Atualizar Certificado de Autenticação VPN SAML de Acesso Seguro (Certificado do Provedor de Serviços)

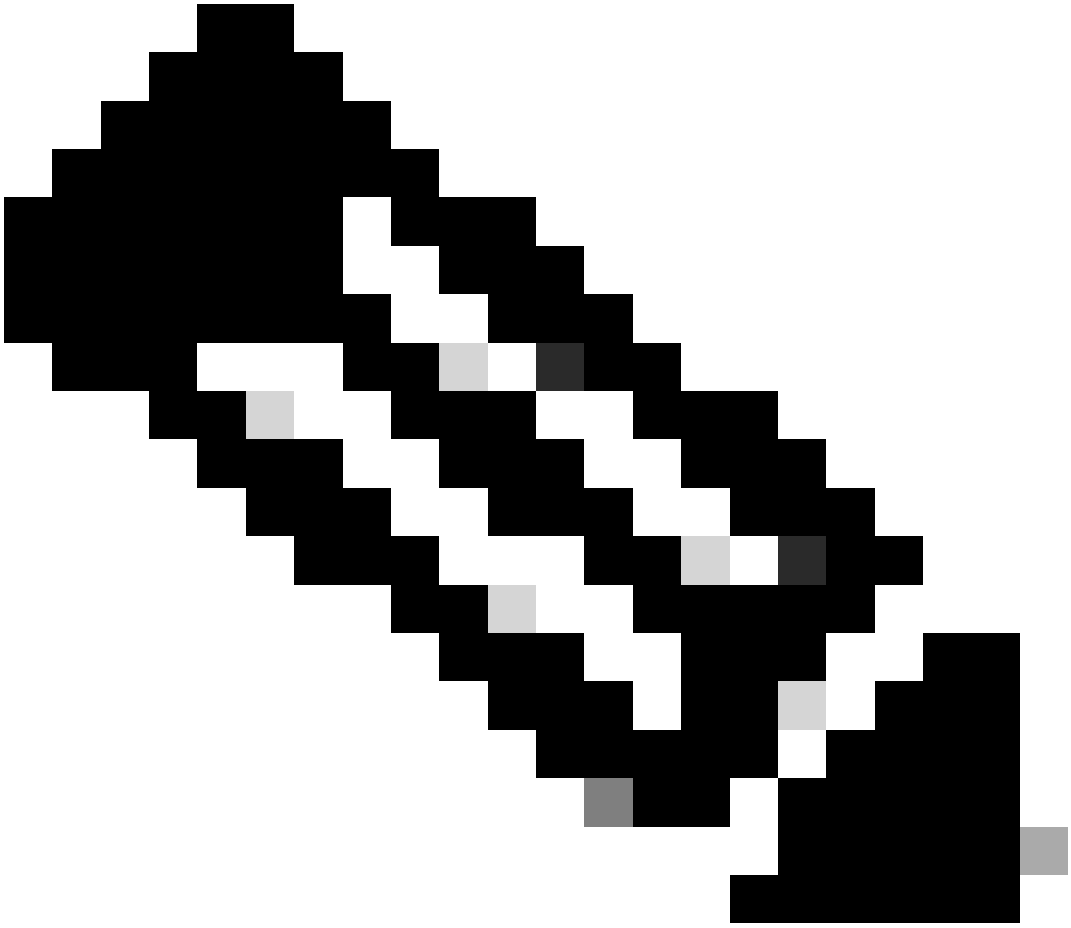
Contents

Introdução

Este documento descreve as etapas necessárias para atualizar o certificado do Provedor de Identidade (IdP) com o novo Certificado do Provedor de Serviços de Acesso Seguro.

Informações de Apoio

O Certificado Cisco Secure Access Security Assertion Markup Language (SAML) usado para a Autenticação de Rede Virtual Privada (VPN) expirará em breve e poderá ser atualizado em seu IdP atual usado para autenticar Usuários VPN caso eles validem esse certificado.
Mais informações sobre isso podem ser encontradas na seção Anúncios de acesso seguro.



Observação: a maioria dos IdPs não verifica esse certificado SAML por padrão e ele não é um requisito, o que significa que nenhuma ação adicional é necessária em seu IdP. Caso seu IdP valide o Certificado de Acesso Seguro, continue atualizando o Certificado de Acesso Seguro em sua configuração do IdP.

Este documento aborda as etapas para confirmar se os IdPs configurados executam validação de certificado: Entra ID (Azure AD), PingIdentity, Cisco DUO, OKTA.

