Utiliser l'URL de métadonnées fixes d'Umbrella pour l'authentification SWG SAML

Table des matières

Introduction

Ce document décrit comment utiliser l'URL de métadonnées fixes d'Umbrella pour l'authentification SAML Secure Web Gateway (SWG).

Conditions préalables

Exigences

Aucune exigence spécifique n'est associée à ce document.

Composants utilisés

Les informations contenues dans ce document sont basées sur Umbrella SWG.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

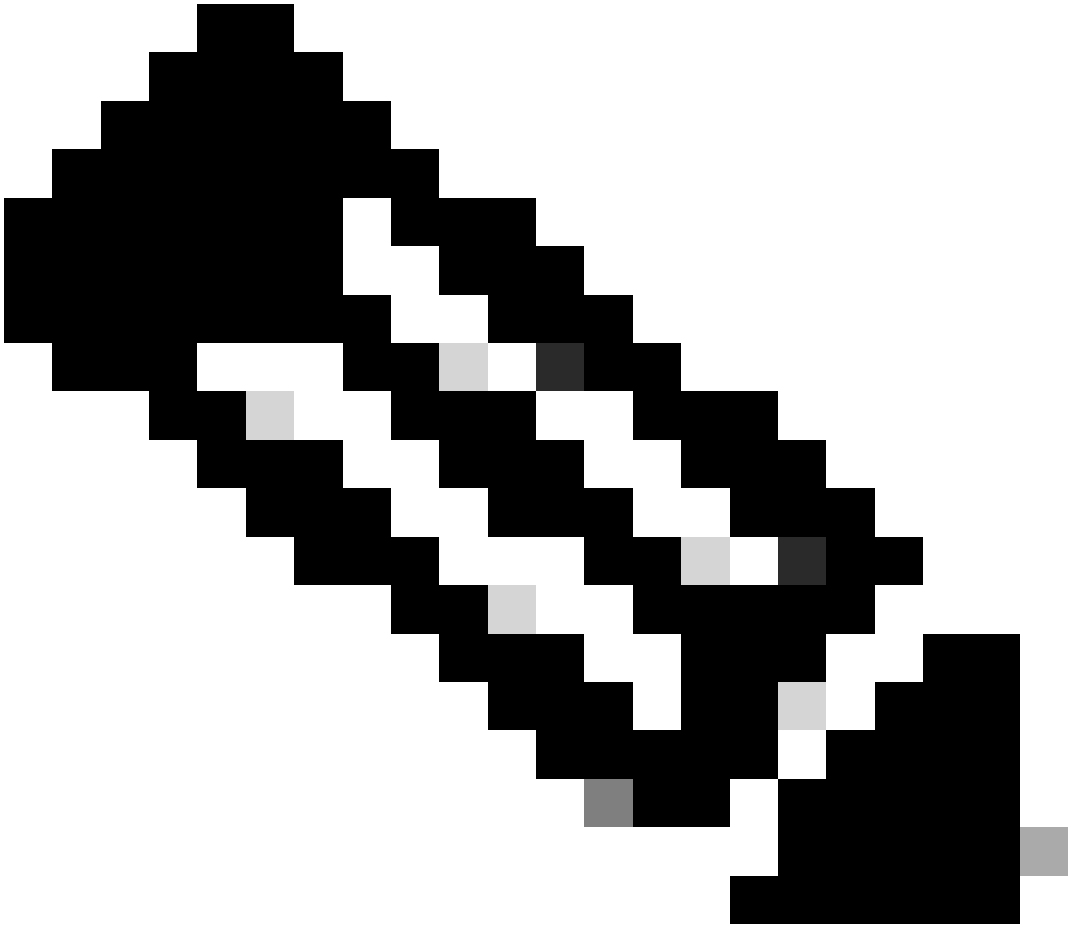
URL de métadonnées fixes

Lors de l'utilisation de l'authentification SAML pour Umbrella SWG, nous fournissons deux options pour importer nos informations de certificat dans votre fournisseur d'identité (IdP). Ceci est requis pour les IdP qui vérifient notre certificat de signature de demande.

1. Configuration automatique via l'URL de métadonnées fixe : https://api.umbrella.com/admin/v2/samlsp/certificates/Cisco_Umbrella_SP_Metadata.xml

2. Importation manuelle de notre nouveau certificat de signature. Cela doit être fait chaque année, car le certificat est remplacé.

La première option est maintenant la méthode de configuration préférée pour les fournisseurs d'identité (IdP) qui prennent en charge les mises à jour automatiques des métadonnées basées sur des URL. Cela inclut les IDp les plus répandus, tels que Microsoft ADFS et Ping Identity. L'avantage est que l'IdP importe automatiquement notre nouveau certificat chaque année sans intervention manuelle.



