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

## Sommario

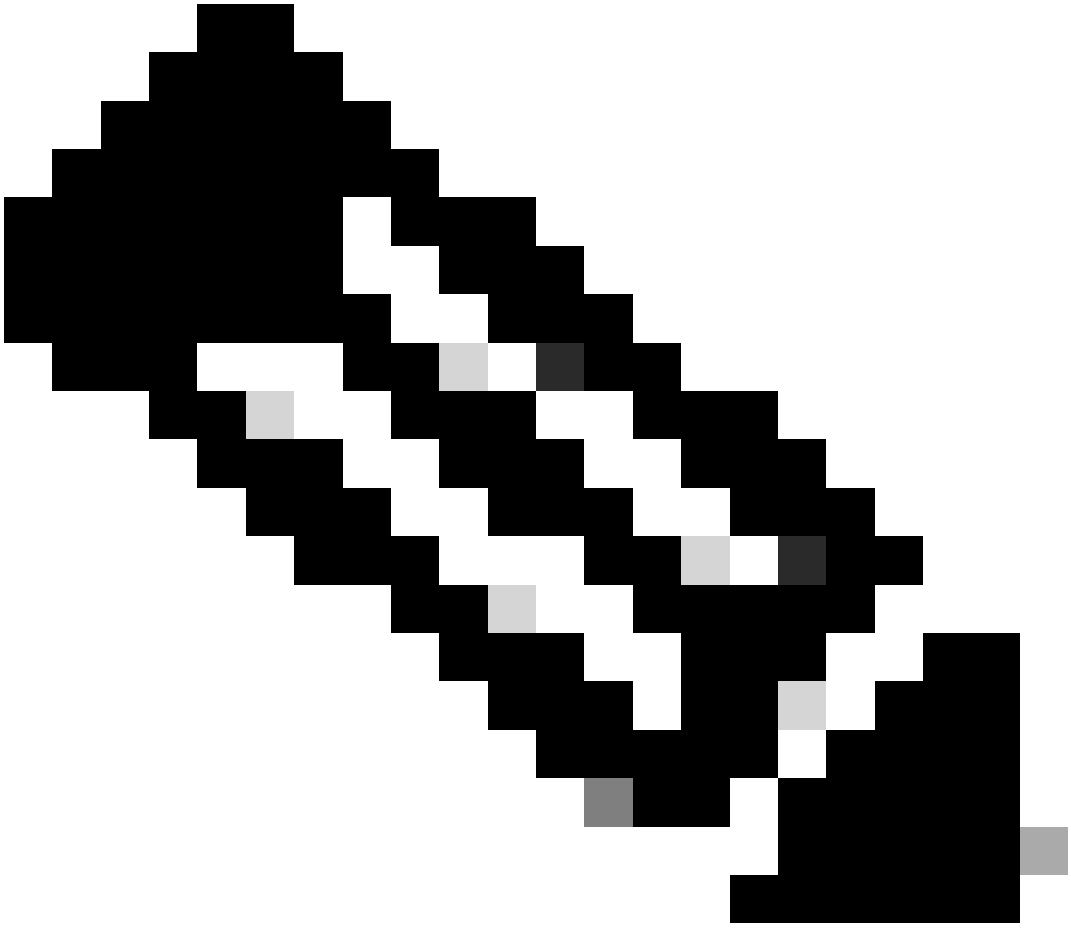


## Introduzione

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.

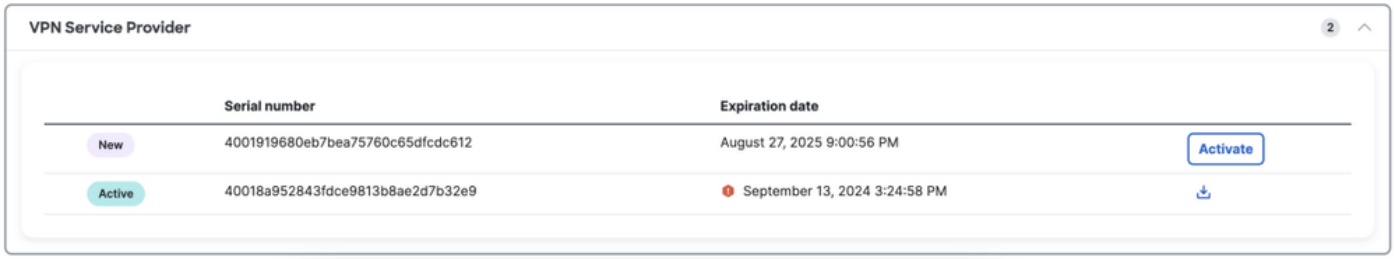
# Cisco Secure Access Dashboard

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.

