを介して送信されるメッセージはすべて、スパムメールの可能性について評価されます。

注:
インスタンスがプライベートメールサーバーを使用している場合は、このトピックは適用できません。詳細については、「スパムメールのスコアリングとフィルタリング」を参照してください。

必須条件

このプロパティを設定する前に、次の手順を実行してください。

glide.email.read.active プロパティを true に設定します。詳細については、「独自の POP3 サーバーの使用を有効にする」を参照してください。

詳細情報

属性	説明
プラグイン名	*com.glide.email_filter*
構成タイプ	[システム定義] > [プラグイン]
カテゴリ	ファイルとリソース
目的	フィルタリングを適用してメールのスパム送信を回避すること
推奨値	有効
セキュリティリスク評価	8.1
機能への影響度	(低) スパムスコアリングの一環として、インスタンスからメールがフィルタリング、ブロック、または隔離されることがなくなります。スコアリングのみが行われた後、インスタンスに送信されます。フィルタリングはすべて、Email Filters プラグインを使用して インスタンス内で行われます。
セキュリティリスク	(中) メールフィルターを使用すると、管理者は条件ビルダーまたは条件付きスクリプトを使用して、既知/不明の送信者からの悪意のある受信メールを無視するタイミングを指定できます。
参照	メールフィルター https://support.servicenow.com/kb_view.do?sysparm_article=KB0549426

プラグインのアクティブ化の詳細については、「Activate a plugin」を参照してください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ウイルス対策スキャンを有効にする

com.glide.snap.enable_scan プロパティはウイルス対策スキャン機能を有効にします。

ウイルス対策スキャンを有効にするには、*com.glide.snap.enable_scan* を推奨値の **true** に設定します。

⚠ 警告:
これはセーフハーバープロパティです。つまり、いったん変更したら変えることはできません。元に戻すことはできません。

詳細情報

属性	説明
プロパティ名	*com.glide.snap.enable_scan*
構成タイプ	システムプロパティ (/sys_properties_list.do)
カテゴリ	ファイルとリソース
目的	特定のインスタンスでウイルス対策スキャンを有効または無効にします。
推奨値	True (デフォルト)
構成タイプ	ブーリアン
セキュリティリスク	(高) Antivirus Scanning を使用すると、インシデント、問題、ストーリーなど、システムレコードに添付ファイルによって持ち込まれるウイルス感染からインスタンスを保護できます。
セキュリティリスク評価	7.7

静的コンテンツでダウンロード可能なファイルタイプを制限する

glide.ui.strict_customer_uploaded_static_content プロパティを使用して、ファイルのアップロード機能でアップロードされた場合にダウンロード可能になるファイルタイプを制限できるようにします。

このプロパティを *glide.ui.strict_customer_uploaded_content_types* プロパティとともに使用すると、制限付きダウンロード可能ファイルタイプのカンマ区切りリストが作成されます。詳細については、「ダウンロード可能なファイルタイプ」を参照してください。

⚠ 警告:
このプロパティの値は、DB なしのオーバーライドです。変更またはオーバーライドすることはできません。

詳細情報

属性	説明
プロパティ名	*glide.ui.strict_customer_uploaded_static_content*
構成タイプ	システムプロパティ (/sys_properties_list.do)
カテゴリ	ファイルとリソース

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

属性	説明
目的	アプリケーションからダウンロードできるファイルタイプを確実に安全なものにすること
推奨値	true
セキュリティリスク評価	3.1
機能への影響度	(低) この修正では、*glide.ui.strict_customer_uploaded_content_types* プロパティで指定された値に基づいてファイルのダウンロード制限が適用されます。詳細については、「ダウンロード可能なファイルタイプ」を参照してください。
セキュリティリスク	(低) ファイルのダウンロード制限は、信頼できないユーザー入力ソースに適用する必要があります。

GraphQL エンドポイントのトレーニングおよび予測フローでの添付ファイルサイズの制限

glide.platform_ml_di.max_attachment_size_graphql プロパティは、トレーニングおよび予測フローの GraphQL エンドポイントで返される添付ファイルの最大サイズをコントロールします。

詳細情報

属性	説明
構成名	*glide.platform_ml_di.max_attachment_size_graphql*
構成タイプ	システムプロパティ (/sys_properties_list.do)
データタイプ	整数
推奨値	5,242,880
デフォルト値	5,242,880
カテゴリ	ファイルとリソース
セキュリティリスク	• 重大度スコア：7.3 • CVSS スコア：中 • セキュリティリスクの詳細：このプロパティが推奨値である 5,242,880 未満に設定されていない場合、大きなファイルが返されるとサービス拒否 (DoS) が発生する可能性があります。
依存関係と前提条件	なし

トレーニングフローと予測フローでの添付ファイルサイズの制限

glide.platform_ml_di.max_attachment_size プロパティは、トレーニングおよび予測フローで返される添付ファイルの最大サイズをコントロールします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

詳細情報

属性	説明
構成名	*glide.platform_ml_di.max_attachment_size*
構成タイプ	システムプロパティ (/sys_properties_list.do)
データタイプ	整数
推奨値	4,000,000
デフォルト値	4,000,000
カテゴリ	ファイルとリソース
セキュリティリスク	• 重大度スコア：7.3 • CVSS スコア：中 • セキュリティリスクの詳細: *glide.platform_ml_di.max_attachment_size* が推奨値の 4,000,000 以下に設定されていない場合、大きなファイルを返すとサービス拒否 (DoS) 攻撃が発生する可能性があります。
依存関係と前提条件	なし

HTTP 応答本文のサイズを制限する

*glide.http.response.get_body.limit.enabled**glide.http.response.get_body.limit*およびプロパティを構成して、インスタンスを *OutOfMemoryExceptions* から保護します。

and *glide.http.response.get_body.limit* プロパティは、*glide.http.response.get_body.limit.enabled*要求応答が大きすぎる結果として *OutOfMemoryExceptions* がスローされないようにする新しい機能を有効にするために導入されました。*OutOfMemoryExceptions* は、サービス拒否 (DoS) 攻撃やその他の問題を引き起こす可能性があり、攻撃者がインスタンスを侵害するのを支援する可能性があります。

これらのセキュリティの脆弱性からインスタンスを保護するには、*glide.http.response.get_body.limit.enabled* が true に設定され、*glide.http.response.get_body.limit* が 524,288,000 メガバイト (500 MB) 以下であることを確認してください。

詳細情報

属性	説明
構成名	*glide.http.response.get_body.limit.enabled* および *glide.http.response.get_body.limit*
構成タイプ	システムプロパティ (/sys_properties_list.do)
データタイプ	ブーリアン
推奨値	true
デフォルト値	true
カテゴリ	ファイルとリソース

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

属性	説明
セキュリティリスク	• 重大度スコア：6.4 • CVSS スコア：中 • セキュリティリスクの詳細:これらのプロパティを推奨値に設定しないと、インスタンスが *OutOfMemoryExceptions* やサービス拒否攻撃に対して脆弱になる可能性があります。
依存関係と前提条件	なし
機能への影響度	このプロパティを使用すると、顧客が誤って大きなファイルをメモリに読み込むことが原因で *OutOfMemoryException* が発生する可能性が低くなります。

メールの最大添付ファイル数の制限

インスタンスで受信メールの添付ファイルの数を設定します。

glide.email.inbound.max_attachment_count プロパティはインスタンスで受信メールの添付ファイルの最大数を制御します。このプロパティが **30** 以下の推奨値に設定されていない場合、受信メールによってインスタンスのパフォーマンスが低下する可能性があります。

詳細情報

属性	説明
構成名	*glide.email.inbound.max_attachment_count*
構成タイプ	システムプロパティ (/sys_properties_list.do)
データタイプ	整数
推奨値	30
デフォルト値	30
カテゴリ	ファイルとリソース
セキュリティリスク	• 重大度スコア：5.3 • CVSS スコア (CVSS score)：中 • セキュリティリスクの詳細 (Security risk details)：プロパティ値を 30 より大きい値に設定すると、デグレードの問題が発生する可能性があります。
依存関係と前提条件	なし
参照	Email properties

許可される添付ファイルサイズを最小化

com.glide.attachment.max_size プロパティを設定して、アップロードされた添付ファイルに許可される最大サイズを制御します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

このプロパティは、アップロードされた添付ファイルの最大サイズを制御します。このプロパティが **1024** 以下の推奨値に設定されていない場合、プラットフォームはストレージを満杯にし、サービス拒否 (DoS) 攻撃につながる可能性がある大きなファイルを受け入れる場合があります。

> **注:**
> 実際の添付ファイルサイズは 1024 x 1024 にプロパティの値を乗算して計算されます。プロパティの値が **1024** の場合、添付ファイルに許可される最大サイズは 1 GB です。

詳細情報

属性	説明
構成名	*com.glide.attachment.max_size*
構成タイプ	システムプロパティ (/sys_properties_list.do)
データタイプ	整数
推奨値	1024
デフォルト値	4096
カテゴリ	ファイルとリソース
セキュリティリスク	• 重大度スコア：6.5 • CVSS スコア (CVSS score)：中 • セキュリティリスクの詳細 (Security risk details)：このプロパティが **1024** 以下に設定されていない場合、プラットフォームは DoS 攻撃につながる可能性のある大きなファイルを受け入れる場合があります。
依存関係と前提条件	なし
参照	Attachment limit properties

AttachmentCreator SOAP Web Service のファイル MIME タイプの検証

glide.attachment.enforce_security_validation プロパティは、 MIME (多目的インターネットメール拡張) ファイルが検証を受けるかどうかを決定します。

*glide.attachment.enforce_security_validation*が推奨値の **true** に設定されていない場合、MIME ファイルが検証されないため、悪意のあるファイルが誤ったファイル拡張子でアップロードされる可能性があります。このプロパティを **true** に設定すると、ファイルは正しいファイルタイプ拡張子でアップロードされます。

詳細情報

属性	説明
構成名	*glide.attachment.enforce_security_validation*
構成タイプ	システムプロパティ (/sys_properties_list.do)
データタイプ	ブーリアン
推奨値	true
デフォルト値	true

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

属性	説明
カテゴリ	ファイルとリソース
セキュリティリスク	• 重大度スコア：7.5 • CVSS スコア：高 • セキュリティリスクの詳細：プロパティが false に設定されている場合、アップロード中に MIME ファイルは検証されません。これにより、悪意のあるファイルがファイル拡張子を変更することで偽装される可能性があります。
依存関係と前提条件	なし
参照	https://developer.mozilla.org/en-US/docs/Web/HTTP/Basics_of_HTTP/MIME_types/Common_types
機能への影響度	アップロードされた添付ファイルに対して MIME タイプとファイル拡張子の検証を実行するには、このハードニング設定を true に設定します。このプロパティが false に設定されている場合、検証は実行されません。このプロパティはデフォルトで [true] に設定されています。

悪意のあるコード

悪意のあるコードのカテゴリでは、コードに脆弱性や不要な機能がないことを確認するための最善の努力が払われます。

これには、悪意のあるアクティビティに対する安全で適切な処理、時間ベースの攻撃がないこと、信頼できない宛先への送信通信がないこと、および承認されていないコードや攻撃者が制御するコードが含まれていないことの確認が含まれます。このカテゴリには、アプリケーションコードベースからの監査ライブラリまたはサードパーティライブラリが含まれます。

ルート化またはジェイルブレイクされたモバイルデバイスのブロック

ジェイルブレイクされたデバイスからの不正アクセスを防止して、インスタンスを保護します。

glide.sg.allow_rooted_jailbroken_device プロパティを使用し、ジェイルブレイクされたデバイスによる不正アクセスからインスタンスを保護します。このプロパティが **false** に設定されているときにユーザーがモバイルアプリを使用してインスタンスへの認証を試みると、次のアラートが表示されます：「This device appears to be jailbroken and cannot be used to access this instance. Please contact your ServiceNow Administrator.)」。アラートメッセージが表示されている間はアプリがフリーズします。このメッセージを消すための唯一の方法は [ログアウト] を選択することです。このプロパティが **true** に設定されている場合、ユーザーはジェイルブレイクされたデバイスを使用してインスタンスに対して認証を行います。

詳細情報

属性	説明
構成名	*glide.sg.allow_rooted_jailbroken_device*
構成タイプ	システムプロパティ (/sys_properties_list.do)
データタイプ	ブーリアン

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

属性	説明
推奨値	false
デフォルト値	false
カテゴリ	悪意のあるコード
セキュリティリスク	• 重大度スコア：4.5 • CVSS スコア：中 • セキュリティリスクの詳細：ジェイルブレイクされたデバイスはセキュリティが欠如するため、デバイスは攻撃者の主要な標的になります。承認されていないエンティティが企業データにアクセスすると、企業ネットワークのセキュリティ体制が弱まる可能性があります。
依存関係と前提条件	なし
参照	アクセス制御

アプリケーション構成データとスクリプトのコード署名を有効にする **(Security Center 1.3.2** で削除)

アプリケーション構成データとスクリプトのコード署名を有効にします。

コード署名を使用すると、機密性の高いアプリケーション構成データとスクリプトを使用する前に検証できるので、セキュリティの強化に役立ちます。コード署名は、データの信頼性と整合性を確認するために後でチェックされるデータのデジタル署名を作成します。この検証により、悪意のあるデータやスクリプトがインスタンスで使用され、インスタンスが完全に侵害される恐れを防ぎます。

com.snc.kmf.signature.validation.flag プロパティを使用して、アプリケーション構成データとスクリプトのコード署名を管理します。このプロパティを **true** に設定すると、アプリケーション構成データとスクリプトのコード署名が有効になります。

> ⚠ **警告:**
> これはセーフハーバープロパティです。つまり、いったん変更したら変えることはできません。元に戻すことはできません。

詳細情報

属性	説明
構成名	*com.snc.kmf.signature.validation.flag*
構成タイプ	システムプロパティ (/sys_properties_list.do)
データタイプ	ブーリアン
推奨値	true
デフォルト値	false
カテゴリ	悪意のあるコード
セキュリティリスク	• 重大度スコア：6 • CVSS スコア：中

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

属性	説明
	• セキュリティリスクの詳細：このプロパティを **true** に設定すると、コード署名が有効になり、機密性の高いアプリケーション構成データとスクリプトを検証することでセキュリティを強化できます。
依存関係と前提条件	なし

セッション管理

このカテゴリは、ユーザーのアプリケーションステータスのセキュリティを調べます。セッションは、各個人に対して一意で、推測または共有できず、何度かの非アクティブ期間の後や不要な場合は無効にされる必要があります。これには、Cookie ベースのセッションの Cookie 属性、セッショントークンの生成とストレージ、およびフェデレーション再認証の要件などの要素が含まれます。

絶対セッションタイムアウト期間の最小化

glide.ui.user_cookie.max_life_span_in_days プロパティを使用して、ユーザーが [記憶する] チェックボックスを選択してログインしたときに作成される Cookie の最大有効期間を設定します。Cookie の有効期間が切れると、[記憶する] チェックボックスを選択したユーザーはインスタンスへの再認証を強制されます。

これによりユーザー Cookie の有効期間は、Cookie が最初に発行されてからの指定の日数になります。デフォルト値は 30 日で、上限は 365 日です。

注:
任意のアクティブユーザーセッションに対して最大セッション時間を適用する場合は、「Managing user sessions」を参照してください。

詳細情報

属性	説明
プロパティ名	*glide.ui.user_cookie.max_life_span_in_days*
構成タイプ	システムプロパティ (/sys_properties_list.do)
カテゴリ	セッション管理
目的	特定の日数後に、[記憶する] チェックボックスを選択したユーザーに再認証を強制します。
機能への影響度	(中) このプロパティは、指定された期間が経過した後、すべての種類の Cookie ローテーションを回避することによって再ログインを強制します。
セキュリティリスク評価	4.2
セキュリティリスク	(中) ユーザーの Cookie が無期限にアクティブになるとセキュリティリスクが発生するため、時間ベースの構成で期限が切れるようにする必要があります。
参照	利用可能なシステムプロパティ [記憶する] チェックボックスと cookie の設定を変更する

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

アクティブセッションタイムアウト例外ロールの定義

glide.active.session.timeout.exception.roles プロパティは、アクティブセッションタイムアウト制限から除外されるロールを制御します。

アクティブセッションタイムアウトにより、認証情報を再度提供しない限り、ハイジャックされたセッションを無期限に使用することができなくなります。このセキュリティリスクを修正するには、*glide.active.session.timeout.exception.roles* プロパティが **edge_encryption, mid_server** に設定されていることを確認してください。

詳細情報

属性	説明
構成名	*glide.active.session.timeout.exception.roles*
構成タイプ	システムプロパティ (/sys_properties_list.do)
データタイプ	文字列
推奨値	edge_encryption、mid_server
デフォルト値	edge_encryption、mid_server
カテゴリ	セッション管理
セキュリティリスク	• 重大度スコア：7.1 • CVSS スコア：高 • セキュリティリスクの詳細：内部の統合アカウントロールについてのみ、アクティブセッションタイムアウト制限例外を検討してください。ロールにセッションタイムアウトの例外が与えられ、そのロールがセッションハイジャック攻撃の被害者であるユーザーに与えられた場合、攻撃者はそのセッションに対して無期限に認証を続けることができます。これにより、攻撃者がハイジャックされたアカウントを使用する時間が増えるため、セキュリティインシデントの影響が高くなる可能性があります。
依存関係と前提条件	なし

UserCookie バージョン 3.1 の有効化

インスタンスで有効になっている UserCookie のバージョンを管理して、ソースコード内の秘密キーのストレージを保護します。

UserCookie v3 は、*glide.ui.secure.cookies.use_kmf* プロパティが無効になっている場合にのみ生成されます。UserCookie v3 は、ハッシュベースのメッセージ認証コード (HMAC) の秘密キーがすべての顧客に同一のソースコードに格納されるため、安全ではありません。攻撃者は、秘密キーを使用してユーザーセッションをハイジャックしようとする可能性があります。このセキュリティ上の脅威を修復するには、*glide.ui.secure.cookies.use_kmf* プロパティが **true** に設定され、UserCookie v3.1 が使用されていることを確認してください。秘密キーは、KMF などの安全なストレージに保存されます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

詳細情報

属性	説明
構成名	*glide.ui.secure.cookies.use_kmf*
構成タイプ	システムプロパティ (/sys_properties_list.do)
データタイプ	ブーリアン
推奨値	true
デフォルト値	false
カテゴリ	セッション管理
セキュリティリスク	• 重大度スコア：7.1 • CVSS スコア：高 • セキュリティリスクの詳細：これを **false** に設定すると、ハッシュベースのメッセージ認証コード (HMAC) の秘密キーがソースコードに格納されるため、セキュリティの脆弱性が発生します。
依存関係と前提条件	なし

API 要求でのパスワードリセットの強制

インスタンスでのパスワードリセット機能の動作方法を管理します。

ユーザーが [パスワードのリセットが必要 **(Password needs reset)**] とマークされている場合、次の認証試行時に新しいパスワードを入力する必要があります。このプロパティは、API 呼び出しを行う前にパスワードのリセットが必須かどうかを制御します。このプロパティが推奨値の **true** に設定されていない場合でも、[パスワードのリセットが必要 **(Password needs reset)**] とマークされたユーザーアカウントは、基本認証を通じてテーブル API をクエリすることで操作を実行できます。このセキュリティの脆弱性により、非アクティブなアカウントが侵害された場合に情報が漏洩する可能性があります。

詳細情報

属性	説明
構成名	*glide.authenticate.api.user.reset_password.mandatory*
構成タイプ	システムプロパティ (/sys_properties_list.do)
データタイプ	ブーリアン
推奨値	true
デフォルト値	true
カテゴリ	セッション管理

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

属性	説明
セキュリティリスク	• 重大度スコア：8.1 • CVSS スコア：高 • セキュリティリスクの詳細：このプロパティを **false** に設定すると、非アクティブなアカウントが侵害された場合に情報が漏洩する可能性があります。
依存関係と前提条件	なし

HTTP のみの Cookie フラグを有効にする

glide.cookies.http_only プロパティを使用して、機密性の高い Cookie の HTTPOnly 属性を有効にします。

HTTPOnly 属性は、JavaScript などのクライアント側スクリプトを使用した Cookie へのアクセスを許可しないため、クロスサイトスクリプティングなどの攻撃を防止するために使用します。クロスサイトスクリプティングのリスクは排除されませんが、一部の悪用ベクトルは排除されます。

警告:
これはセーフハーバープロパティです。つまり、いったん変更したら変えることはできません。元に戻すことはできません。

詳細情報

属性	説明
プロパティ名	*glide.cookies.http_only*
構成タイプ	システムプロパティ (/sys_properties_list.do)
カテゴリ	セッション管理
目的	クライアント側スクリプトが保護された Cookie にアクセスするリスクを軽減すること
推奨値	true
セキュリティリスク評価	8
機能への影響度	(低) この修正では、セッション Cookie に HTTPOnly フラグが追加されるため、Cookie の盗難を防ぎます。 • ユーザーの Cookie にアクセスするために JavaScript を必要とするカスタム機能がある場合、その機能は損なわれます。通常の状況では発生しないはずです。 • Now Platform がセッション管理を処理するため、カスタムスクリプトがユーザーの Cookie にアクセスする理由はありません。
セキュリティリスク	(中) アプリケーションのセッション Cookie はエンドユーザーを認証し、アプリケーションに対する暗黙的なアクセス権限を付与します。つまり、セッション Cookie の盗難やエクスポートの防止が必要になります。HTTP Only フラグは、JavaScript インジェクションまたはクロスサイ

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

属性	説明
	トスクリプティングの脆弱性による盗難からセッション Cookie を保護します。
参照	利用可能なシステムプロパティ

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

同時インタラクティブセッション数の最小化

このプロパティを Limit Concurrent Sessions プラグインと共に使用して、ユーザーが開くことができるアクティブなセッションの数を制御します。

[Glide 認証：同時インタラクティブセッションの最大数] プロパティを **Limit Concurrent Sessions** (*com.glide.limit.concurrent.sessions*) プラグインと共に使用して、ユーザーに開かれるアクティブなセッションの数を制御します。推奨値は **1** です。これにより、開かれるセッションの数が減ります (数が多いほど、セッションがハイジャックされる可能性が高くなります)。

詳細情報

属性	説明
構成名	*glide.authenticate.max.concurrent.interactive.sessions*
構成タイプ	システムプロパティ (/sys_properties_list.do)
データタイプ	整数
推奨値	1
デフォルト値	1
カテゴリ	セッション管理
セキュリティリスク	• 重大度スコア：3.7 • CVSS スコア：低 • セキュリティリスクの詳細： プロパティのデフォルト値を 1 より大きく設定すると、セッションハイジャックの可能性が高まります。
依存関係と前提条件	**Concurrent Interactive Sessions** (*com.glide.limit.concurrent.sessions*) プラグインがアクティブになっている必要があります。
参照	同時セッションの制限

すべてのノードにまたがる同時セッションを制限する

glide.authenticate.limit.concurrent.sessions.across.all.nodes プロパティを Limit Concurrent Sessions プラグインとともに使用して、すべてのノードで追跡されるセッションの数を管理します。

同時セッションの制限 プラグインがアクティブな場合、ユーザーごとに開いているセッションの数を制限できます。このプラグインがアクティブなときに、(**[Glide** 認証：全ノードを対象とした同時セッションの制限]) プロパティが **true** に設定されていることを確認します。これにより、開いているセッションの数が単一のアプリケーションノードではなくすべてのノードで追跡されるようになり

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ます。このプロパティが **false** に設定されている場合、複数のノードで複数のセッションを開くことができるため、セッションハイジャックの可能性が高くなります。

詳細情報

属性	説明
構成名	*glide.authenticate.limit.concurrent.sessions.across.all.n*
構成タイプ	システムプロパティ (/sys_properties_list.do)
データタイプ	ブーリアン
推奨値	true
デフォルト値	true
カテゴリ	セッション管理
セキュリティリスク	• 重大度スコア：3.7 • CVSS スコア：低 • セキュリティリスクの詳細：**Limit Concurrent Sessions** プラグインを使用している場合、このプロパティを **false** に設定すると、複数のノードに渡って複数のセッションが開かれ、セッションハイジャックなどのセキュリティ脆弱性の可能性が高くなります。
依存関係と前提条件	なし
参照	同時セッションの制限

Limit concurrent sessions プラグイン

com.glide.limit.concurrent.sessions プラグインを設定して、インスタンスでのセッションハイジャックの可能性を減らします。

このプラグインを使用すると、管理者はユーザーまたはロールごとのアクティブセッションの数を制限できます。セッションハイジャックの可能性を減らすために、このプラグインを有効にして構成することをお勧めします。このプラグインが有効になっていて構成されている場合、ハイジャックされる可能性がある開かれたセッションの数が制限されます。

詳細情報

属性	説明
構成名	*com.glide.limit.concurrent.sessions*
構成タイプ	システムプロパティ (/sys_properties_list.do)
データタイプ	プラグイン
推奨値	com.glide.limit.concurrent.sessions を有効に構成
デフォルト値	com.glide.limit.concurrent.sessions を有効に構成
カテゴリ	セッション管理

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

属性	説明
セキュリティリスク	• 重大度スコア：3.7 • CVSS スコア：低 • セキュリティリスクの詳細：このプラグインがアクティブでない場合、セッションハイジャックの可能性が高くなります。
依存関係と前提条件	なし

ゲストのアクティブなセッションの有効期間の制限

glide.guest.active.session.life_span プロパティを使用して、アクティブなゲストの HTTP セッションの期間を制御します。

*glide.guest.active.session.life_span*このプロパティは、セッションの非アクティブ状態や、ユーザーが非アクティブ状態のままでセッションがタイムアウトしてクローズするまでの時間に関係なく、アクティブなゲスト HTTP セッションに最大有効期間を適用します。構成値は分単位です。値を 0 にすると、アクティブ セッションのタイムアウトが無効になります。値を大きくすると、攻撃者は盗まれたセッションに長く留まり、セキュリティインシデントの可能性が高くなる可能性があります。このプロパティは、インスタンスへの低い権限アクセスを持つゲストユーザーに制限されています。

このセキュリティの脆弱性を修復するには、0 より大きく 720 以下の値に設定します *glide.guest.active.session.life_span* 。

詳細情報

属性	説明
構成名	*glide.guest.active.session.life_span*
構成タイプ	システムプロパティ (/sys_properties_list.do)
データタイプ	整数
推奨値	1-720 (分)
デフォルト値	0
カテゴリ	セッション管理
セキュリティリスク	• 重大度スコア：4.2 • CVSS スコア：中 • セキュリティリスクの詳細： 最大有効期間を大きな値に設定すると、攻撃者がセッションを盗んだ場合にインスタンス内で操作できる時間がより多くなります。
依存関係と前提条件	なし
機能への影響	この構成では、非アクティブなタイムアウトに関係なく、アクティブなゲスト HTTP セッションに最大有効期間が適用されます。構成値は分単位です。値を 0 にすると、アクティブ セッションのタイムアウトが無効になります。最大有効期間は、非アクティブ タイムアウト

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

属性	説明
	glide.guest.session_timeout (既定値は 30 分) を超える必要があります。

同時インタラクティブセッションの制限

インスタンス上のインタラクティブセッションの数を管理します。

glide.authenticate.limit.concurrent.interactive.sessions プロパティを使用して、インスタンス上のインタラクティブセッションの数を管理します。このプロパティは、 同時セッションの制限 (com.glide.limit.concurrent.sessions) プラグインとともに使用されます。プラグインがアクティブで、プロパティが **false** に設定されている場合、ユーザーはインスタンス上で任意の数の同時インタラクティブセッションを使用することができます。開いているセッションの数が多いほど、セッションハイジャックが発生する可能性が高くなります。

詳細情報

属性	説明
構成名	*glide.authenticate.limit.concurrent.interactive.sessions*
構成タイプ	システムプロパティ (/sys_properties_list.do)
データタイプ	ブーリアン
推奨値	true
デフォルト値	false
カテゴリ	セッション管理
セキュリティリスク	• 重大度スコア：3.7 • CVSS スコア：低 • セキュリティリスクの詳細：プラグインがアクティブで、プロパティが **false** に設定されている場合、ユーザーはインスタンス上で任意の数の同時インタラクティブセッションを使用することができ、そのためにセッションハイジャックの可能性が高くなります。
依存関係と前提条件	なし
参照	同時インタラクティブセッションの制限

統合のアクティブセッションの有効期間の制限

glide.integrations.active.session.life_span プロパティは、非アクティブタイムアウトに関係なく、アクティブなゲスト HTTP セッションに最大の有効期間を適用します。構成値は分単位です。値を 0 にすると、アクティブ セッションのタイムアウトが無効になります。

詳細情報

属性	説明
構成名	*glide.integrations.active.session.life_span*
構成タイプ	システムプロパティ (/sys_properties_list.do)

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

属性	説明
データタイプ	整数
推奨値	0 から 720
カテゴリ	セッション管理
セキュリティリスク	• 重大度スコア：4.2 • CVSS スコア：中 • セキュリティリスクの詳細：最大有効期間が長いほど、攻撃者が盗んだセッションをより長く保持できるので、セキュリティインシデントの範囲が拡大します。このプロパティは、インスタンスへの低いアクセス権を持つ統合に限定されます。glide プロパティ *glide.integrations.active.session.life_span* の値を 0 より大きく、720 以下に設定します。
依存関係と前提条件	なし

UI のアクティブセッションの有効期間の制限

glide.ui.active.session.life_span プロパティは、非アクティブタイムアウトに関係なく、アクティブなゲスト HTTP セッションに最大の有効期間を適用します。

構成値は分単位です。値を 0 にすると、アクティブ セッションのタイムアウトが無効になります。

詳細情報

属性	説明
構成名	*glide.ui.active.session.life_span*
構成タイプ	システムプロパティ (/sys_properties_list.do)
データタイプ	整数
デフォルト値	0
カテゴリ	セッション管理
セキュリティリスク	• 重大度スコア：4.2 • CVSS スコア：中 • セキュリティリスクの詳細:最大有効期間が長くなると、攻撃者が盗まれたセッションに長く留まる可能性があり、セキュリティインシデントの可能性が高くなる可能性があります。
依存関係と前提条件	なし
機能への影響	非アクティブなタイムアウトに関係なく、アクティブな認証済み HTTP セッションに最大有効期間を強制します。構成値は分単位です。値を 0 にすると、アクティブ セッションのタイムアウトが無効になります。最大有効期間は、非アクティブタイムアウト glide.ui.session_timeout (デフォルトは 30 分) より長くする必要があります。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

非アクティブなセッションのプロアクティブな無効化

このプロパティは *glide.active.session.timeout.invalidate.session* 、Tomcat サーバーの前でタイムアウトセッションを事前に無効にするかどうかを制御します。

true *glide.active.session.timeout.invalidate.session*に設定されていない場合、タイムアウトしたセッションが無効にならない短い時間間隔 (キューサイズに応じて 60 秒以上) が存在する可能性があります。セッションがハイジャックされた場合、攻撃者はこの短い期間にセッションを使用できる可能性があります。このセキュリティリスクを修復するには、*glide.active.session.timeout.invalidate.session* を **true** に設定します。

詳細情報

属性	説明
構成名	*glide.active.session.timeout.invalidate.session*
構成タイプ	システムプロパティ (/sys_properties_list.do)
データタイプ	ブーリアン
推奨値	true
デフォルト値	false
カテゴリ	セッション管理
セキュリティリスク	• 重大度スコア：4.6 • CVSS スコア：中 • セキュリティリスクの詳細: このプロパティを推奨値の true に設定しないと、タイムアウトしたセッションが検証されない可能性があります。これにより、攻撃者がセッションをハイジャックする可能性が高くなります。
依存関係と前提条件	なし

HTTP セッション識別子をローテーションする

glide.ui.rotate_sessions プロパティを使用して HTTP セッション識別子のローテーションを有効にし、セキュリティの脆弱性を軽減します。

認証後に非認証ユーザーのセッション ID が変更されない場合、Web アプリケーションはセッション固定化攻撃 に対して脆弱になります。悪意のあるユーザーが非認証セッションを開始し、関連するセッション ID を被害者に提供する可能性があります。被害者が認証されると、悪意のあるユーザーがその認証済みセッションを共有するようになります。

詳細情報

属性	説明
プロパティ名	*glide.ui.rotate_sessions*
構成タイプ	システムプロパティ (/sys_properties_list.do)
カテゴリ	セッション管理
目的	より安全なセッション認証を実現すること

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

属性	説明
推奨値	true
セキュリティリスク評価	8.8
機能への影響度	(中) この修正では、ユーザーが非認証ページから認証済みページに移動したときに SessionID が変更されました。 • ユーザーの初回ログイン時に、または何らかの目的でプロキシを使用したり、SessionID をハードコーディングしたりすると、機能に影響を与える可能性があります。 • Single Sign-on 認証に SAML 2.0 プラグインを使用している場合、インスタンスと ID プロバイダーの間で行われるセッション情報の共有が妨げられる可能性があります。そのような場合、このプロパティを false に設定できます。
セキュリティリスク	(中) SessionID は、ブラウザーでセッションステータスを維持することによって、インスタンスユーザーを処理および認証するために使用されます。したがって、SessionID は機密データと見なされ、デフォルトで安全である必要があります。セッションローテーションは、ユーザーが非認証ページから認証ページへ移動するたびに SessionID の変更を適用するセキュリティコントロールです。
参照	SAML による認証

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

同時インタラクティブセッション数の最小化

このプロパティを Limit Concurrent Sessions プラグインと共に使用して、ユーザーが開くことができるアクティブなセッションの数を制御します。

[Glide 認証：同時インタラクティブセッションの最大数] プロパティを **Limit Concurrent Sessions** (*com.glide.limit.concurrent.sessions*) プラグインと共に使用して、ユーザーに開かれるアクティブなセッションの数を制御します。推奨値は **1** です。これにより、開かれるセッションの数が減ります (数が多いほど、セッションがハイジャックされる可能性が高くなります)。

詳細情報

属性	説明
構成名	*glide.authenticate.max.concurrent.interactive.sessions*
構成タイプ	システムプロパティ (/sys_properties_list.do)
データタイプ	整数
推奨値	1
デフォルト値	1
カテゴリ	セッション管理

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

属性	説明
セキュリティリスク	• 重大度スコア：3.7 • CVSS スコア：低 • セキュリティリスクの詳細： プロパティのデフォルト値を 1 より大きく設定すると、セッションハイジャックの可能性が高まります。
依存関係と前提条件	**Concurrent Interactive Sessions** (*com.glide.limit.concurrent.sessions*) プラグインがアクティブになっている必要があります。
参照	同時セッションの制限

セッションアクティビティのタイムアウト期間を最小化する

glide.ui.session_timeout プロパティを使用して、アクティビティのタイムアウト値を分単位で指定します。

このプロパティを設定すると、機能にいくつかの影響が生じます。

- 指定されたセッションタイムアウトが長いほど、セッションの処理中に使用されるメモリ量が多くなります。ベースシステムでは、デフォルトの Apache Tomcat タイムアウト時間の 30 分を使用します。
- Now Platform は [記憶する] によってもユーザーをログアウトします。アプリケーションで 30 分間操作がなかった場合、ログインページの [記憶する] チェックボックスがオンになっていないかぎり、プラットフォームはユーザーを自動的にログアウトします。違いは、再度ログインして続行することがないことです。
- ユーザーのホームページに自動的に更新されるゲージまたはコンテンツがある場合は、このタイムアウト値に一度も達しない可能性があります。

詳細情報

属性	説明
プロパティ名	*glide.ui.session_timeout*
構成タイプ	システムプロパティ (/sys_properties_list.do)
カテゴリ	セッション管理
目的	セッションタイムアウトを適用すること
推奨値	ユーザー指定のタイムアウト (分)。推奨値は 60 分ですが、この値は機能とセキュリティ要件によって異なる場合があります。この値の設定は 1 日を超えないようにしてください。
セキュリティリスク評価	7.5
機能への影響度	(中) この修正では、ユーザーアカウントのタイムリーな有効期限が適用されます。機能への影響はありませんが、ユーザーエクスペリエンスは変わります。
セキュリティリスク	(高) 無期限にアクティブであるユーザーセッションはセキュリティリスクです。時間ベースの設定で期限切れにする必要があります。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

属性	説明
参照	ユーザーセッションの管理

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

セッションウィンドウのタイムアウト期間の最小化

glide.ui.user_cookie.life_span_in_days プロパティを使用して、「記憶する」Cookie の有効期限を設定します。デフォルト値は 15 日で、上限は 30 日です。

詳細情報

属性	説明
プロパティ名	*glide.ui.user_cookie.life_span_in_days*
構成タイプ	システムプロパティ (/sys_properties_list.do)
カテゴリ	セッション管理
目的	「記憶する」Cookie のデフォルトの有効期限を有効にすること
推奨値	ユーザー定義の整数値 (日数) [例：15]
セキュリティリスク評価	4.9
機能への影響度	(中) エンドユーザーがログインページから [記憶する] チェックボックスをオンにして Now Platform にログインすると、このプロパティが有効になります。
セキュリティリスク	(中) ユーザーの Cookie が無期限にアクティブになるとセキュリティリスクが発生するため、時間ベースの構成で期限が切れるようにする必要があります。
参照	利用可能なシステムプロパティ [記憶する] チェックボックスと cookie の設定を変更する

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

保存された暗号化

このカテゴリは、保存されたデータの暗号化に焦点を当てています。これには、確立されたアルゴリズムと暗号化モジュールの採用、疑似ランダム値の適切な生成、データ分類に基づく暗号化の実装、キーマテリアルの安全な保存と分離など、いくつかの重要な側面が含まれます。

Glide KMF エンクリプターを有効にする **[Security Center 1.3.2** で削除]

インスタンスの Password2 フィールドに使用するエンクリプターを管理します。

glide.kmf.encrypter.enabled プロパティを使用して、KMF エンクリプターを Password2 フィールドのデフォルトのエンクリプターとして設定します。このプロパティにより、従来のエンクリプターではなく、強力で規制に準拠した暗号化標準を確実に使用することができます。従来のエンクリプターの代わりに KMF エンクリプターが使用されるようにするには、このプロパティを **true** に設定します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

詳細情報

属性	説明
構成名	*glide.kmf.encrypter.enabled*
構成タイプ	システムプロパティ (/sys_properties_list.do)
データタイプ	ブーリアン
推奨値	true
デフォルト値	false
カテゴリ	保存された暗号化
セキュリティリスク	• 重大度スコア：4.9 • CVSS スコア：中 • セキュリティリスクの詳細：このプロパティを **true** に設定すると、従来のエンクリプターの代わりに KMF エンクリプターが使用されます。
依存関係と前提条件	なし
参照	Key Management Framework (KMF) による Password2 暗号化

検証、サニタイズ、およびエンコーディング

検証、サニタイズ、およびエンコーディングは、クロスサイトスクリプティング (XSS)、SQL インジェクション、その他の攻撃などに対する脆弱性を防ぐために入力の検証を実施します。

このコントロールでは、入力の検証と出力のエンコーディングが行われ、出力データのエンコーディングやエスケープなどが正しく構成されていることを確認できます。このカテゴリには、オブジェクトの逆シリアル化、必要な場合のサンドボックス化、許可リストによる積極的な検証などのアイテムのチェックも含まれます。

GlideSystemUserSession スクリプト可能 API へのアクセスを制限する

クライアントコール可能な GlideSystemUserSessionSandbox スクリプト可能 API は、GlideSystemUserSession の addErrorMessageNoSainitization メソッドと addInfoMessageNoSainitization メソッドを javascript サンドボックスに公開しています。これにより、すべてのユーザーがスクリプトを介してこのメソッドをコールできます。

true に設定すると、サンドボックス化されたユーザーセッションで、サニタイズなしで情報メッセージやエラーメッセージをコールすることができます。メッセージが呼び出されると、警告がログに記録されます。 **false** に設定すると、コールは許可されません。

⚠ 警告:
これはセーフハーバープロパティです。つまり、いったん変更したら変えることはできません。元に戻すことはできません。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

詳細情報

属性	説明
プロパティ名	*glide.sandbox.usersession.allow_unsanitized_messages*
構成タイプ	システムプロパティ (/sys_properties_list.do)
カテゴリ	アクセス制御
目的	このプロパティにより、サンドボックス化されたユーザーセッションでの、サニタイズされていない情報メッセージまたはエラーメッセージのコールが制限されます。
タイプ	true | false boolean
推奨値	false
セキュリティリスク評価	8.1
機能への影響度	(高) プロパティの値を false に設定すると、これらの関数が呼び出された場合にメッセージが作成されず、ログも記録されません。
セキュリティリスク	(高) 適切にサニタイズされないと、危険性のあるコンテンツにアクセスする可能性があり、サニタイズされていないエラー関数がスクリプトで使用可能になります。
参照	アクセス制御

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

埋め込み HTML で JavaScript タグを無効にする

glide.ui.security.codetag.allow_script プロパティを使用して、[code] タグを使用して作成された HTML JavaScript コードの埋め込みサポートを無効にします。

Now Platform は、エスケープおよびエンコード技術を実装することで、多くのインジェクション攻撃とクロスサイト攻撃を軽減します。その結果、ユーザーはジャーナルフィールドに対して HTML 形式の入力を書き込んで送信することができなくなります。しかしジャーナルフィールドでは、コードタグで囲まれたテキストを HTML としてレンダリングできます。プロパティが *glide.ui.security.codetag.allow_script* sys_propertiesテーブルに存在し、false に設定されていることを確認します。

- ただし、関連するセキュリティリスクがあります。**true** に設定すると、悪意のあるユーザーは、ジャーナルフィールドをレンダリングした後に、別のクライアントブラウザーで実行できる有害な HTML JavaScript コードを書き込むことができます。
- このプロパティを **false** に設定すると、[code] タグのサポートを無効にすることで、ジャーナルフィールドで HTML JavaScript コードがレンダリングされないようにすることができます。

⚠ 警告:
これはセーフハーバープロパティです。つまり、いったん変更したら変えることはできません。元に戻すことはできません。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

詳細情報

属性	説明
プロパティ名	*glide.ui.security.codetag.allow_script*
構成タイプ	システムプロパティ (/sys_properties_list.do)
カテゴリ	検証、サニタイズ、およびエンコーディング
目的	クロスサイトスクリプティングと悪意のあるスクリプトの実行からの保護
推奨値	false
セキュリティリスク評価	8.8
機能への影響度	(中) この修正では、UI で強制的に JavaScript エスケープが行われ、エンコードされた結果がユーザーに対してレンダリングされます。これは、結果のデータを用いたインスタンスのユーザーインタラクションに基づいて、機能に影響を与える可能性があります。
セキュリティリスク	(高) クロスサイトスクリプティング攻撃から防御するために、アプリケーションで入力検証を行う必要があります。これらの攻撃により、ログインしているブラウザーのコンテキストで、ユーザーセッションで外部スクリプトが実行される可能性があります。攻撃者はこれを使用してセッション情報と機密データを盗むことができます。
参照	ジャーナルフィールドの CODE タグを制限する ジャーナルフィールドエントリを HTML としてレンダリングする 高セキュリティ設定

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

強化された **Java** セキュリティマネージャーの有効化

glide.security.manager プロパティには、現行の Java セキュリティマネージャーの Java クラス名が含まれています。

警告:
これはセーフハーバープロパティです。つまり、いったん変更したら変えることはできません。元に戻すことはできません。

詳細情報

属性	説明
構成名	*glide.security.manager*
構成タイプ	システムプロパティ (/sys_properties_list.do)
データタイプ	文字列

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

属性	説明
推奨値	*com.glide.sys.security.ContextualSecurityManager*
デフォルト値	*com.glide.sys.security.ContextualSecurityManager*
カテゴリ	検証、サニタイズ、およびエンコーディング
セキュリティリスク	• 重大度スコア：7.2 • CVSS スコア：高 • セキュリティリスクの詳細：*glide.security.manager* が推奨値の *com.glide.sys.security.ContextualSecurityManager* に設定されていない場合、インスタンスは、予想されるハードニングポリシーのない古い Java セキュリティマネージャーを使用している可能性があります。この強化を行わないと、スクリプト実行アクセス権を持つ悪意のある攻撃者が、インスタンスでリモートでコードが実行される可能性があります。
依存関係と前提条件	なし

HTML サニタイゼーションを強制する

com.glide.security.check_unsanitized_html プロパティを使用して、フィールドアサインのためにグローバルレベルで translated_html フィールドのサニタイズ動作を適用します。

HTML は、辞書フィールドに割り当てることができるタイプの一種です。HTML フィールドを任意のフィールドタイプに割り当てると、HTML タグ (<p>、<a href>、<b>、<font>、<img> など) を使用してコンテンツをフォーマットできるようになります。悪意のあるアクティビティを防ぐために、ブロックリストを使用して特定の HTML タグを禁止することができます。このプロパティは、インスタンスの translated_html フィールドで禁止タグが使用されないようにします。

- このプロパティを **enforce** に設定すると、translated_html フィールドのサニタイズ動作が適用されます。
- プロパティを **disable** に設定すると、html のサニタイズがオフになり、translated_html フィールドでブロックされた html タグが許可されます。

⚠ 警告:
これはセーフハーバープロパティです。つまり、いったん変更したら変えることはできません。元に戻すことはできません。

詳細情報

属性	説明
プロパティ名	*com.glide.security.check_unsanitized_html*
構成タイプ	システムプロパティ (/sys_properties_list.do)
カテゴリ	検証、サニタイズ、およびエンコーディング
目的	クロスサイトスクリプティングなどの攻撃から保護するために、安全でない HTML タグの使用を防止すること
タイプ	文字列

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

属性	説明
推奨値	*enforce*
セキュリティリスク評価	7.3
機能への影響度	(中) この修正では、UI で強制的に HTML サニタイズが行われ、翻訳された html フィールドがユーザーに対してレンダリングされます。読みやすさと書式設定に影響を与える可能性があります。
セキュリティリスク	(高) クロスサイトスクリプティング攻撃から防御するために、アプリケーションで入力検証を行う必要があります。これらの攻撃により、ログインしているブラウザーのコンテキストで、ユーザーセッションで外部スクリプトが実行される可能性があります。攻撃者はこれを使用してセッション情報と機密データを盗むことができます。
参照	HTML サニタイザー

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

クライアント生成スクリプトサンドボックスを強制

glide.script.use.sandbox プロパティを使用して、スクリプトサンドボックスを有効にします。

Now Platform には、クライアントが評価のためにサーバーにスクリプトを送信できるケースが 2 つあります。

フィルターまたはクエリー

: assigned_to=JavaScript:getMyGroups() などのフィルターをサーバーに送信することは合法です。

システム API

: API 呼び出しにより、クライアントはサーバー上で任意のスクリプトを実行して、応答を受信することができます。

スクリプトサンドボックスを有効にすると、これらの 2 つのエントリポイントのいずれかで評価されるスクリプトが、次の特性を持つ権限の低いサンドボックス内で実行されます。

- サンドボックス内では、クライアントコール可能とマークされたビジネスルールのみを使用できます。
- サンドボックス内では、クライアントコール可能とマークされたスクリプトインクルードのみ使用できます。
- 特定の API 呼び出し (直接 DB アクセスを扱うものに概ね限定) は許可されていません。
- サンドボックス内部からデータを挿入、更新、または削除することはできません。たとえば、current.update() の呼び出しはすべて無視されます。スクリプトサンドボックスを有効にせずに Now Platform を実行する場合、これらの制限は適用されません。

警告:
これはセーフハーバープロパティです。つまり、いったん変更したら変えることはできません。元に戻すことはできません。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

詳細情報

属性	説明
プロパティ名	*glide.script.use.sandbox*
構成タイプ	システムプロパティ (/sys_properties_list.do)
カテゴリ	検証、サニタイズ、およびエンコーディング
目的	プラットフォームに対して起動されるクライアント側 JavaScript クエリーの検証を適用すること
推奨値	true
セキュリティリスク評価	9.8
機能への影響度	(重大) この修正では、Now Platform に対して起動されるクライアント側 JavaScript クエリーの検証が適用されます。顧客が CRUD 操作を実行するためにハードコードされた JavaScript クエリーを組み込んだカスタマイズを行っている場合、潜在的な影響があります。
セキュリティリスク	(重大) Now Platform は JavaScript クエリーを介してさまざまな機能を提供します。ただし、適切な承認と検証がないと、攻撃者がプラットフォームに対して不正な操作を実行する可能性があります。
参照	スクリプトサンドボックスプロパティの構成 *glide.script.use.sandbox* は、クライアントからのスクリプトの実行を保護および制限するプロパティと同じファミリーに属します。 • *glide.script.allow.ajaxevaluate*：「AJAXEvaluate を有効にする」を参照 • *glide.script.secure.ajaxgliderecord*：「AJAXGlideRecord ACL チェックの有効化」を参照

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

受信メールの画像を添付ファイルに変換

glide.email.inbound.convert_html_inline_attachment_references プロパティを使用して、メール画像がメール HTML 本文のプレビューに表示されるように受信メール HTML を変換するかどうかを指定します。

glide.email.inbound.convert_html_inline_attachment_reference システムプロパティが false に設定されている場合は、次のように動作します。

- Now Platform で、受信した画像の代わりに破損した cid (コンテンツ ID) リンクが表示されます。メール画像の表示形式は、現在のプロパティ設定ではなく、メールを受信した時点でのプロパティ設定によって異なります。
- 添付ファイルで受信した「悪意のある」コンテンツがメールの HTML で参照されません。添付ファイル自体は [sys_attachment] テーブルに保存されます。
- 受信メール処理で、sys_attachment テーブル内の添付ファイルの保存場所を反映してメールの HTML データが更新されません。その結果、次のように動作します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- インライン画像がアクティビティフォーマッターのメールに表示されない。

  > **注:**
  > アクティビティフォーマッターを使用してこの問題を解決するには、最初にセキュリティ上の懸念がないかどうかを確認してください。次に、*glide.email.inbound.convert_html_inline_attachment_reference* システムプロパティを **true** に設定して、今後受信するメールに、画像の参照に必要な HTML URL を含めるようにしてください。このプロパティを変更しても、既に受信したメールは更新されません。新しい値はプロパティの変更後に受信した受信メールにのみ影響します。

- メールの HTML プレビューでメールを表示するとインライン画像が表示されない。
- コードタグ間の受信アクションで email.body_htm を追加すると、画像が欠落する。

必須条件

このプロパティを設定する前に、*glide.email.read.active* プロパティを true に設定します。詳細については、Enable using your own POP3 server を参照してください。

詳細情報

属性	説明
プロパティ名	*glide.email.inbound.convert_html_inline_attachment_refere*
構成タイプ	システムプロパティ (/sys_properties_list.do)
カテゴリ	検証、サニタイズ、およびエンコーディング
目的	HTML 本文のプレビューでの画像のレンダリングを制限すること
推奨値	false
セキュリティリスク評価	5.4
機能への影響度	(中) このプロパティが設定されると、ユーザーはメール本文の画像プレビューを表示できません。
セキュリティリスク	(中) このプロパティが有効になっていない場合、攻撃者はマルウェアを含む悪意のある画像を送信する可能性があります。
参照	Email properties Inbound mail configuration

システムプロパティの追加または作成に関する詳細については、「Add a system property」を参照してください。

AJAXEvaluate を無効にする

glide.script.allow.ajaxevaluate を使用して、AJAX 呼び出しによるクライアントスクリプト実行の脆弱性からシステム API を保護します。

プロパティを編集するには、security_admin ロールへの昇格が必要です。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

⚠ 警告:
これはセーフハーバープロパティです。つまり、いったん変更したら変えることはできません。元に戻すことはできません。

詳細情報

属性	説明
プロパティ名	*glide.script.allow.ajaxevaluate*
構成タイプ	システムプロパティ (/sys_properties_list.do)
カテゴリ	検証、サニタイズ、およびエンコーディング
目的	ユーザーが管理者権限でスクリプトを実行できないようにする。
推奨値	False
構成タイプ	ブーリアン
機能への影響度	(中) この修正では、AJAXEvaluate プロセッサーが強制的にオフになります。カスタマイズされたスクリプトの一部として AJAX 評価プロセッサーを明示的に使用している場合は、機能に影響を与える可能性があります。
セキュリティリスク	(高) AjaxEvaluator プロセッサーはサンドボックスでクライアントスクリプトを実行しますが、サンドボックス内のアクティビティのスコープを拡張したり、完全にオフにしたりすることができるいくつかの追加のプロパティがあります。
セキュリティリスク評価	7.3
参照	このプロパティは、クライアントからのスクリプトの実行を保護および制限するプロパティと同じファミリーに属します。 • *glide.script.use.sandbox*：「クライアント生成スクリプトサンドボックス」を参照 • *glide.script.allow.ajaxevaluate*：「AJAXEvaluate を有効にする」を参照

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

エンティティ拡張の無効化

カスタマイズでエンティティの拡張が必要ない場合は、*glide.stax.allow_entity_resolution* プロパティを使用して外部エンティティの拡張を完全に無効化します。XML は解析を完了しますが、内部または外部エンティティは含まれません。

- このプロパティを **true** に設定すると、*glide.stax.whitelist_enabled* プロパティの設定に従って、すべての外部エンティティが対象エンティティを解決または拡張しようとします。
- このプロパティを **false** に設定すると、すべてのエンティティの解決と拡張がブロックされます。詳細については、「ホワイトリストによる XMLdoc2 エンティティ検証」を参照してください。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

必須条件

このプロパティを設定する前に、次の手順を実行してください。

- *glide.xml.entity.whitelist.enabled* および *glide.stax.whitelist_enabled* プロパティを true に設定します。詳細については、「ホワイトリストによる XMLdoc/XMLUtil エンティティ検証」および「ホワイトリストによる XMLdoc2 エンティティ検証」を参照してください。
- *glide.xml.entity.whitelist* プロパティでカンマ区切りの FQDN リストを定義してください。XML エンティティ処理を使用してアクセスできるのは、これらの URL のみになります。詳細については、「XML 外部エンティティ処理 - ホワイトリスト」を参照してください。

⚠ 警告:
これはセーフハーバープロパティです。つまり、いったん変更したら変えることはできません。元に戻すことはできません。

詳細情報

属性	説明
プロパティ名	*glide.stax.allow_entity_resolution*
構成タイプ	システムプロパティ (/sys_properties_list.do)
カテゴリ	認証
目的	この修復コントロールは、XML エンティティ拡張/Billion Laugh 攻撃から防御するために有効にする必要があります。
推奨値	false
機能への影響度	(低) カスタマイズでエンティティ拡張を使用している場合、Now Platform が以降の処理をブロックする可能性があります。
セキュリティリスク	(重大) 攻撃者はこの脆弱性を利用してデータを指数関数的に拡張し、すべてのシステムリソースを短時間で消費する可能性があります。
ワークアラウンド	カスタマイズでエンティティ拡張が必要な場合は、このプロパティを true に設定し、「ホワイトリストによる XMLdoc2 エンティティ検証」に記載されている手順を実行してください。

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

OWASp リソースの詳細については、「OWASp」を参照してください。

外部コンテンツ URL の無効化

Connect チャットを使用して、インスタンスでの外部リンクメタデータの使用方法を管理します。

glide.ui.url.external.content プロパティを使用して、インスタンス内の外部リンクメタデータを管理します。プロパティが推奨値の **false** に設定されている場合、外部リンクメタデータは表示されません。**true** に設定されている場合、Connect Chat は、YouTube やニュース記事などのソースから外部リンクメタデータを取得し、よりリッチなメッセージが表示されます。これにより、サーバーサイドリクエストフォージェリ (SSRF) 攻撃が発生する可能性があります。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

詳細情報

属性	説明
構成名	*glide.ui.url.external.content*
構成タイプ	システムプロパティ (/sys_properties_list.do)
データタイプ	ブーリアン
推奨値	false
デフォルト値	true
カテゴリ	検証、サニタイズ、およびエンコーディング
セキュリティリスク	• 重大度スコア：8.1 • CVSS スコア：高 • セキュリティリスクの詳細：このプロパティを **true** に設定すると、インスタンスがサーバーサイドリクエストフォージェリ (SSRF) 攻撃にさらされる可能性があります。
依存関係と前提条件	なし
参照	Connect Chat

ダウンロード可能な **MIME** タイプを制限する

glide.ui.attachment.download_mime_types プロパティは、指定された危険なファイルタイプのリストのファイルを強制的にクライアントにダウンロードし、ブラウザーにインラインで表示しないようにします。

ファイルの MIME タイプが *glide.ui.attachment.download_mime_types* に存在する場合、ダウンロードが強制されます。たとえば、text/html をダウンロードすると、HTML ファイルはブラウザーでインライン表示されるのではなく、ファイルとしてクライアントに強制的にダウンロードされ、XSS 攻撃を防ぐことができます。

既存の MIME タイプのリストを表示するには、「/sys_attachment_icon_rule_list.do」と入力します。これらの MIME タイプのいずれかを有効にして、Now Platform 内のセキュリティコンプライアンス要件を満たすことができます。

注:
プロパティを編集するには、security_admin ロールが必要です。

詳細情報

属性	説明
プロパティ名	*glide.ui.attachment.download_mime_types*
構成タイプ	システムプロパティ (/sys_properties_list.do)
カテゴリ	検証、サニタイズ、およびエンコーディング
目的	ブラウザーで表示できない危険なファイルタイプのリストを適切に管理すると、クロスサイトスクリプティング攻撃 (XSS) を防ぐことができます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

属性	説明
推奨値	適用可能な MIME タイプのリストまたはデフォルト：text/html,image/svg,image/svg+xml,application/xml
構成タイプ	文字列：アプリケーション MIME タイプのカンマ区切り値。
機能への影響度	(低) この修正では、Now Platform アプリケーションで添付ファイルをクリックしたときに、アクションを実行する前に検証チェックを適用します。潜在的な影響はありませんが、ユーザーエクスペリエンスが変わります。
セキュリティリスク	(中) 攻撃者は MIME タイプを悪用し、意図しないスクリプトコンテンツを被害者側の添付ファイルに配置して機密情報を取得することができます。XSS 機能により、管理者などの上位ロールへの権限の昇格が容易になり、横方向の移動を実行しやすくなります。 現在のコンテキストでは、添付ファイル MIME タイプの中でブラウザーでインラインレンダリングしてはいけないものを、カンマ区切りのリストの形式でプロパティに入力します。
セキュリティリスク評価	6.3
関連プロパティ	• *glide.ui.attachment.force_download_all_mime_types* • *glide.ui.attachment.tables_ignore_force_download*
参照	MIME タイプのダウンロードを強制する。

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

制限付きダウンロード可能な **MIME** タイプを定義する

glide.ui.attachment.force_download_all_mime_types プロパティを使用して MIME タイプをダウンロードし、ブラウザーでインライン表示しないようにします。

たとえば、text/html をダウンロードすると、HTML ファイルはブラウザーでインライン表示されるのではなく、ファイルとしてクライアントに強制的にダウンロードされ、XSS 攻撃を防ぐことができます。

既存の MIME タイプのリストを表示するには、「/sys_attachment_icon_rule_list.do」と入力します。これらの MIME タイプのいずれかを有効にして、Now Platform 内のセキュリティコンプライアンス要件を満たすことができます。

詳細情報

属性	説明
プロパティ名	*glide.ui.attachment.force_download_all_mime_types*
構成タイプ	システムプロパティ (/sys_properties_list.do)
カテゴリ	検証、サニタイズ、およびエンコーディング

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

属性	説明
目的	ファイルタイプがブラウザーでレンダリングされないように制限し、悪意のあるスクリプトの実行を回避すること
CVSS 評価	8
推奨値	true
機能への影響度	(低) この修正では、Now Platform アプリケーションで添付ファイルをクリックしたときに、アクションを実行する前に検証チェックを適用します。潜在的な影響はありませんが、ユーザーエクスペリエンスが変わります。
セキュリティリスク	(高) クライアント側のスクリプティング攻撃ベクトルにはさまざまな種類があり、MIME タイプの添付ファイルの悪用も例外ではありません。 攻撃者は MIME タイプを悪用し、意図しないスクリプトコンテンツを被害者側の添付ファイルに配置して機密情報を取得することができます。XSS 機能により、管理者などの上位ロールへの権限の昇格が容易になり、横方向の移動を実行しやすくなります。 現在のコンテキストでは、添付ファイル MIME タイプの中でブラウザーでインラインレンダリングしてはいけないものを、カンマ区切りのリストの形式でプロパティに入力します。 例：text/html、text/csv
関連リンク	MIME タイプのダウンロードを強制する。

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

埋め込み HTML コードを無効にする

glide.ui.security.allow_codetag プロパティを使用して、[code] タグを使用して作成された HTML コードの埋め込みサポートを無効にします。

Now Platform は、エスケープおよびエンコード技術を実装することで、多くのインジェクション攻撃とクロスサイト攻撃を軽減します。その結果、ユーザーはジャーナルフィールドに対して HTML 形式の入力の書き込みや送信ができなくなります。しかしジャーナルフィールドでは、コードタグで囲まれたテキストを HTML としてレンダリングできます。

- ただし、関連するセキュリティリスクがあります。true に設定すると、悪意のあるユーザーは、ジャーナルフィールドをレンダリングした後に、別のクライアントブラウザーで実行できる有害な HTML JS コードを書き込むことができます。
- このプロパティを false に設定すると、[code] タグのサポートを無効にすることで、ジャーナルフィールドで HTML コードがレンダリングされないようにすることができます。

詳細情報

属性	説明
プロパティ名	glide.ui.security.allow_codetag
構成タイプ	システムプロパティ (/sys_properties_list.do)

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

属性	説明
カテゴリ	検証、サニタイズ、およびエンコーディング
Instance Security Center での構成	あり
目的	クロスサイトスクリプティングと悪意のあるスクリプトの実行からの保護
推奨値	false
セキュリティリスク評価	4.2
機能への影響度	(中) この修正では、UI で強制的に HTML エンコードが行われ、エンコードされた結果がユーザーに対してレンダリングされます。 このプロパティはデフォルトで [true] に設定されています。このステータスでは、インスタンスはジャーナルフィールドとフォームにレンダリングされた HTML を表示します。 このプロパティを falseに設定すると、HTML が正しくレンダリングされず、フォームのジャーナルフィールドに HTML タグが表示される場合があります。これは、機能に悪影響を及ぼし、結果のデータを用いたユーザーインタラクションに悪影響を与える可能性があります。
セキュリティリスク	(中) クロスサイトスクリプティング攻撃から防御するために、アプリケーションで入力検証を行う必要があります。これらの攻撃により、ログインしているブラウザーのコンテキストで、ユーザーセッションで外部スクリプトが実行される可能性があります。攻撃者はこれを使用してセッション情報と機密データを盗むことができます。

仮想エージェント内で **HTML** サニタイザーを有効化する

com.glide.cs.html.sanitizer.enabled プロパティを使用して HTML SanitizerService を有効にします。

詳細情報

警告:
これはセーフハーバープロパティです。つまり、いったん変更したら変えることはできません。元に戻すことはできません。

属性	説明
プロパティ名	*com.glide.cs.html.sanitizer.enabled*
構成タイプ	システムプロパティ (/sys_properties_list.do)
カテゴリ	検証、サニタイズ、およびエンコーディング
目的	アプリケーションでクロスサイトスクリプティング攻撃および HTML インジェクション攻撃を防ぐこと。
推奨値	true
セキュリティリスク評価	8

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

属性	説明
機能への影響度	(高) この修正では、ユーザーデータがユーザーにレンダリングされる前に、HTML 出力エンコードメカニズムが適用されます。顧客が HTML 属性またはコンテンツデータのレンダリングを伴うカスタマイズを行っている場合は、機能に影響があります。
セキュリティリスク	(高) データがアプリケーションに格納および処理されるときに、ユーザー入力を安全に処理する必要があります。これにより、データの出力エンコードによるクライアント側のクロスサイトスクリプティング攻撃が低減されます。

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

Jelly JS 補間保護を有効にする

glide.ui.jelly.js_interpolation.protect プロパティを使用して、Jelly ページで実行しようとしているすべての JavaScript が Jelly 補間を使用したインジェクションから確実に保護されるようにします。

プロパティを **true** に設定すると、アプリケーションは (ネストされた) Jelly スクリプトツリーを経由します。潜在的に危険な Jelly 式は、次を実行するフィルターでラップされます。

- 結果をエスケープして安全にします。または、
- 安全性を保証できない場合は SecurityException を生成します。これは、評価される予定の式がセキュリティ上の問題を示している可能性があるためです。

> ⚠ **警告:**
> これはセーフハーバープロパティです。つまり、いったん変更したら変えることはできません。元に戻すことはできません。

詳細情報

属性	説明
プロパティ名	*glide.ui.jelly.js_interpolation.protect*
構成タイプ	システムプロパティ (/sys_properties_list.do)
カテゴリ	検証、サニタイズ、およびエンコーディング
目的	Jelly インジェクションを使用すると発生する可能性がある、悪意のあるコードの実行攻撃を軽減すること
推奨値	true
セキュリティリスク評価	9
機能への影響度	(高) このプロパティは、式が引用符で囲まれているかどうかについて最適な推測を行います。正当な式に誤って引用符を付ける可能性があります。その場合、手動で式に安全とマークする必要がある場合があります。
セキュリティリスク	(中) JEXL インジェクションは、Now Platform に固有の入力インジェクションの形式です。これにより、クロスサイト要求の偽造とコード実行の両方が発生する可能性があります。保護を完全にオフにすると、多くの P1 セキュリティ脆弱性がオープンになるおそれがあります。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

属性	説明
ワークアラウンド	手動で式に安全とマークするには、SAFE というプリフィックスを Jelly 式に追加します。 ${SAFE:sysparm_input}; すべての式に機械的に SAFE を追加するという方法は、セキュリティの脆弱性をオープンにするおそれがあるため、問題へのアプローチとしては不適切です。 • 式に SAFE を追加するのは、式にクライアントからの入力が含まれていないことが保証できる場合に限ってください。 • 含まれている場合、悪意のあるクライアントによって特権 JavaScript が評価される可能性があります。
参照	Jelly のタグ 高セキュリティ設定

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

入れ子になった式での **Jelly JS** 補間保護の有効化

インスタンスの補間保護を管理します。

glide.ui.jelly.js_interpolation.protect_nested_expressions プロパティを使用して、補間保護を管理します。補間保護により、JavaScript で Jelly 式を使用する場合、特定のカテゴリに該当するか、式自体で SAFE とマークすることによって、Jelly 式を必ず安全と見なすことができます。この軽減策が有効になっていない場合、攻撃者が GET パラメーターを Jelly ページに送信し、そのパラメーターのコンテンツが管理者権限を持つサーバー側の JavaScript として評価される可能性があります。このプロパティが推奨値の **true** に設定されていない場合、JavaScript で補間された悪意のある Jelly 式が許可され、ユーザーは Jelly テンプレートを使用してコードを実行できます。

> ⚠ **警告:**
> これはセーフハーバープロパティです。つまり、いったん変更したら変えることはできません。元に戻すことはできません。

詳細情報

属性	説明
構成名	*glide.ui.jelly.js_interpolation.protect_nested_expressions*
構成タイプ	システムプロパティ (/sys_properties_list.do)
データタイプ	ブーリアン
推奨値	true
デフォルト値	false
カテゴリ	検証、サニタイズ、およびエンコーディング

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

属性	説明
セキュリティリスク	• 重大度スコア：9 • CVSS スコア：重大 • セキュリティリスクの詳細：プロパティが **false** に設定されている場合、悪意のある Jelly 式が許可されます。
依存関係と前提条件	なし

相対リンクを強制する

glide.cms.catalog_uri_relative プロパティを使用して、/ess/catalog.do の URL パラメーターからの相対リンクを適用します。

- **true** に設定されている場合、*uri* パラメーターを使用して、/ess/catalog.do ページから相対 URL のみが許可されます。
- **false** に設定すると、すべての URL が許可され、外部の未承認コンテンツへのリンクが許可される可能性があります。

詳細情報

属性	説明
プロパティ名	*glide.cms.catalog_uri_relative*
構成タイプ	システムプロパティ (/sys_properties_list.do)
カテゴリ	検証、サニタイズ、およびエンコーディング
目的	外部の未承認コンテンツへのリンクを制限すること
推奨値	true
セキュリティリスク評価	2.6
機能への影響度	(低) この修正では、相対 URL のみが許可されるようにカタログページの検証が適用されます。外部 Web アプリケーションへの既存のリンクが切断されます。
セキュリティリスク	(高) 絶対 URL をパラメーターまたはフィールド値の一部として使用すると、セキュリティリスクが生じる可能性があるため、ソースページは攻撃者が制御する Web サイトにリダイレクトされます。

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

URL 許可リストチェックを強制

glide.security.url.whitelist プロパティを使用して、導入された外部 URL を包含リストの URL に含めるかどうかを確認するために、検証レイヤーを追加します。

オープンリダイレクトは、脆弱な Web ページのリダイレクト先が、ユーザーを危険にさらす可能性がある、信頼できない悪意のあるページである場合に発生します。オープンリダイレクト攻撃にはフィッシング攻撃が伴います。これは、変更された脆弱なリンクが元のサイトと同じであることから、フィッシング攻撃が成功する可能性が高くなるためです。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

このプロパティは、次の場合に適用されます。

- /logout.do?sysparm_goto_url={External URL}
- /cms_login_redirect.do?sysparm_goto_url={External URL}

ユーザーがインスタンスからログアウトすると、外部の信頼できるサイトに誘導されます。

- /logout_redirect.do?sysparm_url={External URL}
- /saml_redirector.do?sysparm_uri={External URL}

SAML を有効にすると、ID プロバイダー (IDP) のログアウト URL が呼び出されます。

詳細情報

属性	説明
プロパティ名	*glide.security.url.whitelist*
構成タイプ	システムプロパティ (/sys_properties_list.do)
カテゴリ	検証、サニタイズ、およびエンコーディング
目的	ログイン、ログアウト、またはその他のリダイレクト時に安全な URL リダイレクトを実装すること。このプロパティは、「未検証のリダイレクトと転送」と呼ばれる OWASP 上位 10 件の攻撃の 1 つを軽減します。
タイプ	文字列
値	組織の承認済み URL [何らかの定義された FQDN (完全修飾ドメイン名) 例：http://www.servicenow.com]
セキュリティリスク評価	8.3
機能への影響度	(中) この修正では、ログアウトページで検証が適用されます。SSO/SAML 構成のインスタンスのユーザーに機能的な影響を与える可能性があります。
セキュリティリスク	(高) クライアント側のオープンリダイレクトにより、攻撃者は、攻撃者が制御する Web サイトに被害者/ユーザーをリダイレクトできるようになります。これはセキュリティリスクと見なされます。
参照	マルチ SSO (SAML 2.0) のエラーと修正

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

Excel 式をエスケープ

glide.export.escape_formulas プロパティを使用して、Excel のインジェクション (式のインジェクションとも呼ばれる) を防止します。

Excel インジェクションは、Web サイトが Excel ファイル内に信頼できないエントリを埋め込むときに発生します。Microsoft Excel や LibreOffice Call などのスプレッドシートアプリケーションを使用してファイルを開くと、+、-、=、または @ で始まるセルは式として解釈されます。*glide.export.escape_formulas* プロパティを **true** に設定すると、CSV、XLS、または XLSX ファイルにエクスポートする際に、+、-、=、または @ で始まる文字列の値には、先頭にアポストロフィが 1 つ追加されます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

詳細情報

属性	説明
プロパティ名	*glide.export.escape_formulas*
構成タイプ	システムプロパティ (/sys_properties_list.do)
カテゴリ	検証、サニタイズ、およびエンコーディング
目的	アプリケーションで Excel インジェクションまたは式のインジェクションを防止すること
推奨値	true
セキュリティリスク評価	6.5
機能への影響度	(低) 悪意で細工された式を使用すると、スプレッドシートソフトウェアの脆弱性を利用してユーザーのコンピューターをハイジャックすることができます。
セキュリティリスク	(中) 悪意のある式は、閲覧者のコンピューターの侵害に使用される可能性があるため、埋め込みスプレッドシートに機密情報が含まれていない場合であってもリスクを引き起こします。
ワークアラウンド	代替手段として、可能な場合はすべての末尾の空白を削除し、クライアントが提供するすべてのデータを英数字のみに制限することを検討してください。
参照	利用可能なシステムプロパティ

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

リストビューで **HTML** をエスケープする

glide.ui.escape_html_list_field プロパティを使用して、リストビューの HTML フィールドで強制的に HTML をエスケープします。

HTML は、辞書フィールドに割り当てることができるタイプの一種です。HTML フィールドを任意のフィールドタイプに割り当てると、HTML コード (<p>、<a href>、<b>、<font>、<img> など) を使用してコンテンツをフォーマットできるようになります。悪意のあるユーザーは、フォームフィールド内に HTML コードを挿入して、さまざまなクライアント/ユーザーセッションで不要なスクリプトを実行できます。

- このプロパティを **false** に設定すると、テーブルがリストビューとして表示されるときに、レコード/フィールドがブラウザーでレンダリングされる前に HTML エスケープが実行されます。
- **true** に設定し、テーブルまたはレコードリストを表示しているときにリストビューでその列を選択すると、これらの HTML 形式のフィールドが表示される場合があります。

警告:
これはセーフハーバープロパティです。つまり、いったん変更したら変えることはできません。元に戻すことはできません。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

詳細情報

属性	説明
プロパティ名	*glide.ui.escape_html_list_field*
構成タイプ	システムプロパティ (/sys_properties_list.do)
カテゴリ	検証、サニタイズ、およびエンコーディング
目的	アプリケーションでクロスサイトスクリプティング攻撃を防ぐこと
推奨値	false
セキュリティリスク評価	8.8
機能への影響度	(中) この修正では、UI で強制的に HTML パーサーレベルの HTML エンコードが行われ、エンコードされた結果がユーザーに対してレンダリングされます。これは、結果のデータを用いたインスタンスのユーザーインタラクションに基づいて、機能に影響を与える可能性があります。
セキュリティリスク	(高) クロスサイトスクリプティング攻撃から防御するために、アプリケーションで入力検証を行う必要があります。これらの攻撃により、ログインしているブラウザーのコンテキストで、ユーザーセッションで外部スクリプトが実行される可能性があります。攻撃者はこれを使用してセッション情報と機密データを盗むことができます。
参照	高セキュリティ設定

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

JavaScript をエスケープする

glide.html.escape_script プロパティを使用して、リストビュー中に HTML フィールドの JavaScript (<script></script>) タグからのエスケープを適用します。

HTML は、辞書フィールドに割り当てることができるタイプの一種です。HTML フィールドを任意のフィールドタイプに割り当てると、ユーザーは HTML コード (<p>、<a href>、<b>、<font>、<img> など) を使用してコンテンツをフォーマットできるようになります。*glide.html.escape_script* を **false** に設定すると、テーブルまたはレコードリストを表示しているときにリストビューでその列を選択すると、(<script></script>) タグが表示される場合があります。

悪意のある攻撃者は、(<script></script>) タグ内に JavaScript コードを埋め込んで挿入できます。攻撃者は、ユーザーがテーブルレコードを開いたときに実行される可能性のある高度な JS ベクトルを挿入して利用することができます。

⚠ 警告:
これはセーフハーバープロパティです。つまり、いったん変更したら変えることはできません。元に戻すことはできません。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

詳細情報

属性	説明
プロパティ名	*glide.html.escape_script*
構成タイプ	システムプロパティ (/sys_properties_list.do)
カテゴリ	検証、サニタイズ、およびエンコーディング
目的	アプリケーションに対するクロスサイトスクリプティング攻撃を防ぐこと
推奨値	true
セキュリティリスク評価	8.8
機能への影響度	(中) この修正では、UI で強制的に JavaScript エスケープが行われ、エンコードされた結果がユーザーに対してレンダリングされます。これは、結果のデータを用いたインスタンスのユーザーインタラクションに基づいて、機能に影響を与える可能性があります。
セキュリティリスク	(高) クロスサイトスクリプティング攻撃から防御するために、アプリケーションで入力検証を行う必要があります。これらの攻撃により、ログインしているブラウザーのコンテキストで、ユーザーセッションで外部スクリプトが実行される可能性があります。攻撃者はこれを使用してセッション情報と機密データを盗むことができます。
参照	利用可能なシステムプロパティ 高セキュリティ設定

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

Jelly スクリプトをエスケープ

glide.ui.escape_all_script プロパティを使用して、Jelly に挿入されたすべてのスクリプトを強制的にエスケープします。

これは、`<j:jelly> ... </j:jelly>` に含まれるすべての JS および HTML 文字列を、出力ストリームに書き込まれる前にエスケープして、いくつかの XSS 問題が発生しないようにします。

詳細情報

属性	説明
プロパティ名	*glide.ui.escape_all_script*
構成タイプ	システムプロパティ (/sys_properties_list.do)
カテゴリ	検証、サニタイズ、およびエンコーディング
目的	プロパティが **true** に設定されていない場合、開発者は XSS の問題を防ぐために、各カスタム Jelly スクリプトでいくつかの手順を実行する必要があります。これらの手順には、Web ページにレンダリングするために出力スト

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

属性	説明
	リームに送信される Jelly 変数の特定と、次の各タグのエスケープが含まれます。 $â {JS:expression} $â {HTML:expression} OR $â {JS,HTML:expression}
推奨値	true
セキュリティリスク評価	7.3
機能への影響度	(中) この修正では、パーサーレベルで Jelly エスケープが適用されます。結果のデータを用いたユーザーインタラクションに機能的な影響を与える可能性があります。
セキュリティリスク	(高) アプリケーションで入力されるすべてのユーザー入力で入力検証を行う必要があります。これにより、プラットフォームに対するインジェクション攻撃を防御および保護できます。
ワークアラウンド	Web ページでのレンダリング用に設計された一部のスクリプトと HTML タグが破損したように見えるため、UI が影響を受ける可能性があります。この修正では、出力エンコードされたページをブラウザーに送信してレンダリングします。 たとえば、<u> タグが適切にエスケープされると、「my string here」ではなく「<u> my string here</u>」と表示されます。この場合、エスケープを防ぐには、NOESC プリフィックスを Jelly 式に追加して JS エスケープを防止します。例： • 変更前：($[jvar_context_menus]); • 変更後：($[NOESC:jvar_context_menus]); • 変更前：$[jvar_ui_policy_scripts] • 変更後：$[NOESC:jvar_ui_policy_scripts]
参照	高セキュリティ設定 Jelly のタグ

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

スクラッチパッド内のスクリプトのエスケープ

スクラッチパッドがインスタンスのセキュリティ体制にどのように影響するか、また悪意のあるスクリプトがそこで実行されないように管理する方法について説明します。

スクラッチパッドは、ブラウザでアクセスできるサーバー上の情報を簡単に設定する方法です。管理者は、任意のレコードを含むスクラッチパッド上のあらゆるものをスクリプト化できます。このプロパティが推奨値の **true** に設定されていない場合、クロスサイトスクリプティングの脆弱性など、悪意のあるスクリプトが実行される可能性があります。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

詳細情報

属性	説明
構成名	*glide.ui.escape_scratchpad*
構成タイプ	システムプロパティ (/sys_properties_list.do)
データタイプ	ブーリアン
推奨値	true
デフォルト値	true
カテゴリ	検証、サニタイズ、およびエンコーディング
セキュリティリスク	• 重大度スコア：6.5 • CVSS スコア：中 • セキュリティリスクの詳細:プロパティが推奨値の **true** に設定されていない場合、クロスサイトスクリプティングの脆弱性などの悪意のあるスクリプトを実行する可能性があります。
依存関係と前提条件	なし
参照	Workflow administration

XML マークアップをエスケープする

glide.ui.escape_text プロパティを使用して、パーサーレベルで XML 値を強制的にエスケープしてから、クライアントのブラウザに送信します。

クロスサイトスクリプティングは、攻撃者が悪意のある JavaScript をエントリポイントに挿入するときに発生します。プラットフォーム/アプリケーションは、被害者のブラウザに送信して実行する前に悪意のある JavaScript をエスケープすることができません。このコンテキストでのエスケープとは、次のことを意味します。

- **&** --> &
- **<** --> <
- **>** --> >
- **"** --> "
- **'** --> '
- **/** --> /

例:<![CDATA[<script>alert('XSS Attack');]]>

エスケープ：<script>alert('XSS Attack');</script>

プロパティが *glide.ui.escape_text* sys_propertiesテーブルに存在し、true に設定されていることを確認します。

警告:
これはセーフハーバープロパティです。つまり、いったん変更したら変えることはできません。元に戻すことはできません。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

詳細情報

属性	説明
プロパティ名	*glide.ui.escape_text*
構成タイプ	システムプロパティ (/sys_properties_list.do)
カテゴリ	検証、サニタイズ、およびエンコーディング
目的	XML をエスケープすることで、信頼できないデータに埋め込まれた悪意のある JavaScript をブラウザが解析して JavaScript として実行することを確実になくします。 • 悪意のあるユーザーが XSS 攻撃を試みて、他のユーザーのセッションをハイジャクするか、ユーザーを悪意のある Web サイトにリダイレクトする可能性があります。 • NOW Platform には cookie を保護するためのコードが含まれていますが、それをエスケープするにはこのプロパティが **true** に設定されている必要があります。
推奨値	true
セキュリティリスク評価	8.8
機能への影響度	(中) この修正では、UI で XML パーサーレベルの XML エンコードが適用されます。これにより、エンコードされた結果がユーザーに対してレンダリングされるので、結果のデータを用いたインスタンスのユーザーインタラクションに基づいて、機能に影響を与える可能性があります。
セキュリティリスク	(高) クロスサイトスクリプティング攻撃から防御するために、アプリケーションで入力検証を行う必要があります。これらの攻撃により、ログインしているブラウザのコンテキストで、ユーザーセッションで外部スクリプトが実行される可能性があります。攻撃者はこれを使用してセッション情報と機密データを盗むことができます。

ワークアラウンド	このプロパティを **true** に設定すると、カタログアイテムの説明またはカタログアイテム変数のヘルプテキストの HTML タグでレンダリングが停止します。フィールドによっては、HTML 形式を使用できない場合があります。
	
	ただし、*glide.ui.escape_text* プロパティをオフにすると、出力エンコーダーにより、すべての JEXL 式にプリフィックスが付加されます。
	
	`${JS:expression}`
	
	`${HTML:expression}`
	
	または
	
	`${JS,HTML:expression}`

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

XML 応答のエスケープ

インスタンスでの XML エスケープの処理方法を管理します。

このプロパティを使用して、XML 応答をエスケープするかどうかを管理します。プロパティが推奨値の **false** に設定されている場合、XML 応答はエスケープされず、XML インジェクション攻撃につながる可能性があります。意図されていない XML コンテンツが XML メッセージに挿入されると、アプリケーションの意図したロジックが変更される可能性があります。

詳細情報

属性	説明
構成名	*glide.soaprequest.unescape_xml_response*
構成タイプ	システムプロパティ (/sys_properties_list.do)
データタイプ	ブーリアン
推奨値	false
デフォルト値	false
カテゴリ	検証、サニタイズ、およびエンコーディング
セキュリティリスク	• 重大度スコア：6.4 • CVSS スコア：中 • セキュリティリスクの詳細：このプロパティを **false** に設定すると、XML エスケープが無効になり、XML インジェクション攻撃につながる可能性があります。
依存関係と前提条件	なし

HTML サニタイザーを有効にする

glide.html.sanitize_all_fields プロパティを使用して、HTMLSainitizer スクリプトインクルードを有効にし、スクリプトで構成された除外リストおよび包含リストの属性に基づいて HTML 入力をサニタイズします。

辞書/フィールドで利用可能なフィールドタイプには、HTML や翻訳された HTML などがあります。これらの HTML 入力フィールドを使用すると、次のような HTML 形式の入力を記述できます。

<h1>Test</h1>)、<img>、<a href …>、<iframe> などの最も基本的な HTML タグを使用

これにより、悪意のある攻撃者が次のような HTML タグを使用して悪意のあるベクトルを挿入する可能性があります。

[<IMG SRC=" &#14; JavaScript:alert('XSS');">][<IMG onmouseover="alert('xss')">],[a href="" onclick=alert(/xss/)]

詳細情報

属性	説明
プロパティ名	*glide.html.sanitize_all_fields*

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

属性	説明
構成タイプ	システムプロパティ (/sys_properties_list.do)
カテゴリ	検証、サニタイズ、およびエンコーディング
目的	アプリケーションでクロスサイトスクリプティング攻撃および HTML インジェクション攻撃を防ぐこと
推奨値	true
セキュリティリスク評価	8.8
機能への影響度	(高) この修正では、ユーザーデータがユーザーにレンダリングされる前に、HTML 出力エンコードメカニズムが適用されます。顧客が HTML 属性またはコンテンツデータのレンダリングを伴うカスタマイズを行っている場合は、機能に影響があります。
セキュリティリスク	(高) データがアプリケーションに格納および処理されるときに、ユーザー入力を安全に処理する必要があります。これにより、データの出力エンコードによるクライアント側のクロスサイトスクリプティング攻撃が低減されます。
ワークアラウンド	このプロパティは、システム内のすべての HTML フィールドをサニタイズします。個々のフィールドで HTML のサニタイズを有効にする必要がある場合は、「個々のフィールドでサニタイズを有効にする」を参照してください。 包含リストまたは除外リストを設定して、組織のポリシーに従って HTML タグと属性をサニタイズすることもできます。
参照	HTML サニタイザーの有効化 HTML サニタイザー

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

許可された **Java** パッケージの制限

これらのプロパティを設定すると、危険な API がスクリプトエンジンに公開されるのを防ぐことができます。

システムテーブルを設定し、それに応じて推奨されるプラグインをインストールします。

sys_whitelist_member および *sys_whitelist_package* テーブルが空の値でない場合、危険な API がスクリプトエンジンに公開される可能性があります。ServiceNow セキュリティチームによって承認されていない Java 名前空間に対応するエントリ。

パッケージコール削除ツールをインストールします。詳細については、「パッケージコール削除ツール」を参照してください。

これらのテーブルを編集するには、カスタマーサービス & サポートにお問い合わせください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

詳細情報

属性	説明
テーブル、プラグイン名	テーブル： • *sys_whitelist_member* • *sys_whitelist_package* プラグイン：com.glide.script.packages_call_removal
構成タイプ	表形式の構成、プラグイン
カテゴリ	検証、サニタイズ、およびエンコーディング
目的	危険な API がスクリプトエンジンに公開されるのを防ぐ。
推奨値	空
構成タイプ	テーブルリスト、プラグイン
機能への影響度	
セキュリティリスク	(高) 危険な API がスクリプトエンジンに公開されるのを防ぎます。これらのサポートされている API は、インスタンス内を不安定にし、セキュリティ上の問題をもたらす可能性があります。
セキュリティリスク評価	8.2

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

パッケージコール削除ツール

Packages Call Removal Tool (*com.glide.script.packages_call_removal*) プラグインをアクティブ化して実行し、提案されたそれぞれの変更を完了するか却下するかを検討します。

Packages Call Removal Tool は、次のようなプラグインです。

- Now Platform Java クラスに対するパッケージコールのスクリプトをスキャンします。
- 優先する GlideScriptable 名に置き換える変更を提案します。
- スクリプトを容易に変更できるようにします。

注:
このレコードがベースシステムレコードの場合、ツールからの推奨事項を使用すると、アイテムは customer_update としてマークされます。ただし、このツールを使用すると、Packages,xxx のコールにフラグが設定されるので今もなお便利です。

このパッケージコール削除ツールは、sa_mapping_ext_commands および sa_custom_operation で使用されるいくつかのパッケージコールを報告する場合があります。これらのパッケージコールは MID Server に属します。クラスがないため、コードは MID Server で実行されます。[エラー] セクションで次に列記するパッケージコールを見つけた場合は、[却下] (無視) としてマークします。ツールは、そのパッケージコールを再度報告しません。

- Packages.com.snc.sw.util.JSONUtil.toJSONPlain(file_content);
- Packages.com.snc.sw.util.JSONUtil.toJSONPlain(file_name);

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

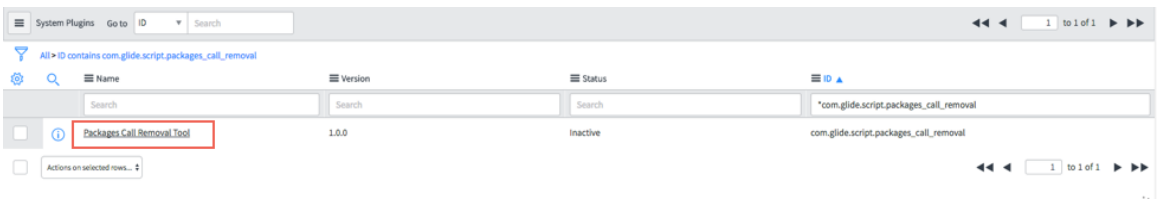
- Packages.com.snc.sw.commands.HttpCallHandler;
- Packages.com.snc.sw.dto.ProviderType.SSH

詳細情報

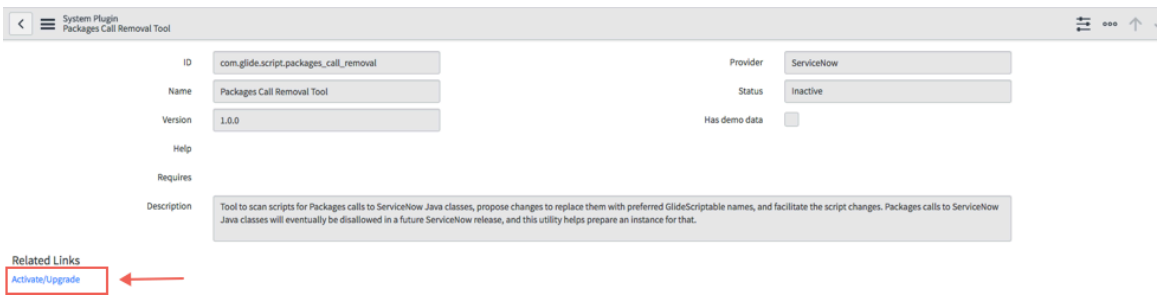
属性	説明
プラグイン名	com.glide.script.packages_call_removal
構成タイプ	[システム定義] > [プラグイン]
目的	承認されたデータアクセスのみを許可する Glide 許容 (GlideScriptable) 名の未承認パッケージ/メンバーコールを削除すること
推奨値	有効
機能への影響度	(低) この修正により、パッケージ呼び出しが `GlideScriptable` API に置き換えられ、パッケージコールを含むカスタマイズに影響を与える可能性があります。このツールは、実際にはパッケージコールを自動的に置き換えるわけではありません。代わりに、packages_call_item テーブルに保存される提案が提供されます。その後、管理者は提案された変更を承認するか却下するかを決定できます。
セキュリティリスク	(中) サーバー上でのデータ取得またはオブジェクトアクセスという結果をもたらすクライアント側 API 呼び出しは、セキュリティの観点から危険であると見なされます。機密オブジェクトへのアクセスを許可および制限するために、検証が必要になります。

設定手順

1. 移動先 システム定義 > プラグイン



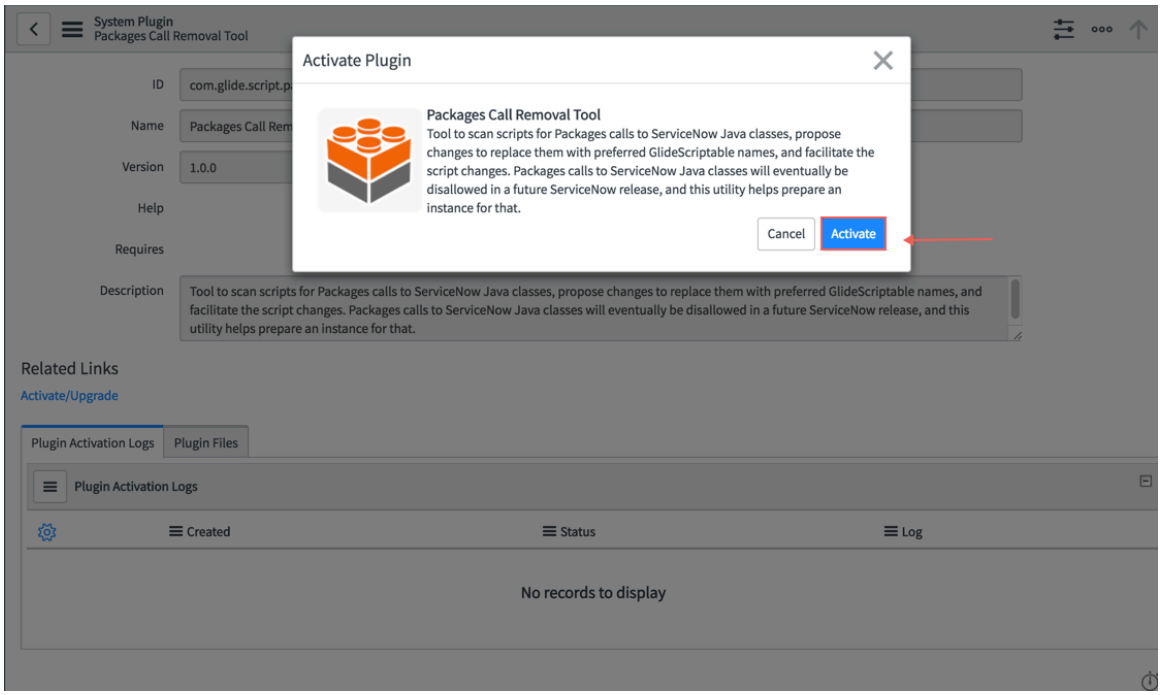
2. プラグイン ID = `com.glide.script.packages_call_removal` を検索します。



3. [アクティブ化/アップグレード **(Activate/Upgrade)]** をクリックしてプラグインをアクティブ化します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



4. 包含リストパッケージコールと包含リストメンバーコールを確認するには、次のトピックの「構成手順」セクションで説明されている手順を完了してください。
   - チェック許可リストメンバーコール
   - チェック許可リストパッケージコール

LDAP 初期識別名の設定解除

このプロパティを使用して、LDAP サーバーレコードの識別名を管理します。

このプロパティは、すぐに利用可能な (OOB) 修正スクリプトの実行時に挿入される LDAP サーバーレコードの識別名をコントロールします。推奨値の "" または空白に設定されている場合は、低い権限のユーザーが LDAP サーバーデータを列挙できます。

詳細情報

属性	説明
構成名	*glide.ldap.initial.dn*
構成タイプ	システムプロパティ (/sys_properties_list.do)
データタイプ	文字列
推奨値	空
デフォルト値	空
カテゴリ	検証、サニタイズ、およびエンコーディング

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

属性	説明
セキュリティリスク	• 重大度スコア：2.7 • CVSS スコア：低 • セキュリティリスクの詳細：プロパティ値を "" または空白に設定すると、権限の低いユーザーが LDAP サーバーデータにアクセスできる可能性があります。
依存関係と前提条件	なし

セッション **Cookie** の厳格なセキュリティを適用する

glide.ui.secure_cookies プロパティを使用して、適切にフォーマットされた Cookie を要求します。

プロパティが true に設定されていると、関連付けられた Cookie が想定される形式でない場合、インスタンスはセッションを拒否します。

警告:
これはセーフハーバープロパティです。つまり、いったん変更したら変えることはできません。元に戻すことはできません。

詳細情報

属性	説明
プロパティ名	*glide.ui.secure_cookies*
構成タイプ	システムプロパティ (/sys_properties_list.do)
カテゴリ	検証、サニタイズ、およびエンコーディング
目的	より安全なセッション認証を実現すること
推奨値	true
セキュリティリスク評価	8.8
機能への影響度	(低) プロパティが true に設定されている場合、不適切な形式の Cookie は却下されます。このような Cookie が却下された場合、ユーザーは再度ログインする必要があります。

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

エンティティ拡張しきい値の最小化

glide.xmlutil.max_entity_expansion プロパティを使用して、エンティティ拡張の上限を小さい数値に変更します。

Now Platform は、このプロパティで指定された許容制限を超えるエンティティ拡張を処理しません。

注:
500 は、によって Now Platform課されるデフォルトの最小値であり、安全なしきい値と見なされます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

詳細情報

属性	説明
プロパティ名	*glide.xmlutil.max_entity_expansion*
構成タイプ	システムプロパティ (/sys_properties_list.do)
カテゴリ	検証、サニタイズ、およびエンコーディング
目的	この修復コントロールは、XML エンティティ拡張/Billion Laugh 攻撃から防御するために有効にする必要があります。
推奨値	3,000
セキュリティリスク評価	5.3
機能への影響度	(低) カスタマイズで大規模なエンティティ拡張を使用している場合、Now Platform が以降の処理をブロックする可能性があります。
セキュリティリスク	(中) 攻撃者はこの脆弱性を利用してデータを指数関数的に拡張し、すべてのシステムリソースを短時間で消費する可能性があります。

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

アップロードされた **MIME** タイプを制限する

glide.security.file.mime_type.validation プロパティを使用して、アップロードする MIME タイプのチェックをアクティブ化します。添付ファイルの MIME タイプ検証を有効 (プロパティを **true** に設定) または無効 (**false** に設定) にすることができます。

必須条件

このプロパティを設定する前に *glide.attachment.extensions* プロパティを設定してください。*glide.attachment.extensions* で指定された拡張子のみがアップロード時に MIME タイプをチェックされます。詳細については、Restrict file extensions を参照してください。

詳細情報

属性	説明
プロパティ名	*glide.security.file.mime_type.validation*
構成タイプ	システムプロパティ (/sys_properties_list.do)
カテゴリ	検証、サニタイズ、およびエンコーディング
目的	ファイルのアップロード中に MIME タイプ/マジックバイトのチェックを適用すること。
推奨値	true
セキュリティリスク評価	5.4
機能への影響度	(中) この修正により、アプリケーションに対して添付ファイルの MIME タイプの検証が有効になります。この検証は MIME タイプとデータ間の不一致をチェックするだけ

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

属性	説明
	であるため、ファイルのアップロードに悪意がある場合を除き、機能への影響はありません。
セキュリティリスク	(中) ファイルの包含や悪意があるファイルのアップロードなどの脆弱性を低減するには、MIME タイプ検証を有効にする必要があります。
参照	Administering attachments

強化のためのプロパティの設定の詳細については、「インスタンスセキュリティ強化設定」を参照してください。

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

XML 外部エンティティの制限

glide.security.file.mime_type.validation プロパティを使用して、アップロードする MIME タイプのチェックをアクティブ化します。添付ファイルの MIME タイプ検証を有効 (プロパティを **true** に設定) または無効 (**false** に設定) にすることができます。

必須条件

このプロパティを設定する前に *glide.attachment.extensions* プロパティを設定してください。*glide.attachment.extensions* で指定された拡張子のみがアップロード時に MIME タイプをチェックされます。

警告:
これはセーフハーバープロパティです。つまり、いったん変更したら変えることはできません。元に戻すことはできません。

詳細情報

属性	説明
プロパティ名	*glide.xml.entity.whitelist*
構成タイプ	システムプロパティ (/sys_properties_list.do)
カテゴリ	検証、サニタイズ、およびエンコーディング
目的	この修復コントロールは、XXE 攻撃から防御するために有効にする必要があります。
推奨値	true
セキュリティリスク評価	5.4
機能への影響度	(低) カスタマイズで *glide.xml.entity.whitelist* プロパティの包含リストではなく外部エンティティを使用している場合、NOW Platform が以降の処理をブロックする可能性があります。
セキュリティリスク	(重大) 攻撃者は DTD を使用して、サーバーが実行する可能性のある任意の HTTP 要求を含めることができます。この場合、サーバーと他のエンティティとの信頼関係を利用する他の攻撃につながる可能性があります。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

allowlistDisable エンティティ拡張による XMLdoc2 エンティティ検証の要求

カスタマイズでエンティティの拡張が必要ない場合は、*glide.xmlutil.max_entity_expansion* プロパティを使用して外部エンティティの拡張を完全に無効化します。XML は解析を完了しますが、内部または外部エンティティは含まれません。

- このプロパティを **true** に設定すると、*glide.stax.whitelist_enabled* プロパティの設定に従って、すべての外部エンティティが対象エンティティを解決または拡張しようとします。
- このプロパティを **false** に設定すると、すべてのエンティティの解決と拡張がブロックされます。詳細については、許可リストを使用した XMLdoc2 エンティティ検証 を参照してください。

必須条件

このプロパティを設定する前に、次の手順を実行してください。

- *glide.xml.entity.whitelist.enabled* および *glide.stax.whitelist_enabled* プロパティを true に設定します。詳細については、「許可リストを使用した XMLdoc/XMLUtil エンティティ検証」と「許可リストを使用した XMLdoc2 エンティティ検証」を参照してください。
- *glide.xml.entity.whitelist* プロパティでカンマ区切りの FQDN リストを定義してください。XML エンティティ処理プロパティを使用してアクセスできるのは、これらの URL のみになります。詳細については、「XML 外部エンティティ処理 - 許可リスト」を参照してください。

⚠ 警告:
これはセーフハーバープロパティです。つまり、いったん変更したら変えることはできません。元に戻すことはできません。

詳細情報

属性	説明
プロパティ名	*glide.xmlutil.max_entity_expansion*
構成タイプ	システムプロパティ (/sys_properties_list.do)
カテゴリ	検証、サニタイズ、およびエンコーディング
目的	この修復コントロールは、XML エンティティ拡張/Billion Laugh 攻撃から防御するために有効にする必要があります。
推奨値	false
セキュリティリスク評価	9.8
機能への影響度	(低) カスタマイズでエンティティ拡張を使用している場合、Now Platform が以降の処理をブロックする可能性があります。
セキュリティリスク	(重大) 攻撃者はこの脆弱性を利用してデータを指数関数的に拡張し、すべてのシステムリソースを短時間で消費する可能性があります。
ワークアラウンド	カスタマイズでエンティティ拡張が必要な場合は、このプロパティを true に設定し、「許可リストを使用した XMLdoc2 エンティティ検証」に記載されている手順を実行してください。

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

OWASp リソースの詳細については、「OWASp」を参照してください。

SVG ファイルの安全なコンテンツセキュリティポリシーの設定

このプロパティ *com.glide.csp.self_script_src_svg* は、翻訳メモリインデックス(IIX)ファイル拡張子を介してスケーラブルベクトルグラフィックス(SVG)にアクセスするときに、 **script-src none** ディレクティブを HTTP コンテンツセキュリティポリシーヘッダーに追加します。

このプロパティは *com.glide.csp.self_script_src_svg* 、クロスサイトスクリプティング (XSS) 攻撃を格納する悪意のある添付ファイルがインスタンスで実行されるのを防ぎます。このポリシーがないと、悪意のあるアクターがユーザーの Web ブラウザーで任意の JavaScript コードを実行し、データ流出やセッションの乗っ取りなどのセキュリティの脆弱性につながる可能性があります。

詳細情報

属性	説明
構成名	*com.glide.csp.self_script_src_svg*
構成タイプ	システムプロパティ (/sys_properties_list.do)
データタイプ	ブーリアン
推奨値	true
デフォルト値	true
カテゴリ	検証、サニタイズ、およびエンコーディング
セキュリティリスク	• 重大度スコア：7.1 • CVSS スコア：高 • セキュリティリスクの詳細:このプロパティを推奨値の true に設定しないと、ユーザーが悪意のあるアクターから任意の JavaScript コードを実行する可能性があります。
依存関係と前提条件	なし
機能への影響度	このプロパティは、Scalable Vector Graphics (SVG) ファイルが外部スクリプトにアクセスするのを防ぎます。

暗号化とキー管理

暗号化は、プレーンテキストを暗号テキストに変換して情報の公開を制御する暗号化手順です。

概要

ServiceNow キー管理には、エンドツーエンドのキーライフサイクルにおける暗号化キーおよび関連するセキュリティパラメーターの処理に関するアクティビティが含まれます。このキー管理は、米国国立標準技術研究所 (NIST) 800-57 ガイドラインに基づく効果的な制御です。

暗号化は、プレーンテキストの文字列を暗号化テキストに変換するために使用されます。暗号化テキストは、正しいキーにアクセスしないと判読できません。暗号化のセキュリティ上のメリットは、アルゴリズムの強度とキー管理の品質の組み合わせから得られます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

すべてのデータですべての情報を暗号化する必要はありません。大量のデータがすべてのアプリケーションでサポートされるため、処理時間が大幅に増加します。データの暗号化が必要であると判断した場合は、次の Now Platform オプションを使用できます。

開始するには

Key Management Framework (KMF) Key Management Framework (KMF) API/UX を使用すると [qa: BEGIN review][End] 、ServiceNow インスタンスで暗号化操作を実行する方法を完全にカスタマイズおよび管理できます [qa: BEGIN review][End] 。	**Column Level Encryption (CLE)** 暗号化モジュールで AES-128 または AES-256 を使用して、文字列、日付、日付/時刻、または添付ファイルフィールドを暗号化できるようにする組み込みアプリケーション。	列レベル暗号化エンタープライズ (CLE_Ent) 顧客指定のキー、API を介したスクリプトアクセス、追加の暗号化モジュール、モジュールアクセスポリシーなど、Column Level Encryption により広範な暗号化ソリューションを提供します。
クラウド暗号化 Cloud Encryption を使用すると、ServiceNow で生成されたキーを使用するか、 [qa: BEGIN review][End] ユーザーが作成して管理するキーを指定できます。	**Platform Encryption** エンタイトルメントバンドル 無制限に使用できる Column Level Encryption Enterprise、Cloud Encryption、およびデータベース暗号化にアップグレードします。	ディスク全体の暗号化 **(FDE)** フルディスク暗号化はデータベースサーバー内のストレージシステム全体にのみ暗号化を適用します。これは、顧客データを格納する唯一のコンポーネントであるためです。
	Edge Encryption 社内の機密データを暗号化してから、 [qa: BEGIN review][End] データをインターネット経由で ServiceNow インスタンスに送信します。データはインスタンス上で暗号化されたままになります。	

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

アクティベーション情報

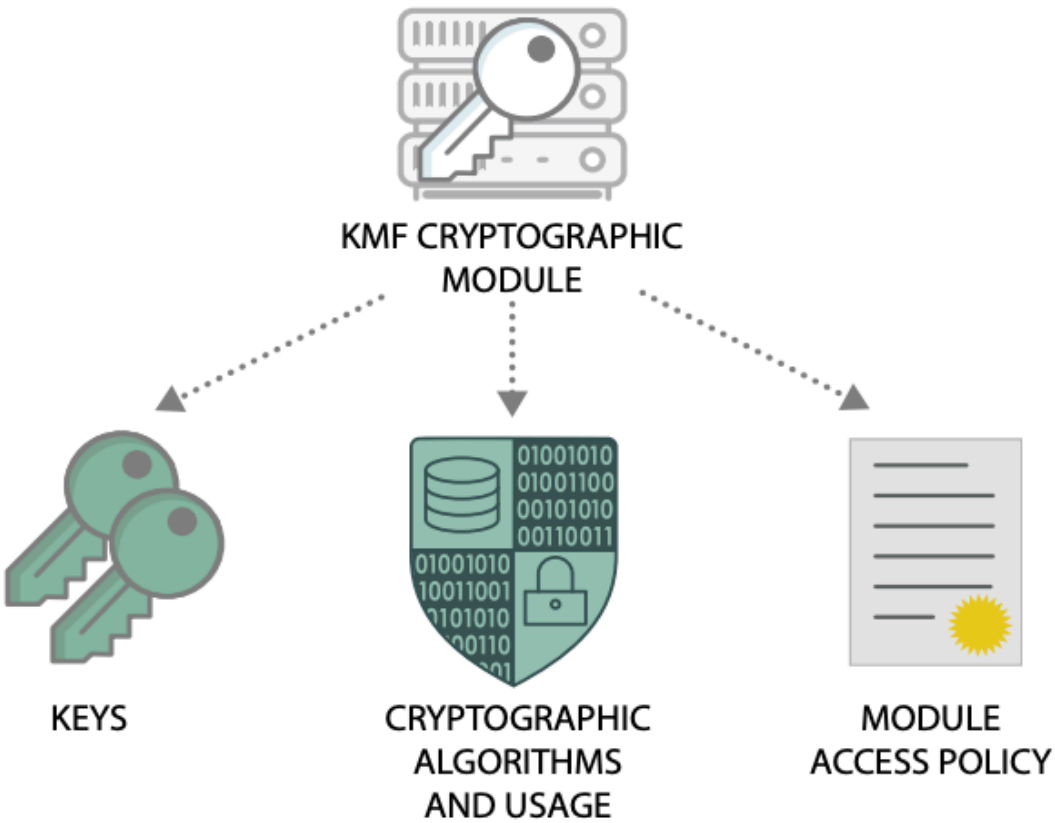
ServiceNow Platform Encryption サブスクリプションバンドルは、列レベル暗号化エンタープライズ、クラウド暗号化、およびデータベース暗号化を含む、商用グループエンタイトルメントです。

列レベル暗号化エンタープライズ は 列レベル暗号化 の無制限ライセンスです。列レベル暗号化 Enterprise プラグインは、 com.glide.now.platform.encryption プラグインをアクティブ化すると利用できます。詳細については、「暗号化とキー管理のサブスクリプションバンドル」を参照してください。

キー管理フレームワークの詳細

Key Management Framework (KMF) API/UX を使用すると、インスタンスで暗号化操作を実行する方法を完全にカスタマイズおよび管理できます。KMF は、インスタンス側の暗号化キー管理サービスのための安全で包括的なインターフェイスを提供します。

Key Management Framework の概要



この図は、KMF を構成するコンポーネントを示しています。

KMF 暗号化モジュール

暗号化モジュールは KMF の中心です。インスタンスの各暗号化モジュールは、特定のユースケースの暗号化方法を定義します。これらのモジュールの詳細については、「」を参照してください 暗号化モジュールの概要。

キー

暗号化キーは、暗号化で使用される文字列です。暗号化アルゴリズムと一緒に使用すると、暗号化データをエンコードまたはデコードできます。これらのキーは暗号化モジュールによって使用されます。生成されたキーを使用するか、Column Level Encryption Enterprise を使用して顧客指定の独自のキーをアップロードするかを選択

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

できます。キーの詳細については、次のリンクを参照してください キー管理フレームワークのインスタンスレベルのキー。

暗号化アルゴリズム

暗号化アルゴリズムは、暗号化キーを使用してデータをエンコードまたはデコードする計算手順です。これらのアルゴリズムは、インスタンスの暗号化仕様設定によって定義されます。

モジュールアクセスポリシー

モジュールアクセスポリシーは、インスタンスレベルでの制御を定義するために暗号化モジュールに適用されるアクセス制御メカニズムです。これらのポリシーは、暗号化モジュールへのアクセスが許可または拒否される条件を決定します。詳細については、「モジュールアクセスポリシーの概要」を参照してください。

キー管理フレームワークワークフロー

1. 管理者を割り当てる。管理者は他のロールを割り当てるKMFKMFことができます。
2. フィールドの暗号化設定を構成して、暗号化用に指定されたキーまたは独自の顧客指定のキー (CSK) を選択します ServiceNow 。
3. 暗号化操作に使用するメカニズムを定義する暗号化モジュールを作成します。
4. 暗号化のアルゴリズムを定義し、キーを生成する暗号化仕様を作成します。
5. データを暗号化または復号化できるコンテキストを決定するモジュールアクセスポリシーを作成します。
6. 暗号化モジュールライフサイクルポリシーを作成します。これらのポリシーは、キーの有効期間など、インスタンスレベルで暗号化モジュールに制限を課します。これらのポリシーは、公開を制限することで暗号化モジュールを保護できます。

これらのプロセスの詳細については、「」を参照してください 。

キー管理フレームワークのメリット

メリット	機能	ユーザー
機密データや専有データを保護します。	暗号化とキー管理	すべて
NIST 800-57 ガイドラインへの準拠を維持します。これらのガイドラインは、ネットワークとデータに対するサイバーセキュリティリスクを軽減するために、米国国立標準技術研究所によって提供されています。	暗号化とキー管理	セキュリティ管理者
キー管理フレームワークを使用して、暗号化キーを生成、アップロード、表示、および管理します。キーローテーションは、キーの手動ローテーションまたはスケジュールされたキーローテーションに使用してセキュリティを強化します。	キー管理フレームワーク	セキュリティ管理者

暗号化とキー管理のサブスクリプションバンドル

キー管理により、Column Level Encryption は追加料金なしで高度に構成可能な暗号化モジュールにアップグレードされます。無制限使用ライセンスにアップグレードするオプションもあります。新しい暗号化エンタイトルメントバンドルである Platform Encryption に登録します。これには 列レベル暗号化エンタープライズクラウド暗号化と が含まれます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Column Level Encryption 機能

暗号化モジュールを使用した Column Level Encryption は無料でインスタンスに含まれており、次のサポートされている機能が搭載された NIST 800-57 キー管理モジュールが含まれています。

- ServiceNow マネージド キーがサポートされています (顧客指定のキーはサポートされていません)。
- 暗号化モジュールへのアクセスはロールベースのみです。
- 無制限の手動キーローテーション。
- 一度に最大 5 つの暗号化モジュールが存在できます。
- 一度に最大 5 つのモジュールアクセスポリシーが存在できます。
- 既存のフィールドタイプがサポートされています。(それ以降のバージョンで作成された新しいフィールド タイプは、非エンタープライズ バージョンではサポートされません)。
- API サポートは、ロールアクセスに基づいて使用できます。
- 暗号化アクションの監査。
- Column Level Encryption のチュートリアル。

ServiceNow Platform Encryption グループ機能

Platform Encryption グループは、次の機能とオファリングを追加します。

- Column Level Encryption Enterprise：
  - 顧客指定のキー
  - 自動キーローテーション
  - 高度なフィールドタイプのサポートと将来の更新

    注:
    拡張されたフィールドタイプのサポートには、[ジャーナル]、[ジャーナルリスト]、[ジャーナル入力]、および **[HTML]** および [翻訳] (フィールド/テキスト/HTML) フィールドタイプが含まれます。

  - 高度な添付ファイルサポート
  - 暗号化モジュールへのアクセスは、以下に基づくモジュールアクセスポリシーで付与できます。
    - システムユーザー
    - スクリプト
    - 特定のアプリケーションスコープ
  - 無制限の暗号化モジュールとモジュールアクセスポリシー
  - Web サービスからキーをインポートします。
  - 暗号化キーの将来のローテーション日を設定します。
- キー管理を使用したクラウド暗号化。

追加情報

キー管理の詳細については、「キー管理フレームワークの理解」を参照してください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

キー管理フレームワークの理解

Key Management Framework (KMF) API/UX を使用すると、ServiceNow インスタンスでの暗号化操作の実行方法を完全にカスタマイズして管理できます。ServiceNow Key Management Framework は、インスタンス側の暗号化キー管理サービスのための安全で包括的なインターフェイスを提供します。

NIST 800-57 ガイドラインに従って、KMF は次の機能を提供します。

- 暗号化の管理と操作、監査、および統合の専用ロールで職務を分離できます。
- 暗号化モジュールにより、一意の暗号化目的とキータイプに合わせて暗号化仕様を設定できます。
  - 対称キー：暗号化と復号化、キーのラッピングとラップ解除、および認証
  - 非対称キー：デジタル署名の生成と検証、暗号化と復号化、キーのラッピングとラップ解除
- いくつかのキーライフサイクルステータスのサポートを含む、キーの生成、ローテーション、取り消し、および一時停止のためのキーライフサイクル管理
- ポリシーで設定されているとおりに暗号化モジュールにのみアクセスが許可されるように、モジュールアクセスポリシーでアクセス制御を強制します。
- キーの保護：連邦情報処理標準 (FIPS) 140-2-L3 ハードウェア Root of Trust (RoT)、公開鍵インフラストラクチャ (PKI)、キー階層、およびエンベロープ暗号化
- 主要な使用統計を含む監査

KMF のアクティブ化

KMF はデフォルトでアクティブになっています。

注:
KMF はドメイン分離をサポートしていませんが、オンプレミスのインスタンスで使用できます。

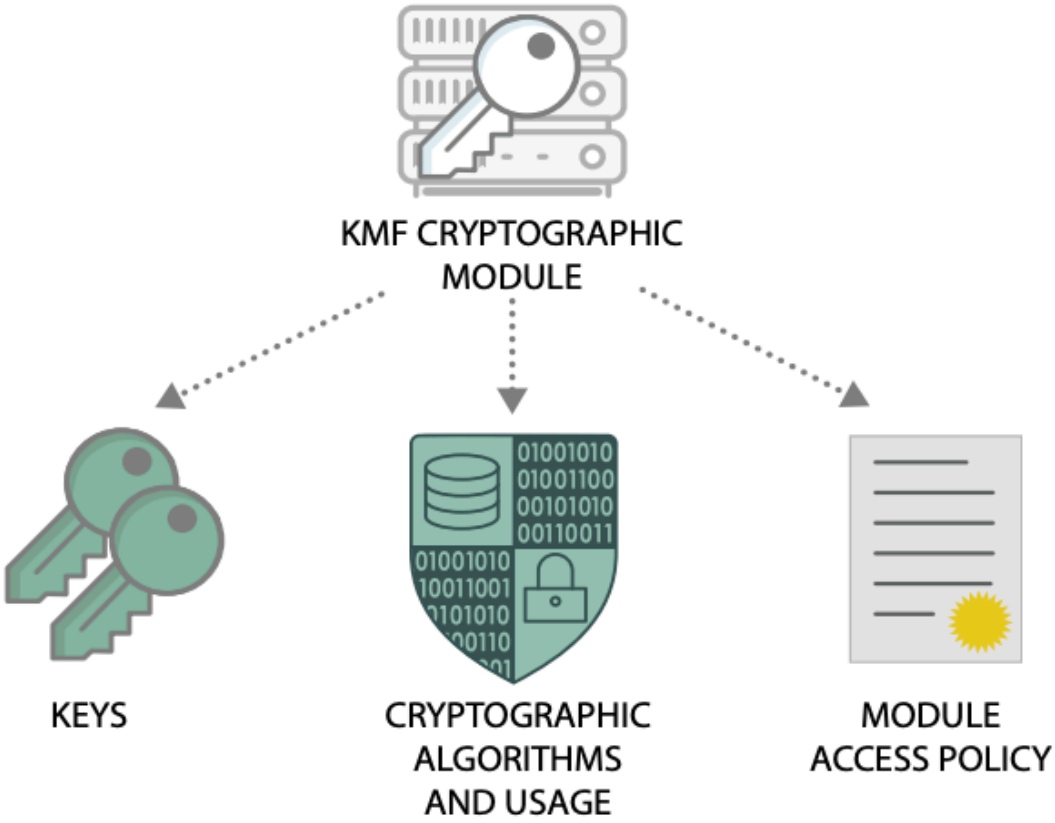
KMF の仕組み

この図は、KMF を構成するコンポーネントを示しています。

- 暗号化モジュールは、暗号化方法を定義するために使用されます。
- 暗号化仕様は、暗号化のアルゴリズムを定義する設定です。
- 仕様では、モジュールのキー、ServiceNow キー、または独自の顧客指定のキーを定義することもできます。
- モジュールアクセスポリシーは、暗号化モジュールへのアクセスが許可または拒否される条件を管理するインスタンスレベルのポリシーです。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



KMF の詳細については、「暗号化モジュールの概要」を参照してください。

Key Management Framework (KMF) では、暗号化モジュールの特定のロールとキー管理関連の設定が導入されます。KMF 管理者のみがユーザーを他の KMF ロールに割り当てることができます。詳細については、「キー管理フレームワークとともにインストールされるロール」を参照してください。

CLE の後継である暗号化フレームワークの詳細については、「Column Level Encryption Enterprise」を参照してください。

暗号化モジュールの概要

暗号化モジュールは (KMF) の中心です。特定のユースケースの暗号化操作に使用される特定の暗号化メカニズムを定義します。

暗号化モジュールは、選択した暗号化メカニズムを、定義したユースケースに適用します。たとえば、256 ビットの対称キーを持つ AES-CBC を使用して人事アプリケーションのデータを保護する場合は、そのためのモジュールを作成できます。

暗号化モジュールは、キーのライフサイクル管理もサポートしています。暗号化キーを作成してローテーションし、暗号化方法を定義できます。暗号化モジュールは、次のコンポーネントで構成されています。

暗号化仕様
: 暗号化の目的や使用するアルゴリズムなど、モジュールの側面を定義します。

暗号化キー
: モジュールが暗号化データのエンコードまたはデコードに使用するキー。これは、インスタンスによって生成されたキーにすることも、作成してアップロードする顧客指定のキーにすることもできます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセスポリシー

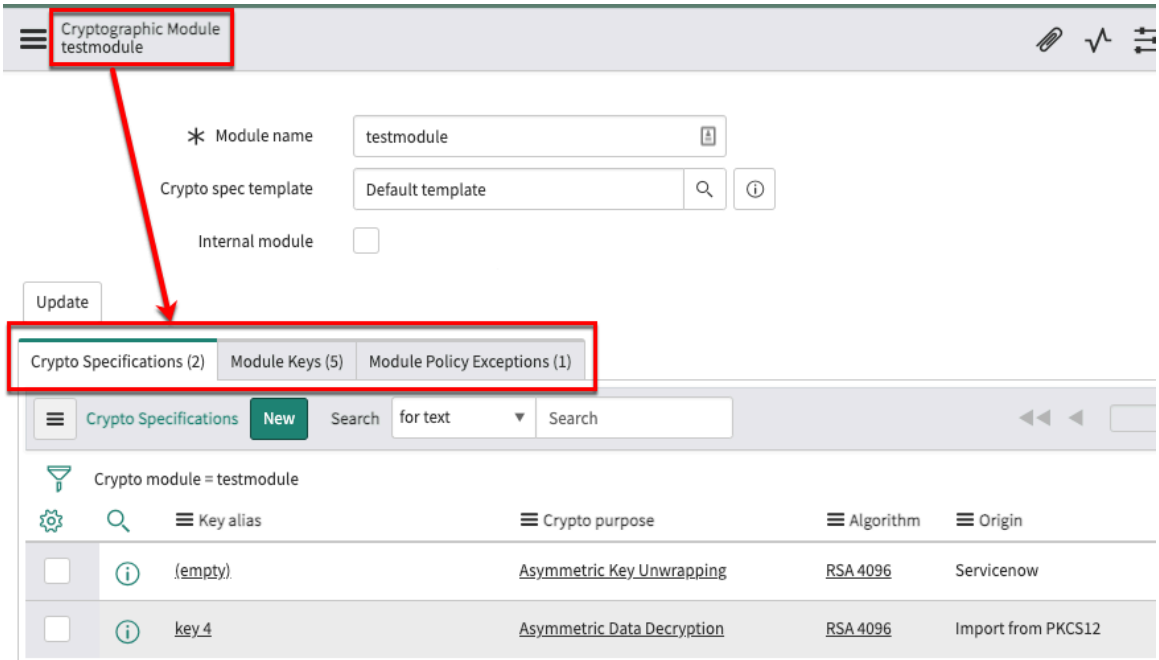
モジュールアクセスポリシーは、データの暗号化または復号化を制限するアクセス制御メカニズムです。

モジュールポリシーの例外

モジュールアクセスポリシーの例外を定義する制御メカニズム。

次の画面は、暗号化モジュール内のこれらのハイレベルのコンポーネントを示しています。

暗号化モジュールのコンポーネント



暗号化モジュールの作成の詳細については、次を参照してください 暗号化モジュールを作成する。

モジュールアクセスポリシーの概要

モジュールアクセスポリシーは、インスタンスレベルでの制御を定義するために暗号化モジュールに適用できるアクセス制御です。

モジュールアクセスポリシー

モジュールアクセスポリシーは、ベースシステムの Key Management Framework (KMF) で導入されます。

注:
列レベル暗号化エンタープライズ 機能を使用するには、サブスクリプションが必要です。詳細については、「」列レベル暗号化エンタープライズを参照してくださいColumn Level Encryption Enterprise のアクティブ化。

モジュールアクセスポリシーは、暗号化モジュールで提供されたロールベースの指定に対して展開されます。モジュールアクセスポリシーは、以下に基づきます。

- 基本 (スコープ)
- ロール
- システムユーザー
- スクリプト

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

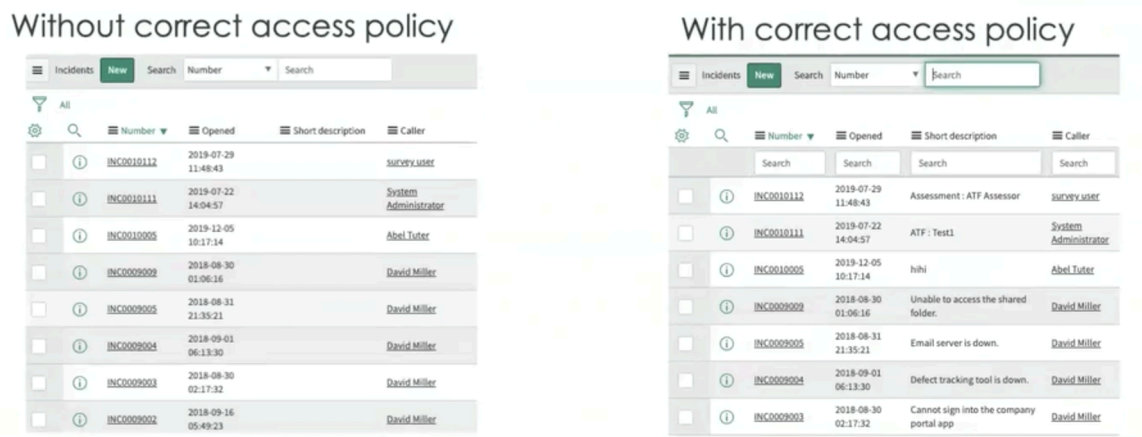
- Resource Exchange

> **注:**
> 詳細については、「キー管理フレームワークリソース交換」を参照してください。

暗号化モジュールでは、正しいモジュールアクセスポリシーを設定して、暗号化されたデータへのアクセス権を割り当てる必要があります。暗号化モジュールにモジュールアクセスポリシーが関連付けられていない場合、暗号化されたデータはユーザーに表示されず、リスト内の関連するフィールドと列は空になります。

この画像では、暗号化された [簡単な説明] フィールドにモジュールアクセスポリシーがないため、インシデントテーブルにアクセスするすべてのユーザーからコンテンツが非表示にされています。モジュールアクセスポリシーを適用すると、許可されたロールを持つユーザーに暗号化されたデータを表示できます。

暗号化された簡単な説明 (モジュールアクセスポリシーあり/なし)



> **注:**
> 列のデータは、モジュールアクセスポリシーで指定された正しいロールを持たないユーザーにも空として表示されます。

セットアップについては、「モジュールアクセスポリシーを作成する」を参照してください。

自動生成ポリシー

自動生成ポリシーは、指定された暗号化モジュールに定義されたデフォルトのモジュールアクセスポリシーに基づいて自動的にシステム生成されます。これらは、システムまたはスクリプトが特定の暗号化モジュールにアクセスしようとしたときに詳細なレベルのポリシーが定義されていない場合に生成および適用されるグローバルレベルのポリシーです。

> **重要:**
> 自動生成ポリシールールは、ジョブスケジュールタイプまたはフィールド暗号化モジュール (親モジュールが Column Level Encryption であるモジュール) には適用されません。

キー管理フレームワークのインスタンスレベルのキー

(KMF) アーキテクチャではKey Management Framework、セキュリティを念頭に置いて構築されたキー構造が導入されています。KMF はハードウェアセキュリティモジュール (HSM) を使用してエンベロープ暗号化で KMF の管理下にあるすべてのプラットフォームキーがキーのチェーンによって保護されるようにします。 KMF によって作成された顧客データ暗号化キー (CDEK) も含まれています。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

インスタンスレベルでは、KMF は Now Platform 全体でさまざまな暗号化の目的で内部的に使用される複数のキーを定義します。

エンベロープ暗号化は、キーを別のキーで暗号化する手法です。次の図は、エンベロープ暗号化の例を示しています。ここで、CDEK は IKEK によってエンベロープ暗号化され、IKEK は IRK によってエンベロープ暗号化され、最終的に IRK が RK によってエンベロープ暗号化されます。HSM のみが IRK にアクセスできるため、復号化のために IKEK をアップロードする必要があります。

この表は、KMFによって管理および保護されている利用可能な顧客/アプリキーのサブセットの例です。

キー	ロケーション	説明
ルートキー (RK)	ハードウェアセキュリティモデル (HSM)	IRK の復号化に使用されるルートキー
インスタンスルートキー (IRK)	HSM	複数のインスタンス内部キーをエンベロープ暗号化するために使用される、インスタンスに固有のキーです。
インスタンス HMAC キー (IHK)	インスタンス	インスタンスごとに固有の IHK は、ハッシュ ベース メッセージ認証コード (HMAC) の目的で内部的に使用されます。 IHK は、モジュールキーの信頼性と整合性を保証するのに役立ち、KeySecure またはファイルキーストアのいずれかにラップされます。
インスタンスキー暗号化キー (IKEK)	インスタンス	IKEK はモジュールキーをラップし、KeySecure またはファイルキーストアのいずれかでラップされます。
インスタンス非対称暗号化キー (IAEK)	インスタンス	非対称暗号化のために内部的に使用される、インスタンスに固有のキー。 IAEKは、消費者の承認中にKey Exchangeインスタンスデータレプリケーション (IDR)インスタンス間で機密メッセージを送信するために使用されます。
インスタンス署名キー (ISK)	インスタンス	署名のために内部的に使用される、インスタンスに固有のキー。
Password2 (PW2)	インスタンス	KMF では、PW2 フィールドのキーは KMF によって完全に管理されます。
顧客データ暗号化キー (CDEK)	インスタンス	によって作成された KMF 暗号化キーは、IKEK によってエンベロープ暗号化されます。
Instance Data Replication (IDR) データ暗号化キー (DEK)	インスタンス	IDR プロセスに使用される特定の暗号化キー

暗号化の目的、アルゴリズム、およびキーの情報

暗号化仕様は、非対称キーと対称キーベースの暗号化の両操作を対象に、指定された暗号化の目的に合わせてカスタマイズすることができます。暗号化の目的を選択すると、サポートされているアルゴリズムとキーの長さの設定をさらに選択できます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

暗号化の目的、アルゴリズム、および重要な情報

暗号化の目的	アルゴリズム	重要な情報
非対称データ復号化	RSA	非対称 – 2048 ビット、3072 ビット、4096 ビットのキー
非対称データ暗号化	RSA	非対称 – 2048 ビット、3072 ビット、4096 ビットのキー
非対称鍵のアンラッピング	RSA	非対称 – 2048 ビット、3072 ビット、4096 ビットのキー
非対称鍵のラッピング	RSA	非対称 – 2048 ビット、3072 ビット、4096 ビットのキー
署名生成	RSA	非対称 – 2048 ビット、3072 ビット、4096 ビットのキー
署名検証	RSA	非対称 – 2048 ビット、3072 ビット、4096 ビットのキー
対称真正性	HMAC	対称 – 256 ビット、384 ビット、512 ビットのキー
対称データの暗号化/復号化*	AES-CBC*	対称 – 128 ビット、192 ビット、256 ビットのキー
	AES-CFB	
	AES-OFB	
	AES-CTR	
	AES-GCM**	
対称キーのラッピング/アンラッピング*	AES-CBC*	対称 – 128 ビット、192 ビット、256 ビットのキー
	AES-CFB	
	AES-OFB	
	AES-CTR	
	AES-GCM**	

* AES-CBC は、等しさを維持するオプションをサポートしています。 列レベル暗号化エンタープライズ は AES-CBC を利用しています。

** AES-GCM にはデータ整合性が組み込まれています。

これらのパラメーターの設定については、「暗号化モジュールを作成する」で説明しています。

キー管理フレームワークのキーライフサイクルステータス

KMF は、特定の許容可能なアクションを強制することで、いくつかの暗号化キーライフサイクルステータスをサポートします。たとえば、アクティブステータスのキーのみが、意図した暗号化目的のために十分使用することができます。次の表は、さまざまなキーライフサイクルステータスの詳細を示しています。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

キーライフサイクルステータスまたはアクション	説明
アクティブ	暗号化モジュール内の特定の暗号化仕様に対して有効なキーは 1 つだけです。
侵害	暗号化モジュールの特定の暗号化仕様では、複数のキーが侵害された状態で存在する可能性があります。アクティブなキーまたは一時停止されたキーは、侵害された状態に移行する可能性があります。 侵害されたキーは、暗号化や署名などの新しいコンテンツを生成するために使用することはできませんが、復号化や検証などの既存のコンテンツの目的を特定するために使用することはできます。
非アクティブ化済み	任意のアクティブなキーを非アクティブにできます。暗号化モジュールの特定の暗号化仕様では、複数のキーが非アクティブにされた状態で存在する可能性があります。 たとえば、キーがローテーションされると、現在アクティブなキーが非アクティブになります。非アクティブ化されたキーは、暗号化や署名などの新しいコンテンツを生成するために使用することはできませんが、復号化や検証などの既存のコンテンツの目的を特定するために使用することはできます。 **注:** 侵害されたキーや失効したキーは、非アクティブ化されたキーとして扱われます。
破壊	キーが破棄されると、キーマテリアルは完全に削除され、暗号化の目的のために使用できなくなります。非アクティブ化されたキーは、設定された指定期間内に使用されなかった場合、ライフサイクル自動化を使用して破棄できます。暗号化モジュールの特定の暗号化仕様では、複数のキーが破壊された状態で存在する可能性があります。 **警告:** 破棄されたキーに関連付けられたデータにはアクセスできなくなるため、キーを破棄するアクションを実行するときは注意が必要です。
生成済み	暗号化モジュールの特定の暗号化仕様では、複数のキーが生成された状態で存在する可能性があります。 指定された暗号化仕様に対応するアクティブなキーが存在しない場合、生成されたキーをアクティブステータスに移行できます。生成された最初のキーは自動的にアクティブに設定されます。 **注:** 新しいキーの生成を選択した場合は、指定された暗号化仕様に生成済みステータスのキーがある場合でも、新しいキーが生成されてアクティブになります。
更改済み	有効期限のあるアクティブなキーは、キーのライフサイクル期間を延長するために何回でも更新できます。 **注:** アクティブ化日と有効期限の差が計算され、有効期限が当日から延期されます。
再開	UI アクションは、指定された暗号化仕様に他のアクティブなキーが存在しない場合に、一時停止されたキーで使用して、アクティブ状態に戻すことができます。

自動翻訳

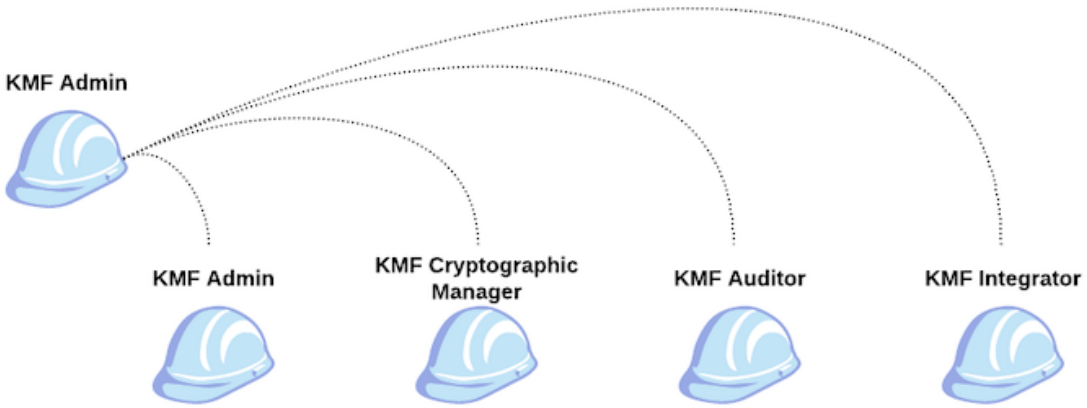
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

キーライフサイクルステータスまたはアクション	説明
取り消し済み	アクティブなキーまたは一時停止されたキーは、取り消された状態に移行する可能性があります。 取り消されたキーは、暗号化や署名などの新しいコンテンツを生成するために使用することはできませんが、復号化や検証などの既存のコンテンツの目的を特定するために使用することはできます。 暗号化モジュールの特定の暗号化仕様では、複数のキーが取り消された状態で存在する可能性があります。
ローテーション済み	キーのローテーションにより、現在のアクティブなキーが非アクティブになり、別のキーがアクティブになります。新しいアクティブなキーを次から選択します。 • 新しいキーの生成。 • 既存のインポートされたキーをポイントします。任意のアクティブなキーをローテーションできます。
一時停止	暗号化モジュールの特定の暗号化仕様では、複数のキーが一時停止された状態にある可能性があります。キーが一時停止され、その暗号化仕様に他のアクティブなキーが存在しない場合は、キーを再開してアクティブステータスに再アサインできます。

キー管理フレームワークとともにインストールされるロール

Key Management Framework (KMF) では、暗号化モジュールの特定のロールとキー管理関連の設定が導入されます。

重要:
KMF admin ロールを割り当てるには、admin、security_admin、および sn_kmf_admin ロールが必要です。他の KMF ロールを割り当てるには、KMF admin ロールを使用します。KMF ロールのアサインの詳細については、「KMF ロールの割り当て」を参照してください。



KMF 管理者 [sn_kmf.admin]

ServiceNow Key Management Frameworkに関する操作を実行するためのロールを他のユーザーにアサインします。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

ロールを含む

ロール内に含まれるロールのリスト。

なし。

グループ

このロールがデフォルトでアサインされているグループのリスト。

なし。

特別な考慮事項

重要:
より分化したロールが利用可能な場合は、管理者ロールを付与しないでください。

- このロールは、KMF ロールの割り当てに示すプロセスを介してアサインされます。
- KMF ロールをアサインし、さらに KMF 暗号化マネージャーのすべての機能を実行するには、このロールが必要です。

KMF 暗号化マネージャー [sn_kmf.cryptographic_manager]

暗号化モジュールに対する作成、読み取り、更新操作 (暗号化使用およびアルゴリズム構成へのキーの関連付け) およびモジュールアクセスポリシー。また、KMF 暗号化マネージャーは、キー管理 (生成、ローテーション、取り消し) およびライフサイクル操作を実行できます。

ロールを含む

ロール内に含まれるロールのリスト。

なし。

グループ

このロールがデフォルトでアサインされているグループのリスト。

なし。

特別な考慮事項

なし。

KMF 暗号化監査人 [sn_kmf.cryptographic_auditor]

暗号化モジュール情報、キーメタデータ、ライフサイクル関連の詳細、およびモジュールアクセスポリシー (MAP) 情報を表示します。

ロールを含む

ロール内に含まれるロールのリスト。

なし。

グループ

このロールがデフォルトでアサインされているグループのリスト。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

なし。

特別な考慮事項

なし。

KMF 暗号化インテグレーター **[sn_kmf.cryptographic_integrator]**

外部鍵ストアまたはシステムと統合 Key Management Framework します。

ロールを含む

ロール内に含まれるロールのリスト。

なし。

グループ

このロールがデフォルトでアサインされているグループのリスト。

なし。

特別な考慮事項

なし。

KMF 暗号化演算子 **[sn_kmf.cryptographic_operator]**

キーライフサイクルの一部 ServiceNow Key Management Framework (更新、ローテーション、取り消し) にアクセスします。

ロールを含む

ロール内に含まれるロールのリスト。

なし。

グループ

このロールがデフォルトでアサインされているグループのリスト。

なし。

特別な考慮事項

なし。

KMF ロールの割り当て

管理者にロールをアサイン KMF します。管理者は他のロールを割り当てる KMF ことができます。

始める前に
必要なロール：admin および security_admin

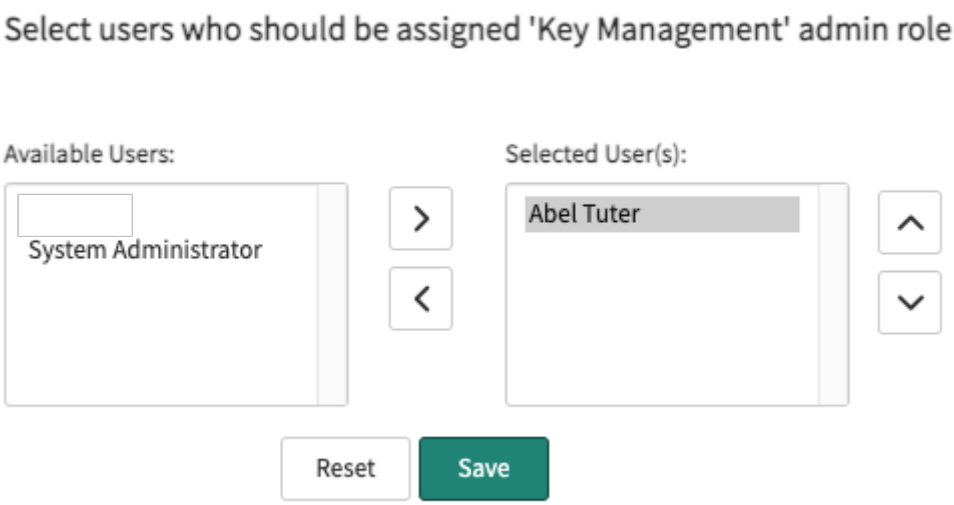
KMF admin ロールを割り当てる前に、security_admin ロールに昇格させる必要があります。詳細については、「特権ロールへの昇格」を参照してください

使用可能なロール KMF の完全なリストとその説明については、「」を参照してください キー管理フレームワークとともにインストールされるロール。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. セキュリティ管理者ロールに昇格します。
2. 移動先 ユーザー管理 > ユーザー をクリックし、管理者にする KMF ユーザーを選択します。
3. ユーザーが既に admin ロールと security_admin ロールを持っていることを確認します。
   そうでない場合は、ロール関連リストで [編集] を選択し、**admin** と **security _admin** を追加します。
4. 移動先 システムセキュリティ > キー管理の管理.
5. [利用可能なユーザー] 列で KMF admin にするユーザーを選択し、[選択したユーザー] 列に移動します。

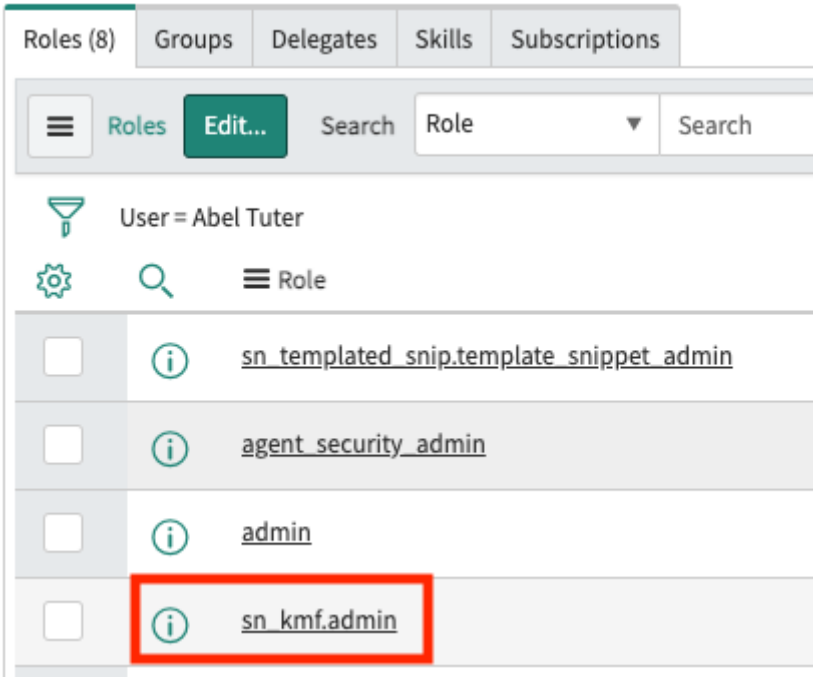


6. [**Save** (保存)] を選択します。
7. 移動先 ユーザー管理 > ユーザー をクリックし、sn_kmf.admin ロールを付与したユーザーを選択します。

自動翻訳

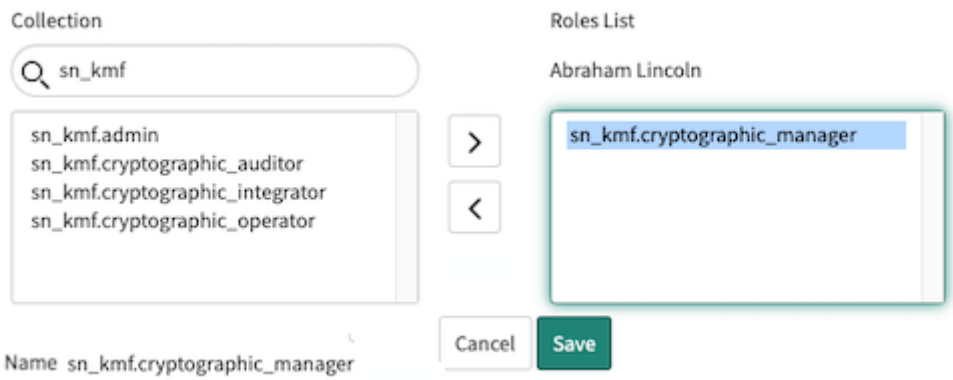
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ユーザーには [ロール] 関連リストに sn_kmf.admin ロールがあり、他の KMF ロールをアサインできます。



次のタスク
KMF admin ロールを持っている場合は、次の手順に従って他の KMF ロールを割り当てます。

1. 移動先 ユーザー管理 > ユーザー をクリックし、KMF 暗号化マネージャーなどの別の KMF ロールを持つユーザーを選択します。
2. ロール関連リストで、[編集] を選択し、ユーザーに割り当てる KMF ロールを選択します。すべての KMF ロールは sn_kmfで始まります。



キータイプを選択するためにフィールドの暗号化を設定する

Now Platform での暗号化に提供されたキーまたは独自の顧客指定のキー (CSK) を使用するように ServiceNow フィールドの暗号化設定を構成します。

始める前に
顧客指定のキーは 列レベル暗号化エンタープライズ でのみサポートされています。

必要なロール：sn_kmf.cryptographic_manager および security_admin

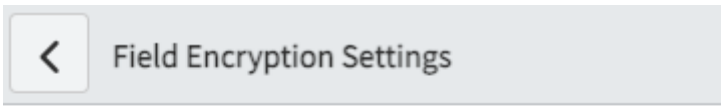
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

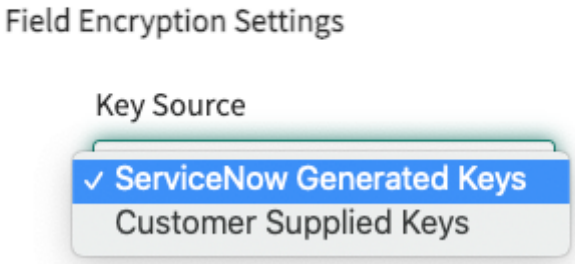
自動翻訳

手順

1. 移動先 すべて > システムセキュリティ > フィールド暗号化設定.
2. [フィールドの暗号化設定] で、**[ServiceNow** によって生成されたキー] または [顧客指定のキー] をキーソースリストから選択します。

キーソースの選択





このオプションで、`com.glide.encryption.cle_kmf.key_source` プロパティを **[ServiceNow** によって生成されたキー]または[顧客指定のキー]に変更します。

3. [保存] を選択します。

次のタスク

- 顧客指定の独自のキーを使用する場合は、「」を参照してください 顧客指定のキーのプロパティを設定する。
- 提供されたキーを使用している場合は ServiceNow 、暗号化モジュールの作成を開始します。「暗号化モジュールを作成する」を参照してください。

暗号化モジュールを作成する

暗号化操作に使用するメカニズムを定義する暗号化モジュールを作成します。モジュールを作成した後、暗号化のアルゴリズムを定義し、キーを生成する暗号化仕様を作成します。

始める前に
独自のキーを指定する場合は、顧客指定のキーの設定とアップロード に移動します。

必要なロール：sn_kmf.cryptographic_manager

このタスクについて
この手順では、ServiceNow プラットフォームベースシステムにおいて、KMF で使用できるオプションについて説明します。列レベル暗号化エンタープライズ 機能は `com.glide.now.platform.encryption` プラグインがアクティブな場合にのみ使用できます。列レベル暗号化エンタープライズ の取得についての詳細は「Column Level Encryption Enterprise のアクティブ化」を参照してください。「Column Level Encryption の暗号化モジュールを作成する」を参照してください。

注:
暗号化モジュール [sys_kmf_crypto_module] レコードは削除できません。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. 移動先 すべて > キー管理 > 暗号化モジュール > 新規作成.
2. フォームのフィールドに入力します。

暗号化モジュールのフィールド

フィールド	説明
モジュール名	スクリプトの実行時に参照される英数字の文字列。
暗号化仕様テンプレート	暗号化仕様でサポートされているアルゴリズムのマッピングが含まれているため、暗号化モジュールの作成に使用するデフォルトのテンプレートを選択します。
デフォルトのモジュールアクセスポリシー値	○ システムのデフォルトに依存： ○ 却下 ○ 追跡
実際のモジュールアクセスポリシーの結果	デフォルトのポリシー値またはモジュールアクセスポリシーの作成時に選択された値に基づいて、却下または追跡します。
名前	アプリケーションスコープ名が先頭に付加される暗号化モジュール名。
暗号化モジュールライフサイクルステータス	ライフサイクルとは、暗号化モジュールの作成、使用、非アクティブ化を指します。設定時に最初は [ドラフト] に設定されます。モジュールを使用する場合は、このフィールドを [公開] に設定します。 [デフォルト] テンプレートは自動的に [公開] に設定されます。

3. [送信] を選択します。

⚠ 警告:

従来の暗号化サポートユーザーの場合：

非エンタープライズバージョンの Column Level Encryption を使用している場合は、5 つのモジュールに制限されます。 この上限を超えると、次の警告が表示されます。

この挿入により、サブスクリプション製品に認められている Column Level Encryption の公開モジュール数の上限を超えました。追加のモジュールには、Column Level Encryption の Enterprise サブスクリプションが必要です。アカウントチームにお問い合わせください。

正常に送信すると、暗号化モジュールが暗号化モジュールテーブルにリストされます。他のスコープ対象アプリケーションとの競合を避けるために、名前の先頭にスコープが付加されます。たとえば、グローバルアプリケーションスコープで my_crypto_module という名前のモジュールを作成した場合、その名前は global.my_crypto_module として保存されます。

次のタスク
暗号化仕様を作成する

。

暗号化仕様を作成する

暗号化モジュールを作成してから、モジュールアルゴリズムを定義する暗号化仕様を作成します。

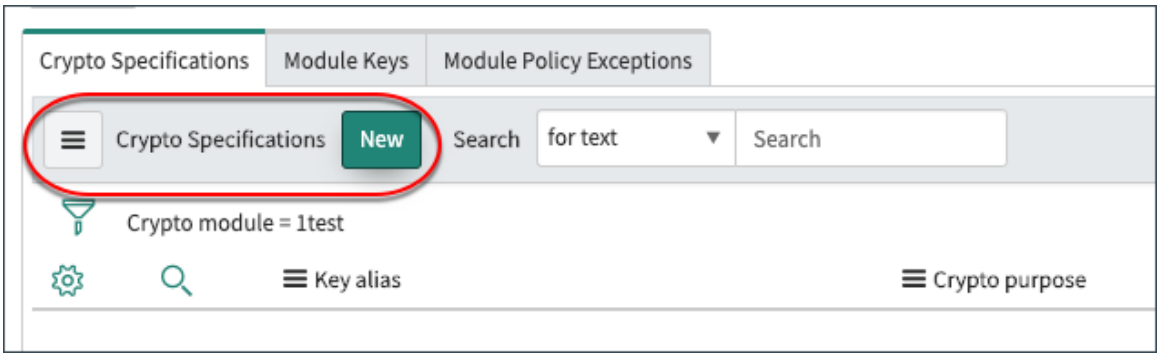
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

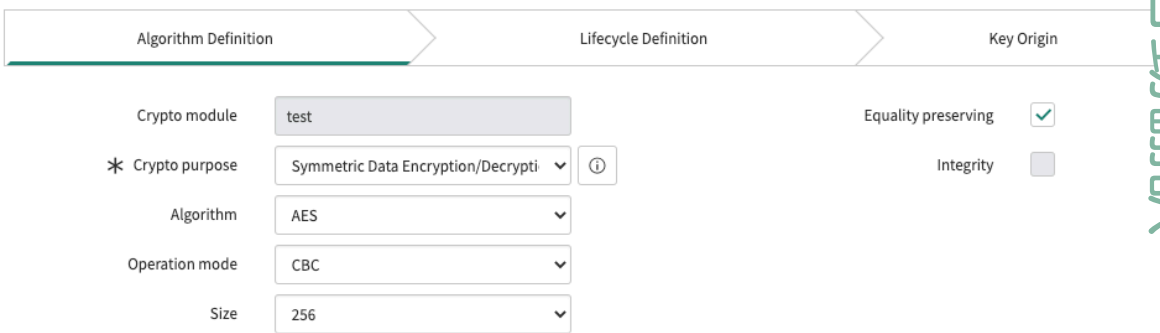
始める前に
必要なロール：sn_kmf.cryptographic_manager

手順

1. 移動先 キー管理 > 暗号化モジュール > すべて.
2. 定義用の暗号化モジュールを選択して、設定オプションを開きます。
3. [暗号化仕様] タブで、[新規] をクリックします。



4. [アルゴリズム定義] フォームに入力します。
詳細については、「暗号化の目的、アルゴリズム、およびキーの情報」を参照してください。



[アルゴリズム定義] 画面が開きます。キー生成のオプションを選択します。選択した暗号化モジュールの複数のキーを生成するには、この手順を繰り返します。

アルゴリズム定義フィールド

フィールド	
暗号化モジュール	読み取り専用。選択した暗号化モジュールの名前が表示されます。
暗号化の目的	このモジュールの目的を選択します。たとえば、データの暗号化、署名の生成、またはキーのラッピングに使用できます。利用可能なアルゴリズムは、選択した暗号化の目的に基づいて調整されます。詳細については、「暗号化の目的、アルゴリズム、およびキーの情報」を参照してください。
アルゴリズム	暗号化の目的を達成するために使用されるアルゴリズムのタイプ。アルゴリズムはキーの作成

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	
	元も制御します。選択した暗号化の目的に基づいて自動的に調整されます。詳細については、「暗号化の目的、アルゴリズム、およびキーの情報」を参照してください。
操作モード	このフィールドは、選択した暗号化の目的に基づいて表示されます。
サイズ	ビットサイズを選択します。
ハッシュ	このフィールドは、選択したアルゴリズムに基づいて使用可能になります。
等価性保存	非決定的暗号化を有効にします。 このオプションは、**AES** を使用した対称データの暗号化/復号化を暗号ブロックチェーン **(CBC)** モードで選択した場合に表示されます。 このオプションを選択すると、同じデータを再度暗号化する場合、エンコードされるデータは毎回同じになります。非決定的暗号化では、等価比較演算子を使用した暗号化データのリストのフィルタリングはサポートされていません。
完全性	GCM 操作モードは完全性を提供します。

5. [次へ] をクリックします。
暗号化仕様は、選択したアルゴリズムに基づいてキーライフサイクルテーブルにリストされます。

次のタスク
次のいずれかの操作を実行します。

- キーライフサイクルテーブルのエントリを選択して、キーライフサイクルの動作を定義します。キーライフサイクル定義の完了に関する詳細については、「キーライフサイクルステータスの設定」を参照してください。
- [次へ] をクリックして暗号化キーを作成します。キーの生成については、次のいずれかのタスクを参照してください。
  - ServiceNow 暗号化キーを生成する。
  - 顧客指定のキーのプロパティを設定する。
  - ラッピング/ラップ解除キーペアのインポート。

キーライフサイクルステータスの設定

暗号化仕様を作成すると、インスタンス内のキーのライフサイクルアクションを設定できます。

始める前に
必要なロール：sn_kmf.admin

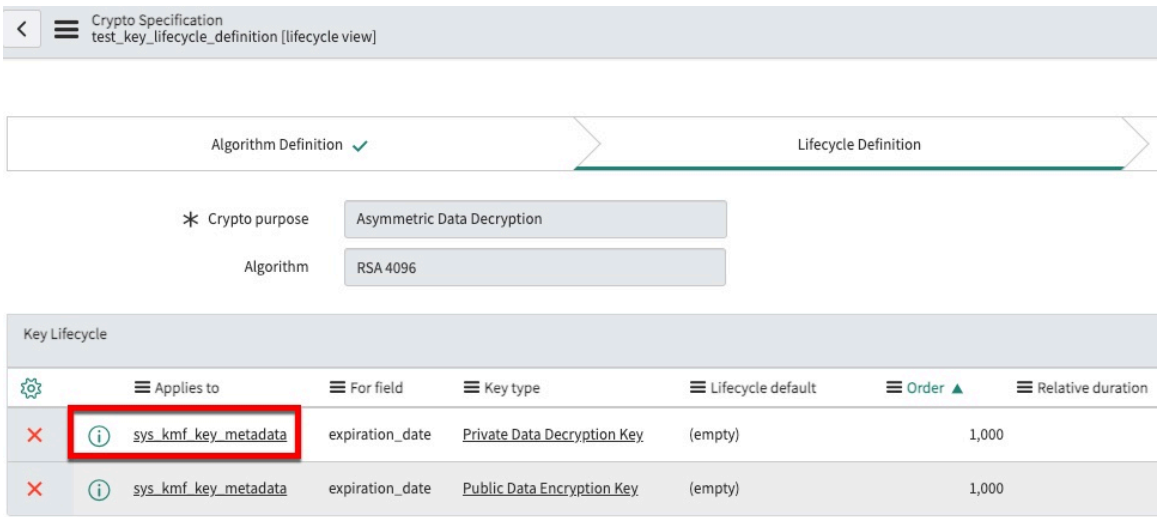
手順

1. 移動先 キー管理 > 暗号化モジュール > すべて.
2. キーのライフサイクルを設定する暗号化モジュールを選択します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

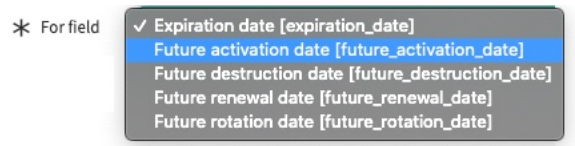
自動翻訳

3. [暗号化仕様] タブでキーエイリアスをクリックします。
   選択したキーのアルゴリズム定義フォームが開きます。



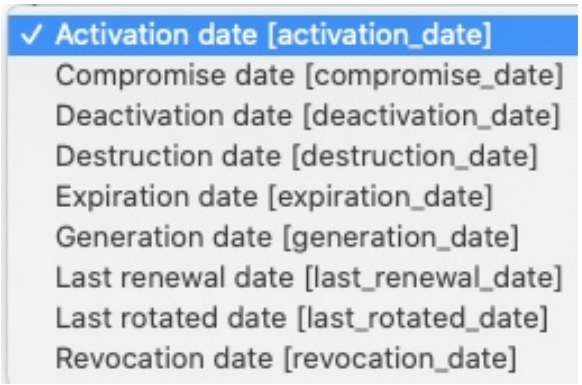
4. [次へ] をクリックします。
   フィールドライフサイクルテンプレートがロードされます。デフォルトのキーライフサイクル値は、定義された暗号化仕様に対して選択されたアルゴリズムに基づいて作成されます。
5. 暗号化仕様のライフサイクル定義ステップの [適用先] 列から、キーライフサイクルを選択します。

キーライフサイクルフィールド

フィールド	説明
適用先	ライフサイクルが適用される選択されたキー。
フィールド用	ライフサイクルが適用されるキーの制御タイプを選択します。 キーライフサイクル管理の「フィールド用」の値 
タイプ	キーライフサイクルの評価が相対値か絶対値かを選択します。 ○ 相対：キーの生成、アクティブ化、非アクティブ化など、システム内の他のデータエントリに依存する値を入力します。 ○ 絶対：日付などの正確な値を入力します。
ライフサイクルのデフォルト	読み取り専用。設定されている場合は値を表示します。
順番	暗号化仕様のキーライフサイクルステータスを処理する順序を入力します。
相対期間タイプ	ライフサイクルの期間：年、月、または日。
相対期間	キーが有効である年数、月数、または日数。
相対操作	前または 後。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
相対的	期間が関連するフィールド。相対期間または操作が選択されているかどうかを表示します。 

ServiceNow 暗号化キーを生成する

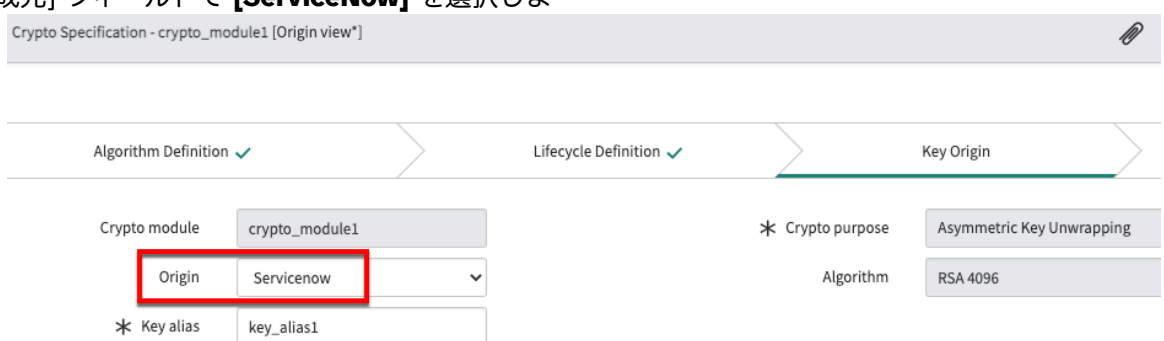
機密データを暗号化するための ServiceNow 暗号化キーをアップロードして設定するには、次の手順に従います。

始める前に
必要なロール：sn_kmf.cryptographic_manager

このタスクについて
暗号化マネージャーは、列レベル暗号化エンタープライズ による Now Platform での暗号化に ServiceNow 提供のキーを使用するか、独自の顧客指定のキー (CSK) を使用するかを選択できます。CSK の詳細については、「顧客指定のキーのプロパティを設定する」を参照してください。

手順

1. ServiceNow で生成されたキーを使用するようにフィールドの暗号化を設定します。詳細については、「キータイプを選択するためにフィールドの暗号化を設定する」を参照してください。
2. 移動先 キー管理 > 暗号化モジュール > すべて.
3. 対応する暗号化モジュールを選択して、暗号化モジュールの詳細ページを開きます。
4. [暗号化仕様] タブでキーエイリアスエントリの行をクリックします。
   キーがまだ生成されていない場合、キーエイリアスフィールドは空です。
5. [次へ] をクリックして、暗号化仕様コンポーネントの [キーの作成元] タブに移動します。
   [ライフサイクル定義] タブがキーライフサイクルテーブルとともに表示され、確認または編集できます。詳細については、「キーライフサイクルステータスの設定」を参照してください。
6. [作成元] フィールドで **[ServiceNow]** を選択します。



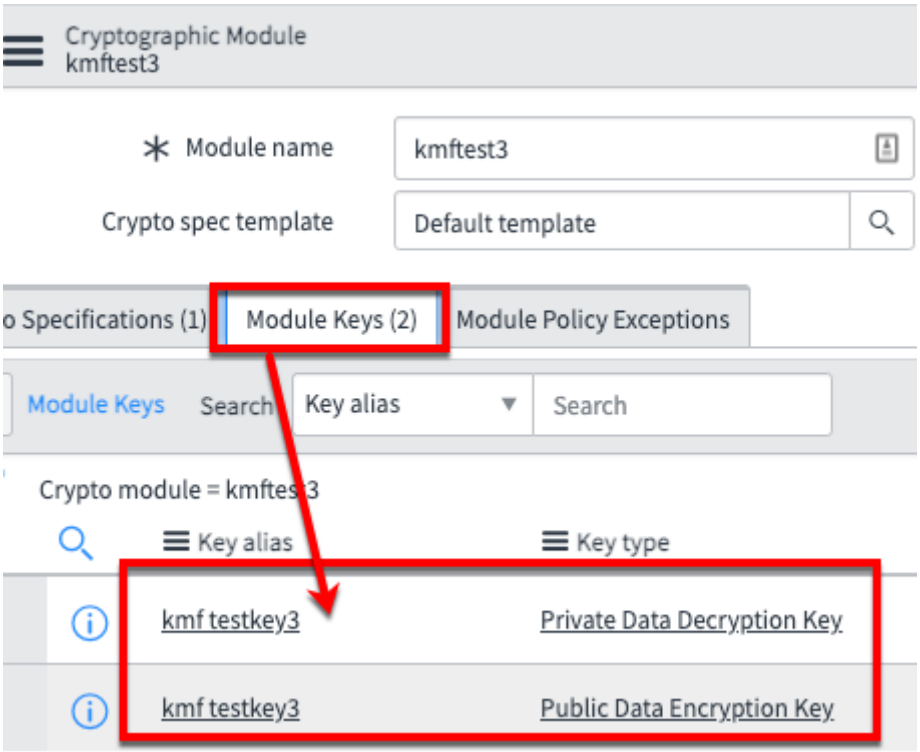
このフィールドは、ステップ 1 のフィールドの暗号化設定と選択したアルゴリズムによって異なります。インポートされたキーを使用するには、「ラッピング/ラップ解除キーペアのインポー

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

ト」を参照してください。独自のキーを使用する場合は、「顧客指定のキーのプロパティを設定する」を参照してください。

7. キーエイリアスのわかりやすい名前を入力します。
8. [次へ] をクリックして [キーの作成] タブに移動します。
9. [キーの生成] をクリックします。
   キーを生成すると、暗号化モジュールフォームが再ロードされて暗号化仕様が表示されます。
10. [モジュールキー] タブをクリックしてキーを表示します。
    キーの安全な情報は、暗号化仕様に存在するキーの数と一緒に [モジュールキー] タブに保存されます。



11. キー管理アクションを実行するキーを選択します。詳細については、「キー管理アクション」を参照してください。

モジュールアクセスポリシーを作成する

モジュールアクセスポリシーを作成して、データの暗号化または復号化を制限する。

始める前に

必要なロール：sn_kmf.cryptographic_manager または sn_kmf.admin

このタスクについて

Column Level Encryption (CLE) は、ロールベースのモジュールアクセスポリシーをサポートしており、(CLE_Ent) 機能で追加の構成オプションを使用できます。

- 対称操作をサポートする暗号化モジュール向けに、モジュールアクセスポリシーで特定の暗号化操作を設定します。たとえば、ユーザーにデータの暗号化を許可し、復号化を許可しないように設定できます。
- 暗号化モジュールごとにデフォルトのモジュールアクセスポリシー値を設定します。
- スクリプトの変更を追跡するスクリプトバージョンを関連付けてスクリプトポリシーを無効にし、スクリプトタイプのモジュールアクセスポリシーのセキュリティを強化します。

自動翻訳

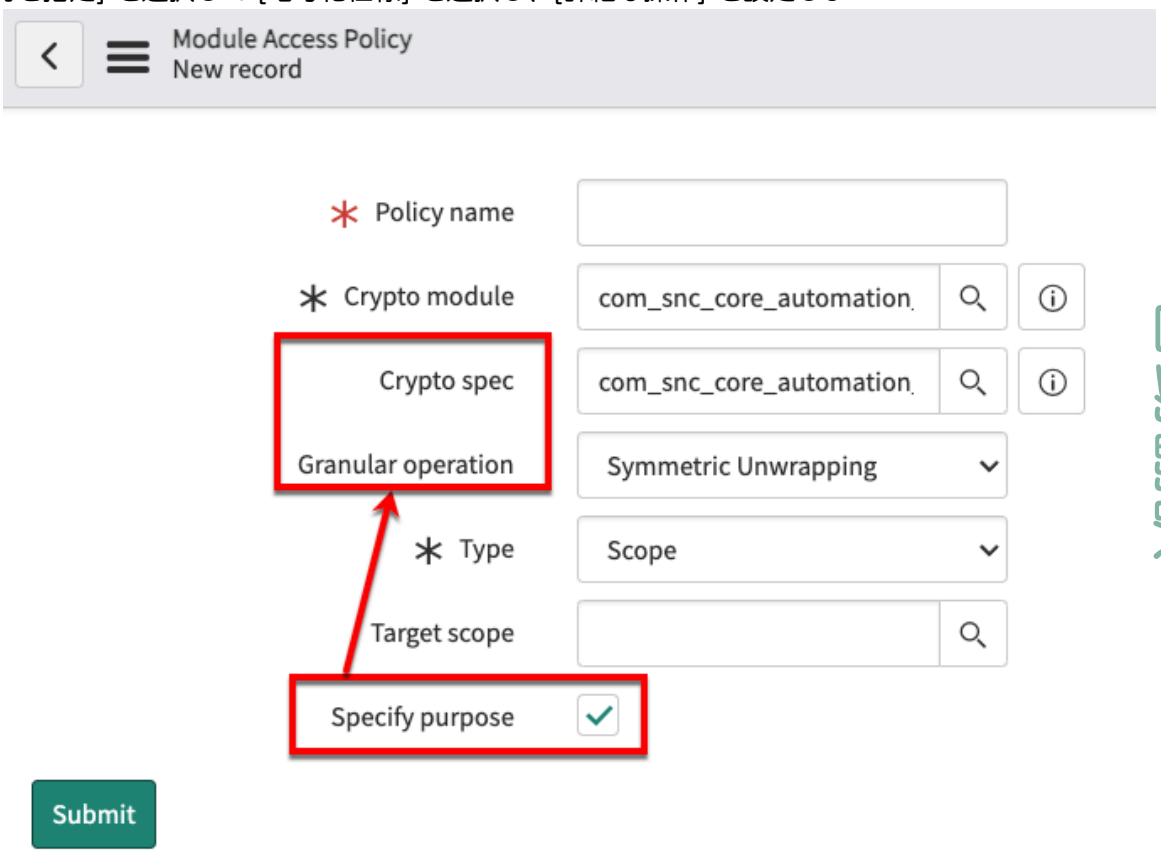
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

CLE_Ent 機能は有料サブスクリプションで利用できます。サポート対象機能と各製品で使用できるオプションについては、「」を参照してください。詳細については、「列レベル暗号化エンタープライズ」を参照してください。

> **注:**
> MAP レコードで明示的に宣言されていない限り、モジュールアクセスポリシー (MAP) のデフォルトの動作は、不正アクセスを防ぐために [拒否] です。

手順

1. 移動先 すべて > キー管理 > モジュールアクセスポリシー > すべて。
   対称データの暗号化/復号化用に構成された暗号化モジュールを作成しない場合、自動生成されたモジュールアクセスポリシーが作成され、テーブルに一覧表示されます。
2. [新規] をクリックします。
   - [目的を指定] を選択して [暗号化仕様] を選択し、[詳細な操作] を設定しま



す。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- 対称データの暗号化/復号化および対称ラッピング/ラップ解除の暗号化仕様では、[目的を指定] チェックボックスをオンにすると [詳細な操作] フィールドを使用できます。

3. フォームに入力します。

[モジュールアクセスポリシー] フィールド

フィールド	説明
ポリシー名	ポリシーの名前を入力します。
暗号化モジュール	検索アイコン ( ) をクリックしてモジュールを選択します。
暗号化仕様	モジュールアクセスポリシーの生成時に、新しい暗号化仕様を選択または作成します。このフィールドは、[目的を指定] チェック ボックスがオンの場合に利用可能です。
詳細な操作	暗号化仕様の暗号化の目的を選択します。使用可能な値は、選択した暗号化仕様のタイプによって異なります。 暗号化の目的の詳細については、「」を参照してください。
タイプ	○ スコープ：アプリケーションスコープ別にアクセスを制御します。 ○ システムユーザー：システムユーザーが暗号化モジュールにアクセスできるようにします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	○ スクリプト：スクリプトでアクセスを制御します。詳細については、を参照してください。 ○ ロール：ユーザーロール別にアクセスを制御します。 ○ リソース交換：Resource Exchange を使用してアクセスを制御します。詳細を参照してください。 **注:** Column Level Encryption では、ロールタイプのみがサポートされています。他のすべてのタイプは 列レベル暗号化エンタープライズ で使用できます。
ターゲットスコープ	フィールドはスコープタイプの識別子として表示されます。ポリシーの機能を参照します。検索メニューでアプリケーションを選択します。 **注:** ターゲットスコープはサポートされておらず、列レベル暗号化エンタープライズ でのみ設定できます。
ターゲットロール	フィールドはロールタイプの識別子として表示されます。このポリシーが適用されるロール。
スクリプトテーブル ターゲットスクリプト	これらのフィールドは、タイプとして [スクリプト] を選択した場合に表示されます。 フィールドはスクリプトタイプの識別子として表示されます。このポリシーが適用されるテーブルを選択します。このポリシーが適用されるドキュメント。[テーブル名] を選択してから、ポリシーの関連ドキュメントを選択します。 スクリプトが暗号化モジュールを初めて呼び出すと、モジュールへのアクセスが拒否され、開発者はエラーを受け取ります。このエラーにより、モジュール所有者はモジュールへのアクセスを許可または拒否できます。
リソース交換： ○ 暗号化仕様 ○ 承認タイプ ○ ターゲットインスタンスホスト	これらのオプションは、タイプとして選択すると表示されます。 Resource Exchange は、KMF と親モジュールが **column_level_encryption**されている場合の両方でサポートされます。 暗号化仕様、1 回または繰り返し、およびターゲットインスタンスの URL を選択します。詳細を参照してください。
代理操作	ロールベースのモジュールアクセスポリシーでは、ユーザーは代理操作セッションを使用して暗号化されたデータにアクセスできます。管理者などのユーザーが他のユーザーの代理操作を行うと、そのような代理操作が有効なモジュールアクセスポリシーが適用されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
目的を指定	[暗号化仕様] フィールドをポリシーで使用可能なフィールドとして切り替える場合に選択します。
有効	ポリシーを有効にする場合に選択します。
結果	次のいずれかを選択します。 ○ **StrictReject** は、すべての状況下でアクセスを拒否します。 ○ [却下] は、別のポリシーでアクセス権が付与されない限り、ターゲット ロール または ターゲットスコープ を持つユーザーによるこの暗号化モジュールへのアクセスを拒否します。 ○ 追跡してモジュールのアクセスを許可し、モジュールの使用を監視します。

4. [送信] を選択します。

> ⚠ 警告:
>
> 従来の暗号化サポートユーザーの場合：
>
> 非エンタープライズバージョンの Column Level Encryption を使用している場合は、5 つのモジュールに制限されます。 この上限を超えると、次の警告が表示されます。
>
> この挿入により、サブスクリプション製品に認められている Column Level Encryption⌧の公開モジュール数の上限を超えました。追加のモジュールには、Column Level Encryption の Enterprise サブスクリプションが必要です。アカウントチームにお問い合わせください。

5. 調べる暗号化モジュールに関連付けられているポリシー名を選択します。
スクリプトタイプモジュールアクセスポリシーの使用：

スクリプトが実行されると、デフォルトのアクセス設定に基づいてモジュールアクセスポリシーが自動生成されます。モジュール名の先頭には AutoGen- が付きます。たとえば、Module-TestPolicy モジュールは、[ポリシー名] 列に AutoGen-Module-TestPolicy として表示されます。

暗号化発信者ポリシーフォームには、選択した発信者ポリシーがリストされます。[ターゲットスコープ] フィールドで、モジュールを使用しようとするスクリプトのスコープを指定します。詳細については、「」を参照してください。

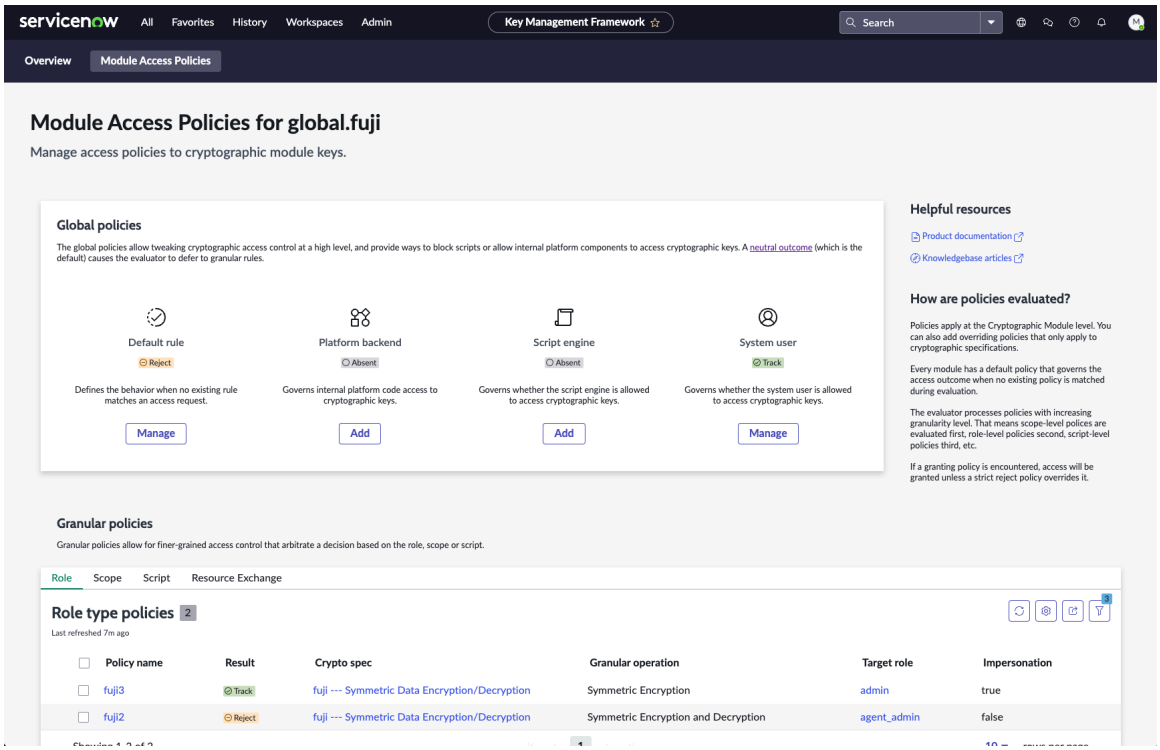
> ℹ 注:
> Column Level Encryption では、最大 5 つのモジュールアクセスポリシーが許可されます。構成オプションについては、「」を参照してください。

モジュールアクセスポリシーのビジュアル化

モジュールアクセスポリシーのビジュアル化を使用して、関連するすべての暗号化モジュール情報を単一の UI ページに表示します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳



Key Management Framework の管理者および暗号化マネージャーは、モジュールアクセスポリシーの UI ページを使用して、単一の暗号化モジュールに関連するすべてのアクセス制御メカニズムを表示できます。この UI ページで収集された情報を使用して、インスタンスで暗号化された情報にアクセスできるユーザーをすばやく判断します。

または*sn_kmf.cryptographic_manager*ロールを持つ*sn_kmf.admin*ユーザーは、次に移動してモジュールアクセスポリシーのビジュアル化 UI ページにアクセスできます すべて > キー管理 > 暗号化モジュール > すべて.

結果ラベル

モジュールアクセスポリシーには、選択した暗号化モジュールへのアクセスを許可するかどうかを決定する [結果] フィールドが含まれています。UI ページには、そのフィールドの値に基づいて UI ページの要素にラベルが表示されます。

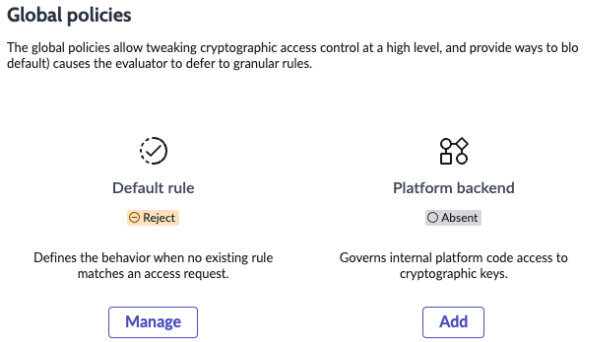
UI ラベル	結果フィールド値	定義
Track	*Track* または *Allow*	すべてのユーザーにスクリプトを含むアクセスが許可されます。
Reject	*Reject*	追跡モジュールアクセスポリシーが見つからない場合、アクセスは拒否されます。
StrictReject	*StrictReject*	アクセスは拒否されます。
Absent	*N/A*	モジュールアクセスポリシーがインスタンスに存在しません。すべてのアクセスは拒否されます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

グローバルポリシー

[グローバルポリシー **(Global policies)**] セクションを使用して、プラットフォームレベルのアクセスを制御するモジュールアクセスポリシーを確認します。

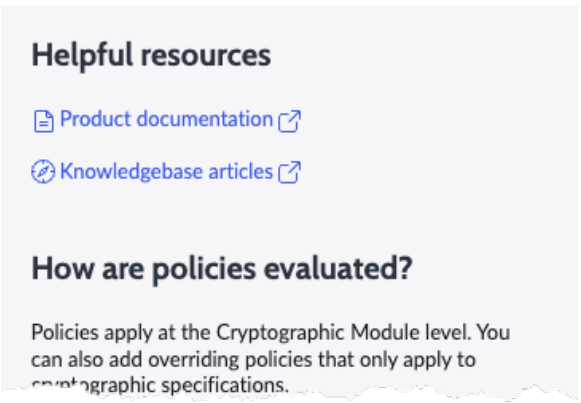
いずれかのポリシーの下にある [管理] ボタンを選択して、そのポリシーレコードに移動します。ポリシーが存在しない場合は、そのエントリの下に [追加] ボタンが表示されます。[追加] ボタンを選択して、ポリシーを定義できる新しいポリシーレコードに移動します。



ポリシー	定義
デフォルトルール	デフォルトのルールポリシーは、アクセス要求に一致する既存のルールがない場合の動作を定義します。
プラットフォームバックエンド	プラットフォームバックエンドポリシーは、暗号化キーへの内部プラットフォームコードアクセスを管理します。
スクリプトエンジン	スクリプトエンジンポリシーは、暗号化キーへのアクセスをスクリプトエンジンに許可するかどうかを管理します。
システムユーザー	システムユーザーポリシーは、暗号化キーへのアクセスをシステムユーザーに許可するかどうかを管理します。

役に立つリソース

[役に立つリソース] セクションを使用して、製品ドキュメント、関連ナレッジ記事、プラットフォームでモジュールアクセスポリシーを評価する方法に関する簡単な説明へのリンクを見つけます。モジュールアクセスポリシーを評価する方法の詳細については、「モジュールアクセスポリシーデバッガ」を参照してください。



自動翻訳

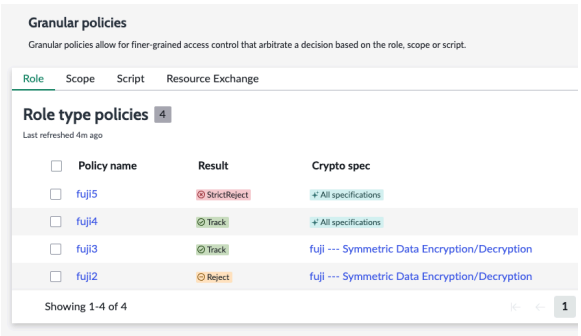
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

詳細なポリシー

[詳細なポリシー **(Granular policies)**] セクションを使用して、モジュールアクセスポリシーのリストをポリシータイプ別に表示します。リストの上にあるタブを使用して、表示するポリシーカテゴリを選択します。

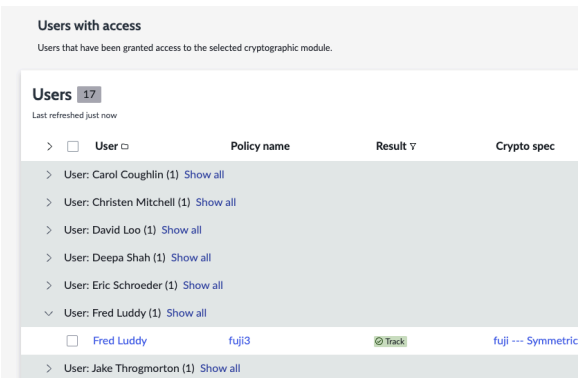
- ロール
- スコープ
- スコープとドメイン (Domain Separation がアクティブな場合)
- スクリプト
- リソース交換 (暗号化モジュールが Password2 または Column Level Encryption サブモジュールの場合)
- ID (シークレット管理 Enterprise がアクティブな場合)

デフォルトでは、各リストにはアクティブなポリシーのみが表示されます。[フィルター] アイコンを使用して、リストのデフォルトのフィルターを変更します。



アクセス権を持つユーザー

[アクセス権を持つユーザー **(Users with access)**] セクションを使用して、選択した暗号化モジュールにアクセスできるすべてのユーザーのリストを表示します。単一ユーザーが暗号化モジュールへのアクセスを許可する複数のロールを設定できるため、リストはユーザー別にグループ化されています。



モジュールアクセスポリシーデバッガ

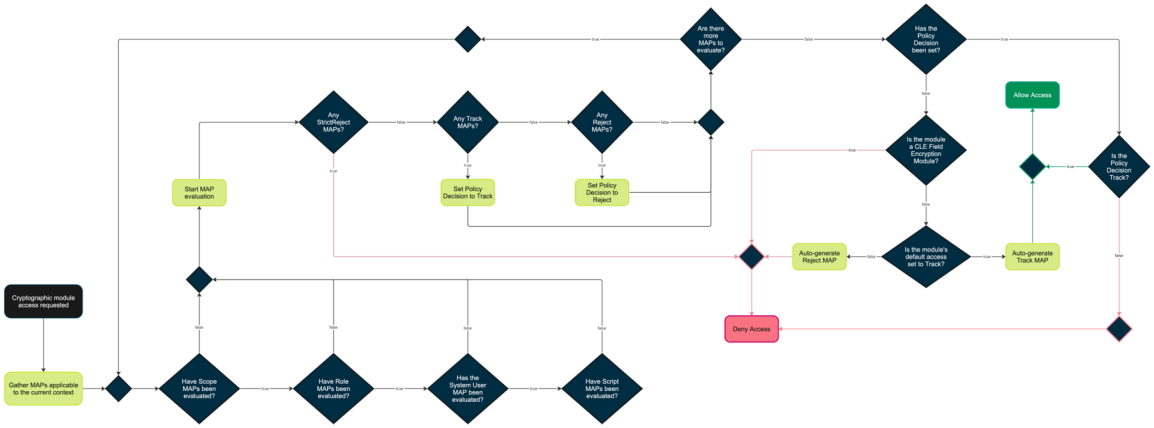
モジュールアクセスポリシーデバッガを使用してログ記録情報を確認し、ユーザーに暗号化コンテキストへのアクセスが許可される理由と許可されない理由を把握します。

モジュールアクセスポリシー (MAP) は、暗号化モジュールへのアクセスに対するインスタンスレベルの制御を定義します。問い合わせユーザー (ユーザーやスクリプトなど) は、暗号化と復号化に暗号化モジュールを使用するために明示的なアクセス権を必要とします。問い合わせユーザーが暗号化モジュールにアクセスを試みたときに評価される MAP は明確ではない場合もあります。デバッガを使用して問い合わせユーザーが暗号化モジュールにアクセスを試みたときに評価されるポリシーを確認し、アクセスが付与される理由とされない理由を確認します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

このフローチャートは、インスタンスが暗号化モジュールへのアクセス要求を評価する方法を示しています。



デバッグログへのアクセスの制御

モジュールアクセスのデバッグログへのアクセスは、ロールによって決まります。*sn_kmf.admin* および *sn_kmf.cryptographic_manager* ロールを持つユーザーは常にデバッガにアクセスできます。*glide.kmf.module_access_policies.debugger.authorized.roles* システムプロパティを使用して、他のロールにアクセス権を付与します。このプロパティの値は、デバッグログにアクセスできるロールのカンマ区切りリストです。

デバッガの有効化または無効化

モジュールアクセスポリシーのデバッグログメッセージを有効にするには、次の場所に移動しますすべて > 診断 > セッションのデバッグ > モジュールアクセスポリシーのデバッグ > .

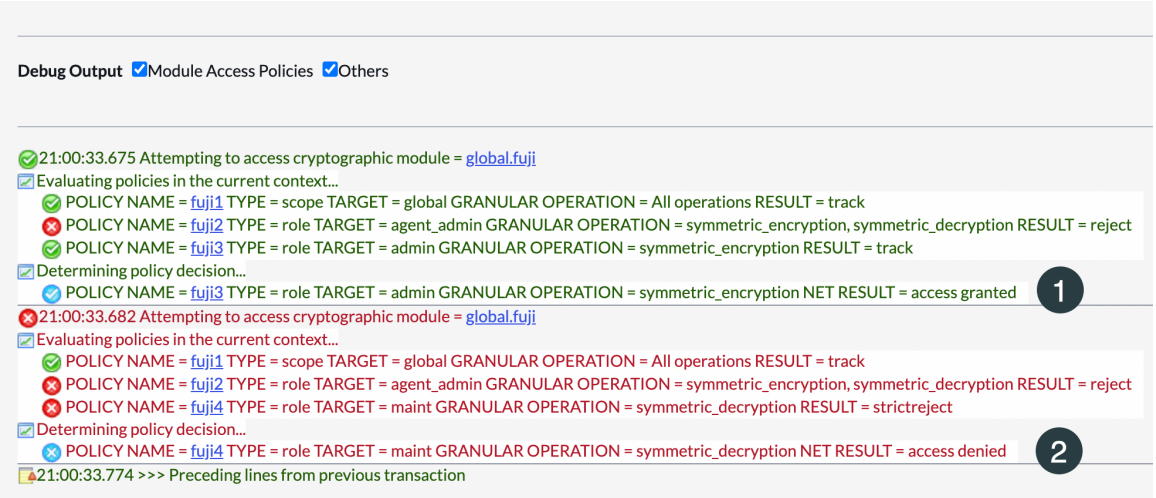
デバッグが完了したら、次の場所に移動してログ メッセージを無効にすることができます。 すべて > 診断 > セッションのデバッグ > すべて無効化 > .

ログへのアクセス

デバッグを有効にした後、MAP 評価をトリガーするページに移動して、MAP デバッグログを表示します。デバッグメッセージがページの下部に表示されます。

ヒント:
代理操作を使用して、他のユーザーのアクセスのトラブルシューティングを行うことができます。代理操作の詳細については、「Impersonating users」を参照してください。別のユーザーの観点からデバッグログを表示するには、*role* タイプのモジュールアクセスポリシーで [代理操作] フィールドが **true** に設定されていることを確認してください。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



この例では、問い合わせユーザーが global.fuji 暗号化モジュールへの 2 つのアクセス要求を呼び出します。対称暗号化は許可され、対称復号化は拒否されています。

ログエントリについて

デバッグ情報は、この形式を使用して構造化されます。

1. この最初の行にはアクセス要求を受信する暗号化モジュールが表示されます。
2. 最初の行と最後の行の間にある行には、評価済みの MAP が評価された順に表示され、名前、タイプ、ターゲット、詳細な操作、および結果が含まれています。
3. 最後の行には、ポリシー決定 (該当する場合) と問い合わせユーザーの正味アクセス結果 (問い合わせユーザーにアクセス権が付与されているかどうか) が表示されます。

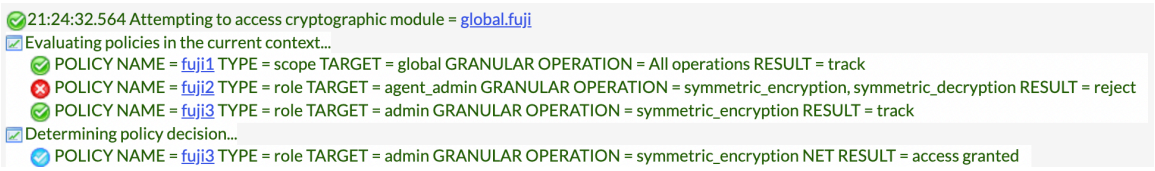
各行はメッセージタイプを示すアイコンで始まります。

メッセージアイコン

アイコン	メッセージタイプ
	情報メッセージ
	モジュールアクセスポリシーによりアクセス権が付与される
	モジュールアクセスポリシーによりアクセスが拒否される
	問い合わせユーザーのアクセスが許可される
	問い合わせユーザーへのアクセスが拒否される
	評価するモジュールアクセスポリシーなし

デバッグログの例

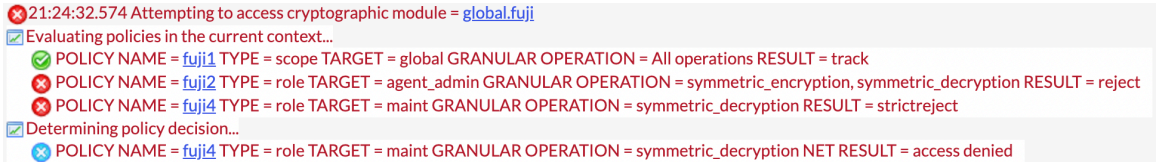
アクセスが許可された場合のメッセージ



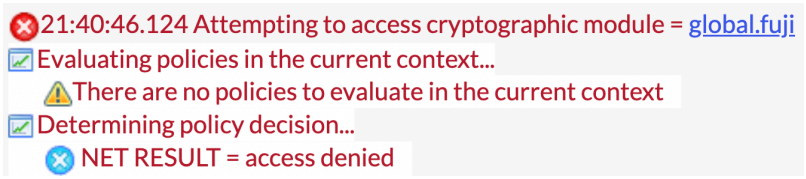
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

アクセスが拒否された場合のメッセージ



アクセスが拒否されました (評価するモジュールアクセスポリシーなし)



アクセスが拒否されました (十分な権限がない)

暗号化モジュールライフサイクルポリシーの作成

暗号化モジュールライフサイクルポリシーを作成して、キーの有効期間など、暗号化モジュールに制限を課します。公開を制限して暗号化モジュールを保護するポリシーを作成します。

始める前に

必要なロール：sn_kmf.cryptographic_manager

このタスクについて

暗号化モジュールライフサイクルポリシーは、インスタンスレベルのポリシーです。暗号化キーが公開される機会が多いほど、侵害される可能性が高くなります。キーの使用期間と使用者を制限して、キーを保護します。

暗号化モジュールは次の機能で制御されます。

- インスタンスポリシーは、インスタンスの境界を設定します。たとえば、有効期限がアクティブ化日から 2 年を超えないようにインスタンスポリシーで指定した場合、ライフサイクルルールを使用してアクティブ化日から 5 年後に有効期限を設定することはできません。
- インスタンスライフサイクルテンプレートを使用すると、異なるキーに異なるポリシーを設定できます。テンプレートには暗号化モジュールのデフォルトのライフサイクルルールが用意されているため、モジュールごとに再作成する必要はありません。たとえば、対称データ暗号化キーには、公開鍵ラッピングキーとは異なる有効期限を設定できます。
- ライフサイクルルールはキーに直接影響します。たとえば、有効期限がアクティブ化日から 2 年後になるようにライフサイクルルールで指定した場合、キーはアクティブ化日から 2 年後に期限切れになります。

手順

1. 移動先 すべて > キー管理 > ライフサイクルポリシー > インスタンスポリシー.
2. 選択 新規.
3. フォームを完了します。

暗号化ライフサイクルポリシーフィールド

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

次のタスク
このライフサイクルポリシーにモジュールレベルで例外を追加する場合は、「」を参照してください モジュールライフサイクルポリシーの例外を作成する。

モジュールライフサイクルポリシーの例外を作成する

モジュールポリシー例外を作成して、インスタンスのモジュールレベルでキーのライフサイクルポリシーを変更します。例外はそのモジュールにのみ適用され、インスタンス全体には適用されません。たとえば、管理者がインスタンスレベルで 1 年間に制限されるように対称キーを設定した場合、モジュールレベルで 2 年間の例外を作成できます。

始める前に
必要なロール：sn_kmf.cryptographic_manager および sn_kmf.admin

手順

1. 移動先 すべて > キー管理 > 暗号化モジュール すべて.
2. ポリシー例外を使用する暗号化モジュールを選択します。
3. [暗号化モジュール] テーブルで、 モジュールポリシー例外 タブに戻ります
4. クリック 新規.
5. フォームを完了します。

モジュールポリシー例外フィールド

フィールド	説明
暗号化モジュール	読み取り専用、選択されたモジュールの名前。
適用先	指定されたキーが自動入力されます。
キータイプ	例外ポリシーは特定のキーに関連しているため、キータイプを選択します。暗号化されたモジュールごとに複数の例外ポリシーを作成できます。
ポリシー条件	ドロップダウンから認定条件を選択し、追加の制約条件を入力します。
新しい条件	必要に応じて、追加のポリシー条件を選択します。
結果	[却下] を選択してキーの使用を却下するか、[追跡] を選択して条件が満たされた場合に使用を許可します。

6. クリック 送信 暗号化モジュールテーブルに返されます。

キー管理アクション

KMF のコア機能の 1 つは、キーの取り消しやローテーションなどのキー管理機能を提供することです。KMF は、最新の暗号化素材とライフサイクル操作を使用して、機密データを適切に保護します。

次の表に、主要なライフサイクル操作と管理アクションの概要を示します。暗号化モジュールの目的は、暗号化モジュール設定のデータに適用され、データには影響しません。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

キー管理アクション	説明
キーの生成	指定された暗号化モジュールの新しいキーを生成します。最初に生成されたキーはアクティブに設定されます。
キーのローテーション	現在のキーを非アクティブにし、新しいキーを生成します。新しいモジュールキーが current (アクティブ) に設定されます。
キーの取り消し	現在のキーとライフサイクルステータスを取り消し済みとしてマークします。暗号化モジュールは、新しいデータに新しいキーを自動生成し、キーのステータスをアクティブに設定します。取り消し済みは、キーが暗号化に使用されなくなったことを意味します。ただし、復号化には引き続き使用できます。キーを破棄することはできません。
キーの一時停止	現在のキーを一時停止としてマークします。暗号化モジュールを再度使用する前に、一時停止したキーを手動で再開するか、一時停止したキーを取り消して新しいモジュールキーを生成します。
キーの再開	一時停止されたキーをアクティブなキーとしてマークします。
キーの更新	現在のキーの有効期間を延長します。[更新] ボタンは、次の状況で使用できるようになります。 • 暗号化マネージャーの役割が割り当てられています。 • ライフサイクルステータスが [アクティブ] または [更新済み] にマークされます。 • 有効期限は、モジュールのライフサイクル定義に設定されます。

キーの表示と管理

キーのステータスを確認して、現在のキーを更新、ローテーション、一時停止、非アクティブ化、破棄するタイミングなどのキーアクションを決定します。

始める前に

必要なロール：sn_kmf.cryptographic_manager

手順

1. 移動先 すべて > キー管理 > 暗号化モジュール > すべて.
2. 暗号化モジュールを選択します。

   暗号化モジュール <モジュール名> フォームが表示されます。
3. [モジュールキー] タブでキーエイリアスを選択して、ライフサイクル <キー名> フォームでキーステータスを確認します。
4. フィールドはすべて読み取り専用であるため、フォームを確認します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

暗号化ライフサイクル キーフィールド

フィールド	説明
生成日	キーが生成された日付が表示されます。
アクティブ化日	キーがアクティブ化された日付が表示されます。
前回の更改日	キーが最後に更新された日付が表示されます。
前回のローテーション日	キーが最後にローテーションされた日付が表示されます。
非アクティブ化日	キーが非アクティブ化された日付が表示されます。
破棄日	キーが破棄された日付が表示されます。
キーのライフサイクルステータス	キーのライフサイクルのステータスを表示します。
今後のアクティブ化日	将来のキーのアクティブ化日が表示されます。
今後の更改日	今後のキーの更改日が表示されます。
今後のローテーション日	キーローテーションの将来の日付が表示されます。
今後の破棄日	キーが破棄される将来の日付が表示されます。
有効期限	キーの有効期限が切れる日付が表示されます。

5. キーに対してアクションを実行するには、次のいずれかを選択してすぐに有効にします。
   - キーの取り消し:キーを無効にして新しいキーを生成する場合に選択します。キーを取り消す理由を入力します。
   - キーのローテーション:現在のキーを無効にし、代わりに新しいキーを生成する場合に選択します。新しいキーがモジュールキーテーブルに一覧表示され、キーのバージョン番号が 1 ずつインクリメントします。詳細については、「」を参照してください。
   - キーの一時停止:現在のキーを非アクティブ化する場合に選択します。
   - 再開キー: 一時停止されたキーをアクティブなキーとしてマークする場合に選択します。このオプションは、アクティブなキーが一時停止された後にのみ使用できます。

キーのローテーション

セキュリティを強化するために、事前に決定されたスケジュールで暗号化キーをローテーションすることができます。暗号化キーが廃止され、新しい暗号化キーを生成して古いキーと置き換えたときにキーロテーションが行われます。

始める前に

必要なロール：sn_kmf.cryptographic_manager

このタスクについて

暗号化モジュールは、暗号化コンテキストとは異なり、新しいキーを使用して再暗号化するためにレコードのリキーをサポートしています。暗号化モジュールでキーローテーション操作を手動で実行する方法を次に示します。

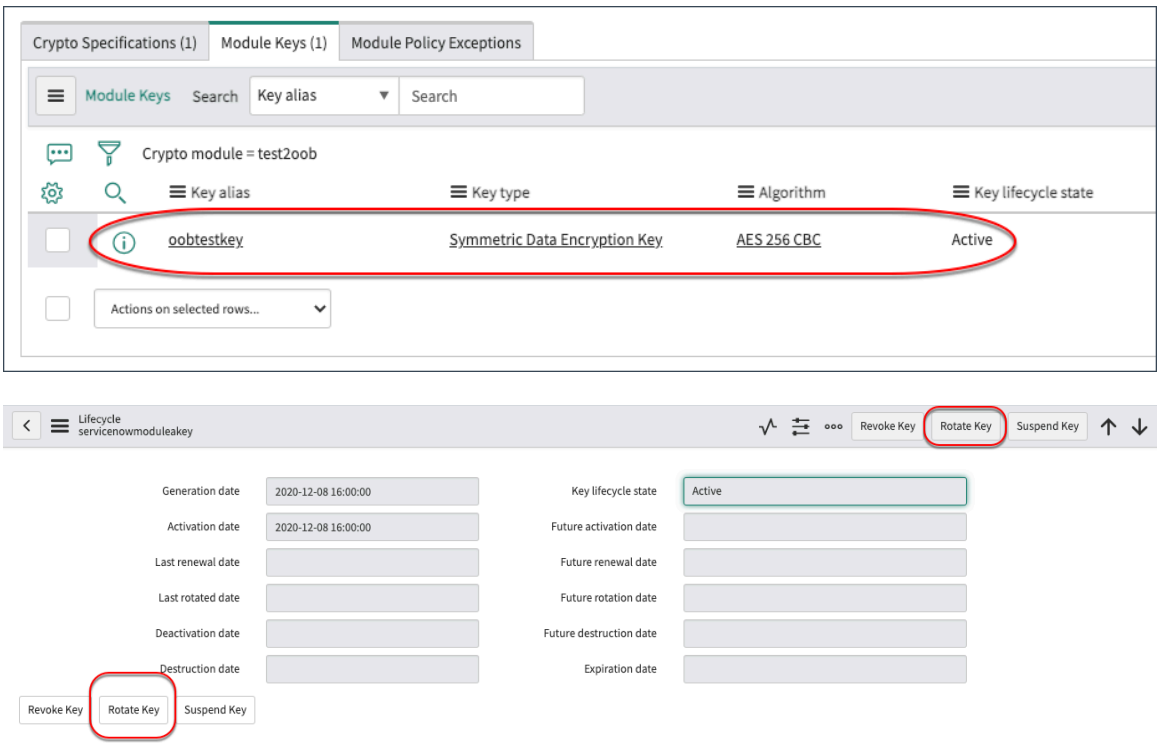
手順

1. 移動先 キー管理 > 暗号化モジュール > すべて.
2. キーローテーションの暗号化モジュールを選択します。
3. [モジュールキー] タブで、アクティブなキーを選択します。

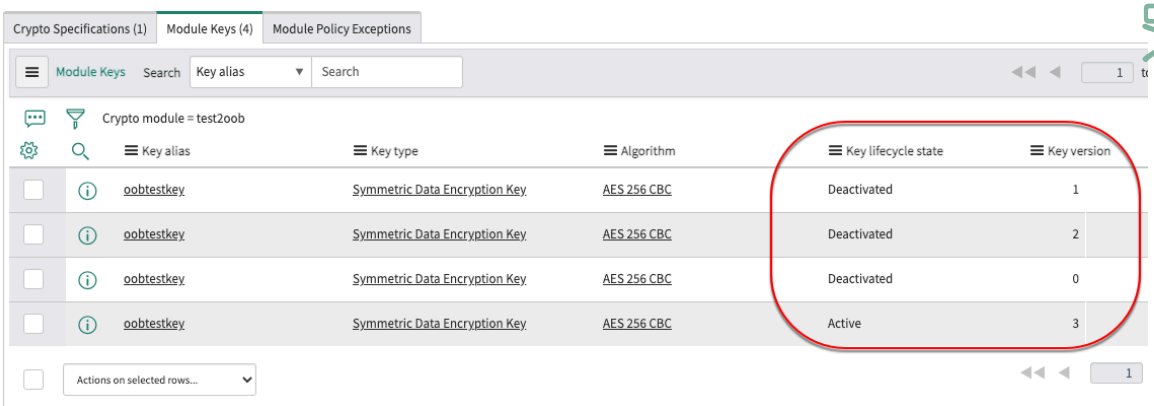
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

アクティブなキーの選択



4. [キーのローテーション] を選択します。
   キーのライフサイクルステータスが [非アクティブ化済み] に変わります。[前回のローテーション日]、[非アクティブ化日]、および [キーバージョン] フィールドが更新されます。
5. 戻る 暗号化モジュール > モジュールキー。



テーブルに追加のモジュールキーがリストされています。新しくローテーションされたキーは「アクティブ」になり、最後のキーは「非アクティブ化済み」になります。

Web サービスからキーをインポートする

Web サービス (キー REST API など) からのキーのインポートを使用して、外部顧客キーをインスタンスに安全にアップロードします。対称キーと非対称公開キーの両方をターゲットの KMF 暗号化モジュールにアップロードできます。

インポートするキー (ターゲットキー) は、インスタンスのターゲットの暗号化モジュールにアップロードする前に、ラッピングキーで暗号化する必要があります。このラッピングキーは、公開鍵/秘密鍵のペアの公開コンポーネントであり、インスタンスに存在する必要があります。このキーは、

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ラップされたターゲットキーを [Web サービスからインポート] を使用してアップロードする前の前提条件です。

次の 2 つの別々の手順 (ラッピングキーペアのインポートと Web サービスからのラップされたターゲットキーのインポート) について、以降のドキュメントで詳しく説明します。このキーペアをインスタンスの内部キーインポート暗号化モジュールで使用できるようにするには、キーペアを生成してアップロードする必要があります。

> **注:**
> この例では、キーと証明書の生成に OpenSSL を使用し、Postman API テストツールを使用して REST API の使用方法が示されています。会社の要件に基づいて、他の同等のツールで置き換えてください。

ラッピング/ラップ解除キーペアのインポート

キーをインポートする前に Key Management Framework インポート設定を構成します。

始める前に
必要なロール：sn_kmf.cryptographic_manager

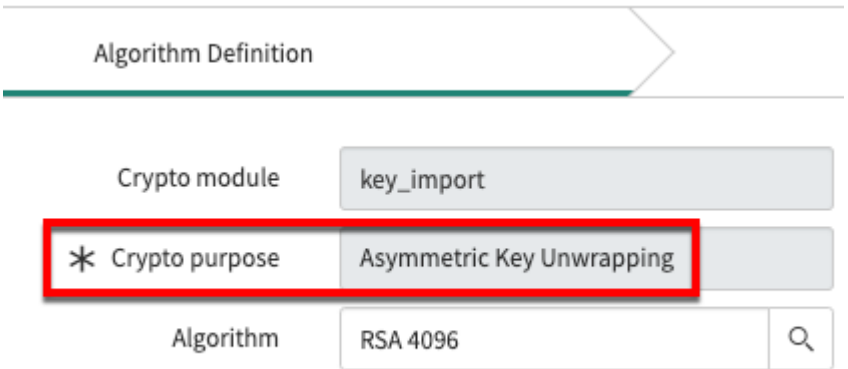
このタスクについて
この例では、OpenSSL を使用してキーと証明書を生成します。会社の要件に基づいて、他の同等のツールで置き換えてください。

手順

1. ローカル環境で、ターミナルを使用して証明書を作成します。
   例：`openssl req -x509 -sha256 -nodes -days 365 -newkey rsa:4096 -keyout wrapping_private.key -out wrapping_public.crt`

   この証明書は、キーを含む公開コンポーネントです。証明書は、AES 対称キーをラップするために使用されます。

2. ローカル環境で、ターミナルを使用して、公開証明書 (ラッピングキー付き) と秘密ラップ解除キーを含むキーストアを作成します。
   例：`openssl pkcs12 -export -in wrapping_public.crt -inkey wrapping_private.key -name "wrapping_key_alias" -out wrapping_keystore.p12`
3. インスタンスで、次の場所に移動します。 すべて > キー管理 > 設定をインポート > キーインポート設定.
4. [アルゴリズム定義] セクションで、[暗号化の目的] が [非対称キーのラップ解除] に設定されていることを確認します。



5. インポートされたキーストアの非対称キーマテリアルに適したアルゴリズムを選択します。
   詳細については、「暗号化の目的、アルゴリズム、およびキーの情報」を参照してください。
6. [次へ] を選択します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

7. [ライフサイクル定義] セクションで、[次へ] を選択して続行します。
8. [キーの作成元] セクションの、[作成元] フィールドで **[PKCS12** からインポート] または **[BCFKS** からインポート] を選択します。

   注:
   ステップ 1 のキーストア例を使用する場合は、**[PKCS12** からインポート] を選択します。

9. キー を識別するキーエイリアス を入力します。
   このエイリアスは、アップロードする証明書またはキーストアを生成するときに指定したキーエイリアス (または「分かりやすい名前」) と一致する必要があります。上記の例を続けた場合、これは wrapper_key_alias になります。
10. [次へ] を選択します。
    [キーの作成] セクションには、キーストアをアップロードするダイアログを表示する [キーのインポート] リンクが含まれています。この例を続けた場合、これは wrapping_keystore.p12 になります。

Web サービスからラップされたキーをインポートする

Web サービスからのキーのインポート機能を使用して、ラップされたキーを暗号化モジュールにアップロードします。この例では、対称キーを使用します。同様の手順を使用して、非対称キーをインポートできます。

始める前に

必要なロール：sn_kmf.cryptographic_manager (モジュール構成)、sn_kmf.cryptographic_operator (REST 操作の基本認証)

このタスクについて

キーのインポートプロセスを完了するには、KMF インポートキーエンドポイントにアクセスする必要があります。

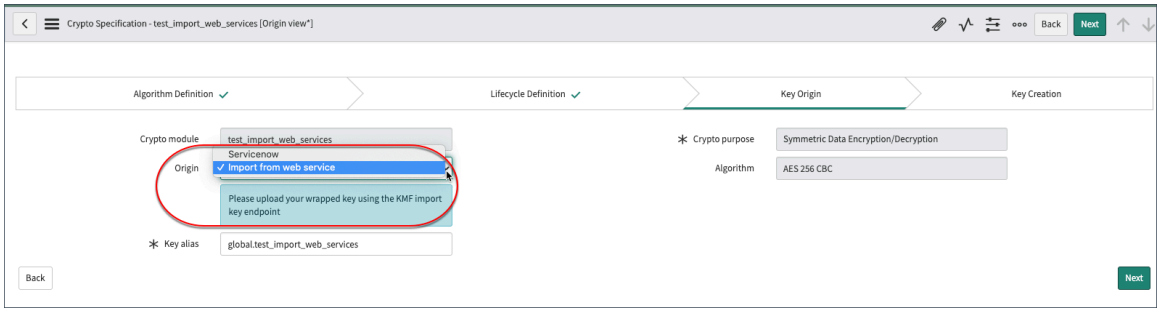
この例では、OpenSSL を使用してキーと証明書を生成します。要件に基づいて、他の同等のツールに置き換えることもできます。

手順

1. ローカルデバイスのターミナルで、キーインポートモジュールの公開鍵ラッピングキーを使用して対称キーをラップします。
   例：openssl pkeyutl -encrypt -pubin -inkey public_wrapping_key.pem -in symmetric_key.bin -pkeyopt rsa_padding_mode:oaep -pkeyopt rsa_oaep_md:sha256 -out wrapped_symmetric_key.txt
   この例では、wrapped_symmetric_key.txt という名前のラップされたキーファイルが作成されます。
2. API に関連付ける暗号化モジュールを作成します。
   詳細については、「または」を参照してください。
3. 次の選択肢を使用して暗号化仕様を追加します。

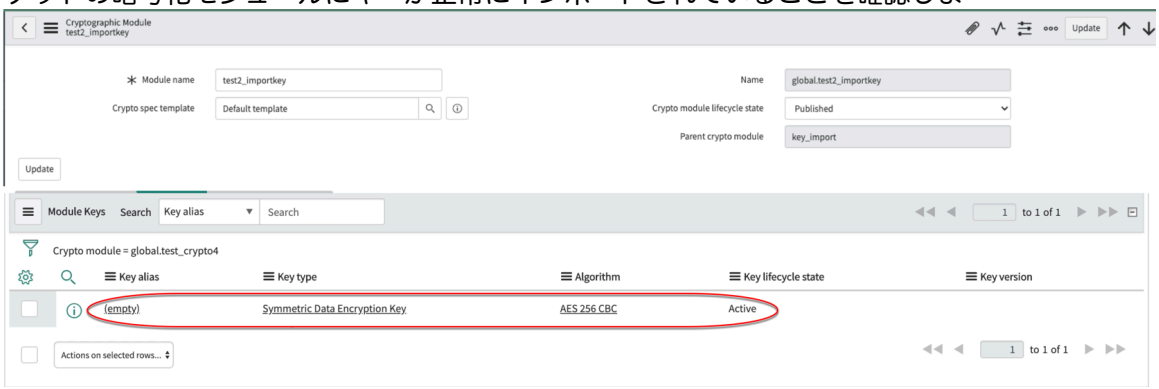
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- 暗号化の目的：対称データの暗号化/復号化
- キーの作成元：*Web* サービスからインポート



詳細については、「または」を参照してください。

4. Web サービス REST エンドポイントからインポートに対する *HTTP POST* 要求 を実行します。公開鍵のインポートに成功すると、ステータス *200* と書かれた HTTP 応答メッセージが返されます。
5. ターゲットの暗号化モジュールにキーが正常にインポートされていることを確認しま



す。

キー管理フレームワークの健全性

Key Management Framework のオンデマンド健全性ステータス情報にアクセスします。警告と誤動作エラーには、詳細なメッセージが含まれています。

始める前に

必要なロール：sn_kmf_cryptographic auditor または sn_kmf_admin または sn_kmf_cryptographic_manager

このタスクについて

Key Management Framework の各コンポーネントの概要が示され、次のステータスと色が示されます。

- 緑/操作可能:コンポーネントは操作可能で、報告するエラーはありません。
- グレー/無効：コンポーネントが非アクティブであるため、健全性チェックは実行されません。
- 黄/デグレード：警告。コンポーネントは動作していますが、遅延/一時的な問題が発生する可能性があります。
- 赤/故障：致命的なエラーによりコンポーネントが動作できず、部分的な機能停止が発生する可能性があります。

コンポーネントには、個々のレポートが含まれるサブコンポーネントを含めることができ、その健全性ステータスは次のように親に影響を与えます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- すべてのサブコンポーネントが非アクティブである場合、親は非アクティブとして表示されます。非アクティブなサブコンポーネントは、親の健康に影響を与えません。
- 1 つ以上のサブコンポーネントがデグレードまたは誤動作している場合、親の健全性はデグレードとして表示されます。
- すべてのサブコンポーネントで誤動作が報告される場合、親でも誤動作が報告されます。

サブコンポーネントの追加情報については、「キー管理フレームワークのインスタンスレベルのキー」を参照してください。

注:
健全性チェックは 15 秒ごとに実行されます。[健全性] ページを更新してレポートを再実行します。

手順

1. 移動先 すべて > キー管理 > > 診断.
2. 次の健全性ステータス情報を確認します。

診断情報

カテゴリ	詳細
キーセキュア	暗号化が試行されているかどうかを確認します。
ファイルキーストア	インスタンスルートキー (IRK) のフェッチが試行されているかどうかを確認します。 **注:** ファイルキーストアは、オンプレミスインスタンスと開発者インスタンスで使用されるキーセキュアのオフラインの代替手段です。
GlideEncrypter	GlideEncrypter インスタンスレベルの暗号化モジュール、仕様、およびキーが存在するかどうかを確認します。 **注:** GlideEncrypter は、を介してフィールドの透過的な暗号化やその他の従来の暗号化 Password2 の使用 Key Management Frameworkを可能にするスクリプト可能なコンポーネントです。
インスタンスキー暗号化キー (IKEK)	キーがファイルキーストアまたは KeySecure から取得できるかどうかを確認します。
インスタンス HMAC キー	キーがファイルキーストアまたは KeySecure から取得できるかどうかを確認します。
ボールト PKI	ボールト接続を確認して、インスタンス非対称暗号化キー (IAEK) とインスタンス署名キー (ISK) が使用可能で、ボールトから取得できるかどうかを確認します。
EJBCA PKI	LDAP 接続を確認して、IAEK と ISK が使用可能で、キャッシュと LDAP から取得できるかどうかを確認します。
インスタンス PKI	ファイルキーストアと KeySecure でキーを確認し、証明書が存在し、対称キーと一致するかどうかを確認します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

カテゴリ	詳細
	注: インスタンス PKI は、データセンター内の ServiceNow インスタンスでのみ使用できます。

トラブルシューティングのサポートについては、カスタマーサービス & サポートにお問い合わせください。

GlideEncrypter の廃止に向けたインスタンスの準備

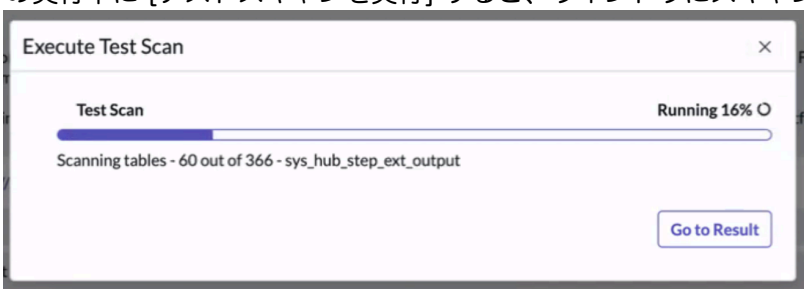
インスタンススキャンスクリプトを使用して、インスタンスで GlideEncrypter API 呼び出しを検索して削除します。これらの呼び出しの削除は、インスタンスで 3DES 暗号化を廃止するために必要なステップです。

始める前に
必要なロール：admin

GlideEncrypter API は、の Xanadu リリース ServiceNowをもって廃止される予定です。スクリプトから GlideEncrypter 呼び出しを削除するのも、インスタンスで 3DES 暗号化を廃止する前の必要なステップです。

手順

1. 移動先 すべて > インスタンススキャン > スイート.
2. [スイート] リストで、[廃止された **API (Deprecated APIs)]** を選択します。
3. [スイート] レコードで、[チェック] 関連リストから [廃止された **API: GlideEncrypter (Deprecated API: GlideEncrypter)]** を選択します。
   [列のタイプのチェック] が表示されます。このレコードには、チェックの説明と、チェックによって見つかったレコードの更新方法に関する情報とリンクが含まれています。
4. [列のタイプのチェック] レコードで、[チェックをテスト **(Test Check)]** を選択してスキャンを実行します。
   スキャンの実行中に [テストスキャンを実行] すると、ウィンドウにスキャンの進捗状況が表示されます。



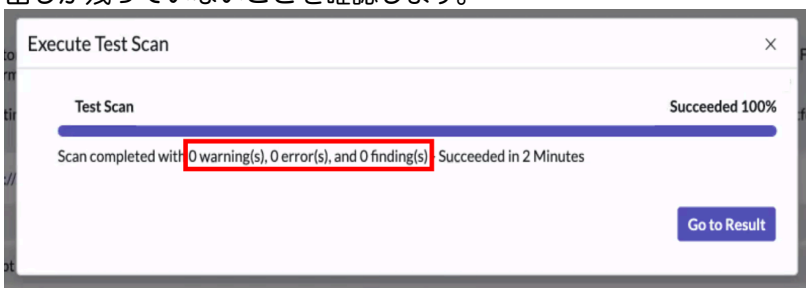
   注:
   このスキャンでは、顧客によって作成または変更されたレコードのみがチェックされます。

5. スキャンが完了したら、[結果に移動] を選択して [スキャン結果] レコードを表示します。
   [スキャン結果] レコードの [スキャン結果] リストには、**GlideEncrypter** API を使用しているインスタンスのレコードリストが表示されます。
6. [スキャン結果] リストで [カウント] フィールドを選択してレコードに移動します。
7. **GlideEncrypter** API を使用するレコード内の任意のスクリプトを変更します。
   GlideEncrypter の代替手段の詳細については、「Alternatives to deprecated GlideEncrypter APIs (廃止された GlideEncrypter API の代替手段)」を参照してください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

8. スクリプトから **GlideEncrypter** 呼び出しを削除した後、スキャンを再度実行して、API への呼び出しが残っていないことを確認します。



次のタスク
password2 フィールドの GlideEncrypter を廃止

password2 フィールドの GlideEncrypter を廃止

インスタンスで 3DES 暗号化標準を廃止すると、インスタンスが Password2 データの暗号化と復号化に対して、より安全な Advanced Encryption Standard (AES) を排他的に使用するようになります。

Rome 以降、password2 データは、より新しい Advanced Encryption Standard (AES) アルゴリズムを使用する Key Management Framework を使用して保護されます。ただし、password2 ロジックの一部の構成と代替では、暗号化と復号化に 3DES アルゴリズムを引き続き使用できます。

Vancouver リリースでは、管理者は 3DES アルゴリズムを完全に廃止することを選択できます。この変更を完了すると、インスタンスは password2 データに関連するすべての暗号化タスクと復号化タスクに対して AES 暗号化を排他的に使用します。この変更では 3DES 暗号化よりも優れたインスタンスセキュリティが提供され、これは、NIST 準拠を維持するために必要です。

廃止前の考慮事項

インスタンス間での password2 データの転送

password2 暗号化テキストを他のインスタンスに転送する場合は、ソースインスタンスとターゲットインスタンスの間で KMF Key Exchange が有効になっていることを確認する必要があります。この構成により、password2 テキストの暗号化に使用されるキーが、password2 暗号化テキストを復号化するために両方のインスタンスで使用できるようになります。3DES を廃止する前に、インスタンス間の password2 データに影響を与える可能性がある次のユースケースを検討してください。

- password2 データを使用するアプリケーションがインスタンスにある場合は、 がそのKMF Resource Exchangeインスタンスにインストールされていることを確認してください。 ソースインスタンスの password2 データの暗号化に使用されるインスタンスレベルのキーが、ターゲットインスタンスで復号化に使用できることを確認します。 KMF Resource Exchange詳細については、「キー管理フレームワークリソース交換」を参照してください。
- XML またはデータソースを介して password2 データをエクスポートする場合は、ターゲットインスタンスで KMF Key Exchange が有効になっていることを確認してください。この構成により、ソースインスタンスの password2 データの暗号化に使用されるインスタンスレベルのキーが、ターゲットインスタンスで復号化に使用で

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

きるようになります。この構成の詳細については、「キー管理フレームワークの鍵交換」を参照してください。

> **重要:**
> 上記の例はより一般的なシナリオですが、他の方法を使用して password2 暗号化テキストをインスタンス間で転送する場合は、KMF Resource Exchange を設定して、ターゲットインスタンスが password2 データを復号化できるようにする必要があります。

3DES 廃止後のインスタンスのダウングレード

以下は、password2 フィールドの入力長が 125 文字を超え、3DES 暗号化が既に廃止されているインスタンスにのみ適用されます。

インスタンスのクローン作成を介して Vancouver より前のリリースにインスタンスをダウングレードするには、クローンを開始する前に次のステップを実行します。

1. データ保持が password2 フィールドデータを保持するように設定されているかどうかを確認します。
2. 設定されている場合は、クローンを要求する前に ServiceNow サポートに連絡して 3DES の廃止を無効にしてください。[理由] フィールドで、[password2 サポートに対するクローンダウングレードの前提条件 (Clone downgrade pre-requisite for password2 support)] を使用します。

従来の Password2 フィールド

インスタンスは 3DES 暗号化を使用して password2 データを従来の (Rome 前の) password2 データに変換します。3DES 暗号化の廃止後、このオプションは使用できなくなります。この機能が引き続き必要な場合は、部分的な廃止を要求します (詳細については次のセクションを参照してください)。

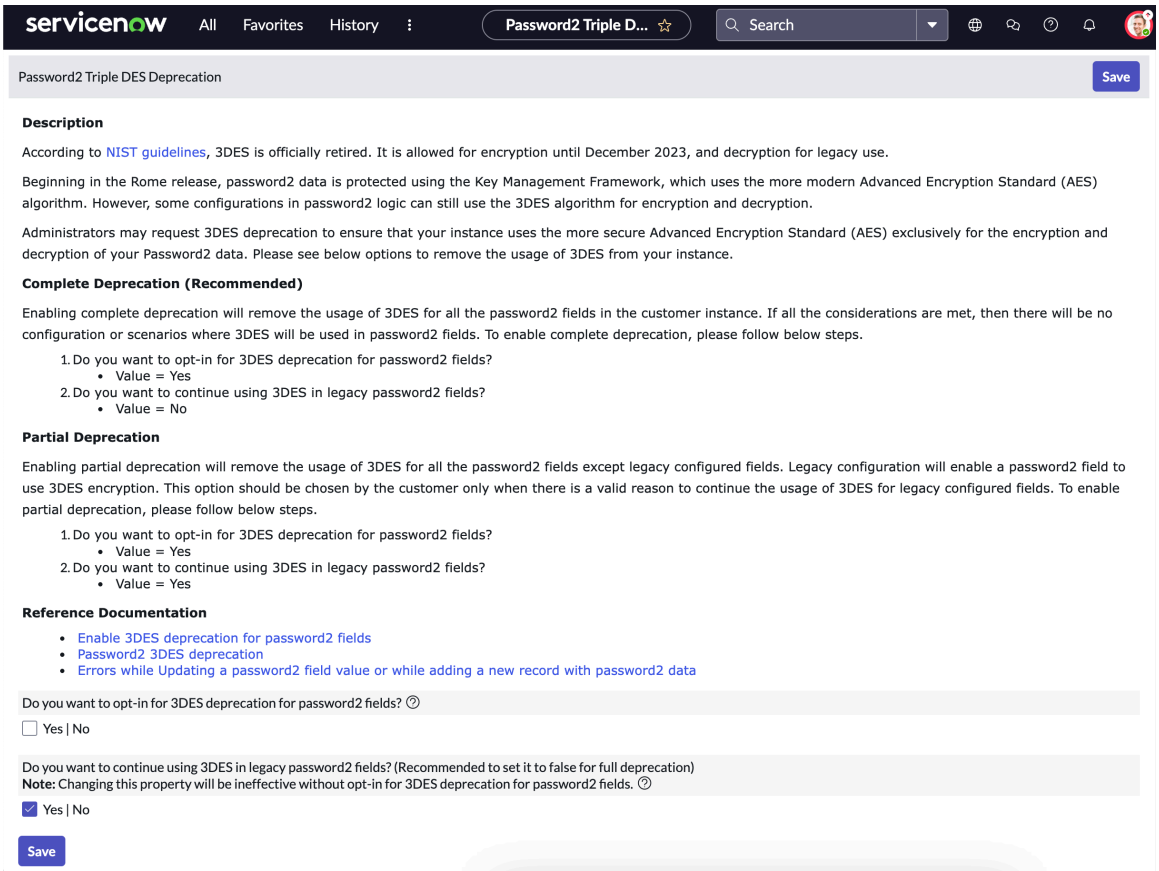
3DES を廃止する方法

上記のユースケースを確認した後、必要に応じて部分的または完全に廃止を有効にします。どちらのオプションでも、次の場所に移動することでフォームにアクセスし、廃止を管理できます すべて > システムセキュリティ > セキュリティコンプライアンス > **Password2** トリプル **DES** の廃止.

> **重要:**
> セキュリティコンプライアンスモジュールを表示してこれらの手順を実行するには、 セキュリティ 管理者に昇格する必要があります。このプロセスの詳細については、「特権ロールへの昇格」を参照してください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



[Password2 トリプル **DES** の廃止 **(Password2 Triple DES Deprecation)]** フォームには、3DES の完全廃止と部分的な廃止の両方のプロセスに関する情報が含まれています。完全または部分的な廃止のオプションを選択し、[保存] を選択します。

完全な廃止

完全な廃止を有効にすると、インスタンスですべての password2 フィールドに対する 3DES の使用が削除されます。すべての前提条件が満たされる場合、password2 フィールドで 3DES が使用される構成またはシナリオはありません。

完全な廃止を有効にするには：

- **[password2** フィールドの **3DES** 廃止をオプトインしますか？] を選択します。
- [従来の **password2** フィールドで **3DES** を引き続き使用しますか？] の選択を解除します。

部分的な廃止

部分的な廃止を有効にすると、従来の構成済みフィールドを除くすべての password2 フィールドで 3DES の使用が削除されます。従来の構成の password2 フィールドでは、引き続き 3DES 暗号化が使用されます。従来の構成済みフィールドに 3DES を引き続き使用する必要がある場合にのみ、このオプションを選択します。

部分的な廃止を有効にするには：

- **[password2** フィールドの **3DES** 廃止をオプトインしますか？] を選択します。
- [従来の **password2** フィールドで **3DES** を引き続き使用しますか？] を選択します。

GlideEncrypter の廃止後

廃止プロセスが完了すると、次の情報がインスタンスに適用されます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

- password2 フィールドでは 3DES 暗号化データの復号化が引き続きサポートされます (ただし、暗号化はサポートされません)。
- password2 フィールドの既存の 3DES 暗号化データは、ユーザーまたはワークフローによってフィールド値が更新されるまで変更されません。
- password2 フィールドの値を更新すると 3DES 暗号化テキストが削除され、AES を使用して KMF で暗号化されたテキストに置き換えられます。
- 場合によっては、パスワードデータの保存時にインスタンスでエラーが表示されます。

  アクションが中止されました：技術的な問題により、パスワード値を保存できません。サポートについては、KB1296997 を参照してください。

  このエラーが表示された場合は、ナレッジベース記事 KB1296997 のサポート情報を参照してください。

キー管理フレームワークリソース交換

ServiceNow® Resource Exchange は、安全な方法でインスタンス間でリソースを交換する機能を提供する KMF の機能です。

用語

Resource Exchangeを使用する場合は、次の用語を参照してください。

Resource Exchange 用語

名前	説明
Resource Exchange	インスタンス間でリソースを交換するプロセス。
Key Exchange (KE)	インスタンス間でキーを交換するプロセス。
キーソースインスタンス (キーソース)	キーを所有するインスタンス。
キーターゲットインスタンス (キーターゲット)	キーを要求するインスタンス。

概要

Resource Exchange は KMF の暗号化 API を使用して、機密性、完全性、認証、および否認防止を提供します。現在、Resource ExchangeはKey Exchange機能をサポートしています。詳細については、「キー管理フレームワークの鍵交換」を参照してください。

キー管理フレームワークの鍵交換

KMF Key Exchange は KMF Resource Exchange のサブセット関数です。Key Exchange は複数のインスタンス間で暗号化されたデータを安全に転送します。

Key Exchange の概要

Key Exchange はインスタンス間でキーを安全に転送します。

KMF Key Exchange は、顧客がインスタンス間で KMF キーを交換するための安全な方法を提供します。アプリケーションのユースケースの 1 つにデータクローンプロセスがあります。Key Exchangeを使用すると、KMF コンポーネントのデータクローン中に暗号化モジュールキーがコピーされます。暗号化モジュール、モジュールキー仕様、およびモジュールアクセスポリシーは、クローンプロセスに含まれます。キーの転送は含まれていません。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Key Exchange の使用

Column Level Encryption に KMF を使用する管理者は、データのクローンを実行するときにKey Exchangeを使用して本番インスタンス間でキーをクローンできます。データのクローン作成では、管理者/ KMF 暗号化マネージャーは次の操作を実行できます。

- すべてのキーを他のインスタンスに交換する。
- 特定のキーを 1 回または定期的に他のインスタンスと交換する。
- ターゲットインスタンスからキーソースインスタンスにオンデマンド要求を送信します。
- 暗号テキストをリキーするためにソースからターゲットにキーを交換する。
  - 要求の有効期限を管理し、要求が期限切れになった場合は、キーを削除するか、鍵交換要求を却下します。
  - 要求が完了してキーがインポートされると、使用したキーは期限切れになり、タイムスタンプが付与されます。
  - ソースのキーで暗号化されたターゲットインスタンスで暗号テキストをリキーします。

サポートされているモード

Key Exchangeは、暗号化モジュールの暗号化仕様レベルでいくつかのモードをサポートしています。

モード	説明
自動 (設定なし、デフォルトの動作)	すべてのキーは、追加の設定なしに、データクローンプロセス中に自動的に送信されます。
設定可能 (1 回限りの設定セットアップ)	管理者は、データクローンプロセス中に送信されるキーを設定します。
手動 (ループ内のユーザー)	管理者は、ターゲットインスタンスのオンデマンド要求をソースに送信します。キーソースインスタンスで管理者が要求を承認する必要があります。
リキー (自動要求)	管理者は、クローンセットアッププロセス中にリキーのオプションを選択します。

鍵交換の設定

Key Management Framework (KMF) は、インスタンスの新規インストールまたはアップグレード時に、サポートされている暗号化モジュールに対する自動鍵交換要求を生成します。 は、インスタンスのデータ暗号化キーをローカルに管理します。

始める前に

キーを持つ暗号化モジュールは、 を使用する Key Exchange前にターゲットインスタンスとソースインスタンスの両方で作成する必要があります。

必要なロール：sn_kmf.cryptographic_manager

このタスクについて

Key Exchange要求はターゲットインスタンスから開始されます。

自動鍵交換は、プロパティがターゲットインスタンスにクローンされるインスタンスをクローンするときにデフォルトで有効になります。KMF とともに、システムプロパティを設定して、インスタンスのクローン中のキーの処理方法を管理します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- 自動鍵交換のオフ：繰り返しクローン要求の *glide_encryption.auto_key_exchange.enabled* プロパティを **false** に設定します。
- 自動鍵交換要求の送信：このプロパティを **true** に設定します。

重要:
ベースシステムプロパティはデフォルトで **true** に設定されています。これは、インスタンスのクローン作成時に自動鍵交換がアクティブ化されることを意味します。または繰り返し鍵交換機能を使用している場合は鍵交換によるリキー暗号テキスト、この値を **false** に設定する必要があります。詳細については「繰り返し鍵交換のチュートリアル」を参照してください。

手順

1. 移動先 すべて > キー管理 > リソース交換要求 > 新規.
2. フォームのフィールドに入力します。

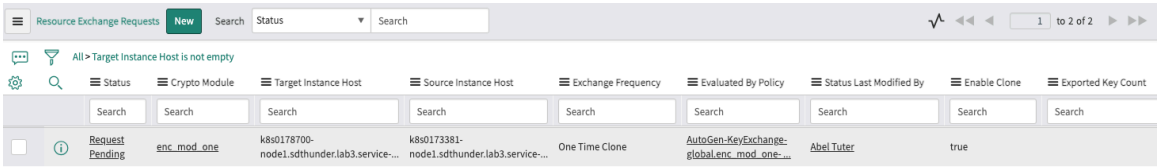
Resource Exchange要求フォームのフィールド

名前	説明
交換頻度	○ アドホック：キーターゲットインスタンスからソースインスタンスへ要求を送信します。ソースのインスタンスの sys_id とホスト情報を入力します。鍵交換のリキーではサポートされていません。 ○ ワンタイムクローン：ソース暗号化仕様からターゲットインスタンスへのキーの 1 回限りの交換。 ○ 繰り返しクローン：定義された繰り返しクローンで、選択したソース暗号化仕様からターゲットインスタンスにキーを交換します。
<Source or Target> インスタンス sys_id	○ アドホック：キーを要求するソースインスタンスの sys_id を入力します。 ○ **1** 回限りのクローン、繰り返しクローン：要求を送信するターゲットインスタンスの sys_id を入力します。 **ヒント:** アプリケーションナビゲーターに「stats.do」と入力してインスタンス ID を見つけます。
<Source or Target> インスタンスホスト	ソースまたはターゲットインスタンスのホストの場所または名前を入力します。 **ヒント:** たとえば 、instanceA.service-now.com
暗号化仕様	暗号化モジュールの暗号化仕様のキーによって、クローンするキーが定義されます。1 回限りのクローン要求と繰り返しのクローン要求の両方で、インスタンスはリソース交換 モジュールアクセスポリシーを自動的に作成します。ポリシーを手動で設定する必要はありません。 **注:** [リストから参照] アイコン ([ ) を選択して、使用可能な暗号化仕様を参照します。
キーのインポート後にリキーを有効にする	自動リキーを有効にするオプション。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

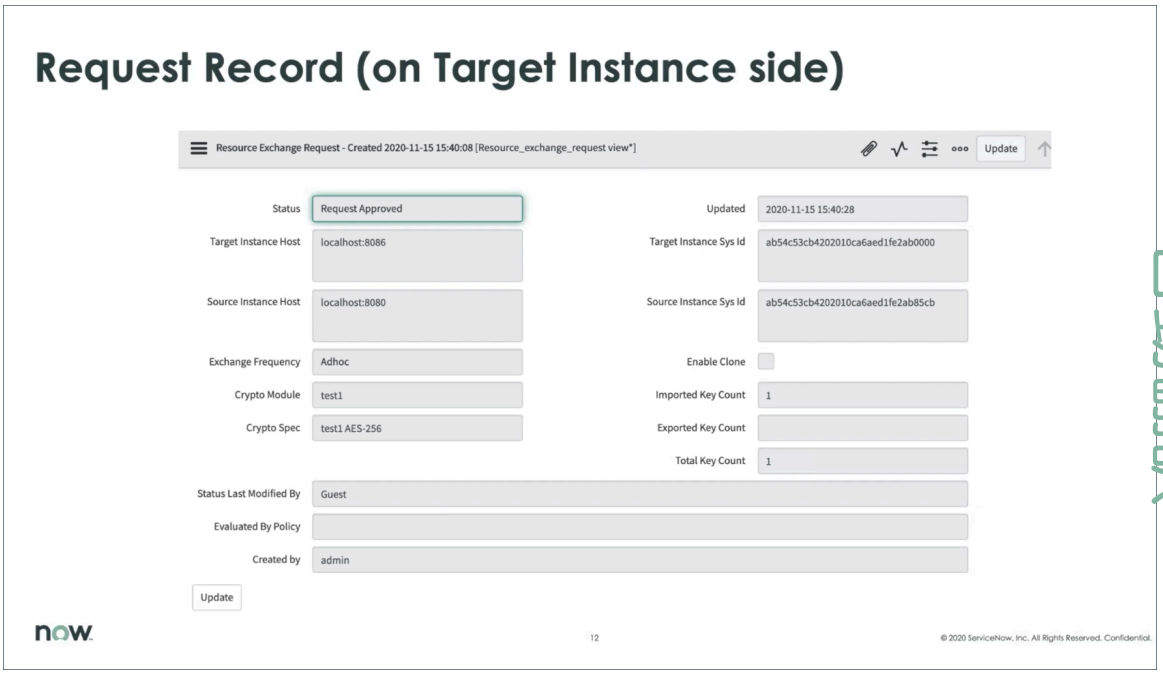
自動翻訳

3. [送信] を選択します。
   成功すると、フォームの上部に確認が表示されます。[要求] テーブルは、ソースインスタンスとターゲットインスタンスの両方で [要求保留中] のエントリで更新されます。要求レコードを開くと、要求のステータス、インポートされたキー数、およびターゲットまたはソースホストの合計キー数が表示されます。



4. 処理待ちの要求がソースインスタンスで受け入れられ、交換が完了します。

   クローン時に、ソースインスタンスのモジュールアクセスポリシーが呼び出され、要求が自動的に承認されて、新しくクローンされたターゲットにキーが送信されます。



タスクの結果
鍵交換が試行された後、非本番インスタンスで *protected.script.values.kmf.rekeyed* システムプロパティが更新されます。このプロパティは、鍵交換が試行された後、システムのプロパティ [sys_properties] テーブルに表示されます。交換されたキーを使用した暗号化が成功した場合、このプロパティの値は **true** です。それ以外の場合、プロパティの値は **false** です。値が false の場合、インスタンスは翌日に暗号化を再試行します。

鍵交換によるリキー暗号テキスト

Resource Exchange は、ソースのキーで暗号化されたターゲットインスタンスで暗号テキストのリキーをサポートします。リキーアクティビティはキーライフサイクルで追跡されます。

概要

Column Level Encryption に KMF を使用する管理者は、データのクローンを実行するときにKey Exchangeを使用して本番インスタンス間で暗号キーのリキーを行えます。リキーにはアクティブなキーが必要であるため、リキーを行うにはまずアクティブなキーをターゲットインスタンスで使用

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

できるようにする必要があります。暗号化ジョブが自動的に作成されて実行されると、ソースキーのローテーションとリキーが行われ、暗号テキストが再暗号化されます。

Key Exchangeを使用して、次の操作を行います。

- リキーの有効期限を設定します。

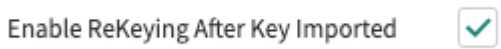
  要求の有効期限が切れている場合、要求は却下され、キーは削除されます。

- ソースインスタンスのキーで暗号化された暗号テキストを自動的にリキーします。

  新しいクローンされた暗号化キーを使用して、ターゲットインスタンスの暗号テキストを再暗号化します。

- リキーの目的はクローンプロセス中に設定され、クローンの一部として自動化されます。
- リキーのアクティビティは、暗号化モジュールの [モジュールキー] タブで追跡されます。キーアクティビティのキーライフサイクルステータスとキーバージョンにアクセスします。詳細については、「キーのローテーション」を参照してください。

Key Exchangeを設定し、[キーのインポート後にリキーを有効にする] チェックボックスを選択してアクティブ化します。詳細については、「鍵交換の設定」を参照してください。



繰り返し鍵交換のチュートリアル

このチュートリアルでは、 と Resource Exchangeを使用してインスタンスで繰り返し鍵交換を設定します。

始める前に

必要なロール：sn_kmf.cryptographic_manager

このタスクについて

この例は、ターゲットインスタンスがホストインスタンスからキーを要求する方法を示しています。

- この手順を実行する前に、インスタンスをクローンする必要があります。詳細については、「システムクローン」を参照してください。
- 自動鍵交換:ベースシステムプロパティ *glide_encryption.auto_key_exchange.enabled* はデフォルトで **true** です。これは、インスタンスのクローン作成時に自動がアクティブ化されることを意味します。プロパティがターゲットインスタンスにクローンされます。
- 自動をオフにするには、プロパティを **false** に設定します。

手順

1. ソースインスタンスで、column_level_encryption を使用して暗号化モジュールを作成するか、既存の暗号化モジュールにアクセスして、Key Exchangeの暗号テキスト暗号化の暗号化フィールド構成を設定します。
   詳細については、「」およびを参照してください。

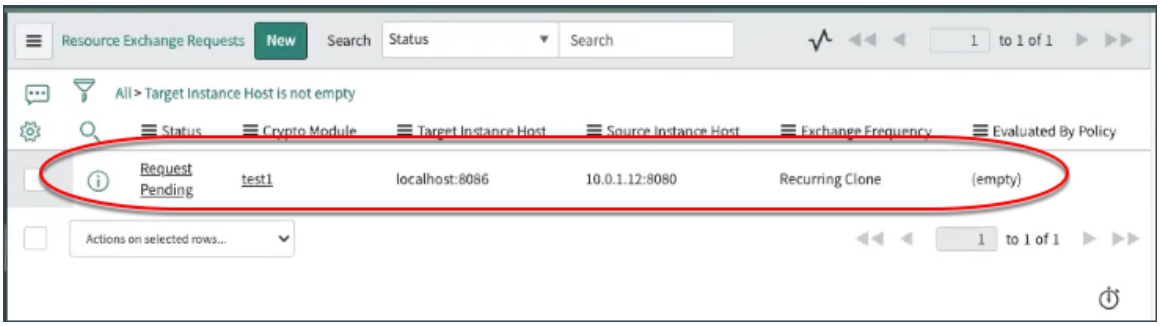
   a. 暗号化モジュールでキーが生成されていることを確認します。

   > **注:**
   > インスタンスは、クローン要求の実行時にモジュールアクセスポリシーを自動的に作成します。

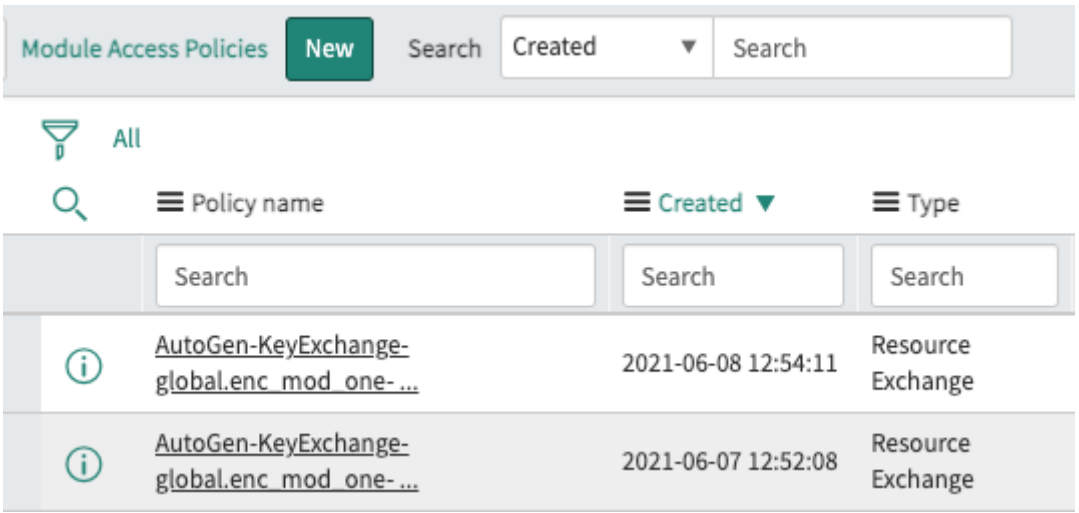
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

2. クローンされたインスタンスから、次の場所に移動します。 キー管理 > リソース交換要求 > 新規.
3. フォームに入力し、 交換頻度として [繰り返しクローン] を選択します。
4. クローンのターゲットインスタンスから、次の場所に移動します。 キー管理 > リソース交換要求.
   ホストインスタンスからの要求がテーブルに表示されます。



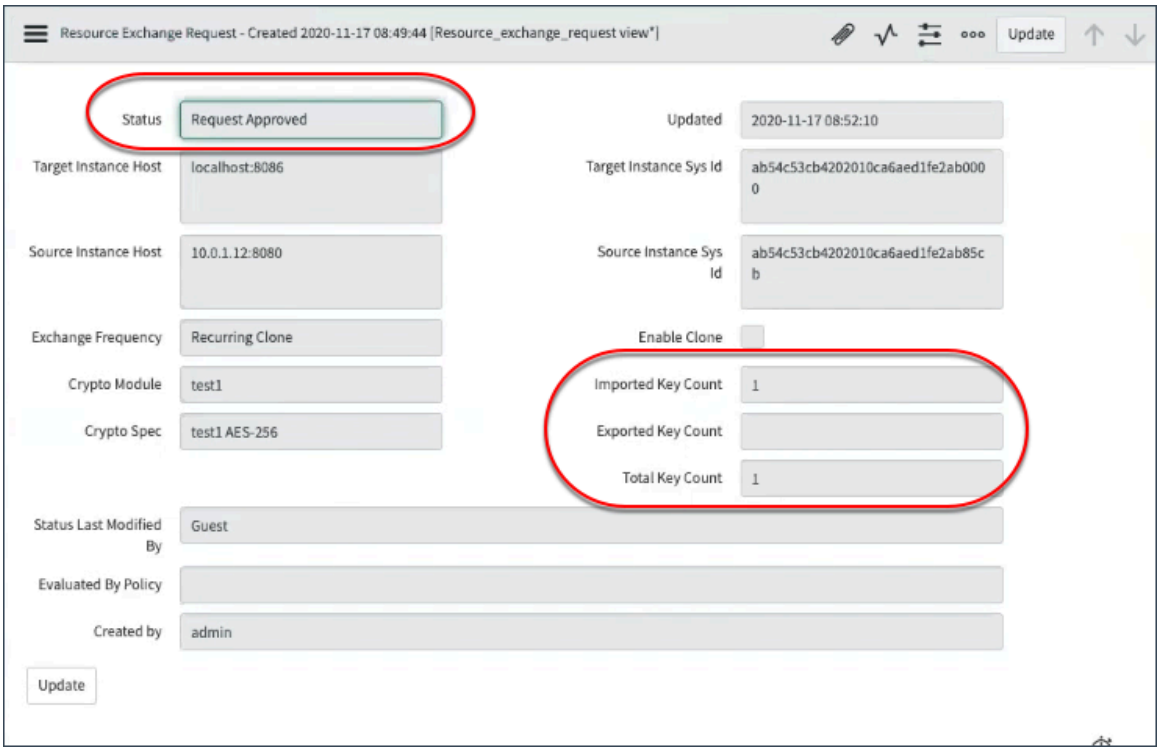
重要:
1 回限りのクローン要求と繰り返しのクローン要求の両方で、インスタンスはモジュールアクセスポリシーを自動的に作成します。ポリシーを手動で設定する必要はありません。クローン時に、ソースインスタンスのこのポリシーが呼び出され、要求が自動的に承認され、新しくクローンされたターゲットにキーが送信されます。



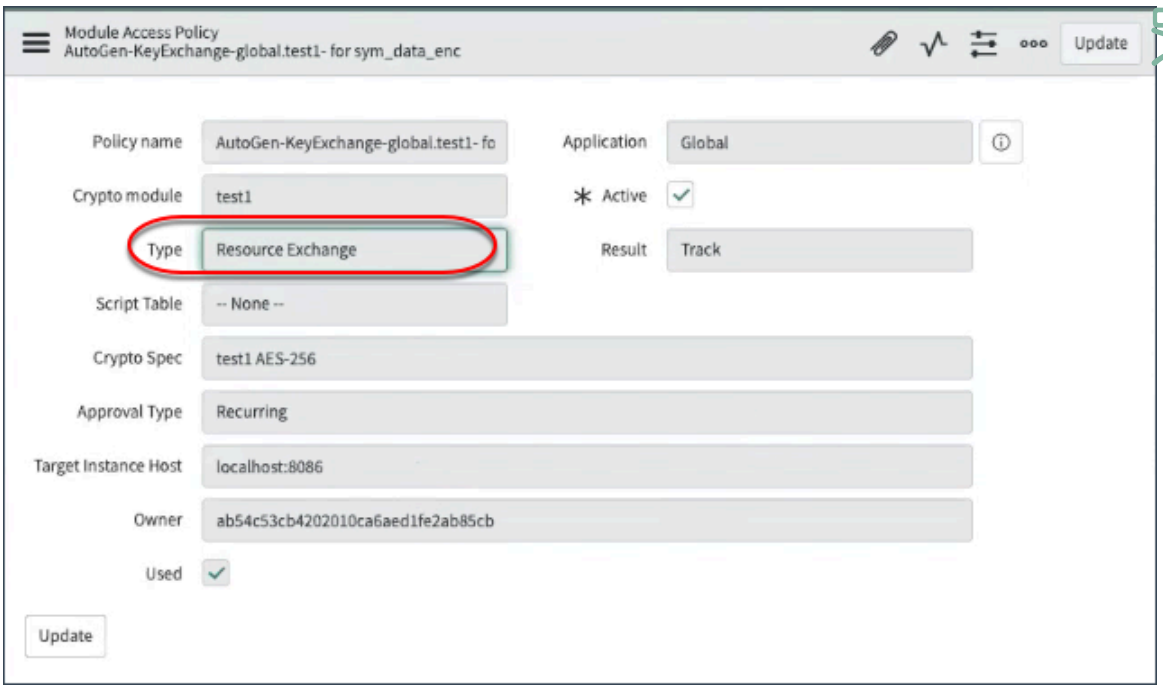
[要求] フォームで、ステータスが [承認された要求] に更新され、[インポートされたキー数] フィールドがレコードに表示されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



5. ホストインスタンスに戻ります。
6. 要求レコードを表示して、エクスポートされたキーの数を確認します。
7. モジュールアクセスポリシーレコードを表示して、[**Type**Resource Exchange] が であることを確認します。



注:
Resource Exchangeは、ターゲットインスタンスの暗号テキストのリキーもサポートしています。詳細については、「」を参照してください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

タスクの結果
鍵交換が試行された後、非本番インスタンスで *protected.script.values.kmf.rekeyed* システムプロパティが更新されます。このプロパティは、システムのプロパティ [sys_properties] テーブルに表示されます。交換されたキーを使用した暗号化が成功した場合、このプロパティの値は **true** です。それ以外の場合、プロパティの値は **false** です。値が false の場合、インスタンスは翌日に暗号化を再試行します。

Column Level Encryption

Column Level Encryption (CLE) (以前の暗号化のサポート) は、ユーザーロールに基づいて暗号化データへのアクセスを許可および拒否します。Column Level Encryption は、追加料金なしで暗号化モジュールを使用する基本的なキー管理を含むように拡張されています。

Column Level Encryption について

注:
以前に設定された暗号化コンテキストは、自動的に暗号化モジュールに変換されます。Column Level Encryption (CLE) は、暗号化のサポートに対する無料のセキュリティ拡張機能です。暗号化オプションの詳細については、「暗号化とキー管理のサブスクリプションバンドル」を参照してください。

列レベルの暗号化の実装は、Now Platformのインスタンスで 1 つ以上の暗号化モジュールを定義することから始まります。このプロセスには、暗号化アルゴリズムの選択と適切な秘密キーの提供が含まれます。機能を使用して後で暗号化されたデータへのアクセスはロールベースで行われ、モジュールはロールに関連付けられています。適切なロールを持たないユーザーには、このフィールドは表示されません。図 1 は、ロールベースの暗号化がどのように機能するかを示しています。

図 **1 –** ロールベースの暗号化の例

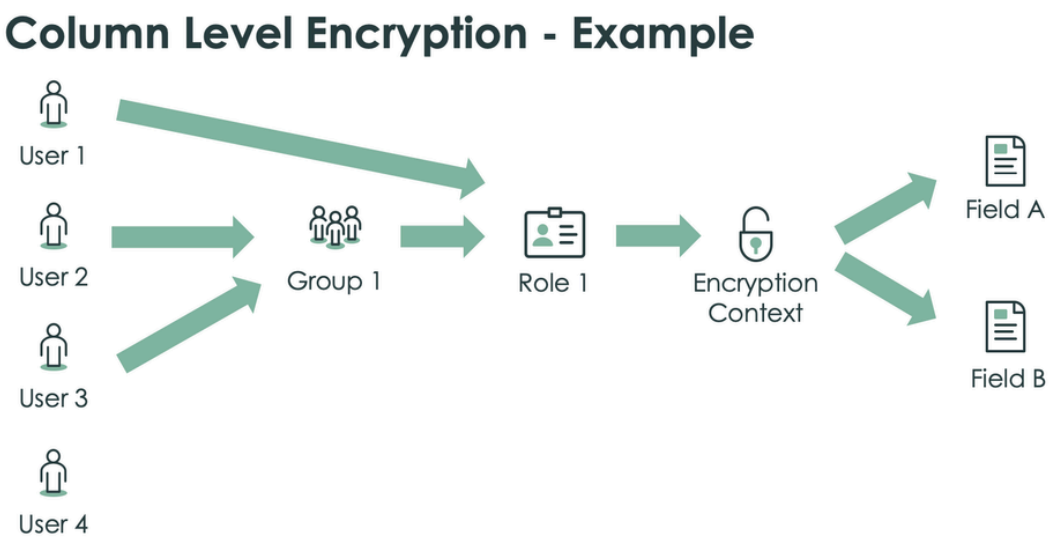


図 1 の関係の結果は次のとおりです。

- ユーザー 1 は、暗号化モジュール 1 へのアクセスを提供するロール 1 のメンバーです。ユーザー 1 は、フィールド A とフィールド B の内容を表示できます。
- ユーザー 2 とユーザー 3 はグループ 1 のメンバーです。グループ 1 はロール 1 のメンバーであるため、グループ 1 の全員が暗号化モジュール 1 にアクセスでき、ユーザー 2 とユーザー 3 がフィールド A とフィールド B の内容を表示できます。
- ユーザー 4 はグループまたはロールのメンバーではないため、暗号化モジュール 1 にアクセスできません。ユーザー 4 はフィールド A またはフィールド B にアクセスできないだけでなく、フォーム上でこれらのフィールドを表示することもできません。リストビューでは、値は空です。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

かなり複雑なロールベースの暗号化も実装できます。

ロールベースのアクセスは、ロールを介して暗号化モジュールを割り当てられたユーザーがそのフィールドにアクセスできるように適切に実装する必要があります。

列レベルの暗号化で使用するすべての顧客暗号化キーは、顧客によって暗号化されたデータが格納されるのと同じ一意のインスタンスデータベースに格納されます。追加のセキュリティ対策として、顧客暗号化キーはそのインスタンスに対して一意のセカンダリキーで再暗号化されます。これにより、インスタンス管理者または ServiceNow による暗号化モジュールの暗号化キーへの直接アクセスが緩和されます。

列レベルの暗号化データはフィルタリングできません。

Column Level Encryption：

- 暗号化されたデータへのアクセスは、ユーザーロールによって決まります。
- 暗号化アルゴリズムの強度は、AES-128 または AES-256 から選択できます。
- 文字列テキスト、日付フィールドと日付/時刻フィールド、添付ファイル、および URL を暗号化できます。
- 暗号化モジュールは等価性保存暗号化を提供します。

列レベル暗号化エンタープライズ は次の追加機能をサポートしています。

- 顧客指定のキー
- キーアクセスにより、モジュールやキーへのアクセス権を持つユーザーセッションが、他のバックエンドプロセスやシステムユーザープロセスにアクセスできるようになります。
- スクリプト、Resource Exchange、およびアプリのアクセス
- 高度な添付ファイルのサポート。
- アプリケーションプログラミングインターフェイス (API) によるアクセスを利用できます。
- 順序保存の暗号化または標準の非決定的暗号化はサポートされていません。

Standard および **Enterprise** エディション

列レベルの暗号化は、Standard バージョンおよび Enterprise バージョンで使用できます。Column Level Encryption Enterprise は、多数のモジュールとモジュールアクセスポリシーに加えて、追加機能を提供する有料プラグインです。

バージョン別の **Column Level Encryption** の機能

Column Level Encryption	Column Level Encryption Enterprise
• 暗号化されたデータへのアクセスは、ユーザーロールによって決まります • 最大 5 つのモジュールとモジュールアクセスポリシー (MAP) のサポート • AES-128 および AES-256 暗号化アルゴリズム • 文字列テキスト、日付フィールドと日付/時刻フィールド、添付ファイル、および URL の暗号化。 • 暗号化モジュールは等価性保存暗号化を提供します。	左にリストされている機能に加えて、Column Level Encryption Enterprise は次の追加機能をサポートしています。 • 5 つ以上のモジュールとモジュールアクセスポリシー (MAP) のサポート • ジャーナル、HTML、翻訳済みフィールドなどの追加のフィールドタイプの暗号化 • 構成可能な自動キーローテーション • 顧客指定のキーデータ暗号化キーのキーライフサイクル全体を管理します。必要に応じ

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

バージョン別の **Column Level Encryption** の機能 (続く)

Column Level Encryption	Column Level Encryption Enterprise
• クリアテキスト値を返し、暗号化フィールドに暗号化されたデータを挿入できる、更新された getDisplayValue() および setDisplayValue() API	て、環境内で生成されたデータ暗号化キーを安全に交換できます。 • 短期暗号化キー • getValue() および setValue() API を更新しました。

この製品の Enterprise バージョンの詳細については、「Column Level Encryption Enterprise」を参照してください。

暗号化方法

Column Level Encryption を使用するフィールドは次のとおりです。

- 新規または既存の [暗号化テキスト] フィールド。
- 暗号化されたフィールド設定レコードに含まれる文字列、日付、日付/時刻、または URL フィールド。

[暗号化フィールドの構成] テーブル [*sys_platform_encryption_configuration*] には、Column Level Encryption で暗号化された各フィールドのレコードが含まれています。このテーブルにより、セキュリティ管理者は Column Level Encryption を使用するインスタンス内のすべてのフィールドを監視できます。

注:
アップグレード時に、既存のすべての暗号化テキストフィールドに対して暗号化フィールドの構成レコードが作成されます。新しい暗号化テキストフィールドが追加されると、暗号化フィールドの設定レコードがデフォルトで作成されます。

暗号化フィールドの構成では、次のいずれかの方法を使用してフィールドを暗号化できます。

メソッド	説明
単一暗号化モジュール	フィールドは [暗号化モジュール] フィールドで定義された暗号化方法で暗号化されます。暗号化モジュールへのアクセス権がないユーザーは、フィールド値を表示または更新できません。
複数暗号化モジュール	フィールドは、そのフィールドにデータを入力する最初のユーザーの暗号化モジュールで暗号化されます。ユーザーが 2 つ以上の暗号化モジュールを持っている場合、暗号化モジュールセレクターで定義されたモジュールが使用されます。暗号化モジュールはレコードごとに設定されるため、リストのフィールドにはさまざまな暗号化モジュールが含まれる可能性があります。ただし、1 つのレコード内では、フィールドは 1 つのモジュールでのみ暗号化できます。 [暗号化テキスト] フィールドが作成されると、複数暗号化モジュール方式で暗号化フィールドの構成が作成されます。[暗号化テキスト] フィールドと複数暗号化モジュールメソッドで暗号化されたフィールドは、同じように動作します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

メソッド	説明
	注: 複数の暗号化モジュールメソッドを使用する場合は、一括暗号化は利用できません。

暗号化されたデータへのアクセス

暗号化モジュールは、暗号化されたデータへのアクセスを決定します。Security_admin ユーザーは、関連するロールをユーザーに付与することで、ユーザーに暗号化モジュールのアクセスポリシーを付与できます。

ロールの割り当てを監視するために、顧客またはプロフェッショナルサービスはセキュリティ対策を設定できます。たとえば、暗号化モジュールに関連付けられたロールがユーザーに付与されるたびに、指定された暗号化マネージャーにメールを送信できます。

注:
代理操作によって、ユーザーが使用できる暗号化モジュールが変更されることはありません。代理操作中であっても、最初に使用可能になっているのは暗号化モジュールのみです。この機能は、「」で Vancouver紹介されています。

アクセスレベル	単一暗号化モジュールメソッドを使用したフィールドへのデータアクセス	複数暗号化モジュールメソッドを使用したフィールドへのデータアクセス
暗号化モジュールを持たないユーザー	フォームでは暗号化フィールドが非表示にされます。リストビューでは、フィールドのデータが復号化されていても、フィールドは空白で表示され、編集できません。	フォームでは暗号化フィールドが非表示にされます。リストビューでは、フィールドのデータが復号化されていても、フィールドは空白で表示され、編集できません。
1 つの暗号化モジュールを持つユーザー	フィールドを使用するには、暗号化フィールドの構成で定義された暗号化モジュールにアクセスする必要があります。ユーザーが暗号化モジュールにアクセスできない場合、フォームではフィールドが非表示にされます。リストビューでは、フィールドは空白で表示され、編集できません。 • フィールドにデータがない場合： ○ ユーザーが暗号化モジュールにアクセスできる場合は、フォームにフィールドが表示されます (UI ポリシーで防止されていないと仮定)。 ○ 暗号化モジュールへのアクセス権を持つユーザーは、空のフィールドを表示して更新できます。 ○ フィールドに入力したデータは暗号化フィールドの構成で定義された暗号化モジュールで暗号化されます。 • フィールドにデータがある場合：ユーザーが暗号化モジュールにアクセスできる場合、ユーザーはフィールドのデータを表示して編集できます。	ユーザーは、暗号化フィールドで暗号化モジュールを自動的に使用します。 • フィールドにデータがない場合： ○ フォームにフィールドが表示されます (UI ポリシーによって禁止されていないことが前提)。 ○ 暗号化モジュールを持つユーザーは、空のフィールドを表示して更新できます。 ○ フィールドにデータを入力すると、現在選択されている暗号化モジュールを使用してデータが暗号化されます。 • フィールドにデータがある場合：ユーザーがフィールドの暗号化に使用される暗号化モジュールにアクセスできる場合、ユーザーはフィールドを表示して編集できます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

アクセスレベル	単一暗号化モジュールメソッドを使用したフィールドへのデータアクセス	複数暗号化モジュールメソッドを使用したフィールドへのデータアクセス
2 つ以上の暗号化モジュールを持つユーザー	フィールドを使用するには、暗号化フィールドの構成で定義された暗号化モジュールにアクセスする必要があります。ユーザーが暗号化モジュールにアクセスできない場合、フォームではフィールドが非表示にされます。リストビューでは、フィールドは空白で表示され、編集できません。 • フィールドにデータがない場合： ○ ユーザーが暗号化モジュールにアクセスできる場合は、フォームにフィールドが表示されます (UI ポリシーで防止されていないと仮定)。 ○ 暗号化モジュールへのアクセス権を持つユーザーは、空のフィールドを表示して更新できます。 ○ フィールドに入力したデータは暗号化フィールドの構成で定義された暗号化モジュールで暗号化されます。 • フィールドにデータある場合： ○ ユーザーが暗号化モジュールにアクセスできる場合、ユーザーはフィールドを表示して編集できます。 ○ フィールドは、常に元の暗号化モジュールを使用してフィールドへの変更を暗号化します。この動作は、2 つ以上の暗号化モジュールを持つユーザーがフィールドの暗号化モジュールを変更できないようにするのに役立ちます。	ユーザーは、ようこそバーの暗号化モジュールセレクターから暗号化モジュールを選択できます。 • フィールドにデータがない場合： ○ フォームにフィールドが表示されます (UI ポリシーで防止されていないと仮定)。暗号化モジュールを持つユーザーは、空のフィールドを表示して更新できます。 ○ フィールドにデータを入力すると、現在選択されている暗号化モジュールを使用してデータが暗号化されます。 ○ フィールドは、常に元の暗号化モジュールを使用してフィールドへの変更を暗号化します。この動作は、2 つ以上の暗号化モジュールを持つユーザーがフィールドの暗号化モジュールを変更できないようにするのに役立ちます。 • フィールドにデータある場合： ○ ユーザーがフィールドの暗号化に使用される暗号化モジュールにアクセスできる場合、ユーザーはフィールドを表示して編集できます。 ○ フィールドは元の暗号化モジュールを使用して、フィールドへの変更を暗号化します。この動作は、複数の暗号化モジュールを持つユーザーがフィールドの暗号化モジュールを変更できないようにするのに役立ちます。

サポートされている構成情報

- 次のフィールド タイプを暗号化できます。
  - 添付ファイル
  - 日付
  - 日付/時刻
  - 文字列テキスト
  - URL

> **注:**
> エンタープライズでは、さらに多くのフィールドタイプを使用できます。詳細については、「」を参照してください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- モジュールはロールに関連付けられ、ロールはユーザーに関連付けられているため、ユーザー以外のセッションからキーにアクセスすることはできません。システムユーザーとして実行されているもの、またはユーザーセッションを持たないスケジュール設定済みジョブは、キーにアクセスしてデータを暗号化または復号化することはできません。
- 「値」または「表示値」にアクセスすることができます。
  - [値] を選択すると、暗号テキストが返されます。
  - 適切なロールを持っている場合は、[表示値] を選択するとクリアテキストが返されます。

  アプリケーションレイヤーの多くのスクリプトは、この区別を無視して値を使用するようにスクリプト化されています。表示値を使用するようにスクリプトを変更しないと、データは暗号化も復号化もされません。

添付ファイルの暗号化

デフォルトでの添付ファイルの暗号化

Column Level Encryption を使用しているお客様の場合、アクティブな暗号化フィールドの構成 (EFC) タイプ `Attachment` のテーブルの添付ファイルはデフォルトで暗号化されています。

EFC 構成で定義されているこのデフォルトの暗号化は、管理者がこれらのテーブルのアップロード時に添付ファイルを暗号化する必要があることを手動で宣言する必要がないことを意味します。

デフォルトの暗号化のオプトアウト

EFC構成に基づいてデフォルトで添付ファイルを暗号化したくない場合は、サポートに連絡してこのオプションをオプトアウトできます。

この機能をオプトアウトするには、サポートを含むサポートケースを作成し、ケースレコードのコメントに次のステートメントを含めます。

「私[顧客名]は、添付ファイルの推奨されるセキュリティのベストプラクティスをオフにするように求めていること、および[顧客の会社]がアプリケーションでの暗号化されていない添付ファイルの構成と使用に関連する追加のリスクを負うことを理解しています。」

暗号化フィールドのフィルタリングと検索

暗号化テキストフィールドまたは暗号化フィールドの構成が適用されたフィールドをフィルターの左オペランドとして選択した場合、次の演算子を利用できます。

- 次の値に等しい
- ではない
- は、空
- は空でない

日付フィールドの場合、日付ピッカーを使用して日付を指定します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

日付/時刻フィールドの場合、日時ピッカーを使用して日時を指定します。

暗号化モジュールを持つユーザーが等価性をフィルタリングするか、リスト内の値を検索した場合:

- ユーザーが使用できる暗号化モジュールで暗号化された値のみが返されます。
- 演算子 [は空] および [は空でない] では、一致するすべてのレコードが返されます。現在のユーザーが使用できない暗号化モジュールで暗号化されたフィールドは空で表示されます。

ユーザーが暗号化モジュールを持っていない場合、レコードは返されません。

リストでは [この値で絞り込み] および [この値を除外] オプションがサポートされています。完全一致のみが返されるか、フィルタリングで除外されます。

> **注:**
> 条件フィルターでの暗号化フィールドの追加は、UI ポリシーやビジネスルールなどのスクリプトでサポートされます。

暗号化フィールドからのデータのエクスポート

リストまたはフォーム内の暗号化フィールドをファイル形式でエクスポートすると、暗号化モジュールによって暗号化されたフィールドのみが、エクスポートされたドキュメントに表示されます。使用する暗号化モジュールは、現在のユーザーが使用できる必要があります。

リストビューからの暗号化データのエクスポートを無効にするには、*glide.encryption.export_encrypted_data.allowed* システムプロパティを追加して、値を **false** に設定します。

システムテーブルの暗号化

Column Level Encryption は現在、システムテーブル (**sys_** で始まるテーブル) のフィールドと添付ファイルの暗号化をサポートしていません。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ユーザーが暗号化されていないファイルを添付できないようにする

暗号化モジュールキーにアクセスできるユーザーが暗号化されていない添付ファイルを添付できないようにするには、com.glide.encryption.enable_attachment_key_uiプロパティを変更します。

始める前に

必要なロール：security_admin

次の手順を実行するには、security_admin ロールに昇格する必要があります。詳細については、「特権ロールへの昇格」を参照してください

デフォルトでは、暗号化モジュールキーにアクセスできるユーザーは、暗号化されていない添付ファイルをアップロードできます。この動作を変更するには、`com.glide.encryption.enable_attachment_key_ui` システムプロパティを使用します。

添付すると、マルチモジュール暗号化フィールド構成を持つレコードの UI ピッカーがユーザーに表示されます。このプロパティを false に設定すると、添付ファイルを暗号化しないオプションがユーザーに表示されなくなります。

手順

1. 移動先 すべて > システムプロパティ > すべてのプロパティ.
2. [システムプロパティ] リストで、当該のシステムプロパティを検索して開きます。
3. プロパティ の値をfalse に設定します。

Column Level Encryption のチュートリアル

このツアーでは、テーブルフィールドまたは添付ファイルを暗号化するために必要な Column Level Encryption (CLE) セットアップの簡単な概要を説明します。☒ィールド暗号化モジュール、モジュールアクセスポリシー、および暗号化フィールドの設定のステップについても説明します。ツアーには、詳細なドキュメントのリンクと ServiceNow University Column Level Encryption の概要のコースが含まれています。☒

始める前に

必要なロール：sn_kmf.crypto_manager または security_admin

> **注:**
> Next Experience が有効になっている場合、チュートリアルはまだ利用できません。

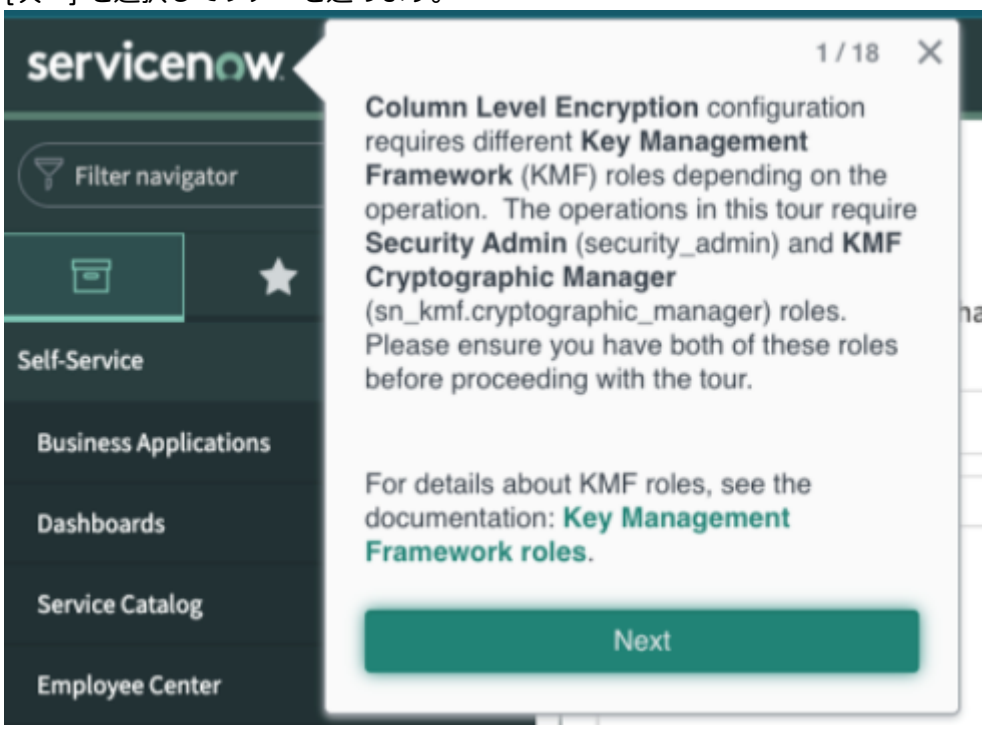
手順

1. インスタンスの **$pa_dashboards_overview.do** UI ページに移動します。
   例:http://yourcompany.servicenow.com/nav_to.do?uri=%2F$pa_dashboards_overview.do あなたの会社をインスタンスの名前に置き換えます。
2. 左上隅にある [ヘルプを表示] アイコン ( ) を開きます。
3. サイドバーの下部にある [ガイドを表示] を選択します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

4. [次へ] を選択してツアーを進めます。



Column Level Encryption Enterprise

列レベル暗号化エンタープライズ (CLE) では、 Key Management Framework (KMF) を使用して、インスタンスでのフィールドと添付ファイルの暗号化方法と復号化方法を完全にカスタマイズおよび管理できます。列レベル暗号化エンタープライズ を利用するには、サブスクリプションが必要です。

重要:
このトピックでは、エンタープライズバージョンの Column Level Encryption について説明します。CLE の標準バージョンの詳細、または 2 つのバージョンの違いについては、を参照してください Column Level Encryption。

列レベル暗号化エンタープライズ は Column Level Encryption (CLE) を前提としており、Key Management Frameworkとそのキー管理機能の完全なサポートを使用します。列レベル暗号化エンタープライズ は、アプリケーションレベルのフィールド暗号化のためのキー保護とキーライフサイクル管理を提供します。すべてのキーは、最終的に FIPS 140-2-L3 ハードウェアセキュリティモジュール (HSM) に基づくキーラッピング階層で保護されます。

列レベル暗号化エンタープライズ を使用すると、サポートされているフィールドを NIST 800-57 プラクティスに従って暗号化および復号化する方法を管理できます。また、適切なキーの保護と管理のための統合を含む、最新バージョンのフィールドレベルの暗号化を使用します。

具体的には、列レベル暗号化エンタープライズ は KMF 暗号化モジュールを使用して、サーバー側の暗号化をより詳細に制御できるようにします。KMF は、キー階層とエンベロープ暗号化を使用して、適切なデータ暗号化キーを保護します。インスタンスは、設定した暗号化モジュールでデータを暗号化します。各モジュールのアクセスポリシーを作成してから、暗号化仕様とアクセスポリシーを設定し、キーライフサイクル管理コントロールを制御できます。

列レベル暗号化エンタープライズ は、以下に基づくモジュールアクセスポリシーをサポートしています。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- スコープ
- ロール
- スクリプト
- リソース交換
- システムユーザー

詳細については、「モジュールアクセスポリシーを作成する」を参照してください。

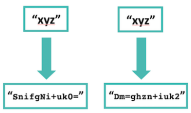
注:
Column Level Encryption のサポートされている機能と、アップグレードして 列レベル暗号化エンタープライズ エンタイトルメントに登録する方法の詳細については、「暗号化とキー管理のサブスクリプションバンドル」を参照してください。

暗号化の用語

用語	説明
キー管理 	キー管理のサポート 列レベル暗号化エンタープライズ の基礎は Key Management Framework (KMF) です。 次の機能が得られます。 • キーのライフサイクル管理 • キーロテーション詳細については、「キーのローテーション」を参照してください。 • FIPS 140-2-L3 ハードウェアセキュリティモジュール (HSM) によるキーの保護と生成 • ロールと職務の分離 • 本番インスタンスと非本番インスタンスなどのインスタンス間でデータ暗号化キーを安全に転送します。 • キーラッピングを使用した顧客指定のキー (CSK) • 非決定的暗号化 • 一括暗号化/復号化 • キーのアクセス/使用の監査 詳細については、「キー管理フレームワークの理解」を参照してください。
顧客指定のキー 	顧客指定のキーのサポート 列レベル暗号化エンタープライズ の最大のメリットの 1 つは、暗号化に独自のキーを使用できることです。管理者は、指定されたキーを使用するか、独自の顧客指定のキー (CSK) Now Platform を暗号化に使用するServiceNowかを選択できます。 キーのライフサイクルを管理し、キーの取り消し、ローテーション、および無効化のタイミングを決定することもできます。顧客指定のキーを有効にして暗号化モジュールを作成した後、トークンと短期公開キーをダウンロードします。トークンと公開鍵を使

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

用語	説明
	用してキーをラップし、インスタンスにアップロードします。顧客指定のキーを使用するには、および顧客指定のキーのプロパティを設定するを参照してくださいキータイプを選択するためにフィールドの暗号化を設定する。
Column Level Encryption	フィールドの暗号化と添付ファイルの暗号化の両方をサポート フィールドの暗号化と添付ファイルの暗号化はどちらも、暗号化フィールド構成を介して暗号化モジュールとアクセスポリシーを使用します。暗号化フィールド構成フォームを使用して、列の暗号化タイプまたは添付ファイルの暗号化を選択します。詳細とサポートされているフィールドタイプについては、「暗号化フィールド構成を設定する」を参照してください。
非決定的暗号化 	非決定的暗号化のサポート 列レベル暗号化エンタープライズ は、セキュリティ強化のために非決定的暗号化をサポートしています。システムが同じデータを複数回暗号化する場合、暗号化テキストは毎回異なります。非決定的暗号化は、暗号ブロックチェーン (CBC) を使用した AES 暗号化で使用できます。 この機能は、暗号化仕様のアルゴリズム定義ステージの等価性保存オプションで有効にできます。暗号化モジュールの暗号化仕様を作成し、キーを暗号化し生成するためのアルゴリズムを定義します。 暗号化操作に使用するメカニズムを定義し、非決定的暗号化を有効にする方法の詳細については、「暗号化モジュールを作成する」を参照してください。
Resource Exchange	Resource Exchange 列レベル暗号化エンタープライズ は KMF 暗号化 API を使用してインスタンス間を保護し、機密性、完全性、認証、および否認防止を提供します。Resource Exchange は、安全な方法でインスタンス間でリソースを交換する機能を提供する KMF 機能です。詳細については、「キー管理フレームワークリソース交換」を参照してください。

注:
列レベル暗号化エンタープライズ を有効にしない場合でも、CLE を使用できます。Column Level Encryption モジュールは、ユーザーロールに基づいて暗号化データへのアクセスを許可および拒否します。詳細については、「Column Level Encryption」を参照してください。

列レベル暗号化エンタープライズ はオンプレミスの顧客をサポートしています。Domain Separation はサポートされていません。

追加のモジュールとモジュールアクセスポリシーのサポート

の列レベル暗号化標準バージョンは、5 つのモジュールとモジュールアクセスポリシー (MAP) に制限されています。 は、より多くのモジュールと MAP をサポートしています。 列レベル暗号化エンタープライズ

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

サポートされるフィールド情報

次のフィールドタイプを暗号化できます。

- 添付ファイル
- 日付
- 日付/時刻
- メール
- HTML
- ジャーナル
- ジャーナル入力
- ジャーナルリスト
- 電話
- 文字列テキスト
- 翻訳 (変換) 済みフィールド
- 翻訳された HTML
- 翻訳されたテキスト
- URL

添付ファイルの暗号化

デフォルトでの添付ファイルの暗号化

Column Level Encryption を使用しているお客様の場合、アクティブな暗号化フィールドの構成 (EFC) タイプ `Attachment` のテーブルの添付ファイルはデフォルトで暗号化されています。

EFC 構成で定義されているこのデフォルトの暗号化は、管理者がこれらのテーブルのアップロード時に添付ファイルを暗号化することを手動で宣言する必要がないことを意味します。

デフォルトの暗号化のオプトアウト

EFC 構成に基づいてデフォルトで添付ファイルを暗号化したくない場合は、ServiceNow サポートに連絡してこのオプションをオプトアウトできます。

この機能をオプトアウトするには、ServiceNow サポートでサポートケースを作成し、ケースレコードのコメントに次のステートメントを含めます。

「I [顧客名], understand that I am asking ServiceNow to turn off a recommended security best practice for attachments, and that [customer company] assumes any additional risk related to their configuration and use of unencrypted attachments in the ServiceNow application.」

API サポート

列レベル暗号化エンタープライズ は、暗号化フィールドに暗号化されたデータを挿入できるように、setDisplayValue() および setValue() API を更新します。また、getDisplayValue() と getValue() がクリアテキスト値を返すようにもなります。

次のスクリプトは、インシデントの簡単な説明が暗号化されている場合の API の変更を示しています。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

```
var gr = new GlideRecord('incident'); //creates a new incident
gr.setValue('short_description','test123'); //sets the value to test123
var sys_ID = gr.insert(); //inserts the record in the Incident table.
gs.info(gr.getValue('short_description')); //displays the unencrypted value
```

getValue() を使用して暗号化テキストを取得すると、スクリプトで暗号テキストを返されなくなります。スクリプトは、ユーザーが暗号化モジュールにアクセスできるという想定で、プレーンテキストを返します。ユーザーが暗号化モジュールにアクセスできない場合、 getValue() は暗号テキストを返します。

Column Level Encryption Enterprise のアクティブ化

サブスクリプションを購入すると、列レベル暗号化エンタープライズ プラグイン (com.glide.now.platform.encryption) をアクティブ化できます。

始める前に
必要なロール：admin

注:
このドキュメントは、Column Level Encryption Enterprise のインストールに関するものです。Column Level Encryption の標準バージョンは、デフォルトでインスタンスに含まれています。

このタスクについて
次のアイテムは、列レベル暗号化エンタープライズ プラグイン (com.glide.now.platform.encryption) でインストールまたは変更されます。

- 暗号化のサポート (com.glide.encryption) プラグインもアクティブ化されます。

  注:
  Key Management Framework (com.glide.kmf.global) プラグインはデフォルトで既にアクティブ化されています。

- glide_encryption.set_value_support_cle.disabled プロパティを **false**に設定すると、SetValue 機能がオンになります。SetValue がサポートされると、setDisplayValue() と setValue() API の両方で暗号化データがサポートされます。また、getDisplayValue() と getValue() の両方でクリアテキスト値を返すこともできます。
- 次の 2 つのジョブスケジュールが有効にされます。

  - **autoKeyMigration**：暗号化コンテキストキーを Key Management Framework (KMF) 暗号化モジュールキーに移行します。
  - **autoDataMigration**：既に暗号化されているデータを KMF 暗号化モジュールキーを使用するように移行します。

  管理者は、ジョブスケジュールをいつ実行するかを変更できます。また、いつでも一時停止または再開できます。

手順

1. 移動先 すべて > システムアプリケーション > 利用可能なすべてのアプリケーション > すべて.
2. フィルター条件と検索バーを使用して、*Platform Encryption - com.glide.now.platform.encryption* プラグインを検索します。

   名前または ID でプラグインを検索できます。プラグインが見つからない場合は、ServiceNow 担当者から要求する必要があります。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

3. [インストール] を選択して、[プラグインをアクティブにする] ダイアログボックスで、[アクティブ化] をクリックします。

   注:
   ドメイン分離と代理管理者がインスタンスで有効になっている場合、管理ユーザーはグローバルドメインに含まれている必要があります。それ以外の場合、次のエラーが表示されます： 別の操作が実行されているため、アプリケーションのインストールは利用できません：<プラグイン名> のプラグインの有効化。

Column Level Encryption Enterprise への移行

ジョブスケジュールにより、キーと暗号化データが暗号化のサポートから 列レベル暗号化エンタープライズ に移行します。

ジョブスケジュールを確認するには、次の場所に移動します。 システムセキュリティ > 高セキュリティ設定 > セキュリティジョブ:

- **autoKeyMigration**：暗号化コンテキストキーを Key Management Framework (KMF) 暗号化モジュールキーに移行します。
- **autoDataMigration**：既に暗号化されているデータを KMF 暗号化モジュールキーを使用するように移行します。

ジョブスケジュールをいつ実行するかを変更できます。また、いつでも一時停止または再開できます。

次に移動して、暗号化フィールド構成で新しく移行したモジュールキーが使用されていることを確認します システムセキュリティ > フィールド暗号化 > 暗号化フィールドの設定. 次のアイテムを探します。

- [メソッド] フィールドは単一モジュールです。
- [暗号化モジュール] フィールドには、自動的に作成される暗号化モジュールの名前が入力されます。そのモジュールとモジュールアクセスポリシーを確認できます。どちらもアクティブで、公開されています。

Column Level Encryption Enterprise とシステムクローン

列レベル暗号化 Enterprise がインスタンスにインストールされている場合、新しいフィールド暗号化モジュール暗号化キーが、クローンプロセスの一部としてターゲットクローンインスタンスに自動的に生成されます。これらのキーは、ユーザーがアクセス権を持ち、まだキーを持っていないすべてのモジュールに対して生成されます。

このため、ターゲットクローンインスタンスのフィールド暗号化モジュールには、次の 2 つのモジュール暗号化キーが存在する場合があります。

- アクティブなモジュール暗号化キー。これは、ユーザーがモジュールにアクセスできて、以前のキーがない場合に、クローン後に生成される新しいキーです。
- 非アクティブ化された暗号化モジュールキー (自動キー交換転送から)

  アクティブなモジュール暗号化キーは、必要に応じてターゲットクローンインスタンスで挿入されたデータを暗号化するために使用されます。非アクティブ化されたモジュールは、システムクローンの一部としてクローン作成された既存のデータを復号化するために使用されます。

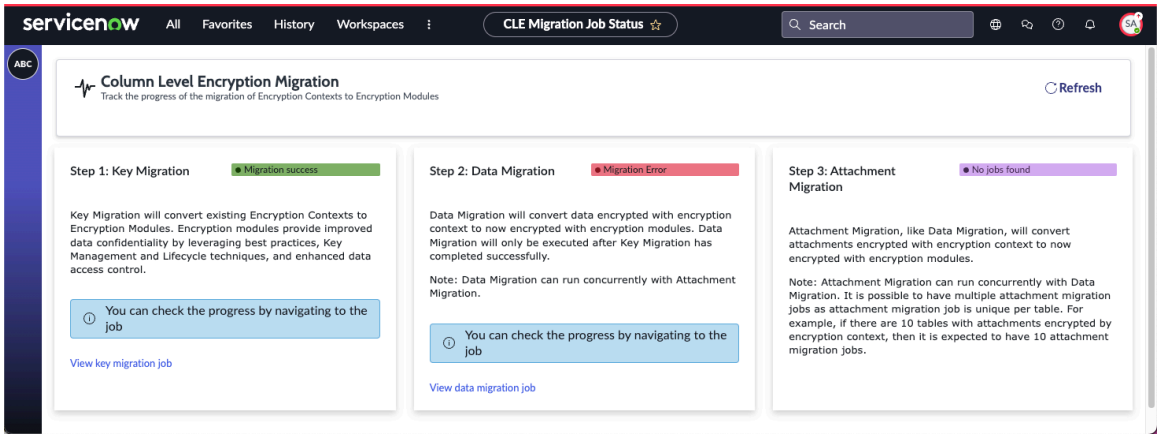
  単一のキーを使用してすべてのデータを復号化および暗号化するには、モジュールのリキージョブを実行します。モジュールのリキージョブの詳細については、「一括暗号化、復号化、およびリキージョブをスケジュールする」を参照してください。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

Column Level Encryption の移行ステータスページ

移行ステータスページを使用して、暗号化コンテキストから暗号化モジュールへの移行を追跡します

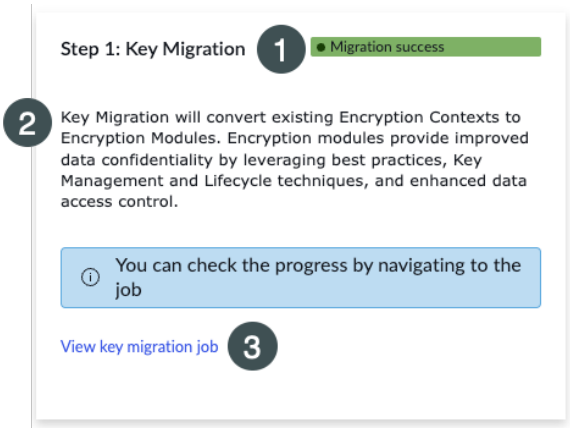


列レベル暗号化 移行ページには、暗号化コンテキストの暗号化モジュールへの移行に関連するステップのステータスが表示されます。3 つのセクションにはそれぞれ、プロセス内の特定のステップのステータスが表示されます。

ページセクションカード

このページには、移行のステップを表す 3 つのカードが含まれています。これらのカードには次のものが表示されます。

- (1) 現在のステップのステータス。このステータスには、ステップが正常に完了したかどうか、または処理するジョブがないかどうかが表示されます。
- (2) リストされたステップの説明。
- (3) 関連する暗号化ジョブ [sys_mass_encryption_job] レコードへのリンク。



Column Level Encryption の暗号化モジュールを作成する

暗号化操作に使用するメカニズムを定義する Column Level Encryption 暗号化モジュールを作成します。

始める前に

必要なロール：sn_kmf.cryptographic_manager または sn_kmf_admin、security_admin、admin

このタスクについて

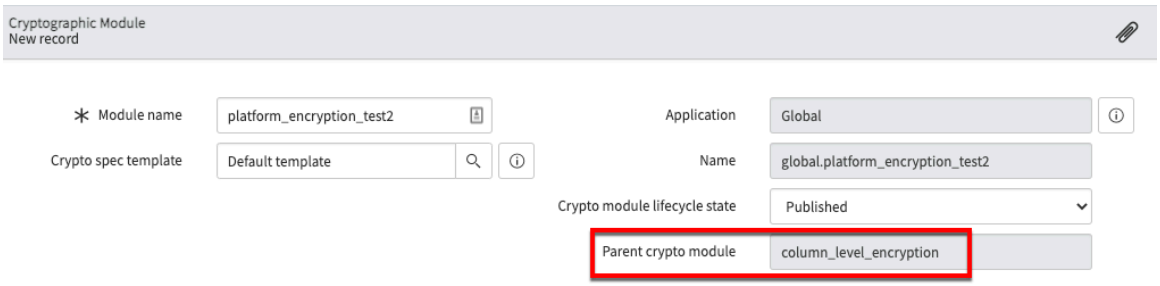
この手順では、ベースシステムを使用した Column Level Encryption (CLE) で使用できるオプションと、列レベル暗号化エンタープライズ (CLE_Ent) 機能で使用可能になる追加の設定オプションについて説明します。列レベル暗号化エンタープライズ は有料サブスクリプションで利用できます。サポート対象機能と各製品で使用できるオプションについては「暗号化とキー管理のサブスクリプションバンドル」を参照してください。列レベル暗号化エンタープライズ の取得についての詳細は「Column Level Encryption Enterprise のアクティブ化」を参照してください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. 移動先 すべて > システムセキュリティ > フィールド暗号化モジュール > 新規.



2. フォームのフィールドに入力します。

暗号化モジュールフォーム

フィールド	説明
モジュール名	スクリプトの実行時に参照される英数字の文字列。
暗号化仕様テンプレート	暗号化の仕様および推奨されるアルゴリズムに対し、多くの暗号化の目的のマッピングを含む、暗号化モジュールの作成に使用されるデフォルトのテンプレート。
アプリケーション	選択したアプリケーションスコープ。
名前	モジュールの作成時に他のスコープ対象のアプリケーションとの競合を避けるために、暗号化モジュール名の先頭にアプリケーションスコープ名が追加されます。たとえば、グローバルアプリケーションスコープで my_crypto_module という名前のモジュールを作成した場合、その名前は global.my_crypto_module として保存されます。
暗号化モジュールライフサイクルステータス	ライフサイクルという用語は、暗号化モジュールの作成、使用、非アクティブ化を指します。設定時に最初は [ドラフト] に設定されます。モジュールを使用する場合は、[公開] に設定します。[デフォルト] テンプレートは自動的に [公開] に設定されます。
親暗号化モジュール	親は **column_level_encryption** として自動的に入力されます。

3. [送信] をクリックします。

正常に送信すると、暗号化モジュールが暗号化モジュールテーブルにリストされます。

自動翻訳

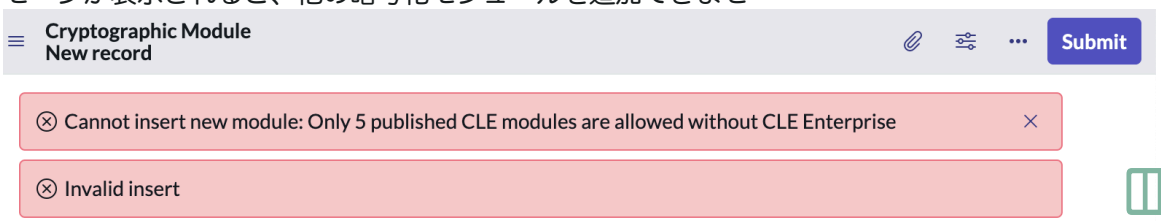
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

> **⚠ 警告:**
>
> 従来の暗号化サポートユーザーの場合：
>
> 非エンタープライズバージョンの Column Level Encryption を使用している場合は、5 つのモジュールに制限されます。 この上限を超えると、次の警告が表示されます。
>
> この挿入により、サブスクリプション製品に認められている Column Level Encryption⌧の公開モジュール数の上限を超えました。追加のモジュールには、Column Level Encryption の Enterprise サブスクリプションが必要です。アカウントチームにお問い合わせください。

デフォルトの暗号化仕様は、暗号化の目的が [対称データ暗号化/復号化] に設定され、アルゴリズムが [AES 256 CBC] に設定されて作成されます。更新のアルゴリズムを選択します。

4. 設定オプションを開くには、新しく作成された暗号化モジュールをクリックします。

> **注:**
> にアップグレード 列レベル暗号化エンタープライズする前に、最大 5 つの Column Level Encryption モジュールが許可されます。エラーメッセージが表示されると、他の暗号化モジュールを追加できませ



ん。

次のタスク
Column Level Encryption の暗号化仕様を作成する。

複数暗号化モジュールの使用

複数の暗号化モジュールでは、複数の暗号化モジュールでデータを暗号化できます。たとえば、ロールに基づく独自のアクセスポリシーが各モジュールにある場合、異なるロールを持つユーザーは同じテーブルでデータを暗号化できますが、互いの暗号化されたデータを表示することはできません。

始める前に
必要なロール：sn_kmf.cryptographic_manager または sn_kmf.admin

このタスクについて

> **注:**
> 列の暗号化のみが複数のモジュールをサポートしています。添付ファイルの暗号化は行いません。複数の暗号化モジュールメソッドを使用する際に、一括暗号化は利用できません。

複数の暗号化モジュールを使用してフィールドを変更し、単一の暗号化モジュールを使用することはできません。

このフィールドは、最初にデータを入力するユーザーの暗号化モジュールで暗号化されます。暗号化モジュールはレコードごとに設定されるため、リストのフィールドにはさまざまな暗号化モジュールが含まれる可能性があります。1 つのレコード内では、フィールドは 1 つのモジュールでのみ暗号化できます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

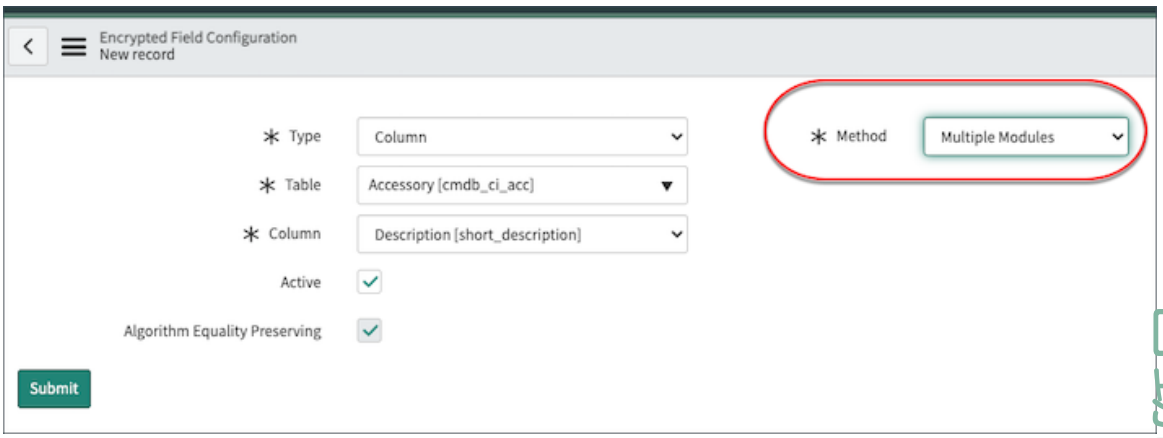
1. 複数の暗号化モジュールとそれぞれのアクセスポリシーを作成します。

   アクセスポリシーを通じて、さまざまな暗号化モジュールにさまざまなロールを付与するようにします。

2. 移動先 システムセキュリティ > フィールド暗号化 > 暗号化フィールドの設定.

   暗号化フィールドの設定の詳細については、「暗号化フィールド構成を設定する」を参照してください。

3. [タイプ] フィールドで、[列] を選択する必要があります。
   添付ファイル暗号化は複数のモジュールをサポートしていません。
4. [メソッド] フィールドで [複数のモジュール] を選択します。



5. 暗号化するテーブルの [テーブル] と [列] を選択します。
6. [送信] をクリックします。

タスクの結果
指定されたフィールドの新しく作成されたデータは、関連するモジュールのキーで暗号化されます。モジュール A のアクセスポリシーで指定されたロールを持つユーザーが、指定されたテーブルに書き込むと、データはモジュール A のキーで暗号化されます。同じロールを持つユーザーのみがデータを読み込むことができます。

Example:
インシデントテーブルの [簡単な説明] 列を暗号化します。次の操作を行います。

1. 2 つの暗号化モジュール A と B を作成します。
2. 各モジュールに、モジュールアクセスポリシーを作成します。

   モジュール A の場合、人事ロールアクセス権をユーザーに付与します。モジュール B の場合、営業ロールアクセス権をユーザーに付与します。

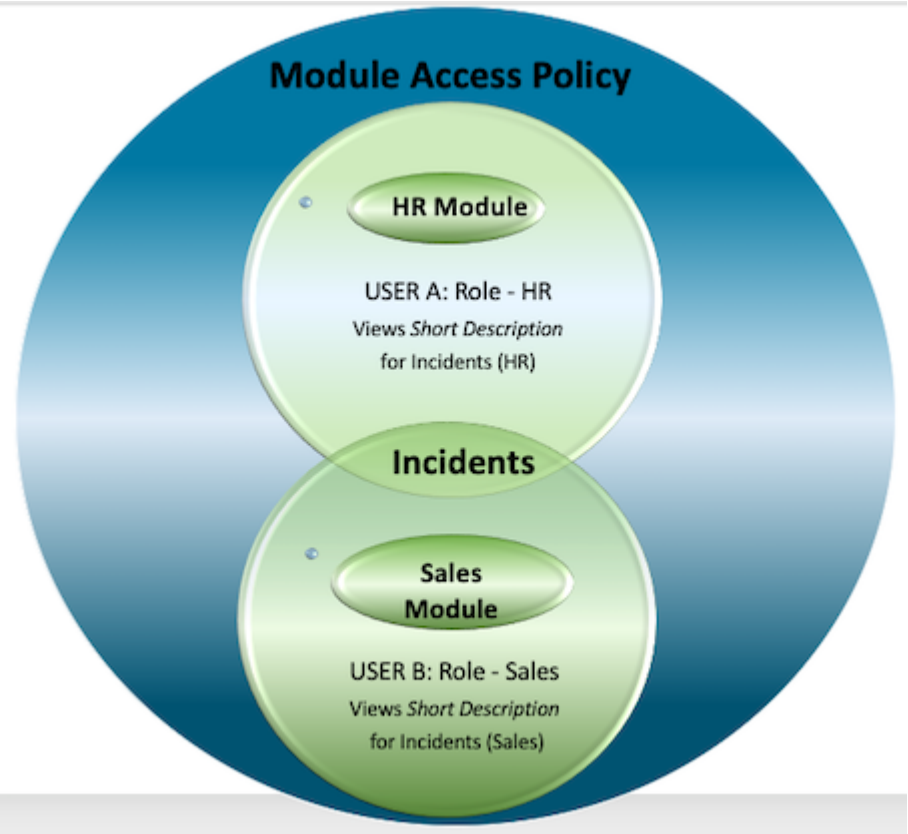
3. インシデントテーブルの [簡単な説明] 列を指定する暗号化フィールドの設定レコードを作成し、[メソッド] フィールドで [複数のモジュール] を選択していることを確認します。
4. 人事ロールのユーザー (ユーザー A) と営業ロールのユーザー (ユーザー B) の 2 人のユーザーに、簡単な説明のあるインシデントを作成させ、両方のユーザーにインシデントのリストを表示させます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

人事ロールのユーザーが作成したインシデントの簡単な説明は、モジュール A のキーで暗号化されます。同様に、営業ロールのユーザーが作成したインシデントの簡単な説明は、モジュール B のキーで暗号化されます。

人事ロールと営業ロールを持つすべてのユーザーがインシデントにアクセスできますが、人事ロールを持つユーザー A が作成したインシデントの簡単な説明を復号化して表示できるのは、人事ロールを持つユーザーのみです。同様に、営業ロールを持っていたユーザー B が作成したインシデントの簡単な説明を復号化して表示できるのは、営業ロールを持つユーザーのみです。



Column Level Encryption の暗号化仕様を作成する

暗号化モジュールを作成してから、対応する暗号化仕様にアクセスし、アルゴリズムを定義します。

始める前に

必要なロール：sn_kmf.cryptographic_manager または sn_kmf_admin および security_admin または admin

このタスクについて

この手順では、基本システムを使用した Column Level Encryption (CLE) で使用できるオプションと、 列レベル暗号化エンタープライズ (CLE_Ent) 機能で利用できるようになる追加の設定オプションについて説明します。列レベル暗号化エンタープライズ 機能は有料サブスクリプションで利用できます。サポート対象機能と各製品で使用できるオプションについては「暗号化とキー管理のサブスクリプションバンドル」を参照してください。列レベル暗号化エンタープライズ の取得についての詳細は「Column Level Encryption Enterprise のアクティブ化」を参照してください。

Column Level Encryption の暗号化モジュールを作成すると、暗号化仕様が作成されます。

.

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. 移動先 システムセキュリティ > フィールド暗号化モジュール > すべて.
2. 暗号化モジュールを選択して設定オプションを開きます。
   暗号化モジュール情報が画面の上部に表示されます。対称データの暗号化/復号化の暗号化仕様は、AES 256 CBC アルゴリズムで自動的に作成されます。
3. テーブルから暗号化仕様を選択して、アルゴリズム定義を開きます。
   列レベル暗号化エンタープライズ については、「Column Level Encryption Enterprise の高度なアルゴリズムを設定する」を参照してください。
4. [次へ] をクリックしてキーライフサイクルにアクセスします。

次のタスク
次のいずれかの操作を実行します。

- キーライフサイクルテーブルのエントリを選択して、キーライフサイクルの動作を定義します。
  キーライフサイクル定義の完了に関する詳細については、「キーライフサイクルステータスの設定」を参照してください。
- [次へ] をクリックして暗号化キーを作成します。このプロセスの詳細については、「ServiceNow 暗号化キーを生成する」を参照してください。

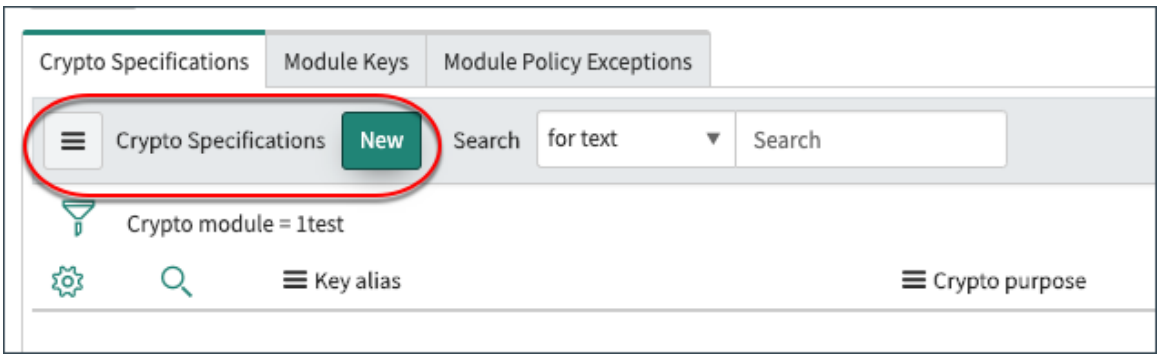
Column Level Encryption Enterprise の高度なアルゴリズムを設定する

暗号化モジュールのアルゴリズムを定義する暗号化仕様を作成します。列レベル暗号化エンタープライズ で利用可能な詳細オプションを使用して、暗号化の仕様をカスタマイズします。

始める前に
必要なロール：admin

手順

1. [暗号化仕様 **(#)**] タブで、[新規] をクリックします。



2. フォームのフィールドに入力します。

アルゴリズム定義フォーム

フィールド	説明
暗号化モジュール	選択した暗号化モジュールの名前が入力されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
暗号化の目的	列レベル暗号化エンタープライズ の場合、値は対象データの暗号化/復号化です
アルゴリズム	列レベル暗号化エンタープライズ の場合、値は **AES** です。
操作モード	列レベル暗号化エンタープライズ の場合、値は **CBC** です。
サイズ	可能な値は **256** と **128**です。 注: 256 ビットサイズが暗号化に最も安全で、列レベル暗号化エンタープライズ の対称データの暗号化/復号化に使用されます。
等価性保存	決定的暗号化を有効にするオプション。 注: このオプションを選択すると、フィールドの値が変わらなければフィールドの暗号化された値も同じになるはずです。 暗号ブロックチェーン **(CBC)** モードで **AES** を使用した対称データの暗号化/復号化を有効にするオプション。
完全性	GCM 操作で完全性を提供するオプションであり、列レベル暗号化エンタープライズ 機能には適用されません。

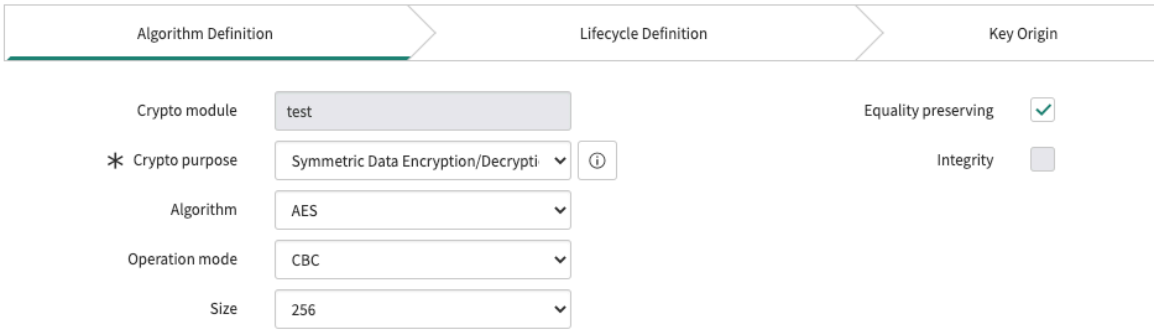
3. [送信] をクリックします。

次の例は、AES CBC-256 暗号化を示しています。列レベル暗号化エンタープライズ がアクティブで、親モジュールが column_level_encryption の場合、対称データ暗号化/復号化 AES

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

CBC-256 のみが暗号化の目的として適用されます。詳細については、「暗号化の目的、アルゴリズム、およびキーの情報」を参照してください。



次のタスク
次のいずれかの操作を実行します。

- キーライフサイクルテーブルのエントリを選択して、キーライフサイクルの動作を定義します。キーライフサイクル定義の完了に関する詳細については、「キーライフサイクルステータスの設定」を参照してください。
- [次へ] をクリックして暗号化キーを作成します。キーの生成については、次のいずれかのタスクを参照してください。
  - ServiceNow 暗号化キーを生成する。
  - 顧客指定のキーのプロパティを設定する。
  - ラッピング/ラップ解除キーペアのインポート。

顧客指定のキーのプロパティを設定する

列レベル暗号化エンタープライズ プラグインが有効になっている場合は、システムプロパティを使用して、顧客指定のキーのキーパディング、短期キーペアのサイズ、およびキーの有効期間を定義できます。

列レベル暗号化エンタープライズ をキー管理とともに使用すると、データ暗号化キーのキーライフサイクル全体を管理できます。必要に応じて、環境内で生成されたデータ暗号化キーを安全に交換できます。

注:
このトピックのこのプロパティは、列レベル暗号化エンタープライズ 機能にのみ適用されます。列レベル暗号化エンタープライズ 機能は、`com.glide.now.platform.encryption` プラグインがアクティブな場合にのみ使用できます。列レベル暗号化エンタープライズ の取得についての詳細は「Column Level Encryption Enterprise のアクティブ化」を参照してください。

データ暗号化キーがインスタンスにインポートされた後、セキュアなラッピングキーによってインスタンスの新しいモジュールキーが保護されます。ラッピングキーは、SafeNet KeySecure のハードウェアセキュリティモジュール (HSM) で生成されたインスタンスキー暗号化キーです。キータイプの詳細については、「キー管理フレームワークのインスタンスレベルのキー」を参照してください。

独自のキーを指定する場合は、RSA 公開キーでラップする必要があります。ラッピング RSA キーペアのサイズ、パディングアルゴリズム、および有効期間は、次の 3 つのプロパティで定義されます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- *glide.kmf.ephemeral_key.key_padding* は、短期キーのキーパディングスキームを制御します。デフォルトのスキームは OAEP SHA256 ですが、SHA1 もサポートされています。
- *glide.kmf.ephemeral_key.key_size* は、短期キーペアのキーサイズを制御します。デフォルトは 4096 ビットですが、2048 ビットもサポートされています。
- *glide.kmf.ephemeral_key.key_validity_period* は、短期キーペアの有効期間を定義します。デフォルト値は 2 時間です。

顧客指定のキーをラップする に続きます。

顧客指定のキーをラップする

顧客指定のキーを使用している場合は、ダウンロードした公開鍵で対称キーをラップします。

始める前に

注:
この手順では、KMF ベースシステムで使用できるオプションと 列レベル暗号化エンタープライズ 機能で使用するオプションについて説明します。列レベル暗号化エンタープライズ機能は、*com.glide.now.platform.encryption* プラグインがアクティブな場合にのみ使用できます。 列レベル暗号化エンタープライズ の取得についての詳細は「Column Level Encryption Enterprise のアクティブ化」を参照してください。

このドキュメントの一部の手順では、ローカルデバイスにインストールされている暗号化ツールを使用する必要があります。このタスクの例では、OpenSSL ツールを使用します。このツールの詳細については、「 https://www.openssl.org 」を参照してください。LibreSSL や GnuTLS などの他の暗号化ツールを使用している場合は、それらの製品のドキュメントで類似した手順について参照してください。

- キーのサイズ、パディングアルゴリズム、および有効期間を制御するオプションのプロパティを変更します。
- 暗号化には対称キー (.BIN) が必要です。
- キーをラップするには、暗号化ツールが必要です。この例では、OpenSSL 1.1 を使用します。

必要なロール：sn_kmf.cryptographic_manager または sn_kmf.admin

手順

1. 移動先 すべて > キー管理フレームワーク > 暗号化モジュール > すべて.
2. 暗号化仕様関連リストから、顧客指定のキーに対して作成した暗号化モジュールを選択します。
3. キーの作成手順に移動します。
4. 以前にラッピングキーをダウンロードしていない場合は、リンクをクリックして *token_publickey<id>.zip* ファイルをダウンロードし、キーと同じ場所に保存します。

   注:
   ダウンロードした *token_publickey<id>* ファイルの名前は変更しないでください。

5. ローカルネットワークにファイルを展開します。
   zip ファイルには、インポートトークンと公開鍵 .PEM 証明書の 2 つのファイルが含まれています。対称キーを公開鍵でラップして暗号化します。
6. *token_publickey* ファイルの名前をクリップボードにコピーします。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

7. コマンドラインから、コピーした *token_publickey* ファイル名を使用して、ラップされたキーのプレースホルダーとして展開されたファイルのフォルダーを開きます。
8. 例を実際の暗号化ファイルの名前に置き換えて、このスクリプトを編集します。

```
"downloads user.name$ cd token_publickey_<token>
openssl pkeyutl -encrypt -pubin -inkey publickey_<keyname>.PEM
-in <keyname.bin>
-out wrapped_key_material -pkeyopt rsa_padding_mode:oaep -pkeyopt
 rsa_oaep_md:sha<128 or 256> "
```

詳細については、次の表のキーラッピングコマンドを確認してください。

キーラッピングコマンド

方向	コマンド	例
ラッピングトークンをダウンロードしたファイルディレクトリを開きます。	`cd`	`cd token_publickey123456789`
publickey.PEM 証明書の名前を貼り付けます。	`openssl pkeyutl -encrypt -pubin -inkey`	`publickey_586798643ffff.PEM`
ここにキーの名前を貼り付けます。	`-in`	`mykey.bin`
<-out> コマンドを入力し、キーが 128 ビットか 256 ビットかを指定します。	`-out wrapped_key_material -pkeyopt rsa_padding_mode:oaep -pkeyopt rsa_oaep_md:sha256`	適用外

9. コマンドを実行します。
システムメッセージに token_publickey_<keynumber> が表示されます。キーが生成され、「*wrapper_key_ material*」ファイルがディレクトリに追加されます。
10. ラップされたキーをアップロードします。

次のタスク
ラップされたキーをアップロードするには 顧客指定のキーの設定とアップロード に戻ります。

顧客指定のキーの設定とアップロード
システム生成キーを使用する代わりに、 ServiceNow® 顧客指定の独自のキーを使用できます。

始める前に
必要なロール：security_admin、sn_kmf.cryptographic_manager

独自のキーを指定しない場合は、この手順を実行する必要はありません。ServiceNow® キーで暗号化モジュールを作成するには、暗号化モジュールを作成する または Column Level Encryption の暗号化モジュールを作成する に移動します。

注:
この手順は、列レベル暗号化エンタープライズ 機能にのみ適用されます。詳細については、「Column Level Encryption Enterprise のアクティブ化」を参照してください。

自動翻訳

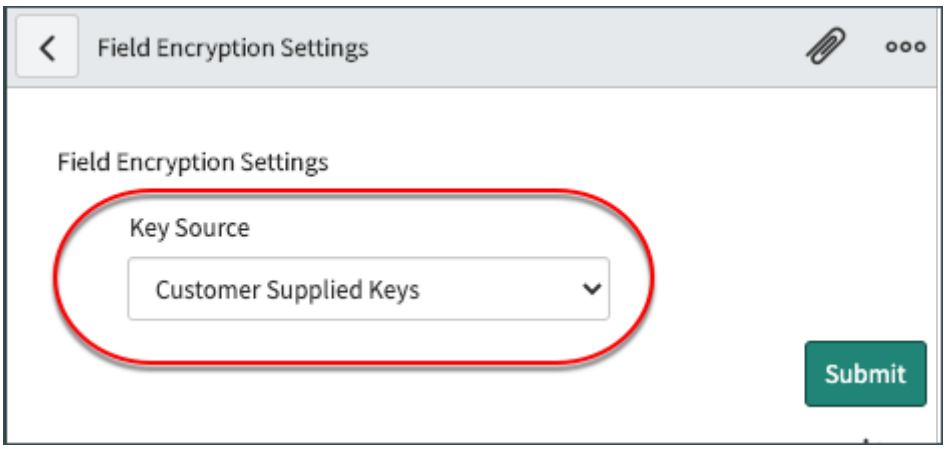
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

重要:
顧客指定のキーを取り消すことはできません。

手順

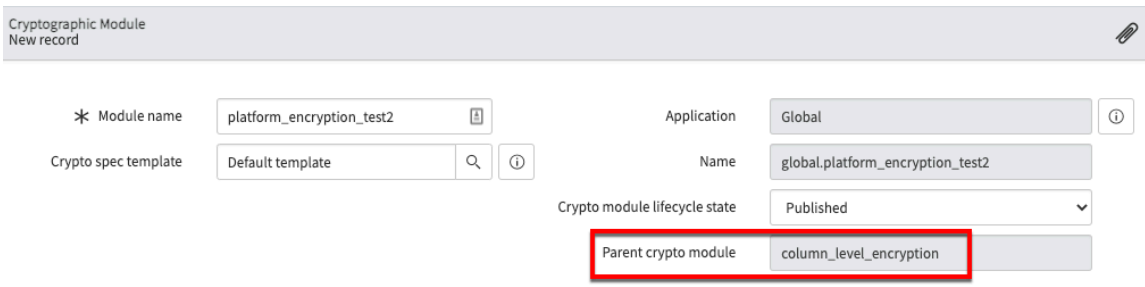
1. 移動先 すべて > システムセキュリティ > フィールド暗号化設定 [顧客指定のキー] が選択されていることを確認します。

キーソースの選択



2. [**Submit** (送信)] を選択します。
3. 戻る システムセキュリティ > フィールド暗号化モジュール > > 新規作成.

新しい暗号化モジュールの作成



4. 暗号化モジュールフォームに次のように入力します。

暗号化モジュールのフィールド

フィールド	説明
モジュール名	モジュールの名前を入力します。
暗号化仕様テンプレート	デフォルトの暗号化テンプレートが選択されています。
名前	モジュール名に基づいて自動入力され、どのアプリケーションが適用されているかを確認するためにスコープが名前の先頭に追加されます。この場合、グローバルスコープが適用されます。
暗号化モジュールライフサイクルステータス	選択 公開済み 暗号化モジュールを有効にします。

自動翻訳

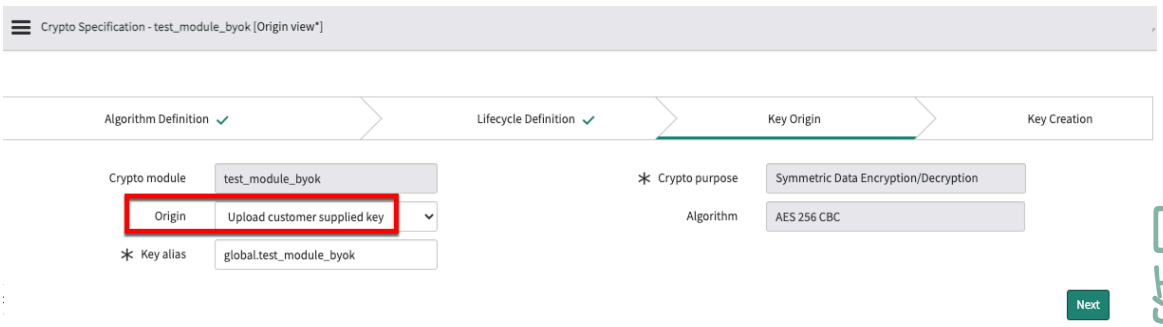
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
親暗号化モジュール	顧客指定のキーと暗号化モジュールを使用すると、親モジュール **column_level_encryption** が自動的に選択されます。

5. [送信] を選択します。
6. テーブルから新しく作成された暗号化モジュールを選択します。
   [暗号化仕様] 関連リストで、AES 256 CDB アルゴリズムを使用して自動生成されたキーエイリアスを選択します。

   暗号化の目的と CLE のアルゴリズムが自動的に入力され、キーの作成元ステージにジャンプします。
7. [顧客指定のキーをアップロード] が [作成元] であり、[キーエイリアス] が既に入力されていることに注意してください。

   キーの作成元

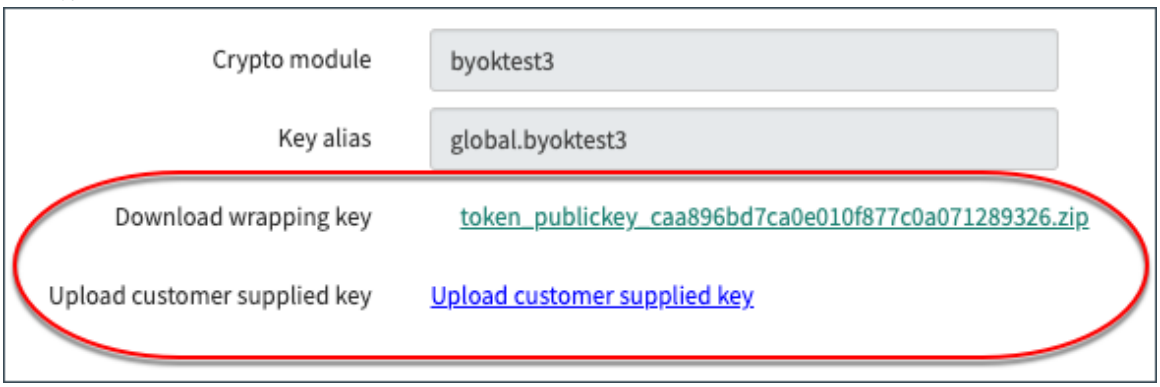


8. [次へ] を選択して [キーの作成] ステージに移動します。

   次の 2 つのリンクがあります。

   - [ラッピングキーをダウンロード] では、インポートトークンと公開鍵証明書 (.PEM ファイル) を含む zip ファイルでキーがダウンロードされます。インポートトークンを使用して、インスタンスのセキュリティ仕様に従ってキーラッピングが成功したことを確認します。公開鍵証明書の .PEM ファイルを使用して、顧客指定のキーを安全にラップしてから、トークンとともにアップロードします。
   - [顧客指定のキーをアップロード] を選択すると、ファイルブラウザーが開き、ラップしたトークンと暗号化キーが選択されます。

     キー作成アップロードリンク



9. [ラッピング キーのダウンロード] を選択してトークンを保存します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

キーがシステムに保存されているのと同じ場所にトークンを保存します。ダウンロードしたトークンの名前を変更しないでください。

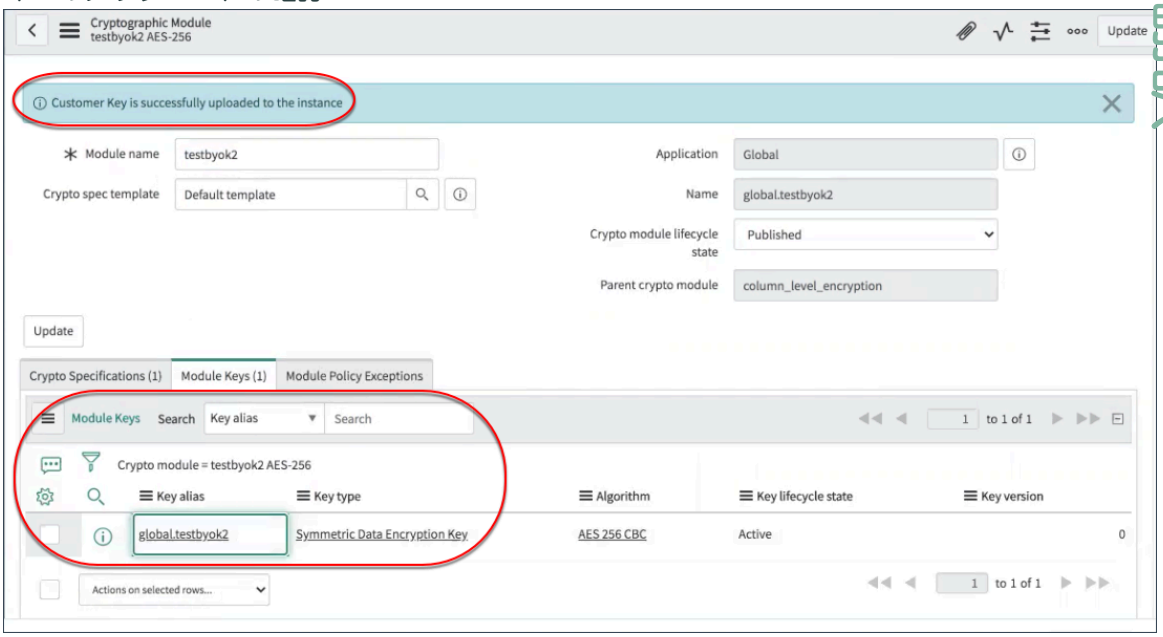
10. 端末で BYOK コマンドを実行してキーをラップします。詳細については、「顧客指定のキーをラップする」を参照してください。
11. [顧客提供のキーのアップロード] を選択します。
12. [参照] を選択して、ラップされたキーとトークン ファイルの 2 つのファイルを選択します。[添付ファイル] ウィンドウに 2 つのファイルが表示されます。

ラップされたキー添付ファイルのアップロード

必要に応じて、削除するファイルを選択して再アップロードします。

13. **[OK]** を選択します。[暗号化モジュール] 画面に戻ります。顧客キーの正常なアップロードを確認するメッセージが表示されます。キーは [モジュールキー] 関連リストにも表示されます。

キーのアップロードの確認



次のタスク

顧客指定のキーを使用した暗号化モジュールの設定が完了したので、「モジュールアクセスポリシーを作成する」に進みます。

フィールドと添付ファイルの暗号化

暗号化モジュールを作成したら、暗号化フィールド構成を作成し、テーブルのフィールドの暗号化または添付ファイルの暗号化を指定します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

フィールドの暗号化方法

注:
暗号化されたフィールドは設計上、監査されません。この動作は設定できません。

1. でキーソースを指定します。システム生成キーまたは顧客指定のキー (独自のキーを使用する) です。 システムセキュリティ > フィールド暗号化設定.
2. キーソースを指定した後、新しい暗号化モジュールを作成するか、既存の暗号化モジュールを使用します。手順については、「暗号化モジュールを作成する」を参照してください。

   注:
   顧客指定のキーを使用する場合は、「Column Level Encryption の暗号化モジュールを作成する」および「顧客指定のキーのプロパティを設定する」の指示に従ってください。

3. 暗号化を実行するテーブルと、暗号化するテーブルの列または添付ファイルのいずれかを指定する、暗号化フィールド構成を作成します。「暗号化フィールド構成を設定する」を参照して開始してください。

注:
顧客指定のキーを使用してフィールドと添付ファイルを暗号化する方法については、「Column Level Encryption Enterprise の例」を参照してください。

暗号化フィールド構成を設定する

事前設定された暗号化モジュールを使用して、暗号化するテーブルの列または添付ファイルを設定します。

始める前に
必要なロール：sn_kmf.cryptographic_manager および security_admin、または security admin へのロールの昇格

このタスクについて
そのスコープ内のテーブルを表示できるように、正しいアプリケーションスコープ内にいることを確認してください。

この暗号化フィールド構成で指定した暗号化モジュールへのアクセス権を持つユーザーのみが、暗号化されたテーブル列のデータを読み取ったり、添付ファイルにアクセスしたりできます。

- ユーザーが書き込みアクセス権を持っているが、読み取りアクセス権がない場合、フィールドは編集モードで表示され、入力されたデータはアスタリスクとして表示されます。
- ユーザーが読み取りアクセス権を持っているが、書き込みアクセス権がない場合、フィールドには復号化されたデータが読み取り専用モードで表示されます。
- ユーザーがすべてのアクセス権を持っている場合、暗号化フィールドで読み取り/書き込み機能を使用できます。

開始するには、「暗号化モジュールを作成する」または「Column Level Encryption の暗号化モジュールを作成する」を参照してください。

手順
1. 移動先 すべて > システムセキュリティ > フィールド暗号化 > 暗号化フィールドの設定 > 新規.
2. [新規] をクリックします。
3. フォームに入力します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
タイプ	テーブル列を暗号化する列、またはテーブルのすべての添付ファイルを暗号化する添付ファイル。 暗号化されるデータのタイプは次のとおりです。 ○ 文字列テキスト ○ 添付ファイル ○ 日付、日付/時間： **注:** 暗号化フィールドの設定を作成して、既存の [日付] および [日付/時刻] フィールドを暗号化することができます。新しい暗号化構成は、親テーブルのみに追加できます。子テーブルには、新しい暗号化設定を追加できません。 ○ URL ○ 列レベル暗号化エンタープライズ では、次のフィールドタイプもサポートされています。 ▪ HTML ▪ ジャーナル ▪ 翻訳済み
テーブル	フィールドまたは添付ファイルを暗号化するテーブルを選択します。
列	タイプとして列を選択した場合は、暗号化する列 (フィールド)。
有効	構成をアクティブとしてマークする場合に選択します。構成がまだ使用されていない場合は選択を解除します。
暗号化モジュール	暗号化フィールド構成が適用される暗号化モジュール。
メソッド	1 つのモジュール全体のフィールド構成を設定するには、単一モジュールを選択します。複数の暗号化モジュールにまたがるロールベースのアクセスの場合は、複数のモジュールを選択します。 単一モジュール 単一モジュールを使用してすべての添付ファイルを暗号化するには、このオプションを使用します。ユーザーにはこのモジュールへのアクセス権が必要です。そうでないと添付ファイルをアップロードできません。 複数モジュール 添付ファイルのアップロード時にユーザーがモジュールを選択できるようにするには、このオプションを使用します。1 つ以上のモジュールへのアクセス権を持つユーザーが、暗号化に使用するモジュールを選択できるようになります。モジュールへのアクセス権のないユーザーは、暗号化されていない添付ファイルをアップロードできます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
アルゴリズム暗号化保存 [読み取り専用]	選択した暗号化モジュールが非決定的暗号化をサポートするように既に設定されているかどうかを示します。これは、同じデータが複数回暗号化されている場合、それぞれの暗号化が毎回異なることを意味します。

4. [送信] をクリックします。

暗号化モジュールのスクリプトアクセス

スクリプトを実行して、暗号化の目的のために暗号化モジュールポリシーにアクセスできます。

Key Management Framework の場合、ポリシーはスクリプトに基づくことができます。スクリプトアクセスに対してアクセスポリシーがトリガーされると、バックエンドスクリプトはスクリプトからモジュールポリシーアクションを実行できます。

暗号化モジュールは、非対称データ復号化や対称データ復号化など、1 つ以上の暗号化の目的をサポートできます。暗号化の目的ごとに、暗号化キーと定義された暗号化の目的を生成する必要があります。

暗号化スクリプト要求を実行するときは、次の点を考慮してください。

- 参照される暗号化の目的は、暗号化モジュールで定義する必要があります。
- 暗号化モジュールに対して生成されたアクティブなキーが存在する必要があります。
- モジュールアクセスポリシータイプはスクリプトに設定する必要があります。

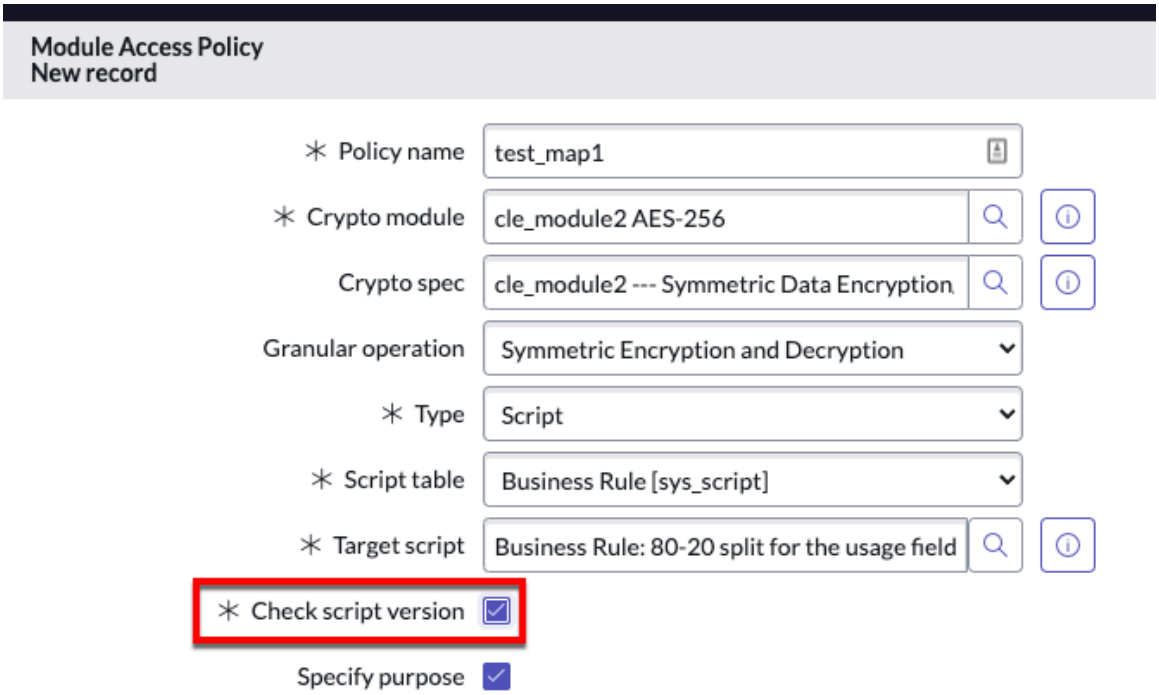
スクリプトバージョンのチェック

スクリプトタイプに設定されたモジュールアクセスポリシーを作成するときに、アクセスするスクリプトバージョンの整合性を検証するオプションがあります。割り当てられたバージョンのスクリプトのみが暗号化モジュールへのアクセスを許可されます。モジュールアクセスポリシーで [スクリプトバージョンのチェック] チェックボックスをオンにすると、スクリプトが実行されるたびにバージョンの比較が実行されます。スクリプトが変更された場合は、ユーザーに通知されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

[スクリプトバージョンのチェック] チェックボックス



暗号化されたデータへのスクリプトアクセスを設定する

スクリプトを実行して、暗号化の目的のために暗号化モジュールポリシーを実行します。特定の読み取り (復号化/ラップ解除) または書き込み (暗号化/ラップ) アクセスは、モジュールアクセスポリシー操作の粒度に基づいて定義できます。

始める前に
必要なロール：sn_kmf.cryptographic_manager

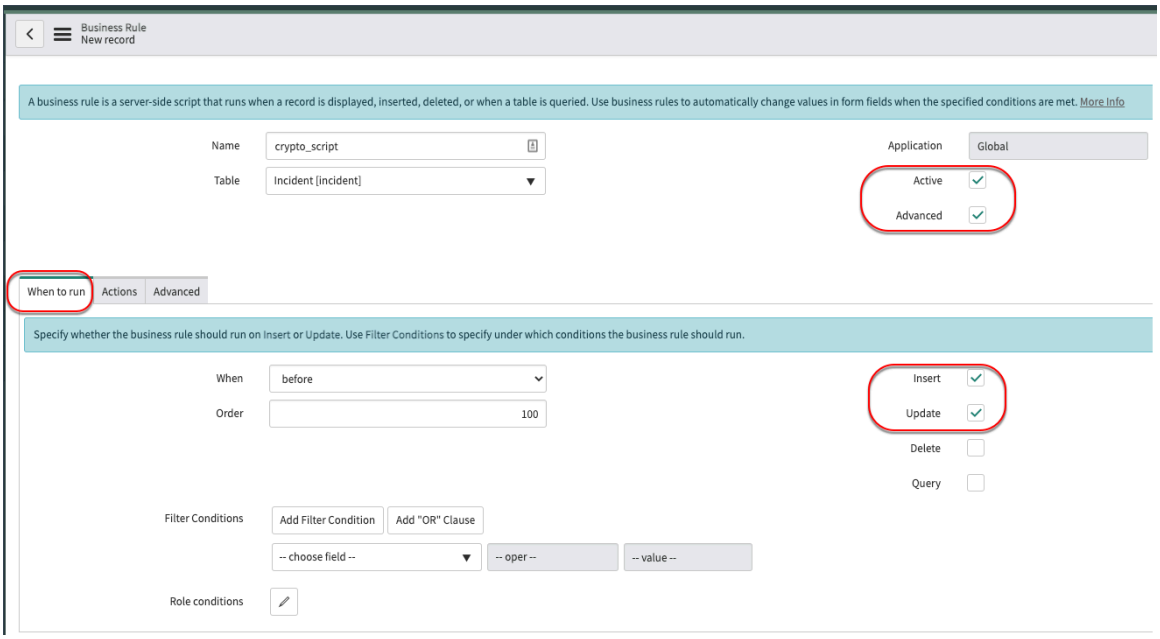
このタスクについて
使用例は、ビジネスルールおよびスクリプトインクルードです。この手順では、ビジネスルールのスクリプトを使用します。

手順

1. 対称データ暗号化/復号化アルゴリズムを使用して暗号化モジュールを作成します。
   詳細については、「暗号化モジュールを作成する」を参照してください。データまたは添付ファイルへの特定のアクセスは、次の特性を持つモジュールアクセスポリシーで制御されます。
   - 対称暗号化：スクリプトはデータを暗号化できますが、復号化することはできません。
   - 対称復号化：スクリプトはアップロードされた暗号化データまたは添付ファイルを復号化できますが、データまたは添付ファイルを暗号化できません。
   - 対称暗号化と復号化：スクリプトはデータまたは添付ファイルの暗号化と復号化の両方を行えます。
2. 移動先 システム定義 > ビジネスルール.
3. [新規] をクリックします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



4. [実行タイミング] タブでフォームに入力し、[詳細] タブでスクリプトを入力します。

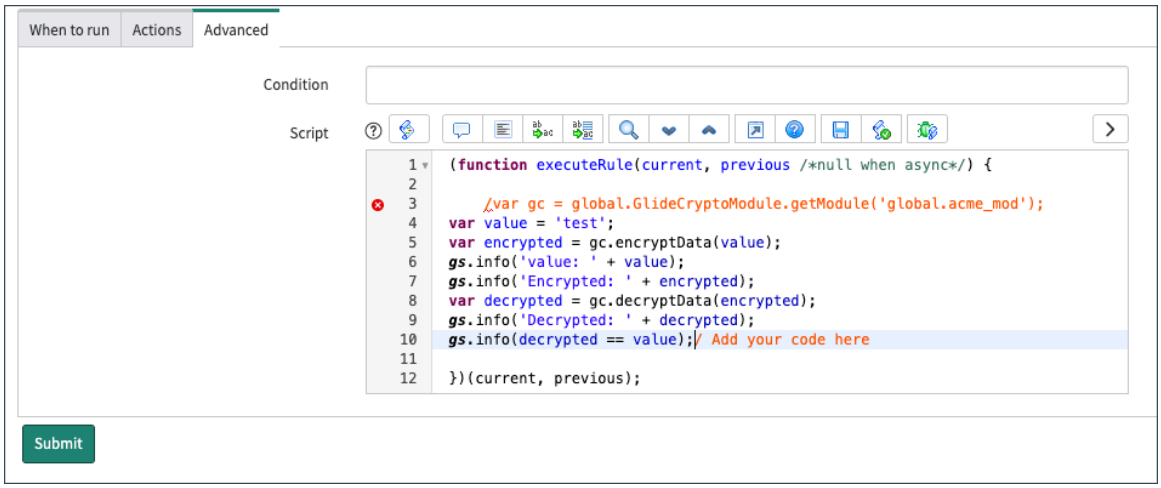
ビジネスルールのフィールド

フィールド	説明
名前	ビジネスルールの名前を入力します。
テーブル	ドロップダウンリストからインシデント [インシデント] を選択します。
アプリケーション	デフォルトでグローバルが選択されています。
有効	ルールをアクティブとしてマークします。
詳細	このチェックボックスをオンにして、詳細オプションを表示します。
[実行タイミング] タブ	[実行タイミング] タブで、[挿入] および [更新] フィールドを有効にします。

[詳細] タブ	[詳細] タブで、次のスクリプトテキストを 3 行目に貼り付けます。
	`//`
	`var gc =`
	`global.GlideCryptoModule.getModule('global.acme_mod');`
	`var value = 'test';`
	`var encrypted = gc.encryptData(value);`
	`gs.info('value: ' + value);`
	`gs.info('Encrypted: ' + encrypted);`
	`var decrypted = gc.decryptData(encrypted);`
	`gs.info('Decrypted: ' + decrypted);`
	`gs.info(decrypted == value);`
	注:
	詳細については、「ビジネスルール詳細タブ」の画像を参照してください。

自動翻訳

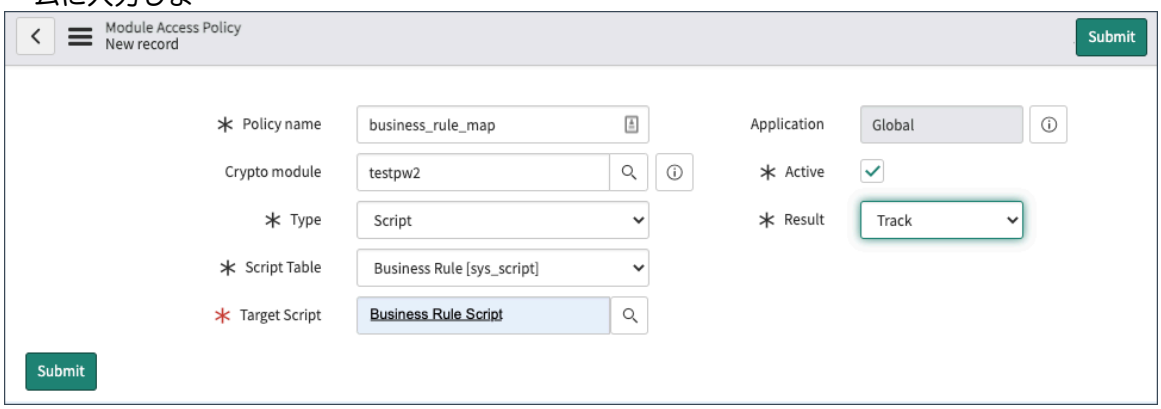
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



5. **[Submit** (送信)] をクリックします。
6. 移動先 キー管理 > モジュールアクセスポリシー > すべて。

   注:
   詳細については、「モジュールアクセスポリシーを作成する」を参照してください。

7. [新規] をクリックします。
8. フォームに入力しま



す。

[モジュールアクセスポリシー] フィールド

9. [送信] をクリックします。
   スクリプトのモジュールアクセスポリシーがシステムで利用できるようになりました。

拒否された暗号化モジュール使用要求を表示する

サポートされていない暗号化メカニズムが原因で、スクリプトによる暗号化要求が却下された暗号化モジュールが表示されます。

始める前に

必要なロール：sn_kmf.cryptographic_manager

このタスクについて

暗号化モジュールは、非対称データ復号化や対称データ復号化など、1 つ以上の暗号化の目的をサポートできます。モジュールアクセスポリシーに基づいてのみ、暗号化されたデータにアクセスできます。スクリプトがモジュールで定義されていない目的で暗号化モジュールを使用しようとすると、スクリプトは暗号化されたデータにアクセスできません。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

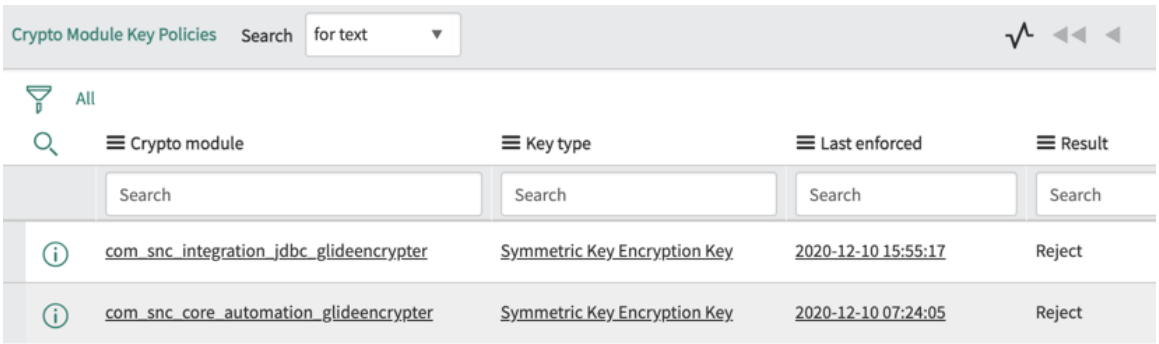
以下の例では、暗号化の目的が暗号化モジュールに割り当てられましたが、そのためのキーは生成されませんでした。

手順

移動先 すべて > キー管理 > モジュールキーポリシー > モジュールキーの拒否.

要求を却下した暗号化モジュールのリストが、対応するスクリプトで使用されている暗号化キーとともに表示されます。

モジュールキーの拒否



注:
異なるスクリプトが同じキータイプを使用して同じ暗号化モジュールを使用しようとすると、前回の強制の値が更新されます。別の行は生成されません。

この例では、モジュール 1 のキーが侵害されたため、2020-02-10_15:55:17 に最初のモジュールが要求を却下しました。2 番目のモジュールのキーが一時停止されているため、2020-02-10_07:24:05 に 2 番目のモジュールが要求を却下しました。

次回実行時に暗号化モジュールを使用する権限をスクリプトに付与するには、スクリプト暗号化のモジュールアクセスポリシーを作成します。詳細については、「暗号化されたデータへのスクリプトアクセスを設定する」を参照してください。

一括暗号化、復号化、およびリキーのジョブをスケジュールする

インスタンスに最適な時間に実行する暗号化、復号化、およびリキーのジョブをスケジュールします。

始める前に
暗号化、復号化、およびリキーのジョブは多くの時間とリソースを必要とするため、ピーク時間外にスケジュールするよう検討してください。また、ジョブをスケジュールしているユーザーが各ジョブに対して適切なアクセス権を持っていることも確認してください。

必要なロール：sn_kmf.cryptographic_manager

このタスクについて
一括暗号化と復号化は、暗号化フィールドの設定フォームからも使用できます。手順については、「一括暗号化または復号化を実行する」を参照してください。

手順

1. 移動先 すべて > システムセキュリティ > 高セキュリティ設定 > セキュリティジョブ.
2. [新規] をクリックします。
3. スケジューリングフォームに入力します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
名前	暗号化、復号化、またはリキージョブの名前
タイプ	ジョブタイプ： ○ モジュールへのキー移行コンテキスト：暗号化モジュールへと暗号化コンテキストキーを一括で移行します (暗号化モジュールでアクセス制御するためのモジュールアクセスポリシーレコードの作成を含む)。 ○ モジュールへのデータ移行コンテキスト：暗号化コンテキストによって暗号化されたデータを暗号化モジュールに移行します。 ○ 一括復号化添付ファイル：[テーブル] フィールドで定義した単一のテーブルのレコード内のすべての暗号化された添付ファイルを復号化します。 ○ 一括暗号化添付ファイル：[テーブル] フィールドで定義した単一のテーブルのレコード内のすべての添付ファイルを暗号化します。 ○ 一括暗号化モジュール：フィールド暗号化設定で使用される、定義された列/フィールドの既存の値を暗号化します。 ○ 一括復号化モジュール：単一モジュールのフィールド暗号化設定で使用されている、定義された列/フィールドの既存の値を復号化します。 ○ 一括復号化マルチモジュール：複数モジュールのフィールド暗号化設定で使用されている、定義された列/フィールドの既存の値を復号化します。 ○ モジュールのリキー：モジュールの現在アクティブなキーを使用して、フィールド暗号化設定で使用されている、定義された列/フィールドの既存の値を再暗号化します。 ○ 添付ファイルコンテキストのモジュールへの移行：フィールド暗号化設定で定義されたテーブルの既存の添付ファイルを暗号化します。以前にコンテキストで暗号化された添付ファイルは、 モジュールで再暗号化されます。
ステータス	初期ジョブのステータスは新規です。ジョブがスケジュールどおりに実行された後、それに応じてステータスが更新されます。
期間開始	24 時間形式のジョブの開始時間。
期間終了	24 時間形式のジョブの終了時間。
テーブル	暗号化または復号化するテーブル。
フィールド	暗号化または復号化するフィールド。
サマリー	ジョブが実行中、完了した、またはエラーがある場合のジョブのステータス情報。

注:
システムオーバーヘッドのために、一括暗号化、復号化、およびリキーのジョブはピーク時間外に実行するようにスケジュールする必要があります。Now Platform は、期間開始と期間終了の間でジョブを実行します。ジョブが 1 つの処理ウィンドウで完了しなかった場合、すべての処理が完了するまで、次の指定された処理ウィンドウでジョブが続行されます。

4. [送信] をクリックします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

5. ジョブをスケジュールすると、次のことができます。
   - 実行中のジョブをキャンセルするには、[ジョブをキャンセル] をクリックします。
   - [開始] をクリックしてジョブをすぐに開始します。
   - [更新] をクリックして、ジョブスケジュールの変更を保存します。
   - [削除] をクリックして、スケジュールしたジョブを削除します。

一括暗号化または復号化を実行する

暗号化設定で一括暗号化を実行したり、一括復号化を実行して以前に暗号化された値を復号化したりすることができます。

始める前に
必要なロール：security_admin

このタスクについて
一括暗号化と一括復号化のためにジョブスケジュールを作成することもできます。手順については、「一括暗号化、復号化、およびリキーのジョブをスケジュールする」を参照してください。

一括暗号化と一括復号化は、暗号化フィールドの構成で単一暗号化モジュールを使用する場合にのみ使用できます。一括復号化は、単一および複数の暗号化方法の両方で使用できます。

> **注:**
> 一括暗号化と一括復号化は、リソースと時間がかかるため、ピーク時間外にのみ実行してください。

手順

1. 移動先 すべて > システムセキュリティ > フィールド暗号化 > 暗号化フィールドの設定.
2. 一括暗号化または一括復号化するフィールドの暗号化フィールド構成を開きます。
3. [関連リンク] で、利用可能なオプションを選択します。
   - 一括復号化ジョブをスケジュール
   - 一括暗号化ジョブをスケジュール
4. ダイアログで選択を確認します。

タスクの結果
一括暗号化を実行する場合、すべての値は暗号化フィールド設定レコードで定義された暗号化モジュールで暗号化されます。一括復号化を実行すると、アクセスできる暗号化モジュールで暗号化されたフィールドのみが復号化されます。

Column Level Encryption Enterprise の例

これらの例では、顧客指定のキーを使用したフィールドと添付ファイルの暗号化について説明します。

フィールド暗号化のチュートリアル

このチュートリアルでは、Key Management Framework (KMF) がある 列レベル暗号化エンタープライズ を使用してインスタンスのフィールドを暗号化する方法を示します。また、独自のキーを使用する方法も示します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

始める前に

> **注:**
> この手順は、列レベル暗号化エンタープライズ 機能にのみ適用されます。列レベル暗号化エンタープライズ の取得についての詳細は「Column Level Encryption Enterprise のアクティブ化」を参照してください。

必要なロール：admin または security_admin

> **注:**
> security_admin は権限ロールです。権限ロールの使用に関する詳細については、「特権ロールへの昇格」を参照してください。

このタスクについて
このチュートリアルは、個人暗号化キーを既に作成してアップロードしたインスタンスから開始します。ServiceNow キーを使用できますが、この例では顧客指定のキーを使用します。

キーが暗号化モジュールに格納されたら、給与や社会保障番号など、特定のユーザーのアクセスが制限されるフィールドの設定を開始できます。暗号化フィールド構成で、機密データにアクセスできる権限を持つ担当者を指定します。

このタスクでは、2 つのシナリオを示します。1 つの例では、機密データを表示する権限のないユーザーのために、インシデントの [簡単な説明] フィールドを暗号化します。

添付ファイルを暗号化して、アクセス権が付与されたユーザーのみに表示するか、データの表示が制限されていないすべてのユーザーに表示することもできます。添付ファイルを暗号化するには、「添付ファイルの暗号化のチュートリアル」を参照してください。

手順

1. 列レベル暗号化エンタープライズ が有効になっていることを確認します。
2. column_level_encryption に暗号化モジュールを作成します。
   詳細については、「Column Level Encryption の暗号化モジュールを作成する 暗号化モジュールを作成する」を参照してください。
3. 移動先 システムセキュリティ > 暗号化フィールドの設定.
4. [新規] をクリックします。
5. フォームのフィールドに入力します。

暗号化フィールドの構成フォーム

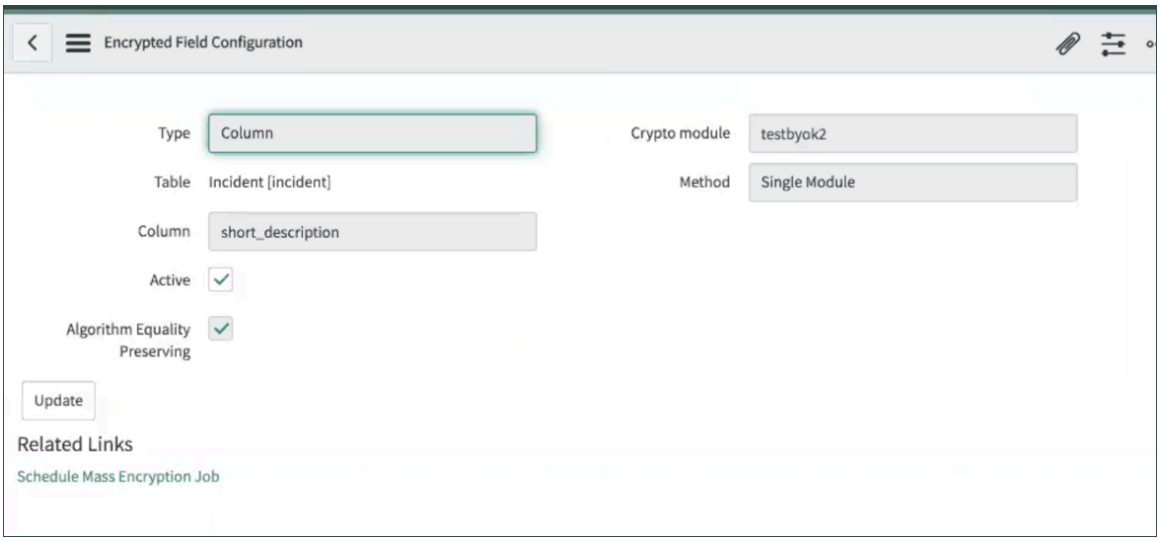
フィールド	説明
タイプ	個人キーを使用するには、列が必要です。
テーブル	機密情報を格納するテーブル。この例では、インシデント [インシデント] を選択します。
列	暗号化する機密データを表す列または特定の情報。この例では、**short_description** を選択します。
有効	フィールド構成を使用するためにアクティブをマークするオプション。
アルゴリズム等価性保存	このオプションは自動的に選択されます。
暗号化モジュール	個人キーで使用するために作成したモジュール。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

フィールド	説明
メソッド	単一モジュールオプションは、1 つのモジュールにポリシーを適用するために使用されます。複数モジュールは、複数のモジュールにまたがってポリシーを適用するために使用されます。

暗号化フィールドの構成の例



6. [送信] をクリックします。

モジュールアクセスポリシーを確立して、暗号化モジュールへのアクセスをアサインします。詳細については、「モジュールアクセスポリシーを作成する」を参照してください。

7. 移動先 キー管理 > モジュールアクセスポリシー > > 新規作成 > .
8. フォームのフィールドに入力します。

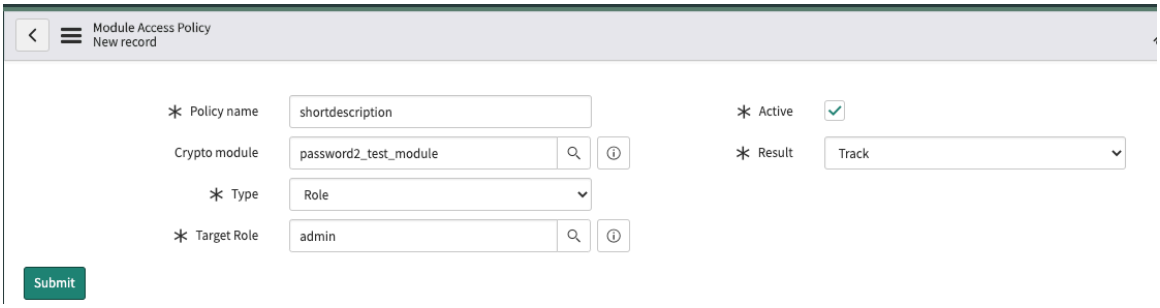
モジュールアクセスポリシーフォーム

フィールド	説明
ポリシー名	簡単な説明などのポリシーの名前。
暗号化モジュール	キーを暗号化するために作成した暗号化モジュール。
タイプ	暗号化ポリシーのアクセス指定のタイプ。ロールを使用して、割り当てられたロールを持つユーザーのみに暗号化フィールドへのアクセス権を付与します。
ターゲットロール	暗号化フィールドにアクセスできるロール。この例では、**Admin** を選択します。
有効	モジュールアクセスポリシーをアクティブ化するオプション。
結果	追跡オプションを使用すると、選択したロールのフィールドにアクセスできます (選択したロールに対してそのフィールドへのアクセスを制限するには、[却下] または [厳格な却下] を選択します)。

自動翻訳

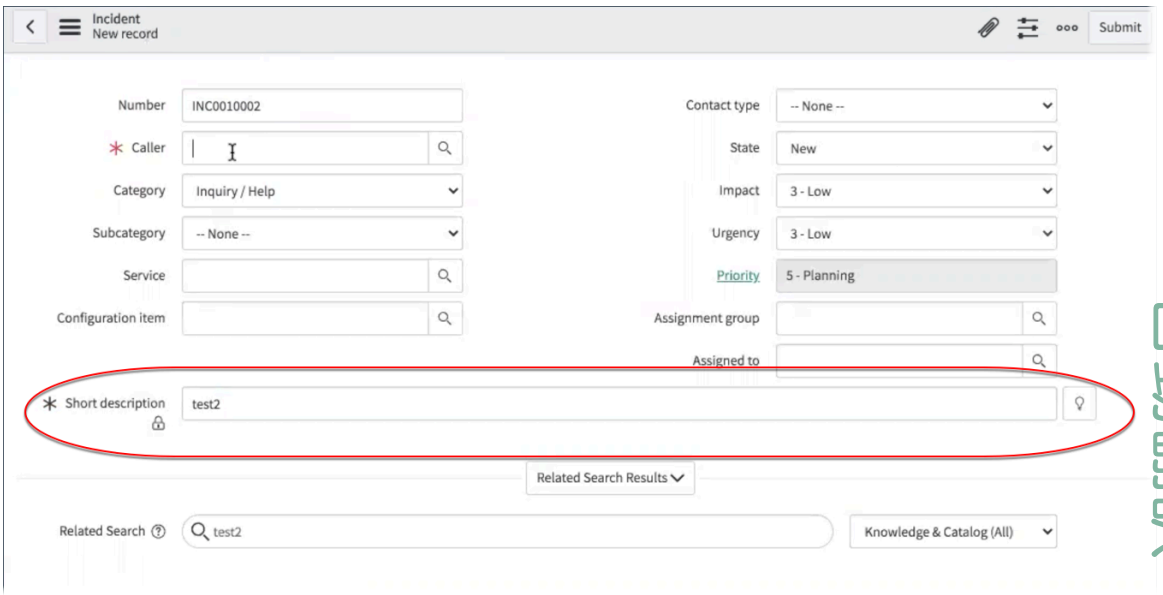
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モジュールアクセスポリシーの例



9. **[Submit** (送信)] をクリックします。
10. sn_kmf.admin ロールを持つユーザーとして、次の場所に移動します。 インシデント > 新規.

