

Actualizar certificado de autenticación VPN SAML de acceso seguro (certificado de proveedor de servicios)

Contenido

[Introducción](#)

[Antecedentes](#)

[Prerequisites](#)

[Requirements](#)

[Panel de Cisco Secure Access](#)

[ID de Microsoft Entry \(Microsoft Azure\)](#)

Introducción

Este documento describe los pasos necesarios para actualizar el certificado del proveedor de identidad (IdP) con el nuevo certificado del proveedor de servicios de acceso seguro.

Antecedentes

El certificado de lenguaje de marcado de aserción de seguridad de acceso seguro (SAML) de Cisco utilizado para la autenticación de red privada virtual (VPN) vencerá pronto y se puede actualizar en el IdP actual utilizado para autenticar usuarios de VPN en caso de que validen este certificado.

Puede encontrar más información al respecto en la sección [Anuncios de acceso seguro](#).



Nota: La mayoría de los IdP no verifican este certificado SAML de forma predeterminada y no es un requisito, lo que significa que no se necesita ninguna otra acción en su IdP. En caso de que su IdP valide el Certificado de Acceso Seguro, continúe con la actualización del Certificado de Acceso Seguro en su configuración de IdP.

Este documento cubre los pasos para confirmar si los IdPs configurados realizan la validación del certificado: Entra ID (Azure AD), PingIdentity, Cisco DUO, OKTA.

Prerequisites

Requirements

- Acceso al panel de Cisco Secure Access.
- Acceso a su panel de IdP.

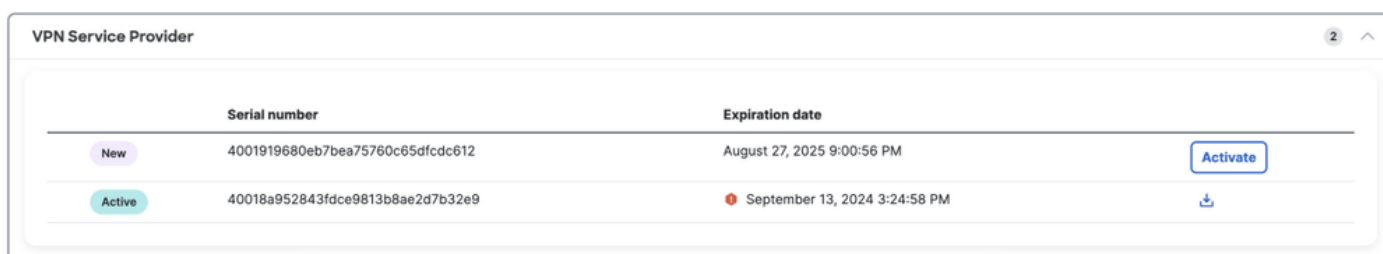
Panel de Cisco Secure Access

Nota: Asegúrese de que después de hacer el siguiente paso que es activar el Nuevo Certificado de Acceso Seguro, si su IdP está haciendo esta Validación de Certificado, actualice su IdP con el nuevo Certificado; de lo contrario, la Autenticación VPN para Usuarios de Acceso Remoto puede fallar.

Si confirma que su IdP está haciendo esta Validación de Certificado, le recomendamos que active el nuevo certificado en Secure Access y lo cargue en su IdP durante el horario no laborable.

En el panel de acceso seguro, la única acción requerida es ir a Secure > Certificates > SAML Authentication > Service Provider certificates, en el certificado "New" haga clic en "Activate".

