

Mettre à jour le certificat d'authentification SAML VPN d'accès sécurisé (certificat du fournisseur de services)

Table des matières

[Introduction](#)

[Informations générales](#)

[Conditions préalables](#)

[Exigences](#)

[Tableau de bord Cisco Secure Access](#)

[Microsoft Entra ID \(Microsoft Azure\)](#)

Introduction

Ce document décrit les étapes requises pour mettre à jour le certificat du fournisseur d'identité (IdP) avec le nouveau certificat du fournisseur de services d'accès sécurisé.

Informations générales

Le certificat Cisco Secure Access Security Assertion Markup Language (SAML) utilisé pour l'authentification VPN (Virtual Private Network) arrive bientôt à expiration et peut être mis à jour dans votre IdP actuel utilisé pour authentifier les utilisateurs VPN dans le cas où ils valident ce certificat.

Pour plus d'informations à ce sujet, consultez la section [Annonces d'accès sécurisé](#).



Remarque : la plupart des fournisseurs d'identités ne vérifient pas ce certificat SAML par défaut et ce n'est pas obligatoire, ce qui signifie qu'aucune autre action n'est nécessaire dans votre fournisseur d'identités. Si votre fournisseur d'accès Internet ne valide pas le certificat d'accès sécurisé, continuez avec la mise à jour du certificat d'accès sécurisé dans votre configuration de fournisseur d'accès.

Ce document couvre les étapes pour confirmer si les IdP configurés effectuent la validation de certificat : Entra ID (Azure AD), PingIdentity, Cisco DUO, OKTA.

Conditions préalables

Exigences

- Accédez à votre tableau de bord Cisco Secure Access.
- Accédez à votre tableau de bord IdP.

Tableau de bord Cisco Secure Access

Remarque : assurez-vous qu'après avoir effectué l'étape suivante consistant à activer le nouveau certificat d'accès sécurisé, si votre fournisseur d'accès effectue cette validation de certificat, mettez à jour votre fournisseur d'accès avec le nouveau certificat ; sinon, l'authentification VPN pour les utilisateurs d'accès à distance peut échouer.

Si vous confirmez que votre fournisseur d'identités procède à cette validation de certificat, nous vous recommandons d'activer le nouveau certificat dans Secure Access et de le télécharger sur votre fournisseur d'identités pendant les heures non ouvrables.

Dans le tableau de bord d'accès sécurisé, la seule action requise est d'aller à Secure > Certificates > SAML Authentication > Service Provider certificates, sur le certificat "New" cliquez sur "Activate".

Une fois que vous avez cliqué sur Activer, vous pouvez télécharger le nouveau certificat d'accès sécurisé à importer dans votre fournisseur d'identité s'il effectue la validation du certificat.

	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 Entra ID (Microsoft Azure)

Entra ID (Azure AD) n'effectuant pas la validation de certificat par défaut.

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?

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

SAML Certificates

Token signing certificate	Active	Edit
Status	Active	
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	

Si l'ID d'entrée du fournisseur d'identité (IdP Entra ID) et la valeur « Certificat de vérification (facultatif) » sont définis sur « Obligatoire = oui », cliquez sur Modifier et sur « Télécharger le certificat » pour télécharger le nouveau certificat VPN SAML d'accès sécurisé.

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

Upload metadata file | Change single sign-on mode

SAML Certificates

Token signing certificate

Status: Active
Thumbprint: 0E8C...
Expiration: 5/21/...

Notification Email
App Federation Metadata Url
Certificate (Base64)
Certificate (Raw)
Federation Metadata XML

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

IdentitéPing

PingIdentity n'effectue pas la validation de certificat par défaut.

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

Si, dans IdP Pingidentity, la valeur Enforce Signed AuthnRequest est définie sur « Enabled », cliquez sur Edit et téléchargez le nouveau certificat VPN SAML d'accès sécurisé.

The screenshot displays the Cisco Duo management interface. On the left, a dark blue sidebar contains navigation links: Getting Started, Overview, Monitoring, Directory, Applications, Application Catalog, Resources, and Application Portal. The 'Applications' link is highlighted with a blue box. The main content area is titled 'Applications' and includes a search bar and a dropdown menu showing '4 Applications by Application Name'. Below this, a card for 'SAML Secure Access' is highlighted with a blue box. To the right, the configuration page for 'SAML Secure Access' is shown, with tabs for 'Overview' and 'Configuration'. The configuration details include: 300 seconds, Target Application URL (Not Specified), Enforce Signed AuthnRequest (Enabled), and Verification Certificates (.vpn.sse.cisco.com (HydrantID Server CA O1) Valid 08-24 to 08-25). The 'Enforce Signed AuthnRequest' and 'Verification Certificates' sections are highlighted with red boxes.

Cisco DUO

Cisco DUO effectue la validation de la demande de signature par défaut, mais il n'exige aucune action sur DUO lui-même à moins que le chiffrement d'assertion soit activé.

pour la signature de la demande, le DUO peut télécharger le nouveau certificat à l'aide du lien ID d'entité de métadonnées fourni par l'administrateur.

Action de signature de réponse et d'assertion

Signing options *

- Sign response
- Sign assertion

Choose at least one option for signing the SAML resq

Paramètres ID entité

Aucune action n'est requise dans cette étape, le DUO peut extraire le nouveau certificat à partir du lien d'ID d'entité : 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?1gn

[+ Add an ACS URL](#)

The service provider endpoint that receives and processes SAML assertions.

Chiffrement d'assertion

Si, dans l'IdP Cisco DUO, la valeur « Assertion encryption » a la valeur « Encrypt the SAML Assertion » marquée, cliquez sur « Choose File » et téléchargez le nouveau certificat VPN SAML d'accès sécurisé.

[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

OKTA

OKTA n'effectue pas de validation de certificat par défaut. Il n'y a pas d'option sous Général > Paramètres SAML, qui indique "Certificat de signature".

← 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

Si dans l'OKTA IdP il y a une valeur sous General > SAML Settings, qui dit "Signature Certificate Assertion encryption", cela signifie qu'OKTA effectue la Validation de Certificat. Cliquez sur "Edit SAML Settings", cliquez sur Signature Certificate et téléchargez le nouveau certificat SAML VPN d'accès sécurisé.

← 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.

Informations connexes

- [Centre d'aide Secure Access \(Guide de l'utilisateur\)](#)
- [Assistance et documentation techniques - Cisco Systems](#)
- [Page Communauté d'accès sécurisé](#)
- [Nouveau certificat d'authentification SAML d'accès sécurisé pour VPN](#)

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.