# Integration von Umbrella mit NetIQ für SSO mit SAML

## Inhalt



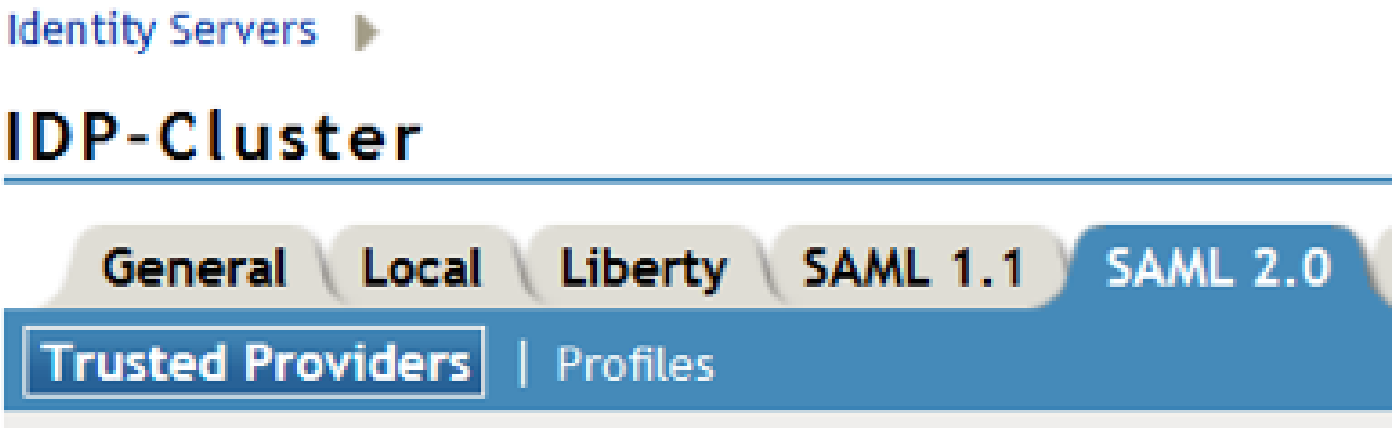
## Einleitung

In diesem Dokument wird die Integration von Cisco Umbrella in NetIQ für Single Sign-on (SSO) mit SAML beschrieben.

## Überblick über die Umbrella SAML Integration für NetIQ

Die Konfiguration von SAML mit NetIQ unterscheidet sich von unseren anderen SAML-Integrationen, da es sich nicht um einen Ein- oder Zwei-Klick-Prozess im Assistenten handelt, sondern Änderungen in NetIQ erforderlich sind, um ordnungsgemäß zu funktionieren. In diesem Dokument werden die Änderungen beschrieben, die Sie vornehmen müssen, damit SAML und NetIQ zusammenarbeiten können. Diese Informationen werden ohne Mängelgewähr bereitgestellt und in Zusammenarbeit mit bestehenden Kunden entwickelt. Der verfügbare Support für diese Lösung ist begrenzt, und der Cisco Umbrella Support ist nicht in der Lage, über die hier beschriebenen allgemeinen Bedingungen hinauszugehen.

Weitere Informationen zur SAML-Integration mit Umbrella finden Sie in unserem Bericht hier: Erste Schritte: Single Sign-On.

