更新安全访问SAML VPN身份验证证书（服务提供商证书）

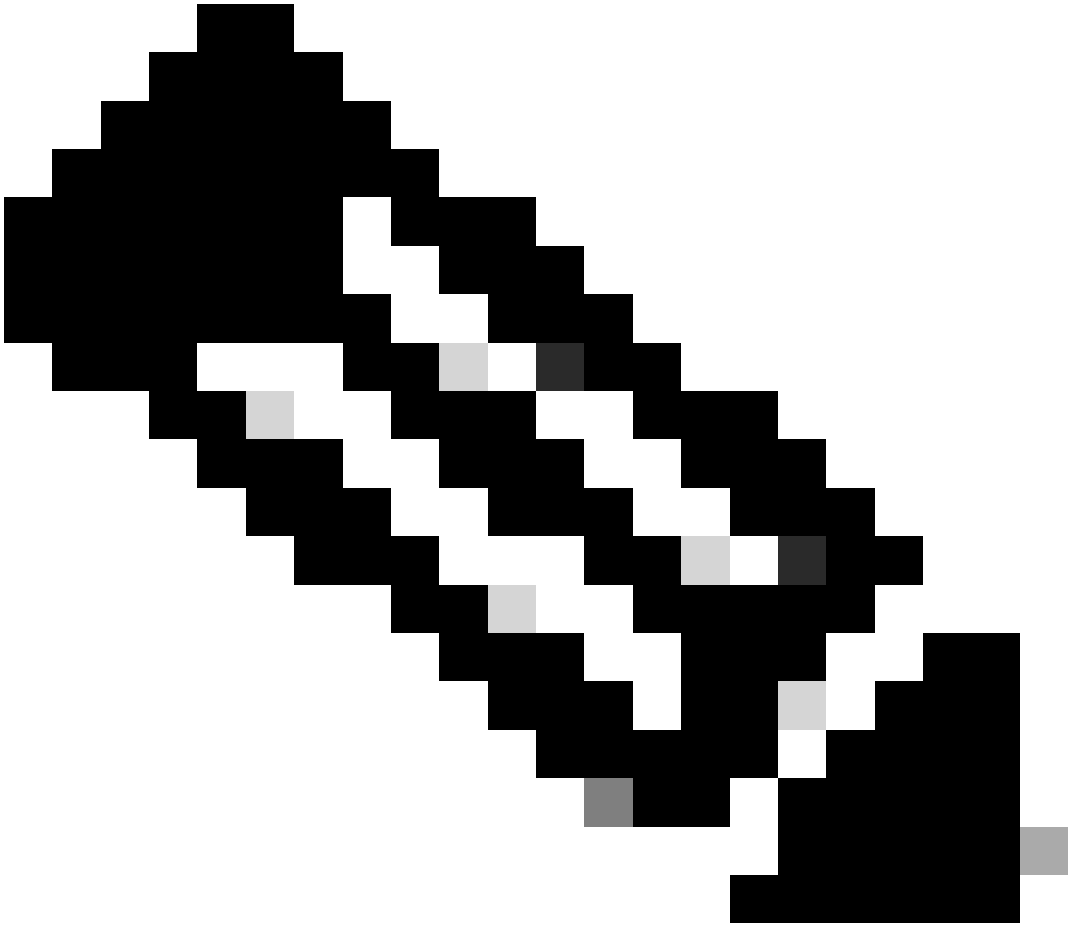
目录

简介

本文档介绍使用新的安全访问服务提供商证书更新身份提供程序(IdP)证书所需的步骤。

背景信息

用于虚拟专用网络(VPN)身份验证的思科安全访问安全断言标记语言(SAML)证书即将过期，并且可以在验证VPN用户时用用于对其进行身份验证的当前IdP进行更新。
有关此功能的详细信息可在安全访问通告部分中找到。



注意：默认情况下，大多数IdP不会验证此SAML证书，这不是要求，这意味着您的IdP中不需要进一步操作。如果IdP确实验证安全访问证书，请继续在IdP配置中更新安全访问证书。

