

De vaste metagegevens-URL van Umbrella gebruiken voor SWG SAML-verificatie

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Vaste metagegevens-URL](#)

[Vereisten](#)

[Voorbeeld: Microsoft ADFS](#)

[Fouten bij probleemoplossing](#)

[Beperking: functie voor organisatiespecifieke entiteit-ID](#)

[Handmatig certificaat importeren \(alternatief\)](#)

Inleiding

In dit document wordt beschreven hoe u de vaste metagegevens-URL van Umbrella kunt gebruiken voor Secure Web Gateway (SWG) SAML-verificatie.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op Umbrella SWG.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Vaste metagegevens-URL

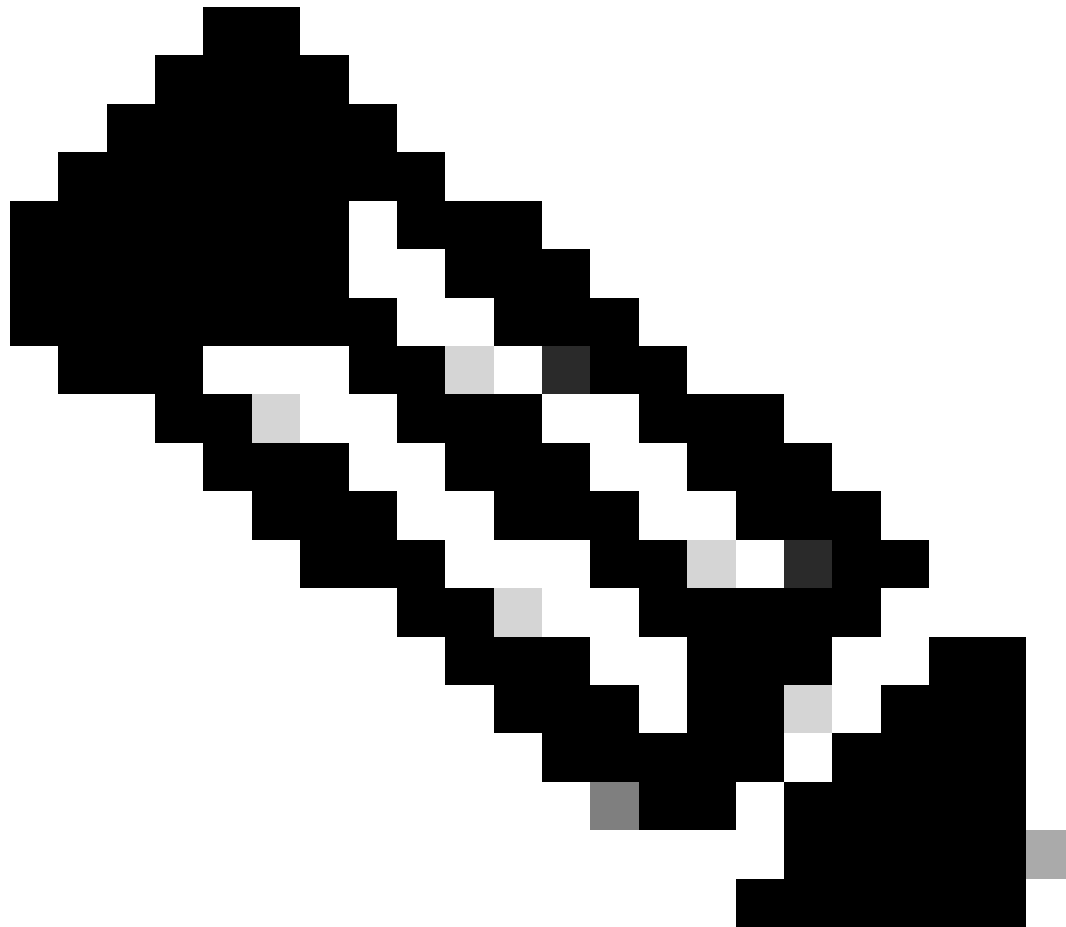
Bij het gebruik van SAML-verificatie voor Umbrella SWG bieden we twee opties voor het importeren van onze certificaatinformatie in uw identiteitsprovider (IdP). Dit is vereist voor die IdP's die ons certificaat voor het ondertekenen van aanvragen verifiëren.

1. Automatische configuratie via vaste metagegevens URL:

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

2. Handmatig importeren van ons nieuwe ondertekeningscertificaat. Dit moet elk jaar gebeuren, omdat het certificaat wordt vervangen.

