Fehler "UPN nicht konfiguriert" nach Verlängerung des Umbrella-Zertifikats in SWG SAML beheben

Inhalt

Einleitung

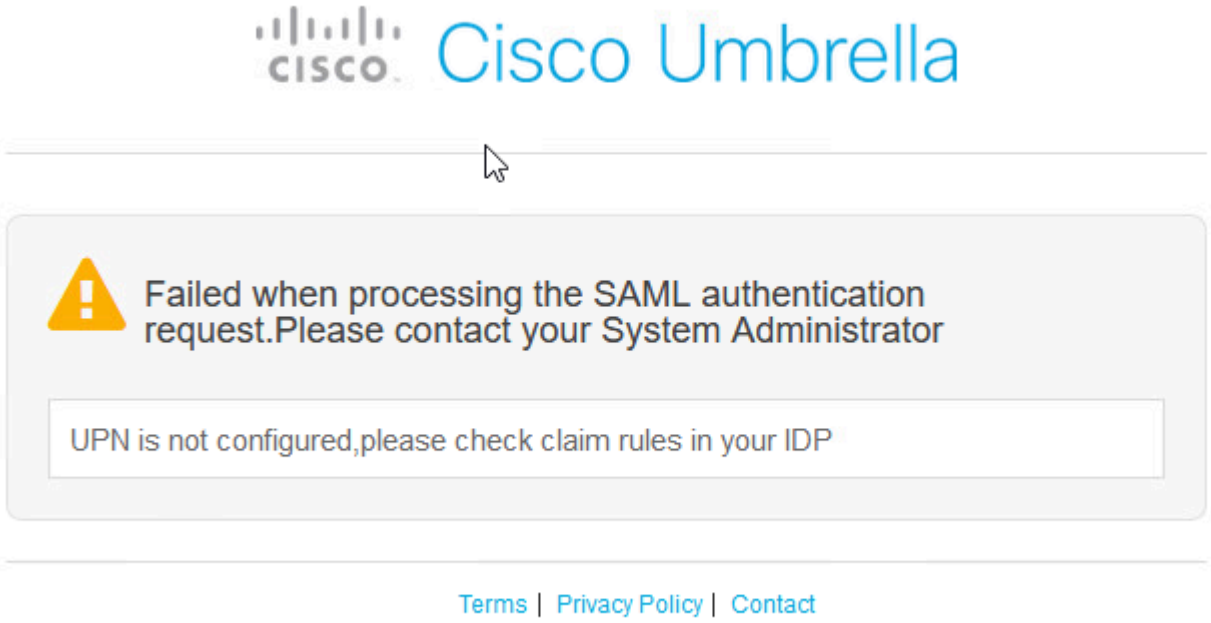
In diesem Dokument wird beschrieben, wie Sie den Fehler "UPN not configured" (UPN nicht konfiguriert) beheben, nachdem Sie das Umbrella SAML-Signaturzertifikat verlängert haben.

Überblick

"UPN nicht konfiguriert" ist ein allgemeiner Fehler, der aus verschiedenen Gründen auftreten kann. Eine mögliche Ursache ist der Ablauf des Umbrella SAML Signaturzertifikats, das jährlich erneuert wird. Aktuelle Informationen zum Ablauf des Zertifikats finden Sie in unserem Ankündigungsportal.

Wenn das Umbrella-Zertifikat abläuft und Sie keine Maßnahmen ergriffen haben, werden die Benutzer mit folgenden möglichen Fehlern vom Internetzugriff blockiert:

- Umbrella-Branded "UPN Not Configured"-Fehler beim Surfen im Internet durch die SWG
- Ein anderer Fehler, der von Ihrem Identitätsanbieter ausgegeben wird.



In diesem Artikel werden zwei verschiedene Szenarien erläutert, die den Fehler verursachen:

- Szenario 1 - Fehler nach dem Importieren eines neuen Umbrella-Zertifikats
- Szenario 2 - Fehler nach Ablauf des Umbrella-Zertifikats

Auswirkungen

Neue Benutzeranmeldungen für die SWG schlagen fehl und blockieren den Internetzugriff. Dies gilt nicht unbedingt für alle Benutzer, wird jedoch ausgelöst, wenn:

- Die Sitzung eines Benutzers läuft aufgrund unserer Einstellungen zur erneuten Authentifizierung ab (z. B. täglich).
- Ein neuer Benutzer meldet sich an
- Ein Benutzer löscht den Browser-Cache oder verwendet einen neuen Browser.