本文档介绍用于确认配置的IdP是否执行证书验证的步骤：Entra ID (Azure AD)、PingIdentity、Cisco DUO、OKTA。

先决条件

要求

- 访问您的思科安全访问控制面板。
- 访问您的IdP仪表板。

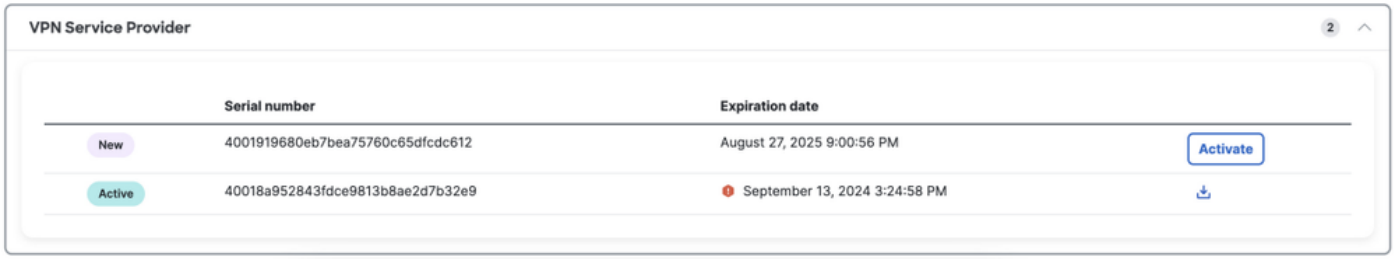
思科安全访问控制面板

注意：请确保在执行激活新安全访问证书的下一个步骤之后，如果您的IdP执行此证书验证，请使用新证书更新您的IdP；否则，远程访问用户的VPN身份验证可能会失败.

如果您确认IdP正在进行此证书验证，我们建议您在Secure Access中激活新证书，并在非工作时间内将其上传到IdP。

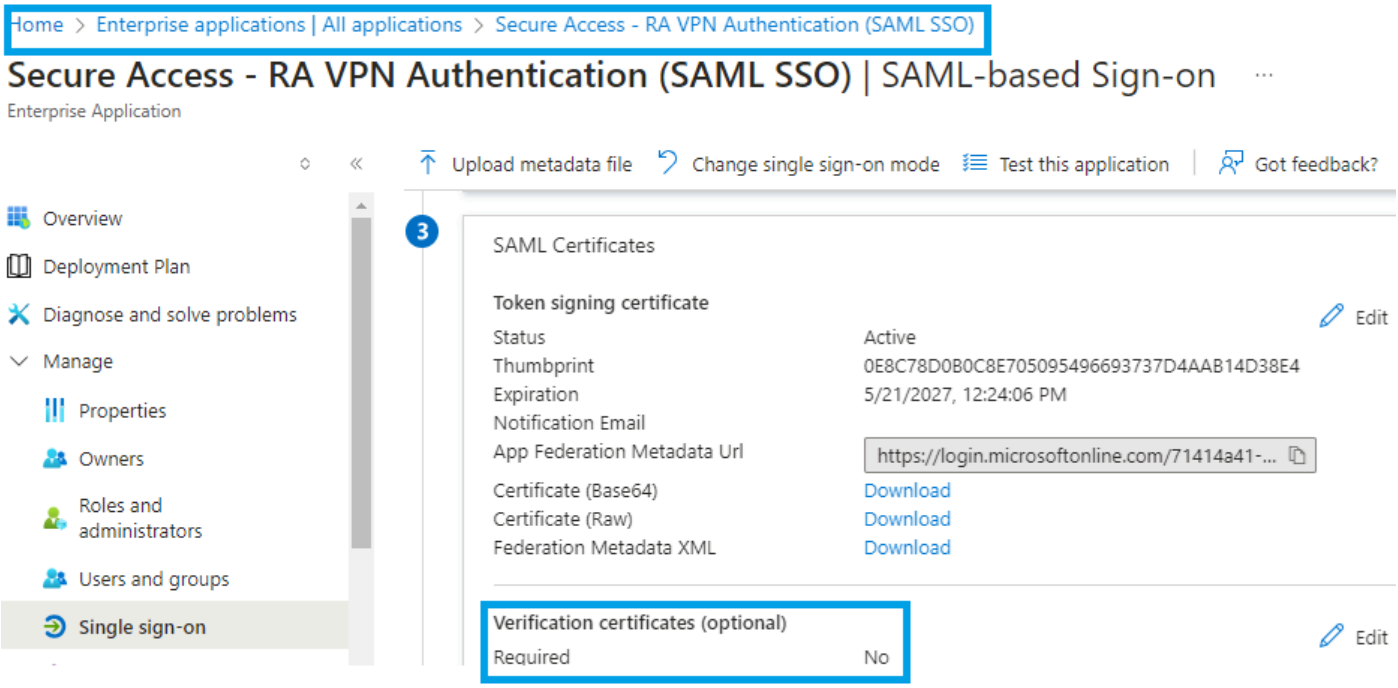
在安全访问控制面板中，只需要转至Secure > Certificates > SAML Authentication > Service Provider certificates，在“New”证书上点击“Activate”。

