Mettre à jour le certificat d'authentification SAML VPN d'accès sécurisé (certificat du fournisseur de services)

Table des matières

Introduction

Informations générales

Conditions préalables

- Exigences

Tableau de bord Cisco Secure Access

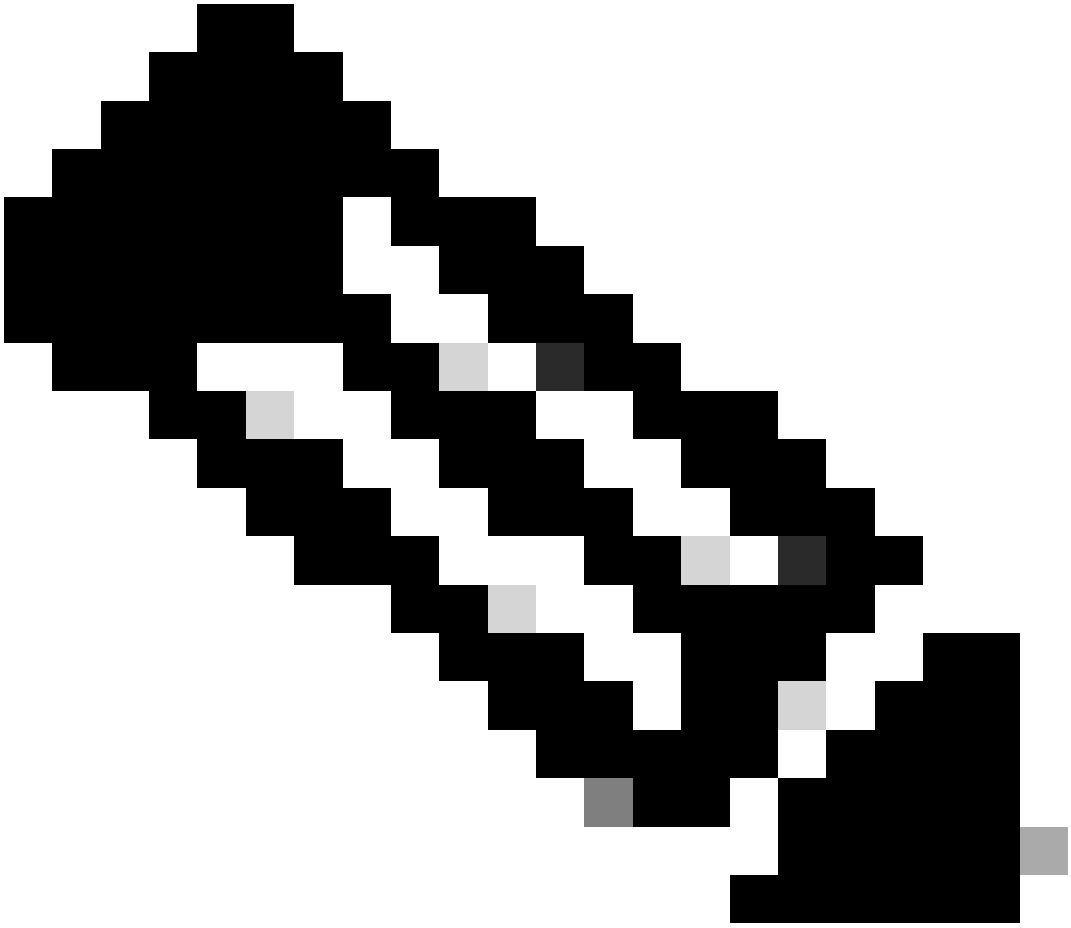
Microsoft Entra ID (Microsoft Azure)

Introduction

Ce document décrit les étapes requises pour mettre à jour le certificat du fournisseur d'identité (IdP) avec le nouveau certificat du fournisseur de services d'accès sécurisé.

Informations générales

Le certificat Cisco Secure Access Security Assertion Markup Language (SAML) utilisé pour l'authentification VPN (Virtual Private Network) arrive bientôt à expiration et peut être mis à jour dans votre IdP actuel utilisé pour authentifier les utilisateurs VPN dans le cas où ils valident ce certificat.
Pour plus d'informations à ce sujet, consultez la section Annonces d'accès sécurisé.



Remarque : la plupart des fournisseurs d'identités ne vérifient pas ce certificat SAML par défaut et ce n'est pas obligatoire, ce qui signifie qu'aucune autre action n'est nécessaire dans votre fournisseur d'identités. Si votre fournisseur d'accès Internet ne valide pas le certificat d'accès sécurisé, continuez avec la mise à jour du certificat d'accès sécurisé dans votre configuration de fournisseur d'accès.

