Update Secure Access SAML VPN-verificatiecertificaat (Serviceprovider-certificaat)

Inhoud

Inleiding

Achtergrondinformatie

Voorwaarden

- Vereisten

Cisco Secure Access Dashboard

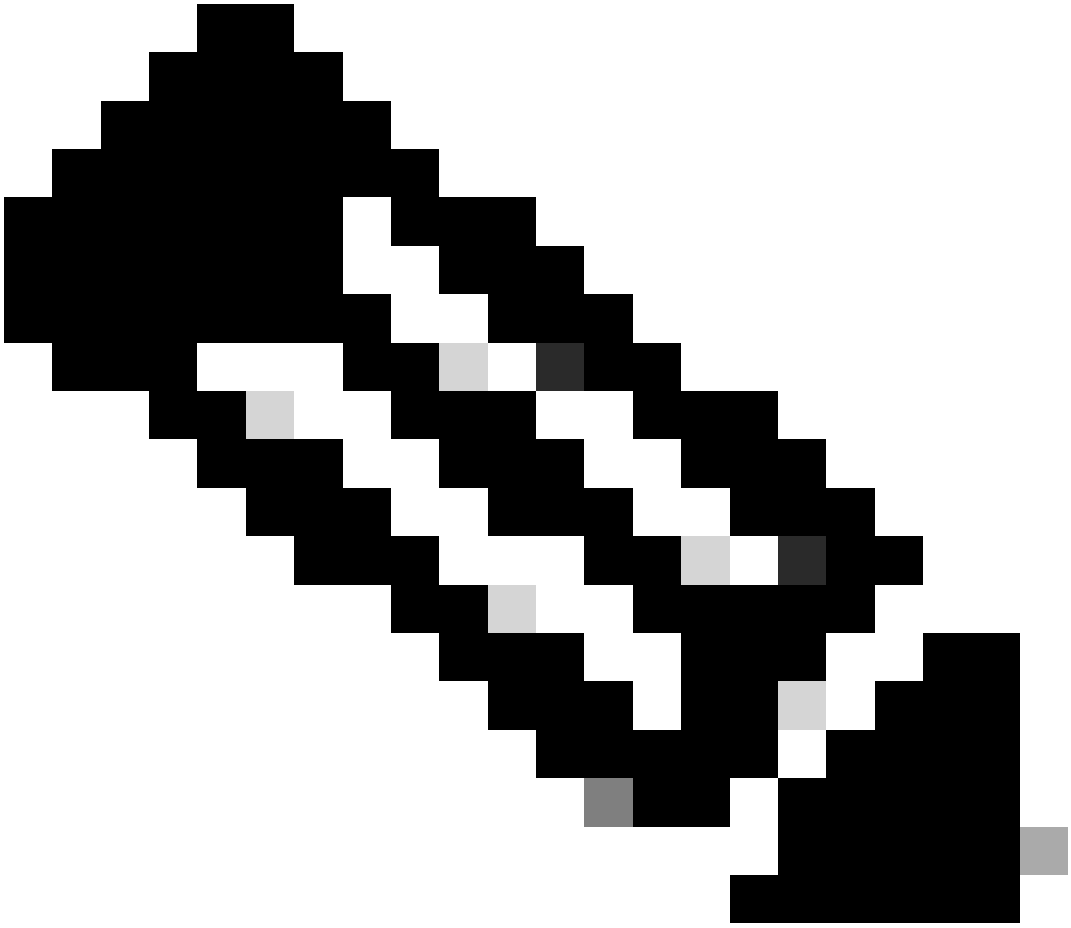
Microsoft Entra ID (Microsoft Azure)

Inleiding

In dit document worden de stappen beschreven die nodig zijn om het Identity Provider (IDP)-certificaat bij te werken met het nieuwe Secure Access Service Provider-certificaat.

Achtergrondinformatie

Het certificaat van Cisco Secure Access Security Assertion Markup Language (SAML) dat wordt gebruikt voor VPN-verificatie (Virtual Private Network) verloopt binnenkort en kan worden bijgewerkt in uw huidige IDp die wordt gebruikt voor de verificatie van VPN-gebruikers in het geval dat ze dit certificaat valideren.
Meer informatie hierover vindt u in het gedeelte Secure Access Announcements.



Opmerking: De meeste IDps verifiëren dit SAML-certificaat niet standaard en het is geen vereiste, wat betekent dat er geen verdere actie nodig is in uw IDp. Als uw IDp het Secure Access Certificate niet valideert, gaat u verder met het bijwerken van het Secure Access Certificate in uw IDp-configuratie.

