

Atualizar Certificado de Autenticação VPN SAML de Acesso Seguro (Certificado do Provedor de Serviços)

Contents

[Introdução](#)

[Informações de Apoio](#)

[Pré-requisitos](#)

[Requisitos](#)

[Painel do Cisco Secure Access](#)

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

Introdução

Este documento descreve as etapas necessárias para atualizar o certificado do Provedor de Identidade (IdP) com o novo Certificado do Provedor de Serviços de Acesso Seguro.

Informações de Apoio

O Certificado Cisco Secure Access Security Assertion Markup Language (SAML) usado para a Autenticação de Rede Virtual Privada (VPN) expirará em breve e poderá ser atualizado em seu IdP atual usado para autenticar Usuários VPN caso eles validem esse certificado.

Mais informações sobre isso podem ser encontradas na seção [Anúncios de acesso seguro](#).



Observação: a maioria dos IdPs não verifica esse certificado SAML por padrão e ele não é um requisito, o que significa que nenhuma ação adicional é necessária em seu IdP. Caso seu IdP valide o Certificado de Acesso Seguro, continue atualizando o Certificado de Acesso Seguro em sua configuração do IdP.

Este documento aborda as etapas para confirmar se os IdPs configurados executam validação de certificado: Entra ID (Azure AD), PingIdentity, Cisco DUO, OKTA.

Pré-requisitos

Requisitos

- Acesso ao Painel do Cisco Secure Access.
- Acesso ao painel do IdP.

Painel do Cisco Secure Access

Observação: certifique-se de que após executar a próxima etapa, que é ativar o novo certificado de acesso seguro, se o seu IdP estiver fazendo a validação do certificado, atualize o seu IdP com o novo certificado; caso contrário, a autenticação VPN para usuários de acesso remoto pode falhar.

Se você confirmar que o seu IdP está fazendo essa Validação de certificado, recomendamos que você ative o novo certificado no Secure Access e carregue-o no seu IdP durante horários não úteis.

No Painel de Controle de Acesso Seguro, a única ação necessária é ir para Seguro > Certificados > Autenticação SAML > Certificados de Provedor de Serviços, no certificado "Novo", clique em "Ativar".

Depois de clicar em Ativar, você poderá baixar o novo certificado do Secure Access para importar em seu IdP se ele estiver fazendo a Validação de 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 do Microsoft Entra (Microsoft Azure)

A ID de Entrada (Azure AD) não está fazendo a Validação de Certificado por padrão.

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 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

Se a ID do IdP Entra o valor "Verification Certificate (optional) estiver definido como "Required = yes" (Obrigatório = sim), clique em Edit (Editar) e em "Upload certificate" (Carregar certificado) para carregar o novo certificado SAML VPN de acesso 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

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

SAML Certificates

Token signing certificate

Status: Active

Thumbprint: 0E8C...

Expiration: 5/21/...

Notification Email: [Redacted]

App Federation Metadata Url: http://...

Certificate (Base64): [Redacted]

Certificate (Raw): [Redacted]

Federation Metadata XML: [Redacted]

Verification certificates (optional)

Required: Yes

Active: 1

IdentidadePing

O PingIdentity não está fazendo a validação de certificado por padrão.

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

Se na Identidade de ping do IdP o valor Enforce Signed AuthnRequest estiver definido como "Enabled", clique em Edit e carregue o novo certificado SAML VPN de acesso seguro.

The screenshot shows the Cisco Duo web interface. On the left is a dark blue navigation sidebar with the following menu items: 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 two tabs: 'Overview' and 'Configuration' (selected). The configuration panel includes the following settings: '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 are: '.vpn.sse.cisco.com (HydrantID Server CA O1)'. The application name 'SAML Secure Access' is also highlighted with a blue box at the bottom of the application list.

Cisco DUO

O Cisco DUO está fazendo a validação da solicitação de assinatura por padrão, no entanto, não requer uma ação no próprio DUO, a menos que a Criptografia de Asserção esteja habilitada.

para assinar a solicitação, o DUO pode baixar o novo certificado usando o link de ID de entidade de metadados fornecido pelo administrador.

Resposta de Assinatura e Ação de Asserção

Signing options *

- Sign response
- Sign assertion

Choose at least one option for signing the SAML response.

Configurações de ID da entidade

Nenhuma Ação é necessária nesta etapa, o DUO pode extrair o novo certificado do Link de ID da Entidade: 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.

Criptografia de Asserção

Se no IdP Cisco DUO o valor "Assertion encryption" tiver "Encrypt the SAML Assertion" marcado, clique em "choose File" e carregue o novo 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

O OKTA não está fazendo a validação de certificado por padrão. Não há uma opção em General > SAML Settings que diga "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

Se no IdP OKTA houver um valor em General > SAML Settings, que diz "Signature Certificate Assertion encryption" significa que o OKTA está fazendo a validação do certificado. Clique em "Edit SAML Settings" (Editar configurações SAML), clique em Signature Certificate (Certificado de Assinatura) e carregue o novo Secure Access SAML VPN Certificate (Certificado VPN SAML de Acesso 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.

Informações Relacionadas

- [Secure Access Help Center \(Guia do usuário\)](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)
- [Página da comunidade de acesso seguro](#)
- [Novo Certificado de Autenticação SAML de Acesso Seguro para VPN](#)

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.