表示される暗号化フィールドの例



これで、モジュールアクセスポリシー構成に基づいて [簡単な説明] フィールドを表示できます。

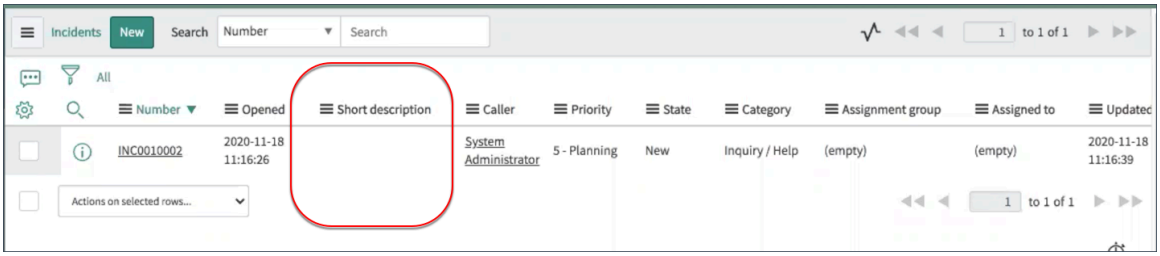
注:
モジュールアクセスポリシーを [追跡] に設定することで、sn_kmf.admin ロールに暗号化フィールド (簡単な説明) へのアクセス権が付与されました。フィールド名の下にあるロックアイコン ( ) は、フィールドが暗号化されていることを示しています。

これで、エンドユーザーとしてインシデントモジュールにアクセスして、暗号化フィールドの設定をテストできます。

11. 構成されたフィールドの暗号化データの表示が制限されるユーザーとしてログインします。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

暗号化されたフィールドレベルデータ



インシデント番号にアクセスしても、[簡単な説明] のデータは表示されません。

タスクの結果

列レベル暗号化エンタープライズ を使用して特定のフィールドへのアクセスを制御する対称キーを正常に使用しました。

添付ファイルの暗号化のチュートリアル

このチュートリアルでは、()KMF を使用してインスタンス列レベル暗号化エンタープライズKey Management Framework 内の添付ファイルを暗号化する方法を示します。また、独自のキーを使用する方法も示します。

始める前に

注:
この手順は、列レベル暗号化エンタープライズ 機能にのみ適用されます。列レベル暗号化エンタープライズ の取得についての詳細は「Column Level Encryption Enterprise のアクティブ化」を参照してください。

必要なロール：kmf 暗号化マネージャー

このタスクについて

このチュートリアルでは、顧客指定の暗号化キーを作成してアップロードしたインスタンスから開始します。ServiceNow　キーを使用できますが、この例では顧客指定のキーを使用します。

機密性の高い添付ファイルをインスタンスにアップロードし、特定のユーザーからのアクセスを制限します。暗号化フィールド構成を使用して、機密データにアクセスできる権限を持つ担当者を指定します。

アクセス権を付与されたユーザーのみに表示するか、または、データの表示を制限されていないすべてのユーザーに表示するために、添付ファイルを暗号化する方法を示します。この例では、特定のロールが インシデントモジュールの添付ファイルにアクセスできないように制限しています。

注:
列の暗号化では複数のモジュールを使用できますが、添付ファイルの暗号化では単一のモジュールを使用する必要があります。

手順

1. 列レベル暗号化エンタープライズ が有効になっていることを確認します。
2. 暗号化モジュールを作成します。
   詳細については、「Column Level Encryption の暗号化モジュールを作成する」を参照してください。
3. 移動先 システムセキュリティ > 暗号化フィールドの設定.
4. [新規] をクリックします。
5. フォームに次のように入力します。

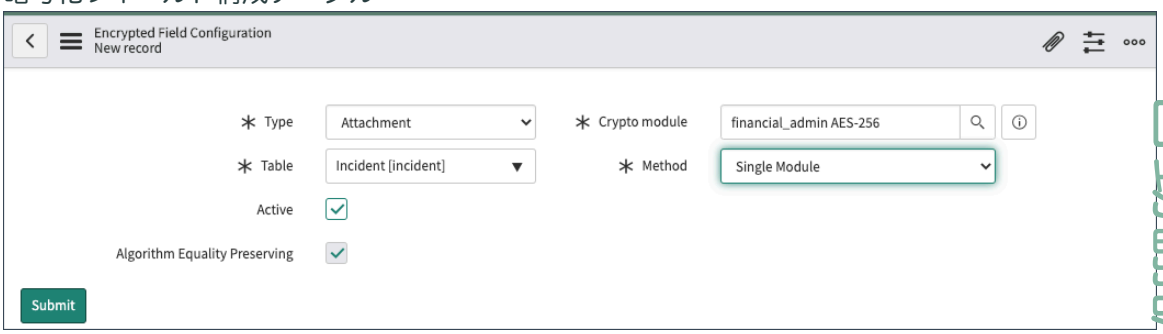
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

暗号化フィールドの構成フィールド

フィールド	説明
タイプ	選択したテーブルから添付ファイルを暗号化するために個人キーを使用するには、添付ファイルを選択します。この例の場合、インシデントを選択します。
テーブル	機密情報にアクセスするテーブルを選択します。この例では、インシデント [インシデント] を選択します。
有効	フィールド構成を使用できるようにするために、アクティブをマークします。
アルゴリズム等価性保存	列レベルの暗号化を選択すると、選択したテーブルに基づいてこのフィールドが表示されます。
暗号化モジュール	個人キーで使用するために作成したモジュールを選択します。
メソッド	単一モジュールオプションは、1 つのモジュールにポリシーを適用するために使用されます。複数モジュールは、複数のモジュールにまたがってポリシーを適用するために使用されます。

暗号化フィールド構成テーブル



6. [送信] をクリックします。

   モジュールアクセスポリシーを確立して、暗号化モジュールへのアクセスをアサインします。詳細については、「モジュールアクセスポリシーを作成する」を参照してください。

7. 移動先 キー管理 > モジュールアクセスポリシー > すべて.
8. [新規] をクリックします。
9. フォームに次のように入力します。

モジュールアクセスポリシーフィールド

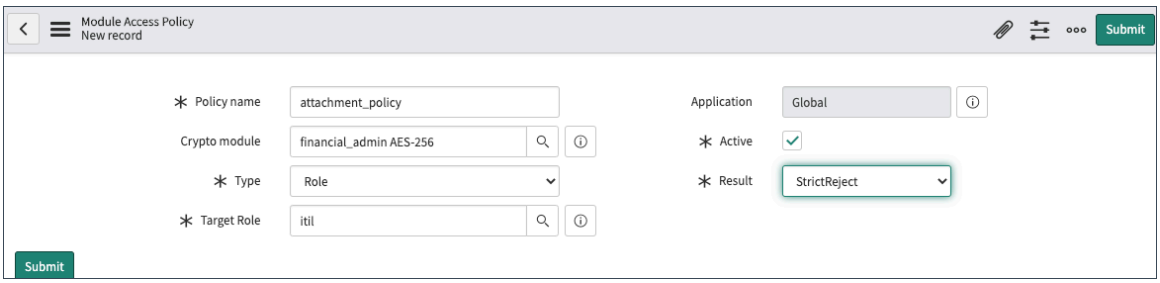
フィールド	説明
ポリシー名	ポリシーの名前 (「添付ファイルポリシー」など) を入力します。
暗号化モジュール	キーを暗号化するために作成した暗号化モジュールを選択します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

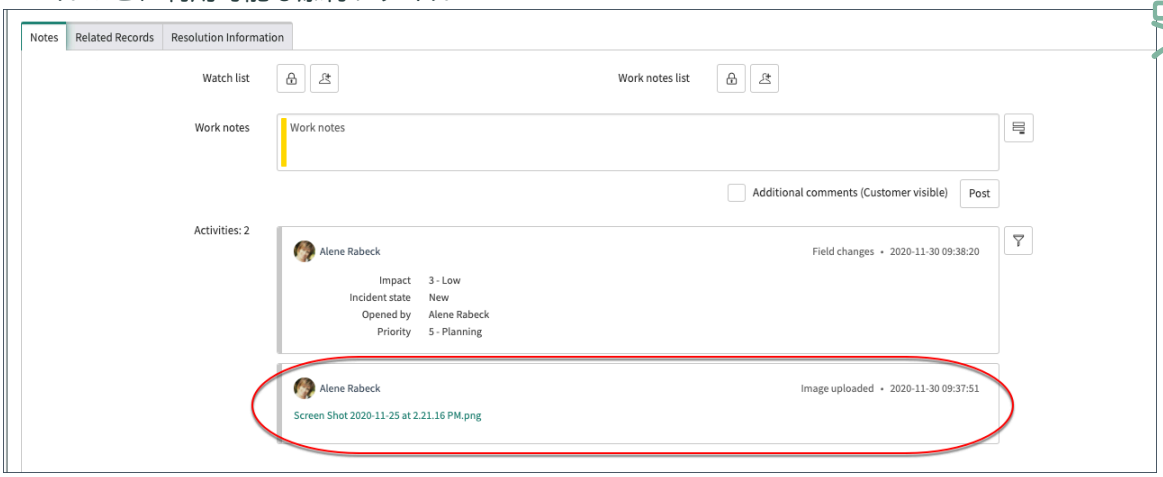
フィールド	説明
タイプ	割り当てられたロールを持つユーザーからの暗号化フィールドへのアクセスを制限するには、ロールを選択します。
ターゲットロール	暗号化フィールドにアクセスできないロールを選択します。この例では、**itil** を選択します。
有効	モジュールアクセスポリシーを使用できるようにするには、このチェックボックスをオンにします。
結果	選択したロールから添付ファイルへのアクセスを制御するには、[厳格な却下] を選択します(選択したロールにアクセス権を付与するには、[追跡] を選択します)。

モジュールアクセスポリシーフォーム



10. [送信] をクリックします。
11. 管理者またはインシデントを作成したユーザーとして、[インシデント] に移動し、メモ関連リストのアクティビティに添付ファイルを追加します。

ロールごとに利用可能な添付ファイル



12. 暗号化された添付ファイルへのアクセスが制限されているユーザーとしてログインします。
13. インシデントを開き、アクティビティ：セクションまでスクロールします。制限付きロールのユーザーは、添付ファイルを開くためのリンクにアクセスできません。
14. これで、顧客指定のキーを使用して、列レベルの暗号化で特定の添付ファイルへのアクセスを制御できました。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Infrastructure Security

Infrastructure Security のツールを使用して、クライアントからサーバーへのトラフィックを暗号化するためにインスタンスが使用する証明書を作成、アップロード、および管理します。

Infrastructure Security プラグインには、トランスポートレイヤーセキュリティ (TLS) の暗号と証明書の管理に使用できるツールが用意されています。インスタンスは TLS を使用して、クライアントからサーバーへのトラフィックを暗号化します。

インスタンスで使用する暗号を選択する

管理者は、[**TLS]** ページを使用して、インスタンスで使用するデータセンターの暗号を構成したり、暗号を試行する順序を選択したりできます。

独自の証明書を生成してアップロードする

Infrastructure Security のツールを使用して、選択した認証局で署名可能な独自の証明書署名要求を生成します。その後、ツールを使用して署名済み証明書をインスタンスのロードバランサーにアップロードできます。

暗号と証明書のステータスを監視する

[TLS 設定] および **[SYOC** 設定] ページを使用して、暗号と証明書に加えた変更のステータスを表示します。

Infrastructure Security プラグインのインストール

これらの機能の使用を開始するための ServiceNow の Infrastructure Security Settings (com.glide.infrastructure_security) プラグインをインストールします。プラグインのアクティブ化の詳細については、「プラグインをアクティブ化する」を参照してください。

プラグインをインストールした後、システムプロパティを true に設定して、Sign Your Own Security (SYOC) 機能を有効にします*sn_infra_sec.syoc.enabled*。

注:
インスタンスで *sn_infra_sec.syoc.enabled* プロパティを使用できない場合は、作成する必要があります。このプロセスの詳細については、「Add a system property」を参照してください。

証明書署名要求の生成

[証明書署名 (CSR) を生成] ページを使用して、インスタンスロードバランサーの顧客署名証明書をサポートする証明書署名要求を作成します。

始める前に
必要なロール：admin

ServiceNow でカスタム URL を使用する方法については、「カスタム URL をインスタンス URL として設定」を参照してください。

手順

1. 移動先 すべて > インフラストラクチャのセキュリティ設定 > **CSR** を生成.
2. 1 つ以上のドメインを要求に追加します。
   a. [ドメイン] 見出しの下にある [追加] ボタンを選択します。
   b. ポップアップウィンドウで、ドメインを入力して **[OK]** を選択します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

c. 必要に応じて、上記の手順を繰り返してさらにドメインを追加します。

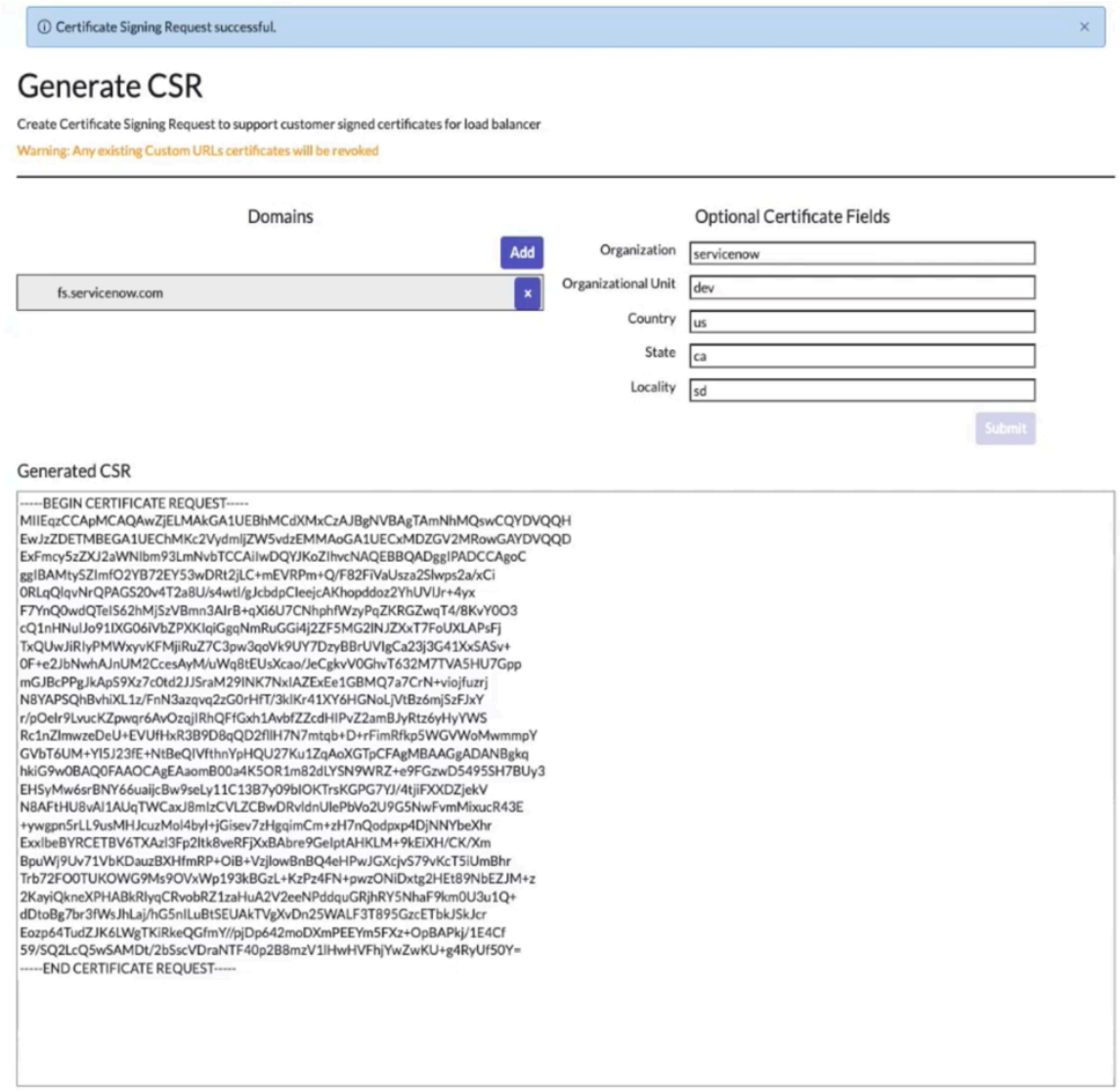
> **注:**
> ドメインを削除するには、各ドメイン エントリの左側にある [X] ボタンを選択します。

3. 要求に含める情報を [オプションの証明書] フィールドに入力します。

4. [送信] を選択します。

> **警告:**
> 別の要求の生成中に要求を送信することはできません。この問題が発生すると、"リソースが競合しています" というエラーが表示されます。処理を続行するには、現在の要求をキャンセルするか、現在の要求が処理されるのを待ってから別の要求を送信します。

[送信] を選択すると、インスタンスによって証明書署名要求が生成されます。要求が [生成された **CSR]** フィールドに表示されます。



5. [生成された **CSR (Generated CSR)]** フィールドの内容をコピーします。

次のタスク

任意の認証局を使用して証明書要求に署名します。選択した認証局によってこのプロセスが定義されます。そのプロセスについては、当局のドキュメントを参照する必要があります。署名付き証明書を

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

取得したら、「」の手順 インスタンスへの証明書のアップロードを使用してインスタンスにアップロードします。

Key Management Framework (KMF) による Password2 暗号化

Key Management Frameworkでサポートされており、Password2 (双方向暗号化) フィールドタイプを使用して、職務の分離、キー保護、およびライフサイクル管理でカスタムフィールドを暗号化および復号化します。この暗号化と復号化は NIST 800-57 ガイドラインに従って行われ、FIPS 140-2-L3 保護を提供します。

Password2 は、双方向暗号化でパスワードを格納するテキストフィールドです。双方向暗号化では、インスタンス内で復号化できるセキュアな暗号化された値としてデータを格納します。

> **ヒント:**
> Vancouver リリース以降、管理者は password2 フィールドの 3DES 暗号化を廃止して、新しい Advanced Encryption Standard (AES) を導入できます。詳細については、「password2 フィールドの GlideEncrypter を廃止」を参照してください。

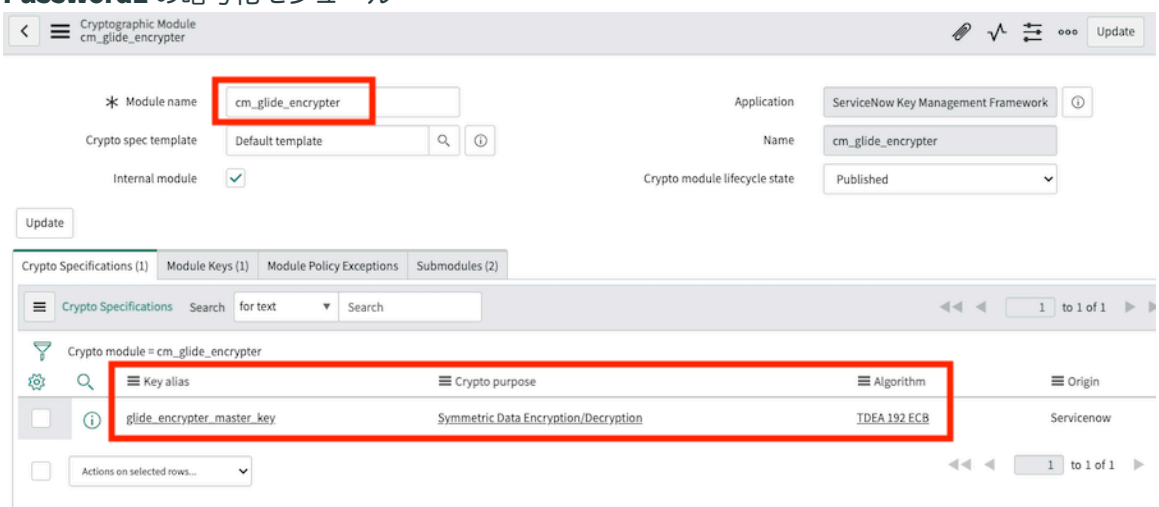
アクティベーション

Password2 機能はデフォルトでアクティブにされています。この機能は *glide.kmf.encrypter.enabled* プロパティで制御され、すべての新しいインスタンスとアップグレードに対して **true** に設定されます。Password2 を使用するために 列レベル暗号化エンタープライズ を有効にする必要はありません。

Password2 の仕組み

Key Management Frameworkでは、基本システムの親暗号化モジュール **cm_glide_encrypter** が提供されます。このモジュールは、暗号化仕様と が従来の Password2 フィールドを復号化できるキーを提供します。

Password2 の暗号化モジュール



この cm_glide_encrypter モジュールにはサブモジュールを含めることができ、それぞれに独自のモジュールキーと仕様があります。Password2 フィールドがあるアプリケーションと同じアプリケーションスコープにサブモジュールが存在する場合、そのサブモジュールが使用されます。たとえば、ServiceNow　カスタマーサービス アプリケーションのテーブルにサブモジュールがあり、カスタマーサービス アプリケーションスコープのテーブルの Password2 フィールドに情報を書き込むと、暗号化プロセスは カスタマーサービス サブモジュールを呼び出します。プロセスでは、一意の AES 256 GCM 暗号化キーによる暗号化と復号化にもそのサブモジュールのキーが使用されます。アプリケーションスコープごとに 1 つのサブモジュールが許可されます。親モ

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ジュールは常にグローバルスコープに使用されるわけではありません。通常、新しいフィールドでは instance_level_glide_encrypter が使用されます。

注:
Washington DC で独自のサブモジュールを作成することはできません。サブモジュールは、Now Platform のさまざまなアプリケーションプラグインで提供されます。サブモジュールのキーはローテーションできますが、親の cm_glide_encrypter モジュールのキーはローテーションできません。

ドメイン分離とオンプレミスの顧客

KMF Password2 では Domain Separation はサポートされていません。Password2 はオンプレミスインスタンスで使用できます。

従来の **Password2** と現在の **Password2**

Washington DCで、既存の Password2 フィールドがアップグレードされました。

Password2 の現在の実装：

- NIST 800-57 キーラッピングガイドラインに従って Key Management Framework を使用し、キー階層全体に FIPS 140-2-L3 保護を提供します。
- 特定のアプリケーション専用の一意の KMF Password2 サブモジュールを作成し、アプリケーションスコープ全体を制御する機能が含まれています。各サブモジュールには、独自の AES 256 GCM 暗号化キーがあります。

スクリプトの **Password2** フィールド

スクリプトを使用して Password2 フィールドにアクセスする場合は、テーブルスコープと同じスコープでスクリプトを実行します。setDisplayValue() を使用して Password2 値を暗号化し、getDecryptedValue() を使用して値を復号化して読み取ります。

注:
Password2 フィールドで GlideEncrypter() API を使用しないでください。

このサンプルスクリプトは、「table_xyz」テーブルの password2 列の my@Password を暗号化する方法を示しています。

```
var  gr =  new GlideRecord('table_xyz');
gr.setDisplayValue('pwd2column_name', 'my@Password');
gr.insert();
```

重要:
Password2 フィールドに setValue() API を使用することはできません。

このサンプルスクリプトは、同じフィールドを復号化して値を取得する方法を示しています。

```
var  gr =  new GlideRecord('table_xyz');
gr.query();
gr.next();
var ge=gr.getElement('pwd2column_name');
var ged1 = ge.getDecryptedValue();
```

重要:
getDecryptedValue() API はスコープ対象ではありません。グローバルに利用可能です。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

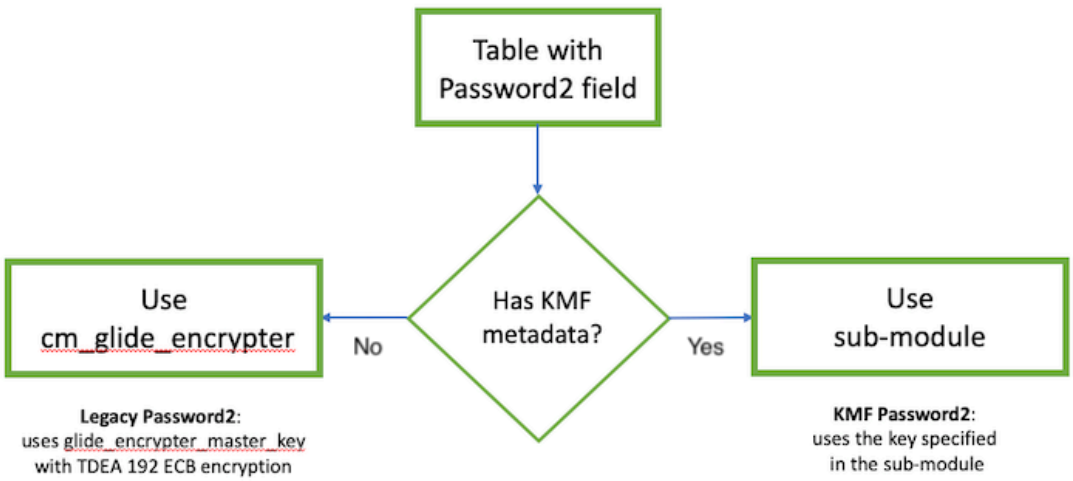
自動翻訳

1. Password2 フィールドのデータを暗号化すると、Password2 フィールドが存在するアプリケーションのスコープが決定されます。
2. プロパティが *true* に設定されている場合、アプリケーションと同じスコープを持つ **cm_glide_encrypter** 親モジュールのサブモジュールが検索されます。

   注:
   同じスコープのサブモジュールが存在する場合は、サブモジュール仕様とキーを使用して暗号化が実行されます。

この図は、インスタンスが Password2 フィールドのデータを復号化する方法を説明しています。

Password2 復号化フロー



KMF Password2 移行ジョブ

以前のリリースからアップグレードする顧客向けに、移行ジョブが提供されています。従来の Password2 暗号化で暗号化されたデータを KMF Password2 サブモジュールキーで再暗号化します。再暗号化は、アプリケーションスコープ内に Password2 フィールドがあり、そのスコープ用に作成されたサブモジュールもあるテーブルにのみ適用されます。たとえば、**XYZ_example** アプリケーション (**XYZ_example** アプリケーションスコープを持つ) の従来の Password2 フィールドは、**XYZ_example** アプリケーションスコープのサブモジュールが cm_glide_encrypter 親モジュールの下に存在する場合にのみ再暗号化されます。

サブモジュール内の KMF Password2 暗号化キーは、KMF キー階層で保護されます (エンベロープ暗号化)。

キー管理を使用したクラウド暗号化

ServiceNow® クラウド暗号化 は、拡張キー管理とともに、ブロック暗号化を使用したデータベースの暗号化ストレージを提供します。クラウド暗号化は ServiceNow Platform Encryption サブスクリプションバンドルで利用可能です。

クラウド暗号化は以下の機能を提供します。

- 職務の分離
- ServiceNow 管理キーのローテーション

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

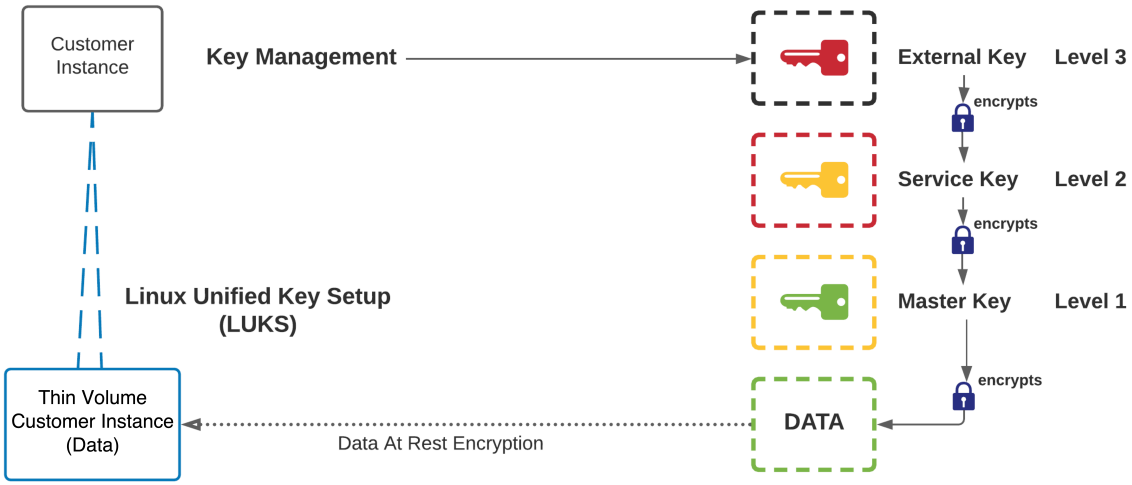
自動翻訳

- 顧客管理キーオプション

> **注:**
> 組織が独自の暗号化ツールまたはライブラリ、エンタープライズキー管理システム、またはハードウェアセキュリティモジュール (HSM) によって生成されたキーマテリアルを使用する必要がある場合は、このオプションを使用します。詳細については、「キー管理操作」を参照してください。

次の図は、クラウド暗号化 の仕組みを示しています。

クラウド暗号化の概要



クラウド暗号化 キー管理モジュールは、次のサブモジュールで構成されています。

- キー管理操作：
  - キーのリストにアクセスします。
  - キーのローテーション操作を実行します。
  - 顧客管理キーを取り消します。
- キー管理トランザクション：

  使用されたキーに対して発生したすべてのトランザクションを参照します。

  独自の顧客管理キーを使用して暗号化を行います。

状況によっては、顧客管理キーの使用時にキーの取り消し要求を選択できます。まず、カスタマーサービス & サポート からキーの取り消し機能を要求して法令による補遺を完了する必要があります。

[クォーラムコントロールポリシー設定 (Quorum Control Policy Settings)] オプションは、取り消し機能が有効の場合にアクティブ化されます。無効の場合、モジュールがメニューに表示されません。この機能は、顧客管理キーを使用する場合にのみアクティブ化できます。このポリシーでは、取り消し機能がアクティブ化されていれば、クォーラムに関する設定を構成できます。この機能の詳細については、「クォーラムコントロールポリシー」を参照してください。

クラウド暗号化 は、本番インスタンスと非本番インスタンスの両方で MariaDB データベースをサポートしています。Swarm64 拡張を使用する Postgres は ServiceNow 読み込みレプリカデータベースでサポートされています。

クラウド暗号化 のライセンスの詳細については、「暗号化とキー管理のサブスクリプションバンドル」を参照してください。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

ライセンスを取得したお客様が Cloud Encryption へのインスタンスの移動を要求するには、KB1117369 の手順に従ってください。インスタンスで **Cloud Encryption** を有効にするために Service Catalog アイテムを要求するには、顧客管理者またはパートナー管理者ロールを持っている必要があります。この機能を有効にするには、1 時間のメンテナンス期間が必要です。

キー管理操作

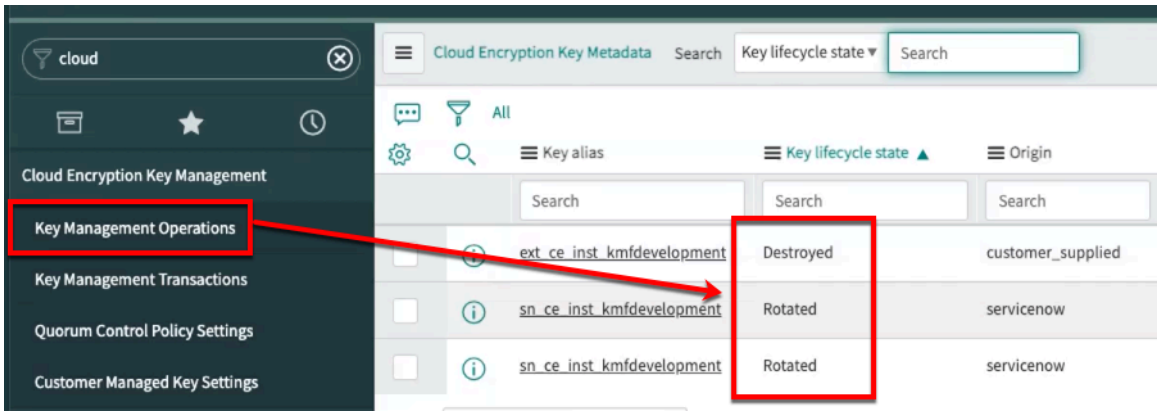
キー管理操作サブモジュールは、で使用される ServiceNow クラウド暗号化すべての暗号化キーを表示および管理するためのアクセスを提供します。

Cloud Encryption の開始

キーのライフサイクルステータス

システムには常に 1 つのアクティブなキーしか存在しません。キーを選択すると、ローテーションされたキーまたは取り消されたキーや対応するタイムスタンプなど、選択したキーのアクティビティにアクセスできます。

キーのライフサイクルステータスは、実行されたキー管理操作に従って更新されます。



詳細は「ServiceNow 管理キーのローテーション」または「顧客管理キーのローテーション」を参照してください。

注:
キーローテーションプロセスは完了までに 20 分かかる場合があります。

ServiceNow 管理キーのローテーション

アクティブなクラウド暗号化 ServiceNow管理キーをローテーションします。

始める前に
必要なロール：kmf_admin、kmf_cryptomanager

重要:
カスタマー マネージド キーを使用している場合は、「」を参照してください 顧客管理キーのローテーション。

手順

1. 移動先 すべて > クラウド暗号化キー管理 > キー管理操作.
   クラウド暗号化 のキーメタデータのリストがロードされます。インスタンスで使用されているすべてのキーがリストされます。一度に 1 つのキーのみをアクティブにすることができます。

   クラウド暗号化モジュールに初めてアクセスすると、最初のキーローテーションが実行された後にキーエントリが使用可能になります。ServiceNow 管理キーがシステムのデフォルトです。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

2. テーブルからアクティブなキーを選択します。
   [キー定義] テーブルに、ServiceNow で生成されたキーに関する一般的な情報が表示されます。
3. [キーのローテーション] ボタンを選択します。
   キーのローテーションを続行するか操作をキャンセルするかを選択できる通知が表示されます。
4. **[OK]** を選択してキーをローテーションします。
   [キー定義] ページの上部に確認メッセージが表示されます。
5. [キー管理操作] 画面に戻り、クラウド暗号化キーメタデータテーブルを更新します。
   現在のアクティブなキーと、現在のアクティブなキーの代わりにローテーションするために生成されているキーのエントリが表示されます。利用可能なさまざまなステータスについては、「キー管理フレームワークのキーライフサイクルステータス」を参照してください。

   アクティブなキーはキーバージョン `0` でリストされ、生成されたキーのバージョンは `1` です。
6. 元のキーのエントリを開くとキー管理トランザクションが表示されます。
   詳細については、「キー管理トランザクション」を参照してください。
   前にアクティブだったキーのバージョン `0` のキーのライフサイクルステータスが [ローテーション済み] にアップデートされ、新しいキーのバージョン `1` が [有効] になります。

顧客管理キーの準備

次の手順に従って、インスタンスにアップロードする顧客管理キーを準備します。

始める前に

必要なロール：sn_kmf.cryptographic_manager、sn_kmf.admin

このタスクについて

カスタマー マネージド キーの場合は、任意の暗号化ライブラリまたは HSM を使用してキーを生成できます。このキーは AES 256 ビットのキーであり、RSAES_OAEP_SHA_256 暗号化スキーマを使用した Cloud Encryption ラッピング証明書でラップされている必要があります。

注:

OpenSSL 暗号化ツールを使用してキーを生成する場合、OpenSSL バージョンはバージョン 1.1.1x 以降である必要があります。

を使用してカスタマー マネージド キー Windowsを作成してラップする場合は、Git Bash などの Bash シェル サポート アプリケーションを使用してラップされたキーを生成する必要があります。

手順

1. OpenSSL を使用して、AES-256 ビット対称キーとして使用するランダム値を生成します。

   互換性のために、対称キーには次の属性が必要です。

属性	値
キータイプ	Advanced Encryption Standard (AES) アルゴリズムベースの対称キー。
鍵サイズ	256 ビット (32 バイト)
キーラッピング要件	○ RSA 暗号化アルゴリズム ○ 最適な非対称暗号化パディング (OAEP)

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

属性	値
	○ SHA-256 ハッシュ関数 (RSAES_OAEP_SHA_256) ○ Base64 アルゴリズムを使用したエンコード

2. 「openssl rand 32 > plaintext_key.bin」のようなファイルにキーを保存します。

> **重要:**
> 今後の参照のためにこのファイルを安全に保存してください。このキーは、アップロード用の公開鍵でラップされます。

3. インスタンスからダウンロードしたラッピング証明書ファイルから公開キーを抽出します。

```
openssl x509 -pubkey -noout -in wrapping_cert.pem > public_key.pem
```

> **注:**
> ラッピング証明書をダウンロードするための情報を参照してください。

4. RSAES_OAEP_SHA_256アルゴリズムを使用して、ラッピング証明書と一緒にダウンロードした公開鍵で生成されたキーをラップします。

```
cat plaintext_key.bin | openssl pkeyutl -encrypt -inkey public_key.pem -pubin -pkeyopt
 rsa_padding_mode:oaep -pkeyopt rsa_oaep_md:sha256 | openssl base64 -A -out
 wrapped_key.txt
```

このコマンドで指定されたファイルには、CMK プロセスの SN に提供できるラップされた顧客管理キーが含まれています。

ServiceNow と顧客管理キーの切り替え

で使用するServiceNow クラウド暗号化カスタマー マネージド キーとServiceNowマネージド キーを切り替えます。

デフォルトでは、インスタンスは ServiceNow 管理キーを使用するように構成されていて、ServiceNow による暗号化キーの生成がアクティブになっています。ただし、管理者はカスタマー マネージド キーを使用することを選択できます。ServiceNow 管理キーに戻すことも選択できます。

顧客管理キーのローテーション

の クラウド暗号化顧客管理キーをラップした後、顧客管理キーをインスタンスにローテーションします。

始める前に

必要なロール：kmf_admin、kmf_cryptomanager

手順

1. 移動先 すべて > クラウド暗号化キー管理 > キー管理操作.
   [Cloud Encryption のキーメタデータ **(Cloud Encryption Key Metadata)]** リストがロードされます。インスタンスで使用されているすべてのキーがリストされます。
2. **[Cloud Encryption** のキーメタデータ **(Cloud Encryption Key Metadata)]** リストで、アクティブなキーのレコードを開きます。
   キーが複数ある場合は、[キーのライフサイクルステータス] が [有効] であるキーを選択します。インスタンスでは、有効なキーは 1 つのみです。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

3. キー定義レコードで、[キーのローテーション] ボタンを選択します。
4. [顧客管理キーをアップロード] ウィンドウで、リストされている手順を実行します。

   a. [ラッピング証明書のダウンロード] を選択します。
   `public_certificate....zip` がローカルマシンにダウンロードされ、顧客管理キーをラップするために使用されます。

   > ⚠ 警告:
   > 顧客管理キーのローテーションや顧客管理キーへの切り替えのたびにラッピング証明書をダウンロードすることで、証明書に関連する潜在的な問題を回避します。

   b. [参照] を選択して顧客管理キーをアップロードし、ラップされた暗号化キーを検索して選択します。
   別のファイルを選択するには、ファイルを選択して [削除] を選択します。

   c. [添付ファイル] ウィンドウを閉じます。

   d. [**OK]** を選択してキーをアップロードします。
   キーが適切な形式である場合は確認メッセージが表示され、それ以外の場合はエラーメッセージが表示されます。キーファイルはキー定義レコードに添付されています。

   [キー管理トランザクション] テーブルに、証明書のダウンロードとキーのアップロードの手順が表示されます。要求ステップの詳細については、「キー管理トランザクション」を参照してください。

5. 移動先 すべて > クラウド暗号化キー管理 > キー管理操作 をクリックしてキーのリストを表示します。
   キーのリストに、顧客管理キーの新しいレコードが表示されます。この新しいキーの [作成元] の値は **[customer_supplied]** で、ステータスは [有効] です。前のキーが [ローテーション済み] ステータスになっています。

顧客管理キーに切り替える

ServiceNow クラウド暗号化 の顧客管理キーを使用します。

始める前に

必要なロール：kmf_admin または kmf_cryptomanager

顧客管理キーに切り替えるには、この手順の一環として、ラップされた顧客管理キーをアップロードする準備ができている必要があります。このキーをアップロードする準備の詳細については、「顧客管理キーの準備」を参照してください。キーのアップロード後、このプロセスによって新しいキーのキーローテーションが開始されます。

手順

1. 移動先 すべて > クラウド暗号化キー管理 > キー管理操作.
2. **[Cloud Encryption** のキーメタデータ **(Cloud Encryption Key Metadata)]** リストで、アクティブなキーのレコードを開きます。
   キーが複数ある場合は、[キーのライフサイクルステータス] が [有効] であるキーを選択します。インスタンスでは、有効なキーは 1 つのみです。
3. フォームの [関連リンク] セクションで、[顧客管理キーに切り替え] リンクを選択します。
4. [顧客管理キーに切り替え] ダイアログ ボックスで、[管理キーをアップロード] ボタンを選択します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

5. [顧客管理キーをアップロード] ダイアログボックスで、リストされている手順を実行します。

   a. [ラッピング証明書のダウンロード] を選択します。

   > ⚠ 警告:
   > 顧客管理キーのローテーションや顧客管理キーへの切り替えのたびにラッピング証明書をダウンロードすることで、証明書に関連する潜在的な問題を回避します。

   b. [参照] を選択し、プロンプトに従ってデバイスからキーを選択してアップロードします。

   c. [顧客管理キーに切り替え] を選択します。

   顧客管理キーに切り替える要求がインスタンスによって生成されます。現在のフォームで、元々アクティブであったキーの [キーライフサイクルステータス] が [ローテーション済み]に変わっていることがわかります。

6. 移動先 すべて > クラウド暗号化キー管理 > キー管理操作 をクリックしてキーのリストを表示します。
   キーのリストに、顧客管理キーの新しいレコードが表示されます。この新しいキーの [作成元] の値は **[customer_supplied]** で、ステータスは [有効] です。

タスクの結果
インスタンスが ServiceNow クラウド暗号化 の顧客管理キーを使用するようになりました。

> ℹ 重要:
> 暗号化キーのコピーは、常に安全な場所でキー管理操作に使用できるように確保します。このキーがないと、インスタンスにアクセスできなくなるおそれがあります。

ServiceNow 管理キーに切り替える

顧客管理キーから ServiceNow クラウド暗号化 管理キーに戻します。

始める前に
必要なロール：kmf_admin または kmf_cryptomanager

手順

1. 移動先 すべて > クラウド暗号化キー管理 > キー管理操作.
2. **[Cloud Encryption** のキーメタデータ **(Cloud Encryption Key Metadata)]** リストで、アクティブなキーのレコードを開きます。
   キーが複数ある場合は、[キーのライフサイクルステータス] が [有効] であるキーを選択します。インスタンスでは、有効なキーは 1 つのみです。
3. フォームの [関連リンク] セクションで、[**ServiceNow** 管理キーに切り替え] リンクを選択します。
4. [ServiceNow 管理キーに切り替え] ダイアログボックスで、[**ServiceNow** 管理キーに切り替え] ボタンを選択します。
   ServiceNow 管理キーに切り替える要求がインスタンスによって生成されます。現在のフォームで、元々アクティブであったキーの [キーライフサイクルステータス] が [ローテーション済み]に変わっていることがわかります。
5. 移動先 すべて > クラウド暗号化キー管理 > キー管理操作 をクリックしてキーのリストを表示します。
   キーのリストに、ServiceNow 管理キーの新しいレコードが表示されます。この新しいキーの [作成元] の値は **[ServiceNow]** で、ステータスは [有効] です。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

キーローテーションをスケジュール

管理キーの自動 ServiceNow ローテーションのスケジュールを設定します。このプロセスでは、暗号化キーが自動で廃止され、古いキーが新しく生成された暗号化キーに置き換えられます。顧客管理キーを使用している場合は、このスケジュールにより、カスタムキーを手動でローテーションするように促すリマインダーを提供できます。

始める前に
必要なロール：admin

手順

1. 移動先 すべて > クラウド暗号化キー管理 > スケジュールされたキーローテーション設定.
2. [スケジュールされたキーローテーションを有効にする] チェックボックスをオンにします。
3. ビジネスニーズに基づいて、残りのフィールドに入力します。

スケジュールされたキーローテーション設定

フィールド	説明
キーローテーション間の月数 (最大 60 か月)	キーローテーション間の月数。この値はデフォルトで 12 で、最大 60 か月にすることができます。
キーローテーションを実行する曜日	キーローテーションを実行する曜日。
キーローテーションを実行する時刻	キーローテーションを実行する時刻。
次回のキーローテーションの日時	次回キーローテーション実行予定の日時。この値は直接編集できず、選択に基づいて自動的に計算されます。
リマインダーを送信するキーローテーションまでの日数 (最大 15 日)	インスタンスが通知を送信するキーローテーションの実行日までの日数。
メール通知は、次に示す承認されたセキュリティ管理者のリストに送信されます	キーローテーションの通知を受信するユーザーのリスト。デフォルトでは、 システム管理者がこのリストに含まれています。

4. [送信] を選択します。
   [送信] を選択すると、フォームの上部に通知が表示されます。通知では、キーのローテーションと通知スケジュールを確認します。

> ⚠ **警告:**
>
> スケジュールされた各キーローテーションには一意の署名があるため、ジョブの完全性が保証され、不正な変更が検出されます。ジョブスケジュールの署名は、インスタンスごとに一意です。キーローテーションのジョブスケジュールをソースインスタンス A からターゲットインスタンス B にクローンすると、インスタンス B のジョブスケジュールは署名検証に失敗します。これが発生した場合は、[スケジュールされたキーローテーションを有効にする] チェックボックスをオフにしてから再度オンにすることで、署名を再作成できます。この問題の詳細については、「 KB1247113 」を参照してください。

顧客管理キーを取り消す

顧客管理キーの取り消し機能が有効になると、[キー管理操作] ページで取り消し操作を使用できるようになります。キーの取り消しとクォーラムの承認操作も管理できます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

始める前に
必要なロール：kmf_admin、kmf_cryptomanager

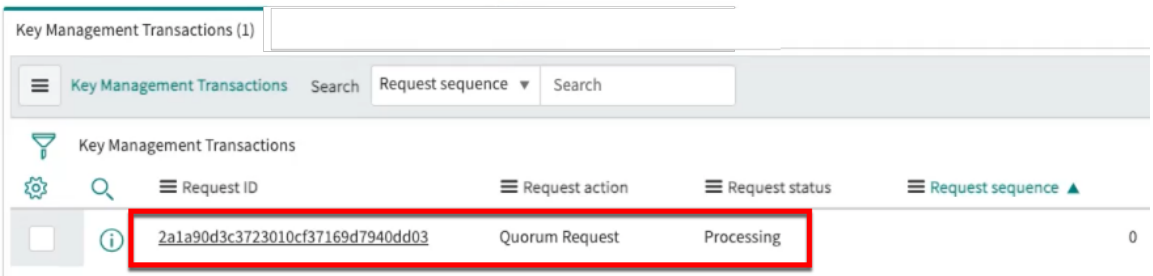
このセクションは、クラウド暗号化 へのオプションのアドオンである Cloud Encryption Withdraw and Resupply がライセンスされている場合にのみ適用されます。

手順

1. 移動先 すべて > クラウド暗号化キー管理 > > キー管理操作.
2. テーブルからアクティブな顧客管理キーを選択します。
   [キー定義] テーブルに、顧客キーに関する一般的な情報が表示されます。キーの取り消し機能が利用可能になります。
3. [キーを取り消す] を選択して、取り消しプロセスをトリガーします。

> **警告:**
>
> キーの取り消しの警告メッセージが表示されます。キーを取り消すと、インスタンスのシャットダウンがトリガーされ、取り消されたキーを使用して復元操作が実行されるまでそのままになります。
>
> > **危険:**
> > 取り消された同じキーでのみ復元操作を実行できます。別のキーにローテーションする場合は、取り消されたキーを復元した後に行う必要があります。
>
> 取り消された顧客管理キーが、ServiceNow がバックアップを保持する期間内に復元されない場合 (詳細については、バックアップおよび復元 SOP [標準運用手順] を参照)、インスタンスデータベースのバックアップにアクセスできなくなります。この方法で失われたバックアップデータは復旧できません。

4. **[OK]** を選択してキーを取り消します。
   キーの取り消し機能に疑問がある場合は、[キャンセル] を選択します。
   [キー定義] 画面に戻り、確認メッセージが表示されます。
5. [キー定義] ページを更新して、保留中の取り消し要求を表示します。



クォーラムコントロールポリシーが有効になっている場合、キーの取り消しを完了するには、承認ワークフローを正常に完了する必要があります。詳細については、「クォーラムコントロールを管理する」を参照してください。

顧客管理キーの再供給

キーの取り消し操作が完了したら、顧客管理キーをインスタンスに再供給する必要があります。

始める前に
必要なロール：kmf_admin、kmf_cryptomanager

> **注:**
> このセクションは、Cloud Encryption Withdraw and Resupply がライセンスされている場合にのみ適用されます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

手順

1. 移動先 Now Support と移動先 サービスカタログ > カタログ > インスタンス管理 > インスタンスの復元:管理キーを補充.
2. [要求] をクリックします。
3. [インスタンスの復元 - 管理キーの再供給 **(Instance Restore - Resupply Managed Key)**] ウィンドウで、[インスタンスを選択 **(Select Instance)**] ドロップダウンでインスタンスを選択します。
4. ラッピング証明書のテキストをクリックして、ラッピング証明書をダウンロードします。

> ⚠ 警告:
> 顧客管理キーをローテーションまたはアップロードするたびに、新しいラッピング証明書をダウンロードする必要があります。

5. アップロードするキーを準備します。
   このプロセスの詳細については、「顧客管理キーの準備」を参照してください。
6. [ステップ **4**] セクションで、[参照してアップロード **(Browse and upload)**] をクリックして、ラップされたキーをローカルデバイスからアップロードします。
   キーがアップロードされると、[以下のファイルは正常にアップロードされました **(Uploaded below file successfully)**] の下にキーが表示されます。キーを再アップロードする必要がある場合は、[ファイルを削除] をクリックし、前の手順で説明したようにキーを再度アップロードします。
7. [キーのローテーション] をクリックして、再供給を完了します。

クォーラムコントロールポリシー

クォーラムコントロールポリシーでは、選択された承認者の合計数が顧客管理キーの取り消しのクォーラムに到達するために必要な承認の最小数を指定します。

> ⚠ 警告:
> キーの取り消し機能をアクティブ化するには、法令による補遺に署名する必要があります。[クォーラムコントロールポリシー設定 (Quorum Control Policy Settings)] オプションは、取り消し機能が有効の場合に利用可能になります。無効の場合、モジュールがアプリメニューに表示されません。キーの取り消し後、暗号化キーが再供給されて再びアクティブになるまで、インスタンスは使用できなくなります。

状況によっては、キーの取り消しを作成できます。まず、カスタマーサービス & サポート からキーの取り消し機能を要求する必要があります。

クォーラムコントロールポリシーでは、選択された承認者の合計数が顧客管理キーの取り消しのクォーラムに到達するために必要な承認の最小数を指定します。たとえば、承認者が合計で 5 人いるのに、クォーラムに到達するために必要な承認が 4 回のみだとします。承認が 4 回得られると、取り消し要求が処理され、キーが取り消されます。

クォーラムの承認が有効なグループで取り消し操作が実行されるたびに、クォーラム承認のワークフローがトリガーされます。承認を出せるすべてのユーザーにメール通知が送信されます。タスクは承認者のアカウントでも生成され、承認者が ServiceNow アカウントにログインするとダッシュボードに表示されます。

このユーザーは、インスタンス、メール、または [キー管理操作] ページから承認を出せます。キーの取り消し操作はクォーラムに到達するまでブロックされます。

承認者の最小数に達すると、クォーラムに到達してキーの取り消しがトリガーされます。取り消しが実行され、要求を承認したユーザーの名前を含めてログに記録されます。

セットアップの詳細については、「クォーラムコントロールポリシー設定の構成」を参照してください。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

クォーラムコントロールポリシー設定の構成

クォーラムコントロールポリシー設定を構成するには、次の手順を実行します。

始める前に

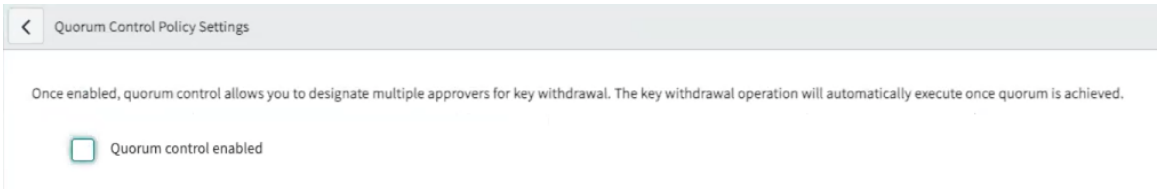
必要なロール：kmf_admin、kmf_cryptomanager

このタスクについて

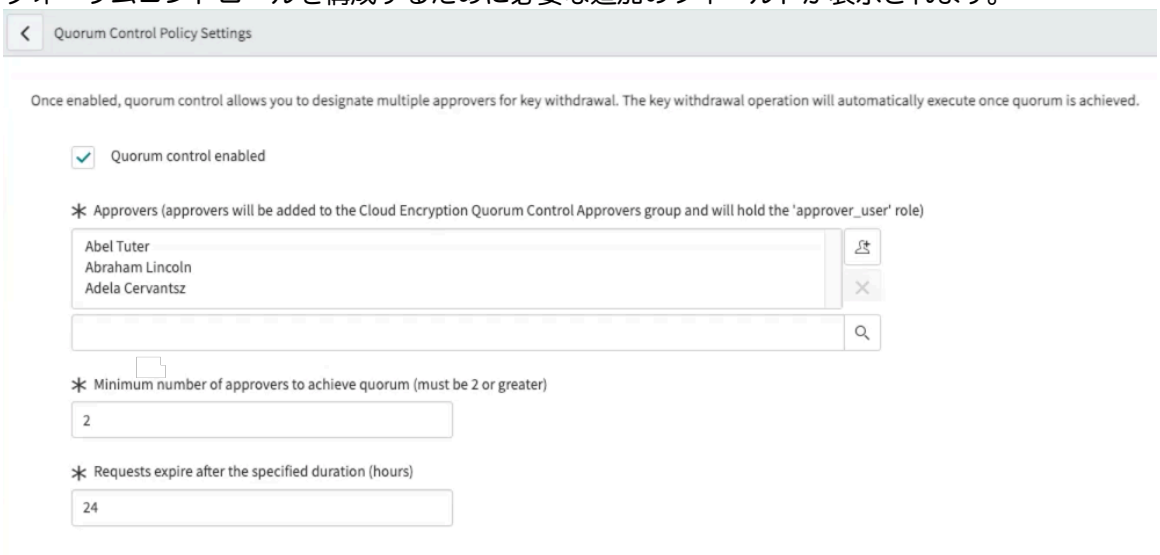
> **警告:**
> キーの取り消し機能をアクティブ化するには、法令による補遺に署名する必要があります。[クォーラムコントロールポリシー設定 (Quorum Control Policy Settings)] オプションは、取り消し機能が有効の場合に利用可能になります。無効の場合、モジュールがアプリメニューに表示されません。キーの取り消し後、暗号化キーが再度アクティブになるまでインスタンスは使用できなくなります。

手順

1. カスタマーサービス & サポート からキーの取り消し機能を要求します。
2. 移動先 クラウド暗号化キー管理 > クォーラムコントロールポリシー設定.
3. [クォーラムコントロールを有効にする **(Quorum control enabled)]** チェック ボックスをオンにします。



クォーラムコントロールを構成するために必要な追加のフィールドが表示されます。



4. フォームのフィールドをすべて入力します。
5. [送信] をクリックします。
   確認メッセージが表示されます。

次のタスク

取り消しのアクションは キー管理操作 で実行可能です。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

クォーラムコントロールを管理する

取り消し操作のワークフローがトリガーされた後に、[キー管理操作] ページからクォーラムアクションを管理できます。キーの取り消し操作はクォーラムに到達するまでブロックされます。

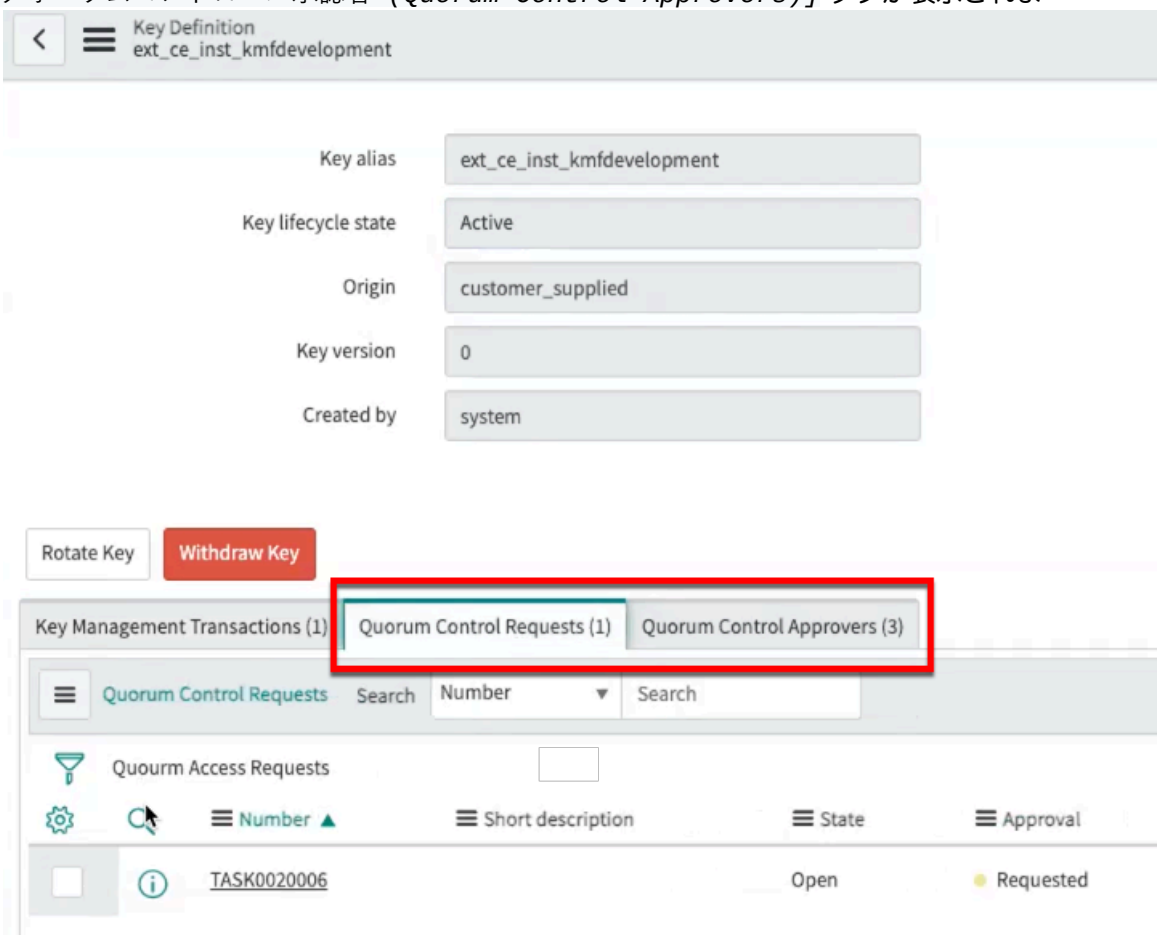
始める前に

必要なロール：kmf_admin または kmf_cryptomanager

クォーラムが承認または却下されると、クォーラムが達成または却下されたことを通知するメールがキー取り消しの要求者に届きます。

手順

1. キー管理操作 で見つかった顧客管理キーを取り消す手順を実行します。
2. アクティブ化した [クォーラムコントロールの要求 *(Quorum Control Requests)*] および [クォーラムコントロール承認者 *(Quorum Control Approvers)*] タブが表示されます。



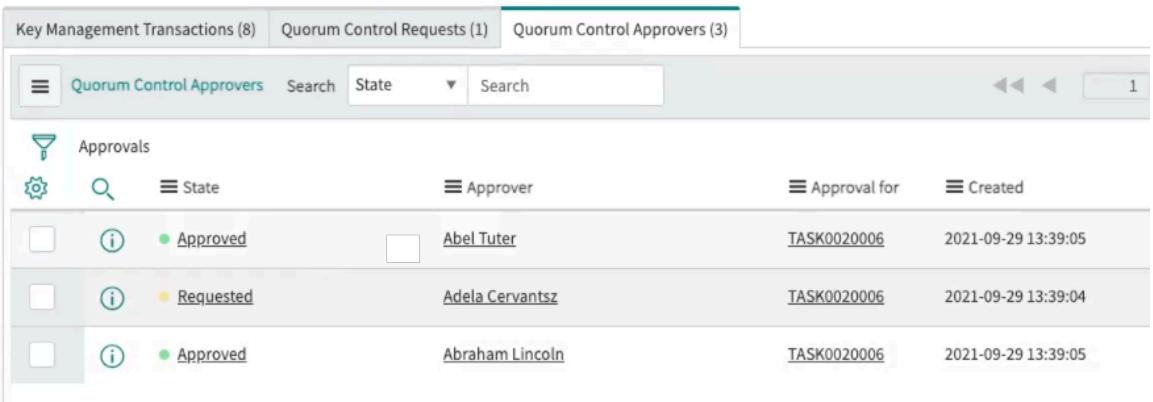
3. を開く クォーラムコントロール要求 作成された実際の要求を表示するタブ。
   - ステータス：
     - オープン：キーの取り消しアクションによってクォーラムの到達が処理待ちになっています。
     - 完了してクローズ：クォーラムに到達しているため、この特定のクォーラム要求に対してこれ以上のアクションを実行できません。
   - 承認：

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- 要求済み：承認メールが送信され、クォーラムに到達するためのワークフローがトリガーされました。
- 承認済み：キーが取り消され、インスタンスがシャットダウンされます。
- 拒否：クォーラム要求はキャンセルされ、この要求に対してこれ以上のアクションは実行されません。キーを取り消すには、新しい取り消し要求が必要となります。

4. [クォーラムコントロール承認者 (Quorum Control Approvers)] タブを開いて、承認者のリストと承認要求のステータスを表示します。



ステータス：

- 要求済み：承認者がまだ承認要求に対してアクションを実行していません。
- 承認済み：要求がメールまたは承認ページから承認されました。

5. [キー管理トランザクション] タブを選択して、キーの取り消し要求ステップの進捗を表示します。
   - ステップ 0 - クォーラム要求：実際のクォーラム要求。キーの取り消しの手順をトリガーするには、クォーラム要求を完了する必要があります。
   - ステップ 1 - キーの取り消し：キーの取り消しのステップ。このステップはステップ 2 ～ 7 で構成されています。
   - ステップ 2 - Request_preparation：トリガーする要求と、ラッピングおよびローテーションを作成します。
   - ステップ 3 - request_integrity_check：要求が正当で安全であることを検証します。
   - ステップ 4 - request_validation：進行中の要求があり、一度に 1 つのローテーション要求のみが処理できることを検証します。
   - ステップ 5 - hsm_key_delete：KeySecure を呼び出してアクティブなキーを削除します。
   - ステップ 6 - key_metadata_withdraw：アクティブなキーのメタデータのライフサイクルステータスを「破棄 (destroyed)」に変換します。
   - ステップ 7 - post_withdraw：インスタンスをシャットダウンする呼び出しを行います。

[クォーラムコントロール承認者 **(Quorum Control Approvers)]** タブ

キー管理トランザクションからのクォーラムコントロール要求を承認または拒否します。

始める前に

必要なロール：kmf_admin、kmf_cryptomanager

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. 移動先 すべて > クラウド暗号化キー管理 > キー管理トランザクション > クォーラムコントロール承認者.
2. テーブルからユーザー名を選択し、要求を [承認] または [拒否] します。

クォーラム要求の承認または拒否

クォーラム要求が作成されると、メンバーが必要とする承認の数が最小限になります。取り消し操作のワークフローがトリガーされた後は、いくつかの手法を用いてクォーラムアクションを管理できます。ユーザーは、[キー管理操作] ページの [インスタンス] にある [自分の承認 **(My Approvals)]** から、または要求メールから直接承認を出すことが可能です。キーの取り消し操作はクォーラムに到達するまでブロックされます。

始める前に
必要なロール：kmf_admin、kmf_cryptomanager

キー管理トランザクション

キー管理トランザクションサブモジュールには、インスタンス内の ServiceNow キーに対して発生したすべてのトランザクションが表示されます。

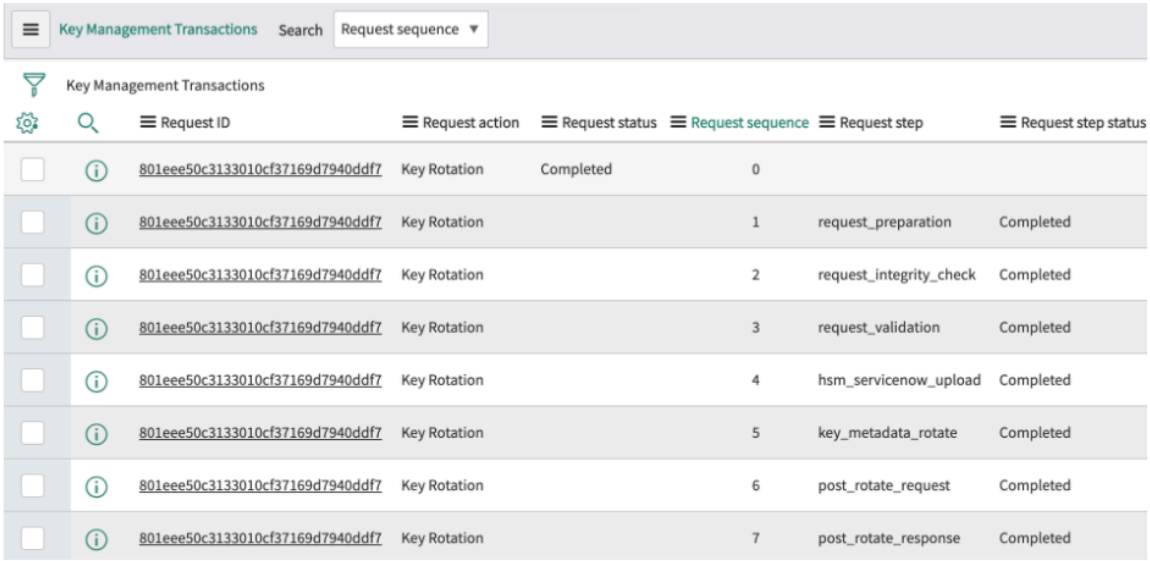
- キートランザクションは以下により定義されます。
  - いくつかの要求ステップで構成されます。
  - 1 つの要求 *ID* がすべての要求ステップで共有されます。
  - トランザクションの最初のステップ (要求シーケンス 0) では、トランザクション全体の現在のステータスが提供されます。

    次の画像で示されているように、最初のステップ 0 の全体的な要求ステータスは [完了] です。
- 個々の要求ステップで、トランザクションに関して以下を識別できます。
  - トランザクションの各ステップの順序は、ステップのシーケンス番号で識別できます。
  - 各トランザクションのステータスは、要求ステップのステータスから確認できます。
  - 最初のステップ以降のステップで失敗すると、トランザクション全体のステータスが [失敗] になります。すべてのステップが完了すると、トランザクションステータスも完了します。

次の画面は、ServiceNow キーのローテーションで表示される情報のタイプ例です。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



次の表は、[キー管理トランザクション] ページで利用可能なフィールド情報を示しています。

キー管理トランザクション

フィールド	説明
要求 ID	実行中のアクションに対する一意のシステム生成 ID 1 つの要求 ID が、すべての要求ステップで共有されます。
要求アクション	実行中のキー操作のアクションが表示されます。
要求ステータス	• 処理中:要求が入力されましたが、まだ完了していません。 • 完了:要求は正常に完了しました。 • 失敗:問題が発生し、プロセスが完了していません。 **注:** カスタマーサービス & サポート に連絡し、エラーが発生した要求番号を提供してください。
キーのエイリアス	英数字のエントリ
キーのライフサイクルステータス	定義については、「キー管理フレームワークのキーライフサイクルステータス」を参照してください。
作成元	• ServiceNow キー • 顧客管理キー
キーバージョン	キーがローテーションされると、バージョン番号がインクリメントされます。
要求シーケンス	システム内で要求が処理されている順序が表示されます。
要求ステップ	キーローテーション中にステップがシステムで処理されているかどうかが表示されます。ステップの数と内容は、実行されたキー操作のタイプによって異なります。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

キー管理トランザクション (続く)

フィールド	説明
	1. request_preparation：トリガーする要求と、ラッピングおよびローテーションを作成します。 **2.** request_integrity_check：要求が正当で安全であることを検証します。 **3.** request_validation:進行中の要求があり、一度に処理できるローテーション要求は 1 つだけであることを検証します。 **4.** attachment_process：添付ファイルからラップされたキーマテリアルを抽出します(顧客管理キーをローテーションする場合の追加ステップ)。 **5.** hsm_<キーのタイプ> _upload：ラップされたキーマテリアルを HSM、KeySecure にアップロードします。 **6.** key_metadata_rotate：新しいキーメタデータを生成します。 **7.** post_rotate_request：キーローテーションを実行する要求を送信します。 **8.** post_rotate_response：顧客インスタンスからの要求に基づいてキーローテーションを実行するための応答。 **注:** 要求ステップが完了しない場合にステータスの進行を分析するための カスタマーサービス & サポート 要求ステップを提供します。
要求ステップのステータス	• 完了：ローテーションに成功しました。 • 失敗:ローテーションに失敗しました。 **注:** 要求ステップが完了しない場合にステータスの進行を分析するための カスタマーサービス & サポート 要求ステップを提供します。

Cloud Encryption のログ記録

クラウド暗号化 のログ記録オプションについて説明します。

Cloud Encryption のログ記録のテーブル

以下のテーブルを使用して、インスタンスでの Cloud Encryption のトランザクションに関連するログ記録情報を検索します。

テーブル	説明
Cloud Encryption のメタデータ (Cloud Encryption Metadata) [dare_key_metadata]	Cloud Encryption のメタデータ (Cloud Encryption Metadata) は、ライフサイクル管理の重要なメタデータをキャプチャします。このテーブルでは、キーのライフサイクル、ステータス、およびバージョン情報を確認できます。このテーブルはキーを操作するたびに更新されます。
キー管理トランザクション [dare_key_request]	キー管理トランザクションは、キー管理トランザクションの情報をキャプチャします。この

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

テーブル	説明
	テーブルでは、トランザクションの各ステップのログ記録を確認できます。このテーブルではトランザクションのエラー情報が [エラーメッセージ] フィールドに記録されます。
システム監査 [sys_audit]	[システム監査] テーブルでは、インスタンスで行われたすべての監査済みレコードに対する挿入と更新をキャプチャします。このテーブルでは、インスタンス上のレコードに対する変更、変更が行われた日時、および変更を開始したユーザーアカウントを確認できます。

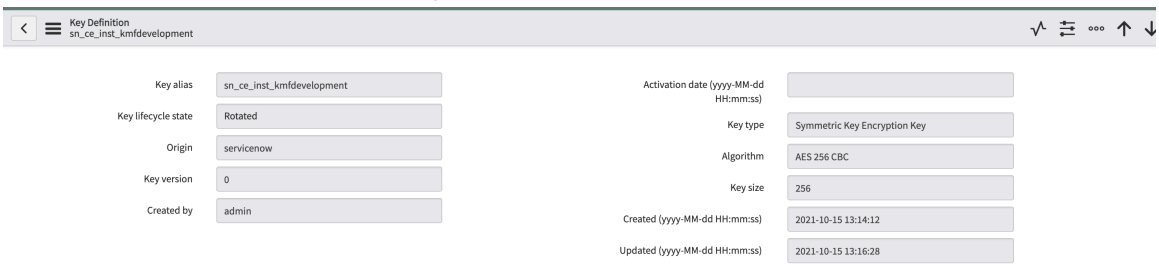
キーローテーション操作の監視

Cloud Encryption のキーメタデータ [dare_key_metadata] テーブルを使用して、キーのライフサイクルに関する情報を検索します。このテーブルでは、キーの作成元、アクティブ化日、ステータス、バージョンなどの情報を確認できます。

キー管理トランザクション [dare_key_request] テーブルを使用して、キー操作のトランザクションを監視します。このテーブルでは、進捗状況やステータス、また要求がプロセスのどのステップであるかなど、キーに関連するすべての要求を検索できます。完了した要求は、[完了] ステータスでこのテーブルに保持されます。

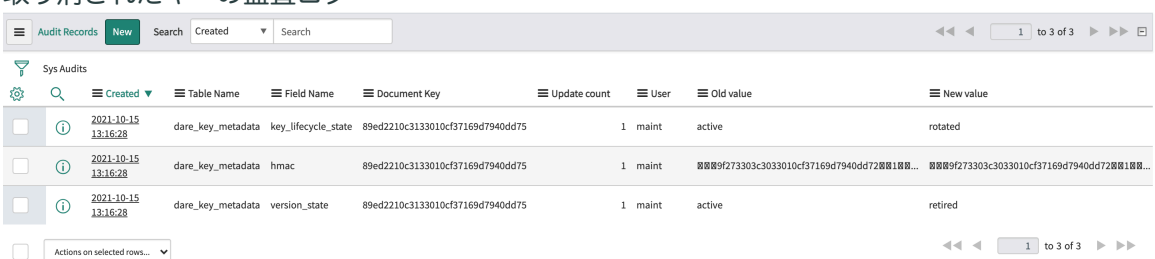
この例は、キーローテーションの操作を示しています。この操作中、古いキーのライフサイクルステータスがアクティブからローテーション済みに更新され、バージョンのステータスがアクティブから廃止に更新されます。

ローテーションされたキーのキー定義



システム監査 [sys_audit] テーブルで、管理者は Cloud Encryption のキーメタデータ [dare_key_metadata] テーブルのレコードに加えられた変更を確認できます。管理者はどのレコードがいつ更新されたかを確認できます。ログエントリには、変更されたフィールドおよび、古い値と新しい値も記録されます。

取り消されたキーの監査ログ

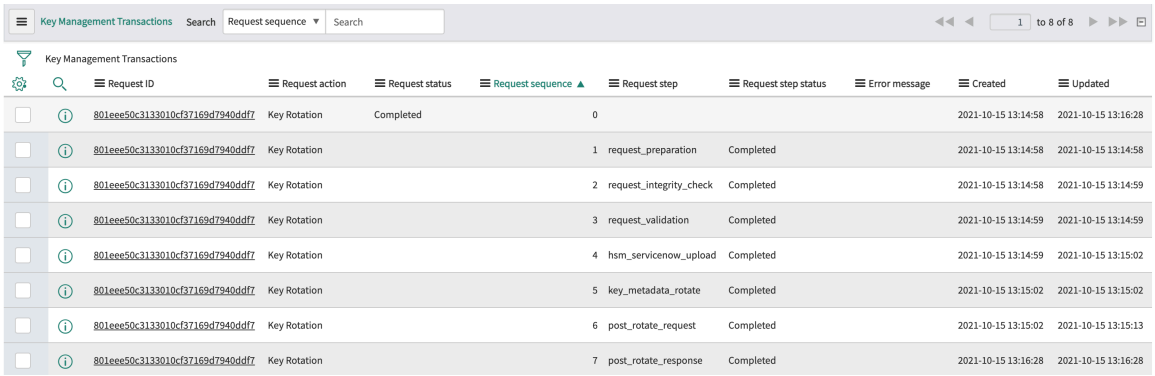


管理者は、Cloud Encryption のキーメタデータ [dare_key_metadata] テーブルにあるレコードを確認できます。以下の監査レコードでは、要求のステータスが処理中から完了に変更されています。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

取り消されたキーの監査ログ

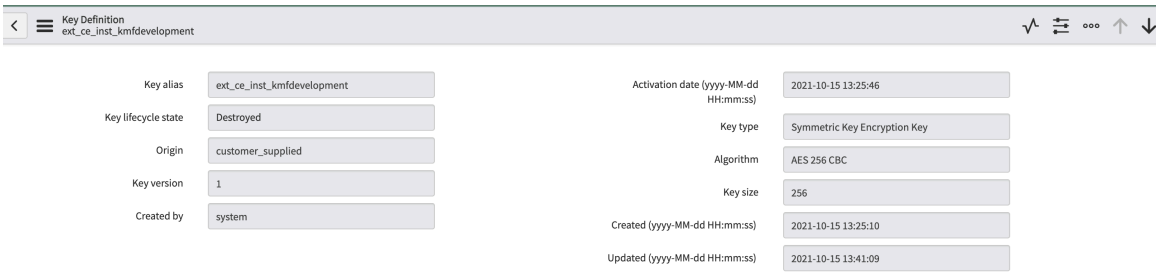


キーの取り消し操作のログ記録

キーの取り消しに関するログ記録情報は、監査 [sys_audit] テーブルに格納されます。このログ記録情報には、キーの取り消しを開始したユーザーと取り消しが行われた日時に関する情報が含まれています。

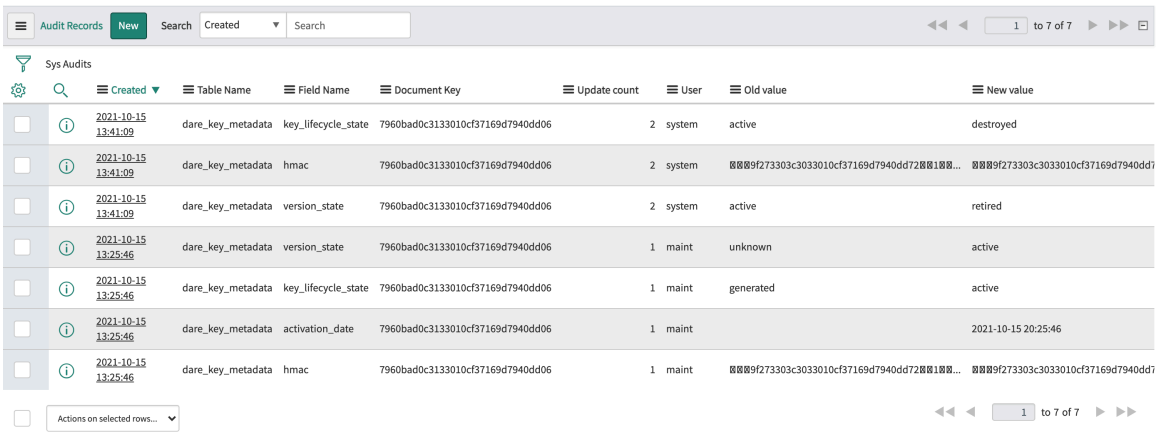
この例は、キーの取り消しの操作を示しています。この操作中に、キーのライフサイクルのステータスが [生成済み] から [アクティブ (active)] や [破棄 (destroyed)] に更新されます。鍵のバージョンが [不明] から [アクティブ] や [廃止] に更新されます。

取り消されたキーのキー定義



システム監査 [sys_audit] テーブルで、管理者は Cloud Encryption のキーメタデータ [dare_key_metadata] テーブルの変更内容を確認できます。

取り消されたキーの監査ログ



改ざん検出

改ざん検出を使用して、クォーラムコントロールの設定に対する不正な変更を検出することでセキュリティを向上させます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

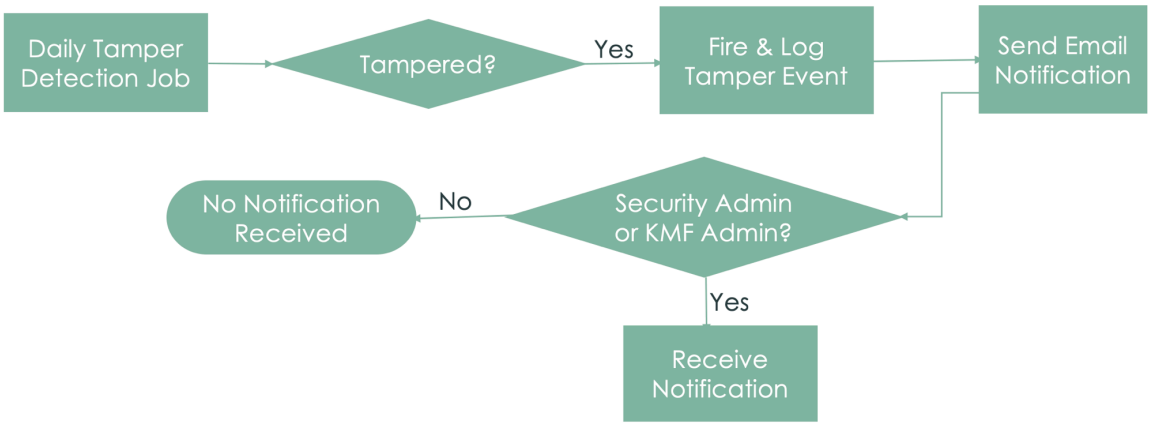
改ざん検出のプロセス

改ざん検出を有効にすると、不正な変更 (改ざん) がないかチェックすることで、クォーラムコントロール設定が検証されます。改ざん検出では、Hash-based Message Authentication Code (HMAC) を使用します。

1. 設定が変更または作成されると、インスタンスが HMAC を作成します。HMAC は設定 (dare_property) レコードの値に基づいて作成されます。
2. インスタンスでこれらの設定が使用されるたび、改ざん検出が HMAC を使用して設定を検証します。
3. 正常に検証された設定はプラットフォームで使用できます。検証されない場合は使用できません。

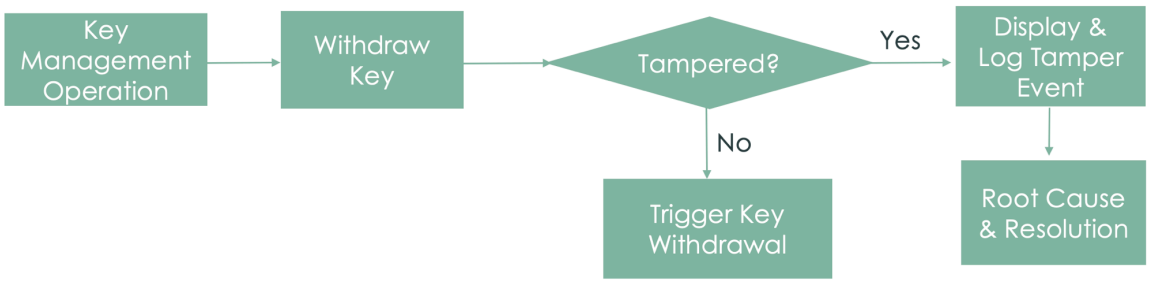
改ざん検出はインスタンスで毎日実行される

改ざん検出は、日次スケジュール設定済みジョブを使用して改ざんの設定をチェックし、検証が失敗した場合はノードログとセキュリティログに報告します。改ざん検出は、検証エラーに関する通知をセキュリティ管理者と KMF 管理者に送信します。



キーの取り消しの実行前に改ざん検出を実行する

改ざん検出では、キーの取り消しを要求するときにもプロパティを検証します。設定が検証に合格しないと、キーの取り消しは実行されません。この場合、キーの取り消しが競合しないうちに検証の問題を解決する必要があります。



改ざんの識別

検証に失敗すると、改ざん検出によってログが更新されます。

改ざん検出でクォーラムコントロール設定の検証に失敗すると、その失敗がノードログとセキュリティログに表示されます。ログのエントリーには、検証に失敗した設定 (dare_property) レコードの sys_id が含まれています。

```
2022-06-28 13:45:46 (582) Default-thread-5
 B6FAC1F6C3D01110CF37169D7940DD6E txid=231c4d72c310 SEVERE
```

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

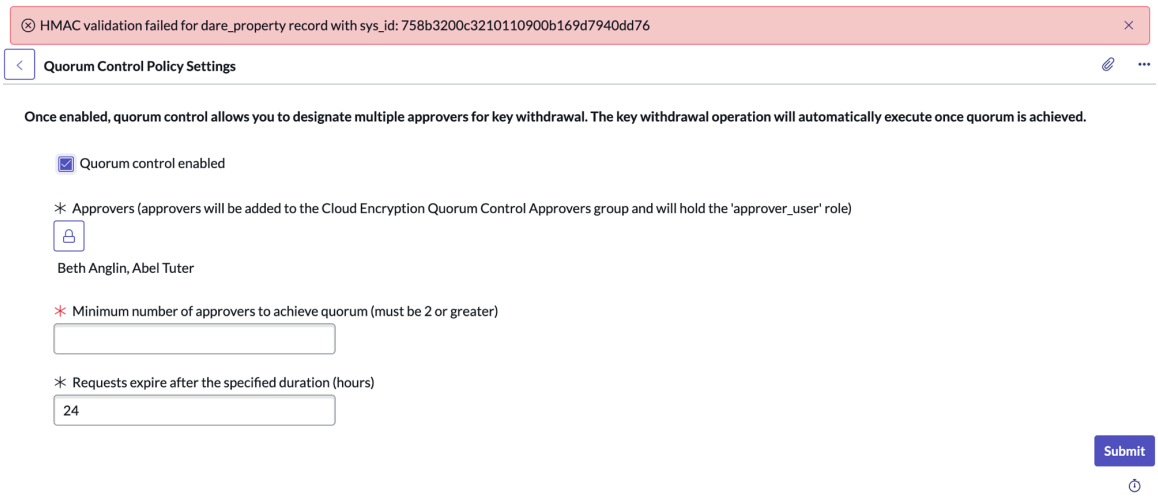
```
HMAC_VALIDATION_FAILED:The dare_property record with sys_id:
776e3200c3210110900b169d7940dd76 failed HMAC validation

2022-06-28 13:47:35 (264) Default-thread-8
B6FAC1F6C3D01110CF37169D7940DD6E txid=8e8cc972c310 SEVERE
HMAC_VALIDATION_FAILED:The dare_property record with sys_id:
758b3200c3210110900b169d7940dd76 failed HMAC validation
```

検証に失敗すると、この例のような情報がログ記録に表示されます。成功した検証はログに表示されません。

改ざん検出によりクォーラムコントロール設定ページに警告メッセージが表示される

クォーラムコントロール設定の検証に失敗した場合、インスタンスで [クォーラムコントロールポリシー設定 (Quorum Control Policy Settings)] ページを表示すると警告が表示されます。警告には、検証に失敗した設定 (dare_property) レコードの sys_id が含まれています。



改ざん検出は *Security Admin* および *KMF Admin* ロールのユーザーに通知を送信する

改ざん検出でクォーラムコントロール設定の検証に失敗した場合、セキュリティ管理者と KMF 管理者にこの例のような通知が届きます。

Subject: IMPORTANT: Cloud Encryption Properties Tampering Detected

The following list of Cloud Encryption properties appear to have been tampered.
Contact ServiceNow support for additional information and how to correct this issue.

Tampered properties:
com.glide.dare_key_mgmt.quorum.approvers(903a3212c3210110cf37169d7940dda8)

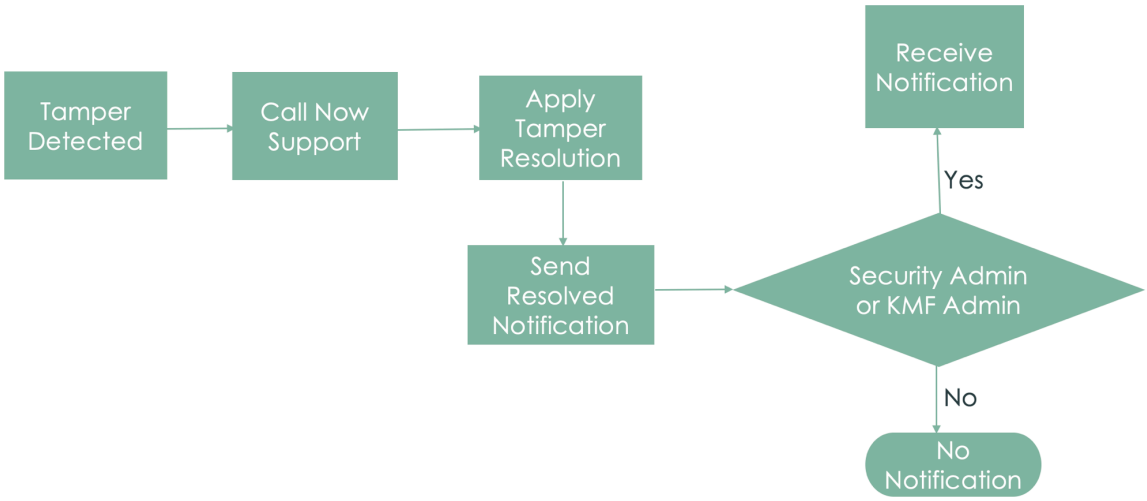
Ref:MSG0000109_q5pzYMS7hcgHXAoUhipc

ServiceNow サポートによる改ざんの問題の解決

重要:
改ざん検出による検証の失敗は、ServiceNow サポートの支援がなければ解決できません。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



改ざん検出でクォーラムコントロールの設定の検証に失敗した場合は、ServiceNow サポートに連絡して問題を解決してください。サポートエージェントが検証の失敗を解決すると、問題が解決されたことを示す通知がセキュリティ管理者と KMF 管理者に届きます。

Subject: IMPORTANT: Cloud Encryption Properties Reset

At your request, ServiceNow support has reset the following list of Cloud Encryption properties to their default values.
If you did not request this action, contact ServiceNow support immediately.

Reset properties:
com.glide.dare_key_mgmt.quorum.approvers(903a3212c3210110cf37169d7940dda8)

Ref:MSG0000116_0HAz8U1r59OmppqV8ysg

データベース暗号化

ServiceNow® は、すべてのデータが停止している時に保護が必要な可能性のあるデータ保護の法的義務を負う顧客向けに、データベース暗号化 (DBE) とフルディスク暗号化方法を提供します。

重要:
このリリース以降 Washington DC 、データベース暗号化は将来の廃止に備えて準備されます。Cloud Encryption は、保管データの暗号化に代わるソリューションです。詳細については、「キー管理を使用したクラウド暗号化」を参照してください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

探索

データベース暗号化の主な機能とビジネス価値について学びます。

要求

データベースキーのローテーションを要求する方法の詳細については、こちらを参照してください。

参照

データベース暗号化の詳細をご覧ください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

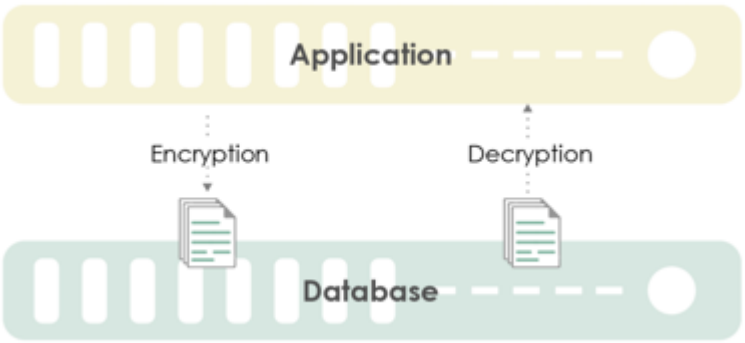
データベース暗号化の概要

ServiceNow® は、すべてのデータが停止している時に保護が必要な可能性のあるデータ保護の法的義務を負う顧客向けに、データベース暗号化 (DBE) とフルディスク暗号化方法を提供します。

重要:
このリリース以降 Washington DC 、データベース暗号化は将来の廃止に備えて準備されます。Cloud Encryption は、保管データの暗号化に代わるソリューションです。詳細については、「キー管理を使用したクラウド暗号化」を参照してください。

データベース暗号化を使用すると、データベースがオンラインかオフラインかに関わらず、すべてのデータを対称 AES-256 暗号化で保護できます。Now Platform の観点から、すべてのデータが復号化されます。

- データベース暗号化では、リアルタイムに保存データの暗号化をサポートし、機能を損なうことなくオンラインとオフラインのデータを保護します。
- フルディスク暗号化は、ディスクの紛失や盗難が発生した場合にオフラインデータを保護します。



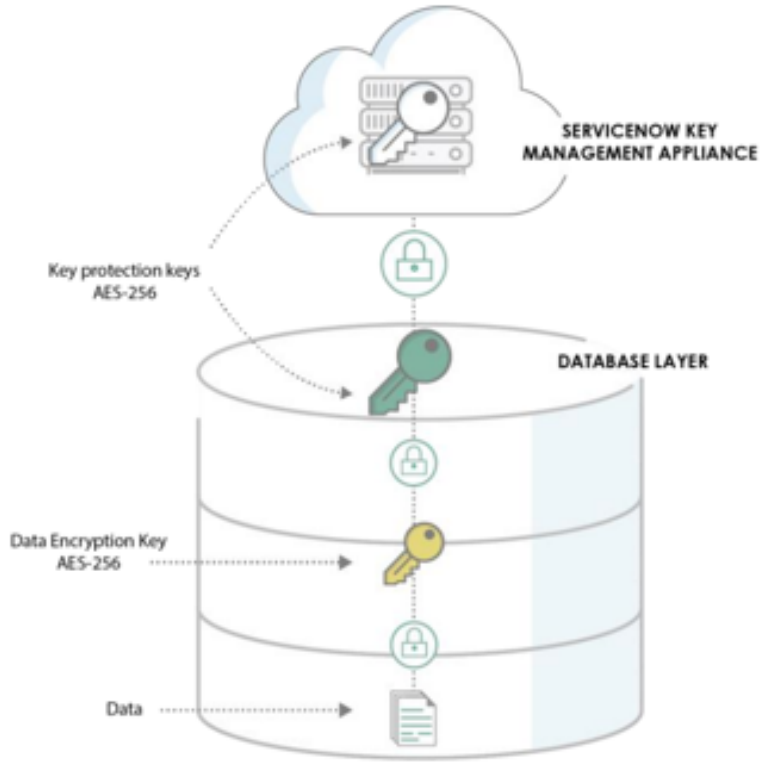
データベース暗号化を使用すると、保存されているすべてのデータが暗号化され、個々のレコードまたはテーブルがアクセス時に復号化されます。新規または変更されたデータは、テーブルに入力されるときに暗号化され、関連するアクティビティログファイル (bin、redo、undo、error) も暗号化されます。

データベース暗号化はユーザーに対して透過的であり、機能が失われることはありません。この機能を使用すると、すべてのインスタンスがレプリケーショントラフィックとバックアップとともに暗号化されます。インスタンスのクローンは引き続き使用できますが、データベース暗号化を使用した場合、パフォーマンスに最大 5% の軽微な影響があります。サポートされているリリースの Now Platform の新規インスタンスと既存のインスタンスの両方で、データベース暗号化を利用できます。

図に示すように、ServiceNow は次の 3 つのレベルのキー階層を使用してキーを格納し、管理します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



1. 顧客固有の AES-256 キーがデータベースエンジンで作成され、データの暗号化に使用されます。
2. 2 つ目の顧客固有の AES-256 キーがデータベースエンジンで作成され、第 1 レベルのキーの保護に使用されます。
3. 3 つ目の AES-256 キーが作成され、ServiceNow データセンターの FIPS 140 検証済みキー管理アプライアンス内に保存されます。このキーは第 2 レベルのキーを保護し、顧客インスタンスごとに一意です。

Now Platform は、顧客指定のスイッチである DBE-CCS を使用したデータベース暗号化もサポートしています。これは、データベースで使用されていないすべてのデータを暗号化する暗号化ソリューションです。機能に影響することなく、業界標準の AES 暗号化を使用します。データはディスクに書き込まれるときに暗号化され、ディスクから読み取られるときに復号化されます。したがって、アプリケーションは常にデータを暗号化されていない状態で保持し、影響を受けることなく必要なロジックと機能を実行することができます。

注:
データベース暗号化は、オンプレミスインスタンスではサポートされていません。

データベースの暗号化に独自のキーを使用する場合は、「カスタマー制御スイッチを使用したデータベースの暗号化」を参照してください。

データベースキーのローテーションの要求

年に 1 回または必要に応じて、サポートに要求を送信して、データベースキーをローテーションします。

始める前に

必要なロール：admin

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

重要:
このリリース以降 Washington DC 、データベース暗号化は将来の廃止に備えて準備されます。Cloud Encryption は、保管データの暗号化に代わるソリューションです。詳細については、「キー管理を使用したクラウド暗号化」を参照してください。

このタスクについて
キーローテーションは、有効期限前 24 時間以内の夜間に行われ、インスタンスのサービスは中断されません。

注:
現在、キーローテーションは ServiceNow Commercial、Government Community Cloud (GCC)、France、および Singapore の環境でのみ利用できます。

手順

カスタマーサービス & サポートに連絡して、次のキーローテーションアクションを要求してください。

- 登録すると、指定したすべてのインスタンスで年に 1 回キーローテーションが実行されます。
- 次の情報を含む、過去 3 回のキーローテーションの履歴レポートを取得できます。
  - インスタンス名
  - キー名とバージョン
  - ローテーションの日付と時刻
- 年に 1 回スケジュールされているローテーション以外に、早期のキーローテーションをスケジュールします。

カスタマー制御スイッチを使用したデータベースの暗号化

カスタマー制御スイッチを使用したデータベースの暗号化 (DBE-CCS) は、データベースで使用されていないすべてのデータを暗号化する暗号化ソリューションです。

重要:
このリリース以降 Washington DC 、データベース暗号化は将来の廃止に備えて準備されます。Cloud Encryption は、保管データの暗号化に代わるソリューションです。詳細については、「キー管理を使用したクラウド暗号化」を参照してください。

概要

カスタマー制御スイッチを使用したデータベースの暗号化では、機能に影響を与えることなく、業界標準の AES 暗号化を使用します。データはディスクに書き込まれるときに暗号化され、ディスクから読み取られるときに復号化されます。アプリケーションは常にデータを暗号化されていない状態で保持し、必要なロジックと機能を実行することができます。

DBE-CCS は、テーブルスペース暗号化または透過的データ暗号化と呼ばれるデータベース固有の技術を使用します。この技術の詳細については、MariaDB Web サイト の「テーブルスペース暗号化」を参照してください。

DBE-CCS では、ServiceNow インスタンスに定期的に秘密キーを提供する HTTPS REST サービスエンドポイントを設定する必要があります。CCS エンドポイントは、データベースインスタンスの公開鍵で暗号化された秘密キーを顧客に返します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

顧客エンドポイント

> **重要:**
> 組織は、CCS エンドポイントの設定と管理に対して単独で責任を負います。顧客エンドポイントの仕様は KB0789788 に記載されています。

ServiceNowテクノロジーパートナーであるFortanixが、顧客エンドポイントの実装に利用できます。統合の詳細については、テクノロジーパートナーに直接お問い合わせください。詳細については、「 ServiceNow での Fortanix データセキュリティマネージャーの使用 」を参照してください。

複数 **ServiceNow** バージョンのサポート

> **重要:**
> データベースの暗号化は、リリースに依存しない有料のインフラストラクチャ製品です。サポートされているリリースと新しいまたは既存のインスタンスに適用することができます。

その他の参考資料

DBE-CCS の詳細については、次の参考資料を参照してください。

参考資料	説明
KB0993681	データベース暗号化のカスタマー制御スイッチの構造
KB0789788	DBE-CCS の実装ガイド

> **注:**
> KB 記事にアクセスするには、まず Now Support への認証を行う必要があります。

フルディスク暗号化

データベースサーバーは顧客データを格納する唯一のコンポーネントであるため、フルディスク暗号化 (FDE) は、データベースサーバー内のストレージシステム全体にのみ適用されます。FDE は、ストレージデバイスの物理的な紛失または盗難からのみ保護します。暗号化されたディスクサーバーの電源がオンで、データが提供されている場合、暗号化で追加の保護は提供されません。

フルディスク暗号化

フルディスク暗号化が、厳しい規制のある組織と関係がある場合があり、顧客の ServiceNow 展開に多大なコストがかかる可能性があります。ストレージデバイスの紛失や盗難を軽減するために ServiceNow によって実施されている対策も、選択の要因になる場合があります。

Now Platform の観点から、すべてのデータが復号化されます。

商用環境では、FIPS 140 検証済みハードウェアまたは検証中のストレージデバイスと、追加料金が必要な ServiceNow 専用ハードウェアオプションを使用できます。FDE はハードウェア自体に適用されるため、割り当てられたすべてのインスタンスに格納されているすべてのデータが暗号化されます。

FDE と専用ハードウェアオプションの選択の詳細については、ServiceNow の担当者にお問い合わせください。

Edge Encryption

ServiceNow® エッジ暗号化™ は、社内の機密データを暗号化 (送信中に暗号化) してから、インターネット経由で ServiceNow インスタンスに送信し、暗号化はそのまま維持されます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

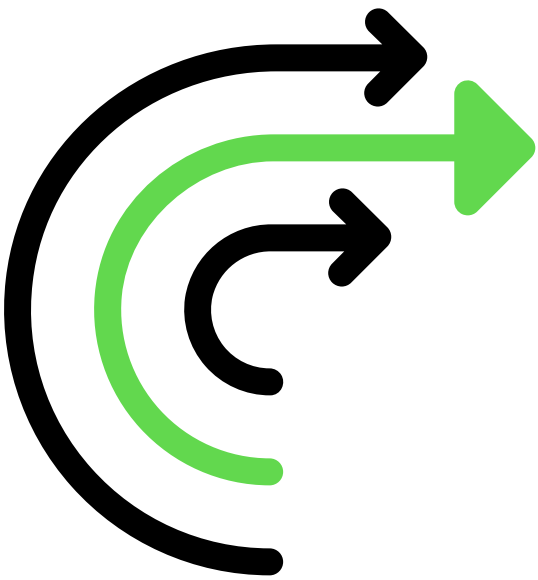
探索

Edge Encryption の機能とビジネス価値について学びます。

プラン

Edge Encryption の計画方法を理解します。

インストール



Edge Encryption をインストールします。

Edge Encryption のアップグレード

アップグレード

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

	Edge Encryption のアップグレード方法を理解します。
構成 	
Edge Encryption の設定方法を理解します。	

エッジ暗号化 の詳細

エッジ暗号化 は、ネットワークに常駐するネットワーク暗号化システムで、データセンターと ServiceNow クラウド間を移動する機密データを暗号化および復号化します。

エッジ暗号化 の概要

「クライアント側」暗号化とも呼ばれる Edge は、インフラストラクチャ上で維持されているプロキシを通過するために、すべての双方向ユーザートラフィックを必要とします。キーはインフラストラクチャ上のプロキシ内に保存されるため、キー管理を完全に制御できます。Now Platform は、暗号テキストを復号化してキーにアクセスすることはできません。

エッジ暗号化 機能は、データのエンドツーエンドの暗号化およびキー管理を制御する機能を提供する追加コストオプションです。エッジ暗号化 は、ServiceNow によって提供され、自身のネットワーク内にインストールされたプロキシアプリケーションを使用します。このプロキシアプリケーションは、指定されたデータパターンをトークン化するか、文字列フィールド、日付フィールド、日付/時刻フィールド、および添付ファイルデータを暗号化してから、環境からインスタンスに送信します。プロキシアプリケーションは、自分のネットワーク内のみに保存されているキーを使用して、同じデータを自分のネットワーク内でのみ復号化します。

関連する暗号化キーおよび構成は、ネットワーク内の Edge プロキシにのみ存在し、ServiceNow には表示されません。データは環境を離れた瞬間から暗号化され、取得時にのみ復号化されます。ServiceNow システムまたは担当者であってもプレーンテキストでデータにアクセスすることはできません。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

エッジ暗号化 のユーザー

ネットワークのプロキシサーバーを介してインスタンスにログインしたユーザーだけが、暗号化されたデータをクリアテキストで表示できます。同様に、ネットワークのプロキシサーバーを介してインスタンスにログインした security_admin ユーザーだけが、エッジ暗号化 を設定および管理できます。

プロキシサーバーはネットワークに常駐しているため、ユーザーが暗号化キーを所有し、管理します。暗号化キーがインスタンスに送信されることは決してありません。そのため、ServiceNow に機密データがクリアテキストで表示されることは決してありません。

ユーザーは Edge プロキシの設定およびルールの管理に加えて、Edge プロキシを有効にしてサポートするために、環境内でサーバーを運用するための通常の要件 (ホスティング、ルーティング、バックアップ、DNS 構成などを含む) を担当します。

暗号化とトークン化

エッジ暗号化 は、機密情報を保護する手段として暗号化 (暗号化設定を使用) とトークン化 (暗号化パターンを使用) の両方をサポートしています。

暗号化設定

暗号化設定を使用して個々のフィールドを暗号化することができます。エッジ暗号化 は、AES 128 ビットと AES 256 ビットの暗号化キーをサポートしています。エッジ暗号化 は、標準、等価性保存、および順序保存の暗号化タイプをサポートしています。

添付ファイルに加えて、以下のフィールドタイプを暗号化できます。

- 日付
- メール
- 日付/時刻
- HTML
- IP アドレス
- ジャーナル
- ジャーナル入力
- 複数行テキスト
- 1 行テキスト
- 文字列
- URL

注:

暗号化対象としてマークされたジャーナル フィールドがアクティビティ ストリームに追加された場合、フィールドへのすべてのユーザー入力がアクティビティ ストリームで暗号化されます。

サポートされているフィールド タイプ内のマルチバイト文字を暗号化できます。

次のサービスカタログ変数タイプを暗号化することもできます。

自動翻訳

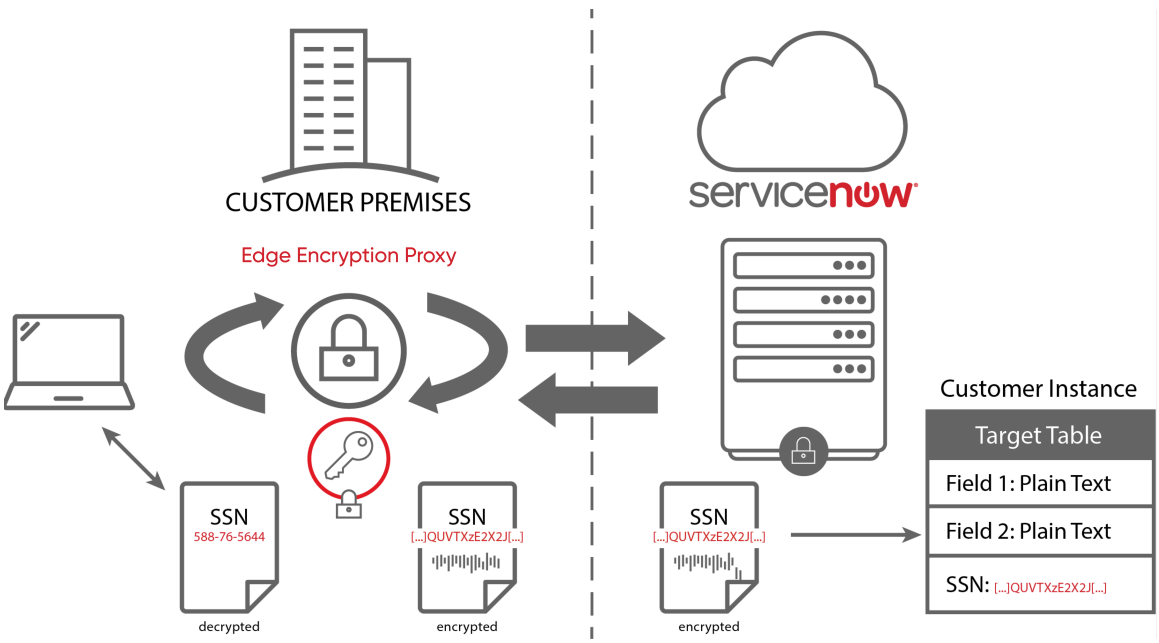
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- 文字列タイプ
- ○ 1 行テキスト
  - ○ 複数行テキスト
  - ○ 幅広 1 行テキスト
- 日付
- 日付/時刻
- URL
- メール
- HTML
- IP アドレス

暗号化パターン

暗号化パターンを使用して、社会保障番号やクレジット カード番号などの規則的なパターンに一致する文字列をトークン化することができます。暗号化の主要な手段としては暗号化設定をお勧めしますが、暗号化フィールド以外の場所にある機密情報を保護する場合は暗号化パターンを補足手段として使用してください。

注:
エッジ暗号化 プロキシサーバーでネットワークにある MySQL データベースが必要になるのは、順序保存の暗号化または暗号化パターンを使用している場合のみです。クリアー テキスト値は、ネットワークのプロキシ データベースに格納されます。このため、プロキシ データベースを保護し、定期的にバックアップすることが重要です。推奨事項については、「Edge Encryption のコンポーネント」を参照してください。



Now Platform 上の エッジ暗号化

エッジ暗号化 は、ブラウザと ServiceNow インスタンス間のゲートウェイとして機能します。ブラウザからのトラフィックは、途中のゲートウェイを経由して ServiceNow インスタンスに達します。さらにゲートウェイは、暗号化対象としてマークされた送信データを暗号化するように設定されます。受信トラフィックはゲートウェイ経由で復号化され、エンド ユーザーのブラウザにはクリアー

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

テキストが表示されます。セキュリティ制御の観点から見た場合、この実装には、暗号化とキー管理が ServiceNow の外部で処理されるという利点があります。

長所と短所

列レベル暗号化エンタープライズ および列レベルの暗号化と同様に、エッジ暗号化 は、追加のセキュリティの結果としてインスタンス内にいくつかの機能制限を課します。ただし、ローカル Edge プロキシは、列レベルの暗号化と比較した場合、ソートに関連するいくつかの追加機能も提供します。

長所：

- エッジ暗号化 は、情報の閲覧者を完全管理し、データ侵害を防止します。
- 情報はプロキシサーバーに残り、暗号化されないままネットワークから離れることはありません。
- 情報は ServiceNow インスタンスに到達する前に、転送中に暗号化されます。
- あなたが、すべての暗号化キーを保持して管理します。ServiceNow 担当者であっても、他者があなたの鍵にアクセスすることはできません。
- 暗号化アルゴリズムの強度は、AES-128 または AES-256 から選択できます。
- エッジ暗号化 には、文字列テキスト、日付フィールドと日付/時刻フィールド、添付ファイル、URL、およびジャーナルを暗号化する機能が含まれています。
- エッジ暗号化 では、データベースおよびインスタンス内に保存されているデータの標準、等価性保存、および順序保存の暗号化が可能です。
- 暗号化ルールを使用すると、暗号化する対象とその暗号化された情報をインスタンス内のどこに配置するかをプロキシサーバーに明確に指示するカスタムスクリプトを作成できます。これらのスクリプトは、データ構造が ServiceNow インスタンスと正確に一致しない場合に便利です。
- 暗号化パターンを使用すると、パスワードなどの情報をトークン化できます。

短所：

- エッジ暗号化 には、Edge プロキシクラスターを介した追加のネットワークホップと追加の処理が必要であり、トラフィックに遅延が生じる可能性があります。追加された エッジ暗号化 アプリケーションの処理遅延は、ネットワークホップに比べてごくわずかです。
- 独自の暗号化キーを管理するのは、複雑で時間がかかる場合があります。
- 最大 2 つのキーを維持できますが、列/データの異なるサブセットや異なるロールなどに対して異なるキーを柔軟に定義することはできません。
- エッジ暗号化 には、サーバーまたはプラットフォームがデータを復号化して、復号化されたデータを操作できないという副作用があります。その結果、Edge Encryption で列を暗号化するときに、Now Platform の機能とデータ処理が制限される可能性があります。

使用前の注意事項

暗号化とトークン化はデータの性質を変える処理であるため、エッジ暗号化 は他のインスタンス プロセスに影響を与える可能性があります。エッジ暗号化 の使用にあたっては、インスタンスに及ぼす影響を慎重に考慮してください。

プロキシサーバーはネットワークにインストールされて維持されるため、エッジ暗号化 ではネットワークの管理が必要になります。円滑な実装ができるように、ネットワーク要件を確認してください。

次のトピックを確認し、インスタンスにおける Edge Encryption の影響を理解してください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- Edge Encryption の計画立案
- エッジ暗号化 のシステム要件
- Edge Encryption 環境のサイジング
- 順序保存とトークン化のデータベースのサイズを計算する
- エッジ暗号化 の制限事項
- Edge Encryption のキー管理

Edge Encryption のコンポーネント

エッジ暗号化 は、 ネットワーク内のサーバー上で実行される エッジ暗号化 プロキシサーバーと、エッジ暗号化 プラグインで構成されます。プラグインは ServiceNow インスタンスにインストールする必要があります。順序保存の暗号化タイプまたは暗号化パターンを使用する場合は、プロキシ データベースもネットワークにインストールする必要があります。

プロキシアプリケーション

エッジ暗号化 プロキシサーバーを通過する際、 エッジ暗号化 プラグインを使用して、どのフィールド、パターン、および添付ファイルを暗号化するかを指定できます。また、暗号化ルールを管理して、特定の要求を暗号化したり、一括暗号化ジョブをスケジュールしたりすることもできます。

プロキシサーバー

エッジ暗号化 プロキシサーバーは暗号化ルールを使用して、HTTP 要求の中で何らかのデータがある場合にどれを暗号化する必要があるかを識別し、そのデータを暗号化してから要求をインスタンスに転送します。復号化では、 エッジ暗号化 プロキシサーバーは、暗号化されたデータが HTTP 応答にないかを調べ、そのデータを復号化してから応答をクライアントに送り返します。この処理を行うためには、すべての HTTP 要求および応答が エッジ暗号化 プロキシサーバーを通過する必要があります。これらの HTTP 要求には、ブラウザから発生した要求や、SOAP 要求、REST 要求などがこれに含まれます。

プロキシデータベース

順序保存の暗号化または暗号化パターンを使用している場合、プロキシサーバーはネットワークにある MySQL データベースを利用します。ネットワーク内のすべてのプロキシサーバーで、同じデータベースを使用する必要があります。

プロキシ データベースには下記のテーブルが含まれています。

プロキシ データベースのテーブル

名前	説明
db_id	一意のデータベース ID
edge_token_map	暗号化パターン データ
token_map	順序保存の暗号化データ

プロキシ データベースのバックアップ

暗号化パターンではトークン化が利用されるため、クリアテキスト値はプロキシデータベースに格納されます。データベースが失われた場合、クリアテキスト値は復元できません。そのため定期的なバックアップが重要になります。データの消失を防ぐため、ServiceNow の推奨事項に従ってプロキシデータベースをバックアップしてください。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- データベースを 24 時間ごとにバックアップします。
- MySQL データベースのバイナリログファイルを少なくとも 2 日間保持します。バックアップの復元が完了したら、バイナリログを使用して、最新のバックアップ以降に失われたデータを再生成します。

エッジ暗号化 クライアント

エッジ暗号化 では 3 つのクライアントを使用して、プロキシがインスタンスを実行中であることをインスタンスに通知したり、プロキシとインスタンスの間の要求を同期したり、潜在的な暗号化後にインスタンスに対するすべてのユーザー要求を転送したりします。

クライアント	説明
ハートビート/キープアライブクライアント	このプロキシが稼働していることをインスタンスに通知できるよう、5 秒間隔で ServiceNow インスタンスに要求を送信することを担当します。要求は、Edge プロキシテーブルの last_response_on フィールドを駆動し、その結果、プロキシの状態を駆動します。システムに要求の送信に関する問題がある場合、または要求や要求処理が遅延する場合、その他のクライアント (ユーザートラフィックに対するものを含む) が稼働している場合でも、インスタンスはプロキシを応答なしとしてマークすることがあります。 このクライアントは、インスタンス上のプロキシのオンラインステータスを制御します。 *`edgeencryption.proxy.keepalive.interval`* プロパティは、このクライアントのポーリングレートを制御します。デフォルトは 5 (秒) です。
ポーリング/同期クライアント	Edge Encryption 設定 (たとえば、暗号化するテーブル、列、添付ファイルや、キー、ジョブ、ルール、トークン化パターン) に従って同期するよう、プロキシがインスタンスに送信するさまざまな要求を担当します。 *`edgeencryption.config.poll.interval`* プロパティは、このクライアントのポーリングレートを制御します。 **⚠ 警告:** この設定を変更しないでください。プロキシのポーリング間隔のデフォルト設定を変更すると、インスタンスの Edge Encryption 設定を更新するときに同期が遅延する可能性があります。
デフォルト/ユーザートラフィッククライアント	その他すべてについて、このクライアントはすべてのエンドユーザー要求を処理し、暗号化がある場合はそれを施した後、ServiceNow インスタンスに転送します。このクライアントは、インスタンスからの応答も処理し、復号化があ

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

クライアント	説明
	る場合はそれを施した後、エンドユーザーに転送します。

Edge Encryption のキー管理

エッジ暗号化 で使用する暗号化キーについては、お客様の責任でその提供と管理を行っていただく必要があります。

このトピックでは、エッジ暗号化 製品のキーについて説明します。Column Level Encryption で使用できるキー管理フレームワークに関する情報をお探しの場合は、「キー管理フレームワーク」を参照してください。

エッジ暗号化 で使用する暗号化タイプをサポートする目的で暗号化キーを取得および作成する際は、次の点を考慮してください。

- AES 128 ビットまたは AES 256 ビットのどちらを使用するか。デフォルトの AES 128 ビット暗号化キーは、使用しない場合でも定義する必要があります。
- ファイルシステム、Java KeyStore、または Enterprise Key Management (EKM) のどれを使用するか。
- 暗号化キーをいつローテートするか。
- どのような場合に一括暗号化ジョブを使用して新しいキーでデータを再暗号化するか。

プロキシ設定ファイルやキーストアからキーを削除する場合は、そのキーを使用しているインスタンス上のすべてのデータを事前に復号化しておくことが重要です。それには、新しい暗号化キーを追加して、一括キー ローテーション ジョブをスケジュールします。

キーストア

エッジ暗号化 は、次のタイプのキー ストレージをサポートしています。

ファイルストア

キーは、エッジ暗号化 プロキシからアクセス可能なファイル システム内のファイルに格納されます。ファイルに保存された暗号化キーは暗号化されていないため、これらのファイルの保護についてはユーザーの責任になります。

Java KeyStore

キーは、Java の JCEKS KeyStore に格納されます。Java KeyStore はパスワードで保護されているため、ファイルストア内のファイルにキーを格納する方法よりも安全です。1 つの Java KeyStore に複数のキーを格納することができます。キーはキー別名により識別されるため、複数のキーを簡単に管理できます。

Enterprise Key Management (EKM)

キーは、SafeNet KeySecure または Unbound Technology のキー管理システムを使用して格納および取得されます。

エッジ暗号化 プロキシの keystore ディレクトリーには、keystore.jceks という名前の Java JCEKS KeyStore ファイルが付属しています。このキーストア ファイルには ServiceNow 公開キーが含まれています。この公開キーは、ServiceNow の署名が付いた暗号化ルールの検証に使用されます。

注:
ベース システムの Java JCEKS KeyStore 以外のキーストアを使用する場合は、ServiceNow 公開キーをキーストアにインポートする必要があります。公開キーの別名は *servicenow* です。

暗号化キーだけでなく、Java JCEKS KeyStore は RSA キー ペアやデジタル証明書の格納にも使用します。RSA キー ペアは、インスタンスに格納される暗号化設定と暗号化ルールにデジタル署名

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

する場合に使用します。デジタル証明書は、エッジ暗号化 プロキシがブラウザーや他のクライアントとのセキュア接続を確立するために使用します。

Edge Encryption の SafeNet キーのバージョニング

SafeNet キーバージョニングを使用してキーの変更を簡素化します。SafeNet キーバージョニングでは、キーごとに新しいエイリアスを作成するのではなく、同じエイリアスを維持してバージョンを増やします。

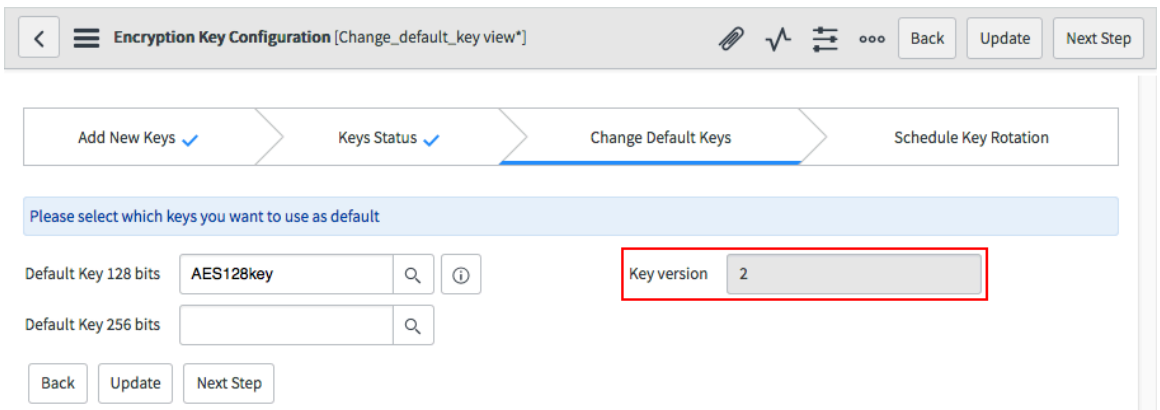
Edge プロキシサーバーで SafeNet キー バージョニングを設定する場合は、SafeNet でキー バージョニングをセットアップする必要があります。

注:
London リリースより前にインストールされた Edge プロキシは、SafeNet キーをサポートしていますが、SafeNet キーバージョニングはサポートしていません。Kingston 以前のプロキシで誤ってバージョニングされたキーを使用した場合、London リリース以降へのアップグレード時に London 以降のプロキシによってこの問題が検出され、データ消失の可能性を防ぐためにプロキシが起動しません。

最初に、一括キー ローテーション ジョブまたは単一のキー ローテーション ジョブをスケジューリングして、古い SafeNet でバージョニングされたキーをバージョニングされていないキーに置き換え、必要に応じて新しい SafeNet でバージョニングされたキーを作成する必要があります。新しくバージョニングされたこのキーは London 以降のプロキシで安全に使用でき、プロキシを再起動することができます。

暗号化キーの設定

SafeNet でバージョニングされたキーを使用する場合、[暗号化キーの設定] フォームの [デフォルトキーの変更] セクションには、デフォルトの 128 ビットおよび 256 ビット キーの [キーバージョン] に対応した新しいフィールドが含まれます。[キーバージョン]フィールドはグレー表示され、編集することはできません。



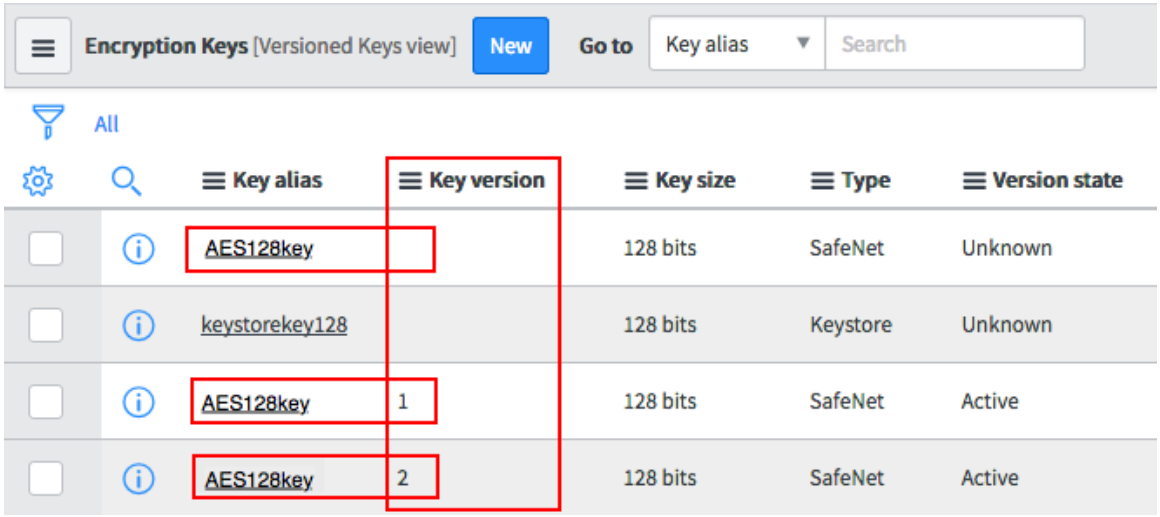
手順については、「インスタンスで暗号化キーを設定する」を参照してください。

バージョニングされたキー

SafeNet でバージョニングされたキーを使用している場合は、 エッジ暗号化の設定 > 暗号化キーの設定 > すべてのキー、バージョニングされたキーには キーバージョンが含まれます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



[暗号化キーの設定] フォームの [デフォルトキーの変更] セクションで入力した最初のエントリについては、バージョン番号は表示されません。プロキシサーバーが SafeNet からキーを要求すると、別名用の新しい行が追加され、[キーバージョン] が追加されます。

上記の例では、**[AES128key]** が 3 回表示されています。

- 1 つ目の表示は最初のエントリで、[キーバージョン] が示されていません。
- 2 つ目の表示は、SafeNet から返されたキーの最初のバージョンで、[キーバージョン] 列に **1** と表示されています。
- 3 つ目の表示は、SafeNet から返されたキーの 2 つ目のバージョンで、[キーバージョン] 列に **2** と表示されています。
- 他のバージョンのキーが SafeNet から返されるたびに、現在使用中の [キーバージョン] を記録するための新しい行が追加されます。

暗号化の設定とパターン

エッジ暗号化 では、フィールドを暗号化して文字列をトークン化することができます。

暗号化設定

暗号化設定を使用して個々のフィールドを暗号化することができます。エッジ暗号化 は、AES 128 ビットの暗号化キーをサポートしています。Java Cryptography Extension (JCE) の Unlimited Strength Jurisdiction Policy (無制限強度管轄ポリシー) ファイルがインストールされている場合、エッジ暗号化 は各暗号化タイプについて AES 256 ビットの暗号化キーをサポートします。エッジ暗号化 は次のタイプの暗号化設定をサポートしています。

標準暗号化

フィールドの暗号化の値は、フィールド値が同じままになる場合でも、フィールドが暗号化されるたびに異なる値になります。標準暗号化は、最も堅牢な暗号化形式です。標準暗号化を使用しているフィールドを、ソート、グループ化、またはフィルターすることはできません。

等価性保存暗号化

フィールドの暗号化の値は、フィールド値が同じままになる場合は同じです。フィールドの等価比較とグループ化操作をサポートします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

> **注:**
> すでにデータが格納されているフィールドに対して等価性保存暗号化を選択した場合は、フィールドでグループ化アクションを実行しても、暗号化フィールドと非暗号化フィールドが混在していると、同じ値を持つフィールドがグループ化されないことがあります。

順序保存暗号化

トークンと暗号化を使用して、プロキシ データベースのデータを保護します。等価比較、グループ化操作、およびデータのソート機能をサポートします。順序保存暗号化タイプは、MySQL データベースが エッジ暗号化 プロキシサーバー用に設定されている場合にのみサポートされます。

> **注:**
> 順序保存暗号化を使用している場合、プロキシ データベースがダウンしたときに、順序保存暗号化を使用してフィールドに更新を加えることができます。ただし、これらのフィールドに基づいてデータをソートしようとすると、ソート順が正しくなりません。また、グループも想定どおりに機能しません。プロキシ データベースが再び稼動したら、順序トークンの修復ジョブをスケジュールして、欠落しているトークンを修復してください。

暗号化タイプ

次の暗号化タイプは、セキュリティの質が低下する順序で記載されています。

暗号化タイプ	説明
標準 AES 256	フィールドをフィルター、ソート、または比較することはできません。
標準 AES 128	フィールドをフィルター、ソート、または比較することはできません。
等価性保存 AES 256	等価比較を使用してフィールドをフィルターすることができます。
等価性保存 AES 128	等価比較を使用してフィールドをフィルターすることができます。
順序保存 AES 256	フィールドをソートでき、等価比較によるフィルターを使用できます。ネットワークで MySQL データベースを使用する必要があります。
順序保存 AES 128	フィールドをソートでき、等価比較によるフィルターを使用できます。ネットワークで MySQL データベースを使用する必要があります。

暗号化パターン

暗号化パターンを使用して文字列内の機密データを保護することができます。暗号化パターンが保存されて有効化されると、エッジ暗号化 プロキシサーバーによって、要求のパターンと一致する文字列が識別されます。見つかったクリアー テキスト文字列はプロキシ データベースに格納され、インスタンス上でトークンに置き換えられます。暗号化パターンを使用して、社会保障番号やクレジットカード番号などの規則的なパターンに一致する文字列をトークン化することができます。暗号化の主要な手段としては暗号化設定をお勧めしますが、暗号化フィールド以外の場所にある機密情報を検索して保護する場合は暗号化パターンを補足手段として使用してください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注:
エッジ暗号化 プロキシサーバーでネットワークにある MySQL データベースが必要になるのは、順序保存の暗号化または暗号化パターンを使用している場合のみです。クリアー テキスト値は、ネットワークのプロキシ データベースに格納されます。このため、プロキシ データベースを保護し、定期的にバックアップすることが重要です。推奨事項については、「Edge Encryption のコンポーネント」を参照してください。

関連情報

暗号化設定を使用したフィールドの暗号化

暗号化パターンを使用して文字列をトークン化する

Edge Encryption と一緒にインストールされるもの

エッジ暗号化 では、暗号化関連のデータを格納するためのテーブル、デフォルトの動作を設定するためのシステムプロパティ、および、エッジ暗号化 を管理するための edge_encryption ロールがインストールされます。

エッジ暗号化 とともにインストールされるテーブル

エッジ暗号化 は、次のテーブルを追加します。

Edge Encryption の設定 [sys_encryption_configuration]
: 添付ファイルが暗号化される際の対象となる暗号化フィールドおよびテーブルが含まれています。

Edge Encryption のルール [sys_encryption_rule]
: 各ルールのレコードが含まれています。ルールは、名前、使用時の条件、スクリプト、および順序フィールドを持っています。

Edge Encryption の無効な挿入ログ [sys_edge_encryption_invalid_insert_log]
: 暗号化されていないデータを暗号化フィールドに保存しようとしたときに作成されるログ メッセージが含まれています。

Edge Encryption のプロキシ [sys_encryption_proxy]
: 暗号化プロキシ アプリケーションに関する情報が含まれています。

Edge Proxy の暗号化タイプ [sys_proxy_encryption_type]
: 暗号化フォームでの暗号化タイプの有効化と無効化に使用されます。

暗号化ジョブの実行 [sys_encryption_job_execution]
: 一括暗号化ジョブをサポートします。

暗号化ジョブ実行チャンク [sys_encryption_job_execution_chunk]
: 一括暗号化ジョブをサポートします。

スケジュールされた暗号化ジョブ [sysauto_encryption_job]
: 暗号化、復号化、キー ローテーション、順序トークンの修復、およびデータベースの回復のための、ジョブスケジュールを列挙します。

暗号化キーの設定 [sys_encryption_key_configuration]
: デフォルト暗号化キーを列挙します。

暗号化キー [sys_encryption_key]
: 利用可能なキーとキー属性を列挙します。

プロキシ暗号化キー [sys_encryption_proxy_key]
: プロキシ暗号化キーを列挙します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

エッジ暗号化でインストールされるプロパティ

エッジ暗号化 は、次のプロパティを追加します。

注:
システムのプロパティ [sys_properties] テーブルを開くには、ナビゲーションフィルターに「sys_properties.list」と入力します。

glide.edge.pattern.disallowed.chars

パターンで許可されていない文字のリスト。

- タイプ：値をカンマで区切ったリストの文字列
- 場所：システムプロパティ [sys_properties] テーブル

glide.edge.pattern.min.size

許容される最小パターン サイズ。パターンを小さくするほど一致が増えるため、オーバーヘッドが増加します。

- タイプ：数値
- デフォルト値：5
- 場所：システムプロパティ [sys_properties] テーブル

sn_edge_encryption.logging.destination

メッセージが記録される場所。

- タイプ：文字列
- デフォルト値：ファイル
- 場所：システムプロパティ [sys_properties] テーブル

sn_edge_encryption.logging.verbosity

使用するログ レベル。

- タイプ：文字列
- デフォルト値: info
- 場所：システムプロパティ [sys_properties] テーブル

sn_edge_encryption.encryption.proxy.buildtag

インスタンスに登録されるプロキシ バージョン。

- タイプ：文字列
- 場所：システムプロパティ [sys_properties] テーブル

sn_edge_encryption.cleartext.allowed

true の場合、クリアー テキストは暗号化フィールドに保存できます。これは、ユーザーが エッジ暗号化 プロキシを通過せずにインスタンスにアクセスしようとした場合に発生します。false の場合、クリアー テキストは暗号化フィールドに保存できなくなります。

- タイプ：ブーリアン
- デフォルト値：false
- 場所：システムプロパティ [sys_properties] テーブル

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Edge Encryption の計画立案

エッジ暗号化 の実装を成功させるためには計画と準備が必要です。

計画段階では次の質問に答えてください。

- 暗号化するフィールドはどれか。
- どの暗号化タイプを使用するか。
- エッジ暗号化 プロキシはいくつ必要か。推奨事項や考慮事項については、「Edge Encryption 環境のサイジング」を参照してください。
- 順序保存の暗号化タイプまたは暗号化パターンを使用する場合、MySQL データベースをどこに配置するか。
- どのキー管理システムを使用するか。

エッジ暗号化 を実装するために必要なタスクは、システム管理者、ネットワーク管理者、およびセキュリティ チームのメンバーで異なります。

- システム管理者には security-admin ロールが必要です。システム管理者は次のことを行う必要があります。
  - エッジ暗号化 プロキシアプリケーションをダウンロードします。
  - プロキシがインスタンスへの接続に使用する エッジ暗号化 ユーザー アカウントをセットアップします。ユーザーに edge_encryption ロールをアサインする必要があります。
  - 暗号化キーの設定を行い、デフォルトキーを設定します。
  - インスタンス上で エッジ暗号化 の設定を行います。
  - 暗号化ジョブをスケジュールします 。
  - エッジ暗号化 を監視します。
  - 暗号化ルールを作成および編集します。
- ネットワーク管理者は次のことを行う必要があります。
  - エッジ暗号化 プロキシアプリケーションをインストールします。
  - 順序保存の暗号化および暗号化パターンに使用されるプロキシサーバーおよびプロキシ データベースのネットワーク アドレスを把握します。
  - 順序保存の暗号化および暗号化パターンに使用するプロキシ データベースをインストールします。
  - プロキシ アプリケーションを開始および停止します。
  - 暗号化キー管理を実行します。
  - ユーザーを暗号化プロキシ アプリケーションにマッピングする方法を決定します。これは DNS 設定またはルーティング ルールを使用して行うことができ、ネットワークごとに固有になります。
  - 複数のプロキシサーバーを管理します。
  - ロードバランサーのプールなどの設定を行います。
- セキュリティ管理者は、各フィールドにアサインする暗号化タイプを決定する必要があります。

エッジ暗号化 のシステム要件

エッジ暗号化 プロキシアプリケーションは、Microsoft Windows または Linux オペレーティング システムを実行しているサーバーまたは仮想マシンで実行できます。パフォーマンスを最適化するため、設定がこれらの要件を満たすことを確認します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

Java の要件

エッジ暗号化 プロキシサーバーをインストールまたは実行するホストマシンでは、サポートされているバージョンの Java を保持する必要があります。現在サポートされているバージョンは 11.x バージョンシリーズの Java 11.0.6 以降です。

注:
Java 8 は Utah リリースからサポートされなくなりました。Utah バージョンの エッジ暗号化 プロキシをインストールする前に、エッジ暗号化 プロキシを使用する環境を Java 11 にアップグレードしてください。

注:
Java は無制限の強度キーを自動的に許可しません。AES 256 ビット暗号化の使用を特別に有効にする必要があります。

OpenJDK のサポート

Now Platform は OpenJDK バージョン 11 をサポートしています。

プロキシサーバーの最小構成

プロキシサーバーには以下の最小構成が必要です。

- プロキシサーバーあたり 4 GB の RAM (ほとんどの展開で 6 GB を推奨)

  注:
  プロキシサーバーホストには、プロキシサーバーより少なくとも 1 GB 多い RAM が必要です。プロキシサーバーホストには、オペレーティングシステムサービス用に追加で 1 GB が必要です。たとえば、プロキシサーバーが RAM を 4 GB 使用するよう設定する場合は、プロキシサーバーホストに少なくとも 5 GB の RAM を取り付ける必要があります。

  プロキシサーバーには少なくとも 4 GBのメモリが必要なため、32 ビット JRE と 32 ビット オペレーティング システムは London リリース以後はサポートされなくなりました。

- 3 GHz 以上の CPU (最適なパフォーマンスには 4 コア CPU を推奨)
- ロードバランサーの背後で稼働する複数のプロキシサーバー。必要なプロキシサーバーの数は、アプリケーションノードの数、同時ユーザー数、およびフェイルオーバーに必要なサーバー数によって異なります。詳細については、「Edge Encryption 環境のサイジング」を参照してください。
- サーバーの使用率やリソースの可用性に応じて他のサービスと同時に実行できる機能

プロキシサーバーをサポートするシステム

次のシステムがサポートされています。

サポートされているシステム	説明
Windows Server 2012、2012-R2、2016、2019 の各エディション	• 仮想マシンまたは物理ハードウェア • 64 ビット システム
Linux	• 仮想マシンまたは物理ハードウェア • 64 ビット システム

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

サポートされているシステム	説明
	64ビットの Linux システムでは、32 ビットの GNU C ライブラリ (glibc) をインストールする必要があります。CentOS のインストールコマンドは yum install glibc.i686 です。

プロキシサーバーのバージョン要件

エッジ暗号化 プロキシバージョンを ServiceNow インスタンスバージョンと同期させてください (たとえば Tokyo などの同じメジャーリリース)。アップグレードプロセス中のダウンタイムをなくすために、 エッジ暗号化 プロキシには下位互換性があります。ただし、ユーザーが新しい機能や重要なバグ修正にアクセスできるようにするために、できるだけ早くアップグレードすることが重要です。

プロキシサーバーの接続要件

エッジ暗号化 アプリケーションを実行するプロキシサーバーは、ネットワーク内のマシンと通信できる必要があります。プロキシサーバーに次のネットワーク権限があることを確認してください。

ネットワーク権限	説明
ファイアウォールアクセス	プロキシサーバーとクライアントデバイスの間にあるファイアウォールの設定を行い、接続を許可します。ネットワークで非武装地帯 (DMZ) を使用してセキュリティの追加層をローカルエリアネットワーク (LAN) に追加していて、ネットワークセキュリティプロトコルによりネットワーク内部から DMZ へのポートアクセスを制限している場合は、プロキシサーバーを DMZ 内のマシンに展開する必要があります。
ネットワークアクセス	プロキシサーバーからの接続が可能になるように各クライアントを設定します。ネットワークセキュリティにより、クライアントに接続できる新しいマシンの設定ができない場合は、接続権限を持つ既存のマシンにプロキシサーバーをインストールします。
インスタンスアクセス	プロキシサーバーがインスタンスにネットワークアクセスできることを確認します。プロキシサーバーネットワークが、TCP ポート 443 経由のトラフィックを許可するように設定されていることを確認します。
ネットワークアカウント	ローカル管理者かドメイン管理者のいずれかを使用して、プロキシサーバーをインストールします。

順序保存およびトークン化データベースのシステム要件

順序保存の暗号化および暗号化パターンでは、エッジ暗号化 プロキシサーバー用に Oracle MySQL データベースを設定する必要があります。順序保存暗号化は、先にデータを復号化しなくても、比較演算を暗号化データに直接適用できます。暗号化パターンを使用すると、データベースに送信して格納する前に、文字列パターンをトークンで置換 (トークン化と呼ばれる) できます。MySQL データベースのサイズが理由で、順序保存およびトークン化データベースを実行するには専用のプロキシサーバーを使用します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

データベースシステムの最低要件には次のものが含まれます。

MySQL データベース	要件
バージョン	MySQL データベースバージョン 5.7 と 8.0 **注:** MySQL バージョン 5.5 および 5.6 はテストされなくなり、サポートが終了しました。
OS	64 ビット システム
CPU	2 GHz 以上の CPU (最適なパフォーマンスには 4 コア CPU を推奨)
RAM	16 GB
ディスク	ストレージエリアネットワーク (SAN) またはローカルストレージ (RAID 10 を推奨)
サイズ	潜在的なレコードの数にレコードサイズを掛けて決定します。「順序保存とトークン化のデータベースのサイズを計算する」を参照してください。
設定	高可用性クラスター。MySQL サーバーの設定方法が分からない場合は、設定情報について MySQL を参照してください。

Edge Encryption 環境のサイジング

環境に合わせてプロキシサーバーの台数を選択することは重要なタスクです。ユーザー数、冗長性の必要性、許容可能なレイテンシーを考慮してください。

冗長性

ハードウェア障害に備えて冗長のプロキシサーバーを維持してください。プロキシサーバーが到達不能になった場合でもすべてのユーザーに機能パスを提供できるように、プロキシサーバーをロードバランサーの背後に配置してください。少なくとも 2 台のプロキシサーバーが常に使用可能となるようにしてください。

サイズ

ここでのサイズとは、データの暗号化によって生じるレイテンシーの増大を避けるために必要なプロキシサーバーの台数のことです。使用状況によっては、プロキシサーバーを追加してレイテンシーを減らすことができます。たとえば、定期的な一括暗号化を実行する場合は、負荷を処理するためにプロキシサーバーを追加するか、ユーザー負荷が軽い状態のときに一括暗号化を実行します。また、プロキシサーバーを実行するハードウェアはパフォーマンスやレイテンシーに影響を与えます。CPU が高速で数が多く、RAM の容量が多いハードウェアでプロキシサーバーを実行する方が、低速で性能が限られたシステムと比べて、よい高いスループットが得られます。

下記のガイドラインでは、プロキシサーバーが最低限のハードウェア要件で実行されていることを前提としています。プロキシサーバーの台数を決定するには次のことを行ってください。

- インスタンス上の 2 つのアプリケーション ノードごとに 1 台ずつプロキシサーバーをセットアップすることを検討します。
- 冗長性を確保するため、ロードバランサーの背後に少なくとも 2 台のプロキシサーバーをセットアップします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- 500 人の同時ユーザーごとに追加のプロキシサーバーを用意します。
- 必要な冗長性に応じて、フェイルオーバー用のプロキシサーバーを追加します。

たとえば、2,000 人のユーザーが存在するインスタンスの場合は、ロードバランサーの背後に少なくとも 5 台のプロキシサーバーを用意します。この計算には、500 人のユーザーごとに 1 台ずつのプロキシサーバーと、フェイルオーバー用の追加のプロキシサーバーが含まれています。ユーザー数がいつしきい値の 500 人に近づくかを事前に判断して、ロードバランサー プールにもう 1 台のプロキシサーバーを配置してください。

ロードバランサー

要求のバランスを保ち、サーバーの応答時間を向上させるために、プロキシサーバーをロードバランサー プールに分散させてください。「最小数の接続」による方法を使用するようにロードバランサーを設定します。この方法では、有効な接続が最も少ないプロキシサーバーに要求が接続され、1 台のプロキシの過負荷が防止されます。

CPU 使用率

データの暗号化とトークン化は CPU に高い負荷がかかる処理です。そのため、データの暗号化中に CPU のスパイクが生じるのは正常であり、予期されることです。CPU 使用率が数分間で一度に 80% を超えると、プロキシサーバーが過負荷状態になる可能性があります。こうした状態が生じると、CPU 使用率が高い間、レイテンシーが増加します。レイテンシーが持続する場合は、もう 1 台のプロキシサーバーを追加することでレイテンシーの減少が促される可能性があります。

メモリ

プロキシサーバーには最低 4 GB の RAM が必要です (6 GB を推奨)。プロキシサーバーの初期メモリ制限と上限メモリ制限を推奨値に設定してください。

順序保存とトークン化のデータベースのサイズを計算する

順序保存の暗号化または暗号化パターンを使用する場合は、潜在的なレコードの数にレコード サイズを掛けて MySQL データベースのサイズを決定します。

始める前に

必要なロール：管理者

このタスクについて

順序保存およびトークン化データベースの実行には専用のマシンを使用してください。プロキシサーバーと同じハードウェア上でデータベースを実行しないでください。

手順

1. 順序保存の暗号化による暗号化フィールドを含む可能性があるレコードについて、その潜在的な数を決定します。
   a. 順序保存の暗号化を使用する暗号化設定の数に、それぞれの設定が適用されるレコードの数を掛けます。
   b. 拡張分を考慮する場合は、結果に 3 を掛けます。
2. 手順 1 の結果に 1,536 を掛けます。
   1,536 はレコードの平均サイズ (バイト単位) です。
3. 暗号化パターンを使用する場合は、トークン化されるレコードについて手順 1 ～ 2 を実行し、結果を合計に加算します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

タスクの結果
以上で計算した値が、順序保存およびトークン化データベースの推奨サイズ (バイト単位) になります。

エッジ暗号化 の制限事項

エッジ暗号化 はシステムの機能に影響を与えます。フィールドの暗号化が及ぼす影響について十分に評価してください。

フィールド タイプの制限

次のフィールドタイプのみを暗号化できます。

- 日付
- メール
- 日付/時刻
- HTML
- IP アドレス
- ジャーナル
- ジャーナル入力
- 複数行テキスト
- 1 行テキスト
- 文字列
- URL

次のフィールドタイプは暗号化できません。

- 選択肢フィールド
- 仮想フィールド
- システムテーブルのフィールド (sys_user の特定のフィールドを除く)
- テーブル内のシステムフィールド
- 自動番号付けスキームに関連付けられている数値フィールド。
- 上記以外のその他のフィールドタイプ

追加の制限：

- ジャーナルフィールドが暗号化されている場合は [投稿] ボタンが無効になります。たとえジャーナルフィールドが複数あり、それらのフィールドのうち 1 つだけが暗号化されている場合でも同様です。
- [検索項目] およびヘッダーフィルターボックスでは、暗号化フィールドは使用できません。
- インデックスとして使用されるフィールドを暗号化するときは、順序保存および等価性保存の暗号化タイプのみを使用できます。標準の暗号化タイプを使用してインデックス付きのフィールドを暗号化することはできません。

詳細については、「フィールドタイプ」を参照してください。

フィルタリングと検索の制限

標準暗号化

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

標準暗号化フィールド設定の文字列、日付、日付/時刻、または URL フィールドをフィルターの左オペランドとして選択した場合、フィルターオプションを利用できません。

等価性保存暗号化

等価性保存暗号化フィールド設定の文字列、日付、日付/時刻、または URL フィールドをフィルターの左オペランドとして選択した場合、次の演算子を利用できます。

- 次の値に等しい
- ではない
- は、空
- は空でない

順序保存暗号化

順序保存暗号化フィールド設定の文字列フィールドをフィルターの左オペランドとして選択した場合、[次の値に等しい]、[次の値ではない]、[は空]、 [は空でない] の他に次の演算子を利用できます。

- **>**
- 次の値未満 **(<)**

順序保存暗号化フィールド設定の日付フィールドまたは日付/時刻フィールドをフィルターの左オペランドとして選択した場合、[次の値に等しい]、[次の値ではない]、[は空]、 [は空でない] の他に次の演算子を利用できます。

- トランザクションの後
- トランザクションの前
- トランザクションの日以降
- トランザクションの日以前

日付および日付/時刻ピッカー

日付フィールドの場合、日付ピッカーを使用して日付を指定します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

日付/時刻フィールドの場合、日時ピッカーを使用して日時を指定します。

条件フィルターのリスト

リストでは [この値で絞り込み] および [この値を除外] オプションがサポートされています。完全一致のみが返されるか、フィルタリングで除外されます。

> **注:**
> 条件フィルターでの暗号化フィールドの追加は、UI ポリシーやビジネスルールなどのスクリプトでサポートされます。

設定の制限

暗号化設定の制限と動作は以下のとおりです。

- フィールドを エッジ暗号化 の設定テーブルに追加した後で、設定レコードを削除することはできません。フィールドの暗号化が不要になった場合は、エッジ暗号化 設定テーブルでレコードを非アクティブ化し、暗号化ジョブをスケジュールしてデータを復号化します。
- 親テーブルのフィールドが暗号化対象としてマークされている場合、すべての継承テーブルのフィールドも暗号化されます。たとえば、タスクテーブルの [簡単な説明] フィールドが暗号化される場合、インシデントテーブルの [簡単な説明] フィールドの内容も暗号化されます。
- 親テーブルから継承されたフィールドが暗号化対象としてマークされている場合、親テーブルのフィールドは暗号化できません。たとえば、インシデントテーブルの [簡単な説明] が暗号化対象としてマークされている場合、タスクテーブルの [簡単な説明] は暗号化できません。この例では、問題テーブルの [簡単な説明] は暗号化できます。
- 暗号化設定が定義されているフィールドを任意の形式にエクスポートすると、プロキシサーバー経由でエクスポートした場合でも、その出力に暗号化された値が含まれます。
- 暗号化設定が定義されているフィールドにデータをインポートすることはできません。
- 継承された日付および日付/時刻フィールドは暗号化できません。親テーブルから継承された日付または日付/時刻フィールドは、[列] フィールドのドロップダウンリストにリストされず、これらのフィールド用に日付または日付/時刻の暗号化設定を作成できません。
- 文字列または URL フィールドは、親テーブルまたは子テーブルからのみ暗号化することができますが、両方からは暗号化できません。

インスタンスの制限

インスタンスで エッジ暗号化 の使用が及ぼす影響は以下のとおりです。

- バックエンドロジックは暗号化されたデータを処理できません。インスタンスに暗号化されたデータが含まれている場合、暗号化フィールドのデータの評価に依存しているビジネスルール、バックエンドスクリプト、またはバックエンド機能は正しく実行されません。

> **注:**
> 等価性保存または順序保存の暗号化により暗号化されたデータもまた、同一の暗号化された値と比較されるときは、等価性のチェックを受けます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- メール処理はメールシステムからインスタンスに直接送られ、Edge プロキシを経由させることはできないため、メールを介して送受信されるデータは Edge プロキシで暗号化または復号化することはできません。
  - 受信メールのデータと添付ファイルは暗号化されません。
  - 送信メールのデータと添付ファイルは暗号化されたままになり、復号化することはできません。
- サーバーで実行されるスクリプトは、暗号化されたデータを変更できません。
- グローバル検索はサポートされていません。グローバル検索では、暗号化されたデータとクリアテキストデータの両方について検索が試みられるため、結果が期待どおりにならないことがあります。
- 暗号化されたデータを、フィールドが暗号化されていないレコードにコピーして貼り付けることはできません。
- 選択した暗号化のタイプによっては、暗号化フィールドのユーザーインターフェイス機能が低下します。たとえば、比較、グループ化、ソート、検索の機能が影響を受ける可能性があります。一般に、選択する暗号化の強度が増すほど、機能性は低下します。
- Java KeyStore、SafeNet、および Unbound Technology 以外の、サードパーティによるソフトウェアまたはハードウェアの暗号化キー管理はサポートされていません。
- 複数のプロキシサーバーから単一のインスタンスへの接続はサポートされていますが、暗号化プロキシクラスターの管理およびモニタリングは利用できません。プロキシはそれぞれ個別に管理する必要があります。
- ワークロードや暗号化フィールド数などのシステム設定は、暗号化フィールドのパフォーマンスに影響する可能性があります。
- エッジ暗号化 プロキシサーバーは 1 つのインスタンスにしか接続できません。
- インスタンスで Oracle データベースを使用していて、暗号化対象としてマークしている文字列フィールドが 2925 文字より多い場合、順序保存の暗号化を選択していてもフィールドをソートできません。
- インスタンスで Oracle データベースを使用している場合、文字セットとしてサポートされるのは Unicode AL32UTF8 のみです。
- 暗号化されたデータはレポートでは使用できません。
- エッジ暗号化 はデータアーカイブでは使用できません。

Edge Encryption のインストール

エッジ暗号化 プロキシは、手動でインストールするか、エッジ暗号化 インタラクティブインストーラーを使用してインストールできます。

Java の要件

エッジ暗号化 プロキシサーバーをインストールまたは実行するホストマシンでは、サポートされているバージョンの Java を保持する必要があります。現在サポートされているバージョンは 11.x バージョンシリーズの Java 11.0.6 以降です。

> **注:**
> Java 8 は Utah リリースからサポートされなくなりました。Utah バージョンの エッジ暗号化 プロキシをインストールする前に、エッジ暗号化 プロキシを使用する環境を Java 11 にアップグレードしてください。

プロキシサーバーのインストール

エッジ暗号化 のインストールには次の手順が含まれます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

- インタラクティブインストーラーまたは手動インストーラーを使用して、ネットワークのサーバーに エッジ暗号化 プロキシアプリケーションをインストールします。
- 暗号化設定と暗号化ルールにデジタル署名するための RSA キー ペアを生成します。
- AES 256 暗号化の使用を予定している場合は、Java Cryptography Extension (JCE) をインストールします。
- セキュア SSL 接続を使用している場合は、サーバー証明書を取得して Java KeyStore にインポートします。
- キーストアと暗号化キーをセットアップします。
- 順序保存の暗号化タイプまたは暗号化パターンを使用する場合は、ネットワークのマシンに MySQL データベースをセットアップします。
- 目的のプロパティを設定します。プロパティは edgeencryption.properties 設定ファイルにあります。
- エッジ暗号化 がプロキシサーバーからの要求を処理できるよう、プロキシサーバーが信頼できるソースであることを指定します。

プロキシサーバーへのアクセス

インストールが完了したら、`<ホスト>:<ポスト>` の URL 形式を使用して各ユーザーのブラウザーから エッジ暗号化 プロキシを参照します。値は、edgeencryption.properties ファイルのホストプロパティとポートプロパティによって決まります。

次の値はそれらの例です。

プロパティ	サンプル値
edgeencryption.proxy.host	hostname.mycompany.com
edgeencryption.proxy.http.port	8081

クライアントはアドレス `http://hostname.mycompany.com:8081/` を使用してプロキシサーバーにアクセスします。

注:
DNS 設定とルーティングルールを使用することもできます。ホストとポートの値はネットワーク管理者が決定します。

Edge Encryption を要求する

エッジ暗号化 プラグイン (com.glide.edgeencryption) は個別のサブスクリプションとして使用できます。

始める前に
サブスクリプションを購入するには、ServiceNow アカウントマネージャーにお問い合わせください。アカウントマネージャーは通常数日以内に、組織の本番および準本番インスタンスでプラグインが有効化されるように手配することができます。

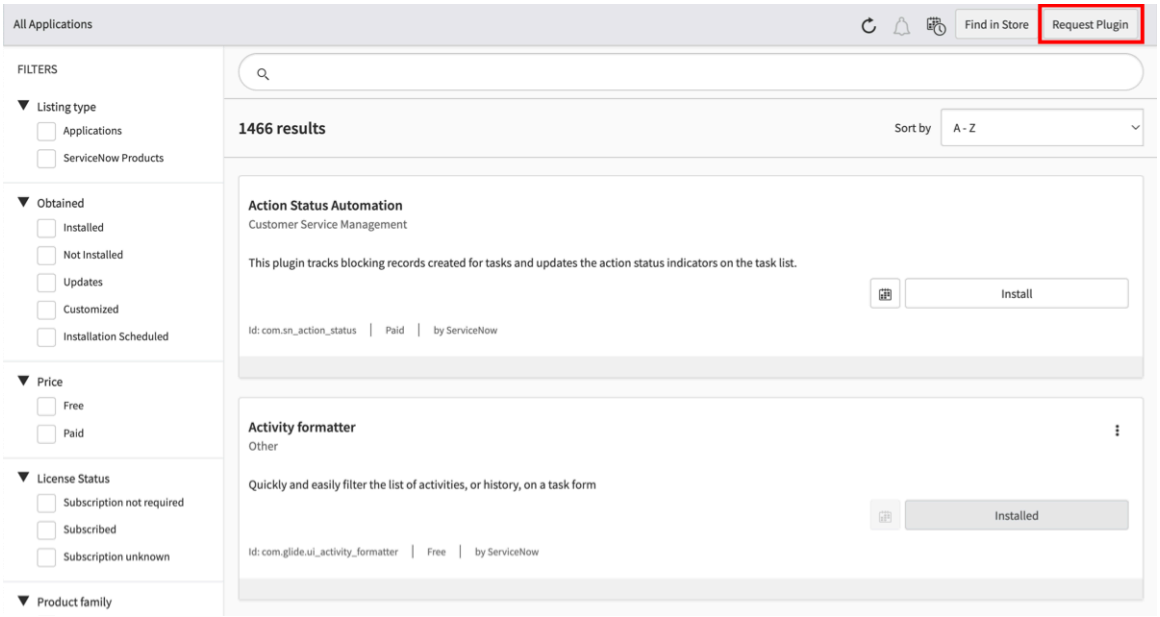
アカウントマネージャーがいない場合、購入後に有効化を延期することを決定するか、無料で準本番インスタンスで製品を評価する場合には次の手順を実行します。

必要なロール：なし

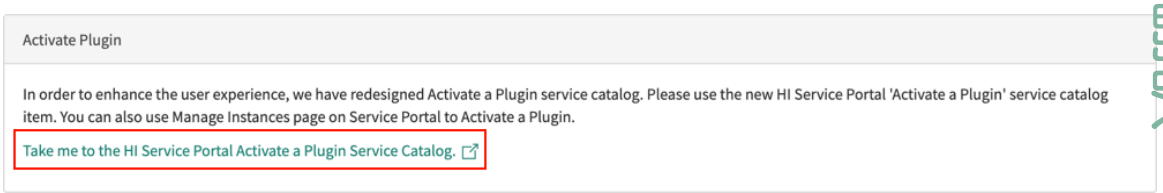
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. 移動先 すべて > システムアプリケーション > 利用可能なすべてのアプリケーション > すべて。
2. [すべてのアプリケーション] ページで [プラグインの要求] をクリックして、Now Support で [プラグインをアクティブ化] フォームを開きます。



3. Now Support で、Now Support サービスポータル サービスカタログ にアクセスするリンクを選択します。



4. インスタンスを選択します。
5. [アクション] > [プラグインのアクティブ化] を選択します。
6. [プラグインのアクティブ化] フォームで、次の情報を入力します。

[プラグインのアクティブ化] フォーム

フィールド	説明
ターゲットインスタンスは何ですか	プラグインをアクティブ化するインスタンス。
どのプラグインをアクティブ化しますか	アクティブ化するプラグインの名前です。

自動翻訳

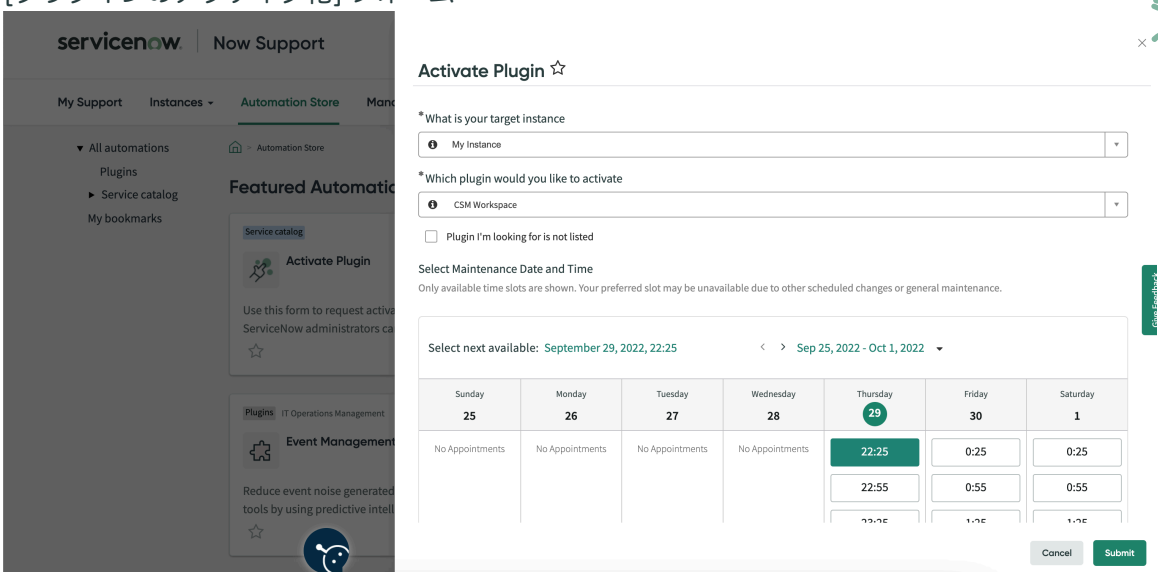
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	注: 必要なプラグインが表示されない場合、または OEM またはオンプレミスのインスタンスでプラグインをアクティブ化している場合は、[探しているプラグインが表示されていません **(Plugin I'm looking for is not listed)]** チェックボックスをオンにして、プラグインの名前を入力します。
メンテナンスの日時を選択 (Select Maintenance Date and Time)	プラグインをアクティブ化する日時。 注: プラグインは、米国太平洋標準時で、毎営業日の朝と夕方の 2 回のバッチでアクティブ化されます。特定の時刻にプラグインをアクティブ化する必要がある場合は、[理由/コメント **(Reason/ Comments)]** フィールドに要求を入力します。

Example

たとえば、 [自分のインスタンス (My Instance)] という名前のインスタンスで CSM Workspace プラグインをアクティブ化するには、次のフォームを参照してください。

[プラグインのアクティブ化] フォーム



7. [送信] を選択します。
プラグインの要求の詳細については、次を参照してください。 の Service Catalog [KB0751715] 記事からのプラグインの要求 Now Support ナレッジベース。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Edge Encryption ユーザー アカウントを設定する

エッジ暗号化 プロキシは、暗号化設定情報を取得および更新するために、ユーザーとしてインスタンスに接続します。この目的のためにユーザー アカウントを作成し、edge_encryption ロールをユーザーに与えます。

始める前に
ロールをアサインする前に エッジ暗号化 プラグインをインストールする必要があります。

必要なロール：admin

手順

1. ServiceNow インスタンスで、エッジ暗号化 プロキシ アプリケーションで使用されるユーザー アカウントを作成します。
2. edge_encryption ロールをユーザーにアサインします。

Edge Encryption プロキシサーバーをダウンロードする

エッジ暗号化 プロキシサーバー アプリケーションをインスタンスからダウンロードし、エッジ暗号化 プロキシサーバーを実行する予定の各コンピューターにファイルをコピーします。

始める前に
この手順を始める前に、エッジ暗号化 プラグインをインスタンスにインストールして有効化する必要があります。

> **注:**
> プロキシ エッジ暗号化 は、Oracle JRE でのみ正式にサポートされています。

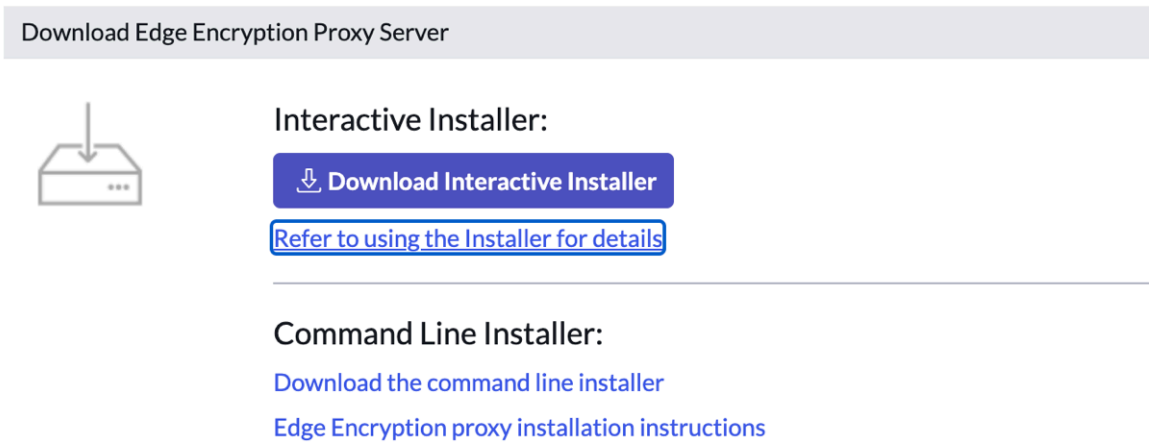
必要なロール：security_admin

このタスクについて

手順

1. 移動先 すべて > エッジ暗号化の設定 > インストールとダウンロード > ダウンロード.
2. 対話型インストーラーを使用するには、[対話型インストーラーのダウンロード] をクリックします。

   プロキシサーバーを手動でインストールする場合は、プロキシサーバーの OS バージョンを選択します。



自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

> **注:**
> プロキシサーバーが稼働するには少なくとも 4 GBのメモリが必要なため、32 ビット JRE と 32 ビットオペレーティングシステムは Washington DC リリース以後はサポートされなくなりました。

3. エッジ暗号化 プロキシサーバーを実行する予定の各コンピューターにインストーラーをコピーします。

> **注:**
> エッジ暗号化 プロキシサーバーを手動でインストールする場合は、エッジ暗号化 プロキシサーバーを実行する予定の各コンピューターに ZIP ファイルをコピーします。

次のタスク

エッジ暗号化 インストーラーをダウンロードしたら、「インタラクティブ インストーラーを使用して Edge Encryption プロキシサーバーをインストールする」の手順を実行します。手動でインストールする場合は、「コマンド ライン インストーラーを使用して Edge Encryption プロキシサーバーをインストールする」のの手順を実行します。

インタラクティブ インストーラーを使用して **Edge Encryption** プロキシサーバーをインストールする

インタラクティブ インストーラーを使用して、Windows または Linux コンピューターに エッジ暗号化 プロキシサーバーをインストールします。

始める前に

> **注:**
> SafeNet KeySecure キーストア ファイルは、エッジ暗号化 インストーラーではサポートされていません。SafeNet KeySecure キーストアを使用するには、「コマンド ライン インストーラーを使用して Edge Encryption プロキシサーバーをインストールする」の手順を実行します。

この手順を始める前に、エッジ暗号化 プラグインをインスタンスにインストールして有効化する必要があります。エッジ暗号化 インストーラーを実行するマシンに Java バージョン 11.0.6 以降がインストールされていることを確認してください。

必要なロール：

- ServiceNow インスタンスでの security_admin
- Windows ホストでのローカル管理者またはドメイン管理者
- Linux ホスト上のファイルシステムへのフルアクセス権限があるサービスユーザー

このタスクについて

新しいプロキシサーバーをインストールした後、再度インストーラーを実行してテストを行い、インストールに関する問題を検出したり、現在の設定を変更したりすることができます。次の選択肢があります。

- [新規インストール]：プロキシサーバーを新規にインストールします。
- [インストールの確認]：以前のインストール環境で問題を検出して修正するためのテストを実行します。
- [既存への再インストール]：以前のインストール環境で問題を検出して修正するためのテストを実行し、既存の設定を表示または変更します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

> **注:**
> Linux マシンの特権ポート (ポート 80 または 443) にプロキシサーバーをインストールする場合は、ファイル システムへのフル アクセス権を持つ root ユーザーとしてインストーラーを実行する必要があります。プロキシサーバーのインストール後にファイル システムのアクセス権を制限する場合、プロキシ インストーラーの SetUID 機能を使用できます。この機能を有効にするには、インストーラーを root または sudo root として起動します。インストーラーのプロンプトが表示されたら、特権のないユーザーのユーザー名とユーザー グループを入力します。指定したユーザーのファイル システム権限を使用して、プロキシサーバーがインストールされます。この手順をスキップして、root 権限でデフォルトのインストールを続けることができます。

手順

インストーラーを使用して、インスタンス用の複数のプロキシを複数のマシンにインストールし、次の条件が適用されることを確認します。

- すべてのプロキシに、同じ暗号キーと同じ RSA キー ペアを持たせる必要があります。これらは、暗号化設定と暗号化ルールへのデジタル署名に使用されます。
- 暗号化キーは、インスタンスで設定されたデフォルトのキーである必要があります。
- プロキシ データベースをインストールの一部としてセットアップする場合、すべてのプロキシで同じプロキシ データベースを使用する必要があります。

  等価性保存の暗号化、順序保存の暗号化、またはトークン化を行う場合、状況に応じてプロキシ データベースが必要になります。これらの機能をどれも使用しない場合は、プロキシ データベースは必要ありません。

次のタスク
NVDA を使用する場合は、「Java アプリケーションで 32 ビット NVDA を使用するように Windows 64 ビットホストを設定する」を参照してください。NVDA は、キーボード ユーザーを対象にアクセシビリティ対応 Java アプリケーションの読み上げのために開発された支援技術 (スクリーンリーダー) です。

エッジ暗号化 プロキシサーバーをインストールしたら、プロキシサーバーの初期メモリ制限と上限メモリ制限を設定します。

エッジ暗号化 プロキシサーバーをインストールする (インタラクティブ インストーラー)

Windows または Linux コンピューターに エッジ暗号化 プロキシをインストールします。

始める前に
必要なロール：管理者

手順

1. Edge Encryption プロキシサーバー インストーラーをダウンロードします。
2. エッジ暗号化 プロキシ インストーラーを開きます。

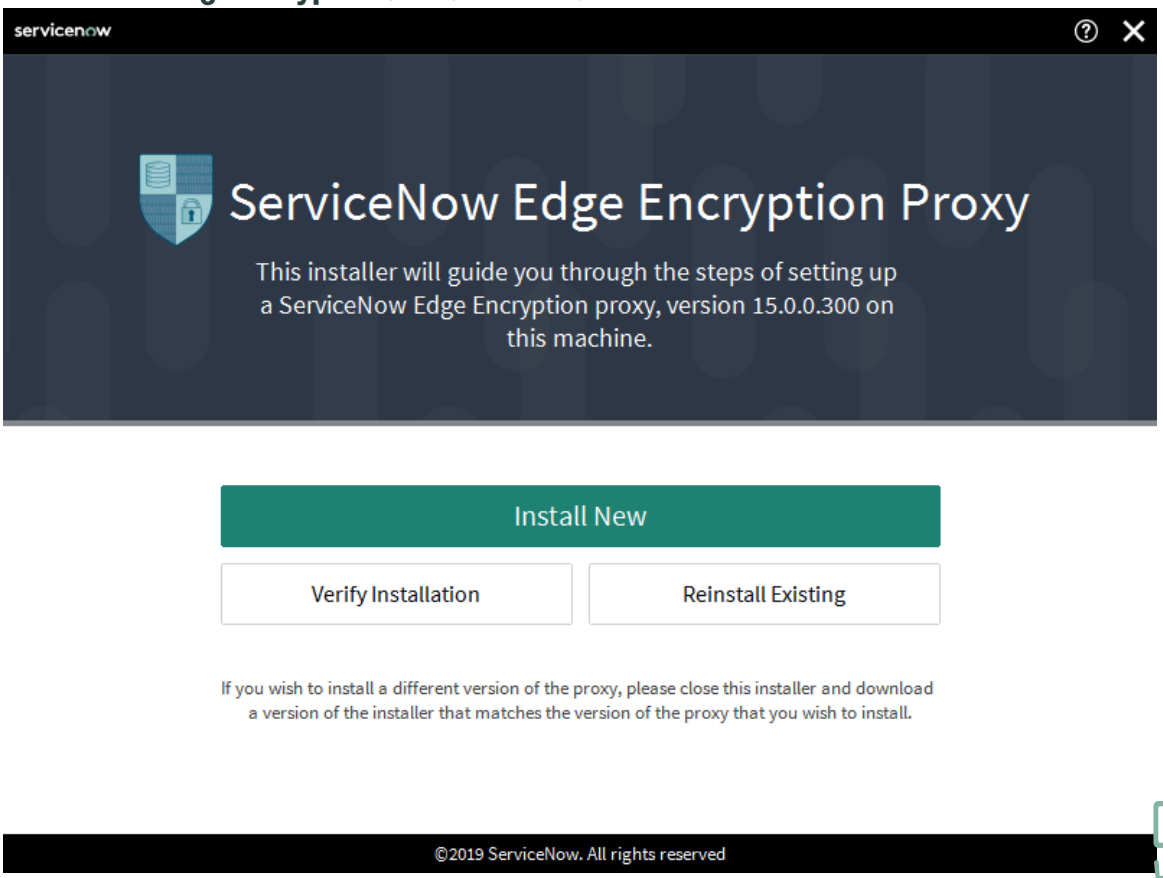
   > **注:**
   > Windows マシンにインストールする場合は、インストーラーを管理者として実行する必要があります。

   a. Windows マシンでインストーラーを管理者として実行するには、コマンド プロンプトを右クリックし、[管理者として実行]を選択します。
   b. コマンド ラインから、ダウンロードした .jar ファイルがあるディレクトリーに移動します。
   c. コマンド `java -jar <ファイル名>.jar` を実行します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

ServiceNow Edge Encryption プロキシインストーラー



自動翻訳

3. プロキシサーバーを新規にインストールするには、[新規インストール] を選択します。
すでにプロキシがインストールされている場合は、インストーラーで次の操作を実行できます。
   - [インストールの確認]：以前のインストール環境で問題を検出して修正するためのテストを実行します。
   - [既存への再インストール]：以前のインストール環境で問題を検出して修正するためのテストを実行し、既存の設定を表示または変更します。
4. インストールの場所とターゲットの **ServiceNow** インスタンスの設定を行います。

   a. [参照] をクリックしてインストールの場所を選択します。または、手動でインストール パスを入力します。

   b. ターゲットの ServiceNow インスタンスの URL を入力します。
   プロトコルとポート番号を含めます。

   Example
   https://example.servicenow.com:443

   c. ターゲットの ServiceNow インスタンスで edge_encryption ロールを持つユーザーのユーザー名とパスワードを入力します。

5. [次へ **(Next)**] をクリックします。
6. 接続設定とプロキシ設定を行います。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

設定	説明
プロキシ ホスト	プロキシサーバーをインストールするマシンの完全修飾ドメイン名。 注: **[FQDN** を検出] をクリックすると、マシンの完全修飾ドメイン名が検索され、[プロキシ ホスト] フィールドに自動入力されます。 このプロパティとポートによって、クライアントがプロキシサーバーへのアクセスに使用する URL が定義されます。
HTTP ポート	HTTP 通信のプロキシのポート。
HTTPS ポート	HTTPS 通信のプロキシのポート。
プロキシ名	プロキシとそのサービスの名前。プロキシ名は一意である必要があります
プロキシ ポーリング間隔	ポーリング間隔 (秒単位)。デフォルト設定では、プロキシが暗号化設定の変更を認識するまでに 5 秒かかります。値を大きくするほど、オンラインになったプロキシをインスタンスが検出するのに時間がかかります。 注: プロキシ ポーリング間隔のデフォルト設定を変更すると、プロキシがオンラインになったときに検出が遅れることがあります。
プロキシ キープアライブ ping 間隔	プロキシからインスタンスに発行される ping の間隔 (秒単位)。プロキシとインスタンス間の接続を確認するために、定期的に ping が発行されます。デフォルト値は 10 です。最小値は 5 です。

7. [インストール]をクリックします。
   エッジ暗号化 プロキシサーバーがインストールされます。インストールには数分かかることがあります。

CyberArk のプロパティの保護を設定する

オプションで、CyberArk のプロパティの保護を設定して、エッジ暗号化 のパスワードを一元管理されたセキュアデジタルボールトに安全に格納します。

始める前に
必要なロール：admin

このタスクについて
CyberArk 接続パラメーターとプロキシサーバーの保護された資格情報を設定する前に、CyberArk AIM (アプリケーション ID 管理) を購入して設定する必要があります。AIM クライアントのインストールの一部として、JavaPasswordSDK.jar ファイルが AIM クライアントインストールディレク

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

トリにインストールされます。CyberArk ボールトは独立した強化されたサーバーにインストールされ、AIM クライアントはそのサーバーに安全にアクセスできます。

> **注:**
> CyberArk AIM クライアントは、Edge プロキシがインストールされているすべてのホスト コンピューターにインストールする必要があります。

Edge インストーラでは、JavaPasswordSDK.jar ファイルの場所を指定して、Edge プロキシへの CyberArk 接続を設定する必要があります。また、AIM クライアントのインストール時に定義した他の値も入力する必要があります。

CyberArk のパスワード保存の設定はオプションです。CyberArk のパスワード保存の設定をしない場合は、CyberArk の画面で [スキップ] をクリックします。

手順

1. エッジ暗号化 インストーラの CyberArk 接続ページで、CyberArk 接続パラメーターを入力します。

CyberArk 接続パラメーター

設定	説明
PasswordSDK.jar へのパス	CyberArk の設定中にホスト Windows マシンにインストールされた JavaPasswordSDK.jar ファイルへのパス。
アプリ ID	CyberArk の設定中に入力された [アプリ **ID]**。
安全な名前	CyberArk の設定中に入力された [安全な名前]。

2. [次へ] をクリックします。
3. インストーラの [CyberArk で保護された認証情報] ページで、CyberArk によって保護される認証情報を入力します。
   - すべての保護されたパスワードに単一の認証情報名を使用するには、[すべての認証情報に単一の認証情報名を適用する] チェックボックスをオンにし、認証情報名を入力して、[適用] をクリックします。
   - 次のフィールドの 1 つ以上に認証情報名を入力します。資格情報の名前は、CyberArk の構成中に SSH キーに入力されるユーザー名です。

CyberArk で保護された資格情報

設定	説明
Edge Encryption ユーザー	Edge Encryption ユーザーの CyberArk 資格情報名。
署名鍵キーストア	署名鍵キーストアの CyberArk 認証情報名。
HTTPS 証明書キーストア	HTTPS 認定キーストアの CyberArk 認証情報名。
暗号鍵キーストア	暗号鍵キーストアの CyberArk 資格情報名。
データベース	データベースキーストアの CyberArk 認証情報名。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

設定	説明
SafeNet HTTPS 証明書キーストア	SafeNet HTTPS 認定キーストアの CyberArk 認証情報名。
SafeNet サーバー	SafeNet サーバーの CyberArk 認証情報名。
フォワードプロキシ	フォワードプロキシの CyberArk 認証情報名。

4. [次へ] をクリックします。

署名キーを設定する

エッジ暗号化 プロキシ インストーラーでプロキシサーバーをインストールした後、署名キーを設定します。

始める前に
必要なロール：管理者

このタスクについて
プロキシサーバーによって設定やプロパティに変更が加えられると、署名キーによる署名が行われます。署名キーは、JCEKS KeyStore の非対称 RSA キー ペアである必要があります。

> **注:**
> 複数のプロキシをインストールする場合は、各プロキシで同じ署名キーを使用する必要があります。

手順

1. エッジ暗号化 インストーラーの [署名キー] ページで、署名キーを格納するためのホスト マシン上のキーストアを選択します。
   - [新しい **Java KeyStore** を作成する]：新しいキーストアのディレクトリーの場所、名前、およびパスワードを入力します。
   - [既存のキーストアを使用する]：キーストア ファイルの場所とパスワードを入力します。
2. [次へ **(Next)**] をクリックします。
3. 署名キーを選択するか作成します。
   - [新しいキー]：このプロキシの署名キーを作成します。
   - [既存のキーを使用する]：選択したキーストアの RSA キーペアを使用します。
   - [既存のキーをインポートする]：別のキーストアから RSA キーペアをインポートします。キーストア ファイルを参照し、キーストアのパスワードを入力し、キー エイリアスを選択します。キーの新しいエイリアスを指定します。
4. [次へ **(Next)**] をクリックします。

HTTPS 証明書を設定する

クライアントからセキュア SSL 接続を使用して エッジ暗号化 プロキシサーバーに接続できるようにするため、HTTPS 証明書をプロキシサーバーにインポートします。

始める前に
必要なロール：管理者

このタスクについて
エッジ暗号化 プロキシは、接続を試みるクライアントに対して、HTTPS 証明書を提供します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. エッジ暗号化 インストーラーの [HTTPS 証明書] ページで、証明書を格納するためのキーストアを選択します。
   - [新しい **Java KeyStore** を作成する]：新しいキーストアのディレクトリーの場所、名前、およびパスワードを入力します。
   - [既存のキーストアを使用する]：キーストア ファイルの場所とパスワードを入力します。
2. [次へ **(Next)**] をクリックします。
3. 証明書を選択するかインポートします。
   キー エイリアスは、証明書に対して与えられるエイリアスです。
   - [既存の証明書を使用する]：選択したキーストアにある既存の証明書を使用します。
   - [ファイルまたはキーストアからインポートする]：別のキーストアまたは .cer ファイルから証明書をインポートします。キーストアまたは .cer ファイルを参照し、パスワードを入力し、エイリアスを選択します。証明書に対して新しいエイリアスを指定する必要があります。
4. [次へ **(Next)**] をクリックします。

AES 128 ビット暗号化キーを設定する

エッジ暗号化 プロキシインストーラーで HTTPS 証明書を設定したら、データを暗号化するように AES 128 ビット暗号化キーを設定します。

始める前に
必要なロール：管理者

このタスクについて
暗号化キーは、/keys ディレクトリーにあるプレーン テキスト ファイルか、キーストア内部にある秘密キーです。AES 128 ビットおよび AES 256 ビットの暗号化キーに対してキーストアを使用する場合は、両方で同じキーストアを使用する必要があります。

Edge プロキシサーバーで SSL 証明書を更新する場合は、「SSL 証明書の更新 (Update SSL certificate)」を参照してください。

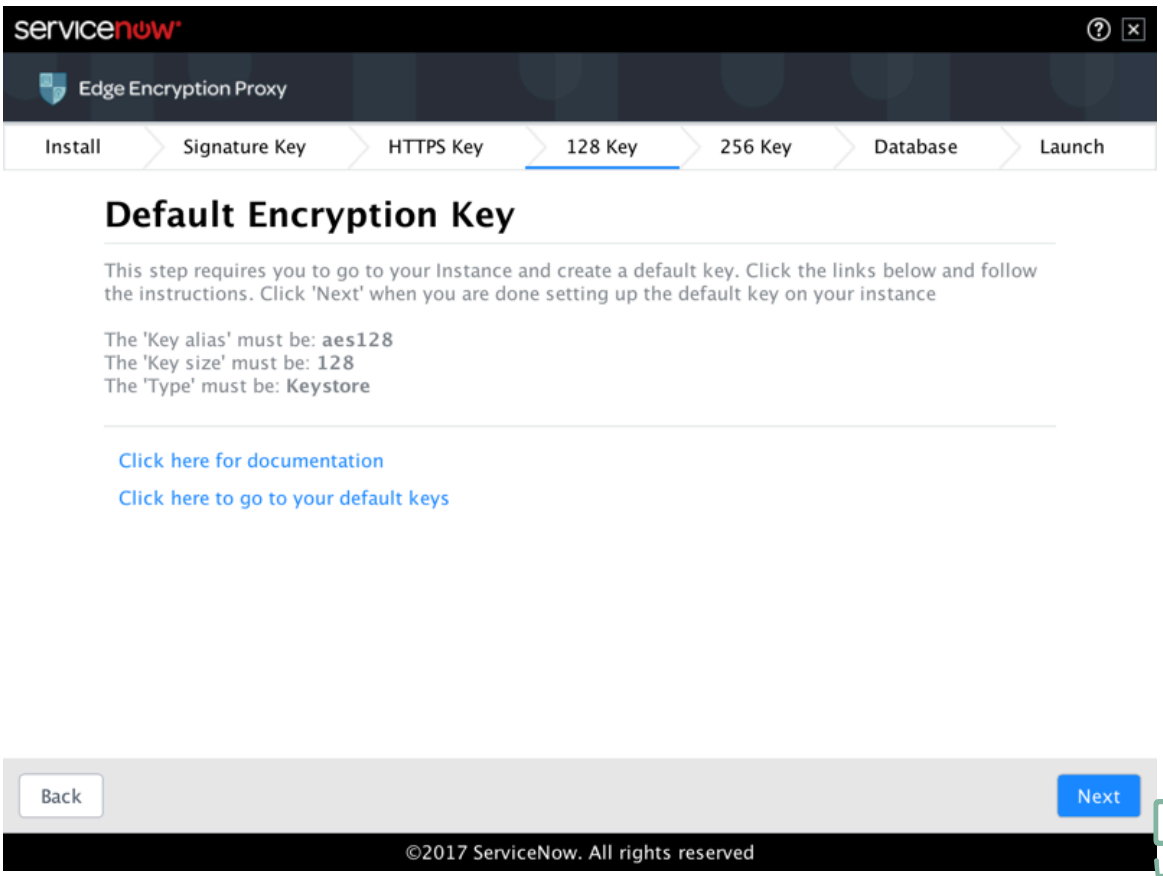
手順

1. 暗号化キーの場所を選択します。
2. [次へ **(Next)**] をクリックします。
3. 暗号化キーを選択または作成します。
4. [次へ **(Next)**] をクリックします。
5. インストーラーで定義した要件に従って、インスタンスのキーを設定します。
   インスタンスのキーを設定するには、インスタンスに移動し、デフォルトキーを定義します。「インスタンスで暗号化キーを設定する」を参照してください。キーのエイリアス、サイズ、タイプがインストーラーで定義した要件と一致していることを確認します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

デフォルトキーの要件



6. インスタンスでキーを設定したら、インストーラーに戻り、[次へ] をクリックします。

AES 256 ビット暗号化キーを設定する

Edge プロキシインストーラーで AES 128 ビット暗号化キーを設定したら、データを暗号化するように AES 256 ビット暗号化キーを設定します (オプション)。

始める前に
必要なロール：管理者

このタスクについて
暗号化キーは、/keys ディレクトリーにあるプレーン テキスト ファイルか、キーストア内部にある秘密キーです。AES 128 ビットおよび AES 256 ビットの暗号化キーに対してキーストアを使用する場合は、両方のキーで同じキーストアを使用する必要があります。AES 256 ビット暗号化キーを設定しない場合は、[スキップ] を選択して、プロキシサーバーのインストールを続行します。

Edge プロキシサーバーで SSL 証明書を更新する場合は、「SSL 証明書の更新 (Update SSL certificate)」を参照してください。

手順

1. 暗号化キーの場所を選択します。

2. [次へ] を選択します。

3. 暗号化キーを選択または作成します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

4. [次へ] を選択します。
5. オプション: AES 256 ビット暗号化を使用する場合は、「AES 256 ビット暗号化キーを設定する」を参照してください。
6. AES 256 ビット暗号化を使用する場合は、AES 256 ビットのデフォルトの暗号化キーをインスタンスに設定する必要があります。

   これを行うには、インスタンスに移動し、デフォルトキーを定義します。「インスタンスで暗号化キーを設定する」を参照してください。キーのエイリアス、サイズ、タイプがインストーラーで定義した要件と一致していることを確認します。
7. インスタンスでキーを設定したら、インストーラーに戻り、[次へ] を選択します。

SSL 証明書の更新

Edge プロキシサーバーで SSL 証明書を更新する場合は、古い証明書を削除する必要があります。

始める前に
必要なロール：admin

このタスクについて
Edge プロキシサーバーで SSL 証明書を更新する場合は、古い証明書も削除する必要があります。削除しない場合、Edge プロキシサーバーが新しい証明書を使用するように設定されていても、古い証明書 (KeyStore ファイルのエイリアス形式) が引き続き使用されます。

手順
1. Edge プロキシサーバーで、Java KeyStore のエントリをリストします。

```
keytool -list -keystore keystore.jceks -storetype jceks -storepass MY_SUPER_PASSWORD
```

2. 古い SSL 証明書を削除します。

```
keytool -delete -alias MY_OLD_ALIAS -keystore keystore.jceks -storetype jceks -storepass
 MY_SUPER_PASSWORD
```

3. Java KeyStore に新しい SSL 証明書を追加します。

Edge Encryption プロキシデータベースを設定する

順序保存の暗号化タイプまたは暗号化パターンを使用する場合は、オプションで エッジ暗号化 プロキシデータベースのプロパティを設定できます。

始める前に
必要なロール：管理者

このタスクについて
順序保存の暗号化タイプまたは暗号化パターンを使用する場合は、ネットワーク内で MySQL データベースを実行する必要があります。このタスクではプロキシからデータベースに接続しますが、データベースのインストールまたは設定は行いません。

> **注:**
> 複数のプロキシサーバーを使用する場合は、すべてのプロキシサーバーで同じプロキシ データベースを使用する必要があります。インストーラーに入力する値は、すべてのプロキシサーバーについて同じにする必要があります。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. プロキシデータベースの場所であるデータベースの URL を確認または変更します。
2. [名前] フィールドに、プロキシ データベースの名前を入力します。
   デフォルト値は [*edgeencryption*] です。
3. プロキシ データベースにアクセスするためのユーザー名とパスワードを入力します。
4. [次へ **(Next)**] をクリックします。

Edge Encryption プロキシサーバーを起動する

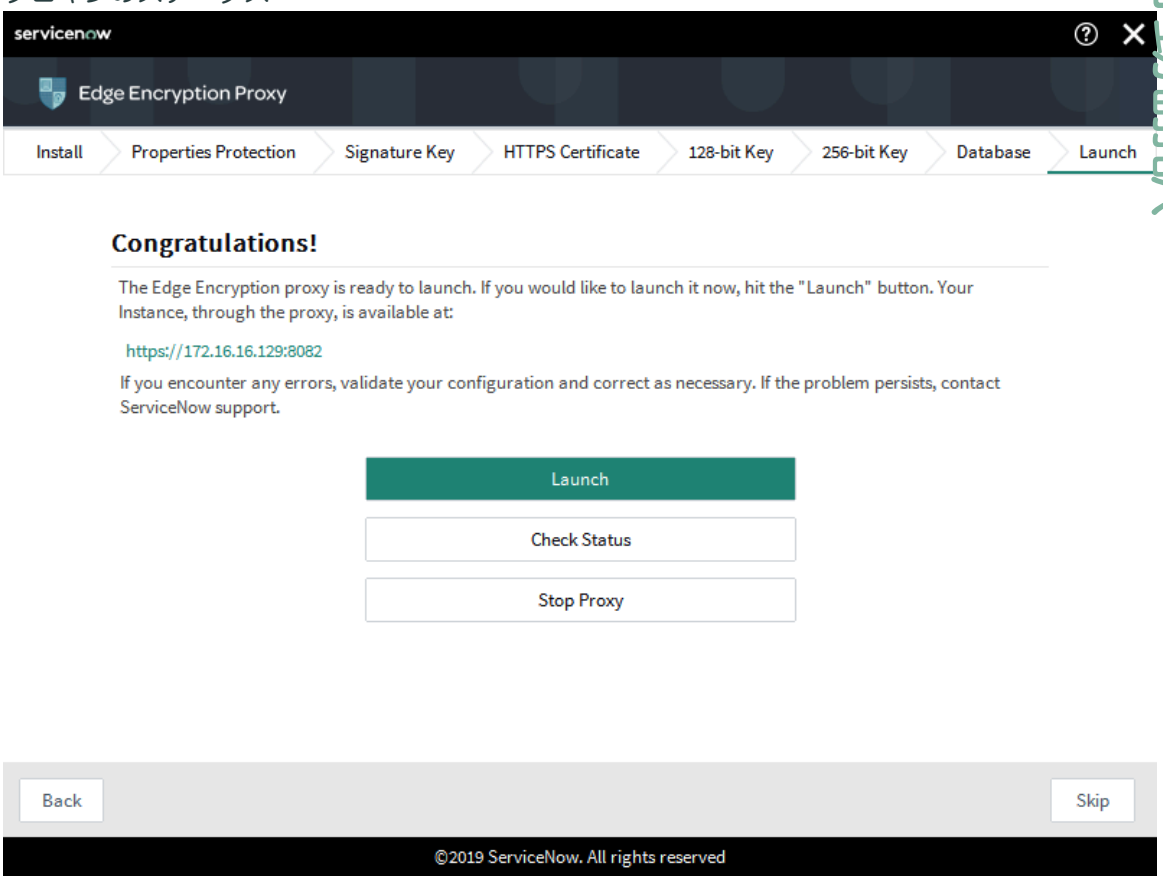
エッジ暗号化 プロキシのインストールと設定を終えたら、インストーラーからプロキシを起動できます。

始める前に
必要なロール：admin

手順

1. インスタンスでキーを設定し、プロキシデータベースを設定したら、エッジ暗号化 プロキシインストーラーに戻り、[起動] をクリックします。
2. 問題が検出された場合、またはプロキシサーバーのステータスを確認する場合は、[ステータスのチェック] をクリックして、プロキシが実行されているかどうかを確認できます。
   プロキシのステータスがメッセージに表示されます。

プロキシのステータス



次のタスク
エッジ暗号化 プロキシサーバーのインストールが正常に完了したら、プロキシサーバーの初期メモリ制限と上限メモリ制限を設定するの手順を実行します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Edge Encryption プロキシサーバーのインストールを検証してトラブルシューティングを行う

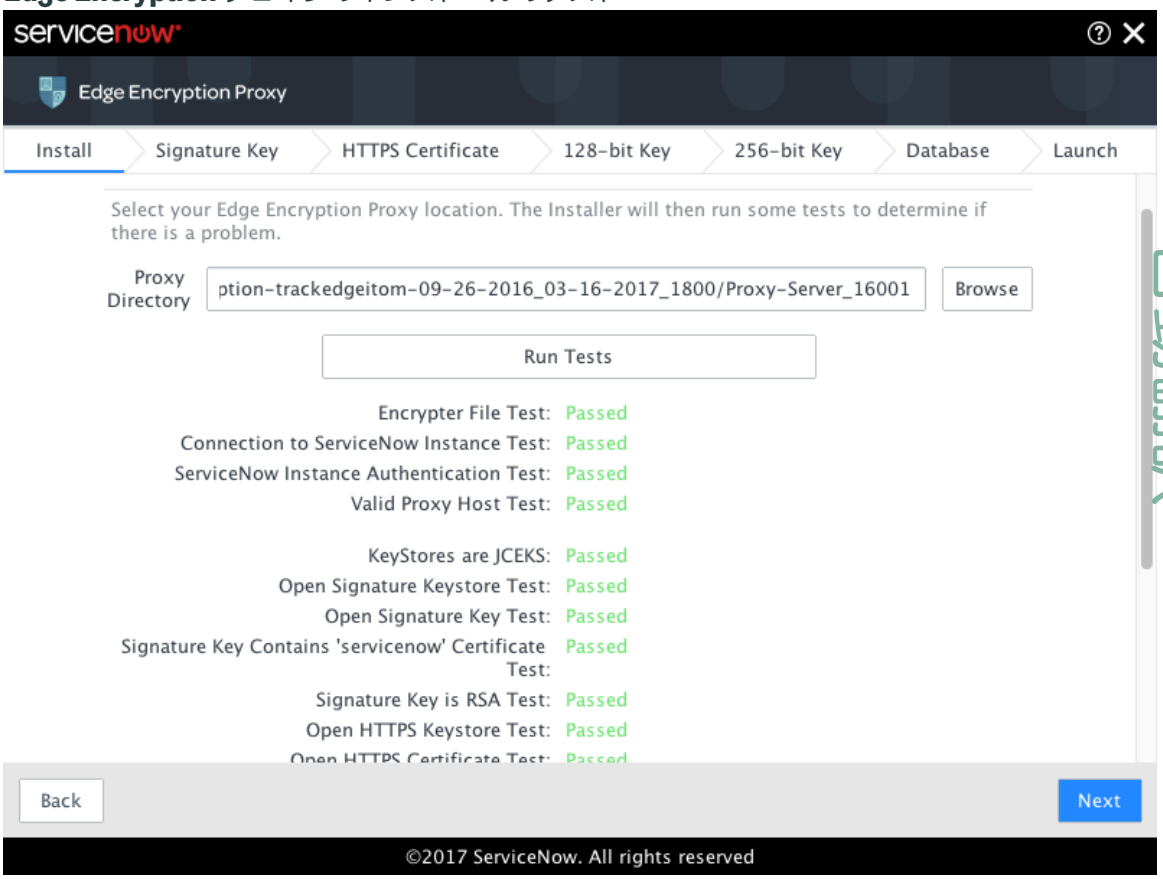
エッジ暗号化 プロキシをインストールした後、インストールを検証して、問題を特定したり、プロキシを開始および停止したりできます。

始める前に
必要なロール：管理者

手順

1. エッジ暗号化 プロキシ インストーラーを開きます。
2. [インストールを検証] を選択します。
3. [プロキシのディレクトリー] をクリックし、プロキシのディレクトリーを選択します。
4. [テストを実行] をクリックします。
   テストの結果が表示されます。

Edge Encryption プロキシのインストールのテスト



5. [次へ **(Next)**] をクリックします。
   問題が発生した場合は、インストーラーの画面を移動して設定を修正できます。問題が検出されない場合、インストーラーは [起動] ページに移動します。[起動] ページから、プロキシのステータスを確認したり、プロキシを停止したり、プロキシを起動したりできます。

コマンド ライン インストーラーを使用して Edge Encryption プロキシサーバーをインストールする

ネットワークに複数の エッジ暗号化 プロキシサーバーを手動でインストールします。

始める前に
必要なロール：security_admin (ServiceNow インスタンス) およびローカル管理者 (ホスト マシン)。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

順序保存の暗号化タイプまたは暗号化パターンを使用する場合は、ネットワークのマシンに MySQL データベースをセットアップします (まだ存在しない場合)。

> **注:**
> Unbound Technology 暗号化キーを エッジ暗号化 とともに使用する場合、Unbound クライアント マシンでコマンドライン インストーラを使用してプロキシサーバーをインストールします。エッジ暗号化 プロキシサーバーは、Unbound テクノロジ クライアントと同じマシンで実行する必要があります。

このタスクについて

最初に、単一の エッジ暗号化 プロキシサーバーをセットアップします。最初のプロキシサーバーが正常に実行されたら、1 つのインスタンスにさらにプロキシサーバーを追加して、最適な環境を確保します。必要な追加のプロキシサーバーの数の決定については、「Edge Encryption 環境のサイジング」を参照してください。

Edge Encryption プロキシサーバーをインストールする (コマンド ライン インストーラー)

64 ビットの Windows または Linux コンピューターに エッジ暗号化 プロキシをインストールします。

始める前に

必要なロール：管理者

インストーラーを実行するには、11.x バージョンシリーズの Java バージョン 11.0.6 以降が必要です。

このタスクについて

ターゲット マシンに適したコマンドを使用して、ネットワークのマシンに エッジ暗号化 プロキシサーバーをインストールします。エッジ暗号化 プロキシサーバーを Windows マシンにインストールする場合は、プロキシサーバーを Windows サービスとしてさらにインストールする必要があります。

Edge Encryption プロキシサーバーをアップグレードすると、現在のインストール ディレクトリー配下の backup.dist-upgrade-<タイムスタンプ> ディレクトリーに、古いプロキシのバックアップが格納されます。このバックアップ ディレクトリーはアップグレード プロセス中に生成されるもので、古いプロキシの情報が格納されます。

コマンド ラインからアップグレードを実行すると、コマンドを実行したディレクトリーに dist-upgrade.log が生成されることがあります。dist-upgrade.log には、アップグレード プロセスのログが記録されています。

アップグレードに失敗した場合は、failed-backup.dist-upgrade-<timestamp> というディレクトリーが作成されます。また、元のプロキシ ディレクトリーの logs/wrapper.log にも、失敗に関する情報が格納される場合があります。

手順

1. インストール ディレクトリーを作成します。
2. エッジ暗号化 プロキシのアーカイブ ファイルをインストール ディレクトリーにコピーします。
3. ターミナルを開き、インストール ディレクトリーに移動します。

> **注:**
> Windows マシンにインストールする場合は、Windows コマンド プロンプトを管理者権限で起動する必要があります。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

4. ターゲット マシンに対してコマンド `java -jar edgeencryption-<version>-all.jar -m install -n <ProxyName> --instancehost <host> -p <InstancePort> --protocol https` を実行し、設定に応じて変数を変更します。

オプション	変数	説明
なし	version	現在の操作の実行に使用している エッジ暗号化 プロキシのバージョン番号。
-m	mode	実行する操作またはモード (install or dist-upgrade)。
-n	ProxyName	暗号化プロキシ インスタンスの名前。特定のプロキシ インスタンスを識別できるように、一意の ProxyName を使用します。
--instancehost	host	ServiceNow インスタンスのホスト名 (たとえば、mycompany.service-now.com)。
-p	InstancePort	インスタンスのポート。プロトコルが https の場合、ポートは通常は 443 です。
--protocol	protocol	ServiceNow インスタンスへのアクセスに使用されるプロトコル (通常は https)。

注:
ブラウザからコマンドをコピー アンド ペーストしないでください。コピー/ペースト操作によって予期しない文字がターゲット マシンに貼り付けられ、コマンドが正しく実行されないことがあります。マニュアルを参考にして手動でコマンドを入力するようにしてください。

ヘルプ画面を表示するには、このコマンドを引数なしで実行します (`java -jar edgeencryption-<version>-all.jar`)。

5. Windows マシンにインストールする場合は、エッジ暗号化 プロキシを Windows サービスとしてインストールします。

   a. オプション: 新しいプロキシで conf/wrapper.conf ファイルを開き、次のテーブルのプロパティを設定して、サービスの名前を変更します。

プロパティ	説明
wrapper.ntservice.name	エッジ暗号化 プロキシ サービスの一意の名前。
wrapper.ntservice.displayname	エッジ暗号化 プロキシ サービスの表示名。
wrapper.ntservice.description (オプション)	プロキシサーバーの説明。

この手順を実行しない場合、エッジ暗号化 プロキシ サービスは **Edge Encryption** という名前でインストールされます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

b. ファイルを保存して閉じます。

c. Windows のコマンドプロンプトを開き、cd ServerName_port/bin を実行します。

d. edgeencryption.bat install を実行します。

タスクの結果

ProxyName_port ディレクトリーが現在のディレクトリーに作成されます。edgeencryption.properties ファイルが、コマンド ラインからのホスト、ポート、プロトコルの値に更新されます。

デジタル署名用の **RSA** キー ペアを作成して設定する

RSA キー ペアを作成します。プロキシサーバーはこれを使用してデジタル署名を作成し、暗号化のプロパティおよび設定への変更に対して署名を行うことができます。

始める前に

必要なロール：管理者

デジタル署名を生成および検証するには、RSA キー ペアを生成して JCEKS Java KeyStore に格納する必要があり、このキー ペアを使用するように各プロキシを設定する必要があります。暗号化キー ペアの生成には keytool コマンドを使用します。

SElinux (CentOS) にインストールされたプロキシで keytool ユーティリティを使用するには、プロキシの java-installation ディレクトリーから共有ライブラリーをロードできるようにする必要があります。それには、次のコマンドを root として実行します。

```
chcon -R -t texrel_shlib_t proxy_install_dir/java/jre /lib
```

Java 1.8 バージョンの keytool ユーティリティを使用する必要があります。ユーティリティのコピーは <プロキシのインストール ディレクトリー>java/jre/bin/keytool にあります。

手順

1. プロキシのダウンロード ディレクトリーの KeyStore ディレクトリーに移動します。
2. デフォルトのパスワードを変更します。

   デフォルトパスワードは *changeme* です。

   ```
   keytool -keystore keystore.jceks -storetype jceks -storepasswd -new <newpassword>
   ```

3. 暗号化キー ペアを作成します。

   注:
   keytool ユーティリティーでパスワードのプロンプトが表示されたときに、キーのパスワードを入力しないでください。

   次のコマンドを 1 行で入力します。

   ```
   keytool -genkeypair -alias <key alias> -keyalg rsa -keystore keystore.jceks
   -storetype jceks -storepass <keystore password> -keysize 2048
   ```

4. 暗号化プロキシのプロパティ ファイル (edgeencryption.properties) を更新します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

a. <インストール ディレクトリー>/conf/ ディレクトリーに移動します。

b. edgeencryption.properties ファイルを開きます。

c. デジタル署名のプロパティを入力します。

これらのプロパティはすべてのプロキシで同じにする必要があります。

5. edgeencryption.properties ファイルを保存して閉じます。

セキュア SSL 接続のための証明書をインポートして設定する

セキュア SSL 接続を使用するには、サーバー証明書をインポートして Java KeyStore に追加します。

始める前に

必要なロール：管理者

Java KeyStore に追加する前に、サーバー証明書および一致する秘密鍵を取得する必要があります。

手順

1. openssl コマンドを使用して証明書署名要求 (CSR) を生成します。

```
openssl req -newkey rsa:2048 -keyout PRIVATEKEY.key -out MYCSR.csr
```

2. CSR (上記の例では MYCSR.csr) を認証局に送信して署名してもらいます。

3. openssl コマンドを使用して、インポートのための P12 キーストアを作成します。

```
openssl pkcs12 -export -in MYSIGNEDCERT.pem -inkey PRIVATEKEY.key -name shared >
 MY_SERVER.p12
```

4. 証明書と秘密鍵を jceks ファイルに格納します。

```
keytool -importkeystore -destkeystore keystore.jceks -deststoretype jceks -srckeystore
 MY_SERVER.p12 -srcstoretype pkcs12 -alias MYALIAS
```

例で MYALIA として表示されているエイリアスは、任意の値にすることができます。このエイリアスは、<installation directory>/conf/ フォルダーにある edgeencryption.properties ファイルの edgeencryption.proxy.https.cert.alias プロパティで使用します。

5. Edge プロキシを停止して再起動します。

> **注:**
> 再起動中、プロキシサーバーは一時的にオフラインになります。その時間の長さは環境、およびプロキシ サービスの停止と再起動にかかる時間によって異なります。

キーストアと暗号化キーをセットアップする

エッジ暗号化 プロキシサーバーで使用されるキーストアと暗号化キーをセットアップします。

始める前に

必要なロール：security_admin

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

手順

1. 組織のニーズに応じて、使用する適切なタイプのキーストアを慎重に決定してください。

サポートされているキーストア	説明
ファイルストア	キーは、エッジ暗号化 プロキシサーバーからアクセスされるファイル システム内のファイルに格納されます。ファイルに格納された暗号化キーは暗号化されていないため、これらのファイルの保護についてはユーザーの責任になります。
Java KeyStore	Java KeyStore では次のようになります。 ○ キーは Java JCEKS KeyStore に格納されます。 ○ パスワードで保護されているため、ファイル システム内のファイルにキーを格納する方法よりも安全です。 ○ 複数のキーを格納できます。各キーをキー エイリアスで表すことで、複数のキーを簡単に管理できます。 エッジ暗号化 プロキシの keystore ディレクトリーには、keystore.jceks という名前の Java JCEKS KeyStore ファイルが付属しています。このキーストア ファイルには ServiceNow 公開キーが含まれています。この公開キーは、ServiceNow の署名が付いた暗号化ルールの検証に使用されます。
Enterprise Key Management (EKM)	**SafeNet KeySecure** キーは、SafeNet KeySecure のキー管理を使用して格納および取得されます。 Gemalto を使用してライセンスを確保し、ライブラリーをダウンロードし、ネットワーク内のホスト マシンに SafeNet KeySecure キーストアをインストールしてから、エッジ暗号化 プロキシサーバーでキーストアを設定する必要があります。 **Unbound Technology** base64 でエンコードされ、ラップされた暗号化キーは、テキストファイルとして エッジ暗号化 プロキシサーバーで保存されます。Unbound Technology の実装 (以前の Dyadic Security) は、ラッピングキーの制御を維持します。 エッジ暗号化 プロキシサーバーは、Unbound technology クライアントと同じマシンで実行する必要があります。

注:
ベース システムの Java JCEKS KeyStore 以外のキーストアを使用する場合は、ServiceNow 公開キーをキーストアにインポートする必要があります。公開キーの別名は *servicenow* です。

2. ローカル ネットワークでキーストアと暗号化キーをセットアップします。

Java KeyStore キーストアをセットアップする

Java KeyStore キーストアを使用して暗号化キーを格納できます。

始める前に
必要なロール：管理者

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Java 1.8 バージョンの keytool ユーティリティを使用する必要があります。ユーティリティのコピーは <プロキシのインストール ディレクトリー>/java/jre/bin/keytool にあります。

このタスクについて

エッジ暗号化 プロキシの keystore ディレクトリーには、keystore.jceks という名前の Java JCEKS KeyStore ファイルが付属しています。このキーストア ファイルには ServiceNow 公開キーが含まれています。この公開キーは、ServiceNow の署名が付いた暗号化ルールの検証に使用されます。

手順

1. キーストアのプロパティをセットアップします。
   a. <インストール ディレクトリー>/conf/ ディレクトリーに移動します。
   b. edgeencryption.properties ファイルを開きます。
   c. Java KeyStore のプロパティを入力します。
2. edgeencryption.properties ファイルを保存して閉じます。

次のタスク

Java KeyStore をセットアップした後、「Java KeyStore keytool を使用して暗号化キーを作成する」の手順を実行します。

Java KeyStore keytool を使用して暗号化キーを作成する

暗号化プロキシの配布に付属している keytool を使用して、AES 128 ビットおよび AES 256 ビットの暗号化キーを作成できます。

始める前に

必要なロール：管理者

Java 1.8 バージョンの keytool ユーティリティを使用する必要があります。ユーティリティのコピーは <プロキシのインストール ディレクトリー>/java/jre/bin/keytool にあります。

keytool ユーティリティの詳細については、Java SE のドキュメント を参照してください。

このタスクについて

注:
Java KeyStore では、エイリアス名 (キー名、キー エイリアス) で小文字と数字を使用する必要があります。

手順

1. キーストア ディレクトリー <インストール ディレクトリー>/keystore/ に移動します。
2. 暗号化キーを作成するには、次のいずれかのコマンドを実行します。

注:
キーストア ディレクトリー以外のディレクトリーからこれらのコマンドを実行する、つまり、前の手順をスキップする場合は、現在のディレクトリーからキーストア ディレクトリーへのパスを含めるように *-keystore* オプションを変更する必要があります。たとえば、現在 <インストールディレクトリー>\bin ディレクトリーにいる場合、オプションは `-keystore ../keystore/keystore.jceks` となります。

オプション	説明
AES 128	`keytool -genseckey -alias 128bitkey -keyalg aes -keysize 128 -keystore keystore.jceks -storetype jceks`

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

オプション	説明
AES 256	keytool -genseckey -alias 256bitkey -keyalg aes -keysize 256 -keystore keystore.jceks -storetype jceks

デフォルトキーを割り当てるときに、インスタンスでエイリアスを追加します。

注:
キーのパスワードはキーストアのパスワードと同じにする必要があります。

SafeNet KeySecure キーストアをセットアップする

SafeNet キーストアを使用している場合は、ライブラリ セットをプロキシ配布ディレクトリーにコピーします。

始める前に

必要なロール：管理者

この手順を実行する前に、SafeNet キーストアをインストールしてセットアップする必要があります。ライブラリをダウンロードするために Thales を使用してライセンスを確保します。

注:
IngianNAE バージョン 8.12 の場合は、commons-collections.jar ファイルもダウンロードする必要があります。

このタスクについて

注:
Linux では、ファイルパスにスラッシュ (/) を使用します。

手順

1. <インストール ディレクトリー>/conf/ ディレクトリーに移動し、edgeencryption.properties ファイルを開きます。
2. SafeNet キーストアのプロパティを入力します。

注:
ユーザー名/パスワード認証とクライアント証明書認証のどちらかを使用して SafeNet キーストアを設定することはできますが、両方を組み合わせることはできません。

Example

ユーザー名とパスワードの認証を使用する SafeNet キーストアの例

```
edgeencryption.nae.retries = 3
edgeencryption.nae.enabled = true
edgeencryption.nae.server = url
edgeencryption.nae.port = 9000
edgeencryption.nae.protocol = ssl
edgeencryption.nae.keystore.path = keystore/safenet_truststore
edgeencryption.nae.keystore.password = password
edgeencryption.nae.user = safenet_user
edgeencryption.nae.password = safenet_password
```

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Example

クライアント証明書の認証を使用する SafeNet キーストアの例。この認証方法では、プロパティファイルに SafeNet サーバーのユーザー名とパスワードを格納する必要がなくなります。

```
edgeencryption.nae.retries = 3
edgeencryption.nae.enabled = true
edgeencryption.nae.server = url
edgeencryption.nae.port = 9000
edgeencryption.nae.protocol = ssl
edgeencryption.nae.keystore.path = keystore/safenet_clientcert
edgeencryption.nae.keystore.password = password
edgeencryption.nae.client.certificate = cert_name
```

3. SafeNet キーストアにキーを追加または作成します。
   デフォルトキーを割り当てるときに、インスタンスでキー名 (エイリアス) を追加します。
4. edgeencryption.properties ファイルを保存して閉じます。

Kingston 以前から London 以降へのアップグレード

Edge でのキーストレージに SafeNet NAE サーバーを使用する場合は、プロキシを Kingston 以前から London 以降にアップグレードする前に、Gemalto SafeNet クライアントの ProtectApp JAR ファイルをコピーし、新しいプロパティを追加する必要があります。

始める前に
必要なロール：admin

このタスクについて

注:
Linux では、ファイルパスにスラッシュ (/) を使用します。

手順

1. 次のファイルを <installation directory>/lib から <installation directory>/nae ディレクトリーにコピーします。
   - commons-collections<version>.jar
   - ingrianlog4j-api-<version>.jar
   - ingrianlog4j-core-<version>.jar
   - ingrianNAE-<version>.jar
2. プロキシの現在のバージョン (未アップグレード) で、<installation directory>/conf/edgeencryption.properties ファイルに次の 2 つのプロパティを追加して更新します。
   - *edgeencryption.ekm.provider.classname* = com.snc.edgeencryption.encryption.CloudEdgeNaeKeyProvider
   - *edgeencryption.thirdparty.vendor.library.path* = <手順 1 の JAR ファイルをコピーしたディレクトリへのディレクトリパス>

     注:
     Java 11 の *edgeencryption.thirdparty.vendor.library.path*
3. 変更内容を保存します。
4. London 以降へのアップグレードを続行します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Unbound Technology のキーのセットアップ

エッジ暗号化 で Unbound Technology (旧 Dyadic Security) のキーを使用するには、base64 エンコードされ、ラップされた暗号化キーをテキストファイルとして エッジ暗号化 プロキシサーバーに格納し、ラッピングキーエイリアスを指定します。Unbound Technology の実装によって、ラッピングキーのコントロールが維持されます。

始める前に
必要なロール：security_admin

Unbound Technology の実装で、ラッピング キーとラップされたキーの両方を識別します。ラッピングとパディングには RSA/ECB/OAEPWITHSHA-256ANDMGF1PADDING アルゴリズムを使用します。ラップされたキーを、base64 エンコードされたテキスト形式でエクスポートします。キー エイリアスを使用し、ファイル拡張子のない名前としてファイルを保存します。

> **注:**
> Unbound Technology 暗号化キーを エッジ暗号化 とともに使用する場合、Unbound クライアント マシンでコマンドライン インストーラを使用してプロキシサーバーをインストールします。エッジ暗号化 プロキシサーバーは、Unbound テクノロジ クライアントと同じマシンで実行する必要があります。

手順

1. ラップされた暗号化キーを、base64 エンコードされたテキスト形式で <プロキシのインストール ディレクトリー>/keys ディレクトリーに追加します。
   ファイルの名前は、ファイル拡張子のないキー エイリアスにする必要があります。
2. edgeencryption.properties ファイルを更新します。
   a. <プロキシのインストール ディレクトリー>/conf ディレクトリーに移動します。
   b. edgeencryption.properties ファイルを開きます。
   c. ファイルストアのプロパティを入力します。*edgeencryption.keyfile.directory* の値を keys に設定します。

      このプロパティの指示によって、プロキシサーバーは <Java ホーム ディレクトリー>/keys ディレクトリーで暗号化キーを探します。

      エッジ暗号化 のプロパティの詳細については、「Edge Encryption プロキシサーバーのプロパティ」を参照してください。
   d. Dyadic プロバイダー設定のプロパティをコメント解除し、*edgeencryption.ekm.provider.rsa.wrapping.key.alias* の値を Unbound 実装のラッピングキーエイリアスに設定します。
   e. ファイルを保存して閉じます。

次のタスク
暗号化キー エイリアスをインスタンスに追加します。暗号化キーエイリアスは、<プロキシインストールディレクトリ>/keys ディレクトリに追加されているラップされた暗号化キーのファイル名です。たとえば、ディレクトリ内のファイルの名前が myunboundkey の場合、この名前を [キーエイリアス] フィールドに追加します。「インスタンスで暗号化キーを設定する」を参照してください。

ファイルに格納する暗号化キーを作成する

シンプルなテキスト ファイルをキーストアとして使用できます。ファイルごとに 1 つずつ暗号化キーを保持します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

始める前に
必要なロール：管理者

このタスクについて
この手順では、キー ストレージと暗号化キーの両方が作成されます。

注:
キー ファイルの名前は、インスタンス内の暗号化キー テーブルで指定されたキー エイリアスに合わせる必要があります。「インスタンスで暗号化キーを設定する」を参照してください。

手順

1. プロキシサーバーのインストール ディレクトリーの /keys フォルダーにファイルを作成します。
2. 暗号化キーをファイルに追加します。

オプション	説明
AES 128	ファイルに暗号化キー (正確な 16 バイト) を配置します。
AES 256	ファイルに暗号化キー (正確な 32 バイト) を配置します。

3. edgeencryption.properties ファイルを更新します。
   a. <インストール ディレクトリー>/conf/ ディレクトリーに移動します。
   b. edgeencryption.properties ファイルを開きます。
   c. ファイルストアのプロパティを入力します。
   d. ファイルを保存して閉じます。

インスタンスで暗号化キーを設定する

エッジ暗号化 では、プロキシをオフラインにせずに暗号化キーを管理するためのツールが提供されています。

始める前に
必要なロール：security_admin

インスタンスで新しい暗号化キーをセットアップする前に、次の手順を実行します。

1. 暗号化キーを作成します。
2. すべての暗号化プロキシで新しいキーを使用できるようにします。各プロキシにファイルまたは Java KeyStore ファイルをコピーします。または、各プロキシから Java KeyStore または Enterprise Key Management (EKM) デバイスにアクセスできることを確認します。

このタスクについて
キー エイリアスは一意である必要があります。キー エイリアスはそれぞれ、各プロキシで同じキーのサイズとタイプにする必要があります。そうしないと、キーをデフォルトとして割り当てることはできません。

手順

1. 移動先 すべて > エッジ暗号化の設定 > 暗号化キーの設定 > キーの設定.
2. フォームの [新しいキーの追加] セクションで、次の手順を実行して新しいキーを追加します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

> **重要:**
> SafeNet でバージョニングされたキーを使用している場合は、[キーバージョン] 用の追加の列が表示されます。[キーバージョン] は編集できません。関連リンクで [最新のキーバージョンを取得] リンクをクリックして、Edge プロキシから各キーの最新バージョンを取得します。

リストで左側の列に **X** 印のある行を削除することができます。以前にデフォルトとして使用されたキー、または [ステータス] が [利用可能] のキーは、削除できません。

a. [新規行を挿入] という行をダブルクリックします。

b. 編集ボックスで、キーの名前を入力し、チェックマークをクリックします。

キー エイリアスは小文字と数字です。[更新] をクリックすると大文字が小文字に変わります。キー エイリアスは一意である必要があります。

> **注:**
> Unbound Technology のキーを使用している場合は、暗号化キー エイリアスを追加します。 暗号化キーエイリアスは、<プロキシインストールディレクトリ>/keys ディレクトリに追加されているラップされた暗号化キーのファイル名です。たとえば、ディレクトリ内のファイルの名前が myunboundkey の場合、この名前を [キーエイリアス] フィールドに追加します。

c. 同じ行で、[キー サイズ] 列をダブルクリックします。

d. 選択ボックスで、キー サイズとして **[128** ビット] または **[256** ビット] を選択し、チェックマークをクリックします。

e. 同じ行で、[タイプ] 列をダブルクリックします。

f. 選択ボックスで、キー タイプとして [ファイル]、[キーストア]、**[SafeNet]**、または **[Unbound]** を選択し、チェック マークをクリックします。

g. キーの追加を終えたら、[次の手順] をクリックします。
次に進む前に、各キーのエイリアス、キー サイズ、およびキー タイプを指定する必要があります。

3. フォームの [キーのステータス] セクションで、キーの [ステータス] を確認し、[利用可能] であることを確認します。

4. キーが [利用可能] な場合は、[次の手順] をクリックします。
これには数分かかる場合があります。

> **注:**
> SafeNet でバージョニングされたキーを使用している場合は、[キーバージョン] 用の追加の列が表示されます。[キーバージョン] は編集できません。

インスタンスでは、どのプロキシでも利用可能なすべての暗号化キーのステータスが追跡されます。すべてのプロキシでキーが使用可能になると、そのステータスが [利用可能] になります。数分経ってもステータスが変わらない場合は、キーがすべてのプロキシで利用可能かどうかを確認してください。ステータスが [利用不可] のままである場合は、1 つ以上のプロキシにキーがありません。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

暗号化キーのステータス

ステータス	説明
利用可能	すべてのオンライン プロキシにキーがあります。
利用不可	これは新しいキーであり、プロキシがまだキーをロードしていないか、少なくとも 1 つのプロキシがキーをロードできませんでした。

5. フォームの [デフォルトキーの変更] セクションで、次のいずれかの操作を行います。
   - キー エイリアスを入力します。
   - 虫眼鏡アイコンをクリックし、エイリアスを選択します。

   注:
   SafeNet でバージョニングされたキーを使用している場合は、[キーバージョン] 用の追加のフィールドが表示されます。[キーバージョン]はグレー表示され、編集することはできません。最新のキーバージョンのみを選択してください。以前のバージョンを選択した場合は、[更新] または [次のステップ] をクリックすると、次のメッセージが表示されます。

   > One of the default keys chosen is not the latest version available for the key. Please use the latest version.

   デフォルトのキーが SafeNet キーの最新バージョンでない場合は、関連リンクに [デフォルトキーを最新バージョンに更新] リンクが表示されます。このリンクをクリックして、最新バージョンを使用するようにデフォルトキーを更新してください。

6. フォームの [キー ローテーションのスケジュール] セクションで、新しい暗号化キーを使用して既存のデータを暗号化するように、一括キー ローテーション ジョブまたは単一キー ローテーション ジョブをスケジュールします。

   一括キー ローテーション ジョブまたは単一キー ローテーションジョブを実行しないと、データに再度アクセスするまで、既存のデータは古いキーで暗号化されたままになります。

Edge Encryption プロパティ ファイルでその他のプロパティを設定する

ネットワークに エッジ暗号化 プロキシサーバーをインストールしてキーストアとキーをセットアップしたら、エッジ暗号化 のその他のプロパティを設定します。

始める前に
必要なロール：管理者

手順

1. <インストールディレクトリー>/conf/edgeencryption.properties ファイルを開き、次の エッジ暗号化 プロキシサーバープロパティを設定します。
   - ターゲット (インスタンス) のプロパティ
   - ユーザー アカウントのプロパティ
   - プロキシのプロパティ

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

- 順序保存の暗号化タイプまたは暗号化パターンを使用する場合は、プロキシデータベースのプロパティを設定します。
- クリアー テキストおよび静的 IV のプロパティ

2. ファイルを保存して閉じます。

Web プロキシを設定する

ネットワークで Web プロキシを使用している場合は、Web プロキシを使用するように エッジ暗号化 プロキシをセットアップできます。

始める前に
必要なロール：管理者

このタスクについて
ネットワークで Web プロキシを使用していない場合は、設定ファイルで Web プロキシ プロパティをコメント アウトしたままにしておきます。

エッジ暗号化 プロキシサーバーは、Web プロキシへの HTTP 接続と、Web プロキシによる基本認証をサポートしています。

手順

1. <インストール ディレクトリー>/conf/ ディレクトリーに移動します。
2. edgeencryption.properties ファイルを開きます。
3. Web プロキシ プロパティを設定します。
4. edgeencryption.properties ファイルを保存して閉じます。
5. Web プロキシで顧客固有のサーバー証明書を使用している場合は、 エッジ暗号化 プロキシサーバーで使用される JVM にその証明書を追加して、Web プロキシと エッジ暗号化 プロキシサーバー間の信頼を確立します。
   a. cd コマンドを使用して、<Java home directory>/jre/lib/security/cacerts に移動します。
   b. コマンド keytool -keystore cacerts -importcert -alias <chooseAlias> -file <certificateFile> を実行します。

プロキシサーバーの初期メモリ制限と上限メモリ制限を設定する

初期メモリ制限と上限メモリ制限を設定して、プロキシサーバーが利用できるメモリ量を指定します。これらの制限を設定することで、エッジ暗号化 の実装でパフォーマンスの問題が回避されます。

始める前に
必要なロール：管理者

このタスクについて
原則として、初期メモリ制限と上限メモリ制限の両方を同じ値に設定してください。どのマシンでも、2 GB の物理メモリをオペレーティング システム (OS) に割り当てます。次に、初期メモリ制限プロパティと上限メモリ制限プロパティを使用して、残りの物理メモリをヒープに割り当てます。たとえば、8 GB のメモリを搭載したマシンでは、OS に 2 GB を割り当て、残りの 6 GB (6144 メガバイト) を初期および上限のメモリに割り当てます。

重要:
エッジ暗号化 プロキシサーバーが実行中の場合は、これらのプロパティを更新した後にプロキシサーバーを停止して再起動する必要があります。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. プロキシサーバーのディレクトリーで、<インストール ディレクトリー>/conf/wrapper.conf を開きます。
2. 初期メモリ制限を設定するには、ファイルの最後に次の行を追加します。

```
wrapper.java.additional.<number>=-Xms<min_memory_in_MB>m
```

<数字> を、wrapper.conf ファイルで定義されている wrapper.java.additional.<数字> プロパティのシーケンスで次に利用可能な <数字> に設定します。

Example
たとえば、次に示す wrapper.java.additional.<数字> プロパティのリストがあるとします。

```
wrapper.java.additional.1=
wrapper.java.additional.2=
```

このリストの最大の <数字> は **2** です。wrapper.java.additional.<数字>=-Xms<min_memory_in_MB>m 行を追加するときは、<数字> を次に利用可能な数字である **3** に設定します。

重要:
番号のシーケンスにはギャップを残さないでください。

<min_memory_in_MB> を、2 GB のメモリを OS に割り当てた後に残っているメモリのメガバイト数に設定します。

3. 上限メモリ制限を設定します。
上限メモリ制限はベース システムで設定されていないため、プロキシサーバーは利用可能なすべてのメモリを使用できます。他のサービスがサーバー上で実行されている場合は、上限メモリ制限を設定することもできます。

ファイルの最後に次の行を追加します。

wrapper.java.additional.<数字>=-Xmx<max_memory_in_MB>m

<数字> を、wrapper.conf ファイルで定義されている wrapper.java.additional.<数字> プロパティのシーケンスで次に利用可能な <数字> に設定します。

Example
たとえば、次に示す wrapper.java.additional.<数字> プロパティのリストがあるとします。

```
wrapper.java.additional.1=
wrapper.java.additional.2=
```

このリストの最大の <数字> は **2** です。wrapper.java.additional.<number>=-Xmx<max_memory_in_MB>m 行を追加するときは、<数字> を次に利用可能な数字である **3** に設定します。

注:
番号のシーケンスにはギャップを残さないでください。

<max_memory_in_MB> を、2 GB のメモリを OS に割り当てた後に残っているメモリのメガバイト数に設定します。

4. ファイルを保存して閉じます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Example: 例：プロキシサーバーの初期および上限のメモリ制限を設定する

```
wrapper.java.additional.1 = -Djava.io.tmpdir=../tmp
wrapper.java.additional.2 = -Dcloudedge.home.dist=..
# must ensure UTF8 encoding when running on Windows
wrapper.java.additional.3 = -Dfile.encoding=UTF8
# additional properties for heap settings
wrapper.java.additional.4 = -Xms6144m
wrapper.java.additional.5 = -Xmx6144m
```

次のタスク
Edge Encryption プロキシを起動する。

Edge Encryption プロキシを起動する

エッジ暗号化 プロキシのインストールと設定を終えたら、コマンド ラインからプロキシを起動できます。

始める前に
必要なロール：管理者

暗号化プロキシを起動する前に、次のことを確認してください。

- エッジ暗号化 プラグインがインスタンスで有効になっている。
- このマシンの edgeencryption.properties ファイルがすでに設定されている。
- 順序保存の暗号化タイプまたは暗号化パターンを使用する場合は、プロキシ データベースが実行されている。

> **注:**
> 初めて edgeencryption.properties ファイルをセットアップするとき、またはプロパティを変更するときに、パスワードの暗号化プロパティの設定を望まない場合があります。すべてが正常に機能していることを確認したら、パスワードの暗号化プロパティを設定し、プロキシをシャット ダウンしてから、プロキシを再起動することができます。

手順

1. プロキシサーバーを実行します。

オプション	説明
Linux マシン	**a.** cd ServerName_port を実行します。 **b.** ./startup.sh を実行します。
Windows マシン	コマンド ラインから admin として次の手順を実行します。 **a.** cd ServerName_port/bin を実行します。 **b.** edgeencryption.bat start を実行します。

2. プロキシサーバーのログを調べて、プロキシが実行されていることを確認します。

プロパティファイルでのパスワードの難読化

edgeencryption.properties ファイルでパスワードを難読化して、クリアテキストのパスワードを公開せずにプロパティファイルを共有することができます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

始める前に
必要なロール：管理者

このプロパティを設定する前に、エッジ暗号化 プロキシサーバーがセットアップされていて正常に実行されていることを確認してください。このプロパティを設定する前に、「Edge Encryption プロキシを停止する」の手順を実行してください。

このタスクについて
このプロパティを設定すると、最初の起動時に接続やアクセスの問題が発生した場合に、それらのデバッグが困難になることがあります。プロキシを正常にセットアップして、テストに成功した後でのみ、本番環境でこのプロパティを設定してください。

手順

1. <インストール ディレクトリー>/conf/ ディレクトリーに移動します。
2. conf ディレクトリーで、パスフレーズとして使用できる複雑な文字列またはフレーズを含むテキスト ファイルを作成します。プロキシはこのファイルを使用して、edgeencryption.properties ファイルのパスワードを難読化します。
   パスフレーズは、パスワード自体と関係のないランダムかつ複雑なフレーズにしてください。
3. edgeencryption.properties ファイルを開きます。
4. パスワードの暗号化プロパティを設定します。
5. edgeencryption.properties ファイルを保存して閉じます。

次のタスク
このプロパティを設定した後に、「Edge Encryption プロキシを起動する」の手順を実行できます。

プロキシの手動追加

最初の エッジ暗号化 プロキシを正しく設定してテストを終えたら、Linux または Windows マシンで追加のプロキシをセットアップできます。複数のプロキシを同じマシンにインストールすることはお勧めしません。

始める前に
必要なロール：管理者

このタスクについて
追加したマシンにさらにプロキシサーバーを追加して、最適な環境を確保します。必要な追加のプロキシ数の決定については、「Edge Encryption 環境のサイジング」を参照してください。

> **注:**
> 必ずすべてのプロキシに同じ暗号キーと同じ RSA キー ペアを持たせてください。これらは、暗号化設定と暗号化ルールへのデジタル署名に使用されます。プロキシ データベースをインストールの一部としてセットアップする場合、すべてのプロキシで同じプロキシ データベースを使用する必要があります。

手順

1. 適切なコマンドを使用してプロキシをインストールします。
   詳細については、「エッジ暗号化 プロキシサーバーをインストールする (インタラクティブ インストーラー)」を参照してください。
2. すべての暗号化キーと edgeencryption.properties ファイルを最初のプロキシから新しいプロキシにコピーします。
   暗号化キーは、プロキシのキーストア、/keys ディレクトリー、または SafeNet KeySecure キーストアにあります。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

3. 新しいプロキシで edgeencryption.properties ファイルを開きます。
4. 次のプロパティを変更します。

プロパティ	説明
edgeencryption.proxy.name	プロキシサーバーの一意の名前。
edgeencryption.proxy.host	プロキシを実行しているコンピューターのサーバー名、IP アドレス、または完全修飾ドメイン名。
edgeencryption.proxy.http.port	HTTP 通信のプロキシのポート。マシン上のすべてのプロセス全体で一意である必要があります。
edgeencryption.proxy.https.port	HTTPS 通信のプロキシのポート。マシン上のプロセス全体で一意である必要があります。

5. Windows マシンにプロキシサーバーをインストールする場合は、新しいプロキシで conf/wrapper.conf ファイルを開き、次の表に示すプロパティを追加することで、サービスの名前を変更する必要があります。

   注:
   この手順は、プロキシサーバーを起動する前に実行する必要があります。

プロパティ	説明
wrapper.ntservice.name	エッジ暗号化 プロキシ サービスの一意の名前。
wrapper.ntservice.displayname	エッジ暗号化 プロキシ サービスの表示名。
wrapper.ntservice.description (オプション)	プロキシサーバーの説明。

6. ファイルを保存して閉じます。
7. 適切なコマンドを使用してプロキシを起動します。
   詳細については、「Edge Encryption プロキシを起動する」を参照してください。

エッジ暗号化 プロキシサーバーを認証する

エッジ暗号化 がプロキシサーバーからの要求を処理できるよう、プロキシサーバーが信頼できるソースであることを指定します。

始める前に
プロキシサーバーが認証されていない場合は、次のメッセージがコンソールログに含まれています。

```
WARN This Edge Encryption proxy has not yet been authenticated by the instance.
Please navigate to the matching Proxy record on your ServiceNow instance and authenticate it.
```

このプロキシにアクセスしようとすると、「This site can't be reached」というメッセージが表示されます。

アップグレードプロセス中にプロキシの運用ステータスを維持するために、プロキシ更新が成功するまで認証は必要ありません。

必要なロール：管理者

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

手順

1. 移動先 すべて > エッジ暗号化の設定 > プロキシ.
2. プロキシを選択し、[認証] をクリックします。

タスクの結果
プロキシが [未認証] から [処理待ち]、[認証済み] へと移動します。認証を開始すると、ステータスが [未認証] から [処理待ち] に変化します。認証が完了すると、ステータスが [処理待ち] から [認証済み] に変化してプロキシにアクセスできるようになり、エッジ暗号化 はプロキシからの要求を受け入れられるようになります。

注:
プロキシを停止して再起動する場合、プロキシは [認証済み] のままになり、正常に再起動します。

Edge Encryption プロキシを停止する

コマンド ラインから エッジ暗号化 プロキシを停止できます。

始める前に
必要なロール：管理者

手順

1. プロキシサーバーを停止します。

オプション	説明
Linux マシン	./shutdown.sh を実行します。
Windows マシン	edgeencryption.bat stop を実行します。 Windows サービスを削除するには、edgeencryption.bat remove を実行します。

2. プロキシサーバーのログを調べて、プロキシが停止したことを確認します。

Linux で Edge Encryption プロキシをアンインストールする

エッジ暗号化 プロキシをアンインストールすることができます。プロキシをアップグレードする場合、現在のバージョンをシャット ダウンしてアンインストールする必要はありません。

始める前に
必要なロール：管理者

エッジ暗号化 プロキシを実行しているコンピューターにアクセスできる必要があります。

このタスクについて
エッジ暗号化 プロキシをシャット ダウンする前に、プロキシを使用してインスタンスに接続しているユーザーがいないことを確認します。

Linux 上で実行される暗号化プロキシは、単一のプロセスとして動作します。暗号化プロキシを別のホスト マシンに再展開する、プロキシのバージョンを更新する、Java のバージョンを更新する、暗号化プロキシを複数のプロキシサーバーに展開するときに暗号化プロキシの一意の名前を変更する、などの作業を実行する際に、このプロセスを終了できます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. edgeencryption.properties ファイルを保存してから配布ディレクトリーを削除することもできます。
2. shutdown.sh シェル スクリプトを実行します。
3. プロキシサーバーのログを調べて、プロキシサーバーがシャット ダウンされたことを確認します。
4. 配布フォルダー内のファイルを削除します。

Windows で Edge Encryption プロキシをアンインストールする

エッジ暗号化 プロキシをアンインストールすることができます。プロキシをアップグレードする場合、現在のバージョンをシャット ダウンしてアンインストールする必要はありません。

始める前に
必要なロール：管理者

エッジ暗号化 プロキシを実行しているコンピューターにアクセスできる必要があります。

エッジ暗号化 プロキシをシャット ダウンする前に、プロキシを使用してインスタンスに接続しているユーザーがいないことを確認します。

手順

1. edgeencryption.properties ファイルを保存してから配布ディレクトリーを削除することもできます。
2. edgeencryption.bat stop を実行します。
3. edgeencryption.bat remove を実行します。
4. プロキシサーバーのログを調べて、プロキシサーバーがシャット ダウンされたことを確認します。
5. 配布フォルダー内のファイルを削除します。

エッジ暗号化 でのマルチプロバイダー SSO のセットアップ

マルチプロバイダー SSO をセットアップして、エッジ暗号化 プロキシサーバーの URL またはインスタンスの URL を経由するログインを有効にします。エッジ暗号化 を有効にした状態でマルチプロバイダーの Single Sign-on (SSO) を実装する場合、一部のユーザーは エッジ暗号化 プロキシサーバーを経由してインスタンスにログインする必要がありますが、他のユーザーはその必要はありません。

始める前に

- Integration - Multiple Provider Single Sign-On Installer プラグイン (com.snc.integration.sso.msoi.installer) を有効にします。
- エッジ暗号化 プラグイン (com.glide.edgeencryption) を有効にし、1 つまたは複数のプロキシサーバーがネットワークにセットアップされていることを確認します。
- ユーザーがマルチプロバイダー SSO を使用してログインする際に経由する エッジ暗号化 プロキシサーバーの URL を決定します。エッジ暗号化 プロキシサーバーの URL を決定するには、「Edge Encryption のインストール」を参照してください。

必要なロール：admin

このタスクについて
ログインするユーザーは、Edge プロキシを使用するかどうかにかかわらず、適切な URL を使用してログインする必要があります。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

- すべてのユーザーを エッジ暗号化 プロキシサーバー経由でルーティングする場合は、ID プロバイダー レコードをセットアップし、**[ServiceNow** ホームページ]、[エンティティ ID/発行者]、[対象者 **URI]** の各フィールドでプロキシサーバー URL を定義します。
- 一部のユーザーをプロキシサーバー経由でルーティングし、他のユーザーをインスタンスにルーティングするには、2 つの ID プロバイダー レコードを作成します。どちらのレコードについても **[ID** プロバイダー **URL]** フィールドで同じ値を使用します。ただし、レコードの一方はプロキシサーバー経由でルーティングし、もう一方はインスタンスにルーティングします。
  - インスタンス名を介したログイン：Edge 以外のプロキシ用 IdP レコードの https://<インスタンス名>.service-now.com/login_with_sso.do?glide_sso_id=<sys_id
  - Edge プロキシを介したログイン：Edge プロキシ用 IdP レコードのhttps://<edge ホスト名>:<ポート>/login_with_sso.do?glide_sso_id=<sys_id

手順

1. ID プロバイダー レコードで ID プロバイダー URL の重複を有効にします。
   一意性の制約により、2 つの異なる ID プロバイダー レコードでの ID プロバイダー URL の重複は防止されています。フィールドを False に設定することで、複数の ID プロバイダー レコードで ID プロバイダ URL の重複を有効にすることができます。
   a. 移動先 システム定義 > ディクショナリ.
   b. ID プロバイダー テーブル [saml2_update1_properties] にある **[idp]** フィールドの定義レコードを開きます。
   c. [一意] フィールドを追加するようにフォームを設定します。
   d. [一意] フィールドの値が **False** に設定されていることを確認します。
2. 移動先 マルチプロバイダー **SSO** > **ID** プロバイダー.
3. 同じ ID プロバイダーに対して 2 つの ID プロバイダー レコードを作成します。一方ではインスタンスの URL を使用し、もう一方では エッジ暗号化 プロキシサーバーの URL を使用します。
   ID プロバイダーレコードを作成するには、「外部 ID プロバイダーの作成」を参照してください。

   a. エッジ暗号化 プロキシサーバーの URL については、次の値をフォームに入力します。

フィールド	値
ID プロバイダー URL	IdP メタデータからインポートします。
ServiceNow のホームページ	プロキシサーバーのホームページの URL。例：https://<プロキシのホスト名>:<ポート>/navpage.do
エンティティ ID/発行者	https://<プロキシのホスト名>:<ポート>
対象者 URI	https://<プロキシのホスト名>:<ポート>

   b. [送信] をクリックします。

   c. インスタンスの URL については、次の値をフォームに入力します。

フィールド	値
ID プロバイダー URL	IdP メタデータからインポートします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	値
ServiceNow のホームページ	https://<インスタンス>.service-now.com/navpage.do
エンティティ ID/発行者	https://<インスタンス>.service-now.com/navpage.do
対象者 URI	https://<インスタンス>.service-now.com/navpage.do

d. [送信] をクリックします。

4. オプション: 複数の ID プロバイダーを使用する場合は、MultiSSO インストレーション イグジットを変更します。

a. 移動先 システム定義 > インストレーションイグジット.
インストレーション イグジットの現在のリストが表示されます。

b. MultiSSO インストレーション イグジットを開きます。

c. [スクリプト] フィールドで次のステートメントを探します。

```
var samlResponseTxt = request.getParameter("SAMLResponse");
if (!GlideSession.get().isLoggedIn() && GlideStringUtil.notNil(samlResponseTxt)) {
    var idpRecord = this.getIdPRecord(request);
    if (idpRecord) {
        SSO_Helper.debug("IdP found based on SAML response: " +
 idpRecord.getUniqueValue());
        return new SSO_Helper(idpRecord.getUniqueValue(), false, null, true);
    }
}
```

d. このステートメントを次のコードに置き換えます。

```
var samlResponseTxt = request.getParameter("SAMLResponse");
if (!GlideSession.get().isLoggedIn() && GlideStringUtil.notNil(samlResponseTxt)) {
   /* // You have two profiles that use the same IdP entity id it cannot use
   // the IdP issuer / entity id from the response otherwise it may result in the
   // wrong IdP profile. IdP initiated login will not work
   var idpRecord = this.getIdPRecord(request);
   if (idpRecord) {
      SSO_Helper.debug("IdP found based on SAML response: " +
 idpRecord.getUniqueValue());
      return new SSO_Helper(idpRecord.getUniqueValue(), false, null, true);
      }*/
   return new SSO_Helper(null, true);
   }
```

注:
この設定では IdP により開始されるログインは機能しません。

e. [更新] をクリックします。

5. オプション: 複数の会社を使用している場合は、ユーザーをマルチプロバイダー SSO 用に構成し、ユーザーに応じて ID プロバイダーレコードの sys_id を更新します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

(Optional) 詳細については、「マルチプロバイダー SSO のユーザーの構成」を参照してください。

- ユーザーが エッジ暗号化 プロキシサーバー経由でログインするように設定するには、エッジ暗号化 プロキシサーバー URL を使用している ID プロバイダー レコードの sys_id を使用します。
- ユーザーがインスタンスにログインするように設定するには、インスタンス URL を使用している ID プロバイダー レコードの sys_id を使用します。

ログイン **URL**

URL	ログイン先
https://<プロキシのホスト名>:<ポート>/login_with_sso.do?glide_sso_id=<プロキシサーバー URL の IdP レコードの sys_id>	プロキシサーバー経由でログインします。
https://<インスタンス名>.service-now.com/login_with_sso.do?glide_sso_id=<インスタンス URL の IdP レコードの sys_id>	インスタンス経由でログインします。

Edge Encryption プロキシサーバーのプロパティ

<インストール ディレクトリー>/conf/ フォルダーにある edgeencryption.properties 設定ファイルには、環境設定に使用するプロパティが含まれています。

プロキシサーバーのプロパティを変更した後は、プロキシサーバーを再起動する必要があります。

クリアー テキストおよび静的 **IV** のプロパティ

edgeencryption.customer.assigned.known.cleartext	すべてのプロキシで同じキーを使用していることをインスタンスに検証させるためのクリアー テキスト。起動時に、プロキシはクリアー テキストを暗号化し、暗号化したテキストをインスタンスに送信します。インスタンス側はクリアー テキストを知らず、キーがインスタンスに送信されることもありません。このプロパティはすべてのプロキシで同じにする必要があります。
edgeencryption.encrypter.static.iv	等価性保存および順序保存の暗号化で使用される静的 IV (初期化ベクトル)。このプロパティはすべてのプロキシで同じである必要があり、正確に 16 バイト (16 文字の ASCII 文字) である必要があります。

デジタル署名のプロパティ

edgeencryption.proxy.signature.keystore.path	パスと Java KeyStore のファイル名。
edgeencryption.proxy.signature.keystore.password	パスワード。デフォルトのパスワードは <changeme> です。Java KeyStore のインストール後にパスワードを変更します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

edgeencryption.proxy.signature.keystore.keyalias	RSA キーペアが生成されるときに -alias 引数として与えられるキーエイリアス。

ファイルストアのプロパティ

edgeencryption.keyfile.directory	このディレクトリは、キー ファイルが格納される場所を指定します。Java KeyStore または SafeNet KeySecure キーストアを使用している場合は、このプロパティをコメント アウトしたままにしておきます。 例： `edgeencryption.keyfile.directory=keys` Unbound Technology のキーを使用している場合は、このプロパティをコメント解除し、値としてキーのディレクトリを設定します。

全般的な設定のプロパティ

edgeencryption.config.poll.interval	ポーリング間隔 (秒単位)。デフォルト設定では、プロキシが暗号化設定の変更を認識するまでに 5 秒かかります。値を大きくするほど、インスタンスがオフラインのプロキシを検出するのに時間がかかります。 **⚠ 警告:** このプロパティは変更しないでください。プロキシ ポーリング間隔のデフォルト設定を変更すると、プロキシがオンラインになったときに検出が遅れることがあります。
edgeencryption.rules.dir	プロキシで暗号化ルールが格納されるフォルダ。
edgeencryption.encryption.order_preserving.cache.enable	順序保存の暗号化タイプをサポートするためにキャッシュを使用するかどうかを決定する設定。
edgeencryption.encryption.order_preserving.cache.size	最大キャッシュ サイズ (バイト単位)。
edgeencryption.jobs.concurrency	このプロキシで同時に実行できる一括暗号化ジョブの最大数。
edgeencryption.jobs.requests_per_second	このプロキシからインスタンスに送信できる 1 秒あたりの HTTP ジョブ要求の数。
edgeencryption.attachments.request.timeout.seconds	添付ファイルのアップロード要求のタイム アウト (秒単位)。
edgeencryption.request.buffer.size	暗号化要求のサイズ。暗号化要求がこのサイズより大きい場合、超過分はディスクに保存されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

	⚠ 警告: このプロパティは変更しないでください。
edgeencryption.httpclient.request.buffer.size	クライアント要求のサイズ。クライアント要求がこのサイズより大きい場合、超過分はディスクに保存されます。 ⚠ 警告: このプロパティは変更しないでください。
edgeencryption.httpclient.header.size	要求/応答ヘッダーのサイズ。 • 最小値：8K • 最大値：32K ⚠ 警告: このプロパティは変更しないでください。
edgeencryption.proxy.idle.timeout	トランザクションがタイム アウトになるまでの時間 (秒単位)。 デフォルト値：300 (秒)
edgeencryption.proxy.keepalive.interval	プロキシからインスタンスに発行される ping の間隔 (秒単位)。プロキシとインスタンス間の接続を確認するために、定期的に ping が発行されます。 • デフォルト値：10 (秒) • 最小値：5 (秒)
edgeencryption.register.retry.count	登録を試みるためにプロキシからインスタンスに対して ping を実行する最大回数。 デフォルト値：0 (無制限)
edgeencryption.tokenization.exclusion.list	暗号化パターンは、これらのフィールドにある文字列をトークン化できません。

Java KeyStore のプロパティ

edgeencryption.keystore.path	Java KeyStore へのパス。ファイルストアまたは SafeNet KeySecure キーストアを使用している場合は、このプロパティをコメントアウトしたままにしておきます。 例： `edgeencryption.keystore.path = keystore/keystore.jceks`
edgeencryption.keystore.password	プロキシが Java KeyStore への接続に使用するパスワード。ファイルストアまたは SafeNet KeySecure キーストアを使用している場合は、

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

	このプロパティをコメントアウトしたままにしておきます。

ログ記録のプロパティ

ログ記録のプロパティは、<installation directory>/conf/ ディレクトリの log4gj2.properties ファイルにあります。これらのプロパティは、トラブルシューティングのため、または ServiceNow サポートから指示された場合にのみ変更され ます。詳細については 、「Edge Encryption プロキシのデバッグログを増やす方法」を参照してください。

NAE デバイスキーストアのプロパティ

edgeencryption.nae.retries	再試行回数。
edgeencryption.nae.enabled	NAE デバイスが使用可能かどうかを示す設定。
edgeencryption.nae.server	NAE サーバーの名前。
edgeencryption.nae.port	NAE サーバーによって使用されるポート。
edgeencryption.nae.protocol	NAE サーバーによって使用されるプロトコル。
edgeencryption.nae.keystore.path	NAE サーバー上のキーストアへのパス。
edgeencryption.nae.keystore.password	NAE キーストアのパスワード。
edgeencryption.nae.username	NAE デバイスでの認証に使用するユーザー名。
edgeencryption.nae.password	NAE デバイスでの認証に使用するパスワード。
edgeencryption.nae.client.certificate	NAE サーバー上のキーストアにある証明書。ユーザー名とパスワードの代わりに証明書を使用して認証を行う場合に、このプロパティを設定します。

パスワードのプロパティ

edgeencryption.encrypter.properties.password	conf フォルダーにあるファイルの名前。このファイルには、edgeencryption.properties ファイルにあるパスワードをセキュアなプロセスの中で難読化するのに使用される文字列が含まれています。 **注:** conf フォルダーにあるファイルの名前。このファイルには、edgeencryption.properties ファイルにあるパスワードをセキュアなプロセスの中で難読化するのに使用される文字列が含まれています。

プロキシのプロパティ

edgeencryption.proxy.host	プロキシを実行しているコンピューターのサーバー名、IP アドレス、または完全修飾ドメイン名。このプロパティとポートによって、クライ

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

	アントがプロキシサーバーへのアクセスに使用する URL が定義されます。
edgeencryption.proxy.name	プロキシ名。プロキシごとに一意である必要があります。
edgeencryption.proxy.http.port	HTTP 通信のプロキシのポート。
edgeencryption.proxy.https.port	HTTPS 通信のプロキシのポート。

プロキシ設定のロックのプロパティ

edgeencryption.proxy.locked	True の場合、プロキシはインスタンスからの暗号化設定の変更または暗号化ルールの変更を受け入れません。すべての暗号化設定およびルールが最終的に決定した後、本番インスタンスでこのプロパティを設定します。

プロキシ データベースのプロパティ

edgeencryption.db.url	プロキシ データベースの場所。同じインスタンスに接続するすべての暗号化プロキシで同じである必要があります。
edgeencryption.db.user	プロキシ データベースにアクセスするためのユーザー名。同じインスタンスに接続するすべての暗号化プロキシで同じである必要があります。
edgeencryption.db.password	プロキシ データベースにアクセスするためのパスワード。同じインスタンスに接続するすべての暗号化プロキシで同じである必要があります。
edgeencryption.db.name	プロキシ データベース名。同じインスタンスに接続するすべての暗号化プロキシで同じである必要があります。このプロパティのデフォルトは edgeencryption です。
edgeencryption.db.bootstrap.file	プロキシ データベースのブートストラップ ファイル。このファイルは sql/ ディレクトリーからの相対パスです。同じインスタンスに接続するすべての暗号化プロキシで同じである必要があります。 **⚠ 警告:** 通常、このパラメーターは変更しないでください。

プロキシサーバーのパフォーマンスのプロパティ

プロキシサーバーのパフォーマンスのプロパティは、デフォルトでは設定ファイルに存在しません。デフォルト値を変更するには、プロパティを追加してプロキシサーバーを再起動する必要があります。詳細については、「Edge Encryption の診断とパフォーマンス」を参照してください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

edgeencryption.stat.collection.enabled	エッジ暗号化 プロキシサーバーのパフォーマンス ダッシュボードで使用される統計情報の収集を有効にします。 デフォルト値：true エッジ暗号化 プロキシサーバーのパフォーマンス ダッシュボードで使用される統計情報の収集を無効にするには、このプロパティを追加して、値を False に設定します。
edgeencryption.stat.collection.interval	エッジ暗号化 プロキシサーバーが統計情報を収集する間隔 (秒単位)。この値は 30 秒未満にすることはできません。 デフォルト値：30 (秒)

SSL 証明書のプロパティ

SSL 証明書プロパティの値を変更した場合は、プロキシを再起動します。システムでは起動時に HTTPS キーペアを使用して、プロキシサーバーの接続を確立し、プロキシがクライアント要求に応答する方法を決定します。

edgeencryption.proxy.https.cert.alias	プロキシサーバーから接続中のクライアントに提供される証明書のエイリアス。
edgeencryption.proxy.https.keystore.path	HTTPS 証明書が格納されているキーストアへのパス。
edgeencryption.proxy.https.keystore.password	HTTPS 証明書が格納されているキーストアのパスワード。

ターゲット (インスタンス) のプロパティ

edgeencryption.target.host	インスタンスのホスト名。同じインスタンスに接続するすべての暗号化プロキシで同じである必要があります。このプロパティは、プロキシのインストール時に設定されます。たとえば、instancename.servicenow.com などです。
edgeencryption.target.port	インスタンスのポート。同じインスタンスに接続するすべての暗号化プロキシで同じである必要があります。このプロパティは、プロキシのインストール時に設定されます。
edgeencryption.target.protocol	インスタンスのプロトコル。同じインスタンスに接続するすべての暗号化プロキシで同じである必要があります。このプロパティは、プロキシのインストール時に設定されます。次のオプションが含まれます。 • http • https

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Unbound Technology プロバイダーのプロパティ

edgeencryption.ekm.provider.classname	実装の内部クラス名。 ⚠ 警告: このプロパティは変更しないでください。
edgeencryption.thirdparty.vendor.library.path	Unbound クライアント マシン上の Unbound API JAR ファイルへのパス。
edgeencryption.ekm.provider.rsa.wrapping.key.alias	Unbound Technology の実装のラッピング キー エイリアス。すべてのプロキシで同じにする必要があります。

ユーザー アカウントのプロパティ

edgeencryption.target.username	プロキシがインスタンスへのログインに使用するユーザー名。ユーザーには edge_encryption ロールが必要です。「Edge Encryption ユーザー アカウントを設定する」を参照してください。
edgeencryption.target.password	プロキシがインスタンスへのログインに使用するパスワード。

Web プロキシのプロパティ

edgeencryption.webproxy.host	Web プロキシの名前または IP アドレス。
edgeencryption.webproxy.port	Webプロキシのポート。
edgeencryption.webproxy.user	Web プロキシへの接続に使用されるユーザー名。Web プロキシで認証を使用しない場合は、このプロパティをコメント アウトしたままにしておきます。
edgeencryption.webproxy.password	Web プロキシへの接続に使用するパスワード。Web プロキシで認証を使用しない場合は、このプロパティをコメント アウトしたままにしておきます。

不使用になったプロキシ暗号化プロパティ

edgeencryption.encrypter.default.key128

現在の AES 128 キーの名前を指定します。AES 128 キーは、使用しなくても利用可能でなければなりません。すべてのプロキシで同じにする必要があります。

インスタンスでこれらのキーのメンテナンスを実行します。

edgeencryption.encrypter.default.key256

現在の AES 256 キーの名前を指定します。すべてのプロキシで同じにする必要があります。

インスタンスでこれらのキーのメンテナンスを実行します。

edgeencryption.encrypter.key

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

キー名をキーごとに指定し、デフォルトのキーを指定するために使用します。これは、暗号化された各アイテムに含まれるメタデータと統合されたキーエイリアスであり、したがってインスタンスに格納されます。キーの名前は小文字を使用する必要があります。

edgeencryption.encrypter.type

暗号化キーストアシステムのタイプを指定します。

edgeencryption.encrypter.file

キーに関連付けられたテキストファイルのパスとファイル名を指定します。

edgeencryption.encrypter.password

キーストアにアクセスするためのパスワードを指定します。

CyberArk と **Edge** プロキシサーバーとの統合

CyberArk を使用して、パスワードを集中管理された安全なデジタルボールトに保存し、以前にクリアテキストで保存され、ファイルアクセスによって保護されたパスワード、または以前に第 2 ファイルで暗号化されたパスワードを保護します。

CyberArk AIM (アプリケーション ID 管理) は、ハードコーディングされたパスワードや可視のパスワードをなくすことで、不正なアクセスを防止します。AIM は、独立した強化サーバー上のデジタル ボールトにパスワードを格納します。ボールトではパスワードはデジタル認証情報として表現されます。AIM クライアント (Edge プロキシサーバー) は、CyberArk のデジタル認証情報を使用して、独立したサーバーにアクセスし、セキュリティ保護されたパスワードを取得します。パスワードは Edge プロキシサーバーにもインスタンスにも格納されません。

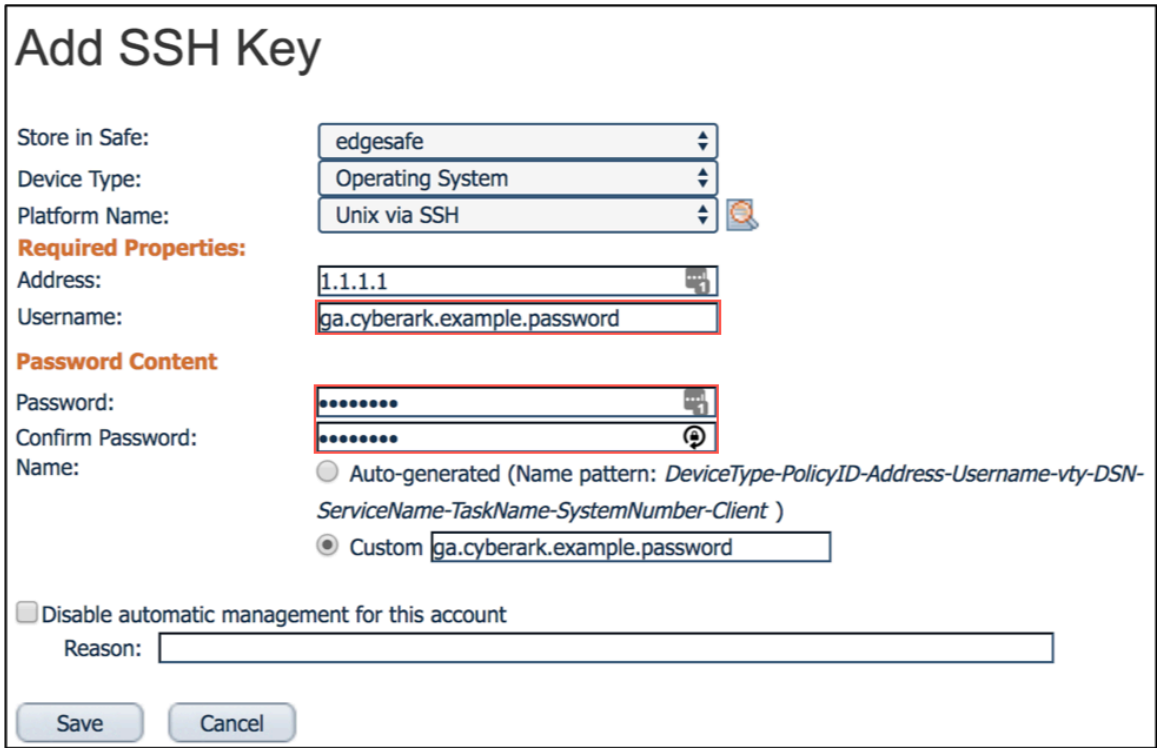
CyberArk のデジタル ボールトの資格情報

CyberArk と Edge プロキシサーバーとの統合をセットアップするには、事前に CyberArk を購入して設定を行う必要があります。

CyberArk に認証情報を追加するには、認証情報の **[Platform Name]** を **[Unix via SSH]** に設定して、**[Custom]** の認証情報 **[Name]** を作成するか、**[Auto-generated]** の認証情報 **[Name]** を書き留めておきます。この認証情報を使用するように Edge プロキシを設定すると、プロキシサーバーは、この認証情報 **[Name]** をプロキシ内の設定に合わせます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



認証情報の各エントリには、セキュリティ保護されている **[Password]** のほか、アプリケーションがそのパスワードへのアクセスに使用する認証情報 **[Name]** が保持されています。

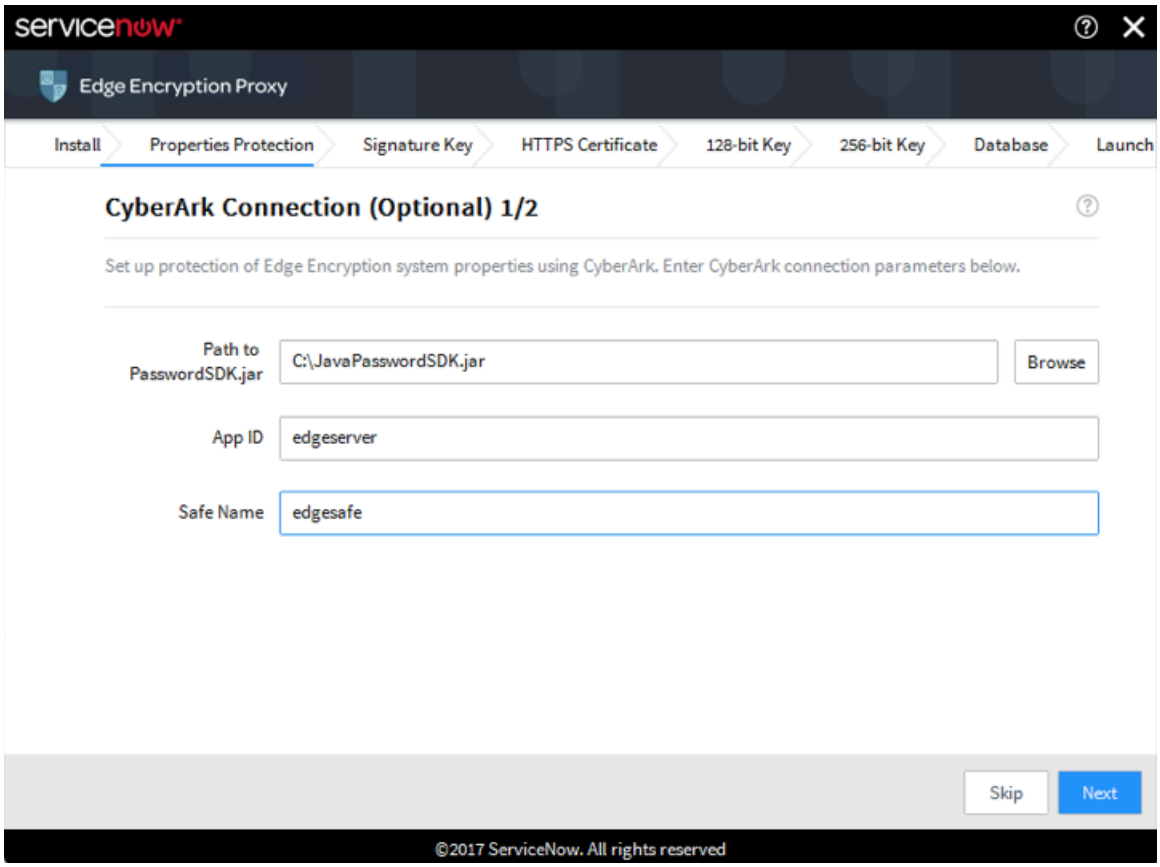
> **注:**
> CyberArk の認証情報は暗号化キーではありません。

Edge プロキシのインストール時に **CyberArk** を追加する

プロキシ インストーラーには、CyberArk との統合を行うための新しい設定ページが含まれています。プロキシ インストーラーによるプロキシのインストール時に CyberArk の追加を希望しない場合は、このページを省略できます。または、設定ファイルで CyberArk の統合を手動でセットアップして設定を行うこともできます。

自動翻訳

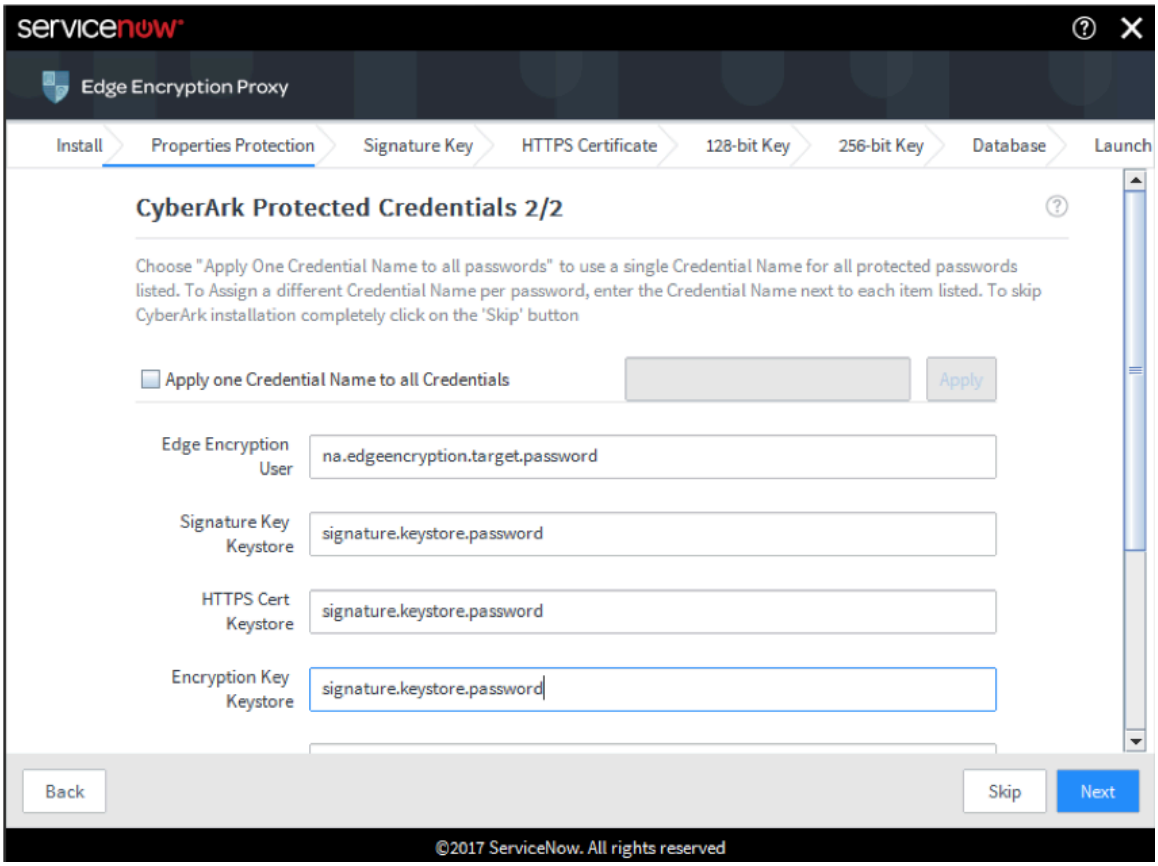
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



プロキシ インストーラーには、CyberArk で保護される認証情報用の新しいページも含まれています。このページでは、1 つまたは複数の認証情報名を使用して、さまざまなプロパティの構成を行うことができます。プロキシ インストーラーによるプロキシのインストール時に CyberArk の追加を希望しない場合は、このページを省略できます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



CyberArk のパスワード保護

Edge プロキシ インストーラーにあるパスワード フィールドのうち、CyberArk のボールトで CyberArk の認証情報が設定されていて、インストーラーの [CyberArk で保護される認証情報] ページで指定されているものは、グレー表示され、「CyberArk による保護」というメッセージが表示されます。

Edge プロキシサーバーでロードバランサーを使用する

ロードバランサーを使用して、Edge Encryption プロキシ設定のプロキシサーバー間の負荷を分散することができます。 ロードバランサーとプロキシサーバーが異なるポートを使用している場合は、ユーザーがブラウザで応答を表示できるように、ロードバランサーのホスト名と HTTPS ポートを指定します。

重要:
すべての本番環境で、冗長性のために Edge Encryption プロキシサーバーを少なくとも 2 つ用意してください。

ロードバランサーを使用しない Edge 要求の処理

ロードバランサーを使用していない場合、要求は次のように処理されます。

1. ユーザーがブラウザーから要求を出します。
2. ブラウザーが Edge プロキシサーバーに要求を送信します。
3. プロキシサーバーが ServiceNow インスタンスに要求を送信します。
4. ServiceNow インスタンスがプロキシサーバーに応答を返します。
5. プロキシサーバーは、ユーザーのブラウザーに応答を返す前に、応答ヘッダーに自分自身のポート番号を追加します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ユーザーは、応答ヘッダーで指定されたポート番号でプロキシサーバーからの応答を表示できます。これで、要求は正常に完了します。

ロードバランサーを使用した Edge 要求の処理

これに対して、ロードバランサーを使用している場合、ユーザーのブラウザーはプロキシサーバーと通信するのではなくロードバランサーと直接通信します。要求は次のように処理されます。

> **注:**
> この例では、プロキシサーバーのポート番号として 1025 を使用しています。

1. ユーザーがブラウザーから要求を出します。
2. ブラウザーが要求をロードバランサー仮想 IP (VIP) (仮想サーバーとも呼ばれます) に送信します。
3. VIP は、プロキシサーバーを指し示すように設定されています (10.2.200.148:1025 など)。そのため、ロードバランサーは要求をプロキシサーバーに転送します。
4. プロキシサーバーが ServiceNow インスタンスに要求を送信します。
5. ServiceNow インスタンスがプロキシサーバーに応答を返します。
6. プロキシサーバーは、応答内のロケーション ヘッダーを、risk-servicenow.dev.echonet:1025 のプロパティで設定された値に書き換えます。
   - ホスト：edgencryption.proxy.host
   - **HTTP** ポート：edgeencryption.proxy.http.port
   - **HTTPS** ポート：edgeencryption.proxy.https.port
7. プロキシサーバーは、プロキシサーバー ポートを指し示しているロケーション ヘッダーを使用して、応答をロードバランサーに転送します。

この結果は、ロードバランサーとプロキシサーバーが同じポートを使用しているかどうかによって異なります。

- ロードバランサーとプロキシサーバーが同じポートを使用している場合、ユーザーは応答ヘッダーで識別される同じポートから応答を受け取るため、要求は成功します。
- ロードバランサーとプロキシサーバーが異なるポートを使用している場合、ユーザーのブラウザーはロードバランサーとのみ通信しますが、応答はプロキシサーバー上にあるため、要求は失敗します。

解決策

この問題は、単にロードバランサーとすべての Edge プロキシサーバーを同じポート上で使用して解決できます。ただし、これは理想的な解決策ではありません。より良い解決策として、ロードバランサーがどのポートを使用しているかをシステムが認識できるようにします。

プロキシサーバーとロードバランサーが異なるポートを使用している場合、次のプロパティを使用すると、Edge プロキシサーバーが応答メッセージをロードバランサーに再ルーティングできます。

- *`edgeencryption.proxy.rewrite.location.host`* は、ロードバランサー経由で ServiceNow にアクセスするために使用するホスト名を指定します。
- *`edgeencryption.proxy.rewrite.location.https.port`* は、ロードバランサー経由で ServiceNow にアクセスするために使用する HTTPS ポートを指定します。

ロードバランサーの設定を行う

ロードバランサーとプロキシサーバーが異なるポートを使用している場合は、ユーザーがブラウザで応答を表示できるように、ロードバランサーのホスト名と HTTPS ポートを指定します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

始める前に
必要なロール：

- Windows ホストでのローカル管理者またはドメイン管理者
- Linux ホスト上のファイルシステムへのフルアクセス権限があるサービスユーザー

手順

1. 管理者、ドメイン管理者、またはサービス ユーザーとして、プロキシサーバー ホストにログインします。
2. Edge プロキシのインストール ディレクトリーに移動し、conf/edgeencryption.properties を選択します。
3. 次のプロパティを設定します。

プロパティ	説明
edgeencryption.proxy.rewrite.location.host	Edge の構成にプロキシサーバー間の負荷分散を行うロードバランサーが含まれている場合は、応答をロードバランサーに書き換えて要求を完了させることができます。 ○ プロキシのセットアップでロードバランサーが存在する場合は、ロードバランサー経由で ServiceNow にアクセスするために使用するホスト名を指定します。 ○ オプション：プロキシのセットアップでロードバランサーが存在しない場合は、プロキシサーバーが使用するホスト名に設定することができます。
edgeencryption.proxy.rewrite.location.https.port	Edge の構成にプロキシサーバー間の負荷分散を行うロードバランサーが含まれている場合は、ロードバランサー経由で ServiceNow にアクセスするために使用する HTTPS ポートを指定します。 ○ 構成にロードバランサーが存在する場合は、ロードバランサー経由で ServiceNow にアクセスするために使用する HTTPS ポートを指定します。 ○ オプション：構成にロードバランサーが存在しない場合は、プロキシサーバーが使用する HTTPS ポートに設定することができます。

4. ファイルを保存します。

タスクの結果
これで、ユーザーはブラウザーでレスポンスを表示できるようになり、要求を完了できます

Edge Encryption のアップグレード

インスタンスのアップグレードとプロキシサーバーのアップグレードのどちらを行う場合も、エッジ暗号化 環境で特別な考慮が必要になります。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

インスタンスのアップグレード

Edge Encryption 環境でインスタンスのアップグレードを行うには、インスタンスのアップグレード後に Edge によるコントロールが正しく機能するように注意する必要があります。

インスタンスのアップグレード中に、次のものを追加、編集、または削除しないでください。

- Edge Encryption の設定
- Edge Encryption のルール
- Edge Encryption のトークン化パターン
- Edge Encryption のジョブスケジュール
- Edge Encryption のキー設定
- Edge Encryption のスケジュール設定済みのアップグレード
- Edge Encryption の拒否リスト IP 設定

インスタンスのアップグレード中に実行されたスケジュール設定済みのジョブは、どれも完了しません。中断されたジョブを完了するには、インスタンスのアップグレードの完了後にジョブを再実行します。ジョブのスケジュールを変更した場合、インスタンスのアップグレード前に発生した処理は失われず、まだ処理が完了していないデータのみの処理がジョブで続行されます。

プロキシサーバーのアップグレード

インスタンスが エッジ暗号化 プロキシサーバーをアップグレードできるようにプロキシをスケジュールするか、任意のタイミングでプロキシサーバーを手動でアップグレードします。

警告:
Windows でのアップグレードでは、ファイルロックの問題が発生し、アップグレードが失敗する可能性があります。アップグレードを正常に完了するには、インストールディレクトリの下のファイルを開いた状態にしないでください。また、インストールディレクトリに既存のシェルが存在しないようにする必要があります。特に、インストールディレクトリでコマンドラインから (bin\edgeencryption.bat install/start 経由で) プロキシを起動する場合は、そのシェルを閉じるか、後でインストールディレクトリから移動させる必要があります。インストールディレクトリにあるファイルを、エディターや他のアプリケーションで開かないでください。

サードパーティのライブラリー

Gemalto などのサードパーティライブラリーは、同じディレクトリに格納されている場合、インスタンスとプロキおよびサーバーのアップグレード時に失われます。アップグレード中にサードパーティのライブラリーが失われないようにするには、以下を実行します。

1. 次のプロパティを edgeencryption.properties に手動で追加します。

   ```
   edgeencryption.ekm.provider.classname =
   com.snc.edgeencryption.encryption.CloudEdgeNaeKeyProvider
   ```

2. *edgeencryption.thirdparty.vendor.library.path* ベンダーライブラリーの場所プロパティを追加し、「/path/to/jars」に設定します。

   たとえば、

   ```
   edgeencryption.thirdparty.vendor.library.path = /app/servicenow/libs
   ```

3. SafeNet JAR をそのパスにコピーします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

エッジ暗号化 インストール外でサードパーティライブラリーをインストールした後、アップグレード中にそのライブラリーが失われることはありません。

スケジュール設定済みのアップグレード

> **重要:**
> ServiceNow インスタンスのアップグレード中に、プロキシサーバーのバージョンもアップグレードしてインスタンスのバージョンに合わせ、互換性の問題が発生する可能性を減らします。

予定された時刻にインスタンスがプロキシサーバーをアップグレードできるように、アップグレードをスケジュールします。この機能は、アップグレード後にデフォルトで使用できます。スケジュール設定済みのアップグレードでは、次のイベントが発生します。

1. プロキシサーバーがインスタンスに問い合わせて、アップグレード可能な新しいバージョンがあるかどうかを確認します。通常、新しいバージョンは、インスタンスがアップグレードされたときに使用可能になります。
2. 新しいバージョンのプロキシサーバーが使用可能になると、管理者はログイン時に通知を受け取ります。
3. 管理者はプロキシサーバーごとに、Edge Encryption プロキシサーバーのアップグレードをスケジュールすることができます。

   > **注:**
   > security_admin ロールを持つユーザーのみが、プロキシサーバー経由でアップグレード スケジュールを作成できます。

4. アップグレードがスケジュールされると、プロキシサーバーは予定された時刻に自動的にアップグレードされます。アップグレード中、プロキシサーバーは一時的にオフラインになります。

   > **注:**
   > プロキシサーバーはアップグレード中に再起動するため、一時的にオフラインになります。その時間の長さは環境、およびプロキシ サービスの停止と再起動にかかる時間によって異なります。

5. スケジュール設定済みのアップグレード中に、新しいプロキシ ディレクトリーが作成され、設定ファイルが新しいディレクトリーにコピーされます。新しいプロパティが既存のプロパティ ファイルに書き込まれます。古いプロキシ ディレクトリにある次のファイルまたはディレクトリーが、新しいプロキシ ディレクトリにコピーされます。
   - /conf ディレクトリー
   - /keys ディレクトリー
   - /keystore ディレクトリー
   - java/jre/lib/security/cacerts ファイル

   その結果、キー、キーストア、設定、および証明書が保持されます。

   > **注:**
   > 新しいプロキシ ディレクトリーにコピーされるのは上記のファイルのみです。プロキシサーバー ディレクトリにあるその他のカスタマイズされたファイルは、スケジュール設定済みのアップグレード中は保存されません。アップグレードのログ ファイルは、元のプロキシ ディレクトリーの <original-proxy-directory>/tmp/upgrade-wrapper/bin フォルダーにあります。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

スケジュール設定済みのアップグレードの必須条件

Edge Encryption プロキシのアップグレードをスケジュールする際は、事前に次の点を確認してください。

1. *JAVA_HOME* 環境変数が、Edge Encryption プロキシのディレクトリー構造以外の場所にあるマシンにインストールされた Java を指し示していること。
2. *JAVA_HOME* 環境変数が、バージョン 1.8_u144 以降としてインストールされた Java を指し示していること。
3. wrapper.conf ファイルの `-Djava.io.tmpdir` パラメーターが、Edge Encryption プロキシのディレクトリー構造「以外の場所」にあるディレクトリーを指し示していて、プロキシがそのディレクトリーに対して読み取り/書き込み/実行の権限を持っていること。オプションで、Java がデフォルトの tmp 場所を使用するように、パラメーター全体をコメント アウトすることもできます。

手動アップグレード

アップグレード スケジュールを作成する代わりに、コマンド ラインから個々のプロキシサーバーを手動でアップグレードすることができます。「Linux で実行中の Edge Encryption プロキシサーバーを手動でアップグレードする」または「Windows で実行中の Edge Encryption プロキシサーバーを手動でアップグレードする」を参照してください。

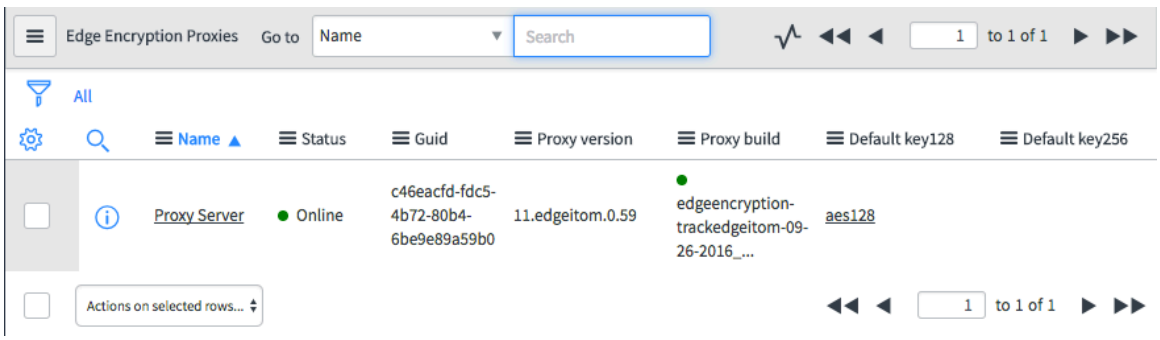
プロキシのビルド ステータス

プロキシサーバーが古くなっているかどうかは、次の場所に移動することで簡単に識別できます エッジ暗号化の設定 > プロキシ > すべて. プロキシのビルド ステータスは [プロキシのビルド] 列に次の色で表示されます。

緑
: プロキシサーバーは最新です。

黄
: プロキシサーバーは古くなっていて、アップグレードが必要です。

オレンジ
: アップグレードに失敗しました。ダウンタイムが発生しないように、プロキシサーバーは古いバージョンに戻されています。



スケジュール設定済みのプロキシ アップグレードが失敗した場合のトラブルシューティング

スケジュール設定済みのプロキシ アップグレードが失敗した場合、プロキシサーバーはアップグレード前のバージョンに戻ります。元のデータ、キー、および設定ファイルはすべて保持されます。このプロセスには数分かかることがあります。カスタマーサービス & サポートに連絡して、アップグレードを確実に成功させてください。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

失敗の原因を調べるには、アップグレード スケジュールで [障害の原因] をチェックします。また、失敗したアップグレードのインストール ディレクトリーは保持されているため、ログ ファイルをトラブルシューティングに使用できます。

> **注:**
> 余分なプロキシ ディレクトリを削除する前に、ログ ファイルを確認してディレクトリーが最新であることを必ず確認してください。ログ ファイルに最近のアクティビティが記録されている場合、プロキシからインスタンスに接続している可能性があります。

スケジュール設定済みのプロキシ アップグレードが繰り返し失敗する場合、プロキシサーバーを手動でアップグレードすることができます。「Linux で実行中の Edge Encryption プロキシサーバーを手動でアップグレードする」および「Windows で実行中の Edge Encryption プロキシサーバーを手動でアップグレードする」を参照してください。

Java の最低要件

エッジ暗号化 プロキシサーバーをインストールまたは実行するホストマシンでは、サポートされているバージョンの Java を保持する必要があります。現在サポートされているバージョンは 11.x バージョンシリーズの Java 11.0.6 以降です。

> **注:**
> Java 8 は Utah リリースからサポートされなくなりました。Utah バージョンの エッジ暗号化 プロキシをインストールする前に、エッジ暗号化 プロキシを使用する環境を Java 11 にアップグレードしてください。

Java 8 update 141 (8u141) 以下で AES 256 ビット暗号化を使用する場合、Java Cryptography Extension (JCE) 管轄ポリシーファイルを、各 エッジ暗号化 プロキシサーバー ホストのシステムの Java ホーム ディレクトリにコピーしてインストールする必要があります。スケジュール設定済みアップグレードまたは手動アップグレードを実行する前に、これらのファイルを <Java-home-directory>/jre/lib/security フォルダに追加します。AES 256 ビット暗号化ポリシーファイルをインストールするには、「AES 256 ビット暗号化キーを設定する」を参照してください。

プロキシのバージョンが混在する環境

古いバージョンのプロキシサーバーを実行しながら最新バージョンのプロキシサーバーを使用する環境は推奨されませんが、すべてのプロキシサーバーがインスタンスと同じバージョン ファミリーである環境はサポートされています。たとえば、Washington DC リリースのインスタンスを使用している環境では、Washington DC のパッチまたはホットフィックスを適用したプロキシサーバーがサポートされます。ただし、次の制限があります。

- あるプロキシサーバーがサポートしている機能を別のプロキシがサポートしていない場合、使用しているプロキシサーバーによっては一貫性のない動作が生じます。
- プロキシサーバーが古くなっている場合、最近のセキュリティ強化が組み込まれていない可能性があります。

以前のリリースのプロキシサーバーがインスタンスの新しいリリースに登録されている場合は、プロキシサーバーが古くなっているという通知が定期的に表示されます。最適で安全な環境を確保するため、ServiceNow では、常にインスタンスでサポートされている最新バージョンのソフトウェアにプロキシサーバーをアップグレードすることをお勧めしています。

Edge Encryption プロキシサーバーのアップグレードをスケジュールする

インスタンスが古いプロキシサーバーをアップグレードできるように、アップグレード スケジュールを作成します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

始める前に
アップグレードをスケジュールするには、プロキシサーバー経由でインスタンスにログインする必要があります。
Java 8 update 141 (8u141) 以下で AES 256 ビット暗号化を使用する場合、Java Cryptography Extension (JCE) 管轄ポリシーファイルを、各 エッジ暗号化 プロキシサーバー ホストのシステムの Java ホーム ディレクトリにコピーしてインストールする必要があります。スケジュール設定済みアップグレードまたは手動アップグレードを実行する前に、これらのファイルを <Java-home-directory>/jre/lib/security フォルダに追加します。AES 256 ビット暗号化ポリシーファイルをインストールするには、「AES 256 ビット暗号化キーを設定する」を参照してください。

必要なロール：security_admin

このタスクについて
アップグレードがスケジュールされると、プロキシサーバーは予定された時刻に自動的にアップグレードされます。アップグレード中、プロキシサーバーは一時的にオフラインになります。

注:
プロキシサーバーはアップグレード中に再起動するため、一時的にオフラインになります。その時間の長さは環境、およびプロキシ サービスの停止と再起動にかかる時間によって異なります。

スケジュール設定済みのアップグレード中に、新しいプロキシ ディレクトリーが作成され、設定ファイルが新しいディレクトリーにコピーされます。新しいプロパティが既存のプロパティ ファイルに書き込まれます。古いプロキシ ディレクトリにある次のファイルまたはディレクトリーが、新しいプロキシ ディレクトリにコピーされます。

- /conf ディレクトリー
- /keys ディレクトリー
- /keystore ディレクトリー
- java/jre/lib/security/cacerts ファイル

その結果、キー、キーストア、設定、および証明書が保持されます。

注:
新しいプロキシ ディレクトリーにコピーされるのは上記のファイルのみです。プロキシサーバー ディレクトリにあるその他のカスタマイズされたファイルは、スケジュール設定済みのアップグレード中は保持されません。アップグレードのログ ファイルは、元のプロキシ ディレクトリーの <original-proxy-directory>/tmp/upgrade-wrapper/bin フォルダーにあります。

複数のプロキシサーバーが古くなっている場合は、プロキシサーバーごとに個別にアップグレードをスケジュールする必要があります。

注:
同じマシンで複数のプロキシサーバーをホストすることは避けてください。ただし、この構成が環境に含まれている場合は、同じマシンで同時に複数のプロキシへのアップグレードをスケジュールしないでください。

手順

1. 移動先 すべて > エッジ暗号化の設定 > プロキシ > スケジュールをアップグレード.
2. [新規] をクリックします。
3. フォームに入力します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Encryption Proxy プロキシのアップグレード スケジュール フォーム

フィールド	説明
プロキシサーバー	アップグレード対象のプロキシサーバー。
ターゲットバージョン	このバージョンにプロキシサーバーをアップグレードします。この値は読み取り専用で、インスタンスで使用可能な最新のプロキシ バージョンに設定されます。
予定開始時間	アップグレードを開始する日時。
有効	スケジュール設定済みのアップグレードが有効かどうか。このフィールドが選択されていない場合、スケジュールされた日時にアップグレードが実行されません。
ステータス	アップグレードのステータス。この値は読み取り専用です。ステータスの候補は次のとおりです。 ○ 処理待ち ○ 実行中 ○ 完了 ○ 失敗

4. [送信] をクリックします。

次のタスク

アップグレードの一般的な時間は 15 分未満です。アップグレードの実行後、アップグレードの詳細を表示して詳しく調べることができます。アップグレードが失敗した場合は、[障害の原因] を確認して、次のステップを決定してください。

アップグレードの詳細

フィールド	説明
前のバージョン	サーバーがアップグレードされる前のバージョン。
後のバージョン	サーバーがアップグレードされた後のバージョン。
実際の開始時間	アップグレードが開始された時間。
終了時間	アップグレードが終了した時間。
障害の原因	アップグレードが失敗した理由。

Linux で実行中の **Edge Encryption** プロキシサーバーを手動でアップグレードする

Linux で実行されているプロキシを更新します。

始める前に

Java 8 update 141 (8u141) 以下で AES 256 ビット暗号化を使用する場合、Java Cryptography Extension (JCE) 管轄ポリシーファイルを、各 エッジ暗号化 プロキシサーバー ホストのシステムの Java ホーム ディレクトリにコピーしてインストールする必要があります。スケジュール設定済

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

みアップグレードまたは手動アップグレードを実行する前に、これらのファイルを <Java-home-directory>/jre/lib/security フォルダに追加します。AES 256 ビット暗号化ポリシーファイルをインストールするには、「AES 256 ビット暗号化キーを設定する」を参照してください。

必要なロール：ホストマシンでの security_admin またはローカル管理者

手順

1. エッジ暗号化 プロキシのアップデート アーカイブ ファイルをインストール ディレクトリーにコピーします。
   a. 移動先 エッジ暗号化の設定 > インストールとダウンロード > ダウンロード
   b. [コマンドラインインストーラをダウンロード] リンクを選択します。
   c. ダウンロードが開始されたら、ダウンロード場所としてインストールディレクトリを選択します。
2. インストール ディレクトリーに移動します。
3. 次のコマンドを実行します。

   `java -jar edgeencryption-dist-<バージョン>-linux-x86-64.jar -m dist-upgrade -c <プロキシのディレクトリー>`

オプション	説明
プロキシのディレクトリー	プロキシが最初にインストールされたインストール ディレクトリー内のディレクトリー。このディレクトリーはインストールによって作成されます。

   ヘルプ画面が必要な場合は、このコマンドを引数なしで実行します：`java -jar edgeencryption-dist-<version>-linux-x86-64.jar`。

   現在のタイムスタンプで新しいプロキシディレクトリが作成されます。古いプロキシディレクトリのバックアップは、新しいプロキシのインストールディレクトリに backup.dist-upgrade_timestamp として保持されます。古いプロキシがシャット ダウンし、新しいプロキシが起動します。古いプロキシサーバーで開いている接続/トランザクションはすべて終了します。
4. 新しいディレクトリーにあるプロキシ ログとインスタンスを調べて、新しいプロキシが実行されていることを確認します。

Windows で実行中の Edge Encryption プロキシサーバーを手動でアップグレードする

Windows で実行されているプロキシを更新します。

始める前に
Java 8 update 141 (8u141) 以下で AES 256 ビット暗号化を使用する場合、Java Cryptography Extension (JCE) 管轄ポリシーファイルを、各 エッジ暗号化 プロキシサーバー ホストのシステムの Java ホーム ディレクトリにコピーしてインストールする必要があります。スケジュール設定済みアップグレードまたは手動アップグレードを実行する前に、これらのファイルを <Java-home-directory>/jre/lib/security フォルダに追加します。AES 256 ビット暗号化ポリシーファイルをインストールするには、「AES 256 ビット暗号化キーを設定する」を参照してください。

必要なロール：ホストマシンでの security_admin またはローカル管理者

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. エッジ暗号化 プロキシのアップデート アーカイブ ファイルをインストール ディレクトリーにコピーします。
   a. 移動先 エッジ暗号化の設定 > インストールとダウンロード > ダウンロード
   b. [コマンドラインインストーラをダウンロード] リンクを選択します。
   c. ダウンロードが開始されたら、ダウンロード場所としてインストールディレクトリを選択します。
2. Windows のコマンド プロンプト プログラムを管理者権限で起動します。
3. インストール ディレクトリーに移動します。
4. 次のコマンドを実行します。

   ```
   java -jar edgeencryption-dist-<バージョン>-all.jar -m dist-upgrade -c <プロキシディレクトリ>
   ```

オプション	説明
プロキシのディレクトリー	プロキシが最初にインストールされたインストール ディレクトリー内のディレクトリー。このディレクトリーはインストールによって作成されます。

   ヘルプ画面が必要な場合は、コマンド `java -jar edgeencryption-dist-<version>-linux-x86-64.jar` を引数なしで実行します。

   現在のタイムスタンプで新しいプロキシディレクトリが作成されます。古いプロキシディレクトリのバックアップは、新しいプロキシのインストールディレクトリに backup.dist-upgrade_timestamp として保持されます。古いプロキシがシャット ダウンし、新しいプロキシが起動します。古いプロキシサーバーで開いている接続/トランザクションはすべて終了します。
5. 新しいディレクトリーにあるプロキシ ログとインスタンスを調べて、プロキシが更新されて実行されていることを確認します。

Edge Encryption プロキシサーバーのアップグレードをロール バックする

プロキシのアップグレードが失敗した場合、以前のバージョンに戻すことができます。

始める前に
必要なロール：管理者

このタスクについて
Washington DC リリースのスケジュール設定済みのアップグレード機能を使用していて、アップグレードが失敗した場合、プロキシサーバーは自動的に古いバージョンにロール バックします。古いプロキシサーバーは無修正でバックアップ ディレクトリーに格納されます。

手動のアップグレードをロール バックする場合は、次の手順に従います。

手順

1. プロキシをシャット ダウンします。
2. 新しいプロキシ ディレクトリーを削除します。
3. バックアップ ディレクトリーの名前をプロキシ名に変更します。
   バックアップ ディレクトリーは、<プロキシ名>_backup という名前のプロキシ インストール ディレクトリーです。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

4. プロキシを起動します。
5. プロキシ ログとインスタンスを調べて、プロキシがオンラインであることを確認します。

Edge Encryption の設定

エッジ暗号化 プロキシサーバーをインストールして実行したら、プロキシサーバーを介して エッジ暗号化 を管理します。

インスタンスで暗号化設定と暗号化パターンを作成する前に、「Edge Encryption のインストール」のすべての手順を完了する必要があります。

注:
エッジ暗号化 の設定にアクセスするには、プロキシサーバーを介してログインし、security_admin ロールに昇格する必要があります。

暗号化キーをローテートする

インスタンスから暗号キーのローテーションを実行します。新しいキーを追加し、デフォルトキーの割り当てを変更してから、一括キーローテーションまたは単一キーローテーションをスケジュールします。

暗号化キーをデフォルトキーとして設定する前に、各プロキシでキーを使用できるようにします。これにより、キーがデフォルトキーとして割り当てられるときに、プロキシでデータを暗号化するためのキーが確保されます。すべてのプロキシは、キーがデフォルトキーとして割り当てられる前に、そのキーにアクセスできる必要があります。

警告:
プロキシからキーを削除する場合は、事前に一括キーローテーションジョブをセットアップして実行し、インスタンスでキーを使用しているデータが存在しないようにしてください。そのキーを使用して暗号化されている情報がまだある場合は、キーを削除した後で情報を復号化することはできません。

Edge のフィルタリングとソートの動作

デフォルトキーを変更した場合は、必ずキーローテーション (一括または単一のいずれかのローテーション) を実行してください。そうでない場合、レコードをソートおよびフィルタリングしたときに予期しない結果が生じることがあります。たとえば次のシナリオを考えます。

1. 1 つの暗号化キーを使用して暗号化レコードを作成します。
2. 新しいキーを作成し、これをデフォルトとして設定します。
3. 新しい暗号化キーを使用して新しい暗号化レコードセットを作成します。

Edge プロキシ経由で接続されているときに任意の暗号化フィールドでフィルタリングする場合、すべてのレコードを適切にフィルタリングで除外できなかったり、レコードが予期せず表示されたりする可能性があります。フィルターは、現在のデフォルトキーを使用して暗号化されたレコードに対してのみ機能します。前のデフォルトキーを使用して暗号化されたレコードは、引き続きリストビューに表示されます。

Edge プロキシ経由で接続されているときに任意の暗号化フィールドでソートする場合、人間が判読可能な同一のテキストが含まれる 2 つのレコードグループが暗号化フィールドに表示されます。

単一のキー ローテーション ジョブをスケジュールする

指定したキー エイリアスを使用して暗号化されたデータを検索し、現在のデフォルトの暗号化キーでデータを再暗号化するジョブをスケジュールします。データは復号化されてから、デフォルトキーで再暗号化されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

始める前に
必要なロール：security_admin
このジョブをスケジュールする前に、次のデフォルトキーを更新してください エッジ暗号化の設定 > 暗号化キーの設定 > デフォルトキーを設定.

手順

1. 移動先 エッジ暗号化の設定 > メンテナンス > 単一のキーローテーションをスケジュール.
2. 必要に応じて、フォームのフィールドに入力します。

フィールド	値
名前	内容を端的に表す名前を入力します。
ジョブタイプ	[単一のキー ローテーション] を選択します。
キー	廃止するキーを入力します。でこのキーがデフォルトキーではなくなったことを確認します エッジ暗号化の設定 > 暗号化キーの設定 > デフォルトキーを設定.
推定レコード数	処理するレコードの推定合計数。単一のキー ローテーションを実行しているときは使用できません。
履歴レコードを処理する	フィールドが監査されている場合は、監査テーブルの履歴レコードを処理するように選択します。監査テーブルのフィールドの履歴レコードを暗号化する場合、新しい値と古い値の両方が暗号化されます。 このフィールドは読み取り専用で有効です。 監査フィールドの詳細については、「監査」を参照してください。
推定最大監査レコード数	処理する監査対象レコードの推定最大数。単一のキー ローテーションを実行しているときは使用できません。
有効	このジョブを非アクティブ化する場合は、このチェックボックスをオフにします。
実行	ジョブの実行間隔を選択します。
開始中	ジョブを初めて実行する日時を入力します。

3. フォーム ヘッダーのメニュー アイコンをクリックし、[保存] を選択します。
監査対象フィールドを処理するときは [推定レコード数] はサポートされません。

一括キー ローテーション ジョブをスケジュールする

以前のキーで暗号化されたデータを検索し、現在のデフォルトの暗号化キーでデータを再暗号化するジョブをスケジュールします。データは復号化されてから、現在のデフォルトキーで再暗号化されます。

始める前に
必要なロール：security_admin

手順

1. 移動先 すべて > エッジ暗号化の設定 > メンテナンス > 一括キーローテーションをスケジュール.
2. 必要に応じて、フォームのフィールドに入力します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	値
名前	内容を端的に表す名前を入力します。
ジョブ タイプ	[一括キー ローテーション] を選択します。
推定レコード数	処理するレコードの推定合計数。一括キー ローテーションを実行しているときは使用できません。
履歴レコードを処理する	フィールドが監査されている場合は、監査テーブルの履歴レコードを処理するように選択します。監査テーブルのフィールドの履歴レコードを暗号化する場合、新しい値と古い値の両方が暗号化されます。 このフィールドは読み取り専用で有効です。 監査フィールドの詳細については、「監査」を参照してください。
推定最大監査レコード数	処理する監査対象レコードの推定最大数。一括キー ローテーションを実行しているときは使用できません。
有効	このジョブを非アクティブ化する場合は、このチェックボックスをオフにします。
実行	ジョブの実行間隔を選択します。
開始中	ジョブを初めて実行する日時を入力します。

3. フォーム ヘッダーのメニュー アイコンをクリックし、[保存] を選択します。
   監査対象フィールドを処理するときは [推定レコード数] はサポートされません。

添付ファイルのキー ローテーション ジョブをスケジュールする

指定したキー エイリアスを使用して暗号化された添付ファイルを検索し、現在のデフォルトの暗号化キーで添付ファイルを再暗号化するジョブをスケジュールします。添付ファイルは復号化されてから、デフォルトキーで再暗号化されます。

始める前に
必要なロール：security_admin

手順

1. 移動先 すべて > エッジ暗号化の設定 > メンテナンス > 添付ファイルのキーローテーションをスケジュール.
2. 必要に応じて、フォームのフィールドに入力します。

フィールド	値
名前	内容を端的に表す名前を入力します。
ジョブ タイプ	[添付ファイルのキー ローテーション] を選択します。
有効	このジョブを非アクティブ化する場合は、このチェックマークをオフにします。
テーブル	テーブルを選択します。
実行	ジョブの実行間隔を選択します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

フィールド	値
開始中	ジョブを初めて実行する日時を入力します。

3. フォーム ヘッダーのメニュー アイコンをクリックし、[保存] を選択します。
4. 更新するレコードの推定数を確認するには、[推定レコード数] をクリックします。
5. ジョブを直ちに実行するには、[今すぐ実行] をクリックします。

暗号化設定を使用したフィールドの暗号化

暗号化設定を作成してフィールドを暗号化します。

エッジ暗号化 の設定を行うには、プロキシ経由でインスタンスに接続する必要があります。本番インスタンスに変更を適用する前に、非本番インスタンスですべての変更をテストしてください。

暗号化キーの定義

1 つ以上のプロキシをセットアップし、デフォルトの暗号化キーを設定した後、すべてのプロキシがそのキーを使用できることがインスタンスによって確認されます。すべてのプロキシに暗号化キーが存在しない限り、その暗号化キーをデフォルトキーにすることはできません。デフォルトキーが定義されると、暗号化設定を作成できるようになります。

暗号化するフィールドと添付ファイルの割り当て

「暗号化するフィールドと添付ファイルを割り当てる」とは、フィールドまたは添付ファイルに暗号化タイプを割り当てることを意味します。フィールドを暗号化対象としてマークする前に、次の問題について検討してください。

- どのシステム機能が影響を受ける可能性があるかを判断します。
- すべてのスクリプトについてフィールドを使用していないかを調べます。
- フィールドのサイズを望ましいサイズに調整します。フィールドの暗号化設定を完了した後は、フィールドサイズを変更できません。

暗号化するフィールドをマークすると、暗号化データが格納されるように、フィールドサイズが拡張されます。テーブルのレコード数によってはフィールドサイズを拡張するプロセスに長時間かかることがあります。

API サポート

Column Level Encryption により、setDisplayValue() および setValue() API が更新され、暗号化されたフィールドに暗号化されたデータを挿入できるようになります。また、getDisplayValue() と getValue() がクリアテキスト値を返すようにもなります。

次のスクリプトは、インシデントの簡単な説明が暗号化されている場合の API の変更を示しています。

```
var gr = new GlideRecord('incident'); //creates a new incident
gr.setValue('short_description','test123'); //sets the value to test123
var sys_ID = gr.insert(); //inserts the record in the Incident table.
gs.info(gr.getValue('short_description')); //displays the unencrypted value
```

getValue() を使用して暗号化テキストを取得すると、スクリプトで暗号テキストを返されなくなります。スクリプトは、ユーザーが暗号化モジュールにアクセスできるという想定で、プレーンテキストを返します。ユーザーが暗号化モジュールにアクセスできない場合、getValue() は暗号テキストを返します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

フィールドの暗号化設定を作成する

暗号化するフィールドを選択し、暗号化タイプを特定します。

始める前に
必要なロール：security_admin

手順

1. 移動先 すべて > エッジ暗号化の設定 > 暗号化設定 > 新規作成.
2. フォームを完了します。

フィールド	説明
テーブル	暗号化するフィールドが含まれているテーブル。
タイプ	テーブルの列を暗号化するか、テーブルの添付ファイルを暗号化するか。[列] を選択します。
列	暗号化するフィールド。[タイプ] が [列] の場合にのみ表示されます。 文字列、日付、日付/時刻、ジャーナル、ジャーナル入力、および URL フィールドのみがサポートされます。 ○ 文字列および **URL** フィールド：親テーブルまたは子テーブルに暗号化設定を追加できます。 ○ 日付および日付/時刻フィールド：親テーブルのみに暗号化設定を追加できます。子テーブルには、新しい暗号化設定を追加できません。 **注:** 暗号化している日付および日付/時刻フィールドの影響を受けるレコード数に応じて、暗号化設定の作成には数分かかることがあります。インスタンスのトランザクション量が低いときは、日付および日付/時刻フィールドの暗号化設定を作成してください。
暗号化タイプ	使用する暗号化タイプ。

注:
特定のテーブルとフィールドの組み合わせには、一度に 1 つの有効な設定のみを持たせることができます。

3. [送信] をクリックします。

次のタスク
暗号化設定レコードを追加したら、既存のデータを暗号化する暗号化ジョブを作成できます。暗号化ジョブを実行しない場合は、次回のデータ変更時に Edge によって既存のデータが暗号化されます。詳細については、「暗号化ジョブをスケジュールする」を参照してください。

変数暗号化設定を作成する

暗号化するサービスカタログ変数を選択し、暗号化タイプを特定します。

始める前に
必要なロール：security_admin

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. 移動先 すべて > エッジ暗号化の設定 > 変数暗号化設定.
2. **[Edge Encryption** の変数設定] リストで、[新規] をクリックします。
3. フォームに入力します。

フィールド	説明
変数	暗号化する変数。
暗号化タイプ	使用する暗号化タイプ。

4. [送信] をクリックします。

次のタスク
暗号化設定レコードを追加したら、既存のデータを暗号化する暗号化ジョブを作成できます。暗号化ジョブを実行しない場合は、次回のデータ変更時に Edge によって既存のデータが暗号化されます。詳細については、「暗号化ジョブをスケジュールする」を参照してください。

暗号化設定を非アクティブ化する

暗号化するフィールドまたはテーブルの添付ファイルを設定した後で、暗号化設定を無効にして暗号化を停止することができます。暗号化を無効にした後、「フィールドの復号化ジョブ」または「添付ファイルの添付ファイル復号化ジョブ」を実行して、暗号化データをインスタンスから削除することができます。

始める前に
必要なロール：security_admin

このタスクについて

警告:
暗号化設定を無効にしても暗号化レコードは削除されず、暗号化タイプは変更できません。

手順

1. 移動先 エッジ暗号化の設定 > エッジ暗号化構成 > すべて.
   [Edge Encryption の設定] リストが表示されます。
2. 無効にする暗号化設定をクリックします。
   [Edge Encryption の設定] フォームが表示されます。
3. [有効] ボックスをクリックします。
   [有効] ボックスがクリアーされます。
4. [更新] をクリックします。
   [Edge Encryption の設定] リストが表示されます。

次のタスク
復号化ジョブまたは添付ファイルの復号化ジョブを実行して、インスタンスのデータを復号化することができます。ジョブを実行しない場合は、次回の変更時に暗号化データが復号化されます。

暗号化ジョブをスケジュールする

フィールドに設定されたデフォルトの暗号化キーを使用して、指定したフィールドの暗号化されていないデータを検索して暗号化するジョブをスケジュールできます。フィールドを暗号化対象として設定した後に暗号化ジョブを作成しない場合は、新しい値のみが暗号化されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

始める前に
必要なロール：security_admin

手順

1. 移動先 エッジ暗号化の設定 > 暗号化設定 > すべて フィールドのジョブを作成するか、または エッジ暗号化の設定 > 変数暗号化設定 をクリックして、変数のジョブを作成します。
2. 暗号化ジョブをスケジュールするフィールドをクリックします。
3. [関連リンク] で、[一括暗号化ジョブをスケジュール] をクリックします。

   [スケジュール設定済みの暗号化ジョブ] フォームが表示され、すべてのフィールドが入力されます。フォームの下部には、以前のジョブの実行があった場合のレコードが表示されます。
4. 必要に応じて、フォームのフィールドに入力します。

フィールド	値
名前	内容を端的に表す名前を入力します。
有効	このジョブを非アクティブ化する場合は、このチェックボックスをオフにします。
ジョブタイプ	[暗号化] を選択します。
テーブル	テーブルを選択します。
列	列を選択します。
推定レコード数	処理するレコードの推定総数です。[推定レコード数] を選択後に入力します。
履歴レコードを処理する	フィールドが監査されている場合は、監査テーブルの履歴レコードを処理するように選択します。監査テーブルのフィールドの履歴レコードを暗号化する場合、新しい値と古い値の両方が暗号化されます。 監査フィールドの詳細については、「監査」を参照してください。
推定最大監査レコード数	処理する監査レコードの推定最大数です。[推定レコード数] を選択後に入力します。このフィールドは、[履歴レコードを処理する] が選択されている場合にのみ表示されます。 **注:** 推定数は、実際に処理されたレコードの数よりも大きくなる場合があります。
実行	ジョブの実行間隔を選択します。
開始中	ジョブを初めて実行する日時を入力します。

5. フォーム ヘッダーのメニュー アイコンをクリックし、[保存] を選択します。
6. 更新するレコードの推定数を確認するには、[推定レコード数] をクリックします。
7. ジョブを直ちに実行するには、[今すぐ実行] をクリックします。

復号化ジョブをスケジュールする

暗号化されたフィールドのデータを復号化し、インスタンスにクリアー データを格納するジョブをスケジュールできます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

始める前に

注:
復号化ジョブを実行するには、フィールドの暗号化レコードを非アクティブとしてマークする必要があります ([有効] ボックスをクリアーします)。

必要なロール：security_admin

手順

1. 移動先 エッジ暗号化の設定 > 暗号化設定 > すべて フィールドのジョブを作成するか、または エッジ暗号化の設定 > 変数暗号化設定 をクリックして、変数のジョブを作成します。
2. 復号化するフィールドをクリックします。
3. [関連リンク] で、[一括復号化ジョブをスケジュール] をクリックします。

   [スケジュール設定済みの暗号化ジョブ] フォームが表示され、すべてのフィールドが入力されます。フォームの下部には、以前のジョブの実行があった場合のレコードが表示されます。
4. 必要に応じて、フォームのフィールドに入力します。

フィールド	値
名前	内容を端的に表す名前を入力します。
ジョブタイプ	[復号化] を選択します。
有効	このジョブを非アクティブ化する場合は、このチェックボックスをオフにします。
テーブル	テーブルを選択します。
列	列を選択します。
推定レコード数	処理するレコードの推定総数です。[推定レコード数] を選択後に入力します。
履歴レコードを処理する	フィールドが監査されている場合は、監査テーブルの履歴レコードを処理するように選択します。監査テーブルのフィールドの履歴レコードを暗号化する場合、新しい値と古い値の両方が暗号化されます。 監査フィールドの詳細については、「監査」を参照してください。
推定最大監査レコード数	処理する監査レコードの推定最大数です。[推定レコード数] を選択後に入力します。このフィールドは、[履歴レコードを処理する] が選択されている場合にのみ表示されます。 注: 推定数は、実際に処理されたレコードの数よりも大きくなる場合があります。
実行	ジョブの実行間隔を選択します。
開始中	ジョブを初めて実行する日時を入力します。

5. フォーム ヘッダーのメニュー アイコンをクリックし、[保存] を選択します。
6. 更新するレコードの推定数を確認するには、[推定レコード数] をクリックします。
7. ジョブを直ちに実行するには、[今すぐ実行] をクリックします。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

標準暗号化を使用して添付ファイルを暗号化する

特定のテーブルについて添付ファイルを暗号化できます。

テーブルに対するすべての添付ファイルには同じ暗号化タイプが使用されます。テキスト検索を実行するときに、暗号化された添付ファイルは検索されません。添付ファイルには標準の暗号化タイプのみ使用できます。順序保存または等価性保存の暗号化タイプは使用できません。

エッジ暗号化 プロキシをバイパスするセッションの場合は次のようになります。

- 添付ファイルの暗号化を有効にしたレコード：
  - ユーザーは、添付ファイルと添付ファイル名が存在することを確認できます。
  - ユーザーは、新しい添付ファイルを追加できません。
- 添付ファイルの暗号化を有効にしていないレコード：
  - ユーザーは、既存の添付ファイルを開いてダウンロードできます。
  - ユーザーは、新しい添付ファイルを追加できます。

暗号化プロキシを使用するセッションの場合、ユーザーは、既存の添付ファイルを開いてダウンロードでき、新しい添付ファイルを追加できます。

添付ファイルの暗号化を設定する

その添付ファイルを暗号化するテーブルを選択して、暗号化タイプを特定します。

始める前に

必要なロール：security_admin

手順

1. 移動先 すべて > エッジ暗号化の設定 > エッジ暗号化構成 > 新規作成.
2. 必要に応じて、フォームのフィールドに入力します。

Edge Encryption の設定

フィールド	説明
テーブル	その添付ファイルを暗号化するテーブルを選択します。
タイプ	テーブルの列を暗号化するか、テーブルの添付ファイルを暗号化するか。[添付ファイル] を選択します。
列	暗号化するテーブル フィールド。 このフィールドは、[タイプ] が [列] の場合に表示され、[タイプ] が [添付ファイル] の場合は表示されません。
暗号化タイプ	使用する暗号化タイプ。添付ファイルの場合は、標準 AES128 と標準 AES256 のみが使用できます。

3. [送信] をクリックします。

次のタスク

暗号化レコードを追加したら、既存の添付ファイルを暗号化する添付ファイルの暗号化ジョブを作成できます。添付ファイルの暗号化ジョブを実行しない場合は、新しい添付ファイルを添付したときに添付ファイルが暗号化されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

> **注:**
> テーブルの [コレクションディクショナリー] エントリで *edge_encryption_clear_attachment_allowed* 属性 を **True** にマークすると、Edge Encryption で暗号化されていない添付ファイルがテーブルに追加されます。この属性を有効にする場合は、「添付ファイルの暗号化ジョブ」をセットアップして、追加された暗号化されていない添付ファイルが暗号化されるようにする必要があります。

添付ファイルの暗号化ジョブをスケジュールする

テーブルに設定されたデフォルトの暗号化キーを使用して、指定したテーブルの暗号化されていない添付ファイルを検索して暗号化するジョブをスケジュールできます。

始める前に
必要なロール：security_admin

手順

1. 移動先 エッジ暗号化の設定 > 暗号化設定 > すべて.
2. 暗号化ジョブをスケジュールするテーブルをクリックします。
3. [関連リンク] で、[一括暗号化ジョブをスケジュール] をクリックします。

   [スケジュール設定済みの暗号化ジョブ] フォームが表示され、すべてのフィールドが入力されます。フォームの下部には、以前のジョブの実行があった場合のレコードが表示されます。
4. 必要に応じて、フォームのフィールドに入力します。

フィールド	値
名前	内容を端的に表す名前を入力します。
有効	このジョブを非アクティブ化する場合は、このチェックボックスをオフにします。
ジョブ タイプ	[添付ファイルの暗号化] を選択します。
テーブル	テーブルを選択します。
実行	ジョブの実行間隔を選択します。
開始中	ジョブを初めて実行する日時を入力します。

5. フォーム ヘッダーのメニュー アイコンをクリックし、[保存] を選択します。
6. 更新するレコードの推定数を確認するには、[推定レコード数] をクリックします。
7. ジョブを直ちに実行するには、[今すぐ実行] をクリックします。

添付ファイルの復号化ジョブをスケジュールする

指定したテーブルの暗号化された添付ファイルを復号化し、クリアーな添付ファイルをインスタンスに格納するジョブをスケジュールできます。

始める前に

> **注:**
> 復号化ジョブを実行する前に、テーブルの暗号化レコードを非アクティブとしてマークする必要があります ([有効] ボックスをクリアーします)。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

必要なロール：security_admin

手順

1. 移動先 エッジ暗号化の設定 > 暗号化設定 > すべて.
2. 復号化する添付ファイルを持つテーブルをクリックします。
3. [関連リンク] で、[一括添付ファイル復号化ジョブをスケジュール] をクリックします。

   [スケジュール設定済みの暗号化ジョブ] フォームが表示され、すべてのフィールドが入力されます。フォームの下部には、以前のジョブの実行があった場合のレコードが表示されます。
4. 必要に応じて、フォームのフィールドに入力します。

フィールド	値
名前	内容を端的に表す名前を入力します。
ジョブ タイプ	[添付ファイルの復号化] を選択します。
有効	このジョブを非アクティブ化する場合は、このチェックマークをオフにします。
テーブル	テーブルを選択します。
実行	ジョブの実行間隔を選択します。
開始中	ジョブを初めて実行する日時を入力します。

5. フォーム ヘッダーのメニュー アイコンをクリックし、[保存] を選択します。
6. 更新するレコードの推定数を確認するには、[推定レコード数] をクリックします。
7. ジョブを直ちに実行するには、[今すぐ実行] をクリックします。

フィールドまたは添付ファイルの暗号化タイプを変更する

フィールドまたは添付ファイルの暗号化タイプを変更するには、既存の暗号化設定レコードで新しい暗号化タイプを選択します。特定のテーブルとフィールドの組み合わせには、一度に 1 つの有効な設定のみを持たせることができます。

始める前に
必要なロール：security_admin

手順

1. 移動先 エッジ暗号化の設定 > 暗号化設定 > すべて.
   [Edge Encryption の設定] リストが表示されます。
2. 暗号化設定を変更するレコードを開きます。
3. [暗号化タイプ] ドロップダウンをクリックし、新しい暗号化タイプを選択します。

   注:
   添付ファイルの場合は、標準 AES128 と標準 AES256 のみが使用できます。
4. 必要に応じて、暗号化または添付ファイルの暗号化ジョブを実行します。
   暗号化ジョブを実行する必要はありません。暗号化ジョブを実行しない場合、フィールドまたは添付ファイルは、次回フィールドまたは添付ファイルが変更されたときに新しい暗号化タイプを使用して暗号化されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

暗号化パターンを使用して文字列をトークン化する

文字列パターンをトークンに置き換え、それからトークンをインスタンスに送信して格納することができます。

始める前に

暗号化パターンを使用するには、ネットワークに MySQL データベースをインストールしてセットアップする必要があります。これは、順序保存の暗号化に使用されるものと同じデータベースです。暗号化パターンを作成または編集するには、プロキシ経由でインスタンスに接続する必要があります。

必要なロール：security_admin

このタスクについて

ベース システムのパターンを使用するか、独自のパターンを作成できます。ベースシステムのパターンは詳細パターンです。暗号化パターンには次の制限があります。

- すべてがアルファベット文字のパターンは使用できません。
- 最小パターン サイズは 5 文字です。システムプロパティを使用してこの設定を変更することができます。
- 暗号化パターンでは * および + の数量指定子は禁止されています。
- 暗号化パターンは、完全な単語に一致し、より大きい文字列に埋め込まれた文字列の一部分には一致しません。単語は、パターンに含めることができない空白と文字で定義されます。
- 同じ文字列が複数回インスタンスに送信された場合は、同じトークンに置き換えられます。
- 完全一致のテキスト検索がサポートされています。クエリー文字列は、インスタンスに送信されたときにトークンと交換され、トークンに対して検索が実行されます。検索結果がプロキシサーバーに返されると、トークンがクリアー テキストに置き換えられます。語幹解釈などの機能はサポートされていません。

パターンを使用しているときは、クリアー テキストがネットワークの外に出ることは決してありません。インスタンスに送られる要求の中で、プロキシサーバーがパターンを照合するときに、プロキシによって文字列が同じサイズのトークンに置き換えられます。このトークンが、クリアー テキスト文字列の代わりにインスタンスに送られます。インスタンスからプロキシサーバーに応答が送られるときは、プロキシによってトークンが文字列に置き換えられます。この文字列は、プロキシサーバーを介して表示されるときにクリアー テキストとして表示されます。

注:
暗号化されたフィールドでは暗号化パターンのチェックは行われません。

手順

1. 移動先 すべて > エッジ暗号化の設定 > 暗号化パターン > 新規作成.
   または、[詳細パターン] に移動して、事前設定されたパターンを有効化または編集することもできます。
2. パターン名を入力します。
3. [エッジ パターン入力タイプ] を定義します。

オプション	説明
基本	一連の文字タイプ。[基本パターンの入力] タブで、[追加] をクリックし、文字タイプを選択します。 文字が追加されるたびに [サンプル パターン] にパターンが表示されます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

オプション	説明
	[新規ブロック] をクリックし、次の文字を次の行に移動します。これで、文字を長いパターンにグループ化できます。 パターンの最後の文字を削除するには **[X]** をクリックします。
詳細	Java の正規表現式。[詳細] を選択した場合、入力タイプを [基本] に戻すことはできません。 [サンプルの一致] フィールドに、正規表現式をテストするためのサンプル パターンを入力します。[パターン] フィールドに、Java の正規表現式を入力します。[検証] をクリックし、式がサンプル パターンと一致することを検証します。

入力タイプは、パターンの入力方法を定義するものです。パターンの使用方法には影響を与えません。

4. [送信] をクリックします。

順序保存の暗号化データの修復または復元

security-admin ロールを持っている場合、 エッジ暗号化 プロキシにより実行され、順序保存の暗号化を使用しているフィールドを修復または復元するジョブをスケジュールできます。

ジョブを次のようにスケジュールします。

- 順序トークンを修復する。
- プロキシデータベースを再作成する。

これらのジョブの実行には時間がかかる場合があり、エッジ暗号化 プロキシのパフォーマンスに影響することがあります。週末の深夜など、システムを使用しているユーザーがまったくいないか最小限の数であるときに、これらのジョブをスケジュールしてください。

順序トークンの修復ジョブをスケジュールする

順序トークンが失われているフィールドを検索して修復するジョブをスケジュールできます。

始める前に
必要なロール：security_admin

このタスクについて
これらのジョブを使用して、テーブル内の個々のフィールドを修復したり、順序保存の暗号化を使用しているすべてのフィールドを修復したりします。このジョブは、インスタンスの実行中にプロキシデータベースがオフラインになったときに実行します。そのようにすると、順序トークンが失われている順序保存のフィールドが得られます。

手順

1. 移動先 すべて > エッジ暗号化の設定 > メンテナンス > 順序トークンの修復をスケジュール.
2. 必要に応じて、フォームのフィールドに入力します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	値
名前	内容を端的に表す名前を入力します。
ジョブ タイプ	[順序トークンの修復] を選択します。
すべてのフィールド	すべてのテーブルを修復するには、このチェック ボックスをオンにします。
テーブル	テーブルを選択します。
列	列を選択します。
有効	このジョブを非アクティブ化する場合は、このチェックボックスをオフにします。
実行	ジョブの実行間隔を選択します。
開始中	ジョブを初めて実行する日時を入力します。

3. フォーム ヘッダーのメニュー アイコンをクリックし、[保存] を選択します。
4. 更新するレコードの推定数を確認するには、[推定レコード数] をクリックします。

プロキシ データベースの復元ジョブをスケジュールする

このジョブは、プロキシ データベースがデータを失ったときに実行します。このジョブは、トークン (順序保存の暗号化タイプ) で暗号化されたすべてのレコードを検索し、それらをプロキシに送信して、プロキシ データベースを再構築できるようにします。

始める前に
必要なロール：security_admin

手順

1. 移動先 すべて > エッジ暗号化の設定 > メンテナンス > データベースの復元をスケジュール.
2. 必要に応じて、フォームのフィールドに入力します。

フィールド	値
名前	このジョブの内容を端的に表す名前を入力します。
ジョブ タイプ	[データベースの復元] を選択します。
有効	このジョブを非アクティブ化する場合は、このチェックボックスをオフにします。
実行	ジョブの実行間隔を選択します。
開始中	このジョブを初めて実行する日時を入力します。

3. フォーム ヘッダーのメニュー アイコンをクリックし、[保存] を選択します。
4. 更新するレコードの推定数を確認するには、[推定レコード数] をクリックします。

IP アドレス拒否リストを設定する

ネットワーク内の IP アドレスがインスタンスに要求を送信しないようにする

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

始める前に
必要なロール：security_admin
エッジ暗号化 プロキシサーバーはネットワークに常駐しているため、ネットワーク ソフトウェアによる脆弱性スキャンの影響を受ける場合があります。IP スキャナーまたは他の要求が ServiceNow インスタンスに転送されるのを防ぐために、IP アドレス、IP 範囲、またはネットワークマスクを拒否リストに追加できます。拒否リストにあるアドレスからのプロキシサーバーへの接続はすべて終了させられ、インスタンスには転送されません。

IP アドレスを拒否リストに登録するには、プロキシサーバー経由でインスタンスにログインする必要があります。

重要:
ネットワークの IP アドレスを拒否リストに登録する際は、事前にネットワークトポロジについての知識が必要です。IP アドレスを拒否リストに追加した場合、その IP アドレスを持つユーザーはすべて、エッジ暗号化 プロキシサーバーへのアクセスがブロックされます。

手順

1. 移動先 すべて > エッジ暗号化の設定 > メンテナンス > 拒否リスト **IP** アドレス.
   暗号化プロキシ IP 拒否リスト [edge_encryption_ip_blacklist] リストビューが開きます。
2. [新規] をクリックします。
3. フォームに入力します。

フィールド	説明
プロキシサーバー	拒否リストに登録されたアドレスからの要求を転送できないようにする エッジ暗号化 プロキシサーバーです。
IP、IP 範囲、またはネットマスク	この IP アドレス、範囲、またはネットワーク マスクからの要求が ServiceNow インスタンスに転送されません。値の例を次に示します。 ○ IP アドレス：10.10.10.5 ○ IP 範囲：10.10.10.1-15 ○ ネットワーク マスク：10.10.10.0/24 **注:** IPv4 または IPv6 アドレスのいずれかを使用できます
有効	レコードが有効かどうか。有効なレコードからの IP アドレスのみが、インスタンスに要求を送信できなくなります。
説明	拒否リストレコードの説明です。

4. [送信] をクリックします。
5. IP アドレスを拒否リストに登録する必要がある他のすべてのプロキシについて、上記の手順を繰り返します。

タスクの結果
エッジ暗号化 プロキシサーバーは、拒否リストに登録された IP アドレス、範囲、またはネットワークマスクからの接続を終了し、要求をインスタンスに転送できません。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

レコードプロデューサーからのデータの暗号化

レコードプロデューサーレコードから暗号化ルールを作成し、レコードプロデューサーからの挿入を許可するように エッジ暗号化 プロキシサーバーを設定します。

始める前に

必要なロール：security_admin
レコードプロデューサーを使用すると、エンドユーザーはインシデントレコードなどのタスクベースのレコードをサービスカタログおよびサービスポータルから作成できます。レコードプロデューサーが、暗号化対象としてマークされたフィールドにデータを挿入しようとすると、無効な挿入のメッセージが表示され、データはフィールドに保存されません。

レコードプロデューサーからのデータを暗号化するには、ターゲットフィールドに対して暗号化設定を定義する必要があります。レコード プロデューサーから暗号化ルールを作成する前に、ターゲットフィールドとテーブルの暗号化設定を作成済みであることを確認してください。「フィールドの暗号化設定を作成する」を参照してください。レコード プロデューサーから添付ファイルを暗号化するには、「添付ファイルの暗号化を設定する」の手順を実行します。

手順

1. エッジ暗号化 プロキシサーバー経由でインスタンスにログインします。
2. 移動先 サービスカタログ > カタログ定義 > レコードプロデューサー.
3. レコードプロデューサーレコードを作成 するか、既存のレコードプロデューサーレコードを開きます。
4. [関連リンク] で、**[Edge Encryption のルールを作成]** を選択します。
   暗号化対象としてにマークされたフィールドにレコード プロデューサーから送信されたデータを暗号化するための、2 つの非アクティブな暗号化ルールが自動的に作成されます。

暗号化ルール	説明
<RecordProducerName>	サービスカタログからの POST パラメーターを処理し、インスタンス内のフィールドに変数をマップするために作成されたルール。
<RecordProducerName>Json	サービスポータルからの JSON ペイロードを処理し、インスタンス内のフィールドに変数をマップするために作成されたルール。

5. レコード プロデューサーによって作成された必要な暗号化ルールを有効にします。
   a. 移動先 エッジ暗号化の設定 > ルール > すべて.
   b. レコード プロデューサーの使用場所に応じて、レコード プロデューサーによって作成された関連する暗号化ルールを開き、[有効] フラグを選択します。
      レコード プロデューサーをサービスカタログで使用する場合は、<RecordProducerName> 暗号化ルールを有効にします。レコード プロデューサーをサービスポータルで使用する場合は、<RecordProducerName>Json 暗号化ルールを有効にします。
6. オプション: 暗号化ルールの [アクション] フィールドを調べ、必要なフィールド名またはステートメントがあれば追加します。

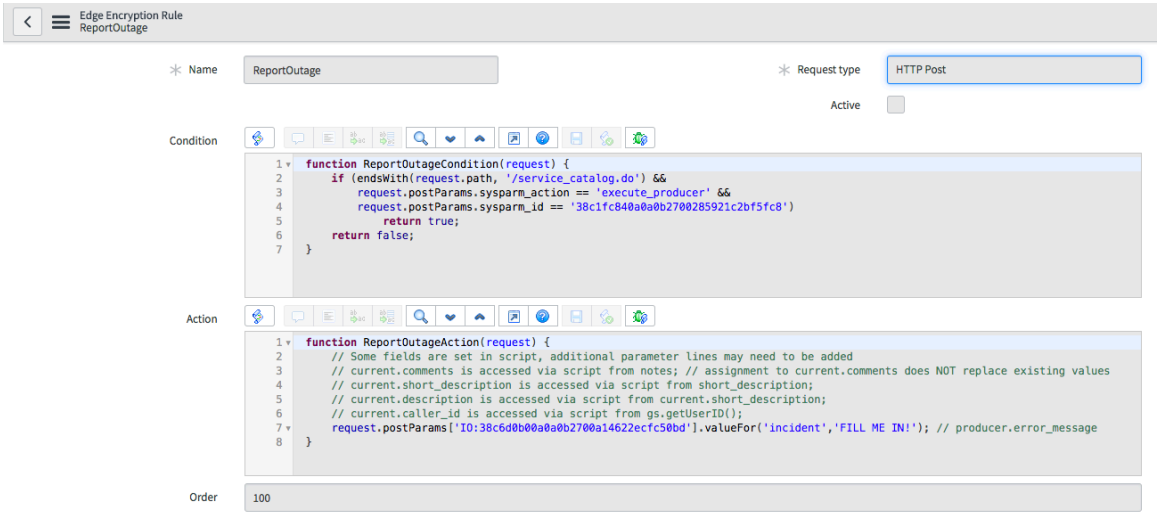
   (Optional) レコード プロデューサーが変数をテーブルのフィールドに直接マップする場合は、暗号化ルールによって変数が正しいフィールドに自動的にマップされます。ただし、変数がプラットフォームのさまざまなスクリプトを介して間接的にマップされる場合は、それぞれの変数が正しいフィールドにマップされるように、状況に応じてルールを更新する必要があります。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

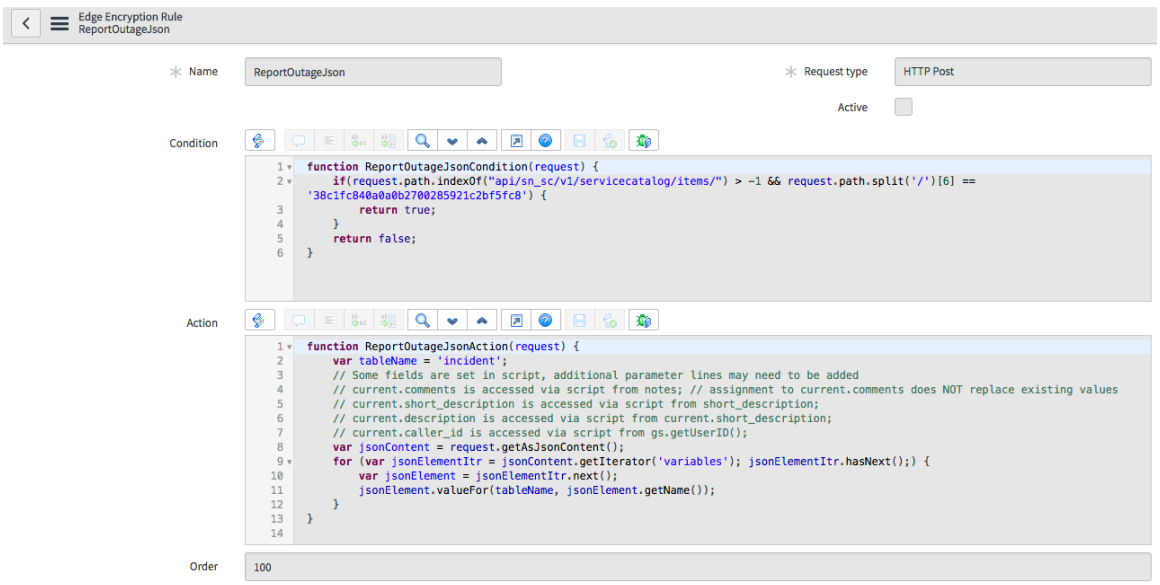
自動翻訳

Example

(Optional) 次の暗号化ルールはレポート機能停止レコード プロデューサーから作成されたもので、サービスカタログからの POST パラメーターを処理してインスタンス内のフィールドに変数をマップします。'FILL ME IN' の部分をターゲットフィールドに置き換えます。



次の暗号化ルールはレポート機能停止レコード プロデューサーから作成されたもので、サービスポータルからの JSON ペイロードを処理してインスタンス内のフィールドに変数をマップします。スクリプト化された変数をターゲットフィールドにマップするステートメントを追加します。



レコード プロデューサーからのペイロードを調べてみると、error_message 要素に short_description フィールドの値が格納されています。次のステートメントを追加することで、スクリプト化された変数 error_message を short_description フィールドにマップできます。

```
if (jsonElement.getName() == 'error_message')
      jsonElement.valueFor(tableName, 'short_description');
```

[アクション] フィールドの値は次のようになります。

```
function ReportOutageJsonAction(request) {
 var tableName = 'incident';
```

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

```
// Some fields are set in script, additional parameter lines may need to be added
// current.comments is accessed via script from notes; // assignment to current.comments
does NOT replace existing values
// current.short_description is accessed via script from short_description;
// current.description is accessed via script from current.short_description;
// current.caller_id is accessed via script from gs.getUserID();
var jsonContent = request.getAsJsonContent();
for (var jsonElementItr = jsonContent.getIterator('variables'); jsonElementItr.hasNext();) {
 var jsonElement = jsonElementItr.next();
 if (jsonElement.getName() == 'error_message')
  jsonElement.valueFor(tableName, 'short_description');
            } else {
        jsonElement.valueFor(tableName, jsonElement.getName());
}
}
```

タスクの結果
2 つの暗号化ルールにより、サービスカタログとサービスポータルのどちらでも、暗号化対象としてマークされたフィールドにレコード プロデューサーから値を挿入できます。

カスタムの暗号化ルールを定義する

場合によっては、HTTP 要求の中で、要求がインスタンスに送られる途中で機密情報を特定して暗号化する必要があります。このような要求のデータを識別、解釈し、暗号化するための暗号化ルールを記述して、要求内のフィールドをインスタンスのテーブルフィールド名にマップすることができます。

暗号化ルールとは

暗号化ルールは、エッジ暗号化 プロキシサーバーで実行され、要求内のフィールドを ServiceNow インスタンス上のテーブル内のフィールドにマップするスクリプトです。暗号化ルールでは、カスタム ペイロードでのデータの暗号化方法を エッジ暗号化 プロキシサーバーに指示します。

注:
暗号化ルールでは ECMAScript 3 またはそれ以前のみがサポートされています。

どのような場合にカスタム ルールを使用するか

エッジ暗号化 プラグインの一部として、1 組の暗号化ルールが組み込まれています。これらのルールは、次のような多くのコアプラットフォームのユースケースを処理します。

- リスト編集フォームからのフィールドの編集
- レコードフォームからのレコードの更新
- ダイレクト Web サービスの管理
- REST アプリケーションプログラムインターフェイス (API) からのデータの処理

標準のフォームとリストを使用して作成されたアプリケーションは、カスタム暗号化ルールがなくても機能します。

暗号化を必要とするデータが含まれているスクリプトを開発する場合は、データを検索して Glide テーブルフィールド名にマップするための暗号化ルールを作成します。例：

- スクリプトプロセッサー
- スクリプト化 Web サービス
- Scripted REST API、UI、または Ajax スクリプト

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

暗号化ルールの形式

ルールには 3 つの要素が含まれています。

- 条件：要求のタイプを識別します。
- アクション：要求内のフィールドをテーブル内のフィールドにマップし、暗号化設定が定義されたフィールドにマップされる値を暗号化します。
- 順序：ルールの優先度。優先度が最も低く、条件が満たされたルールのみが実行されます。ビジネスルールと同様に、ルールは最低から最高の順に実行されます。

添付ファイル要求を除き、HTTP 要求は エッジ暗号化 プロキシサーバーによって評価されます。エッジ暗号化 プロキシサーバーは、すべての条件が False を返すか、または 1 つの条件が True を返すまで、暗号化ルールのすべての条件を優先度順に評価します。条件が True を返すと、要求に対してアクションが実行され、結果がインスタンスに転送されます。他の条件は評価されません。したがって、暗号化ルールの条件はできるだけ具体的にする必要があります。汎用的なルールでは、別のルールによる処理を想定した要求に対して True と評価され、正しくないアクションによって要求が処理される可能性があります。汎用的な条件が避けられない場合は、より具体的なルールが先に評価されるように、ルールを高い優先度の値でマークする必要があります。

暗号化ルールを作成する際のガイドライン

効率的で最適化された暗号化ルールを作成することで、スクリプトの検証処理の時間を短縮できます。

全体的なガイドライン：ルールが長くなる場合は、ブロック数を最小限に抑え、可能な限りルールを分割してください。理想的には、カスタムルールで複数のケースを網羅するのではなく、特定のユースケースに適用し、アクションスクリプトで if ステートメントや switch ステートメントを使用します。

1. ルールを可能な限り分割します。例を次に示します。
   - テーブルごとに異なるルールを作成し、それぞれのルールがそれぞれのテーブルでのみ実行されるようにします。
   - ターゲットとするレコードプロデューサーごとに、または少なくともレコードプロデューサーのサブセットごとに、異なるルールを作成します。1 つのルールで数十もの sys_ids を対象にするのではなく、より少数のレコードプロデューサーを対象にした複数の異なるルールを作成できます。sys_id ごとに 1 つずつルールを作成することもできます。

     注:
     複数のルールを作成すると、それだけ多くのメンテナンスが必要になります。複数のシンプルなルールの方が、長く複雑なルールよりも効率的に検証できます。

2. ブロック数を最小限に抑えます。スクリプトの評価中は処理エンジンによって個々のブロックがスキャンされます。そのため、ブロックが多数あると検証が遅れる原因になります。例を次に示します。
   - すべての if ブロックを配列参照に置き換え、配列参照内のすべてのブロックをただ 1 つの if ブロックに置き換えます。
   - 可能な限り、if ブロックを結合してグループ化します。

暗号化ルール **API**

暗号化ルールは JavaScript で記述されており、エッジ暗号化 の API を利用して、要求の本体に含まれている機密情報を検索して暗号化します。API は、xPath に似た式を使用して、JSON と XML の両方のコンテンツを参照します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

エッジ暗号化 API は、要求が出力ストリームに書き込まれているときはストリームから離れて要求を処理します。ストリームを解析することにより、暗号化ルールをネットワークで実行することができます。ただし、本体から複数回コンテンツを取得して解析した場合、予期しない結果につながる可能性があります。この潜在的な問題を回避するには、アクションによる要求の処理は 1 回のパスで行う必要があります。

暗号化ルールを作成する際、Glide API、スクリプトインクルード、ビジネス ルール、または `current` などのグローバルパラメーターは使用できません。ルールは HTTP オブジェクトに対して作成されるため、グローバルの `request` オブジェクトを使用できます。

暗号化ルールを作成する際は、許可リストマネージャーやスコープ対象のアプリケーションから API を使用することはできません。

エラー処理

暗号化ルールの条件またはアクションから例外がスローされた場合は、プロキシのログでトラブルシューティング情報がないか確認してください。

クライアント要求を調べる

カスタムの暗号化ルールを作成する前に、エッジ暗号化 プロキシサーバーに入力されるクライアント要求の形式を決定する必要があります。

始める前に

必要なロール：admin

このタスクについて

暗号化ルールは、クライアント要求に対して繰り返され、状況に応じて何を暗号化する必要があるかを判断するので、作成するルールの対象となる要求のタイプについて理解する必要があります。クライアント要求の形式によって、暗号化ルールの構造と、ルールで使用できる API が決まります。

手順

1. クライアント要求を調べます。

   要求のソースに応じて、次のツールを利用して要求を調べ、形式を判断することができます。

要求のソース	利用可能なツール
クライアント ブラウザー	ブラウザーの開発者用コンソールを使用して、クライアント要求を調べます。次のツールが役に立ちます。 ○ Firefox ネットワーク モニター ○ Chrome ネットワーク パネル
サードパーティ/外部ソース	HTTP プロトコル アナライザーを使用して要求を調べます。次のツールが役に立ちます。 ○ Wireshark ○ HTTP Scoop

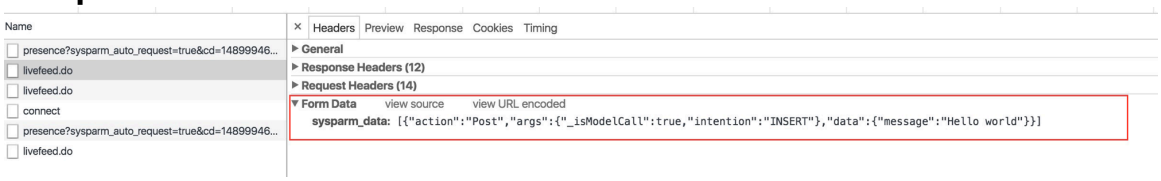
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

要求のソース	利用可能なツール
	または多くの場合、外部ソースのドキュメントを使用して要求の形式を判断することもできます。

2. クライアント要求から、パケットを調べて次のものを判断します。
   - クライアント要求のメソッド
   - 要求の URL パス
   - URL パラメーター
   - POST パラメーター (存在する場合)
   - 要求本体の形式 (含まれている場合)

Example



タスクの結果

要求を調べることで、暗号化ルールの中でフィルタリングや反復処理を必要とするフィールドを把握できます。*request* オブジェクトのフィールドを理解するには、「要求」を参照してください。

暗号化ルールを作成する

暗号化ルールは、HTTP 要求の中で暗号化する必要のある内容を検索するために、プロキシによって使用されます。

始める前に

必要なロール：security_admin
暗号化ルールを作成する前に、「クライアント要求を調べる」の手順を実行して形式を決める必要があります。

このタスクについて

暗号化ルールを作成または編集するには、暗号化プロキシ経由でインスタンスに接続する必要があります。

手順

1. 移動先 すべて > エッジ暗号化の設定 > ルール > 新規作成.
2. [名前] ボックスに名前を入力します。
3. [要求タイプ] で HTTP メソッドを選択します。
   - **HTTP POST**
   - **HTTP Get**
   - **HTTP PUT**
   - **HTTP Patch**
   - **HTTP Delete**

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

> **注:**
> Jakarta 以前のインスタンスでは **[HTTP Get]** メソッドと **[HTTP Post]** メソッドのみを使用できます。

4. [条件] ボックスに、どの場合にルールを実行するかを定義する JavaScript ステートメントを入力します。
5. [アクション] ボックスに、条件が True のときに実行する JavaScript 関数を入力します。
6. [順序] ボックスに、ルールの相対的な優先度を入力します。
7. [送信] をクリックするか、フォームを保存します。

暗号化ルールの条件

暗号化ルールの条件は、ルールを実行する必要があるかどうかを決定します。

ルールにより HTTP 要求を処理する必要がある場合は、暗号化ルールの条件が True を返す必要があります。それ以外の場合は False を返す必要があります。

条件を作成する際は、要求ごとに 1 つのルールしか実行されないことに注意してください。そのため、意図した状況の下で実行されるように、必要に応じて条件を汎用的にしたり具体的にしたりする必要があります。

> **注:**
> 条件内の内容のチェックを実行するときは注意が必要です。過度のチェックはプロキシサーバーに大きな負荷がかかることがあります。また、複雑な要求を処理するときに遅延が増大する要因となる場合があります。

条件では、メソッドのタイプ、コンテンツ タイプ、URL パス、または URL クエリー文字列パラメータを使用して、ルールで要求を処理する必要があるかどうかを判断できます。条件からは、要求オブジェクトを介してこれらのフィールドにアクセスできます。暗号化ルールの条件を作成するにあたっては、必ず事前にクライアント要求を調べ、ルールをトリガーするために必要な条件を理解しておいてください。

> **注:**
> 効率的なルールを作成するため、ルールで評価する必要のない要求を除外するための簡単な方法を検討してください。最初にそれらの要求に対して False を返すように条件を作成します。これによりパフォーマンスが向上し、要求が正しいルールにルーティングされるスピードが速まります。

暗号化ルールのオブジェクトと API を暗号化ルールの条件で使用できます。

path と **postParams** を使用した例

```
/*This condition checks if the request coming in has a path ending in
"/sample_processor.do" and if a post parameter exists in that request called myPostParam */

function SampleCondition(request) {
  if (endsWith(request.path, "/sample_processor.do") && request.postParams.myPostParam) {
     return true;
  }
  return false;
}
```

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

urlParams と contentType を使用した例

```
/* This condition checks if a url parameter exists in the query called
myUrlParam and if the content type contains 'xml'
(if so, you can expect the body to be an XML payload).
Then, it checks if the xml payload contains myXmlTag */

function SampleCondition2(request) {
  if (request.urlParams.myUrlParam && request.contentType.indexOf('xml') > -1 &&
 request.xmlContains('myXmlTag')) {
      return true;
  }
 return false;
}
```

暗号化ルールのアクション

暗号化ルールにより、クライアント要求内のフィールドがインスタンス上のテーブルのフィールドにマップされ、暗号化対象としてマークされたフィールドが識別されます。

暗号化ルールのアクションは、暗号化ルールの条件が True を返すときのみ実行されます。暗号化ルールでは、要求ペイロードで暗号化するデータが識別されます。ルールは要求オブジェクト内のコンテンツに対して繰り返されるので、要求本体の形式と構造を理解して、要求内の何を暗号化する必要があるかを判断する必要があります。暗号化するデータは、次の場所に存在する可能性があります。

- POST または URL パラメーター。
- POST または URL パラメーター内部の JSON または XML の内容。
- JSON ペイロード。
- XML ペイロード。

暗号化ルールのアクションを記述するにあたっては、事前に次のことを確認してください。

- クライアント要求を調べる。
- 機密データが request オブジェクト内のどこにあるのかを特定します。
- データを挿入するフィールドおよびテーブル名を決めます。または、それらを要求から動的に抽出する方法について理解します。

暗号化ルールのオブジェクトと API を暗号化ルールのアクションと条件で使用できます。

暗号化ルールのオブジェクトと API

暗号化ルール API を使用して、エッジ暗号化 プロキシサーバー経由でインスタンスに送られる要求の中の値を解析し、暗号化します。

暗号化ルールに使用できる API は、request オブジェクトの形式によって異なります。たとえば、request オブジェクトの contentType パラメータが XML の場合は、XML API を使用してペイロード内の値を解析し暗号化することができます。要求内のオブジェクトのタイプを決めたら、API を使用して暗号化ルールを作成できます。

暗号化ルール API は、暗号化ルールの条件スクリプトとアクション スクリプトの両方で使用できます。

要求

request オブジェクトは、エッジ暗号化 のルールのアクション スクリプトと条件スクリプトで使用できるグローバル オブジェクトです。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

request オブジェクトは、エッジ暗号化 プロキシサーバーに送られるクライアント要求を表す JavaScript オブジェクトです。作成する暗号化ルールでは、*request* オブジェクトを解析し、*request* オブジェクトの値をインスタンス上のテーブルのフィールドにマップし、*request* オブジェクト内に機密データがある場合にそのデータを暗号化する必要があります。

request オブジェクトには、クライアント要求から得られる次の属性とデータが含まれています。

request オブジェクトのフィールド

フィールド	説明
path	URL のパス部分。
requestMethod	GET、POST、PUT、PATCH、DELETE。
contentType	Content-Type ヘッダー フィールド。
urlParams	クエリー文字列内のパラメーター。これは文字列に評価される可能性もあります。
postParams	これがフォーム ポストの場合は、ポスト パラメーターが含まれています。

request - getAsJsonContent()

要求を *JsonNode* タイプの反復可能なオブジェクトとして返します。

このメソッドは、要求本体が有効な JSON ペイロードである場合に、エッジ暗号化 のルールでのみ使用できます。要求本体にどのような形式が含まれているかわからない場合は、*request* オブジェクトの contentType フィールドを調べます。

要求が *JsonNode* オブジェクトとして返されたら、JSON API を使用してオブジェクトを反復処理し、フィールドを暗号化できます。

パラメーター

名前	タイプ	説明
なし		

返される内容

タイプ	説明
JsonNode	反復可能な *JsonNode* としての要求。

request - getAsXmlContent()

要求の内容を *XMLContent* タイプの反復可能なオブジェクトとして返します。

このメソッドは、要求本体が有効な XML ペイロードである場合に、エッジ暗号化 のルールでのみ使用できます。要求本体にどのような形式が含まれているかわからない場合は、*request* オブジェクトの contentType フィールドを調べます。

要求が *XMLContent* オブジェクトとして返されたら、XML API を使用してオブジェクトを反復処理し、フィールドを暗号化できます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

パラメーター

名前	タイプ	説明
なし		

返される内容

タイプ	説明
XMLContent	*XMLContent* タイプの反復可能なオブジェクトとしての要求。

request - XMLContains(String path)

指定したパスが XML DOM に存在する場合に True を返します。

このメソッドは、要求本体が有効な XML ペイロードである場合にのみ使用できます。要求本体にどのような形式が含まれているかわからない場合は、*request* オブジェクトの contentType フィールドを調べます。

パラメーター

名前	タイプ	説明
path	文字列	検索する XPath ステートメント。

返される内容

タイプ	説明
ブーリアン	指定したパスが XML DOM に存在するかどうか。

POST パラメーターと **URL** パラメーターの **API**

POST パラメーターと URL パラメーターは、request.postParams および request.urlParams を使用して、*request* オブジェクトのプロパティとしてアクセスできます。

request.postParams.myParam を呼び出すことで、任意の単一のパラメーターに *postParams* および *urlParams* の親オブジェクトとしてアクセスできます。この方法でアクセスするパラメーターはすべて、基底クラス *ParameterValue* のオブジェクトです。このクラス内の任意の API を任意のパラメーターで呼び出すことができます。

クライアント要求を調べる作業の後、場合によっては *request* オブジェクトからパラメーター値にアクセスして暗号化する必要があります。クライアント要求内のデータに応じて、複数の方法で値を暗号化し、インスタンスのフィールドにマップすることができます。

既知のテーブルおよびフィールドの値を暗号化する

暗号化データを保持するインスタンスのテーブルおよびフィールドの名前がわかっている場合は、それらを暗号化ルールで明示的に定義できます。たとえば、インスタンスでインシデントを作成するために要求が処理されることが分かっていて、説明フィールドの **text** パラメーターを暗号化する必要があるとします。この場合、次のアクションを作成できます。

```
function SampleAction1() {
    request.postParams.text.valueFor('incident', 'description');
}
```

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

動的に定義したテーブルおよびフィールドの値を暗号化する

逆に、暗号化データを設定するフィールドの名前がわからない場合は、**tableName** および **fieldName** を使用してそれらを動的に定義することができます。

次の例は、インスタンスのさまざまなタスク テーブル (インシデント、問題、change_request など) にデータを格納する可能性のある汎用的な要求を処理します。

```
function SampleAction2() {
    var tableName = request.urlParams.table;
    for (var parameter in request.postParams) {
        var currentParam = request.postParams[parameter];
        var fieldName = currentParam.toString();
        if (fieldName == 'text') {
            currentParam.valueFor(tableName, 'description')
        } else {
            currentParam.valueFor(tableName, fieldName);
        }
    }
}
```

このアクションでは次のことを実行します。

- URL パラメーターから宛先テーブルを取得します。
- URL パラメーターを反復処理します。
- 暗号化対象としてマークされたフィールドに一致する名前を持つすべての URL パラメーターを暗号化するよう、エッジ暗号化 プロキシサーバーに指示します。
- *text* という具体的なパラメーターを探し、インシデント テーブルの説明フィールドの暗号化設定に基づいて値を暗号化するよう エッジ暗号化 プロキシに指示します。

この例で、valueFor() メソッドは実際には暗号化を実行していません。そうではなく、このメソッドは、要求オブジェクト内のテーブル/フィールドのペアが暗号化設定で暗号化対象としてマークされているかどうかを確認し、必要に応じて暗号化するよう、エッジ暗号化 プロキシサーバーに指示しています。

パラメーター内の **JSON** または **XML** を暗号化する

POST パラメーターまたは URL パラメーターには、JSON または XML コンテンツが含まれています。この場合、パラメーター内のコンテンツを処理し、値を反復処理し、必須フィールドを暗号化することができます。次の例で、**tableName** は引き続き POST パラメーターからアクセスされますが、フィールドの値は JSON オブジェクトの **data** です。

```
function SampleAction3() {
    var tableName = request.postParams.table;
    var data = request.postParams.data;
    var dataIterator = data.getAsJsonContent().iterator();
    while (dataIterator.hasNext()) {
        var jsonElement = dataIterator.next();
        var fieldName = jsonElement.getName();
        if (fieldName == 'text') {
            jsonElement.valueFor(tableName, 'description');
        } else {
            jsonElement.valueFor(tableName, fieldName);
        }
```

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

```
    }
}
```

POST パラメーター内の XML を処理する暗号化ルールのアクションの例

```
function SampleAction4() {
    var tableName = request.postParams.table;
    var data = request.postParams.data;
    var dataIterator = data.getAsXmlContent().getIteratorOverAllChildren();
    while (dataIterator.hasNext()) {
        var jsonElement = dataIterator.next();
        var fieldName = jsonElement.getName();
        if (fieldName == 'text') {
            jsonElement.valueFor(tableName, 'description');
        } else {
            jsonElement.valueFor(tableName, fieldName);
        }
    }
}
```

クエリーを暗号化する

クライアント要求のパラメーターの中にエンコードされたクエリーが出現し、そこに機密データが含まれていることがあります。クエリーのフィールドを、インスタンスデータベースの暗号化された値に一致させるには、クエリーのフィールドが暗号化対象としてマークされているかどうかを確認するようプロキシに指示する暗号化ルールを作成する必要があります。encodedQueryFor() メソッドは、指定したテーブルのエンコードされたクエリーを解析し、クエリーのフィールドに暗号化設定があるかどうかを確認します。

この例では、ルールでパラメーターを反復処理して **filter** パラメーターを探します。このパラメーターは Glide のエンコードされたクエリーであると想定しています。

```
function SampleAction5() {
    var tableName = request.urlParams.table;
    for (var parameter in request.postParams) {
        var currentParam = request.postParams[parameter];
        var fieldName = currentParam.toString();
        if (fieldName == 'filter') {
            currentParam.encodedQueryFor(tableName);
        } else {
            currentParam.valueFor(tableName, fieldName);
        }
    }
}
```

たとえば、**filter** の値が short_description=My sensitive information^number=INC000056^category=Outage の場合、クエリーはインスタンス上で short_description=<Encrypted(My sensitive information)>^number=INC000056^category=Outage となります。

ParameterValue - toString()

POST または URL パラメーターの値を文字列に変換します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

パラメーター

名前	タイプ	説明
なし		

返される内容

タイプ	説明
文字列	文字列としてのパラメーター値。

ParameterValue - getAsJsonContent()

要求を `JsonNode` タイプの反復可能なオブジェクトとして返します。

このメソッドは、要求本体が有効な JSON ペイロードである場合に、エッジ暗号化 のルールでのみ使用できます。要求本体にどのような形式が含まれているかわからない場合は、`request` オブジェクトの contentType フィールドを調べます。

要求が `JsonNode` オブジェクトとして返されたら、JSON API を使用してオブジェクトを反復処理し、フィールドを暗号化できます。

パラメーター

名前	タイプ	説明
なし		

返される内容

タイプ	説明
JsonNode	反復可能な `JsonNode` としての要求。

ParameterValue - getAsXmlContent()

要求の内容を `XMLContent` タイプの反復可能なオブジェクトとして返します。

このメソッドは エッジ暗号化 のルールでのみ使用できます。このメソッドでは、要求本体が有効な XML ペイロードであると仮定されます。contentType を確認してそのことを確かめることができます。

要求が `XMLContent` オブジェクトとして返されたら、XML API を使用してオブジェクトを反復処理し、フィールドを暗号化できます。

パラメーター

名前	タイプ	説明
なし		

返される内容

タイプ	説明
XMLContent	`XMLContent` タイプの反復可能なオブジェクトとしての要求。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ParameterValue - encodedQueryFor(String tableName)

要素の値が、指定したテーブルのエンコードされたクエリーであることを指定します。

パラメーターでこの関数を呼び出すと、パラメーターの値が、指定したテーブルのエンコードされたクエリ文字列 であることがプロキシに通知されます。プロキシは、エンコードされたクエリーを解析し、エンコードされたクエリーのフィールドのうち暗号化する必要があるフィールドを暗号化します。

パラメーター

名前	タイプ	説明
tableName	文字列	クエリーの実行を想定するテーブル。

返される内容

タイプ	説明
なし	

ParameterValue - valueFor(String tableName, String fieldName)

要素の値が、指定したテーブルの指定したフィールドにマップされることを指定します。

このメソッドを要素値で呼び出すと、この要素の値が、指定したテーブルの指定したフィールドにマップされることがプロキシに通知されます。プロキシは、フィールドを暗号化する必要があるかどうかを確認します。

パラメーター

名前	タイプ	説明
tableName	文字列	テーブル名。
fieldName	文字列	フィールド名

返される内容

タイプ	説明
なし	

XML API

XML API は、`request` オブジェクトか `ParameterValue` プロパティのどちらかで `getAsXmlContent()` を呼び出した後に使用できます。

XML API を使用して暗号化ルールを記述する際は、次の一般的な形式に従うことができます。

1. `getAsXmlContent()` は、`request` オブジェクトまたは `ParameterValue` プロパティで呼び出します。これは、`XMLContent` 基底クラスの反復可能なオブジェクトを返します。
2. `getIterator()` または `getIterator(String xPath)` は、`XMLContent` オブジェクトで呼び出します。これは、XML 要素の反復処理に使用できる `XMLElementIterator` オブジェクトを返します。
3. `hasNext()` メソッドは、`XMLElementIterator` オブジェクトで別の要素が使用可能かどうかを判断するために呼び出します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

4. `next()` は、`XMLElementIterator` オブジェクトで次の XML 要素を返すために呼び出します。`next()` を呼び出すには先に `hasNext()` を呼び出す必要があります。
5. `valueFor(String tableName, String fieldName)` は、XML 要素で呼び出します。このメソッドは、この要素の値が指定したテーブルの指定したフィールドにマップされることをプロキシに通知します。プロキシは、フィールドを暗号化する必要があるかどうかを確認します。

> **注:**
> XML 要素で `valueFor(String tableName, String fieldName)` を呼び出す必要があるかどうかを判断するために、`getName()` メソッドを使用して要素の名前を返すことができます。

インスタンス上の既知のテーブルフィールドへのマッピング

この例では、インスタンス上で XML ペイロードが処理され、インシデント テーブルにレコードが挿入されます。説明フィールドには、インシデントの short_description が設定されます。

```
<data>
   <record>
      <name>'Test Record 1'</name>
      <description>'Test Record 1 Description'</description>
      <tag>critical</tag>
   </record>
   <record>
      <name>'Test Record 2'</name>
      <description>'Test Record 2 Description'</description>
      <tag>security</tag>
   </record>
</data>
```

暗号化ルールの次のアクションを適用できます。

```
function sampleXmlAction1() {
   var xmlContent = request.getAsXmlContent();
   // This loop iterates over all description tags that match the given path
   var xmlElementIterator = xmlContent.getIterator('data/record/description');
   while (xmlElementIterator.hasNext()) {
      var xmlElement = xmlElementIterator.next();
      xmlElement.valueFor('incident', 'short_decription');
   }
}
```

このアクションは、**description** タグを反復処理し、値を暗号化してインスタンスの incident.short_description に挿入するようプロキシサーバーに指示します。

> **注:**
> このルールは、XML ペイロードのすべての **record** タグの中で **description** タグを探します。暗号化するタグが 1 つしか出現しない場合でも、ルールは xPath と反復構造体を使用します。ただし、ループ内で 1 回しか反復しません。

インスタンス上の未知のテーブルフィールドへのマッピング

この例では、ルールは **record** タグを反復処理しますが、**record** タグの中でどのようなタグが存在するのかはわかりません。わかっているのは、**record** タグ内のタグが、テーブルの URL パラメーターで指定された列の名前と一致する、ということだけです。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

また、テーブルがインシデントの場合、ルールは **description** タグのデータを暗号化し、インスタンスの short_description フィールドに格納します。

```
function sampleXmlAction2() {
   var xmlContent = request.getAsXmlContent();
   var tableName = request.urlParam.table;
   // This first iterator will iterate over all record elements
   var xmlElementIterator = xmlContent.getIterator('data/record');
   while (xmlElementIterator.hasNext()) {
      encryptFieldsInRecord(xmlElementIterator.next());
   }
}
function encryptFieldsInRecord(xmlElement) {
   //Then, iterate over all tags representing fields in the table
   var fieldIterator = xmlElement.getIteratorOverAllChildren();
   while (fieldIterator.hasNext()) {
      var field = fieldIterator.next();
      var fieldName = childElement.getName();
      //if table is incident, then description is encrypted for the short_description field
      if (tableName == 'incident' && fieldName == 'description') {
         field.valueFor(tableName, 'short_description');
      } else {
         //if table is not incident, ask the proxy to check if the given field is encrypted for the
 given table
         field.valueFor(tableName, fieldName);
      }
   }
}
```

`encryptFieldsInRecord()` 関数では、要求に基づいて動的に割り当てられるテーブルおよびフィールドで *`valueFor()`* メソッドを呼び出します。テーブル名とフィールド名は変化する可能性がありますが、その場合でもルールは、定義された暗号化設定に基づいてテーブル内のフィールドを暗号化する必要があるかどうかを確認するようプロキシに指示します。

フィールドが暗号化対象として設定されていない場合、またはタグがテーブルのフィールドと一致しない場合、プロキシはそのタグをスキップします。タグが暗号化対象としてマークされたフィールドに一致する場合、エッジ暗号化 プロキシサーバーは値を暗号化します。

エンコードされたクエリーの使用

この例では、すべてのタグに **filter** 属性があります。この属性は、エンコードされたクエリーがタグに含まれているかどうかを示します。

```
<data>
   <record>
      <name filter="false">'Test Record 1'</name>
      <description filter="false">'Test Record 1 Description'</description>
      <query filter="true">category=1^name=edge</query>
   </record>
   <record>
      <name filter="false">'Test Record 2'</name>
      <description filter="false">'Test Record 2 Description'</description>
      <query filter="true">category=2^severity=3</query>
  </record>
</data>
```

暗号化ルールの次のアクションを適用できます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

```
function sampleXmlAction3() {
  var xmlContent = request.getAsXmlContent();
  var tableName = request.urlParam.table;
  // This first iterator will iterate over all record elements
  var xmlElementIterator = xmlContent.getIterator('data/record');
  while (xmlElementIterator.hasNext()) {
     encryptFieldsInRecord(xmlElementIterator.next());
  }
}
function encryptFieldsInRecord(xmlElement) {
  //this time we want to iterate over all tags representing fields in the table
  var fieldIterator = xmlElement.getIteratorOverAllChildren();
  while (fieldIterator.hasNext()) {
     var field = fieldIterator.next();
     var fieldname = childElement.getName();
     //let's look at the filter attribute, if true, then encrypt as encoded query
     if (field.getAttributeValue('filter') == 'true') {
        field.encodedQueryFor(tableName);
     } else {
        //if it is false then check if the field should be encrypted
        field.valueFor(tableName, fieldName);
     }
  }
}
```

filter 属性の値が True の場合、ルールは、エンコードされたクエリーの値を暗号化するようプロキシサーバーに指示します。False の場合、ルールは、フィールドを暗号化する必要があるかどうかを確認するようプロキシに指示します。

XMLContent

XML コンテンツを反復処理するメソッドを提供するグローバル オブジェクトです。

`XMLContent` オブジェクトにアクセスするには、*`request`*オブジェクトで getAsXmlContent() を呼び出します。

POST または URL パラメーターの XML データにアクセスするには、request.postParams.<パラメーター名>.getAsXmlContent() または request.urlParams.<パラメーター名>.getAsXmlContent() を呼び出します。

XMLContent - getIterator()

XML コンテンツの *`XMLElementIterator`* オブジェクトを返します。

パラメーター

名前	タイプ	説明
なし		

返される内容

タイプ	説明
XMLElementIterator	*`XMLContent`* オブジェクトの要素の反復処理に使用できるオブジェクト。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

XMLContent - getIterator(String xPath)

指定したパラメーターに基づいて、XML コンテンツの `XMLElementIterator` オブジェクトを返します。

パラメーター

名前	タイプ	説明
xPath	文字列	`XMLContent` オブジェクトのどこを出発点にするかを指定する xPath 風の式。

返される内容

タイプ	説明
XMLElementIterator	`XMLContent` オブジェクトの要素の反復処理に使用できるオブジェクト。

XMLElementIterator

XM L要素を反復処理するためのメソッドを提供します。

`XMLElementIterator` オブジェクトを取得するには、`XMLContent` クラスの `getIterator()` メソッドを呼び出します。

XMLElementIterator - hasNext()

利用可能な別の要素があるかどうかを判断します。

パラメーター

名前	タイプ	説明
なし		

返される内容

タイプ	説明
ブーリアン	別の要素が利用可能な場合は True。

XMLElementIterator - next()

反復子の次の要素を返します。

`next()` を呼び出すには先に `hasNext()` を呼び出す必要があります。

パラメーター

名前	タイプ	説明
なし		

返される内容

タイプ	説明
XMLElement	次の XML 要素。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

XMLElement

XML 要素を反復処理して値をテーブルのフィールドにマップするためのメソッドを提供します。

`XMLElement` オブジェクトを取得するには、`XMLElementIterator` オブジェクトの `next()` メソッドを呼び出します。

XMLElement - getIterator(String xPath)

指定したパラメーターに基づいて、XML 要素の `XMLElementIterator` オブジェクトを返します。

パラメーター

名前	タイプ	説明
xPath	文字列	`XMLElement` オブジェクトのどこを出発点にするかを指定する xPath 風の式。

返される内容

タイプ	説明
XMLElementIterator	`XMLElement` オブジェクトの要素の反復処理に使用できるオブジェクト。

XMLElement - getIteratorOverAllChildren()

指定したパラメーターに基づいて、XML 要素のすべての下位要素が含まれている `XMLElementIterator` オブジェクトを返します。

パラメーター

名前	タイプ	説明
なし		

返される内容

タイプ	説明
XMLElementIterator	`XMLElement` オブジェクトの要素の反復処理に使用できるオブジェクト。

XMLElement - valueFor(String tableName, String fieldName)

要素の値が、指定したテーブルの指定したフィールドにマップされることを指定します。

このメソッドを要素値で呼び出すと、この要素の値が、指定したテーブルの指定したフィールドにマップされることがプロキシに通知されます。プロキシは、フィールドを暗号化する必要があるかどうかを確認します。テーブル名およびフィールド名がわからない場合は、要求に基づいて動的に割り当てられるテーブルおよびフィールドで、`valueFor()` 関数を呼び出すことができます。

パラメーター

名前	タイプ	説明
tableName	文字列	テーブル名。
fieldName	文字列	フィールド名

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

返される内容

タイプ	説明
なし	

XMLElement - encodedQueryFor(String tableName)

要素の値が、指定したテーブルのエンコードされたクエリーであることを指定します。

要素でこの関数を呼び出すと、要素の値が、指定したテーブルのエンコードされたクエリ文字列 であることがプロキシに通知されます。プロキシは、エンコードされたクエリーを解析し、エンコードされたクエリーのフィールドのうち暗号化する必要があるフィールドを暗号化します。

パラメーター

名前	タイプ	説明
tableName	文字列	クエリーの実行を想定するテーブル。

返される内容

タイプ	説明
なし	

XMLElement - getName()

要素名を返します。

パラメーター

名前	タイプ	説明
なし		

返される内容

タイプ	説明
文字列	要素名。

XMLElement - getAttributeValue(String attribute)

指定した属性の値を返します。

パラメーター

名前	タイプ	説明
attribute	文字列	属性名。

返される内容

タイプ	説明
文字列	属性値。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

JSON API

JSON API は、*request* オブジェクトか *ParameterValue* プロパティのどちらかで *getAsJsonContent()* を呼び出した後に使用できます。

JSON API を使用して暗号化ルールを記述する際は、次の一般的な形式に従うことができます。

1. *getAsJsonContent()* は、*request* オブジェクトで呼び出します。これは、*JsonNode* 基底クラスの反復可能なオブジェクトを返します。
2. *iterator()* または *getIterator(String xPath)* は、*JsonNode* オブジェクトで呼び出します。これは、JSON オブジェクトのノードの反復処理に使用できる *JsonNodeIterator* オブジェクトを返します。
3. *hasNext()* メソッドは、*JsonNodeIterator* オブジェクトで別の要素が使用可能かどうかを判断するために呼び出します。
4. *next()* は、*JsonNodeIterator* オブジェクトで次の JSON 要素を返すために呼び出します。*next()* を呼び出すには先に *hasNext()* を呼び出す必要があります。
5. *valueFor(String tableName, String fieldName)* は、JSON 要素で呼び出します。このメソッドは、この要素の値が指定したテーブルの指定したフィールドにマップされることをプロキシに通知します。プロキシは、フィールドを暗号化する必要があるかどうかを確認します。

> **注:**
> JSON 要素で *valueFor(String tableName, String fieldName)* を呼び出す必要があるかどうかを判断するために、*getName()* メソッドを使用して要素の名前を返すことができます。

インスタンス上の既知のテーブルフィールドへのマッピング

この例では、インスタンス上で JSON ペイロードが処理され、インシデント テーブルにレコードが挿入されます。説明フィールドには、インシデントの short_description が設定されます。

```
{
   data: {
      records: [
         {
            "name": "Test Record 1",
            "description": "Test Record 1 Description",
            "tag": "security"
         },
         {
            "name": "Test Record 1",
            "description": "Test Record 1 Description",
            "tag": "security"
         }],
      "query": "assigned_to=3D4860165813e63a00d00abd322244b092^category=vulnerability"
   },
   "source": "10.11.13.14"
}
```

次のルールを適用できます。

```
function sampleJsonAction1() {
   var jsonContent = request.getAsJsonContent();
   // This loop iterates over all description elements in the records array
   var jsonNodeIterator = jsonContent.getIterator('/data/records/description');
   while (jsonNodeIterator.hasNext()) {
      var jsonNode = jsonNodeIterator.next();
```

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

```
        jsonNode.valueFor('incident', 'short_decription');
    }
}
```

このアクションは、**description** ノードを反復処理し、値を暗号化してインスタンスの incident.short_description に挿入するようプロキシサーバーに指示します。

> **注:**
> このルールは、JSON ペイロード内のすべての **description** ノードを探します。暗号化するノードが 1 つしか出現しない場合でも、ルールは xPath と反復構造体を使用します。ただし、ループ内で 1 回しか反復しません。

インスタンス上の未知のテーブルフィールドへのマッピング

この例では、ルールは **records** を反復処理しますが、どのノードを想定するかはわかりません。わかっているのは、**records** 内の各オブジェクトについて、ノードがテーブルの URL パラメーターで指定された列の名前と一致する、ということだけです。

また、テーブルがインシデントの場合、ルールは **description** ノードのデータを暗号化し、インスタンスの short_description フィールドに格納します。

```
function sampleJsonAction2() {
    var jsonContent = request.getAsJsonContent();
    var tableName = request.urlParam.table;
    // This first iterator will iterate over all record elements
    var jsonNodeIterator = jsonContent.getIterator('data/records');
    while (jsonNodeIterator.hasNext()) {
        encryptFieldsInRecord(jsonNodeIterator.next());
    }
}
function encryptFieldsInRecord(jsonNode) {
    //this time we want to iterate over all nodes
    var fieldIterator = jsonNode.iterator();
    while (fieldIterator.hasNext()) {
        var field = fieldIterator.next();
        var fieldname = childElement.getName();
        if (fieldName == 'description') {
            field.valueFor(tableName, 'short_description');
        } else {
            field.valueFor(tableName, fieldName);
        }
    }
}
```

`encryptFieldsInRecord()` 関数では、要求に基づいて動的に割り当てられるテーブルおよびフィールドで *`valueFor()`* メソッドを呼び出します。テーブル名とフィールド名は変化する可能性がありますが、その場合でもルールは、定義された暗号化設定に基づいてテーブル内のフィールドを暗号化する必要があるかどうかを確認するようプロキシに指示します。

フィールドが暗号化対象として設定されていない場合、またはノードがテーブルのフィールドと一致しない場合、プロキシはそのノードをスキップします。ノード名が暗号化対象としてマークされたフィールドに一致する場合、プロキシは値を暗号化します。

エンコードされたクエリーの使用

```
function sampleJsonAction3() {
    var jsonContent = request.getAsJsonContent();
```

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

```
    var tableName = request.urlParam.table;
    // This first iterator will iterate over all record elements
    var jsonNodeIterator = jsonContent.getIterator('data');
    while (jsonNodeIterator.hasNext()) {
        var jsonNode = jsonNodeIterator.next();
        if (jsonNode.getName() == 'records')
            encryptRecors(jsonNodeIterator.next());
        else if (jsonNode.getName() == 'query')
            jsonNode.encodedQueryFor(tableName);
    }
}
function encryptRecords(jsonNode) {
    //we iterate over all fields in the node
    var recordIterator = jsonNode.iterator();
    while (recordIterator.hasNext()) {
        encryptFieldsInRecord(recordIterator.next());
    }
}
function encryptFieldsInRecord(jsonNode) {
    //this time we want to iterate over all nodes
    var fieldIterator = jsonNode.iterator();
    while (fieldIterator.hasNext()) {
            var field = fieldIterator.next();
            var fieldname = childElement.getName();
            field.valueFor(tableName, fieldName);
    }
}
```

この例では、ルールは **data** を反復処理します。**records** を見つけるたびに、ルールは、2 つ目の例と同じロジックを実行して、各ノードのフィールドを反復処理します。**query** ノードを見つけると、*encodedQueryFor()* を呼び出して、クエリーで暗号化する必要がある値を暗号化します。

JsonNode

JSON コンテンツを反復処理するメソッドを提供するグローバル オブジェクトです。

JsonNode オブジェクトにアクセスするには、*request*オブジェクトで getAsJsonContent() を呼び出します。

POST または URL パラメーターから JSON コンテンツにアクセスするには、request.postParms.<パラメーター名>.getAsJsonContent() または request.urlParms.<パラメーター名>.getAsJsonContent() を呼び出します。

JsonNode - getIterator(String xPath)

JSON コンテンツの *JsonNodeIterator* オブジェクトを返します。

このメソッドはルート ノードでのみ使用できますが、これを使用して JSON オブジェクトに深くトラバースできます。後続のトラバースでは *iterator()* メソッドを使用する必要があります。

パラメーター

名前	タイプ	説明
xPath	文字列	xPath 式。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

返される内容

タイプ	説明
JsonNodeIterator	JSON オブジェクトのノードを反復処理できるオブジェクト。

JsonNode - iterator()

現在のノードのすべての子ノードを反復処理する `JsonNodeIterator` オブジェクトを返します。

パラメーター

名前	タイプ	説明
なし		

返される内容

タイプ	説明
JsonNodeIterator	JSON オブジェクトのノードを反復処理できるオブジェクト。

JsonNode - getAsString()

現在のノード値を文字列として返します。

パラメーター

名前	タイプ	説明
なし		

返される内容

タイプ	説明
文字列	現在のノード値。

JsonNode - getAsString(String propertyName)

指定したプロパティの文字列値を返します。

パラメーター

名前	タイプ	説明
propertyName	文字列	プロパティの名前。

返される内容

タイプ	説明
文字列	プロパティ値。

JsonNode - getName()

現在の JSON ノードの名前を返します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

パラメーター

名前	タイプ	説明
なし		

返される内容

タイプ	説明
文字列	現在の JSON ノードの名前。

JsonNode - valueFor(String tableName, String fieldName)

JSON プロパティが、指定したテーブルの指定したフィールドにマップされることを指定します。

このメソッドを JSON プロパティで呼び出すと、このプロパティの値が、指定したテーブルの指定したフィールドにマップされることがプロキシに通知されます。プロキシは、フィールドを暗号化する必要があるかどうかを決定します。テーブル名およびフィールド名がわからない場合は、要求に基づいて動的に割り当てられるテーブルおよびフィールドで、`valueFor()` 関数を呼び出すことができます。

パラメーター

名前	タイプ	説明
tableName	文字列	テーブル名。
fieldName	文字列	フィールド名

返される内容

タイプ	説明
なし	

JsonNode - encodedQueryFor(String tableName)

JSON プロパティの値が、指定したテーブルのエンコードされたクエリーであることを指定します。

JSON ノードでこの関数を呼び出すと、その値が、指定したテーブルのエンコードされたクエリ文字列 であることがプロキシに通知されます。プロキシは、エンコードされたクエリーを解析し、エンコードされたクエリーのフィールドのうち暗号化する必要があるフィールドの値を暗号化します。

パラメーター

名前	タイプ	説明
tableName	文字列	クエリーの実行を想定するテーブル。

返される内容

タイプ	説明
なし	

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

JsonNodeIterator

`JsonNodeIterator` オブジェクトを取得するには、`JsonNode` クラスの `getIterator()` メソッドまたは `iterator()` メソッドを呼び出します。

JsonNodeIterator - hasNext()

利用可能な別のプロパティがあるかどうかを判断します。

パラメーター

名前	タイプ	説明
なし		

返される内容

タイプ	説明
ブーリアン	別のプロパティが利用可能な場合は True。

JsonNodeIterator - next()

反復子の次のプロパティを返します。

`next()` を呼び出すには先に `hasNext()` を呼び出す必要があります。

パラメーター

名前	タイプ	説明
なし		

返される内容

タイプ	説明
JsonNode	次の `JsonNode`。

print(String message)

メッセージをラッパー ログ ファイル <プロキシサーバーのディレクトリー>/logs/wrapper_<日付>.log に出力します。

このメソッドは エッジ暗号化 のルール アクション スクリプトでのみ使用できます。

パラメーター

名前	タイプ	説明
message	文字列	ラッパー ログ ファイルに書き込むメッセージ。

返される内容

タイプ	説明
なし	

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

禁止されているキーワード

エッジ暗号化 プロキシは、ルールを保存する前に、暗号化ルールスクリプトを検証します。JavaScript のキーワードの多くは暗号化ルールスクリプトでは使用できません。

禁止されているキーワード

キーワード
__DIR__
__FILE__
__LINE__
__parent__
__proto__
エラー
eval
getClass
getPrototypeOf
Java
javax
javafx
JavaImporter
load
loadWithNewGlobal
新規
パッケージ
オブジェクト
prototype
RegExp
setPrototypeOf
this
throw

Edge Encryption の辞書属性

テーブルとフィールドに辞書属性を追加して、Edge Encryption での動作方法を制御します。

ディクショナリ属性を true に設定するには、[属性] フィールドに「attribute=true」と入力する必要があります。レコードに辞書属性を追加するには、「辞書属性」を参照してください。

Edge Encryption Excluded [edge_encryption_excluded]

フィールドを暗号化から除外するかどうかを決定します。

true に設定すると、フィールドまたはテーブルを暗号化できません。false に設定すると、フィールドを暗号化できます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- 値：true/false
- ターゲット要素：フィールドまたはテーブル
- デフォルト値：false

Edge Encryption Enabled [edge_encryption_enabled]

フィールドが暗号化設定による暗号化の対象かどうかを判断します。

true に設定すると、フィールドが暗号化対象になります。false に設定すると、フィールドは暗号化の対象になりません。この属性はシステムによって使用され、変更できないため、ユーザーには表示されません。

> **注:**
> この属性は、フィールドが暗号化されていることを示すものではなく、フィールドで暗号化ロジックをトリガーするものでもありません。この属性によって、フィールドがユーザーによって暗号化される可能性が決まります。

- 値：true/false
- ターゲット要素：フィールド
- デフォルト値：文字列フィールドの場合は true

Edge Encryption Clear Text Allowed [edge_encryption_clear_text_allowed]

プロキシー サーバー経由で実行されるユーザー アクションや、スケジュール設定済みジョブなどのサーバー側の自動スクリプトにおいて、サーバー側スクリプトがフィールド内の暗号化された文字列に暗号化されていないデータを追加できるかどうかを決定します。

true に設定すると、データを追加できます。false に設定すると、データの追加は許可されません。

- 値：true/false
- ターゲット要素：フィールド
- デフォルト値：false

ドメイン分離と エッジ暗号化

ドメイン分離は、エッジ暗号化 で制限された環境でサポートされます。エッジ暗号化 は、エッジ暗号化 プロキシで定義された特定の設定、ルール、およびキーを使用してお客様の環境の中からデータを暗号化する機能を提供します。エッジ暗号化 プロキシはドメインに対応しておらず、ドメイン固有の設定をサポートすることができません。 ドメイン分離では、データ、プロセス、および管理タスクをドメインと呼ばれる論理的なグループに分けることができます。どのユーザーがデータを表示できるか、データにアクセスできるかなど、このアプリケーションのいくつかの側面を制御できます。

サポートレベル: サポートなし

- ドメインフィールドがデータテーブル に存在している可能性がありますが、データを管理するロジックがありません。
- このレベルでは、ドメイン分割は考慮されません。

サポートレベルの詳細については、「アプリケーションでのドメイン分離のサポート)」を参照してください。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

Edge Encryption におけるドメイン分離の仕組み

Edge Encryption は、ドメイン固有のキー、設定、およびルールが不要となる場合に使用できます。

関連情報

サービスプロバイダーのドメイン分離

エッジ暗号化 とのデータの統合

エッジ暗号化 を使用してサードパーティのデータをインスタンスと統合するには、サポートされている統合を使用してデータを エッジ暗号化 プロキシサーバー経由でルーティングする必要があります。サポートされている統合では、各ペイロードのデータをテーブルのフィールドにマップするベース システムの暗号化ルールが使用されます。

暗号化対象としてマークされたフィールドにデータをアップロードする

エッジ暗号化 では、Excel、CSV、XML、またはその他のファイル タイプと、暗号化設定が定義されたフィールドとの間で、データのインポートまたはエクスポートを行うことはできません。

ODBC ドライバー

エッジ暗号化 プロキシサーバー経由で、ODBC ドライバーを使用して要求を暗号化し、データをクエリーします。

詳細を見る： Edge Encryption と ODBC ドライバーの統合

MID Server

MID サーバー プロキシサーバー経由でデータをルーティングするように エッジ暗号化を設定できます。ただし、いくつかの制限が適用されます。

詳細を見る： Edge Encryption と MID Server の統合

REST/SOAP Web サービス

REST/SOAP Web Services を使用し、エッジ暗号化 プロキシサーバー経由でレコード データを更新または取得します。

詳細を見る：Web サービス

JSONv2 Web サービス

JSONv2 Web サービス API を使用し、エッジ暗号化 プロキシサーバー経由でレコード データを更新または取得します。ベースシステムの暗号化ルールでは、データ取得 API やデータ変更 API をサポートしています。

- データ変更 API を使用して 1 つのレコードを挿入するには、`insert()` メソッドや `insertMutiple()` メソッドを使用します。
- データ変更 API を使用して複数のレコードを挿入するには、`insertMultiple()` メソッドを使用します。

詳細を見る：JSONv2 Web サービス

上記に記載されていないサードパーティのカスタムの統合から得られるデータを暗号化するには、カスタムの暗号化ルールを作成します。「カスタムの暗号化ルールを定義する」を参照してください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

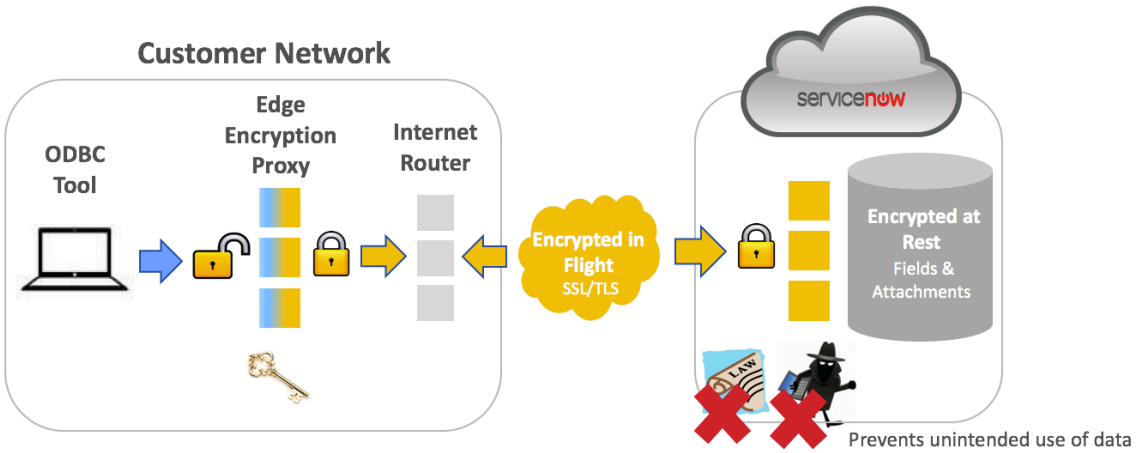
暗号化対象としてマークされたレコードに添付ファイルをアップロードする

REST および SOAP Web サービスを使用して設定した添付ファイル暗号化を使用して、テーブルに添付ファイルをアップロードできます。

Edge Encryption と ODBC ドライバーの統合

エッジ暗号化 により暗号化されたデータをクエリーするように ODBC ドライバーを設定します。エッジ暗号化 が ODBC ドライバーと統合されているとき、ServiceNow プロキシサーバーは、エッジ暗号化 インスタンスへの ODBC ドライバーの要求を暗号化します。

インスタンスからの暗号化された応答は、エッジ暗号化 プロキシサーバーを通じて復号化されてから、ネットワークの ODBC ドライバーに渡されます。



統合を正常に機能させるためには、ODBC ドライバーが エッジ暗号化 プロキシサーバー証明書を信頼する必要があります。エッジ暗号化 プロキシサーバー証明書が、ODBC ドライバーが信頼している認証局によって署名されている場合、エッジ暗号化 プロキシサーバーは自動的に信頼されます。ただし、ODBC ドライバーが信頼している認証局がまだ エッジ暗号化 プロキシサーバー証明書に署名していない場合は、自己署名証明書を ODBC トラストストアにインポートする必要があります。

自己署名証明書を ODBC トラストストアにインポートする

ODBC ドライバーが信頼している認証局がまだ エッジ暗号化 プロキシサーバー証明書に署名していない場合は、自己署名証明書を ODBC トラストストアにインポートする必要があります。エッジ暗号化 プロキシサーバーから証明書をエクスポートし、ODBC トラストストアにインポートすることができます。

始める前に

必要なロール：管理者

ODBC ドライバーが信頼している認証局が エッジ暗号化 プロキシサーバー証明書に署名したかどうかを判断するには、プロキシのホーム ディレクトリーのキーストア ディレクトリーで次のコマンドを実行して、ODBC ドライバーが信頼している認証局の一覧を表示します。

```
keytool -keystore "<ODBC directory>\ip\Java\jre\lib\security\cacerts" -list
```

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注:

ほとんどの場合、クライアントはロードバランサーを介して エッジ暗号化 プロキシに接続するため、証明書はロードバランサーで構成された証明書になります。

クライアントと Edge プロキシサーバーの間にロードバランサーがない場合、証明書は Edge プロキシによって提示される証明書になり、*edgeencryption.properties* ファイルで構成されます。

```
edgeencryption.proxy.https.port = 9090
edgeencryption.proxy.https.keystore.path = keystore/keystore
edgeencryption.proxy.https.keystore.password = password
edgeencryption.proxy.https.cert.alias = jetty
```

プロパティの編集の詳細については、「Edge Encryption プロパティファイルでその他のプロパティを設定する」を参照してください。

手順

1. プロキシのホーム ディレクトリーのキーストア ディレクトリーに移動します。
2. キーストアに自己署名証明書がないか確認します。
   a. キーストアに証明書がないかを確認するには、次のコマンドを実行してキーストア内のすべてのアイテムを一覧表示します。

      ```
      keytool -list -keystore keystore.jceks -storetype jceks -v
      ```

   b. アイテムのリストでキー エイリアスを探します。
3. キー エイリアスを使用して、証明書を .cer ファイルにエクスポートします。

   ```
   keytool -export -alias <key alias> -keystore keystore.jceks -storetype jceks -rfc -file <file name>.cer
   ```

4. ODBC トラストストア ディレクトリー ODBC\ip\Java\jre\lib\security\cacerts に移動します。
5. 証明書を ODBC トラストストアにインポートします。

   ```
   keytool -keystore cacerts -importcert -alias $<key alias> -file <file name>.cer
   ```

ODBC ドライバーのプロパティを設定する

要求が エッジ暗号化 プロキシサーバー経由でルーティングされるように、ODBC ドライバーのプロパティを設定します。

始める前に
必要なロール：管理者

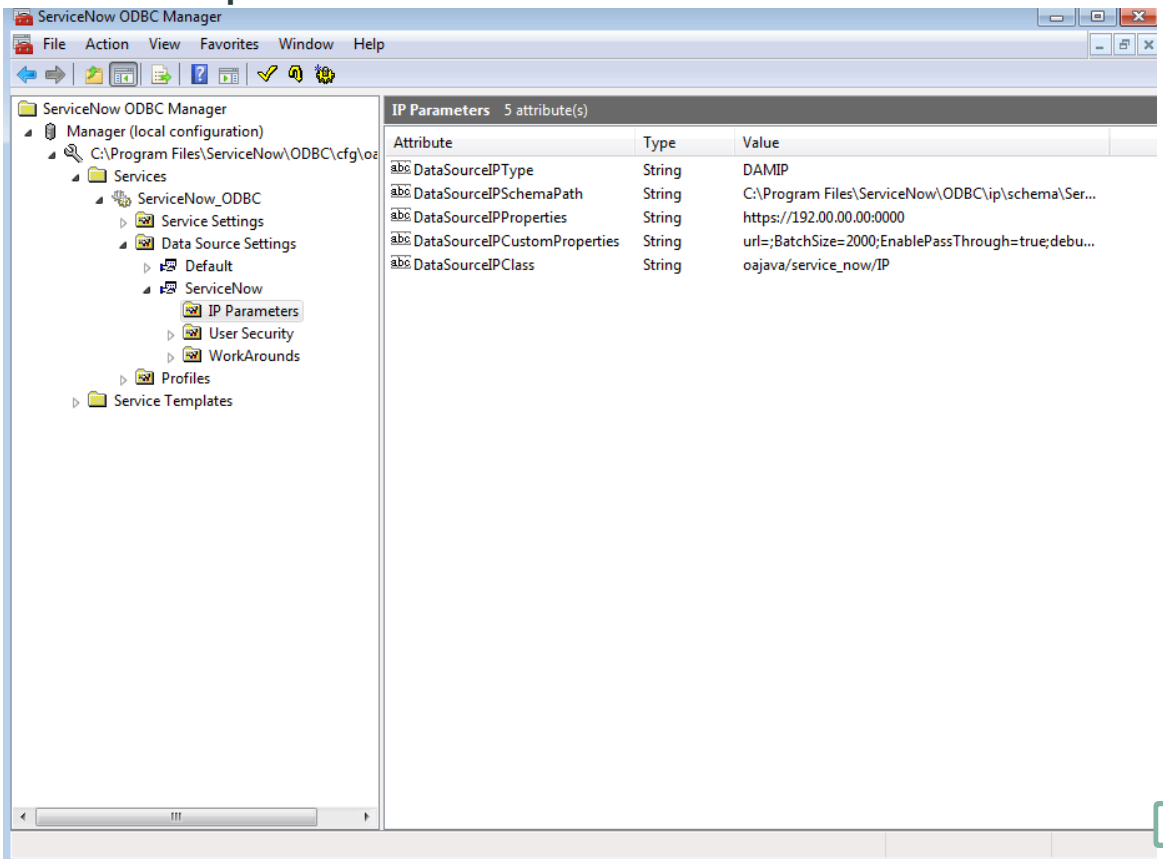
手順

1. Windows で、次の場所に移動します。 開始 > プログラム > **ServiceNow ODBC** 管理コンソール.
2. コンソール ツリーのルートを ServiceNow ODBC Manager\Manager\<インストール場所>\Services\ServiceNow_ODBC\Data Source Settings\ServiceNow\IP Parameters まで展開します。
3. 属性をダブルクリックします。
4. [値] を、Edge Encryption プロキシサーバーの URL (https://<IP アドレス>:<ポート> など) に変更します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

DataSourceIPProperties



5. **[OK]** をクリックします。

次のタスク
これで、要求が エッジ暗号化 プロキシサーバー経由でインスタンスにルーティングされるように、ODBC ドライバーが設定されます。

Edge Encryption と MID Server の統合

MID サーバー プロキシサーバー経由でデータをルーティングするように エッジ暗号化 を設定します。

MID サーバー と統合する場合、エッジ暗号化 プロキシサーバーは MID サーバーのエンドポイントとして機能します。これで、エッジ暗号化 プロキシサーバーは、ServiceNow インスタンスと MID サーバー間で受け渡しされるデータの暗号化と復号化を行います。

MID Server と統合する際の制限事項

MID サーバー プロキシサーバー経由で渡されるように エッジ暗号化のデータを設定する場合、次の制限が適用されます。

- [ECC キュー] フィールドの暗号化はサポートされていません。
- 暗号化されたデータをディスカバリーまたはサービスマッピングで使用することはできません。

MID Server から Edge Encryption プロキシサーバーを指し示す

データを MID サーバーから エッジ暗号化 プロキシサーバー経由で渡すには、MID サーバーから エッジ暗号化 プロキシサーバーを指し示すように、MID サーバーの設定ファイルを更新します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

始める前に
必要なロール：管理者

このタスクについて
MID サーバー プロキシサーバー経由でデータを渡すように エッジ暗号化を設定する場合、MID サーバーの設定ファイルで Web プロキシ プロパティを使用して、トラフィックを エッジ暗号化 プロキシサーバー経由でインスタンスにルーティングすることはできません。代わりに、エッジ暗号化 プロキシサーバーを MID サーバーのエンドポイントとして設定する必要があります。

手順

1. ローカルの MID サーバー ディレクトリーに移動し、config.xml ファイルを開きます。
2. 要素 `<parameter name="url" value="https://YOUR_INSTANCE.service-now.com" />` を探し、値プロパティを エッジ暗号化 プロキシサーバーの URL に変更します。
   たとえば、http://hostname.mycompany.com:8081 などです。
   この手順により、MID サーバー に対して、トラフィックをインスタンスにではなく エッジ暗号化 プロキシサーバーに渡すよう指示します。トラフィックを受信した エッジ暗号化 プロキシサーバーは、必要なフィールドをすべて暗号化し、ペイロードをインスタンスに渡します。
3. ファイルを保存して閉じます。
4. MID サーバーが実行中の場合は再起動します。

Edge Encryption の診断とパフォーマンス

エッジ暗号化 プロキシサーバーのパフォーマンスの傾向を監視し、エッジ暗号化 プロキシサーバーにより生成されるエラーを詳しく調べます。

Edge プロキシのパフォーマンス

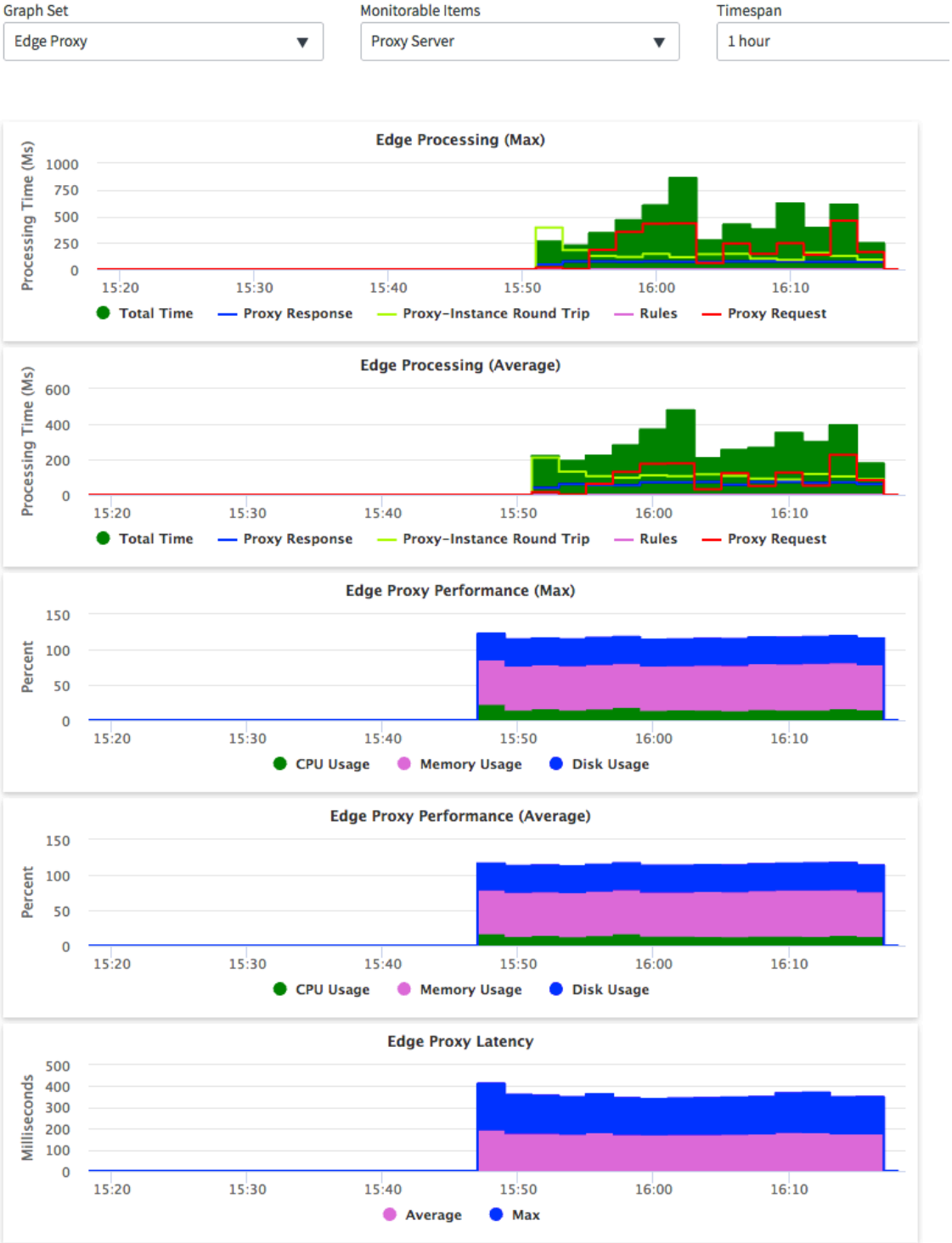
エッジ暗号化 パフォーマンスのホームページで設定されている Edge プロキシ グラフを使用して、ServiceNow プロキシサーバーの主要なパフォーマンスの傾向を表示します。次の傾向を監視します。

- クライアント、プロキシサーバー、およびインスタンスの間の最大および平均の応答時間。
- ホストマシンの CPU、ディスク領域、およびメモリの使用率。
- プロキシサーバーと ServiceNow インスタンス間の最大および平均のネットワークレイテンシー時間。

注:
エッジ暗号化 プロキシサーバーのうち名前が重複しているものについては、パフォーマンスの傾向は報告されません。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



Edge の処理 (最大および平均)

要求を処理するための最大および平均時間 (ミリ秒単位)。これらのデータ ポイントは、一般的な経時的傾向です。

- 合計時間：プロキシサーバーがクライアントから要求を受信して応答を送信するまでの時間。このデータ ポイントは、後続のデータ ポイントの合計です。
- プロキシの応答：プロキシサーバーがインスタンスからの応答を処理する時間。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- プロキシインスタンスの往復：プロキシサーバーがインスタンスに要求を送信して応答を受信するまでの時間。プロキシサーバーとインスタンス間のネットワーク レイテンシーと、インスタンスが要求を処理するために費やした時間が含まれます。
- ルール：プロキシサーバーが定義済みの暗号化ルールを使用して要求を評価する時間。
- プロキシの要求：プロキシサーバーがクライアント要求を処理してインスタンスに転送するまでの時間。

Edge プロキシのパフォーマンス (最大および平均)

ホスト マシンで使用されるリソースの最大および平均のパーセンテージ。

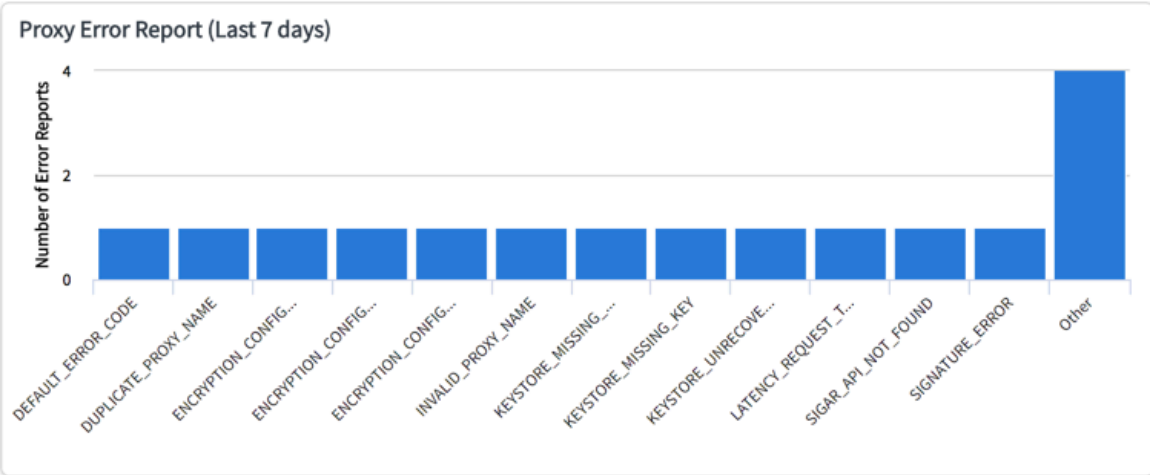
- CPU 使用率
- メモリ使用率
- ディスク使用率

Edge プロキシのレイテンシー

特定の時点における最大および平均のネットワーク レイテンシー (ミリ秒単位)。レイテンシーは、プロキシサーバーが単純な ping をインスタンスに送信して応答を受信するまでの往復時間によって決まります。

プロキシー エラー レポート

移動先 エッジ暗号化の設定 > 診断とトラブルシューティング > プロキシー エラー レポート をクリックして、過去 7 日間に収集されたすべてのプロキシサーバーエラーを表示します。



エラーは 1 分間隔で収集されます。エラー レポートは毎分生成されます。縦軸には、過去 7 日間の各エラーを含むエラー レポートの数が表示されます。たとえば、1 分のレポート期間に DEFAULT_ERROR_CODE エラーが複数回スローされた場合でも、DEFAULT_ERROR_CODE のバーには [エラー レポートの数] 軸上で 1 とのみ表示されます。

この画面から次の操作が行えます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- プロキシ エラー コードの各バーをクリックすると、プロキシサーバーごとの単一のエラーに関するレポートが表示されます。この画面からバーを再度クリックすると、エッジ暗号化 プロキシ統計情報テーブル [edge_encryption_stat] にエラー テキストを表示できます。エラー テキスト内のリンクをクリックすると、エラーの詳細と修正手順の候補を表示できます。
- [その他] をクリックすると、エラー レポートの 2 ページ目が表示されます。

注:
同じ名前のプロキシサーバーが複数ある場合、プロキシ エラー レポートには 1 つの DUPLICATE_PROXY_NAME エラーが表示されます。名前が重複するプロキシサーバーについては、他のエラーは報告されません。このエラーが発生した場合は、すべてのプロキシサーバーに一意の名前が付いていることを確認してください。

その他のモニタリング リソース

インスタンスは、すべての暗号化プロキシを追跡します。エッジ暗号化 プロキシサーバーはそれぞれ、起動時に登録されます。次の場合にインスタンスに通知が送られます。

- 新しい エッジ暗号化 プロキシサーバーが起動したとき。
- エッジ暗号化 プロキシサーバーが意図的にシャット ダウンされたとき。

エッジ暗号化 プロキシサーバーが、エッジ暗号化 がインストールされていないインスタンスを登録しようとした場合、プロキシは起動しません。

すべての暗号化設定ファイルが監査されます。削除済みレコードは、すべての暗号化設定ファイルで監査されます。監査レコードは sys_audit テーブルに格納されます。特定の設定レコードの履歴を表示するには、レコードを表示し、 履歴 > リスト メニューで。一括暗号化ジョブは監査されません。

さらに次のリソースを使用してプロキシサーバーを監視します。

テーブル	説明
無効な挿入試行 [sys_edge_encryption_invalid_insert_log]	次のデータを暗号化されたフィールドに保存しようとした試みのリスト。 • 暗号化されていないデータ。 • エッジ暗号化 プロキシから送られていないデータ。 この場合、インスタンスは、このデータを保存するすべての試行を拒否してログに記録します。security-admin ロールを持っている場合は、「無効な挿入試行」リストでログを表示できます。
ジョブの失敗 [sys_encryption_job_execution]	正常に実行されなかったジョブのリスト。
システムログ	インスタンスは、登録された各プロキシサーバーからのメッセージの有無を定期的にチェックします。プロキシサーバーから必要な期間内にメッセージが送信されなかった場合は、エラーがログに記録されます。ログ メッセージには、暗号化プロキシの情報と、プロキシが最後にインスタンスに ping を実行した時刻が記録されます。オンラインになっている暗号化プロキシがないとインスタンスが判断した場合は、メッセージがログに記録されます。これらのメッセージはシステムログに追加されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Edge プロキシの統計情報の収集を無効化または縮小する

エッジ暗号化 プロキシサーバーから Edge プロキシ グラフ セットの統計情報を ServiceNow パフォーマンスのホームページに送信しないようにするか、統計情報の収集頻度を減らします。

始める前に
必要なロール：admin または security_admin

このタスクについて
edgeencryption.properties 設定ファイルにプロパティを追加することで、次の操作が行えます。

- Edge プロキシ グラフ セットを無効にします。
- エッジ暗号化 プロキシサーバーによる統計情報の収集間隔を変更します。デフォルトでは、統計情報は 30 秒ごとに収集されます。

手順

1. プロキシサーバーのインストール ディレクトリーで、<インストール ディレクトリー>/conf/ フォルダーにある edgeencryption.properties 設定ファイルを開きます。
2. Edge Encryption プロキシサーバーのプロパティ のいずれかを追加します。
3. プロキシサーバーを再起動します。

エッジ暗号化 プロキシのデバッグログ記録を増やす

ログ記録のレベルを上げて、ログを解釈し、プロキシの問題をデバッグします。

現在、エッジ暗号化 プロキシのデバッグログを増やすための、3 つのオプションがあります。問題をデバッグするためにログ記録のレベルを上げることで、問題を調査するためのより詳細なログステートメントでの情報をテクニカルサポートに提供できます。

デバッグしている問題に応じて、次の 3 つの方法のいずれかでデバッグログを設定します。

- SSL 接続以外の問題のデバッグ
- プロキシを介した要求のタイミング測定基準のログ記録
- Edge Encryption プロキシとインスタンス間の SSL 接続に関する問題のデバッグ

すべてのデバッグケースについて、自分でログを表示して解釈するか、インシデントを開いて ServiceNow テクニカルサポートから問題の説明とその再現方法について解釈を得ることができます。

SSL 接続以外の エッジ暗号化 アプリケーションに関する問題のデバッグ

この方法を使用して、プロキシを停止して再起動することなく、エッジ暗号化 アプリケーションの問題をデバッグします。これらの手順により、ログ記録レベルが向上し、詳細なログステートメントを使用して根本原因のトラブルシューティングを行うことができます。

始める前に
必要なロール：admin

注:
$proxy_installation_location/conf/log4j2.properties ファイルに加えられた変更は、変更を行ってから約 60 秒以内にプロキシによって取り込まれます。プロキシを再起動する必要はありません。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. $proxy_installation_location/conf/log4j2.properties ファイルで、次の行を見つけます。

```
logger.edge.level=info
```

2. 上記の行を次のように変更します。

```
logger.edge.level=debug
```

3. 変更を保存します。
   変更が有効になるまでに最大 60 秒かかる場合がありますが、プロキシを再起動する必要はありません。
4. 問題を再現します。
5. $proxy_installation_location/logs/edgeencryption.log ファイルでアプリケーションに関連するデバッグログステートメントを確認します。

タスクの結果
プロパティを変更した後に、$proxy_installation_location/logs/edgeencryption.log ファイルで追加の詳細を確認できます。デバッグが終了したら、$proxy_installation_location/conf/log4j2.properties ファイルに加えた変更を元に戻します。

プロキシを介した要求のタイミング測定基準のログ記録

タイミング測定基準のログ記録を有効にして、エッジ暗号化 プロキシによって処理される各要求の測定基準ステートメントを追加します。これらの各タイミング測定基準ログステートメントには、処理時間や使用された暗号化ルールなど、要求に関する有用な情報が含まれています。

始める前に
必要なロール：admin

注:

追加のログ記録設定が $proxy_installation_location/conf/log4j2.properties ファイルに追加されます。加えられた変更は、ファイルの変更が行われてから約 1 分以内に動的に取り込まれるため、プロキシを再起動する必要はありません。

手順

1. ファイルの末尾に次の行を追加して、$proxy_installation_location/conf/log4j2.properties ファイルを変更します。

```
appender.timinglog.type=RollingFile
appender.timinglog.name=TimingLog
appender.timinglog.fileName=../logs/edgenetwork.log
appender.timinglog.filePattern=../logs/$
${date:yyyy-MM}/edgenetwork-%d{yyyy-MM-dd-HH}-%i.log.gz
appender.timinglog.layout.type=PatternLayout
appender.timinglog.layout.pattern=%d [%t] %-5p %m%n
appender.timinglog.policies.type=Policies
appender.timinglog.policies.size.type=SizeBasedTriggeringPolicy
appender.timinglog.policies.size.size=500MB
appender.timinglog.strategy.type=DefaultRolloverStrategy
appender.timinglog.strategy.max=4

logger.timing.name=com.snc.edgeencryption.metrics.EdgeEncryptionTimingMetricCache
logger.timing.level=debug
```

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

```
logger.timing.additivity=false
logger.timing.appenderRef.rolling.ref=TimingLog
```

2. ファイルを保存します。

タスクの結果
log4j.properties ファイルが保存されると、$proxy_installation_location/logs/edgenetwork.log ログファイルにネットワーク時間に関する次のタイプのメッセージが表示されます。

```
2022-07-21 12:56:15,783 [qtp1971991758-7700] DEBUG
 com.snc.edgeencryption.metrics.EdgeEncryptionTimingMetricCache -
 request_uri=/api/now/ui/presencesysparm_auto_request=true&cd=1658433375754
 request_method=POST client_request_received="2022-07-21 12:56:15,015"
 proxy_request_processing_time=6 all_rules_processing_time=0
 rule_executed="REST JSON" rule_execution_time=1 proxy_instance_round_trip=14
 proxy_response_processing_time=1 total_time_from_proxy=21 reponse_code=201
 glide_user=SCv3_1:BAz1ZK7ee9XoroG2nvMlixHpgTvsT4fY2bwQvnH2WdU=:y5HGsTTqo3Pjq6
G0xk4LoazCwCiWRJk4/6SpbXuBzqg=:6816f79cc0a8016401c5a33be04be441
 jsessionid_suffix=037A66
```

ログメッセージの値は次のとおりです。

```
request_uri: The URI being requested

request_method: The HTTP method being used, for example, GET, POST, PUT, PATCH,
 DELETE

client_request_received: The timestamp noting when the HTTP client request arrived at the
 Edge proxy

proxy_request_processing_time: How long the Edge proxy took to process the request in
 milliseconds

all_rules_processing_time: Total time it took to execute all of the Edge Encryption rules for the
 request in milliseconds

rule_executed: The name of the encryption rule that was executed

rule_execution_time: How long it took to execute listed rule_executed in milliseconds

proxy_instance_round_trip: The time from when the Edge proxy sent the request to the instance
 until the instance sent the response and was received by the edge proxy in milliseconds

proxy_response_processing_time: How long the Edge proxy took to process the response in
 milliseconds

total_time_from_proxy: The total time from when the Edge proxy received the request from the
 client and returned the response to the client in milliseconds

response_code: HTTP response code

glide_user: The glide_user cookie value

jsessionid_suffix: The JSession cookie suffix associated with the request
```

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

エッジ暗号化 プロキシとインスタンス間の **SSL** 接続に関する問題のデバッグ

この方法を使用して、エッジ暗号化 プロキシとインスタンスの間の SSL 接続に関する問題 (プロキシ経由のインスタンスへのアクセスが失敗するなど) をデバッグします。これらの手順により、ログ記録が増加し、詳細なログステートメントを見つけることができます。

始める前に
必要なロール：admin

> **注:**
> SSL 接続のデバッグは、TLS 接続タイプの問題をトラブルシューティングする場合にのみ関連します。実際には、これは一般的ではなく、めったに必要ありません。

手順

1. プロキシサーバーを停止します。
2. $proxy_installation_location/conf/wrapper.confファイル (Java スタートアッププロパティ) に次の行を追加します。

   ```
   wrapper.java.additional.<next available number in sequence> = -Djavax.net.debug=all
   ```

   例：

   ```
   For example: wrapper.java.additional.4 = -Djavax.net.debug=all
   ```

3. 変更を保存し、プロキシサーバーを再起動します。
4. 接続の問題を再現します。

タスクの結果
問題を再現した後、SSL 交換に関連するデバッグログステートメントを $proxy_installation_location/logs/wrapper_<current date>.log ファイルで見つけることができます。デバッグが終了したとき、前の手順で作成された行を削除するかコメントアウトすることで、追加のログ記録をリモートで実行できます。

ログ

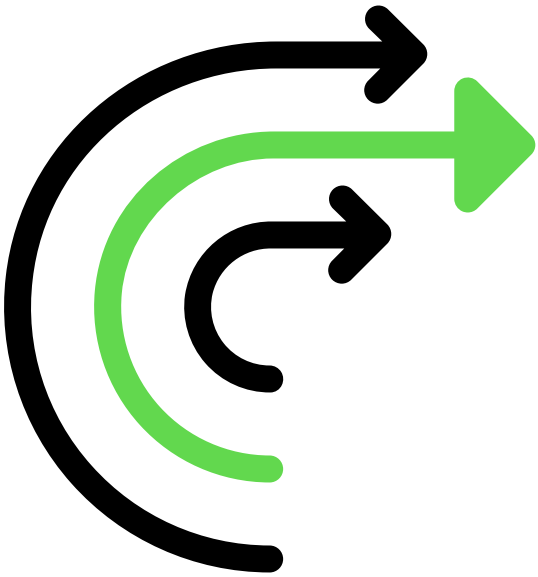
ログモジュールは、インスタンス内で発生するトランザクションやイベントのトラブルシューティングとデバッグに使用できるさまざまなログを提供します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

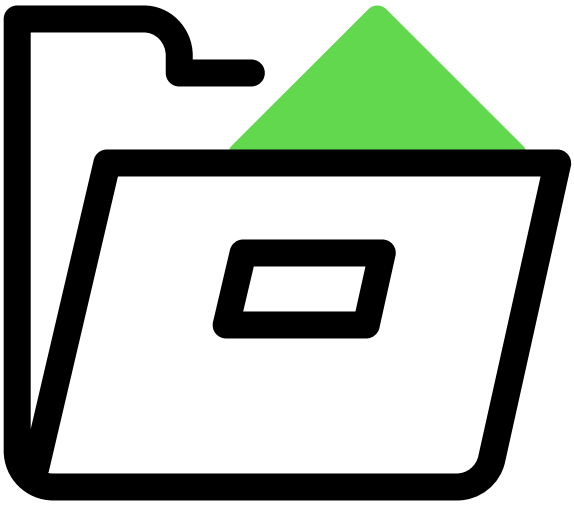
開始するには

システムログ



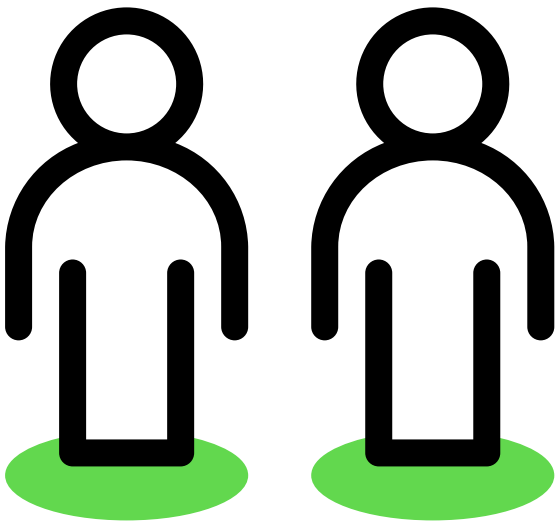
システムログモジュールは、インスタンス内で発生するトランザクションやイベントのトラブルシューティングとデバッグに使用できるさまざまなログを提供します。

ログエクスポートサービス



ログエクスポートサービス (LES) を使用すると、ServiceNow インスタンスからログを選択的に転送し、ログを使用してシステムにフィードできます。

ログ記録、監査、およびエラー



自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ログ記録と監査戦略を適用して、不審なアクティビティを適切なタイミングで特定して対処できるようにします。	

システムログ

システムログモジュールは、インスタンス内で発生するトランザクションやイベントのトラブルシューティングとデバッグに使用できるさまざまなログを提供します。

システムログモジュールから次のログにアクセスします。

ログ	説明
トランザクション	インスタンスのすべてのアプリケーションアクティビティ。
メールとプッシュ	システム内のすべてのインスタンスから送信されたすべてのメール通知とプッシュメッセージ。
イベントログ	システム内で発生するすべてのシステムイベント。
インポート	プラットフォーム内のデータインポートアクティビティ。
テーブル変更	システム内のすべてのテーブルに加えられた変更。
送信 Web サービスのログ記録	REST 要求や SOAP 要求などのすべての送信 Web サービスの要求。
署名画像	人事署名パッドの電子署名。
System	インスタンスプロセス、レコード、およびサーバーマシンのメモリ使用率などの重要でないイベントの警告とエラー。

ログファイルブラウザーを使用して、ログを検索してダウンロードします。ログ履歴でアーカイブされたログを検索することもできます。

その他のログ

インスタンスは、システムログモジュール内のログに加えて他のログを提供します。たとえば、システム診断モジュール はアップグレード履歴と遅いクエリログを提供します。これらを使用すると、クエリがプラットフォームのパフォーマンスにどのように影響しているかを把握できます。顧客アップデートテーブル は、システムで行われたすべての変更を記録します。

システムログ

インスタンスプロセス、レコード、およびサーバーマシンのメモリ使用率などの重要でないイベントの警告とエラーを表示します。

次の情報がシステムログで追跡されます。

- ワークフロー
- 設定
- チャットセッション
- システム内の各ページの各ビューのトランザクション (ネットワーク、サーバー、ブラウザのロード時間など)
- 受信メールと送信メール

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

- システムでトリガーされたイベント
- インポートと統合
- システムの警告、エラー、およびスクリプトログ
- プラグインのアクティベーション、更新セット、またはシステムのアップグレードに関するアップグレード情報

ログエントリは当日にのみ表示されます。他のログファイルを表示するには、ログファイルブラウザを使用します。このログには、すべてのオカレンスに関して次の情報が表示されます。

システムログ

フィールド	説明
作成日時	インスタンスを実行しているマシンのロケールのログ記録アクティビティの日時。
レベル	メッセージのタイプレベルは、デバッグ、エラー、警告、および情報です。 • 警告は、処理されて復旧されたエラーです。 • エラーは修正する必要があります。
メッセージ	オカレンスの性質に関するシステム生成メッセージ。
ソース	オカレンスの影響を受けるプロセスまたはエリアの名前。たとえば、オカレンスのソースはメールまたはメモリです。
ソースパッケージ	オカレンスに関連付けられているアプリケーションパッケージの名前。名前をクリックすると、このパッケージのストアアプリケーション [sys_store_app] レコードが表示されます。

ワークフローログ

- 次を含む、実行された各アクティビティ
  - 開始日時
  - 終了日時
  - ステータス (完了、キャンセル、タイムアウト、エラーなど)
  - 結果
  - 障害の説明 (エラーが発生した場合)
- 次を含む移行履歴：
  - 移行時間
  - アクティビティの移行元
  - アクティビティの移行先
  - トリガーされた移行
- ワークフローに追加されたログステートメントを含むワークフローログ

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

構成情報

- 実行したアクション (挿入、更新、削除など)
- 変更のカテゴリ
- 変更とともに記録されたコメント
- 変更の名前
- 変更の XML の差異
- 変更が関連付けられている更新セット
- 変更の日時
- 変更を加えたユーザー
- 変更が行われたテーブル
- 変更されるオブジェクトの名前
- 変更されるオブジェクトのタイプ
- フォームまたはリストに加えられた変更の表示

トランザクションログ

トランザクションログには、インスタンスのすべてのブラウザアクティビティが記録されます。システム障害のデバッグを支援するために、トランザクションログをアプリケーションスコープでフィルタリングし、表示されるトランザクションを特定のスコープで発生したトランザクションのみに制限することができます。

トランザクション ログは、すべてのアクティビティについて次の情報を提供します。

フィールド	説明
作成日時	インスタンスを実行しているマシンのロケールのアプリケーションアクションの日時。
タイプ	記録されたトランザクションのタイプ。
作成者	このアクティビティを作成したユーザー。
作成元アプリケーション	トランザクションが開始されたアプリケーションスコープ。トランザクションがグローバルスコープで開始された場合、[グローバル] が表示されます。
応答時間	アプリケーション要求の往復応答時間 (ミリ秒)。
ネットワーク時間	アプリケーション要求が行われた後のネットワーク応答の待ち時間 (ミリ秒)。
出力長	インスタンスからアプリケーションに送信される出力文字列のサイズ (バイト)。
SQL カウント	このアクティビティに対して実行された SQL サーバーのコマンド数。
ビジネスルール数	このアクティビティに対して実行されたビジネスルール数。
ビジネスルール時間	このアクティビティのビジネスルールの実行経過時間。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
URL	クライアントアプリケーションによって接続されたアプリケーションまたはモジュール。
Sys ID	要求を行うクライアントインスタンスのシステム生成識別子。この ID は、複数のインスタンス (ノード) がデータベースと通信するクラスター環境で使用されます。
IP アドレス	要求を行うクライアントの IP アドレス。
GZip 完了	圧縮された Web ページがアプリケーションによって要求されたかどうかを示します。
プロトコル	このインスタンスのアプリケーションで使用される HTTP プロトコル。

クライアントトランザクションタイミング

クライアントトランザクションタイミングプラグインは、クライアントとサーバー間で行われるトランザクションの期間に関する追加情報を提供することで、システムログを拡張します。

時間がどこで消費されているか、トランザクション中にどのように時間が費やされたかを表示することで、ソースに至るまでパフォーマンスの問題を追跡できます。

このプラグインでは、応答時間インジケーター 応答時間インジケーター を有効にする必要があり、次のブラウザーから情報を収集します。

- Firefox
- Internet Explorer
- Chrome

クライアントトランザクション情報

このプラグインをインストールすると、クライアントトランザクションモジュールがシステムログアプリケーションに追加されます。これは、最終日内にログに記録されたクライアントとサーバーとの間でのすべてのトランザクションのリストを提供します。

クライアントトランザクション情報

フィールド	説明
作成日時	トランザクションが記録された時刻
応答時間	サーバーがトランザクションの実行に費やしたミリ秒数
ビジネスルール時間	トランザクションによってトリガーされたビジネスルールによって費やされたミリ秒数
SQL 時間	SQL データベースが費やしたミリ秒数
クライアント応答時間	(Load_completion_time) - (start_time)。サーバー時間を含みます。
クライアントネットワーク時間	クライアントがネットワークの接続に費やしたミリ秒数
ブラウザー時間	ブラウザーがトランザクション中に費やしたミリ秒数
クライアントスクリプト時間	クライアントスクリプトの実行に費やされたミリ秒数
UI ポリシー時間	UI ポリシーの実行に費やされたミリ秒数
タイプ	トランザクションタイプ：

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

クライアントトランザクション情報 (続く)

フィールド	説明
	• フォーム • リスト • その他
テーブル	表示されるテーブルの名前。たとえば、incident、change_request など。
表示	このフォーム/リストの表示

クライアント詳細情報

すべてのフォームのレンダリング (リストのレンダリングではない) について、クライアントタイミングのより詳細なブレークダウンも追跡されます。詳細を見るには、特定のクライアントトランザクションレコードをドリルダウンし、画面の下部にある関連リストを確認します。

クライアント詳細情報

フィールド	説明
順番	この操作が行われたロード時の順番
タイプ	操作のタイプ
名前	この特定の操作の説明的な名前
期間	この操作が完了するまでにかかったミリ秒数

プッシュログ

プッシュログを参照して、システムから送信するためにキューに入れられているプッシュ通知のステータスを追跡します。

プッシュログを表示するには、次に移動します。 システムログ > プッシュ通知. プッシュログを表示するには、ユーザーは push_admin または admin ロールを持っている必要があります。

プッシュログフィールド

フィールド	説明
請求	プッシュ通知を送信するスケジュール設定済みジョブによって生成される識別番号。この数は、複数のプッシュジョブスケジュール間で一貫性を確保するために [要求] フィールドに適用されます。
ペイロード	プッシュ通知のコンテンツ。
キュー数	システムがプッシュ通知を送信しようとした回数。プッシュ通知のステータスは、そのキュー数に関連しています。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

プッシュログフィールド (続く)

フィールド	説明
	• キュー数が予想よりも長く 0 になっている場合は、プッシュ通知を送信しようとしているジョブスケジュールはありません。 • キュー数が 0 より大きく、[タイプ] が [成功] の場合、これは最終的に送信する前にシステムがプッシュ通知を送信しようとした回数であると推測できます。 • キュー数が 10 に達すると、プッシュ通知の送信が停止されます。[タイプ]が [失敗] に変わります。
要求 ID	プッシュ通知の一意の識別番号。メールのメッセージ ID と同様に、要求 ID はプッシュ通知の相関トークンとして使用されます。
タイプ	プッシュ通知が送信されたかどうかを示すステータス。[タイプ] 列には、次の値を指定できます。 • **failure**：メッセージを送信できませんでした。 • **pending**：メッセージは処理のためにキューに入れられます。 • **success**：メッセージは正常に送信されましたが、モバイル端末で受信されたとは限りません。

関連情報

ジョブスケジュール

システムメールログおよびメールボックス

システムメールログは、インスタンスが作成またはを受信するすべてのメールを記録します。システムメールボックスは、このログのフィルター済みのビューです。

メール [sys_email] レコードでは、インスタンスが作成または受信する各通知メールが記録されます。これらのレコードのログに移動するには、次の場所を参照してください。 システムログ > メール.

システムメールボックスは、メール [sys_email] テーブルのフィルター済みのビューです。インスタンスは、[タイプ] および [ステータス] フィールドの値に応じてシステムメールボックスに、メールレコードをアサインします。詳細については、「システムメールボックス」を参照してください。

以下のフィールドは、システムログのレイアウトと任意のシステムメールボックスに含めることができます。

メール ログ

フィールド	説明
メールボックス	このメールレコードを表示するシステムメールボックス。インスタンスは、[タイプ] および [ステータス] フィールドの値に応じて、このフィールドの値を設定します。
ステータス	メールの現在の状態 (エラー、無視、処理済み、または準備完了)。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

メール ログ (続く)

フィールド	説明
受信タイプ	受信メールのタイプ (なし、転送、新規、または返信)。
タイプ	メールのステータス。選択肢は次のとおりです。 • received：サーバーでこのメールが受信されました。 • received - ignored：サーバーでこのメールが受信されましたが、受信メールアクションの目的のためにインスタンスによって無視されました。通常、これらのメールはスパムメールまたは自動返信のいずれかです。詳細については、エラー文字列フィールドを参照してください。 • send - failed：サーバーがメールを送信しようとしましたが失敗しました。詳細については、エラー文字列フィールドを参照してください。 • send - ignored：サーバーはこのメールの送信をスキップしました。通常、これは生成されたが受信者のメール アドレスがないメール、または重複したメール用です。詳細については、エラー文字列フィールドを参照してください。 • send - ready：メールは送信準備が整っていますが、メールサーバーによって送信されていません。通常、メールがこの状態になるのは短時間だけです。 • 送信 - 翻訳 - 準備完了：メールの翻訳中にメールが生成され、送信されます。通常、メールがこの状態になるのは短時間だけです。 • sent：エラーや問題なくインスタンスによってメールが送信されました。
ターゲット	特定のレコードの挿入、更新、または削除によってメールが生成された場合、レコードを参照するドキュメント ID。
ユーザー	メール通知が送信されたインスタンスの、ユーザーレコードからのユーザーの名前。 **注:** これは文字列フィールドです。
通知タイプ	通知のタイプ。選択肢は次のとおりです。 • なし • SMS • SMTP
UID	サーバー上で保存されているメールの一意の ID。
作成日時	インスタンスを実行しているマシンのロケールのメールアクティビティの日時。
削除済み	受信メールの場合は、メールがメールサーバーから削除されたかどうかを示します。
重み付け	同じテーブル上の他の通知との相対的な送信優先度を決定する、メールの重み。
重要性	緊急など、重要度が変更されたメールが送信されたことを表示。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

メール ログ (続く)

フィールド	説明
元のイベントおよびメール通知	通知によって生成されたメールの場合、メールを作成したイベントと通知を格納している埋め込みリスト。
件名	メールの件名。通知の場合は、次の件名で件名テキストを作成します。 システム通知 > メール > 通知.
エラー文字列	メールが送信されなかった理由を特定する、メール サーバーからキャプチャされたエラー文字列。これは、メールが送信に失敗した場合にのみ記録されます。
受信者	受信者のメールアドレス。
本文	生の HTML マークアップで表示されるメールの本文。関連リンクの HTML 本文のプレビューを使用して、本文テキストをレンダリングされた HTML として表示します。
コンテンツタイプ	メールのコンテンツ タイプ。
ヘッダー	メールに埋め込まれたヘッダー。

イベントログ

イベントログには、Now Platform 内で発生するすべてのシステムイベントが記録されます。

このログは、発生するすべてのイベントについて次の情報を提供します。

イベントログ

フィールド	説明
作成日時	インスタンスを実行しているマシンのロケールのイベントの日時。
名前	イベント登録にリストされているイベントの名前。
URI	イベントを生成した HTTP クエリ。
Parm1	イベントと受信者に依存するイベント固有の値。
Parm2	イベントと受信者に依存するイベント固有の値。
テーブル	このイベントで機能するデータベーステーブル。
処理日時	イベントが処理された日時。この時間は、インスタンスを実行しているマシンのロケールを反映しています。
処理時間	このイベントの処理に要した時間 (ミリ秒)。
キュー	プロセッサーキュー名。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

インポートログ

インポートログには、プラットフォーム内のデータインポートアクティビティに関する情報が詳細形式で表示されます。

特定のログを生成したインポートセットの詳細については、次を参照してください。 インポートセット > 変換履歴.

このログは、すべてのインポートに次の情報を提供します。

インポートログ

フィールド	説明
作成日時	インスタンスを実行しているマシンのロケールのインポート日時。
レベル	表示されるメッセージのタイプ。インポートファイルの場合、レベルは情報です。
メッセージ	インポートのステータスに関するシステム生成メッセージ。
ソース	統合などのインポートの外部ソースの名前。

システム診断モジュール

システム診断アプリケーションは、プラットフォームに関連するログを提供します。

次のログを利用できます。

アップグレード履歴

インスタンスへのすべてのアップグレードを追跡します。

遅いクエリー

クエリーがプラットフォームのパフォーマンスにどのように影響するかについてのインサイトを提供します。「遅いクエリログの使用」を参照してください。

顧客アップデートテーブル

システムで行われた変更は、顧客アップデート [sys_update_xml] テーブルに時系列に記録されます。以下に示すように、いくつかの例外があります。

このテーブルに移動するには、ナビゲーションフィルターに「sys_update_xml.list」と入力します。Update Sets の詳細については、「System Update Sets」を参照してください。

更新ごとに次の情報が保存されます。

顧客アップデートテーブル

フィールド	説明
名前	更新されたレコードを識別する名前。
作成日時	顧客アップデートレコードが作成された日時。
作成者	変更を実行したユーザー。
タイプ	更新のタイプ。
更新日時	顧客アップデートレコードが更新された日時。
更新者	更新を実行したユーザー。
更新	レコードが更新された回数。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

顧客アップデートテーブル (続く)

フィールド	説明
ターゲット名	変更された要素の名前。
表示	フォームレイアウトの変更である場合、変更されたフォームのビュー。
ペイロード	変更後のレコードの XML コンテンツ。
リモート更新セット	変更がリモート更新セットによって実行された場合は、その更新セットへの参照。
ローカル更新セット	変更が関連付けられている更新セット。

注:
顧客アップデートレコード (sys_update_xml) に表示されないアプリケーションの変更の例：

- updateSynch = false のメタデータのタイプ
- 表示名の変更など、テーブルやフィールドのカスケード変更
- 他のアプリケーションからの未解決のメタデータ参照 (要素に「表示値」がない)
- 結合ファイルの sys_id の変更
- sys_documentation を生成する可能性のあるフロー/フローアクションへの変更
- テーブルの作成時に生成される ua_table_license_config レコード
- 自然言語処理など、バックグラウンドで実行されているジョブ
- sys_update_xml が手動で変更または削除されるケース

詳細については、「変更を収容」を参照してください。

自動翻訳

ログ履歴

古いログは、テーブルローテーションとテーブル拡張を使用してアーカイブされます。

デフォルトでは、次のスケジュールを使用して共通ログがアーカイブされます。

共通ログアーカイブスケジュール

テーブル	アーカイブスケジュール	ローテーション	タイプ
イベント [ecc_event]	毎日	7	ローテーション
キュー [ecc_queue]	毎日	7	ローテーション
イベント [sysevent]	毎日	7	ローテーション
ログ [syslog]	毎週	8	ローテーション
トランザクションログ [syslog_transaction]	毎週	8	ローテーション

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

共通ログアーカイブスケジュール (続く)

テーブル	アーカイブスケジュール	ローテーション	タイプ
メール [sys_email]	30 日ごと	8	拡張

ログファイルブラウザを使用する

インスタンスは、 ユーティリティログファイルブラウザとログファイルのダウンロードを提供します。

使用方法 システムログ > ユーティリティ > ノードログファイルブラウザー をクリックして、システムログエントリを表示します。次のフィルターを使用して、ログファイルを検索できます。

ログファイルブラウザ

フィールド	説明
開始時間	インスタンスを実行しているマシンのロケールに対して検索する範囲の開始日時。
セッション ID	ログエントリを生成したセッションを識別する、システムによって生成された 16 進数の文字列。
終了時間	インスタンスを実行しているマシンのロケールに対して検索する範囲の終了日時。
メッセージ	オカレンスに関するシステム生成の説明。
レベル	表示されるメッセージのタイプ。レベルは、デバッグ、エラー、警告、および情報です。警告は、処理されて復旧されたエラーです。エラーは修正する必要があります。
スレッド名	ログファイルを作成したスレッドのシステム生成識別子。
最大行数	特定のフィルターに対して返されるレコードの最大数。

インスタンスは 2 日ごとにシステムログの圧縮アーカイブを作成し、21 日後にログアーカイブを消去します。

重要:
ノードが廃止されると、ノードのログファイルはすぐに消去されます。つまり、さらに 21 日間はアーカイブされません。

ログファイルのアーカイブをダウンロードして、 システムログ > ユーティリティ > ノードログファイルのダウンロード. リストからログアーカイブを選択し、[関連リンク] の [ログをダウンロード] をクリックしてアーカイブを開くか保存します。

注:
ログファイルは、現在ログインしているノードでのみ使用できます。現在ログインしているノードを表示するには、次に移動します。 システム診断 > 統計.

[トランザクション] フォームと [アクティブなトランザクション] フォームの新しい [**Syslog** レコードを表示] ボタンを使用して、トランザクションの実行中に生成されたシステムログエントリを表

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

示します。トランザクションには、任意の数の syslog エントリを含めることができます。すべてのトランザクションに複数の syslog エントリがあると、トランザクションをそれぞれの syslog エントリに関連付けることが困難になります。[Syslog レコードの表示 **(Show Syslog Records)**] UI アクションは、syslog テーブルをクエリするための URL を作成することで、アクティブなトランザクションと完了したトランザクションをそれぞれの syslog エントリに相互に関連付けるのに役立ちます。特定のトランザクションの正しい syslog エントリを特定すると、セキュリティ上の問題のデバッグと対処に役立ちます。

ログセキュリティの強化

ノードのログ行の [アトリビューション] フィールドを調べて、ログメッセージを生成したスクリプトまたはコンポーネントを特定します。トランザクションの開始行には、実行された要求のタイプを識別する新しいフィールドが含まれます。

新しい機能拡張を使用して、以下を実行します。

- 各ログ行のソースオリジネータをトレース
- 発信者情報が利用できない場合は、Java クラス名と属性を出力します
- 各トランザクション行の先頭には、トランザクション ID とトランザクションタイプが含まれています

各ログ行のトランザクション ID を使用して、各ログ行で指定された情報を把握します。トランザクションタイプを特定すると、各ログ行のオリジネータ情報を取得します。各ログ行のトランザクションタイプとオリジネータ 情報の両方が一緒になって、各ノードログ行の必要なソース情報 を提供します。

注:
アトリビューションのSYS_UI_MACROおよびSERVICE_PORTAL_WIDGETスクリプトタイプは報告されません。

トランザクションタイプ

トランザクションの種類の一覧を次に示します。

- リスト
- フォーム
- XMLHttp
- レポート
- SOAP
- エクスポート
- スケジューラ
- テキスト検索
- その他
- REST
- JSON
- AMB
- アーカイブ
- バッチ REST
- Instance Scan

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

システムプロパティ

この機能に必要なシステムプロパティは次のとおりです。

- Glide.log.append.attribution:このプロパティはデフォルトで有効になっています。各ノードラインの帰属情報のオン/オフを切り替えます
- Glide.db.log.append.classname.attribution:このプロパティはデフォルトで有効になっています。Javaクラス名の属性のログ記録をオン/オフにします

ログの改ざんの回避

システムログテーブルの保護ルールを設定して、アプリケーションログレコードの変更と削除の範囲を制限します。このルールを使用することで、これらのテーブルの変更や変更の試行のログ記録を決定できます。

security_admin であれば、Protected Tables プラグイン (com.glide.Protected_tables) をアクティブ化すると、プラットフォームで次のシステムログテーブルの更新、挿入、および削除操作を制限できます。

- syslog
- syslog_transaction
- sys_outbound_http_log
- sysevent
- sys_audit
- sys_push_notification
- syslog_app_scope
- protected_table_configuration (設定は変更不可)

注:
com.glide.protected_tables プラグインで保護されるのは上記のシステムログテーブルのみです。レコードを更新、挿入、または削除しようとすると、protected_table_log テーブルにメッセージが記録されます。

詳細については、「ログ保護プラグインのインストールと設定」を参照してください。

システムログテーブルごとに、次のいずれかのログ保護レベルを指定できます。

- 試行をブロックしてログ記録：変更をブロックして試行をログに記録する
- 試行のブロックのみ：変更をブロックして試行をログに記録しない
- 試行のログ記録のみ：変更はブロックしないが試行はログに記録する
- 試行をブロックおよびログに記録しない：変更をブロックせず、試行もログに記録しない

レコードが最初に作成された後に変更しようとすると、プラットフォームが各システムログテーブルに指定されたログ保護レベルを使用してその試行をブロックまたはログに記録します。

注:
security_admin であれば、各システムログテーブルのデフォルトのログ保護レベルを上書きすることで、インスタンスのカスタマイズ内容に適合させることができます。

システムログテーブルの変更が試行された場合、その試行は protected_table_log テーブルにログに記録されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

> **注:**
> テーブルに保護レベルが指定されていない場合、変更の試行は protected_table_log テーブルに一切記録されません。

管理パネルのテーブルでプラグイン操作を無効にするには、com.glide.security.protected_table.enabled プロパティを false に設定します。詳細については、「ログ保護のプロパティの作成」を参照してください。

ログ保護プラグインの設定

各テーブルと操作の保護ルールを設定して、ログ保護プラグインの設定を完了します。

始める前に

必要なロール：security_admin

手順

1. 移動先 すべて > 保護テーブル > ログの保護.
   [管理パネル] ページが表示されます。

   > **注:**
   > Utah リリース以降、Protected Tables プラグインはデフォルトでインストールされていますが、無効になっています。

2. プラグインの設定を続行するには、ロールを security_admin に昇格させます。

   a. [システム管理者] を選択します。

   b. [ロールを昇格] を選択します。
   ロールの昇格モーダルが表示されます。

   c. security_admin オプションを選択してロールを昇格し、[更新] を選択します。

3. 各テーブルと操作の保護ルールを設定します。保護ルールは、更新、挿入、削除に適用されます。一部のテーブルでは保護レベルを変更できません。syslog および syslog_app_scope テーブルには、更新および削除保護のための固定値があります。protected_table_configuration テーブルには、3 つの操作すべての固定の保護値があります。

   > **注:**
   > sysevent テーブルでは、挿入保護をブロックに設定できません。
   >
   > 以前のリリースで syslog に対して [子テーブルに適用] をオンにした場合、Utah リリースへのアップグレード時に、syslog と同じ保護ルールで子テーブルがログ保護に追加されます。これは syslog でのみ発生し、他のテーブルでは発生しません。

4. [ログの保護を有効にする **(Enable Log Protection)**] トグルを選択して、機能を有効にします。

   > **注:**
   > このプラグインは、sys_properties テーブルの com.glide.security.protected_table.enabled プロパティを変更するだけで無効にできます。

ログ保護のプロパティの作成

ログの改ざんのリスクを回避するために、ログ保護のプロパティを作成します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

始める前に
必要なロール：admin

手順

1. *com.glide.security.protected_table.enabled* プロパティが [システムプロパティ] リストに存在しない場合は、[新規] を選択します。
   新しいシステムプロパティのフォームが表示されます。
2. フォームで、詳細を入力します。

フィールド	説明
名前	プロパティの名前 com.glide.security.protected_table.enabled
アプリケーション	このプロパティがあるアプリケーション。
説明	プロパティの説明
選択肢	
タイプ	値のタイプ：true または false
値	プロパティの実際の値
キャッシュを無視	キャッシュの内容を無視するオプション
プライベート	プロパティを非公開にするオプション ○ 読み込みロール ○ 書き込みロール

3. [送信] を選択してプロパティを作成します。

ログエクスポートサービス (ルス)

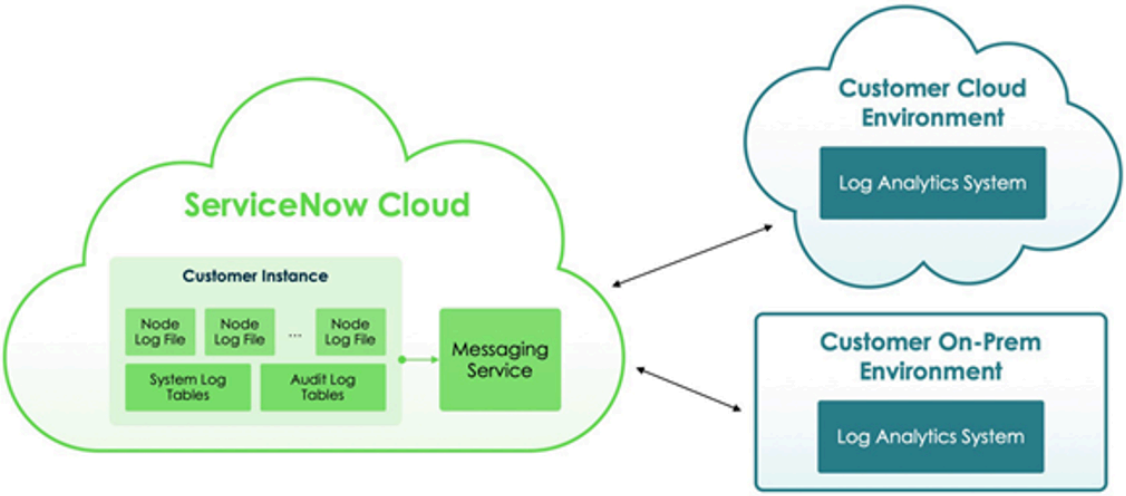
ログエクスポートサービス (LES) を使用すると、インスタンス、システム、およびアプリケーションのログをエンタープライズセキュリティ分析ツールにシームレスにエクスポートできます。このサービスは、セットアップと保守が容易な分析ツールとの非常にスケーラブルでほぼリアルタイムの統合を提供します。

統合ツールを使用すると、分析ソリューションを活用して以下を実行できます。

- セキュリティ上の脅威の検出 ServiceNow とセキュリティインシデントの分析
- アプリのパフォーマンスのトラブルシューティングと最適化ServiceNow
- ユーザーエクスペリエンスの監視と最適化ServiceNow

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



LES は、生成された Hermes メッセージングサービスログ イベントのコピーを .

