SWG SAML認証にUmbrellaの固定メタデータURLを使用

内容

はじめに

このドキュメントでは、Secure Web Gateway(SWG)SAML認証にUmbrellaの固定メタデータURL(PURL)を使用する方法について説明します。

前提条件

要件

このドキュメントに関する固有の要件はありません。

使用するコンポーネント

このドキュメントの情報は、Umbrella SWGに基づくものです。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

固定メタデータURL

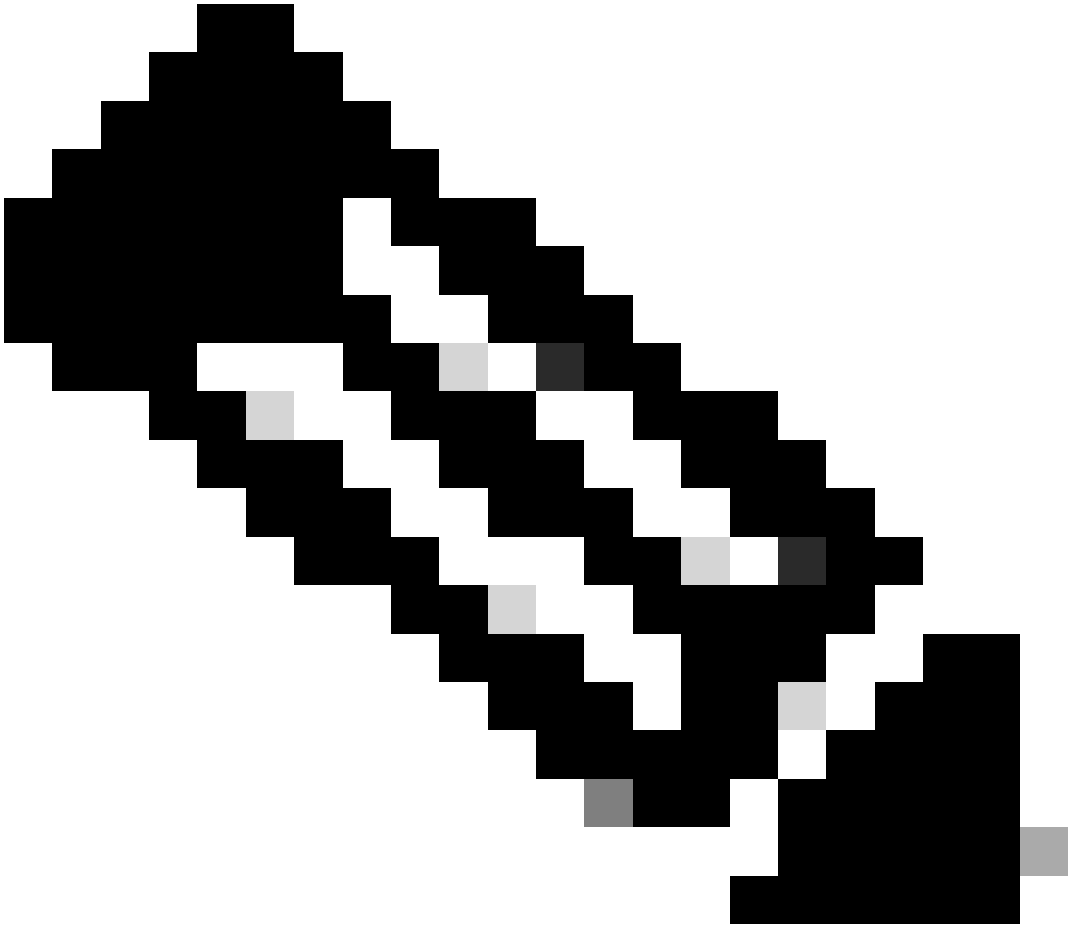
Umbrella SWGでSAML認証を使用する場合、証明書情報をアイデンティティプロバイダー(IdP)にインポートするための2つのオプションがあります。 これは、要求署名証明書を検証するIdPに必要です。

1. 固定メタデータURLによる自動設定

:https://api.umbrella.com/admin/v2/samlsp/certificates/Cisco_Umbrella_SP_Metadata.xml

2. 新しい署名証明書の手動インポート。証明書を置き換えるため、この操作は毎年行う必要があります。

最初のオプションは、メタデータのURLベースの自動更新をサポートするアイデンティティプロバイダー(IdP)に適した設定方法です。これには、Microsoft ADFSやPing Identityなどの一般的なIdPが含まれます。 利点は、手動による介入なしに、IdPが毎年新しい証明書を自動的にインポートすることです。



