セキュアアクセスSAML VPN認証証明書（サービスプロバイダー証明書）の更新

内容

はじめに

背景説明

前提条件

- 要件

シスコセキュアアクセスダッシュボード

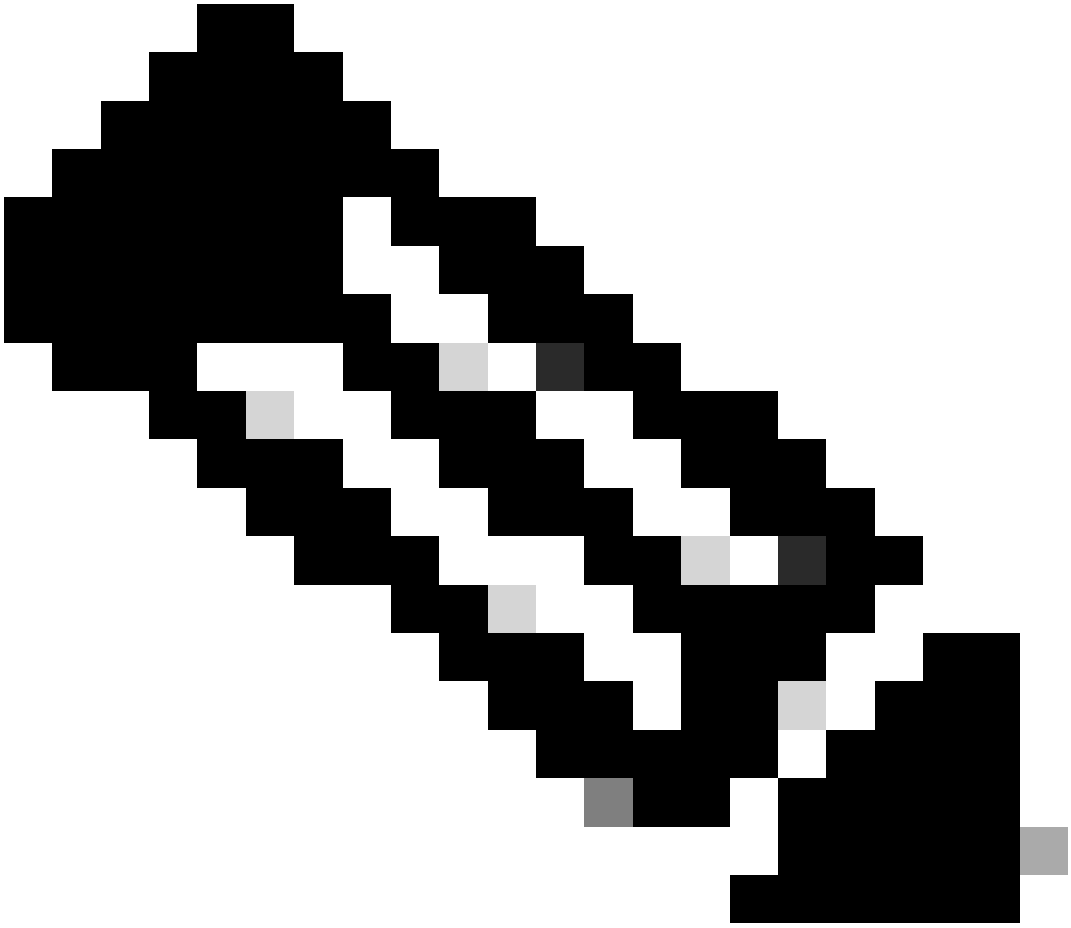
MicrosoftエントリID (Microsoft Azure)

はじめに

このドキュメントでは、アイデンティティプロバイダー(IdP)証明書を新しいセキュアアクセスサービスプロバイダー証明書で更新するために必要な手順について説明します。

背景説明

バーチャルプライベートネットワーク(VPN)の認証に使用されるCisco Secure Access Security Assertion Markup Language(SAML)証明書の有効期限が間もなく切れる予定です。この証明書を検証する場合は、VPNユーザの認証に使用する現在のIdPで更新できます。
これに関する詳細は、「セキュアアクセスに関するアナウンス」セクションを参照してください。



注：ほとんどのIdPはこのSAML証明書をデフォルトで確認しないため、必須ではありません。つまり、IdPでこれ以上のアクションは必要ありません。IdPがセキュアアクセス証明書を検証する場合は、IdP設定のセキュアアクセス証明書の更新に進みます。