Hermes メッセージングサービス は、インスタンスで大量の Kafka イベントを生成および使用可能にする、Apache Kafka に構築されたマルチテナント、マルチクラスター、データトランスポート、およびキューイングサービスです。はHermes メッセージングサービス、、(LES)、および インスタンスデータレプリケーション (IDR) (ログエクスポートサービスIDR) の一部としてApache Kafka 向けストリームコネクト利用可能な Now Platform 機能です。

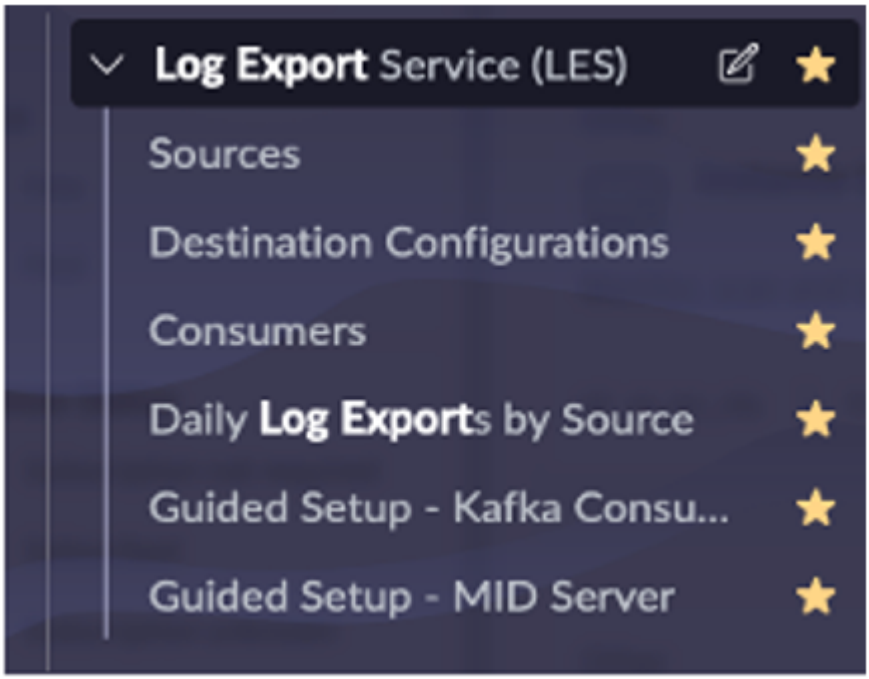
クラウドまたはオンプレミスの外部ログ分析システムは、からのログイベント Hermes メッセージングサービスを使用して使用できます。LES には、ログを使用するための 3 つの接続オプションがあります。

- 専用 :専用MID サーバーMID サーバーはオンプレミスまたはクラウドにインストールされ、自動的に接続Hermes メッセージングサービスされ、ログイベントを継続的にプルし、REST接続を介してログ分析ツールにプッシュします。
- ログ分析ソリューション (Splunk など) から Kafka コネクタを活用する: 選択したログ分析製品の Kafka コネクタは、オンプレミスまたはクラウドにインストールされ、自動的に接続 Hermes メッセージングサービスされます。 からログ イベントを継続的にプルし、ログ分析ツールにプッシュします。
- Kafka システムから直接:Kafka システムは、 に直接接続し、ネイティブの Kafka プロトコルコマンドと接続を使用して、 Hermes メッセージングサービス そこからログイベントをプルします。

LES を構成および管理するには、から LES をインストールする ServiceNow Store必要があります。LES アプリケーションには、サービスのインストールに役立つ Guided Setup、サービス (ログソース、コンシューマー、および宛先) を構成するためのページ、およびログの作成と消費を理解するためのレポートが用意されています。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



注:
新しいソース構成を作成することもできます。詳細については、「ログソース構成の作成」を参照してください。

ログエクスポートサービス ロール

ログエクスポートサービス はこれらのロールに併せてインストールされます。

アプリケーション管理者 **[sn_logstoanalytics.admin]**

ユーザーごとのサブスクリプションの管理の詳細については、アカウント担当者に問い合わせ てください。

このロールは LES アプリケーションとともにインストールされ、管理者以外のロールがアプリケーションを使用できるようにします。

ロールを含む

ロール内に含まれるロールのリスト。

なし。

グループ

このロールがデフォルトでアサインされているグループのリスト。

なし。

昇格

ロールが昇格されたロールかどうか。昇格されたロールはユーザーまたはグループにアサインされず、昇格で使用する必要があります。詳細については、を参照してください特権ロールへの昇格。

なし。

特別な考慮事項

なし。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

システム管理者 [admin]

ユーザーごとのサブスクリプションの管理の詳細については、アカウント担当者に問い合わせ てください。

LES ストアアプリケーションのセットアップには、admin ロールが必要です。

ロールを含む

ロール内に含まれるロールのリスト。

- sn_templated_snip.template_snippet_admin
- sn_employee.admin
- taxonomy_admin
- sn_ace.ace_user
- sn_hr_sp.esc_admin

グループ

このロールがデフォルトでアサインされているグループのリスト。

なし。

昇格

ロールが昇格されたロールかどうか。昇格されたロールはユーザーまたはグループにアサインされず、昇格で使用する必要があります。詳細については、「特権ロールへの昇格」を参照してください。

いいえ。

特別な考慮事項

なし。

ログソース

ログエクスポートサービス (LES) は、一部のシステムログテーブル、監査テーブル、およびアプリケーションノードログファイルからログソースをエクスポートできます。

LES でエクスポートできるログソースは次のとおりです。

- システムログテーブル
  - syslog テーブル:インスタンスプロセス、レコード、およびサーバーマシンのメモリ使用率などの重要でないイベントの警告とエラーを表示します
  - syslog_transactionテーブル:インスタンスのすべてのブラウザーアクティビティを表示します
  - sys_outbound_http_logテーブル:REST や SOAP などの送信 Web サービスのすべての要求と応答を表示します
- 監査テーブル:sys_auditテーブルビューを使用して、監査対象として選択したテーブルに加えられた変更を記録します
- アプリケーションノードのログファイル:localhost ログファイルを使用して、アプリケーションノードのエラーを表示します。インスタンスには複数のノードがあり、各ノードには複数のログファイルがあります。

上記のログソースのスキーマと目的の詳細については、「」を参照してください システムログ 。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

ログソース構成の作成

ログソース構成を作成して、転送するログのフィルターを規制および設定します。

始める前に

必要なロール：admin または sn_logstoanalytics.admin

手順

1. 移動先 すべて > ログエクスポートサービス.
   ソース構成のリストが表示されます。
2. 新しいソース構成を作成する場合は、[新規] を選択します。
   既存のソース構成を選択して変更することもできます。
   [ソース] フォームが表示されます。
3. フォームのフィールドに入力します。

ソースフォーム

フィールド	説明
ソースタイプ	ログソースのタイプ ○ ノードログ ○ テーブル 詳細については、「ログソース」を参照してください。
ログレベル	ログ記録出力を制御するために使用できる一連の標準ログ記録レベル。規則に従って、各レベルは同等以上の重大度のログを転送します。 **注:** このフィールドは、次のいずれかの条件が満たされた場合にのみ表示されます。 ○ ソースタイプとして [ノードログ] を選択した場合 ○ ソースタイプとして [テーブル] を選択し、テーブルが syslog である場合
受け入れ	ログが Hermes に転送される形式を指定します。JSON またはプレーンテキストとして送信できます。
テーブル	テーブルタイプログのテーブルの選択。 **注:** このフィールドは、[ソースタイプ] として [テーブル] を選択した場合にのみ表示されます。
フィルタタイプ	ログを選択的に転送する条件。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	注: このフィールドは、syslog または sys_audit のいずれかをテーブルとして選択した場合にのみ表示されます。

4. 新しいソース構成を作成するには、[送信] を選択します。

LES V2 のセットアップと Hermes からのログの生成/消費

LES V2 をセットアップして、ServiceNow インスタンスまたは MID Server のいずれかを使用して Hermes からログを生成および消費できるようにする新機能を使用します。

注:
ガイド付き設定は LES セットアップで使用できます。以下とアプリケーション UI の指示に従って、LES のセットアップを正常に完了します。

Servicenow インスタンスでの LES V2 セットアップ

ServiceNow インスタンスで LES V2 をセットアップし、Hermes からログを生成して消費します。

始める前に
インスタンスのバージョンは Vancouver 以降である必要があります。

必要なロール：admin

手順

1. LES ストアアプリケーションのエンタイトルメントを取得します。
詳細については、「Entitle an application from your ServiceNow instance」を参照してください。
2. 移動先 システムアプリケーション > 利用可能なすべてのアプリケーション > すべて をクリックしてログエクスポートサービスをインストールします。

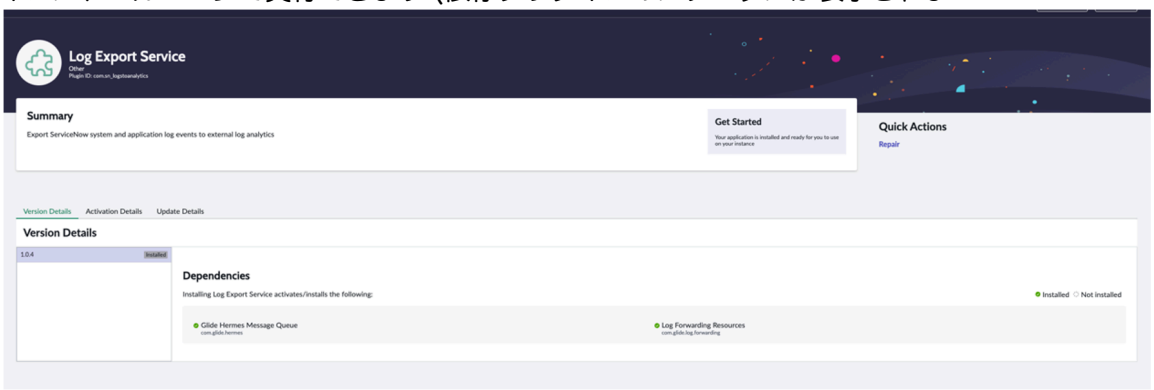
   注:
   バージョンが 2.0.0 以降であることを確認します。

3. インスタンスで Hermes が構成されるまで待ちます。
この構成は、LES アプリケーションのインストール中にバックグラウンドで実行されます。Hermes の構成中にエラーが発生したと思われる場合は、以下を確認してください。

自動翻訳

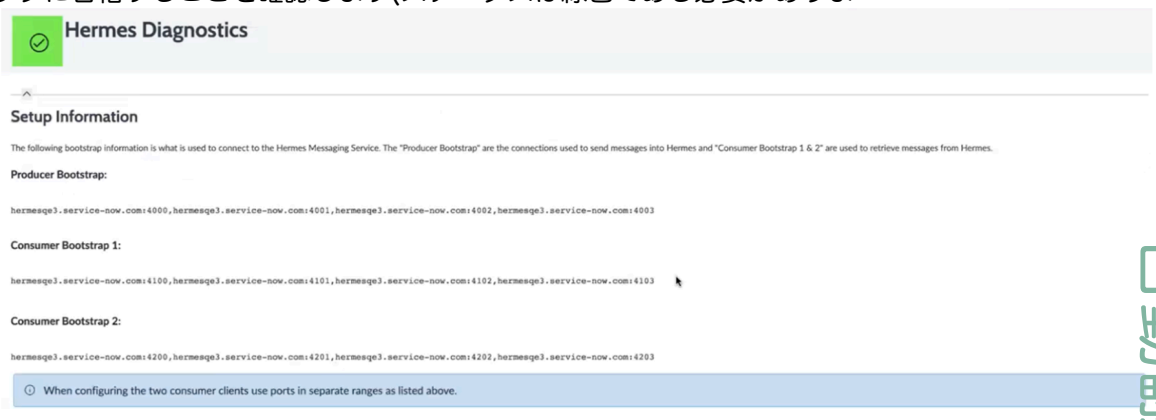
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- Hermes プラグインが正常にインストールされていることを確認します。これは LES インストールページで実行できます (依存プラグインのステータスが表示されま



す)。

- Hermes 診断ページを確認します (admin または hermes_admin ロールが必要です)。移動先 **Hermes** メッセージングサービス > 診断 そして、すべてのチェックに合格することを確認します(ステータスは緑色である必要がありま



す)。

LES は、Hermes Messaging Service と呼ばれる Now Platform 機能を活用します。Hermes Messaging Service は、Apache Kafka 上に構築されたマルチテナント、マルチクラスターのデータ転送、およびキューイングサービスであり、インスタンスで大量の Kafka イベントを生成および消費できます。

Apache Kafka は、組織内のビジネスシステム間でデータを交換するための単一の統合ポイントを提供するオープンソースのデータストリーミングプラットフォームです。詳細については、「Hermes Messaging Service」を参照してください。

ServiceNow は、LES アプリケーションのインストール時に、基盤となる Hermes Messaging Service インフラストラクチャをプロビジョニングします。このプロセスは、LES アプリケーションのインストールを要求してから完了するまでに数時間かかる場合があります。

> **注:**
> Hermes 診断ツールを使用して、Hermes Messaging Service が稼働していることを確認することをお勧めします。これは、後で潜在的な接続の問題をトラブルシューティングする必要がある場合にも役立ちます。

> **注:**
> Hermes がインストールされていない場合は、「ページが見つかりません」というメッセージが表示されるので、システム管理者にお問い合わせください。

4. Hermes から証明書を取得します。

> **注:**
> このステップを完了するには、admin または hermes_admin ロールが必要です。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

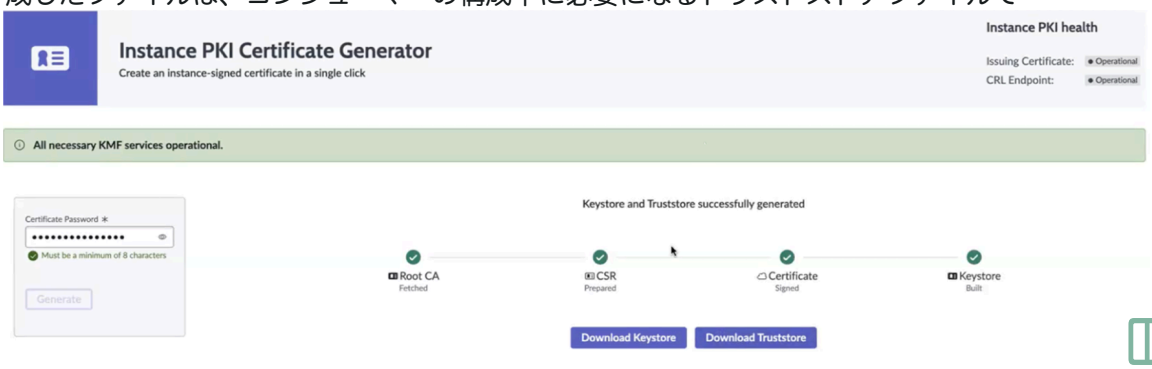
これらは LES ストアアプリを使用して実行するか、独自の独立した Kafka コンシューマーを使用して実行するかに関係なく、Hermes トピックから消費する必要があります。

このプロセスは、「Set up a secure connection to the Hermes Messaging Service」の手順に従って手動で行う必要があります。これらの証明書は、Hermes からログをプルするコンシューマークライアントでの認証と承認に必要になります。

> **注:**
> これらの証明書を正常に生成して取得するまで先に進まないでください。

プロセスが終了するまでに、キーストアとトラストストアの 2 つのファイルがダウンロードされます。両方を専用の LES MID Server に保存します。

> **注:**
> 「Set up a secure connection to the Hermes Messaging Service」の手順を使用して作成したファイルは、コンシューマーの構成中に必要になるトラストストアファイルです。



MID Server での LES V2 のセットアップ

MID Server インスタンスで LES V2 をセットアップし、Hermes からログを生成して消費します。

始める前に
必要なロール：admin

手順

1. MID Server をセットアップします。

   > **注:**
   > MID Server は LES 専用にすることをお勧めします。これは、エクスポートされたログメッセージを REST エンドポイントにタイムリーに配信するために重要です。

   「Download the MID Server files」を参照して MID Server のファイルをダウンロードします。

   新しい MID Server をインストールするには、を使用するか Use MID Server guided setup、手動でインストールします。手動インストールの場合は、最初に「MID Server のネットワーク接続の設定」の指示に従い、その後に「MID Server のインストール」のドキュメントに従ってください。リンクは UI から利用できます。

2. MID Server を ServiceNow インスタンスに接続します。
   詳細については、「MID Server」を参照してください。
3. MID Server を検証して再起動します。
   MID サーバーがインストールされた後は、手動で MID Server を検証して、自動化タスクを実行できるようにする必要があります。MID レコードが正しいことを確認します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

4. 移動先 **MID** サーバー > 拡張 > **LES** コンシューマーコンテキスト 特定の MID Server で実行するように LES コンシューマーレコードを更新しま

す。
次のフィールドを設定して、LES コンシューマーレコードを更新します。インスタンスに接続した MID Server を選択します。

- [実行サーバー] フィールドに特定の MID Server を選択
- 前のステップで [MID Server] フィールドに対して検証した MID Server を選択します

5. [更新] を選択して変更を保存します。
6. 移動先 **MID** サーバー > プロパティ.
既存のプロパティに次の値を追加します。

名前	値
mid.les.kafka.ssl.truststore.password	<パスワード>
mid.les.kafka.ssl.keystore.password	<パスワード>
mid.les.kafka.ssl.key.password	<パスワード>
mid.les.kafka.ssl.truststore.location	<パス>/<トラストストア>.p12
mid.les.kafka.ssl.keystore.location	<パス>/<キーストア>.p12
mid.les.kafka.ssl.truststore.type	PKCS12
mid.les.kafka.ssl.keystore.type	PKCS12
mid.les.kafka.client.id	<インスタンス名>
mid.les.kafka.group.id	snc.<インスタンス名>.group1
mid.les.kafka.bootstrap.servers	<インスタンス名>.<ドメイン>:4100,<インスタンス名>.<ドメイン>:4101,<インスタンス名>.<ドメイン>:4102,<インスタンス名>.<ドメイン>:4103
mid.les.kafka.set2.bootstrap.servers	<インスタンス名>.<ドメイン>:4200,<インスタンス名>.<ドメイン>:4201,<インスタンス名>.<ドメイン>:4202,<インスタンス名>.<ドメイン>:4203

上記の値の一部を取得する方法については、次の注意事項に従ってください。

- <パスワード> はキーストアとトラストストアに設定したパスワードです。
- <パス> は、ダウンロードしたキーストアファイルとトラストストアファイルを保持するディレクトリへのファイルパスです。証明書は MID を実行しているサーバー上にある必要があります。
- <インスタンス名> は ServiceNow インスタンスの名前です不明な場合は、sys_properties テーブルで見つけることができます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- Hermes の診断ページから mid.les.kafka.bootstrap.servers と mid.les.kafka.set2.bootstrap.servers の両方の値を取得できます。移動先 **Hermes** メッセージングサービス > 診断 コンシューマーブートストラップ 1 とコンシューマーブートストラップ 2 の下の文字列をそれぞれコピーします。
- キーストアファイルとトラストストアファイルは、MID を実行しているサーバー上のファイルにセットアップされます。[場所] の値は、MID Server でこれらのキーのパスになります。

Hermes からのログの生成と消費

予定していた LES V2 フローを実装して、ServiceNow または MID Server インスタンスのいずれかを使用して Hermes からログを生成および消費します。

始める前に
必要なロール：admin または sn_logstoanalytics.admin

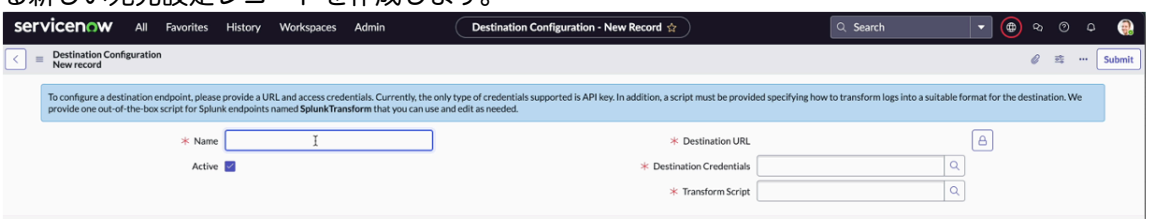
手順

1. 移動先 すべて > ログエクスポートサービス > ソース をクリックして、ログエクスポートの新しいソースを作成します。

> **注:**
> このステップはログの生成中にのみ使用します。

適切なテストソースは、[ソースタイプ] がノードログで、[ログレベル] が INFO です。

2. 移動先 すべて > ログエクスポートサービス > 宛先構成 新しいログ宛先のアクセスの詳細を指定する新しい宛先設定レコードを作成します。



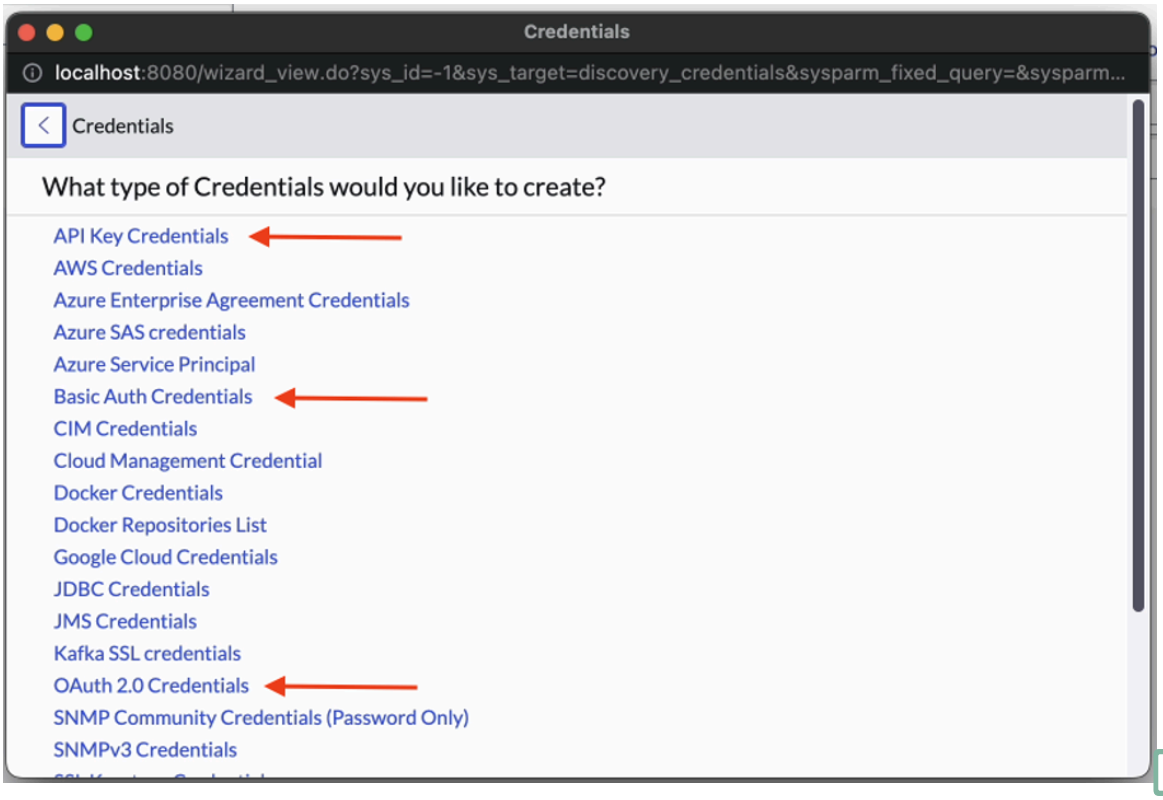
> **注:**
> このステップはログの消費中にのみ使用します。

宛先構成レコードを作成する際は、重要なポイントに従ってください。

自動翻訳

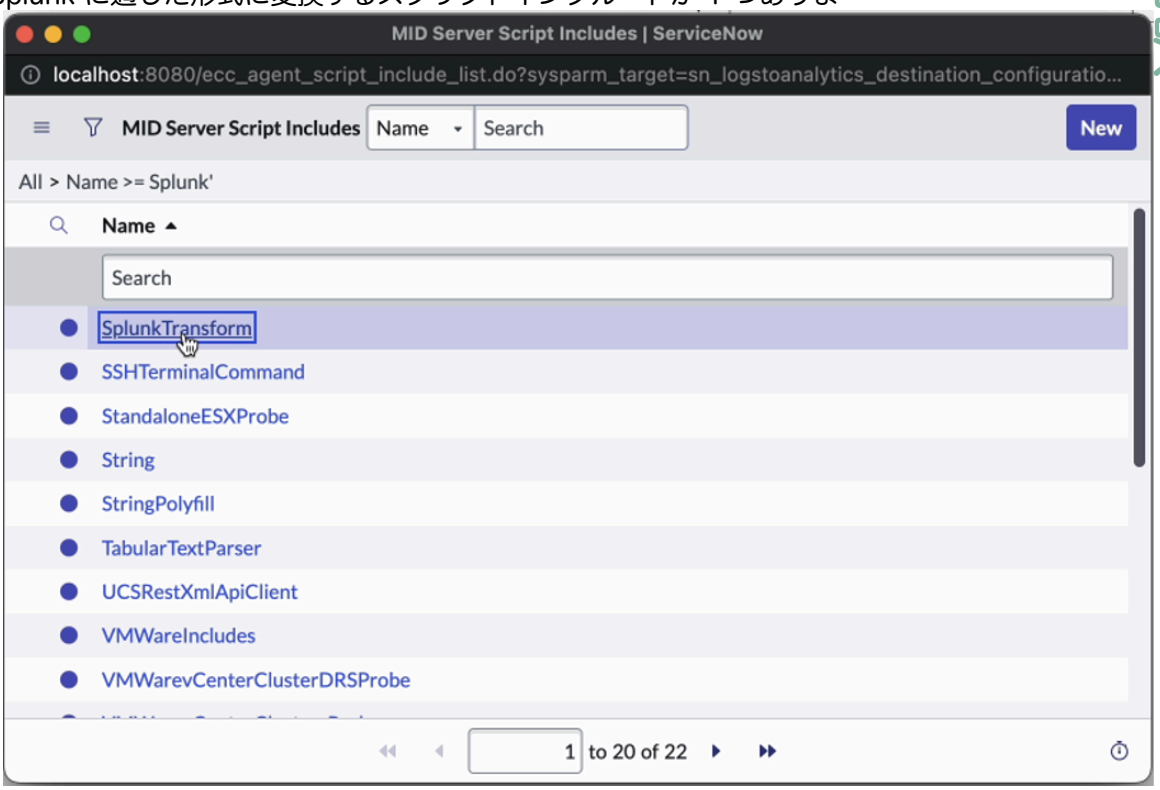
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- エンドポイントの資格情報を作成するときは、LES の V2 で基本認証、oauth、および API キーのみがサポートされていることに注意してくださ



い。

- 宛先構成を作成するときは、ServiceNow 形式のログをエンドポイントに適した形式に変換する MID Server スクリプトインクルードを選択または作成する必要があります。デフォルトでは、LES アプリケーションには、ログを Splunk に適した形式に変換するスクリプトインクルードが 1 つありま

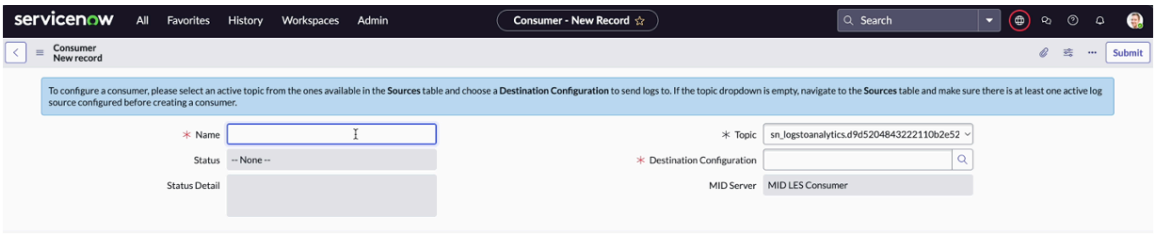


す。

3. 移動先 すべて > ログエクスポートサービス > コンシューマー をクリックして、新しいログコンシューマーを作成します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳



ドロップダウンからソーストピックを選択し、ログの転送先の宛先構成を 1 つ選択します。

> **注:**
> このステップはログの消費中にのみ使用します。

4. コンシューマーテーブルの UI アクションを使用して、コンシューマーを起動します。
5. MID Server のログステートメントを確認し、エンドポイントで ServiceNow ログを探して、ログの消費を検証します。

日次ログエクスポートレポートの確認

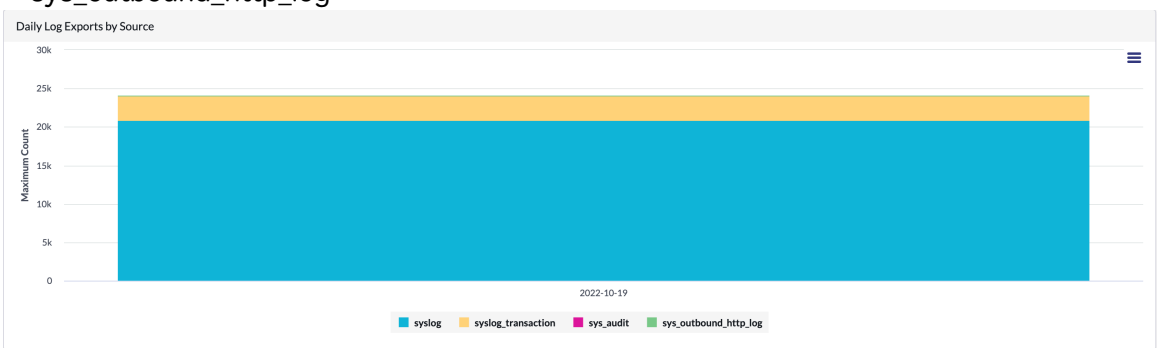
日次ログエクスポート (ソース別) レポートを確認して、各データログソースのサイズを分析します。このレポートには、各ログテーブルによって生成されたログイベントの 1 日あたりの数が示されます。

始める前に

必要なロール：admin または sn_logstoanalytics.admin

手順

1. 移動先 すべて > ログエクスポートサービス > ソース別の日次ログエクスポート.
2. 次のテーブルで 1 日あたりに生成される日次ログ数を確認します。
   - syslog
   - syslog_transaction
   - sys_audit
   - sys_outbound_http_log



データソースのサイズに応じて、そのデータを LES エクスポートレポートに含めるかどうかを決定できます。

> **注:**
> グラフ内の色分けされたバーを選択すると、ログエクスポート日次集計レポートにリダイレクトされ、そこでフィルターを変更してデータをさらに分析できます。ログソースフィルターを設定することで、ログエクスポートサービスによってエクスポートされるログイベントの数を減らすことができます。アプリケーション ノードのログ ファイルは、このレポートには含まれません。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ログ記録、監査、およびエラー (インスタンスセキュリティ強化)

ログ記録と監査戦略を適用して、不審なアクティビティを適切なタイミングで特定して対処できるようにします。

インスタンスのログ記録の詳細については、「システムログ」を参照してください。を使用して、ログインや失敗したログインなどのシステムイベントを監視するスケジュールがあることを確認するシステムログ > イベント.

SQL エラーメッセージの無効化 (インスタンスセキュリティ強化)

glide.db.loguser プロパティを使用して、SQL エラーメッセージがブラウザーでレンダリングされないようにします。

詳細情報

属性	説明
プロパティ名	glide.db.loguser
構成タイプ	システムプロパティ (/sys_properties_list.do)
Instance Security Center で構成可能	いいえ
目的	ブラウザー内での SQL エラーメッセージの表示を無効にすること
タイプ	true | false
推奨値	false
機能への影響度	(低) この修正により、SQL エラーメッセージをレンダリングできなくなります。機能への影響はありません。
セキュリティリスク	(中) 攻撃者に役立つ可能性のある機密の SQL 情報は、Web ページのエラーメッセージに含まれて表示されることはありません。

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

シークレット管理

ServiceNow シークレット管理を使用し、ビジネスニーズに合わせてパスワードへのアクセスを詳細に管理します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

探索

シークレット管理の主な機能と
ビジネス価値について学びます。

分析

シークレット管理ダッ
シュボードを確認します。

構成

コア構成を計画します。

自動翻訳

シークレット管理の詳細

ServiceNow シークレット管理を使用し、ビジネスニーズに合わせてパスワードへのアクセスを詳細に管理します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

重要:
管理者には、シークレット管理に関連するモジュールとレコードを表示するためのロールが必要です。シークレット管理ロールの情報については、「シークレット管理ロール」を参照してください。

シークレット管理の **Core** バージョンと **Enterprise** バージョンからの選択

ビジネスニーズに応じて、[シークレット管理 Core] および [シークレット管理 Enterprise] から選択します。

シークレット管理 **Core**	シークレット管理 **Enterprise**
シークレット管理 Core は、追加コストなしでインスタンスにインストールできます。このプラグインは次の機能を提供します。 • Password2 暗号化モジュールを使用して、パッケージレベルのシークレットグループを作成します。 • シークレットグループ構成ウィザードを使用して、シークレットグループをすばやく構成します。	シークレット管理 Enterprise には、管理者がシークレットグループを作成および管理するのに役立つ追加の機能が含まれています。Enterprise は、Core に一覧表示される機能に加えて次の機能を提供します。 • 詳細なアクセス制御を使用し、次のいずれかの基準に基づいてシークレットグループを作成します。 ○ スコープ ○ テーブル ○ 列 ○ レコード • ServiceNow がアクセスできない独自のキーを使用して暗号化された、クライアントのアクセス可能なシークレットを作成します。 • シークレット管理ダッシュボードを使用して、インスタンスに設定されているシークレットグループを確認し、潜在的なセキュリティの問題について確認します。 **注:** シークレット管理 Enterprise は、ServiceNow 担当者が本番インスタンスで有効にする必要がある有料プラグインです。

シークレットグループを使用したシークレットの整理

シークレット管理を使用してシークレットをグループに整理し、グループレベルでそれらのシークレットにアクセスポリシーを適用します。

基本シークレットグループ

これらのグループは、スコープ内のすべてのシークレットに適用されます。これらのシークレットは、一般的な暗号化モジュールとモジュールアクセスポリシーによって復号化されます。

基準のあるシークレットグループ

基準のあるシークレットグループは、基本シークレットグループと同じように機能しますが、含まれるものが基準によってさらに絞り込まれています。次のような基準があります。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

- アプリケーションスコープ
- パッケージ
- テーブル
- シークレット列
- レコードのフィルタリング

いずれかのタイプのシークレットグループを、インスタンスアクセス可能にするか、クライアントアクセス可能にすることができます。

インスタンス側のシークレットグループ

インスタンス側のシークレットグループには、インスタンスで復号化できるシークレットが含まれています。

クライアント側のシークレットグループ

クライアント側のシークレットグループは、公開鍵と秘密鍵のペアを使用して、クライアントのみがシークレットを復号化できるようにします。クライアントアクセス可能なシークレットグループを作成する場合は、公開鍵をインスタンスにアップロードし、秘密鍵を MID Server に保持します。インスタンスは公開鍵を使用してシークレットを暗号化しますが、秘密鍵を使用してのみ復号化できます。

注:
これらのグループタイプの詳細については、「クライアント側 シークレット管理 について」を参照してください。

シークレットグループを使用したより詳細な制御

password2 は ServiceNow プラットフォームで利用できますが、シークレット管理は次の追加機能を提供します。

詳細なアクセス制御	Password2 password2 を使用すると、管理者はアプリケーションスコープへのアクセスを制御できますが、スコープ内の要素へのアクセスを制限することはできません。 シークレット管理 シークレット管理を使用すると、管理者は定義した基準に基づいてアクセスを制限できます。基準タイプは、パッケージ、テーブル、列などの基準に基づくことができます。
セキュアストレージ	クライアント側シークレットグループの場合、シークレット管理は新しい暗号化スキームを使用します。この暗号化スキームでは、ServiceNow は暗号化キーを保存しません。このため、データのセキュリティは ServiceNow セキュリティに依存しません。

グループへのモジュールアクセスポリシーの適用

シークレットをシークレットグループにグループ化した後で、グループレベルでそれらのシークレットにアクセスする方法を決定するポリシーを適用できます。モジュールアクセスポリシーは、暗号化キーの有効期間などのインスタンスレベルでの制御を定義するために、暗号化モジュールに適用するアクセス制御メカニズムです。モジュールアクセスポリシーの詳細については、「モジュールアクセスポリシーの概要」を参照してください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

シークレット管理とともにインストールされるテーブル

シークレット管理は、次のテーブルを追加または変更します。

新しくなったテーブル	
[sn_sm_secret_group]	シークレットグループを格納します
[sn_sm_secret_group_criteria]	基準シークレットグループを格納します
[sn_sm_secrets]	ラップされたシークレットを格納します
[sn_sm_identity_group]	ID のグループを公開鍵にマッピングするための ID グループを定義します
[sys_kmf_wrapped_module_key]	ラップされた対称暗号化キーを格納します
変更されたテーブル	
[sys_kmf_crypto_module]	追加された暗号化モジュールタイプ(ID 暗号化モジュールまたはシークレットグループ暗号化モジュール)
[sys_kmf_module_key]	• 概念的な秘密暗号化キー (キーマテリアルなし) を格納します • ID 公開鍵を格納します
[sys_kmf_crypto_caller_policy]	新しいモジュールアクセスポリシータイプを追加します

クライアント側 シークレット管理 について

シークレット管理 を使用してシークレットとグループへのアクセスを管理する方法について説明します。

用語

クライアント側シークレット管理は、プロキシを使用せず、さらに復号化されたデータへ ServiceNow のアクセスを付与せずにシークレットを管理する方法を提供するように設計されています。このプロセスを理解するために、まず以下の暗号化の用語を理解してください。

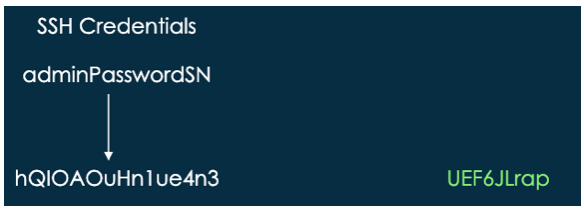
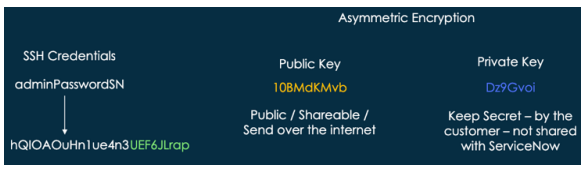
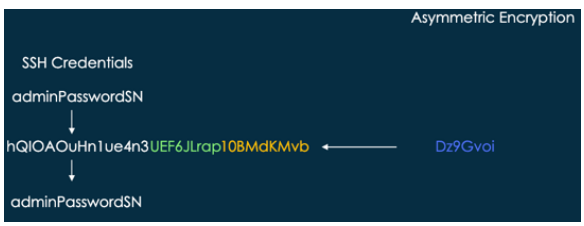
用語	説明
対称暗号化	対称暗号化では、データの暗号化と復号化の両方に 1 つの同じキーを使用します。データが対称キーで暗号化されている場合は、このキーだけで復号化できます。
対称キー	対称キーはシークレットを暗号化し、クリアテキストのパスワードを判読不可能な暗号テキストに変換します。
非対称暗号化	非対称暗号化では、2 つのキーを使用し、1 つは暗号化に、もう 1 つは復号化に使用します。
公開鍵	公開鍵は非対称キーペアの片方のキーです。このキーは、インスタンスに格納され、 キーを使用して対称キーを暗号化します。この暗号化された対称キーは、秘密鍵とペアになっている場合にのみ復号化できます。
秘密鍵	秘密鍵は非対称キーペアの片方のキーです。このキーは、MID Server のキーストアに格納されます。ServiceNow はこのキーにアクセスできません。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

用語	説明
	公開鍵と組み合わせて、非対称キーペアがシークレットを復号化するために使用されます。

クライアント側の暗号化プロセス

対称キーは、資格情報 (この場合は管理者パスワード) を暗号化し、読み取り可能なクリアテキストから暗号化された暗号テキストへと変換します。	
対称キー (緑色で表示) を資格情報に適用して、資格情報を暗号化または復号化できます。	
この時点で、非対称暗号化で公開鍵 (黄色) と秘密鍵 (青色) の使用が開始されます。	
公開鍵は、対称キーとともに資格情報を暗号化します。対称キーは現在保護されているため、資格情報の復号化に使用できません。公開鍵はこの暗号化を実行できますが、単独で復号化に使用することはできません。	
公開鍵で暗号化した後は、資格情報を復号化するために秘密鍵が必要です。顧客のみがこのキーを持っているため、暗号化された資格情報にアクセスできるのは顧客だけです。	

クライアントのアクセス可能なシークレットの構成

クライアントのアクセス可能なシークレットを使用するようにインスタンスを構成する方法について説明します。

この実装例を使用して、プロキシを使用せずにシークレット管理を構成したり、復号化されたデータへの ServiceNow アクセス権を付与したりします。

クライアント側のシークレット管理を使用してパスワードとグループへのアクセスを管理する方法の詳細については、「クライアント側 シークレット管理 について」を参照してください。

これらの手順では、ローカルネットワークに MID Server が構成されていることを前提としています。プロセスの詳細については、「MID Server」を参照してください。

プロセスの概要

1. 暗号化キーと証明書の作成

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

ローカル環境でターミナルコマンドを使用して暗号化キーと証明書を作成します。

2. ServiceNow の信頼できるキーストアに証明書を追加する

   キーと証明書を ServiceNow の信頼できるキーストアにアップロードします。

3. 基準のあるシークレットグループの作成

   シークレットのグループを作成します。シークレットグループを使用してシークレットをグループに整理します。これらのグループを使用して、グループレベルでこれらのシークレットにアクセスポリシーを適用できます。次に、シークレットグループを ID グループに関連付け、MID Server をその ID グループに追加します。

4. 資格情報の作成と資格情報の暗号化のテスト

   サードパーティシステムに対して認証するための資格情報を作成し、ServiceNow でその資格情報にアクセスできないことをテストします。

5. 公開鍵/秘密鍵ペアの MID Server へのアップロード

   公開鍵/秘密鍵ペアを MID Server にアップロードします。このキーペアにより、MID Server はインスタンスからの認証要求を処理できます。

6. 統合を管理するための Flow Designer の構成

   インスタンスで フローデザイナー を使用して、ローカルネットワークとインスタンス間の統合を管理します。

7. エンドツーエンドのクライアント側で暗号化されたシークレットの統合をテストする

   統合をテストし、実行の詳細を確認して、構成が機能していることを確認します。

暗号化キーと証明書の作成

ローカル環境でターミナルコマンドを使用して暗号化キーと証明書を作成します。

始める前に

必要なロール：なし

手順

1. ローカル環境で、ターミナル (Mac または Linux の場合) またはコマンドライン (Windows の場合) を開きます。
2. ターミナルを使用し、`cd` を使用して暗号化キーを保存するフォルダーに移動します。
3. ターミナルを使用して、次のように入力します。

```
openssl req -newkey rsa:4096 -nodes -keyout sm_private_key.pem -x509 -days 365 -out
 sm_public_cert.pem
```

> **注:**
> この例では、OpenSSL を使用してキーと証明書を生成します。要件に基づいて、他の同等のツールに置き換えることもできます。

このコマンドは、秘密鍵と公開証明書 (一致する公開鍵を含む) を生成します。「Country Name」で始まる、必要な情報の一連のプロンプトが表示されます。

4. 要求された情報をプロンプトに入力します。
   次のプロンプトが表示されます。
   - 国名
   - 都道府県名
   - 市区町村名 (市区町村など)
   - 組織名 (会社など)

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

- 組織単位名 (部門など)
- 共通名 (完全修飾ホスト名など)
- メールアドレス

セキュリティチームと協力して、正しい証明書情報が入力されていることを確認します。

```
Country Name (2 letter code) []:US
State or Province Name (full name) []:CO
Locality Name (eg, city) []:Boulder
Organization Name (eg, company) []:ServiceNow
Organizational Unit Name (eg, section) []:Product Management
Common Name (eg, fully qualified host name) []:fake@servicenow.com
Email Address []:fake@servicenow.com
```

5. ステップ 2 で選択したフォルダーをチェックして、秘密鍵と公開証明書が作成されたことを確認します。
   ステップ 3 の例と同じファイル名を使用した場合は、次のファイルが表示されます。
   - sm_private_key.pem
   - sm_public_cert.pem
6. 同じフォルダーで、次のコマンドを使用します。

   ```
   cat sm_private_key.pem sm_public_cert.pem > sm_keypair_bundle.pem
   ```

   このコマンドにより秘密鍵と公開証明書が単一のファイルにバンドルされ、後の手順で MID Server にロードされます。
7. フォルダをもう一度確認して、秘密鍵 (sm_keypair_bundle.pem) と公開証明書を含む新しいファイルが作成されたことを確認します。

ServiceNow の信頼できるキーストアに証明書を追加する

キーと証明書を ServiceNow の信頼できるキーストアにアップロードします。

始める前に
必要なロール：なし

この例で作成した公開証明書は、「自己署名」証明書と見なされます (つまり、信頼できるルート機関からのものではありません)。証明書を使用するには、証明書を ServiceNow の信頼できるキーストアに追加する必要があります。認証局からの証明書を使用する場合は、この手順を完了する必要はありません。

手順

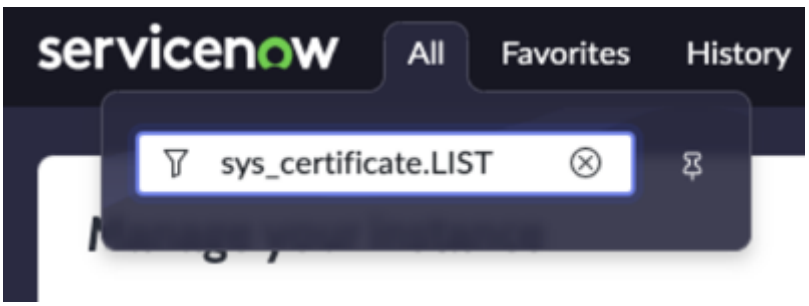
1. ローカル環境で、ターミナル (Mac または Linux の場合) またはコマンドライン (Windows の場合) を開きます。
2. ターミナルを使用し、`cd` を使用して暗号化キーを作成したフォルダーに移動します。
3. ターミナルで、次のコマンドを入力します。

   ```
   cat sm_public_cert.pem
   ```

   公開証明書の内容を表示して、信頼できるキーストアにコピーする必要があります。この `cat` コマンドは証明書を表示します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

4. 証明書情報をクリップボードにコピーします。
   -----BEGIN CERTIFICATE----- 行で始まり -----END CERTIFICATE----- 行で終わるようにします。
5. ServiceNow インスタンスで、ナビゲーションフィルターに「sys_certificate.LIST」と入力し、**[X.509** 証明書] リストに移動します。



6. [新規] を選択して、**[X.509** 証明書] レコードを作成します。
7. フォームで、次のフィールドに入力します。

X.509 証明書のフィールド

フィールド	値
名前	証明書の名前。この名前は任意の名前にすることができます。
フォーマット	**PEM** を選択します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	値
	注: Privacy Enhanced Mail (PEM) ファイルは、キーと証明書に使用される公開鍵インフラストラクチャ (PKI) ファイルの一種です。前のステップで作成したレコードはこのファイルタイプです。
タイプ	[信頼できるストア証明書 **(Trusted Store Cert)**] を選択します。
簡単な説明	証明書の説明。この証明書の使用目的を示す値を入力します。
PEM 証明書	ステップ 4 でコピーした証明書情報を貼り付けます。

8. [送信] をクリックしてレコードを保存します。

基準のあるシークレットグループの作成

シークレットのグループを作成します。シークレットグループでシークレットをグループに整理し、グループレベルでそれらのシークレットにアクセスポリシーを適用できるようにします。次に、シークレットグループを ID グループに関連付け、MID Server をその ID グループに追加します。

始める前に
必要なロール：管理者

手順

1. 移動先 すべて > シークレット管理 > 基準のあるシークレットグループ.
2. [新規] を選択して、[基準のあるシークレットグループ] を作成します。
3. フォームで、次のフィールドに入力します。

基準のあるシークレットグループフィールド

フィールド	値
グループ名	シークレットグループの名前。この名前は任意の名前にすることができます。
シークレットタイプ	[クライアントアクセス可能] を選択します。
自動生成モジュール	ボックスをオンにします。
簡単な説明	シークレットグループの説明。このグループの使用目的を示す値を入力します。
基準タイプ	[ターゲットテーブル] を選択します。
ターゲットテーブル	**SSH** 資格情報 **[ssh_credentials]** を選択します。

4. フォームヘッダーを右クリックし、コンテキストメニューから [保存] を選択してレコードを保存します。
5. [アクティブ] チェックボックスがオフになっていることを確認します。

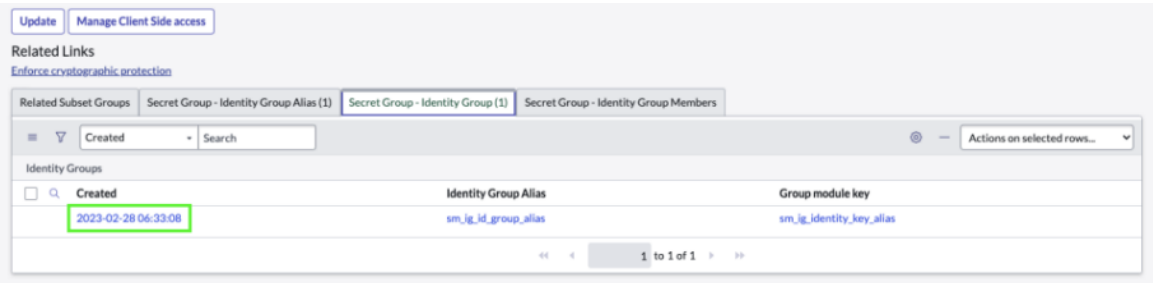
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

6. [クライアント側のアクセスを管理] ボタンを選択して、ID グループを作成します。
   [ID グループエイリアス] ウィンドウが表示されます。
7. [新規] ボタンを選択します。
8. **[ID** グループエイリアス] フィールドの横にある参照アイコン ( ) を選択します。
9. [グループエイリアス名] フィールドに値を入力します。
   この名前は任意の値にすることができます。
10. [送信] を選択します。
11. **[ID** キーをアップロード **(Upload identity key)]** ボタンを選択します。
    [ID 公開鍵証明書をインポート] ウィンドウが表示されます。
12. **[ID** キーエイリアス] フィールドに値を入力します。

> **重要:**
> この値は任意の値にすることができますが、後のステップで MID Server に挿入する値と完全に一致する必要があります。

13. [インポート] を選択します。
    [添付ファイル] ウィンドウが表示されます。
14. [ファイルを選択] を選択します。
15. 前のステップで作成した公開証明書を選択します。
    この証明書は sm_public_cert.pem ファイルである必要があります。
16. [X] アイコンを選択してウィンドウを閉じます。
17. **[OK]** を選択して **[ID** 公開鍵証明書をインポート] ウィンドウを閉じます。
    インポートの成功を確認する青色の [キーと証明書がインスタンスに正常にインポートされました] バナーが表示されます。
18. [送信] を選択します。
    [ID グループ **(Identity groups)]** リストが表示されます。
19. リストの ID グループレコードの左側にあるチェックボックスをオンにします。
20. [シークレットグループの関連付け **(Associate secret group)]** ボタンを選択します。
    [基準のあるシークレットグループ] レコードに戻ります。[シークレットグループ **- ID** グループエイリアス **(Secret Group – Identity Group Alias)]** および [シークレットグループ **- ID** グループ **(Secret Group – Identity Group)]** 関連リストが表示されます。これらの関連リストには、前のステップで作成したレコードが表示されます。
21. [シークレットグループ **- ID** グループ **(Secret Group – Identity Group)]** 関連リストで、そのリストのレコードの [作成日時 **(Created)]** フィールドを選択します。



[ID グループ **(Identity groups)]** レコードが表示されます。

22. **[ID** グループメンバー **(Identity group members)]** 関連リストで、[新規] ボタンを選択します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

[ID グループメンバー **(Identity group members)]** レコードが表示されます。

23. [メンバーテーブル] フィールドで、**[MID Server [ecc_agent]]** を選択します。
24. **[ID** グループメンバー **(Identity group members)]** レコードフィールドの横にある参照アイコン ( ) を選択し、MID Server を選択します。

    注:
    [すべてのレコードを含める **(Include all records)]** チェックボックスをオンにすると、インスタンスに接続されているすべての MID Server が ID グループに追加されます。

25. **[OK]** を選択して、[ドキュメントを選択] ウィンドウを閉じます。
26. [**Submit** (送信)] を選択します。
27. 次に戻ります。 すべて > シークレット管理 > 基準のあるシークレットグループをクリックし、ステップ 2 で作成したレコードを開きます。
28. [アクティブ] フィールドを有効にします。
29. [更新] をクリックしてレコードを保存します。

資格情報の作成と資格情報の暗号化のテスト

サードパーティシステムに対して認証するための資格情報を作成し、ServiceNow でその資格情報にアクセスできないことをテストします。

始める前に
必要なロール：admin

手順

1. ナビゲーションフィルターに「ssh_credentials.list」と入力して、**[SSH** 資格情報] リストに移動します。
2. [新規] を選択して、**[SSH** 資格情報] レコードを作成します。
3. フォームで、次のフィールドに入力します。

SSH 認証情報フォーム

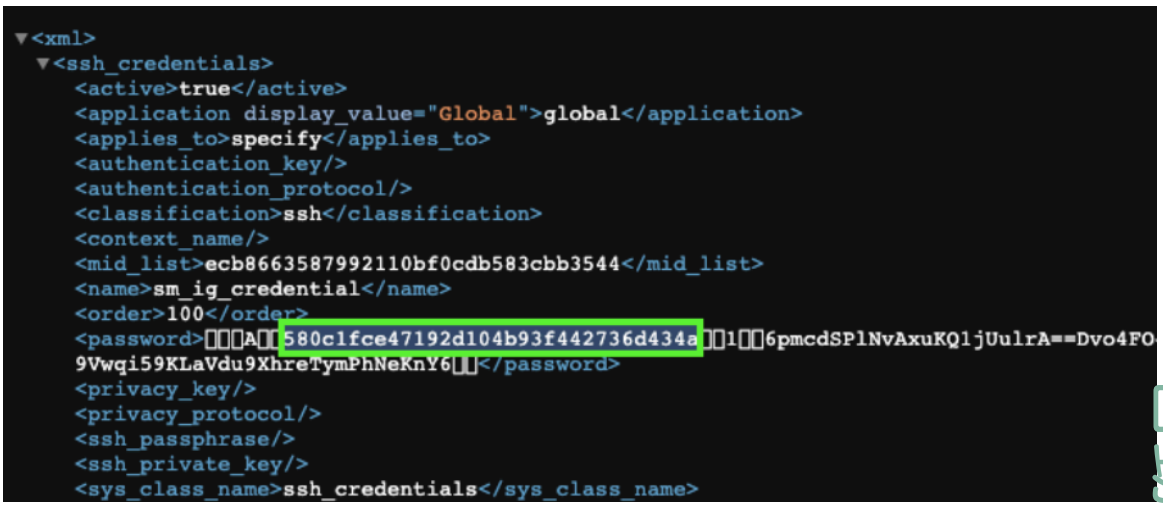
フィールド	値
名前	資格情報レコードの名前を入力します。この名前は任意の値にすることができます。
適用先	[特定の **MID Server]** を選択します。
MID Server	MID Server を選択します。
ユーザー名	ユーザー名を入力します。
パスワード	ユーザーに関連するパスワードを [ユーザー名] フィールドに入力します。

4. [資格情報エイリアス] フィールドの横にあるロックアイコン ( ) を選択します。
5. 参照アイコン ( ) を選択して、[接続 **&** 資格情報エイリアス] リストを開きます。
6. [新規] を選択して、[接続 **&** 資格情報エイリアス] レコードを作成します。
7. [名前] フィールドに名前を入力します。

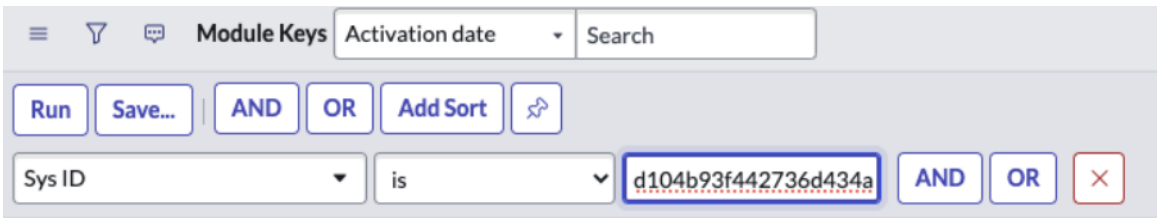
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

8. [タイプ **(Type)**] フィールドで [資格情報 **(Credential)**] を選択します。
9. [送信] を選択します。
   [SSH 資格情報] レコードに戻ります。次のステップでは、資格情報が暗号化されていることをテストします。
10. フォームのヘッダーを右クリックし、**[XML** の表示 **(Show XML)]** を選択します。
11. XML 内で <パスワード> XML タグを見つけます。
12. この <パスワード> タグ内の sys_id をクリップボードにコピーします。
    sys_id は、この資格情報の暗号化に使用されている対称キーを表す 32 文字のコードです。SSH 資格情報テーブルに入力した暗号化パスワードは、この同じ行で 2 つのボックスセットの右側にあります。



13. ナビゲーションフィルターに「sys_kmf_module_key.list」と入力して、[モジュールキー] リストに移動します。
14. **[Sys ID]** フィールドがステップ 12 でコピーした sys_id と一致するレコードのリストをフィルタリングし、[実行] を選択します。



検索すると、単一のモジュールキーレコードが返されます。このレコードは、対称キーを正常に作成して使用していることを示しています。

15. ナビゲーションフィルターに「sys_kmf_wrapped_module_key.list」と入力して、[ラップされたモジュールキー] リストに移動します。
16. [暗号化されたモジュール] フィールドが前のステップで作成した暗号化モジュールと一致するレコードのリストをフィルタリングし、[実行] を選択します。
    検索すると、単一の [ラップされたモジュールキー] レコードが返されます。このリストから、次のことを確認できます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- [ラップされたキーマテリアル] 列には、(SSH 資格情報の暗号化に使用されている) 暗号化モジュール内の対称キーが、ID グループにアップロードした公開鍵によって暗号化されていることが表示されます。
- [ラップされたキーの **Sys id]** フィールドは、[ラッピングキー **sys id]** (ID グループにアップロードされた公開鍵) によって暗号化されているキー (暗号化モジュール対称キー) であることを示しています。

> **注:**
> 上記のフィールドがデフォルトでリストにない場合は、[リストをカスタマイズ] アイコン (⚙) を選択してリストに追加できます。

公開鍵/秘密鍵ペアの **MID Server** へのアップロード

公開鍵/秘密鍵ペアを MID Server にアップロードします。このキーペアにより、MID Server はインスタンスからの認証要求を処理できます。

始める前に
必要なロール：なし

ServiceNow は秘密鍵にアクセスできないため、公開鍵とペアリングして対称キーを復号化してから資格情報を復号化することはできません。MID Server がこの暗号化された資格情報を使用しようとしても、秘密鍵にアクセスせずに認証用の資格情報を復号化することはできません。

これらのステップでは、秘密鍵を MID Server にアップロードして公開/秘密キーチェーンを完了します。このアップロードでは、ServiceNow にアクセス権を付与せずに MID Server にアクセス権を付与します。

MID Server に秘密鍵へのアクセス権を付与するには、PowerShell で管理者として実行するコマンドを構築する必要があります。この例では、コマンドは Azure Windows 仮想マシン用です。

> **重要:**
> これらのステップを実行するシステムで MID Server とキーペアファイルの両方にアクセスできることを確認してください。

手順

1. ローカル環境で、暗号化キーと証明書の作成 のステップでキーペアを作成したフォルダーを見つけます。
2. 完全パスを見つけて `manage-certificates.bat` ファイルにコピーします。

   > **注:**
   > このファイルは MID Server フォルダーにあります。MID Server フォルダーを保存した場所に応じて、パスは次の例のようになります。

   ```
   C:
   \Users\<your_user_account>\Documents\SM_Implementation\mid.utah-07-08-2022__patch4b01-31-2023_02-07-2023_1702.windows.x86-64\sm_ig_MIDS\bin\scripts\manage-certificates.bat
   ```

3. テキストファイルを作成し、パスをファイルに貼り付けます。
4. テキストファイルで、パスの後に次を追加します。
   `-a your_identity_key_alias`

   `your_identity_key_alias` を、公開証明書のアップロード時に作成した ID キーエイリアスの名前に置き換えます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

5. キーペアファイルの完全パスを見つけてコピーします。

   注:
   これらのステップの名前を使用した場合、そのファイルの名前は sm_keypair_bundle.pem になります。

6. テキストファイルで、このパスを行の最後に追加し、このパスと前の情報の間にスペースを追加します。
   テキストファイル内のテキストは、次の例のようになります。

```
C:
\Users\<your_user_account>\Documents\SM_Implementation\mid.utah-07-08-2022__patch4b01-31-2023_02-07-2023_1702.windows.x86-64\sm_ig_MIDS\bin\scripts\manage-certificates.bat -a your_identity_key_alias
 C:\Users\<your_user_account>\Desktop\sm_keypair_bundle.pem
```

   注:
   この例では、パスを短くするために sm_keypair_bundle.pem ファイルがデスクトップにあります。

7. テキストファイルのテキスト全体をクリップボードにコピーします。
8. システムで Powershell を見つけ、[管理者として実行 **(Run as Administrator)]** オプションを選択します。
9. テキストファイルのテキストを Powershell に貼り付け、Enter キーを押します。
   成功すると、次のメッセージが表示されます。

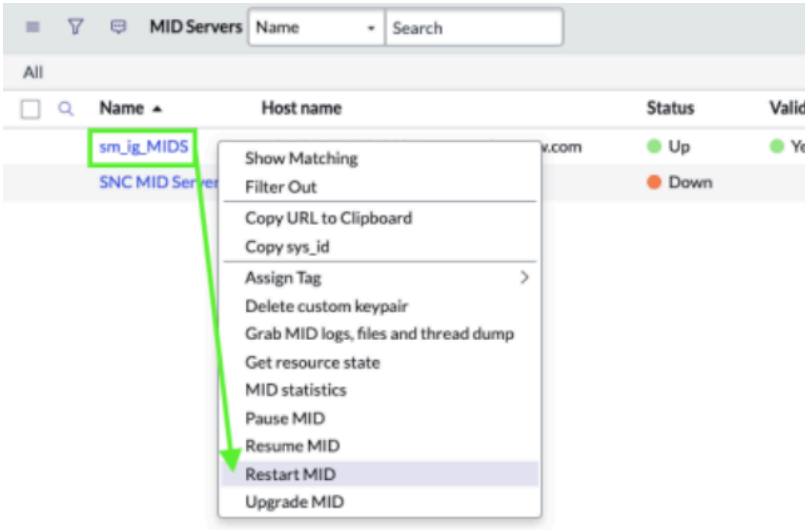
```
Installed certificate with alias: <your_identity_key_alias> into the MID keystore.
```

   ヒント:
   このメッセージが表示されない場合は、コマンドにエラー、スペース、または不要な引用符が含まれていないことを確認してください。完全パスが正しく入力されていることを確認します。

10. MID Server レコードに移動し、レコードを右クリックして **[MID** を再起動] を選択して、MID Server を再起動します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



MID Server を再起動すると、アップロードされたキーペアが MID キーストアに同期され、操作で使用できるようになります。続行する前に、MID Server が再起動し、ステータスが [稼働中 **(Up)]** で検証済みの値が [はい] になるまで待機します。

統合を管理するための **Flow Designer** の構成

インスタンスで フローデザイナー を使用して、ローカルネットワークとインスタンス間の統合を管理します。

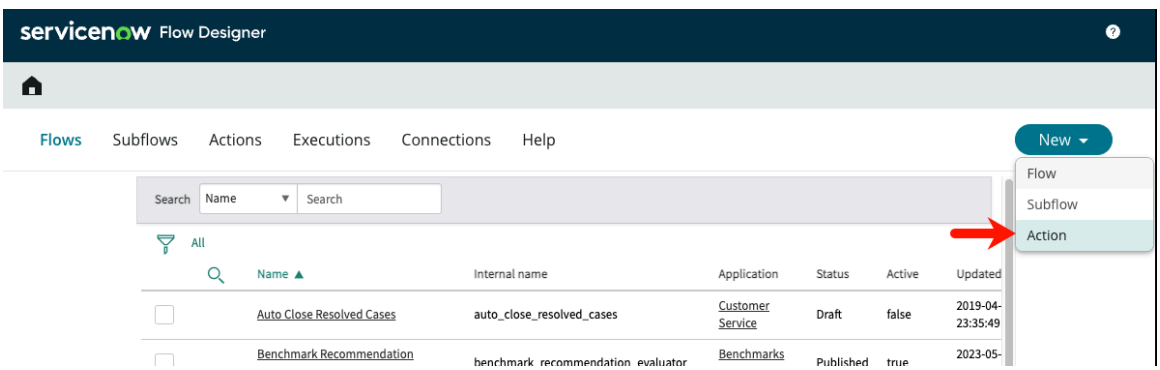
始める前に

必要なロール：admin

これらの手順では、フローデザイナー ワークフローを作成して、ローカルシステムにテキストファイルを作成します。

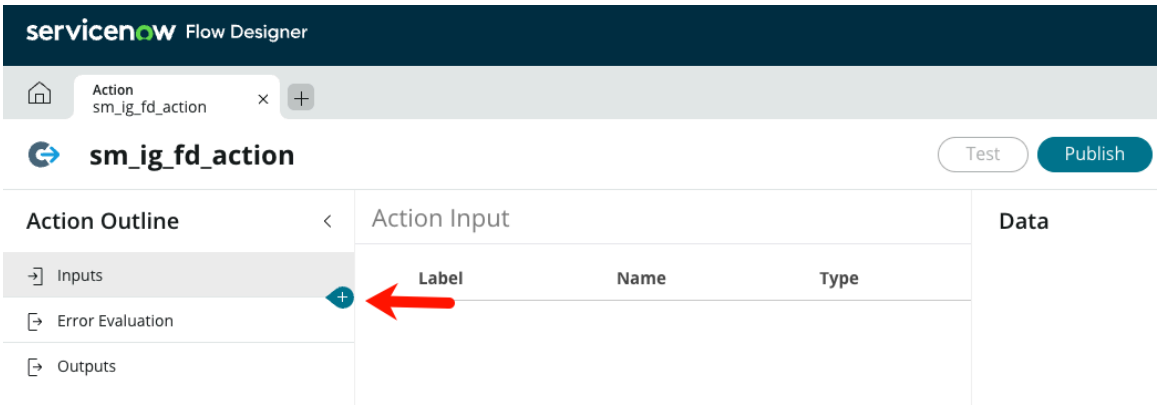
手順

1. インスタンスで、次の場所に移動します。 すべて > プロセス自動化 > フローデザイナー.
2. [新規] を選択し、[アクション] を選択して ServiceNow にアクションを作成します。

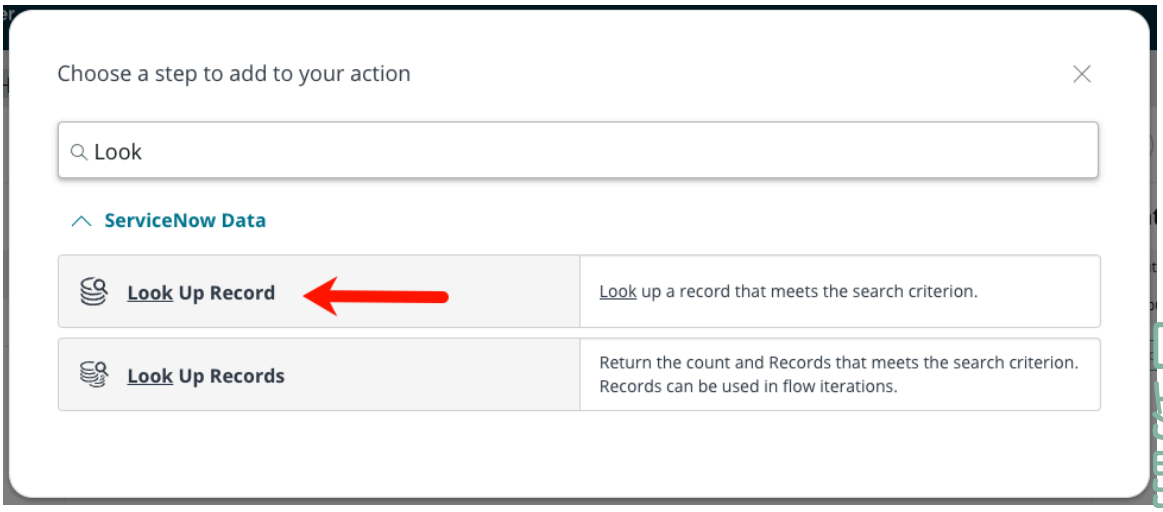


3. [アクション名] フィールドに名前を入力し、[送信] を選択します。
4. [アクションアウトライン] で [入力] と [エラーの評価] の間のプラス記号を選択して、ステップを作成します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



5. [アクションに追加するステップを選択] ウィンドウで、[レコードの検索] を選択します。



6. [レコードの検索 **(Look Up Record)]** ステップセクションで、[テーブル] フィールドで **[MID Server [ecc_agent]]** を選択します。
7. [レコードの検索 **(Look Up Record)]** ステップの下にあるプラス記号を選択して、別のステップを作成します。
8. [アクションに追加するステップを選択] ウィンドウで、**[SSH]** を選択します。

   注:
   [SSH] オプションが表示されない場合は、必要なプラグインを有効にする必要があります。

9. **[SSH** ステップ **(SSH Step)]** セクションで、次の情報を入力します。

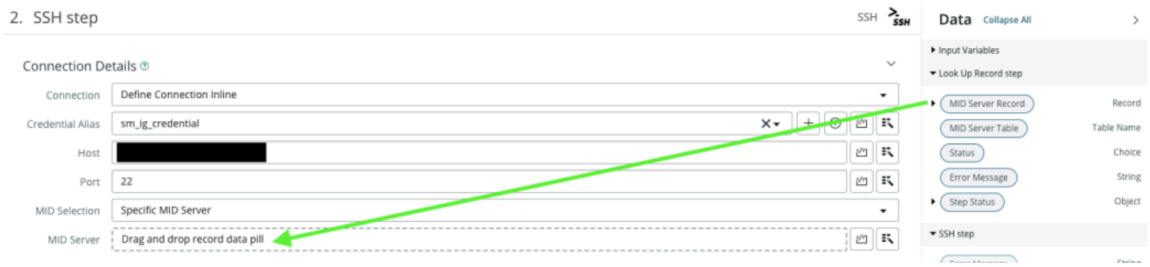
フィールド	値
接続	[インラインで接続を定義] を選択します。
認証情報エイリアス	前のステップで作成した SSH 資格情報の資格情報エイリアスを選択します。
ホスト	SSH 経由で接続するホストの IP アドレスを入力します。
ポート	「22」と入力します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	値
MID 選択	[特定の **MID Server**] を選択します。

10. **[MID Server]** フィールドに入力するには、右側の [データ] セクションから **[MID Server** レコード **(MID Server Record)]** ピルをフィールドにドラッグします。



> **警告:**
> ピルをフィールドにドラッグするときは、ピルの左側にある黒い矢印ではなくピルを選択します。

11. **[SSH** 構成 **(SSH Configuration)]** セクションで、[コマンド] フィールドに次の値を入力します。

```
/bin/date > sm_ig_text_file.txt
```

このコマンドは、MID Server から復号化されたシークレットを使用して、ローカルシステムにテキストファイルを作成します。MID Server は、復号化されたシークレットへのアクセス権を ServiceNow インスタンスに付与せずに、ServiceNow インスタンスへのアクセス権を (フローデザイナー を介して) 付与します。

> **ヒント:**
> `/bin/date` コマンドは、作成されたテキストファイルに現在の日付/時刻を挿入します。このコマンドは、テキストファイルが作成された日時と現在の日時に基づいて、統合がリアルタイムで行われていることを示します。

12. 画面の右上隅にある [保存] ボタンを選択して、ワークフローを保存します。

エンドツーエンドのクライアント側で暗号化されたシークレットの統合をテストする

統合をテストし、実行の詳細を確認して、構成が機能していることを確認します。

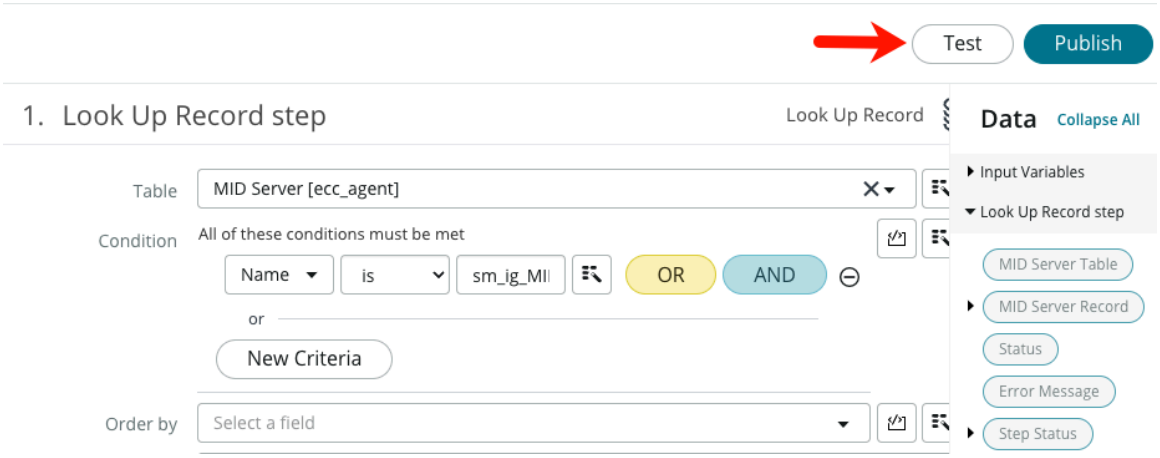
始める前に
必要なロール：admin

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. フローデザイナー で、画面の右上隅にある [テスト] ボタンを選択します。



2. [テストアクション] ウィンドウで、[テストを実行] を選択します。
3. [テストの実行が終了しました。アクションの実行の詳細を表示します **(Your test has finishe drunning. View the action execution details)]** を選択します。
4. 画面の右上に [テスト実行 – 完了] が表示されるまで、画面を更新します。
5. 画面の左下にある [ステップ] 矢印を選択します。
6. [ステップ出力データ] の見出しに次の成功メッセージが表示されるまで下にスクロールします。

```
{"Step Status";{"code";0,"message";"Success"}}
```

7. フローデザイナー でこのメッセージが表示されたら、テキストファイルがローカルシステムに作成されていることを確認します。

シークレット管理ダッシュボード

シークレット管理ダッシュボードを使用して、インスタンスに設定されているシークレットグループを確認し、セキュリティの問題について確認します。

シークレットグループの概要

[シークレットグループの概要] タブには、設定済みのシークレットグループに関する情報が表示されます。このタブを使用して、インスタンスに設定されたシークレットグループに関する情報を表示します。

タイプ別のシークレットグループ

インスタンスにインストールされているシークレットグループをシークレットタイプ (クライアント側のインスタンス側) 別に示す円グラフを表示します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

基準タイプ別のシークレットグループ

インスタンスに設定されている基準を持つシークレットグループを、使用されている基準のタイプ別に示す円グラフを表示します。

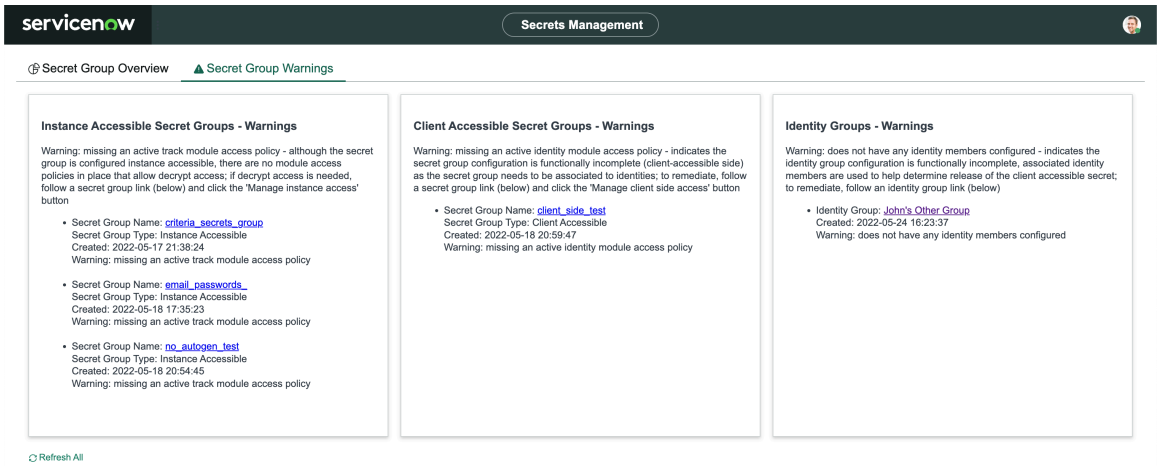
非アクティブなシークレットグループの数

インスタンスに設定されている非アクティブなシークレットグループの数を表示します。

専用シークレットの数

基本シークレットグループ内のシークレットの数を表示します。

シークレットグループの警告



[シークレットグループの警告] タブには、シークレットグループと ID グループに関連する警告が表示されます。

インスタンスアクセス可能なシークレットグループ：警告

アクティブなアクセスポリシーが設定されていないシークレットグループがある場合、このカードは警告を表示します。シークレットグループ名を選択すると、そのレコードが表示されます。

クライアントアクセス可能なシークレットグループ - 警告

アクティブな ID モジュールアクセスポリシー (MAP) を持たないクライアントのアクセス可能なシークレットグループがある場合、このカードは警告を表示します。シークレットグループ名を選択すると、そのレコードが表示されます。

ID グループ：警告

グループメンバーが構成されていない ID グループがある場合、このカードは警告を表示します。ID グループ名を選択すると、レコードが表示されます。

注:
シークレット管理ダッシュボードは、シークレット管理 Enterprise の一部です。シークレット管理 Enterprise は、ServiceNow 担当者が本番インスタンスで有効にする必要がある有料プラグインです。

シークレット管理ロール

シークレット管理は次のロールを追加します。

シークレット管理者 **[sn_secrets.admin]**

管理者以外のシークレットロールを他のユーザーに割り当てます。シークレット管理者には、シークレットマネージャーおよびビューアーと同じ権限があります。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ロールを含む

ロール内に含まれるロールのリスト。

なし。

グループ

このロールがデフォルトでアサインされているグループのリスト。

なし。

特別な考慮事項

重要:
より分化したロールが利用可能な場合は、管理者ロールを付与しないでください。

- ユーザーが sn_secret.admin ロールをアサインされるには、admin ロールと security_admin ロールの両方を持っている必要があります。
- より多くのターゲットロールが利用可能な場合は、admin ロールを付与しないでください。

シークレットマネージャー **[sn_secrets.manager]**

次のいずれかの機能を実行できる必要があるユーザーにこのロールを付与します。

- シークレットおよびシークレットグループレコードを表示する
- アクセス履歴やその他の使用アクティビティ情報を表示する
- シークレットグループとフィルターを作成する
- シークレットプロバイダーを作成する
- シークレットグループ間でのシークレットを移動する
- シークレットグループとシークレットプロバイダーの設定を変更する

ロールを含む

ロール内に含まれるロールのリスト。

なし。

グループ

このロールがデフォルトでアサインされているグループのリスト。

なし。

特別な考慮事項

重要:
シークレットマネージャーは、シークレットをプレーンテキストで表示することはできません。

シークレットビューアー **[sn_secrets.viewer]**

シークレットおよびシークレットグループレコードを表示できる必要があるユーザーにこのロールを付与します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ロールを含む

ロール内に含まれるロールのリスト。

なし。

グループ

このロールがデフォルトでアサインされているグループのリスト。

なし。

特別な考慮事項

なし。

シークレットグループ暗号化モジュールの作成

暗号化と復号化を実行するためのシークレットグループ暗号化モジュールを作成します。

始める前に
必要なロール：

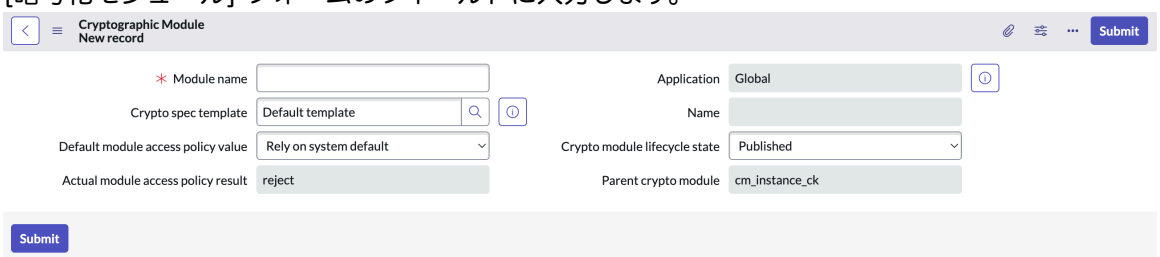
- admin
- sn_secrets.admin
- sn_secrets.secret_manager
- sn_kmf.cryptographic_manager
- sn_kmf.admin

手順

1. 移動先 すべて > シークレット管理 > シークレットグループ暗号化モジュールを作成.
2. 作成するグループ暗号化モジュールのタイプを選択します。

暗号化モジュールタイプ	説明
インスタンスのアクセス可能なシークレット暗号化モジュールを作成	インスタンスで復号化できるインスタンスのアクセス可能なシークレットを作成します。
クライアントのアクセス可能なシークレット暗号化モジュールを作成	ServiceNow がアクセスできない独自のキーを使用して暗号化された、クライアントのアクセス可能なシークレットを作成します。

3. [暗号化モジュール] フォームのフィールドに入力します。



自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
モジュール名	モジュールのわかりやすい名前
アプリケーション	使用中のモジュールを含むアプリケーションスコープこのフィールドには現在のモジュールが自動的に入力されます。
暗号化仕様テンプレート	デフォルトでは、[デフォルトテンプレート] が選択されます。
名前	モジュールの名前。この名前はアプリケーションとモジュール名に基づいて自動的に生成されます。
デフォルトのモジュールアクセスポリシー値	○ システムのデフォルトに依存 ○ 却下 ○ 追跡
暗号化モジュールライフサイクルステータス	モジュールのステータスが [ドラフト] であるか [公開済み] であるか。
実際のモジュールアクセスポリシーの結果	このフィールドは情報提供を目的としており、読み取り専用です。
親暗号化モジュール	前の手順で選択した暗号化モジュールタイプによって決まる親暗号化モジュール。このフィールドは読み取り専用です。

4. [送信] を選択します。

基本シークレットグループの作成

基準に関係なく、任意のシークレットをグループ化する基本シークレットグループを作成します。

始める前に

必要なロール：admin

基本シークレットグループには、テーブル、スコープ、またはアプリケーションに関係なく、追加したシークレットを含めることができます。グループを作成した後、グループにシークレットを手動で追加します。それらの共通の属性を共有するすべてのシークレット専用のグループを作成するには、基準を持つシークレットグループを「基準のあるシークレットグループの作成」の手順を使用して作成します。

手順

1. 移動先 すべて > シークレット管理 > シークレットグループ.
2. [新規] を選択します。
3. [どのタイプのシークレットグループを作成しますか？] で [基本シークレットグループ] を選択します。
4. [シークレットグループ] フォームのフィールドに記入します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

シークレットグループのフィールド

フィールド	説明
グループ名	グループの名前 **注:** シークレットグループ名に使用できるのは、小文字、数字、アンダースコア (_) のみです。
シークレットタイプ	グループが [インスタンスアクセス可能 **(Instance accessible)]** または [クライアントアクセス可能 **(Client accessible)]** かどうか。
自動生成モジュール	このシークレットグループの新しい暗号化モジュールを生成します。このモジュールは、データを暗号化および復号化します。このフィールドはデフォルトで有効になっています。
アプリケーション	このレコードのスコープ対象のアプリケーション。この読み取り専用のフィールドには現在のスコープが自動的に入力されます。
簡単な説明	グループの説明
暗号化モジュール	このグループで使用する暗号化モジュールを選択します。このモジュールは、データを暗号化および復号化します。このフィールドが表示されるのは、[自動生成モジュール] が選択されていない場合のみです。モジュールアクセスポリシーの詳細については、「モジュールアクセスポリシーの概要」を参照してください。 **注:** [インスタンスのアクセスを管理] ボタンを使用して、シークレットグループに関連付けるモジュールアクセスポリシーを確認できます。

5. [送信] をクリックします。

注:
作成したときには、シークレットグループはデフォルトで非アクティブになります。グループをアクティブにするには、グループレコードに戻り、[アクティブ] を選択します。

基準のあるシークレットグループの作成

テーブル、スコープ、アプリケーションなど、共通の基準を共有するときに Password2 フィールドに入力されたシークレットを自動的に整理するための基準を使用して、シークレットグループを作成します。

始める前に
必要なロール：admin

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

このタイプのシークレットグループ内のシークレットは、すべて共通の基準を共有している必要があります。この制限のないグループの場合は、基本シークレットグループを作成することを検討してください。基本シークレットグループの作成については、「基本シークレットグループの作成」を参照してください。

手順

1. 移動先 すべて > シークレット管理 > シークレットグループ.
2. [新規] を選択します。
3. [どのタイプのシークレットグループを作成しますか？] で [基準のあるシークレットグループ] を選択します。
4. [シークレットグループ] フォームのフィールドに記入します。

シークレットグループのフィールド

フィールド	説明
グループ名	グループの名前 **注:** シークレットグループ名に使用できるのは、小文字、数字、アンダースコア (_) のみです。
シークレットタイプ	グループが [インスタンスアクセス可能 **(Instance accessible)]** または [クライアントアクセス可能 **(Client accessible)]** かどうか。
自動生成モジュール	このシークレットグループの新しい暗号化モジュールを生成します。このモジュールは、データを暗号化および復号化します。このフィールドはデフォルトで有効になっています。
アプリケーション	このレコードのスコープ対象のアプリケーション。この読み取り専用のフィールドには現在のスコープが自動的に入力されます。
簡単な説明	グループの説明
基準タイプ	このグループのシークレットが共有する基準 ○ スコープ ○ パッケージ ○ ターゲットテーブル ○ シークレット列 ○ レコードのフィルタリング
暗号化モジュール	このグループで使用する暗号化モジュールを選択します。このモジュールは、データを暗号化および復号化します。このフィールドが表示されるのは、[自動生成モジュール] が選択されていない場合のみです。モジュールアクセスポリシーの詳細については、「モジュールアクセスポリシーの概要」を参照してください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	注: [インスタンスのアクセスを管理] ボタンを使用して、シークレットグループに関連付けるモジュールアクセスポリシーを確認できます。

5. フォームヘッダーを右クリックし、[保存] を選択します。

   注:
   作成したときには、シークレットグループはデフォルトで非アクティブになります。

6. レコードを保存した後に、グループの設定に基づいて追加のフィールドが表示される場合があります。

   追加のシークレットグループフィールド

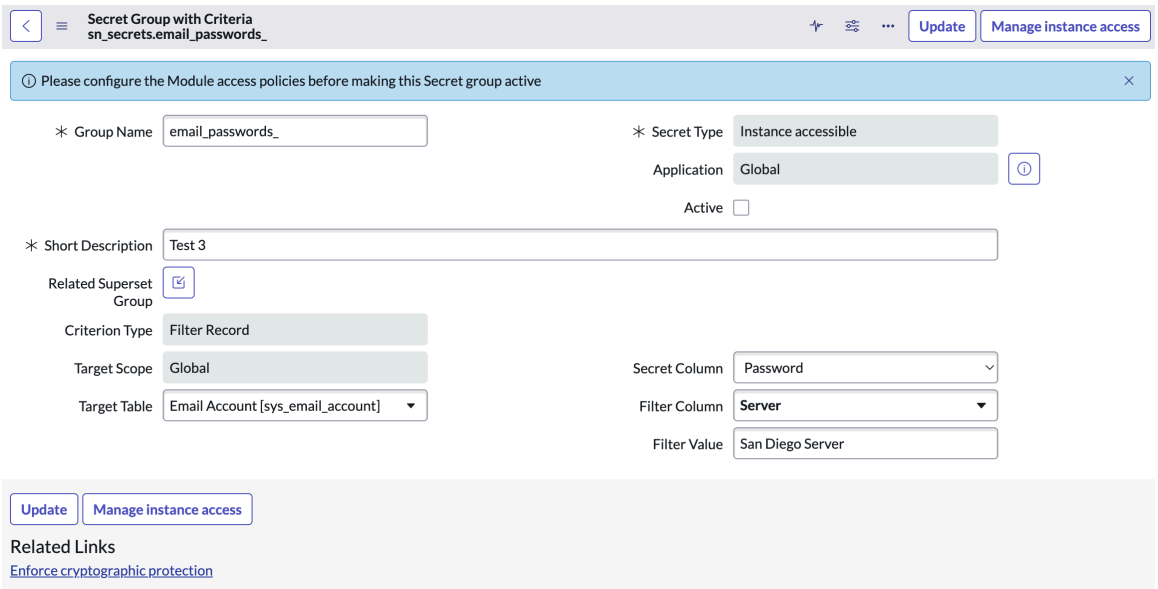
フィールド	説明
ターゲットスコープ	このグループにアサインされるシークレットによって共有されるスコープ。このフィールドは、[基準タイプ] フィールドで [スコープ] を選択した場合にのみ使用できます。
ターゲットパッケージ	このグループにアサインされるシークレットによって共有されるパッケージ。このフィールドは、[基準タイプ] フィールドで [パッケージ] を選択した場合にのみ使用できます。
ターゲットテーブル	このグループにアサインされるシークレットによって共有されるテーブル。このフィールドは、[基準タイプ] フィールドで [テーブル] または [シークレット列] を選択した場合にのみ使用できます。
ターゲットスコープ	[ターゲットテーブル] フィールドで選択されたテーブルのアプリケーションスコープ。このフィールドは、[基準タイプ] フィールドで [テーブル] または [シークレット列] を選択した場合にのみ表示されます。
シークレット列	このグループに含める pasword2 シークレットを含むテーブル列。このリストで使用できるフィールドは、[ターゲットテーブル] フィールドで選択したテーブルによって決まります。 注: 選択したテーブルにシークレットを含む列がない場合、このフィールドには選択肢として [-- なし --] のみが表示されます。
列をフィルター	フィルターとして使用する [ターゲットテーブル] で選択されたテーブルの列。このフィール

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	ドを Password2 フィールドにすることはできません。
フィルター値	フィルターとして使用する値。このフィルターは、[フィルター列] フィールドのフィールド選択に適用されます。

Example: メールサーバーのすべてのメールアカウントのパスワードを含むインスタンスにアクセス可能なグループ



次のタスク
グループを作成すると、条件に一致するすべての新しいレコードが暗号化されます。このグループ暗号化モジュールを使用して既存のレコードを暗号化するには、セキュリティジョブを実行する必要があります。詳細については、「シークレット管理セキュリティジョブの実行」を参照してください。

クライアントのアクセス可能なグループには、シークレットを暗号化するための顧客提供の公開鍵が必要です。このキーをアップロードする手順については、「顧客指定のキーの設定とアップロード」を参照してください。

シークレット管理セキュリティジョブの実行

インスタンスのシークレットフィールドで暗号化タスクを実行するシークレット管理ジョブをスケジュールします。

始める前に
必要なロール：sn_kmf.admin、security_admin、sn_secrets.admin

次の手順を実行するには、security_admin ロールに昇格する必要があります。このプロセスの詳細については、「特権ロールへの昇格」を参照してください

手順

1. 移動先 すべて > システムセキュリティ > セキュリティジョブ > 新規作成.
2. [作成するセキュリティジョブのタイプは？] プロンプトで、[シークレット管理ジョブ] を選択します。
3. フォームのフィールドに入力します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

[シークレット管理ジョブ] フォーム

フィールド	説明
名前	セキュリティジョブの名前
状態	初期ジョブのステータスは新規です。ジョブがスケジュールどおりに実行された後、それに応じてステータスが更新されます。
期間開始	24 時間形式のジョブの開始時間。選択した時刻にジョブの実行が開始されます。
期間終了	24 時間形式のジョブの終了時間。この時点でジョブが終了していない場合は、ジョブが完了するまで、次の指定された処理ウィンドウでジョブが続行されます。
適用レベル	ジョブがすべてのテーブルに影響するか、特定のテーブルまたはフィールドに影響を与えるか。以下から選択します。 ○ All Tables ○ 特定のテーブル ○ 特定のフィールド ○ 特定のパッケージ ⚠ 警告: [すべてのテーブル] オプションを選択すると、インスタンスのパフォーマンスに影響を与える可能性があります。ピーク時間外にスケジュールすることを検討してください。
パッケージ	このジョブに含めるパッケージ。選択したパッケージに暗号化が適用されます。このオプションは、[適用レベル] フィールドが [特定のパッケージ **(Specific Packages)]** に設定されている場合にのみ表示されます
テーブル	このジョブに含めるテーブル。選択したテーブル内のすべての適用可能なフィールドに暗号化が適用されます。このオプションは、[適用レベル] が [特定のテーブル] に設定されている場合にのみ表示されます
フィールド	このジョブに含めるテーブル。選択したすべてのフィールドに暗号化が適用されます。このオプションは、[適用レベル] が [特定のフィールド] に設定されている場合にのみ表示されます
ジョブモード	以下から選択します。 Password2 からシークレット管理 各グループのモジュールアクセスポリシーが定義されている暗号化モジュールを使用して、シー

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	クレットグループ内のすべての Password2 フィールドを暗号化します。 シークレット管理から Password2 Password2 暗号化を使用して、シークレットグループのデータを再暗号化します。この暗号化タイプの詳細については、「KMF による Password2 暗号化」を参照してください。 シークレットグループの適用 [シークレットグループ] フィールドで選択したグループに一致する必要があるすべてのデータをクエリーします。クエリーによって見つかったすべてのデータが既にグループ内にある場合、ジョブは変更を行いません。クエリーでまだグループに含まれていないデータが見つかった場合、ジョブはこのデータをシークレットグループ内で再暗号化します。 **注:** このクエリーで見つかったデータが既に暗号化されていて、インスタンスでそのデータを復号化できない場合は、データは暗号化されずにシークレットグループに追加されます。
シークレットグループ	暗号化するシークレットを含むシークレットグループ。このフィールドは、[ジョブモード] フィールドで [シークレットグループ] が選択されている場合にのみ使用できます。
データのリキーを強制	
サマリー	ジョブの進捗状況に関する情報を表示します。[サマリー] には、ジョブで暗号化できなかったレコードも表示されます。

4. [送信] を選択します。

次のタスク

このジョブは、選択したシークレットグループに一致する必要があるすべてのデータをクエリーします。クエリーによって見つかったすべてのデータが既にグループ内にある場合、ジョブは変更を行いません。クエリーでまだグループに含まれていないデータが見つかった場合、ジョブはこのデータをシークレットグループ内で再暗号化します。(インスタンスで復号化できる場合でも、クライアント側で暗号化されたシークレットは複合化できない可能性があります)。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ServiceNow Vault

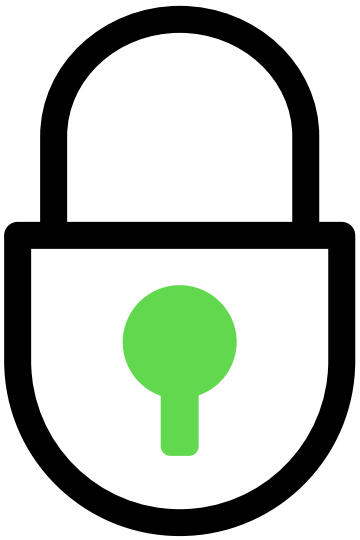
ライフサイクル全体に渡って機密情報を不正なアクセス、破損、または盗難から保護するデータセキュリティツールの ServiceNow Vault 製品セットを使用します。機密情報の編集と監査のために、暗号化、シークレット管理、データプライバシーなどの保護を適用します。ServiceNow Vault ホームページは、ServiceNow Vault データセキュリティ製品を見つけてそこに移動するための単一の表示可能な場所を提供します。

ServiceNow Vault は、ServiceNow 担当者が本番インスタンスで有効にする必要がある有料プラグインです。 ServiceNow Vault には、ここに示すコンポーネントが含まれています。

サブスクリプションを購入するには、ServiceNow アカウントマネージャーにお問い合わせください。サブスクリプションを購入すると、特定のプラグインが自動的にアクティブになります。有料プラグインが自動的にアクティブになっていない場合は、インスタンスの [すべてのアプリケーション] リストから手動でアクティブ化できます。

ServiceNow Vault コンポーネント

暗号化



キー管理と Column Level Encryption は、高度に構成可能な暗号化モジュールのスイートです

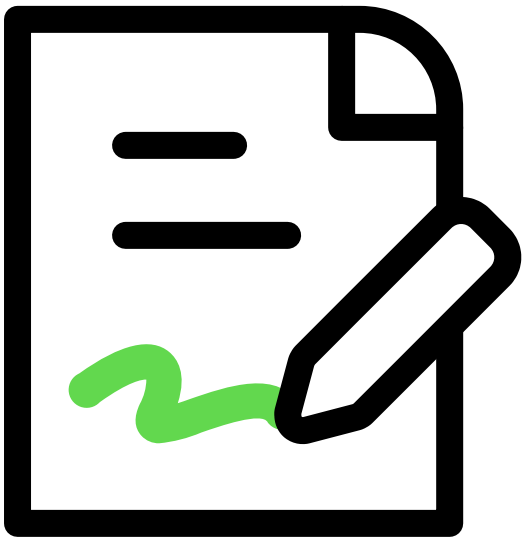
シークレット管理

プラットフォーム上のハードコードされたシークレット (パスワード、証明書、API キーなど) を、顧客によるシークレットの管理に置き換えるソリューション。

自動翻訳

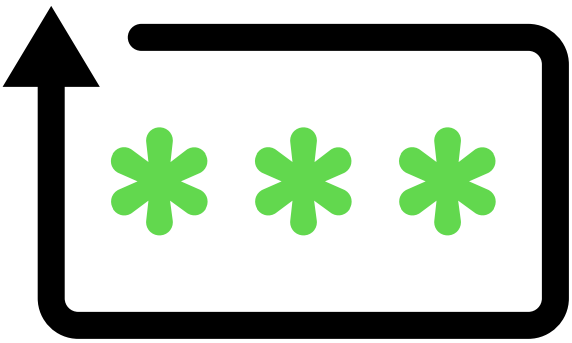
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

コード署名



機密性の高いアプリケーション構成データとスクリプトを使用する前に検証できるので、セキュリティの強化に役立ちます。

Data Privacy



Data Privacy プラグインを使用して、本番インスタンスから非本番インスタンスに移行されるユーザーデータから個人識別可能情報 (PII) を削除します。

Data Discovery

Data Discovery プラグインを使用すると、ユーザーデータから個人を特定できる情報 (PII) を見つけることができます。このデータを分類して、さらにセキュリティ対策を講じることができます。

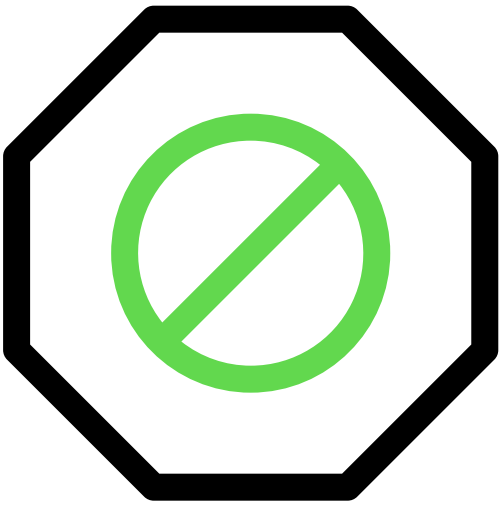
ログ

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ログエクスポートサービスを使用して、ServiceNow ログデータをエンタープライズログ分析にインポート [qa: BEGIN review][End]することで、セキュリティ、パフォーマンス、およびユーザーエクスペリエンスを向上させます。

Zero Trust アクセス



[qa: BEGIN review][End]ServiceNow セッションアクセスを使用すると、組織は Web セッションのユーザー権限を動的に削減できます

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

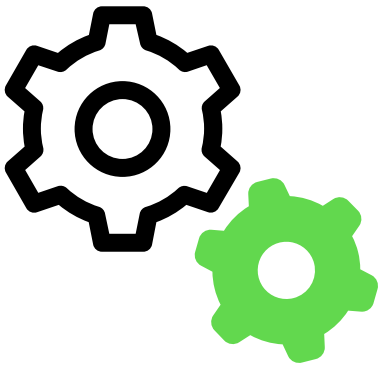
プラットフォームプライバシー

プライバシーを使用すると、インスタンスの機密データをマスクできます。

ACL

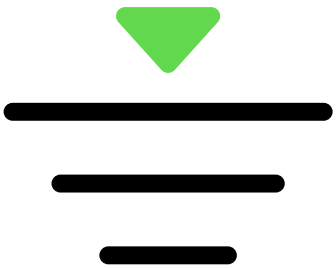
アクセス制御リスト (ACL) のルールは、ユーザーがデータを操作する前に、まず要件のセットをユーザーに要求することで、データへのアクセスを制限します。

データ分類



事前定義またはユーザー定義のデータ分類を使用して、データをタイプ別にグループ化します。ユーザーがデータ分類管理者または監査人ロールを持っている場合は、さまざまなデータクラスを管理したり、インスタンス内のさまざまなタイプのデータの現在のステータスを視覚的に分析したりすることができます。

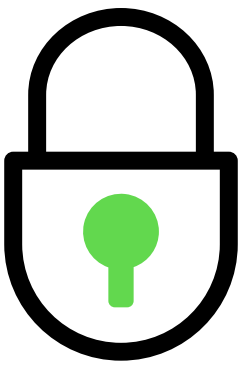
データフィルタリング



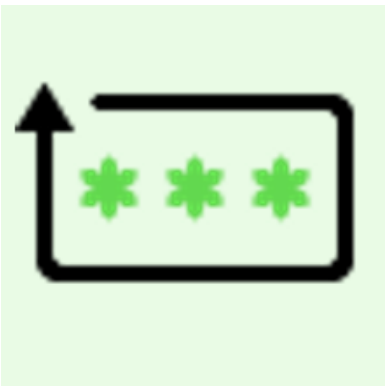
読み込みクエリを実行するときに、データフィルタリングを使用し、対象の属性に基づいてテーブルとレコードへのアクセスを制御します。

Domain Separation

Data Privacy



Data Discovery



Data Discovery を使用してインスタンス内の機密データを識別し、分類、保護、またはレポートします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ServiceNowこのプラットフォームを使用することで、サービスプロバイダー (SP) は、顧客に迅速なオンボーディングを提供し、コンプライアンスを満たし、ドメイン分離を使用してデータを保護できます。	Data Privacy を使用して、機密データを分類し、本番インスタンスのユーザーデータから個人識別可能情報 (PII) を削除して、非本番インスタンスのデータを匿名化します。	

アクセス制御リスト (ACL)

アクセス制御リスト (ACL) のルールは、まず要件のセットをユーザーに要求し、その後でユーザーとやり取りできるようにすることで、データへのアクセスを制限します。

データ分類

事前定義またはユーザー定義のデータ分類を使用して、データをタイプ別にグループ化します。ユーザーがデータ分類管理者または監査人ロールを持っている場合は、さまざまなデータクラスを管理したり、インスタンス内のさまざまなタイプのデータの現在のステータスを視覚的に分析したりすることができます。

データフィルタリング

読み込みクエリを実行するときに、データフィルタリングを使用し、対象の属性に基づいてテーブルとレコードへのアクセスを制御します。

Domain Separation

ServiceNow プラットフォームを使用すると、サービスプロバイダー (SP) は、顧客に迅速なオンボーディングを提供し、コンプライアンスを満たし、Domain Separation を使用してデータを保護できます。クライアントデータ、プロセス、およびレポートをドメインと呼ばれる論理グループに分けることができます。SP は、誰がどのコンテンツを表示してアクセスするかをコントロールします。

Data Privacy

Data Privacy を使用して、機密データを分類し、本番インスタンスのユーザーデータから個人識別可能情報 (PII) を削除して、非本番インスタンスのデータを匿名化します。

Data Discovery

Data Discovery を使用してインスタンス内の機密データを識別し、分類、保護、またはレポートします。

アクセス制御リストのルール

アクセス制御リスト (ACL) のルールは、まず要件のセットをユーザーに要求し、その後でユーザーとやり取りできるようにすることで、データへのアクセスを制限します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

探索

ACL について学習します。

構成

ACL を構成します。

参照

コンテキスト依存セキュリティマネージャーの詳細を取得します。

詳細

ACL の詳細を確認します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

アクセス制御リストの概要

アクセス制御リスト (ACL) を確認します。

ACL のコンポーネント

すべてのアクセス制御リストのルールは、次のものを指定しています。

- 保護されるオブジェクトと操作
- オブジェクトにアクセスするために必要な権限

オブジェクトは、アクセスを制御する必要があるターゲットです。各オブジェクトは、特定のテーブル、フィールド、またはレコードを一意に識別するタイプと名前で構成されます。

たとえば、次のエントリはすべてオブジェクトを指定します。

タイプ	名前	保護されたオブジェクト
レコード	[インシデント]。[-- なし --]	インシデントテーブル。
record	[incident].[active]	インシデントテーブルのアクティブフィールド。
REST_Endpoint	user_role_inheritance	user_role_inheritance Scripted REST API のレコード。

各操作は、指定されたオブジェクトに対してシステムが実行できる有効なアクションを説明しています。レコードなどの一部のオブジェクトは複数の操作をサポートしますが、REST_Endpoint などの他のオブジェクトは 1 つの操作のみをサポートします。

たとえば、これらすべてのエントリは操作を指定します。

タイプ	名前	運用	保護されている操作
record	[incident].[-- None --]	create	インシデントテーブルでのレコードの作成。
record	[incident].[active]	write	インシデントテーブルでのアクティブフィールドの更新。
REST_Endpoint	user_role_inheritance	execute	user_role_inheritance Scripted REST API の実行。

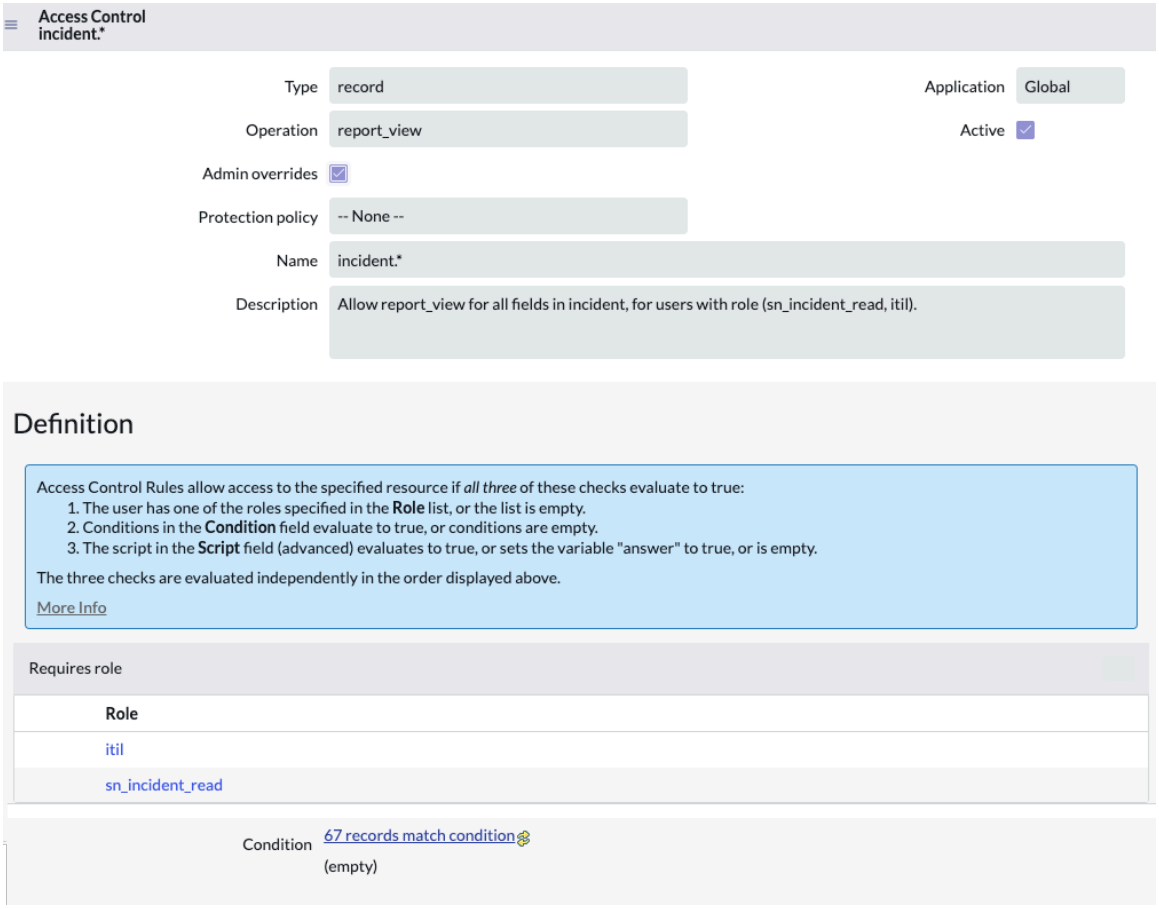
権限は、指定されたオブジェクトと操作に誰がいつアクセスできるかを指定します。セキュリティ管理者は、次のものを追加することで権限要件を指定できます。

- [ロールが必要] リストへの 1 つ以上のユーザーロール。
- 1 つ以上の条件。
- true または false に評価するスクリプト、または `answer` 変数を true または false に設定するスクリプト。

オブジェクトと操作にアクセスするには、ユーザーはアクセス制御にリストされているすべての権限を渡す必要があります。たとえば、このアクセス制御は、インシデントテーブルの書き込み操作へのアクセスを制限します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



インシデントテーブルのレコードを更新するには、ユーザーがリストされているロールを持ち、レコードが条件を満たす必要があります。

権限タイプ	要件	説明
必要なロール	必要なロール：itil	itil ロールを持つユーザーのみがインシデントを更新できます。
条件	[インシデントステータス] [ではない] [クローズ済み]	アクティブなインシデントレコードの更新のみを許可します。

ACL 評価プロセス

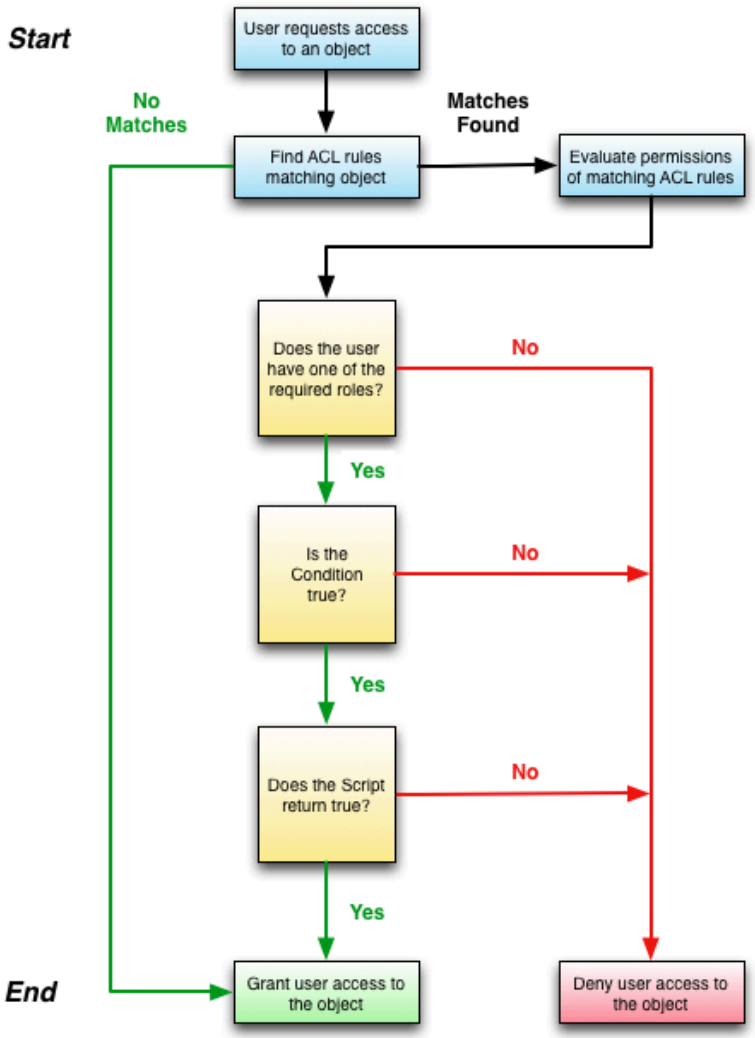
ACL ルールは、ユーザーが一致する ACL ルールに必要なすべての権限を満たしている場合にのみ、オブジェクトへのアクセスを許可します。

- 条件は *true* と評価される必要があります。
- スクリプトは *true* と評価されるか、*true* の値を持つ answer 変数を返す必要があります。
- ユーザーは、必要なロールリストのいずれかのロールを持っている必要があります。リストが空の場合、この条件は *true* と評価されます。
- [レコード ACL ルールのみ] 一致するテーブルレベルの ACL ルールとフィールドレベルの ACL ルールの両方が *true* と評価される必要があります。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ACL 評価権限



セッションでデータが要求されるたびに、要求されたオブジェクトと操作に一致するアクセス制御ルールが検索されます。一致するアクセス制御ルールがある場合、ユーザーがオブジェクトと操作にアクセスするために必要な権限を持っているかどうかが評価されます。アクセス制御ルールで複数の権限が指定されている場合、ユーザーはオブジェクトと操作にアクセスするためにすべての権限を満たす必要があります。いずれかの権限チェックに失敗すると、ユーザーは一致するオブジェクトと操作にアクセスできません。

ユーザーが最初に一致したルールの権限を満たさない場合、アクセス制御処理順序で指定されたとおりに次に一致するアクセス制御ルールの権限が評価されます。ユーザーが一致するアクセス制御ルールを満たしていない場合、要求されたオブジェクトと操作へのアクセスが拒否されます。

注:
要求されたオブジェクトと操作に一致するアクセス制御ルールがない場合、ユーザーにアクセス権が付与されます。実際には、システムにはすべてのレコード操作を保護する一連のデフォルトのアクセス制御ルールがあるため、一致するルールが見つからないことはほとんどありません。

オブジェクトへのアクセスが拒否された場合の影響は、ユーザーが満たしていない ACL ルールによって異なります。たとえば、読み取り操作の ACL ルールを満たしていない場合、ユーザーはオブジェクトを表示できません。保護されているオブジェクトに応じて、ACL ルールによってフォーム上のフィールドが非表示にされたり、リストの行が非表示にされたり、ユーザーが UI ページへのア

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

クセスを禁止されたりします。次の表に、特定の操作とオブジェクトタイプの ACL ルールを満たしていない場合の結果の完全なリストを示します。

クエリー前後の **ACL** チェック

インスタンスは、ユーザーがクエリーを実行する前と後に ACL ルールをチェックします。クエリーの前と後で使用可能な情報が異なるため、結果が異なる可能性があります。

クエリー前の ACL チェック

インスタンスはデータベースクエリを実行する前に、クエリ対象のテーブル内の各フィールドの ACL ルールをチェックして、ユーザーがアクセスできるフィールドを判断します。このチェックでは、ユーザーのロールのみを調べ、これらのロールがフィールドへのアクセスを許可されるかどうかを確認します。このチェックはクエリの前に実行されるため、ACL はテーブルのレコードにアクセスできず、そのデータを考慮することができません。レコードの内容を知ることに依存するスクリプトと条件は評価されません。

この時点でユーザーに読み取りアクセス権がない場合、フィールドの値はユーザーに表示されません。

クエリー後の ACL チェック

クエリーの後に、インスタンスはクエリーによって返された各レコードをチェックします。このチェック中には ACL のコンテキストがあるため、ACL のロール、条件、およびスクリプトの部分が評価されます。この時点でユーザーに読み取りアクセス権がない場合、フィールドの値はユーザーに表示されませんが、ユーザーのロールがフィールドへのアクセスを許可していれば、フィールドラベルが表示されます。

運用	オブジェクトに関する **ACL** ルールを満たしていない場合の結果
execute	ユーザーはレコードまたは UI ページでスクリプトを実行できません。
作成	ユーザーはフォームから 新しい UI アクションを表示できません。ユーザーは、Web サービスなどの API プロトコルを使用してテーブルにレコードを挿入することもできません。 フィールドに特定の値が含まれていることを条件として ACL を作成すると、常に false と評価されます。新しいレコードのフィールドは、レコードが保存されるまで空と見なされます。
read	ユーザはフォームまたはリストでオブジェクトを表示できません。ユーザーは、Web サービスなどの API プロトコルを使用してレコードを取得することもできません。
write	ユーザーにはフォームとリストの読み取り専用フィールドが表示され、Web サービスなどの API プロトコルを使用してレコードを更新することはできません。
delete	ユーザーはフォームから削除 UI アクションを表示できません。ユーザーは、Web サービスなどの API プロトコルを使用してテーブルからレコードを削除することもできません。
edit_task_relations	ユーザーはタスクテーブル間の関係を定義できません。
edit_ci_relations	ユーザーは構成アイテム [cmdb_ci] テーブル間の関係を定義できません。
save_as_template	テンプレートの作成時に保存する必要があるフィールドを制御するために使用されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

運用	オブジェクトに関する **ACL** ルールを満たしていない場合の結果
add_to_list	ユーザーは、リストメカニックの特定の列を表示またはカスタマイズすることはできません。
list_edit	ユーザーはリストからレコード (行) を更新できません。
report_on	ユーザーは ACL テーブルでレポートを作成できません。詳細については、「ACL ルールを使用してレポートの作成を制限する」を参照してください。
report_view	ユーザーは、ACL テーブルまたは ACL フィールドのレポートの内容を表示できません。詳細については、「Reporting」を参照してください。
personalize_choices	ユーザーはリストフィールドを右クリックして [選択を構成] を選択できません。

オブジェクトの **ACL** 一致要件

オブジェクトタイプ	アクセスオブジェクトに必要な一致する **ACL** ルール	既存のワイルドカード **ACL** ルール
クライアントコール可能スクリプトインクルード プロセッサー	ユーザーは次の 2 つの ACL ルールの権限を満たす必要があります。 **1.** オブジェクトのすべてのワイルドカード ACL ルール (操作に対する ACL ルールが存在する場合)。 **2.** オブジェクトの名前に一致する最初の ACL ルール (操作に対する ACL ルールが存在する場合)。	既定では、これらのオブジェクトの種類にワイルドカード (*) 規則はありません。これらのオブジェクトの 1 つにワイルドカード ACL ルールを作成すると、ACL ルールがこのタイプのすべてのオブジェクトに適用されます。
UI ページ レコード	ユーザーは次の 2 つの ACL ルールの権限を満たす必要があります。 **1.** レコードのフィールドに一致する最初の ACL ルール (操作に対する ACL ルールが存在する場合)。 **2.** レコードのテーブルに一致する最初の ACL ルール (操作に対する ACL ルールが存在する場合)。	デフォルトでは、作成、読み取り、書き込み、および削除操作用のワイルドカードテーブルルール (*) と、personalize_choices、作成、およびsave_as_template 操作用のワイルドカードフィールドルール (*.*) があります。テーブルを作成するときは、提供されているワイルドカード ACL ルールを使用する場合を除き、テーブルの ACL ルールを作成します。

注:
セキュリティマネージャーのデフォルトの動作 (`glide.sm.default_mode`) プロパティは、ワイルドカードテーブルの ACL ルールにのみ一致するオブジェクトにユーザーがアクセスできるかどうかを決定します。このプロパティが [アクセスを拒否] に設定されている場合、管理者のみがワイルドカードテーブルの ACL ルールにアクセスできます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注:
作成操作のワイルドカードフィールド ACL ルール (*.*) は、書き込み操作と同じ権限を再利用します。これは、明示的な作成操作の ACL ルールを定義しない限り、作成権限が書き込み権限と同じであることを意味します。

処理順序の同じ時点にある複数の ACL ルール

2 つ以上のルールが処理順序の同じ時点で一致する場合、ユーザーは、オブジェクトにアクセスするためにいずれかの ACL ルールの権限を渡す必要があります。たとえば、*incident.number* に対して 2 つのフィールド ACL ルールを作成した場合、1 つのルールを満たすユーザーは、ユーザーが処理順序の同じ時点で他のフィールド ACL ルールを満たしていないかどうかにかかわらず、その番号フィールドにアクセスできます。

必要なロール

通常の管理者ユーザーは、アクセス制御ルールを表示してデバッグできます。ただし、既存のアクセス制御ルールを作成または更新するには、管理者が security_admin ロールに権限を昇格させる必要があります。手順については、「特権ロールへの昇格」を参照してください。

スコープ対象のアプリケーションの ACL ルール

ACL ルールと同じスコープ内にあるオブジェクトに対して ACL ルールを作成できます。ACL ルールと同じスコープ内にあるフィールドを少なくとも 1 つ持つテーブルに対しても、ACL ルールを作成できます。

ACL ルールレコードとは異なるスコープ内のテーブルの場合は、ルールのタイプが制限されます。

- ACL ルールと同じスコープ内にある任意のテーブル、UI ページ、またはその他のオブジェクトに対して ACL ルールを作成できます。
- ACL ルールと同じスコープ内にあるフィールドに対して ACL を作成できます。
  - テーブルが同じスコープ内にある場合は、スクリプトを使用して権限を評価できます。
  - テーブルが別のスコープ内にある場合は、スクリプトを使用して権限を評価することはできません。
- アプリケーションピッカーで選択したアプリケーションとは異なるスコープにあるオブジェクトの ACL ルールを作成または変更することはできません。これには、異なるスコープの ACL へのロールの追加も含まれます。
- ワイルドカードテーブルルール (*) は、グローバルスコープでのみ作成できます。
- ACL ルールと同じスコープ内のテーブルに対してのみ、ワイルドカードフィールドルール (*) を作成できます。

ACL ルールのタイプ

システムのさまざまなコンポーネントに関する ACL ルールを作成します。

レコードの ACL ルール

レコードの ACL ルールはテーブル名とフィールド名で構成されます。

- テーブル名は保護するテーブルです。他のテーブルがこのテーブルから拡張されている場合、そのテーブルは親テーブルと見なされます。親テーブルの ACL ルールは、親テーブルを拡張するすべてのテーブルに適用されます。
- フィールド名は保護するフィールドです。テーブル拡張により、一部のフィールドが複数のテーブルに含まれています。親テーブル内のフィールドの ACL ルールは、親テーブルを拡張するすべてのテーブルに適用されます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

ACL ルールは、次のレコード操作を保護できます。

運用	説明
create	ユーザーが新しいレコード (行) をテーブルに挿入できるようにします。
read	ユーザーがテーブルのレコードを表示できるようにします。
write	ユーザーがテーブル内のレコードを更新できるようにします。
delete	ユーザーがテーブルからレコードを削除したり、テーブルを削除したりできるようにします。
edit_task_relations	ユーザーがタスク [task] テーブルを拡張できるようにします。
edit_ci_relations	ユーザーが構成アイテム [cmdb_ci] テーブルを拡張できるようにします。
save_as_template	ユーザーがレコードをテンプレートとして保存できるようにします。
add_to_list	ユーザーがリストメカニズムの特定の列を表示またはカスタマイズできないようにします。 **注:** 条件とスクリプトはサポートされていません。
list_edit	ユーザーがリストからレコード (行) を更新できるようにします。
report_on	ユーザーがテーブルでレポートできるようにします。
report_view	ユーザーがフィールド ACL でレポートできるようにします。
personalize_choices	ユーザーがテーブルまたはフィールドを設定できるようにします。

レコードの ACL ルールは次の順序で処理されます。

- オブジェクトをテーブルの ACL ルールと照合します。
- オブジェクトをフィールドの ACL ルールと照合します。

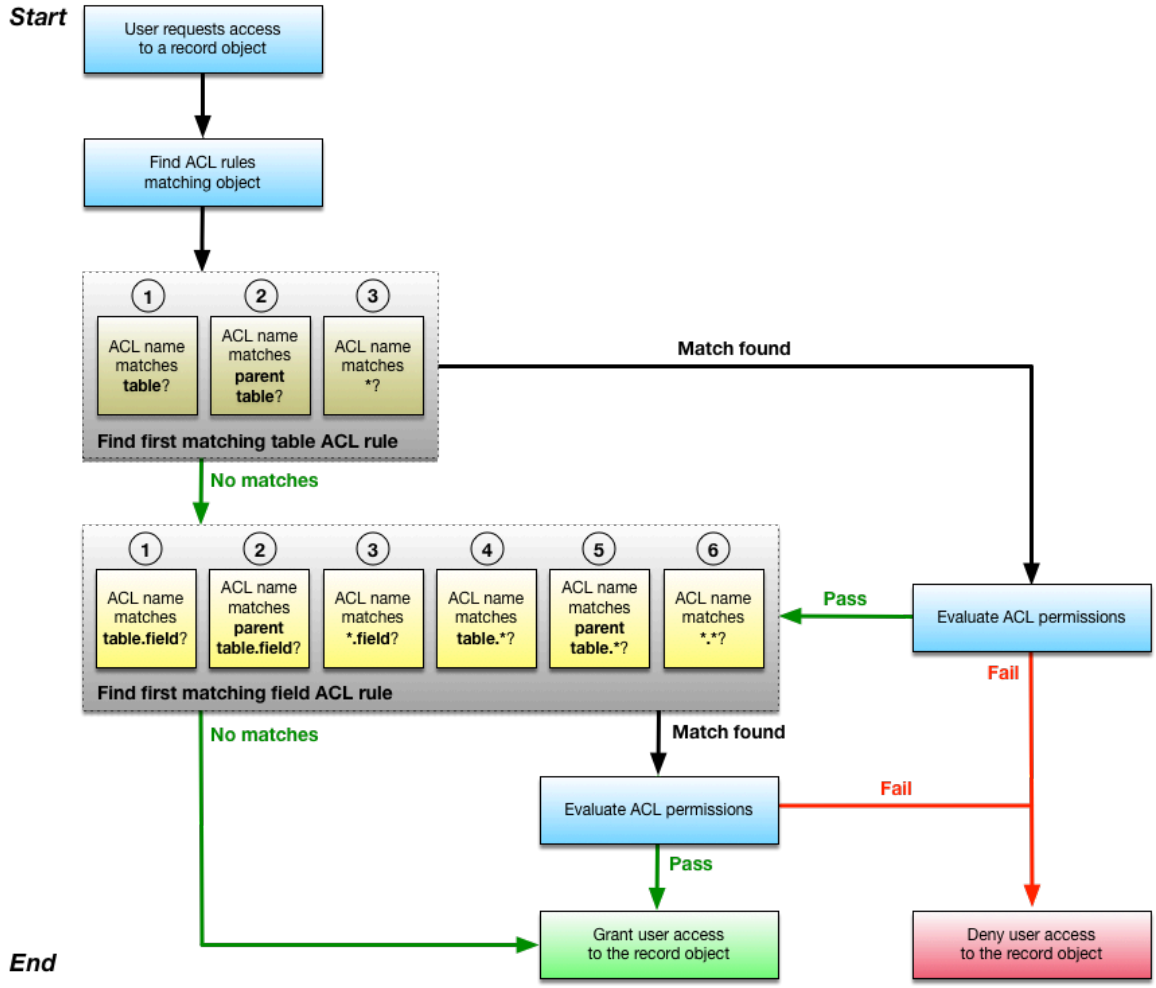
この処理順序により、ユーザーは、より一般的なオブジェクトへのアクセス権を得る前に、より具体的なオブジェクトへのアクセス権を得ることができます。レコードオブジェクトにアクセスするには、テーブルとフィールドの両方の ACL ルールを満たす必要があります。

- ユーザーがテーブルの ACL ルールを満たしていない場合、ユーザーがフィールドの ACL ルールを満たしていても、テーブル内のすべてのフィールドへのアクセスが拒否されます。
- ユーザーがテーブルの ACL ルールを満たしていても、フィールドの ACL ルールを満たしていない場合、ユーザーはフィールドの ACL ルールによって記述されたフィールドにアクセスできません。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ACL の一致



プロセッサの ACL ルール

プロセッサの ACL ルールは、保護するプロセッサを指定します。使用可能なプロセッサのリストについては、次に移動します システム定義 > プロセッサー.

デフォルトでは、メールクライアントを itil ロールを持つユーザーに制限するために、EmailClientProcessor の ACL ルールが含まれています。

プロセッサの ACL ルールは、それらのリソースに対してより具体的な ACL が見つからない場合、星 (*) ルールに従います。

テーブル ACL ルール

ユーザーは最初にテーブルの ACL ルールに合格する必要があります。ベースシステムにはすべてのテーブルに一致する星 (*) テーブルの ACL ルールが含まれているため、ユーザーは常に少なくとも 1 つのテーブル ACL ルールを満たす必要があります。ベースシステムは、特定のテーブルへのアクセスを制御する追加のテーブル ACL ルールを提供します。

テーブルの ACL ルールは次の順序で処理されます。

1. テーブル名と一致します。たとえば、incident などです。
2. 親テーブル名と一致します。たとえば、task です。
3. いずれかのテーブル名 (*) と一致します。たとえば、* です。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ユーザーがすべてのテーブルの ACL ルールを満たしていないと、ユーザーはテーブル内のフィールドにアクセスできません。ユーザーがテーブルの ACL ルールを満たすと、フィールドの ACL ルールが評価されます。

フィールドの **ACL** ルール

ユーザーがテーブルの ACL ルールに合格すると、フィールドの ACL ルールが次の順序で処理されます。

1. テーブルおよびフィールド名と一致します。たとえば、incident.number です。
2. 親テーブルおよびフィールド名と一致します。たとえば、task.number です。
3. いずれかのテーブル (*) およびフィールド名と一致します。たとえば、*.number です。
4. テーブルおよびいずれかのフィールド (*) と一致します。たとえば、incident.* です。
5. 親テーブルおよびいずれかのフィールド (*) と一致します。たとえば、task.* です。
6. いずれかのテーブル (*) およびフィールド (*) と一致します。たとえば、*.* です。

テーブルのフィールドへのアクセスを許可するには、ユーザーがテーブル ACL ルールを満たす必要があります。たとえば、インシデントテーブルの [番号] フィールドにアクセスするには、まずインシデントテーブルのテーブル ACL ルールを満たす必要があります。

最初に成功したフィールド ACL 評価は、フィールドレベルで ACL ルール処理を停止します。ユーザーがフィールド ACL ルールを満たすと、他の一致するフィールド ACL ルールの検索を停止します。たとえば、ユーザーが incident.number のフィールド ACL ルールを満たしている場合、システムはインシデントテーブルの [番号] フィールドを保護する他の ACL ルールの検索を停止します。

保護されたフィールドでは推定データのクエリ情報へのアクセスが制限されているため、予測情報が返されません。

UI ページの **ACL** ルール

UI ページの ACL ルールは、保護する UI ページを指定します。利用可能な UI ページのリストについては、次に移動します システム **UI** > **UI** ページ. UI ページの ACL ルールを定義するときは、完全にスコープ範囲内のページ名を使用します。たとえば、**x_myapp_mypage** です。

> **注:**
> **ui_page** タイプの ACL の [名前] フィールドで星印 (*) 文字を使用して、任意の UI ページに一致させることができます。

UI ページの ACL ルールは、それらのリソースに対してより具体的な ACL が見つからない場合、星 (*) ルールに従います。たとえば、mysecretpage という名前の UI ページがあり、この UI ページの ACL が定義されていない場合は、UI ページプロセッサの星 (*) ルールがアクセスチェックに使用されます。

ACL ルールは、次の UI ページ操作を保護できます。

運用	説明
read	ユーザーが UI ページを表示できるようにします。

クライアントコール可能スクリプトインクルードの **ACL** ルール

スクリプトインクルードの ACL ルールは、保護するクライアントコール可能スクリプトインクルードを指定します。利用可能なスクリプトインクルードのリストについては、次に移動します システ

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

ム定義 > スクリプトインクルード. リストをカスタマイズして [クライアントコール可能] 列を表示できます。

ベースシステムには、クライアントコール可能スクリプトインクルードの ACL ルールが含まれていません。

クライアントコール可能スクリプトインクルードの ACL ルールは、それらのリソースに対してより具体的な ACL が見つからない場合、星 (*) ルールに従います。

機能フィールドの **ACL** 制御

機能フィールドへのアクセスを評価する場合、機能フィールド自体へのアクセスがチェックされるだけでなく、機能の貢献フィールドへのアクセスもチェックされます。貢献フィールドは、指定された機能の定義の引数として使用されるフィールドです。

機能フィールドの詳細については、「機能フィールド」を参照してください。

Rome 以前では、(他のフィールドと同様に) 機能フィールド自体へのアクセスをチェックします。そのフィールドの ACL でアクセスが許可されている場合、ユーザーが貢献フィールドへのアクセス権を持っているかどうかにかかわらず、ユーザーは結果の値を受け取ります。

Washington DC 以降では、機能フィールドへのアクセスを許可するには、すべての貢献フィールドへのアクセスも必要です。1 つ以上の貢献フィールド ACL でアクセスが拒否される場合、機能フィールドでもアクセスが拒否されます。

新しい要件の影響を受ける操作は、読み取りと report_view のみです。report_view には独自の追加要件があります。

操作	説明
読み取り操作	ユーザーは、次の両方の条件に当てはまる場合にのみ、機能フィールドの読み取りアクセス権があります。 • ユーザーは機能フィールドの読み取りアクセス権を持っている。 • ユーザーは、機能で使用されるすべての貢献フィールドの読み取りアクセス権を持っている。
report_view 操作	ユーザーは、次のすべての条件に当てはまる場合にのみ、機能フィールドの report_view アクセス権があります。 • ユーザーは機能フィールドの report_view アクセス権を持っている。 • ユーザーは、各貢献フィールドの report_view アクセス権を持っている。 • 条件とスクリプトのないロールのみの読み取り ACL があり、ユーザーはそのロールを持っている。 • ユーザーは、条件またはスクリプトのない ACL のみが許可されるように、貢献フィールドの読み取り専用アクセス権を持っている。

例

前提：

- テーブル：給与
- 列：基本、ボーナス、合計 (この例ではすべて整数)

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- 機能フィールド：合計列は機能フィールドとしてマークされ、機能の定義は glidefunction:add（基本、ボーナス）です。
- 貢献フィールド：機能の定義で使用されるため、基本とボーナス
- ロール：salary_admin、bonus_admin

例 1：すべてのフィールドでアクセスが可能

ACL	結果
合計、基本、ボーナス：salary_admin ロールの場合、読み取りおよび report_view (条件またはスクリプトなし)	必要なロールを持っているため、salary_admin ロールを持つユーザーには、合計の読み取りと report_view アクセス権が付与されます。

例 2：貢献フィールドで読み取りアクセスが拒否される

ACL	結果
• 合計、基本：salary_admin ロールの場合、読み取りおよび report_view (条件またはスクリプトなし) • ボーナス：salary_admin ロールの場合、report_view (条件またはスクリプトなし) • ボーナス：bonus_admin ロールの場合、読み取り (条件またはスクリプトなし)	salary_admin ロールではボーナスの読み取りアクセスが拒否されるため、salary_admin ロールを持つユーザーは、合計の読み取りと report_view アクセスは拒否されます。

例 3：貢献フィールド **ACL** にスクリプトがある

ACL	結果
• 合計、基本：salary_admin ロールの場合、読み取りおよび report_view (条件またはスクリプトなし) • ボーナス：bonus_admin ロールの場合、report_view (条件またはスクリプトなし) • ボーナス：salary_admin ロールの場合、読み取り、スクリプトあり (内容にかかわらず、スクリプトがあることのみが重要)	すべてのフィールドに対する必要なロールを持っているため、salary_admin ロールを持つユーザーには、合計の読み取りアクセス権が付与されます。 ただし、必要なロールを持っている場合でも、スクリプトのある ACL はデフォルトで読み取りアクセスを拒否するため、salary_admin ロールを持つ同じユーザーは report_view アクセスを拒否されます。

Security Jump-Start - ACL ルールプラグイン

Security Jump-Start Access Control Level (ACL Rules) プラグインは、すべての新しいインスタンスに自動的にインストールされます。このプラグインを使用すると、複数のシステムテーブルを迅速に保護し、組織の本番起動プロセスを迅速化できます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

このプラグインは、本番環境で既に使用されているテーブルへのセキュリティアクセスを変更する可能性があるため、既存のインスタンスを対象としていません。管理者がこのプラグインを既存のインスタンスにインストールすることを強く希望する場合は、最初にテストインスタンスで徹底的にテストすることをお勧めします。これにより、組織の現在の実装との互換性を確保できます。

管理者がこのプラグインによって提供される新しい ACL ルールに関心がある場合は、ACL のリストを指針として使用して、既存のインスタンスに 1 つ以上のルールを手動で作成できます。

このプラグインには次の ACL が含まれています。ヘッダー行のアイコンを選択して、その列を昇順または降順で並べ替えます。操作キーは次のとおりです。

- R = 読み込み
- W = 書き込み
- D = 削除
- C = 作成

名前	運用	説明
cmdb_ci	WCD	構成アイテムレコードの書き込み/作成/削除には、asset または itil ロールが必要です
cmn_department	WD	部門レコードの書き込み/削除には user_admin ロールが必要です
cmn_location	WC	場所レコードの書き込み/作成には user_admin ロールが必要です
core_company	WD	会社レコードの書き込み/削除には user_admin ロールが必要です
kb_knowledge	作成	ナレッジレコードを作成するには「knowledge」ロールが必要です
ldap_ou_config	RWCD	LDAP OU 定義レコードの読み取り/書き込み/作成/削除には、user_admin ロールが必要です
ldap_server_config	RWCD	LDAP サーバーレコードの読み取り/書き込み/作成/削除には、user_admin ロールが必要です
process_guide	WCD	プロセスガイドレコードの書き込み/作成/削除には、admin ロールが必要です
process_step	WCD	プロセスステップレコードの書き込み/作成/削除には、admin ロールが必要です
sc_category	作成	サービスカタログカテゴリレコードの作成には、catalog_admin ロールが必要です
sc_category	削除	サービスカタログカテゴリレコードの削除には、catalog_admin ロールが必要です
sc_category	書き込み	サービスカタログカテゴリレコードへの書き込みには、catalog_admin ロールが必要です
sc_cat_item	書き込み	カタログアイテムレコードに書き込むには「catalog_admin」ロールが必要です
sc_cat_item	削除	カタログアイテムレコードを削除するには「catalog_admin」ロールが必要です

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

名前	運用	説明
sc_cat_item	作成	カタログアイテムレコードを作成するには、「catalog_admin」ロールが必要です
sysevent_email_action	読み込み専用	メール通知レコードは、すべてのユーザーが読み込めます (サブスクリプション目的)
sysevent_register	RWCD	イベント登録レコードの読み取り/書き込み/作成/削除には、admin ロールが必要です
sysevent_script_action	RWCD	スクリプトアクションレコードの読み取り/書き込み/作成/削除には、admin ロールが必要です
syslog	RWCD	ログエントリレコードの読み取り/書き込み/作成/削除には、admin ロールが必要です
sysrule	RWCD	ルールレコード (メール通知、Inbound Email Actions、承認ルールなど) の読み取り/書き込み/作成/削除には、admin ロールが必要です
sysrule	read	すべてのユーザーが (サブスクリプションベースの通知) のメール通知レコードを読み取ることができます
sys_app_application	WCD	アプリケーションレコードの書き込み/作成/削除には、admin ロールが必要です
sys_app_category	WCD	アプリケーションカテゴリレコードの書き込み/作成/削除には、admin ロールが必要です
sys_app_module	WCD	モジュールレコードの書き込み/作成/削除には、admin ロールが必要です
sys_audit	RWCD	監査レコードの読み取り/書き込み/作成/削除には、admin ロールが必要です
sys_dictionary	RWC	辞書レコードの読み取り/書き込み/作成には、personalize_dictionary ロールが必要です
sys_dictionary.*	読み込み専用	「personalize_dictionary」ロールでは、辞書フィールドを読み込むことができます
sys_documentation	削除	フィールドラベルレコードを削除するには「personalize_dictionary」ロールが必要です
sys_documentation	作成	フィールドラベルレコードを作成するには「personalize_dictionary」ロールが必要です
sys_documentation	書き込み	フィールドラベルレコードへの書き込みには personalize_dictionary ロールが必要です
sys_gauge	RWCD	ゲージレコードの読み取り/書き込み/作成/削除には、admin ロールが必要です
sys_gauge_count	RWCD	ゲージカウントレコードの読み取り/書き込み/作成/削除には、admin ロールが必要です
sys_group_has_role	読み込み専用	グループロールレコードを表示するには、itil ロールが必要です
sys_home	WCD	ようこそページセクションレコードの書き込み/作成/削除には、itil_admin ロールが必要です
sys_installation_exit	WCD	インストレーションイグジットレコードの書き込み/作成/削除には、admin ロールが必要です

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

名前	運用	説明
sys_job	WCD	システムジョブレコードの書き込み/作成/削除には、admin ロールが必要です
sys_nav_link	WCD	ナビゲーションリンクレコードの書き込み/作成/削除には、admin ロールが必要です
sys_perspective	WCD	メニューリストレコードの書き込み/作成/削除には、admin ロールが必要です
sys_portal	RWCD	ポータルレコードの読み取り/書き込み/作成/削除には、admin ロールが必要です
sys_portal_page	RWCD	ホームページレコードの読み取り/書き込み/作成/削除には、admin ロールが必要です
sys_portal_preferences	RWCD	ポータル設定レコードの読み取り/書き込み/作成/削除には、admin ロールが必要です
sys_processor	WC	プロセッサーレコードの書き込み/作成には、admin ロールが必要です
sys_properties	WC	システムプロパティレコードの書き込み/作成には、admin ロールが必要です
sys_properties_category	WCD	プロパティカテゴリレコードの書き込み/作成/削除には、admin ロールが必要です
sys_report	delete	レポートレコードを削除できるロール (レポート UI からの削除を制限しない)
sys_report	write	レポートレコードに書き込むことができるロール (レポート UI からの編集を制限しない)
sys_report	read	ユーザーは、各自のレポートレコード、所属グループのレポートレコード、およびグローバル属性のレポートレコードを読み込むことができます (レポート UI を介した表示には影響しません)
sys_report	read	レポートレコードを読み込むことができるロール (レポート UI からの表示を制限しない)
sys_reportroles	読み込み専用	レポートロールレコードの読み込みには admin ロールが必要です
sys_script	WCD	ビジネスルールレコードの書き込み/作成/削除には、admin ロールが必要です
sys_script_ajax	WCD	AJAX スクリプトレコードの書き込み/作成/削除には、admin ロールが必要です
sys_script_client	WCD	クライアントスクリプトレコードの書き込み/作成/削除には、admin ロールが必要です
sys_script_include	WCD	スクリプトインクルードレコードの書き込み/作成/削除には、admin ロールが必要です
sys_security_acl	書き込み	アクセス制御レコードへの書き込みには admin ロールが必要です
sys_security_acl_role	作成	アクセスロールレコードの作成には admin ロールが必要です
sys_security_acl_role	削除	アクセスロールレコードの削除には admin ロールが必要です

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

名前	運用	説明
sys_security_acl_role	書き込み	アクセスロールレコードへの書き込みには admin ロールが必要です
sys_security_operation	削除	セキュリティオペレーションレコードの削除には admin ロールが必要です
sys_security_operation	作成	セキュリティオペレーションレコードの作成には admin ロールが必要です
sys_security_operation	書き込み	セキュリティオペレーションレコードへの書き込みには admin ロールが必要です
sys_security_type	書き込み	セキュリティタイプレコードへの書き込みには admin ロールが必要です
sys_security_type	作成	セキュリティタイプレコードの作成には admin ロールが必要です
sys_security_type	削除	セキュリティタイプレコードの削除には admin ロールが必要です
sys_status	作成	システムステータスレコードの作成には admin ロールが必要です
sys_status	削除	システムステータスレコードの削除には admin ロールが必要です
sys_status	書き込み	システムステータスレコードへの書き込みには admin ロールが必要です
sys_template	書き込み	テンプレートレコードへの書き込みには template_editor ロールが必要です
sys_template	作成	テンプレートレコードの作成には template_editor ロールが必要です
sys_template	削除	テンプレートレコードの削除には template_editor ロールが必要です
sys_template	読み込み専用	テンプレートロールレコードの読み込みには template_editor ロールが必要です
sys_ui_action	作成	UI アクションレコードの作成には admin ロールが必要です
sys_ui_action	delete	UI アクションレコードの削除には admin ロールが必要です
sys_ui_action	write	UI アクションレコードへの書き込みには admin ロールが必要です
sys_ui_action_view	書き込み	UI ビューアクションレコードへの書き込みには admin ロールが必要です
sys_ui_action_view	作成	UI ビューアクションレコードの作成には admin ロールが必要です
sys_ui_action_view	削除	UI ビューアクションレコードの削除には admin ロールが必要です
sys_ui_policy	作成	UI ポリシーレコードの作成には admin ロールが必要です
sys_ui_policy	削除	UI ポリシーレコードの削除には admin ロールが必要です
sys_ui_policy	書き込み	UI ポリシーレコードへの書き込みには admin ロールが必要です

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

名前	運用	説明
sys_ui_policy_action	作成	UI ポリシーアクションレコードの作成には admin ロールが必要です
sys_ui_policy_action	削除	UI ポリシーアクションレコードの削除には admin ロールが必要です
sys_ui_policy_action	書き込み	UI ポリシーアクションレコードへの書き込みには admin ロールが必要です
sys_ui_script	書き込み	UI スクリプトレコードへの書き込みには admin ロールが必要です
sys_ui_script	削除	UI スクリプトレコードの削除には admin ロールが必要です
sys_ui_script	作成	UI スクリプトレコードの作成には admin ロールが必要です
sys_user	write	ロールのないユーザーは、自分のユーザーレコード以外は更新できません
sys_user_grmember	削除	グループメンバーレコードを削除するには「user_admin」ロールが必要です
sys_user_grmember	書き込み	グループメンバーレコードに書き込むには「user_admin」ロールが必要です
sys_user_group	作成	「itil」と上記のロールのみがグループレコードを作成できます
sys_user_group	書き込み	「itil」と上記のロールのみがグループレコードに書き込むことができます
sys_user_has_role	読み込み専用	ユーザーロールレコードを参照するには「itil」ロールが必要です
sys_user_role	作成	ロールレコードの作成には admin ロールが必要です
sys_user_role	削除	ロールレコードの削除には admin ロールが必要です
sys_user_role	書き込み	ロールレコードへの書き込みには admin ロールが必要です
sys_user_role_contains	読み込み専用	包含ロールレコードを参照するには「itil」ロールが必要です
sys_user_role_contains	書き込み	包含ロールレコードへの書き込みには admin ロールが必要です
sys_user_token	RWCD	ユーザートークンレコードの読み取り/書き込み/作成/削除には、admin ロールが必要です

注:
このプラグインの詳細については、「インスタンスセキュリティ強化設定」の「Security Jump Start (ACL ルール) (インスタンスセキュリティ強化)」を参照してください。

ACL ルールの構成

新しいオブジェクトへのアクセスを保護するため、またはデフォルトのセキュリティ動作を変更するためのカスタム ACL ルールを構成します。

始める前に
必要なロール：security_admin

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

このタスクについて
ACL ルールを作成するには、特権を security_admin ロールに昇格させる必要があります。

ACL ルールレコードとは異なるスコープ内のテーブルの場合は、ルールのタイプが制限されます。スコープマスターテーブルでスコープを派生させてスコープ付き ACL を実行するには、*glide.enforce_security_scope.<scope_name>* プロパティを **true** に設定します。すると、該当するテーブルで作成されたスコープ固有の ACL がある場合に、グローバルスコープ内の ACL が一致しなくなります。たとえば、sys_attachment テーブルや sys_question_answer テーブルといったグローバルスコープ内の共有アプリケーションテーブル内のデータを保護する場合などです。

手順

1. security_admin ロールに昇格された特権ロール。

2. 移動先 システムセキュリティ > アクセス制御 **(ACL)**.

3. [新規] をクリックします。

4. フォームに入力します。

アクセス制御フィールド

フィールド	説明
タイプ	この ACL ルールが保護するオブジェクトの種類を選択します。オブジェクトのタイプによって、オブジェクトの命名方法と使用可能な操作が決まります。このフィールドは、ACL ルールが作成された後に読み取り専用になります。タイプを変更する場合は、ACL を削除して正しいタイプで新しい ACL を作成する必要があります。
操作	この ACL ルールで保護する操作を選択します。各オブジェクトタイプには、独自の操作リストがあります。ACL ルールは 1 つの操作のみを保護できます。複数の操作を保護するには、それぞれに個別の ACL ルールを作成します。
管理者優先	admin ロールを持つユーザーがこの ACL ルールの権限チェックに自動的に合格するようにするには、このチェックボックスをオンにします。管理者ユーザーは、適用されるスクリプトまたはロールに関係なく合格します。ただし、ServiceNow の担当者のみが割り当てることができる **nobody** ロールは、管理者上書きオプションよりも優先されます。ACL に **nobody** ロールが割り当てられている場合、[管理者優先] が選択されていても、管理者ユーザーはリソースにアクセスできません。「ベースシステムロール」を参照してください。 管理者がこの ACL ルールで定義された権限を満たして、保護されたオブジェクトにアクセスする必要がある場合は、このチェックボックスをオフにします。管理者は常にロールチェックに合格するため ([必要なロール] フィールドの説明を参照)、条件ビルダーまたは [スクリプト] フィールドを使用して、管理者が合格する必要がある権限チェックを作成します。
有効	この ACL ルールを適用するには、このチェック ボックスをオンにします。
詳細	このチェックボックスをオンにすると、[スクリプト] フィールドが表示されます。 **重要:** [スクリプト] フィールドにスクリプトがある場合。このスクリプトは、フィールドがフォームに表示されていない場合でも実行されます。
名前	保護されるオブジェクトの名前 (レコード名またはテーブル名とフィールド名) を入力します。名前が具体的であるほど、ACL ルールも具体的になります。レコード、テーブ

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	ル、またはフィールド名の代わりにワイルドカード文字のアスタリスク (*) を使用して、レコードタイプ、すべてのテーブル、またはすべてのフィールドに一致するすべてのオブジェクトを選択できます。ワイルドカード文字とテキスト検索を組み合わせることはできません。たとえば、inc* は有効な ACL ルール名ではありませんが、incident.* および *.number は有効な ACL ルール名です。 **注:** 青い三角形をクリックし、レコード名または保護されるオブジェクトのテーブル名とフィールド名を手動で入力します。ドロップダウンに表示されないオブジェクトを保護するには、このオプションを使用します。
説明	この ACL ルールによって保護されるオブジェクトまたは権限の説明を入力します。
必要なロール	このリストを使用して、ユーザーがオブジェクトにアクセスするために必要なロールを指定します。複数のロールをリストする場合、リストされているロールのいずれかを持つユーザーがオブジェクトにアクセスできます。必要なロールリストが関連リストとして表示されます。 **注:** admin ロールを持つユーザーは、他のすべてのロールが自動的に付与されるため、常にこの権限チェックに合格します。
条件	この条件ビルダー を使用して、ユーザーがこのオブジェクトにアクセスするために true でなければならないフィールドと値を選択します。
スクリプト	オブジェクトにアクセスするために必要な権限を記述するカスタムスクリプトを入力します。スクリプトでは、現在および 前のビジネスルールのグローバル変数 およびシステムプロパティの値を使用できます。スクリプトは、次の 2 つの方法のいずれかで true または false の応答を生成する必要があります。 ○ true または false の値に設定された回答変数を返します。 ○ true または false に評価します。 いずれの場合も、スクリプトが true と評価され、ユーザーが ACL ルールの条件を満たしている場合にのみ、ユーザーはオブジェクトにアクセスできます。ユーザーがオブジェクトにアクセスするには、条件とスクリプトの両方が true と評価される必要があります。 **注:** 評価されたアイテムが関連リストにある場合、現在のポイントは、ACL の現在のアイテムではなく、関連リストがあるアイテムを指します。ただし、ACL を評価しているアイテムが関連リストにない場合、現在のポイントは実際のアイテムを指します。

5. フォームヘッダーを右クリックし、[保存] を選択します。

埋め込みリスト内のレコードを保護する

埋め込みリストのレコードにセキュリティを適用するには、埋め込みリストのレコードの編集と削除を特定のロールに制限します。

始める前に

必要なロール：security_admin

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

手順

1. 移動先 すべて > システムセキュリティ > アクセス制御 **(ACL)**.
2. 該当するテーブルの書き込みまたは削除レコードを開きます。
3. フォームの [必要なロール] セクションで、そのテーブルに対する書き込み権限または削除権限を持つロールを追加します。
4. 変更内容を保存します。
   関連付けられたテーブルのレコードが埋め込みリストに表示されると、指定されたロールを持つユーザーのみが編集および削除のオプションを使用できます。

コンテキスト依存セキュリティマネージャー

コンテキスト依存セキュリティマネージャーは、読み取り、書き込み、作成、および削除の認証を制御することにより、データを保護します。

長所

コンテキスト依存セキュリティマネージャーは、システムテーブル階層を認識しているため、階層内の表示場所に基づいてフィールドに特定のセキュリティルールを作成できます。コンテキスト依存セキュリティマネージャーのメリットは次のとおりです。

- コンテキスト依存セキュリティ：レコードの内容に基づいてレコードを保護します。
- 階層セキュリティ：オブジェクト階層内の任意のレベルにセキュリティルールを適用します。

フィールドとテーブルの保護

従来のシンプルセキュリティマネージャーでは、適切な辞書エントリにロールを追加することで、フィールドとテーブルを保護することができました。コンテキスト依存セキュリティマネージャーでは、これらの辞書ロールはテストされなくなりました。代わりに、フィールドとテーブルで ACL ルールを検索します。

⚠ 警告:
コンテキスト依存セキュリティマネージャーをインストールした後、ACL ルールを使用してフィールドとテーブルを保護する必要があります。フォームレイアウト や辞書フォームを設定して辞書エントリにロールを追加しても、権限は変更されません。

コンテキスト依存セキュリティおよびロール

ユーザーまたはグループにロールを付与できます。ただし、コンテキスト依存セキュリティマネージャーのインストール後、ユーザーレコードの [ロール] フィールドをオンにできなくなり、ユーザーフォームとグループフォームに表示されなくなります。代わりに、ユーザーまたはグループレコードではなく、ロール関連リストにロールを追加する必要があります。

アプリケーションとモジュールには、それらを表示するために必要なロールのリストが含まれています。たとえば、システム定義アプリケーションを表示するには、admin ロールが必要です。アプリケーションとモジュールのセキュリティ権限は、引き続きロールアレイを使用して定義されます。

カタログアイテムとカタログ変数の両方に、それらを表示するために必要なロールのリストが含まれています。カタログアイテムとカタログ変数のセキュリティ権限は、引き続きこれらのロールアレイを使用して定義されます。

コンテキスト依存セキュリティマネージャーでは、ロールの継承フラグが *true* に設定されている場合でも、グループに付与されたロールが自動的に継承されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

コンテキスト依存セキュリティマネージャーの有効化

コンテキスト依存セキュリティマネージャーはベースシステムで有効です。ユーザーロールテーブルに重複するエントリが多数ある場合は、重複するロールを排除するために Contextual Security: Role Management V2 へのアップグレードが必要な場合があります。プラグインは次のとおりです。

Contextual Security: Role Management [com.glide.role_management]

コンテキスト依存セキュリティ機能を提供します。このプラグインは、自動的にインストールされます。

Contextual Security: Role Management V2 [com.glide.role_management.inh_count]

ユーザーロール [sys_user_has_role] テーブルで継承されたロールによるエントリの重複を防ぎます。このプラグインは、新しいインスタンスで自動的にインストールされ、アップグレードに対してアクティブ化することができます。Contextual Security: Role Management 機能拡張プラグインは、このプラグインの以前のバージョンです。ロール管理機能拡張プラグインには、RoleManagementVerify() スクリプトは含まれません。このスクリプトは、アップグレードによって実行される変更のリストを返し、プラグインによる変更を監視できるようにします。

注:
Role Management V2 を有効にした後、 glide.role_management.v2.audit_roles システムプロパティを設定して、監査ロールテーブルがユーザーロールに関連する監査レコードを作成できるようにする必要があります。このプロパティの設定と監査ロールテーブルの詳細については、以下を参照してください。

- Contextual Security: Role Management V2 でのロール監査を有効にする。
- インスタンスセキュリティ強化設定の コンテキスト依存セキュリティ：ロール管理プラグイン。
- 監査ユーザーロール

Contextual Security: Role Management V2 による重複エントリの防止

他のロールから継承されたロールは、ユーザーロールテーブル [sys_user_has_role] の個々のエントリとして追加されるため、1 つのロールでエントリが重複する可能性があります。Contextual Security: Role Management V2 は重複エントリを排除し、今後、重複が生じるのを防ぎます。

継承数による重複エントリを排除する

Contextual Security: Role Management V2 は、継承数 (inh_count) 列を使用して、ロールが別のロールまたはグループから継承された回数を追跡します。ユーザーロール [sys_user_has_role] テーブルでは、ユーザーは特定のロールを 1 回のみ継承できるため、エントリが重複することはありません。継承数 (inh_count) 列は読み取り専用で、ユーザーがロールを継承する回数を計算します。

アクティベーションの変更

Contextual Security: Role Management V2 は新しいインスタンスに自動的にインストールされ、アップグレードに対して有効にすることができます。有効にすると、コンテキスト依存セキュリティと Contextual Security: Role Management 機能拡張の両方が Contextual Security: Role Management V2 に置き換わります。

Contextual Security: Role Management V2 が有効になっている場合、次の列の使用は廃止されますが、下位互換性のためにユーザーロールテーブルに残ります。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

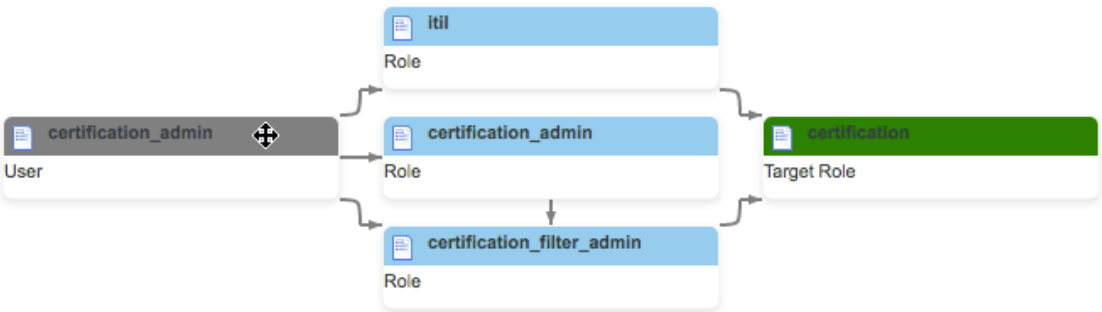
- granted_by (ロールの委任でのみ使用)
- included_in_role
- included_in_role_instance

警告:
これらの列がインスタンスのカスタムスクリプトで使用されている場合は、Role Management V2 にアップグレードしないでください。

ロール継承マップによるロール継承の可視化

ロール継承マップには、継承されたロールが視覚的に表示されます。このマップを使用して、継承数 (inh_count) 列に表示されるロールを理解することができます。ロール継承マップを表示するには、ユーザーロール [sys_user_has_role] テーブルを設定してロール継承マップ列を表示します。

ロール継承マップ



Contextual Security: Role Management V2 へのアップグレード

Contextual Security: Role Management V2 は新しいインスタンスに自動的にインストールされます。Contextual Security: Role Management から Contextual Security: Role Management V2 にアップグレードして、ユーザーロールテーブル内の重複するロールを排除し、今後、重複が起こらないように防ぐことができます。

始める前に

必要なロール：admin、security_admin
有効な security_admin ロールを取得するには、admin ロールと 特権ロールへの昇格 が必要です。

注:
Contextual Security: Role: Management V2 にアップグレードする前に、監査ロールテーブルを有効にして、ユーザーロールに関連する監査レコードを作成する必要があります。必要なシステムプロパティの設定の詳細については、「Contextual Security: Role Management V2 でのロール監査を有効にする」を参照してください。

このタスクについて

この手順では、コンテキスト依存セキュリティロールのアップグレード方法と、次の表で説明されている関連プラグインを有効にする方法について説明します。

Contextual Security: Role Management V2 のプラグイン

プラグイン	説明
Contextual Security: Role Management V2	ユーザーロール [sys_ user_has_role] テーブルでエントリが重複しないようにします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Contextual Security: Role Management V2 のプラグイン (続く)

プラグイン	説明
[com.glide.role_management.inh_count]	security_admin ロールまたは昇格した権限を持つユーザーは、プラグインを有効にするか、カスタマーサービス & サポート に連絡する必要があります。
Contextual Security: Role Management V2 REST API [com.glide.role_management.inh_count.rest_api]	ロール管理の API 機能を有効にします。

Contextual Security: Role Management から Contextual Security: Role Management V2 にアップグレードする前に、スクリプトを実行してアップグレードの結果をテストします。このスクリプトは、アップグレードによって実行される変更のリストを返します。変更を受け入れる場合は、Contextual Security: Role Management V2 プラグインをインストールします。変更を受け入れられない場合は、Contextual Security: Role Management V2 プラグインをインストールしないでください。または、アップグレードを実行してから、必要な変更を手動で行うこともできます。

手順

1. アップグレードの前に次のスクリプトを実行して、アップグレードの影響をテストします。

a. 移動先 システム定義 > スクリプト - バックグラウンド.

b. グローバルスコープで次のスクリプトを実行します。

```
new RoleManagementVerify().verifyInheritedRoles();
```

大きな sys_user_has_role テーブルの場合、実行が完了するまでに数時間かかることがあります。実行中にユーザーロールを編集したり、追加したりしないでください。
テストデータに基づく結果の例：

```
*** Script: 2016-12-01 19:58:54 Starting checking of inherited roles for all users...
*** Script: User: itam, inherited roles to be ADDED: financial_mgmt_user
*** Script: User: bernard.laboy, inherited roles to be DELETED:
 api_analytics_read,pa_viewer,rest_api_explorer,a123
*** Script: User: bernard.laboy, inherited roles to be ADDED: dependency_views
*** Script: Number of inherited-role records in sys_user_has role, current: 260, after
 re-calculation: 258
*** Script: Number of users with discrepancies for inherited roles: 2
*** Script: 2016-12-01 19:58:55 Finished checking of inherited roles for all users!
```

c. スクリプトの結果を評価して、提案された変更を受け入れられるかどうか判断します。

2. Contextual Security: Role Management V2 プラグインをアクティブ化します。

> **重要:**
> security_admin ロールまたは昇格した権限を持つユーザーは、プラグインを有効にするか、カスタマーサービス & サポート に連絡する必要があります。

a. 移動先 システム定義 > プラグイン.

b. プラグイン名を見つけてクリックします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

c. [システムプラグイン] フォームでプラグインの詳細を確認し、[有効化/アップグレード] 関連リンクをクリックします。

d. [アクティブ化] をクリックします。

タスクの結果
Role Management V2 を有効にすると、スクリプトの結果に示されている変更が有効になります。ユーザーロールテーブルの継承数 (inh_count) 列は読み取り専用で、ユーザーがロールを継承した回数を自動的に反映します。

Contextual Security: Role Management V2 でのロール監査を有効にする

システムプロパティを設定して、監査ロールテーブルでユーザーロールに関連する監査レコードを作成できるようにします。

始める前に
必要なロール：管理者

このタスクについて
有効にすると、監査ロール [sys_audit_role] テーブルでユーザーレコードへの変更が保持されます。ロールの監査の詳細については、「監査ユーザーロール」を参照してください。Contextual Security: Role Management V2 [com.glide.role_management.inh_count] プラグインがインストールされている場合は、システムプロパティを **true** に設定してロール監査を有効にする必要があります。

手順

1. システムプロパティ [sys_properties] テーブルに移動します。
2. *glide.role_management.v2.audit_roles* システムプロパティを追加し、**true** に設定します。

   Contextual Security: Role Management V2 [com.glide.role_management.inh_count] プラグインがインストールされている場合、このプロパティを **true** に設定すると、ユーザーロールを変更するときに監査ロール [sys_audit_role] テーブルを有効化して、レコードを作成することができます。

フォーム送信の再確認

現在のユーザーが特定のフィールド (task.number など) に書き込むべきではないとシステムで判断されると、そのフィールドは読み取り専用モードで表示されます。ほとんどのインシデントで番号フィールドに書き込みができないのはそのためです。

受信フィールドの値を書き込めるかどうか再確認するように設定すると、トランザクションの受信レグに同じ一連のセキュリティルールが適用されます。たとえば、インシデントを送信すると、変更を投稿する前に番号フィールドへの書き込みが可能かどうか再確認します。

受信トランザクションを再確認しないように指示すると、クライアントが送り返すトランザクションであれば、名目上の読み取り専用フィールドへの書き込みが許可されます。多くの展開でこれは望ましい動作です。たとえば、クライアントスクリプトを使用して、他の書き込み可能なフィールドでのユーザーの選択に応じて、名目上の読み取り専用フィールドを設定している場合などが該当します。

デフォルトの拒否プロパティ

デフォルトの拒否プロパティ (glide.sm.default_mode) は、一致する ACL ルールがワイルドカードテーブル ACL ルールのみの場合に、セキュリティマネージャーのデフォルトの動作を制御します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

最も一般的なレコードベースの操作 (読み取り、書き込み、作成、および削除) 用の一連のワイルドカードテーブル ACL ルール。システムテーブルへのロールベースでのアクセスを提供する ACL も多数用意されています。たとえば、business_rule_admin ロールに sys_script アクセス権を付与する ACL があります。このロールはビジネスルールを管理できると文書化されています。

glide.sm.default_mode プロパティを使用して、すべてのテーブルでこれらの操作を拒否または許可します。

- アクセスを拒否：ワイルドカードテーブル ACL ルールは、ユーザーが admin ロールを所有しているか、別のテーブル ACL ルールの要件を満たしている場合を除き、読み込み、書き込み、作成、削除の操作をすべてのテーブルで制限します。report_on や personalize_choices などの他の操作は、この設定の影響を受けません。
- アクセスを許可：ワイルドカードテーブル ACL ルールは、そのような操作を制限する特定のテーブル ACL ルールが存在する場合を除き、読み込み、書き込み、作成、および削除の操作をすべてのテーブルで許可します。

[アクセスを拒否 **(Deny Access)]** に設定すると、glide.sm.default_mode を [アクセスを許可 **(Allow Access)]** にリセットすることはできません。

注:
デフォルトでは、ワイルドカードテーブル ACL ルールのみが glide.sm.default_mode プロパティの値をチェックする ACL ルールです。この設定で他の操作を制御する場合は、独自の ACL ルールを作成してこのプロパティ値をチェックします。

このプロパティの詳細については、「インスタンスセキュリティ強化設定」の「デフォルトの拒否」を参照してください。

ACL の詳細設定

新しい ACL の作成や既存の ACL の変更に加えて、ACL 機能の他の側面を設定できます。

タスク	説明
ACL スクリプト条件を参照フィールドに適用する	参照フィールドがフォームまたはリストに表示するデータへのアクセスを制御する場合は、プロパティを有効にしてスクリプト条件を許可し、参照フィールドに適用します。プロパティを有効にすると、インスタンスのパフォーマンスに影響を与える可能性があります。
ACL を AJAXGlideRecord (クライアント側の Glide レコード) に追加	現在接続しているユーザーがアクセス権を持つデータのみを照会するように、`GlideAjax` API 呼び出しに ACL を適用します。
アクセスレベルで管理者優先を評価する	アクセスレベルで管理者の ACL 評価を強制します。デフォルトでは、管理者優先オプションが ACL ルールフォームで選択されている場合、admin ロールのユーザーはこの ACL ルールの権限確認に自動的に合格します。
ACL のデバッグツールとトラブルシューティングツールを使用する	ACL 監視、フィールドレベルのデバッグ、アクセス ACL ルール出力メッセージなどのツールを使用すると、ACL のトラブルシューティングとデバッグに役立ちます。

外部ユーザーへのテーブルアクセス権の提供

snc_external ロールのみを持つユーザーがテーブルのリストビューにアクセスできるようにするには、一連の ACL を作成する必要があります。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

始める前に
必要なロール：security_admin

手順

1. 特権ロールへの昇格。
2. 次の設定を使用して、ACL ルールを作成します。
   - タイプ：ui_page
   - 操作：読み取り
   - 名前：{table_name}_list
   - 必要なロール：snc_external
3. テーブルのデフォルトの読み取り ACL で、[必要なロール] リストに **snc_external** を追加します。
   ACL がまだない場合には作成します。
4. これらの設定を使用して、別の ACL を作成します。
   - タイプ：ui_page
   - 操作：読み取り
   - 名前：{table_name}
   - 必要なロール：snc_external
5. これらの設定を使用して、ユーザーにテーブル内のフィールドへの書き込みアクセス権を付与する別の ACL を作成します。
   - タイプ：レコード
   - 操作：作成
   - 名前：{table_name} {column_name}
   - 必要なロール：snc_external

   ユーザーに書き込みアクセス権を付与するすべてのフィールドに対して、この手順を繰り返します。列名の代わりにアスタリスク (*) を使用すると、すべてのフィールドへのアクセスを一度に提供できます。

ACL スクリプト条件を参照フィールドに適用する

glide.sys_reference_row_check システムプロパティを使用して、参照フィールドのスクリプト化された条件を有効にします。

デフォルトの動作は、インスタンスのパフォーマンスを向上させることを目的としています。参照フィールドのスクリプト条件を有効にするには、次のシステムプロパティを追加します。

注:
システムプロパティの作成の詳細については、「Add a system property」を参照してください。

システムプロパティ

プロパティ	説明
glide.sys_reference_row_check	アクセス制御ルールのスクリプト条件がテーブルの [参照] フィールドに適用されるかどうかをコントロールします。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

システムプロパティ (続く)

プロパティ	説明
	• タイプ：true | false • デフォルト値：**false** • 場所：システムプロパティ [sys_properties] テーブルにシステムプロパティを追加 します。

注:
glide.sys_reference_row_check システムプロパティが存在しない場合、または false に設定されている場合、アクセス制御ルールのスクリプト条件は適用されません。これは、他の ACL 基準 (ロール要件など) が満たされている限り、スクリプト化された条件を含む ACL がチェックに合格することを意味します。

ACL を AJAXGlideRecord (クライアント側の Glide レコード) に追加

クライアントスクリプト内で GlideAjax API を使用してサーバー側のレコード (テーブルなど) にアクセスする場合、システムプロパティを使用してアクセス制御リスト (ACL) ルール検証を実行します。

アクセス制御リスト (ACL) を *GlideAjax* API 呼び出しに適用することを選択すると、現在接続しているユーザーがアクセス権限を持つデータのみを照会できます。たとえば、ユーザーが cmn_location テーブルを読み込む権限のない ESS ユーザーとしてログインすると、*GlideAjax* API 呼び出しは失敗します。

GlideAjax 呼び出しで ACL をチェックせずにシステムを実行すると、API は現在ログインしているユーザーが UI を介してアクセスできなかった情報を返します。

注:
このプロパティの設定 システムプロパティ > **Security** (セキュリティ).

注:

このプロパティの詳細については、「インスタンスセキュリティ強化設定」の「AJAXGlideRecord ACL チェックの有効化」を参照してください。

アクセスレベルで管理者優先を評価する

アクセスレベルで管理者優先の ACL 評価を強制する場合は、システムプロパティを追加できます。

始める前に
必要なロール：security_admin

このタスクについて
ACL は累積的に評価されます。指定されたフィールドに多数の ACL があり、そのうちの 1 つで管理者優先オプションが **false** (未選択) の場合、すべての ACL の有効な管理者優先は **false**と見なされます。これにより管理者は優先を有効にする必要がある ACL を渡すことができなくなります。

手順

システムプロパティテーブルに次のプロパティを追加します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

プロパティ	説明
glide.security.admin.override.accessterm	アクセス期間レベルで管理者優先条件を評価します。 • タイプ：true | false • デフォルト値：新しいインスタンスの場合は **true**、アップグレードされたインスタンスの場合は **false** • 場所：システムプロパティ *[sys_properties]* テーブルに追加 **注:** インスタンスでプロパティが定義されていない場合、値は false と評価されます。

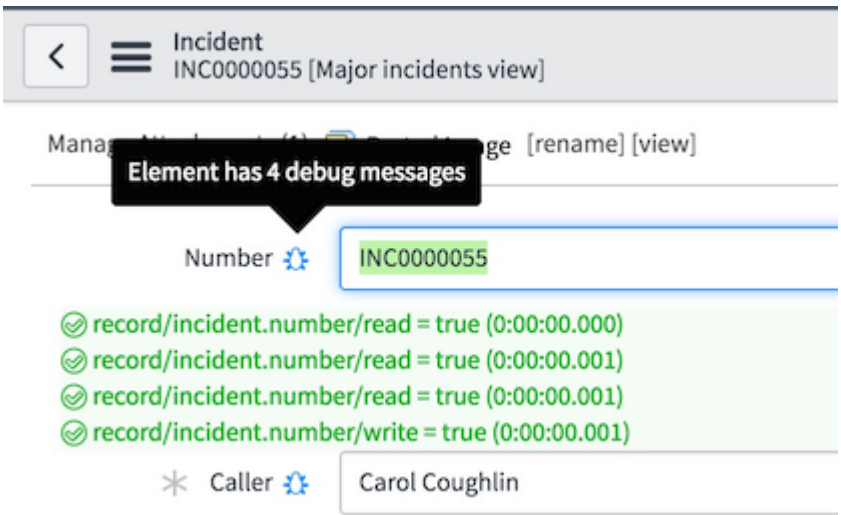
ACL デバッグツール

ACL のトラブルシューティングとデバッグに役立つ、フィールドレベルデバッグおよびアクセス ACL ルール出力メッセージを使用できます。ACL 構成監視を使用すると、変更時にどのような関連する ACL が存在するかがわかります。

フィールドレベルのデバッグ

デバッグを有効にすると、各フィールドの横に小さなバグアイコン ( ) が ACL ルールと一緒に表示されます。アイコンをクリックすると、フィールドに適用される ACL ルールと評価結果が一覧表示されます。次に移動してデバッグを有効にする: システムセキュリティ > デバッグ > セキュリティルールのデバッグ.

インシデントのフィールドレベルのセキュリティ



ACL デバッグを有効にした後、別のユーザーとして操作を行い、ユーザーが合格または不合格になった ACL ルールを確認することができます。ユーザーの代理操作を行うと、そのユーザーに表示が許可されているもののみが表示されます。たとえば、ACL が非表示にしているレコードを表示することはできません。デバッグを容易にするために、特定の ACL 関連テーブルへの読み取り専用アクセスは、テーブルへの読み取りアクセス権を持たないユーザーの代理操作を行う場合でも、デフォルトで有効になっています。この機能を変更するには、次のプロパティを **false** に設定します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ACL ルールのデバッグを有効にするには、次に移動します。 システムセキュリティ > セキュリティルールのデバッグ.

システムプロパティ	説明	デフォルト設定
glide.security.access_acl_as_impersonated	ユーザの代理操作中に、sys_security_acl テーブル、sys_security_operation テーブル、sys_security_type テーブル、および sys_user_role テーブルへの読み取りアクセスを許可します。その結果、代理操作をしているユーザーは、代理操作されたユーザーが読み取ることができないデータを読み取ることができます。	true **注:** プロパティが false に設定されている場合、代理操作されたユーザーは ACL 関連のデータを読み取れない可能性があります。この場合、ACL をデバッグするには、admin または security_admin としてログインする 2 番目のセッションが必要となる可能性があります。

ACL ルール出力メッセージ

ACL デバッグでは、各リストとフォームの下部に ACL ルールの出力メッセージが表示されます。出力メッセージには以下が表示されます。

メッセージ要素	説明
TIME	この ACL ルールの処理に要した合計時間。
パス	<ACL ルールタイプ>/<ACL ルール名> /<操作> の形式で各 ACL ルールを一意に識別する情報。
コンテキスト	ACL ルールで評価されるオブジェクト。
RC	ACL ルールのリターンコード。true の値は、ACL ルールを満たしています。false の値は、ACL ルールを満たしていません。
ルール	プロセッサーとスクリプトの簡単な概要と、それに続く各テーブルレベルとフィールドレベルの ACL 評価の ACL 結果。ほとんどの ACL 評価では、総合的な合格または不合格の結果の後に、ACL 基準のタイプごとに結果のブレークダウンが表示されます。 • iAccessHandler：プラットフォーム上の非表示のソースコードを使用する内部システムチェック。これは変更できないシステムセキュリティチェックです。IAccessHandler は、ACL を評価せずにリソースへのアクセスを許可または拒否できます。IAccessHandler が無視されると、ACL が評価されます。どのような方法でも IAccessHandler チェックは変更できません。たとえば、IAccessHandler 実装はアプリケーションリソースのアクセスチェックに使用され、これは変更できません。 このメソッドは Istanbul 以降のリリースで利用できます。 • ロール：ユーザーが正しいロールを持っていることの検証。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

メッセージ要素	説明
	• 条件：ユーザーが ACL ルールで指定された条件 (存在する場合) を満たしていることの検証。 • スクリプト：ユーザーが ACL ルール (存在する場合) で指定されたスクリプトを満たしていることの検証。

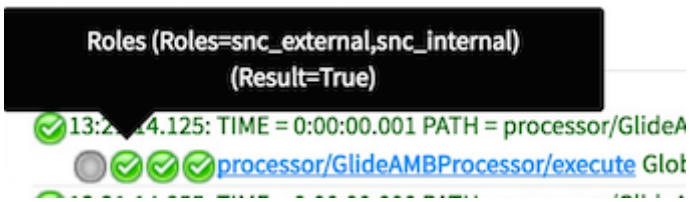
表示されるアイコンは、ACL がどのように評価されたかを示します。

アイコン	説明
緑色のチェックマーク ( )	基準を満たしているテーブルまたはフィールドを示します。
赤色の x アイコン ( )	テーブルまたはフィールドが基準を満たしていないことを示します。
空の灰色の円アイコン ( )	ACL 評価を実行する必要がなかったことを示します。
青色のチェックマーク、x、または空の円	ACL が以前の ACL チェックのキャッシュ結果から取得されたことを示します。アイコンの意味は上記と同じです。

ACL デバッグ出力では、次のアクションを実行できます。

- デバッグ出力の上部にあるチェックボックスをオンまたはオフにします。
  - セキュリティルール：ACL チェックの結果を表示または非表示にします。
  - その他：その他の警告またはメッセージを表示または非表示にします。
- 出力メッセージの横にある ACL の名前をクリックして、その ACL レコードを開きます。

- 4 つの ACL チェックのいずれかのアイコンにカーソルを合わせると、詳細が表示されます。



ACL トラブルシューティングリファレンス

一般的な ACL ルールのエラーとそのソリューションのリスト。

問題のトラブルシューティングに役立つデバッグを有効にします。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

トラブルシューティング

エラーまたは症状	解決策
カスタムテーブルからレコードにアクセスすることはできません。	カスタムテーブルのテーブル ACL ルールを作成し、ユーザーにテーブルへのアクセスを許可します。明示的なテーブル ACL ルールがない場合、ユーザーはテーブルワイルドカード (*) ACL ルールの権限を渡す必要があります。これにより、デフォルトでは管理者のみにアクセスが制限されます。デバッグを有効にし、カスタムテーブルに対して評価する ACL ルールを決定します。
正しく機能しないカスタム ACL ルールを作成します。	最も可能性の高い問題は、処理順序でカスタムルールより別のルールが優先されるか、ユーザーがオブジェクトタイプのすべての権限要件を満たしていないといった問題です。デバッグを有効にし、ACL ルールが評価されていることを確認します。
フィールドの ACL ルールが正しく機能しません。	ユーザーが満たしていないテーブル ACL ルールが存在する可能性があります。デバッグを有効化し、どの ACL ルールをフィールドに対して評価するかを決定します。競合するテーブル ACL ルールまたは重複フィールド ACL ルールがないことを確認します。
テーブル ACL ルールが正常に機能していません。	処理順序の上位にある ACL ルール、またはテーブル ACL ルールを妨げる重複テーブル ACL ルールがあります。デバッグを有効にして、どの ACL をテーブルに対して評価するかを決定します。
リスト内のフィールドは表示できますが、フォームには表示できません。	ACL ルール条件またはスクリプトがリスト内でトリガーされていても、フォームではトリガーされていない可能性があります。デバッグを有効にして、ACL ルールが true と評価されるタイミングを決定します。リストとフォームで同じ動作になるように条件またはスクリプトを更新します。
プロセッサーまたはクライアント呼び出し可能スクリプトインクルードを実行しようとすると、エラーメッセージが表示されます。	ユーザーが満たしていないプロセッサーまたはクライアント呼び出し可能スクリプトインクルードの ACL ルールがあります。ユーザーがオブジェクトにアクセスできる必要がある場合は、デバッグを有効にして、プロセッサーまたはスクリプトインクルードに対して評価される ACL ルールを決定します。オブジェクトにアクセスするために、必要に応じて ACL ルールまたはユーザーロールを更新します。

ACL 構成監視

ACL 構成監視を使用すると、同じテーブルで ACL を挿入、更新、または削除するときに、テーブルにどのような関連する ACL が存在するかがわかります。

ACL 構成監視は、アクセス制御 [sys_security_acl] テーブルに重要な変更を加えるたびに表示されるインターセプターウィンドウです。変更している ACL に関連する ACL を表示できるセキュリティルールのサマリーウィンドウが表示されます。セキュリティルールのウィンドウから ACL を変更することはできません。変更を加えるには、監視ウィンドウを閉じて、ACL に移動します。

次の状況では、ACL 構成監視は表示されません。

- 実際に変更を加えずに ACL レコードを保存または更新した場合。
- スクリプト、条件、管理者優先オプションなどの (挿入や削除ではなく) マイナーな更新を行う場合。
- ACL レコードがアクティブではない場合。

ACL セキュリティルールウィンドウ

構成監視では ACL 実行計画が表示されます。実行計画はセキュリティルールのポップアップウィンドウに表示されます。次のような情報を表示できます。

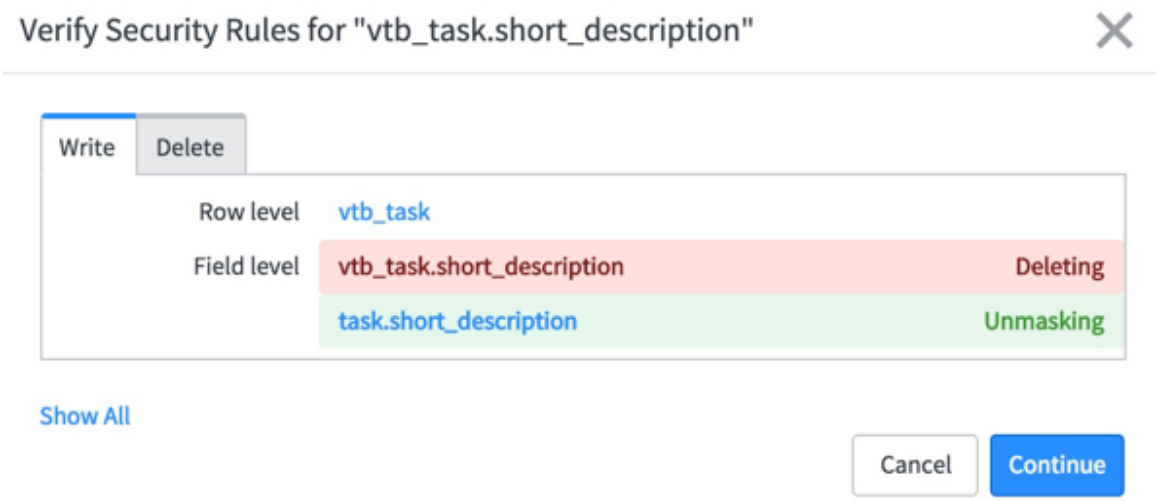
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

ACL 構成ウィンドウの要素

アイテム	説明
赤のハイライト	削除または非アクティブ化された ACL。
青のハイライト	変更された ACL。
緑のハイライト	追加された、またはアクティブになった ACL。
マスク済み	変更を加えるまで有効であった ACL。
マスク解除	変更を加えたときに有効だった ACL。

構成監視の例



自動翻訳

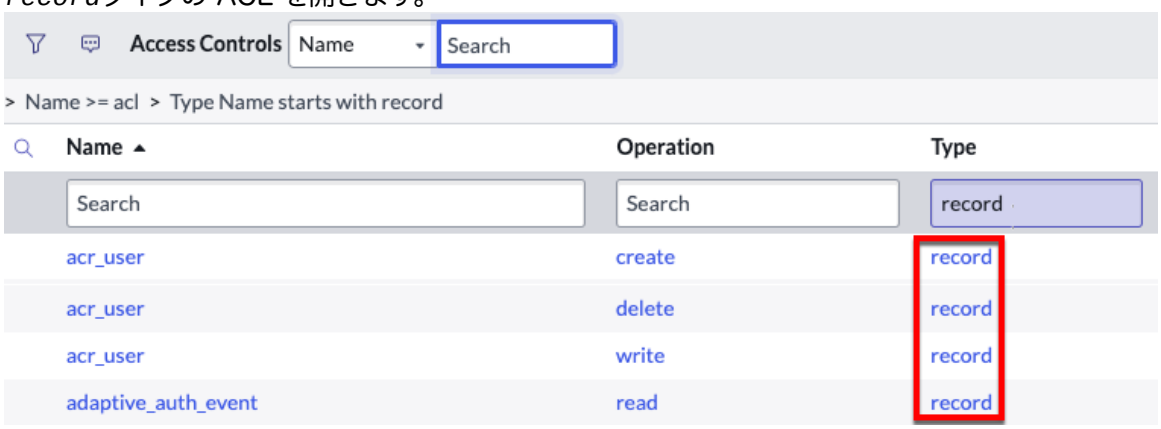
ACL 実行計画を表示する

管理者は、インスタンス内の ACL の実行計画を表示することで、ACL の相互関係を確認できます。

始める前に
必要なロール：security_admin

手順

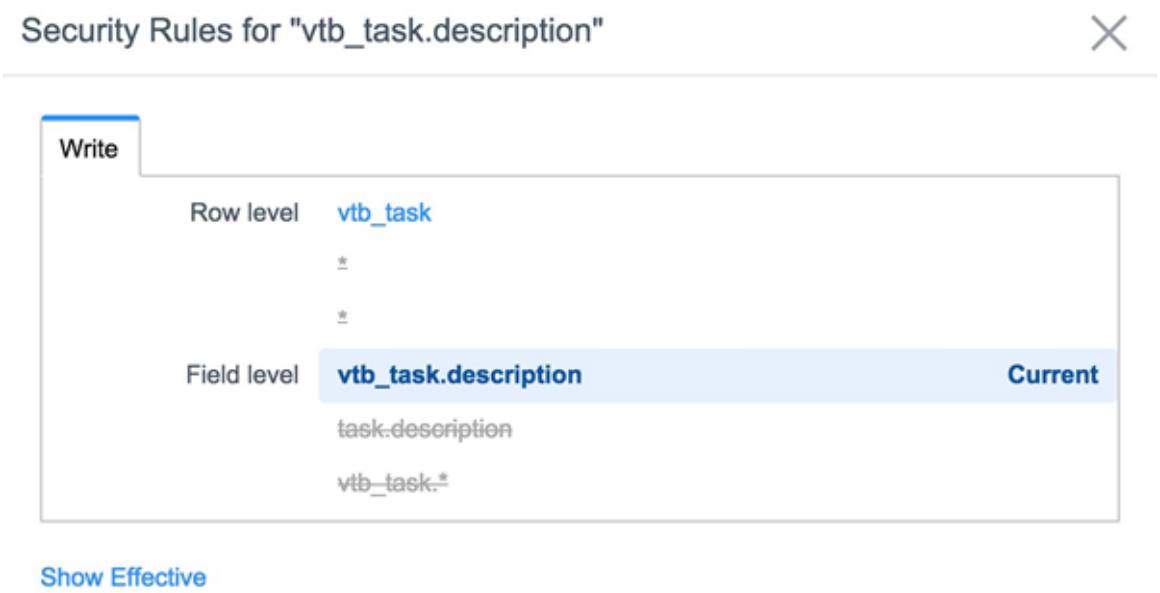
1. 特権ロールへの昇格.
2. 移動先 システムセキュリティ > アクセス制御 **(ACL)**.
3. *record*タイプの ACL を開きます。



© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

4. [関連リンク] セクションで **[ACL** 実行計画を表示] をクリックします。

   ACL のセキュリティルールウィンドウが表示されます。この例では、「vtb_task」の実行計画が表示されます。



ACL 実行計画ウィンドウ

UI アイテム	説明
タイトル	ACL の名前。
タブ名	ACL が作成、読み取り、書き込み、または削除の場合。
行レベル	このテーブルで実行される行レベルの ACL。
フィールドレベル	このフィールド (またはテーブル内の列) でのみ実行されるフィールドレベルの ACL。

5. [すべて表示] をクリックすると、上書きされる ACL やすべてのレコードに適用される汎用 ACL を含む、関連するすべての ACL が表示されます。
   上書きされる ACL の名前には線が引かれています。汎用 ACL の名前にはワイルドカード文字のアスタリスク (*) が付いています。
6. [有効な **ACL** を表示 **(Show Effective)]** をクリックして、表示している ACL に関連する直接の ACL のみを表示し、ACL テーブルの拡張元のテーブルの ACL と汎用ワイルドカード (*) ACL を非表示にします。

ACL 構成監視を使用する

security_admin ロールに昇格した後、ACL 構成監視を使用します。

始める前に
必要なロール：security_admin
特権ロールへの昇格

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

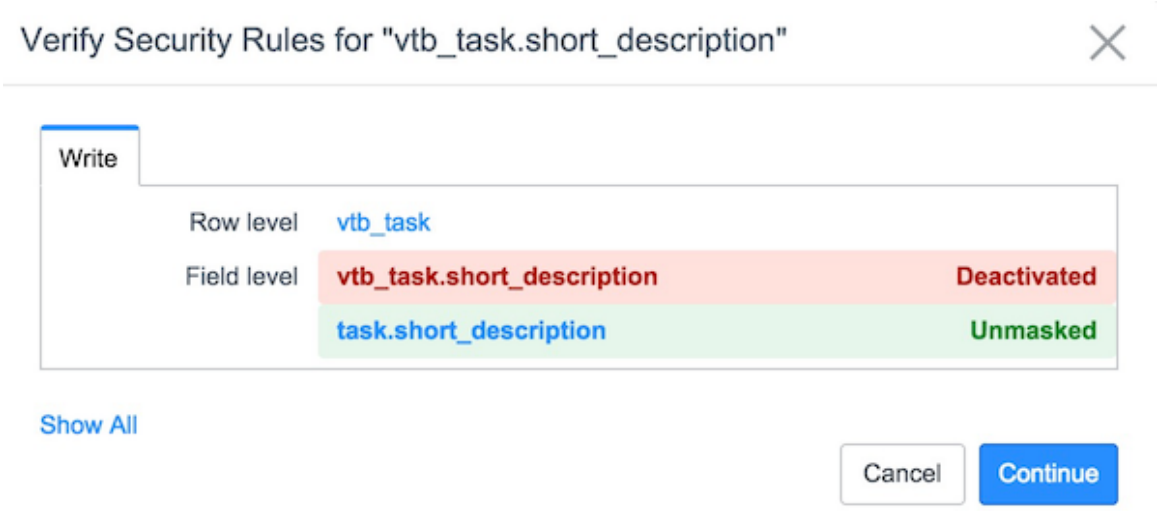
1. レコードタイプの ACL を開きます。
2. 変更や、[挿入] などのコンテキストメニューからのオプション選択など、ACL に対してアクションを実行します。
3. アクセス制御フォームで値を変更した場合は、ヘッダーを右クリックして [保存] を選択するか、[更新] または [削除] をクリックします。

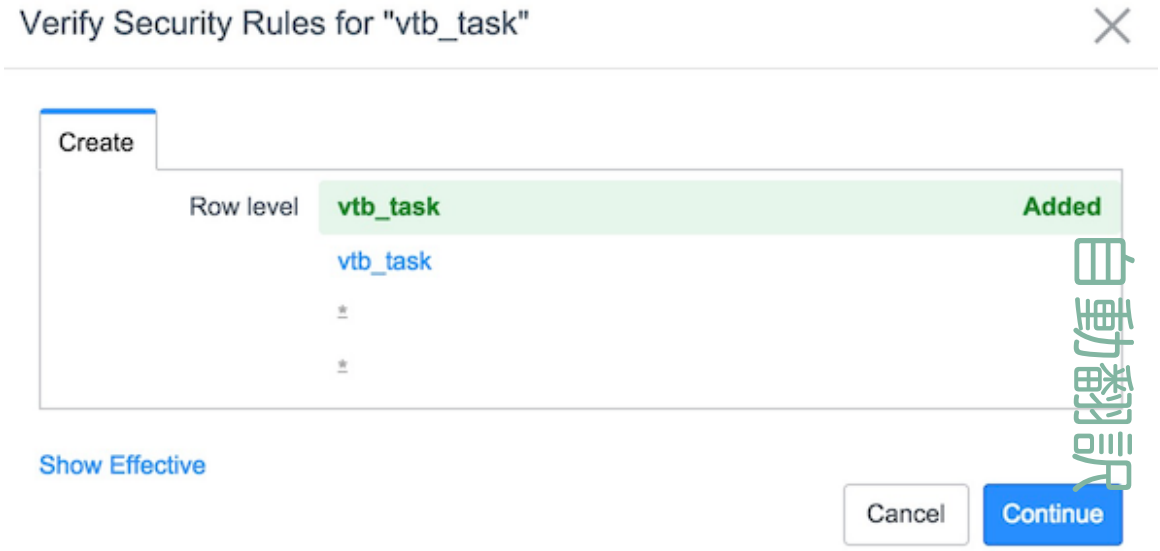
   [セキュリティルール] ウィンドウが表示されます。ACL でデータベースアクションがまだ実行されていないため、変更はまだ保存されていません。

   以下は、Visual Task Boards アプリケーションのプライベートタスク [vtb_task] テーブルのセキュリティルールの例です。このウィンドウのアイテムの説明については、「ACL 構成監視」を参照してください。

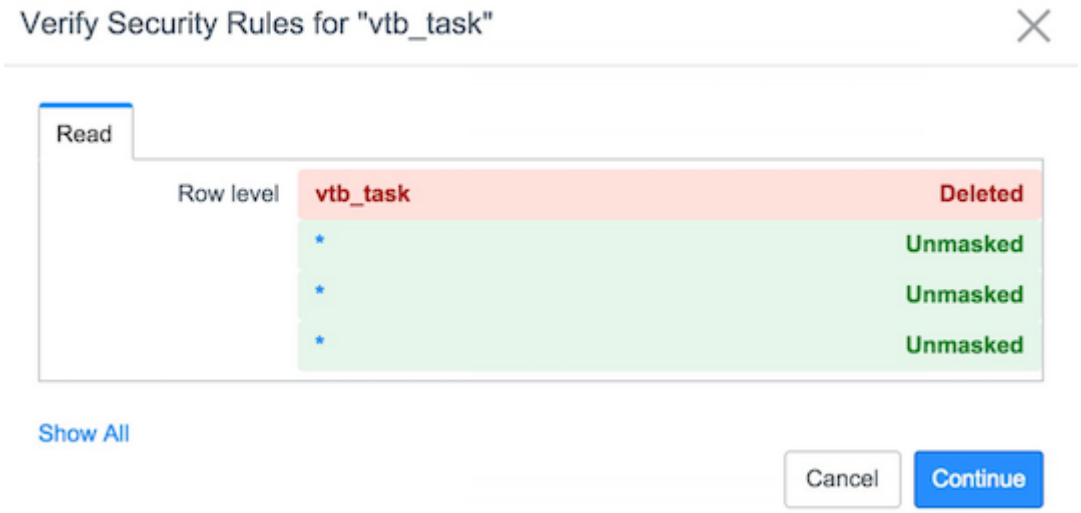
自動翻訳

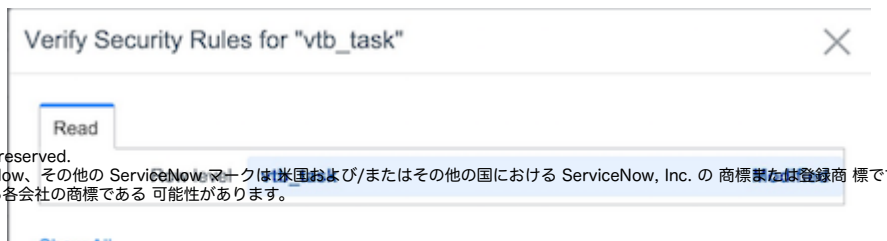
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。





自動翻訳





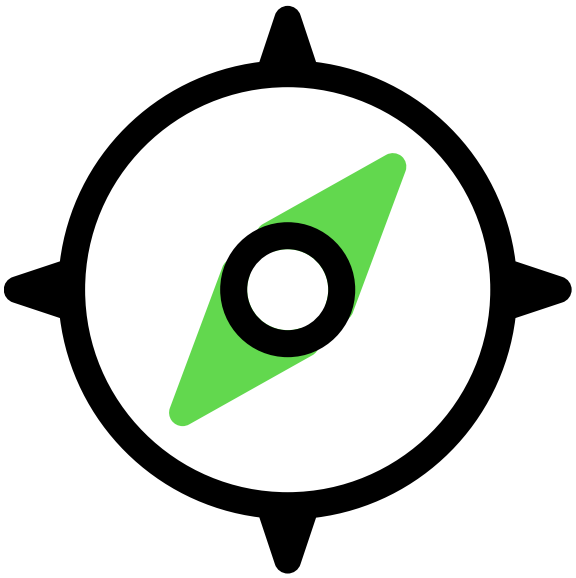
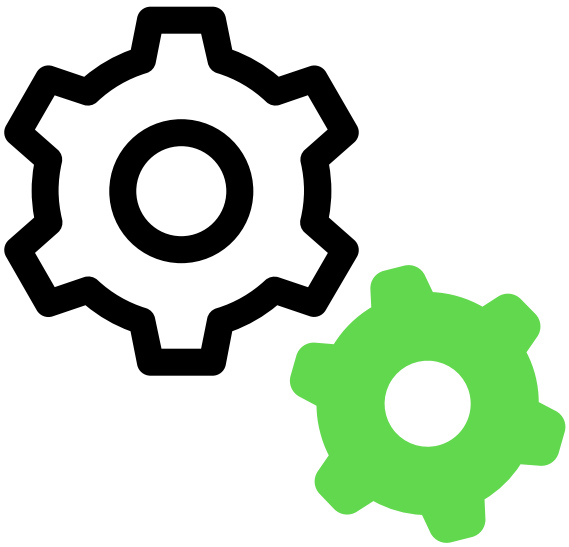
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

4. 実行計画の場合と同様に、[すべて表示] をクリックすると、上書きされたものやすべてのレコードに適用される汎用 ACL を含むすべての関連する ACL が表示されます。[有効な **ACL** を表示 **(Show Effective)]** をクリックすると、表示している ACL に関連する直接の ACL のみが表示されます。
5. いずれかの ACL にカーソルを合わせると、説明が表示されます。

セキュリティ属性ホームページ

セキュリティ属性は、アクセス制御リストの柔軟な代替手段を提供します。

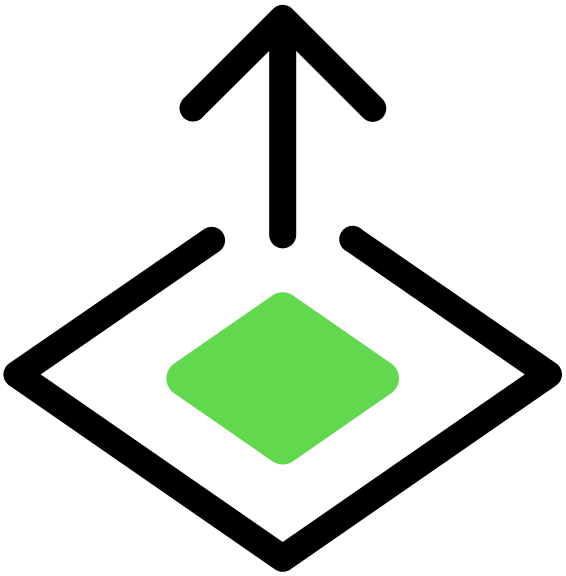
開始するには

セキュリティ属性の詳細	セキュリティ属性を作成
	
セキュリティ属性の基礎を学ぶ	新しいセキュリティ属性を作成

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

OOB (Out-of-Box) セキュリティ属性



OOB セキュリティ属性の説明

セキュリティ属性のログ記録

セキュリティ属性ログ記録の確認

セキュリティ属性の基礎

セキュリティ属性は、サブジェクトまたはその環境に関する高度に構成可能な情報であり、アクセス制御で使用されると、複雑ではない方法できめ細かなセキュリティ構成が可能になります。

概要

セキュリティ属性は、現在使用されている ACL (アクセス制御リスト) 構成に対するロール定義を介したアクセス制御の代替手段を提供します。セキュリティ属性には、ACL ベースの設定にいくつかの利点があります。

セキュリティの向上
: アクセス許可の評価の難読化の改善により、組織のセキュリティが確保されます。

人間が判読可能
: セキュリティ属性は、セキュリティ アクセス許可の作成と使いやすさを簡素化するように設計されています。

柔軟なセキュリティ
: 顧客定義のペルソナと組み合わせて、すぐに使える構成の両方からペルソナ定義を構築します。

ログ記録と監査
: セキュリティ属性は、詳細な監査とログ記録を提供し、セキュリティ対策と理論に関するより多くの洞察を提供します。

セキュリティ属性を作成

ステップバイステップガイドを使用して、新しいセキュリティ属性を作成します。

始める前に
必要なロール：security_admin

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. 移動先 システム セキュリティ > セキュリティ属性.
2. [セキュリティ属性] リストで、[新規] を選択します。
3. [セキュリティ属性フィールド] フォームで、各フィールドに入力します。

セキュリティ属性フィールド

フィールド	説明
ラベル	セキュリティ属性のラベル。
名前	セキュリティ属性の名前。
タイプ	セキュリティ属性のタイプ。 ○ 複合 **注:** 複合セキュリティ属性の詳細については、以下を参照してください。 複合セキュリティ属性 ○ 整数 ○ list ○ 文字列 ○ ブーリアン(true|false)
動的 (Is dynamic)	それぞれでセキュリティ属性値を再評価する必要がある場合
説明	セキュリティ属性のユーザー生成の説明
アプリケーション	静的フィールド、アプリケーションスコープ。
ルックアップ テーブル	評価のために外部テーブルを参照します。
ルックアップテーブル列	評価のためにテーブル列を参照します。
スクリプト	スクリプトから値を導出

OOB (Out-of-Box) セキュリティ属性

一般的に使用され、一般化されたセキュリティ属性ロールをすぐに使用できます。

概要

OOB (Out-of-Box) セキュリティ属性は、一連の事前設定されたセキュリティ属性ロールを使用して、セキュリティ属性の機能の使用と学習を開始する簡単な方法です。OOB セキュリティ属性ロールは、一般的に使用されるアクセス制御ロールです。

独自のセキュリティ属性を作成するか、OOB セキュリティ属性機能を展開するには、以下を参照してください。 複合セキュリティ属性

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

OOB セキュリティ属性

属性	説明
グループ	ユーザーは指定されたグループのメンバーです
GroupExplicit	ユーザーが特定のグループの明示的なメンバーである
hasAdminRole	ユーザーに管理者ペルソナがある
代理操作ユーザー	ユーザーの代理操作
InteractiveSession	現在のセッション インタラクティブ
Loggedin	ユーザーはログインして認証されています
ネットワーククライテリア	追加のネットワーク基準
ロール	ユーザーに特定のロールがある
明示的ロール	ユーザーに特定のロールが明示的に定義されている

非明示的および明示的な動作の説明

セキュリティ属性は、ロール権限の明示的な評価と明示的でない (継承された) 評価により、微妙な権限のニーズに対応します。

[qa: BEGIN review]

Example: IT ペルソナアクセスを **HR** ロールファイルアクセスから分離する
ここでは、管理者が人事関連ファイルを表示できるようにするが、管理者ファイルへのアクセスは許可しないセキュリティ属性を定義します。admin ロールは人事グループの一部として定義されておらず、 _____であるとします。ロールは_____[End]

複合セキュリティ属性

複合セキュリティ属性を使用すると、ビジネスニーズに合った一貫性のある再利用可能なセキュリティ属性プロファイルを作成できます

概要

複合セキュリティ属性は、1 つ以上の既存のセキュリティ属性から定義され、アクセス許可評価用のセキュリティ属性の単一の参照の組み合わせを作成します。

[qa: BEGIN review]

複合セキュリティ属性の動作

[End]

複合セキュリティ属性の作成

簡単に再利用できるように複合セキュリティ属性を作成します。

始める前に
必要なロール：security_admin

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. 移動先 システムセキュリティ > セキュリティ属性.
2. [セキュリティ属性] リストで、[新規] を選択します。
3. [タイプ] フィールドで [複合] を選択します。
4. [セキュリティ属性フィールド] フォームで、各フィールドに入力します。

セキュリティ属性フィールド

フィールド	説明
ラベル	セキュリティ属性のラベル。
名前	セキュリティ属性の名前。
説明	セキュリティ属性のユーザー生成の説明
条件	セキュリティ属性評価を定義するために使用される特定のセキュリティ属性条件。
新しい条件	評価用に **OR** 条件のセットを追加します。

セキュリティ属性 スコープ

セキュリティ属性は、スコーピング機能をサポートしています。

セキュリティ属性スコーピング

セキュリティ属性のスコープ動作は、プラットフォームのスコープ動作と一致しています。スコープ内で作成されたセキュリティ属性は、同じスコープ内のアクセス制御でのみ使用できます。

ローカルおよび既存のセキュリティ属性

既存およびローカルのセキュリティ属性を使用すると、顧客はセキュリティ属性の条件セットを再利用できます。

ローカル属性と既存属性

ACL セキュリティ属性条件ビルダーを使用すると、セキュリティ属性が既存かローカルかを指定できます。

注:
セキュリティ属性条件のデフォルトはローカルです。

ローカルに定義されたセキュリティ属性は、それが作成された単一の ACL にのみ保存されます。

既存のオプションを使用すると、ユーザーは既存のセキュリティ属性条件を条件ビルダーに参照できます。

データ分類

事前定義またはユーザー定義のデータ分類を使用して、データをタイプ別にグループ化します。ユーザーがデータ分類管理者または監査人ロールを持っている場合は、さまざまなデータクラスを管理したり、インスタンス内のさまざまなタイプのデータの現在のステータスを視覚的に分析したりすることができます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

データ分類の探索

データ分類について学習します。

データ分類の構成

独自のデータクラスを作成して設定します。

データ分類の参照

デモデータでデータ分類がどのように機能するかを説明します。

データ分類の分析

データ分類を分析する方法について説明します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

データ分類の概要

データ分類について説明します。

データ分類を使用して次のサポートを有効にできます。

- Now Platform インスタンスでホストされているデータのタイプの可視性。
- プライバシー法を遵守し、金融サービスや医療機器の製造など、業界の規制要件を満たします。

データ分類

データ分類は、任意のテーブルの既存のディクショナリーエントリにデータ分類を手動で適用するスタンドアロンプロセスです。詳細については、「Data dictionary tables」を参照してください。

- ビジネスに適したデータ分類を行い、必要に応じて利用可能なデータクラスを変更できます。
- データを分類するときは、事前定義されたデータ分類を使用することも、独自に作成することもできます。事前定義されたデータ分類の使用はオプションですが、開始点として使用することをお勧めします。これらの事前定義されたデータ分類は、インスタンスにインストールできるデモデータに含まれています。詳細については、「データ分類 プラグインのデモデータをインストールする」と「データ分類デモデータと一緒にインストールされるコンポーネント」を参照してください。
- 独自のデータ分類を作成する場合は、親と子のデータ分類を使用して階層型の階層システムを設計することもできます。

概要ダッシュボード

概要ダッシュボードを使用して、現在のデータテーブルがさまざまなデータ分類にどのようにマッピングされるかを把握することができます。また、グローバル、地域、国際的なユーザーが、データの使用またはアクセスに関して、データ分類にどのように異なるアプローチを必要とするかを分析することもできます。概要ダッシュボードのコンテンツとレイアウトをニーズに合わせてカスタマイズすることもできます。

利用可能なスクリプト化された REST APIs を使用して、既存のプロセス、ワークフロー、およびアプリケーション内に分類メタデータを適用する方法については、以下を参照してください。

- データ分類 - REST API
- DCManager - グローバル
- ScopedDCManager - スコープ指定

注:
データ分類 はドメイン分離をサポートしており、data_classification テーブル自体がプロセス分離されています。

ユースケース

一般データ保護規則 (GDPR) は、個人が自分の個人データを制御できるようにすることを目的とした欧州連合の規制です。個人を特定できる情報などのデータ分類を使用して、個人データがインスタンス内のどこに保存されているかを特定できます。適切なセキュリティメカニズムを適用して個人データの漏洩を防ぐことで、組織は GDPR 要件を満たすことができます。

顧客情報を Now Platform に保存する場合は、現地のプライバシー法の規制の対象となるデータを追跡するために必要な個人情報 (PII) 分類コードを使用します。デモデータをインストールすると、この分類コードがユーザー [sys_user] テーブルの特定のセキュリティ機密フィールドに自動的に適用されます。詳細については、以下を参照してください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- データ分類デモデータと一緒にインストールされるコンポーネント
- 辞書エントリへのデータ分類の割り当て

制限付きデータ分類は、社会保障番号 (SSN) などの従業員の機密情報を格納する従業員テーブル列に適用できます。管理者と監査人は、概要ダッシュボードを使用して、データ分類が正しい列に割り当てられていることを確認できます。また、制限されたタイプの情報の分類の詳細を表示することもできます。

データ分類 プラグインのデモデータをインストールする

Washington DC (以降) にアップグレードまたはインストールすると、データ分類(com.glide.data_classification) プラグインが自動的に有効になります。ただし、プラグインに付属するデモデータは手動でインストールする必要があります。事前定義された重要なデータ分類がいくつか含まれており、そのうちの 1 つをインスタンスの特定のユーザー [sys_user] テーブル列に割り当てます。

始める前に

必要なロール：admin

このタスクについて

デモデータをインストールするかどうかに関係なく、アクティブ化された データ分類 プラグインは次のユーザーロールをインスタンスに追加します。

- data_classification_admin：データ分類のセットアップとアサインを含むデータ分類アプリケーションのすべての側面を管理できます。
- data_classification_auditor：ユーザーのテーブルと列に対するデータ分類コード割り当てを監査できます。

重要:
お客様による使用に関する通知：

このアプリケーションの実装に関連するすべての意思決定は、お客様独自の判断によるものとします。お客様は、アプリケーションの使用は法律または規制の遵守に関する ServiceNow による表明ではなく、アプリケーションですぐに利用できる推奨文言、分野または分類が ServiceNow による法的な助言によるものでないことを承認および同意するものとします。

お客様は、データの保護、セキュリティ要件および個人データの収集、使用、開示、およびプライバシーに関する法律を含む (がそれに限定されない) 該当の法律に基づく法的義務を遵守する責任を単独で負い、お客様の要件を満たすために、テンプレートを含む (がそれに限定されない) このアプリケーションに対する必要な変更を構成および実施する責任を負うものとします。

手順

1. 移動先 システムアプリケーション > 利用可能なすべてのアプリケーション > すべて.
2. フィルター条件と検索バーを使用して、データ分類プラグインを検索します。
   プラグインを見つけると、「インストール済み」というメッセージが表示されます。
3. 縦に並んだ 3 つのドットアイコンをクリックし、[修理] を選択して [プラグインをアクティブ化] ダイアログを選択します。
4. [デモデータのロード] を選択し、[修復] をクリックします。

データ分類デモデータと一緒にインストールされるコンポーネント

データ分類 (com.glide.data_classification) プラグインに含まれるデモデータをインストールすると、いくつかのタイプのコンポーネントがインスタンスにインストールされます。これらのコンポー

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

ネントには、特定のユーザー [sys_user] 列の事前定義されたデータ分類とコード割り当てが含まれます。

インストールされるデータ分類

データ分類	説明
機密	侵害された場合に操作に悪影響を与える可能性がある機密データ。
内部	一般公開用ではない内部データ。
個人識別可能情報	PII とも呼ばれます。特定の個人を識別するために使用される可能性があるデータ。
公開	自由に公開される可能性のあるデータ。
制限付き	機密性の高い企業データで、侵害された場合に組織が財務的または法務的なリスクに晒される可能性があります。

データ分類 割り当て

テーブル	割り当てられた列	割り当てられたデータ分類
sys_user	zip	個人識別可能情報
sys_user	first_name	個人識別可能情報
sys_user	メール	個人識別可能情報
sys_user	city	個人識別可能情報
sys_user	middle_name	個人識別可能情報
sys_user	street	個人識別可能情報
sys_user	mobile_phone	個人識別可能情報
sys_user	last_name	個人識別可能情報
sys_user	country	個人識別可能情報
sys_user	gender	個人識別可能情報
sys_user	name	個人識別可能情報
sys_user	photo	個人識別可能情報
sys_user	state	個人識別可能情報
sys_user	home_phone	個人識別可能情報

データ分類の作成

データ分類 [data_classification] テーブルに独自のユーザー定義のデータ分類を作成し、特定のテーブルの特定の列に割り当てることができます。

始める前に
必要なロール：data_classification_admin、admin

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. 移動先 すべて > システムセキュリティ > データ分類 > データクラス.
2. [新規] を選択します。
3. フォームのフィールドに入力します。

フィールド	説明
分類名	データ分類名。
説明	データ分類の説明。
親	このデータ分類が従属している親データ分類の名前。このデータ分類が子データ分類の親ではない場合はフィールドを空のままにします。
アプリケーション	このデータ分類のアプリケーションスコープ。

4. このデータ分類を子データ分類の親にする必要がある場合は、[新規] をクリックします。
   子データ分類を作成しない場合は、この手順をスキップします。
5. フォームのフィールドに入力します。

   タイトル

フィールド	説明
分類名	子データ分類名。
説明	子データ分類の説明。
親	このデータ分類が従属している親データ分類の名前。このデータ分類が子データ分類の親ではない場合はフィールドを空のままにします。
アプリケーション	この子データ分類のアプリケーションスコープ。

6. [送信] をクリックします。

辞書エントリへのデータ分類の割り当て

辞書 [sys_dictionary] テーブルの特定のテーブル列にデータ分類を割り当てます。データ分類を割り当てると、辞書データクラス [m2m_dictionary_dataclass] テーブルにエントリが作成されます。作成されたエントリは概要ダッシュボードで確認できます。

始める前に

必要なロール：data_classification_admin、admin

手順

1. [ナビゲーション] ペインで、「sys_dictionary.list」と入力します。
2. 辞書エントリで、特定のデータ分類を割り当てる各要素を選択します。
3. 要素を選択したら、[選択した行のアクション] をクリックし、[分類] を選択します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注:
選択した辞書要素に以前に割り当てたデータ分類をクリアするには、[分類をクリア] を選択します。

4. [データクラスにアサイン] ダイアログが表示されたら、選択した辞書要素に割り当てるデータ分類を選択し、[分類] をクリックします。

警告:
これにより、選択した辞書アイテムの既存の分類が上書きされます。

必要に応じて、複数のデータ分類を選択できます。

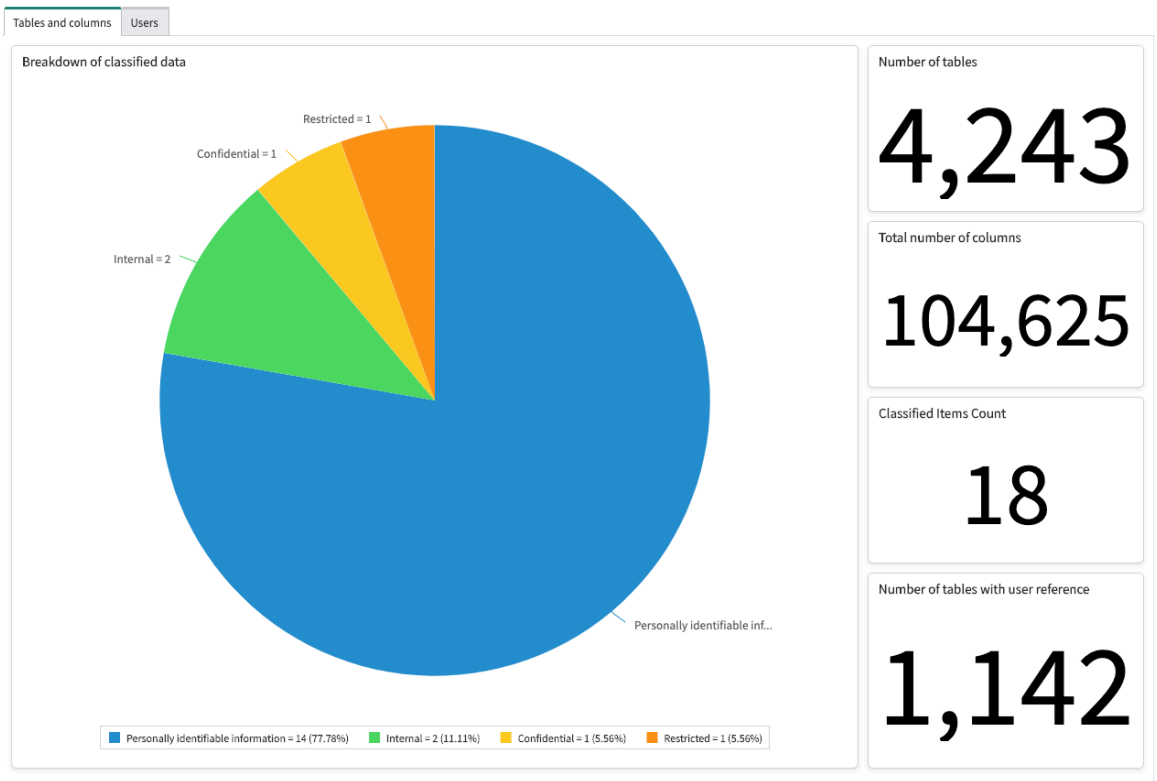
詳細については、「データ辞書テーブル」を参照してください。

概要ダッシュボードを使用したデータ分類の分析

概要ダッシュボードは、インスタンス内のデータ分類の現在のステータスと、ユーザーが場所ごとにどのように分布されているかをレポートします。

ユーザーがデータ分類管理者であるか監査人ロールを持っている場合、インスタンスデータの現在の機密性を視覚化できるため、セキュリティが高まり、プライバシー法への遵守が向上します。管理者は、ユーザーレコードの [場所] フィールドを使用して、プライバシー規制が異なるさまざまな地域にユーザーをマッピングできます。

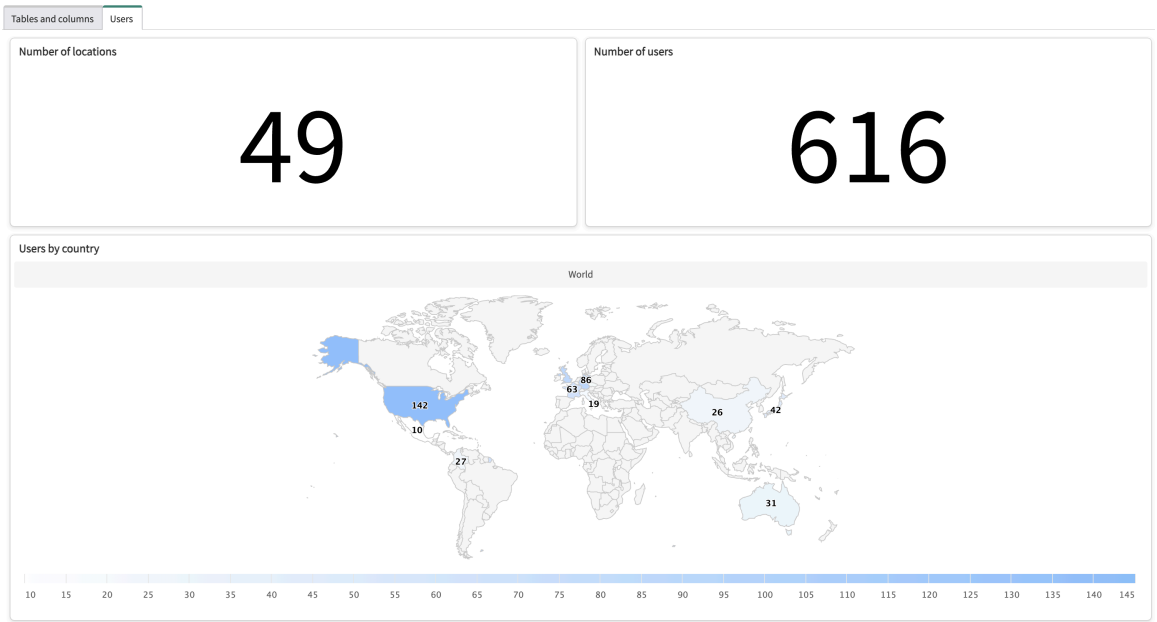
[テーブルと列] タブ



自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

[ユーザー] タブ



必要な **Now Platform** ロール

- data_classification_admin：データ分類のセットアップとアサインを含む データ分類 アプリケーションのすべての側面を管理できます。
- data_classification_auditor：データ分類 コードのアサインを監査します。

ユースケース

組織内のさまざまなユーザーがこのダッシュボードをどのように使用するかのその他の例については、データ分類のユースケースを参照してください。

ユーザー	ダッシュボードの使用法
data_classification_admin	インスタンスの正しいフィールドにデータ分類が割り当てられていることを確認します。
data_classification_auditor	インスタンス内のデータのシニリティとセキュリティを監査します。

レポート

役職	タイプ	ソーステーブル	説明
分類済みデータのブレークダウン	円グラフ	m2m_dictionary_dataclass	データクラス別に、インスタンスデータ分類のブレークダウンを提供します。
合計テーブル数	単一スコア	sys_dictionary	インスタンス内のデータテーブルの合計数。
列の合計数	単一スコア	sys_dictionary	インスタンス内の分類されたデータ列の合計数。この数は、データ

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

役職	タイプ	ソーステーブル	説明
			分類を割り当てた列の数です。
分類済みアイテム数	単一スコア	m2m_dictionary_dataclass	データ分類が割り当てられたテーブルの合計数。
ユーザー参照を持つテーブルの数	単一スコア	sys_dictionary	sys_user テーブルを参照する列が少なくとも 1 つあるテーブルの合計数。
場所の数	単一スコア	sys_dictionary	インスタンス内の場所の合計。
ユーザー数	単一スコア	sys_user	インスタンス内のユーザーの合計人数。
国別のユーザー	マップ	sys_user	国別のユーザーの場所のブレークダウン

ドメイン分離と データ分類

データ分類 ではドメイン分離がサポートされています。 ドメイン分離では、データ、プロセス、および管理タスクをドメインと呼ばれる論理的なグループに分けることができます。どのユーザーがデータを表示できるか、データにアクセスできるかなど、このアプリケーションのいくつかの側面を制御できます。

サポートレベル：拡張

- ベーシックレベルと標準レベルを含みます。
- データドリブンプロセスにより、サービスプロバイダーの顧客は定義されたユースケースに基づくビジネスロジックを変更できます。これらの構成は UI ベースでフェイルセーフであるため、1 人の顧客による構成が別のユーザーに影響を与えることはありません。
- インスタンスのテナントは、それ自体、MVP (minimum viable product) ビジネスロジックとデータパラメーターを設定できる必要があります。アプリケーションの通常の関数では、このロジックとパラメーターが想定されます。

サンプルユースケース：共有環境のテナント顧客は、影響度、緊急性、または優先度のマトリクスに変更を加えて、ドメイン内で優先順位を設定できる必要があります。

サポートレベルの詳細については、「アプリケーションでのドメイン分離のサポート)」を参照してください。

データ分類 におけるドメイン分離の仕組み

ドメイン分離の場合、アプリケーションは データ分類 [sys_data_classification] テーブルにプロセス分離を使用します。辞書データクラス [m2m_dictionary_dataclass] テーブルには、データ分離を使用します。データ分離とプロセス分離の詳細については、「Domain Separation の説明」を参照してください。

関連情報

サービスプロバイダーのドメイン分離

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

データフィルタリング

読み込みクエリを実行するときに、データフィルタリングを使用し、対象の属性に基づいてテーブルとレコードへのアクセスを制御します。

データフィルタリングの詳細

データフィルタリングについて学習します。

データフィルタリングルールの作成

ニーズに合わせて独自のデータフィルタリングルールを作成します。

データのデバッグ

データフィルタリングの結果をデバッグする方法について説明します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

データフィルタリングの概要

読み込みクエリを実行するときに、データフィルタリングを使用し、対象の属性に基づいてテーブルとレコードへのアクセスを制御します。

データフィルタリングは、インスタンスの既存のアクセス制御ルール (ACL) と連携して機能するように設計された、独立した形式のアクセス制御です。データフィルタリングは、管理者によって定義された対象属性と一致しないテーブルおよびレコードへのアクセスを拒否します。データフィルタリングは、監査、レポート、およびトラブルシューティングを簡易に行えるように設計されています。

これは、管理者がインスタンスで有効にできるオプションの機能です。

データフィルタリング機能

データフィルター データフィルターを使用し、レコード内の情報に基づいてアクセス権を付与します。データフィルターは、テーブルフィールドのデータを使用して、ユーザーがレコードを使用できるかどうかを判断します。
対象属性ベースの条件ビルダー 対象属性を使用して、ユーザーロール、グループ、対象基準、または IP ネットワークアドレスを評価します。
データフィルタリングで拒否ベースのモデルを使用する データフィルタリングでは、拒否ベースのモデルを使用してレコードへのアクセスを制御します。データフィルタリングでは、レコードがデータフィルタリングによって定義された基準を満たさない限り、インスタンスはレコードへのアクセスを拒否します。
データフィルタリングの適用 データフィルタリングルールは、READ 操作のデータベースクエリーの後に実行され、ACL の前に評価されます。データフィルタリングルールによって拒否されたレコードは処理されず、ACL ルールによって評価されます。 • データフィルタリングルールの適用は、READ ACL の適用と一貫性があります。 • データフィルタリングは、ACL と同様に、既存の *Report_view access control list* の動作と連携して機能します。これらのレポートコントロールの構成の詳細については、「Report_view アクセス制御」を参照してください。
セッションのデバッグ データフィルタリングはセッションのデバッグをサポートします。セッションのデバッグを使用して、特定のクエリーで適用されるデータフィルタリングレコードを確認します。管理者は、この情報を使用してレコードへのユーザーアクセスのトラブルシューティングを行うことができます。

データフィルタリングのコンポーネント

データフィルタリングは、次のレコードタイプを使用して機能します。

データフィルタリングレコード

データフィルタリング [sys_df_data_filtration] レコードを作成して、インスタンスのテーブルアクセスを許可します。データフィルタリングレコードには、ルールと影響を

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

受けるユーザーを制限するための前述のデータフィルターおよび対象属性条件が含まれています。

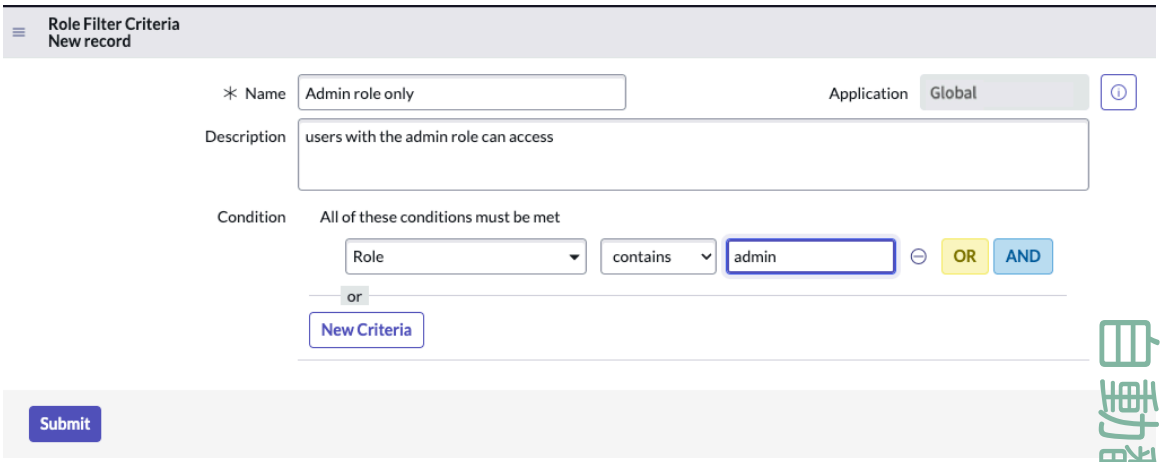
対象基準レコード

対象基準 [sys_df_subject_criteria] レコードは、データフィルタリングルールでアクセスを許可するかどうかを決定するために使用できる特定のユーザー属性を表します。これらの属性は、ユーザーのグループ、ロール、または IP アドレスです。対象基準を作成するには、対象基準レコードと基準入力および基準条件レコードを作成する必要があります。このプロセスの詳細については、「対象基準の作成」を参照してください。

対象基準レコードを作成したら、それをルールに適用できます。これは、データフィルタリングルールの [対象基準] タブで行います。

基準入力レコードの例

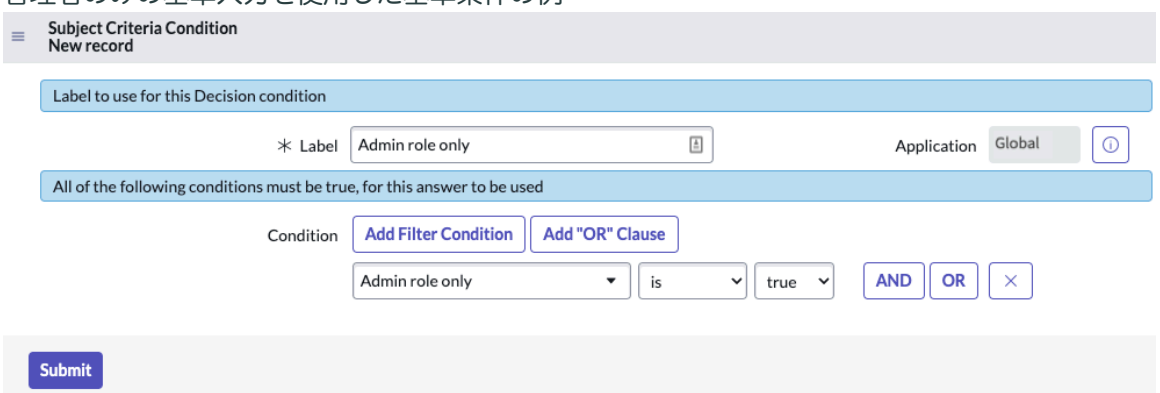
管理者を含むすべてのロールの基準入力の例



基準入力 [sys_df_subject_filter_criteria_m2m] は、ユーザーと比較する基準を含むレコードです。これは、ユーザーグループまたはロール、IP アドレス範囲、または IP アドレスサブネットのリストにすることができます。これらのレコードは、対象基準条件レコードとともに使用され、ユーザーのグループ、ロール、または IP アドレスに対して評価されて、テーブルまたはそのレコードへのアクセスが決定されます。

対象基準の条件レコード

管理者のみの基準入力を使用した基準条件の例



対象基準条件 [sys_df_subject_criteria_condition] レコードを使用して、ユーザー属性を、基準入力で定義されたロール、グループ、または IP アドレスと比較する方法を定義します。単一の対象基準条件で複数の基準入力を使用して、レコードへのアクセスをさらに絞り込むことができます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

データフィルタリングの有効化

インスタンスでデータフィルタリングを有効にする方法について説明します。

始める前に
必要なロール：security_admin

手順

1. 移動先 すべて > システム定義 > プラグイン.
2. 検索フィールドを使用して、Data Filtration (com.glide.data_filtration) プラグインを検索します。
3. [インストール] をクリックして、[プラグインをアクティブにする] ダイアログボックスで、[アクティブ化] をクリックします。

データフィルタリングルールの作成

レコードへのアクセスをユーザーに許可するデータフィルタリングルールの作成方法について説明します。

始める前に
必要なロール：security_admin

注:
データフィルタリングルールを作成または変更するには、 特権ロールに昇格される必要があります。このプロセスの詳細については、「特権ロールへの昇格」を参照してください。

手順

1. 移動先 すべて > データフィルタリング > データフィルタリングレコード.
2. [データフィルタリング] リストで [新規] をクリックします。
   新しいデータフィルタリングフォームが表示されます。
3. 必要に応じて、フォームのフィールドに入力します。

データフィルタリングフォーム

フィールド	説明
テーブル	このデータフィルタリングルールが適用されるテーブル。
アクティブ	データフィルタリングルールをアクティブに設定します。 **注:** 意図せずにユーザーをレコードからロックアウトしないように、テストの準備ができるまでデータフィルタリングルールを無効にします。
説明	データフィルタリングルールの説明。
カスケード	選択して、拡張テーブルに適用されるようにデータフィルタリングルールを設定します。 たとえば、Task[task] テーブルを選択し、カスケードを有効にします。この場合、データフィルタリングルールは、インシデント [incident] や変更要求 [change_request] などのタスクから拡張されたすべてのテーブルにも適用さ

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	れます。テーブル拡張の詳細については、「テーブル拡張とクラス」を参照してください。 注: このフィールドはデフォルトで有効になっています。

4. フォームメニューで、[保存] を選択します。
データフィルタリングルールを保存すると、選択したテーブルのすべてのレコードにこのルールが自動的に適用されます。[データフィルター] タブと [対象基準] タブの条件を使用して、このルールのスコープをテーブルの特定のレコードに絞り込むことができます。

データフィルタリングルールのデータフィルターの追加

必要に応じて、データフィルターを使用して、データフィルタリングルールのスコープをテーブルの特定のレコードにのみ適用されるように絞り込むことができます。

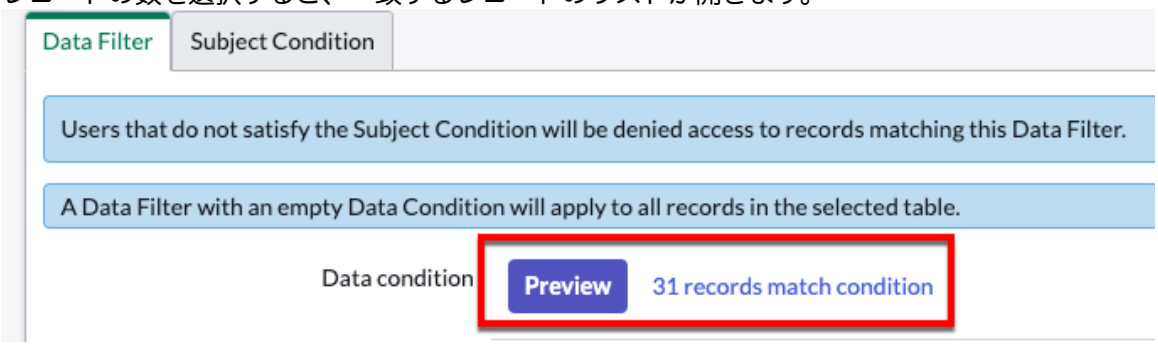
始める前に
必要なロール：admin

手順

1. データフィルタリングレコードで、[データフィルター] タブを開きます。
2. 条件ビルダーを使用して、テーブルレコードのフィールド値をフィルタリングします。
データフィルターは、プラットフォームの他の部分で使用されているものと同じ条件ビルダーを使用します。このインターフェイスの使用の詳細については、「条件ビルダー」を参照してください。

> 重要:
> [テーブル] フィールドでテーブルを選択するまで、[データフィルター] タブは空で表示されます。

3. [プレビュー] ボタンを使用して、データフィルターに一致するレコードの数を確認します。
4. レコードの数を選択すると、一致するレコードのリストが開きます。

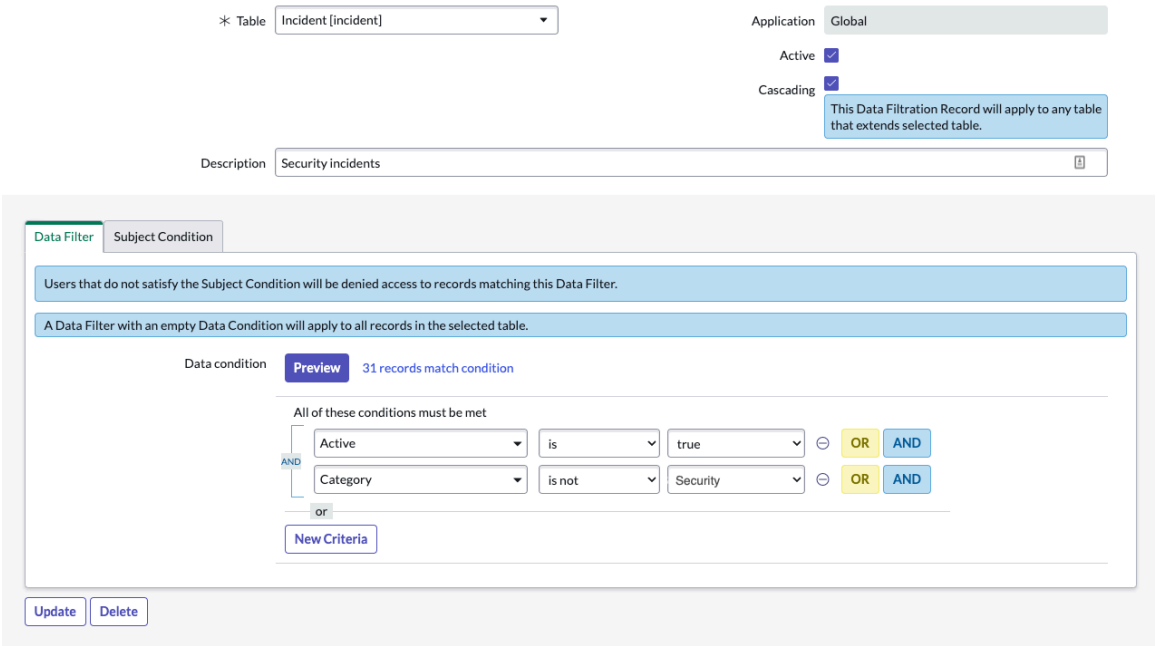


5. [保存] を選択します。

Example:
この例は、Incident[incident] テーブルのデータフィルタリングルールを示しています。データフィルターは、セキュリティカテゴリに含まれていないすべてのアクティブなレコードを選択するように設定されています。このルールをアクティブにすると、ユーザーはこれらのレコードを表示できます。レコードのコンテンツの外部の基準を使用するには、以下のセクションを参照してください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



重要:

インスタンスで使用するデータベースのタイプによっては、条件の **not** 操作で予期しない結果が返される場合があります。たとえば、次のような条件を使用します。

この条件では、結果セットは、会社が ServiceNow ではないすべてのレコードと、**[company]** フィールドに値がないすべてのレコードになることが予想されます。MySQL と Maria 以外のデータベースを使用しているインスタンスは、**[company]** フィールドが空になっているレコードを返しません。これらのインスタンスに対して **not** クエリーを使用する場合は、空の値が返されるようにするための条件を含めます。

データフィルタリングルールに対象属性を追加する

必要に応じて、対象属性を使用し、IP ネットワークアドレス、ユーザーグループとロール、対象基準などの属性に基づいてデータフィルタリングルールのスコープを絞り込みます。

始める前に

必要なロール：admin

手順

1. データフィルタリングレコードで、[対象基準] タブを開きます。
2. 条件ビルダーを使用し、次の 1 つ以上の条件に基づいてテーブルレコードをフィルタリングします。

対象基準オプション

オプション	説明
ネットワーク基準	ネットワーク IP 範囲または IP サブネットに基づいてレコードへのアクセスを許可します。
対象基準	対象基準に基づいてレコードへのアクセスを許可します。対象基準レコードを選択して、その条件をデータフィルタリングルールに適用します。対象基準レコードの作成の詳細については、「対象基準の作成」を参照してください。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

オプション	説明
対象グループ	ユーザーが特定のグループのメンバーである場合にアクセスを許可します。**Groups**[sys_user_group] テーブルからグループを選択します。
対象ロール	ユーザーが特定のグループのメンバーである場合にアクセスを許可します。**Roles**[sys_user_role] テーブルからグループを選択します。

重要:
対象基準条件は **is** 演算子のみをサポートします。

3. 対象基準を追加した後に、[保存] をクリックします。

対象基準の作成

データフィルタリングルールで使用するための対象基準レコードを作成します。

始める前に
必要なロール：security_admin

重要:
データフィルタリングルールを作成または変更するには、 特権ロールに昇格される必要があります。このプロセスの詳細については、「特権ロールへの昇格」を参照してください。

手順

1. 移動先 すべて > データフィルタリング > 対象基準.
2. [対象基準] リストで [新規] ボタンをクリックします。
   新しい対象基準フォームが表示されます。
3. 必要に応じて、フォームのフィールドに入力します。

対象基準のフィールド

フィールド	説明
名前	対象基準の名前。
アプリケーション	対象基準のスコープ対象のアプリケーション。このフィールドは、読み取り専用であり、現在のスコープ対象のアプリケーションが自動的に入力されます。
説明	対象基準の説明。

4. フォームヘッダーを右クリックし、コンテキストメニューから [保存] をクリックします。
   保存した後に、[基準の入力] フィールドと [基準の条件] フィールドが表示されます。

対象基準入力の作成

対象基準の入力を作成して、データフィルタリングルールでフィルタリングする基準を定義します。

始める前に
必要なロール：security_admin

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. 対象基準レコードで、[基準の入力] タブを開きます。
2. [基準の入力] リストで [新規] をクリックします。
3. 作成する基準のポリシーの入力を選択します。

ポリシーの入力

ポリシーの入力	説明
IP フィルター基準	IP アドレスに基づいてポリシー入力を作成します。
ロールフィルター基準	使用ロールに基づいてポリシーの入力を作成します。
グループフィルター基準	ユーザーグループに基づいてポリシーの入力を作成します。

このステップでの選択に応じて、**[IP** フィルター基準]、[ロールフィルター基準]、または [グループフィルター基準] フォームが表示されます。

4. 必要に応じて、フィルター基準フォームのフィールドに入力します。

フィルター基準のフィールド

フィールド	説明
名前	フィルター基準の名前
アプリケーション	対象基準のスコープ対象のアプリケーション。このフィールドは、読み取り専用であり、現在のスコープ対象のアプリケーションが自動的に入力されます。
説明	フィルター基準の説明

5. フォームフィールドの下には、フィルター基準入力の IP アドレス、グループ、またはロールを定義するために使用されるタブがあります。

特定の入力タイプのフィルター基準フィールド

ポリシーの入力のタイプ	説明	作成
IP フィルター基準	IP アドレスの範囲またはサブネットを作成するためのユーザー IP フィルター基準。対象基準は、この範囲またはサブネットに対してユーザーの IP アドレスと比較できます。	**IP** 範囲またはサブネット **(CIDR)** を使用して、入力の IP アドレスを定義します。 IP 範囲 **[IP** 範囲] リストで [新規行を挿入] をダブルクリックし、[開始 **IP]** に開始 IP アドレスを入力します。次に、Tab キーを押して、[終了 **IP]** フィールドに終了 IP アドレスを入力します。最後に、

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ポリシーの入力のタイプ	説明	作成
		Enter キーを押してリストエントリーを保存します。 サブネット (CIDR) [サブネット] リストで、[新規行を挿入] をダブルクリックし、[ネットワーク **IP]** フィールドにネットワーク IP を入力します。次に、Tab キーを押して、[ネットマスク] フィールドにネットマスクを入力します。最後に、 Enter キーを押してリストエントリーを保存します。 **注:** スケジューラーによってトリガーされるジョブスケジュールは、要求元のクライアント IP のコンテキストを持たないため、ネットワーク基準を使用してデータをフィルタリングすることを意図していません。ロール/グループ対象条件のタイプのフィルタリングの方が適している場合があります。
ロールフィルター基準	ロールフィルター基準を使用して、ロールの選択を作成します。その後で対象基準は、この選択に対してユーザーのアサイン済みロールと比較できます。	[条件] フィールドの条件ビルダーを使用して、入力のロールを選択します。
グループフィルター基準	グループフィルター基準を使用して、ユーザーグループの選択を作成します。その後で対象基準は、この選択に対してユーザーのアサイン先グループと比較できます。	[基準のグループ] テーブルで、[新規行を挿入] をダブルクリックし、ユーザーグループを選択します。Enter を押すか、緑色のチェックマークアイコンをクリックしてグループを保存します。 最初のエントリーの下の [新規行を挿入] テキストをクリックして、追加のエントリーを作成します。

6. 入力を定義したら、[送信] をクリックします。

注: 対象基準の基準入力を作成するだけでなく、既存の基準入力を追加することもできます。[基準の入力] タブで [編集] をクリックし、既存の入力から選択します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

対象基準条件の作成

ユーザー情報を既存の対象基準入力と比較するための条件を作成します。

始める前に
必要なロール：security_admin

基準条件は、ユーザー属性を既存の基準入力と比較して、レコードへのアクセスを許可するかどうかを決定します。基準条件を作成するには、対象基準を作成している必要があります。このプロセスの詳細については、「対象基準入力の作成」を参照してください。

手順

1. 対象基準レコードで、[基準の条件] タブを開きます。
2. [基準の条件] リストで [新規] をクリックします。
3. 必要に応じて、[対象基準の条件] フォームのフィールドに入力します。

[対象基準の条件] フォーム

フィールド	説明
ラベル	条件を説明するラベル
アプリケーション	対象基準のスコープ対象のアプリケーション。このフィールドは、読み取り専用であり、現在のスコープ対象のアプリケーションが自動的に入力されます。

4. 条件ビルダーを使用し、次の条件オプションから選択して、対象基準の条件を作成します。
これらの条件オプションには、作成した任意の対象基準の入力が含まれます。
5. オプション: [フィルター条件の追加] または [「OR」節を追加] ボタンをクリックして、さらに条件を作成します。

   注:
   条件が **or** 節で区切られていない限り、対象基準の条件が true と評価されるには、すべての条件が true と評価される必要があります。

6. [送信] をクリックして、対象基準の条件を保存します。

次のタスク
データフィルタリングルールで対象基準を使用して、テーブルとレコードへのアクセスを制限します。データフィルタリングルールでの対象基準の使用方法の詳細については、「対象基準の作成 」を参照してください。

データフィルタリングのデバッグ

セッションログを使用して、データフィルタリングがレコードにどのように影響するかを確認し、ユーザーアクセスの問題をデバッグします。

始める前に
必要なロール：admin

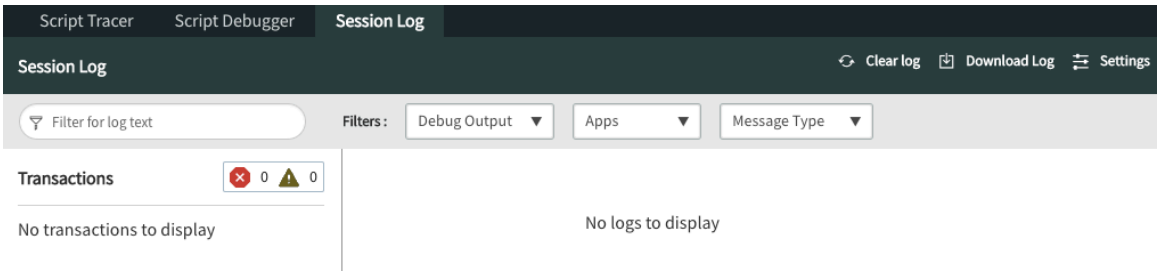
ユーザーがレコードにアクセスすると、出力情報がセッションログに表示されます。このログ記録情報を代理操作とともに使用して、ユーザーにレコードが表示されるかまたは表示されない理由を調べることができます。次にその情報を使用してデータフィルタリングルールを調整し、意図したレコードのみがユーザーに表示されるようにすることができます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

手順

1. 移動先 すべて > システムセキュリティ > デバッグ > すべてのセキュリティをデバッグ.
   スクリプトデバッガーが新しいブラウザータブまたはウィンドウで開きます。



2. [スクリプトデバッガー] ウィンドウで、[セッションログ] タブを選択します。
3. 別のブラウザータブまたはウィンドウで、ユーザーの代理操作を行ってそのユーザーのアクセスをトラブルシューティングします。

   注:
   代理操作により、管理者は別のユーザー設定とアクセス権を持つインスタンスを表示できます。代理操作の詳細については、「ユーザーの代理操作を行う」を参照してください。

4. ユーザーの代理操作中に、予期しない動作が発生したリストまたはレコードにアクセスします。
   この動作は、表示されるべきではないにもかかわらずユーザーに表示されるレコード、またはユーザーに期待どおりに表示されないレコードのリストです。
   代理操作されたユーザーでレコードにアクセスすると、セッションデバッガーで出力が表示されるようになります。
5. セッションデバッガーでデータフィルタリング情報を探します。

   この例は、データフィルターがレコードへのアクセスを拒否した 2 つのログメッセージを示しています。ログエントリーは赤色のテキストとして表示され、データフィルターがアクセスを拒否した理由と、データフィルターの sys_id が含まれます。この sys_id をクリックすると、データフィルタリングレコードを開くことができます。

   この例は、データフィルターがレコードへのアクセスを許可したログメッセージを示しています。これらのログエントリーは緑色のテキストとして表示されます。最初のメッセージと同じように、この sys_id をクリックすると、データフィルタリングレコードを開くことができます。

6. この情報を使用して、データフィルタリングルールを調整します。
   これらの手順を繰り返してルールを調整し、ユーザーに必要なアクセス権を付与します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Data Privacy

Data Privacy を使用して、機密データを分類し、本番インスタンスのユーザーデータから個人識別可能情報 (PII) を削除して、非本番インスタンスのデータを匿名化します。匿名化されると、ユーザーデータは規制対象の個人情報と見なされなくなります。

Data Privacy の探索

詳しくは、データプライバシーについて学習します。

Data Privacy の構成

Data Privacy の設定方法について説明します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Data Privacy におけるロール

Data Privacy のロールの詳細を取得します。

Data Privacy の高度な機能

Data Privacy の高度な機能について説明します。

自動翻訳

Data Privacy の概要

Data Privacy を使用して、機密データを分類し、本番インスタンスのユーザーデータから個人識別可能情報 (PII) を削除して、非本番インスタンスのデータを匿名化します。匿名化されると、ユーザーデータは規制対象の個人情報と見なされなくなります。

開発者は、非本番インスタンスのデータを操作して、実装が期待どおりに機能していることを確認する必要があります。本番インスタンスからのデータのインポートは、本番環境をシミュレートするための便利な方法ですが、セキュリティ上のリスクがあります。Data Privacy を使用すれば、管理者は非本番環境で安全に作業するための、個人情報を含まないデータを開発者に提供できます。

Data Privacy の重要性と、分類および匿名化によって機密情報を保護するために企業が実行できる手順について説明します。Data Privacy ストアアプリケーションを使用して、メインダッシュボードと機能の概要を説明します。

データ分類

インスタンス内のデータタイプの機密性レベルによって決定される事前定義された基準に従って、機密データを識別して分類します。データの機密性レベルは、分類された各データタイプの処理方法を決定するのに役立ちます。基本レベルのデータプライバシーを備えた事前定義されたクラスがいくつか提供されています。Data Privacy の分類セクションを使用して、インスタンス内のデータにラベルを付けてグループ化します。クラスを追加し、データクラス構造を表示して、データを分類します。事前定義またはユーザー定義のデータ分類を使用して、データをタイプ別にグループ化します。

Data Privacy ストアアプリケーションを使用してデータを分類する方法について説明します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ユーザーデータの匿名化

管理者は、すべてのユーザーまたは一部のユーザーの情報をすべて匿名化するかどうかを定義します。匿名化すると、選択したユーザーレコードのデータが、ランダムな値または定義した値に置き換えられます。値を置き換える際は、さまざまな手法でデータ構造を保持できます。

Data Privacy ストアアプリケーションを使用してデータを匿名化する方法について説明します。

Data Privacy オプション

- Data Privacy (Classic)：最初にデータ分類アプリを使用し、事前定義またはユーザー定義のデータ分類を使用して、データをタイプ別にグループ化します。次に、Data Privacy のテクニックとジョブを作成して、PII を匿名化します。
- Data Privacy (ストアアプリ)：Data Privacy アプリ内からすべてのデータを分類して匿名化します。

考慮事項

- 匿名化できるのは、分類されたデータのみです。データのクラスと分類の詳細については、「データ分類」(Classic) または データ分類 ストアアプリを参照してください。
- ログ内の PII およびその他の監査データは匿名化されません。
- 匿名化できるのは、構造化されたデータのみです。ジャーナルフィールド、コメント、添付ファイル、および部分的なテキストが PII を表す可能性があるその他のフィールドなどの非構造化データは匿名化されません。詳細については、「匿名化でサポートされているフィールドタイプ」を参照してください。
- Single Sign-On (SSO) システムとの統合により、信頼できる情報源システムからのユーザー情報を再同期できます。sys_user データの匿名化の永続性を保証するメカニズムはありません。ユーザー管理および sys_users の詳細については、「ユーザー管理」を参照してください。

Domain Separation と Data Privacy

Data Privacy では Domain Separation はサポートされていません。 ドメイン分離では、データ、プロセス、および管理タスクをドメインと呼ばれる論理的なグループに分けることができます。どのユーザーがデータを表示できるか、データにアクセスできるかなど、このアプリケーションのいくつかの側面を制御できます。

サポートレベル: サポートなし

- ドメインフィールドがデータテーブル に存在している可能性がありますが、データを管理するロジックがありません。
- このレベルでは、ドメイン分割は考慮されません。

サポートレベルの詳細については、「アプリケーションでのドメイン分離のサポート)」を参照してください。

関連情報

サービスプロバイダーのドメイン分離

匿名化でサポートされているフィールドタイプ

データを匿名化するときにサポートされているフィールドタイプを確認します。

注:
分類されたすべてのフィールドタイプが匿名化に使用できるわけではありません。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

次の表に示すように、一部の高リスクフィールドタイプはデフォルトでオフになっています。フィールドの詳細については、「フィールドタイプ」を参照してください。

匿名化でサポートされているフィールドタイプ

フィールドタイプ	デフォルトで利用可能
audio	いいえ
状態	いいえ
condition_string	いいえ
currency	はい
decimal	はい
due_date	はい
浮動小数点数	はい
glide_date	はい
glide_date_time	はい
glide_duration	いいえ
glide_time	はい
HTML	いいえ
アイコン	いいえ
integer	はい
ip_addr	いいえ
ip_address	いいえ
journal	いいえ
journal_input	いいえ
journal_list	いいえ
longint	はい
name_values	いいえ
percent_complete	いいえ
phone_number_e164	はい
price	はい
string	はい
string_full_utf8	はい
Translation_html	いいえ
translated_text	いいえ
url	いいえ
user_image	いいえ
video	いいえ
wiki_text	いいえ

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Data Privacy ロール

Data Privacy は次のロールを追加します。

ロールの説明

ロールタイトル [名前]

ロールの名前。かっこ内のテキストは、ロール [sys_user_role] テーブルの [名前] フィールドと一致します。

説明

ロールとその使用目的の説明。

ロールを含む

ロール内に含まれるロールのリスト。

グループ

このロールがデフォルトでアサインされているグループのリスト。

登録

このロールが、このロールを持つユーザーをサブスクリプションに割り当てる必要がある課金可能ユーザーロールかどうか。

昇格

ロールが昇格されたかどうか。昇格されたロールはユーザーまたはグループにアサインされず、昇格で使用する必要があります。詳細については、「特権ロールへの昇格」を参照してください。

考慮事項

管理者向けの警告またはその他の考慮事項。

注:

個々のユーザーではなくグループにロールを割り当てることで、ユーザー管理を簡素化します。特定のペルソナに必要なすべてのロールが含まれるグループを作成し、そのグループにユーザーを割り当てます。ユーザーが新しいロールに移行したときは、グループを再アサインして、ユーザーが予期しないロールを保持するシナリオを回避できます。

ユーザー、グループ、およびロールの管理の詳細については、「ユーザー管理」を参照してください。

Data Privacy 管理者

Data Privacy 管理者ロールは、Data Privacy のテクニックとポリシーを作成するために使用される管理者ロールです。

Data Privacy 管理者 [data_privacy_admin]

ロールを含む

なし

グループにアサイン

なし

登録

いいえ

昇格

いいえ

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

考慮事項

より対象が絞られたロールを使用できる場合は、このロールをユーザーに割り当てないでください。

Data Privacy 監査人

Data Privacy 監査人は、Data Privacy レコードを表示するために使用される読み取り専用のロールです。

Data Privacy 監査人 [data_privacy_auditor]

ロールを含む

なし

グループにアサイン

なし

登録

いいえ

昇格

いいえ

考慮事項

なし

Data Privacy クローンプロセッサー

Data Privacy クローンプロセッサーロールを持つユーザーは、データクラスの Data Privacy ジョブを作成して実行できます。

Data Privacy クローンプロセッサー [data_privacy_clone_processor]

ロールを含む

なし

グループにアサイン

なし

登録

いいえ

昇格

あり

考慮事項

なし

Data Privacy プロセッサー

Data Privacy プロセッサーロールを持つユーザーは、ユーザー [sys_user] テーブルで Data Privacy ジョブを作成して実行できます。

Data Privacy プロセッサー [data_privacy_processor]

ロールを含む

なし

グループにアサイン

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

なし

登録

いいえ

昇格

あり

考慮事項

なし

Data Privacy (Classic)

Data Privacy (Classic) はファミリーリリースとして利用可能です。前回のファミリーの更新は、Tokyo バージョンでリリースされました。

Data Privacy (Classic) のアクティブ化

admin ロールを持っている場合は、プラットフォームセキュリティ の Data Privacy プラグイン (com.glide.data_privacy) をアクティブ化できます。このアプリケーションにはデモデータが含まれています。まだインストールされていない場合は、関連する ServiceNow Storeアプリケーションとプラグインをインストールします。

始める前に
Data Privacy では、他の Now Platform とは別のサブスクリプションが必要です。

サブスクリプションを購入するには、ServiceNow アカウントマネージャーにお問い合わせください。サブスクリプションを購入すると、特定のプラグインが自動的にアクティブになります。有料プラグインが自動的にアクティブになっていない場合は、インスタンスの [すべてのアプリケーション] リストから手動でアクティブ化できます。

注:

サブスクリプションを購入する前に、Now Support サービスカタログ から非本番インスタンスを要求することによって、その機能を課金なしに評価できます。

必要なロール：admin

このタスクについて
次のアイテムが Data Privacy とともにインストールされます。

- プラグイン
- ロール
- テーブル

詳細については、「Data Privacy (Classic) とともにインストールされるもの」を参照してください。

手順

1. 移動先 すべて > システムアプリケーション > 利用可能なすべてのアプリケーション > すべて.
2. フィルター基準と検索バーを使用して Data Privacy プラグイン (com.glide.data_privacy) を検索します。

   名前または ID でプラグインを検索できます。プラグインが見つからない場合は、ServiceNow 担当者から要求する必要があります。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

3. [インストール] を選択して、[プラグインをアクティブにする] ダイアログボックスで、[アクティブ化] をクリックします。

> **注:**
> ドメイン分離と代理管理者がインスタンスで有効になっている場合、管理ユーザーはグローバルドメインに含まれている必要があります。それ以外の場合、次のエラーが表示されます： 別の操作が実行されているため、アプリケーションのインストールは利用できません：<プラグイン名> のプラグインの有効化。

Data Privacy (Classic) とともにインストールされるもの

Data Privacy プラグイン (com.glide.data_privacy) とともにインストールされるコンポーネントについて説明します。

インストールされるテーブル

テーブル	説明
Data Privacy 連携ジョブ [dp_federated_job]	Data Privacy の連携ジョブ
Data Privacy ジョブ [dp_job]	Data Privacy ジョブ
Data Privacy ジョブ [dp_job_summary]	Data Privacy ジョブのサマリー
Data Privacy 手法 [dp_technique]	Data Privacy 手法
プライマリ参照リンク [dp_primary_reference]	プライマリ参照リンク
プライバシーに分類されたフィールドの手法 [dp_field_technique]	Data Privacy に分類されたフィールドの手法
プライバシー構成 [dp_configuration]	Data Privacy 構成
プライバシー手法構成 [dp_technique_with_params]	Data Privacy 手法

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

テーブル	説明
プライバシー手法パラメーター [dp_technique_with_parameter]	Data Privacy 手法とパラメーター
プライバシー手法のパラメーターの値 [dp_technique_with_parameter_value]	Data Privacy 手法とパラメーターで使用されるパラメーター値

Data Privacy (Classic) 構成

Data Privacy 手法とポリシーを作成する方法、および Data Privacy ジョブを作成して実行する方法について説明します。

Data Privacy 手法

Data Privacy 手法は、データの匿名化方法を決定するために選択するオプションです。Data Privacy ジョブで参照する Data Privacy 手法を作成する必要があります。プライバシー手法を関連するプライバシー手法構成に関連付けるには、「Data Privacy 手法構成の作成」を参照してください。

Data Privacy ポリシー

Data Privacy ポリシーを構成して、データを匿名化するときに使用する Data Privacy 手法を指定します。詳細については、「Data Privacy ポリシーの作成」を参照してください。

Data Privacy ジョブ

Data Privacy ジョブは、これらすべてのコンポーネントを使用してデータを匿名化します。これらのジョブの詳細については、「Data Privacy ジョブの構成」を参照してください。

Data Privacy 手法構成の作成

Data Privacy 手法構成を作成して、Data Privacy でデータを匿名化する方法をカスタマイズします。

始める前に
必要なロール：data_privacy_admin および admin

手順

1. **data_privacy_admin** ロールに昇格させます。
   ロールの昇格の詳細については、「特権ロールへの昇格」を参照してください。
2. 移動先 システムセキュリティ > **Data Privacy** > プライバシー手法構成.
3. [新規] をクリックします。
4. [名前] フィールドに、プライバシー手法構成の名前を入力します。
5. [プライバシー手法] フィールドで、プライバシー手法を選択します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Data Privacy 手法

テクニック	説明
アクションなし	この手法はプレースホルダーです。選択されている場合、フィールドは変更されません。
ランダム置換	この手法では、値をランダムに生成された値に置換します。文字列および数値データでこの手法を使用できます。
選択的置換 (Selective Replace)	この手法では、文字列データを選択的に置換します。入力の開始インデックスと終了インデックスの間のすべての文字が、選択した文字に置き換えられます。マスクから除外する文字を指定できます。 ○ start_index：手法は指定された文字以降のデータをマスクします。空白のままにすると、最初の文字からマスクが開始されます。 ○ end_index：手法は文字列の先頭から指定された文字までのデータをマスクします。空白のままにすると、最後の文字でマスクが終了します。 ○ exclude_char：マスクから除外する文字を定義します。 ○ replacement_char：マスクに使用する文字を定義します。何も指定しない場合、デフォルトでアスタリスク (*) が使用されます。
静的置換 (Static Replace)	この手法では、値を静的な値に置換します。文字列、数値、および日付データでこの手法を使用できます。 ○ date_time_value：日付値をこの日付に置き換えます。yyyy-MM-dd HH:mm:ss 形式を使用します。 ○ date_value：日付値をこの日付に置き換えます。 yyyy-MM-dd 形式を使用します。 ○ number_value：数値をこの数値に置き換えます。 ○ string_value：文字列値をこのテキストに置き換えます。
削除	この手法では、値を削除して空の (null) 値に置き換えます。

注:
以前にサポートされていた値 **Replace** は廃止されたので使用しないでください。これは名前が **Replace-Deprecated** に変更されています。

6. ヘッダーを右クリックし、コンテキストメニューの [保存] を選択します。
   レコードが保存されると、[プライバシーのパラメーター化された値] リストが表示されます。
7. [プライバシーのパラメーター化された値] リストのレコードを使用して、Data Privacy 手法の構成をカスタマイズします。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

使用可能なパラメーター化された値は、選択したプライバシー手法によって異なります。[アクションなし] および [削除] 手法にはパラメーター化された値はありません。

選択的置換のプライバシーのパラメーター化された値

プライバシー手法のパラメーターの値	説明	デフォルト値
char_to_replace	選択的置換を使用して値を置換するときに使用する文字。	*
end_index	手法は文字列の先頭から指定された文字までのデータをマスクします。空白のままにすると、最後の文字でマスクが終了します。	(空)
exclude_char	マスクをスキップする文字。この値に使用できるのは 1 文字のみです。複数入力した場合は、最初の文字が使用されます。	(空)
start_index	手法は指定された文字以降のデータをマスクします。	1

置換のプライバシーのパラメーター化された値

プライバシー手法のパラメーターの値	説明	デフォルト値
date_time_value	日時値をこの日付に置き換えます。yyyy-MM-dd HH:mm:ss 形式を使用します。	1988-11-11 10:10:10
date_value	日付値をこの日付に置き換えます。 yyyy-MM-dd 形式を使用します。	1988-11-11
number_value	[数値] の値をこの数値に置き換えます。	1234567
preserve_data_length	データ長を保持する場合は **true** に設定します。匿名化されたデータは、元のデータと同じ長さになります。	true
string_value	文字列値をこのテキストに置き換えます。	TEXT123
use_random_generated_value	データをランダムに生成された値に置き換えるには **true** に設定します。ランダム値に置き換えることができるのは文字列と数値のデータのみです。このオプションは、静的な値を上書きします。	false

8. [保存] をクリックします。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Data Privacy ポリシーの作成

Data Privacy ポリシーを構成して、データを匿名化するときに使用する Data Privacy 手法を指定します。

始める前に

Data Privacy 構成では、ユースケースに応じてテーブル、sys_user など、および列を匿名化するように定義し、データの匿名化中に使用されるパラメーター化される手法のタイプを指定します。

> **注:**
> プライバシー構成を完了するには、最初に Data Privacy 手法構成を設定する必要があります。詳細については、「Data Privacy 手法構成の作成」を参照してください。

必要なロール：data_privacy_admin および admin

手順

1. **data_privacy_admin** ロールに昇格させます。
   ロールの昇格の詳細については、「特権ロールへの昇格」を参照してください。
2. 移動先 システムセキュリティ > データプライバシー (従来) > プライバシーポリシー構成.
3. [新規] を選択します。
4. [名前] フィールドに、プライバシーポリシー構成の名前を入力します。
5. [データクラス] フィールドで、このポリシーで使用するデータクラスを選択します。
   Data Privacy ポリシーは分類されたデータにのみ適用できます。データ分類の詳細については、「データ分類」を参照してください。
   データクラスを選択すると、[プライバシーに分類されたフィールドの手法] と [プライバシーのプライマリ参照リンク] のリストがフォームに表示されます。
6. オプション: [クラスのすべてのデータに適用 **(Apply to All Data in Class)**] を選択すると、選択したデータクラスのすべてのデータに匿名化が適用されます。
   このフィールドを選択しない場合、Data Privacy プロセッサユーザーが、Data Privacy ジョブの作成時に匿名化するユーザーを選択できます。このフィールドを選択した場合、そのオプションは使用できません。
   - [クローン作成時に適用]：このオプションが利用可能になります。選択すると、Data Privacy クローン作成中にプライバシー構成が実行されます。
   - [アプリケーションの順序]：上位のアプリケーション順序を持つクローン後構成の Data Privacy ジョブが、下位のジョブの前に開始される場合があります。

     > **重要:**
     > 同じアプリケーション順序で複数の Data Privacy ポリシーを作成することは避けてください。結果として同じ順序の処理順序の一貫性がなくなります。

7. オプション: Data Privacy ジョブからデータを匿名化解除する機能を有効にするには、[サポートロールバック] を選択します。
   詳細については、「Data Privacy ジョブのロールバック」を参照してください。
   データプライバシージョブの作成時に [サポートロールバック] を選択すると、ジョブをロールバックするオプションが利用可能になります。
8. [プライバシーに分類されたフィールドの手法] タブを選択して、[プライバシーに分類されたフィールドの手法] リストを表示します。
9. [テーブル] フィールドのエントリを選択して、各リストエントリの [プライバシー手法構成] フィールドを開きます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

[プライバシーに分類されたフィールドの手法] リストには、選択したデータクラスで匿名化されるすべてのデータが表示されます。これらのエントリごとに、適用するプライバシー手法を選択する必要があります。

10. 適用するプライバシー手法構成を選択します。

> **重要:**
> エントリを匿名化しない場合は、エントリを空のままにするのではなく、**[DoNothing]** 手法を選択します。[プライバシー手法構成] フィールドの値が空になっているポリシーは、Data Privacy ジョブで使用されるときに実行できません。

11. [送信] または [保存] をクリックしてレコードを保存します。

次のタスク
Data Privacy ジョブの構成。

Data Privacy ジョブの構成

非本番インスタンスでユーザーおよびデータクラスのジョブに匿名化されたデータを使用するように、本番インスタンスで Data Privacy ジョブを構成します。

始める前に
Data Privacy ジョブは、次の 2 つの匿名化ユースケースをサポートしています。

- 特定の sys_users の機密データ
- 特定のデータクラスの機密データ。

必要なロール：data_privacy_processor および admin

手順

1. **data_privacy_processor** ロールに昇格させます。
   ロールの昇格の詳細については、「特権ロールへの昇格」を参照してください。
2. 移動先 システムセキュリティ > **Data Privacy** > データプライバシージョブ.
3. [Data Privacy ジョブ] リストで、[新規] をクリックします。
4. フォームのフィールドに入力します。

Data Privacy ジョブのフィールド

フィールド	説明
名前	ジョブの名前。
説明	ジョブの説明。
プライバシー構成	このジョブに使用するプライバシーポリシー構成。プライバシーポリシー構成の詳細については、「Data Privacy ポリシーの作成」を参照してください。
ユーザー	このジョブで匿名化するユーザーまたはユーザーグループを選択します。最大 1000 人のユーザーグループを処理できます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	注: このフィールドは、選択したプライバシーポリシーの条件でユーザーレコードを選択する必要がある場合にのみ表示されます。
予行演習	ジョブをテストとして実行します。このジョブの実行時に影響を受けるレコードはありません。結果は、ジョブが実行された場合のように [サマリー] フィールドに表示されます。 **注:** ロールバックを使用して Data Privacy ジョブを構成するときは、[予行演習] をオフにする必要があります。詳細については、「Data Privacy ジョブのロールバック」を参照してください。
状態	Data Privacy ジョブのステータス： ○ スケジュールの準備ができました：新しいジョブのデフォルトステータス。 ○ ロールバック中：ジョブは匿名化をロールバックするように設定されています。 ○ ロールバック完了：匿名化ジョブのロールバックが正常に完了しました。 読み取り専用フィールド。
推定レコード数	このジョブが影響するレコードの推定数。読み取り専用フィールド。
サマリー	実行時にジョブの結果を表示する読み取り専用フィールド。
期間開始	このジョブを実行する期間の開始時間。ジョブは、このフィールドに入力された時間の後に実行されます。 有効な時間値は、24 時間表記に基づく世界標準時です。
期間終了	このジョブを実行する期間の終了時間。ジョブは、このフィールドに入力された時間まで実行されます。ジョブがまだ完了していない場合、ジョブは一時停止し、次の期間の開始時に再開されます。終了時間は開始時間よりも後でなければなりません 有効な時間値は、24 時間表記に基づく世界標準時です。

5. フォームヘッダーを右クリックし、コンテキストメニューから [保存] を選択します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

レコードを保存すると、[ジョブをスケジュール] ボタンと [ジョブを削除] ボタンが表示されます。

6. [ジョブをスケジュール] をクリックしてジョブを実行します。
[期間開始] と [期間終了] フィールドで選択した時間の間でジョブが実行されます。ジョブが期間開始と期間終了の間に完了しなかった場合、ジョブは次の期間の開始時に続行されます。

   注:
   [予行演習] が選択されている場合でも、ジョブは 1 回のみ実行できます。同じジョブを再度実行するには、同じフィールド値を使用して Data Privacy ジョブを作成します。

7. オプション: 次のいずれかの機能を選択します。
   - ジョブのキャンセル：Data Privacy ジョブをキャンセルします。
   - 一時停止：ロールバックが選択されている場合、ジョブを一時停止し、記録をロールバックします。ロールバックコンテキストの 3 日間の有効期限が過ぎると、警告メッセージが表示されます。詳細については、「Data Privacy ジョブのロールバック」を参照してください。
   - 再開：一時停止したジョブを再開します。一時停止した場合、再開されたジョブのロールバックはサポートされません。ジョブをキャンセルし、Data Privacy ジョブを作成します。記録では、期限切れになっていないロールバックコンテキストが使用されます。

Data Privacy ジョブのロールバック

変更をロールバックできるように、ジョブやスクリプトなどのアクションでのデータベースの変更が取得されます。人為的なミスによって誤ったユーザー情報が匿名化された場合に、Data Privacy ジョブをロールバックします。ロールバックでは、Data Privacy ジョブのデータの匿名化解除が行われます。

概要

- ロールバックは、新しい RollbackType *REDACT* の RollbackContext の構成済み有効期間ごとに数日間に制限されています。Data Privacy ジョブに関連付けられた RollbackContext の有効期限が切れると、そのジョブではロールバック機能を使用できなくなります。
  - デフォルトでは、匿名化解除からのロールバックコンテキストは 3 日間保存されます。
  - デフォルトの有効期限は、新しい **RollbackType** *REDACT*. の **RollbackContext** において、データプライバシー管理者が 1 より大きい値に設定できます。Glide システムプロパティ `glide.rollback.expiration_days_redact` で値を設定します。詳細については、「ロールバックコンテキスト」を参照してください。

    システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

    参照してください。
- ロールバックは、[完了]、[キャンセル]、または [エラー] ステータスの Data Privacy ジョブで使用できます。
- ロールバックのサポートがオンになっている Data Privacy ポリシーで構成された sys_user 匿名化解除ジョブが成功するたびに、ロールバックコンテキストが作成されます。Data Privacy ジョブごとに設定できるロールバックコンテキストは 1 つだけです。

Data Privacy ジョブのロールバック

本番インスタンスの匿名化されたデータを使用する非本番インスタンスの Data Privacy ジョブを、データクラスまたはユーザージョブの匿名化前の状態にロールバックします。

始める前に

必要なロール：data_privacy_admin または data_privacy_processor、および admin

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

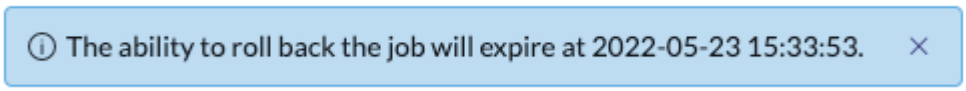
自動翻訳

手順

1. **data_privacy_processor** または **data_privacy_admin** ロールに昇格させます。
   ロールの昇格の詳細については、「特権ロールへの昇格」を参照してください。
2. 移動先 すべて > システムセキュリティ > **Data Privacy** > データプライバシージョブ.

   注:
   事前に、ロールバックをサポートする Data Privacy ポリシー構成を作成する必要があります。Data Privacy ポリシーの作成。

3. Data Privacy ジョブを作成し、ロールバックをサポートするプライバシー構成を選択します。
   「Data Privacy ジョブの構成」を参照してください。
4. データ匿名化のためのジョブをスケジュールします。
   - ジョブが実行されると、選択した構成でデータが匿名化されます。
   - 有効期限を知らせるメッセージがジョブに表示されます。有効期限内であれば、ジョブをロールバックできます。

5. **data_privacy_processor** ロールに昇格させます。
6. ロールバックする Data Privacy ジョブを開きます。
7. [ロールバック] を選択して、データの匿名化を解除します。

Data Privacy クローン

顧客データはソースからターゲットインスタンスに (通常は本番環境から非本番環境に) クローン作成されるため、機密データはターゲットインスタンスで匿名化されます。

Data Privacy 管理者がクローン作成後のポリシーを構成します。 ターゲットインスタンスでクローン後スクリプトが完了した後は、ユーザーには匿名化されたデータが表示され、元のデータにアクセスできなくなります。Data Privacy 管理者は、クローン作成時にターゲットインスタンスに適用する匿名化ポリシーを構成して、ターゲットインスタンスに元の機密データが含まれないようにすることができます。 実行される他のポリシーの中でのこのポリシーの順序を指定します。

注:
Data Privacy のクローン作成は、自己ホストインスタンスで使用できます。

Data Privacy のクローンには、次の追加の属性があります。

- Data Privacy プラグインは、ターゲットインスタンスで実行されるクローン後スクリプトを作成します。
- PostClone 構成用に作成された Data Privacy ジョブは、同じテーブルを含んでいない場合、並行して実行できます。
- アプリケーション順序が上位になっている Postclone 構成用の Data Privacy ジョブは、上位のジョブが他の下位のジョブに関連するテーブルを含んでいない場合、下位のジョブの前に開始されることがあります。
- Data Privacy プラグインを使用する場合、Data Privacy テーブルはデフォルトでクローンデータプリザーバーテーブルセットに含まれます。
- Data Privacy テーブル (dp_[table]) をクローン除外テーブルに追加しようとすると、そのテーブルを除外すべきではないことを示す警告が表示されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Data Privacy クローン要求の構成

Data Privacy クローン統合は、PostClone スクリプトを使用して構成され、ターゲット上で構成されたポリシー用の Data Privacy ジョブを作成して実行します。スクリプトが実行された後は、ユーザーに匿名化されたデータが表示され、元のデータにアクセスできなくなります。

始める前に
必要なロール：data_privacy_clone_processor、data_privacy_admin、および admin

手順

1. ソースインスタンスで Data Privacy プラグイン (com.glide.data_privacy) をアクティブにします。
   プラグインは、カスタマーサービス & サポートのみがインストールできます。
   Data Privacy PostClone スクリプトがインストールされます。
2. **data_privacy_admin** ロールに昇格させます。
   ロールの昇格の詳細については、「特権ロールへの昇格」を参照してください。
3. 移動先 システムセキュリティ > **Data Privacy** > プライバシーポリシー構成.
4. プライバシーポリシー構成を作成します。
   [データクラスのすべてに適用] 選択し、[クローン作成時に適用] を選択します。詳細については、「Data Privacy ポリシーの作成」を参照してください。
5. Data Privacy 構成をバックアップします。
6. Data Privacy 管理者として、クローン要求を送信します。

タスクの結果
Data Privacy PostClone スクリプトはターゲットインスタンスで実行され、PostClone スクリプトはターゲットインスタンス上に Data Privacy 連携ジョブレコードを作成します。連携ジョブは、ターゲットインスタンスで、各クローン後ポリシー用の Data Privacy ジョブを作成してアプリケーションの順序で実行します。 バックアップソースはターゲットインスタンスにクローン作成されます。Data Privacy PostClone スクリプトは、ターゲット上で構成されたポリシー用の Data Privacy ジョブを作成して実行します。

昇格された Data Privacy クローンプロセッサーは、ターゲットインスタンスにログオンし、dp_federated_job.list および dp_job.list でクローン後の連携ジョブのステータスを監視できます。

Data Privacy

Data Privacy ストアアプリは、最新の外観と操作性を備えたデータ分類とデータプライバシーのための Next Experience 更新です。Data Privacy ストアアプリは、Utah 以降でサポートされています。

Data Privacy は、概要、分類、および匿名化という複数のコンポーネントで構成されています。

概要

[概要] セクションを開始点として使用して、データと Data Privacy のコンプライアンスを管理します。詳細については、「Data Privacy の概要」を参照してください。

分類

データ分類は、データをカテゴリに整理して、後で使用するときに簡単に取得、ソート、および保存できるようにするプロセスです。分類システムを使用すると、機密性およびセキュリティポリシーの要件に焦点を当てることができます。データを分類して匿名化に使用できるようにします。データクラスと分類の詳細については、「データ分類」を参照してください。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

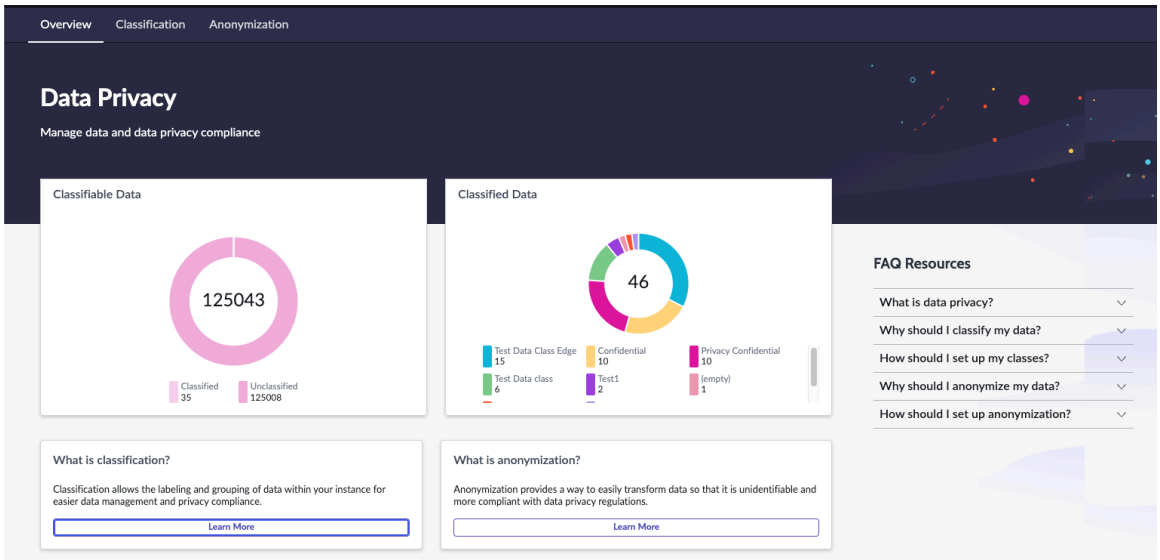
匿名化

すべてのユーザーまたは一部のユーザーの情報を匿名化し、手法を定義します。詳細については、「」を参照してください。

Data Privacy の概要

[概要] ホームページは、データと Data Privacy のコンプライアンスを管理するための開始点です。

概要ダッシュボードは、インスタンス内のデータ分類ジョブおよび匿名化ジョブの現在のステータスをレポートします。概要ダッシュボードでデータを表示し、分類可能なデータの量、利用可能なデータクラス、各クラスのデータ量、および匿名化ジョブの全体的なステータスを確認できます。分類されたデータはさまざまなカテゴリに分類されます。いずれかのチャートでサブカテゴリを選択すると、チャート全体でカテゴリが追加または削除され、数が調整されます。



分類可能なデータ (Classifiable Data)

インスタンス内の分類可能なデータレコードの合計数を表示します。この数は、分類されたデータの合計数と未分類のデータの合計に分類されます。これにより、管理者は使用可能な分類の機会をすばやく把握できます。

分類済みデータ (Classified Data)

インスタンス内の分類済みのデータレコードの合計数を表示します。 この数は、割り当てられた各データクラスの分類済みデータの合計数に分類されます。これにより、各エリアで分類されたデータの量をすばやく把握できます。

匿名化ジョブ

ユーザーおよびデータクラスジョブについて、非本番インスタンスで完了したジョブの現在処理中であるデータプライバシージョブを表示します。

詳細

[詳細] セクションでは、分類と匿名化を簡単に表示できるほか、プロセスを簡単に開始できます。

FAQ リソース (FAQ Resources)

Data Privacy を使用してインスタンスを保護する方法に関する追加情報については、分類と匿名化に関する製品学習リソースにアクセスしてください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Data Privacy のアクティブ化

データプライバシーにはデータ分類と匿名化が含まれ、ServiceNow Store からインストールされます。

始める前に

データの匿名化を使用するには、まず ServiceNow Vault エンタイトルメントを使用して Data Privacy (Classic) を有効にする必要があります。詳細については、「Data Privacy (Classic) のアクティブ化」を参照してください。

必要なロール：管理者

手順

1. 移動先 すべて > システムアプリケーション > 利用可能なすべてのアプリケーション > すべて > **Data Privacy**.
2. フィルター基準と検索バーを使用してアプリケーションを検索します。

   名前または ID でアプリケーションを検索できます。アプリケーションが見つからない場合は、ServiceNow Store へのリクエストが必要になることもあります。

   ServiceNow Store Web サイトにアクセスして利用可能なすべてのアプリを表示し、ストアにリクエストを送信する方法について確認してください。リリースされたすべてのアプリのリリースノート情報については、「ServiceNow Storeバージョン履歴のリリースノート」を参照してください。

3. リストからバージョンを選択し、[インストール] を選択します。

   表示されるインストールダイアログには、アプリケーションとともにインストールされている依存関係が一覧表示されます。

4. プロンプトが表示された場合は、ServiceNow Store へのリンクに従って、依存関係のエンタイトルメントを取得します。
5. オプション: 利用できるデモデータをインストールするには、[デモデータのロード] チェックボックスを選択します。

   (Optional) デモデータには、一般的なユースケース向けのアプリケーション機能を説明するサンプルレコードが含まれています。開発またはテストインスタンスで初めてアプリケーションをインストールする場合は、デモデータを読み込みます。

   > **重要:**
   > インストール時にデモデータを読み込んでおかないと、後から読み込むことはできません。

6. [インストール] を選択します。

データ分類

事前定義またはユーザー定義のデータ分類を使用して、データをタイプ別にグループ化します。ユーザーがデータ分類管理者または監査人ロールを持っている場合は、さまざまなデータクラスを管理したり、インスタンス内のさまざまなタイプのデータの現在のステータスを視覚的に分析したりすることができます。

データ分類を使用して次のサポートを有効にできます。

- Now Platform インスタンスでホストされているデータのタイプの可視性。
- プライバシー法を遵守し、金融サービスや医療機器の製造など、業界の規制要件を満たします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

データ分類

データ分類は、任意のテーブルの既存のディクショナリーエントリにデータ分類を手動で適用するスタンドアロンプロセスです。詳細については、「Data dictionary tables」を参照してください。

- ビジネスに適したデータ分類を行い、必要に応じて利用可能なデータクラスを変更できます。
- データを分類するときは、事前定義されたデータ分類を使用することも、独自に作成することもできます。事前定義されたデータ分類の使用はオプションですが、開始点として使用することをお勧めします。これらの事前定義されたデータ分類は、インスタンスにインストールできるデモデータに含まれています。
- 独自のデータ分類を作成する場合は、親と子のデータ分類を使用して階層型の階層システムを設計することもできます。

注:
データ分類 はドメイン分離をサポートしており、data_classification テーブル自体がプロセス分離されています。詳細については、「ドメイン分離と データ分類」を参照してください。

ユースケース

一般データ保護規則 (GDPR) は、個人が自分の個人データを制御できるようにすることを目的とした欧州連合の規制です。個人を特定できる情報などのデータ分類を使用して、個人データがインスタンス内のどこに保存されているかを特定できます。適切なセキュリティメカニズムを適用して個人データの漏洩を防ぐことで、組織は GDPR 要件を満たすことができます。

顧客情報を Now Platform に保存する場合は、現地のプライバシー法の規制の対象となるデータを追跡するために必要な個人情報 (PII) 分類コードを使用します。

制限付きデータ分類は、社会保障番号 (SSN) などの従業員の機密情報を格納する従業員テーブル列に適用できます。管理者と監査人は、概要ダッシュボードを使用して、データ分類が正しい列に割り当てられていることを確認できます。また、制限されたタイプの情報の分類の詳細を表示することもできます。

データ分類を作成する

[data_classification] テーブルに独自のユーザー定義のデータ分類を作成し、特定のテーブルの特定の列に割り当てることができます。新しいデータクラスを作成して、分類プロセスを開始します。

始める前に

必要なロール：data_classification_admin、admin

手順

1. 移動先 すべて > システムセキュリティ > **Data Privacy** > 分類.
2. [データクラスを追加 **(+Add data class)**] を選択します。

   注:
   ベースシステムには複数のデータクラスが含まれています。

3. フォームのフィールドに入力します。

フィールド	説明
クラス名	データ分類名。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

フィールド	説明
親クラス	このデータ分類が従属している親データ分類の名前。このデータ分類が親データ分類の子ではない場合は、フィールドを空のままにします。
説明	データ分類の説明。

4. [送信] をクリックします。
   新しいデータクラスが追加されます。データクラスが子の場合、左側のナビゲーションバーの親の下に表示されます。

分類済みデータ

事前定義またはユーザー定義のデータ分類を使用して、データをタイプ別にグループ化します。辞書 [sys_dictionary] テーブルの特定のテーブル列にデータ分類を割り当てます。データ分類を割り当てると、辞書データクラス [m2m_dictionary_dataclass] テーブルにエントリが作成されます。作成されたエントリは概要ダッシュボードで確認できます。

始める前に

必要なロール：data_classification_admin、admin

手順

1. [新規] を選択し、分類するテーブルからデータを割り当てます。
2. ドロップダウンからデータクラスを選択します。
3. 分類するテーブルと列を反映するレコードを選択します。
   特定のテーブルを簡単に見つけることができるように、テーブルのページごとに表示する追加の行を選択します。
4. [データを分類] を選択します。
   データは、[分類済みデータ] テーブルで [分類名] で分類されます。
5. データを表示するか、Excel、CSV、JSON、または PDF にエクスポートします。
   選択した形式でデータをダウンロードするか、メールで受信するかを選択します。

データの匿名化

匿名化は、データプライバシー規制に厳格に準拠するように、データを簡単に変換して識別不可能にする方法を提供します。

管理者は、本番インスタンスと非本番インスタンスの両方で匿名化プロセスを実行できます。Data Privacy を本番インスタンスで使用して、ユーザーを匿名化できます。データクラスの匿名化は、非本番インスタンスでのみ使用する必要があります。データ構造を保持すると、メールアドレスや物理アドレスなどのデータが、同様の形式で匿名化されたバージョンに置き換えられます。

管理者は、一般データ保護規則 (GDPR) の忘れられる権利 (RTBF) プロセスの一部として、匿名化を使用してユーザー情報を匿名化することもできます。詳細については、「https://gdpr-info.eu/art-17-gdpr/」を参照してください。

データプライバシーの匿名化セクションを使用して、プライバシーポリシーと手法を作成および表示し、プライバシーの一括割り当てを実行します。すべてのジョブと、その説明、使用されたプライベートポリシー、およびステータスを表示します。匿名化セクションにアクセスするには、管理者は最初に data_privacy_admin および data_privacy_processor ロールに昇格される必要があります。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

匿名化手法

匿名化手法は、データの匿名化方法を決定するために選択するオプションです。匿名化ジョブで参照する匿名化手法を作成する必要があります。プライバシー手法を関連する匿名化手法構成に関連付けるには、「」を参照してください。

匿名化ポリシー

匿名化ポリシーを構成して、データを匿名化するときに使用する Data Privacy 手法を指定します。詳細については、「匿名化ポリシーの作成」を参照してください。

匿名化ジョブ

匿名化ジョブは、これらすべてのコンポーネントを使用してデータを匿名化します。これらのジョブの詳細については、「匿名化ジョブの作成」を参照してください。

匿名化手法の作成

Data Privacy 手法構成を作成して、Data Privacy でデータを匿名化する方法をカスタマイズします。

始める前に
必要なロール：data_privacy_admin および admin

手順

1. **data_privacy_admin** ロールに昇格させます。
   ロールの昇格の詳細については、「特権ロールへの昇格」を参照してください。
2. 移動先 システムセキュリティ > **Data Privacy** > 匿名化.
3. [手法を表示 **(View techniques)]** を選択します。
   いくつかの事前定義された手法を選択できます。

手法	説明
選択的置換 (Selective Replace)	この手法では、文字列データを選択的に置換します。入力の開始インデックスと終了インデックスの間のすべての文字が、選択した文字に置き換えられます。マスクから除外する文字を指定できます。 ○ start_index：手法は指定された文字以降のデータをマスクします。空白のままにすると、最初の文字からマスクが開始されます。 ○ end_index：手法は文字列の先頭から指定された文字までのデータをマスクします。空白のままにすると、最後の文字でマスクが終了します。 ○ exclude_char：マスクから除外する文字を定義します。 ○ replacement_char：マスクに使用する文字を定義します。何も指定しない場合、デフォルトでアスタリスク (*) が使用されます。
静的置換 (Static Replace)	この手法では、値を静的な値に置換します。文字列、数値、および日付データでこの手法を使用できます。 ○ date_time_value：日付値をこの日付に置き換えます。yyyy-MM-dd HH:mm:ss 形式を使用します。 ○ date_value：日付値をこの日付に置き換えます。 yyyy-MM-dd 形式を使用します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手法	説明
	○ number_value：数値をこの数値に置き換えます。 ○ string_value：文字列値をこのテキストに置き換えます。
ランダム置換	この手法では、値をランダムに生成された値に置換します。文字列および数値データでこの手法を使用できます。
削除	この手法では、値を削除して空の (null) 値に置き換えます。
アクションなし	この手法はプレースホルダーです。選択されている場合、フィールドは変更されません。
選択的 X で置換	文字列データを変換し、機密性の高い文字を選択的に文字 X に置き換えます。 **注:** のデータ データディスカバリー の概要パターンのデフォルトの手法。
データパターンの匿名化	は、基礎となるコンテキストを損なわずに、非構造化データフィールド内で検出されたデータパターンのみを匿名化します。 **注:** この手法の設定は、 データディスカバリー の概要のデータパターン匿名化手法の設定を参照します。

4. 事前定義された手法を使用しない場合は、[カスタム手法を追加 **(Add custom technique)]** を選択します。
5. [手法をカスタマイズ **(Customize technique)]** フォームのフィールドに入力します。

フィールド **1**	説明
基本手法	カスタム手法は事前定義された手法に基づいているため、事前定義された手法を選択します。
手法名	手法の名前を入力します。
手法の説明	手法の説明を入力します。

6. [次へ] を選択します。
7. 手法のパラメーターを入力します。
使用可能なパラメーター化された値は、選択したプライバシー手法によって異なります。[アクションなし] および [削除] 手法にはパラメーター化された値はありません。

基本手法のプライバシーのパラメーター化された値

基本手法	プライバシー手法のパラメーターの値	説明	デフォルト値
選択的置換 (Selective Replace)	end_index	手法は文字列の先頭から指定された文字までのデータをマスクします。空白のままにする	(空)

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

基本手法	プライバシー手法のパラメーターの値	説明	デフォルト値
		と、最後の文字でマスクが終了します。	
選択的置換 (Selective Replace)	exclude_char	マスクをスキップする文字。この値に使用できるのは 1 文字のみです。複数入力した場合は、最初の文字が使用されます。	(空)
選択的置換 (Selective Replace)	[replacement_char]	選択的置換を使用して値を置換するときに使用する文字。	他の値が入力されていない場合は、アスタリスク (*) が使用されます。
選択的置換 (Selective Replace)	start_index	手法は指定された文字以降のデータをマスクします。	空白のままにすると、最初の文字からマスクが開始されます。
静的置換 (Static Replace)	date_time_value	日時値をこの日付に置き換えます。yyyy-MM-dd HH:mm:ss 形式を使用します。	1988-11-11 10:10:10
静的置換 (Static Replace)	date_value	日付値をこの日付に置き換えます。 yyyy-MM-dd 形式を使用します。	1988-11-11
静的置換 (Static Replace)	number_value	[数値] の値をこの数値に置き換えます。	1234567
静的置換 (Static Replace)	string_value	文字列値をこのテキストに置き換えます。	TEXT123
ランダム置換	preserve_data_length	データ長を保持する場合は **true** に設定します。匿名化されたデータは、元のデータと同じ長さになります。	true

8. [カスタム手法を作成 **(Create Custom Technique)]** を選択します。
   カスタム手法が匿名化手法に追加されます。

次のタスク
匿名化ポリシーを構成して、データを匿名化するときに使用する手法を指定するには、「匿名化ポリシーの作成」を参照してください。

匿名化ポリシーの作成

匿名化ポリシーを構成して、データを匿名化するときに使用する手法を指定します。

始める前に
Data Privacy 構成では、ユースケースに応じてテーブル、sys_user など、および列を匿名化するように定義し、データの匿名化中に使用されるパラメーター化される手法のタイプを指定します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

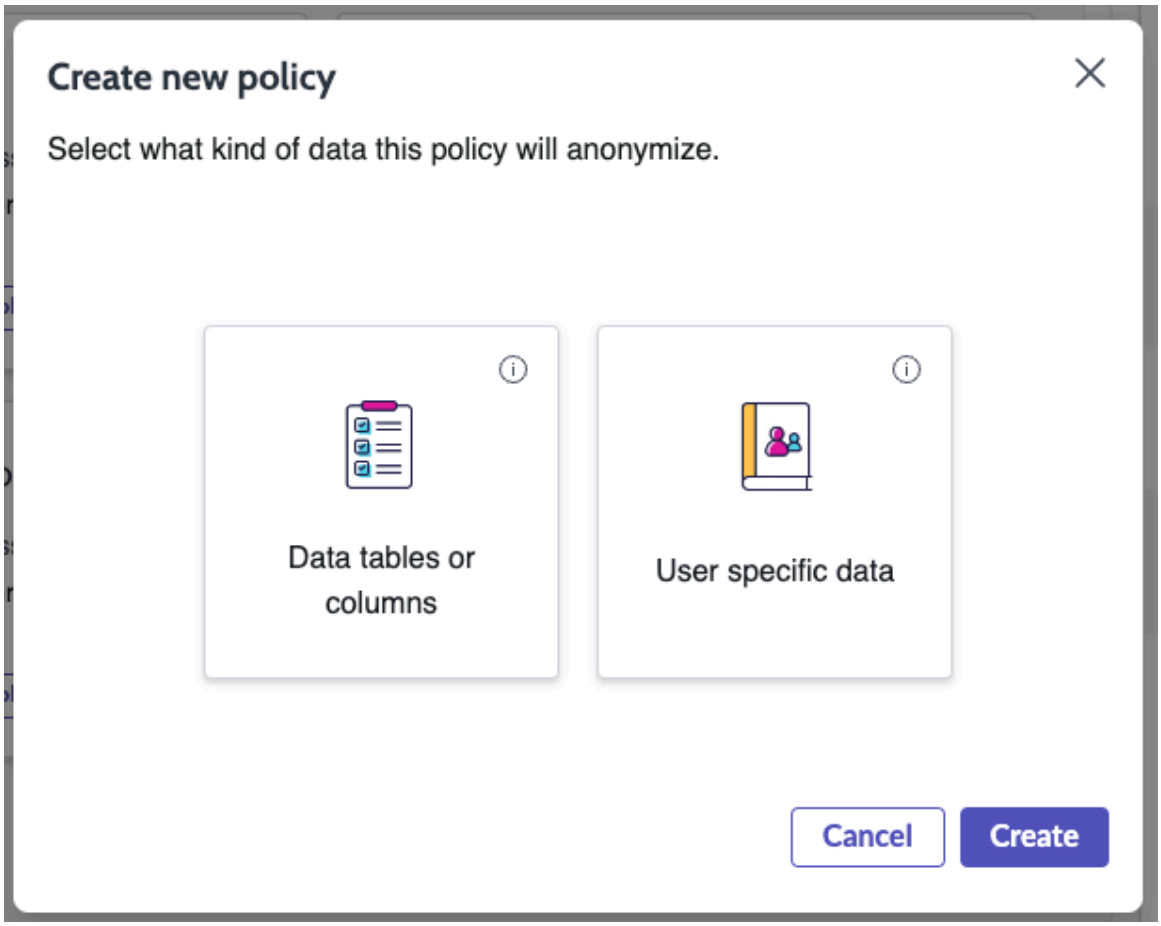
自動翻訳

注:
プライバシー構成を完了するには、最初に Data Privacy 手法構成を設定する必要があります。詳細については、「」を参照してください。

必要なロール：data_privacy_admin および admin

手順

1. **data_privacy_admin** ロールに昇格させます。
   ロールの昇格の詳細については、「特権ロールへの昇格」を参照してください。
2. 移動先 システムセキュリティ > **Data Privacy** > 匿名化.
   すべての匿名化ポリシーが表示されます。公開されたポリシーは、匿名化ジョブをスケジュールするために使用できます。
3. [新しいポリシーを作成] を選択します。
4. データテーブルまたは列またはユーザー固有のデータのどちらを匿名化するかを選択します。



   Data Privacy ポリシーは分類されたデータにのみ適用できます。データ分類の詳細については、「データ分類」を参照してください。

5. [作成] を選択します。
   ポリシー、[詳細を定義]、および [手法を割り当て **(Assign techniques)**]を完了するために必要な一連のステップがあります。ユーザー固有のデータのポリシーを定義する場合は、ユーザー参照の選択も必要です。
6. 新しい匿名化ポリシーの詳細を定義します。

自動翻訳

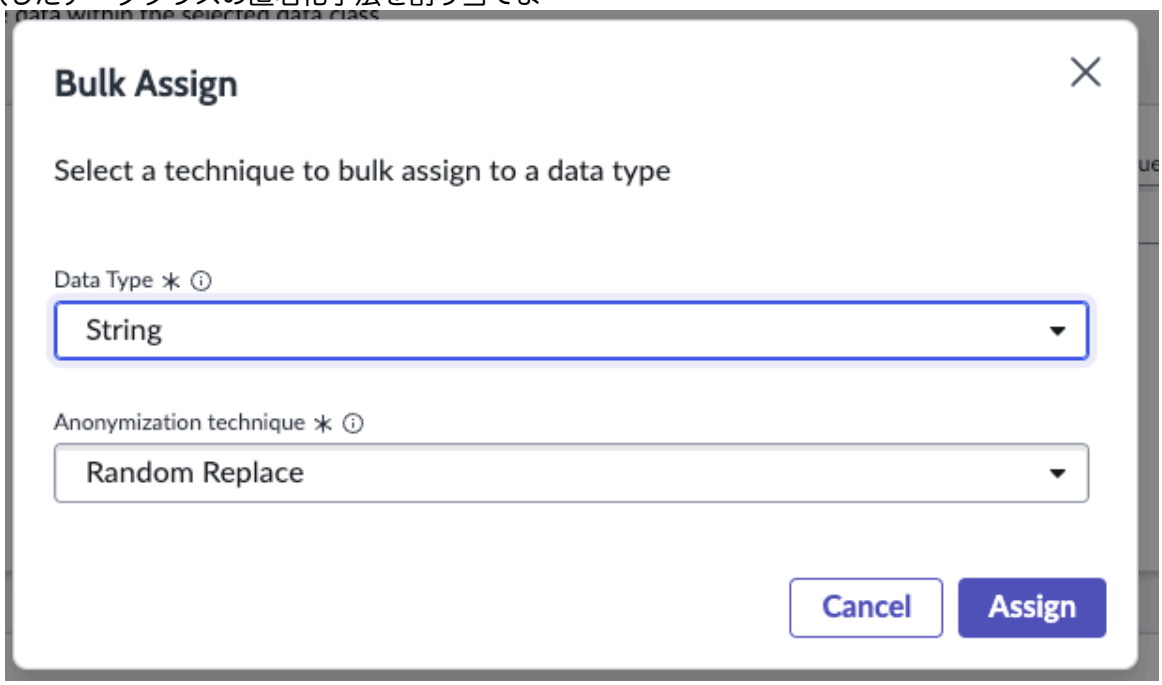
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

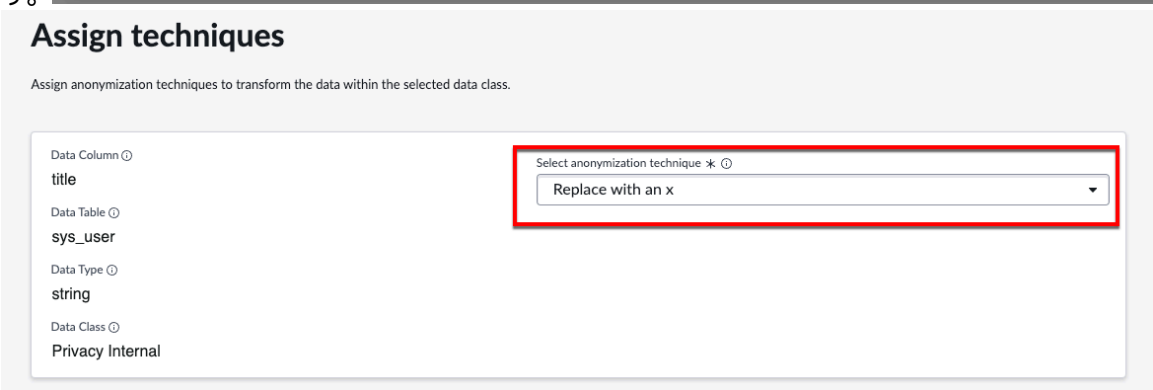
- [名前] フィールドにポリシー名を入力し、[説明] フィールドにポリシーの説明を入力します。
- [データクラス] フィールドで、このポリシーで使用するデータクラスを選択します。

> **注:**
> エントリを匿名化しない場合は、エントリを空のままにするのではなく、**[DoNothing]** 手法を選択します。[プライバシー手法構成] フィールドの値が空になっているポリシーは、Data Privacy ジョブで使用されるときに実行できません。

データクラスを選択した後に、定義されたデータクラスに対して返された各レコードの [手法を割り当て (Assign techniques)] フォームが表示されます。

7. 選択したデータクラスの匿名化手法を割り当てます。





8. オプション: [データパターンの匿名化] を選択した場合は、使用する匿名化手法を選択します。
9. オプション: データパターンの順序を設定します。
10. オプション: [テスト] ボタンを選択してポリシーをテストします。
11. [保存] を選択します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

12. [公開] を選択すると、スケジュール設定の匿名化ポリシーが更新され、匿名化ポリシーに戻ります。

> **注:**
> 匿名化ジョブのスケジュール設定には、公開されたポリシーのみを使用できます。

次のタスク
匿名化ジョブの作成。

データ匿名化クローン要求の設定

Data Privacy クローン統合は、PostClone スクリプトを使用して構成され、ターゲット上で構成されたポリシー用の Data Privacy ジョブを作成して実行します。スクリプトが実行された後は、ユーザーに匿名化されたデータが表示され、元のデータにアクセスできなくなります。

始める前に
Data Privacy PostClone スクリプトは、Data Privacy プラグイン (com.glide.data_privacy) の有効化とともにインストールされます。詳細については、「Data Privacy のアクティブ化」を参照してください。

必要なロール：data_privacy_clone_processor、data_privacy_admin、および admin

手順

1. ソースインスタンスで Data Privacy プラグイン (com.glide.data_privacy) をアクティブにします。
   Data Privacy PostClone スクリプトがインストールされます。
2. **data_privacy_admin** ロールに昇格させます。
   ロールの昇格の詳細については、「特権ロールへの昇格」を参照してください。
3. 移動先 システムセキュリティ > **Data Privacy** > 匿名化.
4. [新しいポリシーを作成] を選択します。
   詳細については、「匿名化ポリシーの作成」を参照してください。
5. データテーブルまたは列を選択します。
6. [作成] を選択します。
7. 名前を入力し、データクラスを選択します。
8. [クローン作成中にポリシーを有効にする **(Activate the policy during cloning)**] を選択します。
9. 複数のクローンポリシーがある場合に実行するポリシーの順序を選択します。
   アプリケーション順序が上位になっている Postclone 構成用の Data Privacy ジョブは、上位のジョブが他の下位のジョブに関連するテーブルを含んでいない場合、下位のジョブの前に開始されることがあります。
10. [続行] を選択します。
11. ポリシー構成を完了し、ポリシーを公開します。
12. Data Privacy 構成をバックアップします。
13. 匿名化ジョブをスケジュールします。
    詳細については、「匿名化ジョブの作成」を参照してください。
14. Data Privacy 管理者として、クローン要求を送信します。

タスクの結果
Data Privacy PostClone スクリプトはターゲットインスタンスで実行され、PostClone スクリプトはターゲットインスタンス上に Data Privacy 連携ジョブレコードを作成します。連携ジョブ

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

は、ターゲットインスタンスで、各クローン後ポリシー用の Data Privacy ジョブを作成してアプリケーションの順序で実行します。 バックアップソースはターゲットインスタンスにクローン作成されます。Data Privacy PostClone スクリプトは、ターゲット上で構成されたポリシー用の Data Privacy ジョブを作成して実行します。

昇格された Data Privacy クローンプロセッサーは、ターゲットインスタンスにログオンし、dp_federated_job.list および dp_job.list でクローン後の連携ジョブのステータスを監視できます。

匿名化ジョブの作成

非本番インスタンスでユーザーおよびデータクラスのジョブに匿名化されたデータを使用するように、本番インスタンスで Data Privacy ジョブを構成します。

始める前に

Data Privacy ジョブは、次の 2 つの匿名化ユースケースをサポートしています。

- 特定の sys_users の機密データ
- 特定のデータクラスの機密データ。

必要なロール：data_privacy_processor および admin

手順

1. **data_privacy_processor** ロールに昇格させます。
   ロールの昇格の詳細については、「特権ロールへの昇格」を参照してください。
2. 移動先 システムセキュリティ > **Data Privacy** > 匿名化.
3. 匿名化ポリシーで、ジョブで使用するポリシーの [ジョブをスケジュール] を選択します。
   匿名化ジョブをスケジュールするには、ポリシーが公開済みステータスである必要があります。

> ⚠ **警告:**
> 匿名化ジョブは非常に破壊的であり、ロールバック時にのみ取り消すことができます。ジョブをスケジュールする前に、処理されたレコードやテーブルなどのすべての情報を再確認してください。

4. フォームのフィールドに入力します。

Data Privacy ジョブのフィールド

フィールド	説明
使用されるポリシー (Policy used)	このジョブに使用する選択されたプライバシーポリシー構成の読み取り専用の名前。ポリシーに関する補足情報を表示するには、ポリシーを編集します。 プライバシーポリシー構成の詳細については、「匿名化ポリシーの作成」を参照してください。
ジョブの説明	ジョブの説明。
開始時間	このジョブを実行する期間の開始時間 (**HH:MM:SS** 形式)。
終了時間	このジョブを実行する期間の終了時間 (**HH:MM:SS** 形式)。終了時間は開始時間よりも後でなければなりません

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	ジョブは、このフィールドに入力された時間まで実行されます。ジョブがまだ完了していない場合、ジョブは一時停止し、次の期間の開始時に再開されます。
予行演習	ジョブをテストとして実行します。このジョブの実行時に影響を受けるレコードはありません。結果は、ジョブが実行された場合のように [ジョブ] リストに表示されます。 **注:** ロールバックを使用して Data Privacy ジョブを構成するときは、[予行演習] をオフにする必要があります。詳細については、「Data Privacy ジョブのロールバック」を参照してください。
ユーザーを選択	このジョブで匿名化する最大 10 人のユーザーを選択します。 **注:** この必須フィールドは、選択したプライバシーポリシーの条件でユーザーレコードを選択する必要がある場合にのみ表示されます。

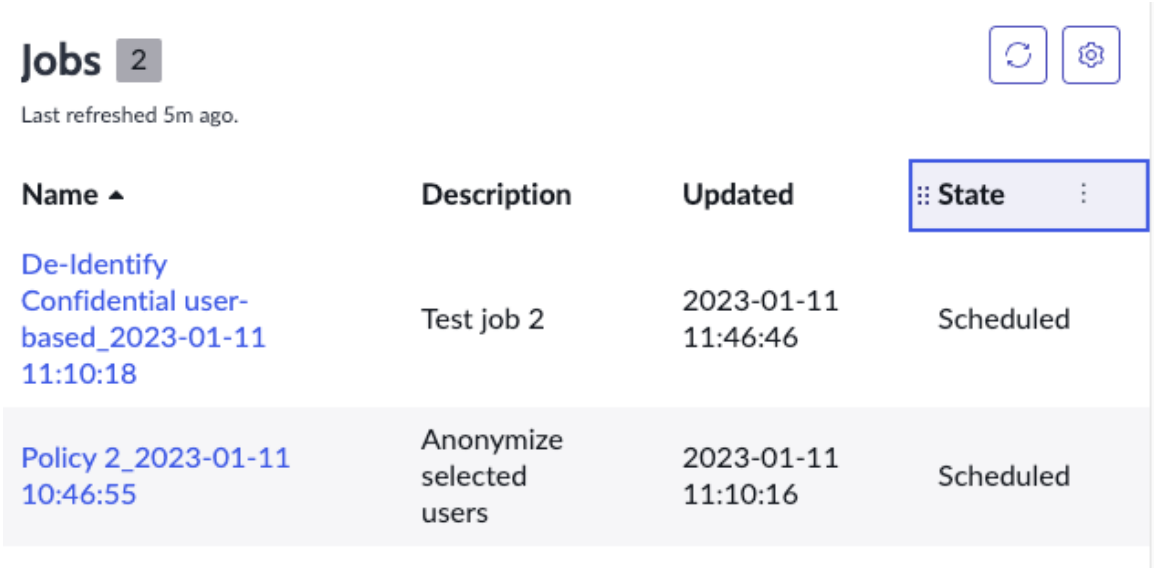
5. フォームで [ジョブをスケジュール] を選択して、匿名化をジョブキューに配置します。
[開始時間] と [終了時間] フィールドで選択した時間の間でジョブが実行されます。ジョブが期間開始と期間終了の間に完了しなかった場合、ジョブは次の期間の開始時に続行されます。

注:
[予行演習] が選択されている場合でも、ジョブは 1 回のみ実行できます。同じポリシーに基づいてジョブを再度実行するには、[ジョブをスケジュール] を選択し、同じフィールド値を使用してフォームに入力します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ジョブが [ジョブ] ペインに一覧表示されま



す。

フィールド	説明
名前	匿名化ジョブの名前。
説明	匿名化ジョブの説明。
更新日時	ジョブが最後に更新された日時。
ステータス	Data Privacy ジョブのステータス： ○ スケジュール済み：新しいジョブのデフォルトステータス。 ○ 完了：ジョブが選択したデータを正常に匿名化しました。 ○ キャンセル：ジョブは手動でキャンセルされました。 ○ エラー：ジョブの保存中に問題が発生しました。ジョブを再スケジュールするか、新しいジョブを作成します。エラーが引き続き発生する場合は、構成に問題がある可能性があります。 ○ ロールバック中：ジョブは匿名化をロールバックするように設定されています。 ○ ロールバック完了：匿名化ジョブのロールバックが正常に完了しました。 読み取り専用フィールド。

6. [ジョブ] ペインからジョブを選択して、ジョブサマリーを開きます。
ジョブがスケジュールされた後、[ジョブのキャンセル] および [一時停止] ボタンがジョブサマリーに表示されます。

ジョブスケジュールの追加フィールド

フィールド	説明
推定レコード数	この予行演習ジョブが実行される前に影響するレコードの推定数。読み取り専用フィールド
処理されるデータレコードの	このジョブによって影響を受ける個々のデータレコードの合計数。読み取り専用フィールド。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
合計数 (Total data records processed)	
処理されるデータテーブルの合計数 (Total data tables processed)	このジョブによって処理されたデータテーブルの合計数。読み取り専用フィールド。
ロールバックの残り時間 (Time remaining to rollback)	完了したデータ匿名化ジョブをロールバックしてデータを匿名化解除できる残り時間。読み取り専用フィールド。
処理されたユーザーの合計数 (Total users processed)	このジョブによって影響を受ける個々のユーザーレコードの合計数。読み取り専用フィールド。
ジョブのキャンセル	匿名化ジョブをキャンセルする場合に選択します。これはジョブの開始時間の前に選択する必要があります。 選択すると、ジョブステータスが [キャンセル] に更新されます。
一時停止	ロールバックが選択されている場合、選択するとジョブが一時停止し、記録がロールバックされます。ロールバックコンテキストの 3 日間の有効期限が過ぎると、警告メッセージが表示されます。 これは、ジョブの開始時間からジョブの終了時間までの間に選択する必要があります。 選択すると、ジョブステータスが [一時停止] に更新されます。
再開	一時停止したジョブを再開します。一時停止した場合、再開されたジョブのロールバックはサポートされません。ジョブをキャンセルし、Data Privacy ジョブを作成します。記録では、期限切れになっていないロールバックコンテキストが使用されます。 選択すると、ジョブステータスが [スケジュール済み] に更新されます。
エクスポート	Data Privacy ジョブの詳細の .PDF ファイルをダウンロードします。

Data Privacy ジョブのロールバック

変更をロールバックできるように、ジョブやスクリプトなどのアクションでのデータベースの変更が取得されます。人為的なミスによって誤ったユーザー情報が匿名化された場合に、Data Privacy ジョブをロールバックします。ロールバックでは、Data Privacy ジョブのデータの匿名化解除が行われます。

概要

- ロールバックは、新しい RollbackType *REDACT* の RollbackContext の構成済み有効期間ごとに数日間に制限されています。Data Privacy ジョブに関連付けられた RollbackContext の有効期限が切れると、そのジョブではロールバック機能を使用できなくなります。
  - デフォルトでは、匿名化解除からのロールバックコンテキストは 3 日間保存されます。
  - デフォルトの有効期限は、新しい **RollbackType** *REDACT*. の **RollbackContext** において、データプライバシー管理者が 1 より大きい値に設定できます。Glide システムプロパティ

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

glide.rollback.expiration_days_redact で値を設定します。詳細については、「ロールバックコンテキスト」を参照してください。

システムプロパティの追加または作成の詳細については、「Add a system property」を参照してください。

参照してください。

- ロールバックは、[完了]、[キャンセル]、または [エラー] ステータスの Data Privacy ジョブで使用できます。
- ロールバックのサポートがオンになっている Data Privacy ポリシーで構成された sys_user 匿名化解除ジョブが成功するたびに、ロールバックコンテキストが作成されます。Data Privacy ジョブごとに設定できるロールバックコンテキストは 1 つだけです。

Data Privacy ジョブのロールバック

本番インスタンスの匿名化されたデータを使用する非本番インスタンスの Data Privacy ジョブを、データクラスまたはユーザージョブの匿名化前の状態にロールバックします。

始める前に
必要なロール：data_privacy_admin または data_privacy_processor、および admin

手順

1. **data_privacy_processor** または **data_privacy_admin** ロールに昇格させます。
   ロールの昇格の詳細については、「特権ロールへの昇格」を参照してください。
2. 移動先 すべて > システムセキュリティ > **Data Privacy** > 匿名化.

   注:
   事前に、ロールバックをサポートする Data Privacy ポリシー構成を作成する必要があります。詳細については、「匿名化ポリシーの作成」を参照してください。

3. [完了] ステータスの匿名化ジョブを選択します。
   - ジョブが実行されると、選択した構成でデータが匿名化されます。
   - ジョブサマリーの [ロールバックの残り時間 **(Time remaining to rollback)**] フィールドに有効期限が表示されます。この期間内であれば、ジョブをロールバックできます。
4. [ロールバック] を選択して、データの匿名化を解除します。
   成功すると、ジョブのステータスが [Rollback_Complete] に更新されます。

データディスカバリー

データディスカバリー を使用して、クレジットカード情報、メール、社会保障番号などのインスタンス内の機密データを識別します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

Data Discovery の詳細

データ検出について学習します。

データ検出の構成

Data Discovery の構成についてサポートを受けます。

Data Discovery でのロール

Data Discovery のロールについて学習します。

データ検出結果

データ検出結果を確認します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

データディスカバリー の概要

データディスカバリー を使用して、クレジットカード情報、メール、社会保障番号などのインスタンス内の機密データを識別します。

データディスカバリー は、一連のテーブルでユーザー定義のジョブセットを実行します。ジョブはデータディスカバリー ダッシュボードでレビューするために機密情報を検索してレポートします。ジョブスケジュールは、実行時にすべてのアクティブなデータパターンとターゲットテーブルを自動的に使用します。

データディスカバリー には、データへのさまざまなアクセスレベルで事前に割り当てられたロールも含まれています。

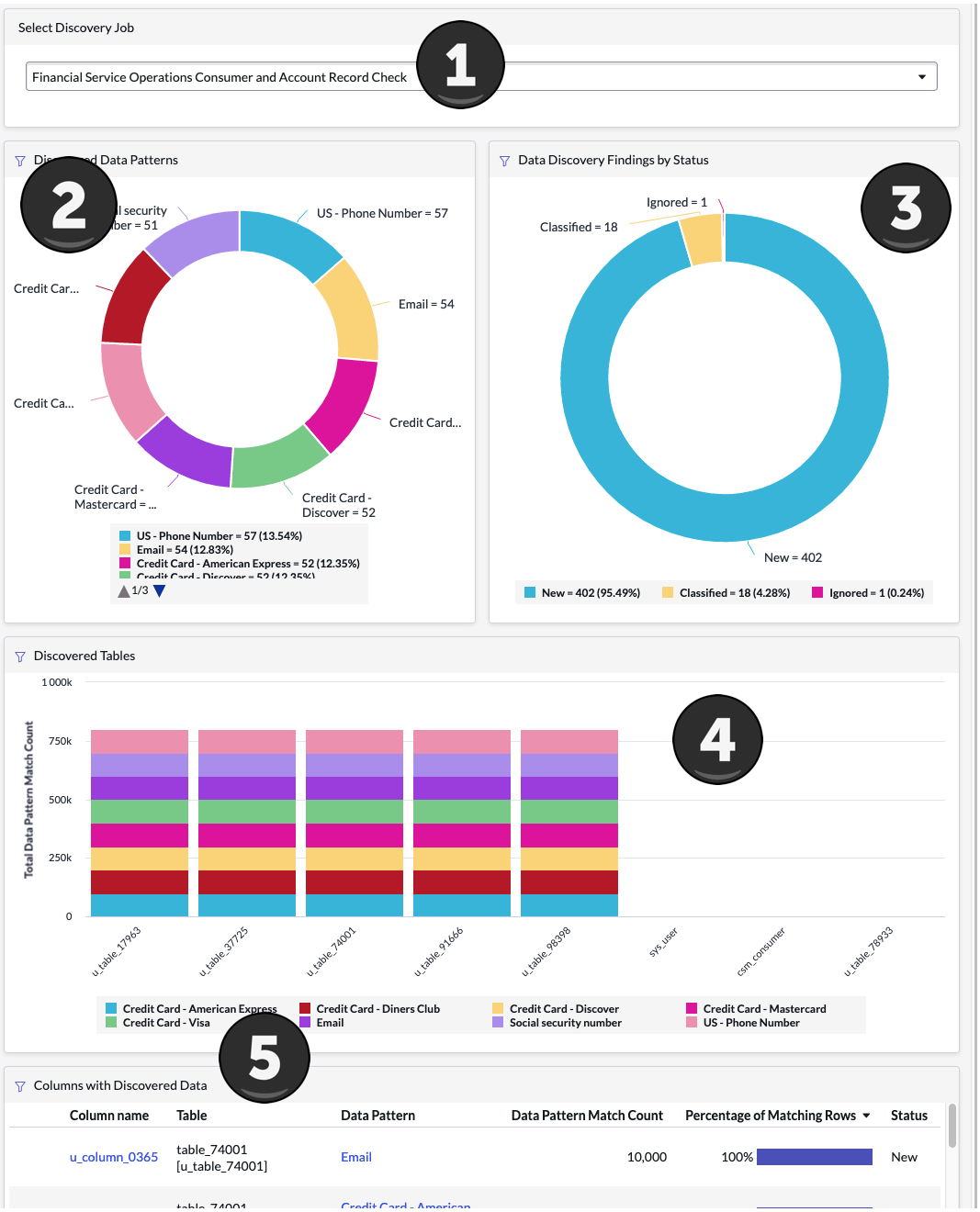
データディスカバリー ダッシュボードにアクセスします。

移動先 すべて > システムセキュリティ > **Data** Discovery（クラシック） > ダッシュボード ダッシュボードを表示し、 データディスカバリー 現在のジョブ結果を確認します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

データディスカバリー ダッシュボード



データディスカバリー ダッシュボードガイド

番号	セクションのタイトル	セクションの詳細
1	検出ジョブを選択 **(Select Discovery Job)**	
2	検出されたデータパターン **(Discovered Data Patterns)**	検出されたデータパターンの数と割合をタイプ別に表示します。
3	ステータス別のデータ検出結果 **(Data Discovery Findings by Status)**	検出されたデータパターンの数と割合をステータス別に表示します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

データディスカバリー ダッシュボードガイド (続く)

番号	セクションのタイトル	セクションの詳細
4	検出されたテーブル **(Discovered Table)**	検出されたパターンをグラフ別に表示します。
5	検出されたデータを含む列 **(Columns with Discovered Data)**	検出されたデータパターンを含む列の詳細を表示します。

データディスカバリー のアクティブ化

このアプリケーションは、データディスカバリー および関連する ServiceNow® Store アプリケーションとプラグインをインストールします (まだインストールされていない場合)。

始める前に

Data Discovery では、他の Now Platform とは別のサブスクリプションが必要です。

サブスクリプションを購入するには、ServiceNow アカウントマネージャーにお問い合わせください。サブスクリプションを購入すると、特定のプラグインが自動的にアクティブになります。有料プラグインが自動的にアクティブになっていない場合は、インスタンスの [すべてのアプリケーション] リストから手動でアクティブ化できます。

注:

サブスクリプションを購入する前に、Now Support サービスカタログ から非本番インスタンスを要求することによって、その機能を課金なしに評価できます。

必要なロール：admin

このタスクについて

次のアイテムが Data Discovery とともにインストールされます。

- ロール
- テーブル

インストールされるロールとテーブルの詳細については、「データディスカバリー ロール」および「デフォルトデータパターン」を参照してください。

手順

1. 移動先 すべて > システムアプリケーション > 利用可能なすべてのアプリケーション > すべて.
2. フィルター条件と検索バーを使用して、Data Discovery プラグイン (sn_data_discovery) を検索します。

   名前または ID でプラグインを検索できます。プラグインが見つからない場合は、ServiceNow 担当者から要求する必要があります。

3. [インストール] を選択して、[プラグインをアクティブにする] ダイアログボックスで、[アクティブ化] をクリックします。

   注:
   ドメイン分離と代理管理者がインスタンスで有効になっている場合、管理ユーザーはグローバルドメインに含まれている必要があります。それ以外の場合、次のエラーが表示されます： 別の操作が実行されているため、アプリケーションのインストールは利用できません：<プラグイン名> のプラグインの有効化。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

データディスカバリー の結果ページでデータを分類する

データディスカバリー の結果を通じて成功したすべてのジョブで見つかった機密データを分類します。

始める前に

必要なロール：data_discovery_admin

結果データを分類された状態で表示するには、ジョブの実行が正常に完了する必要があります。

このタスクについて

データディスカバリー の結果ページには、ジョブによって検出されたすべてのデータエントリが表示されます。結果ページでは、エントリを確認して分類に関連付けることができます。

手順

1. 移動先 システムセキュリティ > データ検出 **(Classic)** > データ検出結果.
2. 分類するエントリを選択します。
3. データディスカバリー の結果リストで、[分類] を選択します。
4. テーブルエントリに関連付けるデータクラスを選択します。
5. [分類] を選択します。

データディスカバリー ジョブ

データディスカバリー では、ユーザー定義のデータパターンとターゲットテーブルを使用して、ターゲット情報をレビューします。

データディスカバリー では、まず **[Data Discovery** ジョブ **(Data Discovery Job)]** セクションでジョブをスケジュールします。ジョブスケジュールが実行されると、現在のターゲットテーブルですべてのアクティブなデータパターンが検索されます。データディスカバリー ジョブの作成と構成の詳細については、「データディスカバリー ジョブの構成」を参照してください。

注:
パターンごとにテーブルあたり最大 10,000 レコードがスキャンされます。

データディスカバリー データパターン

[データパターン **(Data Patterns)]** セクションには、アクティブと非アクティブの両方の現在のすべてのデータパターンが表示されます。データパターンは、機密データの照合に使用される正規表現です。データパターンにアクセスして構成する方法の詳細については、「データディスカバリー パターンの構成」を参照してください。

注:
[アクティブなデータパターン **(Active Data Patterns)]** セクションには、アクティブなパターンのみが表示されます。非アクティブなパターンは表示されません。

ターゲットテーブル

[ターゲットテーブル] セクションには、ジョブで処理できるすべてのテーブルが一覧表示されます。ターゲットテーブルにアクセスするには、[ターゲットテーブル] を選択します。

次のテーブルはサポートされていません。

- sr
- sysx

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

- v
- sh
- syslog
- ua
- usageanalytics
- ecc
- clone
- jrobin
- pa
- sla_repair_log
- scan
- gcf
- fm_log
- log
- np$
- sn_data_discovery
- dp_configuration
- dp_federated_job
- dp_field_technique
- dp_job
- dp_job_summary
- dp_primary_reference
- dp_technique
- data_classification
- m2m_dictionary_dataclass

自動翻訳

データディスカバリー ジョブの構成

データディスカバリー ジョブを構成し、進行中のジョブのステータスを確認します。データディスカバリー ジョブは、ターゲットテーブルでパターンが実行されるタイミングを定義します。

始める前に

必要なロール：data_discovery_admin

手順

1. 移動先 システムセキュリティ > データ検出 **(Classic)** > データ検出ジョブ.
2. データディスカバリー ジョブリストで、[新規] を選択します。
3. データディスカバリー ジョブフォームで、フィールドに入力します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

データディスカバリー ジョブフィールド

フィールド	説明
名前	ジョブの名前。
説明	ジョブの説明。
スキャンタイプ	スキャンするエントリの数。可能なステータスは次のとおりです。 ○ サンプル: 10,000 エントリをスキャンします。 ○ 完全:すべてのエントリをスキャンします。
コンテキスト	スキャンされたパターン、ヒットしたターゲットテーブルエントリ、および経過時間に関するジョブの詳細。
ステータス	データディスカバリー ジョブのステータス。可能なステータスは次のとおりです。 ○ スケジュールの準備ができました：新しいジョブのデフォルトステータス。 ○ スケジュール済み：ジョブの実行がスケジュールされています。 ○ 対応中：ジョブはアクティブに実行されています。 ○ 完了：ジョブの実行が正常に終了しました。 ○ エラー：エラーのため、ジョブの実行が停止しました。 ○ キャンセル済み：ジョブがキャンセルされました。 ○ 一時停止：ジョブは一時停止されています。
サマリ	ジョブを実行した後の結果を表示します。
開始日	ジョブの開始日を設定します。
期間開始	このジョブを実行する期間の開始時間。ジョブは、このフィールドに入力された時間の後に実行されます。[期間開始] フィールドに入力された時間は、[期間終了] フィールドに入力された時間より前である必要があります。 **注:** 有効な時間値は、24 時間表記に基づく世界標準時です。
期間終了	このジョブを実行する期間の終了時間。ジョブは、このフィールドに入力された時間まで実行されます。ジョブがまだ完了していない場合、ジョブは一時停止し、次の期間の開始時に再開されます。[期間終了] フィールドに入力された時間は、[期間開始] フィールドに入力された時間より後である必要があります。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	注: 有効な時間値は、24 時間表記に基づく世界標準時です。

4. [送信] を選択します。
[ジョブをスケジュール] ボタンと [更新] ボタンが表示されます。
5. [ジョブをスケジュール] を選択してジョブを実行します。
[期間開始] と [期間終了] フィールドで選択した時間の間でジョブが実行されます。ジョブが期間開始と期間終了の間に完了しなかった場合、ジョブは次の期間の開始時に続行されます。
6. オプション: 次のいずれかの機能を選択します。
   - ジョブのキャンセル：ジョブをキャンセルします。
   - 一時停止：ジョブを一時停止します。
   - 再開：一時停止したジョブを再開します。

データディスカバリー パターンの構成

データディスカバリー パターンを構成し、現在のパターンを確認します。データディスカバリー パターンは、データをターゲットテーブルと照合するために使用する正規表現を定義します。

始める前に

必要なロール：data_discovery_admin

手順

1. 移動先 システムセキュリティ > **Data Discovery** > すべてのデータパターン.
2. データディスカバリー パターンリストで、[新規] を選択します。
3. データディスカバリー ジョブフィールドフォームで、フィールドに入力します。

データディスカバリー ジョブフィールド

フィールド	説明
内部スコープ	パターンのスコープ
説明	ジョブの説明
名前	データパターンの名前
アプリケーション	パターンのアプリケーションスコープ
式	データパターンを検出するために使用される正規表現
キーワード(オプション)	式の周囲で検索する特定の単語 (またはカンマ区切りの単語)。キーワード近接性とともに使用する必要があります

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	注: キーワードを使用して、パターンの追加コンテキストを検索できます。たとえば、キーワードを使用すると、生年月日と雇用日を区別するのに役立ちます (MM/DD/YY 形式が同じ場合)。
キーワード近接(オプション)	キーワードを検索する際の式からの距離。キーワードと共に使用する必要があります 注: デフォルトは 30、上限は 64 です

4. [送信] を選択します。
   - [テスト] ボタンを使用すると、データパターンリストを送信する前に正規表現をテストできます。

ジョブスケジュールで使用するには、データパターンをアクティブとして設定する必要があります。

5. 移動先 システムセキュリティ > **Data Discovery** > アクティブなデータパターン.
6. データディスカバリー のアクティブなパターンリストで、[編集] を選択します。
7. [利用可能なリスト **(Available Lists)**] からパターンリストを選択し、[選択したリスト **(Selected Lists)**] に移動します。

デフォルトデータパターン

データディスカバリー に含まれるデフォルトデータパターンの正規表現を確認します。これらのデフォルトデータパターンを使用して、さらに分類するためにテーブルエントリをフィルタリングできます。

データ検出に使用できるデフォルトのパターンは次のとおりです。

名前	正規表現
クレジットカード：Visa	\b4[0-9]{12}(?:[0-9]{3})?\b
クレジットカード：American Express	\b3[47][0-9]{13}\b
クレジットカード：Mastercard	\b(?:5[1-5][0-9]{2}|222[1-9]|22[3-9][0-9]|2[3-6][0-9]{2}|27[01][0-9]|2720)[0-9]{12}\b
クレジットカード：Diners Club	\b3(?:0[0-5]|[68][0-9])[0-9]{11}\b
クレジットカード：Discover	\b6(?:011|5[0-9]{2})[0-9]{12}\b
社会保障番号	\b(?!666|000|9\d{2})\d{3}-(?!00)\d{2}-(?!0{4})\d{4}\b
メール	\b[\w!#$%&'*+/=?`{\|}~^-]+(?:\.[\w!#$%&'*+/=?`{|}~^-]+)*@(?:[a-zA-Z0-9-]+\.)+[a-zA-Z]{2,6}\b

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

名前	正規表現
USA：電話番号	\b\(?([0-9]{3})\)?[-.]?([0-9]{3})[-.]?([0-9]{4})\b

ターゲットテーブルの構成データディスカバリー

ジョブで使用する データディスカバリー ターゲットテーブルを追加します。ターゲットテーブルでのみデータパターンがスキャンされます。

始める前に
必要なロール：data_discovery_admin

このタスクについて
ジョブが実行されると、 データディスカバリー すべてのアクティブなパターンを持つすべてのターゲットテーブルに対して実行されます。

手順

1. 選択 システムセキュリティ > **Data** Discovery（クラシック） > ターゲットテーブル.
2. [新規] を選択します。
3. [テーブル名] フィールドでターゲットテーブルを選択します。
4. [送信] を選択します。

データディスカバリー ロール

データディスカバリー ロールをアサインして、特定のデータタイプへのユーザーアクセスを制限できます。

ユーザーロール	アクセスロール
data_discovery_admin **注:** 管理者には、製品のインストール時にこのロールが自動的にアサインされます。	• データパターン ○ 作成 ○ 読み取り ○ 更新 ○ 削除 • アクティブなデータパターン： ○ 削除 ○ 読み取り • ジョブ： ○ 作成 ○ 読み取り ○ 更新 ○ 削除 ○ スケジュール ○ 一時停止

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ユーザーロール	アクセスロール
	○ 再開 ○ キャンセル • ターゲットテーブル： ○ 作成 ○ 読み取り ○ 書き込み
data_discovery_auditor	• データパターンの読み取り • アクティブなデータパターンの読み取り • データディスカバリー ジョブの読み取り • ターゲットテーブルの読み取り
data_classification_admin **注:** データ分類 admin ロールの詳細については、「データ分類 プラグインのデモデータをインストールする」を参照してください。	• データパターンの読み取り • アクティブなデータパターンの読み取り • データディスカバリー ジョブの読み取り • 有効になっている特定のパターン結果が分類されたときの data_classification テーブルの読み取り

データディスカバリー のジョブ結果

[データディスカバリー の結果 (Data Discovery Findings)] ページには、ジョブによって検出されたデータの詳細が表示されます。[結果 (Findings)] ページを使用してジョブの結果を確認し、データの分類を開始できます。

[データディスカバリー の結果 (Data Discovery Findings)] ページには、完了したジョブの後に次の詳細が表示されます。

列	説明
辞書エントリ	データが格納されていたターゲットテーブルの列
テーブル	データが見つかったターゲットテーブル
データパターン (Data Pattern)	データの検索に使用されるデータパターン
データパターン一致数 (Data Pattern Match Count)	データパターンに一致するデータエントリの数
合計行スキャン数 (Total Row Scan Count)	ジョブ中にスキャンされた行数
一致する行の割合 (Percentage of Matching Rows)	データパターンに一致するターゲットテーブルの行の割合
データディスカバリー ジョブ	ターゲットテーブルで使用されるジョブ
ステータス	エントリのステータス

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

データディスカバリー ジョブを実行すると、結果のステータスは [新規] になります。アクションが必要ない場合は、データをそのままにしておくことができます。これにより、ステータスが自動的に [無視] に設定されます。それ以外の場合は、ユーザー定義データ分類の作成などによりデータを分類し、データ分類 ツールを使用してデータの匿名化を準備することができます。

結果を統合

ジョブ結果は、[結果を統合] ボタンを使用して統合できます。2 つの個別のジョブ間で共有されるジョブ結果は、最後に実行されたジョブの下に統合されます。

注:
終了したフルスキャンジョブのみを統合できます

データディスカバリー のジョブ結果ページでデータを分類する

ジョブの結果ページから直接 データディスカバリー のデータを分類します。

始める前に
必要なロール：data_discovery_admin および admin

結果データを分類された状態で表示するには、ジョブの実行が正常に完了する必要があります。

手順

1. 検索項目 システムセキュリティ > **Data Discovery** > データ検出ジョブ.
2. 分類するエントリを選択します。
3. データディスカバリー の結果リストで、[分類] を選択します。
4. テーブルエントリに関連付けるデータ分類を選択します。
5. [分類] を選択します。

サービスプロバイダーの **Domain Separation**

ServiceNow プラットフォームを使用すると、サービスプロバイダー (SP) は、顧客に迅速なオンボーディングを提供し、コンプライアンスを満たし、Domain Separation を使用してデータを保護できます。クライアントデータ、プロセス、およびレポートをドメインと呼ばれる論理グループに分けることができます。SP は、誰がどのコンテンツを表示してアクセスするかをコントロールします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

詳細を読む

Domain Separation について説明します。

構成

Domain Separation を構成します。

参照

Domain Separation の詳細を取得します。

分析

Domain Separation の分析方法の詳細

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Domain Separation の概要

Domain Separation を使用すると、データ、プロセス、管理タスクを論理的に定義されるドメインに分けることができます。

Domain Separation は、以下の顧客にとって最適です。

- ビジネスエンティティ間で絶対的なデータ分離を適用する必要がある (データ分離)。
- 各ドメインのビジネスプロセス定義とユーザーインターフェイスをカスタマイズする (委任管理)。
- 単一のインスタンスでグローバルなプロセスとグローバルなレポートを維持する。
- サービスプロバイダー、顧客、パートナー、またはサブ組織間でデータを分離する。
- 顧客間で軽微なまたは中程度のプロセスの違いがある。

個別のインスタンスと Domain Separation の比較

Domain Separation がマルチテナントのサポートを提供している間は、マルチテナントはまだ単一のインスタンス内に含まれています。一部のグローバルなプロパティ、データ、およびプロセスは、すべてのドメインで共有されます。たとえば、システムのログインページの [記憶する] はグローバルであり、ドメインごとに指定できません。

すべてのシステムのプロパティを完全に分離する必要があり、グローバルレポートまたはグローバルプロセスを必要としない場合、インスタンスの分離が最適なオプションです。

データ分離

ドメインのメンバーは、そのドメインまたはドメイン階層の下位にある子ドメインに含まれるデータのみを表示できます。管理者が特定のドメインにアサインした場合を除き、デフォルトで、すべてのユーザーとすべてのレコードがグローバルドメインのメンバーになります。ユーザーまたはレコードをドメインにアサインすると、そのインスタンスはユーザーのドメインとレコードのドメインを比較して、そのユーザーがそのレコードを表示できるかどうかを判断します。

ServiceNow アプリケーションは、次の増分サポートレベルで定義されています。これらのレベルは、実際のユースケースとペルソナの観点に基づいています。

データ分離：テナントには、表示権限のあるデータのみが表示されます。テナントには、他のテナントデータへのアクセス権を付与できますが、アクセス権がない場合、テナントデータを照会することはできません。

UI 分離：ビュー、リスト、ラベルといった UI 要素のテナント固有のエクスペリエンスをサポートします。

ビジネスロジック分離：メール通知、ビジネスルール、クライアントスクリプト、UI ポリシー、UI アクションなど、テナント固有のシステムポリシーを作成できます。

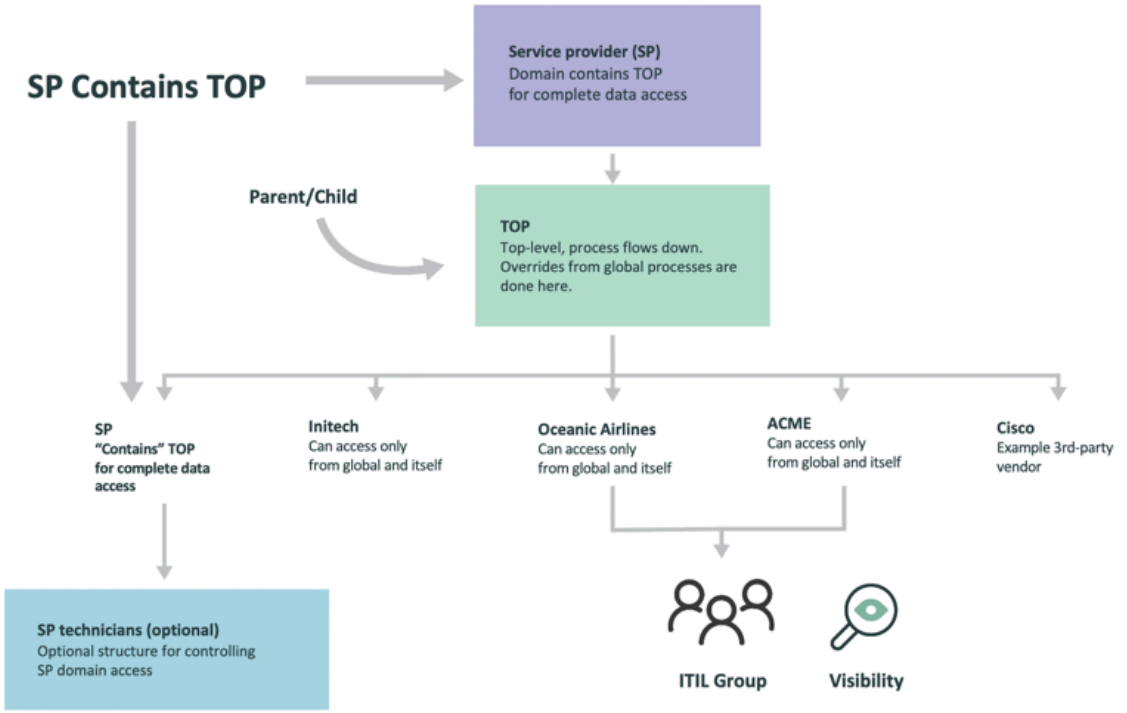
階層モデル：ネストされたマルチテナントであるため、親テナントが子テナントのリソースにアクセスできます。親テナントのビジネスロジックは子テナントに対して自動的に実行され、任意のレベルで上書きできます。

クロステナントインテリジェンス (ドメインスコープ)：追加のテナントデータにアクセスできるテナントのデータ、メタデータ、ビジネスロジック、および処理コンテキストを自動的に処理します。

一般的に、ドメイン階層の上位レベルで定義されたデータは、階層の下位レベルでは表示されません。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

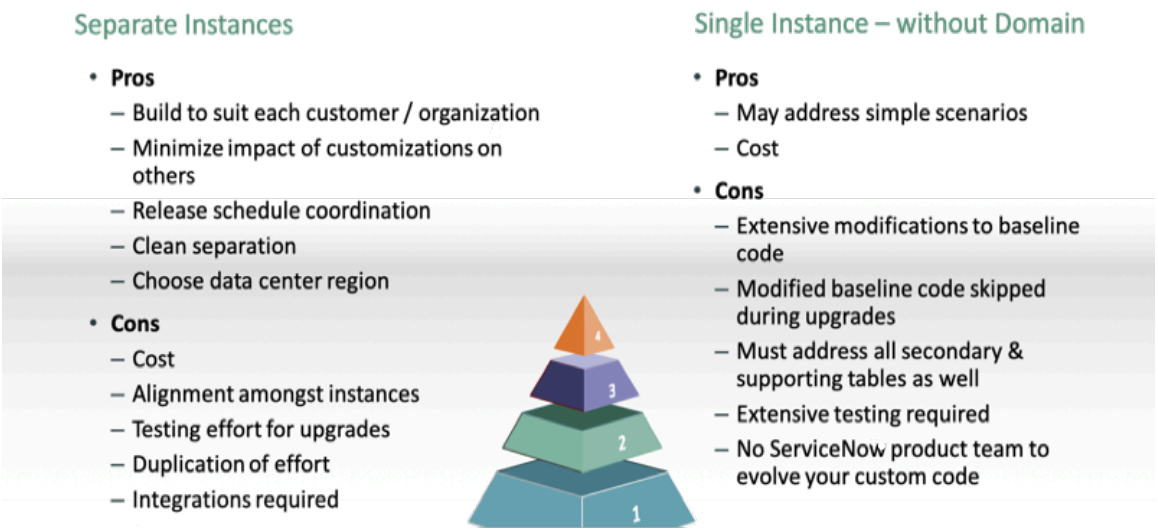


ドメインパスの移行

ドメインパスはすべての顧客に使用されます。ドメインの番号付けは使用されません。カスタマーサービス & サポートがアップグレードのサポートを行います。

Domain Separation の代替手段

個別のインスタンスは、Domain Separation の一般的な代替手段です。これにより、他の人にほとんど影響を与えることなく、顧客やステークホルダーの要件を満たすための柔軟性が高まります。



⚠ 警告:
Domain Separation をアクティブ化する前に、担当者に問い合わせて、お使いの環境に適していることを確認してください。Domain Separation は、一定レベルの管理オーバーヘッドを追加します。無効にすることはできますが、インスタンスから削除することはできません。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

関連情報

サービスプロバイダー向けのドメイン分離の推奨プラクティス

Domain Separation プラグイン

内部や外部の顧客に委任できる構成

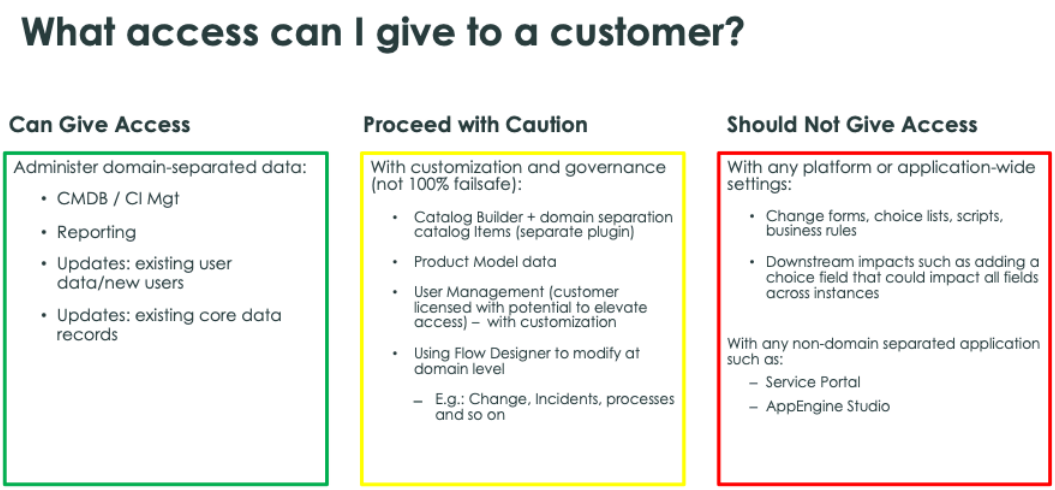
Domain Separation は、ServiceNow® サービスプロバイダー (SP) が顧客に提供するサービスを設定できるように設計されています。このトピックで詳しく説明されているいくつかのエリアを除き、顧客がこれらのサービスを自分で管理できるように設計されていません。

概要

SP の顧客は、ライセンスや他の顧客に影響を与えないドメイン内のデータを自分で安全に管理することができます。たとえば、顧客が新しいレポートを作成したり構成アイテムを管理したりすることは安全ですが、フィールド、選択肢、ビジネスルール、および同じインスタンス上の他の顧客に影響を与える可能性のあるその他のプロセスをカスタマイズすることは安全ではありません。

ServiceNow プラットフォームの ServiceNow ベースシステム管理ロールとそのアクセス制御は、インスタンスごとに 1 人の管理者チーム用に設計されています。たとえば、インスタンスのすべてのドメイン設定を管理し、新しいドメインを作成するために、domain_admin ロールが SP のリソースの 1 つに付与されます。ドメイン固有の管理タスクで SP は、顧客に特定のアクセス権を付与するために、必要に応じて新しい「顧客管理者」ロールとアクセス制御を作成する必要があります。

次の画像は、顧客が安全に実行できるさまざまなカテゴリの一般的な管理者機能の概要で



す。

🟢 アクセス権を付与可能

例：

- CMDB での CI データ管理
- レポートの作成
- 既存のユーザーデータの更新、またはロールのない新規ユーザー
- 部門、グループ、場所、コストセンター、ロールのない新しいグループ、新しい部門/コストセンター/場所などの既存のコアデータレコードを更新します。

🟡 注意して続行

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

例：

- カタログアイテム：顧客が更新できる顧客固有のカタログアイテムを作成するために、次の 2 つの機能を併用できます。カタログアイテムの Domain Separation (Domain Separation と Service Catalog) を使用することで、インスタンスオーナーは顧客のドメイン内にアイテムを作成することができます。インスタンスオーナーは、顧客が価格、説明、画像などの安全なフィールドを更新できるようにするロールを作成できます。カタログビルダー (Quebec リリースの新機能) を使用すると、SP 管理者チームは、規範的な UI エクスペリエンス内から顧客のドメインで新しいアイテムを作成するために、顧客に安全に配布できるアイテムテンプレートを作成できます。
- ユーザー/グループ管理：ユーザーレコードの作成と変更ができる「顧客管理者」ロールを安全に作成できますが、ロールの追加や削除はセキュリティとライセンスに影響を与える可能性があります。ベースシステムでは、顧客が安全に付与できるロールを細分化することはできません。グループの作成と変更についても同様です。グループ自体を変更することはできますが、ロールの追加や削除はコントロールする必要があります。
- Flow Designer ：ServiceNow フローデザイナー は、テーブルのプロセス (ワークフロー) を作成するために使用する構築ツールです。flow_designer ロールで、顧客はスクリプトなしにフローを構築できます。階層内で上位のドメイン内のすべてのフローを読み取ってクローンを作成できます。ドメイン内でフローの作成と変更ができます。ただし、これはサイロでは行えません。プロセスが互いにキャンセルし合ったり、他の競合が発生したりしないように、プロセスに影響を与える可能性のあるユーザーをグローバル管理者チームに追加する必要があります。

アクセス権を付与しない

選択フィールドの仕組みを理解することは、SP 管理者チームのみが選択フィールドを管理する必要がある理由を理解するのに役立ちます。

- 選択フィールドの構造：選択フィールドの値は sys_choice テーブルに格納され、テーブル、ドメイン、および言語に基づいてグループ化されます。

  たとえば、タスクの [ステータス] フィールドは、タスクを拡張するすべてのテーブルで使用できます。したがって、各テーブルが独自の値を持ち、それらの値にドメイン数を乗じ、ドメイン値に言語数を乗じることができます。

  すべてのテーブル、ドメイン、および言語の [ステータス] のすべての値が [ステータス] フィールドの値と見なされます。

- 選択フィールドの変更の仕組み： 選択フィールドが更新されると、そのフィールドのすべての値 (テーブル、ドメイン、言語) を含むペイロードが作成されます。このペイロードをインスタンスにインストールすると、フィールドの既存の値がすべて削除され、新しい値がロードされます。これにより、重複するエントリや残っていた無効な値がなくなります。

  そのため、ドメイン分離されたインスタンスで選択フィールドを直接更新する機能を顧客に提供することはできません。インスタンス全体に影響してしまうためです。また、選択フィールドに影響するインポートされた更新セットにより既存の選択肢が上書きされるため、本番インスタンスで選択肢を直接更新することもできません。場合により、選択フィールドでプロセス自体が実行される可能性があります。このプロセスは、顧客が選択フィールドを変更しようとすると中断されます。

詳細については、以下を参照してください。

- Exploring user administration
- ACL ルールを作成する
- NowLearning のサービスプロバイダーラーニングパス
- サービスプロバイダーの Domain Separation
- サービスプロバイダーの概念

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- Domain Separation のアプリケーションサポート
- Domain Separation のリリースノート

ドメインアサイン

デフォルトでは、Domain Separation は、テーブルとその拡張にドメインフィールドを追加します。

sys_domain フィールドをテーブルの辞書定義に追加することで、作成する任意の新しいテーブルに Domain Separation を拡張することもできます。デフォルトでは、システム専用ドメインは、適切な場合に、プラットフォームとベースラインアプリケーションテーブルを分離します。

警告:
ServiceNow では、予期しない結果が生じる可能性があるため、ドメイン分離プラットフォームテーブル (辞書エントリ [sys_dictionary] や辞書エントリの上書き [sys_dictionary_override] テーブルなどの sys_prefix を持つテーブル) は推奨されません。

各レコードには単一のドメインが割り当てられます。 そのドメインは **sys_domain**フィールドに格納されます。 いくつかのテーブルには、デフォルトで **sys_domain** 列があり、既にドメイン分離されています。

sys_domain フィールドの値には、次のいずれかでレコードに割り当てられたドメインが含まれます。

- ユーザーが所属する会社
- レコード作成時のビジネスルール
- レコードの作成時に使用されるモジュール
- レコードの作成時に使用されるフォームテンプレート
- 親レコードのドメイン
- ユーザーレコードに割り当てられたドメイン
- 作成したユーザーのドメイン

次のテーブルはドメイン分離されません。

- アクセス制御 [sys_security_acl]
- スクリプトインクルード [sys_script_include]
- システムのプロパティ [sys_properties]
- セキュリティ除外/包含リストエンティティ [sys_security_restricted_list]
- 辞書エントリ [sys_dictionary]
- 辞書エントリの上書き [sys_dictionary_override]

会社へのユーザー割り当て

管理者は、ユーザーを会社に割り当てることで、ユーザーをドメインにすばやく割り当てることができます。ユーザーがドメインに割り当てられると、レコードはユーザーのドメインを自動的に継承します。

たとえば、Bow Ruggeri を ACME 社に割り当てると、そのユーザーは自動的に ACME ドメインに割り当てられます。Don Goodliffe を Initech 社に割り当てると、そのユーザーは自動的に Initech ドメインに割り当てられます。作成したレコードは自動的に適切なドメインに追加されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ビジネスルールを使用したドメインの割り当て

管理者は、ビジネスルールを使用して、レコードの作成時にドメイン値を自動的に設定できます。ビジネスルールは **[sys_domain]** フィールドに値を設定する必要があります。管理者は、レコードのテーブルで **[sys_domain]** 列が使用可能であることを確認する必要があります。詳細については、「サービスプロバイダー向けのドメイン分離の推奨プラクティス」を参照してください。

モジュールを使用してドメインを割り当てる

管理者は、**sysparm_domain** URL パラメーターを使用して、モジュールから特定のドメインに新しいレコードを自動的に割り当てることができます。管理者は、**Argument** の値が sysparm_domain=ドメインのsys_ID であるモジュールを作成する必要があります。

フォームテンプレートを使用してドメインを割り当てる

管理者は、フォームテンプレートを使用して、特定のドメインに新しいレコードを自動的に割り当てることができます。管理者は、フォームに **sys_domain** フィールドを追加し、ドメイン値を選択する必要があります。たとえば、**sys_domain** フィールドを **TOP/ACME** ドメイン に設定すると、このテンプレートのすべてのレコードが TOP/ACME ドメインに自動的に割り当てられます。

テーブルのドメイン継承

デフォルトでは、関連レコードは親レコードのドメインを継承します。例：

- 変更タスクレコードは、親変更要求レコードのドメインを継承します。
- 問題レコードは、親インシデントレコードのドメインを継承します。

ユーザードメインに基づく自動ドメインアサイン

他のドメイン条件が適用されない場合、レコードはそれを作成したユーザーのドメインを自動的に継承します。

可視性ドメインと包含ドメイン

可視性ドメインは、特定のユーザーまたはユーザーのグループが表示できる内容をコントロールします。「包含」ドメインは、ユーザーのドメイン全体で表示可能な内容をコントロールします。

可視性ドメイン

「可視性ドメイン」要素は、あるドメインのユーザーが別のドメインのレコードにアクセスできるかどうかを決定します。アクセスする別のドメインのレコードの関連リストにあるユーザー [sys_user] とグループ [sys_user_group] レコードに可視性ドメイン要素を関連付けます。グループは、グループの可視性ドメインをメンバーに付与します。ユーザーがグループを離れると、グループの可視性ドメインは失われます。ユーザーに可視性ドメインを付与すると、ACL (アクセス制御リスト) ルールに基づいて、そのドメイン内のレコードにすべての権限が付与されます。

可視性ドメイン：

- ユーザーとドメインの関係であり、明示的に付与されます。
- 子ドメインではありません。
- ドメインピッカーでの選択でコントロールされません。可視性ドメインへのアクセス権を持つユーザーには、常にそのドメインとその子ドメイン内のデータが表示されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注:
可視性ドメインを過度に使用することはお勧めしません。可視性はユーザーがレコードにアクセスできるようにする 1 つの方法ですが、より強力にコントロールするには包含ドメインをお勧めします。

包含ドメイン

通常、親子関係はドメイン階層を定義します。包含ドメインでは、親子関係に関係なく、必要に応じてドメインを関連付けることができます。ただし、包含ドメインはドメインデータにのみ可視性を付与します。プロセスは包含関係の影響を受けません。

包含ドメイン：

- ドメイン間の多対多の関係です。
- 子ドメインがある場合があります。ドメインを選択すると、そのドメインとその子のデータを表示できます。
- ドメインピッカーでの選択でコントロールされます。

注:
ドメインレコードを開くと、スコープがそのレコードのドメインに設定されるため、子ドメインのみが表示されます。メニューから [ドメインスコープの切り替え] を選択して、関連リストに入力します。

ドメインの例を含める

ユーザーのホームドメインが A で、A ドメインにドメイン B と C が含まれている場合、それらはすべてピアドメインになります。これは、ユーザーがホームドメイン A にいるときにドメイン A、B、および C のデータが表示されることを意味します。ユーザーがドメインピッカーを使用してドメイン B に変更すると、ドメイン B のデータのみが表示されます。ユーザーがドメイン B またはドメイン C のレコードを直接操作すると、そのドメインのデータのみが表示されます。

可視性ドメインの例

ドメインの可視性を使用しているときに、Don Goodliffe がデータベースドメインに、Bow Ruggeri がネットワークドメインにいて、グローバルドメインにインシデントがない場合、データ分離により Don は Bow のインシデントにアクセスできません。

グループメンバーシップに基づく可視性ドメインの継承

ドメインテーブルをグループ [sys_user_group] テーブルに設定すると、ユーザーはグループメンバーシップに基づいて可視性ドメインを継承できます。

関連情報

包含クエリーとドメインアクセス

サービスプロバイダー向けのドメイン分離の推奨プラクティス

ドメインスコープ

ドメインスコープは、ユーザーがアクセスできるものとできないものを定義します。

ドメイン分離されたインスタンスでセッションを確立する場合、すべてのユーザーに 2 つのドメインスコープがあります。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- セッションスコープは、セッションの確立時にユーザーのユーザーレコードにリストされているドメインに設定されます。ユーザーは、ドメインピッカーからセッションのドメインスコープを手動で変更できます。
- レコードスコープはレコードのドメインを使用し、任意のレコードのフォームを表示すると有効になります。

デフォルトでは、レコードスコープがセッションスコープよりも優先されるため、上位レベルのドメインのユーザーは各レコードのデータとプロセスの制約に従います。ただし、これらのユーザーは、ドメインスコープを展開するか折りたたんで、他のドメインからのデータを表示または非表示にすることができます。たとえば、サービスプロバイダー (SP) ドメイン内のユーザーは、ACME ドメインなどの子ドメインへの可視性も持っています。ACME ドメインからのインシデントレコードを調べる場合、ユーザーはドメインスコープを展開して SP ドメインの値を表示するか、ドメインスコープを折りたたんでレコードの ACME ドメインに一致するレコード値のみを表示するかを選択できます。

注:
ユーザーは、ドメインの可視性によって明示的に付与されたドメインのデータに常にアクセスできます。

domain_expand_scope ユーザーロールを持つユーザーは、フォームの [ドメインスコープの切り替え] UI アクションからドメインスコープを選択できます。レコードスコープが有効になると、UI アクションをクリックしてセッションスコープを拡大し、ユーザーのドメインと子ドメインに基づいて使用可能なすべてのデータを表示できます。セッションスコープが有効な場合は、UI アクションをクリックしてレコードスコープを折りたたみ、現在のレコードのドメインと一致するデータのみを表示できます。

注:
レコードがグローバルドメイン内にある場合、またはユーザーのドメインがレコードのドメインと一致する場合、レコードにはドメインスコープを切り替えるための UI アクションは表示されません。

他のドメインからのレコード値の選択

複数のドメインを表示できるユーザーには、レコードのドメインとは異なるドメインからレコード値を選択するオプションがあります。

たとえば、サービスプロバイダーのサービスデスク担当者は、顧客に代わって問題を解決するために、特定のインシデントを自分自身に割り当てることができます。これを行うと、インシデントレコード自体が ACME などの子ドメインに関連付けられていても、インシデントの [アサイン先] フィールドに SP ドメインのユーザーが含まれる可能性があります。

別のドメインからレコード値を選択しても、レコードのドメインは変更されません。レコードは元のドメインを保持します。ユーザーが複数のドメインの値が含まれるレコードを表示する場合、表示される内容はユーザーのドメインの可視性によって決まります。

レコードの値の選択

これらの条件が満たされている場合	ユーザーはこれらの **UI** 要素にアクセスできます
ユーザーは、フィールドで参照されている現在のレコード	ユーザーは次のことができます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

レコードの値の選択 (続く)

これらの条件が満たされている場合	ユーザーはこれらの **UI** 要素にアクセスできます
のドメインにアクセスできます。	• 参照フィールドには、表示値が表示されます。たとえば、[アサイン先] フィールドにユーザー名が表示されます。 • 参照アイコンから関連レコードが表示されます。たとえば、[アサイン先] フィールドでユーザーのユーザーレコードが表示されます。 • 表示されているドメインから値を選択します。たとえば、SP ドメインと ACME ドメインのいずれかからユーザーを選択できます。
ユーザーは、フィールドで参照されている現在のレコードのドメインにアクセスできません。	ユーザーは次のことができます。 • 参照フィールドには、表示値が表示されません (これは、Madrid 以降のリリースで Domain Separation がアクティブにされており、ユーザーがそのレコードのドメインにアクセスできない場合に該当します)。 • レコードのドメインからのみ値を選択します。たとえば、ACME ドメインからのみユーザーを選択できます。

ドメインと関連会社

Domain Separation を使用すると、会社レコードに加えた変更を、会社に関連付けられたドメインと他のレコードにカスケードできます。

デフォルトでは、ユーザーは会社と同じドメインに自動的に割り当てられます。たとえば、ACME 社のすべてのユーザーは自動的に TOP/ACME ドメインのメンバーになります。

注:
admin ロールを持つユーザーは、自分のユーザーレコードを変更できるため、ドメインを変更できます。サービスプロバイダーは、委任管理を無効にするか、ユーザーに admin ロールが必要であることを確認するための承認プロセスを設定することができます。

会社のドメインを変更すると、次の関連レコードのドメインが会社の新しいドメインに合わせて自動的に変更されます。

- 所在地
- 部門
- グループ
- ユーザー

注:
インスタンスは、[管理対象ドメイン] チェックボックスをオンにしたレコードのドメインを自動的に変更しません。

ドメインの非アクティブ化および関連会社

ドメインを非アクティブ化すると、インスタンスでは次のアクションも自動的に完了します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

- ドメイン内のすべての会社を非アクティブにします。
- 非アクティブな会社に割り当てられたすべてのユーザーがログインできないようにします。

注:
非アクティブな会社のユーザーがログインしようとすると、「会社が非アクティブ - このインスタンスへのアクセスは許可されていません(Company inactive - your access to this instance is not authorized)」のようなエラーメッセージが表示されます。

たとえば、サンプルデータから ACME ドメインを非アクティブにすると、インスタンスによって ACME 社も非アクティブにされ、3 人のサンプルユーザーがロックアウトされます。

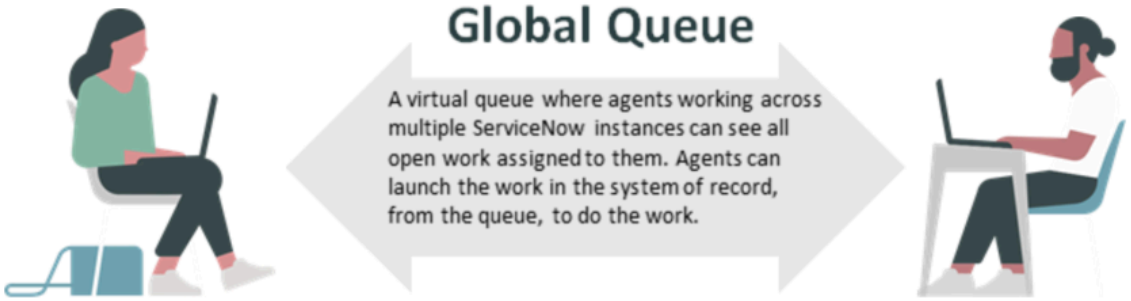
サービスプロバイダーの概念

サービスプロバイダーの概念は、一般的なユースケースの解決に役立つ既存の ServiceNow プラットフォーム機能を扱います。

グローバルキュー **v.2**

グローバルキューの概念は、複数のインスタンスに存在するタスクの単一の仮想ビューを提供します。このコンセプトでは、タスクやデータを複製することなく、複数のインスタンスに存在する作業の履行者ビューを提供するカスタムアプリケーションを作成します。

概要



複数のシステムのタスクを担当するエージェントを持つサービスプロバイダーは、データを中央のインスタンス (またはインスタンス間の「回転椅子」) に統合する傾向があります。この方法が適切な場合もありますが、構築と維持にコストと時間がかかります。また、この方法では、データが存在するすべてのインスタンスで、一般データ保護規則 (GDPR) などの潜在的な監査やデータ要件を考慮する必要があります。

グローバルキュー v.2 は代替手段です。この方法では、エージェントは、ログインしているインスタンスに主権データを保持することなく、単一のインスタンスから自分に割り当てられたデータを表示できます。たとえば、クライアントにデータの所在要件があり、他の国のエージェントによるアクセスが許可されている場合、プロバイダーはグローバルキュー v.2 を使用する「フォローザサン」ヘルプデスクを使用できます。

グローバルキュー v.2 の概念実証 の詳細については、ServiceNow ナレッジサイトを参照してください。

注:
Quebec リリース以降では、グローバルキューの概念実証がグローバルキュー v. 2 にアップグレードされています。

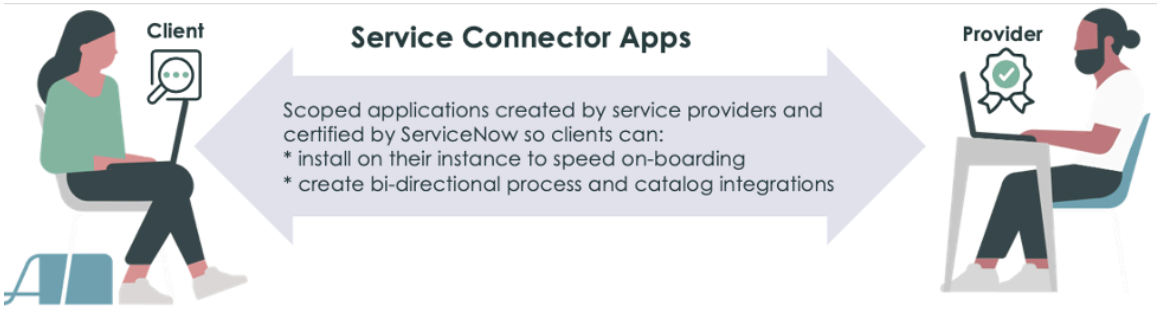
サービスプロバイダーコネクタ

サービスプロバイダーコネクタアプリケーションは、顧客がシステムとの統合に使用する ServiceNow ストアアプリケーションを作成するためのリファレンス設計です。サービスプロバイ

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

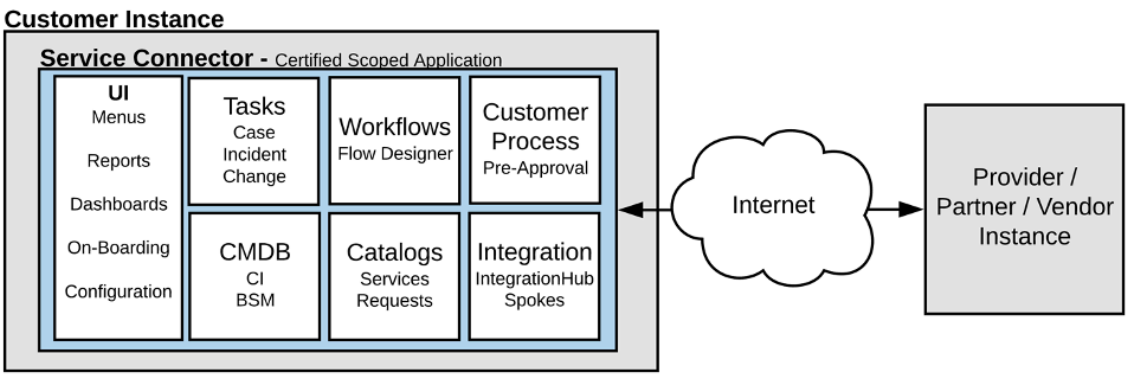
ダーアプリケーションは、オンボーディングを迅速化し、標準化された統合を実現するのに役立ちます。



サービスコネクタのメリット

サービスプロバイダー (ベンダー、サプライヤー、パートナー) がコネクタを公開すると、顧客のオンボーディングが迅速化されるため、請求が速くなります。統合されたインスタンスにより、生産性、ServiceNow エコシステムの可視性、およびパートナープログラムのメリットが向上します。具体的なメリットは次のとおりです。

- カスタム統合 (提供および維持に必要なサービスコストを含む) が不要になります。
- サービスは ServiceNow インスタンス内でプロバイダーによって定義されるため、カスタム統合の複雑さとコストが削減されます。
- ワークフローとカタログ要求は、プロバイダーのプロセスに先行する顧客のプロセスと承認により同期できるため、顧客は独自のプロセスに従うことができます。
- プロバイダーのインスタンスで顧客に対して作成または変更されたデータ (CI など) は、可視性を提供したり、プロセスで使用したりするために、顧客のインスタンスに戻すことができます。



主な機能

機能	説明
ユーザーインターフェイス	サービスコネクタには、少なくとも次の UI コンポーネントが含まれます。 • レポート/ダッシュボード – ペルソナによって可視性が高められた事前定義のレポートとダッシュボード。 • メニューとモジュール – 顧客は、わかりやすいメニュープロバイダー **XYZ** サービスを使用

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

機能	説明
	してアプリケーションを見つけることができます。 • ロール – 顧客によってアクセスをコントロールできるようにするため、すべてのコネクタにユーザーロールと admin ロールが必要です。例：「x_snc_xyz_user」または「x_snc_xyz_admin」。 • オンボーディング – 迅速なオンボーディングは、優れたカスタマーエクスペリエンスに不可欠です。また、顧客が必要なプロフェッショナルサービスを必要とせずに本番稼働できるように、迅速なオンボーディングを Playbook、Guided Setup、またはカタログアイテムによって組み込む必要があります (プロフェッショナルサービスを利用できますが、このサービスを利用せずにオンボーディングを行うことができます)。 • 構成 – データポイントをプロセスに組み込み、顧客が達成する必要がある通常のプロセス構成のほとんどを占めるようにする必要があります。そうすることで、プロフェッショナルサービスの必要性が可能な限り排除されます。 • ドキュメント – 詳細なドキュメントを提供することで、顧客満足度と使いやすさが向上します。 • サポート統合または連絡先情報 – 顧客は、問題、質問、または要求がある場合にサービスプロバイダーと連絡を取り合うための簡単な方法を必要としています。
タスク	インシデントやケース、変更、問題などのタスクをコネクタ内で事前定義する必要がある場合は、Service Exchange (legacy) アプリケーションを使用します。フローデザイナー と 統合ハブ を使用して構築された統合は、高レベルの復元力とパフォーマンスを確保するのに役立ちます。
CMDB	適切な ITIL プロセスに必要な CI などのコアデータ同期は、プロバイダーと顧客のインスタンス間で常に同期する必要があります。
ワークフロー	対障害弾力性とパフォーマンスを確保するには、すべてのワークフローを フローデザイナー で設計する必要があります。
カタログ	顧客が要求するプロバイダーのカタログは、レコード生成カタログとしてアプリケーションに含める必要があります。顧客のインスタンス内のアイテムで生成された要求は、プロバイダーのインスタンスと eBonding する必要があります。プロバイダーのワークフローは、要求を最

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

機能	説明
	新の状態に保ち、顧客のインスタンスに同期します。
カスタマープロセス	要求をプロバイダーのインスタンスと同期するメカニズムでは、要求がプロバイダーのインスタンスに送信される前に、顧客のプロセスがその要求とやり取りできるようにする必要があります。プロバイダーの処理中に、必要に応じて顧客のインスタンスに承認を送信できます。
統合	高レベルの復元力とパフォーマンスを確保するために、統合は フローデザイナー と 統合ハブ を使用して構築する必要があります。

サービスコネクタに含めることができるコンポーネント

コンポーネント	説明
Instance Data Replication (IDR)	レプリケーションが目的の場合： • プロセス統合に使用できるものの、ステータス移行に基づく複雑性統合ロジックによっては厳格すぎる場合があります。 • 詳細については、「Instance Data Replication」を参照してください。
IntegrationHub	プロセス統合が目的の場合： • フローの途中の複雑なステップまたは条件付きステップの一部として、プロセスの途中で簡単に挿入できます。 • 詳細については、「IntegrationHub」を参照してください。
グローバル作業キュー (仮想)	タスクフェデレーションが目的で、データを外部に保存できない場合： • エージェントが複数の ServiceNow インスタンスにまたがって作業していて、割り当てられたすべてのオープン作業を確認する必要がある場合に使用されます。 • 返される行数は 1000 未満に制限する必要があります。 • 詳細については、「グローバル作業キュー」を参照してください。
リモートテーブル	ストレージなしに外部データを使用することが目的である場合： • インスタンスをサードパーティソースまたは別のインスタンスに接続し、外部データを取得して必要に応じてメモリにキャッシュできるようにするために使用します。データは、

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

コンポーネント	説明
	グループ、ソート、集計、フィルターなどの読み取り専用の目的で、インスタンス内のテーブルとして扱われます。 • 詳細については、「リモートテーブルとスクリプトを使用した外部データの取得」を参照してください。
Flow Designer	プロセス設計が目標である場合 • 単一の設計環境でプロセスを自動化するために使用されます。プロセスオーナーは自然言語を使用して、承認、タスク、通知、およびレコード操作をコーディングなしで自動化できます。 • 詳細については、「Flow Designer」を参照してください

サービスコネクタの概念実証 の詳細については、ServiceNow ナレッジサイトを参照してください。

Domain Separation と一緒にインストールされるコンポーネント

いくつかのプラットフォームコンポーネントが、Domain Separation によって追加または変更されます。

ロール

ロール	説明
domain_admin	ドメインの作成、編集、削除ができます。

[sys_domain] フィールドへの追加

次のテーブルに [sys_domain] フィールドが追加されます。

[sys_domain] フィールドを含むテーブル

テーブル
sys_attachment
sys_user_has_role
sys_group_has_role
sys_email
sys_user_group
core_company
cmn_location
cmn_department
sys_gauge

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

[sys_domain] フィールドを含むテーブル (続く)

テーブル
sys_report
kb_feedback
sysapproval_approver
sys_user_grmember

タスクテーブルのフィールド

MSP 拡張は [task_for] フィールドをタスクテーブルに追加します。この参照フィールドはユーザーテーブルを参照します。

グループタイプのオプション

MSP 拡張は、グループテーブルのタイプフィールドにいくつかの新しいデフォルトオプションを追加します。ドメインをサポートするために、必要に応じてこれらのタイプを追加または更新します。

テーブル
セキュリティ
サポート
可視性

ビジネスルール

名前	テーブル	説明
ドメイン - アクティブ化/非アクティブ化	core_company	少なくとも 1 つの会社がアクティブな場合、関連ドメインをアクティブにします。関連するすべての会社が非アクティブな場合は、関連ドメインを非アクティブにします。
ドメイン - カスケード会社	core_company	会社のドメインとユーザー、グループ、部門、および場所との同期を維持します。
ドメイン - カスケードドメイン - メール	sys_email	メールのドメインと添付ファイルとの同期を維持します。
ドメイン - カスケードドメイン - グループ	sys_user_group	グループのドメインと継承されたロール (sys_group_has_role レコード) との同期を維持します。
ドメイン - カスケードドメイン -ナレッジ	kb_knowledge	ナレッジ記事のドメインと関連するフィードバックとの同期を維持します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

名前	テーブル	説明
ドメイン - カスケードドメイン - タスク	タスク	関連タスクと、wf_context、wf_executing、wf_history、添付ファイル、メール、task_sla とそのワークフロー、sysapproval_approver とそのワークフロー、および sysapproval_group とそのワークフローとの同期を維持します。
ドメイン - カスケードドメイン - ユーザー	sys_user	ユーザーのドメインとそのグループメンバーシップ (sys_user_grmember) およびロール (sys_user_has_role) レコードとの同期を維持します。
ドメイン - カスケードドメイン - バージョン	wf_workflow_version	ドメインと wf_activity および wf_transition の関連するワークフローバージョンとの同期を維持します。
ドメイン - 会社の非アクティブ化	domain	ドメインが非アクティブ化されている場合、関連する会社を非アクティブ化します。
ドメイン - デフォルト - タスク	タスク	ユーザーのドメインのタスクに基づいてタスクドメインを設定します。このドメインがグローバルである場合、代わりにドメインをデフォルトに設定します。
ドメイン - デフォルト - ユーザー	sys_user	ドメインがグローバルである場合、ユーザーのドメインをデフォルトに設定します。
ドメイン - グローバルドメインレコードの禁止	domain	global という名前のドメインが作成されないようにします。
ドメイン - 上書きコピー	sys_app_application	ドメインでアプリケーションが上書きされると、新しいアプリケーションにそのモジュールのコピーが作成されます。
ドメイン - 上書きコピー	sys_data_policy2	ドメインでデータポリシーが上書きされると、新しいデータポリシーのデータポリシールールのコピーが作成されます。
ドメイン - 上書きコピー	sys_gauge	ドメインでゲージが上書きされると、新しいゲージのゲージ数のコピーが作成されます。
ドメイン - 上書きコピー	sys_ui_action	ドメインで UI アクションが上書きされると、新しい UI アクションの UI アクションビューのコピーが作成されます。
ドメイン - 上書きコピー	sys_ui_list_control_embedded	ドメインで埋め込みリストコントロールが上書きされると、新しい埋め込みリストコントロールのクライアントおよびサーバースクリプトのコピーが作成されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

名前	テーブル	説明
ドメイン - 上書きコピー	sys_ui_policy	ドメインで UI ポリシードメインが上書きされると、新しい UI ポリシーの UI ポリシーアクションのコピーが作成されます。
ドメイン - ドメインを設定 - 承認	sysapproval_approver	承認されるレコードのドメインに基づいてドメインを設定します。
ドメイン - ドメインを設定 - 添付ファイル	sys_attachment	親レコードのドメインに基づいてドメインを設定します。
ドメイン - ドメインの設定 - CMDB_CI	cmdb_ci	CI のドメインを会社のドメインに設定します。
ドメイン - ドメインを設定 - 部門	cmn_department	部門のドメインを会社のドメインに設定します。
ドメイン - ドメインを設定 - ドメイン	domain	ドメインのドメインをそれ自体に設定します。
ドメイン - ドメインを設定 - メール	sys_email	親レコードのドメインに基づいてドメインを設定します。メールの親レコードは、インスタンスフィールドで指定されたレコードです。
ドメイン - ドメインを設定 -フィードバック	kb_feedback	ナレッジフィードバックのドメインをナレッジ記事のドメインに設定します。
ドメイン - ドメインを設定 - グループ	sys_user_group	グループのドメインを会社のドメインに設定します。
ドメイン - ドメインを設定 -グループ承認	sysapproval_group	承認されるレコードのドメインに基づいてドメインを設定します。
ドメイン - ドメインを設定 - グループロール	sys_group_has_role	グループロールのドメインをグループのドメインに設定します。
ドメイン - ドメイン	cmn_location	場所のドメインを会社のドメインに設定します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

名前	テーブル	説明
を設定 - 場所		
ドメイン - ドメインを設定 - タスク SLA	task_sla	タスク SLA のドメインをそのタスクのドメインに設定します。
ドメイン - ドメインを設定 - ユーザー	sys_user	ユーザーのドメインを会社のドメインに設定します。
ドメイン - ドメインを設定 - ユーザーロール	sys_user_has_role	ユーザーロールのドメインをユーザーのドメインに設定します。
ドメイン - ドメインを設定 - WF アクティビティ履歴	wf_history	親ワークフローコンテキストのドメインに基づいてワークフローアクティビティの履歴ドメインを設定します。
ドメイン - ドメインを設定 - WF コンテキスト	wf_context	参照されるレコードのドメインに基づいてワークフローコンテキストドメインを設定します (存在する場合)。
ドメイン - ドメインを設定 - 実行アクティビティ WF	wf_executing	親ワークフローコンテキストのドメインに基づいてワークフロー実行アクティビティのドメインを設定します。
ドメイン - タスクの設定 - 変更	change-request	チケットを変更要求に変換するときに、[要求元] フィールドの値をチケットのタスクに設定します。
ドメイン - タスクの設定 - インシデント	incident	チケットをインシデントに変換するときに、[問い合わせユーザー] フィールドの値をチケットのタスクに設定します。
ドメイン：デフォルトを検証	domain	1 つのドメインのみに [デフォルト] チェックボックスをオンにします。
ドメイン - プライマリを検証	domain	1 つのドメインのみに [プライマリ] チェックボックスをオンにします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

名前	テーブル	説明
ドメインサポートプラグインと一緒にインストールされるビジネスルール		
ドメインセットを変更	sys_dictionary	現在のドメインに設定されたドメインを設定します。
ドメインサポートプロパティ	sys_properties	ドメインクエリー方法 (ドメインパスまたはドメイン番号付け) に一致するようにシステムプロパティを設定します。

クライアントスクリプト

クライアントスクリプト	説明
ドメイン - 会社と場所を設定 (sys_script)	[インシデントの発信者] フィールドの変更を監視します。[会社] と [場所] フィールドにまだ値が含まれていない場合、スクリプトはこの情報を発信者レコードから追加します。[会社] と [場所] フィールドに既に値が含まれている場合、スクリプトは既存の値を保持します。
非アクティブ化されたスクリプト	
(BP) 場所をユーザーに設定	[インシデントの場所] フィールドを監視し、[場所] フィールドを発信者の場所に設定します。

関連情報

サービスプロバイダー向けのドメイン分離の推奨プラクティス

アプリケーションでのドメイン分離のサポート

多くの ServiceNow アプリケーションはベースシステムでドメイン分離をサポートしていますが、すべてのアプリケーションではありません。一部のサポートされているアプリケーションには、ドメインを分離できるデータ設定と管理設定に関する制限があります。これらの定義は、実際のユースケースとそれを使用するユーザーの観点から、Domain Separation のサポートレベルを示しています。

Domain Separation のサポートレベル

Domain Separation をサポートする ServiceNow アプリケーションは、データとデータルーティングの分離のみをサポートするか、高度なビジネスロジック分離機能があるか、アプリケーションのテナント (顧客) レベルの管理をサポートする可能性があります。ServiceNow アプリケーションは、次の増分サポートレベルで定義されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

サポートはありません

- ドメインフィールドがデータテーブルに存在している可能性がありますが、データを管理するロジックはありません。
- このレベルでは、ドメイン分割は考慮されません。

基本

- アプリケーションサービスプロバイダー (SP) のユースケースに合わせてデータが適切なドメインに送られるようにするビジネスロジックが存在します。
- アプリケーションでは、ユーザーインターフェイス、キャッシュキー、レポート、ロールアップ、集計など、すべて本番環境の実行時にドメインを使用します。
- インスタンスのオーナーは、複数のテナント間で機能するようにアプリケーションをセットアップできる必要があります。

サンプルユースケース：サービスプロバイダーがチャットを使用してテナント顧客のメッセージに応答する場合、クライアントがサービスプロバイダーの応答を確認できるようにする必要があります。

標準

- ベーシックレベルサポートを含みます。
- ビジネスロジック：サービスプロバイダー (SP) によって顧客ごとにプロセスを作成または変更できます。ユースケースには、単一のインスタンスでの複数のサービスプロバイダー顧客によるアプリケーションの正しい使用が反映されています。
- インスタンスのオーナーは、特定のアプリケーションで想定されているテナントあたりの最小実行可能製品 (MVP) ビジネスロジックとデータパラメーターを設定できる必要があります。

サンプルユースケース：管理者は、レコードを他のテナントに対してはクローズしないが、1 つのテナントに対してクローズする場合、コメントを必須にできる必要があります。

拡張機能

- ベーシックレベルと標準レベルを含みます。
- データドリブンプロセスにより、サービスプロバイダーの顧客は定義されたユースケースに基づくビジネスロジックを変更できます。これらの構成は UI ベースでフェイルセーフであるため、1 人の顧客による構成が別のユーザーに影響を与えることはありません。
- インスタンスのテナントは、それ自体、MVP (minimum viable product) ビジネスロジックとデータパラメーターを設定できる必要があります。アプリケーションの通常の関数では、このロジックとパラメーターが想定されます。

サンプルユースケース：共有環境のテナント顧客は、影響度、緊急性、または優先度のマトリクスに変更を加えて、ドメイン内で優先順位を設定できる必要があります。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注:
有効なドメイン **(*)**

ドメインフレームワークが使用されていなくても、プラットフォーム機能またはアプリケーションが SP のユースケースを効果的にサポートできる場合があります。その場合、ユースケースには Domain Separation のサポートが詳述されている必要があります。サポートレベルの後のアスタリスク (*) は、この種類の構成を示します。

サポートされている機能	基本	標準	拡張機能
ベースシステムのアプリケーションテーブルにドメイン列が存在します。	●	●	●
ドメイン固有の構成は、インスタンスオーナーによって管理されます。	●	●	●
テナントドメインは、独自のアプリケーションデータを管理できます。		●	●
アプリケーションプロパティは、必要に応じてドメイン対応です。		●	●
インスタンスオーナーは、ビジネスロジックとプロセスをドメイン分離することができます。		●	●
ビジネスロジックとプロセスはテナントドメインによって管理できます。			●

アプリケーションによるサポートレベル

製品スイート	アプリケーション	サポートレベル
Hyperautomation and low-code	App Engine Studio	サポートはありません
	Automation Center	基本
	Robotic Process Automation (RPA) ハブ	基本
	Table Builder	基本
	App Engine Management Center	サポートはありません
	Decision Builder	標準
	エンタープライズリソースプランニング統合	サポートはありません
	Enterprise Resource Planning Customization Mining	サポートはありません
	Next Experience UI Builder	基本

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

製品スイート	アプリケーション	サポートレベル
Customer Service Management	Communities	サポートはありません
	Customer Service Management	基本
	Release Management	基本*
	Order Management for Customer Service Management	基本
	Post-Sales Support	基本
	Domain separation in Workforce Optimization for Customer Service	基本
DevOps	DevOps	サポートはありません
	DevOps Config	
Employee Service Management	HR Service Delivery	基本*
	Health and Safety	基本
	Legal Service Delivery	基本
	Procurement Service Management (PSM)	サポートはありません
	Safe Workplace Suite	個々のアプリケーションサポートレベルについては、アプリケーションサイトを参照してください
	SharePoint Online 検索コネクター	基本
	Universal Request	基本
	ユニバーサルタスク	基本
	Workforce Optimization for HR	基本
Environmental, Social, and Governance Management	ESG Management	基本
Field Service Management	Field Service Management	基本
Governance, Risk, and Compliance	Business Continuity Management	基本
	Governance, Risk, and Compliance (GRC)	基本
	Operational Resilience	基本
業種別製品		
・	Financial Services Card Operations	基本
	Financial Services Deposit Operations	基本

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

製品スイート	アプリケーション	サポートレベル
	Financial Services Payment Operations	基本
	Intelligent Servicing for Fraud	
	Property and Casualty Insurance Servicing	
	Life Insurance Servicing	
	Insurance Claims	
	Financial Services Know Your Customer	
	Financial Services Credit Operation	
	Financial Services Document Processor	基本
・医療および生命科学	EMR Help	基本
	Healthcare and Life Sciences Service Management Core	基本
	Pre-Visit Management	基本
	Patient Support Services	基本
	Vaccine Administration Management	基本
・製造業	Manufacturing Process Manager	標準
	Operational Technology Manager	標準
	Operational Technology Vulnerability Response	標準
	Operational Technology Service Management	標準
・電気通信	Service Bridge	基本
	Order Management for Telecommunications, Media, and Technology	基本
	Telecommunications and Media Assurance Workflows	標準
IT Asset Management	Cloud Insights	サポートはありません
	Hardware Asset Management	拡張機能
	Software Asset Management	拡張機能
	Enterprise Assest Management	標準
Strategic Portfolio Management	Agile Development	基本*

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

製品スイート	アプリケーション	サポートレベル
	Alignment Planner Workspace	基本
	Application Portfolio Management	基本
	Cost Management	サポートはありません
	Demand Management	基本
	Financial Management	サポートはありません
	Investment Funding	基本
	Project Portfolio Management	基本*
	Release Management	基本*
	Scaled Agile Framework (SAFe)	基本*
	Test Management	基本*
	Goal Framework	基本
IT Operations Management	Cloud Provisioning and Governance	基本
	Agent Client Collector	基本
	Discovery	標準
	Event Management	基本
	Service Operations Workspace for ITOM	基本
	Health Log Analytics	基本
	測定基準インテリジェンス	基本
	Service Mapping	基本
	Cloud Migration Assessment	基本
	アクションライブラリ	サポートはありません
	Cloud Configuration Governance	サポートはありません
	Tag Governance	基本
	Cloud Insights Billing	サポートはありません
	Cloud Provisioning and Governance：Google Cloud	基本
	Cloud Provisioning and Governance Terraform	基本
	Cloud Operation Workspace	基本
	クラウド検出	標準
IT Service Management	Benchmarks	サポートはありません

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

製品スイート	アプリケーション	サポートレベル
	Change Management	基本
	Coaching	基本
	Continual Improvement Management	基本
	Contract Management	サポートはありません
	Expense Line	サポートはありません
	Incident Communications Management	標準
	Incident Management	標準
	Facilities Service Management	標準
	Incident Management	標準
	On-Call Scheduling	標準
	Asset Management	基本
	Problem Management	標準
	Procurement	標準*
	Product Catalog	標準
	Request Management	標準
	Service Catalog	標準
	Service Desk Call	基本
	Service Level Management	標準
	Service Portfolio Management	基本*
	Site Reliability Operations	基本*
	タスクの機能停止	基本
	Domain separation and Vendor Management Workspace	サポートはありません
	Walk-Up Experience	基本
モバイル構成およびナビゲーション	モバイル	基本
Now Intelligence	Dashboards	基本
	Performance Analytics	拡張機能
	Process Optimization	基本
	Reporting	基本
	User Experience Analytics	基本
Now Platform	管理、App Engine Now Platform 機能 ユーザーインターフェイス	

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

製品スイート	アプリケーション	サポートレベル
	Domain separation and Agent Chat	標準
	Advanced Work Assignment	標準
	AI Search	インデックス付きレコードからのドメイン制限を考慮した検索
	App Engine Studio	サポートはありません
	Application Management	サポートはありません
	アセスメント	標準
	Automated Test Framework	標準*
	ServiceNow 音声アシスト機能	
	Contextual Search	標準
	Configuration Management (CMDB)	標準
	コンテンツ管理システム	サポートはありません
	資格情報と接続	標準
	Data Certification	基本*
	データ分類	拡張機能
	Data Privacy	サポートはありません
	データ管理	基本*
	Delegated Development	サポートはありません
	Dependency Views	基本
	ドキュメントサービス	サポートはありません
	Dynamic Translation	基本
	Edge Encryption	サポートはありません
	Column Level Encryption	サポートはありません
	Column Level Encryption Enterprise	サポートはありません
	Cloud Encryption with Key Management	サポートはありません
	フィールド正規化	サポートはありません
	Flow Designer	標準*
	Guided Setup	サポートはありません
	ホームページの管理	基本*
	IntegrationHub	標準*
	サードパーティアプリケーションおよびデータソースとの統合	基本 + 標準
	Knowledge Management	標準

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

製品スイート	アプリケーション	サポートレベル
	Hermes Messaging Service	サポートはありません
	Managed Documents	サポートはありません
	MetricBase	基本
	Natural Laungage Understanding	基本 + 標準
	通知	標準
	ODBC Driver	基本*
	Orchestration	標準*
	Password Reset	標準
	プラットフォームセキュリティ	Domain Separation ランディングページ
	Data Privacy	サポートはありません
	Predictive Intelligence	標準
	プロアクティブトリガー	基本
	Process Automation Designer	基本
	リモートテーブル	サポートはありません
	スケジュール	基本
	スクリプトデバッガー	基本
	検索提案	サポートはありません
	Service Portal	サポートはありません
	Domain separation and Sidebar	標準
	ステータスフロー	サポートはありません
	Subscription Management	基本*
	Survey Management	基本*
	Task Intelligence	サポートはありません
	タイムカード	基本*
	UI Builder	標準
	仮想エージェント	基本
	Visual Task Boards	基本
	Web サービス	標準*
	Workflow	標準*
	ワークスペース	標準
Security Operations	Configuration Compliance	標準
	Configuration Data Management	基本

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

製品スイート	アプリケーション	サポートレベル
	IBM QRadar 違反の取り込み	基本
	Microsoft Graph Security API アラート取り込み統合	基本
	Security Incident Response	標準
	Threat Intelligence	標準
	Trusted Security Circles	標準
	Vulnerability Response	標準
Service Management	Facilities Service Management	標準
	計画メンテナンス	標準*
	プロアクティブトリガー	基本
	Now コードエディター	サポートはありません
	Workforce Optimization for ITSM	基本
	Vendor Management Workspace	基本

サービスプロバイダー向けのドメイン分離の推奨プラクティス

アプリケーションとサービスのドメイン分離を作成、実装、および維持できます。

ドメインの基本

ドメイン分離 (ServiceNow マルチテナントプラットフォームアーキテクチャとも呼ばれる) を使用すると、クロステナントインテリジェンスを使用した階層モデルをサポートする、アプリケーションデータ、ユーザーインターフェイス、およびビジネスロジックを単一の顧客インスタンスに分離できます。ビジネスロジックは、ドメイン分離の構成方法と、構成に影響するルールを記述します。

ドメイン分離のジャーニーを開始する前に、従うべき推奨事項がいくつかあります。必要に応じてトピックを選択するか、画像の下のリンクをクリックして順番にフォローしてください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Domain Separation の説明

Domain Separation を使用すると、アプリケーションデータ、UI、および ビジネスロジック (ルールやワークフローなど) を単一の顧客インスタンスに分離できます。これらの要素を論理的に定義されたドメインに分離することで、アプリケーションを使用するすべての顧客の特定の階層をサポートします。

ドメインの基本

Domain Separation は、ServiceNow マルチテナントプラットフォームアーキテクチャとも呼ばれ、インスタンスの管理にかなりのオーバーヘッドが追加されます。ただし、Domain Separation を正しく使用すると、効率が向上し、セキュリティが強化され、顧客のインスタンスのパフォーマンスが向上します。

一部のグローバル標準とプロパティ (システムプロパティやテーブルスキーマなど) をテナントごとに分離することはできません。

ドメインの分離を開始する前に、次のガイドラインをお読みください。

Domain Separation でできること

- データ分離：ドメインのテナントには、表示権限のあるデータのみが表示されます。テナントには、他のテナントデータへのアクセス権を付与できますが、アクセス権がないテナントデータを照会することはできません。
  - データレコードを更新しても、更新セットレコードは生成されません。
  - 統合に使用される顧客アカウントも含め、ユーザーには、アクセス権限があるドメイン内のデータのみが表示されます。
  - 顧客、エージェント、および履行者には、サポートする顧客と組織に関するデータが表示されます。
- UI 分離：ビュー、リスト、ラベルといった UI 要素のテナント固有のエクスペリエンスをサポートします。

自動翻訳

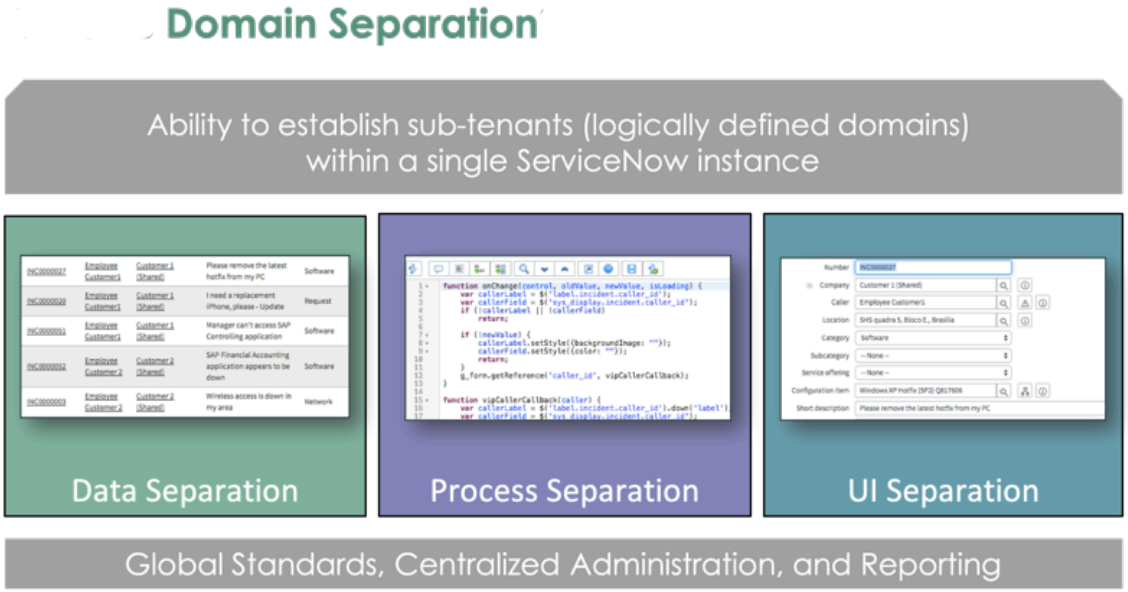
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- アプリケーションメニュー、リスト、フォーム、ダッシュボードなどのブラウザーベースのユーザーインターフェイスを上書きできます。基本的なプロセスロジックを保持したまま、特定のドメインまたは一連のドメイン用にカスタマイズすることもできます。
- サービスプロバイダーは、表示されるブランディングと UI 要素を変更して、個々の顧客のニーズを満たすことができます。

- ビジネスロジック分離：メール通知、ビジネスルール、クライアントスクリプト、UI ポリシー、UI アクションなど、テナント固有のシステムポリシーを作成できます。
- 階層モデル：マルチテナントがネストされるため、親テナントが子テナントのリソースにアクセスできます。親テナントのビジネスロジックは子テナントに対して自動的に実行され、任意のレベルで上書きできます。
- クロステナントインテリジェンス：追加のテナントデータにアクセスできるテナントのデータ、メタデータ、ビジネスロジック、および処理コンテキストを自動的に処理します。

Domain Separation の概要

次の図は、データの分割、プロセス、および UI の分離を示しています。これらの概念については、「推奨プラクティス」セクションで詳しく説明しています。



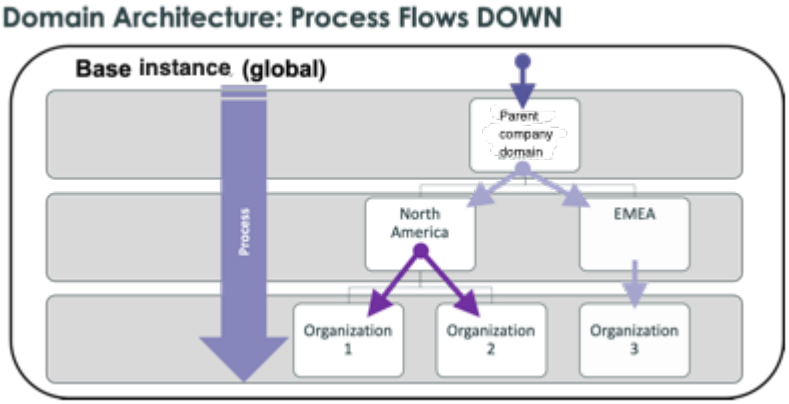
ドメインアーキテクチャ

ユーザーレコードには、ユーザーのホームドメインを表すドメイン値がアサインされます。ユーザーは、親ドメイン、ピアドメイン、または階層の他のブランチ内のドメインのデータにアクセスできません。

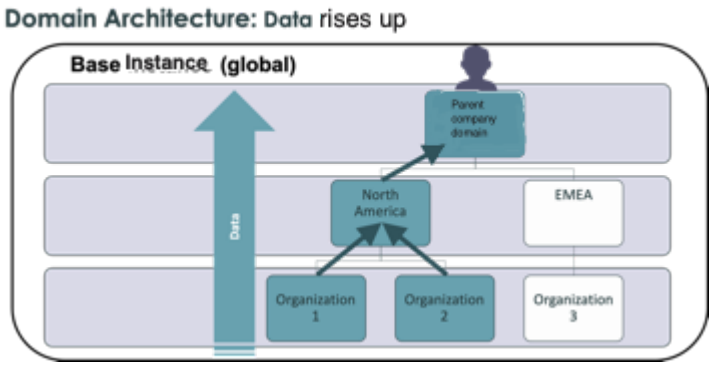
追加のドメインの可視性を付与する詳細オプションについては、「包含クエリーとドメインアクセス」を参照してください。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

次の図は、アーキテクチャプロセスが子ドメインにどのように移行するかを示して



います。



Domain Separation の価値提案

Domain Separation は、マルチテナントインスタンスアーキテクチャをサービスプロバイダーに提供し、そのクライアントに対して効率的かつ安全に製品を提供できるように設計されています。強力なユニバーサルプロセス標準、データ主導型のプロセス設計、厳格なガバナンス、および集中管理により、これらのメリットを最大限に活用できます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ドメイン分離のメリット

ドメインのテナントは、迅速な投資利益率、低い管理経費、およびインスタンスオーナーが提供するビジネスサービスの活用によるメリットを得ることができます。

メリットのクイックビューを以下に示します。

インスタンスオーナー	ドメインテナント
サービスプロバイダーの従業員の生産性	セキュリティを強化できます
プロセスデルタのみが維持されます	事前に構築されたプロセスと機能
管理効率	必要なスタッフの削減
クライアント統合数の削減	迅速なオンボーディング
アップグレード可能性と拡張性	最新リリースの活用
データ分離	インスタンスオーナーが提供するサービス
グローバルレポート	

Domain Separation の定義

Domain Separation (ServiceNow® マルチテナントプラットフォームアーキテクチャとも呼ばれる) を使用すると、クロステナント (顧客) インテリジェンスを使用して、アプリケーションデータ、UI、およびビジネスロジックを単一の顧客インスタンスに分離できます。

Domain Separation のプロパティ

ドメイン分離された ServiceNow アプリケーションは、次のプロパティで定義されます。

データ分離
: 顧客が表示権限を持つデータのみを表示できるようにします。顧客に他の顧客データへのアクセス権を付与できますが、アクセス権がない場合、顧客データを照会することはできません。

UI 分離
: ビュー、リスト、ラベルといった UI 要素の顧客固有のエクスペリエンスをサポートします。

ビジネスロジック分離
: メール通知、ビジネスルール、クライアントスクリプト、UI ポリシー、UI アクションなど、顧客固有のシステムポリシーをサポートします。

階層モデル
: 親テナント (顧客) が子顧客リソースにアクセスできるように、ネストされたマルチテナントをサポートします。親顧客のビジネスロジックは子顧客に対して自動的に実行され、任意のレベルで上書きできます。

クロスカスタマーインテリジェンス (ドメインスコープ)
: 追加のテナントデータにアクセスできるテナントのデータ、メタデータ、ビジネスロジック、および処理コンテキストを自動的に処理します。

ドメイン分離階層

ドメインアーキテクチャを定義するときに、プロセスとワークフローを追跡するための階層を作成します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ドメイン分離階層の例

次の図は、ドメインアーキテクチャを定義するための適切な開始点を示しています。これは、TOP および下位のドメイン間の関係性と、プロセス、データ、およびビジネスルールが親および子ドメインにどのように影響するかを示しています。

- 次の例では、TOP がプロセスドメインです。これにユーザーを含めることはできません。むしろ、TOP には、インスタンスオーナーが開発する新しいプロセスと、これらのプロセスへのグローバルドメインからの上書きを含める必要があります。
- サービスプロバイダー (SP) のみがデフォルトドメインにアクセスできます。このドメインには、アクティブなユーザーは含まれません。ここには、正しいドメインに再アサインする必要がある「消失」データのみがあります。

  注:
  データが特定のドメインにアサインされていない場合、デフォルトドメインに移されます。これは一時的に「消失」した状態であり、正しいドメインにアサインする必要があります。

- ドメインの作成時または更新時に、ドメインのないタスクとユーザーは自動的にデフォルトドメインに配置されます。このアクションを上書きするには、このレコードの [デフォルト] オプションをクリアするか、別のドメインレコードの [デフォルト] オプションを選択します。デフォルトドメインをまだ設定していない場合、ドメインのないタスクとユーザーはグローバルドメインに移されます。
  - インスタンスを使用している間は、ドメイン間でデータを移動しないでください。
  - デフォルトドメインで終了するデータがある場合は、対応するべき構成または手続きの問題があることを意味します。

グローバルドメインは存在しないため、この図には「グローバル」という語は表示されません。「グローバル」とは、レコードにドメインが存在しないことを意味します。

たとえば、[ドメイン] フィールドを持たないテーブルは、テーブルにすべてのグローバルレコードが含まれていることを意味します。[ドメイン] フィールドを含むテーブルは、ドメインのないレコードがグローバルドメインであることを意味します。

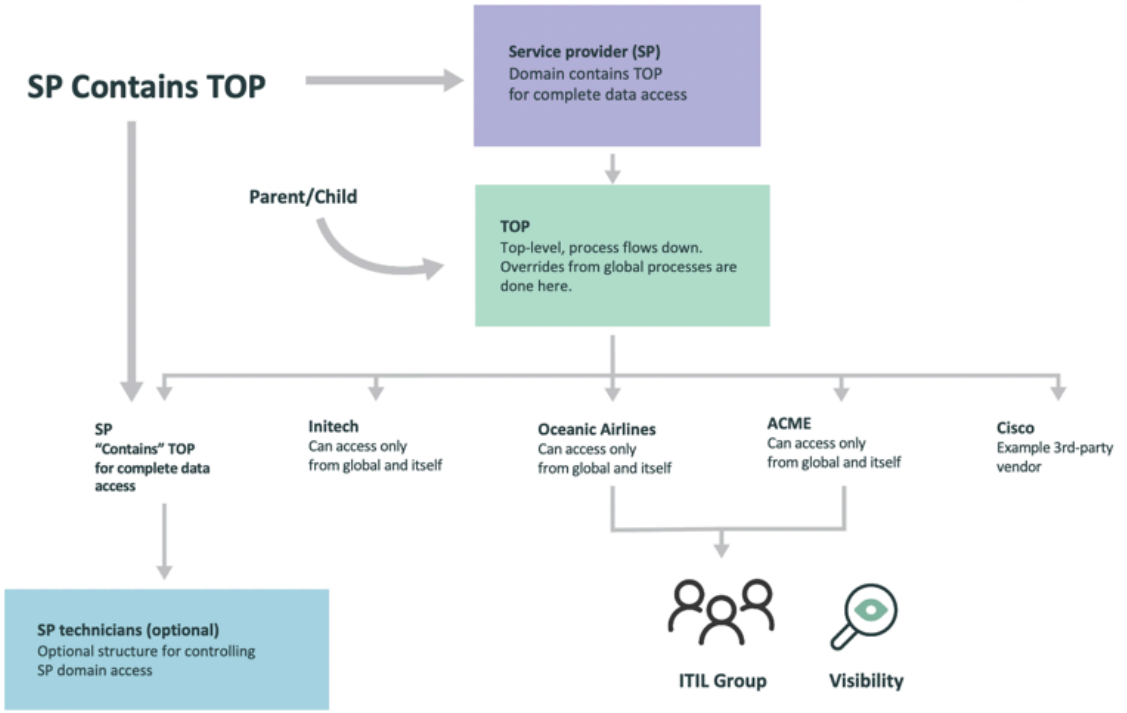
[ドメイン] フィールドには「グローバル」という語があります。レコードにドメインがない場合は、自動的にそこに配置されます。

インスタンスのすべてのユーザーは、セキュリティ構成によって制限されていない限りグローバルレコードを利用できます。

- グローバルレコードを含めるべきでないテーブルにグローバルドメインに留まるレコードが存在しないように、デフォルトドメインを使用してください。
- インスタンス所有者は、デフォルトドメイン内のレコードをトリアージし、正しいドメインに移動する必要があります。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



ドメイン階層

- 親/子： 影響を受けるプロセスとデータ
  - プロセスフローに基づく設計。
  - 親ドメインが子ドメイン内のすべてのデータにアクセスできることに注意してください。
- ドメインを「含む」： 影響を受けるのはデータのみです。たとえば、図の SP に TOP が含まれるようにしても、TOP ドメイン以下で SP のプロセスは実行されません。
  - 特定のドメインへの専用アクセスが必要なグループ内の個々のユーザーに、データアクセス権を付与します。
  - データベースクエリーに追加される原因または条件が含まれ、大規模なドメインやデータセットでパフォーマンスの問題が発生する可能性があります。
- 可視性：アクセス権を付与したユーザーに常に表示される階層。影響を受けるのはデータのみで、プロセスは影響を受けません。
  - 親/子階層の構築時にアクセス権が付与されなかった別のドメインに対して、ドメインのデータアクセス権を付与します。
  - ユーザーがどのレコードを使用しているかにかかわらず、可視性アクセス権を付与されているドメイン内のすべてのデータの表示をユーザーに許可します。

    注:
    可視性は、意図しないような完全なアクセスが許可されてしまうため、慎重に使用してください。

ドメイン階層を定義する基本原則

ドメイン分離の無制限および制限付きユースケース

多くの SP には、ドメインへのアクセスを厳密に制限する必要があることを暗黙的に示す顧客が含まれています。この場合、TOP ドメインでの「包含」機能の使用が制限されます。次の図では、ドメ

自動翻訳

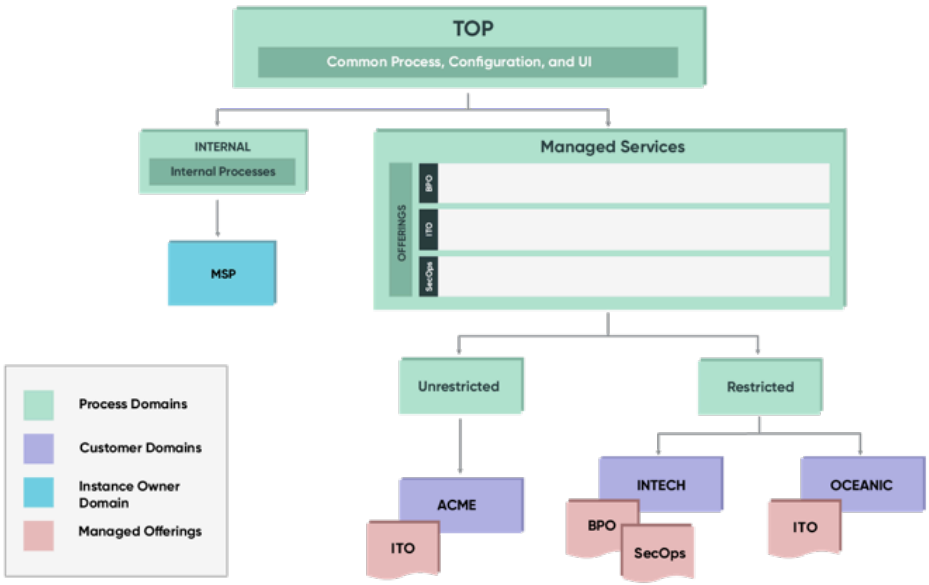
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

インを制限付きドメインと無制限ドメインに分割することで、その規制を軽減する方法について説明します。

1. 顧客は、ドメイン分離階層の特定の「バーティカル」に存在します。つまり、そのドメインと、階層内でそのドメインの上位にあるすべての親ドメインで定義されたプロセスのみを消費します。直線的な親子階層にないドメインで定義されたプロセスは適用されません。

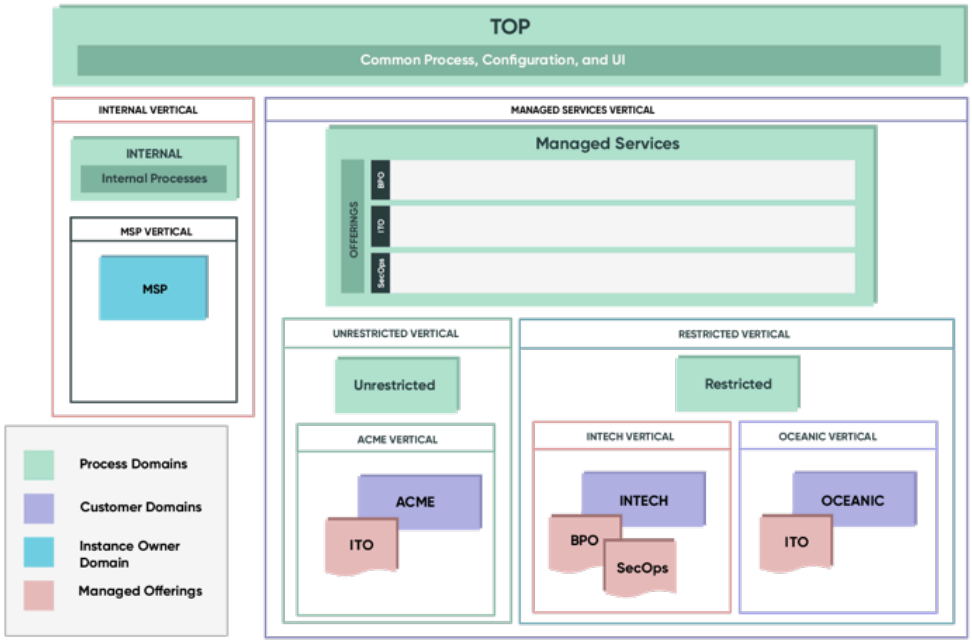
   注:
   顧客または「テナント」は、互いに完全に分離されたエンティティであり、互いにリソースを共有する部門や事業部門とは異なります。

2. スーパーバーティカル (制限付き、マネージャーサービスなど) は、顧客がどちらか一方にしか属さないのであれば、許可されます。
3. すべての顧客が水平に利用できる必要があるサービス、製品、またはオファリングは、個別のドメイン階層内で定義されていません。



自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



サンプルのユースケースは以下のとおりです。

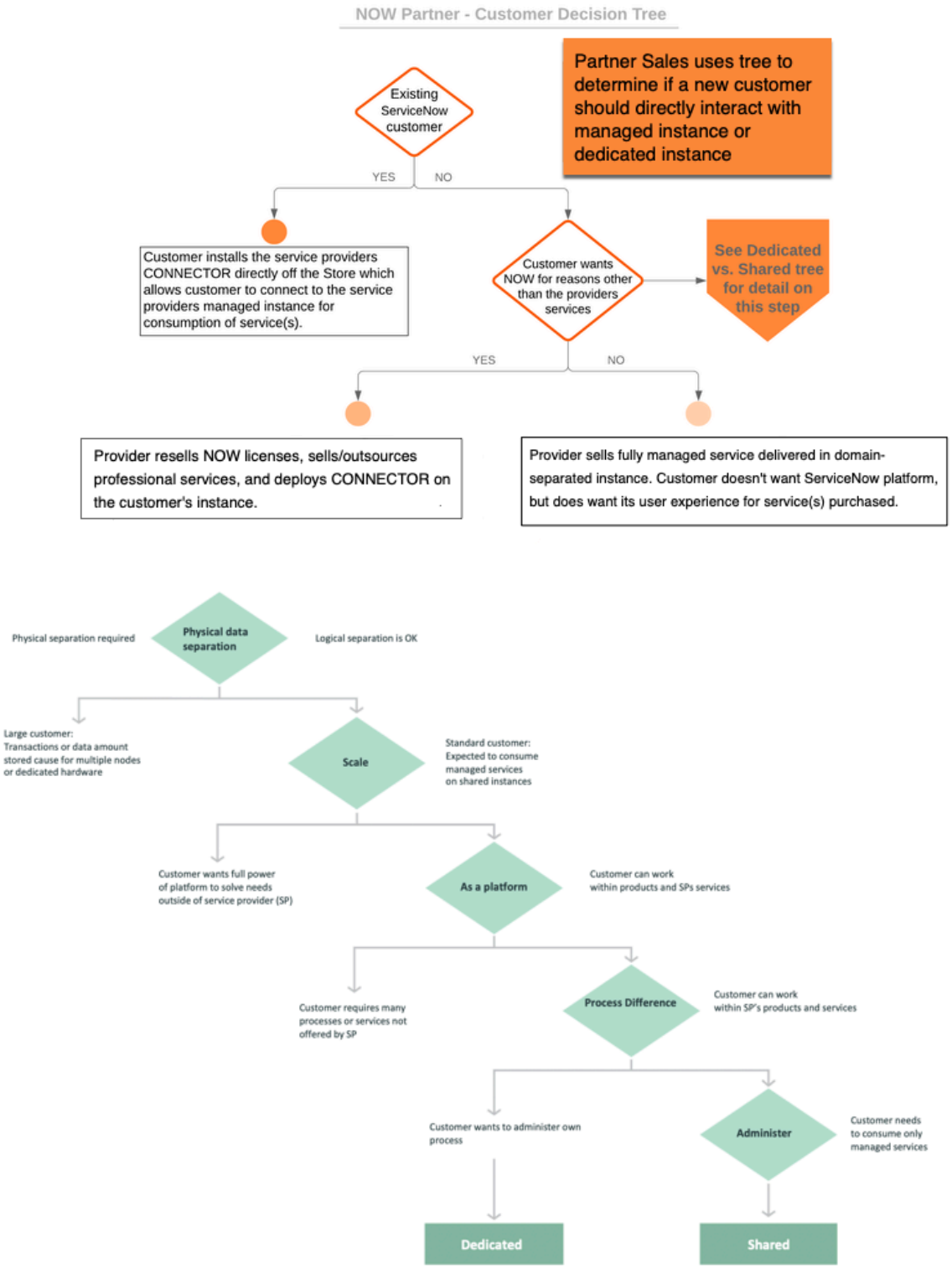
- TOP の下で、[制限なし] と [制限付き] の 2 つのドメインを作成できます。
  - SP の可視性制限がない顧客とそのドメインを [制限なし] ドメインに配置します。
  - この要件がある顧客とそのドメインを [制限付き] ドメインに配置します。
- これにより、システム管理者は、効率的かつターゲットを指定する方法で「包含」および「可視性」機能を使用できます。
  - 「包含」を [制限なし] に適用すれば、1 つの「包含」により、ほとんどの顧客に可視性を付与することができます。
  - ドメインの可視性は、必要に応じて特定のドメインに対して「ドメイン可視性グループ」を使用して適用します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

顧客の決定木

次の図は、適切な階層モデルを選択する方法を説明しています。ドメイン構造に必要なプロセスと機能に応じて、個別の階層、ハイブリッド型、または共有階層を選択できます。



階層アーキテクチャの詳細については、「サービスプロバイダー参照アーキテクチャ」を参照してください。

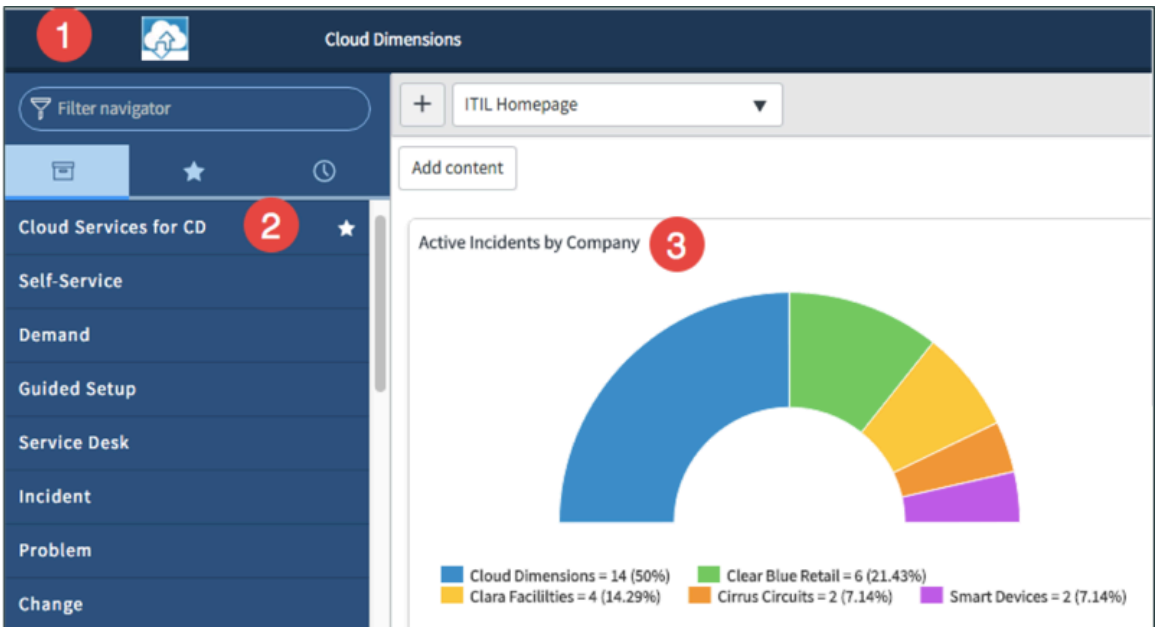
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

コンテキストと **Domain Separation**

ユーザーのセッションのコンテキストによって、ユーザーがリストビュー、ホームページ、レポート、およびナレッジ記事を参照する際のプロセス、データ、およびユーザーインターフェイス (UI) が決まります。コンテキストは、作成するプロセス、設定するビジネスルール、ワークフロー、およびその他の要因によって決まります。

ユーザーセッションコンテキスト

ユーザープロファイル、グループ、会社基準など、多くの要因がユーザーセッションのコンテキストを決定します。次の図では、会社が作成したインシデントがコンテキストの一部であることがわかります。



この例のユーザーのホームドメインは Cloud Dimensions です。

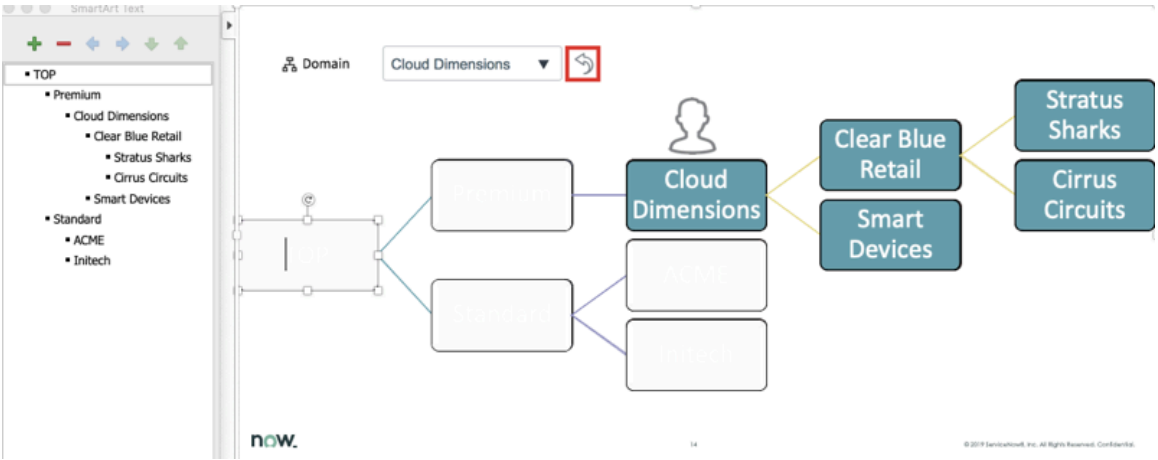
1. ブランディングには、Cloud Dimensions ドメインと会社レコードの設定が反映されます。
2. アプリケーションナビゲーターには、上位レベルのドメインから継承されたアイテムと、Cloud Dimensions ドメインで定義されているモジュールが表示されます。
3. ホームページとリストデータには、ユーザーに表示されるデータが反映されます。このデータは、ユーザーのセッションコンテキストに基づいています。この場合、Cloud Dimensions ドメインのユーザーは、Cloud Dimensions、子ドメイン、およびグローバルドメインのデータを表示できます。

ホームドメインでのユーザーセッションコンテキストの開始

次の図は、コンテキストの要素を示しています。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



システム管理者は、ユーザーのホームドメインをユーザーレコードに設定します。通常、ユーザーのホームドメインは会社のドメインと同じドメインに設定されます。ユーザーがログインすると、ドメインピッカーがユーザーのホームドメインに自動的に設定されます。ユーザーは、ドメインピッカーの矢印アイコンをクリックして、いつでもホームドメインに戻ることができます。

ドメインピッカーのリストには、ユーザーのセッションコンテキスト内のドメインが含まれています。ユーザーは、ピッカーで子ドメインを選択して、セッションコンテキストをさらに制限できます。

ユーザーセッションのコンテキストには、ユーザーのホームドメインと子ドメインが含まれます。ユーザーのセッションコンテキスト内のこの一連のドメインは、データベースに送信されるすべてのクエリに自動的に追加されます。これにより、結果はこれらのドメイン内のデータとグローバルデータのみに制限されます。このプロセスは、アクセスできないコンパイル済みコードに埋め込まれています。

統合に使用されるサービスアカウントにもユーザーセッションコンテキストがあります。ユーザーコンテキストとレコードコンテキストがあり、それぞれ独自のドメインに独自のデータがあります。これらのコンテキストは統合に影響します。データベースクエリー (レコード) は、インタラクティブユーザー (ユーザー) と同じ方法で制限されます。つまり、通常どおりに機能しますが、開発者が設定した制約によって制限されます。

ユーザーのセッションコンテキストにドメインを追加するその他の方法については、「サービスプロバイダー参照アーキテクチャ」を参照してください。

レコードコンテキスト

ユーザーが個々のレコードにドリルダウンすると、レコードコンテキストが有効になります。レコードコンテキストによって、レコードに適用する UI 要素とプロセスが決まります。

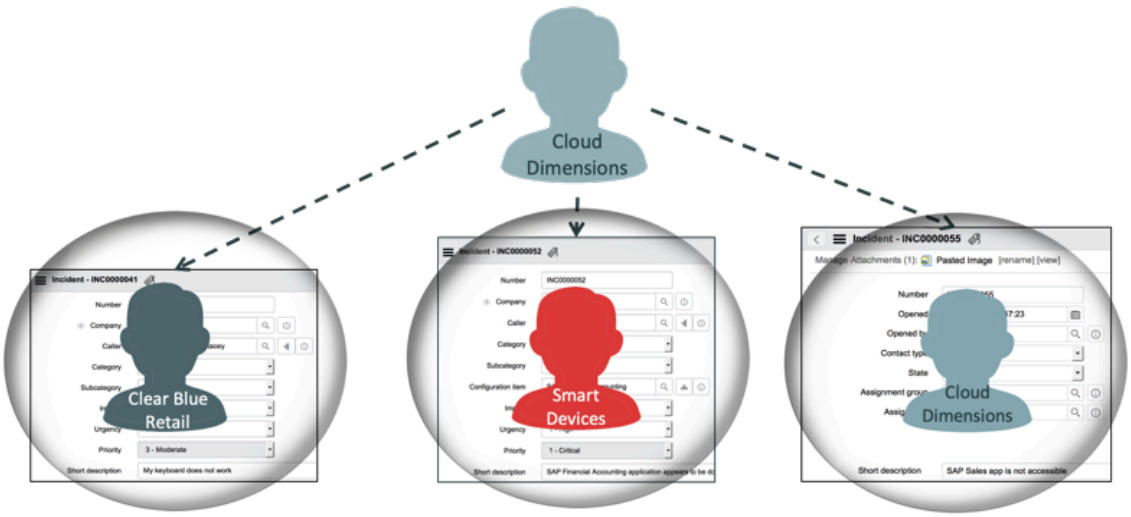
レコードのドメインによって、レコード内のプロセス、データ、および UI 要素の可用性が決まります。

注:

- レコードコンテキストは、ユーザーのドメインが変更されても保持されます。
- ユーザーは、独自のレコードコンテキストを維持しながら、複数のブラウザータブで同時にレコードを表示できます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

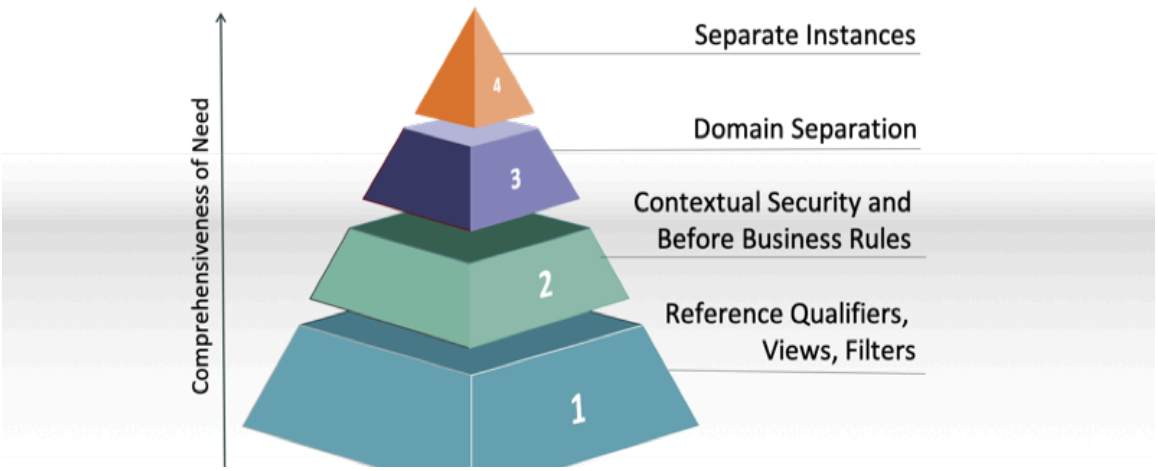


Domain Separation によるデータの分離と保護

顧客のニーズに応じて、ServiceNow プラットフォーム上のデータを複数の方法で分離して保護することができます。

複数の方法でのデータ分離

次の図は、データを分離する 4 つの方法を示しています。データを分離する方法として、個別のインスタンス、Domain Separation、コンテキストセキュリティとビジネスルール、および参照アーキテクチャ自体を使用できます。



次の 4 つの方法でデータを分離できます。

1. 社内の部門やグループが自分の作業に集中できるように、修飾子とフィルターを使用して 参照アーキテクチャ をカスタマイズします。これらの部門またはグループ間でデータを分離することで、部門またはグループは別の部門またはグループのレコードを表示できません。
2. データ侵害から保護するための追加のセキュリティレイヤーとして、コンテキストセキュリティとクエリー前のビジネスルールを追加します。Domain Separation とビジネスルールの詳細については、「コンテキストと Domain Separation」および「クエリ前ビジネスルール」を参照してください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

3. Domain Separation を使用して、会社に別のレベルのセキュリティを追加します。すべてのデータベースクエリーからのデータは、コンテキストセキュリティとビジネスルールが実行される前にドメインに表示されるデータに制限されます。
4. 個別のインスタンスを使用してデータベースとアプリケーションレイヤーでデータを分離します。

個別のインスタンス、Domain Separation、コンテキストセキュリティとビジネスルール、および参照アーキテクチャがデータを分離する方法です。これらの 4 つの方法は、図のニーズの包括性矢印で示されているように互いに関連しています。各レイヤーが他のレイヤーとどのようにやり取りするかは、Domain Separation 構成の設定方法によって異なります。

すべての組織で Domain Separation が必要なわけではありません。個別のインスタンスやドメインのない単一のインスタンスなど、他の代替手段が見つかる場合があります。これらの代替方法の詳細については、「Domain Separation の必要性の評価」を参照してください。

クロステナントインテリジェンス

マルチテナントアーキテクチャでは、単一のインスタンスが複数のテナントに対応します。テナントのデータ、メタデータ、ビジネスロジック、および処理コンテキストは、他のテナントデータにアクセスすることで自動的に処理されます。

単一テナントと複数テナント

単一テナントインスタンス

ServiceNow の顧客であるあなたは、ライセンスを購入したので、自分で必要なサービスを決定できます。必要に応じてアップグレードし、すべての優れた新機能のプレビューを確認して、すぐにインスタンスを設定できます。単一テナントには、次のメリットと制限があります。

- 初期コストと管理費は高くなりますが、自由に再構築や拡張ができます。
- インスタンスを取得して維持し、管理スタッフを用意すると、コストが高くなります。必要に応じて環境を自由に構築できますが、ServiceNow の推奨プラクティスと標準に準拠する必要があります。

複数テナントインスタンス

他のユーザー (複数の顧客を持つサービスプロバイダー) がインスタンスを所有しています。必要に応じてアップグレードし、インスタンスに新しいサービスを提供します。あなたがサービスプロバイダーの顧客である場合、そのサービスプロバイダーが提供する製品を望んでいたため、そのサービスプロバイダーのインスタンスを使用している可能性が高くなります。複数テナントには、次のメリットと制限があります。

- 一元化されたスタッフが構成、統合、およびアップグレードを管理します。
- インスタンスオーナーが追加サービスを提供します。
- ドメインテナントは、ServiceNow プラットフォームを使用するための初期コストが低く、多くのテナントと共有しているため月次コストも低く、環境を管理するスタッフを雇用する必要がありません。
- 他のテナントが開始した要求または変更によりメリットが共有されます。

Domain Separation の代替手段

顧客の Domain Separation の代わりに個別のインスタンスを使用できます。個別のインスタンスを使用すると、組織内のグループや部門内で他の人に影響を与えずにデータ分離の要件を柔軟に満たすことができます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

個別インスタンス

個別インスタンスの長所と短所

個別インスタンス	単一インスタンス - ドメインなし
長所	長所
各顧客/組織に合わせて構築	単純なシナリオに対応可能
他のユーザーへのカスタマイズの影響を最小限に抑える	コスト
リリーススケジュールの調整	短所
明確な分離	ベースラインコードの大幅な変更
データセンターのある地域の選択	変更済みベースシステムコードがアップグレード中にスキップされる
短所	すべてのセカンダリテーブルとサポートテーブルにも対処する必要がある
コスト	広範なテストが必要
インスタンスの配置	カスタムコードを進化させる ServiceNow 製品チームがない
アップグレードのテストの労力	
労力の重複	
統合が必要	

インスタンスごとに個別にアップグレードとリリースの時間を設定できます。ただし、個別のインスタンスを使用する場合は、インスタンスを管理している他のユーザーと多くの調整を行う必要があります。コンテキストセキュリティ、フォームビュー、参照修飾子、フィルター、および堅牢な条件を使用してインスタンスを構成すると、会社で Domain Separation を使用する必要がなくなります。

個別のインスタンスを使用すると、データとプロセスの分離に対処できますが、インスタンス所有者は個別のインスタンスに必要な広範なカスタマイズを維持する必要があります。

関連情報

- コンテキストと Domain Separation
- サービスプロバイダー参照アーキテクチャ

Domain Separation の必要性の評価

Domain Separation が顧客の組織で常に機能するとは限りません。顧客のニーズを考慮して、Domain Separation を使用するかどうかを決定することをお勧めします。

Domain Separation の必要性の評価

Domain Separation を選ぶ理由

次の要因が、顧客の組織の Domain Separation を選ぶ際に役立つ可能性があります。

- 顧客のプロセス調整と一般的なプラットフォーム要件は中程度である。
- 顧客が要求者ではなく履行者としてタスクを処理することを計画している。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- 顧客がデータレコードの分離を要求する契約を結んでいるが、インスタンスオーナーは構成の別の場所でその要件に対処できると判断した。
- 会社のインスタンスオーナーは、物理的に分離された組織として運用され、データを共有しないエンティティを持つが、それでも完全なレポートを必要とする。別々のドメインを使用して、正しく設定すると、データを表示できる。

Domain Separation が設定されない理由

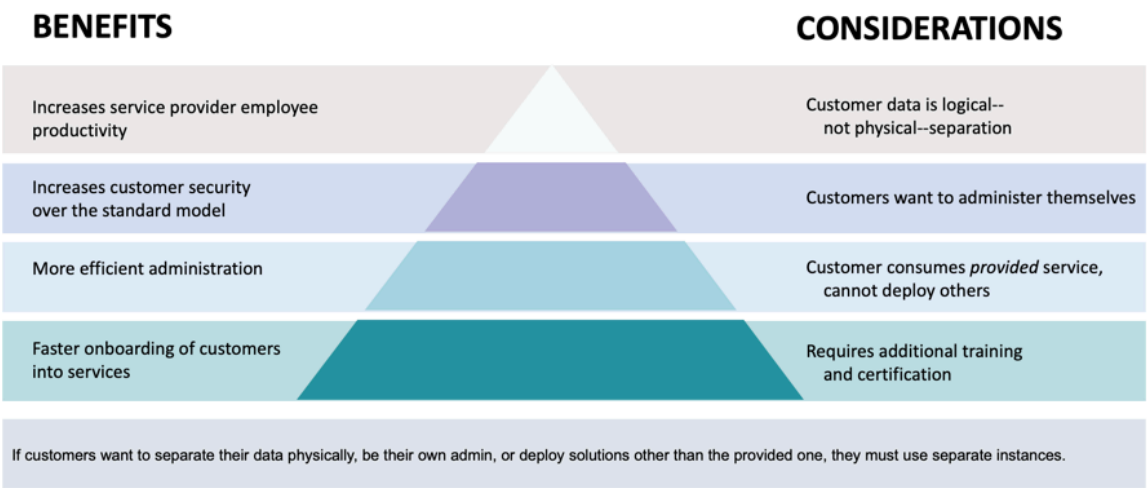
次の要因は、顧客の組織が Domain Separation を設定しない可能性がある理由を示しています。

- 顧客は環境を管理し、その完全な所有権を持ち、拡張のロードマップを設定することを望んでいる。
- 顧客は、物理またはデータベースレベルでデータとプロセスを完全に分離することを要求している。

注:

ドメイン分離されたインスタンスには共有データベースが含まれているため、これは分離要件に反しています。

- 顧客の組織内の部門がレコードを分離することを望んでいる(アクセス制御で十分な可能性がある)。
- すべての顧客が独自のプロセス、ビジネスルール、およびワークフローを必要としている。
- 企業文化は、顧客の組織間の非コラボレーションの 1 つである。
- 顧客はエンドユーザーとしてのみプラットフォームを操作する。



ドメイン分離のメリット

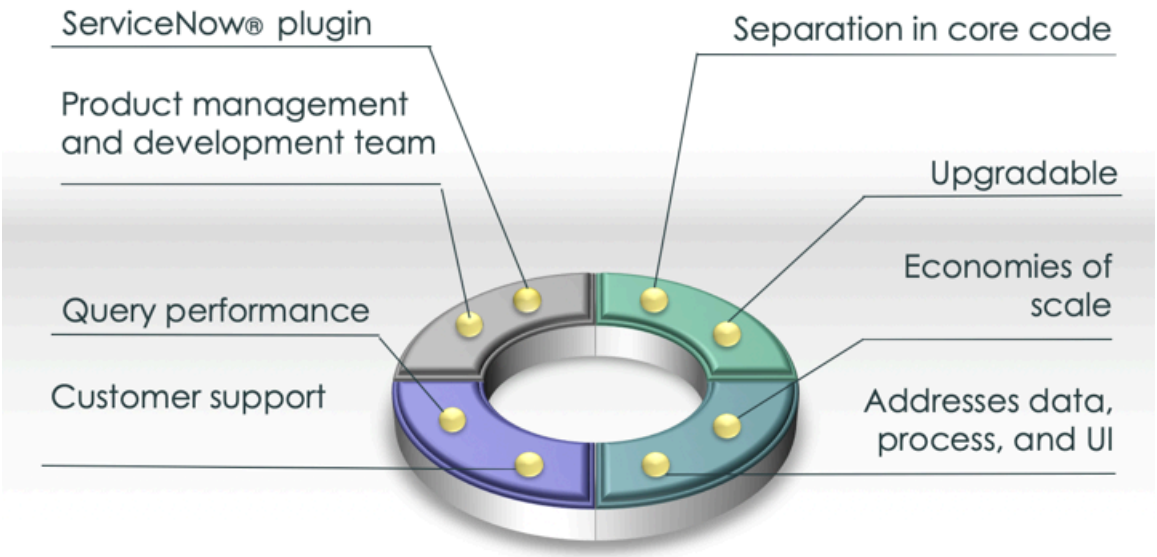
ドメイン分離は、グループや部門間でデータを分離する他の方法よりも顧客の組織で効果的に機能する可能性があります。

ドメイン分離のメリットの概要

コアプラットフォームに機能が組み込まれた ServiceNow プラグインを使用して、ドメイン分離を有効にすることができます。分離ドメイン構成は製品マネージャーが管理し、開発チームが製品マネージャーをサポートします。ServiceNow リリースには、ドメイン分離機能の拡張と修正が含まれており、顧客が使用できるようになりました。インスタンスオーナーは、ドメイン分離のサポートについて、Service Portal など、カスタマーサービス & サポート リソースを参照できます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳



Domain Separation でのデータベースクエリーの仕組み

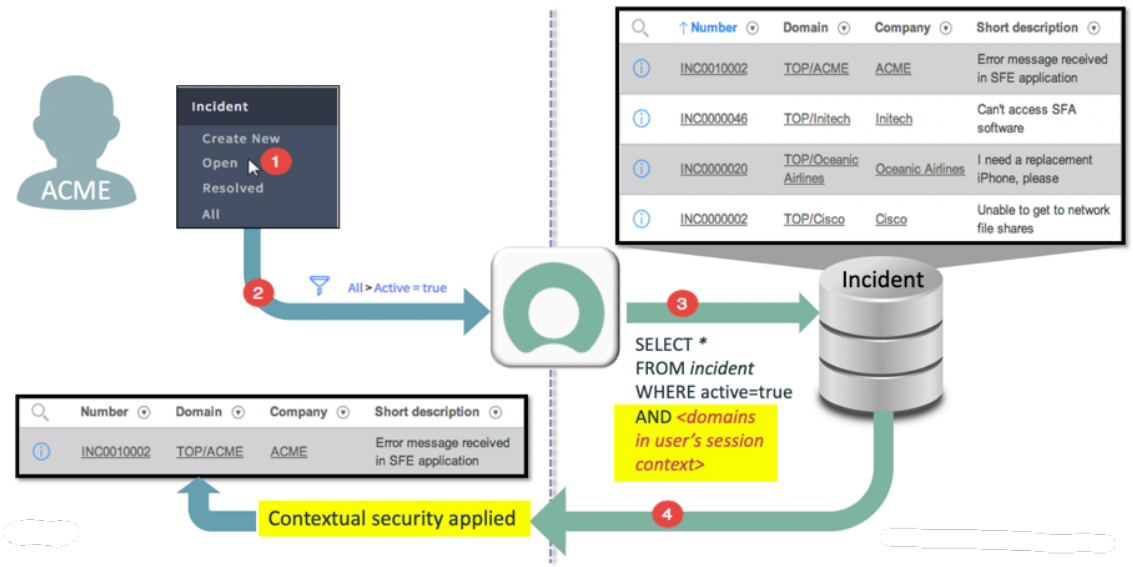
顧客のアプリケーションで Domain Separation を利用してデータベースクエリーを使用すると、顧客のデータを保護するのに役立ちます。これらのクエリーにより、構成と構築のプロセスが迅速化されます。

Domain Separation によるデータ保護方法

次の図には、インシデントテーブル [incident] に、インシデントのタスクから継承されたドメインフィールドがあります。このドメインフィールドが表示されている場合は、テーブル内のレコードにドメインが割り当てられていることがわかります。

ユーザーがログインすると、アクセス可能なドメインのセットとともにホームドメインが表示されます。これは、ユーザーのセッションコンテキストと呼ばれます。セッションコンテキストの詳細については、「コンテキストと Domain Separation」を参照してください。

Domain Separation でのデータベースクエリー



© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

1. ブラウザで、Acme 社のユーザーがオープンインシデントモジュールを選択し、active=true に設定されているすべてのインシデントを表示します。
2. active=true フィルターがアプリケーションに送信されます。
3. アプリケーションは、active=true に WHERE 句を追加して、データベースにクエリーを送信します。WHERE 句は、返されるインシデントレコードを、ユーザーのドメイン内にあるレコードまたはユーザーがアクセスできるドメインに制限します。これらのドメイン内のレコードのみが処理のためにアプリケーションに返されます。
4. コンテキストセキュリティが適用され、ユーザーに返されるデータがさらに制限されます。インシデントレコードがオープンインシデントリストに表示されます。

> **注:**
>
> コンテキストセキュリティを適用すると、ユーザーに返されるデータが制限されます。これらの制限は、ユーザーに表示しない他のコンテンツを保護します。

コンテキストセキュリティの詳細については、「コンテキストと Domain Separation」を参照してください。

> **注:**
> この処理ロジックは、統合を使用してトリガーされるクエリーを含む、データベースに対するすべてのクエリーに適用されます。

Domain Separation のサポートレベル

顧客の組織のアプリケーションの Domain Separation に対し、3 つのカテゴリから選択します。

Domain Separation をサポートするアプリケーションは、データとデータルーティングの分離のみをサポートするか、高度なビジネスロジック分離機能があるか、アプリケーションのテナント (顧客) レベルの管理をサポートすることができます。これらの定義は、実際のユースケースとそれを実装するユーザーの観点からサポートレベルを示しています。

増分 **ServiceNow** サポートレベル

Basic	Standard	Enhanced
• Data is domain-separated • Logic exists to ensure proper data routing, caching, rollups, and aggregations • Global configuration operational for multiple tenants	• Application properties are domain-aware as needed • Business logic can be domain-separated by the instance owner per tenant	• Data-driven process enables failsafe configuration by tenants through the UI to drive business logic

レベル	タイプ	サマリー
サポートはありません		• ドメインフィールドがデータテーブルに存在している可能性がありますが、データを管理するビジネスロジックはありません。 • このレベルでは、ドメイン分割は考慮されません。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

レベル	タイプ	サマリー
基本	顧客データ管理	• アプリケーションサービスプロバイダーのユースケースに合わせてデータが適切なドメインに送られるようにするビジネスロジックが存在します。 • アプリケーションでは、ユーザーインターフェイス、キャッシュキー、レポート、ロールアップ、集計など、すべてにおいて、実行時にドメインのプロパティが考慮されます。 • インスタンスの所有者は、複数のテナント間で正常に機能するようにアプリケーションを設定できる必要があります。 ユースケース：サービスプロバイダーがチャットを使用して顧客のメッセージに応答する際に、クライアントが応答を確認できるようにする必要があります。
標準	顧客プロセス管理	• ベーシックレベルを含みます。 • ビジネスロジック：サービスプロバイダーによって顧客ごとにプロセスを作成または変更できます。ユースケースには、単一のインスタンスで複数のサービスプロバイダー顧客がアプリケーションをどのように使用するかが反映されます。 • インスタンスのオーナーは、特定のアプリケーションに、顧客ごとに MVP (minimum viable product) ビジネスロジックとデータパラメーターを設定できる必要があります。 ユースケース：管理者は、レコードを 1 人の顧客に対してはクローズしないが、別の顧客に対してクローズする場合、コメントを必須にすることができる必要があります。
拡張機能	顧客自己管理構成	• ベーシックレベルと標準レベルを含みます。 • サービスプロバイダーの顧客は定義されたユースケースに基づくビジネスロジックを変更できます。これらの構成は UI ベースでフェイルセーフであるため、1 人の顧客による構成が別の顧客に影響を与えることはありません。 • インスタンスの顧客は、自身で MVP ビジネスロジックとデータパラメーターを設定できる必要があります。 ユースケース：共有環境の顧客は、ドメイン内で影響度、緊急性、または優先度に基づいて変更できる必要があります。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

レベル	タイプ	サマリー
有効なドメイン*		ドメインフレームワークが使用されていなくても、プラットフォーム機能またはアプリケーションがサービスプロバイダーのユースケースをサポートできる場合があります。ユースケースには Domain Separation のサポートが詳述されている必要があります。サポートレベルの後のアスタリスク (*) は、この種類の構成を示します。 ユースケース：New York リリースより前は、サービスカタログ はドメインをサポートしていませんでしたが、インスタンスオーナーはユーザー基準を使用して、ドメイン分離されたインスタンス内の各テナントに個別のカタログとアイテムを設定できました。その結果、各テナントは標準レベルで Service Catalog を使用することができました。

サポートレベル別に一覧表示されたすべてのアプリケーションを表示するには、「アプリケーションでのドメイン分離のサポート」を参照してください。

サマリー

Domain Separation は、アプリケーションで顧客を認識するために使用する必要があるフレームワークです。

フレームワークを使用してアプリケーションをサポート可能にする前に、ドメインフレームワークの機能、アプリケーションのビジネスユースケース、ペルソナの概要、およびアプリケーションの使用方法を検討してください。

サービスプロバイダー参照アーキテクチャ

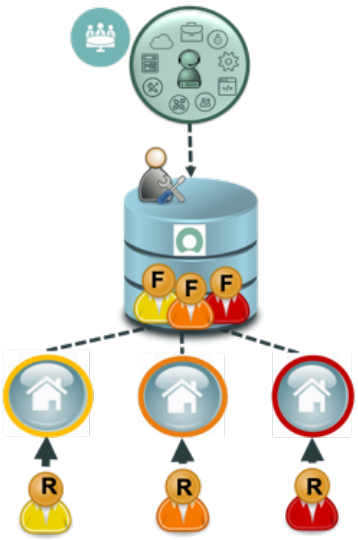
顧客は、ドメイン分離されたインスタンスに到達するために設計されたポータルを使用して、サービスプロバイダー (SP) サービスにアクセスできます。

サービスプロバイダー参照アーキテクチャの基本属性

- 履行者をドメインに割り当てません。代わりに、ドメイン間で共有します。これにより、ドメインあたりの履行者の数を監査することが困難になります。
- ドメイン管理を共有して活用できます。これは、オーバーヘッドがなく、ライセンスを最適化できることを意味します。
- 新しい顧客を取得すると、インスタンスのユーザー数が変更される可能性があります。新しい顧客を取得することで、システム上に数万人から数十万人の新規ユーザーが増える可能性があります。1 つの共有環境での合計ユーザー数は実質的に無制限です。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



- SP customers access SP services via a portal to the SP Domain Separated instance
- SP uses ServiceNow shared instance(s) to manage their service delivery
- SP could have a shared instance per region to support data sovereignty requirements

Legend:

Centralized governance at the SP

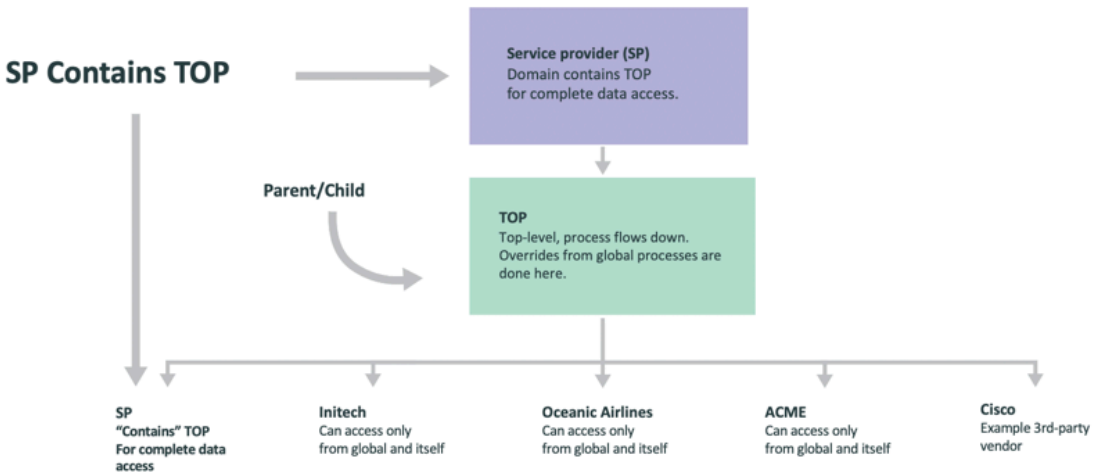
Centralized administration at the SP. Shared business requirements and configurations

Both SP and customer fulfillers on one instance

Customer requesters on each instance

SP サービスのポータルは、SP 共有インスタンス専用または共有です。サービスプロバイダーは、ServiceNow 共有インスタンスを使用してサービスデリバリーを管理します。

ドメイン分離されたインスタンスの参照階層



自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

SP 参照アーキテクチャの比較

Standalone (SA)		Multi-Tenant (MT)		Hybrid (MT+SA)		SIAM (Multi-Vendor)	
Platform as a Service	Enterprise scale	Processes simplified	Cost reduction	Managed Services (MT)	Custom Services (SA)	Service Integration	Multi-supplier governance
Customer wants full power of platform to Solve own needs outside those offered by SP.	Large customer: Transactions or data amount stored cause for multiple nodes or dedicated hardware.	Global governance & admin for business use case & process can be developed & maintained on the instance. Best when used w/ minor-to-moderate process differences among customers or sub-entities.	Lower administration, transaction, & onboarding costs, & ongoing operational costs for resources & licensing. Faster onboarding = more revenue.	Standardized re-usable services. procedures. processes, & resources delivered on a single ServiceNow instance to multiple Customers.	Services for sole use of customer, offerings specific to industry or vertical solutions, government, or regulatory requirements, applications that do not support Domain Separation.	Multiple best in class Service providers for individual services bringing together tooling, reporting, SLAs, strategy, & design for unified customer experience.	Unified governance across all providers to ensure organization requirements are met & that all providers cooperate on behalf of the customer.