Szenario 1 - Fehler nach dem Importieren eines neuen Umbrella-Zertifikats

Tritt der Fehler direkt nach einer Änderung auf (z. B. in Vorbereitung auf die Erneuerung des Umbrella-Zertifikats), ist es wahrscheinlich, dass ein Fehler beim Importieren des Zertifikats aufgetreten ist.

Stellen Sie sicher, dass aktuelle und neue Umbrella-Zertifikate importiert werden.

In Vorbereitung auf die Erneuerung des Zertifikats stellt Umbrella ein neues Zertifikat zur Verfügung. Das neue Zertifikat wird jedoch erst nach Ablauf der Gültigkeit zur Signatur

verwendet. Aus diesem Grund muss Ihre IdP-Konfiguration über zwei Zertifikate verfügen, die in der Konfiguration des Service Providers/der vertrauenden Partei aufgeführt sind. Neukonfiguration aus Metadaten zur Lösung dieses Problems.

- Aktuelles Zertifikat - mit bevorstehendem Ablaufdatum
- Zukünftiges Zertifikat: Dieses Zertifikat ist für das nächste Jahr gültig.

Stellen Sie sicher, dass die Zuordnung für Attributansprüche korrekt ist.

Wenn Sie den Service Provider/die vertrauende Seite neu konfiguriert haben, müssen Sie weitere Konfigurationsänderungen vornehmen, um sicherzustellen, dass die IdP die Attribute sendet, die wir zur Validierung der SAML-Antwort benötigen. Dies ist bei Microsoft ADFS üblich, bei dem die Schadenszuordnung neu erstellt werden muss.

Szenario 2 - Fehler nach Ablauf des Umbrella-Zertifikats

Wenn der Fehler auftritt, nachdem das Umbrella-Zertifikat abgelaufen ist und keine Änderungen am IdP vorgenommen wurden.

Stellen Sie sicher, dass das neue Zertifikat in den Identitätsanbieter importiert wurde.

Um das Problem zu beheben, importieren Sie das neue Zertifikat manuell in Ihren Identitätsanbieter. Wenn die Erneuerung unseres Zertifikats bevorsteht, wird das neue Zertifikat in unserem Ankündigungsportal zur Verfügung gestellt.

(EMPFOHLEN) Automatische Metadatenaktualisierungen konfigurieren

Umbrella stellt nun eine feste Metadaten-URL bereit, die für nahtlose Metadaten-Updates verwendet werden kann. Wir empfehlen, diese Methode zu konfigurieren, um manuelle Aktionen beim nächsten Zertifikatrollover zu verhindern.

Stellen Sie sicher, dass der Identitätsanbieter auf die CRL-Serveradressen (Certificate Revocation List) zugreifen kann.