Pré-requisitos

Requisitos

- Acesso ao Painel do Cisco Secure Access.
- Acesso ao painel do IdP.

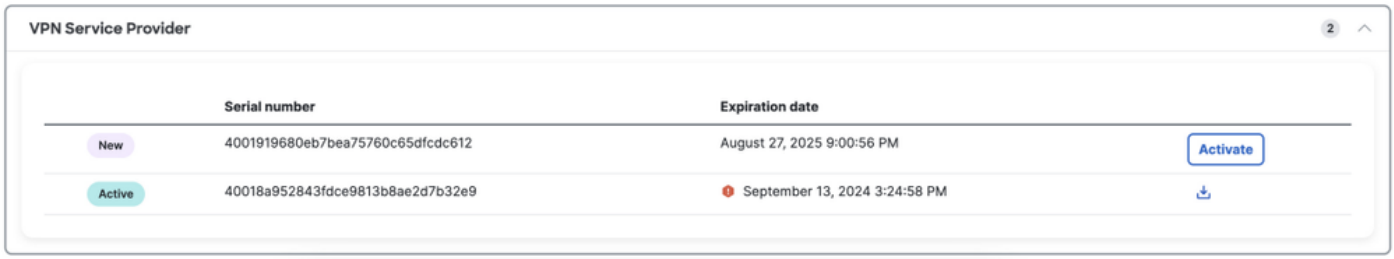
Painel do Cisco Secure Access

Observação: certifique-se de que após executar a próxima etapa, que é ativar o novo certificado de acesso seguro, se o seu IdP estiver fazendo a validação do certificado, atualize o seu IdP com o novo certificado; caso contrário, a autenticação VPN para usuários de acesso remoto pode falhar.

Se você confirmar que o seu IdP está fazendo essa Validação de certificado, recomendamos que você ative o novo certificado no Secure Access e carregue-o no seu IdP durante horários não úteis.

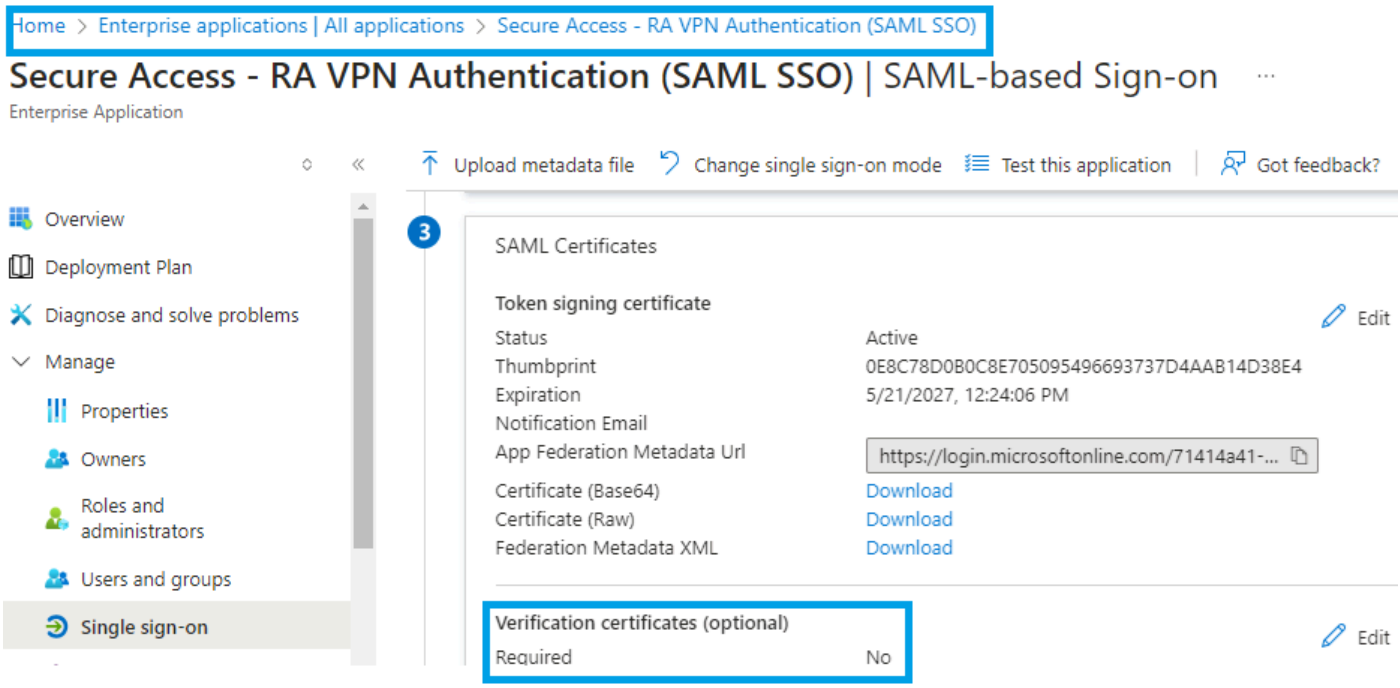
No Painel de Controle de Acesso Seguro, a única ação necessária é ir para Seguro > Certificados > Autenticação SAML > Certificados de Provedor de Serviços, no certificado "Novo", clique em "Ativar".

