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

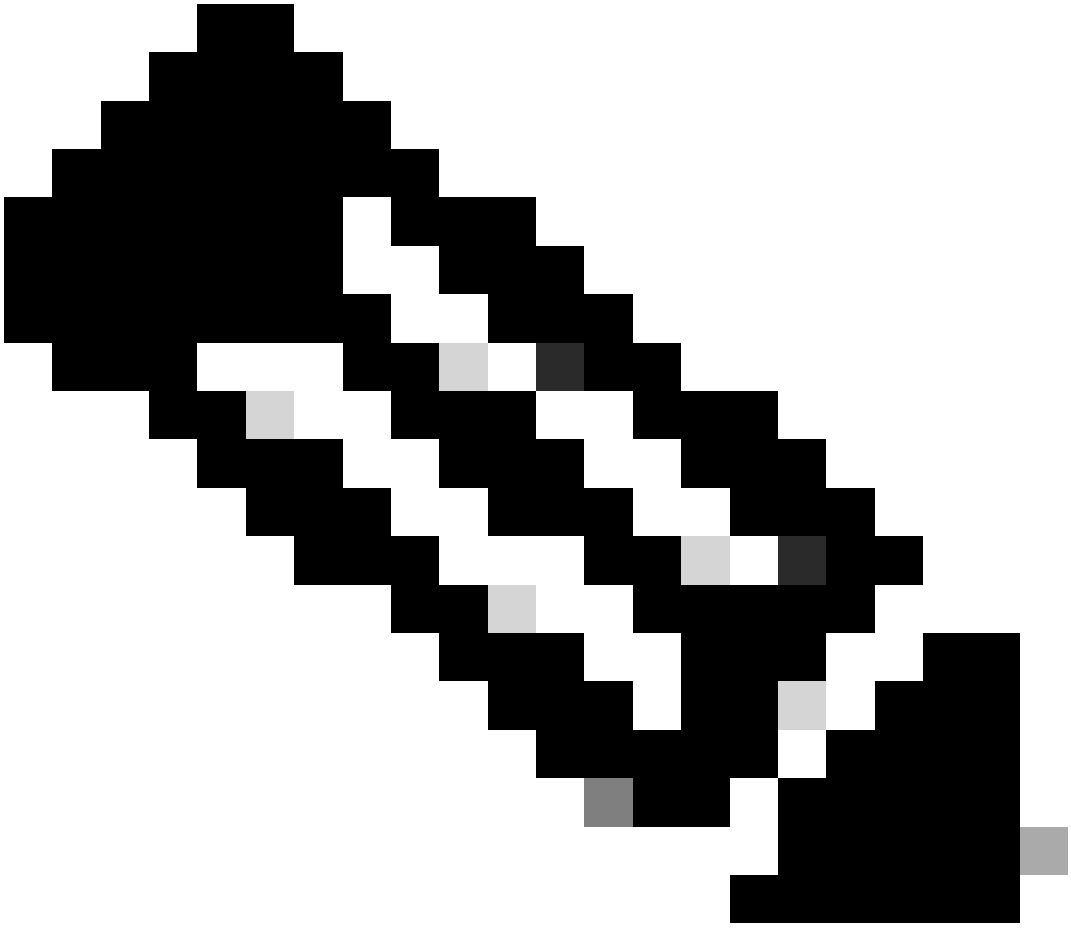
Inhalt

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.

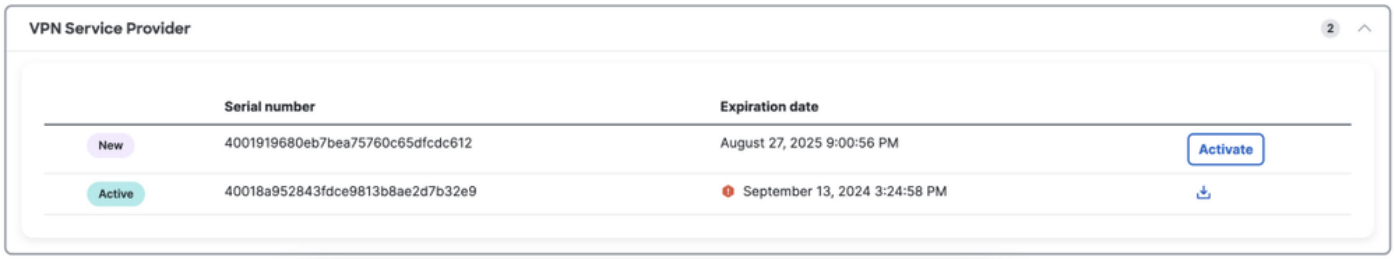
Cisco Secure Access Dashboard

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.