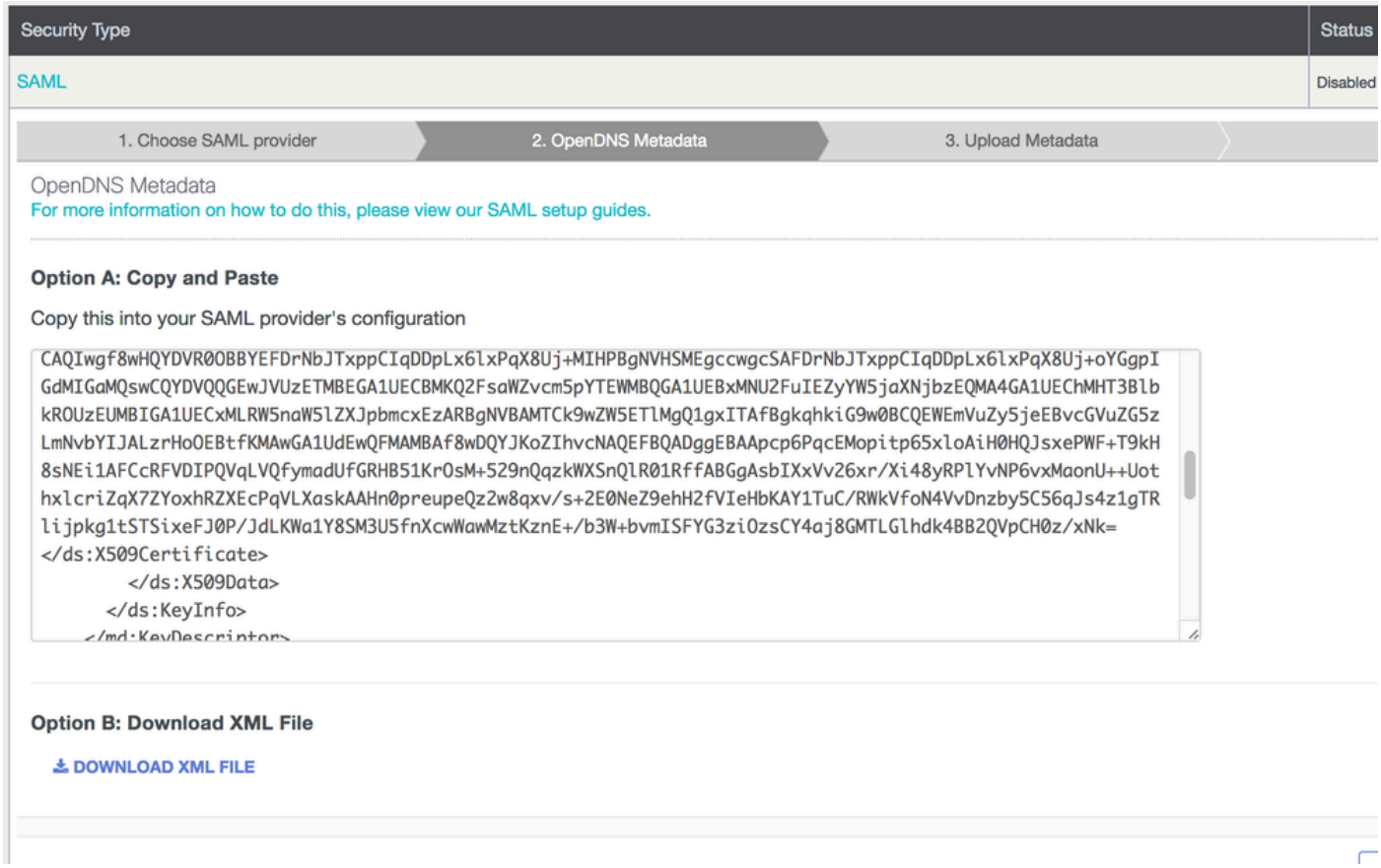



115000348788

# Voraussetzungen

Die Schritte zur ersten Einrichtung von SAML finden Sie hier: Identitätsintegrationen: Voraussetzungen. Wenn Sie die Schritte zum Herunterladen der Cisco Umbrella-Metadaten ausgeführt haben, können Sie die folgenden NetIQ-spezifischen Anweisungen zum Abschließen der Konfiguration verwenden.

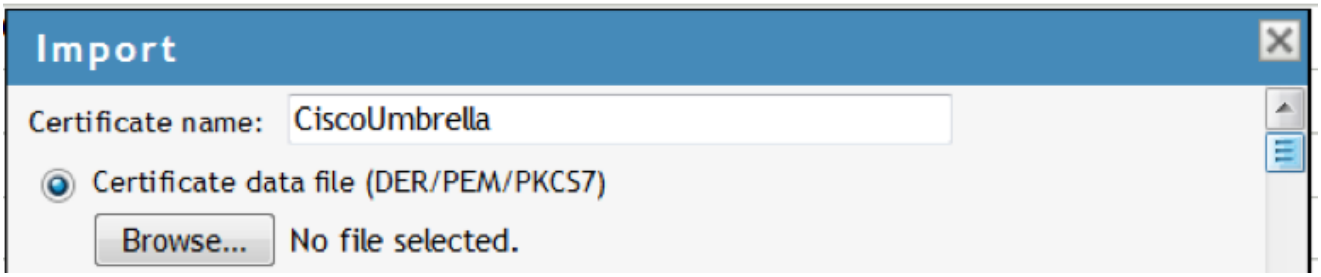
Die Metadaten finden Sie im Cisco Umbrella SAML Setup Wizard (Einstellungen > Authentifizierung > SAML).