このドキュメントでは、設定済みのIdPが証明書の検証を実行するかどうかを確認する手順について説明します(Entra ID(Azure AD)、PingIdentity、Cisco DUO、OKTA)。

前提条件

要件

- シスコセキュアアクセスダッシュボードにアクセスします。
- IdPダッシュボードにアクセスします。

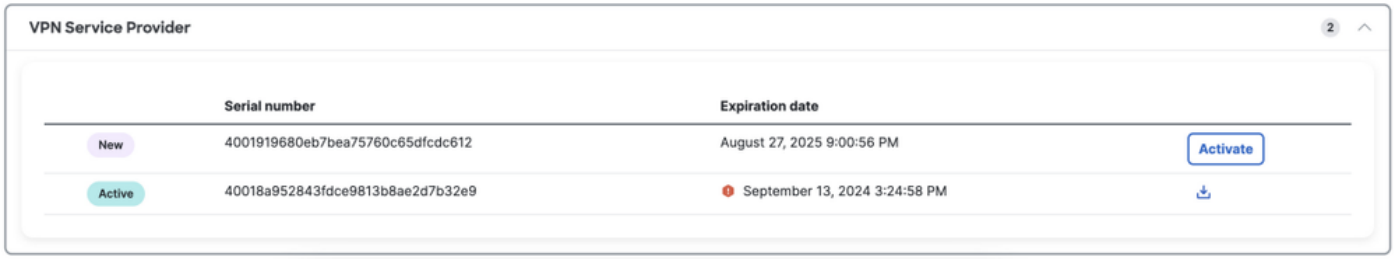
シスコセキュアアクセスダッシュボード

注：次の手順で新しいセキュアアクセス証明書をアクティブにしたことを確認します。IdPでこの証明書の検証を行っている場合は、新しい証明書でIdPを更新してください。そうでない場合、リモートアクセスユーザのVPN認証が失敗する可能性があります.

IdPがこの証明書の検証を行っていることを確認した場合は、セキュアアクセスで新しい証明書をアクティブ化し、営業時間外にIdPにアップロードすることをお勧めします。

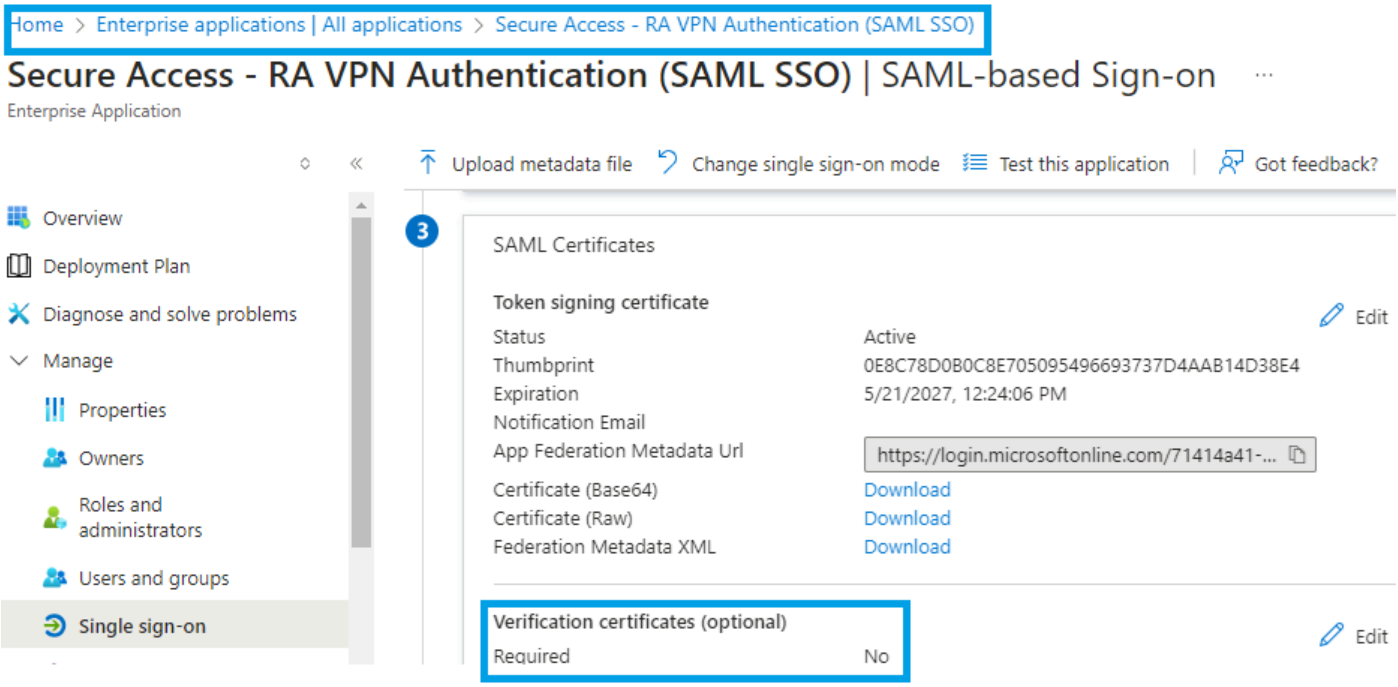
セキュアアクセスダッシュボードで必要なアクションは、Secure > Certificates > SAML Authentication > Service Provider certificatesの順に選択し、New証明書でActivateをクリックすることだけです。

