Utilize Umbrella's Fixed Metadata URL for SWG SAML Authentication

Contents

Introduction

This document describes how to utilize Umbrella's fixed metadata URL for Secure Web Gateway (SWG) SAML authentication.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on 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. If your network is live, ensure that you understand the potential impact of any command.

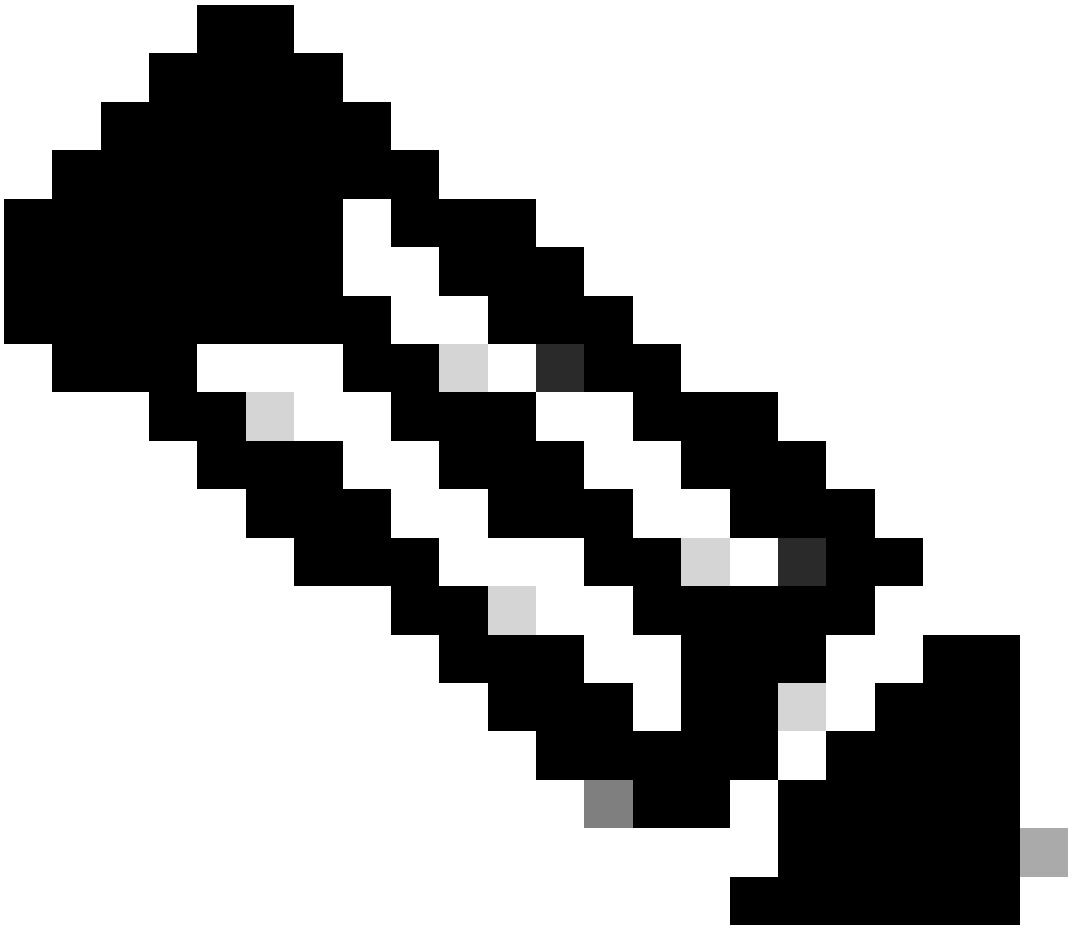
Fixed Metadata URL

When utilizing SAML authentication for Umbrella SWG we provide two options for importing our certificate information into your Identity Provider (IdP). This is required for those IdPs that verify our request signing certificate.

1. **Automatic configuration** via fixed metadata URL: https://api.umbrella.com/admin/v2/samlsp/certificates/Cisco_Umbrella_SP_Metadata.xml
2. **Manual import** of our new signing certificate. This needs to be done each year as the certificate is replaced.

