

# セキュアアクセスのためのSecurity Assertion Markup Language(SAML)証明書の更新 (年間措置が必要)

## 内容

---

[はじめに](#)

[問題](#)

[解決方法](#)

[Azure SAML証明書の設定](#)

[関連情報](#)

---

## はじめに

このドキュメントでは、セキュアアクセスのSAML証明書の更新プロセスについて説明します。

## 問題

有効期限 (毎年6月に期限切れとなる期間) の前に、新しいSecure Access Security Assertion Markup Language(SAML)証明書でアイデンティティプロバイダー(IdP)を更新する必要があります。以下に示すセキュアアクセスSAMLメタデータURLをモニタするようにIDPが設定済みである場合を除き、SAMLユーザ認証の失敗やこれらのユーザのインターネットアクセスの喪失を回避するために、この証明書を更新する必要があります。

## 解決方法

ステップ1: 確認SAML IDPが署名の検証を要求した場合、このオプションが無効になっている場合は、それ以上の操作は必要ありません。残りのプロセスを省略して、通常のSAMLサービスの使用を続行できます。

ステップ2:SAML IDPが署名の検証を要求する場合は、[Secure Access Documentation Page](#) -> Security Notices -> Security Advisories, Responses and Notices ->(Secure Access Notification - SAML Authentication Certificate Expiring)から新しい証明書をダウンロードします。

ステップ3:SAML IDPにログインし、現在のSAML証明書を置き換えます。

## Azure SAML証明書の設定

これは、Azure SAML IDP証明書の置き換えの例です。

ステップ1: [Azure Portal](#)にログインします。



ステップ4：検証証明書オプションを編集します。

ステップ5:([Secure Access Documentation Page](#))で参照されているアナウンスにある新しいSAML証明書をアップロードします。

## Verification certificates



ⓘ Requiring verification certificates will impact certain admin and end-user experiences, such as the Single sign-on testing feature, and the My Apps and M365 app launcher experiences. [Learn more](#)



Verification certificates are used to verify requests coming from this application to Microsoft Entra ID.

[Learn more](#)

Require verification certificates

Allow requests signed with RSA-SHA1

[↑](#) Upload certificate

Thumbprint	Key Id	Start date	Expiration date	
43C5538D5E386F6CF372BC4...	3367a479-945c-46f9...	5/13/2024, 2:01 AM	5/13/2025, 2:00 AM	...

## 関連情報

- [セキュアアクセスに関する文書](#)
- [テクニカル サポートとドキュメント - Cisco Systems](#)

## 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。