点击“激活”(Activate)后，您可以下载新的安全访问证书(New Secure Access certificate)，以便在IdP中导入（如果它正在执行证书验证）。

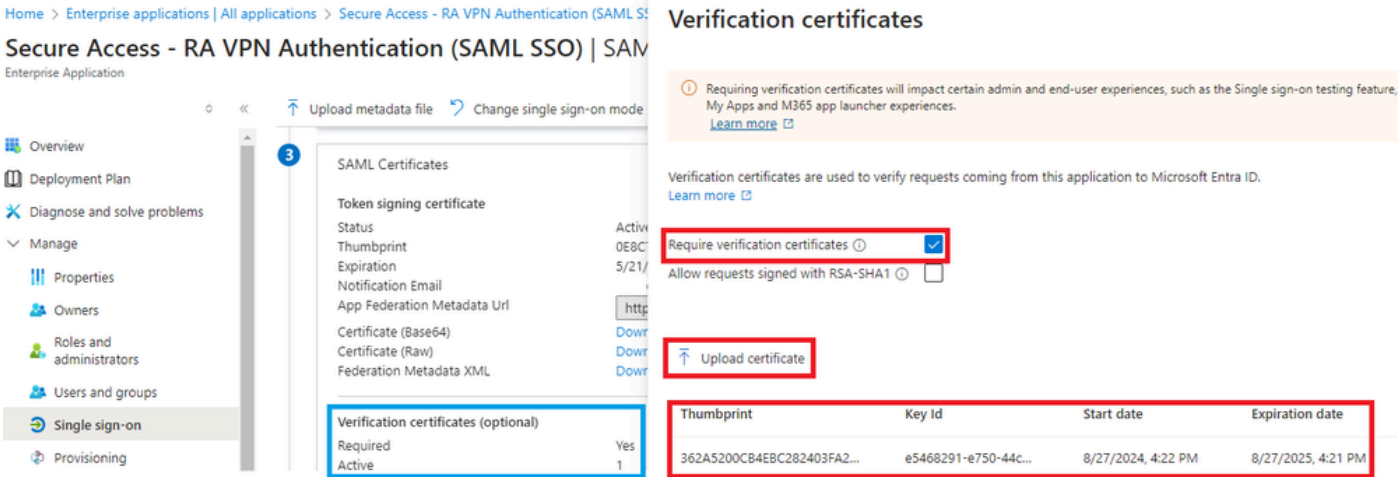


Microsoft Entra ID (Microsoft Azure)