The first option is now the preferred configuration method for identity providers (IdP) that support URL-

Based automatic updates of metadata. This includes popular IdPs such as Microsoft ADFS and Ping Identity. The benefit is that the IdP automatically imports our new certificate each year without manual intervention.



> **Note**: Many IDPs do not perform validation of SAML request signatures and therefore these steps are not required. If in doubt, please contact your Identity Provider vendor for confirmation.

Requirements

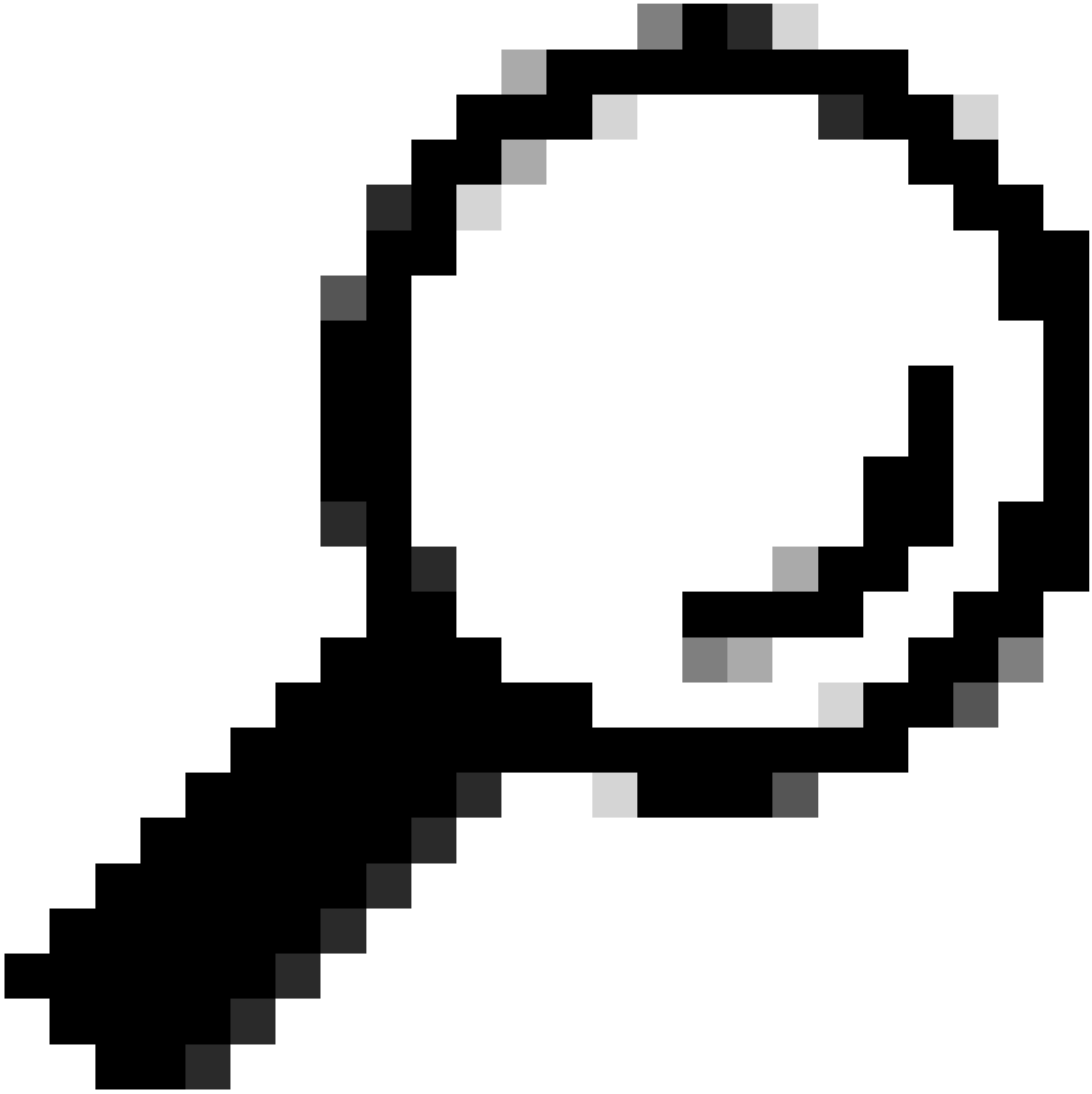
Requirements to access the metadata URL

- An IdP that supports **automatic updates of service provider metadata** from URL (such as ADFS, Ping)