Ce document couvre les étapes pour confirmer si les IdP configurés effectuent la validation de certificat : Entra ID (Azure AD), PingIdentity, Cisco DUO, OKTA.

Conditions préalables

Exigences

- Accédez à votre tableau de bord Cisco Secure Access.
- Accédez à votre tableau de bord IdP.

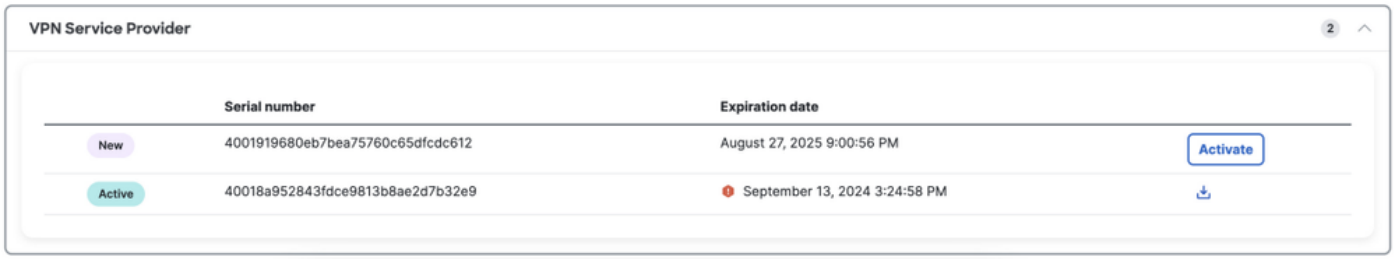
Tableau de bord Cisco Secure Access

Remarque : assurez-vous qu'après avoir effectué l'étape suivante consistant à activer le nouveau certificat d'accès sécurisé, si votre fournisseur d'accès effectue cette validation de certificat, mettez à jour votre fournisseur d'accès avec le nouveau certificat ; sinon, l'authentification VPN pour les utilisateurs d'accès à distance peut échouer.

Si vous confirmez que votre fournisseur d'identités procède à cette validation de certificat, nous vous recommandons d'activer le nouveau certificat dans Secure Access et de le télécharger sur votre fournisseur d'identités pendant les heures non ouvrables.

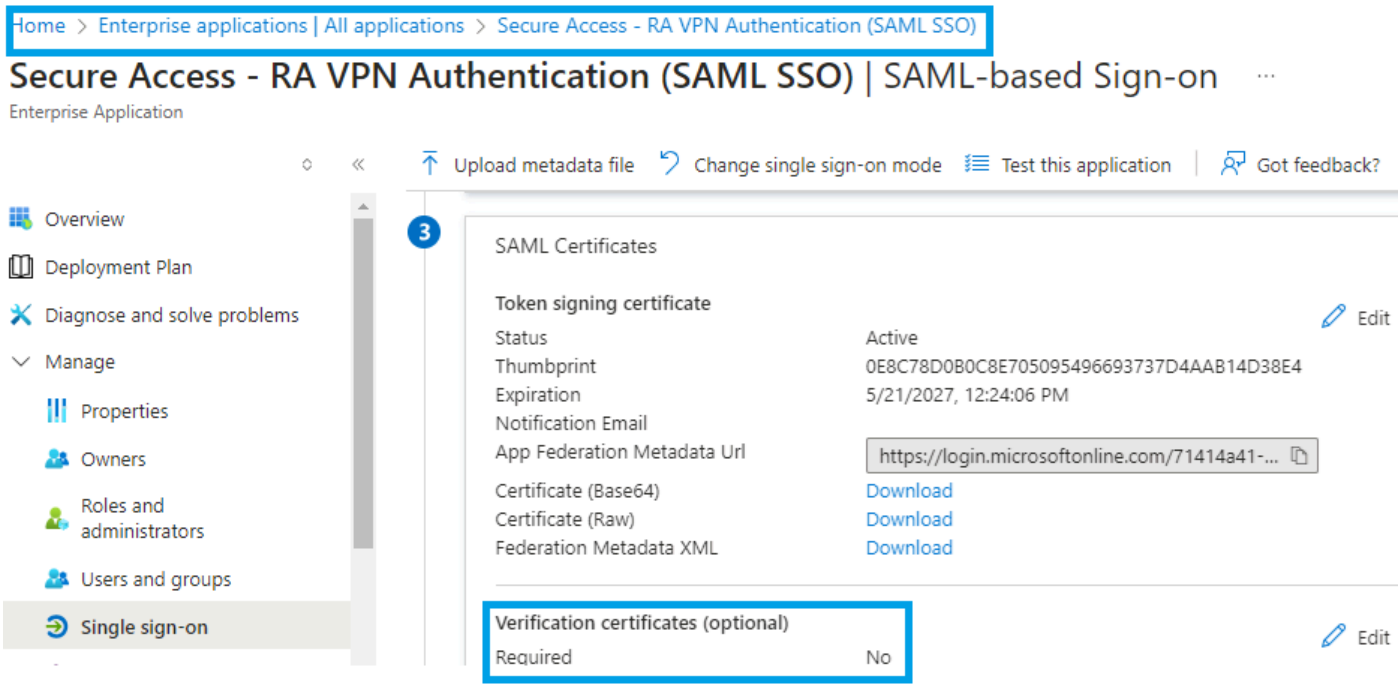
Dans le tableau de bord d'accès sécurisé, la seule action requise est d'aller à Secure > Certificates > SAML Authentication > Service Provider certificates, sur le certificat "New" cliquez sur "Activate".

