

セキュアアクセスSAML VPN認証証明書 (サービスプロバイダー証明書) の更新

内容

[はじめに](#)

[背景説明](#)

[前提条件](#)

[要件](#)

[シスコセキュアアクセスダッシュボード](#)

[MicrosoftエントリID \(Microsoft Azure\)](#)

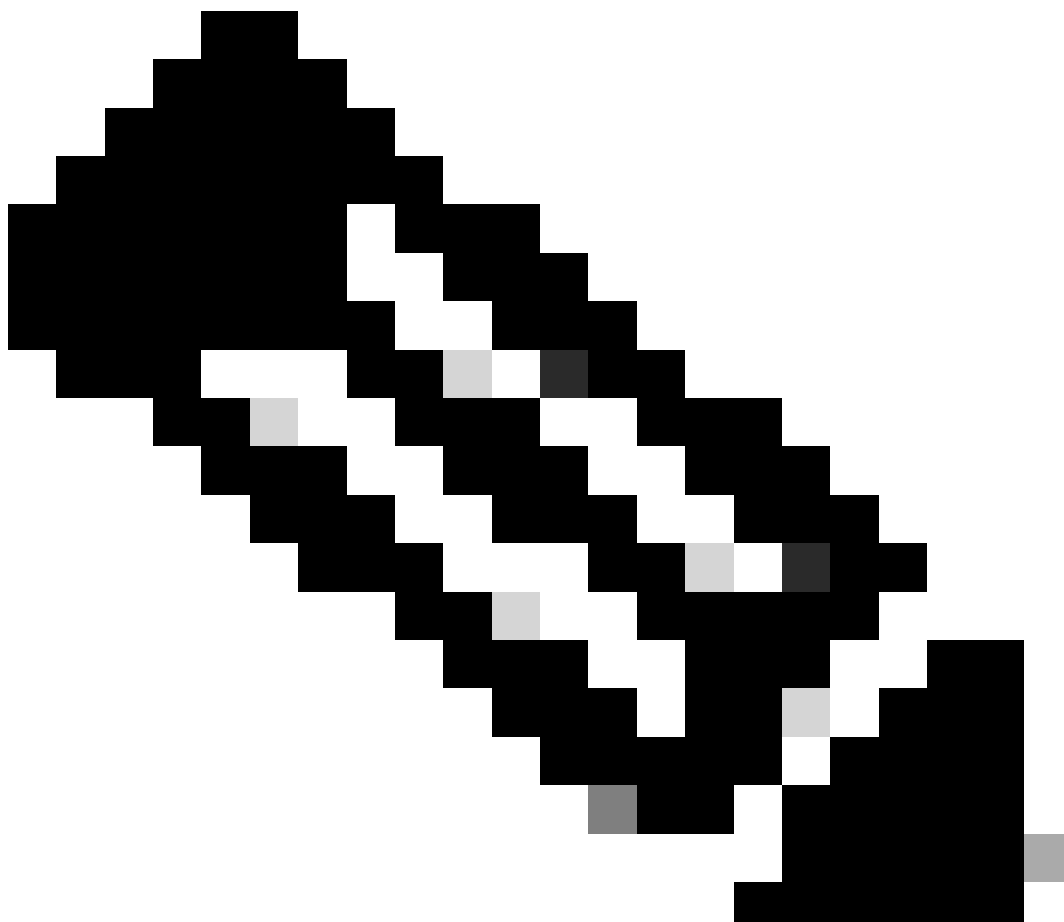
はじめに

このドキュメントでは、アイデンティティプロバイダー(IdP)証明書を新しいセキュアアクセスサービスプロバイダー証明書で更新するために必要な手順について説明します。

背景説明

バーチャルプライベートネットワーク(VPN)の認証に使用されるCisco Secure Access Security Assertion Markup Language(SAML)証明書の有効期限が間もなく切れる予定です。この証明書を検証する場合は、VPNユーザの認証に使用する現在のIdPで更新できます。

これに関する詳細は、「[セキュアアクセスに関するアナウンス](#)」セクションを参照してください。



注：ほとんどのIdPはこのSAML証明書をデフォルトで確認しないため、必須ではありません。つまり、IdPでこれ以上のアクションは必要ありません。IdPがセキュアアクセス証明書を検証する場合は、IdP設定のセキュアアクセス証明書の更新に進みます。