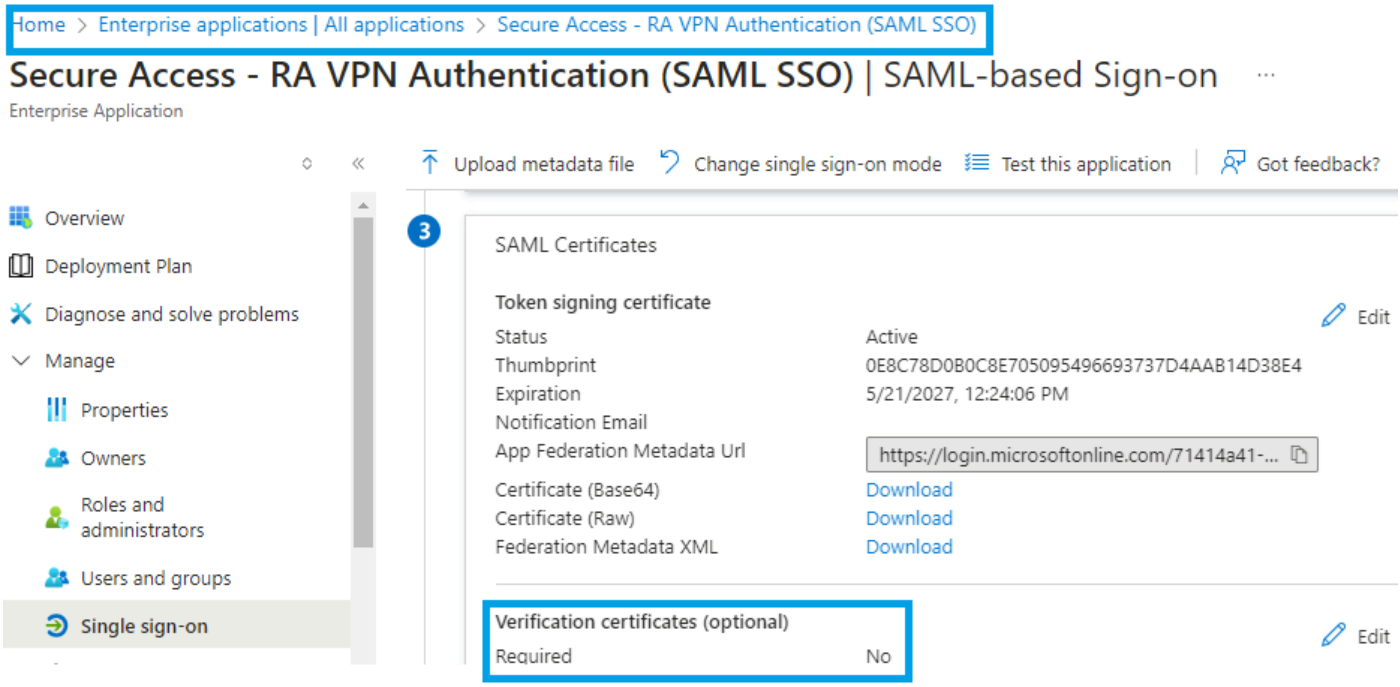
Nel Dashboard di accesso protetto l'unica azione richiesta è passare a Protezione > Certificati > Autenticazione SAML > Certificati provider di servizi, sul "Nuovo" certificato fare clic su "Attiva".

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.