- Your IdP platform must be able to **access our metadata URL** as well as the associated **Certificate Authority URLs**
- Your IdP platform must also be able to access the **Certificate Authority URLs** for the certificate itself
- Your IdP platform must **support TLS 1.2** in order to connect to the metadata URL securely. If the IDP application utilizes .NET framework 4.6.1 or earlier, this might require some further configuration as per Microsoft's documentation.

Example: Microsoft ADFS

The fixed metadata URL can be configured by editing the **Relying Party Trust** setup for Umbrella:

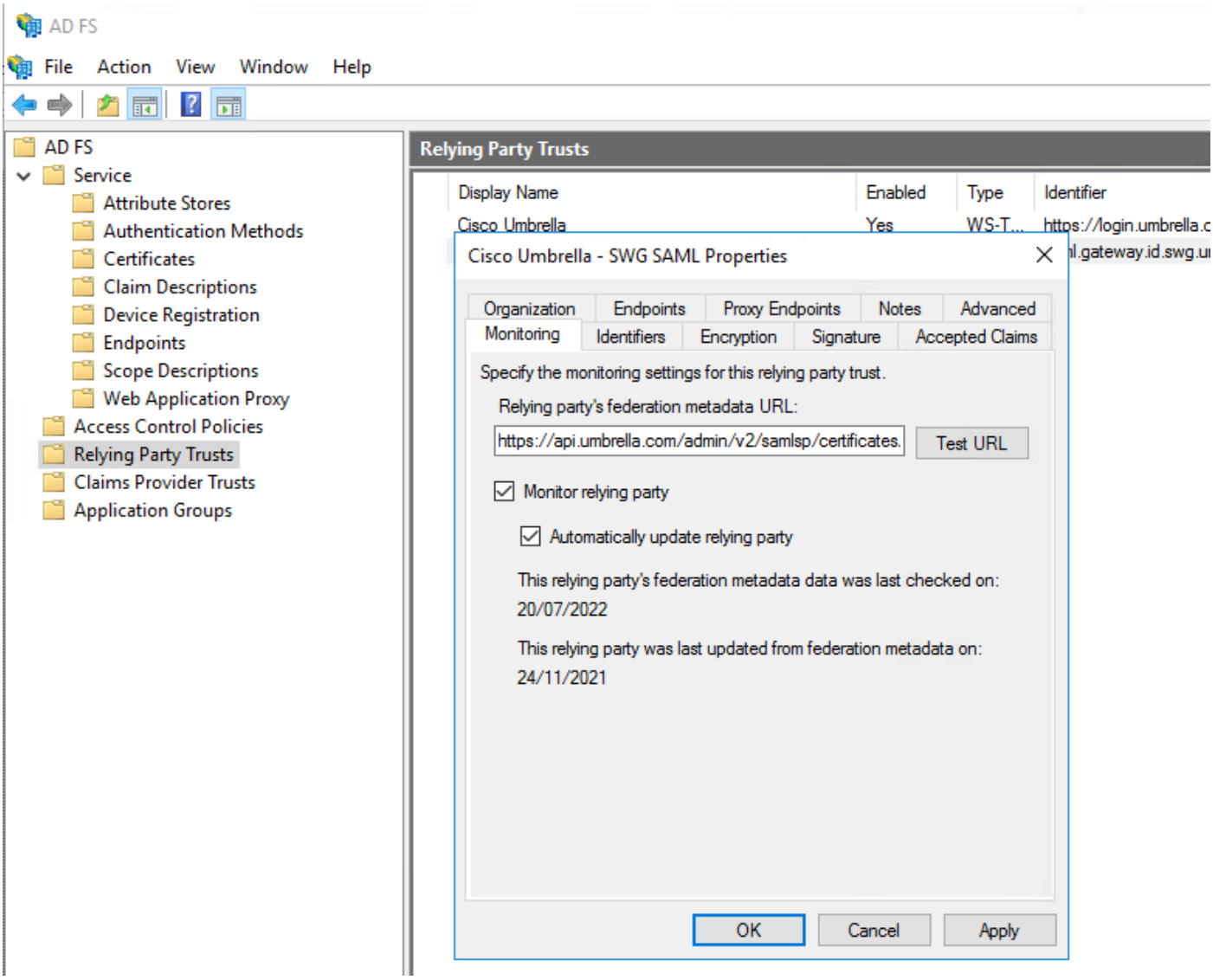
1. Navigate to the **Monitoring** tab and enter the Metadata URL.
2. Select **Monitor Relying Party** and **Automatically Update Relying Party**.