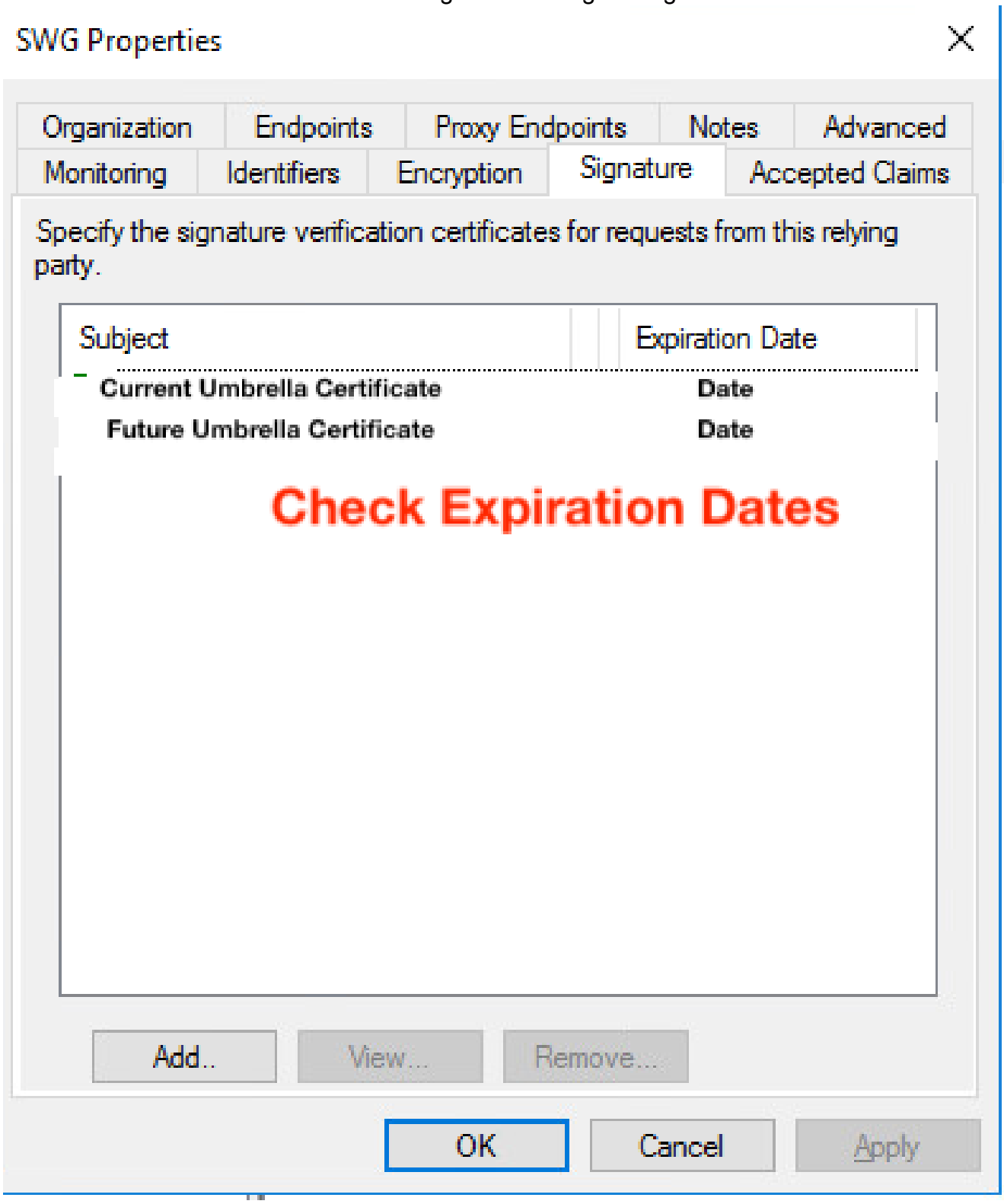
Umbrella verwendet jetzt eine andere Zertifizierungsstelle. Stellen Sie daher sicher, dass diese CRL-/OCSP-Adressen für den IdP-Server verfügbar sind:

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

Microsoft ADFS - Beispiel für manuellen Zertifikatimport

Microsoft ADFS ist eine beliebte IDp, die bekanntermaßen Anforderungssignaturen validiert. Das Zertifikat kann wie folgt aktualisiert werden:

- Offenes AD FS-Management
- Erweitern Sie Vertrauenswürdigkeit der vertrauenden Partei, und suchen Sie den RP für die Umbrella SWG.
- Klicken Sie mit der rechten Maustaste auf die vertrauende Partei in ADFS, und wählen Sie Eigenschaften aus
- Laden Sie das neue Zertifikat auf der Registerkarte Signierung hoch.



Wenn das Ablaufdatum des Zertifikats näher rückt, enthalten die von Cisco bereitgestellten Metadaten mehrere Zertifikate, um ein nahtloses Rollover vorzubereiten. Löschen Sie das aktuelle

Zertifikat nicht, solange es noch gültig ist. Cisco signiert das aktuelle Zertifikat bis zum Ablaufdatum/-uhrzeit weiter.

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.