概要

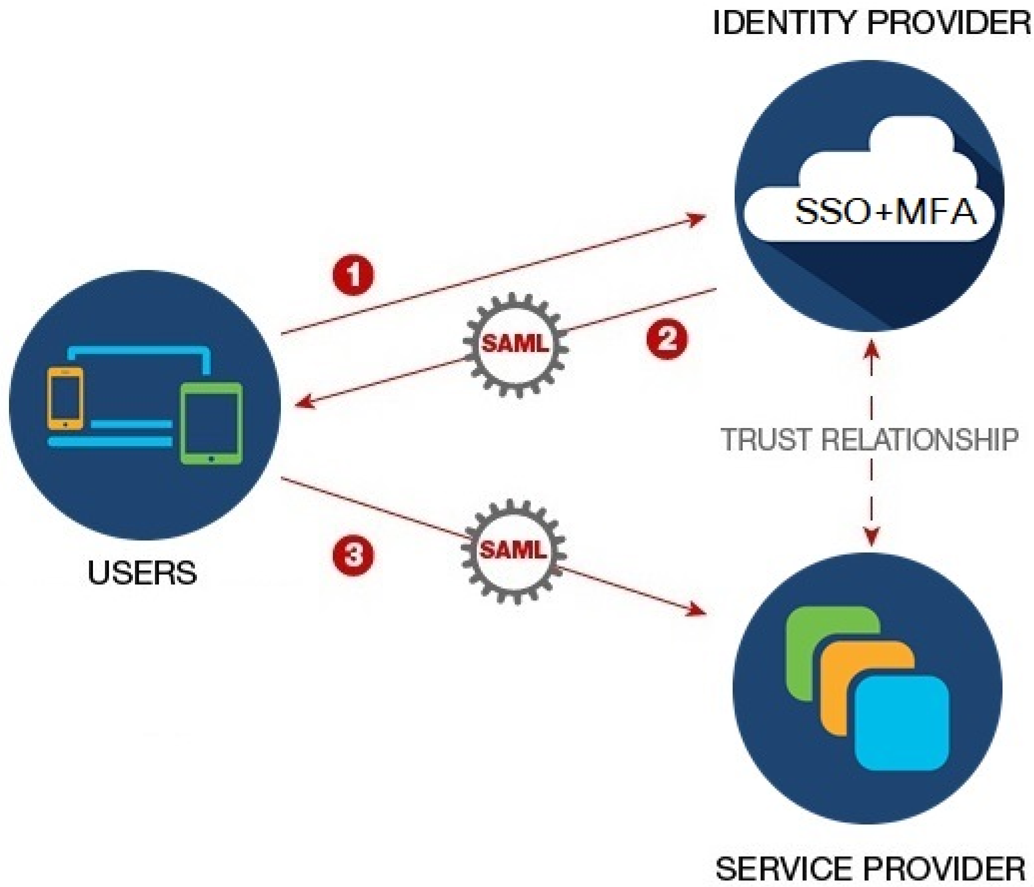
重要 **Enterprise Manager は廃止されました。**Security Cloud Control を使用して ID プロバイダーの統合を管理できるようになりました。詳細については、ID プロバイダー統合ガイドを参照してください。

既存の ID プロバイダー統合データはすべて、Security Cloud Control を介して使用できます。

概要

セキュリティ アサーション マークアップ言語（SAML）を使用して、独自またはサードパーティの ID プロバイダー（IdP）を Cisco Security Cloud Sign On と統合できます。SAML は、ID プロバイダー（IdP）とサービスプロバイダー（SP）の間で認証および許可データを交換するための XML ベースのオープン標準です。ここでのサービスプロバイダーは Security Cloud Sign On です。統合すると、ユーザーはシングルサインオンのクレデンシャルを使用して Security

Cloud Sign On にサインインできるようになります。



多要素認証の要件

Security Cloud Sign On では、すべてのアカウントに Duo 多要素認証が必要です。SAML（セキュリティ アサーション マークアップ言語）を使用して に独自の ID プロバイダーを統合するお客様は、Duo MFA をオプトアウトできます。

Duo MFA に登録すると、ユーザーはオプションで Google Authenticator に登録できます。Google Authenticator に登録すると、その後のサインオンは Google Authenticator チャレンジのみになり、Duo MFA チャレンジは表示されません。

Cisco Customer Identity または Microsoft によるフェデレーションサインオン（Security Cloud Sign On のページの [他のログインオプション（Other login options）]）を使用する場合、これと同じポリシーが適用されます。

既存の IdP 統合を使用しているお客様

このガイドで説明しているセルフサービスツールで作成されていない Security Cloud Sign On との IdP 統合がある場合、このツールを使用して既存の構成を更新することはできません。エンタープライズ設定ウィザード統合について次の設定を変更する必要がある場合は、Cisco TAC でケースをオープンする必要があります。

- SAML シングルサインオン URL またはエンティティ ID URI
- X.509 署名証明書
- 多要素認証（MFA）設定

翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。