Activateをクリックすると、証明書の検証を行っている場合は、新しいセキュアアクセス証明書をダウンロードしてIdPにインポートできます。

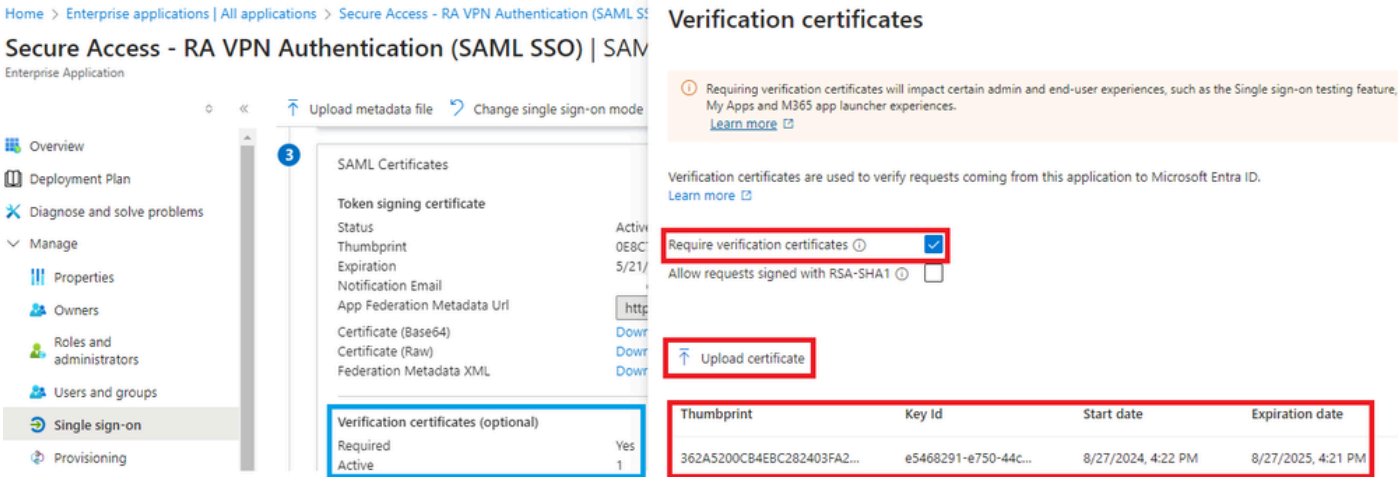


MicrosoftエントリID (Microsoft Azure)