Une fois que vous avez cliqué sur Activer, vous pouvez télécharger le nouveau certificat d'accès sécurisé à importer dans votre fournisseur d'identité s'il effectue la validation du certificat.

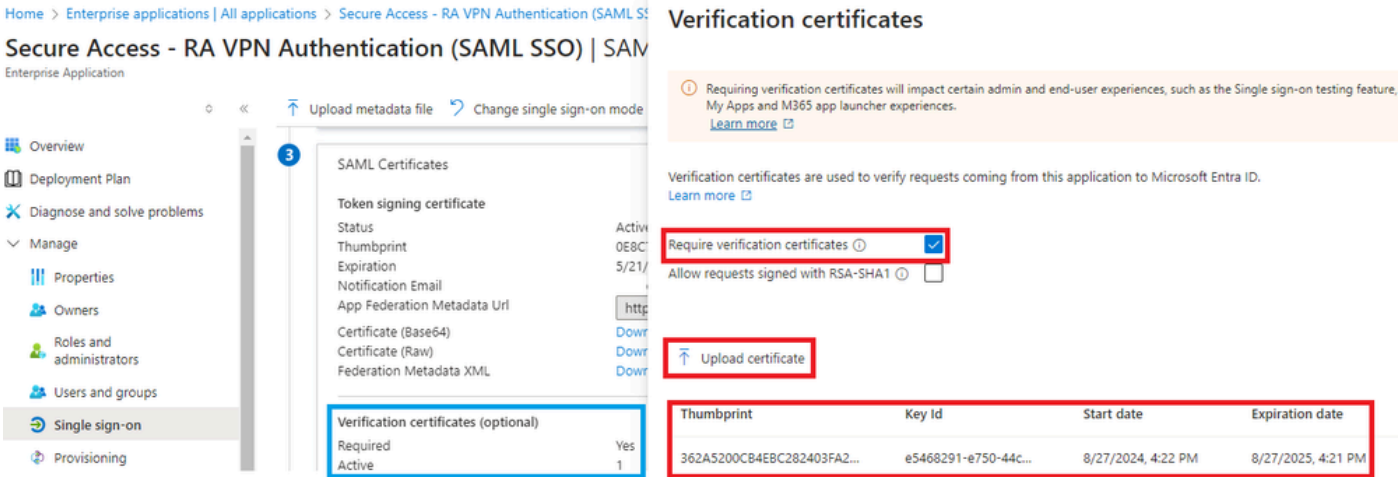


Microsoft Entra ID (Microsoft Azure)

Entra ID (Azure AD) n'effectuant pas la validation de certificat par défaut.

