

Update Secure Access SAML VPN Authentication Certificate (Service Provider Certificate)

Contents

[Introduction](#)

[Background Information](#)

[Prerequisites](#)

[Requirements](#)

[Cisco Secure Access Dashboard](#)

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

Introduction

This document describes the steps required to update the Identity Provider (IdP) certificate with the new Secure Access Service Provider Certificate.

Background Information

The Cisco Secure Access Security Assertion Markup Language (SAML) Certificate used for Virtual Private Network (VPN) Authentication is soon to expire and can be updated in your current IdP used to authenticate VPN Users in the case they do validate this certificate.

More information about this can be found in the [Secure Access Announcements](#) section.



Note: Most IdPs do not verify this SAML certificate by default and it is not a requirement, meaning no further action is needed in your IdP. In the case your IdP does validate the Secure Access Certificate, proceed with updating the Secure Access Certificate in your IdP configuration.

This document covers the steps to confirm if the configured IdPs perform certificate validation: Entra ID (Azure AD), PingIdentity, Cisco DUO, OKTA.

Prerequisites

Requirements

- Access to your Cisco Secure Access Dashboard.
- Access to your IdP dashboard.

Cisco Secure Access Dashboard

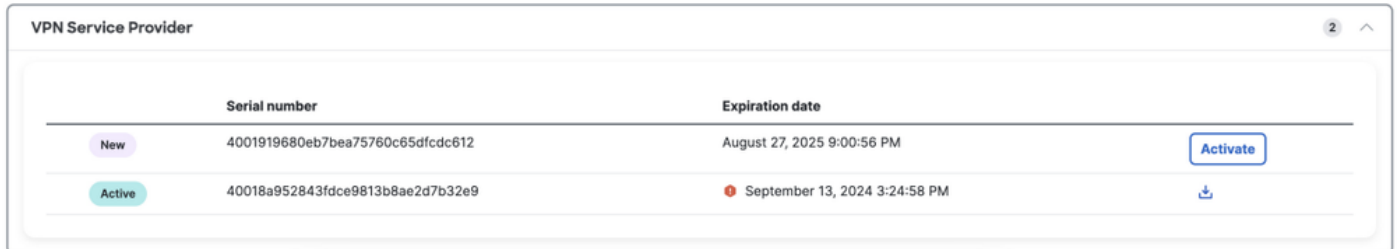
Note: Make sure that after doing the next step which is activating the New Secure Access certificate, if your IdP is doing this Certificate Validation, update your IdP with the new Certificate; otherwise,

the VPN Authentication for Remote Access Users can fail.

If you confirm your IdP is doing this Certificate Validation, we recommend you activate the new certificate in Secure Access and upload it to your IdP during non-working hours.

In the Secure Access Dashboard the only action required is go to **Secure > Certificates > SAML Authentication > Service Provider certificates**, on the "New" certificate click on "Activate".

Once clicked on Activate, you are able to download the New Secure Access certificate to import in your IdP if it is doing the Certificate Validation.



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

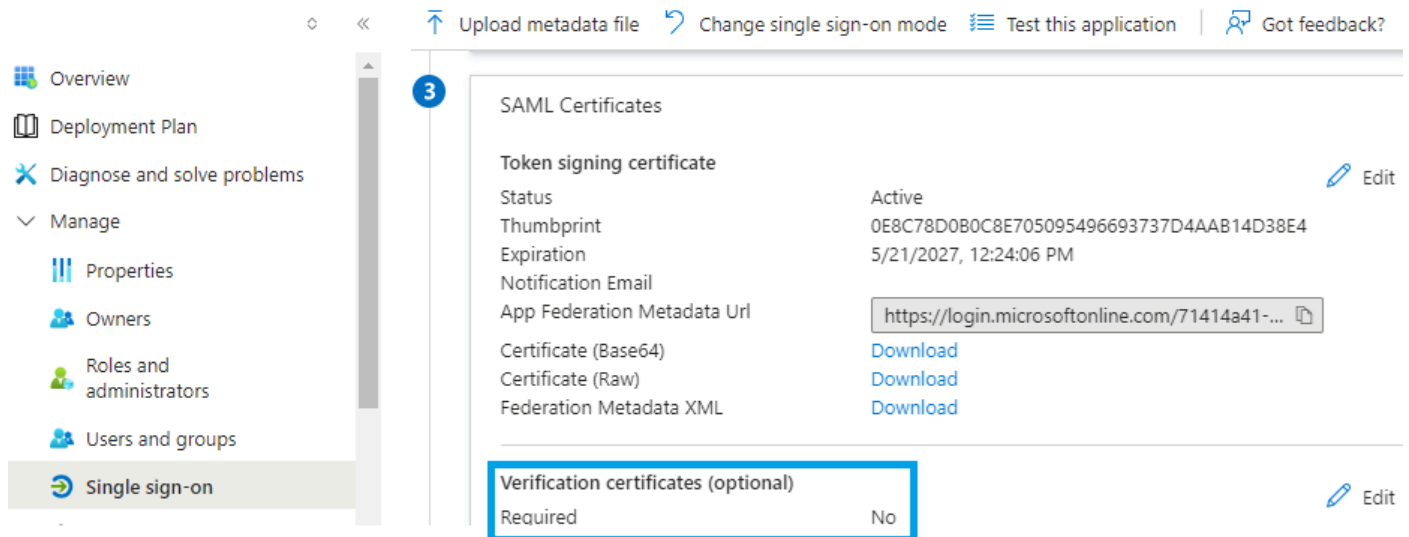
Microsoft Entra ID (Microsoft Azure)

Entra ID (Azure AD) not doing Certificate Validation by default.