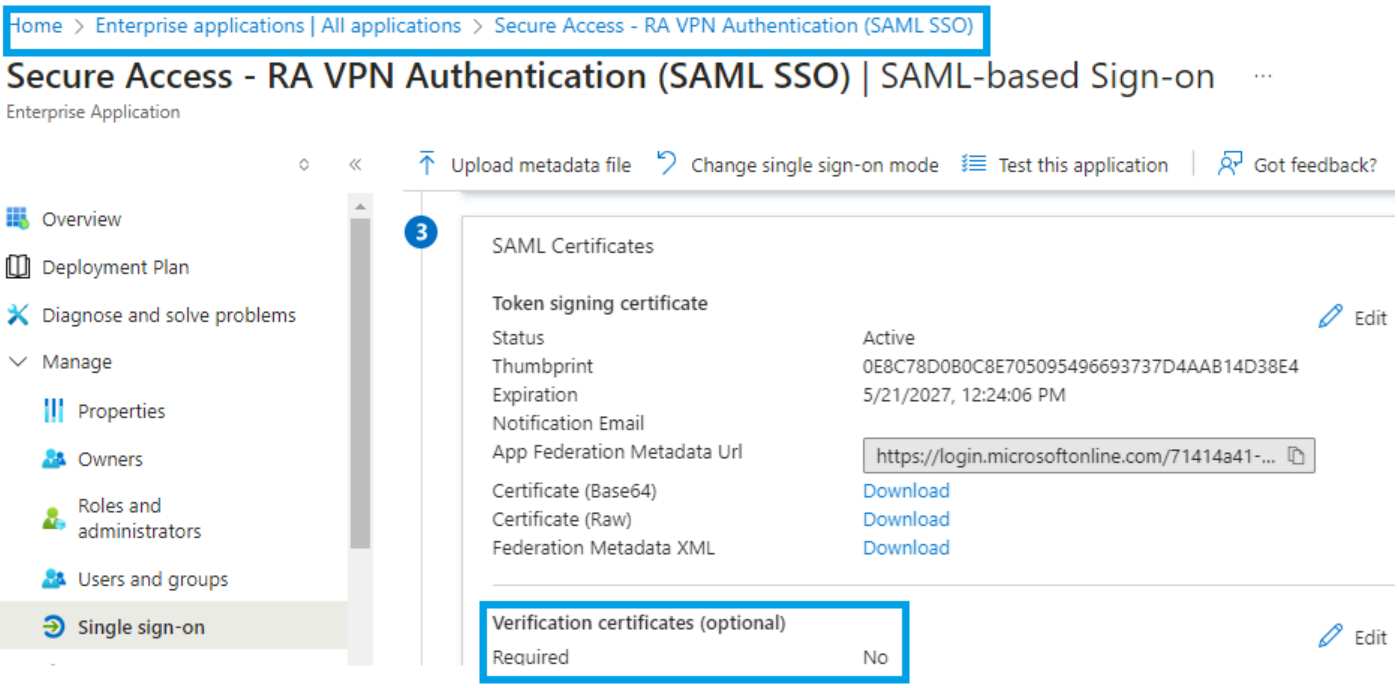
Im Secure Access Dashboard ist die einzige Aktion, die Sie durchführen müssen, Secure > Certificates > SAML Authentication > Service Provider Certificates. Klicken Sie im "New" Certificate auf "Activate".

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.