Dit document beschrijft de stappen om te bevestigen of de geconfigureerde ID's certificaatsvalidatie uitvoeren: Entra ID (Azure AD), PingIdentity, Cisco DUO, OKTA.

Voorwaarden

Vereisten

- Toegang tot uw Cisco Secure Access Dashboard.
- Toegang tot uw IDp dashboard.

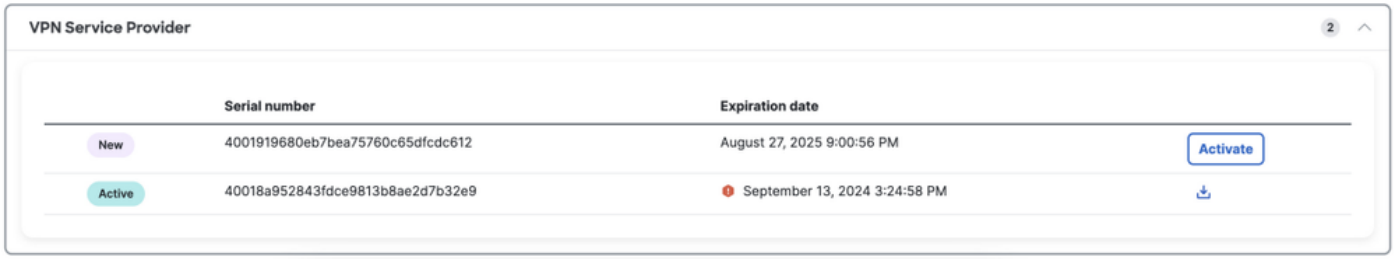
Cisco Secure Access Dashboard

Opmerking: Zorg ervoor dat na het doen van de volgende stap die het nieuwe Secure Access-certificaat activeert, als uw IDP dit certificaat valideert, update uw IDP met het nieuwe certificaat; anders kan de VPN-verificatie voor gebruikers van externe toegang mislukken.

Als u bevestigt dat uw IDp deze certificaatvalidatie uitvoert, raden we u aan het nieuwe certificaat in Secure Access te activeren en het tijdens niet-werkuren naar uw IDP te uploaden.

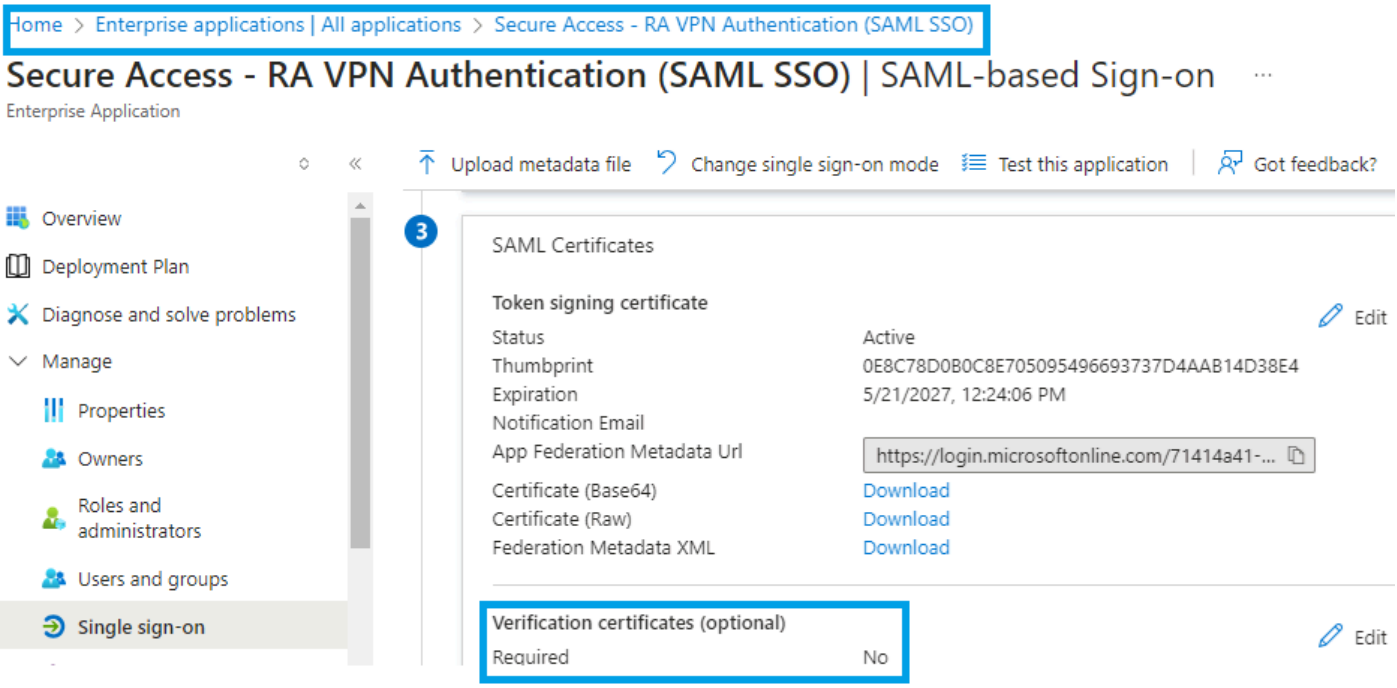
In het Secure Access Dashboard is de enige actie die nodig is om Secure > Certificaten > SAML-verificatie > Serviceprovider-certificaten te beveiligen, klik op "Nieuw"-certificaat op "Activeren".