De eerste optie is nu de voorkeursconfiguratiemethode voor identiteitsproviders (IdP) die automatische updates van metagegevens op basis van URL's ondersteunen. Dit omvat populaire IdP's zoals Microsoft ADFS en Ping Identity. Het voordeel is dat de IdP ons nieuwe certificaat elk jaar automatisch importeert zonder handmatige tussenkomst.



Opmerking: veel IDP's valideren de handtekeningen voor SAML-verzoeken niet en daarom zijn deze stappen niet vereist. Neem in geval van twijfel contact op met de leverancier van uw identiteitsprovider voor een bevestiging.

Vereisten

Vereisten voor toegang tot de metagegevens-URL

- Een IdP die automatische updates van metagegevens van serviceproviders vanuit URL's

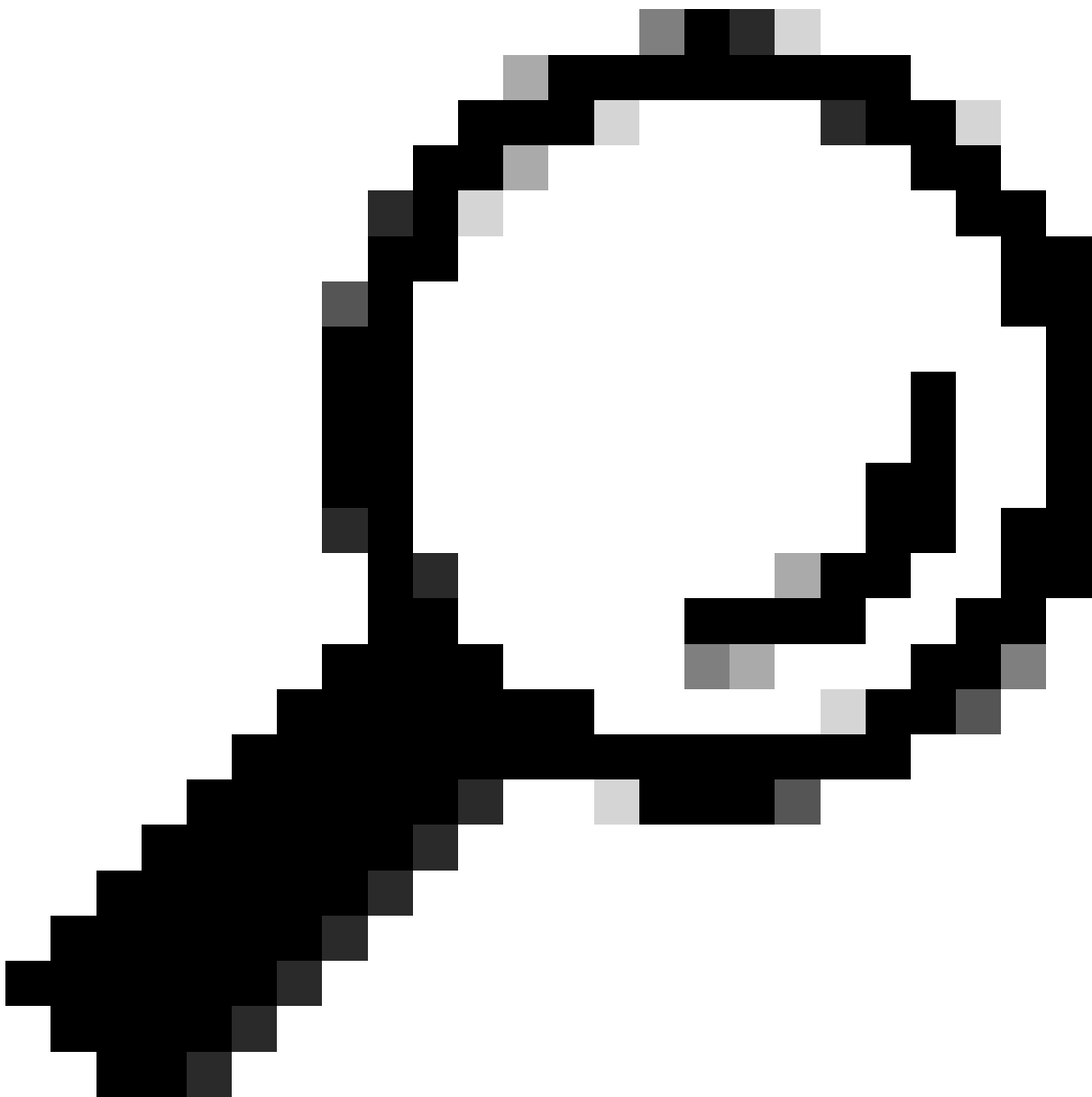
(zoals ADFS, Ping) ondersteunt

- Uw IdP-platform moet toegang hebben tot onze metagegevens-URL en de bijbehorende URL's van de certificeringsinstantie
- Uw IdP-platform moet ook toegang hebben tot de URL's van de certificeringsinstantie voor het certificaat zelf
- Uw IdP-platform moet TLS 1.2 ondersteunen om veilig verbinding te maken met de metagegevens-URL. Als de IDP-toepassing .NET framework 4.6.1 of eerder gebruikt, kan dit enige verdere configuratie vereisen volgens de documentatie van Microsoft.