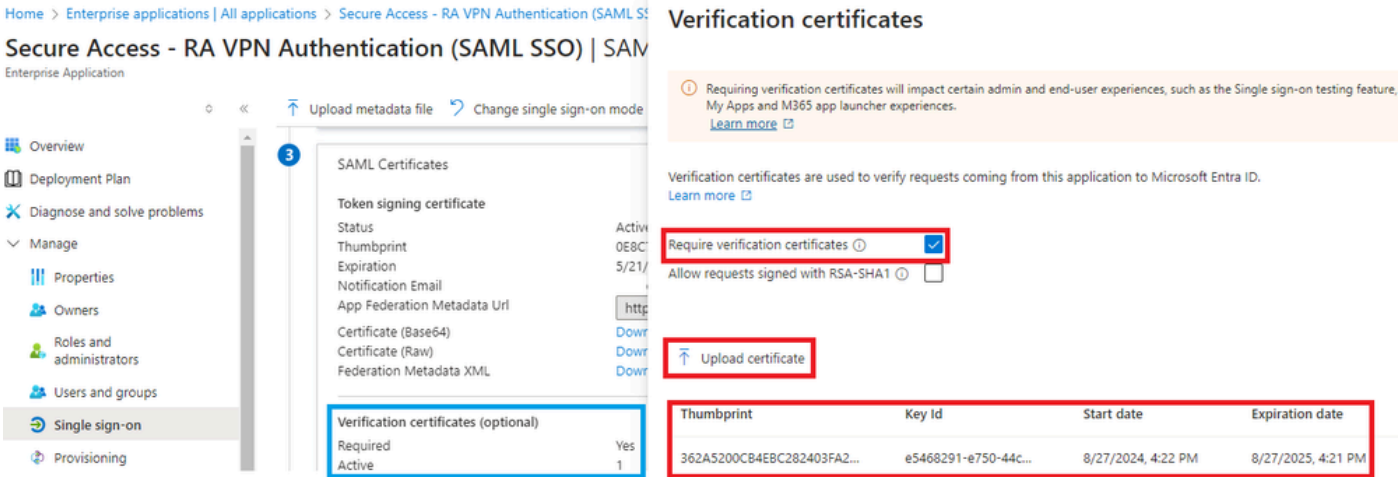


Microsoft Entra ID (Microsoft Azure)