Zodra geklikt op Activeren, kunt u het nieuwe Secure Access-certificaat downloaden om te importeren in uw IDp als het de Certificaatvalidatie uitvoert.

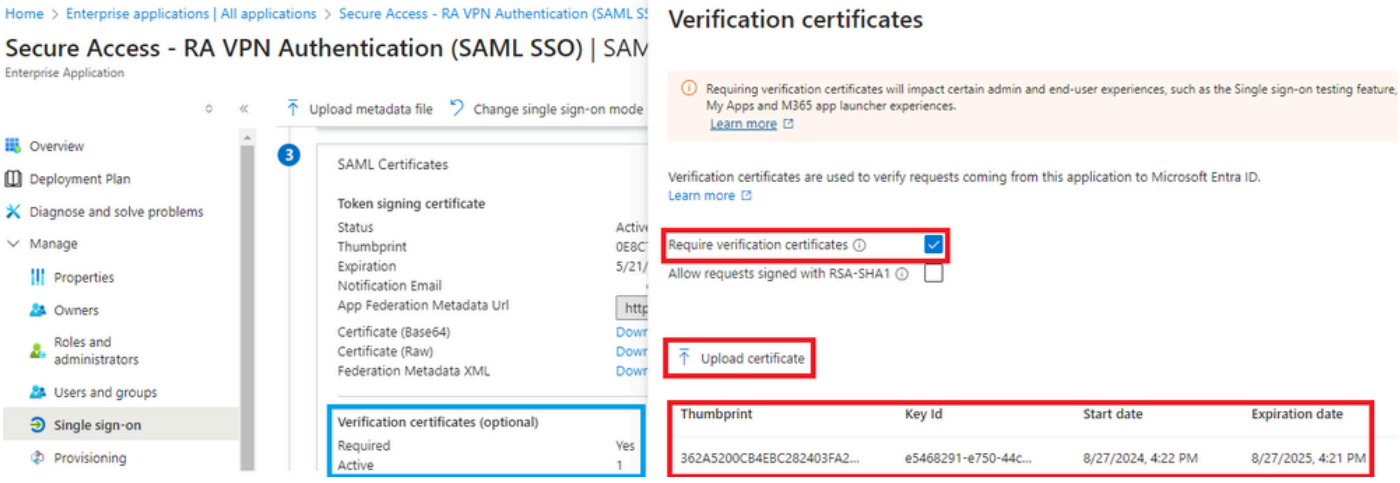


Microsoft Entra ID (Microsoft Azure)

Entra ID (Azure AD) voert standaard geen certificaatvalidatie uit.

