# Cisco Secure Access - IDPによるSAML証明書の更新(Microsoft Entra ID)

## 内容

## お問い合わせ内容

Cisco Secure Accessのアイデンティティプロバイダー(IdP)としてMicrosoft Entry ID SAMLを使用したSSO認証を使用すると、SAML検証証明書の有効期限が近づいています。

組織は、認証の中断を回避するために正しい証明書の更新プロセスを理解し、Entry ID SAML証明書の更新時に新しいシングルサインオン構成をSecure Accessで作成する必要があるかどうかを判断する必要があります。

## 環境

- SSO認証が設定されたCisco Secure Access
- アイデンティティプロバイダーとしてのMicrosoft Entra ID SAML
- 有効期限が近いSAML検証証明書
- SWG(Secure Web Gateway)およびZTNA(Zero Trust Network Access)用の既存のSSO設定

## 解決策

### ステップ1 – 証明書の更新の検出

- アイデンティティプロバイダー(IdP)は、SAML署名証明書を更新または口ーテーションします。
- これは通常、証明書の有効期限が近づくと発生します。

## 手順2：更新されたIdPメタデータの取得

- IdPから新しいIdPメタデータXMLまたは新しい署名証明書を工クスポートします。

## ステップ3：証明書変更の確認

証明書が実際に変更されたことを確認します。

チェック:

- 拇印
- 有効期限
- Issuer

これにより、SPが正しい証明書で更新されます

## サービスプロバイダー構成の更新

Cisco Secure Access Dashboardにログインし、設定を更新します。

Connect - User and Groupsの順に移動します。

Configuration Managementをクリックします

SSO認証：SSO認証プロファイルを編集します。新しい証明書を使用してメタデータファイルをアップロードするか、手動設定の場合は証明書をアップロードします。

## ステップ5：設定の保存と適用

- 更新した設定を保存します。

## 手順6:SSO認証の検証

SSOログインテストを実行します。

# 原因

アイデンティティプロバイダー(IdP)署名証明書は、サービスプロバイダーがSAMLアサーション署名を検証するために使用します。IdPが証明書を更新する場合、SPは信頼できる証明書を更新して、認証要求の検証を続行する必要があります

# 関連コンテンツ

- Cisco Secure Access - SAMLシングルサインオンの概要と設定
- Cisco Secure AccessのSAML SSOの設定（Microsoft Entra IDの例）
- シスコのテクニカルサポートとダウンロード

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。