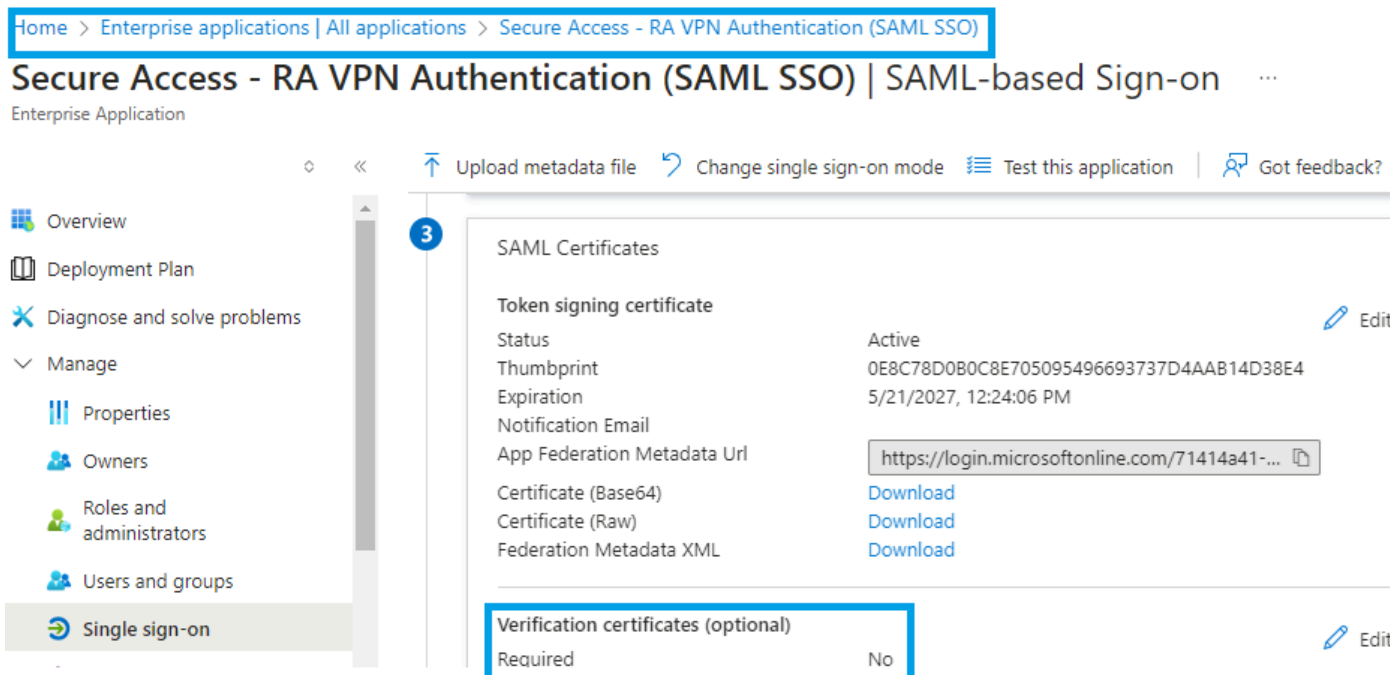
Una vez que haya hecho clic en Activar, podrá descargar el nuevo certificado de acceso seguro para importarlo en su IdP si está realizando la validación del certificado.



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

ID de Microsoft Entry (Microsoft Azure)

El Id. de entrada (Azure AD) no realiza la validación de certificados de forma predeterminada.



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 el ID de entrada de IdP tiene el valor "Certificado de verificación (opcional)" establecido en "Requerido = sí", haga clic en Editar y "Cargar certificado" para cargar el nuevo certificado VPN SAML de acceso seguro.

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 no está realizando la validación de certificados de forma predeterminada.

Getting Started
Overview
Monitoring
Directory
Applications
Application Catalog
Resources
Application Portal