注：多くのIDPはSAML要求シグニチャの検証を実行しないため、これらの手順は必要ありません。 不明な場合は、IDプロバイダーのベンダーに確認を依頼してください。

要件

メタデータURLにアクセスするための要件

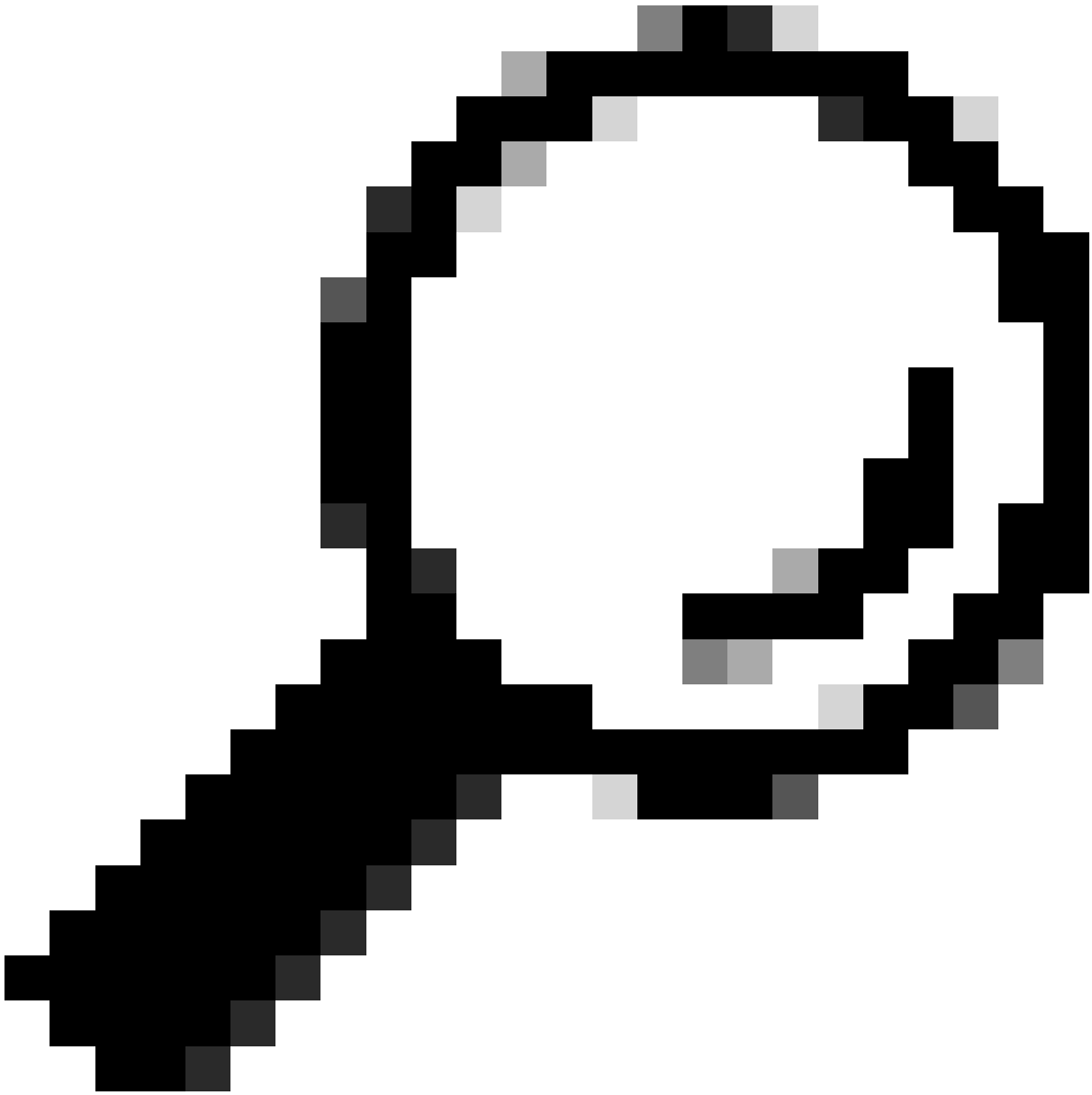
- URL（ADFS、Pingなど）からのサービスプロバイダーメタデータの自動更新をサポートするIdP