默认情况下，Entra ID (Azure AD)不执行证书验证。

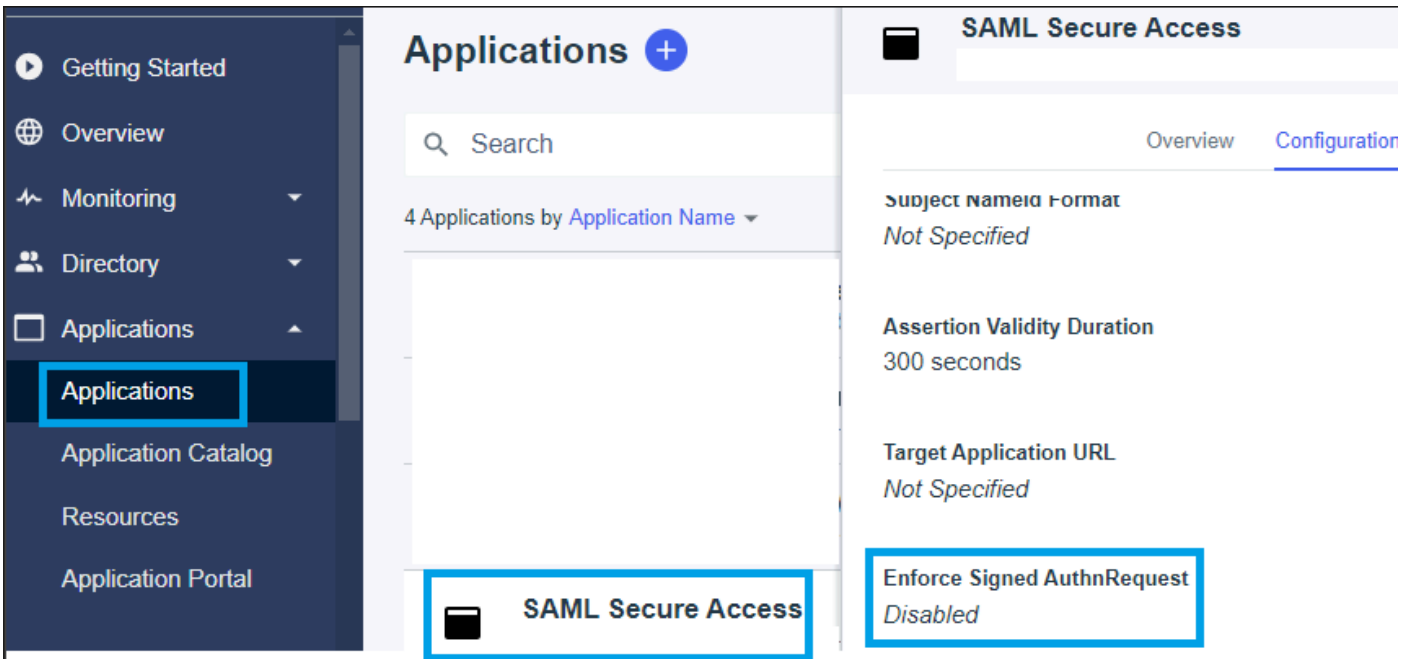


如果IdP Entra ID的值“Verification Certificate (optional)”设置为“Required = yes”，请点击Edit和“Upload certificate”以上传新的安全访问SAML VPN证书。

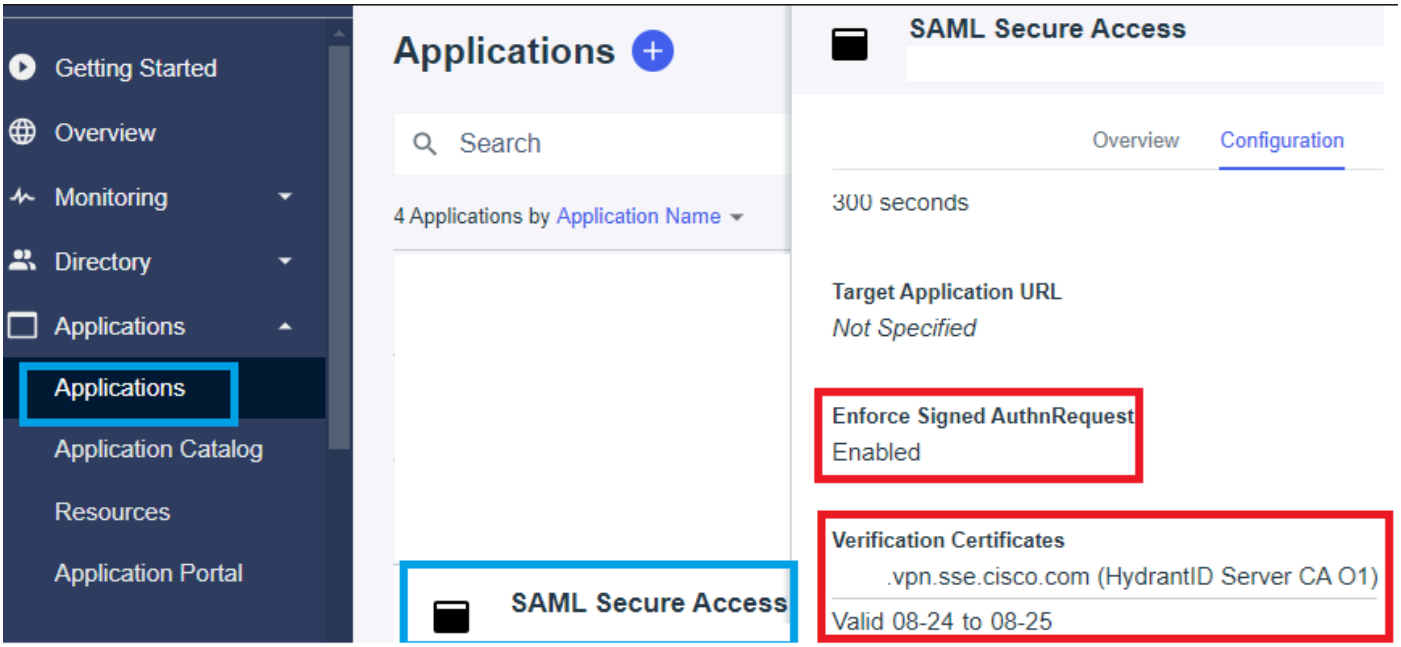


PingIdentity

默认情况下，PingIdentity不执行证书验证。



如果IdP Pingidentity中的值Enforce Signed AuthnRequest设置为“Enabled”，请点击Edit并上传新的安全访问SAML VPN证书。