入力ID (Azure AD)は既定で証明書の検証を行いません。

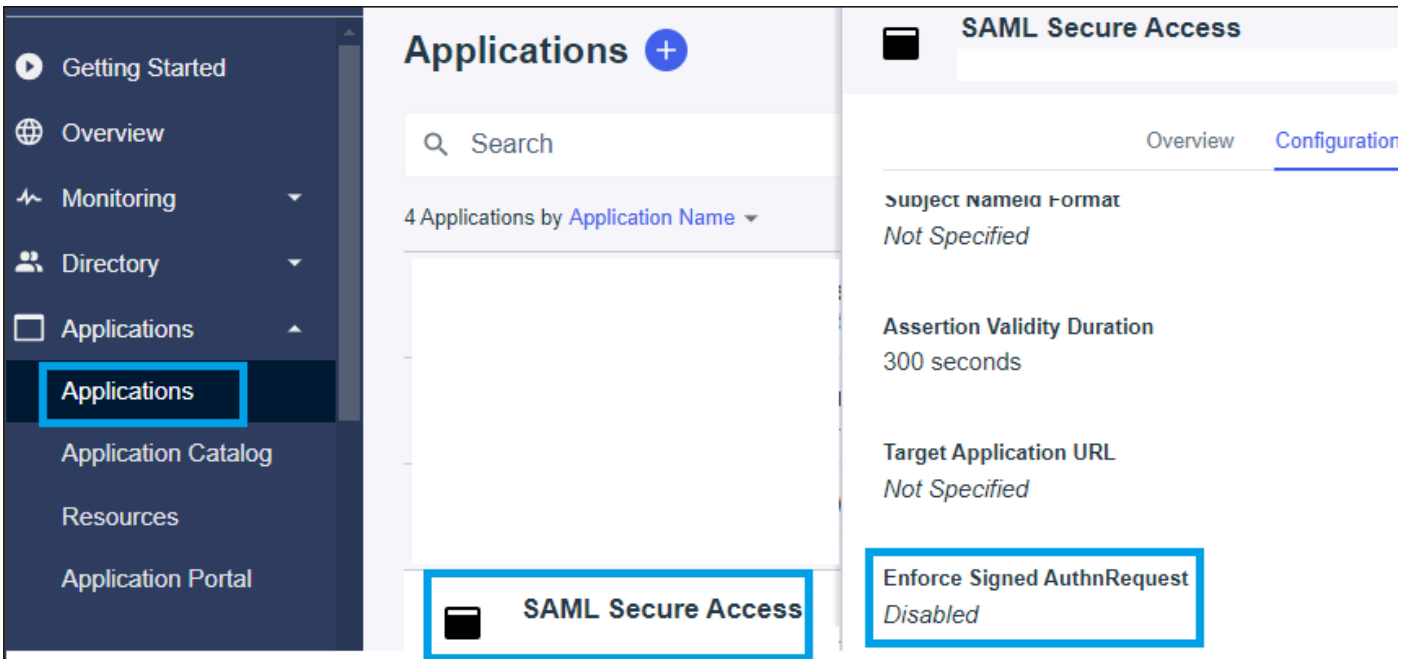


IdP Entra IDの「Verification Certificate (optional)」の値が「Required = yes」に設定されている場合、「Edit」および「Upload certificate」をクリックして、新しいセキュアアクセスSAML VPN証明書をアップロードします。

