SWG SAMLでのUmbrella証明書更新後の「UPN Not Configured」エラーのトラブルシューティング

内容

はじめに

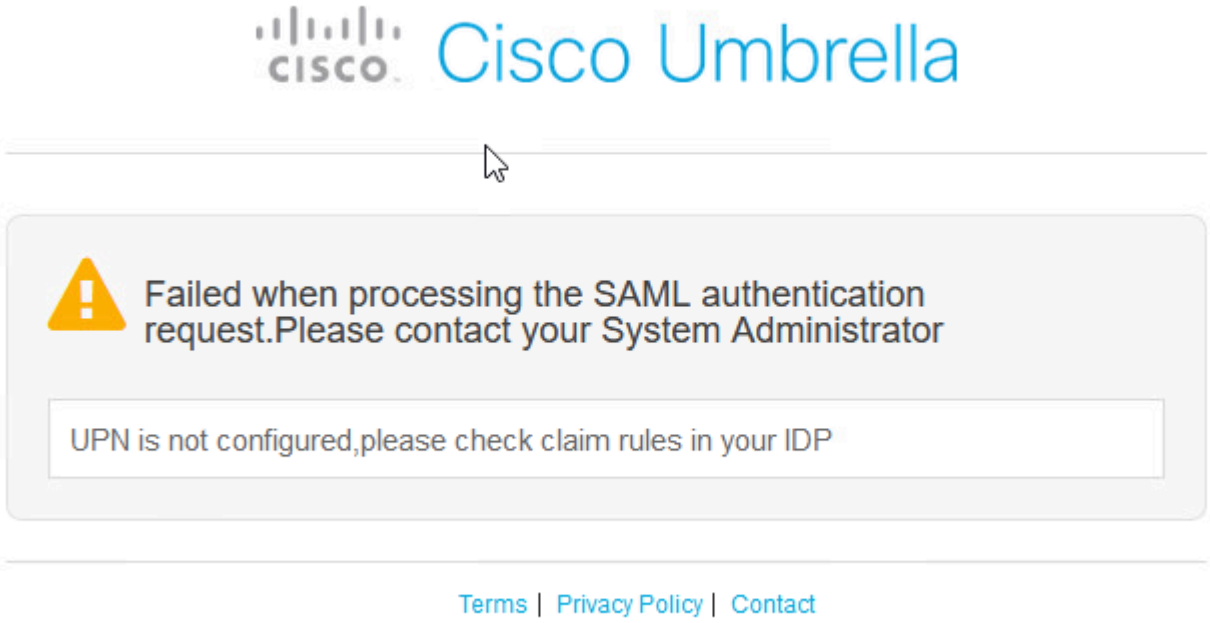
このドキュメントでは、Umbrella SAML署名証明書の更新後に「UPN not configured」エラーを解決する方法について説明します。

概要

「UPN not configured」は、さまざまな理由で発生する可能性のある一般的なエラーです。考えられる原因の1つは、Umbrella SAML署名証明書の有効期限が毎年更新されることです。 証明書の有効期限に関する最新情報については、お知らせポータルをご覧ください。

Umbrella証明書の有効期限が切れてアクションを実行していない場合、ユーザは次のエラーによってインターネットアクセスからブロックされます。

- SWG経由でWebをブラウズする際の包括ブランドの「UPN Not Configured」エラー
- IDプロバイダーから他のエラーが提示されました



この記事では、エラーを引き起こす2つの異なるシナリオについて説明します。

- シナリオ1：新しいUmbrella証明書のインポート後のエラー
- シナリオ2:Umbrella証明書の有効期限後のエラー

影響

SWGの新しいユーザログオンが失敗し、インターネットアクセスがブロックされる。これは必ずしもすべてのユーザに適用されるわけではありませんが、次の場合にトリガーされます。

- 再認証設定（毎日など）により、ユーザのセッションが期限切れになる
- 新しいユーザーがログオンする
- ユーザがブラウザのキャッシュをクリアするか、新しいブラウザを使用する。

シナリオ1：新しいUmbrella証明書のインポート後のエラー

変更を行った直後にエラーが発生する場合（たとえば、Umbrellaの証明書の更新に備えて）、証明書のインポートで誤りが発生した可能性があります。

現在および新しいUmbrella証明書がインポートされていることを確認します。

証明書の更新に備えて、Umbrellaは新しい証明書を使用可能にしますが、有効期限が切れるまで新しい証明書は署名に使用されません。 したがって、IdP設定では、サービスプロバイダー/証明書利用者の設定に2つの証明書がリストされている必要があります。 これを解決するには、metadataから再設定します。

- 現在の証明書 – 有効期限が近づいています

- 将来の証明書：これは来年まで有効です。

属性要求マップが正しいことを確認します。

サービスプロバイダー/証明書利用者を再設定した場合、追加の設定変更を行い、IdPがSAML応答の検証に必要な属性を送信していることを確認する必要があります。これは、要求マップを再作成する必要があるMicrosoft ADFSでは共通です。

