

SAML VPN-Authentifizierungszertifikat für sicheren Zugriff aktualisieren (Service Provider-Zertifikat)

Inhalt

[Einleitung](#)

[Hintergrundinformationen](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Cisco Secure Access Dashboard](#)

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

Einleitung

In diesem Dokument werden die Schritte beschrieben, die erforderlich sind, um das Identity Provider (IdP)-Zertifikat mit dem neuen Secure Access Service Provider-Zertifikat zu aktualisieren.

Hintergrundinformationen

Das Cisco Secure Access Security Assertion Markup Language (SAML)-Zertifikat für die VPN-Authentifizierung (Virtual Private Network) läuft in Kürze ab und kann in Ihrer aktuellen ID aktualisiert werden, die zur Authentifizierung von VPN-Benutzern verwendet wird, falls diese das Zertifikat validieren.

Weitere Informationen hierzu finden Sie im Abschnitt [Ankündigungen für sicheren Zugriff](#).



Hinweis: Die meisten IdPs überprüfen dieses SAML-Zertifikat nicht standardmäßig, und es ist keine Anforderung, d. h. es ist keine weitere Aktion in Ihrem IdP erforderlich. Falls Ihr IdP das Zertifikat für sicheren Zugriff validiert, fahren Sie mit der Aktualisierung des Zertifikats für sicheren Zugriff in Ihrer IdP-Konfiguration fort.

In diesem Dokument werden die Schritte beschrieben, mit denen überprüft werden kann, ob die konfigurierten IDs eine Zertifikatsüberprüfung durchführen: Entra ID (Azure AD), PingIdentity, Cisco DUO, OKTA.

Voraussetzungen

Anforderungen

- Zugriff auf Ihr Cisco Secure Access Dashboard.
- Zugriff auf Ihr IdP-Dashboard.

Cisco Secure Access Dashboard

Hinweis: Achten Sie darauf, dass Sie nach dem nächsten Schritt, der die Aktivierung des Zertifikats "Neuer sicherer Zugriff" umfasst, falls Ihr IdP diese Zertifikatsvalidierung durchführt, Ihren IdP mit dem neuen Zertifikat aktualisieren. Andernfalls kann die VPN-Authentifizierung für RAS-Benutzer fehlschlagen..

Wenn Sie bestätigen, dass Ihr IdP diese Zertifikatsvalidierung durchführt, empfehlen wir Ihnen, das neue Zertifikat in Secure Access zu aktivieren und es außerhalb der Arbeitszeiten in Ihren IdP hochzuladen.

Im Secure Access Dashboard ist die einzige Aktion, die Sie durchführen müssen, Secure > Certificates > SAML Authentication > Service Provider Certificates. Klicken Sie im "New" Certificate auf "Activate".

Sobald Sie auf Aktivieren geklickt haben, können Sie das Zertifikat für neuen sicheren Zugriff herunterladen, um es in Ihre IdP zu importieren, wenn die Zertifikatsvalidierung durchgeführt wird.

	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)

Die Entra-ID (Azure AD) führt standardmäßig keine Zertifikatsvalidierung durch.

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

Wenn die IdP Entra ID den Wert "Verification Certificate (optional)" auf "Required = yes" gesetzt hat, klicken Sie auf Edit und "Upload certificate", um das neue Secure Access SAML VPN Certificate hochzuladen.

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 führt standardmäßig keine Zertifikatsvalidierung durch.

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

Wenn in der IdP-Pingidentity der Wert "Enforce Signed AuthnRequest" auf "Enabled" (Aktiviert) festgelegt ist, klicken Sie auf "Edit" (Bearbeiten), und laden Sie das neue Secure Access SAML VPN-Zertifikat hoch.

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 the 'Verification Certificates' section shows a certificate for '.vpn.sse.cisco.com (HydrantID Server CA O1)' valid from '08-24 to 08-25'.

Cisco DUO

Cisco DUO führt standardmäßig eine Validierung der Signierungsanforderung durch. Es ist jedoch keine Aktion für das DUO selbst erforderlich, es sei denn, die Assertion Encryption ist aktiviert.

für die Anforderungssignierung kann das DUO das neue Zertifikat über den vom Administrator bereitgestellten Link für die Entitäts-ID der Metadaten herunterladen.

Signaturantwort und Erklärungsaktion

Signing options *

- Sign response
- Sign assertion

Choose at least one option for signing the SAML response

Einheiten-ID-Einstellungen

In diesem Schritt ist keine Aktion erforderlich. Das DUO kann das neue Zertifikat aus dem Link für die Element-ID abrufen: 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

Wenn im IdP Cisco DUO der Wert "Assertion encryption" mit "Encrypt the SAML Assertion" markiert ist, klicken Sie auf "Choose File" und laden Sie das neue Secure Access SAML VPN Certificate hoch.

[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 führt standardmäßig keine Zertifikatsvalidierung durch. Unter Allgemein > SAML-Einstellungen gibt es keine Option "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

Wenn in der IdP OKTA ein Wert unter Allgemein > SAML-Einstellungen steht, der "Signature Certificate Assertion encryption" sagt, bedeutet dies, dass OKTA die Zertifikatsvalidierung durchführt. Klicken Sie auf "SAML-Einstellungen bearbeiten", klicken Sie auf Signaturzertifikat und laden Sie das neue Secure Access SAML VPN-Zertifikat hoch.

← 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.

Zugehörige Informationen

- [Secure Access Helpcenter \(Benutzerhandbuch\)](#)
- [Technischer Support und Dokumentation für Cisco Systeme](#)
- [Seite "Sicherer Zugriff auf Community"](#)
- [Neues SAML-Auth-Zertifikat für sicheren Zugriff für VPN](#)

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.