

Aggiorna certificato di autenticazione VPN SAML di accesso sicuro (certificato provider di servizi)

Sommario

[Introduzione](#)

[Premesse](#)

[Prerequisiti](#)

[Requisiti](#)

[Cisco Secure Access Dashboard](#)

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

Introduzione

In questo documento viene descritto come aggiornare il certificato del provider di identità (IdP) con il nuovo certificato del provider di servizi di accesso sicuro.

Premesse

Il certificato SAML (Secure Access Security Assertion Markup Language) di Cisco utilizzato per l'autenticazione VPN (Virtual Private Network) sta per scadere e può essere aggiornato nell'IdP corrente utilizzato per autenticare gli utenti VPN nel caso in cui convalidino questo certificato.

Per ulteriori informazioni, vedere la sezione [Annunci di accesso sicuro](#).



Nota: la maggior parte degli IdP non verifica questo certificato SAML per impostazione predefinita e non è un requisito, pertanto non sono necessarie ulteriori azioni nel provider di identità. Se il provider di identità non convalida il certificato di accesso sicuro, procedere con l'aggiornamento del certificato di accesso sicuro nella configurazione del provider di identità.

In questo documento viene descritto come verificare se gli IdP configurati eseguono la convalida del certificato: Entra ID (Azure AD), Pingidentity, Cisco DUO, OKTA.

Prerequisiti

Requisiti

- Accedere a Cisco Secure Access Dashboard.
- Accedere al dashboard IdP.

Cisco Secure Access Dashboard

Nota: dopo aver eseguito il passaggio successivo relativo all'attivazione del nuovo certificato di accesso sicuro, se il provider di identità esegue questa convalida del certificato, aggiornare il provider di identità con il nuovo certificato. In caso contrario, l'autenticazione VPN per gli utenti di accesso remoto potrebbe non riuscire.

Se si conferma che l'IdP sta eseguendo la convalida del certificato, è consigliabile attivare il nuovo certificato in Accesso sicuro e caricarlo nell'IdP durante l'orario non lavorativo.

Nel Dashboard di accesso protetto l'unica azione richiesta è passare a Protezione > Certificati > Autenticazione SAML > Certificati provider di servizi, sul "Nuovo" certificato fare clic su "Attiva".

Dopo aver fatto clic su Attiva, è possibile scaricare il nuovo certificato di accesso sicuro da importare nel proprio IdP se sta eseguendo la convalida del certificato.

	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 Entra Microsoft (Microsoft Azure)

L'ID Entra (Azure AD) non esegue la convalida del certificato per impostazione predefinita.

[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)

Required	No	Edit
----------	----	------

Se l'ID Entra IdP il valore "Verification Certificate (optional)" è impostato su "Required = yes", fare clic su Edit e "Upload certificate" per caricare il nuovo certificato VPN SAML di accesso sicuro.

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://[redacted]

Certificate (Base64): [redacted]

Certificate (Raw): [redacted]

Federation Metadata XML: [redacted]

Verification certificates (optional)

Required: Yes

Active: 1

IdentitàPing

PingIdentity non esegue la convalida del certificato per impostazione predefinita.

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 nella proprietà IdP Pingidentity il valore Enforce Signed AuthnRequest è impostato su "Enabled", fare clic su Edit and upload the new Secure Access SAML VPN Certificate.

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 card for 'SAML Secure Access' (highlighted with a blue box). To the right of the card is the configuration page for 'SAML Secure Access', which has two tabs: 'Overview' and 'Configuration' (selected). The configuration page shows a timeout of '300 seconds' and a 'Target Application URL' of 'Not Specified'. Two red boxes highlight specific settings: 'Enforce Signed AuthnRequest' is set to 'Enabled', and 'Verification Certificates' is set to '.vpn.sse.cisco.com (HydrantID Server CA O1)' with a validity period of 'Valid 08-24 to 08-25'.

Cisco DUO

Cisco DUO esegue la convalida delle richieste di firma per impostazione predefinita, tuttavia non richiede l'esecuzione di un'azione su DUO stesso a meno che Assertion Encryption non sia abilitata.

per la firma della richiesta, il DUO può scaricare il nuovo certificato utilizzando il collegamento ID entità metadati fornito dall'amministratore.

Risposta firma e azione asserzione

Signing options *

- Sign response
- Sign assertion

Choose at least one option for signing the SAML request

Impostazioni ID entità

In questo passaggio non è richiesta alcuna azione. Il DUO può estrarre il nuovo certificato dal collegamento dell'ID entità: https://<entry-id>.vpn.sse.cisco.com/saml/sp/metadata/<nome_profilo>.

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

Se nell'IdP Cisco DUO il valore "Assertion encryption" ha il contrassegno "Encrypt the SAML Assertion", fare clic su "choose File" (Scegli file) e caricare il nuovo certificato VPN SAML di accesso sicuro.

[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 non esegue la convalida del certificato per impostazione predefinita. In Generale > Impostazioni SAML non è disponibile l'opzione "Certificato 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

Se in IdP OKTA è presente un valore in Generale > Impostazioni SAML, che indica "Crittografia asserzione certificato firma" significa che OKTA sta eseguendo la convalida del certificato. Fare clic su "Edit SAML Settings" (Modifica impostazioni SAML), fare clic su Signature Certificate (Certificato di firma) e caricare il nuovo certificato VPN SAML di accesso sicuro.

← 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.

Informazioni correlate

- [Guida di Secure Access \(Guida dell'utente\)](#)
- [Documentazione e supporto tecnico – Cisco Systems](#)
- [Pagina Secure Access Community](#)
- [Nuovo certificato di autenticazione SAML per accesso sicuro per VPN](#)

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).