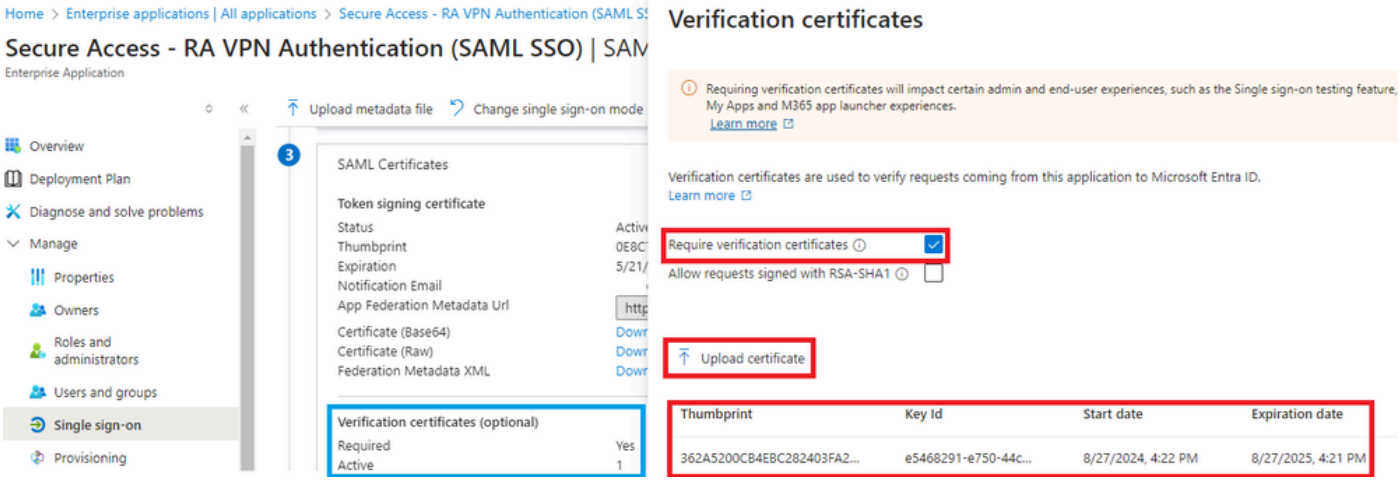



# ID Entra Microsoft (Microsoft Azure)

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

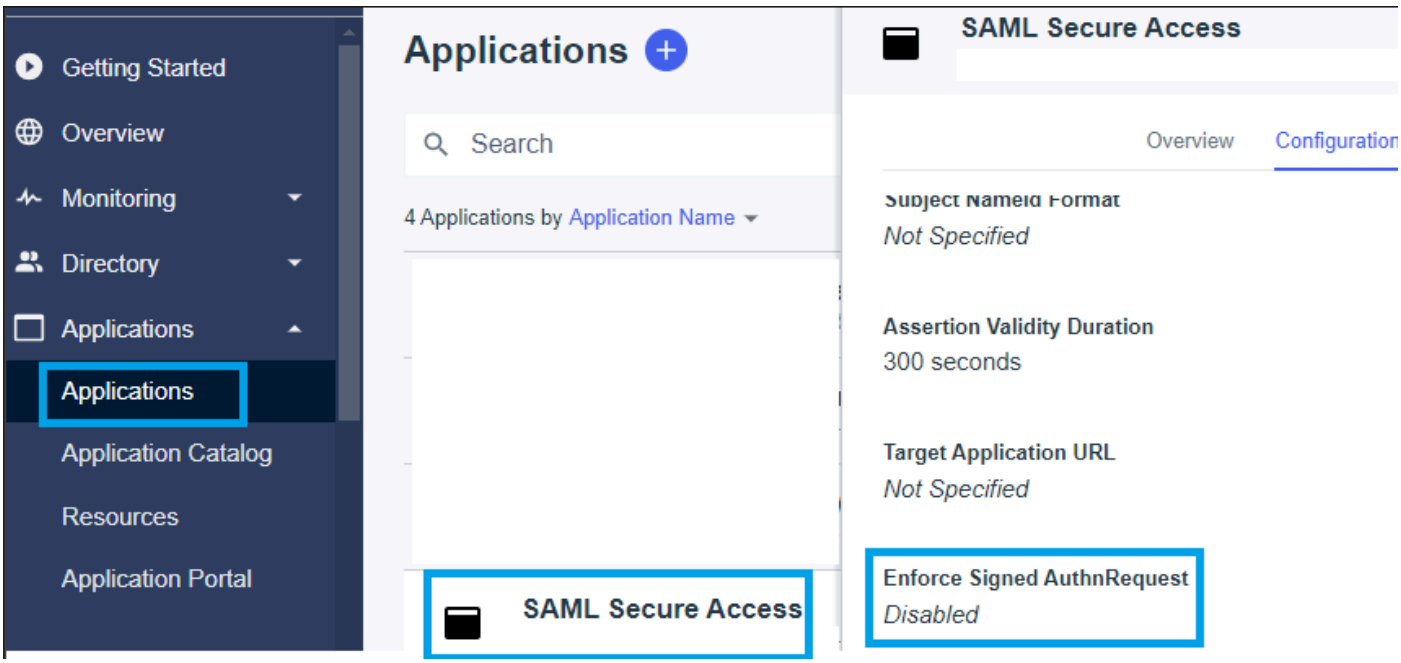



Se l'ID Entra IdP il valore "Verification Certificate (optional)" è impostato su "Required = yes", fare clic su