- お客様のIdPプラットフォームは、メタデータURLおよび関連する認証局URLにアクセスできる必要があります
- IdPプラットフォームは、証明書自体の認証局(CA)URLにもアクセスできる必要があります
- メタデータURLに安全に接続するには、IdPプラットフォームがTLS 1.2をサポートしている必要があります。IDPアプリケーションが.NET framework 4.6.1以前を使用する場合、Microsoftのドキュメントに従って、さらに設定が必要になる場合があります。

例： Microsoft ADFS

Umbrellaの証明書利用者信頼の設定を編集することで、固定メタデータURLを設定できます。

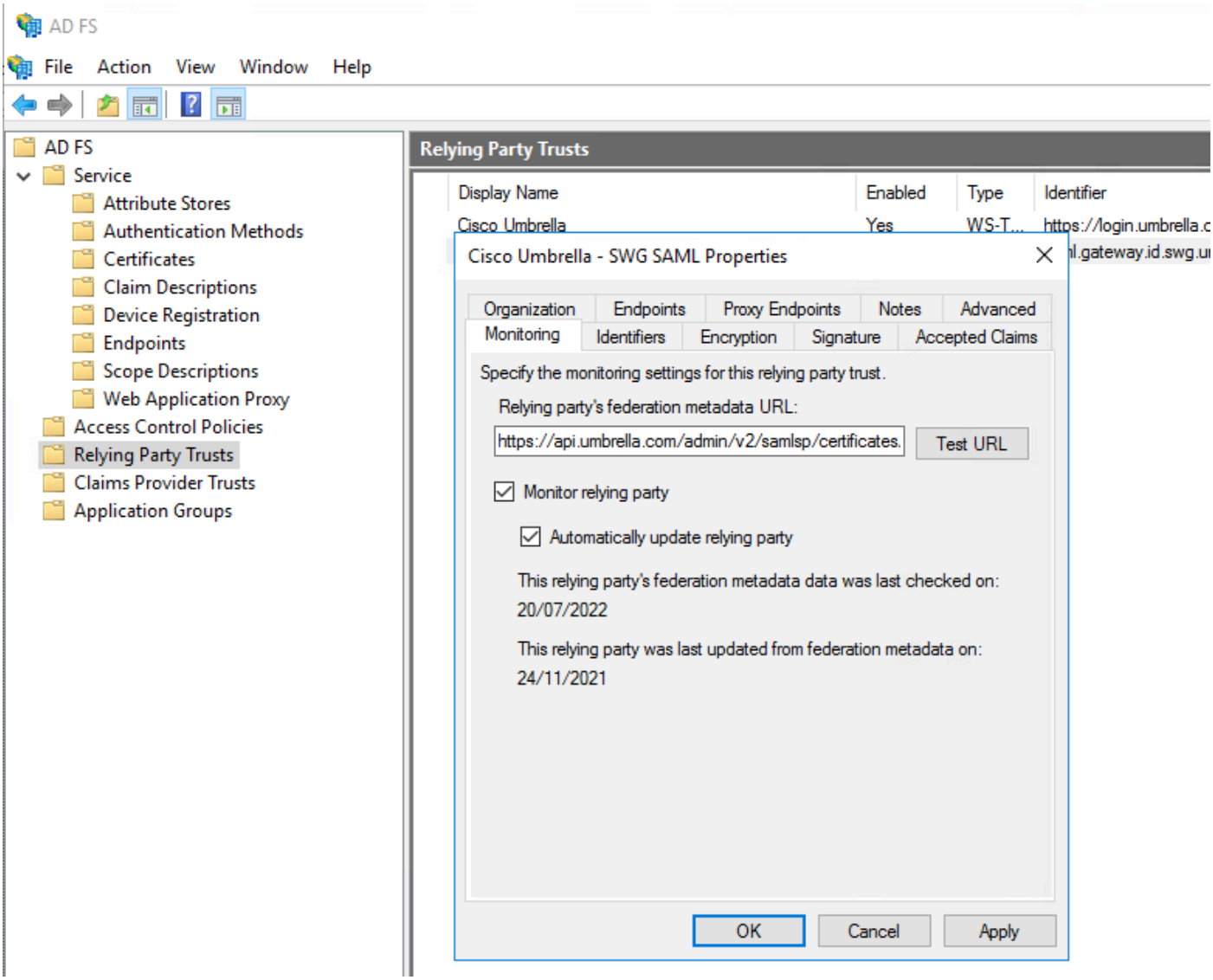
1. Monitoringタブに移動し、メタデータURLを入力します。
2. Monitor Relying Partyを選択して、Automatically Update Relying Partyを選択します。