このドキュメントでは、設定済みのIdPが証明書の検証を実行するかどうかを確認する手順について説明します(Entra ID(Azure AD)、PingIdentity、Cisco DUO、OKTA)。

前提条件

要件

- シスコセキュアアクセスダッシュボードにアクセスします。
- IdPダッシュボードにアクセスします。

シスコセキュアアクセスダッシュボード

注：次の手順で新しいセキュアアクセス証明書をアクティブにしたことを確認します。IdPがこの証明書の検証を行っている場合は、新しい証明書でIdPを更新してください。そうでない場合、リモートアクセスユーザのVPN認証が失敗する可能性があります。

IdPがこの証明書の検証を行っていることを確認した場合は、セキュアアクセスで新しい証明書をアクティブ化し、営業時間外にIdPにアップロードすることをお勧めします。

セキュアアクセスダッシュボードで必要なアクションは、Secure > Certificates > SAML Authentication > Service Provider certificatesの順に選択し、New証明書でActivateをクリックすることだけです。

Activateをクリックすると、証明書の検証を行っている場合は、新しいセキュアアクセス証明書をダウンロードしてIdPにインポートできます。

	Serial number	Expiration date	
New	4001919680eb7bea75760c65dfcdc612	August 27, 2025 9:00:56 PM	Activate
Active	40018a952843fdce9813b8ae2d7b32e9	September 13, 2024 3:24:58 PM	Download

MicrosoftエントリID (Microsoft Azure)

入力ID (Azure AD)は既定で証明書の検証を行いません。

Home > Enterprise applications | All applications > Secure Access - RA VPN Authentication (SAML SSO)

Secure Access - RA VPN Authentication (SAML SSO) | SAML-based Sign-on

Enterprise Application

Upload metadata file | Change single sign-on mode | Test this application | Got feedback?

3 SAML Certificates

Token signing certificate

Status: Active [Edit](#)

Thumbprint: 0E8C78D0B0C8E705095496693737D4AAB14D38E4

Expiration: 5/21/2027, 12:24:06 PM

Notification Email

App Federation Metadata Url: <https://login.microsoftonline.com/71414a41-...>

Certificate (Base64) [Download](#)

Certificate (Raw) [Download](#)

Federation Metadata XML [Download](#)

Verification certificates (optional) [Edit](#)

Required: No

IdP Entra IDの「Verification Certificate (optional)」の値が「Required = yes」に設定されている場合、「Edit」および「Upload certificate」をクリックして、新しいセキュアアクセスSAML VPN証明書をアップロードします。

Home > Enterprise applications | All applications > Secure Access - RA VPN Authentication (SAML SSO) | SAML SSO

Secure Access - RA VPN Authentication (SAML SSO) | SAML SSO

Enterprise Application

- Overview
- Deployment Plan
- Diagnose and solve problems
- Manage
 - Properties
 - Owners
 - Roles and administrators
 - Users and groups
 - Single sign-on**
 - Provisioning

3

Upload metadata file Change single sign-on mode

SAML Certificates

Token signing certificate

Status: Active

Thumbprint: 0E8C...

Expiration: 5/21/...

Notification Email: [redacted]

App Federation Metadata Url: http://[redacted]

Certificate (Base64): [redacted]

Certificate (Raw): [redacted]

Federation Metadata XML: [redacted]

Verification certificates (optional)

Required	Yes
Active	1

Verification certificates

ⓘ Requiring verification certificates will impact certain admin and end-user experiences, such as the Single sign-on testing feature, 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
362A5200CB4EBC282403FA2...	e5468291-e750-44c...	8/27/2024, 4:22 PM	8/27/2025, 4:21 PM

PingIdentity

PingIdentityは既定で証明書の検証を行いません。

Getting Started

Overview

Monitoring

Directory

Applications

Applications

Application Catalog

Resources

Application Portal

Applications

Search

4 Applications by Application Name

SAML Secure Access

SAML Secure Access

Overview Configuration

Subject NameID Format
Not Specified

Assertion Validity Duration
300 seconds

Target Application URL
Not Specified

Enforce Signed AuthnRequest
Disabled

IdP PingidentityでEnforce Signed AuthnRequestの値が「Enabled」に設定されている場合は、Editをクリックして新しいSecure Access SAML VPN Certificateをアップロードします。