Edit e "Upload certificate" per caricare il nuovo certificato VPN SAML di accesso sicuro.

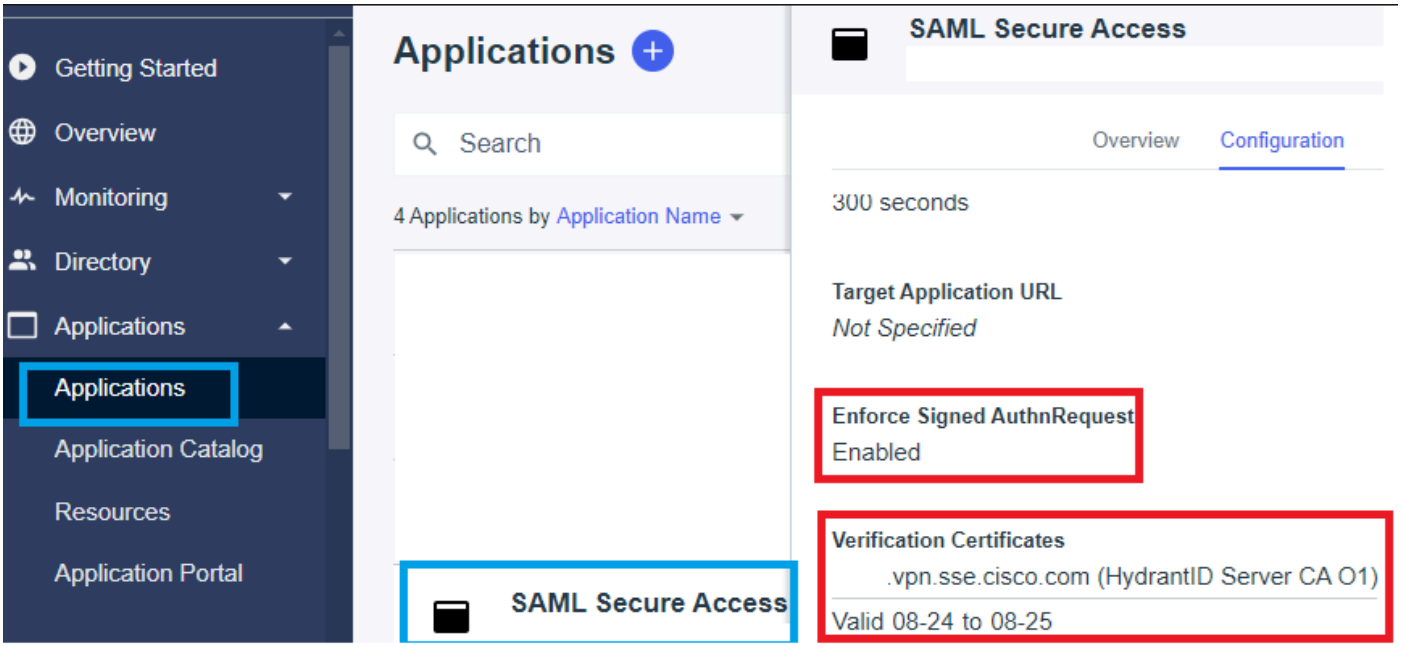



# IdentitàPing

PingIdentity non esegue la convalida del certificato per impostazione predefinita.




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.