> Remarque : De nombreux IDP n'effectuent pas de validation des signatures de demande SAML et ces étapes ne sont donc pas requises. En cas de doute, contactez le fournisseur de votre fournisseur d'identité pour obtenir une confirmation.

Exigences

Conditions requises pour accéder à l'URL des métadonnées

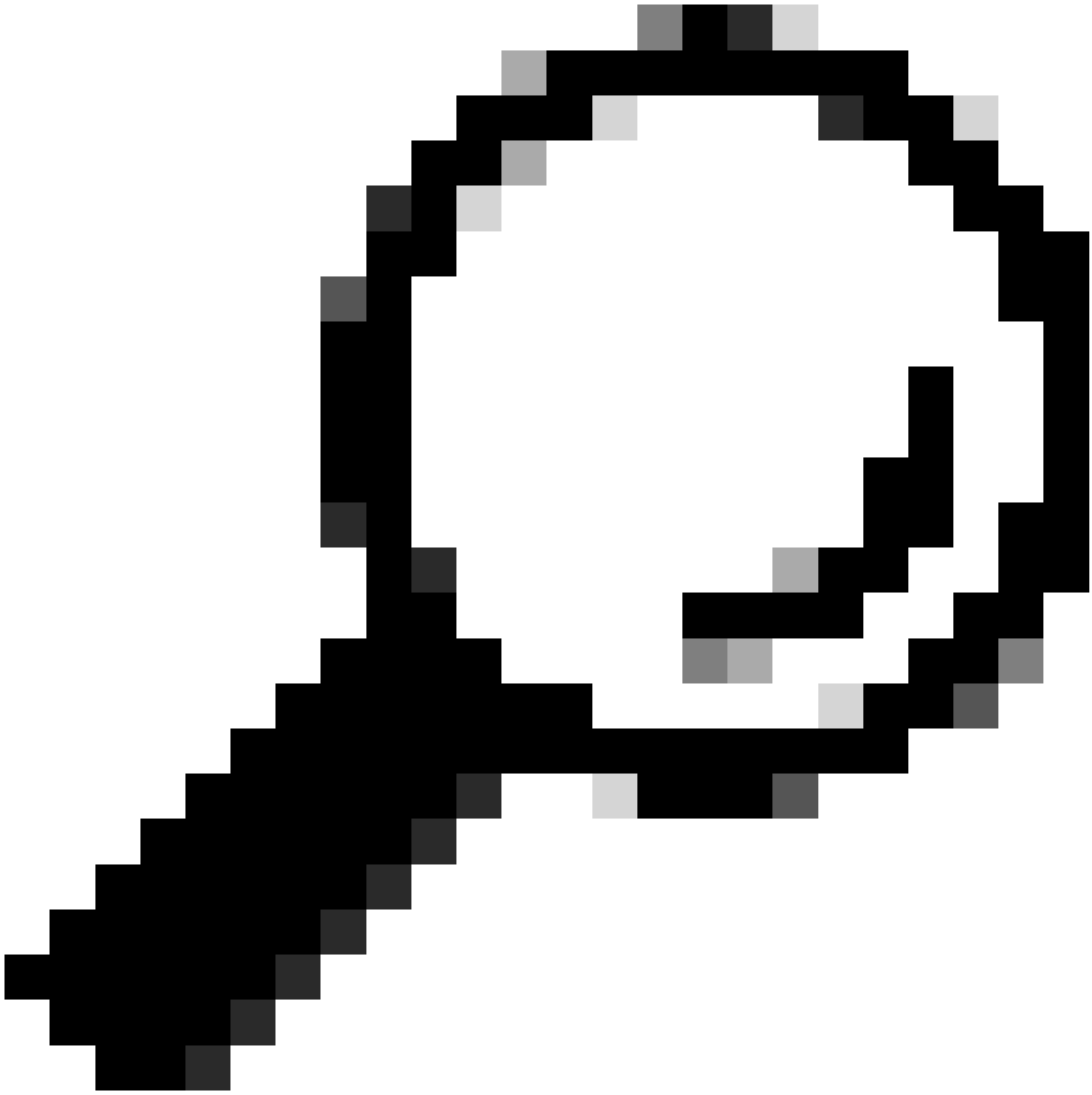
- Un fournisseur d'identité qui prend en charge les mises à jour automatiques des

métadonnées du fournisseur de services à partir des URL (telles que ADFS, Ping)
- Votre plate-forme IdP doit pouvoir accéder à notre URL de métadonnées ainsi qu'aux URL de l'autorité de certification associée
- Votre plate-forme IdP doit également pouvoir accéder aux URL de l'autorité de certification pour le certificat lui-même
- Votre plate-forme IdP doit prendre en charge TLS 1.2 afin de vous connecter à l'URL des métadonnées en toute sécurité. Si l'application IDP utilise .NET framework 4.6.1 ou une version antérieure, cela peut nécessiter une configuration supplémentaire, conformément à la documentation de Microsoft.