シナリオ2:Umbrella証明書の有効期限後のエラー

Umbrella証明書の期限が切れた後にエラーが発生し、IdPが変更されていない場合。

新しい証明書がIDプロバイダーにインポートされていることを確認します

問題を解決するには、新しい証明書をIDプロバイダーに手動でインポートします。 証明書の更新が近づくと、新しい証明書がお知らせポータルで利用可能になります。

（推奨）メタデータの自動更新を構成する

Umbrellaは、メタデータのシームレスな更新に使用できる固定のメタデータURLを提供するようになりました。 次回の証明書ロールオーバー時に手動アクションが実行されないように、この方法を設定することをお勧めします。

IDプロバイダーが証明書失効リスト(CRL)サーバーアドレスにアクセスできることを確認してください

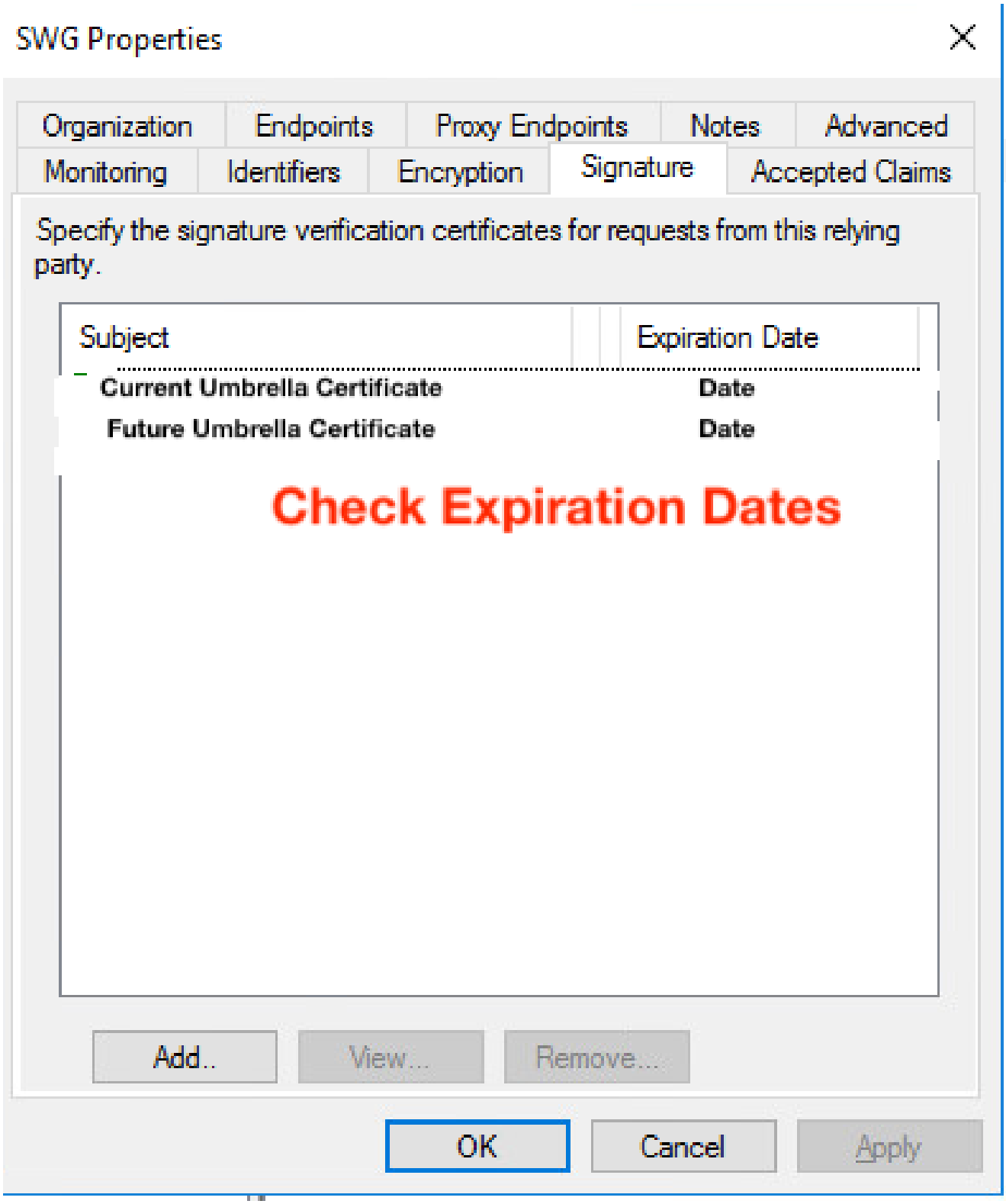
Umbrellaは別の認証局(CA)を使用しているため、次のCRL/OCSPアドレスがIdPサーバで使用できることを確認します。

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

Microsoft ADFS – 証明書の手動インポートの例

Microsoft ADFSは、要求署名を検証することが知られている一般的なIdPです。 証明書は次のように更新できます。

- AD FS管理を開きます
- Relying Party Trustsを展開し、Umbrella SWGのRPを見つけます
- ADFSで証明書利用者を右クリックし、Propertiesを選択します。
- Signingタブで新しい証明書をアップロードします



証明書の有効期限が近づくと、シスコが提供するメタデータに複数の証明書が含まれ、シームレスなロールオーバーの準備が行われます。現在の証明書がまだ有効である間は、削除しないでください。シスコは、有効期限が切れる日時まで、現在の証明書を使用して署名を続けます。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。