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

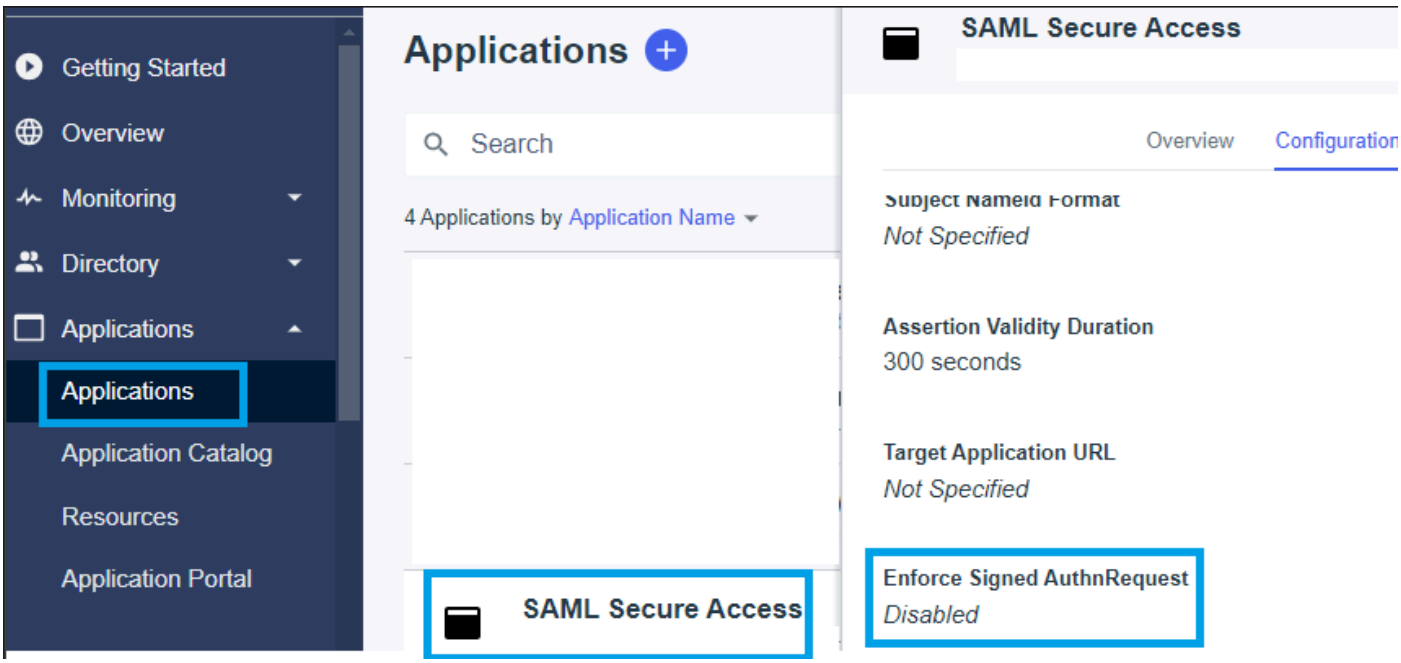


Wenn die IdP Entra ID den Wert "Verification Certificate (optional)" auf "Required = yes" gesetzt hat, klicken Sie auf Edit und "Upload certificate", um das neue Secure Access SAML VPN Certificate hochzuladen.

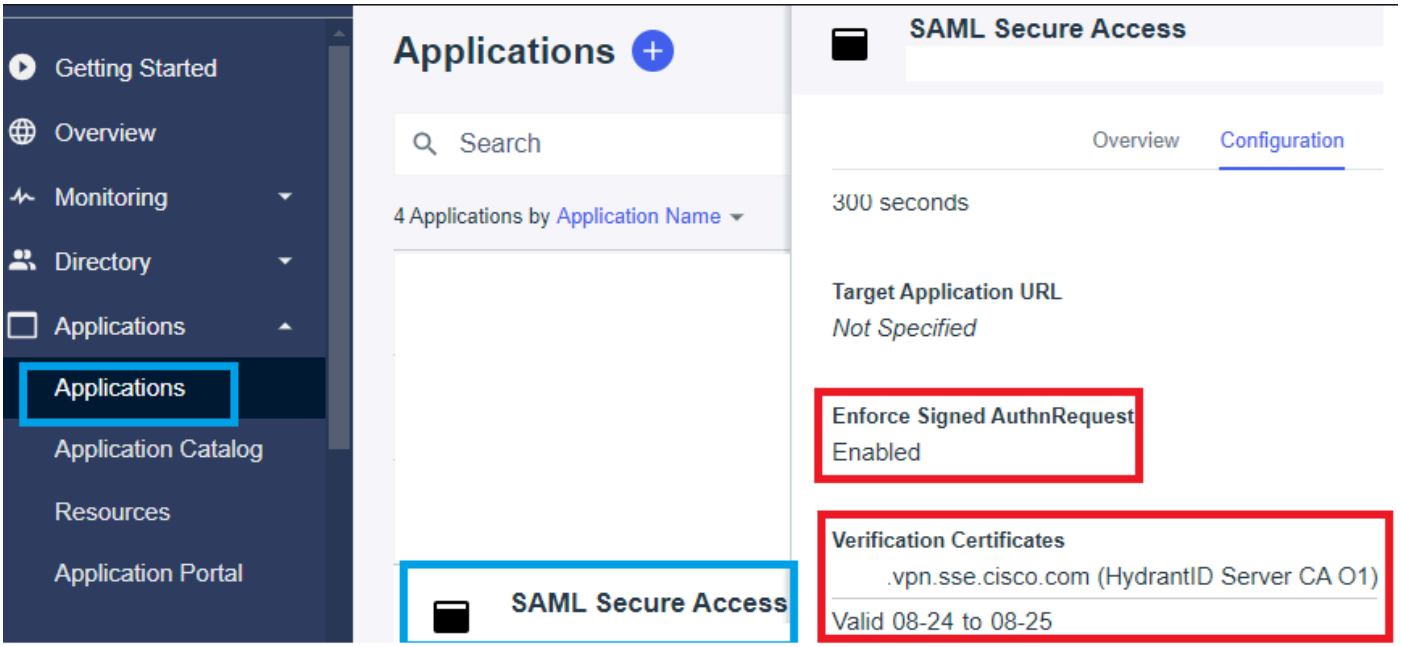


PingIdentity

PingIdentity führt standardmäßig keine Zertifikatsvalidierung durch.