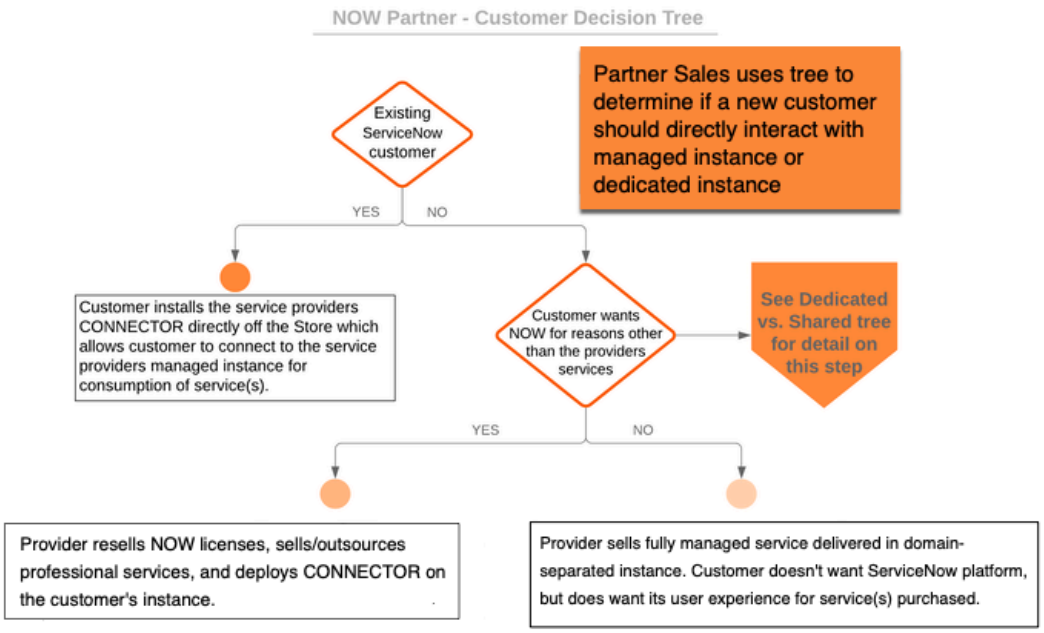
サービスプロバイダー参照アーキテクチャの意思決定ツリー

意思決定ツリーと比較チャートを使用して、新しい顧客を共有インスタンスまたは独自の専用インスタンスに追加する必要があるかどうかを判断できます。

意思決定ツリー

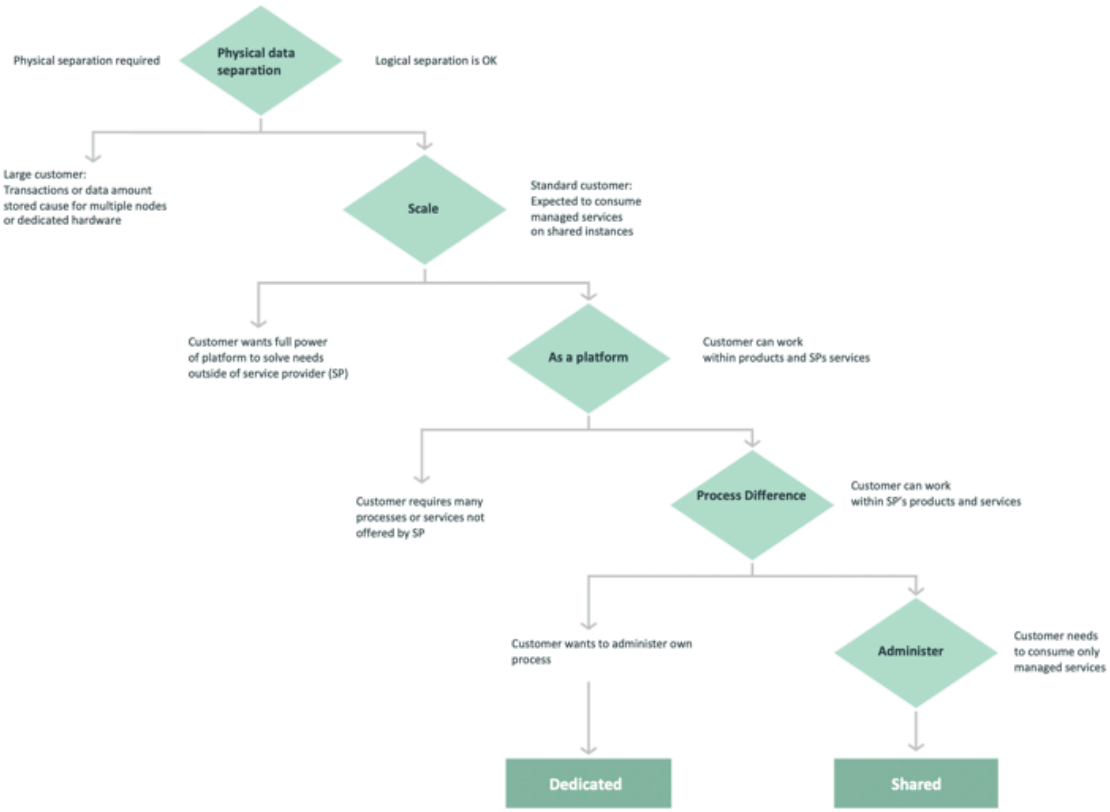
これらの意思決定ツリーを使用して、顧客が管理対象インスタンスを使用するか専用インスタンスを使用するかを決定できます。

顧客の意思決定ツリー



自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



SP 参照アーキテクチャの比較

Standalone (SA)		Multi-Tenant (MT)		Hybrid (MT+SA)		SIAM (Multi-Vendor)	
Platform as a Service	Enterprise scale	Processes simplified	Cost reduction	Managed Services (MT)	Custom Services (SA)	Service Integration	Multi-supplier governance
Customer wants full power of platform to Solve own needs outside those offered by SP.	Large customer: Transactions or data amount stored cause for multiple nodes or dedicated hardware.	Global governance & admin for business use case & process can be developed & maintained on the instance. Best when used w/ minor-to-moderate process differences among customers or sub-entities.	Lower administration, transaction, & onboarding costs, & ongoing operational costs for resources & licensing. Faster onboarding = more revenue.	Standardized re-usable services. procedures. processes, & resources delivered on a single ServiceNow instance to multiple Customers.	Services for sole use of customer, offerings specific to industry or vertical solutions, government, or regulatory requirements, applications that do not support Domain Separation.	Multiple best in class Service providers for individual services bringing together tooling, reporting, SLAs, strategy, & design for unified customer experience.	Unified governance across all providers to ensure organization requirements are met & that all providers cooperate on behalf of the customer.

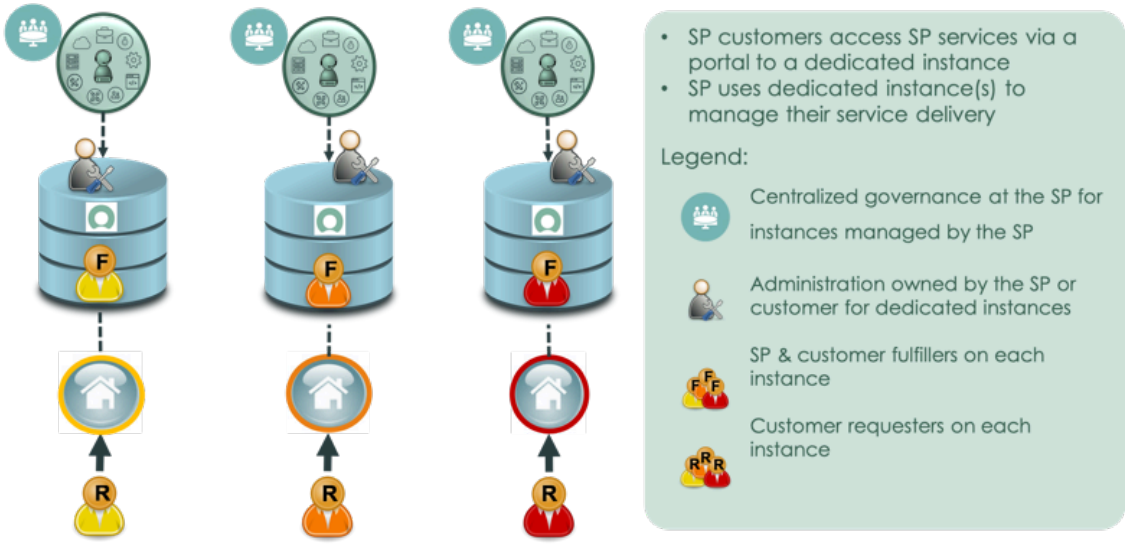
専用インスタンスのサービスプロバイダー参照アーキテクチャ

サービスプロバイダー (SP) の顧客は、専用インスタンスへのポータルを使用して SP サービスにアクセスできます。SP は、 専用インスタンスを使用してサービスデリバリーを管理します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

専用インスタンス

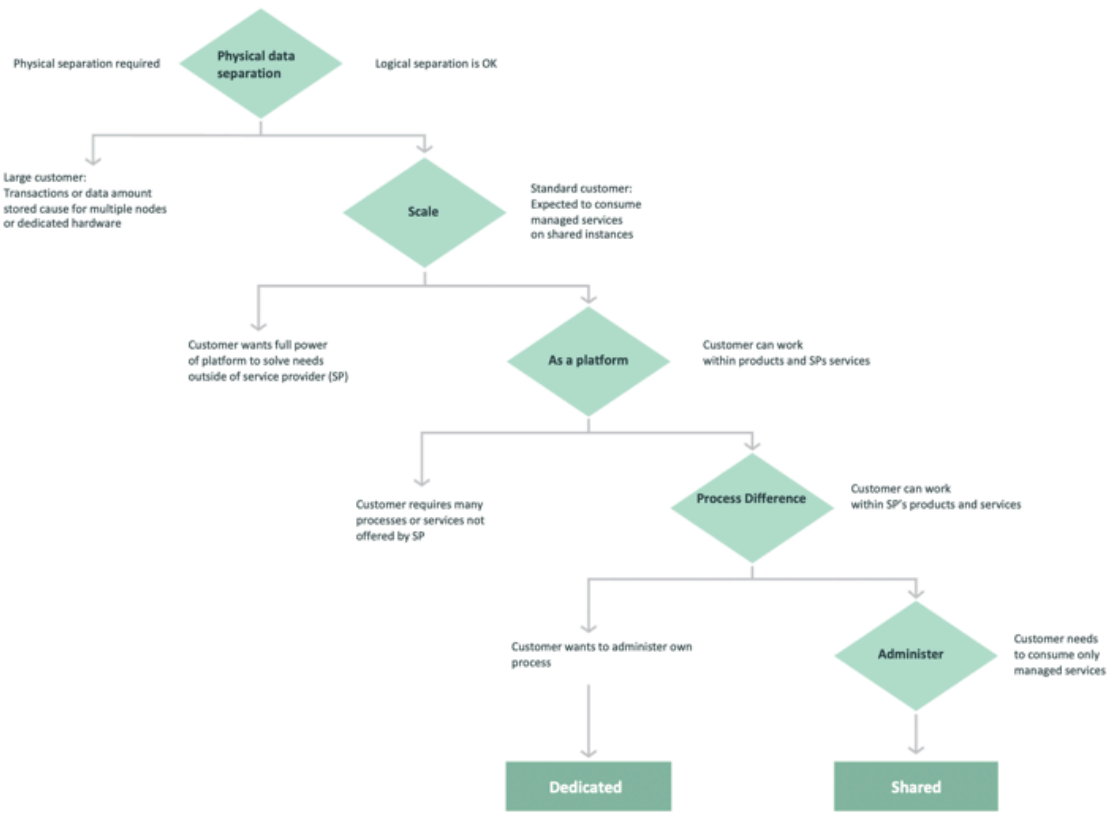


属性

- 専用インスタンスには、個別の管理チームと専門チームが必要です。複数のインスタンスにログインする管理者と開発者には、複数のライセンスが必要です。
- 各インスタンスには、限られた数の要求者と履行者がいます。新規顧客を獲得する場合は、会社の規模とスケールに基づいてインスタンスを調達する必要があります。

共有インスタンス

専用インスタンスと共有インスタンス



自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

SP 参照アーキテクチャの比較

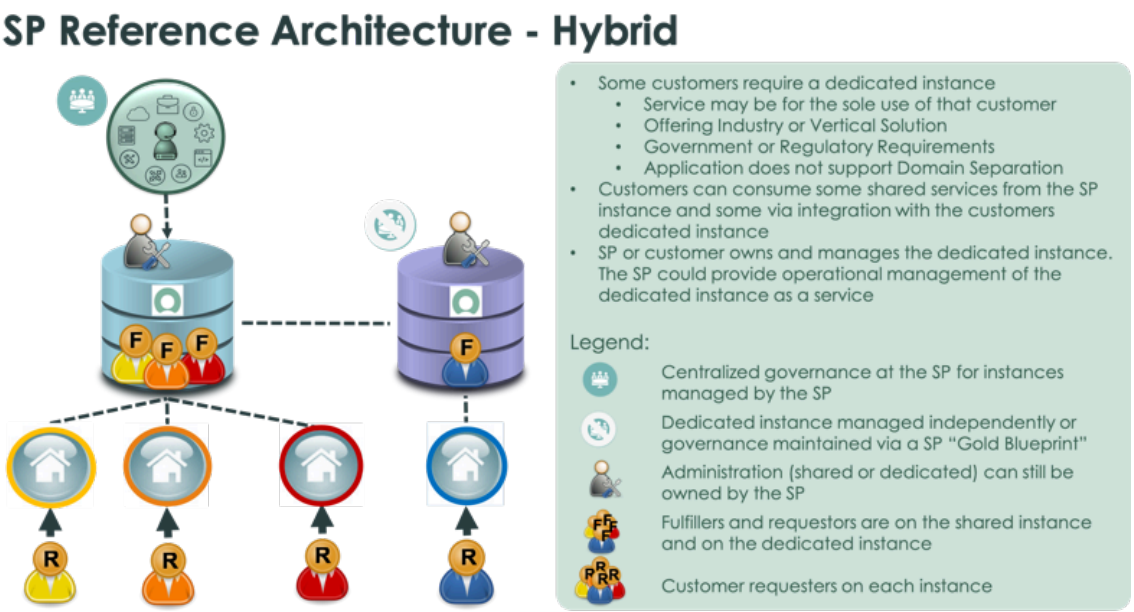
Standalone (SA)		Multi-Tenant (MT)		Hybrid (MT+SA)		SIAM (Multi-Vendor)	
Platform as a Service	Enterprise scale	Processes simplified	Cost reduction	Managed Services (MT)	Custom Services (SA)	Service Integration	Multi-supplier governance
Customer wants full power of platform to Solve own needs outside those offered by SP.	Large customer: Transactions or data amount stored cause for multiple nodes or dedicated hardware.	Global governance & admin for business use case & process can be developed & maintained on the instance. Best when used w/ minor-to-moderate process differences among customers or sub-entities.	Lower administration, transaction, & onboarding costs, & ongoing operational costs for resources & licensing. Faster onboarding = more revenue.	Standardized re-usable services. procedures. processes, & resources delivered on a single ServiceNow instance to multiple Customers.	Services for sole use of customer, offerings specific to industry or vertical solutions, government, or regulatory requirements, applications that do not support Domain Separation.	Multiple best in class Service providers for individual services bringing together tooling, reporting, SLAs, strategy, & design for unified customer experience.	Unified governance across all providers to ensure organization requirements are met & that all providers cooperate on behalf of the customer.

ハイブリッドのサービスプロバイダー参照アーキテクチャ

カスタマイズされたソリューションには、ハイブリッドサービスプロバイダー (SP) の参照アーキテクチャを使用します。顧客には特定のサービスの専用インスタンスが必要です。他のサービスに対しては共有 SP インスタンスを引き続き使用できますが、各インスタンスの統合が必要です。

ハイブリッドアーキテクチャ

顧客がこの追加サービスを直接提供する責任を負う場合があります。顧客が提供する複数の属性のハイブリッドソリューションを構築することが必要になります。



自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

属性

- インスタンスの管理を共有して活用できます。これは、オーバーヘッドがなく、ライセンスを最適化できることを意味します。
- 分散環境に新しいインスタンスがある場合、プログラムチームはそのインスタンスの専用管理者ユーザーとして責任を負い、それに応じて資金が提供されます。すべてのインスタンスが詳細計画に由来する一元化された環境では、複製した管理ライセンスが必要です。
- 履行者をドメインに割り当てません。代わりに、ドメイン間で共有できます。
- 顧客が共有環境と専用環境の両方を共有している場合は、両方の環境で履行者が必要です。共有インスタンスと専用インスタンスのプロセスではインスタンスごとに異なる作業が必要になるため、各チームの作業量が増加します。
- 新しい顧客を取得すると、インスタンスのユーザー数が変更される可能性があります。新しい顧客を取得することで、システム上に数万人から数十万人の新規ユーザーが増える可能性があります。1 つの共有環境での合計ユーザー数は実質的に無制限です。
- 各インスタンスには、限られた数の要求者と履行者がいます。新規顧客を獲得する場合は、会社の規模とスケールに基づいてインスタンスを調達する必要があります。

SP 参照アーキテクチャの比較

Standalone (SA)		Multi-Tenant (MT)		Hybrid (MT+SA)		SIAM (Multi-Vendor)	
Platform as a Service	Enterprise scale	Processes simplified	Cost reduction	Managed Services (MT)	Custom Services (SA)	Service Integration	Multi-supplier governance
Customer wants full power of platform to Solve own needs outside those offered by SP.	Large customer: Transactions or data amount stored cause for multiple nodes or dedicated hardware.	Global governance & admin for business use case & process can be developed & maintained on the instance. Best when used w/ minor-to-moderate process differences among customers or sub-entities.	Lower administration, transaction, & onboarding costs, & ongoing operational costs for resources & licensing. Faster onboarding = more revenue.	Standardized re-usable services. procedures. processes, & resources delivered on a single ServiceNow instance to multiple Customers.	Services for sole use of customer, offerings specific to industry or vertical solutions, government, or regulatory requirements, applications that do not support Domain Separation.	Multiple best in class Service providers for individual services bringing together tooling, reporting, SLAs, strategy, & design for unified customer experience.	Unified governance across all providers to ensure organization requirements are met & that all providers cooperate on behalf of the customer.

サービスインテグレーション管理 **(SIAM)** のサービスプロバイダー参照アーキテクチャ

サービスプロバイダー (SP) アーキテクチャの サービスインテグレーション管理 サービスインテグレーションおよびマネジメント (SIAM) は、統一されたカスタマーエクスペリエンスのためにサービスを統合します。

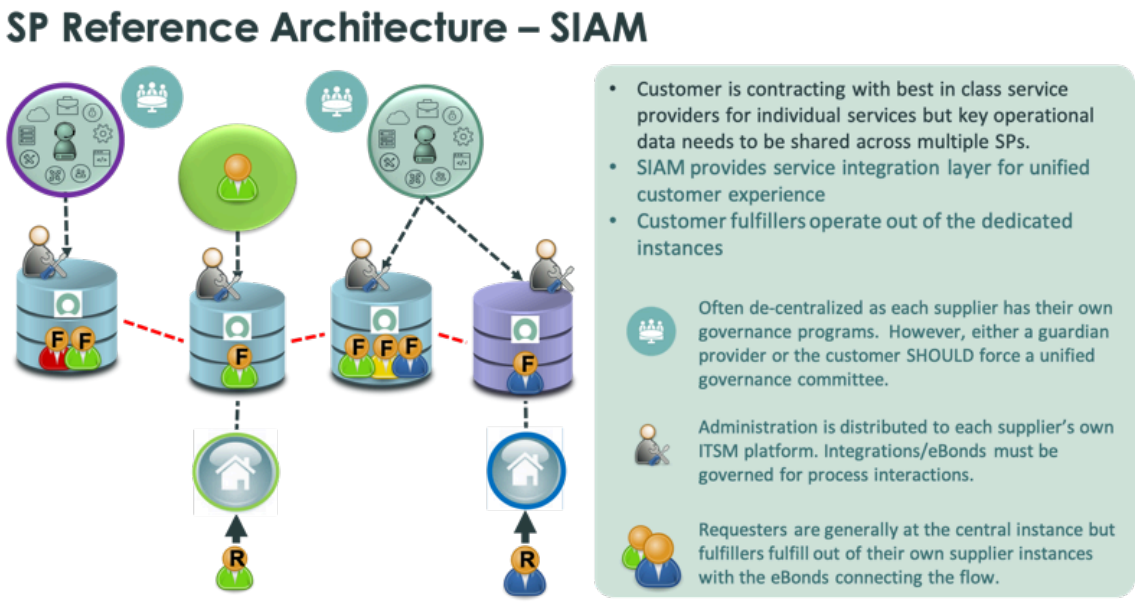
SIAM アーキテクチャの属性

- SP サービスの顧客は、SP 共有インスタンス専用または共有ポータルです。
- SP は、ServiceNow 共有インスタンスを使用してサービスデリバリを管理します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

SIAM アーキテクチャの概要



SP 参照アーキテクチャの比較

Standalone (SA)		Multi-Tenant (MT)		Hybrid (MT+SA)		SIAM (Multi-Vendor)	
Platform as a Service	Enterprise scale	Processes simplified	Cost reduction	Managed Services (MT)	Custom Services (SA)	Service Integration	Multi-supplier governance
Customer wants full power of platform to Solve own needs outside those offered by SP.	Large customer: Transactions or data amount stored cause for multiple nodes or dedicated hardware.	Global governance & admin for business use case & process can be developed & maintained on the instance. Best when used w/ minor-to-moderate process differences among customers or sub-entities.	Lower administration, transaction, & onboarding costs, & ongoing operational costs for resources & licensing. Faster onboarding = more revenue.	Standardized re-usable services. procedures. processes, & resources delivered on a single ServiceNow instance to multiple Customers.	Services for sole use of customer, offerings specific to industry or vertical solutions, government, or regulatory requirements, applications that do not support Domain Separation.	Multiple best in class Service providers for individual services bringing together tooling, reporting, SLAs, strategy, & design for unified customer experience.	Unified governance across all providers to ensure organization requirements are met & that all providers cooperate on behalf of the customer.

自動翻訳

Domain Separation の用語

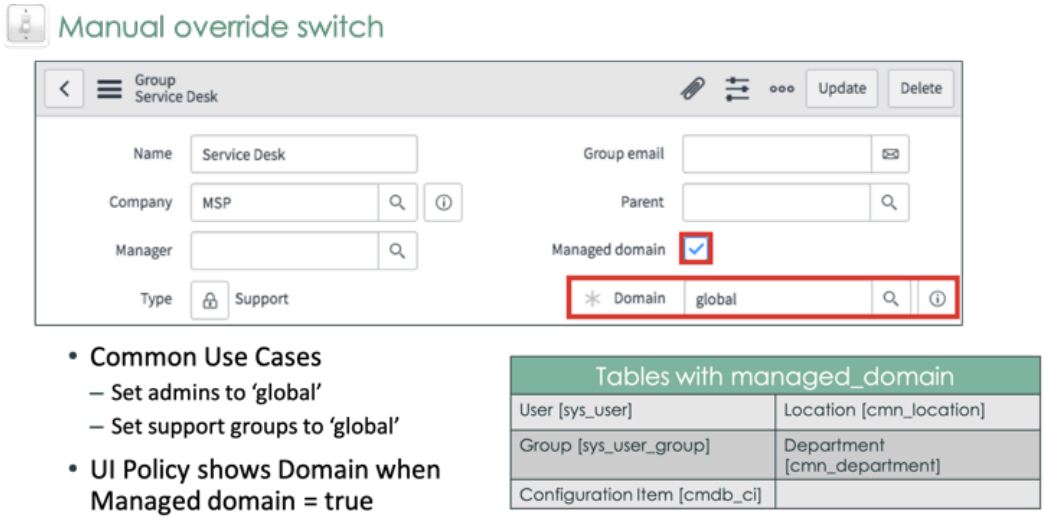
ServiceNow インスタンスを使用すると、効率を向上させ、セキュリティを強化し、顧客の組織のパフォーマンスを向上させることができます。最も一般的な用語を理解しておくと構成を作成する際に役立ちます。

管理対象ドメイン

管理対象ドメインの [管理対象ドメイン] フィールドで、ドメイン管理者は、会社レコードから自動的に割り当てられたドメインを使用するのではなく、ユーザー、グループ、部門、場所、または CI レコードのドメインを手動で選択できます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

これらのプロパティを変更する場合は、上書きして、各ドメイン内のアプリケーションの機能をさらにカスタマイズできます。



プロセステーブル

プロセステーブルで上書き **[sys_overrides]** フィールドに値が表示されている場合は、プロセス上書きレコードが存在します。これは、管理者がドメイン固有のポリシーを設定できる委任管理が有効であることを意味します。グローバルドメインの管理者は、ドメインスコープの展開/折りたたみ関連リンクを使用して上書きレコードを表示できます。

注:
レポートはドメインに分離され、[上書き] フィールドが含まれています。グローバルドメインからすべてのレポートを表示するには、[ドメインスコープを展開] 関連リンクを使用します。

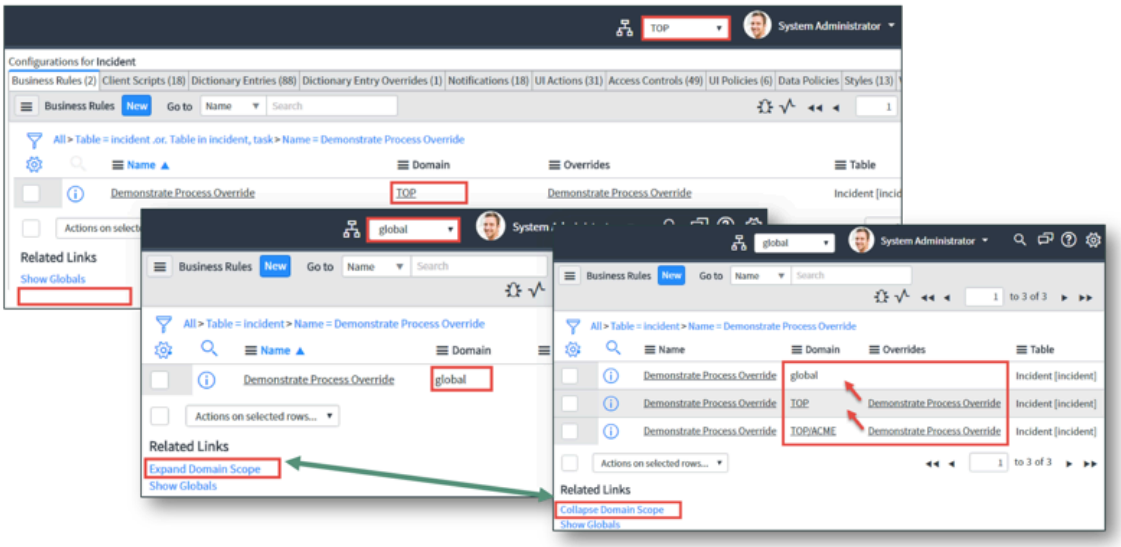
ドメインからプロセステーブルを表示すると、選択したドメインの関連するプロセスレコードのみが表示されます。グローバルドメインからプロセステーブルを表示すると、[ドメインスコープを展開] 関連リンクが表示され、上書きを含むすべてのプロセスレコードを表示できます。グローバルに関連するプロセスレコードのみを再表示するには、[ドメインスコープを折りたたむ] 関連リンクを使用します。

ドメインスコープ機能はプロセステーブルにのみ使用され、テーブルのデータの表示が逆方向に変わります。たとえば、親ドメインのレコードは子で表示できますが、親は子レコードを表示できません。これにより、プロセスが子ドメインに移行します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Overrides [sys_overrides] – Process Tables Only



ドメインのタイプ

さまざまなタイプのドメインは、プロセスとデータ、およびそれらがアプリケーションまたは機能でどのように機能するかを整理するのに役立ちます。

顧客ドメイン

顧客のドメインには、ユーザーインターフェイスと、データの使用方法を制御するプロセスがあります。

次の画像の ACME ドメインは顧客ドメインです。

プロセスドメイン

データの使用方法とドメイン内で実行することのプロセスを作成します。このプロセスには次の属性が必要です。

- 一連のドメインに対する特定のプロセスと UI 設定
- いかなる種類のコアデータ (特定のユーザーデータなど) もありません。
- 次の画像の TOP ドメインはプロセスドメインです。

データドメイン

データドメインは、複数の顧客に関連するデータを保持します。実際の顧客ドメインを共有せずにそのデータを共有できます。各顧客は独自のデータドメインを持ち、そのドメインにアクセスできます。

注:

この種のドメインは一般的ではなく、過度に使用するとパフォーマンスの問題が発生する可能性があります。使用する前に SP アーキテクトに相談してください。

たとえば、ドメインは、ACME、Cisco、および SP のすべてがやり取りする必要があるタスクを保持できます。

次の画像のデフォルトドメインはデータドメインです。

自動翻訳

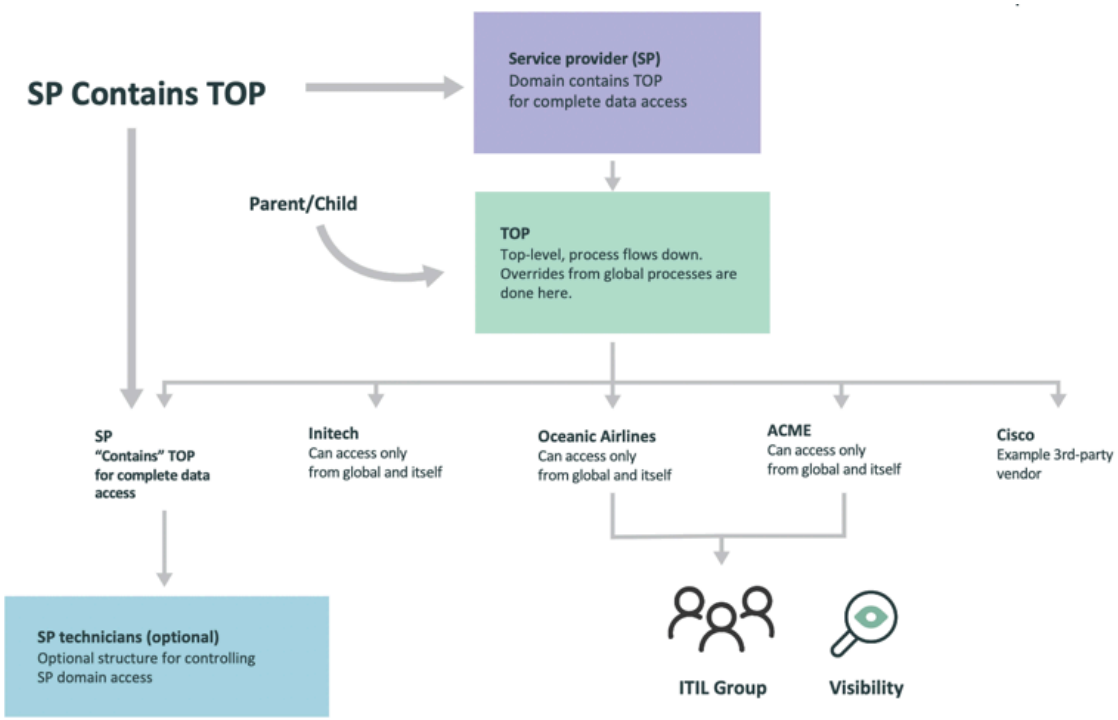
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ユーザーデータ

ユーザーレコードデータがグローバルドメインまたはプロセスドメインに属することはありません。ユーザーは主に顧客ドメインで作成され、場合によってはデータドメインで作成されます。

管理者アカウントは、インスタンスの日常のユーザーとして使用するべきではなく、管理機能を容易にするためにグローバルドメイン内にある必要があるため、特別なアカウントです。

ドメイン階層



リスト、管理者、グローバルプロセス

リスト

グローバルドメインから、任意の選択フィールドのラベルを右クリックし、[選択を設定] を選択して新しい選択肢を追加すると、そのフィールドのすべてのドメイン固有のリストに選択肢が自動的にプッシュされます。新しいオプションが [選択済み] としてマークされている場合は、アクティブとして追加されます。新しいオプションが [利用可能] としてマークされている場合は、非アクティブとして追加されます。

インスタンス管理

インスタンスオーナーの管理者は、ドメイン分離されたインスタンスですべての通常のプロセスの作成、変更、およびメンテナンスを処理する必要があります。個々のドメインマネージャーは、データ駆動型プロセスの一部を維持できます。ドメインマネージャーのタイプは、ユーザー管理、サポートグループメンバーシップ、および場所を維持するか、テナント管理を念頭に置いて設計されたアプリケーションを管理します。

グローバルプロセス/パラメーター

グローバルドメインに影響を与えるプロセスを作成および管理したり、パラメーターを設定したりすることができます。これらのプロパティは、ドメイン分離されたインスタンスのすべてのユーザーに共通です。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

例：システムプロパティ、辞書オーバーライド、sys_documentation (フィールドラベル)、データモデル (クラス、CI タイプなど)、テーブルとフィールド [sys_dictionary] (アクセスを制限可能)、インデックス作成 (テキストインデックスおよびデータベース) 、ACL、インストールイグジット、受信アクション、公開ページ、およびインターセプター。

カスタムテーブルをドメイン分離する

個別のドメインにカスタムテーブルを作成する必要がある場合があります。このトピックでは、カスタムテーブルのドメイン分離の背後にある手順と概念の両方について説明します。

1. sys_domain フィールドを作成します。

> **注:**
> システムテーブルまたはテーブルが Domain Separation プラグインによってドメイン分離されていない場合は、ドメイン分離しないことをお勧めします。

これらのポイントを指針として使用して、sys_domain フィールドを作成します。

- 新しいフィールドを *domain_id* タイプとして作成します。
  - 列名：sys_domain
  - その他の属性：自動的に定義
- sys_domain_path が自動的に作成されます。

列名「**sys_domain**」は Now Platform で予約されています。これは、システムがこれを認識し、適切なフィールドタイプと属性を自動的に適用することを意味します。この自動構成では、対応する **sys_domain_path** フィールドも作成されます。

- ラベルを使用するのではなく、列名を「sys_domain」に設定します。
- Domain Separation はすべてのテーブルに適しているわけではありません。一般に、テーブルがベースインスタンスの一部であり、そのテーブルに **sys_domain** フィールドがない場合は、そのままにしておく必要があります。

「sys_domain」という domain_id タイプのフィールドを作成すると、**sys_domain** フィールドが自動的に作成されます。

2. ドメインを設定するビジネスルールを追加します。

ビジネスルールなし

ドメインは、レコードを作成するユーザーの現在のドメインに設定されます。

ビジネスルールあり

ドメインは、通常は [会社] フィールドに基づいて、スクリプト化されたロジックを使用して割り当てられます。

sys_domain フィールドに加えて、カスタムテーブルには、ドメインフィールドの値を設定するドメイン - ドメインを設定 - タスクに似たビジネスルールが必要です。さらに、最初のルールがドメインの割り当てに失敗した場合に、ドメインのないレコードをデフォルトドメインに移動するドメイン - デフォルト - タスクが必要です。

タスクテーブルで、ドメインのビジネスルールを確認します。[順序] フィールドに特に注意してください。実行の優先度は、低から高まで、[順序] フィールドによって指定されます。

実行される最初のドメイン - ドメインを設定 - タスクルールは、レコードの会社のドメインに基づいてレコードのドメインを設定しようとします。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

最初のルールで適切なドメインが見つからない場合は、2 番目のドメイン - デフォルト - タスクルールが実行されます。このルールは、レコードのドメインをデフォルトのドメインに設定します。

最後に、タスクレコードのドメインが変更されると、ドメイン - カスケードドメイン - タスクビジネスルールによって、ワークフロー、測定基準、SLA、添付ファイルなどのタスクに関連するすべてのレコードのドメインが変更されます。

3. ステップ 2 が失敗した場合のビジネスルールを追加します。

最初のビジネスルールがドメインの設定に失敗し、ドメインがまだ空またはグローバルである場合は、2 番目のビジネスルールが実行されます。このルールは、caller または requested_for フィールドに基づく task_for フィールドを調べます。このルールは、ユーザーのドメインに基づいてレコードのドメインを設定できるかどうかを確認しています。設定できない場合は、ビジネスルールによってドメインがデフォルトドメインに設定されます。

ビジネスルールのサンプルスクリプトは次のとおりです。

```
/* essentially
If (task_for is set)
  set the domain to the user's domain
ELSE
  set the domain to the default domain
*/
```

4. ドメイン - カスケードドメイン - タスク

タスクには、事業達成目標のために連携する多くの関連テーブルを含めることができます。これらの関連レコードには、ワークフロー、SLA、承認、添付ファイル、およびメールが含まれます。タスクのドメインが変更された場合は、関連レコードのドメインも変更して、新しいドメイン内のユーザーに表示されるようにする必要があります。

このカスケードルールは一般に、デフォルトのドメインからレコードを消去するときにトリガーされます。

スクリプトに含まれるカスケードドメインの関連レコードは、次の例のように表示されます。

```
/*
* Keep domains in sync w/related records for:
* workflow context
* workflow history
* approver tables and related workflows
* attachments
* emails
*/
```

ドメインのプロパティとテーマのカスタマイズ

構成したドメイン内の顧客の会社プロパティとテーマをカスタマイズできます。カスタマイズにより、インスタンスを会社の全体的なルックアンドフィールに合わせることができます。

会社のテーマとロゴのカスタマイズ

会社レコードでは、会社ごとに特定のデザインテーマとロゴをカスタマイズできます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ドメインをカスタマイズする

デフォルトでは、サービスプロバイダープラグインがインストールされている場合、コアテーブルに含まれる標準ビジネスルールにより、レコードのドメインがレコードに関連付けられている会社のドメインに設定されます。会社は、タスク、ユーザー、グループ、場所、部門などのテーブルを制御できます。

タスクテーブルを除くこれらすべてのテーブルで、レコードが作成されるドメインを上書きできます。これにより、より多くのカスタマイズオプションが提供されます。

特定の用途のための **Domain Separation** の管理

メール通知に個別のドメインを設定し、カタログ、テーブル、ユーザー、グループ、およびビューのプロパティをカスタマイズすることができます。これにより、各ドメインでより具体的な動作を提供できるため、顧客に柔軟性を提供できます。

メール

メール通知と上書きに個別のドメインを使用できます。通知に個別のドメインを使用する場合、ユーザーのドメイン全体ではなく、添付されたレコードのドメインに基づいて上書きすることができます。

サービスカタログ

Service Catalog はドメイン分離されているため、顧客はカタログを表示してアクセスできます。複数のアイテムが使用される場合、アイテムは OR 条件として処理されます。サービスプロバイダーは、独自の基準に合うようにカテゴリとアイテム自体を管理する必要があります。

ユーザーとグループ

管理者はすべてのドメインにアクセスする必要があるため、グローバルドメインでのみ管理者アカウントを使用してください。グローバルドメインではなく、実際のドメインからすべてのアプリケーションテストを実行します。上書きはグローバルドメインで適切に処理されません。管理者がアプリケーションを使用する場合は、本番環境のユーザーアカウントも指定する必要があります。

フィールドの操作

フィールドを操作する場合は、考慮すべき点がいくつかあります。これらのフィールドには構成に影響する多くのバリエーションが含まれている可能性があるため、注意してください。

リスト
: 個人リスト、グローバルリスト、ドメインリスト、およびそれぞれの複数のビューがあります。

フォーム
: グローバルリストとドメインリスト、およびそれぞれの複数のビューがあります 。

1 つのデータベース
: 作成したフィールドはすべて、すべてのユーザーに対して 1 つのデータベース内に存在します。グローバルな影響度を考慮してから作成してください。

注:
ACL スクリプトは実行されないため、フィールドをリストに表示しないようにすることはできません。ACL がロールベースのみの場合は、READ ACL を追加してユーザーからフィールドを非表示にすることができます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

テーブルの作成

テーブルを作成するときは、sys_domain または sys_overrides フィールドを追加する必要があります。インスタンスユーザーがアクセスする必要があるデータを含むテーブルには、sys_domain フィールドが必要です。プロセスを拡張またはサポートし、子ドメインに移行する必要があるテーブルにも sys_domain フィールドが必要です。

ドメインピッカーを使用した **Domain Separation** の構成

ドメインピッカーを適切に使用し、80/15/5 のアプローチに留意して、インスタンスの過剰なカスタマイズとパフォーマンスへの影響を避けるようにしてください。

変更を行う前にドメインを検証する

ドメインピッカーは、選択できるように、すべてのドメインをリストに収集します。

セッションがタイムアウトすると、ログアウトしていない場合でも、セッションはユーザーレコードのドメインにフォールバックします。同時に、昇格したロールもすべて失われます。この場合、リストの一番上のフレームが再ロードされていなければ、ドメインピッカーには最後に選択したドメインが表示される可能性があります。そのため、一時的にインスタンスから離れている場合は、リストを完全に再ロードする必要があります。

TOP ドメインまたはグローバルドメインでの設定

Domain Separation は、構成およびユーザーとグループの定義がほぼ標準であるサービスを顧客に提供する場合に最適です。カスタマイズして「ワンオフ」ソリューションを作成すればするほど、エラーに対するマージンが増加します。プロセスとビジネスロジックを作成するときは、各顧客に対して自動的に機能するプロパティにバリエーションを設定する必要があります。プロセスは必要に応じて調整できますが、1 人の顧客に一意の構成を作成するタイミングとその程度を決定する際は十分注意してください。

カスタマイズのためのマージンが大きすぎてエラーが発生しないようにするには、ドメインを構成する際に「80-15-5」アプローチを使用する必要があります。

- 構成に推奨されるアプローチ
  - **80%** 以上の標準
  - **15%** 以上のパラメトリック
  - **5%** 未満の構成
- 提案された変更をグローバルプロパティにするか、構成可能なプロパティにするかを決定します。
- 管理が必要なカスタマイズを増やして構築しすぎないでください。代わりに、次の操作を行います。
  - ベースシステム機能から開始し、変更を加える前にギャップを確認します。
  - コードなしのソリューションを探します。
  - サーバー側のスクリプトを使用して、モジュール式の API を構築し、ドメイン分離されたプロパティを構築します。
  - クライアントスクリプトを使用する必要がある場合は、ServiceNow API のみを使用してください。「同期」呼び出し (クライアントとサーバー間でやり取りをするもので、AJAX とも呼ばれます) を制限します。
  - すべてのスクリプトを論理的に記述して、シンプルで効果的なものにします。コード変更のピアレビューを実施し、全員がこのセクションの「サービスプロバイダー向けのドメイン分離の推奨プラクティス」に従っていることを確認します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Domain Separation のパフォーマンスに関する考慮事項

アプリケーションとサービスで Domain Separation を構成するときは、作成するドメインの数とプロパティを必ず考慮してください。プロパティの負荷が大きいドメインが多すぎると、インスタンスのパフォーマンスに影響を与える可能性があります。

プロパティの負荷が大きいドメインの制限

必要な数のドメインを作成できますが、そのインスタンスに不要なドメインを作成しないようにします。多数のプロパティを持つドメインがインスタンス上に多すぎると、インスタンスのパフォーマンスに影響を与える可能性があります。

パフォーマンスに影響を与えるのはドメインに含まれているものではなく、ドメインの数です。プロパティが多すぎると、ドメインピッカーの速度が低下し、顧客の全体的なユーザーエクスペリエンスが低下します。ドメインピッカーをロードしているとき、多くのプロパティを持つ多数のドメインが既に存在する場合、ドメインピッカーはすべてのドメインをロードしてから、セッションのコントロールをユーザーに渡す必要があります。このプロセスにより、ドメインピッカーが終了するまでインスタンス上のものにアクセスできなくなる可能性があります。新しいドメインを作成する前に、以下のドメイン階層に移動します ドメイン管理 > ドメインマップ 実際に新しいドメインを作成する必要があるか、既存の ドメイン階層 が機能するかどうかを確認してください。

コア UI ドメインピッカーの使用

ドメイン参照ピッカーは コア UI で使用できます。参照ピッカーでは、一度にすべてのドメインをロードするのではなく、ドメインの名前をドメインピッカーに入力し始めるとドメインが検索されます。

次の手順に従って、コア UI でドメイン参照ピッカーを有効にします。

1. Application Navigator で、「sys_properties.list」と入力します。
2. *glide.ui.domain_reference_picker.enabled* プロパティを true に設定します。
3. ブラウザを更新します。

> **注:**
> 最初にテストを行わずに統合またはインポートセットを使用して多数のドメイン (30 以上) をアップロードしないでください。インスタンスが停止する可能性があります。

ドメイン階層の設定

ドメイン階層がどのように機能するかを理解し、適切に設定することで、インスタンスの速度低下やパフォーマンスへの影響を回避できます。

ドメイン階層に基づいて、ユーザーはホームドメインと子ドメインのデータにアクセスできます。プロセスは子ドメインに向かって下降し、データは上昇します。

既存のドメイン階層の変更は必要な場合にのみ行ってください。ドメインの親を更新すると、すべての子ドメインとともに親ドメインが再確立され、それによってドメイン階層が変化します。ドメイン階層が更新されると、そのドメインに作成されたレコードのドメインに関連するすべてのテーブルでカスケード更新がトリガーされます。そのため、多数のサポートテーブルも更新する必要があります。

同じ理由から、ドメイン階層を変更する必要がある場合でも、一括更新は行わないでください。ドメイン階層を変更するためにシステムが実行する必要があるクエリーの数を想定してください。更新は常に小さなバッチで行います。次の更新バッチを開始する前に、ドメイン作業要求 (DWR) レコードが処理されていることを確認してください。DWR は、ドメイン階層を変更した後にエラーがあるかどうかを表示するレポートです。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

DWR レコードの追跡

syslog_domain テーブルで、**DWR** の実行が完了したことを示すメッセージ列の情報エントリを探して、DWR が完了したことを確認します。

ドメインログでのエラーと警告の確認

ドメインログを確認して、ドメインパスプロセスと階層構成のエラーまたは警告を特定します。

ドメインログは、ドメインログ [syslog_domain] テーブルにあります。ドメイン階層が更新されると、ドメインパスを再計算するスケジュール設定済みジョブがトリガーされます。ドメインログテーブルは結果をキャプチャします。

このテーブルでエラーと警告を探します。このテーブルを確認した後、これらのエラーを解決し、ドメインパス検証ツールを再度実行する必要があります。

このログの例では、sys_ui_list テーブルで 10 件の孤立レコードが検出されました。ドメインパスを正常に実行するには、これらのレコードのエラーを修正する必要があります。

Error	10 records detected in 'sys_ui_list' that are not in any existing domain and Domain Paths. Fix the domain value in these records & run validator again.	com.glide.domain.validator
Error	10 records detected in 'sys_ui_list' that are not in any existing domain and Domain Paths. Fix the domain value in these records & run validator again. Entries causing the error are as follows:sys_id:1d13ae40470002007f47563dbb9a7170, sys_domain:11722b01473231007f47563dbb9a7154 sys_id:22e34b23470002007f47563dbb9a718c, sys_domain:11722b01473231007f47563dbb9a7154 sys_id:4c85fa809f233100fc6cd4b4232e706b, sys_domain:11722b01473231007f47563dbb9a7154 sys_id:94648b23470002007f47563dbb9a711b, sys_domain:11722b01473231007f47563dbb9a7154 sys_id:a0844b23470002007f47563dbb9a71ef, sys_domain:11722b01473231007f47563dbb9a7154 sys_id:a95ff2c09f233100fc6cd4b4232e7096, sys_domain:11722b01473231007f47563dbb9a7154 sys_id:bd25f4719f233100fc6cd4b4232e70da, sys_domain:11722b01473231007f47563dbb9a7154 sys_id:c1263e809f233100fc6cd4b4232e70f6, sys_domain:11722b01473231007f47563dbb9a7154 sys_id:d8a72c45475002007f47563dbb9a71bb, sys_domain:11722b01473231007f47563dbb9a7154 sys_id:e4c3ce39eb10020045e1a5115206fea0, sys_domain:60e014f69f013100fbf01f80a57fcf00	com.glide.domain.validator

ドメイン分離エラーの詳細については、「Domain Separation エラーのトラブルシューティング」を参照してください。

デフォルトドメインの重要性

ドメインの整理は Domain Separation プロセスの重要な部分です。デフォルトドメインを設定していない場合、新しいタスクとユーザーレコードはグローバルドメインに移動します。グローバルドメイン内のレコードは誰でも表示できるため、本来は表示されないはずのデータが表示される可能性があります。

デフォルトドメインを設定すると、そのレコードは管理者以外のユーザーには表示されません。

注:
デフォルトのアクセス権は、デフォルトドメインまたは親ドメインへの可視性をユーザーに付与することで変更できます。

インスタンスのドメインレコードには常に 1 つのデフォルトドメインを設定する必要があります。ドメインにまだアサインされていないタスクレコードとユーザーレコードが、デフォルトドメインに自動的にアサインされます。

[ドメイン管理] 画面からデフォルトドメインを作成する場合は、他のドメインと区別するために [名前] フィールドに「デフォルト」という名前を追加します。レコードの [デフォルト] チェックボックスをオンにします。

デフォルトドメインで作成したレコードを定期的に管理し、適切なドメインに移動させます。デフォルトドメインでレコードが頻繁に表示される場合は、その理由を調べる必要があります。すべてのレコードが適切なドメイン (グローバルまたはデフォルトドメインではない) に作成されるようにするのが理想的です。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

包含クエリーとドメインアクセス

「包含」クエリーは特別な場合にのみ使用します。たとえば、ユーザーまたはグループがアクセス権のないドメインのデータを表示する必要があるが、それらのユーザーをドメインに移動させない場合などです。ドメインの「包含」およびユーザーアクセスまたはグループアクセスは、絶対に必要な場合にのみ例外的に作成できます。

「包含」は多対多のドメイン間関係であり、プロセスのフローには影響しません。多数のドメイン「包含」関係を作成したり、幅広いアクセス権を提供したりすると、OR 条件の多すぎるクエリーが生成されます。OR 条件を指定すると遅くなり、インスタンスのパフォーマンスに影響を与えます。過多の「包含」関係を使用する代わりに、次のようにドメイン階層を設定します。

サンプルクエリ

```
SELECT ... FROM task task0 ignore index(number) WHERE task0.`sys_class_name`
= 'incident' AND (task0.`sys_domain_path` = '/' OR task0.`sys_domain_path` LI
KE '!!$/!!(/%' OR task0.`sys_domain_path` LIKE '!!$/!!$/!!&/%') ORDER BY task
0.`number` DESC limit 0,20
```

ユーザーをドメインに移動させる前に、ユーザーがそのドメインに本当にアクセスする必要があるか確認してください。メリットと制限事項について熟考します。上記のクエリーは、単に 1 つの包含関係のためのものです。別のドメインが含まれるドメインがあり、そのドメインが他の多数のドメインの親である場合は、さらに多くの OR 条件が発生します。ドメインマップを作成するときは、インスタンスのパフォーマンスに影響を与えないように注意してください。

ドメインパスのクエリー方法

ドメインパスを使用して効果的なクエリーを作成できます。

ドメインスプール (sys_domain) またはドメイン番号付けの代わりにドメインパスを使用します。ドメインパスを使用するクエリーは、スプールや番号付けよりもはるかに高速です。

ドメインパスは、ドメイン分離が有効になっているインスタンスのデフォルトのクエリー方法です。

インスタンスのクエリー方法を検証するには、管理者ダッシュボードで次のシステムプロパティを探します。

- *If domain path is enabled*：システムプロパティテーブルに、glide.sys.domain.provider=domain_paths および glide.sys.domain.paths.installed=true が表示されます。
- *If domain path is not enabled*：システムプロパティテーブルに、glide.sys.domain.provider != domain_paths,glide.sys.domain.paths.installed=false が表示されます。

遅いクエリーと SQL のデバッグ

SQL と遅いクエリーをデバッグすると、インスタンスでの遅い問題を解決できます。

インスタンスをデバッグするときは、SQL デバッグを有効にして遅いクエリーを探すか、[システム診断] > [統計] > [遅いクエリー] に移動して遅いクエリー [sys_query_pattern] テーブルを確認します。このテーブルは、すべての遅いクエリーをインスタンスに格納します。

テーブルを検索するときに、domain_path を含むクエリーを探して、インスタンス内のドメインパスが原因であるかどうかを判断します。

遅いクエリーが見つかった場合は、遅い理由を分析してください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

クエリーが遅い一般的な理由

- クエリーに含まれる OR 条件が多すぎます (詳細については、「包含クエリーとドメインアクセス」を参照してください)。ドメイン階層で、包含または可視性の必要がない階層レベルにユーザーまたはドメインを配置します。
- クエリー方法は、ドメインパスクエリー方法ではありません (詳細については、「ドメインパスのクエリー方法」を参照)。ドメインパスのクエリー方法を使用していない場合は、カスタマーサービス & サポートに連絡してください。
- クエリーでは、データベースの内容をすばやく確認できるようにデータベースをインデックス化する必要があります。遅いクエリーを特定できる場合は、「explain plan」を実行して、インデックス作成のオプションがあるかどうかを確認します。「explain plan」は、クエリーとその処理内容を表示する SQL の機能です。

クエリ前ビジネスルール

クエリ前ビジネスルールを使用して、インスタンスでデータ分離をサポートすることができます。Domain Separation をサポートする ServiceNow アプリケーションは、データとデータルーティングの分離のみをサポートするか、高度なビジネスロジック分離機能があるか、アプリケーションのテナント (顧客) レベルの管理をサポートする可能性があります。

クエリ前ビジネスルールは、ドメイン分離された環境内でデータ分離をサポートするために使用する補足コードです。

⚠ 警告:
Domain Separation プラグインの代わりにクエリ前ビジネスルールを使用しないでください。このビジネスルールは、プラグインほど安全にデータ漏洩を防止しません。

データ分離のためのクエリ前ビジネスルールの使用

次の状況では、クエリ前ビジネスルールをデータ分離と併用できます。

- Domain Separation が ServiceNow アプリケーションでサポートされておらず、サービスプロバイダー組織外の 1 人以上の外部顧客にテーブルまたは行へのアクセスを許可または制限する必要がある場合。

  注:
  開発を開始する前に、その製品のアプリケーションロードマップについて ServiceNow カスタマーサポートにお問い合わせください。ドメインサポートの改善が今後のリリースで計画されている可能性があります。

- テーブルがドメイン分離されていても、システム内の一連のドメインにのみ適用される特定の条件に基づいて、その行へのアクセスを許可または制限する必要がある場合。

  注:
  たとえば、X ドメインの顧客にはそのドメインをサポートする複数のベンダーがあり、それらのベンダーには、割り当てられたレコードのみを表示するためのアクセス権が付与されます。

クエリ前ビジネスルールを作成する前の考慮事項

ユーザー情報、グループメンバーシップ、会社、ロール、またはレコード固有のフィールド条件の組み合わせに基づいて、クエリ前ビジネスルールをスクリプト化して、親テーブルと子テーブルにアクセスできないようにすることができます。クエリ前ビジネスルールは個別のドメインに配置され、ドメイン階層の特定の分岐にグローバルに適用されるように作成されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- 可能な場合は、適用されるユーザーに対してのみルールが実行されるように、ドメイン階層のできる限り低いところでクエリ前ビジネスルールを作成します。
- ビジネスルールが実行されないシナリオや、ユーザーがトリガーしたインタラクションが実行するビジネスルールをトリガーしないシナリオが存在することを理解してください。たとえば、[ビジネスルールを実行] がオフになっている変換マップがある場合、またはワークフローが無効になっているスクリプトがある場合、ビジネスルールは実行されません。
- 必ず条件フィールドを入力して、ルールを実行するタイミングを指定します。たとえば、ビジネスルールをドメイン内の特定のベンダーにのみ適用するかどうかを指定できます。

> **警告:**
> ビジネスルール (特にクエリービジネスルール) を設計およびコーディングするときは、OR 句とインデックスのないフィールドの検索を制限します。インデックス化されていないフィールドで OR 句や検索が多すぎると、クエリが遅くなったり、インスタンスのパフォーマンスに影響したりする可能性があります。

- クエリ前ビジネスルールは必要な場合にのみ使用します。クエリ前ルールが多すぎると、インスタンスのパフォーマンスに影響を与える可能性があります。

クエリ前ビジネスルールは、アクセス制御リスト (ACL) の前に実行され、全体的なパフォーマンスを向上させます。これは、システム内の複数のドメインにアクセスできるサービスプロバイダー (SP) 環境のユーザーに返される結果を制限する場合に特に当てはまります。

> **注:**
> データのフィルタリングは (ACL とは異なり)、データのやり取りをするときに「データセキュリティは…を制限します」というメッセージが表示されないユーザーにとって透過的になります。

クエリ前ビジネスルールと **ACL** を使用しない場合

クエリ前ビジネスルールと ACL を使用して顧客データを分離する場合は注意してください。ビジネスルールと ACL の両方を使用して、カスタマイズを作成し、それを維持する必要があります。カスタマイズはパフォーマンスの問題を引き起こす可能性があります。開発チームは、システムが壊れないようにプロセスを作成する必要があります。

Domain Separation は、広くサポートされているフレームワークである現在のドメインパスクエリー方法 (v3) を使用して、スケーラビリティとガバナンスの両方を提供します。ServiceNow プラットフォームチームとアプリチームは、フレームワークを維持する責任を負い、顧客の負担を軽減します。

多くのインスタンスで多数の顧客を持つ企業では、クエリ前ルールと ACL を過度に使用すると、データベースクエリのパフォーマンスが低下する可能性があります。

Domain Separation を有効にする方法

ServiceNow プラグインを使用して Domain Separation を有効にできます。製品マネージャーが機能を管理し、開発チームが製品マネージャーをサポートします。ServiceNow リリースには、Domain Separation 機能の拡張と修正が含まれています。インスタンスオーナーは、Domain Separation のサポートについて、https://support.servicenow.com の サービスポータル など、カスタマーサービス & サポートリソースを参照できます。

スクリプトでのドメインパスの回避

ドメインパスによってスクリプトの値が変更されたり壊れたりする可能性があるため、スクリプトでは使用しないでください。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

ドメイン階層を変更すると、ドメインパスが再計算されてその値が変更されるため、スクリプトがドメインパスに依存しないようにしてください。このようなことが発生すると、スクリプトが役に立たないか、エラーがスローされたり壊れたりする可能性があります。最適な方法は、ドメインパスに基づいてスクリプトを作成しないことです。

ドメインパスに依存するのではなく、スクリプトで **sys_domain** フィールドを使用します。ドメイン階層を変更すると、ドメインパスが再計算されてその値が変更されるため、スクリプトが役に立たなくなったり、エラーがスローされたり、壊れたりする可能性があります。独自のスクリプトを作成する前に、**[sys_domain]** フィールドを使用するベースシステムのビジネスルールを検索してください。

ServiceNow プラットフォームは、各インスタンスのドメイン階層の違いによる問題を回避するために、更新セットの sys_domain_path 値をキャプチャしません。したがって、更新セットをインポートした後にドメイン階層を検証して、レコードのドメインパス値が正しいことを確認する必要があります。

ドメインパスの詳細については、「Domain Separation を要求する」および「Domain Separation センター」を参照してください。

ドメインアサイン

ドメインのアサイン方法は sys_domain フィールドの値に影響します。アサインには、各ドメインでのアプリケーションの機能に影響するデザインとビジネスプロパティが含まれています。

sys_domain フィールドの値

sys_domain フィールドの値には、次のいずれかでレコードにアサインされたドメインが含まれます。

- ユーザーが所属する会社
- レコード作成時に使用されるビジネスルール
- レコード作成時に使用されるモジュール
- レコード作成時に使用されるフォームテンプレート
- 親レコードのドメイン
- ユーザーレコードにアサインされたドメイン
- 作成したユーザーのドメイン

ドメインアサインの戦略と設計が適切に文書化され、テストされていることを確認して、これらの戦略と設計が正しいドメインに挿入されるようにします。これにより、各ドメインのプロパティを複製または変更する必要があることを確認できます。

ドメイン分離と カスタマーサービス管理 **(CSM)** プラグイン

最良の結果を得るには、CSM プラグインのプロパティがどのように機能するかに注意してください。プラグインを有効にすると、ドメイン内のレコードのステータスを確認できます。

インスタンスオーナーは、*csm_auto_account_domain_generation* プロパティを有効にするためにカスタマーサービス & サポートに連絡する必要があります。

注:
このベースシステムプロパティは、システムプロパティテーブルにあり、CSM プラグインを有効にした後に使用できます。

プロパティの機能

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

Customer Service アプリケーションで新しいアカウントが作成されると、ドメインが作成され、TOP ドメインの下に配置されます。アカウントフォームの親フィールドに値が入力され、新しいレコードが挿入されると、そのアカウントが親のサブドメインとして作成されます。

このプロパティが true でなく、ドメインが有効になっている場合の動作

ドメイン分離された環境の新しいアカウントレコードは、デフォルトのドメインに自動的に配置されます。

ヘッダーバーで、プラグインが有効になっているレコードのステータスを確認できます。

Domain Separation のヘルプ

Domain Separation に関する追加のアシスタンス

Domain Separation の概要については、このショートビデオをご覧ください。

Domain Separation の概要ビデオ

探索、学習、開発

推奨プラクティス

ドメイン構造を適切に作成および開発するためのヒント

サービスプロバイダーの概念

一般的なユースケースの解決に役立つ ServiceNow プラットフォームを扱う概念

アプリケーションによるサポートレベル

アプリケーションで Domain Separation はサポートされていますか？サポートレベルとユースケースを参照してください。

クラス

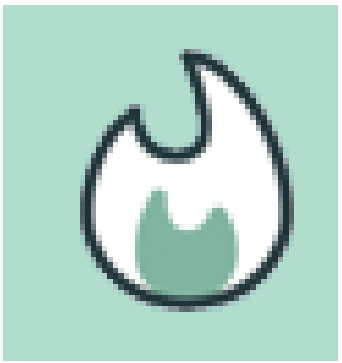
- 開発者向け: ServiceNow 開発者サイトのドメイン分離
- サービスプロバイダー向け：サービスプロバイダー向け Domain Separation (ServiceNow University ログインが必要)

Safe Workplace Suite と Domain Separation

ServiceNow Safe Workplace アプリケーションは、緊急時や COVID-19 のようなパンデミックの後に職場を再開し従業員の健康と安全をサポートするために役立ちます。このスイートには、組織の動員、復旧、および再構築に役立つ多くのアプリケーションが搭載されています。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



セットアップと管理

- アップグレード
- Domain Separation を要求する
- ドメインを作成する
- 内部や外部の顧客に委任できる構成

トラブルシューティング

- Known Error Portal で既知のエラー記事を検索
- 担当者 カスタマーサービス & サポート
- コミュニティで質問や回答をする

Domain Separation のセットアップと管理

Domain Separation を設定するには、プラグインのアクティベーションを要求し、オプションを設定し、ユーザーとレコードをドメインに割り当てる必要があります。

Domain Separation を設定するには、次の操作を行います。

1. Domain Separation を要求する
2. ドメインを作成する
3. テーブルへのドメインフィールドの追加

ドメインでは、次の基本的な管理タスクを実行することもできます。

- ドメインを有効または無効にする
- ドメイン関係を表示する
- ドメインスコープを展開する
- ドメイン固有の選択リストを作成する

Domain Separation を設定して基本的な管理を行った後に実行するタスクのリストについては、「詳細な Domain Separation 管理」を参照してください。

内部や外部の顧客に委任できる構成

Domain Separation は、ServiceNow® サービスプロバイダー (SP) が顧客に提供するサービスを設定できるように設計されています。このトピックで詳しく説明されているいくつかのエリアを除き、顧客がこれらのサービスを自分で管理できるように設計されていません。

概要

SP の顧客は、ライセンスや他の顧客に影響を与えないドメイン内のデータを自分で安全に管理することができます。たとえば、顧客が新しいレポートを作成したり構成アイテムを管理したりすること

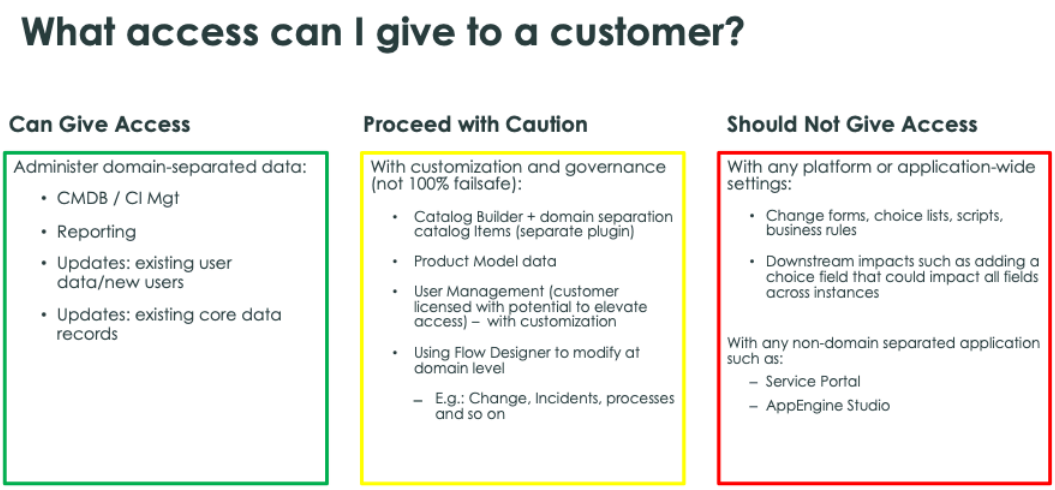
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

は安全ですが、フィールド、選択肢、ビジネスルール、および同じインスタンス上の他の顧客に影響を与える可能性のあるその他のプロセスをカスタマイズすることは安全ではありません。

ServiceNow プラットフォームの ServiceNow ベースシステム管理ロールとそのアクセス制御は、インスタンスごとに 1 人の管理者チーム用に設計されています。たとえば、インスタンスのすべてのドメイン設定を管理し、新しいドメインを作成するために、domain_admin ロールが SP のリソースの 1 つに付与されます。ドメイン固有の管理タスクで SP は、顧客に特定のアクセス権を付与するために、必要に応じて新しい「顧客管理者」ロールとアクセス制御を作成する必要があります。

次の画像は、顧客が安全に実行できるさまざまなカテゴリの一般的な管理者機能の概要で



す。

🟢 アクセス権を付与可能

例：

- CMDB での CI データ管理
- レポートの作成
- 既存のユーザーデータの更新、またはロールのない新規ユーザー
- 部門、グループ、場所、コストセンター、ロールのない新しいグループ、新しい部門/コストセンター/場所などの既存のコアデータレコードを更新します。

🟡 注意して続行

例：

- カタログアイテム：顧客が更新できる顧客固有のカタログアイテムを作成するために、次の 2 つの機能を併用できます。カタログアイテムの Domain Separation (Domain Separation と Service Catalog) を使用することで、インスタンスオーナーは顧客のドメイン内にアイテムを作成することができます。インスタンスオーナーは、顧客が価格、説明、画像などの安全なフィールドを更新できるようにするロールを作成できます。カタログビルダー (Quebec リリースの新機能) を使用すると、SP 管理者チームは、規範的な UI エクスペリエンス内から顧客のドメインで新しいアイテムを作成するために、顧客に安全に配布できるアイテムテンプレートを作成できます。
- ユーザー/グループ管理：ユーザーレコードの作成と変更ができる「顧客管理者」ロールを安全に作成できますが、ロールの追加や削除はセキュリティとライセンスに影響を与える可能性があります。ベースシステムでは、顧客が安全に付与できるロールを細分化することはできません。グルー

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

プの作成と変更についても同様です。グループ自体を変更することはできますが、ロールの追加や削除はコントロールする必要があります。

- Flow Designer：ServiceNow フローデザイナー は、テーブルのプロセス (ワークフロー) を作成するために使用する構築ツールです。flow_designer ロールで、顧客はスクリプトなしにフローを構築できます。階層内で上位のドメイン内のすべてのフローを読み取ってクローンを作成できます。ドメイン内でフローの作成と変更ができます。ただし、これはサイロでは行えません。プロセスが互いにキャンセルし合ったり、他の競合が発生したりしないように、プロセスに影響を与える可能性のあるユーザーをグローバル管理者チームに追加する必要があります。

アクセス権を付与しない

選択フィールドの仕組みを理解することは、SP 管理者チームのみが選択フィールドを管理する必要がある理由を理解するのに役立ちます。

- 選択フィールドの構造：選択フィールドの値は sys_choice テーブルに格納され、テーブル、ドメイン、および言語に基づいてグループ化されます。

  たとえば、タスクの [ステータス] フィールドは、タスクを拡張するすべてのテーブルで使用できます。したがって、各テーブルが独自の値を持ち、それらの値にドメイン数を乗じ、ドメイン値に言語数を乗じることができます。

  すべてのテーブル、ドメイン、および言語の [ステータス] のすべての値が [ステータス] フィールドの値と見なされます。

- 選択フィールドの変更の仕組み： 選択フィールドが更新されると、そのフィールドのすべての値 (テーブル、ドメイン、言語) を含むペイロードが作成されます。このペイロードをインスタンスにインストールすると、フィールドの既存の値がすべて削除され、新しい値がロードされます。これにより、重複するエントリや残っていた無効な値がなくなります。

  そのため、ドメイン分離されたインスタンスで選択フィールドを直接更新する機能を顧客に提供することはできません。インスタンス全体に影響してしまうためです。また、選択フィールドに影響するインポートされた更新セットにより既存の選択肢が上書きされるため、本番インスタンスで選択肢を直接更新することもできません。場合により、選択フィールドでプロセス自体が実行される可能性があります。このプロセスは、顧客が選択フィールドを変更しようとすると中断されます。

詳細については、以下を参照してください。

- Exploring user administration
- ACL ルールを作成する
- NowLearning のサービスプロバイダーラーニングパス
- サービスプロバイダーの Domain Separation
- サービスプロバイダーの概念
- Domain Separation のアプリケーションサポート
- Domain Separation のリリースノート

Domain Separation を要求する

すべてのドメインサポート機能は、**Domain Support - Domain Extensions Installer** と呼ばれるプラグインでアクティブ化されます。管理者は、このプラグインのアクティブ化を要求できます。

始める前に

サブスクリプションを購入するには、ServiceNow アカウントマネージャーにお問い合わせください。アカウントマネージャーは通常数日以内に、組織の本番および準本番インスタンスで

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

com.glide.domain.msp_extensions.installer プラグインがアクティブ化されるように手配することができます。

アカウントマネージャーがいない場合、購入後にアクティブ化を延期することを決定するか、無料で準本番インスタンスで製品を評価する場合には次の手順を実行します。

必要なロール：admin

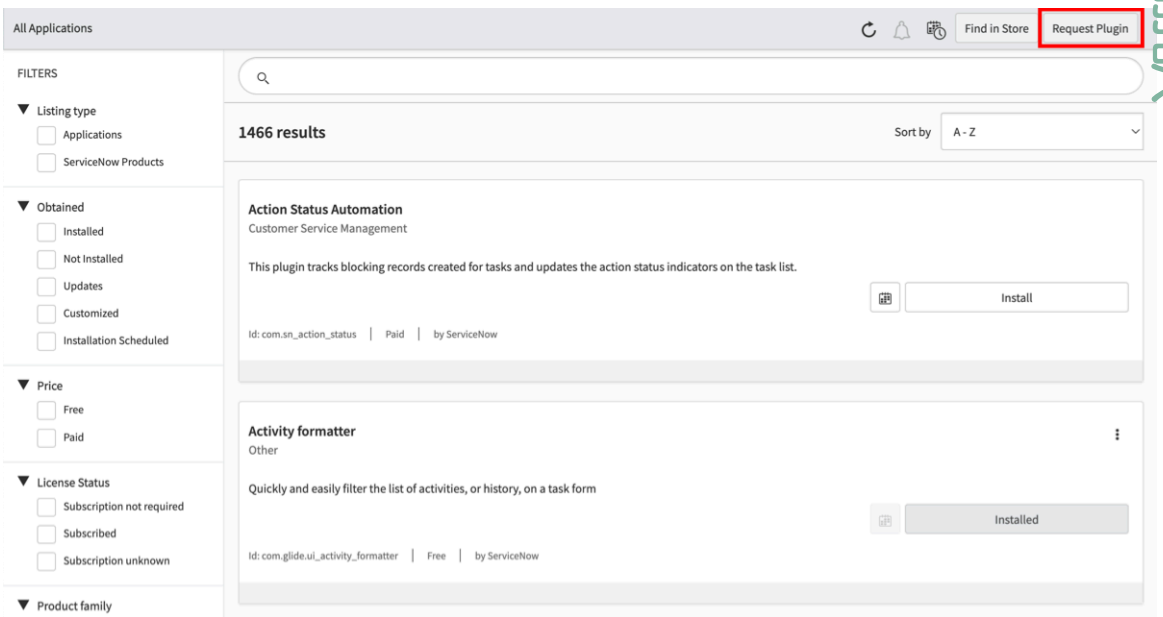
このタスクについて
Domain Support - Domain Extensions Installer プラグインがすでにアクティブな場合、Domain Support - Domain Extensions Installer プラグインのコンテンツは、既存の実装との潜在的な競合を回避するためにインストールされません。

Domain Separation は Company Separation に替わるものです。Helsinki リリース以降、Company Separation プラグインをアクティブ化できなくなりました。ただし、Domain Separation をアクティブ化したときに Company Separation が既にアクティブになっている場合は、両方のプラグインが同時にアクティブになります。*glide.db.separation.field* プロパティを使用して、Company Separation のアクティベーションステータスをコントロールできます。

注:
Helsinki 以降は、ドメインパスはすべての顧客に使用されます。ドメイン番号付けは使用されなくなりました。カスタマーサービス & サポートがアップグレードのサポートを行います。

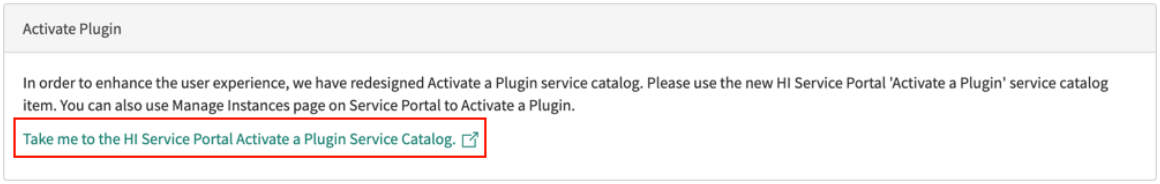
手順

1. 移動先 すべて > システムアプリケーション > 利用可能なすべてのアプリケーション > すべて。
2. [すべてのアプリケーション] ページで [プラグインの要求] をクリックして、Now Support で [プラグインをアクティブ化] フォームを開きます。



3. Now Support で、Now Support サービスポータル サービスカタログ にアクセスするリンクを選択します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



4. インスタンスを選択します。
5. [アクション] > [プラグインのアクティブ化] を選択します。
6. [プラグインのアクティブ化] フォームで、次の情報を入力します。

[プラグインのアクティブ化] フォーム

フィールド	説明
ターゲットインスタンスは何ですか	プラグインをアクティブ化するインスタンス。
どのプラグインをアクティブ化しますか	アクティブ化するプラグインの名前です。 **注:** 必要なプラグインが表示されない場合、または OEM またはオンプレミスのインスタンスでプラグインをアクティブ化している場合は、[探しているプラグインが表示されていません **(Plugin I'm looking for is not listed)]** チェックボックスをオンにして、プラグインの名前を入力します。
メンテナンスの日時を選択 (Select Maintenance Date and Time)	プラグインをアクティブ化する日時。 **注:** プラグインは、米国太平洋標準時で、毎営業日の朝と夕方の 2 回のバッチでアクティブ化されます。特定の時刻にプラグインをアクティブ化する必要がある場合は、[理由/コメント **(Reason/ Comments)]** フィールドに要求を入力します。

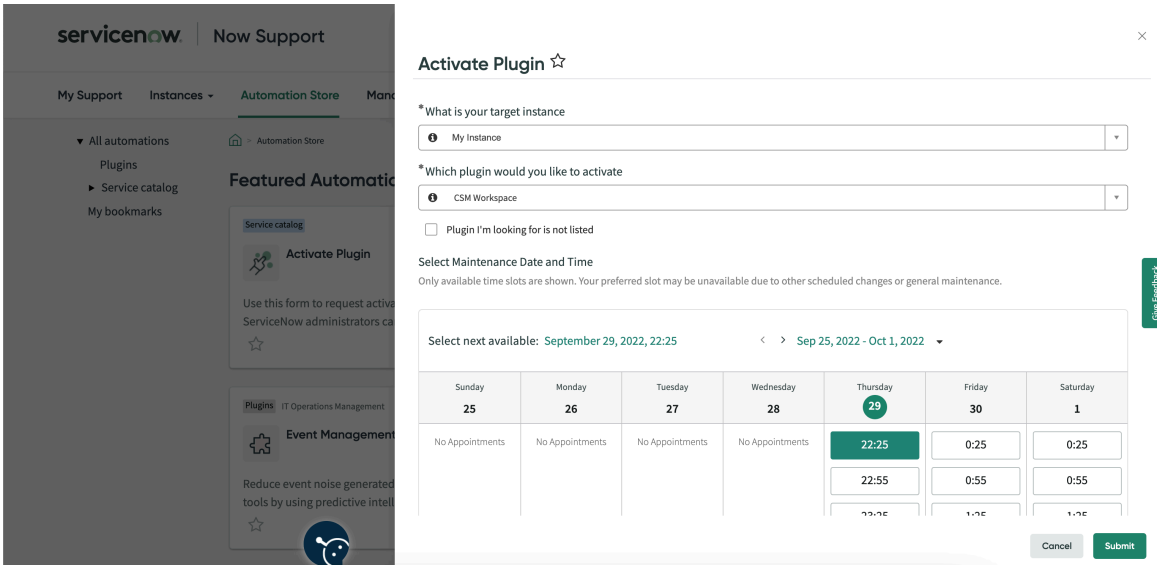
Example

たとえば、 [自分のインスタンス (My Instance)] という名前のインスタンスで CSM Workspace プラグインをアクティブ化するには、次のフォームを参照してください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

[プラグインのアクティブ化] フォーム



7. [送信] を選択します。
プラグインの要求の詳細については、次を参照してください。 の Service Catalog [KB0751715] 記事からのプラグインの要求 Now Support ナレッジベース。

タスクの結果
Domain Extension Installer プラグインをアクティブにすると、次の機能が有効になります。

- Domain Separation はドメイン [sys_domain] テーブルに基づいています。
- 委任管理では、各ドメインに個別のポリシーを設定できます。
- すべてのレコードはグローバルドメインの一部です。
- 現在のユーザーのドメインによって、使用するドメインが決まります。表示 または別のドメインのレコードで操作します。

関連情報

Domain Separation プラグイン

Domain Separation プラグイン

Domain Support - Domain Extensions Installer プラグインは、複数の Domain Separation 機能とプロパティを一度にアクティブにします。このプラグインは通常、Domain Separation プラグインと呼ばれます。

Domain Separation プラグインをアクティブにするための推奨プラクティス

Domain Separation 開発の一環として、管理者はこのプラグインのアクティベーションを要求する必要があります。最良の結果を得るには、開発プロセスの開始時に、他のプラグインをアクティブにする前に、Domain Separation プラグインをアクティブにします。

重要:
Domain Extensions Installer プラグイン (com.glide.domain.msp_extensions.installer) のアクティブ化を要求してから Domain Separation プラグイン (com.snc.pa.domain_support) をアクティブ化するように要求します。

ServiceNow の実装の最後に Domain Separation を有効にした場合、またはインスタンスが稼働すると、アプリケーションのパフォーマンスとプロセスの両方がリスクにさらされます。確立された

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

インスタンスでは、開発の構造によっては、プラットフォームとその使いやすさに対するリスクが高くなる可能性があります。Domain Separation プロセスの詳細については、「Domain Separation の概要」を参照してください。

たとえば、Domain Separation プラグインがアクティブになっている場合、ドメイン (sys_domain) 列がタスクテーブルに追加され、既存のすべてのレコードが自動的にグローバルに配置されます。スクリプトを使用してすべてのレコードを正しいドメインに割り当てるには、確立された親子階層が必要です。これらのタイプのスクリプト化されたアクションでは、大量のデータを移動するときにデータの破損や損失が発生し、本番環境でダウンタイムが発生する可能性があります。ビジネスルール、クライアントスクリプト、フォームビュー、ワークフローなどのプラットフォームコードの多くも、グローバルに配置されます。

顧客がコードを作成したり ServiceNow コードを変更したりすると、プラットフォームのパフォーマンスと使いやすさが低下します。インスタンスオーナーは、このタイプのアプローチでは、実装が大幅に遅れたり、長いダウンタイムが発生したりする可能性があります。

Domain Separation プラグインの機能

プラグインを有効にすると、次の機能が有効になります。

- Domain Separation はドメイン [sys_domain] テーブルに基づいています。
- 委任管理では、各ドメインに個別のポリシーを設定できます。
- すべてのレコードはグローバルドメインの一部です。
- 現在のユーザーのドメインによって、使用するドメインが決まります。表示 または別のドメインのレコードで操作します。

関連情報

サービスプロバイダー向けのドメイン分離の推奨プラクティス

ドメインシステムのプロパティとユーザー初期設定

管理者は、ドメインスコープをコントロールするプロパティとユーザー初期設定にアクセスできます。

プロパティ

Domain Separation を新しくアクティブにすると、関連するすべてのデータまたはプロセスのレコードのドメインスコープが自動的に制限されます。ユーザーがフォームでレコードを表示すると、レコードの関連データ (参照ピッカーや関連リストデータなど) と適用されるプロセス (ビジネスルールやクライアントスクリプトなど) がレコードのドメインスコープに制限されます。複数のタブにレコードがある場合、各タブには、そのタブ内で開かれたレコードに基づく独自のドメインスコープがあります。次のプロパティは、ドメインスコープをレコードのドメインとユーザーの現在のセッションドメインのいずれかに制限します。

ドメインシステムプロパティ

プロパティ	詳細
glide.sys.domain.use_record_domain_for_processes	ドメインスコープをすべてのプロセスのレコードのドメインに制限します。このプロパティはビジネスルールには適用されません。ビジネスルールは常にドメインレコードから処理されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ドメインシステムプロパティ (続く)

プロパティ	詳細
	• タイプ：true | false • デフォルト値：true • 場所：システムプロパティ [sys_properties] テーブル
glide.sys.domain.use_record_domain_for_data	ドメインスコープをすべてのデータのレコードのドメインに制限します。 • タイプ：true | false • デフォルト値：Fuji 以降の新しいドメインアクティベーションでは true (Fuji より古いインスタンスからのアップグレードには、このプロパティはテーブルにありません) • 場所：システムプロパティ [sys_properties] テーブル

glide.sys.domain.use_record_domain_for_processes または *glide.sys.domain.use_record_domain_for_data* プロパティのいずれかが **true** に設定されている場合、次のプロパティは設定に関係なく使用されません。

- *glide.sys.domain.use_record_domain*
- *glide.sys.domain.use_record_domain_for_client_scripts*
- *glide.sys.domain.domain_change_notify*
- *glide.sys.domain.no_change_roles*

プロパティの完全なリストについては、「利用可能なシステムプロパティ」を参照してください。

注:

Jakarta リリース以降の Domain Separation の新しいアクティベーションでは、セッションドメインがドメインテーブルで実行されるビジネスルールを決定します。以前のバージョンでは、ドメインテーブルで実行されるビジネスルールは、新しく作成されたドメインの階層に基づいて設定されていました。この動作は *glide.sys.domain.skip_domain_insert_businessrules* プロパティによって変更されます。このプロパティを true に設定すると、ドメイン挿入のパフォーマンスが大幅に向上します。

ドメインテーブルで実行されるビジネスルールのドメインスコーププロパティ

プロパティ	詳細
glide.sys.domain.skip_domain_insert_businessrules	ドメインテーブルで実行されるビジネスルールのドメインスコープを指定します。Domain Separation の新しいアクティベーションでは、プロパティのデフォルトは true であり、ビ

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ドメインテーブルで実行されるビジネスルールのドメインスコーププロパティ (続く)

プロパティ	詳細
	ジネスルールはセッションドメインによって決定されます。既存の実装では、プロパティのデフォルトは false であり、ビジネスルールは新しく作成されたドメインの階層によって決定されます。 • タイプ：true | false • デフォルト値：Jakarta 以降、新しいドメインのアクティベーションでは true です。既存の実装では False です。
glide.sys.domain.skip_non_global_businessrule_if_nodomain	queryNoDomain() を使用する場合、またはテーブルがドメイン分離されていない場合に、グローバルドメインからの bus.rules のみが実行されるようにするため、他のビジネスルールはスキップできます • タイプ：true | false • プロパティを false に設定すると、以前の動作が復元され、ServiceNow の推奨プラクティスに沿ったものにはなりません。 • 推奨：テーブルをドメイン分離します。セッションドメインではなく、常にレコードのドメインを使用するようにしてください。

ユーザー初期設定

さらに、ユーザー管理者は、次のユーザー初期設定をグローバルまたはユーザーごとに設定できます。

ドメインスコープのユーザー初期設定

設定	カテゴリ	更新者	詳細
glide.domain.session_scope	ドメイン	管理者	true の場合、デフォルトのスコープをレコードのドメインではなくユーザーのセッションドメインに設定します。false の場合、デフォルトのスコープはレコードのドメインで

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ドメインスコープのユーザー初期設定 (続く)

設定	カテゴリ	更新者	詳細
		のみ	す。domain_expand_scope ユーザーロールのユーザーは、必要に応じてドメインスコープを変更できます。 • タイプ：true | false • デフォルト値：false
glide.domain.session_scope_notification	ドメイン	管理者のみ	true の場合、レコード値に展開されたドメインスコープが含まれていることを示す視覚的なキューが表示されます。false の場合、通知は非表示になります。 • タイプ：true | false • デフォルト値：true

関連情報

Domain Separation アプリケーションプロパティ

ドメインを作成する

[domain] テーブルにレコードを作成することで、ドメインを作成できます。

始める前に

必要なロール：管理者

このタスクについて

新しいドメインを作成するときは、次の点に注意してください。

- 1 つのドメインのみをデフォルトドメインにすることができます。
- 1 つのドメインのみをプライマリドメインにすることができます。

手順

1. 移動先 すべて > ドメイン管理 > ドメイン.
2. [新規] をクリックします。
3. 必要なフィールドに入力します (表を参照)。
4. [送信] をクリックします。

ドメインフォームのフィールド

フィールド	説明
名前	ドメインの一意の名前を入力します。
タイプ	ドメインを説明するドメインタイプを選択します。デフォルトでは、ドメインタイプはベンダー、顧客、および *MSP* です。独自の選択肢を追加することもできます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
プライマリ	このドメインを階層のトップレベルドメインにする場合は、このチェックボックスをオンにします。トップレベルドメインには子ドメインのみがあり、親ドメインはありません。
デフォルト	このドメインを階層のデフォルトドメインにする場合に選択します。
親	このドメインを含む階層の上位のドメインの名前を選択します。このフィールドには、ドメインマップに表示されるドメインの値が必要です。
有効	このチェックボックスをオンにしてドメインを使用できるようにします。このドメインをドメインマップに表示するには、このオプションを選択する必要があります。
説明	ドメインの説明を入力します。

各ドメインレコードには、次の複数の関連レコードを含めることもできます。

- 会社
- 包含ドメイン
- 次のものに含まれる：

次のタスク
ドメイン階層を変更するには、包含ドメイン関連リストに移動し、包含関係の子 (含まれている) ドメインであるドメインレコードを選択します。

デフォルトドメインの設定

ドメインを、ドメインにまだアサインされていないタスクレコードおよびユーザーレコードが自動的にアサインされるデフォルトドメインにします。

始める前に
必要なロール：管理者

このタスクについて

注:
デフォルトドメインを設定していない場合、新しいタスクとユーザーレコードはグローバルドメインに配置されます。

手順

1. 移動先 すべて > ドメイン管理 > ドメイン.
2. たとえば Main など、デフォルトドメインにするドメインを開きます。
3. [デフォルト] フィールドを追加するため、フォームレイアウトを設定します。
4. [デフォルト] チェックボックスをオンにします。
5. [更新] をクリックします。

特定のレコードのドメインを手動で管理する

デフォルトでは、ユーザーの会社レコードに基づいてドメインが自動的に割り当てられます。ただし、場合によっては、ドメイン管理者が特定のレコードが属するドメインを手動で管理する必要があります。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

始める前に
必要なロール：管理者

このタスクについて
[管理対象ドメイン] フィールドで、ドメイン管理者は、会社レコードから自動的に割り当てられたドメインを使用するのではなく、ユーザー、グループ、部門、場所、または CI レコードのドメインを手動で選択できます。[管理対象ドメイン] フィールドは、次のレコードタイプで使用できます。

- ユーザーレコード
- グループレコード
- 部門レコード
- 場所レコード
- CI レコード

手順

1. 手動で管理するレコードに移動します。
2. [管理対象ドメイン] チェックボックスをオンにします。
3. [ドメイン] フィールドから、レコードのドメインを選択します。
4. [更新] をクリックします。

   [管理対象ドメイン] チェックボックスをオフにすると、[ドメイン] フィールドが非表示になり、レコードではレコードの会社のドメイン値が使用されます。

関連情報

サービスプロバイダー向けのドメイン分離の推奨プラクティス

ドメイン分離テーブル

ドメイン分離テーブル機能を使用すると、インスタンス内のどのテーブルがドメイン分離されているかを一目で確認できます。

概要

ドメイン分離テーブル機能を使用して、ドメイン分離されているテーブルを確認します。[すべて] フィルターに「ドメイン」と入力し、左側のナビゲーションペインでドメイン分離テーブルにアクセスします。

このビューをフィルタリングして列名を表示または削除し、テーブルに含まれる特定のプロパティまたは属性を検索できます。リストに表示されるテーブルタイプは 2 つあります。

- 明示的な *sys_domain* 列が存在するテーブルで、列名にリストの *sys_domain* の値が表示されます。
- *domain_master* 属性を使用して参照先レコードから Domain Separation を取得しているテーブル。このテーブルには、属性列に *domain_master=ref-field-value* 値が含まれています。

[列名] メニューの [この値で絞り込み] または [除外] の選択肢を使用すると、次の 2 つのタイプのテーブルを表示できます。

ドメイン上書きビューアー

ドメイン上書きビューアーを使用すると、インスタンス全体ですべてのプロセス上書きを一度に表示および管理できます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

概要

スクリプト内でオーバーライドの詳細検索を行う代わりに、ドメイン上書きビューアーを使用してオーバーライドをすばやく検索することができます。[すべて] フィルターに「ドメイン」と入力し、左側のナビゲーションペインでドメイン上書きビューアーにアクセスします。

ドメイン上書きビューアーのテーブルセレクターには、レコードの上書きを含むテーブルのみのリストと、そのテーブル内の上書きの数が表示されます。テーブルを選択すると、上書きを含むすべての親レコードリストが返されます。すべての親レコード、親レコードのドメイン、および各レコードの上書き数をすばやく表示できます。

[ビューの上書き **(View Overrides)]** を選択すると、親レコードを含むすべての上書きが標準リストビューに表示される新しいタブがロードされます。ドロップダウンリストからテーブルを選択すると、すべてのレコードと上書きが表示されます。レコード固有の上書きをすべて表示するには、レコードの [ビューの上書き **(View Overrides)]** を選択します。

注:
上書きされたテーブルのみがリストされます。

詳細については、「ドメイン分離プロパティの上書きを作成する」を参照してください。

ドメインを有効または無効にする

ドメインをアクティブまたは非アクティブにすると、アクティベーションステータスがドメイン内の会社にカスケードされます。

始める前に
必要なロール：管理者

このタスクについて
会社レコードをアクティブにすると、Domain Separation によって会社の関連ドメインが自動的にアクティブになります。たとえば、ACME 社をアクティブにすると、TOP/ACME ドメインもアクティブになります。

手順

1. ドメインレコードに移動します。
2. [アクティブ] チェックボックスをオフまたはオンにします。
3. [更新] をクリックします。

警告:
ドメインを削除しないでください。不要になったドメインは削除するのではなく非アクティブ化します。

テーブルへのドメインフィールドの追加

管理者は、sys_domain フィールドを追加することで、カスタムテーブルをドメイン分離できます。

始める前に
必要なロール：管理者

このタスクについて
注:

ベースシステムテーブルにドメインを追加しないでください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. テーブルのリストビューに移動します。
   たとえば、 <table name>ナビゲーションフィルターに「.list」と入力します。
2. リストヘッダーを右クリックし、 構成 > リストレイアウト.
3. [新規フィールドの作成] セクションで、[名前] に sys_domain を、[タイプ] にドメイン ID を入力します。
4. [追加] をクリックします。
5. [保存] をクリックします。

> **注:**
>
> フィールドを作成する他の方法では、列名に **u_** プリフィックスが追加されます。ただし、ドメインフィールドを使用すると、**u_** プリフィックスなしでフィールドが自動的に作成されます。次の機能をショートカットとして使用できます。**[sys_domain]**フィールドを作成するときは常に、「**sys_domain**」という名前を付け、フィールドタイプはそのままにします。フィールドタイプは自動的にドメイン **ID** に、フィールドラベルはドメインに設定されるため、数回クリックする手間が省けます。
>
> ベースシステムテーブルにドメインを追加するには、非常に徹底的なテスト、更新、および新しいロジックの追加が必要です。また、多くの場合、顧客はソースコードにアクセスできません。

ドメイン関係を表示する

ドメインマップは、インスタンス上のアクティブなドメインとそれらの相互関係の読み取り専用表現をドメイン管理者に提供します。

始める前に
必要なロール：管理者

このタスクについて
すべてのドメインマップには、プライマリドメインとして設定された 1 つのドメインが必要です。さらに、ドメインマップ内の各ドメインは次の基準を満たす必要があります。

- [親] フィールドを入力する必要があります (プライマリドメインはこれに対する唯一の例外です)。
- [アクティブ] チェックボックスをオンにする必要があります。

ドメインマップは、マッピング基準を満たさないドメインのドメイン関係を描画しません。

手順

1. 移動先 すべて > ドメイン管理 > ドメインマップ.
2. ドメインヘッダーのプラス (**+**) またはマイナス (**-**) アイコンをクリックして、サブドメインを表示または非表示にします。

プライマリドメインの選択

プライマリドメインは、ドメインマップのトップレベルドメインを示します。

始める前に
必要なロール：管理者

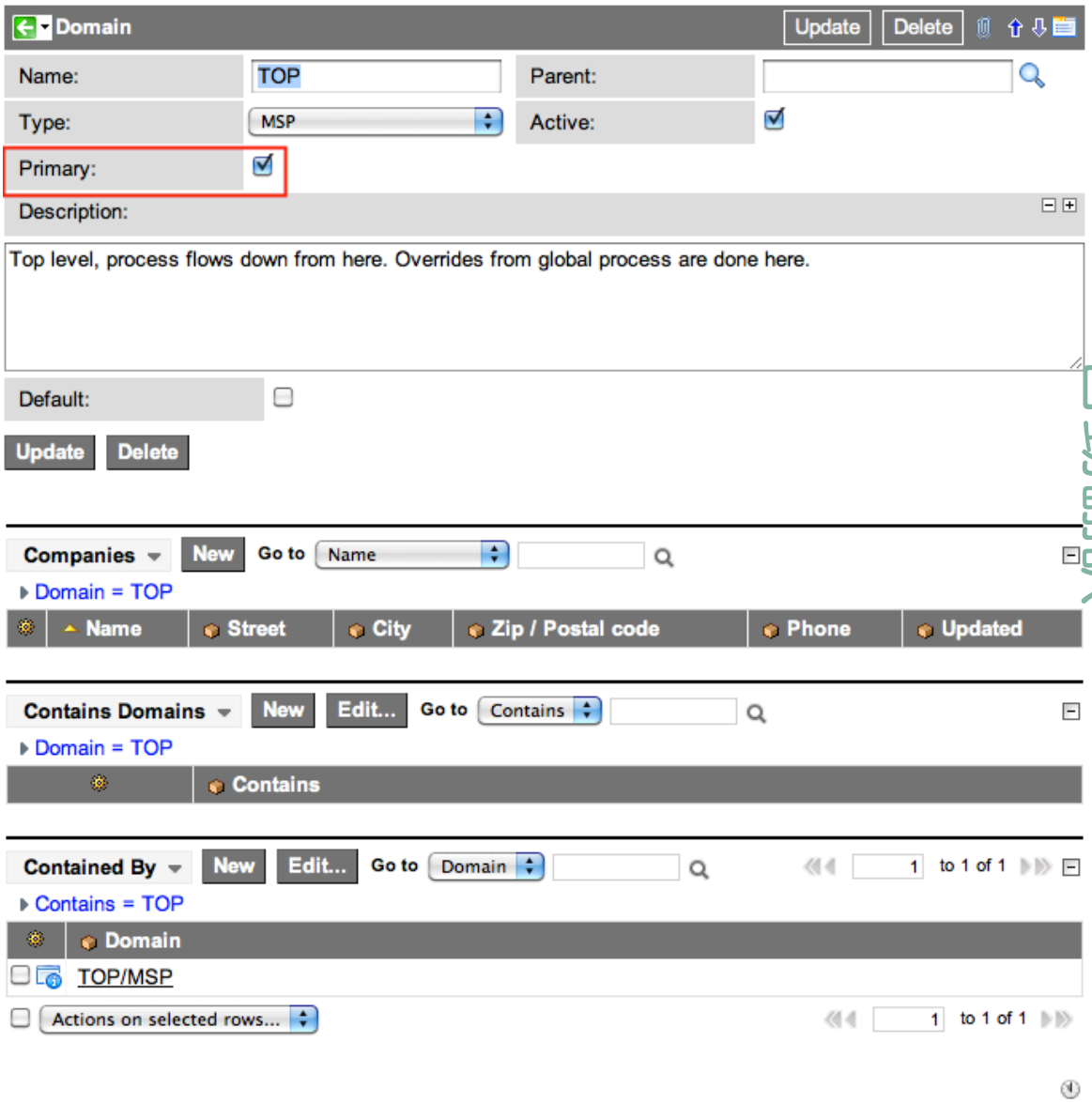
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

このタスクについて
プライマリドメインは親ドメインを持つことができず、少なくとも 1 つの子ドメインを持つ必要があります。一度に存在できるプライマリドメインは 1 つだけです。プライマリドメインとして別のドメインを選択すると、前のプライマリドメインが上書きされます。

手順

1. 移動先 すべて > ドメイン管理 > ドメイン.
2. たとえば TOP など、プライマリドメインにするドメインを選択します。
3. [プライマリ] チェックボックスをオンにします。
4. [更新] をクリックします。



自動翻訳

ドメイン間の包含関係の作成

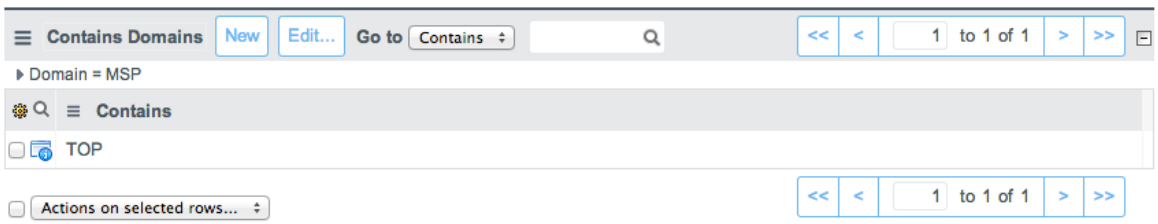
ドメイン間の「包含」関係を作成し、ドメイン階層を変更します。

始める前に
必要なロール：管理者

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

このタスクについて
包含関係のドメインは、包含ドメインの設定を継承します。包含関係ドメインにより、ユーザーは包含ドメイン内のデータとその子を表示できます。プロセスは包含関係の影響を受けません。

手順
1. ドメインテーブルに移動します。
2. 新しい包含関係の親 (コンテナ) ドメインであるドメインレコードを選択します。
3. 必要に応じて、ドメインスコープを切り替えて、セッションスコープとレコードスコープを切り替えます。
4. 包含ドメイン関連リストで [編集] をクリックします。
5. 包含関係の子 (含まれている) ドメインであるドメインレコードを選択します。
   ドメインピッカーが [グローバル] に設定されている場合、デフォルトでは子ドメインのみが表示されます。ドメインスコープを切り替えて、すべてのドメインを表示します。
6. [保存] をクリックしてから、[更新] をクリックします。



関連情報
サービスプロバイダー向けのドメイン分離の推奨プラクティス

ドメインスコープを展開する
デフォルトでは、グローバルドメイン内のユーザーが **sys_overrides** 列を含むテーブルを表示すると、グローバルドメインのレコードのみが表示されます。グローバルドメイン内の管理者がプロセステーブルを表示すると、その管理者にはそのプロセステーブル内のレコードのみが表示されます。

始める前に
必要なロール：管理者

手順
1. *glide.sys.restrict_global_domain_processes* プロパティを **true** に変更します。
2. すべてのドメインのレコードを表示するには、[関連リンク] の [ドメインスコープを展開] をクリックします。
3. グローバルドメインのレコードのみの表示に戻るには、[ドメインスコープを折りたたむ] をクリックします。

可視性ドメインリストにドメインを追加する
可視性ドメインを追加すると、ユーザーまたはグループの通常のドメインメンバーシップに関係なく、ユーザーまたはグループは別のドメインのレコードを表示でき、場合によっては編集できます。

始める前に
必要なロール：管理者

このタスクについて
可視性ドメインを個々のユーザーに付与するよりも、グループのすべてのメンバーに割り当てることをお勧めします。

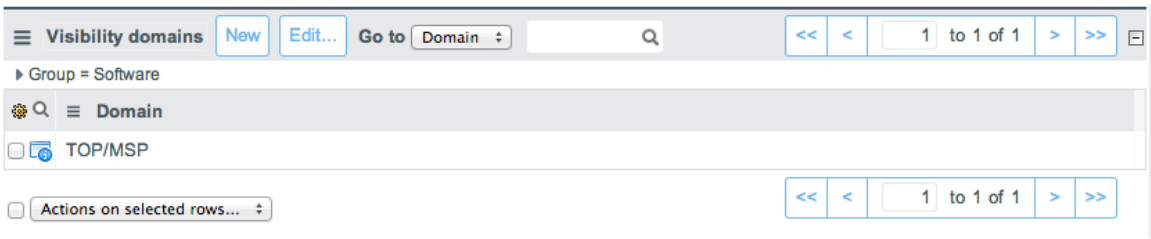
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注:
可視性ドメインを追加しても、テーブルまたはレコードのアクセス制御ルール要件は変更されません。

手順

1. グループテーブルに移動します。
2. 可視性ドメインを提供するグループを選択します。
3. 可視性ドメイン関連リストをフォームに追加します。
4. 可視性ドメイン関連リストで [編集] をクリックします。
5. グループまたはドメインに表示するドメインレコードを選択します。
6. [保存] をクリックしてから、[更新] をクリックします。



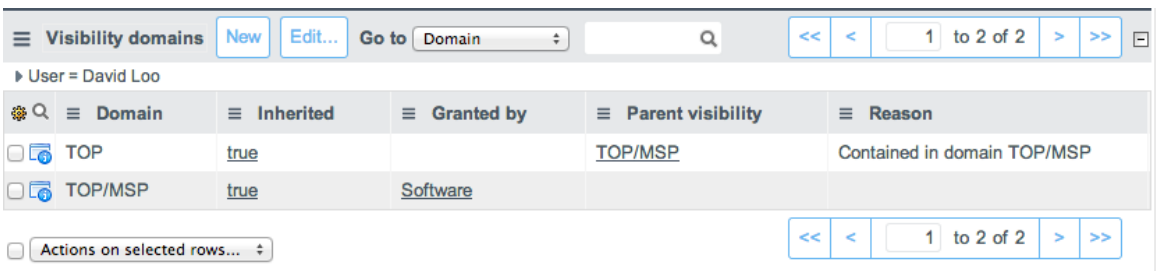
個々のユーザーに可視性ドメインを付与する

ユーザーフォームで特定のユーザーの可視性ドメインを追加することもできますが、グループを介してのみ追加することをお勧めします。そうすることで、個人が部門を変更したり退職したりする場合の権限とアクセス権がコントロールされます。

始める前に
必要なロール：管理者

手順

1. 移動先 すべて > ユーザー管理 > ユーザー.
2. 可視性ドメインを提供するユーザーを選択します。
3. 可視性ドメイン関連リストをフォームに追加します。
4. 可視性ドメイン関連リストで [編集] をクリックします。
5. ユーザーに表示するレコードのドメインを選択します。
6. [保存] をクリックしてから、[更新] をクリックします。



可視性ドメインの埋め込みリストには、次のフィールドが含まれています。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
ドメイン	グループまたはユーザーに表示されるドメイン。
継承	ドメインは、ドメインの可視性または親ドメインから継承されます。
許可者	ドメインの可視性を付与したグループの名前。
親の可視性	親ドメインの名前。レコードのグループ化に使用されます。親レコードが削除されると、同じ親を持つすべてのレコードも削除されます。

ドメイン固有の選択リストを作成する

管理者は、特定のドメインに固有のエントリを含めるように選択リストを構成できます。

始める前に
必要なロール：管理者

手順

1. 選択肢を追加するドメインピッカーからドメインを選択します。
2. カスタマイズする選択肢フィールドを右クリックし、[選択を構成] を選択します。
3. 選択肢を更新または追加します。
4. 更新セットなどの通常の変更プロセスを通じて変更をプッシュします。

> **注:**
> 管理者は、グローバルドメインでの管理上の混乱を防ぐために、ドメイン全体で選択肢が固有になるようにする必要があります。

管理者がグローバルドメインから新しい選択肢を追加すると、階層内の下位のドメインのユーザーには、現在の選択リストの最後に新しい選択肢が表示されます。新しい選択肢がグローバルレベルでアクティブではない場合、ドメインユーザーは [選択を構成] で利用できますが、有効な選択肢としては表示されません。

詳細な **Domain Separation** 管理

管理者は、Domain Separation に関する情報を表示し、潜在的な問題を特定し、構成設定を変更できます。

ドメインでは、次の高度な管理タスクを実行することができます。

- ドメイン選択メニューの使用
- ドメイン関係を表示する

ドメイン選択メニューの使用

インスタンスでは、2 つのメニュー形式でドメインを選択できます。

- ドメインセレクター：利用可能なドメインのシンプルなドロップダウンリストを提供します。
- ドメイン参照ピッカー：フィルタリングとオートコンプリート、先行入力機能を提供する参照フィールドを有効にします。長いリストにはこの形式を使用します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

これらのピッカーの配置と表示または非表示にする手順は、ユーザーインターフェイスのバージョンによって異なります。

コア UI のドメイン選択メニューを有効にする

コア UI でドメインピッカーを表示すると、デフォルトでドメインセレクターが有効になります。ドメインセレクターを有効にした後、システムプロパティを追加してドメイン参照ピッカーを有効にすることができます。

始める前に

> **注:**
> ドメイン参照ピッカーを有効にするには、Domain Separation (plugin com.snc.pa.domain_support) が必要です。

必要なロール：admin

このタスクについて

手順

1. ヘッダーの歯車アイコンをクリックします。
2. [全般] タブで、[ヘッダーにドメインピッカーを表示] スイッチをクリックします。
   ドメインセレクターが コア UI ヘッダーに表示されます。
3. オプション: ドメイン参照ピッカーを有効にします。

   > **注:**
   > ドメイン参照ピッカーを有効にすると、リストからグローバルオプションが削除されます。ホームドメインに戻るには、参照フィールドの横にある戻る矢印をクリックします。管理者ユーザーは、戻る矢印をクリックしてグローバルドメインに戻ることができます。

   a. Application Navigator で「sys_properties.list」と入力します。
   b. まだ存在しない場合は、glide.ui.domain_reference_picker.enabled プロパティを追加し、値を **true** に設定します。
   c. ブラウザを更新します。
   ドメイン参照ピッカーが コア UI ヘッダーに表示されます。

ドメインピッカーへのアクセスを制限する

システムプロパティを使用して、コア UI および Next Experience のドメインピッカーへのアクセスを制限します。

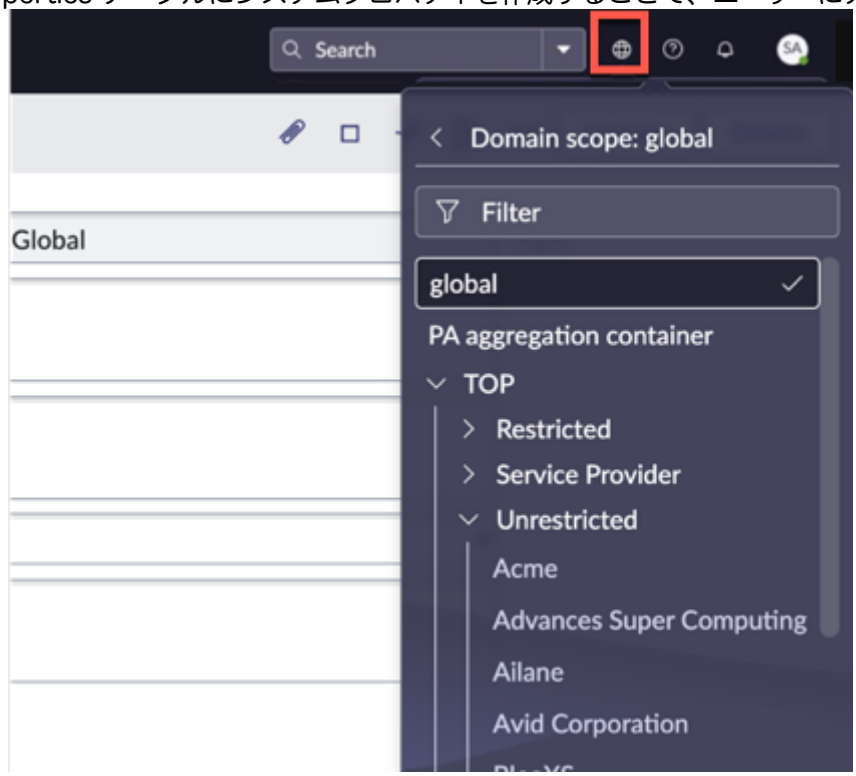
始める前に
必要なロール：admin

このタスクについて
デフォルトでは、ITIL ロールを持つユーザー、および ITIL ロールを含むロール (管理者など) は、Next Experience のドメインピッカーにアクセスできます。他のロールをプロパティに追加してアクセス権を付与するか、ロールを削除して制限することができます。ロールを管理者のみに制限することをお勧めします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

管理者は、sys_properties テーブルにシステムプロパティを作成することで、ユーザーにアクセス権を付与できます。



手順

1. システムプロパティ [sys_properties] テーブルを開きます。
2. glide.ui.polaris.domain_picker.role プロパティを追加します。
3. プロパティ値をロールのカンマ区切りリスト (admin、 **itil**) として設定します。
   詳細については、「Next Experience ピッカーを構成する」を参照してください。

Domain Separation アプリケーションプロパティ

Domain Separation プラグインには 2 つの新しいテーブルがあり、サービスプロバイダーは Domain Separation を使用するアプリケーションをより柔軟にカスタマイズできます。これらのテーブルは、システムアプリケーションプロパティテーブル [sys_application_property] とシステムアプリケーションプロパティ値テーブル [sys_application_property_value] です。

より多くのオプションを提供する新しいテーブル

サービスプロバイダー (SP) アプリケーションでは、ドメインによって特定のアクションが異なる場合があります。ただし、ServiceNow ベースシステムのシステムプロパティ [sys_properties] テーブルはドメイン分離されていないため、Domain Separation を使用するアプリケーションの要件を満たしていません。

各 SP 顧客は、別の方法でのアプリケーションのカスタマイズを望む場合があります。以前は、カスタマイズ可能な機能は 1 つのグローバル値としてのみ定義されていました。アプリケーション開発者は、より柔軟なテーブルが必要です。機能を追加または変更するたびにコードを作成することなく、アプリケーションを変更できるようになりました。

新しいテーブルでの上書き方法

開発者は通常、ServiceNow システムプロパティ [sys_properties] テーブルを使用して、アプリケーションでさまざまな機能を作成します。異なるドメインで異なる動作をするアプリケーションを開発する場合は、自分でカスタマイズする必要があります。

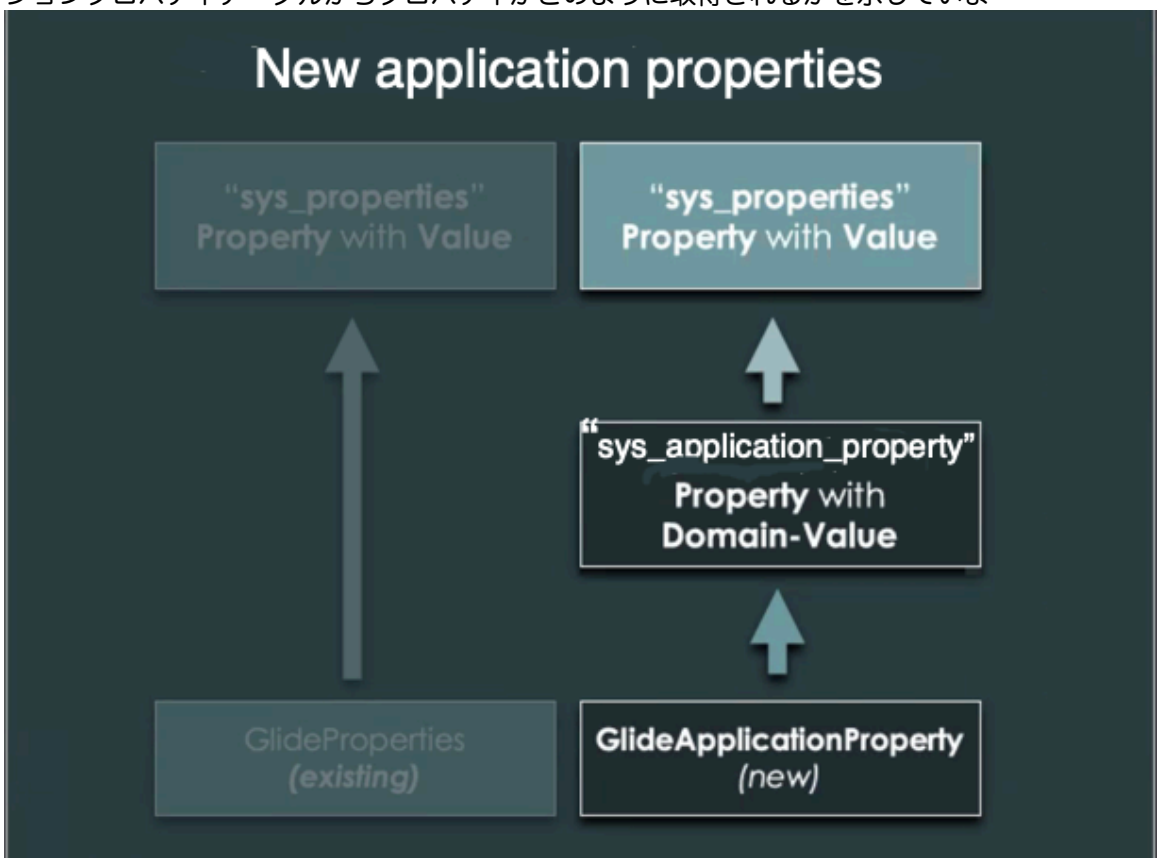
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Paris リリースでは、新しいアプリケーションプロパティ [sys_application_property] テーブルを使用するとそのカスタマイズが簡素化できます。システムプロパティテーブルの値に直接移動する代わりに、アプリケーションプロパティテーブルが最初にシステムアプリケーションテーブルに移動します。この新しいテーブルには、アプリケーションの設定に必要なロジックが格納されています。新しいテーブルでプロパティが見つかると、そのコンテンツが使用されます。そのテーブルに情報がない場合は、ベースシステムプロパティテーブルに移動します。

Domain Separation のサポートを構成すると、この新しいアプリケーションプロパティテーブルにドメインロジックを追加できます。このテーブルには、システムプロパティテーブルに存在しないプロパティを含めることができます。または、システムプロパティテーブルで選択したプロパティを上書きできるプロパティを構成テーブルに追加することもできます。

たとえば、最初の曜日機能を使用してアプリケーションを構成するとします。週の最初の日を日曜日にしたい場合もあれば、別のケースでは、週の最初の日を月曜日にしたい場合もあります。ベースシステムテーブルには、1 日目のオプションが 1 つしかない (日曜日) 場合があります。新しいテーブルを使用して、別のプロパティで 1 日目を日曜日とし、子ドメインでは月曜日として格納することができます。

この図は、システムプロパティ [sys_properties] テーブルに移動する前に、アプリケーションプロパティテーブルからプロパティがどのように取得されるかを示しています。



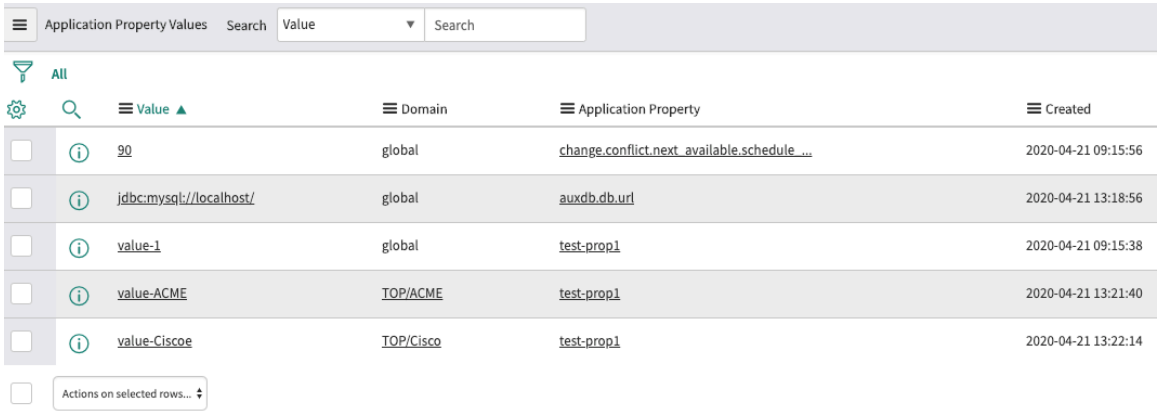
新しいテーブルでのスコープ対象アプリの動作

新しいアプリケーションプロパティテーブルは、スコープ対象のアプリケーションからサポートされています。アプリケーションプロパティ名は、システムプロパティ名と同様に一意です。つまり、グローバルでない場合は、スコープ名がプリフィックスとして付きます。アプリケーションのスコープは構成に影響します。スコープによって、1 日目が日曜日と月曜日のどちらに定義されるかが決まります。同じプロパティを使用できますが、親ドメインでは 1 日目が日曜日、子ドメインでは 1 日目が月曜日になるようにカスタマイズできます。新しいテーブルにはドメイン列とスコープ列の両方があるため、それぞれに対してこれらのプロパティを設定できます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

次の画像に示すように、sys_application_property_value テーブルの [ドメインスコープを展開] ビューを使用して、すべての上書きを表示できます。



注:

これらのテーブルを利用できない場合は、ドメイン拡張インストーラー (com.glide.domain.msp_extensions.installer) プラグインが有効になっていることを確認してください。

新しいアプリケーションプロパティテーブル

新しいシステムアプリケーションプロパティ [sys_application_property] テーブルには、次のフィールドが含まれています。

- name
- 説明
- タイプ (文字列、true | false、整数、タイムゾーン、色など)
- default_value
- プロパティ (sys_properties への参照)
- usage_notes
- read_roles
- write_roles
- 一意のキー：(名前)

新しいシステムアプリケーションプロパティ値 [sys_application_property_value] テーブルには、次のフィールドが含まれています。

- sys_application_property (sys_application_property への参照)
- sys_domain
- sys_overrides
- value
- 一意のキー：(sys_application_property、sys_domain)

新しい API

新しい API はスコープ対象アプリでもサポートされています。ドメイン分離されたアプリケーションプロパティには個別の API があります。GlideApplicationProperty API には、グローバルアプリケーションとスコープ対象のアプリケーションの両方でスクリプト可能な 2 つの新しいメソッドが

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

あります。これらの新しい API の詳細については、「GlideApplicationProperty - スコープ指定、グローバル」を参照してください。

関連情報

サービスプロバイダー向けのドメイン分離の推奨プラクティス

ドメイン移行ツール

ドメイン移行ツールを使用して、ドメイン分離された環境から独自の専用インスタンスに顧客を移動させます。

ドメイン移行ツールプラグイン

ドメイン移行ツールプラグイン (com.glide.domain.migration_tool) により、ドメイン分離された環境からより柔軟な専用インスタンスに顧客が移動するタスクを簡素化することができます。Now Platform の機能を最大限に活用するために、顧客は別のインスタンスに移行することもできます。Domain Separation プラグインがインストールされていても、データとプロセスの分離プロパティはオフになっています。

注:
使用するには、クローンされたインスタンスを要求し、ドメイン移行ツールプラグインのアクティベーションを要求する必要があります。

ドメイン移行ツールは、ドメイン分離されたインスタンスでデータとプロセスの両方の分離が有効になっている場合にのみ実行されます。

- *glide.sys.domain.partitioning* データプロパティは **true** に設定する必要があります。
- *glide.sys.domain.delegated_administration* プロセスプロパティは **true** に設定する必要があります。

移行ツールの機能

- 移行プロセスの多く、特にデータのクリーンアップを自動化します。
- ドメイン分離されたインスタンスを新しい専用インスタンスに移行します。
- 専用インスタンスからデータを削除します。

  注:
  このツールは、グローバル、ターゲットドメイン、または追加のデータドメイン (指定されている場合) のデータを削除しません。

- プロセスデータを折りたたむか、折りたたむことができない場合はプロセスデータを削除します。
- ターゲットドメインに表示されるプロセスレコードを保持します。
- sys_choice、sys_ui_list、および sys_ui_related_list 特殊テーブルを更新します。
- Domain Separation プラグインによって追加されたレコードをクリーンアップします。
  - ビジネスルール
  - UI アクション
  - ジョブスケジュール
  - インストレーションイグジット
  - ナビゲーションモジュール
- Domain Separation を無効にし、クローンされたインスタンスからドメインを削除します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- クローンされたインスタンスで次のプロパティを **false** に設定します。
  - *glide.sys.domain.partitioning*
  - *glide.sys.domain.delegated_administration*
  - *glide.sys.domain.enabled*
- ターゲットドメインと指定された追加のデータドメインを除くすべてのドメインを削除します。

- domain_migration_tool_status テーブルの [ステータス] フィールドを更新します。

テーブルの個々のステータス

ステータス	説明
処理待ち	移行中のドメイン分離テーブルのデフォルトのステータステーブルは移行される予定ですが、まだ移行が開始されていません。
失敗	テーブルレベルのエラー。移行プロセスがエラーで終了した場合、このステータスはどのテーブルにエラーがあるかを示します。
実行中	現在移行中のテーブルのステータス。1 つのテーブルのみがこのステータスになり、現在移行中です。
成功	正常に移行されたテーブルのステータス。
正常に完了しました	移行プロセスはエラーなしで終了しました。
エラーで終了	移行プロセスはエラーで終了しました。

- 進捗状況とステータスを syslog_domain に記録します。

  移行に関連するすべてのログエントリのソースは **MigrationTool** です。

  - 各データテーブルと残りのデータテーブルをログに記録します。
  - 各プロセステーブルと、現在非アクティブ化または削除されているドメインのレコードをログに記録します。

移行ツールに含まれない機能

- インスタンスをクローンします。
- 別のドメイン分離インスタンスを作成します。
- ツールを実行する前にデータまたはプロセス分離プロパティが無効になっている場合は、レコード (データまたはプロセス) を移行します。
- ソースインスタンスのデータを変更します。
- グローバル、ターゲットドメイン、または追加のデータドメイン (指定されている場合) のデータを削除します。

ツールの実行後に行う必要があること

ドメイン移行ツールは、目的のドメイン (ターゲットドメイン、追加のデータドメイン、およびグローバルドメイン) 以外のデータの削除を自動化します。残りの構成をすべて評価して、それらが適切であり、専用のインスタンスに対して機能することを確認する必要があります。たとえば、レコードのドメインフィールドを設定するビジネスルールがある場合、このビジネスルールは役に立たないため、無効にすることができます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ドメイン分離されたインスタンスを専用インスタンスに移行する

ドメイン分離された環境から独自の専用インスタンス環境に顧客を移動します。

始める前に

必要なロール：security_admin および admin

手順

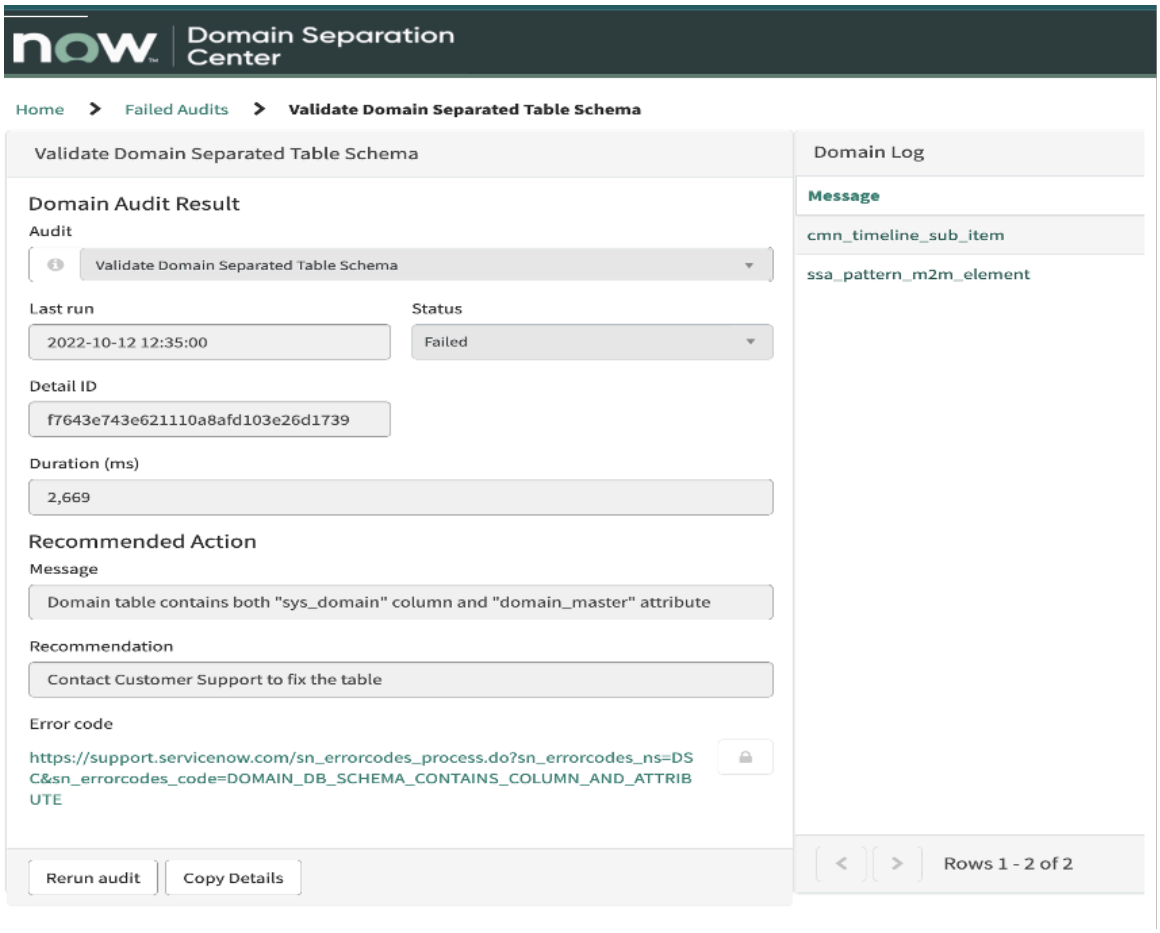
1. security_admin ロールに昇格させます。
   詳細については、「特権ロールへの昇格」を参照してください。
2. 移動先 すべて > ドメイン管理 > ドメイン移行ツール.
   domain_migration_tool_status.list にもアクセスします。
3. [新規] をクリックします。
4. フォームに入力します。

フィールド	説明
ターゲットドメイン	移行するプロセスとデータの両方に使用するドメインを指定します。[追加データドメイン] フィールドで指定されている場合を除き、子ではなくターゲットドメインのみが保持されます。
追加のデータドメイン	必要に応じて、移行する追加のデータドメインを指定します。ターゲットドメインとそのすべての子を移行する場合は、すべての子を指定する必要があります。

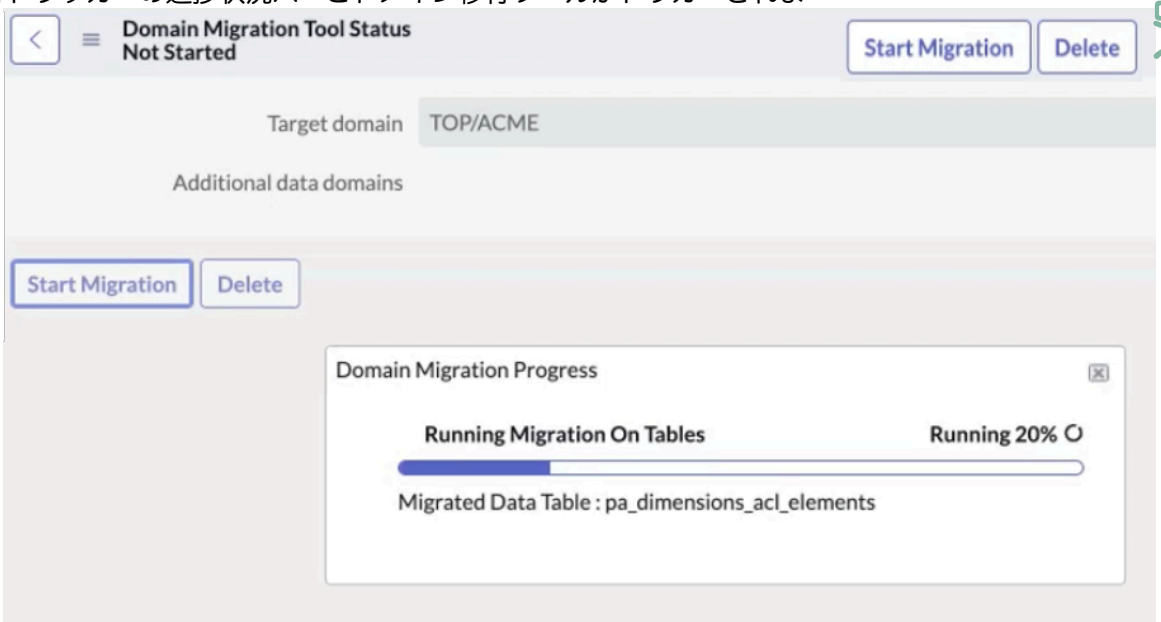
5. [送信] を選択します。
6. 送信したフォームを開きます。
7. 移動先 すべて > ドメイン分離センター > 監査の設定 .
   詳細については、「Domain Separation センター」を参照してください。
8. [ドメイン分離テーブルのスキーマの検証 **(Validate Domain Separated Table Schema)]** 監査を [アクティブ] に設定し、スケジュールをアサインします。
   これは、ドメイン分離されたテーブルの健全性について事前にチェックするための予防的なドメイン監査です。これにより、移行を実行する前にエラーを修正できます。
9. スキーマを含む監査スケジュールを実行します。
   詳細については、「直ちに監査を実行する」を参照してください。
10. 監査から返された問題に対処します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



11. [移行開始] を選択します。
    - 実行トラッカーの進捗状況バーとドメイン移行ツールがトリガーされます。



    - 現在進行中のテーブルが、正常に移行されたテーブルの割合の合計とともに表示されます。
    - すべてのドメイン分離テーブルが、移行ステータス、各テーブルの合計レコード数、および移行されたレコードの数とともに記録されるテーブル。
    - 移行に失敗したテーブルの数も記録されます。
    - [ステータス] は、ツールがその機能を実行するときに更新されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- 進捗状況バーを閉じても、ドメインの移行はバックグラウンドで実行されています。`sys_execution_tracker` テーブルにアクセスし、[テーブルで実行中の移行 **(Running Migration on Tables)**] を探して、バックグラウンドで実行されている移行プロセスを確認します。

ドメイン移行ツールのステータスには、次のフィールドが表示されます。

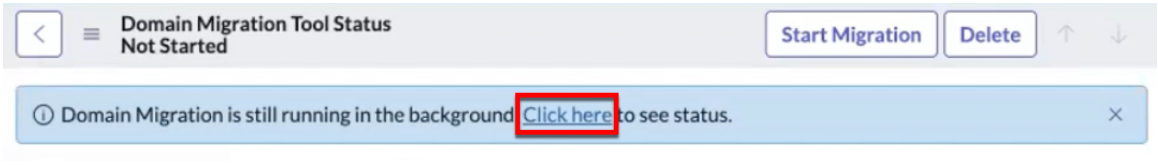
ドメイン移行ツールのステータスフィールド

フィールド	説明
ステータス	移行ステータスを表示します。 ○ データテーブルを移行しています...**(Migrating data tables...)**：進行中のステータス。 ○ 移行に成功しました **(Migration successful)**：移行が成功した後の更新されたステータス。 ○ ドメイン分離されたテーブルの **1** つで不適切な構成が観測されました **(Misconfiguration is observed on one of the domain separated tables)**：データ移行の失敗を示します。スキーマエラーが検出されました。移行は開始されません。[ドメイン分離テーブルのスキーマの検証 **(Validate Domain Separated Table Schema)**] 監査を実行します。監査は失敗し、スキーマ標準に従っていないテーブルが表示されます。 ○ テーブルの再アクセスでエラーが発生して終了しました **(Finished with Errors in Revisit Tables)**：スキーマの移行に対処するためにテーブルの数が表示されます。[再アクセステーブル数] でエラーを特定し、スキーマの問題に対処します。 ○ テーブルのドメイン移行に失敗しました...**(Domain Migration Failed for Tables...)**：失敗したテーブルからターゲット以外のレコードを手動で削除する必要があります。 ○ 正常に完了しました：すべてのテーブルが移行されました。
ターゲットドメイン	移行のために選択されたターゲットドメイン。
追加のデータドメイン	複数の移行ドメインが選択されている場合に入力します。
再アクセステーブル数	このフィールドは、テーブルの移行に失敗した場合にのみ入力されます。エラーがない場合、この数はゼロです。この場合、テーブルに再アクセスして移行を再試行します。エラーがない場合は、テーブルに再アクセスしたり、移行を再試行したりする必要はありません。
現在の進捗中のテーブル	現在移行中のテーブルの名前を表示します。移行が成功すると、このフィールドは空になります。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

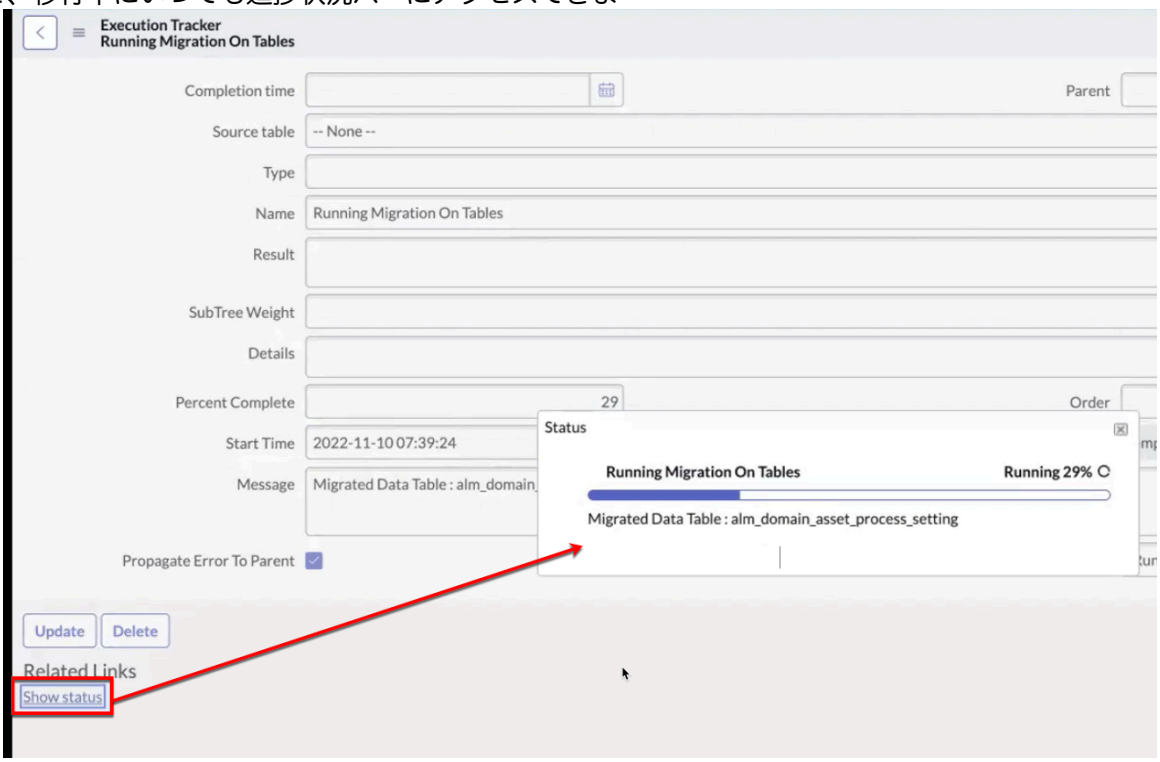
12. [ドメイン移行ツールのステータス] ページで [ここをクリック] リンクを選択して、実行トラッカーを開きま



す。

`sys_execution_tracker` テーブルにアクセスし、[テーブルで実行中の移行 **(Running Migration on Tables)]** を探して、バックグラウンドで実行されている移行プロセスを確認することもできます。

13. [関連リンク] セクションの [ステータスを表示] を選択すると、移行中にいつでも進捗状況バーにアクセスできま



す。

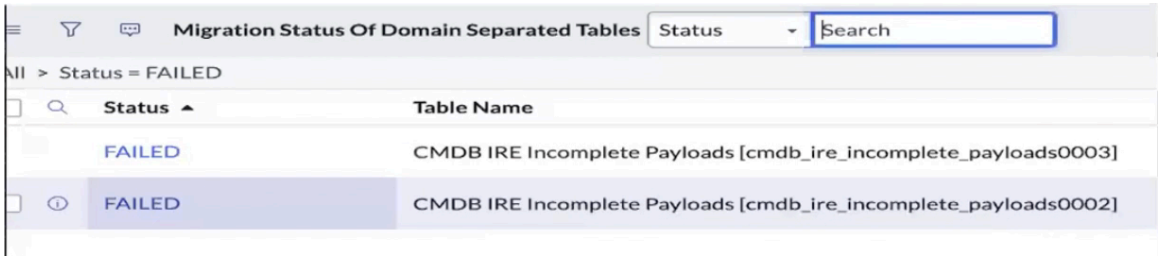
テーブルがスキーマチェックに失敗した場合、ドメイン分離テーブルの全体的な移行ステータスは [失敗] になりま

す。

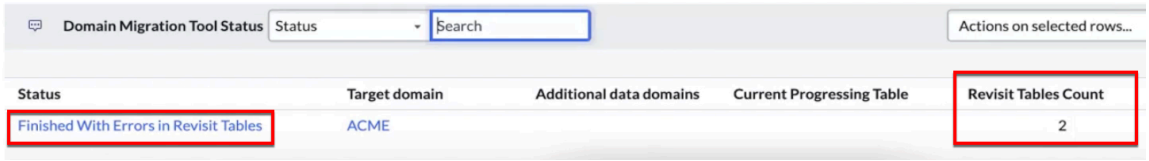
対応するテーブルごとに失敗したエントリがあります。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

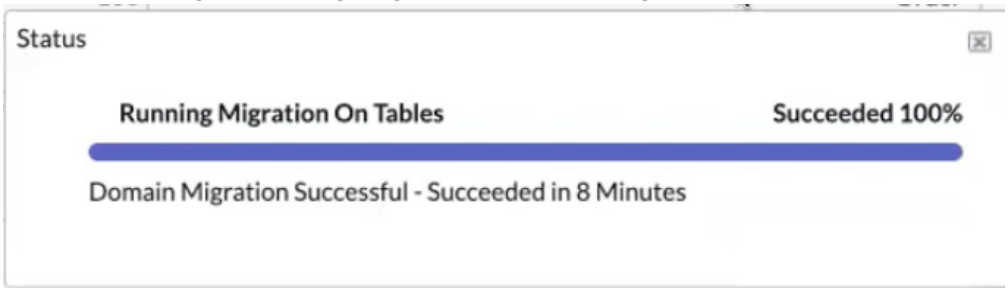
自動翻訳



移行の残りの部分は続行され、失敗したすべてのテーブルのサマリーと再アクセステーブル数の合計数が、ドメイン移行ツールのステータスに入力されます。



移行が完了すると、[ステータス] は [正常に完了しました] になります。



プロセス管理

プロセス管理では、管理者はドメイン固有のポリシーを設定できます。

ドメイン階層の上位に設定されたポリシーは、ドメイン階層の下位に設定されたポリシーで上書きされます。管理者は、ドメイン内で次のグローバルポリシーと設定のドメイン固有のバージョンを設定できます。

- クライアントスクリプト
- システムポリシー
- アプリケーション名とモジュール名
- アプリケーションロール
- モジュールフィルター

> **警告:**
> 管理者は ACL ルールをオーバーライドしてすべてのロールチェックに合格できるため、admin ロールを持つすべてのユーザーは、すべてのシステム機能およびデータへの特別なアクセス権を持ちます。この権限は慎重に付与してください。

ユーザーが **admin** ロールを持っている場合、割り当てられたドメインに関係なく、インスタンス内のすべてのポリシーを使用できます。特定のドメインに入ることができ、そのドメインとその上位ドメインのポリシーのみが、関連するトランザクション中に表示および処理されます。管理者が上位のドメインまたはグローバルドメインにあるポリシーを変更すると、その管理者の現在のドメインの新しいレコードが自動的に作成されます。元のポリシー、アプリケーション、またはモジュールレコードは変更されません。元のレコードはこの新しいレコードで上書きされます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

下位レベルのドメインでポリシーを変更するには、そのドメインに移動してポリシーを変更します。このアプローチでは、元の上位レベルのポリシーレコードを上書きするポリシーレコードがドメインに作成されます。

上位レベルのポリシーを変更した後にそのポリシーの [ドメイン] フィールドを変更しないでください。このアプローチでは、下位レベルのドメインにポリシーレコードは作成されず、上位レベルのドメインのポリシーレコードは保持されません。

[sys_overrides] フィールドは、上位レベルのレコードが階層内の下位レベルのポリシー、アプリケーション、またはモジュールで上書きされることを示します。管理者が階層の上位の別のドメインに属するポリシー、アプリケーション、またはモジュールを変更しようとすると、このフィールドが自動的に設定されます。

更新の試行は、上位レベルのレコードの変更ではなく挿入に変わり、**[sys_overrides]** フィールドは上書きされる上位レベルのポリシー、アプリケーション、またはモジュールを示すように設定されます。後で関連するトランザクションのレコードがロードされると、元のものの代わりに、上書きするドメイン固有のポリシー、アプリケーション、またはモジュールが使用されます。

プロセス管理のドメイン

デフォルトでは、プロセス管理は常にレコードのドメインを使用して、適用するポリシーを決定します。

レコードのドメインがユーザーのドメインよりも優先されます。レコードのドメインにポリシーがない場合、委任管理はドメイン階層の次に高いレベルのポリシーをチェックします。ドメインポリシーの検索は、グローバルドメインに到達するまでドメイン階層の上方向に続行します。ドメイン階層の下位にドメインポリシーがない場合、プロセス管理はグローバルドメインのポリシーを使用します。

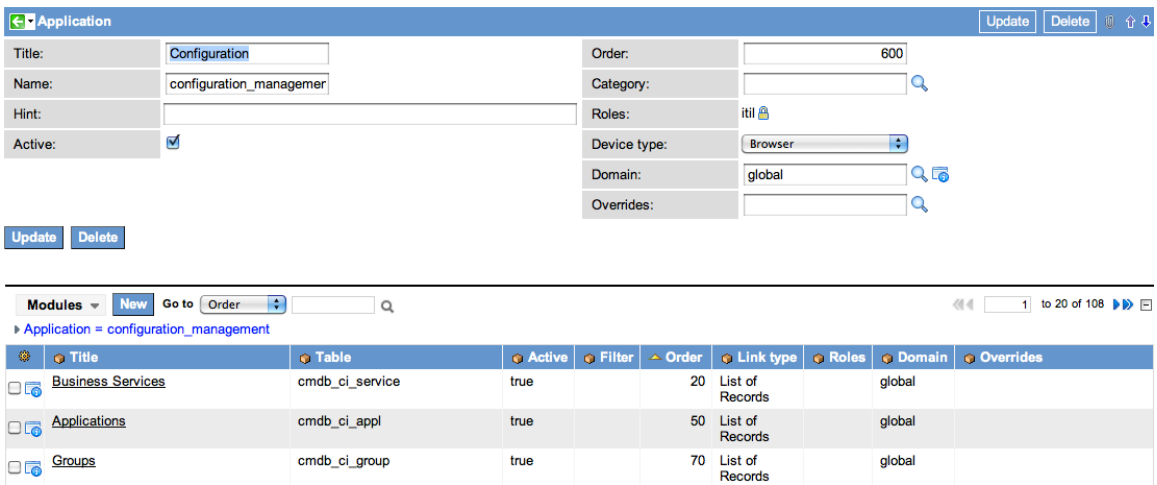
たとえば、Fred Luddy は Acme: Atlanta、Acme: San Diego、Acme: NY の子ドメインのレコードを表示できる Acme ドメインのユーザーであるとします。このユーザーが Acme: San Diego ドメイン内のレコードを開くと、プロセス管理では最初に Acme: San Diego ドメイン内のポリシーがチェックされます。ドメイン階層のこのレベルにポリシーがない場合、プロセス管理は Acme ドメインのポリシーをチェックします。Acme ドメインにポリシーがない場合、ドメイン階層の上位に他のドメインがないため、プロセス管理はグローバルドメインのポリシーを使用します。

ドメイン固有のアプリケーションを使用したプロセス管理の例

次の例は、ドメイン固有のアプリケーションとモジュールを使用したプロセス管理を示しています。

David Loo は、Oceanic ドメインの管理者として、構成アプリケーションをカスタマイズすることにしました。まず、David は構成アプリケーションモジュールで利用可能なモジュールを確認します。

構成アプリケーションの開始ビュー



© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

David は、構成アプリケーションの名前を CMDB に変更し、inventory_admin ロールがアプリケーションを表示できるようにすることにしました。

構成アプリケーションに対するドメイン固有の変更の例

Applications | New | Go to Title | 1 to 20 of 46

All > Active = true > Device type != Mobile

Title	Active	Order	Roles	Name	Domain	Overrides
Asset Management	true	900	asset	asset	global	
BSM Map	true		admin itil	bsm_map	global	
Change	true	400	itil	change_management	global	
CMDB	true	600	itil inventory_admin	configuration_management	Database	configuration_management
Content Management	true		content_admin	cms	global	
Contract Management	true	1,000	asset contract_manager	asset_contracts	global	
Domain Admin	true		domain_admin	domain_admin	global	
ECC	true		admin	ecc	global	
Homepage Admin	true		admin	home	global	
Incident	true	200	itil	incident_management	global	
Instance Clone	true		clone_admin	instance_clone	global	
Knowledge Base	true	800	knowledge	km	global	
Metrics	true		itil_admin metric_admin	metrics	global	
MID Server	true		admin	MID	global	
Organization Management	true	875	asset	organization_management	global	
Problem	true	300	itil	problem_management	global	
Reports	true	1,100	itil	reports	global	
SAML 2 Single Sign-on	true		admin	saml_2_single_sign_on	global	
SAML Single Sign-on	true		admin	SAML Single Sign-on	global	

Activate | Deactivate | Actions on selected rows... | 1 to 20 of 46

次に、David は、開く - 「新規」ステータスモジュールを有効にして、Oceanic カテゴリのオープンインシデントを表示するように新しいフィルターアイテムを追加して、インシデントアプリケーションを変更することにしました。

オープン - 「新規」ステータスモジュールへのドメイン固有の変更の例

Module | = Required field | Update | Delete

Title:	Open - in "New" state	Link type:	List of Records
Table:	Incident [incident]	View name:	
Order:	200	Roles:	
Application:	incident_management		
Hint:			
Active:	☑		
Image:			

Filter:

	Incident state	is	New
and	Active	is	true
and	Category	is	Database

Arguments:

```
incident_state=1^active=true
```

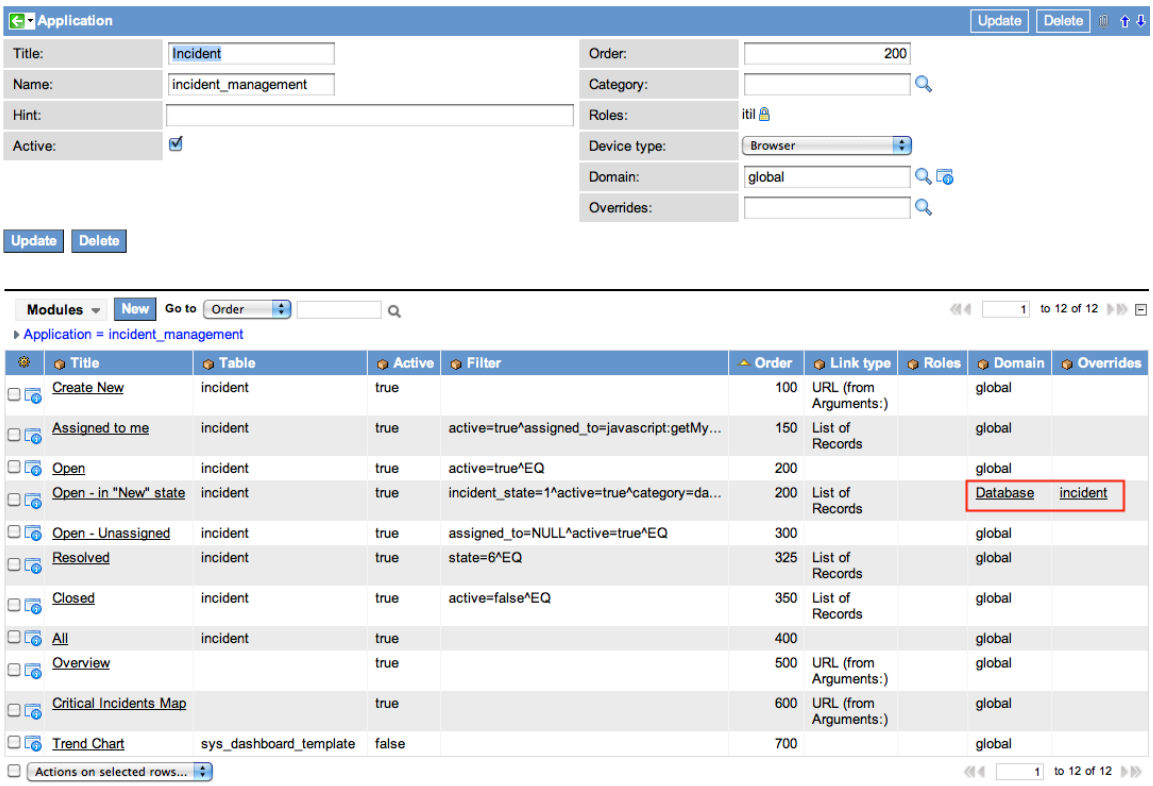
Update | Delete

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

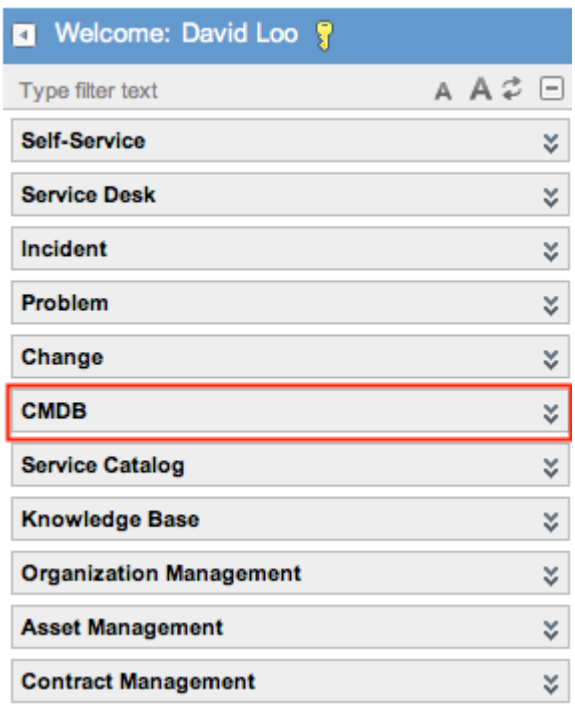
これにより、グローバルドメインの既存のモジュールを上書きするのではなく、アプリケーションに新しいモジュールエントリが作成されます。

インシデントアプリケーションのドメイン固有のビュー



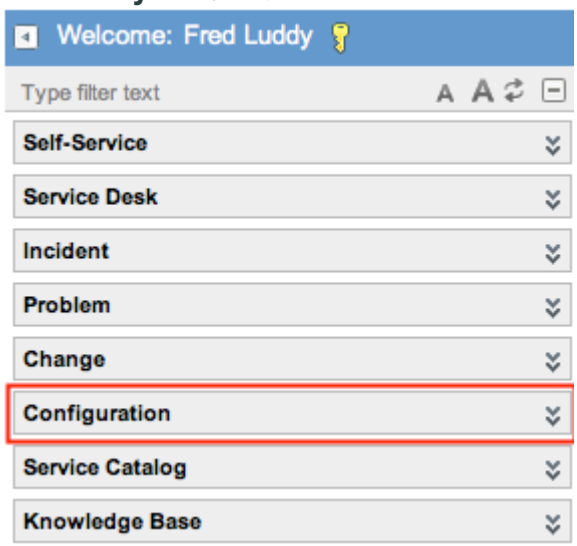
Fred Luddy など、別のドメインの別の管理者がログインして構成アプリケーションを確認すると、グローバルドメインの設定が表示されます。

David Loo のアプリケーションビュー



© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Fred Luddy のアプリケーションビュー



詳細なドメインログ記録とデバッグメッセージを有効にする

ドメインログとデバッグメッセージを使用して、ドメイン構成エラーのトラブルシューティングを行うことができます。

始める前に

必要なロール：管理者
最高のパフォーマンスを得るには、最新のインスタンスを使用してください。

手順

1. Domain Separation センターで、[ドメイン管理] に移動します。
2. [ドメインセンターの構成] をクリックします。
3. [詳細なドメインログ記録を有効にする] で、[はい] チェックボックスをオンにします。
4. [更新] をクリックします。

リアルタイムにドメインメッセージを表示する

システムログからリアルタイムにドメインメッセージを表示できます。

始める前に

必要なロール：管理者

手順

1. 詳細なドメインログ記録を有効にする:次の場所に移動します。 すべて > ドメイン管理 > ドメイン分離センター > ドメインセンターの構成 > 詳細ドメインログ記録を有効にします > はい (またはプロパティ glide.sys.domain.verbose を **True** に設定します)。
2. 移動先 システム診断 > セッションのデバッグ > すべて有効化.
   これはリアルタイムのレビューであるため、ログファイルをチェックする前にデバッグセッションを実行する必要はありません。
3. セッションデバッグコンソールに移動して、詳細なシステムドメインログを表示します。
4. 「 テーブルに対してクエリーを実行する (Query against table)」というテキストを検索します。

   このクエリーは、次の形式のログメッセージを検索します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

```
08:36:43.974: [Domain Paths] Query against table incident restricted by domain values
 [Database Atlanta[db53580b0a0a0a6501aa37c294a2ba6b],
Database[287ee6fea9fe198100ada7950d0b1b73],
Database San Diego[db53a9290a0a0a650091abebccf833c6], global, NY
 DB[5f74727dc0a8010e01efe33a251993f9]]
```

この例では、インシデントテーブルを表示しているユーザーは、Database Atlanta、Database、Database San Diego、グローバル、および NY DB の各ドメインに一致するレコードのみを表示しています。

履歴ドメインメッセージの表示

ログファイル内の履歴ドメインメッセージを表示して、Domain Separation の問題をトラブルシューティングします。

始める前に
必要なロール：管理者

手順

1. 詳細なドメインログ記録を有効にする:次の場所に移動します。 すべて > ドメイン管理 > ドメイン分離センター > ドメインセンターの構成 > 詳細ドメインログ記録を有効にします > はい (またはプロパティ glide.sys.domain.verbose を **True** に設定します)。
2. 移動先 システム診断 > セッションのデバッグ > すべて有効化.
3. ログファイルをチェックする前に、1 日などの期間デバッグセッションを実行します。
4. 移動先 システムログ > ユーティリティ > ノードログファイルのダウンロード.
5. 表示する日のレコードを開きます。
   ログファイルでは、localhost_log.<yyyy-mm-dd>.txt という命名形式が使用されます。
6. ダウンロードログ関連リンクをクリックします。
7. ダウンロードしたログファイルをテキストエディターで開き、次の形式のログメッセージを検索します。

   ドメイン値によって制限されたテーブルインシデントに対するクエリー [global, Software[8a4dde73c6112278017a6a4baf547aa7]]

   この例では、グローバルドメインとソフトウェアドメインに一致するインシデントテーブルのレコードのみが表示されます。

Domain Separation エラーのトラブルシューティング

Domain Separation の問題が発生した場合は、このソリューションのリストを確認してください。

エラーまたは症状	解決策
ドメインの sys_id が存在しないドメインを指している	このエラーは、ユーザーレコードやタスクレコードなどのデータレコードに、現在のドメインテーブルに sys_id が存在しない sys_domain 列値がある場合に発生します。ドメインの sys_id が誤って削除されたか、ドメインテーブルを変更した場合は以前のドメインテーブルを参照している可能性があります。 エラーを修正するには、エラーを含むテーブルのリストを開き、無効な sys_domain 値をフィルタリングします。次に、正しい sys_domain 値を手動で入力するか、削除します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

エラーまたは症状	解決策
	注: ドメインテーブルを参照するすべてのテーブルに、無効なドメインの sys_ids を含めることができます。たとえば、無効なドメイン ID がユーザー可視性ドメイン [sys_user_visibility]、グループ可視性ドメイン [sys_user_group_visibility]、および包含ドメイン [domain_contains] テーブルで発生する可能性があります。
ドメインパスまたはドメイン番号 sys_id が間違ったドメインを指している	このエラーは、ドメイン番号またはドメインパスクエリーが実際のドメイン名と同期していない場合に発生します。このエラーは、ドメインを追加する際に番号の付け直しが必要な場合、またはドメイン番号からドメインパスへの変換中にドメイン番号で発生する可能性があります。 エラーを修正するには、Domain Separation センターで結果を確認します。エラーが解決しない場合は、sys_domain_path 列または sys_domain_number 列の値を手動で編集して、適切なドメインを指すようにします。
ドメインツリー構造が破損している	このエラーは、一連のドメインにドメイン間で無限ループが発生する関係が含まれている場合に発生します。 エラーを修正するには、ドメインテーブルのリストを開き、ループを形成しないようにドメインが含まれている値を手動で編集します。

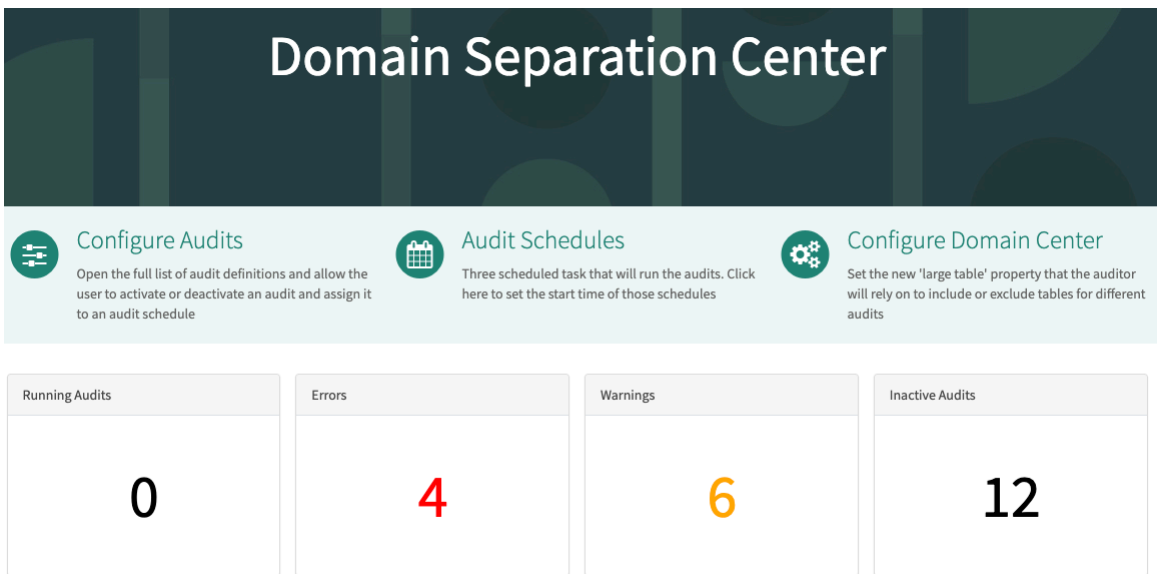
Domain Separation センター

ドメインを定期的に監査して問題を明らかにします。

概要

Domain Separation センター は、domain_audit_definition テーブルに格納されているすべてのドメインの監査をスケジュールおよび設定できるダッシュボードです。このダッシュボードを使用すると、監査結果を確認し、ドメインのエラーと警告をより深く掘り下げることができます。Domain Separation センター のダッシュボードは、<ServiceNow-instance-name>/domaincenter にあります。

Domain Separation センター は多くの監査を提供します。独自の監査を作成することはできません。ただし、実行頻度は設定できます。監査は、domain_audit_definition テーブルに格納されているすべてのドメインで実行されます。



自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

監査を設定する

監査がアクティブかどうかと実行頻度を設定できます。

1. Domain Separation センターで、[監査の設定] をクリックします。

   [監査の設定] ページが表示されます。

2. アクティブにする各監査を設定します。監査はデフォルトで無効にされています。
   a. 監査を選択します。
   b. [アクティブ] ボックスを選択して監査をアクティブにします。
   c. [頻度] フィールドで監査の実行頻度を指定します。

      Domain Separation センターで同じ頻度にマークされているすべての監査を同時に実行します。大きなテーブルで実行する監査に [日次] を選択しないでください。

   d. アクティブにする各監査でこれらの手順を繰り返します。
3. [保存] を選択します。

監査スケジュール

1 つ以上の監査を日次、週次、または月次で実行するように設定します。スケジューラは、これらの監査を実行する日時を指定します。同じスケジュール頻度のすべての監査は、設定した時刻から順番に実行されます。

1. Domain Separation センターで、[監査スケジュール] を選択します。

   [監査スケジュール] ページが表示されます。

2. 監査スケジュールを設定します。
   a. スケジュール名を選択します。
   b. 監査を実行する時刻を指定します。

      時間単位は 24 時間形式です。つまり、14 は午後 2 時です。

   c. 週次スケジュールの場合は、監査を実行する曜日を選択します。1 は日曜日です。
   d. 月次スケジュールの場合は監査を実行する日付になります。
   e. 他のスケジュールについても、この手順を繰り返します。
3. [保存] を選択して設定の変更を保存します。
4. [今すぐ実行] を選択すると、右側のペインの上部に表示される頻度で実行するようにスケジュールされたすべての監査が実行されます。たとえば、ペインのタイトルが「ドメイン監査スケジュール - 日次」の場合、毎日実行されるすべての監査が実行されます。

実行中の監査のステータスを表示するには、Domain Separation センターで [監査の実行] ボックスの番号を選択します。

直ちに監査を実行する

監査は通常、スケジュールどおりに実行されます。ただし、コマンドですべての監査を実行できます。

1. Domain Separation センターで、[監査スケジュール] を選択します。

   [監査スケジュール] ページが表示されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

2. 実行する監査スケジュールの名前 (日次、週次、月次など) を選択します。
3. [今すぐ実行] を選択します。

実行中の監査のステータスを表示するには、Domain Separation センターで [監査の実行] ボックスの番号を選択します。

Domain Separation センター を構成する

1. Domain Separation センターで、[ドメインセンターの構成] を選択します。
2. [ドメインセンターの構成] ページの [詳細なドメインログ記録を有効にする **(Enables detail domain logging)]** で [はい] を選択して、ドメイン関連の問題の診断に役立つ詳細なログを保存します。詳細なログ記録は、パフォーマンスの問題を引き起こす可能性があります。

   これらのログは、syslog_domain テーブルのサーバー側のログを参照します。ログの表示の詳細については、「警告と失敗を含む監査を表示する」を参照してください。
3. スラッシュバケットで、すべての大きなテーブルを選択して [選択済み] 列に移動します。

   日次監査は大きなテーブルでは実行しないでください。[選択済み] 列のグレーアウトされたテーブル名は大きいため、[利用可能] 列に移動できません。
4. [更新] を選択します。

警告と失敗を含む監査を表示する

ダッシュボードの [エラー] および [警告] は、問題が発生した監査に関する詳細情報を提供します。Domain Separation に関連するログは、サーバーの syslog_domain テーブルにあります。

1. Domain Separation センターで、[エラー] または [警告] ボックスの数字を選択します。

   [エラー] または [警告] ページがそれぞれ表示されます。
2. リスト内のいずれかの監査を選択します。

   選択した監査の問題に関する詳細情報がページに表示されます。[監査結果の詳細] のメッセージは、エラーまたは警告を明らかにしたテーブル監査の syslog_domain テーブルの値を参照します。
3. 警告またはエラーの監査に関する情報を提供するサーバーのログを表示するには、次の手順を実行します。
   a. 警告またはエラーの左パネルの [詳細 **ID]** の値をコピーします。
   b. HI のフィルターナビゲーターで「*syslog_domain.do*」と入力します。

      [ドメインログ] ページが表示されます。
   c. [ソース] 検索フィールドに「=<詳細 ID>」 (等号の後にスペースを入れない) を入力します。たとえば、「=f6a00fd29a85b300a9503a81b9169678」と入力します。

      [ドメインログ] ページには、指定した詳細 ID の監査に関連するログのみが表示されます。テーブルの各行には、監査で見つかった問題が明記されます。このページの [メッセージ] フィールドは、ドメインサービスセンターの [メッセージ] 列に表示される値と一致します。メッセージの形式は監査タイプと一致します。
4. 次から選択します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

- [監査を再実行]：監査を再実行して、まだ警告またはエラーが発生するかどうかを確認します。
- [監査の非アクティブ化]：監査を非アクティブにします。
- [詳細をコピー]：監査の詳細をクリップボードにコピーします。

実行中の監査と処理待ちの監査を表示する

アクティブな監査は、スケジュールどおりに定期的に実行されるか、実行キューに格納されます。実行中のステータスを表示できます。

1. [監査の実行] ボックスの数字を選択して、現在実行中または実行処理待ちの監査を表示します。

   [監査の実行] ページが表示されます。

2. 詳細については、監査を選択してください。

非アクティブな監査を表示する

1. [非アクティブな監査] ボックスで数字を選択します。

   [非アクティブな監査] ページには、現在非アクティブ化されているすべての監査が表示されます。

2. いずれかの監査を選択すると、それに関する詳細情報が表示されます。
3. 監査をアクティブにするには、[アクティブ] ボックスを選択し、[頻度] フィールドを使用して監査の実行頻度を指定します。
4. [更新] を選択します。

Domain Separation センター を構成する

ドメイン内のどのテーブルが大きいか、および詳細なログ記録が必要かどうかを指定します。

始める前に
必要なロール：admin

このタスクについて
監査は、日次、週次、または月次ベースで実行するようにスケジュールできます。大きなテーブルで実行される監査には、かなりの時間がかかります。そのため、大きなテーブルで毎日監査を実行しないようにしてください。実行に 1 日以上かかっている新しい監査を開始すると、悪影響を与える可能性があります。

詳細なログ記録により、監査中に見つかった問題についてより詳細な情報を得ることができますが、パフォーマンスの問題が発生する場合があります。

手順

1. Domain Separation センターで、[ドメインセンターの構成] を選択します。
   [ドメインセンターの構成] ページが表示されます。
2. [詳細なドメインログ記録を有効にする **(Enables detail domain logging)]** で [はい] を選択して、ドメイン関連の問題の診断に役立つ詳細なログを保存します。
   これらのログは、ドメインログ [syslog_domain] テーブルのサーバー側のログを参照します。ログの表示の詳細については、「警告と失敗を含む監査を表示する」セクションを参照してください。
3. リストで、すべての大きなテーブルを [選択済み] 列に移動します。
   日次監査は大きなテーブルでは実行しないでください。[選択済み] 列のグレーアウトされたテーブル名は大きいため、[利用可能] 列に移動できません。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

4. [更新] を選択します。
5. 監査する必要がない大きなテーブルがある場合は、*com.glide.domain.audit.big_tables.additional* システムプロパティをそれらのテーブル名のカンマ区切りリストに設定します。

監査の設定

監査がアクティブかどうか、および監査の実行頻度を設定します。

始める前に

必要なロール：管理者

手順

1. Domain Separation センターで、[監査の設定] をクリックします。
   T が表示されます。
2. [監査の設定] ページで、アクティブにする各監査を設定します。
   監査はデフォルトで無効にされています。
   a. [監査] をクリックします。
   b. [アクティブ] チェックボックスをクリックして監査を有効にします。
   c. [頻度] フィールドで監査の実行頻度を指定します。
      Domain Separation センターで同じ頻度にマークされているすべての監査を同時に実行します。大きなテーブルで実行する監査に [日次] を選択しないでください。
   d. アクティブにする各監査で a ～ c の手順を繰り返します。
3. [保存] をクリックします。

監査のスケジュール

監査を実行する日時を指定します。

始める前に

必要なロール：admin

このタスクについて

1 つ以上の監査を日次、週次、または月次で実行するように設定しました。スケジューラは、これらの監査を実行する日時を指定します。同じスケジュール頻度のすべての監査は、設定した時刻から順番に実行されます。

手順

1. Domain Separation センターで、[監査スケジュール] をクリックします。
   [監査スケジュール] ページが表示されます。
2. 監査スケジュールを設定します。
   a. スケジュール名をクリックします。
   b. 監査を実行する時刻を指定します。
      時間単位は 24 時間形式 (14 は午後 2 時) です。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

c. 週次スケジュールの場合は、監査を実行する曜日を選択します。1 は日曜日です。

d. 月次スケジュールの場合は監査を実行する日付になります。

e. 他のスケジュールについても、この手順を繰り返します。

3. [保存] をクリックして設定を保存します。
4. オプション: [今すぐ実行] をクリックすると、右ペインの上部に表示されている頻度で実行するようにスケジュールされたすべての監査が実行されます。
   たとえば、ペインタイトルが「ドメイン監査スケジュール - 日次」の場合、[今すぐ実行] は毎日実行するようにスケジュールされているすべての監査をすぐに実行します。

次のタスク
実行中の監査のステータスを表示するには、Domain Separation センターで [監査の実行] ボックスの番号をクリックします。

直ちに監査を実行する

監査は通常、スケジュールどおりに実行されます。ただし、コマンドですべての監査を実行できます。

始める前に
必要なロール：admin

このタスクについて
個々の監査を手動で実行することはできません。ただし、同じスケジュール頻度で設定されたすべての監査を実行できます。たとえば、毎日実行するように設定されているすべての監査を実行できます。

手順

1. Domain Separation センターで、[監査スケジュール] をクリックします。
2. 実行する監査スケジュールの名前 (日次、週次、月次など) をクリックします。
3. [今すぐ実行する] をクリックします。

次のタスク
実行中の監査のステータスを表示するには、Domain Separation センターで [監査の実行] ボックスの番号をクリックします。

警告と失敗を含む監査を表示する

Domain Separation センター は、監査エラーと警告に関する詳細を提供します。

始める前に
必要なロール：admin

このタスクについて
Domain Separation ダッシュボードの [エラー] および [警告] は、問題が発生した監査に関する詳細情報を提供します。Domain Separation に関連するログは、サーバーの syslog_domain テーブルにあります。エラーは、即時の対応が必要な問題です。警告は失敗につながることはありませんが、ドメイン名を長くしすぎないなどのベストプラクティスを示します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. Domain Separation センターで、[エラー] または [警告] ボックスの数字をクリックします。
   [エラー] または [警告] ページが表示されます。
2. リスト内のいずれかの監査をクリックします。
   選択した監査の問題に関する詳細情報がページに表示されます。[監査結果の詳細] のメッセージは、エラーまたは警告を明らかにしたテーブル監査について、サーバー上の syslog_domain テーブルの値を参照します。
3. 警告またはエラーの監査に関する情報を提供するサーバーのログを表示するには、次の手順を実行します。

   a. 警告またはエラーの左パネルの [詳細 **ID]** の値をコピーします。

   b. Domain Separation センター を実行しているインスタンスで、[フィルターナビゲーター] に「*syslog_domain.list*」と入力します。
   [ドメインログ] ページが表示されます。

   c. [ソース] 列の検索フィールドに、「=<詳細 ID>」 (等号の後にスペースを入れない) を入力します。たとえば、「=f6a00fd29a85b300a9503a81b9169678」と入力します。
   [ドメインログ] ページには、指定した詳細 ID の監査に関連するログのみが表示されます。テーブルの各行には、監査で見つかった問題が明記されます。このページの [メッセージ] フィールドは、ドメインサービスセンターの [メッセージ] 列に表示される値と一致します。メッセージに含まれる情報は監査タイプと一致します。

4. オプション: 次のいずれかを選択します。
   - [監査を再実行]：監査を再実行して、まだ警告またはエラーが発生するかどうかを確認します。
   - [非アクティブ化]：監査を非アクティブにします。
   - [詳細をコピー]：監査の詳細をクリップボードにコピーします。

実行中の結果と処理待ちの結果を表示する

実行中の監査と処理待ちの監査を表示して、そのステータスを確認できます。

始める前に

必要なロール：admin

このタスクについて

アクティブな監査は、スケジュールどおりに定期的に実行されるか、実行キューに格納されます。実行中のステータスを表示できます。

手順

1. [監査の実行] ボックスの数字をクリックして、現在実行中または実行処理待ちの監査を表示します。
   [監査の実行] ページが表示されます。
2. 実行中の監査または処理待ちの監査をクリックすると、それに関する情報が表示されます。

非アクティブな監査を表示する

すべての非アクティブな監査を 1 つの場所で表示し、オプションでそれらをアクティブにすることができます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

始める前に
必要なロール：admin

手順

1. [非アクティブな監査] ボックスの数字をクリックします。
   [非アクティブな監査] ページには、現在非アクティブ化されているすべての監査が表示されます。
2. いずれかの監査をクリックすると、それに関する詳細情報が表示されます。
3. オプション: 監査をアクティブにするには、[アクティブ] ボックスをクリックし、[頻度] フィールドに監査の実行頻度を指定します。
4. [更新] をクリックします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ID

インスタンス内の ID の詳細を確認します。

アクセスアナライザー

アクセスアナライザは ServiceNow® アクセス診断ツールであるアプリ。リソースにアクセスできるユーザーを診断するのに役立ちます。

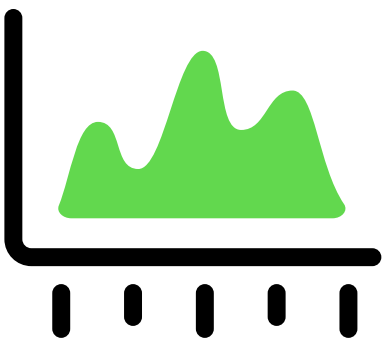
Global Identity

グローバル ID は、ServiceNow® 1 つのインスタンスまたは複数のインスタンス) からインスタンスにアクセスしてユーザー属性を更新できるストアアプリです。

ID センター

ID センターでは ID ベースのリスクとセキュリティギャップを監視および管理し、最小限に抑えることができます。

クロスドメイン ID 管理システム (SCIM)



クロスドメイン ID 管理システム (SCIM) API は、SCIM プロトコルを使用してユーザーとグループの操作を作成、読み取り、更新、および削除するためのエンドポイントを提供します。

ID とアクセスの監査

ID およびアクセスの監査を使用して、ユーザー、グループ、ロール、および ACL に加えられた変更を把握します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

アクセスアナライザー

Access Analyzer は、アクセス診断ツールである ServiceNow® ストアアプリです。リソースにアクセスできるユーザーを判断するのに役立ちます。

Global Identity

Global Identity は、1 つのインスタンスからインスタンス (複数のインスタンス) へのユーザー属性の更新と同期を実現する ServiceNow® ストアアプリです。

ID とアクセスの監査

ID およびアクセスの監査を使用して、ユーザー、グループ、ロール、および ACL に加えられた変更を把握します。

ID センター

ID センターでは ID ベースのリスクとセキュリティギャップを監視および管理し、最小限に抑えることができます。

クロスドメイン ID 管理システム (SCIM)

クロスドメイン ID 管理システム (SCIM) API は、SCIM プロトコルを使用してユーザーとグループの操作を作成、読み取り、更新、および削除するためのエンドポイントを提供します。

アクセスアナライザー

ServiceNow® アクセス アナライザー は 、リソースの ID のアクセス許可を表示するのに役立つアクセス診断ツールです。

自動翻訳

探索

Access Analyzer の機能とビジネス価値について説明します。

使用方法

Access Analyzer の使用方法を理解します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

権限の評価

権限がどのように評価されるかを把握します。

よく寄せられる質問

Access Analyzer に関してよく寄せられる質問の詳細を取得します。

自動翻訳

Access Analyzer® の概要

ServiceNow インスタンスの ID を分析します。

ServiceNow Access Analyzer は、管理者と開発者が選択したユーザー、ロール、グループの権限を表示するのに役立つアプリケーションです。

注:

- Access Analyzer は ServiceNow Store 製品です。ServiceNow ストア Web サイトにアクセスして、利用可能なすべてのアプリを表示し、要求をストアに送信する方法について確認してください。
- Access Analyzer は ID レコードを代理操作して権限に関する詳細を取得しますが、ID の個人データや機密データを読み取ったり保存したりすることはありません。
- Access Analyzer の評価結果は、Zero Trust アクセス (ZTA) などの、ユーザーに対して定義されているアクセスポリシーに関係なく同じです。ポリシーは、実際のユーザーログイン中にのみ評価され、アクセスアナライザーフロー中には評価されません。
- Access Analyzer には、管理対象スコープリソースと委任開発者に関連するリソースのアクセスの正確な評価に関する制限があります。

アクセスを評価

アクセスの評価は、管理者と開発者が選択したユーザー、ロール、またはグループの権限を表示するのに役立つ、アクセスアナライザーの機能 ServiceNow です。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

これにより、テーブルのユーザー、グループ、ロール、クライアントコール可能スクリプトインクルード、UI ページ、および REST エンドポイントの権限を分析および表示できます。

Access Analyzer を使用すると、組織はセキュリティ体制、ID ガバナンス、リスク管理を改善し、コンプライアンス目標を達成して、どのユーザー (ID) が何 (リソース) にアクセスできるかを把握できます。

アクセスの比較

アクセスの比較は、管理者、開発者、およびサポートエージェントがユーザーアクセスを比較し、インスタンスのユーザーのServiceNow適切なアクセスレベルを決定できるようにする、アクセスの比較 V2 の機能ServiceNowです。

比較 ユーザーレコードとアクセス制御について、ユーザー間でアクセスを実行できます。

アクセスの比較では、次の分析を実行できます。

- レベル 1:ユーザーレコードを比較して、属性、ロール、およびグループを把握します。
- レベル 2:アクセス制御を比較し、アクセスの問題を見つけて根本原因分析を実行します。

利点

Access Analyzer を使用するメリットは次のとおりです。

- リソース (テーブル) へのアクセスを分析します。
- 2 人のユーザーのアクセス権を比較します。
- 2 人のユーザーのロールとグループを比較します。
- 権限のオーバープロビジョニングを防止します。
- ID がリソース (テーブル) にアクセスできるかどうかを示すレポートを生成します。
- 重要なセキュリティ検疫にアクセスできるユーザーを把握します。
- アクセス許可のオーバープロビジョニングを防ぐのに役立ちます。
- アクセス制御を実装するときに、最低限の権限のプリンシパルを実現します。
- アプリケーション、テーブル、行または列、その他のリソースを含む特定のデータへのアクセスを制限します。
- 分析結果のレポート機能を提供します。
- ユーザーレコードとアクセス制御の間でアクセスを比較します。
- インスタンスのユーザーの ServiceNow 適切なアクセスレベルを決定します。

Access Analyzer の使用

インスタンスでの ID とそのアクセスを分析します ServiceNow®。

始める前に
必要なロール：admin

次の手順では、Access Analyzer にアクセスし、Access Analyzer 内のさまざまな機能を使用するステップについて説明します。

注:
Access Analyzer は ServiceNow® Store 製品です。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. 移動先 すべて > アクセスアナライザー > 分析権限.
   [アクセスと権限の分析 (Analyze access and permissions)] ホームページが表示されます。

   アクセスアナライザには次の機能があります。

   - アクセスを評価
   - ユーザーレコードの比較
   - アクセス制御の比較

2. 要件に基づいて Access Analyzer を使用するそれぞれのタブを選択します。

評価アクセスの使用

ServiceNow® インスタンスの ID を分析します。

始める前に

必要なロール：admin

次の手順では、アクセスアナライザーでアクセスの評価にアクセスし、そのさまざまな機能を使用するための手順について説明します。

注:
Access Analyzer は製品です ServiceNow Store 。

手順

1. 移動先 すべて > アクセスアナライザー > 分析権限.
   [アクセスと権限の分析 (Analyze access and permissions)] ホームページが表示されます。
2. [アクセスの評価] タブを選択します。
3. 次のように基準を選択します。

アクセスと権限を分析するための基準を選択します

フィールド	説明
分析者 (Analyze by) *	ユーザー、ロール、グループのアクセスを分析します。
ユーザーを選択 *	リストから選択するユーザー名を指定します。
ルールタイプ *	テーブル、UI ページ、REST エンドポイント、またはクライアントコール可能スクリプトインクルードのアクセスを分析します。
テーブルを選択 *	リストから選択するテーブル名を指定します。
レコードを選択	リストから選択するレコード名を指定します。
フィールドを選択	リストから選択するフィールド名を指定します。

4. [説明] フィールドに説明を指定します。
5. [権限を分析 **(Analyze Permissions)]** を選択します。

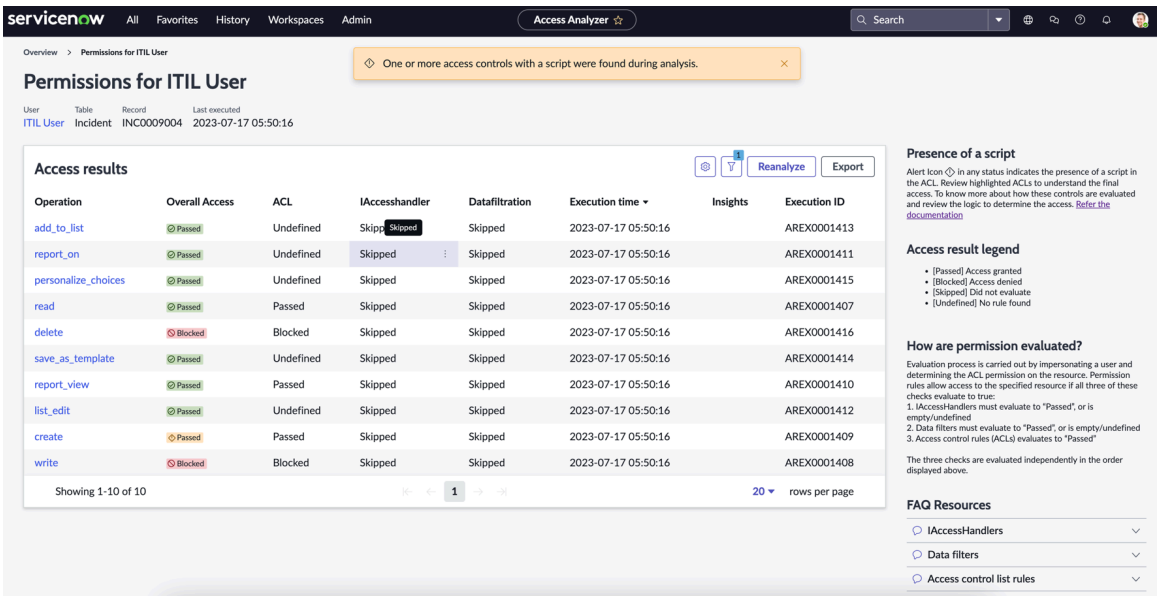
   ユーザーのアクセス結果が表示されます。同様に、次のルールの種類について、グループまたはロールのアクセス許可を分析できます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

- テーブル (レコード)
- クライアントコール可能スクリプトには以下が含まれます。
- REST エンドポイント

アクセス結果が表示されます。



アクセス結果テーブルには、次のフィールドが含まれています。

アクセス結果

フィールド	説明
操作	選択したテーブル、レコード、またはフィールドに対してユーザー、グループ、またはロールが実行できる操作のタイプ。
全体的なアクセス (Overall Access)	全体的なアクセスの結果。結果は次のとおりです。 ○ [合格] アクセスが許可されました ○ [ブロック済み] アクセスが拒否されました ○ [スキップ済み] 評価されませんでした ○ [未定義] ルールが見つかりません
ACL	選択した操作に ACL が定義されているかどうか。
IAccesshandler	プラットフォーム上の非表示のソースコードを使用する内部システムチェック。IAccessHandler は、ACL を評価せずにリソースへのアクセスを許可または拒否できます。IAccessHandler が無視されると、ACL が評価されます。
データフィルタリング	データフィルターは、インスタンスの既存のアクセス制御ルール (ACL) と連携して機能するように設計されたアクセス制御の一種です。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
実行時間	アクセス結果が実行された時刻。
インサイト	選択した操作に関する詳細情報
実行 ID	アクセス結果実行ごとの一意のID。

ユーザーの権限の表示

Access Analyzer を使用して選択したユーザーの権限を表示します。

始める前に

必要なロール：admin

次の手順では、選択したユーザー (**ITIL** ユーザー) の権限を表示し、 アクセス アナライザーの評価アクセス権を使用してインシデントテーブルの権限を表示するサンプルステップについて説明します。

注:
Access Analyzer は ServiceNow® Store 製品です。

手順

1. 移動先 すべて > アクセスアナライザー > 分析権限.
   [アクセスと権限の分析 (Analyze access and permissions)] ホームページが表示されます。
2. 次のように基準を選択します。

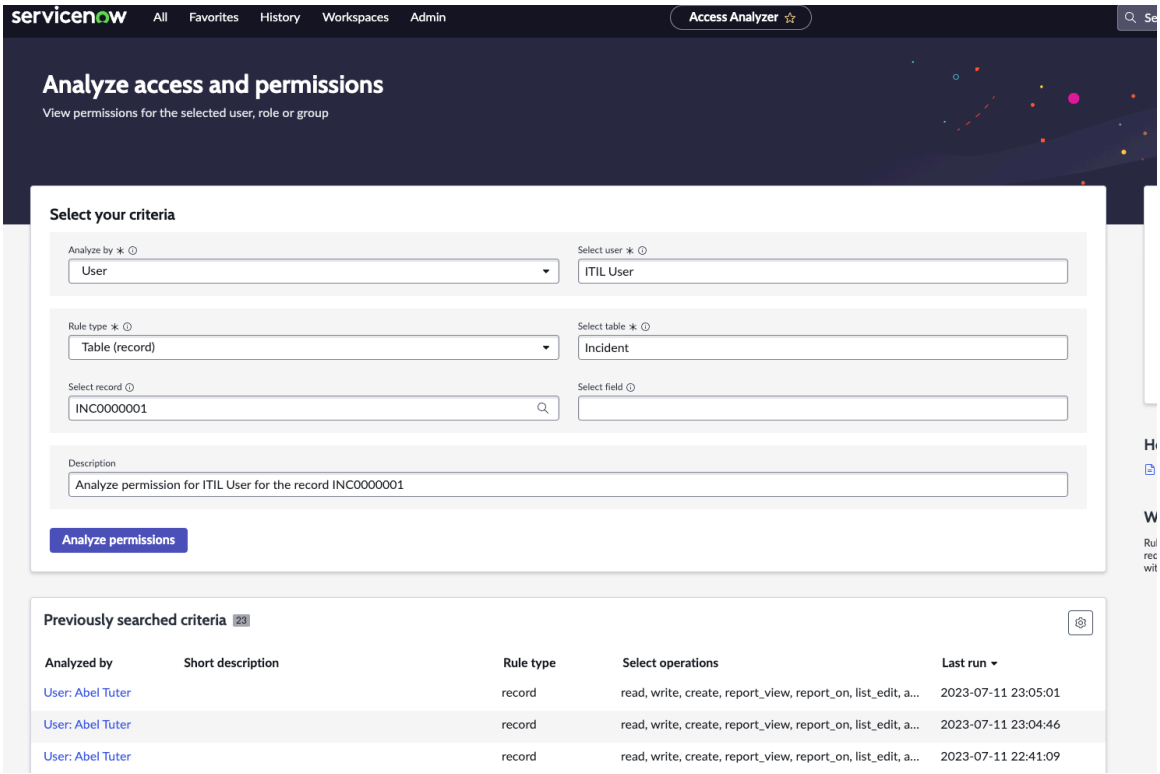
   アクセスと権限を分析するための基準を選択します

フィールド	説明
分析者 (Analyze by) *	[ユーザー] を選択します。
ユーザーを選択 *	リストから選択するユーザー名を指定します。この例では、**[ITIL** ユーザー **(ITIL User)]** です。
ルールタイプ *	テーブル、**UI** ページ、**REST** エンドポイント、またはクライアントコール可能スクリプトインクルードのアクセスを分析します。この例では、テーブルです。
テーブルを選択 *	リストから選択するテーブル名を指定します。この例では、[インシデント] です。
レコードを選択	リストから選択するレコード名を指定します。この例では、**INC0000001** です。
フィールドを選択	リストから選択するフィールド名を指定します。このフィールドは、フィールドレベルで権限を分析するためにも使用できます。たとえば、アクティブ、作成者などです。

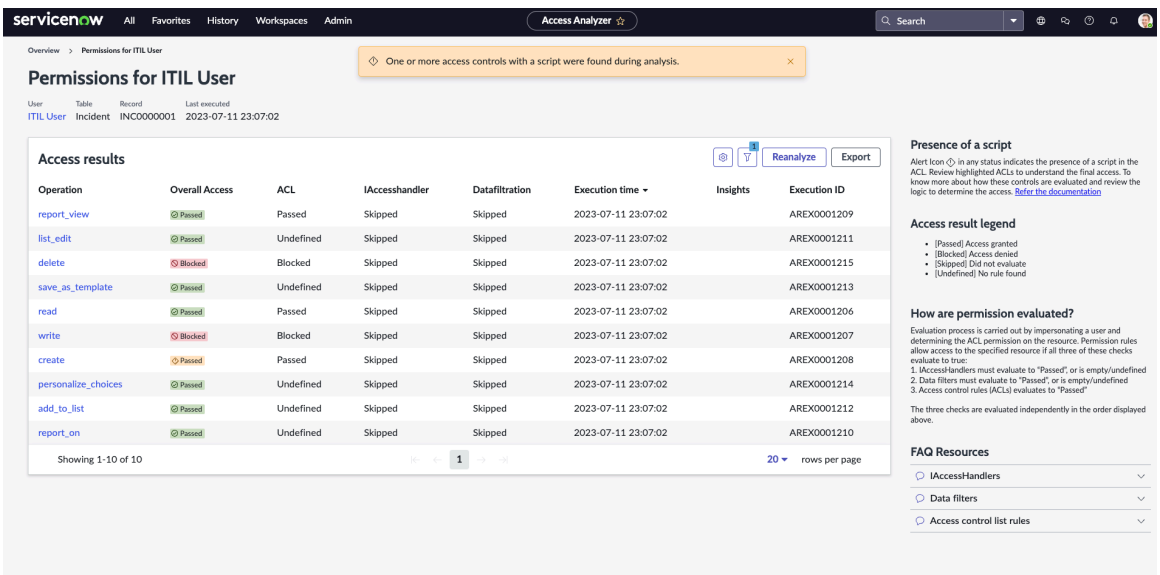
3. [説明] フィールドに説明を指定します。
4. [権限を分析 **(Analyze Permissions)]** を選択します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



[ITIL ユーザー (ITIL User)] の [アクセス結果 **(Access results)]** が表示されます。



この結果は、凡例、アクセス制御リスト (ACL)、IAccesshandler、データフィルターを参照して読み取ることができます。

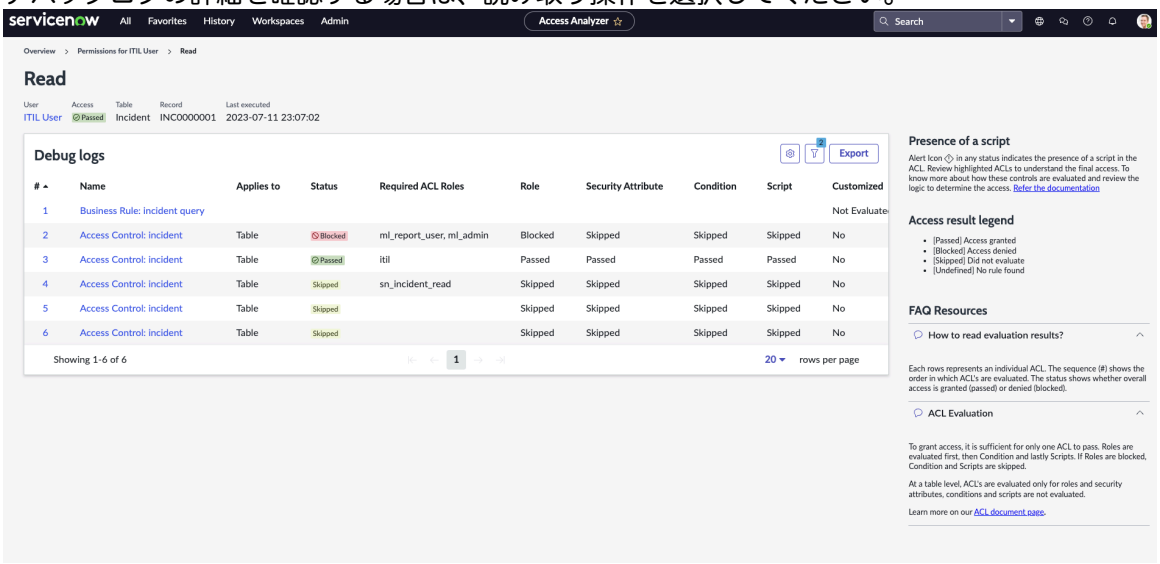
[読み取り] 操作の例を確認します。**[ITIL ユーザー (ITIL User)]** の場合、全体的なアクセス権は「合格」です。これは、ユーザーが正しい権限 (ACL) でレコードの読み取りができることを意味します。

同様に、[作成] 操作では、全体的なアクセス権は合格であり、アラートアイコンが表示されます。これは、ACL 評価用のスクリプトが存在する可能性があることを意味します。

> **注:**
> この例では、選択したユーザーの [書き込み] 操作と [削除] 操作がブロックされ、ユーザーは選択したレコード (INC0000001) を編集または削除できません。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

5. デバッグログの詳細を確認する場合は、読み取り操作を選択してください。

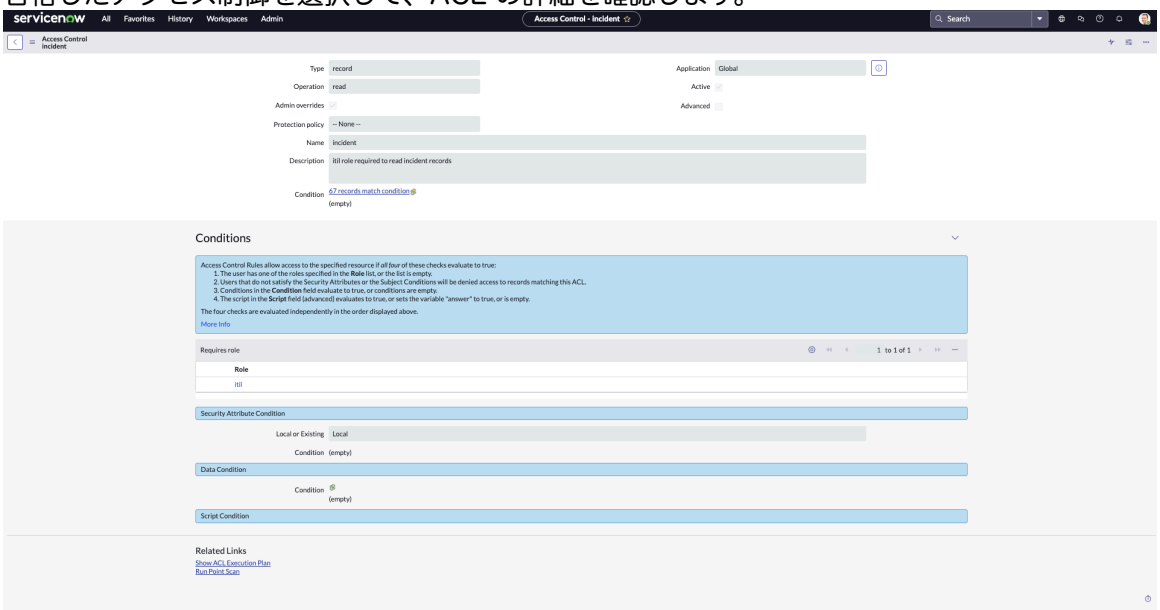


[デバッグログ] ページには、レコードの [読み取り] 操作を実行するために必要なビジネスルールと関連する ACL が表示されます。

デバッグログには、読み取り操作に関連付けられたビジネスルールと 4 つの ACL があることが示されています。

いずれかの ACL に [合格] ステータスが表示されています。これは、選択したレコードを読み取り、ユーザーに必要な ACL があり、レコードを読み取ることができることを意味しています。ACL の 1 つが [合格]であるため、他の ACL 評価は [スキップ済み]になります。

6. 合格したアクセス制御を選択して、ACL の詳細を確認します。

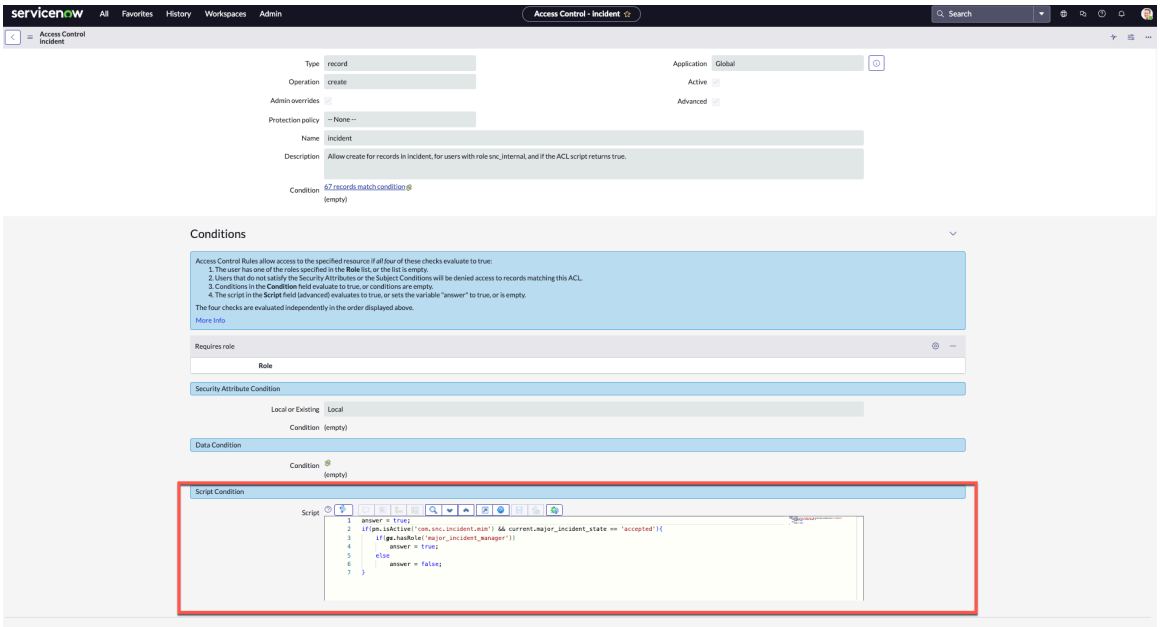


選択した ACL のアクセス制御の詳細が表示されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

選択した操作は [合格] であり、スクリプトが存在します。[アクセス制御] ページには、レコードに関連するスクリプトが表示されます。



ロールの権限の表示

Access Analyzer を使用して選択したロールの権限を表示します。

始める前に

必要なロール：admin

次の手順では、選択したロール (**user_admin**) の権限を表示し、アクセスアナライザーの評価アクセス権を使用して REST API エンドポイントの権限を表示するサンプルステップについて説明します。

> **注:**
> Access Analyzer は ServiceNow® Store 製品です。

手順

1. 移動先 すべて > アクセスアナライザー > 分析権限.
   [アクセスと権限の分析 (Analyze access and permissions)] ホームページが表示されます。
2. 次のように基準を選択します。

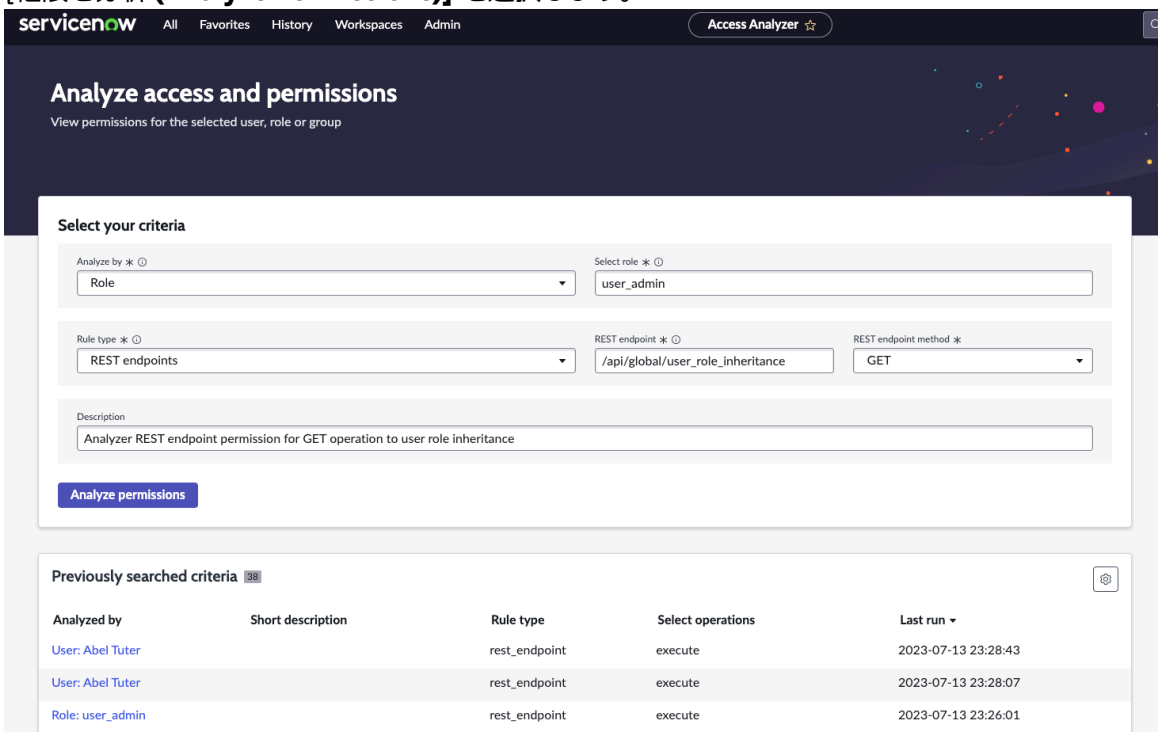
アクセスと権限を分析するための基準を選択します

フィールド	説明
分析者 (Analyze by) *	[ロール] を選択します。
ユーザーを選択 *	リストから選択するロールを指定します。 例：**user_admin**
ルールタイプ *	テーブル、UI ページ、REST エンドポイント、またはクライアントコール可能スクリプトインクルードのアクセスを分析します。例：**REST エンドポイント (REST endpoint)**

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
REST エンドポイント (REST endpoint)*	REST エンドポイントを指定します。 例：/api/global/user_role_inheritance **注:** 選択したフィールドを使用する場合は、完全な REST エンドポイントを使用する必要があります。
REST エンドポイントメソッド (REST endpoint method) *	REST エンドポイントメソッドを指定します。 例：GET

3. [説明] フィールドに説明を指定します。
4. [権限を分析 **(Analyze Permissions)]** を選択します。



user_admin ロールの [アクセス結果 **(Access results)]** が表示されます。

この結果は、凡例、アクセス制御リスト (ACL)、IAccesshandler、データフィルターを参照して読み取ることができます。

ロールの全体的なアクセス権が合格します。これは、ロール (**user_admin**) が、選択した **[GET]** メソッドの **[REST** エンドポイント **(REST endpoint)]** にアクセスできることを意味します。

グループの権限の表示

Access Analyzer を使用して選択したグループの権限を表示します。

始める前に

必要なロール：admin

次の手順では、選択したグループ (インシデント管理) の権限を表示し、アクセスアナライザーの評価アクセス権を使用してインシデント**UI** ページの権限を表示するサンプルステップについて説明します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注:
Access Analyzer は ServiceNow® Store 製品です。

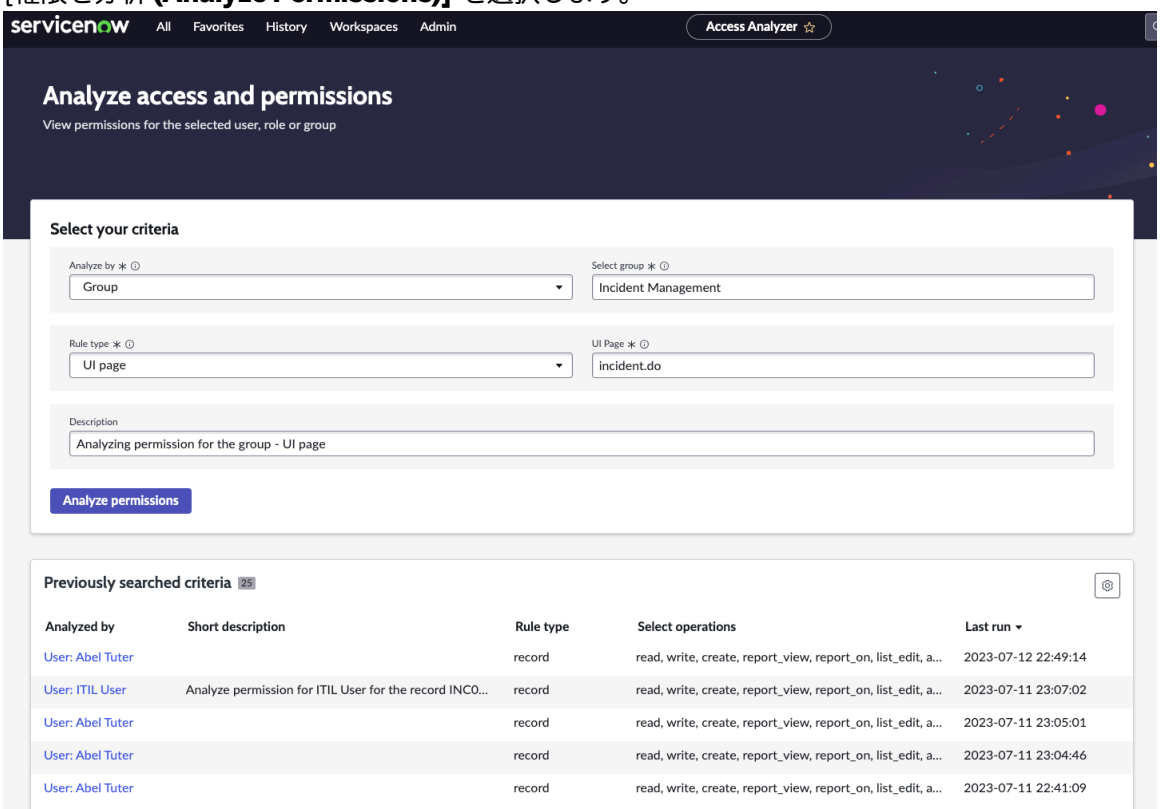
手順

1. 移動先 すべて > アクセスアナライザー > 分析権限.
   [アクセスと権限の分析 (Analyze access and permissions)] ホームページが表示されます。
2. 次のように基準を選択します。

アクセスと権限を分析するための基準を選択します

フィールド	説明
分析者 (Analyze by) *	[グループ] を選択します。
ユーザーを選択 *	リストから選択するユーザー名を指定します。例：**Incident Management**
ルールタイプ *	テーブル、UI ページ、REST エンドポイント、またはクライアントコール可能スクリプトインクルードのアクセスを分析します。例：**UI** ページ
UI ページ*	UI ページを指定します。例：**incident.do**

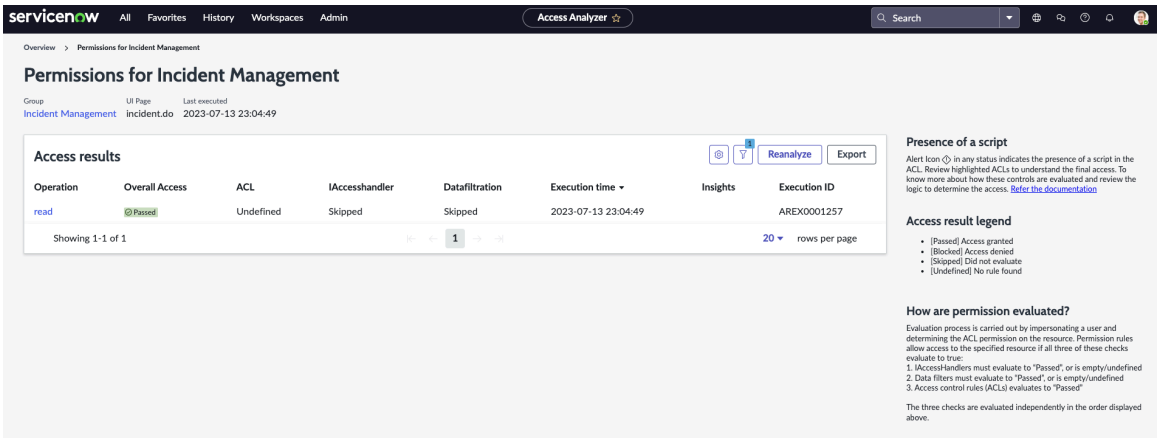
3. [説明] フィールドに説明を指定します。
4. [権限を分析 **(Analyze Permissions)]** を選択します。



[Incident Management] グループの [アクセス結果 **(Access results)]** が表示されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



この結果は、凡例、アクセス制御リスト (ACL)、IAccesshandler、データフィルターを参照して読み取ることができます。

グループの全体的なアクセス権は合格です。これは、グループ内のユーザー (**Incident Management**) がインシデントレコードにアクセスできることを意味します。

Access Analyzer クエリのエクスポート

Access Analyzer を使用して分析されたクエリをエクスポートします。

始める前に

必要なロール：admin

次の手順では、Access Analyzer にアクセスし、Access Analyzer 内のさまざまな機能を使用するステップについて説明します。

> **注:**
> Access Analyzer は ServiceNow® Store 製品です。

手順

1. 移動先 すべて > アクセスアナライザー > 分析権限.
   [アクセスと権限の分析 (Analyze access and permissions)] ホームページが表示されます。
2. 次のように基準を選択します。

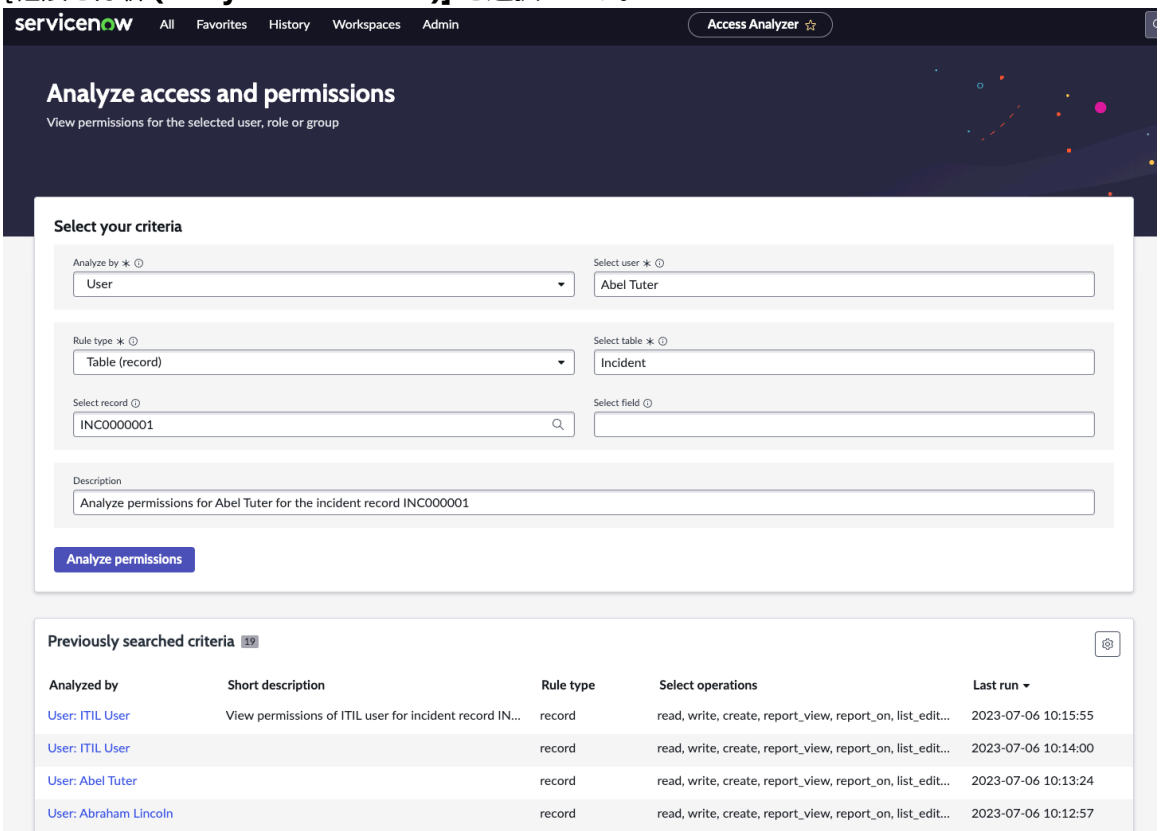
アクセスと権限を分析するための基準を選択します

フィールド	説明
分析者 (Analyze by) *	ユーザー、ロール、グループのアクセスを分析します。
ユーザーを選択 *	リストから選択するユーザー名を指定します。
ルールタイプ *	テーブル、UI ページ、REST エンドポイント、またはクライアントコール可能スクリプトインクルードのアクセスを分析します。
テーブルを選択 *	リストから選択するテーブル名を指定します。
レコードを選択	リストから選択するレコード名を指定します。
フィールドを選択	リストから選択するフィールド名を指定します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

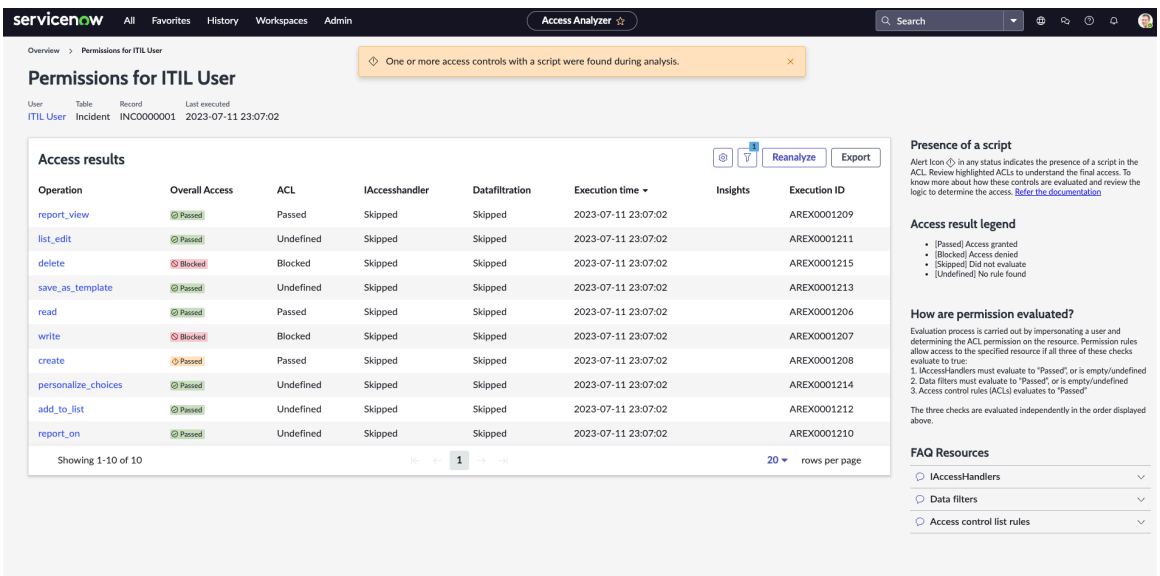
3. [説明] フィールドに説明を指定します。
4. [権限を分析 **(Analyze Permissions)**] を選択します。



ユーザーのアクセス結果が表示されます。同様に、次のルールタイプについて、グループ、ロールの権限を分析できます。

- テーブル (レコード)
- クライアントコール可能スクリプトインクルード
- REST エンドポイント

選択したルールタイプの [アクセス結果 **(Access results)**] が表示されます。



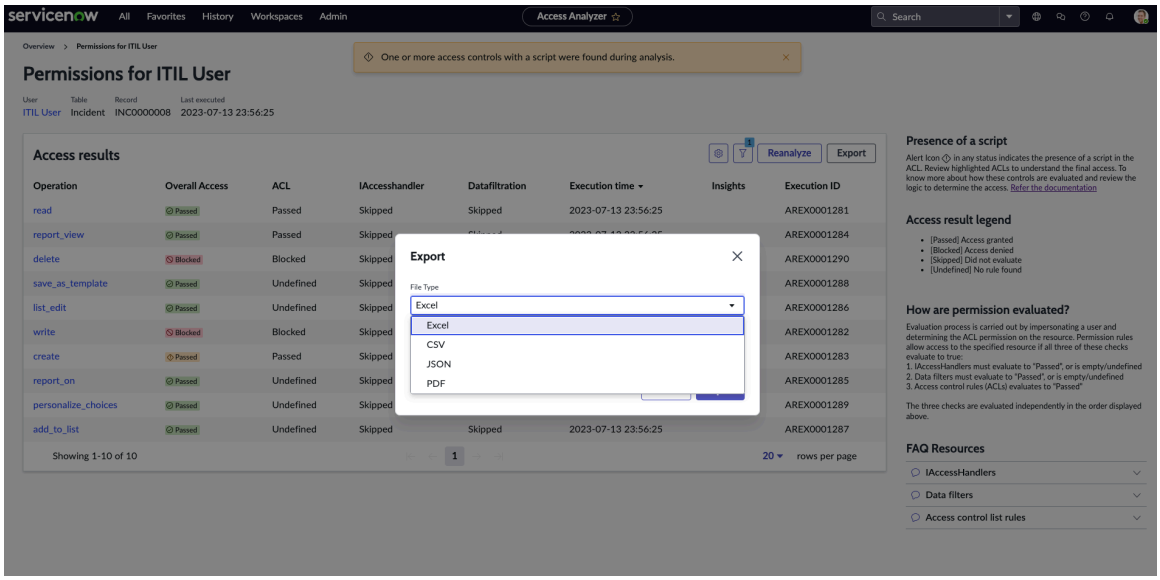
5. [エクスポート] をクリックします。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

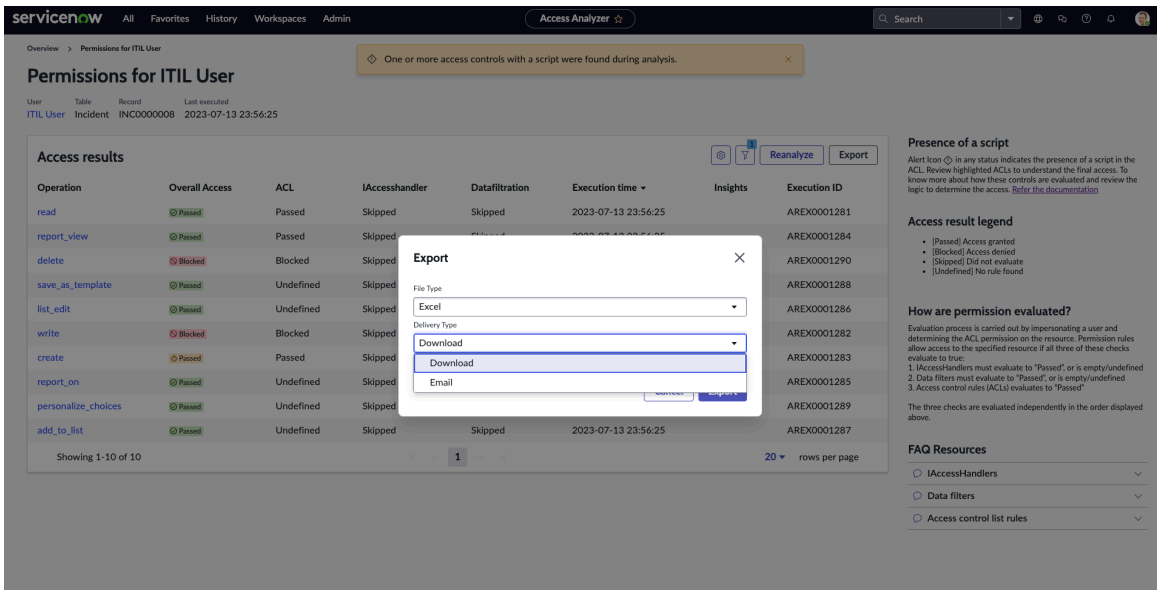
a. ファイルタイプを選択します。

利用可能なファイルタイプは、Excel、CSV、JSON、PDF です。



b. [配送タイプ] を選択します。

利用可能な配送タイプは、ダウンロードとメールです。



ユーザーレコードの比較

ユーザーレコードを比較して、2 人のユーザー間のアクセスを把握します。

始める前に
必要なロール：admin

次の手順では、アクセスアナライザーを使用してユーザーレコードを比較するステップについて説明します。

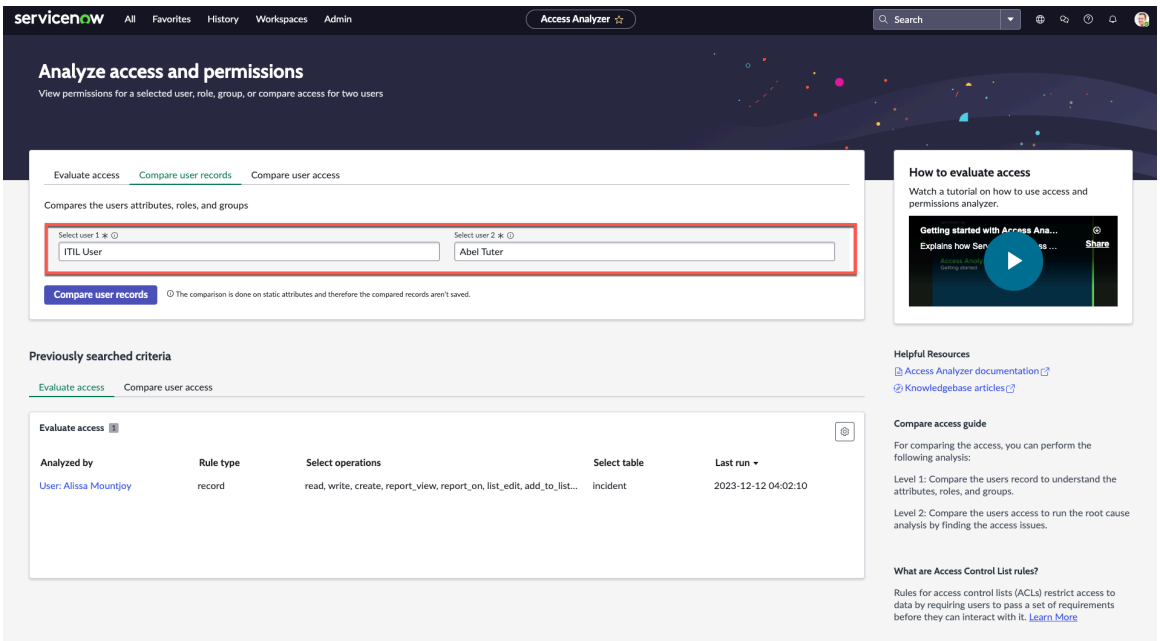
注:
Access Analyzer は製品です ServiceNow® Store 。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. 移動先 すべて > アクセスアナライザー > 分析権限.
   [アクセスと権限の分析 (Analyze access and permissions)] ホームページが表示されます。
2. [ユーザーレコードの比較 **(Compare user records**)] タブを選択します。
3. 比較するユーザー **1** と ユーザー **2** を選択します。

   たとえば、ユーザー 1 は ITIL ユーザー、ユーザー**2** は Abel Tuter です。



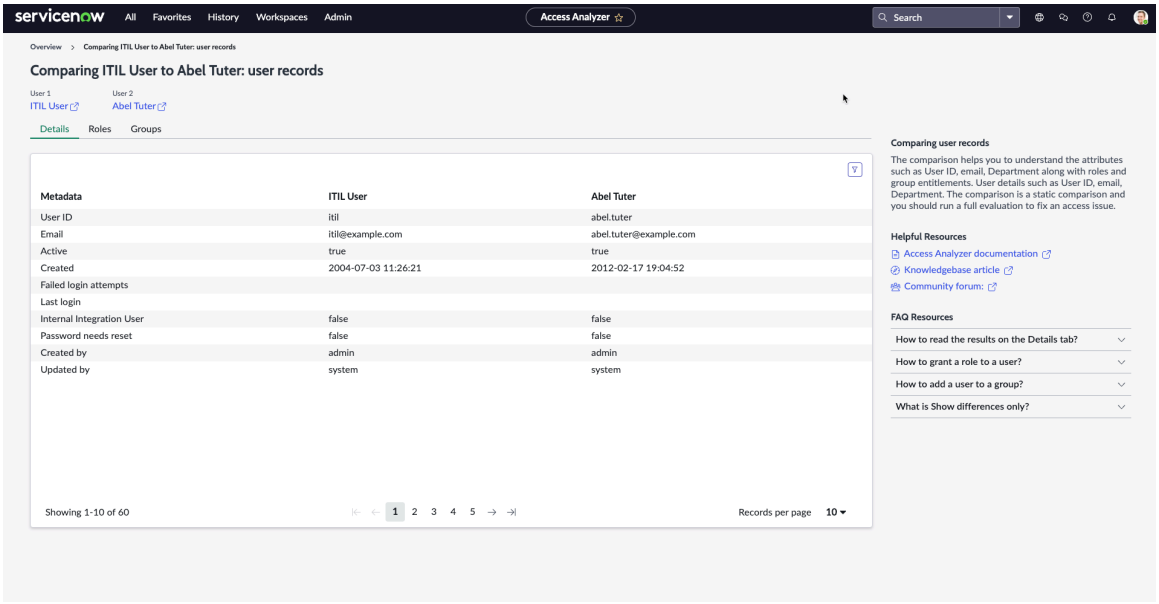
4. [ユーザー レコードの比較] を選択します。

   結果は次のタブに表示されます。

自動翻訳

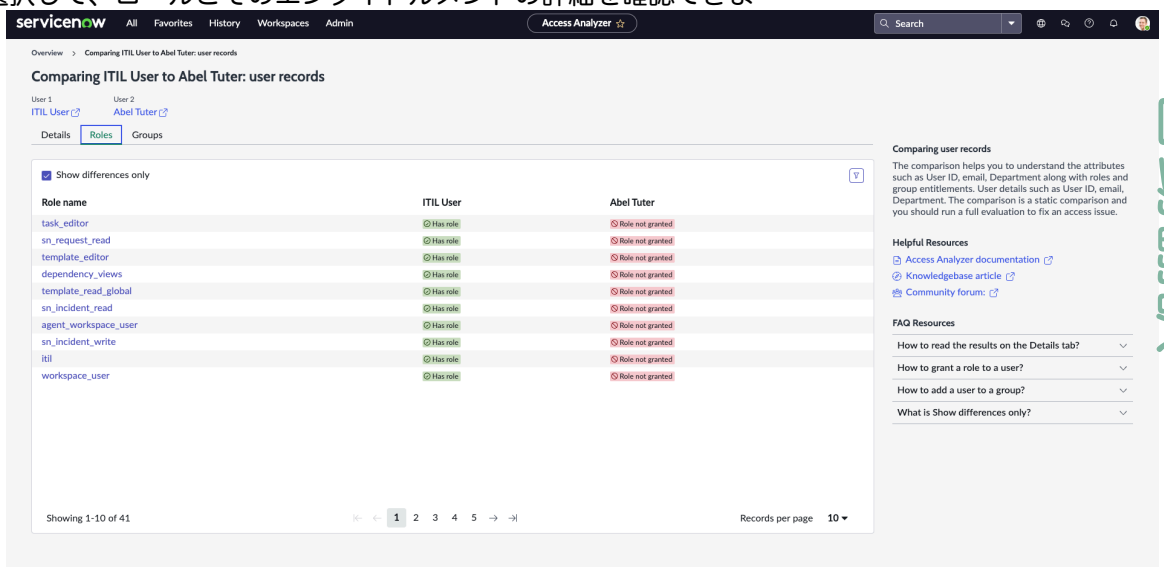
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- 詳細: ユーザーのメタデータを表示しま



す。

- ロール:ユーザーに割り当てられているロールを表示します。ロールを選択して、ロールとそのエンタイトルメントの詳細を確認できま

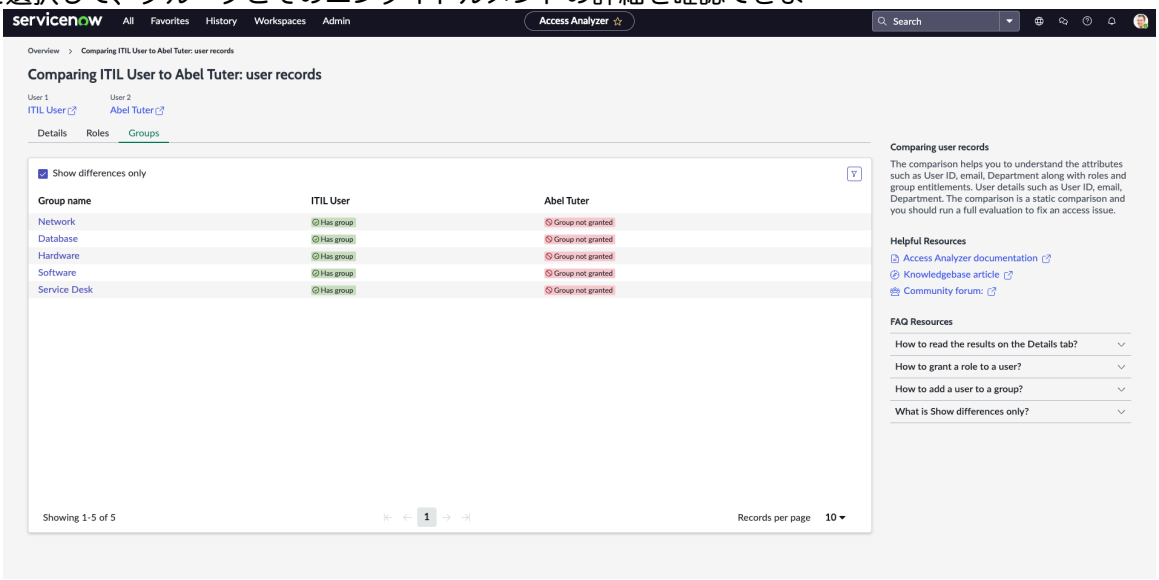


す。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- グループ:ユーザーに割り当てられているグループを表示します。グループを選択して、グループとそのエンタイトルメントの詳細を確認できます。



同様に、インスタンス内の ServiceNow さまざまなユーザーを比較して、ユーザーに割り当てられているアクセス権を把握できます。

ユーザーアクセスの比較

アクセスアナライザーを使用して、ユーザーのアクセス制御を比較します。

始める前に
必要なロール：admin

次の手順では、アクセスアナライザーを使用するユーザー間でアクセス制御を比較する手順について説明します。

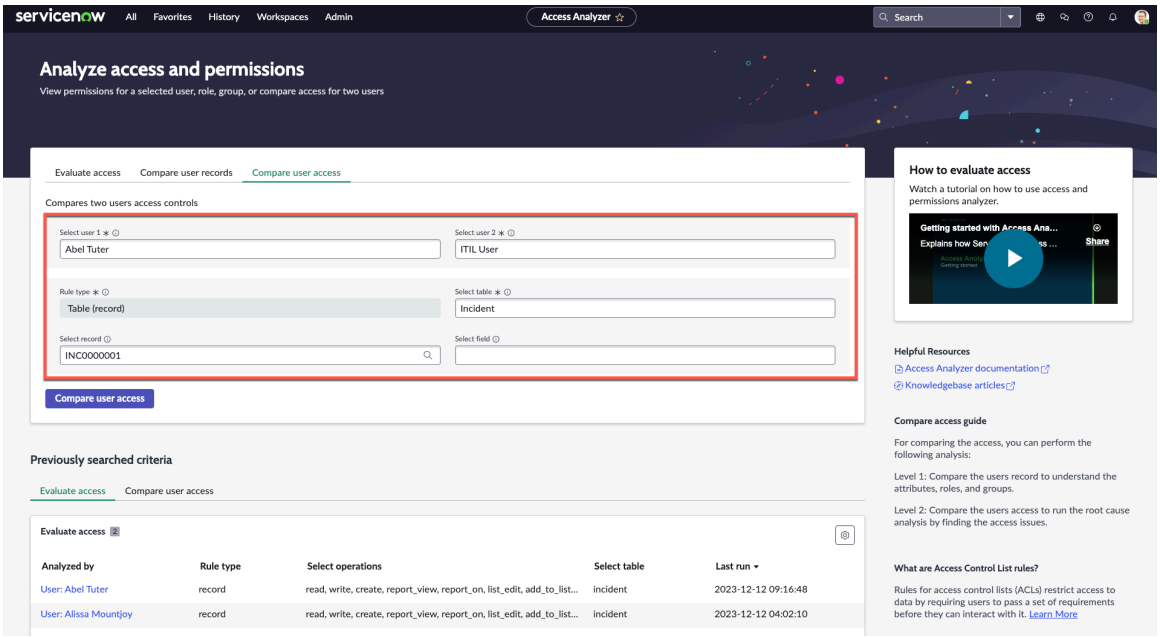
注:
Access Analyzer は製品です ServiceNow® Store 。

手順

1. 移動先 すべて > アクセスアナライザー > 分析権限.
   [アクセスと権限の分析 (Analyze access and permissions)] ホームページが表示されます。
2. [ユーザー アクセスの比較] タブを選択します。
3. 次のフィールドに入力します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



ユーザーアクセスの比較

フィールド	説明
ユーザー 1* を選択	比較のためにリストから選択するユーザー名を指定します。
ユーザー 2 を選択*	ユーザー 1 と比較するためにリストから選択するユーザー名を指定します。
ルールタイプ*	テーブルのアクセス許可を分析します。 **注:** ユーザー比較アクセスで使用できるのは、テーブルのアクセス権限のみです。
テーブルを選択*	リストから選択するテーブル名を指定します。
レコードを選択	リストから選択するレコード名を指定します。
フィールドを選択	リストから選択するフィールド名を指定します。

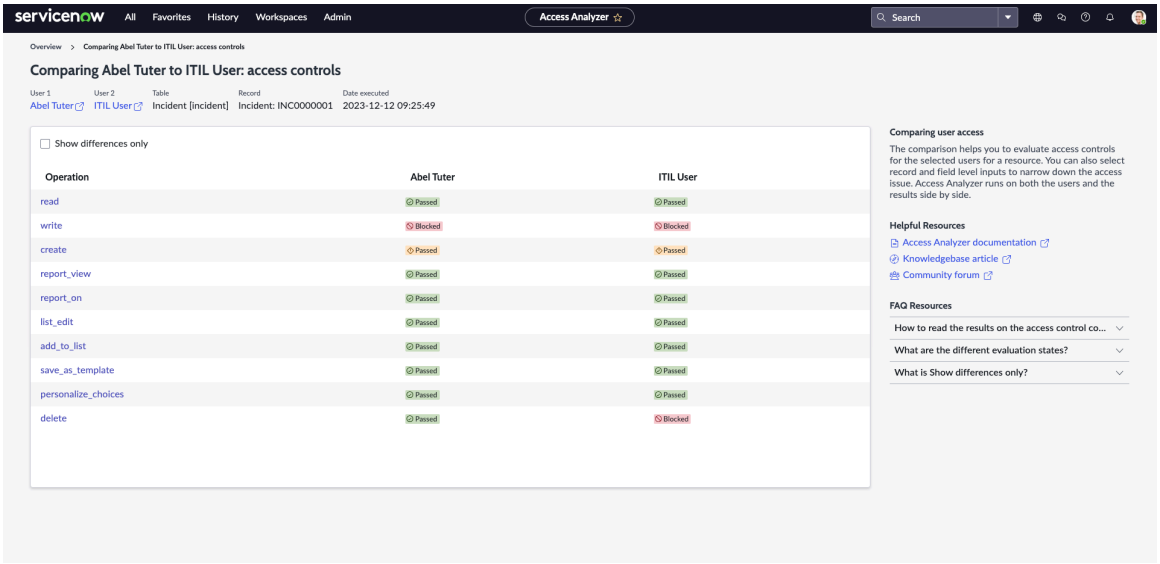
自動翻訳

4. [ユーザー アクセスの比較] を選択します。

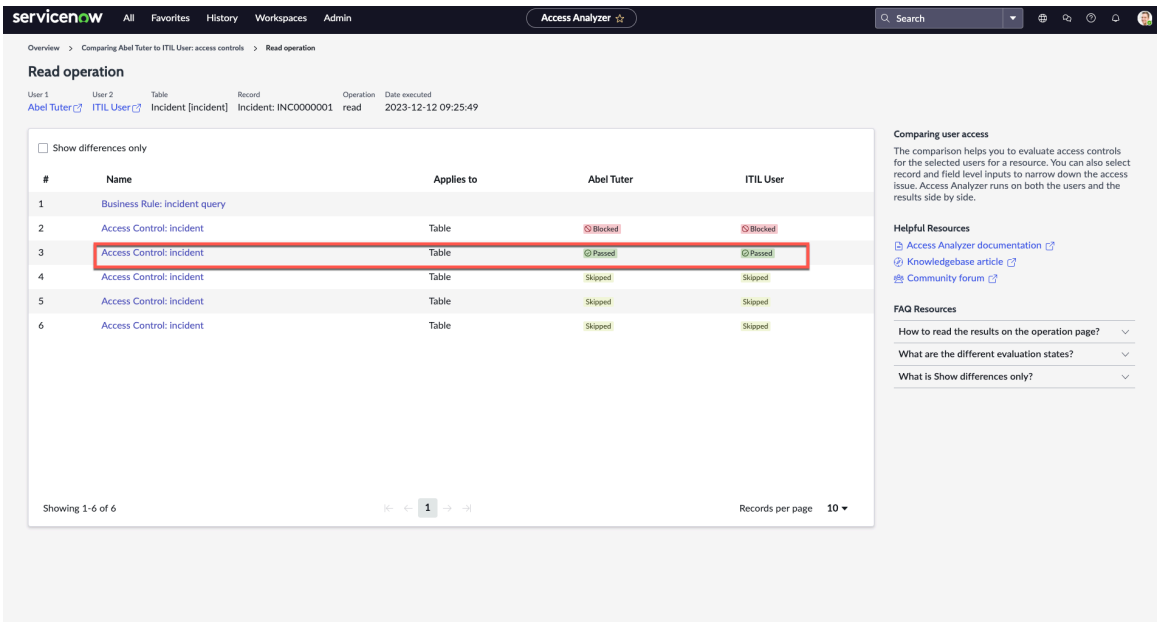
   選択したユーザーの ユーザーアクセスの比較 結果が表示されます。

   ユーザーアクセスの比較結果には、ユーザーの操作とアクセス評価ステータスが表示されます。たとえば、Abel Tuter と ITIL User などです。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

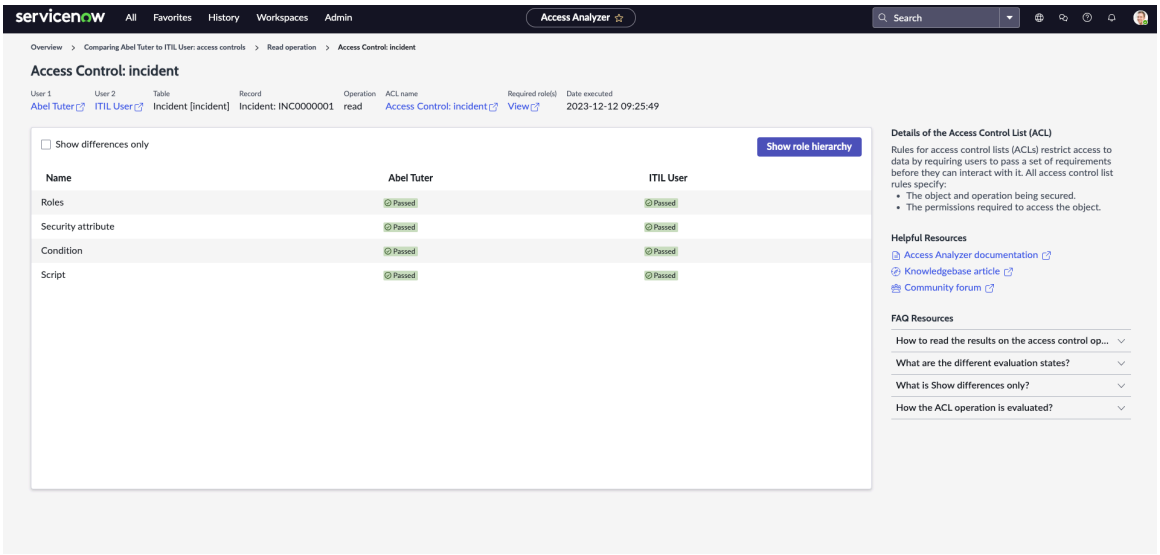


5. [操作] を選択して、権限の評価とユーザーに割り当てられているロールの詳細を確認します。たとえば、 読み取り 操作です。
6. アクセスの詳細を確認するには、いずれかの アクセス制御 を選択します。



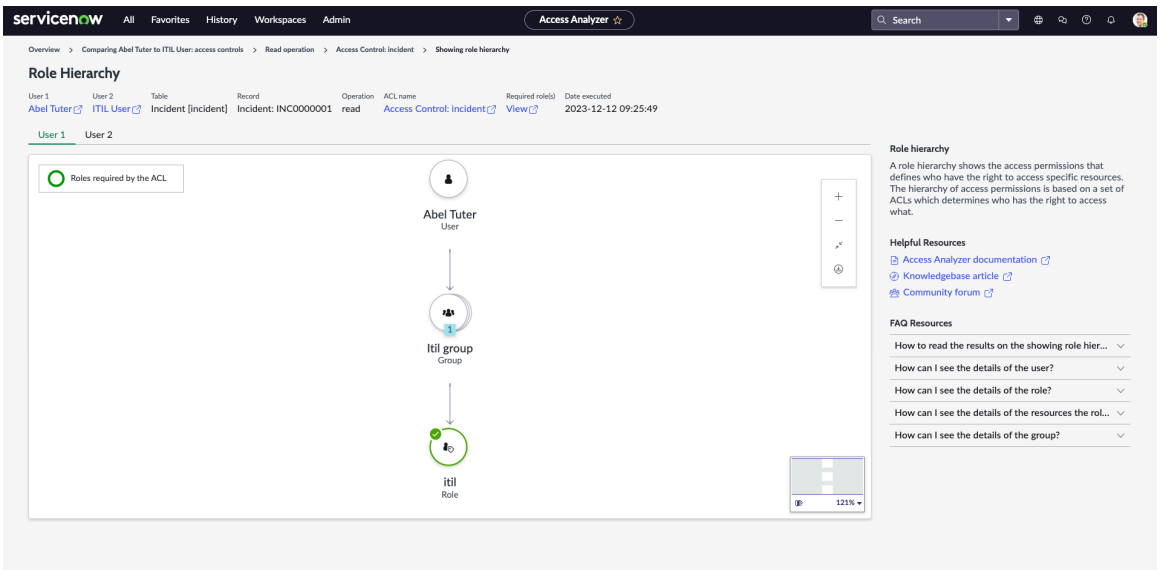
ロール、セキュリティ属性、条件、スクリプト評価ステータスなどのアクセス制御の詳細が表示されます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



7. [ロール階層の表示] を選択して、ユーザーに割り当てられているロールとグループの詳細を確認し、両方のユーザーを比較します。

ロール階層に基づいて、リソース (テーブル) にアクセスするために必要なロールとグループのアサインをユーザーにアサインできます。

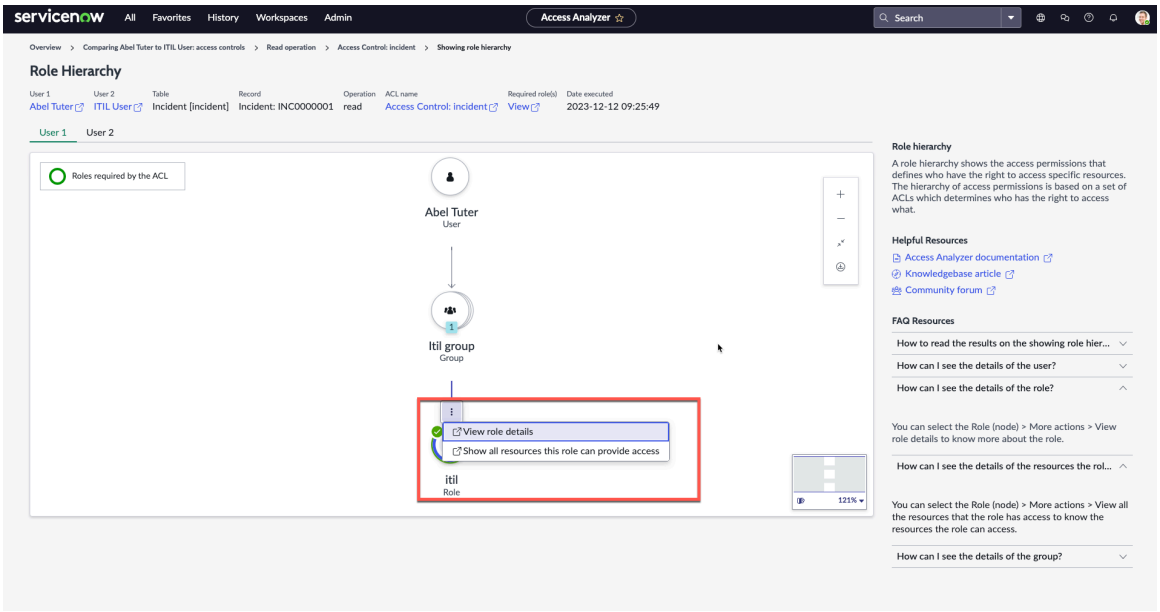


この例では、 **Abel Tuter** と **ITIL** ユーザーの両方に itil ユーザーがアサインされています。したがって、両方のアクセス制御が渡されました。ロール階層を調べることで、ユーザーに必要なロールとグループの割り当てを決定できます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ノードを選択すると、ロール、ロールがアクセスできるリソース、またはグループの詳細を確認できます。



アクセスアナライザークエリの表示 - 以前に検索した条件

以前に検索した Access Analyzer の基準を表示します。

始める前に

必要なロール：admin

> **注:**
> Access Analyzer は製品です ServiceNow® Store 。

手順

1. 移動先 すべて > アクセスアナライザー > アクセスアナライザークエリ.

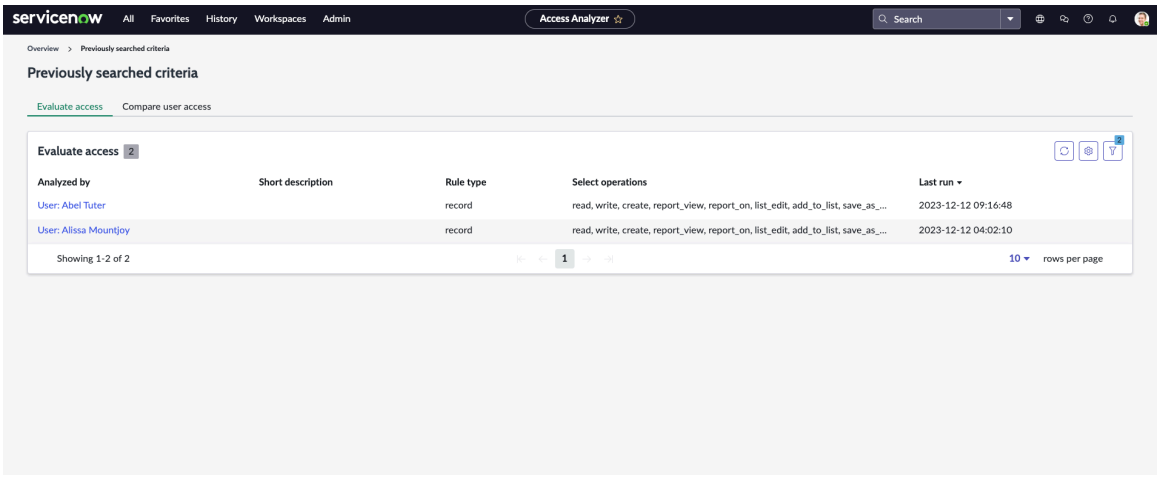
   以前に検索された条件には、次のセクションがあります。

   - アクセスの評価: アクセスの評価 機能によって行われたクエリに基づいて結果を表示します。
   - ユーザー アクセスの比較: ユーザー アクセスの比較機能によって行われたクエリに基づいて結果を表示します。

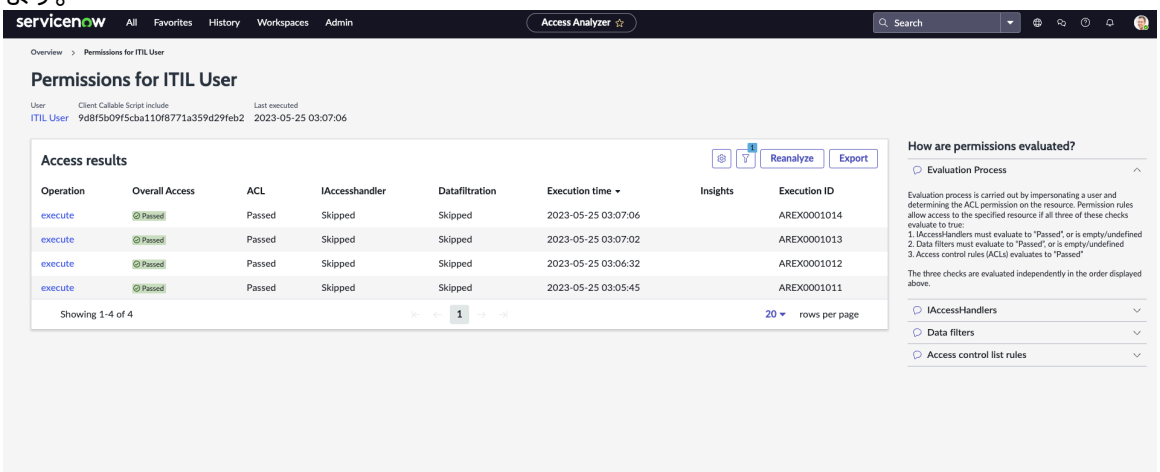
   > **注:**
   > ユーザーレコードの比較機能を使用する場合、以前に検索した条件は保存されません。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

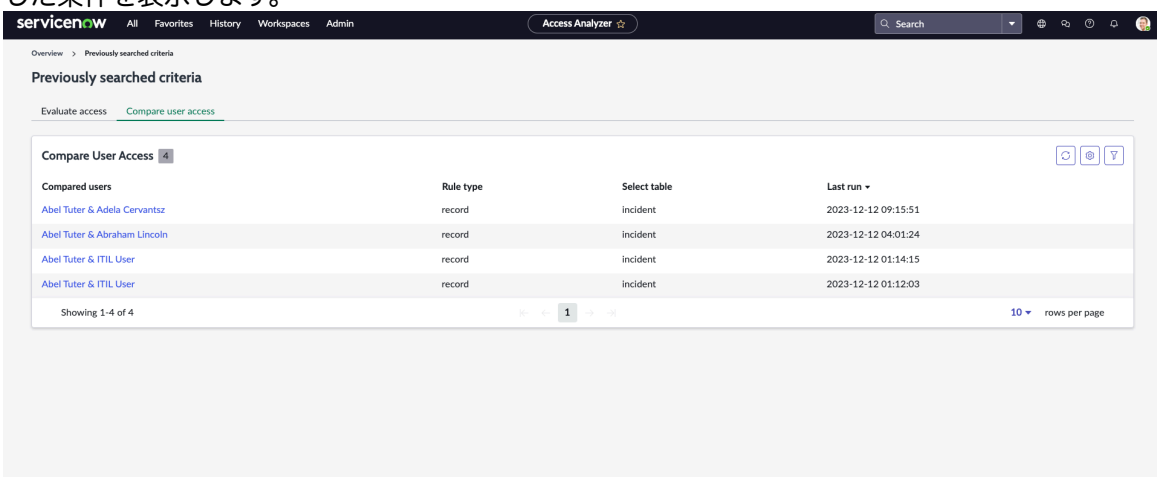


2. [アクセスの評価] セクションから以前に検索した条件を表示するには、[分析者] リンクを選択します。



[ユーザーのアクセス を再分析 する] を選択できます。[エクスポート] オプションを使用して詳細をエクスポートします。

3. [比較されたユーザー] リンクを選択して、[ユーザーアクセスの比較] セクションから以前に検索した条件を表示します。



権限の評価

Access Analyzer を使用する場合の権限の評価基準です。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

評価階層

選択したユーザー、グループ、ロールの権限は、次の階層で評価されます。

- ビジネスルール：ビジネスルールとは、レコードが表示、挿入、更新、または削除されるとき、またはテーブルに対してクエリが実行されるときに実行する、サーバー側スクリプトです。
- アクセスハンドラー：プラットフォーム上の非表示のソースコードを使用する内部システムチェックです。
- データフィルタリング：データフィルターは、インスタンスの既存のアクセス制御ルール (ACL) と連携して機能するように設計されたアクセス制御の形式です。データフィルターでは読み取り操作のみがサポートされます。
- アクセス制御リスト (ACL)：アクセス制御リスト (ACL) のルールは、まず要件のセットをユーザーに要求し、その後でユーザーとやり取りできるようにすることで、データへのアクセスを制限します。ACL 内では、次の階層が評価されます。
  - ロール
  - セキュリティ属性
  - 条件
  - スクリプト

Access Analyzer を使用して、選択したユーザー、ロール、またはグループのアクセス権と権限を分析できます。権限は、次のルールタイプに基づいて評価されます。

- テーブルレベルの評価 **(Table Level Evaluation)**：テーブルレベルの評価には、ロールとセキュリティ属性の ACL が使用されます。
- レコードまたはフィールドレベルの評価 **(Record or Field level Evaluation)**：レコードまたはフィールドレベルの評価には、ロール、セキュリティ属性、条件、およびスクリプトレベルの ACL が使用されます。
- **UI** ページ：準備完了操作のみをサポートします。読み取りレベルの ACL のみが評価されます。
- **REST** エンドポイント **(REST Endpoint)**：実行操作のみをサポートします。実行レベルの ACL のみが評価されます。

アクセス結果の重要なフィールドの詳細は次のとおりです。

- スクリプトの存在
- アクセス結果の凡例
- 評価プロセス
- IAccessHandler
- データフィルター
- アクセス制御リストのルール

スクリプトの存在

ステータスのアラートアイコンは ACL にスクリプトが存在することを示します。ハイライト表示された ACL を確認して、最終的なアクセス権を把握します。これらの制御を評価する方法の詳細を把握し、アクセスを決定するロジックを確認するには、「Access Analyzer のデバッグログ」を参照してください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Access Analyzer の凡例

アクセスと権限を分析する際、評価プロセスの一部として凡例が表示されます。凡例は次のとおりです。

- [合格] アクセスが許可されました
- [ブロック] アクセスが拒否されました
- [スキップ] 評価しませんでした
- [未定義] ルールが見つかりませんでした

評価プロセス

評価プロセスは、ユーザーの代理操作を行い、リソースに対するアクセス制御リスト (ACL) 権限を決定することによって実行されます。次のチェックが true と評価された場合、権限ルールにより、指定されたリソースへのアクセスが有効になります。

- IAccessHandler は「合格」と評価されるか、空または未定義である必要がある
- データフィルターは「合格」と評価されるか、空または未定義である必要がある
- アクセス制御ルール (ACL) が「合格」と評価される

IAccessHandler

プラットフォーム上の非表示のソースコードを使用する内部システムチェック。IAccessHandler は、ACL を評価せずにリソースへのアクセスを許可または拒否できます。IAccessHandler が無視されると、ACL が評価されます。

IAccessHandler チェックは変更できません。たとえば、IAccessHandler 実装は読み取りアクセスなどのアプリケーションリソースのアクセスチェックに使用されます。

データフィルター

データフィルターは、インスタンスの既存のアクセス制御ルール (ACL) と連携して機能するように設計されたアクセス制御の形式です。

アクセス制御リストのルール

アクセス制御リスト (ACL) のルールは、まず要件のセットをユーザーに要求し、その後でユーザーとやり取りできるようにすることで、データへのアクセスを制限します。

よく寄せられる質問

アクセス アナライザーの使用中によく寄せられる質問。

アクセスを評価

以下は、アクセスアナライザーのアクセスの評価機能を使用する際によく寄せられる質問の一部です。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

よく寄せられる質問

質問	説明
Access Analyzer によって表示される評価結果の読み方を教えてください。	各行は個々のアクセス制御リスト (ACL) を表します。結果のシーケンス (#) は ACL が評価される順序です。ステータスは、全体的なアクセスが許可 (合格) されるのか、拒否 (ブロック) されるのかを示します。
ACL はどのように評価されますか？	テーブルレベルでは、ACL はロールとセキュリティ属性に対してのみ評価され、条件とスクリプトは評価されません。 ロールが最初に評価されます。ロールがブロックされている場合、条件とスクリプトはスキップされます。詳細については、「ACL ルールの構成」を参照してください。
Access Analyzer にはどのような凡例がありますか？	アクセスと権限を分析する際、評価プロセスの一部として凡例が表示されます。以下は凡例です: • [合格] アクセスが許可されました • [ブロック済み] アクセスが拒否されました • [スキップ済み] 評価されませんでした • [未定義] ルールが見つかりませんでした
アクセス結果のアラートアイコンは何を意味しますか？	ステータスのアラートアイコンは ACL にスクリプトが存在することを示します。ハイライト表示された ACL を確認して、最終的なアクセス権を把握します。これらの制御を評価する方法の詳細を把握し、アクセスを決定するロジックを確認するには、「Access Analyzer のデバッグログ」を参照してください。
IAccesshandler とは何ですか？	プラットフォーム上の非表示のソースコードを使用する内部システムチェック。これは変更できないシステムセキュリティチェックです。**IAccessHandler** は、ACL を評価せずにリソースへのアクセスを許可または拒否できます。 この **IAccessHandler** が無視されると、ACL が評価されます。どのような方法でも **IAccessHandler** チェックは変更できません。たとえば、**IAccessHandler** 実装は読み取り専用アクセスなどのアプリケーションリソースのアクセスチェックに使用されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

よく寄せられる質問 (続く)

質問	説明
データフィルターとは何ですか？	データフィルターは、インスタンスの既存のアクセス制御ルール (ACL) と連携して機能するように設計されたアクセス制御の形式です。
ACL ルールとは何ですか？	アクセス制御リスト (ACL) のルールは、ユーザーがデータを操作する前に、まず要件のセットをユーザーに要求することで、データへのアクセスを制限します。

結果に影響する可能性がある、ユーザーに対して時間制限付きロールの割り当てが見つかりました。ユーザーに割り当てられている時間制限付きロールは、ここで確認できます。

ユーザーレコードの比較

以下は、アクセスアナライザーのユーザーレコードの比較機能を使用する際によく寄せられる質問の一部です。

よく寄せられる質問

質問	説明
[詳細]タブで結果を読むにはどうすればよいですか?	[詳細] タブには、ユーザー 1 とユーザー 2 に関連付けられたメタデータが表示されます
ユーザーにロールを付与するには?	[ユーザー] タブで、ユーザーに付与する必要があるロールを確認し、そのロールを割り当てることができます。
グループにユーザーを追加するにはどうすればよいですか?	[グループ] タブで、ユーザーを追加する必要があるグループを確認し、ユーザーをグループに追加できます。
[差異のみを表示] とは何ですか?	[相違点のみ表示] チェック ボックスをオンにすると、ユーザー 1 とユーザー 2 の間で異なるロールまたはグループのみが表示されます。

ユーザーアクセスの比較

以下は、アクセスアナライザーのユーザーアクセスの比較機能を使用する際によく寄せられる質問の一部です。

よく寄せられる質問

質問	説明
アクセス制御比較ページで結果を読む方法は?	アクセス制御比較ページには、さまざまな ACL 操作の評価ステータスが表示されます。
評価状態にはどのようなものがありますか?	ユーザー間でアクセス制御を比較する場合、さまざまな評価状態は次のとおりです。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

よく寄せられる質問 (続く)

質問	説明
	• 合格 • ブロック済み
差異のみの表示とは何ですか?	[相違点のみ表示] チェック ボックスをオンにすると、ユーザー 1 とユーザー 2 の間で異なる操作評価状態のみが表示されます。
ACL 操作はどのように評価されますか?	アクセス制御リスト (ACL) は、アクセス制御リスト (ACL) のルールであり、ユーザーがデータを操作する前に、まず要件のセットをユーザーに要求することで、データへのアクセスを制限します。ACL 内では、次の階層が評価されます。 • ロール • セキュリティ属性 • 条件 • スクリプト
表示されているロール階層ページで結果を読むにはどうすればよいですか?	表示されているロール階層ページには、ユーザー 1 とユーザー 2 に割り当てられているロールが表示されます。特定の ACL 操作でユーザーに必要なロールを理解できます。
ユーザーの詳細を確認するにはどうすればよいですか?	あなたは選ぶことができます ユーザー (ノード) > その他のアクション > ユーザーの表示 ユーザーの詳細を知るための詳細。
ロールの詳細を確認するにはどうすればよいですか?	あなたは選ぶことができます ロール (ノード) > その他のアクション > 表示ロール ロールの詳細を確認します。
ロールがアクセスできるリソースの詳細を確認するにはどうすればよいですか?	あなたは選ぶことができます ロール (ノード) > その他のアクション > ロールがアクセスできるすべてのリソースの表示 ロールがアクセスできるリソースを把握するため。
グループの詳細を確認するにはどうすればよいですか?	あなたは選ぶことができます グループ (ノード) > その他のアクション > グループを表示 グループの詳細を確認します。

Access Analyzer のデバッグログ

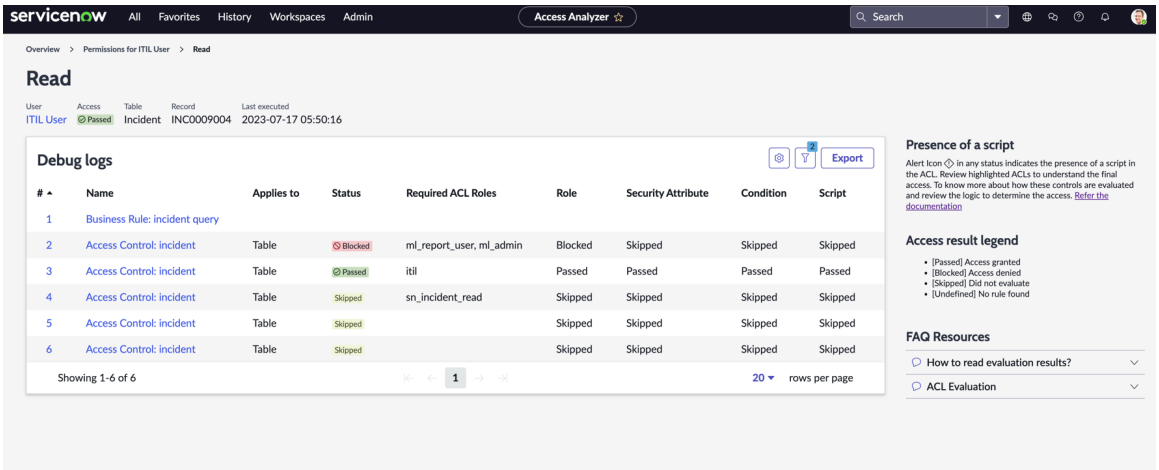
デバッグログには、アクセス結果の選択操作の詳細が表示されます。

デバッグログのフィールド

Access Analyzer のデバッグログには、選択した操作に関する情報が表示され、操作に関連付けられた権限、ビジネスルール、および ACL を把握できます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



デバッグログのフィールドとその説明は次のとおりです。

デバッグログ

フィールド	説明
名前	ビジネスルールまたは ACL に関する詳細。ACL のビジネスルールを選択すると、詳細を確認できます。
適用先	フィールド、レコード、またはテーブルレベルでの ACL の適用に関する詳細。
ステータス	関連するロールと権限の ACL のステータス
ACL が必要 (Requires ACL)	フィールド、レコード、またはテーブルへのアクセスに必要なロール
ロール	アクセス制御でブロック中、合格中、スキップされているロールに関する詳細。
セキュリティ属性	アクセス制御でブロック、合格、スキップされるセキュリティ属性に関する詳細。
条件	アクセス制御に対するブロック済み、合格、スキップ済みの条件に関する詳細
スクリプト	アクセス制御でブロック、合格、スキップされているスクリプトに関する詳細。
カスタマイズ済み	アクセス制御用にカスタマイズされた ACL の詳細 (存在する場合)。
アプリケーション	アプリケーションのステータス。グローバルまたはストア

評価階層

選択したユーザー、グループ、ロールの権限は、次の階層で評価されます。

- ビジネスルール：ビジネスルールとは、レコードが表示、挿入、更新、または削除されるとき、またはテーブルに対してクエリが実行されるときに実行する、サーバー側スクリプトです。
- アクセスハンドラー：プラットフォーム上の非表示のソースコードを使用する内部システムチェックです。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- データフィルタリング:データフィルターは、インスタンスの既存のアクセス制御ルール (ACL) と連携して機能するように設計されたアクセス制御の形式です。データ フィルターは読み取り操作のみをサポートします。
- アクセス制御リスト (ACL)：アクセス制御リスト (ACL) のルールは、まず要件のセットをユーザーに要求し、その後でユーザーとやり取りできるようにすることで、データへのアクセスを制限します。ACL 内では、次の階層が評価されます。
  - ロール
  - セキュリティ属性
  - 条件
  - スクリプト

アクセス制御リストの評価

操作の ACL は、次の順序で評価されます。

- ロール
- セキュリティ属性
- 条件
- スクリプト

スクリプトの存在

ステータスのアラートアイコンは ACL にスクリプトが存在することを示します。ハイライト表示された ACL を確認して、最終的なアクセス権を把握します。

注:
Access Analyzer のクエリでは、ビジネスルールが最初に実行され、次にアクセス制御リストが実行されます。

実行順序

さまざまなシナリオでのアクセス結果の実行順序は次のとおりです。

- 継承された **ACL** またはワイルドカード **ACL** の存在：実行順序では、継承された ACL が最初に評価され、次にワイルドカード ACL が評価されます。
- **1** つの **ACL** が渡され、他の **ACL** がスキップされます:権限の実行および評価中に、一方の ACL が合格すると、もう一方の ACL の実行と評価がスキップされます。ID のフィールド、レコード、またはテーブルにアクセスするには、選択した操作の全体的な権限に 1 つの ACL が必要であるためです。
- フィールドレベルの **ACL** とテーブルレベルの **ACL** の実行：実行では、ID のアクセスを分析するときに詳細な結果を提供するため、フィールドレベルの ACL が最初に実行され、次にテーブルレベルの ACL が実行されます。
- スクリプト化された **ACL** が存在する場合の評価：スクリプトが存在する場合、ACL 内のスクリプトを示すアラートアイコンとともに操作の全体的なアクセスが合格します。

Global Identity

Global Identity は、複数のインスタンス間で一意のユーザーを識別できるようにする ServiceNow® 製品です。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

Global Identity は、複数の ServiceNow® インスタンスでユーザー、その属性、およびその他の基盤データを複数の ServiceNow インスタンス間で管理するのに役立ちます。

詳細 フェデレーション ID

フェデレーション ID の主な機能とビジネス価値について学びます。

フェデレーション ID へのアクセス

フェデレーション ID にアクセスします。

ID フィールドの更新

フェデレーション ID を更新して設定します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フェデレーション ID の探索

ユーザー名とメールに基づいて複数のインスタンス間でユーザーを特定し、インスタンス全体でユーザーに一意の ID (フェデレーション ID) を提供します。

フェデレーション ID は、複数の ServiceNow® インスタンス間でユーザーを識別するために使用されます。フェデレーション ID に基づいてユーザーを識別し、複数のインスタンス間で正確なユーザー数を判断できます。詳細については、フェデレーション ID を参照してください。

注:
ユーザー名はフェデレーション ID を生成するために必要です。

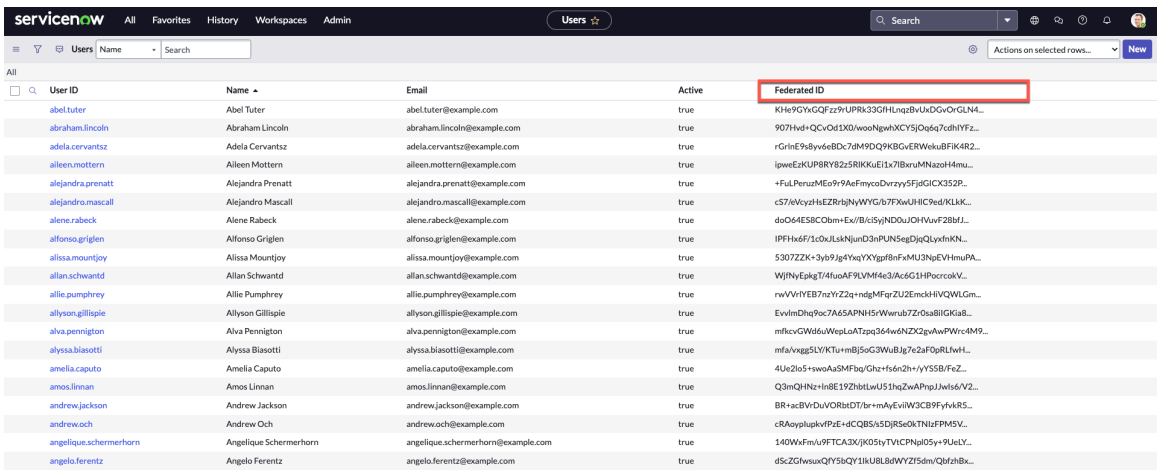
フェデレーション ID は、ServiceNow® インスタンス全体でハッシュ関数を使用する ID の一意の識別子です。

インスタンス全体でユーザーの [ユーザー **ID**] と [メール] を使用することで、フェデレーション ID が作成され、sys_user テーブルに表示されます。

Washington DC リリースにアップグレードすると、Federated ID Generation (com.glide.identity.globalid) プラグインがすべてのインスタンスに自動インストールされます。

注:

- ユーザー名はフェデレーション ID を生成するために必要です。
- ユーザー名とメールはフェデレーション ID を生成するためにデフォルトで使用されます。要件に基づいてフェデレーション ID を生成するためのフィールドを更新するには、「ID フィールドの更新」を参照してください。
- 構成を更新するには、**Iamsync_admin** ロールが必要です。
- ユーザー名とメールが重複しているユーザーがいる場合、フェデレーション ID は 1 人のユーザーに対してのみ生成されます。ユーザー名が null または空の場合、フェデレーション ID は null です。



プラグインをインストールした後のスキーマの変更は次のとおりです。

- sys_user テーブルに新しい列フェデレーション ID が作成されます。
- 新しいテーブル iamsync_type には、sys_user テーブルのデフォルト構成が自動的に入力されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フェデレーション ID は sys_user テーブルと sys_user テーブルを拡張するすべてのテーブルでのみサポートされています。

Washington DC リリースにアップグレードすると、Federated ID Generation (com.glide.identity.globalid) プラグインがすべてのインスタンスに自動インストールされます。

フェデレーション ID 基準へのアクセス

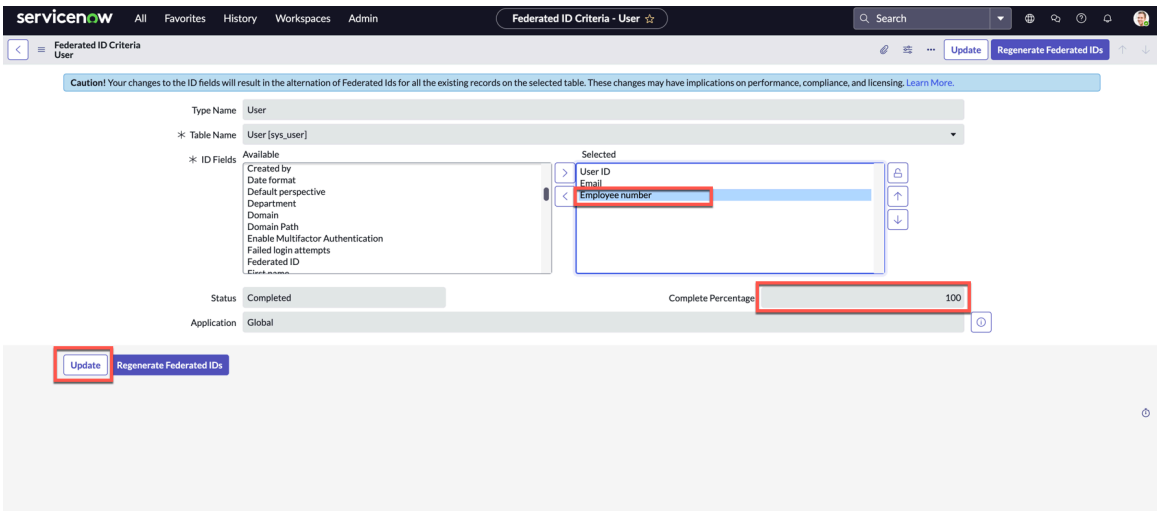
フェデレーション ID 基準にアクセスして、フェデレーション ID の生成に使用された ID フィールドについて確認します。

始める前に
必要なロール：iamsync_admin

手順

1. 移動先 すべて > フェデレーション **ID** を管理 > フェデレーション **ID** 基準.
2. [フェデレーション ID 基準 (Federated ID Criterias)] ページには、次の詳細を含むレコードが表示されます。
   - タイプ名：ユーザー
   - テーブル名：ユーザー **[sys_user]**
   - ID フィールド：user_name、email (フェデレーション ID の生成に使用されるデフォルトフィールド)。
   - ステータス：完了 (フェデレーション ID 生成ステータス)。利用可能なステータス：準備完了、実行中、完了、エラー

   注:
   - ユーザー名はフェデレーション ID を生成するために必要です。
   - ユーザー名とメールはフェデレーション ID を生成するためにデフォルトで使用されます。



注:
ID フィールドのみを更新して既存のレコードの新しいフェデレーション ID を生成できます。詳細については、「ID フィールドの更新」を参照してください。

ID フィールドの更新

ID フィールドを更新し、更新されたフィールドに基づいてフェデレーション ID を再生成します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

始める前に
必要なロール：iamsync_admin

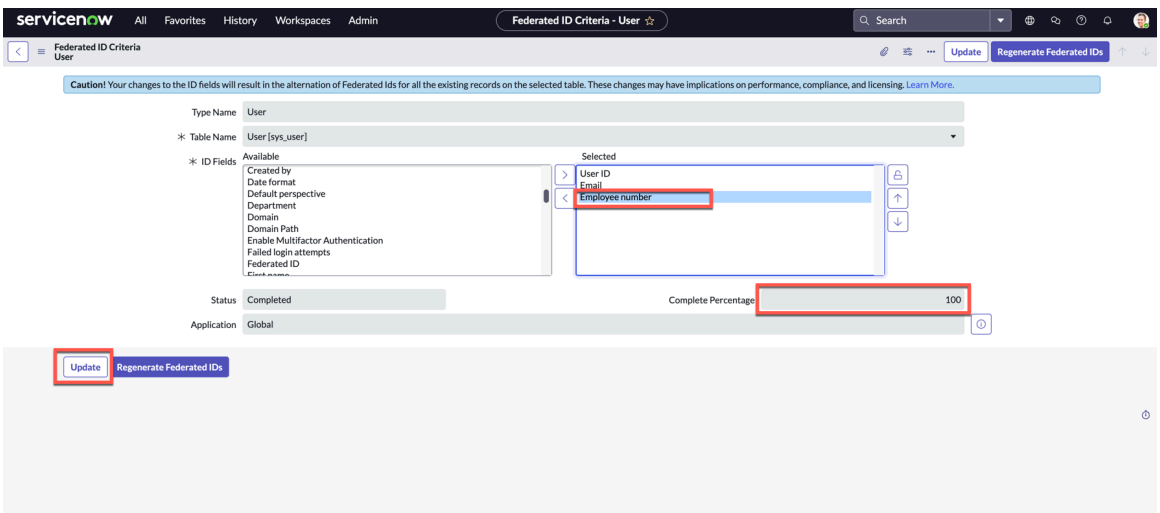
> **注:**
> ID フィールドを変更すると、選択したテーブルのすべての既存レコードのフェデレーション ID が変更されます。これらの変更は、パフォーマンス、コンプライアンス、およびライセンスに影響を与える可能性があります。

手順

1. 移動先 すべて > フェデレーション **ID** を管理 > フェデレーション **ID** 基準.
2. タイプ名 (ユーザー) を選択します。
3. [フェデレーション ID 基準ユーザー (Federated ID Criteria User)] ページで、矢印ボタンを使用して [利用可能] から [選択済み] に追加する新しい ID フィールドを選択します。

   例：[従業員番号]

   > **注:**
   > - ユーザー名はフェデレーション ID を生成するために必要です。
   > - ユーザー名とメールはフェデレーション ID を生成するためにデフォルトで使用されます。
   > - ユーザー名とメールが重複しているユーザーがいる場合、フェデレーション ID は 1 人のユーザーに対してのみ生成されます。ユーザー名が null または空の場合、フェデレーション ID は null です。



   選択した [従業員番号] は、フェデレーション ID を生成するための別の属性になります。

4. [更新] を選択してフェデレーション ID を生成します。

   > **注:**
   > 最初に [更新] を選択し、別の更新を開始する前に完了率 (100) を確認します。

   ステータスの割合は、インスタンス全体のすべての ID のフェデレーション ID の生成を示します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注:

- 前の更新ジョブが完了するまで、フィールドを変更しないでください。
- 更新されるフィールドは文字列タイプである必要があります。
- ID フィールドとして選択できないフィールドは次のとおりです。
  - システムレベルフィールド
  - Edge Encryption フィールド
  - パスワードフィールド

5. sys_user テーブルに移動して、ID フィールドの更新によって生成された新しいフェデレーション ID を表示します。

注:
XML インポート、低レベルのデータベース更新を介してユーザーが作成または更新され、インスタンスが正しく機能しない場合は、[フェデレーション **ID** を再生成 **(Regenerate Federated IDs)]** を選択します。[フェデレーション **ID** を再生成 **(Regenerate Federated IDs)]** を選択すると、現在の ID フィールド基準を使用して、すべてのユーザーの ID が再生成されます。

ID とアクセスの監査

ID およびアクセス監査を使用して、ユーザー、グループ、ロール、および ACL に加えられた変更を把握します。

自動翻訳

探索

ID とアクセスの監査の機能とビジネス価値について説明します。

構成

ID とアクセスの監査を構成する方法を理解します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

監査結果	
ID とアクセスの監査の結果を表示します。	

ID およびアクセス監査の詳細

ID およびアクセス監査を使用して、ユーザー、グループ、ロール、および ACL に加えられた変更を把握します。

IDとアクセス監査は、ユーザーアカウント、グループ、およびロールで誰が何を、どこで、いつ変更したかに関する重要な情報を理解するのに役立ちます。

悪意のあるユーザーを検出し、インスタンス内の ServiceNow® 異常なアクティビティを追跡し、アクセスの変更を追跡できるコンプライアンス標準に準拠するのに役立ちます。

Identity and Access Audit (Identity Security Audit) はプラグイン (com.glide.security.audit) で、自動インストールされます。

監査機能は、glide.identity.security.audit.enabled システムプロパティを切り替えることでオンまたはオフにできます。デフォルトでは、このプロパティは true に設定されています。

ID とアクセスの監査により、次のことが可能になります。

- 過去 30 日間にユーザー、グループ、ロール ACL 属性、ロールメンバーシップ、グループメンバーシップ、および ACL ロールに対して行われた変更を表示します。
- インスタンスの変更を追跡します ServiceNow 。
- 潜在的なセキュリティおよび規制上のリスクを軽減するのに役立ちます。
- 組織内のさまざまなグループの監査人によるコンプライアンスを実証します。
- 組織が、ユーザーグループの可視性の欠如とロールの変更に関連する脅威に対して脆弱ではないことを示します。

ID アクセスと監査のユーザーペルソナ

ID とアクセスの監査のさまざまなユーザー ペルソナを次に示します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

- 管理者:監査レコードと構成を表示します。
- セキュリティ管理者:次の監査証跡を表示します。構成を変更して、特定のテーブルの監査を有効または無効にしたり、監査対象のフィールドを変更したりします。

監査テーブル

次のテーブルは、[ID とアクセスの監査] を使用して監査できます。

- グループ [sys_user_group]
- ロール [sys_user_role]
- アクセス制御 [sys_security_acl]
- ユーザー [sys_user]
- グループロール [sys_group_has_role]
- ユーザーロール [sys_user_has_role]
- アクセスロール [sys_security_acl_role]
- 含まれているロール [sys_user_role_contains]
- グループメンバー [sys_user_grmember]

ID およびアクセス監査のモジュール

ID とアクセスの監査には、インスタンスに次のモジュールがあります ServiceNow 。

モジュール	説明
監査結果	インスタンスで ServiceNow 発生した監査を表示します。
テーブルとフィールドの設定	ID とアクセスの監査で利用可能なフィールドを使用して、システムテーブルとフィールドを構成します。
保存期間を構成	監査対象データの保持期間を設定します。設定できる最大期間は 30 日間です。
ユーザー記録	ユーザーの監査を表示します。
グループ記録	グループの監査を表示します。
ロール記録	ロールの監査を表示します。
ACL 記録	ACL の監査を表示します。

監査結果

インスタンスで ServiceNow® 発生した監査を表示します。

監査結果には ServiceNow 、インスタンス内のユーザー、グループ、ロール、および ACL に加えられた変更が表示されます。

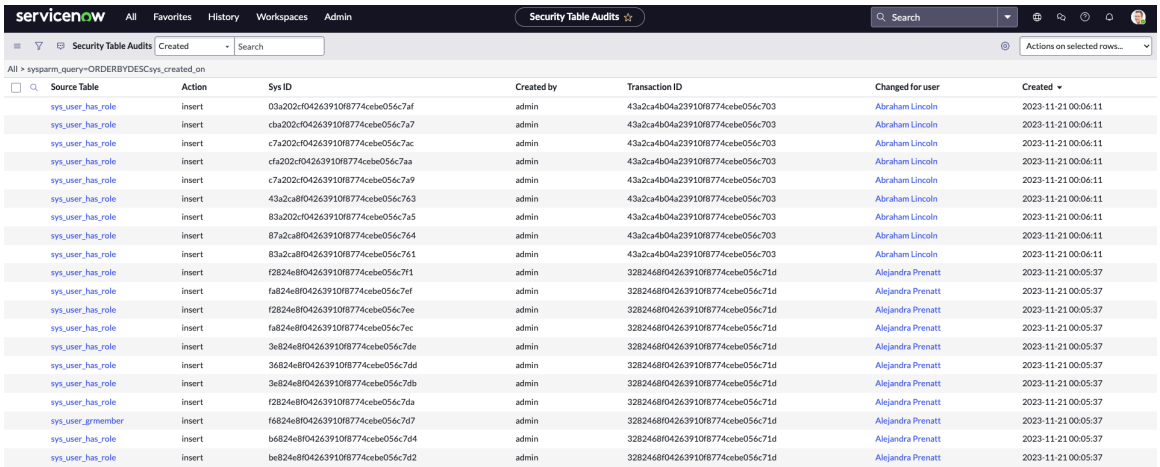
監査結果にアクセスするには、次に移動します すべて > システムセキュリティ > **ID** とアクセスの監査 > 監査結果. [セキュリティテーブルの監査] ページに次の情報が表示されます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

セキュリティテーブル監査

列名	説明
ソーステーブル	監査が発生したソーステーブルの詳細。
アクション	監査アクションについて説明します。
Sys_id	監査対象レコードのsys_idに関する詳細。
作成者	作成された監査の詳細。
トランザクション ID	実行された特定の監査のすべてのアクションを表す一意の ID。
変更依頼者	監査が実行されたときのユーザーの名前。
作成日時	監査が実行された日時。



ユーザー記録

インスタンス内の ServiceNow® ユーザーの監査を表示します。

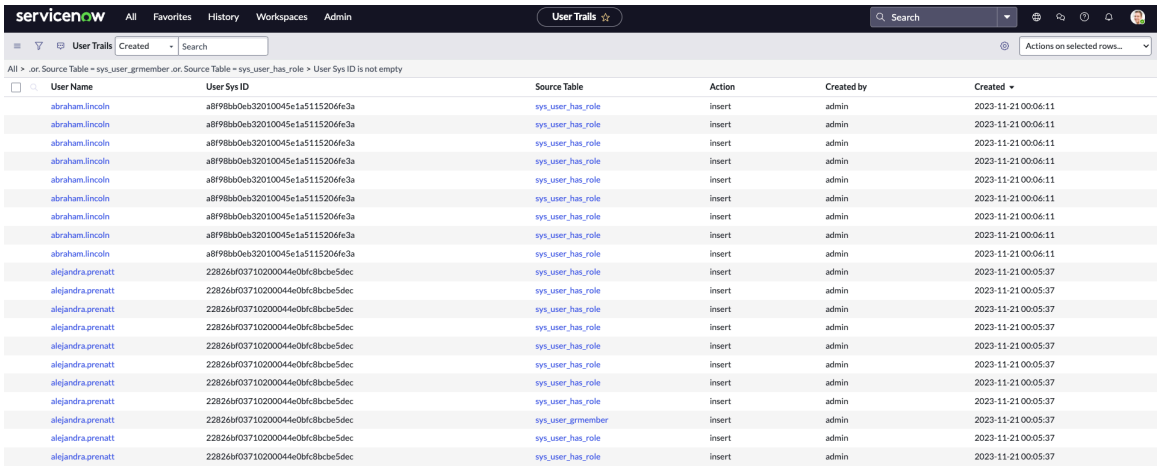
ユーザー証跡には、ユーザーの ID 属性の変更、ロールメンバーシップの変更、およびグループメンバーシップの変更が表示されます。

ユーザー証跡にアクセスするには、次に移動します。 すべて > システムセキュリティ > **ID** とアクセスの監査 > ユーザー記録. 「ユーザー証跡」ページに次の情報が表示されます。

ユーザー記録

ユーザー名	ユーザーの名前。
ユーザー Sys ID	監査済みレコードのユーザー sys_idに関する詳細。
ソーステーブル	監査が実行されたソーステーブルの詳細。
アクション	監査アクションについて説明します。
作成者	変更を加えたユーザー。
作成日時	監査が実行された日時。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



グループ記録

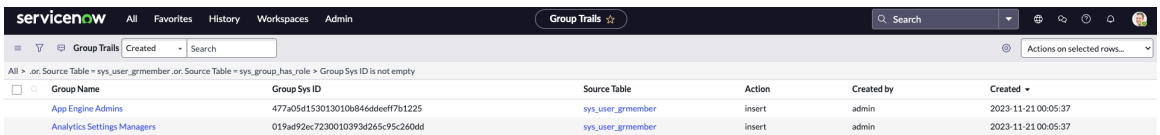
インスタンス内の ServiceNow® グループの監査を表示します。

グループ証跡には、グループの属性の変更、メンバーシップの変更、およびロールの変更が表示されます。

グループ証跡にアクセスするには、次に移動します。 すべて > システムセキュリティ > **ID** とアクセスの監査 > グループ記録. 「グループ証跡」ページに次の情報が表示されます。

グループ記録

グループ名	グループの名前。
グループ Sys ID	監査対象レコードのグループsys_idに関する詳細。
ソーステーブル	監査が実行されたソーステーブルに関する詳細。
アクション	監査アクションについて説明します。
作成者	変更を加えたユーザー。
作成日時	監査が実行された日時。



ロール記録

インスタンス内の ServiceNow® ロールの監査を表示します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

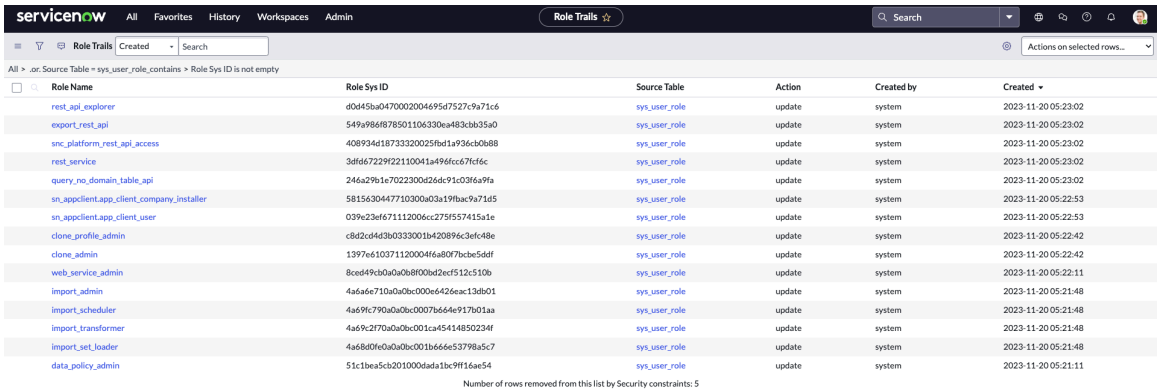
自動翻訳

ロール証跡には、ロールの属性の変更と親子関係の変更が表示されます。

ロール証跡にアクセスするには、次に移動します。 すべて > システムセキュリティ > **ID** とアクセスの監査 > ロール記録. 「ロール証跡」ページに次の情報が表示されます。

ロール記録

ロール名	ロールの名前。
ロール Sys ID	監査対象レコードのロールsys_idに関する詳細。
ソーステーブル	監査が実行されたソーステーブルに関する詳細。
アクション	監査アクションについて説明します。
作成者	変更を加えたユーザー。
作成日時	監査が実行された日時。



ACL 記録

インスタンス内の ServiceNow® ACL の監査を表示します。

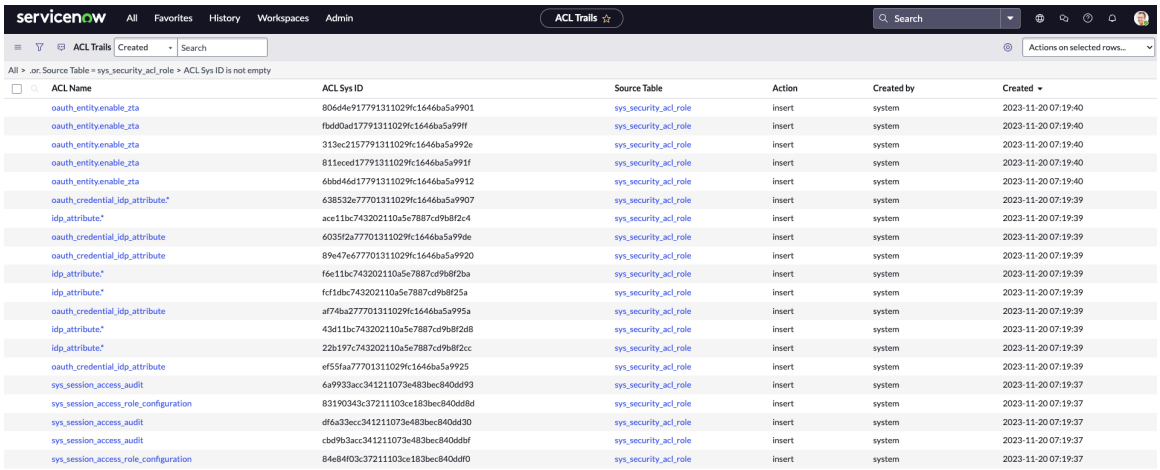
ACL 記録には、ACL の属性の変更と必要なロール関係の変更が表示されます。

ACL 記録にアクセスするには、次に移動します。 すべて > システムセキュリティ > **ID** とアクセスの監査 > **ACL** 記録. [ACL 記録] ページに次の情報が表示されます。

ACL 記録

ACL 名	ACL の名前。
ACL Sys ID	監査対象レコードの ACL sys_idに関する詳細。
ソーステーブル	監査が実行されたソーステーブルの詳細。
アクション	監査アクションについて説明します。
作成者	変更を加えたユーザー。
作成日時	監査が実行された日時。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



セキュリティ監査可能フィールド

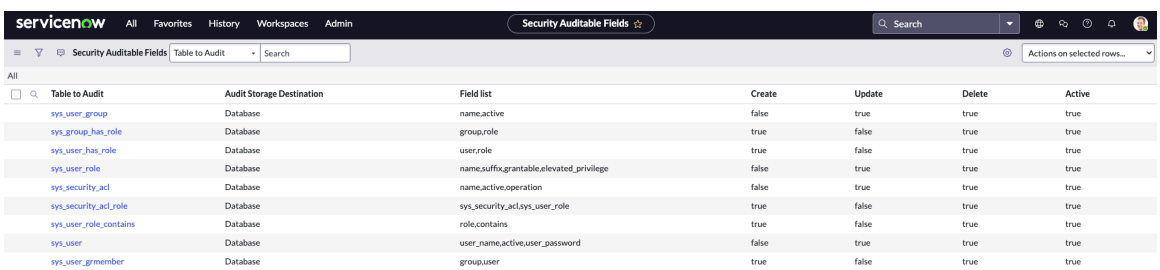
インスタンスで ServiceNow® 監査されるテーブルおよびフィールド レベルの詳細を表示します。

[セキュリティ監査可能フィールド] には、インスタンスで ServiceNow 監査されるテーブルとフィールドの詳細が表示されます。

[セキュリティ監査可能フィールド] ページにアクセスするには、次の場所に移動します。 すべて > システムセキュリティ > **ID** とアクセスの監査 > テーブルとフィールドを構成. [セキュリティ監査可能フィールド] ページに次の情報が表示されます。

セキュリティ監査可能フィールド

列名	説明
監査するテーブル	監査対象のテーブルの詳細。
監査ストレージの保存先	監査の詳細が格納される宛先の詳細。
フィールドリスト	監査は、リストで指定されたフィールドに対して実行されます。
作成	作成操作に関連する変更を監査します。
更新	更新操作に関連する変更を監査します。
削除	削除操作に関連する変更を監査します。
アクティブ	テーブルの構成がアクティブな場合にのみ監査します。



次のテーブルは、ID とアクセスの監査を使用して監査できます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

- グループ [sys_user_group]
- ロール [sys_user_role]
- アクセス制御 [sys_security_acl]
- ユーザー [sys_user]
- グループロール [sys_group_has_role]
- ユーザーロール [sys_user_has_role]
- アクセスロール [sys_security_acl_role]
- 含まれているロール [sys_user_role_contains]
- グループメンバー [sys_user_grmember]

テーブルとフィールドの構成

ユーザー、グループ、ロール、および ACL に加えられた変更を把握するための ID およびアクセス監査。

始める前に

必要なロール：security_admin

ID とアクセス監査のテーブルとフィールドを設定するには、ロールをセキュリティ管理者に昇格させる必要があります。

次のテーブルを監査用に構成できます。

- グループ [sys_user_group]
- ロール [sys_user_role]
- アクセス制御 [sys_security_acl]
- ユーザー [sys_user]
- グループロール [sys_group_has_role]
- ユーザーロール [sys_user_has_role]
- アクセスロール [sys_security_acl_role]
- 含まれているロール [sys_user_role_contains]
- グループメンバー [sys_user_grmember]

注:
テーブルに設定できるフィールドを理解するには、「」を参照してください ID アクセスと監査でサポートされているフィールドとサポートされていないフィールド。

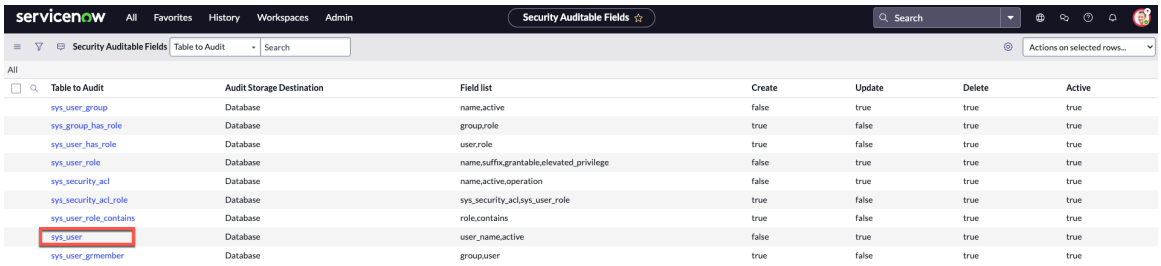
手順

1. 移動先 すべて > システムセキュリティ > **ID** とアクセスの監査 > テーブルとフィールドを構成.
2. フィールドを監査するテーブルを選択します。

   たとえば、**sys_user** などです。

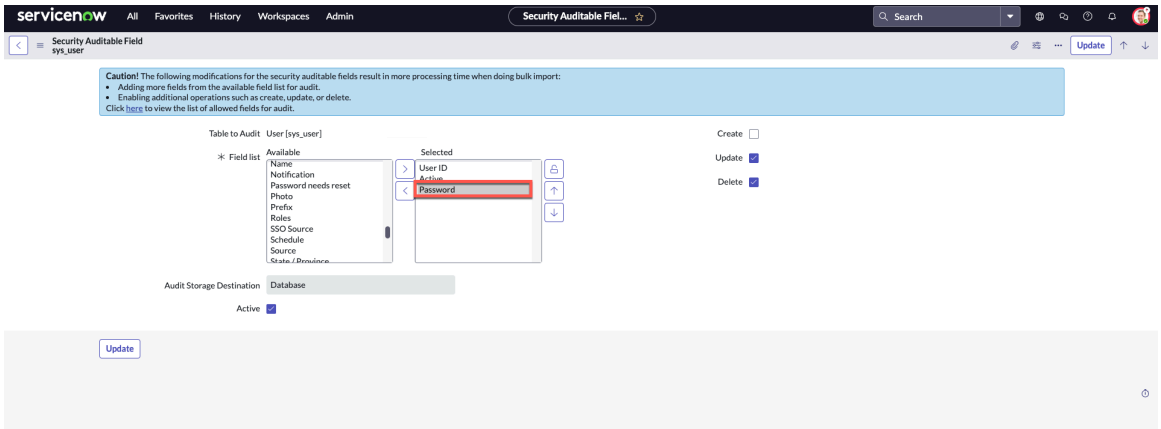
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



3. 監査するフィールドを追加します。

たとえば、 パスワード。

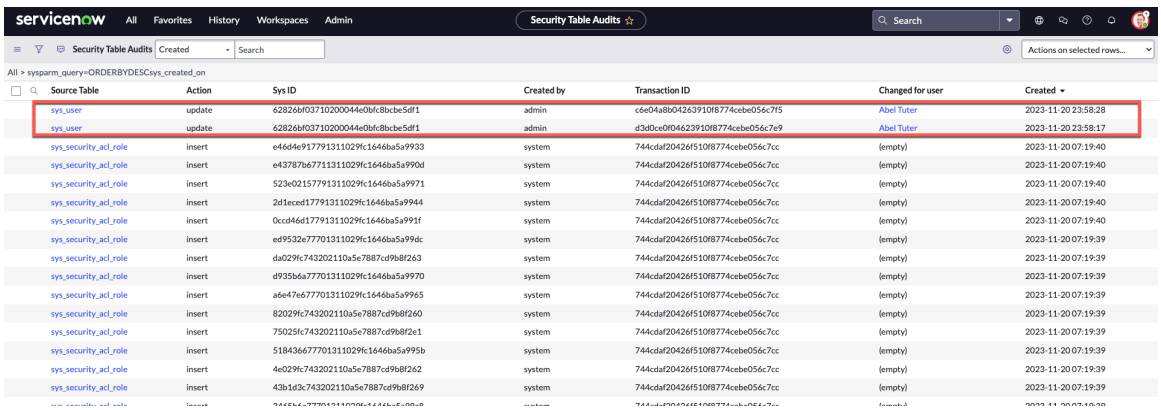


注:
セキュリティ監査可能フィールドを次に変更すると、一括インポート時の処理時間が長くなります。

- 監査に使用可能なフィールド リストからさらにフィールドを追加します。
- 作成、更新、削除などの追加操作を有効にします。

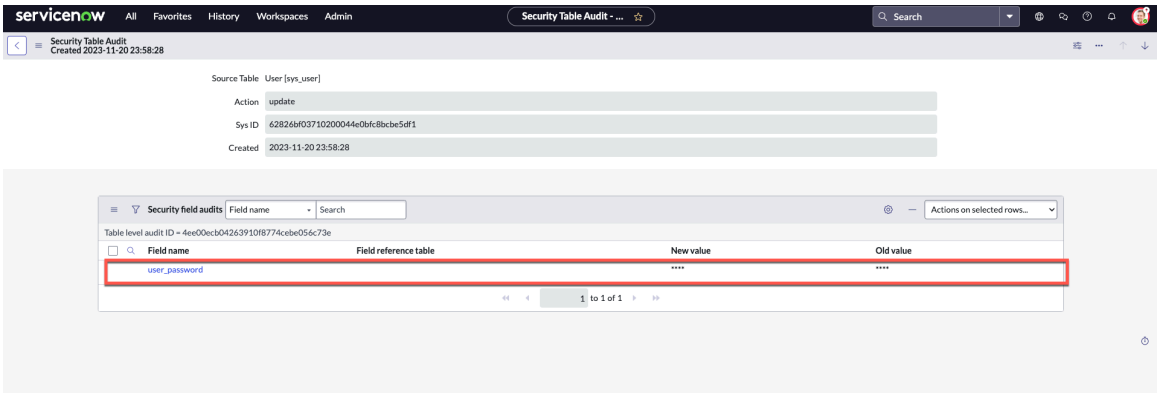
4. レコードを更新します。

パスワードフィールドを変更すると、セキュリティテーブル監査に新しいレコードが追加されます。この例では、監査によりユーザー **Abel Tuter** の変更されたパスワードフィールドが表示されます。



© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

作成したレコードを選択すると、変更内容の詳細が表示されます。



保存期間を構成

ID とアクセス監査の保持期間を構成します。

始める前に

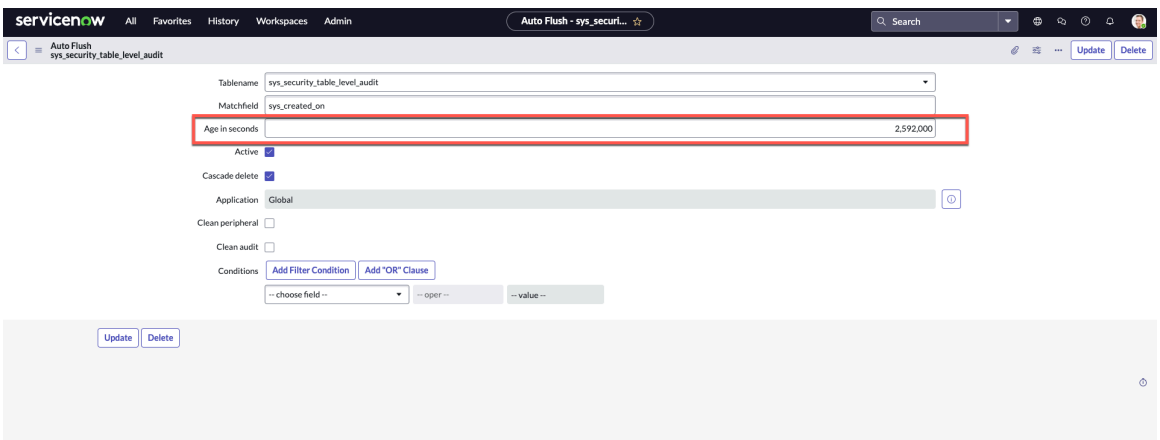
必要なロール：管理者

手順

1. 移動先 すべて > システムセキュリティ > **ID** とアクセスの監査 > 保存期間を構成.

2. フォームで経過時間を秒単位で変更できます。

> **注:**
> ID とアクセスの監査の最大日数は 30 日 (2,592,000 秒) です。



3. レコードを [保存] または [更新] します。

ID アクセスと監査でサポートされているフィールドとサポートされていないフィールド

監査でサポートされているフィールドとサポートされていないフィールドのリスト。

監査フィールドの検証では、セキュリティフィールド監査構成 (sys_sec_field_audit_config) テーブルのfield_listで一部のフィールドが選択されなくなります。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

監査でサポートされているフィールドまたはサポートされていないフィールド

テーブル	フィールドがサポート対象またはサポート対象外
すべてのテーブル	サポートされていないフィールド: • 作成日 (sys_created_on) • 作成者 (sys_created_by) • 更新者 (sys_updated_by) • 更新日 (sys_updated_on)
ユーザーにロールがある **(sys_user_has_role)**	サポートされているフィールド: • ユーザー • ロール • 継承 • カウント
ユーザー **(sys_user)**	サポートされていないフィールド: • 前回のログイン (last_login) • 前回のログイン時間 (last_login_time) • 前回のログインデバイス (last_login_device) • マルチファクター認証 (enable_multifactor_authn) を有効にする • デフォルトの視点 (default_perspective) • カレンダー統合 (calendar_integration) • フェデレーション ID (federated_id) • パスワードのリセットが必要 (password_needs_reset) • 失敗した試行 (failed_attempts) • 前回のパスワード (last_password) • LDAP サーバー (ldap_server) • ロックアウト (locked_out) • 通知 (通知) • ロール (ロール) • ドメイン (sys_domain) • ドメインパス (sys_domain_path) • 時間形式 (time_format) • ハッシュ化されたユーザー ID (hashed_user_id)

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

監査でサポートされているフィールドまたはサポートされていないフィールド (続く)

テーブル	フィールドがサポート対象またはサポート対象外
	• クラス名 (sys_class_name) • モッズカウント (sys_mod_count)

ID センター

ID ベースのリスクとセキュリティギャップを監視および管理し、最小限に抑えることができます。

探索

ID センターの機能とビジネス価値について説明します。

アクティブ化

ID センターをアクティブ化する方法を理解します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

管理者の ID 測定基準

権限がどのように評価されるかを把握します。

ユーザー向け ID センター

Access Analyzer に関するよくある質問の詳細を確認します。

自動翻訳

ID センターの概要

ID センターは、ユーザーの属性、アクセス、デバイス、ログイン履歴、セキュリティアクティビティなどのコレクションです。

ID センターは、ID ベースのリスクとセキュリティギャップを監視および管理し、最小限に抑える機能を提供します。

ID センターでは、ServiceNow の 1 つの場所で、ID ベースのリスクとセキュリティギャップを監視および管理し、最小限に抑えることができます。

ID センターを有効にするには、Identity Center (com.snc.identity_center) プラグインをインストールします。エンドユーザーは ID センターを使用して、ID センターでアクティブなセッション、ログイン履歴、および信頼できるデバイスの詳細を表示できます。詳細については、「ユーザー向け ID センター」を参照してください。

ID センターのアクティブ化

ID センターの場合、Identity Center (com.snc.identity_center) プラグインをインストールします。

始める前に
必要なロール：admin

手順

1. 移動先 すべて > システムアプリケーション > 利用可能なすべてのアプリケーション > すべて.
2. フィルター基準と検索バーを使用して Identity Center (com.snc.identity_center) プラグインを検索します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

名前または ID でプラグインを検索できます。プラグインが見つからない場合は、ServiceNow 担当者から要求する必要があります。

3. [インストール] を選択して、[プラグインをアクティブにする] ダイアログボックスで、[アクティブ化] をクリックします。

> **注:**
> ドメイン分離と代理管理者がインスタンスで有効になっている場合、管理ユーザーはグローバルドメインに含まれている必要があります。それ以外の場合、次のエラーが表示されます： 別の操作が実行されているため、アプリケーションのインストールは利用できません：<プラグイン名> のプラグインの有効化。

ユーザー向け ID センター

ID センターを使用して、アクティブなセッション、ログイン履歴、および信頼できるデバイスの詳細を表示します。

ID センターは、ユーザーの属性、デバイス、ログイン履歴、セキュリティアクティビティなどのコレクションです。すべてのデータを 1 つのウィンドウで表示し、追加のセキュリティコントロールと通知機能を提供します。

ID センターを使用して、アクティブなセッション、ログイン履歴、および信頼できるデバイスの詳細を表示できます。

ユーザー向けの ID センターにアクセスするには、次のいずれかに移動します。

- で Now Platform、移動先 すべて > セルフサービス > プロファイル をクリックし、[関連リンク] セクションで [**ID** センターを表示] を選択します。

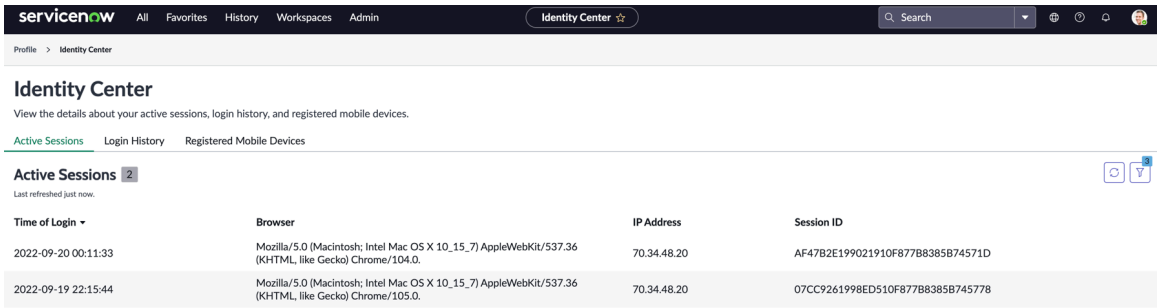
> **注:**
> インスタンスヘッダーで自分のユーザー名を選択して、プロファイルにアクセスすることもできます。

- Now Support でプロファイルを選択し、ページの下部にある **[ID** センターを表示] を選択します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

[ID センター] ページが次のように表示されます。



ID センターには次のタブがあります。

- アクティブセッション
- ログイン履歴
- 登録済みモバイルデバイス

これらのタブを選択すると、ブラウザ、IP アドレス、セッション関連情報、ログイン情報、登録済みモバイルデバイスなどの詳細を表示できます。

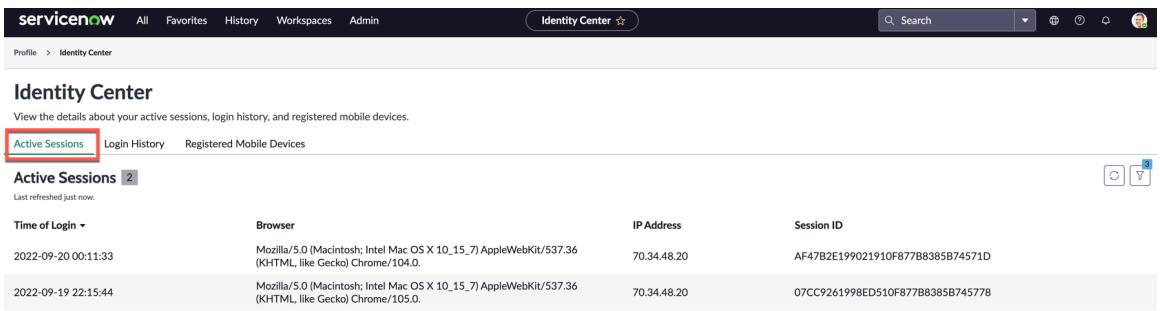
アクティブセッションの表示

ユーザーセッションに関する情報を表示します。

アクティブセッションは、さまざまなブラウザーまたはデバイスを使用して、現在の ServiceNow® インスタンスで開かれているセッションです。

ID センターの [アクティブセッション] タブは、ブラウザー、IP アドレス、およびセッション ID に基づいてセッションを識別するのに役立ちます。この情報を使用して、セッションの延長や終了などの必要なアクションを取ることができます。

この情報を使用すると、セッションが本物かどうか、またはセキュリティ上の問題が発生していないことを判断できます。



ログイン履歴の表示

ログイン履歴の詳細を提供します。

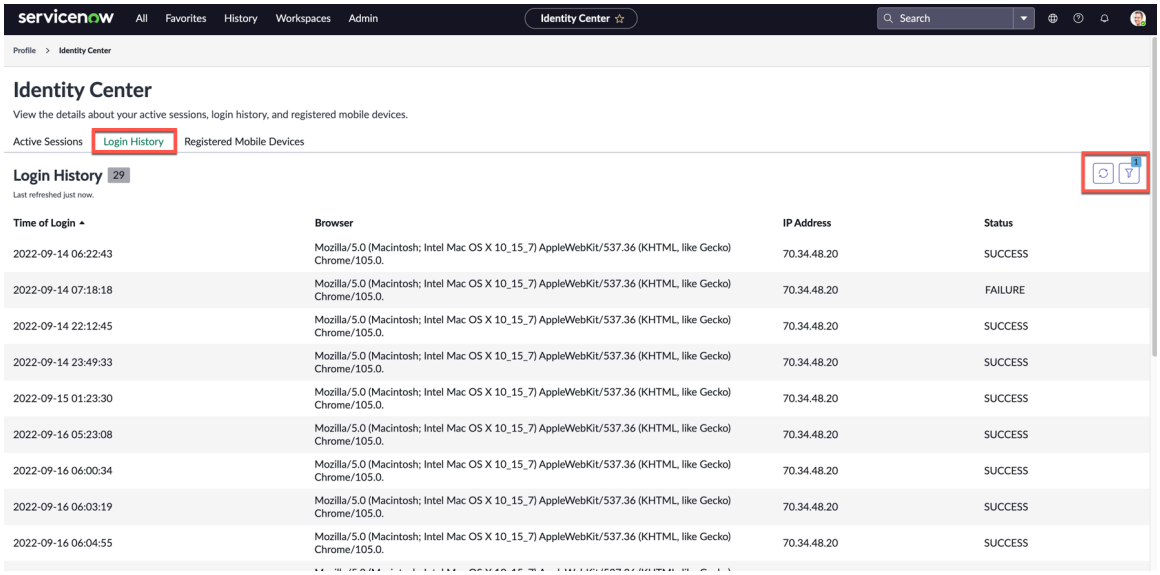
ID センターの [ログイン履歴] タブは、ログイン情報とログインのステータスの確認に役立ちます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィルターを使用して、セキュリティ調査に役立つログインアクションを指定できます。フィルターは、アクティビティが本物か疑わしいかを判断し、その情報を管理者に報告するのに役立ちます。

ログイン履歴のページネーションはデフォルトで 20 で、最大 100 に設定できます。



以下は、ログイン履歴からのその他の詳細の一部です。

- ログイン時刻は、モバイルデバイスを使用してインスタンスにアクセスするときに更新された時刻です。
- レコードは ID センターに 30 日間保存されます。

登録済みモバイルデバイスの表示

ServiceNow インスタンスの登録済みモバイルの詳細を示します。

ID センターの [登録済みモバイルデバイス (Registered Mobile Devices)] タブには、ServiceNow インスタンスへのアクセスに使用された登録済みデバイスの詳細が表示されます。

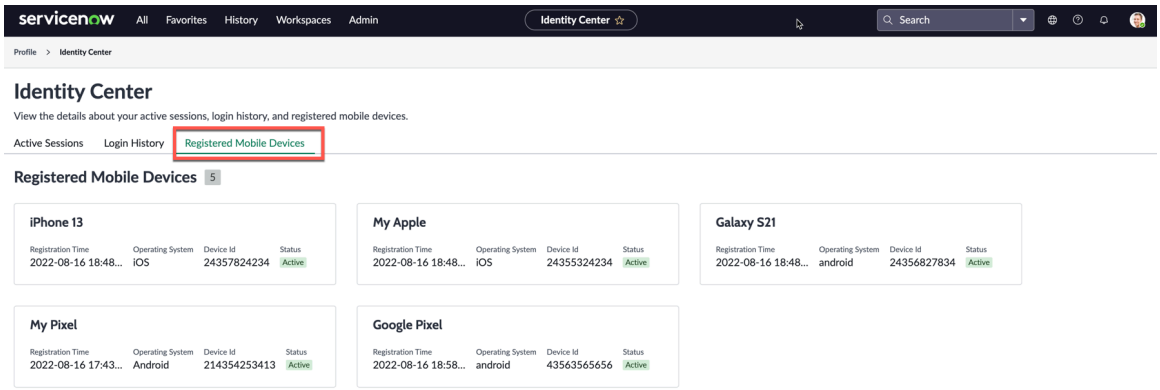
適応認証モジュールが有効になっていて、登録済みモバイルデバイスが登録されている場合、ID センターには登録済みデバイスの詳細が表示されます。

さらに、オペレーティングシステム、デバイス ID、デバイスのステータスなどのデバイスの詳細と、デバイスの登録時間も表示されます。

モバイルデバイスを登録するには、適応認証 (*com.snc.adaptive_authentication*) プラグインがインストールされ、信頼できるモバイルアプリ機能が有効になっていることを確認する必要があります。詳細については、「信頼できるモバイルアプリのアクティブ化」を参照してください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



管理者の ID 測定基準

ServiceNow インスタンスのユーザー、特権ユーザー、アクティブなセッション、および統合されたアカウントの傾向を表示します。

管理者の ID 測定基準には、次の傾向があります。

- ユーザー
- 特権ユーザー
- 統合または人間以外のアカウント
- アクティブセッション
- 非アクティブなセッション

詳細については、「セキュリティセンターの測定基準」を参照してください。

クロスドメイン ID 管理システム (SCIM)

クロスドメイン ID 管理システム (SCIM) API は、SCIM プロトコルを使用してユーザーとグループの操作を作成、読み取り、更新、および削除するためのエンドポイントを提供します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

SCIM プロバイダー

SCIM プロバイダーは、レコードの作成、更新、削除など、IdP の ID に対して行われた変更を同期します。

SCIM クライアント

SCIM クライアントは、SCIM に準拠する REST 要求をサポートするシステムで ID リソースを作成、更新、および削除する際に使用します。

自動翻訳

SCIM プロトコルは、HTTP (RFC7230) 標準を基礎とするアプリケーションレベルの HTTP ベースプロトコルです。この API はユーザーやグループなどの ID データのプロビジョニングと管理に使用します。エンタープライズからクラウドへのサービスプロバイダーやクラウド間のシナリオなど、Web およびクロスドメイン環境で API を使用します。

この API にアクセスするには、SCIM v2 - ServiceNow® Cross-domain Identity Management (com.snc.integration.scim2) プラグインを有効にする必要があります。

SCIM API の詳細については、「クロスドメイン ID 管理システム (SCIM) API」を参照してください。

SCIM プロバイダー

サービスプロバイダーは、SCIM API を使用してユーザーとグループをプロビジョニングします。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

探索

SCIM プロバイダーの詳細を確認します。

アクティブ化

SCIM をアクティブ化します。

SCIM のカスタマイズ

SCIM をカスタマイズする方法の詳細を取得します。

ソース定義

SCIM のソース定義について詳細を確認します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

SCIM プロバイダーの概要

サービスプロバイダーは、SCIM API を使用してユーザーとグループをプロビジョニングします。

SCIM プロバイダーとして、ServiceNow スキーマは、ユーザーとグループをプロビジョニングする SCIM API をサポートしています。

SCIM プロバイダーは、レコードの作成、更新、削除など、IdP の ID に対して行われた変更を同期します。これらの変更は、SCIM プロトコルに従って自動的にプロバイダーに同期されます。また、IdP ではプロバイダーから ID を読み取って IdP ディレクトリーに追加することができます。その後、セキュリティの脆弱性を作成する可能性のあるプロバイダーの誤った値を検出することが可能です。この同期によって、エンドユーザーが最新のプロファイルと権限を使用して、自身が割り当てられたアプリケーションにシームレスにアクセスすることが可能になります。

SCIM プロバイダーの設定

SCIM プロバイダーを設定するには、次のタスクを実行します。

- **SCIM v2 - ServiceNow Cross-domain Identity Management** プラグインをアクティブ化します。詳細については、「SCIM プラグインのアクティブ化」を参照してください。
- SCIM に必要な他のプラグインをアクティブ化します。
  - OAuth 2.0
  - REST API Provider
  - REST API Access Policy
- SCIM サービスの一部として scim_admin ロールを追加します。☒

> ⚠ **警告:**
> このロールは慎重に付与してください。scim_adminロールは、scmin_adminが個人識別可能情報 (PII) を追加または更新できる admin ロールをユーザーに付与することと同じです。

テーブル

sys_user と sys_group の 2 つのテーブルには、既存の ServiceNow テーブルにマッピングされない SCIM 属性が含まれています。テーブルの詳細については、「SCIM 固有のテーブル」を参照してください。

SCIM プラグインのアクティブ化

SCIM をアクティブ化するには、SCIM v2 - ServiceNow Cross-domain Identity Management (com.snc.integration.scim2) プラグインをインストールします。

始める前に

必要なロール：admin

手順

1. 移動先 すべて > システムアプリケーション > 利用可能なすべてのアプリケーション > すべて.
2. フィルター基準と検索バーを使用して、SCIM v2 - ServiceNow Cross-domain Identity Management (com.snc.integration.scim2) プラグインを検索します。

   名前または ID でプラグインを検索できます。プラグインが見つからない場合は、ServiceNow 担当者から要求する必要があります。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

3. [インストール] を選択して、[プラグインをアクティブにする] ダイアログボックスで、[アクティブ化] をクリックします。

> **注:**
> ドメイン分離と代理管理者がインスタンスで有効になっている場合、管理ユーザーはグローバルドメインに含まれている必要があります。それ以外の場合、次のエラーが表示されます： 別の操作が実行されているため、アプリケーションのインストールは利用できません：<プラグイン名> のプラグインの有効化。

チュートリアル：**Azure AD** でユーザープロビジョニングするための **SCIM** の構成

Azure AD のプロビジョニングサービスを使用して、SCIM によりユーザーとグループが ServiceNow に自動的にプロビジョニングおよびプロビジョニング解除されるように Azure AD を構成します。

始める前に
SCIM プラグインのインストール

必要なロール：scim_admin

> **警告:**
> このロールは慎重に付与してください。scim_adminロールは、scmin_adminが個人識別可能情報 (PII) を追加または更新できる admin ロールをユーザーに付与することと同じです。

このタスクについて
次の認証方法で SCIM を使用してユーザーをプロビジョニングできます。

- 基本認証
- OAuth

基本認証を使用するユーザーのプロビジョニング

基本認証を使用する Azure AD のプロビジョニングサービスを使用して、SCIM によりユーザーとグループが ServiceNow に自動的にプロビジョニングおよびプロビジョニング解除されるように Azure AD を構成します。

始める前に
必要なロール：scim_admin

> **警告:**
> このロールは慎重に付与してください。scim_adminロールは、scmin_adminが個人識別可能情報 (PII) を追加または更新できる admin ロールをユーザーに付与することと同じです。

- SCIM プラグインのアクティブ化

手順

1. 移動先 すべて > システム **Web** サービス > **REST API** アクセスポリシー をクリックして、REST API アクセスポリシーの詳細を確認します。
2. API アクセスポリシーページで、**[SCIM API** ポリシー **(SCIM API Policy)]** レコードをクリックします。
3. [認証プロファイル] セクションで **[SCIM API** 基本認証 **(SCIM API Basic Auth)]** レコードが利用可能であることを確認します。
4. 以前にアプリケーションレジストリとして構成または検証された **[SCIM API]** レコードで [基本認証] フィールドが指定されているかどうかを確認します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

5. Azure Portal にサインインします。
6. 移動先 エンタープライズアプリケーション > すべてのアプリケーション.
7. アプリケーションのリストから、ServiceNow を選択するか、新しい ServiceNow アプリケーションを作成します。
8. [プロビジョニング] タブを選択し、[プロビジョニングモード] を [自動] に設定します。
9. [管理者資格情報] セクションで、次のように指定します。
   - 認証方法：基本認証
   - インスタンス名
   - 管理ユーザー名
   - 管理者パスワード
10. [テスト接続] を選択して、Azure AD が ServiceNow に接続できることを確認します。

> **注:**
> 接続に失敗した場合は、ServiceNow アカウントに管理者権限があることを確認して、再試行しください。

OAuth を使用するユーザーのプロビジョニング

OAuth を使用する Azure AD のプロビジョニングサービスを使用して、SCIM によりユーザーとグループが ServiceNow に自動的にプロビジョニングおよびプロビジョニング解除されるように Azure AD を構成します。

始める前に
必要なロール：scim_admin

> **警告:**
> このロールは慎重に付与してください。scim_adminロールは、scmin_adminが個人識別可能情報 (PII) を追加または更新できる admin ロールをユーザーに付与することと同じです。

- SCIM プラグインのアクティブ化

手順

1. 移動先 すべて > システム **OAuth** > アプリケーションレジストリー.
2. [アプリケーションレジストリ] ページで、**[SCIM API]** レコードをクリックします。
3. **[SCIM API]** レコードの詳細を確認します。

   これらの詳細は、Azure AD で ServiceNow アプリケーションを構成するときに指定する必要があります。
4. 移動先 すべて > システム **Web** サービス > **REST API** アクセスポリシー をクリックして、REST API アクセスポリシーの詳細を確認します。
5. API アクセスポリシーページで、**[SCIM API** ポリシー **(SCIM API Policy)]** レコードをクリックします。
6. [認証プロファイル] セクションで **[SCIMAPIOAuthOnly]** レコードが利用可能であることを確認します。
7. 以前にアプリケーションレジストリとして構成または検証された **[SCIM API]** レコードで **[OAuth** エンティティ] フィールドが指定されているかどうかを確認します。
8. Azure Portal にサインインします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

9. 移動先 エンタープライズアプリケーション > すべてのアプリケーション.
10. アプリケーションのリストから、ServiceNow を選択するか、新しい ServiceNow アプリケーションを作成します。
11. [プロビジョニング] タブを選択し、[プロビジョニングモード] を [自動] に設定します。
12. [管理者資格情報] セクションで、次のように指定します。
    - 認証方法：OAuth

      注:
      SCIM でプロビジョニングするために OAuth フィールドに入力するには、アプリケーションを SCIM 2.0 エンドポイントに更新する必要があります。更新方法の詳細については、Azure のドキュメント を参照してください。

    - インスタンス名
    - 管理ユーザー名
    - 管理者パスワード
13. [テスト接続] を選択して、Azure AD が ServiceNow に接続できることを確認します。

    注:
    接続に失敗した場合は、ServiceNow アカウントに管理者権限があることを確認して、再試行しください。

SCIM のトラブルシューティング

SCIM と統合する一般的なエラーシナリオ。

無効な REST API URL

アクション：有効な API URL を入力します。**[REST API Explorer]** で REST API URL をクロスチェックできます。

ServiceNow インスタンスにリダイレクト URL が設定されていない

アクション：ServiceNow に SCIM OAuth エンティティの有効なリダイレクト URL を入力します。ServiceNow で OAuth エンティティを構成するときにリダイレクト URL を入力します。

リダイレクト URL が要求と異なる

アクション：[認証エンドポイント **(Authorization Endpoint)]** で指定された **[redirect_url]** は、ServiceNow で構成された OAuth エンティティと同じである必要があります。

注:

このエラーは、Azure の「認証エンドポイント」と ServiceNow の「リダイレクト URL」の間に不一致がある場合に発生します

無効なクライアントシークレットが渡された

アクション：「クライアントシークレット」に入力された値は、ServiceNow で構成された OAuth エンティティと同じである必要があります。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Azure の「認証エンドポイント」で無効な「ClientId」が渡された

アクション：「認証エンドポイント」の「client_id」パラメーターに入力された値は、ServiceNow で構成された OAuth エンティティと同じである必要があります。

SCIM のカスタマイズ

ID 管理用の SCIM プロトコルをカスタマイズします。

SCIM をカスタマイズすると、次のことができるようになります。

- 動的な拡張スキーマを生成することで、sys_user および sys_user_group テーブルのカスタムフィールドをサポートする。
- デフォルトの SCIM マッピングを上書きする機能を実現する。

SCIM 管理者は、ユーザーリソースとグループリソースのカスタム拡張スキーマを定義できます。カスタム拡張スキーマで定義された属性は、sys_user または sys_user_group テーブルのフィールドにマッピングできます。

SCIM のカスタマイズの設定

SCIM のカスタマイズでは、次のタスクを実行する必要があります。

- SCIM 拡張スキーマテーブルでユーザーとグループのカスタム拡張スキーマを定義します。詳細については、「SCIM 拡張スキーマの作成」を参照してください。
- カスタムスキーマ属性の ETL 定義にエンティティを作成します。エンティティは、sys_user または sys_user_group 属性のいずれかでマッピングされたターゲットテーブルに対して作成されます。詳細については、「SCIM ETL 定義の作成」を参照してください。
- これら 2 つのエンティティ間に RTE マッピングを作成します。詳細については、「SCIM ETL 定義の作成」の手順 5 を参照してください。
- SCIM API 要求ペイロードのデータを含むカスタムスキーマ属性を送信します。

SCIM API が、定義されたマッピングを使用して RTE エンジンを呼び出します。マッピングで定義されたターゲットテーブルの各フィールドにデータが格納されます。

SCIM のカスタマイズのプロパティとスキーマ

SCIM のカスタマイズには、次のようなプロパティ、サポート済みスキーマ、およびサポートされていないスキーマが含まれています。

プロパティ

SCIM のカスタマイズでは、次のシステムプロパティが追加されます。

プロパティ

名前	説明
com.snc.integration.scim2.max.member.count	SCIM の最大メンバー数。
com.snc.integration.scim2.resolve.external.id.conflict	外部 ID の SCIM フィルターで複数のリソースが見つかった場合は、要求元クライアントのソース定義に基づいて SCIM リソースを解決します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

プロパティ (続く)

名前	説明
	注: 前提条件として、複数のソースからプロビジョニングを行う場合は、[SCIM ソース定義] テーブルでソースを定義する必要があります。ソースが定義されていない場合、またはこのプロパティが非アクティブな場合は、一致するすべてのリソースが外部 ID のフィルター応答で返されます。
com.snc.integration.scim2.user.etl.definition.id	SCIM ユーザー ETL 定義 ID。
com.snc.integration.scim2.group.etl.definition.id	SCIM グループ ETL 定義 ID。
com.snc.integration.scim2.rte.verbose.logging.enabled	SCIM ユーザーおよびグループ RTE 定義の詳細なログ記録を有効にします。
com.snc.integration.scim2.string.field_length_validation.enabled	フィールドの長さの検証。このプロパティは、フィールドを切り捨てて保存するのではなく、検証を有効にするものです。
com.snc.integration.scim2.provider.customization.script.id	SCIM 応答をカスタマイズするためのスクリプトインクルードの ID。

サポート済みスキーマ

SCIM のカスタマイズでは、次のサポート済みスキーマが追加されます。

サポート済みスキーマ

スキーマ	説明	プリフィックス	例
urn:ietf:params:scim:schemas:core:2.0:User	ユーザーのコア属性が含まれます。	none	name.middleName
urn:ietf:params:scim:schemas:extension:servicenow:2.0:User	ServiceNow に関連する属性が含まれます。	servicenow	servicenow.manager.value
urn:ietf:params:scim:schemas:extension:custom:2.0:User	コア拡張または ServiceNow 拡張スキーマの一部としてマッピングされていないカスタム属性が含まれます。	custom	custom.socialId

サポートされていないスキーマ

urn:ietf:params:scim:schemas:extension:enterprise:2.0:User：ビジネスや企業に所属する、またはその組織を代表するユーザーを表す際に一般的に使用される属性が含まれます。

注:
Enterprise スキーマは有効なスキーマですが、その属性はどのテーブルにもマッピングされます。データベースの永続性がサポートされていないため、Enterprise スキーマが要求本文に含まれている場合でもエラーは表示されません。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

SCIM 拡張スキーマの作成

コアスキーマまたは ServiceNow 拡張スキーマの一部としてマッピングされていないフィールドにマッピングするカスタム属性を作成します。

始める前に
必要なロール：scim_admin

> **警告:**
> このロールは慎重に付与してください。scim_adminロールは、ユーザーに admin ロールを付与することと同じです。ここで、scmin_adminロールは、ビジネスロジックまたは ACL 保護をバイパスできるテーブルに新しいレコードを挿入できます。

手順

1. 移動先 すべて > **SCIM** > **SCIM** 拡張スキーマ.
2. [新規] をクリックします。
3. フォームのフィールドに入力します。

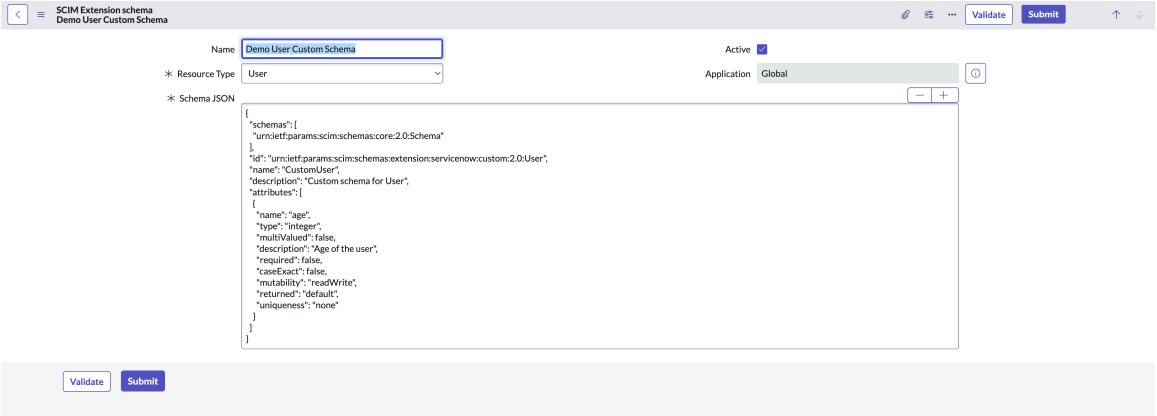
> **注:**
> [リソースタイプ] フィールドにマッピングできる拡張スキーマは 1 つだけです。たとえば、リソースタイプとしてのユーザーは、ユーザー拡張スキーマにマッピングできます。

SCIM 拡張スキーマ

フィールド	説明
名前	拡張スキーマの名前。
アクティブ	スキーマをアクティブ化するオプション。レコードをカスタム拡張スキーマと見なす必要がある場合は、このフィールドを選択します。ユーザータイプとグループタイプのどちらに対しても、特定のリソースタイプに対して一度にアクティブ化できるカスタム拡張スキーマレコードは 1 つだけです。
リソースタイプ	拡張スキーマにマッピングする必要があるリソースタイプ。オプションは次のとおりです。 ○ ユーザー ○ グループ
アプリケーション	このレコードのアプリケーションスコープ。
スキーマ JSON	JSON スキーマ内の詳細情報。属性を含む拡張スキーマの定義の詳細については、Datatracker を参照してください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



4. [検証] をクリックして属性を検証します。
5. [送信] をクリックします。

タスクの結果

ユーザーまたはグループのリソースタイプに関連するカスタム属性を持つ拡張スキーマが作成されます。SCIM ETL 定義を使用して、sys_user および sys_user_group テーブルの拡張スキーマに基づいてリソースをマッピングします。詳細については、「SCIM ETL 定義の作成」を参照してください。

SCIM ETL 定義の作成

SCIM ETL 定義を使用して、カスタム属性を sys_user または sys_user_group テーブルにマッピングします。

始める前に

必要なロール：scim_admin

警告:
このロールは慎重に付与してください。scim_adminロールは、ユーザーに admin ロールを付与することと同じです。ここで、scmin_adminロールは、ビジネスロジックまたは ACL 保護をバイパスできるテーブルに新しいレコードを挿入できます。

注:

- SCIM グループと SCIM ユーザー ETL 定義は、リソースマッピングのベースシステムの一部です。同じリソースマッピングを使用して、必要に応じて基準を変更することも、新しいリソースマッピングを作成することもできます。
- SCIM マッピングでは、RTE を介した [*] フィールドはサポートされていません。

手順

1. 「抽出変換ロード (ETL) 定義を作成する」の指示に従います。
2. 新しく作成されたレコードを開いて詳細を表示します。
3. [ETL エンティティ] セクションで、[新規] をクリックしてエンティティを作成します。
   エンティティを作成する必要があるユーザーは次のとおりです。
   - scim-user：SCIM のフィールド用。
   - ユーザー (sys_user) またはグループ (sys_user_group) テーブル：SCIM を使用してデータベーステーブルからマッピングするフィールド用。たとえば、SCIM を使用してユーザーの詳細をカスタマイズするには、sys_user テーブルを使用します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

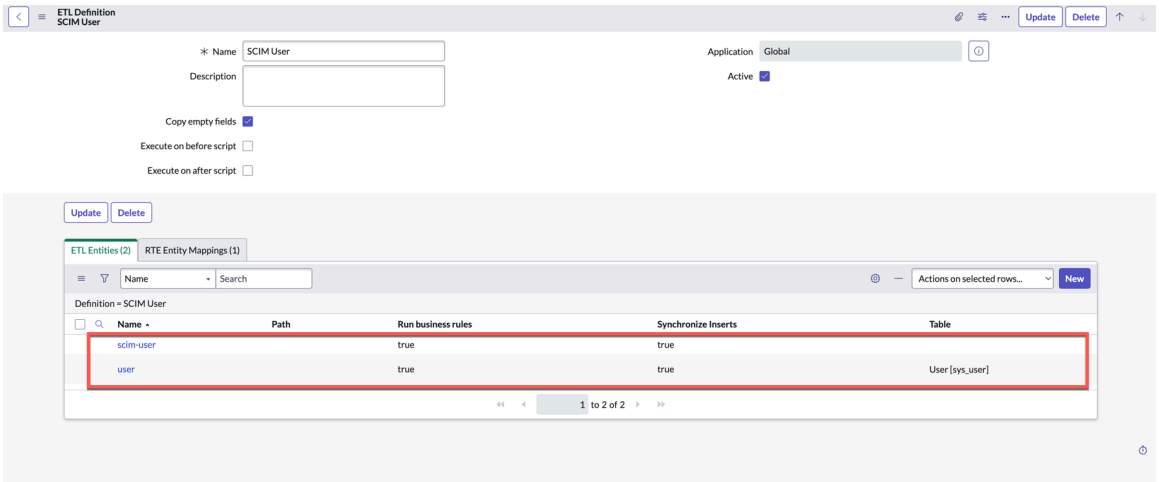
a. フォームのフィールドに入力します。

[ETL エンティティ] フォーム

フィールド	説明
名前	ETL エンティティの名前。
アプリケーション	このレコードのアプリケーションスコープ。
テーブル	ETL エンティティのターゲットテーブル。
定義	選択された ETL エンティティ。
パス	このエンティティの一意のパス。インポートセットテーブルを表すエンティティのパスを指定しないでください。エンティティがコレクションを表す場合、パスはアスタリスク (*) で終わる必要があります。この要件は、中間エントリとターゲットテーブルエンティティに適用されます。
挿入を同期する	レコード挿入を同期することで一意の結合フィールド値のある 1 つのレコードのみを保証するオプション。
ビジネスルールを実行	ビジネスルールを実行するオプション。

b. [送信] をクリックします。

scim-user および user テーブルに対して ETL エンティティが作成されます。この ETL エンティティ内に ETL エンティティフィールドを作成し、RTE エンティティマッピングを作成して両方のエンティティをマッピングする必要があります。



4. エンティティを作成してマッピングします。

a. 送信されたレコード (scim-user と user) を開きます。

b. [ETL エンティティ] の各フィールドで、[新規] をクリックしてフィールドを追加します。

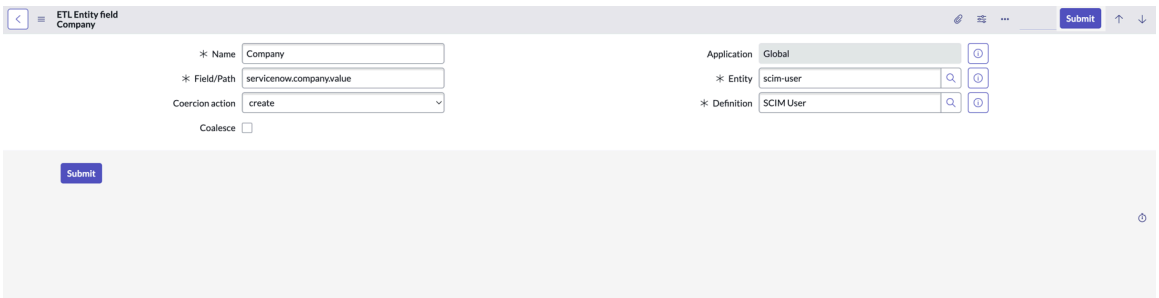
c. フォームのフィールドに入力します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

[ETL エンティティ] フォーム

フィールド	説明
名前	[ETL エンティティ] フィールド定義の名前。
アプリケーション	このフィールド定義が属する選択された ETL エンティティ。
フィールド/パス	このフィールドは列またはパスです。 ▪ エンティティがインポートテーブルまたはターゲットテーブルの場合、フィールドは列名です。 ▪ フィールドにネストされた構造がある場合、フィールドはパスです。
エンティティ	この操作が適用されるエンティティ。検索アイコンを使用してエンティティを選択します。
強制アクション	参照または選択肢が見つからない場合にシステムで行われる必要がある操作です。オプションは次のとおりです。 ▪ 作成：新しい参照か選択肢を作成します。現在のレコードに参照または選択肢を割り当てます。 ▪ 却下：レコード全体をデータベースに保存しません。 ▪ 無視：現在の値を空に設定します。
定義	このフィールド定義が属する選択された ETL エンティティ。
結合	既存のレコードをクエリするオプション。



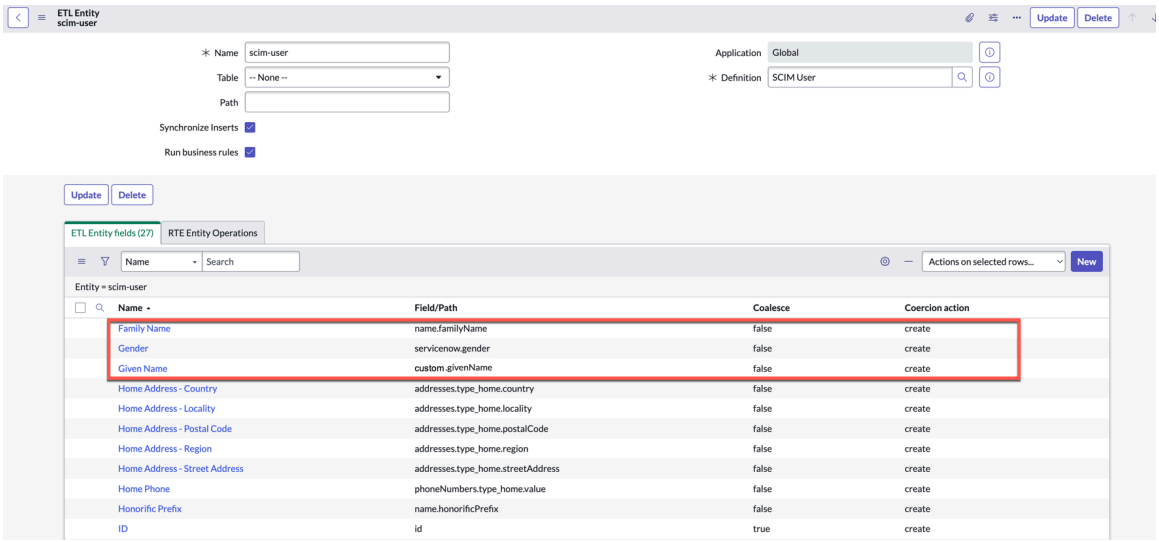
d. [送信] をクリックしてエントリを送信します。

要件に基づいて、複数のエントリを [ETL エンティティ] フィールドとして追加できます。

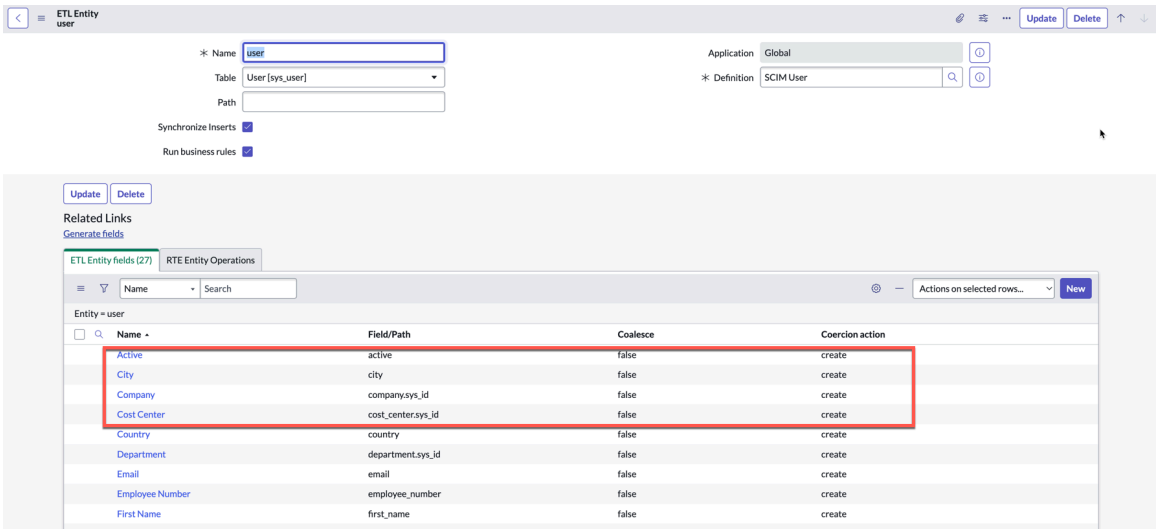
scim-user の ETL エンティティには、コア拡張 (user)、ServiceNow 拡張、またはカスタム拡張を持つエンティティを含めることができます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



user の ETL エンティティには、データベーステーブルのエンティティを含めることができます。たとえば sys_user テーブルなどです。



注:
受信する SCIM のフィールドにフィルターを追加するには、アンダースコア (_) を使用します。このアンダースコアは EQ フィルターに変換されます。たとえば、属性 *email.type_work.value* はメールの SCIM フィルター *[type eq "work"].value* を適用します。

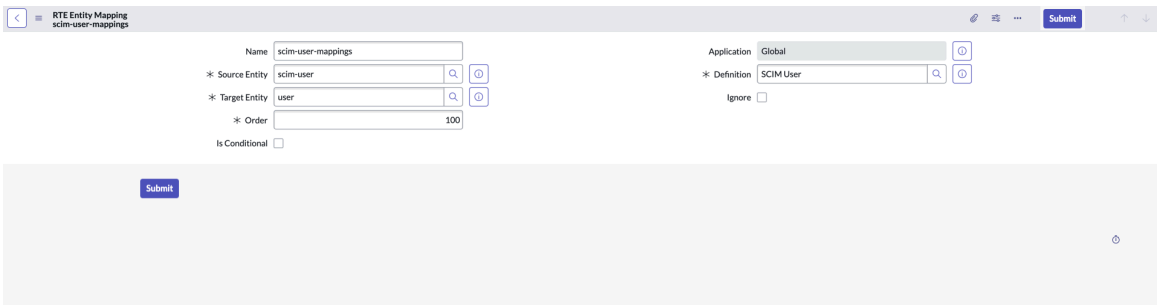
scim-user と user の [ETL エンティティ] レコードの両方でフィールドを作成したら、RTE エンティティのマッピングレコードを作成する必要があります。その後、ソースとターゲットの定義を指定して、両方のフィールドをマッピングする必要があります。

5. [RTE エンティティマッピング] セクションで、[新規] をクリックしてエンティティマッピングを作成します。
6. フォームの各フィールドに入力します。

フィールド	説明
名前	マッピングの名前。

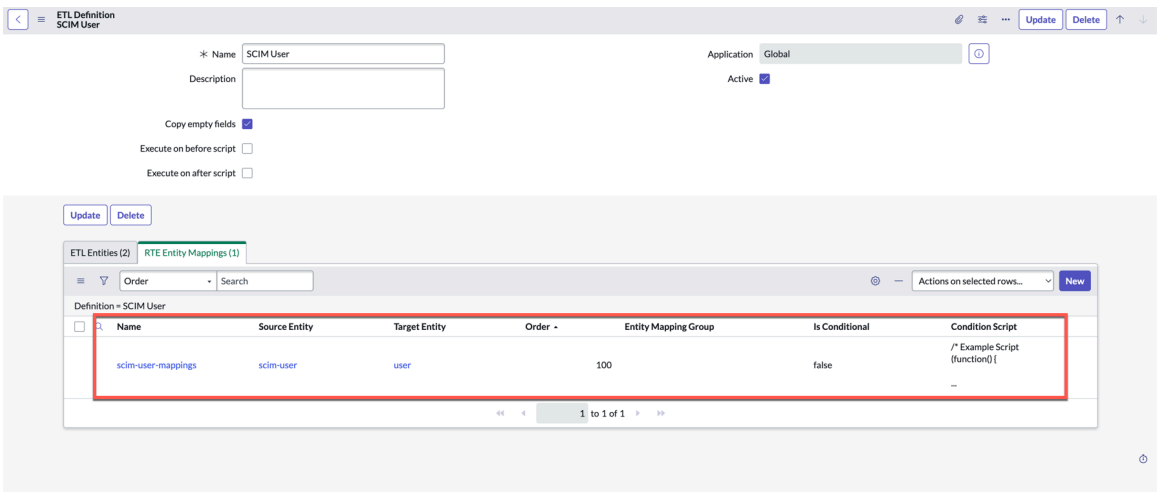
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
ソースエンティティ	マッピングのソースエンティティ。
ターゲットエンティティ	マッピングのターゲットエンティティ。
順番	マッピングを処理する順序。
条件つき	マッピングを条件付きとして指定するオプション。
条件スクリプト	マッピングのために満たす必要のある条件を定義するスクリプト。
アプリケーション	このレコードのアプリケーションスコープ
定義	このマッピングが属する選択された ETL エンティティ。
無視	強力なインポートセット変換 (RTE) を使用してデータを統合するときに、この ETL エンティティマッピングを無視するかどうかを指定するオプション。



7. [送信] をクリックします。

   次の例は、[ETL エンティティ] の scim-user と user の両レコードをマッピングするために作成されたレコードを示しています。



8. 送信済みのレコード (scim-user-mappings) を開き、[ETL エンティティ] の scim-user と user のレコード間のマッピングを作成します。

   a. [RTE フィールドマッピング] セクションで、[新規] をクリックします。

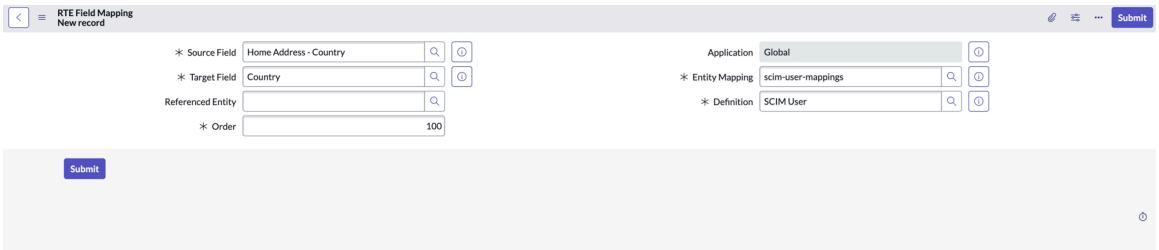
   b. フォームのフィールドに入力します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

ETL エンティティフィールド

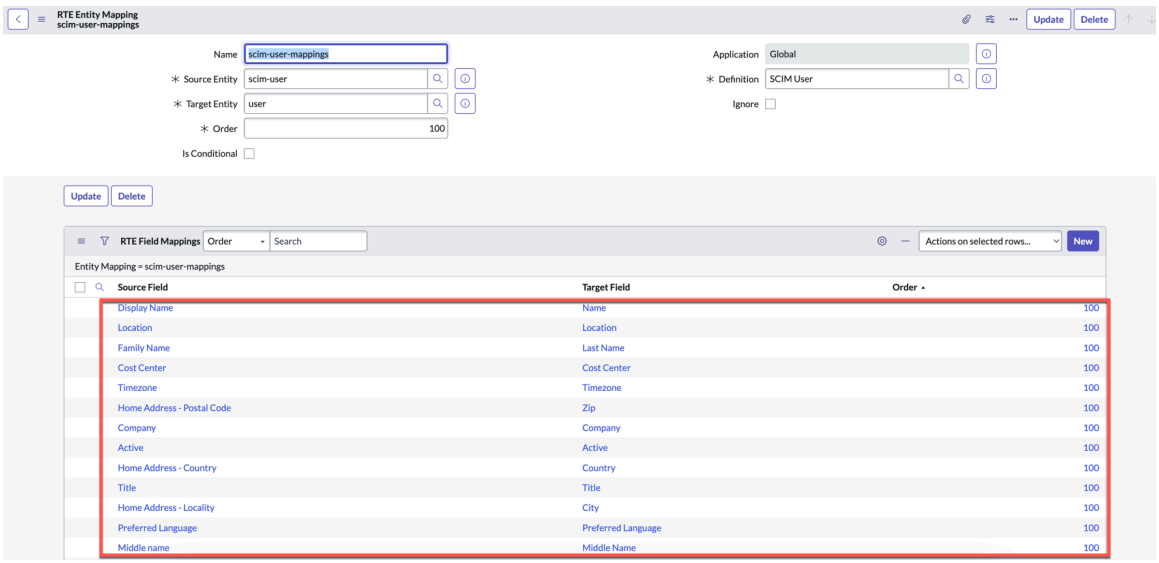
フィールド	説明
ソースフィールド	このレコードのアプリケーションスコープ。
アプリケーション	このフィールド定義が属する選択された ETL エンティティ。
ターゲットフィールド	操作が単一の出力を受け取る場合は、操作の ETL フィールドを出力します。
エンティティマッピング	この操作が適用されるエンティティマッピング。
参照エンティティ	参照されるエンティティとそれが適用される操作。
定義	このフィールド定義が属する選択された ETL エンティティ。
順番	エンティティで実行される操作の順序。



ソースフィールドの [自宅住所 - 国] (scim-user の ETL エンティティ) は、ターゲットフィールドを [国] (user の ETL エンティティ) としてマッピングします。

c. [送信] をクリックしてエントリを送信します。

要件に基づいて、複数のエントリを RTE エンティティマッピングとして追加できます。



ソースフィールドとターゲットフィールドが設定どおりにマッピングされています。SCIM を使用して CRUD 操作を実行すると、カスタマイズした値がそれぞれのテーブルで更新されます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

タスクの結果
このように ETL の定義とマッピングを設定することで、ソーステーブルからデータを抽出し、必要に応じてデータを変換して、データをターゲットテーブルにロードすることが可能になります。

関連情報

抽出変換ロード (ETL) 定義を作成する

マップされていないフィールドの処理

SCIM のカスタマイズでは、マップされていないフィールドをさまざまな方法で処理できます。

SCIM のカスタマイズ中、sys_user および sys_user_group テーブルに含まれていないフィールドは、次の機能を実行することでマッピングできます。

SCIM のカスタマイズ (作成または更新)

SCIM クライアントを作成または更新できます。

- SCIM 管理者は、ETL 定義または RTE にマッピングされていないフィールドの *onBefore* および *onAfter* スクリプトにカスタムスクリプトを追加できます。
- SCIM 管理者は、*onBefore* および *onAfter* スクリプトにカスタムスクリプトを追加することで、RTE マッピングを上書きできます。
- RTE の *onBefore* または *onAfter* スクリプトでスクリプト可能な API を呼び出し、着信した要求にアクセスして他のテーブルやリスト、マッピングされていない属性の変換を実行できます。
- *sn_auth.SCIM2Util.getScimProviderCustomizationContext()* メソッドを使用して、*scimResource* オブジェクトを含む SCIM 要求コンテキストを提供できます。各操作におけるコンテキスト内の *scimResource* は次のものを表します。
  - **POST**：要求ペイロードで送信される SCIM リソース。
  - **PUT**：要求ペイロードで送信された SCIM リソースで置き換えられる、データベースの現在の SCIM リソース。
  - **PATCH**：パッチ操作を実行した後のデータベースの現在の SCIM リソース。

onAfter スクリプトの例を次に示します。

```
(function onAfter(source, target, importLog) {

    var ctx = sn_auth.SCIM2Util.getScimProviderCustomizationContext();
    gs.info("scim context ee: " + JSON.stringify(ctx.scimResource));

    var roles = ctx.scimResource.roles;
    if(roles) {
        var removingRolesGR = new GlideRecord("sys_user_has_role");
        removingRolesGR.addQuery("user", target.sys_user[0].sys_id);
        removingRolesGR.query();
        removingRolesGR.deleteMultiple();

    for (var i = 0; i < roles.length; i++) {
        var addingRolesGR = new GlideRecord("sys_user_has_role");
        addingRolesGR.setValue("user", target.sys_user[0].sys_id);
        addingRolesGR.setValue("role", roles[i].value);
        addingRolesGR.setValue("state", "active");
        addingRolesGR.insert();
        }
        }
```

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

```
    var customUserExtn = new
global.SCIMProviderCustomization().getCustomExtensionUrn('User');
    var salary = ctx.scimResource[customUserExtn].salary;
    if (salary) {
      var gr = new GlideRecord("u_user_salary");
      gr.addQuery("user", target.sys_user[0].sys_id);
      gr.query();
      if (gr.next()) {
        gr.setValue("salary", salary);
        gs.info("scim update: " + gr.update());
      } else {
      gr.setValue("salary", salary);
      gr.setValue("user", target.sys_user[0].sys_id);
      gr.insert();
      }
     }

})(source, target, importLog);
```

SCIM の応答をカスタマイズする

GET API 呼び出しの場合、SCIM クライアントへの応答は *SCIMProviderCustomization* スクリプトを拡張することでカスタマイズできます。

スクリプトを拡張する際に、作成者は *customizeUserResponse* および *customizeGroupResponse* メソッドを上書きして、ユーザーリソースとグループリソースの応答を変更できます。

com.snc.integration.scim2.provider.customization.script.id プロパティを使用すると、応答のカスタマイズに使用するスクリプトを SCIM プラグインで使用できるようになります。

ベーススクリプトの拡張例を次に示します。

```
var SCIMCustomizationScript = Class.create();
SCIMCustomizationScript.prototype = Object.extendsObject(SCIMProviderCustomization, {
  initialize: function() {
    SCIMProviderCustomization.prototype.initialize.call(this);
  },
  customizeUserResponse: function(context) {
    try {
      var rolesGR = new GlideRecord("sys_user_has_role");
      rolesGR.addQuery("user", context.scimResource.id);
      rolesGR.query();
      var i = 0;
      context.scimResource.roles = [];
      while (rolesGR.next()) {
        context.scimResource.roles[i] = {
          display: rolesGR.getElement('role.name').getValue(),
          value: rolesGR.getElement('role.sys_id').getValue()
        };
        i++;
      }
      var userGR = new GlideRecord("u_user_salary");
      userGR.addQuery("user", context.scimResource.id);
      userGR.query();
      if (userGR.next()) {
        var salary = userGR.getValue("salary");
```

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

```
            if (salary) {
                var customExtensionValue =
SCIMProviderCustomization.prototype.getCustomExtensionNodeValue.call(this, "User",
context);
                customExtensionValue.salary = salary;
                SCIMProviderCustomization.prototype.setCustomExtensionNodeValue.call(this,
"User", context, customExtensionValue);
            }
        }
    } catch (ex) {
        gs.error("err: " + ex);
    }
    return context;
  },
  customizeGroupResponse: function(context) {
    return context;
  },
  type: 'SCIMCustomizationScript'
});
```

注:

- *customizeUserResponse* および *customizeGroupResponse* メソッドに含まれるパラメーターは、*scimResource*という 1 つの属性を持つコンテキストオブジェクトです。この属性には、ユーザーまたはグループのリソースオブジェクトの属性がすべて含まれています。
- カスタマイズされたスクリプトインクルードは、管理者のみが作成および表示できます。
- ユーザーリソースやグループリソースが変更された場合は、コンテキストを元に戻す必要があります。
- リソースオブジェクトに属性の変更がない場合は、*com.snc.integration.scim2.provider.customization.script.id* を空に設定するか、 null として返します。
- *onAfter* スクリプトを使用して特定の属性を保持する場合は、カスタマイズされたスクリプト内の *scimResource* オブジェクトにデータベース値を設定する必要があります。このアクションが必要なのは、システムが次の操作を実行できるようにするためです。
  - PUT と PATCH の操作中に *onAfter* スクリプトの正しい *scimResource* オブジェクトを取得する。
  - *onAfter* スクリプトによって保持された属性をクライアントへの応答に含める。

ヘルパー関数

SCIM のカスタマイズに使用するヘルパー関数の一部を次に示します。これらの関数で、さまざまなタイプの情報をフェッチしたり設定したりすることが可能です。

ヘルパー関数

関数	目的
SCIMProviderCustomization.prototype.getCustomExtensionNodeValue.call(this, "User");	カスタム拡張スキーマの値をフェッチする。
SCIMProviderCustomization.prototype.getServiceNowExtensionNodeValue.call(this, "User");	ServiceNow 拡張スキーマの値をフェッチする。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

ヘルパー関数 (続く)

関数	目的
`SCIMProviderCustomization.prototype.getCustomExtensionUrn.call(this, "User", context);`	応答からエクステンションURNを取得する。
`SCIMProviderCustomization.prototype.getCustomExtensionNodeValue.call(this, "User", context);`	ServiceNowエクステンションノードを応答からフェッチする。
`SCIMProviderCustomization.prototype.setCustomExtensionNodeValue.call(this, "User", context, customExtensionValue);`	応答内にエクステンションノードを設定する。

ヘルパー関数の使用例を次に示します。

```
var customExtensionUrn =
SCIMProviderCustomization.prototype.getCustomExtensionUrn.call(this, "User");
var customExtensionValue =
SCIMProviderCustomization.prototype.getCustomExtensionNodeValue.call(this, "User",
 context);
customExtensionValue.age = "18";
SCIMProviderCustomization.prototype.setCustomExtensionNodeValue call(this, "User", context,
 customExtensionValue);
```

注:
RTE は、sys_user および sys_user_group テーブル以外のテーブルのデータ設定をサポートしています。

ソース定義の作成

ソース定義を作成して、リソースのプロビジョニング元となる ID ソースに関する情報をキャプチャします。

始める前に

必要なロール：scim_admin

警告:
このロールは慎重に付与してください。scim_adminロールは、scmin_adminが個人識別可能情報 (PII) を追加または更新できる admin ロールをユーザーに付与することと同じです。

このタスクについて

ソース定義を使用すると、プロビジョニング中の認証に使用する OAuth エンティティに、プロビジョニング ID ソースをマッピングできます。

ソース定義が作成されると、その ID ソースからプロビジョニングされるすべてのリソースが、対応するソース定義 ID にマッピングされます。

ソース定義では、次のような動作によって、必要なソース情報がキャプチャされます。

- リソースのプロビジョニング元の SCIM クライアントを識別する。
- 外部 ID から提供された重複情報を解決する。
  - 複数の ID ソースがプロビジョニングリソースである場合、外部 ID は ID ソースに対してのみ一意であるため、複数のリソースが同じ外部 ID 値を持つ可能性があります。
  - 外部 ID の SCIM フィルターで複数のリソースが返された場合は、要求元の ID ソースのソース定義に基づいてリソースを解決できます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注:
ソース定義は、OAuth 認証方法を使用する ID ソースに対してのみ作成できます。

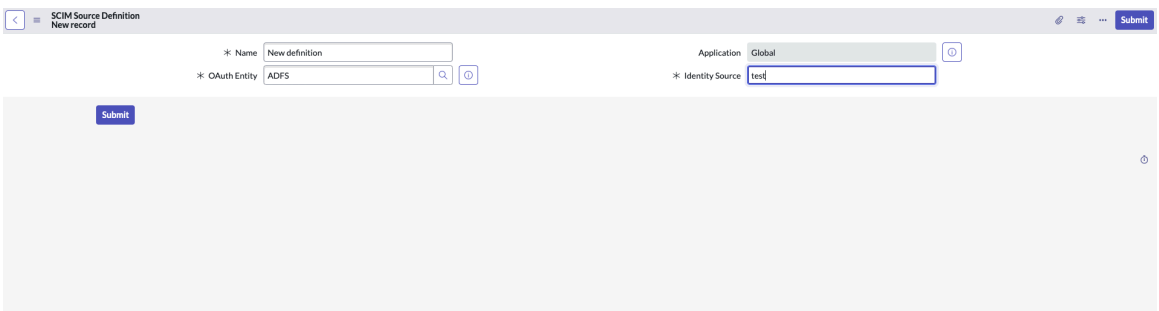
手順

1. 移動先 すべて > **SCIM** > ソース定義.
2. [SCIM ソース定義] ページで、[新規] をクリックします。
3. フォームのフィールドに入力します。

SCIM ソース定義

フィールド	説明
名前	ソース定義の名前。
アプリケーション	このレコードのアプリケーションスコープ。
OAuth エンティティ	統合ユーザーの OAuth エンティティ。このエンティティは、ID ソースプロバイダーがユーザーをプロビジョニングするために使用されます。
ID ソース	ID ソースプロバイダーの名前。例：Azure AD、Okta など

注:
com.snc.integration.scim2.resolve.externalid.conflict プロパティを有効にすると、要求元の ID ソースによって作成された SCIM リソースのみが返されます。デフォルトでは、外部 ID フィルターを持つすべての一致するリソースが返されます。



4. [送信] をクリックします。

タスクの結果
SCIM ソース定義が作成されます。SCIM ETL 定義を使用して、sys_user および sys_user_group テーブルの拡張スキーマに基づいてリソースをマッピングします。詳細については、「SCIM ETL 定義の作成」を参照してください。

SCIM クライアント

SCIM クライアントは、外部システム上の SCIM エンドポイントで公開された CRUD 操作を通じて、ID リソースのプロビジョニングと更新を容易にするものです。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

探索

SCIM クライアントの詳細を確認します。

アクティブ化

SCIM クライアントをアクティブにします。

SCIM クライアントプロパティ

SCIM をカスタマイズする方法の詳細を取得します。

トラブルシューティング

SCIM のソース定義について詳細を確認します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

SCIM クライアントの概要

SCIM クライアントは、外部システム上の SCIM エンドポイントで公開された CRUD 操作を通じて、ID リソースのプロビジョニングと更新を容易にするものです。

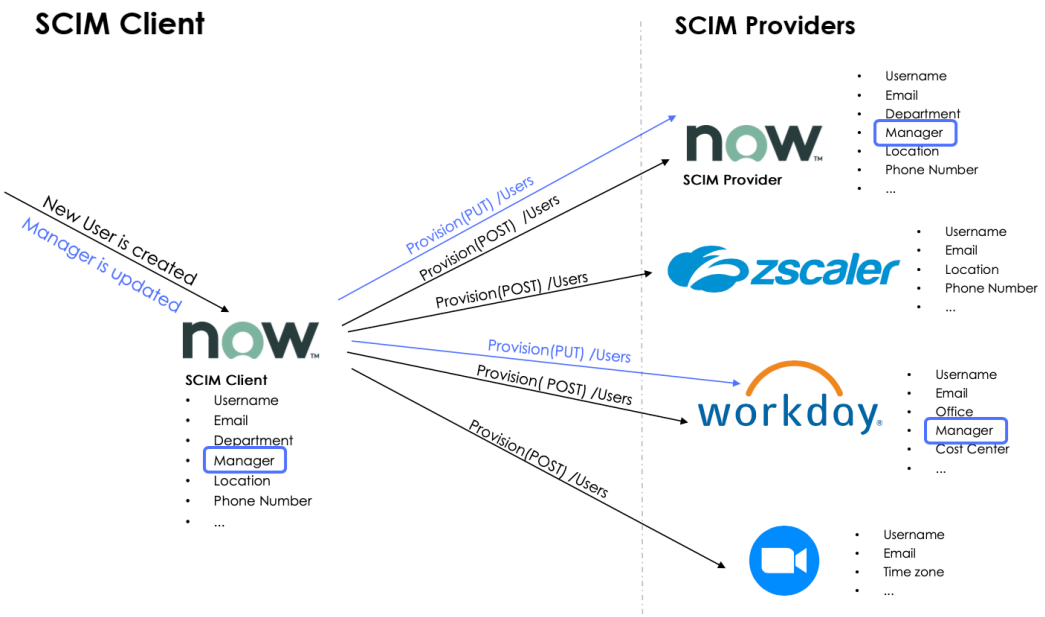
SCIM クライアントは、SCIM に準拠する REST 要求をサポートするシステムで ID リソースを作成、更新、および削除する際に使用します。このクライアントを使用して、ID ライフサイクルの管理や、ServiceNow インスタンス間または ServiceNow と他の SCIM プロバイダー間での ID 属性の同期を行います。☒

API はクライアントによって公開されるため、単一または複数の SCIM プロバイダーのリソースを作成、更新、または削除するプロセスを自動化できます。たとえば、開発者が組織に参加した場合には、Git や職場などへのアクセス権を付与する必要があります。

SCIM クライアントでは、次のアクションを実行できます。

- ユーザーまたはグループのメンバーシップの ID とアクセスをプロビジョニングする。
- ID および関連リソースを SCIM 準拠のシステムと同期する。
- 任意の SCIM プロバイダーを ServiceNow® に統合する。
- ID とアクセスをプロビジョニング解除する。

SCIM クライアントは、指定されたジョブを実行するワークフローや自動化を構築する際に統合開発者が使用できるスクリプト可能な API を提供します。スクリプト可能 API の詳細については、「SCIM2Client API」を参照してください。



SCIM クライアントの設定

SCIM クライアントを設定するには、次のタスクを実行します。

- 特定の SCIM プロバイダーのすべての発信コールに対して REST メッセージを作成します。詳細については、「REST メッセージの作成」を参照してください。
- SCIM プロバイダーを作成して、その SCIM プロバイダーから REST メッセージを使用してリソースタイプとスキーマ情報をフェッチします。SCIM プロバイダー内のリソースを更新するには、HTTP メソッド (PUT または PATCH) の設定を有効にします。詳細については、「SCIM プロバイダーの作成」を参照してください。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- 特定のリソースタイプと SCIM プロバイダーの ServiceNow 属性に対する SCIM 属性のマッピングを作成します。 詳細については、「SCIM プロバイダーリソースマッピングの作成」を参照してください。
- データベーステーブルとフィールド名で SCIM フィールドのマッピングを実行します。デフォルト値を渡すか、値をフェッチするスクリプトを記述します。詳細については、「SCIM 属性マッピングの作成」を参照してください。

SCIM クライアントプラグインのアクティブ化

SCIM クライアントをアクティブ化するには、SCIM v2 - ServiceNow Cross-domain Identity Management Client (com.snc.integration.scim2.client) プラグインをインストールします。

始める前に
必要なロール：admin

手順

1. 移動先 すべて > システムアプリケーション > 利用可能なすべてのアプリケーション > すべて.
2. フィルター基準と検索バーを使用して、SCIM v2 - ServiceNow Cross-domain Identity Management Client (com.snc.integration.scim2.client) プラグインを検索します。

   名前または ID でプラグインを検索できます。プラグインが見つからない場合は、ServiceNow 担当者から要求する必要があります。
3. [インストール] を選択して、[プラグインをアクティブにする] ダイアログボックスで、[アクティブ化] をクリックします。

   注:
   ドメイン分離と代理管理者がインスタンスで有効になっている場合、管理ユーザーはグローバルドメインに含まれている必要があります。それ以外の場合、次のエラーが表示されます： 別の操作が実行されているため、アプリケーションのインストールは利用できません：<プラグイン名> のプラグインの有効化。

SCIM クライアントのプロパティ、テーブル、スクリプト可能な API およびログ

SCIM v2 - ServiceNow Cross-domain Identity Management Client (com.snc.integration.scim2.client) プラグインには、次のシステムプロパティ、テーブル、スクリプト可能な API、およびログが含まれています。

プロパティ

SCIM クライアントでは、次のシステムプロパティが追加されます。

プロパティ

名前	説明
com.snc.integration.scim2.client.log.request.status	このプロパティは、すべてのログレコードを書き込むか、エラーログレコードのみを書き込むかを決定します。設定可能な値は **FAILURE** または **ALL** です。 デフォルト値：**ALL**
com.snc.integration.scim2.client.log.cleanup.duration	このプロパティは、ログをクリアするまでの日数を決定します。

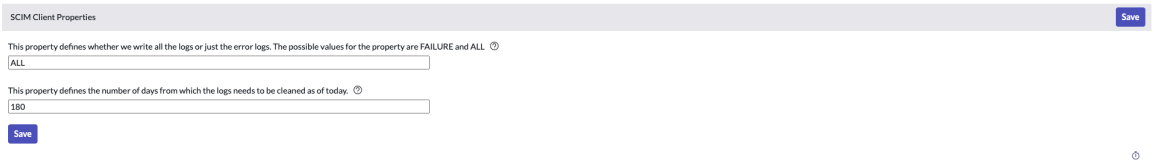
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

プロパティ (続く)

名前	説明
	デフォルト値：**180**

プロパティを設定するには、次の場所に移動します。 すべて > **SCIM** > **SCIM** クライアントプロパティ.



