

Update Secure Access SAML VPN-verificatiecertificaat (Serviceprovider-certificaat)

Inhoud

[Inleiding](#)

[Achtergrondinformatie](#)

[Voorwaarden](#)

[Vereisten](#)

[Cisco Secure Access Dashboard](#)

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

Inleiding

In dit document worden de stappen beschreven die nodig zijn om het Identity Provider (IDP)-certificaat bij te werken met het nieuwe Secure Access Service Provider-certificaat.

Achtergrondinformatie

Het certificaat van Cisco Secure Access Security Assertion Markup Language (SAML) dat wordt gebruikt voor VPN-verificatie (Virtual Private Network) verloopt binnenkort en kan worden bijgewerkt in uw huidige IDp die wordt gebruikt voor de verificatie van VPN-gebruikers in het geval dat ze dit certificaat valideren.

Meer informatie hierover vindt u in het gedeelte [Secure Access Announcements](#).



Opmerking: De meeste IDps verifiëren dit SAML-certificaat niet standaard en het is geen vereiste, wat betekent dat er geen verdere actie nodig is in uw IDp. Als uw IDp het Secure Access Certificate niet valideert, gaat u verder met het bijwerken van het Secure Access Certificate in uw IDp-configuratie.

Dit document beschrijft de stappen om te bevestigen of de geconfigureerde ID's certificaatsvalidatie uitvoeren: Entra ID (Azure AD), PingIdentity, Cisco DUO, OKTA.

Voorwaarden

Vereisten

- Toegang tot uw Cisco Secure Access Dashboard.
- Toegang tot uw IDp dashboard.

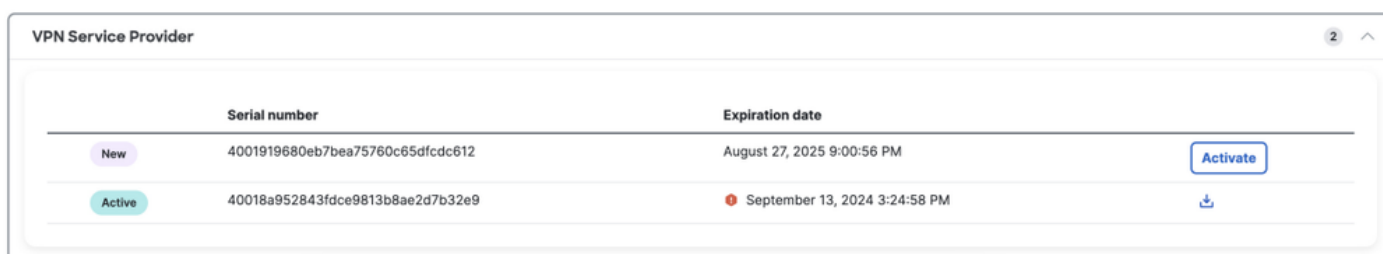
Cisco Secure Access Dashboard

Opmerking: Zorg ervoor dat na het doen van de volgende stap die het nieuwe Secure Access-certificaat activeert, als uw IDP dit certificaat valideert, update uw IDP met het nieuwe certificaat; anders kan de VPN-verificatie voor gebruikers van externe toegang mislukken.

Als u bevestigt dat uw IDP deze certificaatvalidatie uitvoert, raden we u aan het nieuwe certificaat in Secure Access te activeren en het tijdens niet-werkuren naar uw IDP te uploaden.

In het Secure Access Dashboard is de enige actie die nodig is om Secure > Certificaten > SAML-verificatie > Serviceprovider-certificaten te beveiligen, klik op "Nieuw"-certificaat op "Activeren".

Zodra geklikt op Activeren, kunt u het nieuwe Secure Access-certificaat downloaden om te importeren in uw IDP als het de Certificaatvalidatie uitvoert.