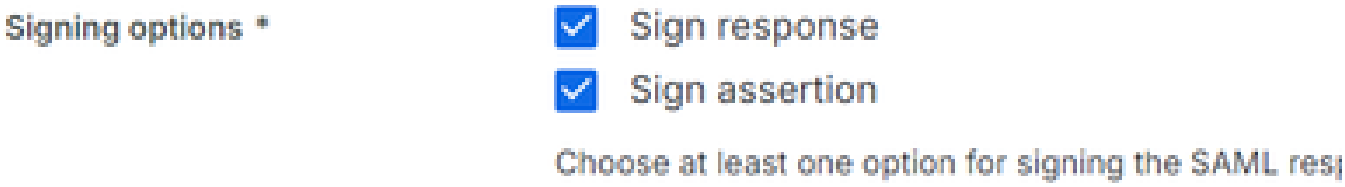


思科DUO

默认情况下，Cisco DUO执行签名请求验证，但是，除非启用断言加密，否则不需要对DUO本身执行操作。

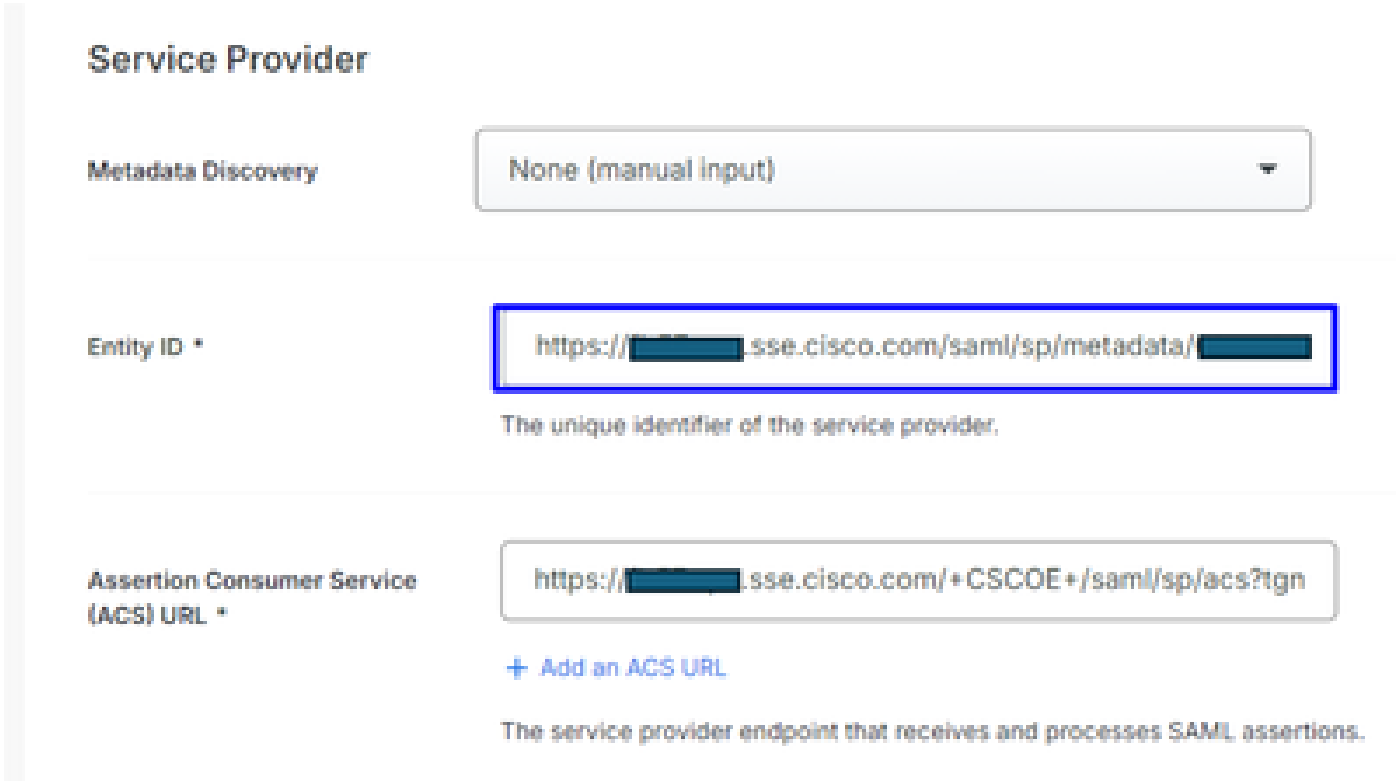
对于签名请求，DUO可以使用管理员提供的元数据实体ID链接下载新证书。

签名响应和断言操作