テーブル

SCIM クライアントでは、次のテーブルが追加されます。

テーブル

名前	説明
SCIM プロバイダー (sys_scim_provider)	名前や REST メッセージリソース定義など、各 SCIM プロバイダーのデータを格納します。
SCIM プロバイダーリソースマッピング (sys_scim_provider_resource_mapping)	各プロバイダーとリソース名のプライマリテーブル情報を格納します。
SCIM 属性マッピング (sys_scim_attribute_mapping)	テーブルフィールドやスクリプトなど、各 SCIM 属性値の取得元となるソースの詳細を格納します。
SCIM クライアントログ (sys_scim_client_logs)	SCIM プロバイダーに対してトリガーされた各コールのステータスを格納します。

スクリプト可能 **API**

SCIM2Client API は、クロスドメイン ID 管理システム (SCIM) (サーバーロール) を呼び出して、サービスプロバイダー (SP) のデータを作成、更新、または削除します。SCIM クライアントのスクリプト可能 API は、システムのコンテキストで実行されているスクリプト内で使用するか、システム管理者ユーザーが使用する必要があります。

たとえば、システムユーザーとして Integration Hub ワークフローを実行しているときや、ジョブスケジュールを実行しているときなどに、スクリプトを使用できます。

スクリプト可能 API を使用するユースケースをいくつか次に示します。

- 管理者が、バックグラウンドスクリプト、ビジネスルール、スクリプトインクルード呼び出し、ワークフローなどから ID 情報をプロビジョニングする。
- 管理者が、ID プロビジョニングのスケジュール設定済みジョブまたはオンデマンドジョブを実行する。
- プロビジョニングスクリプト可能 API の呼び出しを使用して、 スクリプトステップでワークフローやサブワークフローを実行する。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- プロビジョニングスクリプトをビジネスルールやスクリプトインクルードに直接追加する。スクリプトは管理者以外のユーザーがトリガーしてもかまわない。このユースケースは、次のような状況で有効に働きます。
  - ユーザーがトークンにアクセスできる。すなわち、REST テンプレートからトークンを生成するロールを持っている。
  - ユーザーが、マッピングされたテーブルから SCIM 属性値を取得するためのアクセス権を持っている。

スクリプト可能 API の詳細については、「SCIM2Client API」を参照してください。

SCIM クライアントログ

SCIM クライアントログには、SCIM API に関するプロビジョニングステータスが表示されます。プロビジョニングステータスを表示するには、次に移動します すべて > **SCIM** > **SCIM** クライアントログ.

REST メッセージの作成

特定の SCIM プロバイダーのすべての発信コールに対する REST メッセージを設定します。

始める前に

必要なロール：管理者

手順

1. 移動先 すべて > システム **Web** サービス > 送信 > **REST** メッセージ.
2. [新規] をクリックします。
3. フォームのフィールドに入力します。

SCIM プロバイダー

フィールド	説明
名前	このメッセージのわかりやすい名前。
エンドポイント	SCIM プロバイダーのベース URL。 例：https://example.service-now.com/api/now/scim
認証タイプ	外部の SCIM プロバイダーへの接続に使用される認証のタイプ。詳細については、「送信 REST の認証」を参照してください。
HTTP ヘッダー	外部の SCIM プロバイダーから期待されるコンテンツタイプ。 たとえば、ヘッダー名は Content-type: application/scim+json という API 要求の本文のコンテンツタイプです。

4. [HTTP メソッド] 関連リストで、**[New]** をクリックします。
5. 次の HTTP メソッドを設定します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

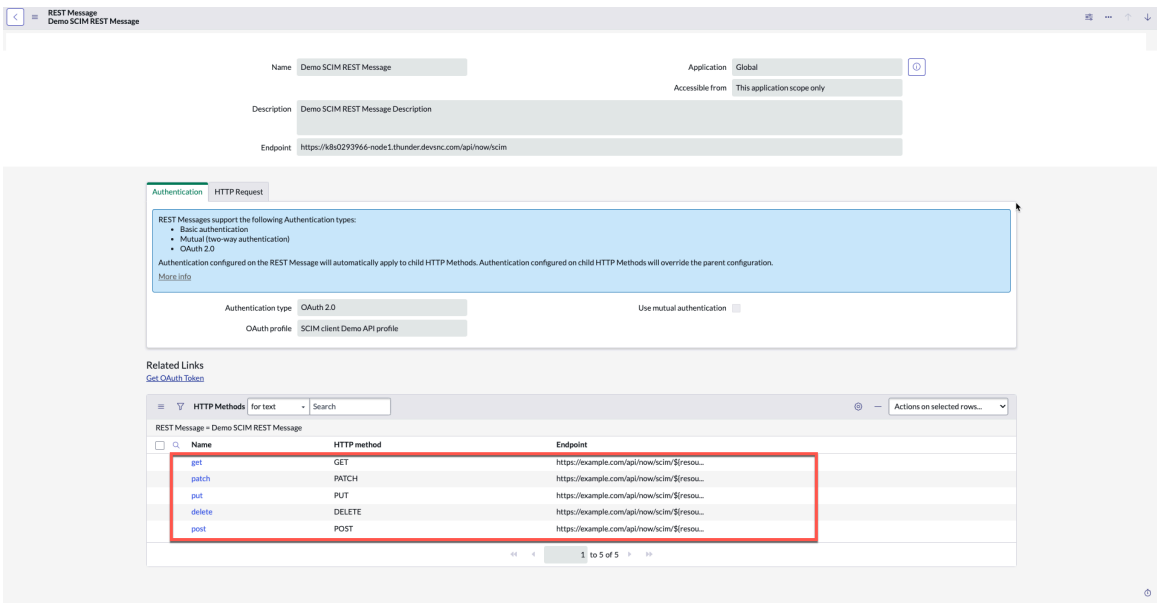
注:
URL には、置き換える必要のある変数があります。

HTTP メソッド

メソッド	サンプル URL
GET	https://example.com/api/now/scim/${resourceName}
PATCH	https://example.com/api/now/scim/${resourceName}/${resourceId}
PUT	https://example.com/api/now/scim/${resourceName}/${resourceId}
DELETE	https://example.com/api/now/scim/${resourceName}/${resourceId}
POST	https://example.com/api/now/scim/${resourceName}/${resourceId}

注:

- SCIM クライアントの操作に使用するすべての HTTP メソッドを作成する必要があります。
- サンプル REST メッセージはベースシステムから入手できます。



6. [送信] をクリックします。

タスクの結果
REST メッセージレコードが作成されます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

次のタスク
REST メッセージを使用して SCIM プロバイダーを作成します。詳細については、「SCIM プロバイダーの作成」を参照してください。

REST メッセージの作成方法の詳細については、「REST メッセージの作成」を参照してください。

SCIM プロバイダーの作成

SCIM プロバイダーを作成して、その SCIM プロバイダーから REST メッセージを使用してリソースタイプとスキーマ情報をフェッチします。SCIM プロバイダー内のリソースを更新するには、HTTP メソッド (PUT または PATCH) の設定を有効にします。

始める前に

注:
サンプルの SCIM プロバイダーはベースシステムに含まれています。これを使用して自社の要件に基づいて設定しても、新しいレコードを作成してもかまいません。

必要なロール：admin

手順

1. 移動先 すべて > **SCIM** クライアント > **SCIM** プロバイダー.
2. [SCIM プロバイダー] ページで、[新規] をクリックします。
3. フォームのフィールドに入力します。

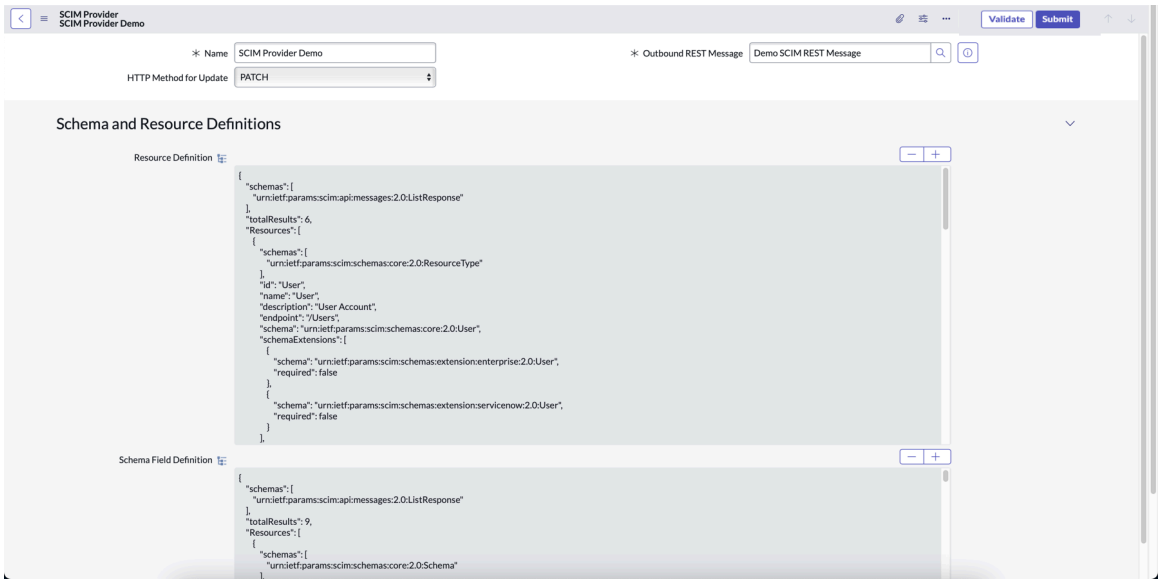
[SCIM プロバイダー] フォーム

フィールド	説明
名前	SCIM プロバイダーの名前
送信 REST メッセージ	SCIM プロバイダーの API を呼び出すために使用するメッセージ。詳細については、「REST メッセージの作成」を参照してください。
更新のための HTTP メソッド	リソースマッピングの更新に使用する HTTPS メソッドのタイプ。PATCH または PUT メソッドは、既存のリソースのプロビジョニング中にクライアントが ID リソースを更新するときに使用可能です。

注:
- [リソース定義] および [スキーマフィールド定義] フィールドは、SCIM プロバイダーの */ResourceTypes* および */Schemas* 公開エンドポイントから取得されます。これらのフィールドは、REST メッセージの選択後に自動入力されます。
- SCIM プロバイダーで REST メッセージ、スキーマ、またはリソースタイプが更新された場合は、 [リフレッシュ] をクリックしてから [更新] をクリックし、[リソース定義] フィールドと [スキーマフィールド定義] フィールドを更新します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



4. [送信] をクリックします。

タスクの結果

SCIM プロバイダーの詳細が正常に作成されます。SCIM プロバイダーリソースマッピングを使用して、SCIM プロバイダーの詳細をユーザーやグループなどのリソースにマッピングします。詳細については、「SCIM プロバイダーリソースマッピングの作成」を参照してください。

SCIM プロバイダーリソースマッピングの作成

特定のリソースタイプと SCIM プロバイダーの ServiceNow 属性に対する SCIM 属性のマッピングを定義します。

始める前に

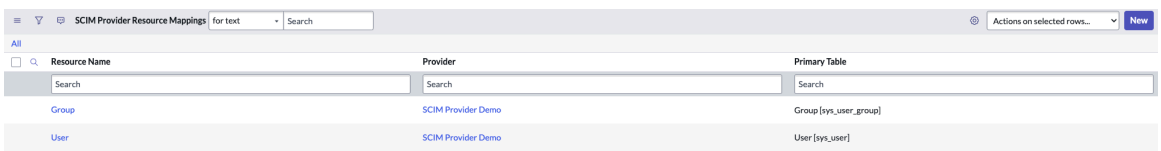
必要なロール：admin

手順

1. 移動先 すべて > **SCIM** クライアント > **SCIM** プロバイダーリソースマッピング.

SCIM プロバイダーリソースマッピングには、デフォルトでユーザーとグループのマッピングが入っています。

> **注:**
> このユーザーやグループのマッピングの中に、参考として使用できるサンプルマッピングが入っています。ユーザーリソースやグループリソースに基づいてマッピングを作成することもできます。



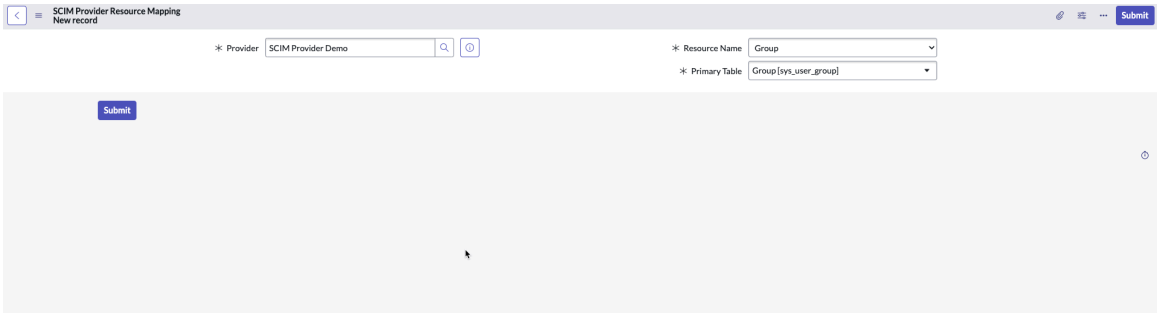
2. [新規] をクリックして、リソースマッピングを作成します。

3. フォームのフィールドに入力します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

リソースマッピング

フィールド	説明
プロバイダー	SCIM プロバイダーの名前。SCIM プロバイダーの作成時に設定されたプロバイダー名を参照します。
リソース名	マッピングを定義する必要があるリソース。
プライマリテーブル	マッピングされるリソースの sys_id を含むテーブル。



4. [送信] をクリックします。

タスクの結果
レコードが作成され、[SCIM プロバイダーリソースマッピング] ページに表示されます。SCIM 属性マッピングを使用して、スキーマから属性をさらにマッピングします。詳細については、「SCIM 属性マッピングの作成」を参照してください。

SCIM 属性マッピングの作成

SCIM 属性マッピングを作成し、それを ServiceNow テーブルのフィールドに対するリソースの単一のソースとして使用します。

始める前に
必要なロール：admin

このタスクについて
属性マッピングのタイプとその説明は次のとおりです。

属性マッピングのタイプ

属性マッピングのタイプ	説明
直接	SCIM 属性は、[データベーステーブル名] フィールドと [データベースフィールド名] フィールドを使用して入力されます。
定数	SCIM 属性は、指定されたデフォルト値を活用して入力されます。
スクリプト/カスタム	SCIM 属性は、スクリプトの戻り値を活用して入力されます。この属性では、[スクリプトを実行] オプションを有効にする必要があります。

自動翻訳

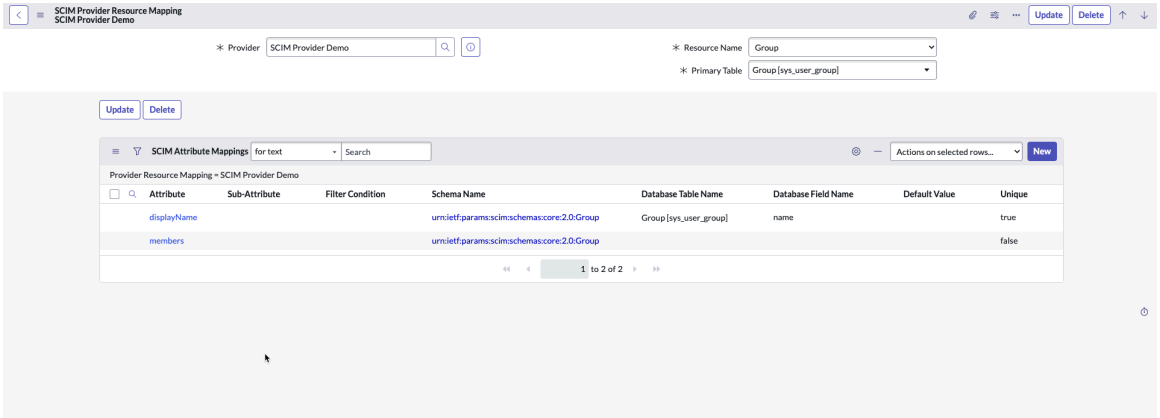
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注:

- パスワード属性はサポートされていません。
- ユーザーリソースおよびグループリソースのサンプルの属性マッピングは、ベースシステムに入っています。これを使用して自社の要件に基づいてマッピングを設定しても、新しいレコードを作成してもかまいません。

手順

1. 移動先 すべて > **SCIM** クライアント > **SCIM** プロバイダーリソースマッピング.
2. 設定用に作成された SCIM リソースマッピングを選択しました。
3. [SCIM 属性マッピング] 関連リストで [新規] をクリックします。



4. フォームのフィールドに入力します。

[SCIM 属性マッピング] フォーム

フィールド	説明
プロバイダーリソースマッピング	プロバイダーとリソースの組み合わせに対する属性マッピング。 このフィールドが自動的に入力されない場合は、検索オプションを使用します。プロバイダーリソースマッピングのレコードを選択します。
スキーマ名	マッピングを定義する必要のある SCIM 属性のスキーマ名。 `urn:ietf:params:scim:schemas:core:2.0:User` など。
属性	マッピングを定義する必要のある属性。`userName` など。
サブ属性	マッピングを定義する必要のあるサブ属性 (あれば)。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	たとえば、*name.familyName* のような複合的なタイプ属性がある場合、属性は **name** で、サブ属性は **familyName** となります。
フィールドタイプ	SCIM 属性のデータタイプ。このフィールドは、SCIM プロバイダーによって定義されたスキーマから自動的に入力されます。 **boolean** など。
複数値	属性に割り当てられる複数の値。1 つの属性に、仕事用メール、自宅用メール、その他のメールなど複数の値を設定できます。 *emails* など。 このフィールドは、SCIM プロバイダーによって定義されたスキーマを使用して入力されます。
フィルター条件	複数の値を持つ属性には、[フィルター条件]を使用して指定できる追加情報を入力することができます。フィルター条件の選択肢は、SCIM プロバイダーによって定義されたスキーマを使用して入力されます。 たとえば、*phoneNumbers* 属性には、職場、モバイル、自宅といった複数のタイプがあります。
一意	SCIM クライアントと SCIM プロバイダーのシステム間でリソースを一意に識別するオプション。複数値の属性を一意としてマークすることはできません。 たとえば、ユーザーリソースでは、*username* 属性を一意とすることができます。
データベーステーブル名	このフィールドを使用して、属性テーブル名を ServiceNow テーブル名にマッピングします。直接の属性マッピングを選択した場合は、このフィールドを定義する必要があります。 たとえば、*username* SCIM 属性は [データベーステーブル名] フィールドの [ユーザー] フィールドにマッピングできます。
データベースフィールド名	[データベースフィールド名] フィールドでは、SCIM 属性を、その SCIM 属性でマッピングされる ServiceNow フィールド名にマッピングします。直接の属性マッピングを選択した

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	場合は、このフィールドを定義する必要があります。 たとえば、*username* SCIM 属性は [データベースフィールド名] フィールドの [ユーザー **ID]** フィールドにマッピングできます。
デフォルト値	SCIM プロバイダーに渡されるデフォルト値 の詳細。 フィールドの直接の属性マッピングが null を返す場合、またはデフォルトを使用してハードコードされた値を返せる場合に使用できます。 ハードコードされた値の場合は、データベーステーブル名とフィールド名を [なし] にする必要があります。 たとえば、仕事用メールのプライマリサブ属性の値は **true**としてハードコードできます。
スクリプトを実行	スクリプトを介して属性の値をフェッチするオプション。 このオプションは、フィルター条件を含まない複数値の属性に必要です。複合タイプの属性の場合、スクリプトは属性またはサブ属性レベルで値を指定できます。 たとえば、グループリソースの [メンバー] 属性にはフィルター条件がありません。したがって、スクリプトオプションは [メンバー] 属性の親属性レベルで定義する必要があります。
スクリプト	属性値をフェッチするために使用するスクリプト。 スクリプトの戻り値のタイプは、文字列、または文字列として変換された JSON である必要があります。 スクリプトの出力は、その属性に対してプロバイダーが想定する適切な形式である必要があります。

5. [送信] をクリックします。

属性マッピングの参照

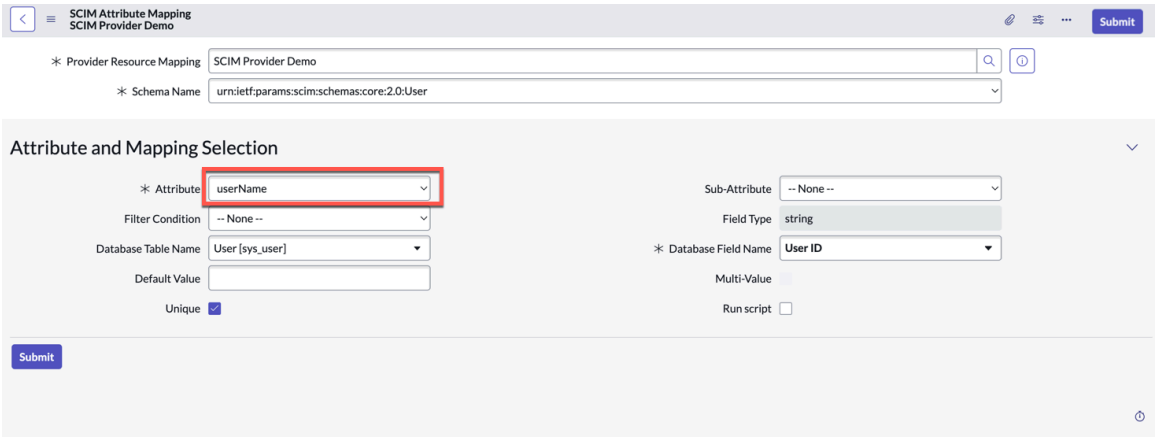
属性マッピングを使用すると、ServiceNow のテーブルフィールドに対するリソースの単一のソースとして属性を使用できます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

属性

マッピングを定義する必要のある属性。*userName* など。

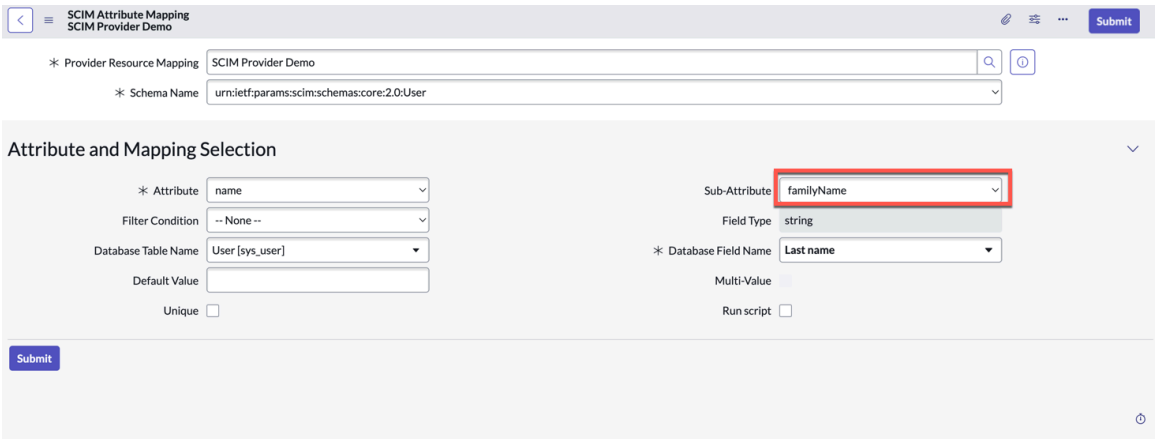


サブ属性

マッピングを定義する必要のあるサブ属性を選択します (ある場合)。

たとえば、*name.familyName* のような複合的なタイプ属性がある場合、属性は *name* で、サブ属性は *familyName* となります。

ユーザー名のような単純な属性の場合、[サブ属性] の値は [なし] になります。



フィルター条件

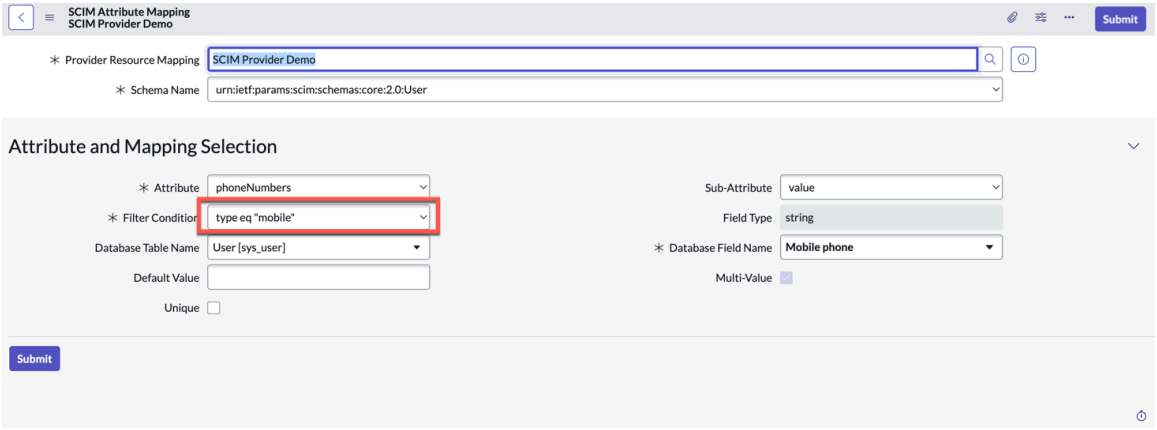
複数値の属性には、フィルター条件を使用して指定可能な追加情報を設定できます。フィルター条件の選択肢は、SCIM プロバイダーによって定義されたスキーマを使用して入力されます。

たとえば、*phoneNumbers* 属性には、職場、モバイル、自宅といった複数のタイプがあります。

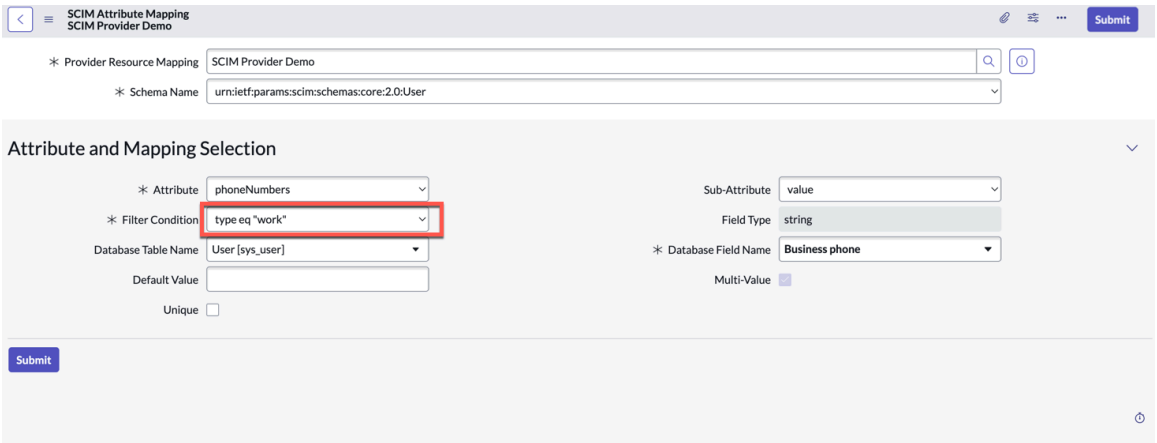
一連の可能な値からフィルター条件を指定できます。たとえば、*phoneNumber* 属性にはフィルター条件を **type eq "mobile"** として設定できます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



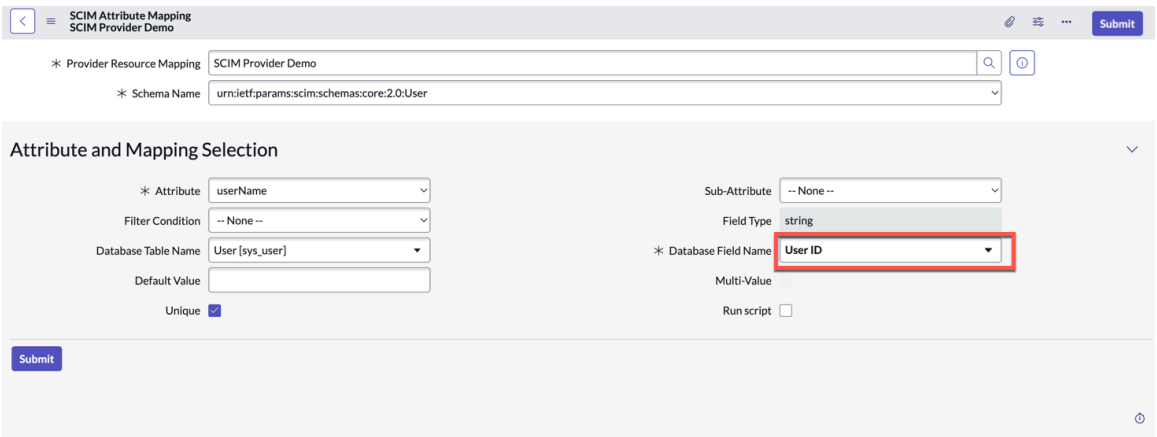
phoneNumber 属性には **type eq "work"** のフィルター条件を設定することもできます。



データベースフィールド名

直接の属性マッピングのオプションを選択した場合は、この属性を定義する必要があります。[データベースフィールド名] フィールドには SCIM 属性がマッピングされた ServiceNow フィールド名が表示されます。

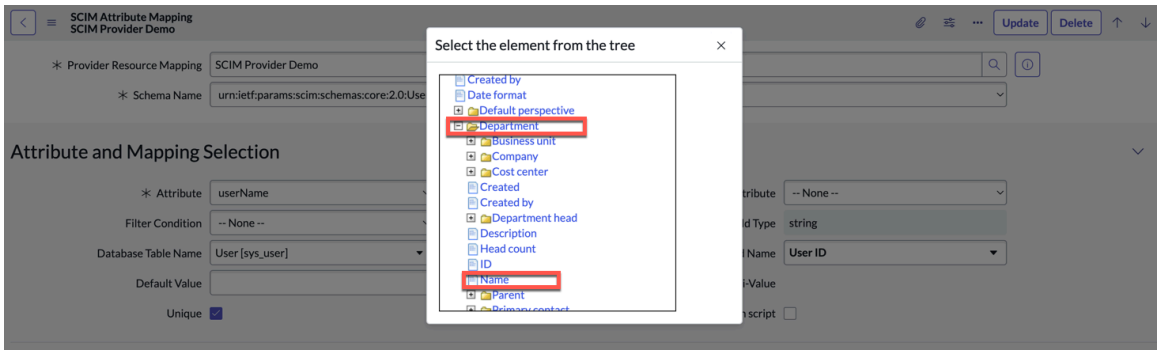
たとえば、*username*という SCIM 属性は、ユーザーには [データベーステーブル名] フィールドとして、ユーザー ID フィールドには [データベースフィールド名] フィールドとしてマッピングできます。



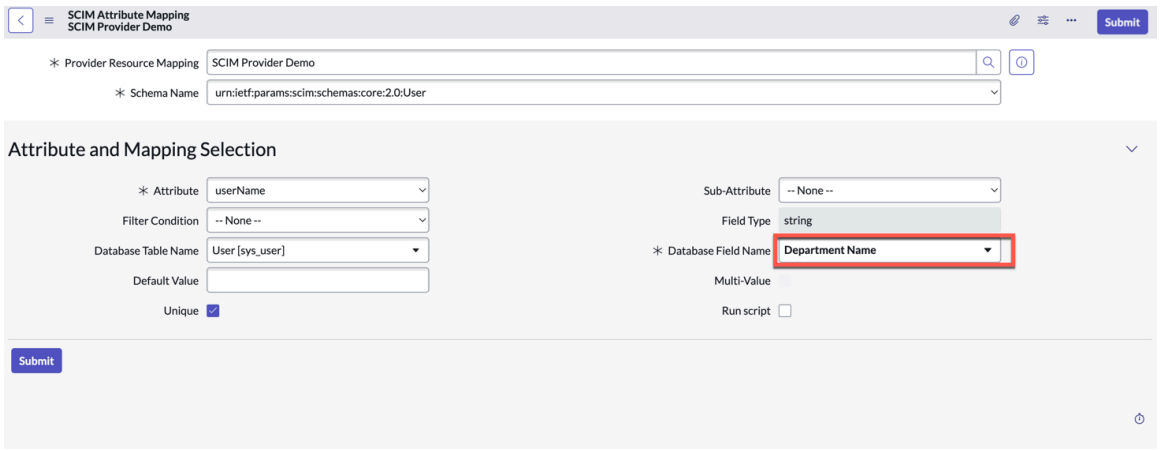
[データベースフィールド名]を使用してドット連結することもできます。たとえば、部門という SCIM 属性は [部門名] フィールドにマッピングできます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



ここでは、[データベーステーブル] は [ユーザー] で、[データベースフィールド名] は [部門名] です。

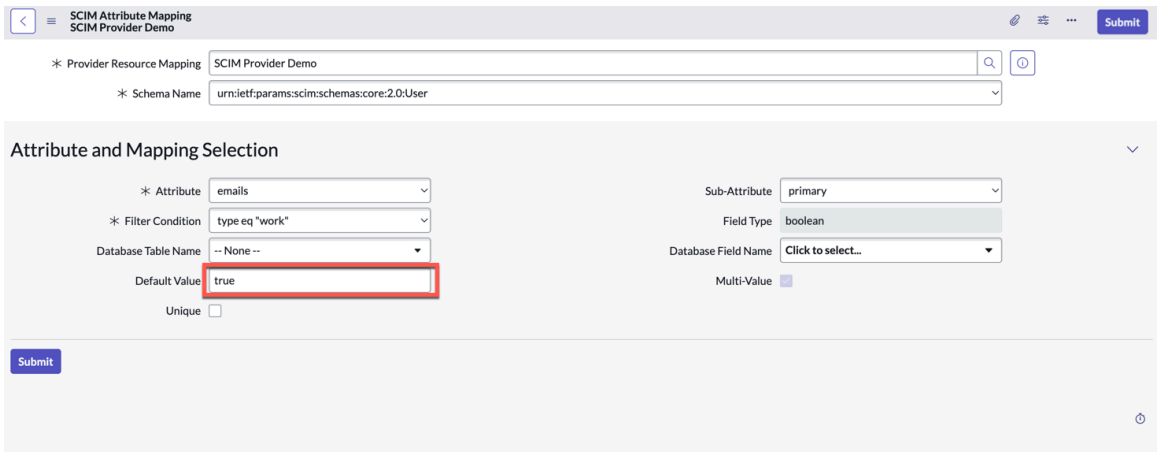


デフォルト値

そのフィールドの直接の属性マッピングが null を返すと、デフォルト値が SCIM プロバイダーに渡されます。そのデフォルト値を使用してハードコードされた値を返すこともできます。

ハードコードされた値の場合は、データベーステーブル名とフィールド名を [なし] にする必要があります。

たとえば、仕事用メールのプライマリサブ属性の値は **true**としてハードコードできます。



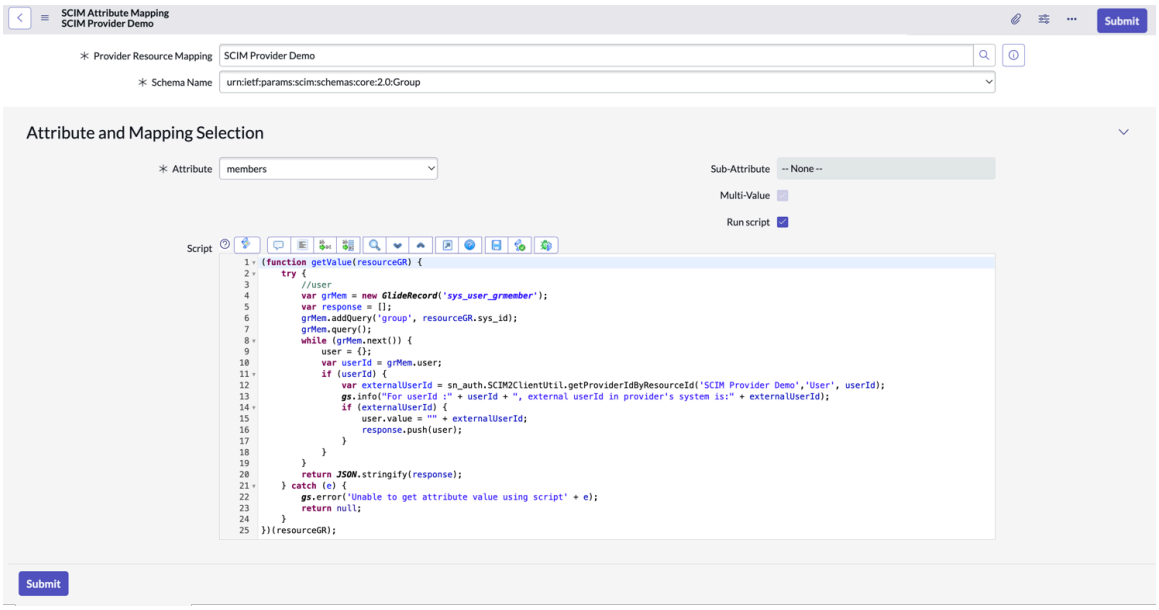
スクリプト

属性値をフェッチするためにはスクリプトを使用します。スクリプトの戻り値のタイプは常に、文字列、または文字列として変換された JSON である必要があります。スクリプトの出力は、その属性に対してプロバイダーが想定する適切な形式である必要があります。

自動翻訳

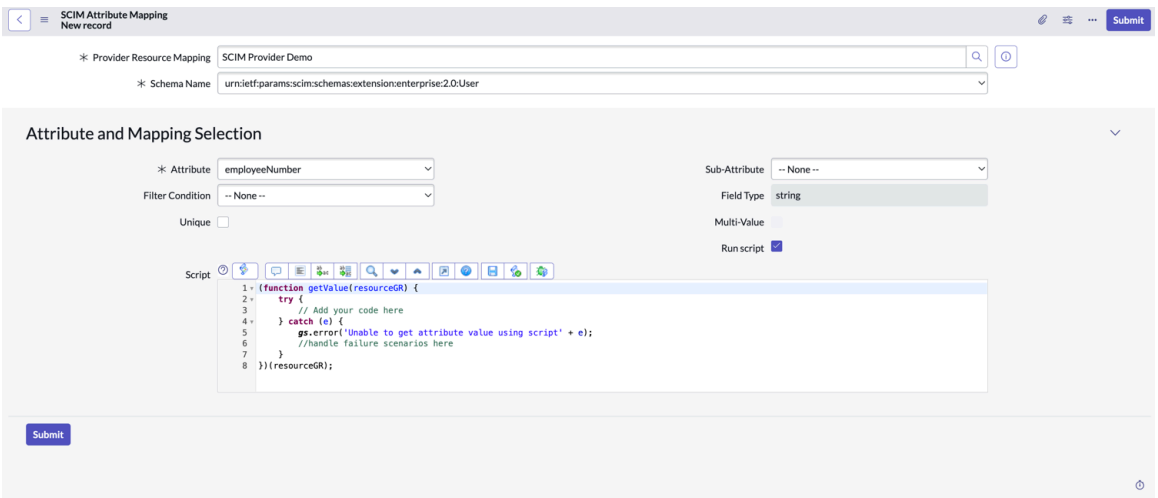
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

複数値の属性のサンプルスクリプトは次のとおりです。



スクリプトの出力には、文字列化された JSON アレイが必要です。

単純な値の属性のサンプルスクリプトは次のとおりです。



スクリプトの出力は文字列である必要があります。

SCIM クライアントのトラブルシューティング

トラブルシューティングのアクションは、SCIM クライアントの設定や実行時の一般的な問題解決に役立ちます。

トラブルシューティング

問題	アクション
応答に含まれるメッセージは次のとおりです。 “message":"Unable to access the table core_company with id: 0c441abbc6112275000025157c651c89, Please cross check the Access control rules"	このメッセージは、API がユーザーコンテキストで呼び出され、ユーザーがテーブルにアクセスできない場合に表示されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

トラブルシューティング (続く)

問題	アクション
	スクリプト可能 API がシステムコンテキストで呼び出されていることを確認する必要があります。
応答に含まれるメッセージは次のとおりです。 `{"message":"User Not Authenticated","detail":" Required to provide Auth information”}`	• 対応する REST メッセージによってトークンが生成され、トークンが有効であることを確認してください。 • スクリプト可能 API がシステムコンテキストで呼び出されていることを確認してください。
応答に含まれるメッセージは次のとおりです。 `Script execution failed, the reason is: Cannot cast java.lang.Integer to java.lang.String`	SCIM 属性マッピングで、この問題のあるスクリプトからフェッチするようにフィールドが定義されている場合は、戻り値のタイプが常に文字列であることを確認します。
応答に含まれるメッセージは次のとおりです。 `"status": "400", "scimType": "invalidValue", "detail": "Manager id : 02826bf03710200044e0bfc8bcbe5ds8 doesn't exist"`	ID を期待する SCIM 属性では、その ID は常にプロバイダーシステムの ID です。ペイロードで渡される ID がプロバイダーシステムで有効であることを確認してください。

トラブルシューティングの際に確認する領域

SCIM クライアント使用時のエラーのトラブルシューティングの際に確認可能な領域の一部を以下に示します。

- スクリプト可能 API の実行中に問題が見つかった場合は、「SCIM クライアントログ」セクションを参照してください。

ログのフィールド

フィールド	説明
要求 ID	呼び出されたスクリプト可能 API を表す固有の ID。
SCIM プロバイダー	API の呼び出し対象となるプロバイダー名。
リソース	API の呼び出し対象となるリソースの名前。
リソース ID	API の呼び出し対象となる ID。削除の場合、ID はプロバイダーシステムのリソース ID を表します。この ID はクライアントシステムにあります。
アクション	呼び出される API。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
ステータス	ログのステータス。成功または失敗になります。
メッセージ	成功またはエラーメッセージ。エラーメッセージは、SCIM プロバイダーから出される場合と、SCIM クライアントの構成の問題が原因の場合があります。

- 発信コールを設定および表示して、要求の本文を確認します。詳細については、「送信 Web サービスのログ記録」を参照してください。
- コンテンツタイプを追加し、サンプルをテストし、対応するプロバイダーの REST メッセージ内の対応する [HTTP メソッド] フォームに移動して、ログのレベルを更新します。
- 要求の本文が切り捨てられている場合は、システムプロパティ `glide.outbound_http.content.max_limit` を使用して上限を増やします。

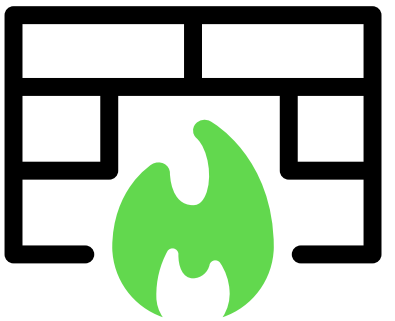
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

アクセス管理

アクセス管理を使用して ServiceNow® インスタンスに安全にアクセスできます。

認証

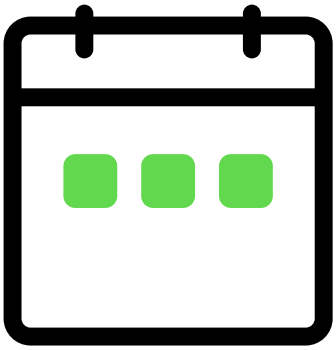


ServiceNow® の認証は、インスタンスにアクセスするユーザーの ID を検証し、ユーザーのロールまたは職務に一致する機能に対してユーザーを許可します。

接続と資格情報

ディスカバリー、Service Mapping、および Cloud Management にコンピューターまたはネットワークデバイスへのアクセス権を得る、またはオーケストレーションを使用して作業を実行するには、資格情報と接続情報が必要です。

ログインと認証のセキュリティ



インスタンスへのアクセスを制御するログインセキュリティオプションを設定します。

Web サービスセキュリティ

基本認証、相互認証、または WS-Security を使用してセキュリティを適用します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

認証

ServiceNow® の認証は、インスタンスにアクセスするユーザーの ID を検証し、ユーザーのロールまたは職務に一致する機能に対してユーザーを許可します。

接続と資格情報

ディスカバリー、サービスマッピング、およびクラウド管理用にコンピューターまたはネットワークデバイスへのアクセス権を得る、またはオーケストレーションを使用して作業を実行するには、認証情報と接続情報が必要です。

ログインと認証のセキュリティ

インスタンスへのアクセスを制御するログインセキュリティオプションを設定します。

Web サービスセキュリティ

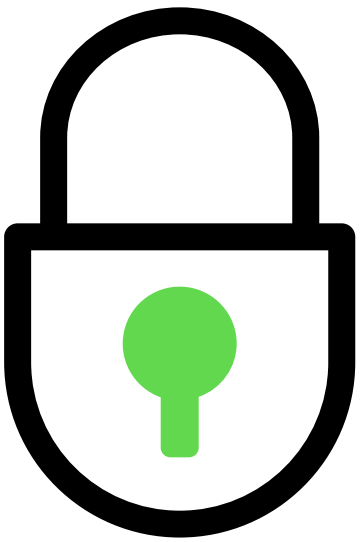
基本認証、相互認証、または WS-Security を使用してセキュリティを強制します。

認証

ServiceNow® の認証は、インスタンスにアクセスするユーザーの ID を検証し、ユーザーのロールまたは職務に一致する機能に対してユーザーを許可します。

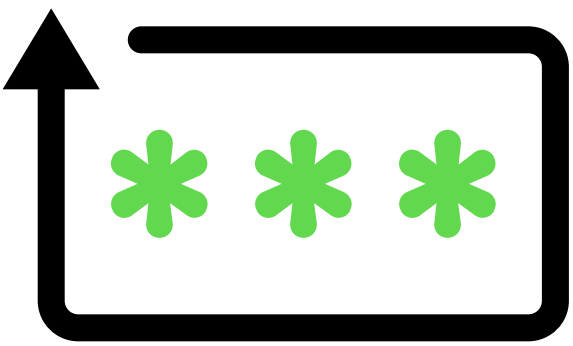
開始するには

自動翻訳



複数プロバイダーの **Single Sign-on (SSO)**

データベース内に一致するユーザーアカウントがある ID プロバイダーで構成されたユーザー名とパスワード。



OAuth 受信と送信

データベース内に一致するユーザーアカウントがある OAuth ID プロバイダーのユーザー名とパスワード。

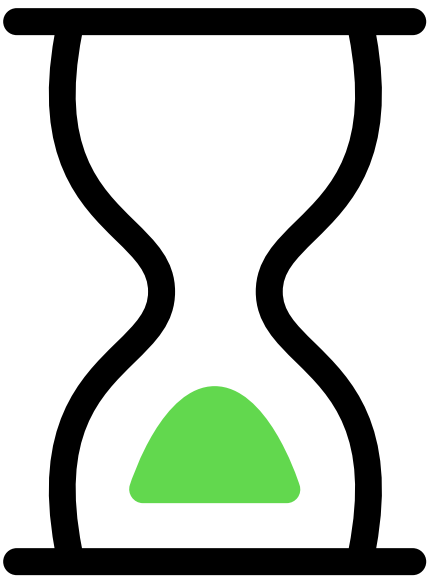
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

API アクセスポリシー

API アクセスポリシーは、API へのアクセス権限と期間を定義します。

ダイジェストトークン認証

テーブル内のユーザー名とシークレットは、SHA1、SHA 256、MD5 などのユーザー固有のハッシュ動作を実行します。この値は、URL サフィックスの一部として追加する必要があります。これはクエリーパラメーターで機能します。



時間制限付き認証

マルチファクター認証 **(MFA)**

QR コードからのパスコード。インスタンス名、ユーザー名またはユーザーアカウント情報、および認証用のコードなどの情報を持つ秘密コードが下部に含まれています。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

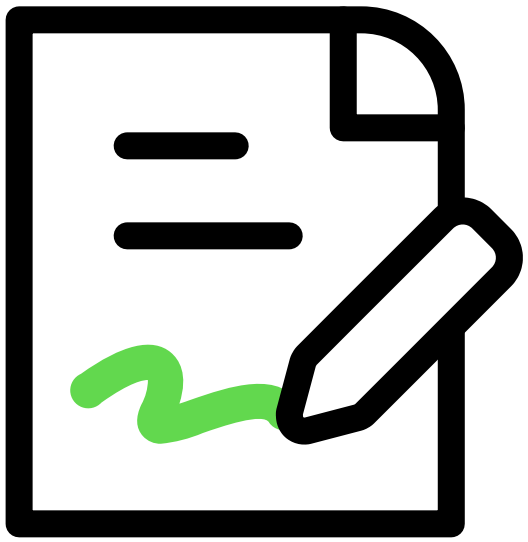
でのリンクベースの認証の構成

[qa: BEGIN review][End]

ServiceNow インスタンス構成されたリンクは、メールまたは SMS を介してユーザーと共有でき、ユーザーはそれらのリンクを使用してインスタンスにログインできます。

証明書ベースの認証

ユーザー名とパスワードの代わりにユーザーにマップされた一意の PEM エンコード証明書。



自己登録

インスタンスデータベースのユーザーレコード内のユーザー名とパスワード。

Zero Trust アクセス

LDAP

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Zero Trust アクセスでは、ユーザーの ID 検証とリスクアセスメントの後にのみ、アプリケーションとデータへのすべてのアクセスが最小限の権限で付与されます。	データベース内に一致するユーザーアカウントがある LDAP アカウントのユーザー名とパスワード。

ユーザーの認証には、数種類の異なる方法を使用できます。ユーザーの資格情報は、各方法に対して保存された各種資格情報と照合されます。

注:

- Okta SSO プラグインは廃止されました。
- 認証処理に影響するセキュリティプロパティの詳細については、「インスタンスセキュリティ強化設定」の「アクセス制御」を参照してください。
- Multiple Provider SSO アプリケーションを介して SAML および Digest Authentication を使用できます。

適応認証

適応認証ポリシーフレームワークを使用すると、適切なタイミングで適切なユーザーにコンテキスト認証コントロールを適用できます。適応認証では、認証ポリシーを使用して認証要求を評価してから、指定されたポリシー条件に基づいてインスタンスへのアクセスを拒否または許可します。

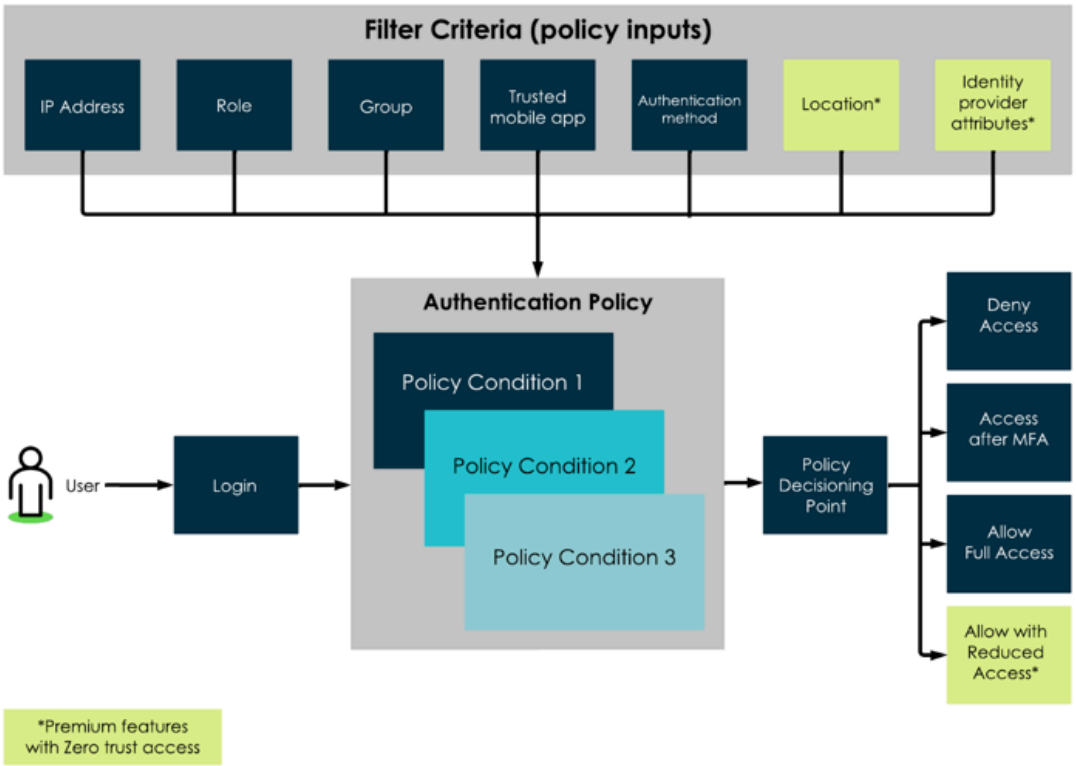
適応認証ポリシーとコンテキストを使用して、IP アドレス、ユーザーロール、ユーザーグループなどの基準に基づいて、ユーザーおよび API のインスタンスへのアクセスを制限します。セキュリティ要件に従って、ビルトイン認証ポリシーを設定できます。

たとえば、管理者は [*Allow Access Policy*] を使用して、信頼できる IP アドレス範囲内にあり、特定のロールのメンバーであるユーザーからのログインのみを許可するように設定できます。*Post-authentication context*に割り当てると、アクセスポリシーは信頼できない IP アドレスからのアクセスを拒否します。

インスタンスの言語でカスタムメッセージを設定するには、sys_ui_message.list にキーと値のペアを追加し、sys_ui_message レコードを更新する必要があります。誤ったパスワードでログインすると、優先言語のカスタムメッセージが表示されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



適応認証コンポーネント

認証ポリシー

認証ポリシーは、指定されたポリシー条件に基づいて認証要求を評価し、ポリシー条件評価の出力に応じてアクセスを許可または拒否します。たとえば、[アクセス許可ポリシー] で指定されたすべてのポリシー条件が true と評価された場合にのみ、アクセスが許可されます。

認証ポリシーは、フィルター基準によって提供される情報を使用してポリシーの条件と比較し、インスタンスへのアクセスを許可するかどうかを決定します。たとえば、フィルター基準はユーザーの IP アドレスを提供し、ポリシー条件はアクセスを許可する前にこのアドレスが特定の範囲内かどうかを判断します。認証ポリシーの詳細については、「認証ポリシー」を参照してください。

認証ポリシーのコンテキスト

認証ポリシーのコンテキストは、ログインプロセス中にポリシーを強制適用する方法とタイミングを定義します。事前認証コンテキストは、ユーザーにログイン画面が表示される前に実行されます。認証後コンテキストは、ユーザーが資格情報を入力した後に実行されます。ポリシーを使用するには、ポリシーコンテキストにアサインする必要があります。これらのコンテキストの詳細については、「認証ポリシーのコンテキスト」を参照してください。

フィルター基準

フィルター基準 (ポリシー入力とも呼ばれます) は、ポリシー条件の入力として使用されます。ポリシー条件では、これらの入力を使用して認証要求の要件を検証して満たします。これらの入力は、ユーザーロール、IP 範囲、ID プロバイダーなどの情報を提供します。フィルター基準の詳細については、「フィルター基準」を参照してください。

認証プロパティ

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

認証プロパティを使用して、インスタンスで適応認証を有効にするかどうかを制御します。プロパティを使用してデバッグを有効にし、アクセスがブロックされたときにユーザーに表示されるメッセージを定義することもできます。これらのプロパティの詳細については、「適応認証プロパティの設定」を参照してください。

REST API アクセスポリシー

適応認証フレームワークのフィルター基準を使用して、受信した ServiceNow REST API へのアクセスを制限できます。詳細については、「REST API アクセスポリシー」を参照してください。

ドメイン分離と適応認証

適応認証は、認証ポリシー条件レベルでドメイン分離されたインスタンスでサポートされています。ポリシー条件は、レコードの ドメイン [sys_domain] フィールドのドメインに影響します。グローバルドメインのポリシー条件は、すべてのドメインに影響します。

適応認証のアクティブ化

admin ロールを持っている場合は、適応認証の適応認証プラグイン (com.snc.adaptive_authentication) をアクティブ化できます。

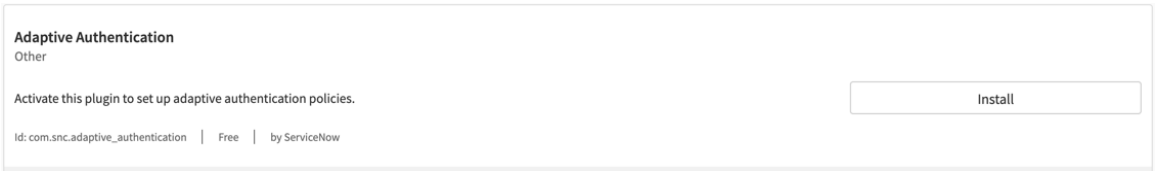
始める前に

必要なロール：admin

このタスクについて

手順

1. 移動先 すべて > システムアプリケーション > 利用可能なすべてのアプリケーション > すべて.
2. フィルター基準と検索バーを使用して適応認証 (com.snc.adaptive_authentication) プラグインを検索します。



名前または ID でプラグインを検索できます。プラグインが見つからない場合は、ServiceNow 担当者から要求する必要があります。

3. [インストール] を選択して、[プラグインをアクティブにする] ダイアログボックスで、[アクティブ化] をクリックします。

> **注:**
> ドメイン分離と代理管理者がインスタンスで有効になっている場合、管理ユーザーはグローバルドメインに含まれている必要があります。それ以外の場合、次のエラーが表示されます： 別の操作が実行されているため、アプリケーションのインストールは利用できません：<プラグイン名> のプラグインの有効化。

次のタスク

認証ポリシーを構成して、インスタンスにコンテキスト認証制御を適用します。

ポリシーを設定した後、[認証ポリシーの有効化 **(Enable Authentication Policy)]** ポリシーを使用して適応認証を有効にします。適応認証プロパティの詳細については、「適応認証プロパティの設定」を参照してください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィルター基準

フィルター基準 (ポリシー入力とも呼ばれます) は、ポリシー条件の入力として、認証要求の要件を検証し、その要件を満たすために使用されます。

フィルター基準を使用して、ユーザーの IP アドレス、ロール、グループなどの情報認証ポリシーを指定します。ポリシーの [ポリシー条件] セクションにこれらの基準を追加します。

適応認証で使用されるフィルター基準は 7 種類あります。認証ポリシーでは、これらの基準を 1 つ以上使用して認証要求を評価できます。

フィルター基準タイプ

タイプ	説明
IP フィルター基準	IP フィルター基準を使用して、ユーザーの IP アドレスに基づいてユーザーをフィルタリングします。IPv4 と IPv6 の両方がサポートされています。
ロールフィルター基準	ロールフィルター基準を使用して、ユーザーのロールに基づいてユーザーをフィルタリングします。
グループフィルター基準	グループフィルター基準を使用して、ユーザーが属するユーザーグループに基づいてユーザーをフィルタリングします。
場所のフィルター基準	場所のフィルター基準を使用して、ユーザーの場所に基づいてユーザーをフィルタリングします。
ID プロバイダー属性のフィルター基準	IdP からの SAML 応答から受信した ID プロバイダー属性を認証のフィルター基準として使用します。

汎用基準

前述のタイプに加えて、4 種類の汎用的なフィルター基準があります。これらの基準はフィルターナビゲーターには表示されませんが、認証ポリシーにポリシー入力を追加するときに選択できます。

汎用的なフィルター基準タイプ

タイプ	説明
認証スキーム	ユーザーの認証スキームに基づいてフィルタリングするために使用します。この基準は、次の 2 つのオプションを持つ選択肢タイプです。 • ローカルログインを示すユーザー名とパスワード☒ • マルチ SSO (SAML、OIDC、または Digest) ベースのログインを示す SSO。 **注:** **Integration - Multiple Provider Single Sign-On Installer** [com.snc.integration.sso.multi.installer] プラグインがインストールされている場合のみフィルター基準を使用できます。
Identity Provider	ユーザーの ID プロバイダーに基づいてフィルタリングするために使用します。認証スキーム基準とともに使用して、ログインプロセスを細やかに制御します。この基準は、**ID** プロバイダー [sso_properties] テーブルへの参照です。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

汎用的なフィルター基準タイプ (続く)

タイプ	説明
	注: **Integration - Multiple Provider Single Sign-On Installer** [com.snc.integration.sso.multi.installer] プラグインがインストールされている場合のみフィルター基準を使用できます。
ロールベースの MFA	ロールベースの MFA 機能に基づいてフィルタリングするために使用します。この基準は、ユーザーに対してロールベースの MFA が有効かどうかを示すブールタイプのフィルター基準です。☒
ユーザーベースの MFA	ユーザーベースの MFA 機能に基づいてフィルタリングするために使用します。この基準は、ユーザーに対してユーザーベースの MFA が有効かどうかを示すブーリアン型のフィルター基準です。
信頼できるモバイルアプリ	モバイルアプリからのインスタンスへのアクセスを有効にするための信頼できるモバイルアプリフィルター。

IP フィルター

IP フィルター基準を使用して、ユーザーの IP アドレスに基づいてユーザーをフィルタリングします。IPv4 と IPv6 の両方がサポートされています。

IP フィルター基準を使用すると、ユーザーの IP アドレスに基づいてユーザーをフィルタリングできるようになります。特定のアドレスまたはアドレス範囲へのアクセスを許可または拒否するように認証ポリシーを設定できます。

IP フィルター基準の作成

IP フィルター基準を使用すると、ユーザーの IP アドレスに基づいてユーザーをフィルタリングできるようになります。特定のアドレスまたはアドレス範囲へのアクセスを許可または拒否するように認証ポリシーを設定できます。

始める前に
必要なロール：管理者

手順

1. 移動先 すべて > 適応認証 > フィルター基準 > **IP** フィルター基準.
2. [新規] をクリックします。
3. フォーム上で、以下のフィールドに記入します。

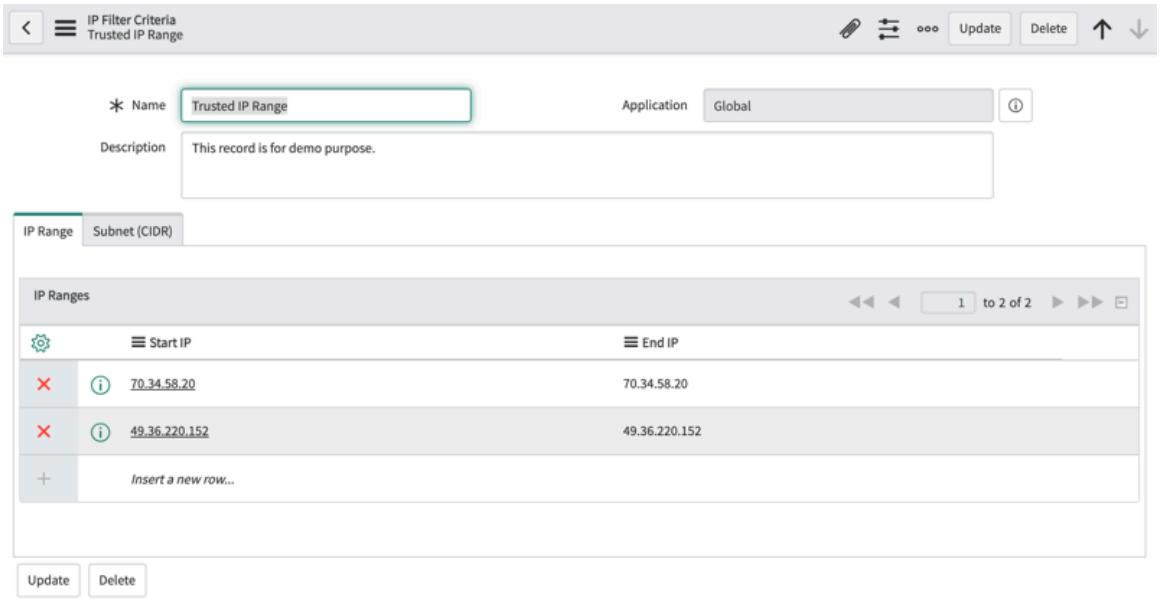
[IP フィルター基準] フォーム

フィールド	説明
名前	IP ネットワークを識別する名前
説明	IP ネットワークの簡単な説明
アプリケーション	アプリケーションのスコープ

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

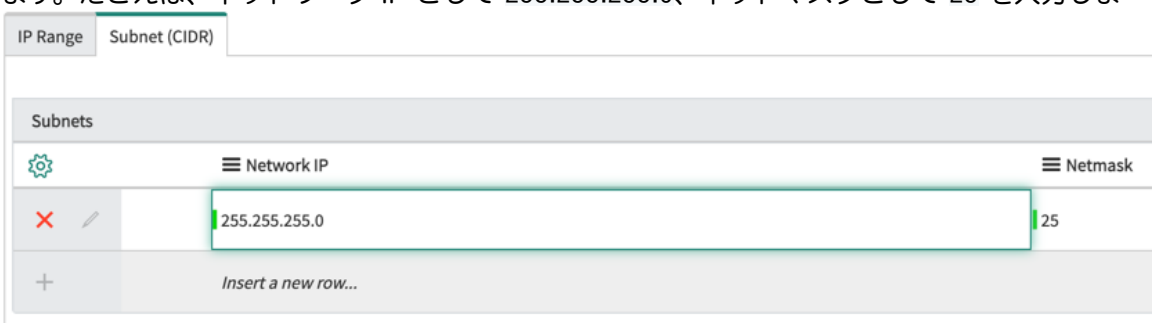
IP フィルター基準レコードの例



4. フォームヘッダーを右クリックし、[保存] をクリックします。
5. **[IP** 範囲] タブで、[新規行を挿入] をダブルクリックします。
   単一の IP アドレスまたは複数の IP アドレス範囲を入力できます。たとえば、IP アドレスの範囲の場合は、[開始 **IP]** 列に「 192.0.2.0」、[終了 **IP]** 列に「192.0.2.255」と入力します。

   注:
   単一の IP アドレスの場合は、[開始 **IP]** 列と [終了 **IP]** 列に同じ IP アドレスを入力する必要があります。[開始 **IP]** 列に IP アドレスを入力する際に、[終了 **IP]** 列を空白にしたままでレコードを保存してください。[終了 **IP]** 列には、[開始 **IP]** と同じアドレスが自動的に入力されます。

6. [サブネット **(CIDR)]** タブで、[新規行を挿入] をダブルクリックします。
   クラスレスドメイン間ルーティング (CIDR) 形式でネットワーク IP アドレスとネットマスクを入力します。たとえば、ネットワーク IP として 255.255.255.0、ネットマスクとして 25 を入力します。



ロールフィルター

ロールフィルター基準を使用して、ユーザーのロールに基づいてユーザーをフィルタリングします。

ロールフィルター基準を使用すると、ロールに基づいてユーザーをフィルタリングできるようになります。ユーザーロールのリストへのアクセスを許可または拒否するように認証ポリシーを設定できます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ロールフィルター基準の作成

ロールフィルター基準を使用すると、ロールに基づいてユーザーをフィルタリングできるようになります。ユーザーロールのリストへのアクセスを許可または拒否するように認証ポリシーを設定できます。

始める前に

必要なロール：管理者

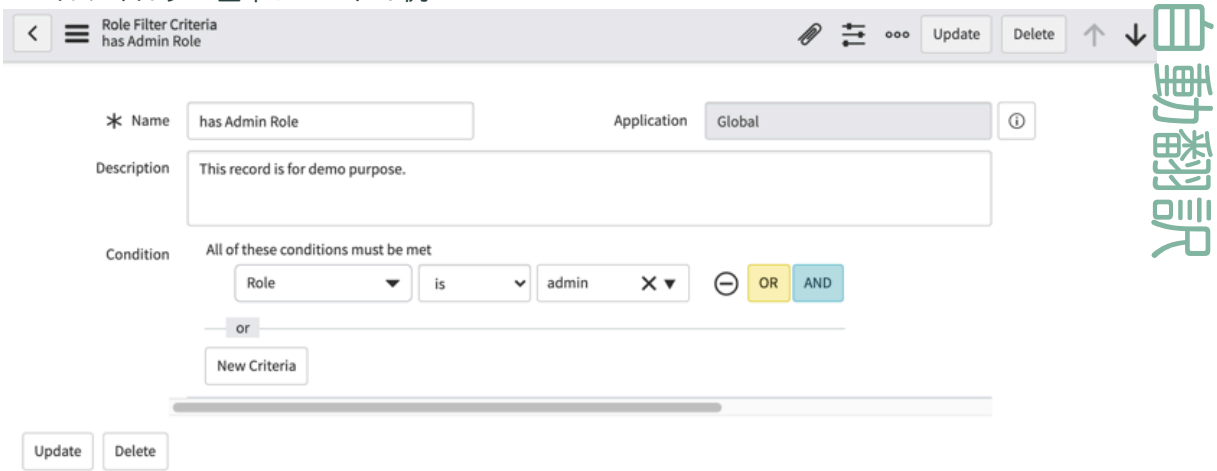
手順

1. 移動先 すべて > 適応認証 > フィルター基準 > ロールフィルター基準.
2. [新規] をクリックします。
3. フォーム上で、以下のフィールドに記入します。

[ロールフィルター基準] フォーム

フィールド	説明
名前	ロールを識別する名前
アプリケーション	アプリケーションのスコープ
説明	ロールの簡単な説明

ロールフィルター基準レコードの例

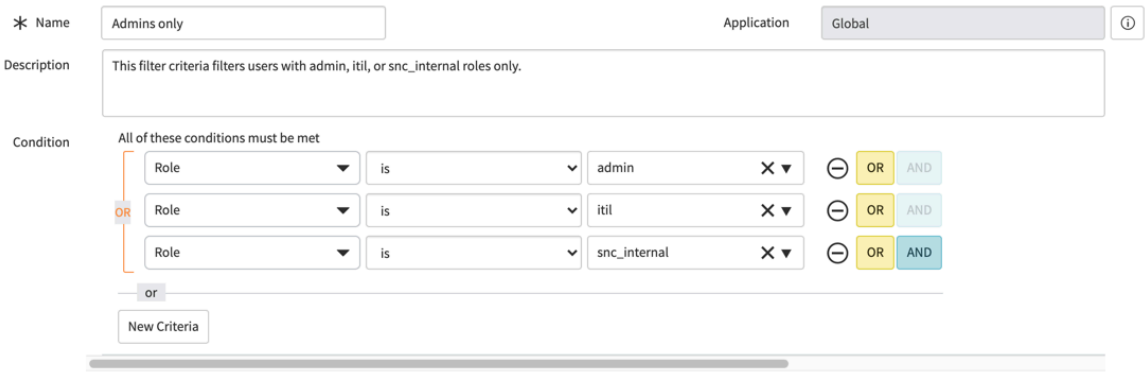


4. [基準のロール] から、[新規行を挿入] をダブルクリックします。
5. 条件ビルダーを使用して特定のロールの条件を作成します。たとえば、admin、itil、または snc_internal ロールを持つユーザーのみを許可する条件を作成できます。条件ビルダーの詳細については、「Create a condition statement using the condition builder (条件ビルダーを使用した条件ステートメントの作成)」を参照してください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注:
現在、ロールフィルター基準ではドット連結はサポートされていません。



グループフィルター

グループフィルター基準を使用して、ユーザーが属するユーザーグループに基づいてユーザーをフィルタリングします。

グループフィルター基準を使用して、ユーザーが属するユーザーグループに基づいてユーザーのアクセスを許可または拒否します。

グループフィルター基準の作成

グループフィルター基準を使用して、ユーザーが属するユーザーグループに基づいてユーザーのアクセスを許可または拒否します。

始める前に
必要なロール：管理者

手順

1. 移動先 すべて > 適応認証 > フィルター基準 > グループフィルター基準.
2. [新規] をクリックします。
3. フォーム上で、以下のフィールドに記入します。

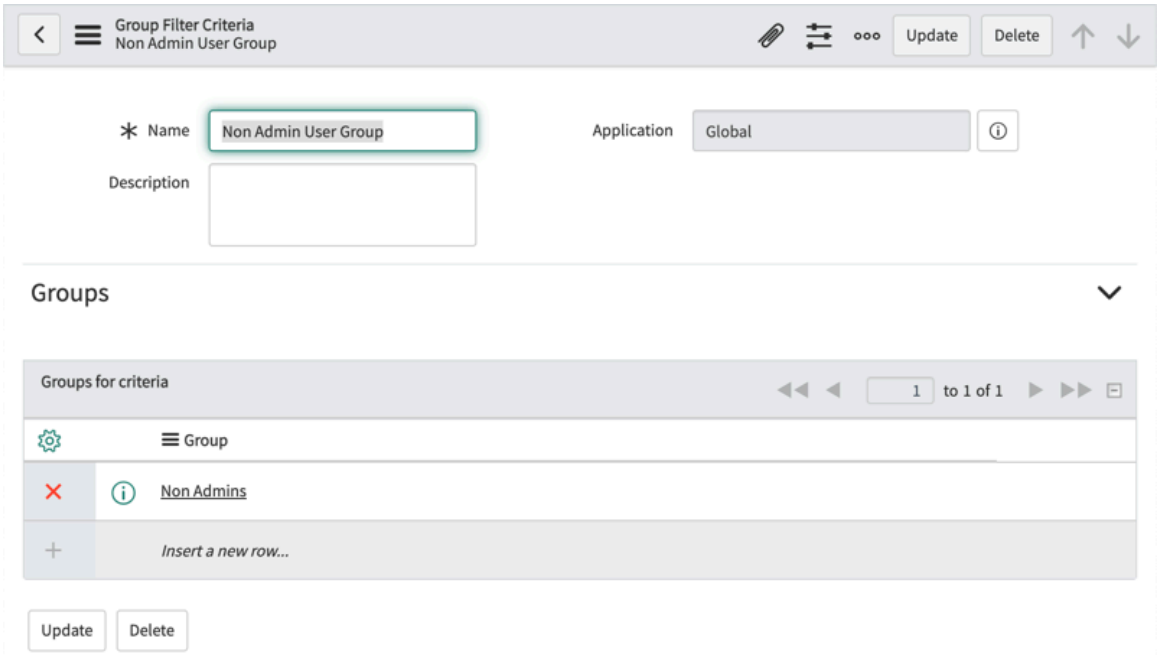
グループフィルター基準

フィールド	説明
名前	グループを識別する名前
説明	グループの簡単な説明
アプリケーション	アプリケーションのスコープ

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

グループフィルター基準レコードの例



4. [基準のグループ] タブから、[新規行を挿入] をダブルクリックします。
5. 検索アイコン ( ) をクリックして、ユーザーグループを検索して選択します。
6. 保存アイコン ( ) をクリックします。

場所フィルター

場所フィルター基準を、ユーザーの場所に基づいたユーザーのフィルター入力として使用できます。

場所フィルターは、管理者がデバイスの物理的な場所に基づいて認証ポリシーを作成するときに使用できるフィルター基準です。

注:

- 場所フィルター基準は有料のプラグインであり、ライセンスが必要です。
- このインスタンスは ADCv2 上にある必要があります。インスタンスが ADCv2 上にない場合、ユーザーの場所情報は利用できません。

場所フィルター基準を使用して、次のことを実行できます。

- 認証の要件を検証して満たすために、ポリシー条件に対するポリシー入力として機能します。
- [国] に基づいて適応認証ポリシーを作成する機能を提供します。
- 指定された地域へのインスタンスアクセスを許可するかどうかを指定します。
- 位置情報に基づく事前認証または事後認証ポリシーを使用して、次のことを行います。
  - 会社の判断により、プライバシーが厳格に制御されている地域以外の制裁対象国からアクセスを防止します。
  - 該当するプライバシー対象地域と会社の判断による範囲内でのみ、エリアへのアクセスを許可します。
  - 認証のための国ベースの許可リストを構成します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ユースケース

適応認証に場所フィルター基準を使用するユースケースの一部を次に示します。

- 国からのインスタンスへのアクセスをブロックします。
- 特定の国からのインスタンスへのアクセスのみを許可します。
- 国に基づいてログインするためのステップアップ認証または MFA を強制します。
- 国に基づいてユーザーのロールを削減または制限します。
- 場所フィルター基準は、MFA、Zero Trust Access (ZTA)、認証前コンテキスト、および認証後コンテキストに使用できます。

場所の識別

ユーザーの場所を識別するための位置情報サービスは、サードパーティサービス MaxMind によって提供されます。

ユーザーの場所は、VPN を介して x-forwarded-for ヘッダーから識別されます。サービスによってヘッダーが入力されていない場合は、VPN IP (場所) のみがユーザーの場所として表示されます。

注:
場所フィルターの構成後に誤った場所が表示される場合は、KB 記事 を参照してトラブルシューティングを行います。

場所ベースのアクセスのアクティブ化

管理者がユーザーの場所に基づいて適応認証ポリシーを設定できるようにするには、**[Zero Trust - Location Based Access (Zero Trust - Location Based Access)]** (com.snc.zero_trust_location_access) を有効にします。

始める前に
必要なロール：admin

- 依存プラグイン：Adaptive authentication
- プラグインタイプ：有料でライセンスが必要です。
- このインスタンスは ADCv2 上にある必要があります。インスタンスが ADCv2 上にない場合、ユーザーの場所情報は利用できません。

手順

1. 移動先 すべて > システムアプリケーション > 利用可能なすべてのアプリケーション > すべて.
2. フィルター基準と検索バーを使用して、**Zero Trust - Location Based Access** (com.snc.zero_trust_location_access) プラグインを検索します。

   名前または ID でプラグインを検索できます。プラグインが見つからない場合は、ServiceNow 担当者から要求する必要があります。

3. [インストール] を選択して、[プラグインをアクティブにする] ダイアログボックスで、[アクティブ化] をクリックします。

   注:
   ドメイン分離と代理管理者がインスタンスで有効になっている場合、管理ユーザーはグローバルドメインに含まれている必要があります。それ以外の場合、次のエラーが表示されます： 別の操作が実行されているため、アプリケーションのインストールは利用できません：<プラグイン名> のプラグインの有効化。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

場所のフィルター基準の作成

場所のフィルター基準を使用して、ユーザーの場所に基づいてユーザー認証の入力をフィルタリングします。

始める前に

必要なロール：admin

必要なプラグイン：**Zero Trust - Location Based Access** (com.snc.zero_trust_location_access)

プロパティ： [適応認証] プロパティを有効にします。

> **注:**
> 管理者は、場所が現在のユーザーセッションで利用可能な場合にのみ場所フィルターに基づいてポリシーを作成できます。

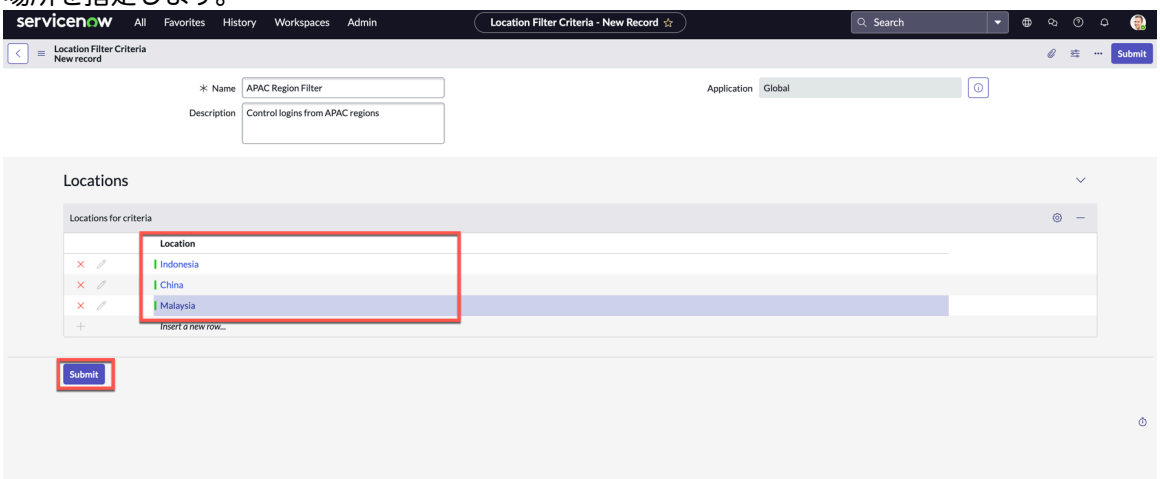
手順

1. 移動先 すべて > 適応認証 > フィルター基準 > 場所フィルター基準.
2. [新規] を選択します。
3. フォーム上で、以下のフィールドに記入します。

場所のフィルター基準フォーム

フィールド	説明
名前	基準を識別する名前
説明	基準の簡単な説明
アプリケーション	アプリケーションのスコープ

4. [場所] セクションの [基準の場所 (Locations for criteria)] タブで、[新しい行を挿入] をダブルクリックします。
5. 場所を指定します。



6. [送信] を選択します。

チュートリアル：場所のフィルター基準を使用する

認証ポリシーで場所フィルター基準を使用し、場所に基づいてユーザーへのアクセスを制限する手順について説明します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

始める前に
必要なロール：admin

必要なプラグイン：**Zero Trust - Location Based Access** (com.snc.zero_trust_location_access)

プロパティ： [適応認証] プロパティを有効にします。

注:
管理者は、場所が現在のユーザーセッションで利用可能な場合にのみ場所フィルターに基づいてポリシーを作成できます。

次の手順では、場所のフィルター基準を作成して認証ポリシーで使用する方法について説明します。

手順

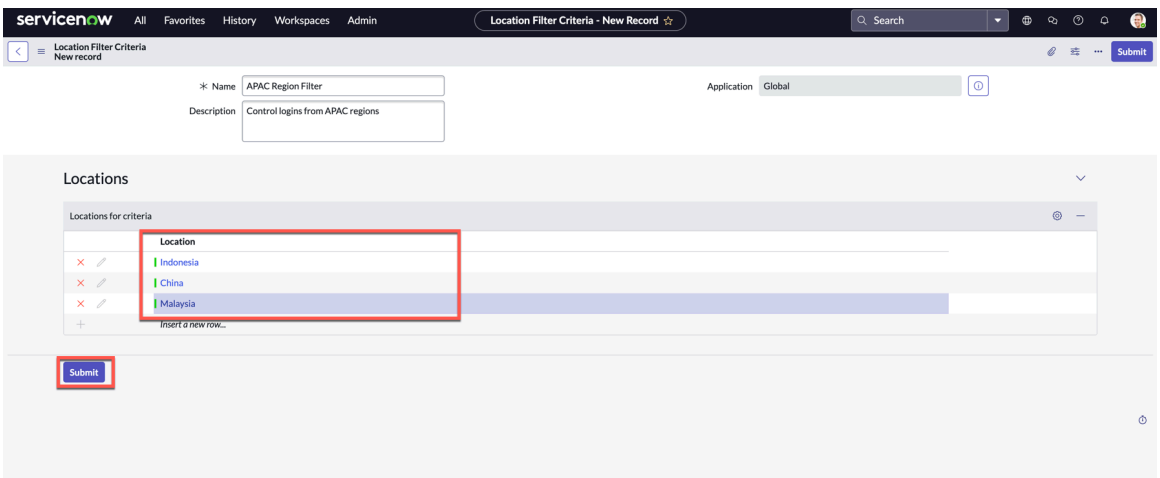
1. 移動先 すべて > 適応認証 > フィルター基準 > 場所フィルター.
2. [新規] を選択します。
3. フォーム上で、以下のフィールドに記入します。

場所のフィルター基準フォーム

フィールド	説明
名前	基準を識別する名前
説明	基準の簡単な説明
アプリケーション	アプリケーションのスコープ

4. [場所] セクションの [基準の場所 (Locations for criteria)] タブで、[新しい行を挿入] をダブルクリックします。
5. 場所を指定します。

   たとえば、一部の APAC 地域を使用して APAC からのユーザーのログインを制御します。



   例で設定された基準に基づいて、インスタンスの Indonesia、China、および Malaysia からのログインを制御できます。

6. [送信] を選択します。
7. 任意の認証コンテキスト (事前、事後、MFA) およびセッションアクセスで作成されたフィルター基準を使用します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

認証コンテキストとセッションアクセスに基づく構成の詳細については、以下を参照してください。

- 事前承認コンテキストでの場所のフィルター
- 認証後コンテキストでの場所のフィルター
- MFA コンテキストでの場所のフィルター
- セッションアクセスでの場所のフィルター

認証ポリシーの失敗が原因でログインが失敗したときにユーザーに表示されるプロパティ ID - エラーメッセージ (glide.auth.policy.ui.error.message) を使用して、エラーメッセージをカスタマイズできます。

事前認証コンテキストで場所のフィルターを使用する

事前認証コンテキストで作成された場所のフィルター基準を使用します。

始める前に

必要なロール：admin

必要なプラグイン：**Zero Trust - Location Based Access** (com.snc.zero_trust_location_access)

場所に基づいてユーザーへのアクセスを制限する国で、場所のフィルターを作成します。詳細については、「場所のフィルター基準の作成」を参照してください。

手順

1. 移動先 すべて > 適応認証 > 認証ポリシーのコンテキスト > 事前認証のコンテキスト.

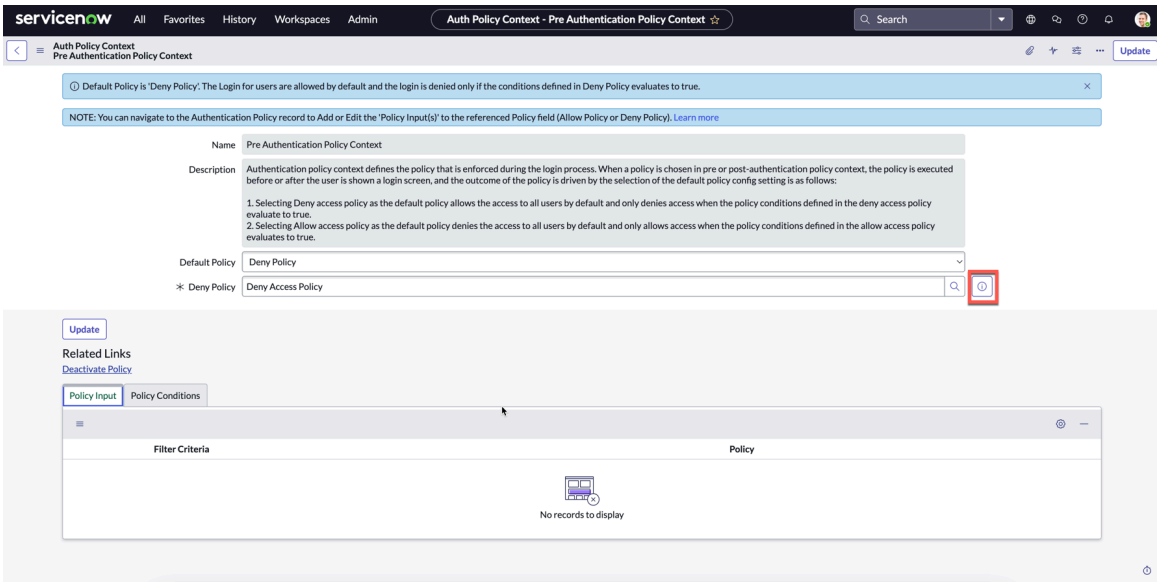
   ポリシーが事前認証ポリシーコンテキストで選択された場合：

   - [アクセス拒否ポリシー (Deny access policy)] をデフォルトポリシーとして選択すると、デフォルトですべてのユーザーへのアクセスが許可され、アクセス拒否ポリシーで定義されたポリシー条件が true と評価された場合にのみアクセスが拒否されます。
   - [アクセス許可ポリシー (Allow access policy)] をデフォルトポリシーとして選択すると、デフォルトですべてのユーザーへのアクセスが拒否され、アクセス許可ポリシーで定義されたポリシー条件が true と評価された場合にのみアクセスが許可されます。

   この例は、指定された場所からのログインを制限する方法を示しています。事前認証ポリシーとして [アクセスを拒否 (Deny Access)] および関連するポリシー ([アクセスを拒否 (Deny Access)]) を選択して、ポリシーの入力と条件を指定できます。

自動翻訳

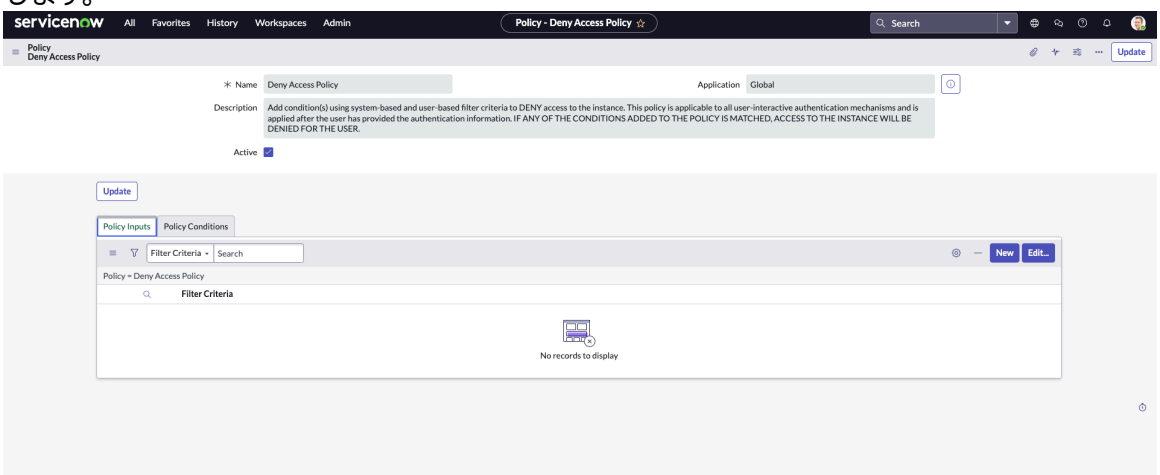
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



2. 情報アイコンを選択して [拒否ポリシー] レコードを開きます。

> **注:**
> このタスクで説明する例は [拒否ポリシー] です。[許可ポリシー] を使用して条件を適宜設定し、ログインを制御することもできます。

3. [アクセス拒否ポリシー (Deny access policy)] の [ポリシーの入力] セクションで、[新規] を選択します。

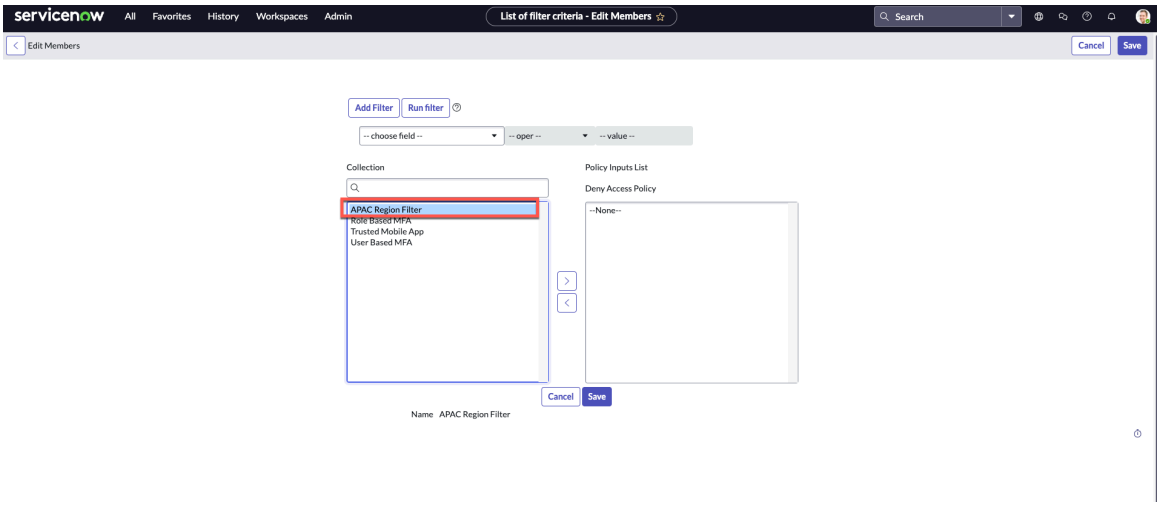


4. 場所のフィルター入力を追加して、[保存] を選択します。

例：APAC 地域

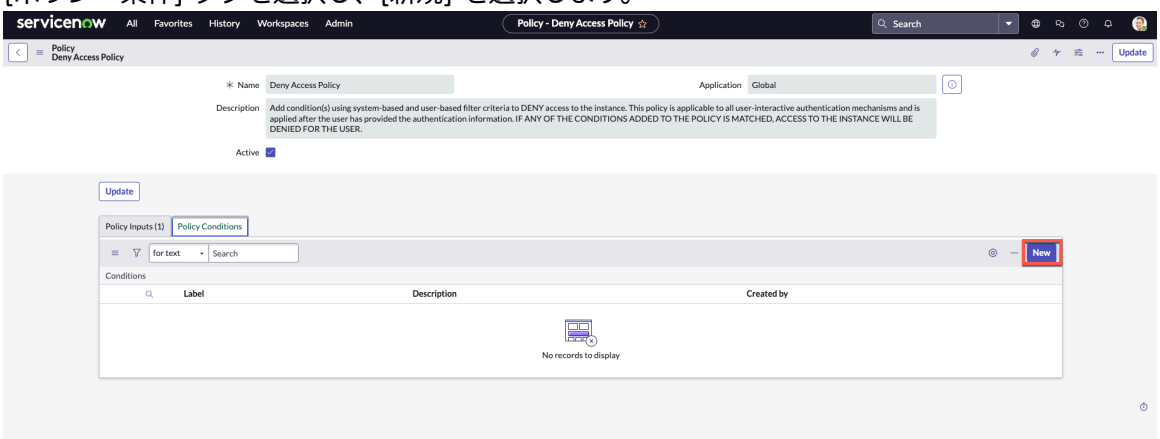
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

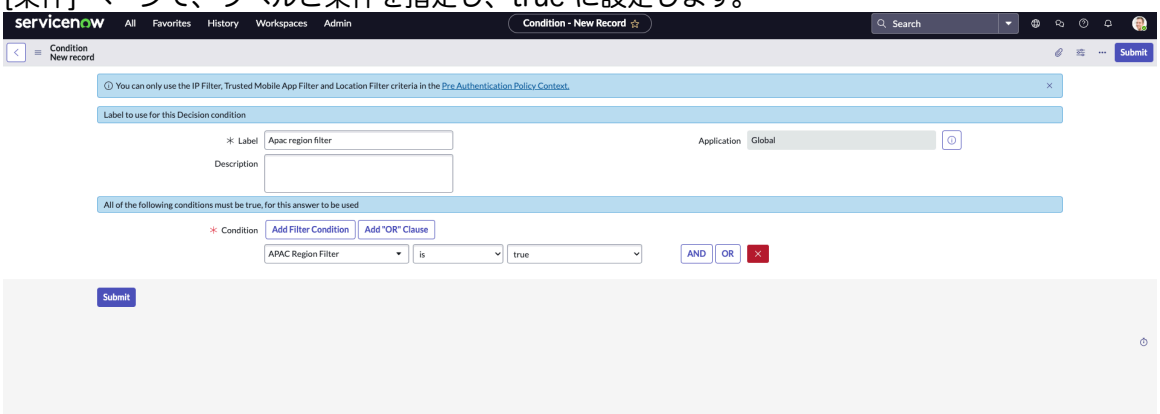


フィルターは [ポリシーの入力] として追加されます。

5. [ポリシー条件] タブを選択し、[新規] を選択します。



6. [条件] ページで、ラベルと条件を指定し、true に設定します。



注:

- この例では、条件として true を選択すると、設定された地域からログインしているユーザーがインスタンスにログインできなくなることを示しています。
- 条件が false に設定されている場合、設定された地域からのユーザーのみがインスタンスにログインでき、他のユーザーはインスタンスにログインできません。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

7. [送信] を選択します。
   インスタンスリンクを選択し、設定された国からログインしているユーザーには、アクセス拒否に関するエラーメッセージ (ポリシーのプロパティページで管理者が設定したエラーメッセージ) が表示されます。

認証後コンテキストでの場所フィルターの使用

認証後コンテキストで作成された場所のフィルター基準を使用します。

始める前に

必要なロール：admin

必要なプラグイン：**Zero Trust - Location Based Access** (com.snc.zero_trust_location_access)

場所に基づいてユーザーへのアクセスを制限する国で、場所のフィルターを作成します。詳細については、「場所のフィルター基準の作成」を参照してください。

手順

1. 移動先 すべて > 適応認証 > 認証ポリシーのコンテキスト > 認証後のコンテキスト.

   ポリシーが認証後ポリシーコンテキストで選択された場合：

   - [アクセス拒否ポリシー (Deny access policy)] をデフォルトポリシーとして選択すると、デフォルトですべてのユーザーへのアクセスが許可され、アクセス拒否ポリシーで定義されたポリシー条件が true と評価された場合にのみアクセスが拒否されます。
   - [アクセス許可ポリシー (Allow access policy)] をデフォルトポリシーとして選択すると、デフォルトですべてのユーザーへのアクセスが拒否され、アクセス許可ポリシーで定義されたポリシー条件が true と評価された場合にのみアクセスが許可されます。

   この例は、指定された場所 (米国) からのみインスタンスにアクセスするという条件を使用して itil ユーザーを構成する方法を示しています。また、itil ユーザーは他の国からログインできません。

   ユーザーがログインページで資格情報を入力した後、認証後ポリシーとして [アクセスを許可 (Allow Access)] および関連するポリシー ([アクセスを許可 (Allow Access)]) を選択して、ポリシーの入力と条件を指定できます。

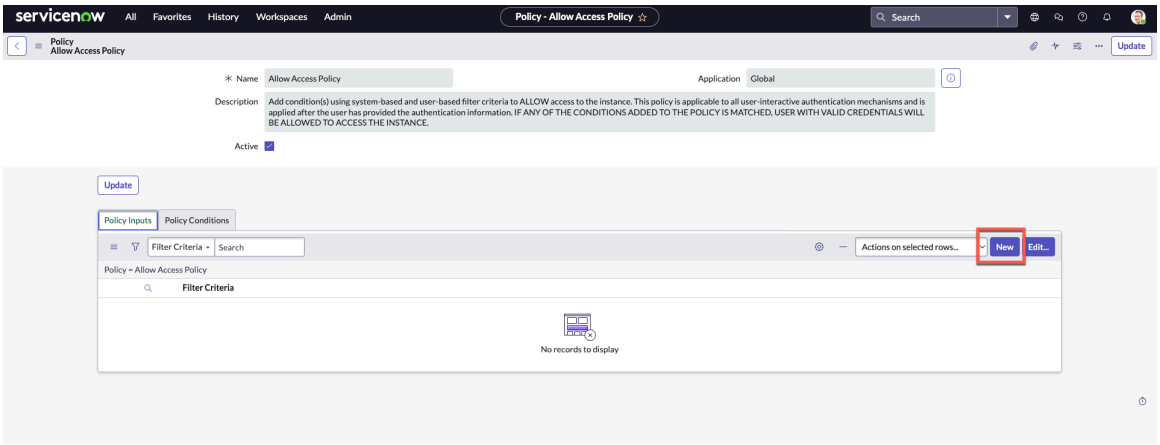
2. 情報アイコンを選択して [許可ポリシー] レコードを開きます。

   注:
   このタスクで説明する例は [許可ポリシー] です。[拒否ポリシー] を使用して条件を適宜設定し、ログインを制御することもできます。

3. [アクセス許可ポリシー (Allow Access Policy)] の [ポリシーの入力] セクションで、[新規] を選択します。

自動翻訳

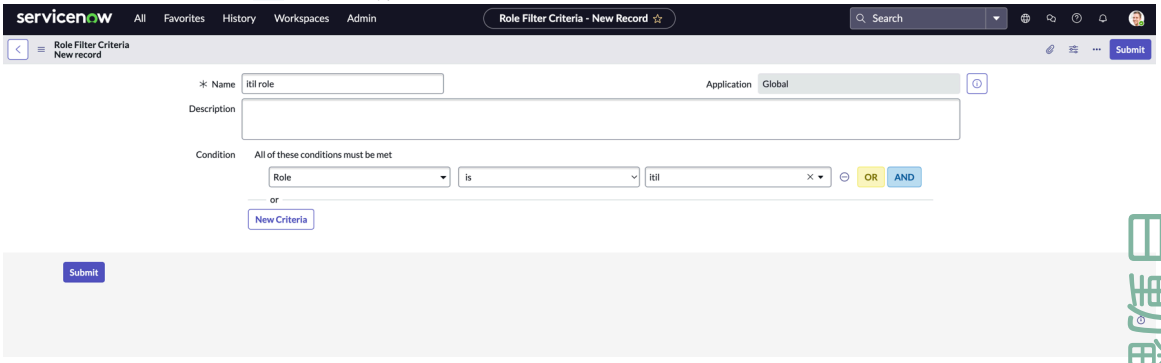
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



4. ロールフィルター基準と場所フィルター基準を追加します。

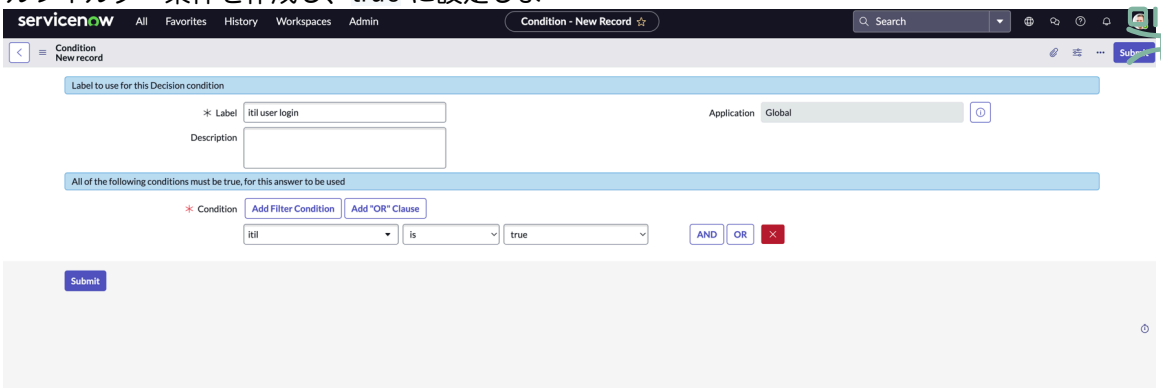
a. ロールフィルター基準を追加する場合：

- ロールフィルター入力を itil として作成しま



す。

- ロールフィルター条件を作成し、true に設定しま



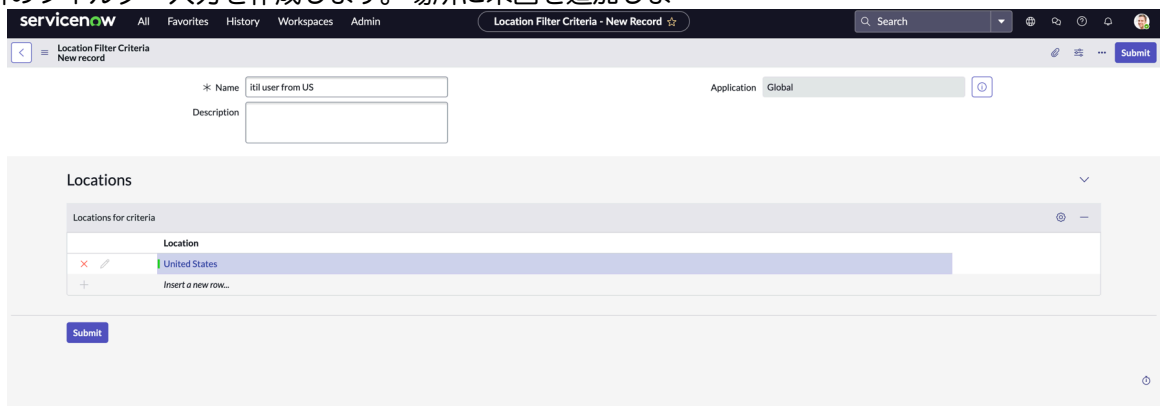
す。

ロールフィルター基準を作成する方法の詳細については、「ロールフィルター基準の作成」を参照してください。

b. 場所のフィルター基準を追加する場合：

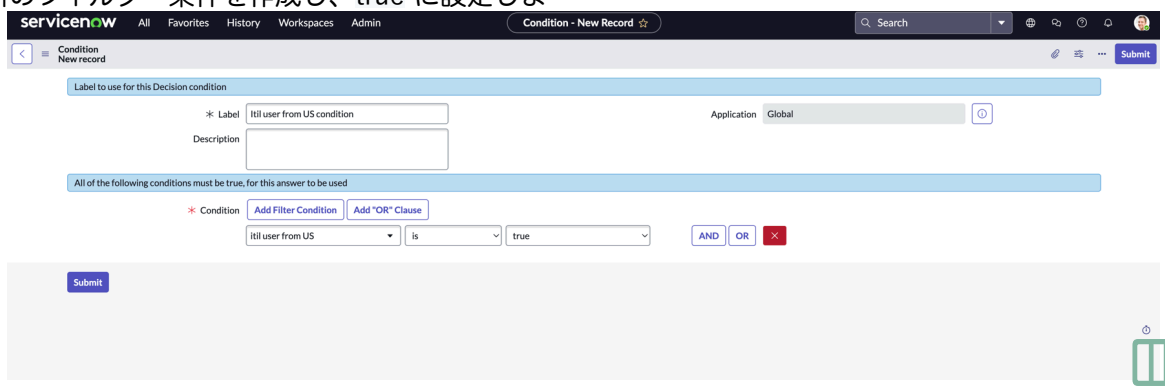
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- 場所のフィルター入力を作成します。場所に米国を追加しま



す。

- 場所のフィルター条件を作成し、true に設定しま



す。

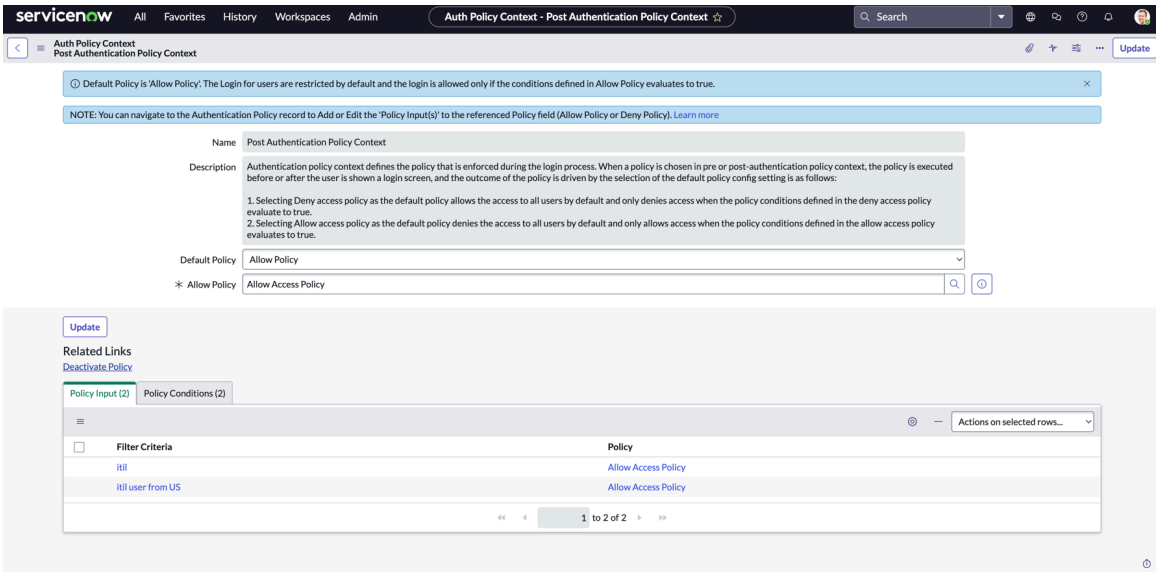
ロールフィルター基準を作成する方法の詳細については、「場所のフィルター基準の作成」を参照してください。

[アクセス許可ポリシー (Allow Access Policy)] には、前のステップで作成されたポリシーの入力と条件が表示されます。

- ポリシーの入力：itil、米国の itil ユーザー
- ポリシー条件：itil ユーザーログイン、米国からの itil ユーザー条件

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



注:

- この例では、条件として true を選択すると、設定された国 (米国) からログインしている itil ユーザーがインスタンスにログインできることを示しています。
- 条件が false に設定されている場合、設定された国 (米国) からの itil ユーザーはインスタンスにログインできず、他のユーザーもインスタンスにログインできません。

5. [送信] または [更新] を選択して、認証後のコンテキストを更新します。
インスタンスリンクを選択し、資格情報を指定してから設定された国 (米国) 以外からログインしている itil ユーザーには、アクセス拒否に関するエラーメッセージ (ポリシーのプロパティページで管理者が設定したエラーメッセージ) が表示されます。

MFA コンテキストで場所のフィルターを使用する

MFA コンテキストで作成された場所のフィルター基準を使用します。

始める前に

必要なロール：admin

必要なプラグイン：**Zero Trust - Location Based Access** (com.snc.zero_trust_location_access)

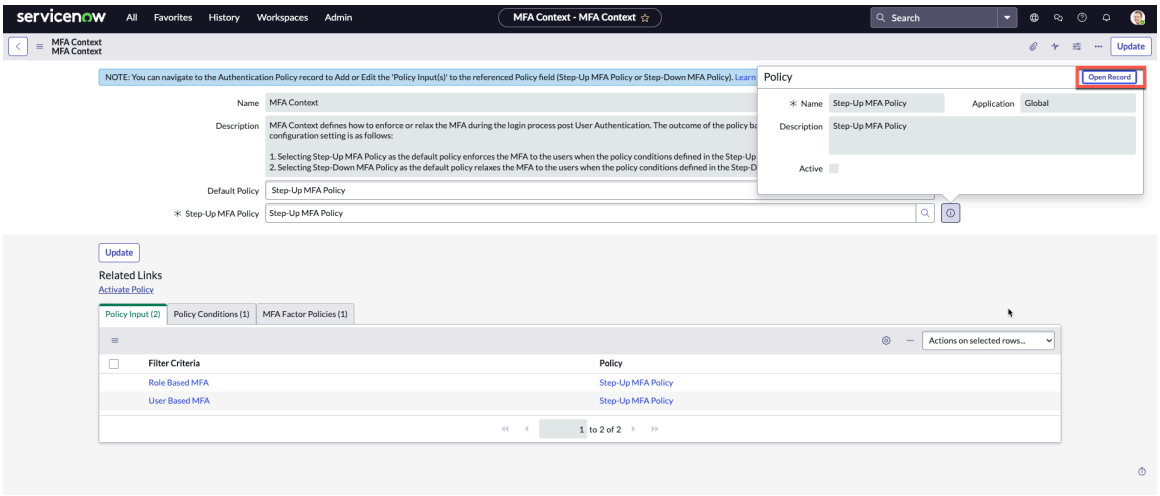
次の手順では、場所に基づいてユーザーを認証する場合に、MFA を認証の第 2 要素として構成する国で場所のフィルターを作成する手順について説明します。

手順

1. 移動先 すべて > 適応認証 > 認証ポリシーのコンテキスト > **MFA** コンテキスト.
2. **[MFA** コンテキスト] ページで、[ステップアップ **MFA** ポリシー] 情報アイコンを選択し、レコードを開きます。

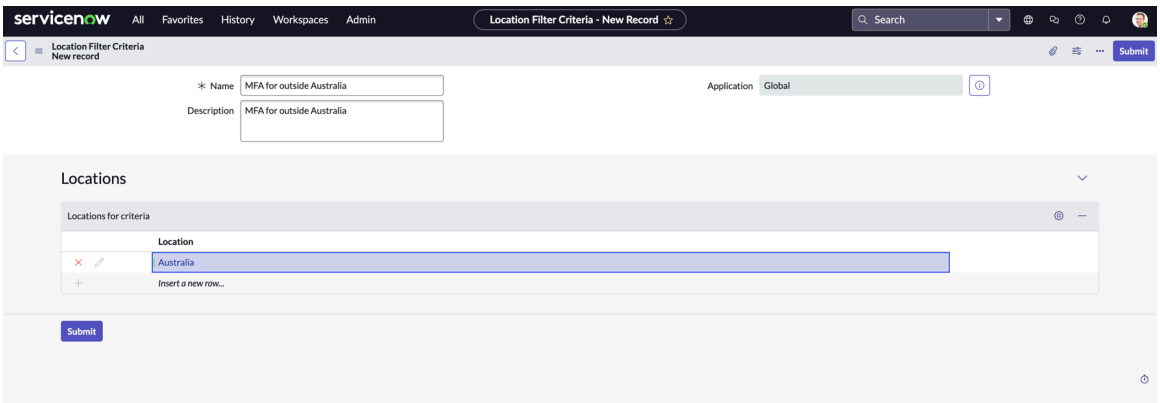
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

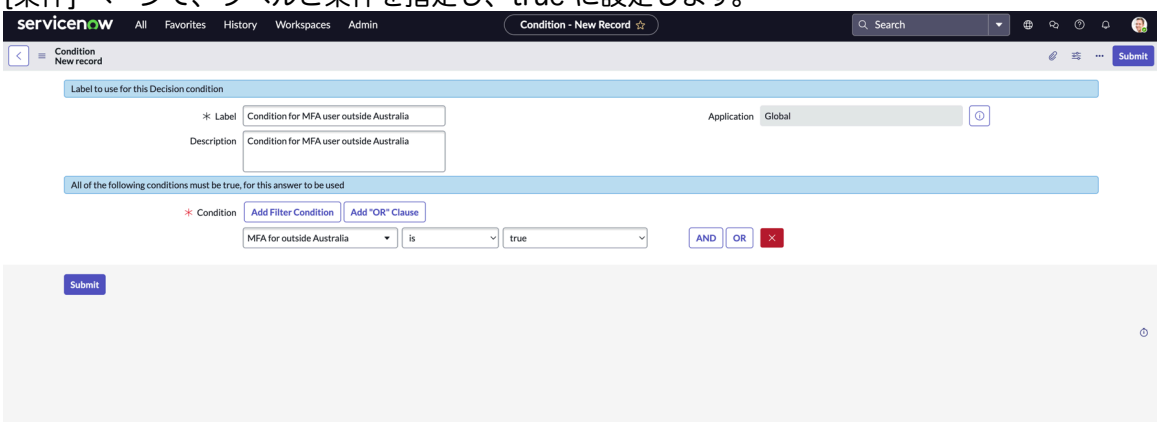


3. [ステップアップ MFA ポリシー] ページの [ポリシーの入力] タブで、[新規] を選択します。
4. 場所のフィルター入力を追加して、[送信] を選択します。

   たとえば、オーストラリア国外でインスタンスにログインしているユーザーに MFA を表示するとします。



5. [ステップアップ MFA ポリシー] ページの [ポリシー条件] タブで、[新規] を選択します。
6. [条件] ページで、ラベルと条件を指定し、true に設定します。



7. [送信] を選択します。
8. [ステップアップ MFA ポリシー] ページで、MFA ポリシーが [非アクティブ化済み] の場合はアクティブ化します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

9. [更新] を選択して構成を更新します。

インスタンスリンクを選択し、資格情報を指定する設定された国 (オーストラリア) 以外のユーザーには、インスタンスにログインするための第 2 要素の資格情報を提供するための MFA 画面が表示されます。

セッションアクセスに対する場所のフィルターの使用

セッションアクセスで作成された場所のフィルター基準を使用して、ユーザーの場所に基づいてロールを削減します。

始める前に

必要なロール：admin

必要なプラグイン：**Zero Trust - Location Based Access** (com.snc.zero_trust_location_access)

次の手順では、場所に基づいてロールを削除または制限する国で場所のフィルターを作成する手順について説明します。

手順

1. 移動先 すべて > **Zero Trust** アクセス > セッションアクセスロール構成.
2. セッションアクセスロールの構成を作成するには、[新規] を選択します。
3. フォームの各フィールドに入力します。

セッションアクセスのロール構成

フィールド	説明
名前	構成の名前
説明	構成の簡単な説明
ポリシー	アクセスポリシーを選択します。ルックアップアイコンを使用して、ポリシーのリストを表示します。 **注:** ポリシーレコードを開いて、場所のフィルター入力と条件を追加する必要があります。
アクション	[ロールを削除] または [ロールに制限 **(Limit to Roles)**] ○ ロールを削除：構成されたユーザーがログインすると、ロールリストまたはグループリストで提供されたロールのリストがログインセッションに対して削除されます。 ○ ロールに制限 **(Limit to Roles)**：構成されたユーザーがログインすると、選択されたロールのみがユーザーに提供され、他のすべてのロールはログインセッションから削除されます。
ロールリスト	ロールリストからロールを選択します。
グループリスト	グループリストからロールを選択します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

4. [送信] を選択します。

   構成された国に基づいたユーザーのログインは次のとおりです。

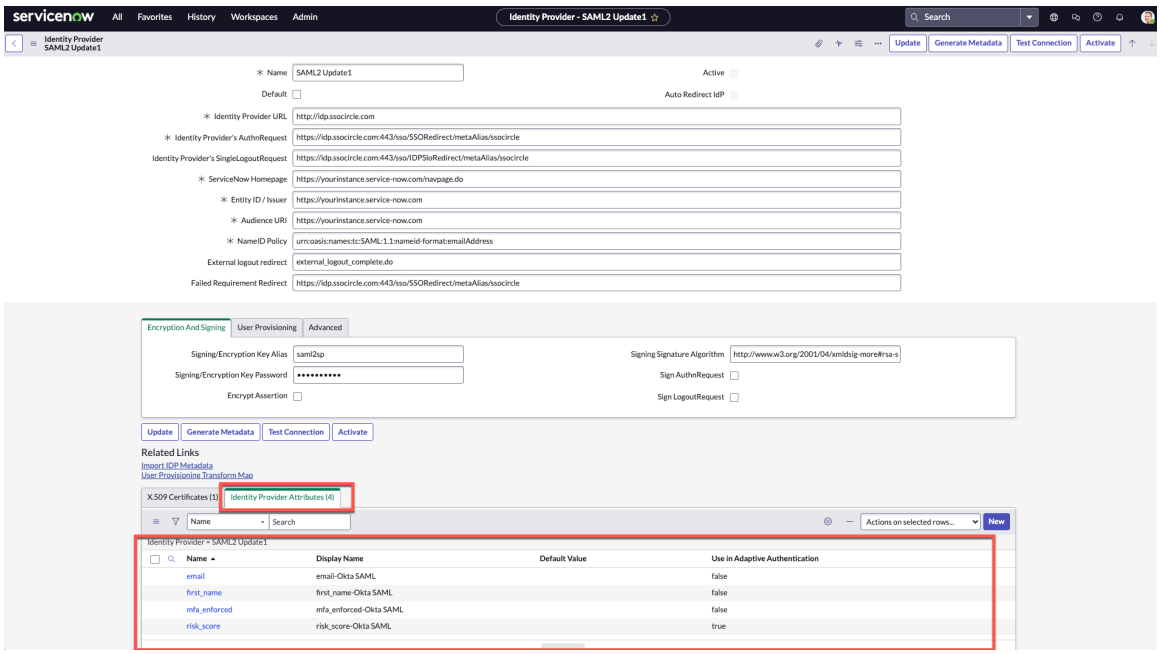
   - [ロールを削除] の場合、場所のフィルターで構成された国のユーザーがセッションに対して構成されたロールとともに削除されます。
   - [ロールに制限 **(Limit to Roles)**] の場合、場所のフィルターで構成された国のユーザーはセッションに対して構成されたロールのみを持ちます。

   セッションに対してロールを削除または制限する方法の詳細については、「チュートリアル：Zero Trust アクセスを使用する」を参照してください。

ID プロバイダー属性フィルター

ID プロバイダー (IdP) からのセキュリティアサーションマークアップ言語 (SAML) 応答から受信した ID プロバイダー属性を認証のフィルター基準として使用します。

SAML 応答を介して IdP からすべての属性をフェッチするには、IdP とのテスト接続を実行する必要があります。テスト接続に成功すると、属性が ID プロバイダー構成ページの新しいタブに追加されます。



ID プロバイダー属性セクションから [新規] を選択して属性を追加し、`true` に設定してそれらの属性を適応認証に使用することもできます。

[ID プロバイダー属性 (Identity Provider Attributes)] が次の詳細とともに表示されます。

場所のフィルター基準フォーム

フィールド	説明
名前	ID プロバイダーによって提供される属性名
表示名	表示名はフィルター基準に使用される詳細な名前です。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

場所のフィルター基準フォーム (続く)

フィールド	説明
	注: ID プロバイダーによって指定された表示名が長くて判読できないことがあるため、表示名として判読可能な名前を指定できます。
デフォルト値	デフォルト値は、SAML 応答に属性がない場合にフィルター基準の評価に使用されます。
適応認証で使用	適応認証で属性を使用するオプション。

注:
Azure IdP から入力される属性は、属性の名前の長さにより、名前と表示名が文字数に制限されています。

[ID プロバイダー属性 (Identity Provider Attributes)] セクションで [新規] を選択して、新しい属性を追加することもできます。

[適応認証で使用 (Use in Adaptive Authentication)] が true に設定されている場合、選択した属性が汎用的なフィルター基準のフィルター基準として追加されます。たとえば、**risk_score** を true に設定します。汎用的なフィルター基準ページに新しいフィルターが作成されます。

ID プロバイダー属性をフィルター基準として使用する

セキュリティアサーションマークアップ言語 (SAML) 応答からの ID プロバイダー (IDP) 属性を認証ポリシーのフィルター基準として使用します。

始める前に
必要なロール：admin

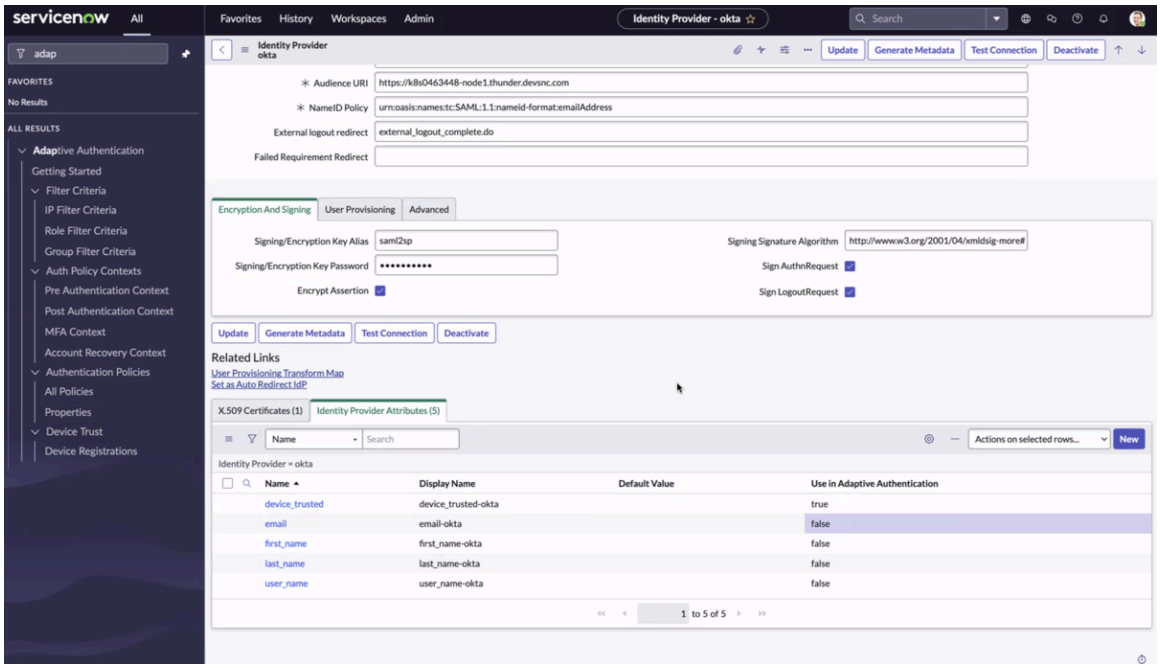
ポリシーコンテキスト (事前認証、認証後、マルチファクター認証) とフィルター基準 (ロール、グループ、IP、場所) をポリシーの入力と条件とともに使用して、セッションアクセスポリシーを作成できます。

次の手順は、SAML 応答の IdP 属性をポリシーの入力として設定し、[認証後のコンテキスト]、[マルチファクター認証 **(MFA)** コンテキスト]、および **[Zero Trust - Policy Based Session Access]** で認証を制御する手順を示しています。

Okta IDP 属性は、次のスクリーンショットに表示されているとおりです。[認証後のコンテキスト]、[マルチファクター認証 **(MFA)** コンテキスト]、および **[Zero Trust - Policy Based Session Access]** ポリシーで使用するには、[適応認証で使用 (Use in Adaptive Authentication)] を true に設定する必要があります。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



注:
認証後、MFA、 Zero Trust - Policy Based Session Access のポリシーは、ユーザーが資格情報または SSO 応答を入力した後に実行されます。

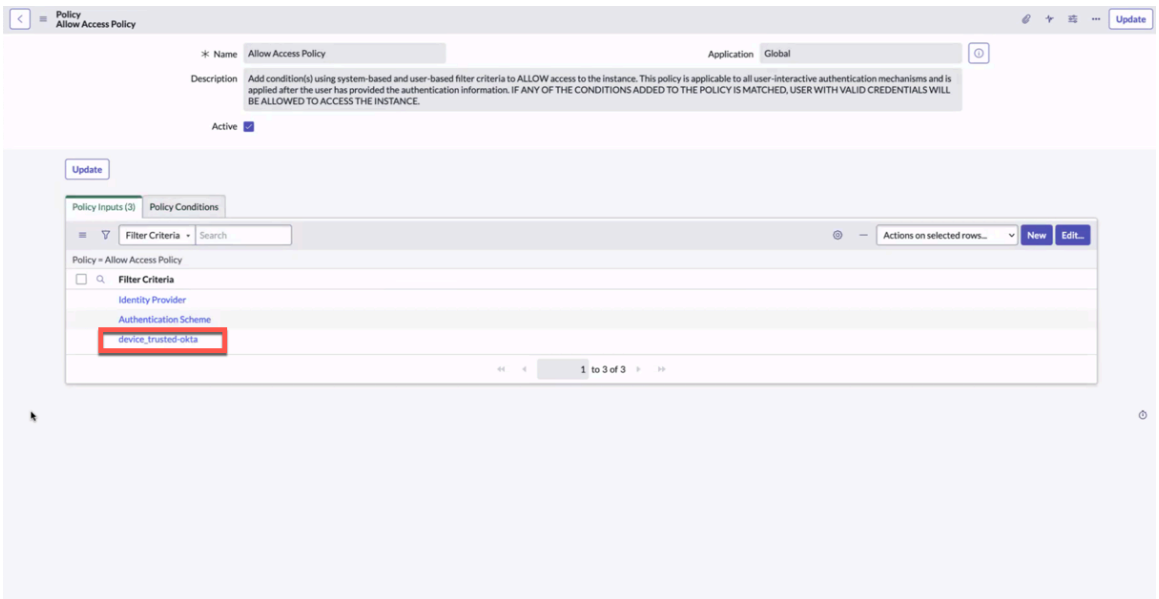
手順

1. 認証後ポリシーのコンテキストでの IDP 属性の使用
   例：デバイスが信頼できる場合に、Okta IDP 属性からのログインを有効にするように設定します。

   a. 移動先 すべて > 適応認証 > 認証ポリシーのコンテキスト > 認証後ポリシーのコンテキスト。.

   b. [許可ポリシー] を選択し、ポリシーレコードを開きます。

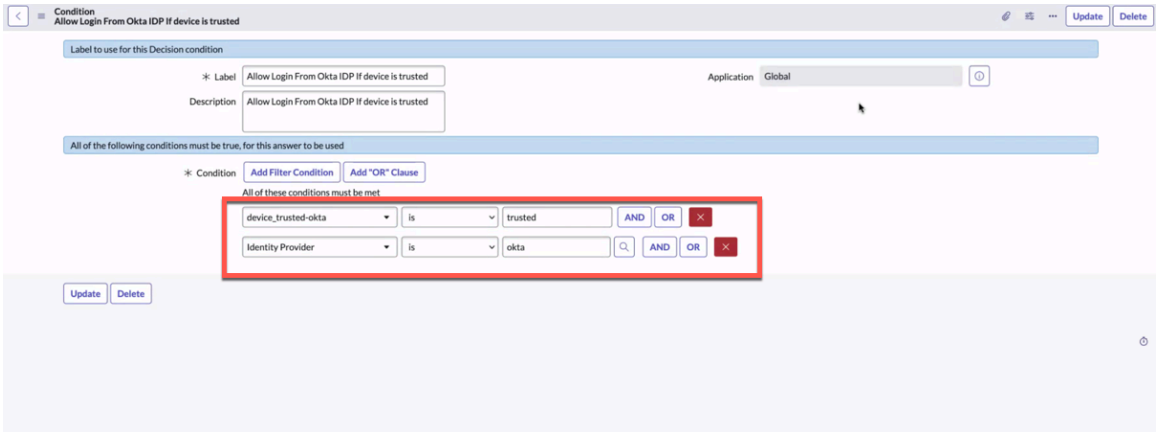
   c. ポリシー入力で、ポリシーの入力と条件を作成します。
      - ポリシー入力：**device_trusted-okta** を追加します。



自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- ポリシー条件：**[device_trusted-okta]** は trusted であり、**[ID** プロバイダー] は Okta です。



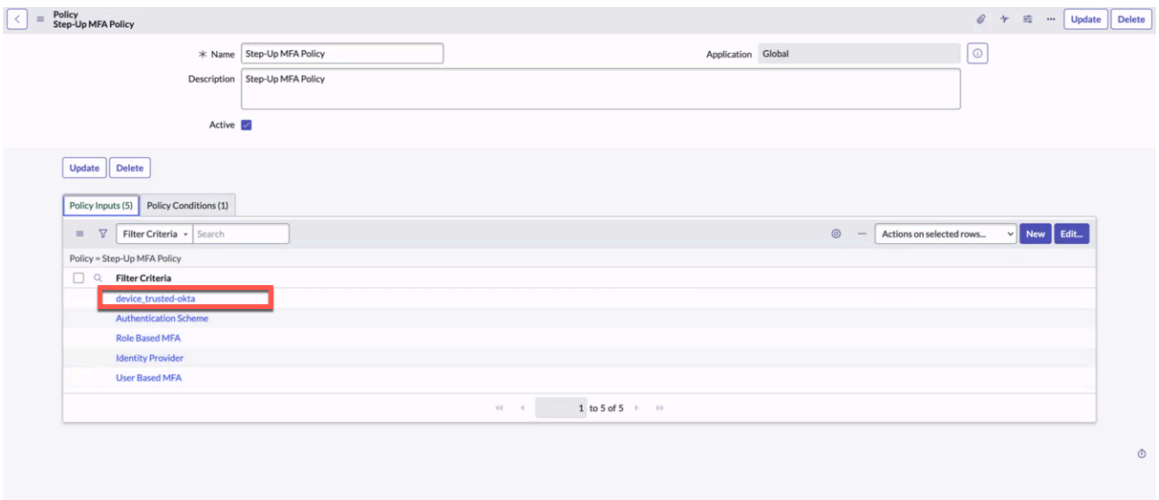
この構成に基づいて、デバイスが Okta (IdP) から信頼されている場合、ユーザーはインスタンスに対して認証されます。

ポリシーと条件で認証後のコンテキストを作成する方法の詳細については、「認証後コンテキスト」を参照してください。

2. MFA ポリシーのコンテキストでの IDP 属性の使用
例：デバイスが信頼できない場合に、Okta IDP 属性からの MFA を有効にするように設定します。

   a. 移動先 すべて > 適応認証 > 認証ポリシーのコンテキスト > **MFA** 認証ポリシーのコンテキスト.

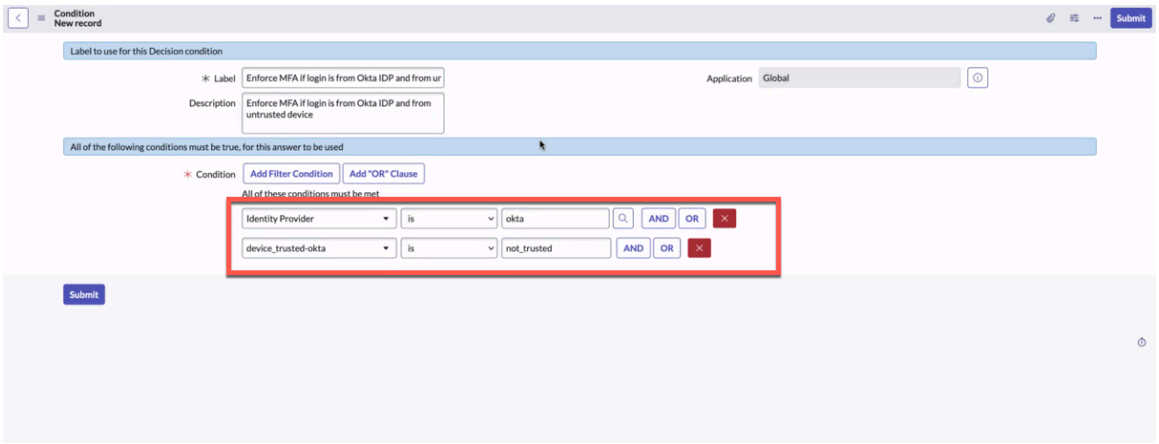
   b. ポリシー入力で、ポリシーの入力と条件を作成します。
   - ポリシー入力：**device_trusted-okta** を追加します。



自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- ポリシー条件：**[device_trusted-okta]** は not_trusted であり、**[ID** プロバイダー] は Okta です。



この構成に基づいて、デバイスが Okta (IdP) から信頼されていない場合、ユーザーにはインスタンスにログインするための第 2 要素認証が表示されます。

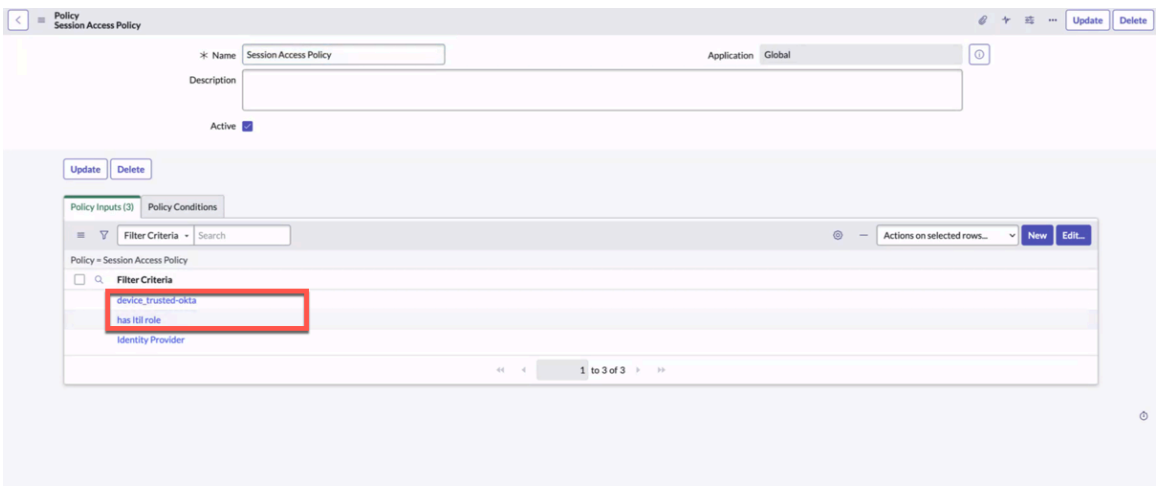
ポリシーと条件で MFA コンテキストを作成する方法の詳細については、「MFA (マルチファクター認証) コンテキスト」を参照してください。

3. Zero Trust - Policy Based Session Access での IDP 属性の使用
例：デバイスが信頼できない場合に、Okta IDP 属性からの Itil ロールの特権を減らすように設定します。

   a. 移動先 すべて > **Zero Trust** アクセス > セッションアクセスロール構成.

   b. セッションアクセスのロール構成を作成します。

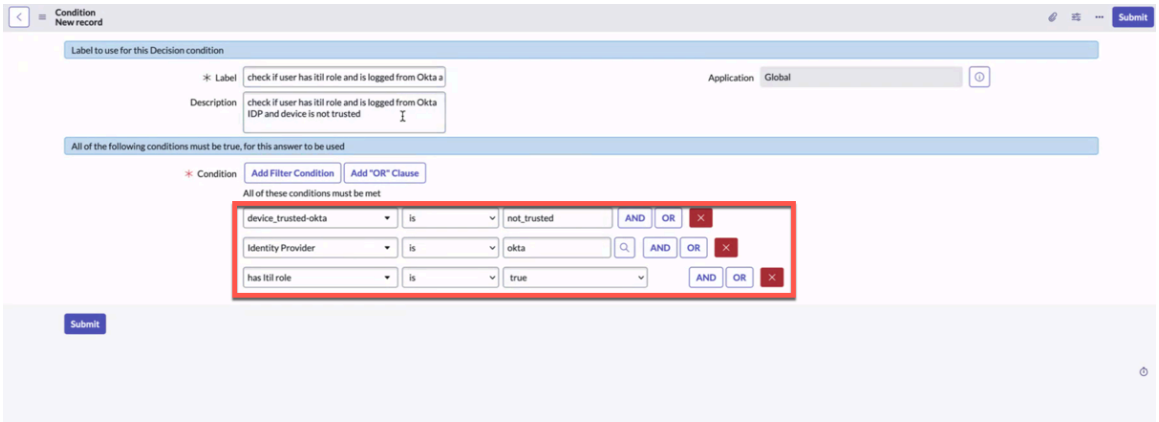
   c. ポリシー入力で、ポリシーの入力と条件を作成します。
      - ポリシー入力：**device_trusted-okta** と **has itil role** を追加します。



自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- ポリシー条件：**[device_trusted-okta]** は not_trusted であり、**[ID プロバイダー]** は Okta であり、**[has itil role]** は true です。



この構成に基づいて、Okta (IdP) から信頼されていないデバイスを itil ユーザーが使用すると、ログインセッションに対するユーザーの権限が減らされます。

ポリシーと条件で Zero Trust - Policy Based Session Access を作成する方法の詳細については、「Zero Trust アクセス」を参照してください。

認証ポリシーのコンテキスト

認証ポリシーコンテキストを使用して、インスタンスで認証ポリシーを適用する方法とタイミングを決定します。

認証コンテキストは、ログインプロセス中にポリシーを適用する方法とタイミングを定義します。ポリシーコンテキストにポリシーを割り当て、インスタンスが認証を処理する方法に関する入力と条件を定義します。

事前承認コンテキスト

事前承認コンテキストのポリシーは、ユーザーによるインスタンスへの初回アクセス時に、ログイン画面を表示する前に実行されます。事前承認コンテキストを使用して、選択したポリシーに基づいてユーザーに対してログイン資格情報が要求される前に、アクセスを許可または拒否できます。これらのポリシーはユーザーが情報を入力する前に評価されるため、ユーザーのロールやグループなどの基準を考慮することはできません。

このコンテキストの詳細については、「事前承認コンテキスト」を参照してください。

認証後コンテキスト

承認後コンテキストのポリシーは、ユーザーが資格情報または SSO 応答を入力した後に実行されます。インスタンスは、選択したポリシーに基づいてアクセスを許可または拒否します。ユーザーはログイン資格情報を使用して本人確認を行ったため、ポリシーでは、ユーザー情報を使用してアクセスを許可するかどうかを決定できます。

このコンテキストの詳細については、「認証後コンテキスト」を参照してください。

MFA (マルチファクター認証) コンテキスト

MFA コンテキストに割り当てられたポリシーは、ログインプロセス中に MFA を適用するかどうかを定義します。インスタンスで MFA が適用されるかどうかは、このコンテキストのポリシーの構成によって決まります。このコンテキストの詳細については、「MFA (マルチファクター認証) コンテキスト」を参照してください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

アカウント復旧のコンテキスト

管理者は、アカウント復旧 (ACR) を設定して、SSO の設定ミスや期限切れの証明書への対処などの復旧アクティビティを実行できます。アカウント復旧を使用するには、少なくとも 1 つの管理者アカウントをアカウント復旧ユーザーとして登録する必要があります。少なくとも 1 つのアカウントが設定されるまで、インスタンスで Single Sign-on を有効にすることはできません。設定可能なコンテキストの詳細については、「アカウント復旧のコンテキスト」を参照してください。

セッション検証コンテキスト

セッション検証コンテキストは、適応認証ポリシーフレームワークで使用できます。フレームワークは、認証ポリシーを使用して認証要求 (セッション) を評価し、ポリシー条件に基づいてアクセスを拒否または許可します。詳細については、「セッション検証コンテキスト」を参照してください。

デフォルトポリシー

ポリシーコンテキスト内で、デフォルトポリシーを [デフォルトポリシー] フィールドに定義できます。このデフォルトは、インスタンスがポリシーの結果にどのように応答するかを定義します。使用可能なデフォルトのポリシーオプションは、使用しているコンテキストによって決まります。これらのオプションの詳細については、個々のコンテキストの説明書を参照してください。

事前承認コンテキスト

事前認証ポリシーのコンテキストは、ログインプロセス中にポリシーを適用する方法とタイミングを定義します。このコンテキストで使用されるポリシーは、ユーザーにログイン画面が表示される前に実行されます。

事前認証コンテキストレコード

事前承認コンテキストのポリシーは、ユーザーによるインスタンスへの初回アクセス時に、ログイン画面を表示する前に実行されます。

事前認証コンテキストを使用して、選択したポリシーに基づいてユーザーがログイン資格情報を要求する前に、アクセスを許可または拒否できます。これらのポリシーはユーザーが情報を入力する前に評価されるため、ユーザーのロールやグループなどの基準を考慮することはできません。

事前認証ポリシーコンテキストレコードのフィールドを使用して、インスタンスでのポリシーの使用方法を定義します。

[事前認証コンテキスト] フォーム

フィールド	説明
名前	ポリシーコンテキストの名前このフィールドは静的であり、変更することはできません。
説明	コンテキストの説明
デフォルトポリシー	ポリシーを評価するときの、このコンテキストのデフォルト動作を定義します。次のオプションのいずれかを選択します。 許可ポリシー デフォルトですべてのユーザーへのアクセスを拒否し、 [許可ポリシー] フィールドでポリシーが選択した条件が true と評価された場合にのみアクセスを許可します。 拒否ポリシー

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

[事前認証コンテキスト] フォーム (続く)

フィールド	説明
	デフォルトですべてのユーザーへのアクセスを許可し、 [拒否ポリシー] フィールドでポリシーが選択した条件が true と評価された場合にのみアクセスを拒否します。
許可ポリシー	このコンテキストで使用されるポリシー。このフィールドは、[デフォルトポリシー] フィールドが [許可ポリシー] に設定されている場合にのみ表示されます。
拒否ポリシー	このコンテキストで使用されるポリシー。このフィールドは、[デフォルトポリシー] フィールドが [拒否ポリシー] に設定されている場合にのみ表示されます。

注:

事前認証ポリシーコンテキストでは、IP フィルター、信頼できるモバイルアプリフィルター、および場所フィルターの基準のみを使用できます。

ポリシーの入力と条件

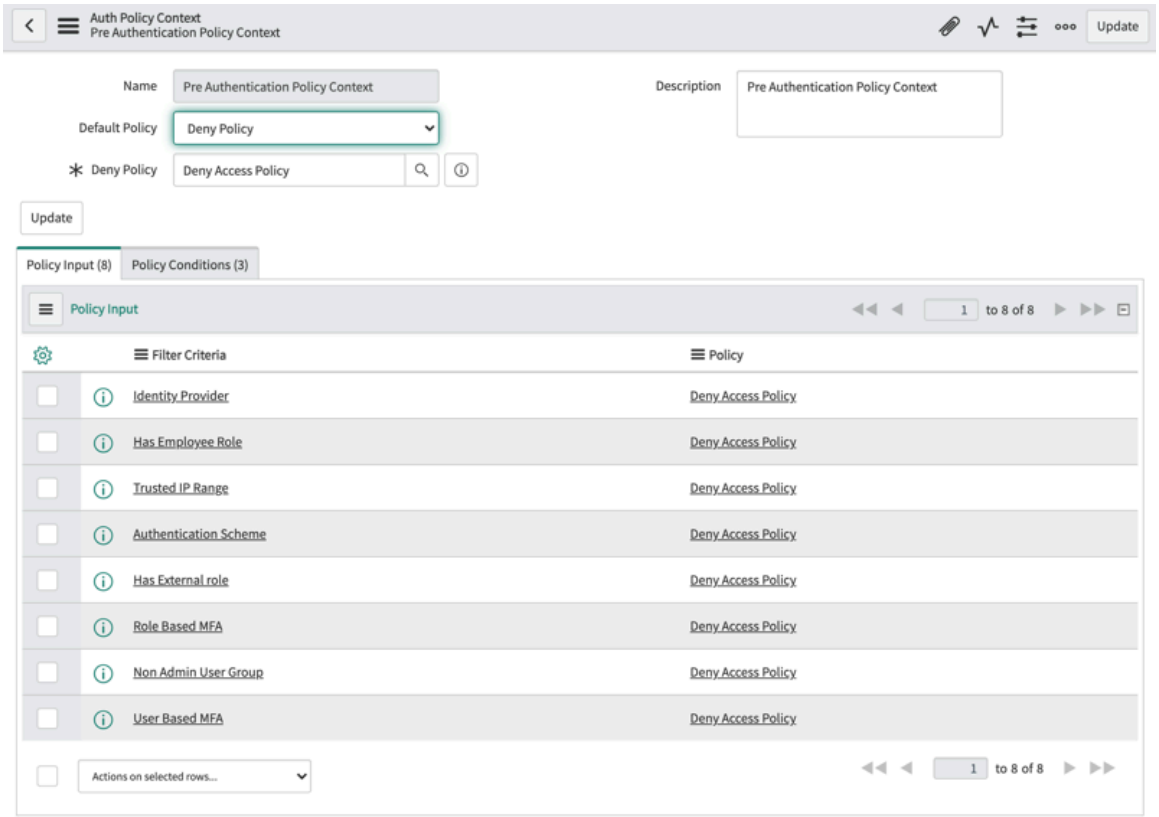
[ポリシー入力] タブと [ポリシー条件] タブには、[許可ポリシー] または [拒否ポリシー] フィールドで選択されたポリシーの入力と条件が表示されます。これらのタブは参照できますが、ポリシーの入力や条件を変更するために使用することはできません。ポリシーを変更するには、[許可ポリシー] または [拒否ポリシー] フィールドの横にある参照アイコン ( ) を使用してポリシーに移動します。

この例は、デフォルトでアクセスを拒否するように設定された事前認証ポリシーコンテキストレコードを示しています。コンテキストでは、[アクセスポリシーの拒否] と呼ばれるポリシーを使用します。そのポリシーには、[ポリシー入力] タブと [ポリシー条件] タブに表示される一連の入力と条件があります。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

[事前認証ポリシーのコンテキスト] フォーム



認証後コンテキスト

認証後ポリシーのコンテキストは、ログインプロセス中にポリシーを適用する方法とタイミングを定義します。このコンテキストで使用されるポリシーは、ユーザーにログイン画面が表示された後に実行されます。

認証後コンテキストレコード

承認後コンテキストのポリシーは、ユーザーが資格情報または SSO 応答を入力した後に実行されます。インスタンスは、選択したポリシーに基づいてアクセスを許可または拒否します。ユーザーはログイン資格情報を使用して本人確認を行うため、ポリシーでは、ロールやグループなどのユーザー情報を使用してアクセスを許可するかどうかを決定できます。

認証後ポリシーコンテキストレコードのフィールドを使用して、インスタンスでのポリシーの使用方法を定義します。

認証後コンテキストフォーム

フィールド	説明
名前	ポリシーコンテキストの名前このフィールドは静的であり、変更することはできません。
説明	コンテキストの説明
デフォルトポリシー	ポリシーを評価するときの、このコンテキストのデフォルト動作を定義します。次のオプションのいずれかを選択します。 許可ポリシー デフォルトですべてのユーザーへのアクセスを拒否し、 [許可ポリシー] フィールドでポリシーが選択した条件が true と評価された場合にのみアクセスを許可します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

認証後コンテキストフォーム (続く)

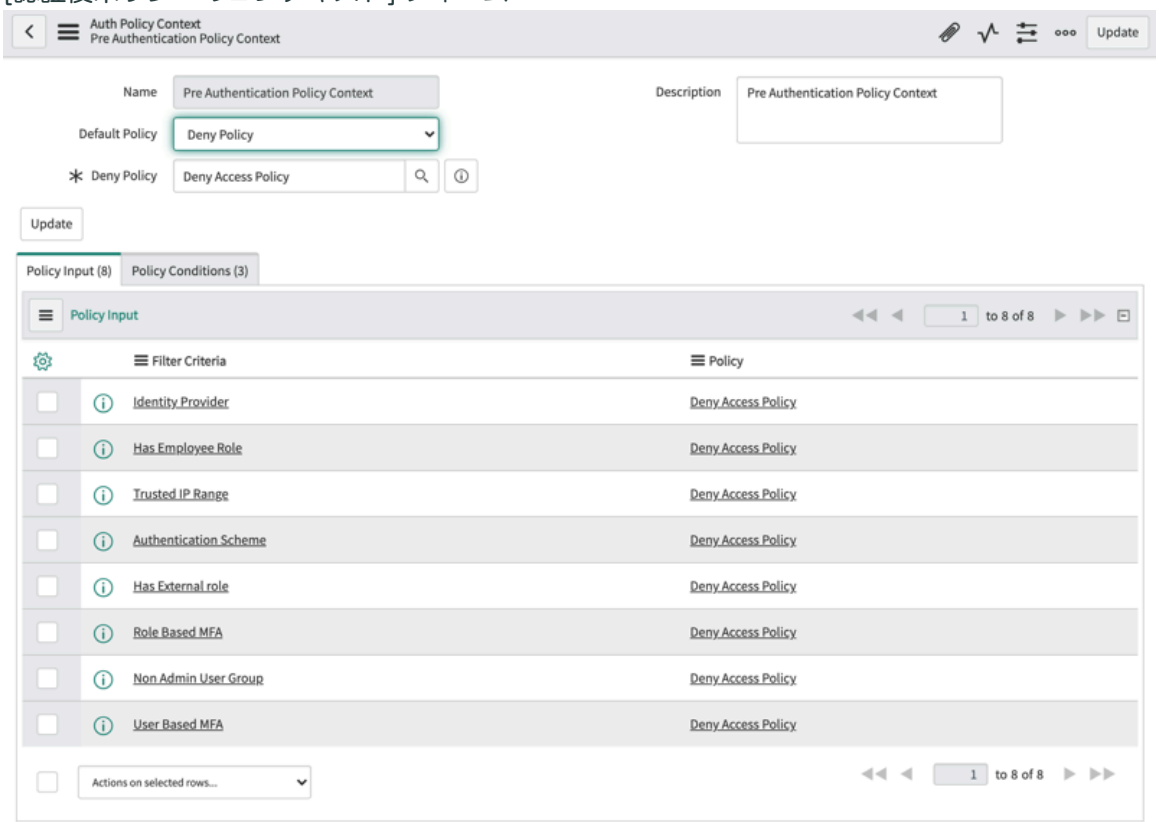
フィールド	説明
	拒否ポリシー デフォルトですべてのユーザーへのアクセスを許可し、 [拒否ポリシー] フィールドでポリシーが選択した条件が true と評価された場合にのみアクセスを拒否します。
許可ポリシー	このコンテキストで使用されるポリシー。このフィールドは、[デフォルトポリシー] フィールドが [許可ポリシー] に設定されている場合にのみ表示されます。
拒否ポリシー	このコンテキストで使用されるポリシー。このフィールドは、[デフォルトポリシー] フィールドが [拒否ポリシー] に設定されている場合にのみ表示されます。

ポリシーの入力と条件

[ポリシー入力] タブと [ポリシー条件] タブには、[許可ポリシー] または [拒否ポリシー] フィールドで選択されたポリシーの入力と条件が表示されます。これらのタブは参照できますが、ポリシーの入力や条件を変更するために使用することはできません。ポリシー設定を変更するには、[許可ポリシー] または [拒否ポリシー] フィールドの横にある参照アイコン (ⓘ) を使用してポリシーに移動します。

この例は、デフォルトでアクセスを拒否するように設定された認証後ポリシーコンテキストレコードを示しています。コンテキストでは、[アクセスポリシーの拒否] と呼ばれるポリシーを使用します。そのポリシーには、[ポリシー入力] タブと [ポリシー条件] タブに表示される一連の入力と条件があります。

[認証後ポリシーのコンテキスト] フォーム



自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

MFA (マルチファクター認証) コンテキスト

MFA (マルチファクター認証) ポリシーコンテキストは、ポリシーを使用して、ログインプロセス中に MFA を適用する方法とタイミングを定義します。

MFA コンテキストレコード

MFA (マルチファクター認証) ポリシーコンテキストは、ユーザーがログインする際に 2 番目の認証フォームを提供する必要があるかどうかを定義します。このコンテキストは、認証後および認証前のポリシーとしてインスタンスへのアクセスを拒否するわけではありません。このコンテキストで選択したポリシーは、マルチファクター認証のユーザーまたはロールベースの構成よりも優先されます。

MFA コンテキストにアクセスするには、次に移動します すべて > マルチファクター認証 > **MFA** コンテキスト.

認証後ポリシーコンテキストレコードのフィールドを使用して、インスタンスでのポリシーの使用方法を定義します。

注:

- デフォルトのポリシーがステップアップ **MFA** ポリシーの場合、ステップアップ **MFA** ポリシーで構成されたポリシーが true と評価されると、ユーザーにはマルチファクター認証が表示されます。ポリシーは、ユーザーまたはロールベースの構成よりも優先されます。
- SSO ログインを使用する MFA は、glide.authenticate.mfa.with.multisso.enabled プロパティが true に設定されている場合にのみ使用できます。
- [認証ポリシー] レコードに移動して、参照されているポリシーフィールド ([ステップアップ **MFA** ポリシー] または [ステップダウン **MFA** ポリシー]) に「ポリシー入力」を追加または編集します。

MFA コンテキストフォーム

フィールド	説明
名前	ポリシーコンテキストの名前このフィールドは静的であり、変更することはできません。
説明	コンテキストの説明
デフォルトポリシー	ポリシーを評価するときの、このコンテキストのデフォルト動作を定義します。次のオプションのいずれかを選択します。 ステップアップ MFA ポリシー [ステップアップ **MFA** ポリシー] フィールドで定義されたポリシー条件が true と評価された場合に MFA がユーザーに強制されます。 ステップダウン MFA ポリシー デフォルトで MFA を適用します。[ステップダウン **MFA** ポリシー] フィールドで定義されたポリシー条件が true と評価された場合にかぎり、MFA はユーザーに強制されません。
ステップアップ MFA ポリシー	このコンテキストで使用されるポリシー。このフィールドは、[デフォルトポリシー] フィールドが [ステップアップ **MFA** ポリシー] に設定されている場合にのみ表示されます。
ステップダウン MFA ポリシー	このコンテキストで使用されるポリシー。このフィールドは、[デフォルトポリシー] フィールドが [ステップダウン **MFA** ポリシー] に設定されている場合にのみ表示されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

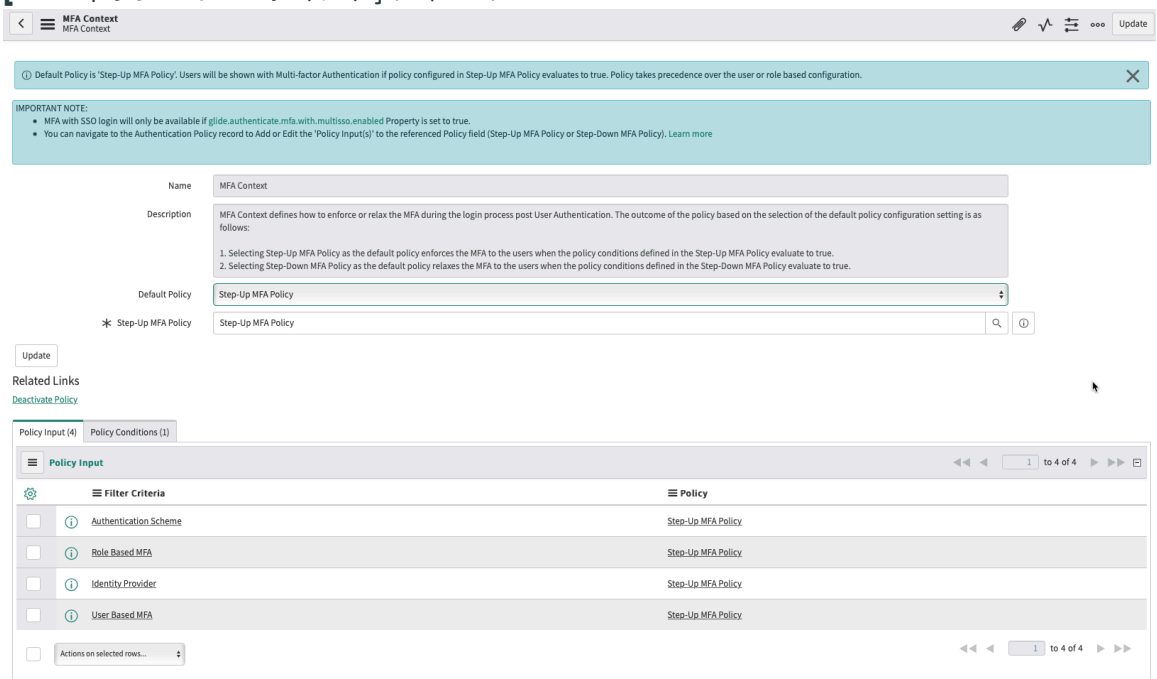
ポリシーの入力と条件

[ポリシー入力] タブと [ポリシー条件] タブには、[ステップアップ **MFA** ポリシー] または [ステップダウン **MFA** ポリシー] フィールドで選択されたポリシーの入力と条件が表示されます。これらのタブは参照できますが、ポリシーの入力や条件を変更するために使用することはできません。ポリシー設定を変更するには、[ステップアップ **MFA** ポリシー] または [ステップダウン **MFA** ポリシー] フィールドの横にある参照アイコン (ⓘ) を使用してポリシーに移動します。

注:
ポリシー条件はここから作成できますが、ポリシーページから新しいポリシー条件を追加することをお勧めします。

この例は、ステップアップ MFA ポリシーを使用して構成された MFA コンテキストレコードを示しています。このデフォルトポリシーは、ポリシーで定義されている条件が true と評価された場合にのみ MFA が適用されることを意味します。コンテキストは、[ステップアップ **MFA** ポリシー] と呼ばれるポリシーを使用します。そのポリシーには、[ポリシー入力] タブと [ポリシー条件] タブに表示される一連の入力と条件があります。

[MFA ポリシーのコンテキスト] フォーム



アカウント復旧のコンテキスト

アカウント復旧コンテキストでは、ポリシーを使用して、アカウント復旧を確立する方法とタイミングを定義します。

管理者は、次の場所に移動して、このコンテキストとそれに関連するポリシーを表示および変更できます マルチプロバイダー **SSO** > アカウント復旧 > アカウント復旧のコンテキスト.

注:
デフォルトでは、ポリシーは [許可ポリシー] です。ユーザーのログインはデフォルトで制限されており、[許可ポリシー] で定義された条件が true と評価された場合にのみログインが許可されます。

アカウント復旧コンテキストレコードのフィールドを使用して、インスタンスでのポリシーの使用方法を定義します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

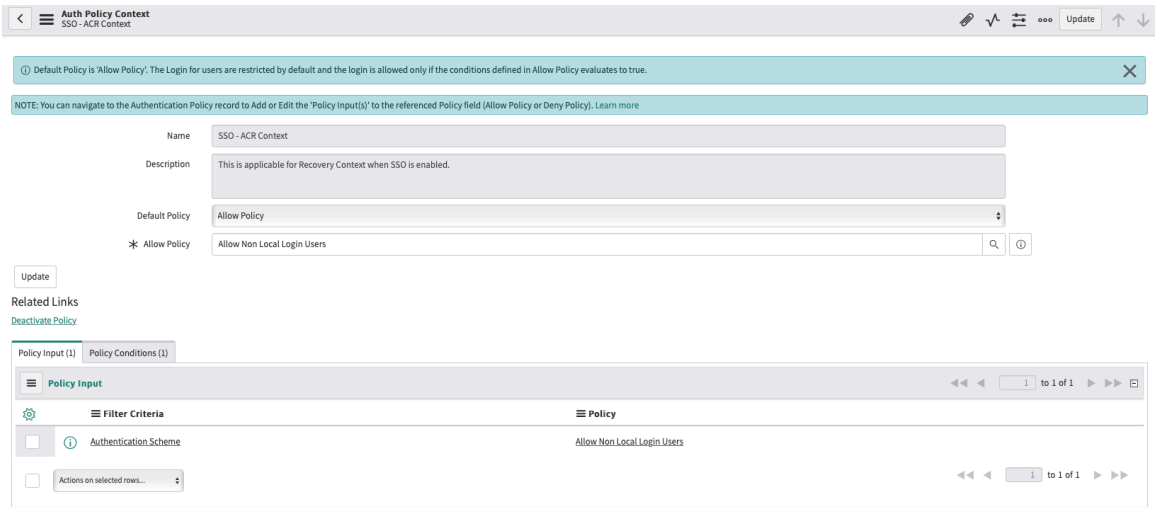
アカウント復旧のコンテキストフォーム

フィールド	説明
名前	ポリシーコンテキストの名前このフィールドは静的であり、変更することはできません。
説明	コンテキストの説明
デフォルトポリシー	ポリシーを評価するときの、このコンテキストのデフォルト動作を定義します。次のオプションのいずれかを選択します。 • 許可ポリシー • 拒否ポリシー
許可ポリシー	このフィールドは、[デフォルトポリシー] フィールドが [許可ポリシー] に設定されている場合にのみ表示されます。
拒否ポリシー	このフィールドは、[デフォルトポリシー] フィールドが [拒否ポリシー] に設定されている場合にのみ表示されます。

ポリシーの入力と条件

[ポリシー入力] タブと [ポリシー条件] タブには、[許可ポリシー] または [拒否ポリシー] フィールドで選択されたポリシーの入力と条件が表示されます。これらのタブは参照できますが、ポリシーの入力や条件を変更するために使用することはできません。ポリシー設定を変更するには、[許可ポリシー] または [拒否ポリシー] フィールドの横にある [このレコードをプレビュー **(Preview this record)]** アイコンを使用してポリシーに移動します。

注:
ポリシー条件はここから作成できますが、ポリシーページから新しいポリシー条件を追加することをお勧めします。



セッション検証コンテキスト

セッション検証コンテキストは、セッションまたは Cookie のハイジャックに対する追加の保護レイヤーとして使用します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ポリシーフレームワークで 適応認証 セッション検証コンテキストを使用できます。フレームワークは、認証ポリシーを使用して認証要求を評価してから、ポリシーの入力と条件に基づいてアクセスを拒否または許可します。

セッション検証コンテキストポリシーは、認証後ポリシーと組み合わせて使用することができ、管理者はログインセッション中に特定またはすべてのユーザーに IP 制限を適用できます。

セッション検証コンテキスト機能は、設定した条件に基づいて IP アドレスを評価し、セッション内のインスタンスへのアクセスを許可します。セッション検証コンテキストの結果は次のとおりです。

- 拒否ポリシー: 既定のポリシーとして [拒否アクセス ポリシー] を選択すると、ユーザーは既定でセッションを続行できます。セッションは、アクセス拒否ポリシーで定義されているポリシー条件の 1 つが true と評価された場合にのみ終了します。
- 許可ポリシー: 既定のポリシーとして [アクセス許可ポリシー] を選択すると、アクセス許可ポリシーで定義されているポリシー条件の 1 つが true と評価されない限り、ユーザー セッションがすぐに終了します。

注:

- 認証ポリシーのセッション検証コンテキストは、既定で 許可ポリシー に設定されています。
- セッション検証コンテキストは、許可ポリシーによって実装されます。コンテキストを拒否ポリシーに設定することはお勧めしません。

セッション検証コンテキストは、次のメカニズムに基づいて機能します。

- ユーザー要求からのセッション作成時にユーザーの IP アドレスをキャプチャし、セッションとデータベースに保存します。
- 要求の IP アドレスがセッション内の IP アドレスと異なる場合、またはお客様が定義した有効な IP 範囲の範囲外である場合に、要求を拒否します。

注:
セッション検証コンテキストは次のとおりです。

- 認証されたユーザーのみが使用できます。
- ゲストユーザーセッションまたはネイティブモバイルアプリには適用されません。
- オプションであり、構成できるという要件に基づいています。
- ログイン後の要求に対してのみ実行されます。

セッション検証の利点

セッション検証コンテキストには、次の利点があります。

- ハイジャック犯がユーザーのセッションCookieをあるデバイスから別のデバイスにコピーしてセッションを偽装するときのアクセス ServiceNow を制限します。
- ユーザーが安全でないネットワークを使用している場合、ユーザーのセッションアクセスを制限します。
- ユーザーログインのユーザーグループまたはロール別にさまざまなルールと IP 範囲を設定します。

セッション検証コンテキストレコード

セッション検証コンテキストのポリシーは、ログイン後の要求を実行します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

セッション検証ポリシーコンテキストレコードのフィールドを使用して、インスタンスでのポリシーの使用方法を定義します。

[セッション検証コンテキスト] フォーム

フィールド	説明
名前	ポリシーコンテキストの名前このフィールドは静的であり、変更できません。
説明	コンテキストの説明。
デフォルトポリシー	ポリシーを評価するときの、このコンテキストのデフォルト動作を定義します。次のオプションのいずれかを選択します。 許可ポリシー デフォルトですべてのユーザーへのアクセスを拒否し、[許可ポリシー] フィールドの条件が true と評価された場合にのみアクセスを許可します。 拒否ポリシー デフォルトですべてのユーザーへのアクセスを許可し、[拒否ポリシー] フィールドの条件が true と評価された場合にのみアクセスを拒否します。
許可ポリシー	このコンテキストで使用されるポリシー。このフィールドは、[デフォルトポリシー] フィールドが [許可ポリシー] に設定されている場合にのみ表示されます。
拒否ポリシー	このコンテキストで使用されるポリシー。このフィールドは、[デフォルトポリシー] フィールドが [拒否ポリシー] に設定されている場合にのみ表示されます。

ポリシー入力とポリシー条件に基づいて、[セッション検証ポリシー] を [許可ポリシー] または [拒否ポリシー] として選択できます。

注:

セッション検証ポリシーには、IP、ロール、およびグループのフィルター基準のみを使用できます。

ポリシーの入力と条件

[ポリシー入力] タブと [ポリシー条件] タブには、[許可ポリシー] または [拒否ポリシー] フィールドで選択されたポリシーの入力と条件が表示されます。これらのタブは参照として機能します。ただし、ポリシーの入力や条件を変更するために使用することはできません。ポリシーを変更するには、[許可ポリシー] または [拒否ポリシー] フィールドの横にある参照アイコン ( ) を使用してポリシーに移動します。

セッション検証コンテキストの有効化

セッション検証コンテキストを使用して、ハイジャック犯があるデバイスから別のデバイスにユーザーのセッションCookieをコピーしてセッションを偽装するときにアクセスを制限したり、安全でないネットワークを使用している場合はユーザーのセッションアクセス ServiceNow を制限したりします。.

始める前に
必要なロール：admin

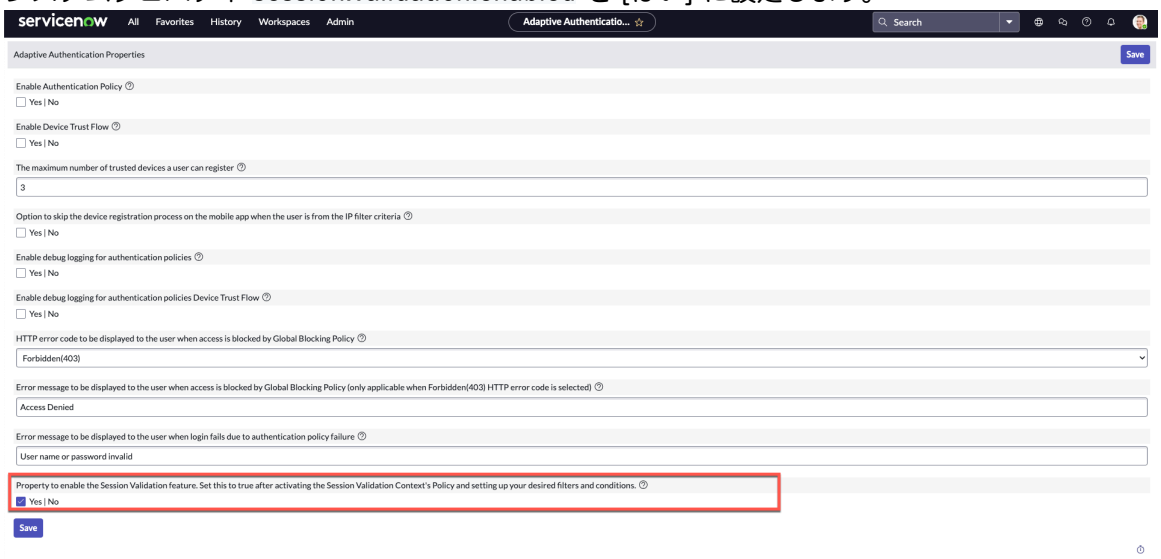
セッション検証を使用するには、次の手順を実行する必要があります。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

手順

1. 移動先 すべて > 適応認証 > 認証ポリシー > すべてのポリシー.
2. [ポリシー (sys_authentication_policy_list.do)] ページでセッション検証ポリシーを選択します。
3. ポリシー 入力 と ポリシー条件を指定します。
4. 追加したフィルターの条件を **true** または **false** に設定します。
5. ポリシー入力と条件で [セッション検証ポリシー] を設定した後、[アクティブ] チェックボックスをオンにしてポリシーを有効にします。
6. インスタンスに SSO が設定されている場合は、sso_properties テーブルのデフォルトの ID プロバイダーの [**AuthnRequest** の強制 **(Force AuthnRequest**)] チェックボックスをオンにします。
7. 移動先 すべて > 適応認証 > 認証ポリシー > プロパティ.
8. システムプロパティ session.validation.enabled を [はい] に設定します。



自動翻訳

タスクの結果
セッション検証機能が有効になります。この機能を使用するために、ポリシーのポリシー入力と条件を構成できます。詳細については、「チュートリアル: セッション検証の設定」を参照してください。

チュートリアル: セッション検証の設定

適応認証フレームワーク内でセッション検証を構成して、セッションまたは Cookie ハイジャックに対する保護の追加レイヤーとして提供します。

始める前に
必要なロール：admin

必要なプラグイン: 適応認証 (com.snc.adaptive_authentication)

セッション検証を構成するには、次の手順を実行する必要があります。

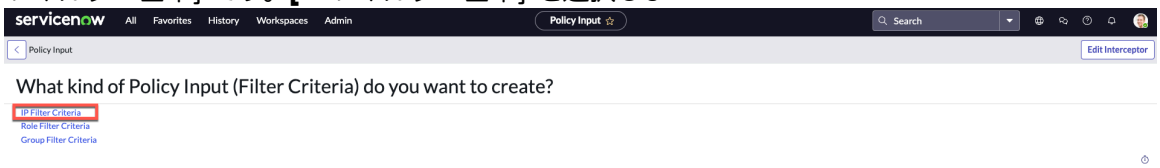
手順

1. 移動先 すべて > 適応認証 > 認証ポリシー > すべてのポリシー.
2. [ポリシー (sys_authentication_policy_list.do)] ページでセッション検証ポリシーを選択します。
3. [ポリシーの入力] を選択します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

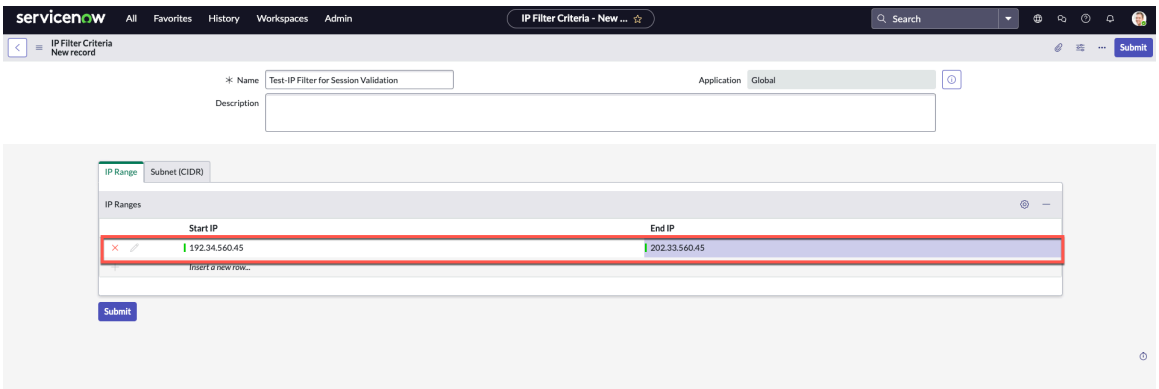
a. [新規] または [編集] を選択します。

b. 作成するポリシー入力の種類 (フィルター基準) を選択します。使用可能なオプションは、[IP]、[ロール]、および [グループのフィルター基準] です。**[IP** フィルター基準] を選択します。



す。

c. フォームにフィルターの詳細を入力し、 **IP** 範囲を入力します。



IP フィルタの作成方法の詳細については、次を参照してください IP フィルター基準の作成。

d. [送信] を選択します。

4. [セッション検証ポリシー] ページで [ポリシー条件] を選択します。

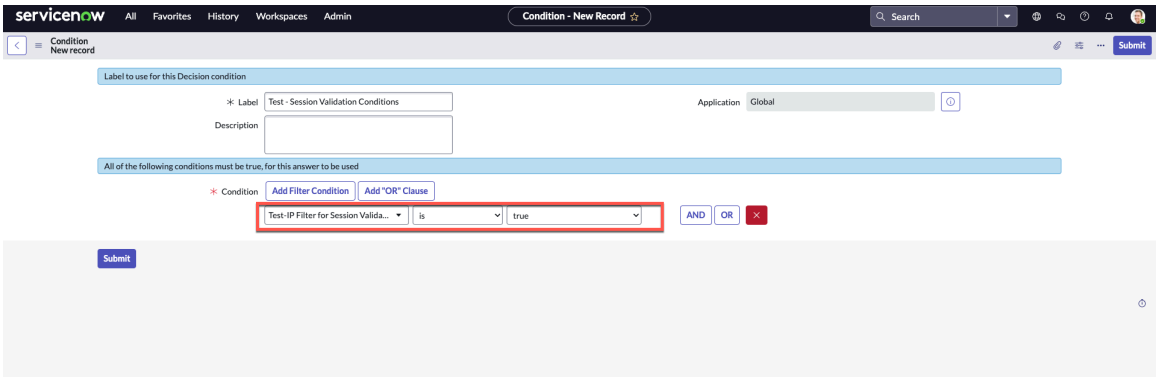
a. [新規] を選択します。

b. フォームに入力し、ポリシー入力の条件を設定します。

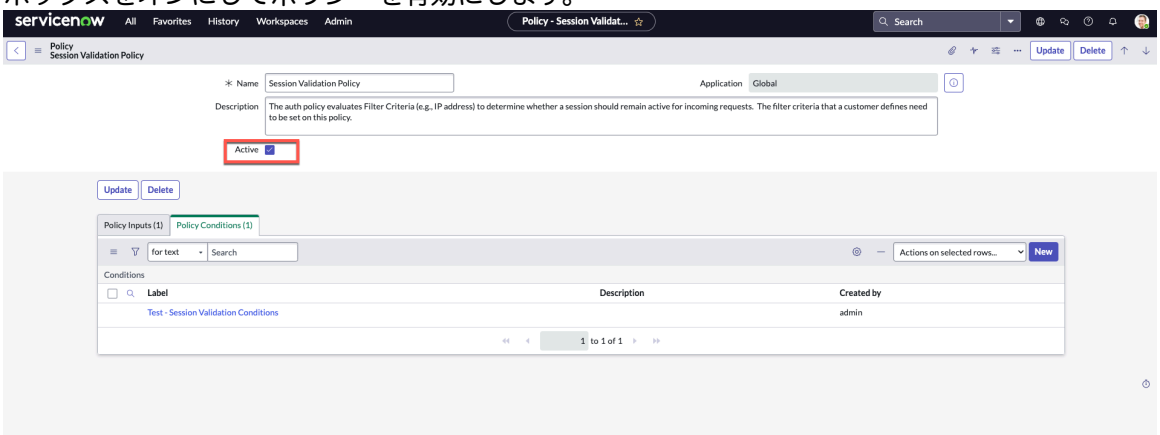
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

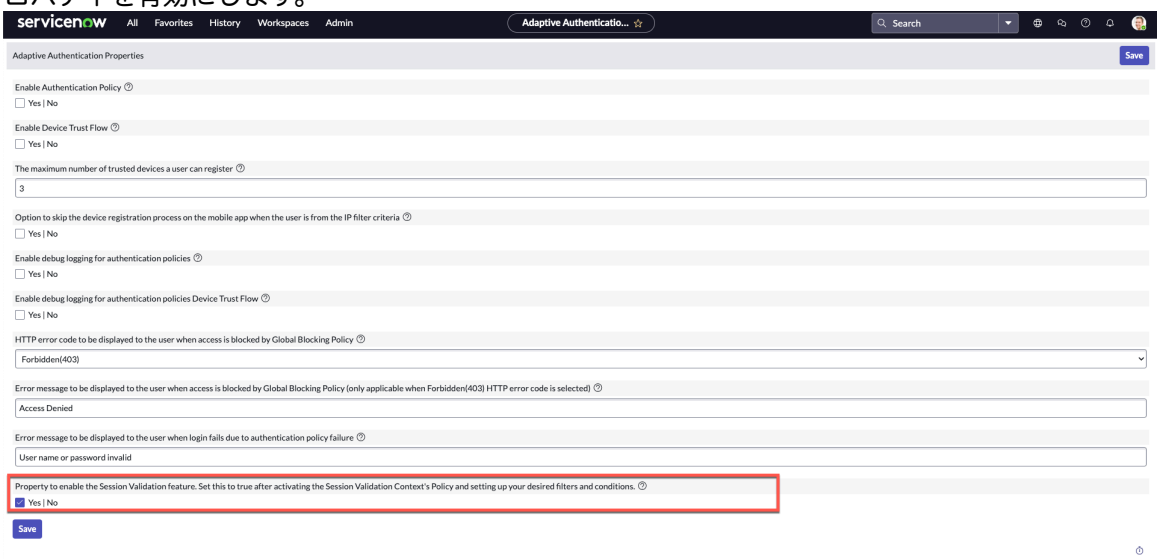
注:
ポリシー入力の構成に基づいて、条件を true または false に設定できます。この例では true に設定されています。この場合、条件を true に設定すると、設定された IP アドレスを持つユーザーのみがログインできます。



5. ポリシー入力と条件でセッション検証ポリシーをセットアップした後に、[アクティブ] チェックボックスをオンにしてポリシーを有効にします。



6. 移動先 すべて > 適応認証 > 認証ポリシー > プロパティ をクリックし、[Session Validation] プロパティを有効にします。

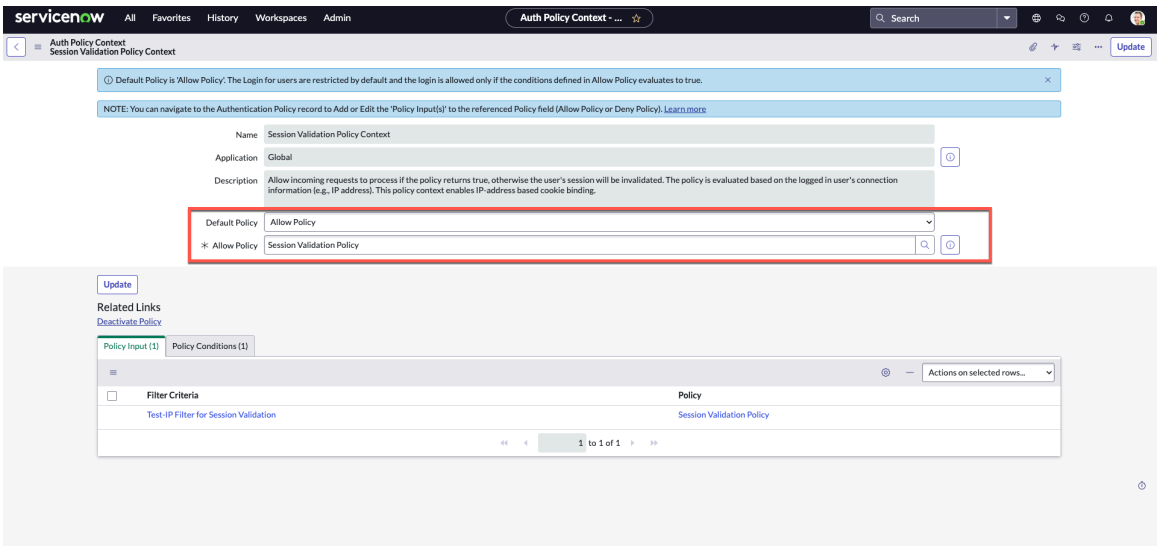


7. 移動先 すべて > 適応認証 > 認証ポリシーのコンテキスト > セッション検証コンテキスト.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

8. デフォルトポリシーを [許可ポリシー] または [拒否 ポリシー] に設定して、ポリシー入力とポリシー条件に従ってセッション検証コンテキストを設定します。

   注:
   デフォルトでは、アクセス権限は以下のように設定されます。
   - セッション検証コンテキストが [許可ポリシー] に設定されている。
   - セッション検証ポリシーとして [許可ポリシー] が選択されています。



タスクの結果
この設定では、以下に基づいてログインセッションが評価されます。

- ハイジャック犯があるデバイスから別のデバイスにユーザーのセッション Cookie をコピーしてセッションを偽装するときに、インスタンスへのアクセス ServiceNow を制限します。
- ユーザーが安全でないネットワークを使用している場合、ユーザーのセッションアクセスを制限します。

認証ポリシー

認証ポリシーは、指定されたポリシー条件に基づいて認証要求を評価し、ポリシー条件評価の出力に応じてアクセスを許可または拒否します。たとえば、[アクセス許可ポリシー] で指定されたすべてのポリシー条件が true と評価された場合にのみ、アクセスが許可されます。

ビルトイン認証ポリシーを使用するか、セキュリティ要件に従って認証ポリシーを作成します。インスタンスのポリシーを確認するには、次の場所に移動します。 適応認証 > 認証ポリシー > すべてのポリシー.

注:
どの時点でも、[アクセスポリシーを許可] または [アクセスポリシーを拒否] のいずれかを実行できますが、両方を実行することはできません。

ポリシー	説明
アクセスポリシーを許可	デフォルトですべての認証要求を拒否します。指定されたポリシー条件に一致する認証要求のみを許可します。
アクセス事前認証ポリシーを許可	アクセス事前認証ポリシーを許可します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ポリシー	説明
ローカルログイン以外のユーザーを許可 (Allow non local login users)	ローカルログイン以外のユーザーを許可するには、このポリシーを選択します。SSO 復旧フローのコンテキストで使用されます。
アクセスポリシーの拒否	デフォルトですべての認証要求を許可します。指定されたポリシー条件に一致する認証要求のみを拒否します。
グローバルブロックポリシー	認証前にユーザーと API のアクセス要求を拒否します。このポリシーは、IP アドレスアクセス制御の代わりに使用できます。
セッション検証ポリシー	認証ポリシーは、フィルター基準 (IP アドレスなど) を評価して、着信要求に対してセッションをアクティブなままにしておく必要があるかどうかを判断します。このポリシーのフィルター基準を設定する必要があります。
ローカルログイン拒否ポリシー (Local login deny policy)	すべてのローカルログインをブロックするには、このポリシーを選択します。SSO 復旧フローのコンテキストで使用されます。
ステップダウン MFA ポリシー	ユーザーが MFA 認証を必要としない場合は、デフォルトのポリシーとして [ステップダウン **MFA** ポリシー] を選択します。ステップアップ MFA ポリシーで定義されているポリシー条件が true と評価される場合、ユーザーは MFA を使用してログインする必要はありません。
ステップアップ MFA ポリシー	ステップアップ MFA ポリシーで定義されたポリシー条件が true と評価される場合、MFA 認証を要求するデフォルトポリシーとして [ステップアップ **MFA** ポリシー] を選択します。

自動翻訳

認証ポリシーの構成

認証ポリシーを構成して、インスタンスへのアクセスを許可したり、マルチファクター認証を適用したりするために使用する入力と条件を定義します。

始める前に

必要なロール：管理者

手順

1. 移動先 すべて > 適応認証 > 認証ポリシー > すべてのポリシー.

> **注:**
> 完成したポリシーの例として、次のポリシーをインスタンスで確認できます。
> - デモ POLICY - 管理者のローカルログインを信頼できる IP 範囲からのみ許可
> - デモ POLICY - 管理者のローカルログインのみ許可
> - デモ POLICY - ユーザー名およびパスワードベースの認証を特定のユーザーに制限

2. [新規] ボタンをクリックして、新しいポリシーレコードを作成します。

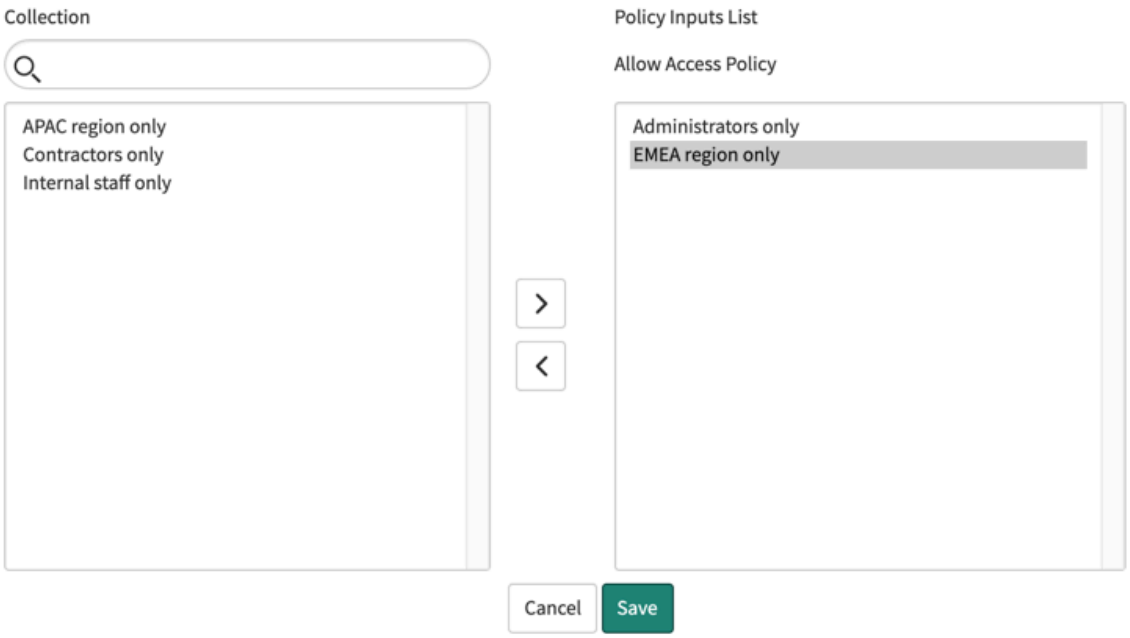
3. [ポリシー] フォームの各フィールドに入力します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ポリシーフォーム

フィールド	説明
名前	ポリシーの名前。
アプリケーション	ポリシーのスコープ対象のアプリケーション。このフィールドには現在のアプリケーションが自動的に入力されます。
説明	ポリシーの説明
有効	ポリシーがアクティブかどうか。

4. [ポリシーの入力] タブで、[編集] をクリックします。
5. [コレクション] リストから 1 つ以上のフィルター基準を選択し、[アクセスポリシーを許可] リストの [ポリシー入力] リストに移動します。



注:
このセクションで使用する独自のフィルター基準を作成する方法については、「フィルター基準 」を参照してください。

6. [ポリシー条件] タブで、[新規] をクリックします。
7. フォームのフィールドに入力します。

[条件] フォーム

フィールド	説明
ラベル	条件を識別する名前
説明	条件の説明
条件	認証要求を評価するために使用される複数のポリシー入力 (フィルター基準) の論理的な組み合わせ。たとえば、信頼できる IP アドレスの

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	リストから請負会社のみを許可するような条件を作成できます。

8. オプション: 追加のポリシー条件を作成するには、手順 7 を繰り返します。

   注:
   複数のポリシー条件を作成する場合、アクセスポリシーの最終的な出力は、すべてのポリシー条件の論理 OR 出力によって決まります。これは、ポリシー条件のいずれかが満たされると、ポリシーが true と評価されることを意味します。

9. [保存] をクリックします。

認証ポリシーを認証ポリシーコンテキストに追加

認証ポリシーを、認証ポリシーコンテキストのいずれかに追加します。認証コンテキストは、ポリシー入力と条件を使用して、ユーザーによるインスタンスへのアクセスが許可されているかどうか、またはユーザーに MFA が適用されているかどうかを判断します。

始める前に
必要なロール：管理者

手順

1. 移動先 すべて > 適応認証 > 認証ポリシーのコンテキストをクリックし、必要に応じていずれかのエントリーを選択します。

   事前認証のコンテキスト

   事前承認コンテキストを使用して、ユーザーにログイン画面が表示される前にポリシーを評価します。ユーザーは、この評価に基づいてアクセスを許可または拒否されます。

   認証後のコンテキスト

   ユーザーがログイン資格情報を入力した後、承認後のコンテキストを使用してポリシーを評価します。ユーザーは、この評価に基づいてアクセスを許可または拒否されます。この評価はインスタンスがユーザーを識別した後に行われるため、このコンテキストのポリシーは、ロールやグループなどのユーザーデータに基づいて評価を行うことができます。

   MFA コンテキスト

   MFA コンテキストを使用して、ユーザーがログイン時にマルチファクター認証を使用する必要があるかどうかを判断します。

   セッション検証コンテキスト

   セッション検証コンテキストを使用して、フィルターとして定義された条件に基づいて設定された IP アドレスを評価し、セッション内のインスタンスへのアクセスを許可します。

2. [デフォルトポリシー] フィールドで、値を選択します。このフィールドの値は、ポリシーの条件の結果をコンテキストでどのように使用するのかを決定します。
   このフィールドで使用できるオプションは、選択したコンテキストによって異なります。これらのコンテキストの詳細については、「認証ポリシーのコンテキスト」を参照してください。

3. コンテキストにポリシーをアサインします。フィールドの名前は、選択したコンテキストによって異なります。

   認証前および認証後のコンテキスト

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

これらのコンテキストには、[デフォルトポリシー] フィールドの選択に応じて [拒否ポリシー] または [許可ポリシー] フィールドがあります。

MFA コンテキスト

このコンテキストには、[デフォルトポリシー] フィールドの選択に応じて [ステップアップ **MFA** ポリシー] または [ステップダウン **MFA** ポリシー] フィールドがあります。

セッション検証コンテキスト

このコンテキストには、[デフォルトポリシー] フィールドの選択に応じて [許可ポリシー] または [拒否ポリシー] フィールドがあります。

4. [更新] をクリックします。
レコードを更新した後、[ポリシー入力] タブと [ポリシー条件] タブでポリシーの入力と条件を確認できます。

適応認証プロパティの設定

適応認証をアクティブ化した後、セキュリティ要件に従って適応認証プロパティを設定します。

始める前に

必要なロール：管理者

手順

1. 移動先 すべて > 適応認証 > 認証ポリシー > プロパティ.

2. 次のプロパティを設定します。

適応認証プロパティ

プロパティ	説明	値
認証ポリシーの有効化 (glide.authenticate.auth.policy.enabled)	認証ポリシーを有効にするオプション	◯| #
認証ポリシーのデバッグログ記録の有効化 (glide.authenticate.policy.debug)	認証ポリシーのデバッグログ記録を有効にするオプション	◯| #
グローバルブロックポリシーによってアクセスがブロックされたときにユーザーに表示される HTTP エラーコード (glide.authenticate.global.blocking_policy.error_code)	グローバルブロックポリシーによってユーザーのログインがブロックされている場合にログイン中に表示される HTTP エラーコード (HTTP error code that displays during login when the Global Blocking Policy blocks a user login.)	次から選択します。 ◦ Forbidden(403) ◦ Not Found(404)
グローバルブロックポリシーによってアクセスがブロックされたときにユーザーに表示されるエラーメッセージ (Forbidden (403) HTTP エラーコードが選択されている場合にのみ適用されます) (glide.authenticate.global.blocking_policy.error_message)	グローバルブロックポリシーがアクセスをブロックするときに表示されるエラーメッセージ。	テキストフィールド
デバイス信頼フローの有効化 (glide.authenticate.preauth.allow.trusted.device)	信頼できるデバイスフローを有効にするオプション。	◯| #

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

プロパティ	説明	値
ユーザーが登録可能な信頼できるデバイスの最大数 (glide.trusted.device.max.count)	ユーザーが登録可能な信頼できるデバイスの最大数です。	テキストフィールド
ユーザーが信頼できるネットワークからアクセスしている場合、デバイス信頼フローでのデバイス登録をスキップ (glide.authenticate.preauth.skip.user.registration)	ユーザーが信頼できるネットワークから登録しようとしている場合に登録をスキップするオプション	◯| #
セッション検証機能を有効にするプロパティ。セッション検証コンテキストのポリシーを有効にし、必要なフィルターと条件 (session.validation.enabled) を設定した後に、これを true に設定します	セッション検証機能を有効にするオプション。セッション検証コンテキストのポリシーをアクティブにし、必要なフィルターと条件を設定した後に、これを true に設定します。	◯| #

チュートリアル：適応認証の設定

次の手順例を使用して、インスタンスで適応認証を設定します。

このチュートリアルを使用するには、適応認証がアクティブ化されているインスタンスが必要です。このプロセスの詳細については、「適応認証のアクティブ化」を参照してください。

この例では、新しいポリシーを作成してインスタンスに適用する手順を示します。このチュートリアルでは、次のことを実行します。

フィルター基準レコードの作成

ポリシーの入力として使用するグループフィルター基準レコードを作成します。このレコードにより、ポリシーはユーザーのグループに基づいてアクセスを決定できます。これらの手順では、ポリシーがアクセスを決定するために使用するグループを定義します。

ポリシーの作成

ユーザーがインスタンスにアクセスできるかどうかを決定するポリシーを作成します。このポリシーでは、作成するグループフィルター基準レコードを入力として使用します。これらの手順では、ポリシーがポリシー入力を使用してユーザーアクセスを決定する方法を定義するポリシー条件も定義します。

ポリシーコンテキストの設定

新しいポリシーを使用する認証後ポリシーのコンテキストを設定します。設定すると、インスタンスは、フィルター基準レコードで定義されたグループ内のユーザーのアクセスを拒否します。

フィルター基準レコードの作成

適応認証ポリシーのポリシー入力として使用する基準レコードの作成方法を説明します。

始める前に

必要なロール：admin

ユーザーグループに基づいてインスタンスへのアクセスを拒否するには、グループフィルター基準レコードを作成する必要があります。このレコードは、ポリシーでアクセスを許可または拒否できるユーザーグループまたはユーザーグループセットを定義します。この例では、単一のユーザーグループのグループフィルター基準レコードを作成します。

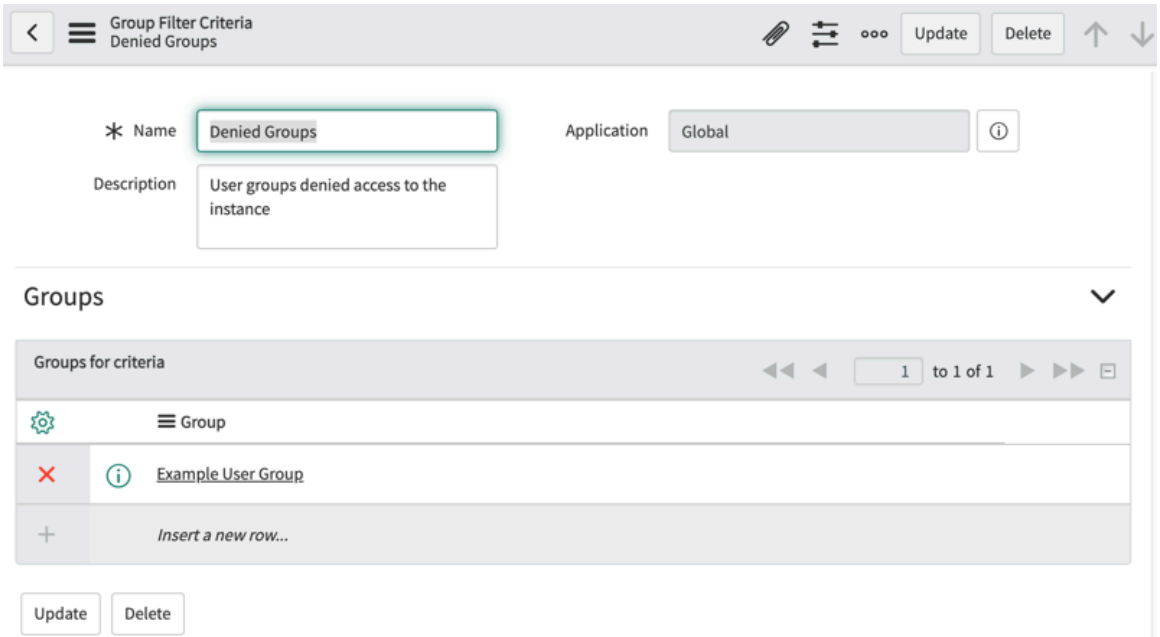
ユーザーグループとインスタンスでの使用方法の詳細については、「」を参照してください Exploring user administration 。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. 移動先 すべて > 適応認証 > フィルター基準 > グループ基準.
2. [新規] をクリックして、新しいレコードを作成します。
3. [名前] フィールドに、レコードの名前を入力します。例：拒否グループ。
4. [説明]フィールドに、簡単な説明文を入力します。例：インスタンスへのアクセスを拒否するユーザーグループ。
5. [基準のグループ] リストで、[新規行を挿入...] をダブルクリックします。
6. ユーザーグループの名前を入力するか、参照アイコン ( ) をクリックしてリストからグループを選択します。
   フィルター基準の新しいユーザーグループを作成する場合は、参照アイコン ( ) をクリックしてから、[新規] ボタンをクリックします。ユーザーグループの作成の詳細については、「ユーザーグループの作成」を参照してください。
7. ユーザーグループを追加したら、[送信] をクリックして基準レコードを保存します。



ポリシーの作成

グループフィルター基準で定義されたユーザーグループへのアクセスを拒否するポリシーを作成する方法について説明します。

始める前に

必要なロール：管理者

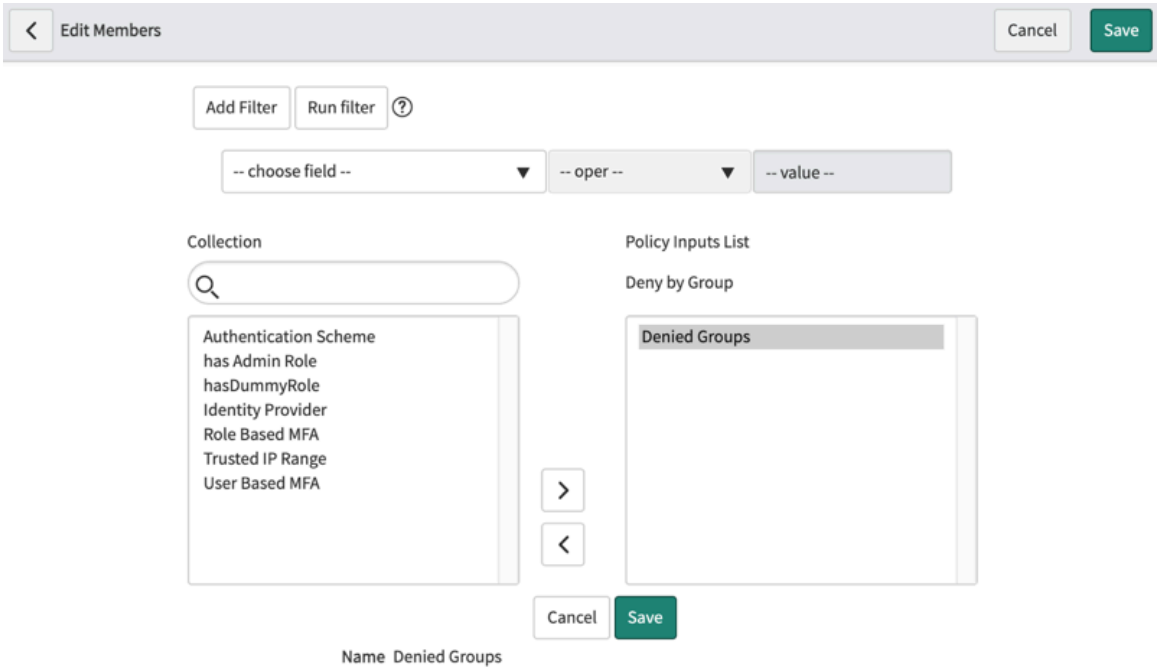
手順

1. 移動先 すべて > 適応認証 > 認証ポリシー > すべてのポリシー.
2. [ポリシー] リストで、[新規] をクリックします。
3. [名前] フィールドに、レコードの名前を入力します。例：拒否グループ。
4. [説明]フィールドに、簡単な説明文を入力します。例：インスタンスへのアクセスを拒否するユーザーグループ。
5. フォームヘッダーを右クリックし、[保存] をクリックします。
   保存した後、[ポリシー入力] および [ポリシー条件] リストがフォームに表示されます。

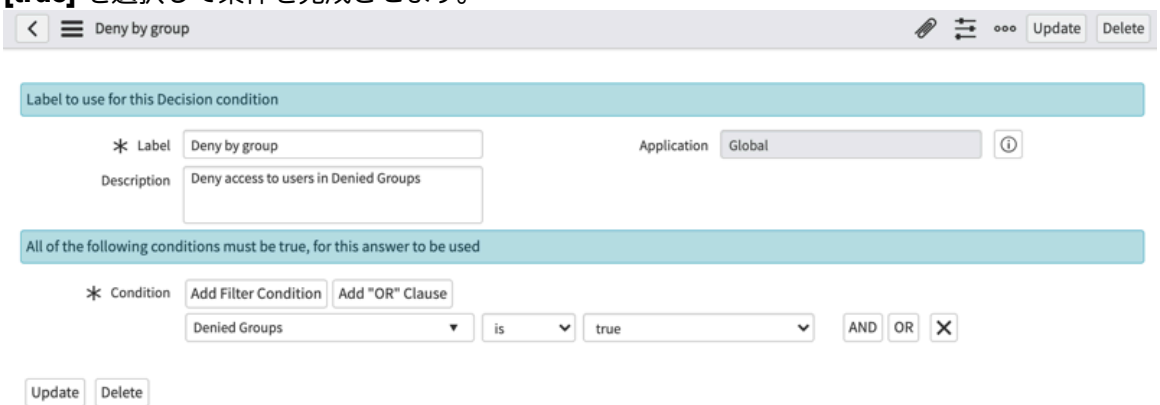
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

6. [ポリシーの入力] リストで、[編集] をクリックします。
7. リストコレクターで、前のステップで作成したフィルター基準をポリシーに追加します。



8. [保存] をクリックします。
   インスタンスはポリシー入力を保存し、ポリシーレコードを再度表示します。
9. [ポリシー条件] 関連リストで、[新規] をクリックします。
10. [ラベル] フィールドで、この条件のラベルを作成します。例：拒否グループ。
11. [説明]フィールドに、簡単な説明文を入力します。例：拒否グループのユーザーへのアクセスを拒否。
12. [条件] フィールドで、前の手順で作成したフィルター基準を選択し、[次の値に等しい **(=)]** と **[true]** を選択して条件を完成させます。



13. [保存] をクリックします。

ポリシーコンテキストの設定

新しいポリシーを使用する認証後ポリシーのコンテキストを設定します。設定すると、インスタンスでは、フィルター基準レコードで定義されたグループにいるユーザーへのアクセスを拒否します。

始める前に

必要なロール：管理者

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. 適応認証 > 認証ポリシーのコンテキスト > 認証後のコンテキスト.
   このチュートリアルで使用するポリシーはユーザーがどのグループに属しているかを評価する必要があるため、認証後コンテキストを使用する必要があります。この情報は、資格情報を入力した後にのみ使用できます。
2. [デフォルトポリシー] フィールドで、[拒否ポリシー] を選択します。
   ここでは、デフォルトでユーザーにアクセス権が付与され、ポリシー条件が true と評価された場合にのみアクセスを拒否します。
3. [拒否ポリシー] フィールドで、これまでのステップで作成した通知を選択します。
4. [更新] をクリックして、ポリシーコンテキストレコードを保存します。

信頼できるモバイルアプリ向け適応認証 (Adaptive Authentication for Trusted Mobile Apps)

信頼できないネットワークから ServiceNow にアクセスする際は、Now Mobile アプリを使用します。

信頼できるモバイルアプリ向け適応認証 (Adaptive Authentication for Trusted Mobile Apps)

信頼できるモバイルアプリ向け適応認証により、ユーザーは Now Mobile アプリ を使用して ServiceNow インスタンスにアクセスできます。インスタンスは、信頼できる IP ネットワークの境界の内側で保護されます。

ネットワーク外にいるときにインスタンスにアクセスする必要があるシナリオとしては、次のようなものがあります。

従業員がネットワーク外から Now Mobile アプリ および Employee Service Center (ポータル) にアクセスする必要がある場合。信頼できるモバイルアプリのフィルターを使用すると、ユーザーアカウントにリンクされている信頼できる Now Mobile アプリ からの受信要求を識別できます。

管理者は、ポリシーを設定できます。このポリシーによって、ユーザーが自分のモバイルデバイスを登録し、信頼できるネットワークからインスタンスにアクセスすることが可能になります。

ユーザーは、インスタンスに表示されている QR をスキャンしてモバイルデバイスを登録できます。登録後、資格情報を使用して Now Mobile アプリからインスタンスにログインできます。

> **注:**
> モバイルデバイスを登録するには、信頼できるネットワークに接続している必要があります。登録を済ませれば、他のネットワークからもインスタンスにログインできます。

特徴

管理者は、次の機能を使用できます。

- 信頼できるアプリのフィルター基準を使用してポリシーを設定する。
- 信頼できるモバイルアプリの新しいフィルター基準を使用してポリシー条件を作成する。
- ユーザーの信頼できるモバイルアプリにおけるすべてのログイン方法 (ローカルログイン、SAML、OIDC、および MFA) をサポートする。
- 信頼できるデバイスを取り消す。
- デバイス登録や取り消しのすべてのアクションに対するセキュリティイベントを追加する。追加したイベントを使用して、ユーザーに通知できます。
- 署名の失敗、Cookie の検証の失敗、無効なトークン、無効なヘッダー、またはクエリパラメーターに関するセキュリティイベントに対応する。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

- 登録されたデバイスの最大数を制御する。
- ユーザーが既存のペアリングされたデバイスを削除しない限り、新しいデバイスを登録できないようにする。
- デバイスが最後に使用された時間をキャプチャする。

信頼できるモバイルアプリのアクティブ化

認証ポリシーとフィルター条件を使用して、信頼できるモバイルアプリを使用した適応認証を有効にします。

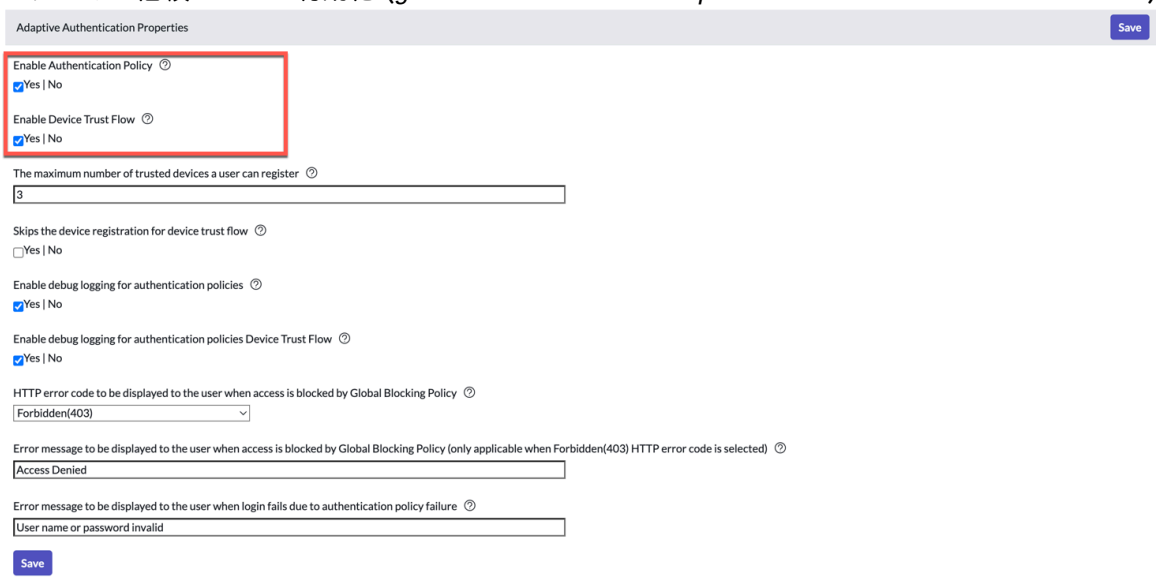
始める前に

適応認証 (*com.snc.adaptive_authentication*) プラグインがインストールされていることを確認します。

必要なロール：管理者

手順

1. 移動先 すべて > 適応認証 > 認証ポリシー > プロパティ.
2. [適応認証プロパティ] ページで、次のプロパティを有効にします。
   - 認証ポリシーの有効化 (Enable Authentication Policy) (*glide.authenticate.auth.policy.enabled*)
   - デバイス信頼フローの有効化 (*glide.authenticate.preauth.allow.trusted.device*)



> **注:**
> デバイス信頼フローのプロパティを無効にするには、信頼できるモバイルフィルターを使用して条件を削除する必要があります。そうしないと、条件の削除を要求するエラーメッセージが表示されます。

3. 移動先 すべて > 適応認証 > 認証ポリシーのコンテキスト > 事前認証のコンテキスト.
4. 事前認証のコンテキストで条件を定義します。
   詳細については、「事前承認コンテキスト」を参照してください。

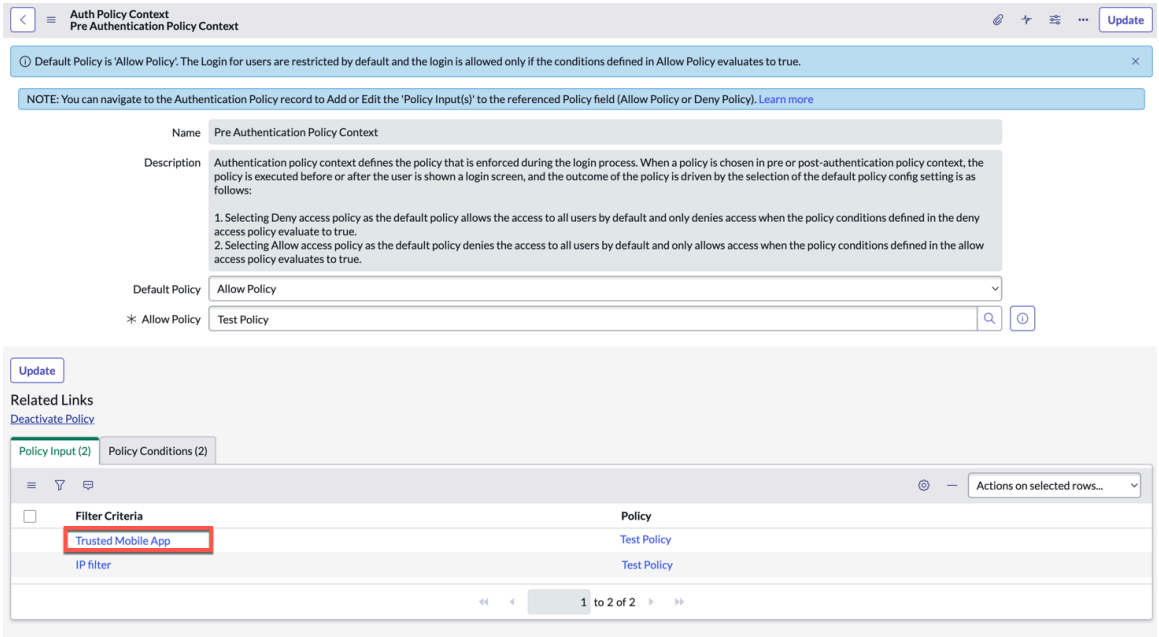
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注:
デフォルトでは、ポリシー条件は [拒否ポリシー]です。[許可ポリシー **(Allow Policy)]** に変更できます。この 2 つのポリシーは正反対です。

- [許可ポリシー **(Allow Policy)]** では、デフォルトですべてのユーザーがアクセスを拒否され、アクセス許可ポリシー条件が true の場合のみアクセスが許可されます。
- [拒否ポリシー] を使用すると、デフォルトですべてのユーザーにアクセスが許可され、アクセス拒否ポリシー条件が true の場合のみアクセスが拒否されます。

[ポリシー入力] では、[信頼できるモバイルアプリ] が、信頼できるモバイルアプリのポリシー入力となります。



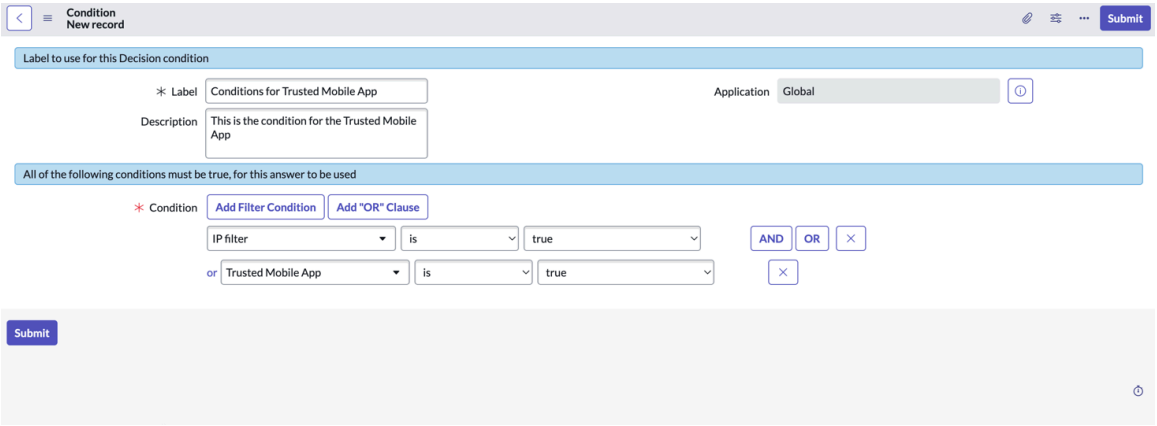
5. [ポリシー条件] で、[新規] をクリックして条件を作成します。
6. フォームの各フィールドに入力します。

[フィルター条件] フォーム

フィールド	説明
ラベル	条件の名前
説明	条件の説明
アプリケーション	このレコードのアプリケーションスコープ。
条件	AND および OR に基づく条件。認証ポリシーが [許可ポリシー **(Allow Policy)]** であるため、この画像の例では [信頼できるモバイルアプリ] の条件が true に設定されています。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



7. [送信] をクリックします。

タスクの結果

[信頼できるデバイス (Trusted Device)] 機能に対して、ポリシー入力とフィルター条件が作成されます。ユーザーは [信頼できるデバイス (Trusted Device)] 機能を使用して、信頼できないネットワークから Now Mobile アプリ を使用して ServiceNow インスタンスにアクセスできます。詳細については、「信頼できるデバイスを登録する」を参照してください。

信頼できるデバイスを登録する

ネットワーク外から ServiceNow インスタンスにアクセスできるように、信頼できるデバイスを登録します。

始める前に

信頼できるデバイスの登録を実行するには、信頼できるネットワークに入っている必要があります。

必要なロール：なし

手順

1. 次のいずれかのメニューオプションに移動します。

- Now Platformで、次の場所に移動します。 すべて > セルフサービス > プロファイル.

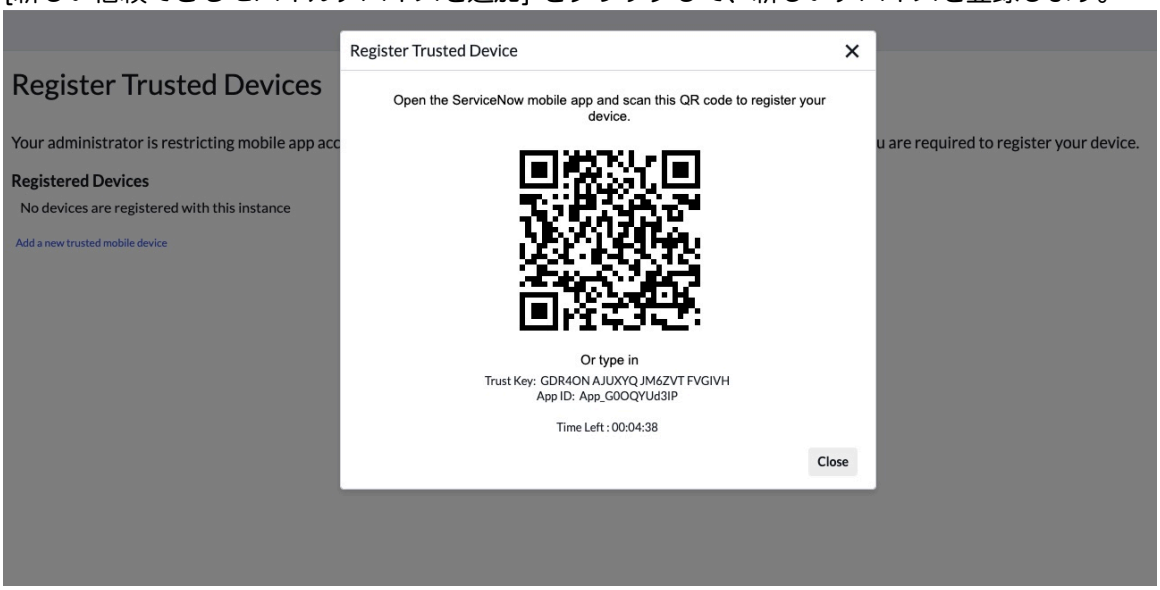
> **注:**
> インスタンスヘッダーで自分のユーザー名をクリックして、プロファイルにアクセスすることもできます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- Now Supportでプロファイルをクリックし、[信頼できるデバイス **(Trusted Device)]** を選択します。

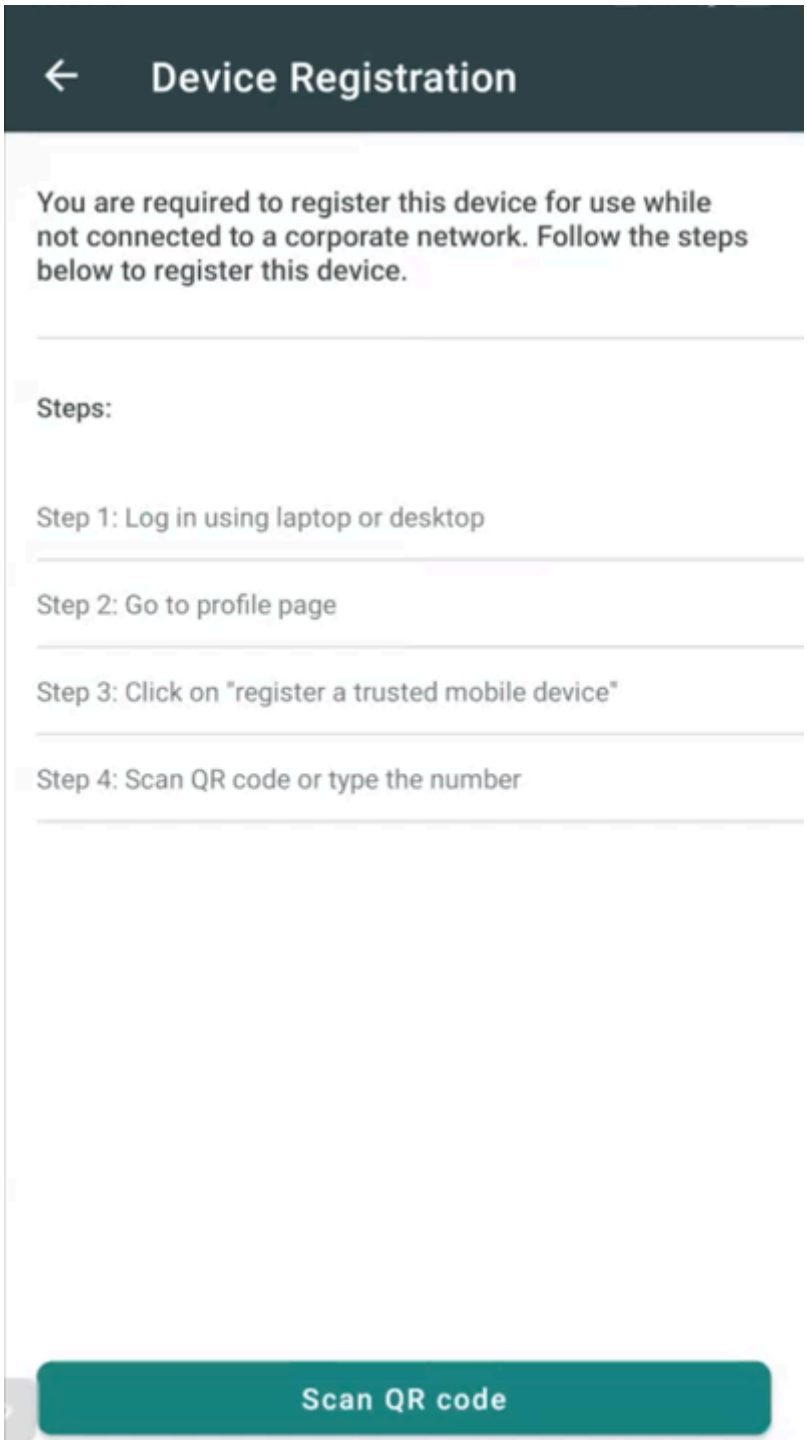
2. ユーザープロファイルで、[関連リンク] セクションの [信頼できるモバイルデバイスを登録] をクリックします。
   [信頼できるデバイスを登録] ページが表示されます。
3. [新しい信頼できるモバイルデバイスを追加] をクリックして、新しいデバイスを登録します。



4. ServiceNow モバイルアプリの [デバイス登録 (Device Registration)] 画面で、**[QR** コード をスキャン] ボタンをタップし、ラップトップまたはデスクトップに表示されている QR コードをスキャンします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



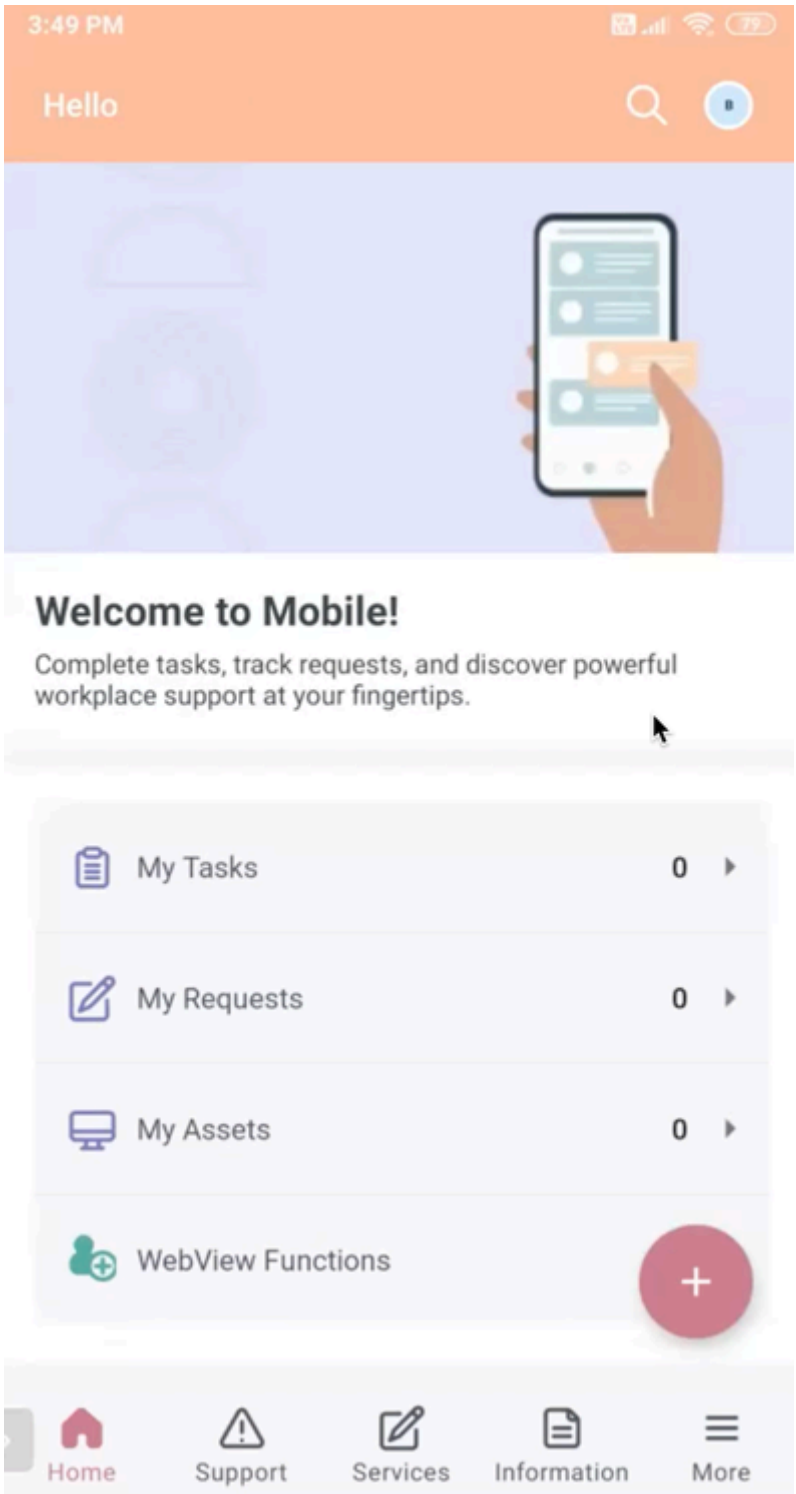
登録プロセスが完了し、認証を完了するためのログインページが表示されます。

5. 資格情報を指定して Now Mobile アプリ にログインします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

モバイルホーム画面が表示されます。



タスクの結果

ラップトップまたはデスクトップの [信頼できるデバイスを登録] ページに、登録されたデバイスが表示されます。 アイコンを使用すると、登録されたデバイスをページから削除できます。

次のタスク

移動先 すべて > 適応認証 > デバイス信頼 > デバイス登録 をクリックして、登録されたデバイスのすべての詳細を表示します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

信頼できるデバイスの管理

信頼できるデバイス登録ページから、信頼できるデバイスを管理します。

始める前に
必要なロール：なし

手順

1. 次のいずれかのメニューオプションに移動します。
   - Now Platformで、次の場所に移動します。 すべて > セルフサービス > プロファイル.

     注:
     インスタンスヘッダーで自分のユーザー名をクリックして、プロファイルにアクセスすることもできます。

   - Now Supportでプロファイルをクリックし、[信頼できるデバイス **(Trusted Device)]** を選択します。
2. ユーザープロファイルで、[関連リンク] セクションの [信頼できるデバイスを登録] をクリックします。
   [信頼できるデバイスを登録] ページが表示されます。
3. [信頼できるデバイスを登録] ページで、 アイコンをクリックしてデバイスを削除します。

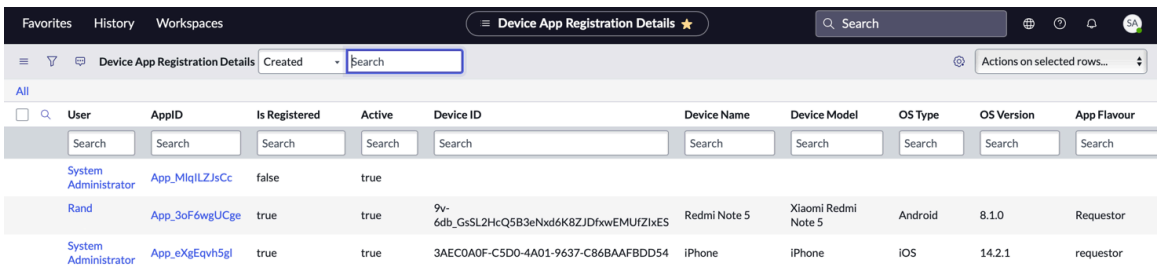
   注:
   削除されたモバイルデバイスは、再登録しないとインスタンスにアクセスできません。

登録済みデバイスの登録の詳細

ServiceNow インスタンスに登録されているデバイスの詳細を確認します。

インスタンスに登録されているデバイスの詳細をすべて表示するには、次に移動します すべて > 適応認証 > デバイス信頼 > デバイス登録.

フィルターを使用して当該のデバイスを識別します。**[AppID]** フィールドをクリックすると、登録されたデバイスの詳細が表示されます。



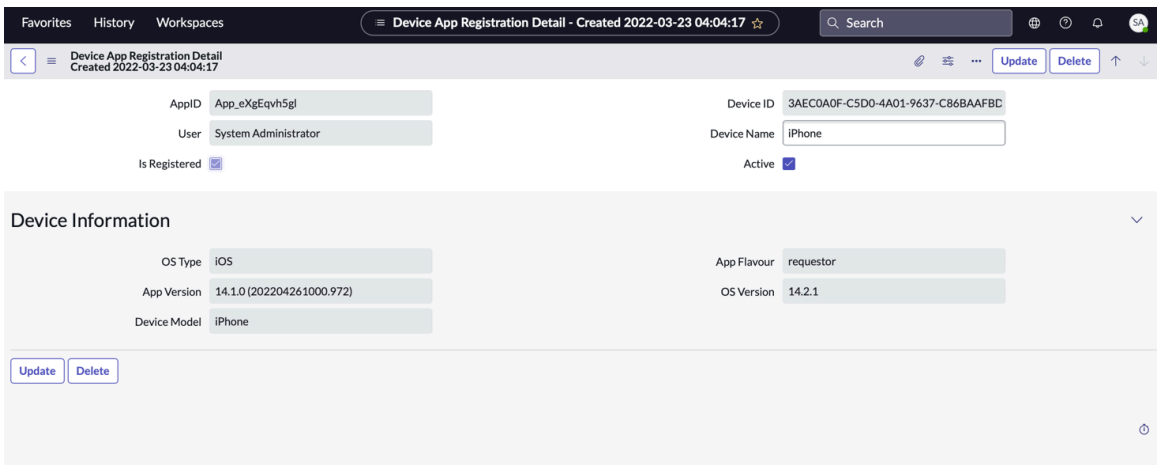
表示されるデバイスの詳細情報は次のとおりです。

- AppID
- デバイス ID

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- ユーザー
- デバイス名
- デバイス情報：
  - OS タイプ
  - アプリフレーバー
  - アプリバージョン
  - OS バージョン
  - デバイスモデル



信頼できるモバイルアプリのトラブルシューティング

信頼できるモバイルアプリの問題を解決するには、次のトラブルシューティングシナリオを確認してください。

以下のセクションで、いくつかのトラブルシューティングのシナリオとその方法について説明します。

インスタンスとモバイルに時差 (クロックスキュー) がある

クロックスキューがある場合、信頼できるデバイスを使用するにはモバイルデバイスのクロックを調整またはリセットするとよいでしょう。

QR コードが 5 分以内に期限切れになる

信頼できるデバイス機能の QR コードは 5 分以内で期限切れになります。このような場合は、クリックすると新しい QR コードを取得できます。

> **注:**
> QR コードの有効期限は延長できます。コードの有効期限を延長するには、管理者にお問い合わせください。

システムプロパティが変わっている

システムプロパティが変わっている場合は、ログインに使用できる有効な資格情報のシステムプロパティに基づいて登録を確認します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

登録デバイス数が最大に達した

デバイス登録の最大数に達した場合は、既存のデバイスを削除するか、管理者に連絡して最大デバイス数を変更してください。

API 認証

API の認証構成。

ServiceNow® API ベースの認証は、インスタンスにアクセスするユーザーの ID を検証し、インスタンスへの ServiceNow® API 呼び出しを行う際に、ユーザーのロールまたは職務に一致する機能に対してユーザーを許可します。

ServiceNow® API 認証のタイプは次のとおりです。

- 証明書ベースの認証
- OAuth
- トークンベースの認証

証明書ベースの認証

証明書ベースの認証では、信頼できる認証局 (CA) からの証明書を使用して、受信 API 要求を相互に認証できます。

受信 Web サービスの証明書ベースの認証

ServiceNow SOAP および REST API への受信要求を認証します。受信 Web サービスの相互認証を設定するには、「証明書ベースの認証の設定」を参照してください。

OAuth

OAuth ベースの認証は、認証プロトコルを使用してシステムで信頼を確立しようとするクライアントの ID を検証します。

OAuth 2.0 - オープン認証は認証の業界標準プロトコルであり、Web アプリケーション、デスクトップアプリケーション、およびモバイルデバイス向けの特定の認証フローを提供すると同時に、クライアント開発者の簡素化を実現します。

インバウンド

インスタンスにアクセスする外部クライアント用のエンドポイントを作成し ます。これにより、OAuth クライアントアプリケーションレコードが作成され、クライアントがインスタンスの制限付きリソースにアクセスするために必要なクライアント ID とクライアントシークレットが生成されます。詳細については、「OAuth 受信」を参照してください。

トークンベースの認証

API キーまたは HMAC を使用する受信 REST API 構成のトークンベース認証。

ユーザー認証用の REST API エンドポイント ServiceNow® の API トークンをサポートします。

受信 REST API 構成のトークンベースの認証は、ServiceNow® API キーまたは HMAC トークンを使用してインスタンスで実行できます。

受信 **REST API** の **API** キーと **HMAC** 認証

ユーザー名とパスワードが Webhook URL に表示されないように ServiceNow®、REST API エンドポイントの API トークンをサポートします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

API キーベースの認証を有効にして、受信 Webhook URL を安全に認証します。

API キーと HMAC 認証を使用するには、インスタンスに ServiceNow® (Plugin: com.glide.tokenbased_auth) をインストールする必要があります。

> ⚠ 警告:
> サーバーに機密情報を送信する場合は、 **POST** 要求を使用します。

API キーと HMAC 認証のインストールには、次のプラグインの依存関係があります。

- REST API Auth Scope プラグイン (com.glide.rest.auth.scope)
- REST API Access Policy プラグイン (com.glide.rest.policy)
- 認証スコープ (com.glide.auth.scope)

メリット

受信 REST API の API キーと HMAC 認証により、次のことが可能になります。

- REST API 認証用の API キーまたは HMAC トークンを指定する機能。
- ユーザーアカウントを API キーまたは HMAC トークンに関連付ける機能。
- REST API コール内でトークンをクエリーパラメーターまたはヘッダーとして指定する機能。
- 認証スコープを API キーまたは HMAC トークン構成に関連付けて、API キーを使用して特定のスコープに関連付けられた API を呼び出す機能。
- API キーまたは HMAC トークン構成を、API アクセスポリシーで使用できる認証プロファイルに関連付ける機能。

API キーと HMAC 認証のアクティブ化

インスタンスでServiceNow® プラグイン API キーと HMAC 認証 (com.glide.tokenbased_auth) を有効にすることができます。

始める前に

必要なロール：admin

手順

1. 移動先 すべて > システムアプリケーション > 利用可能なすべてのアプリケーション > すべて.
2. フィルター基準と検索バーを使用して、 API キーと HMAC 認証 プラグイン (com.glide.tokenbased_auth) を検索します。

   名前または ID でプラグインを検索できます。プラグインが見つからない場合は、ServiceNow 担当者から要求する必要があります。
3. [インストール] を選択して、[プラグインをアクティブにする] ダイアログボックスで、[アクティブ化] をクリックします。

   > ℹ 注:
   > ドメイン分離と代理管理者がインスタンスで有効になっている場合、管理ユーザーはグローバルドメインに含まれている必要があります。それ以外の場合、次のエラーが表示されます： 別の操作が実行されているため、アプリケーションのインストールは利用できません：<プラグイン名> のプラグインの有効化。

API キーの構成 - トークンベースの認証

REST API エンドポイントの認証をサポートするように API キーを設定します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

始める前に
必要なロール：admin

必要なプラグイン:API キーと HMAC 認証 (com.glide.tokenbased_auth)

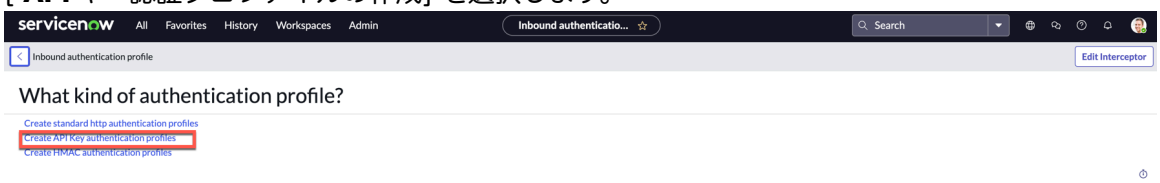
手順

1. 受信認証プロファイルを作成します。

a. 移動先 すべて > システム **Web** サービス > **API** アクセスポリシー > 受信認証プロファイル.

b. [新規] を選択します。
「認証プロファイルの種類は？」というメッセージが表示されます。

c. [**API** キー認証プロファイルの作成] を選択します。



d. フォームのフィールドに入力します。

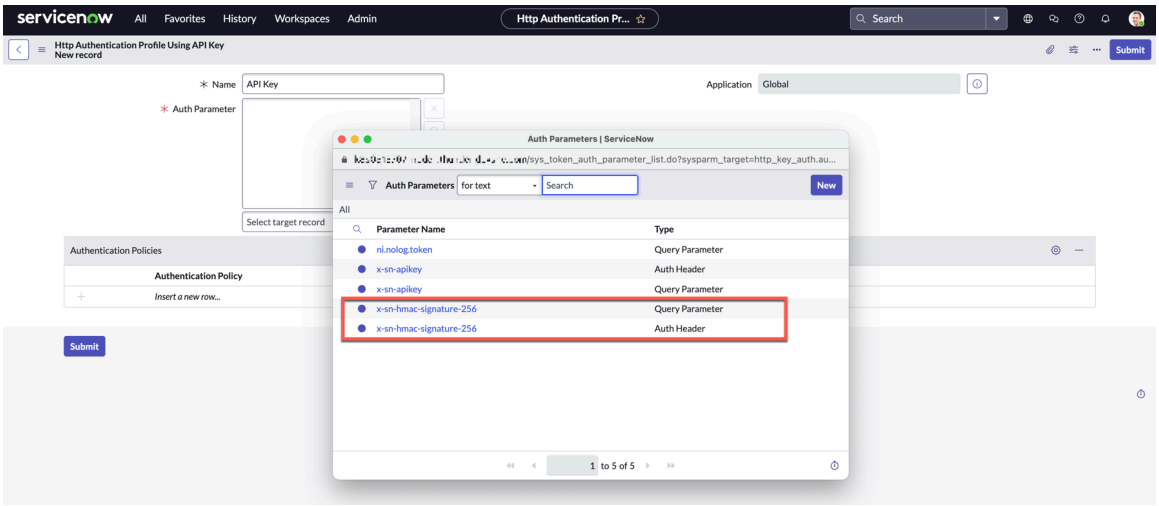
API キー認証プロファイル

フィールド	説明
名前	認証ポリシーを識別する名前
アプリケーション	認証ポリシーの範囲
認証パラメーター	認証要求の認証パラメーターを選択します。デフォルトのオプションを選択するか、新しい認証パラメーターを作成できます。 ▪ x-sn-apikey:認証ヘッダー ▪ X-SN-APIKEY:クエリパラメーターヘッダー

注:
選択したオプションは、認証ヘッダーまたはクエリパラメーターの一部として REST 呼び出しで定義する必要があります。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



e. フォームを送信します。

2. REST API キーを作成します。

a. 移動先 すべて > システム **Web** サービス > **API** アクセスポリシー > **REST API** キー.

b. [新規] を選択します。

c. フォームの各フィールドに入力します。

API キー

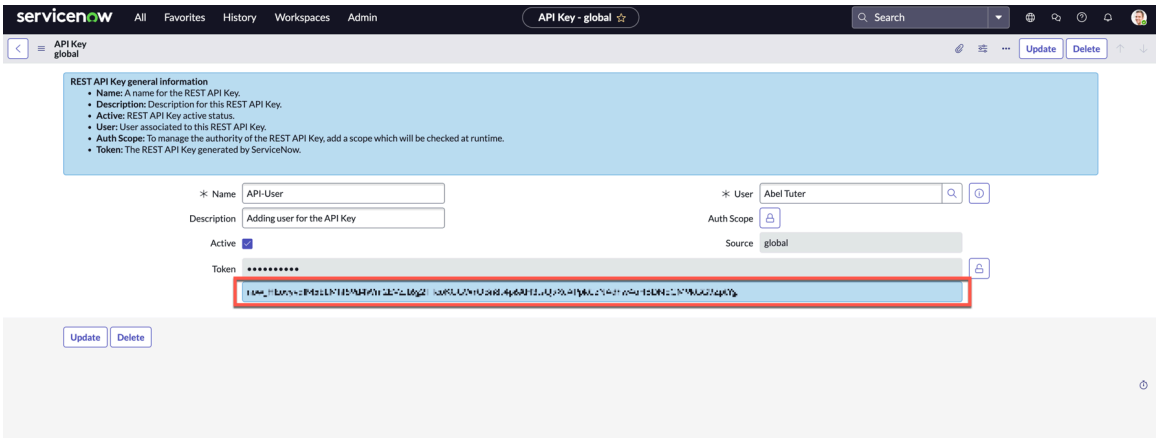
フィールド	説明
名前	REST API キーを識別するための名前
説明	REST API キーの説明。
アクティブ	REST API キーのステータス。
ユーザー	REST API キーに関連付けられたユーザー。検索アイコンを使用してユーザーを選択します。
認証スコープ	REST API キーの権限を管理する認証スコープを追加するオプション。
トークン	によって生成された Now PlatformREST API キー。ヘッダーまたはクエリパラメーター内で REST API コールの一部として使用するキーをコピーします。

d. フォームを送信します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

e. 作成されたレコードを開いて、ユーザーに対して生成された Now Platform トークンを表示します。



3. REST API アクセスポリシーを作成します。

a. 移動先 すべて > システム **Web** サービス > **REST API** アクセスポリシー.

b. [新規] を選択します。

c. フォームのフィールドに入力します。

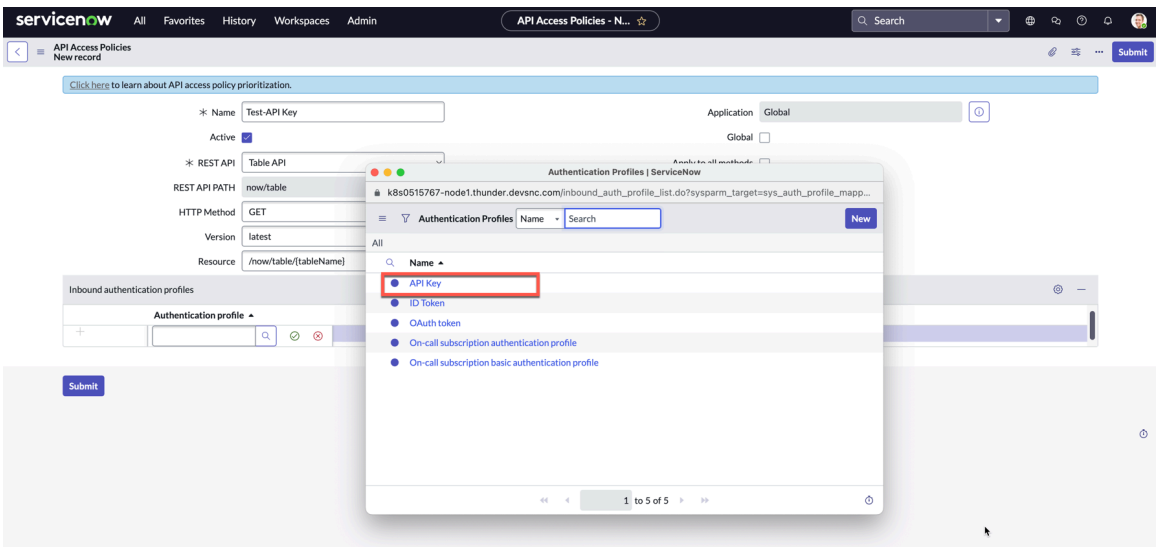
API アクセスポリシー

フィールド	説明
名前	API アクセスポリシーの一意の名前。
有効	API アクセスポリシーをアクティブにするオプション
REST API	アクセスポリシーが適用される REST API。例：添付ファイル **API**
REST API パス	REST API の API パス。このフィールドは、選択した REST API に基づいて自動入力されます。たとえば、**now/attachment** です。
HTTP メソッド	API とのやり取りに使用されるメソッド。このフィールドは、選択した REST API に基づいて自動入力されます。
バージョン	API のバージョン。- 例：**v1**。このフィールドは、選択した REST API に基づいて自動入力されます。 注: REST API のすべてのバージョンに対して認証ポリシーを作成する場合は、バージョンごとに個別のポリシーを作成する必要があります。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
リソース	REST API の子リソース。このフィールドは、選択した REST API に基づいて自動入力されます。例：**/now/attachment**
アプリケーション	アプリケーションのスコープ。
グローバル	このフィールドを有効にすると、API のすべてのメソッド、バージョン、およびリソースに認証ポリシーが適用されます。 **注:** グローバル REST API ポリシーではトークンベースの認証は許可されていません。
すべてのメソッドに適用	このフィールドを有効にすると、API のすべてのメソッド、バージョン、およびリソースに API の認証ポリシーが適用されます。
すべてのリソースに適用	このフィールドを有効にすると、API の認証ポリシーがすべてのバージョンに適用されます。
すべてのバージョンに適用	このフィールドを有効にすると、API の認証ポリシーがすべてのリソースに適用されます。



d. 作成された API 認証プロファイルを追加します。

e. フォームを送信します。

認証の構成に基づいて、ヘッダーパラメーターまたはクエリパラメーター内で API キーの作成時に生成された Now Platform x-sn-apikey (トークン) を使用して REST API 呼び出しを送信できます。

警告:
サーバーに機密情報を送信する場合は、 **POST** 要求を使用します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

HMAC の構成 - トークンベースの認証

REST API エンドポイントの認証をサポートするように HMAC を構成します。

始める前に
必要なロール：admin

必要なプラグイン:API キーと HMAC 認証 (com.glide.tokenbased_auth)

手順

1. HMAC 構成を作成します。

   a. 移動先 すべて > システム **Web** サービス > **API** アクセスポリシー > **HMAC** 構成.

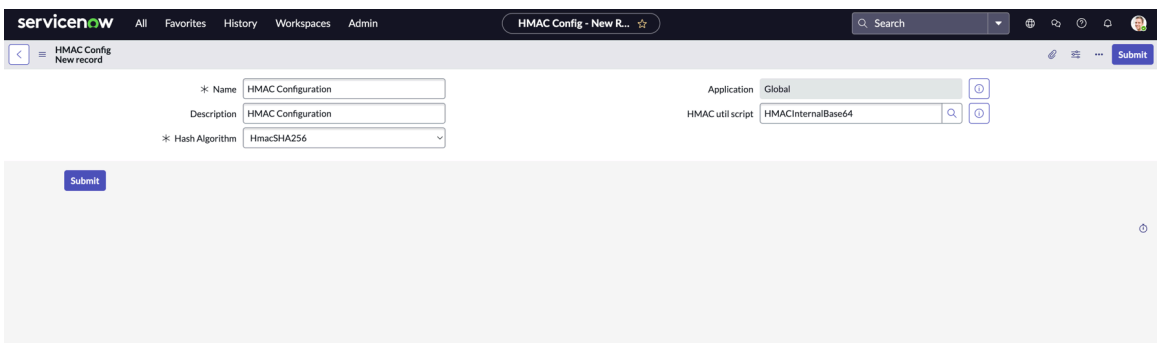
   b. [新規] を選択します。

   > **注:**
   > プラグインのインストール時に作成される デフォルトの **HMAC SHA256 Base64** エンコーディング を使用することもできます。

   c. フォームの各フィールドに入力します。

   HMAC 構成

フィールド	説明
名前	HMAC 構成の名前。
アプリケーション	構成のスコープ。
説明	構成に関する詳細な説明。
ハッシュアルゴリズム	ハッシュ アルゴリズムを選択します。利用可能なオプション: ▪ HmacSHA256 ▪ HmacSHA384 ▪ HmacSHA512
HMAC ユーティリティスクリプト	HMAC のユーティリティスクリプト。



   d. レコードを送信します。

2. 受信認証プロファイルを作成します。

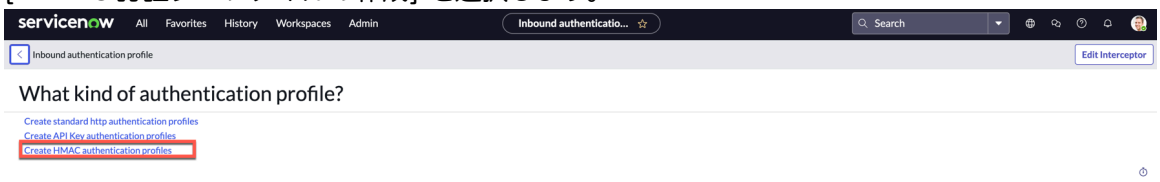
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

a. 移動先 すべて > システム **Web** サービス > **API** アクセスポリシー > 受信認証プロファイル.

b. [新規] を選択します。
「認証プロファイルの種類は？」というメッセージが表示されます。

c. [**HMAC** 認証プロファイルの作成] を選択します。



d. フォームのフィールドに入力します。

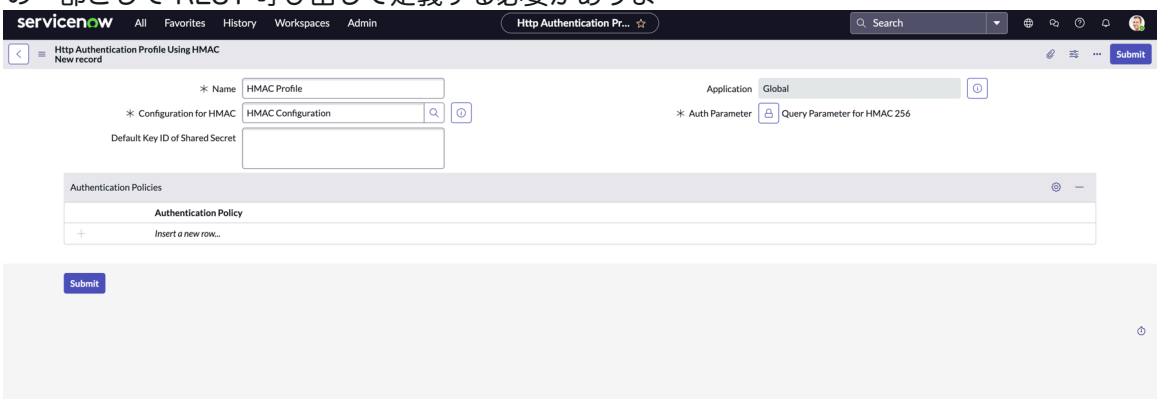
HMAC 認証プロファイル

フィールド	説明
名前	認証ポリシーを識別する名前
アプリケーション	認証ポリシーの範囲
HMAC の構成	作成された HMAC 構成を選択します。
認証パラメーター	認証要求の認証パラメーターを選択します。デフォルトのオプションを選択するか、新しい認証パラメーターを作成できます。 ▪ x-sn-hmac-signature-256:認証ヘッダー ▪ x-sn-hmac-signature-256:クエリパラメーターヘッダー
共有シークレットのデフォルトキー ID	HMAC を使用するためにこのフィールドで更新できるトークン情報。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注:
選択したオプションは、認証ヘッダーまたはクエリパラメーターの一部として REST 呼び出しで定義する必要があります。



e. フォームを送信します。

3. HMAC シークレットを作成します。

a. 移動先 すべて > システム **Web** サービス > **API** アクセスポリシー > **REST API HMAC** シークレット.

b. [新規] を選択します。

c. フォームの各フィールドに入力します。

REST API HMAC シークレット

フィールド	説明
名前	REST API HMAC シークレットを識別するための名前。
説明	REST API HMAC シークレットの説明。
アクティブ	REST API HMAC シークレットのステータス。
ユーザー	REST API HMAC シークレットに関連付けられているユーザー。検索アイコンを使用してユーザーを選択します。
キー ID	REST 呼び出しの一部として送信する必要があるキー ID。キー ID はフォームの送信後に生成されます。
共有シークレット	ユーザーの共有シークレット。たとえば、パスワードです。
ソース	レコードのソース。

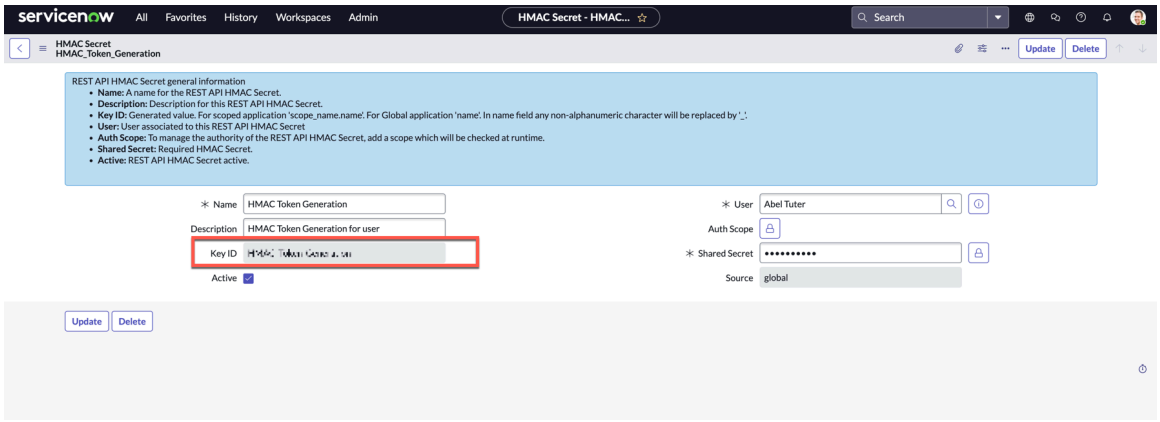
d. フォームを送信します。

e. 作成されたレコードを開きます。

ユーザーに対して生成された Now Platform キー ID を検索します

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



。

> **注:**
> API 呼び出しの認証パラメーターまたはクエリパラメーターを指定しない場合は、HMAC 用に作成された認証プロファイルのキー ID 中に生成されたキー ID を追加できます。

4. REST API アクセスポリシーを作成します。

a. 移動先 すべて > システム **Web** サービス > **REST API** アクセスポリシー.

b. [新規] を選択します。

c. フォームのフィールドに入力します。

API アクセスポリシー

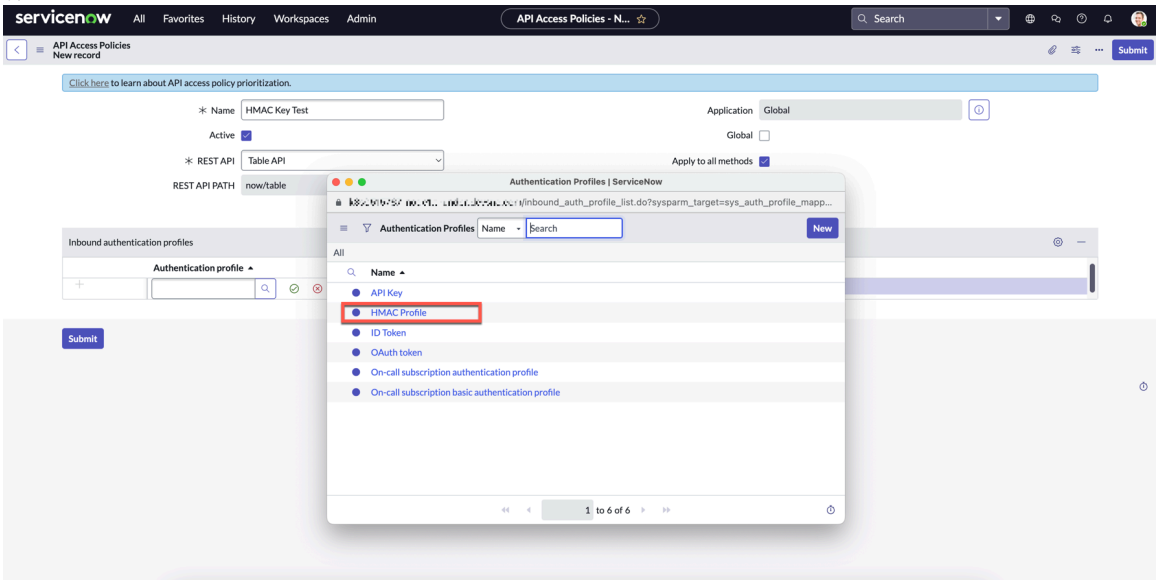
フィールド	説明
名前	API アクセスポリシーの一意の名前。
有効	API アクセスポリシーをアクティブにするオプション
REST API	アクセスポリシーが適用される REST API。例：添付ファイル **API**
REST API パス	REST API の API パス。このフィールドは、選択した REST API に基づいて自動入力されます。たとえば、**now/attachment** です。
HTTP メソッド	API とのやり取りに使用されるメソッド。このフィールドは、選択した REST API に基づいて自動入力されます。
バージョン	API のバージョン。- 例：**v1**。このフィールドは、選択した REST API に基づいて自動入力されます。 **注:** REST API のすべてのバージョンに対して認証ポリシーを作成する場合は、バージョンごとに個別のポリシーを作成する必要があります。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
リソース	REST API の子リソース。このフィールドは、選択した REST API に基づいて自動入力されます。例：**/now/attachment**
アプリケーション	アプリケーションのスコープ。
グローバル	このフィールドを有効にすると、API のすべてのメソッド、バージョン、およびリソースに認証ポリシーが適用されます。 **注:** グローバル REST API ポリシーではトークンベースの認証は許可されていません。
すべてのメソッドに適用	このフィールドを有効にすると、API のすべてのメソッド、バージョン、およびリソースに API の認証ポリシーが適用されます。
すべてのリソースに適用	このフィールドを有効にすると、API の認証ポリシーがすべてのバージョンに適用されます。
すべてのバージョンに適用	このフィールドを有効にすると、API の認証ポリシーがすべてのリソースに適用されます。

d. 作成された API 認証プロファイルを追加します。



e. フォームを送信します。
次の方法で REST API 呼び出しを送信できます。

- 認証用の構成に基づいてヘッダーまたはクエリパラメーター内の API キー作成中に生成された x-sn-hmac-signature-256 ServiceNow を使用します。
- 共有シークレットが要求の一部として指定された事前要求スクリプトあり。

警告:
サーバーに機密情報を送信する場合は、 **POST** 要求を使用します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

API アクセスポリシー

API アクセスポリシーは、API へのアクセス権限と期間を定義します。

API アクセスポリシーを使用すると、認証タイプとアクセスポリシーの指定されたフィルター基準に基づいて、受信 ServiceNow API へのアクセスを制限できます。

次に、非インタラクティブセッションでの 3 つのレベルの認証ポリシーのサポートを示します。

- **REST API**：管理者は、グローバル API 認証ポリシーまたは API 固有の認証ポリシーを定義できます。
- **SOAP API**：管理者は、グローバル API 認証ポリシーまたは API 固有の認証ポリシーを定義できます。
- システム/エクスポートプロセッサー：管理者は、プロセッサー API 認証ポリシーまたはプロセッサー固有の認証ポリシーに認証プロファイルを適用するために使用できる、すぐに利用可能な 5 つの認証プロファイルを定義できます。

注:
グローバル認証ポリシーを追加すると、そのポリシーはすべての REST APIs、SOAP API、またはシステム/エクスポートプロセッサーに適用されます。

API ポリシーと認証スコープに固有の次のプラグインが自動的にインストールされます。

- com.glide.rest.policy
- com.glide.soap.policy
- com.glide.processor.policy
- com.glide.rest.auth.scope

デフォルトのグローバルブロックポリシーを設定するか、セキュリティ要件に従ってカスタム API アクセスポリシーを作成できます。

さらに、認証ポリシーのポリシー入力として使用されるフィルター条件またはクエリが含まれているフィルター基準も適用します。

ServiceNow® では次の API アクセスポリシーがサポートされています。

- REST API アクセスポリシー
- SOAP API アクセスポリシー

エクスポートプロセッサーに関連するポリシーの詳細については、「システム/エクスポートプロセッサーのアクセスポリシー」を参照してください。

REST API アクセスポリシー

REST API アクセスポリシーを使用すると、認証タイプとアクセスポリシーの指定されたフィルター基準に基づいて、受信 REST API へのアクセスを制限できます。

REST API は RESTful API ともいい、REST アーキテクチャスタイルのガイドラインに準拠したアプリケーションプログラミングインターフェイス (API) の一種です。REST API は柔軟性が高く、Web 全体で広く使用されています。

フィルター基準には、認証ポリシーのポリシー入力として使用されるフィルター条件またはクエリーが含まれています。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

デフォルトのグローバルブロックポリシーを設定するか、セキュリティ要件に従ってカスタム API アクセスポリシーを作成できます。たとえば、指定された IP アドレス範囲から OAuth 2.0 認証タイプのみを許可するカスタム API アクセスポリシーを作成できます。他の認証タイプの認証要求、および指定された IP アドレス以外の IP アドレスからのアクセス要求は拒否されます。

REST API アクセスポリシーのアクティブ化

admin ロールがあれば、REST API Access Policy プラグイン (com.glide.rest.policy) をアクティブ化できます。このアプリケーションにはデモデータが含まれています。まだインストールされていない場合は、関連する ServiceNow Store アプリケーションとプラグインをインストールします。

始める前に
必要なロール：admin

このタスクについて
REST API アクセスポリシーとともにインストールされるアイテム：

- プラグイン：
  com.gilde.auth.profile、com.snc.adaptive_authentication、com.snc.platform.security.oauth
- テーブル：
  sys_api_access_policy、sys_auth_profile_mapping、auth_policy_mapping、inbound_auth_profile、std_http

詳細については、「適応認証」を参照してください。

手順

1. 移動先 すべて > システムアプリケーション > 利用可能なすべてのアプリケーション > すべて.
2. フィルター基準と検索バーを使用して、REST API Access Policy プラグイン (com.glide.rest.policy) を検索します。

   名前または ID でプラグインを検索できます。プラグインが見つからない場合は、ServiceNow 担当者から要求する必要があります。
3. [インストール] を選択して、[プラグインをアクティブにする] ダイアログボックスで、[アクティブ化] をクリックします。

   注:
   ドメイン分離と代理管理者がインスタンスで有効になっている場合、管理ユーザーはグローバルドメインに含まれている必要があります。それ以外の場合、次のエラーが表示されます： 別の操作が実行されているため、アプリケーションのインストールは利用できません：<プラグイン名> のプラグインの有効化。

認証プロファイルの作成

認証プロファイルを作成し、1 つ以上の認証ポリシーをプロファイルに追加します。デフォルトで利用可能な **ID** トークンおよび **OAuth** トークンの認証プロファイルを設定することもできます。

始める前に
必要なロール：admin

注:
相互認証とカスタマイズされた認証を使用して、認証ポリシー、IP 範囲、ロールベース、ユーザーベースなどを適用できます。

手順

1. 移動先 すべて > システム **Web** サービス > **API** アクセスポリシー > 受信認証プロファイル.
2. [新規] をクリックします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

「認証プロファイルの種類は？」というメッセージが表示されます。

3. [標準の **http** 認証プロファイルを作成] を選択します。
4. フォームのフィールドに入力します。

[標準の認証プロファイル] フォーム

フィールド	説明
名前	認証ポリシーを識別する名前
説明	認証ポリシーの説明
有効	認証ポリシーをアクティブにするオプション
アプリケーション	認証ポリシーの範囲
タイプ	利用可能な認証のタイプ。[基本認証]、**[ID** トークン]、[証明書ベースの認証]、**[OAuth]** を選択できます。
OAuth エンティティ	OAuth エンティティプロファイル。このフィールドは、[タイプ] で **[ID** トークン] または **[OAuth]** を選択した場合のみ表示されます。

5. [新規行を挿入] をダブルクリックします。
6. リストから認証ポリシーを選択し、保存アイコン ( ) をクリックします。

注:
[アクセスポリシーを許可] または [アクセスポリシーを拒否] は選択しないでください。これらのポリシーは、ユーザーログインのみを対象としています。

1 つ以上の複数の認証ポリシーを認証プロファイルに追加できます。

REST API アクセスポリシーの作成

API アクセスポリシーを作成し、認証プロファイルをマップして REST API の認証タイプを制限します。たとえば、REST API の ID トークン認証のみを許可する API アクセスポリシーを作成できます。

始める前に

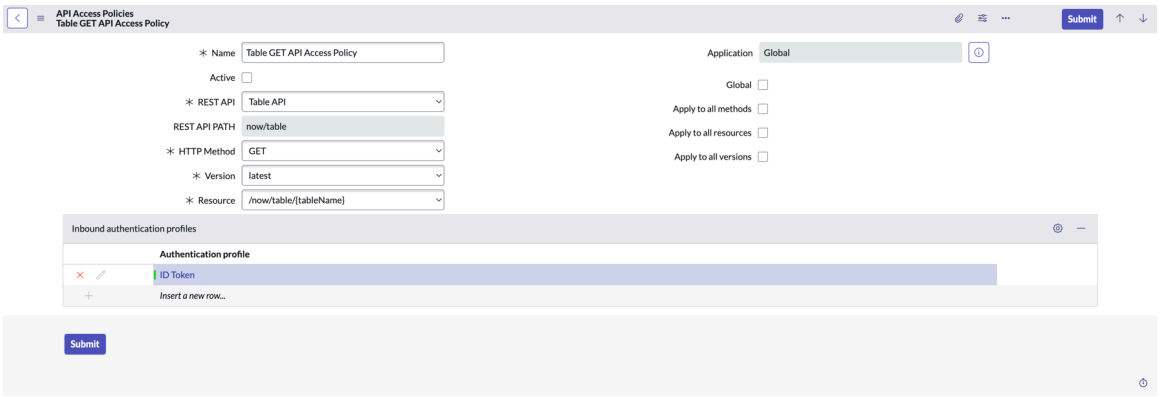
- 必要なロール：admin
- 認証プロファイルが作成されていることを確認します。詳細については、「認証プロファイルの作成」を参照してください。

手順

1. 移動先 すべて > システム **Web** サービス > **REST API** アクセスポリシー.
2. [新規] をクリックします。
3. フォームのフィールドに入力します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



API アクセスポリシー

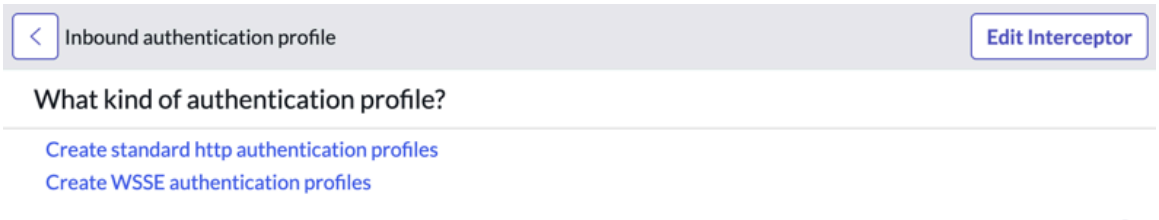
フィールド	説明
名前	API アクセスポリシーの一意の名前。
有効	API アクセスポリシーをアクティブにするオプション
REST API	アクセスポリシーが適用される REST API。例：添付ファイル **API**
REST API パス	REST API の API パス。このフィールドは、選択した REST API に基づいて自動入力されます。たとえば、**now/attachment** です。
HTTP メソッド	API とのやり取りに使用されるメソッド。このフィールドは、選択した REST API に基づいて自動入力されます。
バージョン	API のバージョン。- 例：**v1**。このフィールドは、選択した REST API に基づいて自動入力されます。 **注:** REST API のすべてのバージョンに対して認証ポリシーを作成する場合は、バージョンごとに個別のポリシーを作成する必要があります。
リソース	REST API の子リソース。このフィールドは、選択した REST API に基づいて自動入力されます。例：**/now/attachment**
アプリケーション	アプリケーションのスコープ。
グローバル	API のすべてのメソッド、バージョン、およびリソースに認証ポリシーを適用可能にします。
すべてのメソッドに適用	API のすべてのメソッド、バージョン、およびリソースに API の認証ポリシーを適用可能にします。
すべてのリソースに適用	すべてのバージョンに API の認証ポリシーを適用可能にします。
すべてのバージョンに適用	すべてのリソースに API の認証ポリシーを適用可能にします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

> **注:**
> API アクセスポリシーの優先順位付けの詳細については、「API アクセスポリシーの優先順位付け」を参照してください。

4. [新規行を挿入] をダブルクリックします。
5. リストから受信認証プロファイルを選択し、保存アイコン ( ) をクリックします。
   たとえば、基本認証、**ID** トークン、証明書ベースの認証、**OAuth**、または **WSSE** 認証 を追加できます。
   a. 1 つ以上の受信認証プロファイルを追加するには、[新規] をクリックして新しいプロファイルを作成します。
   b. [認証プロファイルの種類は？] を選択します。
      - 標準の **http** 認証プロファイルを作成
      - **WSSE** 認証プロファイルを作成



   c. 認証プロファイルを作成したら、レコードを保存します。
6. [送信] をクリックして REST API アクセスポリシーを送信します。

API アクセスポリシーの優先順位付け

ServiceNow® インスタンスに複数の API アクセスポリシーが設定されている場合のポリシーの優先順位付けのロジックについて説明します。

API アクセスポリシーは、ServiceNow® インスタンスに設定された REST API ポリシーのタイプに基づいて優先順位が付けられます。

このアプローチでは、メソッド、リソース、バージョンなどの API の各部分に異なる重み付けを定義します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

API ポリシーでは、最初に非グローバル、次にグローバルが優先されます。つまり、非グローバルアクセスポリシーは常にグローバル API アクセスポリシーを上書きします。

優先順位付けのロジックは次のとおりです。

優先順位付け

フィールド	優先度	優先順位付けのロジック
メソッド、リソース、およびバージョン	1	3 つのフィールドがポリシーと一致する場合、そのポリシーが 1 番目の優先順位になります。
メソッド + リソース	2	2 つのフィールドがポリシーと一致する場合、そのポリシーが 1 番目の優先順位になります。
リソース + バージョン	3	2 つのフィールドおよび [すべてのメソッドに適用] フィールドがポリシーと一致する場合、そのポリシーが 3 番目の優先順位になります。
リソース	4	フィールドおよび [すべてのメソッドに適用] フィールドがポリシーと一致する場合、そのポリシーが 4 番目の優先順位になります。
メソッド + バージョン	5	2 つのフィールドおよび [すべてのリソースに適用] フィールドがポリシーと一致する場合、そのポリシーが 5 番目の優先順位になります。
メソッド	6	フィールドおよび [すべてのリソースに適用] フィールドがポリシーと一致する場合、そのポリシーが 5 番目の優先順位になります。
バージョン	7	フィールドおよび [すべてのメソッドに適用] フィールドおよび [すべてのバージョンに適用] フィールドがポリシーと一致する場合、そのポリシーが 7 番目の優先順位になります。
グローバルおよびすべてのメソッドに適用	8	[グローバル] フィールドが [true] で、[すべてのメソッドに適用] が [false] の場合、そのポリシーは 8 番目の優先順位になります。
グローバルおよびすべてのメソッドに適用	9	[グローバル] フィールドが [true] で、[すべてのメソッドに適用] が [true] の場合、そのポリシーは 9 番目の優先順位になります。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

API のフィルター基準

フィルター基準には、認証ポリシーのポリシー入力として使用されるフィルター条件またはクエリーが含まれています。ポリシー入力は 1 つ以上のフィルター基準をグループ化し、認証ポリシーのポリシー条件を定義するために使用されます。たとえば、IP フィルター基準は、クラスレスドメイン間ルーティング (CIDR) 形式の IP アドレスまたは IP アドレス範囲を定義します。

ユーザーの IP アドレス、ロール、およびユーザーが属するユーザーグループに基づいて、フィルター基準を作成できます。

注:
適応認証モジュールから作成されたフィルター基準も使用します。詳細については、「適応認証」を参照してください。

適応認証のフィルター基準と同じプロセスを使用して、API のフィルター基準を作成できます。詳細については、「フィルター基準」を参照してください。

関連情報

- IP フィルター基準の作成
- ロールフィルター基準の作成
- グループフィルター基準の作成

API 認証ポリシー

認証ポリシーは、指定されたポリシー条件に基づいて認証要求を評価し、一致する基準に応じてアクセスを許可または拒否します。

組み込みのグローバルブロックポリシーを使用するか、セキュリティ要件に従って認証ポリシーを作成できます。グローバルブロックポリシーは、指定されたフィルター基準に基づいてユーザーと API の認証要求を拒否します。

注:
[アクセスポリシーを許可] および [アクセスポリシーの拒否] を使用または変更しないでください。これらのポリシーは、ユーザーログインのみを対象としています。

API 認証ポリシーの作成

認証ポリシーを使用すると、指定されたフィルター基準に基づいて API のアクセス制限を適用できます。

始める前に
必要なロール：管理者

手順

1. 移動先 すべて > システム **Web** サービス > **API** 認証ポリシー.
2. [新規] をクリックします。
3. フォーム上で、以下のフィールドに記入します。

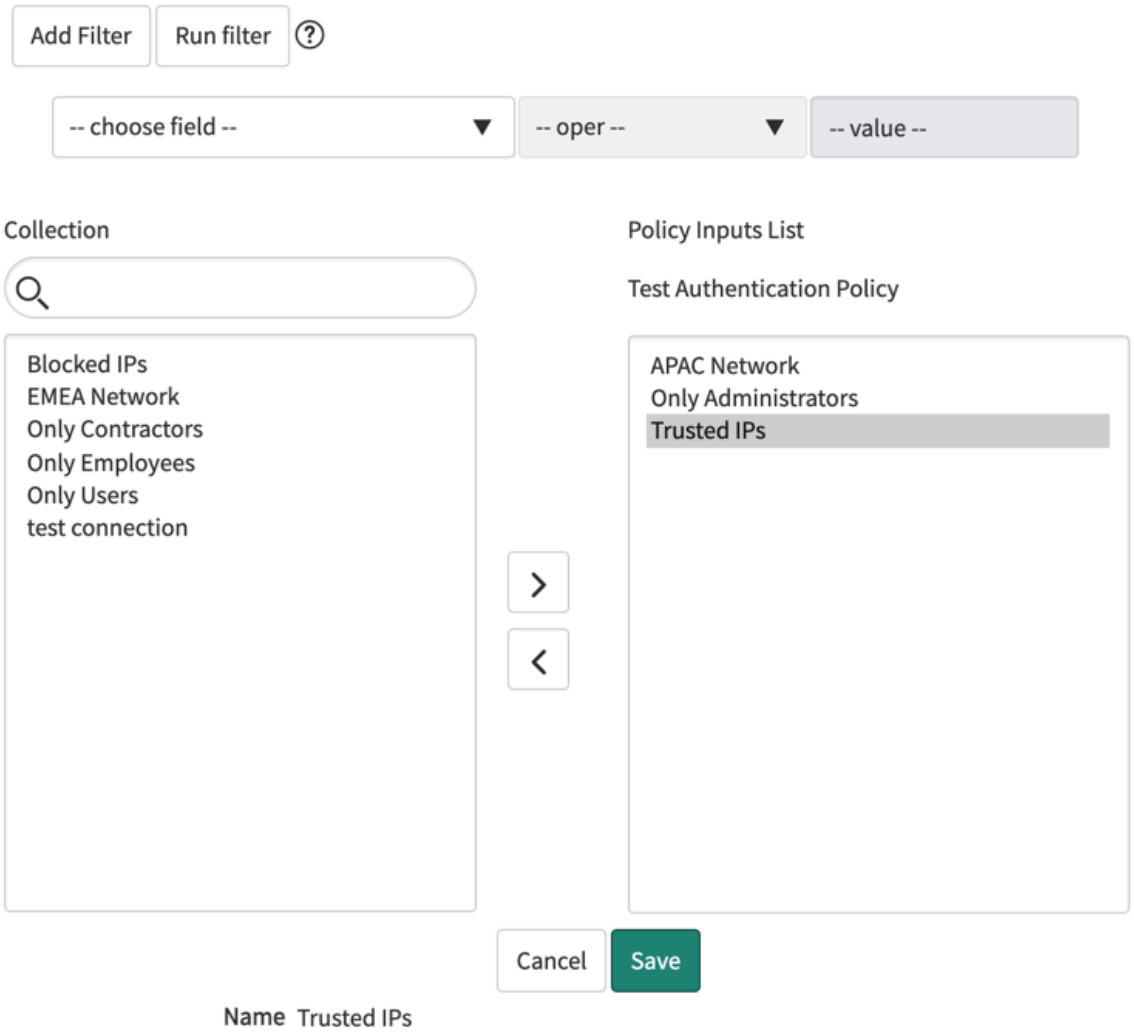
ポリシーフォーム

フィールド	説明
名前	ポリシーを識別する名前。
説明	ポリシーの簡単な説明。
アプリケーション	アプリケーションのスコープ

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

4. フォームヘッダーを右クリックし、[保存] を選択します。
5. [ポリシーの入力] タブで、[編集] を選択して既存のフィルター基準を追加します。
   新しいポリシー入力を作成することもできます。詳細については、「ポリシー入力の作成」を参照してください。
6. 1 つ以上のフィルター基準を、[コレクション] リストから [ポリシー入力リスト] に移動しま



す。

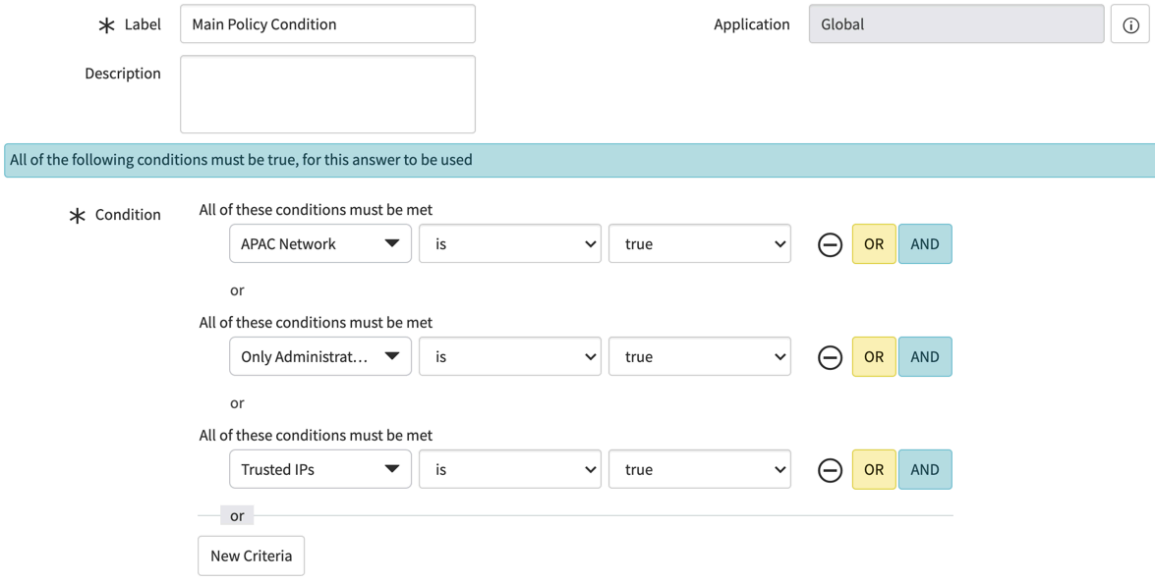
7. [保存] を選択します。
8. [ポリシー条件] タブで、[新規] をクリックします。
9. フォーム上で、以下のフィールドに記入します。

[条件] フォーム

フィールド	説明
ラベル	ポリシー条件の名前
説明	ポリシー条件の簡単な説明
アプリケーション	アプリケーションのスコープ
条件	**OR** フィルターと組み合わされた 1 つ以上の条件。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



10. [送信] を選択します。

API のグローバルブロックポリシーの設定

グローバルブロックポリシーは、指定されたフィルター条件に基づいてユーザーと API の認証要求を拒否します。このポリシーは、IP アドレスアクセス制御の代わりに使用できます。

始める前に
必要なロール：管理者

手順

1. 移動先 すべて > システム **Web** サービス > **API** アクセスポリシー > グローバルブロックポリシー.
2. [ポリシーの入力] タブで、[編集] をクリックします。
3. [コレクション] リストから 1 つ以上のフィルター基準を選択し、[グローバルブロックポリシー] リストに移動します。
   他のフィルターを追加することもできます。
4. [ポリシー条件] タブで、[新規] をクリックします。
5. フォームの各フィールドに入力します。

[条件] フォーム

フィールド	説明
ラベル	条件を識別する名前
説明	条件の説明
条件	認証要求を評価するために使用される複数のポリシー入力 (フィルター基準) の論理的な組み合わせ。たとえば、信頼できる IP アドレスのリストから請負会社のみを許可するような条件を作成できます。

REST API 認証スコープ

REST API の認証スコープのサポート。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

Washington DC より前のリリースでは、すべてのアクセストークンまたは OIDC トークンが、ユーザーの REST API へのフルアクセス権を持つ useraccount スコープにリンクされています。Washington DC リリース以降では、特定の REST API のみへのアクセスを提供するため、OAuth トークンのスコープが導入されています。

OAuth エンティティが認証スコープにリンクされている場合、その OAuth エンティティによって発行または管理されるトークンは、REST API へのアクセスにしか使用できません (1 つの OAuth エンティティを複数の認証スコープにリンクすることは可能です)。新しい OAuth エンティティでは、デフォルトの認証スコープは空です。認証スコープを OAuth エンティティに手動でリンクする必要があります。

注:

- REST API 認証スコープが有効になって REST API の認証スコープに追加された後は、管理者がこの認証スコープを対応する OAuth エンティティに追加しない限り、既存のすべての OAuth トークンがこの API にアクセスできなくなります。
- 認証スコープを REST API にリンクした後に oauth_entity に適切な認証スコープがあることを確認する責任は、管理者が負います。
- ServiceNow によって発行された OAuth アクセストークンは認証スコープをサポートします。
- ServiceNow によって発行されていない OIDC トークンは ServiceNow によって検証されます。
- ID トークンが必要な場合は、OIDC トークンに IDP からのスコープがあります。ここでは、認証スコープはサードパーティ (IdP) 用ではなく ServiceNow 用です。

REST API スコープの設定

REST API スコープを設定するには、次のタスクを実行します。

- 認証スコープを作成する
- 認証スコープを REST API にリンクする
- 認証スコープを OAuth エンティティにリンクする
- OAuth フローを実行して OAuth アクセストークンを取得する
- OAuth アクセストークンを使用して API 呼び出しを行う

REST API 認証スコープのアクティブ化

REST API Auth Scope プラグイン (com.glide.rest.auth.scope) をアクティブ化して、OAuth エンティティを認証スコープにリンクすることができます。

始める前に
次のプラグインをインストールします。

- OAuth 2.0
- REST API Provider
- Authentication scope
- REST API Scope

注:
REST API Scope プラグインは Tokyo リリースの一部として追加されます。

必要なロール：admin

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. 移動先 すべて > システムアプリケーション > 利用可能なすべてのアプリケーション > すべて.
2. フィルター基準と検索バーを使用して、REST API auth Scope (*com.glide.rest.auth.scope*) プラグインを検索します。

   名前または ID でプラグインを検索できます。プラグインが見つからない場合は、ServiceNow 担当者から要求する必要があります。
3. [インストール] を選択して、[プラグインをアクティブにする] ダイアログボックスで、[アクティブ化] をクリックします。

   注:
   ドメイン分離と代理管理者がインスタンスで有効になっている場合、管理ユーザーはグローバルドメインに含まれている必要があります。それ以外の場合、次のエラーが表示されます： 別の操作が実行されているため、アプリケーションのインストールは利用できません：<プラグイン名> のプラグインの有効化。

REST API Auth Scope のプロパティとテーブル

REST API Auth Scope プラグイン (com.glide.rest.auth.scope) には、次のシステムプロパティ、テーブル、およびスクリプトが含まれています。

REST API Auth Scope のプロパティ

REST API Auth Scope では、次のシステムプロパティが追加されています。

プロパティ

名前	説明
com.glide.rest.api.auth.scope.check.enable	このプロパティは、プラットフォームレベルの認証スコープのチェックをオフにするために使用します。 false に設定すると、実行時に REST API にリンクされているかどうかにかかわらず、認証スコープのチェックがスキップされます。 デフォルトでは、このプロパティは [true] に設定されます。このプロパティは、以前のリリースの動作に戻す場合に使用します。
com.glide.oauth.token.scope.useraccount	このプロパティは、エンドユーザーが *useraccount* 認証スコープを削除して手動で追加するときにのみ使用します。 その場合は、*useraccount* のシステム ID が変更されます。このプロパティを新しい sys_id に更新する必要があります。 実行時は、認証スコープ名の代わりに認証スコープのシステム ID が使用されます。

REST API 認証スコープのテーブル

REST API 認証スコープには次のテーブルがあります。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

テーブル

名前	説明
認証スコープ (sys_auth_scope)	このテーブルでは、REST API および OAuth エンティティとリンクできる認証スコープを定義します。 認証スコープ名は一意である必要があり、グローバルで使用します。
REST API 認証スコープ (sys_api_access_scope)	このテーブルでは、REST API を認証スコープにリンクします。

REST API 認証スコープの設定

OAuth エンティティを認証スコープにリンクすることで、認証スコープにリンクされている REST API にアクセスするためのトークンを管理します。

始める前に
次のプラグインをインストールします。

- OAuth 2.0
- REST API Provider
- Authentication scope
- REST API Auth Scope

注:
REST API Auth Scope プラグインは Tokyo リリースの一部として追加されます。

必要なロール：管理者

手順

1. 移動先 すべて > **API** 認証スコープ > **REST API** 認証スコープ.
   [REST API 認証スコープ] ページが表示されます。
2. 新しい REST API 認証スコープを設定するには、[新規] をクリックします。
3. フォームのフィールドに入力します。

REST API 認証スコープ

名前	REST API 認証スコープを識別する一意の名前。
有効	チェックボックスをオンにすると、設定がアクティブになります。
アプリケーション	読み込み専用のアプリケーションスコープ
REST API	認証スコープが適用される REST API。たとえば、テーブル API などです。
認証スコープ	検索アイコンから認証スコープを選択します。

自動翻訳

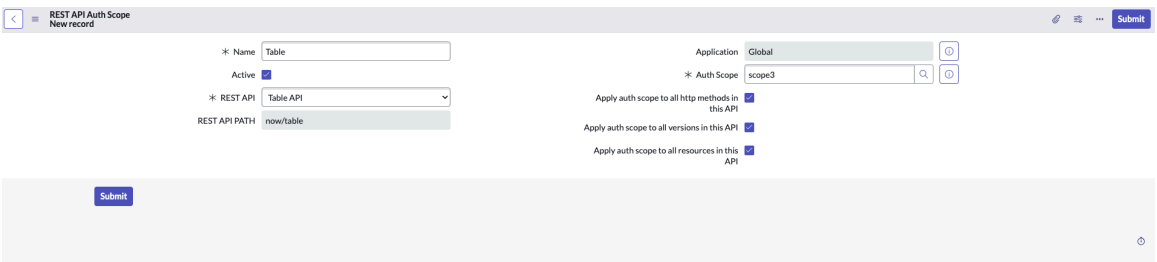
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

REST API パス	REST API の API パス。このフィールドは、選択した REST API に基づいて自動入力されます。例：now/table
HTTP メソッド	API とのやり取りに使用されるメソッド。ドロップダウンリストからメソッドを選択します。 フォームの [この **API** のすべての **HTTP** メソッドに認証スコープを適用] フィールドを手動で無効にすると、メソッドを選択できます。
REST API バージョン	API のバージョン。- 例：v1。このフィールドは、選択した REST API に基づいて自動入力されます。 フォームの [この **API** のすべてのバージョンに認証スコープを適用] フィールドを手動で無効にすると、バージョンを選択できます。
リソース	REST API の子リソース。このフィールドは、選択した REST API に基づいて自動入力されます。例：/now/table フォームの [この **API** のすべてのリソースに認証スコープを適用] フィールドを手動で無効にすると、リソースを選択できます。
この API のすべての HTTP メソッドに認証スコープを適用	これを有効にすると、API のすべての HTTP メソッドに認証スコープが適用されます。
この API のすべてのバージョンに認証スコープを適用	これを有効にすると、API のすべてのバージョンに認証スコープが適用されます。
この API のすべてのリソースに認証スコープを適用	これを有効にすると、API のすべてのリソースに認証スコープが適用されます。

4. [送信] をクリックします。
   選択された REST API と認証スコープに基づいて、API はスコープに固有の情報を取得します。

Example: テーブル **API** に対して **3** つの **REST API** 認証スコープを作成することを検討してください。

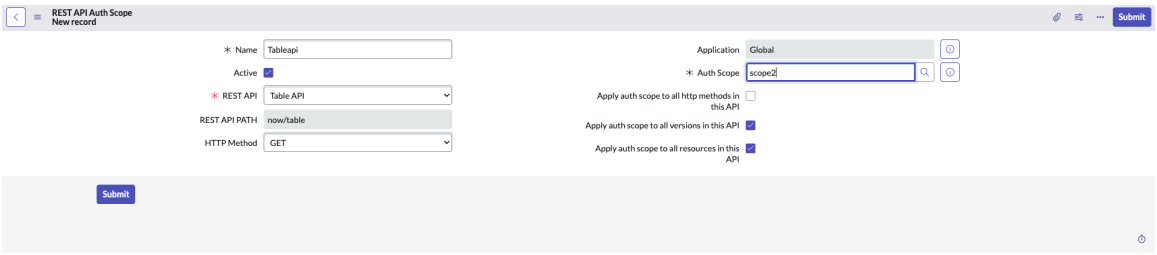
1 つ目の認証スコープは、すべての HTTP メソッド、バージョン、およびリソースが有効な状態で [テーブル **API]** にマッピングされます。



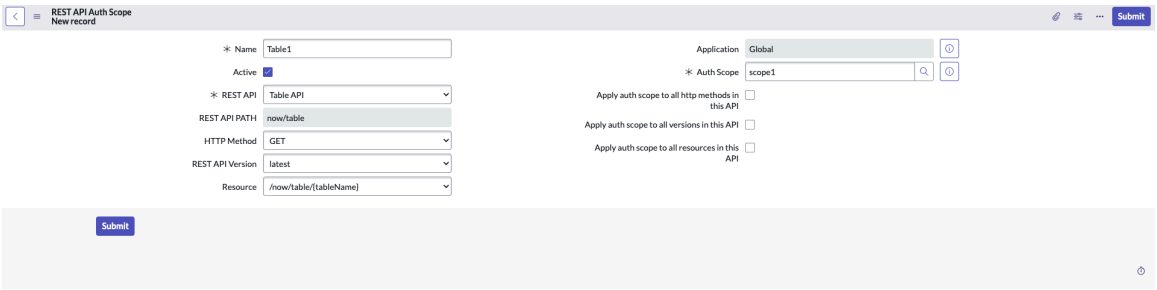
2 つ目の認証スコープは、すべてのバージョンとリソースが有効な状態で [テーブル **API]** にマッピングされます。ただし、HTTP メソッド (この例では **GET** メソッド) は選択してください。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳



3 つ目の認証スコープは、HTTP メソッド、バージョン、およびリソースが有効でない状態で [テーブル **API]** にマッピングされます。ただし、HTTP メソッド、バージョン、およびリソースは手動で選択してください。この例では、HTTP メソッドは **GET**、REST API のバージョンは最新、リソースは /now/table/{tableName} です。



これらの認証スコープがすべて作成されると、3 つのスコープすべてで **GET** メソッドを使用できますが、**POST**、**PUT**、**DELETE**、または **PATCH** メソッドでは **scope3** しか使用できません。

REST API スコープのトラブルシューティング

トラブルシューティングのアクションは、REST API スコープの設定や実行時の一般的な問題解決に役立ちます。

トラブルシューティング

問題	アクション
REST API が認証スコープにリンクされているのに、ベアラートークン認証を使用しても実行時に認証スコープのチェックが行われない。	• sys_api_access_policy レコードがアクティブであることを確認します。ランタイムでは非アクティブなレコードが無視されます。 • プロパティ *com.glide.rest.api.auth.scope.check.enable* が false に設定されているかどうかを確認します。 • OAuth トークンに useraccount 認証スコープがあるかどうかを確認します。
REST API が *auth_scope1*にリンクされているのに、*auth_scope2* があるアクセストークンでも REST API にアクセスできてしまう。	• このレコードがアクティブかどうかを確認します。 • この REST を確認して、API が同じでありながら異なるメソッド、バージョン、またはリソースを適用する他のレコードがあるかどうかを確認します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

トラブルシューティング (続く)

問題	アクション
REST API が認証スコープにリンクされているのに、*basicAuth* と *mutualAuth* に対して実行時に認証スコープのチェックが行われない。	REST API 認証スコープは OAuth アクセストークンまたは OIDC トークンにのみ適用されるため、これは予想どおりの動作です。BasicAuth、セッション Cookie、および証明書ベースの認証は適用されません。
OAuth アクセストークンを使用すると、REST API の呼び出しで 403 が返される。	「必要な API アクセススコープがありません (Missing required api access scope)」というエラーメッセージがあるかどうか確認してください。もしあれば、この REST API の認証スコープのチェックは失敗します。
事前定義した useraccount が削除されて復元できない。	useraccount を他のインスタンスから xml としてエクスポートしてインポートするか、useraccount を作成して、システムプロパティ *glide.oauth.token.scope.useraccount* を新しく作成された sys_id レコードに変更します。

よく寄せられる質問

REST API 認証スコープを使用する際によく寄せられる質問を以下に示します。

1 つの OAuth トークンを複数の認証スコープにリンクすることはできますか。

はい。1 つの oauth_entity を複数の認証スコープとリンクすることができます。この oauth_entity によって発行されるすべての OAuth トークンに同じ認証スコープが設定されます。

認証スコープが異なる別々の OAuth トークンで同じ REST API にアクセスできますか。

はい。異なる認証スコープで同じ REST API に対してアクセスできます。1 つの認証スコープが一致する限り、認証スコープから結果が返されます。

useraccount 認証スコープのある OAuth アクセストークンで任意の REST API にアクセスできますか。

はい。useraccount には認証スコープへのフルアクセス権があります。

OAuth アクセストークンの OAuth スコープは動的に変更できますか。

はい。oauth_credential テーブルでは認証スコープがアクセストークンでハードコードされていません。代わりに、実行時にリンクされた oauth_entity から認証スコープが取得されます。

OAuth トークンは更新後も同じ認証スコープを保持できますか。

はい。oauth_admin が oauth_entityにリンクされた認証スコープを変更しない限り、トークンの更新後も認証スコープは変更されません。

事前定義された useraccount 認証スコープのレコードが削除されました。useraccount という名前の新しい認証スコープを作成できますか。

同じ useraccount で新しい認証スコープを作成することはできません。ランタイムでは、名前の代わりに sys_id を使用して認証スコープのチェックを行い、システムプロパティ *glide.oauth.token.scope.useraccount* を新しく作成された sys_id レコードに変更します。

oauth_entity にリンクされた認証スコープを管理者が変更すると、この OAuth エンティティによって発行された既存のすべての OAuth アクセストークンも変更されますか。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

はい。認証スコープは OAuth アクセストークンに直接リンクされておらず、実行時に oauth_entity から取得されます。

同じ oauth_entity によって発行された別々の OAuth アクセストークンに異なる認証スコープを設定することはできますか。

いいえ。トークンへのすべてのアクセスが同じ oauth_entity によって発行されているため、認証スコープは常に同じになります。

ユーザーが特定のエンドポイントに対して複数の異なる認証スコープを定義することはできますか。

いいえ。特定の REST API エンドポイントに対しては一意の制約チェックがあります。ただし、同じ REST API エンドポイントに対しては、複数の一致する認証スコープが存在する場合があります。

認証スコープのチェックは BasicAuth にも使用されますか。

いいえ、認証スコープのチェックは OAuth アクセストークンと OIDC トークンのみであり、*basicAuth* と *mutualAuth*には適用されません。

SOAP API アクセスポリシー

SOAP API アクセスポリシーを使用すると、認証タイプとアクセスポリシーの指定されたフィルター基準に基づいて、受信 SOAP API へのアクセスを制限できます。

SOAP API アクセスポリシーを使用すると、受信認証プロファイルと API アクセスポリシーを受信 SOAP およびスクリプト化された SOAP API に適用できます。

IP 範囲やロールベースの制限などの ServiceNow API アクセスポリシーを活用し、認証に基づいて受信 SOAP API 呼び出しを許可または禁止できます。

管理者は、次のアクションを実行してポリシーを適用できます。

- SOAP API Access Policy プラグインとAuthentication Profile プラグインを有効にします。詳細については、「SOAP API アクセスポリシーのアクティブ化」を参照してください。
- SOAP API アクセスポリシーを作成し、それらのポリシーを認証プロファイルに関連付けます。詳細については、「SOAP API アクセスポリシーの作成」と「認証プロファイルの作成」を参照してください。

  注:
  ポリシーは、SOAP テーブル API またはスクリプト化された SOAP API に適用されます。標準の http および WSSE 認証プロファイルに加えて。

- IP 範囲、ロールベースの制限などの認証ポリシーを作成し、このポリシーを認証プロファイルに関連付けます。詳細については、「API 認証ポリシーの作成」を参照してください。

SOAP API アクセスポリシーのアクティブ化

SOAP API アクセスポリシーの場合は、SOAP API Access Policy (com.glide.soap.policy) プラグインをインストールします。

始める前に
必要なロール：admin

このタスクについて
次のアイテムは、SOAP API Access Policy プラグインとともにインストールされます： プロセッサーアクセスポリシー (com.glide.processor.policy)

依存プラグイン：Authentication Profile (com.glide.auth.profile)

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

手順

1. 移動先 すべて > システムアプリケーション > 利用可能なすべてのアプリケーション > すべて.
2. フィルター基準と検索バーを使用して、SOAP API Access Policy プラグイン (com.glide.soap.policy) を検索します。

   名前または ID でプラグインを検索できます。プラグインが見つからない場合は、ServiceNow 担当者から要求する必要があります。
3. [インストール] を選択して、[プラグインをアクティブにする] ダイアログボックスで、[アクティブ化] をクリックします。

   注:
   ドメイン分離と代理管理者がインスタンスで有効になっている場合、管理ユーザーはグローバルドメインに含まれている必要があります。それ以外の場合、次のエラーが表示されます： 別の操作が実行されているため、アプリケーションのインストールは利用できません：<プラグイン名> のプラグインの有効化。

認証プロファイルの作成

認証プロファイルを作成し、1 つ以上の認証ポリシーをプロファイルに追加します。デフォルトで利用可能な **ID** トークンおよび **OAuth** トークンの認証プロファイルを設定することもできます。

始める前に
必要なロール：admin

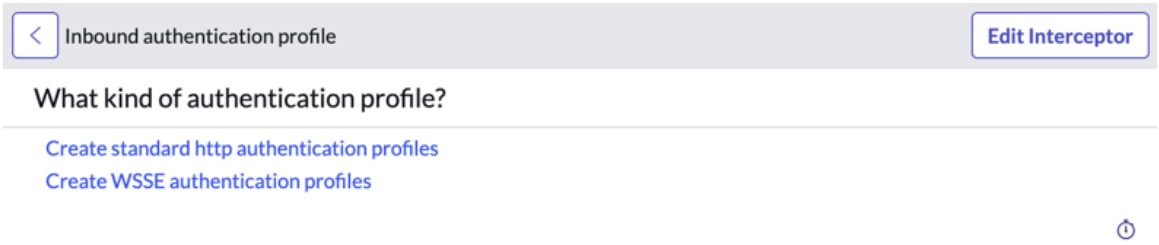
注:
相互認証とカスタマイズされた認証を使用して、認証ポリシー、IP 範囲、ロールベース、ユーザーベースなどを適用できます。

手順

1. 移動先 すべて > システム **Web** サービス > **API** アクセスポリシー > 受信認証プロファイル.
2. [新規] をクリックします。
   「認証プロファイルの種類は？」というメッセージが表示されます。
3. [認証プロファイルの種類は？] を選択します。
   - 標準の **http** 認証プロファイルを作成
   - **WSSE** 認証プロファイルを作成

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



4. フォームのフィールドに入力します。

[標準の認証プロファイル] フォーム

フィールド	説明
名前	認証ポリシーを識別する名前
説明	認証ポリシーの説明
有効	認証ポリシーをアクティブにするオプション
アプリケーション	認証ポリシーの範囲
タイプ	利用可能な認証のタイプ。[基本認証]、**[ID** トークン]、[証明書ベースの認証]、**[OAuth]** または **[WSSE]** (WSSE 認証プロファイルの場合) を選択できます。
OAuth エンティティ	OAuth エンティティプロファイル。このフィールドは、[タイプ] で **[ID** トークン] または **[OAuth]** を選択した場合のみ表示されます。

5. [新規行を挿入] をダブルクリックします。

6. リストから認証ポリシーを選択し、保存アイコン ( ) をクリックします。

注:
[アクセスポリシーを許可] または [アクセスポリシーを拒否] は選択しないでください。これらのポリシーは、ユーザーログインのみを対象としています。

1 つ以上の複数の認証ポリシーを認証プロファイルに追加できます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

SOAP API アクセスポリシーの作成

API アクセスポリシーを作成し、認証プロファイルをマップして SOAP API の認証タイプを制限します。たとえば、SOAP API の ID トークン認証のみを許可する API アクセスポリシーを作成できます。

始める前に

- 認証プロファイルが作成されていることを確認します。詳細については、「認証プロファイルの作成」を参照してください。
- 必要なロール：管理者

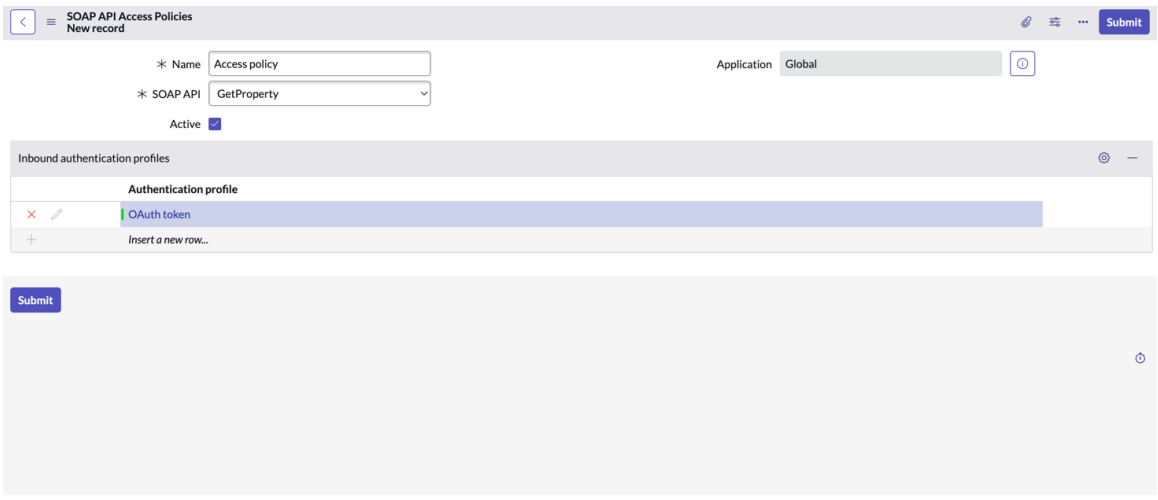
手順

1. 移動先 すべて > システム **Web** サービス > **API** アクセスポリシー > **SOAP API** アクセスポリシー.
2. [新規] をクリックします。
3. フォームのフィールドに入力します。

[API アクセスポリシー] フォーム

フィールド	説明
名前	API アクセスポリシーの一意の名前。
SOAP API	アクセスポリシーが適用される SOAP API。 例：**GetProperty API**。
アプリケーション	アプリケーションのスコープ。
有効	API アクセスポリシーをアクティブにするオプション。

4. [受信認証] セクションで、[新規行を挿入] をダブルクリックします。
5. リストから受信認証プロファイルを選択し、保存アイコン ( ) をクリックします。
たとえば、基本認証、**ID** トークン、証明書ベースの認証、**OAuth**、または **WSSE** 認証 を追加できま



す。

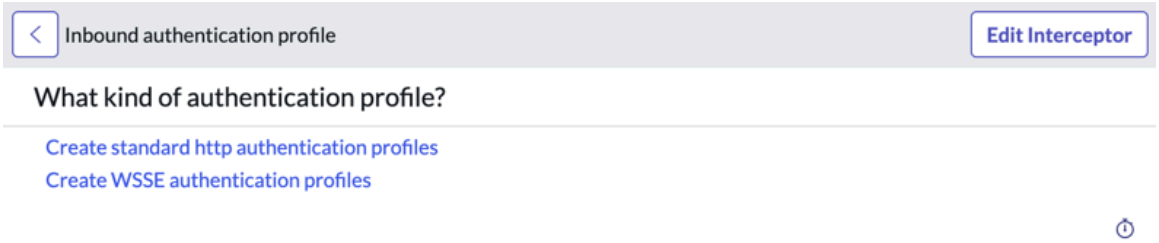
   a. 1 つ以上の受信認証プロファイルを追加するには、[新規] をクリックして新しいプロファイルを作成します。

   b. [認証プロファイルの種類は？] を選択します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

- 標準の **http** 認証プロファイルを作成
- **WSSE** 認証プロファイルを作成



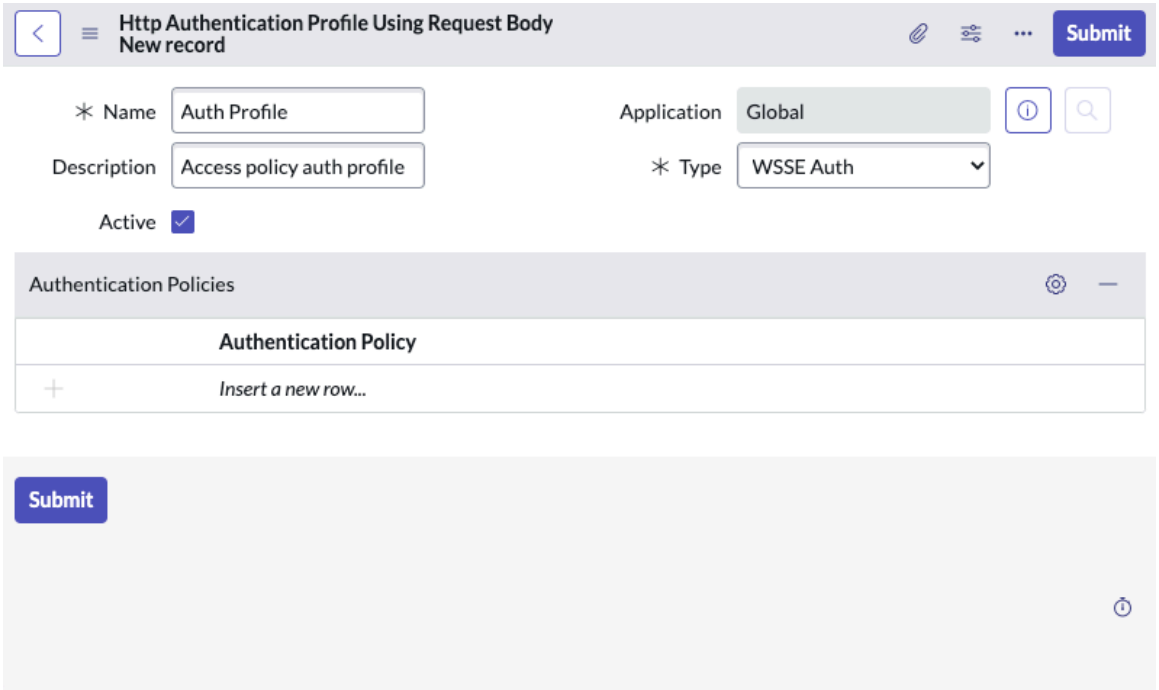
c. WSSE 認証プロファイルを作成するには、フォームのフィールドに入力します。

WSSE 認証プロファイル

フィールド	説明
名前	API アクセスポリシーの一意の名前。
説明	認証プロファイルの説明。
アプリケーション	アプリケーションのスコープ。
有効	API アクセスポリシーをアクティブにするオプション。
タイプ	認証プロファイル WSSE (Web セキュリティ) としての WSSE 認証。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



d. 認証プロファイルを作成したら、レコードを保存します。

6. [送信] をクリックして SOAP API アクセスポリシーを送信します。

SOAP API を保護するためのグローバル API アクセスポリシーの作成

すべての SOAP API を保護する単一のグローバル API アクセスポリシーを作成します。

始める前に

- 必要なロール：admin
- **Processor Access policy** (com.glide.processor.policy) プラグインをインストールします。
- 認証プロファイルが作成されていることを確認します。詳細については、「認証プロファイルの作成」を参照してください。

次の手順では、すべての SOAP API を保護する単一のグローバル API アクセスポリシーを作成する方法について説明します。

> **注:**
> 個々の SOAP API レベルで定義されたポリシーは、**SOAPProcessor** レベルのグローバルアクセスポリシーを上書きします。

手順

1. 移動先 すべて > システムセキュリティ > プロセスアクセスポリシー.

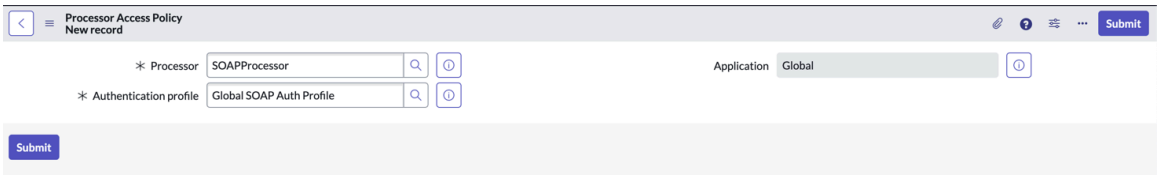
2. フォームのフィールドに入力します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

プロセスアクセスポリシーフォーム

フィールド	説明
プロセッサ	認証ポリシーを識別する名前。たとえば、**[SOAPProcessor]** (認証プロファイル) を選択します。
アプリケーション	認証ポリシーの範囲デフォルト：グローバル
認証プロファイル	認証プロファイルのタイプ。[グローバル **SOAP** 認証プロファイル **(Global SOAP Auth Profile)]** を選択します。



3. [送信] を選択します。

API のフィルター基準

フィルター基準には、認証ポリシーのポリシー入力として使用されるフィルター条件またはクエリーが含まれています。ポリシー入力は 1 つ以上のフィルター基準をグループ化し、認証ポリシーのポリシー条件を定義するために使用されます。たとえば、IP フィルター基準は、クラスレスドメイン間ルーティング (CIDR) 形式の IP アドレスまたは IP アドレス範囲を定義します。

ユーザーの IP アドレス、ロール、およびユーザーが属するユーザーグループに基づいて、フィルター基準を作成できます。

注:
適応認証モジュールから作成されたフィルター基準も使用します。詳細については、「適応認証」を参照してください。

適応認証のフィルター基準と同じプロセスを使用して、API のフィルター基準を作成できます。詳細については、「フィルター基準」を参照してください。

関連情報

IP フィルター基準の作成

ロールフィルター基準の作成

グループフィルター基準の作成

API 認証ポリシー

認証ポリシーは、指定されたポリシー条件に基づいて認証要求を評価し、一致する基準に応じてアクセスを許可または拒否します。

組み込みのグローバルブロックポリシーを使用するか、セキュリティ要件に従って認証ポリシーを作成できます。グローバルブロックポリシーは、指定されたフィルター基準に基づいてユーザーと API の認証要求を拒否します。

注:
[アクセスポリシーを許可] および [アクセスポリシーの拒否] を使用または変更しないでください。これらのポリシーは、ユーザーログインのみを対象としています。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

API 認証ポリシーの作成

認証ポリシーを使用すると、指定されたフィルター基準に基づいて API のアクセス制限を適用できます。

始める前に

必要なロール：管理者

手順

1. 移動先 すべて > システム **Web** サービス > **API** 認証ポリシー.
2. [新規] をクリックします。
3. フォーム上で、以下のフィールドに記入します。

ポリシーフォーム

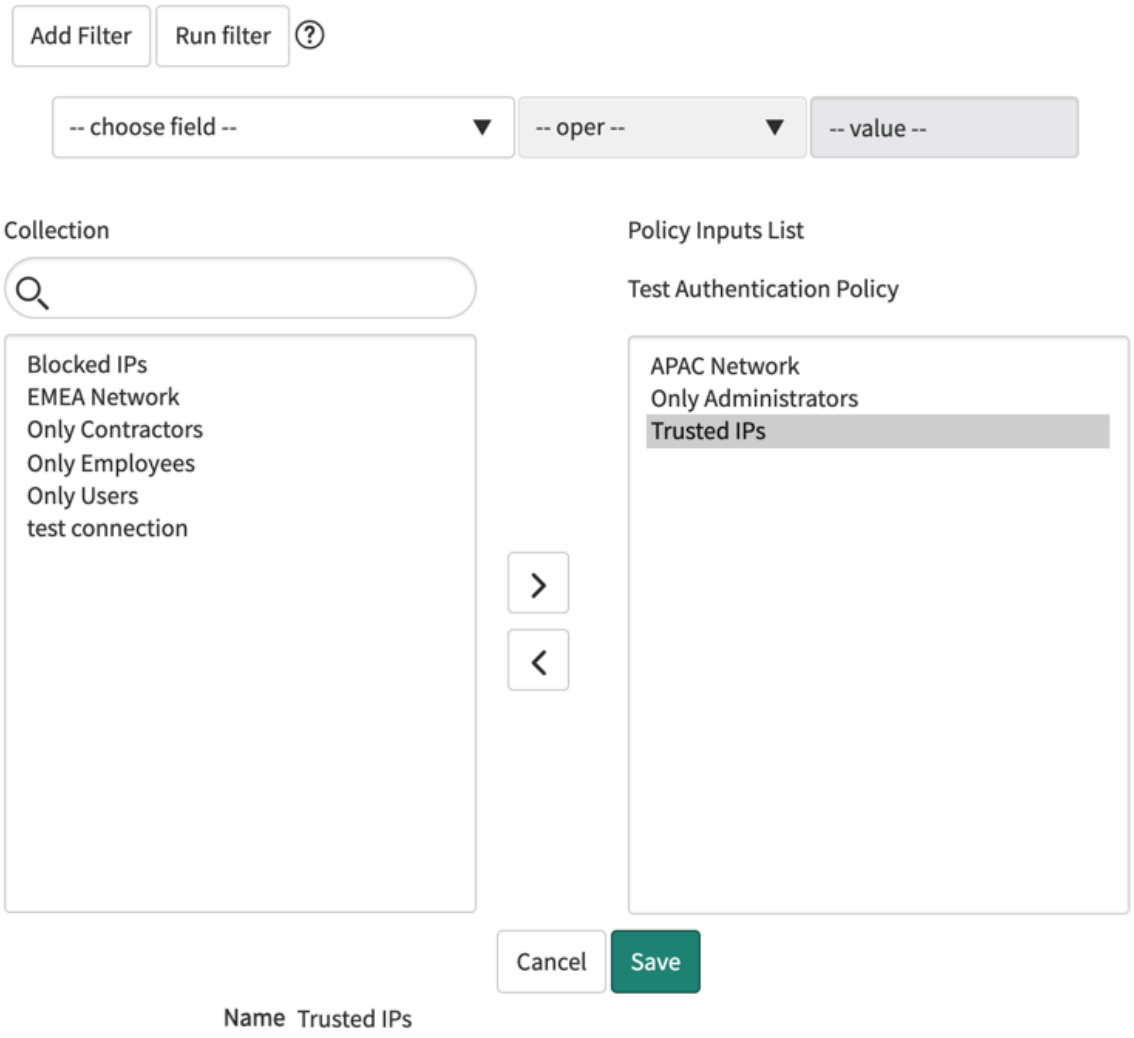
フィールド	説明
名前	ポリシーを識別する名前。
説明	ポリシーの簡単な説明。
アプリケーション	アプリケーションのスコープ

4. フォームヘッダーを右クリックし、[保存] を選択します。
5. [ポリシーの入力] タブで、[編集] を選択して既存のフィルター基準を追加します。
   新しいポリシー入力を作成することもできます。詳細については、「ポリシー入力の作成」を参照してください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

6. 1 つ以上のフィルター基準を、[コレクション] リストから [ポリシー入力リスト] に移動しま



す。

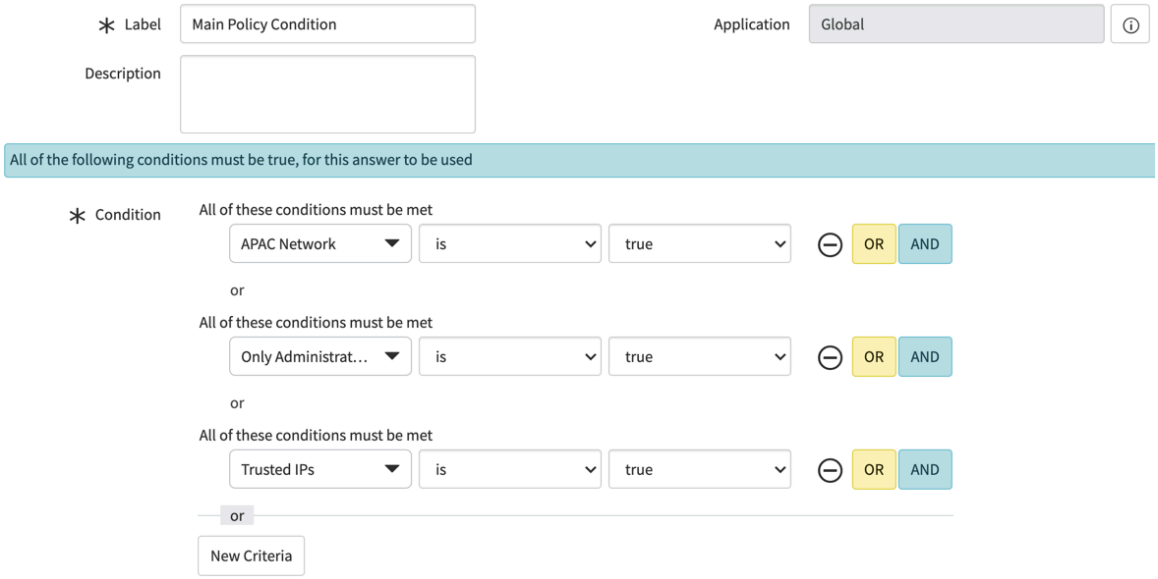
7. [保存] を選択します。
8. [ポリシー条件] タブで、[新規] をクリックします。
9. フォーム上で、以下のフィールドに記入します。

[条件] フォーム

フィールド	説明
ラベル	ポリシー条件の名前
説明	ポリシー条件の簡単な説明
アプリケーション	アプリケーションのスコープ
条件	**OR** フィルターと組み合わされた 1 つ以上の条件。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



10. [送信] を選択します。

API のグローバルブロックポリシーの設定

グローバルブロックポリシーは、指定されたフィルター条件に基づいてユーザーと API の認証要求を拒否します。このポリシーは、IP アドレスアクセス制御の代わりに使用できます。

始める前に

必要なロール：管理者

手順

1. 移動先 すべて > システム **Web** サービス > **API** アクセスポリシー > グローバルブロックポリシー.
2. [ポリシーの入力] タブで、[編集] をクリックします。
3. [コレクション] リストから 1 つ以上のフィルター基準を選択し、[グローバルブロックポリシー] リストに移動します。
   他のフィルターを追加することもできます。
4. [ポリシー条件] タブで、[新規] をクリックします。
5. フォームの各フィールドに入力します。

[条件] フォーム

フィールド	説明
ラベル	条件を識別する名前
説明	条件の説明
条件	認証要求を評価するために使用される複数のポリシー入力 (フィルター基準) の論理的な組み合わせ。たとえば、信頼できる IP アドレスのリストから請負会社のみを許可するような条件を作成できます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

システム/エクスポートプロセッサーのアクセスポリシー

システム/エクスポートプロセッサーがプロセッサーアクセスポリシーを活用してすべてのエクスポートエンドポイントを保護する機能。

すべてのエクスポートエンドポイントを保護し、グローバルまたはインスタンスレベルで受信認証プロファイルとプロセッサーアクセスポリシーを適用する機能。

注:

- アクセスポリシーでは、CSV、PDF などのエクスポートプロセッサーを含む非公開プロセッサーがサポートされています。
- アクセスポリシーではスクリプトプロセッサーもサポートされています。

サンプルユースケース

- 管理者は、API アクセスポリシーを利用することで、RSS プロセッサーを使用しない場合にそれをブロックできます。
- 管理者は、基本認証を使用して認証プロファイルを作成し、常に false と評価される認証ポリシーを関連付けることができます。

  例：0.0.0.0 ～ 255.255.255.255 の範囲で IP 基準を作成し (Ipv6 アドレススペースも追加します)、false 演算子を使用してポリシー条件を追加します。このようにすると、ポリシー条件は常に false と評価され、API アクセスポリシーは要求の送信元に関係なくアクセスをブロックします。

- 信頼できるネットワークからのみプロセッサーへのアクセスを許可します。

プロセッサアクセスポリシーのアクティブ化

プロセッサーの場合は、Processor Access policy (com.glide.processor.policy) プラグインをインストールします。

始める前に
必要なロール：admin

このタスクについて
次のアイテムはプロセッサーアクセスポリシーとともにインストールされます。

- システムプロパティ：com.glide.auth.profile.supported.processor.list
- ナビゲーションのモジュール：プロセッサーアクセスポリシー

手順

1. 移動先 すべて > システムアプリケーション > 利用可能なすべてのアプリケーション > すべて.
2. フィルター基準と検索バーを使用して、Processor Access policy (com.glide.processor.policy) プラグインを検索します。

   名前または ID でプラグインを検索できます。プラグインが見つからない場合は、ServiceNow 担当者から要求する必要があります。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

3. [インストール] を選択して、[プラグインをアクティブにする] ダイアログボックスで、[アクティブ化] をクリックします。

> **注:**
> ドメイン分離と代理管理者がインスタンスで有効になっている場合、管理ユーザーはグローバルドメインに含まれている必要があります。それ以外の場合、次のエラーが表示されます： 別の操作が実行されているため、アプリケーションのインストールは利用できません：<プラグイン名> のプラグインの有効化。

次のタスク

。
プロセッサーの認証プロファイルを設定します。詳細については、「プロセッサーの認証プロファイルの設定」を参照してください。

プロセッサーの認証プロファイルの設定

エクスポートプロセッサーの認証プロファイルを適用します。

始める前に
必要なロール：admin

必要なプラグイン：Processor Access Policy (com.glide.processor.policy)

手順

1. 移動先 すべて > システムセキュリティ > プロセスアクセスポリシー.
2. プロセッサーに認証プロファイルを追加するには、[新規] をクリックします。
3. フォームのフィールドに入力します。

プロセスアクセスポリシーフォーム

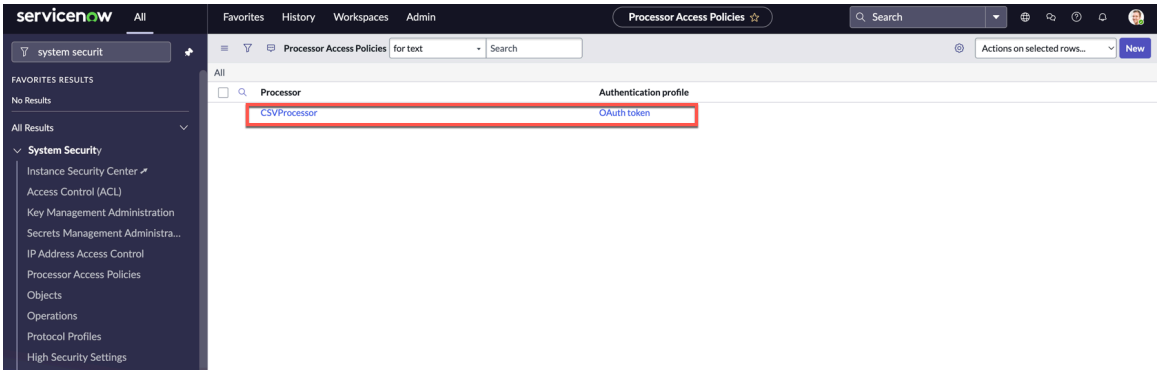
フィールド	説明
プロセッサ	認証ポリシーを識別する名前。 **注:** 公開プロセッサーはサポートされていません。サポートされていないプロセッサーを選択すると、プロセッサーの送信中にエラーが表示されます。
アプリケーション	認証ポリシーの範囲デフォルト：グローバル
認証プロファイル	認証プロファイルのタイプ。**[ID** トークン] または **[OAuth** トークン] を選択できます。

4. [送信] をクリックします。
認証プロファイルがプロセッサーに適用されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

たとえば、CSV プロセッサーに対して OAuth 認証プロファイルが構成されているとします。この場合、エクスポートオプションとして CSV を使用し、OAuth アクセストークンを使用する必要があります。



証明書ベースの認証

証明書ベースの認証では、信頼できる認証局 (CA) からの証明書を使用して、ユーザーのログインまたは受信 API 要求を相互に認証できます。

注:
証明書ベースの認証は、オンプレミスおよび Edge Encryption が有効なインスタンスではサポートされていません。

ユーザーインターフェイスログインのための証明書ベースの認証

エンドユーザーが、ユーザー名とパスワードを使用する代わりに PIV (個人 ID 検証) または CAC (Common Access Card) カードを使用して Now Platform または サービスポータル にログインできるようにします。ユーザーインターフェイスログインの相互認証を設定するには、「証明書ベースの認証の設定」を参照してください。

証明書ベースの認証が設定されると、エンドユーザーは設定を完了してログインできます。「証明書ベースの認証を使用したログイン」を参照してください。

受信 Web サービスの証明書ベースの認証

ServiceNow SOAP および REST API への受信要求を認証します。受信 Web サービスの相互認証を設定するには、「証明書ベースの認証の設定」を参照してください。

証明書ベースの認証の設定

ユーザーインターフェイスベースのログインまたは受信 Web サービスの相互認証を設定します。

始める前に
必要なロール：admin

インスタンスで ADCv2 ロードバランサーを使用していることを確認します。詳細は、ADCv2 移行に関するナレッジ記事 を参照してください。インスタンスで ADCv2 ロードバランサーを使用していない場合は、Now Support にお問い合わせください。

手順

証明書ベースの認証を設定する目的：

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- エンドユーザーが PIV または CAC カードを使用して Now Platform または サービスポータル に安全にログインできるようにするため。証明書ベースの認証を有効にした後、PEM 証明書を自己登録するか、管理者が証明書をマッピングすることができます。「証明書ベースの認証を使用したログイン」を参照してください。
- 受信 Web サービスの相互認証を有効にするため。証明書ベースの認証が設定されると、システムでは提供された証明書を使用して、ServiceNow REST API および SOAP API にアクセスするために要求を相互認証します。

証明書ベースの認証のアクティブ化

admin ロールを持っている場合は、 Now Platform の 証明書ベースの認証プラグイン (com.glide.auth.mutual) をアクティブ化できます。

始める前に
必要なロール：admin

このタスクについて
次の テーブルが証明書ベースの認証とともにインストールされます。

- sys_user_certificate
- sys_ca_certificate
- sys_ca_certificate_api_track

手順

1. 移動先 すべて > システムアプリケーション > 利用可能なすべてのアプリケーション > すべて.
2. フィルター基準と検索バーを使用して Certificate-based authentication プラグイン (com.glide.auth.mutual) を検索します。

   名前または ID でプラグインを検索できます。プラグインが見つからない場合は、ServiceNow 担当者から要求する必要があります。
3. [インストール] を選択して、[プラグインをアクティブにする] ダイアログボックスで、[アクティブ化] をクリックします。

   注:
   ドメイン分離と代理管理者がインスタンスで有効になっている場合、管理ユーザーはグローバルドメインに含まれている必要があります。それ以外の場合、次のエラーが表示されます： 別の操作が実行されているため、アプリケーションのインストールは利用できません：<プラグイン名> のプラグインの有効化。

CA 証明書の登録

ルート証明書または中間証明書を登録して、認証に使用できるようにします。

始める前に
必要なロール：管理者

手順

1. 移動先 すべて > 証明書ベースの認証 > **CA** 証明書チェーン.
2. [新規] をクリックします。
3. フォームのフィールドに入力します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

[相互認証 **CA** 外部審査済み書] フォーム

フィールド	説明
名前	証明書を識別する名前
有効期限通知	証明書の有効期限が近づいたときにユーザーに警告するオプション。
期限切れ時に通知	証明書の有効期限が切れたときに通知を受信するユーザーのリスト。
有効期限切れ前に警告	証明書の有効期限が切れる前に通知を送信する日数。
有効	クライアント証明書をアクティブにするオプション。
フォーマット	PEM
タイプ	証明書のタイプ。次のオプションが含まれます。 ○ **CA** 証明書：ルート CA 証明書。チェーンに中間証明書を含めることもできます。CA 証明書は自動的にロードバランサーと同期されます。できるだけこのオプションを使用して、チェーン内の必要な証明書が欠落しないようにしてください。 ○ 中間証明書：証明書チェーン内の中間証明書。この証明書はインスタンスにのみ残り、ロードバランサーとは同期されません。このオプションは、既存のチェーンに中間証明書を追加する必要がある場合にのみ使用します。
簡単な説明	ユーザーのクライアント証明書の簡単な説明。

注:
証明書のアップロード中に、読み取り専用フィールドの [有効開始日]、[有効期限]、[数日中に期限切れ **(Expires in days)]**、[発行者]、[件名]、[証明書チェーン]、および **[PEM** 証明書] が抽出されて自動入力されます。

4. [送信] をクリックします。
5. オプション: 証明書を検証するには、[ストア/証明書を検証] をクリックします。

PEM 証明書をユーザーにマップ

PEM 証明書をユーザーにマップし、ユーザーが PIV または CAC カードを使用してログインしたり、受信要求を認証したりできるようにします。複数の PEM 証明書をユーザーにマップできます。

始める前に

- 必要なロール：admin
- ユーザーのプライバシー拡張メール (PEM) 証明書があることを確認します。

注:
PEM 証明書をユーザー構成にマッピングすると、「証明書の検証」が失敗します。これは、PEM 証明書が保存されていないためです。

手順

1. 移動先 すべて > 証明書ベースの認証 > ユーザーから証明書へのマッピング をクリックし、「 新規」をクリックします。
2. フォームのフィールドに入力します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

[ユーザークライアント外部審査済み書] フォーム

フィールド	説明
名前	ユーザーのクライアント証明書の名前
有効期限通知	証明書の有効期限が近づいたときにユーザーに警告するオプション。
有効期限切れ前に警告	証明書の有効期限が切れる前に通知を送信する日数。
期限切れ時に通知	証明書の有効期限が切れたときに通知を受信するユーザーのリスト。
有効	クライアント証明書をアクティブにするオプション。
ユーザー	クライアント証明書にマップされているユーザー。 システムは、受信要求または証明書登録からクライアント証明書を受信した後、このフィールドで指定されたユーザーを使用して要求を実行するセッションを開始します。
簡単な説明	ユーザーのクライアント証明書の簡単な説明。
フォーマット	Privacy Enhanced Mail (PEM) 形式は、base-64 でエンコードされた Distinguished Encoding Rules (DER) 証明書です。
タイプ	クライアント証明書。このフィールドは読み取り専用です。

注:
証明書のアップロード中に、読み取り専用フィールドの [有効開始日]、[有効期限]、[数日中に期限切れ **(Expires in days)]**、[発行者]、および [件名] が抽出されて自動入力されます。

3. 添付ファイルアイコンをクリックして証明書をアップロードします。
4. [送信] をクリックします。
証明書が信頼できる認証局 (CA) からのものである場合、証明書が検証され、指定されたユーザーにマップされます。

証明書ベースの認証プロパティの設定

システムプロパティを使用して、証明書ベースの認証機能を有効または無効にします。

始める前に
必要なロール：管理者

手順

1. 移動先 すべて > 証明書ベースの認証 > プロパティ.
2. フォームのフィールドに入力します。

[証明書ベースの認証プロパティ **(Certificate Based Authentication Properties)]** フォーム

プロパティ	説明
外部審査済み書ベースの認証を有効にする	ユーザーインターフェイスのログインと受信 Web サービスの両方に対して証明書ベースの認証を有効にするオプション

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

プロパティ	説明
	デフォルト：true
ログイン画面に [PIV / CAC でログイン (Log in with PIV/CAC)] オプションを表示します	ログイン画面に **[PIV/CAC** カードでログイン] オプションを表示します。ユーザーがユーザーインターフェイスを使用して証明書ベースの認証を使用できるようにします。 デフォルト値：false
証明書ベースのログインの自動リダイレクトを有効にします	登録された証明書を選択して PIN を入力した後に、ユーザーが **[PIV/CAC** カードでログイン] をクリックする必要があるかどうかを決定します。アクティブ化すると、登録されたクライアント証明書を選択して PIN を入力した後に、ユーザーが自動的にログインされます。非アクティブ化すると、登録されたクライアント証明書を選択して PIN を入力した後に、ユーザーは **[PIV/CAC** カードでログイン] をクリックする必要があります。 デフォルト値：false

自動翻訳

証明書ベースの認証を使用したログイン

管理者が証明書ベースの認証を設定すると、PIV (Personal Identity Verification) または CAC (Common Access Card) カードを使用してクライアント証明書を登録し、ログインできるようになります。

PIV または **CAC** カードのクライアント証明書の登録

PIV または CAC カードを使用して Now Platform にログインする前に、PIV または CAC カードのクライアント証明書を登録する必要があります。クライアント証明書を登録できない場合は、管理者にお問い合わせください。管理者は、PIV または CAC カードのクライアント証明書を登録することもできます。

始める前に

- 証明書ベースの認証が有効になっていることを確認します。
- カードリーダーがコンピューターに接続され、PIV または CAC カードが挿入されていることを確認します。
- 必要なロール：なし

このタスクについて

クライアント証明書を登録するために管理者が必要な場合は、「PEM 証明書をユーザーにマップ」を参照してください。

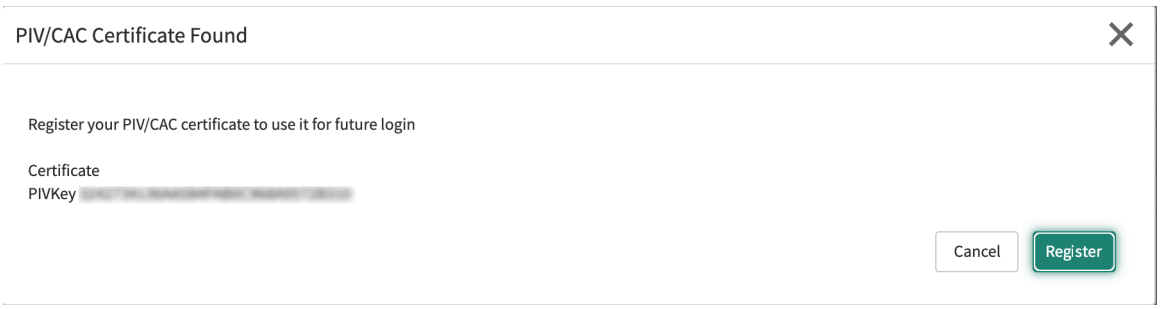
手順

1. ユーザー名とパスワードを使用して Now Platform にログインします。
2. ユーザーメニューから自分の名前をクリックし、[プロファイル] を選択します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

3. [関連リンク] から、[クライアント証明書を登録] をクリックします。

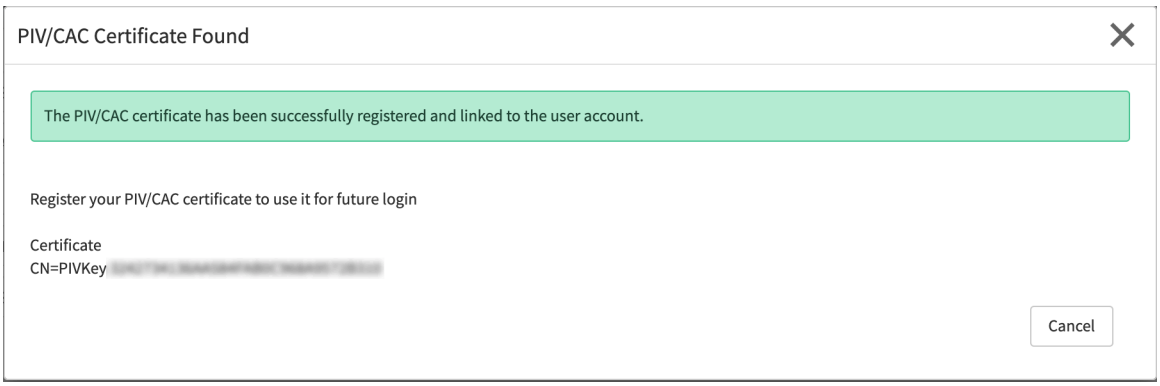
   有効な証明書が利用可能な場合は、次のメッセージが表示されます。



4. [登録] をクリックします。

   登録に成功すると、次のメッセージが表示されます。

   PIV/CAC 証明書が正常に登録され、ユーザーアカウントにリンクされました。



   Now Platform に次回ログインするときは、PIV または CAC カードを使用してログインできます。詳細については、「PIV または CAC カードを使用して Now Platform にログイン」を参照してください。

PIV または CAC カードを使用して Now Platform にログイン

Now Platform で証明書ベースの認証が有効になっている場合は、ユーザー名とパスワードの代わりに PIV または CAC カードを使用してログインできます。

始める前に

- 必要なロール：なし
- 証明書ベースの認証が有効になっていることを確認します。
- PIV または CAC のカードリーダーがコンピューターに接続されていることを確認します。
- PIV または CAC カードのクライアント証明書がマップされていることを確認します。詳細については、「CA 証明書の登録」を参照してください。

自動翻訳

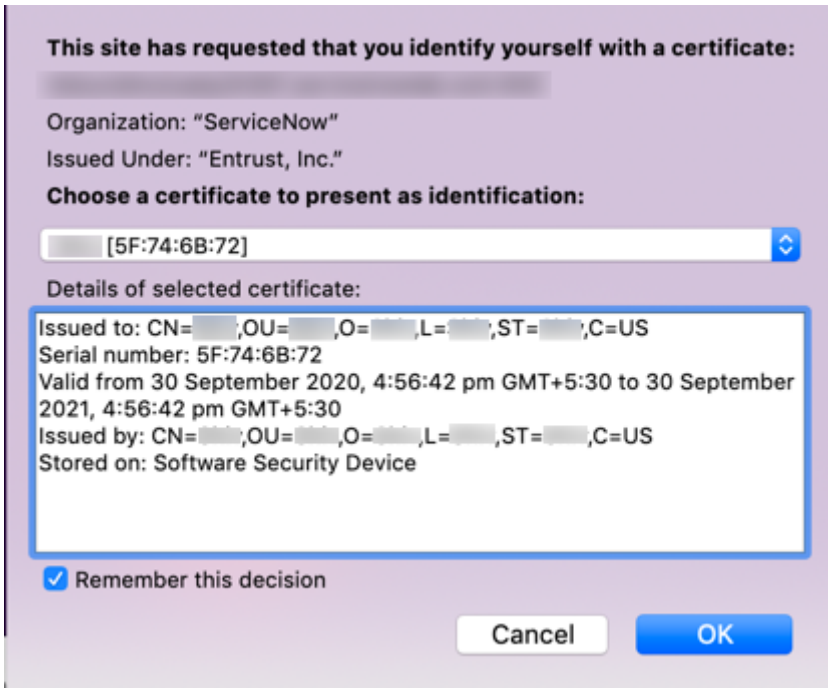
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. PIV または CAC カードをカードリーダーに挿入します。
2. ブラウザーでインスタンスに移動します。
   PIV または CAC カードの PIN を入力するよう求めるプロンプトがブラウザーに表示されます。
3. ブラウザーのプロンプトに PIV または CAC カードの PIN を入力します。

   注:
   PIN を忘れた場合は、管理者にお問い合わせください。

4. 正しい PIN を入力すると、証明書を選択するためのプロンプトがブラウザーに表示されます。

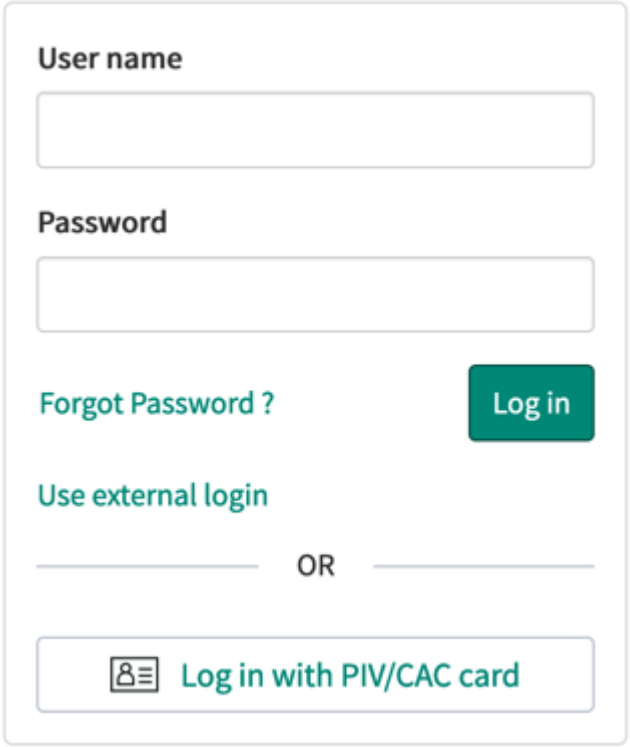


5. ブラウザープロンプトから証明書を選択します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

証明書が有効かつマップされている場合は、ログインページにリダイレクトされま



す。

6. **[PIV/CAC** カードでログイン] ボタンをクリックします。

   Now Platform からログアウトするには、カードリーダーから PIV または CAC を取り出してブラウザーを閉じる必要があります。

クライアント証明書の管理

アカウントに関連付けられているクライアント証明書を表示および削除します。

始める前に

- 証明書ベースの認証が有効になっていることを確認します。
- 必要なロール：なし

手順

1. ユーザー名とパスワードを使用して Now Platform にログインします。
2. ユーザーメニューから自分の名前をクリックし、[プロファイル] を選択します。

3. [関連リンク] から、[クライアント証明書を管理] をクリックします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ユーザークライアント証明書 [sys_user_certificate] テーブルが開き、アカウントに関連付けられている証明書が表示されます。

4. アカウントに関連付けられている証明書を表示または削除します。

インスタンスへのカスタム URL の関連付け

会社ブランドまたはカスタム URL から ServiceNow インスタンスにアクセスできるようにすることができます。

カスタム URL の概要

カスタム URL を使用すると、1 つまたは複数の会社ブランドやカスタム URL から ServiceNow インスタンスにアクセス可能にすることができます。

カスタム URL は特定のポータルに関連付けることができます。たとえば、管理者であれば CSM ポータルでは http://support.acme.com を、人事ポータルでは http://hr.acme.com を定義できます。このような状況では、ユーザーがアクセスしているカスタム URL に基づいて、ユーザーを認証のため別の IdP にリダイレクトする必要があります。

重要:

- インスタンスあたりのドメイン数が 100 を超えるカスタム URL を作成しないでください。
- 最初に ServiceNow インスタンスからカスタム URL レコードを削除してから、任意のドメインネームサーバー (DNS) エントリを DNS サーバーから削除する必要があります。
- カスタム URL レコードを ServiceNow インスタンスから削除する前に DNS エントリを DNS サーバーから削除すると、ServiceNow から対応する他のカスタム URL レコードの削除がブロックされる可能性があります。

Tokyo 以降は、カスタム URL レコードで定義された指定の IdP にユーザーが自動でリダイレクトできるようにすることができます。

注:
カスタム URL は、オンプレミスの顧客または開発者インスタンスには使用できません。また、URL は公開されている必要があります。

トップレベルドメイン (TLD) または任意のサブドメインの所有者のみが、DNS サブドメインにカスタム URL を設定できます。たとえば、インスタンスに次のような指定 URL と追加のカスタム URL があるとします。

カスタム URL の例

URL 例	使用法
https://acme.service-now.com	ServiceNow インスタンスに付属する Acme の初期ドメイン名。
https://support.acme.com	ServiceNow インスタンスに関連付けられているカスタム URL。この URL は、初期ドメイン名のエイリアス (CNAME) と呼ばれます。
https://US-support.acme.com	インスタンスのサービスポータルに関連付けられている予備のカスタム URL。インスタンスは、同じサービスポータルに対するカスタム URL を複数サポートできます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

インスタンス外のカスタム URL に関する考慮事項

カスタム URL を関連付けるには、その前にドメインプロバイダーを介して URL を所有 (または購入) する必要があります。また、カスタム URL を作成してインスタンスに関連付ける前に、特定の構成も必要になります。

カスタム URL 構成

構成アイテム	説明
プロバイダーでの CNAME 設定 (Set the CNAME with the provider)	CNAME レコードは ServiceNow インスタンス URL として設定する必要があります。
専用 VIP ステータスの確認 (Determine your dedicated VIP status)	VIP のステータス

注:
インスタンスを指す CNAME レコードを削除または更新する場合は、インスタンス内でレコードが不安定な状態にならないよう、このシーケンスに従う必要があります。まずインスタンスから CNAME レコードを削除し、次に DNS プロバイダーで CNAME 設定を削除または更新します。

カスタム URL のアクティブ化

ServiceNow インスタンスでカスタム URL を設定できるようにします。管理者ロールを持っている場合は、Custom URL プラグイン (com.snc.customurl) をアクティブ化することができます。

始める前に
必要なロール：管理者

手順

1. 移動先 すべて > システム定義 > プラグイン.
2. **[Custom URL]** プラグインを検索してクリックします。

   注:
   [Custom URL - Internal] プラグインは選択しないでください。これはスクリプト化されたカスタム URL API の内部コンポーネントです。

3. カスタム URL レコードで、[アクティブ化/修復] 関連リンクをクリックします。
4. [プラグインアクティベーション] ウィンドウで、[アクティブ化 **(Activate)]** をクリックします。[プラグインのアクティベーション] ウィンドウが再度開き、プラグインがアクティブ化されたというメッセージが表示されたら、[フォームを閉じて再ロード] をクリックしてこのフォーム に留まります。
5. [プラグインファイル] 関連リストで、次のプロパティを検索して設定値を変更します。

オプション	説明
glide.customurl.enabled	カスタム URL を有効にするには、値を **True** に設定します。デフォルトでは、このプロパティは **False** に設定されています。この場合、カスタム URL を関連付けることはできません。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

オプション	説明
	注: この機能を無効にするには、 プロパティを **False** に設定します。

6. [更新] をクリックします。

カスタム **URL** をインスタンス **URL** として設定

ServiceNow URL の代わりにカスタム URL を使用するインスタンス構成に追加します。

始める前に

必要なロール：admin
カスタム URL をインスタンスに追加する前に、Custom URL プラグインをアクティブ化して URL を購入または登録する必要があります。

手順

1. 移動先 すべて > カスタム **URL** > カスタム **URL**. 次のいずれかを実行する必要があります。
   - [新規] をクリックして、インスタンスに新しいドメイン名を関連付けます。
   - インスタンス URL として設定するために、すでに設定されているカスタム URL を選択します。
2. 適宜フィールドに入力します。

カスタム **URL** フィールド

フィールド	説明
ドメイン名	カスタム URL の完全修飾ドメイン名 (FQDN) FQDN は、カスタムドメインのネームサーバーレコードに作成された CNAME リダイレクトです。 注: たとえば、acme.com のネームサーバーで、次のようにエントリを作成します。 `support.acme.com 300 IN CNAME acme.servicenow.com`
インスタンス URL である	すべての送信 URL に対してこのカスタム URL を有効にするチェックボックス。アクティブなカスタム URL を 1 つだけインスタンス URL にすることができます。 カスタム URL に対してこの設定を有効にするには、URL レコードの [インスタンス **URL** として設定] をクリックします。以前のカスタム URL はすべて削除されます。
ステータス	カスタム URL レコードのステータス。ステータスが [アクティブ] の場合、カスタム URL は

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	プロビジョニングされ、使用する準備ができています。
Service Portal	カスタム URL を使用してユーザーをインスタンスにリダイレクトするときに使用するサービスポータル
ID プロバイダー	カスタム URL の ID プロバイダーでは、カスタム URL レコードで定義された指定の IdP にユーザーが自動でリダイレクトできるようにすることが可能です。

カスタム URL は、インスタンスで 6 時間以内にアクティブ化する必要があります。バックグラウンドジョブは、30 分ごとにカスタム URL ジョブの完了をポーリングします。

注:

- 最初に ServiceNow インスタンスからカスタム URL レコードを削除してから、任意のドメインネームサーバー (DNS) エントリを DNS サーバーから削除する必要があります。
- カスタム URL レコードを ServiceNow インスタンスから削除する前に DNS エントリを DNS サーバーから削除すると、ServiceNow から対応する他のカスタム URL レコードの削除がブロックされる可能性があります。

ID プロバイダーを含むカスタム URL

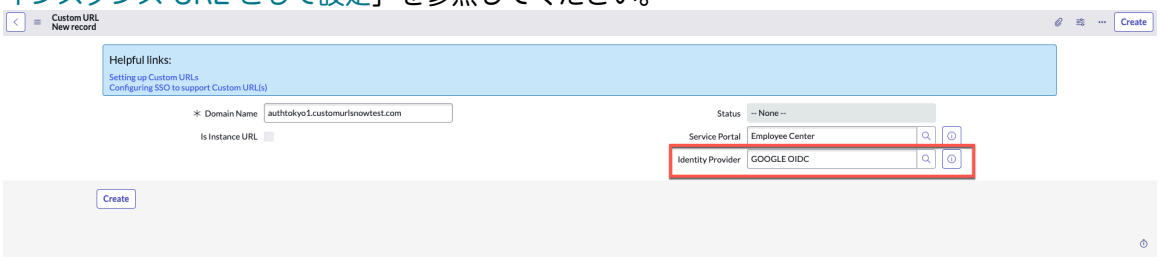
ID プロバイダーを含むカスタム URL を設定し、ユーザーが自身の IdP でログインできるようにします。

始める前に

必要なロール：管理者

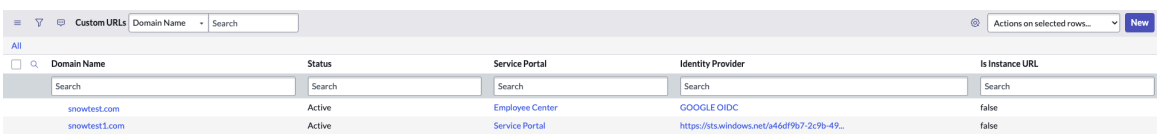
手順

1. 移動先 すべて > カスタム **URL** > カスタム **URL**.
2. [新規] をクリックします。
3. **[ID** プロバイダー] フィールドに IdP の詳細を入力します。
   その他のフィールドの詳細については、「カスタム URL をインスタンス URL として設定」を参照してください。



4. [作成] をクリックします。

   レコードが作成され、[カスタム URL] ページに表示されます。



自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ユーザーがカスタム URL にアクセスすると、設定されている ID プロバイダーにリダイレクトされます。このケースでは、snowtest.com にアクセスすると、ユーザーは **Employee Center**に移動し、Google ID プロバイダーにリダイレクトされます。

注:

- [サービスポータル] フィールドが空で [ID プロバイダー] フィールドが定義されている場合、ユーザーがカスタム URL にアクセスすると、ユーザーは設定された ID プロバイダーへ直接移動されします。
- [サービスポータル] フィールドと [ID プロバイダー] フィールドがどちらも定義されている場合、サービスポータル が定義されているカスタム URL にユーザーがアクセスすると、ユーザーは設定された ID プロバイダーへ移動します。
- [サービスポータル] フィールドと [ID プロバイダー] フィールドがどちらも定義されている場合、別のポータルが定義されているカスタム URL にユーザーがアクセスすると、自動リダイレクト ID プロバイダーがインスタンス上で設定されていれば、ユーザーはそこへ移動します。

5. 資格情報を使用してアプリケーションにログインします。

カスタム **URL** データセンタージョブ情報

インスタンスに関連付けられているすべてのカスタム URL には、対応する ServiceNow データセンタージョブがあり、このジョブが実行されて、インスタンスに関連する URL 情報が表示されます (表を参照)。

ジョブフィールド	説明
ジョブ ID	カスタム URL のドメインを確認するジョブの一意の ID
前回実行日時	ジョブが実行された最新の日時
ペイロード	証明書プロビジョニングのためにデータセンターに送信されたドメインまたはカスタム URL のリスト
ポーリング数	このジョブに対して結果がポーリングされた回数
結果	ペイロードで送信された各ドメインまたはカスタム URL を検証します。
ステータス	データセンタージョブのステータス

SAML/SSO カスタム **URL** インストール用の **SP** メタデータの生成

SAML または SSO のインストールでは、カスタム URL インスタンスが生成される前に、IdP に対して生成された SP メタデータが必要です。

始める前に
必要なロール：admin
IdP には、要求を認証して転送するために、インスタンスの SP メタデータが必要です。

注:
Assertion Consumer Service URL (SP ログイン URL) の追加は、IdP (Azure、ADFS、または Okta) ごとに異なる場合があります。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

手順

1. インストールされている SSO プラグインを選択します。

オプション	説明
マルチプロバイダー SSO	移動先 マルチプロバイダー **SSO** > **ID** プロバイダー. IdP を選択し、[メタデータを生成] ボタンをクリックします。統合により、システムプロパティ設定からインスタンスの SP メタデータが自動的に生成されます。
SAML 2 SSO	移動先 **SAML 2** シングルサインオン > メタデータ. 統合により、システムプロパティ設定からインスタンスの SP メタデータが自動的に生成されます。

2. テキストボックスに SP メタデータをコピーします。

   例：

```
<EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata"
 entityID="https://yourinstance.service-now.com">
  <SPSSODescriptor AuthnRequestsSigned="false" WantAssertionsSigned="true"
 protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
  <SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
 Location="https://yourinstance.service-now.com/navpage.do" />

 <NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress</NameIDFor
mat>
  <AssertionConsumerService isDefault="true" index="0"
 Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
 Location="https://yourinstance.service-now.com/navpage.do" />
  <AssertionConsumerService index="1"
 Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
 Location="https://yourinstance.service-now.com/consumer.do"/>
 </SPSSODescriptor>
</EntityDescriptor>
```

3. インスタンス SP メタデータを IdP に提供します。
   たとえば、SSOCircle を使用すると、ユーザーは SP メタデータをオンラインで提供できます。
4. オプション: Azure でカスタム URL を設定するには：
   a. [アプリの登録] に移動します
   b. ドロップダウンメニューから [すべてのアプリ] を選択します
   c. **[ServiceNow** アプリ] を選択し、設定をクリックします
5. オプション: OAuth 認証を使用するには、外部クライアントアプリケーションの OAuth アプリケーションエンドポイント構成で、登録されたすべてのカスタム URL としてリダイレクト URL を設定します。
   リダイレクト URL は、認証サーバーがリダイレクトするコールバック URL と同義です。
6. オプション: Google reCAPTCHA サービスを使用するには、API キーペアを設定します。

カスタム **URL** のエラーと修正

カスタム URL のセットアップと構成に関する一般的なエラーと関連する修正のリストを以下に示します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

セットアップ中のエラー

エラーメッセージ	修正
カスタム URL を作成できません。(Unable to create a Custom URL.) 後でもう一度お試しください。(Try again later.)	制御範囲外の問題があり、カスタム URL を作成できない可能性があります。サポートに連絡する前に、時間をおいてから実行してみてください。 **注:** 通常、カスタム URL の作成には 30 分かかります。それ以上かかる場合は、https://support.servicenow.com/now?draw=case にお問い合わせください。
インスタンスに対する別のカスタム URL 要求がまだ処理中であるため、新しいカスタム URL 要求を送信できません。	新しい要求を送信する前に、自分のカスタム URL ジョブのステータスを確認してください。
インスタンス URL を設定する前に、プロパティ Glide Proxy、Glide Servlet をクリアする必要があります。(You must clear the following properties before the instance URL can be set: Glide Proxy, Glide Servlet.)	
<custom_domain> のプロビジョニングはまだ処理中です。(The provisioning of <custom_domain> is still in progress.) このプロセスには最大 X 時間かかる場合があります。(This process can take up to X hours.) このプロセスが完了すると、インスタンス管理者に通知が送信されます。(Your instance administrator will receive a notification when this process completes.)	カスタム URL のインスタンスでプロビジョニングが開始された後、ステータスが変更される前に、プロセスの完了を待つ必要があります。
<custom_domain> が新しいインスタンス URL として設定されました。<base.service-now.com> はサービス中ですが、通知などに含まれる新しい URL には、すべて <custom_domain> が使用されます。(<custom_domain> is now set as the new instance URL. <base.service-now.com> is still in service, but all new URLs, such as in notifications, will use <custom_domain>.)	インスタンス URL として指定できる URL は 1 つだけです。インスタンスに関連付けられている他の URL をアクティブにすることはできますが、通知を使用できるのはインスタンス URL のみです。
カスタム URL <custom_domain> はインスタンス構成からすぐに削除され、<base.service-now.com> に戻るように設定されています。<custom_domain> は、DNS の CNAME レコードが設定されているかぎり、このインスタンスに関連したままになります。(The Custom URL <custom_domain> is set to be immediately removed from the instance configuration and revert back to <base.service-now.com>. <custom_domain> continues an association to this instance as	このメッセージは、カスタム URL を変更する意図があることを確認します。この確認を受け入れることで、インスタンスへの URL の変更を開始します。[ドメイン名] リストにある URL はいずれもカスタム URL としてアクティブにすることができますが、プロバイダーの CNAME レコードから削除した場合は例外です。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

エラーメッセージ	修正
long as the CNAME record in your DNS is set.)	
glide.servlet.uri を変更することはできません。(You cannot modify glide.servlet.uri.) このプロパティはカスタム URL によって設定されます。	
glide.proxy.host を変更することはできません。(You cannot modify glide.proxy.host.) このプロパティはカスタム URL によって設定されます。	
<custom_domain> の CNAME レコードは <base.service-now.com> をポイントしません。(The CNAME record for <custom_domain> does not point to <base.service-now.com>.)	URL プロバイダー側の構成が正しくありません。CNAME レコードの設定を確認してください。
<custom_domain> の CNAME レコードがありません。(Missing CNAME record for <custom_domain>.)	インスタンスにカスタム URL を設定する前に、URL プロバイダーから CNAME レコードを設定する必要があります。

LDAP 統合

LDAP 統合により、インスタンスで既存の LDAP サーバーをユーザーデータのプライマリソースとして使用できます。

管理者は、ライトウェイトディレクトリアクセスプロトコル (LDAP) ディレクトリと統合して、ユーザーログインプロセスを簡素化し、ユーザーの作成やユーザーへのロールの割り当てなどの管理タスクを自動化します。LDAP 統合により、システムは既存の LDAP サーバーをユーザーデータのプライマリソースとして使用できます。通常、LDAP 統合も Single Sign-on 実装の一部です。

統合では、LDAP サービスアカウントの資格情報を使用して、LDAP サーバーからユーザーの識別名 (DN) を取得します。ユーザーの DN 値を指定すると、統合はユーザーの DN とパスワードを使用して LDAP に再バインドします。ユーザーが入力するパスワードは、HTTPS セッションに完全に含まれています。統合では LDAP パスワードは保存されません。

統合は、LDAP ディレクトリに書き込むことのない読み取り専用接続を使用します。統合は情報をクエリするだけで、それに応じて内部データベースを更新します。

注:
統合の設定の詳細については、「LDAP 統合のセットアップ」を参照してください。

注:
インスタンスが LDAP 統合を使用していて、Active Directory 設定でユーザーがログイン時にパスワードをリセットする必要がある場合、ユーザーはインスタンスにログインできません。インスタンスは、ユーザーの Active Directory のパスワードを変更できません。

LDAP 統合の機能

LDAP 統合機能は次のとおりです。

スケジュールされた LDAP リフレッシュ

LDAP サーバーのスケジュール設定済みスキャンは通常、夜間に 1 回実行されます。該当するすべてのユーザーレコードの属性を照会し、それらをサーバー上のアカウントと比較します。差異がある場合は、変更された属性を使用してユーザーレコードを変更

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

します。リフレッシュ中に LDAP サーバーにかかる負荷は、照会されるレコードの数と比較される属性の数によって異なります。ピーク時間外にリフレッシュをスケジュールすることをお勧めします。大規模なリフレッシュ操作は、レポートの実行などの他のスケジュールされた操作に影響を与える可能性があるため、競合を最小限に抑えるように計画する必要があります。

LDAP リスナー

LDAP リスナーは永続クエリ (または永続検索) のバージョンです。LDAP サーバーに加えられた変更に対して継続的なクエリを発行し、常に応答をリッスンします。サーバーが永続検索をサポートしていると仮定すると、該当する LDAP アカウントに加えられた変更はすべて LDAP リスナーに返され、約 10 秒以内にインスタンスに送信されます。これは非常に便利なツールであり、次にスケジュールされたリフレッシュを待たずに、ユーザーのアカウントの詳細をほぼリアルタイムでコピーできます。

オンデマンド LDAP ログイン

LDAP 統合が確立されると、インスタンスのアカウントがまだない場合でも、新しいユーザーがシステムにログインできるようになります。新しいユーザーがインスタンスにログインしようとすると、統合はこのユーザーがインスタンスにアカウントを持っているかどうかを確認します。統合で既存のユーザーアカウントが見つからない場合は、入力されたユーザー名が LDAP サーバーに自動的に照会されます。一致する LDAP アカウントが見つかった場合、統合はユーザーが入力したパスワードを使用して認証を試行します。パスワードが有効な場合、インスタンスはユーザーのアカウントを作成し、該当するすべての LDAP 情報をアカウントに指定して、ユーザーをインスタンスにログインさせます。

オンデマンドログインでは、LDAP ユーザーインポート変換マップを使用します。変換マップの要件の詳細については、「LDAP 変換マップ」を参照してください。

LDAP データの入力

> **注:**
> この統合で説明されている機能は、デフォルトでは利用できません。この統合では、経験豊富な管理者または ServiceNow プロフェッショナルサービスコンサルタントによって実行される展開後のカスタマイズが含まれます。

LDAP サーバーとの統合により、既存の LDAP データベースのユーザーレコードをインスタンスのデータベースに迅速かつ簡単に入力できます。データの不整合を防ぐために、着信 LDAP レコードを作成、無視、またはスキップすることができます。

LDAP 属性を指定して統合がインポートするデータを制限し、インスタンスに公開するデータのみをインポートすることもできます。通常、指定する LDAP 属性は統合変換マップの一部になります。LDAP 属性を指定しない場合、統合は LDAP サーバーから利用可能なすべてのオブジェクト属性をインポートします。インスタンスは、インポートされた LDAP データを一時インポートセットテーブルに格納するため、インポートする属性が多いほど、インポート時間が長くなります。詳細については、「LDAP 属性の指定」を参照してください。

LDAP Authentication

LDAP Authentication を使用するには、LDAP 資格情報を使用してアクセスします。

ユーザーがログインページでネットワーク資格情報を入力すると、次のようになります。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

1. インスタンスは、資格情報を LDAP サーバーに渡してインスタンスを検索します。
2. RDN を使用して、ユーザーの DN 文字列を検証します。table=sys_user の LDAP OU 構成の少なくとも 1 つに RDN が構成されている場合にのみ検証されます。
3. LDAP サーバーは、システムがアクセスを許可するかどうかを判断するために使用する、許可または許可されていないメッセージで応答します。

LDAP サーバーに対して認証することで、ユーザーはネットワークドメイン上の他の内部リソースに使用するものと同じ資格情報を使用してプラットフォームにアクセスします。また、既存のパスワードとセキュリティポリシーを再利用することもできます。たとえば、LDAP サーバーには既にアカウントロックアウトとパスワードの有効期限ポリシーが設定されている場合があります。

LDAP を有効にすると、次のフィールドでユーザーレコードが更新されます。

LDAP ユーザーレコードの更新

フィールド	説明
ソース	LDAP を使用してユーザーを検証するかどうかを示します。ソースが ldap で始まる場合、ユーザーは LDAP を介して検証されます。ソースが ldap で始まらない場合、ユーザーレコードのパスワードは、ログイン時にユーザーを検証するために使用されます。
LDAP サーバー	複数の LDAP サーバーがある場合に、ユーザーを認証する LDAP サーバーを識別します。

注:
システムは、MID Server を介した LDAP パスワード認証をサポートしていません。インスタンスは、パスワード認証をサポートするために LDAP サーバーに直接接続できる必要があります。

自動翻訳

LDAP 統合について

LDAP 統合により、インスタンスで既存の LDAP サーバーをユーザーデータのプライマリソースとして使用できます。

LDAP 統合の前提条件

- ディレクトリサービスサーバーは LDAP v3 に準拠している必要がある
- ファイアウォール経由の受信ネットワークアクセスを (LDAP サーバーに対して) 許可する必要がある
- LDAP サーバーの外部 IP または名前
- 読み取り専用アクセス権を持つユーザー資格情報
- LDAPS の場合は PKI 証明書

LDAP 統合のタイミング

LDAP 統合は通常、インスタンスの本番稼働前に行われますが、いつでも統合できます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

LDAP サーバーのデータ整合性

一部のユーザーは、第三者 (この場合はインスタンス) が LDAP サーバーを変更 (書き込み) することを懸念しています。LDAP 統合では、インスタンスは内部 LDAP ディレクトリに書き込みません。インスタンスは情報を照会し、それに応じてデータベースを更新します。

インスタンスによって内部 LDAP サーバーが変更されることはありません。サービスアカウントは読み取り専用です。

LDAP サーバーへのほとんどの変更 (追加を含む) は、完全な LDAP 統合のコンポーネントの数に応じて、数秒でインスタンスで利用可能になります。

LDAP レコードの同期を維持するには、LDAP サーバーの定期的なスキャンをスケジュールして変更を取得します。

インスタンスは部門レコードを同期しません。ユーザーとグループのメンバーシップは、LDAP リスナーメカニズムと日次の完全な LDAP ブラウザーによって最新の状態に維持されますが、LDAP から消えたこれらのエントリは削除されません。

エントリを削除すると、履歴全体も削除され、そのエントリへの参照がクリアされるか削除されます。構成アイテム (CI)、 SLA 契約、ソフトウェアライセンス、発注書、および Service Catalog エントリにはすべて部門への参照があり、部門が削除されると、それらの参照はクリアされます。ユーザーへの参照が多数あるため、ユーザーを削除すると、そのユーザーが行ったすべての履歴が失われます。現在、削除するかどうかはお客様が決定します。

セキュリティ

接続は、ファイアウォール上の特定のポートを介して、固定 IP アドレスを使用して単一のマシンから行われます。認証は、選択した読み取り専用の LDAP アカウントで行われます。標準 LDAP を使用するか、ディレクトリにインストールされている SSL 証明書の公開側をロードできます。その場合は、LDAPS を使用できます。別のセキュリティレイヤーを追加するために、ポイントツーポイント IPSEC VPN トンネルのオプションも提供しています。詳細と価格については、アカウントマネージャーにお問い合わせください。

セキュア **LDAP** 接続

接続	説明
MID Server	LDAP サーバーを外部ネットワークトラフィックから保護するには、ローカルネットワークに MID Server をインストールし、安全なチャネルを介して MID Server と通信するようにシステムを設定します。
LDAPS	暗号化された LDAPS 接続を確立するには、LDAP サーバーの SSL 証明書の公開側をロードします。統合では、証明書を使用して LDAP サーバーとインスタンス間のすべての通信を暗号化します。
VPN	暗号化されたポイントツーポイント IPSEC VPN トンネルを使用して LDAP サーバーを保護するには、詳細と価格についてアカウントマネージャーにお問い合わせください。

考慮すべきもう 1 つのセキュリティ面は、LDAP 統合で共有されるデータです。インスタンスに公開されるデータを制限するには、変換マップで属性を指定します。詳細については、「LDAP 変換マップ」を参照してください。

LDAP データのインスタンスへのインポート

必要なデータのみをインポートするように属性を定義することをお勧めします。定義された属性がインスタンスユーザーデータベースにマッピングされます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

どの属性が必要かは、プロジェクトのスコープとビジネス要件によって決まるため、回答できません。

サポートされている LDAP サーバーのタイプ

インスタンスは、Microsoft Active Directory、Novell、Domino (Louis Notes)、および Open LDAP と正常に統合されています。LDAP サーバーとのインターフェイスには JNDI を使用します。LDAP サーバーが LDAP v3 に準拠している限り、統合は成功します。

LDAP Single-sign-on

LDAP インポートで提供されるデータ入力機能に加えて、アプリケーションでサポートされている外部認証機能を使用して、ユーザーが毎回サインオンする必要がないようにすることができます。

複数の LDAP ドメイン

複数のドメインを処理する場合は、ドメインごとに個別の LDAP サーバーレコードを作成することをお勧めします。各 LDAP サーバーレコードは、そのドメインのドメインコントローラーを指す必要があります。これは、ローカルネットワークが各ドメインコントローラーへの接続を許可する必要があることを意味します。

複数のネットワークドメインに展開した後、アプリケーションユーザー名の一意の LDAP 属性を特定し、結合値をインポートすることが重要です。Active Directory の一般的な一意の結合属性は objectSid です。一意のユーザー名は、LDAP データ設計によって異なる場合があります。一般的な属性は email または userPrincipalName です。

クエリ制限の処理

デフォルトでは、Active Directory 2000/2003 には、過度の負荷とサービス拒否攻撃を防ぐために、1000 オブジェクトの LDAP クエリ制限 (maxPageSize) があります。この制限に対処する方法は 2 つあります。

デフォルトの方法では、一度に 1000 未満のオブジェクトを返すようにクエリを分割します。たとえば、「a」で始まるオブジェクトのみをクエリしてから、「b」オブジェクトをクエリします。大規模な環境でより効率的に行う方法は、ページングを有効にすることです。ページングは、すべての Microsoft Active Directory サーバーでデフォルトでサポートされています。結果は自動的に複数の結果セットに分割されるため、クエリを複数の要求に分割する必要はありません。

LDAP クエリタイプ。

LDAP パスワードが指定されている場合は、「簡易バインド」が実行されます。LDAP パスワードが指定されていない場合は「none」が使用されます。この場合、LDAP サーバーは匿名ログインを許可する必要があります。

LDAP Authentication

提供された LDAP のサービスアカウント資格情報を使用して、LDAP サーバーからユーザー DN を取得します。ユーザーの DN 値を指定して、ユーザーの DN とパスワードを指定して LDAP に再バインドします。

パスワードストレージ

ユーザーが入力するパスワードはすべて HTTPS セッションに含まれます。そのパスワードはどこにも保存されません。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

LDAP Authentication の設定

ユーザーレコードの次のフィールドは LDAP に関連しています。

- ソース：[ソース] フィールドは、ユーザーが LDAP を使用して検証されているかどうかを示します。[ソース] フィールドが「ldap」で始まる場合、ユーザーは LDAP を介して検証されます。[ソース] フィールドが「ldap」で始まっていない場合、ユーザーレコードのパスワードを使用してログイン時にユーザーが検証されます。
- **LDAP** サーバー：インスタンスは複数の LDAP サーバーをサポートしているため、[LDAP サーバー] フィールドによってユーザーの認証に使用するサーバーが決まります。

LDAP 統合要件

PKI 証明書、LDAP 準拠のディレクトリサービスサーバーを含む、LDAP 統合の要件を確認します。

LDAP 統合には以下が必要です。

- LDAP v3 準拠のディレクトリサービスサーバー
  - ファイアウォール経由の (LDAP サーバーへの) 受信ネットワークアクセスを許可
  - (オプション) 匿名ログインを承認
  - (オプション) 大規模な LDAP クエリのページングをサポート
- LDAP サーバーの外部 IP アドレスまたは完全修飾ドメイン名。MID Server を使用することもできます。
- 選択した読み取り専用の LDAP アカウント
- 複数のドメインの場合、各ドメインコントローラのネットワークアクセス
- LDAPS の場合は PKI 証明書
- LDAP リスナーの場合は、永続クエリ (ADNotify) をサポートする Microsoft Active Directory サーバー

サポート対象 LDAP サーバー

JNDI を使用して LDAP サーバーと連携することで、インスタンスは次のサーバーと正常に統合されています。

- Microsoft Active Directory
- Novell
- Domino (Locus Notes)
- LDAP を開く

LDAP クエリの制限

デフォルトでは、Active Directory 2000/2003 には、過度の負荷とサービス拒否攻撃を防ぐために、1000 オブジェクトの LDAP クエリ制限 (maxPageSize) があります。システムには、この制限に対処する 2 つの方法があります。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- デフォルトの方法では、一度に 1000 未満のオブジェクトを返すようにクエリを分割します。たとえば、「a」で始まるオブジェクトのみをクエリしてから、「b」オブジェクトをクエリします。
- 大規模な環境でより効率的な方法は、すべての Microsoft Active Directory サーバーでデフォルトでサポートされているページングを有効にすることです。ページングでは、結果を自動的に複数の結果セットに分割するため、統合によってクエリを複数の要求に分割する必要はありません。

LDAP 統合のセットアップ

管理者は、LDAP 統合を有効にして、会社の LDAP ディレクトリからのユーザーのサインオンを許可できます。

LDAP は通常、次のいずれかの通信チャネルを使用します。

LDAP 通信チャネル

接続	説明	LDAP インポートのサポートは？	LDAP Authentication のサポートは？
MID Server 接続	デフォルトでは、ポート 80 で HTTP を介して通信します。この通信チャネルには証明書は必要ありません。MID Server とインスタンス間の接続は HTTPS (ポート 443) です。MID Server を使用して LDAP 経由でデータをインポートできますが、LDAP Authentication に MID Server を使用することはできません。「LDAP サーバーの定義」に進みます。	あり	なし
標準 LDAP 統合	デフォルトでは、ポート 389 で TCP を介して通信します。この通信チャネルには証明書は必要ありません。「LDAP サーバーの定義」に進みます。	あり	あり
SSL 暗号化 LDAP 統合 (LDAPS)	デフォルトではポート 636 で通信します。この通信チャネルには証明書が必要です。LDAP X.509 SSL 証明書をインストールする に進み、証明書を取得してアップロードしてください。	あり	あり
VPN 接続	IPSEC トンネルを介して通信します。ローカルネットワークで IPSEC トンネルを購入または作成します。「LDAP サーバーの定義」に進みます。	あり	あり

MID Server を使用する場合、MID Server はインスタンスに接続し、続いて MID Server は LDAP サーバーにも接続します。どちらの場合も、MID Server が接続を開始します。

1. まず、MID Server はポート 389 で LDAP を介して LDAP サーバーに接続します。
2. 次に、MID Server はポート 443 でインスタンスへの HTTPS 暗号化接続を開始し、データをインスタンスにプッシュします。

VPN、MID Server、および LDAP の詳細については、コミュニティの「VPN Part II は必要ありません (You Don't Need A VPN Part II)」を参照してください。

LDAP X.509 SSL 証明書をインストールする

LDAP 統合用の X.509 証明書をインストールできます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

始める前に
必要なロール：管理者

手順

1. LDAP サーバーで SSL 証明書を購入または生成します。
2. 移動先 **LDAP** > 証明書 をクリックし、「 新規」をクリックします。
3. フォームフィールドに記入します。

フィールド	説明
名前	証明書名。
有効期限通知	[期限切れ時に通知] フィールドで選択したユーザーに通知を送信するには、このオプションを選択します。デフォルトでは、これは有効になっています。
期限切れ時に通知	証明書の有効期限に関する通知を有効にするユーザーを選択します。ユーザーが選択されていない場合、ログインしているユーザーは、最後にログインした 2 人の管理者ロールとともに追加されます。
有効期限切れ前に警告	インスタンスが通知を送信する期限切れまでの日数。20 以上の値を入力してください。Istanbul 以降のリリースにアップグレードしたインスタンスでは、より大きい値を指定しない限り、この値は 20 に設定されます。
アクティブ	この証明書がアクティブであることを示すチェックボックス。
フォーマット	証明書の形式。
タイプ	証明書コンテナー。インスタンスは、トラストストア、Java キーストア、および PKCS#12 キーストアからの証明書を認識します。
有効開始日	インスタンスは、証明書の有効開始日を自動的にこのフィールドに追加します。証明書を X.509 証明書レコードに添付して、このフィールドに入力します。
有効期限	インスタンスは、証明書の有効期限をこのフィールドに自動的に追加します。証明書を X.509 証明書レコードに添付して、このフィールドに入力します。
数日中に期限切れ	有効期限までの計算された日数。
簡単な説明	証明書の説明。
発行者	インスタンスは、証明書発行者をこのフィールドに自動的に追加します。証明書を X.509 証明書レコードに添付して、このフィールドに入力します。
件名	インスタンスは、このフィールドの対象となる証明書を自動的に追加します。証明書を X.509 証明書レコードに添付して、このフィールドに入力します。
PEM 証明書	X509 証明書の値を入力します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注:
統合は現在、インスタンスと IdP 間の通信で証明書に署名しません。

4. [保存] をクリックします。

次のタスク
[ストア/証明書を検証] をクリックして、トラストストアと証明書をテストします。

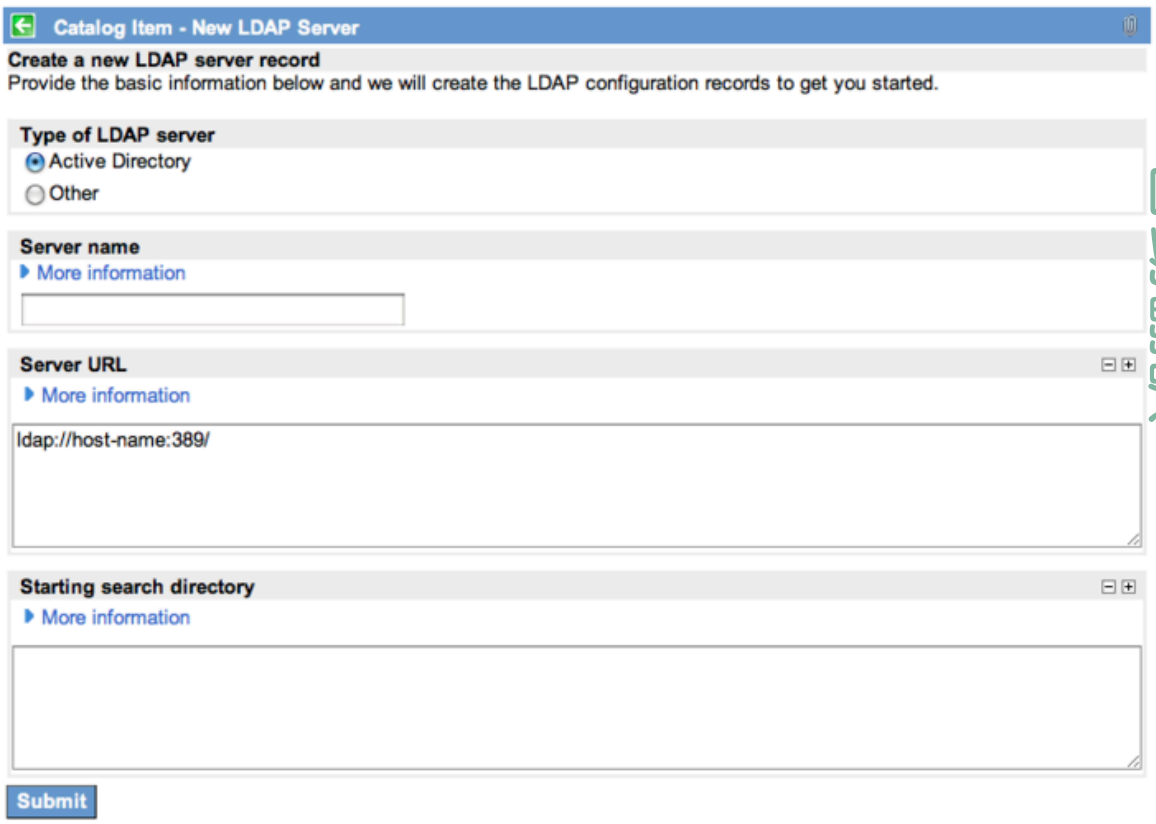
LDAP サーバーを定義する

インスタンスに新しい LDAP サーバーレコードを作成します。

始める前に
必要なロール：admin

手順

1. 移動先 すべて > システム **LDAP** > 新規サーバーを作成.
2. フォームフィールドに記入します。



[サーバー **URL]** フィールドには、すべてのサーバーの有効な URL がスペースで区切られて表示されます。サーバーは最初に運用ステータス順に並べ替えられます。[稼働中] のサーバーが最初に表示され、次に指定した [順序] の値順に並べ替えられます。リストの最初のサーバーはプライマリ LDAP サーバーです。その他は冗長サーバーです。

注:
実際の運用ステータスの変更と表示の間にはわずかな遅延があります。

または、既存の LDAP サーバーレコードに移動し、[LDAP サーバー URL] 埋め込みリストに行を挿入することで、冗長な LDAP サーバーを追加することもできます。

自動翻訳

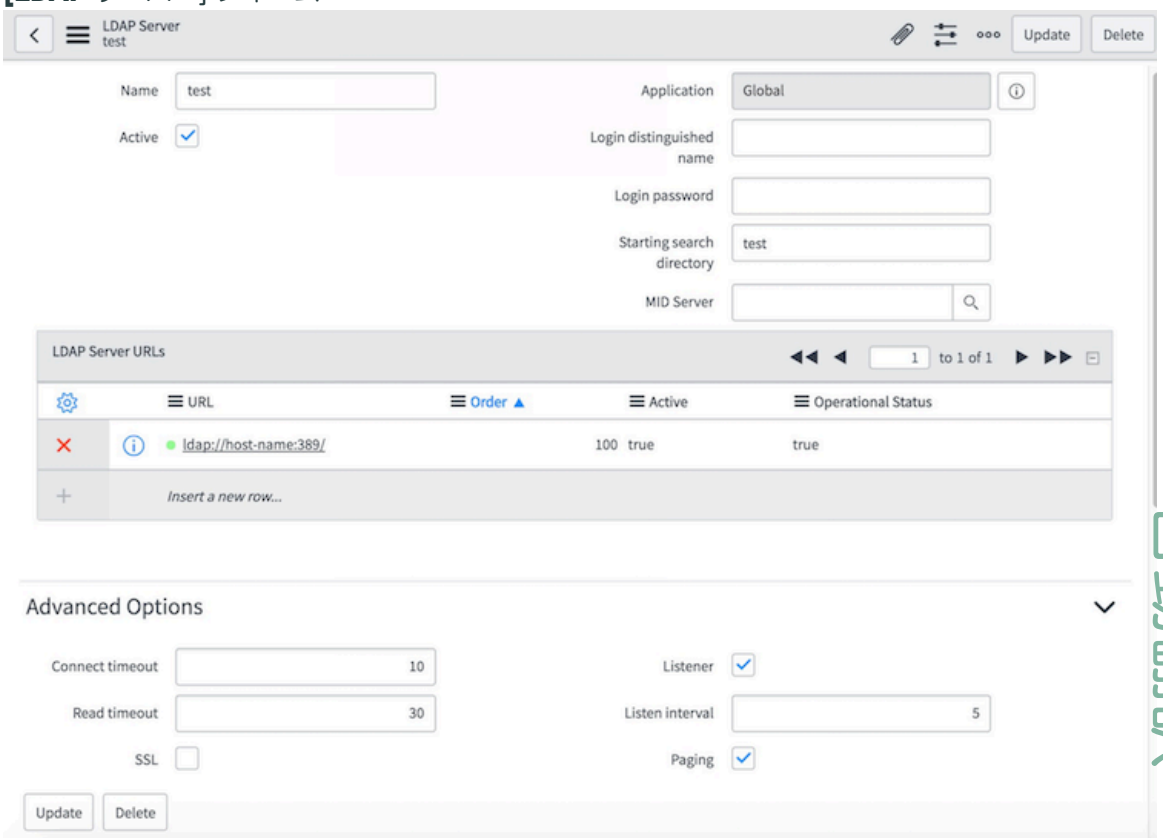
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

3. **[Submit** (送信)] をクリックします。

> **注:**
> 次の場所に移動して、既存の LDAP サーバーレコードを変更することもできます。 システム **LDAP** > **LDAP** サーバー 必要な変更を行います

4. 必要に応じてフィールドを変更します。

[LDAP サーバー] フォーム



フィールド	説明
名前	サーバーの名前を入力します。
アクティブ	サーバーがアクティブな場合は、このチェックボックスをオンにします。
LDAP サーバー URL	プライマリ LDAP サーバーとバックアップ LDAP サーバーの URL を入力します。サーバーは最初に運用ステータス順に並べ替えられます。[稼働中] のサーバーが最初に表示され、次に指定した [順序] の値順に並べ替えられます。リストの最初のサーバーはプライマリ LDAP サーバーです。その他は冗長サーバーです。
サーバー URL	サーバーの URL を入力します。必要に応じて、このフィールドを追加するフォームを設定します。これは計算された読み取り専用フィールドで、**[LDAP** サーバー **URL]** フィールドにも表示される LDAP サーバーのリストをスペースで区切って、運用ステータスと URL の順序値で表示します。
ログイン識別名	LDAP 接続を認証するユーザーの識別名 (DN) を入力します。 LDAP ディレクトリサーバーにアクセスするには、ユーザー名を完全な識別名形式 (servicenow@service-now.com) にする必要があります。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
ログインパスワード	サーバーのパスワードを入力します。
検索開始ディレクトリ	デフォルトの検索ディレクトリの相対識別名 (RDN) を入力します。この LDAP サーバーに対するすべてのクエリは、この RDN から開始されます。
MID Server	LDAP サーバーへの接続に使用する MID Server を選択します。MID Server を使用して LDAP 接続を確立すると、LDAP サーバーを外部ネットワークトラフィックに公開する必要がなくなります。また、LDAP サーバーと ServiceNow データセンター間に VPN トンネルを確立する必要がなくなります。 注: ◦ LDAP サーバー設定レコードを読み取れるようにするには、MID Server ユーザーに user_admin ロールが必要です。 ◦ 以下は MID Server では利用できません。 ▪ LDAP Authentication ▪ SSL 接続
接続タイムアウト	MID Server が設定されている場合、この設定に関係なく、接続は 10 秒後にタイムアウトします。この設定はハードコードされており、変更することはできません。
読み込みタイムアウト	統合が LDAP データを読み取るために必要な秒数を指定します。接続が読み込みタイムアウトを超えると、統合は LDAP データの読み込みを停止します。SSL 接続を有効にすると、*com.glide.ssl.read.timeout*システムプロパティを使用して読み取りタイムアウト値を設定することもできます。このフィールドとシステムプロパティの両方にタイムアウト値を入力すると、最も低いタイムアウト値が優先されます。
SSL	LDAP サーバーに SSL 暗号化接続を要求するには、このチェックボックスをオンにします。MID Server を選択した場合、このフィールドは使用できません。 LDAPS 統合を使用していて、デフォルトの SSL ポートが 636 である場合、それ以上の設定は必要ありません。SSL は自動的に有効になります。LDAPS 統合で別の SSL ポートを使用する場合は、代替 SSL 接続プロパティを定義します。 注: アプリケーションサーバーが LDAP サーバーにアクセスできるように、ネットワーク管理者がローカルファイアウォールを設定していることを確認してください。LDAP サーバーが内部ネットワーク内にある場合、ファイアウォールはアプリケーションサーバーの IP アドレスを正しいポートのファイアウォールで転送 (NAT) します。
リスナー	このチェックボックスをオンにすると、統合により、永続的な検索要求のコントロールをサポートする Microsoft Active Directory サーバーまたは LDAP サーバーを定期的にポーリングできます。さらに、MID Server を選択した場合は、その MID Server で

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	リスナー機能を使用できます。詳細については、「LDAP リスナーを有効にしてシステムプロパティを設定する」を参照してください。
リッスン間隔 (タイムアウト値)	統合がすべての接続で LDAP データをリッスンするリスナーのタイムアウト値を分単位で指定します。接続がリッスン間隔を超えると、統合は LDAP データのリッスンを停止します。
ページング	このチェックボックスをオンにすると、LDAP サーバーは LDAP 属性データを複数のクエリを送信するのではなく、複数の結果セットに分割します。

注:
LDAP パスワードを指定すると、統合によって簡易バインド操作が実行されます。LDAP パスワードを指定しない場合、LDAP サーバーは匿名ログインを許可する必要があります。そうしないと、統合は LDAP サーバーにバインドできません。

タスクの結果
LDAP サーバーレコードがアクティブに設定されている場合、システムはすべての接続を自動的にテストして検証します。
検証には以下が含まれます。

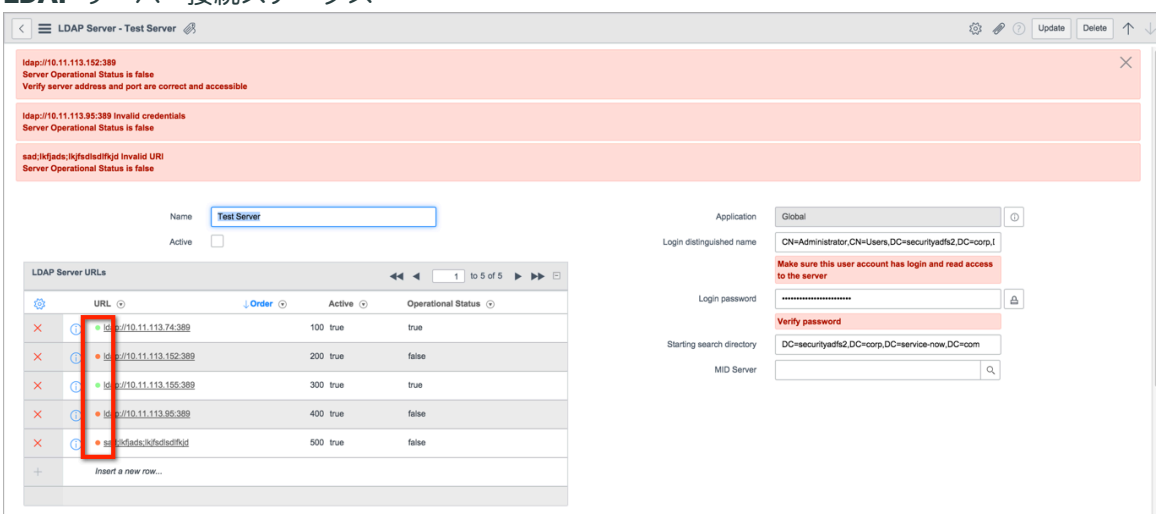
- 指定された URL とポートで LDAP サーバーにアクセスできる
- LDAP サーバーの URL が適切に形式化されている
- ログイン資格情報が有効である

Fuji リリース以降、各サーバーの URL の横に色付きのドットが表示されます。

LDAP サーバー接続アイコン

色	説明
緑	サーバーはアクティブで運用中です。
グレイ	サーバーはアクティブでも運用中でもありません。
赤	サーバーはアクティブですが、運用されていません。

LDAP サーバー接続ステータス



© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

LDAP リスナーを有効にしてシステムプロパティを設定する

リスナーの有効化はオプションです。有効にすると、LDAP サーバーで更新が行われた直後に、LDAP レコードを処理するようにリスナーがシステムに通知します。

始める前に
必要なロール：admin

このタスクについて
リスナーは、LDAP サーバー上の変更を定期的に検索する専用のプロセスです。

リスナーは、永続クエリ (ADNotify) をサポートする Microsoft Active Directory サーバー、または永続的な検索要求コントロール (OID 2.16.840.1.113730.3.4.3) をサポートする LDAP サーバーに展開できます。

LDAP サーバーが永続的な検索をサポートしている場合、LDAP リスナーは、該当する LDAP アカウントに加えられたユーザーとグループの変更を認識し、約 10 秒以内にインスタンスに転送します。これにより、インスタンスは、次にスケジュールされたリフレッシュを待たずに、ユーザーのアカウントの詳細のコピーをほぼリアルタイムで保持できます。LDAP リスナーは、ユーザー [sys_users] テーブルとグループ [sys_user_group] テーブルにマップされるオブジェクトのみを同期できます。

注:
ユーザーがリスナーを介して追加されても、そのユーザーが OU フィルターで定義されている要件を満たしていない場合、インスタンスは LDAP サーバーのレコードを無視します。条件を満たす場合、ユーザーはインスタンスに追加されます。

リスナーを有効にするには：

手順

1. 移動先 すべて > システム **LDAP** > **LDAP** サーバー.
2. 設定する LDAP サーバーを選択します。
3. [リスナー] チェックボックスをオンにします。
4. [更新] をクリックします。

   注:

   LDAP OU フィルターに一致するユーザーレコードのみがインポートされます。フィルター要件を満たさない受信ユーザーレコードは無効としてフラグが付けられ、インポートによって無視されます。管理者は、詳細な LDAP ログ記録を有効にして、受信レコードが LDAP OU フィルターに一致していないかどうかを判断できます。

5. オプション: システムのプロパティ [sys_properties] テーブルに移動し、LDAP リスナーのシステムプロパティを設定します。

   LDAP リスナーのプロパティ

プロパティ	説明
glide.ldap.listener.use_background_transaction	true の場合、LDAP リスナーはバックグラウンドトランして開始されます。LDAP リスナーをバックグラウンドンとして実行すると、最大期間 (デフォルトでは 5 分) にクォータルール LDAP リスナーの開始/停止トランザクザクションをキャンセルできます。この動作により、LD無制限に待機することを防止します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

プロパティ	説明
	注: このプロパティは、MID Server を使用しない LDAP 接続にのみ適用されます。*glide.ldap.listener.mid.use_backgrou* を使用して、MID Server を経由する LDAP 接続のロールします。 ○ タイプ：true | false ○ デフォルト値：false ○ 場所：システムプロパティ [sys_properties] テーブル
glide.ldap.listener.mid.use_background_transaction	true の場合、LDAP リスナーはバックグラウンドトランして開始されます。LDAP リスナーをバックグラウンドンとして実行すると、最大期間 (デフォルトでは 5 分) にクォータルール LDAP リスナーの開始/停止 MID トラントランザクションをキャンセルできます。この動作によりナーが無制限に待機することを防止します。 注: このプロパティは、MID Server を使用する LDAP 接続にのみ適用されます。*glide.ldap.listener.use_backg ound_t* を使用して、MID Server を経由しない LDAP 接続トロールします。 ○ タイプ：true | false ○ デフォルト値：false ○ 場所：システムプロパティ [sys_properties] テーブル
glide.ldap.listener.mid.one_listener	true の場合、MID Server を介して LDAP リスナーを開するための ECC キューメッセージが 1 つだけ作成されま場合、複数の ECC キューメッセージが作成され、LDAP始または停止する複数のスレッドが作成されます。 ○ タイプ：true | false ○ デフォルト値：true ○ 場所：システムプロパティ [sys_properties] テーブル

LDAP 属性の指定

LDAP サーバーの [属性] フィールドを使用して、LDAP サーバーのクエリに含まれる属性を指定します。これにより、パフォーマンスとセキュリティを強化できます。

始める前に
必要なロール：管理者

このタスクについて
デフォルトでは、LDAP サーバーからの読み取り権限を持つ各オブジェクトのすべての属性がロードされます。[属性] フィールドを使用して、LDAP クエリが返す属性を指定して制限することができます。大規模な LDAP インポートにこのアプローチを使用すると、インポートの速度を大幅に向上させることができます。

自動翻訳

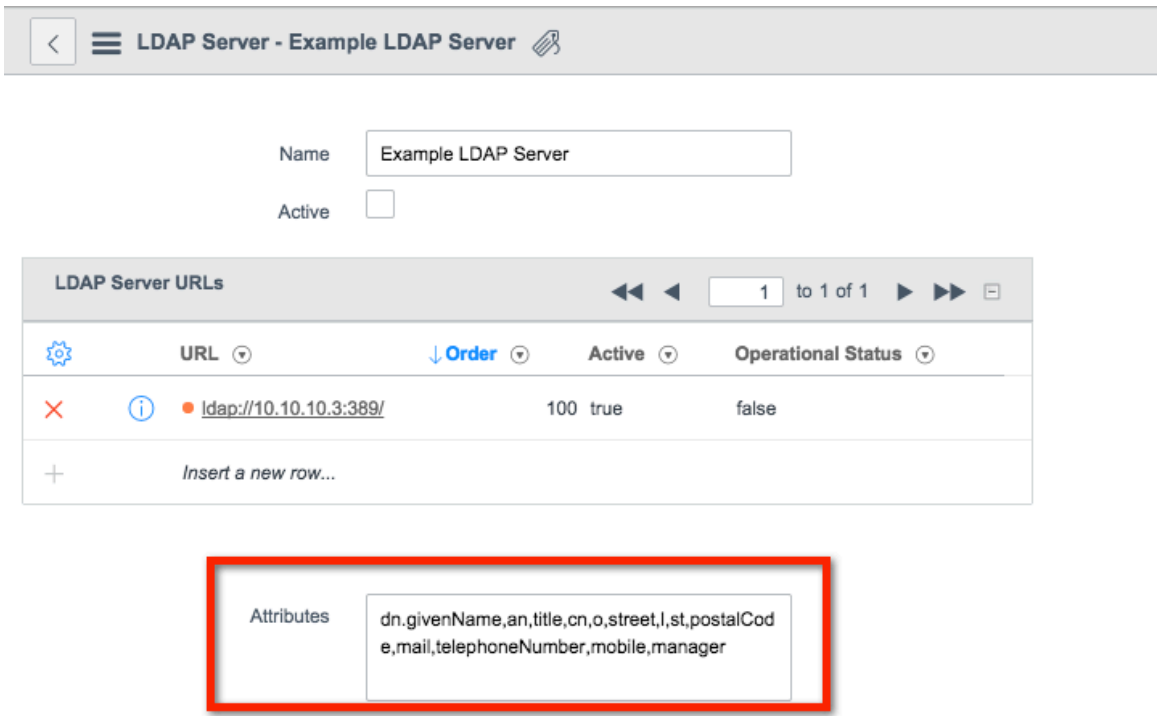
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

可能な場合は属性を明示的に定義します。

インスタンスに公開しない情報がある場合は、 属性を除外します。LDAP サーバー属性を指定しないと、新しい属性が LDAP サーバーオブジェクトに追加されたときに、新しい属性からのデータのロードがビジー状態になるため、ユーザートランザクションが長時間フリーズすることがあります。

注:
「LDAP データの変換マップの選択または作成 (Select or Create a Transform Map for LDAP Data)」で説明されているマネージャールックアップスクリプトを使用するには、[属性] フィールドで **[manager]** と **[dn]** (識別名) を指定します。どちらの属性も変換マップの一部である必要はありません。



LDAP 接続をテストする

ユーザーが [LDAP サーバー] フォームを開くたびに、インスタンスによって接続が自動的にテストされます。または、[LDAP サーバー] フォームから LDAP サーバーへの接続を手動でテストすることもできます。

始める前に
必要なロール：管理者

このタスクについて
デフォルトでは、LDAP サーバーへの接続に問題がある場合、[LDAP サーバー] フォームにエラーメッセージが表示されます。

注:
従業員は、インスタンスと LDAP サーバー間の接続を確認することもできます。LDAP 接続の確認については、テクニカルサポートにお問い合わせください。

接続を手動でテストするには：

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. 移動先 すべて > システム **LDAP** > **LDAP** サーバー.
2. テストする LDAP サーバーを選択します。
3. [関連リンク] で、[テスト接続] をクリックします。
4. [関連リンク] で [参照] をクリックし、適切な LDAP ディレクトリ構造がシステムに表示されていることを確認します。
5. (オプション) 接続に成功した場合は、[参照] をクリックして、インスタンスに表示されるソース LDAP ディレクトリ構造を表示します。

   注:
   [参照] ウィンドウの左側の [フィルター] および **[RDN]** フィールドは、右側の検索フィールドを使用すると無視されます。

タスクの結果
インスタンスは、接続テストの結果に応じて LDAP サーバーの運用ステータスを変更します。

- インスタンスが [運用ステータス] の値が [ダウン] のサーバーへの接続を確立すると、[運用ステータス] の値は自動的に [稼働中] に変更されます。この機能は、自動接続テストと手動接続テストの両方でサポートされています。
- [運用ステータス] の値が [稼働中] のサーバーへの接続を確立できない場合、[運用ステータス] の値は自動的に [ダウン] に変更されます。この機能は、手動テストではなく、自動接続テストでのみサポートされています。

LDAP 組織単位の定義

組織単位 (OU) の定義は、統合に利用可能な LDAP ソースディレクトリを指定します。

始める前に
必要なロール：admin

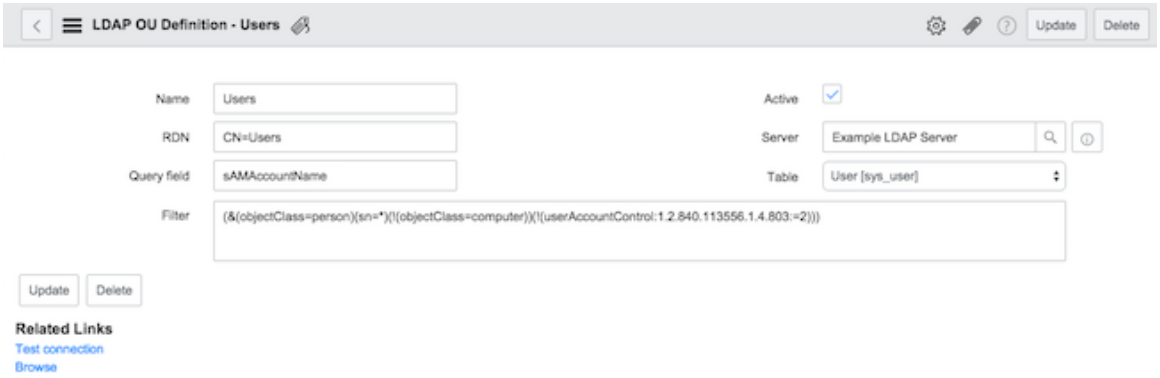
このタスクについて
OU 定義には、場所、ユーザー、またはユーザーグループを含めることができます。すべての LDAP サーバー定義には、システムへのグループのインポート用とユーザー用の 2 つのサンプル OU 定義が含まれています。

手順

1. 移動先 すべて > システム **LDAP** > **LDAP** サーバー.
2. 設定する LDAP サーバーを選択します。
3. **[LDAP OU** 定義] 関連リストで、[グループ] または [ユーザー] のいずれかのサンプル OU 定義を選択します。
4. [LDAP OU 定義] フォームに入力します (表を参照)。
5. [更新] をクリックします。
   LDAP サーバーへの接続が自動的にテストされます。
6. [関連リンク] で、[参照] をクリックして、OU 定義が返す LDAP ディレクトリレコードを表示します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



OU 定義フォーム

フィールド	説明
名前	この OU を参照するときに統合で使用する名前を指定します。ここに入力した名前は、データソースレコードの LDAP ターゲットになります。
RDN	検索するサブディレクトリーの相対識別名を指定します。この RDN は、LDAP サーバー定義の検索開始ディレクトリーと組み合わされて、この組織単位の情報を含むサブディレクトリーを識別します。たとえば、サンプル OU 定義では、RDN 値 CN = Users を使用して、LDAP ディレクトリー CN=Users,DC=service-now,DC=com およびこのポイントより下の任意のディレクトリーを検索します。このフィールドは、LDAP システムのサブディレクトリーと一致する必要があります。
クエリフィールド	レコードを照会する LDAP サーバー内の属性の名前を指定します。クエリフィールドは、単一のドメインインスタンスと複数のドメインインスタンスの両方で一意である必要があります。最良の結果を得るには、複数のドメインインスタンスでユーザーを一意に識別するメールアドレスまたはその他の資格情報を使用します。Active Directory は **sAMAccountName** 属性を使用します。他の LDAP サーバーは、**cn** 属性を使用する傾向があります。 **注:** [クエリ] フィールドは、ユーザー [sys_user] テーブルの [ユーザー **ID]** フィールドにマップする必要があります。たとえば、Active Directory ユーザーが joe.example としてログインする場合、[ユーザー**ID]** の値 **joe.example** を持つユーザーレコードと、**sAMAccountName** の値 **joe.example** を持つ LDAP レコードが必要です。
有効	OU 定義を有効にし、管理者がデータのインポートをテストできるようにするには、このチェックボックスをオンにします。ただし、統合では、有効な OU 定義からのみシステムにデータを取り込むことができます。
テーブル	LDAP サーバーからマップされたデータを受け取るテーブルを指定します。ユーザーの場合は [ユーザー **(sys_user)]** を選択し、グループの場合は [グループ **(sys_group)]** を選択します。
フィルター	LDAP フィルター文字列を入力して、OU からインポートする特定のレコードを選択します。LDAP フィルタークエリが具体的であればあるほど、クエリの効率は高くなります。 たとえば、ユーザー LDAP OU 定義では、次のフィルターを使用して、個人として分類され、**sn** 属性値を持ち、コンピューターではなく、無効としてフラグ付けされていないレコードを選択します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	(&(objectClass=person)(sn=*)(!(objectClass=computer)) (!(userAccountControl:1.2.840.113556.1.4.803:=2))) LDAP フィルター構文の説明については、インターネットで LDAP フィルター RFC を検索してください。

Example: 組織単位の定義の例

次のディレクトリ構造の LDAP サーバーがあるとします。

dc=my-domain,dc=com

- ou=Groups
  - cn=Development
  - cn=HR
  - cn=Sales
- ou=Users
  - ou=Development
  - ou=HR
  - ou=Sales

さらに、アプリケーションから人事グループと人事ユーザーを除外するとします。次の操作を実行します。

1. 検索開始ディレクトリが dc=my-domain,dc=com の LDAP サーバーレコードを作成します。
2. cn=HR を除外するフィルターで ou=Groups の OU 定義レコードを作成します。
3. ou=HR を除外するフィルターで ou=Users の OU 定義レコードを作成します。

OU 定義で追加の属性またはフィルターを指定しない場合、LDAP クエリは開始ディレクトリと RDN からサブツリー全体を返します。

これらの例では、RDN 値が ou=Groups で、フィルターがない OU 定義はすべてのグループを返します。同様に、RDN 値が ou=Users でフィルターがない OU 定義では、すべてのユーザーと子組織単位が返されます。

LDAP のデータソースを作成する

各 LDAP 組織単位 (OU) 定義には、独自のデータソースの関連リストがあります。

始める前に
必要なロール：管理者

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

このタスクについて

注:
テストロードアクションを正しく機能させるには、**[LDAP** サーバー] と **[LDAP OU** 定義] の両方を有効にする必要があります。テストロードが初めて有効になると、インポートセットフィールドの長さを決定するために最大 20 のレコードがサンプリングされます。サンプリングされたレコードに [ユーザー **ID]** フィールドの値が含まれていない場合、後続のすべてのインポートのフィールド長がデフォルトの長さの 40 に設定されます。インポートでは、インポートされたデータがインポートセットテーブルのフィールド長を超えている場合、超えた分は切り捨てられます。また、[ユーザー **ID]** フィールドは最大 40 文字に短縮されます。ロードされた 20 件のレコードは変換できず、テストのみを目的としていることに注意してください。テストレコードに [ユーザー **ID]** フィールドの値が含まれている場合、フィールド長はテストレコード内の最長のユーザー ID のフィールド長に基づいて設定されます。

新しいデータソースを作成するには：

手順

1. 移動先 すべて > システム **LDAP** > **LDAP** サーバー.
2. 設定する LDAP サーバーを選択します。
3. **[LDAP OU** 定義] 関連リストで、[グループ] や [ユーザー] などのアイテムを選択します。
4. [データソース] 関連リストで、[新規] をクリックします。
5. [データソース] フォームに入力します (表を参照)。
6. [送信] をクリックします。
7. [関連リンク] で、**[20** 件のレコードのテストロード] をクリックして、データソースが LDAP データをインポートテーブルに取り込むことができるかどうかをテストします。

[データソース] フォーム

フィールド	説明
名前	このデータソースを参照するときに統合で使用する名前を指定します。
インポートセットテーブル名	インポートされた LDAP レコードと属性が一時的に配置されるステージングテーブルの名前を入力します。インポートされた LDAP レコードを表示するには、このテーブルを確認してください。すべての LDAP データソースに同じインポートセットテーブル名を使用できます。
タイプ	インポートされたデータが LDAP データであることを示すには、**[LDAP]** を選択します。タイプ **[LDAP]** を選択すると、フォームに **[LDAP** ターゲット] フィールドが表示されます。
LDAP ターゲット	このデータソースに関連付けられた LDAP OU 定義を選択します。

LDAP ユーザーを自動でプロビジョニングする

LDAP サーバーにいるが、まだインスタンスにないユーザーは自動的にプロビジョニングされます。

始める前に
必要なロール：管理者

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

手順

システムのプロパティ [sys_properties] テーブルに次のプロパティを作成します。

LDAP プロパティ

LDAP プロパティ	説明
glide.ldap.authentication	LDAP を使用して LDAP Authentication を有効にし、ユーザーを認証します。このプロパティを **[true]** (デフォルト値) に設定します。
glide.ldap.user.autoprovision	ユーザーが LDAP に存在するが、まだインスタンスに存在しない場合、LDAP によりユーザー [sys_user] テーブルにユーザーが自動的に作成されます。このプロパティを **[true]** (デフォルト値) に設定します。

自動プロビジョニングを機能させるには、これらのプロパティを両方とも **[true]** に設定する必要があります。

MID Server を介した **LDAP** 統合

管理者は、管理、計測、検出 (MID) サーバー上で LDAP データソースを使用して統合できます。

MID Server は、Now Platform と外部アプリケーション、データソース、およびサービス間のデータの通信と移動を可能にします。MID Server のインストールの詳細については、「MID Server のインストール」を参照してください。

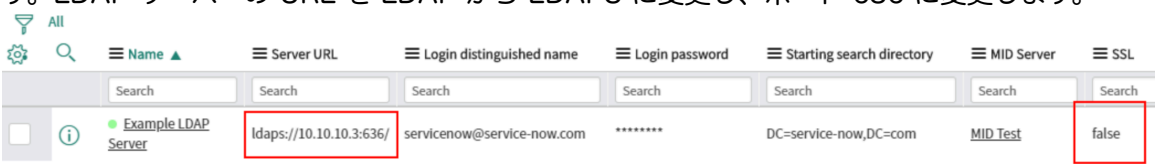
MID Server を使用して LDAP 接続を確立すると、LDAP サーバーを外部ネットワークトラフィックに公開する必要がなくなります。LDAP サーバーとデータセンター間に VPN トンネルを確立する必要がなくなります。LDAP サーバー設定レコードを読み取れるようにするには、MID Server ユーザーに user_admin ロールが必要です。

注:
MID Server では UI アクション `<インスタンス>/sys_ui_action.do?sys_id=1b4f7ef30a0001060058e223c9a5744c` を使用して、LDAP からユーザーおよびグループのレコードをリフレッシュすることはできません。

MID Server 接続は、デフォルトではポート 80 で HTTP を介して通信します。この通信チャネルには証明書は必要ありません。MID Server とインスタンス間の接続は HTTPS (ポート 443) です。インスタンスは、LDAP または LDAPS を使用して LDAP サーバーに直接接続します。この接続は、インターネット経由または VPN トンネル経由のいずれかを使用することができます。

注:
LDAP は、パスワード認証を使用して MID Server を介して通信することはできません。

SSL を介した安全な通信のために、MID Server に SSL 証明書を追加する必要があります。LDAP サーバーの URL を LDAP から LDAPS に変更し、ポート 636 に変更します。



注:
新しい LDAP サーバーを作成すると、MID Server の SSL フラグはデフォルトで [false] に設定されます。この動作は無視できます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

特定の LDAP サーバーの接続プロパティを設定するには、「LDAP サーバーを定義する」を参照してください。

LDAP 接続の監視を設定する

LDAP 接続の監視と通知を変更または無効にします。

始める前に
必要なロール：管理者

このタスクについて
LDAP サーバーの接続が失敗すると、LDAP Admins グループに設定されたユーザーにインスタンスが自動的にメールを送信します。これは、**LDAP** 接続テストのジョブスケジュールによって起動される のメール通知を使用します。このメール通知はデフォルトで有効になっています。

> **注:**
> LDAP 管理者グループに少なくとも 1 人のメンバーが存在しない限り、インスタンスはメール通知を送信しません。メールを受信するユーザーをこのグループに入力してください。

デフォルトでは、スケジュール設定済みジョブは 15 分ごとに接続をテストします。この間隔を変更するか、監視を無効にするには：

手順

1. 移動先 すべて > システム定義 > スケジュール済みジョブ.
2. **[LDAP** 接続テスト **(LDAP Connection Test)]** を開きます。
3. 次のいずれかの操作を行います。
   - [繰り返し間隔] フィールドで間隔を変更します。
   - [アクティブ] チェックボックスをオフにして、監視を無効にします。

MID Server を介してバイナリデータをインポートする

管理者は、MID Server を介して LDAP 統合によりバイナリラージオブジェクト (BLOB) データをインポートできます。

始める前に
必要なロール：管理者

このタスクについて

手順

1. バイナリデータをインポートする LDAP 列の名前をシステムプロパティ glide.ldap.binary_attributes に追加します。
2. 名前が glide.ldap.binary_attributes で、システムプロパティに設定した値と同じ MID Server プロパティを追加します。

MID Server を介して LDAP 統合をトラブルシューティングする

MID Server を介して LDAP を統合するときに、次の領域で問題が発生する可能性があります。

これらの問題のトラブルシューティングを行うには、外部通信チャネル (ECC) キュー (ディスカバリー > 出力とアーティファクト > **ECC** キュー).