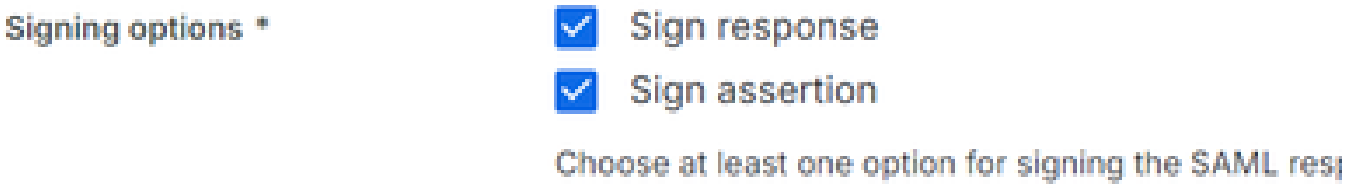



# Cisco DUO

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.

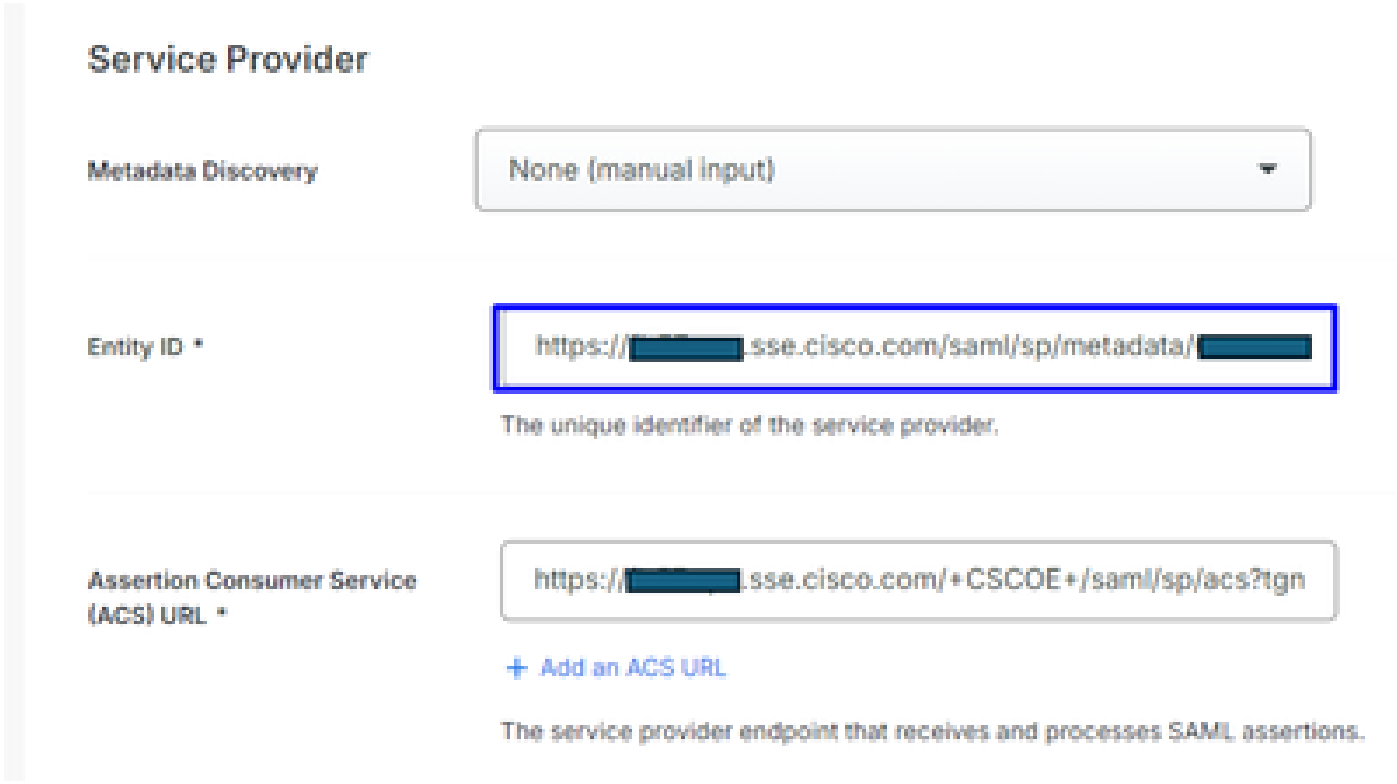
per la firma della richiesta, il DUO può scaricare il nuovo certificato utilizzando il collegamento ID entità metadati fornito dall'amministratore.