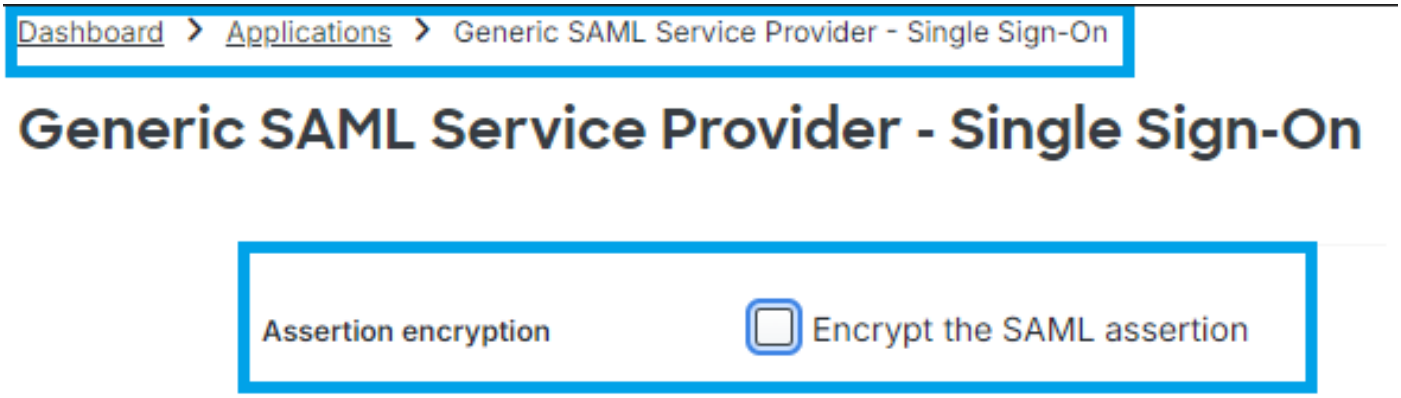
实体ID设置

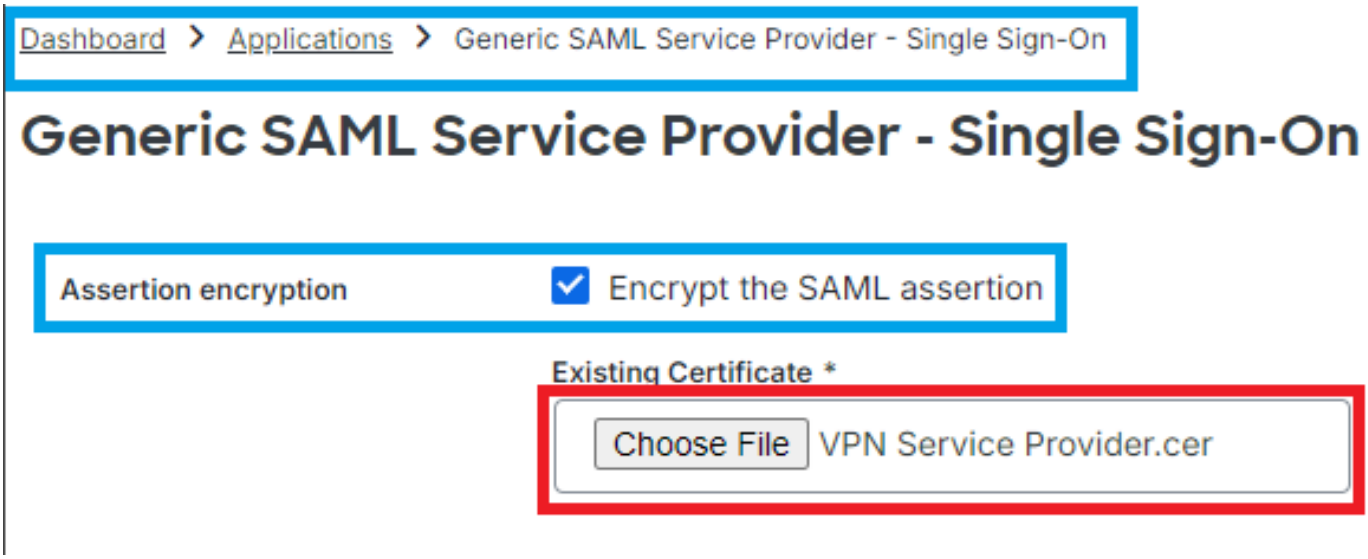
此步骤中不需要执行任何操作，DUO可以从实体ID链路中提取新证书：https://<entry-id>.vpn.sse.cisco.com/saml/sp/metadata/<profile_name>。