Depois de clicar em Ativar, você poderá baixar o novo certificado do Secure Access para importar em seu IdP se ele estiver fazendo a Validação de certificado.

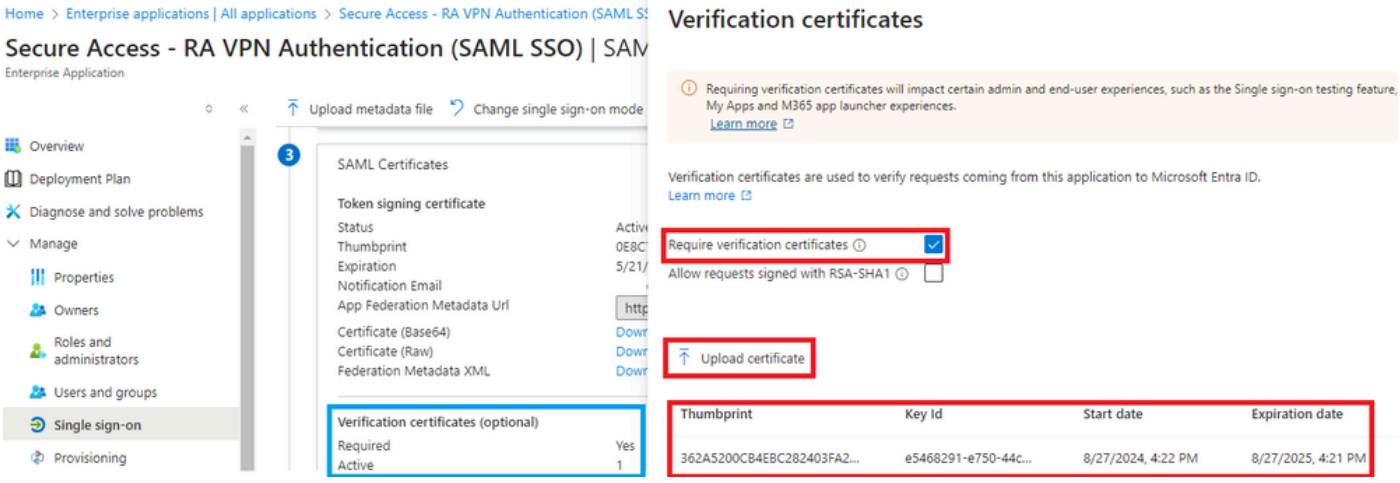


ID do Microsoft Entra (Microsoft Azure)

A ID de Entrada (Azure AD) não está fazendo a Validação de Certificado por padrão.