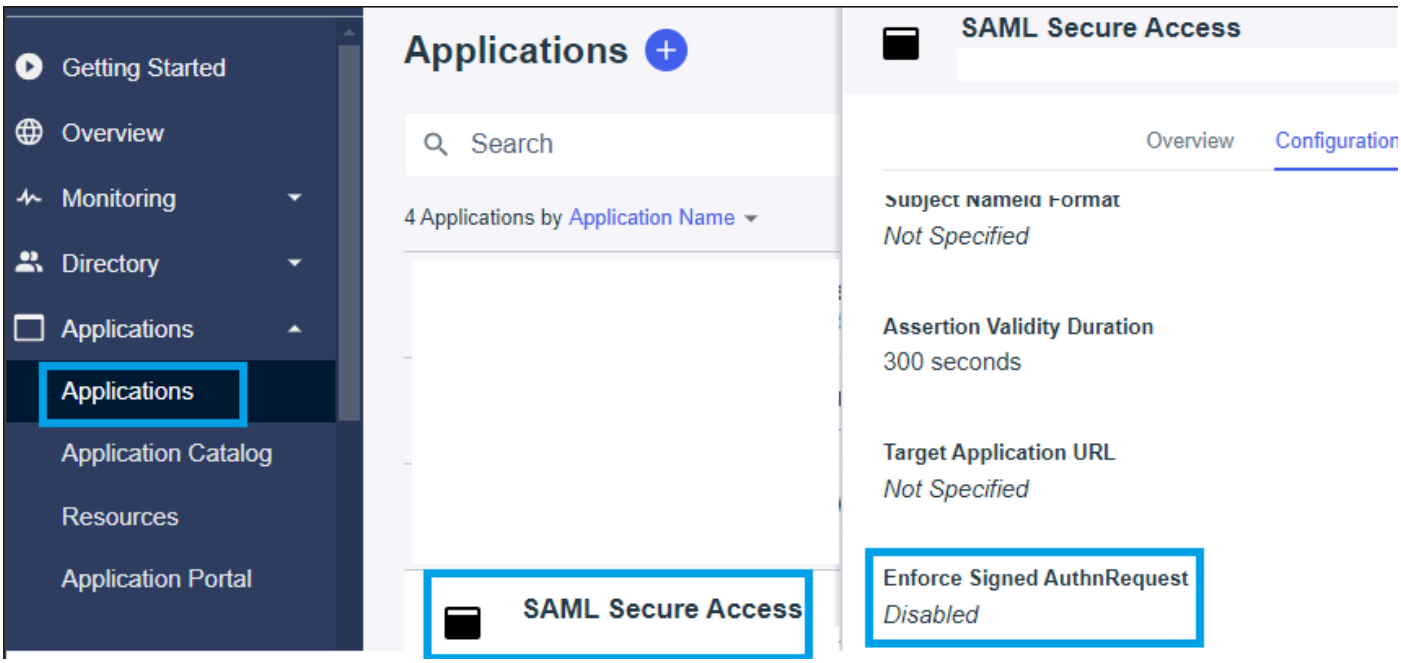


Als de IDp Entra-id de waarde "Verificatiecertificaat (optioneel)" is ingesteld op "Vereist = ja", klik dan op Bewerken en "Upload certificaat" om het nieuwe Secure Access SAML VPN-certificaat te uploaden.