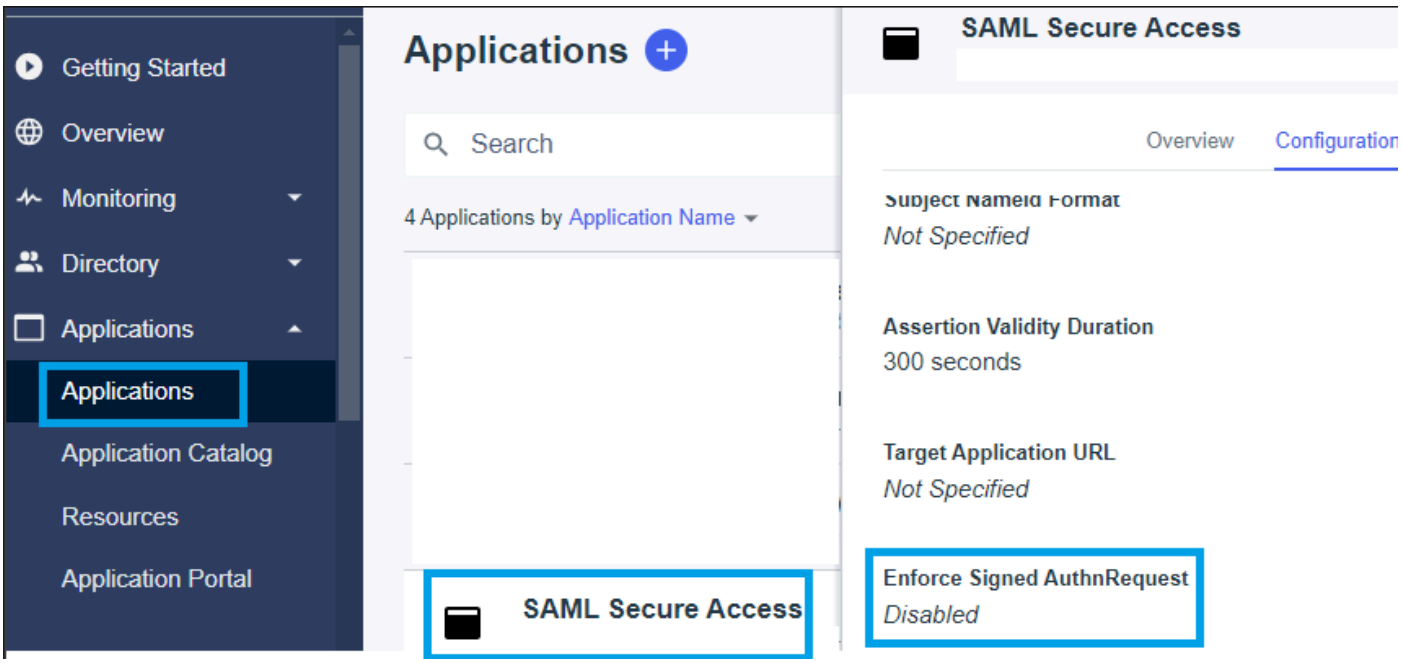


Si l'ID d'entrée du fournisseur d'identité (IdP Entra ID) et la valeur « Certificat de vérification (facultatif) » sont définis sur « Obligatoire = oui », cliquez sur Modifier et sur « Télécharger le certificat » pour télécharger le nouveau certificat VPN SAML d'accès sécurisé.