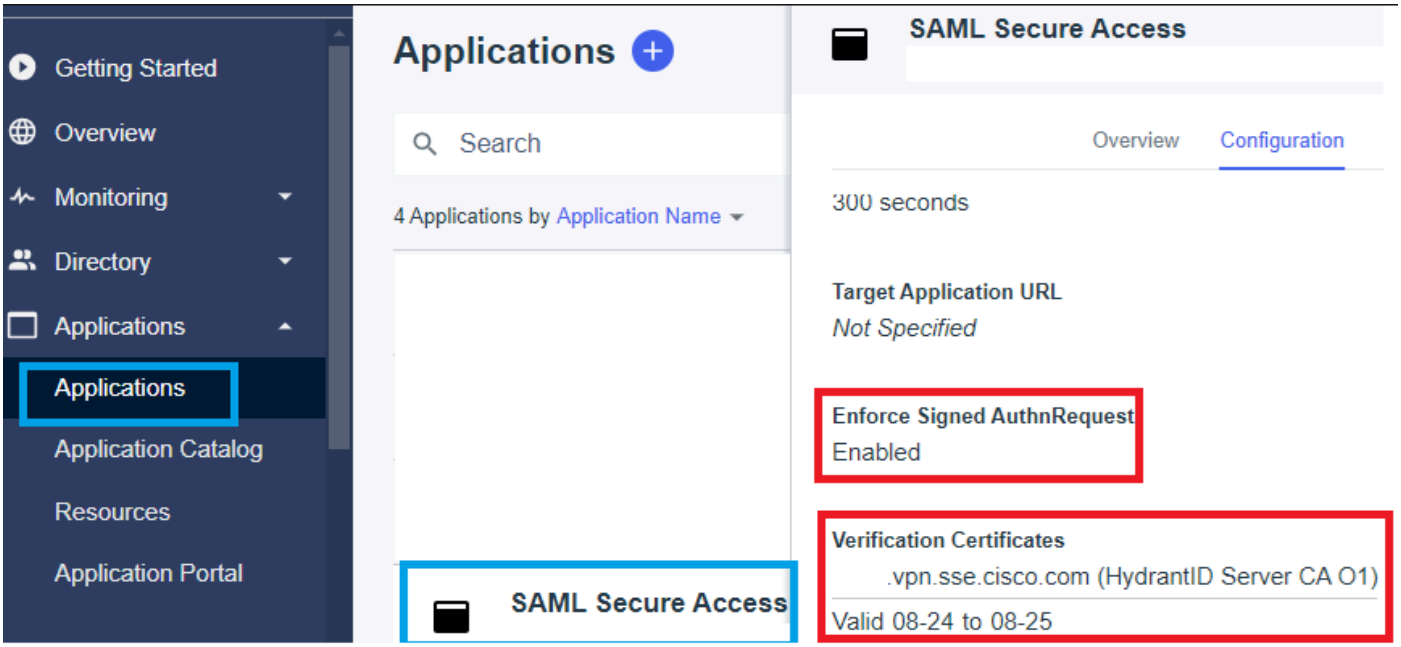


PingIdentity

PingIdentityは既定で証明書の検証を行いません。



IdP PingidentityでEnforce Signed AuthnRequestの値が「Enabled」に設定されている場合は、Editをクリックして新しいSecure Access SAML VPN Certificateをアップロードします。



シスコDUO

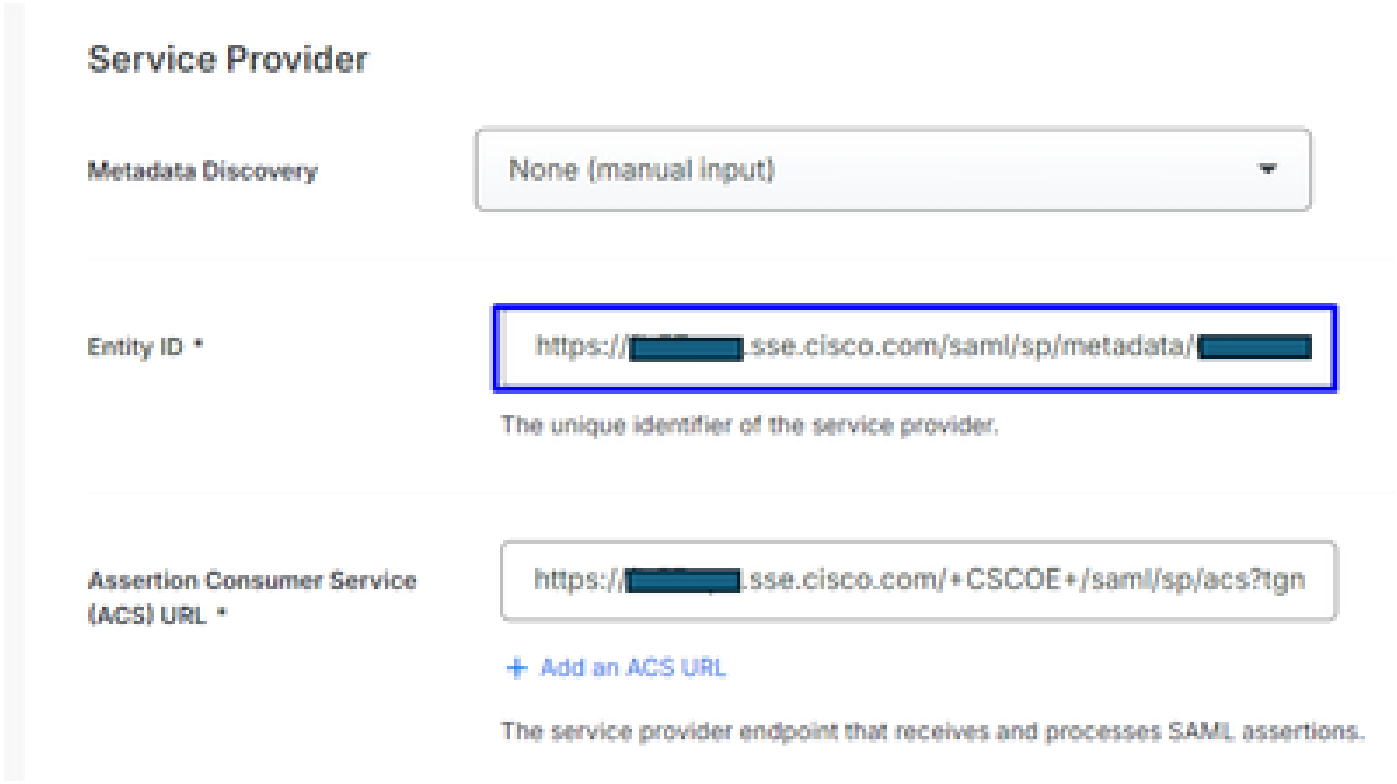
Cisco DUOはデフォルトで署名要求の検証を行いますが、アサーション暗号化が有効でない限り、DUO自体でアクションを実行する必要はありません。