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.



Cisco DUO

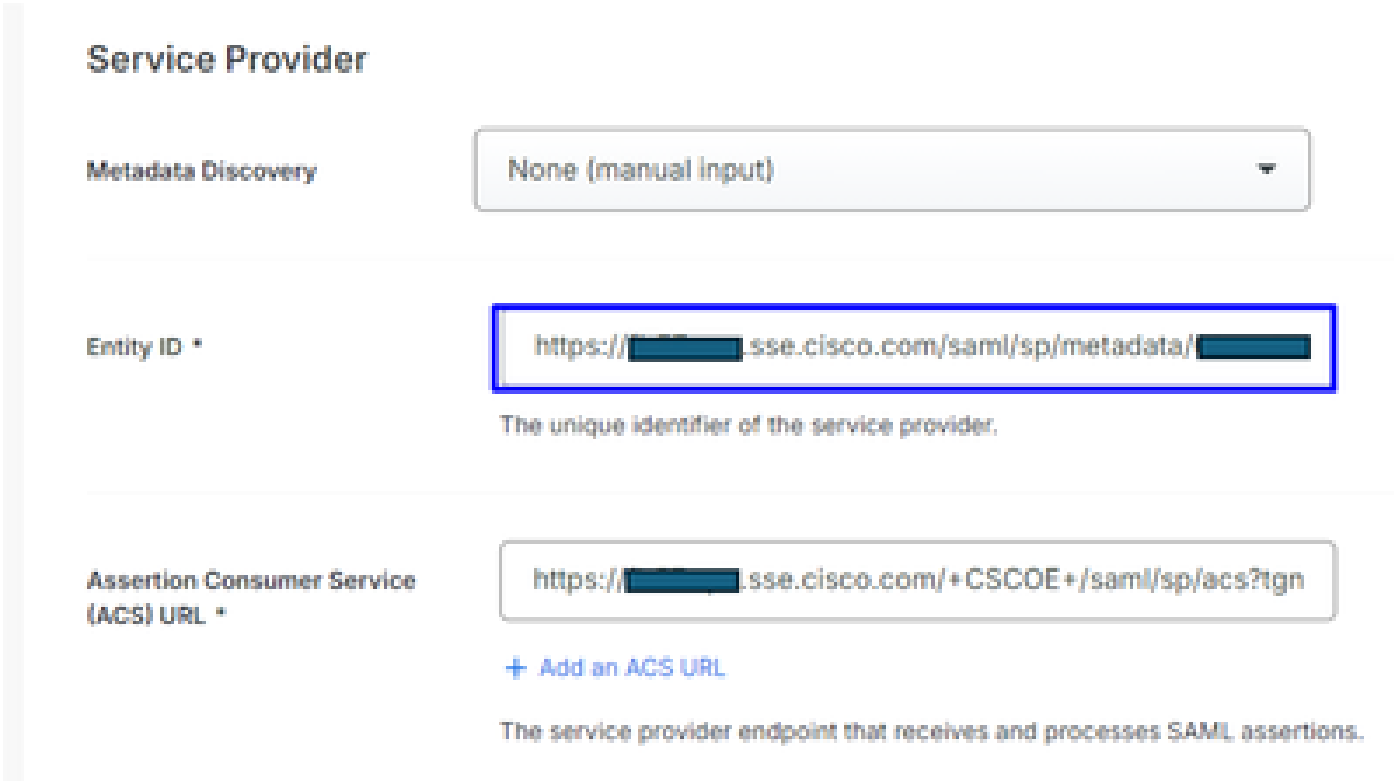
Cisco DUO führt standardmäßig eine Validierung der Signierungsanforderung durch. Es ist jedoch keine Aktion für das DUO selbst erforderlich, es sei denn, die Assertion Encryption ist aktiviert.