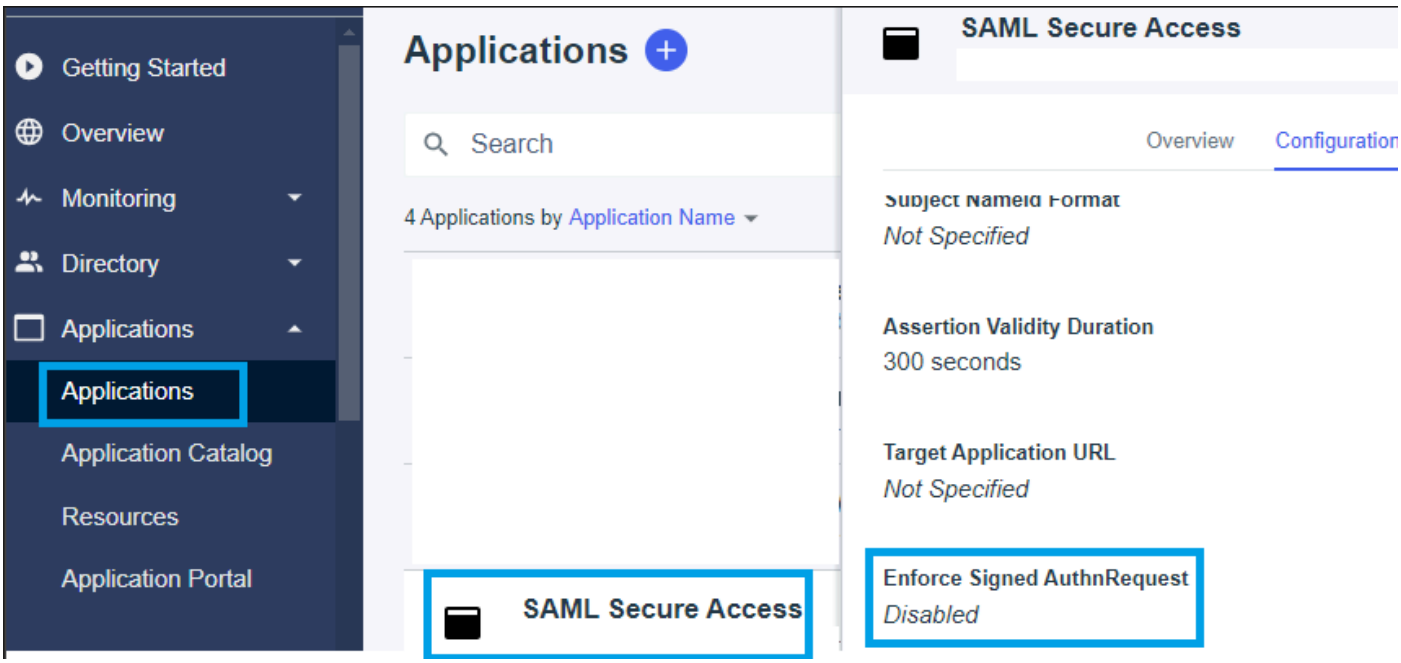


Se a ID do IdP Entra o valor "Verification Certificate (optional) estiver definido como "Required = yes" (Obrigatório = sim), clique em Edit (Editar) e em "Upload certificate" (Carregar certificado) para carregar o novo certificado SAML VPN de acesso seguro.

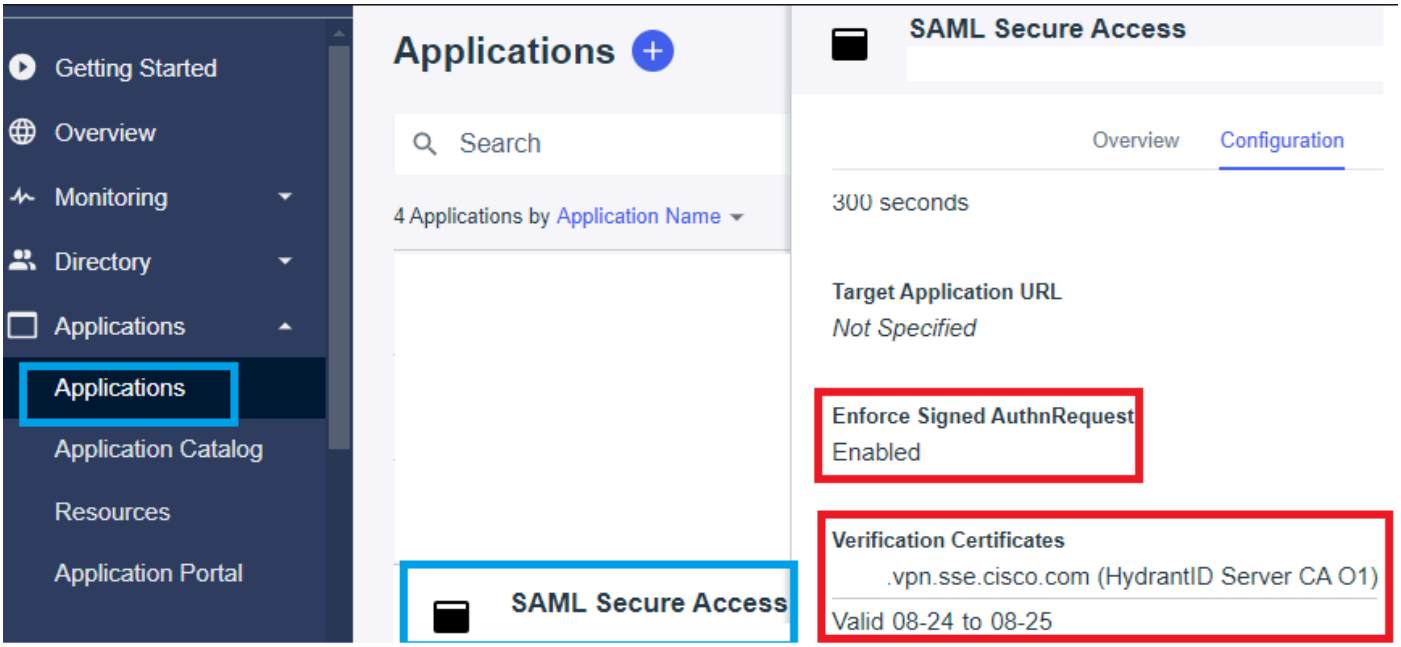


IdentidadePing

O PingIdentity não está fazendo a validação de certificado por padrão.