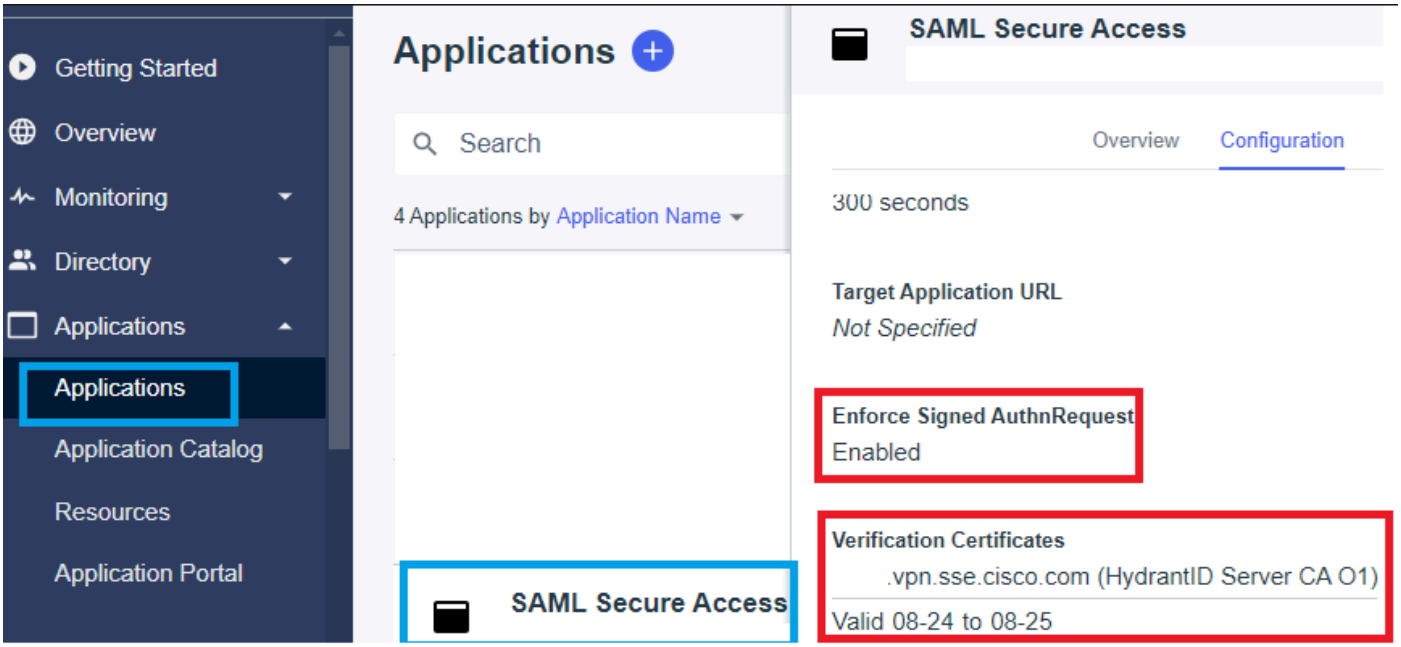


PingIdentity

PingIdentity voert standaard geen certificaatvalidatie uit.



Als in de IDp Pingidentiteits de waarde Enforce Signed Authnrequest is ingesteld op "Enabled", klik dan op Bewerken en uploaden van het nieuwe Secure Access SAML VPN-certificaat.



Cisco DUO

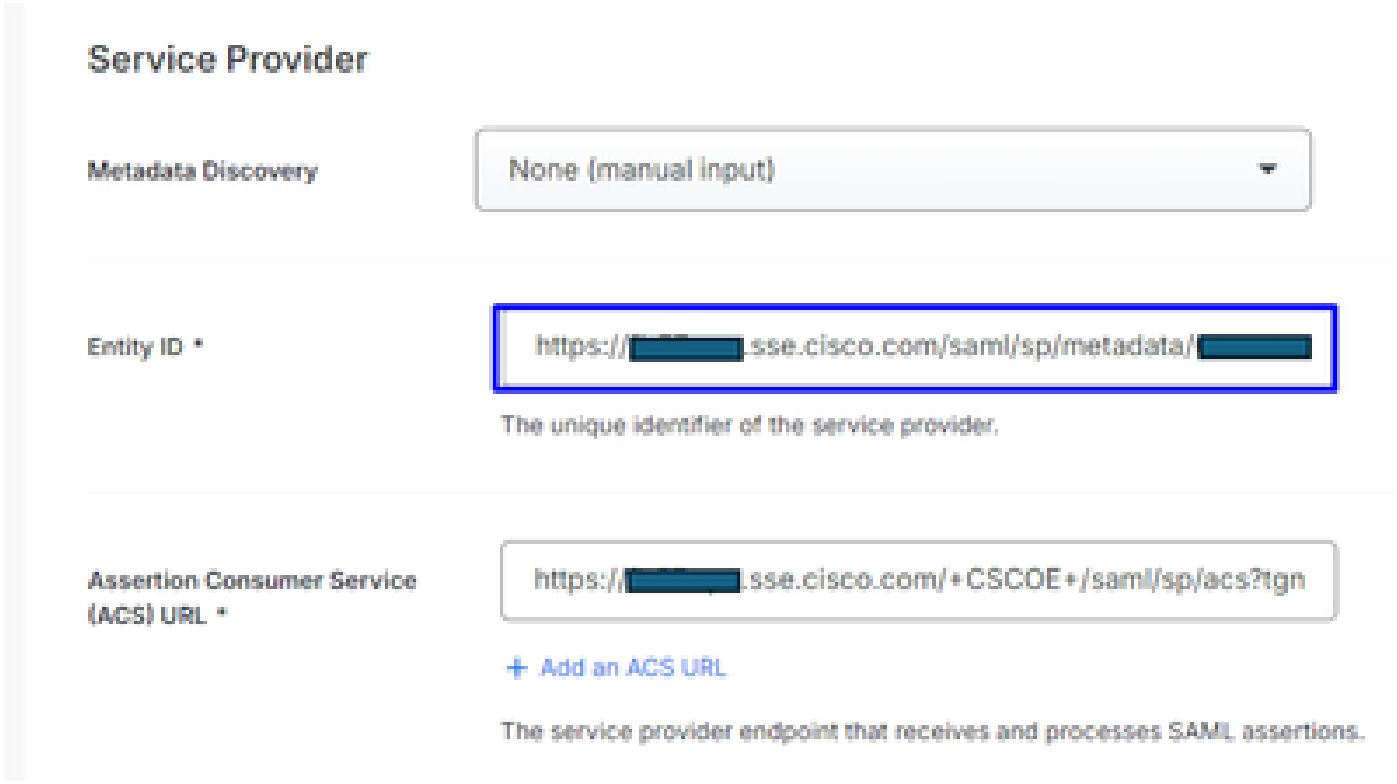
Cisco DUO ondertekent standaard de validatie van aanvragen, maar er is geen actie nodig op DUO zelf, tenzij de Assertion Encryption is ingeschakeld.

voor een verzoek kan de DUO het nieuwe certificaat downloaden via de metagegevens-entiteit-ID-link die door de beheerder wordt geboden.