115001332488

# Metadaten und Cisco Umbrella Certificate importieren

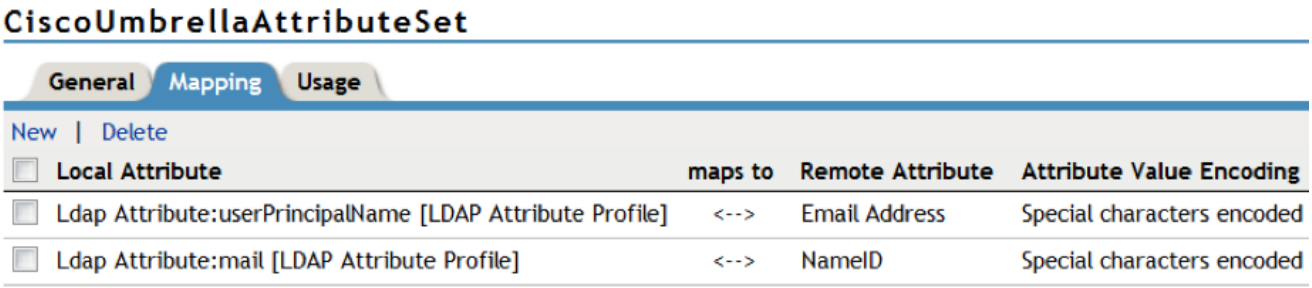
1. Öffnen Sie die Cisco Umbrella-Metadaten (heruntergeladen unter Voraussetzungen) in einem Texteditor, und extrahieren Sie das X509-Zertifikat. Das Zertifikat beginnt mit ds:X509Certificate und endet mit /ds:X509Certificate - nur von Anfang bis Ende kopieren.
2. Speichern Sie die neue Datei unter dem Namen CiscoUmbrella.cer.
3. Konvertieren Sie das x509-Zertifikat in PKCS7 / PEM. Die Methoden hierfür variieren, aber dieser Befehl führt den Trick aus: **openssl x509 -in CiscoUmbrella.cer -out CiscoUmbrella.pem -outform PEM**
4. Starten Sie in NetIQ NAM unter Trusted Roots (Vertrauenswürdige Roots).
5. Wählen Sie Neu > Durchsuchen und importieren Sie CiscoUmbrella.pem.




115000349367

## Attributgruppe erstellen

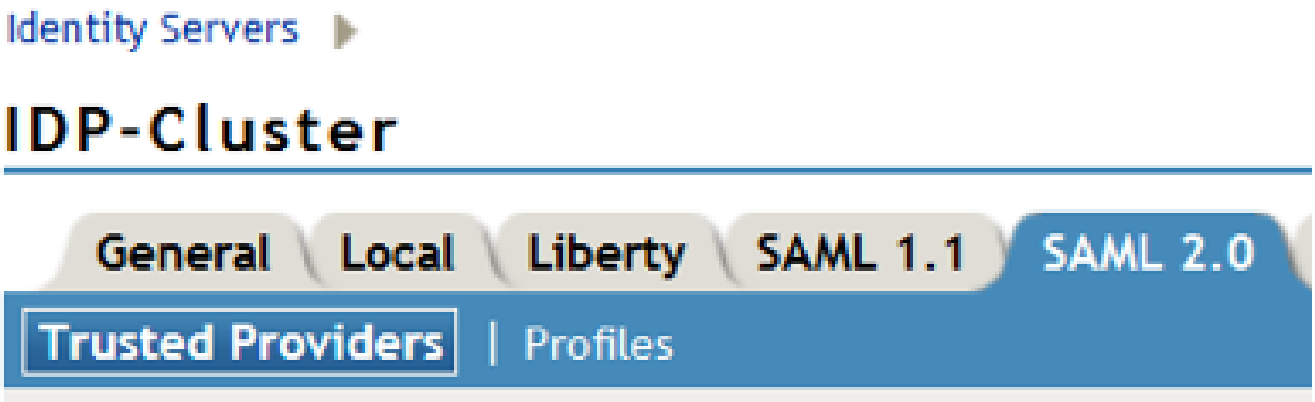
1. Gehen Sie zu Identity Servers > NetIQ NAM.
2. Klicken Sie auf Attributsätze.
3. Wählen Sie Neu aus, und ordnen Sie die LDAP-Attribute zu:



