Troubleshoot UPN Not Configured Error after Umbrella Certificate Renewal in SWG SAML

Contents

Introduction

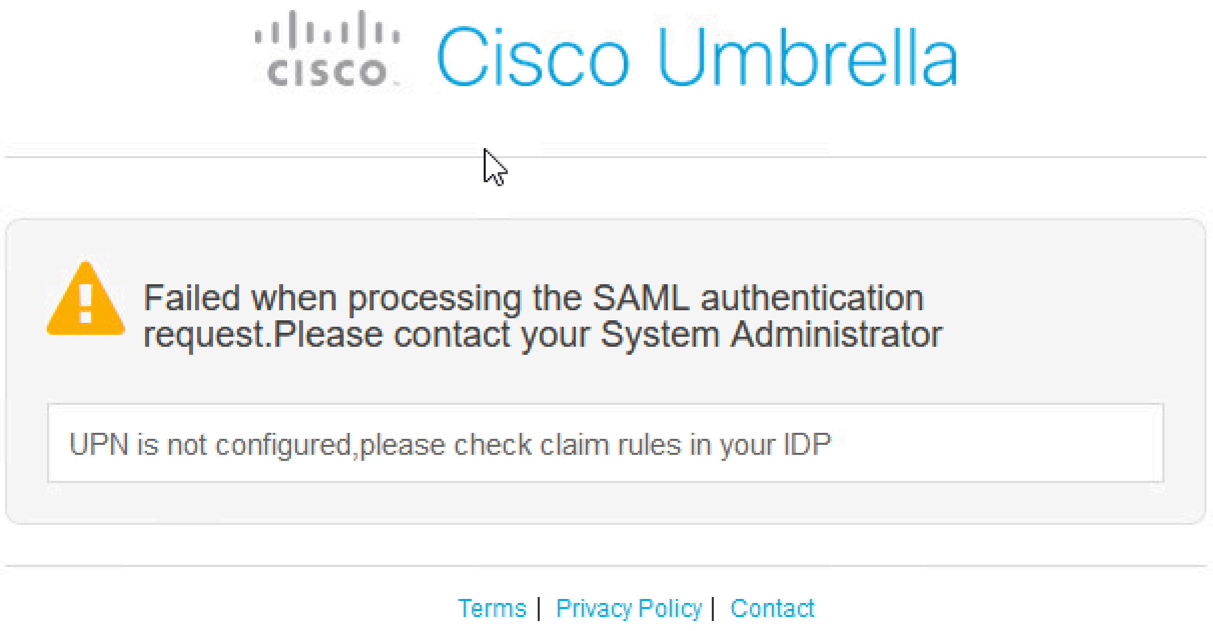
This document describes how to resolve a "UPN not configured" error after renewing the Umbrella SAML signing certificate.

Overview

"UPN not configured" is a generic error that can occur for a number of reasons. One potential cause is related to the expiration of the Umbrella SAML signing certificate which is renewed on an annual basis. For the latest details on certificate expiration, please read our Announcements portal.

If the Umbrella certificate expires and you have not taken action then users are be blocked from internet access with these potential errors:

- Umbrella-branded “UPN Not Configured” error when browsing the web through SWG
- Some other error presented by your Identity Provider


Failed when processing the SAML authentication request.Please contact your System Administrator

UPN is not configured,please check claim rules in your IDP

This article discusses 2 different scenarios that cause the error:

- **Scenario 1** - Error after importing new Umbrella Certificate
- **Scenario 2** - Error after Umbrella Certificate Expiry

Impact

New user logons for SWG fails, blocking internet access. This does not necessarily apply to all users but are triggered when:

- A user's session expires due to our re-authentication setting (for example, daily)
- A new user logs on
- A user clears the browser cache or uses a new browser.

Scenario 1 - Error after importing new Umbrella Certificate

If the error occurs directly after making a change (for example, in preparation for Umbrella's certificate renewal) then it is likely that a mistake has been made with the certificate import.

Ensure both Current & New Umbrella certificates are imported

In preparation for certificate renewal Umbrella makes a new certificate available, but the new certificate is not used for signing until expiry time. Therefore your IdP configuration must have two certificates listed in the Service Provider / Relying Party configuration. Reconfigure from metadata to resolve this.

- **Current Certificate** - With an upcoming expiry date
- **Future Certificate** - Which is valid for the next year.

Ensure the Attribute Claims map is correct

If you have reconfigured the Service Provider / Relying party, you need to make additional configuration changes to ensure the IdP is sending the attributes we need to validate the SAML response. This is common with Microsoft ADFS where our Claims map needs to be recreated.

Scenario 2 - Error after Umbrella Certificate Expiry

If the error occurs after Umbrella certificate expired and no changes have been made to the IdP.

Ensure the new certificate has been imported to the Identity Provider

To resolve the problem **Manually import** the new certificate into your identity provider. When our certificate is approaching renewal, the new certificate is made available in our Announcements portal.

(RECOMMENDED) Configure automatic metadata updates

Umbrella now provides a fixed metadata URL which can be used for seamless metadata updates. We recommend to configure this method to prevent manual action during the next certificate rollover.