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

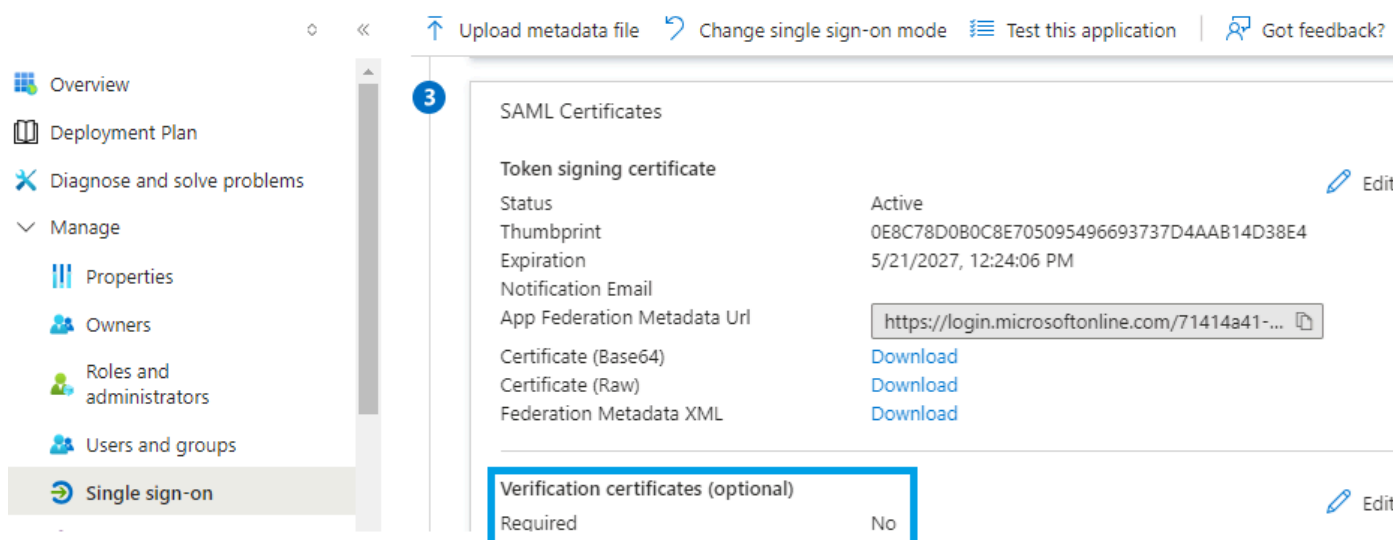
Microsoft Entra ID (Microsoft Azure)

Entra ID (Azure AD) voert standaard geen certificaatvalidatie uit.

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		
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)		
Required	No	Edit

Als de IDP Entra-id de waarde "Verificatiecertificaat (optioneel)" is ingesteld op "Vereist = ja", klik dan op Bewerken en "Upload certificaat" om het nieuwe Secure Access SAML VPN-certificaat te uploaden.

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: [redacted]
App Federation Metadata Url: http://[redacted]
Certificate (Base64): [redacted]
Certificate (Raw): [redacted]
Federation Metadata XML: [redacted]

Verification certificates (optional)

Required	Active
Yes	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 voert standaard geen certificaatvalidatie uit.

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

Als in de IDp Pingidentiteits de waarde Enforce Signed Authnrequest is ingesteld op "Enabled", klik dan op Bewerken en uploaden van het nieuwe Secure Access SAML VPN-certificaat.

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

Cisco DUO

Cisco DUO ondertekent standaard de validatie van aanvragen, maar er is geen actie nodig op DUO zelf, tenzij de Assertion Encryption is ingeschakeld.

voor een verzoek kan de DUO het nieuwe certificaat downloaden via de metagegevens-entiteit-ID-link die door de beheerder wordt geboden.

Reactie- en aanhoudingsactie ondertekenen

Signing options *

- Sign response
- Sign assertion

Choose at least one option for signing the SAML response

Instellingen entiteit-ID

In deze stap is geen actie vereist. Het DUO kan het nieuwe certificaat ophalen uit de link Entiteit-ID: 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?tgn

[+ Add an ACS URL](#)

The service provider endpoint that receives and processes SAML assertions.

Assertion-encryptie

Als in de IDp Cisco DUO de waarde "Assertion encryptie" de markering "Encrypt the SAML Assertion" heeft, klik dan op "Select File" en upload het nieuwe Secure Access SAML VPN-certificaat.

[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 voert standaard geen certificaatvalidatie uit. Onder General > SAML Settings is er geen optie waar staat "Signature Certificate".

← 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

Als er in de IDP OKTA een waarde onder General > SAML Settings staat, die zegt "Signature Certificate Assertion encryptie" betekent dat OKTA Certificaat Validatie doet. Klik op "SAML-instellingen bewerken", klik op Handtekeningcertificaat en upload het nieuwe Secure Access SAML VPN-certificaat.

← 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.

Gerelateerde informatie

- [Secure Access Help Center \(gebruikershandleiding\)](#)
- [Technische ondersteuning en documentatie – Cisco Systems](#)
- [Secure Access-communitypagina](#)
- [Nieuw Secure Access SAML-autorisatiecertificaat voor VPN](#)

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.