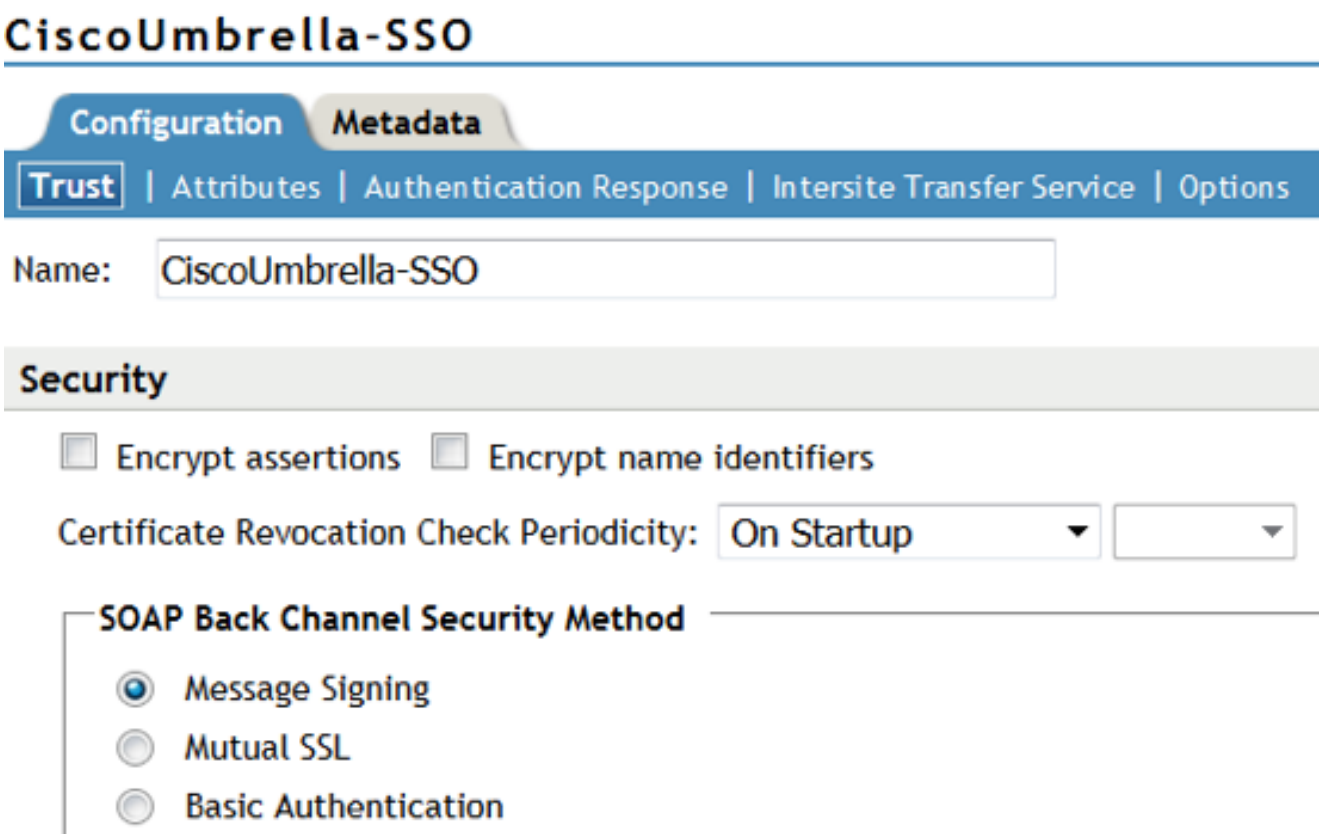

115000349567

## Erstellen eines neuen Vertrauensanbieters

1. Wechseln Sie zur Registerkarte IDP General (Allgemein), und wählen Sie SAML 2.0 aus.
2. Wählen Sie Neuen Vertrauenswürdigen Anbieter erstellen aus.