The screenshot shows the Cisco Duo management console. On the left is a navigation menu with 'Applications' selected. The main area is titled 'Applications' and shows a search bar and a list of 4 applications. The 'SAML Secure Access' application is highlighted. On the right, the configuration page for 'SAML Secure Access' is shown, with tabs for 'Overview' and 'Configuration'. The configuration page includes a search bar, a dropdown for '4 Applications by Application Name', and a list of applications. The 'SAML Secure Access' application is highlighted. The configuration page shows '300 seconds' for a timeout, 'Target Application URL' as 'Not Specified', 'Enforce Signed AuthnRequest' as 'Enabled', and 'Verification Certificates' as '.vpn.sse.cisco.com (HydrantID Server CA O1)' with a validity period of 'Valid 08-24 to 08-25'.

シスコDUO

Cisco DUOはデフォルトで署名要求の検証を行います。アサーション暗号化が有効でない限り、DUO自体でアクションを実行する必要はありません。

リクエストの署名のために、DUOは管理者が提供するメタデータのエンティティIDリンクを使用して新しい証明書をダウンロードできます。

署名応答およびアサーションアクション

Signing options *

- Sign response
- Sign assertion

Choose at least one option for signing the SAML response.

エンティティIDの設定

このステップでアクションは必要ありません。DUOは、エンティティIDリンクから新しい証明書を取得できます：https://<entry-id>.vpn.sse.cisco.com/saml/sp/metadata/<profile_name>。

Service Provider

Metadata Discovery

None (manual input)

Entity ID *

https://[redacted].sse.cisco.com/saml/sp/metadata/[redacted]

The unique identifier of the service provider.

Assertion Consumer Service (ACS) URL *

https://[redacted].sse.cisco.com/+CSCOE+/saml/sp/acs?ign

[+ Add an ACS URL](#)

The service provider endpoint that receives and processes SAML assertions.

アサーション暗号化

IdP Cisco DUOで「Assertion encryption」の値に「Encrypt the SAML Assertion」とマークされている場合は、「Choose File」をクリックし、新しいセキュアアクセスSAML VPN証明書をアップロードします。

[Dashboard](#) > [Applications](#) > Generic SAML Service Provider - Single Sign-On

Generic SAML Service Provider - Single Sign-On

Assertion encryption

Encrypt the SAML assertion

Generic SAML Service Provider - Single Sign-On

Assertion encryption

Encrypt the SAML assertion

Existing Certificate *

VPN Service Provider.cer

オクタ

OKTAは既定で証明書の検証を行いません。General > SAML Settingsには、「Signature Certificate」というオプションはありません。

← Back to Applications



Secure Access - VPN

Active ▾



[View Logs](#) [Monitor Imports](#)

GENERAL

Single Sign On URL

Recipient URL

Destination URL

Audience Restriction

Default Relay State

Name ID Format

EmailAddress

Response

Signed

Assertion Signature

Signed

Signature Algorithm

RSA_SHA256

Digest Algorithm

SHA256

Assertion Encryption

Unencrypted

SAML Single Logout

Disabled

IdP OKTAのGeneral > SAML Settingsに値がある場合は、「[Signature Certificate Assertion encryption](#)」と表示されており、OKTAが証明書の検証を行っていることを意味します。「SAML設定の編集」をクリックし、署名証明書ををクリックして、新しいセキュアアクセスSAML VPN証明書をアップロードします。

← Back to Applications



Secure Access - VPN

Active ▾



View Logs Monitor Imports

Signature Certificate ⓘ



VPN Service Provider.cer X

Uploaded by Josue Brenes on September 5, 2024 at 11:25:06 AM CST

CN=HydrantID Server CA 01,OU=HydrantID Trusted Certificate Service,O=IdenTrust,C=US
Valid from August 27, 2024 at 4:22:25 PM CST to August 27, 2025 at 4:21:25 PM CST

Certificate expires in 356 days

Enable Single Logout ⓘ

Allow application to initiate Single Logout

Signed Requests ⓘ

Validate SAML requests with signature certificates.

関連情報

- [セキュアアクセスヘルプセンター \(ユーザガイド \)](#)
- [テクニカル サポートとドキュメント - Cisco Systems](#)
- [セキュアアクセスコミュニティページ](#)
- [VPN用の新しいセキュアアクセスSAML認証証明書](#)

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。