Feste Metadaten-URL von Umbrella für SWG SAML-Authentifizierung verwenden

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie die feste Metadaten-URL von Umbrella für die SAML-Authentifizierung des Secure Web Gateway (SWG) verwendet wird.

Voraussetzungen

Anforderungen

Es gibt keine spezifischen Anforderungen für dieses Dokument.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf Umbrella SWG.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Feste Metadaten-URL

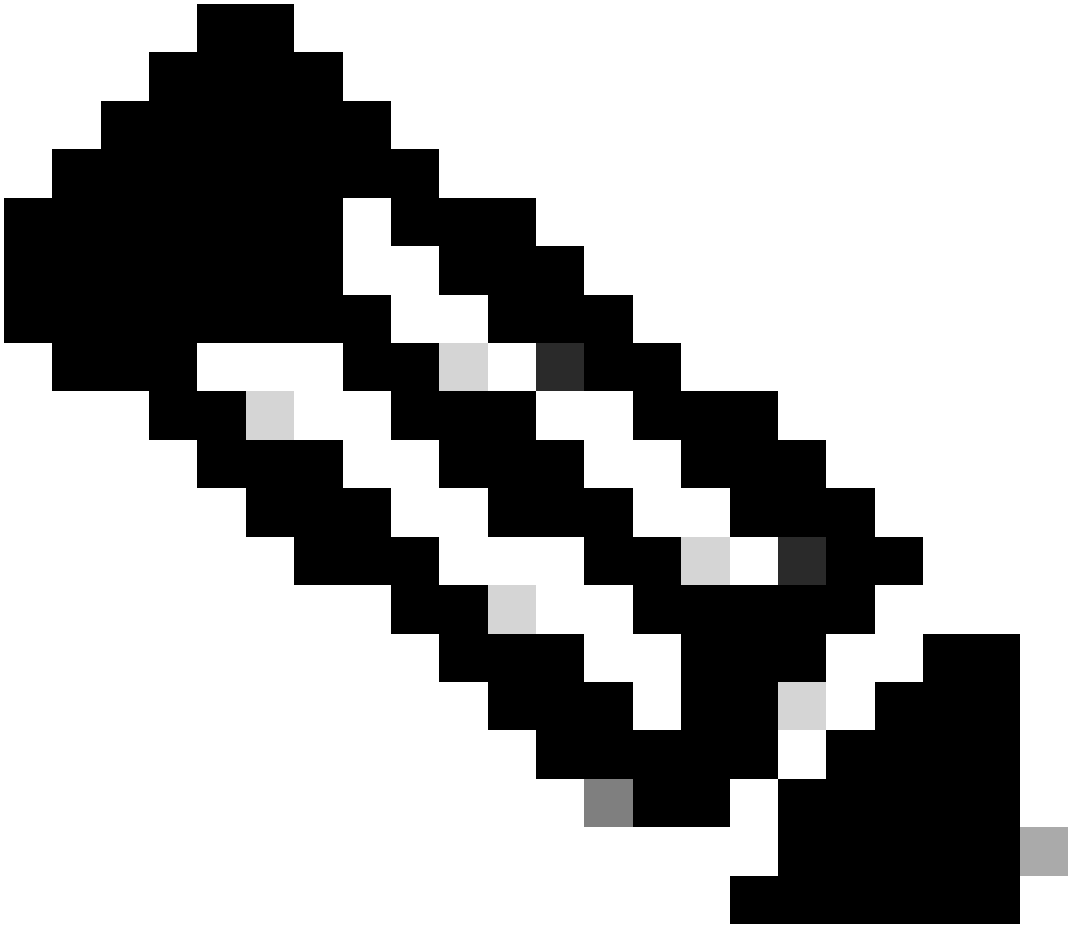
Bei der Verwendung der SAML-Authentifizierung für Umbrella SWG bieten wir zwei Optionen zum Importieren unserer Zertifikatinformationen in Ihren Identity Provider (IdP) an. Dies ist für die IDs erforderlich, die unser Anforderungssignaturzertifikat überprüfen.

1. Automatische Konfiguration über feste Metadaten-URL:

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

2. Manueller Import unseres neuen Signaturzertifikats. Dies muss jedes Jahr erfolgen, wenn das Zertifikat ersetzt wird.

Die erste Option ist jetzt die bevorzugte Konfigurationsmethode für Identitätsanbieter (IdP), die automatische URL-basierte Updates von Metadaten unterstützen. Dazu gehören gängige IDs wie Microsoft ADFS und Ping Identity. Der Vorteil besteht darin, dass die IdP unser neues Zertifikat jedes Jahr ohne manuellen Eingriff automatisch importiert.