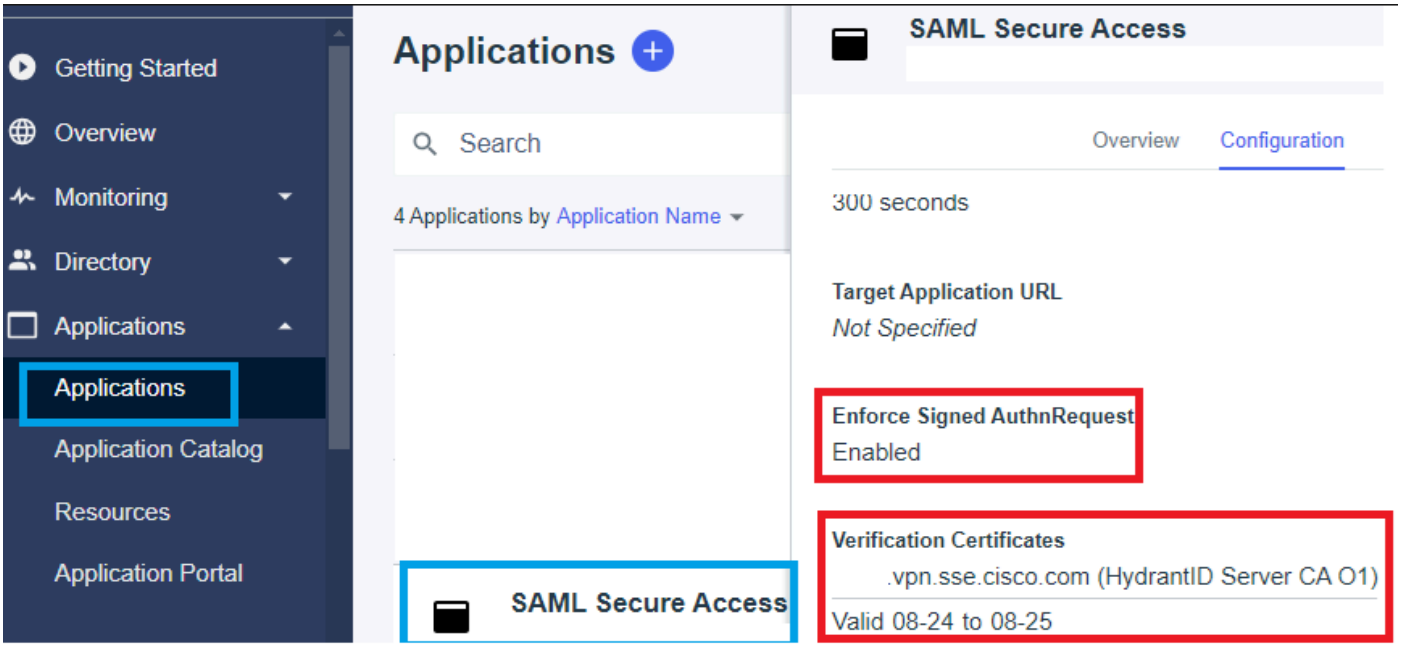


IdentitéPing

PingIdentity n'effectue pas la validation de certificat par défaut.



Si, dans IdP Pingidentity, la valeur Enforce Signed AuthnRequest est définie sur « Enabled », cliquez sur Edit et téléchargez le nouveau certificat VPN SAML d'accès sécurisé.



Cisco DUO

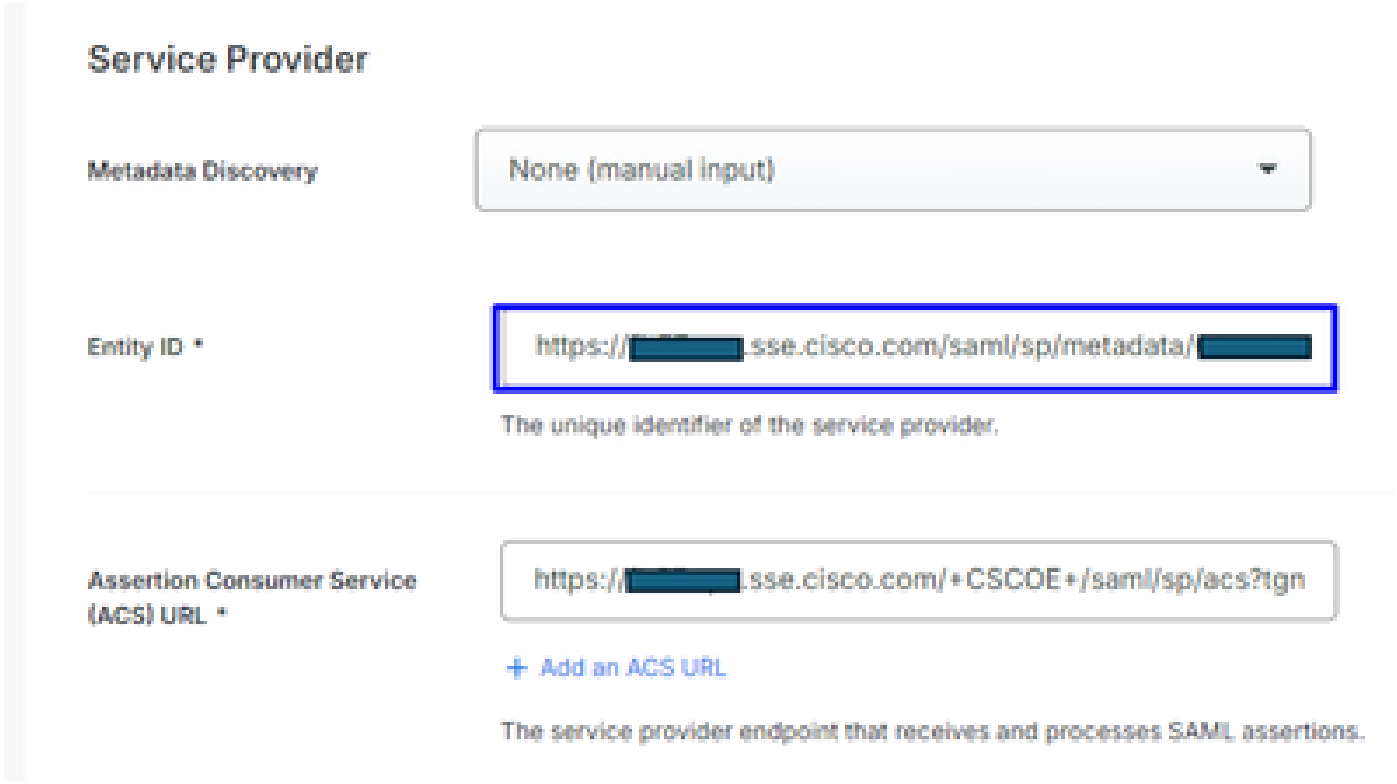
Cisco DUO effectue la validation de la demande de signature par défaut, mais il n'exige aucune action sur DUO lui-même à moins que le chiffrement d'assertion soit activé.

pour la signature de la demande, le DUO peut télécharger le nouveau certificat à l'aide du lien ID d'entité de métadonnées fourni par l'administrateur.