断言加密

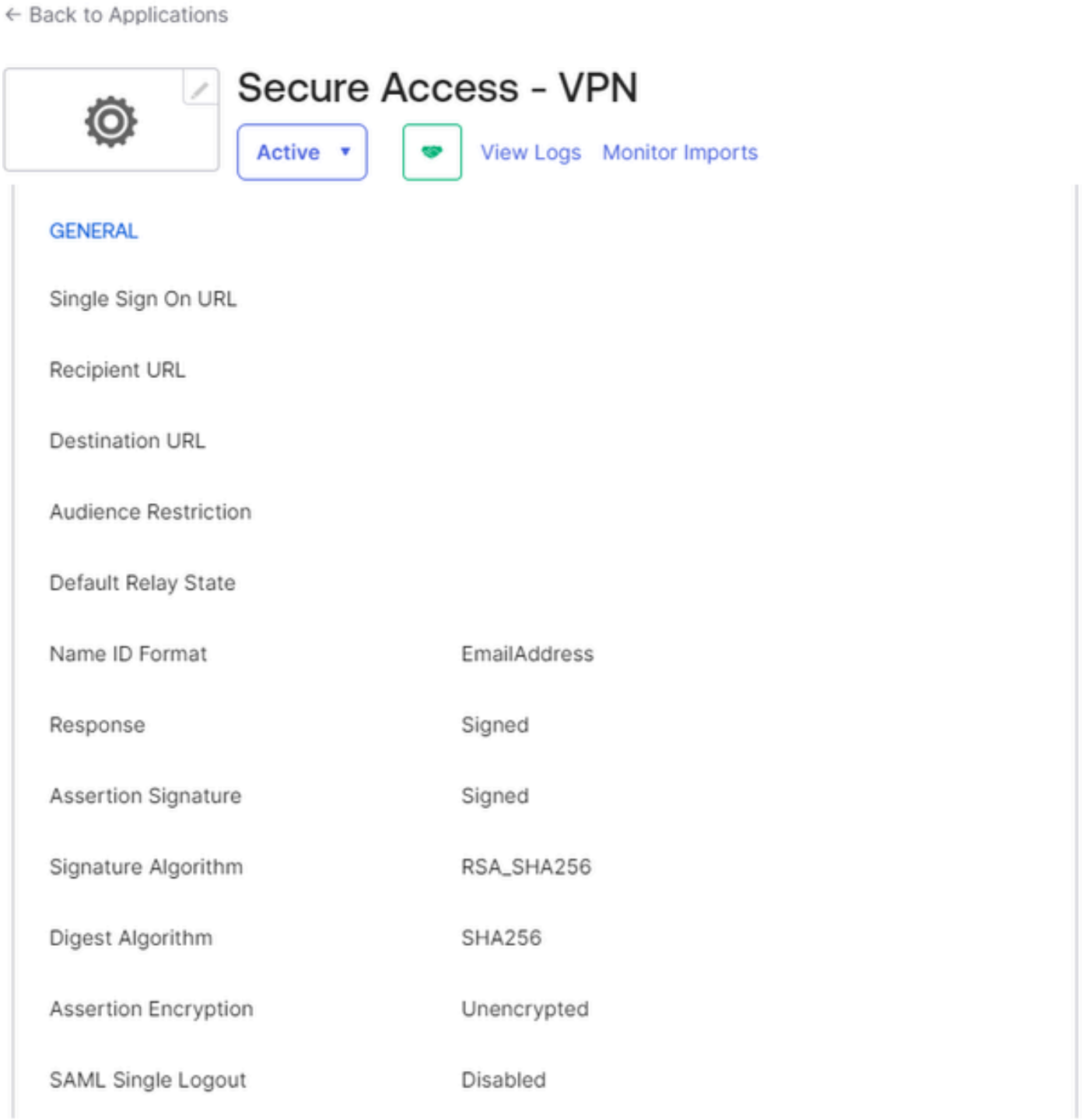
如果在IdP思科DUO中，值“Assertion encryption”标记“Encrypt the SAML Assertion”，请点击“choose File”并上传新的安全访问SAML VPN证书。