Se na Identidade de ping do IdP o valor Enforce Signed AuthnRequest estiver definido como "Enabled ", clique em Edit e carregue o novo certificado SAML VPN de acesso seguro.



Cisco DUO

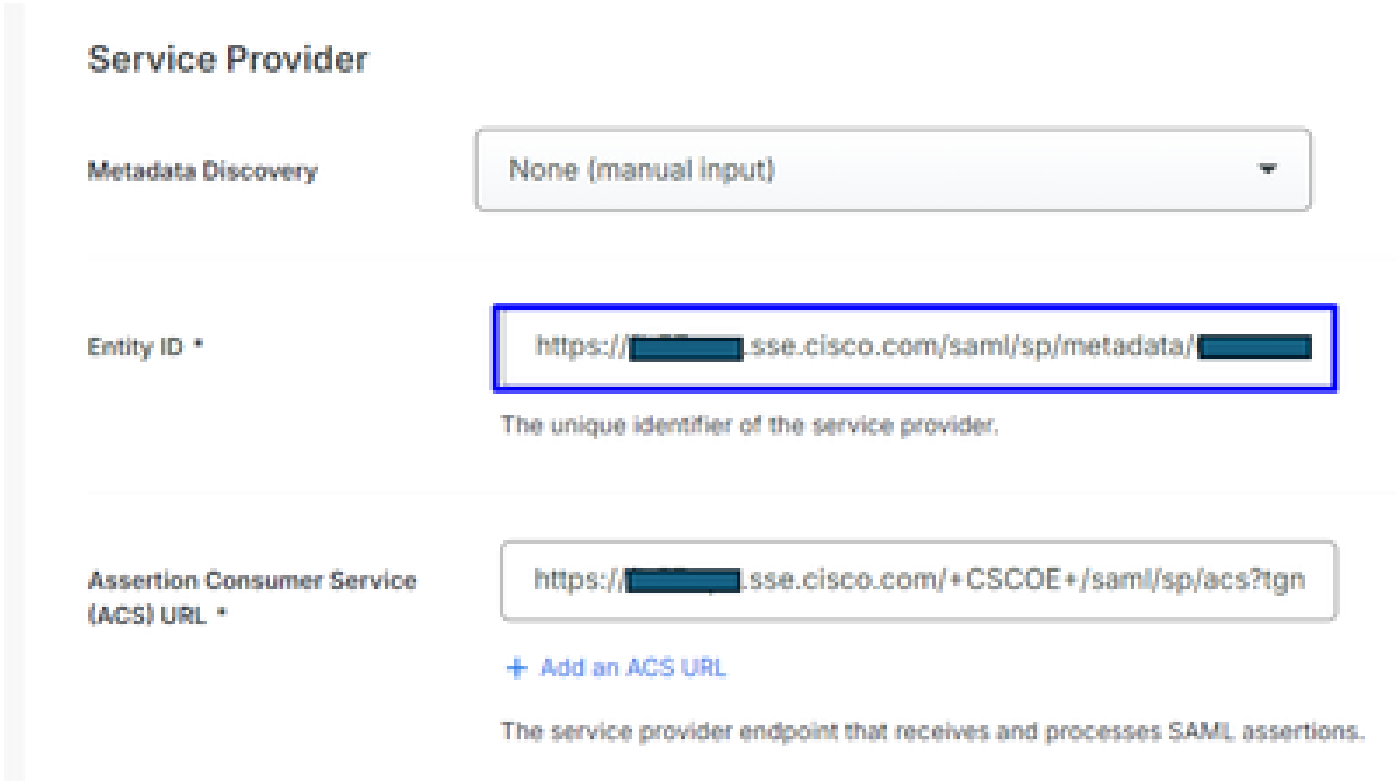
O Cisco DUO está fazendo a validação da solicitação de assinatura por padrão, no entanto, não requer uma ação no próprio DUO, a menos que a Criptografia de Asserção esteja habilitada.

para assinar a solicitação, o DUO pode baixar o novo certificado usando o link de ID de entidade de metadados fornecido pelo administrador.