## Risposta firma e azione asserzione



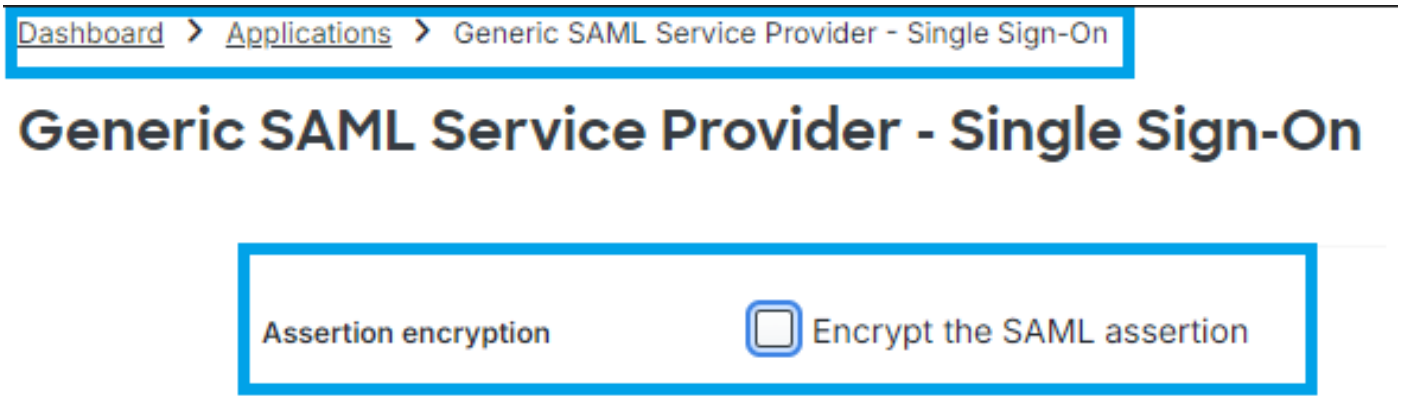

## Impostazioni ID entità

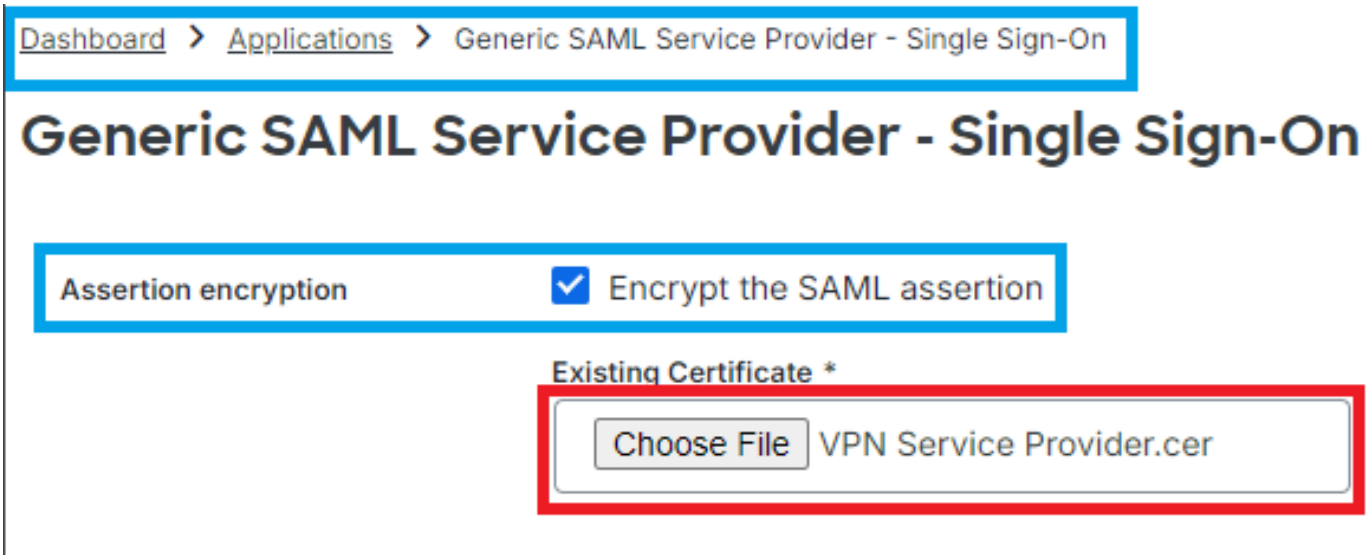
In questo passaggio non è richiesta alcuna azione. Il DUO può estrarre il nuovo certificato dal collegamento dell'ID entità: https://<entry-id>.vpn.sse.cisco.com/saml/sp/metadata/<nome_profilo>.