Action de signature de réponse et d'assertion

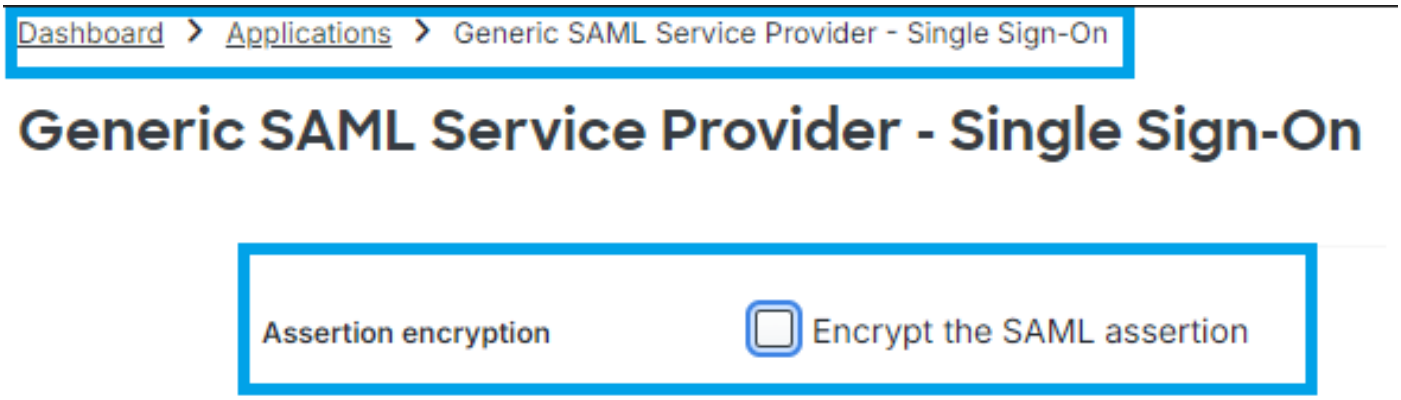
Paramètres ID entité

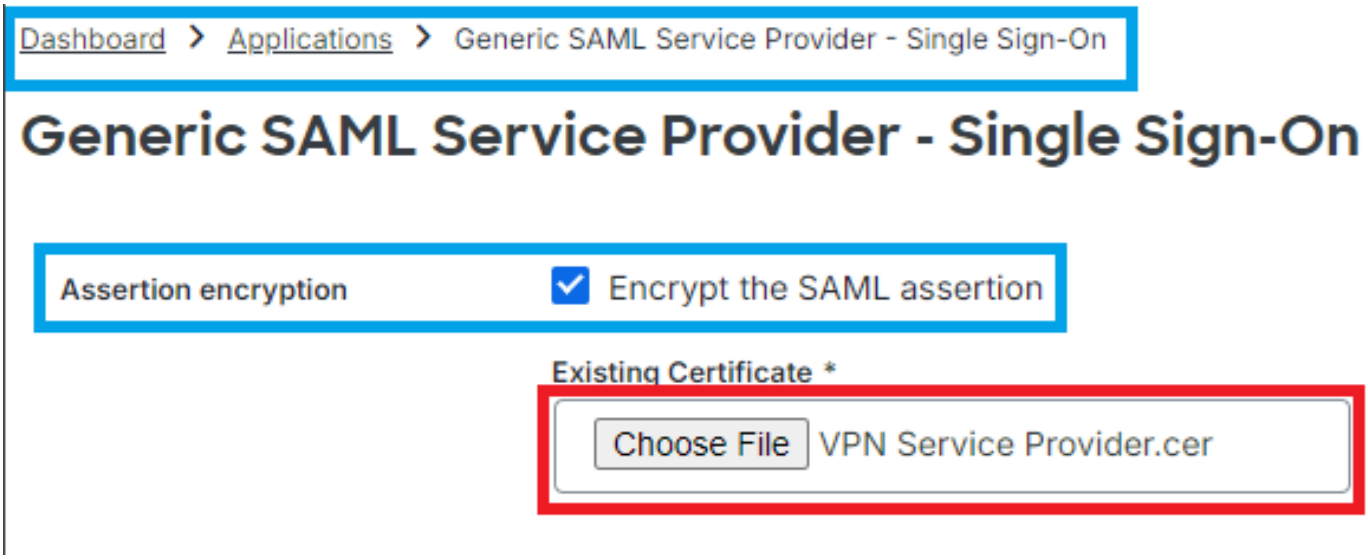
Aucune action n'est requise dans cette étape, le DUO peut extraire le nouveau certificat à partir du lien d'ID d'entité : https://<entry-id>.vpn.sse.cisco.com/saml/sp/metadata/<profile_name>.