Applications

Search

4 Applications by Application Name

SAML Secure Access

SAML Secure Access

Overview | Configuration

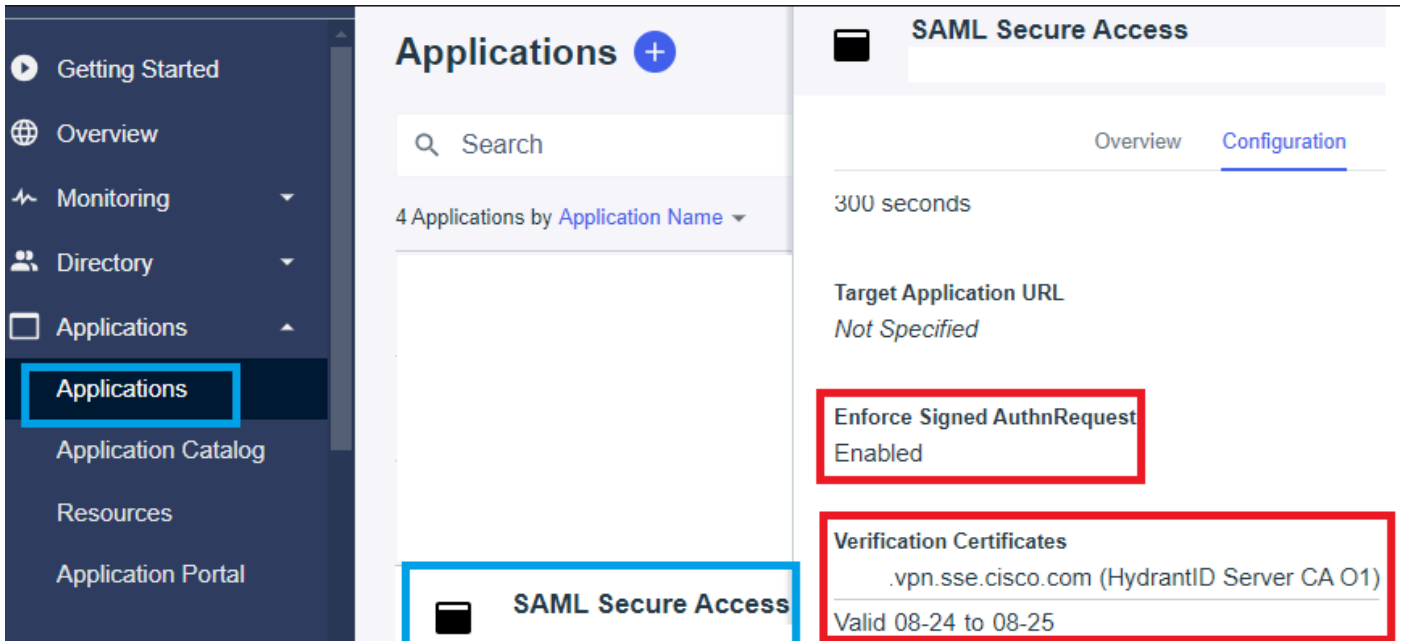
Subject NameID Format
Not Specified

Assertion Validity Duration
300 seconds

Target Application URL
Not Specified

Enforce Signed AuthnRequest
Disabled

Si en IdP Identity el valor Enforce Signed AuthnRequest está configurado en "Enabled", haga clic en Edit y cargue el nuevo Certificado VPN SAML de Secure Access.



Cisco DUO

Cisco DUO realiza la validación de la solicitud de firma de forma predeterminada; sin embargo, no requiere que se realice ninguna acción en el propio DUO a menos que se habilite el cifrado de aserción.

para la firma de solicitud, el DUO puede descargar el nuevo certificado mediante el enlace de ID de entidad de metadatos proporcionado por el administrador.

Respuesta de firma y acción de aserción

Signing options *

- Sign response
- Sign assertion

Choose at least one option for signing the SAML response

Configuración de ID de entidad

No se requiere ninguna acción en este paso, el DUO puede extraer el nuevo certificado del enlace de ID de entidad: 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.

Cifrado de aserción

Si en el IdP de Cisco DUO el valor "Encriptación de aserción" tiene marcada la opción "Cifrar la aserción SAML", haga clic en "Elegir archivo" y cargue el nuevo certificado VPN SAML de acceso seguro.

[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 no está realizando la validación de certificados de forma predeterminada. No existe ninguna opción en General > Configuración SAML que diga "Certificado de firma".

← 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 en el IdP OKTA hay un valor bajo General > Configuración SAML, que dice "Cifrado de afirmación de certificado de firma" significa que OKTA está haciendo la Validación de Certificado. Haga clic en "Editar configuración SAML", haga clic en Certificado de firma y cargue el nuevo Certificado VPN SAML de acceso seguro.

← 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.

Información Relacionada

- [Centro de ayuda de Secure Access \(Guía del usuario\)](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)
- [Página Comunidad de Secure Access](#)
- [Nuevo certificado de autenticación SAML de acceso seguro para VPN](#)

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).