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	

If the IdP Entra ID the value "Verification Certificate (optional) is set to "Required = yes", click on Edit and "Upload certificate" to upload the new Secure Access SAML VPN Certificate.

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: http://...
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

PingIdentity

PingIdentity not doing Certificate Validation by default.

Getting Started
Overview
Monitoring
Directory
Applications
Applications
Application Catalog
Resources
Application Portal

Applications

Search

4 Applications by Application Name

SAML Secure Access

Overview Configuration

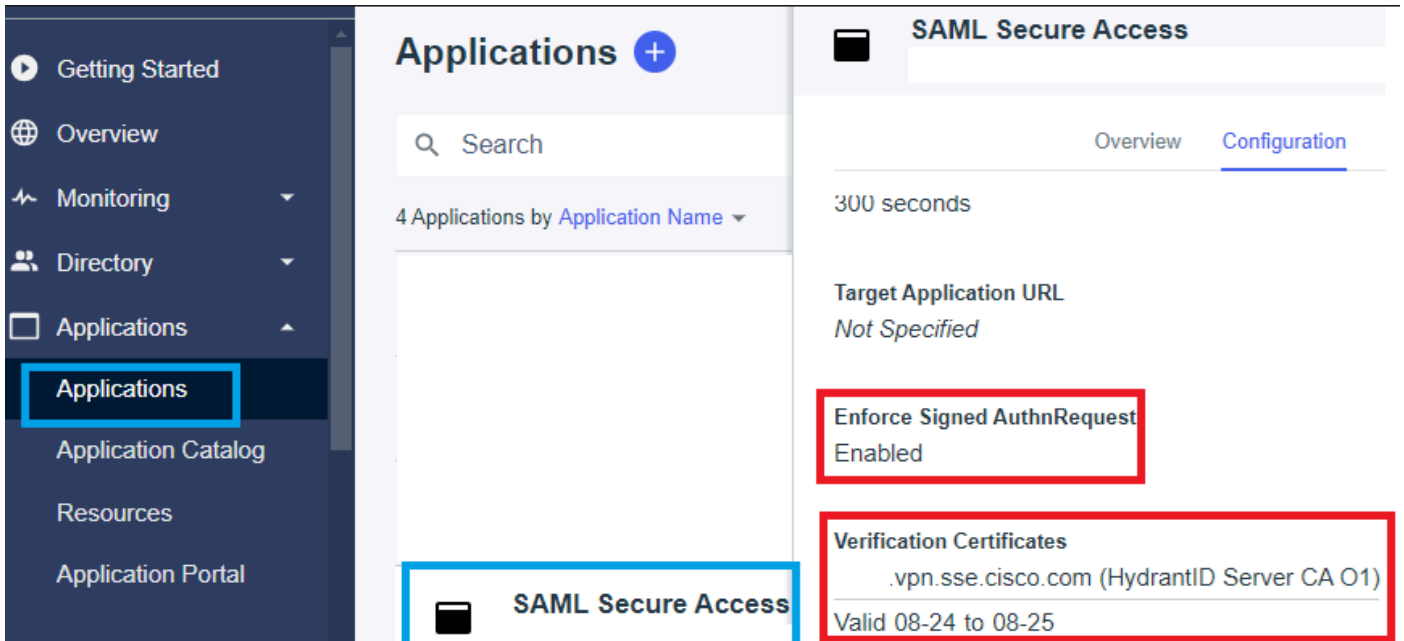
Subject NameId Format
Not Specified

Assertion Validity Duration
300 seconds

Target Application URL
Not Specified

Enforce Signed AuthnRequest
Disabled

If in the IdP Pingidentity the value Enforce Signed AuthnRequest is set to "Enabled ", click on Edit and upload the new Secure Access SAML VPN Certificate.



Cisco DUO

Cisco DUO is doing signing request validation by default, however it does not require an action to be done on DUO itself unless the Assertion Encryption is enabled.

for request signing the DUO can download the new certificate using the metadata Entity ID link provided by the admin.

Signing Response and Assertion Action

Signing options *

- Sign response
- Sign assertion

Choose at least one option for signing the SAML request

Entity ID Settings

No Action is required in this step, the DUO can pull the new certificate from the Entity ID Link:
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 Encryption

If in the IdP Cisco DUO the value "Assertion encryption" has the "Encrypt the SAML Assertion" marked, click on "choose File" and upload the new Secure Access SAML VPN Certificate.

[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 not doing Certificate Validation by default. There is not an option under General > SAML Settings, that says "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

If in the IdP OKTA there is a value under General > SAML Settings, that says "Signature Certificate Assertion encryption" it means OKTA is doing Certificate Validation. Click on "Edit SAML Settings", click on Signature Certificate and upload the new Secure Access SAML VPN Certificate.

← 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.

Related Information

- [Secure Access Help Center \(User Guide\)](#)
- [Technical Support & Documentation - Cisco Systems](#)
- [Secure Access Community Page](#)
- [New Secure Access SAML Auth Certificate for VPN](#)