Resposta de Assinatura e Ação de Asserção

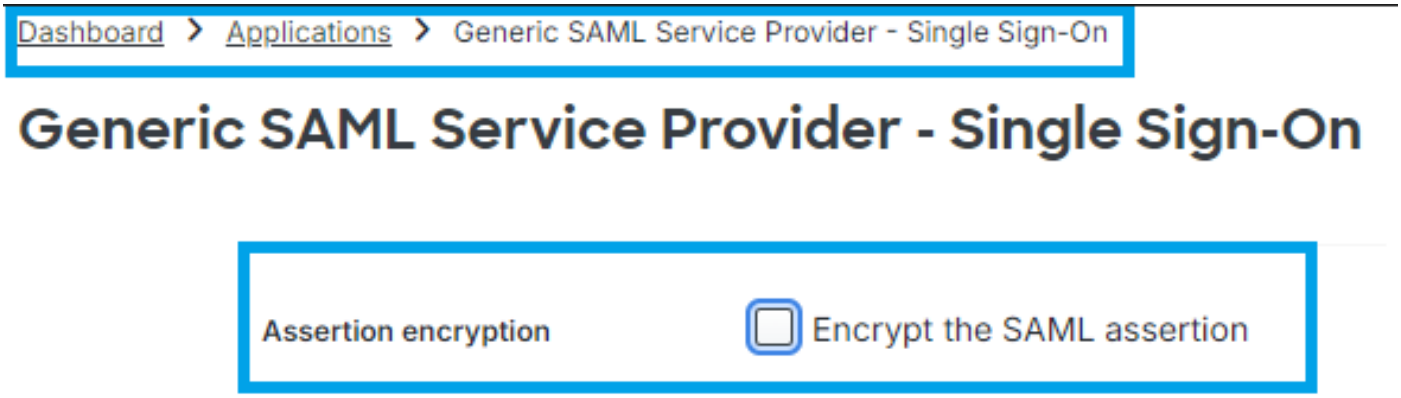
Configurações de ID da entidade

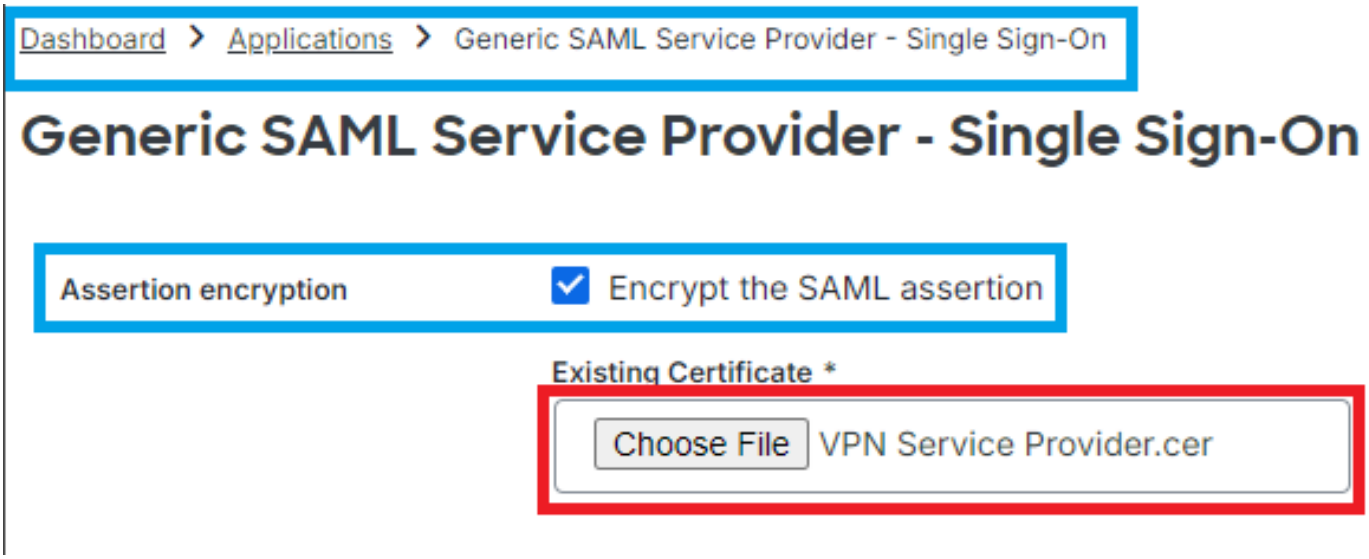
Nenhuma Ação é necessária nesta etapa, o DUO pode extrair o novo certificado do Link de ID da Entidade: https://<entry-id>.vpn.sse.cisco.com/saml/sp/metadata/<profile_name>.