Voorbeeld: Microsoft ADFS

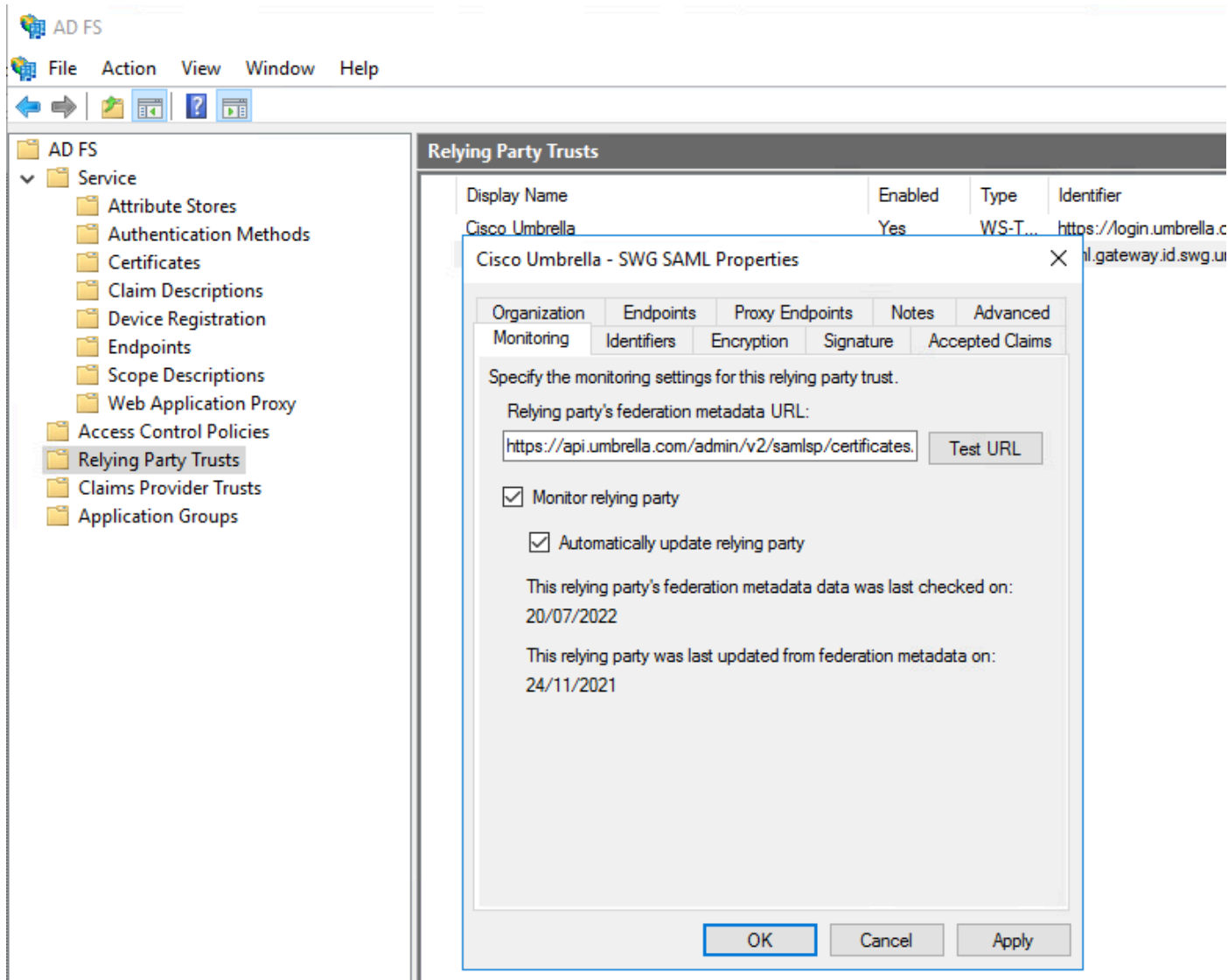
De vaste metagegevens-URL kan worden geconfigureerd door de Relying Party Trust-instelling voor Umbrella te bewerken:

1. Navigeer naar het tabblad Monitoring en voer de metagegevens-URL in.
2. Selecteer Betrouwbare partij controleren en Betrouwbare partij automatisch bijwerken.