Ensure the Certificate Revocation List (CRL) server addresses are accessible to the Identity Provider

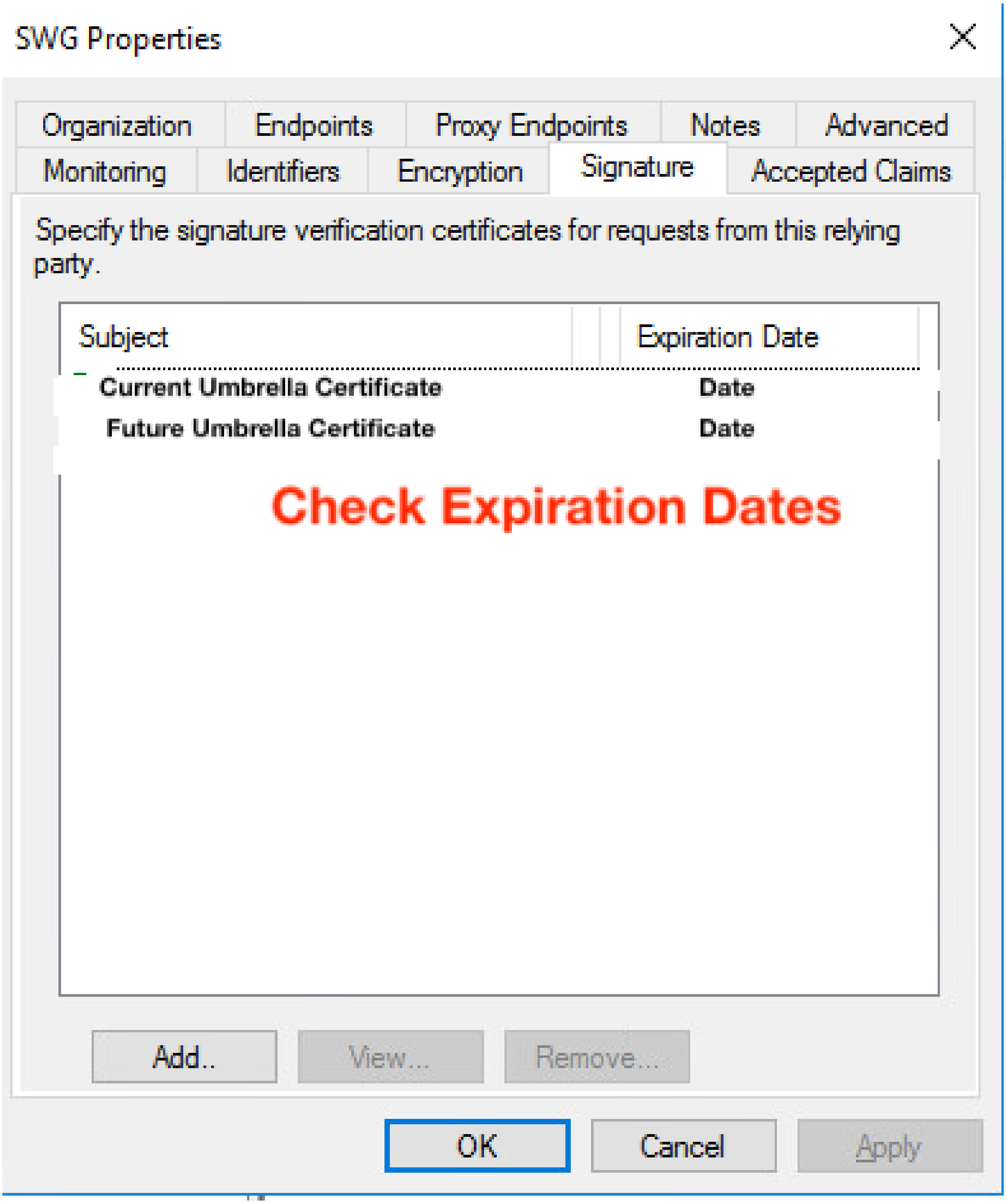
Umbrella now use a different Certificate Authority so ensure these CRL/OCSP addresses are available to the IdP server:

- http://validation.identrust.com
- http://commercial.ocsp.identrust.com

Microsoft ADFS - Manual Certificate Import Example

Microsoft ADFS is a popular IdP which is known to validate request signatures. The certificate can be updated as follows:

- Open **AD FS** management
- Expand **Relying Party Trusts** and locate the RP for Umbrella SWG
- Right-Click on the **Relying Party** in ADFS and select **Properties**
- Upload the new certificate on the **Signing** tab



Specify the signature verification certificates for requests from this relying party.

Subject	Expiration Date
Current Umbrella Certificate	Date
Future Umbrella Certificate	Date

Check Expiration Dates

When approaching the certificate expiration date the metadata provided by Cisco includes multiple certificates to prepare for seamless rollover. **Do not delete the current certificate whilst it is still valid.** Cisco continues signing with the current certificate up until the expiration date/time.