Reactie- en aanhoudingsactie ondertekenen

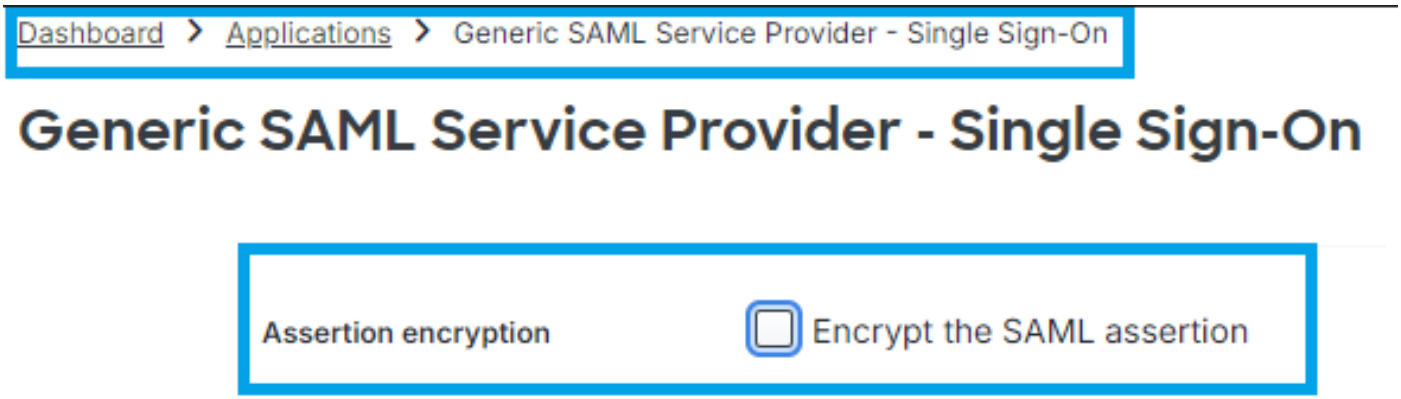
Instellingen entiteit-ID

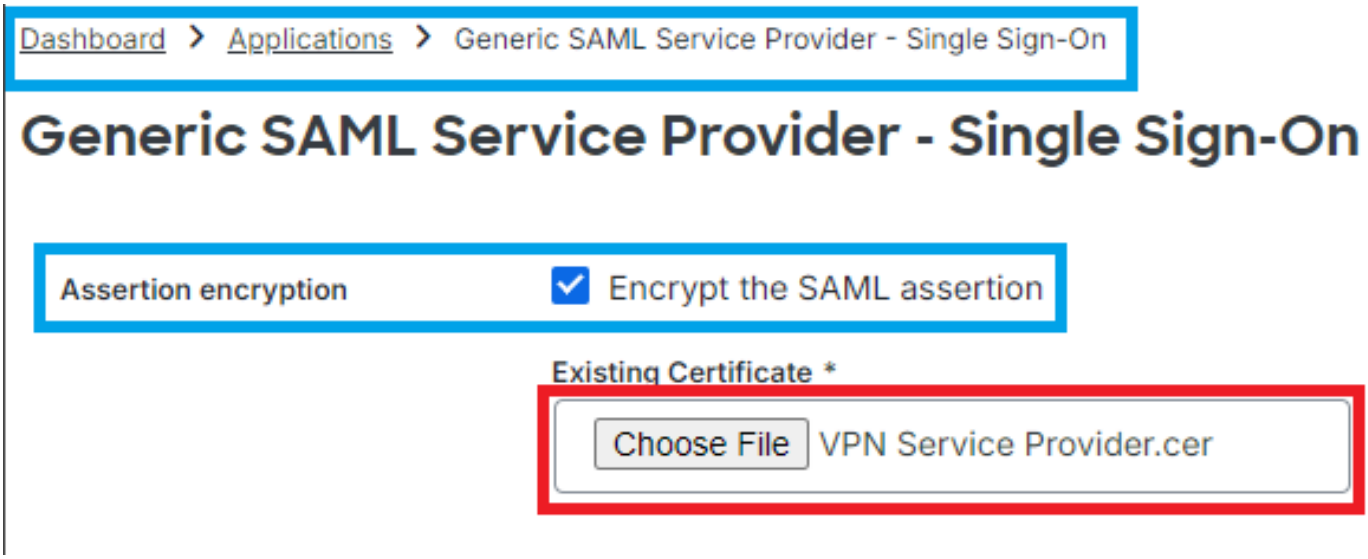
In deze stap is geen actie vereist. Het DUO kan het nieuwe certificaat ophalen uit de link Entiteit-ID: https://<entry-id>.vpn.sse.cisco.com/saml/sp/metadata/<profile_name>.