## Assertion Encryption

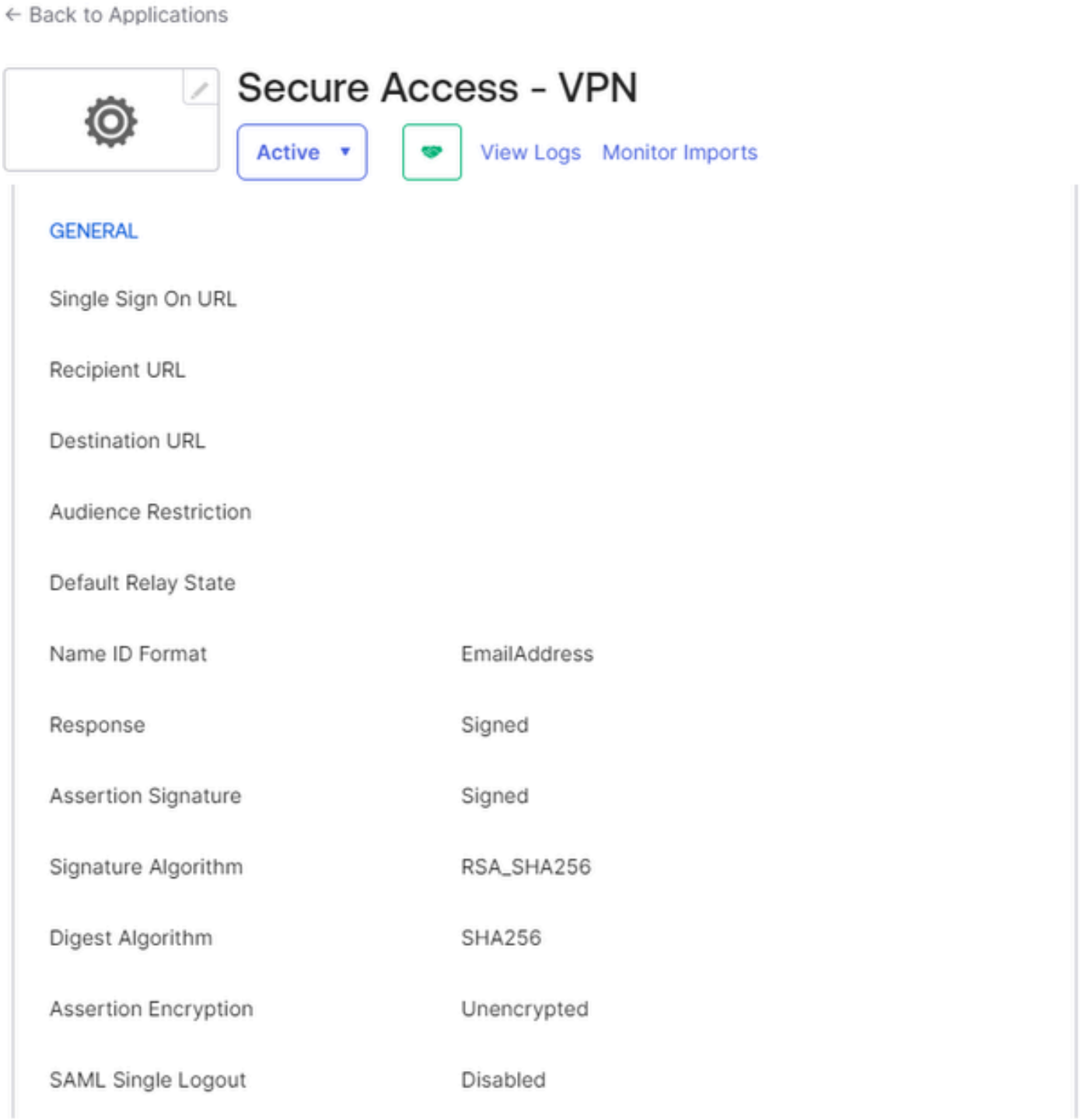
Se nell'IdP Cisco DUO il valore "Assertion encryption" ha il contrassegno "Encrypt the SAML Assertion", fare clic su "choose File" (Scegli file) e caricare il nuovo certificato VPN SAML di accesso sicuro.