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

テスト接続の問題

サーバー内で OU を定義する場合は、[テスト接続] 関連リストを使用して LDAP 接続を確認します。このリンクをクリックすると、ECC キューには、**[LDAPConnectionTesterProbe]** のトピック名を持つ単一の出力メッセージが表示されます。MID Server でテストが完了すると、ECC キューに同じトピック名の入力メッセージが表示されます。入力メッセージの [名前] 列に **[true]** が表示されている場合、テストは成功しています。レコードにドリルダウンしてペイロードを表示し、エラーメッセージが含まれていないことを確認します。

テスト接続

Created	Agent	Topic	Name	Source	Queue	State	Processed
2013-07-29 13:24:17	mid.server.local_mid	LDAPConnectionTesterProbe	true	04a952038f21010036bf21ca47e79a30	input	processed	2013-07-29 13:24:19
2013-07-29 13:24:04	mid.server.local_mid	LDAPConnectionTesterProbe		04a952038f21010036bf21ca47e79a30	output	processed	2013-07-29 13:24:17

問題を参照する

サーバー内で OU を定義する場合、OU 定義が返す LDAP ディレクトリレコードを表示するために使用される [参照] 関連リストがあります。このリンクをクリックすると、 ECC キューに **[LDAPBrowseProbe]** のトピック名を持つ単一の出力メッセージが表示されます。MID Server からデータが返された後、ECC キューに同じトピック名の入力メッセージが表示されます。入力メッセージの [名前] 列に **[true]** が表示されている場合、テストは成功しています。レコードにドリルダウンしてペイロードを表示し、エラーメッセージが含まれていないことを確認します。

インポート負荷の問題

データをアップロードするとき (たとえば、20 件のレコードのテストロード機能を使用するとき)、ECC キューには、**[LDAPProbe]** のトピック名を持つ単一の出力メッセージが表示されます。

MID Server からデータが返された後、ECC キューには **[LDAPProbeCompleted]** と呼ばれる別の入力メッセージが表示されます。この入力メッセージの [名前] 列には、返されたレコードの合計数が表示されます。

[LDAPProbe] という名前の追加の入力メッセージが表示されます。この入力メッセージの [名前] 列には、バッチ内の最大のレコード番号が表示されます。返されたレコードの合計数が 258 で、バッチサイズが 200 (デフォルト) の場合、2 つの LDAPProbe (200、258) 受信メッセージが受信され、1 つの LDAPProbeCompleted (258) 受信メッセージが受信されます。

レコードにドリルダウンしてペイロードを表示し、エラーメッセージが含まれていないことを確認します。

インポート負荷

Created	Agent	Topic	Name	Source	Queue	State	Processed
2013-07-29 13:09:48	mid.server.local_mid	LDAPProbeCompleted	11	ed0a0d7a8f32010036bf21ca47e79a56	input	processed	2013-07-29 13:09:51
2013-07-29 13:09:48	LDAPProbeResult	LDAPProbe	11	ed0a0d7a8f32010036bf21ca47e79a56	input	processed	2013-07-29 13:09:51
2013-07-29 13:09:36	mid.server.local_mid	LDAPProbe		ed0a0d7a8f32010036bf21ca47e79a56	output	processed	2013-07-29 13:09:46

[LDAPProbeError] という名前の出力メッセージにも注意してください。

エラーメッセージ

All > Created on Today > Topic = LDAPProbeError

Created	Agent	Topic	Source	Queue	State	Processed	Error string
2014-02-20 14:52:55	mid.server.localdublinmid	LDAPProbeError	MID Server reported error: java.lang.Exc...	output	error	2014-02-20 14:53:02	No message handler for this message.

[名前] 列のリンクをクリックして、エラーの詳細を表示します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

LDAP ページング

LDAP サーバーのページングサイズが 1000 未満の場合、LDAP ページングは機能しません。MID Server プロパティ *glide.ldap.max_results* を LDAP サーバーのページングサイズ以下の値に設定します。

LDAP がバイナリデータのインポートに失敗する

ユーザーの写真などのバイナリデータを LDAP 経由でインポートするには、MID Server プロパティ *glide.ldap.binary_attributes* にバイナリ属性を含める必要があります。ユーザーの写真の例では、属性は「jpegphoto」になります。

データのインポートとマッピング

LDAP インポートマップは、LDAP データベースのフィールドをインスタンスのフィールドと照合します。

注:
LDAP マッピングはパフォーマンスに影響するため、ピーク時間外にスケジュールするか、一度に処理するレコードを少数にしてシステムの可用性を維持することをお勧めします。

必要な属性または要求されている属性のみをインポートする変換マップを定義します。使用しているインスタンスのバージョンに応じて、LDAP マッピング関係を指定する方法は異なります。

LDAP 統合にシステム LDAP アプリケーションを使用するバージョンを実行しているかどうかを確認する最も簡単な方法は、アプリケーションナビゲーターからアプリケーションを見つけることです。

[ビジネスルールを実行] オプションはターゲットテーブルにのみ適用されます。ターゲットテーブルに関連付けられた変換マップのみが、さまざまなテーブルに関連付けられたビジネスルールを実行します。ユーザーグループを更新していて、ユーザーグループテーブルで実行されているビジネスルールがある場合は、そのグループにロールが定義されている必要があります。

LDAP インポートマッピングオプション

システム **LDAP** アプリケーションは？	マップ
あり	変換マップを使用してマッピングを指定します。
なし	LDAP の従来のインポートマップを使用して、マッピング、またはベースラインインスタンスに含まれるデフォルトの LDAP 変換を指定します。正しいフィールドと一致するように [結合] フィールドを忘れずに調整してください。

インポートスケジュール

管理者は、インポートスケジュールを使用して、定期的に LDAP データをインポートできます。デフォルトでは、LDAP 統合には次の 2 つのインポートスケジュールが含まれています。

- サンプル LDAP ユーザーインポート (Example LDAP User Import)
- サンプル LDAP グループインポート (Example LDAP Group Import)

どちらのサンプルもデフォルトではアクティブではありません。会社のビジネスニーズに合わせてこれらのインポートスケジュールを変更します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

LDAP 変換マップ

変換マップは、データをインポートセットテーブルからターゲットテーブル (ユーザーまたはグループ) に移動します。

LDAP 統合では、標準のインポートセットと変換マップが使用されます。カスタム LDAP 変換マップを作成することもできます。

重要:
カスタム LDAP 変換マップを選択するか作成するかにかかわらず、一連のソースおよびターゲットテーブルに対して 1 つのアクティブな変換マップが必要です。一致するフィールドに対して結合しない限り、同じソーステーブルとターゲットテーブルに対して複数の変換マップを有効にすると、ターゲットテーブルに重複するエントリが生成される可能性があります。

デフォルトの LDAP 変換マップ

デフォルトでは、LDAP データの変換マップは 2 つあります。

デフォルトの **LDAP** 変換マップ

変換マップ	ソーステーブル	ターゲットテーブル	説明
LDAP ユーザーインポート	[ldap_import]	[sys_user]	LDAP オンデマンドログインの一部として LDAP 資格情報からユーザーレコードを作成するためのデフォルトの変換マップ。Active Directory LDAP サーバーのマッピングが含まれています。
LDAP グループインポート	[ldap_group_import]	[sys_user_group]	LDAP OU からグループレコードを作成するためのデフォルトの変換マップ。Active Directory LDAP サーバーのマッピングが含まれています。

注:
デフォルトでは、LDAP 部門レコードの変換マップはありません。

カスタム LDAP 変換マップの要件

カスタム変換マップを作成する場合、変換マップは次のマッピング要件を満たす必要があります。

カスタム **LDAP** 変換マップの要件

ソーステーブル	ソースフィールド	ターゲットテーブル	ターゲットフィールド	結合	説明
ldap_import	u_source	sys_user	ソース	false	**[u_source]** フィールドは、インポートされたユーザーまたはグループの LDAP DN を識別します。システムはこのフィールドを使用して、ユーザーに LDAP Authentication が必要かどうかを判断し、

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

カスタム **LDAP** 変換マップの要件 (続く)

ソーステーブル	ソースフィールド	ターゲットテーブル	ターゲットフィールド	結合	説明
					ユーザーのマネージャーを見つけて、ユーザーをグループに入れます。
ldap_import	次のいずれかのフィールドを選択します。 • u_samaccountname • u_dn • u_cn	sys_user	user_name	true	LDAP が Active Directory に統合されている場合は、ソースフィールドとして **[u_samaccountname]** を選択します。他の LDAP ディレクトリを使用する場合は、ソースフィールドとして **[u_dn]** または **[u_cn]** を選択します。

LDAP 変換マップと従来のインポートマップの違い

変換マップを使用して LDAP マッピング関係を指定する場合、マネージャーと部門で参照フィールドの設定方法に大きな違いがあります。

変換マップを使用する場合は、変換スクリプトを使用して参照を作成する必要があります。これは、「manager」などの LDAP 属性に関連付けられた値がマネージャーの識別名 (DN) であるためです。

追加のロジックがない場合、LDAP でのユーザーの識別名であるマネージャー名でユーザーレコードが作成されます。統合には、これらの参照の作成を容易にする変換スクリプトが含まれています。デフォルトの変換マップ「LDAP ユーザーインポート」には、これらの参照の変換スクリプトが含まれています。

既存のマッピング関係

従来のインポートマップを変換マップに更新する場合、システム LDAP アプリケーションが追加される前に存在していた LDAP マッピング関係を保持できます。LDAP サーバーには、従来のインポートマップへの参照である [マップ] フィールドがあります。

> **注:**
> デフォルトでは、このフィールドは非表示になっているため、表示するようにフォームを構成する必要があります。

変換マップの使用に移行する場合は、従来のインポートマップへの参照をクリアします。

LDAP インポートマップ設定

属性を確認して使用し、統合が LDAP ソースからインポートするフィールドを制限します。さらに、user_name フィールドをユーザーのログイン ID を含む LDAP 属性にマッピングすることが重要です。Active Directory の場合、これは通常 sAMAccountName 属性です。バイナリ属性 (objectSID や objectGUID など) をインポートして結合する場合は、カスタム変換スクリプトを作成する必要があります。

> **注:**
> user_name フィールドにマッピングされた値は一意である必要があります。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

変換マップ (LDAP ユーザーインポートなど) を指定しない場合、統合では次のデフォルトマッピングが使用されます。

LDAP インポートのデフォルトマッピング

ユーザーフィールドまたは変数	**LDAP** 属性
user_name	sAMAccountName
email	mail
phone	telephoneNumber
home_phone	homePhone
mobile_phone	mobile
first_name	givenName
last_name	sn
title	title
department	department
manager	manager
middle_name	initials
u_memberof	groups
u_member	メンバー
u_manager	manager

LDAP データ変換

LDAP 属性に簡易データが含まれている場合、変換マップはインポートされた LDAP 属性をターゲットテーブル (ユーザーまたはグループ) にリンクします。たとえば、sAMAccountName 属性のサンプルデータは、ユーザーテーブルの [ユーザー **ID**] フィールドにマッピングされます。

インポートされた LDAP データが参照フィールドにマッピングされると、インスタンスは既存の一致するレコードを検索します。一致するレコードが存在しない場合、フィールドマッピングで指定されていない限り、インスタンスは参照フィールドの新しいレコードを作成します。

たとえば、ユーザーテーブルの [場所] 参照フィールドに対する LDAP 属性 l マップを想定します。インポートによって既存の場所レコード値と一致しない属性値が取り込まれるたびに、変換マップによって新しい場所レコードが作成されます。新しい場所レコードはインポートされた属性と同じ値になり、インポートされたユーザーレコードには新しい場所レコードへのリンクが含まれます。

ただし、LDAP 属性が識別名 (DN) を返す場合があります。これは、基本的に LDAP ディレクトリ内の別のレコードへの参照です。たとえば、マネージャー属性には通常、現在の LDAP ディレクトリエントリのマネージャーの識別名が含まれています。インポートされた DN は通常、 cn=Beth Anglin,ou=Users,dc=my-domain,dc=com のような長いテキスト文字列を使用します。

⚠ 警告:
ターゲットフィールドが DN を含むのに十分な長さであることを確認してください。多くのテキストフィールドでは、デフォルトの長さである 40 が使用されています。これは、一部の DN 値では長さが足りない場合があります。ServiceNow システムでは、フィールドの長さを超える値は切り捨てられます。

新しいユーザーは既存のユーザーと関連付けられていないため、管理者は通常、DN 値から新しいユーザーが作成されることを望んでいません。代わりに、管理者は、インポートでマネージャー

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

の既存のユーザーレコードを見つけて、新しくインポートされたユーザーに関連付けたいと考えています。LDAPUtils スクリプトインクルードには、DN を解析して既存のユーザーを検索できる setManager 関数と processManagers 関数が含まれています。最良の結果を得るには、これらの関数を使用してカスタム変換マップを作成します。

たとえば、LDAP User Import 変換マップスクリプトは setManager 関数を呼び出します。

```
//
// The manager coming in from LDAP is the DN value for the manager.
// The line of code below will locate the manager that matches the
// DN value and set it into the target record.  If you are not
// interested in getting the manager from LDAP then remove or
// comment out the line below
ldapUtils. setManager (source , target ) ;
```

場合によっては、統合により、関連付けられたマネージャーのユーザーレコードがインポートされる前に、ユーザーのレコードがインポートされます。このようなケースを処理するには、変換の完了後に processManagers 関数を呼び出します。たとえば、**[LDAP** ユーザーインポート] 変換マップは、onComplete 変換スクリプトを使用して processManagers 関数を呼び出します。

```
// It is possible that the manager for a user did not exist in the database when // the
 user was processed and therefore we could not locate and set the manager field. // The
 processManagers call below will find all those records for which a manager could  // not be
 found and attempt to locate the manager again. This happens at the end of the  // import and
 therefore all users should have been created and we should be able to  // locate the manager
 at this point
ldapUtils. processManagers ( ) ;
```

LDAP 統合でマネージャー属性を使用しない場合は、setManager および processManagers 関数呼び出しを削除するかコメントアウトします。

LDAP スクリプティング

データをインポートするときの要件を指定するカスタム変換マップ、スクリプト、およびビジネスルールを作成します。

カスタム変換マップには、onStart および onAfter 変換スクリプトを含める必要があります。

onStart スクリプトは LDAPUtils スクリプトインクルードを呼び出してログ記録を開始する必要があります。たとえば、**[LDAP** ユーザーインポート] 変換マップには、次のコードを使用する onStart スクリプトがあります。

```
gs.include ( "LDAPUtils" ) ; var ldapUtils  = new LDAPUtils ( ) ;
ldapUtils. setLog (log ) ;
```

onAfter スクリプトは addMembers 関数を呼び出します。例：

```
ldapUtils.addMembers (source , target ) ;
```

無効な **Active Directory** ユーザーを非アクティブに設定する

関連付けられた AD ユーザーが無効になっている場合は、次のスクリプトを使用してユーザーを自動的に非アクティブ化します。

始める前に
必要なロール：管理者

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

このタスクについて
無効な Active Directory ユーザーは、userAccountControl 属性の値を確認することで識別できます。このルールは、userAccountControl の値が変更されるたびに実行され、[ユーザーアカウント制御] が無効な AD アカウントを示している場合はユーザーアカウントを非アクティブ化します。

関連付けられた AD ユーザーが無効になっている場合は、次のスクリプトを使用してユーザーを自動的に非アクティブ化します。

手順

1. [ユーザー] フォームを設定し、[ユーザーアカウント制御] という名前の新しい整数フィールドを作成します。
2. userAccountControl (外部) のマッピングを新しいフィールドに追加します。
3. 次のプロパティを使用して、新しいビジネスルールを作成します。

AD ユーザーのビジネスルールを無効にする

[ビジネスルール] フィールド	値
名前	AD ユーザーを無効化
テーブル	ユーザー [sys_user]
時期	前
条件	current.u_user_account_control.changes()

[スクリプト] フィールドには、以下を含める必要があります。

```
var disabledFlag = 2;
//perform a bitwise comparison on userAccountControl to see if the 2 bit flag is enabled
if (current.u_user_account_control & disabledFlag) {
  gs.log('Disabling user: ' + current.user_name + 'userAccountControl=' +
 current.u_user_account_control);
  current.active='false';
  current.locked_out='true';
}
```

LDAP フィールド値の割り当て

スクリプトを使用して、フィールドマッピングがあるフィールドに値を割り当てることができます。

たとえば、[sys_user.company] フィールドに値を割り当てるには、[会社] フィールドのフィールドマップを作成し、次の変換スクリプトを追加します。

```
company = "Don's Sporting Goods";
```

特定の **LDAP** ユーザーを除外する

LDAP フィルタープロパティを使用して LDAP ユーザーリストを完全にフィルタリングできない場合は、マップスクリプトを使用してユーザーを除外できます。

インポートしないユーザーを識別するロジックを実行した後、user_name フィールドを空の文字列に設定すると、このユーザーはインポートされません。

```
user_name='';
```

除外するユーザーを識別する方法の 1 つは、DistinguusedName 属性で文字列を検索することです。たとえば、このスクリプトは、ユーザー OU にないアカウントを除外します。ユーザー OU が

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

多すぎてターゲット OU LDAP オプションに含めることができない場合は、このスクリプトを使用できます。

```
//vdn is a variable mapped to distinguishedName
gs.include("LDAPUtils");
var vdn = source.getElement(this.distinguishedName);
if (vdn.indexOf('OU=Users')<0) {
  user_name='';
  gs.log('LDAP Import Skipping User: ' + vdn);
}
```

フィルタリングのより複雑な方法は、正規表現を使用することです。

```
//vcn is a variable mapped to cn
//vdn is a variable mapped to distinguishedName
//c is the regular expression string
gs.include("LDAPUtils");
var vdn = source.getElement(this.distinguishedName);
var vcn = source.getElement(this.cn);
var c = /^[a-z][a-z][a-z][0-9][0-9][0-9]$/;
var nvcn = vcn.toLowerCase();
//test to see if the cn is in the form of 3 letters followed by 3 numbers, only import these
if (c.test(nvcn)) {
 user_name = nvcn;
} else {
 gs.log("LDAP import rejected username: " + vcn + " for DN: " + vdn);
 user_name = "";
}
```

参照フィールドのインポートの選択肢アクションを設定する

LDAP 変換マップは、インポートセットテーブルのフィールドをインシデントやユーザーなどの既存のテーブルのフィールドにマッピングする方法を決定します。

始める前に
必要なロール：管理者

このタスクについて
LDAP 変換マップがインポートセットテーブルのフィールドを更新すると、LDAP データに新しいレコードがあるたびに統合によって新しいレコードが自動的に作成されます。LDAP 変換マップが別のテーブルのデータを格納する参照フィールドを更新する場合、管理者は新しい LDAP レコードを作成するか、無視するか、または却下するかを選択できます。
たとえば、統合が既存の部門と一致しない新しい部門レコードを受信した場合、インスタンスに新しい部門レコードを作成せずに他のすべての LDAP レコードフィールドを更新できます。変換マップを使用すると、各参照フィールドのレコード作成オプションを設定できます。

手順

1. 移動先 すべて > システム **LDAP** > 変換マップ.
2. [フィールドマップ] 関連リストで、[選択肢アクション] フィールドから次のいずれかのアクションを選択します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- 作成 – 一致するレコードが存在しない場合、新しい参照フィールドレコードを作成します。
- 無視 – 参照フィールド内の新しいレコードを無視し、変換マップ内の他のすべてのフィールドの処理を完了します。
- 却下 – レコード全体の変換を停止します。

> **注:**
> フィールドマップには、参照フィールドの [選択肢アクション] フィールドのみが表示されます。

LDAP マッピングを確認する

LDAP 変換マップを作成したら、LDAP データをリフレッシュして、変換マップが想定どおりに機能することを確認します。

始める前に
必要なロール：管理者

手順

1. 移動先 すべて > システム **LDAP** > ロードスケジュール.
2. LDAP インポートジョブをクリックします。
3. [今すぐ実行する] をクリックします。

LDAP 統合をトラブルシューティングする

LDAP サーバーを統合する際に質問がある場合は、以下のアイテムが問題のトラブルシューティングに役立つ可能性があります。

予備チェック

- LDAP が利用できない場合、ユーザーはインスタンスにログインできません。LDAP が停止した場合でも管理者がインスタンスにアクセスできるように、管理者用のローカルアカウントを用意することをお勧めします。
- サービスアカウントが期限切れになっていないか、またはロックアウトされていないかを確認します。
- ユーザー名の形式を確認してください。ユーザー名のみを使用する代わりに、ユーザー名とドメイン (ユーザー名@ドメイン) を使用してみてください。
- ldap_server_config レコードの system_id エントリを変更したことを確認します。更新セットを使用して意図せず system_id を変更すると、system_id はターゲットインスタンスの間違ったノードを指し示し、機能しません。

エラーコード

LDAP ログファイルには、LDAP と Active Directory (AD) の両方の業界標準エラーコードが一覧表示されます。LDAP ログファイルはラッパーファイルに含まれています。LDAP エラーコードは 2 桁の数字ですが、Active Directory のエラーコードは 3 桁の数字です。最も一般的なエラーコードのリストについては、「LDAP エラーコード」を参照してください。

複数のドメインを統合する

同じフォレスト内または完全に信頼されていないドメイン内で複数のドメインを統合できます。ドメインごとに個別の LDAP サーバーレコードを作成することをお勧めします。各 LDAP サーバーレコードは、指定されたドメインのドメインコントローラーを指す必要があります。これは、各ドメイ

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ンコントローラーへの接続を許可する必要があることを意味します。1 つの LDAP アカウントでの LDAP による複数の AD フォレストはサポートされていません。

複数のドメインに展開する場合は、アプリケーションのユーザー名に一意の LDAP 属性を特定し、結合値をインポートすることが重要です。Active Directory の一般的な一意の結合属性は objectSid です。一意のユーザー名は、LDAP データ設計によって異なります。一般的な一意の属性は email または userPrincipalName です。

受信レコード

参照フィールドで一致する値が欠落している受信 LDAP レコードを統合で処理する方法を設定するには、「LDAP 変換マップ」を参照してください。

一般的な認証エラー

- ユーザーがログインできない (無効な DN)
- 無効な CN
- 無効な接続

自動 **LDAP** 接続テスト

LDAP サーバーへの接続を手動でテストすることも、ServiceNow で自動的に接続をテストすることもできます。

接続が自動的にテストされます。

- ユーザーが [LDAP サーバー] フォームを開くたびに行われます。
- デフォルトで 15 分ごとに実行される LDAP 接続テストのスケジュール設定済みジョブを使用します。

  このスケジュール設定済みジョブの実行頻度は変更できます。このスケジュール設定済みジョブが接続を確立できない場合、新しい 1 回限りのスケジュール設定済みジョブによって、5 分またはスケジュール設定済みジョブの [繰り返し間隔] 値の半分のいずれか早い時点で接続テストが再試行されます。

LDAP サーバーへの接続に問題がある場合は、フォームにエラーメッセージが表示されます。MID Server の背後にあるサーバーのテスト接続もサポートされています。

LDAP モニターを表示する

LDAP モニターを使用して、LDAP サーバーとリスナーに関する現在の情報を表示できます。

始める前に
必要なロール：管理者

このタスクについて
使用可能なステータスは、次のとおりです。

- アクティブ
- 非アクティブ
- エラー
- アクティブ (シャットダウン中...)
- エラー (シャットダウン中...)

現在のステータスに加えて、モニターには次の情報も表示されます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

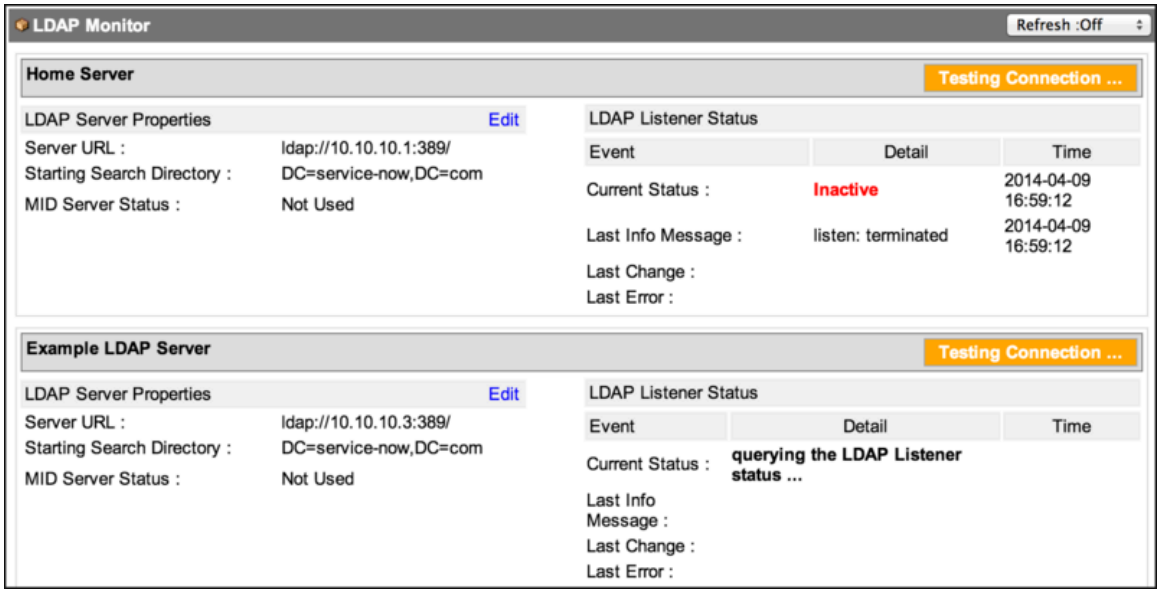
自動翻訳

- LDAP 変更の待機中、接続エラーなど、リスナーによって検出された最後のメッセージ。
- 新規ユーザー、更新されたユーザーなど、前回の LDAP ユーザーの変更。
- 発生した最後のエラー。

LDAP モニターを表示するには：

手順

移動先 すべて > **LDAP** > システム **LDAP** > **LDAP** モニター.



画面のプロパティとフィールドの説明については、表を参照してください。

LDAP モニター

フィールド	説明
リフレッシュ	リフレッシュレートを設定するには、[LDAP サーバーモニター (LDAP Server Monitor)] ヘッダーバーの [リフレッシュ] フィールドをクリックし、各データのリフレッシュ間隔を秒数で選択します。[なし] を選択してリフレッシュを抑制することもできます。
接続ステータス	サーバー接続インジケーターは、[LDAP リスナー状態] フィールド上部の右側にあります。サーバーが接続されると、ボックスが緑色になり、「接続」と表示されます。サーバーが接続されていない場合、ボックスが赤色になり、「未接続」と表示されます。サーバー接続のテスト中は、ボックスが黄色になり、「接続をテストしています」と表示されます。
LDAP サーバープロパティ	
編集	LDAP サーバーを監視するときは、[LDAP サーバーモニター (LDAP Server Monitor)] 画面で [編集] をクリックしてプロパティを変更できます。
サーバー URL	LDAP サーバーが待機しているサーバー名とサーバーポートの組み合わせ。多くの場合、ポートは次のいずれかに設定されます。 • 389：クリアテキストで LDAP に接続するためのデフォルトのポート • 636：SSL 接続を介して LDAP に接続するための標準ポート

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	値の例：ldap://10.10.10.3:389/ LDAP サーバーに複数の URL アドレスがある場合があります。これは、別の LDAP サーバーエントリを作成することによってデータをインポートできる複数のディレクトリ構造を確立するわけではありませんが、複数の LDAP サーバーがある場合は単一障害点を回避するために提供します。LDAP URL アドレスはスペース文字で区切られ、有効な接続が確立されるまで各サーバーアドレスが順番に試行されます。
検索開始ディレクトリ	システムがユーザーまたはグループの検索を開始するディレクトリまたは RDN (相対識別名)。 値の例：DC=service-now,DC=com このポイントより上のデータはインポートできません。インスタンスは、LDAP 階層内の指定されたディレクトリおよびその下のディレクトリを確認できます。
MID Server ステータス	MID Server の現在の接続ステータス。
LDAP リスナーステータス	
現在のステータス	リスナーがアクティブかどうかを示します。
最後の情報メッセージ	ユーザーとグループの変更に関連して LDAP サーバーが最後に受信したメッセージと、メッセージが受信された時間を表示します。
前回の変更	LDAP サーバーに最後に加えられた変更と、それが行われた時刻を表示します。
前回エラー	LDAP サーバーで最後に発生したエラーと、その発生時刻が表示されます。

LDAP エラーコード

LDAP ログファイルには、LDAP と Active Directory (AD) の両方の業界標準エラーコードが一覧表示されます。

標準のエラーコード

標準的な **LDAP** エラー

エラー / データコード	テキスト	説明
0	LDAP_SUCCESS	要求されたクライアント操作が正常に完了したことを示します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

標準的な **LDAP** エラー (続く)

エラーデータコード	テキスト	説明
2	LDAP_PROTOCOL_ERROR	サーバーがクライアントから無効な要求または誤った形式の要求を受信したことを示します。
3	LDAP_TIMELIMIT_EXCEDED	クライアントまたはサーバーによって指定された操作の時間制限を超えたことを示します。検索操作では、不完全な結果が返されます。
4	LDAP_SIZELIMIT_EXCEEDED	検索操作で、クライアントまたはサーバーによって指定されたサイズ制限を超えたことを示します。不完全な結果が返されます。
5	LDAP_COMPARE_FALSE	エラー状態を示すものではありません。比較操作の結果が false であることを示します。
6	LDAP_COMPARE_TRUE	エラー状態を示すものではありません。比較操作の結果が true であることを示します。
7	LDAP_AUTH_METHOD_NOT_SUPPORTED	バインド操作中に、クライアントが LDAP サーバーでサポートされていない認証方法を要求したことを示します。
8	LDAP_STRONG_AUTH_REQUIRED	次のいずれかを示します。 バインド要求で、LDAP サーバーは強力な認証のみを受け入れます。クライアント要求で、クライアントが強力な認証を必要とする削除などの操作を要求しました。切断の一方的な通知では、LDAP サーバーは、クライアントとサーバー間の通信を保護するために予期しない障害が発生したか、侵害されていることを検出します。
9		予約済み。
10	LDAP_REFERRAL	エラー状態を示すものではありません。LDAPv3 で、サーバーが要求のターゲットエントリを保持していないが、照会フィールド内のサーバーが保持している可能性があることを示します。
11	LDAP_ADMINLIMIT_EXCEEDED	管理権限によって設定された LDAP サーバーの制限を超えたことを示します。
12	LDAP_UNAVAILABLE_CRITICAL_EXTENSION	1 つ以上の重要な拡張が利用できなかったため、LDAP サーバーが要求を満たすことができなかったことを示します。サーバーがコントロールをサポートして

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

標準的な **LDAP** エラー (続く)

エラーデータコード	テキスト	説明
		いないか、コントロールが操作タイプに適していません。
13	LDAP_CONFIDENTIALITY_REQUIRED	セッションが、セッションの機密性を提供するトランスポートレイヤーセキュリティ (TLS) などのプロトコルによって保護されていないことを示します。
14	LDAP_SASL_BIND_IN_PROGRESS	エラー状態を示すのではなく、サーバーがプロセスの次のステップを実行する準備ができていることを示します。クライアントは、プロセスを続行するために同じ SASL メカニズムをサーバーに送信する必要があります。
15		使用されていません。
16	LDAP_NO_SUCH_ATTRIBUTE	変更または比較操作で指定された属性がエントリに存在しないことを示します。
17	LDAP_UNDEFINED_TYPE	変更または追加操作で指定された属性が LDAP サーバーのスキーマに存在しないことを示します。
18	LDAP_INAPPROPRIATE_MATCHING	検索フィルターで指定された一致ルールが属性の構文に定義されたルールと一致しないことを示します。
19	LDAP_CONSTRAINT_VIOLATION	DN の変更、追加、または変更操作で指定された属性値が、属性に課せられた制約に違反していることを示します。制約は、サイズまたはコンテンツ (文字列のみ、バイナリなし) のいずれかです。
20	LDAP_TYPE_OR_VALUE_EXISTS	変更または追加操作で指定された属性値がその属性の値として既に存在することを示します。
21	LDAP_INVALID_SYNTAX	追加、比較、または変更操作で指定された属性値が、属性の認識できない構文または無効な構文であることを示します。
22 ～ 31		使用されていません。
32	LDAP_NO_SUCH_OBJECT	ターゲットオブジェクトが見つからないことを示します。このコードは、検索ベースを検索するものの検索フィルターに一致するエントリを見つけられない検索操作や、バインド操作では返されません。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

標準的な **LDAP** エラー (続く)

エラー / データコード	テキスト	説明
33	LDAP_ALIAS_PROBLEM	エイリアスが逆参照されたときにエラーが発生したことを示します。
34	LDAP_INVALID_DN_SYNTAX	DN の構文が正しくないことを示します (DN 構文が正しいにもかかわらず、LDAP サーバーの構造ルールで操作が許可されていない場合、サーバーはコード 53: LDAP_UNWILLING_TO_PERFORM を返します)。
35	LDAP_IS_LEAF	指定された操作をリーフエントリで実行できないことを示します (このコードは現在 LDAP 仕様に含まれていませんが、この定数用に予約されています)。
36	LDAP_ALIAS_DEREF_PROBLEM	検索操作中に、クライアントにエイリアスオブジェクトの名前を読み込むアクセス権がないか、逆参照が許可されていないことを示します。
37 ～ 47		使用されていません。
48	LDAP_INAPPROPRIATE_AUTH	バインド操作中に、クライアントが正しく使用できない認証方法を使用しようとしていることを示します。たとえば、次のいずれかがこのエラーの原因です。強力な資格情報が必要な場合、クライアントは簡単な資格情報を返します。または、エントリにパスワードが定義されていない場合、クライアントは簡易バインドの DN とパスワードを返します。
49	LDAP_INVALID_CREDENTIALS	バインド操作中に、クライアントが誤った DN またはパスワードを渡した、またはパスワードの有効期限が切れたか、侵入者検出によってアカウントがロックされたか、あるいはその他の同様の理由によりパスワードが正しくなくなったことを示します。詳細については、データコードを参照してください。
49 / 52e	AD_INVALID CREDENTIALS	Active Directory (AD) の AcceptSecurityContext エラーを示します。これは、ユーザー名が有効であるが、パスワードとユーザー資格情報の組み合わせが無効である場合に返されま

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

標準的な **LDAP** エラー (続く)

エラー / データコード	テキスト	説明
		す。これは、LDAP エラーコード 49 に相当する AD です。
49 / 525	USER NOT FOUND	ユーザー名が無効な場合に返される Active Directory (AD) の AcceptSecurityContext データエラーを示します。
49 / 530	NOT_PERMITTED_TO_LOGON_AT_THIS_TIME	ユーザーが現時点でログオンを許可されていないために発生したログオンの失敗である、Active Directory (AD) の AcceptSecurityContext データエラーを示します。有効なユーザー名と有効なパスワードの資格情報が提示された場合にのみ返されます。
49 / 531	RESTRICTED_TO_SPECIFIC_MACHINES	ユーザーがこのコンピューターからのログオンを許可されていないために発生したログオンの失敗である、Active Directory (AD) の AcceptSecurityContext データエラーを示します。有効なユーザー名と有効なパスワードの資格情報が提示された場合にのみ返されます。
49 / 532	PASSWORD_EXPIRED	ログオンの失敗である Active Directory (AD) の AcceptSecurityContext データを示します。指定されたアカウントのパスワードの有効期限が切れています。有効なユーザー名とパスワードの資格情報が提示された場合にのみ返されます。
49 / 533	ACCOUNT_DISABLED	ログオンの失敗である Active Directory (AD) の AcceptSecurityContext データを示します。アカウントは現在無効です。有効なユーザー名とパスワードの資格情報が提示された場合にのみ返されます。
49 / 568	ERROR_TOO_MANY_CONTEXT_IDS	ログオン試行中に、ユーザーのセキュリティコンテキストで蓄積されたセキュリティ ID が多すぎることを示します。これは、LDAP 管理者が調査する必要がある特定の LDAP ユーザーオブジェクト/アカウントの問題です。
49 / 701	ACCOUNT_EXPIRED	ログオンの失敗である Active Directory (AD) の AcceptSecurityContext データを示します。ユーザーのアカウントの有効期限

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

標準的な **LDAP** エラー (続く)

エラー / データコード	テキスト	説明
		が切れています。有効なユーザー名とパスワードの資格情報が提示された場合にのみ返されます。
49 / 773	USER MUST RESET PASSWORD	Active Directory (AD) の AcceptSecurityContext データエラーを示します。最初にログオンする前に、ユーザーのパスワードを変更する必要があります。有効なユーザー名とパスワードの資格情報が提示された場合にのみ返されます。
50	LDAP_INSUFFICIENT_ACCESS	問い合わせユーザーに、要求された操作を実行するための十分な権限がないことを示します。
51	LDAP_BUSY	現時点では LDAP サーバーがビジー状態でクライアント要求を処理できないことを示しますが、クライアントが要求を待機してから再送信した場合、サーバーはそれを処理できる可能性があります。
52	LDAP_UNAVAILABLE	LDAP サーバーがクライアントのバインド要求を処理できないことを示します。通常はシャットダウン中であることが理由です。
52e	AD_INVALID CREDENTIALS	Active Directory (AD) の AcceptSecurityContext エラーを示します。これは、ユーザー名が有効であるが、パスワードとユーザー資格情報の組み合わせが無効である場合に返されます。これは、LDAP エラーコード 49: LDAP_INVALID_CREDENTIALS に相当する AD です。
53	LDAP_UNWILLING_TO_PERFORM	サーバー定義の制限のために LDAP サーバーが要求を処理できないことを示します。このエラーは、エントリの追加要求がサーバーの構造ルールに違反している、ユーザーが変更できない属性が属性の変更要求に指定されている、パスワードの制限によりアクションが実行できない、または接続制限によりアクションが実行できないという理由で返されます。
54	LDAP_LOOP_DETECT	クライアントがエイリアスまたは照会ループを検出したため、この要求を完了できないことを示します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

標準的な **LDAP** エラー (続く)

エラーデータコード	テキスト	説明
55 ～ 63		使用されていません。
64	LDAP_NAMING_VIOLATION	DN の追加または変更操作がスキーマの構造ルールに違反していることを示します。たとえば、要求はエントリをエイリアスの下に配置します。要求は、格納規則で禁止されているコンテナにエントリを配置します。エントリの RDN で禁止されている属性タイプが使用されています。
65	LDAP_OBJECT_CLASS_VIOLATION	追加、変更、または DN の変更操作がエントリのオブジェクトクラスルールに違反していることを示します。たとえば、追加または変更操作で必須属性の値なしでエントリを追加しようとする要求、追加または変更操作でクラス定義に含まれていない属性の値を使用してエントリを追加しようとする要求、変更操作で必須属性を定義する補助クラスを削除せずに必須属性を削除しようとする要求でこのエラーが返されます。
66	LDAP_NOT_ALLOWED_ON_NONLEAF	要求された操作がリーフエントリでのみ許可されることを示します。たとえば、クライアントによる親エントリでの削除操作の要求、クライアントによる親エントリでの DN の変更操作の要求でことエラーが返されます。
67	LDAP_NOT_ALLOWED_ON_RDN	変更操作で、エントリの相対識別名を形成する属性値を削除しようとしたことを示します。
68	LDAP_ALREADY_EXISTS	追加操作で既に存在するエントリを追加しようとしたか、変更操作で既に存在するエントリの名前に変更しようとしたことを示します。
69	LDAP_NO_OBJECT_CLASS_MODS	変更操作でオブジェクトクラスの構造ルールを変更しようとしたことを示します。
70	LDAP_RESULTS_TOO_LARGE	CLDAP 用に予約されています。
71	LDAP_AFFECTS_MULTIPLE_DSAS	DN の変更操作で LDAP サーバー間でエントリが移動され、複数の LDAP サーバーが必要であることを示します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

標準的な **LDAP** エラー (続く)

エラー / データコード	テキスト	説明
72 ～ 79		使用されていません。
80	LDAP_OTHER	不明なエラー状態を示します。これは、他の LDAP エラーコードにマップされない NDS エラーコードのデフォルト値です。
775	USER_ACCOUNT_LOCKED	ユーザーアカウントがロックされているため、ユーザーがログインできないことを示します。

カスタマイズ済みエラーコード

カスタマイズ済み **LDAP** エラーコード

エラー / データコード	テキスト
10000	LDAP_ERROR_GENEREL
10001	LDAP_ERROR_MAL_FORMED_URL
10002	LDAP_ERROR_UNAUTHENTICATED_BIND
10300	LDAP_ERROR_COMMUNICATION_EXCEPTION
10301	LDAP_ERROR_SOCKET_TIMEOUT
10302	LDAP_ERROR_CONNECTION_REFUSED
10303	LDAP_ERROR_CONNECTION_RESET
10304	LDAP_ERROR_NO_ROUTE
10305	LDAP_ERROR_UNKNOW_HOST
10400	LDAP_ERROR_SSL_EXCEPTION
10401	LDAP_ERROR_SSL_EMPTY_CERT_STORE
10402	LDAP_ERROR_SSL_CERT_NOT_FOUND
10403	LDAP_ERROR_SSL_CERT_EXPIRED
10500	LDAP_ERROR_INVALID_SEARCH_FILTER_EXCEPTION

LDAP サーバーのダウン時にワンタイムパスワードを送信する

LDAP プロパティは、LDAP サーバーがダウンしているためにユーザーがログインできない場合に、ワンタイムパスワードを送信するために使用できます。別のプロパティを設定して、パスワードの有効期間をコントロールすることもできます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

始める前に
必要なロール：管理者
ワンタイムパスワードを受信するには、ユーザープロファイルで通知を有効にする必要があります。通知はメールメッセージのみです。SMS メッセージはサポートされていません。

このタスクについて
どちらのプロパティもデフォルトで有効になっています。パスワードの有効性をコントロールするプロパティのデフォルト値は 10 分です。

手順

1. アプリケーションナビゲーターのフィルターに「sys_properties.list」と入力して、システムプロパティのリストを開きます。
2. *glide.ldap.onetime.password.enabled* プロパティを検索します。
3. プロパティを [true] に設定します。
4. ユーザーのパスワードの有効時間を変更するには、プロパティ *glide.authenticate.onetime.password.validity* を整数の分数に設定します。

LDAP レコードを同期する

管理者は、非アクティブ、無効、または削除された LDAP レコードを自身の LDAP レコードと同期できます。

LDAP レコードの同期は、LDAP サーバー上の非アクティブなレコードを検出し、対応する LDAP レコードを更新するプロセスです。非アクティブな LDAP レコードを検出するには、各ユーザーオブジェクトの一貫したデータインジケーターを定義し、LDAP データをインポートし、データインジケーターを評価する必要があります。

データインジケーターは次のようになります。

- [日付] フィールド
- *useraccountcontrol* 属性を使用した、特定の OU のメンバーシップ (*dn* 属性を解析して識別)
- これらのインジケーターの組み合わせ

インポートされたデータは、データを評価および処理できるインポートセットテーブルを介してインスタンスに取り込まれます。

インポートプロセスでは、複数のインポートジョブで LDAP リフレッシュフィルターを使用して、さまざまなタイプのユーザーレコードを分割し、レコードを分離して個別に処理できます。

LDAP リフレッシュフィルター

LDAP リフレッシュプロセスのフィルターを使用して、無効なユーザーの挿入を無視する処理を指定できます。

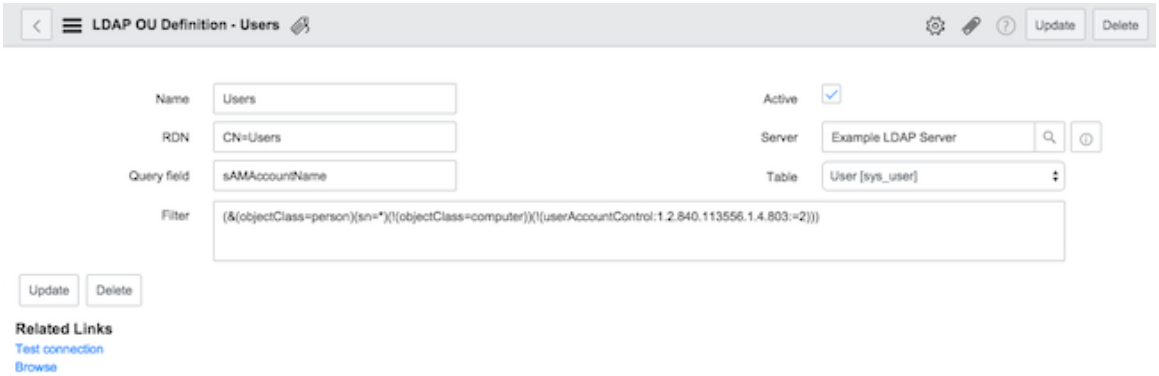
LDAP OU フィルターを緩和して、すべてのデータをインポートセットテーブル (非アクティブなユーザーを含む) に取り込み、無効なユーザーの挿入を無視する処理を指定できます。インスタンスがすぐに利用可能な LDAP サンプルで提供する、サンプルの「ユーザー」OU 定義には、フィルターが含まれています。

このフィルターは、評価対象のインポートセットテーブルに取り込まれるユーザーレコードを定義するため重要です。データのロードは小さくなりますが、このフィルターの制限により、非アクティブなユーザーが除外されるため、非アクティブなユーザーレコードはインポートセットの一時テーブルにインポートされません。非アクティブなユーザーレコードは表示されないため、レコードインジケーターを評価することはできません。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

LDAP OU フィルター



メインの LDAP リフレッシュプロセス内でフィルタリングを使用するには、すべてのユーザーレコードを取り込むようにフィルターを変更します。結果として、すべてのレコードがインポートセットの一時テーブルにロードされ、そこで評価および変換が可能になります。

注:
ここで注意が必要です。フィルタリングではすべてのレコードが取り込まれるため、インスタンスに挿入すべきではない古い非アクティブな LDAP アカウントが大量に存在する可能性があります。無効なユーザーに対してユーザーレコードを作成しないでください。

LDAP 抽出

LDAP 抽出プロセスを実装して、無効なユーザーを検出できます。

LDAP ソースからの抽出は、インポートのすべてのレコードに設定できるアクティブフラグを使用して、無効なユーザーをフィルタリングできます。('target.active=false') を指定し、テーブル変換マップレコードの [スクリプト] フィールドに直接コピーします。

利点

この方法のメリットは次のとおりです。

- スクリプティングが簡単
- 既存のユーザーレコードが処理に関与しない
- 非アクティブなユーザーが一時インポートテーブルにロードされない
- パフォーマンスへの影響がない

欠点

この方法のデメリットは次のとおりです。

- 追加のプロセスが作成される
- データソースがアクセスできる場所に抽出セットを配置する必要がある

代替方法

LDAP リフレッシュフィルターでは、複数のインポートジョブを使用して異なるタイプのユーザーレコードを分割し、レコードを分離して個別に処理します。

非アクティブな LDAP ユーザーアカウント

既存の現在のユーザーアカウントが非アクティブであるか、Active Directory (AD) LDAP から削除されていることを検出します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

LDAP 統合の一般的な問題は、Active Directory (AD) で無効化または削除されたユーザーを検出し、インスタンスでそれらを非アクティブ化する方法です。Active Directory LDAP では、通常、更新時に非アクティブなユーザーを除外するようにフィルターが設定されているため、インスタンスは AD で無効化または削除されたユーザーを認識しません。問題は、既存の現在のユーザーが非アクティブであること、または AD から削除されたことを検出する方法です。

注:
推奨されるアプローチは、ユーザーレコードと他のすべてのタイプのレコードを削除することではなく、それらを非アクティブ化にすることです。各レコードは他のレコードにリンクされており、レコードを削除すると他のレコードとの関係がすべて破棄されます。レコードを非アクティブ化すると、これらの関係は維持されます。

userAccountControl フィールドを使用した非アクティブな LDAP アカウントの検索

Active Directory (AD) ユーザーがいつ削除されるか (または非アクティブになるか) を識別します。

始める前に
必要なロール：管理者

このタスクについて
1 つの方法は、AD ユーザーのアクティブステータスを追跡し、AD アカウントが非アクティブなときに対応するアカウントを更新するビジネスルールを作成することです。

手順

1. ユーザー [sys_user] テーブルに新しい文字列フィールドを作成して、AD **[userAccountControl]** フィールドの値を追跡します。
   例：`u_ad_user_account`
2. フィールド値を設定する LDAP 変換スクリプトを作成します。

   Example

   ```
   target.u_ad_user_account = source.userAccountControl
   ```

3. LDAP フィルターを更新して、無効な AD アカウントを表示します。

   Example
   フィルターの例を次に示します。

   ```
   (&(objectClass=person)(sn=*)(!(objectClass=computer))(!
   (userAccountControl:1.2.840.113556.1.4.803:=2)))
   ```

   使用できる交換用フィルターの例を次に示します。

   ```
   (&(objectClass=person)(sn=*)(!(objectClass=computer)))
   ```

4. [u_ad_user_account] フィールドの値が 514 の場合は常に active フィールドを false に設定する onChange ビジネスルールを作成します。
   「514」は非アクティブなアカウントを示します。

LDAP スクリプトの例

次のスクリプトの例では、LDAP サーバーに Active Directory (AD) を使用していることを前提としています。

userAccountControl 属性値スクリプト
この例では、無効なユーザー (514 または 546) に関連付けられた userAccountControl 属性値をソースでテストします。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

```
//Deactivate LDAP-disabled users during transform based on 'userAccountControl' attribute
if(source.u_useraccountcontrol == '514' || source.u_useraccountcontrol == '546'){
  target.active=false;
  target.locked_out=true;
}
```

ビットごとのチェックを使用した例を次に示します。

```
if(source.u_useraccountcontrol & 2){
  active = false;
}
```

userAccountControl 属性スクリプト

この例では、userAccountControl 属性を調べますが、特定の値をテストしません。LDAP ユーザーアカウントを再有効化するオプションも含まれています。

```
/*
* Deactivate LDAP-disabled users during transform based on 'userAccountControl' attribute
* Convert the userAccountControl attribute back to a hex value
*/
var ctrl = parseInt(source.u_useraccountcontrol, 10);
ctrl = ctrl.toString(16);

/*
* The only digit we care about is the final one
* A final hex digit value of '2' in 'ctrl' means disabled
*/
if(ctrl.substr(-1) == "2"){

  //Deactivate and lock the user account
  target.active = false;
  target.locked_out = true;

  //Ignore any insert of a disabled record
  if(action == 'insert'){
    ignore = true;
  }
}
/* Optional: Uncomment else block to reactivate and unlock the user account
else {
  target.active = true;
  target.locked_out = ctrl.substr(-2, 1) == "1";
}
*/
```

onBefore 変換マップスクリプト

onBefore 変換マップスクリプトの例を次に示します。スクリプトは、無効なレコードと挿入されるレコードを識別します。無効なユーザーの挿入が発生している場合、操作の変換はレコードを無視します。

```
//Ignore any insert of a disabled record as defined by the 'userAccountControl' attribute
var uc = source.u_useraccountcontrol;
if((uc == '514' || uc == '546') && action == 'insert'){
  ignore = true;
}
```

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

DN メンバースクリプト

このスクリプトの例では、546 および 514 userAccountControl 値に依存せずに、ユーザーが特定の識別名 (DN) のメンバーであるかどうかをチェックすることで、柔軟性を導入しています。このスクリプトは、「テーブル変換マップ」レコードの [スクリプト] フィールドまたは onBefore 変換マップスクリプトで使用できます。

```
//Deactivate LDAP-disabled users during transform based on OU membership in 'dn'
if(source.u_dn.indexOf('OU=Disabled Accounts') > -1){
  target.active = false;
  target.locked_out = true;
}
```

Active Directory Application Mode (ADAM)

Active Directory Application Mode (ADAM) は、Lightweight Directory Access Protocol (LDAP) 準拠のディレクトリサービスです。

注:
このトピックを理解するには、Microsoft Windows サーバーと Active Directory の基本を理解する必要があります。ADAM 用に構成するサーバーの管理者権限も必要です。

これらはサンプル手順です。インストールと環境はさまざまであるため、直接サポートを提供することはできません。Microsoft コンサルタントに相談することをお勧めします。

ADAM は、Windows オペレーティングシステムで簡単にインストールでき、サービスとして実行されます。完全にカスタマイズしてアプリケーションコンポーネントとして配布することも、スタンドアロンの LDAP ディレクトリとして使用することもできます。ADAM は、Active Directory ドメインコントローラーと同じテクノロジー (レプリケーション機能と委任機能を含む) を使用し、独自の管理機能とカスタマイズ機能を備えています。Windows サービスとして実行できます。ADAM は、Windows XP、2000、2003、および 2008 のオペレーティングシステムにインストールできます。ADAM は、Windows Server 2003 R2 および Windows Server 2008 の一部として含まれています。以前のオペレーティングシステムについては、http://www.microsoft.com/downloads http://www.microsoft.com/downloads からダウンロードできます。

セキュリティ

会社のセキュリティポリシーによっては、外部ベンダーやパートナーが Active Directory (AD) ドメインコントローラに直接接続することが禁止されています。特定の AD オブジェクトまたは属性を外部ベンダーまたはパートナーに公開することが禁止されている場合は、AD セキュリティアクセス制御エントリ (ACE または ACL) を使用してオブジェクトおよび属性へのアクセスをブロックできます。セキュリティ要件に応じて、この方法では統合が複雑になる可能性があります。複数のドメインとフォレストを統合することをお勧めします。すべての LDAP インポートと認証を単一のソース経由で行う必要がある場合は、統合ソースとして ADAM を使用できます。Windows 2008 のリリースで、この機能は Light-Weight-Directory Service (LDS) に名前が変更されました。インストールと構成は Windows Server 2003 R2 と同様です。

推奨ナレッジ

このタスクでは、AD、オブジェクトクラス、および属性を理解する必要があります。統合を正常に行うには、現在の AD オブジェクト構造を理解し、Active Directory の委任に精通し、ADAM を使用する方法と目的について戦略を立てる必要があります。AD または ADAM に精通していない場合は、AD 管理者と協力して新しい ADAM 環境を構成してください。

信託

userProxy オブジェクトを使用する場合、ADAM をホストするコンピューターは、AD アカウントを持つドメインのメンバーであるか、信頼できるドメインのメンバーである必要があります。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

内部接続

userProxy オブジェクトを使用する場合、ADAM コンピューターは関連するドメインコントローラに接続してプロキシ認証を実行できる必要があります。

関連情報

http://www.microsoft.com/downloads/en/details.aspx?familyid=9688f8b9-1034-4ef6-a3e5-2a2a57b5c8e4&displaylang=en%7C

ADAM を使用してインスタンスを構成する

初回インストールでは、ADAM ファイルがコンピューターにコピーされ、必要なコンポーネントが登録され、アプリケーションのショートカットが作成されます。

始める前に
必要なロール：管理者

このタスクについて
デフォルトでは、アプリケーションファイルはすべて %systemroot%\ADAM にインストールされます。

- Windows Server 2003 R2 - ADAM は、 [コントロール パネル] > [プログラムの追加と削除] > [オプションのコンポーネント マネージャー].
- Windows Server 2000 および Windows XP - Microsoft から http://www.microsoft.com/downloads をダウンロードします。

ADAM によってホストされる最初のディレクトリサービスとして機能する最初のインスタンスサービスを作成します。次のいずれかの操作を行います。

手順

- ADAM フォルダーから *adaminstall.exe* を実行します。
- から **ADAM** インスタンスを作成する ショートカットを使用する [スタート] メニュー > **ADAM** > プログラム フォルダー。

1. [一意のインスタンス] インストールオプションを選択します。

   注:
   このオプションを使用して、2 番目のサーバーにインスタンスのレプリカをインストールして、フォールトトレラントなシステムを提供できます。

2. フィールドに入力します。

ADAM インスタンス

フィールド	説明
インスタンス名	主に Windows サービス名と表示名を識別するために使用します。
ポート	LDAP および LDAPS リスナーに使用するポート番号を設定します。デフォルトの LDAP ポートは 389、LDAPS は 636 です。これらのポートがサーバーで使用されている場合、セットアップウィザードは新しいポートを選択します。ネットワーク管理者と協力して、使用するのに最適なポートを決定してください

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
アプリケーションディレクトリパーティション	アプリケーションディレクトリパーティションを作成します。この段階では必要ありませんが、ここで新しいパーティションを作成することをお勧めします。フォレストまたはドメインと同じ識別名を使用することをお勧めしますが、最上位レベルのドメインを com または local ではなく adam に置き換えます。たとえば、フォレストパーティションが *dc=myCompany,dc=com* の場合、ADAM パーティションを *dc=myCompany,dc=adam* として作成します。
ファイルの場所	ADAM パーティションデータの場所を選択します。
サービスアカウントの選択	インスタンスを実行するサービスアカウントを選択します。スタンドアロンサービスの場合は、デフォルトのネットワークサービスアカウントを使用できます。レプリカを使用する場合は、すべての ADAM インスタンスにアクセスできるアカウントを使用する必要があります。
ADAM 管理者	Windows 統合認証を利用する ADAM ディレクトリの委任。管理用の初期アクセス権はこの方法で付与されます。最初のアカウントに権限が付与されると、このユーザーまたはグループは他の Windows ユーザーまたは ADAM ユーザーに権限を委任します。デフォルトを選択して、現在のユーザーにのみ管理者アクセス権を付与することも、必要に応じて別のユーザーまたはグループにアクセス権を付与することもできます。
LDIF ファイルのインポート	インポートするファイル。MS-UserProxy はインポートする最も重要なファイルですが、スキーマにほとんどオーバーヘッドがなく、後でニーズが拡大した場合に拡張する必要がないため、利用可能なすべてのファイルを追加する価値があります。詳細を確認すると、ウィザードが設定を完了します。

関連情報

http://www.microsoft.com/downloads/en/details.aspx?familyid=9688f8b9-1034-4ef6-a3e5-2a2a57b5c8e4&displaylang=en%7C

ADAM コンソールの設定

ADAM コンソールを設定します。ADAM と Active Directory の間には多くの類似点がありますが、[ユーザーとコンピューター] の管理コンソールがないため、管理は大きく異なります。

始める前に

必要なロール：管理者

このタスクについて

一般的な管理のほとんどは、**[ADAM]** スタートメニューから利用可能な ADAM ADSI MG コンソールを使用して行われます。ADAM ADSI コンソールを初めて実行するときは、作成したパーティションに接続する必要があります。

手順

1. 左フレームの **[ADAM ADSI Edit]** アイテムを右クリックします。
2. 新しい接続に名前を付け、インスタンスの作成時に使用した情報でサーバー名とポートのフィールドを更新します。
3. [識別名] または [命名コンテキスト **(naming context)]** を選択し、以前に作成したアプリケーションパーティションの識別名を指定します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

詳細設定オプションの [構成およびスキーマ *(Configuration and Schema)*] パーティションに接続できます。
これで、LostAndFound、NTDS クォータ、およびロールのパーティションとデフォルトのコンテナが表示されます。ロールコンテナがまだ構成されていません。

関連情報

http://www.microsoft.com/downloads/en/details.aspx?familyid=9688f8b9-1034-4ef6-a3e5-2a2a57b5c8e4&displaylang=en%7C

ADAM のコンテナと組織単位の作成

ADAM に格納されているオブジェクトを、Active Directory の場合と同様に、コンテナと組織単位 (OU) に論理的にグループ化します。

始める前に
必要なロール：管理者

手順

1. ルートパーティションを右クリックし、 新規 > オブジェクト > 組織単位.

   注:
   利用可能な他のオブジェクトのリストを表示することもできます。このリストは、LDF ファイルをインポートしたときにインストールされたスキーマ拡張によって異なります。

2. 値の入力を求められたら、Users などの OU の名前を入力します。
   画面に [その他の属性] ボタンが表示されます。
3. ボタンを使用して、追加の属性に値を割り当てます。
   OU とコンテナの場合、追加の値は必要ありません。
   OU を作成すると、新しい OU がルートオブジェクトの子としてリストされます。

関連情報

http://www.microsoft.com/downloads/en/details.aspx?familyid=9688f8b9-1034-4ef6-a3e5-2a2a57b5c8e4&displaylang=en%7C

ADAM を使用して委任する

OU 構造が作成されたら、限られたユーザーにオブジェクトを適切に保護するための権限委任を定義します。

Active Directory と同様に、権限を付与する一般的な方法は 2 つあります。

- 適切な権限が既に割り当てられているグループにユーザーを追加します。
- ADAM オブジェクトに対する新しい権限を定義します。

このタスクでは、オブジェクトレベルの権限について説明します。グループメンバーシップの詳細については、「グループ管理 (Group Administration)」セクションを参照してください。

ADAM 用の [ユーザーとコンピューター] コンソールがないため、オブジェクトレベルの権限はすべて Active Directory ユーティリティ *DSACLS.exe* を使用して定義されます。このファイルは ADAM プログラムディレクトリにあります。ADAM ユーティリティを実行する場合は、ADAM ツールのコマンドプロンプトを起動することをお勧めします。これにより、ツールのバージョンが適切になります。DSALCS は、オブジェクトのアクセス権を表示および設定するために使用されます。

例：「dsacls \\localhost:50010\dc=myCompany,dc=adam」は、localhost ポート 50010 で実行されているパーティション *dc=myCompany,dc=adam* のルートに割り当てられた権限を表示しま

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

す。DSACLS は、複雑な委任を作成するために使用される複雑なツールです。使用上の注意については「DSACLS /?」を実行します。

関連情報

ADAM のコンテナと組織単位の作成

ADAMSync を使用して ADAM に入力する

http://www.microsoft.com/downloads/en/details.aspx?familyid=9688f8b9-1034-4ef6-a3e5-2a2a57b5c8e4&displaylang=en%7C

ADAM オブジェクトを設定する

ADAM オブジェクトには、ユーザーオブジェクト、UserProxy オブジェクト、およびグループオブジェクトが含まれます。

ユーザーオブジェクト

ユーザーは、OU の作成と同様に ADAM ADSI Edit コンソールを使用して作成できます。AD コマンドラインツールを使用してユーザーを管理することもできますが、これについてはこのドキュメントでは説明しません。新しいユーザーオブジェクトに必須の属性は *cn* のみです。これはユーザーの短い名前またはフルネームです。Active Directory ユーザー属性と同様の幅広いオプション属性もあります。ユーザーオブジェクトからプロパティを選択することで、属性の完全なリストにアクセスできます。

UserProxy オブジェクト

ServiceNow LDAP 統合では、関連する AD ユーザーアカウントにリンクするプロキシアカウントを作成する ADAM の *UserProxy* オブジェクトを使用することをお勧めします。これにより、ServiceNow がドメインコントローラに直接接続しなくても、ドメインの AD ユーザー名とパスワードを使用して ADAM でログオン資格情報を認証できます。*UserProxy* オブジェクトは、パスワードを格納せず、リンクされた AD ユーザーオブジェクトの SID を含む *objectSID* 属性を持つ点を除いて、AD および ADAM ユーザーオブジェクトとよく似ています。プロキシは以上のように動作します。*UserProxy* オブジェクトは *ADSIEdit* コンソールまたはコマンドラインツールを使用して作成されますが、この作業には手間がかかります。以下で定義されている自動化プロセスを使用することをお勧めします。

グループオブジェクト

グループは、ADSIEdit コンソールと AD コマンドラインツールを使用して作成されます。グループの概念は AD に似ており、グループとメンバーを ServiceNow に統合するために使用されます。最大の違いは、ADAM グループには ADAM または信頼できる AD ドメインのメンバーを含めることができるということです。

ADAM オブジェクトの作成を自動化する

Active Directory アカウントを ADAM に同期する場合は、 Microsoft アダムシンク 移動します これは、ServiceNow LDAP 統合のための ADAM の最も一般的な使用法です。

権限の委任について

ADAM には、デフォルトの権限を持つビルトイングループがいくつか含まれています。これらのグループは、*cn=roles,dc=myCompany,dc=adam* コンテナにあります。これらはドメインレベルグループに似ており、現在のパーティション内のオブジェクトに対する権限があります。AD フォレストと同様に、*cn=roles,cn=configuration,dc=myCompany,dc=adam* のデフォルトグループを使用して、より高いレベルの権限を設定することもできます。*ADSIEdit* の構成パーティションに接続する必要があります。デフォルトでは、管理者グループにはセットアップ中に指定されたアカウントが含まれています。このメンバーは構成グループを介して継承されるため、常に表示されるわけで

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

はありません。管理者は、すべてのパーティションオブジェクトを完全に制御できます。デフォルトでは、リーダーグループにはメンバーが含まれておらず、パーティション内のすべてのオブジェクトに対する読み取りアクセス権があります。ユーザーグループは、Active Directory と同様に動的なグループです。推移的には、パーティションに作成されたすべての ADAM ユーザーが含まれます。

関連情報

http://www.microsoft.com/downloads/en/details.aspx?familyid=9688f8b9-1034-4ef6-a3e5-2a2a57b5c8e4&displaylang=en%7C

ADAM セットアップをテストしてトラブルシューティングする

テストに使用される主要なツールは LDP です。これにより、ユーザー認証を完全にテストできます。

オブジェクトと属性のコレクション全体へのアクセスを提供する ADAM ADSI Edit コンソールを使用して、オブジェクト管理のほとんどを実行できます。ADAM サービスの最高レベルの制御とトラブルシューティングでは、インスタンスのセットアップ中に作成された Windows サービスを使用します。サービス名は作成されたインスタンスの名前によって異なります。ADAM サービスを実行するには、このサービスが実行されている必要があります。接続の問題が発生している場合は、ネットワーク構成を確認して、サーバーと ADAM ポートに接続するための適切なネットワークアクセス権があることを確認する必要があります。インストールされている ADAM インスタンスごとに、Windows イベントログが作成されます。これは、ADAM サービスのトラブルシューティングにも最適なツールです。

Windows セキュリティイベントログは、*userProxy* 認証のトラブルシューティングにも役立ちます。すべての *userProxy* ログオン試行はセキュリティログに記録され、リモートクライアントデバイスのアドレス、ログオンしようとしているユーザーの識別名、および結果またはステータスコードを参照します。

関連情報

http://www.microsoft.com/downloads/en/details.aspx?familyid=9688f8b9-1034-4ef6-a3e5-2a2a57b5c8e4&displaylang=en%7C

ADAM でバックアップして復旧する

すべての ADAM データは、標準のファイルシステムバックアップ方法を使用してバックアップできます。

冗長性

ADAM には、AD と同じテクノロジーに基づくレプリケーションユーティリティが組み込まれています。ADAM パーティションの完全な読み取りおよび書き込みレプリカは、同じまたは別のコンピューターに存在できます。このレプリカをさまざまな方法で使用して、インスタンスとのフォールトトレラントな LDAP 統合を提供できます。1 つは、両方のパーティションをファイアウォール経由でインスタンスに公開し、[LDAP プロパティサーバー (LDAP Properties server)] フィールドの両方のサーバーを定義するという方法です。

関連情報

Active Directory Application Mode (ADAM)

http://www.microsoft.com/downloads/en/details.aspx?familyid=9688f8b9-1034-4ef6-a3e5-2a2a57b5c8e4&displaylang=en%7C

ADAM で LDAPS を使用する

userProxy オブジェクト認証のデフォルト構成では、LDAPS (セキュア LDAP) 通信を強制します。LDAPS では、ネットワークトラフィックを保護するために SSL 証明書が必要です。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

この要件を削除するには、構成パーティションに接続されている *ADSIEdit* コンソールを使用して次の変更を行います。

```
Object: CN=Directory Service, CN=Windows NT, CN=Services, CN=Configuration
Attribute: msDS-Other-Setings
Value: change RequiresSecureProxyBind from 1 (enforced) to 0 (disabled)
```

新しい設定を使用するには、ADAM サービスを再起動します。

セキュアなバインドをサポートし、送信されるユーザーとパスワードの情報を暗号化するには、サーバーと LDAP クライアントに SSL 証明書をインストールする必要があります。ADAM サービスには制限付きで制御された使用法があるため、証明書のコストや認証局 (CA) インフラストラクチャを構築することなく、ニーズを満たす自己署名証明書を使用することができます。既に CA がある場合は、証明書を発行できます。ない場合は、自己署名証明書を作成します。

自己署名証明書を作成する

selfssl ユーティリティを使用するには、Internet Information Services (IIS) をインストールする必要があります。このサービスは、証明書を生成した後に削除できます。selfssl.exe ユーティリティは IIS Resource Kit から入手できます。IIS が既にインストールされている場合は、証明書の生成中に現在のサイトが影響を受けないように新しい Web サイトを作成します。selfssl は、新しい自己発行の証明書を有効な Web サイトに一時的に添付する必要があります。

selfssl はコマンドラインツールであり、次の一般的なパラメーターがあります。

selfssl パラメーターの説明

パラメーター	説明
/T	ローカルマシンの「信頼できる証明書」に証明書を追加します
/N:cn	証明書の共通名を設定します。これは、証明書を使用する Web サービスを実行しているサーバーの完全修飾ドメイン名と一致する必要があります
/K	キーサイズの強度をビット単位で設定します
/V	証明書が有効な日数
/S	証明書を添付する Web サイト ID
/P	Web サービスの IP ポート

共通名属性は、インスタンスが ADAM コンピューターに接続するために使用する外部名またはアドレスと一致する必要があります。デフォルトの Web サイト ID である 1 を使用し、selfssl コマンドで定義する必要がない場合を除き、IIS Web サイトのサイト ID を取得する必要があります。myCompany の証明書を生成するサンプルコマンドは次のとおりです。

```
selfssl /N:CN=myCompany.externaldomain.com /K:1024 /V:3650 /S:12345 /P:50001 /T
```

このステートメントは、10 年間有効な証明書を作成します。値を任意の期間に設定します。ただし、古い証明書が期限切れになる前に新しい証明書を生成してインスタンスに送信する必要があることに注意してください。証明書の有効期限をメモすることをお勧めします。

証明書が生成されたら、Web サイトから削除するか、一時サイトを作成した場合は Web サイト全体を削除できます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

関連情報

http://www.microsoft.com/downloads/en/details.aspx?familyid=9688f8b9-1034-4ef6-a3e5-2a2a57b5c8e4&displaylang=en%7C

ADAM への証明書の割り当て

セキュアなバインドをサポートし、送信されるユーザーとパスワードの情報を暗号化するには、サーバーと LDAP クライアントに SSL 証明書をインストールします。

始める前に
必要なロール：管理者

このタスクについて
ADAM サービスには制限付きで制御された使用法があるため、証明書のコストや認証局 (CA) インフラストラクチャを構築することなく、ニーズを満たす自己署名証明書を使用することができます。

手順

1. 証明書 MM コンソールを開き、2 つのコンソール接続を作成します。1 つはローカルコンピューター証明書用で、もう 1 つは新しい ADAM サービスのローカルコンピューターサービス証明書用です。
   新しい証明書は、Certificates (ローカルコンピューター)\Personal\Certificates にあります
2. ADAM サービスのコンテナ Certificates – Service (ADAM Service Name)\ADAM_ADAM Service Name\Trusted Root Certificates\Certificates に証明書をコピーし、 Certificates – Service (ADAM Service Name)\ADAM_ADAM Service Name\Personal\Certificates に証明書をコピーします。
3. コピーした証明書の [詳細] タブを開き、有効開始日の日付スタンプをメモして、証明書キーファイルへの読み取りアクセス権を割り当てます。
   C:\Documents and Settings\All Users\Application Data\Microsoft\Crypto\RSA\MachineKeys に移動し、一致するタイムスタンプで証明書を特定します。ADAM を実行しているサービスアカウントに読み取りおよび実行の権限を割り当てます。デフォルトでは、これは [ネットワークサービス] です。
4. 新しい証明書を有効にするには、ADAM サービスを再起動します。

関連情報

http://www.microsoft.com/downloads/en/details.aspx?familyid=9688f8b9-1034-4ef6-a3e5-2a2a57b5c8e4&displaylang=en%7C

公開鍵証明書のエクスポート

インスタンスを含む LDAPS クライアントには、ADAM への安全な接続を行うために公開鍵証明書が必要です。

始める前に
必要なロール：管理者

このタスクについて
上記で使用したサーバー証明書コンソールから、クライアントが使用する公開鍵をエクスポートします。

手順

1. 証明書を選択し、右クリックして [すべてのタスク/エクスポート **(all tasks/export)]** を選択します。
   秘密鍵をエクスポートしないでください。デフォルトの DER エンコードバイナリ X.509 形式を選択し、エクスポートファイル名を指定します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

2. LDAPS を使用してサーバーに接続する LDAP クライアントに公開証明書をインストールします。
   プロンプトが表示されたら、*Trusted Root Certificate Authorities* ストアに証明書を追加します。

関連情報

http://www.microsoft.com/downloads/en/details.aspx?familyid=9688f8b9-1034-4ef6-a3e5-2a2a57b5c8e4&displaylang=en%7C

Active Directory Application Mode (ADAM) アクセスアカウント

システムには、アプリケーションインスタンスにインポートされた Active Directory Application Mode (ADAM) オブジェクト情報を読み込むためのユーザーアカウントが必要です。

次の方法のいずれかを使用してアカウントを作成します。

- ローカル ADAM ユーザーアカウントを作成し、それにパスワードを割り当て、権限を割り当てます。
- ADAM パーティションの Windows ドメインアカウントに権限を割り当てます。
- *userProxy* アカウントを使用します。

ADAM を LDAP ソースとして使用する場合は、インスタンスの LDAP サーバーの [ログイン識別名] フィールドで ADAM アカウントの完全修飾識別名 (FQDN) を指定する必要があります。

関連情報

Active Directory Application Mode (ADAM)

http://www.microsoft.com/downloads/en/details.aspx?familyid=9688f8b9-1034-4ef6-a3e5-2a2a57b5c8e4&displaylang=en%7C

LDAPS 接続のテスト

LDAPS 接続をテストします。2 つのコンソール接続があります。1 つはローカルコンピューター証明書用で、もう 1 つは新しい ADAM サービスのローカルコンピューターサービス証明書用です。

始める前に
必要なロール：管理者

手順

1. *LDP.exe* を ADAM インストールフォルダー c:\windows\adam から実行します。
   これは標準の Windows LDP クライアントではないため、ADAM バージョンが選択されていることを確認します。
2. [接続/接続する **(Connection/Connect)]** メニューを使用して、新しい接続を開きます。
   サーバー名は、証明書に割り当てられた CN と一致する必要があります。
3. **[LDAPS** ポート **(LDAPS port)]** を入力し、**[SSL]** チェックボックスをオンにします。
   接続に成功すると、一般的なサーバー情報が表示され、エラーはありません。
4. サービスにバインド (ログイン) します。
   一般的な LDAP クライアント接続をレプリケートするには、[シンプルバインド] オプションを選択します。[ユーザー] フィールドに有効な ADAM ユーザーまたは *userProxy* 識別名と関連するパスワードを入力します。
   「次のように認証されました：…。(Authenticated as:….)」というメッセージが表示された場合は、LDAPS を使用して正常に接続しています。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

関連情報

http://www.microsoft.com/downloads/en/details.aspx?familyid=9688f8b9-1034-4ef6-a3e5-2a2a57b5c8e4&displaylang=en%7C

ADAMSync を使用して ADAM に入力する

管理者は MS ADAMSync を使用して、MS ADAM を使用する LDAP ディレクトリを設定します。

注:

このドキュメントは、Microsoft Windows Server、Active Directory、および ADAM について少なくとも基本レベルの理解があり、パーティションを備えた機能的な Active Directory Application Mode (ADAM) インスタンスを既に持っていることを前提としています。

これらはサンプル手順です。複雑であり、お使いの環境で実行されているため、直接サポートを提供することはできません。問題が発生した場合は、Microsoft または Microsoft のコンサルタントに相談することをお勧めします。

ADAM がインストールされ、最初のパーティションが作成されたら、そのパーティションにオブジェクトを設定できます。

次のオプションが使用可能です。

- GUI またはスクリプトを使用して手動でオブジェクトを作成します。このオプションは非効率的で時間がかかります。
- Microsoft 統合情報サーバーを使用して Active Directory と統合します。このオプションは、最終的に最も柔軟性と機能性を備えていますが、いくつかの高度な設定が必要です。Active Directory、ADAM、および Exchange の Microsoft グローバルアドレス一覧と互換性のある MIIS の無料バージョンがあります。MIIS を使用した経験がある場合を除き、LDAP 統合専用の新しい環境を実装しないことをお勧めします。
- Microsoft が ADAM に提供する同期ツールである Adamsync を使用します。このオプションについてはここで説明します。

ADAM ユーザーアカウントの定義

ADAM でユーザーアカウントを定義します。ユーザーアカウントの 1 つは接続するインスタンスに使用され、もう 1 つのユーザーアカウントは ADAMSync に使用されます。

始める前に

必要なロール：管理者

このタスクについて

これらのアカウントは、ローカルの ADAM ユーザーオブジェクト、UserProxy オブジェクト、または信頼できるドメインの Windows アカウントにすることができます。

ADAM User アカウントには、インスタンスにインポートするディレクトリ構造への読み取り専用アクセスが必要です。これを実現する最善の方法は、cn=roles,dc=myCompany,dc=adam にあるリーダーグループのメンバー属性にアカウントを追加することです。

新しい ADAM ユーザーアカウントはデフォルトで無効になっています。新しいアカウントを有効にしてパスワードを設定する必要があります。

手順

1. ユーザーを有効にするには、属性 msDS-UserAccountDisabled を FALSE に変更します。
2. ユーザーオブジェクトを右クリックし、パスワードをリセットします。
3. Active Directory Application Mode (ADAM) で定義されている LDP を使用して新しいアカウントをテストし、接続できることを確認します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

次を使用： **LDAP** > ビュー/ツリー オプションを使用し、[ベース DN] を空白のままにして、新しいアカウントを使用してディレクトリ内のオブジェクトを表示できるようにします。[構成]、[スキーマ]、および [ドメイン] パーティションが左ペインに表示されます。[ドメイン] パーティションを走査します。新しいローカル ADAM アカウントを使用している場合は、「子なし (No Children)」と表示されます。これは、オブジェクトへの読み取りアクセス権がないことを意味します。セットアップグループメンバーシップを確認し、再テストします。

ADAMSync は *ADAMSync User* アカウントを使用して ADAM パーティション内のオブジェクトを管理します。このアカウントは ADAM オブジェクトを作成、更新、削除するため、管理者レベルの権限が必要です。

ADAMSync は *ADAMSync AD* アカウントを使用して、ADAM に同期される AD オブジェクトを読み取ります。

ADAMSync の設定

ADAMSync は Windows Server 2003 R2 に含まれています。別の OS を使用している場合は、ADAMSync をダウンロードしてインストールします。

スキーマを拡張する

ADAMSync をサポートするには、ADAM スキーマを拡張する必要があります。

1. c:\windows\adam から次のコマンドを実行して、ADAMSync スキーマ拡張をインポートします。現在のユーザーにアクセス権がない場合は、 server:port を変更して資格情報を追加する必要があります。詳細については、AdamSyncMetadata.ldf ファイルを参照してください。

```
ldifde -i -f MS-AdamSyncMetadata.LDF -s localhost:50000 -j . -c "cn=Configuration,dc=X"
 #configurationNamingContext
```

2. Windows 2003 の属性をサポートするには、MS-AdamSchemaW2k3.ldf で同じ操作を行います。

```
ldifde -i -u -f MS-AdamSchemaW2K3.LDF -s localhost:50000 -j . -c "cn=Configuration,dc=X"
 #configurationNamingContext
```

推奨されるスキーマの変更

推奨される追加のスキーマ変更を以下に示します。

1. 新しい MMC コンソールを開き、ADAM スキーマスナップインを追加します。
2. ADAM インスタンスに接続します。
3. [クラス] フォルダーを展開し、 [userProxy] クラスを見つけて [プロパティ] を開きます。
4. [属性] タブで次のオプションの属性を確認し、まだ存在しないものを追加します。
   - company
   - department
   - givenNane
   - mail
   - physicalDeliveryOfficeName
   - sAMAccountName
   - sn
   - telephoneNumber
   - title

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

- userAccountControl
- userPrincipalName

5. ADAM サービスを再起動して、新しい設定を有効にします。

ADAM 構成ファイルのインストール

Windows のコマンドラインから ADAM 構成ファイルをインストールします。

始める前に
必要なロール：管理者

手順

1. 構成ファイルをインストールします。

```
C:\WINDOWS\adam>adamsync /install localhost:50000 MS-AdamSyncConf-SNC.XML
```

2. 同期ファイルを実行してコンソールにログを記録します。

```
C:\WINDOWS\adam>adamsync /sync localhost:50000
"ou=users,dc=service-now,dc=adam" /log -
```

3. ADSIEdit コンソールを使用して結果を確認します。
   ADAMSync によって作成された新しいオブジェクトと属性が表示されます。
4. ldap を実行して UserProxy 認証をテストします。
   同期プロセスの自動化

   同期プロセスを Windows スケジュール設定済みタスクとして設定します。構成ファイルまたはコマンドラインで資格情報を入力するか、アクセスできるアカウントでスケジュール設定済みタスクを実行する必要があります。

   特記事項

   - 複数の構成ファイルとジョブスケジュールを作成して、複数のソースから ADAM を同期できます。

     この例では、アプリケーションログオンとして使用できる sAMAccountName 属性をインポートします。ソースを同期する場合は、ログオン資格情報に使用できる一意の属性値があることを確認する必要があります。sAMAccountName は、複数のドメイン間ではなく、ドメイン内で一意であることが保証されています。

   - Microsoft Exchange を使用している場合は、オブジェクトフィルター構成の一部として cn=SystemMailbox* オブジェクトを除外することをお勧めします。

ADAM 構成ファイルの例

ADAMSync の構成はすべて xml ファイルに格納されます。

コメントを含むデフォルトの構成ファイル

ADAMSync のインストールには、 MS-AdamSyncConf.xml と呼ばれるデフォルトの構成ファイルが含まれています。このファイルのコピーを作成して、後で参照する基本の例を用意してください。この例は、コメントが追加されたデフォルトの構成ファイルです。

```
<?xml version="1.0"?>
<doc>
 <configuration>
<!-- Sync File Description -->
```

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

```
<description>MyCompany ADAMSync Configuration</description>
 <security-mode>object</security-mode>;
<!-- source-ad-name = fqdn of the domain controller -->;
 <source-ad-name>;fully.qualified.domain.name.of.domain.controller</source-ad-name>;
<!-- source-ad-partition = root AD domain partition -->;
 <source-ad-partition>;dc=myCompany,dc=com</source-ad-partition>;
<!-- source-ad-account = use this to specify an account to connect to AD -->;
<!-- if not used, the current user will be used  -->;
 <source-ad-account>;</source-ad-account>;
 <account-domain>;</account-domain>;
<!-- target-dn = target ADAM OU -->;
 <target-dn>;ou=servicenow users,dc=myCompany,dc=adam</target-dn>;
 <query>;
<!-- base-dn = should be the root AD partition if you want all users -->;
  <base-dn>;dc=myCompany,dc=com</base-dn>;
<!-- object-filter = standard ldap query format, this will grab all users -->;
<!-- need to review results to see if you should modify this filter -->;
  <object-filter>;(objectCategory=person)</object-filter>;
  <attributes>;
<!-- include=userproxy requires objectSID to link back to the AD account -->;
   <include>;objectSID</include>;
   <include>;givenName</include>;
   <include>;sn</include>;
   <include>;description</include>;
   <include>;title</include>;
   <include>;company</include>;
   <include>;department</include>;
   <include>;mail</include>;
   <include>;physicalDeliveryOfficeName</include>;
   <include>;telephoneNumber</include>;
   <include>;sAMAccountName</include>;
  </attributes>;
 </query>;
<!-- map for user-to-userproxy object types -->;
 <user-proxy>;
  <source-object-class>;user</source-object-class>;
  <target-object-class>;userProxy</target-object-class>;
 </user-proxy>;
 <schedule>;
  <aging>;
   <frequency>;0</frequency>;
   <num-objects>;0</num-objects>;
  </aging>;
  <schtasks-cmd>;</schtasks-cmd>;
 </schedule>;
</configuration>;
<synchronizer-state>;
 <dirsync-cookie>;</dirsync-cookie>;
 <status>;</status>;
 <authoritative-adam-instance>;</authoritative-adam-instance>;
 <configuration-file-guid>;</configuration-file-guid>;
 <last-sync-attempt-time>;</last-sync-attempt-time>;
 <last-sync-success-time>;</last-sync-success-time>;
 <last-sync-error-time>;</last-sync-error-time>;
 <last-sync-error-string>;</last-sync-error-string>;
 <consecutive-sync-failures>;</consecutive-sync-failures>;
 <user-credentials>;</user-credentials>;
```

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

```
 <runs-since-last-object-update>;</runs-since-last-object-update>;
 <runs-since-last-full-sync>;</runs-since-last-full-sync>;
 </synchronizer-state>;
</doc>;
```

LDAP フィルター構成ファイル

構成ファイルの object-filter 値には、任意のレベルのフィルタリングを指定できます。標準の演算子の代わりに、次の xml エスケープ文字を使用して、標準の LDAP クエリ構文を使用します。

- AND =「&」& に置き換える
- OR =「|」(縦線) | に置き換える
- NOT =「!」! に置き換える

構成ファイルの参照

サンプルとして参照できる実際の構成ファイルを次に示します。

```
<?xml version="1.0"?>;
<doc>;
 <configuration>;
<description>;SNCTest ADAMSync Configuration</description>;
 <security-mode>;object</security-mode>;
 <source-ad-name>;domaincontroller.service-now.com</source-ad-name>;
 <source-ad-partition>;dc=service-now,dc=com</source-ad-partition>;
 <source-ad-account>;</source-ad-account>;
 <account-domain>;</account-domain>;
 <target-dn>;ou=servicenow users,dc=service-now,dc=adam</target-dn>;
 <query>;
  <base-dn>;dc=service-now,dc=com</base-dn>;
  <object-filter>;(objectCategory=person)</object-filter>;
  <attributes>;
   <include>;objectSID</include>;
   <include>;givenName</include>;
   <include>;sn</include>;
   <include>;description</include>;
   <include>;title</include>;
   <include>;company</include>;
   <include>;department</include>;
   <include>;mail</include>;
   <include>;physicalDeliveryOfficeName</include>;
   <include>;telephoneNumber</include>;
   <include>;userAccountControl</include>;
  </attributes>;
 </query>;
 <user-proxy>;
  <source-object-class>;user</source-object-class>;
  <target-object-class>;userProxy</target-object-class>;
 </user-proxy>;
 <schedule>;
  <aging>;
   <frequency>;0</frequency>;
   <num-objects>;0</num-objects>;
  </aging>;
  <schtasks-cmd>;</schtasks-cmd>;
 </schedule>;
```


© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

```
</configuration>;
<synchronizer-state>;
 <dirsync-cookie>;</dirsync-cookie>;
 <status>;</status>;
 <authoritative-adam-instance>;</authoritative-adam-instance>;
 <configuration-file-guid>;</configuration-file-guid>;
 <last-sync-attempt-time>;</last-sync-attempt-time>;
 <last-sync-success-time>;</last-sync-success-time>;
 <last-sync-error-time>;</last-sync-error-time>;
 <last-sync-error-string>;</last-sync-error-string>;
 <consecutive-sync-failures>;</consecutive-sync-failures>;
 <user-credentials>;</user-credentials>;
 <runs-since-last-object-update>;</runs-since-last-object-update>;
 <runs-since-last-full-sync>;</runs-since-last-full-sync>;
</synchronizer-state>;
</doc>;
```

セキュアな **LDAPS** 通信のための **Microsoft Active Directory** を設定する

証明書のペアを使用して、Microsoft Active Directory (AD) LDAPS 通信を有効にします。

注:
これらの手順は、Windows 2003 R2 Standard Edition を使用して設計およびテストされており、Windows 2003 のすべてのバージョンで機能します。

セキュア LDAP (LDAPS) 通信は、サーバーとクライアント間のデータを暗号化する点で SSL (HTTPS) 通信に似ています。これを実現するために、サーバーとクライアントは証明書のペアを使用して共通の情報を共有します。サーバーは秘密鍵証明書を保持し、クライアントは公開鍵証明書を保持します。これらの証明書は、Microsoft Active Directory (AD) LDAPS 通信を有効にするために必要です。

Active Directory の LDAPS を設定するには、次のことを行う必要があります。

- Active Directory ドメインが設定され、インスタンスがファイアウォール経由で Active Directory サーバーに接続できることを確認します。
- ドメインコントローラー (DC) の証明書を発行できる認証局 (CA) があることを確認します。CA インフラストラクチャをまだ使用していない場合は、2 つのオプションがあります。
  - 証明書を発行するためのスタンドアロン CA のセットアップ
  - サードパーティの証明書の要求
- 既に CA がある場合は、内部 CA から証明書を生成できます。

すべての証明書には有効期限があり、証明書のプロパティで確認できます。証明書の有効期限が切れると、すべての LDAPS トラフィックが失敗し、ユーザーはインスタンスにログインできなくなります。これを解決するには、新しい証明書を発行してインスタンスにインストールする必要があります。

Microsoft CA 証明書のデフォルトの有効期限は 1 年です。外部 CA 証明書は通常 1 年単位で購入します。証明書の有効期限が切れたときに注意するか、アプリケーションの有効期限通知機能(システム **LDAP** > 証明書). 古い証明書の有効期限が切れる前に、新しい証明書があることを確認してください。これにより、古い証明書の有効期限が切れる前に新しい証明書をインストールしてテストする時間が確保できます。

Active Directory のスタンドアロン認証局を設定する

SSL アクセス用に Microsoft Active Directory を設定する最初のステップは、スタンドアロンの認証局 (CA) を設定することです。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

始める前に
必要なロール：admin

このタスクについて
必要なサービス (IIS と CA) はどちらも証明書の発行後に無効にできるため、追加のリソース使用率について心配する必要はありません。

手順

1. Internet Information Server (IIS) をインストールします。
2. スタンドアロンモードで認証局サービスをインストールします。
3. 証明書サービス Web アプリケーションがインストールされ、アクティブになっていることを確認します。

次のタスク
IIS マネージャーコンソールを使用して、ローカルコンピューターを展開し、*[Web* サイト] を選択します。[既定の **Web** サイト] のステータスは [実行中] である必要があります。また、[既定の **Web** サイト] の下に *CertSrv* アプリケーションが表示されます。サイトが実行されていないか、アプリケーションが存在しない場合は、続行する前に問題を解決する必要があります。

内部認証局からの証明書を生成する

SSL アクセス用に Microsoft Active Directory を設定する場合は、内部証明書を生成して外部証明書を要求する必要があります。

始める前に
必要なロール：管理者

このタスクについて
これらの手順は、Microsoft CA サービスに適用されます。別の内部 CA プラットフォームを使用している場合は、ローカル CA 管理者にサポートを依頼してください。

手順

1. 証明書を作成するドメインコントローラー (DC) から、`http://localhost/certsrv` を参照するか、CA サーバー名がリモートサーバー上にある場合は指定します。
2. [ようこそ] ページで、[証明書の要求] をクリックし、[証明書の要求の詳細設定] を選択します。
3. [証明書の要求の詳細設定] ページで、[作成] を選択して、この CA に要求を送信します。
4. [証明書の要求の詳細設定] を次のように入力します。

[証明書の要求の詳細設定] フィールド

フィールド	エントリ
名前	証明書を要求している DC の完全修飾ドメイン名 (FQDN)。
メール	証明書の責任者のメールアドレス。
会社	会社名。
キーオプション設定	
新しいキーセットの作成	それを選択します。
CSR	Microsoft RSA SChannel 暗号化プロバイダー。
主な使用法	交換。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	エントリ
キーサイズ	1024 をお勧めします。インスタンスは最大 2048 をサポートします。
自動キーコンテナー名	それを選択します。
ローカルコンピューター証明書ストアへの証明書の保存	それを選択します。

5. [送信] をクリックします。
   [要求 **ID]** が記載されたページが表示されます。この ID をメモします。
6. 処理待ちの要求を処理するには、次の手順を実行します。
   a. 認証局管理コンソールを開きます。
   b. サーバーノードを展開し、[要求処理待ち] を選択します。
   c. 送信した要求の要求 ID を見つけて右クリックし、[すべてのタスク/要求を承認して証明書を発行するために発行する *(All Tasks/Issue to approve the request and issue the certificate)]* を選択します。
7. 発行された証明書を取得するには、次の手順を実行します。
   a. 要求を行った DC から、http://localhost/certsrv を参照するか、リモートサーバー上にある場合は CA サーバー名を指定します。
   b. [処理待ちの証明書の要求の状態] を選択します。
   c. 新しい証明書へのリンクを選択します。
   d. [この証明書のインストール] のリンクを選択します。

次のタスク

サードパーティの証明書を要求する必要があります。外部 CA からの証明書は年間 30 ドルで購入できます。外部 CA からの証明書を要求する詳細な手順については、Microsoft の記事『321051』を参照してください。受領、インストール、およびテスト後、エクスポート手順に従います。

LDAPS 接続のローカルテスト

SSL アクセス用に Microsoft Active Directory を設定する場合は、内部証明書とサードパーティの証明書をインストールした後に LDAPS 接続をテストします。

始める前に

必要なロール：admin

手順

1. Windows サポートツールがドメインコントローラー (DC) にインストールされていることを確認します。
   Support Tools のセットアップ (suptools.msi) は、Windows Server CD の `\Support\Tools` ディレクトリにあります。
2. 移動先 開始 > すべてのプログラム > **Windows** サポートツール > コマンドプロンプト.
   コマンドラインで「ldp」と入力してツールを開始します。
3. *ldp* ウィンドウで、 接続 > コネクト ローカル FQDN とポート番号 (636) を指定します。
   また、*[SSL]* を選択します。
   成功すると、Active Directory SSL 接続に関連する情報がウィンドウに表示されます。接続に失敗した場合は、システムを再起動してこの手順を繰り返します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

公開鍵証明書のエクスポートによる **LDAP** 証明書の信頼

SSL アクセス用に Microsoft Active Directory を設定する場合は、公開鍵証明書をエクスポートしてアプリケーションにインポートします。

始める前に
必要なロール：管理者

このタスクについて
認証局が信頼できるサードパーティベンダーでない場合は、発行元 CA の証明書をエクスポートして、信頼できるようにする必要があります。また、関連性別に LDAP サーバー証明書を信頼することもできます。MS 証明書サービスユーザーは、エクスポートに使用するコンソールで証明書を表示することで証明書パスを表示できます。[証明書パス] タブを選択します。チェーン内のすべての証明書をエクスポートする必要があります。[証明書パス] で名前を探すと、LDAP 証明書と同じフォルダーで CA 証明書を見つけることができます。インスタンスにインポートするすべての証明書を送信します。

手順

1. 現在または新しい MMC コンソールから、証明書 (ローカルコンピューター) スナップインを追加します。
2. Personal/Certificate フォルダーを開きます。
3. 新しい証明書を見つけます。
   [発行先] 列には、ドメインコントローラーの FQDN が表示されます。
4. 証明書を右クリックして、[すべてのタスク/エクスポート *(All Tasks/Export)]* を選択します。
5. DER または Base-64 形式にエクスポートします。
   ファイルに「MyCompany.cer」という形式の名前を付けます。これは、ドメインコントローラーと安全に通信するためにインスタンスで使用する必要がある公開鍵証明書です。
6. 証明書をインスタンスに送信する前に、LDAPS をローカルでテストします。

次のタスク
この手順を完了したら、公開鍵証明書をアプリケーションにインポートします。
証明書をアプリケーションにアップロードするには、「LDAP X.509 SSL 証明書をインストールする」を参照してください。

LDAP グローバルカタログの使用

DC にはグローバルカタログ (GC) ロールを付与できます。グローバルカタログ (GC) ロールは、フォレスト内のすべてのドメインのすべてのオブジェクトの部分的な表現で構成される LDAP 準拠のディレクトリです。

管理者は、次のいずれかのホスティング方法を使用して、ライトウェイトディレクトリアクセスプロトコル (LDAP) ディレクトリ情報をホストするように Active Directory を設定します。

- LDAP ディレクトリ情報をホストする一般的な方法は、ポート 389 または 636 でデフォルトの LDAP または LDAPS (セキュア LDAP) を使用することです。これらの標準 LDAP ポートは常にドメインコントローラー (DC) 上に存在し、ほとんど変更されません。このディレクトリパーティションにアクセスすると、DC でホストされているドメイン内のすべてのオブジェクトにアクセスできます。この方法を使用して他のドメインからオブジェクトにアクセスする方法はありません。
- DC にはグローバルカタログ (GC) ロールを付与することもできます。グローバルカタログ (GC) ロールは、フォレスト内のすべてのドメインのすべてのオブジェクトの部分的な表現で構成される LDAP 準拠のディレクトリです。この LDAP ディレクトリにはポート 3268 でアクセスでき、LDAPS ではポート 3269 でアクセスできます。LDAPS とデフォルトの LDAP ポートの証明書要件は同じです。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

グローバルカタログ LDAP 依存関係

- インスタンスが接続するドメインコントローラーでは、グローバルカタログロールが有効になっている必要があります。
- ファイアウォールルールでは、ポート 3268 (LDAP) または 3269 (LDAPS) でドメインコントローラーへの受信トラフィックを許可する必要があります。

特記事項

- すべての属性が GC パーティションにレプリケートされるわけではありません。名、姓、メール、電話番号、説明、住所などの一般的な属性が含まれています。他の属性を GC に追加できますが、フォレストレプリケーショントラフィックへの影響を最小限に抑えるために制限する必要があります。
- 標準の LDAP 統合では、通常、sAMAccountName をインスタンスの UserID として使用し、LDAP インポートマップの結合キーとして使用します。これは、ドメイン内で一意であることが保証されているためです。ドメインのフォレスト全体を表示する場合、この属性は一意ではなくなります。新しい一意の属性を、UserID および結合キーとして識別する必要があります。これらは同じ属性である必要はなく、フォレストの設計に応じて異なる場合があります。Active Directory 管理者に相談してください。通常、userPinicpaalName はドメイン間で一意の属性です。これはログインするのに分かりやすい名前ではありませんが、インポート時に一意の識別子として使用できます。UserID に使用される一般的な属性はメールアドレスです。これらの決定は、LDAP プロパティと LDAP マッピングに影響します。
- LDAP インポートマップの結合キーに使用される値は一意であり、インポートされるすべてのオブジェクトに存在する必要があります。一意でないか、存在しない場合は、誤ったレコードが変更されて更新されます。
- 既に LDAP 統合があり、それを GC に変更する場合は、インポート結合キーを変更します。結合キーを変更する前に、新しいキー値をインポートする必要があります。
- 統合が壊れるような変更を LDAP に加えた場合、まずそれらの変更を元に戻す必要があります。その後、試行内容に関する完全な情報を カスタマーサービス & サポート に連絡してください。

OpenLDAP のマイナーなスキーマ変更

back-bdb (Berkley バックエンド) を使用する OpenLDAP 2.3 システムでは、管理者がスキーマに軽微な変更を加えて統合を促進します。

> ⚠ **警告:**
> ここに記載されているカスタマイズは、特定のインスタンスで使用するために開発されたものであり、Now Support ではサポートされていません。この方法は現状のまま提供され、実装の前に完全にテストする必要があります。このカスタマイズに関するすべての質問およびコメントは、コミュニティフォーラム に投稿してください。

OpenLDAP 2.3 では、back-bdb は不等式インデックス (順序) を制限付きでサポートしています。これは、generalizedTime および ChangeSequenceNumber 構文に対してのみ実装されます。サブ文字列をサポートする構文ではサポートされません。不等式を含む検索フィルターは、プレゼンスインデックスを使用して処理されます。

既にインデックス化されているものやスキーマに存在するものを変更するのではなく、この目的のためにカスタム属性を作成することをお勧めします (*servnowid* など)。

OpenLDAP スキーマの変更

OpenLDAP スキーマを変更します。以下の手順では、ある顧客から提供された OpenLDAP 2.3 へのスキーマ変更によってインスタンスと統合する方法について詳しく説明します。

始める前に
必要なロール：管理者

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

このタスクについて

> ⚠ 警告:
> ここに記載されているカスタマイズは、特定のインスタンスで使用するために開発されたものであり、Now Support ではサポートされていません。この方法は現状のまま提供され、実装の前に完全にテストする必要があります。このカスタマイズに関するすべての質問およびコメントは、コミュニティフォーラム に投稿してください。

インスタンスとの統合のために OpenLDAP スキーマを変更するには：

手順

1. カスタム属性を作成します。

   Example

```
attribute ( 1.3.6.1.4.1.3403000.2.1.8

    NAME 'servnowid'
 ORDERING caseIgnoreOrderingMatch
 EQUALITY caseIgnoreMatch
 SYNTAX '1.3.6.1.4.1.1466.115.121.1.15' )
```

2. 選択したオブジェクトクラス OID に属性を含めます。

   Example

```
objectclass ( 1.3.6.1.4.1.3403000.2.2.1
    NAME 'BcfUserIdentifiers' SUP top AUXILIARY
 MAY ( uniqid $ unixid $ servnowid ) )
```

   OpenLDAP 2.3 では、サーバー構成を動的に変更できますが、拡張できるのはスキーマのみです。既存のスキーマを変更または削除することはできません。動的構成でこの属性に別のオブジェクトクラスを作成する代わりに、静的構成ファイル slapd.conf を使用します。

3. slapd.conf で、メインデータベースバックエンドの bdb セクションに新しい属性のインデックスを追加します。

   Example

```
database bdb (configs here) ....

index servnowid pres

(other indexes here) .....
```

4. ルートとして、slapindex を実行してこの属性をインデックス化し、検索フィルターで使用できるようにします。
   slapindex を開始する前に、OpenLDAP デーモンが実行されていないか、読み取り専用モードであることを確認してください。

LDAP レコードの削除

デフォルトでは、LDAP から削除された後、インスタンスはエントリを削除しません。

エントリ (レコードとも呼ばれます) を削除すると、履歴全体と削除されたエントリへの参照も削除されます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

たとえば、構成アイテム (CI)、SLA 契約、ソフトウェアライセンス、発注書、およびサービスカタログエントリにはすべて部門への参照があり、部門が削除されると、その部門へのすべての参照がクリアされます。また、ユーザーを削除すると、そのユーザーの実行履歴がすべて失われます。

組織のニーズに応じて、すべてのレコードを保持するか削除するか を決定します。

同時セッションの制限

すべてのノードにわたって、インスタンスのユーザーまたはロールの同時インタラクティブセッションの数を制限できます。

探索	アクティブ化
同時セッション制限の機能とビジネス価値について説明します。	同時セッションの制限を有効にする方法を理解します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

設定

ユーザーまたはロールの同時セッション数を設定します。

無効化

同時セッションの制限を無効にする方法について理解してください。

自動翻訳

[同時セッションの制限] の詳細

すべてのノードにわたって、インスタンスのユーザーまたはロールの同時インタラクティブセッションの数を制限できます。

同時インタラクティブセッションは、ユーザーが ServiceNow インスタンスごとにアクティブにできるセッションの数を参照します。アクティブなインスタンスセッションは、特定の ServiceNow インスタンスに新たにログインするたびに発生します。デフォルトでは、ユーザーが保持できるアクティブなインスタンスセッションの数に制限はありません。

Jakarta リリースでは、ユーザーごとのアクティブな同時セッション数を制限できます。アクティブなセッションの最大数に達した後にユーザーがログインすると、最も古いアクティブセッションが終了し、新しいインタラクティブセッションがアクティブになります。ユーザーがブラウザーを介してクローズ済みセッションにアクセスしようとすると、ユーザーはログインページにリダイレクトされます。

注:
セッションの上限を有効にするには、**Limit concurrent sessions** プラグインをアクティブ化する必要があります。制限は、 glide.authenticate.max.concurrent.interactive.sessions プロパティによって設定されます。上限値は、制限プロパティがアクティブなすべてのユーザーまたはロールに適用されます。ユーザーまたはユーザーに接続されているロールは、開始するセッションの制限に対して limit_concurrent_sessions 値を true に設定する必要があります。Jakarta リリースの場合、この機能はネイティブモバイルアプリまたは非インタラクティブメカニズムによって作成されたセッションをサポートしません。

最大同時セッション数が 1 に設定されている場合の一般的なユースケース：

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

1. ユーザーは、Chrome を介して最初の ServiceNow インスタンスにアクセスします。
2. ユーザーが正常にログインすると、ServiceNow によってユーザーにセッション 1 (S1) が作成されます。
3. ユーザーは、Firefox を介して ServiceNow インスタンスへの別のアクセスを開始することにします。
4. ユーザーが正常にログインすると、ServiceNow によってユーザーにセッション 2 (S2) が作成されます。
5. ユーザーの同時セッション数の上限は 1 であるため、S2 セッションが作成されると S1 が無効になります。
6. ユーザーが Chrome から S1 ServiceNow インスタンスに再度アクセスすると、S1 が無効であるため、ユーザーはログインページにリダイレクトされます。

同時セッション制限は、すべての ServiceNow 認証メカニズム (SAML、LDAP、およびローカルデータベース認証) で機能します。また、マルチファクター認証とすべてのインタラクティブ ServiceNow 認証メカニズムでも機能します。セッションのソースは、[タイプ] 列の **sys_user_session** テーブルを介して表示できます。値は次のとおりです。

- Web ブラウザー
- モバイルブラウザー
- ServiceNow モバイルアプリ
- 非インタラクティブ (SOAP、WSDL、OAuth)

「同時セッションの制限」プラグインのアクティブ化と構成

admin ロールを持っている場合は、Limit Concurrent Sessions プラグイン (com.glide.limit.concurrent.sessions) をアクティブ化できます。

始める前に

必要なロール：管理者

このタスクについて

手順

1. 移動先 すべて > システム定義 > プラグイン.
2. Limit Concurrent Sessions プラグインを見つけてクリックします。
3. [システムプラグイン] フォームでプラグインの詳細を確認し、[有効化/アップグレード] 関連リンクをクリックします。
4. [アクティブ化] をクリックします。
5. この機能を有効にして同時セッションの上限を設定するには、[プラグインファイル] タブに移動し、次のプロパティを見つけて設定値を変更します。

オプション	説明
glide.authenticate.limit.concurrent.interactive.sessions	値を **True** に設定することで、同時セッションを制限する機能を有効にできます。デフォルトでは、このプロパティは **False**に設定されています。つまり、ユーザーがアクティブにできるインタラクティブセッションの数に制限がないことを意味します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

オプション	説明
	注: この機能を無効にするには、 プロパティを **False** に設定します。
glide.authenticate.max.concurrent.interactive.sessions	すべてのノードにわたって、インスタンス上でユーザーが同時にアクティブにできるインタラクティブセッションの最大数を設定できます。

6. オプション: 必要に応じて、次のプロパティを変更することもできます。

オプション	説明
glide.authenticate.session.types.to.limit.concurrency	このプロパティはセッションタイプを制限します。デフォルトでは、Web ブラウザセッションにのみ制限があります。セッションタイプは次のとおりです。 ○ Web ブラウザ (1) ○ モバイルブラウザ (2) ○ ServiceNow モバイルアプリ (3) ○ 非インタラクティブ (10) Web ブラウザの場合は「1」、モバイルブラウザの場合は「2」、またはその両方の場合は「1,2」に値を設定できます。 注: Web およびモバイルブラウザセッションでのみ制限を設定できます。ServiceNow モバイルアプリまたは非インタラクティブセッションから発生するセッションには制限がありません。
glide.authenticate.limit.concurrent.sessions.at.cluster.node	このプロパティは、 ServiceNow インスタンスのすべてのノードにわたって同時セッションを制限するのではなく、ノードごとに同時セッション数を制限します。デフォルトでは、値は true に設定されており、すべてのノードでユーザーセッションが制限されます。プロパティが false に設定されている場合、そのノードのセッションのみが制限の対象になり、他のノードのセッションは対象になりません。

7. [更新] をクリックして設定を有効にします。

次のタスク

ユーザーまたはロール別の同時セッション制限の設定。

関連情報

プラグインのリスト (Washington DC)

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ユーザーまたはロール別の同時セッション制限の設定

特定のユーザーまたは特定のロールに同時セッション制限を設定できます。

始める前に
必要なロール：管理者

手順

1. 移動先 すべて > ユーザー管理 > ユーザー または ユーザー管理 > ロール.
2. 同時セッション制限を設定するユーザーまたはロールを選択し、[同時セッションを制限] チェックボックスをオンにして、[更新] をクリックします。
   ユーザーまたはロールには、一度にオープンできる同時セッション数の制限があります。

ユーザーまたはロール別の同時セッション制限の無効化

特定のユーザーまたは特定のロールに対して同時セッション制限を無効にできます。

始める前に
必要なロール：管理者

手順

1. 移動先 すべて > ユーザー管理 > ユーザー または ユーザー管理 > ロール.
2. 同時セッション制限を無効にするユーザーまたはロールを選択し、[同時セッションを制限] チェックボックスをオフにして、[更新] をクリックします。
   ユーザーまたはロールは、一度にオープンできる同時セッション数の制限対象ではなくなりました。

マルチファクター認証 (MFA)

マルチファクター認証をアクティブ化して構成する方法について説明します。

探索

アクティブ化

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

MFA の機能とビジネス価値について学習します。

MFA をアクティブ化する方法を理解します。

使用方法

MFA を構成して使用します。

Single Sign-on (SSO) を使用した MFA

シングルサインオン (SSO) を使用して MFA を構成する方法を理解します。

自動翻訳

マルチファクター認証の詳細

マルチファクター認証をアクティブ化して構成する方法について説明します。

MFA のアクティブ化

Integration - Multifactor Authentication (com.snc.integration.multifactor.authentication) プラグインをアクティブ化して、インスタンスで MFA の使用を開始します。このプラグインをアクティブ化するには、管理者ロールが必要です。このプロセスの詳細については、「MFA プラグインのアクティブ化」を参照してください。

マルチファクター基準

マルチファクター基準を使用して、2 ステップマルチファクター検証の使用が必要なユーザーとロールを決定します。これらの基準は、ビジネスニーズに合わせて単独でも組み合わせても使用できます。

ユーザーベースのマルチファクター基準

ユーザーベースのマルチファクター基準を使用して、MFA を使用したログインが必要なユーザーを個別に選択します。管理者は、ユーザーレコードの [マルチファクター認証を有効にする] フィールドを更新して、ユーザーの MFA 要件を有効または無効にし

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ます。このプロセスの詳細については、「ユーザーベースのマルチファクター基準の設定」を参照してください。

ロールベースのマルチファクター基準

ロールベースのマルチファクター基準を使用して、特定のロールに割り当てられたすべてのユーザーに MFA ログインを要求します。マルチファクター基準 [multi_factor_criteria] テーブルの [ロールベースのマルチファクター認証 **(Role-based multi-factor authentication)]** レコードには、MFA ログインが必要なロールのリストが含まれています。このリストの管理の詳細については、「ロールベースのマルチファクター基準の設定」を参照してください。

適応認証ポリシーベースのマルチファクター基準

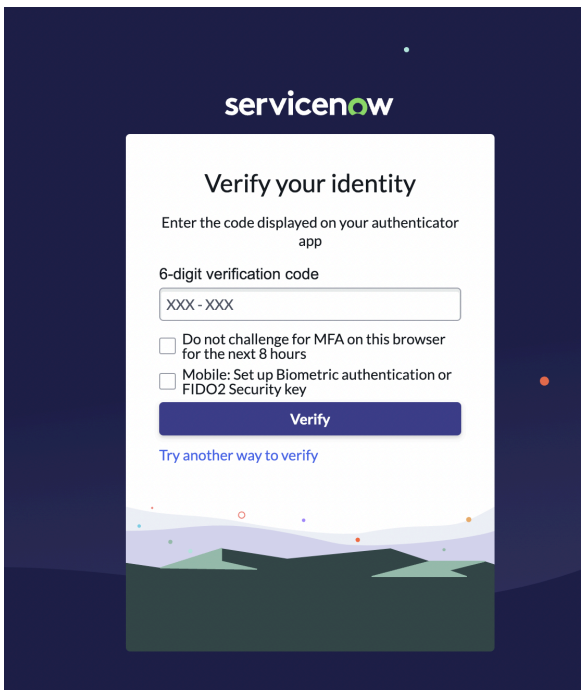
適応認証を使用して、インスタンスで MFA が必要な場合を判断します。適応認証では、認証ポリシーを使用して、ユーザーの IP アドレスやユーザーグループなどの基準を評価します。適応認証機能の詳細については、「適応認証」を参照してください。

マルチファクター認証手法

ユーザーは、ユーザー名とパスワードに加えて次のオプションを使用して、マルチファクター認証の要件を満たすことができます。

認証アプリケーション

認証アプリケーションは、一時的なパスコードを生成するサードパーティソフトウェアです。ユーザーは、これらのパスコードをパスワードとともに使用して、マルチファクター認証 (MFA) を必要とするインスタンスにログインできます。これらのアプリケーションの詳細については、「認証アプリケーション」を参照してください。



自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

生体認証スキャナー

生体認証装置は、指紋または顔認識を使用してユーザーを識別します。ユーザーは、マルチファクターログインプロセスの一部としてデバイスでこれらの認証システムを使用できます。生体認証装置の登録の詳細については、「生体認証装置の登録」を参照してください。

ハードウェアキー

ハードウェアキーは、認証に使用できる物理ハードウェアです。ハードウェアキーをデバイスのポートに挿入して認証します。ハードウェアキーの登録の詳細については、「ハードウェアセキュリティキーの登録」を参照してください。

自動翻訳

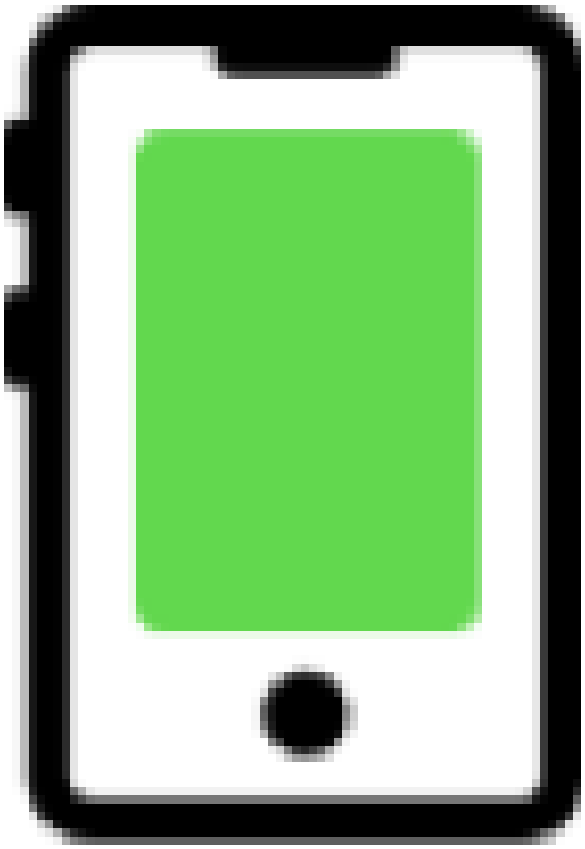
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

SMS

管理者は、インスタンスにログインしようとするユーザーに SMS ベースの OTP の使用を要求するように ServiceNow インスタンスを設定できます。

ユーザーが ServiceNow にログインしようとすると、sys_user レコードに関連付けられた携帯電話番号に SMS OTP が送信されます。ユーザーは、モバイルデバイスに送信された 6 桁の検証コードを入力して本人確認を行うことができます。

詳細については、「SMS を使用したマルチファクター認証」を参照してください。



メール

管理者は、インスタンスにログインしようとするユーザーにメールベースの OTP の使用を要求するように ServiceNow インスタンスを設定できます。

ユーザーが ServiceNowにログインしようとすると、メール OTP がユーザーのメールアドレスに送信されます。ユーザーは、メールアドレスに送信された 6 桁の検証コードを入力して本人確認を行うことができます。

詳細については、「メールを使用したマルチファクター認証」を参照してください。

マルチファクター認証プロパティ

マルチファクター認証プロパティを使用して、インスタンスで MFA を有効化、無効化、および設定します。これらのプロパティの詳細については、「マルチファクター認証システムプロパティ」を参照してください。

MFA のアクティブ化、サポートされているメソッドおよびワークフロー

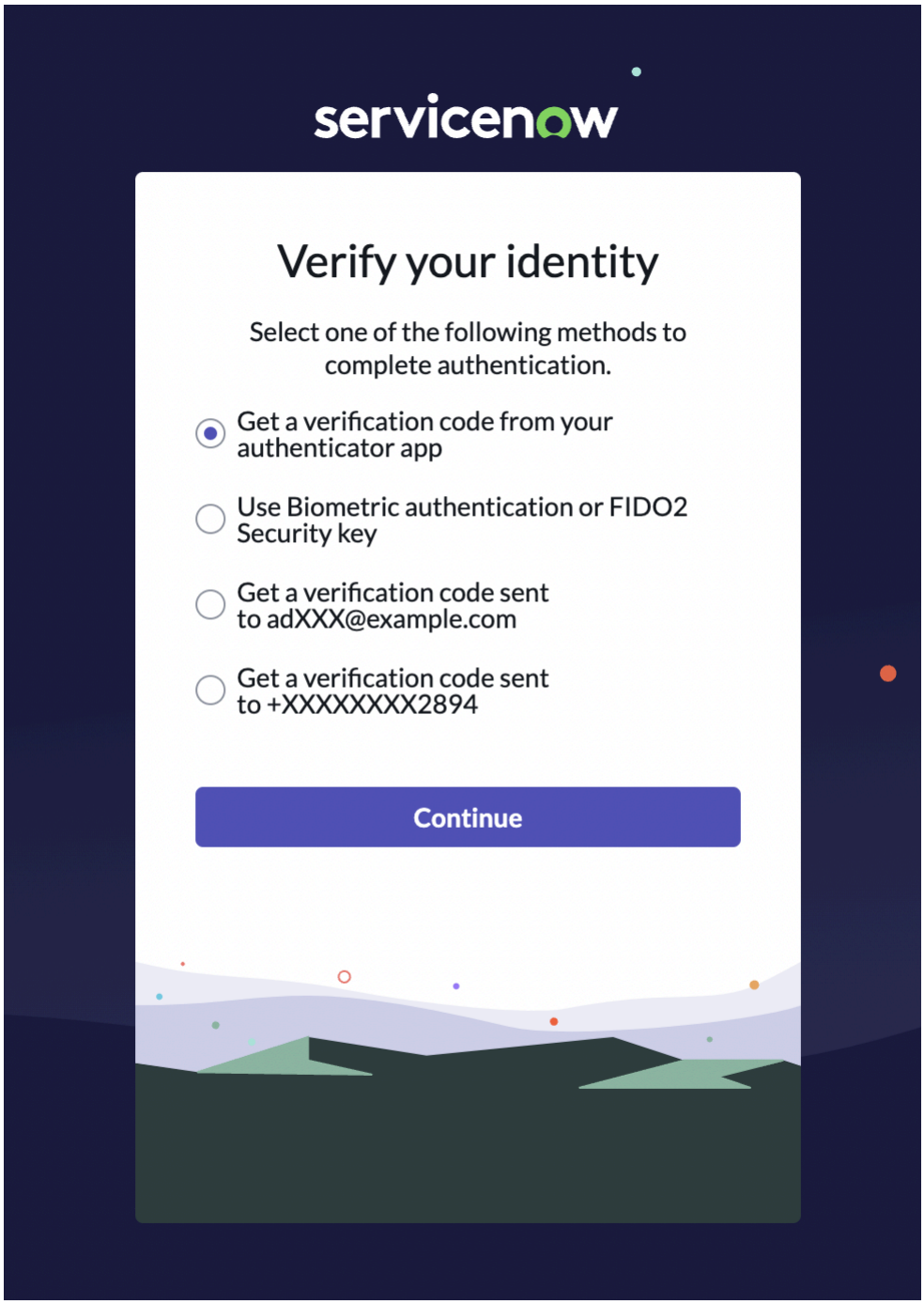
MFA は 2 ステップ検証とも呼ばれ、インスタンスにアクセスするためにユーザーは複数の資格情報セットを入力するというセキュリティ要件です。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

インスタンスに対する基本的な認証レベルは、ユーザーがユーザー名とパスワードの組み合わせを入力するローカルデータベース認証です。MFA により、管理者とユーザーは第 2 レベルの認証を要求できます。この 2 番目の認証は次のようになります。

- 認証アプリからのパスコード
- ハードウェアキー
- 指紋リーダーや顔認識などの生体認証装置。
- SMS またはメール



管理者は、個々のユーザー、または特定ロールのユーザー全員に対して MFA を要求できます。ユーザーが MFA をオプトインして使用できるようにすることもできます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

アクティブ化

Integration - Multifactor Authentication (com.snc.integration.multifactor.authentication) プラグインはデフォルトでインスタンスにインストールされますが、管理者がシステムプロパティを使用して有効にする必要があります。詳細については、「マルチファクター認証システムプロパティ」を参照してください。

注:
インスタンスをクローンした後、クローンされたインスタンスで MFA を再度有効にする必要があります。詳細については、KB 記事 KB0657100、KB0860689、KB0825390、KB0779908、KB0717367、KB0727991 を参照してください。

サポートされている認証手法

MFA は次の認証手法で使用できます。

- ローカルデータベース認証 (ネイティブ ServiceNow 認証)
- LDAP 統合
- SSO SAML
- SSO OIDC

注:
ユーザーは、ハードウェアキーまたは生体認証装置を設定する前に、認証アプリケーションを設定する必要があります。認証アプリケーションの設定の詳細については、「ユーザープロファイルでのマルチファクター認証のセットアップ」を参照してください。

マルチファクター認証設定ワークフロー

管理者によるマルチファクター認証の有効化

Integration - Multifactor Authentication (com.snc.integration.multifactor.authentication) プラグインは、デフォルトでインスタンスでアクティブ化されています。MFA の使用を開始するには、管理者がシステムプロパティを使用して MFA を有効にする必要があります。有効にしたら、管理者は MFA ログインが必要なユーザーまたはロールを選択します。

MFA 用に設定された管理者の詳細については、「マルチファクター認証 (MFA)」を参照してください。

認証アプリを使用したユーザーのログイン

ユーザーは、初回ログイン時に認証アプリを使用するように求められます。この手順は、ユーザーが生体認証またはハードウェアキーを使用する場合でも必要です。ログインしているユーザーには QR コードが表示され、これをスキャンすると認証アプリを簡単に設定できます。この初回ログインプロセスの詳細については、「ユーザープロファイルでのマルチファクター認証のセットアップ」を参照してください。

認証アプリはモバイルアプリケーションとして利用できます。認証アプリの中には、モバイルデバイスへのアクセス権がないユーザー向けにデスクトップブラウザの拡張機能として利用できるものもあります。

初回ログインの後にユーザーが追加の認証システムを設定可能

初回ログインの後、ユーザーはハードウェアキーまたは生体認証装置を登録できます。

これらの、または他のユーザー側 MFA 構成の詳細については、「マルチファクター認証 (MFA) の使用」を参照してください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Web 認証

Integration - Web Authentication (com.snc.integration.webauthn) をアクティブ化して、インスタンスでハードウェアキーまたは生体認証リーダーの認証を許可します。

ハードウェアキーは、認証に使用できる物理ハードウェアです。ハードウェアキーをデバイスのポートに挿入して認証します。ハードウェアキーの登録の詳細については、「ハードウェアセキュリティキーの登録」を参照してください。

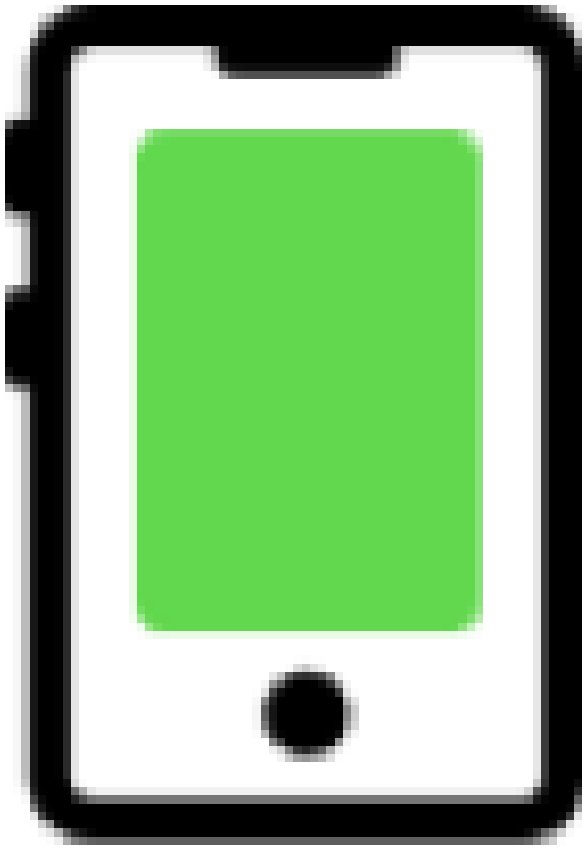
生体認証装置は、指紋または顔認識を使用してユーザーを識別します。ユーザーは、マルチファクターログインプロセスの一部としてデバイスでこれらの認証システムを使用できます。生体認証装置の登録の詳細については、「生体認証装置の登録」を参照してください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

SMS またはメール (ワンタイムパスワード)

ユーザーが外出先で ServiceNow インスタンスにログインし、よりスムーズなエクスペリエンスを実現できるように、SMS とメールによる MFA がサポートされています。



管理者は、インスタンスにログインしようとするユーザーに SMS ベースの OTP の使用を要求するように ServiceNow インスタンスを設定できます。

ユーザーが ServiceNow にログインしようとすると、sys_user レコードに関連付けられた携帯電話番号に SMS OTP が送信されます。ユーザーは、モバイルデバイスに送信された 6 桁の検証コードを入力して本人確認を行うことができます。

詳細については、「SMS を使用したマルチファクター認証」を参照してください。

管理者は、インスタンスにログインしようとするユーザーにメールベースの OTP の使用を要求するように ServiceNow インスタンスを設定できます。

ユーザーが ServiceNowにログインしようとすると、メール OTP がユーザーに関連付けられているメールアドレスに送信されます。ユーザーは、メールアドレスに送信された 6 桁の検証コードを入力して本人確認を行うことができます。

詳細については、「メールを使用したマルチファクター認証」を参照してください。

MFA プラグインのアクティブ化

Integration - Multifactor Authentication プラグインはデフォルトでアクティブになっています。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

始める前に
必要なロール：admin

手順

1. 移動先 すべて > システムアプリケーション > 利用可能なすべてのアプリケーション > すべて.
2. フィルター基準と検索バーを使用して、**Integration - Multifactor Authentication** (com.snc.integration.multifactor.authentication) プラグインを検索します。

   名前または ID でプラグインを検索できます。プラグインが見つからない場合は、ServiceNow 担当者から要求する必要があります。
3. [インストール] を選択して、[プラグインをアクティブにする] ダイアログボックスで、[アクティブ化] をクリックします。

   注:
   ドメイン分離と代理管理者がインスタンスで有効になっている場合、管理ユーザーはグローバルドメインに含まれている必要があります。それ以外の場合、次のエラーが表示されます： 別の操作が実行されているため、アプリケーションのインストールは利用できません：<プラグイン名> のプラグインの有効化。

ユーザーベースのマルチファクター基準の設定

ユーザーベースのマルチファクター基準を使用して、ユーザーの MFA を有効にします。

始める前に
必要なロール：管理者

手順

1. 移動先 すべて > ユーザー管理 > ユーザー.
2. [マルチファクター認証を有効にする] 列を表示するようにリストを構成します。
3. 選択したユーザーの [マルチファクター認証を有効にする] 列の値を **true** に変更します。

   ユーザーがユーザー名とパスワードを使用してログインすると、マルチファクター認証を設定するように求められます。

ロールベースのマルチファクター基準の設定

ロールベースのマルチファクター基準を使用して、特定のロールに割り当てられたすべてのユーザーにマルチファクター認証を適用します。

始める前に
必要なロール：管理者

手順

1. 移動先 すべて > マルチファクター認証 > マルチファクター基準.
2. [マルチファクター基準] リストで、[ロールベースのマルチファクター認証 **(Role-based multi-factor authentication)]** レコードを開きます。
3. [マルチファクターロール] リストを使用して、ロールを追加または削除します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

オプション	説明
ロールを追加	[新規行を挿入...] をダブルクリックし、ロール名を入力または選択します。保存アイコン ( ) をクリックしてエントリを保存します。
ロールを削除	削除アイコン ( ) をクリックして、リストからロールを削除します。

4. [更新] をクリックします。

タスクの結果
インスタンスは、[マルチファクターロール] リストに記載されているロールのメンバーであるユーザー全員に対してマルチファクター認証を適用します。

重要:
ロールベースのマルチファクター認証を適用するには、レコードをアクティブにする必要があります。

ユーザーのマルチファクター認証 **(MFA)** をリセットする

管理者は、アプリを削除したユーザー、デバイスへのアクセス権を失ったユーザー、またはデバイスに代替 MFA が関連付けられていないユーザーの MFA をリセットできます。

始める前に
必要なロール：admin

次の手順では、ServiceNow® 管理者が MFA 検証をリセットしてユーザーのブロックを解除し、ユーザーが MFA を再登録できるようにする方法について説明します。

管理者が支援するマルチファクター認証のリセット

手順

1. 移動先 すべて > マルチファクター認証 > ユーザーマルチファクター設定.
2. ユーザーテーブルで、ブロックを解除するユーザーを検索します。
3. [検証] を **false** に設定します。
   値を **false** に変更するとユーザーのブロックが解除され、MFA を再登録できるようになります。ブロック解除されたユーザーが資格情報を入力してログインすると、[マルチファクター認証 **(MFA)** を有効にする] ページが表示されます。ユーザーは、ページの手順に従って MFA を再登録できます。

適応認証ポリシーベースのマルチファクター基準の設定

適応ポリシーを使用して、2 ステップマルチファクター (MFA) 検証の使用が必要なユーザーを決定します。

始める前に
必要なロール：admin

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注:

- このオプションは、[複数プロバイダー **SSO** プラグイン **(Multi-Provider SSO plugin)]** がインスタンスでアクティブになっている場合にのみ表示されます。この機能の詳細については、「外部 Single Sign-on (SSO)」を参照してください。
- デフォルトのポリシーがステップアップ **MFA** ポリシーの場合、ステップアップ **MFA** ポリシーで構成されたポリシーが true と評価されると、ユーザーにはマルチファクター認証が表示されます。ポリシーは、ユーザーまたはロールベースの構成よりも優先されます。
- SSO ログインを使用する MFA は、glide.authenticate.mfa.with.multisso.enabled プロパティが true に設定されている場合にのみ使用できます。
- [認証ポリシー] レコードに移動して、参照されているポリシーフィールド ([ステップアップ **MFA** ポリシー] または [ステップダウン **MFA** ポリシー]) に「ポリシー入力」を追加または編集します。

手順

1. 移動先 すべて > 適応認証 > 認証ポリシーのコンテキスト > **MFA** コンテキスト.
   [MFA コンテキスト] ポリシーコンテキストレコードが開きます。
2. [デフォルトポリシー] フィールドでデフォルトポリシーを選択します。
   この選択により、MFA が必要かどうか判断するために、インスタンスがポリシー条件を使用する方法が決まります。

デフォルトポリシー

デフォルトポリシー	定義
ステップアップ MFA ポリシー	選択すると、[ステップアップ **MFA** ポリシー] で定義されたポリシー条件が true と評価された場合に MFA が適用されます。
ステップダウン MFA ポリシー	選択すると、[ステップダウン **MFA** ポリシー] で定義されたポリシー条件が true と評価された場合に MFA がバイパスされます。

3. [ステップアップ **MFA** ポリシー] フィールドで、このコンテキストで使用するポリシーを選択します。
   ポリシーとポリシー構成の詳細については、次を参照してください。
4. [更新] をクリックします。
   レコードを保存した後、[ポリシー入力] と [ポリシー条件] のリストが更新され、[ステップアップ **MFA** ポリシー] フィールドで選択されたポリシーに関連付けられているポリシー入力と条件が表示されます。

マルチファクター認証システムプロパティ

システムプロパティを使用すると、MFA を有効化してカスタマイズし、セキュリティ要件を満たすことができます。

マルチファクター認証プロパティ

プロパティ	説明
マルチファクター認証を有効にする (*glide.authenticate.multifactor*)	ユーザーと管理者がこの機能を使用できるようにするオプション。デフォルトでは有効です。このプロパティの詳細については、「インスタンスセキュリティ強化設定」の「マルチファク

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

マルチファクター認証プロパティ (続く)

プロパティ	説明
	ター認証 (MFA) を有効にする」を参照してください。
ユーザーがマルチファクター認証をバイパスできる回数 (*glide.authenticate.multifactor.setup.bypass.count*)	ユーザーが MFA のセットアップをスキップできる回数。ユーザーがモバイルデバイスを持っていない場合でも、引き続きインスタンスにログインできます。この機能を無効にしてから再度有効にすると、カウンターが最初から開始されます。デフォルトは 3 です。
ユーザーのメールアドレスに送信されたワンタイムコードが有効である時間 (分) (*glide.multifactor.onetime.code.validity*)	リセットコードが有効である時間 (分)。「マルチファクター認証によるログイン」を参照してください。デフォルトは 10 です。
クロックスキューを考慮してコードを有効にする追加の秒数。最大値は 60 秒です (*glide.authenticate.multifactor.clock_skew*)	リセットコードを有効にする追加の秒数。最大値は 60 です。デフォルトは 10 です。 インスタンスは、現在時刻に生成された単一のアプリ生成コードに対して、ユーザーが入力したコードを検証します。このプロパティを使用して期間をスキューし、期間中に生成された 1 つ以上のコードが有効と見なされるようにすることができます。 プロパティの値は、次の計算で使用されます：「現在時刻 - X/2」および「現在時刻 + X/2」、ここで「X」はこのプロパティの値です。たとえば、値 10 を使用すると、インスタンスは、「現在時刻 - 5 秒」から「現在時刻 + 5 秒」の時間範囲内にアプリが生成したコードを有効と見なします。 このプロパティを使用すると、ユーザーがデフォルトで割り当てられた時間内に正しいコードを入力できない場合のログインの問題を防ぐことができます。
マルチファクター認証のためのブラウザを保存する機能を有効にします。 (*glide.authenticate.multifactor.remember.browser.enable*)	ユーザーが新しいデバイスまたはブラウザーからログインしたときに MFA のプロンプトを表示するようにインスタンスを設定します。デフォルトは [はい] です。
ブラウザーの指紋認証の有効期限 (時間) (*glide.authenticate.multifactor.browser.fingerprint.validity*)	MFA がブラウザーを記憶した後、ユーザーはこの期間、同じブラウザーで MFA から干渉を受けません。デフォルトは 8 時間です。
ユーザーが記憶できるブラウザーの最大数 (*glide.authenticate.multifactor.remembered.browser.max.count*)	このユーザーについて MFA が記憶しているブラウザーの数
[マルチファクター検証] ページのブラウザーを保存するためのチェックボックスのデフォルト値 (*glide.authenticate.multifactor.remember.browser.default*)	[マルチファクター検証] ページのブラウザーを保存するためのチェックボックスのデフォルト値

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

マルチファクター認証プロパティ (続く)

プロパティ	説明
Web 認証 (FIDO2) ベースの MFA を有効にする (*glide.webauthn.enabled*)	ハードウェアキーや生体認証などのパスワードなしの認証方法を有効にするオプション

生体認証を使用した **MFA** の構成

管理者は、[ユーザーの公開資格情報] リストを使用して、ユーザーが作成した資格情報を表示および管理できます。

ユーザーが認証アプリケーション、生体認証、またはハードウェアキーを登録すると、インスタンスにより、ユーザー公開資格情報 [sys_user_public_credential] テーブルにレコードが作成されます。このテーブルを使用して、認証システムを登録したユーザー、認証システムのタイプ、および認証システムが登録および使用された時期を確認します。これらのレコードを非アクティブとしてマークし、ユーザーがこれらの資格情報を使用できないようにすることもできます。

ユーザーの公開資格情報フォーム

フィールド	説明
資格情報ニックネーム	資格情報のニックネーム。このニックネームは、ユーザーが認証システムを登録するときに選択します。
ユーザー	資格情報に関連付けられたユーザー
アクティブ	この資格情報がアクティブかどうか。管理者は、レコードを非アクティブに設定して、ユーザーがこの資格情報を使用して認証されるのを防ぐことができます。
認証システム	ユーザーによって登録された認証システムのタイプ
登録時間	ユーザーがこの資格情報を作成した日時
前回の使用時間	ユーザーがこの資格情報を使用してログインした前回の日時

制限付き認証システムのタイプ

生体認証装置など認証方法を制限している場合、ユーザーはそのタイプの新しい資格情報を作成できません。ただし、この制限を行う前に作成された資格情報は引き続き機能します。[ユーザーの公開資格情報] テーブルのレコードを無効にして、作成後にこれらの資格情報が使用されることがないようにすることができます。

認証システムの構成オプション

[認証システムの構成] ページを使用して、インスタンスの認証システムのオプションを管理します。

移動先 マルチファクター認証 > **Web** 認証 > 認証システムの構成 をクリックして、デフォルトの構成オプションを表示および編集します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

[認証システムの構成] フォーム

フィールド	説明
許可された認証システムのタイプ	登録が許可されている認証システムのタイプ。次から選択します。 • プラットフォーム：認証システムが接続されているか、デバイスに組み込まれています。モバイルデバイスで利用可能な指紋リーダーまたは顔認識 (Apple FaceID や TouchID など) はこのカテゴリに分類されます。 • ローミング：認証システムをコンピューターや他のクライアントデバイスから取り除いて、別の場所で使用できます。ハードウェアキーはこのカテゴリに分類されます。
証明書タイプ	値を [直接] または [間接] に設定するには、登録時に認証システムの来歴を証明するために認証システムのメタデータをインポートする必要があります。 • なし • 直接 • 間接
プラットフォームの自己証明書	プラットフォーム認証システムに対して自己証明書が有効になっているかどうか。
クロスプラットフォームの自己証明書	ローミング認証システムに対して自己証明書が有効になっているかどうか。
ユーザー検証	[優先] または [必須] から選択します。必要に応じて、Web 認証フローは PIN または生体認証を使用した検証をユーザーに要求します。
ユーザーのプレゼンスを検証	Web 認証フローでユーザーのプレゼンスの検証が必要かどうか。
レジデントキー	[優先] または [必須] から選択します。必要に応じて、認証システムは認証システムのストレージ内に公開鍵資格情報を保持します。
タイムアウト (ミリ秒)	Web 認証の登録と認証を完了するための最大時間制限。時間はミリ秒単位です。

SMS を使用したマルチファクター認証

認証要素として SMS を使用するマルチファクター認証 (MFA)

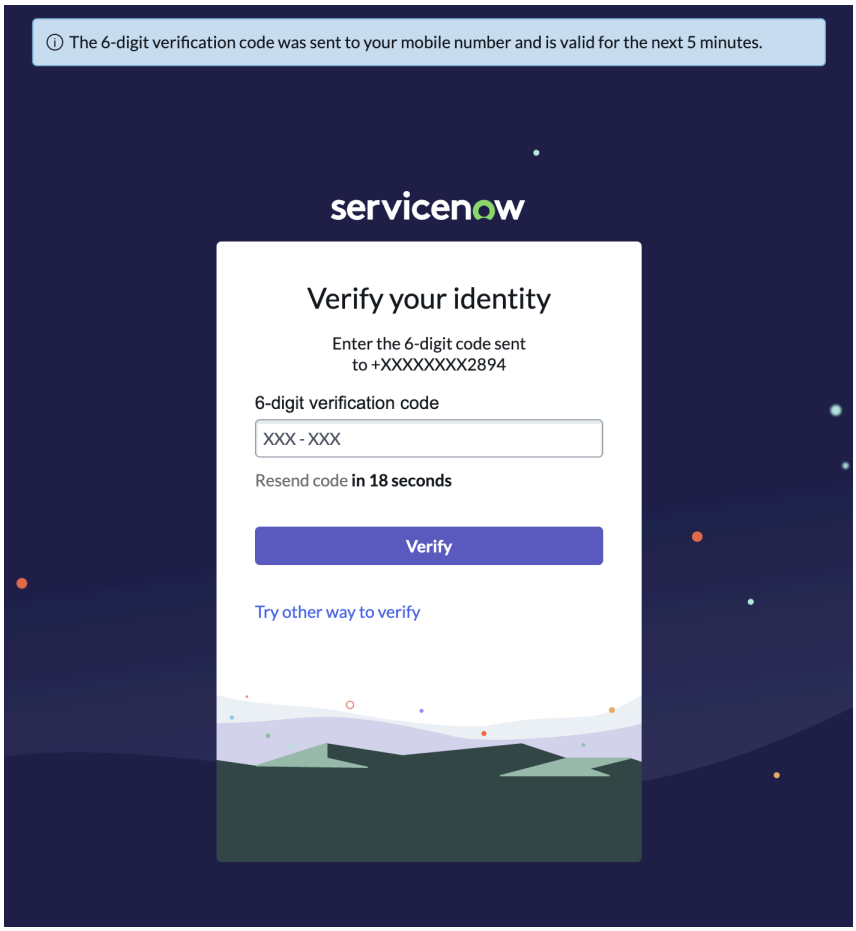
管理者は、インスタンスにログインしようとするユーザーに SMS ベースの OTP の使用を要求するように ServiceNow インスタンスを設定できます。

ユーザーが ServiceNow にログインしようとすると、sys_user レコードに関連付けられた携帯電話番号に SMS OTP が送信されます。ユーザーは、モバイルデバイスに送信された 6 桁の検証コードを入力して本人確認を行うことができます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

すぐに利用可能な Twilio を使用して、SMS で MFA を構成することもできます。詳細については、「マルチファクタ認証プロバイダー」を参照してください。



さらに、SMS を使用した MFA は、フィルター基準を使用してポリシー入力と条件に基づいて制御できます。フィルター基準のタイプは次のとおりです。

- IP フィルター基準
- ロールフィルター基準
- グループフィルター基準

MFA with SMS プラグインの有効化

SMS を使用した MFA の場合、Multi-factor Authentication with SMS (com.snc.authentication.sms_mfa) プラグインをインストールします。

始める前に
必要なロール：admin

このタスクについて
次のアイテムは、Multi-factor Authentication with SMS とともにインストールされます。

- 適応認証 (com.snc.adaptive_authentication)
- Notify Twilio Direct Driver (com.snc.notify.twilio_direct)

依存プラグイン：Integration - Multifactor Authentication (com.snc.integration.multifactor.authentication)

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

> **注:**
> SMS を生成するためのカスタムプロバイダーを設定する場合は、プラグインのインストール時にデモデータをロードできます。

手順

1. 移動先 すべて > システムアプリケーション > 利用可能なすべてのアプリケーション > すべて.
2. フィルター基準と検索バーを使用して、Multi-factor Authentication with SMS プラグイン (com.snc.authentication.sms_mfa) を検索します。

   名前または ID でプラグインを検索できます。プラグインが見つからない場合は、ServiceNow 担当者から要求する必要があります。
3. [インストール] を選択して、[プラグインをアクティブにする] ダイアログボックスで、[アクティブ化] をクリックします。

> **注:**
> ドメイン分離と代理管理者がインスタンスで有効になっている場合、管理ユーザーはグローバルドメインに含まれている必要があります。それ以外の場合、次のエラーが表示されます： 別の操作が実行されているため、アプリケーションのインストールは利用できません：<プラグイン名> のプラグインの有効化。

SMS を MFA 要素として設定

認証の MFA 要素ポリシーとして SMS OTP を表示するようにポリシー入力と条件を設定します。

始める前に
必要なプラグイン：Multi-factor Authentication with SMS (com.snc.authentication.sms_mfa)。

必要なロール：admin

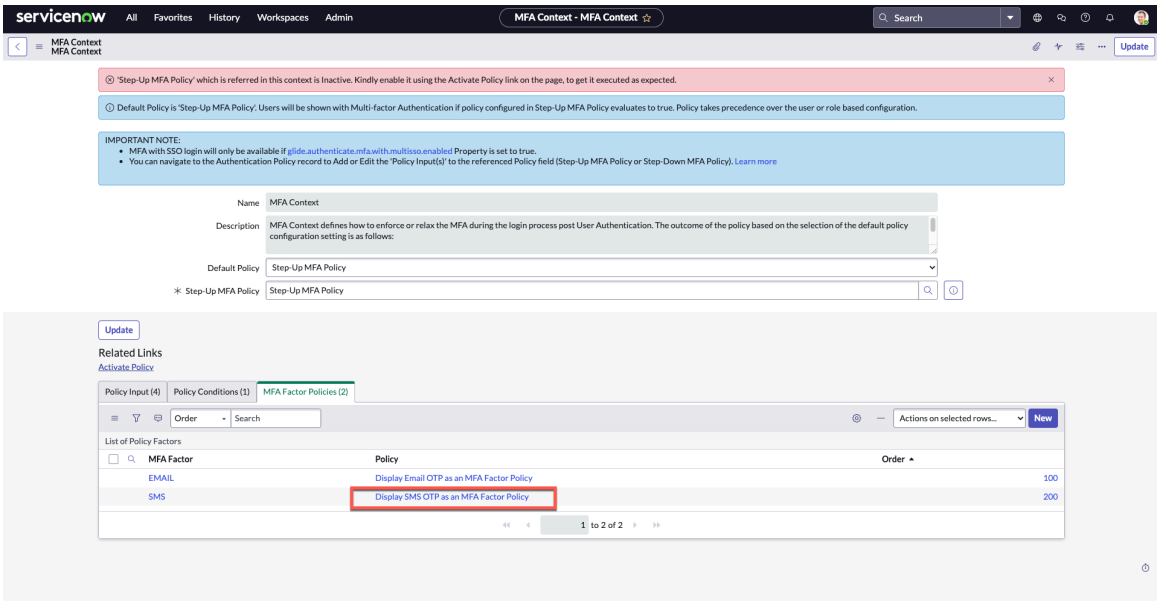
> **注:**
> SMS 要素ポリシーを適用するには、MFA コンテキストポリシーが true と評価される必要があります。

手順

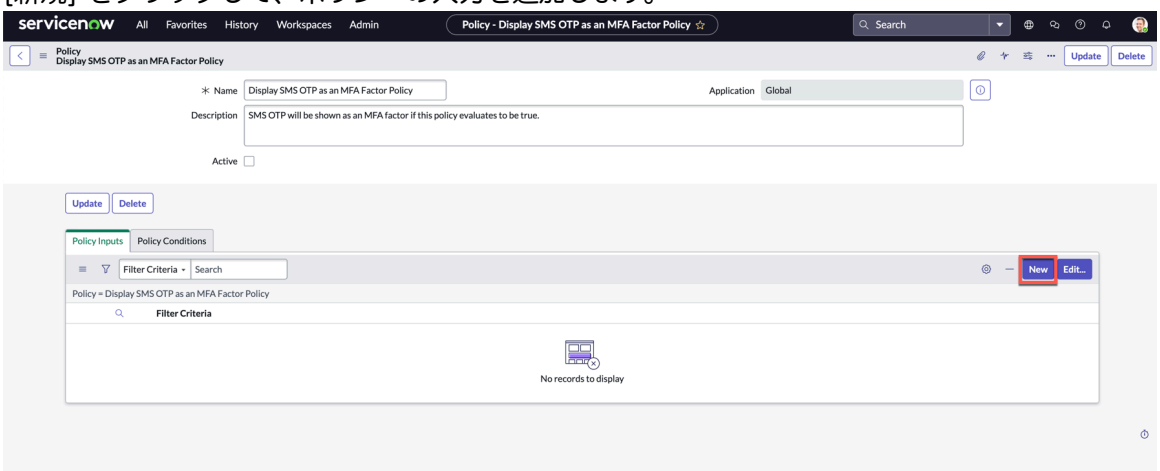
1. 移動先 すべて > マルチファクター認証 > **MFA** コンテキスト.
2. **[MFA** 要素ポリシー] タブをクリックします。
3. **[SMS OTP** を **MFA** 要素ポリシーとして表示 **(Display SMS OTP as an MFA Factor Policy)]** を選択します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



4. [新規] をクリックして、ポリシーの入力を追加します。

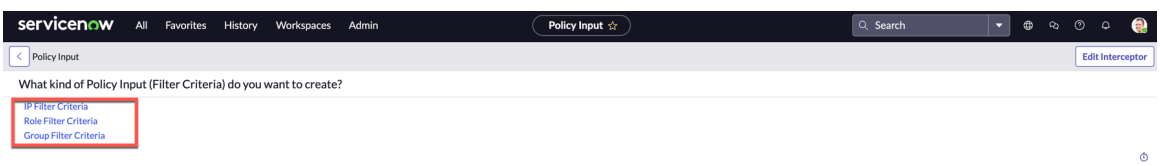


5. 作成するフィルター基準を選択します。

フィルター基準のタイプは次のとおりです。

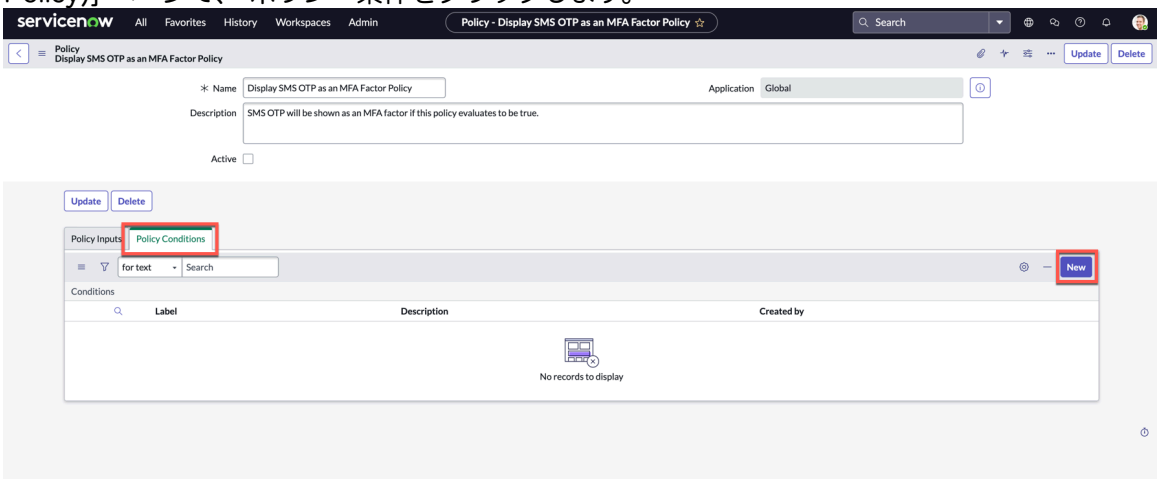
- IP フィルター基準
- ロールフィルター基準
- グループフィルター基準

例：ロールフィルター基準



© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

6. [ロールフィルター基準] をクリックし、ロールフィルター基準のフィールドに入力してレコードを送信します。新しいポリシーが作成されます。詳細については、「ロールフィルター基準」を参照してください。
7. [ポリシー - SMS OTP を MFA 要素ポリシーとして表示 (Display SMS OTP as an MFA Factor Policy)] ページで、 ポリシー条件をクリックします。



8. [新規] をクリックして、ポリシー条件を追加します。
9. フォームのフィールドに入力します。

[条件] フォーム

フィールド	説明
ラベル	条件を識別する名前
説明	条件の説明
条件	認証要求を評価するために使用される複数のポリシー入力 (フィルター基準) の論理的な組み合わせ。 条件に対して作成されたロールベースのフィルター基準ポリシーを選択します。

10. [送信] をクリックします。
11. オプション: 追加のポリシー条件を作成するには、手順 8 を繰り返します。

> **注:**
> 複数のポリシー条件を作成する場合、アクセスポリシーの最終的な出力は、すべてのポリシー条件の論理 OR 出力によって決まります。これは、ポリシー条件のいずれかが満たされると、ポリシーが true と評価されることを意味します。

ロールフィルター (ユーザー) ポリシーに基づいて、ロールに指定された条件が一致すると、MFA 要素としての SMS がユーザーの認証のオプションとして表示されます。

マルチファクタ認証プロバイダー

MFA プロバイダーを使用して SMS およびメールベースの認証を構成し、すべてのユーザーが安全にログインできるようにします。

Now Platform では、メールや SMS などのマルチファクター認証を使用するメカニズムで MFA プロバイダーを構成できます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Now Platform 内の MFA で利用可能な次のプロバイダー構成を使用できます。

- メールプロバイダー構成
- Twilio プロバイダー構成
- Infobip プロバイダー構成

> **注:**
> Twilio および Infobip プロバイダー構成は、Multi-factor Authentication with SMS (com.snc.authentication.sms_mfa) および Notify - Twilio Direct Driver (com.snc.notify.twilio_direct) プラグインをインストールするときに [デモデータのロード] を有効にすると自動的に入力されます。

独自のプロバイダー構成を作成して、SMS とメールを使用したマルチファクター認証を有効にすることもできます。

> **注:**
> Infobip プロバイダー構成はデモデータの一部として提供されます。独自のプロバイダーを構成するための要件に基づいてフィールドを編集できます。

MFA プロバイダーの構成

プロバイダーと SMS およびメールを構成して、すべてのユーザーが安全にログインできるようにします。

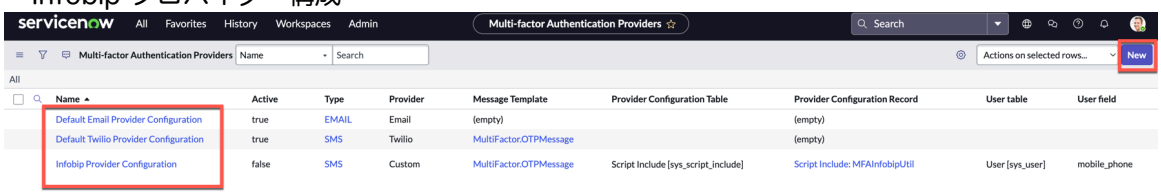
始める前に
必要なロール：管理者

手順

1. 移動先 すべて > マルチファクター認証 > プロバイダー.

   Now Platform 内の MFA で次のプロバイダー構成を使用できます。

   - メールプロバイダー構成
   - Twilio プロバイダー構成
   - Infobip プロバイダー構成



2. 新しいプロバイダーを作成するには、[新規] をクリックします。
3. フォームの各フィールドに入力します。

[条件] フォーム

フィールド	説明
名前	レコードの名前
タイプ	レコードの説明です。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

フィールド	説明
プロバイダー	**[Twilio]** または [カスタム] を選択します。 注: Twillio を設定するには、「Twilio の使用を Notify で設定する」を参照してください。 [カスタム] を選択する場合は、次のフィールドを指定する必要があります。 ○ プロバイダー構成テーブル ○ プロバイダー構成レコード ○ スクリプト ○ ユーザーテーブル ○ ユーザーフィールド
メッセージテンプレート	レコードのメッセージテンプレート
有効	プロバイダー構成をアクティブにするオプション

4. [送信] をクリックします。

   メッセージテンプレートとプロバイダー構成に基づいて、ログインプロセス中に認証のための要素として SMS またはメールがユーザーに送信されます。

Vonage プロバイダーのカスタム構成 (チュートリアル)

SMS と Vonage プロバイダーを構成して、すべてのユーザーが安全にログインできるようにします。

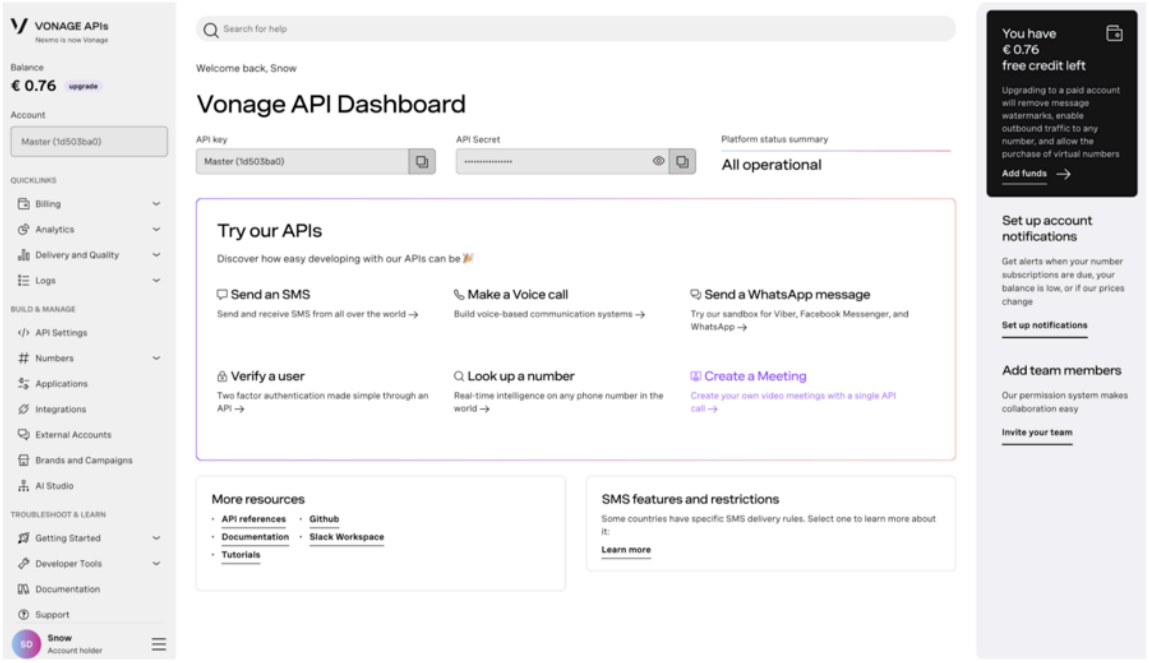
始める前に
必要なロール：管理者

自動翻訳

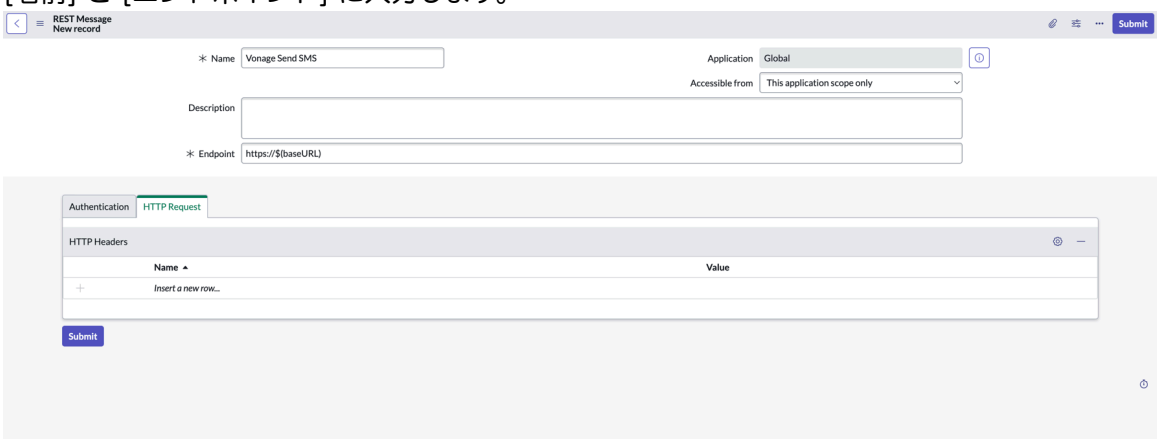
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. 移動先 すべて > システム **Web** サービス > 送信 > **REST** メッセージ Vonage API ダッシュボードからの情報に基づいて REST メッセージの構成を実行します。



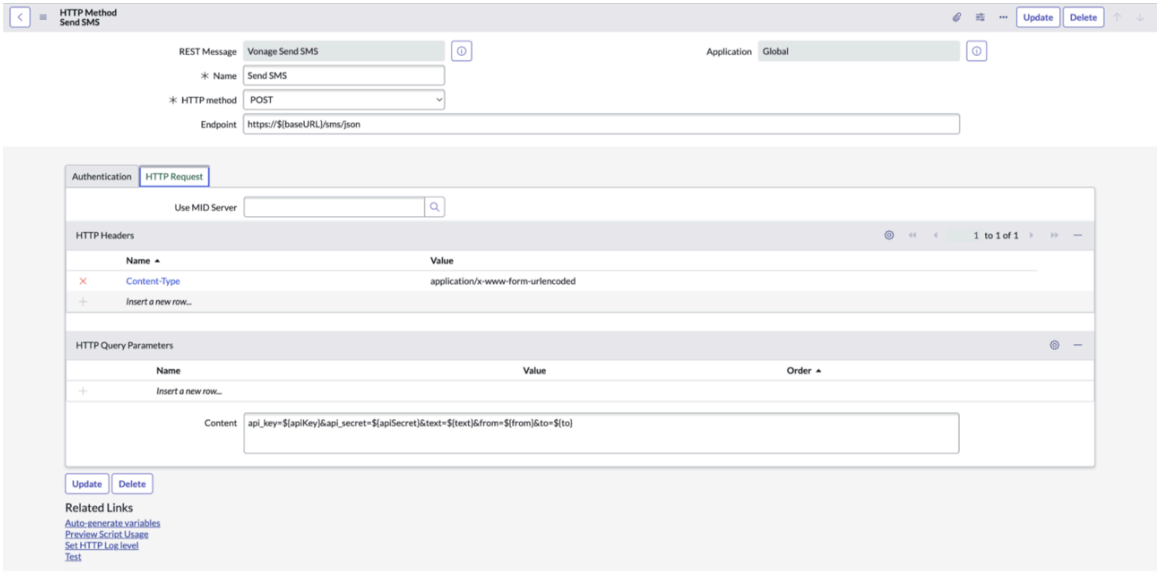
2. [新規] をクリックし、新しい **REST** メッセージを作成します。
3. [名前] と [エンドポイント] に入力します。



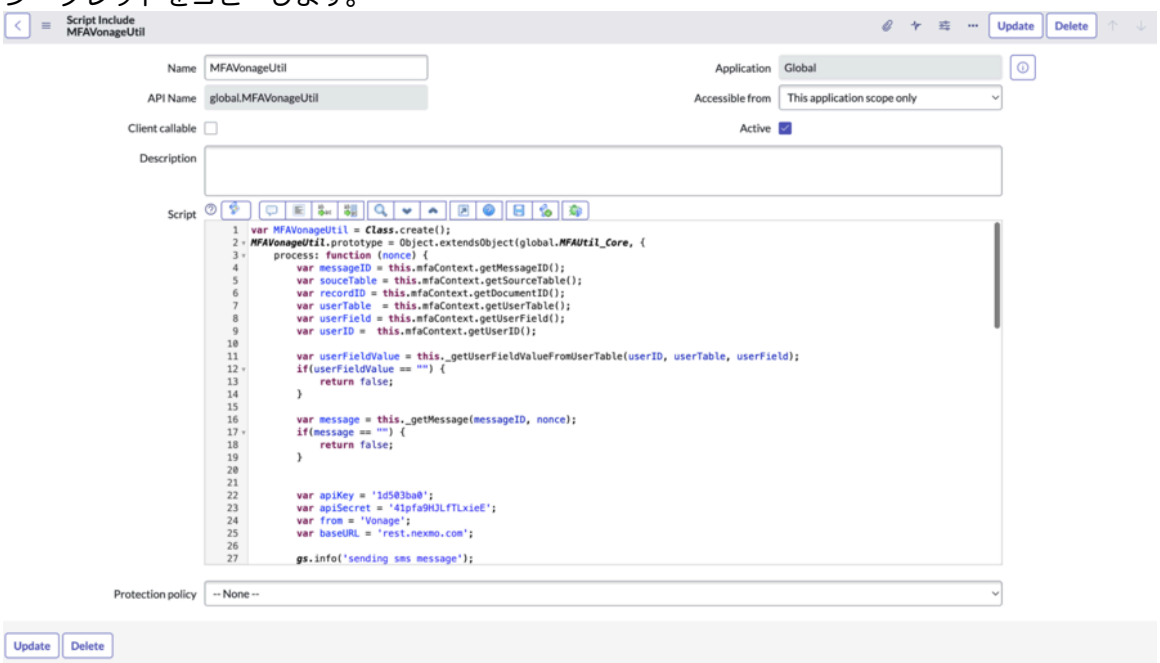
4. [送信] をクリックします。
5. **[HTTP** メソッド] 関連リストで、作成したレコードを開き、[新規] をクリックして、**POST** として HTTPメソッドを選択します。
6. 次のフィールドに入力します。
   - エンドポイント： `https://${baseURL}/sms/json`
   - コンテンツ：`api_key=${apiKey}&api_secret=${apiSecret}&text=${text}&from=${from}&to=${to}`
   - コンテンツタイプ：`application/x-www-form-urlencoded`

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



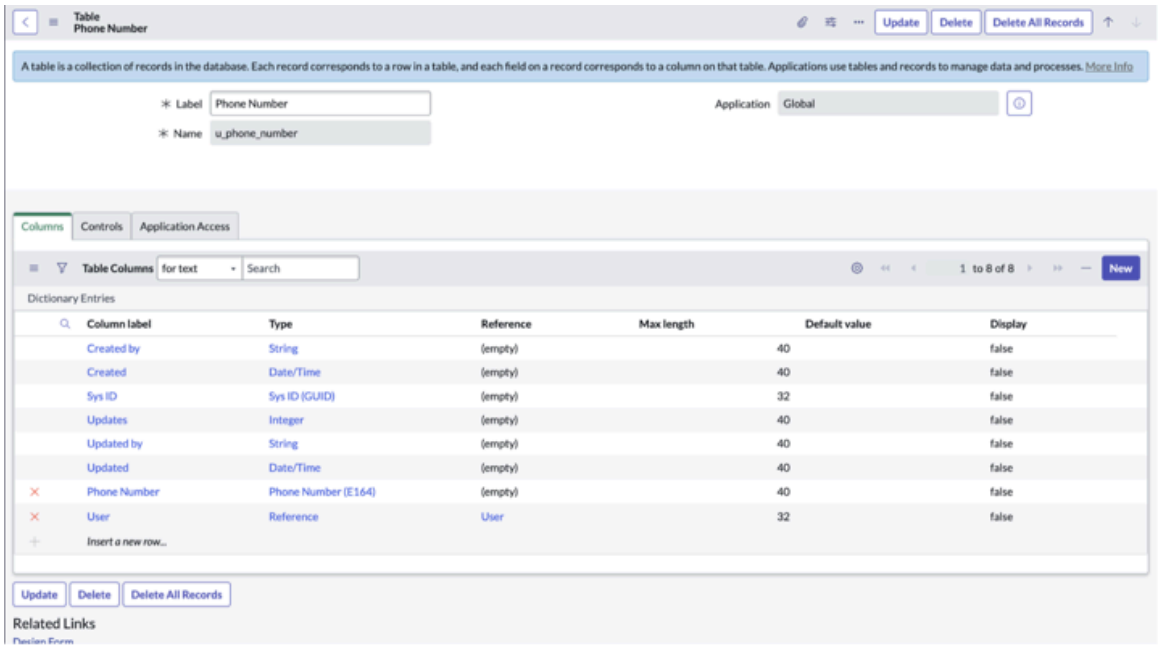
7. レコードを更新します。
8. [関連リンク] セクションで [変数の自動生成] をクリックします。
9. フォルダーで共有されている SI をインポートし、Vonage API ダッシュボードから apiKey とシークレットをコピーします。



10. 次の例のように、2 つの列を持つカスタムテーブルの電話番号を作成します。
    - 列ラベル：ユーザー、タイプ：参照、参照：ユーザー (sys_user)。
    - 列ラベル：電話番号、タイプ：電話番号 (E164)。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



11. マルチファクタープロバイダーテーブルにカスタムプロバイダーを作成します。

プロバイダー構成の詳細については、「MFA プロバイダーの構成」を参照してください。

Vonage プロバイダーに関連する詳細な手順については、次の KB 記事を参照してください。

メールを使用したマルチファクター認証

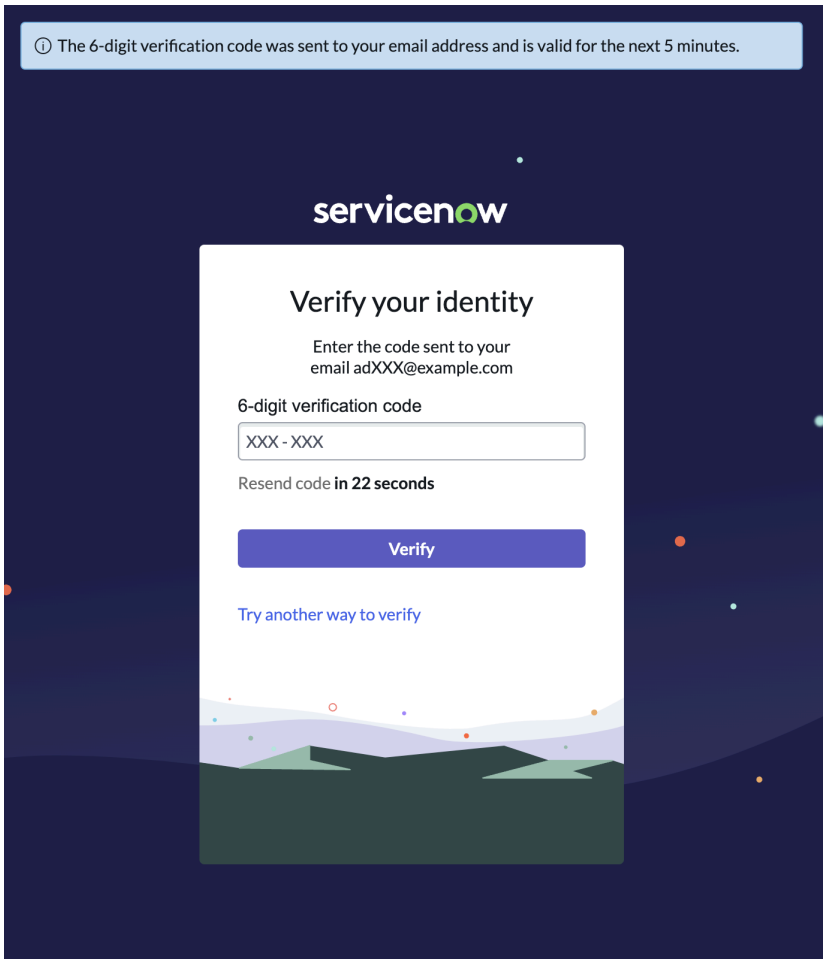
認証要素としてメールを使用するマルチファクター認証 (MFA)。

管理者は、インスタンスにログインしようとするユーザーにメールベースの OTP の使用を要求するように ServiceNow インスタンスを設定できます。

注:
メールを使用した MFA は、Integration - Multifactor Authentication (com.snc.integration.multifactor.authentication) プラグインでデフォルトでアクティブ化されています。ポリシーの入力と条件を設定する必要があります。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



ユーザーが ServiceNow にログインしようとすると、メール OTP が、関連付けられているメールアドレスに送信されます。ユーザーは、メールアドレスに送信された 6 桁の検証コードを入力して本人確認を行うことができます。

自動翻訳

メールを **MFA** 要素として設定

認証の MFA 要素ポリシーとして メール OTP を表示するようにポリシー入力と条件を設定します。

始める前に

必要なロール：管理者

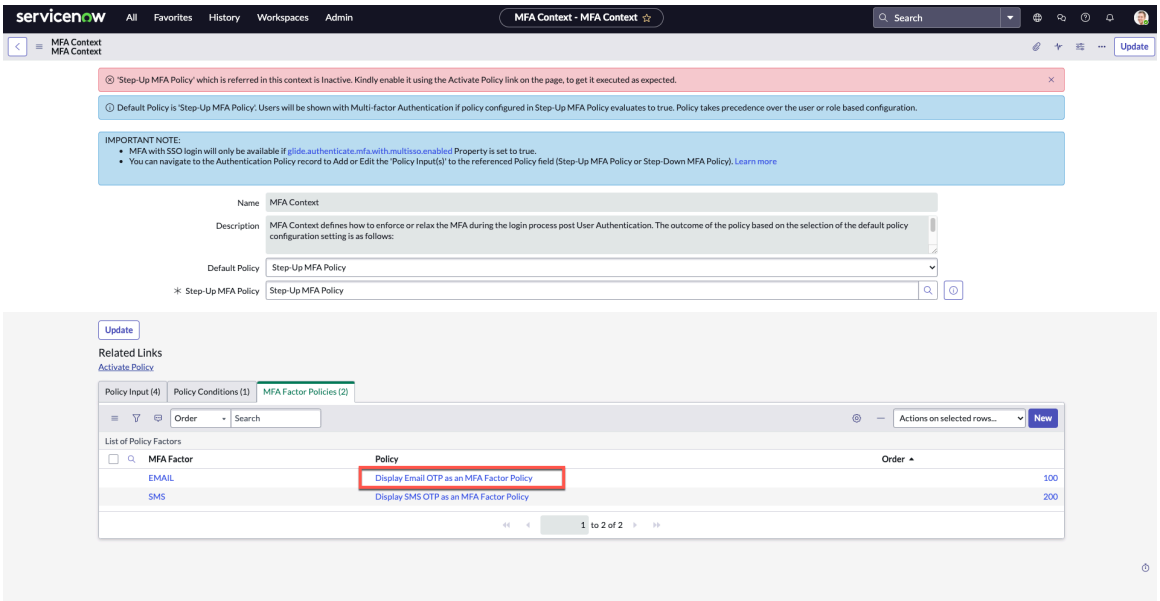
手順

1. 移動先 すべて > マルチファクター認証 > **MFA** コンテキスト.
2. **[MFA** 要素ポリシー] タブをクリックします。

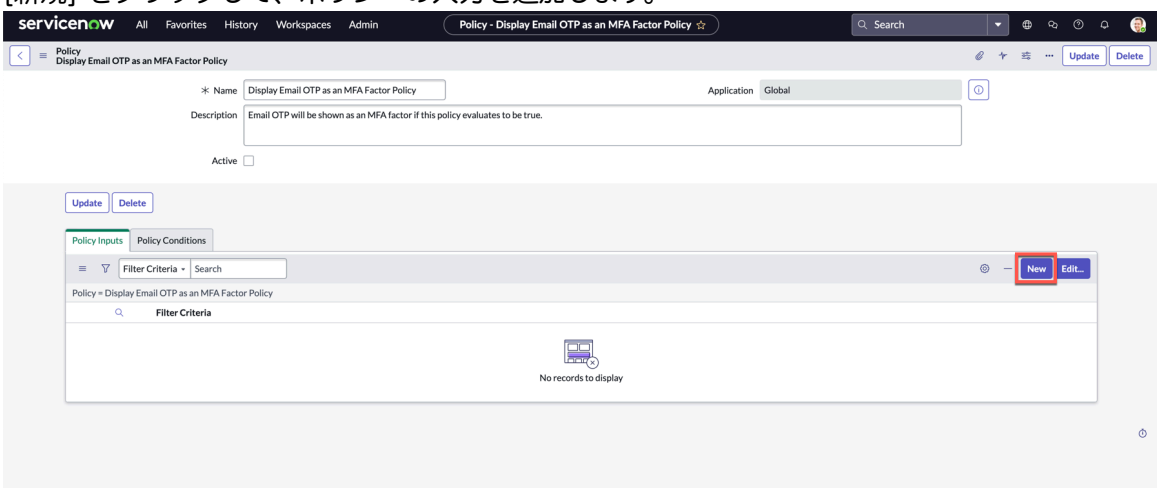
   注:
   デフォルトでは、ポリシー付きの **MFA** 要素としてメールを利用できますポリシーを編集し、ポリシーの入力と条件を指定できます。

3. [メール **OTP** を **MFA** 要素ポリシーとして表示 **(Display Email OTP as an MFA Factor Policy)]** を選択します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



4. [新規] をクリックして、ポリシーの入力を追加します。



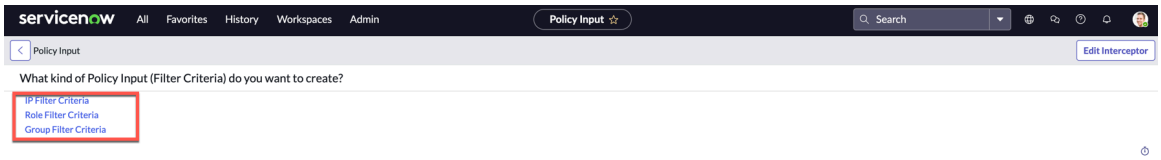
5. 作成するフィルター基準を選択します。

フィルター基準のタイプは次のとおりです。

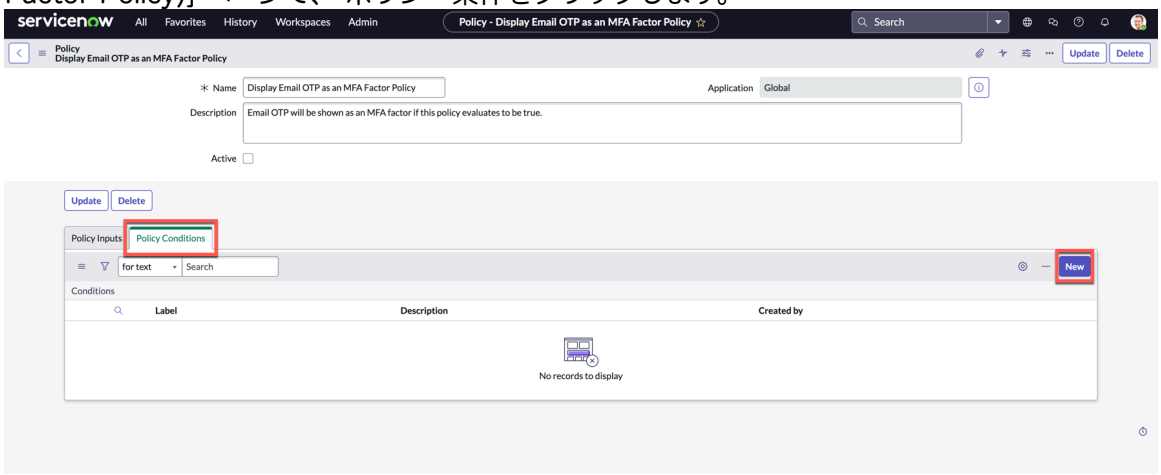
- IP フィルター基準
- ロールフィルター基準
- グループフィルター基準

例：ロールフィルター基準

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



6. [ロールフィルター基準] をクリックし、ロールフィルター基準のフィールドに入力してレコードを送信します。新しいポリシーが作成されます。詳細については、「ロールフィルター基準」を参照してください。
7. [ポリシー - メール OTP を MFA 要素ポリシーとして表示 (Display Email OTP as an MFA Factor Policy)] ページで、 ポリシー条件をクリックします。



8. [新規] をクリックして、ポリシー条件を追加します。
9. フォームのフィールドに入力します。

[条件] フォーム

フィールド	説明
ラベル	条件を識別する名前
説明	条件の説明
条件	認証要求を評価するために使用される複数のポリシー入力 (フィルター基準) の論理的な組み合わせ。 条件に対して作成されたロールベースのフィルター基準ポリシーを選択します。

10. [送信] をクリックします。
11. オプション: 追加のポリシー条件を作成するには、手順 8 を繰り返します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注:
複数のポリシー条件を作成する場合、アクセスポリシーの最終的な出力は、すべてのポリシー条件の論理 OR 出力によって決まります。これは、ポリシー条件のいずれかが満たされると、ポリシーが true と評価されることを意味します。

ロールフィルター (ユーザー) ポリシーに基づいて、ロールに指定された条件が一致すると、ユーザーの認証のオプションとしてメール MFA 要素が表示されます。

マルチファクター認証 (MFA) の使用

マルチファクター認証ツールを使用してインスタンスに安全にアクセスする方法について説明します。

MFA でログイン

ServiceNow では、時間ベースのワンタイムパスワード (TOTP) をサポートする認証アプリケーションが必要です。ServiceNow は次の認証システムで MFA をテストします。

- Google 認証システム
- Microsoft 認証システム
- LastPass 認証システム
- Authy
- FreeOTP
- Duo
- Okta Verify

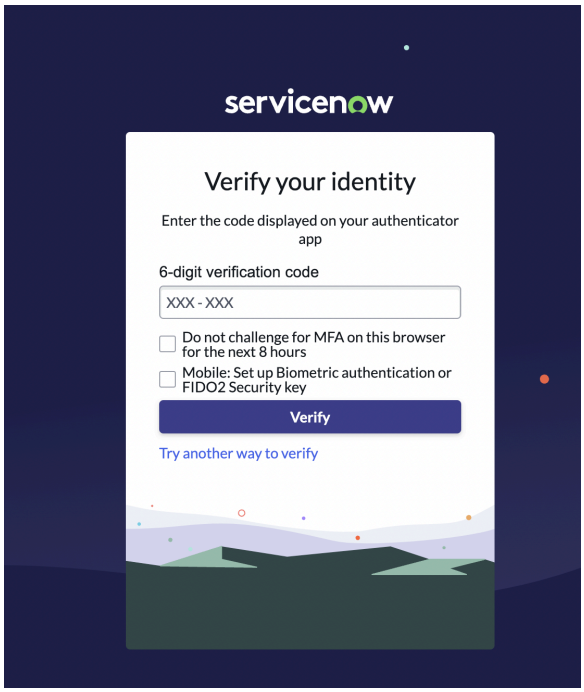
注:
リストにない他の認証システムも適合する可能性がありますが、ServiceNowではテストされていません。

注:
ブラウザ固有の動作の変更に関連する情報については、このナレッジベース記事 を参照してください。

管理者がインスタンスでマルチファクター認証 (MFA) を有効にしている場合は、ユーザー名とパスワードを入力した後に 2 番目の認証が要求されます。MFA ログインプロセスの詳細については、「マルチファクター認証によるログイン」を参照してください。 2 番目の認証フォームを設定していない場合は、ログイン後に設定ページが表示され、認証アプリの設定手順が示されます。このセットアップの詳細については、「初期ログイン時にマルチファクター認証を設定する」を参照してください。	認証アプリによる検証

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



認証アプリに表示されたコードを入力してログインします。

認証デバイスの登録

認証アプリを構成した後、他の認証方法を登録できます。

生体認証装置

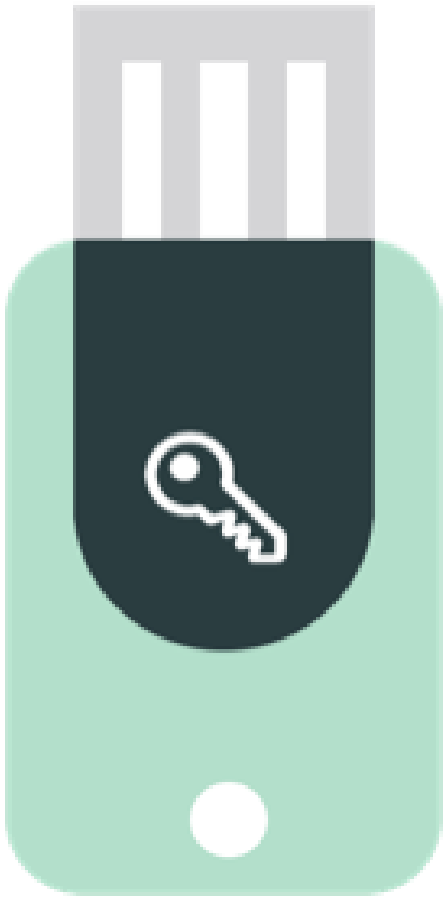
2 番目の MFA 認証として、指紋認証や顔認識などの生体認証を使用できます。管理者がこのオプションを許可している場合は、「生体認証装置の登録」の手順を使用して生体認証装置を設定できます。

ハードウェアキー認証システム

ハードウェアキーは、認証に使用できる物理的なセキュリティデバイスです。「ハードウェアセキュリティキーの登録」の手順を使用して、インスタンスで使用するハードウェアデバイスを登録できます。

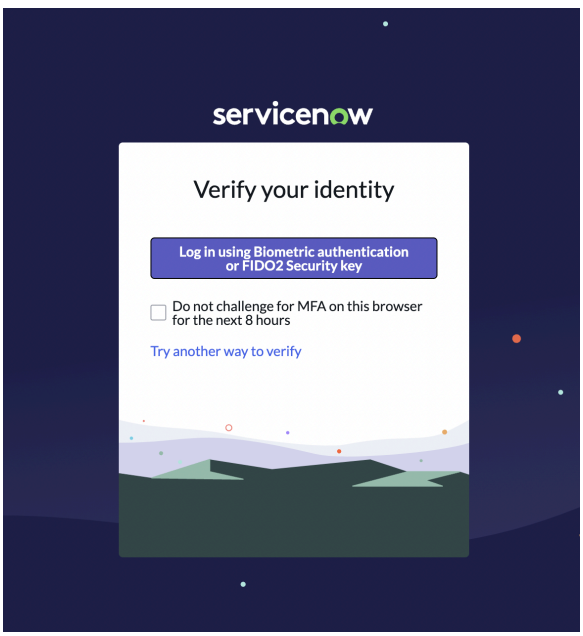
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



生体認証またはセキュリティキーを使用してログインします。

生体認証またはハードウェアキーを使用した検証



自動翻訳

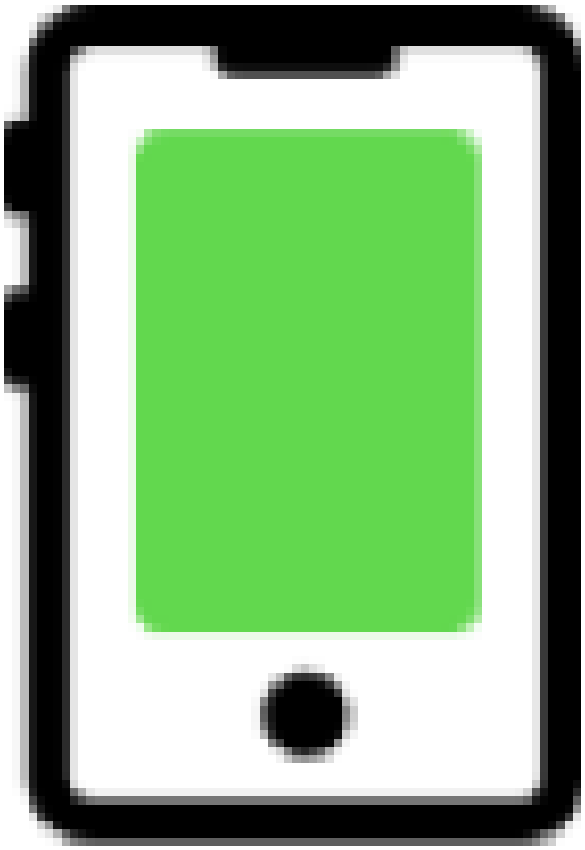
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

OTP 用の電話番号の登録

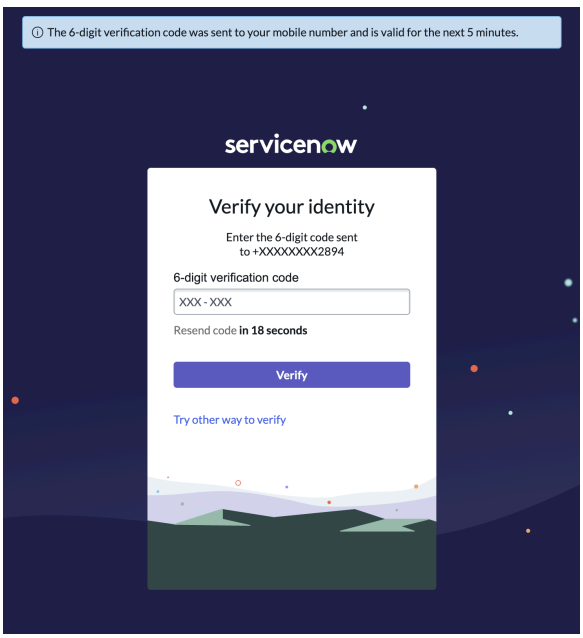
SMS

管理者は、インスタンスにログインしようとするユーザーに SMS ベースの OTP の使用を要求するように ServiceNow インスタンスを設定します。

ユーザーが ServiceNow にログインしようとすると、sys_user レコードに関連付けられた携帯電話番号に SMS OTP が送信されます。ユーザーは、モバイルデバイスに送信された 6 桁の検証コードを入力して本人確認を行うことができます。



SMS を使用した検証



携帯電話番号に送信された 6 桁のコードを入力してログインします。送信されたコードは 5 分間有効です。コードの再送信を使用してコードを再送信できます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

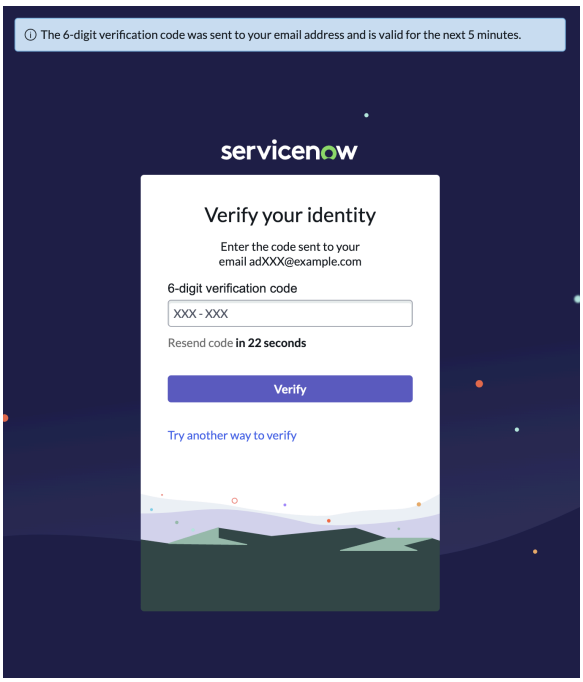
OTP のメールアドレスの登録

メールアドレス

管理者は、インスタンスにログインしようとするユーザーにメールベースの OTP の使用を要求するように ServiceNow インスタンスを設定します。

ユーザーが ServiceNowにログインしようとすると、メール OTP がユーザーに関連付けられているメールアドレスに送信されます。ユーザーは、モバイルデバイスに送信された 6 桁の検証コードを入力して本人確認を行うことができます。

メールを使用した検証



メールアドレスに送信された 6 桁のコードを入力してログインします。送信されたコードは 5 分間有効です。コードの再送信を使用してコードを再送信できます。

初期ログイン時にマルチファクター認証を設定する

管理者がプロファイルでマルチファクター認証を有効にしていても、アプリケーションをまだ設定していないという場合は、ログイン時に設定できます。

始める前に

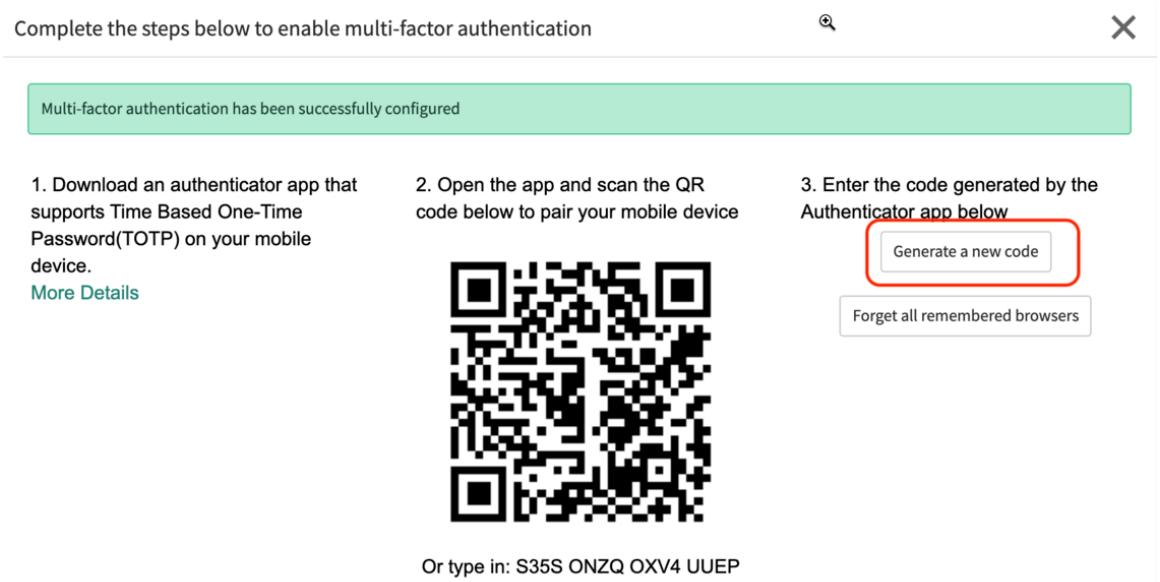
必要なロール：なし

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. ユーザー名とパスワードを使用してインスタンスにログインします。マルチファクター認証の設定画面がログインをインターセプトします。



2. ここで設定した認証をスキップする場合は、[バイパス設定] をクリックします。管理者が許可する限られた回数だけ、マルチファクター認証をバイパスできます。最終的には、マルチファクター認証を構成する必要があります。
3. Google Authenticator アプリケーションで QC コードの写真を撮るか、アプリケーションに文字列を手動で入力します。
4. コードを入力し、[デバイスをペアリングしてログイン **(Pair device and log in)]** をクリックします。

   アプリケーションは、30 秒ごとに更新される 6 桁のコードで応答します。正しいコードを入力すると、マルチファクター認証が設定されていることを示すメッセージが表示されます。無効なコードを入力した場合は、更新されている可能性があるため、モバイルデバイスでコードを再度検索し、表示されたコードを入力してください。

   注:
   コードが正しく機能するためには、コンピューターのシステム時刻がモバイル デバイスの時刻と同じタイムゾーンである必要があります。

ユーザープロファイルでのマルチファクター認証のセットアップ

ユーザープロファイル設定で、 アカウントのマルチファクター認証を有効にします。

始める前に

必要なロール：なし

インスタンスでマルチファクター認証を有効にする必要があります。

注:
管理者がマルチファクター認証の使用を要求する場合があります。この場合、ログインすると自動的にプロンプトが表示されます。「初期ログイン時にマルチファクター認証を設定する」を参照してください。管理者がマルチファクター認証のオプトインを許可している場合は、以下のプロセスを使用します。

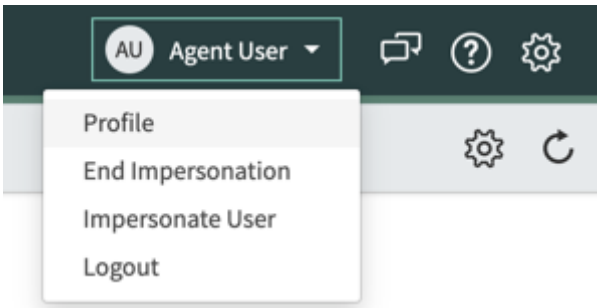
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

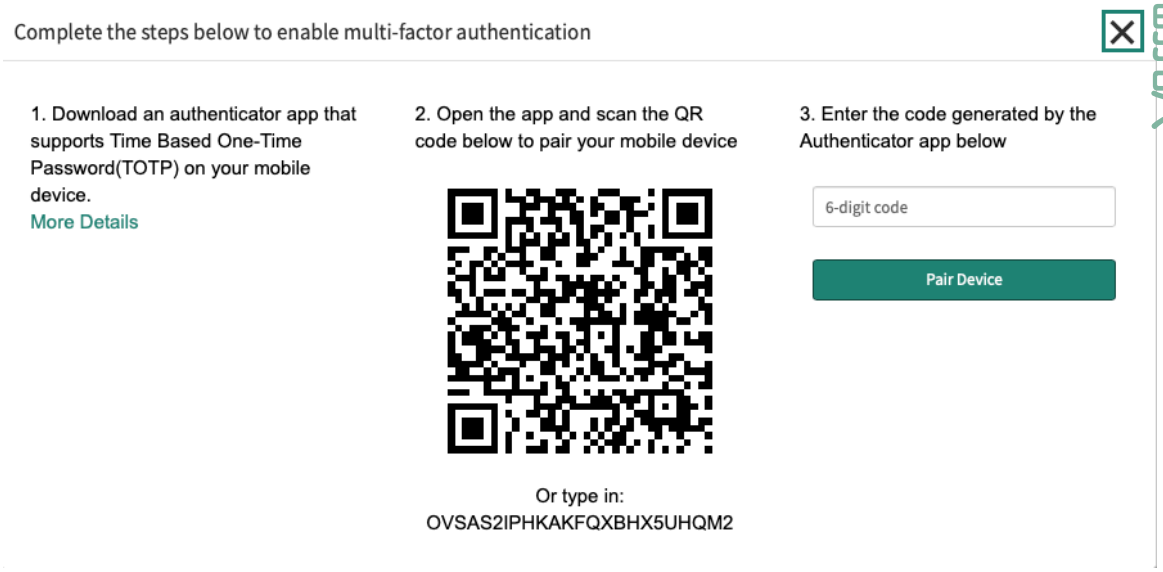
1. 移動先 すべて > セルフサービス > プロファイル.

   注:
   インスタンスヘッダーのユーザー名をクリックして、プロファイルにアクセスすることもできます。



2. ユーザープロファイルで、[関連リンク] セクションの [マルチファクター認証 **(Muti-factor Authentication)]** または [アカウント復旧の有効化] をクリックします。
3. 画面の指示に従って、認証アプリを登録します。ServiceNow は、モバイルアプリとブラウザー拡張機能の両方で認証システムをサポートしています。これらのアプリについての詳細は、「認証アプリケーション」を参照して ください。

   注:
   生体認証またはハードウェアキーを使用して認証する場合でも、最初に認証アプリを登録する必要があります。



タスクの結果
ユーザーアカウントでマルチファクター認証が有効になっています。次回ログイン時に、マルチファクター認証を使用するように求められます。

注:
アカウントでマルチファクター認証を有効にした後で、無効にすることはできません。マルチファクター認証を無効にする必要がある場合は、管理者にお問い合わせください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

次のタスク
ハードウェアキーまたは生体認証装置を使用してインスタンスにログインする場合に、これらの認証システムを登録できるようになりました。詳細については、「生体認証装置の登録」および「ハードウェアセキュリティキーの登録」を参照してください。

マルチファクター認証によるログイン

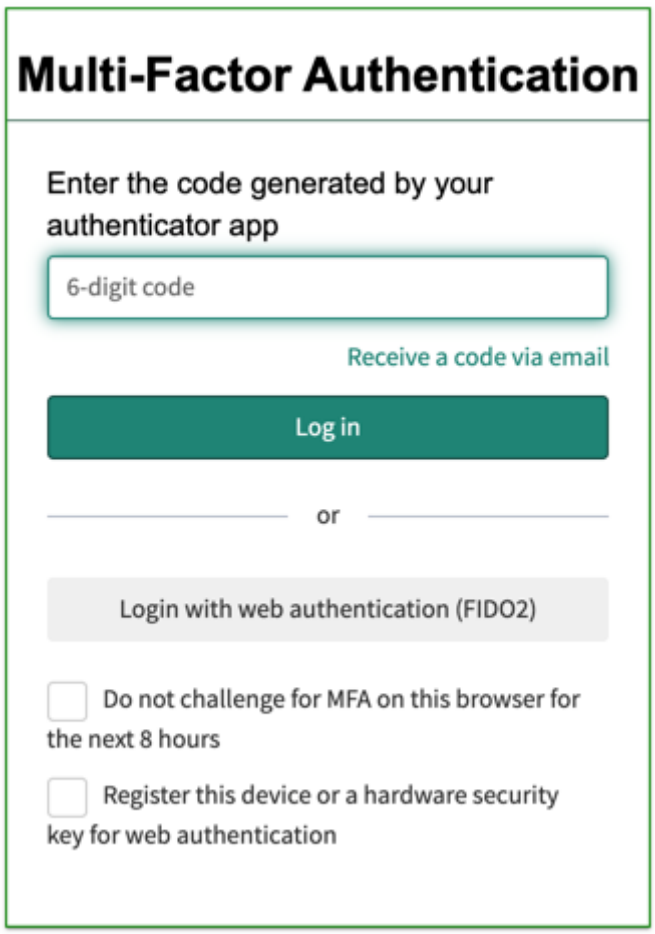
ユーザープロファイルに対してマルチファクター認証を有効にすると、Google Authenticator アプリから提供されるパスコードを追加してログインできます。

始める前に

プロファイルに対してマルチファクター認証を有効にする必要があります。ユーザープロファイルで自分で有効にすることも、管理者が有効にすることもできます。
必要なロール：なし

手順

1. インスタンスの URL に移動して、ログイン画面を開きます。
2. ユーザー名とパスワードを入力します。
3. [ログイン] をクリックします。
   マルチファクター認証画面が表示されます。



4. モバイルデバイスまたはブラウザー拡張機能で認証システムを開き、番号をメモします。この番号は 30 秒ごとに更新されます。
5. 6 桁の認証コードを入力します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

6. オプション: [次の **8** 時間このブラウザーで **MFA** に干渉しない **(Do not challenge for MFA on this browser for the next 8 hours)]** を有効にすると、その後 8 時間はログイン時に認証システムをスキップします。
7. オプション: **[Web** 認証用にこのデバイスまたはハードウェアセキュリティキーを登録します] を有効にして、ログインした後に生体認証デバイスまたはハードウェアセキュリティキーを登録します。
8. オプション: 生体認証スキャナーまたはハードウェアキーを既に登録している場合は、**[Web** 認証 **(FIDO2)** でログイン **(login with web authentication (FIDO2))]** をクリックし、プロンプトに従ってログインプロセスを完了します。
9. オプション: パスコードを忘れた場合、または認証システムへのアクセス権がない場合は、[メールでコードを受信] リンクをクリックします。

   インスタンスが一時的なパスコードをメールアドレスに送信します。この一時パスコードは 1 回のみ使用でき、10 分間のみ有効です。

   > **注:**
   > このメールメッセージを受信するには、インスタンスのユーザープロファイルにメールアドレスを設定する必要があります。

10. [ログイン] をクリックします。

認証アプリケーション

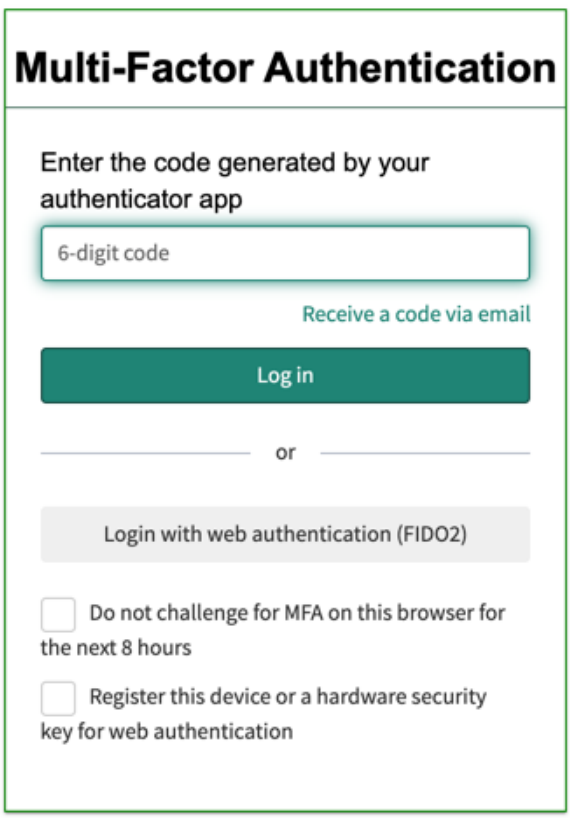
サードパーティの認証アプリケーションを使用して、一時的な MFA パスコードを生成します。

認証アプリケーションは、一時的なパスコードを生成するサードパーティソフトウェアです。これらのパスコードをパスワードとともに使用して、マルチファクター認証 (MFA) を必要とするインスタンスにログインできます。

管理者がインスタンスで MFA を有効にしている場合、ログイン中にユーザーとパスワードを入力するとパスコードの入力が求められます。

ServiceNow では、時間ベースのワンタイムパスワード (TOTP) をサポートする認証アプリケーションが必要です。ServiceNow は次の認証システムで MFA をテストします。

- Google 認証システム
- Microsoft 認証システム
- LastPass 認証システム
- Authy
- FreeOTP
- Duo
- Okta Verify



自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注:
リストにない他の認証システムも適合する可能性がありますが、ServiceNowではテストされていません。

認証アプリの変更

デバイスの認証アプリを変更するための新しいコードを生成します。

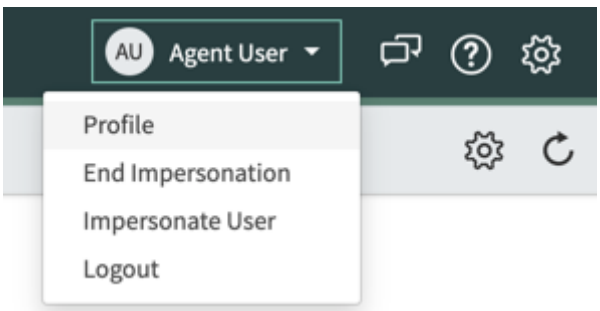
始める前に

プロファイルに対してマルチファクター認証を有効にする必要があります。ユーザープロファイルで自分で有効にすることも、管理者が有効にすることもできます。
必要なロール：なし

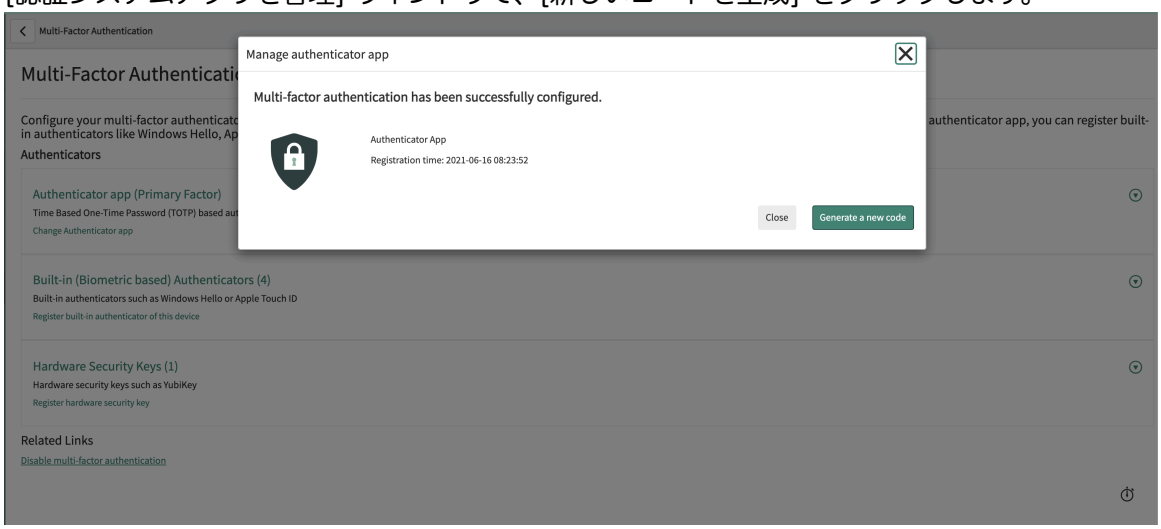
手順

1. 移動先 すべて > セルフサービス > プロファイル.

   注:
   インスタンスヘッダーのユーザー名をクリックして、プロファイルにアクセスすることもできます。



2. ユーザープロファイルで、[関連リンク] セクションの [マルチファクター認証 **(Muti-factor Authentication)]** をクリックします。
3. [認証アプリ (プライマリファクター)] で、[認証アプリを変更] をクリックします。
4. [認証システムアプリを管理] ウィンドウで、[新しいコードを生成] をクリックします。



5. 画面の指示に従って、認証アプリをデバイスに登録します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Web 認証

ユーザーは、ハードウェアキーまたはデバイスの生体認証リーダー (FIDO2) を使用して、インスタンスに対する認証を行うことができます。

ハードウェアキー

ハードウェアキーは、認証に使用できる物理ハードウェアです。ハードウェアキーをデバイスのポートに挿入して認証します。ハードウェアキーの登録の詳細については、「ハードウェアセキュリティキーの登録」を参照してください。

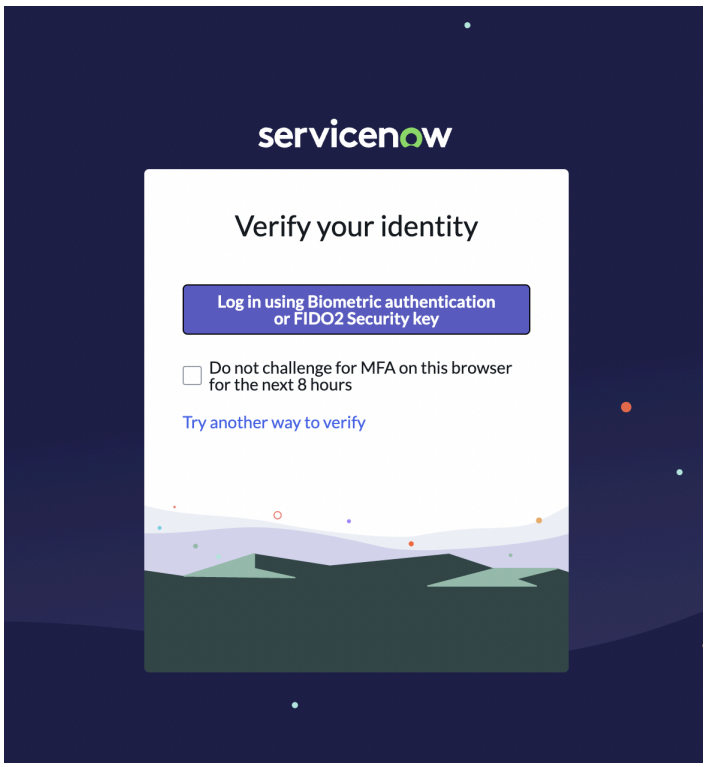
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

生体認証

生体認証装置は、指紋または顔認識を使用してユーザーを識別します。ユーザーは、マルチファクターログインプロセスの一部としてデバイスでこれらの認証システムを使用できます。生体認証装置の登録の詳細については、「生体認証装置の登録」を参照してください。

インスタンスに対する認証を行う第 2 要素を選択します。



Web 認証プラグインを設定するには、「Web Authentication プラグインのアクティブ化」を参照してください。

Web Authentication プラグインのアクティブ化

Web 認証 (FIDO2) を行うには、Integration - Web Authentication プラグインをアクティブ化する必要があります 。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

始める前に
必要なロール：admin

手順

1. 移動先 すべて > システムアプリケーション > 利用可能なすべてのアプリケーション > すべて.
2. フィルター基準と検索バーを使用して、**Integration - Web Authentication** (com.snc.integration.webauthn) プラグインを検索します。

   名前または ID でプラグインを検索できます。プラグインが見つからない場合は、ServiceNow 担当者から要求する必要があります。
3. [インストール] を選択して、[プラグインをアクティブにする] ダイアログボックスで、[アクティブ化] をクリックします。

   注:
   ドメイン分離と代理管理者がインスタンスで有効になっている場合、管理ユーザーはグローバルドメインに含まれている必要があります。それ以外の場合、次のエラーが表示されます： 別の操作が実行されているため、アプリケーションのインストールは利用できません：<プラグイン名> のプラグインの有効化。

生体認証装置の登録

マルチファクター認証ログインの一部として使用する生体認証装置を登録します。

始める前に
必要なロール：なし

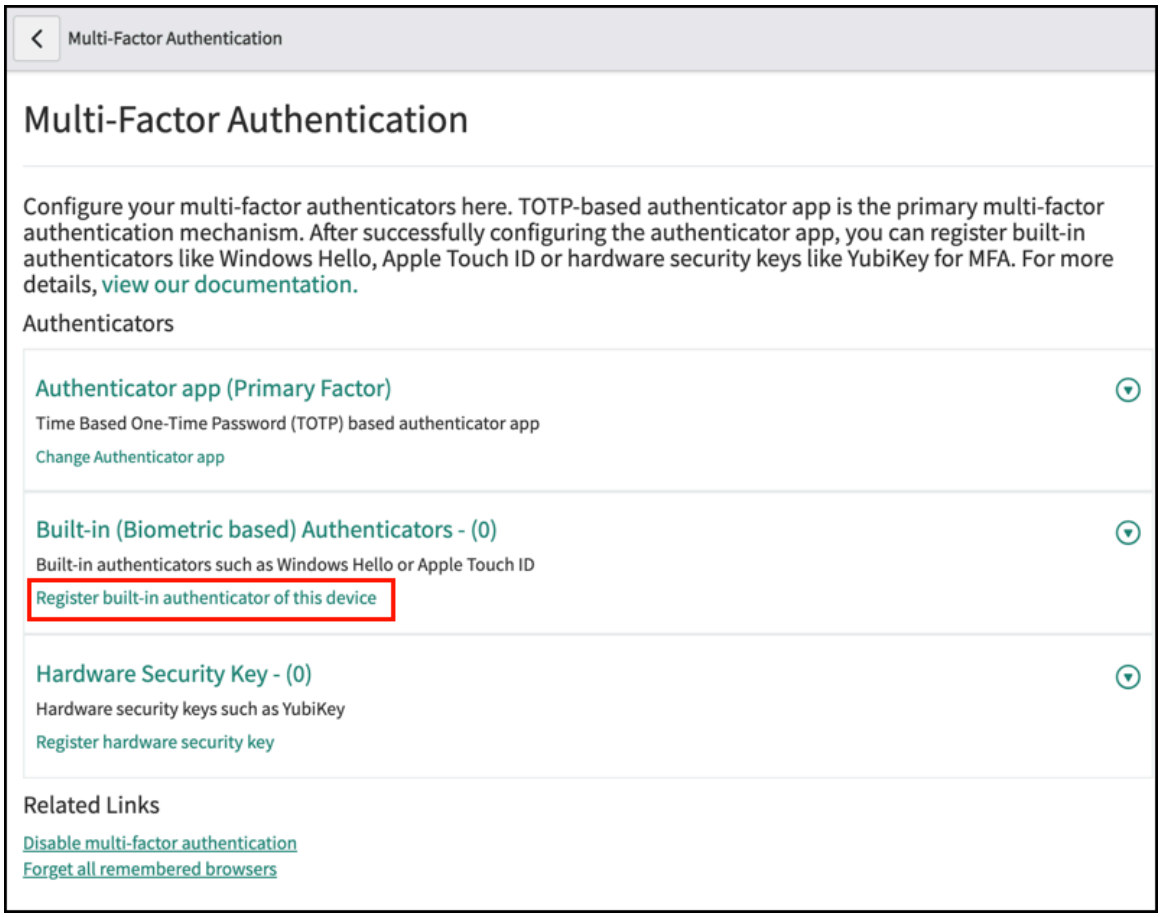
注:
ユーザーは、生体認証装置を設定する前に、まず認証アプリケーションを設定する必要があります。認証アプリケーションの設定の詳細については、「ユーザープロファイルでのマルチファクター認証のセットアップ」を参照してください。

手順

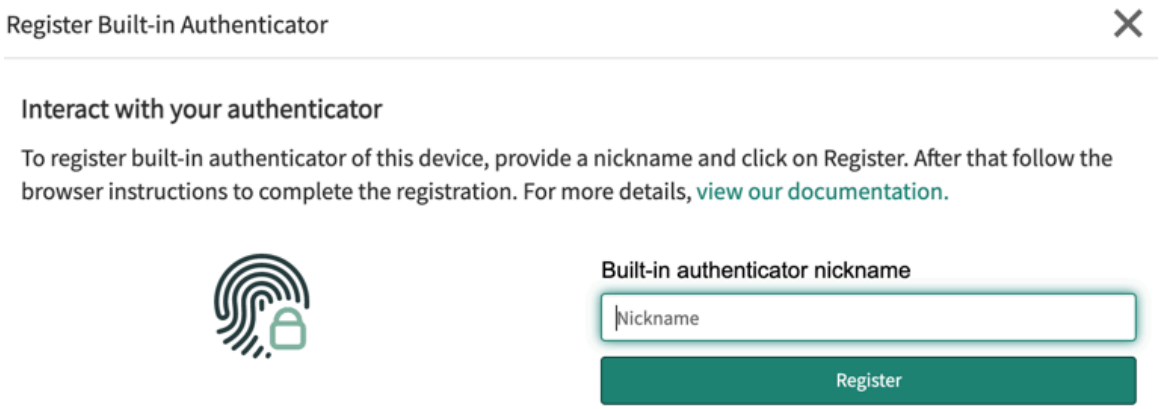
1. 移動先 すべて > セルフサービス > プロファイル.
2. [関連リンク] で、[マルチファクター認証] をクリックします。
   [マルチファクター認証] ページが開きます。
3. [このデバイスのビルトイン認証システムを登録] をクリックします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



4. 認証システムのニックネームを入力し、[登録] をクリックします。

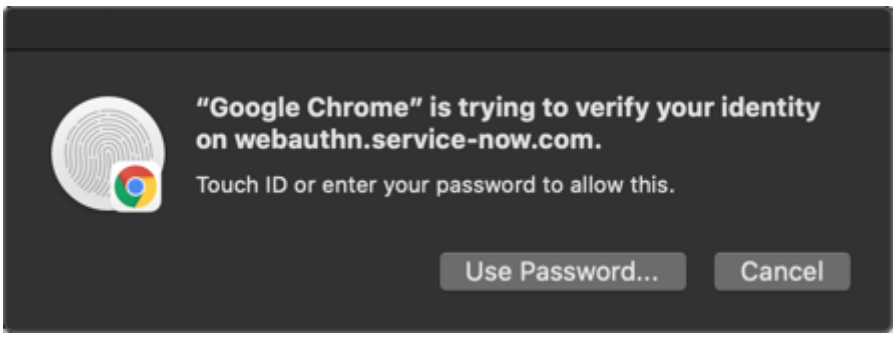


5. プロンプトが表示されたら、画面の指示に従って生体認証装置で認証します。
このメッセージは、個々の認証システムによって異なります。

自動翻訳

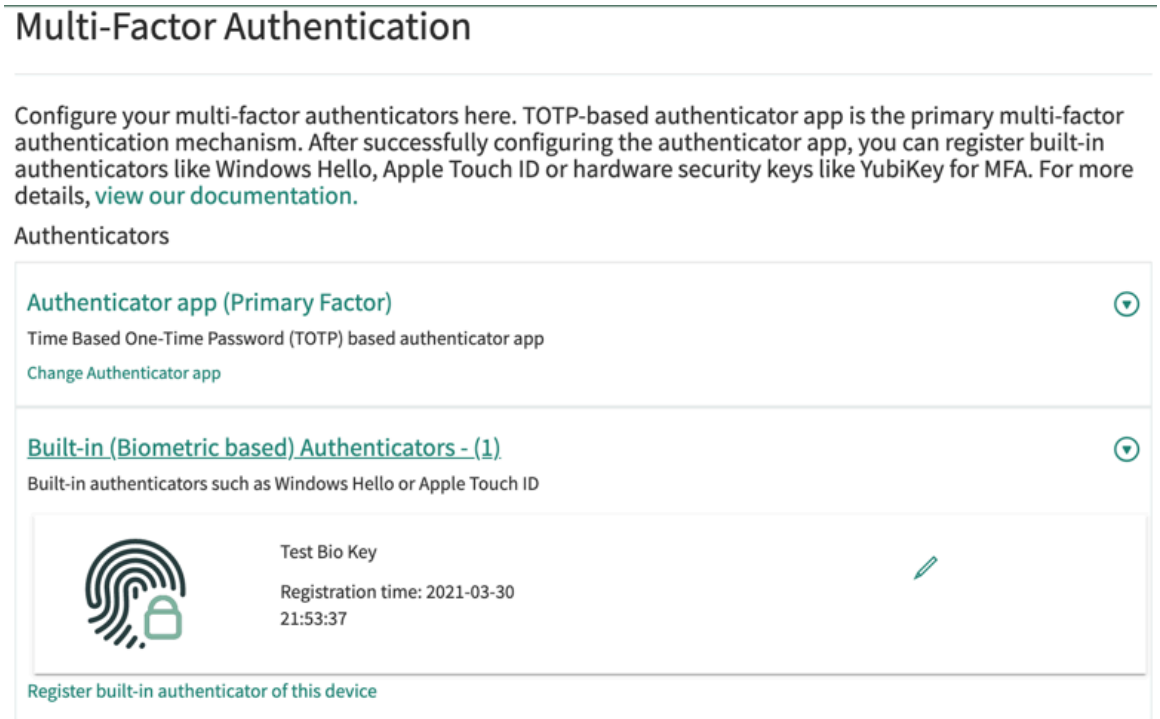
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

生体認証要求の例



6. 正常に認証されると、確認ウィンドウが表示されます。[X] をクリックして確認画面を閉じます。

タスクの結果
生体認証装置が登録されました。[マルチファクター認証] ページに認証システムのリストが表示されま



す。

ハードウェアセキュリティキーの登録

マルチファクター認証ログインの一部として使用するハードウェアキーを登録します。

始める前に
必要なロール：なし

> **注:**
> ユーザーは、ハードウェアキーを設定する前に、まず認証アプリケーションを設定する必要があります。認証アプリケーションの設定の詳細については、「ユーザープロファイルでのマルチファクター認証のセットアップ」を参照してください。

手順

1. 移動先 すべて > セルフサービス > プロファイル.

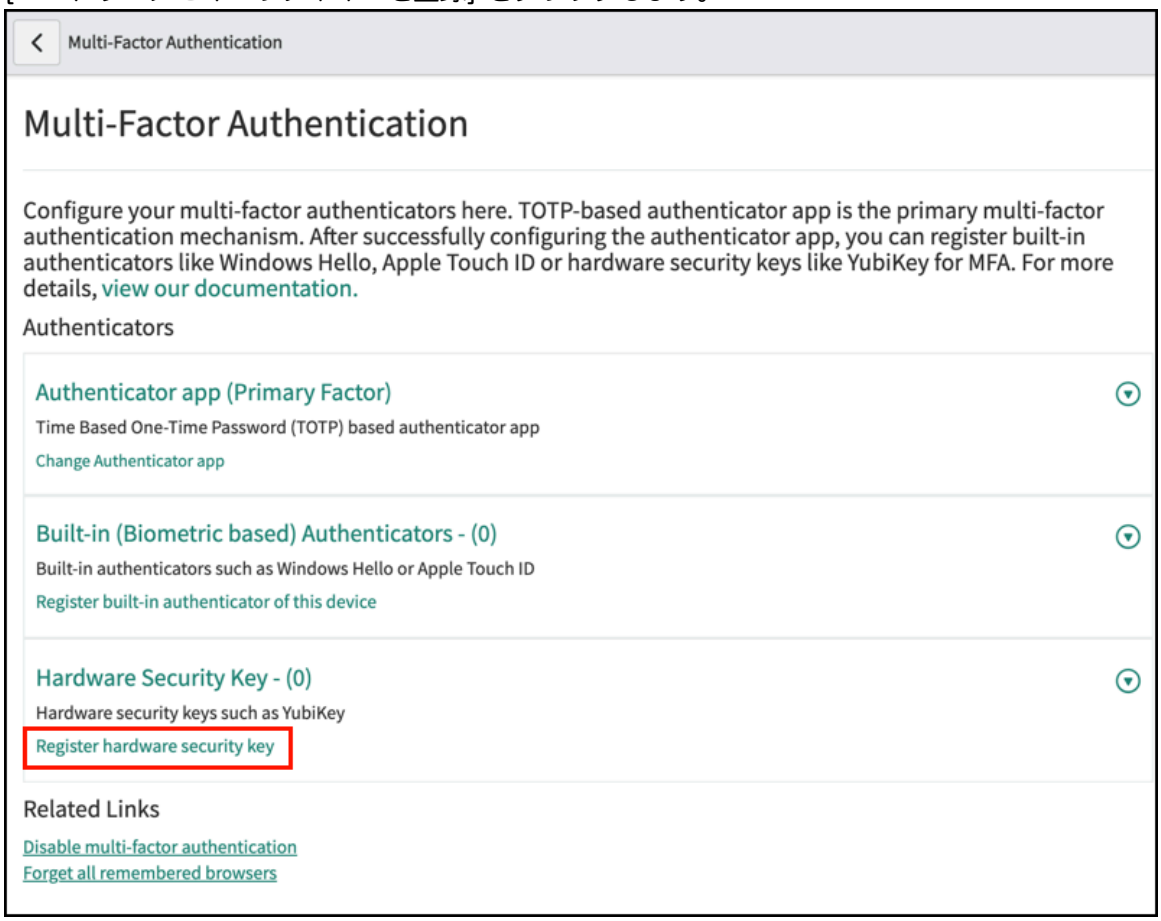
2. [関連リンク] で、[マルチファクター認証] をクリックします。

自動翻訳

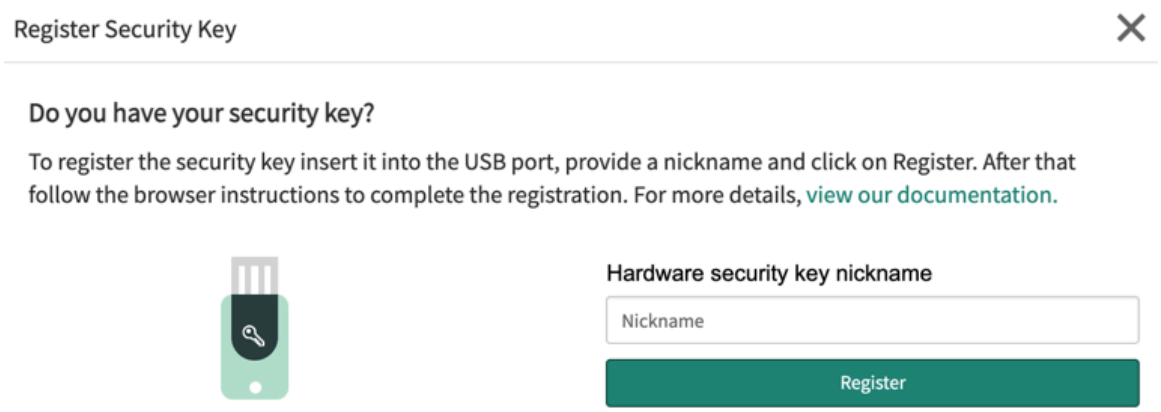
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

[マルチファクター認証] ページが開きます。

3. [ハードウェアセキュリティキーを登録] をクリックします。



4. ハードウェアキーのニックネームを入力し、[登録] をクリックします。



5. プロンプトが表示されたら、ハードウェアセキュリティキーを挿入してアクティブ化します。
6. 正常に認証されると、確認ウィンドウが表示されます。[X] をクリックして確認画面を閉じます。

タスクの結果
ハードウェアキーが登録されました。[マルチファクター認証] ページにキーがリスト表示されます。

Single Sign-on によるマルチファクター認証

ServiceNow インスタンスのマルチファクター認証 (MFA) を Single Sign-on (SSO) プロバイダーを使用して構成します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

組織内では多くのユーザーが企業ネットワークにログインして ServiceNow インスタンスにアクセスしているため、安全な認証の必要性はますます強くなっています。

MFA と SSO の組み合わせにより、インスタンスのセキュリティが強化されます。この機能は、ユーザーに対して条件付きで MFA を有効にする柔軟性を提供します。

注:

- ServiceNow MFA は、ID プロバイダーでの認証成功後にユーザーがリダイレクトされた後で適用されます。
- San Diego リリースより前の SSO では、MFA は適用されませんでした。

たとえば、外部ユーザーに追加のセキュリティプロトコルを付与する場合は、それらのユーザーにのみ MFA を適用できます。このようにして追加の認証機能を追加して、ユーザーアクセスを制御できます。

SAML、OpenID Connect、Digest などの SSO ベースのログインでは、認証に MFA を適用できます。

SSO を使用した MFA は、要件に基づいてオンデマンドで構成できます。認証スキームと ID プロバイダーを使用すると、特定のログインメカニズムで特定のユーザーに MFA を適用できます。

次の条件に対して MFA を適用できます。

- 認証スキーム
- ID プロバイダー

SSO を使用する MFA は、適応認証プラグイン (com.snc.adaptive_authentication) の一部として提供されます。適応認証の設定方法の詳細については、「適応認証」を参照してください。

SSO を使用した MFA の構成

組織内外のユーザーに対して、SSO で MFA を適用します。

始める前に

SSO 機能を使用する MFA は、適応認証プラグイン (com.snc.adaptive_authentication) の一部として提供されます。SSO 機能とともに MFA を使用するには、[適応認証] プロパティを有効にする必要があります。適応認証の設定方法の詳細については、「適応認証」を参照してください。

注:
glide.authenticate.mfa.with.multisso.enabled プロパティが **true** に設定されている場合は、SSO ログインを使用する MFA を使用できます。

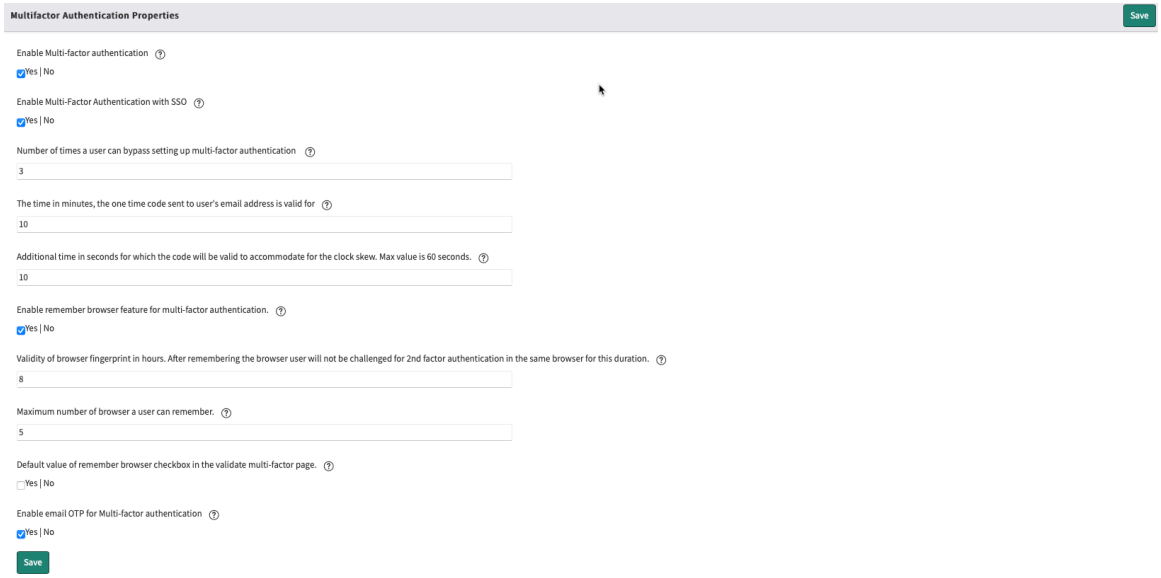
必要なロール：管理者

手順

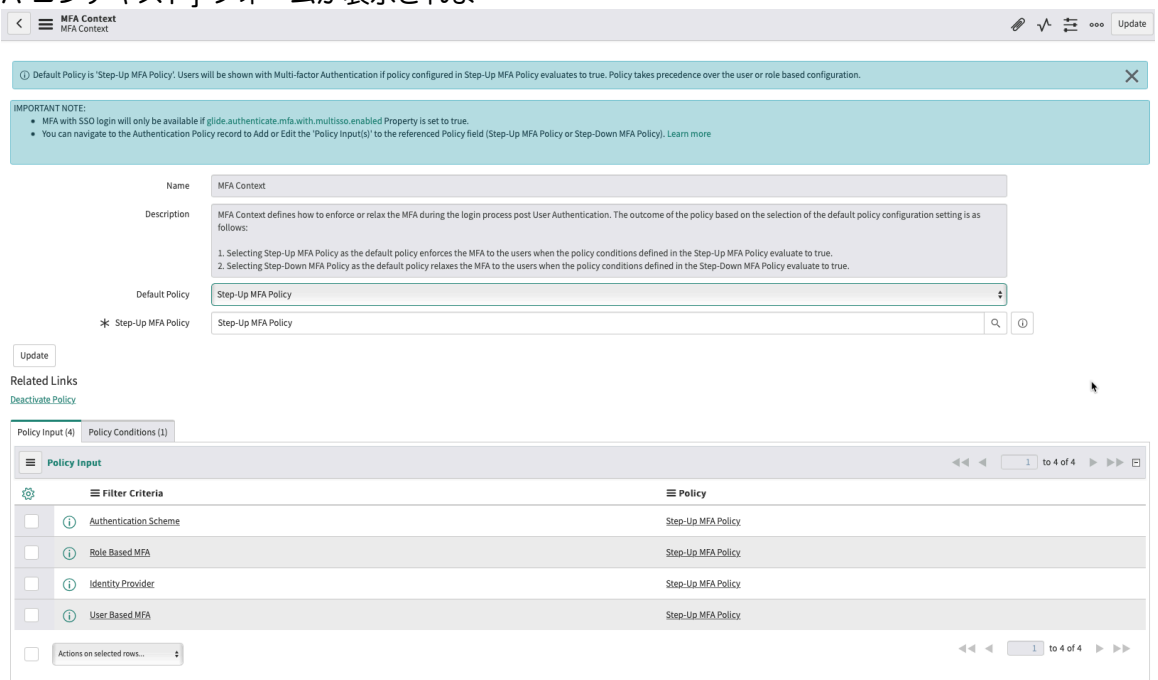
1. 移動先 すべて > マルチファクター認証 > プロパティ.
2. [マルチファクター認証を有効にする] および **[SSO** を使用したマルチファクター認証を有効にする] チェックボックスをオンにします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



3. [保存] をクリックします。
4. 移動先 マルチファクター認証 > **MFA** コンテキスト.
   [MFA コンテキスト] フォームが表示されま



す。

> **注:**
> デフォルトでは、ポリシーは [ステップアップ **MFA** ポリシー] です。[ステップアップ **MFA** ポリシー] で設定された条件が **true** と評価された場合、ユーザーにはマルチファクター認証が表示されます。ポリシーは、ユーザーまたはロールベースの構成よりも優先されます。

5. オプション: ポリシーを編集するには、[認証ポリシー] レコードに戻り、条件を変更してから戻ります。
   [認証ポリシー] レコードに移動する際に、参照されているポリシーフィールド ([ステップアップ **MFA** ポリシー] または [ステップダウン **MFA** ポリシー]) に対して「ポリシー入力」を追加または編集できます。
6. 新しいポリシー条件を設定するには、[ポリシー条件] をクリックします。
7. [新規] をクリックします。

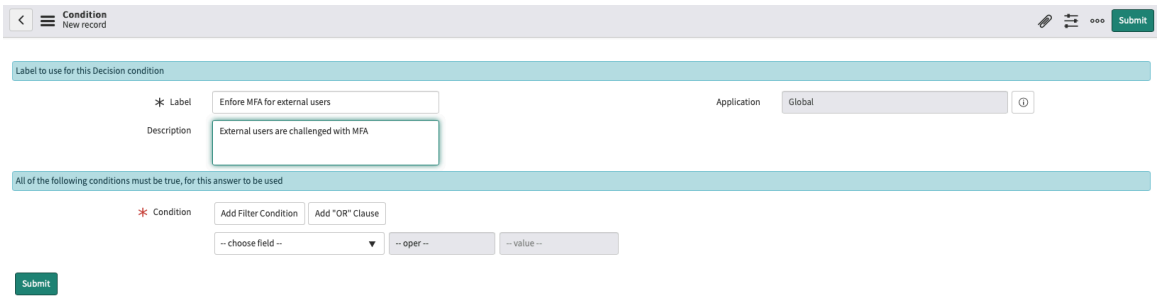
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

8. フォームのフィールドに入力します。

[条件] フォーム

フィールド	説明
ラベル	ラベルに対して作成する条件の一意の名前
説明	ポリシー条件の説明
条件	ポリシーに適用する条件のタイプ。フィルター条件と「OR」節を追加できます。 **注:** さまざまなフィルター条件と節を追加すると、特定のユーザーに MFA を要求することができます。



Example
条件を設定するには、次の例を検討してください。外部ユーザーの条件として ID プロバイダーを使用する認証スキームを設定したいとします。条件は次のように設定できます。

a. [認証スキーム] を選択し、基準を **[Single Sign-on]** または [ユーザー名とパスワード] として設定します。

この選択に基づいて、SSO ベースのログインまたはユーザー名とパスワードを指定するためのログインフォームがユーザーに表示されます。

b. **[ID** プロバイダー] を選択し、MFA を有効にする IDP レコードとしてプロバイダーを指定します。たとえば、**Okta** などです。

この選択に基づいて、ユーザーが SSO を使用してログインした場合、MFA からのチャレンジはありません。逆に、ユーザーが Okta を使用してログインすると MFA からのチャレンジがあります。

9. [送信] をクリックします。

関連情報

適応認証

MFA プラグインのアクティブ化

Single Sign-on によるマルチファクター認証

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

複数プロバイダーの Single sign-on (SSO)

外部 SSO を使用すると、組織内で複数の SSO ID プロバイダー (IdP) を使用して認証を管理し、同時にローカルデータベース (基本) 認証も保持できます。

統合は、単一のインスタンスでのローカル認証方法と外部認証方法をどのように組み合わせてもサポートします。

- SAML 2.0
- Digest Authentication
- OpenID Connect

複数プロバイダー SSO を設定するには、プロパティの設定、ID プロバイダー (IdP) の作成、SSO を使用するユーザーの設定など、いくつかの手順を実行する必要があります。

たとえば、世界中に拠点が分散している企業では、従業員に対して 1 つの SSO プロバイダー、ベンダーに対して別のプロバイダー、管理者に対してローカルデータベース認証が必要になることがあります。また、同じインスタンスに SAML 2.0 とダイジェストトークン認証ソリューションを実装するような会社もあります。

複数プロバイダー SSO のプロパティ、テーブル、およびスクリプト

Integration - Multiple Provider Single Sign-On Installer プラグインには、次のようなシステムプロパティ、テーブル、およびスクリプトが含まれています。

プロパティ

複数プロバイダー SSO は、次のシステムプロパティを追加します。

複数プロバイダー SSO のプロパティ

名前	説明
glide.authenticate.multisso.debug	複数プロバイダー SSO 統合のデバッグログを有効 (true) または無効 (false) にします。 • タイプ：true | false • デフォルト値：false
glide.authenticate.multisso.enabled	複数プロバイダー SSO を有効 (true) または無効 (false) にします。 • タイプ：true | false • デフォルト値：false

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

複数プロバイダー **SSO** のプロパティ (続く)

名前	説明
	注: インスタンスでアカウント復旧 (ACR) が有効になっている場合、このプロパティを false に設定しても、マルチプロバイダー SSO は無効になりません。ユーザー名とパスワードでログインするには、*glide.sso.acr.enabled* プロパティを使用して ACR も無効にする必要があります。このプロパティの詳細については、「アカウント復旧プロパティ」を参照してください。
glide.authenticate.multissov2_feature.enabled	このプロパティは、MultiSSOv2 バージョンがインスタンスで有効になっているかどうかを決定します。

テーブル

複数プロバイダー SSO は、以下のテーブルを追加します。

複数プロバイダー **SSO** のテーブル

名前	説明
SSO プロパティ [sso_properties]	各 IdP、スキーマ、共通 SSO データなどを保存します。
SAML 2 Update 1 プロパティ [saml2_update1_properties]	SAML 2.0 Update 1 の構成データ (SAML 証明書など) を保存します。
ダイジェストプロパティ [digest_properties]	ダイジェストトークン認証の構成データを保存します。
SSO フェデレーション [sso_fedation]	各 SSO フェデレーションのデータを保存します。
OIDC ID プロバイダー [oidc_identity_provider]	Open ID Connect ベースの ID プロバイダーのデータを保存します。

スクリプト

複数プロバイダー SSO は、以下のスクリプトを追加します。

複数プロバイダー **SSO** スクリプト

名前	説明
MultiSSO	顧客が会社ごとに SSO タイプを定義できるようにします。
MultiSSOLogin	各ドメインが独自のログインスクリプトを保持できるようにします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

複数プロバイダー **SSO** スクリプト (続く)

名前	説明
MultiSSOLogout	各ドメインが独自のログアウトスクリプトを保持できるようにします。
MultiSSO_OIDC_custom	ユーザーが OIDC 接続のカスタム Single Sign-on スクリプトを定義できるようにします。
MultiSSO_OIDC_logout_custom	ユーザーが OIDC 接続のカスタムログアウトスクリプトを定義できるようにします。
MultiSSO_Abstract_Core	すべての複数プロバイダー SSO クラスの基底クラスを提供します。
MultiSSO_ClientHelper	複数プロバイダー SSO 用のクライアントコール可能ユーティリティ関数を提供します。
MultiSSO_DigestedToken	ダイジェストトークン認証の基本システムロジックを提供します。
MultiSSO_SAML2_Update1	マルチテナント Single Sign-on 用の SAML 2.0 Update 1 認証を処理するロジックを提供します。

Multi-Provider SSO プラグインのアクティブ化

この統合には、 Integration - Multiple Provider Single Sign-On Installer プラグイン (com.snc.integration.sso.msoi.installer) が必要です。

始める前に
必要なロール：admin

com.snc.integration.sso.multi.installer プラグインは、OIDC、SAML、および Digest にも使用できます。

必要なロール：admin

手順

1. 移動先 すべて > システムアプリケーション > 利用可能なすべてのアプリケーション > すべて.
2. フィルター基準と検索バーを使用して、Integration - Multiple Provider Single Sign-On Installer プラグイン (com.snc.integration.sso.msoi.installer) を見つけます。

   名前または ID でプラグインを検索できます。プラグインが見つからない場合は、ServiceNow 担当者から要求する必要があります。
3. [インストール] を選択して、[プラグインをアクティブにする] ダイアログボックスで、[アクティブ化] をクリックします。

   注:
   ドメイン分離と代理管理者がインスタンスで有効になっている場合、管理ユーザーはグローバルドメインに含まれている必要があります。それ以外の場合、次のエラーが表示されます： 別の操作が実行されているため、アプリケーションのインストールは利用できません：<プラグイン名> のプラグインの有効化。

複数プロバイダー **SSO** の設定

複数プロバイダー SSO を設定するには、プロパティの設定、ID プロバイダー (IdP) の作成、SSO を使用するユーザーの設定など、いくつかの手順を実行する必要があります。

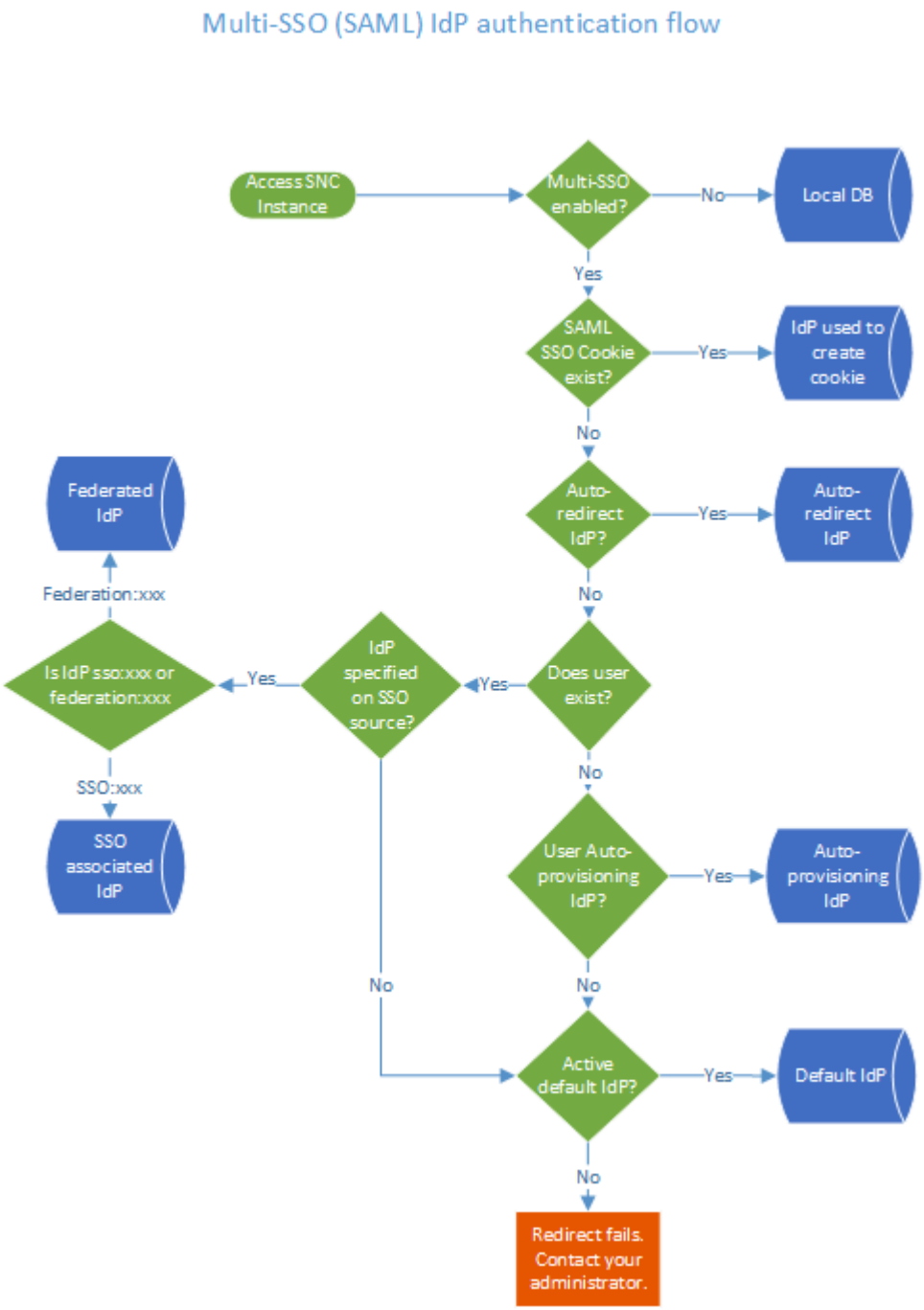
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

複数プロバイダー **SSO (SAML) IdP** 認証フロー

SAML マルチ SSO を介してユーザーを認証できるさまざまなエンティティについて説明します。

認証フローに従うと、エンティティがマルチ SSO を使用してユーザーを認証するタイミングを把握できます。



ローカル DB
: マルチ SSO が有効になっていない場合、認証はローカル DB に送信されます。

SAML SSO Cookie IdP
: SAML SSO cookie が存在する場合、この cookie で指定された IdP がユーザーを認証します。

自動リダイレクト IdP
: 自動リダイレクト IdP が有効になっている場合、この IdP がユーザーを認証します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フェデレーション IdP

ユーザーのブラウザーが外部認証 (login_locate_sso.do) のログイン画面にリダイレクトされ、**[SSO** ソース] フィールドで IdP が [フェデレーション：xxx (federation:xxx)] に設定されたユーザーがユーザーテーブル内に存在する場合、フェデレーション IdP がユーザーを認証します。

関連 IdP

ユーザーのブラウザーが外部認証 (login_locate_sso.do) のログイン画面にリダイレクトされ、**[SSO** ソース] フィールドで IdP が [SSO：xxx] に設定されたユーザーがユーザーテーブル内に存在する場合、関連 IdP がユーザーを認証します。

自動プロビジョニング IdP

ユーザーのブラウザーが外部認証 (login_locate_sso.do) のログイン画面にリダイレクトされ、ユーザーテーブル内にユーザーが存在しないが自動プロビジョニングが有効になっている場合は、自動プロビジョニング IdP がユーザーを認証します。

> **注:**
> 複数の自動プロビジョニング IdP が有効になっている場合、ユーザーは使用可能な自動プロビジョニング IdP を選択できます。

デフォルト IdP

ユーザーのブラウザーが外部認証 (login_locate_sso.do) ログイン画面にリダイレクトされ、ユーザーが次のいずれかの場合：

- ユーザーテーブル内に存在せず、自動プロビジョニングが有効になっておらず、アクティブなデフォルト IdP がある場合
- ユーザーテーブル内に存在し、SSO ソースユーザーまたは会社レコードに IdP が指定されておらず、アクティブなデフォルト IdP がある場合

デフォルトの IdP がユーザーを認証します。

マルチプロバイダー **SSO** プロパティの設定

SSO プロパティを設定し、さらにシステムのプロパティテーブルにプロパティを追加して IdP 包含リストを設定します。

始める前に

必要なロール：管理者

手順

1. 移動先 すべて > マルチプロバイダー **SSO** > 管理 > プロパティ.
2. [マルチプロバイダー **SSO** の有効化 **(Enable Multi-Provider SSO)]** チェックボックスをオンにします。
   この選択により、[外部ログインを使用] リンクがログインページに追加されます。
3. IdP のユーザーでユーザーテーブルを更新するには、[自動インポートの有効化 **(Enable Auto Importing)]** オプションを選択します。
4. コンテンツフレームの下部にデバッグメッセージを表示できるようにするには、[マルチプロバイダー **SSO** 統合のデバッグログの有効化 **(Enable debug logging for the Multi-Provider SSO integration)]** チェックボックスをオンにします。
   有効にすると、デバッグログ機能によってパフォーマンスが低下し、ログ生成のためにディスクスペースが使用されます。
5. [ユーザー **ID** ログインページへのアクセス時にユーザーを識別するユーザーテーブル上のフィールド **(The field on the user table that identifies a user accessing the User identification login**

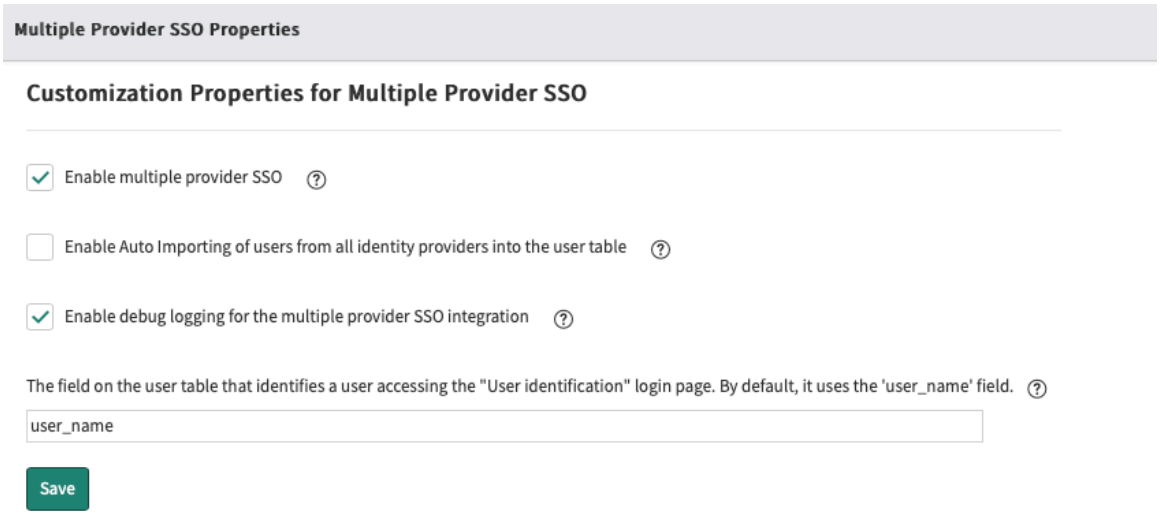
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

page)] プロパティで、IdP がユーザーを識別するために使用する値を含むユーザーテーブルのフィールドを入力します。デフォルト値は **user_name** です。

デフォルト値は **user_name** です。

マルチプロバイダー **SSO** のプロパティ



6. [保存] をクリックします。
7. ユーザーがインスタンスにログインするときには、[外部ログインを使用] リンクをクリックするように指示してください。

関連情報

SAML ユーザープロビジョニング

外部 **ID** プロバイダーの作成

複数プロバイダー SSO プロパティを設定した後、SAML 2.0 またはダイジェストトークン ID プロバイダーを更新または作成できます。

始める前に

必要なロール：管理者

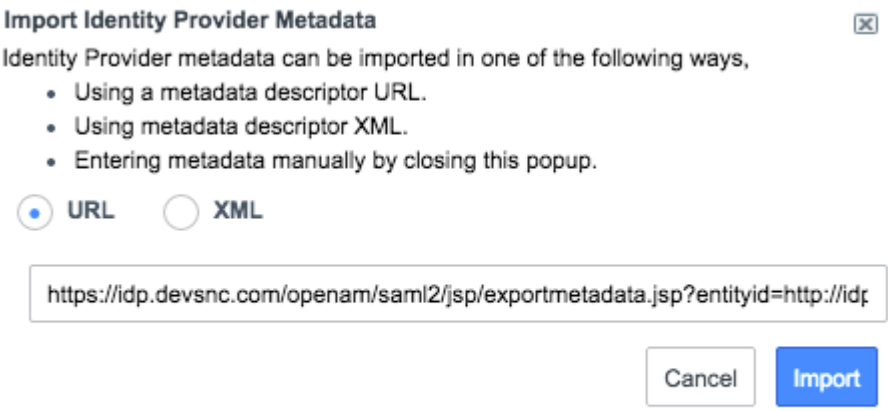
手順

1. 移動先 すべて > マルチプロバイダー **SSO** > **ID** プロバイダー.
2. ID プロバイダー レコードを編集するには、レコードをクリックします。
   - ダイジェストトークン構成の場合は、プロパティを手動で更新します。
   - SAML2 Update 1 構成の場合は、**[ID** プロバイダーのメタデータをインポート] 関連リンクを使用して ID プロバイダーのメタデータを自動的に更新するか、プロパティを手動で更新します。
   - OpenID Connect 構成の場合は、プロパティを手動で更新します。
3. 新しい ID プロバイダーを作成するには、[新規] をクリックします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- ダイジェストトークン構成の場合：**[SSO をダイジェスト (Digest SSO)]** をクリックし、複数プロバイダー Single Sign-on のダイジェストプロパティを入力します。
- SAML2 構成の場合：**[MultiSSOV2_SAML2_custom]** をクリックし、URL から ID プロバイダーのメタデータを XML としてインポートするか、ID プロバイダー情報を手動で入力します。



- OpenID Connect の場合：**[OpenID Connect]** をクリックし、クライアント ID、クライアントシークレット、および既知の構成 URL を入力します。

4. IdP をフェイルオーバー IdP (デフォルトの IdP が利用できない場合に使用される) にするには、[デフォルト] チェックボックスをオンにします。

   SAML 2 Update 1 をアクティブにして Fuji リリースにアップグレードすると、SAML 2 Update 1 IdP がデフォルトのフェイルオーバーとして選択されます。新しいインスタンスの場合、または SAML 2 Update 1 がアクティブでないリリースからアップグレードする場合は、デフォルトのフェイルオーバー IdP は選択されていません。

   注:
   メタデータのインポートプロセスでは、ID プロバイダーの証明書レコードが自動的に作成されます。**x509** 証明書モジュールに移動して、証明書を表示します。

   注:
   Single Sign-on の証明書は、SAML 証明書を扱うため、常に PEM 形式になっている必要があります。

5. 電子署名がアクティブな場合は、[ID プロバイダー] フォームを設定し、**[eSignature** 認証用のアサーションコンシューマー **URL]** フィールドを追加します。
   ほとんどの場合、この URL は https://YOURINSTANCE.service-now.com/consumer.do です。ただし、電子署名の SAML 認証を処理する方法をカスタマイズして使用する場合は、独自のコンシューマー URL を設定できます。SAML 2.0 Update 1 のみを使用しており、複数プロバイダー Single Sign-on を使用していない場合は、電子署名の SAML プロパティを使用してアサーションコンシューマー URL を設定します。

SAML のインスタンスサービスプロバイダー (SP) メタデータの生成

SSO 構成の一部として、インスタンス SP メタデータを生成して IdP に提供できます。

始める前に
必要なロール：管理者

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

このタスクについて
IdP には、要求の認証と転送を行うためにインスタンスの SP メタデータが必要です。

手順

1. インストールされている SSO プラグインを選択します。

オプション	説明
マルチプロバイダー SSO	移動先 マルチプロバイダー **SSO** > **ID** プロバイダー. IdP を選択し、[メタデータを生成] ボタンをクリックします。統合により、システムプロパティ設定からインスタンスの SP メタデータが自動的に生成されます。
SAML 2 SSO	移動先 **SAML 2** シングルサインオン > メタデータ. 統合により、システムプロパティ設定からインスタンスの SP メタデータが自動的に生成されます。

2. テキストボックスに SP メタデータをコピーします。

例：

```
<EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata"
 entityID="https://yourinstance.service-now.com">
  <SPSSODescriptor AuthnRequestsSigned="false" WantAssertionsSigned="true"
 protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
  <SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
 Location="https://yourinstance.service-now.com/navpage.do" />

 <NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress</NameIDFor
mat>
  <AssertionConsumerService isDefault="true" index="0"
 Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
 Location="https://yourinstance.service-now.com/navpage.do" />
  <AssertionConsumerService index="1"
 Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
 Location="https://yourinstance.service-now.com/consumer.do"/>
 </SPSSODescriptor>
</EntityDescriptor>
```

3. インスタンス SP メタデータを IdP に提供します。
たとえば、SSOCircle を使用すると、ユーザーは SP メタデータをオンラインで提供できます。

複数プロバイダー **SSO** のユーザーの構成

管理者は、会社に所属する個別のユーザーまたはユーザー全員に対して複数プロバイダー SSO を構成できます。グループに対して複数プロバイダー SSO を構成することはできません。

始める前に
必要なロール：管理者

手順

1. 移動先 すべて > マルチプロバイダー **SSO** > **ID** プロバイダー.

2. ID プロバイダーのレコードを右クリックし、**[sys_id** のコピー] を選択します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

3. データをクリップボードにコピーします。
4. ユーザーレコードまたは会社レコードに移動します。
5. フォームを設定し、**[SSO** ソース] フィールドを追加します。
6. **[SSO** ソース] フィールドに、次のいずれかを入力します。
   - **SAML** ユーザー：「**sso:**」に続けて ID プロバイダーのレコードの sys_id を入力します。
   - **SSO** フェデレーション ユーザー：「**federation:**」に続けてフェデレーションレコードの sys_id を入力します。
7. [更新] をクリックします。

IdP 接続のテスト

IdP への接続をテストすると、外部認証を有効にする前に設定が検証されます。

始める前に

必要なロール：管理者

このタスクについて

Jakarta リリースでは、ポップアップウィンドウ内のテスト接続をサポートしています。このオプションで IdP が正しく機能しない場合は、このデフォルト設定をオフにできます。
MultiSSO IDP メタデータのリフレッシュジョブは、接続の作成、更新、またはテスト中に IdP の証明書をフェッチして更新します。

> **注:**
> 一部の idp ケースでは、テスト接続に失敗した場合、値が false の glide.authenticate.multisso.test.connection.mandatory を作成する必要があります。作成すると、テスト接続なしで idp をアクティブ化することができます。

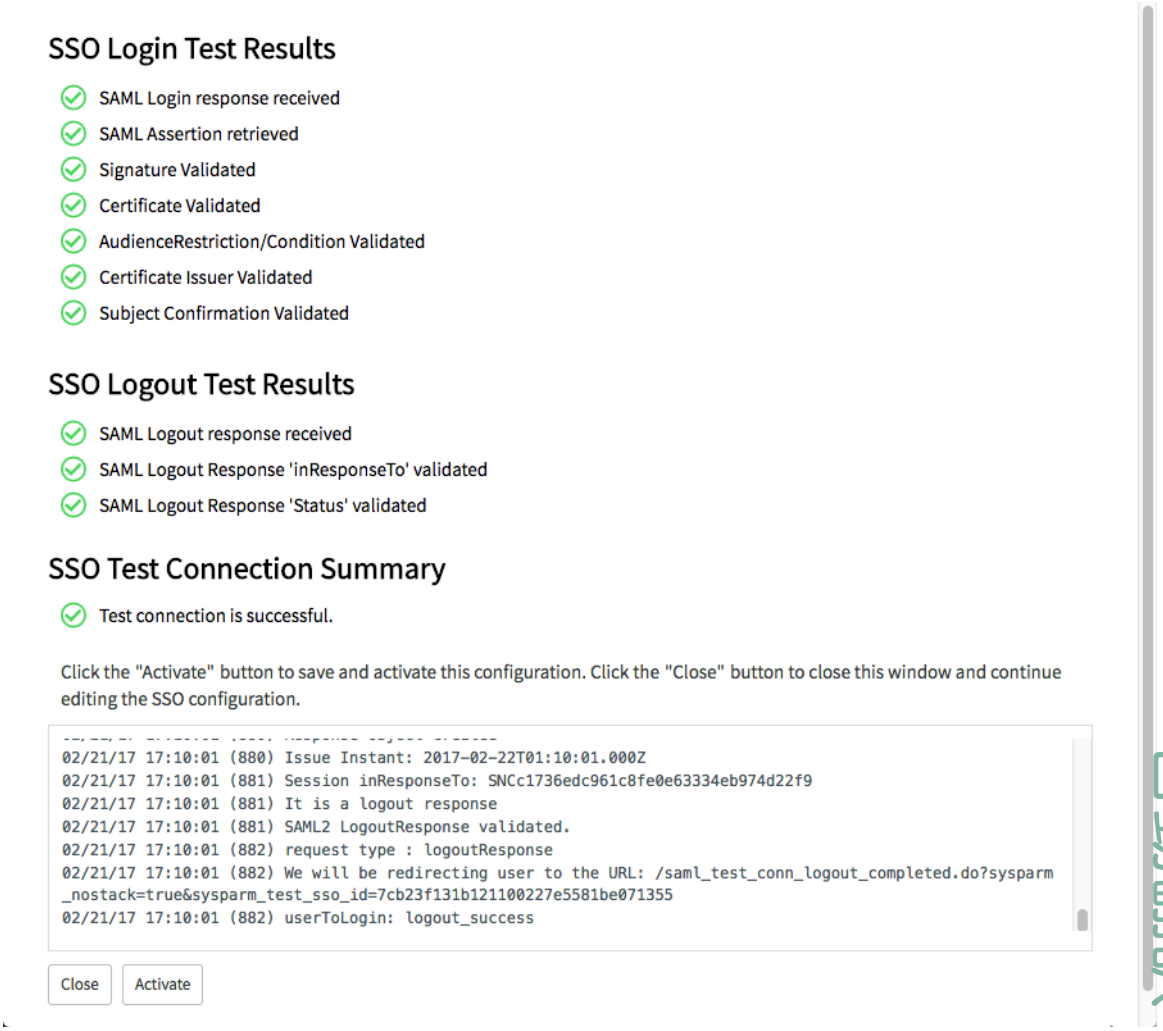
手順

1. 移動先 すべて > マルチプロバイダー **SSO** > **ID** プロバイダー.
2. 定義済みの IdP を選択するか、[新規] をクリックして新しい IdP を定義します。
3. オプション: 新しい IdP を設定する場合は、ID プロバイダーを構成します。
4. [テスト接続] をクリックし、IdP のログイン資格情報を入力してログインを確認します。
   テスト接続が成功するまで、IdP をアクティブ化することはできません。テストに失敗した場合は、構成情報を更新して保存できますが、この構成をアクティブ化することはできません。
5. **[SSO** テスト結果/サマリー **(SSO Test Results/Summary)]** または **[SSO** ログのテスト中] セクションを使用してログメッセージを表示して、結果を確認します。
   エラーが発生した場合は、「マルチ SSO (SAML 2.0) のエラーと修正」を参照してください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

6. テストが完了したら [キャンセル] をクリックします。



一般的な IdP 接続エラー

次の表では、一般的な IdP 接続エラーとその解決策について説明します。

IdP テスト接続のトラブルシューティング

エラーメッセージ	解決策
ユーザーフィールドの検証に失敗しました。無効なユーザーフィールド「<フィールド名>」は sys_user テーブルのフィールドではありません。(Invalid User Field '<field name>' is not a field on sys_user table.)	選択したユーザーテーブルフィールドの内容が SAML NameID トークンと一致していることを確認します。
アサーションの発行者が無効です。	**[ID プロバイダー URL]** に IdP への有効な URL が含まれていることを確認します。各 IdP URL は一意である必要があります。
AudienceRestriction の検証に失敗しました。	[対象者 **URI]** にインスタンスへの有効な URL が含まれていることを確認します。
IdP のセッションからログアウトできません。	**SingleLogoutRequest** URL に IdP のログアウトサービスへの有効な

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

IdP テスト接続のトラブルシューティング (続く)

エラーメッセージ	解決策
	URL が含まれていることを確認します。
署名が資格情報のキーに対して検証されませんでした。(Signature did not validate against the credential's key.)	IdP に有効な証明書がインストールされていることを確認します。

マルチ **SSO (SAML 2.0)** のエラーと修正

マルチ SSO (SAML 2.0) のセットアップと構成に関する一般的なエラーと関連する修正のリスト。

マルチ **SSO (SAML 2.0)** セットアップ中のエラー

インスタンスログのエラー	テスト接続メッセージ	**SAML** プロパティ	診断	修正
NotAfter：<Thu Jun 05 22:57:44 PDT 2014>	IDP x509 証明書が存在し、有効かつアクティブであることを確認してください。	適用外	現在の証明書または SAML アサーションの有効期限が切れました。	• SNC クロックを SAML IdP サーバークロックと同期します。 • SAML 2.0 証明書レコードを更新します。
• SAML 2.0 証明書を特定できません。 • ServiceNow インスタンスに保存されているデジタル署名が見つかりませんでした。(Could not find a digital signature stored in the ServiceNow instance.)	IDP x509 証明書が存在し、有効かつアクティブであることを確認してください。	PEM 形式の文字列を [PEM 証明書] フィールドに入力する必要があります。	SAML 証明書が存在しません。非アクティブの可能性があります。	正しい PEM 形式の証明書がインスタンスにアップロードされていることを確認します。
証明書が一致しません。(Certificates do not match.) 想定：<certStr>、実際：<inboundCert> (Expect: <certStr>, actual: <inboundCert>.)	IDP x509 証明書が存在し、有効かつアクティブであることを確認してください。	適用外	SNC で利用可能な証明書がアサーションの証明書と一致しません。次のような原因が考えられます。 • IdP では証明書が更新されているが、ServiceNow インスタンスで更新されていない。 • 証明書の形式が正しくない。	SAML 2.0 証明書レコードの PEM 形式の文字列が、ユーザー IdP の SAMLResponse の X509 証明書と一致していることを確認します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

マルチ **SSO (SAML 2.0)** セットアップ中のエラー (続く)

インスタンスログのエラー	テスト接続メッセージ	**SAML** プロパティ	診断	修正
証明書の有効性の確認に失敗しました。(Failure to check the validity of the certificate.)	IDP x509 証明書が存在し、有効かつアクティブであることを確認してください。	適用外	現在の証明書の有効期限が切れている可能性があります。	SAML 2.0 証明書レコードを更新します。
署名プロファイルの検証に失敗しました。(Failure to validate signature profile.)	IDP x509 証明書が存在し、有効かつアクティブであることを確認してください。	適用外	アサーションが別の証明書で署名されている可能性があります。	IdP に SNC インスタンスと同じ証明書があるかどうかを確認します。
SubjectConfirmationData の InResponseTo 属性が一致しません。(InResponseTo attribute in SubjectConfirmationData mismatch.) 想定：<inResponseTo>、実際：<inResponseTo> (Expect: <inResponseTo>, actual: <inResponseTo>.)	SubjectConfirmation の検証に失敗しました。	適用外	このエラーは、次のいずれかの状況が発生した場合に表示されます。 • IdP が別の SAMLRequest の SAMLResponse を返す場合 • ユーザーがインスタンス URL ではなく SAMLRequest を使用して URL をブックマークする場合 • null 値が想定される場合、インスタンスに複数のノードがあると、応答が別のノードに送信される可能性があります。	IdP 管理者は、想定される SAMLReponse が返されていることを確認する必要があります。この状況は、ロードバランサーまたはインフラストラクチャの問題である可能性があります。
SessionIndex 値が見つかりません：<メッセージ>... (SessionIndex value not found: <message>...)	SessionIndex が有効ではありません。(SessionIndex not valid.)	適用外	SNC インスタンスには SessionIndex が必要です。IdP はこれを SAML 応答で返して正常に認証します。	IdP 管理者は、SessionIndex が SAMLResponse で定義されていることを確認する必要があります。
有効な SubjectConfirmation が見つかりません。	SubjectConfirmation の検証に	適用外	IdP のエラーにより、条件が欠落している可能性があります。	SAMLResponse を確認し

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

マルチ **SSO (SAML 2.0)** セットアップ中のエラー (続く)

インスタンスログのエラー	テスト接続メッセージ	**SAML** プロパティ	診断	修正
	失敗しました。		応答の StatusCode には、想定される成功ではなくレスポンダーが含まれます。	て、SAMLResponse に条件が含まれているかどうかを判断します。 有効な件名確認データの有効期限が切れているか、対象者に対して適切でない可能性があります。
アサーション対象者が一致しません。(Assertion audience mismatch.) 想定：<propAudience>、実際：<audienceUri> (Expect: <propAudience>, actual: <audienceUri>.) または AudienceRestriction の検証に失敗しました。一致する対象者が見つかりません。(No matching audience found.)	[対象者 URI] フィールドが正しく設定されていることを確認します (Ensure that the 'Audience URI' field is set correctly)	SAML2 トークンを受け入れる対象者 URI (通常、インスタンス URI。たとえば https://demo.service-now.com)。	SNC インスタンスで構成された対象者 URI は、IdP の値と一致する必要があります。	ログの SAMLResponse で <saml2:Audience> を探し、値がインスタンスの値と一致することを確認します。
アサーションの発行者が無効です。想定：<value on instance>、実際：<value returned by IdP> (Expect: <value on instance>, actual: <value returned by IdP>)	アサーションの発行者が無効です。	ユーザー情報と一緒に SAML2 セキュリティトークンを発行する ID プロバイダの URL。	IdP エンティティ ID (発行者) が SNC インスタンスで定義された値と一致しません。	• IdP または SP の設定が不適切でないか確認します。 • SAML プロパティ (ユーザー情報と一緒に SAML2 セキュリティトークンを発行する ID プロバイダの URL) が正しく設定されているか確認します。
件名は将来有効になります。(Subject is valid in the future.) 現在：<now>、NotBefore：<notBefore> (Now:	件名の検証確認に失敗しました。(Subject validation confirmation failed.)	notBefore 制約の前、または notOnOrAfter 制約の後に、まだ有効で	IdP クロックが SP クロックと同期していません。	SAML プロパティ glide.authenticate.sso.saml2.clockske をより大きな値に更新します。デフォルトは 180 秒です。場合によっては 300 以上の設定が必要になります。IdP サーバーの時

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

マルチ **SSO (SAML 2.0)** セットアップ中のエラー (続く)

インスタンスログのエラー	テスト接続メッセージ	**SAML** プロパティ	診断	修正
<now>, NotBefore: <notBefore>) または 件名の有効期限が切れました。(Subject is expired.) 現在：<now>、NotOnOrAfter：<notOnOrAfter> (Now: <now>, NotOnOrAfter: <notOnOrAfter>)		あるとみなされる時間の秒数。		間も確認する必要があります。
アサーションは将来有効になります。現在：<now>、notBefore：<notBefore> (Assertion is valid in the future, now: <now>, notBefore: <notBefore>) または アサーションの有効期限が切れました。現在：<now>、notOnOrAfter：<notOnOrAfter>	アサーションが無効です。	notBefore 制約の前、または notOnOrAfter 制約の後に、まだ有効であるとみなされる時間の秒数。	IdP クロックが SP クロックと同期していません	SAML プロパティをより大きな値に更新します。デフォルトは 60 秒です。場合によっては 300 以上の設定が必要になります。IdP サーバーの時間も確認する必要があります。

一般的なログインおよび **IdP** エラー

エラーまたは症状	診断	修正
高セキュリティがアクティブな場合、ログイン要求はシステムと IdP の間で無限ループを生成します。	• 通常、URL エンドポイントはエラーページまたはログアウトページになります。 • IdP ホスト名をプロパティ値に追加せずに *`glide.security.url.whitelist`* を定義すると、logout_redirect.do によって	失敗した認証要求をこの URL にリダイレクトするには、システムプロパティ glide.authenticate.failed_redirect を設定 (または作成) します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

一般的なログインおよび **IdP** エラー (続く)

エラーまたは症状	診断	修正
	このループが作成される可能性があります。 **注:** このプロパティの詳細については、「インスタンスセキュリティ強化設定」の「ログアウトリダイレクトの URL 許可リスト」を参照してください。	
ユーザーまたは要求の認証に使用されるトークンが、署名アルゴリズム http://www.w3.org/2001/04/xmldsig-more#rsa-sha256 で署名されています。これは、想定される署名アルゴリズム http://www.w3.org/2000/09/xmldsig#rsa-sha1 とは異なります。	イベントの詳細については、[アラートコンテキスト (Alert Context)] タブを確認してください。	[証明書利用者信頼設定 (Relying Party Trust configuration)] ダイアログの [詳細] タブに移動し、アルゴリズムが SHA-256 ではなく SHA-1 に設定されていることを確認します。
エラーメッセージ urn:oasis:names:tc:SAML:2.0:sta がシステムログ (syslog) テーブルに表示されます。	IdP (ADFS など) の応答が oasis:names:tc:SAML:2.0:status:Requester のステータスの場合は、送信された要求に関する問題が原因で IdP がログインを拒否したことを意味します。ほとんどの場合、IdP から受信した SAML 応答にはエラーの詳細が記載されていません。	IDP に送信された SAML 要求を確認し、IDP 管理者と協力してインスタンスの SAML 設定を更新して、エラーを回避してください。ログイン失敗の理由については、IDP プロバイダーにお問い合わせください。

SAML によるスクリプトの問題のトラブルシューティング

SAML によるスクリプトの問題をトラブルシューティングします。複数の Single Sign-On をアクティブ化するときに SAML が既にアクティブであり、インストールを既にカスタマイズしている場合は、スクリプトの問題が発生する可能性があります。

始める前に

必要なロール：管理者

手順

1. 変更されたインストール終了 SAML2SingleSignon_update1 とスクリプトインクルード SAML2_update1 をバックアップします。
2. インストレーションイグジットとスクリプトインクルードの両方を、ベースラインシステムで使用可能なバージョンに戻します。
3. **Integration - Multiple Provider Single Sign-On Installer** プラグインをアクティブ化するか、またはアップグレードします。
   SAML と必要なすべてのファイルが SAML 2 Update 1 にアップグレードされます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

4. [複数の SSO (Multiple SSO)] プロパティページを開き、[マルチプロバイダー **SSO** の有効化 **(Enable Multi-Provider SSO)]** チェックボックスをオンにして有効にします。
5. SAML2SingleSignon_update1 インストレーションイグジットの変更をベースラインスクリプトインクルード **MultiSSO_SAML2_Update1** に入力し、SAML2_update1 スクリプトインクルードの変更をベースライン SAML2_update1 スクリプトインクルードに入力します。

複数プロバイダー **SSO** を使用したログイン

ユーザーが複数プロバイダー SSO を使用してログインするために推奨される最も効率的な方法は、特別に設定された URL を使用する方法です。

始める前に
必要なロール：管理者

このタスクについて
複数プロバイダー SSO の設定後は、パラメーター文字列で正しい IdP を使用して URL をユーザーに送信できます。例：

```
/login_with_sso.do?glide_sso_id=<sys_id of the sso configuration>
```

ユーザーが IdP ページに正常にログインすると、IdP sys_id を含む cookie がブラウザーに追加されます。次にユーザーがログインしようとすると、ユーザーは IdP サーバーへのログインにリダイレクトされ、インスタンスへの自動ログインが行われます。

URL パラメーターが設定されていないか、ブラウザーのキャッシュがクリアされている場合は、次のように操作することもできます。

手順

1. ログインページの [外部ログインを使用] リンクをクリックします。

   外部ログインページが表示されます。[ローカルログインを使用] をクリックすると、標準ログインページに戻ることができます。

2. 複数プロバイダー SSO プロパティで設定したユーザーテーブルの指定されたフィールドの値を入力します。

   ユーザーは IdP サーバーにリダイレクトされ、そこでログインします。

タスクの結果
ユーザーが IdP に正常にログインすると、インスタンスにアクセスしようとするたびにその IdP に自動的にリダイレクトされます。ユーザーが別の IdP にアクセスできるようにするには、 パラメーターに新しい IdP 情報を含む URL を送信します。ユーザーが正常にログインすると、新しい IdP が cookie 内の古い IdP を上書きします。ユーザーが正常にログインしない場合、古い IdP 情報は cookie に保持されます。

ユーザーによるログイン用 **ID** プロバイダーの選択の有効化

SSO フェデレーションのサポートにより、ユーザーはログインする IdP を選択できるようになります。

始める前に
必要なロール：管理者

このタスクについて
SSO フェデレーションは、インスタンスを含む複数の IdP およびサービスプロバイダーからのメタデータを集計します。フェデレーションは、IdP 名や IdP 証明書などの情報を含むメタデータを XML ファイルとして公開します。その後、管理者は XML ファイルを読み込むようにインスタンス

自動翻訳

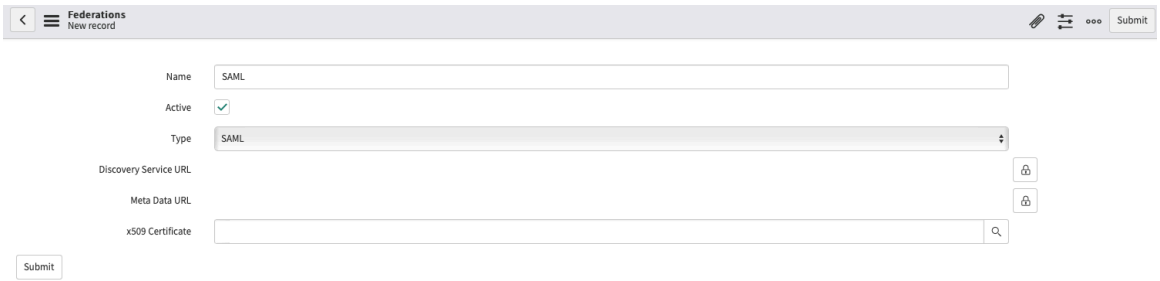
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

に指示し、必要なすべての IdP 情報を SSO プロパティテーブルに自動的に入力することができます。

手順

1. 移動先 すべて > マルチプロバイダー **SSO** > フェデレーション.
2. [新規] をクリックします。
3. 必要に応じて、フィールドに値を入力します (表を参照)。
4. [送信] をクリックします。
5. フェデレーションの設定後、[SSO メタデータのリフレッシュ (Refresh SSO Metadata)] ジョブスケジュールを有効にしてから、フェデレーション IdP にアクセスするユーザーを設定します。作成したフェデレーションレコードの sys_ID を使用します。

   作成したフェデレーションレコードの sys_ID を使用します。



インスタンスが SSO プロパティテーブルに IdP 情報を入力します。フェデレーションを使用するように設定されたユーザーがログインすると、設定した検出サービス URL にリダイレクトされます。次に、IdP を選択して必要な資格情報を入力します。または、パラメーターで IdP を使用して URL をユーザーに送信します。

ユーザーにログイン用 **ID** プロバイダーの選択を許可

フィールド	説明
名前	フェデレーションの説明的な名前を入力します。
有効	インスタンスがフェデレーションから XML ファイルをプルできるようにするには、このチェックボックスをオンにします。
タイプ	このフェデレーションがサポートする認証のタイプを選択します。
ディスカバリーサービス URL	このフェデレーションの検出サービスの URL を入力します。これは、ユーザーが IdP を選択してログインするように指示されるサイトです。
メタデータ URL	フェデレーションメタデータを保持する XML ファイルの URL を入力します。
x509 証明書	フェデレーション証明書を選択します。
ドメイン	データが属するドメインを選択します。

注:
InCommon フェデレーション ID 管理 IdP が事前設定されています。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

複数プロバイダー **SSO** で サービスポータル を使用して **URL** をリダイレクトする

サービスポータル システムのプロパティとスクリプトインクルードを組み合わせて使用し、ポータルにログインするユーザーに対してシステムが URL リダイレクトを処理する方法を決定します。

始める前に
必要なロール：管理者

このタスクについて
システムプロパティを使用してプライマリ ID プロバイダー (IdP) に自動的にリダイレクトする場合、サービスポータル によってその IdP に自動的にリダイレクトされます。IdP が複数ある場合、サービスポータル では、ログインページで [外部ログインを使用] へのリンクが表示されます 。

手順

1. Service Portal ログインページの設定
2. ログイン後に Service Portal へリダイレクトする

アカウント復旧 **(ACR)**

管理者は、アカウント復旧 (ACR) を設定して、SSO の設定ミスや期限切れの証明書への対処などの復旧アクティビティを実行できます。

> **注:**
> ACR を有効にすると、インスタンスに対して SSO が有効になっている場合に、ローカルのインタラクティブログイン (ユーザー名またはパスワードベース) が無効になります。

ACR は次の機能を提供します。

- Single Sign-on (SSO) ログインをバイパスして、管理者として SSO 構成の問題に対処します。
- SSO を使用してログインし、アカウント復旧として設定された管理者アカウントでタスクを実行します。
- ACR フローにより、管理者は、SSO の構成ミスや期限切れの証明書など復旧を必要とする場合に、セルフサービス機能を使用して、アカウントの復旧に対処できるようになります。
- インスタンスへの不正アクセスを減らし、SSO ユースケース外で ACR を使用するための強力な基盤を提供します。

新しいインスタンス

新しいインスタンスで ACR を使用するには、次の操作を行う必要があります。

- Mutli-SSO プラグイン (com.snc.integration.sso.multi.installer) をアクティブにします。
- ACR を有効にします (glide.sso.acr.enabled)。新しいインスタンスの場合、これはデフォルトで有効になっています。
- SSO プロパティ (glide.authenticate.multisso.enabled) を有効にする前に、管理者は ACR ユーザーとして登録する必要があります。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

> **注:**
> インスタンスでアカウント復旧 (ACR) が有効になっている場合、このプロパティを false に設定しても、マルチプロバイダー SSO は無効になりません。ユーザー名とパスワードでログインするには、 *glide.sso.acr.enabled* プロパティを使用して ACR も無効にする必要があります。このプロパティの詳細については、「アカウント復旧プロパティ」を参照してください。

- 管理者は、ACR ユーザーとして登録する前に、ローカルログインのパスワードを設定し、MFA を登録する必要があります。

アップグレードされたインスタンス

アップグレードされたインスタンスで ACR を使用するには、次の操作を行う必要があります。

- Mutli-SSO プラグイン (com.snc.integration.sso.multi.installer) をアクティブにします。
- ACR を有効にします (glide.sso.acr.enabled)。

> **注:**
> アップグレードされたインスタンスの場合、管理者は ACR を有効にする必要があります。

- SSO プロパティ (glide.authenticate.multisso.enabled) を有効にする前に、管理者は ACR ユーザーとして登録する必要があります。
- 管理者は、ACR ユーザーとして登録する前に、ローカルログインのパスワードを設定し、MFA を登録する必要があります。

アカウント復旧ユーザーの設定

アカウント復旧を使用するには、少なくとも 1 つの管理者アカウントをアカウント復旧ユーザーとして登録する必要があります。少なくとも 1 つのアカウントが設定されるまで、インスタンスで Single Sign-on を有効にすることはできません。このプロセスの詳細については、「[アカウント復旧プロパティ] ページからのアカウント復旧ユーザーの設定」を参照してください。

> **注:**
> すでに Single Sign-on を使用しているインスタンスを Rome 以降のリリースにアップグレードする場合、Single Sign-on は復旧ユーザーが設定されていなくても引き続き機能します。

アカウント復旧の構成

このアカウント復旧機能は、**Integration - Multiple Provider Single Sign-On Installer (com.snc.integration.sso.msoi.installer)** プラグインに含まれています。この機能はデフォルトで有効になっています。このアカウントおよび他のアカウントの復旧設定は、システムプロパティを使用して変更できます。これらのプロパティの詳細については、「アカウント復旧プロパティ」を参照してください。

アカウント復旧ポリシーのコンテキスト

アカウント復旧ユーザーを登録し、Single Sign-on (SSO) を有効にすると、インスタンスはすべてのローカルログインを制限します。この制限は、**SSO - ACR** コンテキスト認証ポリシーコンテキストで定義されています。コンテキストの詳細については、「アカウント復旧のコンテキスト」を参照してください。

認証ポリシーとポリシーコンテキストの詳細、およびインスタンスでの動作の詳細については、「適応認証」を参照してください。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

アカウント復旧ユーザーの設定

インスタンスでアカウント復旧アクティビティを実行するアカウント復旧ユーザーを設定します。

アカウント復旧ユーザーは、SSO の設定ミスへの対処や期限切れの証明書への対処などのアカウント復旧タスクを実行するために、管理者が使用できるユーザーアカウントです。

> **注:**
> インスタンスでアカウント復旧を使用する場合は、アカウント復旧ユーザーを設定する必要があります。この手順は、インスタンスで複数プロバイダー Single Sign-on を有効にする前に必要です。

[アカウント復旧プロパティ] ページからのアカウント復旧ユーザーの設定

[アカウント復旧プロパティ] ページからアカウントの復旧を設定します。

始める前に

必要なロール：admin

新しいインスタンスで ACR を設定するには、次の操作を行う必要があります。

- Mutli-SSO プラグイン (com.snc.integration.sso.multi.installer) をアクティブにします。
- ACR を有効にします (glide.sso.acr.enabled)。新しいインスタンスの場合、これはデフォルトで有効になっています。
- SSO プロパティ (glide.authenticate.multisso.enabled) を有効にする前に、管理者は ACR ユーザーとして登録する必要があります。
- 管理者は、ACR ユーザーとして登録する前に、ローカルログインのパスワードを設定し、MFA を登録する必要があります。

アップグレードされたインスタンスで ACR を使用するには、次の操作を行う必要があります。

- Mutli-SSO プラグイン (com.snc.integration.sso.multi.installer) をアクティブにします。
- ACR を有効にします (glide.sso.acr.enabled)。

  > **注:**
  > アップグレードされたインスタンスの場合、管理者は ACR を有効にする必要があります。

- SSO プロパティ (glide.authenticate.multisso.enabled) を有効にする前に、管理者は ACR ユーザーとして登録する必要があります。

  > **注:**
  > インスタンスでアカウント復旧 (ACR) が有効になっている場合、このプロパティを false に設定しても、マルチプロバイダー SSO は無効になりません。ユーザー名とパスワードでログインするには、 `glide.sso.acr.enabled` プロパティを使用して ACR も無効にする必要があります。このプロパティの詳細については、「アカウント復旧プロパティ」を参照してください。

- 管理者は、ACR ユーザーとして登録する前に、ローカルログインのパスワードを設定し、MFA を登録する必要があります。

手順

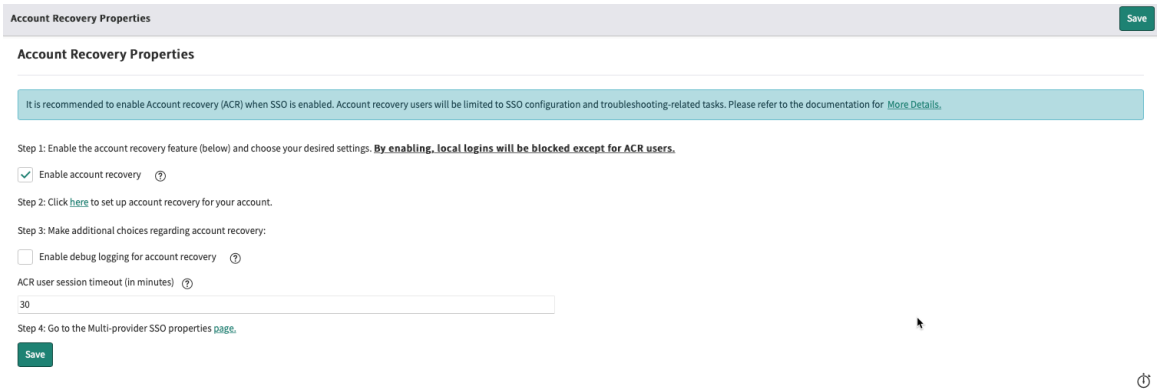
1. 移動先 すべて > アカウント復旧 > プロパティ.
2. [アカウント復旧の有効化] をクリックします。

自動翻訳

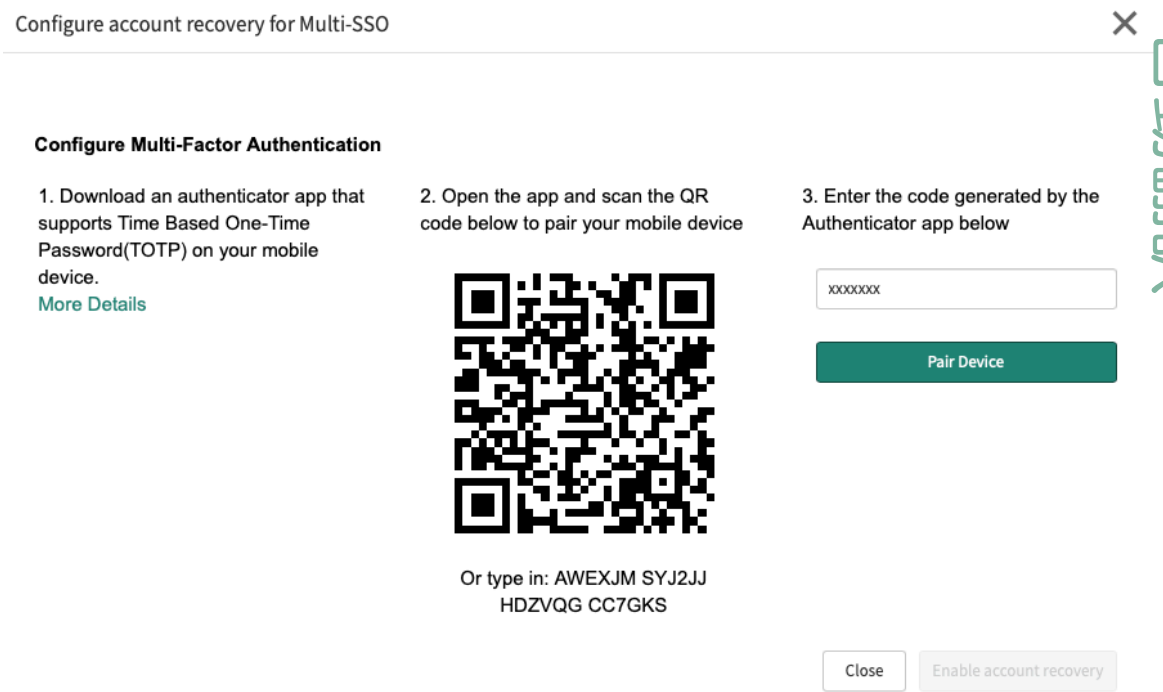
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注:
SSO が有効になっている場合は、アカウント復旧を有効にする必要があります。アカウント復旧ユーザーは、SSO 構成とトラブルシューティング関連のタスクに制限されます。

3. ステップ 2 にある文字 [ここ **(here)]** をクリックします。



4. [マルチ **SSO** のアカウント復旧を設定 **(Configure account recovery for Multi-SSO)]**モーダルの画面の指示に従って操作します。



画面の手順を完了すると、[アカウント復旧の有効化] が有効になります。

5. [アカウント復旧の有効化] をクリックします。

タスクの結果
ユーザーアカウントをアカウント復旧ユーザーとして設定しました。次の場所に移動すると、このアカウントを確認し、他の構成済みアカウント復旧ユーザーを確認できます マルチプロバイダー **SSO** > アカウント復旧 > ユーザー.

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

管理者ユーザープロファイルからのアカウント復旧ユーザーの設定

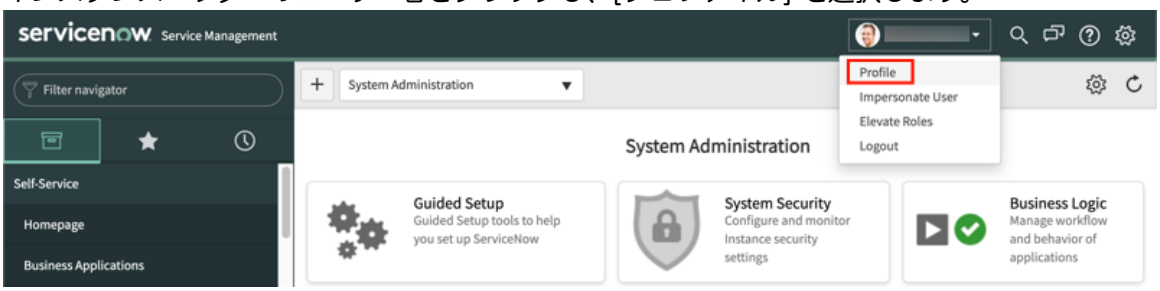
管理者ユーザープロファイルから、管理者をアカウント復旧ユーザーとして設定します。

始める前に

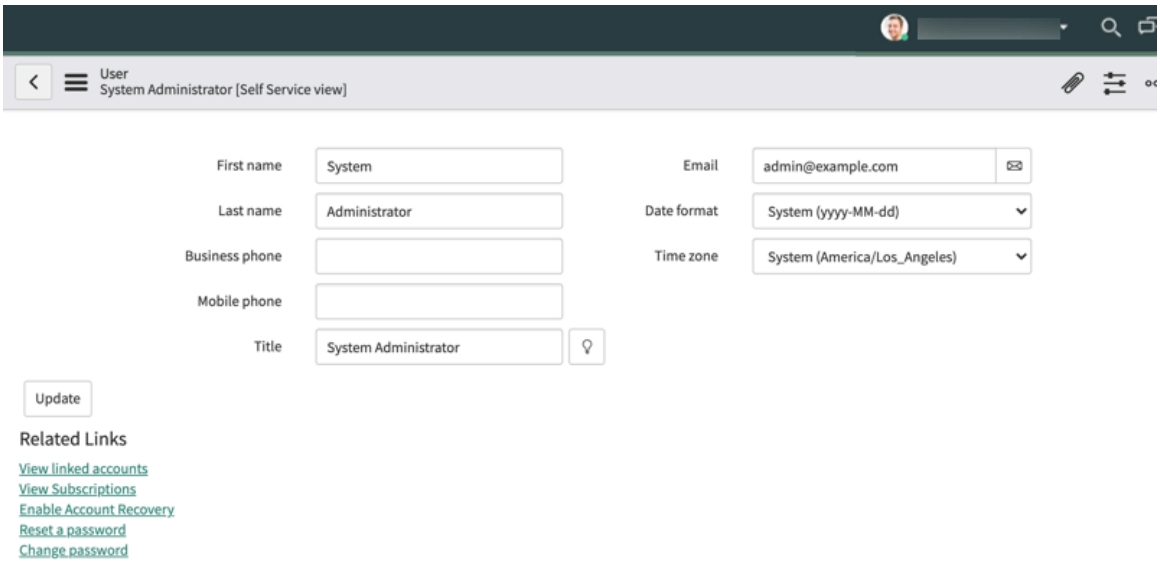
必要なロール：admin

手順

1. 管理者アカウントを使用してインスタンスにログインします。
2. インスタンスヘッダーのユーザー名をクリックし、[プロファイル] を選択します。



3. [ユーザー] フォームで、[関連リンク] セクションの [アカウント復旧の有効化] をクリックします。



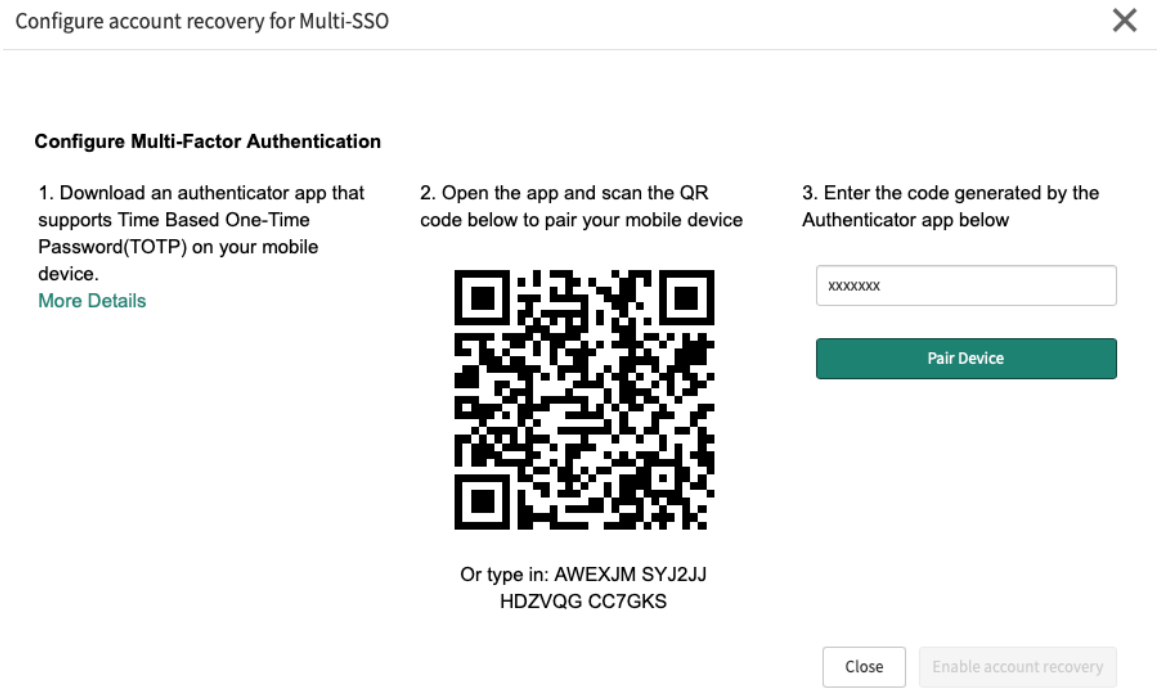
注:

選択したユーザーが既にアカウント復旧を有効にしている場合、関連リンクに [アカウント復旧の有効化] は表示されません。代わりに [アカウント復旧の無効化] オプションが表示されます。

4. [マルチ **SSO** のアカウント復旧を設定 **(Configure account recovery for Multi-SSO)]**モーダルの画面の指示に従って操作します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



画面の手順を完了すると、[アカウント復旧の有効化] が有効になります。

5. [アカウント復旧の有効化] をクリックします。

タスクの結果

ユーザーアカウントをアカウント復旧ユーザーとして設定しました。次の場所に移動すると、このアカウントを確認し、他の構成済みアカウント復旧ユーザーを確認できます マルチプロバイダー **SSO** > アカウント復旧 > ユーザー.

アカウント復旧プロパティ

システムプロパティを使用して、インスタンスでアカウント復旧 (ACR) を設定します。

インスタンスのアカウント復旧プロパティにアクセスするには、次の場所に移動します。 マルチプロバイダー **SSO** > アカウント復旧 > プロパティ.

アカウント復旧システムプロパティ

プロパティ	説明
アカウント復旧機能を有効にします [glide.sso.acr.enabled]	インスタンスでアカウント復旧機能が有効になっているかどうか。このプロパティはデフォルトで有効になっています。
アカウント復旧のデバッグログ記録を有効にします [glide.sso.acr.debug.log.enabled]	インスタンスのデバッグログにアカウント復旧情報が含まれているかどうか。このプロパティは、デフォルトでは無効になっています。
ACR ユーザーセッションタイムアウト (分) [glide.sso.acr.ui.session.timeout]	インスタンスがアカウント復旧ユーザーセッションを終了するまでの非アクティブ時間 (分) このプロパティのデフォルト値は 30 です。

マルチプロバイダー **SSO** の電子署名

マルチプロバイダー SSO を使用した電子署名では、SAML または OIDC プロパティの代わりに電子署名プロパティを認証に使用できます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

認証中のシングルサインオン (SSO) 検証で、電子署名を送信する前にユーザーに資格情報の提供を要求する場合は、署名を送信する前にユーザー資格情報の入力を求めるように認証を構成できます。

Approvals with e-signature (com.glide.e_signature_approvals) プラグインをインストールして、SSO ログインの電子署名を構成できます。

注:
電子署名プラグインをインストールするには、コード署名の署名 (com.glide.code_signing.signatures) をインストールする必要があります。

電子署名による承認プラグインのアクティブ化

電子署名による承認プラグイン (com.glide.e_signature_approvals) を使用すると、ユーザーはログイン資格情報を再入力して要求を承認することができます。

始める前に
必要なロール：admin

注:
電子署名プラグインをインストールするには、コード署名の署名 (com.glide.code_signing.signatures) をインストールする必要があります。

手順

1. 移動先 すべて > システムアプリケーション > 利用可能なすべてのアプリケーション > すべて.
2. フィルター基準と検索バーを使用してプラグインを検索します。

   名前または ID でプラグインを検索できます。プラグインが見つからない場合は、ServiceNow 担当者から要求する必要があります。
3. [インストール] を選択して、[プラグインをアクティブにする] ダイアログボックスで、[アクティブ化] をクリックします。

   注:
   ドメイン分離と代理管理者がインスタンスで有効になっている場合、管理ユーザーはグローバルドメインに含まれている必要があります。それ以外の場合、次のエラーが表示されます： 別の操作が実行されているため、アプリケーションのインストールは利用できません：<プラグイン名> のプラグインの有効化。

複数プロバイダー **SSO** を使用した **SAML 2.0** 認証の **SSO** 承認の設定

電子署名による SSO 承認では、SAML IdP および ServiceNow インスタンスの設定が必要です。

始める前に
必要なロール：管理者

このタスクについて
SAML IdP は、SAML アサーション要求で forceAuthn 属性をサポートし、優先する必要があります。この IdP 設定がないと、電子署名は機能しません。SAML 2.0 認証の資格情報を使用して電子署名による承認を設定します。

手順

1. Activate Multi-Provider SSO プラグインを使用して、SAML 2.0 を有効にするか、SAML 2.0 にアップグレードします。
2. Approval with E-Signature プラグインをアクティブ化します。
3. 移動先 マルチプロバイダー **SSO** > **ID** プロバイダー 2.0 SAML IdP 構成の [詳細] タブに **[AuthnRequest** の強制] 属性がオンになっていることを確認します。

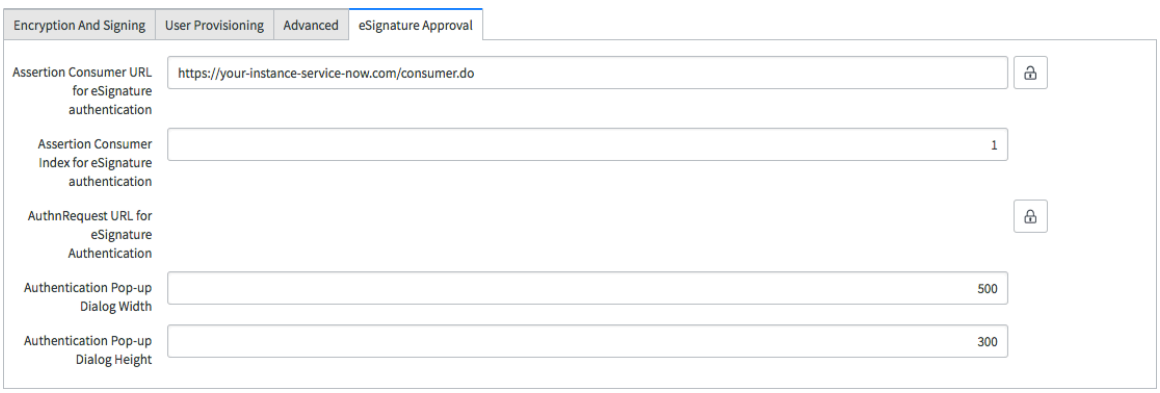
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

SAML 2.0 IdP が **[AuthnRequest** の強制] 属性をサポートしている必要があります。サポートしていない場合、電子署名はサポートされません。

4. [eSignature の承認] タブで、次の電子署名の SAML プロパティを入力します。

オプション	説明
eSignature 認証用の Assertion Consumer URL	このプロパティのデフォルトは、適切な URL です。このプロパティを設定するには、ロックアイコンを選択してこのフィールドを編集可能にします。編集後、そのアイコンを選択してフィールドをロックします。
eSignature 認証用の Assertion Consumer Index	サービス プロバイダーが AssertionConsumerURL の複数の URL セットを保有している場合は、eSignature で使用するためにインデックス 1 以上で始まるインデックスを設定できます。
eSignature 認証用の AuthnRequest URL	eSignature 認証用の SAML 2.0 IdP AuthnRequest URL を示す URL を入力できます。URL が Assertion Consumer URL と同じである場合は、この設定を空のままにすることができます。
認証ポップアップダイアログの幅	ユーザーが eSignature を使用して要求を承認すると、ポップアップが開き、認証情報を入力できます。この設定は、ダイアログ ボックスの幅を制御します。デフォルトは 500 です。
認証ポップアップダイアログの高さ	ユーザーが eSignature を使用して要求を承認すると、ポップアップが開き、認証情報を入力できます。この設定は、ダイアログ ボックスの高さを制御します。デフォルトは 300 です。



5. タブの下にある [メタデータを生成] ボタンを選択して、サービス プロバイダーのメタデータを再生成します。
6. サービスプロバイダーのメタデータをコピーし、SAML IdP でそれを更新します。

複数プロバイダー **SSO** を使用した **OIDC** 認証の **SSO** 承認の設定

電子署名による SSO 承認では、SAML IdP および ServiceNow インスタンスの設定が必要です。

始める前に
必要なロール：admin

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

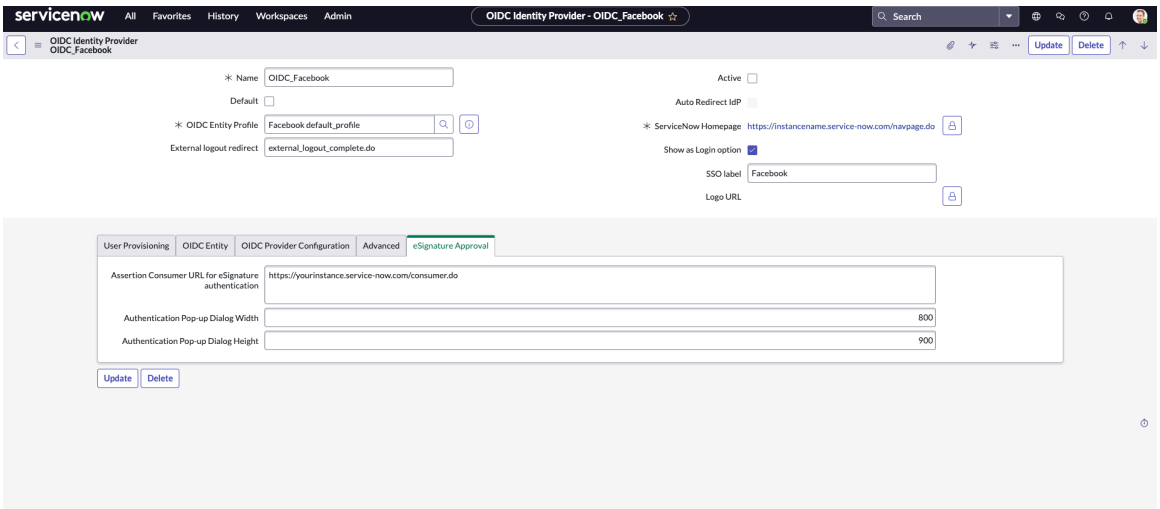
自動翻訳

このタスクについて
SAML IdP は、SAML アサーション要求で forceAuthn 属性をサポートし、優先する必要があります。この IdP 設定がないと、電子署名は機能しません。SAML 2.0 認証の資格情報を使用して電子署名による承認を設定します。

手順

1. Approval with E-Signature プラグインをアクティブ化します。
2. 移動先 マルチプロバイダー **SSO** > **ID** プロバイダー OIDC プロバイダー構成を確認します
3. [eSignature の承認] タブで、次の電子署名の SAML プロパティを入力します。

オプション	説明
eSignature 認証用の Assertion Consumer URL	このプロパティのデフォルトは、適切な URL です。このプロパティを設定するには、ロックアイコンを選択してこのフィールドを編集可能にします。編集後、そのアイコンを選択してフィールドをロックします。
認証ポップアップダイアログの幅	ユーザーが eSignature を使用して要求を承認すると、ポップアップが開き、認証情報を入力できます。この設定は、ダイアログボックスの幅を制御します。デフォルト値は 800 です。
認証ポップアップダイアログの高さ	ユーザーが eSignature を使用して要求を承認すると、ポップアップが開き、認証情報を入力できます。この設定は、ダイアログボックスの高さを制御します。デフォルトは 900 です。



4. OIDC の初期セットアップ中に電子署名を設定する場合は [送信] を選択し、電子署名の詳細を更新する場合は [更新] を選択します。

Single Sign-on (SSO) ID プロバイダー (IdP) としての OpenID Connect (OIDC)

OpenID Connect (OIDC) は OAuth プロトコル上に構築された ID レイヤーで、最新の直感的な Single Sign-on (SSO) エクスペリエンスをユーザーやエンドユーザーに提供します。OIDC は、ユーザーがソーシャル ID プロバイダーを使用して ServiceNow アプリケーションにログインできるようにすることで、モバイルアプリケーションのログインエクスペリエンスも向上させます。たとえば、管理者は、OpenID Connect をサポートするサードパーティの ID プロバイダーを使用して Single Sign-on を設定できます。ユーザーは、ID プロバイダーの資格情報を使用してカスタム ServiceNow アプリケーションにログインできます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

企業/顧客間 (B2C) ユーザーには Google などのソーシャル ID プロバイダーを使用し、企業間ユーザーには Okta 、Microsoft Azure AD などのエンタープライズ ID プロバイダーを使用できます。

Single Sign-on (SSO) 用の OpenID Connect (OIDC) 構成の作成

Multi-Provider SSO プラグインを使用して、OpenID Connect (OIDC) 構成を作成または更新します。

始める前に

- OIDC アプリケーションを ID プロバイダー (IdP) に登録し、クライアント ID、クライアントシークレット、および既知の構成 URL をメモします。
- Multi-Provider SSO プラグインのアクティブ化
- マルチプロバイダー SSO プロパティの設定
- Approval with e-Signature プラグインをアクティブ化して、OIDC IdP の電子署名を有効にします。
- 必要なロール：admin

Single Sign-on (SSO) 用の OpenID Connect (OIDC) 構成

ID プロバイダーのクライアント ID、クライアントシークレット、および既知の構成 URL がある場合は、SSO の OIDC 構成を直接インポートできます。

> **注:**
> Domain Separation プラグインがインストールされている場合、OIDC IdP を使用したログインオプションはサポートされません。

ID プロバイダーに関する必要な情報がない場合は、手動で SSO 用に OIDC を設定できます。構成が完了すると、ユーザーは Google Okta などのサードパーティのソーシャル ID プロバイダーを使用して ServiceNow アプリケーションにログインできます。

手順

1. 移動先 すべて > マルチプロバイダー **SSO** > **ID** プロバイダー.
2. 次のいずれかのオプションを選択します。
   - 既存の構成を更新するには、OIDC ID プロバイダーレコードをクリックします。
   - 新しい構成を作成するには、[新規] をクリックし、**[OpenID Connect]** を選択します。
3. 新しい構成の場合は、次のいずれかの方法で OIDC 構成情報を入力します。

オプション	説明
OpenID Connect の既知の構成をインポート	関連するクライアント資格情報とともに既知の構成 URL がある場合は、OIDC 構成を直接インポートできます。 **注:** OIDC の既知の構成をインポートすると、関連するすべてのフィールドが自動入力されます。
OIDC ID プロバイダーフォームの手動構成	既存の OAuth OIDC エンティティがない場合は、[OpenID Connect の既知の構成をインポート] ポップアップを閉じて、[OIDC ID プロ

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

オプション	説明
	バイダー] フォームのフィールドに手動で入力します。

[OpenID Connect の既知の構成をインポート] のフィールド

プロパティ	説明
名前	OIDC ID プロバイダー構成の一意の名前。
クライアント ID	サードパーティの OIDC ID プロバイダーに登録されているアプリケーションのクライアント ID。
クライアントシークレット	サードパーティの OIDC ID プロバイダーに登録されているアプリケーションのクライアントシークレット。
既知の設定 URL	サードパーティ OIDC ID プロバイダーに関するメタデータを含む URL。

[OIDC ID プロバイダー] フォームのすべての必須フィールドに入力する必要があります。

OIDC ID プロバイダーフォームに手動で入力する前に、OIDC IdP の OAuth エンティティプロファイルがあることを確認してください。

OAuth エンティティプロファイルがない場合は、Okta、Azure などのデフォルトの外部 OIDC プロバイダーテンプレートを使用して作成できます。

OAuth エンティティプロファイルの権限許可タイプには、認証コードが入っている必要があります。詳細については、「Now Platform で OAuth OIDC プロバイダーを構成する (Configure an OAuth OIDC provider on the Now Platform)」を参照してください。

注:
Multiple Provider Single Sign-On Installer プラグインのデモデータでは、サードパーティの ID プロバイダーである Auth0、Azure AD、Google、および Okta のテンプレートを使用できます。

OIDC ID プロバイダーのフィールド

プロパティ	説明
名前	OIDC ID プロバイダーレコードの名前
有効	OIDC IdP 構成をアクティブにするオプション **注:** このオプションは、テスト接続が成功した後にのみアクティブに設定できます。
デフォルト	OIDC 構成が複数ある場合に、OIDC IdP 構成をデフォルトとして設定するオプション
自動リダイレクト IdP	ID プロバイダーのログインページへユーザーを自動リダイレクトできるようにするオプション。このフィールドは、[自動リダイレクト **IdP** として設定] オプションが [関連リンク] セクションで設定されている場合に表示されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

プロパティ	説明
	注: 新しい自動リダイレクト IdP 構成をアクティブにすると、*glide_sso_id* cookie が新しい自動リダイレクト IdP で自動的に更新されます。*glide.authenticate.sso.update.idp.cookie* システムプロパティは、この機能を制御します。
OIDC エンティティプロファイル	OIDC 構成の OAuth エンティティプロファイル。
ServiceNow のホームページ	認証に使用されるログイン ページの URL。このフィールドは、自動的にインスタンス URL に設定されます。URL の形式は https://yourinstance.service-now.com/navpage.do です。
外部のログアウトのリダイレクト	ログアウト後に統合によりリダイレクトされる URL。通常は、SSO に使用されるポータルです。このフィールドは自動的に external_logout_complete.do に設定されます (例：https://yourinstance.service-now.com/external_logout_complete.do)。
ログインオプションとして表示	OIDC IdP をログインページのログインオプションとして表示するオプション。ログインオプションは 、**[ID プロバイダーでログイン (login with Identity provider)]** ボタンとして表示されます。
SSO ラベル	ログインページに表示される OIDC IdP のラベル。このフィールドは、[ログインオプションとして表示] が有効になっている場合にのみ表示されます。
ロゴ URL	OIDC IdP プロバイダーのロゴを含む公開 URL。このフィールドは、[ログインオプションとして表示] が有効になっている場合にのみ表示されます。

4. オプション: [ユーザープロビジョニング] タブ > [ユーザープロビジョニング] タブで自動ユーザープロビジョニングを有効にします。

   (Optional) ユーザーのログイン時に自動ユーザープロビジョニングを有効にするよう選択できます。自動ユーザープロビジョニングが有効になっている場合、ユーザーレコードが存在しなければ ServiceNow インスタンスに自動的に作成されます。

   [ユーザープロビジョニング] のフィールド

プロパティ	説明
ユーザーを自動プロビジョニング	自動ユーザープロビジョニングを有効にするオプション。このプロパティにより、ユーザーが IdP に存在するがユーザーテーブルに存在しない場合に、インスタンスユーザー (sys_user) テーブルにユーザーが作成されます。
プロビジョニングに使用	ID トークン、ユーザー情報エンドポイント、または ID トークンとユーザー情報の両方を ServiceNow ユーザーに変換するために使用するデータソース。ルックアップリストを使用して、事前定義されたデータソーステンプレートを選択し、レコードを開いて変換テーブルのマッピングを構成します。
データソースをプロビジョニング	ユーザーのプロビジョニングに使用される ID トークンデータソース。
ユーザー情報データソース	ユーザープロビジョニングに使用されるユーザー情報エンドポイントデータソース。このフィールドは、[プロビジョニングに使用] フィールドで [ユーザー情報] または [ID トークンとユーザー情報の両方 (Both ID Token and User Info)] が選択されている場合に表示されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

プロパティ	説明
次回のログイン時にユーザーを更新	次回のログイン時にユーザーを更新できるようにするオプション。
ユーザー更新の時間間隔 (秒)	後続のログインの間にユーザーレコードを更新するための最小時間間隔 (秒)。このフィールドは自動的に 3,600 秒に設定されます。たとえば、ユーザーがログインした後、次のログインまで 3,600 秒後にユーザーレコードが更新されます。このフィールドは、 [次回のログイン時にユーザーを更新] フィールドが有効になっている場合にのみ使用できます。
プロビジョニングされたユーザーに適用されるユーザーロール	新しくプロビジョニングされたユーザーに適用されるロールのリスト。

5. [OIDC エンティティ] タブ
   エンティティレコードを使用して、OIDC クライアント構成と OIDC 接続フローを表示および変更できます。
6. [OIDC プロバイダー構成] タブ
   OIDC IdP または ID トークン要求検証の既知の構成 URL を表示および変更できます。
7. オプション: [詳細] タブ

   (Optional) Single Sign-on およびログアウト時に実行されるスクリプト

   [詳細] フィールド

プロパティ	説明
Single Sign-on スクリプト	Single Sign-on 中に実行されるスクリプト。このフィールドは自動的に MultiSSO_OIDC_custom に設定されます。
ログアウトスクリプト	ユーザーがログアウトした後に実行されるスクリプト。このフィールドは自動的に MultiSSO_OIDC_logout_custom に設定されます。

8. オプション: [電子署名の承認 (eSignature Approval)] タブで、OIDC IDp の電子署名を構成します。

   注:
   [電子署名の承認 (eSignature Approval)] タブは、 **Approval with e-Signature** プラグイン (com.glide.e_signature_approvals) をインストールした場合にのみ表示されます。

   [電子署名の承認 **(eSignature Approval)]** フィールド

プロパティ	説明
eSignature 認証用の Assertion Consumer URL	eSignature の OIDC 認証を処理する方法をカスタマイズして使用する場合は、独自のコンシューマー URL を設定できます。たとえば、マルチプロバイダー SSO を使用している場合は、このプロパティを使用する必要はありません。URL の形式は https://

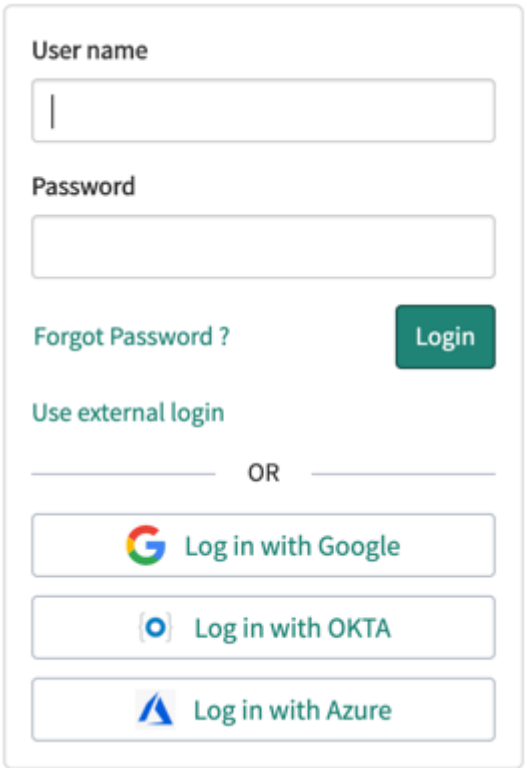
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

プロパティ	説明
	yourinstance.service-now.com/consumer.do です。
認証ポップアップダイアログの幅	認証ポップアップダイアログの幅。このフィールドは自動的に 800 に設定されます。
認証ポップアップダイアログの高さ	認証ポップアップダイアログの高さ。このフィールドは自動的に 900 に設定されます。

9. オプション: インスタンスのログインページに移動して、IdP がログインオプションとして表示されていることを確認します。
URL は、次の形式にする必要があります。https://yourinstance/login_with_sso.do?glide_sso_id=sysId_IdP

   注:
   [ログインオプションとして選択 **(Selected as login Option)]** を有効にしている場合は、インスタンスのログイン URL に移動できます。



自動翻訳

Facebook ベースの **Single Sign-on (SSO)** の使用

Facebook ベースの SSO で Facebook 資格情報を使用して、ServiceNow インスタンスにログインします。

始める前に
Facebook ベースの SSO は ServiceNow インスタンスとともに出荷されます。

ID プロバイダー (Idp) 構成を、使用する **ID** プロバイダーとして **OIDC_Facebook** IdP に定義できます。Idp 構成の詳細については、「Facebook ベースの Single Sign-on (SSO) の構成」を参照してください。

必要なロール：管理者

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. 移動先 すべて > マルチプロバイダー **SSO** > **ID** プロバイダー.
2. **[OIDC_Facebook]** を選択します。
3. [OIDC_Facebook] ページで、次のフィールドを指定します。

注:

- デフォルトの IdP を使用すると、ほとんどのフィールドが自動入力されます。
- ServiceNow ホームページの詳細を指定する必要があります。
- Facebook からのクライアント ID やクライアントシークレットなどのユーザー関連の詳細を、IdP 内に指定する必要があります。

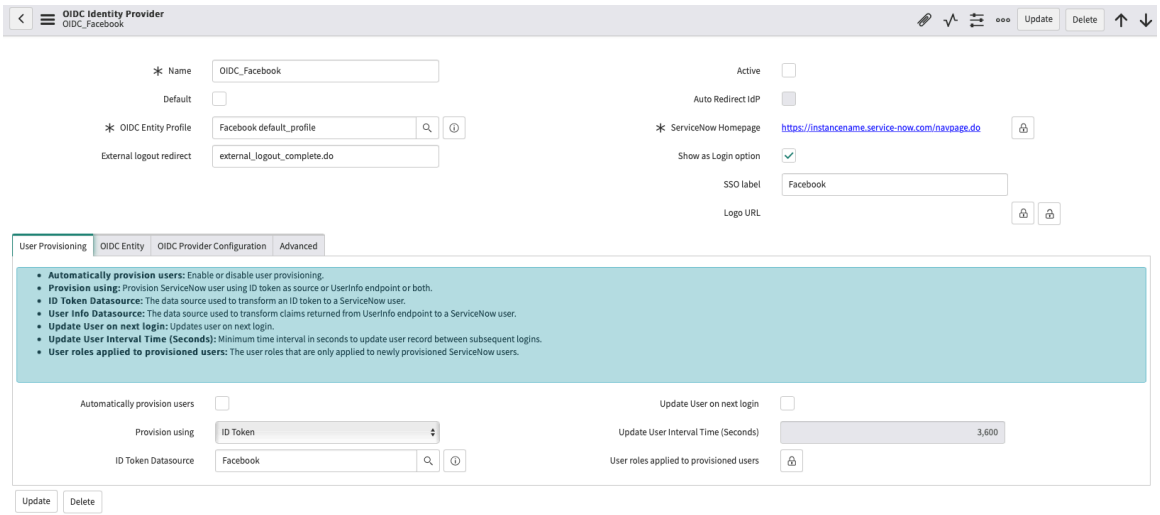
OIDC_Facebook ID プロバイダーの詳細

フィールド	説明
名前	OIDC IdP レコードの名前を記録します。「OIDC_Facebook」と入力します。
デフォルト	OIDC IdP 構成をデフォルトとして設定するオプション。
OIDC エンティティプロファイル	OIDC 構成の OAuth エンティティプロファイル。「Facebook default_profile」と入力します。
外部のログアウトのリダイレクト	ログアウト後に統合によりリダイレクトされる URL。通常、この URL は SSO に使用されるポータルです。このフィールドは自動的に **external_logout_complete.do** に設定されます。例：https://<yourinstance>.service-now.com/external_logout_complete.do
有効	OIDC IdP 構成をアクティブにするオプション 注: このオプションは、テスト接続が成功した後にのみアクティブに設定できます。
自動リダイレクト IdP	ID プロバイダーのログインページへユーザーを自動リダイレクトできるようにするオプション。
ServiceNow のホームページ	認証に使用されるログイン ページの URL。このフィールドは、自動的にインスタンス URL に設定されます。URL の形式は https://<インスタンス>.service-now.com/navpage.do です。
ログインオプションとして表示	OIDC IdP をログインページのログインオプションとして表示するオプション。この場合、ログインオプションは **[Facebook** でログイン **(Login with Facebook)]** ボタンとして表示されます。
SSO ラベル	ログインページに表示される OIDC IdP のラベル。このフィールドは、[ログインオプション

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	として表示] が有効になっている場合にのみ表示されます 。
ロゴ URL	OIDC IdP プロバイダーのロゴを含む公開 URL。このフィールドは、[ログインオプションとして表示] が有効になっている場合にのみ表示されます 。



4. オプション: [ユーザープロビジョニング] タブを開き、フィールドに入力します。

> **注:**
> Facebook から、ユーザーのクライアント ID やクライアントシークレットなどの OIDC 関連情報を設定する必要があります。

[ユーザープロビジョニング] タブ

フィールド	説明
ユーザーを自動プロビジョニング	自動ユーザープロビジョニングを有効にするオプション。このプロパティにより、ユーザーが IdP に存在するがユーザーテーブルに存在しない場合に、インスタンスユーザー [sys_user] テーブルにユーザーが作成されます。 **注:** ユーザーのログイン時に自動ユーザープロビジョニングを有効にするよう選択できます。自動ユーザープロビジョニングが有効になっている場合、ユーザーレコードが存在しなければ ServiceNow インスタンスに自動的に作成されます。
プロビジョニングに使用	ServiceNow ユーザーに変換するために使用するデータソース。選択肢は次のとおりです。 ○ **ID** トークン ○ ユーザー情報エンドポイント ○ **ID** トークンとユーザー情報の両方 ルックアップリストを使用して、事前定義されたデータソーステンプレートを選択し、レコードを開いて変換テーブルのマッピングを構成します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
データソースをプロビジョニング	ユーザーのプロビジョニングに使用される ID トークンデータソース
ユーザー情報データソース	ユーザープロビジョニングに使用されるユーザー情報エンドポイントデータソース。このフィールドは、[プロビジョニングに使用] フィールドで [ユーザー情報] または **[ID** トークンとユーザー情報の両方] が選択されている場合にのみ表示されます。
次回のログイン時にユーザーを更新	次回のログイン時にユーザーを更新できるようにするオプション。
ユーザー更新の時間間隔 (秒)	後続のログイン間でユーザーレコードを更新するための最小時間間隔 (秒)。このフィールドは自動的に 3,600 秒に設定されます。たとえば、ユーザーがログインした後、次のログインまで 3,600 秒後にユーザーレコードが更新されます。このフィールドは、 [次回のログイン時にユーザーを更新] フィールドが有効になっている場合にのみ使用できます。
プロビジョニングされたユーザーに適用されるユーザーロール	新しくプロビジョニングされたユーザーに適用されるロールのリスト。

5. **[OIDC** エンティティ] タブでエンティティレコードを使用して、OIDC クライアント構成と OIDC 接続フローを表示および変更できます。
   OIDC ベースの構成の詳細については、「Now Platform での OAuth OIDC プロバイダーの設定」を参照してください。
6. **[OIDC** プロバイダー構成] タブで、OIDC IdP の既知の構成 URL を表示して変更します。
7. オプション: [詳細] タブを開き、フィールドに入力します。

   [詳細] タブ

プロパティ	説明
Single Sign-on スクリプト	Single Sign-on 中に実行されるスクリプト。
ログアウトスクリプト	ユーザーがログアウトした後に実行されるスクリプト。

   注:
   スクリプトは、Single Sign-on およびログアウト時に実行されます。

8. 構成を有効にしてテストするには、[アクティブ **(Active)]** をクリックします。
9. レコードを更新するには、[更新] をクリックします。
   Facebook ベースのログインオプションがログインフォームに表示されます。
10. ログインフォームでログインするときは、次の操作を行います。
    a. Facebook オプションを選択します。
    b. ServiceNow インスタンスにログインするには、Facebook 資格情報を指定します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Facebook ベースの Single Sign-on (SSO) の構成

Facebook ベースの SSO を ServiceNow インスタンスに構成します。

始める前に
Facebook から IdP として構成された有効なクライアント ID が必要です。

以下のプロパティを有効にします。

- マルチプロバイダー SSO を有効にします。
- マルチプロバイダー SSO 統合に対してデバッグログを有効にします。

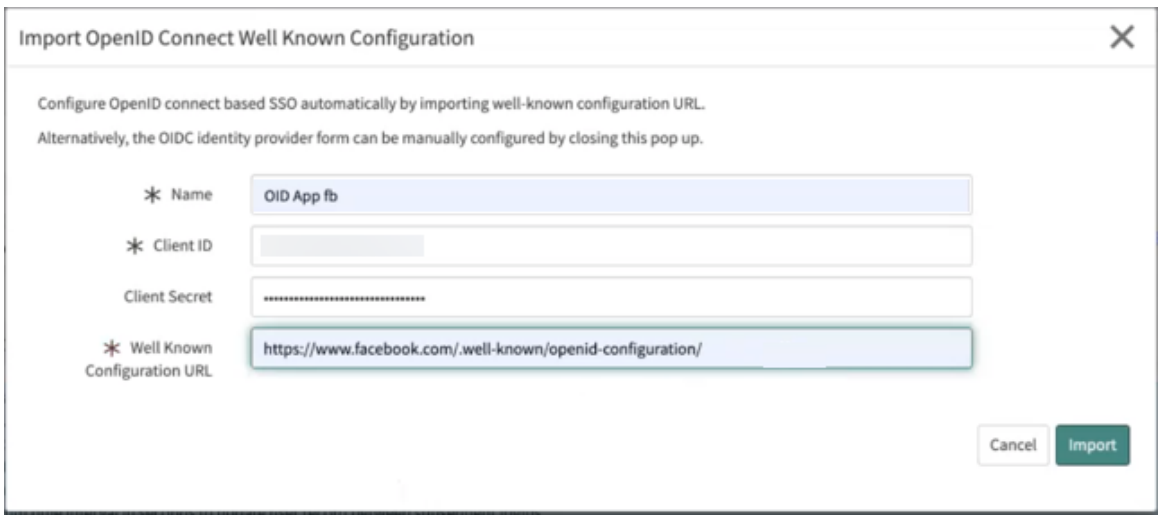
必要なロール：管理者

手順

1. 移動先 すべて > マルチプロバイダー **SSO** > **ID** プロバイダー.
2. 新しい Facebook ID プロバイダーを作成するには、[新規] をクリックします。
3. **[OpenID Connect]** をクリックします。
4. フォームのフィールドに入力します。

[OpenID Connect の既知の構成をインポート] フォーム

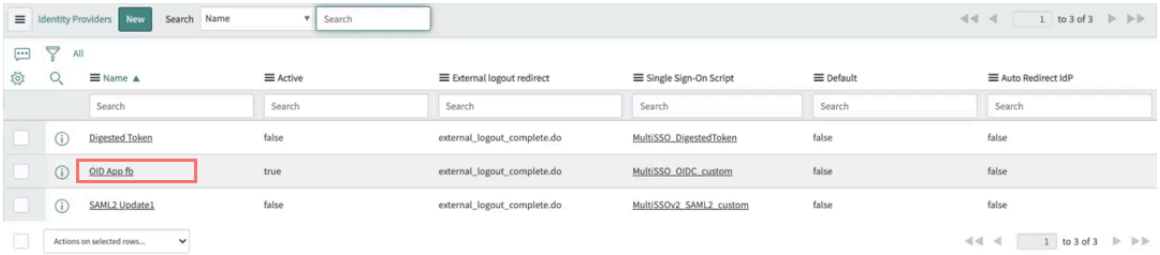
フィールド	説明
名前	OIDC ID プロバイダー構成の一意の名前。
クライアント ID	サードパーティの OIDC ID プロバイダーに登録されているアプリケーションのクライアント ID
クライアントシークレット	サードパーティの OIDC ID プロバイダーに登録されているアプリケーションのクライアントシークレット
既知の設定 URL	サードパーティ OIDC ID プロバイダーに関するメタデータを含む URL。



5. [インポート] をクリックします。
   Facebook ベースの IdP が作成されます。

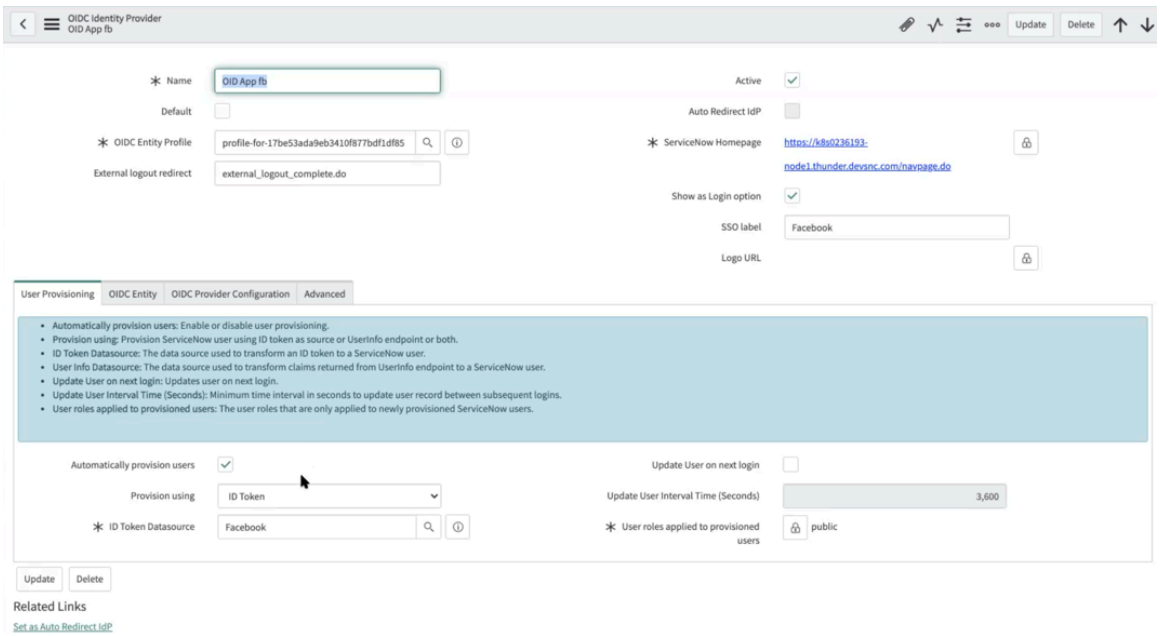
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



6. Facebook IdP を選択します。
7. Facebook idP で、次の操作を行います。
   a. [名前]、**[OIDC** エンティティプロファイル]、[外部のログアウトのリダイレクト]、**[ServiceNow** ホームページ] などのすべてのフィールドを検証します。
   b. **SSO** ラベルを入力します。
8. [ユーザープロビジョニング] タブで、ユーザーを特定のユーザープロビジョニングとロールに設定するために必要なフィールドを指定します。

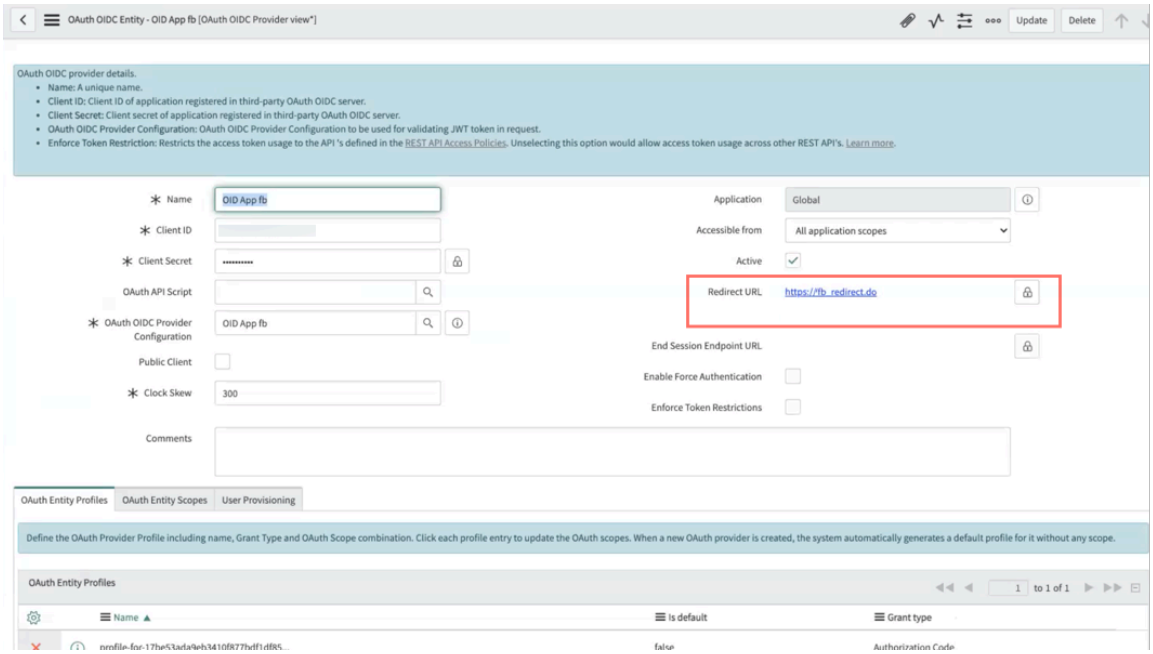
   必要なのは必須フィールドのみです。その他のフィールドは、必要に応じて指定できます。



9. **[OIDC** エンティティ] タブで、次の操作を行います。
   a. エンティティをクリックします。
   b. [リダイレクト **URL]** フィールドを Facebook リダイレクト URL に設定します。

自動翻訳

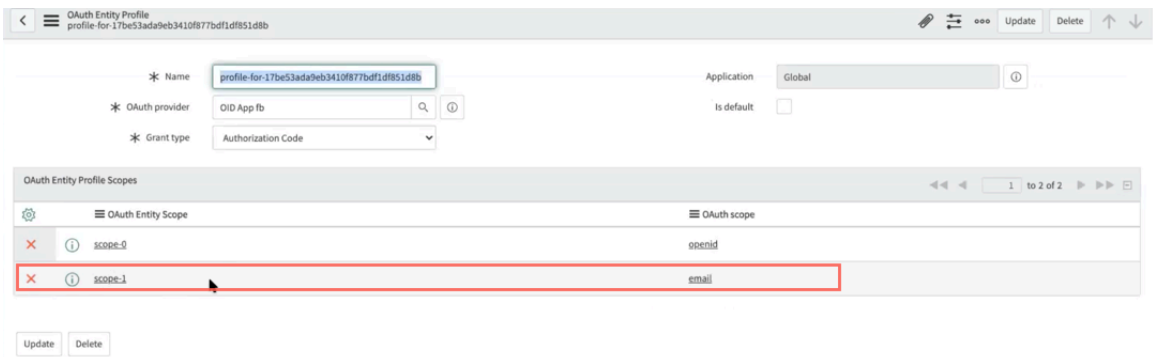
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



10. **[OAuth** エンティティプロファイル] タブで、次の操作を行います。

    a. プロファイルの詳細で、プロファイルをクリックします。

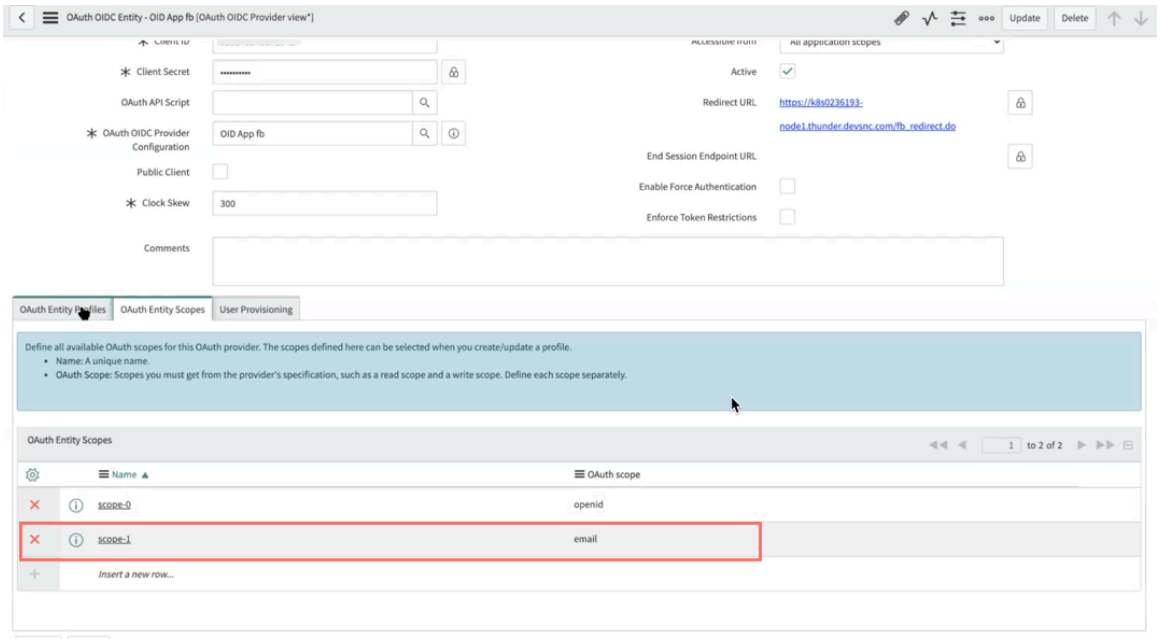
    b. スコープを選択し、詳細を確認します。
    たとえば、**[scope-1]** を選択します。



11. **[OAuth** エンティティスコープ] タブで **[scope-1]** リンクをクリックし、スコープを email として追加します。

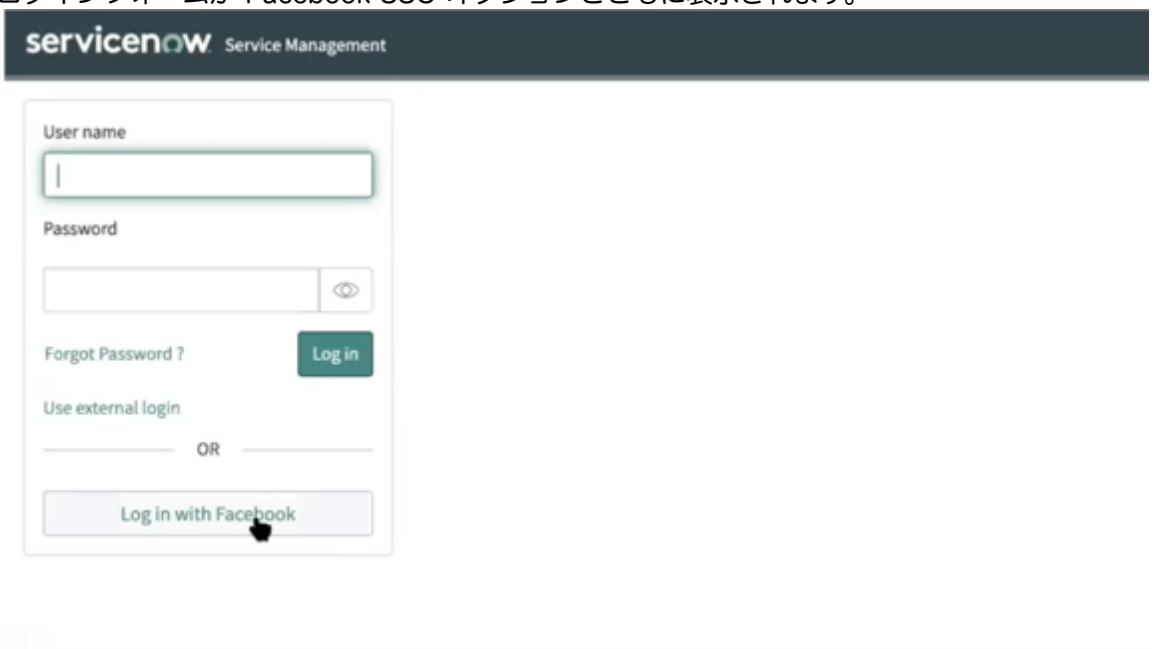
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



12. 構成を保存するには、ヘッダーを右クリックして [保存] をクリックします。
13. 構成をアクティブとして設定するには、[アクティブ **(Active)]** を選択します。

タスクの結果
ログインフォームが Facebook SSO オプションとともに表示されます。



自動翻訳

Single Sign-on (SSO) 用の **OpenID Connect (OIDC)** 構成の作成

Multi-Provider SSO プラグインを使用して、OpenID Connect (OIDC) 構成を作成または更新します。

始める前に

- OIDC アプリケーションを ID プロバイダー (IdP) に登録し、クライアント ID、クライアントシークレット、および既知の構成 URL をメモします。
- Multi-Provider SSO プラグインのアクティブ化

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- マルチプロバイダー SSO プロパティの設定
- Approval with e-Signature プラグインをアクティブ化して、OIDC IdP の電子署名を有効にします。
- 必要なロール：admin

Single Sign-on (SSO) 用の OpenID Connect (OIDC) 構成

ID プロバイダーのクライアント ID、クライアントシークレット、および既知の構成 URL がある場合は、SSO の OIDC 構成を直接インポートできます。

> **注:**
> Domain Separation プラグインがインストールされている場合、OIDC IdP を使用したログインオプションはサポートされません。

ID プロバイダーに関する必要な情報がない場合は、手動で SSO 用に OIDC を設定できます。構成が完了すると、ユーザーは Google Okta などのサードパーティのソーシャル ID プロバイダーを使用して ServiceNow アプリケーションにログインできます。

手順

1. 移動先 すべて > マルチプロバイダー **SSO** > **ID** プロバイダー.
2. 次のいずれかのオプションを選択します。
   - 既存の構成を更新するには、OIDC ID プロバイダーレコードをクリックします。
   - 新しい構成を作成するには、[新規] をクリックし、**[OpenID Connect]** を選択します。
3. 新しい構成の場合は、次のいずれかの方法で OIDC 構成情報を入力します。

オプション	説明
OpenID Connect の既知の構成をインポート	関連するクライアント資格情報とともに既知の構成 URL がある場合は、OIDC 構成を直接インポートできます。 **注:** OIDC の既知の構成をインポートすると、関連するすべてのフィールドが自動入力されます。
OIDC ID プロバイダーフォームの手動構成	既存の OAuth OIDC エンティティがない場合は、[OpenID Connect の既知の構成をインポート] ポップアップを閉じて、[OIDC ID プロバイダー] フォームのフィールドに手動で入力します。

[OpenID Connect の既知の構成をインポート] のフィールド

プロパティ	説明
名前	OIDC ID プロバイダー構成の一意の名前。
クライアント ID	サードパーティの OIDC ID プロバイダーに登録されているアプリケーションのクライアント ID。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

プロパティ	説明
クライアントシークレット	サードパーティの OIDC ID プロバイダーに登録されているアプリケーションのクライアントシークレット。
既知の設定 URL	サードパーティ OIDC ID プロバイダーに関するメタデータを含む URL。

[OIDC ID プロバイダー] フォームのすべての必須フィールドに入力する必要があります。

OIDC ID プロバイダーフォームに手動で入力する前に、OIDC IdP の OAuth エンティティプロファイルがあることを確認してください。

OAuth エンティティプロファイルがない場合は、Okta、Azure などのデフォルトの外部 OIDC プロバイダーテンプレートを使用して作成できます。

OAuth エンティティプロファイルの権限許可タイプには、認証コードが入っている必要があります。詳細については、「Now Platform で OAuth OIDC プロバイダーを構成する (Configure an OAuth OIDC provider on the Now Platform)」を参照してください。

注:
Multiple Provider Single Sign-On Installer プラグインのデモデータでは、サードパーティの ID プロバイダーである Auth0、Azure AD、Google、および Okta のテンプレートを使用できます。

OIDC ID プロバイダーのフィールド

プロパティ	説明
名前	OIDC ID プロバイダーレコードの名前
有効	OIDC IdP 構成をアクティブにするオプション **注:** このオプションは、テスト接続が成功した後にのみアクティブに設定できます。
デフォルト	OIDC 構成が複数ある場合に、OIDC IdP 構成をデフォルトとして設定するオプション
自動リダイレクト IdP	ID プロバイダーのログインページへユーザーを自動リダイレクトできるようにするオプション。このフィールドは、[自動リダイレクト **IdP** として設定] オプションが [関連リンク] セクションで設定されている場合に表示されます。 **注:** 新しい自動リダイレクト IdP 構成をアクティブにすると、*glide_sso_id* cookie が新しい自動リダイレクト IdP で自動的に更新されます。*glide.authenticate.sso.update.idp.cookie* システムプロパティは、この機能を制御します。
OIDC エンティティプロファイル	OIDC 構成の OAuth エンティティプロファイル。
ServiceNow のホームページ	認証に使用されるログイン ページの URL。このフィールドは、自動的にインスタンス URL に設定されます。URL の形式は https://yourinstance.service-now.com/navpage.do です。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

プロパティ	説明
外部のログアウトのリダイレクト	ログアウト後に統合によりリダイレクトされる URL。通常は、SSO に使用されるポータルです。このフィールドは自動的に external_logout_complete.do に設定されます (例：https://yourinstance.service-now.com/external_logout_complete.do)。
ログインオプションとして表示	OIDC IdP をログインページのログインオプションとして表示するオプション。ログインオプションは 、**[ID プロバイダーでログイン (login with Identity provider)]** ボタンとして表示されます。
SSO ラベル	ログインページに表示される OIDC IdP のラベル。このフィールドは、[ログインオプションとして表示] が有効になっている場合にのみ表示されます。
ロゴ URL	OIDC IdP プロバイダーのロゴを含む公開 URL。このフィールドは、[ログインオプションとして表示] が有効になっている場合にのみ表示されます。

4. オプション: [ユーザープロビジョニング] タブ > [ユーザープロビジョニング] タブで自動ユーザープロビジョニングを有効にします。

   (Optional) ユーザーのログイン時に自動ユーザープロビジョニングを有効にするよう選択できます。自動ユーザープロビジョニングが有効になっている場合、ユーザーレコードが存在しなければ ServiceNow インスタンスに自動的に作成されます。

   [ユーザープロビジョニング] のフィールド

プロパティ	説明
ユーザーを自動プロビジョニング	自動ユーザープロビジョニングを有効にするオプション。このプロパティにより、ユーザーが IdP に存在するがユーザーテーブルに存在しない場合に、インスタンスユーザー (sys_user) テーブルにユーザーが作成されます。
プロビジョニングに使用	ID トークン、ユーザー情報エンドポイント、または ID トークンとユーザー情報の両方を ServiceNow ユーザーに変換するために使用するデータソース。ルックアップリストを使用して、事前定義されたデータソーステンプレートを選択し、レコードを開いて変換テーブルのマッピングを構成します。
データソースをプロビジョニング	ユーザーのプロビジョニングに使用される ID トークンデータソース。
ユーザー情報データソース	ユーザープロビジョニングに使用されるユーザー情報エンドポイントデータソース。このフィールドは、[プロビジョニングに使用] フィールドで [ユーザー情報] または [ID トークンとユーザー情報の両方 (Both ID Token and User Info)] が選択されている場合に表示されます。
次回のログイン時にユーザーを更新	次回のログイン時にユーザーを更新できるようにするオプション。
ユーザー更新の時間間隔 (秒)	後続のログインの間にユーザーレコードを更新するための最小時間間隔 (秒)。このフィールドは自動的に 3,600 秒に設定されます。たとえば、ユーザーがログインした後、次のログインまで 3,600 秒後にユーザーレコードが更新されます。このフィールドは、 [次回のログイン時にユーザーを更新] フィールドが有効になっている場合にのみ使用できます。
プロビジョニングされたユーザーに	新しくプロビジョニングされたユーザーに適用されるロールのリスト。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

プロパティ	説明
適用されるユーザーロール	

5. [OIDC エンティティ] タブ
エンティティレコードを使用して、OIDC クライアント構成と OIDC 接続フローを表示および変更できます。
6. [OIDC プロバイダー構成] タブ
OIDC IdP または ID トークン要求検証の既知の構成 URL を表示および変更できます。
7. オプション: [詳細] タブ

(Optional) Single Sign-on およびログアウト時に実行されるスクリプト

[詳細] フィールド

プロパティ	説明
Single Sign-on スクリプト	Single Sign-on 中に実行されるスクリプト。このフィールドは自動的に MultiSSO_OIDC_custom に設定されます。
ログアウトスクリプト	ユーザーがログアウトした後に実行されるスクリプト。このフィールドは自動的に MultiSSO_OIDC_logout_custom に設定されます。

8. オプション: [電子署名の承認 (eSignature Approval)] タブで、OIDC IDp の電子署名を構成します。

> 注:
> [電子署名の承認 (eSignature Approval)] タブは、 **Approval with e-Signature** プラグイン (com.glide.e_signature_approvals) をインストールした場合にのみ表示されます。

[電子署名の承認 **(eSignature Approval)]** フィールド

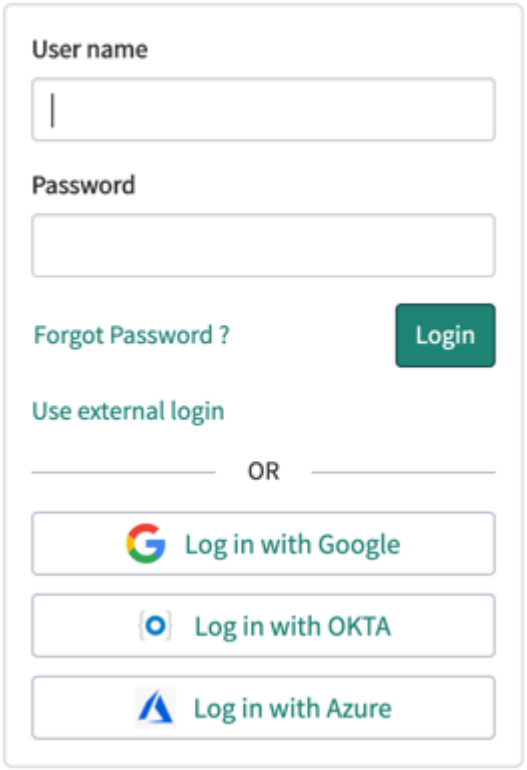
プロパティ	説明
eSignature 認証用の Assertion Consumer URL	eSignature の OIDC 認証を処理する方法をカスタマイズして使用する場合は、独自のコンシューマー URL を設定できます。たとえば、マルチプロバイダー SSO を使用している場合は、このプロパティを使用する必要はありません。URL の形式は https://yourinstance.service-now.com/consumer.do です。
認証ポップアップダイアログの幅	認証ポップアップダイアログの幅。このフィールドは自動的に 800 に設定されます。
認証ポップアップダイアログの高さ	認証ポップアップダイアログの高さ。このフィールドは自動的に 900 に設定されます。

9. オプション: インスタンスのログインページに移動して、IdP がログインオプションとして表示されていることを確認します。
URL は、次の形式にする必要があります。https://yourinstance/login_with_sso.do?glide_sso_id=sysId_IdP

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注:
[ログインオプションとして選択 **(Selected as login Option)]** を有効にしている場合は、インスタンスのログイン URL に移動できます。



SAML

セキュリティアサーションマークアップ言語 (SAML) は、セキュリティドメイン間で認証および承認データを交換するための XML ベースの規格です。

SAML は、ID プロバイダー (アサーションのプロデューサー) とサービスプロバイダー (アサーションのコンシューマー) の間でセキュリティ情報を交換します。SAML は OASIS セキュリティサービス技術委員会の製品です。正しく実装された場合、SAML は利用可能な Single Sign-on (SSO) の最も安全な方法のひとつになります。

SAML 2.0 統合では、XML トークンを外部の ID プロバイダー (IdP) と交換することで SSO が有効になります。IdP はユーザーを認証し、NameID トークンをシステムに渡します。一致する NameID トークン (メールアドレスなど) を持つユーザーが見つかると、インスタンスはそのユーザーをログインさせます。

SSO 認証に SAML 2.0 プラグインを使用している場合は、glide.ui.rotate_sessions プロパティを false に設定する必要があります。設定しない場合、インスタンスと ID プロバイダーの間で行われるセッション情報の共有が妨げられます。昇格された security_admin 権限を持つユーザーは、このプロパティにアクセスできます。

注:
既存の SAML 2.0 統合を使用しているお客様には、Multi-Provider SSO プラグインへのアップグレードをお勧めします。

SAML 2.0 のアクティブ化と設定

Integration - Multiple Provider Single Sign-On Installer プラグインを使用して SAML 2.0 をアクティブ化します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

始める前に

注:

必要なロール：Admin

Integration - Multiple Provider Single Sign-on Installer プラグインをアクティブ化して SAML 2.0 認証を設定します。プラグイン名を検索してクリックするように指示された場合は、このプラグインを参照してください。

手順

1. 移動先 すべて > システムアプリケーション > 利用可能なすべてのアプリケーション > すべて.
2. フィルター基準と検索バーを使用してプラグインを検索します。

   名前または ID でプラグインを検索できます。プラグインが見つからない場合は、ServiceNow 担当者から要求する必要があります。
3. [インストール] を選択して、[プラグインをアクティブにする] ダイアログボックスで、[アクティブ化] をクリックします。

   注:
   ドメイン分離と代理管理者がインスタンスで有効になっている場合、管理ユーザーはグローバルドメインに含まれている必要があります。それ以外の場合、次のエラーが表示されます： 別の操作が実行されているため、アプリケーションのインストールは利用できません：<プラグイン名> のプラグインの有効化。

ID プロバイダー (IdP) システムのプロパティ

一般に、IdP は認証およびログアウトのメタデータを含む XML ドキュメントを提供します。

たとえば、SSOCircle はメタデータ をオンラインで公開しています。

IdP メタデータを参照して、次のエントリを見つけます。

- HTTP-Redirect の値を含む Binding 属性を持つ SingleSignOnService 要素。Location 属性には、AuthnRequest サービスのために統合に必要な URL がリストされます。
- HTTP-Redirect の値を含む Binding 属性を持つ SingleLogoutService 要素。Location 属性には、SingleLogoutRequest サービスに必要な URL がリストされます。

注:
SAML 2.0 統合は、HTTP リダイレクトによる IdP サービスへのバインディングのみをサポートしています。

例：

```
<SingleSignOnServiceBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"Location="https://idp.ssocircle.com:443/sso/SSORedirect/metaAlias/ssocircle"/>
```

```
<SingleLogoutServiceBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"Location="https://
idp.ssocircle.com:443/sso/IDPSloRedirect/metaAlias/ssocircle"ResponseLocation="https://
idp.ssocircle.com:443/sso/IDPSloRedirect/metaAlias/ssocircle"/>
```

IdP 発行者 URL の設定

セキュリティトークンを発行する IdP の URL を指定します。

始める前に
必要なロール：管理者

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

このタスクについて
統合では、各 SAML 応答に含まれ、このシステムプロパティにリストされている URL が、*Issuer* 要素にリストされている URL と同じであることが確認されます。例を次に示します。

```
<samlp:Responsexmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
 Destination="https://demoi2.service-now.com/navpage.do"
 ID="s28da6774c88ae1eab292bf25fe625db81919d8e1e"
InResponseTo="SNC841720c227c81948cfd68cadcad235c6"
IssueInstant="2012-01-30T20:07:10Z"  Version="2.0"><saml:Issuer
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">http://idp.ssocircle.com</saml:Issuer>
  ...
  <saml:Assertion xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
    ID="s2f347f973c063836cf70ea38302d94976f9c5b851"
IssueInstant="2012-01-30T20:07:10Z"
Version="2.0"><saml:Issuer>http://idp.ssocircle.com</saml:Issuer>
    ...
  </saml:Assertion></samlp:Response>
```

手順

1. 移動先 すべて > **SAML 2** シングルサインオン > プロパティ.
2. [ユーザー情報と一緒に *SAML2* セキュリティトークンを発行する *ID* プロバイダの *URL]* プロパティで IdP への URL を入力します。

   各 IdP URL は一意である必要があります。デフォルトでは、SSOCircle への URL が統合に含まれます。詳細については、「http://idp.ssocircle.com」を参照してください。

AuthnRequest サービス **URL** の設定

IdP のメタデータを使用して、統合の IdP の要求サービス URL を設定します。

始める前に
必要なロール：管理者

手順

1. プロパティ *[ID* プロバイダーの *AuthnRequest* サービスのベース URL。AuthnRequest は、この *URL* に *SAMLRequest* パラメーターとしてポストされます] で、SingleSignOnService 要素から取得した HTTP リダイレクトバインディングへの URL を入力します。
2. *[AuthnRequest* に署名] の横にあるチェックボックスをオンにすると、ID プロバイダーの Single Sign-on サービスが署名済みの AuthnRequest を受信できるようになります。
3. プロパティ [セッションが認証されないために *SAML 2.0 Single Sign-on* に失敗した場合、またはこれが最初のログインである場合は、この *URL* にリダイレクトされます。これは、最初の *SAML 2.0 AuthnRequest* が *SAMLRequest* パラメーターを使用して送信されたベース *URL* です。] で、SingleSignOnService 要素から取得した HTTP リダイレクトバインディングへの URL を入力します。

   デフォルトでは、SSOCircle サービスへの URL が統合に含まれます。

SingleLogoutRequest サービス **URL** の設定

IdP のメタデータを使用して、統合の IdP の要求サービス URL を設定します。

始める前に
必要なロール：管理者

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

手順

1. *[ID プロバイダーの SingleLogoutRequest サービスのベース URL。LogoutRequest は、この URL に SAMLRequest パラメーターとしてポストされます]* プロパティで、SingleLogoutService 要素から取得された URL を入力します。
   LogoutRequest は、この URL に SAMLRequest パラメーターとしてポストされます。デフォルトでは、SSOCircle サービスへの URL が統合に含まれます。
2. [ログアウト後にユーザーをリダイレクトする URL。通常は *SSO* を有効にしたポータルに戻る *(http://portal.companya.com/logout* など)] プロパティで、ユーザーが正常にログアウトした後にリダイレクトする URL を入力します。

   IdP でフォームベースの認証を使用する場合は、IdP のログインフォームへの URL を入力します。IdP で Kerberos などのフォームベース以外の認証方法を使用する場合は、URL を静的ログアウトページに設定する必要があります。このようにすると、ログアウトしたユーザーがすぐに IdP にリダイレクトされて再度ログインさせられることはありません。デフォルトでは、統合には静的 UI ページ external_logout_complete.do への URL が含まれています。

(オプション) 署名付きログアウト要求の有効化

一部の IdP では、サービスプロバイダーが証明書を使用してログアウト要求に署名する必要があります。

始める前に
必要なロール：管理者

このタスクについて
IdP で署名されたログアウト要求が必要な場合は、IdP のメタデータを使用して次のシステムプロパティを設定します。

手順

1. [詳細] タブで、プロパティ *[LogoutRequest* の署名] 署名済みの *LogoutRequest* を *ID* プロバイダーの *SingleLogoutRequest* サービスが必要とする場合は、このプロパティを *True* に設定します] では、[はい] を選択すると IdP には署名されたログアウト要求が必要であることが指定され、[いいえ] を選択すると署名なしのログアウト要求が使用されます。
2. *[LogoutRequest* の署名] に対して [はい] を選択した場合は、*[ID* プロバイダーの *SingleLogoutRequest* サービスのプロトコルバインディング(値には、「urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect」または「urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST」のいずれかを指定できます)] プロパティに、SingleLogoutService 要素の Binding 属性にリストされているサポート対象の値を 1 つ入力します。

   デフォルトでは、統合には HTTP リダイレクトバインディングが使用されます。
3. [更新] をクリックします。
4. サービスプロバイダー (SP) キーストアをインストールします。

サービスプロバイダー **(SP)** システムプロパティ

これらのシステムプロパティは、インスタンスがサービスプロバイダーとして IdP とやり取りする方法を定義します。

順序に従って操作し、IdP をサービスプロバイダーとして定義します。

SAML のインスタンス **URL** の設定

インスタンス固有の URL を設定して、IdP がユーザーを認証できるようにします。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

始める前に
必要なロール：管理者

手順

1. *[Service-now* インスタンス (通常はこのインスタンス) *(The URL to the Service-now instance (usually this instance))]* プロパティに、IdP が認証するインスタンスの URL (ログインページを含む) を入力します。
   例：https://yourinstance.service-now.com/navpage.do
2. プロパティ [エンティティ ID、または発行者] で、IdP が認証するインスタンスのベース URL (ログインページを除く) を入力します。
   例：https://yourinstance.service-now.com/

SAML の対象 URL の設定

対象者プロパティを使用して、SAML 応答の意図した受信者であることをインスタンスで確認できます。

始める前に
必要なロール：管理者

このタスクについて
統合では、各 SAML 応答に含まれ、このシステムプロパティにリストされている URL が、*Audience* 要素にリストされている URL と同じであることが確認されます。例を次に示します。

```
<samlp:Responsexmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
 ID="s2cdc74f37f923e26fe1aeec42b70a93d24230334f"
InResponseTo="90AA6073F01567BFB0DF194F596314E2"
 Version="2.0"  IssueInstant="2010-04-29T23:21:51Z"
Destination="https://dloomac.service-now.com/navpage.do">
...
<saml:Conditions NotBefore="2012-01-30T19:57:10Z"
 NotOnOrAfter="2012-01-30T20:17:10Z"><saml:AudienceRestriction><saml:Audience>http
s://
demoi2.service-now.com</saml:Audience></saml:AudienceRestriction></saml:Conditions>
...
</samlp:Response>
```

手順

1. 移動先 すべて > **SAML 2** シングルサインオン > プロパティ.
2. プロパティ *[SAML2* トークンを受け入れる対象者 *URI* (通常、インスタンス URI。例：*https://<instance name>.service-now.com)]* で、インスタンスの URL を入力します。
   たとえば https://demoi2.service-now.com などです。この URL は、SAML 応答の *Audience* 要素の値と一致する必要があります。
3. [更新] をクリックします。

SAML の NameID ポリシーの設定

SAML の NameID ポリシーを設定します。SAML 2.0 では、IdP がサービスプロバイダーと NameID トークンを交換する必要があります。

始める前に
必要なロール：管理者

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

このタスクについて
SAML 2.0 統合の場合、NameID トークンをユーザーテーブルの特定のフィールドにマッピングする必要があります。統合では、NameID トークンの値を使用して、IdP が認証するユーザーを決定します。

手順

1. IdP メタデータを参照して、emailAddress の値を含む NameIDFormat 要素を見つけます。この要素の値は、統合で使用されるデフォルトの形式です。
2. 他の NameIDFormat 要素を確認して、ユーザーテーブルの他のフィールドに一致する形式があるかどうかを判断します。

NameID トークンに一致するユーザーテーブルフィールドの判別

ID プロバイダーは、NameID トークンの形式を指定します。

始める前に
必要なロール：管理者

このタスクについて
SAML 2.0 を設定するには、 NameID トークンの形式に一致するフィールドをユーザーテーブルから選択する必要があります。通常、IdP には NameID トークンとしてメールアドレスを使用するオプションがあります。ユーザーテーブルにはメールフィールドが含まれているため、このフィールドが NameID トークンとして使用するための論理的な選択肢となります。ユーザーテーブルの別のフィールドを NameID トークンとして使用する場合は、まず IdP がユーザーテーブルのフィールドの値と一致する NameID 形式を提供していることを確認します。この場合、ユーザーテーブルへフィールドの追加が必要になることがあります。

手順

1. IdP の NameIDFormat 要素で利用可能な形式を、ユーザーテーブルのフィールドと比較します。
2. ユーザーテーブルに一致する値がある NameID 形式を選択します。
3. *[SAMLResponse* の件名の *NameID* 要素と照合する [ユーザー] テーブルフィールド] フィールドに、NameID トークンで一致する値を検索するための [ユーザー] テーブルフィールドの名前を入力します。

   デフォルトでは、統合でメールフィールドを使用します。

IdP NameID ポリシーの設定

IdP が NameID トークンに使用する形式を指定します。

始める前に
必要なロール：管理者

このタスクについて
この形式は、IdP のメタデータの一部としてリストされます。

手順

1. プロパティ *[SAMLResponse* の件名の *NameID* を返すために使用する *NameID* ポリシー。SAML *ID* プロバイダーは、そのメタデータでポリシーを宣言して、これをサポートする必要があります。NameID 値は、[ユーザー] テーブルの特定のフィールドと照合し、ユーザーを検索するのに使用されます。] に、統合で使用される NameIDFormat 要素の値を入力します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

デフォルトでは、統合でメールアドレスに SSOCircle NameIDFormat を使用します。

2. [保存] をクリックします。

SAML の [ユーザー] テーブルフィールドの値

統合の [ユーザー] テーブルフィールドには、適切な一致する値が確実に含まれるようにします。

たとえば、統合がメールフィールドを NameID トークンとして使用する場合は、インスタンスに IdP と同じメールアドレスがリストされていることを確認してください。統合では、NameID トークンに一致する値を持たないユーザーを認証できません。

(オプション) SAML の認証コンテキストクラスを提供可能にする

インスタンスの優先認証要求形式を含む認証コンテキストクラス要求を IdP に送信できるようにすることができます。

始める前に
必要なロール：管理者

このタスクについて
AuthContextClass メッセージの作成を可能にする場合は、認証コンテキストクラス参照形式も指定する必要があります。

> **注:**
> IdP の中には、サービスプロバイダーによる認証コンテキストクラスの設定を許可しないものがあります。この設定を無効にすると、IdP が認証コンテキストクラスを選択できるようになります。

手順

1. *[AuthnRequest* ステートメントに *AuthnContextClass* 要求を作成します] プロパティから、[はい] を選択して Password Protected Transport などの特定のコンテキストクラスを指定するか、[いいえ] を選択して最も適切なコンテキストクラスを IdP が選択するようにします。
2. *[AuthnRequest* ステートメントに *AuthnContextClass* 要求を作成します] に [はい] を選択した場合は、 *[SAML 2.0 AuthnRequest to the Identity Provider* で要求する *AuthnContextClassRef* メソッド *(The AuthnContextClassRef method that we will request in our SAML 2.0 AuthnRequest to the Identity Provider)]* プロパティに、認証に使用するコンテキストクラスの URN を入力します (表を参照)。

AuthnContextClass URN オプション

認証タイプ	認証コンテキストクラス URN
フォームベースの認証	urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport
Kerberos ベースの認証	urn:federation:authentication:windows

デフォルトでは、Password Protected Transport 認証メソッドが統合で使用されます。

3. [更新] をクリックします。

(オプション) SAML のログアウト要求に署名するためのキーストアプロパティの設定

キーストアプロパティを設定すると、統合で署名済みサーバーと署名済み CA 証明書を使用してログアウト要求に署名できます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

始める前に
必要なロール：管理者

手順

1. プロパティ *[SAML 2* 要求の署名に使用する *SAML 2.0 SP Keystore* に保存されているキーエントリのエイリアス *(The alias of key entry stored in SAML 2.0 SP Keystore used to sign SAML 2 requests)]* に、SAML 2.0 Keystore 用に作成したエイリアス名を入力します。
   デフォルトでは、統合はエイリアス *saml2sp* を検索します。
2. プロパティ *[SAML 2* 要求の署名に使用する *SAML 2.0 SP Keystore* に保存されているキーエントリのパスワード *(The password of key entry stored in SAML 2.0 SP Keystore used to sign SAML 2 requests)]* に、SAML 2.0 Keystore のパスワードを入力します。
   デフォルトでは、パスワードはデフォルトのエイリアス名と同じです。
3. [更新] をクリックします。
4. SP メタデータを再生成します。
   詳細については、「SP メタデータ」を参照してください。

SAML のサービスプロバイダーキーストアの作成

インスタンスがログアウト要求に署名するには、次のアイテムを含む Java キーストアを作成する必要があります。

始める前に
必要なロール：admin

このタスクについて

- インスタンスの署名済みサーバー証明書
- 署名済み CA 証明書
- 公開鍵と秘密鍵のペア

プライベート認証局で独自の署名付き証明書を作成することも、パブリック認証局から購入することもできます。

次の手順は、新しい Java Keytool キーストアファイルを生成し、証明書の署名要求 (CSR) を作成し、証明書をインポートする方法を示しています。ルート証明書や中間証明書はいずれも、ドメインのプライマリ証明書をインポートする前にインポートする必要があります。コマンドラインインターフェイスで次のコマンドを入力します。

> **注:**
> これらの手順はプラットフォーム固有のものではなく、完了するためにはセキュリティ証明書に関する技術的な知識が必要です。テクニカルサポートは証明書の作成を支援できません。

手順

1. Java キーストアとキーペアを生成します。

```
keytool -genkey -alias mydomain -keyalg RSA -keystore my.keystore
```

2. 既存の Java キーストアの CSR を生成します。

```
keytool -certreq -alias mydomain -keystore my.keystore -file mydomain.csr
```

3. ルートまたは中間認証局 CA 証明書を既存の Java キーストアにインポートします。

```
keytool -import -trustcacerts -alias root -file Thawte.crt -keystore my.keystore
```

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

4. 署名済みプライマリ証明書を既存の Java キーストアにインポートします。

```
keytool -import -trustcacerts -alias mydomain -file mydomain.crt -keystore my.keystore
```

SAML 要求に署名するためのサービスプロバイダーキーストアのインストール

次の手順では、既存のサンプルキーストアを削除し、公開鍵と秘密鍵のペアを含む独自のサービスプロバイダーキーストアをインストールします。

始める前に
必要なロール：管理者

手順

1. サービスプロバイダーキーストアを作成します。
2. 移動先 **SAML 2** シングルサインオン > 証明書 または マルチプロバイダー > 管理者 > **x509** 証明書.
3. **[SAML 2.0 Keystore_Key2048_SHA256]** をクリックします。
4. [添付ファイルを管理] リンクをクリックします。
5. *[saml2sp_key2048withsha256.jks]* の横にある [削除] チェックボックスをオンにします。
6. [削除] をクリックします。
7. [ファイルを選択] をクリックし、署名付き証明書を含むキーストアを選択します。
8. [添付] をクリックします。
9. [添付ファイル] ポップアップを閉じます。

   注:
   新しく添付された証明書には別の名前を指定することをお勧めします。

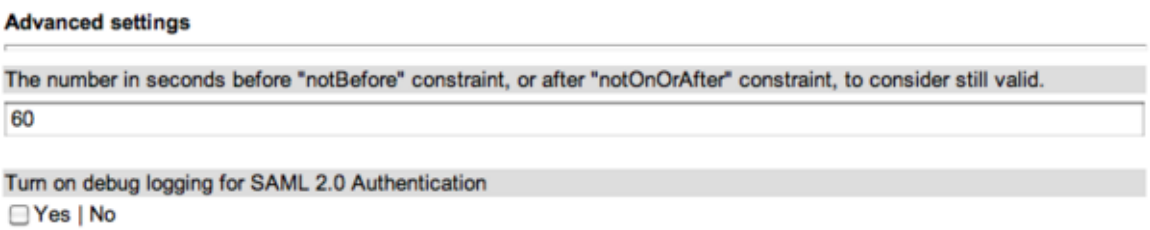
10. [キーストアパスワード] に、SAML 2 エイリアスにアクセスするためのパスワードを入力します。
11. [更新] をクリックします。

(オプション) 詳細な SAML プロパティ

次の詳細設定を使用すると、セキュリティを強化し、統合をデバッグできます。

詳細設定

移動先 すべて > **SAML 2** シングルサインオン > プロパティ.