Exemple : Microsoft ADFS

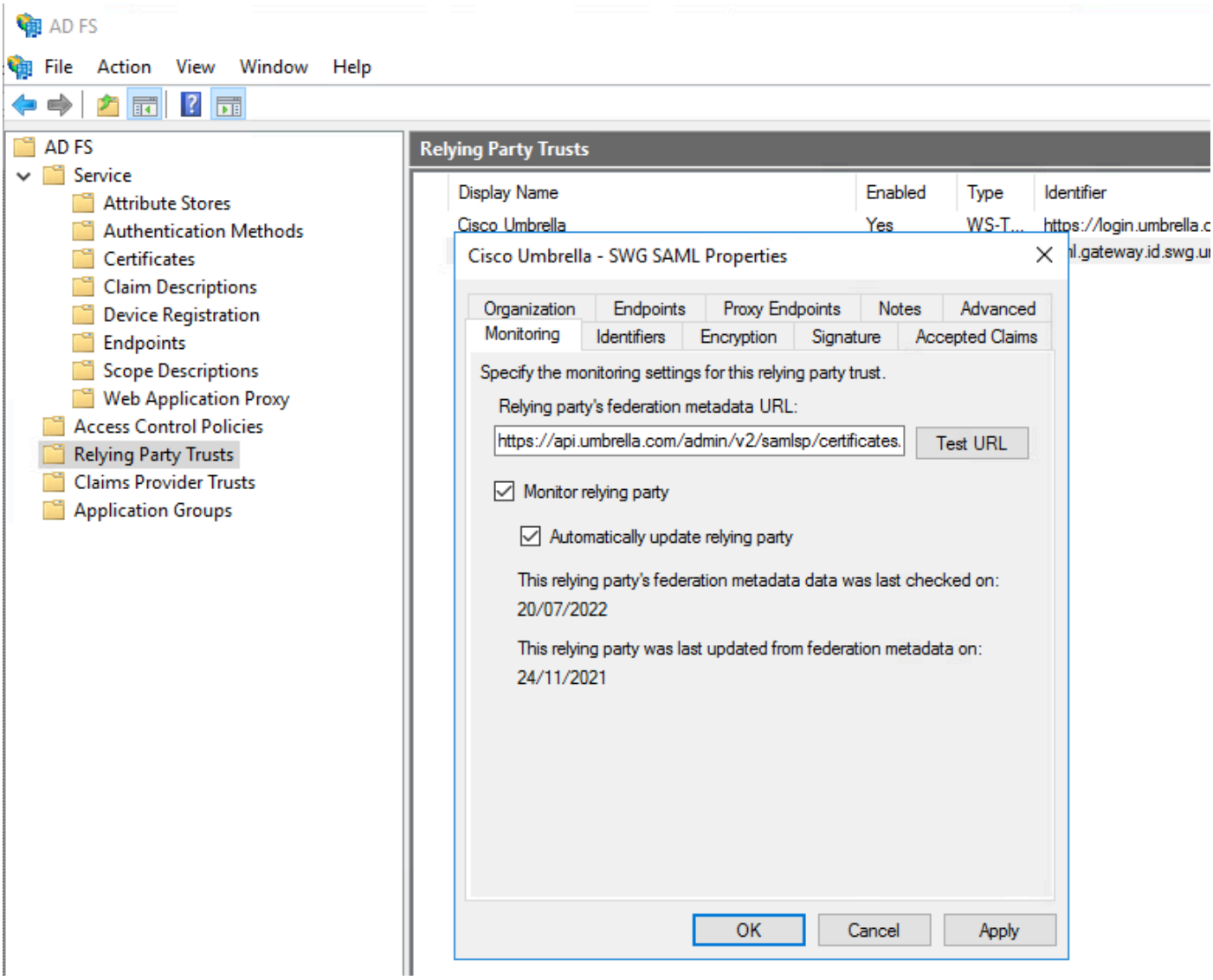
L'URL de métadonnées fixe peut être configurée en modifiant la configuration de l'approbation de la partie de confiance pour Umbrella :

1. Accédez à l'onglet Surveillance et entrez l'URL des métadonnées.
2. Sélectionnez Contrôler la partie de confiance et Mettre à jour automatiquement la partie de confiance.