Tip: Selecteer de knop URL testen om te controleren of ADFS met succes contact opneemt met de URL.

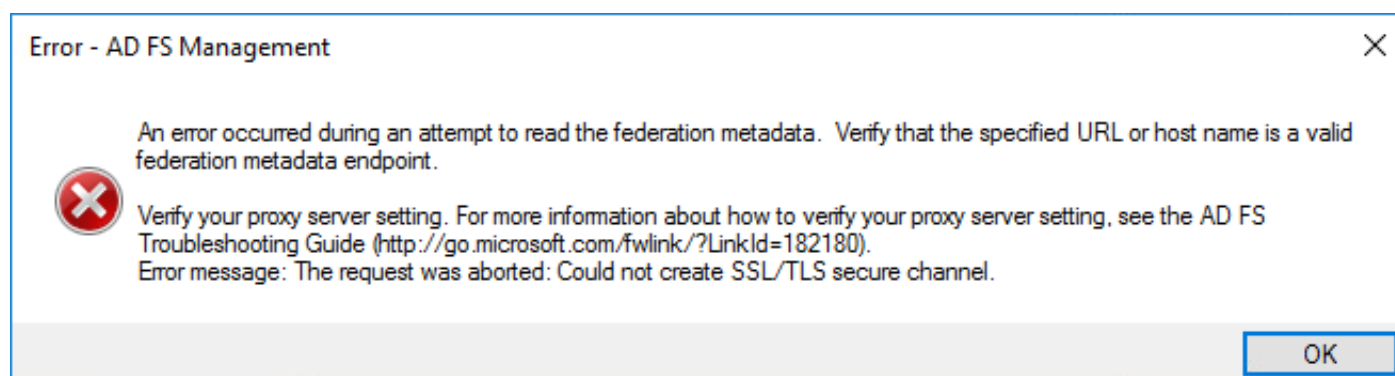
3. Selecteer Toepassen.



ADFS_RelyingPartyTrust.png

Fouten bij probleemoplossing

Als u de fout "Er is een fout opgetreden tijdens een poging om de metagegevens van de federatie te lezen. Controleer of de opgegeven URL of hostnaam een "geldig federatief metagegevenseindpunt" is bij het testen van de URL, dit geeft meestal aan dat een registerwijziging vereist is om uw .NET Framework-versie in te stellen om sterke crypto te gebruiken en TLS 1.2 te ondersteunen.



ADFSmetadata_TLS_error.png

Alle details over deze wijzigingen worden door Microsoft gepubliceerd in het gedeelte .Net Framework van de Microsoft-documentatie.

Doorgaans moet u deze sleutel maken en vervolgens de ADFS-beheerconsole sluiten en opnieuw openen:

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

Beperking: functie voor organisatiespecifieke entiteit-ID

Als u de Umbrella SAML Org-Specific EntityID-functie gebruikt, mag u niet het updatemechanisme voor op URL gebaseerde metagegevens gebruiken. Org-Specific Entity ID is alleen van toepassing als u meerdere Umbrella-organen hebt die zijn gekoppeld aan dezelfde Identity Provider. In dit scenario moet u het certificaat handmatig toevoegen aan elke IDP-configuratie.

Handmatig certificaat importeren (alternatief)

Als uw IdP geen ondersteuning biedt voor URL-gebaseerde updates, moet u het nieuwe ondertekeningscertificaat voor het Umbrella-verzoek elk jaar handmatig importeren naar uw identiteitsprovider.

- Het certificaat wordt elk jaar kort voor de vervaldatum verstrekt in onze aankondigingen portal. Abonneer u op de portal voor meldingen
- Voeg het nieuwe certificaat toe aan de lijst met certificaten van Serviceverlener / Vertrouwende partij in uw IdP.
 - Verwijder geen huidige certificaten. Paraplu blijft ondertekenen met het oude certificaat tot het moment van verstrijken.
- Als uw IdP geen mogelijkheid bevat om een certificaat van de Serviceverlener/Vertrouwende partij te importeren, is dit een sterke indicatie dat het SAML-verzoeken niet valideert en dat er geen verdere actie vereist is. Neem contact op met uw IdP-leverancier om dit te bevestigen.

Als u na het importeren van het nieuwe certificaat een foutmelding "UPN is niet geconfigureerd" tegenkomt, geeft dit aan dat er een fout is gemaakt. Raadpleeg dit artikel voor probleemoplossing: SWG SAML - UPN Not Configured Error

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.