Assertion-encryptie

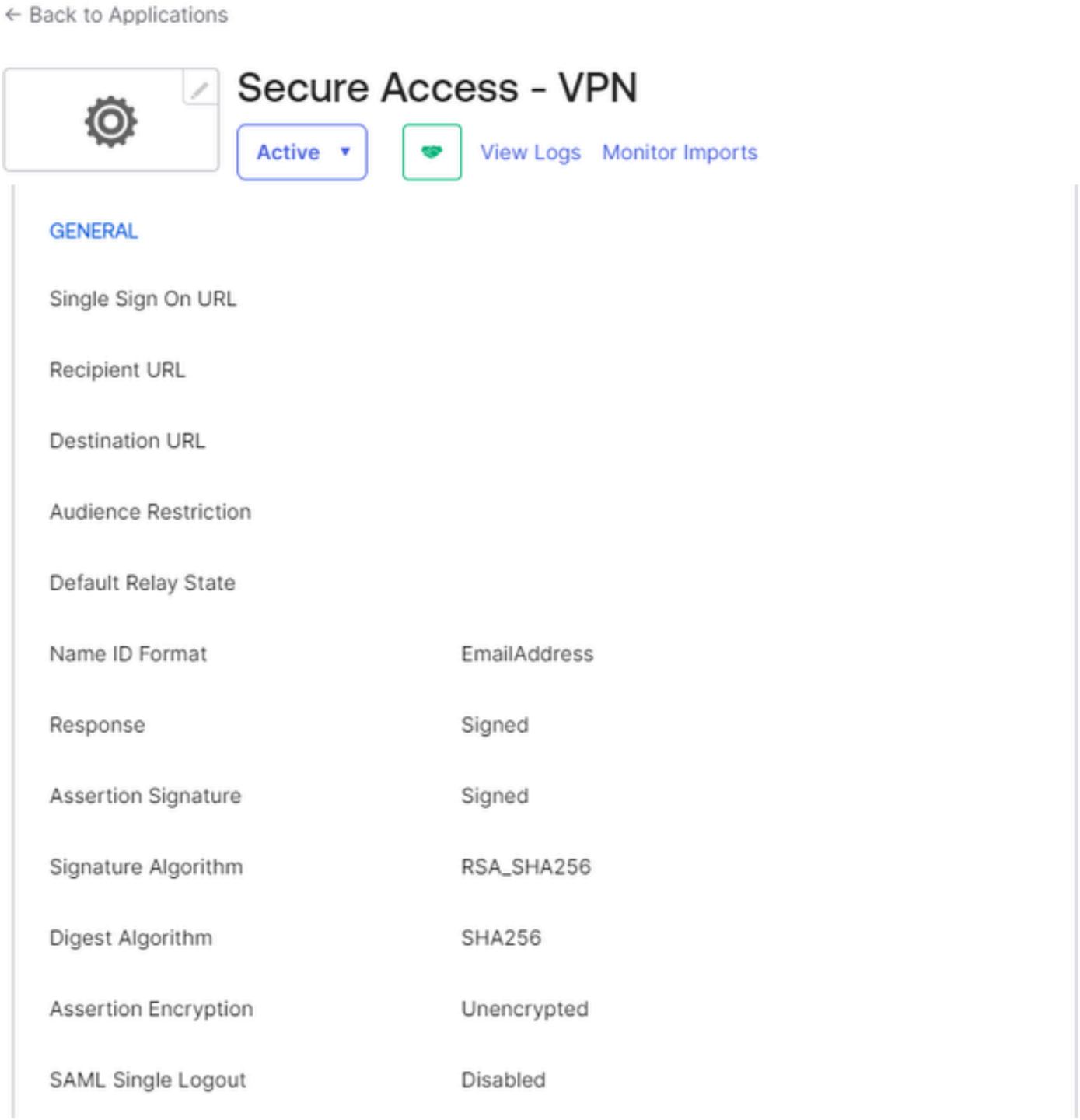
Als in de IDp Cisco DUO de waarde "Assertion encryptie" de markering "Encrypt the SAML Assertion" heeft, klik dan op "Select File" en upload het nieuwe Secure Access SAML VPN-certificaat.