自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

詳細システムプロパティテーブル

プロパティ	説明
「notBefore」制約の前、または「notOnOrAfter」制約の後に、まだ有効であるとみなされる時間の秒数。	IdP クロックと SP クロックの時差を考慮して、*NotBefore* および *NotOnOrAfter* の制約に追加する秒数を入力します。これらの制約は、指定された期間内に行われない要求を拒否することによって、リプレイ攻撃を防止します。IdP クロックと SP クロックが大幅に異なる場合、ネットワーク遅延により SAML 要求が認可されないことがあります。このプロパティは、SAML 要求と応答がまだ有効であると見なされる猶予期間を追加します。
SAML 2.0 認証のデバッグロギングをオンにします	[はい] を選択すると、SAML 2.0 イベントの追加のログ情報が有効になります。

ID プロバイダー証明書のインストール

ID プロバイダーがサービスプロバイダーとの通信を検証できるように、PEM 証明書を X.509 証明書フォームに貼り付けることができます。

始める前に
必要なロール：管理者

このタスクについて
IdP の証明書は IdP のメタデータ内にあります。IdP 開発者は、ローカル IdP を作成するときに証明書のメタデータをどこに置くか決定します。

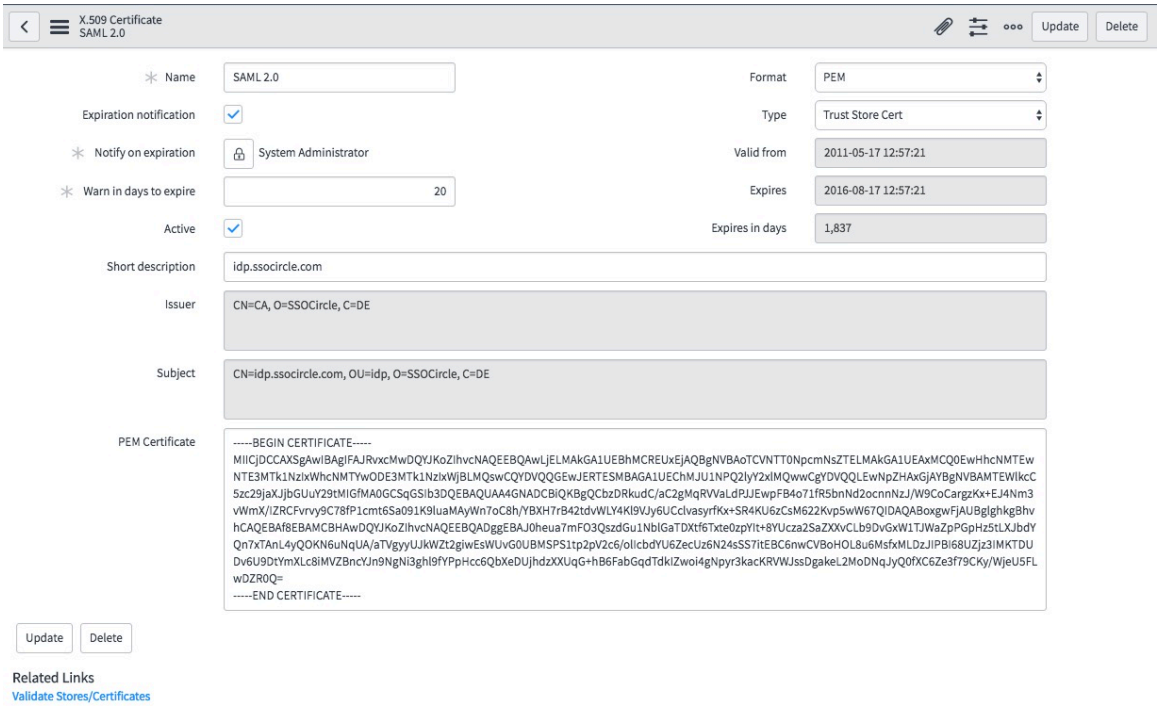
> **注:**
> Single Sign-on の証明書は、SAML 証明書を扱うため、常に PEM 形式になっている必要があります。

手順

1. 移動先 すべて > **SAML Single Sign-on** > 証明書.
2. フォームフィールドに入力します (表を参照)。
3. [保存] をクリックします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



注:
統合は現在、インスタンスと IdP 間の通信で証明書に署名しません。

フィールド	説明
名前	証明書名。[名前] エントリは変更しないでください。統合で X.509 証明書を使用するには、その名前が *SAML 2.0* である必要があります。この要件は、複数プロバイダーの Single sign-on (SSO) を使用していない場合にのみ当てはまります。
有効期限通知	[期限切れ時に通知] フィールドで選択したユーザーに通知を送信するには、このオプションを選択します。デフォルトでは、これは有効になっています。
期限切れ時に通知	証明書の有効期限に関する通知を有効にするユーザーを選択します。ユーザーが選択されていない場合、ログインしているユーザーは、最後にログインした 2 人の管理者ロールとともに追加されます。
有効期限切れ前に警告	インスタンスが通知を送信する期限切れまでの日数。20 以上の値を入力してください。Istanbul 以降のリリースにアップグレードしたインスタンスでは、より大きい値を指定しない限り、この値は 20 に設定されます。
アクティブ	この証明書がアクティブであることを示すチェックボックス。
フォーマット	証明書の形式。SAML は PEM 形式を使用します。
タイプ	証明書コンテナー。インスタンスは、トラストストア、Java キーストア、および PKCS#12 キーストアからの証明書を認識します。
有効開始日	インスタンスは、証明書の有効開始日を自動的にこのフィールドに追加します。証明書を X.509 証明書レコードに添付して、このフィールドに入力します。
有効期限	インスタンスは、証明書の有効期限をこのフィールドに自動的に追加します。証明書を X.509 証明書レコードに添付して、このフィールドに入力します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
数日中に期限切れ	有効期限までの計算された日数。
簡単な説明	証明書の説明。
問題	インスタンスは、証明書発行者をこのフィールドに自動的に追加します。証明書を X.509 証明書レコードに添付して、このフィールドに入力します。
件名	インスタンスは、このフィールドの対象となる証明書を自動的に追加します。証明書を X.509 証明書レコードに添付して、このフィールドに入力します。
PEM 証明書	X509 証明書の値を入力します。

次のタスク
[ストア/証明書を検証] をクリックして、トラストストアと証明書をテストします。

SAML の欠落している証明書を置き換える

証明書モジュールに空白のページが表示される場合は、SAML 2.0 証明書レコードが削除されています。証明書レコードを手動で作成することで、欠落している証明書を置き換えることができます。

始める前に
必要なロール：管理者

手順

1. 移動先 すべて > システム定義 > 証明書.
2. SAML 2.0 という新しいレコードを作成します。

> **重要:**
> この名前を使用する必要があります。この要件は、複数プロバイダーの Single sign-on (SSO) を使用していない場合にのみ当てはまります。

3. クリック **SAML 2** シングルサインオン > 証明書.
4. *[PEM* 証明書] フィールドで、IdP のメタデータから ds:X509Certificate 要素の値を入力します。
5. [保存] をクリックします。

SAML 要求に署名するためのサービスプロバイダーキーストアのインストール

次の手順では、既存のサンプルキーストアを削除し、公開鍵と秘密鍵のペアを含む独自のサービスプロバイダーキーストアをインストールします。

始める前に
必要なロール：管理者

手順

1. サービスプロバイダーキーストアを作成します。
2. 移動先 **SAML 2** シングルサインオン > 証明書 または マルチプロバイダー > 管理者 > **x509** 証明書.
3. **[SAML 2.0 Keystore_Key2048_SHA256]** をクリックします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

4. [添付ファイルを管理] リンクをクリックします。
5. *[saml2sp_key2048withsha256.jks]* の横にある [削除] チェックボックスをオンにします。
6. [削除] をクリックします。
7. [ファイルを選択] をクリックし、署名付き証明書を含むキーストアを選択します。
8. [添付] をクリックします。
9. [添付ファイル] ポップアップを閉じます。

   注:
   新しく添付された証明書には別の名前を指定することをお勧めします。

10. [キーストアパスワード] に、SAML 2 エイリアスにアクセスするためのパスワードを入力します。
11. [更新] をクリックします。

SAML 統合のテスト

他のすべてのセットアップタスクを完了した後、SAML 統合をテストします。

始める前に
必要なロール：管理者

手順

1. admin ロールを持つユーザーとしてインスタンスにログインします。
2. 移動先 **SAML 2** シングルサインオン > プロパティ.
3. [外部認証を有効にします] プロパティで、[はい] を選択します。

   注:

   外部認証を有効にするには、すべてのユーザーが SAML 2.0 Single Sign-on を使用する必要があります。誰かが未認証の状態でアプリケーションにアクセスしようとすると、インスタンスは自動的に (IdP に) 認証要求を送信し、ユーザーを [SAML IdP 認証 (SAM IdP Authentication)] ページにリダイレクトします。

4. [保存] をクリックします。
5. インスタンスからログアウトします。
6. インスタンス URL を参照します。
   統合が正常に機能している場合、IdP はユーザーの資格情報を要求します。

関連情報

マルチ SSO (SAML 2.0) のエラーと修正

マルチ SSO (SAML 2.0) のエラーと修正

マルチ SSO (SAML 2.0) のセットアップと構成に関する一般的なエラーと関連する修正のリスト。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

マルチ **SSO (SAML 2.0)** セットアップ中のエラー

インスタンスログのエラー	テスト接続メッセージ	**SAML** プロパティ	診断	修正
NotAfter：<Thu Jun 05 22:57:44 PDT 2014>	IDP x509 証明書が存在し、有効かつアクティブであることを確認してください。	適用外	現在の証明書または SAML アサーションの有効期限が切れました。	• SNC クロックを SAML IdP サーバークロックと同期します。 • SAML 2.0 証明書レコードを更新します。
• SAML 2.0 証明書を特定できません。 • ServiceNow インスタンスに保存されているデジタル署名が見つかりませんでした。(Could not find a digital signature stored in the ServiceNow instance.)	IDP x509 証明書が存在し、有効かつアクティブであることを確認してください。	PEM 形式の文字列を [PEM 証明書] フィールドに入力する必要があります。	SAML 証明書が存在しません。非アクティブの可能性があります。	正しい PEM 形式の証明書がインスタンスにアップロードされていることを確認します。
証明書が一致しません。(Certificates do not match.) 想定：<certStr>、実際：<inboundCert> (Expect: <certStr>, actual: <inboundCert>.)	IDP x509 証明書が存在し、有効かつアクティブであることを確認してください。	適用外	SNC で利用可能な証明書がアサーションの証明書と一致しません。次のような原因が考えられます。 • IdP では証明書が更新されているが、ServiceNow インスタンスで更新されていない。 • 証明書の形式が正しくない。	SAML 2.0 証明書レコードの PEM 形式の文字列が、ユーザー IdP の SAMLResponse の X509 証明書と一致していることを確認します。
証明書の有効性の確認に失敗しました。(Failure to check the validity of the certificate.)	IDP x509 証明書が存在し、有効かつアクティブであることを確認してください。	適用外	現在の証明書の有効期限が切れている可能性があります。	SAML 2.0 証明書レコードを更新します。
署名プロファイルの検証に失敗しました。(Failure to validate signature profile.)	IDP x509 証明書が存在し、有効かつ	適用外	アサーションが別の証明書で署名されている可能性があります。	IdP に SNC インスタンスと同じ証明書があるかどうかを確認します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

マルチ **SSO (SAML 2.0)** セットアップ中のエラー (続く)

インスタンスログのエラー	テスト接続メッセージ	**SAML** プロパティ	診断	修正
	アクティブであることを確認してください。			
SubjectConfirmationData の InResponseTo 属性が一致しません。(InResponseTo attribute in SubjectConfirmationData mismatch.) 想定：<inResponseTo>、実際：<inResponseTo> (Expect: <inResponseTo>, actual: <inResponseTo>.)	SubjectConfirmation の検証に失敗しました。	適用外	このエラーは、次のいずれかの状況が発生した場合に表示されます。 • IdP が別の SAMLRequest の SAMLResponse を返す場合 • ユーザーがインスタンス URL ではなく SAMLRequest を使用して URL をブックマークする場合 • null 値が想定される場合、インスタンスに複数のノードがあると、応答が別のノードに送信される可能性があります。	IdP 管理者は、想定される SAMLReponse が返されていることを確認する必要があります。この状況は、ロードバランサーまたはインフラストラクチャの問題である可能性があります。
SessionIndex 値が見つかりません：<メッセージ>... (SessionIndex value not found: <message>...)	SessionIndex が有効ではありません。(SessionIndex not valid.)	適用外	SNC インスタンスには SessionIndex が必要です。IdP はこれを SAML 応答で返して正常に認証します。	IdP 管理者は、SessionIndex が SAMLResponse で定義されていることを確認する必要があります。
有効な SubjectConfirmation が見つかりません。	SubjectConfirmation の検証に失敗しました。	適用外	IdP のエラーにより、条件が欠落している可能性があります。 応答の StatusCode には、想定される成功ではなくレスポンダーが含まれます。	SAMLResponse を確認して、SAMLResponse に条件が含まれているかどうかを判断します。 有効な件名確認データの有効期限が切れているか、対象者に対して適切でない可能性があります。
アサーション対象者が一致しません。(Assertion audience	[対象者 URI] フィールドが正し	SAML2 トークンを受け入れる対象	SNC インスタンスで構成された対象者 URI は、IdP の値と一致する必要があります。	ログの SAMLResponse で <saml2:Audience> を探し、値がインスタン

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

マルチ **SSO (SAML 2.0)** セットアップ中のエラー (続く)

インスタンスログのエラー	テスト接続メッセージ	**SAML** プロパティ	診断	修正
mismatch.) 想定：<propAudience>、実際：<audienceUri> (Expect: <propAudience>, actual: <audienceUri>.) または AudienceRestriction の検証に失敗しました。一致する対象者が見つかりません。(No matching audience found.)	く設定されていることを確認します (Ensure that the 'Audience URI' field is set correctly)	者 URI (通常、インスタンス URI。たとえば https://demo.service-now.com)。		スの値と一致することを確認します。
アサーションの発行者が無効です。想定：<value on instance>、実際：<value returned by IdP> (Expect: <value on instance>, actual: <value returned by IdP>)	アサーションの発行者が無効です。	ユーザー情報と一緒に SAML2 セキュリティトークンを発行する ID プロバイダの URL。	IdP エンティティ ID (発行者) が SNC インスタンスで定義された値と一致しません。	• IdP または SP の設定が不適切でないか確認します。 • SAML プロパティ (ユーザー情報と一緒に SAML2 セキュリティトークンを発行する ID プロバイダの URL) が正しく設定されているか確認します。
件名は将来有効になります。(Subject is valid in the future.) 現在：<now>、NotBefore：<notBefore> (Now: <now>, NotBefore: <notBefore>) または 件名の有効期限が切れました。(Subject is expired.) 現在：<now>、NotOnOrAfter：<notOnOrAfter> (Now: <now>, NotOnOrAfter: <notOnOrAfter>)	件名の検証確認に失敗しました。(Subject validation confirmation failed.)	notBefore 制約の前、または notOnOrAfter 制約の後に、まだ有効であるとみなされる時間の秒数。	IdP クロックが SP クロックと同期していません。	SAML プロパティ glide.authenticate.sso.saml2.clockske をより大きな値に更新します。デフォルトは 180 秒です。場合によっては 300 以上の設定が必要になります。IdP サーバーの時間も確認する必要があります。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

マルチ **SSO (SAML 2.0)** セットアップ中のエラー (続く)

インスタンスログのエラー	テスト接続メッセージ	**SAML** プロパティ	診断	修正
アサーションは将来有効になります。現在：<now>、notBefore：<notBefore> (Assertion is valid in the future, now: <now>, notBefore: <notBefore>) または アサーションの有効期限が切れました。現在：<now>、notOnOrAfter：<notOnOrAfter>	アサーションが無効です。	notBefore 制約の前、または notOnOrAfter 制約の後に、まだ有効であるとみなされる時間の秒数。	IdP クロックが SP クロックと同期していません	SAML プロパティをより大きな値に更新します。デフォルトは 60 秒です。場合によっては 300 以上の設定が必要になります。IdP サーバーの時間も確認する必要があります。

一般的なログインおよび **IdP** エラー

エラーまたは症状	診断	修正
高セキュリティがアクティブな場合、ログイン要求はシステムと IdP の間で無限ループを生成します。	• 通常、URL エンドポイントはエラーページまたはログアウトページになります。 • IdP ホスト名をプロパティ値に追加せずに *glide.security.url.whitelist* を定義すると、logout_redirect.do によってこのループが作成される可能性があります。 **注:** このプロパティの詳細については、「インスタンスセキュリティ強化設定」の「ログアウトリダイレクトの URL 許可リスト」を参照してください。	失敗した認証要求をこの URL にリダイレクトするには、システムプロパティ glide.authenticate.failed_redirect を設定 (または作成) します。
ユーザーまたは要求の認証に使用されるトークンが、署名アルゴリズム http://www.w3.org/2001/04/xmldsig-more#rsa-sha256 で署名されています。これは、想定される署名アルゴリズム http://www.w3.org/	イベントの詳細については、[アラートコンテキスト (Alert Context)] タブを確認してください。	[証明書利用者信頼設定 (Relying Party Trust configuration)] ダイアログの [詳細] タブに移動し、アルゴリズムが SHA-256 ではなく SHA-1 に設定されていることを確認します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

一般的なログインおよび **IdP** エラー (続く)

エラーまたは症状	診断	修正
2000/09/xmldsig#rsa-sha1 とは異なります。		
エラーメッセージ urn:oasis:names:tc:SAML:2.0:sta がシステムログ (syslog) テーブルに表示されます。	IdP (ADFS など) の応答が oasis:names:tc:SAML:2.0:status:Requester のステータスの場合は、送信された要求に関する問題が原因で IdP がログインを拒否したことを意味します。ほとんどの場合、IdP から受信した SAML 応答にはエラーの詳細が記載されていません。	IDP に送信された SAML 要求を確認し、IDP 管理者と協力してインスタンスの SAML 設定を更新して、エラーを回避してください。ログイン失敗の理由については、IDP プロバイダーにお問い合わせください。

シングルサインオン **(SSO)** ログインのリダイレクト

SSO を有効にすると、ユーザーを特定のページにリダイレクトしたり、ユーザーにローカルログインを誘導したりすることができます。

たとえば、ユーザーが https://customerX.service-now.com にアクセスしようとすると、デフォルトのログインページの代わりに社内ポータルが表示されます。または、ユーザーがアプリケーションからログアウトするときに、ブラウザーはユーザーを特定の内部ページにリダイレクトできます。インスタンス内でリダイレクトプロパティを設定して、ユーザーにデフォルトのログインページではなく SSO ログインページが確実に表示されるようにできます。

注:
次のプロパティは SSO を強制しません。login.do ページには引き続きアクセスでき、ユーザーは、ローカルパスワードを設定していればシステムにログインできます。

リダイレクトのプロパティ

ユーザーがログアウトした場合、または SSO を使用したサインオンに失敗した場合に、ユーザーが次に移動する場所 (メインポータルページや SSO ログイン情報を含むナレッジベース記事) を定義できます。URL を指定するには、次のプロパティを使用します。これらのプロパティのいずれかがインスタンスに存在しない場合は、プロパティを作成できます。

glide.authenticate.failed_requirement_redirect
: ユーザーがプライベートページにアクセスしようとしたときに (インシデントを表示しようとした場合など)、SSO 資格情報を提供しない場合にリダイレクトされる URL。通常、このプロパティは顧客のログインポータル (http://portal.companya.com/ など) に設定されます。

glide.authenticate.failed_redirect
: SSO 試行の失敗後にユーザーをリダイレクトする URL。エラーについての説明と役に立つリンクがある公開ナレッジ記事にリダイレクトできます (例：http://portal.companya.com/error)。

glide.authenticate.external.logout_redirect
: ログアウト後にユーザーをリダイレクトする URL。通常は SSO ログインを有効にしたポータルに戻ります (http://portal.companya.com/logout など)。

glide.authentication.external.disable_local_login
: true に設定すると、メインログインページの SSO 資格情報が必要になります。デフォルト：false このプロパティは、*glide.authenticate.failed_requirement_redirect* プロパティと組み合わせて使用する必要があります。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

次の表は、インストレーションイグジットの戻り値、プロパティ、および予想される動作の関係を示しています。

SSO のみを使用したログインの強制

値を返す	プロパティ	動作
failed_missing_requirement	*glide.authenticate.failed_requirement_redirect*	この値が返された場合に資格情報がセッションにとを示しています。ログセッションはプロパティURL にリダイレクトさ常、ログインが要求され集される SSO プロバイす。
failed_authentication	*glide.authenticate.failed_redirect*	この値が返される場合にSSO 資格情報が認証にザーが存在しないか、ユアウトされていることをインに失敗し、セッションで指定された URL にリます。これは通常、ログれ、資格情報が収集されイダーの URL です。
<user_id>	適用外	*<user_id>* で指定されザーにログインが許可されす。この値は、SSO プ*glide.authenticat*(「受信ヘッダーと照合用するインスタンスの(the instance's field n against the incoming 義されたフィールド名と

ローカルログインの制限

セキュリティ上の予防措置として、ローカルログインを防ぐために、リダイレクトプロパティを使用する以上のことをする必要があります。ユーザーがローカルにログインせず、常に内部の Single Sign-on システムによって認証される場合は、インスタンスにインポートする各ユーザーにランダムなパスワードを割り当てる必要があります。ランダムなパスワードは、ユーザーのインポート時に最も簡単に設定できます。ユーザーデータがインポートセットを介してシステムにインポートされる場合は、次のコードを使用して onBefore 変換スクリプトを作成できます。

```
var r  = new Packages. java. util. Random ( ) ;

 var str1  = Packages. java. lang. Long. toString (Packages. java. lang.
 Math. abs (r. nextLong ( ) ) , 36 ) ; var str2  = Packages. java. lang.
 Long. toString (Packages. java. lang. Math. abs (r. nextLong ( ) ) , 36
 ) ;

 var newPass  = str1  + str2 ;

target. user_password = newPass ;

 //password now set to a random string like this:
 //qvm81zdrn7cwwylpvw94eebk
```

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

SAML 統合によるインスタンスのクローン作成

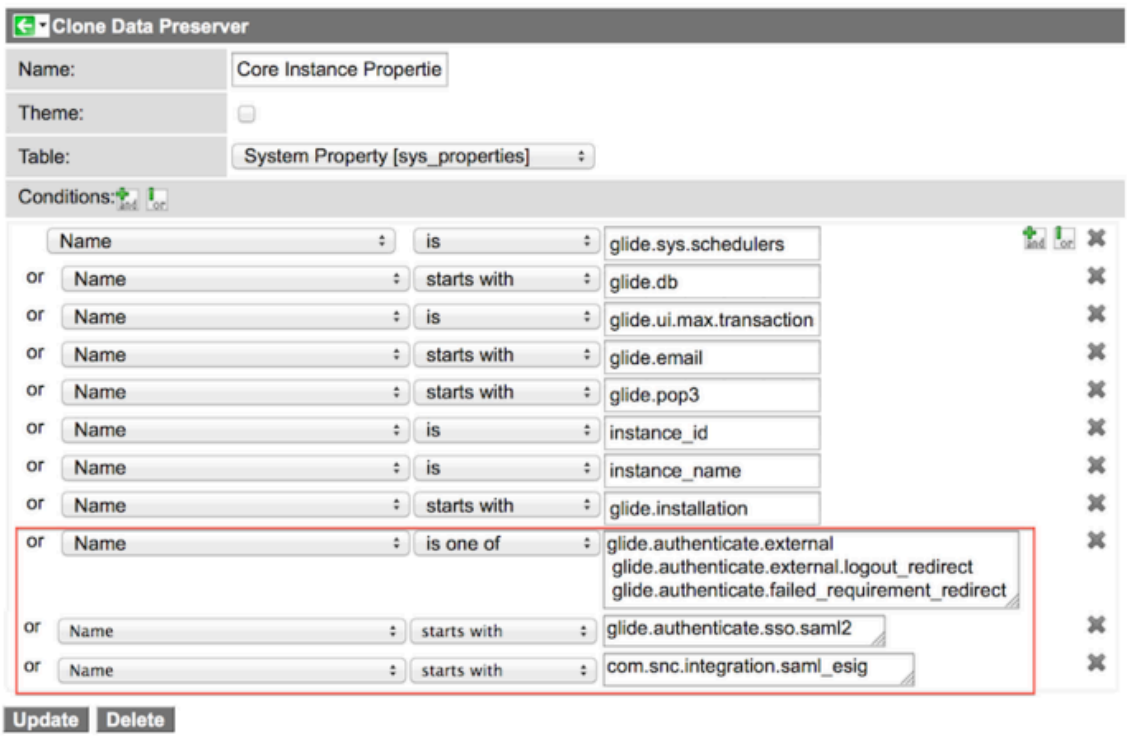
SAML 統合によりインスタンスのクローンを作成します。SAML 2.0 を使用するインスタンスのクローンを作成する前に、ターゲットインスタンスの SAML SSO 関連の設定を保存します。そうしないとターゲットインスタンスがアクセスできなくなる場合があります。

始める前に

必要なロール：管理者

手順

1. ソースインスタンスで、次に移動します。 システムクローン > データを保存 > コアインスタンスのプロパティ.
2. 条件を使用して、次の SAML SSO 関連プロパティが保持されていることを確認します。
   - glide.authenticate
   - glide.security
   - glide.entry
   - glide.script
   - glide.session
   - glide.saml2
   - com.glide.communications
   - com.snc.integration.saml_esig



注:
クローンを作成するときには、証明書がターゲットインスタンスに引き継がれるように添付ファイルを含めます。また、[テーマ] チェックボックスをオフにして、インスタンステーマを保持するかどうかに関係なく、これらのプロパティが保持されるようにします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

3. ソースインスタンスで、次に移動します。 システムクローン > データを保存 sys_certificate の SAML 証明書と SAML/SSO/マルチ SSO に関連するsys_userの SAML ユーザーを保存します。

   必要な場合は、XML にエクスポートしてから、ターゲットに手動でインポートします。

   > ⚠ 警告:
   > あるシステムから別のシステムに SAML/SSO/マルチ SSO セットアップのクローンを作成しようとしないでください。ほとんどの場合、SAML/SSO またはマルチ SSO 設定の転送は、ID プロバイダーで構成する必要があるため機能しません。作業セットアップを上書きすると、ターゲットインスタンスが認証に失敗するため、ターゲットインスタンスにアクセスできなくなります。また、マルチ SSO プロバイダーレコードの sys_id を変更しないでください。変更すると、ユーザーは cookie を強制的にフラッシュします。クローンする際の注意事項の詳細については、「インスタンスをクローンする前のチェックリスト (Checklist before cloning an instance)」を参照してください。

4. マルチ SSO テーブルの sso_properties、digest_properties、および saml2_update1_properties を除外します。
5. 各インスタンスで SAML/SSO/マルチ SSO レコードを手動で作成し、ID プロバイダーでもレコードを設定します。
6. ターゲットインスタンスの sys_user (LDAP でも SAML でもない) レコードで、ソースインスタンスに存在しない sys_id を使用して、LOCAL 管理者アカウントを手動で作成します。
7. [更新] をクリックします。

SAML 2.0 のコンセプト

次の SAML のコンセプトについて説明します。

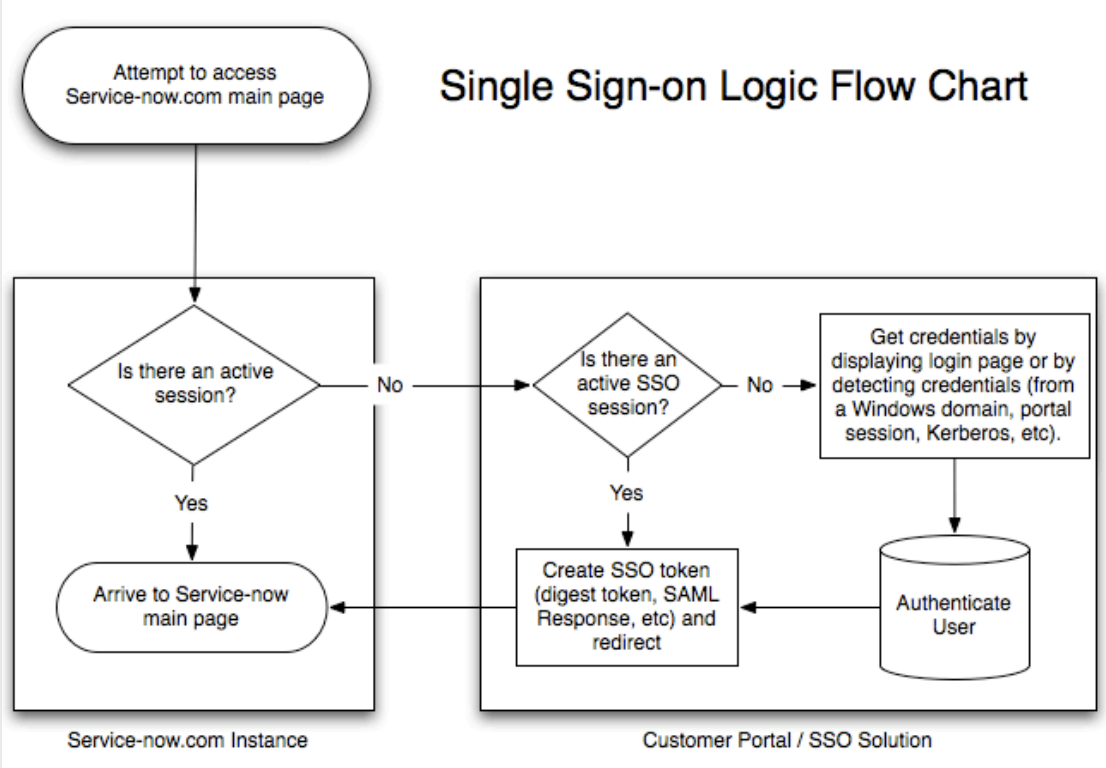
一般的な SAML プロセスフロー (図)

一般的な SSO ロジックフローには、アクティブなセッションの検索、ユーザー資格情報の確認、必要なトークンの作成が含まれます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

SSO 標準



ログイン (AuthnRequest) プロセスフロー

SAML 2.0 は、Web ブラウザで ID プロバイダー (IdP)、サービスプロバイダー (SP)、プリンシパル (ユーザー) の間で情報を交換する Web ブラウザ SSO プロファイルを指定します。

ID プロバイダーは、SAML 認証サービスを提供する任意の SSO サービス (SSOCircle など) にすることができます。サービスプロバイダーは常にインスタンスです。メッセージフローは、サービスプロバイダーの保護されたリソースの要求から始まります。

SP でのターゲットリソースの要求

プリンシパルは、サービスプロバイダーでターゲットリソースを要求します。

https://instance.service-now.com/

インスタンスは要求を確認して、SAMLRequest および RelayState URL パラメーターが存在するかどうかを把握します。存在する場合、ユーザーは IdP で既に検証済みであるため、ステップ 2 ～ 6 をスキップできます。

ID プロバイダーに AuthnRequest を発行

インスタンスは、SAMLRequest 値を使用して IdP に送信される AuthnRequest を作成します。インスタンスは、さらに RelayState URL パラメーター値も作成して送信します。

RelayState トークンは、サービスプロバイダーで維持されるステータス情報への不透過型参照です。SAMLRequest パラメーターの値は、<samlp:AuthnRequest> 要素を縮小した base64 エンコード値です。

```
<samlp:AuthnRequest    xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
   xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"    ID="identifier_1"
   Version="2.0"    IssueInstant="2004-12-05T09:21:59Z"
AssertionConsumerServiceIndex="0"><saml:Issuer>https://
```

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

```
sp.example.com/SAML2</saml:Issuer><samlp:NameIDPolicy      AllowCreate="true"
 Format="urn:oasis:names:tc:SAML:2.0:nameid-format:transient"/></samlp:AuthnRequest>
```

その後、統合は <samlp:AuthnRequest> 要素を URL エンコードし、それを SAMLRequest URL パラメーターとして送信します。

SSO サービスは、URL デコード、base64 デコード、拡張の順に <samlp:AuthnRequest> 要素を処理します。次に、セキュリティチェックを実行します。ユーザーが有効なセキュリティコンテキストを持っていない場合、IdP はログイン資格情報を要求してユーザーを識別します。ユーザーがすでにログインしている場合、IdP は単に SAMLResponse<tt> および <tt>RelayState URL パラメーターで応答します (ステップ 3 を参照)。

SAMLResponse と RelayState での応答

必要なログイン資格情報を収集した後、SSO サービスは要求を検証し、XHTML フォームを含むドキュメントで応答します。

```
<formmethod="post"action="https://instance.service-now.com/navpage.do" ...><input
 type="hidden" name="SAMLResponse" value="response ..." /><input type="hidden"
 name="RelayState" value="token ..." />
   ...
   <input type="submit" value="Submit" /></form>
```

RelayState パラメーターの値はこのステップから取得されます。SAMLResponse パラメーターの値は、次の <samlp:Response> 要素の base64 エンコードです。

```
<samlp:Responsexmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
 ID="s2cdc74f37f923e26fe1aeec42b70a93d24230334f"
 InResponseTo="90AA6073F01567BFB0DF194F596314E2"
 Version="2.0"  IssueInstant="2010-04-29T23:21:51Z"
 Destination="https://dloomac.service-now.com/navpage.do"><saml:Issuer
 xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">http://
idp.ssocircle.com</saml:Issuer><samlp:Status
 xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"><samlp:StatusCode
 xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
 Value="urn:oasis:names:tc:SAML:2.0:status:Success"></samlp:StatusCode></samlp:Status>
<saml:Assertion xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
   ID="s23e536bfc51b8487d4d3299dec162d9c2e338823b"
 IssueInstant="2010-04-29T23:21:51Z"
 Version="2.0"><saml:Issuer>http://idp.ssocircle.com</saml:Issuer><Signature
 xmlns="http://www.w3.org/2000/09/xmldsig#">

...
     </Signature><saml:Subject><saml:NameID
 Format="urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress"
          NameQualifier="http://idp.ssocircle.com"
 SPNameQualifier="https://
dloomac.service-now.com/navpage.do">david.loo@service-now.com</saml:NameID><saml:Su
bjectConfirmation
 Method="urn:oasis:names:tc:SAML:2.0:cm:bearer"><saml:SubjectConfirmationData
           InResponseTo="90AA6073F01567BFB0DF194F596314E2"
           NotOnOrAfter="2010-04-29T23:31:51Z"
 Recipient="https://dloomac.service-now.com/navpage.do" /
></saml:SubjectConfirmation></saml:Subject><saml:Conditions
 NotBefore="2010-04-29T23:11:51Z"
 NotOnOrAfter="2010-04-29T23:31:51Z"><saml:AudienceRestriction><saml:Audience>http
s://
dloomac.service-now.com</saml:Audience></saml:AudienceRestriction></saml:Conditions>
```

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

```
<saml:AuthnStatement AuthnInstant="2010-04-29T23:21:51Z"
 SessionIndex="s2dbf89ab99001e0e8cdaed67266d9d4b21b968a04"><saml:AuthnContext><sa
ml:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTranspo
rt</saml:AuthnContextClassRef></saml:AuthnContext></saml:AuthnStatement></saml:Asse
rtion></samlp:Response>
```

SAMLResponse の検証

SAMLResponse の値は base64 でデコードされて拡張され、ステップ 3 の XML ドキュメントが表示されます。ログインスクリプトは //Subject/NameID 要素から XML 値を抽出し、それを使用してユーザーテーブルで既存のユーザーを検索します。

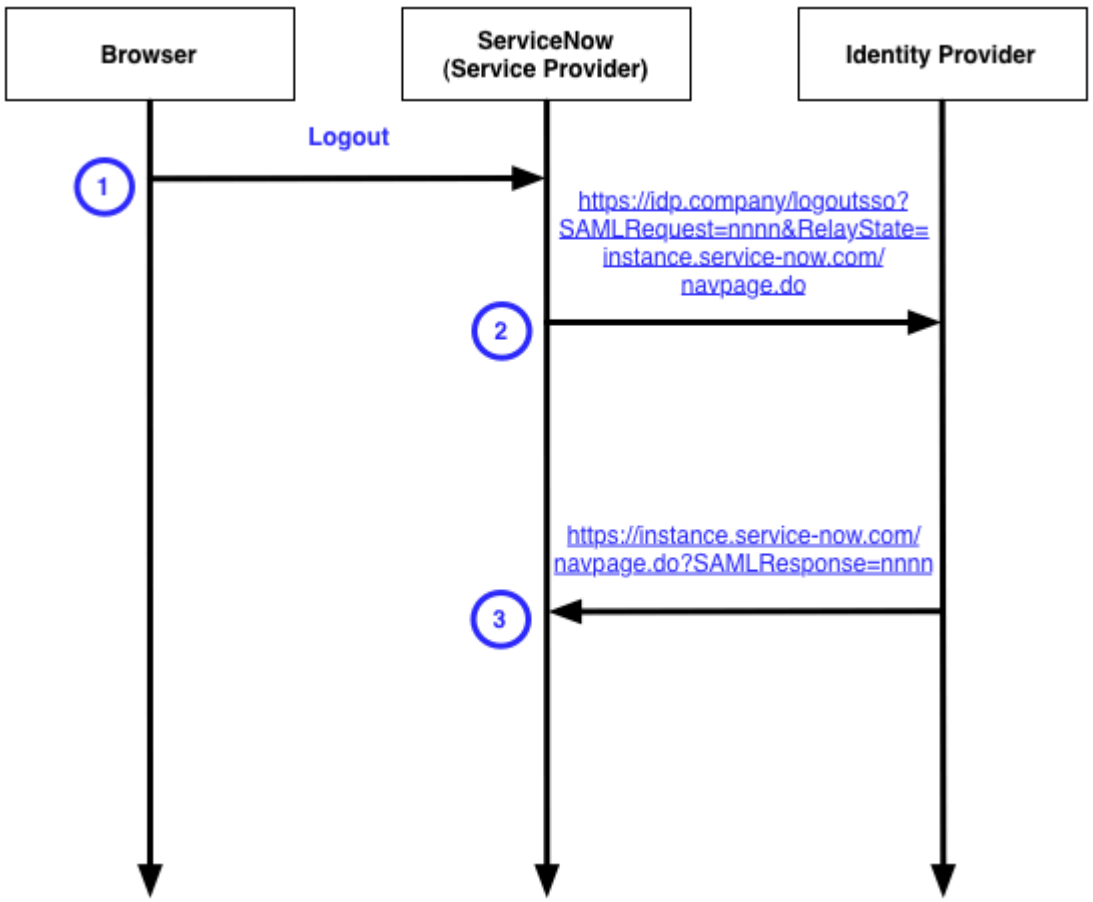
ログインスクリプトは、//AuthnStatement/@SessionIndex 要素からセッション ID を抽出し、LogoutRequest 用に格納します。

ログアウト (LogoutRequest) プロセスフロー

ログアウト時に、インスタンスは SAML 2.0 *LogoutRequest* サービス コールを IdP に発行します。

このサービスは、ユーザーをログアウトさせた後、指定されたログアウト URL にリダイレクトします。

SAML 2 ログアウト



ユーザーが [ログアウト] ボタンをクリック

ユーザーが [ログアウト] ボタンをクリックすると、インスタンスはログアウトスクリプトを実行します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

LogoutRequest の発行

ログアウトスクリプトは SAML 2.0 LogoutRequest を作成し、それを IdP で事前設定された SingleLogoutRequest SAML 2.0 サービスに投稿します。IdP は要求を縮小し、それを base64 エンコードします。LogoutRequest の例は次のようになります。

```
<saml2p:LogoutRequestxmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol"
 ID="21B78E9C6C8ECF16F01E4A0F15AB2D46"  IssueInstant="2010-04-28T21:36:11.230Z"
 Version="2.0"><saml2:Issuer
 xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">https://dloomac.service-now.com
 </saml2:Issuer><saml2:NameID xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"
        Format="urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress"
        NameQualifier="http://idp.ssocircle.com"
 SPNameQualifier="https://
dloomac.service-now.com/navpage.do">david.loo@service-now.com</saml2:NameID><saml2
p:SessionIndex>s211b2f811485b2a1d2cc4db2b271933c286771104
 </saml2p:SessionIndex></saml2p:LogoutRequest>
```

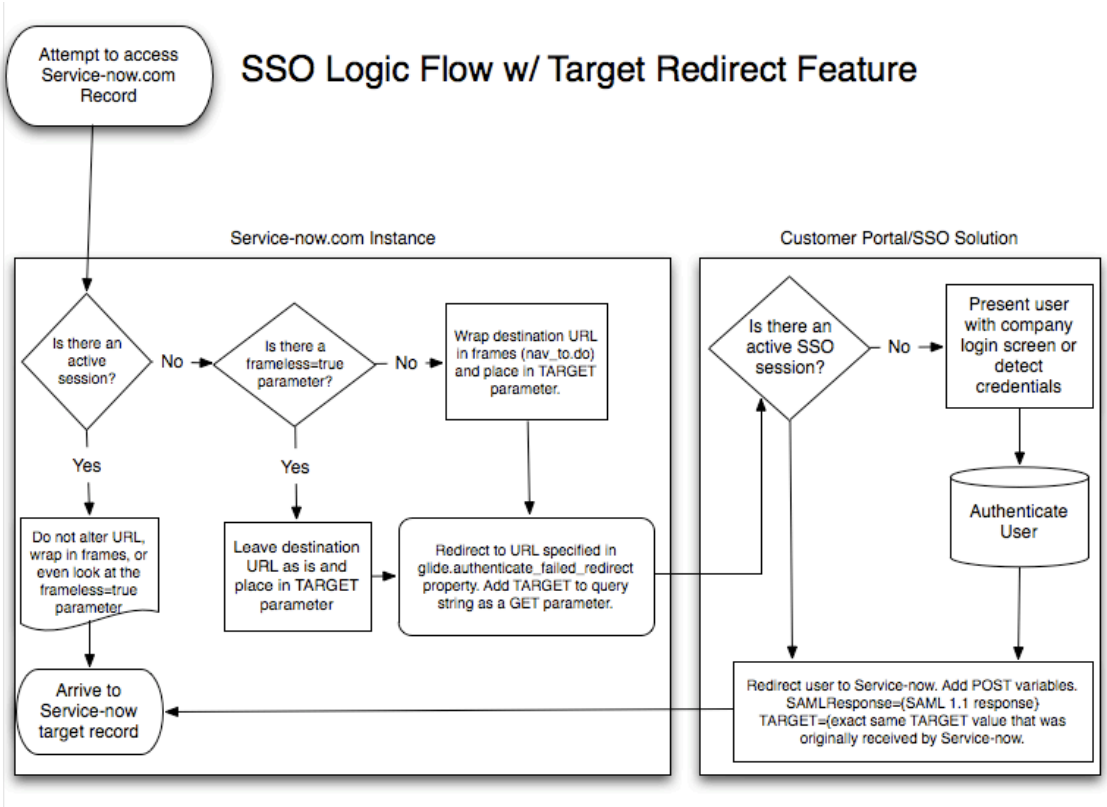
ユーザーのログアウト

ユーザーが IdP からログアウトします。IdP はリダイレクトされてインスタンスに戻りますが、ユーザーがログインしていないため、再度 IdP にリダイレクトされます。

SSO プロバイダーの URL 情報

SSO セッションを必要とするインスタンスへの URL リンクによってログインが阻止される際、SSO プロバイダーに対して参照 URL を指定し、認証後に URL をインスタンスに戻して正しいリソースにリンクできるようにする必要がある場合があります。

SSO ターゲットリダイレクト



インストレーションイグジットの戻り値は、プロパティで定義された URL の代わりに、または URL に加えて渡すように拡張されました。通常は、ユーザー名または事前定義された文字列値を返

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

して、SSO セッションを許可するか阻止するかを制御します。次の例は、URL を渡す拡張動作を示しています。

```
return
 "failed_missing_requirement:%26amp;TARGET=https://
instance.service-now.com/nav_to.do?uri=incident.do?sys_id=12345";
```

上記の例では、URL https://instance.service-now.com/nav_to.do?uri=incident.do?sys_id=12345 を、TARGET という名前の URL パラメーターの形式で SSO プロバイダーに渡します。

注:
SSO プロバイダーは、ユーザー資格情報が収集されて認証が渡されると、TARGET パラメーターのその情報を使用してインスタンスにリダイレクトすると想定されます。

コロン (:) は 2 つの戻り値を区切り、エンコードされた & (%26amp;) はプロパティ *glide.authenticate.failed_missing_requirement* と TARGET パラメーターで定義された URL を連結します。

マルチプロバイダー **SSO** を使用した **SAML 2.0** 構成

マルチプロバイダー SSO 機能から SAML 2.0 SSO 構成を作成または更新できます。

始める前に
必要なロール：管理者

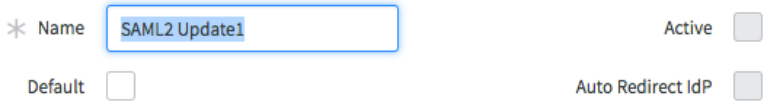
このタスクについて
注:
Jakarta リリースから新たに、IdP 構成をアクティブ化する前にテスト接続機能を使用して構成を検証することが必要になりました。更新機能を使用して構成データを保存することはできますが、テスト接続が成功しないとアクティブな構成になりません。

手順

1. 移動先 すべて > マルチプロバイダー **SSO** > **ID** プロバイダー.
2. 次のいずれかのオプションを実行します。
   - 構成を更新するには、SSO 設定レコードをクリックします。
   - 新しい構成を作成するには、 新規 > **SAML**.
3. 新しい構成の場合は、次のいずれかの方法で IdP 情報を入力します。

オプション	説明
メタデータ記述子 URL を使用	[URL] チェックボックスをクリックし、使用している IdP の URL を入力します。
メタデータ記述子 XML ファイルを使用	[XML] チェックボックスをクリックし、使用している IdP から生成された XML データを貼り付けます。
メタデータを手動入力	ポップアップウィンドウを閉じて、プロパティフィールドに手動でデータを入力します。

[ID プロバイダー] フォームのすべての必須フィールドに入力する必要がありま



す。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

[マルチプロバイダー **SSO (Multi-provider SSO)**] フィールド

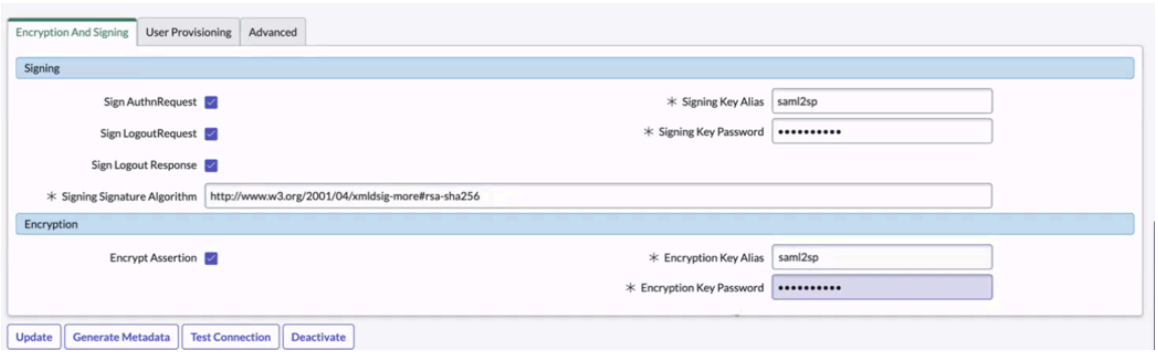
プロパティ	必須	説明
名前	あり	IdP の名前を入力します。この IdP は自動リダイレクト Sys ID です。
有効	はい	IdP を認証に使用するには、[有効] を true に設定する必要があります。 **注:** このプロパティを設定するオプションは、テスト接続が成功した後にのみ表示されます。
デフォルト	なし	自動リダイレクト IdP (旧称「プライマリ IdP」) は、ユーザーをベースインスタンス URL に自動的にリダイレクトします。このプロパティは、この IdP 構成をデフォルトとして設定します。
自動リダイレクト IdP	なし	この IdP 構成を自動リダイレクト IdP として設定します。 **注:** 新しい自動リダイレクト IdP 構成をアクティブにすると、 `glide_sso_id` cookie が新しい自動リダイレクト IdP で更新されます。自動的に有効になる `glide.authenticate.sso.update.idp.cookie` システムプロパティは、この機能を制御します。
ID プロバイダー URL	あり	IdP への URL を入力します。各 IdP URL は一意である必要があります。
ID プロバイダーの AuthnRequest	あり	SingleSignOnService 要素から取得した HTTP リダイレクトバインディングへの URL を入力します。
ID プロバイダーの SingleLogoutRequest	なし	SingleLogoutService 要素から取得した URL を入力します。
ServiceNow のホームページ	あり	IdP が認証するインスタンスの URL (ログインページを含む) を入力します。例：https://yourinstance.service-now.com/navpage.do
エンティティ ID/発行者	あり	IdP が認証するインスタンスのベース URL (ログインページを除く) を入力します。例：https://yourinstance.service-now.com/
対象者 URI	あり	IdP が認証するインスタンスのベース URL (ログインページを除く) を入力します。例：https://yourinstance.service-now.com/
NameID ポリシー	あり	統合で使用される NameIDFormat 要素の値を入力します。
外部のログアウトのリダイレクト	なし	ログアウト後に統合がリダイレクトする URL を入力します。
要件のリダイレクトに失敗	なし	失敗した認証要求をリダイレクトするための URL を入力します。デフォルトでは、これは IdP で設定されたエラーページまたはログアウトページの URL エンドポイントです。この値は glide.authenticate.failed_requirement_redirect フィールドに入力できます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

4. オプション: [暗号化と署名] タブ

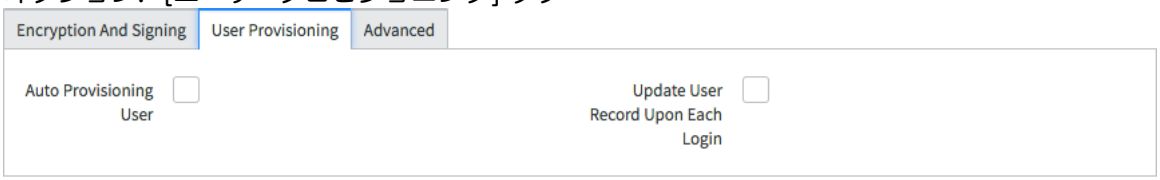
注:
暗号化と署名には独自の証明書を使用することをお勧めします。



[暗号化と署名] フィールド

プロパティ	説明
署名キーエイリアス	SAML 2.0 SP Keystore に格納されているキーエントリの署名エイリアスを入力します。
署名キーパスワード	SAML 2.0 SP Keystore に格納されているキーエントリの署名パスワードを入力します。
暗号化キーのエイリアス	SAML 2.0 SP Keystore に格納されているキーエントリの暗号化エイリアスを入力します。
暗号化キーのパスワード	SAML 2.0 SP Keystore に格納されているキーエントリの暗号化パスワードを入力します。
アサーションを暗号化	SAML 応答のアサーションを暗号化するには、このチェックボックスをオンにします。IDP 用に生成されたメタデータには、IDP が生成する SAML 応答のアサーションを暗号化するために使用する x509 証明書が埋め込まれています。
署名アルゴリズムの署名	eSignature 認証用の SAML 2.0 Identity Provider AuthnRequest Consumer を示す URL を入力します。
AuthnRequest に署名	このチェックボックスをオンにすると、IdP Single Sign-on サービスが署名済みの AuthnRequest を受信できるようになります。
LogoutRequest の署名	このチェックボックスをオンにすると、IdP Single Sign-on サービスが署名済みの LogoutRequest を受信できるようになります。
ログアウト応答に署名	このチェックボックスをオンにすると、IdP Single Sign-on サービスが署名付きのログアウト応答を受信できるようになります。

5. オプション: [ユーザープロビジョニング] タブ



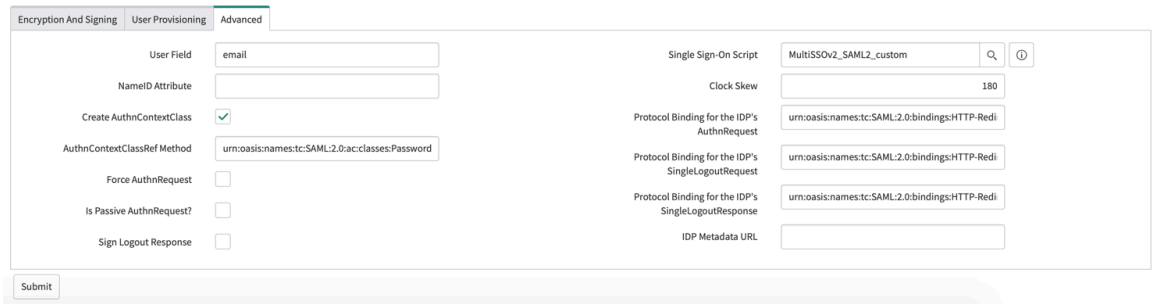
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

[ユーザープロビジョニング] のフィールド

プロパティ	説明
自動プロビジョニングユーザー	自動ユーザープロビジョニングを有効にします。IdP によって提供される情報に基づいてユーザーがインスタンスユーザーテーブルに存在しない場合は、ユーザーを作成します。
各ログイン時のユーザーレコードの更新	ユーザーが SAML を使用してログインするたびに、インスタンスユーザーテーブルのユーザー情報を IdP の情報で更新します。

6. オプション: [詳細] タブ



[詳細] フィールド

プロパティ	説明
ユーザーフィールド	ユーザーを識別するために IdP に必要な値を含むユーザーテーブルのフィールドに入力します。これは応答の一部としての一意の ID です。たとえば、ユーザー名、従業員 ID などがあります。システムユーザーテーブルで、この一意の ID がユーザーの詳細と照合されます。
NameID 属性	新しい NameID ポリシーを設定する場合を除き、このフィールドは空白のままにします。新しいポリシーを設定する場合、システムではログインするユーザーを識別するためのユーザーテーブルを使用する必要があります。ここで、システムは NameID トークンを、そのユーザーテーブルフィールドの名前と照合します。
AuthnContextClass の作成	[パスワードで保護されたトランスポート (Password Protected Transport.)] などの特定のコンテキストクラスを指定するには、このチェックボックスをオンにします。チェックボックスをオフにすると、IdP によって最も適切なコンテキストクラスが選択されます。
AuthnContextClassRef メソッド	IdP がユーザーを認証するために使用するログインメカニズムの URN を入力します。
AuthnRequest の強制	AuthnRequest を強制的に発生させるには、このチェックボックスをオンにします。
Passive AuthnRequest か	AuthnRequest がパッシブの場合は、このチェックボックスをオンにします。
Single Sign-on スクリプト	Single Sign-on スクリプトを選択します。デフォルトは *MultiSSOV2_SAML2_custom* です。
ログアウト応答に署名	このフィールドにログアウト応答の詳細を入力します。
クロックスキュー	SAMLResponse ノンスを構成する 2 つの属性間の秒数を入力します。デフォルトは 60 です。有効な SAMLResponse は、*notBefore*

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

プロパティ	説明
	と *notOnOrAfter* の日付と時刻の値の範囲内である必要があります。SAMLResponse メッセージのサンプルについては、「Sample SAML 2 Response with the SubjectConfirmation and SubjectConfirmationData Elements (SubjectConfirmation および SubjectConfirmationData 要素を含む SAML 2 応答のサンプル)」と、「Sample SAML 2 Response with the AudienceRestrictions and Audience Elements (AudienceRestrictions および Audience 要素を含む SAML 2 の応答サンプル)」を参照してください。
IDP の SingleLogoutRequest のプロトコルバインディング	SingleLogoutService 要素の [バインディング] 属性に記載されているサポート対象の値を 1 つ入力します。
IDP プロパティのインポート元のメタデータ URL	IdP プロパティはこの URL からインポートされます。設定すると、以前の証明書の有効期限が切れた場合に、IdP からの SAML 証明書の自動インポートが有効になります。 **注:** SAML2 Update 1 からマルチプロバイダー SSO にアップグレードする場合、または SSO 接続を手動で設定する場合、IdP メタデータ URL は自動的に入力されません。
要求	要求の一部としての一意の ID。ID にはユーザー名、従業員 ID などがあります。 **注:** 要求では、リダイレクトとポストバインディングの両方がサポートされています。このフィールドを設定するオプションは、テスト接続が成功した後にのみ表示されます。詳細については、「IdP 接続のテスト」を参照してください。
応答	応答の一部としての一意の ID。ID にはユーザー名、従業員 ID などがあります。 **注:** 応答では、リダイレクトとポストバインディングの両方がサポートされています。このフィールドを設定するオプションは、テスト接続が成功した後にのみ表示されます。詳細については、「IdP 接続のテスト」を参照してください。

SAML の **X.509** 証明書

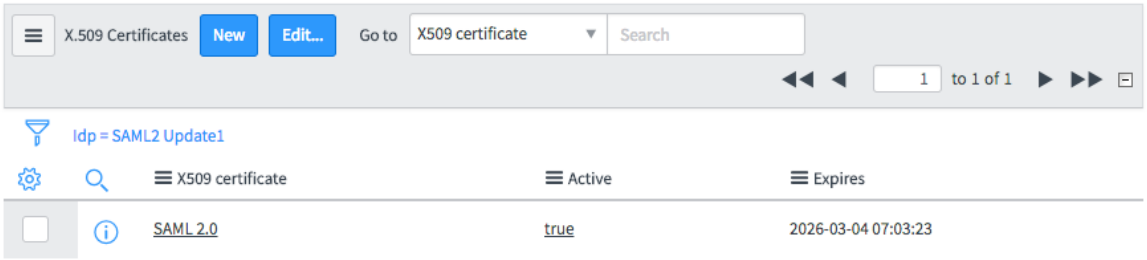
SAML 構成に必要な IdP 証明書を保存してアクティブ化します。

X.509 証明書は、SAML 構成で使用される IdP 証明書です。証明書をインストールした後、必要な数の証明書を追加できます。複数の証明書がある場合は、最初に見つかったアクティブな証明書が使用されます。**IDP** プロパティのインポート元のメタデータ **URL** フィールドに URL を設定すると、証明書が有効でなくなった場合に現在の有効な証明書のために IdP が自動的にポーリングされます。これにより証明書がインスタンスに追加され、アクティブな SAML 構成に使用されます。

注:
ポーリングは、ネットワークの外部から IdP にアクセスできる場合に発生します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



SAML チュートリアル

SAML チュートリアルを使用して、Single Sign-On 用の SAML を設定します。

SAML チュートリアルは、ServiceNow® インスタンスの SSO のトレーニングと設定に役立ちます。管理者はチュートリアルを選択して、インスタンスの SSO を設定するときに必要なアクションをすばやく把握できます。

チュートリアルを使用する前に、Okta、Microsoft Azure、ADFS などの優先 ID プロバイダーで SAML アプリケーションを構成する必要があります。SAML アプリケーションの構成方法については、次のドキュメントを参照してください。

- Okta：Okta の場合、次を実行する必要があります。
  - Okta SAML アプリケーションの追加
  - 用の SAML 2.0 の設定 ServiceNow®
- Microsoft Azure： とのシングルサインオン (SSO) の統合 ServiceNow®
- Ping： を使用した SAML SSO の構成 ServiceNow®
- ADFS：SAML 2.0 との統合

SAML チュートリアルを使用するには、Integration - Multiple Provider Single Sign-On Installer プラグインをアクティブ化します。詳細については、「Multi-Provider SSO プラグインのアクティブ化」を参照してください。

SAML チュートリアルを使用するには、次の手順を実行します。

1. 移動先 すべて > マルチプロバイダー **SSO** > **ID** プロバイダー.
2. [新規] をクリックします。
3. **[SAML]** を選択します。
4. [ヘルプ] アイコンをクリックします。
5. **[Take Tour]** をクリックします。

SAML チュートリアルは、複数のページにまたがる一連の手順を使用して構成を完了し、ツアーの一部として提供される手順と指示に従ってチュートリアルを完了します。SAML構成の詳細については、「マルチプロバイダー SSO を使用した SAML 2.0 構成」を参照してください。

SAML 2.0 と他の機能の統合

SAML 2.0 ソリューションを、電子署名、ディープリンク、ADFS などの他の機能と統合できます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

SAML のディープリンクサポートの追加

ディープリンクにより、インスタンスはシステム内の特定のレコードへの直接メールリンクをサポートできます。

SAML 2.0 統合を有効にすると、IdP が最初に要求された URL にユーザーをリダイレクトする前に、ディープリンク URL が認証チェックに合格する必要があります。たとえば、https://<instance name>.service-now.com/nav_to.do?uri=incident.do?sys_id=46c88ac1a9fe1981014de1c831fbcf6d という URL がメールに含まれているとします。

インスタンスは IdP に認証要求を送信し、RelayState URL パラメーターを使用して最初に要求されたリソース (この場合は uri=incident.do?sys_id=46c88ac1a9fe1981014de1c831fbcf6d) を保持します。IdP がユーザーを認証した後、インスタンスは RelayState URL パラメーターの値を読み取り、要求されたリソースにユーザーをリダイレクトします (インスタンスに存在する場合)。

ディープリンクのサポートを追加するには、ID プロバイダーが RelayState URL パラメーターをサポートしていることを確認します。

ADFS と SAML 2.0 との統合

ServiceNow Multi-Provider SSO プラグインは、SAML 2.0 Single Sign-on (SSO) と Microsoft ADFS との統合をサポートしています。

ADFS のインストールと構成の詳細については、「Active Directory Federation Services Overview (Active Directory フェデレーションサービスの概要)」を参照してください。Multi-Provider SSO プラグインは、SAML 2.0 SSO と ADFS 2.0、3.0、Azure AD との 統合を使用して構成およびテストされています。複数行の属性は、ADFS に関する ServiceNow の SAML 応答ではサポートされていません。

SAML 向け ADFS の設定

SAML 向けの ADFS を設定します。この手順では、ADFS 2.0 を使用し、ADFS Web サイトとして samportal.example.com を表示します。これを ADFS の Web サイトアドレスに置き換えます。

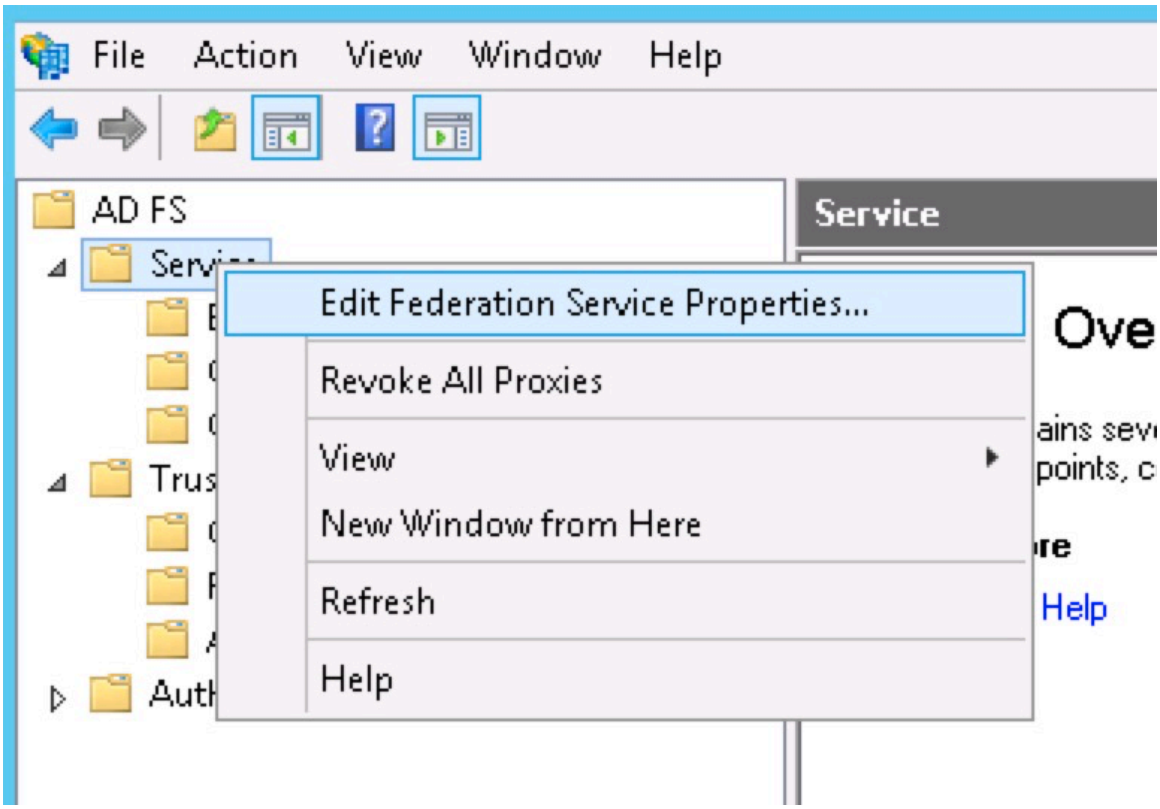
始める前に
必要なロール：管理者

手順

1. ADFS 3.0 サーバーにログインして管理コンソールを開きます。
2. [サービス] を右クリックし、[フェデレーションサービスプロパティの編集 **(Edit Federation Service Properties)]** を選択します。

自動翻訳

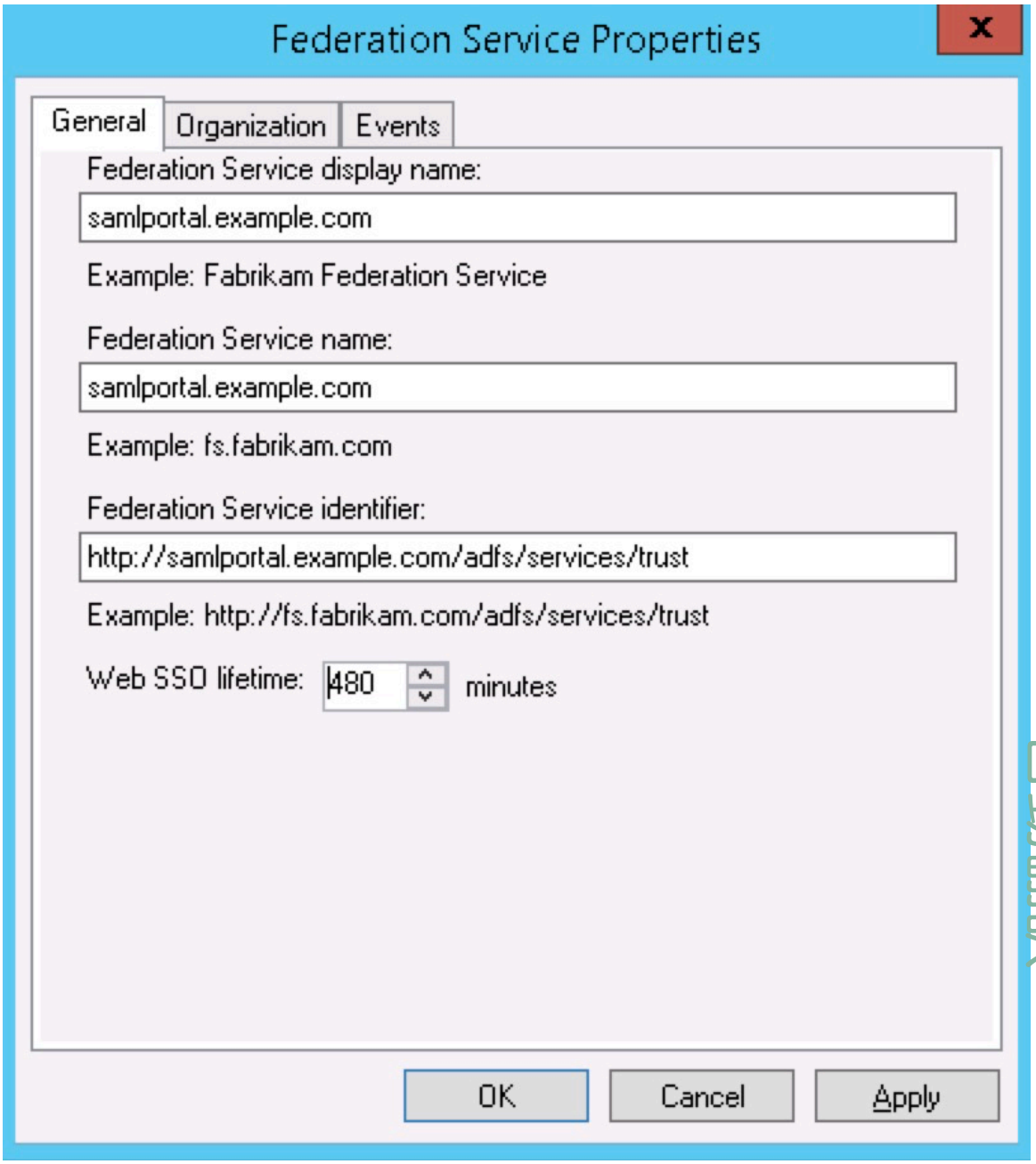
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



3. 全般設定が DNS エントリと証明書名と一致していることを確認します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



自動翻訳

4. 証明書を参照し、トークン署名証明書をエクスポートします。

a. 証明書を右クリックし、[証明書を表示 **(View Certificate)]** を選択します。

b. [詳細] タブを選択します。

c. [ファイルにコピー **(Copy to File)]** をクリックします。
証明書のエクスポートウィザードが開きます。

d. [次へ] を選択します。

e. [いいえ、秘密鍵をエクスポートしません **(No, do not export the private key)]** オプションが選択されていることを確認し、[次へ] をクリックします。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

f. **[DER** エンコード バイナリ **X.509 (.cer) (DER encoded binary X.509 (.cer))]** を選択し、[次へ] をクリックします。

g. ファイルを保存する場所を選択して名前を付け、[次へ] をクリックします。

h. [完了] を選択します。
インスタンスでは、この証明書が PEM 形式である必要があります。この証明書は、クライアントツールや、SSL Shopper のようなオンラインツールを使用して変換できます。

5. 作成した DER/バイナリ証明書を使用し、標準 PEM 形式でエクスポートします。

ADFS のインスタンス設定

インスタンスと SAML 2.0 設定を構成して、ADFS を使用できるようにします。

始める前に
これらの手順は、SAML 用の ADFS を設定した後にのみ実行してください。このプロセスの詳細については、「SAML 用の ADFS の設定」を参照してください。

必要なロール：admin

手順

1. Integration - Multiple Provider Single Sign-On Installer プラグインがアクティブでなければアクティブ化します。
2. SAMLを設定します。ただし、IdP 証明書をインストールする際には、SAML 向け ADFS の設定の実行時に作成した PEM 証明書を添付してください。
3. [保存] をクリックします。
4. [問題] および [件名] フィールドに値が入力され、エラーがないことを確認します。
エラーが発生した場合は、保存した PEM 形式の証明書をメモ帳で開き、証明書をコピーして [PEM 証明書] フィールドに貼り付けます。
5. SAML2SingleSignon_update1 インストレーションイグジットがアクティブであることを確認します。
6. SAML 2.0 の構成を続行します。

> **注:**
> ADFS サーバーで証明書が更新されている場合は、更新された証明書へのインスタンスもアップロードする必要があります。

ADFS 証明書利用者の構成

インスタンスメタデータを取得して ADFS サーバーにインポートします。ただし、証明書利用者を手動で構成する方が簡単に実装できます。

始める前に
必要なロール：管理者

手順

1. 移動先 すべて > マルチプロバイダー **SSO** > **ID** プロバイダー > **SAML2** アップデート **1** > 暗号化と署名 SAML プロパティ Sign AuthnRequest (*glide.authenticate.sso.saml2.require_signed_authnrequest*) が有効でないことを確認します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

署名された要求が必要であることを ADFS 管理者が確認できる場合にのみ、このプロパティをアクティブにしてください。

2. SAML 2 メタデータリンクを介して生成したメタデータをコピーし、ファイルに保存します。
3. ADFS サーバーにログインして管理コンソールを開きます。
4. [証明書利用者信頼 **(Relying Party Trusts)]** を選択します。
5. ウィンドウの右上隅から [証明書利用者信頼の追加 **(Add Relying Party Trusts)]** を選択します。

   追加ウィザードが表示されます。
6. [開始] をクリックして開始します。
7. [ファイルをインポート] オプションを使用して、メタデータファイルをインポートします。
8. ServiceNow などの表示名を設定し、必要であればメモを入力します。
9. **[ADFS 3.0** プロファイル **(ADFS 3.0 Profile)]** を選択します。
10. トークン暗号化証明書を選択しないでください。
    すでにエクスポートされているサービスで定義されている証明書が使用されます。証明書を定義すると、インスタンスと適切に通信できなくなります。
11. **[URL** の構成 **(Configure URL)]** の設定を有効にしないでください。
12. 証明書利用者信頼の識別子として、接続したインスタンスサイトを入力します。
    この場合は、https://company.service-now.com を使用して、[追加] をクリックします。
13. すべてのユーザーにこの証明書利用者へのアクセスを許可します。
14. [次へ] をクリックし、[終了時に要求を開く **(Open the Claims when this finishes)]** チェックボックスをオフにします。
15. このページを閉じます。
    新しい証明書利用者信頼がウィンドウに表示されます。
16. 証明書利用者信頼を右クリックし、[プロパティ] を選択します。
17. [詳細] タブを参照して、[セキュアハッシュアルゴリズム **(Secure hash algorithm)]** を SHA-256 または SHA-1 に設定します。
18. [エンドポイント] タブを参照し、**SAML Assertion Consumer** をポストバインディングと https://company.service-now.com/navpage.do の URL で追加します。

ADFS 証明書利用者要求ルールの構成

要求ルールを編集して、インスタンスと適切に通信できるようにします。

始める前に
必要なロール：管理者

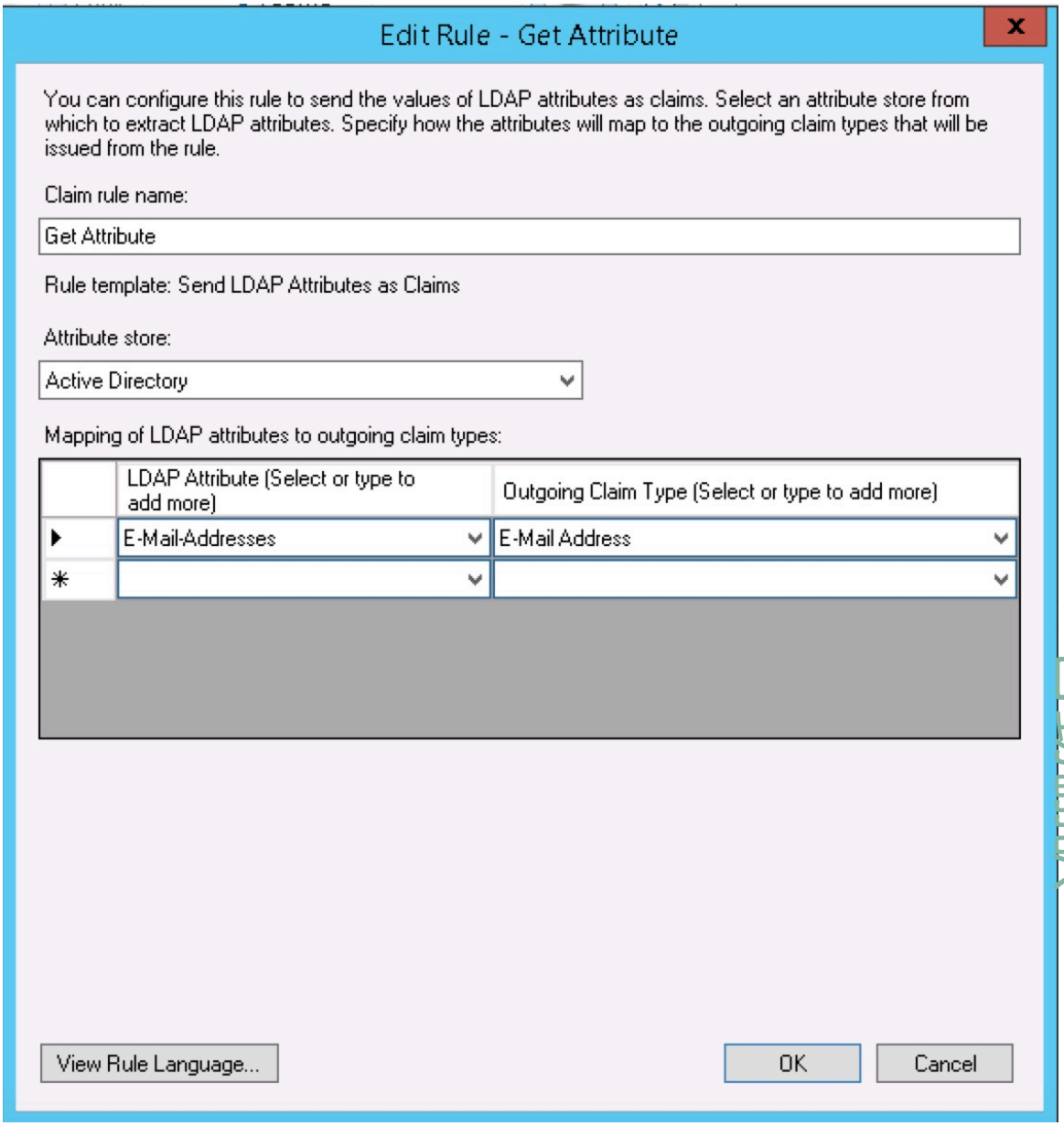
手順

1. ADFS サーバーにログインして管理コンソールを開きます。
2. 証明書利用者信頼を右クリックして、[要求ルールの編集 **(Edit Claim Rules)]** を選択します。
3. [発行変換ルール **(Issuance Transform Rules)]** タブをクリックします。
4. [ルールの追加 **(Add Rules)]** を選択します。
5. 使用する要求ルールのテンプレートとして **[LDAP** 属性を要求として送信 **(Send LDAP Attribute as Claims)]** を選択します。
6. 要求に「Get LDAP Attributes」などの名前を付けます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

7. [属性ストア **(Attribute store)]** を [Active Directory]、**[LDAP** 属性] を [E-Mail-Addresses]、[送信要求タイプ **(Outgoing Claim Type)]** を [E-Mail-Addresses] に設定します。




```
c:[Type ==
 "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname", Issuer
 == "AD AUTHORITY"]
=> issue(store = "Active Directory",
types = ("http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress"),
query = ";mail;{0}", param = c.Value);
```

8. [完了] を選択します。
9. [ルールの追加 **(Add Rules)]** を選択します。
10. 使用する要求ルールテンプレートとして [受信要求を変換 **(Transform an Incoming Claim)]** を選択します。
11. 要求に、「Email to Name ID」などの名前を付けます。

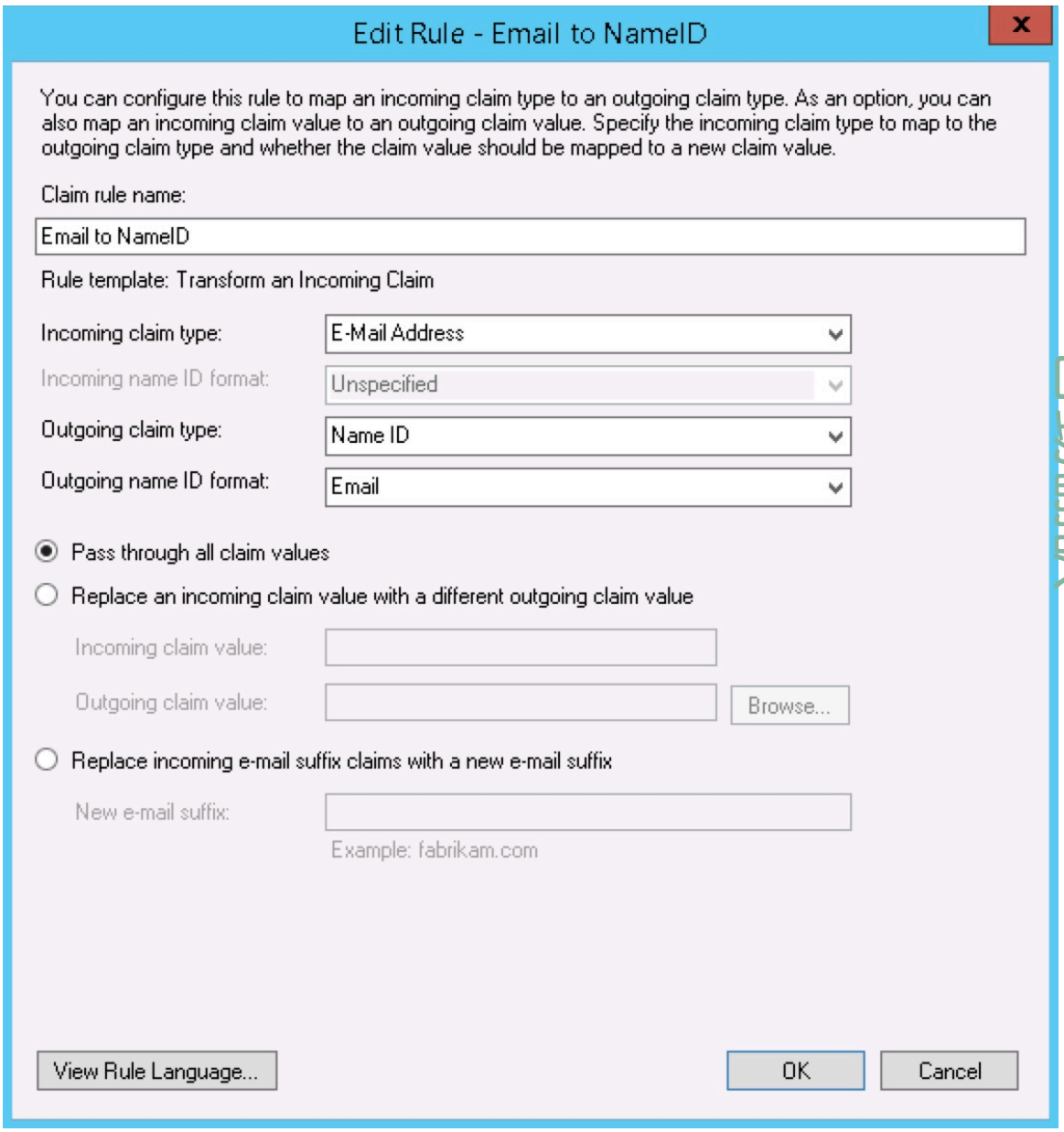
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

12. [受信要求タイプ **(Incoming claim type)]** を前のルールの [送信要求タイプ **(Outgoing Claim Type)]** に設定します。
たとえば「E-Mail Address」などとします。
13. [送信要求タイプ **(Outgoing claim type)]** を [Name ID] に設定し、[送信名 **ID** 形式 **(Outgoing name ID format)]** を [Email] に設定します。

> **注:**
> これらの値は、SAML 2.0 の構成時に定義する名前 ID ポリシーと一致する必要があります。

14. [すべての要求値をパススルー] を選択します。



この要求ルールは、次のルール言語のようになります。

```
c:[Type == "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress"]
 => issue(Type = "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier",
Issuer = c.Issuer, OriginalIssuer = c.OriginalIssuer, Value = c.Value, ValueType =
 c.ValueType,
```

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

```
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/format"]
= "urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress");
```

15. [完了] をクリックします。

SAML ログアウトエンドポイントの作成

SAML ログアウトエンドポイントを作成してシングルログアウトを許可します。

始める前に
必要なロール：管理者

このタスクについて
詳細については、ADFS サインアウトに関するこの記事 を参照してください。

手順

1. 検索項目 **ADFS** マネージャー > 信頼関係 > 証明書利用者信頼 > プロパティ.
2. [エンドポイント] タブで、**[SAML** を追加 **(Add SAML)]** をクリックします。
3. 設定の構成：
   - エンドポイントタイプ：SAML ログアウト
   - バインディング：POST
   - 信頼できる **URL (Trusted URL)**：ADFS サーバーの URL。例を次に示します。

     ```
     https://myadfsserver.domain.net/adfs/ls/?wa=wsignout1.0
     ```

   - 応答 **URL**：アプリケーションのログアウト URL。例を次に示します。

     ```
     https://{instancename}.service-now.com/external_logout_complete.do
     ```

ADFS 構成のテスト

ADFS 構成をテストして、ID プロバイダーとして適切に機能していることを確認します。

始める前に
必要なロール：管理者

手順

1. Internet Explorer ブラウザを開きます。
2. ADFS ポータルに移動します。例：`https://samportal.example.com/adfs/ls/idpinitiatedsignon.aspx`

   例：`https://samportal.example.com/adfs/ls/idpinitiatedsignon.aspx` このページには、構成されている証明書利用者信頼をすべて含むドロップダウンリストがあります。
3. インスタンスに関連付けられている証明書利用者を選択します。
4. [サインインを続行 **(Continue to Sign In)]** をクリックします。

   SAML 2.0 外部認証を適切に設定している場合は、インスタンスに自動的にログインします。
5. `https://samportal.example.com/adfs/ls/idpinitiatedsignon.aspx?logintoRP=https://company.service-now.com` に移動して、直接ログイン URL をテストします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

(ワークアラウンド) サービスプロバイダーが開始する認証の有効化

SAML 2.0 Update 1 がないために認証に失敗した場合は、ワークアラウンドを使用します。この問題は、ユーザーが IdP 認証をスキップしてインスタンスに直接移動しようとした場合に発生する可能性があります。

始める前に
必要なロール：管理者

このタスクについて
このエラーは、SAMLResponse の SPNameQualifier 属性に必要な定義とセマンティクスを、インスタンスが ADFS に提供しないときに発生します。

次のいずれかを実行し、サービスプロバイダーが開始する認証を有効にします。

手順

- SAML 2.0 Update 1 にアップグレードし、 AuthnContextClass 要求を作成するオプションをオフにします。「SAML 2.0 のアクティブ化と設定」を参照してください。
- SAML 2.0 がアクティブ (*SAML 2.0 Update 1* ではない) になっている場合は、SAML2 スクリプトインクルードを変更して、SPNameQualifier 属性の定義をコメント化します。

  createNameID および createNameIDPolicy 関数の次の行をコメントアウトします。

```
//nid.setSPNameQualifier (serviceURL ) ;

 //nameIdPolicy. setSPNameQualifier (serviceURLStr ) ;
```

次のタスク
インスタンスへのアクセス時に ADFS サーバーからのログインプロンプトを表示したくない場合は、次の SAML 2.0 Update 1 プロパティを false に設定します：**AuthnRequest** ステートメントで **AuthnContextClass** 要求を作成する (`glide.authenticate.sso.saml2.createrequestedauthncontext`)。

(ワークアラウンド) **Kerberos** 認証のサポート

SAML 2.0 統合には、認証コンテキストをフォームベースの認証から Windows ベースの認証に変更するワークアラウンドがあります。

始める前に
必要なロール：管理者

このタスクについて
現在、SAML 2 統合では、PasswordProtectedTransport または「フォームベースの認証」認証コンテキストを使用しています。この認証コンテキストでは、ユーザーに認証資格情報のフォームを表示するために IdP が必要です。Kerberos では、確立された Windows ログインを通じて SAML セッションが既にアクティブになっているため、ユーザーは IdP で認証する必要はありません。

手順

1. 移動先 すべて > マルチプロバイダー **SSO** > **ID** プロバイダー.
2. **[SAML2 Update1]** IdP レコードを開きます。
3. **[SAML 2.0 AuthnRequest to the Identity Provider** に含める **AuthnContextClassRef** メソッド] を、次のいずれかに設定します。

AuthnContextClassRef メソッドの値
urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport (デフォルト)

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

urn:federation:authentication:windows

4. [更新] をクリックします。

Azure AD と SAML 2.0 との統合

ServiceNow を Azure Active Directory (Azure AD) と統合します。

ServiceNow を Azure AD と統合すると、次のことが可能になります。

- ServiceNow にアクセスできる Azure AD をコントロールする
- ユーザーが Azure AD アカウントで ServiceNow に自動的にサインインできるようにする
- Azure ポータルでアカウントを管理する

前提条件

開始するには、次を実行する必要があります。

- Azure AD のサブスクリプション。サブスクリプションがない場合は、無料のアカウントを取得できます。
- ServiceNow Single Sign-on (SSO) が有効になっている。
- San Diego バージョン以降をサポートする ServiceNow の ServiceNow インスタンスまたはテナント。
- ServiceNow テナントで Multiple Provider Single Sign On プラグインを有効にする必要があります。
- 自動構成の場合は、ServiceNow のマルチプロバイダープラグインを有効にする必要があります。

構成に対する一連のアクション

Azure AD を構成するために実行する必要がある一連のアクションは次のとおりです。

- ギャラリーから ServiceNow を Azure AD に追加する
- Azure AD SSO を構成する
- Azure AD テストユーザーを作成する
- Azure AD テストユーザーをアサインする
- ServiceNow を構成する

ギャラリーから ServiceNow を追加する

ギャラリーから Azure AD の管理対象 SaaS アプリのリストに ServiceNow を追加します。

始める前に
必要なロール：Azure admin

手順

1. Microsoft アカウントを使用して Azure ポータルにサインインします。
2. 左ペインから **[Azure Active Directory]** サービスを選択します。
3. 移動先 エンタープライズアプリケーション > すべてのアプリケーション.
4. 新しいアプリケーションを追加するには、[新しいアプリケーション] を選択します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

5. [ギャラリーから追加する] セクションで、検索ボックスに「ServiceNow」と入力します。
6. 結果のパネルから ServiceNow を選択し、アプリを追加します。
7. アプリがテナントに追加されるまで数秒待ちます。

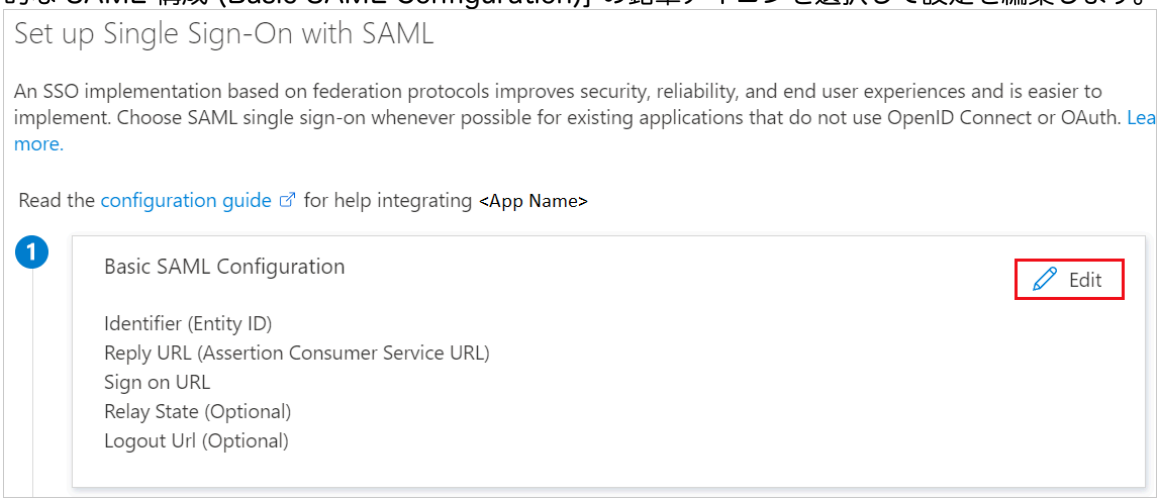
Azure AD SSO の構成

Azure ポータルで Azure AD SSO を構成します。

始める前に
必要なロール：Azure admin

手順

1. Azure ポータルの ServiceNow アプリケーション統合ページで、[管理] セクションを見つけます。
2. [シングルサインオン] を選択します。
   [シングルサインオン方式の選択 single sign-on method] ページで [SAML] を選択します。
3. [SAML Single Sign-on のセットアップ (Set up single sign-on with SAML)] ページで、[基本的な SAML 構成 (Basic SAML Configuration)] の鉛筆アイコンを選択して設定を編集します。



4. [基本的な SAML 構成 (Basic SAML Configuration)] セクションで、次の手順を実行します。

   a. [サインオン **URL (Sign on URL)**] に、次のいずれかの URL パターンを入力します。

   ```
   https://<instancename>.service-now.com/navpage.do
   https://<instance-name>.service-now.com/login_with_sso.do?glide_sso_id=<sys_id of the sso configuration>
   ```

   > **注:**
   > この URL 内に sys_id を指定する必要があります。

   b. [識別子 (エンティティ ID) (Identifier (Entity ID))] で、パターンが https://<インスタンス名>.service-now.com の URL を入力します。

   c. [応答 **URL (Reply URL)**] に、次のいずれかの URL パターンを入力します。

   ```
   https://<instancename>.service-now.com/navpage.do
   https://<instancename>.service-now.com/customer.do
   ```

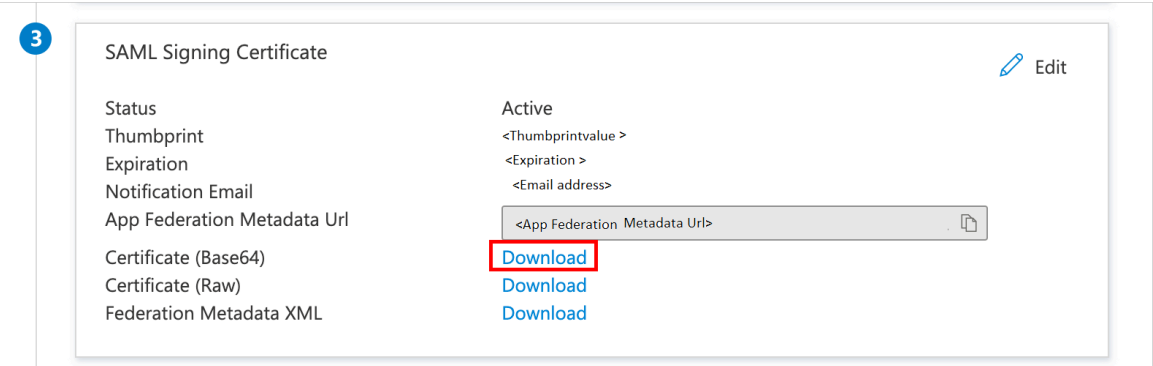
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

d. [ログアウト URL] に、パターンが https://<インスタンス名>.service-now.com/navpage.do の URL を入力します。

> **注:**
> 実際のサインオン URL、応答 URL、ログアウト URL、および識別子を更新する必要があります。これらの URL に表示される値はデモ用です。

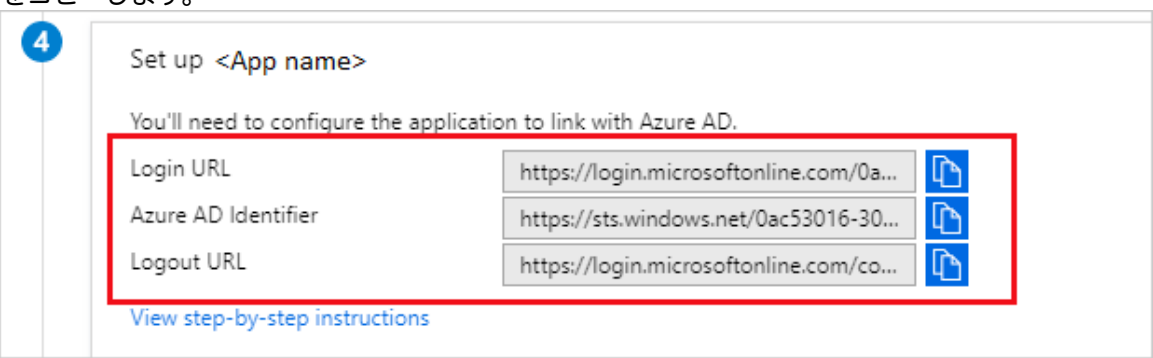
5. [SAML Single Sign-on のセットアップ (Set up single sign-on with SAML)] ページの [SAML 署名証明書 (SAML Signing Certificate)] セクションで、[証明書 **(Base64) (Certificate (Base64))]** を見つけます。



a. [コピー] ボタンを選択して [アプリフェデレーションメタデータ **URL (App Federation Metadata Url)]** をコピーし、メモ帳に貼り付けます。
この URL は追加の構成で必要です。

b. [ダウンロード] を選択して証明書 (Base64) をダウンロードします。

6. [ServiceNow のセットアップ (Set up ServiceNow)] セクションで、要件に基づいて適切な URL をコピーします。



Azure AD テストユーザーを作成する

Azure AD でテストユーザーを作成します。

始める前に
必要なロール：Azure admin

手順

1. Azure ポータルで、次の場所に移動します。 すべて > **Azure Active Directory** > ユーザー > 全ユーザー.

2. [新規ユーザー] を選択します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

3. [ユーザープロパティ] で、次の情報を入力します。
   - 名前
   - ユーザー名
   - パスワード
4. [作成] をクリックします。

Azure AD テストユーザーをアサインする

ServiceNow へのアクセス権を付与することで、Azure Single Sign-on を使用するために作成された Azure AD テストユーザーをアサインします。

始める前に
必要なロール：Azure admin

手順

1. Azure ポータルで、次の場所に移動します。 すべて > エンタープライズアプリケーション > すべてのアプリケーション.
2. アプリケーションリストから、ServiceNow を選択します。
3. アプリのページの [管理] セクションで、[ユーザーとグループ] を選択します。
4. [ユーザーを追加] を選択します。
5. [アサインを追加] ウィンドウで、[ユーザーとグループ] を選択します。
6. [ユーザーとグループ] ウィンドウで、ユーザーリストから作成された [test user] を選択します。
7. 必要に応じて、[ロールの選択 **(Select a role)]** ドロップダウンからアサインされたユーザーのロールを選択します。
8. [アサインを追加] ウィンドウで、[アサイン **(Assign)]** を選択します。

ServiceNow の構成

SSO を使用するには、ServiceNow で Azure AD の詳細を構成します。

始める前に
プラグイン：Integration - Multiple Provider single sign-on Installer

マルチプロバイダー SSO のプロパティを有効にします。

- [マルチプロバイダー **SSO** を有効化 **(Enable multiple provider SSO)]** を選択します。
- [デフォルトの **ID** プロバイダーからユーザーテーブルへのユーザーの自動インポートを有効化] を選択します。
- [マルチプロバイダー **SSO** 統合のデバッグログを有効化 **(Enable debug logging for the multiple provider SSO integration)]** を選択します。
- ユーザーテーブル上のフィールドに「**email**」と入力します。

必要なロール：管理者

手順

1. 移動先 すべて > マルチプロバイダー **SSO** > **ID** プロバイダー.
2. [ID プロバイダー] ページで、[新規] を選択します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

3. [ID プロバイダー] ウィンドウで、**[SAML]** を選択します。
4. [ID プロバイダーのメタデータをインポート] で、次のいずれかを実行できます。
   - **URL**：ID プロバイダー構成ページに詳細を自動入力するためのアプリフェデレーションメタデータ URL。
   - インポート：XML をインポートして、[ID プロバイダー構成] ページの詳細をインポートします。
5. 画面の上部を右クリックし、**[sys_id のコピー]** をクリックし、この値を [基本的な **SAML** 構成] セクションの [サインオン **URL]** で使用します。
6. フォームのフィールドに入力します。

[マルチプロバイダー **SSO]** フィールド

プロパティ	必須	説明
名前	はい	IdP の名前。この IdP は自動リダイレクト Sys ID です。
有効	はい	IdP を認証に使用するには、[有効] を true に設定する必要があります。 **注:** このプロパティを設定するオプションは、テスト接続が成功した後にのみ表示されます。
デフォルト	いいえ	自動リダイレクト IdP (旧称「プライマリ IdP」) は、ユーザーをベースインスタンス URL に自動的にリダイレクトします。このプロパティは、この IdP 構成をデフォルトとして設定します。
自動リダイレクト IdP	いいえ	自動リダイレクト IdP として設定できる IdP 構成。 **注:** 新しい自動リダイレクト IdP 構成をアクティブにすると、 *glide_sso_id* cookie が新しい自動リダイレクト IdP で更新されます。自動的に有効になる *glide.authenticate.sso.update.idp.cookie* システムプロパティは、この機能を制御します。
ID プロバイダー URL	はい	IdP への URL。各 IdP URL は一意である必要があります。
ID プロバイダーの AuthnRequest	はい	SingleSignOnService 要素から取得した HTTP リダイレクトバインディングへの URL。
ID プロバイダーの SingleLogoutRequest	いいえ	SingleLogoutService 要素から取得した URL。
ServiceNow のホームページ	はい	IdP が認証するインスタンスの URL (ログインページを含む)。例：https://yourinstance.service-now.com/navpage.do
エンティティ ID/発行者	はい	IdP が認証するインスタンスのベース URL (ログインページを除く)。例：https://yourinstance.service-now.com/
対象者 URI	はい	IdP が認証するインスタンスのベース URL (ログインページを除く)。例：https://yourinstance.service-now.com/

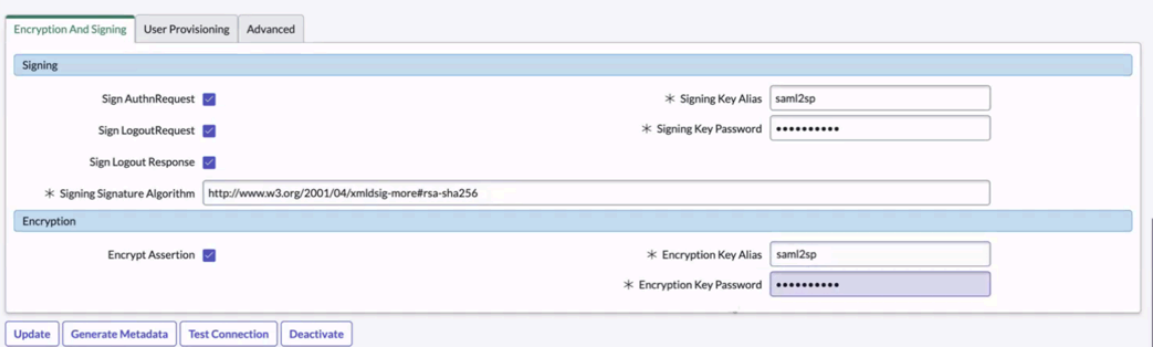
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

プロパティ	必須	説明
NameID ポリシー	はい	統合で使用される NameIDFormat 要素の値。
外部のログアウトのリダイレクト	いいえ	ログアウト後に統合によりリダイレクトされる URL。
要件のリダイレクトに失敗	いいえ	失敗した認証要求をリダイレクトするための URL。デフォルトでは、これは IdP で設定されたエラーページまたはログアウトページの URL エンドポイントです。この値は glide.authenticate.failed_requirement_redirect フィールドに入力できます。

7. オプション: [暗号化と署名] タブ

注:
暗号化と署名には独自の証明書を使用します。



タブ

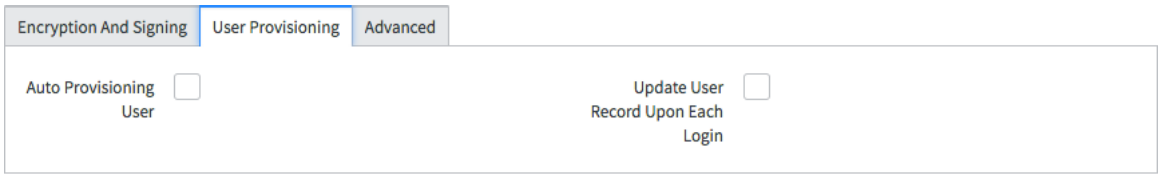
[暗号化と署名] フィールド

プロパティ	説明
署名/暗号化キーのエイリアス	SAML 2.0 SP Keystore に保存されているキーエントリのエイリアス。
署名キーパスワード	SAML 2.0 SP Keystore に保存されているキーエントリのパスワード。
アサーションを暗号化	SAML 応答のアサーションを暗号化するためのチェックボックス。IDP 用に生成されたメタデータには、IDP が生成する SAML 応答のアサーションを暗号化するために使用する x509 証明書が埋め込まれています。
署名アルゴリズムの署名	eSignature 認証用の SAML 2.0 Identity Provider AuthnRequest Consumer を示す URL。
AuthnRequest に署名	IdP Single Sign-on サービスが署名済みの AuthnRequest を受信できるようにするためのチェックボックス。
LogoutRequest の署名	IdP Single Sign-on サービスが署名済みの LogoutRequest を受信できるようにするためのチェックボックス。

8. オプション: [ユーザープロビジョニング] タブ

自動翻訳

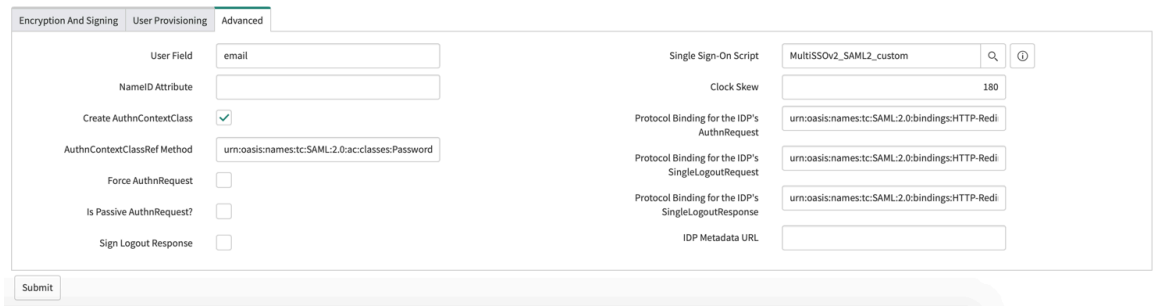
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



[ユーザープロビジョニング] フィールド

プロパティ	説明
自動ユーザープロビジョニング	自動ユーザープロビジョニングでは、IdP によって提供される情報に基づいてユーザーがインスタンスユーザーテーブルに存在しない場合に、ユーザーを作成します。
各ログイン時のユーザーレコードの更新	ユーザーが SAML を使用してログインするたびに、インスタンスユーザーテーブルのユーザー情報を IdP の情報で更新します。

9. オプション: [詳細] タブ



[詳細] フィールド

プロパティ	説明
ユーザーフィールド	ユーザーを識別するために IdP に必要な値を含むユーザーテーブルのフィールド。これは応答の一部としての一意の ID です。たとえば、ユーザー名、従業員 ID などがあります。システムユーザーテーブルで、この一意の ID がユーザーの詳細と照合されます。
NameID 属性	新しい NameID ポリシーを設定する場合を除き、空白のままにするフィールド。新しいポリシーを設定する場合、システムではログインするユーザーを識別するためのユーザーテーブルを使用する必要があります。システムは NameID トークンを、そのユーザーテーブルフィールドの名前と照合します。
AuthnContextClass の作成	[パスワードで保護されたトランスポート (Password Protected Transport)] などの特定のコンテキストクラスを指定するためのチェックボックス。チェックボックスをオフにすると、IdP によって最も適切なコンテキストクラスが選択されます。
AuthnContextClassRef メソッド	IdP がユーザーを認証するために使用するログインメカニズムの URN。
AuthnRequest の強制	AuthnRequest を強制的に発生させるためのチェックボックス。
Passive AuthnRequest か	AuthnRequest がパッシブの場合にオンにするチェックボックス。
Single Sign-on スクリプト	Single Sign-on スクリプト。デフォルトは *MultiSSOV2_SAML2_custom* です。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

プロパティ	説明
ログアウト応答に署名	このフィールドにログアウト応答の詳細入力します。
クロックスキュー	SAMLResponse ノンスを構成する 2 つの属性間の秒数。デフォルトは 60 です。有効な SAMLResponse は、*notBefore* と *notOnOrAfter* の日付と時刻の値の範囲内である必要があります。SAMLResponse メッセージのサンプルについては、「Sample SAML 2 Response with the SubjectConfirmation and SubjectConfirmationData Elements (SubjectConfirmation および SubjectConfirmationData 要素を含む SAML 2 応答のサンプル)」と、「Sample SAML 2 Response with the AudienceRestrictions and Audience Elements (AudienceRestrictions および Audience 要素を含む SAML 2 の応答サンプル)」を参照してください。
IDP の SingleLogoutRequest のプロトコルバインディング	SingleLogoutService 要素の [バインディング] 属性に記載されているサポート対象の値の 1 つ。
IDP プロパティのインポート元のメタデータ URL	IdP プロパティはこの URL からインポートされます。設定すると、以前の証明書の有効期限が切れた場合に、IdP からの SAML 証明書の自動インポートが有効になります。 **注:** SAML2 Update 1 からマルチプロバイダー SSO にアップグレードする場合、または SSO 接続を手動で設定する場合、IdP メタデータ URL は自動的に入力されません。
要求	要求の一部としての一意の ID。ID には、ユーザー名、従業員 ID などがあります。 **注:** 要求では、リダイレクトとポストバインディングの両方がサポートされています。このフィールドを設定するオプションは、テスト接続が成功した後にのみ表示されます。詳細については、「IdP 接続のテスト」を参照してください。
応答	応答の一部としての一意の ID。ID には、ユーザー名、従業員 ID などがあります。 **注:** 応答では、リダイレクトとポストバインディングの両方がサポートされています。このフィールドを設定するオプションは、テスト接続が成功した後にのみ表示されます。詳細については、「IdP 接続のテスト」を参照してください。

10. ページの右上隅にある [テスト接続] を選択します。
11. 資格情報を入力します。
    [SSO ログアウトのテスト結果] が表示されます。
12. [アクティブ化] を選択して、構成をアクティブ化します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

外部認証を使用したメールリンク

ダイジェストトークン外部認証を使用する場合はメールリンクを使用できますが、メール通知のリンクの処理方法を確立する必要があります。

デフォルトのリンクには、SSO 資格情報を取り込まずに、インシデントや変更要求などのインスタンス内の特定の場所に誘導する URL が含まれています。以下は、インスタンスのログインページでログインせずにユーザーをインスタンス内の場所に誘導する例です。

- /demo インスタンスに接続するための非暗号化 HTTP テクニック (特定のレコードに移動しない)：

  ```
  https://<instance
   name>.service-now.com/?
  SM_USER=user_name&DE_USER=lQjlVp7aRJtyPx5+2O/vgU24tbE=
  ```

- ユーザーが最初に自社のログインポータルに移動するための特定のレコードへのリンク (メール通知内)：

  ```
  https://login.company_portal_page.com/nav_to.do?uri=incident.do?sys_id=009f8eda0a0a0b2b01ab4eb094223466%26sysparm_stack=incident_list.do%3Fsysparm_query=active=true
  ```

  インスタンスの *glide.email.override.url* プロパティを設定して、会社のポータルページの URL を含める必要があります。このプロパティが存在しない場合は作成できます。

- 次に、企業ポータルはその URL を取得して、インスタンスへのリダイレクト URL を構築する必要があります。その際、特定のレコードへのアクセスに必要なセグメントは保持され、URL の末尾に SSO 資格情報が追加されます。

  ```
  https://<instance
   name>.service-now.com/nav_to.do?uri=incident.do?sys_id=009f8eda0a0a0b2b01ab4eb094223466%26sysparm_stack=incident_list.do%3Fsysparm_query=active=true&SM_USER=user_name&DE_USER=lQjlVp7aRJtyPx5+2O/vgU24tbE=
  ```

SAML の電子署名サポートの追加

セキュリティアサーションマークアップ言語 (SAML) 2.0 update 1 で電子署名の次のプロパティを設定します。

マルチ SSO で電子署名が有効な場合、SAML プロパティは使用されません。電子署名プロパティが SAML2 Update1 プロパティ [saml2_update1_properties] テーブルに追加されます。

プロパティ	説明	デフォルト
eSignature 認証用の Assertion Consumer Index	エンドポイントを識別するインデックス番号	1
eSignature 認証用の Assertion Consumer URL	コンシューマーを識別する URL	https://yourinstance.service-now.com/consumer.do
eSignature 認証用の AuthnRequest URL	認証用の URL	なし

SAML 1.0 または SAML 2.0 (update 1 を含まない) で電子署名を使用している場合は、特別な設定手順「マルチプロバイダー SSO の電子署名」を参照してください。

注:
電子署名を使用する生命科学関連のお客様の場合は、ユーザーのセルフロックアウト防止ビジネスルールを非アクティブ化してください。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

既存の SAML 1.1 統合から SAML 2.0 への移行

SAML 1.1 統合から SAML 2.0 統合に移行するには、カスタマーサポートにお問い合わせください。

既存の SAML 2.0 統合の更新

既存の SAML 2.0 統合を更新します。

始める前に
必要なロール：管理者

このタスクについて
SAML 2.0 Update 1 プラグインの要求カスタマーサービス & サポート に連絡して、*SAML 2.0 Single Sign-On - Update 1: security enhancements* プラグインを要求します。このプラグインは、更新されたバージョンの *SAML2SingleSignon* インストレーションイグジット (ログインスクリプト)、*SAML2Logout* インストレーションイグジット (ログアウトスクリプト)、および *SAML2* スクリプトインクルード (スクリプトオブジェクト) に適用されます。

既存のインストレーションイグジットスクリプトからのカスタマイズを新しいスクリプトに結合します。更新により、統合のオリジナルのインストレーションイグジットスクリプトの非アクティブなコピーが保存されます。これらのコピーを使用して、ログインおよびログアウトスクリプトに加えたカスタマイズをすべて、これらのインストールの新しいバージョンに結合できます。

既存のインストレーションイグジットスクリプトのカスタマイズを新しいスクリプトに結合

オリジナルのインストレーションイグジットスクリプト名	オリジナルのスクリプトステータス	新規インストレーションイグジットのスクリプト名	新規スクリプトステータス
SAML2SingleSignon	非アクティブ	SAML2SingleSignon_update1	アクティブ
SAML2	非アクティブ	SAML2_update1	アクティブ
SAML2Logout	非アクティブ	SAML2Logout_update1	アクティブ

SAML 2.0 ログインおよびログアウトのインストレーションイグジットスクリプトには、次のようなパスで移動できます。

- **SAML 2** シングルサインオン > ログインスクリプト.
- **SAML 2** シングルサインオン > ログアウトスクリプト.
- システム定義 > インストレーションイグジット.

SAML 2.0 update 1 スクリプトインクルードには、次のようなパスで移動できます。

- **SAML 2** シングルサインオン > スクリプトオブジェクト.
- システム定義 > スクリプトインクルード.

更新をテストします。

手順

1. 値が *true* の `glide.authenticate.sso.saml2.debug` というシステムプロパティを追加します。
2. SAML 2.0 ログインを試行します。
3. システムログを確認します。SAML2 検証エラーの先頭の文字は *SAML2ValidationError* です。
4. 一般的なログインエラーを特定して修正します。
   詳細については、「マルチ SSO (SAML 2.0) のエラーと修正」を参照してください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

更新後の **SAML 2** 応答のサンプル

次のセクションでは、IdP が SAML 応答で指定する必要がある新しい要素と属性を示しています。

Issuer 要素を含む **SAML 2** 応答のサンプル

次の SAML 2 応答では *Issuer* 要素を使用します。

```
<samlp:Responsexmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
 Destination="https://demoi2.service-now.com/navpage.do"
 ID="s28da6774c88ae1eab292bf25fe625db81919d8e1e"
InResponseTo="SNC841720c227c81948cfd68cadcad235c6"
IssueInstant="2012-01-30T20:07:10Z"  Version="2.0"><saml:Issuer
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">http://idp.ssocircle.com</saml:Issuer>
  ...
  <saml:Assertion xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
    ID="s2f347f973c063836cf70ea38302d94976f9c5b851"
IssueInstant="2012-01-30T20:07:10Z"
Version="2.0"><saml:Issuer>http://idp.ssocircle.com</saml:Issuer>
    ...
  </saml:Assertion></samlp:Response>
```

SubjectConfirmation および **SubjectConfirmationData** 要素のあるサンプル **SAML 2** 応答

次に示す SAML 2 応答は、 *NotOnOrAfter* および *Recipient* 属性を備えた *SubjectConfirmation* および *SubjectConfirmationData* 要素を使用します。

```
<saml:SubjectConfirmationMethod="urn:oasis:names:tc:SAML:2.0:cm:bearer"><saml:Subject
ConfirmationData InResponseTo="SNC841720c227c81948cfd68cadcad235c6"
 NotOnOrAfter="2012-01-30T20:17:10Z"
 Recipient="https://demoi2.service-now.com/navpage.do"/></saml:SubjectConfirmation>
```

AudienceRestrictions と **Audience** 要素を含むサンプル **SAML 2** 応答

次に示す SAML 2 応答は、*NotBefore* および *NotOnOrAfter* 属性を備えた *AudienceRestrictions* および *Audience* 要素を使用します。

```
<saml:ConditionsNotBefore="2012-01-30T19:57:10Z"
 NotOnOrAfter="2012-01-30T20:17:10Z"><saml:AudienceRestriction><saml:Audience>http
s://
demoi2.service-now.com</saml:Audience></saml:AudienceRestriction></saml:Conditions>
```

SAML ユーザープロビジョニング

ユーザーが IdP に存在していてもインスタンスに存在しない場合は、SAML ユーザープロビジョニングによってインスタンスのユーザー [sys_user] テーブルにユーザーが自動的に作成されます。

マルチ SSO が有効になっている場合、SAML 2.0 Update 1 では SAML ユーザープロビジョニングがサポートされます。

SAML ユーザープロビジョニングの仕組み

SAML ユーザープロビジョニングが有効になっている場合、インスタンスに存在しない新しいユーザーが検出されると、インスタンスによって u_imp_saml_user_<suffix> という名前の一時テーブルにレコードが自動的に作成されます。<suffix> には自動的に生成されるテキスト識別子が入ります。インポートテーブルとユーザーテーブルの間のデータ関係を指定する変換マップも作成されます。シ

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

ステムで識別される各 IdP には、独自の変換マップがあります。変換マップは IdP ごとに 1 回作成されます。管理者は必要に応じて変換マップを更新できます。

ユーザーがログインすると、IdP にアクセスしてログインします。

- SAML ユーザープロビジョニングを使用できるすべての IdP のリストが表示されます。SAML ユーザープロビジョニングを使用できる IdP が 1 つしかない場合は、それが自動的に使用されます。
- 上記のいずれの条件にも当てはまらない場合、自動リダイレクト IdP が使用されます。

SAML ユーザープロビジョニングの管理

IdP のユーザーでユーザーテーブルを更新するには、最初にフィールドマッピングを設定してから、マルチ SSO IdP 設定を使用してユーザープロビジョニングを有効にします。

始める前に

IdP マッピングを設定して、ユーザーテーブルの正しいフィールドにマッピングされている IdP のフィールドを特定します。

必要なロール：管理者

手順

1. 移動先 すべて > マルチプロバイダー **SSO** > プロパティ.
2. この機能をアクティブ化するには、[デフォルトの **ID** プロバイダからユーザーテーブルへのユーザーの自動インポートを有効化] (*glide.authenticate.multisso.user.autoprovision*) を選択します。
3. [保存] をクリックします。
4. 移動先 マルチプロバイダー **SSO** > **ID** プロバイダー.
5. **[SAML2 Update1]** レコードを開きます。
6. ユーザーがまだ存在しない場合にユーザーテーブルにレコードを作成するには、[ユーザーの自動プロビジョニング **(Auto-provision Users)]** を選択します。
   このリリースにアップグレードした場合は、フォームを設定してこのフィールドを追加する必要があります。
7. ユーザーが IdP にログインし、IdP の情報がユーザーテーブルの情報よりも古い場合にユーザーレコードを更新できるようにするには、[各ログイン時のユーザーレコードの更新] を選択します。
   このリリースにアップグレードした場合は、フォームを設定してこのフィールドを追加する必要があります。
8. [ユーザープロビジョニングの変換マップ] をクリックして、自動的に作成されるマップを表示します。
9. 必要に応じてマップを変更します。

タスクの結果

不明ユーザーが最初にログインしようとすると、metadata.xml ファイルからインポートセットテーブルにフィールドが作成されます。

注:
この最初のユーザーがログインするまで、IdP テーブルのフィールドはマップできません。

SAML 2.0 のトラブルシューティング

サポートに連絡する前に、Hi に基づくナレッジベースで入手可能なトラブルシューティングの解決策を試してみてください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注:
インスタンスは、外部サイトから提供されるソリューションをサポートしていません。

ナレッジベース記事：KB0540617「SAML Error Matrix (SAML エラーマトリクス)」を参照してください。

その他のよくある問題

エラーまたは症状	解決策
エラーメッセージ：「関数ではありません (is not a function)」 この問題は、マルチノード環境で発生する可能性があります。プラグインがすべてのノードでアクティブ化されていない場合、次のようなエラーが表示されます。 org.mozilla.javascript.EcmaError：*`[JavaPackage org.opensaml.saml2.core.impl.AuthnRequestBuilder]`* は関数ではありません (is not a function)。	このエラーは、プラグインがアクティブではなく .jar ファイルをロードしなかったために発生します。したがって、コードが欠落しているように見えます。プラグインが存在しないノードを再起動するには、テクニカルサポートにお問い合わせください。
SAML が CMS ページにアクセスするユーザーを認証しません。	デフォルトでは、CMS ページは公開されているため、認証は必要ありません。SAML で CMS ページを認証する場合は、*view_content.do* 公開ページを *active=true* から *active=false* に変更します。
SAML 認証後にユーザーを CMS ページにリダイレクトすることができません。	デフォルトで、SSO 統合は *URI* と呼ばれる URL パラメーターを使用して、IdP で認証した後のユーザーの誘導先を制御します。SSO は相対 URL を無視します。たとえば、SSO はユーザーを */ess* 相対 URL にリダイレクトできません。代わりに、ユーザーはディープリンク構文を使用する */nav_to.do?uri=/ess*などの URL に移動する必要があります。 ただし、この場合 ESS ポータルはメインナビゲーションコンテンツの IFrame 内に配置されます。つまり、サイトはページ全体を占有するのではなく、インスタンス内のページとしてロードされます。詳細については、CMS サイトと Single Sign-on を参照してください。 *view_content.do* を *active=false* に設定して CMS エントリページをプライベートにした場合、ディープリンクの動作には、インストレーションイグジットログインスクリプトのカスタマ

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

その他のよくある問題 (続く)

エラーまたは症状	解決策
	イズが必要です。URL の *URI* 部分を検索し、IdP での認証後にユーザーをリダイレクトするための相対 URL パスを含む *RelayState* URL パラメーターを構築するスクリプトを作成します。
SAML が認証後にユーザーを適切なページにリダイレクトしません。	リレーステータスが IdP に渡され、認証中に返されるかどうかを確認します。これは、HTTP 要求ヘッダーと POST 情報を保存できるブラウザー (開発者ツールを備えた Chrome、または HTTPfox というアドオンを備えた Firefox など) を使用して実行できます。Internet Explorer の場合は、Fiddler などのサードパーティアプリケーションを使用してください。その目的は、クライアント (ブラウザー) からインスタンスへ、またクライアントから IdP へ渡される要求を監視することです。

ログインアクティビティのイベントキューの監視

Single Sign-on 統合はすべて、ログインアクティビティのイベントを作成します。

これらのイベントを使用してログインの失敗を監視し、対処すべきセキュリティ上の懸念があるかどうかを判断できます。

ログイン失敗のイベントキューの監視

イベント名	説明	レコード	パラメーター **1**	パラメーター **2**
external.authentication.succeeded	外部認証に成功し、ユーザーがインスタンス URL にアクセスしました。	セッション ID	正常にログインしたユーザーのユーザー ID	ユーザーがアクセスした URL (ディープリンクの場合あり)
external.authentication.failed	Single Sign-on 要件がないか、指定されていません。		セッション ID	不足している認証要件
external.authentication.failed	ユーザー [sys_user] テー		ユーザー ID	文字列「ユーザーは存在しません」

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ログイン失敗のイベントキューの監視 (続く)

イベント名	説明	レコード	パラメーター 1	パラメーター 2
	ブルにユーザーが存在しません			
external.authentication.failed	ユーザーはロックアウトされています。		ユーザー ID	文字列「ユーザーがロックアウトされました (User locked out.)」

イベントキューのログインイベント

SAML 2.0 統合は、ログインアクティビティのためのイベントを作成します。

これらのイベントを使用してログインの失敗を監視し、対処すべきセキュリティ上の懸念があるかどうかを判断できます。

ログインアクティビティイベント

イベント名	説明	イベントで使用される ID	イベント文字列
saml2.logout.validation.failed	IdP からのログアウト応答がログアウト要求の検証に失敗しました。このイベントは、<inResponseTo> 要素をセッション ID に対して検証します (<saml2p:LogoutRequest> 要素の ID 属性)。たとえば、発行されたログアウト要求のワークフローを参照してください。	セッション ID	文字列「SAML ログアウト応答の検証に失敗しました (SAML2 LogoutResponse validation failed)」
external.authentication.succeeded	外部認証に成功しました。		文字列「認証に成功しました (Authentication Successed)」
external.authentication.succeeded	外部認証に成功し、ユーザーがインスタンス URL にアクセスしました。	正常にログインしたユーザーのセッション ID とユー	ユーザーがアクセスした URL (ディープリンクの場合あり)

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ログインアクティビティイベント (続く)

イベント名	説明	イベントで使用される **ID**	イベント文字列
		ザー ID	
external.authentication.failed	Single Sign-on 要件がないか、指定されていません。	セッション ID	不足している認証要件
external.authentication.failed	ユーザー [sys_user] テーブルにユーザーが存在しません。	ユーザー ID	文字列「ユーザーが存在しません」
external.authentication.failed	ユーザーはロックアウトされています。	ユーザー ID	文字列「ユーザーがロックアウトされました (User locked out)」

SAML 2.0 およびダイジェストトークン構成への変更

複数プロバイダー Single Sign-on により、管理者は認証方法として SAML 2.0 Update 1 とダイジェストトークンを設定できます。

SAML 2.0 Update 1 およびダイジェストトークンプロパティを設定する前に、複数プロバイダー Single Sign-on をアクティブ化する必要があります。複数プロバイダー SSO を要求してアクティブ化したら、設定する必要があります。複数プロバイダー SSO を設定すると、SAML 2.0 Update 1 およびダイジェストトークン構成を作成または更新できます。複数プロバイダー SSO では、いずれかまたは両方の認証ソリューションを使用できます。

注:
Integration - Multiple Provider Single Sign-On Installer プラグインは、ナビゲーターから SAML アプリケーションを削除します。必要な SAML 設定は、Multi-Provider SSO アプリケーションの SAML2 移行済みテーブルに移行されます。x509 証明書、IdP の詳細などのアイテムは、Multi-Provider SSO アプリケーションを使用して引き続き変更できます。

OAuth 受信および送信認証

OAuth ベースの認証は、認証プロトコルを使用してシステムで信頼を確立しようとするクライアントの ID を検証します。

OAuth 2.0 - オープン認証は認証の業界標準プロトコルであり、Web アプリケーション、デスクトップアプリケーション、およびモバイルデバイス向けの特定の認証フローを提供すると同時に、クライアント開発者の簡素化を実現します。

これは、Web サイトまたはアプリケーションがユーザーの代わりに他の Web アプリによってホストされているリソースにアクセスできるように設計された標準です。

リソースユーザーの資格情報を使用して保護されたリソースにアクセスする代わりに、クライアントはアクセストークンを取得します。ユーザーの承認を得てアクセストークンがサードパーティクライアントに発行され、クライアントはアクセストークンを使用して保護されたリソースにアクセスします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

受信

インスタンスにアクセスする外部クライアント用のエンドポイントを作成し ます。これにより、OAuth クライアントアプリケーションレコードが作成され、クライアントがインスタンスの制限付きリソースにアクセスするために必要なクライアント ID とクライアントシークレットが生成されます。詳細については、「OAuth 受信」を参照してください。

送信

インスタンスへのアクセスを承認するサードパーティ OAuth プロバイダーを使用します。別の OAuth プロバイダーに接続する場合は、OAuth プロファイルと OAuth スコープを指定します。詳細については、「OAuth 送信」を参照してください。

OAuth 2.0

OAuth 2.0 を使用すると、ユーザーは、各リソース要求でログイン資格情報を入力するのではなく、トークンを取得することで、外部クライアントを介してインスタンスリソースにアクセスできます。

OAuth 統合を管理するには、security_admin ロールが必要です。次のようなシナリオで OAuth 2.0 を設定します。

- **OAuth** 外部クライアントシナリオ (受信)：インスタンスは、インスタンスからデータをプルするためのサードパーティクライアント用のエンドポイントを提供します。
- **OAuth** プロバイダーシナリオ (送信)：インスタンスがサードパーティプロバイダーからデータをプルします。

> **注:**
> トークンを初めて取得するには、ユーザー認証を行う必要があります。その後は、トークンの有効期限が切れるまでユーザーアカウントを使用して認証する必要はありません。

OAuth 2.0 は、シンプルなセキュリティフレームワークと高セキュリティフレームワークの両方でサポートされています。高セキュリティをお勧めします。高度なセキュリティが既に有効になっているバージョン、および高度なセキュリティをアクティブ化する方法について、情報を参照してください。

OAuth 2.0 実装の重要なコンセプト

コンセプト	説明
リソース所有者	保護されたリソースへのアクセスを許可できるエンティティ。リソース所有者が個人である場合は、エンドユーザーと呼ばれます。リソース所有者は常にユーザーアカウントです。
クライアント	リソース所有者の承認により、リソース所有者の代わりに保護されたリソースに対する要求を行うアプリケーション。
リソースサーバー	保護されたリソースをホストし、保護されたリソースへの要求を受け入れて応答できるサーバー。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

コンセプト	説明
認証サーバー	リソース所有者を正常に認証して認可を取得した後、クライアントにアクセストークンを発行するサーバー。
認証要求	保護されたリソースにアクセスするためにクライアントが必要とする権限。認証要求は常に、リソース所有者の代わりに動作するクライアントの ID と要求を許可する資格情報を含む HTTP POST メッセージです。
認証権限許可	リソースにアクセスするための、リソース所有者からの認可を表す資格情報。認証権限許可は、ユーザーのログイン資格情報またはリフレッシュトークンのいずれかです。
アクセストークン	保護されたリソースにアクセスするためにクライアントが使用する安全な文字列。インスタンスは、有効な認証権限許可を持つクライアントにアクセストークンを発行します。各アクセストークンには、特定のスコープ、有効期間、およびその他の属性が含まれます。 デフォルトで、インスタンスが OAuth プロバイダーであるシナリオでは、インスタンスは 30 分の有効期間でアクセストークンを発行します。サードパーティのトークンの場合は 30 日間です。
リフレッシュトークン	クライアントが追加のユーザー認証を要求せずに新しいアクセストークンを取得するために使用する資格情報。インスタンスは、初めてアクセストークンを持つことが許可されると、クライアントにリフレッシュトークンを発行します。 デフォルトで、インスタンスが OAuth プロバイダーであるシナリオでは、インスタンスは 100 日の有効期間でリフレッシュトークンを発行します。サードパーティのトークンの場合は 365 日間です。
自己署名証明書	Now Platform は自己署名証明書をサポートしていません。OAuth クライアントは証明書トラストストアを使用せず、自己署名証明書を組み込んだ OAuth エンドポイントへの接続を許可しません。
ユーザーエージェント	クライアントアプリケーション (多くの場合は Web サイト) へのアクセス権を委任するユーザー。アクセス権により、クライアントアプリケーションまたは Web サイトは、ユーザーがアクセス権を持つインスタンス内のデータへのアクセスを許可されます。ユーザーエージェントはシナリオで使用されます。

OAuth 権限許可タイプ

権限許可タイプは、クライアントがアクセストークンを取得する方法です。次の権限許可タイプがサポートされています。

- 認証コード：コンシューマーは最初に認証コードを取得し、それを使用してアクセストークンを取得します。OAuth プロファイルを指定 し、この権限許可タイプを指定することができます。認証コードを使用するプロセスは、*auth* コードフローまたは認証コードフローとも呼ばれます。
- リソース所有者のパスワード資格情報：リソースのコンシューマーは、アクセストークンを取得するためのユーザー資格情報をすでに持っています。このプロセスは、パスワードフローとも呼ばれます。
- クライアント資格情報：リソースのコンシューマーは、アプリケーションレジストリにすでに設定されているクライアント ID とクライアントシークレットを使用します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

認証資格情報のストレージ

OAuth クライアントシークレットは *password2* タイプフィールドとして格納され、KMF で暗号化されます。受信エンドポイント要求のチェックに使用されるユーザーパスワードは、ユーザーテーブルの *password* タイプフィールド (SHA 256) にハッシュ値として格納されます。この暗号化の詳細については、「KMF による Password2 暗号化」を参照してください。

OAuth の設定

OAuth を設定してアクティブ化し、OAuth システムプロパティを有効にし、外部クライアントアプリケーションがインスタンスにアクセスするための OAuth アプリケーションエンドポイントを作成し、OAuth パラメーターを設定します。

始める前に
必要なロール：管理者

手順

1. OAuth プラグインがアクティブで、OAuth アクティブ化プロパティが true に設定されていることを確認します。
2. 次のいずれかの方法を使用して、OAuth アプリケーションレジストリを作成します。
   - インスタンスにアクセスする外部クライアント用のエンドポイントを作成し ます。これにより、**OAuth** クライアントアプリケーションレコードが作成され、クライアントがインスタンスの制限付きリソースにアクセスするために必要なクライアント ID とクライアントシークレットが生成されます。
   - インスタンスへのアクセスを承認するサードパーティ OAuth プロバイダーを使用します。

     別の OAuth プロバイダーに接続する場合は、OAuth プロファイルを指定 し、OAuth スコープを指定 します。
3. OAuth トークンを要求する HTTP POST を作成するように、クライアントアプリケーションを設定します。
   アプリケーションは、返されたアクセストークンとリフレッシュトークンを使用するために、JSON 応答も解析できるようにする必要があります。

OAuth のアクティブ化

デフォルトでは、**OAuth 2.0 (com.snc.platform.security.oauth)** プラグインは新規インスタンスおよびアップグレードされたインスタンスでアクティブになっています。インスタンス上でプラグインがアクティブでない場合は、アクティブ化することができます。

始める前に
必要なロール：管理者

手順

1. 移動先 すべて > システムアプリケーション > 利用可能なすべてのアプリケーション > すべて.
2. フィルター基準と検索バーを使用してプラグインを検索します。

   名前または ID でプラグインを検索できます。プラグインが見つからない場合は、ServiceNow 担当者から要求する必要があります。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

3. [インストール] を選択して、[プラグインをアクティブにする] ダイアログボックスで、[アクティブ化] をクリックします。

> **注:**
> ドメイン分離と代理管理者がインスタンスで有効になっている場合、管理ユーザーはグローバルドメインに含まれている必要があります。それ以外の場合、次のエラーが表示されます： 別の操作が実行されているため、アプリケーションのインストールは利用できません：<プラグイン名> のプラグインの有効化。

OAuth プロパティの設定

登録済みアプリケーションに対して OAuth 2.0 トークンを生成するには、インスタンスに対して com.snc.platform.security.oauth.is.active プロパティがアクティブである必要があります。

始める前に
必要なロール：管理者

手順

1. OAuth 2.0 を使用するには、ワークスペースのフィルターナビゲーターに「**sys_properties.list**」と入力し、[新規] をクリックします。
2. 次の設定をフォームに入力します。
   - 名前：com.snc.platform.security.oauth.is.active
   - タイプ：true | false
   - [値]：true

OAuth パスワードパラメーターの変更

このプロパティを使用して、サポートされているすべての権限許可タイプの入力として POST 本文パラメーターのみが受け入れられるようにします。

URI クエリーパラメーターを介して機密情報を送信すると、要求間でクライアント、サーバー、またはホストによる機密情報の漏洩につながる可能性があります。Madrid リリース以降、この新しいプロパティにより、サポートされるすべての権限許可タイプに対して、POST 本文パラメーターのみが入力として受け入れられることが保証されています。サポートされている権限許可タイプは次のとおりです。

- 認証コード
- パスワード
- クライアント資格情報
- リフレッシュトークン

OAuth パスワードパラメーターのプロパティ

プロパティ	説明
glide.oauth.allow.parameters.in.post.body.only	このプロパティは、OAuth 2.0 プラグインの一部として、zBoot にのみ true に設定されます。インスタンスにこの設定が必要な場合は、プロパティを作成して true に設定します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

OAuth 受信

OAuth 受信は、インスタンスからデータをプルするためのサードパーティクライアント用のエンドポイントを提供します。

OAuth 統合を管理するには、security_admin ロールが必要です。

インスタンスからデータをプルするためのサードパーティクライアント用のエンドポイントをインスタンスに提供させたい場合は、**OAuth** 外部クライアントシナリオ (受信) 統合を構成できます。

> **注:**
> トークンを初めて取得するには、ユーザー認証を行う必要があります。その後は、トークンの有効期限が切れるまでユーザーアカウントを使用して認証する必要はありません。

次の権限許可タイプに応じて、OAuth 受信を構成できます。

- 認証コード：ユーザー名またはパスワードの入力を要求せずに、アクセストークンを使用して認証用の許可された URL を設定できる、ユーザーが開始した権限許可フローの場合に使用します。詳細については、「OAuth 認証コード権限許可フロー」を参照してください。
- リソース所有者のパスワード資格情報：認証にユーザーインタラクションを必要とする、ユーザーが開始した権限許可フローの場合に使用します。詳細については、パスワード権限許可フローの構成を参照してください。

  > **注:**
  > 認証コードフローの場合、ユーザーはローカルログイン、SSO、または MFA による認証を完了し、同意する必要があります。

- **JWT** ベアラー：ユーザーの介入が必要ないシステム間の統合の場合に使用します。詳細については、JWT ベアラー権限許可フローの構成を参照してください。
- **ID** トークンフロー：Okta、Azure などのサードパーティ OIDC プロバイダーによって発行された ID トークンを使用する場合に使用します。詳細については、認証の ID トークンフローを参照してください。
- **OAuth** の暗黙的な権限許可 **(OAuth implicit grants)**：ユーザーエージェント (通常は Web ブラウザまたはモバイルデバイス) を介してクライアントアプリケーションへのアクセストークンの直接付与を許可する場合に使用します。詳細については、「OAuth の暗黙的な権限許可」を参照してください。
- クライアント資格情報:サードパーティの OAuth クライアントからプラットフォームへのインバウンド統合に OAuth クライアント資格情報権限許可タイプを使用する場合ServiceNow 。詳細については、「クライアント資格情報」を参照してください。

OAuth スコープ

REST API の OAuth 認証スコープのサポートを詳しく調べることができます。OAuth スコープは、特定の REST APIs へのアクセスのみを提供します。詳細については、「REST API 認証スコープ」を参照してください。

OAuth 認証コード権限許可フロー

認証コード権限許可フローでは、リソースを信頼する OAuth サーバーで直接認証することで、ユーザーはリソースへのアクセスを許可されます。これは、ユーザー名/パスワード資格情報を使用した認証とは対照的です。

この OAuth 認証コードフローの実装により、REST を介してリソースにアクセスできるようになります。認証コードフレームワークは、ユーザーにユーザー名/パスワードの入力を要求するのではなく、ユーザーが設定した承認済み URL を介してアクセストークンを取得します。ユーザー名/パスワードは、リソースへのアクセスを要求しているクライアントに公開されることはありません。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

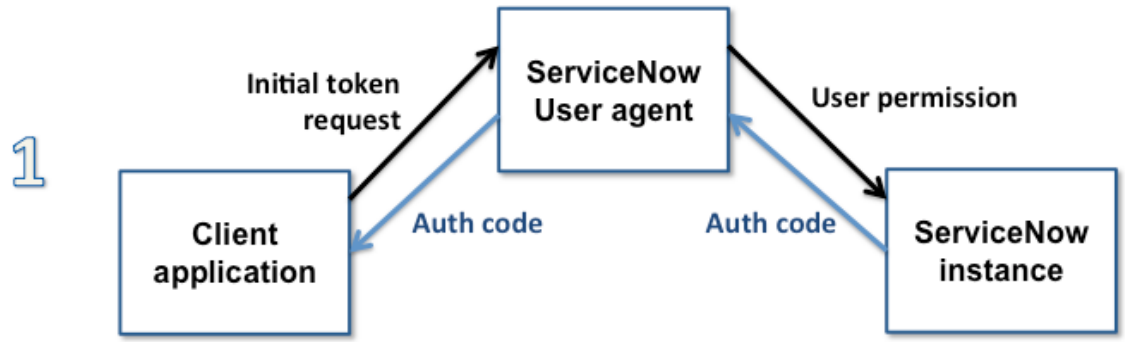
認証サーバーとしての **ServiceNow** インスタンス

OAuth サーバーは通常、サードパーティの認証サーバーです。認証コードフローのトークンを発行する認証サーバーとして ServiceNow インスタンスを指定することもできます。

制限付きリソースを所有するユーザーは、アクセスを許可する必要があります。またユーザーは、発行されたアクセストークンをいつでも取り消してアクセスを終了できます。

認証コード権限許可フロープロセス

認証コード権限許可フロープロセスは、次の 3 段階のステップで構成されています。



ステップ 1 では、クライアントアプリケーションまたは Web サイトが、ユーザーエージェントを介してインスタンスへの GET 要求の形式で REST API 呼び出しを開始します。通常、REST 呼び出しは、エンドユーザーがクライアントアプリケーションまたは Web サイトのボタンまたはリンクをクリックしてアクセストークンを要求すると開始されます。クライアントアプリケーションでは、エンドユーザーは認証 URL、トークン URL、クライアント ID、およびクライアントシークレットも指定する必要があります。これらのアイテムの説明については、「サードパーティ OAuth プロバイダーの使用」に記載されているフィールドの説明を参照してください。クライアントが権限許可タイプを要求した場合、エンドユーザーは認証コードを選択する必要があります。

クライアントアプリケーションからインスタンスへの GET 要求の例：

```
https://myinstance.service-now.com/oauth_auth.do?response_type=code&redirect_uri={the_redirect_url}&client_id={the_client_identifier}
```

注:
response_type は、標準の OAuth コード権限許可フローを使用するための **code** である必要があります。

エンドユーザーは、インスタンスの制限付きリソースへのアクセスを手動で許可する必要があります。ServiceNow 実装では、エンドユーザーはインスタンスにログインする必要があります。インスタンスは、[許可] および [拒否] ボタンがある UI ページでエンドユーザーにプロンプトを表示します。手順を参照してください。

クライアントアプリケーションが実際にトークンフォームを要求しているアイテムは、作成した OAuth プロバイダーアプリケーションレジストリレコードで、認証エンドポイントとも呼ばれます (「サードパーティ OAuth プロバイダーの使用」を参照してください)。認証コードが認証エンドポイントからクライアントに送信されます。この場合、クライアントには直接移動せず、認証エンドポイントフォームで指定するリダイレクト **URL** に移動します。この URL はコールバック URL とも呼ばれます。この URL は、クライアントアプリケーションまたは Web サイトから取得できます。

認証コードを提供する、インスタンスからクライアントアプリケーションへの応答の例：

```
https/http://{callbackURL}?code={the actual auth code}
```

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

クライアントアプリケーションは認証コードを取得したので、クライアントはそのコードを使用してアクセストークンを要求します。認証コードは、ユーザーがステップ 1 で同意したことを証明します。

クライアントアプリケーションから ServiceNow インスタンスへの POST 要求の例 (認証コードを提供し、アクセストークンを要求) :

```
https://myinstance.service-now.com/oauth_token.do?grant_type=authorization_code&code={the auth
 code}&redirect_uri={the_same_redirect_url}&client_id={the_same_client_identifier}&client_secret={client_secret_value}
```

インスタンスのエンドポイントは、アクセストークンとリフレッシュトークンを返します。リフレッシュトークンを使用して、追加のアクセストークンを要求できます。

インスタンスでは、トークンの取り消しなどのトークンの管理を実行できます。「OAuth トークンの管理」を参照してください。

クライアントアプリケーションは、アクセストークンを使用して REST API を認証します。クライアントアプリケーションを認証した後、REST API は要求されたデータを JSON ペイロードで返します。

インシデント [incident] テーブルのデータの JSON ペイロードの GET 要求の例 :

```
https://myinstance.service-now.com/api/now/table/incident?access_token={the_token}
```

注:
システムは、暗黙的な権限許可コードフローとも呼ばれる OAuth 暗黙的な権限許可もサポートしています。

統合サポート

認証コードフローは、インスタンスについて次の統合をサポートしています。

- マルチ SSO
- SAML 2.0 Update 1
- マルチファクター認証

モバイルインターフェイスもサポートされています。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

認証コードフローを使用した **OAuth** エンドポイントへのアクセス許可

ServiceNow インスタンスの保護されたリソースを所有するエンドユーザーは、インスタンスがアクセストークンを提供できるようにする前に、リソースへのアクセスを許可する必要があります。

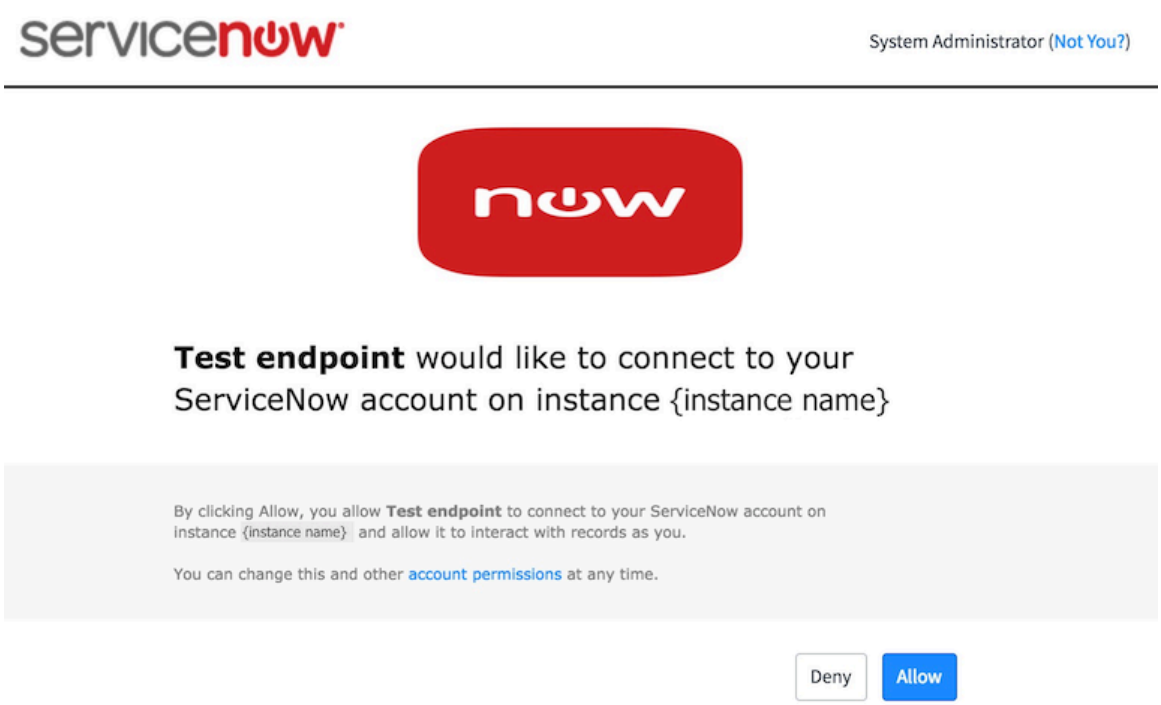
始める前に

必要なロール：なし。保護されたリソースを保持するインスタンスにすでにログインしている必要があります。あるいは、ServiceNow 管理者が設定済みの認証方法 (マルチファクター認証や SAML など) を使用してログインすることもできます。

手順

1. インスタンスの保護されたリソースへのアクセスを要求しているクライアントアプリケーションのリンクまたはボタンをクリックします。
   これにより、トークン要求が開始されます。あるインスタンスから別のインスタンスへの REST 呼び出しを行う場合、このリンクは REST メッセージフォームの **[OAuth** トークンの取得] になります。
2. ログインしていない場合は、今すぐログインしてください。
   右上隅で指定されているユーザーと同じユーザーでない場合は、[別のユーザーである場合] をクリックしてログインします。
3. アカウントの権限をクリックして、発行済みのアクセストークンのリストを開きます。
   これは、 セルフサービス > 自分の接続済み アプリトークンリスト。
4. [許可] をクリックしてアクセスを許可し、インスタンスに認証コード (認証コードフローを使用する場合) またはアクセストークン (暗黙的な権限許可タイプを使用する場合) を発行させます。

   [拒否] をクリックすると、認証は許可されませんが、インスタンスからログアウトされることはありません。



アクセスを確認するメッセージが表示されます。インスタンスの REST メッセージフォームからアクセスを要求すると、フォームの上部に [OAuth リフレッシュトークンが利用可能になり、{date} に期限切れになります (OAuth Refresh token is available and will expire at {date})] というメッセージが表示されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

認証コードフローステータスパラメーターの要件

glide.oauth.state.parameter.required システムプロパティを使用すると、認証コードフローの OAuth 要求でステータスパラメーターを要求できます。

ステータスパラメーター

必要なロール：なし。

Madrid リリース以降、システムプロパティ *glide.oauth.state.parameter.required* によって OAuth 要求のステータスパラメーターが追加されます。zboot インスタンスの場合、このプロパティは true です。アップグレードされたインスタンスの場合、このプロパティは存在しないため、ステータスパラメーターは有効になりません。ステータスパラメーターは文字列値であり、特殊文字を含めることはできません。ステータスパラメーターを空または空白文字にすることはできません。

ステータスパラメーターの検証

インスタンスにアクセスするクライアント用のエンドポイントを作成し ます。oauth_auth.do の認証コードフローを開始します。例：

```
http://myinstance.service-now.com/oauth_auth.do?grant_type=authorization_code&client_id=e9dba45b380d1300e676ccc91cef468f&response_type=code
```

要求でステータスパラメーターを指定しないと、エラーが発生し、認証コードは返されません。(要求にステータスパラメーターがありません。(Missing State parameter in request.))

ステータスパラメーターを要求に追加します。

```
http://myinstance.service-now.com/oauth_auth.do?grant_type=authorization_code&client_id=e9dba45b380d1300e676ccc91cef468f&response_type=code&state=123
```

ステータスパラメーターを追加すると、ログイン画面にリダイレクトされ、通常の認証コードフローが認証コードを返します。

> **注:**
> 応答 URL には、要求で渡されたステータスパラメーターが含まれています。この例では、追加されたパラメーターは state=123 です。

認証コードフローが oauth_initiator.do から開始される場合：

```
http://myinstance.service-now.com/oauth_initiator.do?oauth_requestor_context=sys_rest_message&oauth_requestor=eab8341fec0d1300964f214a2c2fcf67&oauth_provider_profile=dfa8f01fec0d1300964f214a2c2fcf51&response_type=code
```

ステータスパラメーターは、oauth_auth.do によってリダイレクトされると自動的に追加されます。

```
http://myinstance.service-now.com/oauth_auth.do?response_type=code&state=-790938844&redirect_uri=http://10.11.95.5:16001/oauth_redirect.do&client_id=e9dba45b380d1300e676ccc91cef468f
```

認証コードフローの例：認証サーバーとしての **ServiceNow** インスタンス

インスタンスを認証サーバーとして使用し、認証コードフローを使用してクライアントにトークンを発行するすることもできます。

始める前に

必要なロール：なし。

この例では、2 つのインスタンスを使用します。1 つは認証サーバーとして、もう 1 つはクライアントとして使用します。1 つのインスタンスが REST 呼び出しを使用して、別のインスタンスからトークンを要求します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

両方のインスタンスで OAuth のアクティブ化 を実行する必要があります。

手順

1. 承認サーバー インスタンス (Istanbul 以降のリリースを実行している) で、次の場所に移動します。 システム **OAuth** > アプリケーションレジストリー をクリックし、[新規] をクリックします。
2. [外部クライアント用の **OAuth API** エンドポイントを作成 **(Create an OAuth API endpoint for external clients)]** をクリックします。
3. 「インスタンスにアクセスするクライアント用のエンドポイントを作成し ます。」の説明に従って、OAuth アプリケーションレコードのフォームフィールドに入力します。
これらの手順を完了すると、認証サーバーが設定されます。次の手順に従って、クライアントサーバーを設定します。
4. クライアントインスタンスで、次の場所に移動します。 システム **OAuth** > アプリケーションレジストリー をクリックし、[新規] をクリックします。
5. [サードパーティ **OAuth** プロバイダーに接続 **(Connect to a third party OAuth Provider)]** をクリックします。
6. 「サードパーティ OAuth プロバイダーの使用」の説明に従って、OAuth アプリケーションレコードのフォームフィールドに入力します。
次のフィールド値に注意：
   - 名前：OAuth アクセスが必要なアプリケーションを識別する一意の名前。
   - クライアント **ID**：認証サーバー用に作成したアプリケーションレジストリレコードのクライアント ID。
   - クライアントシークレット：[読み取り専用] 自動生成された一意のアプリケーション ID。インスタンスは、アクセストークンを要求するときにクライアント ID を使用します。
   -
   - デフォルトの権限許可タイプ：[認証コード] を選択します。
   - 認証 **URL**：認証サーバーであるインスタンスの URL。URL の末尾に `oauth_auth.do` を追加することを忘れないでください。
   - ロゴ **URL**：アプリケーションロゴとして使用するイメージを含む URL。ユーザーがインスタンス上で制限されているリソースへのアクセスをクライアントアプリケーションに許可する要求を受け取ると、承認ページにロゴが表示されます。
   - トークン **URL**：認証サーバーであるインスタンスの URL。URL の末尾に `oauth_token.do` を追加することを忘れないでください。
   - リダイレクト **URL**：このインスタンスの URL：クライアントサーバーインスタンス。URL の末尾に `oauth_redirect.do` を追加することを忘れないでください。
7. 認証コード権限許可タイプでレコードのプロファイルを作成します。
クライアントサーバーがセットアップされます。これで、送信 REST メッセージを作成し、OAuth トークンを取得できるようになりました。
8. 移動先 システム **Web** サービス > 送信 > **REST** メッセージ をクリックし、[新規] をクリックします。
9. 「」の説明に従って、OAuth アプリケーションレコードのフォームフィールドに入力します。
次のフィールド値に注意：
   - エンドポイント：認証サーバーであるインスタンスの URL
   - 認証タイプ：**OAuth 2.0**
   - **OAuth** プロファイル：クライアントサーバー用に作成した OAuth プロファイル

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

10. REST メッセージレコードで、**[OAuth** トークンを取得] をクリックします。
11. トークンを提供するインスタンスで認証します。方法は Single Sign-on 統合に応じて変わります。
    使用できるものは次のとおりです。
    - インスタンスへの認証に使用するユーザー名とパスワード。
    - 有効になっている場合は IdP のユーザー名とパスワード。[外部ログインを使用] をクリックして IdP ログイン画面にアクセスします。

      注:
      IdP ログインページに自動的にリダイレクトするには、glide.authenticate.external システムプロパティを設定する必要があります。

    - MFA が有効になっている場合は、コード。
12. [許可] または [拒否] をクリックして認証を完了し、トークンを発行します。
    この後のプロセスの概要は「OAuth 認証コード権限許可フロー」で説明されています。

インスタンスにアクセスするクライアント用のエンドポイントを作成し ます。

外部クライアントアプリケーションが ServiceNow インスタンスにアクセスするための OAuth アプリケーションエンドポイントを作成します。

始める前に
必要なロール：管理者

手順

1. 移動先 すべて > システム **OAuth** > アプリケーションレジストリー をクリックし、[新規] をクリックします。
2. インターセプターページで、[外部クライアント用の **OAuth API** エンドポイントを作成] をクリックし、フォームに入力します。

フィールド	説明
名前	OAuth アクセスが必要なアプリケーションを識別する一意の名前。
クライアント ID	[読み取り専用] 自動生成された一意のアプリケーション ID。インスタンスは、アクセストークンを要求するときにクライアント ID を使用します。
クライアントシークレット	[必須] インスタンスとクライアントアプリケーションまたは Web サイトの両方が、相互通信を許可するために使用する共有シークレット文字列。インスタンスは、アクセストークンを要求するときにクライアントシークレットを使用します。インスタンスでクライアントシークレットを自動生成するには、このフィールドを空白のままにします。既存のクライアントシークレットを表示するには、ロックアイコンをクリックします。
リダイレクト URL	認証サーバーがリダイレクトするコールバック URL。リソースへのアクセスを要求しているクライアントの完全な URL を、末尾に /oauth_redirect.doを付けて入力します。たとえば、http://token_consumer:port/oauth_redirect.do のようになります。考えられるすべてのトークンコンシューマーに対して必要な数の URL を入力します。インスタンス

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	は、受信要求の URL をいずれかのリダイレクト URL と照合します。一致するものがない場合、インスタンスは最初のリダイレクト URL を使用します。
ロゴ URL	アプリケーションロゴとして使用するイメージを含む URL。ユーザーがインスタンス上で制限されているリソースへのアクセスをクライアントアプリケーションに許可する要求を受け取ると、承認ページにロゴが表示されます。
アクティブ	チェックボックスをオンにすると、アプリケーションレジストリがアクティブになります。
リフレッシュトークンの有効期間	リフレッシュトークンが有効である秒数。インスタンスは、リフレッシュトークンを要求するときに有効期間の値を使用します。デフォルトでは、リフレッシュトークンは 100 日 (8640000 秒) で期限切れになります。
トークン制限の適用	認証プロファイルを許可するように設定された API でのみトークンの使用を許可する場合に選択します。API アクセスポリシーを使用してアクセス許可を設定できます。詳細については、「REST API アクセスポリシーの作成」を参照してください。 デフォルト：未選択。
モバイルクライアント	モバイルアプリまたは Web のエンティティを表します。この情報は、モバイルまたは Web でログイン情報を分析するために使用されます。
アクセストークン有効期間	アクセストークンが有効である秒数。インスタンスは、アクセストークンを要求するときに有効期間の値を使用します。デフォルトでは、アクセストークンは 30 分 (1800 秒) で期限切れになります。
コメント	アプリケーションに関連付ける追加情報。

3. [送信] をクリックします。

タスクの結果

システムにより、OAuth クライアントタイプのレコードがアプリケーションレジストリ [oauth_entity] テーブルに作成されます。インスタンスが実際にトークンと認証コードを発行すると、それらはテーブルに格納されます。詳細については、「OAuth トークンの管理」を参照してください。

OAuth API 応答パラメーター

OAuth 2.0 API は、次のパラメーターを name:value ペアとして含む JSON 応答を生成します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

アクセストークン応答パラメーター

応答パラメーター	説明
scope	アクセストークンによって付与されるアクセスの範囲。スコープは常に **useraccount** です。これは、アクセストークンがトークンを承認したユーザーアカウントと同じ権限を持つことを意味します。たとえば、Abel Tuter がログイン資格情報を提供してアプリケーションを承認した場合、その結果生じるアクセストークンは Abel Tuter と同じアクセス権限をトークンベアラーに付与します。
token_type	OAuth RFC で定義されている要求によって発行されたトークンのタイプ。トークンタイプは常にベアラー です。これは、アクセストークンを持っているすべてのユーザーが、暗号化キーを提供しなくても保護されたリソースにアクセスできることを意味します。OAuth 2.0 でのベアラートークンの使用方法の詳細については、RFC6750 を参照してください。
expires_in	アクセストークンの有効期間 (秒単位)
refresh_token	リフレッシュトークンの文字列値
access_token	アクセストークンの文字列値アクセストークンの有効期限内に行われたアクセス要求は、常に現在のアクセストークンを返します。
format	[オプション] 応答の出力形式。この値は常に JSON です。

注:
OAuth プロバイダーが応答の本文を「Content-Type」でなく「content-type」として送信すると、OAuth HTTP クライアントで応答が正しく解析されない可能性があります。この問題を修正するには、次のパラメーターを使用してシステムプロパティを作成します。

フィールド	値
名前	glide.oauth.inhouse.httpclient.enabled
タイプ	true | false
値	false

システムプロパティの作成の詳細については、「システムプロパティを追加する」を参照してください。

次の例は、アクセストークン要求によって返される JSON 文字列を示しています。(読みやすくするためにスペースを追加しました)。

```
{"scope":"useraccount","token_type":"Bearer","expires_in":1800,
"refresh_token":"w599voG89897rGVDmdp12WA681r9E5948c1CJTPi8g4HGc4NWaz62k6k1K0FMxHW40H8yOO3Hoe",
"access_token":"F0jh9korTyzd9kaZqZ0SzjKZuS3ut0i4P46Lc52m2JYHiLIcqzFAumpyxshU9mMQ13gJHtxD2fy"}
```

OAuth API 要求パラメーター

アクセストークン要求が使用する OAuth API 要求パラメーターについて説明します。

注:
OAuth API のコンテンツタイプは `application/x-www-form-urlencoded` である必要があります。コンテンツタイプが `application/json` の場合、詳細不明のエラーが発生します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

アクセストークン要求パラメーター

要求パラメーター	説明
grant_type	[必須] アクセストークンの要求を許可する資格情報のタイプ。このパラメーターは、次のいずれかの値でなければなりません。 • **password**：アクセストークン要求を許可するためのユーザー資格情報のセット。ユーザー名とパスワードのパラメーターでユーザー資格情報を指定します。 • **refresh_token**：既存のリフレッシュトークンによってアクセストークン要求が許可されます。refresh_token パラメーターでリフレッシュトークンを指定します。
client_id	[必須] アクセストークンを要求するクライアントアプリケーションに対して自動的に生成される一意の ID
client_secret	[必須] インスタンスと OAuth アプリケーションが相互の通信を許可するために使用する共有シークレット文字列
ユーザー名	アクセストークン要求を許可するユーザーアカウント名。このパラメーターは、**password** の **grant_type** を使用したアクセストークン要求に必要です。
パスワード	アクセストークン要求を許可するユーザーアカウントのパスワード。このパラメーターは、**password** の **grant_type** を使用したアクセストークン要求に必要です。
refresh_token	アクセストークン要求を許可する既存のリフレッシュトークン。このパラメーターは、**grant_type** の **refresh_token** を使用したアクセストークン要求に必要です。

ユーザー資格情報を使用した要求

インスタンスでは、最初にクライアントを許可するとき、または新しいリフレッシュトークンの作成を許可するときに、ユーザーのログイン資格情報を提供することをクライアントに要求します。このタイプの要求は、常に次の 2 つのトークンを返します。

- アクセストークン
- リフレッシュトークン

インスタンスは、ユーザーがアクティブであり、現在ロックアウトされておらず、インタラクティブセッションがあることを確認します。これらの条件のいずれかが false の場合、インスタンスはアクセストークンを生成しません。アクセストークンの有効期限内に行われたアクセス要求は、常に現在のアクセストークンを返します。

注:
このタイプの認証権限許可は、送信中にユーザー資格情報を保護するために TLS 暗号化に依存しています。

次の例は、一連のユーザー資格情報を使用してアクセストークンを要求する方法を示しています (読みやすくするためにスペースが追加されています)。

```
$ curl -d"grant_type=password&client_id=be3aeb583ace210011c15b24a43e25d8
&client_secret=client_password
&username=admin&password=admin"
https://instancename.service-now.com/oauth_token.do
```

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

リフレッシュトークンを使用した要求

インスタンスは、既存のリフレッシュトークンを使用して新しいアクセストークンを作成できます。このタイプの要求は、アクセストークンのみを返します。インスタンスは、新しいアクセストークンを生成する前に、リフレッシュトークンが期限切れになっていないことを確認します。リフレッシュトークンの有効期限内に行われたアクセス要求は、常に現在のリフレッシュトークンを返します。一般に、リフレッシュトークンを送信する方が、ユーザー資格情報を送信するよりも安全です。次の例は、既存のリフレッシュトークンを使用してアクセストークンを要求する方法を示しています (読みやすくするためにスペースが追加されています)。

```
$ curl -d"grant_type=refresh_token&client_id=be3aeb583ace210011c15b24a43e25d8
&client_secret=client_password
&refresh_token=w599voG89897rGVDmdp12WA681r9E5948c1CJTPi8g4HGc4NWaz62k6k1K0FM
xHW40H8yOO3Hoe"
https://instancename.service-now.com/oauth_token.do
```

外部クライアント向けの **OAuth JWT API** エンドポイントの作成

OAuth JSON Web トークン (JWT) API エンドポイントを作成して、外部クライアントが Web トークンを使用して ServiceNow インスタンスにアクセスできるようにします。

始める前に

必要なロール：admin

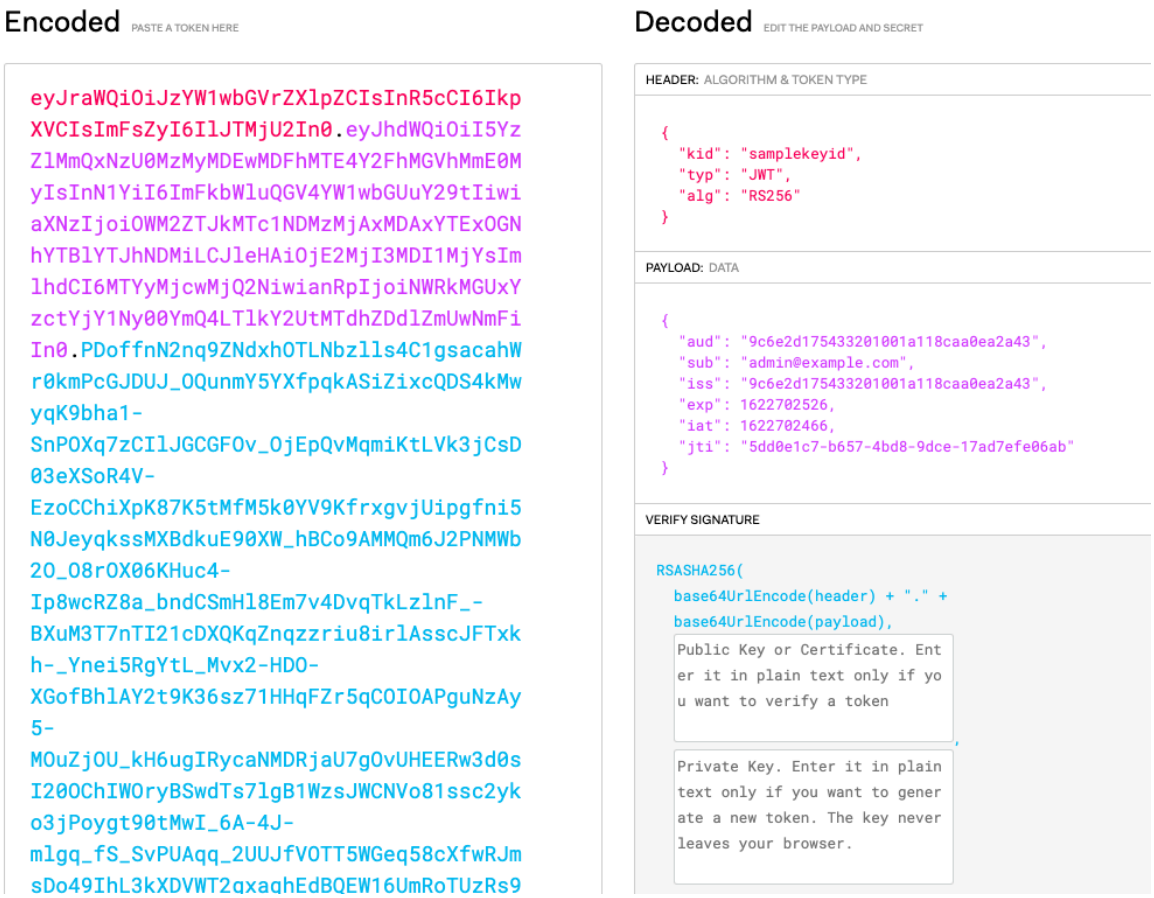
次の要求を含む JSON Web トークン (JWT) を生成します。

- `aud`：クライアント ID の値と一致する必要があります。
- `sub`：トークンを関連付けるユーザーのメールなど、ユーザー識別子である必要があります。
- `iss`：クライアント ID の値と一致させることをお勧めします。
- `exp`：任意の有効期限

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

デコードされた **JSON Web** トークンの例



JSON Web トークンの詳細については、「https://jwt.io/」を参照してください。

このタスクについて
外部 Web アプリケーションが、エンドユーザーに手動ログインを要求せず、代わりに受信 JWT 権限許可タイプを使用して、インスタンスでシームレスに認証できるようにします。JWT 権限許可タイプを使用すると、要求にパスワードが含まれないため、Web サービス間のセキュリティを強化できます。たとえば、外部アプリケーションを開発し、トークンを使用して ServiceNow インスタンスへの受信要求を認証できます。

手順

1. キーペアを作成し、公開鍵を X.509 証明書 (sys_certificate) テーブルに追加します。
2. ServiceNow インスタンスの構成を設定して、受信 JWT を確認します。

   a. 移動先 システム **OAuth** > アプリケーションレジストリー.

   b. [外部クライアント向けの **OAuth JWT API** エンドポイントの作成] を選択します。

   c. トークンに関する情報をフォームに入力します。

[OAuth JWT] テーブル

フィールド	説明
名前	JWT OAuth アクセスが必要なアプリケーションを識別する一意の名前

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

フィールド	説明
クライアント ID	自動生成された一意のアプリケーション ID。システムは、このフィールドの値を使用して公開鍵または共有鍵を取得し、JWT を検証します。このフィールドの値は、JWT の発行者要求および対象者要求の値と一致する必要があります。
クライアントシークレット	インスタンスとクライアントアプリケーションまたは Web サイトの両方が、相互通信を許可するために使用する共有シークレット文字列。インスタンスでクライアントシークレットを自動生成するには、このフィールドを空白のままにします。既存のクライアントシークレットを表示するには、ロックアイコンをクリックします。 **注:** [公開クライアント] を選択した場合は、[クライアントシークレット] を省略できます。
ロゴ URL	アプリケーションロゴとして使用するイメージを含む URL。ユーザーがインスタンス上で制限されているリソースへのアクセスをクライアントアプリケーションに許可する要求を受け取ると、承認ページにロゴが表示されます。
ユーザーフィールド	JWT の件名要求の値を照合するためにシステムが使用するユーザー (sys_user) テーブル内のフィールド。たとえば、件名要求の値が user.name@example.com であるトークンを追加する場合は、ユーザーフィールドを [メール] に設定します。このフィールドは、メールフィールドで user.name@example.com の値を検索し、一致するユーザーレコードを受信要求で使用するようにシステムに指示します。
JTI 検証を有効化	トークン交換のたびに新しいトークンを要求する場合に選択します。 デフォルト：オン
アプリケーション	読み込み専用のアプリケーションスコープ
アクセス可能	Cross-scope Access ポリシー。詳細については、「アプリケーションのアクセス設定」を参照してください。
アクセストークン有効期間	トークンが有効である時間 単位：秒
クロックスキュー	JWT の `exp` および `nbf` 要求を検証する際のサーバークロックとクライアントクロック間の許容時間差 単位：秒 デフォルト：300
トークン制限の適用	認証プロファイルを許可するように設定された API でのみトークンの使用を許可する場合に選択します。API アクセスポリシーを使用してアクセス許可を設定できます。詳細については、「REST API アクセスポリシーの作成」を参照してください。 デフォルト：未選択。
コメント	アプリケーションに関連付ける追加情報。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
公開クライアント	JWT クライアントが公開の場合は、このフィールドをフォームに追加します。選択した場合、クライアントシークレットを含める必要はありません。 デフォルト：未選択。

d. フォームを保存します。

e. [JWT 検証者マップ] 関連リストにレコードを追加して、JWT 署名を検証します。

JWT 検証者マップテーブル

フィールド	説明
名前	JWT マッピングレコードの名前。
Kid	JWT からのキー ID。
共有キー	指定されたキー ID の共有キー。
アプリケーション	読み込み専用のアプリケーションスコープ
システム外部審査済み書	X.509 証明書 (sys_certificate) テーブルの証明書レコード。

f. JWT に関連付けられているカスタム要求をすべて [OAuth JWT 要求検証] 関連リストに追加します。

次に示す必須要求には、レコードを追加する必要はありません。

- iss
- aud
- sub
- exp

[OAuth JWT 要求検証] テーブル

フィールド	説明
自分の外部クライアント (My external client)	OAuth JWT レコードが自動入力されます。
要求値タイプ	請求値のデータタイプ
要求名	追加する要求の名前
要求値	要求の値
アプリケーション	読み込み専用のアプリケーションスコープ

3. JWT トークンを含む cURL 要求を送信して、インスタンスからアクセストークンを取得します。

Example

アクセストークンを要求する cURL コマンドのサンプルを次に示します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

```
$ curl -d"grant_type= urn:ietf:params:oauth:grant-type:jwt-bearer
&client_id=be3aeb583ace210011c15b24a43e25d8
&client_secret=client_password
&assertion=
 eyJraWQiOiJzYW1wbGVrZXIpZCIsInR5cCI6IkpXVCIsImFsZyI6IlJTMjU2In0.eyJhdWQiOiI5YzZl
MmQxNzU0MzMyMDEwMDFhMTE4Y2FhMGVhMmE0MyIsInN1YiI6ImFkbWluQGV4YW1wbG
UuY29tIiwiaXNzIjoiOWM2ZTJkMTc1NDMzMjAxMDAxYTExOGNhYTBlYTJhNDMiLCJleHAiOjE
2MjI3MDI1MjYsImlhdCI6MTYyMjcwMjQ2NiwianRpIjoiNWRkMGUxYzctYjY1Ny00YmQ4LTlkY
2UtMTdhZDdlZmUwNmFiIn0.PDoffnN2nq9ZNdxhOTLNbzlls4C1gsacahWr0kmPcGJDUJ_OQu
nmY5YXfpqkASiZixcQDS4kMwyqK9bha1-SnPOXq7zCIIJGCGFOv_OjEpQvMqmiKtLVk3jCsD03
eXSoR4V-EzoCChiXpK87K5tMfM5k0YV9KfrxgvjUipgfni5N0JeyqkssMXBdkuE90XW_hBCo9AM
MQm6J2PNMWb2O_O8rOX06KHuc4-Ip8wcRZ8a_bndCSmHI8Em7v4DvqTkLzlnF_-BXuM3T7n
TI21cDXQKqZnqzzriu8irlAsscJFTxkh-_Ynei5RgYtL_Mvx2-HDO-XGofBhlAY2t9K36sz71HHqFZr
5qCOIOAPguNzAy5-MOuZjOU_kH6ugIRycaNMDRjaU7gOvUHEERw3d0sI20OChIWOryBSwdT
s7lgB1WzsJWCNVo81ssc2yko3jPoygt90tMwI_6A-4J-mlgq_fS_SvPUAqq_2UUJfVOTT5WGeq58
cXfwRJmsDo49IhL3kXDVWT2gxaqhEdBQEW16UmRoTUzRs9A9sOm18y3skmOVtnEOm-MIJM
FQZ754UMzbiH0ZsMmk1ivCGIjex5J0_IDjKElWF5RHGz3YShCoa4JKDZsqYMvIk1SvzyQXjuFqP
dS2vzg2m1eKGUwr3m6uNs_HflcDystwVdMZ7nLIBG4"
https://instancename.service-now.com/oauth_token.do
```

JWT クライアントが Mobile SDK などの公開クライアントである場合は、要求から client_id パラメーターと client_secret パラメーターを省略できます。client_id および client_secret を省略するアクセストークンを要求する cURL コマンドのサンプルを次に示します。

```
$ curl -d"grant_type= urn:ietf:params:oauth:grant-type:jwt-bearer
&assertion=
 eyJraWQiOiJzYW1wbGVrZXIpZCIsInR5cCI6IkpXVCIsImFsZyI6IlJTMjU2In0.eyJhdWQiOiI5YzZl
MmQxNzU0MzMyMDEwMDFhMTE4Y2FhMGVhMmE0MyIsInN1YiI6ImFkbWluQGV4YW1wbG
UuY29tIiwiaXNzIjoiOWM2ZTJkMTc1NDMzMjAxMDAxYTExOGNhYTBlYTJhNDMiLCJleHAiOjE
2MjI3MDI1MjYsImlhdCI6MTYyMjcwMjQ2NiwianRpIjoiNWRkMGUxYzctYjY1Ny00YmQ4LTlkY
2UtMTdhZDdlZmUwNmFiIn0.PDoffnN2nq9ZNdxhOTLNbzlls4C1gsacahWr0kmPcGJDUJ_OQu
nmY5YXfpqkASiZixcQDS4kMwyqK9bha1-SnPOXq7zCIIJGCGFOv_OjEpQvMqmiKtLVk3jCsD03
eXSoR4V-EzoCChiXpK87K5tMfM5k0YV9KfrxgvjUipgfni5N0JeyqkssMXBdkuE90XW_hBCo9AM
MQm6J2PNMWb2O_O8rOX06KHuc4-Ip8wcRZ8a_bndCSmHI8Em7v4DvqTkLzlnF_-BXuM3T7n
TI21cDXQKqZnqzzriu8irlAsscJFTxkh-_Ynei5RgYtL_Mvx2-HDO-XGofBhlAY2t9K36sz71HHqFZr
5qCOIOAPguNzAy5-MOuZjOU_kH6ugIRycaNMDRjaU7gOvUHEERw3d0sI20OChIWOryBSwdT
s7lgB1WzsJWCNVo81ssc2yko3jPoygt90tMwI_6A-4J-mlgq_fS_SvPUAqq_2UUJfVOTT5WGeq58
cXfwRJmsDo49IhL3kXDVWT2gxaqhEdBQEW16UmRoTUzRs9A9sOm18y3skmOVtnEOm-MIJM
FQZ754UMzbiH0ZsMmk1ivCGIjex5J0_IDjKElWF5RHGz3YShCoa4JKDZsqYMvIk1SvzyQXjuFqP
dS2vzg2m1eKGUwr3m6uNs_HflcDystwVdMZ7nLIBG4"
https://instancename.service-now.com/oauth_token.do
```

インスタンスは、その応答でアクセストークンを返します。

```
{
   "access_token":
 "KynMY2H0uwWkRc8g8YLXjnQxWbH5_wbnSiLsnaOoKw61GZkkV0ytZP74uF7hJyjfsWfaaFijq
Qzq2kcABNJxNA",
   "scope": "useraccount",
   "token_type": "Bearer",
   "expires_in": 1799
}
```

注:
受信 JWT 権限許可タイプには、リフレッシュトークンは含まれません。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

4. アクセストークンを使用してリソースにアクセスするための REST API 呼び出しを行います。

Example

トークンを使用してインシデントテーブルにアクセスする cURL コマンドは次のとおりです。

```
$ curl -H "Authorization: Bearer
 KynMY2H0uwWkRc8g8YLXjnQxWbH5_wbnSiLsnaOoKw61GZkkV0ytZP74uF7hJyjfsWfaaFijq
Qzq2kcABNJxN"
https://instancename.service-now.com/api/now/v1/table/incident
```

タスクの結果
システムが REST 呼び出しでアクセストークンを取得し、要求されたリソースへのアクセスを許可します。

Now Platform での OAuth OIDC プロバイダーの設定

OAuth OIDC プロバイダーで、受信 API 呼び出しまたは Single Sign-on オプション (複数プロバイダー SSO) を使用して、サードパーティの OIDC プロバイダーによって生成された ID トークンを受け入れるように設定できます。

始める前に
必要なロール：admin

このタスクについて
Now Platform は、受信 API 呼び出しに加えて、外部 Single Sign-on (SSO) 実装を通じて OIDC をサポートします。OIDC プロバイダー構成の例については、「Azure AD の設定」を参照してください。OIDC プロバイダー構成の SSO 固有の例については、「「Create an OpenID Connect (OIDC) configuration for Single Sign-On (SSO) (Single Sign-on (SSO) 用の OpenID Connect (OIDC) 構成の作成)」を参照してください。

手順

1. 移動先 すべて > システム **OAuth** > アプリケーションレジストリー.
   - [新規] をクリックして **[ID** トークンを検証するために **OIDC** プロバイダを構成] を選択して、フォームに入力します。
   - 既存のテンプレートを OIDC プロバイダー (ADFS、Auth0、Azure AD、Google、Okta) に選択して、フォームに入力します。

     注:
     OIDC プロバイダテンプレートは、デモデータを OAuth 2.0 プラグインを使用してロードした後に利用できます。

フィールド	説明
名前	OAuth OIDC エンティティを識別する一意の名前。
クライアント ID	サードパーティの OAuth OIDC サーバーに登録されているアプリケーションのクライアント ID。インスタンスは、アクセストークンを要求するときにクライアント ID を使用します。
クライアントシークレット	サードパーティの OAuth OIDC サーバーに登録されているアプリケーションのクライアントシークレット

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
OAuth API スクリプト	外部 OAuth プロバイダーへの要求および応答のカスタマイズに使用されるスクリプト
OAuth OIDC プロバイダ設定	OIDC プロバイダー (ADFS、Auth0、Azure AD、Google、Okta) を使用して、JWT トークンを検証できます。OIDC プロバイダー構成のレコードをクリックして、[ユーザー要求] と [ユーザーフィールド] が適切に設定されていることを検証します。**[JTI 要求検証を有効化]** をオンにすると、ServiceNow JWT トークン検証では、プロバイダーによって送信された JTI も検証されます。 **注:** 検証がチェックされない場合、JWT トークンに存在するかどうかにかかわらず、JTI を検証できません。
クロックスキュー	制約が有効と見なされる秒数。デフォルトは 300 です。
コメント	アプリケーションに関連付ける追加情報。
アプリケーション	このエンティティを含むアプリケーションの名前
アクセス可能	すべてのアプリケーションスコープから、またはこのアプリケーションスコープからのみアクセスできるようにするオプションを選択します。
トークン制限の適用	認証プロファイルを許可するように設定された API でのみトークンの使用を許可する場合に選択します。API アクセスポリシーを使用してアクセス許可を設定できます。詳細については、「REST API アクセスポリシーの作成」を参照してください。 デフォルト：未選択。
アクティブ	チェックボックスをオンにすると、OAuth アプリケーションがアクティブになります。
リダイレクト URL	認証コードを受信するための OAuth アプリケーションの URL
セッション終了のエンドポイント URL	セッションの終了後に有効になる URL エンドポイント
強制認証の有効化	ユーザーの強制認証を有効にするオプション。

2. [送信] をクリックします。
レコードは、アプリケーションレジストリー [oauth_entity] テーブルに保存されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

インスタンスがトークンと認証コードを発行すると、アプリケーションレジストリ [oauth_entity] テーブルに、外部 **OIDC** プロバイダータイプのレコードが作成されます。詳細については、を参照してください。

3. オプション: レコードの OAuth エンティティプロファイルの関連リストに移動し、スコープのない新規 OAuth プロバイダーのシステム生成デフォルトプロファイルを検証します。
名前、権限許可タイプ、OAuth スコープなどの OAuth プロバイダープロファイルを変更または追加できます。
4. オプション: レコードの OAuth エンティティスコープの関連リストに移動し、この OAuth プロバイダーで利用可能なすべての OAuth スコープを定義します。
定義されたスコープは、プロファイルを作成または更新するときに選択できます。定義された各 OAuth スコープには、読み取りスコープや書き込みスコープなど、プロバイダーの仕様からの取得が必要な名前とスコープが含まれています。各スコープは個別に定義する必要があります。
5. オプション: ユーザープロビジョニングレコードの関連リストに移動して、自動ユーザープロビジョニングを有効にします。

オプション	説明
ユーザーを自動プロビジョニング	ユーザーの強制認証を有効にするオプション。
データソースをプロビジョニング	OIDC トークンを ServiceNow ユーザーに変換するために使用するデータソース。ルックアップリストを使用して、事前定義されたデータソーステンプレートを選択し、レコードを開いて変換テーブルのマッピングを構成します。変換マッピングを構成する際に、ソースフィールドは *JWT token*から取得され、ターゲットフィールドは *sys_user* テーブルから取得されます。
プロビジョニングされたユーザーに適用されるユーザーロール	新しくプロビジョニングされた ServiceNow ユーザーに適用されるユーザーロール。

OAuth の暗黙的な権限許可

ServiceNow インスタンスは、アクセストークンの暗黙的な権限許可をサポートしています。

暗黙的な権限許可タイプは、*implicit grant code flow*とも呼ばれ、ユーザーエージェント (通常は Web ブラウザーまたはモバイルデバイス) を介してクライアントアプリケーションにアクセストークンを直接付与できます。リフレッシュトークンは付与されません。この場合でも、エンドユーザーは標準の場合と同様に、インスタンスの保護されたリソースへのアクセスを許可する必要があります。

OAuth の暗黙的な権限許可フロープロセス

標準の認証コードフロープロセスと同様に、クライアントアプリケーションはインスタンスで制限付きリソースの使用を要求し、エンドユーザーはそれを承認します。要求はインスタンスに送信される URL の形式です。URL には次のようなパラメーターを含める必要があります。

- client_id=<必要なクライアント ID>。これは、クライアントアプリケーションがアクセスしようとしている保護リソースを識別するために必須です。
- response_type=token。これはアクセストークンを直接要求するために必須です (認証コードの要求とは対照的)。暗黙的な権限許可では、値は token になります。標準の認証コードフローの例では、応答タイプは code です。
- redirect_uri=<a URL>：トークンが送信される場所。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

認証サーバーは、ユーザーエージェントを通じて、認証コードではなくアクセストークンをクライアントアプリケーションに送信します。

インシデント [incident] テーブルのデータの JSON ペイロードを取得する GET 要求の例を示します。

```
https://myinstance.servicenow.com/oauth_auth.do?response_type=token&redirect_uri={the_redirect_url}&client_id={the_client_identifier}
```

ユーザーがアクセスを許可すると、トークンがリダイレクト (コールバック) URL に含まれます。

```
https/http://{callbackURL}?access_token={the_token}
```

OAuth トークンの管理

制限付きリソースへのアクセスを提供する OAuth トークンを開きます。

始める前に

必要なロール：任意のユーザーまたは admin

このタスクについて

インスタンスとサードパーティの OAuth プロバイダーによって発行された OAuth トークンは、[oauth_credential] テーブルに格納されます。

このテーブルの重要な列には次のようなものがあります。

- トークン： ServiceNow インスタンスによって発行されたトークンの値。
- タイプ：トークンがアクセストークンかリフレッシュトークンかを判断します。
- 有効期限：アクセストークンまたはリフレッシュトークンの有効期限が切れる日付/時刻。
- 受信したトークン：サードパーティの OAuth プロバイダーによって発行されたトークンの値。この値は暗号化された形式です。

トークンの有効期限と有効性は次のとおりです。

- アクセストークン：デフォルトで、インスタンスが OAuth プロバイダーであるシナリオでは、インスタンスは 30 分の有効期間でアクセストークンを発行します。
- リフレッシュトークン：デフォルトで、インスタンスが OAuth プロバイダーであるシナリオでは、インスタンスは 100 日の有効期間でリフレッシュトークンを発行します。

手順

1. 次のいずれかのメニューオプションに移動します。
   - セルフサービス > 自分の接続済みアプリ をクリックして、インスタンスのリソースへのアクセスを許可したときにインスタンスが作成したトークンを表示します。
   - システム **OAuth** > トークンを管理 をクリックして、すべてのトークンを表示します。このモジュールへは、管理者のみがアクセスできます。
2. [名前] をクリックしてトークンを開きます。
3. [アクセスを取り消す] をクリックして、制限付きリソースへのアクセスを防止します。
4. アクセスが許可されているスコープや有効期限など、トークンに関するその他の情報を表示することもできます。

OAuth トークンの取り消し

セキュリティ上の理由から、OAuth アクセス権を取り消したり、トークンをリフレッシュしたりすることができます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

始める前に
必要なロール：管理者

このタスクについて
トークンの取り消しは、インスタンスが OAuth リソースサーバーとして機能する状況に関連しています。URL または次を使用してトークンを取り消すことができます。

手順

oauth_revoke_token.do を使用してインスタンスにアクセスし、アクセストークンまたはリフレッシュトークンを追加します。

例：https://[Your_ServiceNow_Instance]:[port]/oauth_revoke_token.do?token=[access or refresh token] (角かっこ [ ] は削除)

タスクの結果
このエンドポイントアクセスには認証は必要ありません。この要求のトークンは期限切れとしてマークされています。

クライアント資格情報

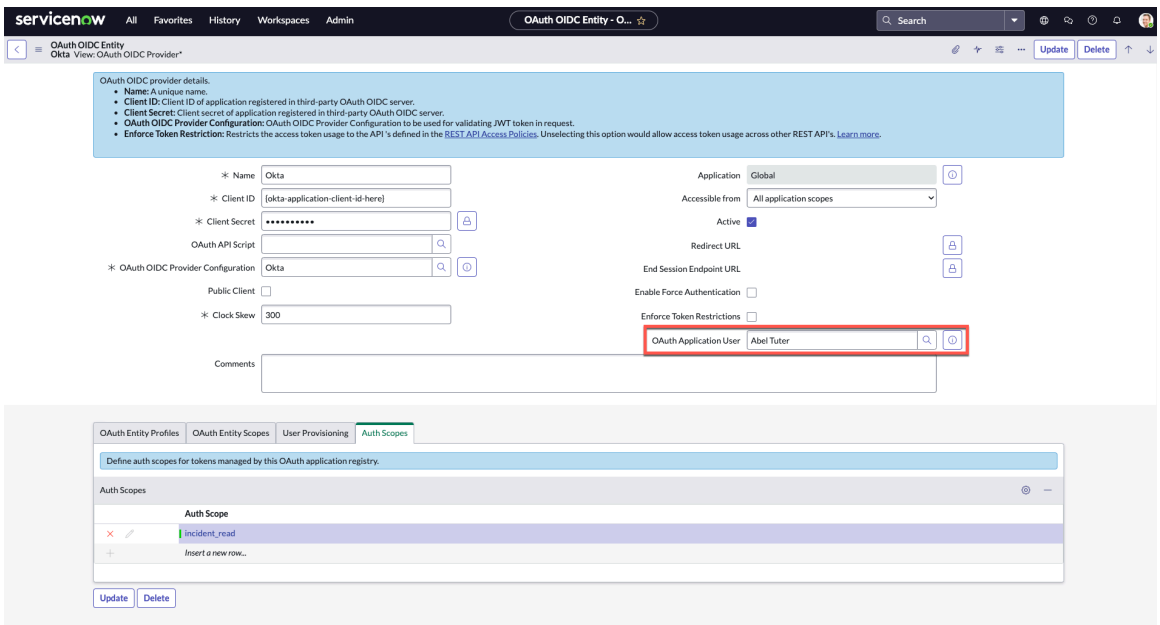
サードパーティの OAuth クライアントからプラットフォームへのインバウンド統合には ServiceNow 、OAuth クライアント資格情報権限許可タイプを使用します。

管理者は、クライアント資格情報 (CC) 権限許可タイプを使用して、サードパーティの OAuth クライアントからプラットフォームへの ServiceNow 統合を有効にできます。

受信クライアント資格情報権限許可タイプは、システムプロパティを介して制御できる機能です。デフォルトでは、システムプロパティは false になっています。

クライアント資格情報権限許可タイプを使用するには、次の手順を実行する必要があります。

- glide.oauth.inbound.client.credential.grant_type.enabled システムプロパティを作成します。
- **OAuth** エンティティフォームに **OAuth** アプリケーションユーザーフィールドを追加します。



クライアント資格情報システムプロパティの作成

OAuth インバウンド統合にクライアント資格情報権限許可タイプを使用するには、glide.oauth.inbound.client.credential.grant_type.enabled システムプロパティを作成します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

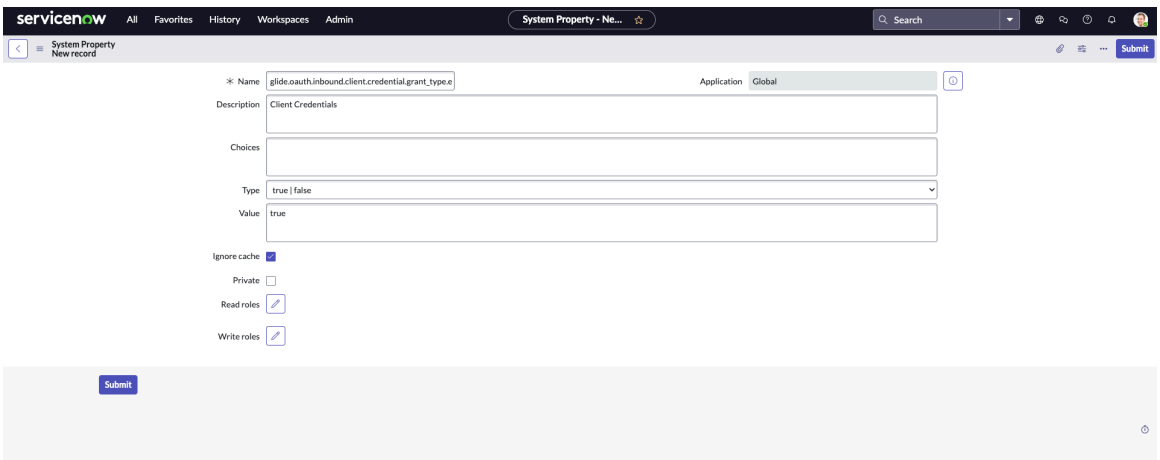
始める前に
必要なロール：admin

必要なプラグイン:OAuth 2.0。

手順

1. ナビゲーションフィルターで、「sys_properties.list」と入力します。
   システム プロパティ [sys_properties] テーブル内のプロパティの全リストが表示されます。
2. [新規] を選択します。
3. フォームの以下のフィールドに入力します。

フィールド	説明
名前	作成しているプロパティの名前。この場合は、glide.oauth.inbound.client.credential.grant_type.enabled です。
説明	プロパティの機能を説明する簡単な説明文を入力します。
タイプ	リストから適切なデータタイプを選択します。この場合、 true | false です。
値	プロパティの目標値を設定します。この場合、true にすると、OAuth インバウンド統合のクライアント資格情報権限許可タイプが有効になります。



注:
選択肢、キャッシュを無視、プライベート、読み取りロール、書き込みロールなどのフォームの他のフィールドは、要件に従って構成できます。

4. [送信] を選択します。

注:
[キャッシュを無視] チェックボックスをオンにすると、パラメーターが変更されたときにサーバーのキャッシュがフラッシュされます。

次に、OAuth クライアント (外部クライアント用の OAuth API エンドポイント) を作成し、OAuth クライアントレコードに [OAuth アプリケーションユーザー] フィールドを追加する必要があります。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

OAuth アプリケーションユーザーの追加

OAuth インバウンド統合にクライアント資格情報権限許可タイプを使用するには、OAuth エンティティフォームに [OAuth アプリケーションユーザー] フィールドを追加します。

始める前に

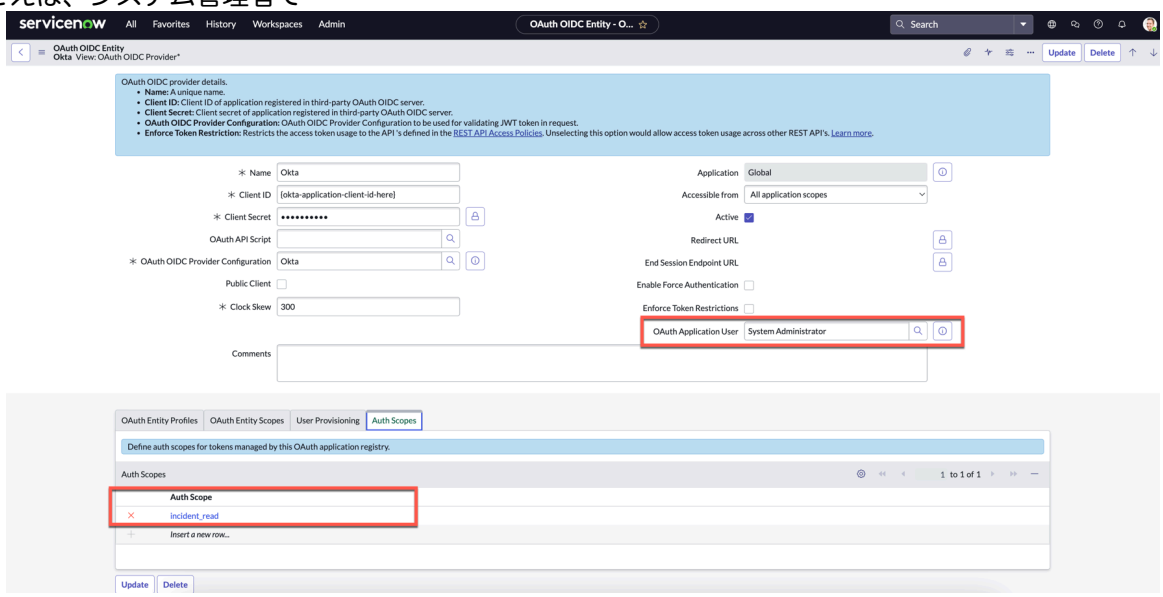
必要なロール：admin

必要なプラグイン:OAuth 2.0。

OAuth クライアントを作成する必要があります。詳細については、「インスタンスにアクセスするクライアント用のエンドポイントを作成し ます。」を参照してください。

手順

1. 作成された OAuth クライアントレコードを開きます。
2. ページヘッダーの [その他のオプションを選択] アイコン。
3. 選択 構成 > フォームデザイン.
4. [フォームデザイン] ページで、フィールドのリストから **OAuth** アプリケーションユーザー を追加します。
5. フォームを保存または更新します。
6. **OAuth** アプリケーションユーザーのユーザーを選択します。
   たとえば、システム管理者で



す。

> **注:**
> サードパーティのクライアントに提供されるアクセスを制御するには、クライアント資格情報権限許可タイプで REST API 認証スコープを使用する必要があります。

7. フォームを保存または更新します。

権限許可タイプがクライアント資格情報、クライアント **ID**、およびシークレットである認証要求は、 でServiceNow 関連付けられた OAuth アプリケーションユーザに渡されます。

> **注:**
> OAuth クライアントレコードで OAuth アプリケーションユーザーが選択されていない場合、またはクライアント資格情報プロパティが `false` に設定されている場合、認証要求は渡されません。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

OAuth 送信

OAuth 送信を使用すると、サードパーティプロバイダーからインスタンスにデータをプルできます。

OAuth 統合を管理するには、security_admin ロールが必要です。

次の権限許可タイプに対して送信 OAuth 2.0 を設定できます。

- サードパーティプロバイダーに接続 **(Connect to third-party provider)**：クライアント ID とシークレットを使用して OAuth プロバイダーに送信します。詳細については、「サードパーティ OAuth プロバイダーへの接続」を参照してください。
- **JWT** ベアラー：認証サーバーは、ID とセキュリティ情報をセキュリティドメイン間で共有できるようにする JWT トークンを検証します。詳細については、「JWT ベアラー権限許可タイプで OAuth プロバイダーを設定」を参照してください。
- **SAML2** ベアラー：SAML2 アサーションを生成し、プロバイダーとアクセストークンのアサーションを交換します。

  注:
  SuccessFactors への送信要求では、**[SAML2** ベアラー] をデフォルトの権限許可タイプとして使用します。

- 認証コード：アクセストークンを取得するためにクライアントに付与され、リソースへのアクセス権を取得するために使用されるコード。このオプションを選択する場合は、認証 URL (認証サーバーの URL) が必要です。
- リソース所有者のパスワード資格情報：リソースへのアクセス権の取得を試行するユーザーのユーザー名とパスワード。
- クライアント資格情報：どちらもアクセストークンを取得するために使用されるクライアント ID とクライアントシークレット。このメソッドはリフレッシュトークンを提供しません。

OAuth プロバイダーシナリオ (送信) を構成できます。インスタンスがサードパーティプロバイダーからデータをプルします。

注:
トークンを初めて取得するには、ユーザー認証を行う必要があります。その後は、トークンの有効期限が切れるまでユーザーアカウントを使用して認証する必要はありません。

サードパーティ OAuth プロバイダーへの接続

クライアント ID とシークレットを OAuth プロバイダーに送信する方法を設定します。

始める前に
必要なロール：管理者

手順

1. 移動先 すべて > システム **OAuth** > アプリケーションレジストリー をクリックし、[新規] をクリックします。
2. インターセプターページで、[サードパーティ **OAuth** プロバイダーに接続します] をクリックし、フォームに入力します。

フィールド	説明
名前	サードパーティ OAuth 接続のための一意の名前

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

フィールド	説明
クライアント ID	サードパーティの OAuth サーバーに登録されているアプリケーションのクライアント ID
クライアントシークレット	サードパーティの OAuth サーバーに登録されているアプリケーションのクライアントシークレット
OAuth API スクリプト	外部 OAuth プロバイダーへの要求および応答のカスタマイズに使用されるスクリプト
ロゴ URL	OAuth アプリケーションのロゴの URL
デフォルトの権限許可タイプ	トークンを確立するために使用するデフォルトの権限許可タイプ次の選択肢があります。 ○ 認証コード：アクセストークンを取得するためにクライアントに付与され、リソースへのアクセス権を取得するために使用されるコード。このオプションを選択する場合は、認証 URL (認証サーバーの URL) が必要です。 ○ リソース所有者のパスワード資格情報：リソースへのアクセス権の取得を試行するユーザーのユーザー名とパスワード。 ○ クライアント資格情報：どちらもアクセストークンを取得するために使用されるクライアント ID とクライアントシークレット。このメソッドはリフレッシュトークンを提供しません。 ○ **JWT** ベアラー：認証サーバーは、ID とセキュリティ情報をセキュリティドメイン間で共有できるようにする JWT トークンを検証します。 ○ **SAML2** ベアラー：SAML2 アサーションを生成し、プロバイダーとアクセストークンのアサーションを交換します。 **注:** SuccessFactors への送信要求では、**[SAML2** ベアラー] をデフォルトの権限許可タイプとして使用します。
リフレッシュトークンの有効期間	リフレッシュトークンが有効になる時間 (秒) デフォルトの時間は 86,400,000 秒です。
公開クライアント	パブリッククライアントが認証に PKCE を要求できるようにします。 **注:** PKCE が有効になっている場合、*`Default Grant type`*として使用できるのは認証コードのみです。
コードの課題メソッド	OAuth PCKE ワークフローで使用されるコード課題メソッド次の選択肢があります。 ○ S256 [デフォルト] ○ プレーン ○ なし
コメント	OAuth アプリに関するコメントを追加します。
アプリケーション	このレコードを含むアプリケーションとスコープです。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
アクセス可能	すべてのアプリケーションスコープから、またはこのスコープからのみアプリにアクセスできるようにします。
アクティブ	チェックボックスをオンにすると、アプリがアクティブになります。
認証 URL	OAuth 認証コードのエンドポイント
トークン URL	OAuth サーバートークンエンドポイント
トークン失効 URL	OAuth サーバートークン失効エンドポイント
リダイレクト URL	OAuth コールバックエンドポイント空白のままにすると、インスタンスによってエントリが自動生成されます。
相互認証を有効にします	トークンの要求と取り消しに相互認証を使用するチェックボックス。この機能では、相互認証プロファイルを指定する必要があります。
資格情報の送信	OAuth クライアントが要求にクライアント資格情報を入力します。 ○ 要求本文内 (フォーム URL エンコード) ○ 基本認証ヘッダー ○ 秘密キー JWT として

システムにより、タイプが OAuth プロバイダーのレコードがアプリケーションレジストリ [oauth_entity] テーブルに作成されます。

3. オプション: レコードの OAuth エンティティプロファイルの関連リストに移動し、スコープのない新規 OAuth プロバイダーのシステム生成デフォルトプロファイルを検証します。
名前、権限許可タイプ、OAuth スコープなどの OAuth プロバイダープロファイルを変更または追加できます。
4. オプション: レコードの OAuth エンティティスコープの関連リストに移動し、この OAuth プロバイダーで利用可能なすべての OAuth スコープを定義します。
プロファイルを作成または更新するときにスコープを選択できます。各 OAuth スコープには、読み取りスコープや書き込みスコープなど、プロバイダーの仕様からの取得が必要な名前とスコープが含まれています。各スコープは個別に定義する必要があります。

JWT ベアラー

JSON Web トークン (JWT) を使用すると、ServiceNow と外部 API プロバイダーの間でユーザーの介入を必要とせずにサーバー間 API のやり取りを設定する機能が有効化されます。

JSON Web トークン (JWT) ベアラー権限許可は、アクセストークンを発行する前に、認証サーバー側の JWT 権限許可ハンドラーによって評価および検証される要求値を含む JSON 文字列です。

JWT ベアラー権限許可タイプを使用すると、送信 REST メッセージの OAuth 2.0 JWT ベアラー権限許可フローを構成できます。

JWT ベアラー権限許可タイプで OAuth プロバイダーを設定

JSON Web トークン (JWT) を使用すると、ServiceNow と外部 API プロバイダーの間でユーザーの介入を必要とせずにサーバー間 API のやり取りを設定する機能が有効化されます。このサポートにより、統合ハブ や JWT を使用する他の自動化タスクが、API およびサービスとさまざまなプロバイダーとの統合を構成できるようになります。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

始める前に
必要なロール：admin

このタスクについて
次のタスクは、OAuth 2.0 クライアント認証および認証権限許可に JWT を使用するように ServiceNow を設定する方法を示しています。ServiceNow は OAuth クライアントで、Box や Docusign などの OAuth プロバイダーを構成できます。

手順

1. Java KeyStore 証明書のアップロード
   JWT クライアント認証を有効にするために使用する JKS 証明書をインスタンスに添付します。
2. JWT 署名キーの構成
   Java KeyStore (JKS) 証明書にアサインする JWT 署名キーを作成します。
3. JWT 署名キーを使用した JWT プロバイダーの作成
   JWT プロバイダーを ServiceNow インスタンスに追加します。
4. サードパーティ OAuth プロバイダーへの接続
   ServiceNow アプリケーションレジストリのデフォルトの権限許可タイプとして JWT ベアラーを使用して、サードパーティ OAuth プロバイダーを作成します。
5. OAuth プロファイルの指定
   OAuth プロバイダーの OAuth エンティティプロファイルを開き、JWT プロバイダーをアサインします。

Java KeyStore 証明書のアップロード

JWT クライアント認証を有効にするために使用する Java KeyStore (JKS) 証明書をインスタンスに添付します。

始める前に
必要なロール：管理者

手順

1. 移動先 すべて > マルチプロバイダー **SSO** > **x509** 証明書.
2. 必要に応じてフォームに入力します。

オプション	説明
名前	証明書の一意の名前
期限切れ時に通知	証明書の有効期限が切れたときに通知するユーザーを指定します。
有効期限切れ前に警告	証明書の有効期限が切れる前に、証明書マネージャーにメール通知を送信します。
アクティブ	トークン要求に使用する証明書を有効にします。
タイプ	アップロードする証明書のタイプ
数日中に期限切れ	証明書の有効期限が切れるまでの日数
キーストアパスワード	証明書に関連付けられたパスワード

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

オプション	説明
簡単な説明	

3. [送信] をクリックします。

JWT 署名キーの構成

Java KeyStore (JKS) 証明書にアサインする JSON Web トークン (JWT) 署名キーを作成します。

始める前に
必要なロール：admin

注:
JWT キーの一部としてヘッダーに **X.509** 証明書 **SHA-1** サムプリント **int (x5t)** を追加する場合は、フォームを構成し、[**X.509** 証明書 **SHA-1** サムプリント **int (x5t)**] フィールドを追加する必要があります。

手順

1. 移動先 すべて > システム **OAuth** > **JWT** キー.
2. 必要に応じてフォームに入力します。

オプション	説明
名前	JWT キー署名構成の一意の名前。
署名キーストア	JWT に署名するときに指定されたキーストア。
キー ID	Key ID (kid) は、複数のキーを使ってトークンに署名する際に、どのキーを使用するかを識別するのに役立ちます。 注: このフィールドを設定した場合、キー ID 要求は JWT に含まれます。このフィールドを設定しない場合、JWT にキー ID 要求はありません。
署名アルゴリズム	JWT キーでの署名に使用するアルゴリズム。使用可能なアルゴリズムは RSA 256 のみです。
署名キーパスワード	署名キーに関連付けられたパスワード。
アクティブ	JWT キーエイリアスが JWT プロバイダーからアクティブに参照されることを指定します。

3. [送信] をクリックします。

JWT 署名キーを使用した JWT プロバイダーの作成

JSON Web トークン (JWT) プロバイダーを ServiceNow インスタンスに追加します。

始める前に
必要なロール：管理者

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. 移動先 すべて > システム **OAuth** > **JWT** プロバイダー.
2. フォームに入力し、[送信] をクリックします。

オプション	説明
名前	JWT プロバイダー構成の一意の名前
有効期限の間隔 (秒)	JWT プロバイダーによって生成されたトークンの有効期間 (秒)
署名構成	適用する ServiceNow JWT 署名キー構成

JSON Web トークン (JWT) の生成

Now Platform で二者間で安全にクレームを表すための JSON Web トークン (JWT) を作成します。

GlideJWT API は、JWT を生成するスコープ付きのスクリプト可能な API です。JWT を生成する前に必要な引数は 3 つあります。

- JWT プロバイダーの Sys_id
- JSON シリアル化ヘッダー
- JSON シリアル化ペイロード

JWT プロバイダーを構成するときに使用できる JWT API スクリプトは、JWTTokenInternal と JWTTokenRestricted の 2 つです。JWTTokenRestricted スクリプトを使用すると、管理者は JWT を生成できるユーザーを設定できます。JWTTokenInternal スクリプトは読み取り専用で、ログインしたユーザーのみが JWT を生成できます。

JWT を生成するには：

- 共有キー (HMAC) または署名キーストア (RSA) を使用して JWT キーを作成します
- JWT キーを参照して JWT プロバイダーを署名構成に関連付けます

API を使用してトークンを作成できます。

JWT プロバイダーを構成するときには、標準およびカスタム要求を使用できます。generateJWT API 署名の一部として、動的なヘッダーとペイロードの要求を渡すことができます。

API をテストするサンプルスクリプト：

```
var jwtAPI = new sn_auth.GlideJWTAPI();
var headerJSON = {  "kid": "a1234"  };
var header = JSON.stringify(headerJSON);

var payloadJSON = { "jti": "testjti", "iss": "testiss", "sub": "testsub" };
var payload = JSON.stringify(payloadJSON);

var jwtProviderSysId = "7a40dde2d5303300964fb7c8f3c14ab5";
var jwt = jwtAPI.generateJWT(jwtProviderSysId, header, payload);

gs.info("JWT:" + jwt);
```

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

OAuth クライアント API

OAuth クライアント API は、OAuth トークンを要求するメソッドや取り消すためのメソッドを提供します。

OAuth クライアントは次のクラスを提供します。

- GlideOAuthClient ：リフレッシュトークンとアクセストークンの要求と取り消しを行うメソッド。
- GlideOAuthClientRequest ：クライアント要求を処理するためのメソッド。
- GlideOAuthClientResponse ：クライアント応答を処理するためのメソッド。
- GlideOAuthToken ：アクセストークンと、アクセストークンに関する情報を取得するためのメソッド。

OAuthUtil スクリプトインクルードをカスタマイズして、要求パラメーターをインターセプトし、外部 OAuth プロバイダーからの応答を解析することもできます。

スコープ付きスクリプトで OAuth クラスを使用する場合は、`sn_auth` 名前空間識別子を使用します。

デフォルトプロファイルサポート用の OAuth パラメーター

デフォルトのプロファイル機能には、*`setParameter()`* API と同時に使用して、OAuth リクエスター、リクエストのコンテキスト、プロバイダー プロファイルを指定できる一連のパラメーターが必要です。

OAuth プロバイダーのシナリオでは、デフォルトで使用する OAuth プロファイルを OAuth プロバイダーに指示する 3 つのパラメーターを設定する必要があります。これらの 3 つのパラメーターが設定されると、アクセストークンがインスタンスデータベースに保存されます。パラメーターは *`GlideOAuthClientRequest`* と共に使用します。

デフォルトプロファイルサポート用の OAuth パラメーター

パラメーター	説明
oauth_requestor	オブジェクトの sys_id。これはユーザーレコードまたは電子メールアカウントです。
oauth_requestor_context	OAuth リクエスターのコンテキストを提供する記述子。oauth_requestor オブジェクトが保存されたテーブルの名前を使用することをお勧めします。
oauth_provider_profile	デフォルトの OAuth プロファイルレコードの sys_id (「OAuth プロファイルの指定 」を参照)。

値は OAuth プロファイルレコードで設定されているため、パラメーターを使用して権限許可タイプとスコープを設定する必要はありません。パラメーターを使用しない場合は、GlideOAuthClientRequest API メソッド *`setScope`* および *`setGrantType`* を使用できます。追加情報については、「setScope 」と「setGrantType 」を参照してください。

OAuth 2.0 クライアント認証での秘密キー JWT サポート

OAuth 2.0 クライアント認証の JWT サポートをサポートします。

秘密キー JWT クライアント認証は、トークンエンドポイントを使用するときにクライアントが承認サーバーに対する認証に使用できる認証方法です。

この認証メカニズムでは、公開キーを登録し、そのキーを使用して JWT に署名したクライアントのみが認証できます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

JWT には、必須の要求値を含める必要があり、オプションの要求値を含めることができます。private_key_jwt認証用の JWT に必要な要求値の詳細については、OpenID Connect コア ドキュメントの「クライアント認証」セクションを参照してください。

> **注:**
> 認証トークンは、client_assertionパラメーターの値として送信する必要があります。**client_assertion_type** パラメーターの値は、urn:ietf:params:oauth:client-assertion-type:jwt-bearer である必要があります。
>
> JWT トークンを使用した OAuth 2.0 クライアント認証に必要なプラグイン:
>
> - **OAuth 2.0 (com.snc.platform.security.oauth):**このプラグインは、新規およびアップグレードされたインスタンスで有効です。インスタンス上でプラグインがアクティブでない場合は、アクティブ化することができます。
> - 統合 - マルチプロバイダー シングル サインオン インストーラー **(com.snc.integration.sso.msoi.installer):**OIDC ベースのシングル サインオンのユースケース用。

次の目的で、秘密キー JWT を使用した OAuth 2.0 クライアント認証を使用できます。

- OIDC ベースの Single Sign-on
- 送信 OAuth 統合

OIDC ベースの SSO 用の秘密キー JWT の構成

OIDC ベースの SSO 統合用に秘密鍵 JWT を構成します。

始める前に
必要なロール：admin

OIDC ベースの SSO に秘密鍵 JWT を選択する前に、次のタスクを実行する必要があります。

- Java KeyStore 証明書のアップロード:JWT クライアント認証を有効にするために使用する JKS 証明書をインスタンスに添付します。
- JWT 署名キーの構成:Java KeyStore (JKS) 証明書にアサインする JWT 署名キーを作成します。

  > **注:**
  > JWT キーの一部としてヘッダーに **X.509** 証明書 **SHA-1** サムプリント **int (x5t)** を追加する場合は、フォームを構成し、[**X.509** 証明書 **SHA-1** サムプリント **int (x5t)]** フィールドを追加する必要があります。

- JWT 署名キーを使用した JWT プロバイダーの作成:JWT プロバイダーを ServiceNow インスタンスに追加します。

OIDC ベースの ID プロバイダーの JWT キーを含めるには、次のことを行う必要があります。

- Integration - **Multiple Provider Single Sign-On Installer** プラグイン (com.snc.integration.sso.msoi.installer) をインストールします。
- 複数プロバイダー **SSO** のプロパティを有効にします。詳細については、「複数プロバイダー SSO のプロパティ、テーブル、およびスクリプト」を参照してください。
- OIDC ID プロバイダーを作成します。詳細については、「Single Sign-on (SSO) 用の OpenID Connect (OIDC) 構成の作成」を参照してください。

自動翻訳

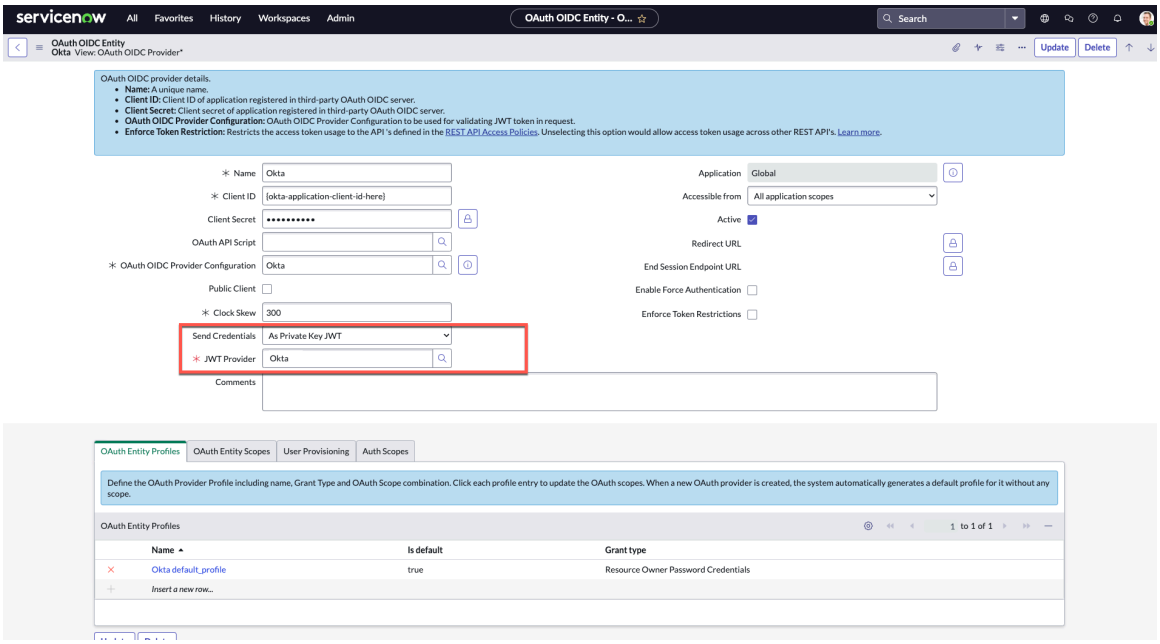
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. 移動先 すべて > システム **OAuth** > アプリケーションレジストリー.
2. 作成した OIDC ID プロバイダーを選択します。
3. フォームの上部で、 構成 > フォームデザイン.

> **注:**
> OIDC ベースの ID プロバイダー認証要求に秘密キー JWT を使用するには、[資格情報を送信] フィールドと **[JWT** プロバイダー] フィールドをフォームに追加する必要があります。

4. [資格情報の送信] に [秘密キーとして **JWT**] を選択します。
5. **JWT** プロバイダーを選択します。



ユーザーが認証されると、認証ページにOkta経由でログインするオプションが表示されます。

送信 **OAuth** の秘密キー **JWT** の構成

送信 OAuth 統合用の秘密鍵 JWT を構成します。

始める前に

必要なロール：admin

送信 OAuth 統合用の秘密キー JWT を設定する前に、次のタスクを実行する必要があります。

- Java KeyStore 証明書のアップロード:JWT クライアント認証を有効にするために使用する JKS 証明書をインスタンスに添付します。
- JWT 署名キーの構成:Java KeyStore (JKS) 証明書にアサインする JWT 署名キーを作成します。

> **注:**
> JWT キーの一部としてヘッダーに **X.509** 証明書 **SHA-1** サムプリント **int (x5t)** を追加する場合は、フォームを構成し、[**X.509** 証明書 **SHA-1** サムプリント **int (x5t)]** フィールドを追加する必要があります。

- JWT 署名キーを使用した JWT プロバイダーの作成:JWT プロバイダーを ServiceNow インスタンスに追加します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

手順

1. 移動先 すべて > システム **OAuth** > アプリケーションレジストリー をクリックし、[新規] をクリックします。
2. インターセプターページで、[サードパーティ **OAuth** プロバイダーに接続します] をクリックし、フォームに入力します。

注:
送信 OAuth 認証要求に秘密キー JWT を使用するには、[資格情報を送信] フィールドと **[JWT** プロバイダー] フィールドをフォームに追加する必要があります。

フィールド	説明
名前	サードパーティ OAuth 接続のための一意の名前
クライアント ID	サードパーティの OAuth サーバーに登録されているアプリケーションのクライアント ID。
クライアント シークレット	サードパーティの OAuth サーバーに登録されているアプリケーションのクライアントシークレット
OAuth API スクリプト	外部 OAuth プロバイダーへの要求および応答のカスタマイズに使用されるスクリプト
ロゴ URL	OAuth アプリケーションのロゴの URL
デフォルトの権限許可タイプ	次を選択します。 クライアント資格情報: どちらもアクセストークンを取得するために使用されるクライアント**ID**とクライアントシークレット。このメソッドはリフレッシュトークンを提供しません。
リフレッシュトークンの有効期間	リフレッシュトークンが有効になる時間 (秒) デフォルトの時間は 86,400,000 秒です。
公開クライアント	パブリッククライアントが認証に PKCE を要求できるようにします。 注: PKCE が有効になっている場合、*`Default Grant type`*として使用できるのは認証コードのみです。
コメント	OAuth アプリに関するコメントを追加します。
アプリケーション	このレコードを含むアプリケーションとスコープです。
アクセス可能	すべてのアプリケーションスコープから、またはこのスコープからのみアプリにアクセスできるようにします。
アクティブ	チェックボックスをオンにすると、アプリがアクティブになります。
認証 URL	OAuth 認証コードのエンドポイント
トークン URL	OAuth サーバートークンエンドポイント
トークン失効 URL	OAuth サーバートークン失効エンドポイント

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
リダイレクト URL	OAuth コールバックエンドポイント空白のままにすると、インスタンスによってエントリが自動生成されます。
相互認証を有効にします	トークンの要求と取り消しに相互認証を使用するチェックボックス。この機能では、相互認証プロファイルを指定する必要があります。
資格情報の送信	選択: 秘密キー **JWT** として
JWT プロバイダー	JWT プロバイダーの詳細。ルックアップを使用して JWT プロバイダーを選択できます。

プライベート JWT キー認証に使用できる OAuth プロバイダータイプのレコードがアプリケーションレジストリ [oauth_entity] テーブルに作成されます。

パスワードの複雑さの要件

ServiceNow® インスタンスのパスワードは複雑さの要件を満たす必要があります。

探索

パスワードの複雑さの要件の機能とビジネス価値について学びます。

有効化

パスワードの複雑さの要件を有効にする方法を理解します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

構成

パスワードの複雑さの要件を設定します。

参照:サポートされていないパスワード文字

サポートされていないパスワード文字について理解してください。

自動翻訳

パスワードの複雑さの要件の詳細

ServiceNow® インスタンスのパスワードは複雑さの要件を満たす必要があります。

パスワードの複雑さに関する要件ポリシー設定は、パスワードが一連の強力なパスワードガイドラインを満たす必要があるかどうかを決定します。

パスワードの複雑さの要件は、パスワードが変更または作成されるときに適用されます。

パスワードの複雑さの要件は、以下の条件に基づいて遵守され、機能します。

- *glide.apply.password_policy.on_login* プロパティが有効になっている場合、ログイン時にユーザーに対してパスワードポリシーチェックが適用されます。ログイン時に、ユーザーはパスワードポリシーに従い、インスタンスのパスワードを変更する必要があります。
- パスワードポリシー要件は、現代の言語すべての文字を含む Basic Multilingual Plane (BMP) に基づいています。ServiceNow インスタンスには、約 10,000 文字の BMP が付属しています。
- 許容される BMP 内のパスワードをインスタンスに設定できます。これらの BMP に準拠しないパスワードは許可されません。

必要に応じて、少なくとも 90 日ごとにパスワードを変更するように要求できます。

要件と禁止文字

安全なネットワーク環境を有効にするには、文字、数字、および記号を組み合わせた強力なパスワードを使用する必要があります。このような組み合わせを使用することで、権限のないユーザーが主に手動または自動化された方法で脆弱なパスワードを推測することが起こりにくくなります。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

インスタンスのパスワードは、次の要件を満たしている必要があります。

- 最小 8 文字
- 最大 100 文字
- 小文字と大文字を含む
- 特殊文字を含む
- 数字を含む

次のような、一連のよくある不適切なパスワードを禁止できます。

- 「123456」、「qwerty」、「!@#$%^」、「aaaaa」などの予測可能な繰り返しシーケンス
- 従業員名またはユーザー名
- 関連するブランド名または製品名
- 本社、都市、国などの場所名
- 会社固有の内部用語または略語
- 絵文字

> **注:**
> パスワードに使用できないユーザー、ブランド、または会社固有の文字は、[パスワードポリシー] または [パスワードを除外] ページで設定できます。

インスタンスでのパスワードポリシーの有効化

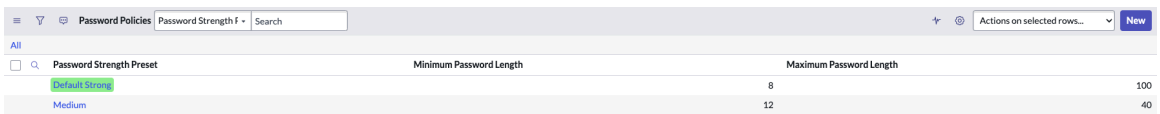
ログイン時にパスワードポリシーコントロールを実装します。パスワードがパスワードポリシー基準を満たしていない場合、ユーザーにパスワードの変更を強制します。

始める前に
必要なロール：admin

このタスクについて
Password Policy プラグイン (com.glide.password_policy) はデフォルトで有効になっています。ユーザーがパスワードを変更またはリセットすると、ポリシーが有効になります。
[パスワード強度のプリセット] フィールドは、自動的に [デフォルトは強] に設定されます。新しい基準を追加する場合は、次の手順を実行できます。

`ValidatePasswordStronger` インストレーションイグジットまたはパスワードリセット資格情報ストアの *`pwd_cred_store`* プロパティを使用してインスタンスをカスタマイズした場合は、パスワードポリシーのプロパティを参照して、インスタンスのパスワードポリシーを実装する方法を確認してください。

> **注:**
> 次のように、インスタンスのアクティブなパスワードポリシーが強調表示されます。



パスワードポリシーを変更するには、次の場所に移動します。 すべて > パスワードリセット > 資格情報ストアで、資格情報を選択し、[パスワードポリシー] フィールドを必要なポリシー入力に変更します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. 移動先 すべて > パスワードのポリシー > パスワードのポリシー.
2. [新規] をクリックします。
   [パスワードポリシー] フォームが表示されます。
3. パスワードポリシーの [名前] を指定します。
4. [パスワードポリシー基準] セクションで、[パスワード強度のプリセット] フィールドから次のいずれかのプリセットを選択します。

   注:
   パスワードポリシーは、選択したプリセットに基づいて適用されます。

5. フォームの残りのフィールドに入力します。

[パスワードのポリシー] フォーム

フィールド	説明
パスワードの最小長	パスワードの最小長。このオプションは、[詳細] を除くすべてのプリセットで表示されます。このフィールドは最低 8 ～ 10 文字に設定します。
パスワードの最大長	パスワードの最大長。このオプションは、[詳細] を除くすべてのプリセットで表示されます。このフィールドは最大 100 文字に設定します。
大文字の最小文字数	パスワードに使用する大文字の最小数 (0 ～ 10)。
小文字の最小数	パスワードに使用する小文字の最小数 (0 ～ 10)。
数値の最小文字数	パスワードに使用する数字の最小数 (0 ～ 10)。
特殊文字の最小文字数	パスワードに使用する特殊文字の最小数 (0 ～ 10)。
含まれる特殊文字	区切り文字のない特殊文字セットの使用を制限できるようにします。 たとえば「$,!」と入力すると、ユーザーはパスワードの特殊文字として「$」と「!」のみを使用できます。他の特殊文字は使用できません。他の特殊文字を含むパスワードは使用できません。
除外される特殊文字	区切り文字のない特殊文字セットの使用を制限できるようにします。 たとえば「@$!」と入力すると、ユーザーはパスワードの特殊文字として「@」、「$」、「!」を使用できなくなります。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	注: このオプション は、*glide.password_policy.use_excluded_specia* プロパティが有効になっている場合に使用できます。
ユーザーデータを禁止	認証関連のユーザーデータを禁止するオプション
シーケンス長のしきい値	パスワードのシーケンス長
繰り返しの長さのしきい値	パスワードの繰り返しの長さ。 注: ○ シーケンス長しきい値と繰り返し長さのしきい値は、どちらも最大 8 文字を設定できます。これらのフィールドを使用すると、「123456」、「qwerty」、「!@#$%^」、「aaaaa」などの予測可能な繰り返しシーケンスを持つ脆弱なパスワードの組み合わせを制限できます。 ○ [パスワード強度のプリセット] が [デフォルトは強] に設定されている場合、シーケンス長のしきい値と繰り返し長さのしきい値は、両方とも 4 文字に設定されます。
パスワードをテスト	このフィールドに実際のパスワードを指定します。

6. [パスワードをテスト] をクリックします。
7. パスワードが有効であることを確認したら、[送信] をクリックしてパスワードを送信します。

注:
送信する前に必ずパスワードをテストしてください。

パスワードポリシープロパティ

パスワードポリシープロパティを使用すると、パスワードポリシーを管理し、リストパスワードを除外し、ログイン時にパスワードポリシーを適用できます。

移動先 パスワードのポリシー > プロパティ をクリックして、パスワードポリシーのプロパティを表示および編集します。

プロパティ	説明
glide.enable.password_policy	インスタンスでパスワードポリシーを有効にします。ユーザーがパスワードを変更またはリセットすると、ポリシーが有効になります。このプロパティは自動的に **true** に設定されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

プロパティ	説明
	注: • *ValidatePasswordStronger* インストレーションイグジットまたは Password Reset 資格情報ストア [pwd_cred_store] を介してインスタンスがカスタマイズされている場合は、このプロパティを作成してシステムプロパティに追加する必要があります。 • Orlando より前のリリースでは、*ValidatePasswordStronger* インストレーションイグジットを使用してインスタンスをカスタマイズした場合、パスワードポリシーを機能させるにはパスワードポリシープロパティを作成する必要がありました。 • Orlando リリース以降は、インストレーションイグジットのカスタマイズはありません。パスワードポリシープロパティはデフォルトで機能します。これらのプロパティは手動でオフにすることができます。
glide.enable.blacklist_password	特定のパスワードの使用を禁止します。管理者は、[除外されたパスワード] テーブルにパスワードを挿入できます。このプロパティは自動的に **true** に設定されます。
glide.apply.password_policy.on_login	既存のパスワードが現在のパスワードポリシーに準拠していない場合、次回ログイン時にユーザーにパスワードの変更を強制します。 このプロパティは自動的に **false** に設定されます。値を **true** に設定すると、ログイン時にパスワードポリシーが適用されます。 注: このプロパティを有効にすると、新しいパスワードポリシーに準拠していないユーザーが大量にパスワードの変更を強制される可能性があります。
glide.password_policy.user_excluded_special_char	パスワードポリシー] フォームで [除外される特殊文字] オプションの使用を有効化します。
glide.validate.sys_user.password.field	管理者が sys_user フォームまたはリストビューを編集するときに、パスワードポリシーに対してユーザーパスワードを検証できるようにします。
glide.password.policy..generate.password.field.disabled	sys_user フォームのパスワード設定ポップアップで、[パスワード] フィールドを無効にします。
glide.user.show.password.field	sys_user フォームの [パスワード] フィールドを有効にします。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

プロパティ	説明
glide.password_policy.debug	パスワードポリシーのデバッグログを有効にします。

パスワード・ポリシーの構成

パスワードポリシー基準により、パスワードを保護して、パスワードの複雑さの最小要件を遵守することができます。

始める前に

必要なロール：admin

このタスクについて

Password Policy (com.glide.password_policy) プラグインはデフォルトで有効になっています。ユーザーがパスワードを変更またはリセットすると、ポリシーが有効になります。ValidatePasswordStronger インストレーションイグジットまたは Password Reset 資格情報ストア [pwd_cred_store] を使用してインスタンスをカスタマイズした場合は、「パスワードポリシープロパティ」を参照してください。

手順

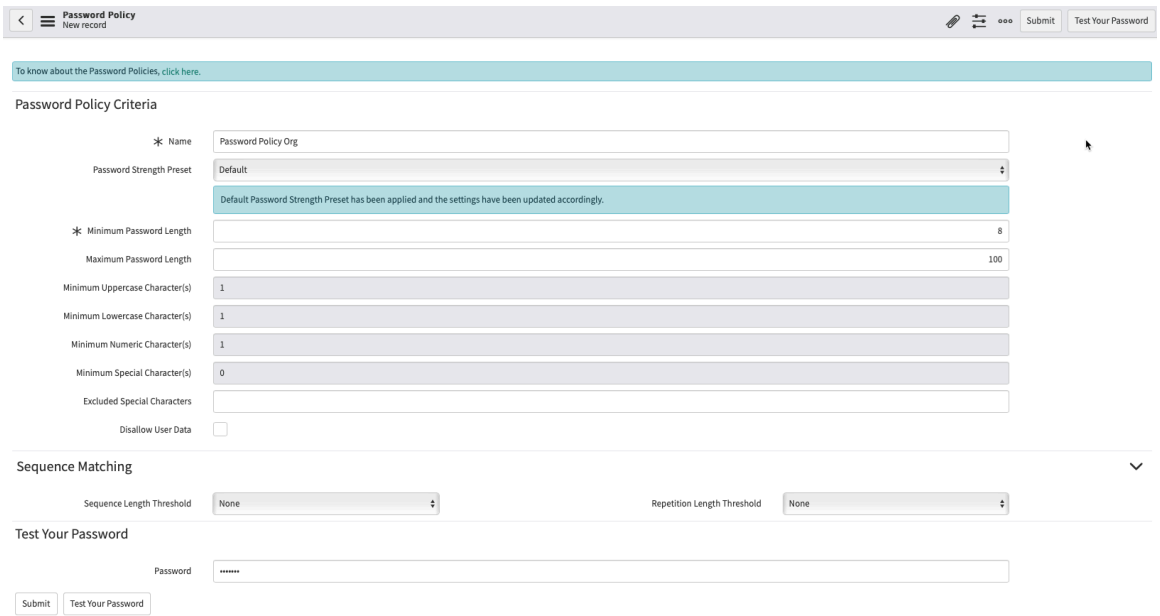
1. 移動先 すべて > パスワードのポリシー > パスワードのポリシー.

> **注:**
> [デフォルトは強] のプリセットが、デフォルトのパスワード受け入れ条件として有効になっています。場合により、新しい基準を追加する場合は、次の手順を実行できます。

2. [新規] をクリックします。

[パスワードポリシー] の [新規レコード] ページには次のセクションがあります。これらを指定してパスワードを設定します。

- パスワードポリシー基準
- シーケンスマッチング
- パスワードをテスト



3. パスワードポリシーの [名前] を指定します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

4. [パスワードポリシー基準] セクションで、[パスワード強度のプリセット] からプリセットを選択します。選択可能なプリセットは次のとおりです。

パスワード強度のプリセットとその説明

パスワード強度のプリセット	説明
デフォルト	[デフォルト] を選択すると、必要なパスワード文字を次のように自動入力します。 ○ 大文字を最低 1 文字 ○ 小文字を最低 1 文字 ○ 数字を最低 1 文字
中	[中] を選択すると、次の条件に基づいて、必要なパスワード文字を自動入力します。 ○ 大文字を最低 1 文字 ○ 小文字を最低 1 文字 ○ 数字を最低 1 文字 ○ 特殊文字を最低 1 文字
高	[高] を選択すると、パスワード文字を次のように自動入力します。 ○ 大文字を最低 1 文字 ○ 小文字を最低 2 文字 ○ 数字を最低 1 文字 ○ 特殊文字を最低 3 文字
デフォルトは強	[デフォルトは強] を選択すると、次の条件に基づいて、必要なパスワード文字を自動入力します。 ○ 大文字を最低 1 文字 ○ 小文字を最低 1 文字 ○ 数字を最低 1 文字 ○ 特殊文字を最低 1 文字
カスタム	[カスタム] を選択すると、次の条件に基づいて、必要なパスワード文字を自動入力します。 ○ 大文字を最低 1 文字 ○ 小文字を最低 1 文字 ○ 数字を最低 1 文字 ○ 特殊文字を最低 1 文字 表示されるパスワードポリシーのスクリプトをカスタマイズすることもできます。
詳細	[詳細] を選択すると、[パスワードのルールスクリプト] と [パスワードの安全性スクリプト]

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

パスワード強度のプリセット	説明
	が表示されます。要件に基づいて、これらのスクリプトをカスタマイズできます。

注:
パスワードポリシーは、選択したプリセットに基づいて適用されます。

5. テーブルに記載されているフィールドを次のように指定します。

[パスワードのポリシー] フォーム

フィールド	説明
パスワードの最小長	パスワードの最小長。このオプションは、[詳細] を除くすべてのプリセットで表示されます。 **注:** [パスワードの最小長] は必須フィールドであり、最低でも 8 ～ 10 文字に設定することをお勧めします。
パスワードの最大長	パスワードの最大長。このオプションは、[詳細] を除くすべてのプリセットで表示されます。 **注:** [パスワードの最大長] はオプションのフィールドです。最大 100 文字に設定することをお勧めします。
大文字の最小文字数	パスワードに使用する大文字の最小数 (0 ～ 10)。
小文字の最小数	パスワードに使用する小文字の最小数 (0 ～ 10)。
数値の最小文字数	パスワードに使用する数字の最小数 (0 ～ 10)。
特殊文字の最小文字数	パスワードに使用する特殊文字の最小数 (0 ～ 10)。
含まれる特殊文字	区切り文字のない特殊文字セットの使用を制限できるようにします。たとえば「$,!」と入力すると、ユーザーはパスワードの特殊文字として「$」と「!」のみを使用できます。他の特殊文字は使用できず、他の特殊文字を含むパスワードは使用できません。
除外される特殊文字	区切り文字のない特殊文字セットの使用を制限できるようにします。たとえば「@$!」と入力すると、ユーザーはパスワードの特殊文字として「@」、「$」、「!」を使用できなくなります。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	注: このオプションは、glide.password_policy.use_excluded_special_char プロパティが有効になっている場合に使用できます。
ユーザーデータを禁止	ユーザーデータを禁止することが可能です。

6. [シーケンスマッチング] セクションで、[シーケンス長のしきい値] と [繰り返しの長さのしきい値] を指定します。

   注:
   - シーケンス長しきい値と繰り返し長さのしきい値は、どちらも最大 8 文字を設定できます。これらのフィールドを使用すると、「123456」、「qwerty」、「!@#$%^」、「aaaaa」などの予測可能な繰り返しシーケンスを持つ脆弱なパスワードの組み合わせを制限できます。
   - [デフォルトは強] の場合、シーケンス長のしきい値と繰り返し長さのしきい値は、両方とも 4 文字で選択されます。

7. [パスワードをテスト] セクションで、パスワードを指定します。
8. [パスワードをテスト] をクリックします。
9. パスワードが有効であれば、[送信] をクリックしてパスワードを送信します。

   注:
   送信する前に必ずパスワードをテストしてください。

自動翻訳

ユーザーのパスワードの構成

設定されているパスワードポリシーに基づいて、インスタンスのユーザーのパスワードを設定します。

始める前に

最初のログイン用のパスワードを設定するために作成されたユーザー。詳細については、「ユーザーの作成」を参照してください。

ユーザーフォームの [パスワード] フィールドに直接入力するには、[**sys_user** フォームでのパスワードの表示を有効にする **(Enable to show the password field on the sys_user Form)**] (glide.user.show.password.field) を有効にします。プロパティの詳細については、「パスワードポリシープロパティ」を参照してください。

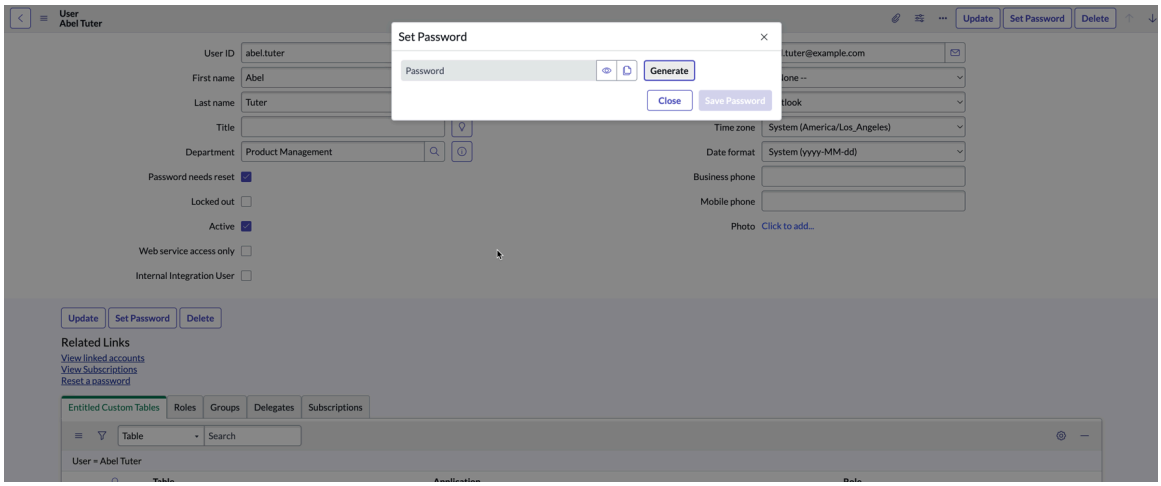
必要なロール：管理者

手順

1. 移動先 すべて > ユーザー管理 > ユーザー.
2. [ユーザー (Users)] ページのリストからユーザーを選択します。
3. パスワードポリシーに基づいてパスワードを設定するには、[パスワードを設定] をクリックします。

   [パスワードを設定] ポップアップが表示されます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



4. [パスワードを設定] で、次の操作を実行します。

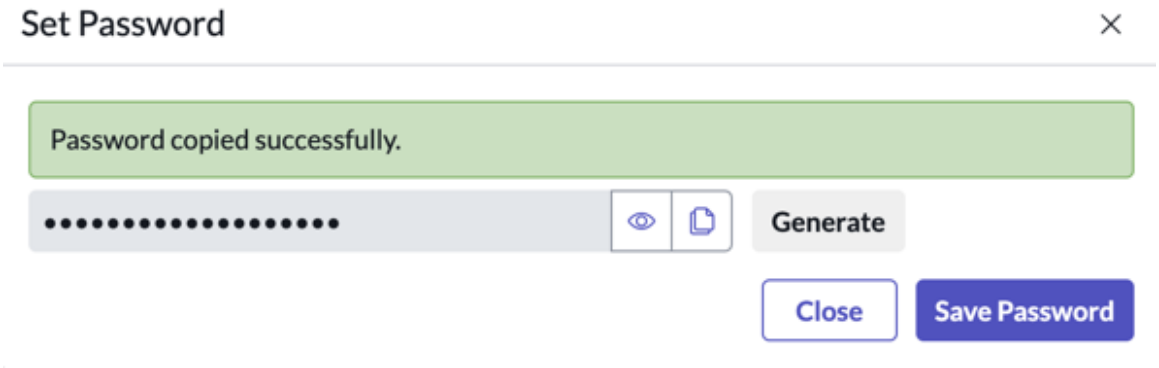
a. [生成] をクリックしてパスワードを生成します。

b. [表示] アイコンをクリックしてパスワードを表示します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

c. [コピー] アイコンをクリックして、ユーザーと共有するパスワードをコピーします。



5. [パスワードを保存] をクリックします。

   ユーザーにパスワードが設定されます。また、[パスワード休止 (Password needs rest)] チェックボックスが自動的に有効になります。

   ユーザーは、最初のログイン時は同じパスワードを使用し、ログインしたら管理者が設定したパスワードポリシーに従ってパスワードを変更する必要があります。

インスタンスのパスワードポリシーによるパスワードの除外

[除外されたパスワード] テーブルにパスワードを追加して、インスタンスのユーザーが特定のパスワードを使用できないようにします。

始める前に
必要なロール：admin

このタスクについて
必要に応じていくつでもパスワードを禁止できます。いくつかの例を次に示します。

- 「123456」、「qwerty」、「!@#$%^」、「aaaaa」などの予測可能な繰り返しシーケンス
- 従業員名またはユーザー名
- 関連するブランド名または製品名
- 本社、都市、国などの場所名
- 会社固有の内部用語または略語
- 絵文字

手順

1. 移動先 すべて > パスワードのポリシー > 除外されたパスワード.
2. 除外リストにパスワードを追加するには、[新規] をクリックしてパスワードを入力します。
3. 移動先 パスワードのポリシー > 除外リストの管理 でユーザーのパスワードを管理し、ユーザーがインスタンスに対して間違ったパスワードを使用しないようにします。

   [除外リストの管理] には、一般的に使用される約 5000 のパスワードがあります。

サポートされていないパスワード文字

サポートされていないパスワード文字があります。ServiceNow パスワードの複雑さの要件に基づいて、ユーザーはこれらの文字を使用できなくなります。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

安全なネットワーク環境を有効にするには、文字、数字、および記号を組み合わせた強力なパスワードを使用する必要があります。このような組み合わせを使用することで、権限のないユーザーが主に手動または自動化された方法で脆弱なパスワードを推測することが起こりにくくなります。

- パスワードポリシー要件は、現代の言語すべての文字を含む Basic Multilingual Plane (BMP) に基づいています。ServiceNow インスタンスには、約 10,000 文字の BMP が付属しています。
- この許容 BMP 内のパスワード文字は、インスタンスに設定できます。この BMP 内にないパスワード文字は許可されません。

注:
パスワードに使用できないユーザーまたは会社固有の文字は、除外パスワードリストで設定できます。

パスワードポリシーのプロパティの詳細については、「パスワードポリシープロパティ」を参照してください。

ServiceNow インスタンスへの自己登録

外部ユーザーの自己登録を使用して、大量の外部ユーザーをインスタンスにオンボーディングします。この機能によって本人確認を強化して、カスタマーエクスペリエンスを向上させて一般的に使用される登録フローをサポートします。

詳細を読む

自己登録の機能とビジネス価値について説明します。

アクティブ化

外部自己登録をアクティブ化する方法を把握します。

構成

有効化

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自己登録を設定します。

自己登録のプロパティについて把握します。

自己登録の詳細

外部ユーザーの自己登録を使用して、大量の外部ユーザーをインスタンスにオンボーディングします。この機能によって本人確認を強化して、カスタマーエクスペリエンスを向上させて一般的に使用される登録フローをサポートします。

外部ユーザー自己登録によって、大規模なユーザーグループが管理者のサポートなしで ServiceNow アプリに登録できます。たとえば、大学の構内に駐車場を必要とする学生グループが多い大学では、学生自身がキャンパスパーキングアプリに登録できます。各学生には駐車場に固有の制限付きの特権セットが付与されて、自動登録プロセスが完了します。このシステムは各学生に固有の駐車番号を生成して、駐車スペースを確保できるようにします。

自己登録フローは、カスタム ServiceNow アプリ、この場合はキャンパスパーキングアプリで構成されます。必要なテーブルでアプリを構成後、管理者は登録前フロー、フィールドマッピング、登録後マッピング、キャプチャ、ロールマッピング、登録後フローを含む登録を構成します。

外部ユーザー自己登録の有効化

admin ロールを持っている場合は、External User Registration プラグイン (com.snc.external_user_self_registration) をアクティブ化することができます。

始める前に

必要なロール：admin

このタスクについて

手順

1. 移動先 すべて > システムアプリケーション > 利用可能なすべてのアプリケーション > すべて.
2. フィルター基準と検索バーを使用してプラグインを検索します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

名前または ID でプラグインを検索できます。プラグインが見つからない場合は、ServiceNow 担当者から要求する必要があります。

3. [インストール] を選択して、[プラグインをアクティブにする] ダイアログボックスで、[アクティブ化] をクリックします。

> **注:**
> ドメイン分離と代理管理者がインスタンスで有効になっている場合、管理ユーザーはグローバルドメインに含まれている必要があります。それ以外の場合、次のエラーが表示されます： 別の操作が実行されているため、アプリケーションのインストールは利用できません：<プラグイン名> のプラグインの有効化。

自己登録の外部ロール

不注意で外部ユーザーにアクセスさせないように、すべての外部ユーザーに snc_external ロールを割り当てることができます。

自己登録する外部ユーザーには、最小限の権限を持つ snc_external ロールを割り当てる必要があります。snc_external ロールは、ユーザーが組織の外部にあり、リソースへのアクセス権を持たないことを示します。ただし、ACL を通じて snc_external ロールか、または snc_external ロールを継承する追加ロールに対して明示的に許可された場合は例外です。

デフォルトでは、snc_external ロールを持つユーザーはアクセスできません。

- 外部とマークされていない Scripted REST APIs リソース。
- snc_external ロールまたは公開ロールを継承するロールがないテーブル。
- snc_external ロールまたは snc_external ロールを継承するロールを持たないプロセッサーや UI ページなど、レコードタイプ以外のリソース。
- Now Intelligence ダッシュボード

Paris リリース以降、snc_external ロールの明示的な割り当てを強制するには、exclude-list プロパティを有効にする必要があります。プロパティの有効化については、「外部ユーザーに対する今後の内部ロールの割り当てを防止する」を参照してください。

外部ユーザーのユーザー登録構成の構成

ユーザー登録構成レコードを作成して、外部ユーザーのオンボーディングプロセスをカスタムの ServiceNow アプリケーションにブートストラップします。このフォームは、自己登録プロセスを通じて外部ユーザーをガイドします。

始める前に

- 必要なロール：管理者
- 外部ユーザー自己登録の有効化

手順

1. 移動先 すべて > 外部ユーザー自己登録 > ユーザー登録構成 をクリックし、「 新規」をクリックします。
2. フォームのフィールドに入力します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

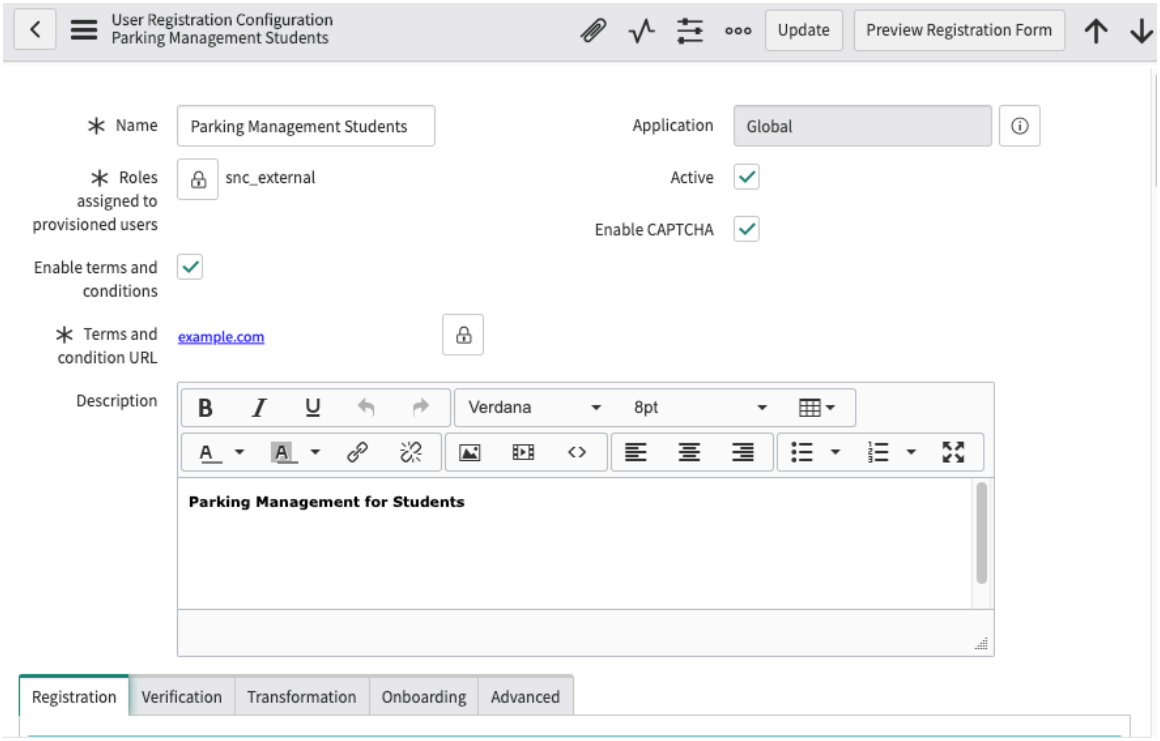
[ユーザー登録構成] フォーム

フィールド	説明
名前	登録フォームの名前。たとえば、学生の駐車場登録の場合は [学生駐車場管理 (Parking Management Students)] などになります。
プロビジョニングされたユーザーへアサインされたロール	プロビジョニングされたユーザーへアサインされたロール。指定されたロールは、snc_external ロールに拡張するか、このロールを含んでいる必要があります。指定されたロールは、snc_external ロールにすることもできます。外部ユーザーの場合は、外部ユーザーを記録するために各ロールに snc_external が必要です。事前設定されたロールがある場合は、ロールのロックを解除してユーザーを検索する際に、そのロールにアクセスできる必要があります。
契約条件を有効化	登録ページに契約条件の URL を追加するオプション
契約条件 URL	登録フォームの契約条件が記載されている公開の URL。このフィールドは、[契約条件を有効化] が選択されている場合にのみ表示されます。
説明	登録フォームの説明。このフィールドは、構成を保存または送信するときにのみ表示されます。このフィールドには、登録フォームに関する情報を追加できます。 **注:** 説明は、ユーザー登録構成を保存または更新した後にのみ追加できます。
アプリケーション	このレコードを含んでいるアプリケーションです。アプリケーションは自動的に [グローバル] に設定されます。
有効	ユーザー登録構成をアクティブにするオプション。このオプションがデフォルトで選択されています。
CAPTCHA を有効化	登録フォームに CAPTCHA を追加するオプション。デフォルトの CAPTCHA プロバイダーは Google reCAPTCHA です。 **注:** ユーザー登録の CAPTCHA を有効にするには、「外部ユーザー自己登録のための Google reCAPTCHA の設定」の手順に従います。

3. [送信] をクリックします。
デフォルト設定のユーザー登録構成が作成されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



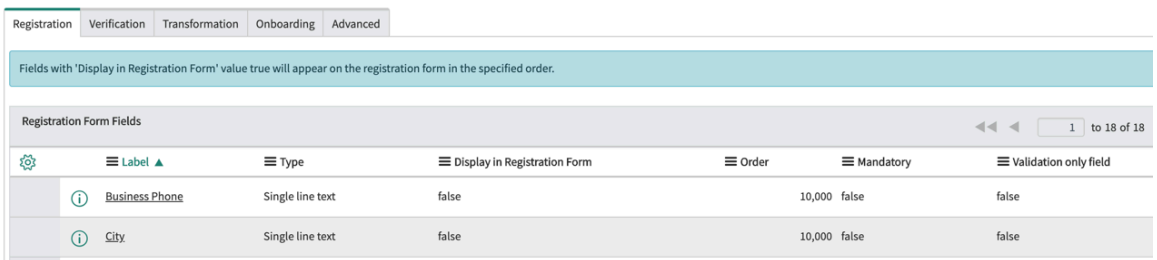
4. オプション: フィールドとその表示順序を表示するように [登録] タブを設定します。

登録フォームフィールド

列	説明
登録フォームに表示	表示したいフィールドをすべて True に設定します。
順番	フォームにフィールドを表示する順序番号を設定します。
必須	必須にしたいフィールドをすべて True に設定します。
検証のみのフィールド	検証にのみ使用するフィールドを設定します。たとえば、登録コードなどです。

デフォルトのフォームフィールドを表示することも、カスタムフォームフィールドを登録フォームに追加することもできます。詳細については、「デフォルトの登録フォームのフィールド」を参照してください。

[登録] タブ



カスタムの登録フォームのフィールドを追加することもできます。詳細については、「カスタム登録フォームフィールドの追加」を参照してください。

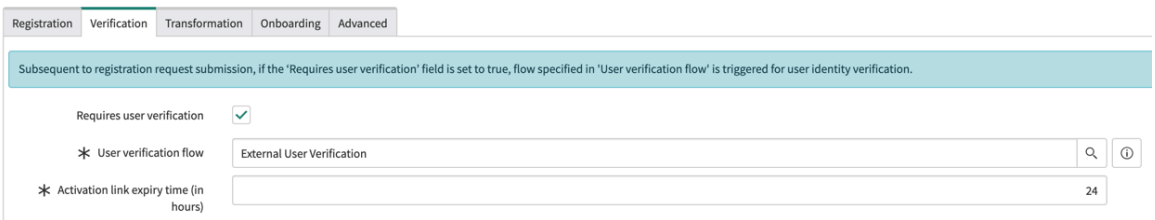
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

5. オプション: [検証] タブを設定して、登録されたユーザーの本人確認を行います。ユーザー検証フローがトリガーされると、ユーザーの登録済みメールアドレスにアクティベーションリンクが送信されます。

[検証] タブのフィールド

フィールド	説明
ユーザー検証を要求	ユーザー登録後に実行されるユーザー検証サブフローをトリガーするオプション。このサブフローはユーザーの本人確認用です。
ユーザー検証フロー	ユーザーの本人確認に使用されるサブフロー。サブフローは、ユーザー検証を有効にした場合にのみトリガーされます。 (Optional) 外部ユーザーの検証 サブフローはデフォルトで利用可能です。フローデザイナーにデフォルトのサブフローのコピーを作成し、要件に応じて変更できます。詳細については、「Flow Designer」を参照してください。 注: 新しいタブで外部ユーザーの検証 サブフローをプレビューするには、次のショートカットを使用します。 ○ Macintosh：Command + クリック ○ Windows：Control + クリック
アクティベーションリンクの有効期限 (時間)	アクティベーションリンクが期限切れになるまでの時間数。デフォルト値は 24 です。

[検証] タブ

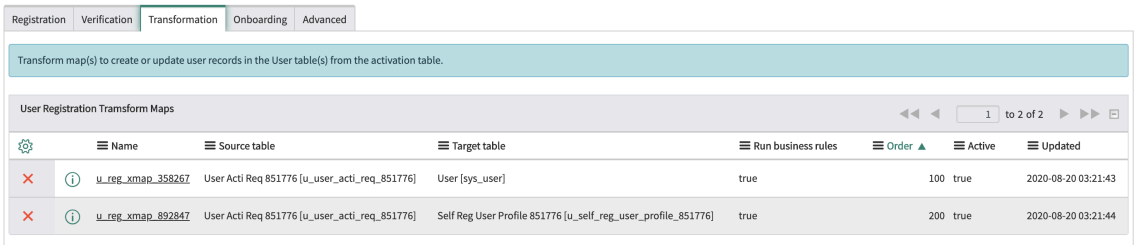


6. オプション: [変換] タブを設定し、自己登録ユーザーとアクティブ化されたユーザーをマップします。
登録済みユーザーをユーザーアクティビティ要求 [number] テーブルから自己登録ユーザー [number] テーブルに自動的にマップする変換マップ (u_reg_xmap_[number]) は 2 種類あります。デフォルトの変換マップのコピーを作成し、そのマップを要件に応じて変更できます。詳細については、「変換マップ」を参照してください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

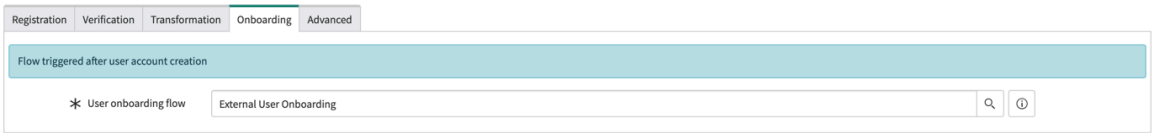
[変換] タブ



7. オンボーディングがアクティブ化されているユーザーのサブフローをトリガーするように、[オンボーディング] タブを設定します。
デフォルトの外部ユーザーのオンボーディング サブフローは、パスワードをリセットするためのリンクを記載したメールをユーザーに送信します。デフォルトのサブフローのコピーを作成し、要件に応じて変更できます。

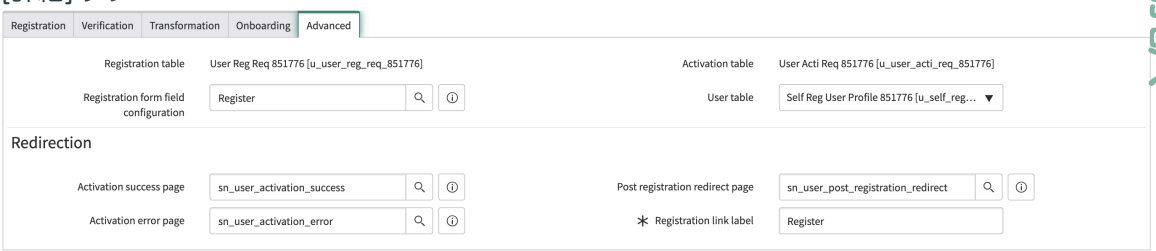
   注:
   外部ユーザーのオンボーディングサブフローは、パスワードをリセットするためのリンクを記載したメールをユーザーに送信します。

   [オンボーディング] タブ



8. オプション: 登録フォームのユーザーテーブルとリダイレクトページをマップするように、[詳細] タブを設定します。

   [詳細] タブ



[詳細] タブ

フィールド	説明
登録テーブル	登録フォーム情報が保存されるテーブルの名前
登録フォームフィールド構成	レコードプロデューサーの登録フォームに関連付けられたレコード
アクティベーションテーブル	ユーザーのアクティベーションに使用されるテーブルのラベルと名前。アクティベーションテーブルには、検証が完了したユーザーのレコードが含まれています。
ユーザーテーブル	ユーザープロファイルテーブルのラベルと名前
アクティベーション成功ページ	アクティベーションが成功した後にユーザーがリダイレクトされるページ

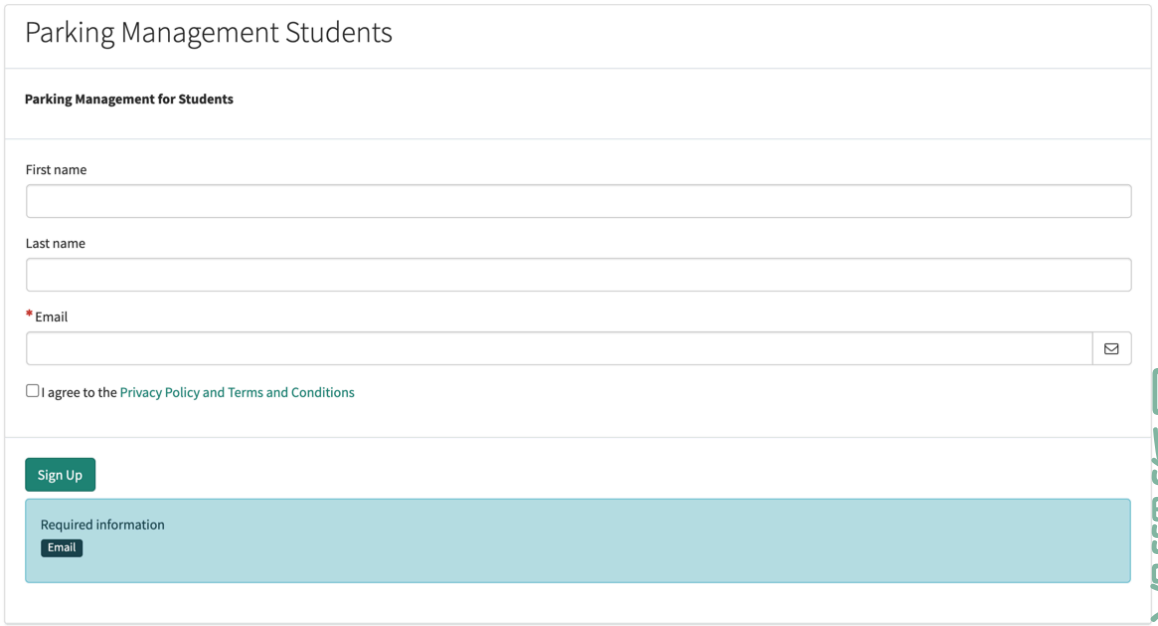
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
アクティベーションエラーページ	アクティベーションに失敗したときにユーザーがリダイレクトされるページ。
登録後リダイレクトページ	登録後にユーザーがリダイレクトされるページ。
登録リンクラベル	サービスポータルからの登録に使用されるボタン名。デフォルト値は [登録] です。

ユーザー登録構成の変更中またはすべての変更が完了した後、[登録フォームのプレビュー] ボタンを使用して登録フォームの変更をプレビューできます。

登録フォームのプレビュー



外部ユーザー自己登録のための **Google reCAPTCHA** の設定

Google reCAPTCHA サービスを使用するには、Google に API キーペアを要求し、関連するシステムプロパティを設定する必要があります。

始める前に

- https://www.google.com/recaptcha で Google から API キーペア (サイトキーとシークレット) を要求します。
- 必要なロール：管理者

このタスクについて

手順

1. 移動先 すべて > システムプロパティ > すべてのプロパティ.
2. 次のプロパティを検索し、値を設定します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

プロパティ	値
glide.user.registration.google.recaptcha.secret	シークレットは、アプリケーションと reCAPTCHA サーバー間の通信を許可します。 タイプ：password2
glide.user.registration.google.recaptcha.site_key	登録ページで reCAPTCHA サービスを呼び出すために使用されるサイトキー タイプ：文字列
glide.user.registration.captcha.widget	Captcha ウィジェットの Sys_ID タイプ：文字列

デフォルトの登録フォームのフィールド

デフォルトの登録フォームフィールドを使用することも、カスタムの登録フォームフィールドを作成することもできます。

登録フォームフィールド

デフォルトでは、次のフォームフィールドが登録フォームに追加されます。

フィールドラベル	タイプ
勤務先電話	1 行テキスト
市区町村	1 行テキスト
国	選択ボックス
EDU ステータス スタッフ、学生、訪問者を区別するために使用されます。 **注:** このフィールドは、登録フォームが教育機関用である場合に便利です。	選択ボックス
メール	メール
名	1 行テキスト
性別	1 行テキスト
自宅電話	1 行テキスト
言語	選択ボックス
姓	1 行テキスト
ミドルネーム	1 行テキスト

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールドラベル	タイプ
携帯	1 行テキスト
名前	1 行テキスト
プリフィックス ユーザーの敬称。たとえば「様」、「先生」などです。	選択ボックス
都道府県	1 行テキスト
番地	ワイドな 1 行テキスト
役職	選択ボックス
郵便番号	1 行テキスト

注:
デフォルトの登録フォームフィールドは削除できません。

カスタム登録フォームフィールドの追加

ユーザー自己登録フォームにカスタムフィールドを追加できます。

始める前に
必要なロール：管理者

手順

1. 移動先 すべて > 外部ユーザー自己登録 > ユーザー登録構成.
2. 必要なユーザー登録構成のレコードを開きます。
3. [登録フォームフィールド] セクションの末尾に移動し、 [新規行を挿入...] をクリックします。
4. [ラベル] 列の下にフィールド名を入力し、チェックマークをクリックします。
   デフォルト値を用いて新しい行が追加されます。要件に基づいてカスタム登録フォームフィールドを設定できます。

登録フォームフィールドの列

列	説明
ラベル	登録フォームに表示されるフィールド名。
タイプ	ユーザーインターフェイス要素のタイプ。サポートされているタイプは次のとおりです。 ○ 1 行テキスト ○ メール ○ 日付 ○ 日付/時刻 ○ はい/いいえ ○ ワイドな 1 行テキスト ○ 複数選択肢 ○ 選択ボックス

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

列	説明
登録フォームに表示	登録フォームにフィールドを表示するオプション
順番	フォームフィールドが登録フォームに表示される順序。順序値が最も小さいフィールドが最初に表示され、順序値が最も大きいフィールドが最後に表示されます。デフォルト値は 10,000 です。
必須	登録フォームでフィールドを必須にするオプション
検証のみのフィールド	検証目的に限定してフィールドを使用するオプション。たとえば、登録コードなどです。true に設定すると、このフィールドはユーザーテーブル (sys_user) に保存されません。

5. 変更を保存または更新します。

の外部ユーザー自己登録の有効化 サービスポータル

サービスポータル によって外部ユーザーが ServiceNow アプリに登録できるようにします。

始める前に

必要なロール：admin

手順

1. 移動先 すべて > サービスポータル > ポータル.
2. ポータルレコードを開きます。
3. フォームの [外部ユーザー登録構成] フィールドに入力します。

   ユーザー登録構成を選択します。
4. [更新] をクリックします。

タスクの結果

ログインウィジェットには、以前に構成した登録フォームへのリンクが含まれています。

自己登録の外部ロール

不注意で外部ユーザーにアクセスさせないように、すべての外部ユーザーに snc_external ロールを割り当てることができます。

自己登録する外部ユーザーには、最小限の権限を持つ snc_external ロールを割り当てる必要があります。snc_external ロールは、ユーザーが組織の外部にあり、リソースへのアクセス権を持たないことを示します。ただし、ACL を通じて snc_external ロールか、または snc_external ロールを継承する追加ロールに対して明示的に許可された場合は例外です。

デフォルトでは、snc_external ロールを持つユーザーはアクセスできません。

- 外部とマークされていない Scripted REST APIs リソース。
- snc_external ロールまたは公開ロールを継承するロールがないテーブル。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- snc_external ロールまたは snc_external ロールを継承するロールを持たないプロセッサーや UI ページなど、レコードタイプ以外のリソース。
- Now Intelligence ダッシュボード

Paris リリース以降、snc_external ロールの明示的な割り当てを強制するには、exclude-list プロパティを有効にする必要があります。プロパティの有効化については、「外部ユーザーに対する今後の内部ロールの割り当てを防止する」を参照してください。

ユーザー自己登録要求の確認

サービスポータル からユーザーを登録すると、ユーザーレコードが登録要求モジュールに追加されます。サービスポータル で正常に登録されたユーザーのリストを表示できます。

始める前に
必要なロール：管理者

手順

1. 移動先 すべて > 外部ユーザー自己登録 > 登録要求.
   ユーザーレコードリストが表示されます。
2. (オプション) 個々のユーザーレコードを確認し、要件に従って変更します。たとえば、ユーザーレコードフォームのステータスを [処理待ち] から [処理済み] に変更できます。

トークンベースの認証 (ユーザーログイン)

ユーザーがトークンベースの認証を使用してネットワークにアクセスするためのセキュリティメカニズムを強化します。

時間制限付き認証

ダイジェストトークン認証

ダイジェストトークン認証は、暗号化されていない HTTP ヘッダー内のユーザー資格情報とダイジェストトークンを渡します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

トークンベースの認証は、ユーザーが自分のIDを確認し、代わりに一意のアクセストークンを受け取ることができるプロトコルです。

これは、ユーザーがネットワークにアクセスするためのセキュリティメカニズムを強化するのに役立ちます。

時間制限付き認証

ServiceNow インスタンスの時間制限付き認証をサポートします。

探索

時間制限付き認証の機能とビジネス価値について説明します。

アクティブ化

時間制限付き認証をアクティブ化する方法を理解します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

チュートリアル:時間制限付き認証

Zero Trust Access のプロパティについて説明します。

自動翻訳

時間制限付き認証の探索

ServiceNow インスタンスの時間制限付き認証をサポートします。

注:
時間制限付き認証は、ServiceNow インスタンスに固有であり、ユーザー向けのカスタマイズされたリンクは ServiceNow 内でのみ作成できます。

管理者は、ServiceNow インスタンスでリンクベースの認証を設定できます。設定されたリンクはメールまたは SMS で共有でき、ユーザーはそれらのリンクを使用してインスタンスにログインできます。

この認証スキームを使用したインスタンスへのログインは、ServiceNow インスタンスで構成された適応認証ポリシーを介してコントロールされます。

時間ベースの認証を使用すると、次のことができます。

- 管理者は、有効期限まで使用できるリンクベースの認証を設定できます。
- アプリケーションチームは、公開されたスクリプト可能 API を使用して、特定の構成アイテムのリンクとともに使用するノンスを取得できます。リンクの生成はアプリケーションチームが行います。
- アプリケーションチームは、リンクを生成し、既存のチャネルを介してユーザーに送信できます。
- リンクを持つユーザーは、構成の一部として指定された有効期限内であれば、インスタンスに 1 回ログインできます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- 管理者は、認証スキーム用に低い権限のロールを設定できます。
- 管理者は、TLA リンクを使用した認証の第 2 要素として、認証スキーム用の MFA を強制できます。

時間制限付き認証のアクティブ化

Integration - Multiple Provider Single Sign-On Installer プラグインを使用して時間制限付き認証をアクティブ化します。

始める前に
必要なロール：admin

> **注:**
> 時間制限付き認証は、ServiceNow インスタンスに固有であり、ユーザー向けのカスタマイズされたリンクは ServiceNow 内でのみ作成できます。

手順

1. 移動先 すべて > システムアプリケーション > 利用可能なすべてのアプリケーション > すべて.
2. フィルター基準と検索バーを使用して Time Limited Authentication (*com.snc.authenticate.time_limited_authentication*) プラグインを検索します。

   名前または ID でプラグインを検索できます。プラグインが見つからない場合は、ServiceNow 担当者から要求する必要があります。
3. [インストール] を選択して、[プラグインをアクティブにする] ダイアログボックスで、[アクティブ化] をクリックします。

   > **注:**
   > ドメイン分離と代理管理者がインスタンスで有効になっている場合、管理ユーザーはグローバルドメインに含まれている必要があります。それ以外の場合、次のエラーが表示されます： 別の操作が実行されているため、アプリケーションのインストールは利用できません：<プラグイン名> のプラグインの有効化。

SMS を使用した時間制限付き認証 **- Twilio** チュートリアル

Twilio を使用して、SMS などの MFA 要素で時間制限付き認証を設定します。

始める前に
必要なロール：admin

次のプラグインが必要です。

- *com.snc.authenticate.time_limited_authentication* (時間制限付き認証)
- *com.snc.authentication.sms_mfa* (SMS を使用したマルチファクター認証)

> **注:**
> 時間制限付き認証 (TLA) は、ServiceNow インスタンスに固有であり、ユーザー向けのカスタマイズされたリンクは ServiceNow 内でのみ作成できます。

提供されているチュートリアルの指示により、管理者は、第 2 要素 (MFA) として SMS を使用したリンクベースのログインを、特定のロールを持つユーザーに提供できます。

構成が正常に完了すると、リンクが生成され、通知 (メール/SMS) チャネルを介してリンクがユーザーと共有されます。リンクをクリックすると、ユーザーロール (構成) に基づいてメールまたは SMS 要素に送信される OTP を指定するように求められます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

注:

- TLA には常に MFA が続き、管理者は TLA ログインのために適応認証を使用して MFA を有効にする必要があります。適応認証を使用して MFA を構成する方法の詳細については、「MFA (マルチファクター認証) コンテキスト」を参照してください。
- TLA は、権限が制限されているユーザー用に使用する必要があります。

手順

1. Twilio 構成の作成

a. Twilio テストアカウントを作成します。詳細については、次を参照してください： Twilio .

b. 移動先 すべて > 通知 > 管理 > **Twilio** ダイレクト構成.

c. アカウント **SID** と認証トークン (Twilioから作成) を入力し、レコードを保存します。

注:
独自のプロバイダー構成を作成し、それを TLA に使用できます。この例では、Twilio です。MFA プロバイダー構成の作成方法の詳細については、「MFA プロバイダーの構成」を参照してください。

2. 時間制限付き認証 (TLA) レコードを構成して有効にします。

a. 移動先 すべて > 時間制限付き認証構成レコード をクリックし、「 新規」をクリックします。

b. フォームの各フィールドに入力します。

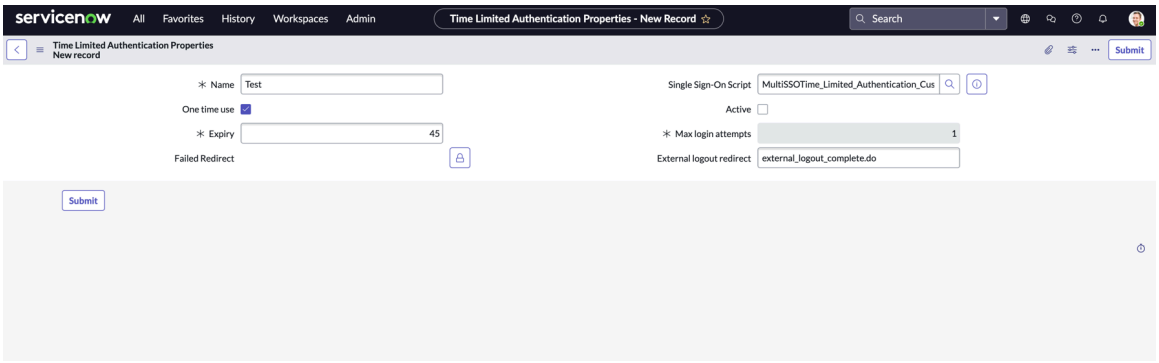
時間制限付き認証プロパティ

フィールド	説明
名前	レコードの名前。
1 回のみ使用	TLA リンクを 1 回使用できるようにします。
有効期限	リンクの有効期限を秒単位で指定します。デフォルトは 45 分です。
リダイレクトに失敗しました	認証に失敗した後にユーザーをリダイレクトする URL を入力します。
Single Sign-on スクリプト	使用する SSO スクリプトの詳細。
有効	構成を有効にするオプション。
最大ログイン試行回数	生成された TLA リンクで許可されるログイン試行回数を指定します。**[1** 回のみ使用] チェックボックスをオフにして、最大試行回数を指定します。
外部のログアウトのリダイレクト	ログアウト後にユーザーをリダイレクトする URL を入力します。

c. [送信] をクリックします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



d. 移動先 すべて > マルチプロバイダー **SSO** > 管理 > プロパティ をクリックし、[**Enable multiple provider SSO**] プロパティを有効にして **[Save]** を選択します。

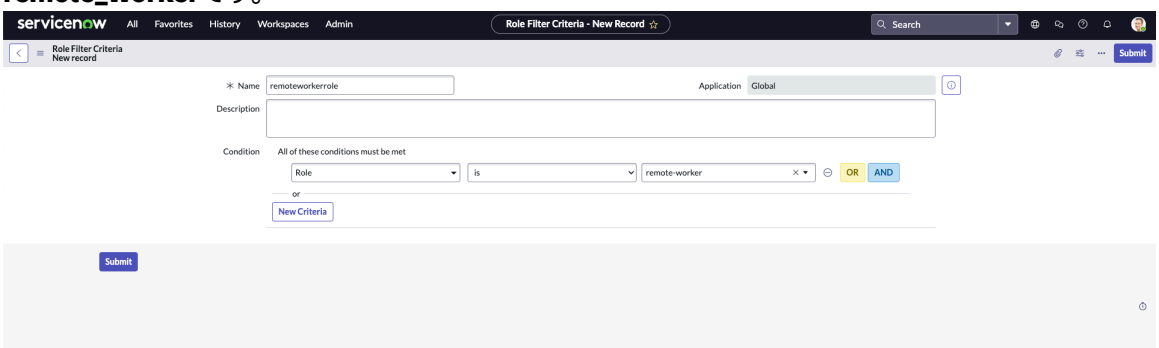
3. 認証後のコンテキストポリシーを使用して、特定のユーザーペルソナにのみ TLA を許可します。

a. [ロール] に移動し、ロールを作成します。例：remote_worker。

b. 有効なメール ID と携帯電話番号を持つユーザーを作成します。ユーザーの作成方法については、「ユーザーの作成」を参照してください。

c. ユーザーにユーザーロールをアサインします。ユーザーにロールを割り当てる方法については、「 ユーザーへのロールの割り当て」を参照してください。

d. ロールフィルター基準を作成するには、次の場所に移動します すべて > 適応認証 > ロールフィルター基準、新しいフィルターを作成します リモートワーカー ロールと条件 ロールは **remote_worker**です。

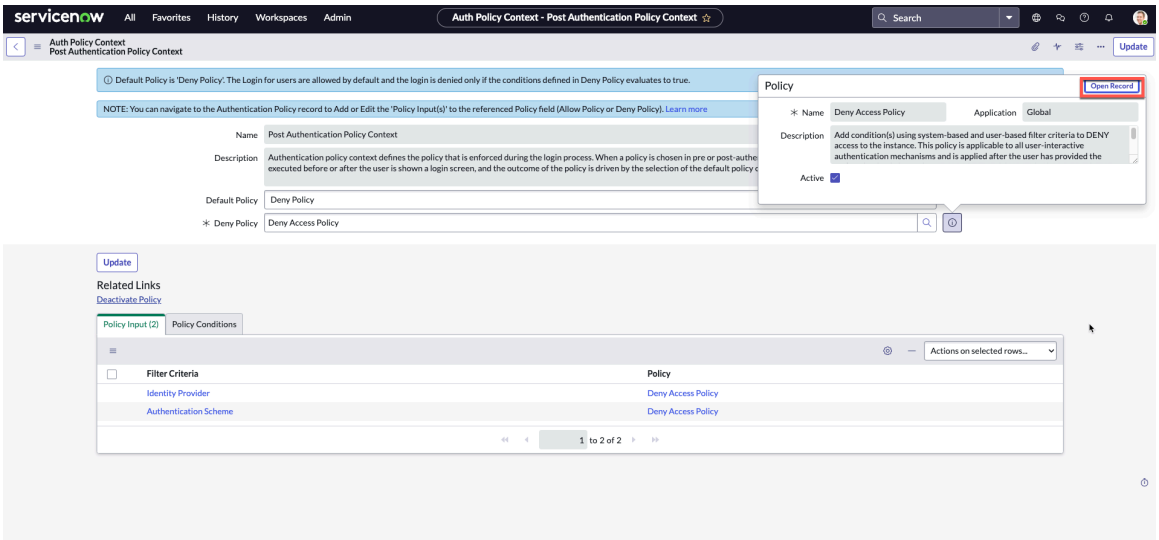


e. IdP およびロールフィルター基準に基づく拒否ポリシーコンテキストに基づいてポリシー条件を追加するには、次に移動します。 すべて > 適応認証 > 認証後のコンテキスト.

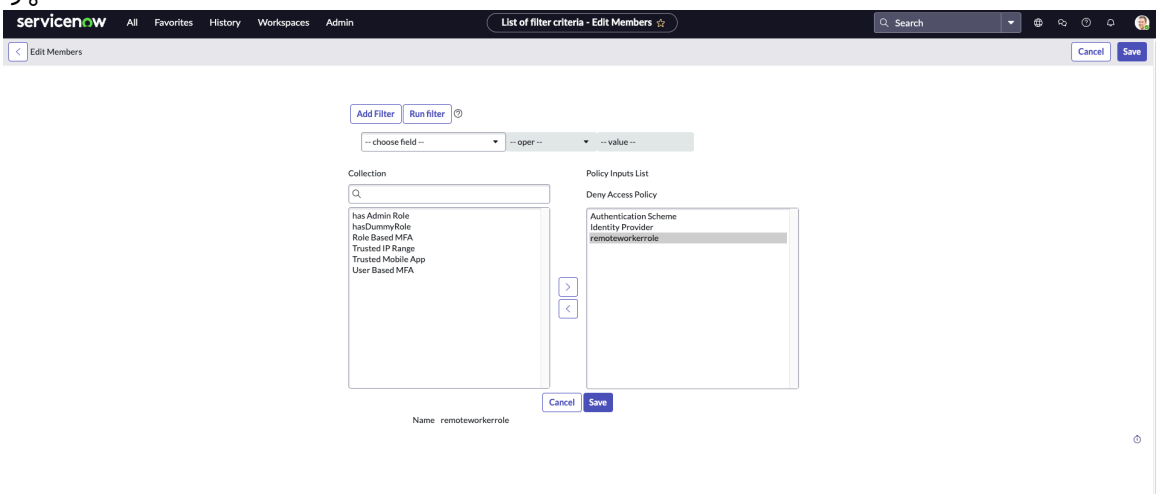
f. 情報アイコンをクリックして、レコードを開きます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



g. [ポリシーの入力] で [編集] をクリックし、ロール (remoteworkerrole) を追加して、保存します。



h. [ポリシー条件] で、ポリシー入力の条件を追加し、レコードを送信します。

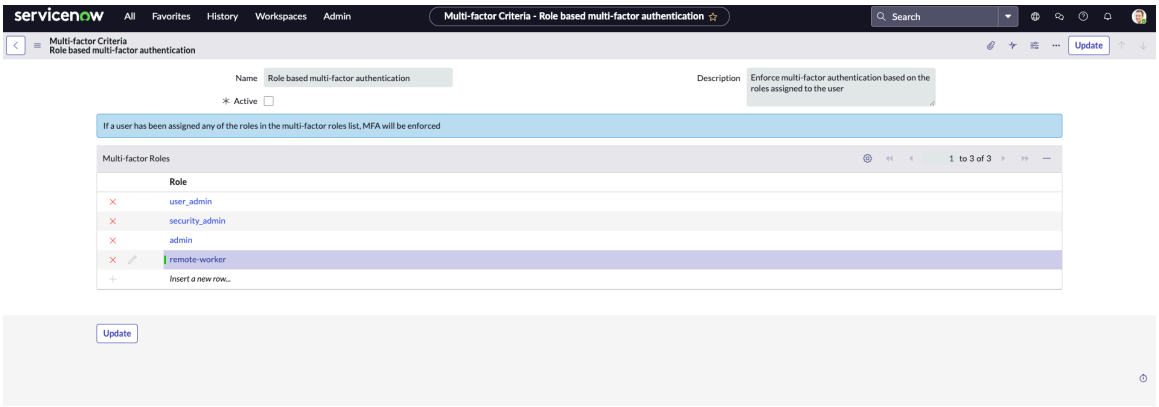
4. ステップアップ認証ポリシー - MFA コンテキストを構成します。

a. 移動先 すべて > マルチファクター基準.

b. [ロールベースのマルチファクター認証 **(Role-based multi-factor authentication)]** を選択し、[マルチファクターロール] セクションでロールを追加し、更新します。この例では **remote_worker** です。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

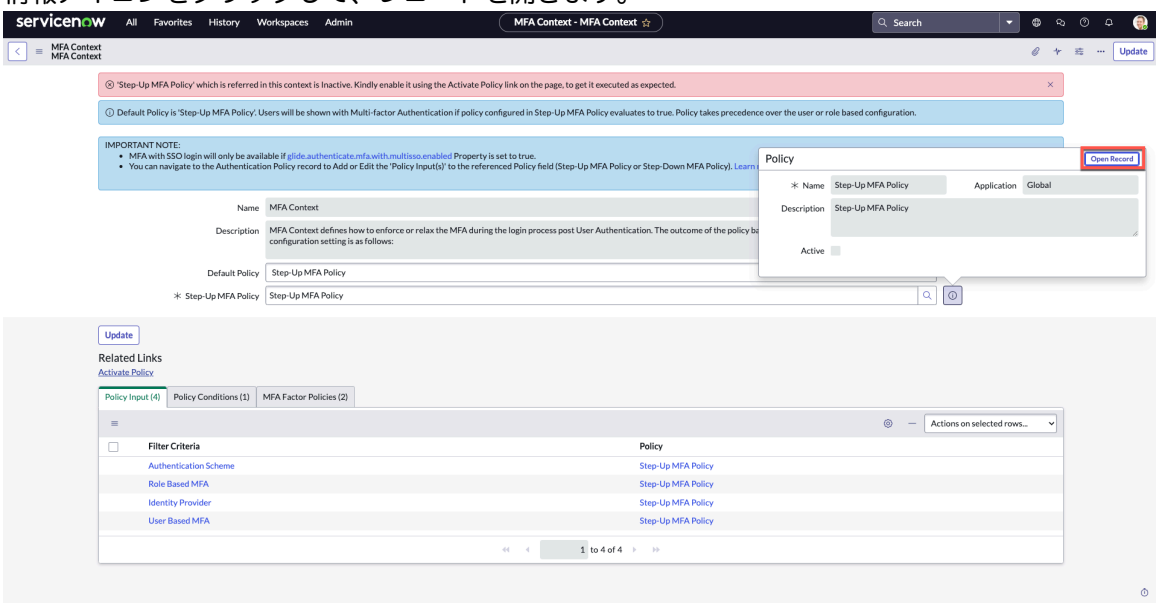


c. 移動先 すべて > 適応認証 > **MFA** コンテキスト.

d. 次のことを確認してください。

- [デフォルトポリシー] フィールドが [ステップアップ **MFA** ポリシー] になっている
- ステップアップ MFA ポリシーがステップアップ **MFA** ポリシーになっている

e. 情報アイコンをクリックして、レコードを開きます。



f. [ステップアップ MFA ポリシー] フォームの [ポリシーの入力] で、[編集] をクリックします。

g. ロールベースのマルチファクター認証をリストに追加し、保存します。この例では **remoteworkerrole**です。

h. [ポリシー条件] で、[ロールベースまたはユーザーベースの **MFA** 設定が **true** の場合は **MFA** を強制する **(Enforce MFA if Role based or User based MFA settings are true)]** をクリックします。

i. [ロールベースまたはユーザーベースの MFA 設定が true の場合は MFA を強制する (Enforce MFA if Role based or User based MFA settings are true)] ページで、 [ロールベースの **MFA]** が **true** になっていることを確認します。

5. MFA 要素ポリシーとして SMS を使用するように MFA を強制します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

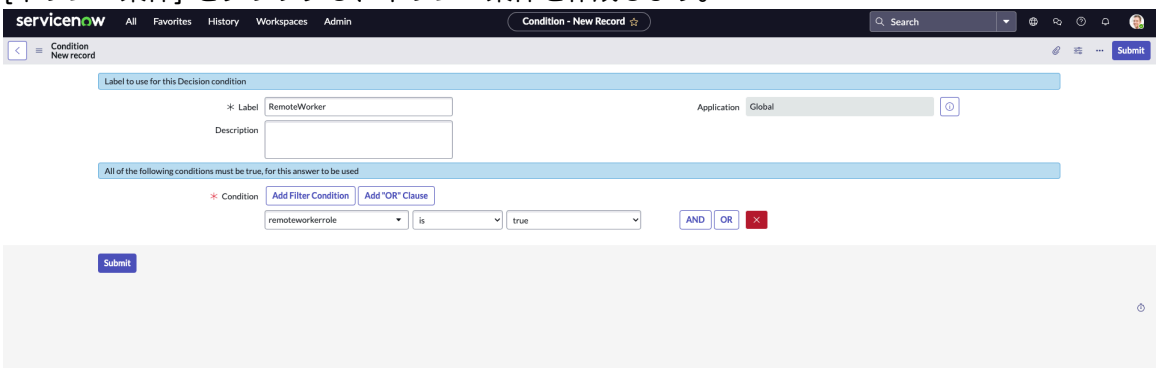
自動翻訳

a. 移動先 すべて > 適応認証 > **MFA** コンテキスト.

b. [MFA コンテキスト] ページで、**[MFA** 要素ポリシー] をクリックし、**[SMS OTP** を **MFA** 要素ポリシーとして表示 **(Display SMS OTP as an MFA Factor Policy)]** をクリックします。

c. [ポリシーの入力] で [編集] をクリックし、**remoteworkerrole** を追加します。

d. [ポリシー条件] をクリックし、ポリシー条件を作成します。



e. [送信] をクリックします。

TLA リンクが生成され、**remoteworkerole** がロールとしてアサインされたユーザーと共有されます。このリンクは、インスタンスにログインするための第 2 要素として SMS コードを使用するように昇格されます。

6. 他の必要なプロパティを有効にします。

a. 移動先 すべて > マルチファクター認証 > プロパティ.

b. 次のチェックボックスをオンにします。
- マルチファクター認証を有効にする
- **SSO** を使用したマルチファクター認証を有効にする

c. レコードを保存します。

d. 移動先 すべて > 適応認証 > 認証ポリシー > プロパティ.

e. [認証ポリシーの有効化 **(Enable Authentication Policy)]** チェックボックスをオンにします。

f. レコードを保存します。

7. TLA リンクの生成 – 例

a. 移動先 すべて > システム定義 > スクリプト – バックグラウンド.

b. ユーザーの sysid と構成 ID を指定して、次の API を使用します。
`var tla=new global.TimeLimitedAuthentication(); gs.info(tla.generateNonce("user_sysid", "config1_sys_id","IAR2"));`

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

> **注:**
> ソース (IAR2) は必須パラメーターではありません。

c. クエリーパラメーターは次のように返されます。
`nonce=VCeinfboDt0M&glide_sso_id=b3277f1b44351110f8779b5a2d9909f3&user=3b0277d344351110f8779b5`

d. 次の形式で URL を作成します。
`https://<instance-url> /login_with_sso.do?uri=<encoded url>&`
`nonce=2olIQSxdgkjs&glide_sso_id=0c15bf09c3711110c5ec4e483c40dd7a&user=62826bf03710200044e0bfc8`

8. URL をクリックすると、次のようなログイン用の MFA 画面が表示されます。

ダイジェストトークン認証

ダイジェストトークン認証は、暗号化されていない HTTP ヘッダー内のユーザー資格情報とダイジェストトークンを渡します。

探索	構成
ダイジェストトークン認証の機能とビジネス価値について学びます。	ダイジェストトークン認証の構成方法を理解します。

自動翻訳

ダイジェストトークン認証の詳細

インスタンスは HTTP ヘッダー値を読み取り、ダイジェストトークンの計算されたハッシュ値と比較します。計算されたハッシュ値がダイジェストトークン値と一致する場合、インスタンスはユーザーテーブルで一致する値を検索します。ユーザーテーブルに一致する値がある場合、インスタンスはユーザーが事前認証されているとみなしてログインさせます。

ダイジェストトークン認証は暗号化されていない単純な HTTP ヘッダーよりも安全です。暗号化されていない HTTP ヘッダーを誤って (または意図的に) 変更すると異なるハッシュ値が生成されるか

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

らです。ハッシュ値が一致しない場合、インスタンスは要求されたインスタンスへのユーザー アクセスを拒否します。これにより、ユーザーは別のユーザーの資格情報でログインできなくなります。

ダイジェストリンクの有効期限の詳細については、この KB 記事 を参照してください。

注:
時間制限付き認証 (TLA) を使用して、時間ベースの有効期限リンクを設定します。詳細については、「時間制限付き認証」を参照してください。

統合の要件

ダイジェストトークン認証の統合には次のものが必要です。

- Web サーバー
- ローカルネットワークでユーザーを事前認証する SiteMinder または別の Single Sign-on アプリケーション
- 次のいずれかの形式でユーザー資格情報をターゲットインスタンスに渡す Web ページまたはポータル
  - HTTP ヘッダー
  - URL パラメーター
  - cookie
- 次のいずれかのエンコード技術を使用して、ダイジェストトークンを作成してターゲットインスタンスに渡す Web ページまたはポータル
  - SHA1
  - MD5
  - SHA 256 (推奨)

複数プロバイダー **Single Sign-on (SSO)** のダイジェストプロパティの設定

ダイジェストインストレーションイグジットスクリプトを有効にした後、複数プロバイダー SSO のプロパティを設定します。

始める前に
必要なロール：管理者

このタスクについて
複数プロバイダー Single Sign-on を使用していない場合は、標準の Single Sign-on プロパティを設定します。

手順

1. 移動先 すべて > マルチプロバイダー **SSO** > **ID** プロバイダー.
2. [ダイジェストプロパティ] フォームのフィールドに入力します。

オプション	説明
名前	ダイジェストトークンの名前を入力します。
ユーザー	受信ヘッダーの一致するデータを含む [sys_user] フィールドを入力します。
HTTP ダイジェストヘッダー名	生成された HTTP ヘッダーを入力します。 例：DE_USER

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

オプション	説明
HTTP ヘッダー名	作成したダイジェストトークン用に生成した HTTP ヘッダーを入力します。例：SM_USER。
秘密のパスフレーズ	ダイジェストキーのエンコードに使用する秘密キーを入力します。例： 32 文字以上。
[SSO リダイレクトに失敗しました] フィールド	認証に失敗した後にユーザーをリダイレクトする URL を入力します。
外部のログアウトのリダイレクト	ログアウト後にユーザーをリダイレクトする URL を入力します。
Single Sign-on スクリプト	**[MultiSSO_DigestedToken]** を選択します。

3. [更新] をクリックします。
4. ダイジェストトークンをデフォルトで true に設定します。
   デフォルトを true に設定すると、SSO に関連付けられたシステムのデフォルトダイジェストトークンレコードが上書きされます。最初の複数プロバイダー SSO 関連の IdP レコードがアクティブ化すると、複数プロバイダー SSO に関連付けられたレコードのみが使用されます。

   ダイジェストプロパティテーブルに存在するダイジェストトークンレコードは、IdP の Sys_ID を追加することによって個別に呼び出すことができます。たとえば、次の認証 URL のダイジェストトークンレコードです。https://<instance_name>.service-now.com/login_with_sso.do?glide_sso_id=<sys_id_of_Digest_token_record>&SM_USER=<user_name>&DE_USER=<digested_token>

ダイジェストトークンの実装例

ここでは、ダイジェストトークンの作成例をいくつか示します。

ダイジェスト認証の実装例

ダイジェスト構築のツール	秘密キーの値	ハッシュメソッド	例
Java	32 文字以上	SHA256	暗号化のためのサンプル Java ダイジェストアルゴリズム
C	sharedKey パラメーターの値	strEncryptionMethod パラメーターの値 (SHA256 または MD5)	サンプル C

暗号化のためのサンプル **Java** ダイジェストアルゴリズム

この Java アルゴリズムは、HTTP ヘッダーからダイジェストトークンを作成する方法を示しています。

このサンプルでは、以下を前提としています。

- Web サーバーは Java をサポート
- ハッシュ計算方法は SHA1
- 秘密キーの値は abc123
- 暗号化されていない HTTP ヘッダー名は user_name

別のハッシュ計算メカニズム (MD5 など) を使用するように Java コードを変更するか、秘密キー値または HTTP ヘッダー名を変更します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

```
public class DigestTest
{
   private static final String MAC_ALG = "HmacSHA256";
     fKey  = {32 or more characters};
   public byte[] getDigest(String acct) {
      try {
         byte[] bkey = fKey.getBytes();
         byte[] data = acct.getBytes();
         Mac mac = null;
         try {
            mac = Mac.getInstance(MAC_ALG);
            mac.init(new SecretKeySpec(bkey, MAC_ALG));
         } catch (Exception e) {
            e.printStackTrace();
         }
         byte[] sig = mac.doFinal(data);
         String signature = new String(sig);
         System.out.println("value:" + acct);
         System.out.println("digested value:  " + signature);
         return sig;
      } catch (IllegalStateException e) {
         e.printStackTrace();
      }
      return null;
   }
   public static void main(String[] args) {
      BASE64Encoder encoder = new BASE64Encoder();
      DigestTest test = new DigestTest();
      String userName = "user_name";
      System.out.println("base 64 digest username: " +
 encoder.encode(test.getDigest(userName)));
   }
}
```

自動翻訳

サンプル C

この C クラスは、3 つの入力パラメーターからダイジェストトークンを作成する方法を示しています。

- strEncryptionMethod – ハッシュ計算方法 (SHA1、SHA256、または MD5) をリスト
- message – ダイジェストトークンに変換する値をリスト
- sharedKey – 秘密キーをリスト

注:
ダイジェストトークンの生成には、SHA256 などのより強力で安全なハッシュアルゴリズムを使用します。

この例では、以下を前提としています。

- Web サーバーは C をサポート
- 他のコードがこのクラスを呼び出し、予想されるパラメーターを渡す

サンプルコード

```
private stringdigestData(string strEncryptionMethod , string message , string sharedKey ) {
        UnicodeEncoding myUnicodeEncoding  = new UnicodeEncoding ( ) ;
```

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

```
        byte [ ] messageBytes  = System. Text. Encoding. ASCII. GetBytes (message ) ;
        byte [ ] sharedKeyBytes  = System. Text. Encoding. ASCII. GetBytes (sharedKey ) ;
        byte [ ] hashedMessage ;

        string b64SHA1Message ;

         if (this. DEBUG ) {
           TextBoxMessage. Text = message ;
           TextBoxSecret. Text = sharedKey ; }

         switch ( (strEncryptionMethod ) )

        { case "SHA1" :

              HMACSHA1 hmacsha1  = new HMACSHA1 ( ) ;
              hmacsha1. Key = sharedKeyBytes ;
              hashedMessage  = hmacsha1. ComputeHash (messageBytes ) ;
              b64SHA1Message  = Convert. ToBase64String (hashedMessage ) ; if (this.
DEBUG ) TextBoxDigest. Text = Convert. ToString (hashedMessage ) ; break ;

           case "MD5" :

              HMACMD5 hmacmd5  = new HMACMD5 (sharedKeyBytes ) ;
              hashedMessage  = hmacmd5. ComputeHash (messageBytes ) ;
              b64SHA1Message  = Convert. ToBase64String (hashedMessage ) ; if (this.
DEBUG ) TextBoxDigest. Text = Convert. ToString (hashedMessage ) ; break ;

           default :

              b64SHA1Message  = "Unknown Encryption Method" ; break ;

        }


       TextBoxBase64. Text = b64SHA1Message ; return b64SHA1Message ;

     }
```

Zero Trust アクセス

ゼロトラストアクセス(ZTA)は、デフォルトで信頼されるユーザーまたはデバイスがないことを前提とするセキュリティモデルです。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

探索

ゼロトラストアクセスの機能と
ビジネス価値について学びます。

アクティブ化

ゼロトラストアクセスを有
効にする方法を理解します。

構成

Zero Trust アクセスを構成します 。

参照:プロパティ

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Zero Trust Access の探索

ゼロトラストアクセス(ZTA)は、デフォルトで信頼されるユーザーまたはデバイスがないことを前提とするセキュリティモデルです。

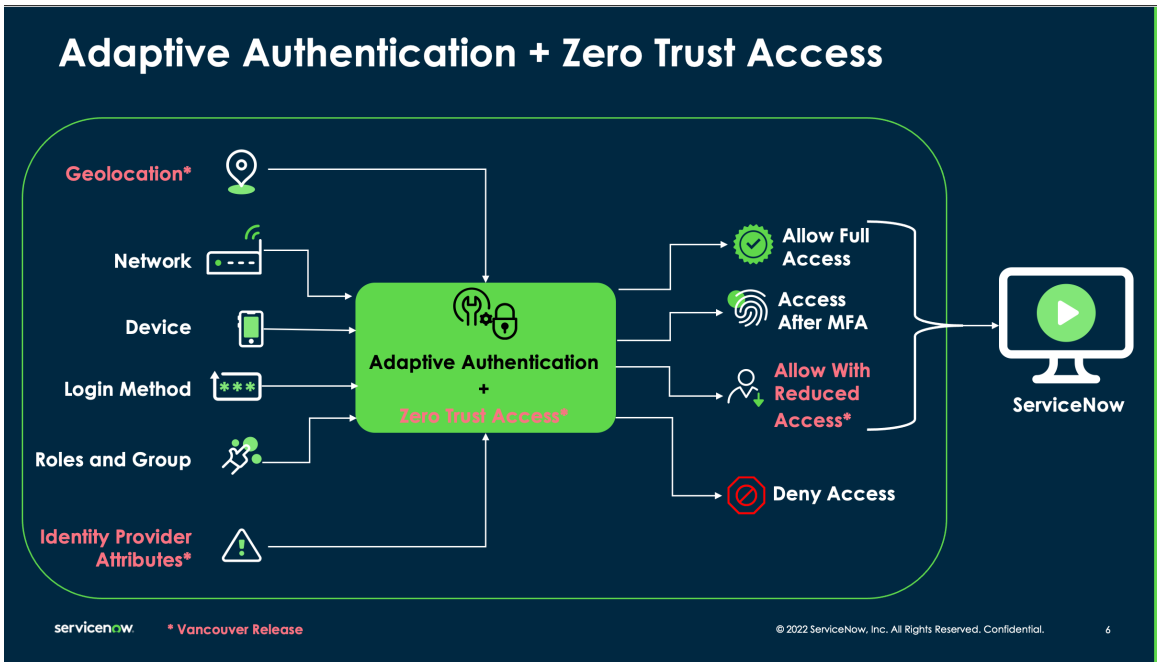
ZTA では、ユーザーの ID 検証とリスクアセスメントの後にのみ、アプリケーションとデータへのすべてのアクセスが最小限の権限で付与されます。

Zero Trust - Policy Based Session Access

ServiceNow® Zero Trust - Policy Based Session Access (Session Access) を使用すると、IP アドレス、場所、認証方法、ユーザーのロール、グループ、MFA と ID プロバイダー (IDP) によって共有される属性を持つユーザーなど、さまざまな要素に基づいて Web セッションのユーザー権限を動的に削減できます。これにより、高権限ユーザーが信頼できないデバイスや場所からアプリケーションにアクセスする場合でも、無許可のアクセスやデータ侵害から組織を保護できます。

Zero Trust - Policy Based Session Access

これにより、セキュリティ管理者は、適応認証ポリシーを使用して、IP アドレス、場所、ID プロバイダー属性、およびユーザー属性に基づいて、セッションでのユーザーアクセスを削減または制限できます。



自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注:

- セッションアクセスの構成は security_admin ロールでのみ実行できます。ロールを security_admin に昇格させる必要があります。
- セッションアクセスは統合をサポートしていません。
- 削減または制限されたロールがユーザーに割り当てられていない場合、セッションアクセスは影響を与えません。この場合、ログインしたセッションに変更はありません。ユーザーは引き続き、アサインされた権限でインスタンスにアクセスできます。
- ユーザーがすでにインスタンスにログインし、同時に管理者がポリシーを設定している間は、セッションアクセスに影響はありません。ポリシーを有効にするには、ユーザーがセッションからログアウトする必要があります。
- ユーザーが信頼できるネットワーク内にいて、後でセッション内で VPN (場所またはネットワークの変更) に切り替わった場合、セッションアクセスは影響を与えません。
- セッションアクセスはログイン時に適用されます。セッション中にリスクパラメーターが変更されても、アクセスが制限されることはありません。たとえば、ユーザーがセッションの確立後に企業ネットワークから信頼できないネットワークに切り替えても、ユーザーがログアウトして再度ログインしない限り、アクセスは減少しません。

ユースケース

以下は、ゼロトラストアクセスのユースケースの一部です。

- セッションに関連するリスクに基づいて権限を削減します。たとえば、信頼できるネットワークの外部からログインする履行者ロールユーザーは、セッションの要求者ロールのみを持つように設定できます。
- ユーザーが信頼できないデバイスを使用している場合は、ユーザーセッションの IDP 応答に基づいてアクセスを削減します。詳細については、「セッションアクセスの IDP 属性の構成」を参照してください。

このロールの降格により、ユーザーがセッションで他の既存の権限を持たないことが保証されます。ユーザーが信頼できるネットワークからログインすると、既存のすべての権限がセッションに割り当てられます。

複数の IP 条件と複数のロールまたはグループのアサインをポリシーの一部として定義できます。

Zero Trust アクセス - モバイル

適応認証ポリシー内でゼロトラストアクセス - セッションアクセスポリシーを使用して、モバイルの特定のセッションのロールまたは権限を減らすことができます。

Zero Trust Access - セッションアクセスモバイルを有効にするには、システムプロパティテーブルから **glide.authenticate.session_access.mobile.enabled** を有効にします。

IDP 属性で Zero Trust Access - Session Access Mobile を使用するには、**glide.authenticate.session_access.mobile.refresh_token_interval** フィールドを設定します。これにより、管理者はリフレッシュトークンに基づいてセッションアクセスを効果的に制御できます。

詳細については、「Configure Zero Trust Access for mobile」を参照してください。

Zero Trust アクセスのアクティブ化

Zero Trust - Policy Based Session Access com.snc.zero_trust_session_accessポリシーをアクティブ化して、セキュリティ管理者が適応認証ポリシーを使用して、IP アドレス、場所、ID プロバイダー属性、およびユーザー属性に基づいてセッションでのユーザーアクセスを削減または制限できるようにします。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

始める前に
必要なロール：admin

手順

1. 移動先 すべて > システムアプリケーション > 利用可能なすべてのアプリケーション > すべて.
2. フィルター基準と検索バーを使用して、**Zero Trust - Policy Based Session Access** (com.snc.zero_trust_session_access) プラグインを検索します。

   名前または ID でプラグインを検索できます。プラグインが見つからない場合は、ServiceNow 担当者から要求する必要があります。
3. [インストール] を選択して、[プラグインをアクティブにする] ダイアログボックスで、[アクティブ化] をクリックします。

   注:
   ドメイン分離と代理管理者がインスタンスで有効になっている場合、管理ユーザーはグローバルドメインに含まれている必要があります。それ以外の場合、次のエラーが表示されます： 別の操作が実行されているため、アプリケーションのインストールは利用できません：<プラグイン名> のプラグインの有効化。

セッションアクセスロールの構成

適応認証ポリシーを使用してセッションアクセスを構成し、IP、場所、ID プロバイダー属性、およびユーザー属性に基づいてセッションでのユーザーアクセスを削減します。

始める前に
必要なロール：security_admin

注:

- セッションアクセスの構成は security_admin ロールでのみ実行できます。ロールを security_admin に昇格させる必要があります。
- セッションアクセスは統合をサポートしていません。
- 削減または制限されたロールがユーザーに割り当てられていない場合、セッションアクセスは影響を与えません。この場合、ログインしたセッションに変更はありません。ユーザーは引き続き、アサインされた権限でインスタンスにアクセスできます。
- ユーザーがすでにインスタンスにログインし、同時に管理者がポリシーを設定している間は、セッションアクセスに影響はありません。ポリシーを有効にするには、ユーザーがセッションからログアウトする必要があります。
- セッションアクセスはログイン時に適用されます。セッション中にリスクパラメーターが変更されても、アクセスが制限されることはありません。たとえば、ユーザーがセッションの確立後に企業ネットワークから信頼できないネットワークに切り替えても、ユーザーがログアウトして再度ログインしない限り、アクセスは低下しません。

手順

1. 移動先 すべて > **Zero Trust** アクセス > セッションアクセスロール構成.
2. セッション アクセス ロール構成を作成するには、 [新規] を選択します。
3. フォームの各フィールドに入力します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

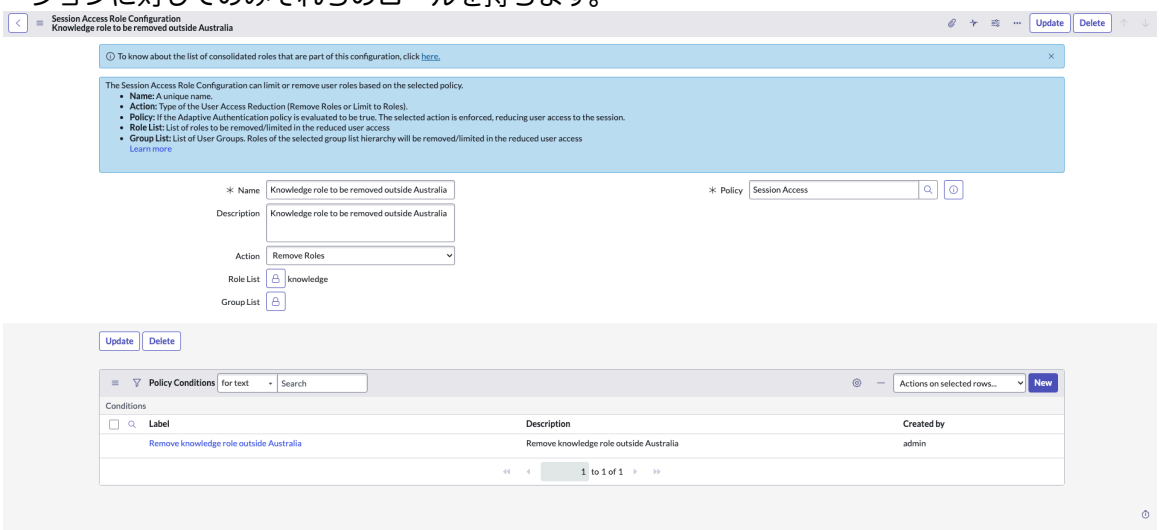
セッションアクセスのロール構成

フィールド	説明
名前	構成の名前
説明	構成の簡単な説明
ポリシー	適応認証ポリシーを選択します。ルックアップアイコンを使用して、ポリシーのリストを表示します。
アクション	[ロールを削除] または [ロールに制限 **(Limit to Roles)**] ○ ロールの削除: 設定されたユーザーがログインすると、ロールまたはグループリストで提供されているロールのリストがセッションに対して削除されます。 ○ ロールの制限:設定されたユーザがログインすると、選択したロールのみがユーザに提供され、他のすべてのロールはセッションで削除されます。
ロールリスト	ロールリストからロールを選択します。
グループリスト	グループリストから、削除するロールを選択するか、ユーザーに制限します。

4. [送信] を選択します。

構成された国に基づいたユーザーのログインは次のとおりです。

- [ロールを削除] で、選択したロールを持つ構成済みの国のユーザーは、セッションに対してそれらのロールを持たなくなります。
- [ロールに制限 **(Limit to Roles)**] で、選択したロールを持つ構成済みの国のユーザーは、セッションに対してのみそれらのロールを持ちます。



サンプルユースケースで説明されているセッションに対してロールを削除または制限する方法の詳細については、「チュートリアル：Zero Trust アクセスを使用する」を参照してください。

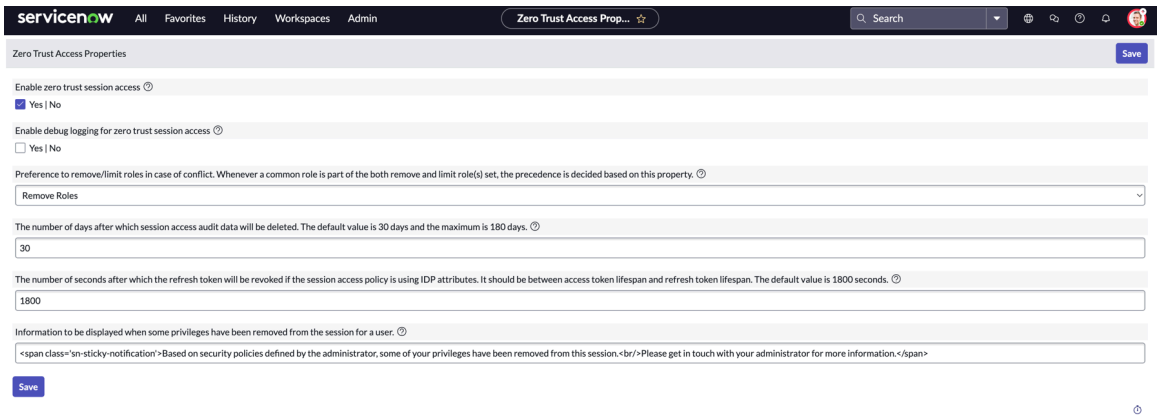
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

Zero Trust アクセスのシステムプロパティ

システムプロパティを使用すると、Zero Trust アクセスを有効化してカスタマイズし、セキュリティ要件を満たすことができます。

プロパティ



Zero Trust アクセスのシステムプロパティ

プロパティ	説明
ゼロトラストセッションアクセスを有効にする	管理者がゼロトラストセッションアクセス機能を使用できるようにするオプション。デフォルト値は false です。
ゼロトラストセッションアクセスのデバッグログを有効にする	ゼロトラストセッションアクセスのデバッグログを有効にするオプション。
競合が発生した場合にロールを削除/制限する設定。共通ロールが削除ロールと制限ロールの両方のセットに含まれる場合は常に、このプロパティに基づいて優先順位が決定されます。(Preference to remove/limit roles in case of conflict. Whenever a common role is part of both remove and limit role(s) set, the precedence is decided based on this property.)	[ロールを削除] または [ロールに制限 **(Limit to Roles)**]
セッションアクセス監査データが削除されてからの日数。デフォルト値は 30 日で、上限は 180 日です。(The number of days after which session access audit data will be deleted. The default value is 30 days and the maximum is 180 days.)	デフォルトは 30 日です。
セッションアクセスポリシーが IDP 属性を使用している場合に、リフレッシュトークンが取り消されるまでの秒数。アクセストークンの有効期間と更新トークンの有効期間の間である必要があります。デフォルト値は 1800 秒です。	デフォルトでは 1800 秒です。
ユーザーのセッションから一部の権限が削除されたときに表示される情報 (Information to be	権限の制限または削除に関してユーザーに表示する説明。サンプルの説明は次のとおりです。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Zero Trust アクセスのシステムプロパティ (続く)

プロパティ	説明
displayed when some privileges have been removed from the session for a user.)	管理者によって定義されたセキュリティポリシーに基づいて、一部のロールがこのセッションから削除されました。詳細については、管理者にお問い合わせください。(Based on security policies defined by the administrator, some of your roles have been removed from this session. Please get in touch with your administrator for more information.)

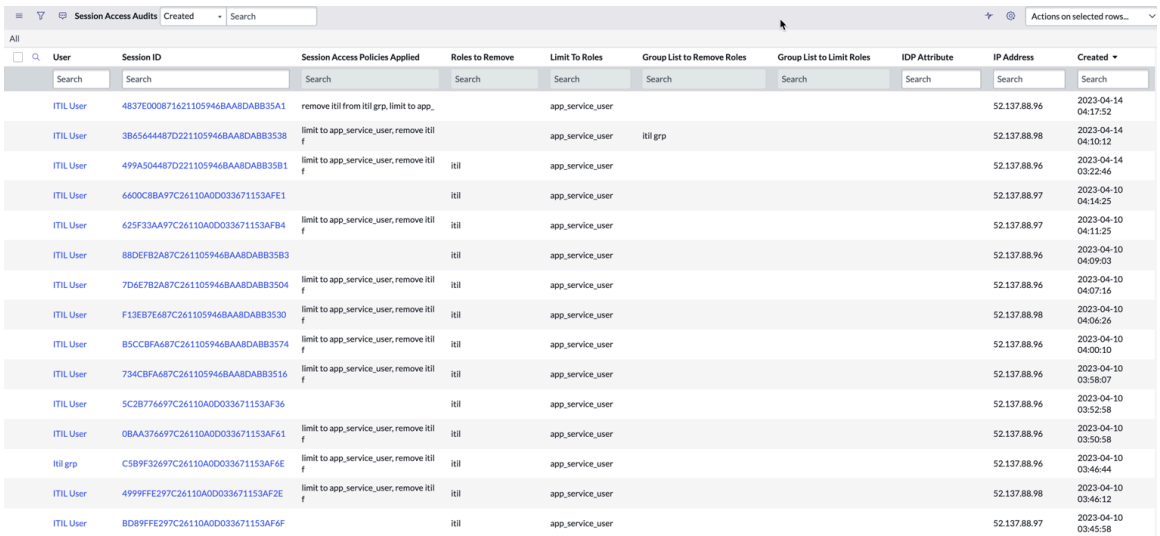
セッションアクセス監査

セッションアクセス監査には、ユーザーのセッションに関連するセッションアクセスログと情報が表示されます。

監査

セッションアクセス監査では、監査情報が次のように表示されます。

注:
glide.authenticate.session_access.log_audit_event プロパティを使用して監査情報を入力します。



セッションアクセス監査

フィールド	説明
ユーザー	ユーザーの詳細
セッション ID	一意の ID として表示されるセッションの詳細
モバイルクライアント	モバイルクライアントの詳細。**ServiceNow** Agent (Now Agent) および **ServiceNow Request** (Now Mobile)。
セッションアクセスポリシーが適用されました	適用されるセッションアクセスポリシー。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

セッションアクセス監査 (続く)

フィールド	説明
削除するロール	ログイン中にユーザーから削除されたロール。
ロールに制限	ログイン中にユーザーに制限されたロール
ロールを削除するグループリスト	ユーザーのロールを削除したグループに関する情報。
ロールを制限するグループリスト	ユーザーのロールが制限されているグループに関する情報。
モバイルクライアント	モバイルからログインしているが、アクセス権が制限または削除されたユーザーの詳細。
IDP 属性	そのセッションに使用された IDP
IP アドレス	ユーザーがログインに使用する IP アドレスの詳細
作成済み	作成されたユーザーレコードの日時の詳細

チュートリアル：**Zero Trust** アクセスを使用する

エンドツーエンドのユースケースで Zero Trust Access 機能を使用する手順。

始める前に

必要なロール：security_admin

[セッションアクセスの有効化 **(Enable Session Access property)]** を有効にします。

注:

- セッションアクセスの構成は security_admin ロールでのみ実行できます。ロールを security_admin に昇格させる必要があります。
- セッションアクセスは統合をサポートしていません。
- 削減または制限されたロールがユーザーに割り当てられていない場合、セッションアクセスは影響を与えません。この場合、ログインしたセッションに変更はありません。ユーザーは引き続き、アサインされた権限でインスタンスにアクセスできます。
- ユーザーがすでにインスタンスにログインし、同時に管理者がポリシーを設定している間は、セッションアクセスに影響はありません。ポリシーを有効にするには、ユーザーがセッションからログアウトする必要があります。
- セッションアクセスはログイン時に適用されます。セッション中にリスクパラメーターが変更されても、アクセスが制限されることはありません。たとえば、ユーザーがセッションの確立後に企業ネットワークから信頼できないネットワークに切り替えても、ユーザーがログアウトして再度ログインしない限り、アクセスは低下しません。

セッションアクセスは、ユーザーが信頼できないネットワークからのログイン、別のデバイスからのログインなど、異なる環境からインスタンスにログインしようとしているときに、管理者がユーザーに対して一連のロールを動的に削減または制限できるようにする機能です。

セッションアクセスは、構成を実行するときに作成されたポリシーと選択したアクションによって制御できます。シナリオの一部は次のとおりです。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- ポリシーが true で、ロールアクションが [ロールを削除] に設定されている場合、ユーザーがインスタンスにログインしようとすると、選択したロールとそれに関連する子ロールがそのユーザーから削除されます。
- ポリシーが true で、ロールアクションが [ロールに制限 **(Limit To Roles)]** に設定されている場合、ユーザーがインスタンスにログインしようとすると、選択したロールとそれに関連付けられた子ロールのみがそのユーザーにアサインされます。

次の手順では、インスタンスにログインしているユーザーにロールが制限されるセッションアクセス構成のエンドツーエンド構成について説明します。同様に、構成中に [ロールを削除] オプションを選択して、ロールを削除することもできます。

手順

1. 移動先 すべて > セッションのアクセス > セッションアクセスロール構成.
2. [セッションアクセスロールの構成 (Session Access Role Configurations)] ページで、[新規] を選択します。
3. ユーザーのロールを制限するには、フォームの各フィールドに入力します。
   - 名前
   - 説明
   - ポリシー
   - アクション
   - ロールリスト
   - グループリスト

   a. [ロールに制限 **(Limit to Roles)]** を選択して、ユーザーのロールを制限します。
   例：**itil**

   b. ロールリストから [ナレッジ] ロールを選択します。

   c. [ポリシー] を選択します。

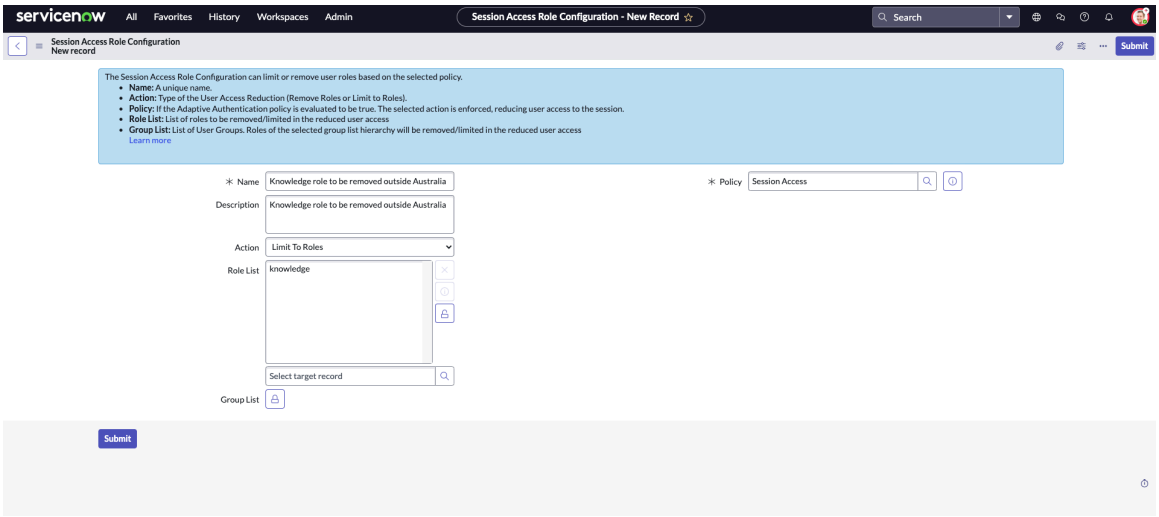
   ポリシーの入力と条件で認証ポリシーとフィルター基準 (ロール、グループ、IP、場所) を使用して、セッションアクセスポリシーを作成できます。

   セッションアクセス構成でポリシーを使用します。たとえば、ロール (ナレッジ) を、場所 (オーストラリア) の外部でログインしているユーザーに制限するとします。

   d. [アクション] で [ロールに制限 **(Limit to Roles)]** を選択します。ポリシーが true の場合、ユーザーはインスタンスにログインしようとするときに、選択したロールとそれに関連する子ロールのみを使用できます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

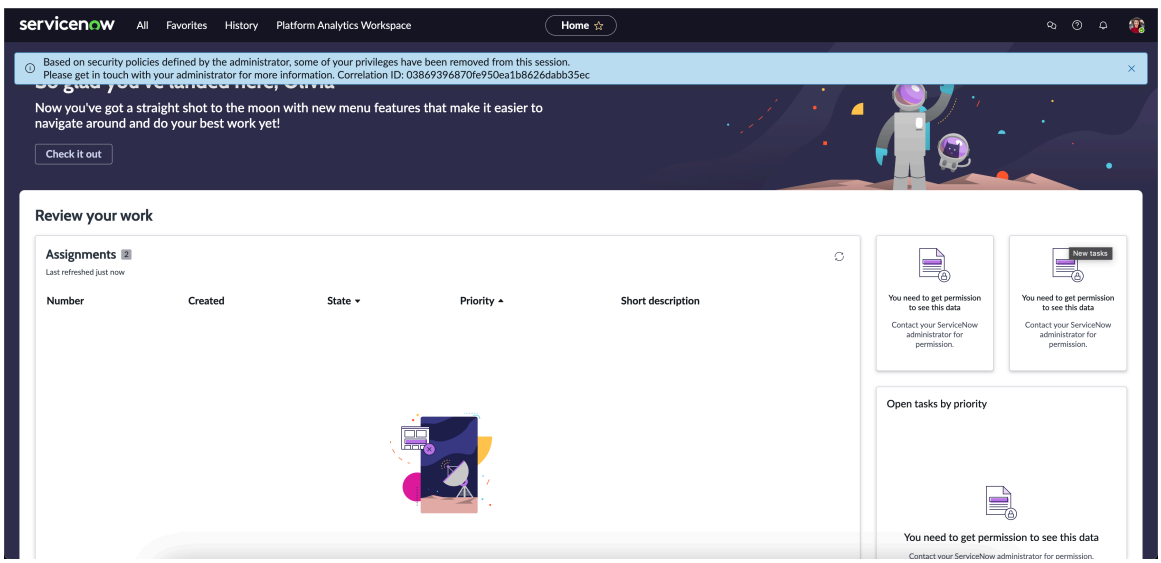


e. [送信] を選択します。

同様に、グループリストからグループを選択して、グループ内のユーザーのロールを制限または削除できます。

ユーザーがオーストラリア国外のインスタンスにログインすると、[ナレッジ] ロールとそれに関連する子ロールのみがログインセッションにアサインされ、ユーザーに対する他のロールは制限されます。

ログイン後、ユーザーのプロファイルセクションにプラットフォームの次のエラーメッセージが表示されます。



ユーザーは管理者に連絡し、調査のために相関 ID を提供できます。

> **注:**
> 相関 ID は、セッションアクセス監査テーブル内で対応する監査レコードの sys_id です。

セッションアクセスの **IDP** 属性の構成

セキュリティアサーションマークアップ言語 (SAML) 応答から作成された ID プロバイダー (IDP) 属性を使用して、インスタンスへのユーザーセッションアクセスを削除または制限します。

始める前に
必要なロール：security_admin

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

[セッションアクセスの有効化 **(Enable Session Access property)]** を有効にします。

> **注:**
> セッションアクセスロール構成を使用するには、ロールを security_admin に昇格させる必要があります。

セッションアクセスは、構成を実行するときに作成されたポリシーと選択したアクションによって制御できます。シナリオの一部は次のとおりです。

- ポリシーが true で、ロールアクションが IDP 属性の入力と条件とともに [ロールを削除] に設定されている場合、ユーザーがインスタンスにログインしようとすると、選択したロールとそれに関連付けられた子ロールが削除されます。
- ポリシーが true で、ロールアクションが IDP 属性の入力と条件とともに [ロールに制限] に設定されている場合、インスタンスにログインしようとすると、選択したロールとそれに関連付けられた子ロールのみがユーザーにアサインされます。

次の手順は、SAML 応答から IDP 属性をポリシー入力に設定してセッションアクセスを制御する方法を示しています。

手順

1. 移動先 すべて > セッションのアクセス > セッションアクセスロール構成.
2. [セッションアクセスロールの構成 (Session Access Role Configurations)] ページで、[新規] を選択します。
3. ユーザーのロールを削除するには、フォームのフィールドに入力します。
   - 名前
   - 説明
   - ポリシー
   - アクション
   - ロールリスト
   - グループリスト

   a. [ロールを削除] を選択して、ユーザーのロールを削除します。例：**itil**

   b. ロールリストから **[itil]** ロールを選択します。

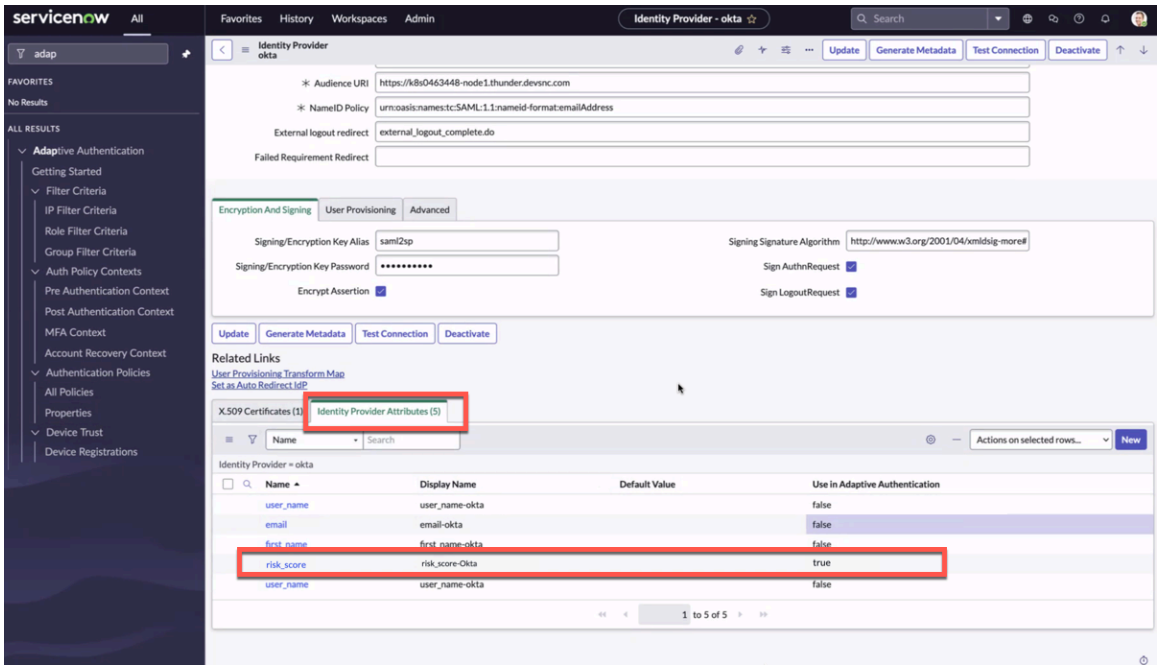
   c. [ポリシー] を選択します。適応認証ポリシーの作成を使用してさまざまなフィルター基準でポリシーを作成する方法の詳細については、「フィルター基準」を参照してください。

   d. [アクション] で [ロールを削除] を選択します。ポリシーが true で、ロールアクションが [ロールを削除] に設定されている場合、ユーザーがインスタンスにログインしようとすると、選択したロールがそのユーザーから削除されます。

   e. ポリシー入力で、ポリシーの入力と条件を作成します。例：
      - ポリシー入力:Okta (IDP) からのリスクスコア属性
      - ポリシー条件：条件としての 60 ～ 80 のリスクスコア

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



この構成に基づいて、Okta (IDP) からのリスクスコア属性値が 80 を超えると、ユーザーはインスタンスに削除されたロール (従業員) とその子ロールで認証されず、割り当てられた他のロールでのみ認証されます。リスクスコアが 60 ～ 80 の場合、ユーザーはすべてのロールでインスタンスに認証されます。

ポリシーと条件で認証後コンテキストのポリシーを作成する方法の詳細については、「認証後コンテキスト」を参照してください。

注:
[セッションアクセスを有効にする] プロパティが無効の場合、セッションアクセスの構成はユーザーのロールを制限または削除しません。

f. [送信] を選択します。

モバイル向け **Zero Trust** アクセス

ゼロトラストアクセス(ZTA)は、デフォルトで信頼されるユーザーまたはデバイスがないことを前提とするセキュリティモデルです。

適応認証ポリシー内でゼロトラストアクセス - セッションアクセスポリシーを使用して、ユーザーのモバイルでの特定のセッションのロールまたは権限を減らすことができます。

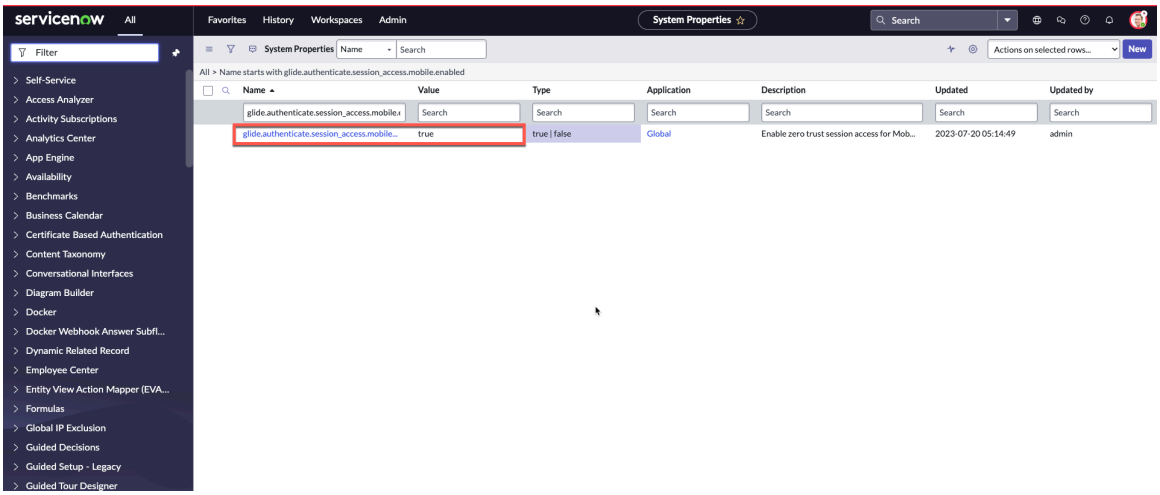
モバイルで Zero Trust アクセスを有効にするには、次のタスクを実行する必要があります。

- セッションアクセスの構成は security_admin ロールでのみ実行できます。ロールを security_admin に昇格させる必要があります。
- ゼロトラスト - ポリシーベースのセッションアクセス com.snc.zero_trust_session_accessポリシーを有効にします。

自動翻訳

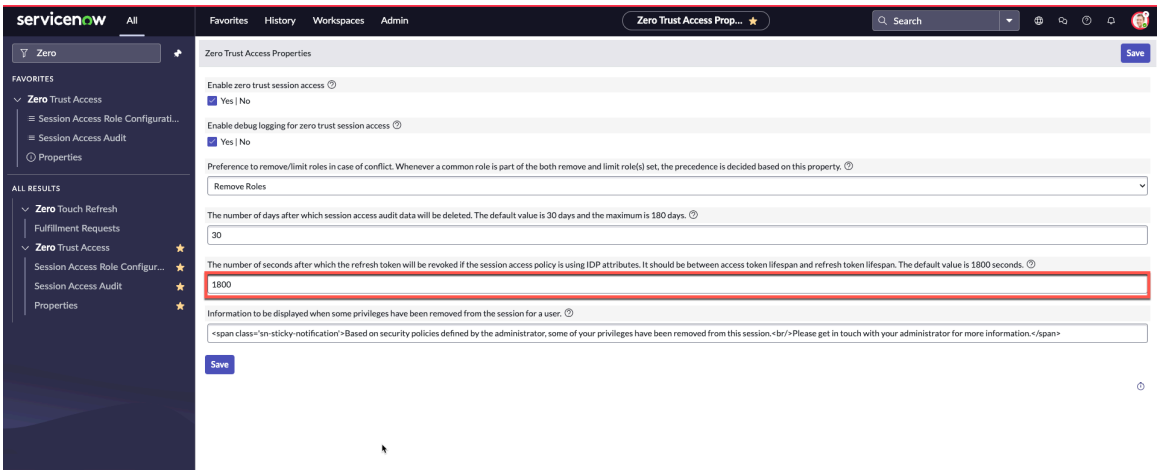
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- システムのプロパティテーブルから **glide.authenticate.session_access.mobile.enabled** を有効にしま



す。

- リフレッシュトークンに基づいてモバイルでのセッションアクセスを制御するように **glide.authenticate.session_access.mobile.refresh_token_interval** フィールドを設定しま



す。

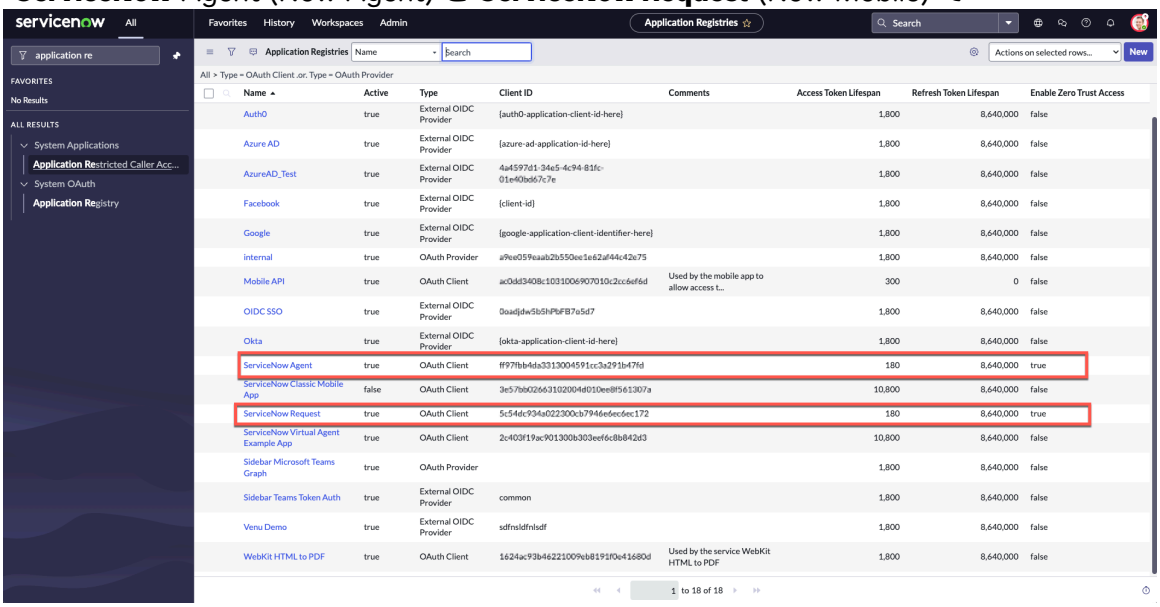
> **注:**
> モバイルアプリのログインに IDP を使用する場合は、リフレッシュトークンの秒数を設定する必要があります。デフォルトでは、ユーザーは 1800 秒 (30 分) 後にモバイルアプリからログアウトされます。

- [Zero Trust アクセスを有効にする] は、モバイルクライアントアプリケーション (OAuth クライアント **)** の [アプリケーションレジストリ] で有効になっています。この場合

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

は、 **ServiceNow** Agent (Now Agent) と **ServiceNow Request** (Now Mobile) で



す。

- ポリシーの入力と条件に基づいてログ記録を行うユーザーのロールを減らすか削除するように、セッションアクセスロールを構成します。構成の詳細については、以下を参照してください セッションアクセスロールの構成。

構成では、ログインを評価し、ポリシーフィルターと条件に基づいて、インスタンスにアクセスする ServiceNow　ユーザーのロールを削減または削除します。詳細については、「Configure Zero Trust Access for mobile」を参照してください。

接続と資格情報

ディスカバリー、サービス マッピング、およびクラウド管理用にコンピューターまたはネットワークデバイスへのアクセス権を得る、またはオーケストレーションを使用して作業を実行するには、認証情報と接続情報が必要です。共有または AppStore にコンテンツを追加すると、作成されたコンテンツを変更することなく、環境に関連する接続と認証情報を設定することができます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

探索

資格情報について学習します。

構成

資格情報を設定します。

参照

資格情報の詳細を取得します。

トラブルシューティング

接続と資格情報の問題をトラブルシューティングする方法について説明します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

資格情報、接続、およびエイリアスの概要

Now Platform でのすべてのアプリケーション統合では、接続、資格情報、およびエイリアスを使用して、それぞれのアプリケーションがリソースにアクセスできるようにします。

Now Platform でアプリケーションデータ連携を実行する前に、接続情報および対応する資格情報を作成して、エイリアスを追加する必要があります。ServiceNow でのこれらの用語の定義を確認するには：

接続

「接続」とは、プロトコルを使用する IP アドレスやエンドポイントなどの、システムとのデータ連携です。これには、データベースと統合する際のデータベースの詳細など、特定の詳細が含まれています。

資格情報

「資格情報」とは、ID やパスワードなど、接続に必要な認証データです。

エイリアス

「エイリアス」とは、インスタンス上の一連の接続または資格情報に関連付けられている命名規則またはタグです。エイリアスには、アプリケーションのデータ連携に必要な接続および資格情報が含まれています。データ連携するたびにその情報を入力する代わりに、エイリアスを使用できます。たとえば、同じアプリケーションデータ連携の QA、開発、および本番資格情報を格納するエイリアスを指定できます。エイリアスは、各環境のアプリケーションデータ連携を解決します。

Now Platform は、さまざまなタイプのエイリアスを区別します。

資格情報エイリアス

このエイリアスは資格情報データにのみ関連付けられ、実行時に解決します。

接続および資格情報エイリアス

このエイリアスは、データ連携を完了するために必要な接続情報と資格情報データに関連付けられ、実行時に解決します。

接続および資格情報エイリアス内で、「子エイリアス」と呼ばれる追加のエイリアスを作成することもできます。子エイリアスを使用すると、同じアプリケーションデータ連携内で複数の接続を作成できます。子エイリアスを作成すると、作成したエイリアスが属するエイリアスが「親エイリアス」になります。子エイリアスは親エイリアスからプロパティを継承しますが、子エイリアスは独自の接続および資格情報を保持します。

接続、資格情報、およびエイリアスを使用するメリット

- 外部サービスの資格情報を一元的に保存および管理できます
- 一度定義すれば、複数のプラットフォーム機能に再利用できます
- 他のプラットフォーム機能の構成を最小限に抑えることができます
- 管理者以外のユーザーに、事前定義された接続および資格情報の使用を許可できます
- セキュリティを強化できます

接続、資格情報、およびエイリアスを使用する機能

以下の機能では、接続、資格情報、およびエイリアスを使用します。

- Flow Designer
- IntegrationHub

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- Cloud Management
- Discovery
- Orchestration
- Service Mapping

Now Platform でエイリアスを設定するには、次の 2 つの方法のいずれかを使用します。

- 接続情報と認証情報 モジュールを使用します。「接続情報および認証情報エイリアスの作成」を参照してください。
- 統合ハブ の接続ダッシュボードで設定します。「接続の追加」を参照してください。

> **注:**
> 統合ハブ では別のサブスクリプションが必要です。詳細については、次を参照してください： 要求 統合ハブ.

MID Server での認証情報の同期

インスタンスと同期しているネットワーク内の各 *MID Server* は、作成したすべての資格情報のコピーを保持します。管理、計測、検出 (MID) サーバーは、ServiceNow インスタンスと外部のアプリケーション、データソース、サービスの間で行われるデータの通信や移動を支援する Java アプリケーションです。この同期により、ディスカバリー や サービスマッピング などのアプリケーションがネットワーク上の複数のデバイスにアクセスする必要がある場合に認証情報の読み取り速度が向上します。MID Server は、ECC キューで `credentials_reload` ジョブが見つかったときに同期します。再ロード ジョブは、すべてのフィールド値を含む資格情報 [discovery_credentials] テーブル内の資格情報のリスト全体を取得するために、MID Server にインスタンスへの SOAP 呼び出しの実行を指示します。詳細については、「MID Server」を参照してください。

インスタンスを各 MID Server に送信する SOAP 応答には、カスタマイズした認証情報フォームに追加したカスタム フィールドも含まれます。参照フィールドを追加すると、参照テーブルのデータも SOAP 応答の一部として送信されます。これにより、複数の MID Server で認証情報の同期が発生したときにパフォーマンスの問題が発生する可能性があります。これを制御するには、次のプロパティをシステム プロパティ [sys_properties] テーブルに手動で追加します。

> **注:**
> 次のプロパティの値を変更するには、それらの値をシステム プロパティ [sys_properties] テーブルに追加します。それらの値を追加しない場合、デフォルト値が使用されます。

プロパティ	説明
com.snc.credentials_user_fields	認証情報の同期でカスタマイズされたすべてのフィールドが含まれます。資格情報フォームに追加したフィールドを含めない場合は、このプロパティを false に設定します。 • タイプ：true | false • デフォルト値：true
com.snc.credentials_recursion_depth	資格情報の同期メカニズムによって参照テーブルからフィールドが収集されるときにトラバースするテーブルの数を定義します。パフォーマンスの問題が発生し、参照フィールドも含まれているテーブルへの参照フィールドを含む認証情報フォームをカスタマイズしている場合は、この数を少なくします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

プロパティ	説明
	• タイプ：整数 • デフォルト値：3

資格情報および接続のスコープ保護

特定のタイプの接続 & 資格情報レコードをスコープに属するものとして分類し、スコープの保護をそれらに拡張することができます。 これらのスコープポリシーは、テーブルで作成したレコードを保護し、別のスコープとのプライベートなレコードのやり取りを防止します。

接続 [sys_connection] テーブルおよび Discovery 資格情報 [discovery_credentials] テーブルの [アプリケーション] フィールドを使用して、これらのタイプのレコードを特定のスコープに関連付けることができます。Washington DC の UI フォームには表示されませんが、簡単に追加できます。これらのレコードタイプの詳細と、UI フォームへのフィールドの追加方法については、以下を参照してください。

- 接続を開始
- 認証情報の開始
- Discovery の資格情報エイリアス
- フォームレイアウトの構成

接続 & 資格情報レコードの使用を特定のスコープに制限することは、セキュリティを強化する必要があるアプリケーションを管理するために重要です。これらのアプリケーションには HR サービスデリバリ (HRSD) または Security Operations スコープ指定の管理対象アプリケーションで作成された接続および資格情報レコードは、管理者ユーザーには表示されません。 接続および資格情報レコードを特定のアプリケーションスコープに関連付けると、次の保護が得られます。

- 制限付きスコープにアクセス制御リストルール (ACL) が適用されます。スコープ指定の ACL の詳細については、「アクセス制御リストのルール」を参照してください。

  注:
  スコープ管理および強化セキュリティを使用する一部のアプリケーションでは、追加のセットアップが必要になる場合があります。詳細については、「人事ロールの管理」を参照してください。

- スクリプトを使用してクエリーが実行されたときにレコードを保護します。グローバルスコープからクエリーを実行し、接続および資格情報レコードが保護されたスコープ内にある場合、アクセス権が付与されていない限り、クエリーには表示されません。

制限付きの発信者アクセスを使用して、クエリー制限付きレコードへのアクセスをカスタマイズおよび付与できます。詳細については、「制限付き発信者アクセス特権の設定」を参照してください。スコーピング制限は、接続 [sys_connection] テーブルおよび Discovery 資格情報 [discovery_credentials] テーブルのすべての子テーブルにも適用されます。空のフィールドおよびその他のスコープは制限されません。

注:
スコープ保護は、新しいレコードを設定する際の混乱を避けるために、特定の保護されたスコープに対してのみ有効になります。誰かがスコープ対象のアプリケーションスコープで接続を行っても、自動的にスコープが制限されることはありません。

ドメイン分離、資格情報および接続

ドメイン分離は資格情報および接続でサポートされています。 ドメイン分離では、データ、プロセス、および管理タスクをドメインと呼ばれる論理的なグループに分けることができます。どのユー

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ザーがデータを表示できるか、データにアクセスできるかなど、このアプリケーションのいくつかの側面を制御できます。

サポートレベル：標準

- ベーシックレベルサポートを含みます。
- ビジネスロジック：サービスプロバイダー (SP) によって顧客ごとにプロセスを作成または変更できます。ユースケースには、単一のインスタンスでの複数のサービスプロバイダー顧客によるアプリケーションの正しい使用が反映されています。
- インスタンスのオーナーは、特定のアプリケーションに期待される通りに、テナントごとに MVP ビジネスロジックとデータパラメーターを設定できる必要があります。

サンプルユースケース：管理者は、レコードを他のテナントに対してはクローズしないが、1 つのテナントに対してクローズする場合、コメントを必須にすることができる必要があります。

サポートレベルの詳細については、「アプリケーションでのドメイン分離のサポート)」を参照してください。

概要

認証情報は、インスタンス外のシステムにアクセスするさまざまなServiceNow機能に関連付けられます。認証情報は、認証情報を使用する機能に関連付けられたドメイン分離に従います。

接続情報は、インスタンス外のターゲット ホストを参照するプロトコル固有の情報です。接続情報には、アクティビティを実行するドメインを指定できます。

資格情報および接続情報でのドメイン分離の仕組み

認証情報は、インスタンス外のリソースにアクセスし、 検出 、 オーケストレーション 、 サービスマッピング 、および Cloud Provisioning and Governance 得られますこれらの資格情報は、特定のドメインに関連付けられるのではなく、アプリケーションにバインドされ、アプリケーションで使用されるドメイン分離に従います。また、資格情報を MID Server に割り当てて、MID サーバー 構成で指定されたドメイン分離に従うこともできます。

接続情報によって、*JMS*、*JDBC*、または *HTTP(S)* 接続を使用してターゲットホストにアクセスします。接続元となるグローバル ドメインまたは特定のドメインを指定できます。

関連情報

サービスプロバイダーのドメイン分離

接続と資格情報の構成テンプレート

管理者および flow_designer ロールを持つユーザーは、カスタマイズ可能な単一のフォームを使用して、サードパーティシステムとのスポーク統合を設定できます。

たとえば、OAuth プロバイダーを登録し、トークンを生成し、接続レコードおよび資格情報レコードを作成する OAuth データ連携を設定できます。アクションデザイナーまたは開発者は構成テンプレートを使用して 1 つの場所でスポークを設定でき、関連付けられたレコードがシステムによって作成されます。

利点

構成テンプレートを使用することで以下のことができるようになります。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- 管理者またはフロー設計者が、単一のフォームを使用して複雑な統合を設定できるようになります。
- 開発者がデータ連携で静的な値を設定し、管理者およびフロー設計者のセットアッププロセスを簡素化できるようになります。

サポートされている資格情報タイプ

次の資格情報タイプとの統合用の構成テンプレートを作成できます。

- 基本認証
- API キー
- OAuth JWT ベアラー権限許可タイプ
- OAuth 認証コード権限許可タイプ
- カスタム認証

構成テンプレートのコンポーネント

デフォルトのデータテンプレート

すべてのデータ連携に適用される静的情報を設定します。たとえば、値がすべてのデータ連携に適用される場合は、API およびトークンの URL を設定できます。

動的データテンプレート

統合を設定するためにユーザーが完了する必要のある情報を定義します。たとえば、ユーザー名とパスワードのキーと値のペアを追加して、ユーザー定義の値を収集することができます。

後処理スクリプト

統合によって必要とされる追加のレコードを作成します。たとえば、スポークにカスタムテーブルが含まれている場合は、構成テンプレートのユーザー入力に基づいてそれらのテーブルにレコードを作成できます。このスクリプトは、接続と資格情報レコードが作成された後に実行されます。

事前編集スクリプト

既存の接続を編集するときに、[追加情報] セクションのカスタムフィールドを事前に入力します。カスタムフィールドを事前入力すると、カスタムフィールドに関連付けられている現在の値を表示できます。

デモデータ

接続と資格情報のテンプレート [sys_alias_templates] テーブルには、一般的な認証タイプのテンプレートを設定する方法を示すテンプレートの例が含まれています。独自の例を作成するときは、これらの例をガイドとして使用してください。

OAuth JWT ベアラー権限許可タイプのテンプレートの構成

この構成テンプレートの例では、Docusign への要求を認証するために JWT ベアラー権限許可タイプを使用して、資格情報レコードおよび接続レコードを設定します。

デフォルトのデータテンプレート

デフォルトのデータテンプレートの各トップレベルのアイテムでは、関連するレコードが作成されます。テンプレートには、次のセクションが含まれています。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- 資格情報：資格情報テーブルにレコードを作成します。
- 接続：接続 [sys_connection] テーブルおよび関連する接続レコードにレコードを作成します。
- 追加：オプションでカスタムテーブルにレコードを作成します。後処理スクリプトは、システムがこれらのレコードを処理する方法を指定します。

次の例では、OAuth JWT ベアラー権限許可タイプ認証に必要なレコードを作成します。

```
{
 "credential": {
  "oauth_entity": {
   "oauth_entity_profile": [
    {
     "grant_type": "urn:ietf:params:oauth:grant-type:jwt-bearer",
     "name": "Docusign Profile",
     "default": true,
     "oauth_entity_profile_scope": [
      "users:read.email"
     ]
    }
   ],
   "code_challenge_method": "S256",
   "type": "consumer",
   "oauth_entity_scope": [
    {
     "oauth_entity_scope": "users:read.email",
     "name": "email"
    }
   ],
   "client_id": "<provider-client-id>",
   "use_mutual_auth": false,
   "revoke_token_url": "https://<provider-domain-name>.com/oauth2/revoke",
   "default_grant_type": "urn:ietf:params:oauth:grant-type:jwt-bearer",
   "public_client": false,
   "oauth_api_script": "3e3a3a11c333210016194ffe5bba8f70",
   "name": "Docusign Spoke OAuth",
   "client_secret": "<provider-client-secret>",
   "auth_url": "https://<provider-domain-name>.com/oauth2/auth",
   "token_url": "https://<provider-domain-name>.com/oauth2/token",
   "redirect_url": "https://<instance-name>.service-now.com/oauth_redirect.do"
  },
  "jwt_provider": {
   "jwt_keystore_aliases": {
    "kid": "<provider-key-id>",
    "name": "Docusign Spoke JWT Key",
    "signing_keystore": "<signing-keystore-sys-id>",
    "signing_algorithm": "rsa_256",
    "signing_key_password": "password"
   },
   "jwt_claim_validation" : [ {
    "name" : "iss",
    "is_standard" : true,
    "data_type" : "string",
    "value":"<docusign-iss-claim>"
   }, {
    "name" : "sub",
```

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

```
      "is_standard" : true,
      "data_type" : "string",
      "value":"<docusign-sub-claim>"
    }, {
      "name" : "aud",
      "is_standard" : true,
      "data_type" : "string",
      "value":"<docusign-aud-claim>"
    }, {
      "name" : "scope",
      "is_standard" : false,
      "data_type" : "string",
      "value" : "signature impersonation"
    } ],
    "name": "Docusign Spoke JWT Provider",
    "jwt_api_script": "9ef6af86ff10330001d3cd6bd53bf144"
  },
  "name": "Docusign Spoke Credential",
  "table": "oauth_2_0_credentials"
 },
 "connection": {
  "use_mid": false,
  "connection_url": "https://<provider-domain-name>.com",
  "name": "Docusign Spoke Connection",
  "table": "http_connection"
 },
"additional":{
  "docusign_account_name": "<docusign-account-name>",
  "docusign_account_email": "<docusign-account-email>"
}
}
```

動的なデータスキーマ

動的なデータスキーマは、ユーザーが接続および資格情報エイリアスを作成して入力を収集するときに表示される内容を定義します。ドット連結構文を使用して、デフォルトのデータテンプレートで作成されたフィールドにユーザー入力をマッピングします。たとえば、connection_fields は、デフォルトのデータテンプレートによって作成された connection オブジェクトの connection_url フィールドにユーザー入力をマッピングします。

```
{
 "connection_fields": [
  {
   "name": "connection.connection_url",
   "label": "Connection URL",
   "type": "text",
   "defaultValue": "https://demo.docusign.net",
   "hint": "Connection URL for Docusign"
  }],
"additional_fields":[
  {
   "name": "additional.docusign_account_id",
   "label": "Docusign Account Number",
   "type": "text",
   "hint": "Docusign Account Number"
  },
  {
```

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

```
    "name": "additional.docusign_account_name",
    "label": "Docusign Account Name",
    "type": "text",
    "hint": "Name to identify the Docusign account"
   },
   {
    "name": "additional.docusign_account_email",
    "label": "Docusign Account Email",
    "type": "text",
    "hint": "Docusign Account Email"
   }
 ],
 "credential_fields": [
   {
    "name": "credential.oauth_entity.client_id",
    "label": "OAuth Client ID",
    "type": "text",
    "hint": "Client ID for Docusign"
   },
   {
    "name": "credential.oauth_entity.redirect_url",
    "label": "OAuth Redirect URL",
    "type": "text",
    "defaultValue": "https://<instance-name>.service-now.com/oauth_redirect.do",
    "hint": "Callback URL for Docusign"
   },
{
    "name": "credential.jwt_provider.jwt_claim_validation[0].value",
    "label": "Issuer (iss) Claim value",
    "type": "text",
    "hint": "The integrator key (also known as client ID) of the application"
   },
{
    "name": "credential.jwt_provider.jwt_claim_validation[1].value",
    "label": "Subject (sub) Claim value",
    "type": "text",
    "hint": "The user ID of the user to be impersonated"
   },
{
    "name": "credential.jwt_provider.jwt_claim_validation[2].value",
    "label": "Audience (aud) Claim value",
    "type": "text",
    "defaultValue": "account-d.docusign.com",
    "hint": "The URI of the authentication service instance to be used e.g.
account.docusign.com"
   },
   {
    "name": "credential.jwt_provider.jwt_keystore_aliases.kid",
    "label": "Key ID (kid)",
    "type": "text",
    "hint": "Indicates which key was used to secure the JWS"
   },
   {
    "name": "credential.jwt_provider.jwt_keystore_aliases.signing_keystore",
    "label": "Key Store",
    "type": "file"
   }
```


自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

```
 ]
}
```

後処理スクリプト

次の後処理スクリプトは、ユーザー入力を sn_docusign_spoke_accounts テーブルのフィールドにマッピングします。

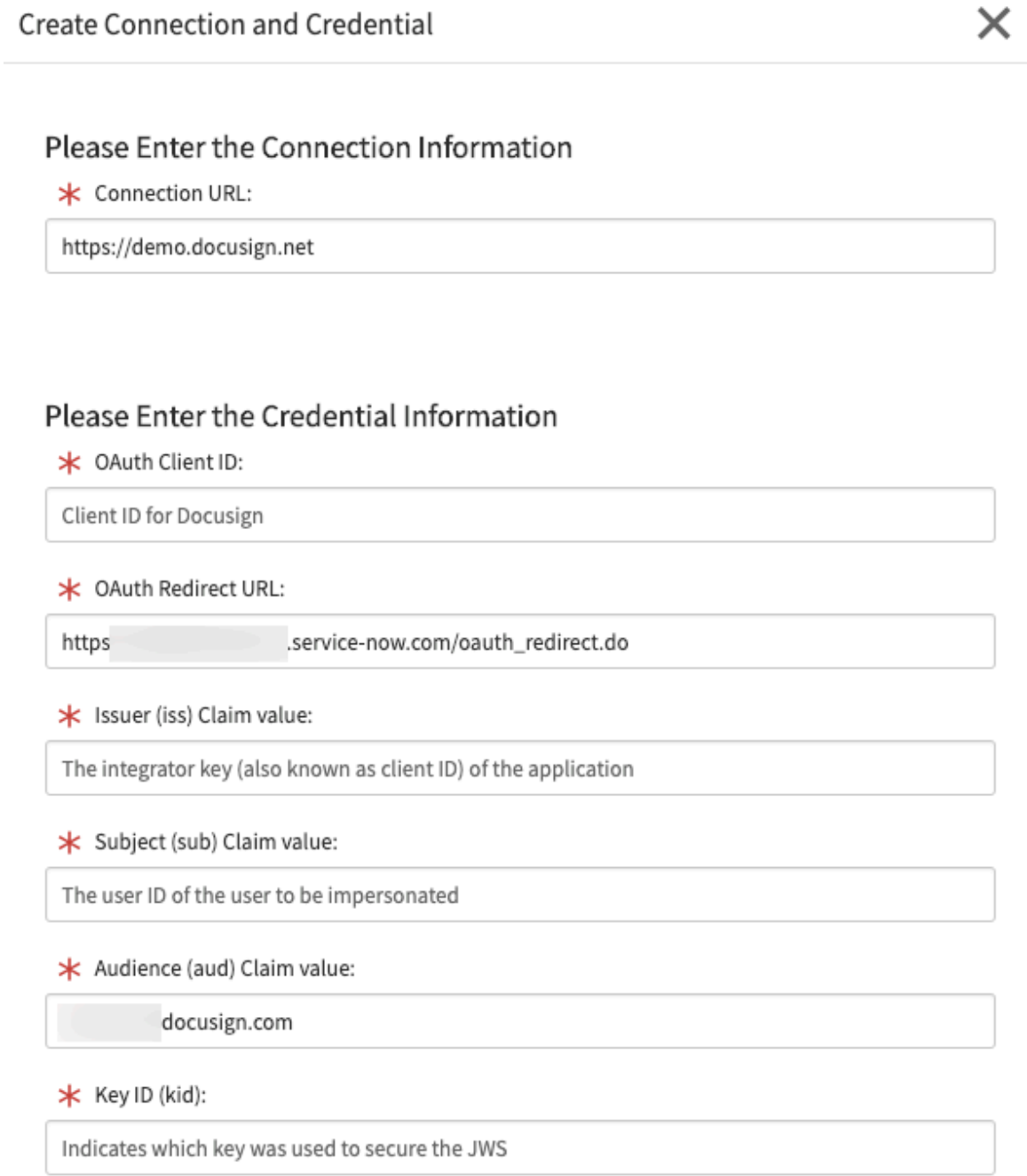
```
(function execute(aliasId, connectionSysId, jsonDefaultData, jsonDynamicData) {
 var jsonDynamicDataP = JSON.parse(jsonDynamicData);
 var accountGR = new GlideRecord("sn_docusign_spoke_accounts");
   accountGR.setValue("account_name",
 jsonDynamicDataP["additional.docusign_account_name"]);
   accountGR.setValue("alias", aliasId);
   accountGR.setValue("email", jsonDynamicDataP["additional.docusign_account_email"]);
   accountGR.setValue("id", jsonDynamicDataP["additional.docusign_account_id"]);
   accountGR.insert();
})(aliasId, connectionSysId, jsonDefaultData, jsonDynamicData);
```

結果の **Docusign** 接続および資格情報の構成フォーム

ユーザーが関連する Docusign 接続および資格情報エイリアスに移動して [新しい接続と資格情報の作成] を選択すると、次のダイアログが表示されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



自動翻訳

構成テンプレートの作成

スポークの設定に必要な入力を定義するテンプレートを作成します。静的なキーと値のペアを設定してレコードを作成し、すべてのデータ連携に適用される値を設定します。動的なキーと値のペアを設定してユーザー入力を収集し、さまざまなフィールド値を設定します。このテンプレートを使用すると、管理者およびフロー設計者は単一のフォームからスポークを設定できます。

始める前に
必要なロール：adminまたはアクションデザイナー

手順

1. 移動先 すべて > 統合ハブ > 接続 **&** 認証情報 > 構成テンプレート.

2. [新規] をクリックします。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

3. 作成する構成テンプレートのタイプを選択します。タイプを選択すると、テンプレートの構成に役立つスターターデータが提供されます。

4. [名前] フィールドに、テンプレートを識別するための名前を追加します。

5. [デフォルトのデータテンプレート] フィールドで必要な変更を行います。このフィールドで、すべてのデータ連携に適用される静的情報を設定します。たとえば、値がすべてのデータ連携に適用される場合は、API およびトークンの URL を設定できます。

   デフォルトのデータテンプレートにある次のオブジェクトは必須です。

   - `credential`：必須フィールドを持つ資格情報レコードを作成します。
   - `connection`：必須フィールドを持つ接続レコードを作成します。`extended_attributes` 子オブジェクトを使用して接続属性にアクセスします。たとえば、

```
"connection": {
        "extended_attributes": {
           "api_version": "v1"

        },
     "connection_url": "https://<provider-domain-name>.com",
     "name": "Spoke Connection",
     "table": "http_connection"
  }
```

   `additional` オブジェクトを使用してカスタムテーブルのデータを設定し、後処理スクリプトを使用してデータをテーブルに挿入できます。

   注:
   OAuth 認証コード権限許可タイプのデフォルトのデータテンプレートでは、`oauth_entity_profile_scope` キーと `oauth_entity_scope` キーの値が一致する必要があります。次の例では、両方のキーが `[Read user's email]` 値を持ちます。

```
"oauth_entity_profile": [
      {
       "grant_type": "authorization_code",
       "name": "<provider-name> Profile",
       "default": true,
       "oauth_entity_profile_scope": [
        "Read user's email"
       ]
      }
     ],
     "code_challenge_method": "S256",
     "type": "consumer",
     "oauth_entity_scope": [
      {
       "oauth_entity_scope": "Read user's email",
       "name": "email"
      }
     ],
```

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

6. [動的なデータスキーマ] フィールドで必要な変更を行います。このフィールドは統合を設定するためにユーザーが完了する必要のある情報を定義します。たとえば、ユーザー名とパスワードのキーと値のペアを追加して、ユーザー定義の値を収集することができます。

   動的なデータスキーマのフィールドには、次のプロパティが含まれます。

   - name：ユーザーの入力がマッピングされるフィールドです。たとえば、ユーザー入力を接続レコードの [接続 URL] フィールドにマッピングするには、「connection.connection_url」と入力します。
   - label：テンプレートの完成時にユーザーに表示されるフィールドラベルです。
   - type：フィールドタイプです。このデータタイプが、値をマッピングするフィールドのデータタイプと一致することを確認してください。
   - defaultValue：オプションです。このフィールドのデフォルト値です。デフォルトが指定されていない場合は、ヒントが表示されます。
   - hint：オプションです。デフォルト値がない場合に表示されるヒントテキストです。

   注:
   OAuth JWT ベアラー権限許可タイプ認証用のテンプレートを設定する場合は、jwt_claim_validation アレイ内の単一のキーと値のペアに対するユーザー入力が必要になる場合があります。アレイ内のインデックスを参照することで、動的なデータスキーマ内の単一のキーと値のペアを参照できます。たとえば、デフォルトのデータテンプレートにはこのスニペットが含まれている場合があります。

   ```
   "jwt_claim_validation" : [ {
         "name" : "iss",
         "is_standard" : true,
         "data_type" : "string",
         "value":"<docusign-iss-claim>"
       }, {
         "name" : "sub",
         "is_standard" : true,
         "data_type" : "string",
         "value":"<docusign-sub-claim>"
       }, {
         "name" : "aud",
         "is_standard" : true,
         "data_type" : "string",
         "value":"<docusign-aud-claim>"
       }, {
         "name" : "scope",
         "is_standard" : false,
         "data_type" : "string",
         "value" : "signature impersonation"
       } ],
   ```

   アイテムのゼロベースのインデックス (credential.jwt_provider.jwt_claim_validation[0].value) を使用して、iss キーと値のペアを参照します。

7. オプション: [後処理スクリプト] フィールドに、統合によって必要とされる追加のレコードを作成します。たとえば、スポークにカスタムテーブルが含まれている場合は、構成テンプレートのユーザー入力に基づいてそれらのテーブルにレコードを作成できます。このスクリプトは、接続と資格情報レコードが作成された後に実行されます。のスクリプトを追加します
   後処理スクリプトは、次のグローバルオブジェクトにアクセスできます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

グローバルオブジェクト	説明
aliasId	接続および資格情報エイリアス [sys_alias] テーブルのエイリアスレコードの sys_id
connectionSysId	テンプレートによって作成された接続レコードの sys_id
jsonDefaultData	文字列形式の [デフォルトのデータテンプレート] フィールドの JSON コンテンツ
jsonDynamicData	文字列形式の [動的データテンプレート] フィールドの JSON コンテンツ

8. [事前編集スクリプト **(Pre-Edit Script)]** フィールドで、接続を編集するときの追加のフィールドを事前入力するスクリプトを追加します。このスクリプトではオブジェクトのアレイが返されます。オブジェクトごとに、追加フィールドを設定するための名前と値のペアがあります。たとえば、接続にカスタムテーブル内のフィールドが必要な場合は、そのフィールドをカスタムテーブルにマッピングできます。
事前編集スクリプトがアクセスできるグローバルオブジェクトは次のとおりです。

グローバルオブジェクト	説明
aliasId	接続および資格情報エイリアス [sys_alias] テーブルのエイリアスレコードの sys_id
connectionSysId	テンプレートによって作成された接続レコードの sys_id
jsonDefaultData	文字列形式の [デフォルトのデータテンプレート] フィールドの JSON コンテンツ
jsonDynamicData	文字列形式の [動的データテンプレート] フィールドの JSON コンテンツ

スクリプト内の各オブジェクトには、次のプロパティがあります。

- `name`：接続の値を指定するカスタムフィールドの名前。
- `value`：カスタムフィールドに入力するマッピング対象の値。関数または変数を使用するか、またはハードコーディングすることによって、フィールドをマッピングできます。

フィールドに対してサポートされているデータタイプは次のとおりです。

フィールドに対してサポートされるデータタイプ

タイプ	説明
テキスト	文字列値。
ブーリアン	選択ボックス。選択されている場合は true、選択されていない場合は false の値を示します。
番号	数値。
日付	yyyy-mm-dd 形式の日付の値。GlideDate オブジェクトを使用することもできます。
選択肢	[動的なデータスキーマ] フィールドで定義されている有効な選択肢のリスト。
参照	有効な GlideRecord。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

タイプ	説明
ラジオ グループ	さまざまなフィールドのセットを含むグループ。これらのグループは、接続を編集するときのドロップダウンリストの選択肢として使用できます。ドロップダウンリストから必要なグループを選択すると、各グループのフィールドが表示されます。 たとえば、[動的なデータスキーマ] フィールドで定義された次の構造のラジオグループを考えてみましょう。 `{ "name": "radio_groups", "label": "Radio Groups", "type": "radio", "groups": [{ "name": "radio_group1", "label": "Radio Group 1", "fields": [{ "name": "radio_field1", "label": "Radio Field 1", "type": "text", "defaultValue": "efgh", "mandatory": true }] }, { "name": "radio_group2", "label": "Radio Group 2", "fields": [{ "name": "radio_field2", "label": "Radio Field 2", "type": "text", "defaultValue": "abcd", "mandatory": true }], "default_group": true }`  この例では、次のコードスニペットを使用して、ラジオグループがどのようにドット連結を使用してスクリプト内で使用されているかを理解できます。  `{ name: "radio_field.first_radio_group.radio_field1", value: "radio field 1" }, { name: "radio_field.second_radio_group.radio_field2", value: "radio field 2" }, { name: “radio_groups”, value: gr.getValue(‘radio_groups’) }` ドット連結の使用方法の詳細については、「ドット連結」を参照してください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ヒント:
事前設定された値が接続の編集中にフィールドに表示されない場合は、 システム診断 > セッションのデバッグ > デバッグログ 問題を診断します。

9. テンプレートを接続および資格情報エイリアスに追加します。
   a. 移動先 統合ハブ > 接続 & 認証情報 > 接続 & 資格情報エイリアス.
   b. スポークのエイリアスレコードを開きます。
   c. [構成テンプレート] フィールドで、ルックアップアイコンをクリックします。
   d. 作成したテンプレートをリストから選択します。
   e. [更新] をクリックします。

タスクの結果
ユーザーが関連する接続および資格情報エイリアスに移動して [新しい接続 & 資格情報の作成] を選択すると、ユーザー入力を取得するダイアログが表示されます。OAuth 認証コード権限許可タイプのテンプレートを作成した場合は、このダイアログから OAuth トークンを取得することもできます。

次のタスク
関連する接続および資格情報エイリアスに移動し、[新しい接続 & 資格情報の作成] を選択して、テンプレートをテストします。ダイアログが必要なデータを収集し、システムに必要なレコードを作成することを確認します。

接続を開始

接続テーブルを使用して、ターゲットホストへの基本接続、JMS 接続、JDBC 接続、または HTTP(s) 接続を設定します。

接続テーブル

接続テーブル (sys_connection) は、すべての接続テーブルの基本テーブルです。次のプロトコルの接続を設定できます。

- PowerShell および SSH 用の基本接続
- JDBC
- JMS
- HTTP(S)

接続テーブルは、接続エイリアステーブルを参照します。これにより、接続エイリアスが接続情報に結合されます。接続ごとに次の情報が記録されます。

基本接続のプロパティ

フィールド	説明
名前	接続の名前。このフィールドは、テーブル上で一意でなければなりません。
資格情報	この接続で使用する資格情報を指定します。これはオプションです。
接続エイリアス	接続エイリアスにより、実行時に接続と資格情報が解決されます。接続エイリアスごとに一度に 1 つの接続のみアクティブになります。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

基本接続のプロパティ (続く)

フィールド	説明
アクティブ	この接続をアクティブにする場合はオンにします。
ドメイン	接続が属するドメイン。

空でない場合、認証情報は有効な接続全体で一意です。

接続情報のアップグレード

- JDBC 接続 [jdbc_connection] テーブルと JMS 接続[orch_jms_ds] テーブルは、既存のオーケストレーション接続テーブルであり、接続 [sys_connection] テーブルから拡張されています。テーブルは本来、sys_metadata から拡張されています。sys_metadata 関連データは削除されます。
- テーブルは、オーケストレーション ランタイム プラグイン [com.snc.runbook_automation.runtime] から [認証情報 & 接続] プラグインに移動します。
- アップグレード プロセスでは、JDBC および JMS 接続情報が取得され、対応する接続エイリアスが作成され、対応する接続にそのエイリアスが割り当てられます。
- JDBC フィールド名の変更：
  - JDBC サーバーの名前が host に変更されました
  - データベース ポートの名前が port に変更されました
  - アップグレード時に JDBC サーバーおよびデータベースのデータが host および port に移行されました

PowerShell および SSH 用の基本接続の作成

PowerShell または Secure Shell (SSH) プロトコルを使用するカスタムアクティビティまたはアクションで使用する接続情報を設定します。

始める前に

必要なロール：admin または connection_admin

手順

1. 移動先 すべて > 認証情報 **&** 接続 > 接続.
2. [新規] をクリックします。
3. **[PowerShell** および **SSH** 用の基本接続] を選択します。
4. フォームに入力します。

フィールド	説明
名前	接続レコードの一意の名前。
資格情報	接続を許可するために使用する資格情報レコードを選択します。
接続エイリアス	この接続に関連付けるエイリアス レコードを選択します。エイリアスを使用すると、エイリアスを使用するアクションまたはアクティビティを再設定することなく、接続レコードを更新できます。
ホスト	アクティビティまたはアクションが実行されるターゲット ホストの完全修飾ドメイン名。たとえば、host.domain.com です。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
有効	この接続を有効にする場合に選択します。
ドメイン	アクティビティが実行されるドメインを決定します。フロー デザイナーでは、ドメイン分離がサポートされていないため、このフィールドは無視されます。
Override default port (デフォルトポートに上書きする)	接続で使用されるターゲット ポート。このフィールドを空白のままにすると、デフォルトのポート値が使用されます。
MID サーバーを使用する	MID サーバー を介してターゲット ホストに接続する場合に選択します。選択した場合、[MID Server 詳細設定] セクションでフィールドを定義します。 **注:** PowerShell には MID サーバー が必要です。
MID 選択	特定の MID Server または MID クラスターを選択するオプション。 ○ **MID Server** の自動選択：MID Server を自動的に選択します。 ○ 特定の **MID Server**：選択した MID Server を使用します。 ○ 特定の **MID** クラスター：選択した MID クラスターを使用します。 このフィールドは、**[MID Server** を使用] のチェックがオンの場合に利用可能です。 **注:** オーケストレーション 接続レコードではなく、統合ハブ 接続レコードが参照されていることを確認してください。
できること	MID サーバーが選択対象となるためにサポートする必要がある機能です。選択した機能をサポートする MID サーバーからアクションまたはアクティビティが実行されます。**[MID Server** を使用] が選択されている場合のみ表示されます。 必要な機能によって、実行時にどのMID サーバーが選択されるかが決定されます。実行時に MID サーバー が選択される方法の詳細については、「MID Server の選択」を参照してください。このフィールドは、MID 選択リストから **[MID Server** の自動選択] が選択されている場合にのみ表示されます。
MID アプリケーション	MID サーバーが選択対象となるためにサポートする必要があるアプリケーションです。選択したアプリケーションをサポートする MID サーバーからアクションが実行されます。**[MID Server** を使用] が選択されている場合のみ表示されます。 実行時にMID サーバーがどのように選択されるかについての詳細は、「MID Server selection」を参照してください。
MID Server	ステップが実行される特定の MID サーバー です。このフィールドは、MID 選択リストから [特定の **MID Server]** が選択されている場合にのみ表示されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
MID クラスター	使用する特定の MID クラスター。このフィールドは、**[MID Server** を使用] チェックボックスがオンになっていて、MID 選択リストから [特定の **MID** クラスター] が選択されている場合に利用可能です。

5. [送信] をクリックします。

HTTP(S) 接続を作成

HTTP(S) 接続は、カスタム HTTP(S) アクションまたはアクティビティが接続に使用する情報を提供します。

始める前に
必要なロール：connection_admin

手順

1. 移動先 すべて > 認証情報 **&** 接続 > 接続をクリックし、[新規] をクリックして [**HTTP(s)** 接続] を選択します。
2. 次の接続情報を追加して [送信] をクリックします。

フィールド	説明
名前	この HTTP(S) 接続の一意の名前。
資格情報	接続を許可するために使用する資格情報レコードを選択します。
接続エイリアス	この接続に関連付けるエイリアス レコードを選択します。エイリアスを使用すると、エイリアスを使用するアクションまたはアクティビティを再設定することなく、接続レコードを更新できます。
URL ビルダー	手動で接続 URL を入力するか、システムを使用して入力に基づいて URL を作成します。デフォルトはオフです。オンにすると、次のフィールドから接続 URL が計算されます。 ○ [相互認証] - 相互認証を使用する場合はオンにします。 ○ [プロトコル] - 相互認証を使用しない場合は、プロトコルを入力します。デフォルトは HTTPs です。 ○ [プロトコル プロファイル] - 相互認証を使用する場合は、sys_protocol_profile からプロトコル プロファイルを入力します。 ○ ホスト ○ ポート ○ ベースパス - 接続文字列のパス。 **注:** 相互認証をオンにした場合は、接続 URL が作成されます (プロトコル + :// + host:port +URL)。相互認証をオフにした場合は、接続 URL が作成されます (プロトコル プロファイル + :// + host:port +URL)。
接続 URL	URL ビルダーをオフにした場合は、このフィールドに接続 URL を入力します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	注: 相互認証をオンにした場合は、接続 URL が作成されます (プロトコル + :// + host:port +URL)。相互認証をオフにした場合は、接続 URL が作成されます (プロトコル プロファイル + :// + host:port +URL)。
アクティブ	この接続を有効にする場合にオンにします。
ドメイン	アクションまたはアクティビティが実行されるドメインを決定します。
MID Server を使用	このアクションまたはアクティビティで MID Server を使用するには、オンにします。選択した場合、[MID Server 詳細設定] セクションでフィールドを定義します。
MID 選択	特定の MID Server または MID クラスターを選択するオプション。 ○ **MID Server** の自動選択：MID Server を自動的に選択します。 ○ 特定の **MID Server**：選択した MID Server を使用します。 ○ 特定の **MID** クラスター：選択した MID クラスターを使用します。 このフィールドは、**[MID Server** を使用] のチェックがオンの場合に利用可能です。 **注:** オーケストレーション 接続レコードではなく、統合ハブ 接続レコードが参照されていることを確認してください。
できること	MID サーバーが選択対象となるためにサポートする必要がある機能です。選択した機能をサポートする MID サーバーからアクションまたはアクティビティが実行されます。**[MID Server** を使用] が選択されている場合のみ表示されます。 必要な機能によって、実行時にどのMID サーバーが選択されるかが決定されます。実行時に MID サーバー が選択される方法の詳細については、「MID Server の選択」を参照してください。このフィールドは、MID 選択リストから **[MID Server** の自動選択] が選択されている場合にのみ表示されます。
MID アプリケーション	MID サーバーが選択対象となるためにサポートする必要があるアプリケーションです。選択したアプリケーションをサポートする MID サーバーからアクションが実行されます。**[MID Server** を使用] が選択されている場合のみ表示されます。 実行時にMID サーバーがどのように選択されるかについての詳細は、「MID Server selection」を参照してください。
MID Server	ステップが実行される特定の MID サーバー です。このフィールドは、MID 選択リストから [特定の **MID Server]** が選択されている場合にのみ表示されます。
MID クラスター	使用する特定の MID クラスター。このフィールドは、**[MID Server** を使用] チェックボックスがオンになっていて、MID 選択リストから [特定の **MID** クラスター] が選択されている場合に利用可能です。
接続タイムアウト	システムがホスト接続の成功を待機するミリ秒数。この間に接続が成功しない場合、接続要求はタイムアウトします。システムのデフォルトの接続タイムアウト値を使用するには、このフィールドを空のままにします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

3. [送信] をクリックします。
   これで、カスタム HTTP(S) アクションまたはアクティビティを作成する準備ができました。

JDBC 接続を作成

JDBC 接続は、カスタム JDBC アクションまたはアクティビティがさまざまなターゲット データベースへの接続に使用する情報を提供します。

始める前に

インスタンスに付属するかどうかに関係なく、適切な JAR ファイル、またはカスタム JAR ファイルが必要です。

注:
ServiceNow インスタンスでは、mysql-connector-java-5.1.21.jar、sql-server-jdbc-4.0.jar、および ojdbc6.jar の各ファイルが現在のリリースの一部として提供され、MySQL、SQLServer、および Oracle データベースをサポートしています。Sybase や DB2 Universal などの他のデータベースでは、カスタム JAR ファイルを使用する必要があります。このファイルは、JDBC 接続を設定する前にインスタンスにアップロードする必要があります。

必要なロール：connection_admin

このタスクについて

JDBC 資格情報は、アクティビティデザイナーテンプレートによって別々に取得され、CyberArk などの外部認証情報ストレージをサポートします。

手順

1. 移動先 すべて > 認証情報 **&** 接続 > 接続をクリックし、「 新規 」をクリックして 「JDBC 接続」を選択します。
2. テーブル内のフィールドを使用して、フォームに入力します。
   [フォーマット] フィールドのデータベース選択により、利用可能なフィールドが決定されます。

JDBC 接続フィールド

フィールド	データベース形式	説明
名前	すべて	この JDBC 接続の一意の名前。たとえば、**JDBC MySQLProd** を入力します。
資格情報	すべて	JDBC プロバイダーの資格情報を追加します。
接続エイリアス	すべて	この接続に関連付けるエイリアス レコードを選択します。エイリアスを使用すると、エイリアスを使用するアクションまたはアクティビティを再設定することなく、接続レコードを更新できます。
クエリー タイムアウト	すべて	JDBC クエリが応答なしで実行される最大経過時間。
接続タイムアウト	すべて	システムが JDBC 接続の成功を待機する秒数。この間に接続が成功しない場合、接続要求はタイムアウトします。システムのデフォルトの接続タイムアウト値を使用するには、このフィールドを空のままにします。
有効	すべて	これを有効な接続にするには、オンにします。
ドメイン	すべて	このテーブルのドメイン。デフォルトでは、グローバル ドメインで JDBC 接続 [jdbc_connection] テーブルが実行されます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

フィールド	データベース形式	説明
フォーマット	すべて	この接続のデータベース タイプ。デフォルトの選択肢は次のとおりです。 ○ **MySQL** ○ **Oracle** ○ **SQLServer** ○ なし 適切な JDBC ドライバー JAR ファイルをインスタンスにアップロードすることで、**[Sybase]** または **[DB2 Universal]** を選択リストに追加できます。オーケストレーション は、これらのドライバーがシステムにロードされると自動的に認識し、このリストに追加します。
ホスト	Oracle、MySQL、SQLServer	データベース サーバーのホスト名または IP アドレス。
Oracle SID	Oracle	Oracle データベース サイトの識別子。デフォルト値は **orcl** です。
Oracle ポート	Oracle	Oracle データベースが使用しているポート。デフォルト値は **1521** です。
データベース名	MySQL、SQLServer	データベースの名前。
ポート	MySQL、SQLServer	選択したデータベースが使用しているポート。
インスタンス名	SQLServer	選択した SQLServer のインスタンス名
接続 URL	すべて	指定したデータベースへの接続に MID Server が使用する URL。この URL は、フォームを保存したときに自動的に作成され、デフォルトのデータベースでは読み取り専用になります。 **注:** 選択した形式がデフォルトのデータベースのものでない場合は、接続 URL を手動で作成して、MID Server が接続の作成方法を認識できるようにする必要があります。
JDBC ドライバー	なし、DB2 Universal、Sybase	デフォルトのデータベースでない場合にこの接続に使用する JDBC ドライバー。 **注:** Sybase または DB2 Universal Database を追加する場合、このフィールドにドライバー名を入力して、そのドライバー JAR ファイルをインスタンスにアップロードする必要があります。
MID Server を使用	すべて	このアクションまたはアクティビティで MID Server を使用するには、オンにします。選択した場合、[MID Server 詳細設定] セクションでフィールドを定義します。
MID 選択	すべて	特定の MID Server または MID クラスターを選択するオプション。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	データベース形式	説明
		○ **MID Server** の自動選択：MID Server を自動的に選択します。 ○ 特定の **MID Server**：選択した MID Server を使用します。 ○ 特定の **MID** クラスター：選択した MID クラスターを使用します。 このフィールドは、**[MID Server** を使用] のチェックがオンの場合に利用可能です。 **注:** オーケストレーション 接続レコードではなく、統合ハブ 接続レコードが参照されていることを確認してください。
できること	すべて	MID サーバーが選択対象となるためにサポートする必要がある機能です。選択した機能をサポートする MID サーバーからアクションまたはアクティビティが実行されます。**[MID Server** を使用] が選択されている場合のみ表示されます。 必要な機能によって、実行時にどのMID サーバーが選択されるかが決定されます。実行時に MID サーバー が選択される方法の詳細については、「MID Server の選択」を参照してください。このフィールドは、MID 選択リストから **[MID Server** の自動選択] が選択されている場合にのみ表示されます。
MID アプリケーション	すべて	MID サーバーが選択対象となるためにサポートする必要があるアプリケーションです。選択したアプリケーションをサポートする MID サーバーからアクションが実行されます。**[MID Server** を使用] が選択されている場合のみ表示されます。 実行時にMID サーバーがどのように選択されるかについての詳細は、「MID Server selection」を参照してください。
MID Server	すべて	ステップが実行される特定の MID サーバー です。このフィールドは、MID 選択リストから [特定の **MID Server]** が選択されている場合にのみ表示されます。
MID クラスター	すべて	使用する特定の MID クラスター。このフィールドは、**[MID Server** を使用] チェックボックスがオンになっていて、MID 選択リストから [特定の **MID** クラスター] が選択されている場合に利用可能です。

3. [送信] をクリックします。

関連情報

JDBC 認証情報

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

JMS 接続の作成

カスタム JMS アクティビティまたはアクションで Java Messaging Service (JMS) を使用するようにシステムを設定します。

始める前に

必要なロール：connection_admin

このタスクについて

MID Serverには、組織に適切な JMS 接続ファクトリーが必要です。プロパティで *mid.property.jms.command.allowed_factory_names* これらの値を設定します。 **MID** サーバー > プロパティ. このプロパティのデフォルト値は、サードパーティの JMS プロバイダーが通知する任意の値またはカンマ区切りの値リストに変更できます。

手順

1. 移動先 認証情報 **&** 接続 > 接続.
2. [新規]をクリックして **[JMS** 接続] を選択し、フォームに入力して [送信] をクリックします。

オプション	説明
名前	この接続ファクトリーの一意の名前。
資格情報	JMS プロバイダーの認証情報を追加します。
接続エイリアス	この接続に関連付けるエイリアス レコードを選択します。エイリアスを使用すると、エイリアスを使用するアクションまたはアクティビティを再設定することなく、接続レコードを更新できます。
初期コンテキスト ファクトリー	InitialContext の作成に使用する JNDI クラスの名前。 **注:** たとえば、ActiveMQ V5.10 (JMS プロバイダー) に接続する場合、値は org.apache.activemq.jndi.ActiveMQInitialContextFactory です。
プロバイダー URL	実行中の JMS プロバイダーのインストールの場所。 **注:** たとえば、ActiveMQ V5.1 に接続するには、tcp：//ipAddressOrHostName：61616になります。
有効	これを有効な接続にするには、オンにします。
ドメイン	アクションまたはアクティビティが実行されるドメインを決定します。
MID Server を使用	このアクションまたはアクティビティで MID Server を使用するには、オンにします。選択した場合、[MID Server 詳細設定] セクションでフィールドを定義します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

オプション	説明
MID 選択	特定の MID Server または MID クラスターを選択するオプション。 ○ **MID Server** の自動選択：MID Server を自動的に選択します。 ○ 特定の **MID Server**：選択した MID Server を使用します。 ○ 特定の **MID** クラスター：選択した MID クラスターを使用します。 このフィールドは、**[MID Server** を使用] のチェックがオンの場合に利用可能です。
MID クラスター	使用する特定の MID クラスター。このフィールドは、**[MID Server** を使用] チェックボックスがオンになっていて、MID 選択リストから [特定の **MID** クラスター] が選択されている場合に利用可能です。
機能	MID サーバーが選択対象となるためにサポートする必要がある機能です。選択した機能をサポートする MID サーバーからアクションまたはアクティビティが実行されます。**[MID Server** を使用] が選択されている場合のみ表示されます。 実行時にMID サーバーがどのように選択されるかについての詳細は、「MID Server selection」を参照してください。
MID アプリケーション	MID サーバーが選択対象となるためにサポートする必要があるアプリケーションです。選択したアプリケーションをサポートする MID サーバーからアクションが実行されます。**[MID Server** を使用] が選択されている場合のみ表示されます。 実行時にMID サーバーがどのように選択されるかについての詳細は、「MID Server selection」を参照してください。

3. 移動先 接続 **&** 認証情報 > 認証情報.
4. [新規]をクリックして **[JMS** 認証情報] を選択し、 MID で JMS プロバイダーとの通信に使用されるユーザー名とパスワードを入力します。
   詳細については、「JMS 資格情報」を参照してください。
5. [送信] をクリックします。
   これで、カスタム JMS アクションまたはアクティビティを作成する準備ができました。

IntegrationHub の接続属性を作成

統合ハブ統合ステップで使用できる接続固有の変数を定義します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

始める前に
必要なロール：

- 接続属性を作成するには、admin ロールが必要です。
- 属性値を割り当てるには、connection_admin または admin ロールが必要です。
- カスタム アクションで属性を使用するには、action_designer または admin ロールが必要です。

接続属性は、統合ステップでのみ使用され、統合ハブ に対するサブスクリプションが必要です。のアクティブ化 統合ハブの詳細については、 を要求する 統合ハブ プラグイン.