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

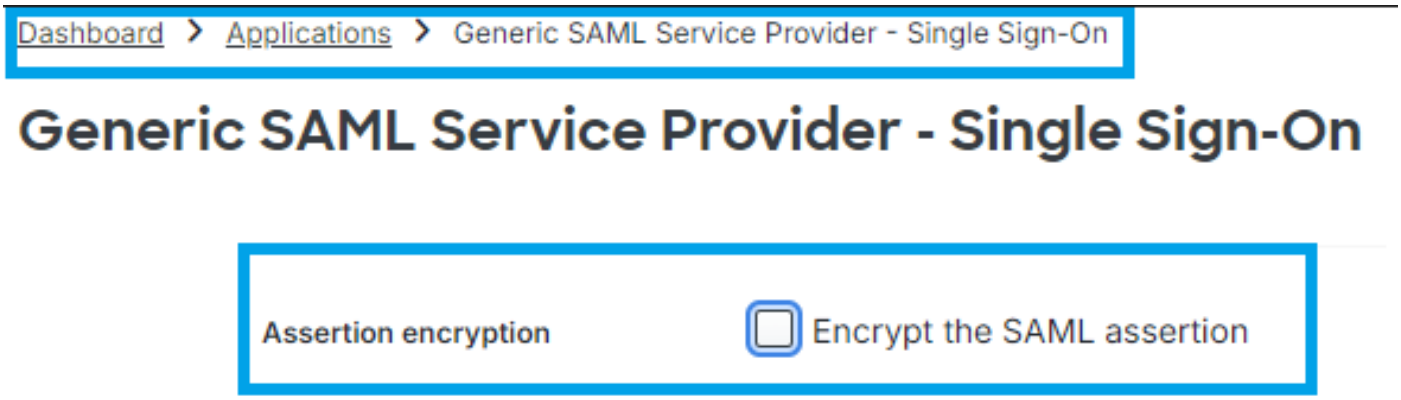
Einheiten-ID-Einstellungen

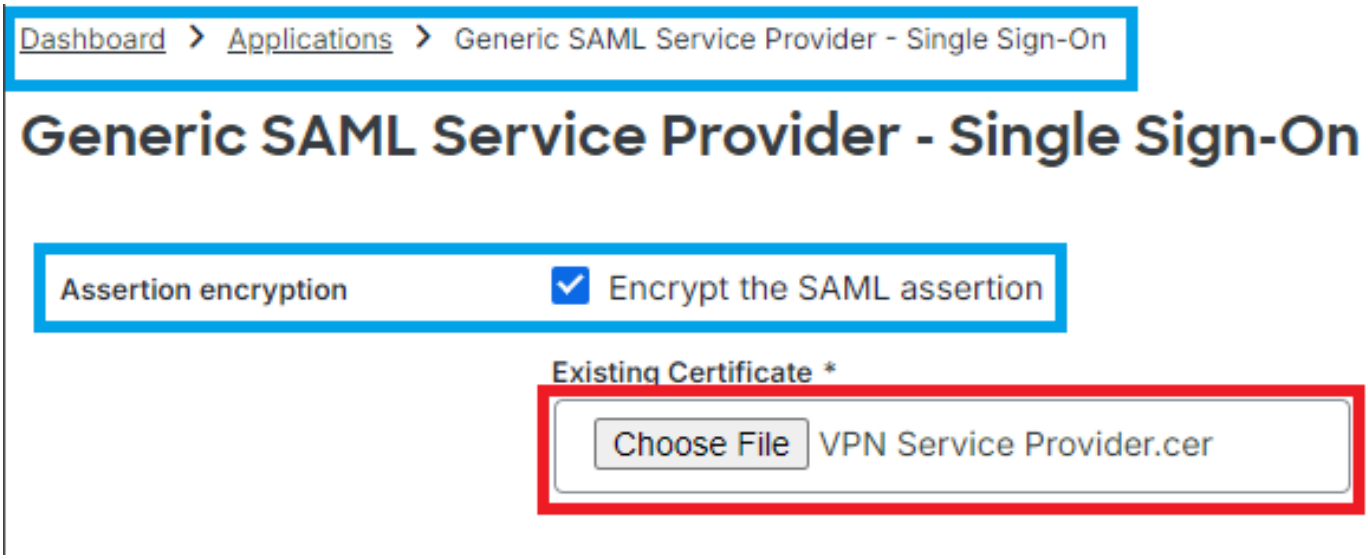
In diesem Schritt ist keine Aktion erforderlich. Das DUO kann das neue Zertifikat aus dem Link für die Element-ID abrufen: https://<entry-id>.vpn.sse.cisco.com/saml/sp/metadata/<profile_name>.