Chiffrement d'assertion

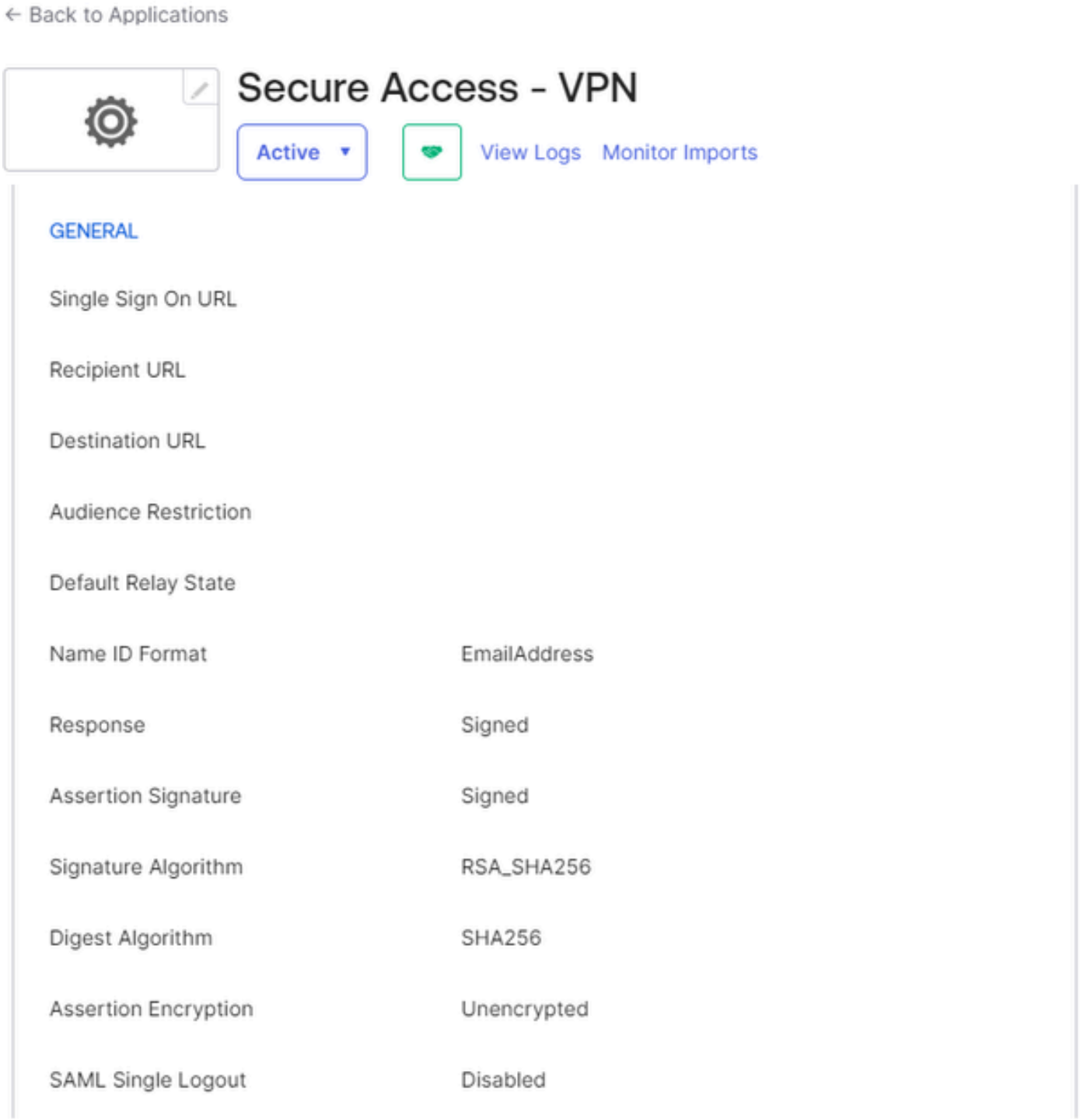
Si, dans l'IdP Cisco DUO, la valeur « Assertion encryption » a la valeur « Encrypt the SAML Assertion » marquée, cliquez sur « Choose File » et téléchargez le nouveau certificat VPN SAML d'accès sécurisé.