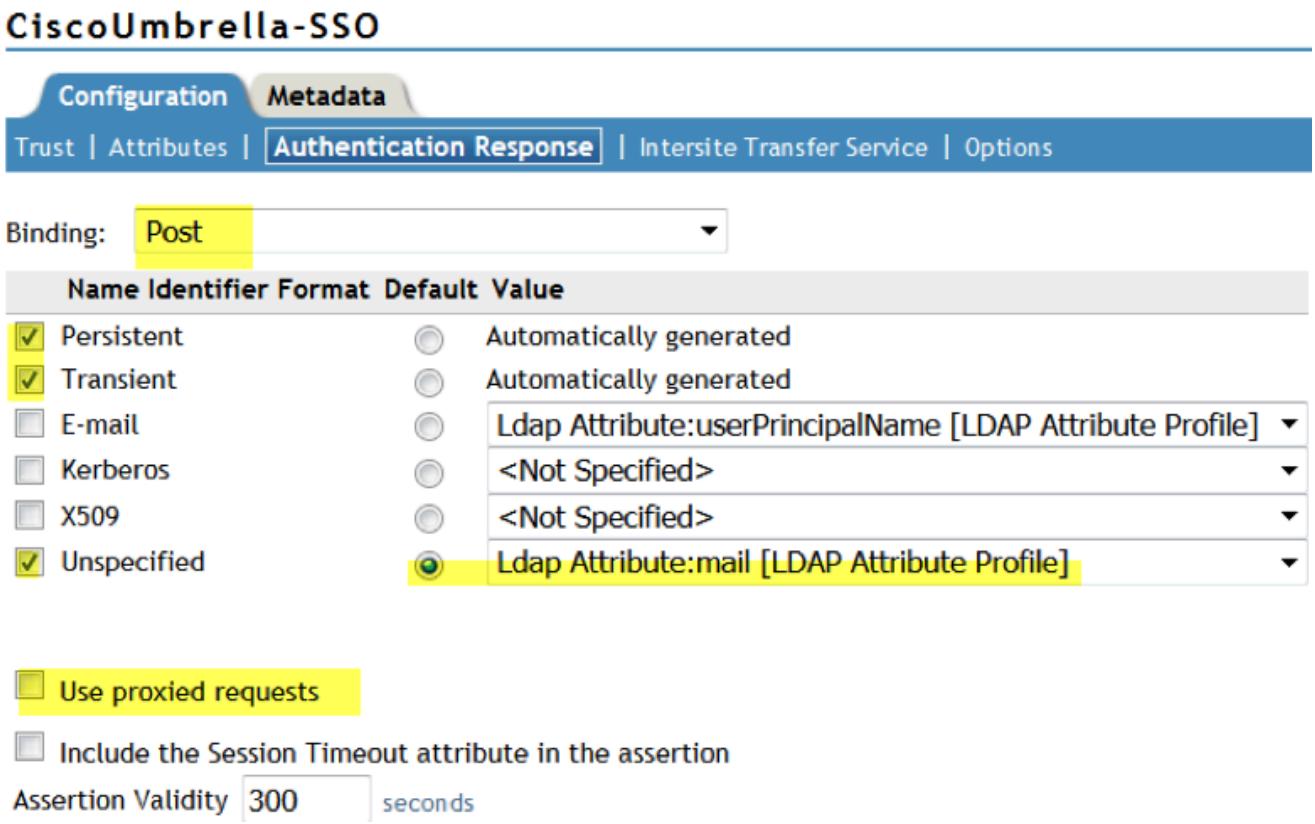



115000348788



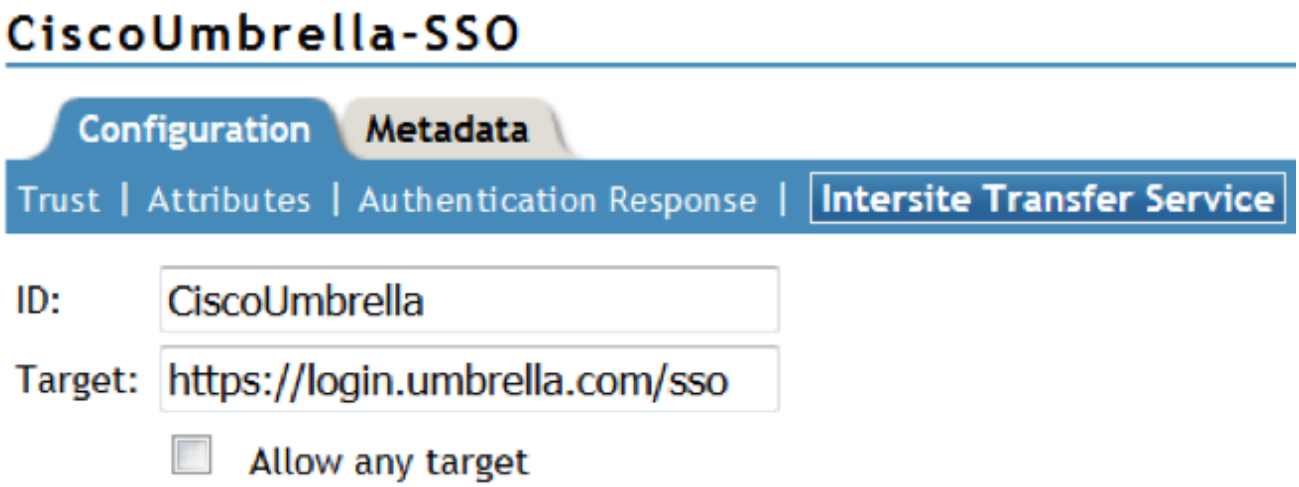

115000349827

3. Wählen Sie das soeben erstellte Attribut aus, und wählen Sie Mit Authentifizierung senden aus. Wählen Sie als Authentifizierungsantwort Post Binding, Persistent, Transient und Unspecified (Nicht angegeben).