Anmerkung: Viele IDPs führen keine Validierung von SAML-Anforderungssignaturen durch, daher sind diese Schritte nicht erforderlich. Wenden Sie sich im Zweifelsfall an Ihren Identity Provider-Anbieter, um eine Bestätigung zu erhalten.

Anforderungen

Anforderungen für den Zugriff auf die Metadaten-URL

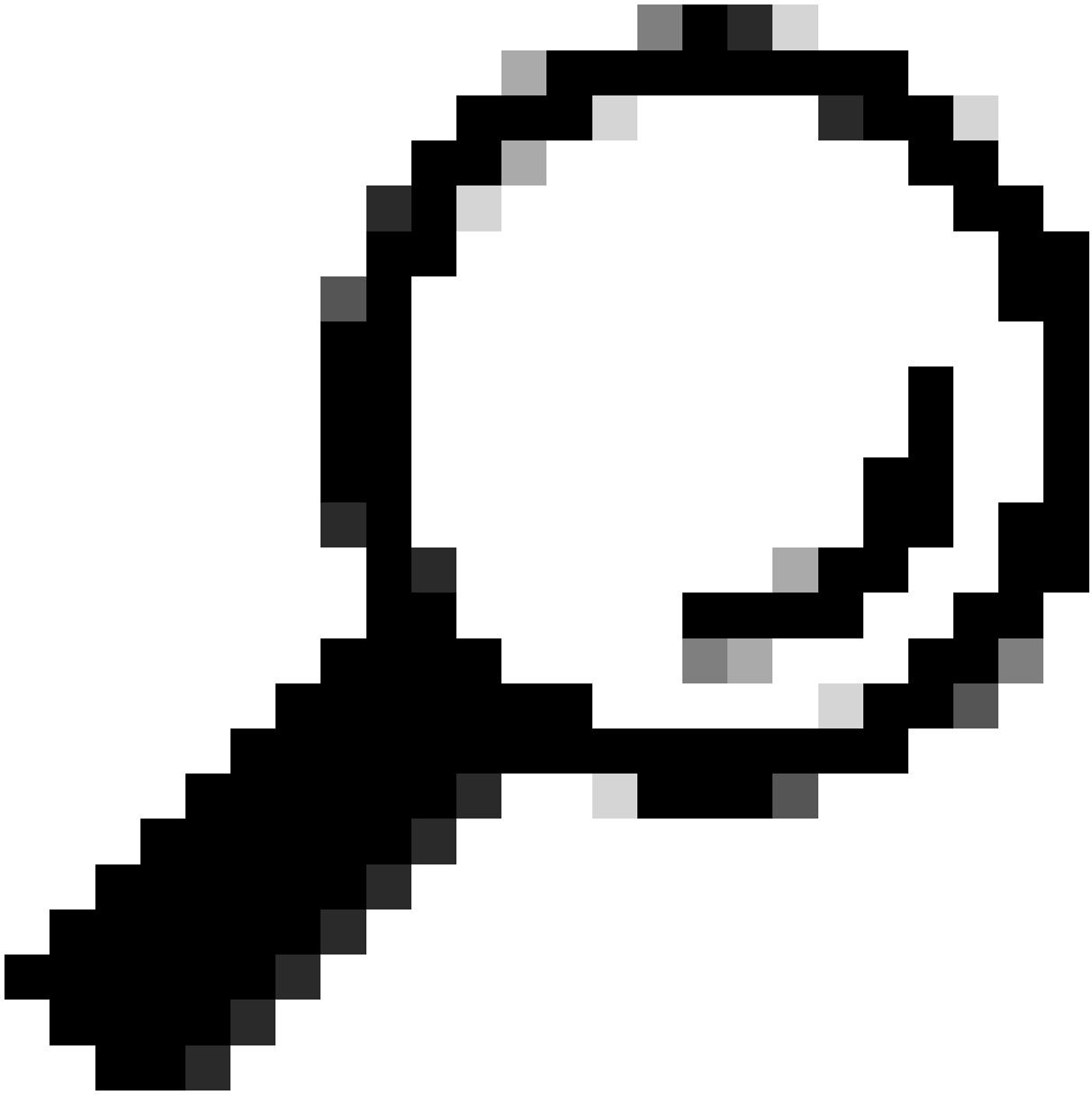
- Eine IdP, die automatische Updates von Dienstanbieter-Metadaten aus URLs unterstützt (z.

B. ADFS, Ping)
- Ihre IdP-Plattform muss auf unsere Metadaten-URL sowie die zugehörigen Zertifizierungsstellen-URLs zugreifen können.
- Ihre IdP-Plattform muss auch auf die Zertifizierungsstellen-URLs für das Zertifikat selbst zugreifen können.
- Ihre IdP-Plattform muss TLS 1.2 unterstützen, um eine sichere Verbindung zur Metadaten-URL herzustellen. Wenn die IDP-Anwendung .NET Framework 4.6.1 oder frühere Versionen verwendet, ist möglicherweise eine weitere Konfiguration gemäß Microsoft-Dokumentation erforderlich.