リクエストの署名のために、DUOは管理者が提供するメタデータのエンティティIDリンクを使用して新しい証明書をダウンロードできます。

署名応答およびアサーションアクション

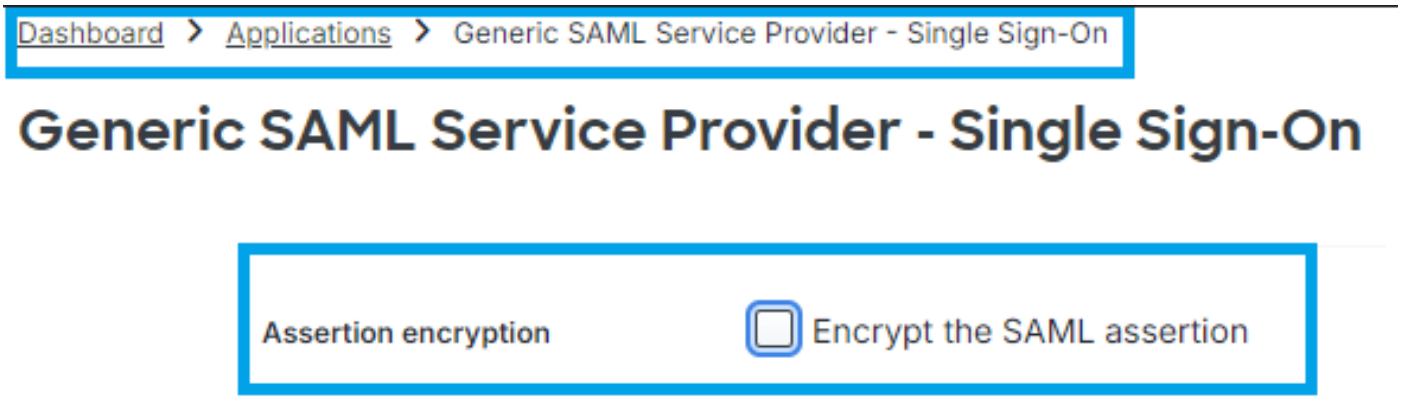
エンティティIDの設定

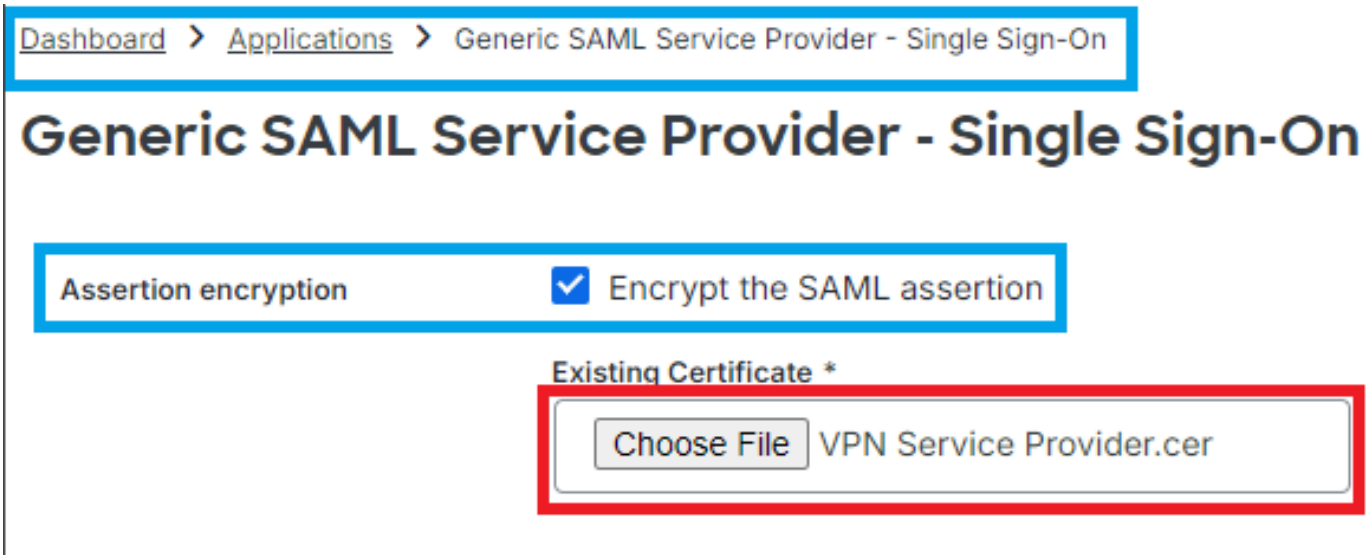
このステップでアクションは必要ありません。DUOは、エンティティIDリンクから新しい証明書を取得できます：https://<entry-id>.vpn.sse.cisco.com/saml/sp/metadata/<profile_name>。