Conseil : Cliquez sur le bouton Tester l'URL pour vérifier qu'ADFS contacte l'URL avec succès.

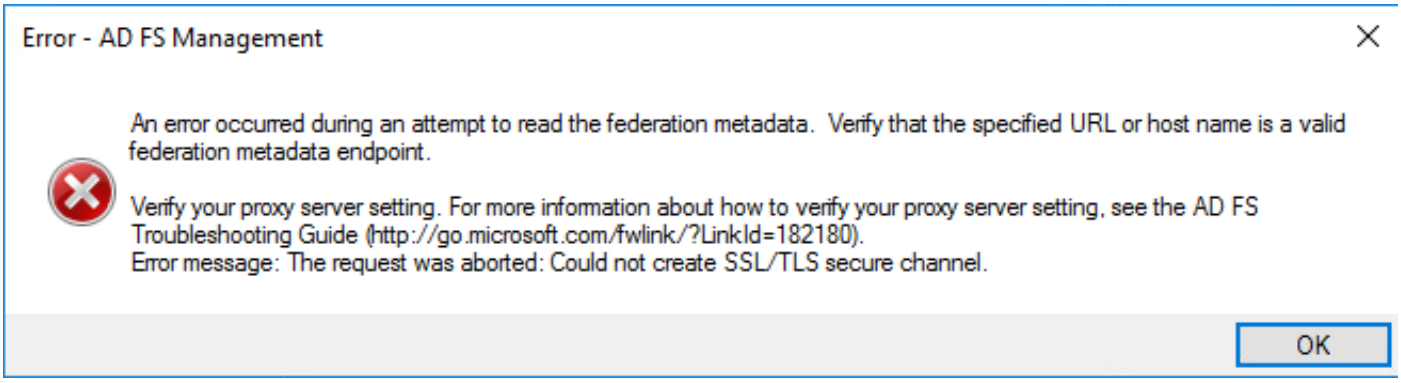
3. Sélectionnez Appliquer.



ADFS_RelyingPartyTrust.png

Dépannage des erreurs

Si vous recevez l'erreur, « Une erreur s'est produite lors d'une tentative de lecture des métadonnées de fédération. Vérifiez que l'URL ou le nom d'hôte spécifié est un « point de terminaison de métadonnées de fédération valide » lors du test de l'URL. Cela indique généralement qu'une modification du Registre est nécessaire pour configurer votre version du .NET Framework afin qu'elle utilise le chiffrement fort et prenne en charge TLS 1.2.



ADFSmetadata_TLS_error.png

Les détails complets de ces modifications sont publiés par Microsoft dans la section .Net Framework de la documentation Microsoft.

Cependant, cela nécessite généralement la création de cette clé, puis la fermeture et la réouverture de la console de gestion ADFS :

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

Limite: Fonction EntityID spécifique à l'organisation

Si vous utilisez la fonctionnalité EntityID spécifique à l'organisation SAML Umbrella, vous ne devez pas utiliser le mécanisme de mise à jour des métadonnées basé sur les URL. L'ID d'entité spécifique à l'organisation ne s'applique que si plusieurs organisations parapluie sont liées au même fournisseur d'identités. Dans ce scénario, vous devez ajouter manuellement le certificat à chaque configuration IDP.

Importation manuelle de certificat (alternative)

Si votre fournisseur d'identité ne prend pas en charge les mises à jour basées sur des URL, vous devez importer manuellement le nouveau certificat de signature de demande Umbrella chaque année à votre fournisseur d'identité.

- Le certificat est fourni dans notre portail Annonces chaque année peu avant la date d'expiration. S'inscrire au portail pour recevoir des notifications
- Ajoutez le nouveau certificat à la liste des certificats de fournisseur de services/de partie de confiance dans votre fournisseur d'identité.
    - NE supprimez PAS les certificats actuels. Umbrella continue à signer avec l'ancien certificat jusqu'à l'expiration.
- Si votre fournisseur d'identité ne contient pas de possibilité d'importer un certificat de fournisseur de services/de partie de confiance, cela indique clairement qu'il ne valide pas les demandes SAML et qu'aucune autre action n'est requise. Contactez votre fournisseur IdP pour confirmer.

Si vous rencontrez une erreur « UPN is not configured » après l'importation du nouveau certificat, cela indique qu'une erreur a été commise. Consultez cet article pour le dépannage : SWG SAML - Erreur UPN non configurée

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.