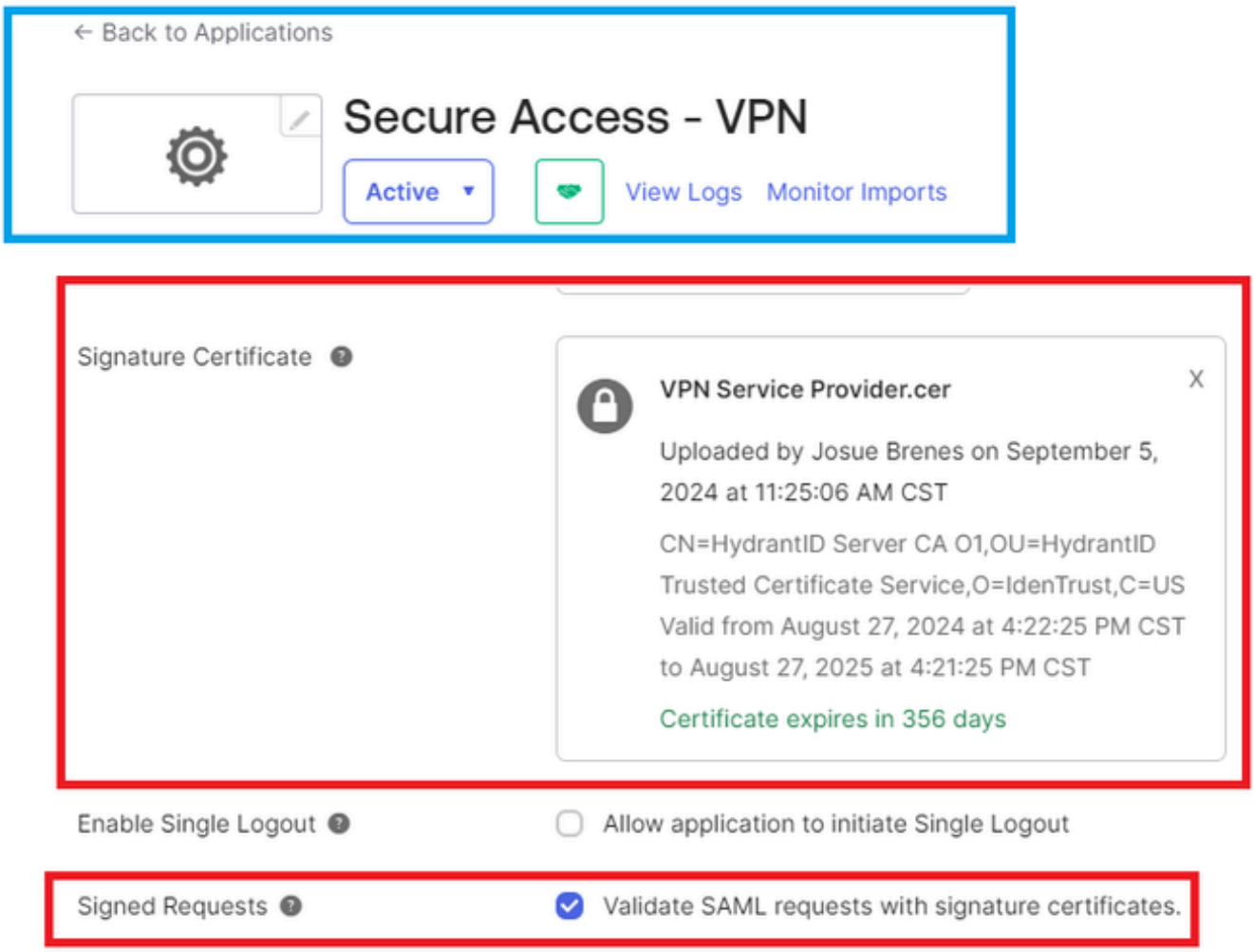


OKTA

默认情况下，OKTA不执行证书验证。General > SAML Settings下没有选项表示“Signature Certificate”。



如果在IdP OKTA中，在General > SAML Settings下有一个值为“Signature Certificate Assertion encryption”的值，则表示OKTA正在执行证书验证。点击“编辑SAML设置”(Edit SAML Settings)，点击签名证书(Signature Certificate)并上传新的安全访问SAML VPN证书。



相关信息

- [安全访问帮助中心（用户指南）]
- [技术支持和文档 - Cisco Systems]
- [“安全访问：社区”页]
- [VPN的新安全访问SAML身份验证证书]

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。