アサーション暗号化

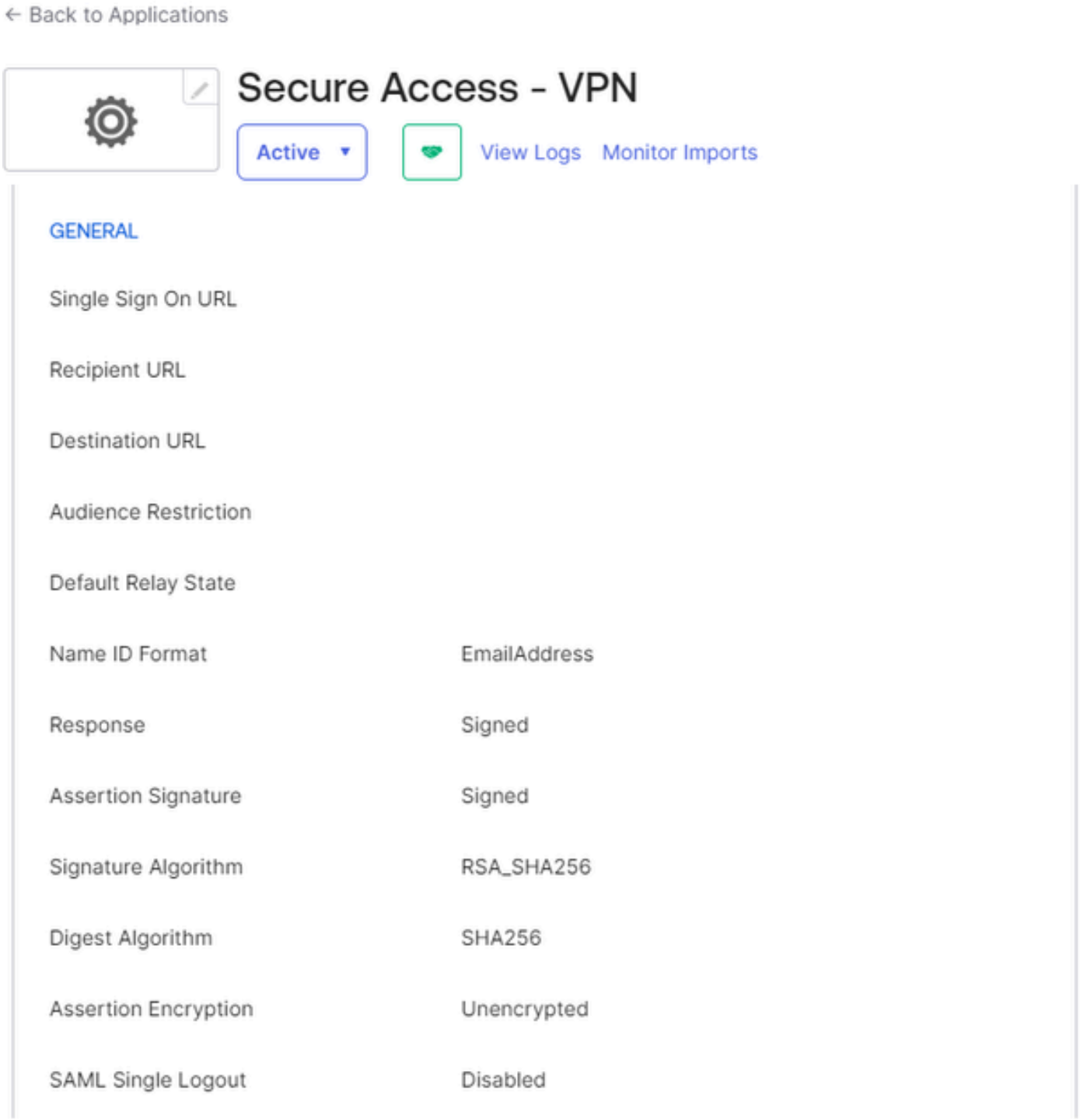
IdP Cisco DUOで「Assertion encryption」の値に「Encrypt the SAML Assertion」とマークされている場合は、「Choose File」をクリックし、新しいセキュアアクセスSAML VPN証明書をアップロードします。