Beispiel: Microsoft ADFS

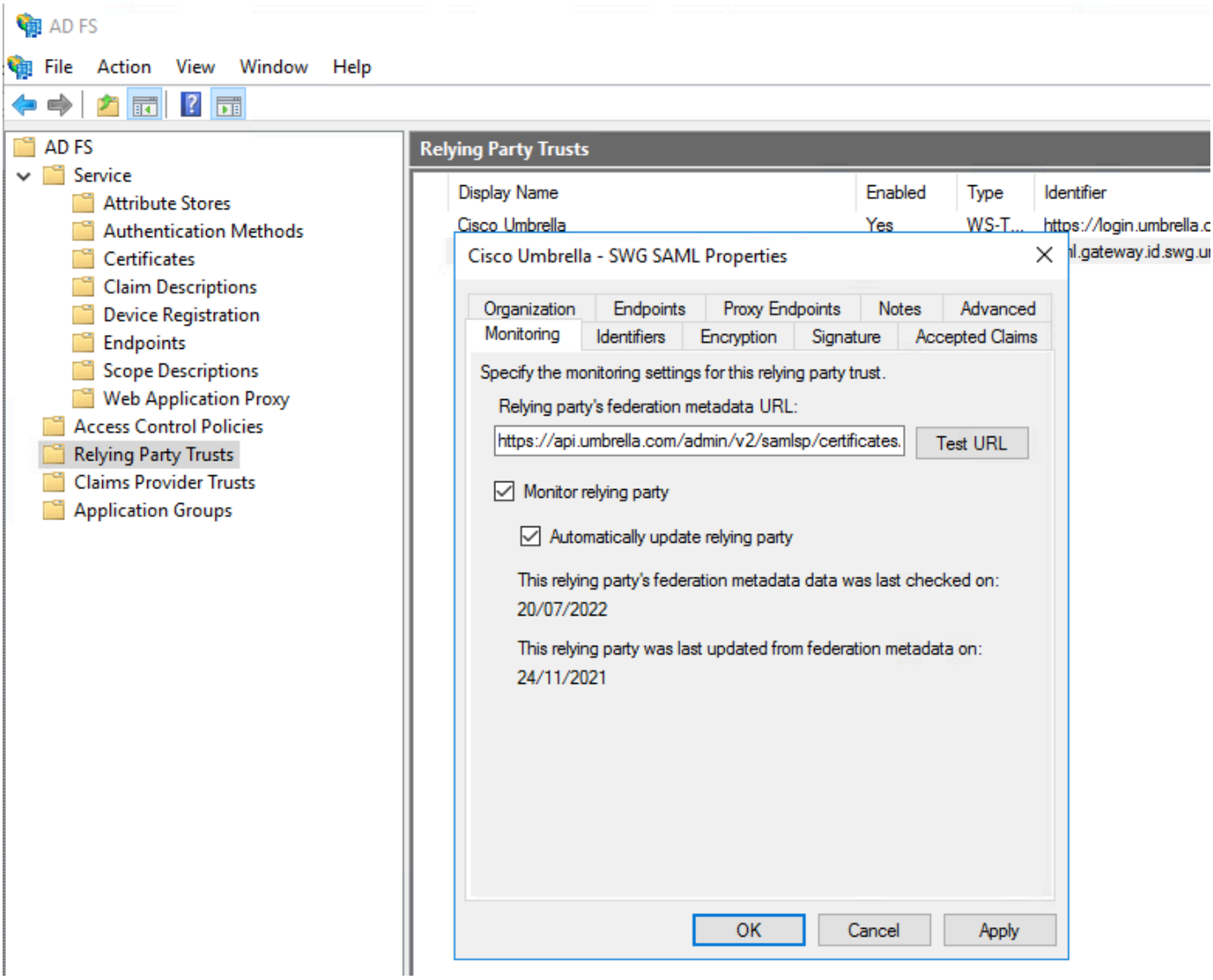
Die feste Metadaten-URL kann durch Bearbeiten der Einstellungen für die Vertrauensstellung der vertrauenden Partei für Umbrella konfiguriert werden:

1. Navigieren Sie zur Registerkarte Monitoring (Überwachung), und geben Sie die Metadaten-URL ein.
2. Wählen Sie Vertrauende Partei überwachen und Vertrauende Partei automatisch aktualisieren aus.



Tipp: Wählen Sie die Schaltfläche Test URL (URL testen), um zu überprüfen, ob ADFS die URL erfolgreich kontaktiert.