Criptografia de Asserção

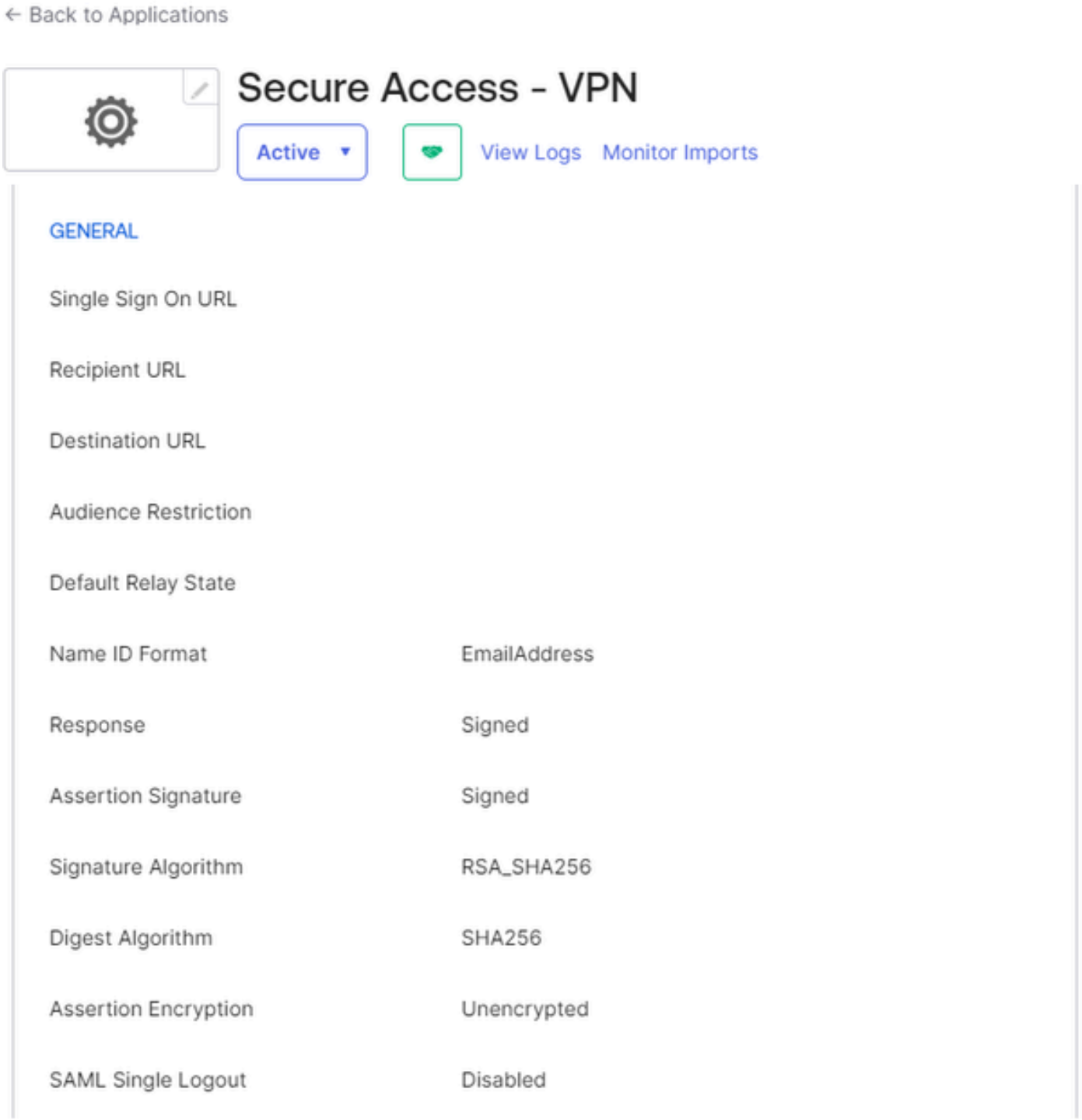
Se no IdP Cisco DUO o valor "Assertion encryption" tiver "Encrypt the SAML Assertion" marcado, clique em "choose File" e carregue o novo Secure Access SAML VPN Certificate.