Assertion Encryption

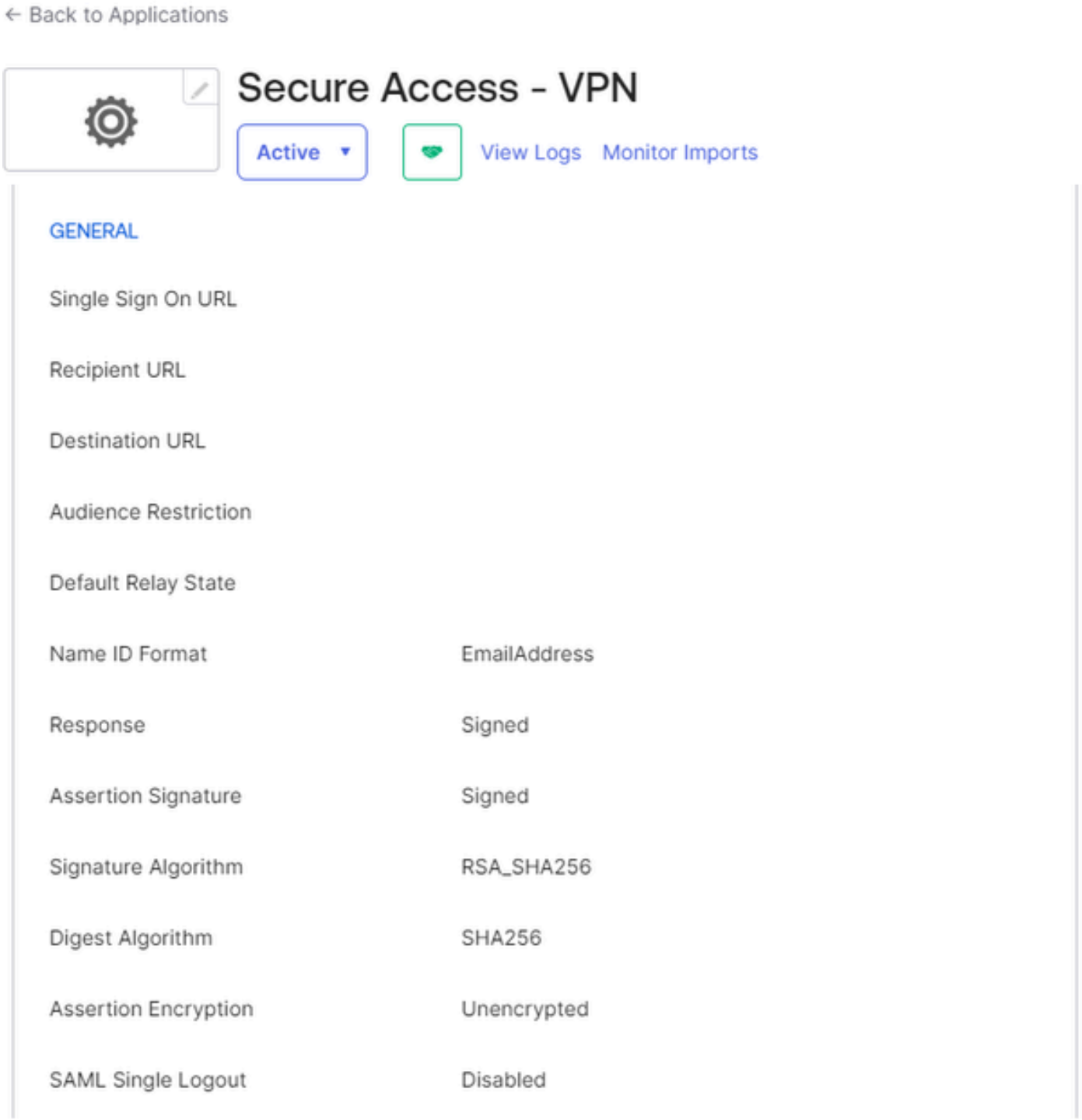
Wenn im IdP Cisco DUO der Wert "Assertion encryption" mit "Encrypt the SAML Assertion" markiert ist, klicken Sie auf "Choose File" und laden Sie das neue Secure Access SAML VPN Certificate hoch.