4. LDAP-Attribut auswählen: mailen Sie [LDAP-Attributprofil] und geben Sie es als Standard an.



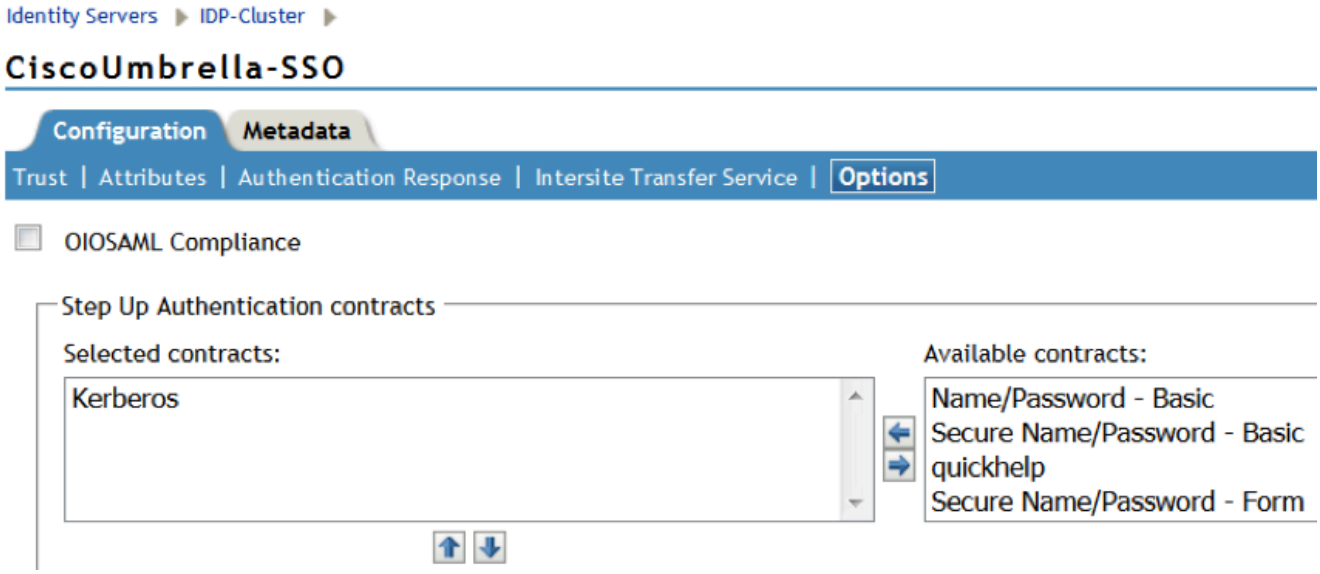
115000355688

5. Navigieren Sie zu Configuration > Intersite Transfer Service. Geben Sie ihm einen Namen wie Cisco Umbrella SAML, und fügen Sie die Cisco Umbrella SSO-Anmelde-URL als Ziel hinzu (https://login.umbrella.com/sso).