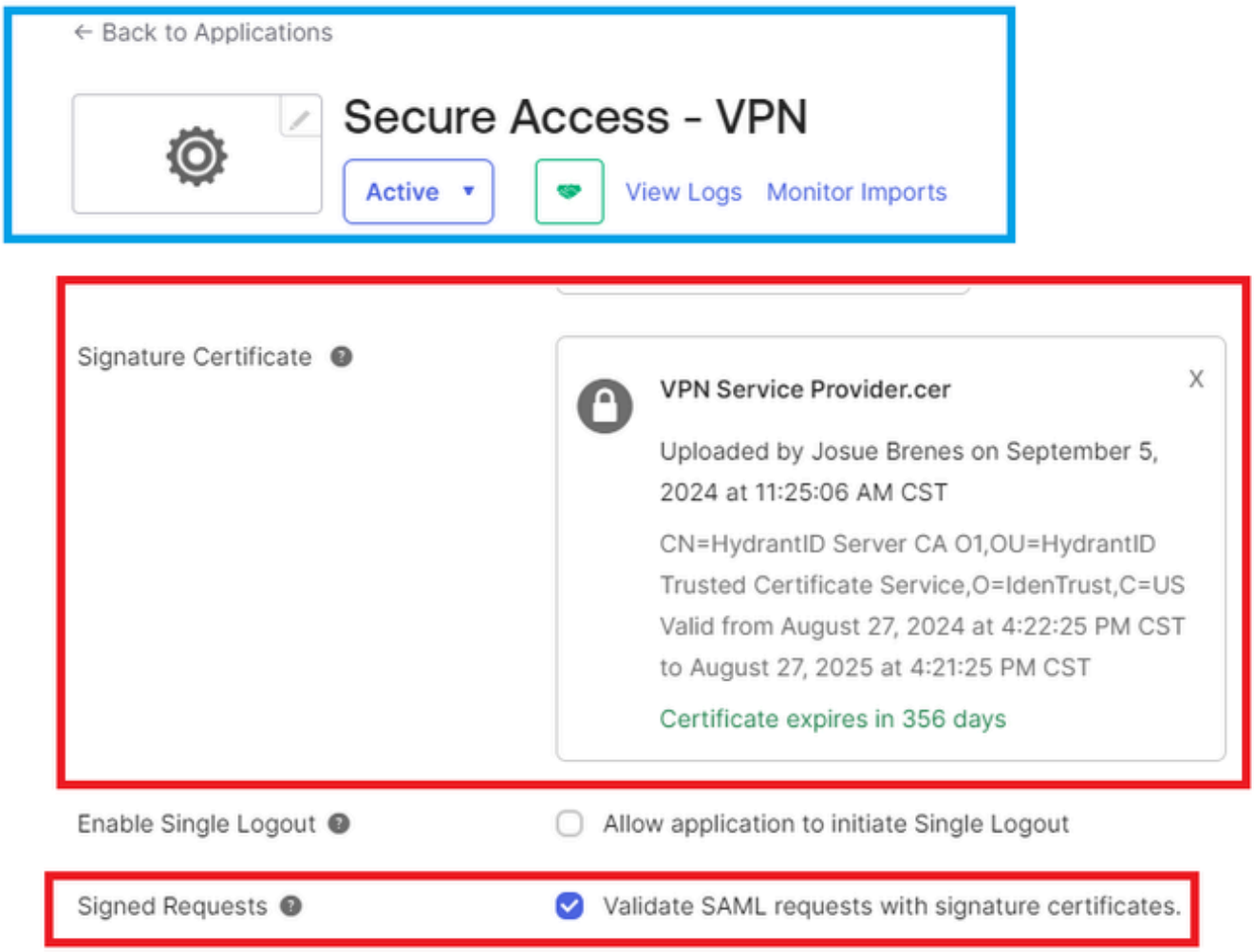


OKTA

O OKTA não está fazendo a validação de certificado por padrão. Não há uma opção em General > SAML Settings que diga "Signature Certificate".



Se no IdP OKTA houver um valor em General > SAML Settings, que diz "Signature Certificate Assertion encryption" significa que o OKTA está fazendo a validação do certificado. Clique em "Edit SAML Settings" (Editar configurações SAML), clique em Signature Certificate (Certificado de Assinatura) e carregue o novo Secure Access SAML VPN Certificate (Certificado VPN SAML de Acesso Seguro).



Informações Relacionadas

- Secure Access Help Center (Guia do usuário)
- Suporte Técnico e Documentação - Cisco Systems
- Página da comunidade de acesso seguro
- Novo Certificado de Autenticação SAML de Acesso Seguro para VPN

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.