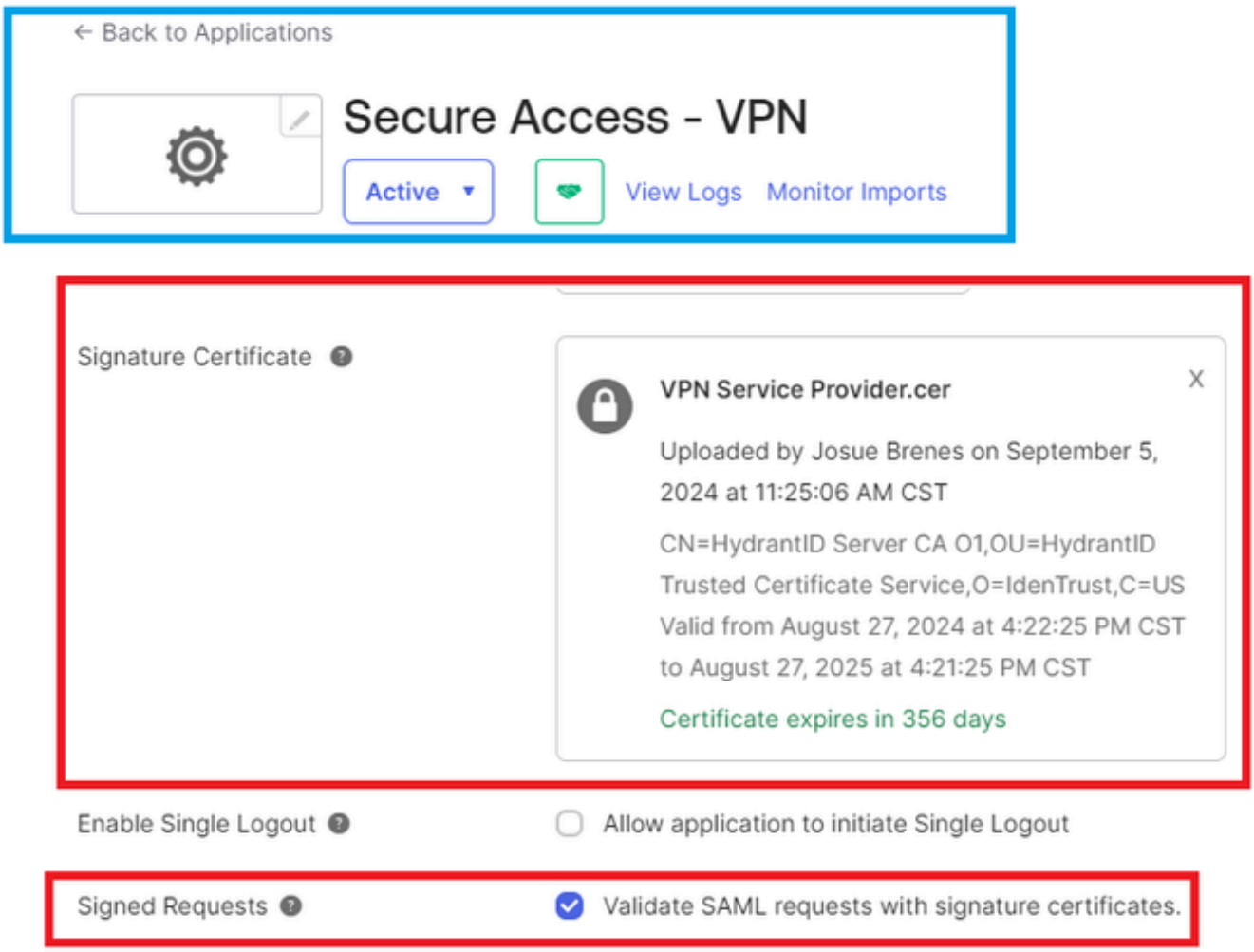


OKTA

OKTA n'effectue pas de validation de certificat par défaut. Il n'y a pas d'option sous Général > Paramètres SAML, qui indique "Certificat de signature".



Si dans l'OKTA IdP il y a une valeur sous General > SAML Settings, qui dit "Signature Certificate Assertion encryption", cela signifie qu'OKTA effectue la Validation de Certificat. Cliquez sur "Edit SAML Settings", cliquez sur Signature Certificate et téléchargez le nouveau certificat SAML VPN d'accès sécurisé.



Informations connexes

- [Centre d'aide Secure Access (Guide de l'utilisateur)]
- [Assistance et documentation techniques - Cisco Systems]
- [Page Communauté d'accès sécurisé]
- [Nouveau certificat d'authentification SAML d'accès sécurisé pour VPN]

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.