Tip: Select the **Test URL** button to verify that ADFS contacts the URL successfully.

---

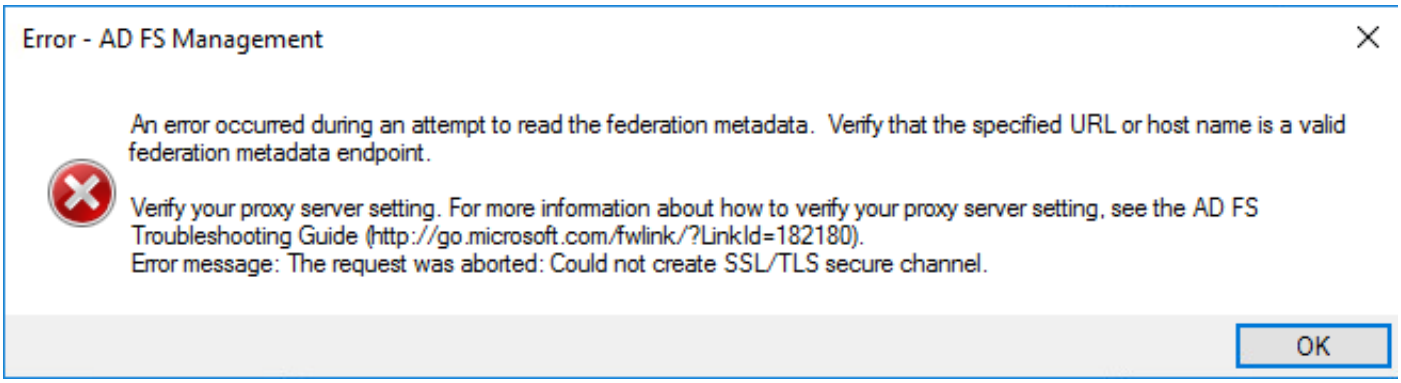
3. Select **Apply.**



ADFS_RelyingPartyTrust.png

Troubleshooting Errors

If you receive the error, "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" when testing the URL, this typically indicates that a registry change is required to set your .NET Framework version to use strong crypto and support TLS 1.2.



ADFSmetadata_TLS_error.png

Full details on these changes are published by Microsoft in the .Net Framework section of the Microsoft

documentation.

Typically, though, this requires the creation of this key, then closing and re-opening the ADFS Management console:

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

Limitation: Org-Specific EntityID Feature

If using the Umbrella SAML **Org-Specific EntityID feature**, then you must not use the URL-based metadata update mechanism. Org-Specific Entity ID only applies if you have multiple Umbrella orgs linked to the same Identity Provider. In this scenario you must manually add the certificate to each IDP configuration.

Manual Certificate Import (Alternative)

If your IdP does not support URL-Based updates you must manually import the new Umbrella request signing certificate each year to your Identity Provider.

- The certificate is provided in our Announcements portal each year shortly before the expiry date. Subscribe to the portal for notifications
- Add the new certificate to the list of Service Provider / Relying Party certificates in your IdP.
    - **DO NOT** delete any current certificates. Umbrella continues signing with the old certificate until the time of expiry.
- If your IdP does not contain have the capability to import a Service Provider/Relying party certificate this is a strong indication that it does not validate SAML requests, and no further action is required. Contact your IdP vendor to confirm.

If you encounter a "UPN is not configured" error after importing the new certificate this indicates an error has been made. Consult this article for troubleshooting: SWG SAML - UPN Not Configured Error