このタスクについて
統合ステップを使用する場合は、外部システムとの接続を確立する必要があります。接続をインラインで定義する代わりに、接続 & 資格情報エイリアスを使用します。エイリアスを使用すると、すべてのアクションを再設定することなく、接続の詳細を 1 回で更新できます。エイリアスを使用するアクション ステップは、エイリアスに関連付けられた属性を継承します。フローデザイナーには、アクション ステップにドラッグできるデータ ピルとして属性が表示されます。たとえば、REST ステップのクエリー パラメーターになるページ サイズ属性を作成できます。

カスタム フローデザイナー アクションの構築の詳細については、次を参照してください アクションデザイナー.

手順

1. 移動先 すべて > 認証情報 **&** 接続 > 接続 **&** 資格情報エイリアス.
2. エイリアス レコードを作成または選択します。
3. 接続属性関連リストから、[新規] をクリックします。
4. 属性ラベルとフィールド タイプを定義します。
   フィールドタイプのリストについては、「フィールドタイプ」を参照してください。
5. [詳細ビュー] 関連リンクをクリックして、属性のディクショナリー詳細設定を設定します。
   たとえば、動的に計算された値を持つ属性を作成するには。「辞書エントリフォーム」を参照してください。
6. [送信] をクリックします。
7. 接続レコードで属性値を定義します。

   a. 移動先 認証情報 **&** 接続 > 接続.

   b. エイリアスと同じ接続タイプの接続レコードを作成または選択します。

   c. [接続エイリアス] で、接続属性を持つエイリアスを選択します。

   d. レコードを保存します。
      [属性] タブに、エイリアス レコードで定義された接続属性が入力されます。

   e. 属性の値を設定します。
      エイリアスで [複数のアクティブな接続をサポート] が有効になっている場合、複数の接続レコードをエイリアスに関連付けて、接続レコードごとに属性値を定義することができます。同じエイリアスの属性値を持つ接続レコードが複数ある場合は、 フローが実行されるときに使用される接続によって属性値が決まります。たとえば、production と test という 2 つのアクティブ接続エンドポイントを持つエイリアスを使用するアクションが 1 つあるとします。この属性は、実行時に使用される接続によって定義された値に解決されます。

8. アクションデザイナー の統合ステップにエイリアスを追加します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

a. フローデザイナー に移動して、アクションを作成または選択します。

b. <アクションに統合ステップを追加します。

c. [接続の詳細] で、属性を作成したエイリアスを追加します。

エイリアスに関連付けられている接続属性が、[データ] ペインにデータ ピルとして表示されます。

> **注:**
> エイリアスをステップに関連付けると、接続属性ラベルおよびデータタイプの変更は追跡されません。接続属性ラベルまたはデータタイプをリフレッシュするには、ステップからエイリアスを削除して再度追加します。

認証情報の開始

MID Server では、認証情報 [discovery_credentials] テーブルで作成した認証情報を使用して、ディスカバリー、オーケストレーション、サービス マッピング、およびクラウド管理のリソースにアクセスします。

MID Server が資格情報を使用する仕組み

デフォルトでは、Windows MID Server は、ホストマシン上の MID Server サービスのログイン資格情報を使用して、ネットワーク内の Windows デバイスを検出します。Windows MID Server サービス資格情報を設定 して、最低限ローカル管理者権限を持つようにする必要があります。UNIXマシンとネットワークデバイスの場合Linux、MID Server は次のインスタンスで構成された SSH および SNMP 資格情報を使用します。 ディスカバリー > 資格情報.

オーケストレーション で使用される MID Server には、[ワークフローアクティビティ] で指定されているとおり、ネットワーク内のコンピューター上でコマンドを実行するために必要な資格情報へのアクセス権が必要です。Orchestration では、ディスカバリー と同じ SSH および SNMP 資格情報を使用できますが、特定のワークフローアクティビティ用に設計された 2 つの追加資格情報：Windows (PowerShell アクティビティ 用) と VMware があります。

暗号化と復号化

プラットフォームでは、資格情報 [discovery_credentials] テーブルの暗号化フィールドに資格情報を保存します。認証情報が入力されると、認証情報は表示できません。

MID Server によって資格情報が要求されると、Now Platform で次のプロセスを使用して資格情報が復号化されます。

1. password2 固定キーを使用してインスタンスに対して認証情報が復号化されます。
2. 資格情報は、MID Server の公開鍵を使用してインスタンス上で再暗号化されます。
3. 資格情報は、SSL を使用してロード バランサー上で暗号化されます。
4. 資格情報は、SSL を使用して MID Server 上で復号化されます。
5. 資格情報は、MID Server の秘密鍵を使用して MID Server 上で復号化されます。

> **注:**
> プラットフォームには、マルチテナント インスタンス用の個別の暗号鍵はありません。

資格情報の順序

認証情報には、 [Credentials Form] (認証情報フォーム) の順序値を割り当てることができます。これにより、特定の順序ですべての認証情報をアプリケーションで自由に試行させることができ

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

ます。順序値を指定しない場合、アプリケーションは、有効な資格情報が見つかるまで、資格情報 [discovery_credential] テーブルの資格情報をランダムに試行します。たとえば、次の場合です。

- Orchestration は、Linux マシンや UNIX マシンなどの SSH サーバーでコマンドを実行しようとします。
- Discovery は、プリンター、ルーター、UPS などの SNMP デバイスのクエリーを試行します。

デバイスの資格情報を特定した後、ディスカバリー とオーケストレーションでは、資格情報親和性 [dscy_credentials_affinity] テーブルを使用して資格情報とデバイス間の親和性が作成されます。後続のすべての検出またはオーケストレーション アクティビティで、このテーブルの資格情報が、親和性が存在するデバイスと照合されます。デバイスの資格情報が変更された場合、 ディスカバリー とオーケストレーションでは、新しい親和性を作成するまで利用可能な資格情報をすべて再試行します。

注:
オーケストレーションと ディスカバリー がインストールされ、資格情報エイリアスが有効になっている場合、複数の親和性が存在する可能性があります。この場合、プラットフォームでは、親和性ごとに資格情報が検索され、順序が最も低い親和性の資格情報がプローブに挿入されます。

認証情報の順序付けは、次の場合に役立ちます。

- 認証情報テーブルには多くの認証情報が含まれており、一部の認証情報が他の認証情報よりも頻繁に使用される場合があります。たとえば、テーブルに 150 個の SSH 資格情報が含まれていて、そのうちの 5 個がデバイスの 90% へのログインに使用されている場合は、その 5 個の資格情報の順序値を小さくすることをお勧めします。これにより、その 5 個が実行リストの最上部に配置されます。このようにして、よく使用する資格情報が最初に試行されると、ディスカバリー および Orchestration の動作がより迅速になります。最初の接続に成功した後、Now Platform によりデバイスごとに次回使用する資格情報が認識されます。
- Now Platform には、積極的なログインセキュリティがあります。たとえば、ネットワーク内の Solaris データベースサーバーが、ログイン試行を 3 回失敗すると MID Server からロックアウトされる場合は、データベース資格情報の順序値を小さくします。

資格情報エイリアス

資格情報エイリアスは Discovery と Orchestration で使用できます。

Discovery にエイリアスを使用すると、管理者は以下の操作が可能です。

- 設定可能なコンプライアンスレベルで資格情報フィルタリング動作を使用します。
- 複数の資格情報エイリアスを検出スケジュールに割り当てます。
- 不適切な資格情報や機密の資格情報を使用する資格情報親和性の作成を防止します。詳細については、「資格情報親和性」を参照してください。

Orchestration にエイリアスを使用すると、ワークフロー作成者は以下の操作が可能です。

- 個々の認証情報をオーケストレーション ワークフローの任意のアクティビティに割り当てる。
- 個々の資格情報をフロー デザイナーの任意のアクションに割り当てる。
- オーケストレーション ワークフローで同じアクティビティ タイプが発生するたびに異なる資格情報を割り当てる。
- デザイナー フローで同じアクションが発生するたびに異なる認証情報を割り当てる。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

外部の認証情報ストア

インスタンスに資格情報を保存しない場合は、外部の資格情報リポジトリを使用できます。外部の認証情報ストアにより、インスタンスによってアクセスできる外部サイトに認証情報が保存されます。CyberArk は、サポートされている唯一の外部認証情報ストアです。ただし、ServiceNow API を使用して他の外部ストアを構成することもできます。

接続情報および認証情報エイリアスの作成

資格情報または接続情報レコードにラベルを付けるエイリアスを定義します。

始める前に

必要なロール：

- エイリアスを作成するには、admin ロールが必要です。
- credential_admin ロールと connection_admin ロールには、エイリアス レコードへの読み取りアクセス権があります。

このタスクについて

接続 & 認証情報エイリアスは、認証情報または接続レコードにラベルを付けるエイリアスを定義します。エイリアスには次のフィールドが含まれています。

手順

1. 移動先 すべて > 接続 **&** 認証情報 > 接続 **&** 資格情報エイリアス.
2. [新規] をクリックします。
3. フォームのフィールドに入力します。

接続および資格情報エイリアス

フィールド	説明
名前	エイリアスの名前。エイリアスには、英数字とアンダースコアだけを使用できます。 アップグレード時に、認証情報レコードのタグが接続 & 認証情報エイリアスに移行します。資格情報タグに英数字とアンダースコア以外の特殊文字が含まれている場合、タグ名はアップグレード後も保持されます。この移行されたエイリアスは引き続き使用できますが、名前を変更して命名の制限を満たすまでエイリアスを更新することはできません。
ID	形式 scope_name.alias_name に基づく、接続および資格情報エイリアスの一意の識別子です。 ○ スコープがグローバルである場合、ID はエイリアス名です。たとえば、グローバルスコープで作業日エイリアスを作成すると、ID は workday に設定されます。 ○ HR アプリケーションスコープで作業日エイリアスを作成すると、ID は x_hr_app.workday に設定されます。
タイプ	[資格情報] または [接続と資格情報] を選択します。デフォルトは [接続と認証情報] です。
アプリケーション	接続および資格情報エイリアスの割り当て対象のアプリケーションスコープです。アプリケーションピッカーで最後に選択した現在のセッションスコープが表示されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	○ たとえば、[グローバル] がこのセッションの現在のスコープである場合はそのように表示されます。 ○ エイリアスを作成する前に、アプリケーションピッカーでスコープを変更できます。アプリケーションスコープおよびその選択方法の詳細については、以下を参照してください。 ▪ アプリケーションスコープ ▪ アプリケーション ピッカーからのアプリケーションの選択
接続タイプ	接続タイプの名前 (基本、HTTP、JDBC、JMS、または Kafka)。デフォルトは [HTTP] です。
複数の有効な接続をサポート	エイリアスが複数の有効な接続をサポートするかどうかを指定する指定子です。接続テーブルを使用して接続を追加し、接続関連リストを使用してその接続をエイリアスに関連付けます。
デフォルトの再試行ポリシー	エイリアスの再試行ポリシーです。詳細については、「再試行ポリシー」を参照してください。
構成テンプレート	接続および資格情報レコードの作成に使用する構成テンプレートです。

4. [保存] をクリックします。
接続と接続属性関連リストが表示されます。

関連リスト	説明
接続	このエイリアスに関連付けられた関連接続レコード。エイリアスを作成した後、接続レコードを定義してエイリアスに関連付けることができます。[複数の有効な接続をサポート] を選択した場合、複数の接続をエイリアスに関連付けることができます。
接続属性	接続の属性です。接続に固有のデータを定義し、 統合ハブ統合ステップでそのデータを使用します。詳細については、「IntegrationHub の接続属性を作成」を参照してください。
子エイリアス	親エイリアスに関連付けられた子エイリアスです。接続および資格情報エイリアスを作成した後、子エイリアスを作成して、同じアプリケーションデータ連携のために複数の接続を構成できます。

関連リスト	説明
接続	このエイリアスに関連付けられた関連接続レコード。エイリアスを作成した後、接続レコードを定義してエイリアスに関連付けることができます。[複数の有効な接続をサポート] を選択した場合、複数の接続をエイリアスに関連付けることができます。
接続属性	接続の属性です。接続に固有のデータを定義し、 統合ハブ統合ステップでそのデータを使用します。詳細については、「IntegrationHub の接続属性を作成」を参照してください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

5. オプション: 資格情報エイリアスに関連付けられた新しい資格情報および接続を作成する場合は、*Related Links*で [新しい接続と資格情報の作成] をクリックします。
   結果の接続および資格情報レコードは、事前定義された構成テンプレートに基づいています。「接続と資格情報の構成テンプレート」を参照してください。
6. オプション: 接続および資格情報エイリアスの子エイリアスを作成する場合は、[子エイリアス] 関連リストで [新規] を選択します。

   a. 子エイリアスの名前を入力し、[送信] を選択します。
      子エイリアスは、親エイリアスからプロパティを継承します。その後、子エイリアスを設定して、独自の接続および資格情報のセットを含めることができます。

次のタスク
エイリアスまたは子エイリアスに関連付ける 1 つ以上の接続レコードを作成します。接続の作成に関する詳細については、「接続を開始」を参照してください。接続属性をエイリアスに追加して、接続メタデータを フローデザイナー のフローで利用できるようにします。

Discovery の資格情報エイリアス

ディスカバリー の資格情報エイリアスを使用すると、管理者は Discovery スケジュールで特定の資格情報を使用できます。システムで使用方法を厳密に適用する方法を決定する、エイリアスの動作を設定できます。

資格情報エイリアスがない場合、検出スケジュールは、インスタンスで定義されているすべての資格情報にアクセスできます。状況によっては、特に昇格した権限を持つ資格情報の場合には、この動作は望ましくありません。資格情報エイリアスを使用すると、検出スケジュールで使用できる資格情報を細かく制御し、昇格した権限を持つ資格情報が不必要に公開されないようにすることができます。

資格情報エイリアスの仕組み

「*Discovey* 親和性および資格情報エイリアスの挿入」(従来の「*Discovery* 親和性の挿入」) と呼ばれるビジネスルール は、レコードが ECC キューに挿入されたときに実行されます。MID Server が資格情報をフィルタリングできるように、ビジネスルールは、検出スケジュールで定義されている資格情報エイリアスをプローブに添付します。MID Server の最初のタスクは、検索する資格情報のリストを作成することです。これにより、資格情報が親和性、次にタグによってフィルタリングされます (存在する場合)。親和性がリストの一番上に移動し、一致するタグがリストの一番下に移動します。MID Server は、有効である資格情報が見つかるまでリストを反復処理します。その後、MID Server でこの資格情報に対して親和性が作成されます。

注:
資格情報はすべての資格情報タグと一致する必要があります。

デバイスの親和性が存在するとビジネスルールが判断した場合、ルールは使用する適切な *credential_id* を識別します。これは、資格情報 *[discovery_credentials]* テーブル内のレコードの sys_id です。資格情報エイリアス値 (ビジネスルールの *credential_alias* で定義) との親和性がプラットフォームで見つかると、ビジネスルールにより、親和性によって参照される資格情報に指定されたエイリアスがあるかどうかが判断されます。エイリアスがある場合、ビジネスルールにより、エイリアスの *credential_id* が選択され、その値が MID Server に渡されます。認証情報に指定された認証情報エイリアスがない場合は、ターゲットシステムに存在するその他の親和性が確認されます。

Discovery 資格情報エイリアスの作成

エイリアスを作成し、資格情報レコードで資格情報にそのエイリアスを追加します。複数のエイリアスに 1 つの資格情報を追加することも、1 つのエイリアスに複数の資格情報を追加することもできます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

始める前に
必要なロール：admin、credential_admin (読み込みアクセスのみ)、connection_admin (読み込みアクセスのみ)

このタスクについて
検出スケジュールは、そのスケジュール用に定義されたエイリアスに含まれている資格情報のみを使用します。

注:
資格情報エイリアスがスケジュールに定義されている場合、その資格情報エイリアスを使用するようにセットアップされたスケジュールで検出されたターゲットと資格情報間の既存の資格情報親和性は無視されます。

手順

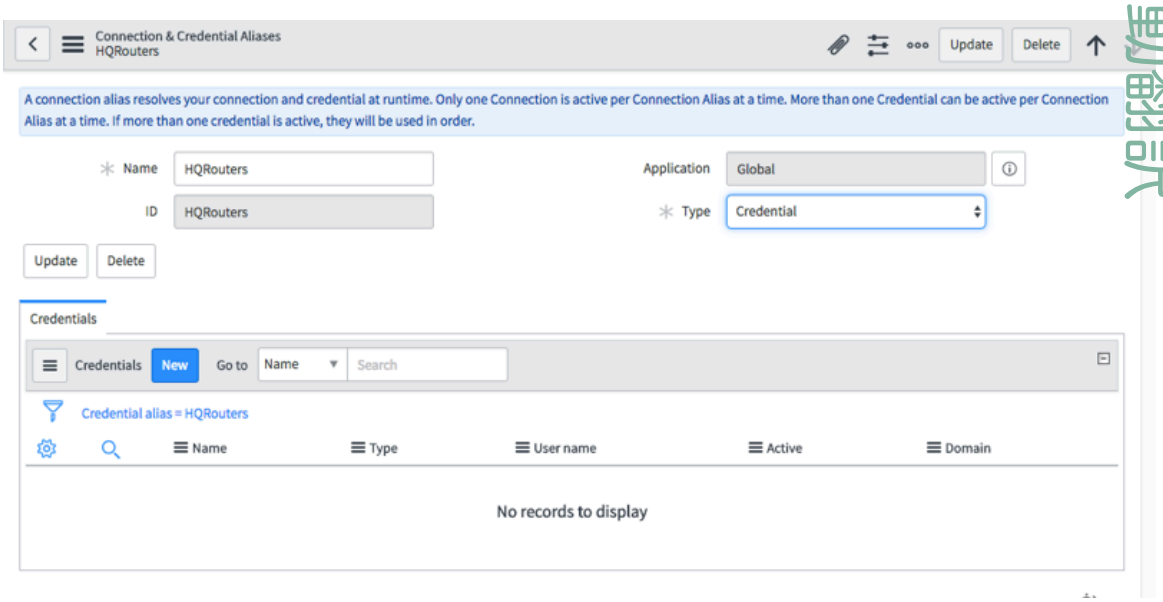
1. エイリアスを作成します。

a. 移動先 接続 **&** 認証情報 > 接続 **&** 資格情報エイリアス.

b. [新規] をクリックします。

c. エイリアスの一意の名前を入力し、エイリアスの [タイプ] の [資格情報] を選択します。

d. [送信] をクリックします。
[資格情報] 関連リストが表示されます。このリストでは、このエイリアスの新しい資格情報を追加できますが、既存の資格情報は追加できません。



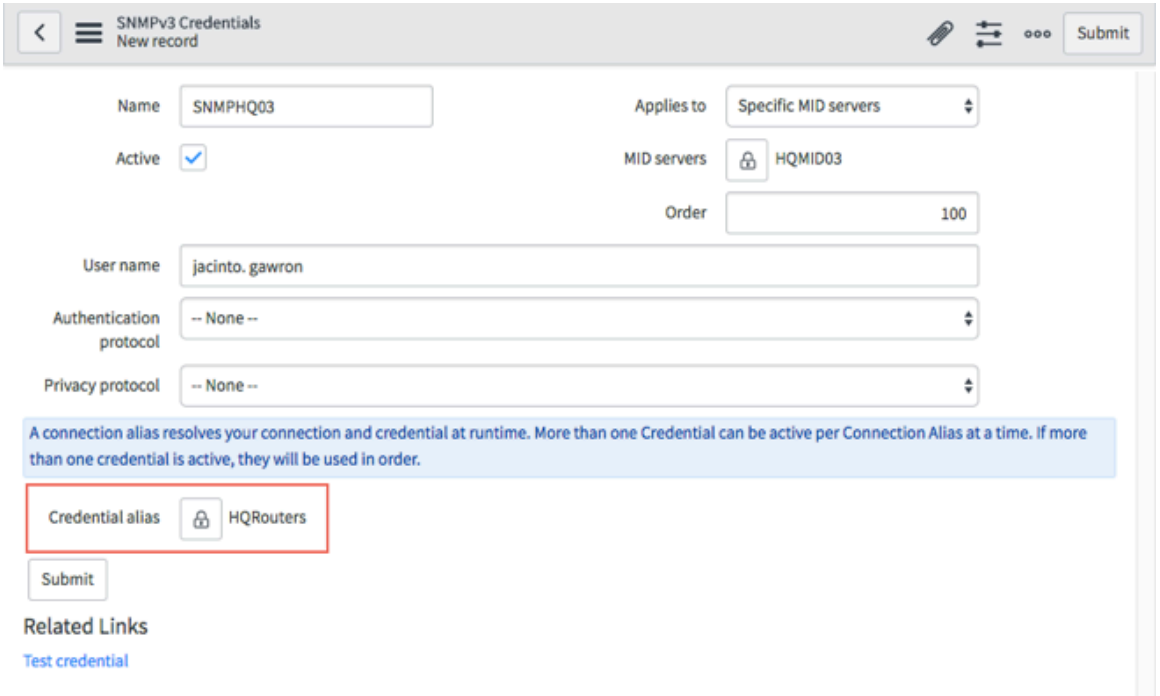
2. 新しいエイリアスの資格情報を設定します。

a. 移動先 接続 **&** 認証情報 > 認証情報.

b. リストから既存の資格情報を選択するか、[新規] をクリックして新しい資格情報を作成します。

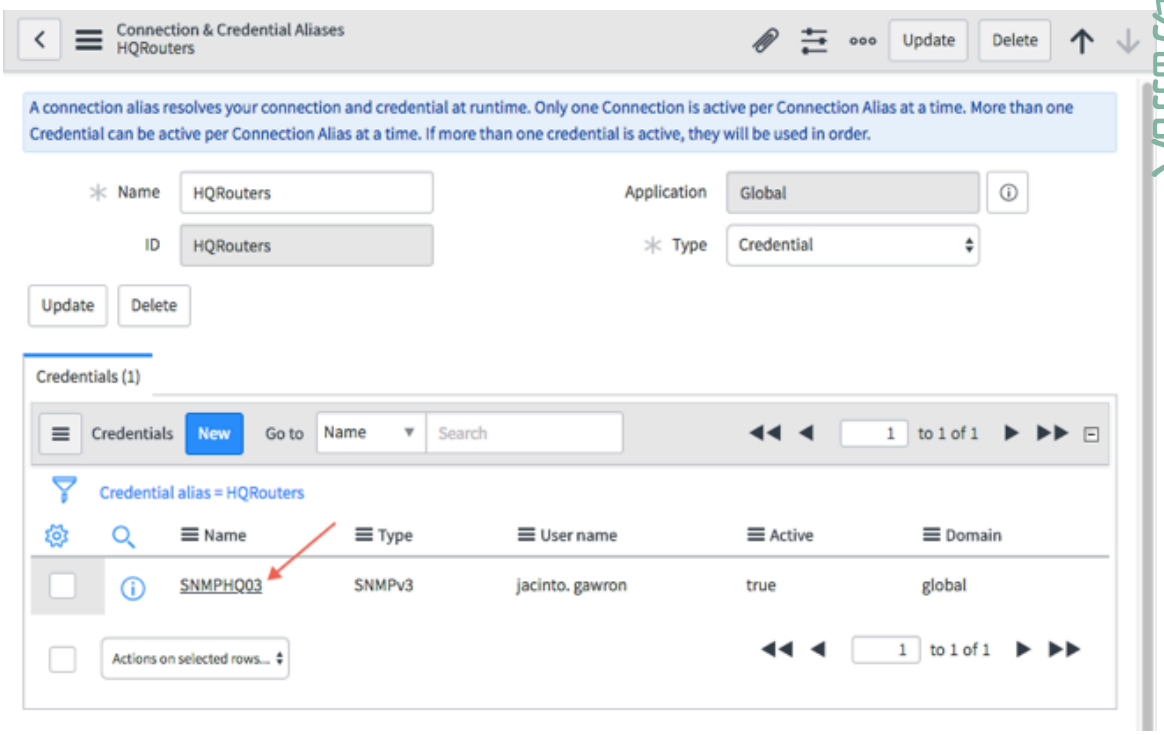
c. 資格情報レコードで、[資格情報エイリアス] フィールドのロックを解除し、作成したエイリアスを選択します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



d. レコードを保存または送信します。

3. 戻る 接続 **&** 認証情報 > 接続 **&** 資格情報エイリアス をクリックし、新しいエイリアスを開きます。
エイリアスに添付した資格情報が関連リストに表示されます。



4. このエイリアスに追加の資格情報を作成するには、関連リストで [新規] をクリックし、資格情報タイプを選択します。
エイリアス名は資格情報レコードの [資格情報エイリアス] フィールドに事前に設定されています。

5. フォーム内のフィールドに入力し、レコードを送信します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Orchestration アクティビティの認証情報エイリアス

認証情報エイリアスを使用すると、管理者はオーケストレーション アクティビティで使用される認証情報をより詳細に制御できます。

これは、アクティビティがタスクを実行するために特定の信任状を必要とする場合に便利です。[資格情報] タグを使用して、個々の資格情報を Orchestration ワークフロー内の任意のアクティビティに割り当てたり、Orchestration ワークフロー内の同じアクティビティタイプが発生するたびに異なる資格情報を割り当てたりすることができます。

資格情報エイリアスは、資格情報親和性とやり取りして、どの資格情報を Orchestration アクティビティに使用するかを決定します。

認証情報エイリアスの仕組み

Discovery 親和性の挿入 (Geneva リリースの「資格情報親和性の挿入」から改名) と呼ばれるビジネス ルール は、レコードが ECC キューに挿入されたときに実行されます。このルールにより、デバイスに資格情報親和性が存在するかどうかが判断され、使用する適切な *credential_id* (資格情報 [discovery_credentials] テーブル内のレコードの *sys_id*) が特定されます。認証情報エイリアス値が定義された (ビジネス ルールの *credential_alias*) 親和性がプラットフォームで見つかると、ビジネス ルールにより、親和性によって参照される認証情報に指定されたエイリアスがあるかどうかが判断されます。エイリアスがある場合、ビジネス ルールにより、認証情報エイリアスの *credential_id* が選択され、その値が MID Server に渡されます。認証情報に指定された認証情報エイリアスがない場合は、ターゲット システムに存在するその他の親和性が確認されます。親和性が適切にタグ付けされた認証情報を参照していない場合、MID Server で認証情報 *[discovery_credentials]* テーブルが繰り返し処理され、適切なタグを含む認証情報が選択されます。その後、MID Server でこの認証情報に対して新しい親和性が作成されます。

認証情報の作成およびテスト

ディスカバリー、サービス マッピング、クラウド管理、およびオーケストレーションでネットワーク内のハードウェアとソフトウェアへのアクセスに必要な認証情報を作成およびテストします。

始める前に

必要なロール：管理者
組織内のセキュリティチームとともにセキュリティポリシーおよびオプションを確認してください。

このタスクについて

このタスクには、認証情報を作成するための一般的な手順が含まれています。特定のフィールドおよび要件の詳細については、「認証情報タイプのドキュメント」を参照してください。

サポートされている資格情報タイプ

適用可能な認証情報	基本認証資格情報	Chef サーバー認証情報
CIM 資格情報	クラウド資格情報	Infoblox 認証情報
JDBC 認証情報	JMS 資格情報	OAuth 2.0 認証情報
SAP 認証情報	SNMP 資格情報	SSH 資格情報
VMware 資格情報	Windows 認証情報	

注:
セキュリティを強化するには、資格情報のスコープを特定の MID Server またはスケジュールに制限して、不要な資格情報を回避します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. 次のいずれかのモジュールに移動します。
   - ディスカバリー > 認証情報
   - サービスマッピング > 認証情報
   - オーケストレーション > 認証情報
2. [新規] をクリックします。
3. [認証情報] ページで、認証情報タイプのリンクをクリックしてフォームに入力します。

   詳細については、選択した認証情報タイプのドキュメントを参照してください。

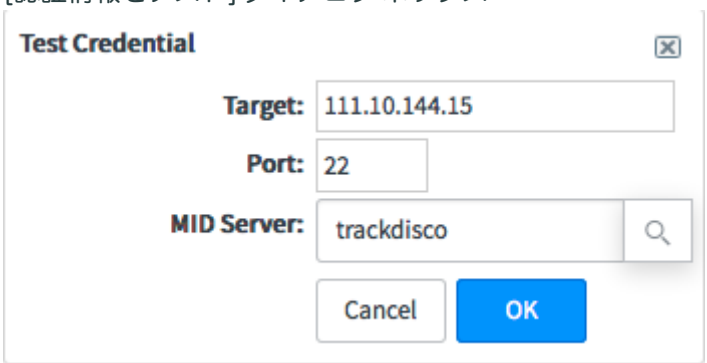
   最初に認証情報レコードを送信してから後でテストするか、認証情報を保存する直前にテストすることができます。

   次の認証情報タイプで認証情報のテストがサポートされています。
   - SSH 秘密鍵
   - Windows
   - SNMP v3
   - VMware
   - JDBC
   - JMS
4. [関連リンク] で、[認証情報をテスト] をクリックします。

   注:
   認証情報は、テスト時に常に暗号化されます。

5. [資格情報をテスト] ダイアログボックスのフィールドに入力します。

[認証情報をテスト] ダイアログ ボックス



認証情報テスト フィールド

フィールド	説明	資格情報タイプ
ターゲット	これらの認証情報が実行されるターゲット ホスト。この値は、VMware 以外のすべての認証情報タイプの IP アドレスである必要があります。これはホスト URL にすることができ	すべて

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明	資格情報タイプ
	ます。MID Server をターゲットにすることはできません。 **注:** JMS の場合、これはプロバイダー URL です。この URL の情報により、JMS プロバイダーを検索してアクセスする方法が JNDI に通知されます。ActiveMQ V5.1 に接続するための値の例は、tcp：//ipAddressOrHostName：61616 です。	
ポート	このテストに使用するターゲット上のポート。このフィールドには、選択した認証情報タイプのデフォルト ポートが事前入力されています。	すべて
MID Server	このテストに使用する MID Server。Windows 認証情報をテストするには、Windows MID Server を使用する必要があります。起動中および検証済みの MID Server のみを利用できます。	すべて
DB タイプ	これらの認証情報をテストするデータベースのタイプ。	JDBC
DB 名	これらの認証情報をテストするデータベースの名前。	JDBC
初期コンテキスト ファクトリー	InitialContext の作成に使用する JNDI クラスの名前。この [初期コンテキスト ファクトリー] を使用すると、JMS 接続などのさまざまな JMS オブジェクトが作成されます。たとえば、ActiveMQ V5.10 (JMS プロバイダー) に接続する場合、このフィールドの値は org.apache.activemq.jndi.ActiveMQInitialContextFactory です。	JMS

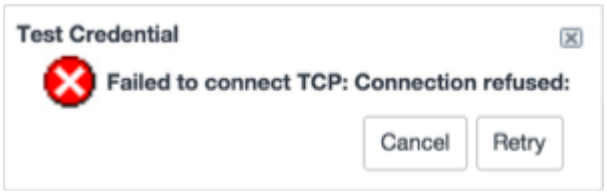
6. **[OK]** をクリックしてテストを開始します。
インジケーターが表示され、入力した認証情報を使用したターゲットへの接続の試行が示されます。インスタンスがターゲットに接続すると、成功メッセージが表示されます。入力したテスト入力に関する問題がインスタンスで発生すると、該当するエラーメッセージが表示されます。よくあるエラーメッセージは次のとおりです。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

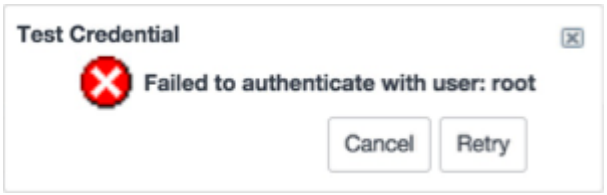
- 不適切なターゲットまたはポート番号：

  TCP 接続エラー

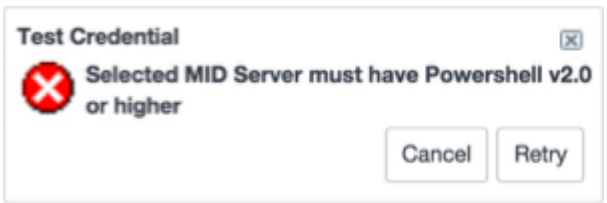
- ユーザー名またはパスワードが間違っています。

  認証失敗

- Windows 認証情報の MID Server が正しくありません。

  MID Server エラー

7. [再試行] をクリックして [認証情報をテスト] ダイアログ ボックスを開き、入力エラーを修正します。
8. 認証情報テストが成功したら、[送信] をクリックしてレコードを保存します。

> **重要:**
> 認証情報のテストでは、目的の検出またはオーケストレーションのワークフロー タスクに必要な権限が認証情報にあるとは保証されません。

Ansible Tower 資格情報

Ansible 構成管理アカウントにアクセスするには、Ansible Tower 資格情報が必要です。これらの資格情報を使用して、クラウド管理アプリケーションで Ansible リソースを管理します。

Cloud Provisioning and Governance と Ansible 構成管理アカウントを統合するには、Ansible で管理者アカウントのユーザー名およびパスワードを設定する必要があります。

Ansible Tower 資格情報のフォームフィールド

フィールド	説明
名前	わかりやすい名前を入力します。
ユーザー名/パスワード	管理者権限を持つ Ansible Tower ユーザーの認証資格情報を入力します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注:
その他のフィールドを設定する必要はありません。

API キー認証情報

API キーは、コール元アプリケーションまたはユーザーを識別するために API に渡される一意のコードです。

API キー認証情報

API キー資格情報フォームのフィールド

フィールド	入力値
名前	この資格情報のわかりやすい一意の名前を入力します。
アクティブ	これらの資格情報の使用を有効または無効にします。
API キー	API キーを入力します。
資格情報エイリアス	フローおよびワークフローの作成者は、個々の認証情報をフローまたはワークフロー内の任意のアクティビティに割り当てたり、フローまたはワークフロー内の同じアクティビティタイプが発生するたびに異なる認証情報を割り当てたりすることができます。
適用先	これらの認証情報をネットワーク内の [すべての **MID** サーバー] または 1 つ以上の [特定の **MID** サーバー] に適用するかどうかを選択します。**[MID** サーバー] フィールドでこれらの認証情報を使用する MID サーバー を指定します。
順番	ディスカバリー がデバイスにログオンしようとするときに、この認証情報を試行する順序 (シーケンス) 。番号が小さいほど、この認証情報がリストの上位に表示されます。多くの資格情報を使用する場合、またはログイン試行が 3 回失敗してセキュリティによってユーザーがロックアウトされた場合、資格情報の順序を確立します。すべての資格情報の順序番号が同じ (または順序番号がない) 場合、インスタンスは資格情報をランダムな順序で試行します。

適用可能な認証情報

ホストマシンに必要な認証情報に加え、一部のアプリケーションでは認証情報が必要です。これらのアプリケーションにアクセスするために必要な認証情報は、適用可能な認証情報と呼ばれています。

一般的な資格情報には、デバイスまたはアプリケーションにログインするためのユーザー名とパスワードが含まれています。ほとんどのアプリケーションでは、アクセスに必要な資格情報は 1 つだけですが、ホストとアプリケーションによっては、セキュリティを強化するために別の資格情報を持つ場合もあります。たとえば、ABAP SAP Central Services (ASCS) では、ASCS をホストするサーバーの SSH または Windows ホスト資格情報に加えて、適用可能な資格情報が必要です。

注:
ServiceNowアプリケーションは、構成アイテム (CI) としてアプリケーションサービスを構成するデバイスおよびアプリケーションを参照します。

ホスト資格情報と同様に、適用可能な資格情報を MID サーバー に割り当てます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

CI タイプごとに適用可能な資格情報を作成します。たとえば、ASCS の CI タイプは SAP ASCS アプリケーション [cmdb_ci_appl_sap_ascs] です。この CI タイプに属する CI を検出するための事前設定されたパターンには、MID サーバーにこの CI タイプに適用可能な資格情報を使用することを求めるコマンドが含まれています。この CI タイプに対して複数の資格情報が設定されている場合、MID サーバーは適合する資格情報が見つかるまで、これらの資格情報を定義された順序で試行します。

特定のアプリケーション CI に適用可能な資格情報が必要かどうかを判断するには、ServiceNow のドキュメントの ディスカバリー 要件に関する情報を確認してください。ディスカバリー の必須条件に言及されていなければ、適用可能な資格情報を設定する必要はありません。

適用可能な認証情報フォームのフィールド

フィールド	説明
名前	認証情報の名前です。Oracle DB または London Oracle DB (Oracle データベースの場合) などのわかりやすい名前を使用します。資格情報名にスペースまたは特殊文字を使用することはできません。
アクティブ	認証情報を使用するには、このチェックボックスをオンにします。
ユーザー名	適用可能な認証情報の実際のユーザー名を入力します。
パスワード	適用可能な資格情報の実際のパスワードを入力します。資格情報名にスペースまたは特殊文字を使用することはできません。
CI タイプ	CI が属する CI タイプを選択します。
資格情報エイリアス	特定の検出スケジュールに対して特定の資格情報をアサインするエイリアスを作成します。エイリアスをアサインする際、アプリケーションが使用する適用可能な資格情報を持つ CI タイプのテーブル名を識別する必要があります。アプリケーションは、それ自身とは異なる CI タイプの適用可能な資格情報を使用する場合があります。特定のアプリケーションについては、次の該当するテーブルのリストを参照してください。 • ABAP SAP Central Services (ASCS): cmdb_ci_appl_sap_ascs • IBM Security Access Manager アプライアンス：cmdb_ci_app_server_webseal • SAP Central インスタンス: cmdb_ci_appl_sap_ascs • SAP Central Services (SCS): cmdb_ci_appl_sap_ascs • SAP Evaluated Receipt Settlement (ERS): cmdb_ci_appl_sap_ascs • SAP Java クラスター: cmdb_ci_appl_sap_ascs • SAP NetWeaver Dialog インスタンス: cmdb_ci_appl_sap_ascs • Microsoft Exchange Mailbox (Microsoft Exchange の場合): cmdb_ci_exchange_mailbox • Microsoft SQL Database: cmdb_ci_db_mssql_instance • MySQL Server: cmdb_ci_db_mysql_instance • Oracle Advanced Queue Queue: cmdb_ci_db_ora_instance

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

適用可能な認証情報フォームのフィールド (続く)

フィールド	説明
	• Oracle Database: cmdb_ci_db_ora_instance • Oracle E-Business Suite: cmdb_ci_db_ora_instance • Oracle WebLogic モジュール: cmdb_ci_app_server_weblogic • Tibco Enterprise Message Service (EMS): cmdb_ci_appl_tibco_message
適用先	これらの認証情報をネットワーク内の [すべての **MID** サーバー] または 1 つ以上の [特定の **MID** サーバー] に適用するかどうかを選択します。**[MID** サーバー] フィールドでこれらの認証情報を使用する MID サーバー を指定します。
順序	ディスカバリー がデバイスにログオンしようとするときに、この認証情報を試行する順序 (シーケンス) 。番号が小さいほど、この認証情報がリストの上位に表示されます。多くの資格情報を使用する場合、またはログイン試行が 3 回失敗してセキュリティによってユーザーがロックアウトされた場合、資格情報の順序を確立します。すべての資格情報の順序番号が同じ (または順序番号がない) 場合、インスタンスは資格情報をランダムな順序で試行します。

基本認証資格情報

基本認証資格情報タイプにより、基本認証資格情報を保存するためのアクセス権が管理されます。

次のフィールドは、基本認証の認証情報フォームで使用できます。

基本認証資格情報フォーム

フィールド	入力値
名前	この資格情報のわかりやすい一意の名前を入力します。たとえば、**Basic Authentication** と入力します。
ユーザー名	ユーザー名を入力します。
パスワード	パスワードを入力します。
資格情報 ID	CyberArk の外部認証情報ストレージ システムでこれらの認証情報に設定されている一意のキーを入力します。認証情報 ID は、複数のセーフが使用されている場合に安全な上書きとして使用できます。デフォルトで、[資格情報 **ID]** フィールドの構文は *<safe name>:<Credential ID>* です。セーフ名を省略する場合、config.xml ファイルで定義されているセーフ名が必要です。区切り文字をデフォルトのコロンから別の文字に変更するには、値をオプションの *ext.cred.safe_name* パラメーターで上書きします。[資格情報 **ID]** フィールドには 40 文字の制限があります。 このフィールドは、**[External storage]** (外部ストレージ) チェック ボックスがオンになっている場合にのみ表示されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

基本認証資格情報フォーム (続く)

フィールド	入力値
外部の資格情報ストア	外部認証情報ストレージシステムを使用するには、このチェックボックスをオンにします。このオプションを選択すると、[ユーザー名] フィールドと [パスワード] フィールドが [認証情報 **ID]** フィールドに置き換えられます。現在サポートされている外部ストレージ システムは CyberArk だけです。
順番	ディスカバリー がデバイスにログオンしようとするときに、この認証情報を試行する順序 (シーケンス) 。番号が小さいほど、この認証情報がリストの上位に表示されます。多くの資格情報を使用する場合、またはログイン試行が 3 回失敗してセキュリティによってユーザーがロックアウトされた場合、資格情報の順序を確立します。すべての資格情報の順序番号が同じ (または順序番号がない) 場合、インスタンスは資格情報をランダムな順序で試行します。

Chef サーバー認証情報

Chef サーバー認証情報は、インスタンスとの Chef 統合にアクセスします。

次のフィールドは、Chef サーバー タイプの認証情報の認証情報フォームで利用可能です。この情報は、[Chef server installation] (Chef サーバー インストール) の実行時に設定した設定から取得されます。

フィールド	説明
名前	この資格情報のわかりやすい一意の名前を入力します。
アクティブ	これらの資格情報の使用を有効または無効にします。
管理者名	Chef サーバーのインストール時に作成した管理者名を入力します。
管理キー	管理者の作成時に Chef サーバーによって生成された RSA 秘密鍵を入力します。
検証ツール名	検証ツールを入力します。
検証ツールキー	組織の作成時に Chef サーバーによって生成された RSA 秘密鍵を入力します。
証明書名	認定名を入力します。
証明書キー	認定キーを入力します。

CIM 資格情報

CIM 資格情報タイプは、VMware ESX サーバーについての情報を得るための CIM サーバー (別名 CIMOM - 共通情報モデル オブジェクト マネージャー) へのアクセス権を管理します。 この認証情報タイプはディスカバリーで使用できます。

次のフィールドは、CIM の認証情報フォームで使用できます。

フィールド	説明
名前	この資格情報のわかりやすい一意の名前を入力します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
アクティブ	これらの資格情報の使用を有効または無効にします。
ユーザー名	[認証情報] テーブルに、作成するユーザー名を入力します。ユーザー名の先頭または末尾にはスペースを使用しないでください。プラットフォームでユーザー名の先頭または末尾のスペースが検出されると、警告が表示されます。CIM 検出の場合、ユーザーには admin ロールが必要です。
パスワード	パスワードを入力します。
資格情報 ID	外部認証情報システム用に MID Server にアップロードされた JAR ファイルに外部認証情報用に設定された一意のキーを入力します。[資格情報 **ID]** フィールドには 40 文字の制限があります。 このフィールドは、[外部の認証情報ストア] チェックボックスがオンになっている場合にのみ表示されます。
資格情報エイリアス	ワークフロー作成者は、個々の資格情報を Orchestration ワークフロー内の任意のアクティビティに割り当てたり、Orchestration ワークフロー内で同じアクティビティタイプが発生するたびに異なる資格情報を割り当てたりすることができます。 Service Mapping および検出パターンを使用してこの CI タイプに属していない CI を検出するために資格情報を使用するには、CI が属する CI タイプのテーブル名 (cmdb_ci_apache_web_server など) を入力します。詳細については、「資格情報をデフォルト以外に変更する」を参照してください。
外部の資格情報ストア	外部認証情報ストレージシステムを使用するには、このチェックボックスをオンにします。このオプションを選択すると、[ユーザー名] フィールドと [パスワード] フィールドが [認証情報 **ID]** フィールドに置き換えられます。外部の認証情報ストレージは、 外部認証情報ストレージ プラグインをアクティブ化した場合にのみ使用できます。 **注:** 現在サポートされている外部ストレージ システムは CyberArk だけです。
適用先	これらの認証情報をネットワーク内の [すべての **MID** サーバー] または 1 つ以上の [特定の **MID** サーバー] に適用するかどうかを選択します。**[MID** サーバー] フィールドでこれらの認証情報を使用する MID サーバー を指定します。
MID Server を使用	使用可能な MID Server のリストから 1 つ以上の MID Server を選択します。このレコードで設定された認証情報は、このリストの MID Server で使用できます。このフィールドは、[適用先] フィールドで [特定の **MID** サーバー] を選択した場合のみ使用できます。 **注:** [特定の **MID Server]** を選択しても、MID Server の選択には影響しません。これは、資格情報を表示する必要がある MID Server を決定するためにのみ使用されます。[特定の **MID Server]** はオーケストレーションアクティビティではサポートされていません。
順序	ディスカバリー がデバイスにログオンしようとするときに、この認証情報を試行する順序 (シーケンス) 。番号が小さいほど、この認証情報がリストの上位に表示されます。多くの資格情報を使用する場合、またはログイン試行が 3 回失敗してセキュリ

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

フィールド	説明
	ティによってユーザーがロックアウトされた場合、資格情報の順序を確立します。すべての資格情報の順序番号が同じ (または順序番号がない) 場合、インスタンスは資格情報をランダムな順序で試行します。
Windows MID サーバー サービスアカウント	有効な場合、定義された資格情報は MID サーバー サービスアカウントを表します。

NetApp ストレージデバイスでの **CIM** 資格情報の設定

ディスカバリー で NetApp ストレージデバイスを検出するには、追加の設定が必要です。

始める前に
必要なロール：管理者

手順

1. ストレージ デバイス ホスト上に SMI-S エージェント をインストールします。

   手順および要件については、「Data ONTAP SMI-S Agent 5.2 のインストールおよび設定ガイド」を参照してください。

   注:

   ServiceNow では、このサイトでこのドキュメントを管理していません。このドキュメントは、予告なしに変更される可能性があります。

2. SMI-S エージェントのユーザーアカウントとパスワードを作成します。
3. SMI-S エージェント認証情報の認証情報レコードを作成します。
   認証情報タイプを **[CIM]** に設定します。

クラウド資格情報

クラウド認証情報タイプにより、Amazon Web Services や Microsoft Azure クラウドなどのクラウドベースのアプリケーションへのアクセス権が管理されます。

AWS Identity and Access Management (IAM) ロール

AWS クラウドの Amazon EC2 に MID Server がインストールされていて、その MID Server がクラウド内のリソースを検出するように設定されている場合は、インスタンスで管理されている資格情報ではなく、AWS Identity and Access Management (IAM) ロールによって提供されるセキュリティ資格情報を使用できます。これらの AWS 資格情報は、ロールに基づいて、インスタンスプロファイルを通じてクラウドでの権限を付与します。これらの資格情報は一時的なものであり、構成可能な間隔で自動的にローテーションされます。MID Server で IAM ロールが定義されている場合。詳細については、「AWS IAM ロール用の MID Server の構成」を参照してください。

Discovery はインスタンスに格納されているすべての資格情報を無視し、インスタンスプロファイルのロールによって付与された資格情報を優先します。AWS インスタンスプロファイルの詳細については、「Amazon EC2 の IAM ロール (IAM Roles for Amazon EC2)」を参照してください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

AWS 資格情報

AWS 認証情報フォームのフィールド

フィールド	入力値
名前	AWS 資格情報の分かりやすい一意の名前。
アクティブ	資格情報を使用するオプション。
アクセスキー ID	AWS 管理コンソールで生成された [アクセスキー **ID**] (例：APIAIOSFODNN7EXAMPLE)。
秘密アクセスキー	AWS 管理コンソールで生成された [秘密アクセスキー] (例：wPalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY)。

Azure サービスプリンシパル資格情報フォームフィールド

フィールド	値
名前	インスタンスに登録するサービスプリンシパルの名前を入力します。
テナント ID および	Azure ポータルの Azure ディレクトリ **ID** の値を クラウド管理 [テナント **ID**] フィールドに貼り付けます。
クライアント ID	Azure に登録したアプリケーションの Azure アプリケーション **ID** の値を クラウド管理 [クライアント **ID**] フィールドに貼り付けます。
認証方法	[クライアントシークレット] を選択します。 **注:** [クライアントアサーション] はサポートされていません。
秘密キー	Azure サービスプリンシパルの作成中に生成された秘密キーを貼り付けます。 このフィールドは、[認証手法] が [クライアントシークレット] のときに表示されます。

Azure エンタープライズ契約認証情報

Azure エンタープライズ契約認証情報は、クラウド管理アプリケーションで提供される請求機能に必要です。

Azure エンタープライズ契約認証情報フォームのフィールド

フィールド	説明
名前	内容を端的に表す名前を入力します。
登録数	Azure からの登録番号を入力します。
アクセス キー	Azure が提供するアクセス キーを貼り付けます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

クラウド管理認証情報

この認証情報タイプはオーケストレーションで使用できます。

クラウド管理資格情報フォームのフィールド

フィールド	入力値
名前	この資格情報のわかりやすい一意の名前を入力します。たとえば、**Cloud Atlanta** と入力します。
有効	これらの資格情報の使用を有効または無効にします。
タイプ	**[AWS]** を指定します。
ユーザー名	認証情報テーブルに作成する CIM ユーザー名を入力します。ユーザー名の先頭または末尾にはスペースを使用しないでください。プラットフォームでユーザー名の先頭または末尾のスペースが検出されると、警告が表示されます。
パスワード	CIM パスワードを入力します。
SSH パスフレーズ	キーの生成用に覚えやすいフレーズを入力します。たとえば、**Friday is a good day** と入力します。
SSH 秘密鍵	SSH 秘密鍵を入力します。
認証プロトコル	[認証キー] の生成に使用した **[MD5]** または **[SHA]** の認証プロトコルを選択します。
認証キー	SSH で生成された認証キーを入力します。
プライバシープロトコル	[プライバシー キー] の暗号化を説明する次のいずれかのプライバシー プロトコルを入力します。 • **3DES** (Triple Data Encryption Standard (DES) の場合) • **AES128** (128 ビット暗号化を使用する Advanced Encryption Standard (AES) の場合) • **AES192** (192 ビット暗号化を使用する AES の場合) • **AES256** (256 ビット暗号化を使用する AES の場合) • **DES** (レガシー DES 暗号化の場合)
追加のプライバシー キーを入力します。	
資格情報エイ	ワークフロー作成者は、個々の資格情報を Orchestration ワークフロー内の任意のアクティビティに割り当てたり、Orchestration ワークフロー内で同じアクティビティタイプが発生するたびに異なる資格情報を割り当てたりすることができます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

クラウド管理資格情報フォームのフィールド (続く)

フィールド	入力値
リアス	
外部の資格情報ストア	外部認証情報ストレージシステムを使用するには、このチェックボックスをオンにします。このオプションを選択すると、[ユーザー名] フィールドと [パスワード] フィールドが [認証情報 **ID]** フィールドに置き換えられます。現在サポートされている外部ストレージ システムは CyberArk だけです。
適用先	これらの認証情報をネットワーク内の [すべての **MID** サーバー] または 1 つ以上の [特定の **MID** サーバー] に適用するかどうかを選択します。**[MID** サーバー] フィールドでこれらの認証情報を使用する MID サーバー を指定します。
分類	CI 検出のアプリケーション分類を入力します。
順番	ディスカバリー がデバイスにログオンしようとするときに、この認証情報を試行する順序 (シーケンス) 。番号が小さいほど、この認証情報がリストの上位に表示されます。多くの資格情報を使用する場合、またはログイン試行が 3 回失敗してセキュリティによってユーザーがロックアウトされた場合、資格情報の順序を確立します。すべての資格情報の順序番号が同じ (または順序番号がない) 場合、インスタンスは資格情報をランダムな順序で試行します。

クラウド管理 **(CMP)** ノード認証情報

クラウド管理 (CMP) ノード認証情報は、クラウド管理によってプロビジョニングされた仮想サーバーの認証情報を関連付けます。クラウド管理アプリケーションにより、これらの認証情報が自動的に作成されます。

注:
これらの認証情報を使用しない場合の非アクティブ化、順序の優先順位の変更、またはこれらの認証情報へのアクセスが許可されている MID Server の選択が必要な場合があります。それ以外の場合は、このタイプの認証情報を手動で作成または変更する必要はありません。

CMP ノード認証情報フォームのフィールド

フィールド	説明
名前	仮想マシンが配置されているデータセンターに基づいて自動的に生成される名前。
有効	資格情報がアクティブな場合。
適用先	この認証情報を特定の MID Server またはすべての MID Server で利用できるかどうかを選択します。
順番	ディスカバリー がデバイスにログオンしようとするときに、この認証情報を試行する順序 (シーケンス) 。番号が小さいほど、この認証情報がリストの上位に表示されます。多くの資格情報を使用する場合、またはログイン試行が 3 回失敗してセキュリティによってユーザーがロックアウトされた場合、資格情報の順序を確立します。すべての資格情報の順序番号が同じ (または順序番号がない) 場合、インスタンスは資格情報をランダムな順序で試行します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

CMP ノード認証情報フォームのフィールド (続く)

フィールド	説明
ユーザー名とパスワード	仮想サーバーのユーザー名とパスワード。
SSH パスフレーズと SSH 秘密鍵	仮想サーバーでキーが必要な場合にそのキーを保護する秘密鍵とパスフレーズ。
認証プロトコルと認証キー	仮想サーバーでキーが必要な場合にそのキーを保護する秘密鍵とパスフレーズ。
プライバシープロトコルとプライバシーキー	仮想サーバーで使用される暗号化プロトコル。プライバシー キーを入力します。
資格情報エイリアス	ワークフロー作成者は、個々の資格情報を Orchestration ワークフロー内の任意のアクティビティに割り当てたり、Orchestration ワークフロー内で同じアクティビティタイプが発生するたびに異なる資格情報を割り当てたりすることができます。

クラウド管理 **(CMP) SSH** キー ペア認証情報

ユーザーがスタック リソースをプロビジョニングしたときに、クラウド管理 (CMP) SSH キー ペアにより、クラウド管理アプリケーションで自動的に生成されるキーが保存されます。

注:
これらの認証情報を使用しない場合は、これらの認証情報を非アクティブ化する必要があります。それ以外の場合は、このタイプの認証情報を手動で作成または変更する必要はありません。

CMP SSH キー ペア認証情報フォームのフィールド

フィールド	説明
名前	自動的に生成される名前。
有効	資格情報がアクティブな場合。
SSH 公開鍵	公開鍵。
SSH 秘密鍵	SSH ログインのパスワードの代わりに使用できる安全な秘密鍵。

Infoblox 認証情報

Infoblox 認証情報は、クラウド管理アプリケーションで IP プール (IPAM) を設定するために必要です。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

次のフィールドは、Infoblox タイプの認証情報の認証情報フォームで使用できます。

フィールド	説明
名前	この資格情報のわかりやすい一意の名前を入力します。
アクティブ	これらの資格情報の使用を有効または無効にします。
適用先	この認証情報を特定の MID Server またはすべての MID Server で利用できるかどうかを選択します。
順番	ディスカバリー がデバイスにログオンしようとするときに、この認証情報を試行する順序 (シーケンス) 。番号が小さいほど、この認証情報がリストの上位に表示されます。多くの資格情報を使用する場合、またはログイン試行が 3 回失敗してセキュリティによってユーザーがロックアウトされた場合、資格情報の順序を確立します。すべての資格情報の順序番号が同じ (または順序番号がない) 場合、インスタンスは資格情報をランダムな順序で試行します。 ディスカバリー がデバイスにログオンしようとするときに、この認証情報を試行する順序 (シーケンス) 。番号が小さいほど、この認証情報がリストの上位に表示されます。多くの資格情報を使用する場合、またはログイン試行が 3 回失敗してセキュリティによってユーザーがロックアウトされた場合、資格情報の順序を確立します。すべての資格情報の順序番号が同じ (または順序番号がない) 場合、インスタンスは資格情報をランダムな順序で試行します。
WAPI バージョン	使用している WAPI のバージョン を入力します。
ユーザー名とパスワード	InfoBlox のユーザー名とパスワードを入力します。

JDBC 認証情報

JDBC 認証情報タイプにより、Java Database Connectivity (JDBC) 接続へのアクセスが管理されます。この認証情報タイプはディスカバリーとオーケストレーションで使用できます。

次のフィールドは、JDBC タイプの認証情報の認証情報フォームで使用できます。

フィールド	説明
名前	この資格情報のわかりやすい一意の名前を入力します。
アクティブ	これらの資格情報の使用を有効または無効にします。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
ユーザー名	[認証情報] テーブルに、作成するユーザー名を入力します。ユーザー名の先頭または末尾にはスペースを使用しないでください。プラットフォームでユーザー名の先頭または末尾のスペースが検出されると、警告が表示されます。CIM 検出の場合、ユーザーには admin ロールが必要です。
パスワード	パスワードを入力します。
資格情報 ID	外部認証情報システム用に MID Server にアップロードされた JAR ファイルに外部認証情報用に設定された一意のキーを入力します。[資格情報 **ID]** フィールドには 40 文字の制限があります。 このフィールドは、[外部の認証情報ストア] チェックボックスがオンになっている場合にのみ表示されます。
資格情報エイリアス	ワークフロー作成者は、個々の資格情報を Orchestration ワークフロー内の任意のアクティビティに割り当てたり、Orchestration ワークフロー内で同じアクティビティタイプが発生するたびに異なる資格情報を割り当てたりすることができます。 Service Mapping および検出パターンを使用してこの CI タイプに属していない CI を検出するために資格情報を使用するには、CI が属する CI タイプのテーブル名 (cmdb_ci_apache_web_server など) を入力します。詳細については、「資格情報をデフォルト以外に変更する」を参照してください。
外部の資格情報ストア	外部認証情報ストレージシステムを使用するには、このチェックボックスをオンにします。このオプションを選択すると、[ユーザー名] フィールドと [パスワード] フィールドが [認証情報 **ID]** フィールドに置き換えられます。外部の認証情報ストレージは、 外部認証情報ストレージ プラグインをアクティブ化した場合にのみ使用できます。 **注:** 現在サポートされている外部ストレージ システムは CyberArk だけです。
適用先	これらの認証情報をネットワーク内の [すべての **MID** サーバー] または 1 つ以上の [特定の **MID** サーバー] に適用するかどうかを選択します。**[MID** サーバー] フィールドでこれらの認証情報を使用する MID サーバー を指定します。
MID Server を使用	使用可能な MID Server のリストから 1 つ以上の MID Server を選択します。このレコードで設定された認証情報は、このリストの MID Server で使用できます。このフィールドは、[適用先] フィールドで [特定の **MID** サーバー] を選択した場合のみ使用できます。 **注:** [特定の **MID Server]** を選択しても、MID Server の選択には影響しません。これは、資格情報を表示する必要がある MID Server を決定するためにのみ使用されます。[特定の **MID Server]** はオーケストレーションアクティビティではサポートされていません。
順序	ディスカバリー がデバイスにログオンしようとするときに、この認証情報を試行する順序 (シーケンス) 。番号が小さいほど、この認証情報がリストの上位に表示されます。多くの資格情報を使用する場合、またはログイン試行が 3 回失敗してセキュリティによってユーザーがロックアウトされた場合、資格情報の順序を確立します。すべての資格情報の順序番号が同じ (または順序番号がない) 場合、インスタンスは資格情報をランダムな順序で試行します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
Windows MID サーバー サービスアカウント	有効な場合、定義された資格情報は MID サーバー サービスアカウントを表します。

JMS 資格情報

JMS 認証情報タイプにより、Java Message Service (JMS) へのアクセスが管理されます。この認証情報タイプはディスカバリーとオーケストレーションで使用できます。

次のフィールドは、JMS 認証情報フォームで使用できます。

フィールド	説明
名前	この資格情報のわかりやすい一意の名前を入力します。
アクティブ	これらの資格情報の使用を有効または無効にします。
ユーザー名	[認証情報] テーブルに、作成するユーザー名を入力します。ユーザー名の先頭または末尾にはスペースを使用しないでください。プラットフォームでユーザー名の先頭または末尾のスペースが検出されると、警告が表示されます。CIM 検出の場合、ユーザーには admin ロールが必要です。
パスワード	パスワードを入力します。
資格情報 ID	外部認証情報システム用に MID Server にアップロードされた JAR ファイルに外部認証情報用に設定された一意のキーを入力します。[資格情報 **ID]** フィールドには 40 文字の制限があります。 このフィールドは、[外部の認証情報ストア] チェックボックスがオンになっている場合にのみ表示されます。
資格情報エイリアス	ワークフロー作成者は、個々の資格情報を Orchestration ワークフロー内の任意のアクティビティに割り当てたり、Orchestration ワークフロー内で同じアクティビティタイプが発生するたびに異なる資格情報を割り当てたりすることができます。 Service Mapping および検出パターンを使用してこの CI タイプに属していない CI を検出するために資格情報を使用するには、CI が属する CI タイプのテーブル名 (cmdb_ci_apache_web_server など) を入力します。詳細については、「資格情報をデフォルト以外に変更する」を参照してください。
外部の資格情報ストア	外部認証情報ストレージシステムを使用するには、このチェックボックスをオンにします。このオプションを選択すると、[ユーザー名] フィールドと [パスワード] フィールドが [認証情報 **ID]** フィールドに置き換えられます。外部の認証情報ストレージは、 外部認証情報ストレージ プラグインをアクティブ化した場合にのみ使用できます。 **注:** 現在サポートされている外部ストレージ システムは CyberArk だけです。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
適用先	これらの認証情報をネットワーク内の [すべての **MID** サーバー] または 1 つ以上の [特定の **MID** サーバー] に適用するかどうかを選択します。**[MID** サーバー] フィールドでこれらの認証情報を使用する MID サーバー を指定します。
MID Server を使用	使用可能な MID Server のリストから 1 つ以上の MID Server を選択します。このレコードで設定された認証情報は、このリストの MID Server で使用できます。このフィールドは、[適用先] フィールドで [特定の **MID** サーバー] を選択した場合のみ使用できます。 **注:** [特定の **MID Server]** を選択しても、MID Server の選択には影響しません。これは、資格情報を表示する必要がある MID Server を決定するためにのみ使用されます。[特定の **MID Server]** はオーケストレーションアクティビティではサポートされていません。
順序	ディスカバリー がデバイスにログオンしようとするときに、この認証情報を試行する順序 (シーケンス) 。番号が小さいほど、この認証情報がリストの上位に表示されます。多くの資格情報を使用する場合、またはログイン試行が 3 回失敗してセキュリティによってユーザーがロックアウトされた場合、資格情報の順序を確立します。すべての資格情報の順序番号が同じ (または順序番号がない) 場合、インスタンスは資格情報をランダムな順序で試行します。
Windows MID サーバー サービスアカウント	有効な場合、定義された資格情報は MID サーバー サービスアカウントを表します。

OAuth 2.0 認証情報

OAuth 2.0 の認証情報により、ServiceNow は HTTP サービス上のユーザーアカウントにアクセスできるようになります。

次のフィールドは、OAuth 2.0 の認証情報フォームで使用できます。

OAuth 2.0 認証情報フォーム

フィールド	入力値
名前	この資格情報のわかりやすい一意の名前を入力します。たとえば、 **OAuth2 credential** と入力します。
有効	この認証情報がアクティブかどうかを指定します。
OAuth エンティティプロファイル	OAuth プロファイルは、権限付与タイプと少なくとも 1 つのスコープを組み合わせたものです。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

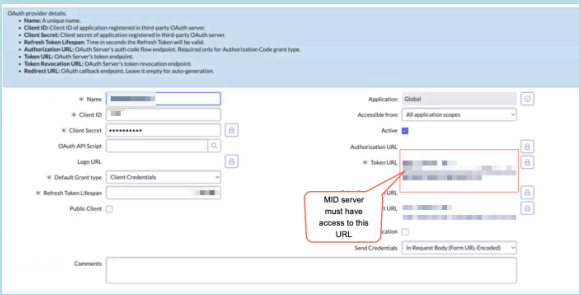
OAuth 2.0 認証情報フォーム (続く)

フィールド	入力値
MID サーバー経由で認証サーバーに接続	を介してファイアウォールの内側にあるオンプレミスの OAuth サーバーにインスタンスを接続し ServiceNow ます MID サーバー。また、 ServiceNow MID Server を介してインスタンスをクラウドベースの OAuth サーバーに接続することもできます。このオプションを有効にすると、OAuth トークンの要求が を介して送信されます MID サーバー。 **重要:** • このオプションは、OAuth エンティティプロファイルの [権限許可タイプ] フィールドの値が [クライアント資格情報] に設定されている場合に表示されます。サードパーティ OAuth プロバイダーの OAuth エンティティ プロファイルを設定する方法については、次を参照してください サードパーティ OAuth プロバイダーへの接続。 • [**MID Server** 経由で認証サーバーに接続] チェックボックスをオンにした場合は、[適用先] リストから必要な MID サーバー OR MID サーバー を特定する必要があります。
適用先	認証情報レコードがすべての MID Server または特定の MID Server に適用できるかどうかを指定します。特定の MID Server に適用する場合は、必要に応じてその MID Server を追加します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

OAuth 2.0 認証情報フォーム (続く)

フィールド	入力値
	重要: [**MID Server** 経由で認証サーバーに接続] チェックボックスをオンにした場合は、これらの考慮事項に注意してください。 • [適用先] で選択したすべてのユーザーが MID サーバー 認証サーバーと通信できることを確認します。これは、OAuth プロバイダーレコードに記載されている (OAuth 2.0 資格情報レコードで指定された OAuth エンティティプロファイルにリンクされている **)** トークン **URL** に対してトークン要求を実行するために必要です。  • 次の構成を持つものが少なくとも 1 つMID サーバーあることを確認します (MID サーバー[適用先] で選択済み)。 ◦ [状態] フィールドの値は [稼働中] です。 ◦ [検証済み] フィールドの値は [はい] です。 ◦ の機能は MID サーバー**REST** または **ALL** に設定されています。MID Serverの構成方法については、「」を参照してください https://www.webstg.servicenow.com/docs/access?context=configure-capabilities&version=washingtondc&pubname=washingtondc-integrate-applications&ft:locale=en-US 。 これらのステータスの詳細については、以下を参照してください MID Server dashboard 。
順番	ディスカバリー がデバイスにログオンしようとするときに、この認証情報を試行する順序 (シーケンス) 。番号が小さいほど、この認証情報がリストの上位に表示されます。多くの資格情報を使用する場合、またはログイン試行が 3 回失敗してセキュリティによってユーザーがロックアウトされた場合、資格情報の順序を確立します。すべての資格情報の順序番号が同じ (または順序番号がない) 場合、インスタンスは資格情報をランダムな順序で試行します。
資格情報エイリアス	OAuth 2.0 資格情報に関連付ける資格情報エイリアスを指定します。
統合タイプ	資格情報の統合タイプを示します。システムまたはユーザー固有の OAuth トークンを生成する OAuth 要求を使用して、サードパーティの API を呼び出します。統合タイプは次のとおりです。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

OAuth 2.0 認証情報フォーム (続く)

フィールド	入力値
	• システム：要求者プロファイルに基づいてトークン情報をプルします。 • 個人: ユーザー固有のトークン情報をプルします。セッションを開始するユーザーです。 [OAuth 要求者プロファイル] ページで [この個人 (This Personal)] が選択されている場合は、[個人 (**Personal**)] と呼ばれる追加のフラグが表示されます。 注: • ユーザーに関連する情報には、[統合タイプ] が [個人] のユーザー固有の OAuth トークンでのみアクセスできます。 • セッション ユーザー関連のトークンを使用するには、[フロー] プロパティで [実行 **]** フィールドを[セッションを開始するユーザー] として選択する必要があります。

SAP 認証情報

SAP 認証情報タイプにより、SAP JCo システムへのアクセスが管理されます。この認証情報タイプはディスカバリーとオーケストレーションで使用できます。

次のフィールドは、SAP タイプの認証情報の認証情報フォームで使用できます。

フィールド	説明
名前	この資格情報のわかりやすい一意の名前を入力します。
アクティブ	これらの資格情報の使用を有効または無効にします。
ユーザー名	[認証情報] テーブルに、作成するユーザー名を入力します。ユーザー名の先頭または末尾にはスペースを使用しないでください。プラットフォームでユーザー名の先頭または末尾のスペースが検出されると、警告が表示されます。CIM 検出の場合、ユーザーには admin ロールが必要です。
パスワード	パスワードを入力します。
資格情報 ID	外部認証情報システム用に MID Server にアップロードされた JAR ファイルに外部認証情報用に設定された一意のキーを入力します。[資格情報 **ID]** フィールドには 40 文字の制限があります。 このフィールドは、[外部の認証情報ストア] チェックボックスがオンになっている場合にのみ表示されます。
資格情報エイリアス	ワークフロー作成者は、個々の資格情報を Orchestration ワークフロー内の任意のアクティビティに割り当てたり、Orchestration ワークフロー内で同じアクティビティタイプが発生するたびに異なる資格情報を割り当てたりすることができます。 Service Mapping および検出パターンを使用してこの CI タイプに属していない CI を検出するために資格情報を使用するには、CI が属する CI タイプのテーブル名

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	(cmdb_ci_apache_web_server など) を入力します。詳細については、「資格情報をデフォルト以外に変更する」を参照してください。
外部の資格情報ストア	外部認証情報ストレージシステムを使用するには、このチェックボックスをオンにします。このオプションを選択すると、[ユーザー名] フィールドと [パスワード] フィールドが [認証情報 **ID]** フィールドに置き換えられます。外部の認証情報ストレージは、 外部認証情報ストレージ プラグインをアクティブ化した場合にのみ使用できます。 **注:** 現在サポートされている外部ストレージ システムは CyberArk だけです。
適用先	これらの認証情報をネットワーク内の [すべての **MID** サーバー] または 1 つ以上の [特定の **MID** サーバー] に適用するかどうかを選択します。**[MID** サーバー] フィールドでこれらの認証情報を使用する MID サーバー を指定します。
MID Server を使用	使用可能な MID Server のリストから 1 つ以上の MID Server を選択します。このレコードで設定された認証情報は、このリストの MID Server で使用できます。このフィールドは、[適用先] フィールドで [特定の **MID** サーバー] を選択した場合のみ使用できます。 **注:** [特定の **MID Server]** を選択しても、MID Server の選択には影響しません。これは、資格情報を表示する必要がある MID Server を決定するためにのみ使用されます。[特定の **MID Server]** はオーケストレーションアクティビティではサポートされていません。
順序	ディスカバリー がデバイスにログオンしようとするときに、この認証情報を試行する順序 (シーケンス) 。番号が小さいほど、この認証情報がリストの上位に表示されます。多くの資格情報を使用する場合、またはログイン試行が 3 回失敗してセキュリティによってユーザーがロックアウトされた場合、資格情報の順序を確立します。すべての資格情報の順序番号が同じ (または順序番号がない) 場合、インスタンスは資格情報をランダムな順序で試行します。
Windows MID サーバー サービスアカウント	有効な場合、定義された資格情報は MID サーバー サービスアカウントを表します。

SNMP 資格情報

ディスカバリー では、SNMP プロトコルを使用して、多くの種類のデバイス (スイッチ、ルーター、プリンターなど) を調べます。SNMP の認証情報にはユーザー名が含まれておらず、コミュニティ文字列と呼ばれるパスワードのみが含まれています。

多くの SNMP デバイス向けのデフォルトの読み取り専用コミュニティ文字列はパブリックであり、ディスカバリーは自動的にその文字列を試行します。*public* コミュニティ文字列ではない場合は、適切な SNMP 資格情報を入力してください。

SNMP を検出すると、設定されているすべてのコミュニティ文字列が使用されます。この動作は、SNMPv3 の検出には適用されません。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

デフォルトのオーケストレーション アクティビティの SNMP クエリーは、デバイスのオブジェクト識別子 (OID) を返し、SNMP 認証情報を求めます。

SNMP コミュニティ資格情報

SNMP コミュニティ認証情報タイプにより、SNMP プロトコルを使用して多くの種類のデバイス (スイッチ、ルーター、プリンターなど) を検出するためのアクセスが管理されます。この認証情報タイプは ディスカバリー、 サービスマッピング、および オーケストレーション で使用できます。

SNMP の認証情報にはユーザー名は含まれておらず、パスワード (コミュニティ文字列) のみが含まれます。多くの SNMP デバイス向けのデフォルトの読み取り専用コミュニティ文字列はパブリックであり、自動的にその文字列が試行されます。パブリックのコミュニティ文字列ではない場合は、適切な SNMP 認証情報を入力してください。

次のフィールドは、SNMP コミュニティの認証情報フォームで使用できます。

フィールド	説明
名前	この資格情報のわかりやすい一意の名前を入力します。
アクティブ	これらの資格情報の使用を有効または無効にします。
ユーザー名	[認証情報] テーブルに、作成するユーザー名を入力します。ユーザー名の先頭または末尾にはスペースを使用しないでください。プラットフォームでユーザー名の先頭または末尾のスペースが検出されると、警告が表示されます。CIM 検出の場合、ユーザーには admin ロールが必要です。
パスワード	パスワードを入力します。
資格情報 ID	外部認証情報システム用に MID Server にアップロードされた JAR ファイルに外部認証情報用に設定された一意のキーを入力します。[資格情報 **ID]** フィールドには 40 文字の制限があります。 このフィールドは、[外部の認証情報ストア] チェックボックスがオンになっている場合にのみ表示されます。
資格情報エイリアス	ワークフロー作成者は、個々の資格情報を Orchestration ワークフロー内の任意のアクティビティに割り当てたり、Orchestration ワークフロー内で同じアクティビティタイプが発生するたびに異なる資格情報を割り当てたりすることができます。 Service Mapping および検出パターンを使用してこの CI タイプに属していない CI を検出するために資格情報を使用するには、CI が属する CI タイプのテーブル名 (cmdb_ci_apache_web_server など) を入力します。詳細については、「資格情報をデフォルト以外に変更する」を参照してください。
外部の資格情報ストア	外部認証情報ストレージシステムを使用するには、このチェックボックスをオンにします。このオプションを選択すると、[ユーザー名] フィールドと [パスワード] フィールドが [認証情報 **ID]** フィールドに置き換えられます。外部の認証情報ストレージは、 外部認証情報ストレージ プラグインをアクティブ化した場合にのみ使用できます。 **注:** 現在サポートされている外部ストレージ システムは CyberArk だけです。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
適用先	これらの認証情報をネットワーク内の [すべての **MID** サーバー] または 1 つ以上の [特定の **MID** サーバー] に適用するかどうかを選択します。**[MID** サーバー] フィールドでこれらの認証情報を使用する MID サーバー を指定します。
MID Server を使用	使用可能な MID Server のリストから 1 つ以上の MID Server を選択します。このレコードで設定された認証情報は、このリストの MID Server で使用できます。このフィールドは、[適用先] フィールドで [特定の **MID** サーバー] を選択した場合のみ使用できます。 **注:** [特定の **MID Server]** を選択しても、MID Server の選択には影響しません。これは、資格情報を表示する必要がある MID Server を決定するためにのみ使用されます。[特定の **MID Server]** はオーケストレーションアクティビティではサポートされていません。
順序	ディスカバリー がデバイスにログオンしようとするときに、この認証情報を試行する順序 (シーケンス) 。番号が小さいほど、この認証情報がリストの上位に表示されます。多くの資格情報を使用する場合、またはログイン試行が 3 回失敗してセキュリティによってユーザーがロックアウトされた場合、資格情報の順序を確立します。すべての資格情報の順序番号が同じ (または順序番号がない) 場合、インスタンスは資格情報をランダムな順序で試行します。
Windows MID サーバー サービスアカウント	有効な場合、定義された資格情報は MID サーバー サービスアカウントを表します。

SNMPv3 認証情報

SNMPv3 資格情報は、プライバシープロトコルと追加のプライバシーキーを受け入れ、Discovery と Orchestration で使用できます。CyberArk の外部ストレージでは、プライバシーアカウントキーを選択できます。

次のフィールドは、SNMPv3 の認証情報フォームで使用できます。

SNMPv3 資格情報フィールド

フィールド	入力値
名前	この認証情報にわかりやすい一意の名前。たとえば、**SNMP Community Atlanta** と入力します。
有効	これらの資格情報の使用を有効または無効にします。
適用先	これらの資格情報をネットワーク内の [すべての **MID Server]** または 1 つ以上の [特定の **MID Server]** に適用するかどうかを選択します。**[MID Server]** フィールドでこれらの資格情報を使用する MID Server を指定します。
MID Server を使用	使用可能な MID Server のリストから 1 つ以上の MID Server を選択します。このレコードで設定された認証情報は、このリストの MID

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

SNMPv3 資格情報フィールド (続く)

フィールド	入力値
	Server で使用できます。このフィールドは、[適用先] フィールドで [特定の **MID Server]** を選択した場合のみ使用できます。
順番	ディスカバリー がデバイスにログオンしようとするときに、この認証情報を試行する順序 (シーケンス) 。番号が小さいほど、この認証情報がリストの上位に表示されます。多くの資格情報を使用する場合、またはログイン試行が 3 回失敗してセキュリティによってユーザーがロックアウトされた場合、資格情報の順序を確立します。すべての資格情報の順序番号が同じ (または順序番号がない) 場合、インスタンスは資格情報をランダムな順序で試行します。
ユーザー名	SNMP ユーザー名を入力します。ユーザー名の先頭または末尾にはスペースを使用しないでください。プラットフォームでユーザー名の先頭または末尾のスペースが検出されると、警告が表示されます。
認証プロトコル	この認証情報に使用する認証タイプを選択します。以下から選択可能です。 • MD5 • SHA-1 • SHA-224 • SHA-256 • SHA-384 • SHA-512
認証キー	この資格情報に使用する認証キーを入力します。
プライバシー プロトコル	この資格情報の暗号化プロトコルを選択します。以下から選択可能です。 • 3DES • AES128 • AES192 • AES256 • DES
プライバシー キー	選択したプライバシー プロトコルに関連付けられたキーを入力します。
資格情報 ID	外部資格情報プロバイダーに対して MID Server にアップロードされた JAR ファイルの外部資格情報用に設定された一意のキーを入力します。[資格情報 **ID]** フィールドには 40 文字の制限があります。 このフィールドは、[外部の認証情報ストア] チェックボックスがオンになっている場合にのみ表示されます。
プライバシー資格情報 ID (Privacy Credential ID)	CyberArk で SNMPv3 の資格情報用に設定されたプライバシーアカウントキーを入力します。CyberArk でプライバシープロトコルを使用している場合、このフィールドに CyberArk SNMPv3 プラ

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

SNMPv3 資格情報フィールド (続く)

フィールド	入力値
	イバシーアカウントの [名前] フィールドと同じ値を指定する必要があります。このフィールドは、[資格情報ストアタイプ] フィールドから [**CyberArk**] を選択した場合に、SNMPv3 に対してのみ表示されます。CyberArk のプライバシーキーを使用していない場合は、このフィールドを空白のままにします。
資格情報エイリアス	ワークフロー作成者は、個々の資格情報を Orchestration ワークフロー内の任意のアクティビティに割り当てたり、Orchestration ワークフロー内で同じアクティビティタイプが発生するたびに異なる資格情報を割り当てたりすることができます。
外部の資格情報ストア	外部認証情報ストレージシステムを使用するには、このチェックボックスをオンにします。外部ストレージが有効になっている場合は、[資格情報 **ID**] フィールドが表示されます。外部の資格情報ストレージは、 外部資格情報ストレージプラグインをアクティブ化し、[外部ストレージ **(External Storage)**] ビューが選択されている場合にのみ使用できます。
資格情報ストアタイプ	外部ストレージプロバイダーを選択します。CyberArk SNMPv3 プライバシーキーを使用している場合のみ、[**CyberArk**]を選択します。[プライバシー資格情報 **ID (Privacy Credential ID)**] フィールドが表示され、キーのエントリーが許可されます。
コンテキストを使用	この資格情報のコンテキスト値を追加するには、このチェックボックスをオンにします。このフィールドは [**Discovery**] ビューに表示されます。現在、外部資格情報ストレージではコンテキストはサポートされていません。 **注:** コンテキストは、特定の OID を参照する SNMPv3 資格情報によってアクセスされる管理情報の集合です。通常の資格情報ではアクセスできないデバイスに関する情報を収集するために、コンテキストが参照されることがあります。コンテキストは、メーカーが提供することも、個別に設定することもできます。追加情報については、「コンテキスト名とコンテキスト ID (Context Name and Context ID)」を参照してください。同じユーザー名とキーを持つ複数の SNMPv3 資格情報がある場合、一部のデバイスにコンテキストが必要であっても、その他のデバイスに必要なければ、デバイスごとに個別のレコードを作成する必要があります。
コンテキスト名	この資格情報のコンテキスト名の値を入力します。これは、フルアクセスでこの値が必要なデバイスがある場合のみ使用する必要があります。このフィールドは、[コンテキストを使用 **(Use Context)**] チェックボックスがオンになっている場合にのみ表示されます。

SSH 資格情報

ディスカバリー、Orchestration、統合ハブ では、SSH 資格情報を使用して UNIX デバイスと Linux デバイスを探索し、Secure Shell (SSH) を介してコマンドを実行します。SSH コマンドは、ルート資格情報または sudo を使用してルート権限で実行する必要があります。SSH 秘密鍵資格情報はセキュリティを強化します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

ルート権限の付与

ルート権限を付与する前に、組織内のセキュリティチームとともにセキュリティポリシーとオプションを確認してください。

次のいずれかの方法を使用すると、ユーザーはルート権限で SSH コマンドを実行することができます。

- ディスカバリー、Orchestration、統合ハブ の他の資格情報を指定しますが、これらの資格情報のユーザーには sudo を使用してルート権限で特定のコマンドを実行する権限を付与します。これによって、限られた特権を安全に付与できます。ディスカバリー、Orchestration、統合ハブ では、must_sudo パラメーターを [**true**] (デフォルトは [**false**]) に設定した任意のプローブで sudo を使用します。ただし、sudo が動作するように各システムを設定する必要があります。これを行うには、**visudo** コマンドを使用して **/etc/sudoers** ファイルを編集します。
- ルート認証情報を指定します。これらは明らかに最も強力な資格情報ですが、セキュリティの観点からは望ましくない場合があります。ディスカバリー、Orchestration、統合ハブ に任意の UNIX システムまたは Linux システムに対するルート資格情報がある場合は、それ以上構成する必要はありません。

特権コマンド

プラットフォームでは、MID Server で使用されるデフォルトの特権コマンドと、システムに他のコマンドを追加する機能が用意されています。sudo およびその他の特権コマンドの使用の詳細については、「MID Server の特権コマンド」を参照してください。

SSH 秘密鍵資格情報タイプ

注:
通常は SSH 秘密鍵資格情報を使用してください。SSH パスワード資格情報よりもセキュリティが優れています。

フィールド	入力値
名前	この認証情報にわかりやすい一意の名前。たとえば、**SSH Atlanta** と入力します。
アクティブ	これらの資格情報の使用を有効または無効にします。
ユーザー名	UNIX または Linux のユーザー名を入力します。ユーザー名の先頭または末尾にはスペースを使用しないでください。プラットフォームでユーザー名の先頭または末尾のスペースが検出されると、警告が表示されます。
パスワード	UNIX または Linux のパスワードを入力します。**[SSH** 秘密鍵] タイプの認証情報でユーザー名にパスワードが必要な場合は、sudo パスワードを入力します。
SSH パスフレーズ	セキュアな SSH パスフレーズを入力します。このフィールドは、**[SSH** 秘密鍵] の認証情報にのみ使用できます。
SSH 秘密鍵	SSH ログインのパスワードの代わりに使用できる安全な RSA、DSA、または ECDSA 秘密鍵を入力します。 秘密鍵は、正しく暗号化されるように、適切な形式で入力する必要があります。秘密鍵は、文字列 -----BEGIN で始める必要があります。 正しい形式の RSA 秘密鍵の例を次に示します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	入力値
	-----BEGIN RSA PRIVATE KEY----- MIIEogIBAAKCAQEAsEK65scPssPSobpDFMpR+Btv3MS4Q7NP8ERaStRZsh3IWz+x... ...7hrxV2dbSug60FahyupGWBGtPnXm5PaE2X5WPLuUj94ue48i1Fs -----END RSA PRIVATE KEY----- DSA キーの例を次に示します。 -----BEGIN DSA PRIVATE KEY----- MIIEogIBAAKCAQEAsEK65scPssPSobpDFMpR+Btv3MS4Q7NP8ERaStRZsh3IWz+x... ...7hrxV2dbSug60FahyupGWBGtPnXm5PaE2X5WPLuUj94ue48i1Fs -----END DSA PRIVATE KEY----- ECDSA キーの例を次に示します。 -----BEGIN EC PRIVATE KEY----- MIIEogIBAAKCAQEAsEK65scPssPSobpDFMpR+Btv3MS4Q7NP8ERaStRZsh3IWz+x... ...7hrxV2dbSug60FahyupGWBGtPnXm5PaE2X5WPLuUj94ue48i1Fs -----END EC PRIVATE KEY----- Now Platform では、OpenSSH ssh-keygen ユーティリティで生成された PEM 形式の秘密鍵をサポートしています。PuTTY によって生成された PPK キーを変換するには、次の手順に従います。 • PuTTYGen で秘密鍵を開きます。 • メニューからOpenSSH形式でエクスポートします 変換 > **OpenSSH** キーをエクスポート. • 新しい OpenSSH キーを保存します。
SSH 証明書	証明書を使用して SSH ログイン用の RSA ベースの OpenSSH 証明書を入力します。証明書を入力すると、証明書ベースの認証に秘密キーが使用されます。この認証は OpenSSH 7.8 以降でサポートされています。
資格情報エイリアス	• Flow Designer が別名を使用して接続と資格情報を管理できるようにします。エイリアスを使用することで、複数の環境を使用する場合に、複数の資格情報と接続情報プロファイルを構成する必要がなくなります。接続または資格情報が変更された場合、接続を使用するどのアクションも更新する必要はありません。詳細については、「接続と資格情報」を参照してください。 • ワークフロー作成者は、個々の資格情報を Orchestration ワークフロー内の任意のアクティビティに割り当てたり、Orchestration ワークフロー内で同じアクティビティタイプが発生するたびに異なる資格情報を割り当てたりすることができます。
外部の資格情報ストア	外部認証情報ストレージシステムを使用するには、このチェックボックスをオンにします。このオプションを選択すると、[ユーザー名] フィールドと [パスワード] フィールドが [認証情報 **ID]** フィールドに置き換えられます。現在サポートされている外部ストレージ システムは CyberArk だけです。
MID Server を使用	使用可能な MID Server のリストから 1 つ以上の MID Server を選択します。このレコードで設定された認証情報は、このリストの MID Server で使用できます。このフィールドは、[適用先] フィールドで [特定の **MID Server]** を選択した場合のみ使用できます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	入力値
適用先	これらの資格情報をネットワーク内の [すべての **MID Server]** または 1 つ以上の [特定の **MID Server]** に適用するかどうかを選択します。**[MID Server]** フィールドでこれらの資格情報を使用する MID Server を指定します。
順序	プラットフォームがデバイスへのログインを試行するときにこの資格情報を試行する順序 (シーケンス)。番号が小さいほど、この資格情報がリストの上位に表示されます。多くの資格情報を使用する場合、またはログイン試行が 3 回失敗してセキュリティによってユーザーがロックアウトされた場合、資格情報の順序を確立します。すべての資格情報に同じ順序番号を設定した場合、または何も設定しない場合、Discovery または Orchestration では、資格情報をランダムな順序で試行します。

SSH 資格情報タイプ

次のフィールドは、SSH 資格情報フォームで使用できます。

フィールド	説明
名前	この資格情報のわかりやすい一意の名前を入力します。
アクティブ	これらの資格情報の使用を有効または無効にします。
ユーザー名	[資格情報] テーブルに、作成するユーザー名を入力します。ユーザー名の先頭または末尾にはスペースを使用しないでください。プラットフォームでユーザー名の先頭または末尾のスペースが検出されると、警告が表示されます。CIM 検出の場合、ユーザーには admin ロールが必要です。
パスワード	パスワードを入力します。
資格情報 ID	外部認証情報システム用に MID Server にアップロードされた JAR ファイルに外部認証情報用に設定された一意のキーを入力します。[資格情報 **ID]** フィールドには 40 文字の制限があります。 このフィールドは、[外部の認証情報ストア] チェックボックスがオンになっている場合にのみ表示されます。
資格情報エイリアス	• Flow Designer が別名を使用して接続と資格情報を管理できるようにします。エイリアスを使用することで、複数の環境を使用する場合に、複数の資格情報と接続情報プロファイルを構成する必要がなくなります。接続または資格情報が変更された場合、接続を使用するどのアクションも更新する必要はありません。詳細については、「接続と資格情報」を参照してください。 • ワークフロー作成者は、個々の資格情報を Orchestration ワークフロー内の任意のアクティビティに割り当てたり、Orchestration ワークフロー内で同じアクティビティタイプが発生するたびに異なる資格情報を割り当てたりすることができます。Service Mapping および検出パターンを使用してこの CI タイプに属していない CI を検出するために資格情報を使用するには、CI が属する CI タイプのテーブル名 (cmdb_ci_apache_web_server など) を入力します。詳細については、「資格情報をデフォルト以外に変更する」を参照してください。
外部の資格情	外部認証情報ストレージシステムを使用するには、このチェックボックスをオンにします。このオプションを選択すると、[ユーザー名] フィールドと [パスワード] フィールドが

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
報ストア	[認証情報 **ID]** フィールドに置き換えられます。外部の認証情報ストレージは、 外部認証情報ストレージ プラグインをアクティブ化した場合にのみ使用できます。 **注:** 現在サポートされている外部ストレージ システムは CyberArk だけです。
適用先	これらの認証情報をネットワーク内の [すべての **MID** サーバー] または 1 つ以上の [特定の **MID** サーバー] に適用するかどうかを選択します。**[MID** サーバー] フィールドでこれらの認証情報を使用する MID サーバー を指定します。
MID Server を使用	使用可能な MID Server のリストから 1 つ以上の MID Server を選択します。このレコードで設定された認証情報は、このリストの MID Server で使用できます。このフィールドは、[適用先] フィールドで [特定の **MID Server]** を選択した場合のみ使用できます。
順番	ディスカバリー がデバイスにログオンしようとするときに、この認証情報を試行する順序 (シーケンス) 。番号が小さいほど、この認証情報がリストの上位に表示されます。多くの資格情報を使用する場合、またはログイン試行が 3 回失敗してセキュリティによってユーザーがロックアウトされた場合、資格情報の順序を確立します。すべての資格情報の順序番号が同じ (または順序番号がない) 場合、インスタンスは資格情報をランダムな順序で試行します。

Discovery、Orchestration、統合ハブ のルート権限が必要なコマンド

次の例では、ユーザー名が **Disco** であることを前提とします。実際のユーザー名に置き換えて、コマンドのパスがシステム上のパスと一致することを確認してください。

注:
sudo コマンドに入力するパスワードがないため、sudo コマンドは秘密鍵資格情報と連携しません。解決策は、*NOPASSWD* オプションを sudo 構成に追加することです。たとえば、disco ALL=(root) NOPASSWD:/usr/sbin/dmidecode,/usr/sbin/lsof,/sbin/ifconfig と入力します。

ルート権限が必要な **UNIX** コマンドおよび **Linux** コマンド

コマンド	目的
HP-UX	
adb	CPU の速度とメモリーを収集します。 • [**/etc/sudoers** 行の例]：Disco ALL=(root) /usr/bin/adb • [使用者]：Discovery
Linux および **UNIX** のすべてのバージョン	
chage	前回のパスワード変更日からパスワードを変更するまでの日数を変更します。 • [**/etc/sudoers** 行の例]：Disco ALL=(root) /usr/bin/chage • [使用者]：Orchestration と 統合ハブ
chpasswd	ユーザーパスワードを変更します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ルート権限が必要な **UNIX** コマンドおよび **Linux** コマンド (続く)

コマンド	目的
	• [**/etc/sudoers** 行の例]：Disco ALL=(root) /etc/chpasswd • [使用者]：Orchestration と 統合ハブ
すべての **Linux**	
dmidecode	マザーボード内に埋め込まれたシリアル番号など、ハードウェアに関するいくつかの情報を収集します。 • [**/etc/sudoers** 行の例]：Disco ALL=(root) /sbin/dmidecode • [使用者]：Discovery
fdisk	システム上のディスクおよびサイズ情報を収集します。 • [**/etc/sudoers** 行の例]：Disco ALL=(root) /usr/bin/fdisk -l • [使用者]：Discovery
multipath	MPIO のデバイス マッピングを収集します。 • [**/etc/sudoers** 行の例]：Disco ALL=(root) /usr/bin/multipath -ll • [使用者]：Discovery
Linux および **Solaris**	
dmsetup	低レベルのボリュームを調べます。 • [**/etc/sudoers** 行の例]： ◦ Disco ALL=(root) /usr/bin/dmsetup table * ◦ Disco ALL=(root) /usr/bin/dmsetup ls • [使用者]：Discovery
UNIX のすべてのバージョン	
lsof	プロセスとシステムへの接続との関係を決定します。 • [**/etc/sudoers** 行の例]：Disco ALL=(root) /sbin/lsof • [使用者]：Discovery
oratab	Oracle ホームおよび pfile を検索するために oratab ファイルへの読み取りアクセス権を付与します。 • [**/etc/sudoers** 行の例]：N/A • [使用者]：Discovery
Solaris	
iscsiadm	iSCSI IQNs を取得

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ルート権限が必要な **UNIX** コマンドおよび **Linux** コマンド (続く)

コマンド	目的
	• [**/etc/sudoers** 行の例]：${sudo:iscsiadm list target -S} • [使用者]：Discovery
fcinfo	ポートの WWPN を取得します。 • [**/etc/sudoers** 行の例]：${sudo:fcinfo remote-port -sl -p $port} • [使用者]：Discovery
prtvtoc	ディスク パーティションに関する情報をレポートします。 • [**/etc/sudoers** 行の例]：Disco ALL=(root) /usr/bin/prtvtoc • [使用者]：Discovery
pfiles	TCP 接続情報を収集するために使用されます。 • **/etc/sudoers** 行の例:Disco ALL=(root) /usr/bin/pfiles • [使用者]：Discovery
Pgrep	pfile を実行する特定の領域のプロセス ID をリストするために使用されます。 • **/etc/sudoers** 行の例:Disco ALL=(root) /usr/bin/pgrep • [使用者]：Discovery
/usr/bin/ps	実行中のプロセスを一覧表示します。ルート アクセスで実行する代わりに、proc_owner ロールを追加します。 • [**/etc/sudoers** 行の例]：Disco ALL=(root) /usr/bin/ps • [使用者]：Discovery
/usr/ucb/ps	実行中のプロセスを一覧表示します。ルート アクセスで実行する代わりに、proc_owner ロールを追加します。 `/usr/ucb/ps` コマンドの使用は、Solaris 11 の時点で廃止となっています。ディスカバリー、オーケストレーション、統合ハブ では、Solaris のすべてのバージョンに対してこのコマンドを使用しなければならないため、Solaris 11 システムに ucb ユーティリティを手動でインストールする必要があります。手順については、「KB0564262」を参照してください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ルート権限が必要な **UNIX** コマンドおよび **Linux** コマンド (続く)

コマンド	目的
	• [**/etc/sudoers** 行の例]：Disco ALL=(root) /usr/ucb/ps • [使用者]：Discovery

Discovery および Service Mapping に必要な特権コマンドのリストについては、「Service Mapping commands requiring a privileged user」を参照して、組織内で Unix ベースのホストを検出およびマッピングするために、昇格された権限を必要とするコマンドのリストを確認してください。

ルート以外の認証情報のアクセス要件

ディスカバリー にルート アクセスの資格情報を指定しない場合は、次のアクセス要件で資格情報を指定する必要があります。

アプリケーション	ファイルまたはディレクトリー	必要なアクセス権
Apache	httpd.conf	読み取り
Hbase	hbase-site.xml	読み取り
JBoss	jboss-service.xml	読み取り
	JBoss ホーム ディレクトリー	読み取り
	web.xml	読み取り
MySQL	my.cnf	読み取り
NGINX	nginx.conf	読み取り
Oracle	oratab	読み取り
	関連する pfile	読み取り
Oracle リスナー	lsnrctl	実行
	listener.ora	読み取り
Tomcat	catalina.jar	読み取り
	server.xml	読み取り
	web.xml	読み取り
Unix	/etc/*release	読み取り
	/etc/bashrc	読み取り
	/etc/profile	読み取り
	/proc/cpuinfo	読み取り
	/proc/vmware/sched/ncpus	読み取り
	/var/log/dmesg	読み取り
	APD ディレクトリー	読み取り
WebSphere	cell.xml	読み取り
	server.xml	読み取り

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

アプリケーション	ファイルまたはディレクトリー	必要なアクセス権
	serverindex.xml	読み取り

VMware 資格情報

VMware 認証情報タイプは、vCenter 認証情報へのアクセスを管理します。

VMware クラウドリソースにアクセスするアプリケーションは、VMware 資格情報にアクセスする必要があります。 たとえば、ディスカバリーでは、VMware 認証情報タイプを使用すると、Windows マシン上で実行されている VMware の vCenter を検索して、ESX マシン、仮想マシン、およびリソースプールを検出できます。VMware ディスカバリー および自動化 API (vCenter API) により、コンピューター CI に対してグローバルに一意なシリアル番号が提供されます。各 VMware ホストへのアクセスを有効にするために、CIM 認証情報は必要ありません。

注:
有効な VMware 認証情報を使用している場合、vCenter ディスカバリー に Windows 認証情報は不要です。

重要:
vCenter によってクローンされた個々の仮想マシン上で作業 (Linux VM の再起動など) を実行するオーケストレーション アクティビティには、**[VMware]** タイプの認証情報を使用しないでください。これらのアクティビティの場合、認証情報の [種類] は仮想マシンのオペレーティング システム (**[SSH]** または **[Windows]**) によって決まります。

[VMWare 認証情報] フォーム

フィールド	説明
名前	VMware 資格情報のわかりやすい一意の名前を入力します。
有効	これらの資格情報の使用を有効または無効にします。
ユーザー名	VMware アカウントに使用するユーザー名を入力します。ユーザー名の先頭または末尾にはスペースを使用しないでください。プラットフォームでユーザー名の先頭または末尾のスペースが検出されると、警告が表示されます。 VMware 資格情報は、vCenter で読み取り専用ロールを持っている必要があります。
パスワード	VMware アカウントのパスワードを入力します。
適用先	使用可能な MID サーバーのリストから 1 つ以上 MID サーバーを選択します。このレコードで設定された認証情報は、このリストの MID サーバーで使用できます。このフィールドは、[適用先] フィールドで [特定の **MID** サーバー] を選択した場合のみ使用できます。
順序	ディスカバリー がデバイスにログオンしようとするときに、この認証情報を試行する順序 (シーケンス) 。番号が小さいほど、この認証情報がリストの上位に表示されます。多くの資格情報を使用する場合、またはログイン試行が 3 回失敗してセキュリティによってユーザーがロックアウトされた場合、資格情報の順序を確立します。すべての資格情報の順序番号が同じ (または順序番号がない) 場合、インスタンスは資格情報をランダムな順序で試行します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Windows 資格情報

Windows 認証情報により、Windows コンピューターへのアクセス権が付与されます。この認証情報タイプはディスカバリーとオーケストレーションで使用できます。

認証情報の要件

ディスカバリーとオーケストレーションには、Windows 認証情報に関して次の要件があります。

- MID Server を Windows ホストにサービスとしてインストールする。
- 次のいずれかの場所に Windows 認証情報を追加する。
  - 認証情報 [windows_credentials] テーブルのエントリー
  - 特定の Windows ユーザーまたはドメイン アカウントとして実行する MID Server サービスアカウント

適切な権限の付与

十分な権限を与えるには、 Windows 認証情報は次のいずれかでなければなりません。

- ターゲット の Windows ホストでローカル管理者アクセス権を持つドメイン ユーザー。
- 同じターゲット ホストで管理者権限とユーザー アクセス制御 (UAC) が無効になっているローカル アカウント。
- Windows プローブとパーミッション の要件を満たすユーザー (ディスカバリー のみ)。
- 実行する Orchestration アクティビティの要件を満たすユーザー (Orchestration のみ)。

注:
ログオン権限は必要ありません。アカウントはインタラクティブである必要はありません。

特権アクセスの付与に関するセキュリティは、JEA プロファイルを使用して ディスカバリー を実行することで強化できます。詳細については、「Discovery 用 Microsoft Just Enough Administration (JEA) 」を参照してください。

ワークグループ コンピューター

Powershell コマンドを実行してワークグループ コンピューターを検出するには、次のいずれかのユーザーに対して MID Server の認証情報を設定します。

- ワークグループ コンピューターに組み込まれた管理者アカウント。
- ワークグループ コンピューターのドメイン ユーザー。

マルチドメイン構成

Windows 認証情報を複数のドメイン間で機能させるには、正しい名前形式と MID Server 構成を使用していることを確認してください。

ディスカバリーとオーケストレーションでは、Windows ドメイン認証情報をユーザープリンシパル名とダウンレベル ログオン名の両方のユーザー名形式でサポートしています。たとえば、**Domain\UserName** または **UserName@example.domain.com** です。WORKGROUP\UserName の形式で Windows ワークグループの認証情報を入力できます。

注:
また、**.** ユーザー名を使用してローカル アカウントを入力することもできます。

これらの追加の操作は、認証情報を複数の Windows ドメインにわたって機能させるために必要です。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

条件	必要な他のアクション
Windows ターゲットと同じドメイン上の MID Server ホスト。	なし
Windows ターゲットとは異なるドメイン上の MID Server ホスト。	PowerShell 3.0 (以降 5.1 以前) が MID Server ホストにインストールされていることを確認してください。
Microsoft SQL Server ターゲットとは異なるドメイン上の MID Server ホスト。	「MSSQL サーバーの検出」を参照してください。

Windows 資格情報タイプ

次のフィールドは、Windows の認証情報フォームで使用できます。

フィールド	説明
名前	この資格情報のわかりやすい一意の名前を入力します。
アクティブ	これらの資格情報の使用を有効または無効にします。
ユーザー名	[認証情報] テーブルに、作成するユーザー名を入力します。ユーザー名の先頭または末尾にはスペースを使用しないでください。プラットフォームでユーザー名の先頭または末尾のスペースが検出されると、警告が表示されます。CIM 検出の場合、ユーザーには admin ロールが必要です。
パスワード	パスワードを入力します。
資格情報 ID	外部認証情報システム用に MID Server にアップロードされた JAR ファイルに外部認証情報用に設定された一意のキーを入力します。[資格情報 **ID]** フィールドには 40 文字の制限があります。 このフィールドは、[外部の認証情報ストア] チェックボックスがオンになっている場合にのみ表示されます。
資格情報エイリアス	ワークフロー作成者は、個々の資格情報を Orchestration ワークフロー内の任意のアクティビティに割り当てたり、Orchestration ワークフロー内で同じアクティビティタイプが発生するたびに異なる資格情報を割り当てたりすることができます。 Service Mapping および検出パターンを使用してこの CI タイプに属していない CI を検出するために資格情報を使用するには、CI が属する CI タイプのテーブル名 (cmdb_ci_apache_web_server など) を入力します。詳細については、「資格情報をデフォルト以外に変更する」を参照してください。
外部の資格情報ストア	外部認証情報ストレージシステムを使用するには、このチェックボックスをオンにします。このオプションを選択すると、[ユーザー名] フィールドと [パスワード] フィールドが [認証情報 **ID]** フィールドに置き換えられます。外部の認証情報ストレージは、 外部認証情報ストレージ プラグインをアクティブ化した場合にのみ使用できます。 **注:** 現在サポートされている外部ストレージ システムは CyberArk だけです。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
適用先	これらの認証情報をネットワーク内の [すべての **MID** サーバー] または 1 つ以上の [特定の **MID** サーバー] に適用するかどうかを選択します。**[MID** サーバー] フィールドでこれらの認証情報を使用する MID サーバー を指定します。
MID Server を使用	使用可能な MID Server のリストから 1 つ以上の MID Server を選択します。このレコードで設定された認証情報は、このリストの MID Server で使用できます。このフィールドは、[適用先] フィールドで [特定の **MID** サーバー] を選択した場合のみ使用できます。 **注:** [特定の **MID Server]** を選択しても、MID Server の選択には影響しません。これは、資格情報を表示する必要がある MID Server を決定するためにのみ使用されます。[特定の **MID Server]** はオーケストレーションアクティビティではサポートされていません。
順序	ディスカバリー がデバイスにログオンしようとするときに、この認証情報を試行する順序 (シーケンス) 。番号が小さいほど、この認証情報がリストの上位に表示されます。多くの資格情報を使用する場合、またはログイン試行が 3 回失敗してセキュリティによってユーザーがロックアウトされた場合、資格情報の順序を確立します。すべての資格情報の順序番号が同じ (または順序番号がない) 場合、インスタンスは資格情報をランダムな順序で試行します。
Windows MID サーバー サービスアカウント	有効な場合、定義された資格情報は MID サーバー サービスアカウントを表します。

MID Server 用の **Windows** 認証情報の設定

独自の Windows サービスの認証情報または認証情報 [discovery_credentials] テーブルの認証情報を使用するように MID Server を設定します。

始める前に
必要なロール：admin

手順

1. MID Server サービスアカウントの資格情報を使用するように MID Server を設定します。
   a. [Windows MID Server サービスの資格情報の設定] を、権限の要件を満たすユーザーに設定します。
   b. ユーザー名が名前形式の要件を満たしていることを確認します。
   c. 必要に応じて、フォームのフィールドに入力します。
   d. 認証情報がドメイン要件を満たしていることを確認します。
2. 認証情報 [discovery_credentials] テーブルの認証情報を使用するように MID Server を設定します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

a. 個々の Windows 認証情報を認証情報 [windows_credentials] テーブルに追加します。
- 各認証情報が権限の要件を満たしていることを確認します。
- 各ユーザー名が名前形式の要件を満たしていることを確認します。
- 各認証情報が Windows ドメイン要件を満たしていることを確認します。

b. オプション: mid.use_powershell パラメーターを **true** に設定することで、PowerShell を使用するように MID Server を設定します。
「MID Server の構成」を参照してください。

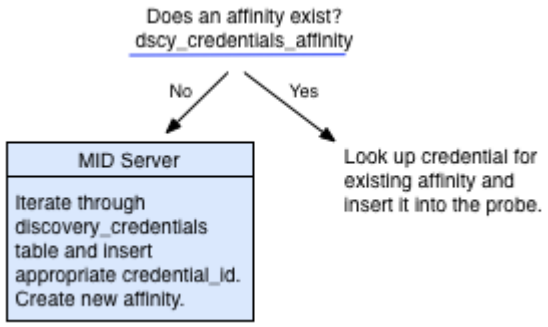
c. 特定の Windows ユーザーまたはドメインアカウントとして実行する Windows MID Server サービスアカウントを表す資格情報を作成するには、[Windows MID Server サービスアカウント (Windows MID Server Service Account)] チェックボックスをオンにします。

ディスカバリーとオーケストレーションの資格情報親和性

資格情報親和性とは、一連の資格情報とネットワーク上のデバイス間の関連付けです。

ディスカバリー またはオーケストレーションで初めてデバイスにアクセスしようとすると、正しい資格情報が見つかるまで利用可能なすべての資格情報が試行されます。デバイスの資格情報を特定した後、ディスカバリー とオーケストレーションでは、資格情報親和性 [dscy_credentials_affinity] テーブルを使用して資格情報とデバイス間の親和性が作成されます。後続のすべての検出またはオーケストレーション アクティビティで、このテーブルの資格情報が、親和性が存在するデバイスと照合されます。デバイスの資格情報が変更された場合、 ディスカバリー とオーケストレーションでは、新しい親和性を作成するまで利用可能な資格情報をすべて再試行します。

資格情報親和性の図



注:
オーケストレーションと ディスカバリー がインストールされ、資格情報エイリアスが有効になっている場合、複数の親和性が存在する可能性があります。この場合、プラットフォームでは、親和性ごとに資格情報が検索され、順序が最も低い親和性の資格情報がプローブに挿入されます。

認証情報のトラブルシューティング

ECC キュー ペイロードの <credentials_debug> セクションをレビューして、認証情報に関する問題をトラブルシューティングします。

特定のプローブでは資格情報のデバッグがサポートされています。資格情報のデバッグにより、MID Server が返すペイロードの <credentials_debug> セクションがインスタンス ECC キューに挿入されます。<credentials_debug> セクションを表示して、認証情報ルックアップに関する詳細を確認できます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

次の場合に、<credentials_debug> セクションがペイロードに表示されます。

- WMIRunner プローブ、 PowerShell プローブ、 JMS、または SSHCommand プローブ の資格情報が失敗した場合。
- WMIRunner プローブ、PowerShell プローブ、または SSHCommand プローブの *credentials_debug* パラメーターを **true** に設定します。そのパラメーターを true に設定すると、認証情報ルックアップが成功した場合でも、<credentials_debug> セクションが表示されます。

<credentials_debug> セクションに表示される内容は次のとおりです。

- 認証情報のタイプ、タグ、親和性など、認証情報の検索に関する情報。
- ターゲットとなる IP アドレス。
- タイプ、分類、タグ、名前、システム ID、外部資格情報 ID (存在する場合) など、MID Server が使用した各資格情報 (順番に) に関する情報。

無効な認証情報を示すサンプル ペイロード

Payload XML


```
<?xml version="1.0" encoding="UTF-8"?><results probe_time="6891" result_code="0"><result
id="6f10ed420a0a0b7e49052d83a32b586f" name="sh ${file:esx.sh}" order="1" topic="SSHCommand"><results
error="SSHCommand: Adding target to blacklist.  No valid credential found for types [SSH Password,SSH
Private Key]" probe_time="6860" result_code="42"><result error="SSHCommand: Adding target to blacklist.
No valid credential found for types [SSH Password,SSH Private Key]"><debug_info>{"debug_info":
[{"10.11.129.81":{"credentials_attempted":[{"credential_type":"SSH
Password","credential_name":"badCredential1","credential_order":"100","credential_success":false,"credenti
al_id":"6b43751d1362a200efffb6004244b0c3"},{"credential_type":"SSH
Password","credential_name":"badCredential2","credential_order":"200","credential_success":false,"credenti
al_id":"1553b11d1362a200efffb6004244b01b"},{"credential_type":"SSH
Password","credential_name":"badCredential3","credential_order":"300","credential_success":false,"credenti
al_id":"7d63f11d1362a200efffb6004244b0b0"}],"adding_key_to_target_blacklist":true,"connection_parameters":
{"credential_types":["SSH Password","SSH Private Key"],"target":"10.11.129.81"}}}]}</debug_info></result>
<parameters><parameter name="discover" value="CIs"/><parameter name="agent"
value="mid.server.demonightlyIstanbul_MID"/><parameter name="glide.xmlhelper.trim.enable" value="true"/>
<parameter name="use_class" value="discovery_classy_unix"/><parameter name="source" value="10.11.129.81"/>
<parameter name="priority" value="0"/><parameter name="use_snc_ssh" value="true"/><parameter name="probe"
value="10e0eebd0a0a0b4f61f46a5027df7fb6"/><parameter name="port_probe"
value="97ff2abd0a0a070300b7f37daa11a241"/><parameter name="port" value="22"/><parameter name="cidata"
value="&lt;CIData&gt;&lt;data&gt;&lt;fld name=&quot;ip_address&quot;&gt;10.11.129.81&lt;/fld&gt;&lt;/data&
gt;&lt;/CIData&gt;"/><parameter name="used_by_discovery" value="true"/><parameter name="name" value="sh
${file:esx.sh}"/><parameter name="topic" value="SSHCommand"/><parameter name="esx.sh" value="#!/bin
/sh&#13;&#10;# This command is rarely installed, so a Bourne shell script is used to squelch the exit
status and sensor warning when not found.&#13;&#10;# tcsh doesn't squelch exist status codes within
backticked statements&#13;&#10;echo `vmware -v 2&gt;&amp;1`"/><parameter name="ecc_queue" value=""/>
</parameters></results></result><result id="e5e075a2a9fe1561018f2a9636d5ec39" name="uname -a" order="1"
topic="SSHCommand"><results error="SSHCommand: Target is blacklisted.  No valid credential found for
```


以下の場合、PowerShell パラメーターの詳細が表示されます。

- すべての Windows 資格情報が失敗した後にローカル MID Server 資格情報が使用された場合。
- MID Server がオンになっている同じマシンを検出しようとしているために資格情報がスキップされた場合。
- mid.powershell.use_credentials パラメーターが true に設定されている場合。

以下の場合、SSHCommand の詳細が表示されます。

- ターゲット IP が除外されているために資格情報の検索がスキップされた場合。
- ターゲット IP が除外リストに追加された場合。

注:
MID Server では、失敗した資格情報検索の IP アドレスがキャッシュメモリーの除外リストに保存されます。この除外リストにより、MID Server でアクセスの試行を停止するデバイスが指定されます。すべての資格情報が失敗すると、IP アドレスが除外リストに追加されます。IP アドレスは、MID Server が再起動された場合、またはインスタンスの資格情報レコードが更新された場合のいずれかで、5 分後に除外リストキャッシュから消去されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

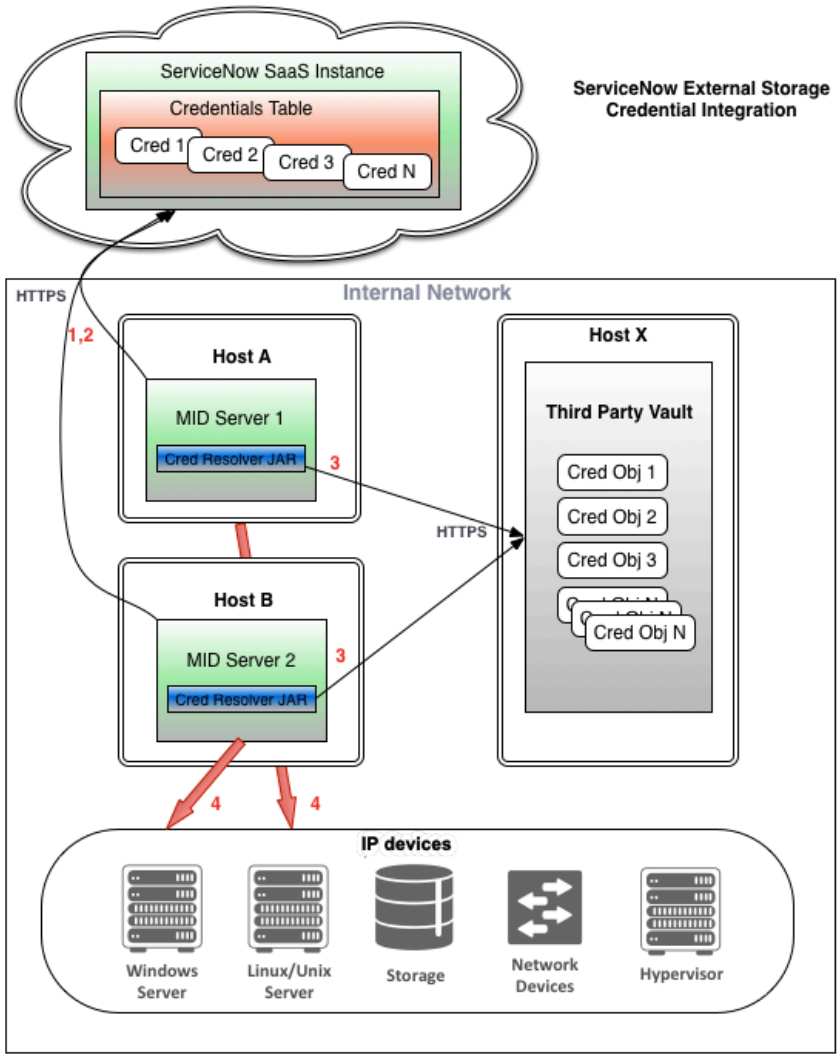
外部認証情報ストレージ

インスタンスは、 ディスカバリー、オーケストレーション、および サービスマッピング で使用される認証情報を ServiceNow 認証情報レコードに直接保存する代わりに、外部認証情報リポジトリーに保存することができます。

インスタンスは、各認証情報の一意の識別子、認証情報タイプ (SSH、SNMP、Windows など)、および任意の資格情報親和性を保持します。MID Server は、インスタンスから認証情報識別子を取得してから、顧客が提供した JAR ファイルを使用してその識別子をリポジトリーから使用可能な認証情報に解決します。現在、ServiceNow プラットフォームでは、外部認証情報ストレージ用に CyberArk ボールトの使用がサポートされています。

外部認証情報ストレージのアーキテクチャ

外部認証情報ストレージのアーキテクチャ



認証情報プロセス フロー

MID Server は、次のプロセスを使用して外部ストアから認証情報を取得します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

1. MID Server は、ターゲット ボールトの対応する認証情報 ID が含まれている ServiceNow 認証情報 [discovery_credentials] から認証情報オブジェクトをダウンロードします。
2. 各プローブまたはパターンが ディスカバリー または オーケストレーション ジョブから実行されると、MID Server は、資格情報 ID、ターゲット IP アドレス、資格情報タイプなどの情報を資格情報リゾルバー Java Jar ファイルに渡すことによって資格情報を要求します。ボールトから取得する正しい資格情報オブジェクトに関する詳細は、資格情報リゾルバーによって決定されます。

   CyberArk などの多くの資格情報リゾルバーは、MID Server と同じマシン上で実行されているサードパーティのボールトベンダーが提供するアプリケーションを呼び出します。多くの場合、このアプリケーションは資格情報をキャッシュするように構成でき、ボールトで資格情報が変更されたときにキャッシュを更新させることができます。これは、MID Server が資格情報を要求するたびにボールトへの不要なネットワーク呼び出しを回避するために非常に重要です。資格情報リゾルバー (オプションのベンダーアプリケーションが存在する場合はそれを使用) はボールトを呼び出し、実際のユーザー名やパスワードなどを取得します。

   すぐに利用可能な資格情報リゾルバー (現在は CyberArk のみ) の場合、MID Server は、MID Server プロセスメモリーの暗号化を使用して、最大数秒間だけ資格情報をキャッシュします。これは、単一のデバイスを検出する場合でも、MID Server が同じ資格情報の資格情報リゾルバーに対して複数の要求を行うことができることを意味します。他の資格情報リゾルバーのキャッシュ実装については、サードパーティベンダーにお問い合わせください。
3. MID Server は、適切な認証情報を使用してプローブを実行します。

注:
資格情報親和性は引き続き適用されます。メカニズムは同じままです。MID Server の観点との唯一の違いは、実際の認証情報の詳細 (ユーザー名とパスワード) がサードパーティのボールトから取得される点です。

外部資格情報ストレージのログ記録

MID Server から外部認証情報ストレージに関する関するログ メッセージが投稿されます。

資格情報要求を解決しようとしているときにリポジトリにエラーが発生した場合、MID Server は「クライアントの CredentialResolver に関する問題：」というプリフィックスが付いたログメッセージを送信します。

外部認証情報ストレージとともにインストールされるコンポーネント

ビジネスルール

外部資格情報ストレージのビジネスルールは、管理者が [外部資格情報ストレージの有効化] プロパティを変更すると、次のタスクを実行します。

- 認証情報レコードリストおよびフォームのビューを外部ストレージビューに変更します。このビューを使用すると、ユーザーはリスト内の [資格情報 **ID]** 列を確認できます。
- MID Server に、資格情報の取得方法の変更に備えて、資格情報キャッシュを更新するように指示します。

プロパティ

外部認証情報ストレージの有効化 [com.snc.use_external_credentials] と呼ばれるプロパティは、External Credential Storage プラグインがアクティブにされた後で、それを有効または無効にします。プロパティの場所は ディスカバリー定義 > プロパティ および オーケストレーション > **MID** サーバープロパティであり、プラグインを有効にすると有効になります。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

システムプロパティを使用して外部認証情報ストレージを無効にする場合、システムは自動的にすべての外部認証情報をインスタンス内で非アクティブに設定します。このプロパティを使用して機能を再度有効にしても、外部認証情報レコードはアクティブにリセットされません。それぞれの資格情報レコードを手動で再アクティブ化する必要があります。

Discovery および Orchestration 用の外部資格情報ストレージの要求

外部資格情報ストレージ プラグインは、リクエストにより利用可能です。

始める前に

必要なロール：admin

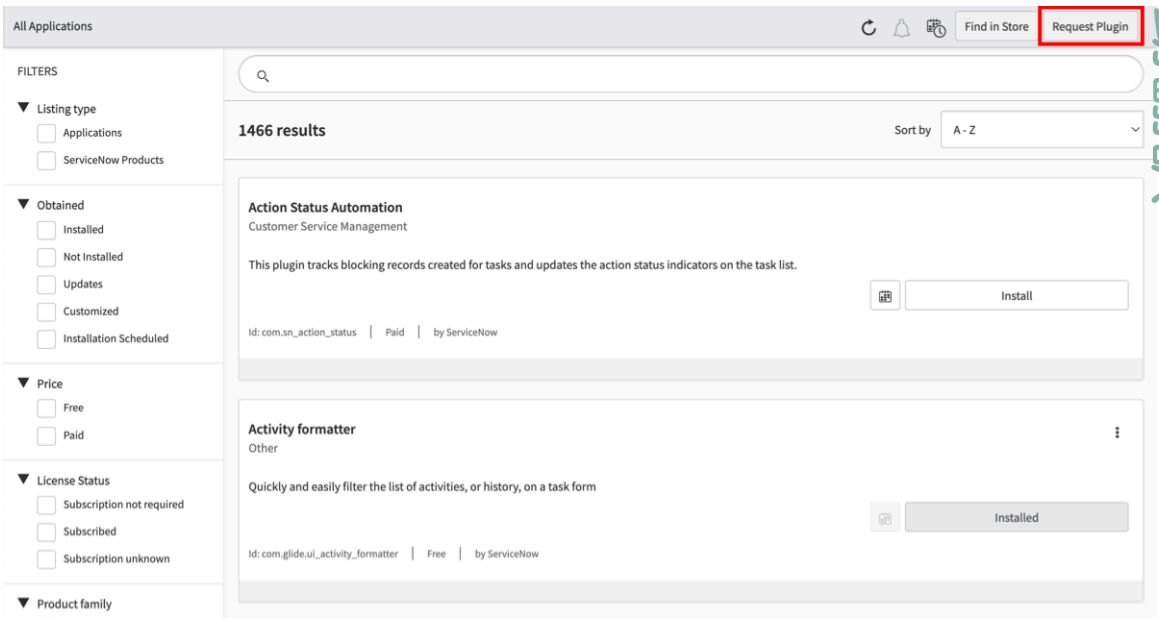
このタスクについて

プラグインを要求するには、次の 2 つの方法があります。

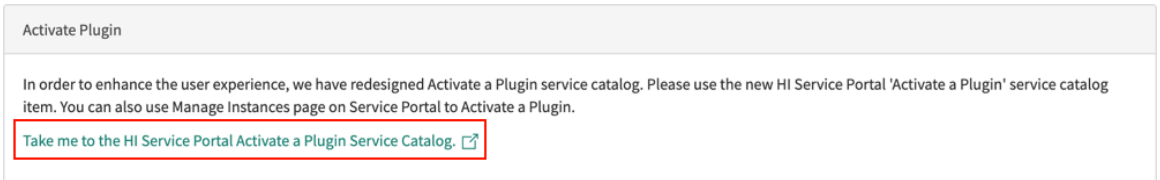
- Service Catalog Now Support に直接アクセスするには、次の項目を選択します。 すべて > サービスカタログ > プラグインをアクティブ化 オン Now Support。
- 次の手順に従い、インスタンスの [すべてのアプリケーション] ページから Now Support サービスカタログにアクセスします。

手順

1. 移動先 すべて > システムアプリケーション > 利用可能なすべてのアプリケーション > すべて。
2. [すべてのアプリケーション] ページで [プラグインの要求] をクリックして、Now Support で [プラグインをアクティブ化] フォームを開きます。



3. Now Support で、Now Support サービスポータル サービスカタログ にアクセスするリンクを選択します。



4. インスタンスを選択します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

5. [アクション] > [プラグインのアクティブ化] を選択します。
6. [プラグインのアクティブ化] フォームで、次の情報を入力します。

[プラグインのアクティブ化] フォーム

フィールド	説明
ターゲットインスタンスは何ですか	プラグインをアクティブ化するインスタンス。
どのプラグインをアクティブ化しますか	アクティブ化するプラグインの名前です。 **注:** 必要なプラグインが表示されない場合、または OEM またはオンプレミスのインスタンスでプラグインをアクティブ化している場合は、[探しているプラグインが表示されていません **(Plugin I'm looking for is not listed)]** チェックボックスをオンにして、プラグインの名前を入力します。
メンテナンスの日時を選択 (Select Maintenance Date and Time)	プラグインをアクティブ化する日時。 **注:** プラグインは、米国太平洋標準時で、毎営業日の朝と夕方の 2 回のバッチでアクティブ化されます。特定の時刻にプラグインをアクティブ化する必要がある場合は、[理由/コメント **(Reason/ Comments)]** フィールドに要求を入力します。

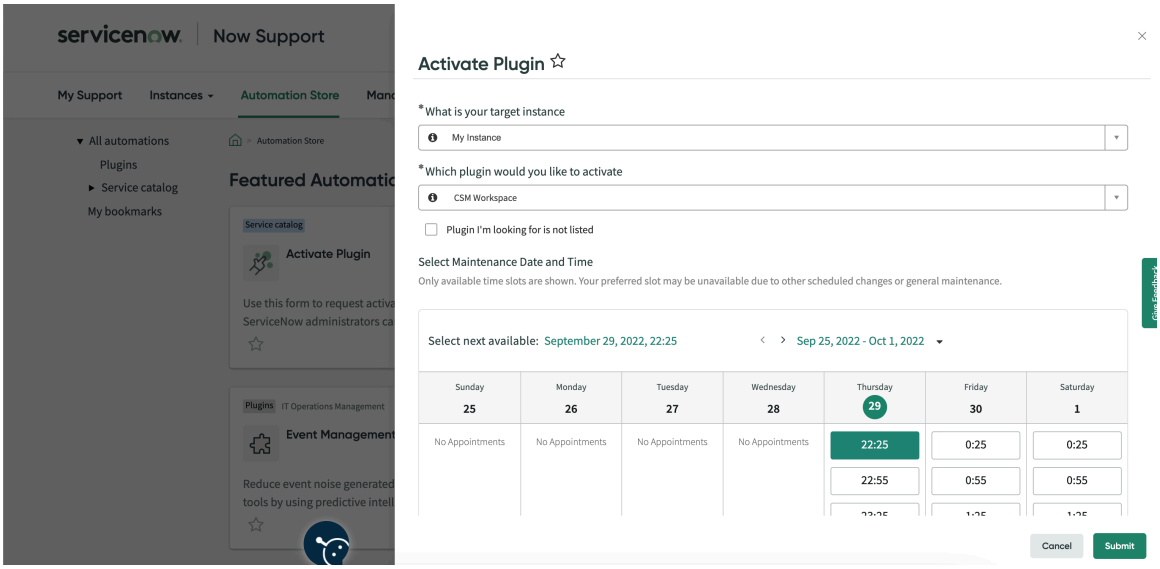
Example

たとえば、 [自分のインスタンス (My Instance)] という名前のインスタンスで CSM Workspace プラグインをアクティブ化するには、次のフォームを参照してください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

[プラグインのアクティブ化] フォーム



7. [送信] を選択します。
プラグインの要求の詳細については、次を参照してください。 の Service Catalog [KB0751715] 記事からのプラグインの要求 Now Support ナレッジベース。

外部認証情報ストレージの設定

リモート リポジトリーから認証情報を取得するようにインスタンスを設定します。

次の手順では、保護する認証情報で外部リポジトリーを設定していることを前提としています。ServiceNow インスタンスで設定されている認証情報識別子は、JAR ファイルを使用してリポジトリー内の実際の認証情報にマップする必要があります。

> **注:**
> ServiceNow では、一度に 2 つの外部ボールトがサポートされています。1 つはデフォルトの CyberArk 資格情報リゾルバー、もう 1 つはカスタム外部資格情報リゾルバーです。カスタム CyberArk 資格情報リゾルバーを作成すると、引き続き 2 つ目のカスタム外部ボールトが使用され、追加のカスタム外部ボールトを使用することはできません。

外部認証情報ストレージを設定するには、次のタスクを順に実行します。

資格情報を解決するための **JAR** ファイルの作成

MID Server から送信された資格情報の識別子をリポジトリーの実際の資格情報に解決するために、JAR ファイルを作成します。

始める前に

必要なロール：agent_admin または admin

インスタンスが予期するすべての資格情報要素 (秘密鍵など) を含めるようにしてください。

資格情報を解決するための JAR ファイルを作成するには、次の手順に従います。

手順

ServiceNow github で提供されているテンプレートまたはサンプル Java ファイルのいずれかを使用します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

⚠ 注意:
これらのサンプルはテンプレートとしてのみ使用してください。お使いの環境に合わせて変更しないまま本番環境でこのコードを使用しないでください。

a. ServiceNow github からの指示に従って、オープンソースの JAR ファイルをダウンロードします。

- HashiCorp 外部資格情報リゾルバー
- CyberArk 外部資格情報リゾルバー

b. 次のサンプル Java ファイルをテンプレートとして使用し、環境に合わせて変更します。

Example

```
package com.snc.discovery;

import java.util.*;
import java.io.*;

/**
 * Basic implementation of a CredentialResolver that uses a properties file.
 */

public class CredentialResolver {

 private static String ENV_VAR = "CREDENTIAL_RESOLVER_FILE";
 private static String DEFAULT_PROP_FILE_PATH = "C:\\dummycredentials.properties";

 // These are the permissible names of arguments passed INTO the resolve()
 // method.

 // the string identifier as configured on the ServiceNow instance...
 public static final String ARG_ID = "id";

 // a dotted-form string IPv4 address (like "10.22.231.12") of the target
 // system...
 public static final String ARG_IP = "ip";

 // the string type (ssh, snmp, etc.) of credential as configured on the
 // instance...
 public static final String ARG_TYPE = "type";

 // the string MID server making the request, as configured on the
 // instance...
 public static final String ARG_MID = "mid";

 // These are the permissible names of values returned FROM the resolve()
 // method.

 // the string user name for the credential, if needed...
 public static final String VAL_USER = "user";

 // the string password for the credential, if needed...
 public static final String VAL_PSWD = "pswd";
```

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

```
// the string pass phrase for the credential if needed:
public static final String VAL_PASSPHRASE = "passphrase";

// the string private key for the credential, if needed...
public static final String VAL_PKEY = "pkey";

// the string authentication protocol for the credential, if needed...
public static final String VAL_AUTHPROTO = "authprotocol";

// the string authentication key for the credential, if needed...
public static final String VAL_AUTHKEY = "authkey";

// the string privacy protocol for the credential, if needed...
public static final String VAL_PRIVPROTO = "privprotocol";

// the string privacy key for the credential, if needed...
public static final String VAL_PRIVKEY = "privkey";


private Properties fProps;

public CredentialResolver() {
}

private void loadProps() {
 if(fProps == null)
  fProps = new Properties();

 try {
  String propFilePath = System.getenv(ENV_VAR);
  if(propFilePath == null) {
   System.err.println("Environment var "+ENV_VAR+" not found. Using default file:
"+DEFAULT_PROP_FILE_PATH);
   propFilePath = DEFAULT_PROP_FILE_PATH;
  }

  File propFile = new File(propFilePath);
  if(!propFile.exists() || !propFile.canRead()) {
   System.err.println("Can't open "+propFile.getAbsolutePath());
  }
  else {
   InputStream propsIn = new FileInputStream(propFile);
   fProps.load(propsIn);
  }

 //fProps.load(CredentialResolver.class.getClassLoader().getResourceAsStream("dummycred
entials.properties"));
 } catch (IOException e) {
  System.err.println("Problem loading credentials file:");
  e.printStackTrace();
 }
}

/**
 * Resolve a credential.
 */
public Map resolve(Map args) {
```

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

```
 loadProps();
 String id = (String) args.get(ARG_ID);
 String type = (String) args.get(ARG_TYPE);
 String keyPrefix = id+"."+type+".";

 if(id.equalsIgnoreCase("misbehave"))
  throw new RuntimeException("I've been a baaaaaaaaad CredentialResolver!");

 // the resolved credential is returned in a HashMap...
 Map result = new HashMap();
 result.put(VAL_USER, fProps.get(keyPrefix + VAL_USER));
 result.put(VAL_PSWD, fProps.get(keyPrefix + VAL_PSWD));
 result.put(VAL_PKEY, fProps.get(keyPrefix + VAL_PKEY));
 result.put(VAL_PASSPHRASE, fProps.get(keyPrefix + VAL_PASSPHRASE));
 result.put(VAL_AUTHPROTO, fProps.get(keyPrefix + VAL_AUTHPROTO));
 result.put(VAL_AUTHKEY, fProps.get(keyPrefix + VAL_AUTHKEY));
 result.put(VAL_PRIVPROTO, fProps.get(keyPrefix + VAL_PRIVPROTO));
 result.put(VAL_PRIVKEY, fProps.get(keyPrefix + VAL_PRIVKEY));

 System.err.println("Error while resolving credential id/type["+id+"/"+type+"]");

 return result;
}


/**
 * Return the API version supported by this class.
 */
public String getVersion() {
 return "1.0";
}

public static void main(String[] args) {
 CredentialResolver obj = new CredentialResolver();
 obj.loadProps();

 System.err.println("I spy the following credentials: ");
 for(Object key: obj.fProps.keySet()) {
  System.err.println(key+": "+obj.fProps.get(key));
 }

}
}
```

自動翻訳

資格情報を解決するための **JAR** ファイルのインポート

MID Server から送信された資格情報識別子をリポジトリーの実際の資格情報に解決するために作成した JAR ファイルをインポートします。

始める前に
必要なロール：agent_admin または admin

JAR ファイルの作成後、そのファイルをインスタンスにインポートします。ここで、MID Server にアクセス可能になります。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. JAR ファイルとプロパティ ファイルの作成後、プロパティ ファイルを MID Server にコピーします。
2. 移動先 **MID** サーバー > **JAR** ファイル.
3. [新規] をクリックします。
4. 次のフィールドに入力します。

フィールド	説明
名前	インスタンス内のファイルを識別するためのわかりやすい一意の名前。
バージョン	ファイルのバージョン番号 (使用可能な場合)。
ソース	参照用の JAR ファイルの場所。ソース情報はシステムで使用されません。
説明	インスタンス内の JAR ファイルとその目的の簡単な説明。

5. バナーにあるクリップ アイコンをクリックして JAR ファイルをレコードに添付します。

Example

JAR ファイルの添付

6. [送信] をクリックします。
7. MID Server サービスを再起動します。
プラットフォームにより、インスタンスと通信するように設定された任意の MID Server で JAR ファイルが使用可能になります。

認証情報識別子の設定

インスタンスで認証情報識別子を設定します。

始める前に

必要なロール：管理者
次の項目を確認します。

- 外部認証情報ストレージ プラグインが有効になっていること。
- 外部認証情報ストレージ検出プロパティが有効になっていること。

手順

1. 移動先 すべて > ディスカバリー > 認証情報 または オーケストレーション > 認証情報.
2. [新規] をクリックします。
3. 認証情報タイプを選択します。
4. **[External credential store]** (外部の資格情報ストア) チェック ボックスをオンにします。
[ユーザー名] フィールドおよび [パスワード] フィールドは消去され、[資格情報 **ID]** フィールドおよび [資格情報ストレージ **Vault]** メニューが表示されます。
5. [資格情報ストレージ **Vault]** メニューから、[なし]、[CyberArk vault]、またはカスタム外部資格情報ストレージ vault のいずれかを選択します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

注:

[CyberArk vault] が選択されている場合は、[ルックアップキー] メニューに、[資格情報 ID]、[ルックアップキー]、[FQDN]、[上記のすべて] の 4 つのルックアップキーの選択肢が表示されます。[上記のすべて] を選択すると、 vault に複数回アクセスする必要があるため、パフォーマンスが低下する可能性があります。

a. カスタム外部資格情報ストレージ vault を使用するには、インスタンスの Vault 構成 [vault_configuration.list] に移動します。

b. カスタム資格情報リゾルバーのインポートされた JAR ファイルに関連付けられた名前を使用して、新しいレコードを作成します。

カスタム外部資格情報ストレージ vault の作成については、手順「資格情報を解決するための JAR ファイルの作成」および「資格情報を解決するための JAR ファイルのインポート」を参照してください。

6. 以下のテーブルのフィールドを使用して、資格情報フォームに入力します。

フィールド	説明
名前	この資格情報のわかりやすい一意の名前を入力します。
アクティブ	これらの資格情報の使用を有効または無効にします。
資格情報 ID	外部認証情報システム用に MID Server にアップロードされた JAR ファイルに外部認証情報用に設定された一意のキーを入力します。これは、パラメーター マップで Java クラスに渡される ID です。 `public static final String ARG_ID = "id";` MID Server は、この識別子を使用して、リポジトリー上の実際の認証情報を解決します。 **注:** このフィールドは、[外部の認証情報ストア] チェックボックスがオンになっている場合にのみ表示されます。
タグ	ワークフロー作成者は、個々の資格情報を Orchestration ワークフロー内の任意のアクティビティに割り当てたり、Orchestration ワークフロー内で同じアクティビティタイプが発生するたびに異なる資格情報を割り当てたりすることができます。
外部の資格情報ストア	外部認証情報ストレージシステムを使用するには、このチェックボックスをオンにします。このオプションを選択すると、[ユーザー名] フィールドと [パスワード] フィールドが [認証情報 **ID]** フィールドに置き換えられます。外部の認証情報ストレージは、 外部認証情報ストレージ プラグインをアクティブ化した場合にのみ使用できます。
資格情報ストレージ Vault	利用可能な Vault のリストから外部資格情報ストレージ Vault を選択します。メニューは、Vault 構成 [vault_configuration.list] のレコードで構成されています。新しいレコードを追加し、カスタム資格情報リゾルバー JAR ファイルに関連付けられた名前を使用できます。カスタム外部資格情報ストレージ vault の作成については、手順「資格情報を解決するための JAR ファイルの作成」および「資格情報を解決するための JAR ファイルのインポート」を参照してください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
適用先	これらの資格情報をネットワーク内の [すべての **MID Server]** または 1 つ以上の [特定の **MID Server]** に適用するかどうかを選択します。**[MID Server]** フィールドでこれらの資格情報を使用する MID Server を指定します。
MID Server を使用	使用可能な MID Server のリストから 1 つ以上の MID Server を選択します。このレコードで設定された認証情報は、このリストの MID Server で使用できます。このフィールドは、[適用先] フィールドで [特定の **MID Server]** を選択した場合のみ使用できます。
順番	プラットフォームがデバイスにログオンしようとするときに、この認証情報を試行する順序 (シーケンス) を入力します。番号が小さいほど、この資格情報がリストの上位に表示されます。多くの資格情報を使用する場合、またはログイン試行が 3 回失敗してセキュリティによってユーザーがロックアウトされた場合、資格情報の順序を確立します。すべての資格情報に同じ順序番号を設定した場合、または何も設定しない場合、Discovery または Orchestration では、資格情報をランダムな順序で試行します。

7. [送信] をクリックします。

AWS の認証情報識別子の設定

リモート リポジトリーから認証情報を取得するようにインスタンスを設定します。

始める前に

必要なロール：cloud_admin

次のプラグインがアクティブであり、MID Server がインストールされていることを確認します。

- Discovery [com.snc.discovery]
- Cloud Provisioning and Governance [com.snc.cloud.mgmt]
- 外部資格情報ストレージ [com.snc.discovery.external_credentials]

このタスクについて

次の手順では、保護する認証情報で外部リポジトリーを設定していることを前提としています。ServiceNow インスタンスで設定されている認証情報識別子は、JAR ファイルを使用してリポジトリー内の実際の認証情報にマップする必要があります。

手順

1. 移動先 すべて > ディスカバリー > 資格情報.

2. 外部資格情報ストレージプロバイダーがサポートする資格情報を選択します。

3. テーブル内のフィールドを使用して、フォームに入力します。

フィールド	説明
名前	この認証情報にわかりやすい一意の名前。たとえば、Amazon Web サービスです。
適用先	これらの資格情報を使用できる MID Server を選択します。選択肢は、[すべての **MID Server]** または [特定の **MID Server]** です。後者を選択すると、**[MID Servers]** フィールドが表示されます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

フィールド	説明
有効	認証情報を有効または無効にするためのチェック ボックス。
AWS アカウント	AWS 資格情報が外部ストレージプロバイダーにある場合は、AWS アカウント ID を入力します。
MID Server	これらの資格情報を使用できる MID Server を 1 つ以上選択します。
資格情報 ID	この資格情報が外部資格情報ストレージプロバイダーに保存される名前を入力します。
プライバシー資格情報 ID (Privacy Credential ID)	CyberArk の SNMPv3 プライバシーキーの名前を入力します。このフィールドは、[資格情報ストアタイプ] フィールドから [**CyberArk**] を選択した場合に、SNMPv3 に対してのみ表示されます。CyberArk のプライバシーキーを使用していない場合は、このフィールドを空白のままにします。
資格情報エイリアス	特定の動作を含むこの資格情報のエイリアスを選択します。詳細については、「Discovery の資格情報エイリアス」を参照してください。
外部の資格情報ストア	外部認証情報ストレージシステムを使用するには、このチェックボックスをオンにします。外部ストレージが有効になっている場合は、[資格情報 **ID**] フィールドが表示されます。このチェックボックスが表示されていない場合は、ヘッダーバーのメニューアイコンをクリックして、 ビュー > 外部ストレージ コンテキストメニューから。
資格情報ストアタイプ	CyberArk SNMPv3 プライバシーキーを使用している場合のみ、[**CyberArk**]を選択します。[プライバシー資格情報 **ID (Privacy Credential ID)**] フィールドが表示され、キーのエントリーが許可されます。

4. [送信] をクリックします。

CyberArk 認証情報ストレージの統合

MID サーバー と CyberArk ボールトの統合により、インスタンスに資格情報を保存せずに、ServiceNow オーケストレーション、ServiceNow ディスカバリー および ServiceNow サービスマッピング を実行することができます。

CyberArk の概要

CyberArk の Application Identity Management (AIM) 製品では、Privileged Account Security ソリューションを使用して、アプリケーション、スクリプト、または構成ファイルに組み込まれたアプリケーション パスワードを保存する必要性をなくします。さらに、この製品により、CyberArk ボールト内でこれらの非常に機密性の高いパスワードの保存、ログ記録、および管理を一元的に行うことができます。このアプローチにより、組織は定期的なパスワード交換の社内要件および規制要件を遵守し、オンプレミスかクラウドかに関係なく、あらゆる種類の特権 ID に関連付けられたアクティビティを監視することができます。

インスタンスは、各認証情報の一意の識別子、認証情報タイプ (SSH、SNMP、Windows など)、および任意の 資格情報親和性を保持します。MID サーバー は、インスタンスから認証情報識別子、認証情報タイプ、および IP アドレスを取得し、CyberArk ボールトを使用してこれらの要素を使用可能な認証情報に解決します。資格情報リゾルバーは、ホスト名「fqdn」を検索し、リバース DNS ルックアップを使用して「fqdn」を取得することもできます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

CyberArkこの統合には外部ServiceNow 認証情報ストレージプラグインが必要です。これは、 システム定義 > プラグイン.MID サーバー は、CyberArk AIM API/クライアントと同じマシンにインストールする必要があります。

CyberArkとともにインストールされる内容

- ビジネスルール：外部認証情報ストレージのビジネス ルールは、管理者が外部認証情報ストレージ プロパティを変更すると、次のタスクを実行します。
  - 認証情報レコードリストおよびフォームのビューを外部ストレージビューに変更します。このビューを使用すると、ユーザーはリスト内の [資格情報 ID] 列を確認できます。
  - MID サーバー に、資格情報の取得方法の変更に備えて、非外部資格情報キャッシュを更新するように指示します。
- システムプロパティ：外部認証情報ストレージの有効化と呼ばれるプロパティ [com.snc.use_external_credentials] は、外部認証情報ストレージプラグインがアクティブにされた後で、それを有効または無効にします。このホテルは、ディスカバリー定義 > プロパティそしてオーケストレーション > **MID** サーバープロパティプラグインを有効にすると有効になります。

> **注:**
> システム プロパティを使用して外部認証情報ストレージを無効にすると、すべての外部認証情報がインスタンス内で非アクティブに自動的に設定されます。このプロパティを使用して機能を再度有効にしても、外部認証情報レコードはアクティブにリセットされません。それぞれの認証情報レコードを手動で再アクティブ化する必要があります。

サポートされている資格情報タイプ

CyberArk の統合では、次の ServiceNow 認証情報タイプがサポートされています。

- GCP
- Azure
- CIM
- JMS
- SNMP フォーラム
- SNMPv3
- 基本認証
- SSH キーペア
- SSH 秘密鍵 (キー、パスフレーズ、およびパスワードを含む)
- VMware
- Windows
- 適用可能な資格情報

> **注:**
> CyberArk 統合を GCP 資格情報タイプと使用するには、外部資格情報ストレージ jar を変更する必要があります。詳細については、「CyberArk を使用した ServiceNow GCP 資格情報リゾルバー」を参照してください。

また、次のネットワークプロトコルを使用する Now Platform 機能では、CyberArk ボールトに保存された資格情報の使用がサポートされています。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ネットワークプロトコルでサポートされている資格情報

ネットワークプロトコル	ServiceNow フローデザイナー でのサポート	オーケストレーション でのサポート
SOAP	SOAP ステップ	基本認証を上書きして、SOAP Web サービスアクティビティを作成 します。
REST	REST ステップ	基本認証を上書きして、REST Web サービスアクティビティを作成 します。
JDBC	JDBC ステップ	JDBC アクティビティ
SSH	SSH ステップ	SSH アクティビティ
PowerShell	PowerShell ステップ	PowerShell アクティビティ
SFTP	SFTP ステップ	SFTP アクティビティ
JMS		JMS アクティビティ

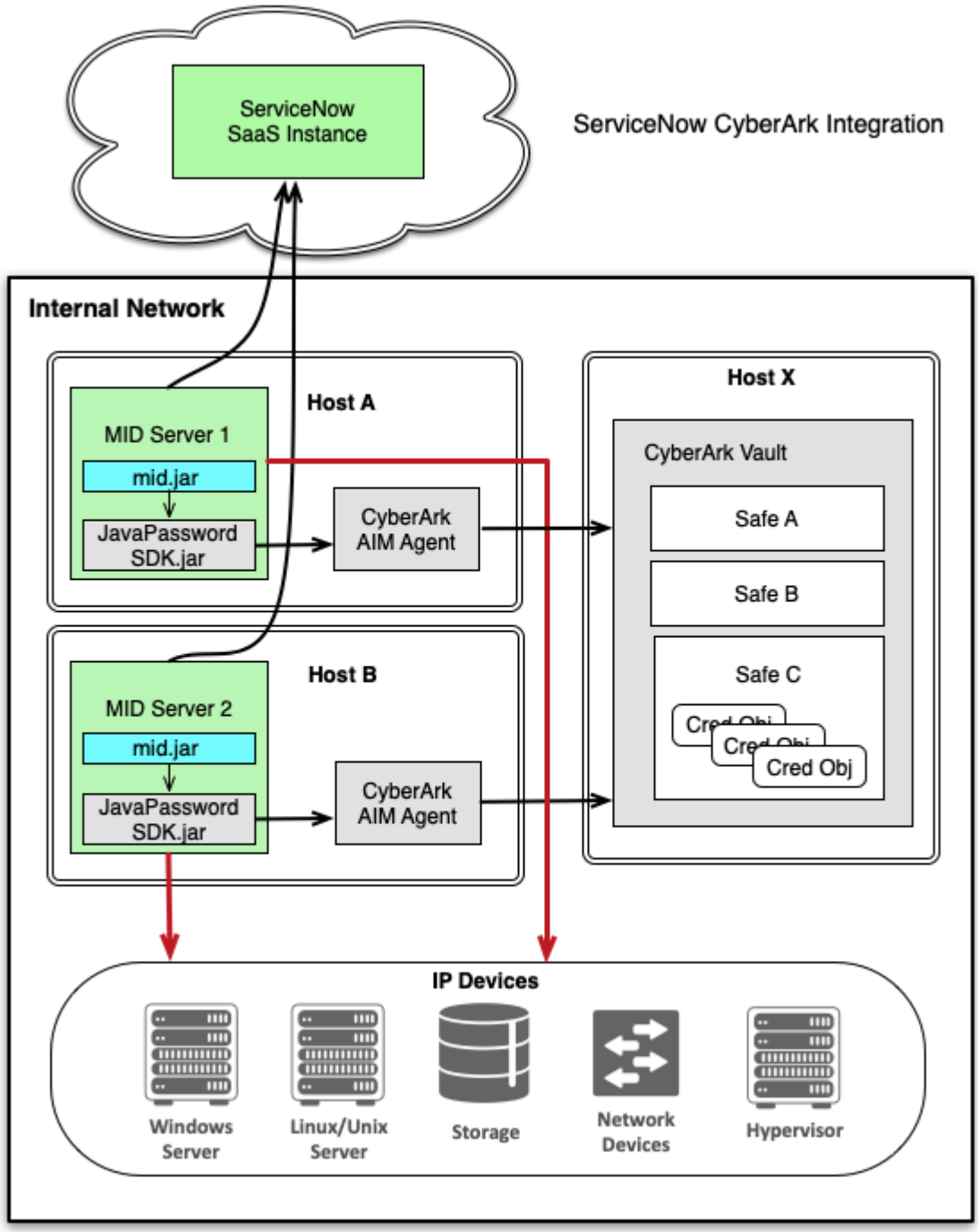
重要:
同じ MID サーバー を使用して、CyberArk ボールトに保存されている資格情報とカスタムの外部認証情報ストレージを管理することはできません。MID サーバー は、CyberArk AIM API/クライアントと同じマシンにインストールする必要があります。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

CyberArk アーキテクチャ

CyberArk のストレージアーキテクチャ



注:
CyberArk は、ベースシステムの `mid.jar` ファイルを使用して資格情報を解決します。

MID サーバー による Windows アカウントの処理方法

まず、認証情報ルックアップでは、指定した認証情報 ID と CyberArk ボールトの [名前] フィールドの照合を試行します。一致するものが見つかると、その認証情報が返されます。一致するもの

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

が見つからない場合は、認証情報ルックアップで IP アドレスを使用して一致の検索が試行されます。IP アドレス ルックアップが同じサーバー上の Windows や Tomcat など複数の認証情報と一致する場合、そのルックアップは失敗します。この問題を回避するには、MID サーバー の config.xml ファイルにある *ext.cred.type_specifier* パラメーターを **[true]** に設定し、CyberArk が資格情報タイプと IP アドレスの両方に一致する資格情報を返すようにします。たとえば、IP アドレスが Windows と Tomcat の両方で共有されている場合、Windows の認証情報タイプにより、Windows 認証情報のみが返されます。

CyberArk の統合設定

次の手順には、適切な CyberArk ドキュメントへの参照など、CyberArk と ServiceNow の両方の設定タスクが含まれています。

ServiceNow インスタンスで設定されている認証情報識別子は、CyberArk ボールト内の認証情報名にマップする必要があります。資格情報を参照するときに、MID Server は資格情報識別子をボールト内の名前と照合して、資格情報を検索します。名前は一意でなければなりません。資格情報識別子が空の場合、MID Server は IP アドレスで資格情報を検索します。IP アドレスで認証情報を特定するために、認証情報タイプが調べられ、そのアドレスでそのタイプの認証情報が 1 つだけ存在することが確認されます。たとえば、Windows サーバーと vCenter が両方とも同じ IP アドレスで実行されている場合です。このような厳密な認証情報要件を SSH 環境でサポートするために、MID Server の設定パラメーターを使用すると、要求された認証情報タイプが CyberArk から返されるタイプと一致することを要求できます。

> **注:**
> [資格情報 **ID]** フィールドは、SNMPv3 を除くすべてのケースで資格情報を CyberArk にマッピングするために必要な唯一のフィールドです。[プライバシー資格情報 **ID]** フィールドはオプションであり、SNMPv3 資格情報を使用しており、資格情報にプライバシープロトコルを使用している場合にのみ必要です。詳細は、CyberArk 認証情報識別子の設定を参照してください。

CyberArk ボールトから認証情報を取得するようにインスタンスを設定するには、下記に示す順序で次のタスクを実行します。

CyberArk ボールトの設定と AIM API のインストール

MID Server にアクセスできるように CyberArk ボールトを設定し、MID Server マシンに CyberArk AIM API をインストールします。

始める前に

必要なロール：管理者
この手順を開始する前に、外部認証情報ストレージ プラグインがアクティブ化されていることを確認してください。

手順

1. 認証情報を要求するすべての MID Server で使用されるアプリケーション ID および認証詳細を使用して、CyberArk ボールトを設定します。
   詳細については、『CyberArk Credential Provider and ASCP Implementation Guide (CyberArk Credential Provider および ASCP 実装ガイド)』を参照してください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

a. CyberArk で *ServiceNow_MID_Server* と呼ばれるアプリ ID を作成して、MID Server がボールトにアクセスできるように CyberArk が設定されていることを確認します。

b. *ServiceNow_MID_Server* アプリ ID へのアクセスに MID Server に必要なすべての資格情報が与えられることを確認します。

> **注:**
> ext.cred.app_id パラメーターを使用して、MID Server の config.xml ファイルにあるデフォルトの **ServiceNow_MID_Server** アプリ ID を上書きすることができます。このパラメーターの値を変更する場合は、ボールトで一致する値を設定してください。

2. 認証情報ストアへのアクセスに使用使用する MID Server サービスをホストする各マシンに、CyberArk Credential Provider (AIM API を含む) をインストールします。
3. CyberArk アカウントをプロビジョニングし、アプリケーション アクセスの権限を設定します。詳細については、『CyberArk Privileged Account Security Implementation Guide (CyberArk Privileged Account Security 実装ガイド)』を参照してください。
   a. CyberArk Password Safe で、さまざまなデバイスにアクセスするためにディスカバリー、オーケストレーション、またはサービス マッピングで必要な特権アカウントを作成し、これらのアカウントが、必要な認証情報が保存されているセーフのメンバーであることを確認します。
   b. Credential Provider およびアプリケーションのユーザーを、アプリケーションのパスワードが保存されている Password Safe のメンバーとして追加します。

CyberArk JAR ファイルのインポート

CyberArk JavaPasswordSDK.jar ファイルをインスタンスにインポートして、MID Server にアクセスできるようにします。

始める前に

必要なロール：agent_admin または admin
この手順を開始する前に、MID Server が認証情報にアクセスできるように CyberArk が設定されていることを確認してください。ボールトへのアクセスに使用する MID Server をホストする各サーバーに CyberArk AIM API がインストールされていることを確認してください。

このタスクについて

JavaPasswordSDK.jar ファイルがすでに MID Server に存在する場合でも、このプロセスを使用します。

手順

1. 移動先 すべて > **MID** サーバー > **JAR** ファイル.
2. [新規] をクリックします。
3. テーブル内のフィールド使用して、フォームに値を入力します。

JAR ファイル フォームのフィールド

フィールド	説明
名前	インスタンス内のファイルを識別するためのわかりやすい一意の名前。
バージョン	ファイルのオプション バージョン番号 (使用可能な場合)。
ソース	JAR ファイルのプロバイダー。ソース情報はシステムで使用されません。
説明	インスタンス内の JAR ファイルとその目的の簡単な説明。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

4. このレコードに JAR ファイルを添付します。
   AIM JavaPasswordSDK.jarファイルは、AIM SDK インストール ファイルに付属しており、通常、MID Server の AIM インストールディレクトリー <install_dir>/CyberArk/ApplicationPasswordSdk にあります。
5. [送信] をクリックします。
6. MID Server サービスを再起動します。
   プラットフォームにより、インスタンスと通信するように設定された任意の MID Server で JAR ファイルが使用可能になります。

CyberArk 用の MID Server の設定

MID Server に CyberArk ボールトへのアクセスを付与するように config.xml を設定します。

始める前に
必要なロール：管理者
この手順を開始する前に、JavaPasswordSDK.jar ファイルをインスタンスにインポートします。

手順

次のパラメーターを使用して MID Server の MID Server のパラメーターを追加 ファイルを手動で設定します。

この設定は、インスタンスから実行することはできません。

必要な設定パラメーター

パラメーター	値	説明
ext.cred.safe_folder	NameOfFolder	すべての認証情報ルックアップに使用するフォルダー。たとえば、ルートです。
ext.cred.use_cyberark	true	この MID Server が CyberArk と統合されることを示すブーリアン パラメーター。

オプションの設定パラメーター

パラメーター	値	説明
ext.cred.safe_timeout	5 (秒)	ボールト内の各認証情報ルックアップのタイムアウト (秒単位)。
ext.cred.safe_name	NameOfSafe	すべての認証情報ルックアップに使用されるデフォルトの安全な名前。パラメーターが複数のセーフにある場合、資格情報 ID は *<safeName>:<CredentialID>* の形式で指定することができます。このように設定した場合、**[NameOfSafe]** フィールドは無視されます。すべての外部認証情報にこの形式で指定された認証情報 ID がある場合は、**[NameOfSafe]** フィールドをスキップします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

パラメーター	値	説明
		注: デフォルトでは、この形式の区切り文字はコロンです。区切り文字として任意の文字を割り当てるには、safe.cred.split.string=<string> の行を CredMap.properties ファイルに追加します。
ext.cred.app_id	ServiceNow_MID_Server	CyberArk ボールトにアクセスするために MID Server に許可を与えるために使用されるアプリ ID を指定します。CyberArk ボールトでデフォルト値 **ServiceNow_MID_Server** を定義する必要があります。このパラメーターを使用して、デフォルトを上書きして独自のアプリ ID を指定することができます。このパラメーターでアプリ ID を編集する場合は、CyberArk が一致するようにこれを設定してください。
ext.cred.type_specific	true	CyberArk プラットフォーム ID と IP アドレスの両方に一致する資格情報を返すよう IP アドレスルックアップに強制します。たとえば、IP アドレスが Windows と Tomcat の両方で共有されている場合、**Win** で始まるプラットフォーム ID を含む認証情報により、Windows 認証情報のみが返されます。このパラメーターを true に設定すると、CyberArk では、次で始まるプラットフォーム ID が検索されます。 • Win：Windows • Unix：SSH • VMWare：VMware
ext.cred.check_ssh_type	false	true に設定した場合、CyberArk から返される SSH 認証情報のタイプが、要求された認証情報のタイプと一致する必要があります。たとえば、通常の SSH ユーザー名/パスワード認証情報が要求され、SSH キーのみが使用可能な場合、認証情報ルックアップは失敗します。

SNMPv2 認証情報用の CyberArk の設定

システムで SNMPv2 が使用される場合は、認証情報の属性をコミュニティ文字列にマップする特別なファイルを作成することができます。

始める前に
必要なロール：管理者
この手順を開始する前に、CyberArk ボールトにアクセスできるように MID Server を設定してください。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

このタスクについて

注:
コミュニティ文字列が CyberArk 認証情報のパスワード フィールドに表示される場合は、この手順を実行する必要はありません。

SNMPv2 は、CyberArk ではネイティブにサポートされていません。組織が、コミュニティ文字列が認証情報のパスワード フィールドに表示されないカスタムの SNMPv2 認証情報を作成した場合は、この手順を使用して、認証情報の属性をコミュニティ文字列にマップします。

手順

1. テキスト エディターで、次のコードを含む、CredMap.properties と呼ばれるファイルを作成します。
   SNMPv2.Community=attribute_name
2. このファイルを MID Server インストールの /agent ディレクトリーに保存します。
   認証情報ルックアップで、MID Server は認証情報のこの属性の検索を試行します。属性が見つからない場合、MID Server はパスワード フィールドを確認します。パスワード フィールドが空の場合、認証情報ルックアップは失敗します。

CyberArk 認証情報識別子の設定

外部リポジトリー内の特定の認証情報を識別するために CyberArk で使用できる一意のキーを作成します。

始める前に
必要なロール：管理者
この手順を開始する前に、外部認証情報ストレージ プラグインが有効化され、com.snc.use_external_credentials システム プロパティが true に設定されていることを確認してください。

手順

1. 移動先 すべて > ディスカバリー > 認証情報 または オーケストレーション > 認証情報.
2. [新規] をクリックします。
3. 認証情報タイプのリストから、 CyberArk の外部ストレージをサポートするタイプを選択します。
4. 認証情報タイプのフィールドを使用してフォームに入力します。
5. **[External credential store]** (外部の資格情報ストア) チェック ボックスをオンにします。
   [ユーザー名] フィールドと [パスワード] フィールドが [認証情報 **ID]** フィールドに置き換えられます。

   注:
   チェックボックスが表示されていない場合は、ヘッダーバーのメニューアイコンをクリックし、 ビュー > 外部ストレージ.

6. 次のいずれかの形式を使用して、[認証情報 **ID]** フィールドに式を入力します。
   - すべての認証情報が同じセーフにある場合は、ext.cred.safe_name パラメーターを使用して MID Server の config.xml ファイルにこの安全な名前を設定してから、認証情報 ID を **<credential ID>** として名前のみで指定します。
   - 特定のセーフにある指定したプラットフォームの認証情報に名前を付けるには、認証情報 ID を **<safe>:<credential ID>:<platform ID>** として定義します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

- 認証情報が複数のセーフにある場合は、認証情報 ID を **<safe>:<credential ID>** の形式で指定します。
- CyberArk が別のセーフを使用して IP アドレスで認証情報を検索できるようにする場合は、認証情報 ID を **<safe>:** の形式で指定します。
- CyberArk が同じセーフで別のプラットフォーム ID の認証情報を検索できるようにする場合は、**::<platform ID>** の形式を使用します。
- CyberArk が、設定されたセーフで認証情報を認証情報 ID ではなく IP アドレスで検索できるようにする場合は、このフィールドを空白のままにします。これは、各サーバーに一意の資格情報があるインストールを処理するためのベスト プラクティスです。このタイプのルックアップがない場合は、環境内のすべてのサーバーのインスタンスで認証情報 ID レコードを作成する必要があります。

注:
資格情報 ID は、CyberArk アカウントの [名前] フィールドの値と一致する必要があります。[資格情報 **ID]** フィールドには 180 文字の制限があります。

7. SNMPv3 資格情報を CyberArk に保存していて、プライバシープロトコルおよびプライバシーキーを使用している場合は、次のように ID を設定します。

   a. [資格情報ストアタイプ] フィールドで **[CyberArk]** を選択します。
   [プライバシー資格情報 **ID]** フィールドが表示されます。

   b. [プライバシー資格情報 **ID]** フィールドに CyberArk SNMPv3 プライバシーアカウントの [名前] を入力します。

8. [送信] をクリックします。

CyberArk ボールトでの AWS 資格情報の設定

インスタンスで使用するために取得する AWS 資格情報を使用して CyberArk ボールトを設定します。

始める前に
必要なロール：管理者

このタスクについて
資格情報を SSH キーとして CyberArk ボールトに保存します。インスタンスでボールトへのアクセスを設定する場合は、SSH キーに付けた名前も資格情報 ID として使用される必要があります。

手順

1. CyberArk で、次の場所に移動します。 アカウント > **SSH** キーを追加.
2. 以下の情報を入力します。

CyberArk 資格情報

フィールド	値
デバイス タイプ	[クラウド サービス] を選択します。
Platform Name (プラットフォーム名)	**[Amazon Web** サービス] **- [AWS] -** [アクセスキー] を選択します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	値
AWS Access Key ID (AWS アクセス キー ID)	AWS から提供された AWS アクセス キーを入力します。
AWS IAM ユーザー名	CyberArk で設定した AWS IAM ユーザー名を入力します。
パスワード	AWS から提供された AWS 秘密アクセス キーを入力します。
名前	このキーの名前を入力します。

3. [保存] を選択します。

次のタスク
まだ作成していない場合は、インスタンスで資格情報識別子を作成して CyberArk ボールトへのアクセスを設定します。詳細については、「AWS の外部資格情報ストレージへのアクセスの設定」を参照してください。

CyberArk ボールトでの Azure 資格情報の設定

インスタンスで使用するために取得する Azure 資格情報を使用して CyberArk ボールトを設定します。

始める前に
必要なロール：admin

このタスクについて
Azure 資格情報を保存するには、最初に CyberArk ボールトに Azure 資格情報テンプレートを作成します。このプロセスは、ボールトに対して 1 回だけ完了する必要があります。

手順

1. 管理モードで CyberArk にログインします。
2. [管理] タブに移動します。
3. [システム構成] で **[Platform Management]** を編集します。
4. [クラウドプロバイダーテンプレート **(Cloud Provider Template)]** に移動して複製します。
5. Azure 資格情報のテンプレートを編集します。
6. 次の 2 つのプロパティを追加します。
   - *`Username`* として *`Name`*、および *`Client ID`* として *`Display Name`*
   - *`Address`* として *`Name`*、および *`Tenant ID`* として *`DisplayName`*
7. 変更を適用します。
8. [アカウント] セクションに移動し、[アカウントの追加] を選択します。
9. [安全] を選択します。
10. [デバイスタイプ] を [クラウドサービス] に設定します。
11. 以前に編集した Azure テンプレートを選択します。
12. [クライアント **ID]**、[テナント **ID]**、および [パスワード] フィールドの情報を入力します。
13. [保存] を選択します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

認証アルゴリズム

認証アルゴリズムを使用して送信者の本人確認を行う

統合ステップで、複雑な、または非標準の接続メカニズムや資格情報メカニズムを必要とする Web サービスを使用した認証が可能になります。認証アルゴリズムを資格情報エイリアスや接続エイリアスに関連付けることで、統合ステップを手動で設定する必要がなくなります。

認証アルゴリズムを使用して、統合ステップで使用するカスタム認証データを生成できます。統合ステップでは、この動的データを使用して、ターゲット Web サービスを使用した認証に必要なカスタムアーティファクトを作成できます。たとえば、REST ステップでは、認証ヘッダーやクエリーパラメーター、トークンを作成できます。

認証アルゴリズムは、次のステップをサポートしています。

- 接続情報の取得ステップ
- REST ステップ
- SOAP ステップ

詳細については、「統合ステップ」を参照してください。

認証アルゴリズムのタイプ

- **Amazon** 署名バージョン **4**：これは、Amazon Web Services に接続するための構築済み認証アルゴリズムです。
- カスタム認証：これは、開発者が独自の認証アルゴリズムを作成するために使用できるテンプレートです。

認証アルゴリズムの設定方法の詳細については、「認証アルゴリズムの構成」を参照してください。

スクリプト

インスタンス認証スクリプトは、*sys_script_include* テーブルのインスタンススクリプト部分にあります。

インスタンスでの認証スクリプト

RequestAuthInternal	送信要求と一緒に送信される AWS V4 署名またはカスタム認証の生成をサポートする、インスタンスの読み取り専用スクリプト。
RequestAuthAWSV4Signer	AWS V4 署名を生成する署名者を実装するための RequestAuthInternal を拡張するスクリプト。
RequestAuthTwitterSigner	OAuth 1.0a を使用して Twitter の署名を生成する署名者を実装するための RequestAuthInternal を拡張するスクリプト。
RequestAuthSampleCustomSigner	インスタンスでカスタム署名者を記述する方法を理解するための RequestAuthInternal を拡張するサンプルスクリプト。

MID 認証スクリプトは、*ecc_agent_script_include* テーブルの MID スクリプト部分にあります。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

MID での認証スクリプト

RequestAuthInternal	送信要求と一緒に送信される AWS V4 署名またはカスタム認証の生成をサポートする、MID の読み取り専用スクリプト。
RequestAuthAWSV4MIDSigner	AWS V4 署名を生成する署名者を実装するための RequestAuthInternal を拡張するスクリプト。
RequestAuthTwitterSigner	OAuth 1.0a を使用して Twitter の署名を生成する署名者を実装するための RequestAuthInternal を拡張するスクリプト。
RequestAuthSampleMidCustomSigner	MID でカスタム署名者を記述する方法を理解するための RequestAuthInternal を拡張するサンプルスクリプト。

JavaScript API

認証アルゴリズム用の JavaScript API は次のとおりです。

- AuthCredential
- HttpRequestAuthedData
- HttpRequestData
- RequestAuthAPI

認証アルゴリズムの構成

送信 HTTP 要求に署名できるように、認証アルゴリズムを構成します。

始める前に

認証アルゴリズムを構成する前に、スクリプトインクルードを構成しておく必要があります。
必要なロール：管理者

手順

1. 移動先 すべて > 認証情報 **&** 接続 > 認証アルゴリズムをクリックし、[新規] をクリックします。
2. フォームのフィールドに入力します。
   [フォーマット] フィールドのデータベース選択により、利用可能なフィールドが決定されます。

認証フォーム

フィールド	説明
名前	このアルゴリズムの一意の名前
アルゴリズム	発信リクエストタイプ
説明	アルゴリズムの実行内容の説明
アプリケーション	アプリケーションが実行されるスコープ
インスタンスでの認証スクリプト	スクリプトインクルードテーブルから選択したスクリプト

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
MID での認証スクリプト	MID Server スクリプトインクルード [Discovery view] テーブルから選択したスクリプト

3. [送信] をクリックします。

Amazon 署名ベースのカスタムアルゴリズムの設定

スクリプトを実行して、Web サービスへの認証に必要な Amazon 署名ベースのデータを生成します。

始める前に

- JavaScript に関する知識
- REST に関する知識
- ターゲットの Web サービス API に関する知識
- 接続、資格情報、およびエイリアスに関する知識
- 必要なロール：開発者

このタスクについて

認証には接続エイリアスおよび資格情報エイリアスと Amazon 署名バージョン 4 ベースのアルゴリズムを使用します。

手順

1. 移動先 すべて > 認証情報 **&** 接続 > 認証アルゴリズムをクリックし、[新規] をクリックします。
2. フォームのフィールドに入力します。
   [フォーマット] フィールドのデータベース選択により、利用可能なフィールドが決定されます。

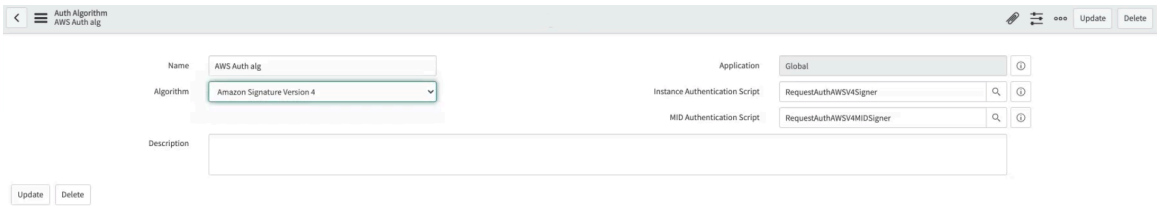
   認証フォーム

フィールド	説明
名前	このアルゴリズムの一意の名前
アルゴリズム	発信リクエストタイプ**[Amazon** 署名バージョン **4]** を選択します。
説明	アルゴリズムの実行内容の説明
アプリケーション	アプリケーションが実行されるスコープ
インスタンスでの認証スクリプト	スクリプトインクルードテーブルから選択したスクリプト**[Amazon** 署名バージョン **4]** アルゴリズムの場合は、**[RequestAuthAWSV4Signer]**を選択します。使用可能なスクリプトは次のとおりです。 ○ RequestAuthAWSV4Signer ○ RequestAuthInternal ○ RequestAuthSampleCustomSigner ○ RequestAuthTwitterSigner

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

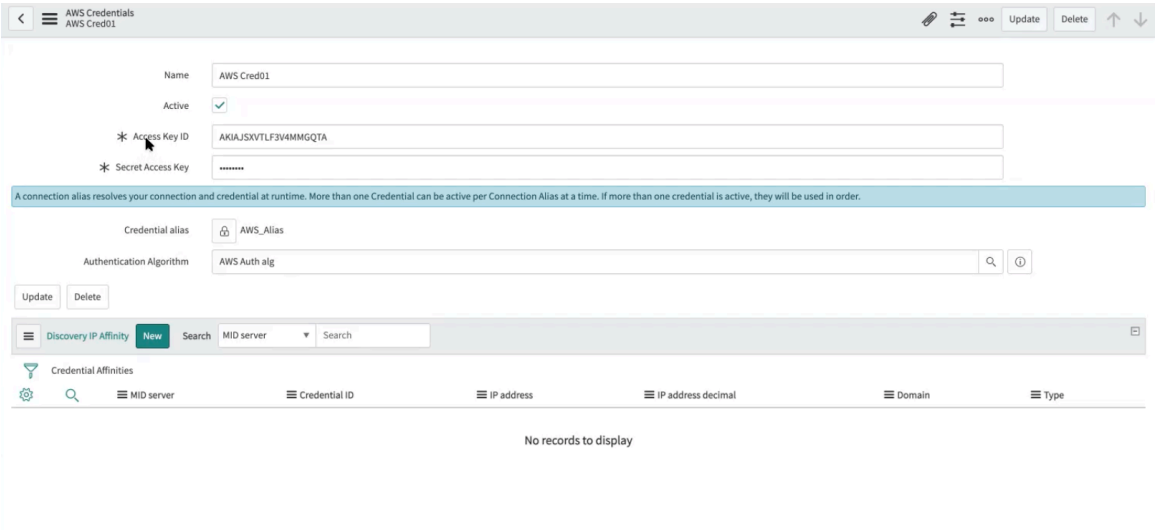
フィールド	説明
	注: スクリプトの詳細を確認するには、フィールドの横にある情報アイコンをクリックします。[名前]、[API 名]、[アプリケーション]、[アクセス可能]、[スクリプト] などのスクリプトの詳細が表示されます。
MID での認証スクリプト	MID Server スクリプトインクルード [Discovery view] テーブルから選択したスクリプト使用可能なスクリプトは次のとおりです。 ○ RequestAuthAWSV4Signer ○ RequestAuthInternal ○ RequestAuthSampleCustomSigner ○ RequestAuthTwitterSigner



3. [更新] をクリックします。
4. 移動先 すべて > 接続 **&** 認証情報 > 資格情報.
5. [新規] をクリックします。
6. 認証アルゴリズムを使用して AWS 資格情報を作成します。
   この場合は **AWS Auth alg** です。
7. 以下の項目を指定します。
   - 名前
   - 有効
   - アクセスキー ID
   - 秘密アクセスキー
   - 資格情報エイリアス
   - 認証アルゴリズム

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



8. [更新] をクリックします。

タスクの結果
選択したスクリプトと認証アルゴリズムに基づいて、設定された資格情報 (アクセスキー ID と秘密アクセスキー) またはユーザーの資格情報 (アクセスキー **ID**、秘密アクセスキー、およびセッショントークン) によって、プロバイダー (この場合AWS) からServiceNow送信要求として送信される V4 署名が生成されます。Amazon

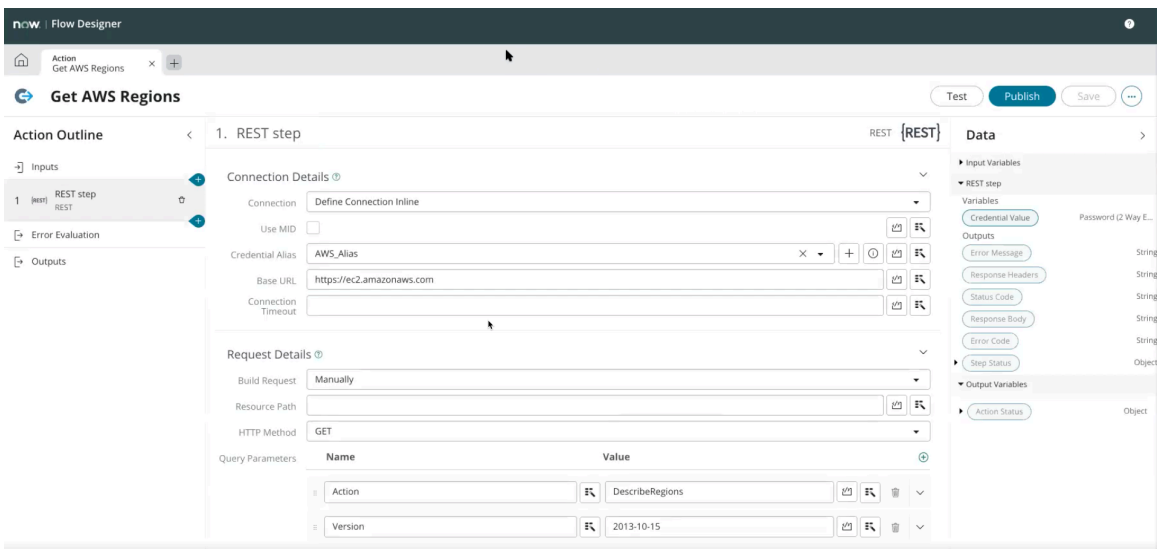
Example: AWS での REST ステップ

> **注:**
> Amazon V4 署名ベースの認証は、スクリプトのバックグラウンドからも使用できます。

アクション：AWS リージョンを取得する

AWS での REST ステップを次のように入力します。

- 資格情報エイリアス：AWS 用に作成されたエイリアス。
- ベース **URL**：AWS からのベース URL の詳細。
- **HTTPS** メソッド：この場合は GET メソッドです。
- クエリーパラメーター：アクション。値は **DescribeRegions**。



© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

アクションをテストできます。テストすると関連するリージョンが表示されます。応答の本文は次のとおりです。

Amazon V4 は、認証メカニズムをサポートするアルゴリズムの標準セットで定義されています。このアルゴリズムを使用すると、REST ステップを使用して認証 (HTTP 要求) の認証ヘッダーとして署名が追加されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

カスタムの認証アルゴリズムの構成

スクリプトを実行して、Web サービスへの認証に必要なカスタムのデータを生成します。

始める前に

- JavaScript に関する知識
- REST に関する知識
- ターゲットの Web サービス API に関する知識
- 接続、資格情報、およびエイリアスに関する知識
- 必要なロール：開発者

このタスクについて

認証には接続エイリアスおよび資格情報エイリアスと、カスタム認証ベースのアルゴリズムを使用します。

手順

1. 移動先 すべて > 認証情報 **&** 接続 > 認証アルゴリズムをクリックし、[新規] をクリックします。
2. フォームのフィールドに入力します。
   [フォーマット] フィールドのデータベース選択により、利用可能なフィールドが決定されます。

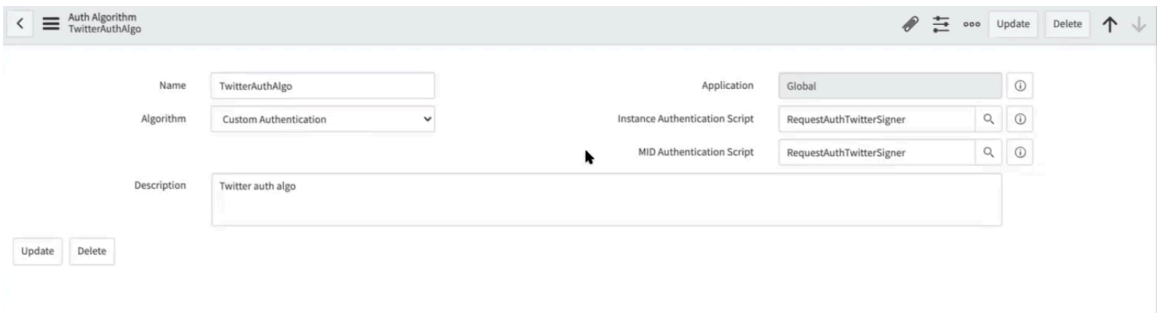
認証フォーム

フィールド	説明
名前	このアルゴリズムの一意の名前
アルゴリズム	発信リクエストタイプ[カスタム認証] を選択します。
説明	アルゴリズムの実行内容の説明
アプリケーション	アプリケーションが実行されるスコープ
インスタンスでの認証スクリプト	スクリプトインクルードテーブルから選択したスクリプト使用可能なスクリプトは次のとおりです。 ○ RequestAuthAWSV4Signer ○ RequestAuthInternal ○ RequestAuthSampleCustomSigner ○ RequestAuthTwitterSigner **注:** ○ スクリプトの詳細を確認するには、フィールドの横にある情報アイコンをクリックします。[名前]、[API 名]、[アプリケーション]、[アクセス可能]、[スクリプト] などのスクリプトの詳細が表示されます。 ○ Twitter でのカスタム認証の場合は、**RequestAuthTwitterSigner**を選択できます。この方法では OAuth 1.0a の認証方法を使用するためです。その際、認証ヘッダーで渡す署名の作成に使用できる **API** キーとシークレット、アクセストークンとシークレットなどの情報が必要です。詳細については、「Twitter での認証(Authentication in Twitter)」を参照してください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
MID での認証スクリプト	MID Server スクリプトインクルード [Discovery view] テーブルから選択したスクリプト使用可能なスクリプトは次のとおりです。 ○ RequestAuthAWSV4Signer ○ RequestAuthInternal ○ RequestAuthSampleCustomSigner ○ RequestAuthTwitterSigner

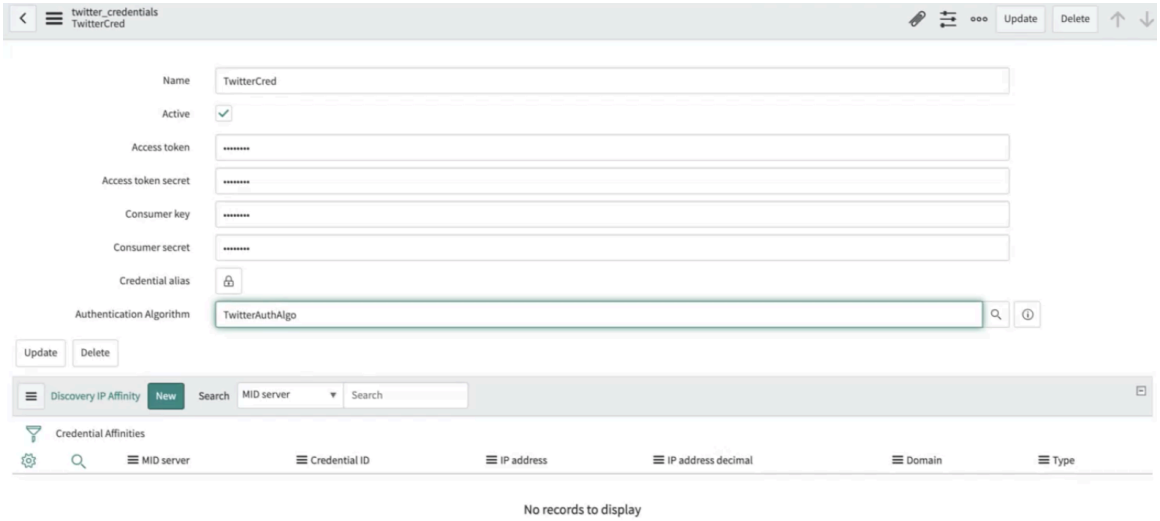


選択したスクリプトと認証アルゴリズムに基づき、設定された資格情報が送信要求として ServiceNow からプロバイダーに送信されます。

3. [更新] をクリックします。
4. 移動先 すべて > 接続 **&** 認証情報 > 資格情報.
5. [新規] をクリックします。
6. 認証アルゴリズムを使用して Twitter 資格情報を作成します。
   この場合は **TwitterAuthAlgo** です。
7. 以下のフィールドを指定します。
   - 名前
   - 有効
   - アクセストークン
   - アクセストークンシークレット
   - コンシューマーキー
   - コンシューマーシークレット
   - 資格情報エイリアス
   - 認証アルゴリズム

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



8. [更新] をクリックします。

Example: Twitter での REST ステップ

Twitter の場合は、次のスポークまたは資格情報が利用可能であることを確認する必要があります。

- アクセストークン
- アクセストークンシークレット
- コンシューマーキー
- コンシューマーシークレット
- 認証アルゴリズム

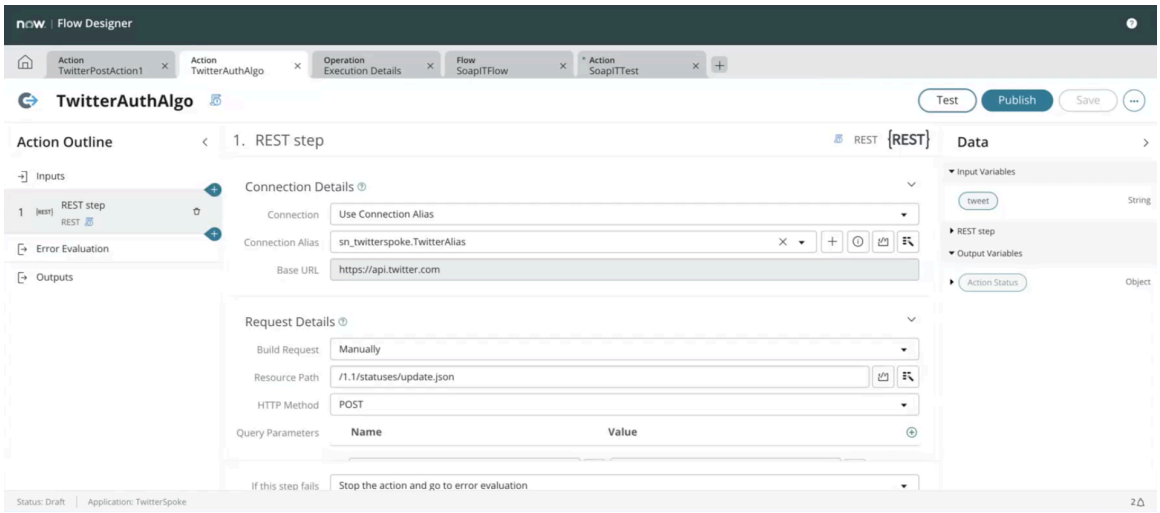
アクション：TwitterAuthAlgo

Twitter で REST ステップを次のように入力します。

- 資格情報エイリアス：Twitter 用に作成されたエイリアス。
- ベース **URL**：Twitter からのベース URL の詳細。
- **HTTPS** メソッド：この場合は POST メソッドです。ツイートを投稿します。
- クエリーパラメーター：[アクション] が **tweet**。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。



アクションをテストできます。ツイートが Twitter ページに投稿されます。

Discovery と Orchestration における IP サービスの親和性の確認

IP サービステーブルで、プロトコルに関連付けられている IP アドレスのリストを確認できます。

始める前に

必要なロール：管理者

このタスクについて

IP サービステーブルは、ポートをプロトコルにマッピングします。HTTP の場合はポート 80、SSH の場合はポート 22、SNMP の場合はポート 161 など、一般的に使用されるポートとプロトコルの組み合わせに対して、デフォルトでいくつかのマッピングが提供されています。*`glide.discovery.ip_service_affinity`* と呼ばれるシステムプロパティにより、検出された IP アドレスの最後のポートを ディスカバリー で記憶できます。デフォルトでは、このプロパティは **false** に設定されています。

> **重要:**
> 組織でカスタムポートを使用しない限り、IP サービスを変更しないでください。

手順

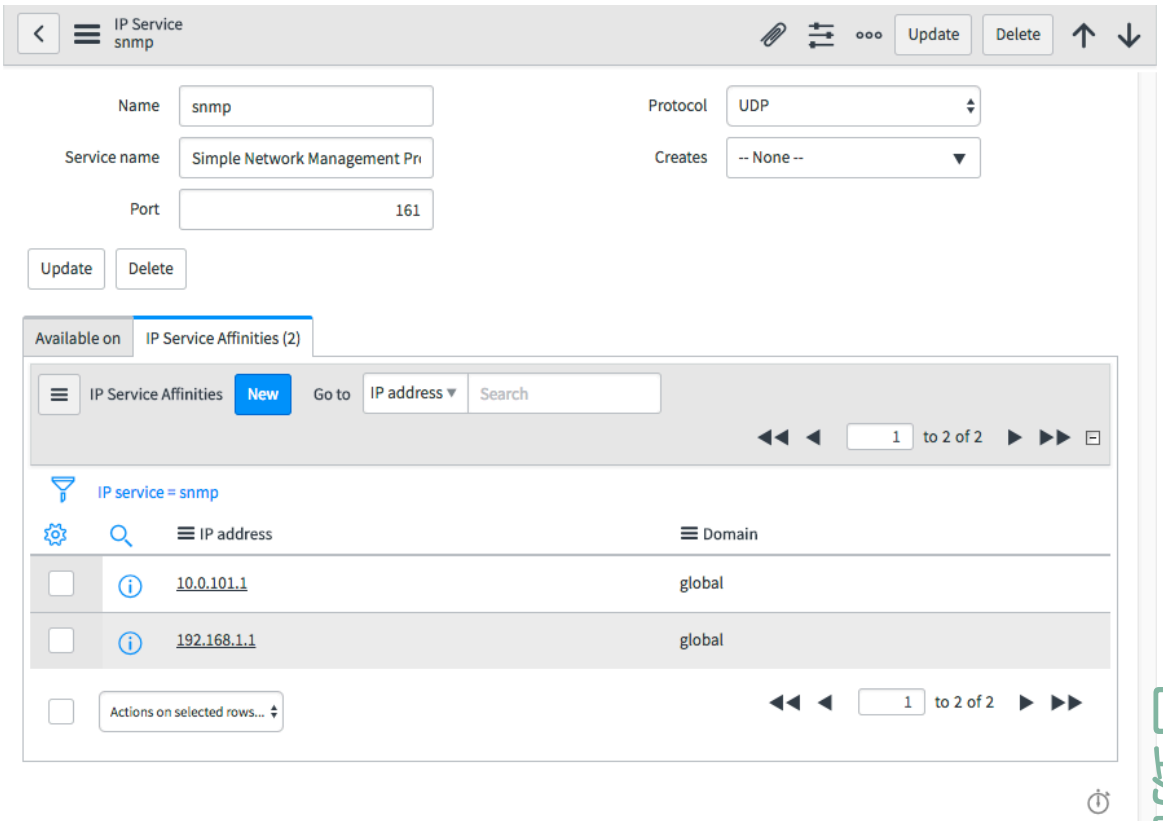
1. 移動先 すべて > ディスカバリー定義 > **IP** サービス.
2. リストをフィルタリングして、適切な IP サービスを探します。
3. そのサービスの名前をクリックしてその IP サービスページに移動します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

4. そのサービスに関連付けられている IP アドレスのリストの **[IP** サービスの親和性] タブをクリックします。

IP サービスの親和性



ログインと認証のセキュリティ

インスタンスへのアクセスを制御するログインセキュリティオプションを設定します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ログインと認証のセキュリティの詳細

ログインセキュリティの機能とビジネス価値について説明します。

ログインセキュリティを設定する

高セキュリティを構成する方法について説明します。

ログインシナリオの定義

ログインシナリオを定義します。

Password Reset

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ログイン パスワードのリセットについては、こちらをご覧ください。

ログインと認証のセキュリティの詳細

インスタンスへのアクセスを制御するログインセキュリティオプションを設定します。

セキュリティオプション

ユーザーのログインと認証セキュリティのいくつかの側面を制御できます。

機能	説明	関連トピック
ログインおよびログアウトのコントロール	ログイン時にユーザーに表示するランディングページを指定するなど、ユーザーのログインおよびログアウトプロセスのいくつかの側面を制御します。また、ユーザーのログアウト方法を制御します。	• ログインシナリオの定義 • ログアウト確認プロンプトの構成 • ログアウトボタンの削除 • インストレーションイグジット • 失敗したログイン試行のロックアウトを指定する
認証セキュリティ	パスワードリセットプロセスと [記憶する] オプションなどの機能を制御します。インスタンスへのアクセスに IP アドレスベースのコントロールを使用することができます。また、Single Sign-on Digest Authentication で使用するノンスを実装することもできます。	• パスワード・ポリシーの構成 • パスワード検証ルールの強化 • 参照例：デフォルトのセルフサービス パスワードリセット プロセス • [記憶する] チェックボックスと cookie の設定を変更する

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

機能	説明	関連トピック
		• IP 範囲ベースの認証 • ノンスの実装

ログアウト確認プロンプトの構成

ログアウト確認プロンプトを有効にして、ユーザーが誤ってログアウトしないようにすることができます。

始める前に
必要なロール：管理者

このタスクについて
注:
次の手順は、最新かつ最も一般的に使用されている コア UI より前の UI バージョンでのみ機能します。

手順

1. 移動先 すべて > システムプロパティ > システム.
2. ログアウト要求を確認するメッセージをユーザーに表示するプロパティを見つけて、チェックボックスをオンにします。
3. ユーザーが [ログアウト] ボタンをクリックすると、確認ダイアログボックスが表示されます。

パスワードリセット プロパティの構成

エンド ユーザーの パスワードリセット エクスペリエンスを設定するプロパティを指定できます。

始める前に
必要なロール：password_reset_admin

このタスクについて
プロパティに入力できる値の範囲に制限はありませんが、1 以上の正の整数値のみを使用することをお勧めします。プロパティの上限範囲を決めるときは、ユーザーがどのようなタスクを実行するのかを考慮してください。

たとえば、ユーザーの本人確認の試行を 100 回許可することは通常は望まれません。一般的に許可する試行回数の値は 3 回です。同様に、登録プロセスを完了するために、時間をかけてセキュリティの質問を 30 個選択して回答するようユーザーに強制することも、通常は望まれません。一般的に使用するセキュリティの質問の数は 5 ～ 7 個です。

手順

1. 移動先 すべて > パスワードリセット > プロパティ.
   プロパティの詳細については パスワードリセット 、次を参照してください: パスワードリセットのグローバルプロパティ .
2. 必要に応じて設定を更新し、[保存] をクリックします。

ログインシナリオの定義

ログイン後にすべてのユーザーを同じページに誘導することができます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

始める前に
必要なロール：admin

このタスクについて
ユーザーが http://{instance_name}.service-now.com/ にアクセスするなど、インスタンスに直接ログオンすると、システムは次のことを行います。

1. プロパティ *glide.entry.page.script* の値にアクセスします。プロパティのデフォルト値は、*CMSEntryPage* という名前のスクリプトインクルードから派生します。
2. エントリページでログインが必要な場合、ユーザーをインスタンスのログインページに誘導します。
3. ログインルールがある場合は、ユーザーに適用します。

ログイン後にすべてのユーザーを同じページに誘導するようにするには、次の手順を実行します。

手順

1. 移動先 すべて > コンテンツ管理 > 構成 > 環境設定ページ.
2. [ログインページ] フィールドの値を選択するか、必要に応じて新しいページを作成します。このページがサイトのデフォルトページでない場合は、常にここにリダイレクトされます。サイトのデフォルトページの場合は、ログインルールが適用されます。この値が null の場合、システムは navpage.do をエントリページとして使用します。ここにログインページを入力しないでください。入力すると、ユーザーは 2 回ログインする必要があります。

   インスタンスにログインしてレコードにアクセスする場合：

   ユーザーがインスタンスにログインして、http://{instance}.service-now.com/incident.do?sys_id={sys_id} などのグローバルに一意な識別子 (sys_id) でレコードにアクセスすると、システムは以下を実行します。

   a. まだログインしていない場合は、ユーザーをログインページに誘導します。
   b. アクセスが許可されている場合、ユーザーを適切なレコードに誘導します。ユーザーがレコードへのアクセス権を持っていない場合は、アクセスを拒否するメッセージが表示されます。

   Service Portal または CMS サイトにログインする場合：

   ユーザーが Service Portal または CMS サイト (http://<instance>.service-now.com/site-name/page.do など) にログオンすると、システムは以下を実行します。

   - Service Portal または CMS サイトフォームの [ログインページ] フィールドに値がある場合、ユーザーはそのログインページに誘導され、ログインルールがある場合はそれが適用されます。
   - ログインページが指定されていない場合は、Service Portal または CMS サイトフォームの [ホームページ] フィールドの値に誘導されます。

   Service Portal または CMS サイトにログインしてレコードにアクセスする場合：

   ユーザーがレコードにアクセスするために Service Portal または CMS サイト (http://{instance}.service-now.com/ess/incident_detail.do?sysparm_document_key=incident,{sys_id} など) にログオンすると、同じ手順が実行され、最後にレコードに誘導されます。ユーザーがレコードへのアクセス権を持っていない場合は、アクセスを拒否するメッセージが表示されます。

ログインと従業員セルフサービスポータル

ユーザーが従業員セルフサービスポータルにログインしようとしても、ユーザーがアクセスしようとしている最初のページの追跡を続けます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

次のシナリオを考えてみましょう。

例 1：

1. ユーザーはログインしておらず、特定の SYS ID を URL 内で使用してレコードにアクセスしようとします。
2. ユーザーはログインページにリダイレクトされます。
3. ユーザーはログインするのではなく、従業員セルフサービス (/ess) ポータルなどの別のサイトにアクセスしようとします。
4. ユーザーはログインページに再度リダイレクトされます。
5. ユーザーはログインすると、従業員セルフサービスポータルではなく、ユーザーが最初にアクセスしようとしたレコードにリダイレクトされます。

例 2：

1. ユーザーはログインしておらず、従業員セルフサービス (/ess) ポータルから特定の SYS ID を URL 内で使用してレコードにアクセスしようとします。
2. ユーザーはログインページにリダイレクトされます。
3. ログインするのではなく、ユーザーは従業員セルフサービスポータルから別のレコードにアクセスしようとします。
4. ユーザーはログインページに再度リダイレクトされます。
5. ユーザーはログインすると、2 番目のレコードではなく最初のレコードにリダイレクトされます。

ログインランディングページの指定

デフォルトでは、ログイン時にホームページが表示されます。システムプロパティまたはコンテンツ管理システムを使用して、別のログインランディングページを指定することができます。

始める前に

必要なロール：管理者

このタスクについて

すべてのユーザーのログインランディングページを指定するには、sys_properties テーブルのプロパティ値を変更します。

手順

1. ナビゲーションフィルターで、「sys_properties.list」と入力します。
2. **glide.login.home** システムプロパティを見つけます。
3. [値] フィールドに、ログイン時にすべてのユーザーに表示されるページ名を入力します。

   <page name>.do を使用すると、URL の http://"instance".service-now.com/ の部分を省略できます。システム内のページ名またはページの URL を指定するために、リンクをポイントすることができます。可能なページは、welcome.do と incident.doです。

   ダッシュボードのランディングページを指定するには、プロパティを $dashboards.do?dashboard=<SYS_ID> に設定します。<SYS_ID> をダッシュボードの sys_id に置き換えます。

   ユーザーをサービスポータルに誘導するには、プロパティを /sp に設定します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

> **注:**
> このプロパティはシステム全体に適用されるため、設定はすべてのユーザーに影響します。ロールのないユーザー専用のログインを設定するには、同じ手順を適用し、**glide.entry.loggedin.page_ess** プロパティを使用します。

コンテンツ管理システムでログインランディングページを指定することもできます。

失敗したログイン試行のロックアウトを指定する

システムで提供されている非アクティブなスクリプト アクションを使用すると、ユーザー アカウントをロックする前のログイン試行の失敗回数を指定でき、ログイン成功後にカウントをリセットすることができます。

始める前に

必要なロール：管理者

手順

移動先 すべて > システムポリシー > スクリプトアクション スクリプトを表示またはアクティブ化します。

> **注:**
> Kingston リリース以降の zBoot 以後では、「**SNC** ユーザーのロックアウトの確認と自動ロック解除」および「**SNC** ユーザーのクリア」のスクリプトアクションがアクティブ化されています。
>
> 失敗したログインの試行に影響するプロパティの詳細については、インスタンスセキュリティ強化設定の「失敗したログインの試行の管理 (インスタンスセキュリティ強化)」を参照してください。

スクリプトアクション	説明
SNC ユーザーのロックアウトの確認と自動ロック解除	• *glide.user.max_unlock_attempts* プロパティの値を使用して、ログイン試行の失敗回数の制限を設定します。 • *glide.user.unlock_timeout_in_mins* プロパティで指定された時間が経過すると、ユーザーアカウントのロックが解除されます。値を指定しない場合は、デフォルトの 15 分後にユーザーアカウントのロックが解除されます。
SNC ユーザーのロックアウトの確認	ログイン試行の失敗回数を追跡し、指定した回数のログイン試行の失敗後にユーザーアカウントをロックします (デフォルトは 5 回)。
SNC ユーザーのクリア	ログイン成功後にユーザーレコードを更新します。ログイン試行の失敗回数をリセットし、最終ログイン日を更新します。

次のタスク

ユーザーがログインを試みると、そのたびにアクションがイベントログに記録されます。ログイン試行の失敗のログを表示できます。

1. 移動先 システムポリシー > イベントログ.
2. [名前] フィールドでフィルターを適用し、**[login.failed]** を探します。試行されたログインの名前、日付、およびログイン試行が行われた IP アドレスを表示できます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

UI ページを公開または非公開にする

ユーザーがログインせずにページを表示できるようにするには、ページを公開にします。

始める前に
必要なロール：管理者

このタスクについて
ほとんどのページは、ログインしたユーザーにのみ表示されます。限られた数のページ (ようこそページ、フロントページ、ログインページとログアウトページなど) は、ユーザーがログインしなくても表示できるように公開されています。

> ⚠ 警告:
> 多くの機能にはいくつかのベースシステムの公開ページが必要です。ベースシステムの公開ページを無効にしないでください。

手順

1. アプリケーションナビゲーターフィルターに「csm_table_map.list」と入力します。
2. [新規] をクリックします。
3. sys_public テーブルで、次の値のレコードを作成します。

フィールド	説明
ページ	ページ名例：$sp
有効	選択すると、ページが公開されます。ページを非公開にする場合は、[アクティブ] オプションの選択を解除します。

4. [保存] をクリックします。
   アクティブを true に設定するとページが公開されるため、<instance_name>/sp または <instance_name>/$sp.do によってページにアクセスできます。

参照例：デフォルトのセルフサービス パスワードリセット プロセス

デフォルトのセルフサービス パスワードリセット プロセスでは、ユーザーはサービスデスク担当者から支援を受けずにパスワードをリセットできます。

Example: デフォルトのセルフサービスパスワードリセットフロー

1. ユーザーがパスワードを忘れた場合、ユーザーはログイン画面で [パスワードを忘れた場合] リンクをクリックします。
2. パスワードリセット アプリケーションが起動します。[識別] ページで、ユーザーは [ユーザー名] を入力して自分自身を識別します。
3. [検証] ページで、ユーザーは、自分がユーザー名に関連付けられた人物であることを証明します。この例では、ユーザーはユーザー プロファイルに関連付けられたメール アドレスを入力します。管理者は別の検証方法を設定することができます。または、ユーザーだけが回答できる個人的な質問などの追加の検証を義務付けることができます。
4. [リセット] ページで、メールで手順を確認するようユーザーに指示します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

5. ユーザーはメールを開き、パスワードをリセットするための [ここ] リンクをクリックします。リンクは、ユーザーが指定した期間有効です (**password_reset.request.expiry** プロパティを使用します)。
6. [パスワードのリセット] ページで、パスワードをリセットするための案内がユーザーに表示されます。

デフォルトのセルフサービス パスワードリセット プロセス (com.glideapp.password_reset) では次のものを定義します。

- ユーザーが [パスワードを忘れた場合] をクリックしたときのリダイレクト先を指定する URI。デフォルトでは、この値は **/$pwd_reset.do?sysparm_url=ss_default** です。これは *glide.security.password_reset.uri* プロパティで使用されている値と同じです。以前のリリースでは、この値は **/reset_password.do** に設定されていました。
- [パスワードリセット **URL** を有効にする] オプション。ユーザーが [パスワードを忘れた場合] オプションをクリックした後に、パスワードをリセットするためのリンクを含むメールを受信することを指定します。
- パーソナル データ - 3 段階の Password Reset フローを指定するメールアドレス入力検証フロー。

このフォームにアクセスしてフィールドを設定する方法については、「Password Reset プロセスの設定」を参照してください。

注:

- この機能は、ローカルで認証されたユーザー (ユーザーレコードで指定されたユーザー名とパスワードを入力したユーザー) の場合に有効です。SSO ソリューションまたは LDAP 統合を使用してインスタンスにログインしているユーザーは、セルフサービス パスワードリセット プロセスの例を使用してパスワードをリセットすることはできません。
- エンドユーザーは通知設定を有効にして設定する必要があります。「サブスクリプションベースの通知」を参照してください。管理者は、エンドユーザーに送信されるメールを変更することができます。

自動翻訳

パスワードリセット 通知メールテキストの変更

セルフサービスの パスワードリセット プロセスのユーザーは、パスワードのリセットを要求するとメール通知を受け取ります。メールのテキストや通知のその他の要素を変更できます。

始める前に

必要なロール：管理者

このタスクについて

このプロセスは、ユーザーがサブスクリプションベースの通知 である場合にのみ該当します。

手順

1. 移動先 すべて > システム通知 > 通知.
2. [パスワードリセット **URL]** 通知を選択します。
3. [内容 **(What it will contain)]** セクションでメールのテキストを変更します。
   通知のその他の側面の設定に関する詳細については、「メール通知を作成する」を参照してください。

ログアウトボタンの削除

[ログアウト] ボタンを削除すると、誤ってログアウトするのを防ぐことができます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

始める前に
必要なロール：管理者

このタスクについて

注:
次の手順は コア UI では機能しません。

手順

1. 移動先 すべて > ユーザー管理 > ユーザー初期設定.
2. システム環境設定 *user.can.logout* を削除します。

インストレーションイグジット

インストレーションイグジットは、Java からイグジットしてスクリプトを呼び出してから Java に戻るカスタマイズ機能です。

注:
ここで説明する機能には、**admin** ロールが必要です。

利用可能なインストレーションイグジット

移動先 システム定義 > インストレーションイグジット. 一部のインストレーションイグジット名 (Login、Logout、ValidatePassword、ExternalAuthentication) は予約されており、変更できません。他のインストレーションイグジットは、デフォルトのインストレーションイグジットのスクリプトを置き換えるカスタムスクリプトで上書きすることができます。

ベースシステムでは、次のインストレーションイグジットを使用できます。

インストレーションイグジット	説明
ログイン	ユーザー名とパスワードのペアを取得し、ユーザーオブジェクトで認証します。
ログアウト	サインアウト時にようこそページに移動します。LogoutRedirect で上書きすることができます。
LogoutRedirect	サインアウト時に指定された URL に移動します。
ExternalAuthentication	ヘッダー、パラメーター、または cookie を使用して認証します。DigestSingleSignOn と PGPSingleSignOn で上書きすることができます。
DigestSingleSignOn	ヘッダー、パラメーター、または cookie を使用して認証し、ダイジェスト暗号を復号化します。
PGPSingleSignOn	ヘッダー、パラメーター、または cookie を使用して認証し、PGP 暗号を復号化します。
ValidatePassword	Helsinki リリース以降、デフォルトでアクティブ化されます。それにより、顧客が独自のパスワード検証を定義できます。また、ValidatePasswordStronger で上書きできます。
ValidatePasswordStronger	パスワードは 8 文字以上で、数字、大文字、および小文字を含める必要があります。
GetIntegrationSessionTimeout	デフォルトの統合セッションのタイムアウト動作を実装します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ログインの変更

ログインインストレーションイグジットを次のように変更すると、ユーザーがログインする時に、各ユーザーのセッションタイムアウト値が設定されます。この特定の例では、ユーザー名が *admin* の場合、セッションは 30 秒でタイムアウトに設定されます。

```
gs.include("PrototypeServer");

var Login = Class.create();
Login.prototype = {
 initialize : function() {
 },

      process : function() {
        // the request is passed in as a global
        var userName = request.getParameter("user_name");
        var userPassword = request.getParameter("user_password");

        var authed = GlideUser.authenticate(userName, userPassword);
        if (authed) {
          // ************************************************************
          // customization - if the userName == admin, set the session
          // timeout to be 30 seconds. You can implement your own
          // session timeout algorithm here by checking to see if a user
          // belongs to a certain group or has a certain role.
          // Values of setMaxInactiveInterval exceeding 1440 minutes are
          // treated as one day (1440 minutes).

         if (userName == "admin") {
            request.getSession().setMaxInactiveInterval(30);
          }
          // ************************************************************
          return GlideUser.getUser(userName);
        }

        this.loginFailed();

        return "login.failed";
      },

      loginFailed : function() {
        var message = GlideSysMessage.format("login_invalid");
        var gSession = GlideSession.get();
        gSession.addErrorMessage(message);

        var userName = request.getParameter("user_name");
        EventManager.queue("login.failed", "", userName, "");
      }

}
```

セッションタイムアウトは、IP アドレスに基づいて設定することもできます。

```
gs.include("PrototypeServer");

var Login = Class.create();
Login.prototype = {
```

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

```
initialize : function() {
},

    process : function() {
      // the request is passed in as a global
      var userName = request.getParameter("user_name");
      var userPassword = request.getParameter("user_password");

      var authed = GlideUser.authenticate(userName, userPassword);
      if (authed) {

      // ************************************************************
      // customization - if the user is logging in from a particular IP
      // range starting with XXX.XXX you can implement your own
      // session timeout algorithm here by checking the login IP
      //
      // Values of setMaxInactiveInterval exceeding 1440 minutes are
      // treated as one day (1440 minutes).

      var clientIP = gs.getSession().getClientIP().toString();

      // if client IP starts with specified range
      if (clientIP.indexOf('XXX.XXX') == 0) {
        // set to 10 hours
        request.getSession().setMaxInactiveInterval(60 * 60 * 10);
      }
      // ************************************************************

        return GlideUser.getUser(userName);
      }

      this.loginFailed();

      return "login.failed";
    },

    loginFailed : function() {
      var message = GlideSysMessage.format("login_invalid");
      var gSession = GlideSession.get();
      gSession.addErrorMessage(message);

      var userName = request.getParameter("user_name");
      EventManager.queue("login.failed", "", userName, "");
    }

}
```

関連情報

強力なパスワードを強制する

パスワード検証ルールの強化

パスワード検証に関連付けられたインストレーションイグジットを上書きすることで、[パスワード変更] 画面のパスワード強度検証ルールをカスタマイズできます。

始める前に

必要なロール：管理者

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. 移動先 すべて > システム定義 > インストレーションイグジット.
2. **ValidatePassword** (デフォルトでは非アクティブ) と **ValidatePasswordStronger** (デフォルトではアクティブ、Helsinki リリース以降) を探します。
3. `ValidatePasswordStronger` スクリプト (以下を参照) は、正規表現を使用して `ValidatePassword` スクリプトを上書きするサンプルスクリプトです。パスワードは 8 文字以上で、数字を含め、大文字と小文字を組み合わせる必要があります。

```
gs.include("PrototypeServer");
 var ValidatePasswordStronger = Class.create();
 ValidatePasswordStronger.prototype = {
    process : function() {
      var user_password = request.getParameter("user_password");
      var min_len = 8;
      var rules = "Password must be at least " + min_len +
        " characters long and contain a digit, an uppercase letter, and a lowercase letter.";
      if (user_password.length() < min_len) {
        gs.addErrorMessage("TOO SHORT: " + rules);
        return false;
      }
      var digit_pattern = new RegExp("[0-9]", "g");
      if (!digit_pattern.test(user_password)) {
        gs.addErrorMessage("DIGIT MISSING: " + rules);
        return false;
      }
      var upper_pattern = new RegExp("[A-Z]", "g");
      if (!upper_pattern.test(user_password)) {
        gs.addErrorMessage("UPPERCASE MISSING: " + rules);
        return false;
      }
      var lower_pattern = new RegExp("[a-z]", "g");
      if (!lower_pattern.test(user_password)) {
        gs.addErrorMessage("LOWERCASE MISSING: " + rules);
        return false;
      }
      return true; // password is OK
    }
 }
```

`Class.create()` で作成されたスクリプト変数は、インストレーションイグジットと同じ名前 (この例では「ValidatePasswordStronger」) にする必要があります。このスクリプトは、パスワードが受け入れ可能な場合は true を返し、パスワードを変更する必要がある場合は false を返す `process()` 関数を実装しています。`gs.addErrorMessage` 関数を使用すると、[パスワード変更] 画面でエラーメッセージを返すことができます。アクティブなフラグを確認してレコードを更新することで、インスタンスでこのインストレーションイグジットを試すことができます。変更が認識されるように、試行後に必ずキャッシュをクリアしてください。

また、これらのスクリプトを変更しても、デフォルトの ServiceNow の動作は変更されないことに注意してください。デフォルトでは、空のパスワードは引き続き禁止されています。また、パスワードフィールドとパスワード検証フィールドは一致している必要があります。

タスクの結果

テストするには、ユーザーレコードの [パスワードのリセットを強制] ボックスをオンにして、そのユーザーでログインします。ユーザーがパスワードを設定しようとすると、検証が行われます。管理

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

者ユーザーがユーザーレコードのパスワードを直接更新する場合、検証は適用されません (管理者はパスワードフィールドに何でも入力できます)。

注:
[パスワード変更] 画面は、Single Sign-on を使用せず、ローカル LDAP と統合されていない顧客にのみ適用されます。

[記憶する] チェックボックスと **cookie** の設定を変更する

[記憶する] チェックボックスがログイン時に選択されている場合、ユーザーのコンピューターに cookie が保存されます。この cookie は、その後のアクセス時にユーザーを自動的に認証します。

ユーザーがログアウトすると、cookie は破棄されます。[記憶する] チェックボックスのデフォルト値は 1 つのプロパティで制御されます。チェックボックスがログインページに表示されるかどうかは別のプロパティで制御されます。

2 つのプロパティ *glide.ui.user_cookie.life_span_in_days* および *glide.ui.user_cookie.max_life_span_in_days* は、glide_user システムによって生成された cookie の有効期限の値を制御します。ユーザーが「記憶する」が有効になっているインスタンスにアクセスすると、Cookie の有効期限は最大 (glide.ui.user_cookie.max_life_span_in_days) 有効期限に達するまでになります。

注:
これらのプロパティの詳細については、「インスタンスセキュリティ強化設定」の以下のトピックを参照してください。

- 絶対セッションタイムアウト
- セッションウィンドウのタイムアウト

[記憶する] チェックボックスのデフォルト値を変更する

[記憶する] チェックボックスのデフォルト値を変更することができます。

始める前に
必要なロール：管理者

手順

1. 移動先 すべて > システムプロパティ > **UI** プロパティ.
2. *Default value of "Remember me" checkbox on login page* プロパティ (*glide.ui.remember.me.default*) を探します。
3. [記憶する] チェックボックスのデフォルト値を [いいえ] に設定するには、このプロパティのチェックボックスをオフにします。
4. [記憶する] チェックボックスのデフォルト値を [はい] に復元するには、プロパティのチェックボックスを選択します。

[記憶する] チェックボックスを削除する

[記憶する] チェックボックスを削除して、ユーザーがこの機能にアクセスできないようにすることができます。

始める前に
必要なロール：security_admin

注:
このプロパティの詳細については、「インスタンスセキュリティ強化設定」の「[記憶する] の削除」を参照してください。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

手順

1. ロールを security_admin に昇格させます。
2. 移動先 システムプロパティ > **UI** プロパティ.
3. *Remove "Remember me" checkbox from login page* プロパティ (*glide.ui.forgetme*) を探します。
4. プロパティのチェックボックスを選択します。
   この設定により、 [記憶する] チェックボックスが削除され、既存の cookie が無効になり、記憶する機能が完全に無効になります。
5. [記憶する] チェックボックスをログインページに復元するには、プロパティのチェックボックスをクリアします。

IP 範囲ベースの認証

Web ベースのアプリケーションを保護する 1 つの方法は、IP アドレスに基づいてアクセスを制限することです。

悪意のある個人に属すると思われる特定のアドレスまたはアドレス範囲へのアクセスをブロックできます。インスタンスにより、IP アドレスでアクセスを制御できます。

注意事項および制限事項：

- 自分自身をロックアウトすることはできないため、現在のアドレスがロックアウトされるようなルールを追加しようとすると、警告が表示されて挿入が拒否されます。
- 企業イントラネット内にいる場合は、IP ルールの設定に十分注意してください。通常、自分のコンピューターに表示される IP アドレス (10.10.10.25 など) は、実際にインターネット上に表示される IP アドレスとは無関係です。会社は、ユーザーのアドレスを予測可能な送信アドレスにプロキシしたり、NAT を行ったりします。これについては、ネットワークチームに問い合わせる必要があります。
- アクセスルールに基づいてアクセスが制限されているユーザーには、ブラウザーで 403 エラーが表示されます。
- 制限付きユーザーは、トランザクション、セマフォ、またはサーバーリソースカウントを使用しません。
- たとえば、データセンターへの VPN を実行している場合、この機能が既存のアクセス制御ルールに優先されることも上書きされることもありません。これは、PIX で設定されている可能性があるアクセス制御に加えて満たす必要がある追加のチェックです。
- 許可ルールは常に拒否ルールより優先されます。そのため、アドレスが (1 つのルールで) 許可され、(2 番目のルールで) 拒否される場合、実際には許可されます。
- 現在、アスタリスクと CIDR ブロックはサポートされていません。
- 転送プロキシアドレスについては、チェーン内の各アドレスに許可ルールが適用され、一致する許可ルールがない場合はチェーン内の各アドレスに拒否ルールが適用されます。
- IP 範囲ベースの認証は、Update Sets の転送に影響を与える可能性があります。ソースインスタンスで IP アドレスアクセス制御が有効になっている場合は、インスタンスをサポートするすべてのアプリケーションノードの IP アドレスを例外として追加します。

> **注:**
> インスタンスの IP 情報を見つけるには、次にログインします。 ServiceNow - 今すぐサポート をクリックし、[自分の **IP** 情報] サービスカタログアイテムを検索します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注:
特定の IP 範囲へのインスタンスアクセスを制限する *com.snc.ipauthenticator* プロパティと *glide.ip.authenticate.strict* プロパティの詳細については、「インスタンスセキュリティ強化設定」の以下のトピックを参照してください。

- 特定の IP 範囲へのアクセスを制限する
- 厳格な IP 制限

IP アドレスのアクセス制御

送信トラフィック、受信トラフィック、または双方向トラフィックに IP アクセス制御を適用します。一致する拒否ルールが存在し、一致する許可ルールが存在しない場合にのみ、IP アドレスがブロックされます。デフォルトでは、インスタンスへのアクセスに制限はありません。

始める前に
必要なロール：管理者

手順

1. 移動先 すべて > システムセキュリティ > **IP** アドレスアクセス制御 をクリックして、IP アクセス制御のリストを表示します。
   IP 範囲ベースの認証 [com.snc.ipauthenticator] プラグインを有効にする必要がある場合があります。
2. フォームを完了します。

注:
インスタンスの IP 情報を見つけるには、次にログインします。 ServiceNow - 今すぐサポート をクリックし、[自分の **IP** 情報] サービスカタログアイテムを検索します。

フィールド	説明
タイプ	含めるアクセス制御ルールのタイプ。 ○ 許可：この範囲内のすべての IP アドレスがこのインスタンスとやり取りができます。 ○ 拒否：この範囲内の IP アドレスは、許可ルールにリストされていない限り、このインスタンスとやり取りができません。また、拒否ルールを追加するときに、自分のパブリック IP アドレスを拒否できないか、インスタンスが拒否ルールを更新しません。 **注:** メンテナンス、アップグレード、および カスタマーサービス & サポート をサポートするため、一部の ServiceNow の内部 IP は拒否ルールでブロックできません。
方向	IP アクセス制御ルールの方向。 ○ 受信：受信トランザクションを許可または拒否します。これらは、インスタンスの外部から開始されたトランザクションです。 ○ 送信：送信トランザクションを許可または拒否します。これらは、インスタンスの内部から開始されたトランザクションです。 ○ 双方向：受信トランザクションと送信トランザクションの両方を許可または拒否します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
有効	選択すると、フォームがアクティブ化されます。
説明	アクセス制御の説明。
範囲開始	許可または拒否する IP アドレスの開始範囲。 注: これらのルールは、更新セットの転送にも影響します。IP アドレスアクセス制御によって更新セットが失敗しないようにするには、ターゲットインスタンスを例外として追加します。
範囲終了	許可または拒否する IP アドレスの終了範囲。 注: 特定の VPN アドレスのみにアクセスを制限するには、[拒否] フィールドに **0.0.0.0** ～ **255.255.255.255** の範囲を入力し、特定の許可された VPN 範囲のみを入力します。

3. [送信] をクリックします。

拒否された **IP** アドレスを検索する

インスタンスのノードログファイルで、拒否された IP アドレスを検索します。

始める前に
必要なロール：admin

このタスクについて
ブロックされた IP アドレスのログエントリは、2015-10-21 18:37:43 (175) http-30 警告 *** 警告 *** セキュリティ制限：アクセスが制限されています (xx.xx.xxx.xxx は許可されていません) のように表示されます。

注:
拒否された IP アドレスは、表示可能なインスタンスのノードログファイルであり、システムログからは表示できません。

手順

1. 移動先 すべて > システムログ > ユーティリティ > ノードログファイルブラウザ。.
2. 期間やメッセージなどの基準でログを参照します。
3. 探しているログがわかっている場合は、次の場所に移動してログファイルをダウンロードすることもできます。 システムログ > ユーティリティ > ノードログファイルのダウンロード.

ノンスの実装

Single Sign-on Digest Authentication で使用するノンスを実装することができます。

Single Sign-on の暗号化されていないトークン方式または暗号化されたトークン方式でノンスを使用するには、これらの手順をいくつかの小さな変更でのみ適用します。

注:
ノンスはログイン要求にのみ使用され、他のタイプの要求には使用されません。ログイン後にノンス値を受信した場合、ノンスは消費されません。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

利点

ノンスを使用すると、悪意のあるユーザーがシステムにログインするためにリプレイ攻撃を実行できなくなります。

ノンスプロセスフロー

ダイジェストトークンの Single Sign-on を実装し、ノンスのセキュリティを追加する場合は、特定のプロセスフローに従います。

1. ユーザーが顧客のポータルにログインします。
2. 顧客は必要な SSO パラメーターを生成し、末尾にランダムなノンスを追加します。たとえば、顧客がクエリー文字列を使用して認証応答を転送している場合は、次のようになります。

```
SM_USER=itil&DE_USER=V1QuWMmxSfBgfRS099X0cAjKo5Q=&NONCE=1407743018
```

インスタンスはこの要求を受信し、認証変数を取得します。認証応答の整合性を検証する前に、インスタンスは内部テーブル (u_authentication_nonce) に対してノンスを確認し、そのノンスがまだ存在しないことを確認します。そのテーブルにノンスが存在しない場合は、ノンスがテーブルに追加され、認証プロセスが許可されます。そのノンスの値がすでにテーブルに存在する場合、認証の試行はキャンセルされ、failed_missing_requirement というエラーコードが返されます。これにより、通常、ユーザーはログインページに戻ります。

ノンスを実装する

暗号化ノンスを認証ヘッダーに追加して、1 回のみ使用できるようにします。

- *glide.authenticate.header.nonce_key* という名前のシステムプロパティを作成し、その値を NONCE や NCE など、ノンスに使用している変数名に設定します。
- u_authentication_nonce という名前の新しいテーブルを作成します。u_nonce という名前のテーブルにフィールドを追加します。
- 検索項目 システムプロパティ > インストレーションイグジット そして、ExternalAuthentication (*glide.authenticate.external_property*) を上書きする DigestSingleSignOnNonce というアイテムを作成します。
- 新しく作成した DigestSingleSignOnNonce のスクリプト部分に次のコードを追加します。

```
gs.include("PrototypeServer");

var DigestSingleSignOnNonce = Class.create();
DigestSingleSignOnNonce.prototype = {

 process : function() {

 var headerKey = GlideProperties.get("glide.authenticate.header.key", "SM_USER");
 var headerDigestKey = GlideProperties.get("glide.authenticate.header.encrypted_key",
"DIGEST");
 var headerNonceKey = GlideProperties.get("glide.authenticate.header.nonce_key", "NCE");
 var fieldName = GlideProperties.get("glide.authenticate.header.value", "user_name");
 var fkey = GlideProperties.get("glide.authenticate.secret_key");

 // Look in the Headers
 var data = request.getHeader(headerKey);
 var encdata = request.getHeader(headerDigestKey);
 var nonce = request.getHeader(headerNonceKey);
```

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

```
// If not, then check the URL Parameters
if (data == null || encdata == null || nonce == null) {
 data = request.getParameter(headerKey);
 encdata = request.getParameter(headerDigestKey);
 nonce = request.getParameter(headerNonceKey);
}

// then maybe its a cookie
if (data == null || encdata == null || nonce == null) {
 var cookies = request.getCookies();
 data = GlideCookieMan.getCookieValue(cookies, headerKey);
 encdata = GlideCookieMan.getCookieValue(cookies, headerDigestKey);
 nonce = GlideCookieMan.getCookieValue(cookies, headerNonceKey);
}

// if found run encryption
if (data != null && encdata != null && nonce != null) {
 try {

  // Replace all spaces with plus(+)'s, converted in url
  encdata = encdata.replaceAll(' ', '+');

  // ----- Encrypt the username|nonce
  var key = this.getDigest( data + "|" + nonce, fkey);

  // Check for match of received encoded data
  // and your encoding of user name
  if (encdata == key) {
   var ugr = new GlideRecord("sys_user");
   ugr.initialize();
   if (!ugr.isValidField(fieldName)) {
    GlideLog.warn("External authorization is set to use field: '"+ fieldName + "' which doesn't
exist");
    return "failed_missing_requirement";
   }
   ugr.addQuery(fieldName, data);
   ugr.query();
   if (!ugr.next()) {
    var userLoad = GlideUser.getUser(data);
    if (userLoad == null)
     return "failed_authentication";

    ugr.initialize();
    ugr.addQuery(fieldName, data);
    ugr.query();
    if (!ugr.next())
     return "failed_authentication";

   }

   if (this.processNonce(nonce)){
    var userName = ugr.getValue("user_name");
    return userName;
   }
   else return "failed_missing_requirement";
   }
  else {
```

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

```
    return "failed_authentication";
   }
  } catch(e) {
   gs.log(e);
   return "failed_authentication";
  }
  // Encoded data didn't match recieved Encoded data
 } else {

  return "failed_missing_requirement";
 }
},

getDigest : function( data, fkey ) {
 try {
  // default to something JDK 1.4 has
  var MAC_ALG = "HmacSHA1";
  return SncAuthentication.encode(data, fkey, MAC_ALG);

 } catch (e) {
  gs.log(e.toString());
  throw 'failed_missing_requirement';
 }
} ,

processNonce : function( sentNonce ) {
 var ngr = new GlideRecord("u_authentication_nonce");

 ngr.addQuery("u_nonce", sentNonce);
 ngr.query();
 if (ngr.next()) {
  gs.log("This SSO entry has already been processed! (Nonce: " + sentNonce + ")");
  return false;
 }
 var ngrNew = new GlideRecord("u_authentication_nonce");
 ngrNew.initialize();
 ngrNew.u_nonce = sentNonce;
 ngrNew.insert();
 gs.log("Inserted new nonce: " + sentNonce);
 return true;
}
};
```

- 新しいインストレーションイグジットを保存したら、DigestSingleSignOn インストレーションイグジットに移動し、Active=false に設定されていることを確認します。

これで、インスタンスがノンスを実装するように設定されているはずです。

Web サービスセキュリティ

基本認証、相互認証、または WS-Security を使用してセキュリティを強制します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

ウェブセキュリティの詳細

Web サービスセキュリティの機能と
ビジネス価値について説明します。

相互認証の構成

相互認証の使用方法と
構成方法を理解します。

Web サービスセキュリティ

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

Web サービスのセキュリティについて学習します。

Web サービスセキュリティの詳細

基本認証、相互認証、または WS-Security を使用してセキュリティを適用します。

基本認証

WSDL 文書または SOAP メッセージの投稿の各要求で基本認証を適用するには、*glide.basicauth.required* プロパティを true に設定します。その場合、WSDL または SOAP の各要求には、基本認証 プロトコルで指定されているように「認証」ヘッダーを含める必要があります。要求は非インタラクティブであるため、要求の実行中は常に認証ヘッダーが必要になります。

必要かどうかに関わらず基本認証資格情報を提供すると、Web サービスの呼び出し結果として行われるデータの作成または更新が、基本認証資格情報で提供されたユーザーの代理で実行されるというメリットがあります。たとえば、インシデントレコードを作成すると、ジャーナルフィールドには、デフォルトのゲストユーザーではなく基本認証ユーザーのユーザー ID が割り当てられます。

認証ヘッダーで大文字化ルールを無視するには、*glide.security.script.include.name.case.insensitive.list* プロパティを使用します。システムプロパティ [sys_properties] テーブルでこのプロパティを変更して、認証を処理するために必要なスクリプトインクルードを追加できます。デフォルトでは、このプロパティには次の値があります。

- BasicAuth
- CustomAuth

必要に応じて他のスクリプトインクルードを追加します。

Perl と SOAP::Lite ライブラリの使用時に基本認証を提供するには、次の機能を実装できます。

```
sub SOAP :: Transport :: HTTP :: Client :: get_basic_credentials { return 'user_name' =>
 'password' ; }
```

- C#.NET VS 2005 以前のバージョンを使用している場合は、Credentials オブジェクトを利用できます。

```
System.Net . ICredentials cred  = new System.Net . NetworkCredential ( "user_name",
 "password" ) ;

service . ServiceNow proxy  = new service . ServiceNow ( ) ;
service . get getService  = newservice . get ( ) ;
service . getResponse getServiceResponse  = new service . getResponse ( ) ;

 try {
  proxy . Credentials = cred ;
  getService . sys_id = "bf522c350a0a140701972dbf876f1610" ;
  getServiceResponse  = proxy . get (getService ) ; catch (Exception ex ) { }
```

- C#.NET VS 2008 を使用している場合は、ClientCredentials オブジェクトを利用できます。

```
Demo_Incident. ServiceNowSoapClient client  = new Test08WebService . Demo_Incident .
 ServiceNowSoapClient ( ) ;
```

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

```
client . ClientCredentials . UserName . UserName = "admin" ;
client . ClientCredentials . UserName . Password = "admin" ;
```

次に、app.config ファイルで以下を探し、「None」を「Basic」に変更します。

```
<transport clientCredentialType= "None" proxyCredentialType= "None" realm= "" />
```

- VB .NET を使用している場合は、Credentials オブジェクトを利用すると次のようになります。

```
Sub Main()
        Dim cred  As New System.Net.NetworkCredential( "user_name",  "password")

        Dim proxy  As New VB_Democm.incident.ServiceNow
        Dim getIncident  As New VB_Democm.incident. get Dim getResponse  As New
 VB_Democm.incident.getResponse

       proxy.Credentials = cred

       getIncident.sys_id =  "[your sysID here]"

       getResponse = proxy. get(getIncident)

    End Sub
```

基本認証がオンになっており、認証情報が提供されていない場合の結果の応答は、次のようになります。

```
<html> <head > <title >Apache Tomcat/5.0.28 - Error report </ title > <style > <!--H1
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:22px;}
 H2
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:16px;}
 H3
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:14px;}
   BODY {font-family:Tahoma,Arial,sans-serif;color:black;background-color:white;}
 B {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;}    P
{font-family:Tahoma,Arial,sans-serif;background:white;color:black;font-size:12px;}   A
{color : black;}   A.name {color : black;}   HR {color : #525D76;}--> </
style > </ head > <body > <h1 >HTTP Status 401 -\ </ h1 > <HR size = "1" noshade =
"noshade" > <p >< b >type </ b > Status report </ p > <p >< b >message </ b > <u >< /
u >< / p > <p >< b >description </ b > <u >This request requires HTTP authentication ().
</ u >< / p > <HR size = "1" noshade = "noshade" > <h3 >Apache Tomcat/5.0.28 </ h3 >
</ body > </ html >
```

相互認証の構成

相互認証では、SSL (Secure Sockets Layer) 証明書を交換することによって信頼を確立します。

クライアントは、サーバーに接続する前に SSL 証明書を要求します。サーバーは、応答として、クライアントに独自の証明書を送信するように要求します。どちらも、HTTPS 接続を開始する前に証明書を検証し、確認応答を送信することで応答します。

管理者は、認定要求を実行する前に、キーストアを設定して証明書を生成する予備作業を行います。

⚠ 警告:
この機能で相互認証が可能になるのは、送信 HTTPS 接続だけです。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

キーストアの作成

インスタンスは現在、秘密鍵、公開証明書のペア、およびその署名済み証明書を格納する Java キーストアファイルのアップロードをサポートしています。

次の手順では、コマンドを使用して、新しい Java Keytool キーストアファイルの生成、証明書署名要求 (CSR) の作成、証明書のインポートを行うことができます。ルート証明書や中間証明書はいずれも、ドメインのプライマリ証明書をインポートする前にインポートする必要があります。コマンドラインインターフェイスで次のコマンドを入力します。

1. Java キーストアとキーペアを生成します。

```
keytool -genkey -alias mydomain -keyalg RSA -keystore my.keystore
```

2. 既存の Java キーストアの CSR を生成します。

```
keytool -certreq -alias mydomain -keystore my.keystore -file mydomain.csr
```

3. ルートまたは中間認証局 CA 証明書を既存の Java キーストアにインポートします。

```
keytool -import -trustcacerts -alias root -file Thawte.crt -keystore my.keystore
```

4. 署名済みプライマリ証明書を既存の Java キーストアにインポートします。

```
keytool -import -trustcacerts -alias mydomain -file mydomain.crt -keystore my.keystore
```

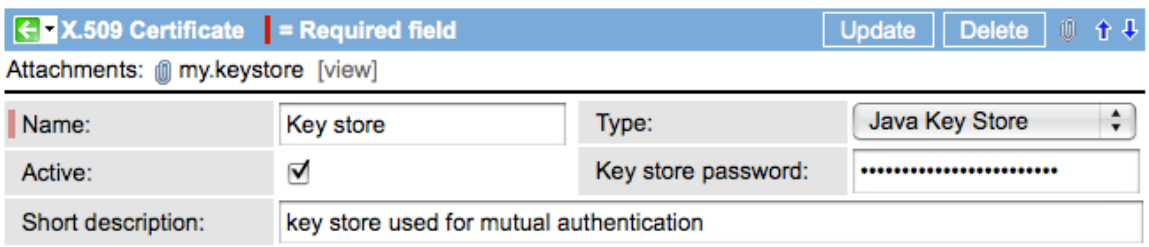
キーストアの設定

キーストアが作成されたので、証明書テーブルにアップロードできます。対象： システム定義 > 証明書 ページで、[新規] をクリックし、次のフィールドを設定します。

- 証明書の名前を入力します。
- キーストアをアクティブとして格納します。
- タイプを **[Java** キーストア] に設定します。
- キーストアパスワードを入力します。これは、キーストアの作成に使用されたパスワードです。

[送信] をクリックして Java キーストアエントリを作成します。

キーストア



信頼できるサーバー証明書の指定

送信 SSL 接続 (HTTPS Web サービス呼び出し) では、サービスプロバイダーによって提供される証明書を指定して、SSL 接続中のサービスプロバイダーの妥当性を保証することができます。たとえば、証明書で識別される安全なサービスにブラウザが接続しようとしている場合などです。

信頼できるサーバー証明書をアップロードすることで、ServiceNow により、接続しているサービスの妥当性と安全性を確保できます。

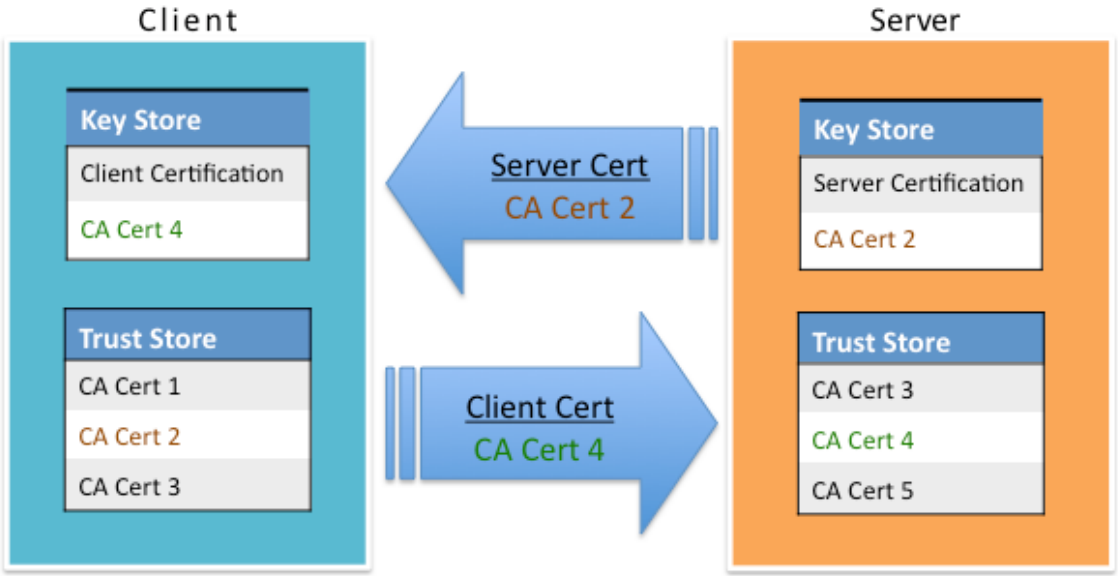
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

「信頼ストア証明書」タイプで新しい証明書エントリを作成し、DER 形式の証明書を添付するか、その PEM 形式をコピーして **[PEM** 証明書] フィールドに貼り付けます。

相互認証要求の処理

証明書の交換



- クライアントが認証のためにサーバー証明書を要求すると、証明書署名要求 (CSR) が生成されます。
- CSR に応答するために、サーバーは 2 つの一意の暗号化キー：サーバーへのメッセージを暗号化するために使用される公開鍵とメッセージを復号化するために使用される秘密鍵を生成します。両方のキーがキーストアに保持されます。
- キーを使用して、クライアントの安全なメッセージを復号化し、サーバーで読み取りができるようにします。HTTPS になるすべての送信接続は、キーストアを確認してその公開認定を提供することで、認定を検証し、トラストストア証明書を使用して相互の信頼性を検証します。
- クライアントとサーバーとの間で安全なリンクを確立するために、サーバーは証明書を対応する秘密鍵と照合します。サーバーのみが秘密鍵にアクセスできるため、サーバーはクライアントからのデータを復号化できます。

ポート 443 で `com.glide.certificates.DBKeyStoreSocketFactory` ソケットファクトリを使用して MYHTTPS を登録するコマンドの例を次に示します。データベースキーストアファクトリは、SSL 交換プロセス中に相互認証用のクライアント証明書を提供するために使用されます。

```
glide.httpclient.protocol.myhttps.class = "com.glide.certificates.DBKeyStoreSocketFactory"
glide.httpclient.protocol.myhttps.port = "443"
```

上記の設定は、SSL 中にカスタムソケットファクトリを使用して証明書を交換するための送信 myhttps://host.domain.com/target URL に影響します。

注:
デフォルトの HTTPS プロトコルソケットファクトリを上書きすると、すべての送信 HTTPS 接続に影響します。通常、これは望ましくありません。

サーバーは証明書を送信して応答します。これがクライアントが受け入れる証明書ですか？そうである場合、証明書を受け入れるメッセージがサーバーに送信され、安全なチャネルが開始されます。証明書が承認されない場合は、認定にルート権限が必要であることを意味します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

参照：**WS-Security**

WSS X.509 トークンプロファイルおよび WSS ユーザー名トークンプロファイルの形式での WS-Security 1.1 は、受信 SOAP 要求でサポートされます。

WS-Security を使用する構成は、基本認証を強制する要件とは別であり、SOAP エンベロープに WS-Security ヘッダーが含まれている場合に適用されます。

WS セキュリティプロファイル

WS セキュリティプロファイルモジュールには、現在有効な WS-Security プロファイルがリストされます。プロファイルの順序は、受信 SOAP 要求中にすべてのプロファイルがチェックされる認証の順序を示します。プロファイルが認証に失敗すると、次の順番のプロファイルは実行されません。[セッションのバインド] チェックボックスは、セッションの ID を引き継ぐために使用するプロファイルを示します。「バインドされた」セッションは 1 つしか存在できません。

WSS X.509 トークンプロファイル

Web Services Security: SOAP Message Security specification (Web サービス セキュリティ：SOAPメッセージセキュリティ仕様) で定義されている通りに X.509 認証フレームワークを使用します。X.509 証明書は、公開鍵と、(少なくとも) 件名、発行者名、シリアル番号、および有効期間を含む一連の属性とのバインディングを指定します。X.509 証明書は、着信 SOAP メッセージを知らせるために使用される公開鍵を検証するために使用されます。証明書モジュールの証明書をアップロードして、**[X509** 証明書] フィールドで参照します。これがバインドされたセッションの場合は、WS-Security 認証が成功したときになりすますユーザーを選択します。

http://www.oasis-open.org/committees/download.php/16785/wss-v1.1-spec-os-x509TokenProfile.pdf のドキュメントを参照してください。

WSS ユーザー名トークンプロファイル

X.509 トークンプロファイルを指定するのに加えて、SOAP 要求ではユーザー名トークンも指定できます。ユーザー名トークンは、「ユーザー名」で要求者を識別する手段として使用され、オプションでパスワード (または共有秘密キー、またはパスワードと同等のもの) を使用して、その ID をインスタンスに対して証明します。ユーザー名トークンプロファイルは、現在は X.509 トークンプロファイルから独立して使用することはできません。

1. 受信 SOAP 要求のユーザー名を使用して、**UserName** 値に一致する指定されたユーザーフィールドでユーザーを検索します。受信ユーザー名トークンのパスワード値は、要求を認証するために使用されます。[バインドセッション] オプションを選択すると、認証に成功したユーザーがセッションに使用されます。
2. ユーザーテーブル内のユーザーとは無関係な別のユーザー名/パスワードのペアを使用して認証します。バインドセッションオプションが選択されている場合、[ユーザーとして実行] フィールドで指定されているユーザーがセッションに使用されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

WS-Security SOAP エンベロープヘッダーの例

注:

このサンプルは、フレームに収まるように改行を使用してフォーマットされています。

```
<SOAP-ENV:Header><wsse:Securityxmlns:wsse =
 "http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd"
SOAP-ENV:mustUnderstand = "1" ><wsse:BinarySecurityTokenxmlns:wsu =
 "http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd"E
ncodingType =
 "http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0
#Base64Binary"ValueType =
 "http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0#X50
9v3"wsu:Id = "CertId-2D914AB929A6719E7F13068829874641"xmlns:wsse =
 "http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd"
 >
  MIIEgzCCA2ugAwIBAgILAQAAAAABLOZQMtEwDQYJKoZIhvcNAQ
  EFBQAwQDEXMBUGA1UEChMOQ3liZXJ0cnVzdCBJbmMxJTAjBg
  NVBAMTHEN5YmVydHJ1c3QgU3VyZWNyZWRlbnRpYWwgQ0Ew
  HhcNMTAxMjE0MTgyMjU1WhcNMTECMjE0MTgyMjU1WjB3MQsw
  CQYDVQQGEwJVUzEUMBIGA1UEChMLU2VydmljZS1Ob3cxKDA
  mBgkqhkiG9w0BCQEWGWRhdmlkLmxvb0BzZXJ2aWNlLW5vdy5jb
  20xKDAmBgNVBAMTH1NlcnZpY2UtTm93IFBhcn3uZXIgRGV2ZWx
  vcG1lbnQwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIB
  AQCvtcRIb6zkGnN9uyhtcSDNSIuCW6FgnTbTDUvw2nGlNA9y9iEV
  wTp5TG3eELOOFBCuRLeY5x28lN+cJ72v+zCwi/rZcbEPj8oWyLVA
  OqJThgrzhDabj0vDM/zU8bvAXcw6FoCUDFKkc64WC7Y4HpBdfW4
  JT7FBgDQ3LEudq80Up+TfETiGwrEA3jRgy9fF92TKD7MN3Vkyhz2
  xZLOFiN5HJixl9juNJmLWugqqIG04yZSuCutc1gjCy0U+f0NXKgh0Q
  rRheNpwcqWbbJvLbR9Ybso6l3UAYCQ09hrRnI7VaPvfiueUvuLopap
  o4Kel6iL8aMUAfEUDtkf1AbqRIIQ5AgMBAAGjggFFMIIBQTAfBgNVH
  SMEGDAWgBRJTJILzUojts557p5VM2taRMACITA7BgNVHR8ENDA
  yMDCgLqAshipodHRwOi8vY3JsLm9tbmlyb290LmNvbS9TdXJlQ3JlZ
  GVudGlhbC5jcmwwHQYDVR0OBBYEFB+OqlvcdiYmq0enW6mgaV
  wZp9eaMA8GA1UdEwEB/wQFMAMCAQAwDgYDVR0PAQH/BAQD
  AgTwMBEGCWCGSAGG+EIBAQQEAwIFoDBJBg3rBgEFBQcBA1Q
  9MDswOQYIKwYBBQUHMAKGLWh0dHA6Ly9jYWNlcnQub21uaXJv
  b3QuY29tL3N1cmVjcmVkZW50aWFsLmNydDAkBgNVHREEHTAbg
  RlkYXZpZC5sb29Ac2VydmljZS1ub3cuY29tMB0GA1UdJQQWMBQG
  CCsGAQUFBwMCBggrBgEFBQcDBDANBgkqhkiG9w0BAQUFAAO
  CAQEAmeoP0Bgtx2JN1ldLnnK6WLEqDk25zaHP5wTxqVlFxzJy1zi6
  A0lk5U0T5LKYjjGWRIOoSeK8iBU0p7Mq4PE8QCETkjYNyuWJd9zm
  7GPCHdOoL18rQHQRsU8pTDHA10zG+i3zdxAMrHI/H673E4myzvU
  DkJnxNAZdw4h4Ba/Y1+VFCWhOm2GwZdXtzklyZaKtMp+31qmf3bG
  OSU34M/dW40pXgfLDqdGD+6YDQPg25aYeCqcNhwg6VlAWG566g
  aWXYxRaVj0qotSDMdaK8b+7Vlo7KhGGaE62v7f44OSekJeBvTfZCR
  7zRSK8N+0qUpqP/n8vgDkmYIE5IQrRE0rEWA==
 </wsse:BinarySecurityToken><ds:Signature xmlns:ds =
"http://www.w3.org/2000/09/xmldsig#"Id = "Signature-2" ><ds:SignedInfo xmlns:ds
= "http://www.w3.org/2000/09/xmldsig#" ><ds:CanonicalizationMethodAlgorithm
= "http://www.w3.org/2001/10/xml-exc-c14n#" xmlns:ds =
"http://www.w3.org/2000/09/xmldsig#" /><ds:SignatureMethod
Algorithm = "http://www.w3.org/2000/09/xmldsig#rsa-sha1"xmlns:ds =
"http://www.w3.org/2000/09/xmldsig#" /><ds:Reference URI = "#Timestamp-1"
xmlns:ds = "http://www.w3.org/2000/09/xmldsig#" ><ds:Transforms
xmlns:ds = "http://www.w3.org/2000/09/xmldsig#" ><ds:Transform
 Algorithm = "http://www.w3.org/2001/10/xml-exc-c14n#"xmlns:ds =
 "http://www.w3.org/2000/09/xmldsig#" /></ds:Transforms><ds:DigestMethod
 Algorithm = "http://www.w3.org/2000/09/xmldsig#sha1"xmlns:ds
```

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは、米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商標です。
その他の会社名と 製品名は、関連する各会社の商標である可能性があります。

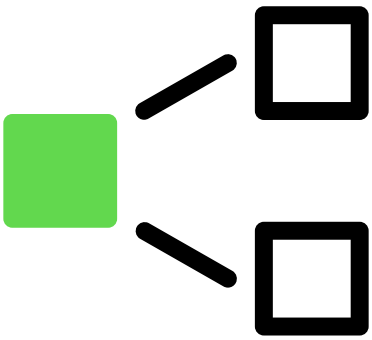
一般的なプラットフォームのセキュリティ設定

一般的なプラットフォームのセキュリティ設定について詳細を確認します。

ウイルス対策スキャン機能

インシデント、問題、ストーリーなどのシステムレコードへの添付ファイルによって持ち込まれる可能性のあるウイルス感染からインスタンスを保護するために使用します アンチウイルススキャン 。

HTML Sanitizer

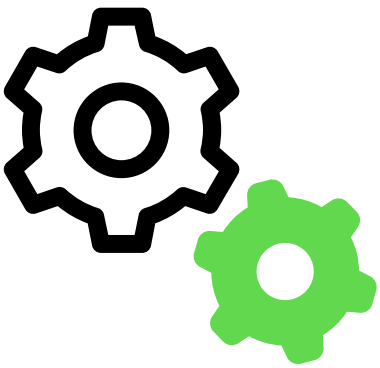


HTML フィールドと翻訳された HTML フィールドの HTML マークアップをサニタイズして不要なコードを削除し、クロスサイトスクリプト攻撃などのセキュリティ上の懸念から保護します。

監査

監査が有効にされたテーブルのレコードの変更を追跡します。デフォルトでは、インシデントテーブル、変更テーブル、および問題テーブルなどに対して行われた変更が追跡されます。

高セキュリティ設定



高セキュリティ設定とは、インスタンスで利用可能な複数のセキュリティオプションを指します。

ServiceNow® アクセス制御

SNC Access Control プラグインでは、どのカスタマーサービス & サポート従業員がインスタンスにいつアクセスできるかを制御できます。

仮想プライベートネットワーク (VPN)

仮想プライベートネットワーク (VPN) を使用して、インターネット経由でインスタンスを外部データソースと統合します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

その他の設定とセキュリティリソース Instance Security Center の外部でセキュリティプロパティを設定します。また、その他のセキュリティ関連のリソースについても説明します。		

アンチウイルススキャン

アンチウイルススキャン を使用すると、インシデント、問題、ストーリーなど、システムレコードに添付ファイルによって持ち込まれるウイルス感染からインスタンスを保護できます。

HTML サニタイザー

HTML フィールドと翻訳された HTML フィールドの HTML マークアップをサニタイズして不要なコードを削除し、クロスサイトスクリプト攻撃などのセキュリティ上の懸念から保護します。

監査

監査が有効にされたテーブルのレコードの変更を追跡します。デフォルトでは、インシデントテーブル、変更テーブル、および問題テーブルなどに対して行われた変更が追跡されます。

高セキュリティ設定

高セキュリティ設定とは、インスタンスで利用可能な複数のセキュリティオプションを指します。

ServiceNow® アクセス制御

SNC Access Control プラグインでは、どのカスタマーサービス & サポート従業員がインスタンスにいつアクセスできるかを制御できます。

その他の設定とセキュリティリソース

Instance Security Center の外部でセキュリティプロパティを設定します。また、その他のセキュリティ関連のリソースについても説明します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

仮想プライベートネットワーク (VPN)

仮想プライベートネットワーク (VPN) を使用して、インターネット経由でインスタンスを外部データソースと統合します。

アンチウイルススキャン

アンチウイルススキャン を使用すると、インシデント、問題、ストーリーなど、システムレコードに添付ファイルによって持ち込まれるウイルス感染からインスタンスを保護できます。

ウイルス対策スキャンの詳細

ウイルス対策スキャンの価値を学びます。

ウイルス対策保護を構成する

ウイルス対策保護の構成方法を理解します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

感染したファイルの解決

感染したファイルの処理方法を学びます。

Antivirus Scanning の参照

Antivirus Scanning の辞書属性に関する情報にアクセスします。

自動翻訳

Antivirus Scanning の詳細

アンチウイルススキャン を使用すると、インシデント、問題、ストーリーなど、システムレコードに添付ファイルによって持ち込まれるウイルス感染からインスタンスを保護できます。

アンチウイルススキャン は添付ファイル [sys_attachment] テーブルに保存されている添付ファイルをスキャンして、ユーザーが感染したファイルをアップロードおよびダウンロードするのを防ぎます。プラットフォームでサポートされているすべてのドキュメントタイプが、Antivirus Scanning でスキャンされます。

ウイルス対策保護 プラグイン (com.glide.snap) は、インスタンスでデフォルトでアクティブ化されています。管理者は、スイッチを切り替えることで、インスタンス全体で アンチウイルススキャン 機能を非アクティブ化および再アクティブ化し、構成オプションを設定して、インスタンスのウイルス対策アクティビティを確認することができます。

注:

- アンチウイルススキャン は、政府機関向けコミュニティクラウド (GCC) および商用環境の顧客も利用できます。機能の使用を開始するには、(com.glide.snap.fed_enable_scan) プロパティを True に設定する必要があります。
- HTTP および HTTPS 通信プロトコルがサポートされています。
- Edge で暗号化されたファイルはこのスキャンから除外されます。
- アンチウイルス定義は毎日更新されます。
- ファイルサイズが 100 MB を超えるファイルはスキャンされません。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

メールと添付ファイルのスキャン

受信メールは、 ではなく、アンチウイルススキャンシステムのメール フィルター によってウイルス スキャンが行われます。

画像を除く、zz_yyテーブルに添付されているすべての添付ファイルがスキャンされます。画像添付ファイルの場合は、SVG 画像のみがスキャンされます。JPG、JPEG、PNG などの他の画像タイプの場合は、プロパティに必要な *com.glide.snap.zz_yy.image_scan_extensions* 拡張子を設定します。

スキャンシナリオ

これらのアップロードおよびダウンロードのシナリオを確認し、システムがレコードに添付されたファイルから潜在的なセキュリティ上の脅威を識別する方法を理解してください。

シナリオ 1 - ファイルのアップロード

1. ユーザーは感染したファイルを知らないうちにレコードにアップロードします。
2. システムはファイルをスキャンして隔離します。
3. ファイルは [添付ファイル] ウィンドウに表示され、 利用不可としてマークされます 。
4. ユーザーがファイルを選択すると、「Infected_testing.txt ファイルはセキュリティ スキャンに合格しませんでした」というエラーメッセージが表示されます。レコード INC0000059 からファイルを削除して、再試行してください。
5. ユーザーとウイルス対策管理者にメール通知が送信されます。
6. ユーザーが [添付ファイル] ウィンドウを閉じてレコードに戻ります。感染 ファイルは 利用不可としてヘッダーに表示されます。例：infected_testing123.txtZ [unavailable]

シナリオ 2 -ファイルのダウンロード

1. ユーザーはレコードを開き、添付されているファイルをダウンロードします。
2. ファイルが感染していることに気付かず、ユーザーはそのファイルを選択してダウンロードします。
3. システムはファイルをスキャンして、隔離状態に移し、次のようなメッセージを表示します。ファイル infected_testing123.txt はセキュリティスキャンをパスしていないため、ダウンロードすることはできません
4. ユーザーがメッセージを閉じると、画面が更新され、ファイルを使用できないことが表示されます。
5. ユーザーとウイルス対策管理者にメール通知が送信されます。

シナリオ 3 - ZIP ファイルのダウンロード

1. ユーザーがレコードを開き、添付されている ZIP ファイルをダウンロードします。
2. システムは ZIP ファイルを個別にスキャンします。
3. 1 つのファイルが セキュリティスキャンに合格せず 、利用不可としてマークされます。残りのファイルは圧縮され、正常にダウンロードされます。
4. ユーザーが ZIP ファイルを開くと、正常にダウンロードされたファイルに加えて「error.txt」ファイルが表示されます。このファイルには、スキャンに合格しなかっ

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

たために ZIP に含まれなかったファイルを示すエラーメッセージが含まれています。

5. ユーザーがレコードを再度開くと、使用できないファイルが [添付ファイル] ウィンドウの [潜在的なセキュリティリスク] セクションに移動され、 ダウンロードできない ことがわかります。

アンチウイルススキャン の構成

インスタンス全体およびテーブルレベルで アンチウイルススキャン を構成します。

始める前に
必要な役割：antivirus_admin または admin

このタスクについて
アンチウイルススキャン はインスタンスでデフォルトで有効になっており、添付ファイルを自動的にスキャンして、ウイルスに感染しているファイルを特定します。インスタンス全体でスキャンが有効になっていることを確認し、スキャンから除外するテーブルを特定して、機能を設定します。

手順

1. 移動先 すべて > ウィルス対策 > 構成.
2. 機能を設定するときは、次の点を考慮してください。

3. [保存] を選択します。
4. 除外されたテーブルのリストに除外するテーブルを追加して、ウイルス対策スキャンからテーブルを除外します。
   a. [システム定義] → [ディクショナリー] に移動します。
   b. スキャンから除外するテーブルを検索し、[タイプ] が [コレクション] に設定されているテーブルを選択します。
   c. [属性] タブで、[新規] を選択します。
   d. [属性] フィールドに Exclude_from_antivirus_scan を追加し、[値] フィールドに「True」と入力します。
   e. [送信] を選択します。

タスクの結果
アンチウイルススキャン がインスタンスで有効になっており、[ウイルス対策構成] ページの [除外されたテーブル] のリストに、スキャンから除外したすべてのテーブルが入力されています。

隔離されたファイルの確認

隔離された添付ファイルを確認し、必要に応じてさらにアクションを実行します。

始める前に
必要な役割：antivirus_admin または admin

このタスクについて
[ウイルス対策隔離] ページで隔離されたファイルのエントリを定期的に監視して、次のいずれかのアクションを実行します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. 移動先 すべて > ウィルス対策 > 隔離.
2. 使用可能なアクションを実行する、隔離された各エントリの横にあるチェックボックスをオンにします。
3. バナーの [選択した行でアクションを実行] ドロップダウンを選択して、選択した行の隔離されたエントリに実行するアクションを選択します。

タスクの結果
確認が求められ、入力に応じて選択されたアクションを実行します。

関連情報

Instance Security Center

ウイルス対策測定基準

ウイルス対策アクティビティの確認

感染した可能性があるファイルに対して発生したすべてのアクティビティを、検出されて隔離された時点から追跡する、ウイルス対策アクティビティログを確認します。

始める前に
必要な役割：antivirus_admin または admin

このタスクについて
このログは、検出、削除、その他の隔離されたファイルイベントなどのウイルス対策アクティビティをキャプチャするレポートとして機能します。

手順

1. 移動先 すべて > ウィルス対策 > アクティビティ.
2. 隔離されたファイルのログを確認します。
   隔離された各ファイルに対して実行されたアクションを [イベント] 列に表示できます。

次のタスク
削除、復元、ダウンロード、またはログに保持するレコードを決定します。「隔離されたファイルの確認」を参照してください。

アンチウイルススキャン の辞書属性について

辞書属性は、辞書レコードが記述するテーブルまたは要素の動作を変更します。管理者は、辞書属性の値を設定して、デフォルトの Antivirus Scanning 設定の動作を変更できます。

アンチウイルススキャン の辞書属性

名前	値	ターゲット要素	説明
Exclude_from_antivirus_scan	True/False	任意のテーブル	true の場合、テーブルの添付ファイルはウイルス対策スキャンから除外されます。「アンチウイルススキャン の構成」を参照してください。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

アンチウイルススキャン の辞書属性 (続く)

名前	値	ターゲット要素	説明
Supress_antivirus_email_notification	True/False	任意のテーブル	true の場合、感染した可能性があるファイルが特定されると、プラットフォームで生成されたメール通知の送信を停止します。
Suppress_antivirus_ui_notification	True/False	任意のテーブル	true の場合、感染した可能性のあるファイルが特定されると、プラットフォームで生成された UI 通知を停止します。

関連情報

辞書属性

監査

監査が有効にされたテーブルのレコードの変更を追跡します。デフォルトでは、インシデントテーブル、変更テーブル、および問題テーブルなどに対して行われた変更が追跡されます。

探索

監査の機能とビジネス価値について説明します。

構成

監査の構成方法について説明します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ビュー	参照
システム監査テーブルおよびリレーションシップ変更の監査テーブルを確認します。	履歴セットに関する情報にアクセスします。

自動翻訳

監査の詳細

監査が有効にされたテーブルのレコードの変更を追跡します。デフォルトでは、インシデントテーブル、変更テーブル、および問題テーブルなどに対して行われた変更が追跡されます。

監査を有効にすると、テーブル内のすべてのレコードの作成、更新、および削除が追跡されます。テーブル内の個々のフィールドを監査する場合は、辞書属性を使用して追跡しないフィールドを非表示にすることができます。

監査情報は次のテーブルに保持されます。

- 監査テーブル
- 履歴セットについて テーブル。

警告:
ワークフローコンテキスト [wf_context] や Event Management アラート [em_alert] などの大量のトラフィックを受信するシステムテーブルの監査では、パフォーマンスに影響を与える可能性があります。そのため、em_alert テーブル全体を監査することはできません。代わりに、次の方法で選択した対象フィールドを監査します。em_alert テーブルと選択したフィールドの両方で `audit=true` を設定します。監査するフィールドはできる限り少なくしてください。

親テーブルと子テーブルの監査

テーブルは、親または子の監査対象テーブルから監査フラグを取得しません。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- たとえば、構成アイテム [cmdb_ci] テーブルの監査を有効にすると、そのベーステーブルに格納されている CI のみが監査されます。
- 同様に、コンピューター [cmdb_ci_computer] テーブルの監査を有効にすると、構成アイテム [cmdb_ci] テーブルから派生したコンピューター [cmdb_ci_computer] テーブルのフィールドを含む、コンピューターの CI レコードのみが監査されます。

監査システムテーブル

デフォルトでは、システムテーブルからのレコードの削除は監査されません。システムテーブルを監査するには、*glide.ui.audit_deleted_tables* プロパティリスト内のテーブルのリストにそのシステムテーブルを追加します。

フォームまたはリストからの削除の監査

デフォルトでは、フォームから個々のレコードの削除が監査されます。監査されないようにするには、テーブルの辞書属性 *no_audit_delete* を設定します。

テーブル辞書で監査が選択されており、テーブルが *glide.db.audit.ignore.delete* プロパティにリストされていない場合、リストからの削除が監査されます。

注:
デフォルトでは、この *glide.db.audit.ignore.delete* プロパティはシステムプロパティ [sys_properties] テーブルにありません。プロパティとその関連付けられた値を変更するには、まず手動で追加する必要があります。ただし、手動で追加すると、次のデフォルト値が上書きされます。

```
glide.db.audit.ignore.delete =
sys_mutex,sys_db_cache,sys_lucene_block,sys_lucene_file,sys_lucene_directory,sys_user_preference,sys_aud
cmdb_ci_windows_service, cmdb_sam_sw_install, cmdb_software_instance,
cmdb_sam_sw_usage, sam_sw_counter_detail
```

システムプロパティの追加の詳細については、「システムプロパティを追加する」を参照してください。

監査された情報

監査では次のレコードの変更を追跡します。

- 変更されたレコードの一意のレコード識別子 (sys_id)
- 変更されたフィールド
- 新しいフィールド値
- 以前のフィールド値
- このレコードとフィールドが更新された回数
- 変更された日時
- 変更を加えたユーザー
- 変更理由 (変更と関連する理由がある場合)
- レコードに複数のバージョンがある場合、レコードの内部チェックポイント ID。

監査から除外される情報

テーブルの監査を有効にしていても、一部の更新は監査されません。レコードの履歴には 132 件の更新が表示されますが、監査された更新が 7 件のみであるのはそのためです。

監査では、次の情報が除外されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- アップグレードによる更新。
- インポートセットによる更新。
- 親または子テーブルのレコード。
- no_audit 辞書属性を持つフィールド。
- *glide.ui.audit_deleted_tables* プロパティリストにリストされていないシステムテーブル。
- sys_class_name 列と sys_domain_id 列を除く sys_ prefix (システムフィールド) で始まるフィールド。
- UI ページは、監査ログを作成せずにレコードの更新をトリガーすることがあります。
- 滞留アクティビティモニターがレコードに接触したとき。これにより、有用なデータに干渉するノイズが生じて、インシデントに対してリストにされる何百もの更新が表示されなくなります。
- パフォーマンスアナリティクス スコアの手動変更。

テーブルの監査

テーブルの監査方法の手順については、「テーブルの監査の構成」を参照してください。

デフォルトでは、監査対象テーブルのすべてのフィールドが追跡されます。次の 2 つの方法のいずれかで、テーブル内のフィールドのサブセットを監査できます。

- テーブル全体の監査を有効にしてから、含めないフィールドを除外することができます。この方法は、すべてではないがほとんどのフィールドを監査する場合に適しており、除外リストと呼ばれます。詳細については、「フィールドの監査対象からの除外 (除外リスト)」を参照してください。
- 指定されたフィールドに対してのみ、テーブルの監査を有効にすることもできます。この方法は、少数のテーブルのフィールドのみ監査する場合に適しており、包含リストと呼ばれます。包含リストを使用してフィールドを含める方法の詳細については、「監査にテーブルフィールドを含める (包含リスト)」を参照してください。

キャンセル不可能な監査レコード

新しいデフォルト設定でトランザクションがキャンセルされたときに監査レコードが記録されない可能性を減らします。

ターゲットレコードの書き込み操作と同じトランザクションですぐにレコードを作成するように監査が設定されています。ターゲットレコードが削除されても、監査は **NCA** テスト監査削除 モジュールで作成および保持されます。

注:
拡張監査プロセスはデフォルトで有効になっています。glide.db.audit.lazy プロパティが True に設定されている場合、拡張監査プロセスは無効になります。

リリース前に Washington DC トランザクションがキャンセルされると、特定の監査可能な操作が記録されませんでした。これは、レコードの変更の間にプラットフォームが一部の操作を実行し、監査の作成前にキャンセルされるためです。ただし、レコードが変更された直後に監査が作成されるようになったため、監査が記録される前にキャンセルされたトランザクションによって操作が中止される可能性が低くなります。

監査は、トランザクションと同じスレッドに記録されるようになりました。以前の監査はバックグラウンドスレッドで作成されていました。この変更により、 glide.db.audit.lazy プロパティのデフォルト値が True から False に再定義されます。大部分のインスタンスが新しいデフォルト値と動作を使用し始めるため、このプロパティは通常 Properties テーブルでは定義されません。一部のインスタンスでは、このプロパティが既に存在し、True に設定されている可能性があり、これは、これらのインスタンスがこの変更を使用して動作を監査できないことを意味します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

注:
更新を利用するには、このプロパティを削除することをお勧めします。

テーブルの監査の構成

テーブルの監査を有効にして、テーブルのすべてまたは一部のフィールドの変更を追跡できます。

始める前に
必要なロール：admin

注:
暗号化されたフィールドは設計上、監査されません。この動作は設定できません。

手順

1. 移動先 すべて > システム定義 > ディクショナリ.
   辞書エントリのリストが表示されます。リストには、各テーブルの行と、テーブルの各列 (フィールド) の行が含まれます。
2. 辞書エントリのリストで、監査するテーブルに対応する列 (cmdb_ci_computer) を探します。
   正しいテーブル名、列名の空のエントリ、および コレクションの種類の行を探して、テーブルの列の行とテーブル自体の行を区別できます。
3. テーブルに対応する辞書エントリを選択します。
   辞書エントリのフォームが表示されます。
4. [監査] チェックボックスをオンにします。
5. [更新] を選択します。

次のタスク
テーブル内のいくつかのフィールドのみを監査する場合、テーブルの包含リスト監査の有効化。ほとんどのフィールドを監査して、一部のフィールドを除外する場合、「フィールドの監査対象からの除外 (除外リスト)」を参照してください。

テーブルの包含リスト監査の有効化

明示的に指定したフィールドのみをテーブルで監査できるようにします。これは、監査対象テーブル内の少数のフィールドのみを監査する場合に便利です。

始める前に
必要なロール：管理者
テーブルで監査を有効にする必要があります。

手順

1. 移動先 すべて > システム定義 > ディクショナリ.
   辞書エントリのリストが表示されます。リストには、各テーブルの行と、テーブルの各列 (フィールド) の行が含まれます。
2. 必要に応じて、リストビューをカスタマイズして、属性の列を表示します。
3. 辞書エントリのリストで、監査するテーブルに対応する列 (cmdb_ci_computer) を探します。
   正しいテーブル名、列名の空のエントリ、および *collection* の種類の行を探して、テーブルの列の行とテーブル自体の行を区別できます。
4. 該当する行の [属性] フィールドに「*audit_type=whitelist*」と入力します。

次のタスク
テーブルのどのフィールドを監査するか指定します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールドの監査対象からの除外 (除外リスト)

これらのフィールドを監査から除外することで、Now Platform が監査対象テーブルのフィールドのサブセットを追跡しないようにすることができます。

始める前に

必要なロール：管理者
テーブル内のフィールドを監査から除外するには、まずそのテーブルの監査を有効にする必要があります。

このタスクについて

監査可能なテーブルのほとんどのフィールドを監査する場合は、一連のフィールドを除外リストに追加します。いくつかのフィールドのみを監査する場合は、代わりに包含リストの手順に従います。

> **注:**
> ジャーナルベースのフィールドの監査を無効にすると、アクティビティフォーマッターなどの機能に影響を与える可能性があります。詳細については、「KB0743142」を参照してください。

手順

1. 移動先 すべて > システム定義 > ディクショナリ.
2. 必要に応じて、リストビューをカスタマイズして、属性の列を表示します。
3. 監査から除外するテーブルとフィールド (列) に対応する行に移動します。
4. その行の属性の列で、「`no_audit`」と入力します。

監査にテーブルフィールドを含める (包含リスト)

監査対象テーブルのフィールドのサブセットを追跡するには、それらのフィールドを包含リストに追加します。

始める前に

必要なロール：管理者
テーブルのフィールドを包含リストに追加するには、まずそのテーブルの監査を有効にし、そのテーブルに対して包含リストの監査を有効にする必要があります。

このタスクについて

監査対象テーブルの少数のフィールドのみを監査する場合は、一連のフィールドを包含リストに追加します。ほとんどのフィールドを監査し、少数のフィールドのみ除外する必要がある場合は、代わりに、除外リストの手順に従います。

手順

1. 移動先 すべて > システム定義 > ディクショナリ.
2. 必要に応じて、含めるリストビューをカスタマイズして、属性の列を表示します。
3. 包含リストに追加するテーブルとフィールド (列) に移動します。
4. [属性] フィールドに「*`audit=true`*」と入力します。

システムテーブルの監査を有効にする

sys_ prefix があるテーブルからの削除は、デフォルトでは監査されません。これらのテーブルからの削除を追跡するには、テーブル名を *`glide.ui.audit_deleted_tables`* プロパティに追加します。削除済みレコードの復元プラグインを有効にすると、このプロパティにいくつかのデフォルト値が追加されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

始める前に
必要なロール：管理者

手順

1. 移動先 すべて > システムプロパティ > **UI** プロパティ.
2. 削除の監査プロパティを持つシステムテーブルのリスト (「sys_」で始まる、カンマ区切り) を見つけます。
3. テーブル名を追加または削除します。テーブル名は、スペースを入れずにカンマで区切る必要があります。
4. [保存] をクリックします。

> **注:**
> 監査の詳細については、「sys 監査テーブルの理解」を参照してください。

システム監査テーブルおよびリレーションシップ変更の監査テーブルの表示

Now Platform は、システム監査 (sys_audit) テーブルとリレーションシップ変更の監査 (sys_audit_relation) テーブルの挿入と更新を追跡します。

Now Platform は監査テーブルを追跡します。テーブルを追跡するには、ディクショナリーレコードの [監査] チェックボックスをオンにして、値を true に設定します。デフォルトでは、更新セットテーブルなどのシステムテーブルのレコードは監査されません。

> **注:**
> パフォーマンスの問題や無限ループを防ぐために、システム監査テーブルへ挿入することでトリガーされるビジネスルールやワークフローはスキップされます。

システム監査テーブルの列

sys_audit テーブルレコードに次の列が表示されます。

フィールド	説明
テーブル名	監査レコードの対象となるテーブル (「incident」など)
フィールド名	監査レコードの対象となるテーブルの列 (「assigned_to」など)
ドキュメントキー	監査レコードに関連付けられている元のレコードの Sys_id (一意のレコード識別子)。
ユーザー	変更を作成したユーザーの名前。 **注:** 一部の自動プロセスでは、システムまたはゲストユーザーを使用して、レコードへの変更を適用および追跡します。詳細については、「システムユーザーとゲストユーザー」を参照してください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
以前の値	この sys_audit レコードで表されるフィールド変更の以前の値。 • 参照フィールド：変更されたレコードの一意の sys_id 値。 • 日付/時刻のフィールド：データベースに格納されている協定世界時 (UTC) の値。
新しい値	この sys_audit レコードで表されるフィールド変更の新しい値。 • 参照フィールド：変更されたレコードの一意の sys_id 値。 • 日付/時刻のフィールド：データベースに格納されている協定世界時 (UTC) の値。

リレーションシップ変更の監査 (sys_audit_relation) テーブルの仕組み

システム監査 [sys_audit] テーブルは、監査対象としてフラグが付けられたテーブルのアクティビティを追跡します。このアクティビティには、ジャーナルフィールドエントリと履歴セットが含まれます。リレーションシップ変更の監査 [sys_audit_relation] テーブルは、sys_audit テーブルレコードと監査されるレコードの作成元であるソーステーブルとの関係の変更を追跡します。また、レコードが削除された可能性がある場合も追跡します。

- テーブル内のレコードを監査するたびに、データを記録するストアに対して、さまざまな元のテーブル間の関係が作成されます。この関係性の情報は、sys_history_set、sys_history_line、および sys_journal テーブルに保存されます。
- 監査対象テーブルレコードに関連するフィールドを削除すると、sys_audit_relation テーブルに削除が記録されます。つまり、監査済みレコードを変更すると、まず過去の要素を削除してから、sys_audit_relation テーブルに新しいドキュメント ID が作成されます。

履歴セットについて

ユーザーがレコードを作成するか、その履歴を表示すると、必要に応じて監査テーブルから履歴セットレコードが自動的に生成されます。

レコードが監査対象テーブルにある場合、レコードが挿入されたとき、またはユーザーがレコードを表示したときに、その履歴セットが生成されます。

注:
履歴セットを使用してレポートを生成しないでください。

いくつかの情報のフィールドが履歴セットレコードにキャプチャされ、リストビューに表示されます。

リストビューレコードフィールド

フィールド	入力値
ID	履歴が記録されているレコードのドキュメント ID。
テーブル	履歴が記録されているレコードの監査対象テーブル。
ロード時間	履歴セットの生成に要した時間。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

監査履歴レコードフィールド

フィールド	入力値
ラベル	変更されたフィールドのラベル。
以前 (Old)	変更前の値。
新規	変更後の値。
タイプ	エントリが通常のフィールド用か、メールレコード用か、関係変更レコード用かを示します。
更新回数	このフィールドが変更された回数。-1 の値は、レコードが作成または削除された時点を示します。
更新時間	変更した日時。 **注:** 自動生成された履歴行の更新時間は、特定の処理状況でのレコードの作成時刻または更新時間と一致しません。レコードの履歴セットを初めて表示すると、履歴行のレコードの最初のセットが自動的に生成されます。アップグレードでのファイルの変更は監査されないため、この日付の不一致は次の場合に発生します。 • レコードに変更が加えられた後に履歴セットを表示した場合。 • ただし、将来のアップグレードで別の変更が行われる前。
ユーザー名	変更を作成したユーザーの名前。

自動翻訳

カレンダービューの履歴セット

履歴セットがアクティブになると、履歴コンテキストメニューの選択肢に、sys_audit テーブルからの情報ではなく、履歴セットの情報が入力されます。ユーザーの側から捉えた場合、同じ履歴データを同じユーザーインターフェイスで使用できますが、情報の保存方法は異なります。

履歴ビューにはカレンダービューが含まれていますが、通常のリストインターフェイスを使用して履歴レコードのフィルタリングと操作は行われないため、次の操作は可能になります。

- 履歴データの検索とフィルタリング
- 履歴データのエクスポート

履歴セットの表示

履歴セットを表示するには 2 つの方法があり、コンテキストメニューアクション履歴からアクセスできます。

監査セットと履歴セットの違い

監査 [sys_audit]、履歴セット [sys_history_set]、および履歴 [sys_history_line] テーブルは同じデータを格納しますが、目的やデータの管理方法は異なります。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

監査 [sys_audit] テーブル

監査 [sys_audit] テーブルには、すべてのレコードの履歴情報が格納されます。これらのレコードは、管理者が監査済みレコードの履歴を常に追跡できるように、永久に保持されるようになっています。監査レコードの数は時間の経過とともに増加するため、履歴情報について監査テーブルを直接クエリーするのは非効率的です。実際に履歴情報を表示する必要がある、より少量のサブセットレコードでのみクエリーを実行する方がはるかに効率的です。

履歴セット [sys_history_set] テーブル

履歴セット [sys_history_set] テーブルは、監査対象テーブルのどのレコードに履歴情報があるかを識別します。履歴 [sys_history_line] テーブルには、発生したフィールド値に加えた実際の変更が保存されます。

- ユーザーがレコードを作成するか、その履歴をリクエストすると、必要に応じて、監査テーブルから履歴セットと履歴レコードが自動的に生成されます。
- 履歴セットと履歴レコードには、システム内のすべての変更の完全な履歴ではなく、ユーザーが履歴情報の作成やリクエストを行った、レコードの履歴情報の最近のサブセットのみが含まれます。
- 監査データに加えて、履歴セットには、レコードの挿入中に設定された情報 (ジャーナルフィールドエントリなど) も含まれます。レコードの作成前に作成したジャーナルフィールドエントリは、レコード作成時に作成されたジャーナルエントリと同じ方法で処理されます。これらのジャーナルエントリは、関連レコード自体と同じ作成時刻と作成者のデータで履歴セットに表示されます。

履歴セットと履歴レコードは次のように制限されます。

- テーブルクリーナーを使用して、30 日間更新されていない履歴セットレコードを削除できます。
- テーブルローテーションを使用して、4 つの履歴テーブルを 7 日ごとにローテーションします。28 日以上経過した履歴レコードは削除されます。

後日、履歴情報が再度必要になった場合は、監査ソースレコードから再生成することができます。

履歴セットレコードが生成された後は、コンテキストメニューの [履歴] で監査レコードではなく履歴セットが使用されます。ユーザーの側から捉えた場合、同じ履歴データを同じユーザーインターフェイスで使用できますが、情報の保存方法は異なります。

自動翻訳

履歴へのアクセスを制御する

監査履歴を表示するためのアクセス権は、システムプロパティを設定することでロールに付与できます。

始める前に

必要なロール：管理者

手順

1. 移動先 すべて > システムプロパティ > システム.
2. テーブルから *glide.history.role* プロパティを選択します。
3. *List of roles (comma-separated) that can access the history of a record*で、履歴にアクセスするユーザーロールを選択します。
4. [保存] を選択します。

タスクの結果

読み取りアクセス権のないユーザーがレコードの履歴を表示する場合、フィールドへの変更は省略されます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

履歴エントリ数を変更する

デフォルトでは、履歴には最大 250 件の履歴エントリが表示されますが、この値を変更することができます。

始める前に

必要なロール：管理者

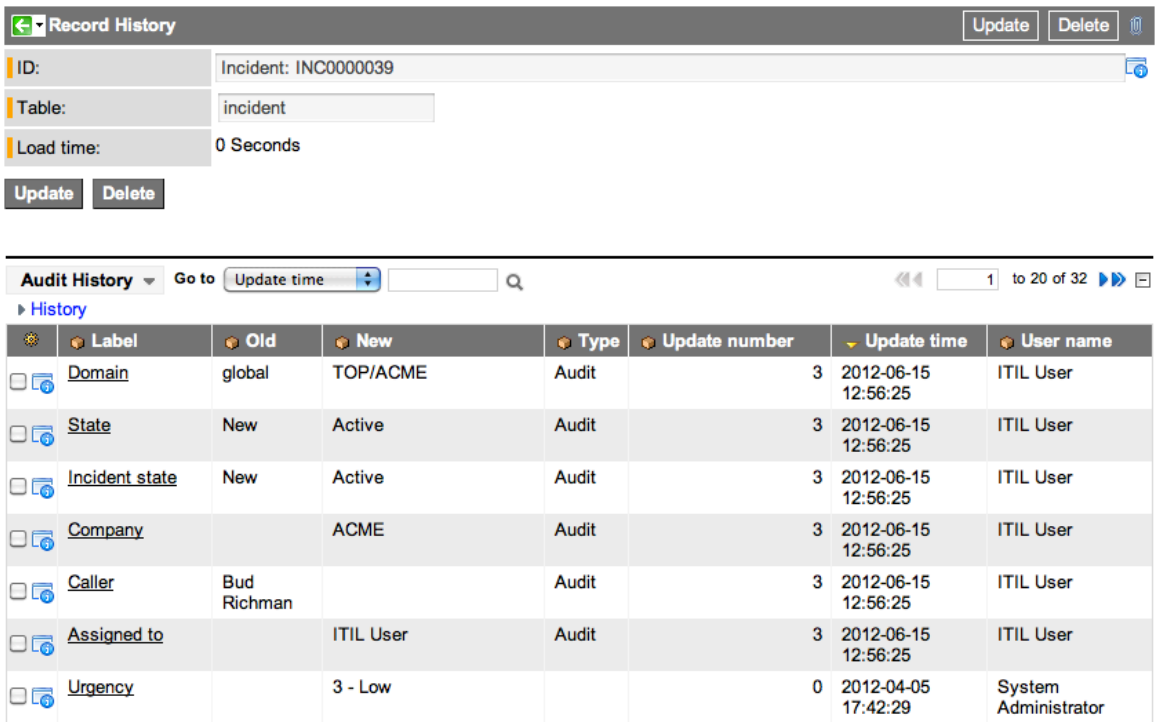
手順

1. 移動先 すべて > システムプロパティ > システム.
2. *glide.history.max_entries* プロパティを選択します。
3. *Maximum number of field entries displayed in record history, default is 250* 値を表示するエントリの新しい最大数を設定します。

履歴リスト

履歴リストには、各変更が変更リスト内の独自の行として表示されます。

履歴リストを表示する



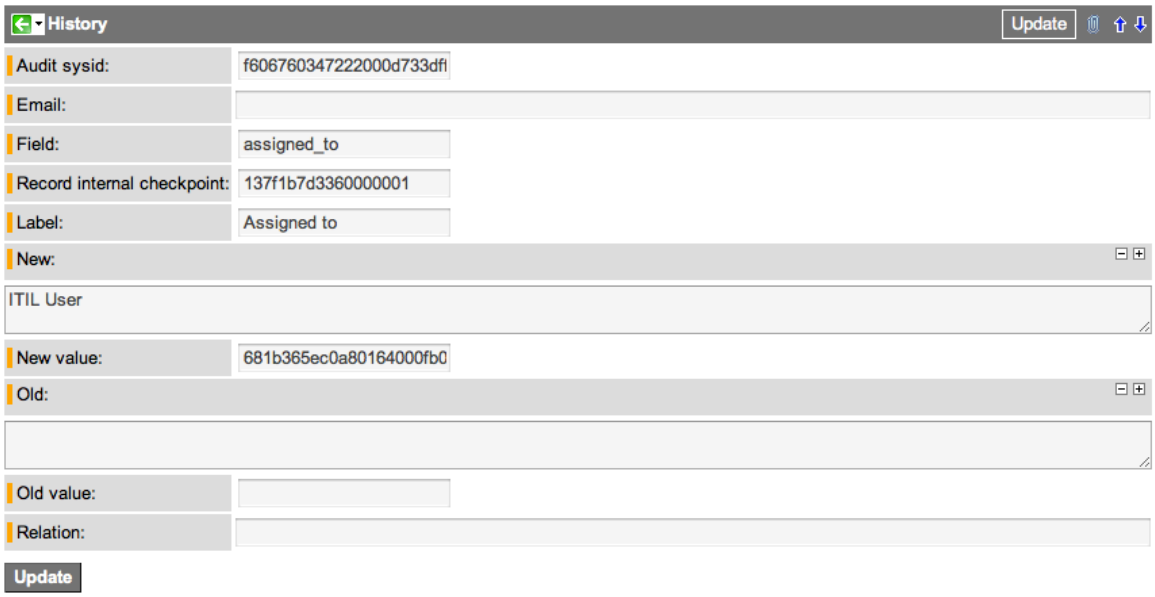
	Label	Old	New	Type	Update number	Update time	User name
	Domain	global	TOP/ACME	Audit	3	2012-06-15 12:56:25	ITIL User
	State	New	Active	Audit	3	2012-06-15 12:56:25	ITIL User
	Incident state	New	Active	Audit	3	2012-06-15 12:56:25	ITIL User
	Company		ACME	Audit	3	2012-06-15 12:56:25	ITIL User
	Caller	Bud Richman		Audit	3	2012-06-15 12:56:25	ITIL User
	Assigned to		ITIL User	Audit	3	2012-06-15 12:56:25	ITIL User
	Urgency		3 - Low		0	2012-04-05 17:42:29	System Administrator

行アイテムをクリックすると、変更に関する詳細が表示されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

リストの変更を表示する



要件

履歴リストを表示するには、次の要件を満たす必要があります。

監査

履歴リストを表示するには、テーブルの監査を有効にする必要があります。

ACL

デフォルトでは、管理者ユーザーロールのユーザーのみがリスト履歴オプションを使用できます。管理者以外のユーザーに対してこのオプションを有効にするには、カスタム ACL ルールを作成して、レコード履歴 [sys_history_set] テーブルへの読み取りアクセス権を付与します。

ロール

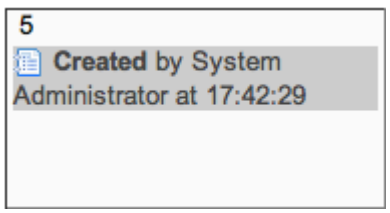
ユーザーが持つロールの少なくとも 1 つを *glide.history.role* プロパティに含める必要があります。このプロパティにはデフォルトで itil ロールが含まれます。

履歴カレンダー

履歴カレンダーには、レコードの変更日、変更者、および変更時間が表示されます。

履歴カレンダーは更新番号でソートされます。各ユーザーには色が割り当てられているため、特定のユーザーがレコードを変更した回数を一目で把握できます。例：

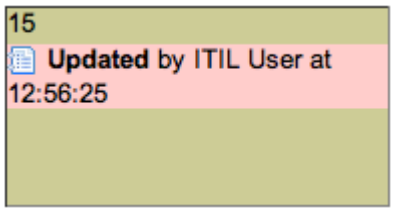
システム管理者が行った変更



自動翻訳

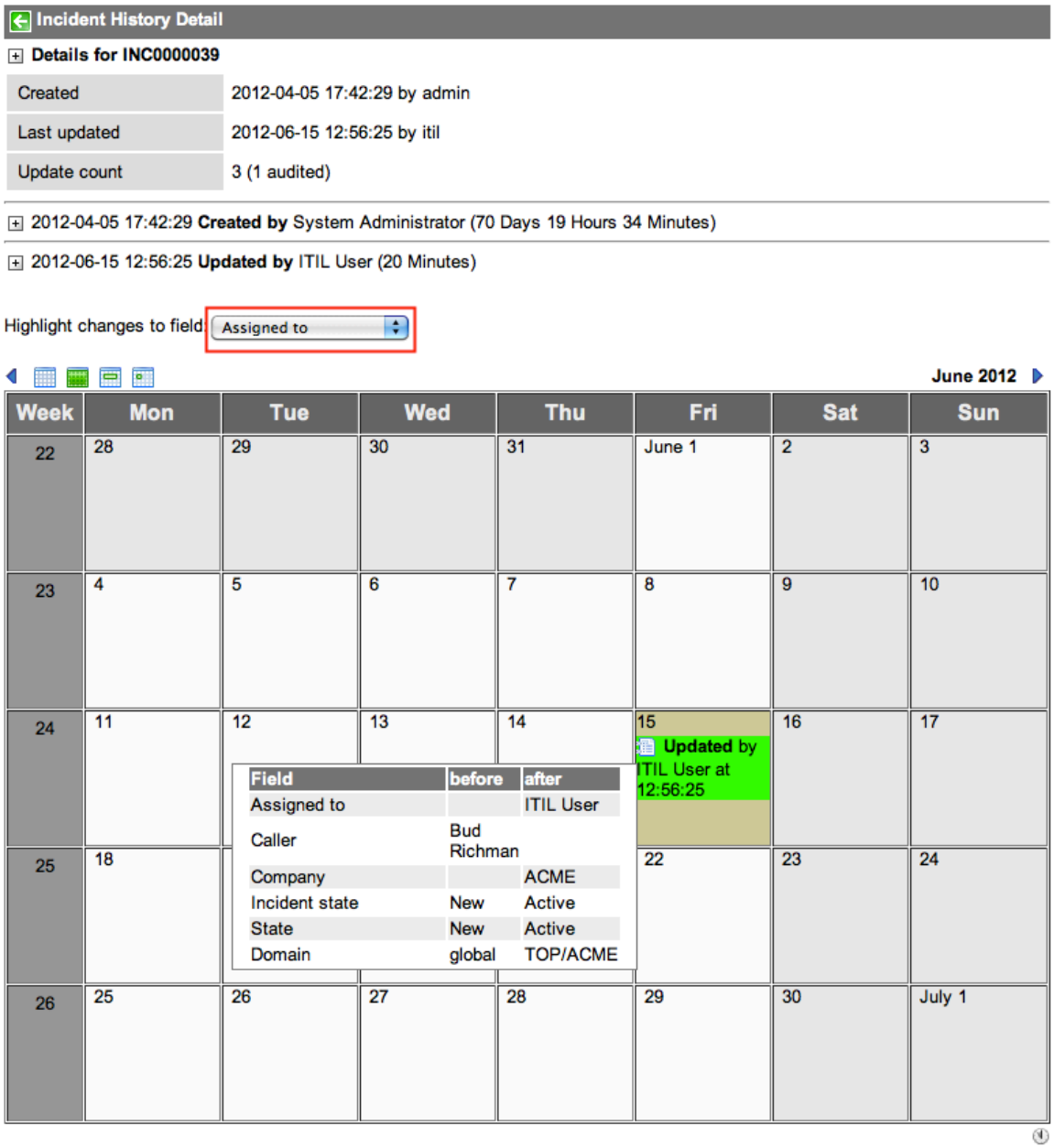
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ITIL ユーザーが行った変更



特定のフィールドの変更をハイライト表示するには、[フィールドへの変更をハイライト] 選択ボックスのフィールドを選択します。この選択ボックスのフィールドを選択すると、カレンダーが変更され、そのフィールドが変更された時間が強調表示されます。ハイライト表示された変更のいずれかのテキストにカーソルを合わせると、値の変更が表示されます。

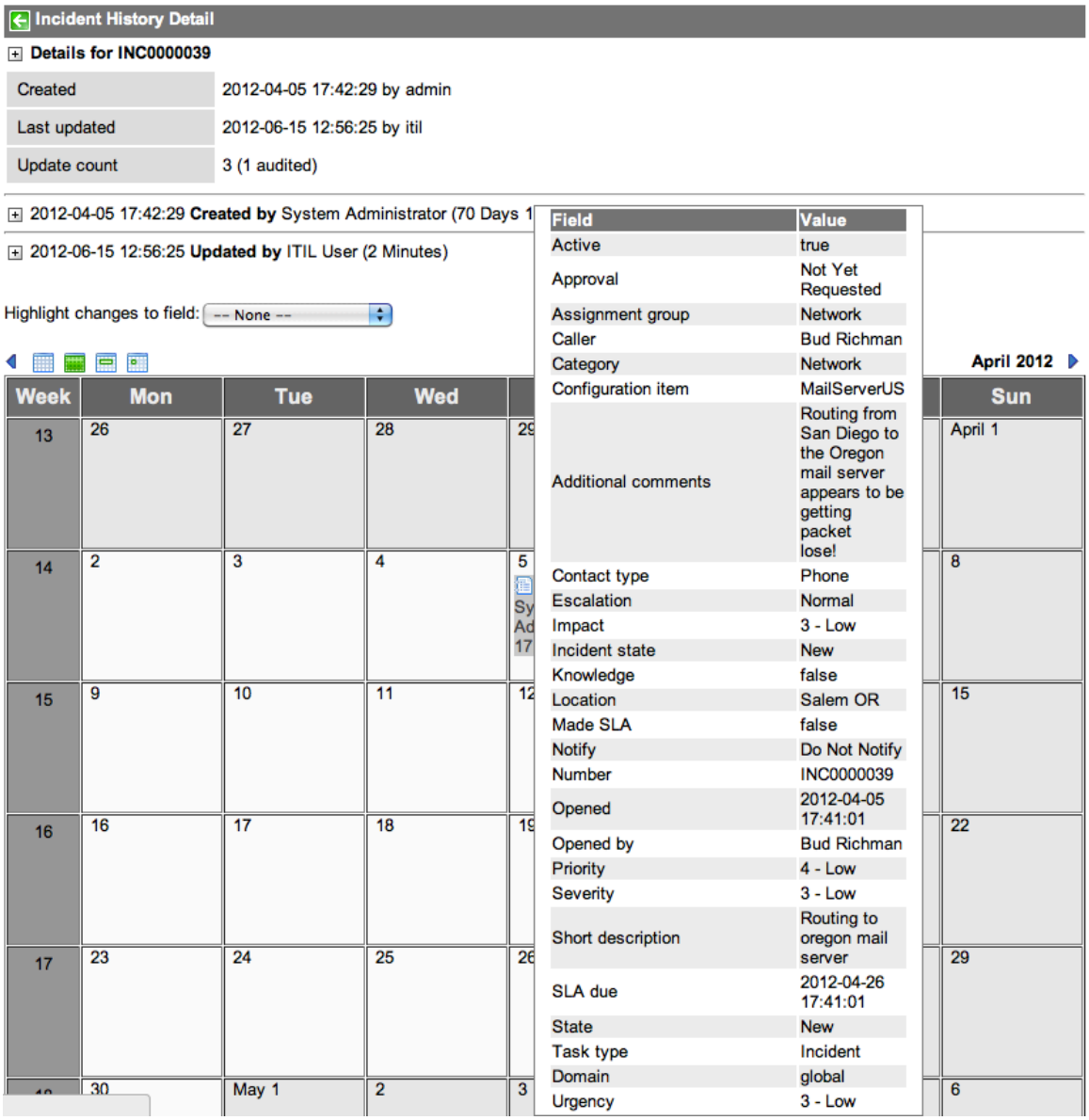
ハイライト表示された変更を表示する



エントリ内のアイコンにカーソルを合わせると、すべての値の変更がポップアップに表示されます。これは、フォームの上部に表示される情報と同じです。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

カレンダーの変更を表示する



日数をクリックすると、その日の変更が表示されます。左側の週番号をクリックして週次ビューを表示することもできます。月をスクロールして変更を確認できます。

履歴タイムライン

CI とその関連レコード、関係、ベースライン、および CI に対して提案された変更のタイムラインを表示できます。タイムラインは、構成アイテム [cmdb_ci] テーブルまたはこのテーブルの子孫 (テーブルの監査が有効になっている場合) の CI で使用できます。

必要なロール：このビューの ACL は、*glide.history.role* システムプロパティで定義されたロールに基づいており、デフォルトでは itil に設定されています。また、ユーザーは、デフォルトで管理者に付与されている履歴セット [sys_history_set] テーブルへの読み取りアクセス権も持っている必要があります。

CI の履歴を表示すると、タイムラインを開くことができます。タイムラインに表示される期間、時間範囲、およびプロパティを指定できます。特定の変更セットの変更内容を表示することも、CI 全体を表示して問題のトラブルシューティングを行うこともできます。CI の関連レコードに対する変更のタイムラインを表示し、任意の時点での CI のスナップショットをエクスポートして比較することもできます。

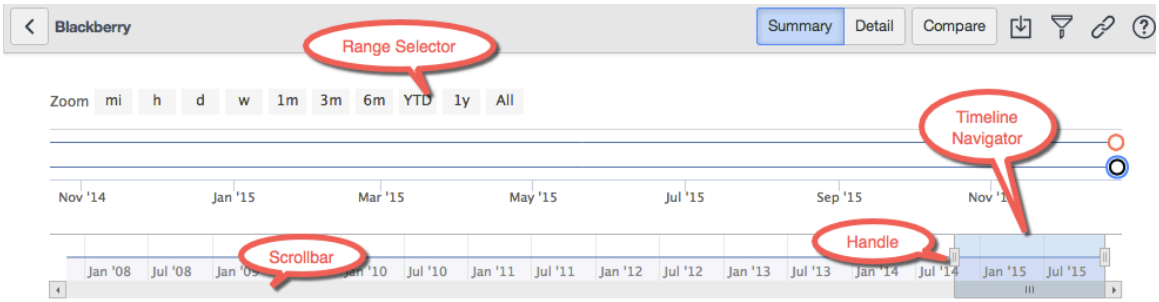
自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

CI の変更は、タイムラインに沿ってさまざまな形や色のバブルで表されます。各バブルの形状はさまざまなタイプの変更を表し、各バブルの色は変更が有効か無効かを示します。CI のベースラインは、カーソルを合わせると詳細を表示できる黒い円で表されます。**[?]** アイコンをクリックしてバブルの形状と色の定義を表示し、バブルをポイントして変更セットの詳細を表示します。

関係への変更は、Change Magement によって適用された場合にのみ有効と見なされます。提案された変更フレームワークを介して変更が適用された場合、その変更は有効です。追加の検証手順については、「 予定されている検証スクリプトの作成または編集 」を参照してください。

履歴タイムライン表示



タイムラインのバブル

注:
開始予定日がない提案された変更は、将来の時点に配置されます。

タイムラインナビゲーター

タイムラインナビゲーターの両端にあるハンドルを使用して、表示される期間を延長または短縮します。

タイムラインナビゲーターの下部をクリックし、ナビゲーターを左右にドラッグすると、別の期間にスクロールできます。

Zoom

デフォルトでは、先月のタイムラインが表示されます。タイムラインの上にある [ズーム] ラベルの横で、別の時間間隔を選択できます。間隔は 1 分から全期間まで選択できます。

期間中に多くの CI 変更があると、表示されるバブルが密集しすぎる可能性があります。次のいずれかの方法で、バブルを拡大または縮小できます。

- タイムラインの時間間隔を変更します。時間間隔を短くするとズームインし、間隔を長くするとズームアウトします。
- ズームインするタイムラインのセクションを選択します。

プロパティフィルター

表示されるバブルをフィルタリングできます。デフォルトでは、CI のすべてのプロパティの変更を表すバブルがすべて表示されます。選択したプロパティが変更されたバブルのみを表示し、選択されていないプロパティのみが変更されたバブルを除外するようにビューを制限できます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

[詳細] ビューと [サマリー] ビューでは、変更されたフィルタースコープ内のプロパティがハイライト表示されます。変更されたプロパティはライトブルーでハイライト表示されます。

[サマリー] ビューでは、CI のすべてのプロパティを含めるか、変更されたプロパティのみを含めるかを選択できます。[サマリー] ビューですべてのプロパティを表示する場合、変更されたプロパティは未変更のプロパティの前に表示されます。

サマリービュー

[サマリー] ビューには、各バブルで表される CI のスナップショットが表示されます。各スナップショットには、変更セットに従って CI のフィールドと関係への変更が表示されます。変更前後の以前の値と新しい値、および追加または削除された関係が表示されます。

スナップショット表示の両側にある **[>]** および **[<]** ボタンを使用して、次の変更セットレコードと前の変更セットレコードを時系列にスクロールします。

詳細ビュー

[詳細] ビューでは、バブルに対応する CI のスナップショットが表示されます。各スナップショットには、プロパティフィルターのスコープ内にあるフィールドが含まれており、変更されたプロパティがライトブルーの背景で表示されます。バブルをクリックすると、対応する CI のスナップショットが表示されます。表示されるデータは読み取り専用です。

両側の **[>]** と **[<]** ボタンを使用して、次や前の変更セットレコードを時系列にスクロールします。

関連レコードの変更のタイムラインを表示する

CI レコードの変更のタイムラインでは、CI の関連レコードの変更のタイムラインを表示することもできます。

始める前に

必要なロール：admin

- ターゲットテーブル：CI レコードは構成アイテム [cmdb_ci] テーブルまたはこのテーブルの子孫に存在している必要があります。
- 監査：CI を含むテーブルに対して有効にする必要があります。

手順

1. CI のタイムラインを開きます。
2. [関連レコード] アイコンを選択して、[関連レコードリスト] から表示する関連レコードを選択します。
   [関連レコード] アイコンを再度クリックすると、関連レコードのタイムラインが表示されます。

タスクの結果

CI の関連レコードに対する変更のタイムラインは、CI のタイムラインのすぐ上に表示されます。すべての関連レコードをオフにすると、関連レコードのタイムラインは非表示になります。

次のタスク

関連レコードタイムラインの変更バブルにカーソルを合わせると、変更されたプロパティの日付や数などの詳細が表示されます。フォーカスされる時間間隔を変更したり、ズームインまたはズームアウトすると、CI タイムラインと関連レコードのタイムラインの両方に同時に影響します。

CI のスナップショットをエクスポートする

CI のスナップショットをそのタイムラインからエクスポートすることができます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

始める前に
CI が構成アイテム [cmdb_ci] テーブルまたはそのテーブルの子孫に存在している必要があります。
監査は CI を含むテーブルに対して有効にする必要があります。
必要なロール：admin

このタスクについて
CI のスナップショットは XML、PDF (ポータル)、または PDF (横向き) 形式でエクスポートすることができます。

手順

1. CI のタイムラインを開きます。
2. CI のスナップショットをエクスポートする時間を表すバブルを選択します。
3. エクスポートアイコン ( ) をクリックします。
4. エクスポートに使用するファイル形式を選択します。
   ファイルをシステムにダウンロードして表示することができます。

CI スナップショットを比較する

タイムライン内の 2 つの異なる時点の CI のプロパティと関係を比較できます。

始める前に
CI が構成アイテム [cmdb_ci] テーブルまたはそのテーブルの子孫に存在している必要があります。
監査は CI を含むテーブルに対して有効にする必要があります。
必要なロール：admin

手順

1. CI のタイムラインを開きます。
2. [比較] をクリックします。
3. 開始日と終了日を選択します。
4. [比較] をクリックします。

参照フィールドの変更の追跡

管理者は、参照フィールドの表示値の変更を追跡できます。

参照フィールドには ID 値のみが格納されるため、通常は ID 値が変更された場合にのみ変更を監査できます。デフォルトでは、参照フィールドの表示値が変更されても、変更は監査されません。

次の状況を考えてみましょう。ユーザーが名前を「Jane Smith」から「Jane Miller」に変更します。ユーザー名はユーザーテーブルの表示値であるため、Jane Smith への以前の参照は Jane Miller を参照します。管理者が既存のユーザーレコードの名前を更新したばかりの場合は、監査レコードと履歴レコードには新しい名前である Jane Miller のみが表示されます。デフォルトでは、元のユーザー名で行われた変更と新しいユーザー名で行われた変更を区別する方法は提供されていません。

監査ポリシーでユーザー名の変更を追跡するよう求められている場合は、次のことができます。

- 新しい名前の新しいユーザーレコードを作成し、以前のユーザーレコードを無効にします。以前のユーザー名の監査レコードは保持され、新しいユーザー名で将来の監査レコードが作成されます。
- 以前の名前と名前変更の日付を保存するカスタムフィールドとビジネスルールを作成します。この情報を使用して、監査レコードと履歴レコードで適切な名前が作成されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

挿入の追跡

デフォルトでは、挿入が監査テーブルのサイズの 80% を超える可能性があるため、挿入の監査レコードは作成されません。

挿入を追跡しないと、パフォーマンスが向上し、監査テーブルが大幅に小さくなります。管理者は、*glide.sys.audit_inserts* プロパティを *true* に設定することで、挿入の監査を有効にできます。

CI 関係の追跡

CI 関係 (CI 関係、CI/ユーザー関係、または CI/グループ関係) への変更は、変更が手動か ディスカバリー の結果であるかにかかわらず、変更された関係の両側のアイテムの履歴に表示されます。

たとえば、コンピューターアルファにコンピューターベータから使用されているという CI 関係がある場合、アルファの履歴にはベータとの関係がいつ確立されたかが記録され、同様に、ベータの履歴にはアルファとの関係がいつ確立されたかが記録されます。この例は、一部の CI 関係が確立され、その後、いずれかの関係が削除されたときに表示される履歴を示しています。

CI 関係履歴

⊟ 2008-12-03 10:49:37 **Updated by** Guest (19 Hours 54 minutes ago) - CI Relationship Change

- created 2 Days 2 Hours 51 minutes earlier

Relationship	Before	After
Runs	(relationship added)	Tomcat@tomdmac
Runs	(relationship added)	MySQL Server@tomdmac

⊞ 2008-12-03 10:49:38 **Updated by** Guest (19 Hours 54 minutes ago) - Mac OS X - Disks

⊞ 2008-12-03 10:49:43 **Updated by** Guest (19 Hours 54 minutes ago) - Mac OS X - Active Connections

⊞ 2008-12-03 10:50:02 **Updated by** Guest (19 Hours 53 minutes ago)

⊟ 2008-12-04 06:43:39 **Updated by** Glide Maintenance (just now) - CI Relationship Change

- last activity was 19 Hours 53 minutes earlier
- created 2 Days 22 Hours 45 minutes earlier

Relationship	Before	After
Runs	MySQL Server@tomdmac	(relationship removed)

作成された黒い丸は、CI、ユーザー、またはグループが作成された日付を示します。最後のアクティビティの黒い丸は、関係が最後に変更された日時を示します。いずれかまたはすべての CI 関係タイプの CI 関係履歴を表示しない場合は、CI 関係テーブル (CI 関係 [cmdb_rel_ci]、CI/ユーザー関係タイプ [cmdb_rel_user_type]、またはグループ関係 [cmdb_rel_group]) の監査を無効にしてオフにすることができます。

高セキュリティ設定

高セキュリティ設定とは、インスタンスで利用可能な複数のセキュリティオプションを指します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

高セキュリティ設定の詳細

高セキュリティ設定の機能とビジネス価値について学習します。

高セキュリティ設定のアクティブ化

高セキュリティ設定を有効にします。

高セキュリティ設定の構成

高セキュリティ設定を構成する方法について説明します。

自動翻訳

高セキュリティ設定の詳細

高セキュリティ設定とは、インスタンスで利用可能な複数のセキュリティオプションを指します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

高セキュリティ設定モジュールは、High Security Settings プラグインで有効になり、新しいインスタンスではデフォルトで有効になります。インスタンスで高セキュリティ設定がアクティブでない場合は、「高セキュリティ設定のア有効化を要求する」を参照してください。このプラグインの詳細については、「インスタンスセキュリティ強化設定」の「高セキュリティプラグイン」を参照してください。次のタイプの高セキュリティ設定のプロパティを使用できます。

- デフォルトのプロパティ値：すべての重要なセキュリティ設定を 1 つの場所で管理および監査することで、プラットフォームのセキュリティを強化します。
- デフォルトの拒否プロパティ：テーブルアクセスのデフォルトのセキュリティ動作を制御するセキュリティマネージャープロパティを提供します。
- セキュリティ管理者ロール：主要なセキュリティ設定とリソースの変更を防止するロールを提供します。セキュリティ管理者ロールは admin ロールによって継承されないため、明示的にアサインする必要があります。
- 昇格された権限：セキュリティ管理者ロールを持つユーザーが、通常のユーザーのコンテキストで操作し、必要に応じてより高いセキュリティロールに昇格できるようにします。
- プロパティアクセス制御：セキュリティ管理者は、プロパティの読み取りと書き込みに必要なロールを設定できます。
- システムログ：読み取り専用です。
- アクセス制御ルール：ユーザーがアクセスできるデータとアクセス方法を制御します。

注:

- 高セキュリティ設定では、コンテキストセキュリティプラグインも自動的に有効になります (まだ有効になっていない場合)。さらに、プラットフォームセキュリティ設定 - 高は、インスタンスのセキュリティを強化するための設定と機能を提供します。
- [インスタンスセキュリティ強化設定] コンテンツには、Now Platform のセキュリティ関連のシステムプロパティとプラグインの詳細な説明とコンプライアンス値が含まれています。これらのプロパティの詳細については、「インスタンスセキュリティ強化設定」を参照してください。
- これらのプロパティの詳細については、「インスタンスセキュリティ強化設定」を参照してください。

高セキュリティ設定プロパティを設定または変更するには 2 つの方法があります。

- 移動先 システムセキュリティ > 高セキュリティ設定.

  [高セキュリティプロパティ] ページのオプションは [はい] または [いいえ] です。

- **sys_properties.list** に移動し、設定または変更するプロパティを検索します。

  システムプロパティテーブル [sys_properties.list] のオプションは **true** または **false** です。

プロパティアクセス制御

高セキュリティ設定がアクティブな場合、プロパティ [sys_properties] テーブルに 2 つの追加列が作成されます。

- **read_roles**：このプロパティのすべてのフィールドを読み込むことができるロール名のカンマ区切りリスト。
- **write_roles**：このプロパティのすべてのフィールドに対して書き込み/変更ができるロール名のカンマ区切りリスト。

自動翻訳

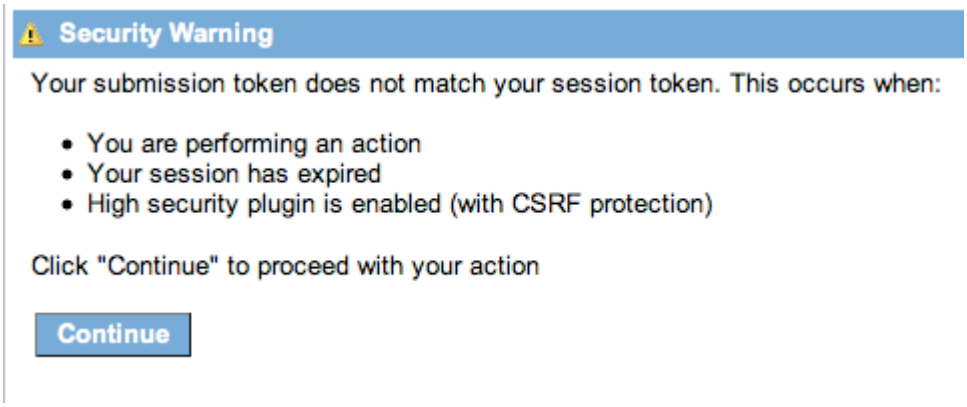
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

プロパティテーブルにリストされているプロパティには、admin の **read_roles** と security_admin の **write_roles** があります。admin ロールを持つユーザーはプロパティ値を表示して読み取ることができますが、変更するには security_admin ロールに昇格する必要があります。

通知

高度なセキュリティ設定を有効にすると、セキュリティ警告メッセージも有効になります。承認後に表示されるメッセージの例を次に示します。

セキュリティ警告通知



高セキュリティ設定プロパティ

プロパティ	説明	デフォルト値	インスタンスセキュリティ強化設定
glide.ui.escape_text	ユーザーインターフェイスのパーサーレベルで XML 値をエスケープします。反映および格納されたクロスサイトの防止スクリプティング攻撃を防止します。このプロパティは、Service Portal には適用されません。 **注:** Vancouver 以降のリリースでは、このプロパティはデフォルトで **true** に設定されており、管理者が変更することはできません。プロパティを変更する必要があるユースケースについては、カスタマーサポートにお問い合わせください。	はい	XML をエスケープする

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

プロパティ	説明	デフォルト値	インスタンスセキュリティ強化設定
glide.ui.escape_all_script	デフォルトで、Jelly JavaScript <![CDATA[<script type="text/javascript">]]> タグ内のすべての式をエスケープするように強制します。]]> タグのタイプ<![CDATA[<script>属性が空の場合、または値が text/javascript、text/ecmascript、application/javascript、application/ecmascript、または application/x-javascript の場合にのみ、エスケープを強制します。	はい (新しいインスタンスの場合)	Jelly をエスケープする
glide.ui.rotate_sessions	HTTP セッション識別子をローテーションしてセキュリティの脆弱性を低減します。参照：http://www.owasp.org/index.php/Session_Management#	はい 注: Single Sign-on 認証に SAML 2.0 プラグインを使用している場合、このプロパティを [いいえ] に設定します。設定しない場合、インスタンスと ID プロバイダーの間で行われるセッション情報の共有が妨げられます。	HTTP セッション識別子をローテーションする ifiers
glide.ui.secure_cookies	有効化セキュアセッションの cookie：追加の cookie セキュリティを有効にします。「はい」の場合、厳格なセッション cookie 検証が適用されます。	はい	セキュアセッションの cookie
glide.security.password_reset.uri	モバイルの パスワードリセット では、ユーザーが [パスワードを忘れた場合] ボタンを		なし

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

プロパティ	説明	デフォルト値	インスタンスセキュリティ強化設定
	クリックしたときに移動する URL を指定できます。		
glide.security.strict.updates	フォーム送信時に受信トランザクションのセキュリティを再確認します (フォーム生成時に常に権限が確認されます)。 **注:** Vancouver 以降のリリースでは、このプロパティはデフォルトで **true** に設定されており、管理者が変更することはできません。プロパティを変更する必要があるユースケースについては、カスタマーサポートにお問い合わせください。	はい	受信トランザクションを再確認する
glide.security.strict.actions	実行前に UI アクションの条件をチェックします。通常、条件はフォームのレンダリング中にのみチェックされます。	はい	実行前に UI アクションをチェックする
glide.security.use_csrf_token	セキュアなトークンの使用を有効にして、受信要求を識別して検証します。このトークンはクロスサイトリクエストフォージェリ攻撃を防ぐために使用されます。	はい	CSRF 対策トークン
glide.ui.escape_html_list_field	リストビュー内の HTML フィールドに対して HTML をエスケープします。	はい	HTML をエスケープする

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

プロパティ	説明	デフォルト値	インスタンスセキュリティ強化設定
glide.html.escape_script	HTML フィールドの javascript タグをエスケープします。	はい	Javascript をエスケープする
glide.ui.forgetme	ログインページから [記憶する] チェックボックスを削除します。	はい	[記憶する] の削除
glide.smtp.auth	ユーザー名とパスワードのプロパティで SMTP サーバーを認証します。 **注:** このプロパティは廃止されました。	はい	SMTP 認証 (使用廃止)
glide.script.use.sandbox	権限が軽減されたサンドボックス内でクライアント生成スクリプト (AJAXEvaluate およびクエリー条件) を実行します。[はい] の場合、[クライアントコール可能] チェックボックスが [はい] に設定されているビジネスルールとスクリプトインクルードのみを使用でき、特定のバックエンド API 呼び出しは禁止されます。詳細については、「スクリプトサンドボックスプロパティの構成」を参照してください。	はい	クライアント生成スクリプトサンドボックス
glide.soap.strict_security	着信 SOAP 要求に厳格なセキュリティを適用します。着信 SOAP 要求は、セキュリティマネージャーを経由してテーブルとフィールドにアクセスし、SOAP ユーザーに Web サービスを使用するための正しいロー	はい	SOAP 要求の厳格なセキュリティ

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

プロパティ	説明	デフォルト値	インスタンスセキュリティ強化設定
	ルがあるかをチェックする必要があります。		
glide.basicauth.required.wsdl	着信 WSDL 要求に認証を要求します。 注: 着信 WSDL 要求に認証を要求することを選択しない場合、アクセス制御 (ACL) ルールを変更してゲストユーザーが WSDL コンテンツにアクセスできるようにする必要があります。	はい	WSDL 要求認証
glide.basicauth.required.csv	着信 CSV 要求に基本認証を要求します 。	はい	CSV 要求認証
glide.basicauth.required.excel	着信 Excel 要求に基本認証を要求します。	はい	Excel 要求認証
glide.basicauth.required.importprocessor	着信インポート要求に基本認証を要求します。	はい	要求認証をインポートする
glide.basicauth.required.pdf	着信 PDF 要求に基本認証を要求します。	はい	PDF 要求認証
glide.basicauth.required.rss	着信 RSS 要求に基本認証を要求します。	はい	RSS 要求認証
glide.basicauth.required.scriptedprocessor	着信スクリプト要求に基本認証を要求します。	はい	スクリプト要求認証
glide.basicauth.required.soap	着信 SOAP 要求に基本認証を要求します。	はい	基本認証：SOAP 要求
glide.basicauth.required.unl	着信アンロード要求に基本認証を要求します。	はい	要求認証をアンロードする

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

プロパティ	説明	デフォルト値	インスタンスセキュリティ強化設定
glide.basicauth.required.xml	着信 XML 要求に基本認証を要求します。	はい	XML 要求認証
glide.basicauth.required.xsd	着信 XSD 要求に基本認証を要求します。	はい	XSD 要求認証
glide.cms.catalog_uri_relative	/ess/catalog.do の URL パラメーターからの相対リンクを適用します。「はい」の場合、*uri* パラメーターを使用して、/ess/catalog.do ページから相対 URL のみが許可されます。「いいえ」の場合、すべての URL が許可され、外部の許可されていないコンテンツへのリンクが許可される可能性があります。	はい	相対リンクを強制する
glide.set_x_frame_options	このプロパティを有効にして、すべての UI ページの SAMEORIGIN に対して X-Frame-Options 応答ヘッダーを設定します。X-Frame-Options HTTP 応答ヘッダーは、<frame> または <iframe> 内のページの表示をブラウザに許可するかどうかを示すために使用されます。サイトでは、このプロパティを使用して、このコンテンツがその他のサイトに組み込みできないようにすることで、クリックジャッキング攻撃を回避することができます。 https://developer.mozilla.org/en/the_x-frame-options_response_header	はい	X-Frame-Options：SAMEORIGIN

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

プロパティ	説明	デフォルト値	インスタンスセキュリティ強化設定
glide.ui.attachment.download_mime_types	ブラウザにインラインで表示されない、カンマ区切りの添付 MIME タイプのリスト。クロスサイトの防止スクリプティング攻撃を防ぎます。たとえば、text/html は、HTML ファイルをブラウザでインライン表示するのではなく、添付ファイルとしてクライアントに強制的にダウンロードします。	text/html,image/svg,image/svg+xml	MIME タイプのダウンロードを強制する
glide.security.groupby_acl_check	このプロパティが有効である場合、GroupBy 操作について、グループの実際のデータに基づきグループ名の ACL チェックが実行されます。	はい	なし
glide.security.diag_txns_admin	「はい」の場合、admin ユーザーまたは許可されている IP アドレスからのユーザーのみが stats.do、threads.do、および replication.do にアクセスできます。	いいえ	パフォーマンス監視 (ACL)
glide.ui.security.codetag.allow_script	埋め込み HTML ([code] タグを使用) に JavaScript タグを含めることができます。	いいえ	埋め込み HTML コードを許可する

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

プロパティ	説明	デフォルト値	インスタンスセキュリティ強化設定
	注: Vancouver 以降のリリースでは、このプロパティはデフォルトで **true** に設定されており、管理者が変更することはできません。プロパティを変更する必要があるユースケースについては、カスタマーサポートにお問い合わせください。		
glide.script.allow.ajaxevaluate	AJAXEvaluate プロセッサを有効にします。*AJAXEvaluate* API 呼び出しにより、クライアントはサーバー上で任意のスクリプトを送信して実行できます。	いいえ	AJAXEvaluate を有効にする
glide.login.autocomplete	ブラウザがログインフォーム上のパスワードフィールドでオートコンプリート機能を使用することを許可します。	いいえ	パスワードフィールドのオートコンプリート

次のプロパティは sys_properties テーブルで定義されますが、[高セキュリティ設定] ページには表示されません。

プロパティ	説明	デフォルト値	インスタンスセキュリティ強化設定
com.glide.communications.httpclient.verify_hostname	リモート SSL ホストによって提示されたホスト名と証明書チェーンを確認します。中間者 (MITM) 攻撃から保護します。 詳細については、「Kubernetes Spoke を設定」を参照してください。	true	なし

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

プロパティ	説明	デフォルト値	インスタンスセキュリティ強化設定
	注: このプロパティは、com.glide.communications.trustmanager_trust_allプロパティを上書きします。		
glide.basicauth.required.schema	受信テーブルスキーマ要求に対して基本認証を要求します。	true	なし
glide.security.csrf_previous.allow	期限切れのセキュアトークンの使用を許可して、受信要求を識別して検証します。このトークンはクロスサイトリクエストフォージェリ攻撃を防ぐために使用されます。	false	なし
glide.security.csrf_previous.time_limit	保護トークンが期限切れになるまでの時間 (秒)。以前のCSRF トークンが有効である期間の長さを制御できます。ユーザーセッションが期限切れになると、*glide.security.csrf_previous.allow*プロパティが有効になっていて、このプロパティで指定された期間内にない限り、セキュアトークンも期限切れになります。このトークンはクロスサイトリクエストフォージェリ攻撃を防ぐために使用されます。	86400 注: 値は秒単位です。1 日に相当します。	なし
glide.security.csrf.strict.validation.mode	CSRF トークンの厳格な妥当性確認が実施されるため、CSRF トークンが一致しない場合、ユーザーは要求を再送信できません。	false	CSRF 厳格検証
com.glide.security.check_unsanitized_html	クロスサイトスクリプティング攻撃に対処するために、グローバルレベルでtranslated_html	enforce	なし

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

プロパティ	説明	デフォルト値	インスタンスセキュリティ強化設定
	フィールドのサニタイズ動作を強制します。		

スクリプトサンドボックスプロパティの構成

スクリプトサンドボックスプロパティ (*glide.script.use.sandbox*) を有効にして、権限が制限されているサンドボックス内でクライアントが生成したスクリプトを実行します。

システム内には、クライアントが評価のためにサーバーにスクリプトを送信できるケースが 2 つあります。

- フィルター/クエリー：assigned_to=javascript:getMyGroups() などのフィルターをサーバーに送信することは合法です。
- システム API：*AJAXEvaluate* API 呼び出しにより、クライアントはサーバー上で任意のスクリプトを送信して、応答を受信することができます。

スクリプトサンドボックスプロパティ (*glide.script.use.sandbox*) を有効にすると、これらの 2 つのエントリポイントのいずれかを介して評価されるスクリプトは、次の特性を持つ、権限が減らされたサンドボックス内で実行されます。

- サンドボックス内では、クライアントコール可能とマークされたビジネスルールのみを使用できます。
- サンドボックス内では、クライアントコール可能とマークされたスクリプトインクルードのみ使用できます。
- 特定の API 呼び出し (直接 DB アクセスを扱うものに概ね限定) は許可されていません。
- サンドボックス内からデータを挿入、更新、または削除することはできません。たとえば、*current.update()* の呼び出しは無視されます。

注:
このプロパティの詳細については、「インスタンスセキュリティ強化設定」の「クライアント生成スクリプトサンドボックス」を参照してください。

スクリプトサンドボックスが有効になっている場合、これらのメソッドはクライアントで生成されたスクリプトで許可されません。

制限付きメソッド

クラス	メソッド
GlideRecord	*deleteMultiple()*、 *deleteRecord()*、 *insert()*、 *update()*、 *updateMultiple()*
GlideSystem (gs)	*addErrorMessage()*、 *addInfoMessage()*、*addMessage()*、*eventQueue()*、*flus workflowFlush()*
ScopedGlideRecord	*deleteMultiple()*、 *deleteRecord()*、 *insert()*、 *update()*、 *updateMultiple()*

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

制限付きメソッド (続く)

クラス	メソッド
ScopedGlideSystem (gs)	`addErrorMessage()`、`addInfoMessage()`、`debug()`、`eventQueue()`、`executeNo`
GlideDateTime/GlideTime/GlideDate	`getDayOfWeek()`、`getDayOfWeekUTC`、`getDayOfWeekLocal`
GlideSchedule	`isInSchedule()`、`add()`、`Load()`、`whenNext()`

注:
GlideSystem (gs) メソッドの `log()`、`logError()`、および `logWarning()` は、`glide.security.sandbox_no_logging` システムプロパティを falseに設定することで、スクリプトサンドボックスで有効にできます。

スクリプトサンドボックスを有効にせずにシステムを実行する場合、これらの制限は適用されません。

注:
このプロパティは、高セキュリティ設定プラグインを有効にするとデフォルトで有効になります。プラグインの外部でこのプロパティを有効にしないでください。

高セキュリティ設定の有効化

High Security Settings プラグインは、すべての新しいインスタンスでデフォルトで有効です。インスタンスで有効にされていない場合は、プラグインを要求できます。

始める前に
必要なロール：なし

既存のインスタンスで高セキュリティ設定を有効にする前に次のことを実行します。

1. 新しい動作を理解するには、次の情報を確認してください。
   - アクセス制御リストのルール
   - 高セキュリティ設定
   - デフォルトの拒否プロパティ
2. 非本番インスタンスでプラグインを有効にします。最新の本番クローンが推奨されます。
3. 変更された機能、特に追加された ACL とデフォルト拒否機能をテストします。システムが期待どおりに動作するまでテストを続行します。ユーザーが予定されているリソースにアクセスできない場合は、アクセス権を付与するための適切なロールと ACL ルールがあることを確認してください。
4. 本番環境に適用できるように、必要な変更の更新セットを作成します。

注:
このプラグインの詳細については、「インスタンスセキュリティ強化設定」の「高セキュリティプラグイン」を参照してください。

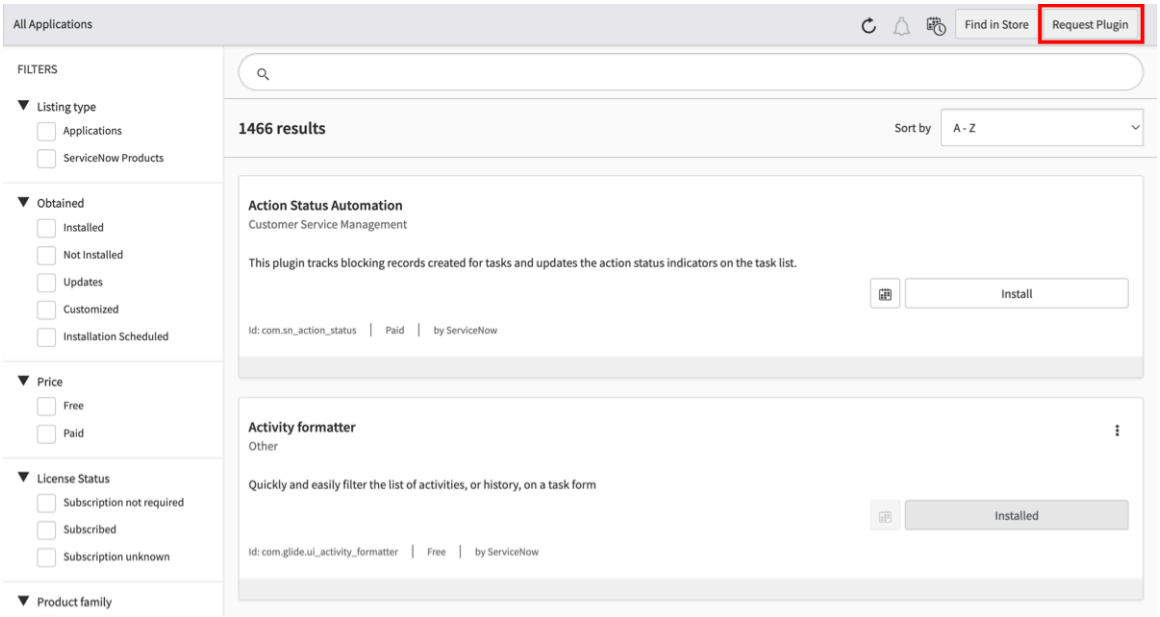
必要なロール：admin

自動翻訳

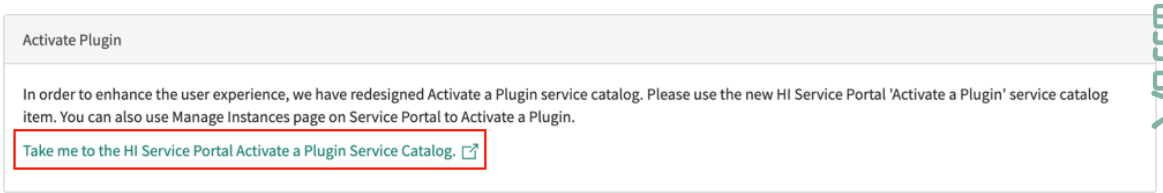
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

手順

1. 移動先 すべて > システムアプリケーション > 利用可能なすべてのアプリケーション > すべて。
2. [すべてのアプリケーション] ページで [プラグインの要求] をクリックして、Now Support で [プラグインをアクティブ化] フォームを開きます。



3. Now Support で、Now Support サービスポータル サービスカタログ にアクセスするリンクを選択します。



4. インスタンスを選択します。
5. [アクション] > [プラグインのアクティブ化] を選択します。
6. [プラグインのアクティブ化] フォームで、次の情報を入力します。

[プラグインのアクティブ化] フォーム

フィールド	説明
ターゲットインスタンスは何ですか	プラグインをアクティブ化するインスタンス。
どのプラグインをアクティブ化しますか	アクティブ化するプラグインの名前です。

自動翻訳

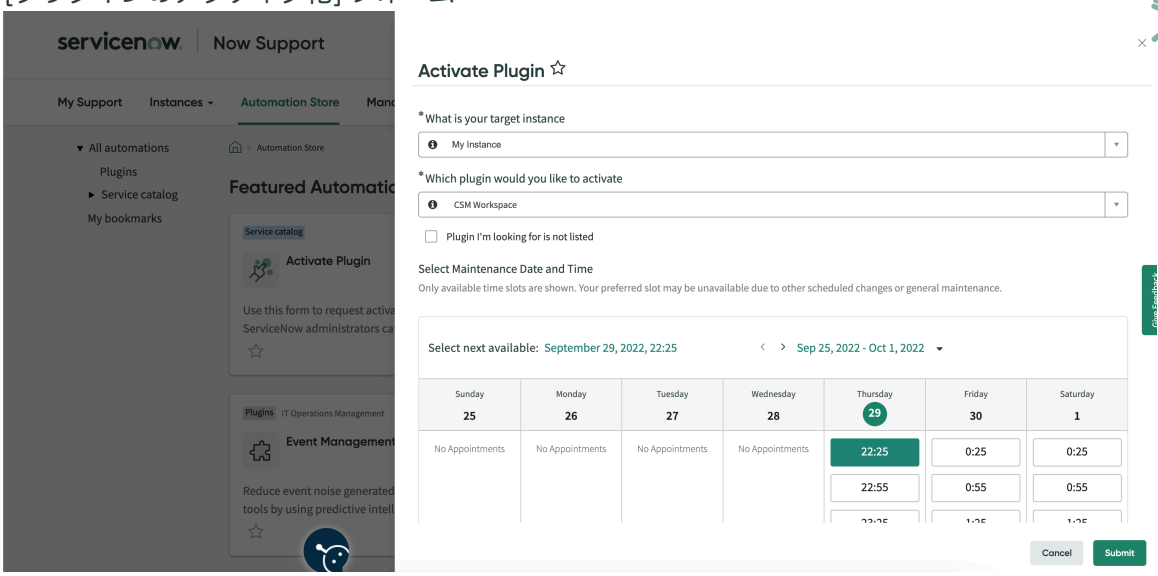
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

フィールド	説明
	注: 必要なプラグインが表示されない場合、または OEM またはオンプレミスのインスタンスでプラグインをアクティブ化している場合は、[探しているプラグインが表示されていません **(Plugin I'm looking for is not listed)]** チェックボックスをオンにして、プラグインの名前を入力します。
メンテナンスの日時を選択 (Select Maintenance Date and Time)	プラグインをアクティブ化する日時。 注: プラグインは、米国太平洋標準時で、毎営業日の朝と夕方の 2 回のバッチでアクティブ化されます。特定の時刻にプラグインをアクティブ化する必要がある場合は、[理由/コメント **(Reason/ Comments)]** フィールドに要求を入力します。

Example

たとえば、 [自分のインスタンス (My Instance)] という名前のインスタンスで CSM Workspace プラグインをアクティブ化するには、次のフォームを参照してください。

[プラグインのアクティブ化] フォーム



7. [送信] を選択します。
プラグインの要求の詳細については、次を参照してください。 の Service Catalog [KB0751715] 記事からのプラグインの要求 Now Support ナレッジベース。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

HTML サニタイザー

HTML フィールドと翻訳された HTML フィールドの HTML マークアップをサニタイズして不要なコードを削除し、クロスサイトスクリプト攻撃などのセキュリティ上の懸念から保護します。

HTML サニタイザーを探索する

詳しくは、HTML サニタイザーの仕組みをご覧ください。

HTML サニタイザーを設定する

HTML サニタイザーを設定します。

HTML サニタイザーを有効にする

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

詳しくは、HTML サニタイザーを有効にする方法をご覧ください。

HTML サニタイザーの詳細

HTML フィールドと翻訳された HTML フィールドの HTML マークアップをサニタイズして不要なコードを削除し、クロスサイトスクリプト攻撃などのセキュリティ上の懸念から保護します。

HTML のサニタイズを使用して、インスタンス内の HTML コンテンツに潜在的に有害なコンテンツが含まれないようにします。HTML のサニタイズは、インスタンスを侵害するために使用される可能性のある HTML タグ (<![CDATA[<script>]]>、 などの<embed>タグや、インスタンスで不要なスクリプトを実行したり、ユーザーを不要なコンテンツに誘導したりするために使用される可能性のあるタグ<link>を削除することで機能します。コンテンツのフォーマットを制御する安全なタグは保持されます。管理者は、削除または保持するコンテンツをカスタマイズできます。また、サニタイズをすべてのコンテンツに適用するか、指定したフィールドのみに適用するかを制御することもできます。

HTML サニタイザーは、常に保持する必要があるマークアップのビルトイン包含リストをチェックすることで機能します。サニタイザーは、管理者がビルトイン包含リストを変更するために使用できる *HTMLSanitizerConfig* スクリプトインクルードを提供します。アイテムを除外リストに追加して、HTML マークアップを削除することもできます。除外リストの内容で包含リストは上書きされます。

次のタイプのアイテムを包含リストと除外リストに追加できます。

- グローバル属性
- HTML 要素

注:
デフォルトでは、href や src などの URL 属性は次のプロトコルのみをサポートしています。

- http
- https
- mailto
- data

例：

```
<a href="https://community.servicenow.com/community">ServiceNow Community</a>
```

注:
HTML サニタイザーの使用を制御する *glide.html.sanitize_all_fields* プロパティの詳細については、「インスタンスセキュリティ強化設定」の「HTML サニタイザー」を参照してください。

urlAttributes とプロトコルを設定する

HTMLSanitizer スクリプトインクルードで urlAttributes とそのプロトコルを設定できます。例：

```
HTML_WHITELIST : {
urlAttributes: { "protocols" : [ "file", "notes" ] },
            - -
            - -
    }
```

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

この例では、`メモ` が包含リストに含まれているため、この URL はサニタイズされません。

```
<a title=“Lotus”
 href=“Notes://
ABC/X575C90019DE33/ABC594DCB76D86EB4925653E0011C4C1/ZZ90B7E2D33964749257EE
A003456FD”>Lotus</a></p>
```

デフォルト包含リスト

注:
デフォルト包含リストはシステムリストであり、インスタンス内のユーザーはアクセスできません。

```
BUILTIN_HTML_WHITELIST :{

   globalAttributes:{ attribute:["id","class","lang","title","style"],

                              attributeValuePattern:{}},

   label:{ attribute:["for"]},

   font:{ attribute:["color","face","size"]},

   a:{ attribute:["href","nohref","name","shape"]},

   img:{ attribute:["src","name","alt","border","hspace","vspace","align","height","width"},

   table:{ attribute:["border","cellpadding","cellspacing","bgcolor","background","align","no
 resize","height","width","summary","frame","rules"]},


 th:
{ attribute:["background","bgcolor","abbr","axis","headers","scope","nowrap","height","width","al
ign","valign","char off","char","colspan","rowspan"]},


 td:
{ attribute:["background","bgcolor","abbr","axis","headers","scope","nowrap","height","width","al
ign","valign","char off","char","colspan","rowspan"]},

   tr:{ attribute:["background","height","width","align","valign","char off","char"]},

   thead:{attribute:["align","valign","char off","char"]},

   tbody:{attribute:["align","valign","char off","char"]},

   tfoot:{attribute:["align","valign","char off","char"]},

   colgroup:{attribute:["align","valign","char off","char","span","width"]},

   col:{attribute:["align","valign","char off","char","span","width"]},

   p:{attribute:["align"]},

   style:{attributeValuePattern:{"type":"text/css"}}
```

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

```
    canvas:{ attribute:["height","width"]},

    details:{ attribute:["open"]},

    summary:{ attribute:["open","valign","char off","char"]},

    button:{ attribute:["disabled","accesskey","type"]},

    form:{},

 input:{ attribute:["size","maxlength","checked","alt","src","type","disabled","readonly","accessk
ey","border","usemap"]},

    select:{ attribute:["disabled","multiple","size"]},

    textarea:{ attribute:["rows","cols","disabled","readonly","accesskey"]},

    option:{ attribute:["disabled","label","selected"]},

    div:{ attribute:["align"]},

    ol:{ attribute:["start","type","square"]},

    ul:{ attribute:["type","square","itemscope","itemtype","itemref"]},

    li:{ attribute:["value","fb__id","itemprop"]},

    span:{ attribute:["color","size","data-mce-bogus","itemprop","face"]},

    br:{ attribute:["clear"]},

    h3:{ attribute:["itemprop"]},

    html:{ attribute:["xmlns","lang","xml:lang"]},

    link:{ attribute:["rel","type","href","charset"]},

    meta:{ attribute:["name","content","scheme","charset","http-equiv"]},

    pre:{ attribute:["xml:space"]},

    noscript:{},   h1:{},   h2:{},    h4:{},   h5:{},   h6:{},

    i:{},   b:{},   u:{},   strong:{},   em:{},   small:{},   big:{},

    pre:{},   code:{},   cite:{},   samp:{},   sub:{},   sup:{},

    strike:{},   center:{},  blockquote:{},   hr:{},    map:{},

    dd:{},   dt:{},   dl:{},  fieldset:{},   legend:{}, figure:{},  tt:{},

    body:{},   caption:{},   head:{},   title:{},  shape:{},},
```

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

HTML サニタイザーの構成

HTML サニタイザーの構成を変更するには、スクリプトインクルードを変更する必要があります。

始める前に
必要なロール：管理者

手順

1. 移動先 すべて > システム定義 > スクリプトインクルード.
2. **HTMLSanitizerConfig** を開きます。
3. 除外リストにアイテムを追加するには、HTML_BLACKLIST クラスを使用します。

   包含リストにアイテムを追加するには、HTML_WHITELIST クラスを使用します。

   次の形式を使用します。

```
HTML_XXXXLIST :{
      globalAttributes :{

         attribute:[attribute-name1,...],
         attributeValuePattern:{ attribute-name2:attribute-value-regex-pattern,...}

      },<html-element-name>:{// Same as Above},----}
```

   - *globalAttributes* には、すべての HTML 要素にグローバルに適用可能な属性または attributeValuePattern アイテムが含まれています。
   - *attribute* は属性のカンマ区切りリストです。
   - *attributeValuePattern* は、属性-値-正規表現-パターンのペアに関する属性のディクショナリです。属性-値-正規表現-パターンは、属性値と一致する必要がある正規表現です。

Example:
次の例を考えてみましょう。

```
HTML_WHITELIST:{
      globalAttributes:{
         attribute:["id","name"],},
      img:{
         attribute:["style","align"],
         attributeValuePattern:{src:".*jpeg"}},
      iframe:{},}
```

次のアイテムが包含リストに追加されます。

- グローバル属性の ID と名前。これは、すべての要素にグローバルに適用できる文字列のリストです。
- 属性がスタイルと配置である img 要素。
- 画像のソース属性が .jpeg 拡張子のファイルである img 要素。これは、属性値と一致する正規表現パターンの例です。
- iframe 要素。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

HTML サニタイザーの有効化

HTML サニタイザーは、システム内のすべての HTML フィールドのサニタイザーを有効または無効にするプロパティを提供します。

始める前に
必要なロール：管理者

このタスクについて
デフォルトでは、このプロパティは新しいインスタンスで true に設定されます。

手順

1. ナビゲーションフィルターで、「sys_properties.list」と入力します。
2. *glide.html.sanitize_all_fields* プロパティと *glide.translated_html.sanitize_all_fields* プロパティを **true** に設定します。

   注:
   このプロパティの詳細については、「インスタンスセキュリティ強化設定」の「HTML サニタイザー」を参照してください。

Trouble?

[システムのプロパティ] テーブルにプロパティが存在しない場合は追加できます。

個別フィールドのサニタイズの有効化

フィールド属性を使用して、個々のフィールドでサニタイザーを有効または無効にすることができます。

始める前に
必要なロール：管理者

このタスクについて
最初にサニタイザープロパティを false に設定してから、任意のフォームのフィールドごとにサニタイザーを有効にする必要があります。

手順

1. sys_properties テーブルに移動し、*glide.html.sanitize_all_fields* を **false**に設定します。
   これにより、システム内のすべての HTML フィールドのサニタイザーが無効になります。
2. HTML フィールドを含むフォームに移動します。
3. HTML フィールドラベルを右クリックし、[ディクショナリを設定] を選択します。
   HTML フィールドのディクショナリエントリフォームが開きます。
4. [属性] フィールドに次のいずれかを入力します。
   - サニタイズを無効にするには、「html_sanitize=false」と入力します。
   - サニタイズを有効にするには、「html_sanitize=true」と入力します。
5. [更新] をクリックします。
6. 翻訳された HTML フィールドの HTML サニタイザーを有効にするには、*glide.translated_html.sanitize_all_fields* プロパティを **true**に設定します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

HTML サニタイザーログ記録の有効化

HTML サニタイザーが要素または属性を削除すると、それらはシステムログに追加されます。

始める前に
必要なロール：管理者

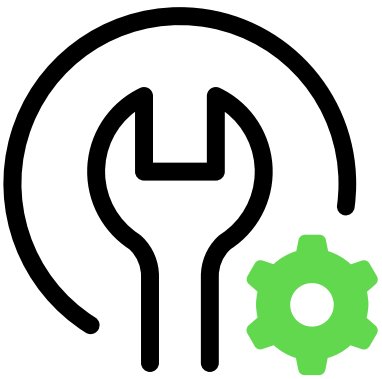
このタスクについて
/syslog_list.do?sysparm_query=source%3DHTMLSanitizer をインスタンス URL に追加して、これらのサニタイズされた要素を確認することができます。

手順

1. これらのサニタイズされた要素を確認するには、/syslog_list.do?sysparm_query=source%3DHTMLSanitizer をインスタンス URL に追加します。
2. ログ記録を有効または無効にするには、glide.html_sanitize.discarded_log.enable プロパティをシステムプロパティに追加し、値を **true** (有効) または **false** (無効) に設定します。
   このプロパティはデフォルトで **true** に設定されています。

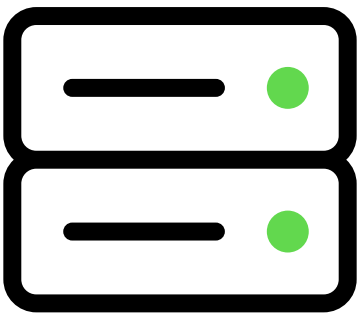
その他の設定とセキュリティリソース

このセクションでは、Instance Security Center の外部で設定するセキュリティプロパティについて説明します。また、その他のセキュリティ関連のリソースについても説明します。



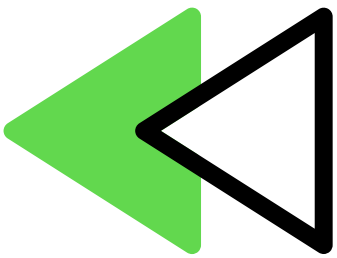
セキュリティシステムプロパティ

セキュリティ設定には、インスタンスのセキュリティレベルを制御するプロパティがいくつかあります。



MID Server 展開ガイド

ServiceNow Management, Integration, and Discovery (MID) サーバーは、仮想マシンを含む標準ハードウェア上で Windows サービスまたは UNIX デーモンとして動作する軽量の Java アプリケーションです。

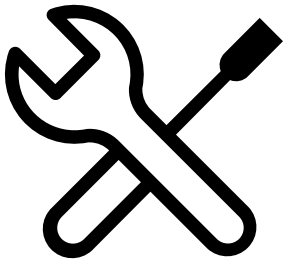
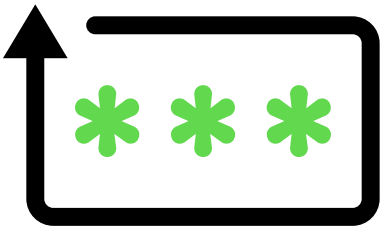
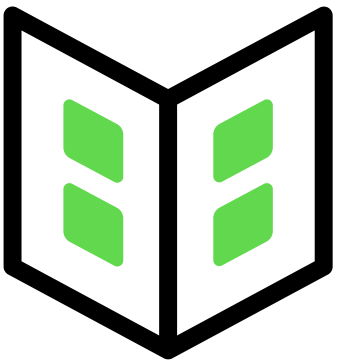


元に戻せる動作

「safe_overrides」または「no_db_override」のいずれかに分類されるシステムプロパティがあります。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

		
減価償却済みセキュリティプロパティ	**Javascript** コンテンツアクセス制御の使用	その他のセキュリティ強化リソース
これらのセキュリティプロパティは、以前のリリースで廃止されました。	JavaScript コンテンツアクセス制御を使用して、インスタンス内でブロックされたサードパーティの JavaScript URL のリストを変更できます。	Now Platform に関連する、セキュリティコントロールの強化に関するその他の情報源。

セキュリティ設定プロパティ

セキュリティ設定には、インスタンスのセキュリティレベルを制御するプロパティがいくつかあります。

一般的なセキュリティ設定のプロパティを設定または変更するには、いくつかの方法があります。

- 移動先 システムプロパティ > **Security** (セキュリティ).

  [セキュリティ] ページのオプションは [はい] または [いいえ] です。

- **sys_properties.list** に移動し、設定または変更するプロパティを検索します。

  システムプロパティテーブル [sys_properties.list] のオプションは **true** または **false** です。

- 移動先 システムセキュリティ > インスタンスセキュリティセンターをクリックし、[ハードニング] をクリックします。

  最も重要なセキュリティプロパティの設定を構成できます。[インスタンスセキュリティ強化設定] コンテンツには、Now Platform のセキュリティ関連のシステムプロパティとプラグインの詳細な説明とコンプライアンス値が含まれています。これらのプロパティの詳細については、「インスタンスセキュリティ強化設定」を参照してください。

⚠ 警告:
これらのセキュリティ機能を実装する場合は、本番インスタンスに展開する前に機能を十分にテストする必要があります。

エスケープと埋め込みスクリプトのサポート

glide.ui.security.allow_codetag	[code] タグを使用した埋め込み HTML コードをサポートします。 デフォルト値：はい

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

	注: インスタンスセキュリティ強化設定：埋め込み HTML コードを許可する
glide.ui.security.codetag.allow_script	埋め込み HTML ([code] タグを使用) に Javascript タグを含めることができます。 注: Vancouver 以降のリリースでは、このプロパティはデフォルトで **true** に設定されており、管理者が変更することはできません。プロパティを変更する必要があるユースケースについては、カスタマーサポートにお問い合わせください。詳細については、「埋め込み HTML で JavaScript タグを許可する」を参照してください。
glide.ui.escape_all_script	デフォルトで、Jelly JavaScript <![CDATA[<script type="text/javascript">]]> タグ内のすべての式をエスケープするように強制します。]]> タグのタイプ<![CDATA[<script>属性が空の場合、または値が text/javascript、text/ecmascript、application/javascript、application/ecmascript、または application/x-javascript の場合にのみ、エスケープを強制します。 • デフォルト値： ○ 新規/zboot インスタンス：true ○ アップグレードされたインスタンス： false • 推奨値：はい 注: インスタンスセキュリティ強化設定：Jelly をエスケープする

添付ファイルの制限と動作

com.glide.attachment.max_size	メガバイト単位で添付ファイルの最大サイズを設定します。
glide.attachment.role	添付ファイルを作成できるロールをリストします (カンマ区切り形式)。
glide.attachment.extensions	添付ダイアログからドキュメントに添付できるファイル拡張子をリストします (カンマ区切り形式)。拡張子にはドット (.) を含めないでください。例：xls、xlsx、doc、docx。すべての拡張子を許可するには、空白のままにします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

	注: インスタンスセキュリティ強化設定：ファイル拡張子を制限する
glide.ui.attachment.force_download_all_mime_types	すべての多目的インターネットメール拡張 (MIME) タイプの添付ファイルを強制的にダウンロードします。 デフォルト値： • 新規/zboot インスタンス：はい • アップグレードされたインスタンス：いいえ 注: インスタンスセキュリティ強化設定：MIME タイプのダウンロードを強制する
glide.security.file.mime_type.validation	添付ファイルに対する MIME タイプの検証を有効 (**true**) または無効 (**false**) にします。*glide.attachment.extensions* で設定されたファイル拡張子は、アップロード時に MIME タイプがチェックされます。 デフォルト値： • 新規/zboot インスタンス：はい • アップグレードされたインスタンス：いいえ 注: インスタンスセキュリティ強化設定：MIME タイプ制限をアップロードする

顧客アップロード

これらのプロパティは、顧客のアップロードにのみ影響します。添付ファイルには影響しません。

glide.ui.strict_customer_uploaded_static_content	このプロパティを [はい] に設定すると、Now Platform のファイルのアップロード機能を使用してアップロードされた場合、ダウンロードされるファイルのタイプを制限する機能が有効になります。*glide.ui.strict_customer_uploaded_content_type* とともに使用 注: インスタンスセキュリティ強化設定：ファイルのダウンロード制限を有効にする

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

glide.ui.strict_customer_uploaded_content_types	このパラメーターに、Now Platform のファイルのアップロード機能を使用してアップロードされた、カンマ区切りのファイルタイプのリストが含まれている場合、これらのファイルタイプのみをインスタンスからダウンロードできます。 **注:** インスタンスセキュリティ強化設定：ダウンロード可能なファイルタイプを指定する

セキュリティマネージャーとオプション

glide.security.manager	セキュリティマネージャー
glide.sm.default_mode	テーブルに ACL がない場合のセキュリティマネージャーのデフォルト動作
glide.security.strict.updates	フォーム送信時に受信トランザクションのセキュリティを再確認します。権限はフォーム生成時に常にチェックされます。 **注:** このプロパティはデフォルトで **true** に設定されており、管理者が変更することはできません。プロパティを変更する必要があるユースケースについては、カスタマーサポートにお問い合わせください。詳細については、「受信トランザクションを再確認する」を参照してください。
glide.security.strict.actions	実行前に UI アクションの条件をチェックします。通常、条件はフォームのレンダリング中にのみチェックされます。 **注:** インスタンスセキュリティ強化設定：実行前に UI アクションをチェックする
glide.security.granular.create	新しいレコードに作成ルールを適用します (作成と更新を含む場合がある書き込みルールとは異なります)。
glide.security.explain.write.locks	ロックされたフォームエレメントに説明が表示されます。

cookie

glide.ui.forgetme	インスタンスが LDAP または DB ログインを使用している場合、ログインページから [記憶

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

	する] チェックボックスを削除します。ユーザーのアクティブなログインセッションは、操作がないと X 分後にタイムアウトします。ここでの X は **glide.ui.session_timeout** システムプロパティの値です。 デフォルト値：はい (新規および Z ブート) インスタンス **注:** インスタンスセキュリティ強化設定：[記憶する] の削除
glide.ui.secure_cookies	追加の cookie セキュリティを強制するために、セキュアなセッション cookie を有効にします。「はい」の場合、厳格なセッション cookie 検証が適用されます。バージョン 3 の cookie を有効にすると、追加のセキュリティ要件も適用されます。 **注:** インスタンスセキュリティ強化設定：セキュアセッションの cookie
glide.secure_cookie.debug	セキュアなセッション cookie のデバッグ。セキュアなセッションの cookie 操作の詳細なデバッグログを有効にする場合に選択します。

クライアントからのスクリプト実行のセキュリティ制限

glide.script.use.sandbox	権限が軽減されたサンドボックス内でクライアント生成スクリプト (AJAXEvaluate およびクエリー条件) を実行します。有効にされている場合、[クライアントコール可能] チェックボックスがオンになっているビジネスルールとスクリプトインクルードのみを使用でき、特定のバックエンドアプリケーションプログラミングインターフェイス (API) 呼び出しは禁止されます。 **注:** インスタンスセキュリティ強化設定：クライアント生成スクリプトサンドボックス
glide.script.allow.ajaxevaluate	AJAXEvaluate プロセッサを有効にします。 **注:** インスタンスセキュリティ強化設定：AJAXEvaluate を有効にする
glide.script.secure.ajaxgliderecord	標準セキュリティアクセス制御リスト (ACL) を AJAXGlideRecord 呼び出しに適用します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

	デフォルト値：新規およびアップグレード済みインスタンスの場合、[はい] ([はい] の場合は [いいえ] に変更できません)。 **注:** インスタンスセキュリティ強化設定：AJAXGlideRecord ACL チェックの有効化

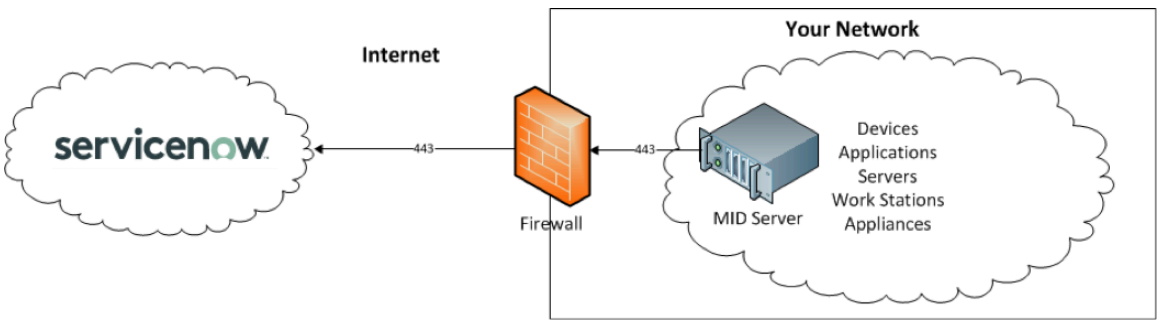
その他

com.glide.communications.trustmanager_trust_all	デフォルトでは、インスタンスは証明書の認証局 (CA) を信頼します。インスタンスが自己発行の証明書を受け入れるようにします。証明書の CA を検証するには、このプロパティを [いいえ] に設定します **注:** インスタンスセキュリティ強化設定：証明書の信頼
glide.outbound.sslv3.disabled	アクティブな場合、インスタンスからの送信接続でセキュアソケットレイヤー (SSL) の代わりにトランスポートレイヤーセキュリティ (TLS) が使用されるようにします。 **注:** インスタンスセキュリティ強化設定：SSLv2/SSLv3 の無効化

高セキュリティ設定 では追加のプロパティを使用できます。

MID Server の安全な展開ガイド (インスタンスセキュリティ強化)

ServiceNow の管理、統合、検出サーバー (MID Server) は、仮想マシンを含む標準ハードウェア上で Windows サービスまたは UNIX デーモンとして動作する軽量の Java アプリケーションです。



独自のログイン資格情報を使用して ServiceNow クラウド内のインスタンスに対して安全に認証し、アプリケーション、データソース、およびサービスによるデータ送信を容易にします。複数の MID Server をさまざまなネットワークセグメントに展開して、スケーラビリティを向上させることができます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

MID Server のセキュリティに関して、次の要素を考慮してください。

物理セキュリティ

MID Server、または仮想化された MID Server のハイパーバイザーをホストする物理ハードウェアを保護します。

- 不正アクセスからハードウェアを保護する安全な場所にハードウェアを配置します。
- 電子カードリーダーと CCTV 監視を使用して、この場所へのアクセスを保護します。
- 物理的なハードウェアを、ロックされたゲージまたは物理キーのアクセス制御を備えたラックに入れます。

仮想インフラストラクチャのセキュリティ

仮想化を柔軟に使用して、仮想化されたオペレーティングシステムに複数の MID Server をインストールし、共有の物理ハードウェアにネットワークをインストールします。

仮想化された MID Server の不正なクローン作成を防ぐために、ハイパーバイザーおよび仮想インフラストラクチャ管理コンソールへのアクセスを保護する必要があります。

- 信頼できる少数の管理者によるハイパーバイザーおよび仮想インフラストラクチャ管理コンソールへのアクセスを制限します。
- ESX サーバーや VirtualCenter などの管理コンソールに対しては、内部の信頼できるネットワークのみ接続を許可します。
- VLAN を使用してネットワーク攻撃を防止します。
- ベンダーの仮想化強化ガイドで公開されているセキュリティガイドラインに従ってください。

オペレーティングシステムのセキュリティ

インスタンスに対する安全な認証のために、`config.xml` という名前の構成ファイルに記載された Now Platform ユーザー名とパスワードがどのように MID Server に格納されるかを学習します。

資格情報を不正アクセスから保護するために、セキュアで強化されたオペレーティングシステムに MID Server を展開する必要があります。

- オペレーティングシステムへのアクセスを、数人の信頼できる管理者に制限します。
- オペレーティングシステムのログを監視して、不正なアクセス、特に config.xml ファイルへのアクセスを検出します。このファイルには重要な MID Server 構成情報が含まれているからです。
- オペレーティングシステムのセキュリティパッチを最新のアンチウイルスソフトウェアで定期的にインストールし、アンチウイルス定義を定期的に更新します。
- MID Server を実行するには、最新の Java フレームワークが必要です。Java を定期的に更新します。
- 不要なサービスやアプリケーションを削除または無効化します。
- OS ファイアウォールをインストールして、許可されていないポートへのアクセスを制限します。
- ベンダーのオペレーティングシステム強化ガイドで公開されているセキュリティガイドラインに従ってください。

ネットワークセキュリティ

MID Server は SSL を使用してポート 443 でインスタンスと通信します。受信接続は必要ありません。

ネットワーク内の MID Server を適切に保護するには、次の手順を実行します。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

- 企業ファイアウォールの背後にある保護されたサーバーに MID Server をインストールして、インターネットから不正アクセスされないようにします。
- オペレーティングシステムとハードウェアの企業管理に必要な受信接続以外は受け入れないように、MID Server のファイアウォールを設定します。
- MID Server をホストするシステムが **install.servicenow.com** で ServiceNow ダウンロードサイトにアクセスできる必要があります。

  注:
  この URL は ServiceNow ダウンロードサイトを示しており、このトピックからはアクセスできません。

  MID Server のホストマシンは、そのサイトにアクセスしてインストーラーパッケージをダウンロードできる必要があります。60 分ごとに **install.servicenow.com** にアクセスして新しいバージョンが利用可能かどうかを確認し、利用可能な場合は自動アップグレードを実行します。MID Server のアップグレードは、インスタンスをアップグレードするときにも行われます。

ファイアウォール

MID Server からインスタンスや自動アップグレードサーバーへの送信ネットワークトラフィックを許可するようにファイアウォールを設定します。

ファイアウォールを設定するには、次の構文例を使用します。

- `<source IP> TO <instance_name>.service-now.com ON PORT 443`
- `<source IP> TO install.service-now.com ON PORT 443`

管理とマネージメント

このセクションでは、お使いの環境で MID Server を管理するためのセキュリティプラクティスとガイドラインについて説明します。

mid_server ロールを持つアカウントの作成

mid_server ロールを含むインスタンスにユーザーアカウントを作成します。

ユーザーアカウントを作成するときは、次のガイドラインに従ってください。

- MID Server のインスタンスで管理アカウントを使用しないでください。
- MID Server アカウントに対して、十分に長く複雑なパスワードを使用します。
- パスワードは、大文字、小文字、数字、および特殊文字を含めて 12 文字以上にする必要があります。
- インスタンス内の異なる MID Server に対して、一意のパスワードを持つ異なる MID Server アカウントを使用します。
- で有効にすることで、厳格な SOAP セキュリティ機能を使用して、すべてのテーブルをアクセス制御リスト (ACL) で保護 *`Enforce strict security on incoming SOAP requests`* します。 システムプロパティ > **Web** サービス.
- 組織のパスワードポリシーを満たす頻度で MID Server のパスワードを変更します。

注:
詳細については、「MID Server ユーザーの作成とロールの付与」を参照してください。

Windows ホストでの **MID Server** の設定

Windows ホストに MID Server をインストールすると、Windows サービスが作成されます。デフォルトでは、このサービスはローカル Windows システムアカウントとして実行されます。インス

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

トールが完了したら、新しく作成された Windows サービスを、Windows ホストで MID Server を実行するために必要な最小限の権限を持つアカウントに変更します。

1. 移動先 コンピュータ管理 > サービスとアプリケーション > サービス.
2. **[ServiceNow MID Server]** を右クリックし、[プロパティ] をクリックします。
3. ポップアップウィンドウで [ログオン] タブをクリックします。
4. [このアカウント **(This account)]** の横にあるラジオボタンをクリックします。
5. サービスを実行するアカウントのユーザー名とパスワードを適宜入力します。
6. **[OK]** をクリックします。
7. [サービス] ウィンドウで、**[ServiceNow MID Server]** を右クリックし、[再起動] をクリックします。
8. MID Server が正常に再起動し、インスタンスに接続できることを確認します。

Windows Discovery と **Orchestration** の資格情報

ターゲットシステムで、必要な最小限の権限を備えたローカルの Windows または Active Directory アカウントを設定します。ドメイン管理者の資格情報は、使用する必要がない場合があります。

次の製品ドキュメントのページには、使用が必要なアカウントのタイプと必要な権限に関するガイダンスが記載されています。

- Windows 資格情報
- Windows プローブと権限
- Discovery 用 Microsoft Just Enough Administration (JEA)

Linux Discovery と **Orchestration** の資格情報

検出とオーケストレーションを実行するときは、ターゲット Linux システムで制限付きの sudo 権限を持つ非ルートアカウントを使用します。

次のガイドラインを使用してください。

- Linux アカウントに対して、十分に長く複雑なパスワードを使用します。パスワードは、大文字、小文字、数字、および特殊文字を含めて 12 文字以上にする必要があります。
- sudo 権限を設定する場合、実行している Linux ディストリビューションによっては、実行可能なバイナリファイルへのローカルパスが異なる場合があります。「MID Server 特権コマンド」を参照してください。

MID Server ログイン資格情報の暗号化

デフォルトで、MID Server のログイン資格情報は、config.xml ファイル内で暗号化されます。

config.xml ファイルを編集してパスワードを指定するときは、次の構文を使用して、`encrypt="true"` 属性を確保してください。

```
<parameter name="MID.instance.username" value="MIDsrvadmin" />
```

```
<parameter name="MID.instance.password" encrypt="true" value="$ECUREpassw0rd"/>
```

注:
MID Server のログイン資格情報の暗号化は、物理セキュリティおよびネットワークセキュリティが不十分である危険なサーバーホストを置き換えるものではありません。config.xml ファイルに格納されているパスワードは、MID Server の初回起動時、または既存の MID Server の場合は再起動時に暗号化されます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

DH グループの最小サイズを 2048 ビットに設定

米国国立標準技術研究所 (NIST) は、2013 年以降、Diffie-Hellman (DH) 1024 ビットキーの使用を禁止しています。代わりに、DH グループの最小サイズを 2048 ビットに設定します。

1. インスタンスで、次の場所に移動します。 **MID** サーバー > サーバー.
2. この機能を無効にする MID Server の名前をクリックします。
3. MID Server 構成で、[構成パラメーター] の横にある [新規] ボタンをクリックします。
4. [MID Server 構成パラメーター] で、次のパラメーター設定を構成します。
   - パラメーター名 mid.ssh.dh_group_length_min
   - 値 2048

送信 SSL の無効化

Now Platform で SSLv2 および SSLv3 を無効にすることができます。このプロパティを設定すると、REST 要求や SOAP 要求などの送信接続を行うときに、MID Server は TLS を使用して強化されたセキュリティを利用します。

1. インスタンスで、次の場所に移動します。 **MID** サーバー > プロパティ.
2. 設定パラメーターを追加し、値を次のように設定します。
   - 名前 glide.outbound.sslv3.disabled
   - 値 true

弱いアルゴリズムの無効化

弱いアルゴリズムを無効にして、以前は機能していた、TLS 1.2 に準拠していない HTTP サーバーへの要求が失敗するようにすることができます。

次の構文を使用して、agent フォルダーの jre/lib/security/java.security ファイルを編集します。

jdk.tls.disabledAlgorithms=SSLv3, TLSv1, TLSv1.1, [その他の弱いアルゴリズム…]

注:
このファイルはアップグレード時に上書きされるため、アップグレードするたびにこのファイルを再更新するプロセスを実行する必要があります。

Powershell ユーザーは、Windows 管理者に問い合わせて、古いバージョンの TLS を無効にする必要があります。Powershell で使用されている TLS のバージョンの詳細については、[enum]::GetNames([Net.SecurityProtocolType]) コマンドを使用してください。

元に戻せる動作

「safe_overrides」または「no_db_override」のいずれかに分類されるシステムプロパティがあります。

安全なオーバーライド

これらのプロパティの値は、一度変更すると変えることができなくなります (元に戻すことはできません)。

注:
管理者は、安全なオーバーライドプロパティの名前を変更したり、削除したりすることはできません。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

属性	カテゴリ
デフォルトの拒否	アクセス制御
AJAXGlideRecord ACL チェックの有効化	アクセス制御
クライアント呼び出し可能スクリプトインクルードのプライバシー	アクセス制御
クライアント生成スクリプトサンドボックス	入力の検証
コレクションモードのオーバーライド (使用廃止)	セキュリティ包含リスト

DB オーバーライドなし

これらのプロパティの既存の値を変更またはオーバーライドすることはできません。

属性	カテゴリ
ファイルのダウンロード制限を有効にする	添付ファイル

廃止されたセキュリティプロパティ

これらのセキュリティプロパティは、以前のリリースで廃止されました。

コレクションモードのオーバーライド (使用廃止)

glide.whitelist.manager.collection_mode.override プロパティは、高度にカスタマイズされたインスタンスに下位互換性を提供するように設計されています。このプロパティでは、Calgary より前のバージョンで作成されたパッケージコールを使用していましたが、それ以降は廃止されました。

詳細情報

属性	説明
プロパティ名	glide.whitelist.manager.collection_mode.override
構成タイプ	システムプロパティ (/sys_properties_list.do)
Instance Security Center での構成	なし
目的	[コレクションモード (Collection Mode)] プロパティを無効にして、Java パッケージコールをインスタンスにインポートする場合のセキュリティギャップを解消します。
推奨値	false
機能への影響度	(低) セクション 10.6 の結果を確認して承認しているかぎり、影響はありません。インスタンスが確実に正しく機能するようにするには、本番環境に展開する前に非本番環境でテストします。
セキュリティリスク	(高) サーバー上のデータ取得またはオブジェクトアクセスという結果になるクライアント側 API 呼び出しは、セキュリティの観点から危険であると見なされます。機密オ

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

属性	説明
	ブジェクトへのアクセスを許可および制限するために検証してください。
参照	https://support.servicenow.com/kb_view.do?sysparm_article=KB0621483

SMTP 認証 (使用廃止)

glide.smtp.auth プロパティは、SMTP サーバーがユーザー名とパスワードの認証エントリを必要とするかどうかを指定していました。

詳細情報

属性	説明
プロパティ名	glide.smtp.auth
構成タイプ	システムプロパティ (/sys_properties_list.do)
Instance Security Center での構成	なし
目的	SMTP 認証の適用
推奨値	true
機能への影響度	(高) この修正では、コンテンツがメールの形式で配信される前に、外部メール サーバーへの認証が適用されます。自動化でメールコンテンツを配信するように設定されている場合は、プロパティを設定し、該当するユーザー名/パスワードを入力してメールサーバーにアクセスするまでは、影響が生じる可能性があります。
セキュリティリスク	(低) コンテンツを外部メールサーバーに送信する前に SMTP 認証を有効にします。認証は、常に、インスタンスとの間でトランザクションが発生する前に行う必要があります。
参照	メールプロパティ

JavaScript コンテンツアクセス制御の使用

アップグレードしたお客様は、JavaScript コンテンツアクセス制御を使用することで、インスタンス内のブロックされたサードパーティの JavaScript URL のリストを変更できます。

始める前に

アップグレードしたお客様には、テーブルへの読み取りおよび書き込みアクセス権があります。

新規のお客様ではすべてのレコードが非表示になります。 ServiceNow® サポートにお問い合わせください。

必要なロール：admin

手順

1. アプリケーションナビゲーターで、 sys_js_content_provider_rule.listを検索します。
2. [新規] をクリックします。
3. フォームのフィールドに入力します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

自動翻訳

JavaScript コンテンツプロバイダールール

フィールド	説明
アクティブ	選択するとルールがアクティブになるオプション。オフにすると、一致する他のルールがない場合に、[パス] の URL が許可されます。
パス	JavaScript ファイルへの絶対 URL。 **注:** すべてのパスに 4 つのバリエーションがあります。たとえば、/scripts/lib/jquery/jquery-1.8.2.min.js というパスは次の URL をブロックします。 ○ /scripts/lib/jquery/jquery-1.8.2.min.js ○ /scripts/lib/jquery/jquery-1.8.2.min.jsx ○ /lib/jquery/jquery-1.8.2.min.js ○ /lib/jquery/jquery-1.8.2.min.js
アクション	次の操作を行うオプション。 ○ 拒否：[パス] の URL またはそのバリエーションに対して、サーバーが **404 Not Found** 応答を返します。 ○ 許可：サーバーが、[パス] の URL またはそのバリエーションのファイルのコンテンツを返します。 ○ リダイレクト：サーバーが、[リダイレクトパス] フィールドで指定された代替ファイルの内容を返します。
アプリケーション	ルールのスコープを指定するオプション。デフォルトは [グローバル] です。 **注:** この機能は、スコープやアプリケーション、またはドメインに依存しません。
リダイレクトパス	リダイレクト先のパスを明確にするフィールド。 [アクション] を [リダイレクト]に設定すると、[パス] の URL への要求に対して、この URL の内容が代わりに提供されます。

4. [送信] をクリックします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

その他のセキュリティ強化リソース

Now Platform に関連するセキュリティコントロールの強化に関しては、他にも次のような情報源があります。

リソース	説明
セキュリティテストポータル	HI のセキュリティサービスポートフォリオ
KB0538598	顧客アプリケーションのペネトレーションテスト | ポリシーおよび手順
KB0546756	公開コンテンツ管理システム (CMS) アクセスの無効化
KB0550071	ServiceNow, Inc. インスタンスアクセス制御のレビュー
KB0550613	IP アドレス制限の識別と有効化
KB0550828	GlideAjax トランザクションの監査とレビュー
KB0550837	スクリプトサンドボックスの修復
KB0551031	パスワードリセット UI のセキュリティ修正
KB0552835	デモユーザーアカウントの修正
KB0529232	ServiceNow, Inc. Monitoring - 概要とインサイト
KB0564232	外部認証による ServiceNow, Inc. モバイルアプリの使用
セキュリティとリスク	ServiceNow, Inc. コミュニティ

ServiceNow® アクセス制御

SNC アクセス制御プラグイン (com.snc.snc_access_control) を有効にして、どのカスタマーサービス & サポート従業員がインスタンスにいつアクセスできるかを制御できます。

ServiceNow アクセス制御の詳細

ServiceNow アクセス制御を有効にする

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

アクセス制御の機能 ServiceNow® について説明します。

アクティブな ServiceNow® アクセス制御。

ServiceNow アクセス制御を設定する

アクセス制御の構成 ServiceNow® 方法を理解します。

監査ログ

アクセス制御監査ログについて学習し、 ServiceNow® 確認します。

自動翻訳

ServiceNow® アクセス制御の詳細

SNC Access Control プラグイン (com.snc.snc_access_control) を有効にして、どの カスタマーサービス & サポート 従業員がインスタンスにいつアクセスできるかを制御できます。

初めてプラグインを有効にすると、カスタマーサービス & サポート の従業員はインスタンスにログインできません。現在ログインしている カスタマーサービス & サポート の従業員はログインしたままになります。特定の SNC 従業員またはすべての従業員にアクセス権を付与するレコードを SNC アクセス制御テーブルに作成します。

プラグインにより、カスタマーサービス & サポートの担当者が特別な許可なしにインスタンスにアクセスできないようにします。ただし、製品をサポートおよび管理し、使用状況を確認する能力を持つ他の認定 ServiceNow 運用担当者は、基盤となるインフラストラクチャで管理アクションを実行する必要があります。このインフラストラクチャには、SaaS を構成する他のインフラストラクチャコンポーネントの中でも、サーバーとデータベースが含まれます。このアクセス方法は監査可能および追跡済み。

このプラグインを使用すると、特別な権限なしにインスタンスへのアクセスを制限できるため、サポートのサービスレベルと可用性 SLA に影響を与える可能性があります。可用性 SLA は、サポートスタッフ担当者がインスタンスへのアクセスを許可された時間から測定されます。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ログインセキュリティ

権限のあるカスタマーサービス & サポートの従業員によるインスタンスへのログインのセキュリティは、安全なサーバーで生成された暗号化されたトークンを使用して確保されます。適切に認証されたカスタマーサービス & サポートの従業員のみがインスタンスへのアクセスを許可されます。SNC アクセス制御プラグインがない場合、セキュリティサーバーは hi.service-now.com でアクセス権を適用します。プラグインが有効な場合、暗号化されたログイントークンは、これらのレコードで定義された条件を使用して、プラグインで提供されるアクセスリストの名前と一致する必要があります。この認証方法により、カスタマーサービス & サポートの従業員の誰がいつインスタンスにアクセスできるかを正確に判断できます。

このシステムに選択されたアーキテクチャには、インスタンスのセキュリティを強化するように設計されたいくつかの機能があります。

セキュリティサーバー

セキュリティサーバーは、ServiceNow セキュリティ担当者のみがアクセスできる、ロックダウンされた Linux ホストです。このサーバーは、ログイントークンを生成するために必要な重要な秘密暗号化キーにアクセスできる唯一のシステムです。このコンパートメント化 (標準的なセキュリティプラクティス) を使用することで、万一、攻撃者が HI インスタンスを侵害した場合でも秘密キーが保護されます。

合成ユーザー

権限のあるカスタマーサービス & サポートの従業員がインスタンスにログインできるようにするインスタンスの機能では、そのインスタンスにアカウントをプロビジョニングする必要はありません。プロビジョニングされたユーザーレコードはなく、永続的な資格情報もありません。代わりに、カスタマーサービス & サポートの従業員のログオンごとに合成ユーザーが作成されます。このユーザーはメモリ内にのみ存在し、継続的な権限を提供しません。SNC アクセス制御プラグインが有効になっている場合、いつでもカスタマーサービス & サポートの従業員の許可を解除できます。

トークン

セキュリティトークンは、インスタンスと特定のカスタマーサービス & サポートの従業員に固有です。さらに、トークンを生成するメカニズムは、代理操作されたユーザーではなく、HI への実際のカスタマーサービス & サポート従業員ログインでのみ機能します。セキュリティトークンが生成されると、特定のカスタマーサービス & サポートの従業員のみがインスタンスにログインできます。

時間制限

セキュリティトークンは、生成されてから 4 時間後に期限切れになります。この有効期限は、この短い期間にのみ使用できるハイジャックされたトークンのユーティリティを制限します。

ログ記録

カスタマーサービス & サポートの従業員によるインスタンスへのログインは、ログインイベントとして記録されます。

- ログインしているカスタマーサービス & サポートの従業員が実行したすべてのアクションは、データベースのトランザクションログに追加されます。
- また、ほとんどの ServiceNowの従業員がアクセスできないファイルシステムのインスタンスログにも追加されます。
- ユーザー名はすべて @snc で終わるため、カスタマーサービス & サポートの従業員のログインとアクションは簡単に識別できます (例：frodo.baggins@snc)。

これらのアクションにより、従業員以外のアクセスに対して、使いやすく、堅牢で信頼性の高いセキュリティログ記録が提供されます。

自動翻訳

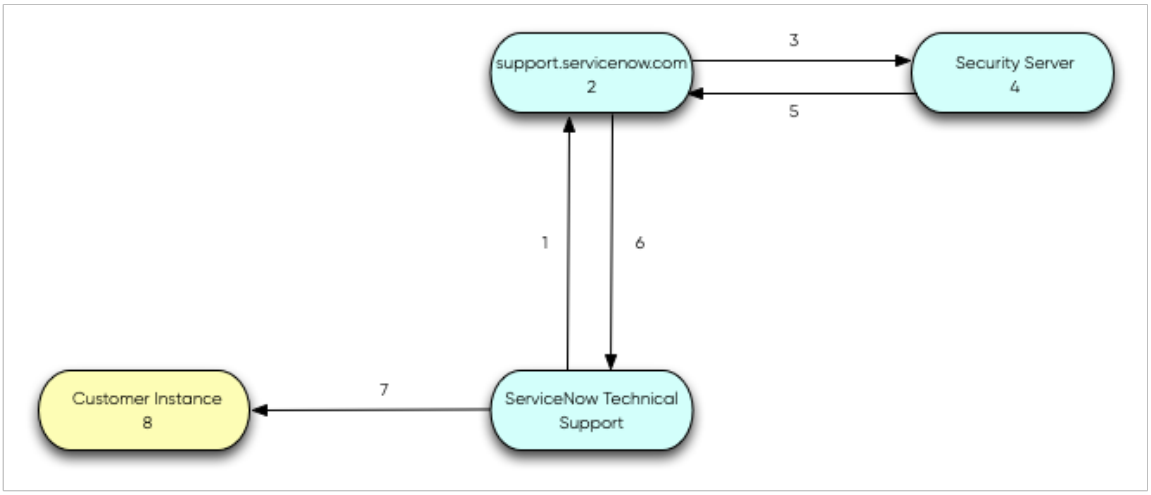
© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

セキュリティ処理フロー

カスタマーサービス & サポートの従業員がインスタンスにログインする場合、セキュリティ処理フローは次のようになります。

1. カスタマーサービス & サポートの技術者が hi.service-now.com からインスタンスへのログインを要求します。
2. HI は、技術者がインスタンスへのアクセスを許可する適切なロールを持っていることを確認します。
3. ユーザーが適切なロールを持っている場合、HI はアクセス要求をセキュリティサーバーに送信します。
4. セキュリティサーバーは、要求が HI IP アドレスから送信されたことを確認し、要求 (ユーザー、ロール、および要求者の IP アドレス) を評価します。要求が有効な場合、セキュリティサーバーはその要求を承認してトークンを構築します。このトークンには、ユーザー名、ロール、インスタンス ID、および時刻 (4 時間のトークン有効期間の開始) が含まれています。最後に、セキュリティサーバーは秘密暗号化キーを使用してトークンを暗号化します。
5. セキュリティサーバーが暗号化されたトークンを HI に送信します。
6. HI はサポート技術者のブラウザにトークンを送信します。
7. サポート技術者のブラウザは、`@snc` で終わる特別なユーザー名を使用して、インスタンスへのログインを開始します。
8. インスタンスは公開鍵を使用してトークンを復号化します。トークンを検証するために、インスタンスはトークンを前のステップで指定されたユーザー名、インスタンス ID、および許可された時間枠と照合します。SNC アクセス制御プラグインが有効になっている場合、インスタンスはユーザーが次の条件を満たしていることを確認します。
   - リスト済み
   - 有効
   - 現在の期間内にインスタンスにアクセスするように設定されています。
9. ユーザーが認証されると、インスタンスは指定されたロールを持つ合成ユーザーをメモリ内に作成します。このユーザーは、時間制限が切れるか、ユーザーがログオフするか、またはインスタンスが再起動された後は存続しません。

ServiceNow セキュリティアクセスプロセスフロー



自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

監査ログ

次のログ記録は、カスタマーサービス & サポートの従業員によるログインとアクティビティを追跡します。

- イベントログ：イベントログには、インスタンスへのすべてのカスタマーサービス & サポートのログインが表示されます。
- トランザクションログ：トランザクションログには、ログの削除を含むインスタンスのすべてのアクティビティが表示されます。

注:
このプラグインの詳細については、「インスタンスセキュリティ強化設定」の「SNC アクセス制御プラグイン」を参照してください。

ServiceNow® アクセス制御の有効化

SNC Access Control プラグイン (com.snc.snc_access_control) のアクティブ化を要求できます。

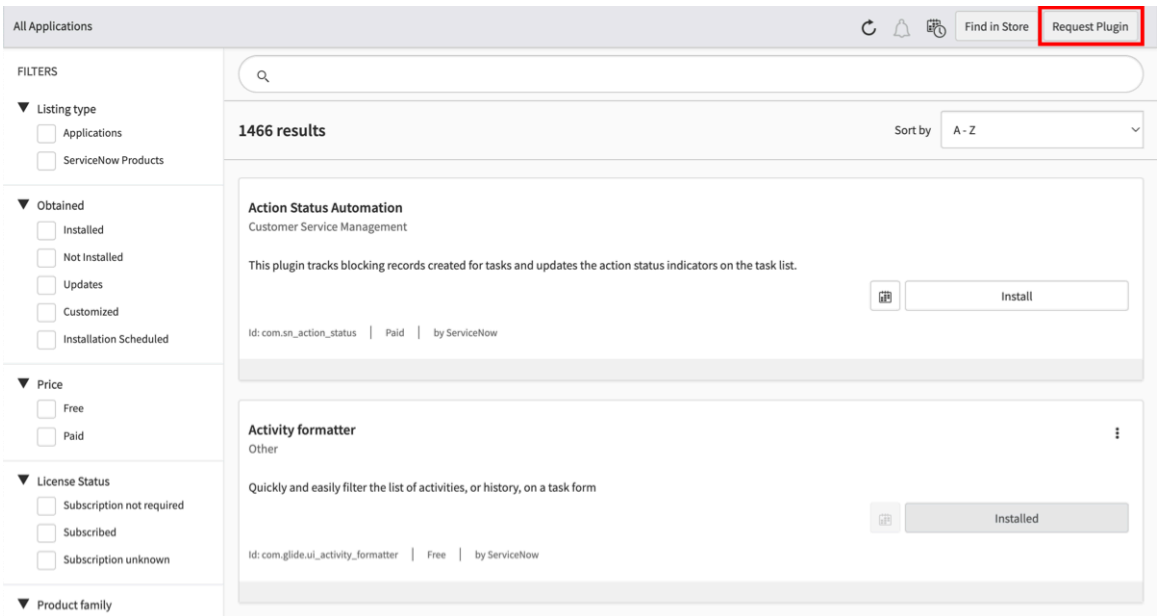
始める前に
必要なロール：admin

このタスクについて
プラグインを要求するには、次の 2 つの方法があります。

- Service Catalog Now Support に直接アクセスするには、次の項目を選択します。 すべて > サービスカタログ > プラグインをアクティブ化 オン Now Support。
- 次の手順に従い、インスタンスの [すべてのアプリケーション] ページから Now Support サービスカタログにアクセスします。

手順

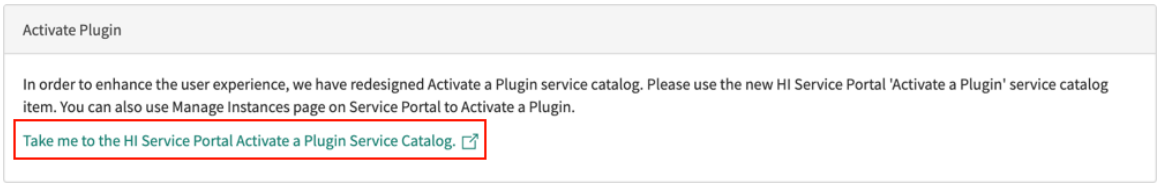
1. 移動先 すべて > システムアプリケーション > 利用可能なすべてのアプリケーション > すべて。
2. [すべてのアプリケーション] ページで [プラグインの要求] をクリックして、Now Support で [プラグインをアクティブ化] フォームを開きます。



自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

3. Now Support で、Now Support サービスポータル サービスカタログ にアクセスするリンクを選択します。



4. インスタンスを選択します。
5. [アクション] > [プラグインのアクティブ化] を選択します。
6. [プラグインのアクティブ化] フォームで、次の情報を入力します。

[プラグインのアクティブ化] フォーム

フィールド	説明
ターゲットインスタンスは何ですか	プラグインをアクティブ化するインスタンス。
どのプラグインをアクティブ化しますか	アクティブ化するプラグインの名前です。 **注:** 必要なプラグインが表示されない場合、または OEM またはオンプレミスのインスタンスでプラグインをアクティブ化している場合は、[探しているプラグインが表示されていません **(Plugin I'm looking for is not listed)]** チェックボックスをオンにして、プラグインの名前を入力します。
メンテナンスの日時を選択 (Select Maintenance Date and Time)	プラグインをアクティブ化する日時。 **注:** プラグインは、米国太平洋標準時で、毎営業日の朝と夕方の 2 回のバッチでアクティブ化されます。特定の時刻にプラグインをアクティブ化する必要がある場合は、[理由/コメント **(Reason/ Comments)]** フィールドに要求を入力します。

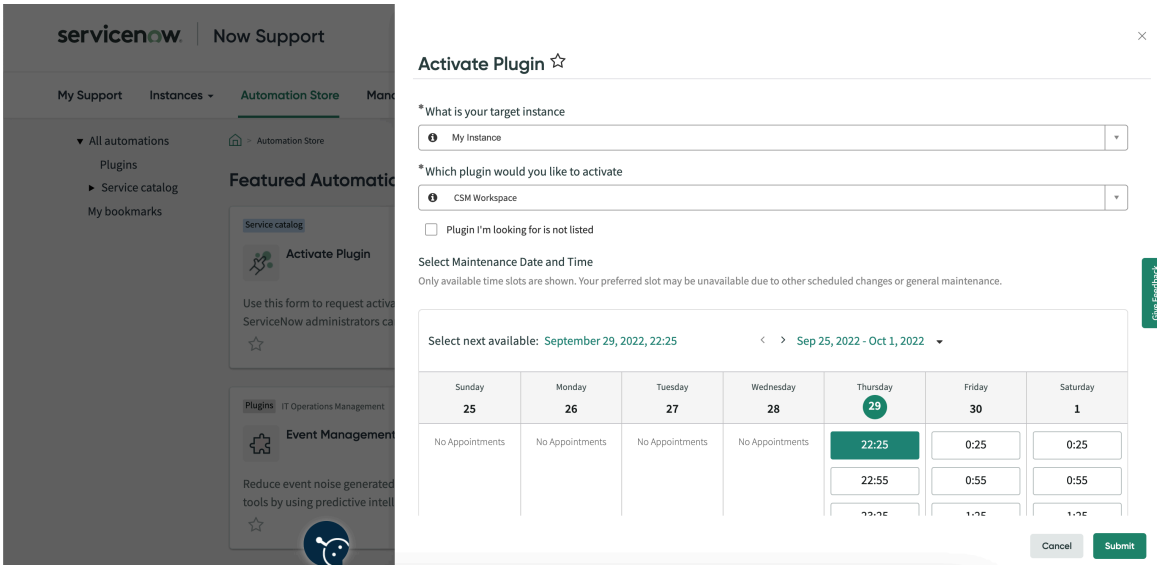
Example

たとえば、 [自分のインスタンス (My Instance)] という名前のインスタンスで CSM Workspace プラグインをアクティブ化するには、次のフォームを参照してください。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

[プラグインのアクティブ化] フォーム



7. [送信] を選択します。
プラグインの要求の詳細については、次を参照してください。 の Service Catalog [KB0751715] 記事からのプラグインの要求 Now Support ナレッジベース。

ServiceNow® アクセス制御の構成

アクセス制御レコードを設定して、インスタンスにログインする権限を持つ 1 人以上の カスタマーサービス & サポート の従業員を指定します。

始める前に
必要なロール：管理者

このタスクについて

注:
SNC アクセス制御 (com.snc.snc_access_control) プラグインにより、カスタマーサービス & サポートの担当者が特別な権限なくインスタンスにアクセスできなくなります。ただし、製品をサポートおよび管理する権限を持つ ServiceNow 運用担当者は、基礎となるインフラストラクチャで管理アクションを実行する必要があります。このインフラストラクチャには、SaaS を構成する他のインフラストラクチャコンポーネントの中でも、サーバーとデータベースが含まれます。このアクセス方法は監査可能および追跡済み。

このプラグインを使用すると、特別な権限なしにインスタンスへのアクセスを制限できるため、サポートのサービスレベルと可用性 SLA に影響を与える可能性があります。可用性 SLA は、サポートスタッフ担当者がインスタンスへのアクセスを許可された時間から測定されます。

手順

1. 移動先 すべて > システムセキュリティ > **SNC** アクセス制御.

2. [新規] をクリックします。

3. フォームフィールドに入力します (表を参照)。

4. [送信] をクリックします。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

SNC アクセス制御

フォームのフィールド	説明
名前	このインスタンスにログインする権限を持つ各カスタマーサービス & サポートの従業員の名前。 ○ 名前を小文字の firstname.lastname として、ピリオドで区切って表します (例：john.smith)。各名前には、*support.servicenow.com* で対応するユーザーレコードが必要です。 ○ 複数のカスタマーサービス & サポートの従業員がこのインスタンスにログインする権限を持っている場合は、複数の名前を入力し、それらをカンマで区切ります。 ○ カスタマーサービス & サポートの従業員全員がインスタンスにアクセスできるようにするには、名前の代わりにアスタリスク (*) を入力します。 ○ インスタンスへのカスタマーサービス & サポート従業員のアクセスを制限する場合は、[名前] フィールドの値にアスタリスク (*) を使用しないでください。
理由	アクセス権を付与する理由を説明する、分かりやすいフィールド。このフィールドはオプションです。
開始	指定されたカスタマーサービス & サポートの従業員がログインアクセス権を持つ期間の開始日時を指定します。このフィールドは必須です。
終了	指定されたカスタマーサービス & サポートの従業員がログインアクセス権を持っている期間の終了日時を指定します。このフィールドは必須です。
有効	この権限レコードがアクティブかどうかを制御します。デフォルトは [アクティブ] です。

監査ログ

次のログ記録は、ServiceNowの従業員のログインとアクティビティを追跡します。

イベントログ	イベントログには、カスタマーインスタンスへのすべての ServiceNow ログインが表示されます。
トランザクションログ	トランザクションログには、ログの削除を含む、インスタンスのすべてのアクティビティが表示されます。

仮想プライベートネットワーク (VPN)

仮想プライベートネットワーク (VPN) を使用して、インターネット経由でインスタンスを外部データソースと統合します。

詳細	有効化

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

仮想プライベートネットワークの機能とビジネス価値について説明します。

仮想プライベートネットワークを有効にします。

構成

仮想プライベートネットワークの構成方法について説明します。

自動翻訳

仮想プライベートネットワーク **(VPN)** の詳細

仮想プライベートネットワーク (VPN) を使用して、インターネット経由でインスタンスを外部データソースと統合します。

ライトウェイトディレクトリアクセスプロトコル (LDAP) や HTTPS などの暗号化されたプロトコルを使用する統合を設定する場合は、インターネットを転送メカニズムとして使用することをお勧めします。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

ただし、データセンターとビジネスネットワーク間でサイト間インターネットプロトコルセキュリティ (IPSEC) 仮想プライベートネットワーク (VPN) 接続の使用を指示するセキュリティまたはネットワークアーキテクチャ要件がある場合があります。VPN は、インスタンスとネットワーク間で必要な暗号化通信をサポートします。

このビデオでは、会社の各インスタンスの IP アドレスを見つける方法について説明します。

自分の IP 情報

VPN 接続

ServiceNowVPN インフラストラクチャは、VPN の終了ポイントとして機能する Cisco 適応型セキュリティアプライアンス (ASA) デバイスのペアを使用します。

インスタンスとネットワーク間の VPN は、既存のネットワークハードウェアを使用して通信をサポートします。ハードウェアをインストールする必要はありません。構成は顧客ごとに異なるため、インスタンスには柔軟な VPN ソリューションが提供されています。インスタンスには、チェックポイント、Juniper、Nortel、およびその他の IPSEC VPN 対応デバイスへのトンネルが構築されています。

インスタンスとネットワーク間の VPN 接続は、ネットワークへの暗号化されたトラフィックフローをサポートするために作成されます。多くの場合、VPN を使用する統合では、基礎となるプロトコルの一部として暗号化は行われません。たとえば、VPN 経由の LDAP とインターネット経由の LDAPS、VPN 経由の HTTP とインターネット経由の HTTPS などです。

ネットワークでは、受信から ServiceNow への統合またはエンドユーザーから ServiceNow へのトラフィックが VPN 接続を走査することは許可されていません。この制限付き通信には、プラットフォームへのエンドユーザーアクセス、プラットフォームの管理、Web サービスの統合、および MID Server を使用するように設定されたその他の統合が含まれます。インスタンスへのこのような受信通信はすべて、HTTPS を使用してインターネット経由で実行する必要があります。この設定では、暗号化された通信チャネルが提供されます。暗号化チャネルは、IP アクセス制御とともに、このトラフィックフローのセキュリティ要件を満たしています。

VPN 通信用のアドレス

内部 ServiceNow ネットワークまたはネットワーク内の別の内部 IP アドレススキームとの競合または重複を防ぐために、暗号化ドメイン内のすべてのトンネルトラフィックは、トンネルの両側で RFC-1918 以外のアドレスを使用する必要があります。

ServiceNow は、ネットワークに対するクエリのソースの単一 IP アドレスを提供します。インスタンスと統合している各ホストのネットワークアドレス変換 (NAT)、非 RFC-1918 アドレスを指定する必要があります。このようなパブリックアドレスは組織が所有する必要があります。サードパーティのアドレスはトンネル内で使用できません。また、暗号化ドメインに VPN ピアの IP アドレスを含めることはできません。

冗長トンネル

次の 2 つの方法でトンネルの冗長性を構築することができます。

- 両方のピアの背後で同じ暗号化ドメインを使用する。これが推奨される方法です。
- 各ピアの背後で異なる暗号化ドメインを使用する。

最初の方法では、各ピアの背後に同じ NAT アドレスを指定し、そのアドレスを使用してサーバーへの接続パスを作成する必要があります。サーバーへのパスは、同じ物理マシンにすることも、同じサービスを提供するミラーにすることもできます。この方法では、プライマリトンネルとセカンダリトンネルのどちらがアクティブであるかに関係なく、インスタンスは同じ IP アドレスを使用してサーバーに接続します。複数のサーバーがある場合は、追加のサーバーでもこの同じスキームに従います。この方法はユーザーにとって最も透明性が高いため、推奨されます。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

2 番目の方法では、インスタンスを構成して冗長性を持たせる必要があります。たとえば、LDAP にトンネルを使用する場合は、インスタンスに冗長化した LDAP サーバーを構築することができます。この方法では、インスタンスがセカンダリサーバーに接続しようとする前に、最初に設定された LDAP サーバーへの接続がタイムアウトする必要があります。このような追加の時間遅延があるため、最初のオプションが達成できない場合にのみこのソリューションを実装してください。また、インスタンスですべてのサービスに冗長性を提供できるわけではないためご注意ください。LDAP 以外のものに VPN トンネルを使用しているために冗長性が必要な場合は、複数のアドレスに対応できる構成であることを確認するか、上記の最初のオプションを参照してください。

VPN の使用の代替

この代替手段は、インスタンスを ServiceNow データセンターのリソースに接続するより簡単な方法とより優れた暗号化を提供します。また、VPN トンネルに問題がある場合にユーザーがインスタンスを使用できなくなるといった、VPN のダウンタイムによって発生する可能性のある問題を回避できます。

Single Sign-on と MID Server

VPN を使用して LDAP サーバーをインスタンスに接続するのではなく、認証用の Single Sign-on (SSO) とユーザーデータの同期用の MID Server を組み合わせて使用することを検討してください。LDAP 以外の統合の場合は、証明書ベースの暗号化を使用することを検討してください。

MID Server で LDAP リスナーを使用すると、ユーザーテーブルをほぼリアルタイムで同期できます。

このアプローチの利点は、ファイアウォールの穴、ルート、VPN トンネル、またはその他の特別なネットワーク設定を構成して維持する必要がないことです。SSO/MID Server ソリューションは、完全な LDAP 統合を実現するための最も柔軟かつ安全でコスト効率の高い方法です。

LDAP over SSL

VPN トンネルを使用する別の方法として、インターネット経由で直接 LDAP Over SSL (LDAPS) を設定する方法があります。選択したインスタンスのソースアドレスと宛先ポートのみを使用して、読み取り専用のドメインコントローラーを構成し、DMZ 内のインスタンスをロックすることができます。LDAP のポートはインスタンスで設定できるため、必要に応じてポートアドレス変換 (PAT) を実行できます。LDAPS では、暗号化されたチャネルを介してインスタンスにアップロードされる証明書を制御します (「インスタンスへの証明書のアップロード」を参照)。証明書がないとパケットを暗号化または復号化できません。

このアプローチの利点は、より強力な暗号化と復号化のメカニズムが提供されることです。パスワードと同様に、VPN は調整された事前共有キーを使用して、インターネット上の 2 つのピア間のトラフィックを暗号化および復号化することができます。LDAPS は、アプリケーションレイヤーでエンドツーエンドの長い暗号化パスを提供し、IPSec トンネルが使用する事前共有キーよりもはるかに複雑な証明書を提供します。

VPN セットアップ

VPN 要求が送信されてから、通常、1 週間以内に VPN 構築が完了します。インスタンスと組織の冗長性の要件に対応するために、2 ～ 4 つの VPN がプロビジョニングされます (アクティブサイトからアクティブサイトへ、またはアクティブサイトから DR サイトへなど)。

暗号化ドメインをできるだけ限定することをお勧めします。暗号化ドメインには、統合に必要な特定のホストのみを含めることが理想的です。大きな暗号化ドメインでは、ルーティングの不一致が発生する可能性があります (VPN とインターネット)。

自動翻訳

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。

VPN を作成するために、インスタンスでは次のことが行われます。

1. 各データセンターから VPN ピアとホストアドレスが提供されます。
2. 2 つのデータセンターからネットワークへの必要な VPN 接続が構築されます。冗長性と災害復旧 (DR) の要件に対応するために、VPN を 2 つのデータセンターから 2 つのネットワークにプロビジョニングすることができます。

インスタンスでは、複数の地理的リージョンまたは子会社に接続する目的で、顧客のネットワークに複数の VPN トンネルを構築することはできません。複数の VPN トンネルを持つのではなく、独自の内部ネットワーク内でサイト間ルーティング、トラフィック分散、またはトラフィックシェーピングを実行する必要があります。

VPN サービスのアクティブ化

プロビジョニング、変更、または一般的な質問を含むすべての VPN 要求に Service Catalog VPN 要求フォームを使用します。

始める前に

必要なロール：管理者

手順

1. https://support.servicenow.com/now?draw=case に移動します。
2. [オートメーションストア] タブを選択します。
3. 左側のツリーを使用して移動 すべての自動化 > **Service catalog** > クラウドインフラストラクチャ.
4. **[VPN** 要求] を選択します。
5. 適切な VPN 要求タイプを選択します。
6. 質問に回答します。
   質問は、選択した要求タイプによって変わります。
7. [送信] をクリックします。

タスクの結果

要求が送信されると、ServiceNow はネットワークエンジニアと協力して、VPN が正常にトラフィックを通過していることをテストし、検証します。質問に適切なタイミングで回答できるように、このプロセス中に VPN に関する質問に対処してください。

VPN 通信用のアドレスの構成

内部 ServiceNow ネットワークまたは別の顧客の内部 IP アドレススキームとの競合または重複を防ぐために、インスタンスでは、暗号化ドメインのすべてのトンネルトラフィックにおいてトンネルの両側で非 RFC 1918 アドレスを使用する必要があります。

始める前に

必要なロール：管理者

このタスクについて

インスタンスは、ネットワークに対するクエリのソースの単一 IP アドレスを提供します。

手順

インスタンスと統合している各ホストのネットワークアドレス変換 (NAT)、非 RFC-1918 アドレスを指定します。

© 2025 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは 米国および/またはその他の国における ServiceNow, Inc. の 商標または登録商 標です。
その他の会社名と 製品名は、関連する各会社の商標である 可能性があります。