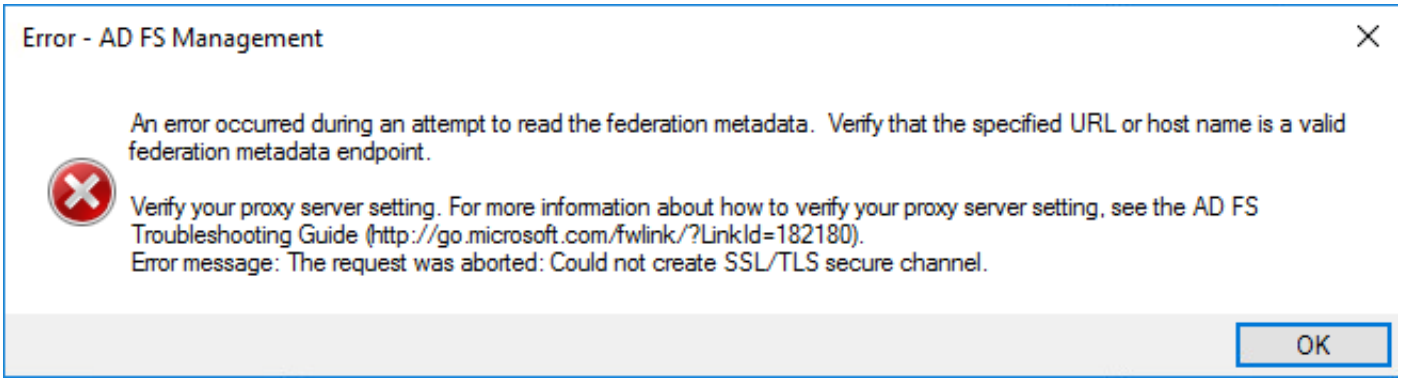
3. Wählen Sie Anwenden.



ADFS_RelyingPartyTrust.png

Fehlerbehebung

Wenn Sie den Fehler erhalten, "Fehler beim Lesen der Verbundmetadaten. Stellen Sie beim Testen der URL sicher, dass die angegebene URL oder der angegebene Hostname ein gültiger Endpunkt für Verbundmetadaten ist. Dies weist in der Regel darauf hin, dass eine Registrierungsänderung erforderlich ist, damit die .NET Framework-Version eine starke Verschlüsselung verwendet und TLS 1.2 unterstützt.



ADFSmetadaten_TLS_error.png

Vollständige Details zu diesen Änderungen werden von Microsoft im Abschnitt .Net Framework der Microsoft-Dokumentation veröffentlicht.

In der Regel ist dazu jedoch die Erstellung dieses Schlüssels und das Schließen und erneute Öffnen der ADFS-Verwaltungskonsole erforderlich:

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

Einschränkung: Org-spezifische EntityID-Funktion

Wenn Sie die Umbrella SAML Org-Specific EntityID-Funktion verwenden, dürfen Sie nicht den URL-basierten Metadaten-Aktualisierungsmechanismus verwenden. Die organisationsspezifische Objektkennung gilt nur, wenn mehrere Umbrella-Organisationen mit demselben Identitätsanbieter verknüpft sind. In diesem Szenario müssen Sie das Zertifikat manuell zu jeder IDP-Konfiguration hinzufügen.

Manueller Zertifikatimport (alternativ)

Wenn Ihr IdP keine URL-basierten Updates unterstützt, müssen Sie das neue Signaturzertifikat für Umbrella-Anfragen jedes Jahr manuell in Ihren Identity Provider importieren.

- Das Zertifikat wird jedes Jahr kurz vor dem Ablaufdatum in unserem Ankündigungsportal bereitgestellt. Portal für Benachrichtigungen abonnieren
- Fügen Sie das neue Zertifikat der Liste der Service Provider-/Relying Party-Zertifikate in Ihrer IdP hinzu.
    - Aktuelle Zertifikate NICHT löschen. Umbrella unterschreibt das alte Zertifikat bis zum Ablauf der Gültigkeit.
- Wenn Ihr IdP nicht über die Möglichkeit verfügt, ein Zertifikat eines Service Providers/einer vertrauenden Partei zu importieren, ist dies ein starker Hinweis darauf, dass SAML-Anfragen nicht validiert werden und keine weiteren Maßnahmen erforderlich sind. Wenden Sie sich zur Bestätigung an Ihren IdP-Anbieter.

Wenn nach dem Importieren des neuen Zertifikats der Fehler "UPN ist nicht konfiguriert" auftritt, weist dies auf einen Fehler hin. Weitere Informationen zur Fehlerbehebung finden Sie in diesem Artikel: SWG SAML - Fehler: UPN nicht konfiguriert

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.