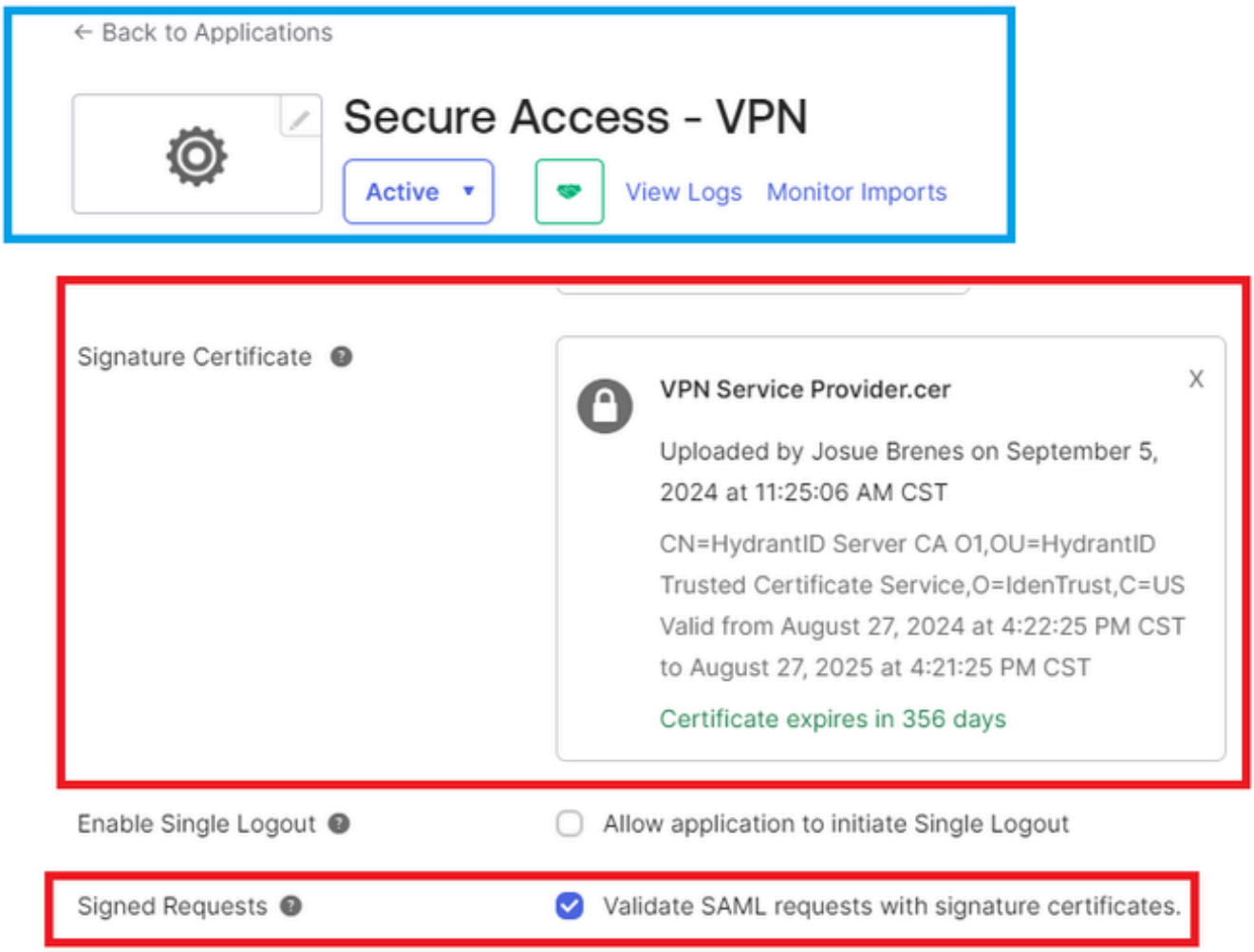


オクタ

OKTAは既定で証明書の検証を行いません。General > SAML Settingsには、「Signature Certificate」というオプションはありません。



IdP OKTAのGeneral > SAML Settingsに値がある場合は、「Signature Certificate Assertion encryption」と表示されており、OKTAが証明書の検証を行っていることを意味します。「SAML設定の編集」をクリックし、署名証明書をクリックして、新しいセキュアアクセスSAML VPN証明書をアップロードします。



関連情報

- セキュアアクセスヘルプセンター (ユーザガイド)
- テクニカル サポートとドキュメント - Cisco Systems
- セキュアアクセスコミュニティページ
- VPN用の新しいセキュアアクセスSAML認証証明書

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。