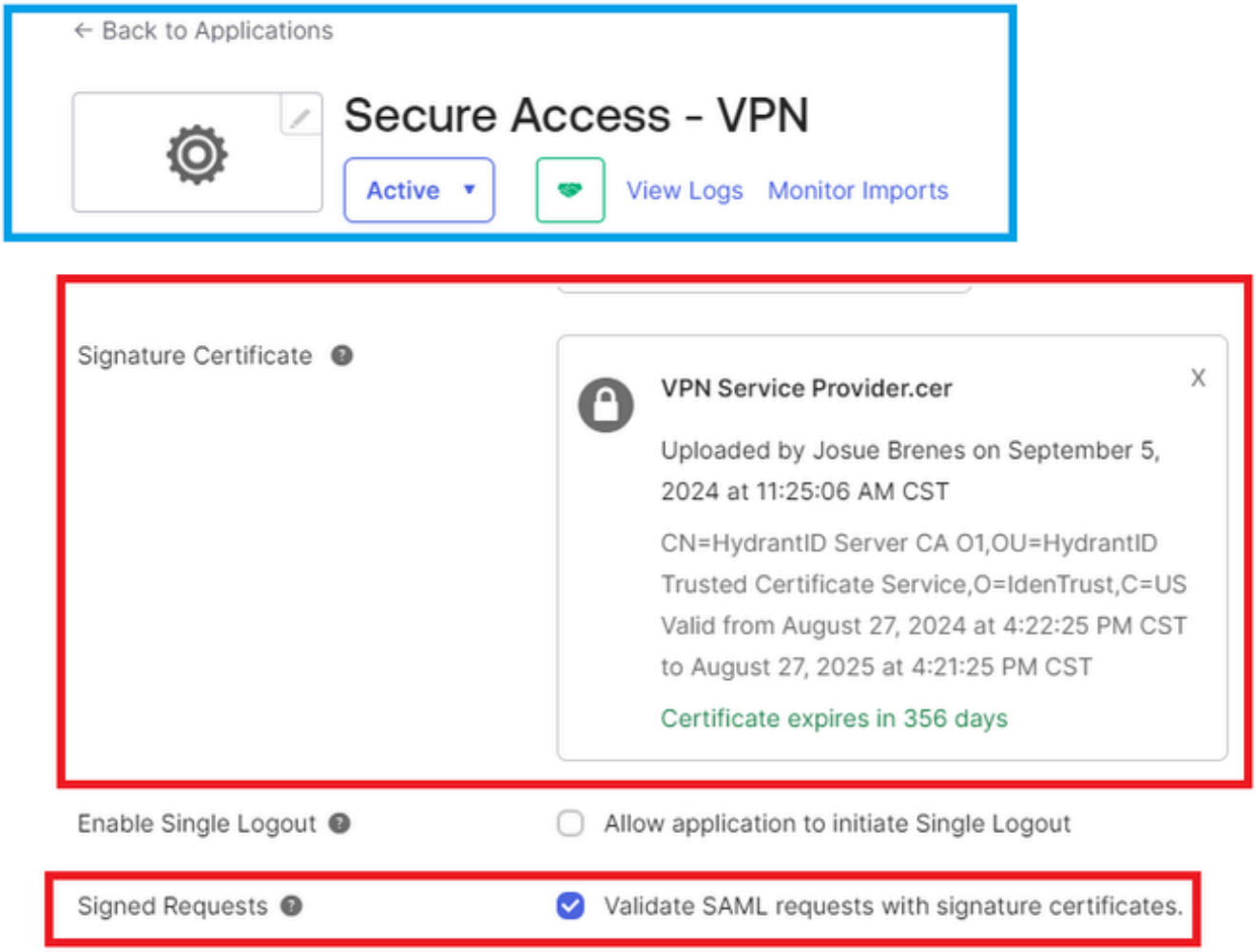


OKTA

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



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.



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.