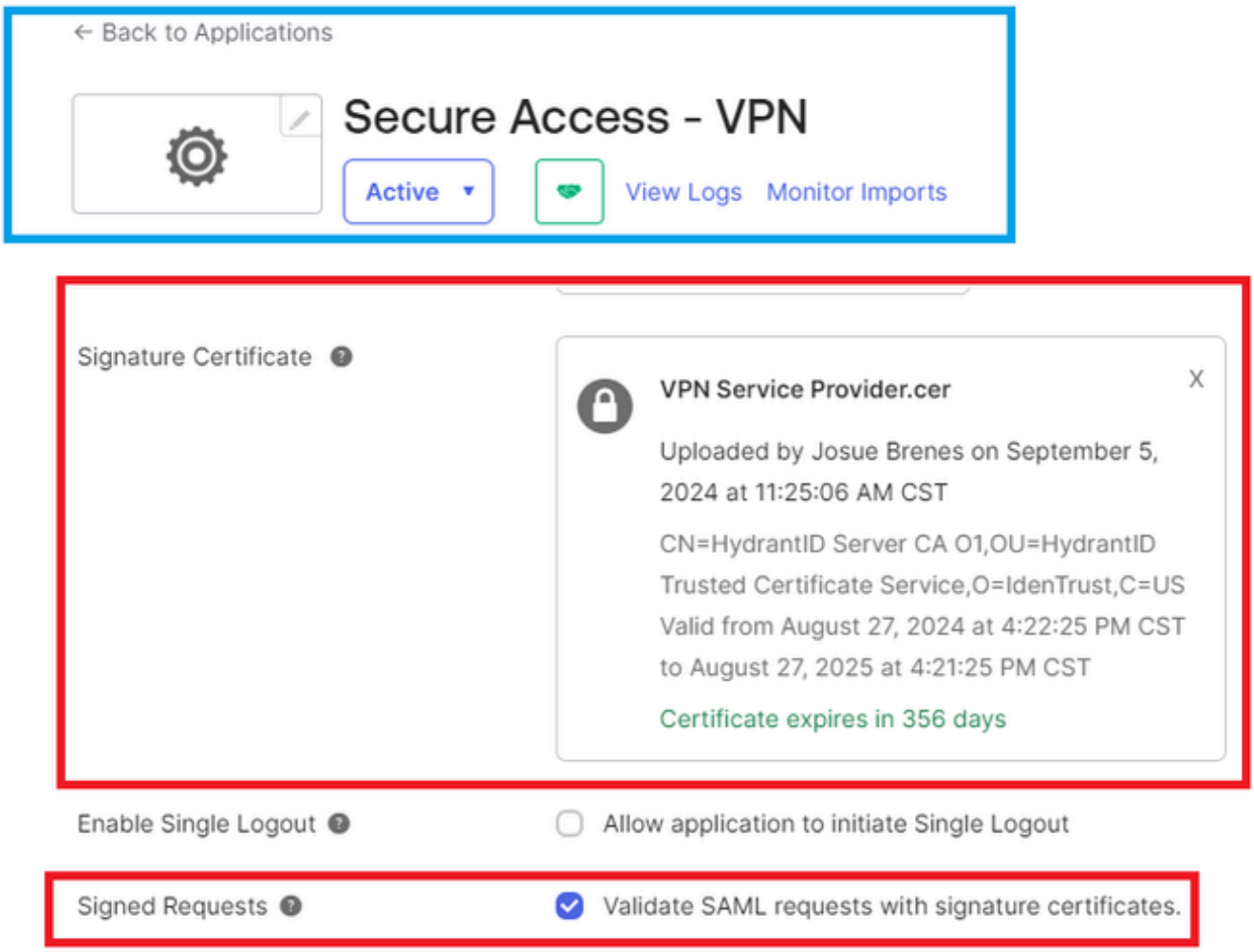


OKTA

OKTA voert standaard geen certificaatvalidatie uit. Onder General > SAML Settings is er geen optie waar staat "Signature Certificate".



Als er in de IDP OKTA een waarde onder General > SAML Settings staat, die zegt "Signature Certificate Assertion encryptie" betekent dat OKTA Certificaat Validatie doet. Klik op "SAML-instellingen bewerken", klik op Handtekeningcertificaat en upload het nieuwe Secure Access SAML VPN-certificaat.



Gerelateerde informatie

- [Secure Access Help Center (gebruikershandleiding)]
- [Technische ondersteuning en documentatie – Cisco Systems]
- [Secure Access-communitypagina]
- [Nieuw Secure Access SAML-autorisatiecertificaat voor VPN]

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.