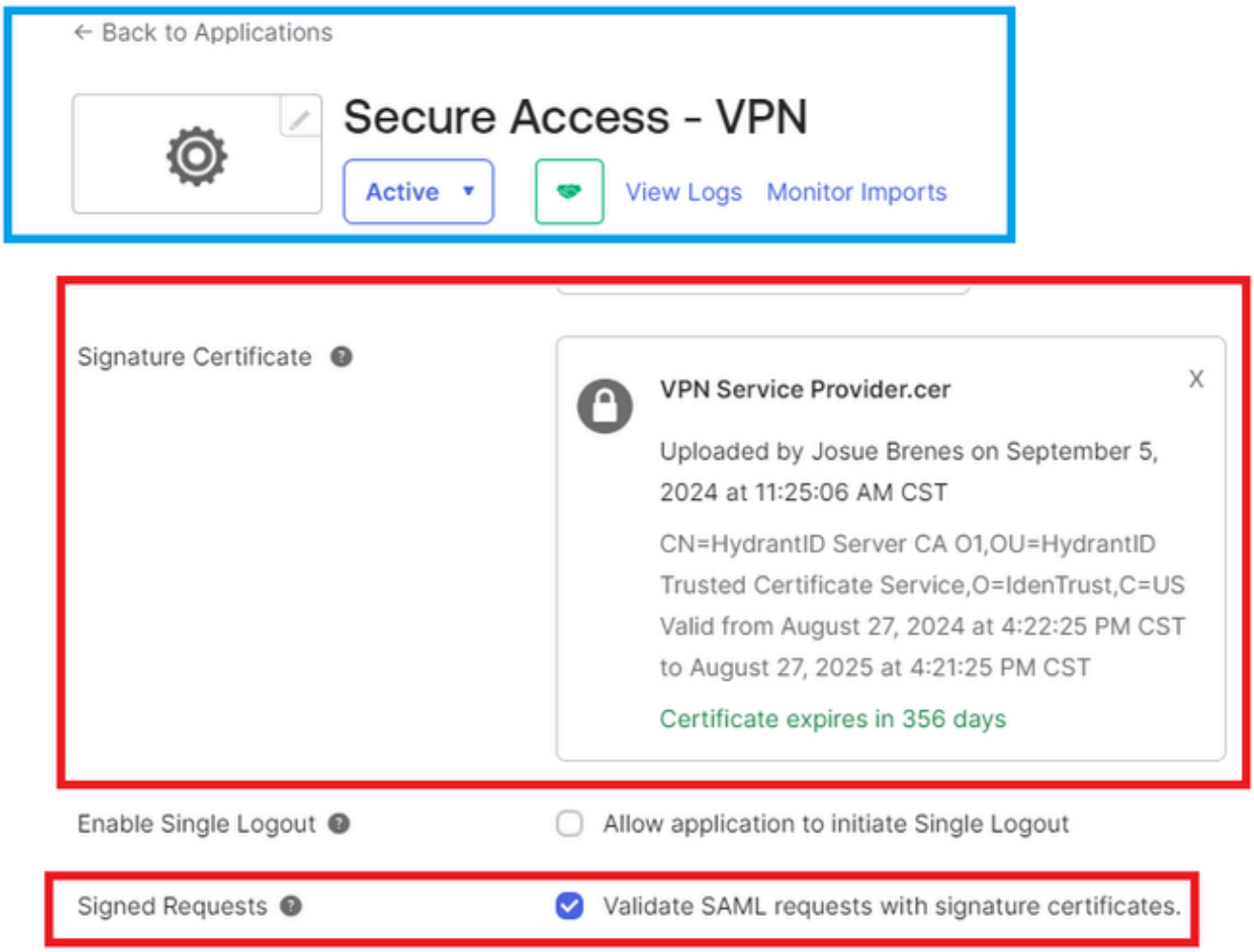



## OKTA

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




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.




## 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).