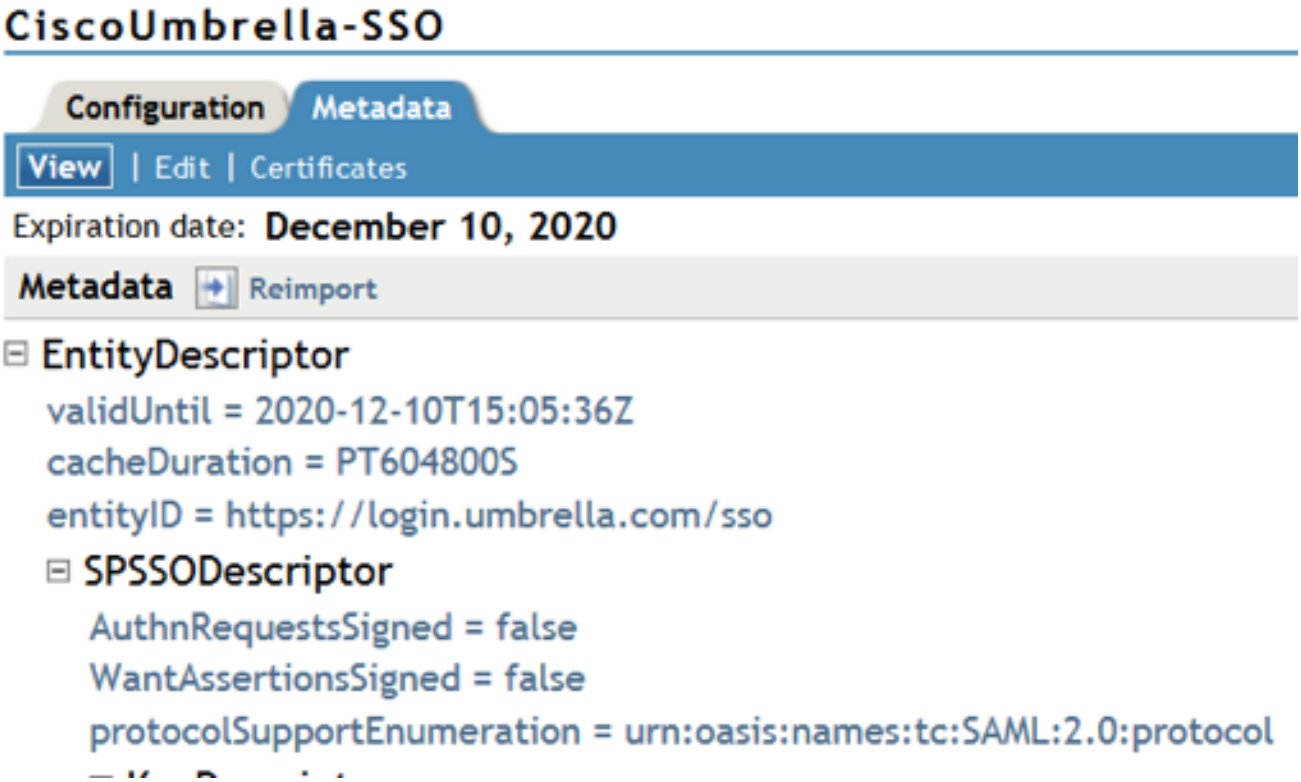

115000356827

6. Gehen Sie zu Konfiguration > Optionen, und wählen Sie Kerberos als Ausgewählte Verträge aus:



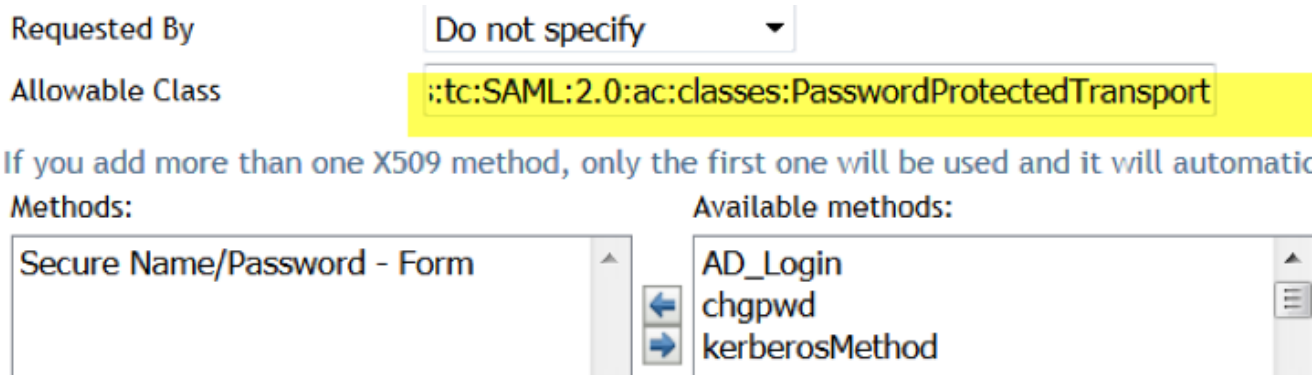

115000356068

7. Öffnen Sie die Cisco Umbrella-Metadatendatei. Aktualisieren Sie das Feld EntityDescription vaildUntil auf zukünftige Daten, z. B. 2020-12-10T20:50:59Z (wie im Screenshot gezeigt).
8. Gehen Sie zurück zu NetIQ > Metadaten, und importieren Sie die aktualisierte Metadatendatei.



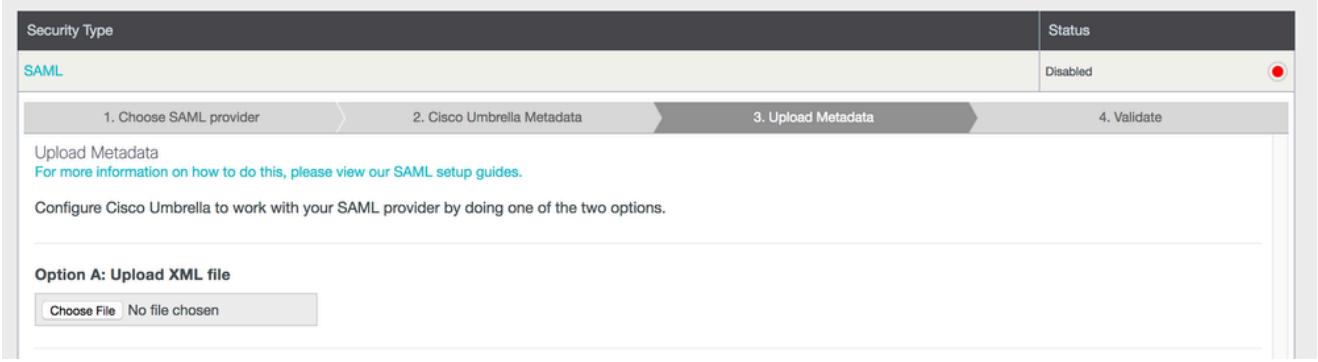

115000357147

9. Fügen Sie der Assertion eine Klasse hinzu. Die Cisco Umbrella Assertion erfordert die Klasse **urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport**
10. Gehen Sie zu Lokal > Verträge, wählen Sie Sicherer Name/Kennwort aus, und fügen Sie das Feld Zulässige Klasse hinzu. Fügen Sie dann die Klasse oben hinzu:




115000357247

11. Aktualisieren Sie Identity Services und Access Gateways, um sicherzustellen, dass sie gültig und auf dem neuesten Stand sind. Laden Sie dann die NetIQ-Metadaten herunter.
12. Verwenden Sie die heruntergeladenen Metadaten, um den Cisco Umbrella "Other" SAML-Assistenten auszuführen. In Schritt 3 werden Sie aufgefordert, die Metadaten hochzuladen:




115001186107

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.