ヒント:ADFSがURLへの接続に成功したことを確認するには、[URLのテスト]ボタンを選

択します。

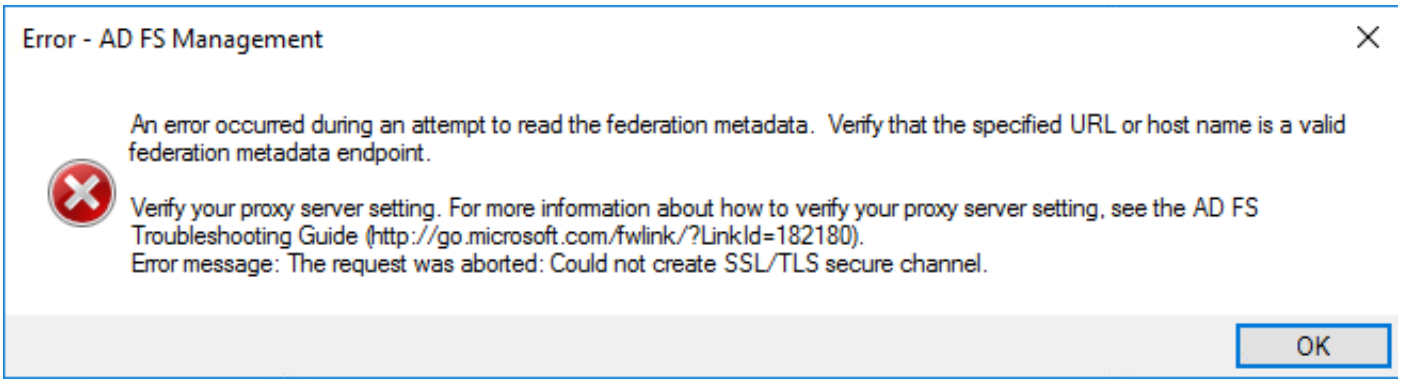
3. Applyを選択します。



ADFS_証明書利用者信頼.png

エラーのトラブルシューティング

エラー「An error occured during an attempt to read the federation metadata.Verify that the specified URL or host name is a valid federation metadata endpoint」というメッセージが表示される場合は、通常、レジストリを変更して.NET Frameworkバージョンで強力な暗号化を使用し、TLS 1.2をサポートするように設定する必要があります。



ADFSmetadata_TLS_error.png（ファイルの拡張子がADFSmetadata_TLS_error.png）

これらの変更の詳細については、MicrosoftがMicrosoftのドキュメントの.Net Frameworkセクションで公開しています。

ただし、通常はこのキーを作成してから、ADFS管理コンソールを閉じてから再度開く必要があります。

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319]
"SchUseStrongCrypto" = dword:00000001
```

制限：組織固有のEntityID機能

Umbrella SAML 組織固有のEntityID機能を使用する場合は、URLベースのメタデータ更新メカニズムを使用しないようにする必要があります。組織固有のエンティティIDは、同じアイデンティティプロバイダーに複数のUmbrella組織がリンクされている場合にのみ適用されます。このシナリオでは、証明書を各IDP設定に手動で追加する必要があります。

証明書の手動インポート（代替）

IdPがURLベースの更新をサポートしていない場合は、毎年、新しいUmbrella要求署名証明書をアイデンティティプロバイダーに手動でインポートする必要があります。

- 証明書は、有効期限が近い年にシスコのお知らせポータルで提供されます。通知を受け取るにはポータルを購読してください
- IdPのサービスプロバイダー/証明書利用者証明書のリストに新しい証明書を追加します。
  - 現在の証明書は削除しないでください。 Umbrellaは、有効期限が切れるまで古い証明書で署名を続行します。
- IdPにサービスプロバイダー/証明書利用者の証明書をインポートする機能が含まれていない場合、これはSAML要求を検証しないことを明確に示しており、それ以上のアクションは必要ありません。 確認するには、IdPベンダーに問い合わせてください。

新しい証明書をインポートした後に「UPN is not configured」エラーが発生した場合は、エラーが発生したことを示しています。 トラブルシューティングについては、次の記事を参照してください。SWG SAML - UPN Not Configuredエラー

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。