UmbrellaとNetIQを統合してSAMLでSSOを実現

内容

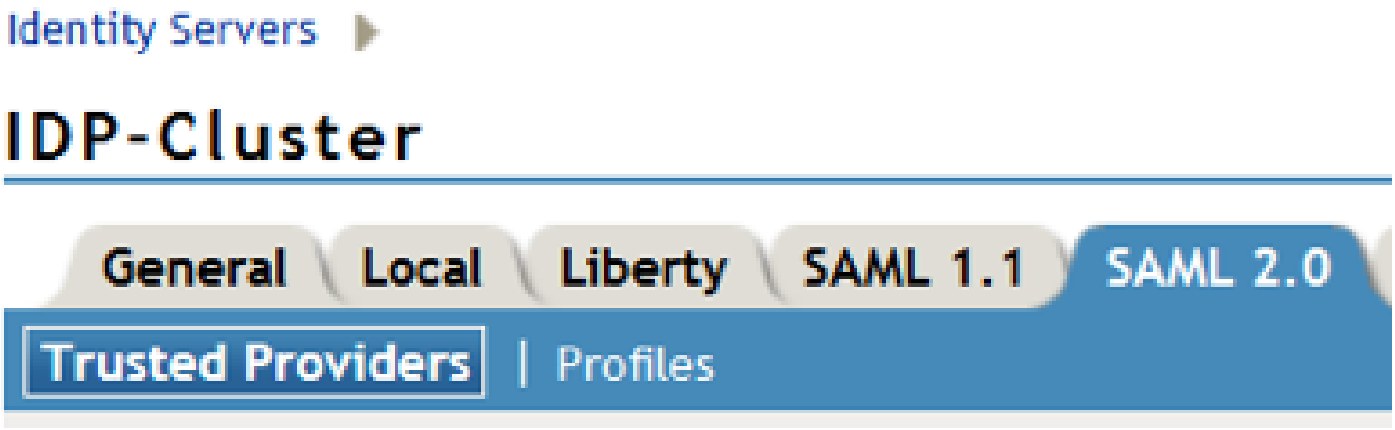
はじめに

このドキュメントでは、Cisco UmbrellaとNetIQ for Single Sign-on(SSO)をSAMLと統合する方法について説明します。

NetIQ向けUmbrella SAML統合の概要

NetIQによるSAMLの設定は、ウィザードでの1回または2回のクリックではなく、NetIQの変更が正しく動作する必要があるため、他のSAML統合とは異なります。このドキュメントでは、SAMLとNetIQを連携させるために必要な変更の詳細について説明します。そのため、この情報は「現状のまま」提供され、既存のお客様と共同で開発されました。このソリューションで利用可能なサポートは限られており、Cisco Umbrellaのサポートでは、ここで説明する一般的な概要を超えたサポートは提供できません。

SAML統合とUmbrellaの連携の詳細については、こちらのレビュー「シングルサインオンを開始する」を参照してください。



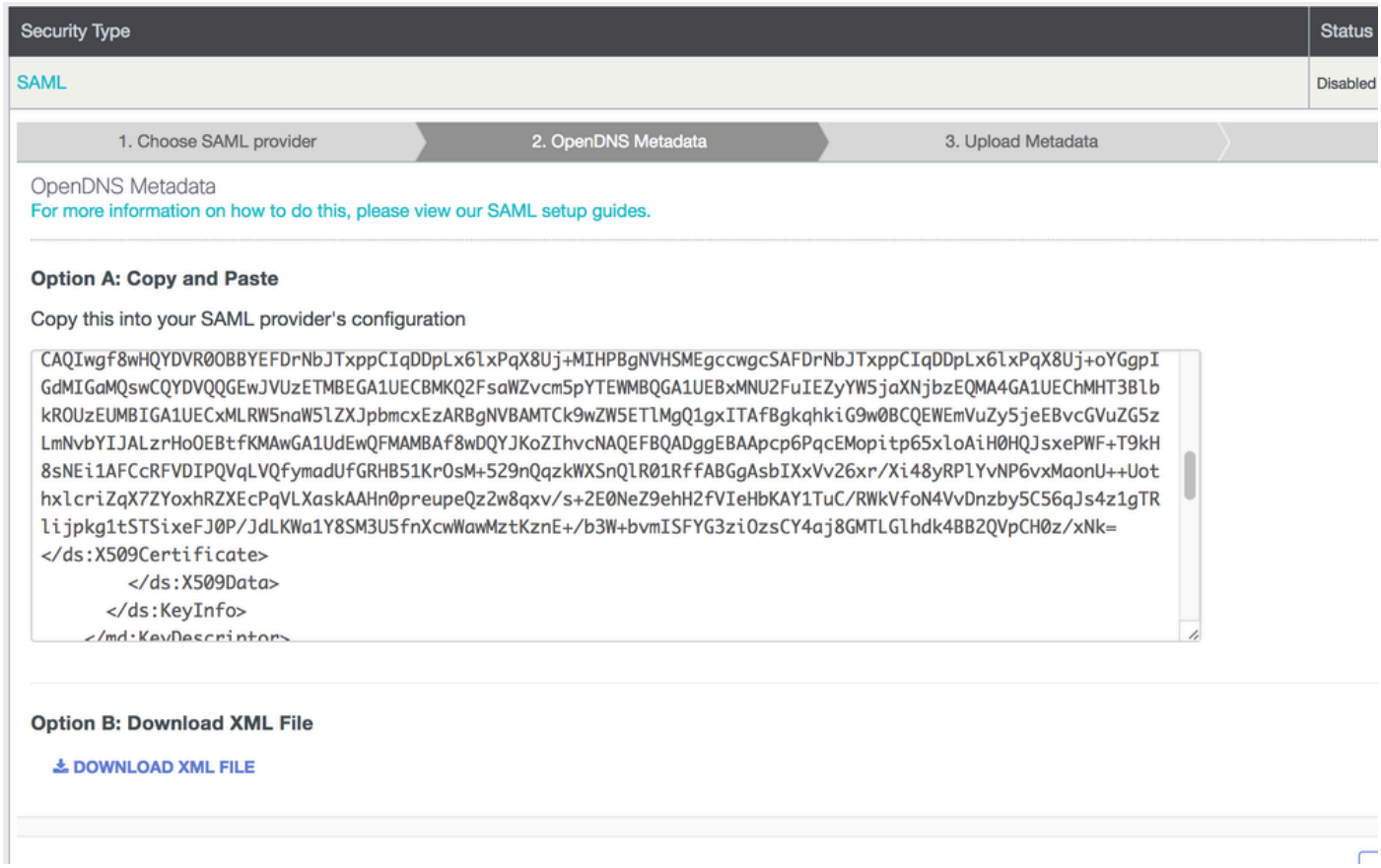
115000348788

前提条件

SAMLの初期設定の手順については、Identity Integrations: Prerequisitesを参照してください。

Cisco Umbrellaメタデータのダウンロードを含むこれらの手順を完了したら、次のNetIQ固有の手順を使用して設定を完了できます。

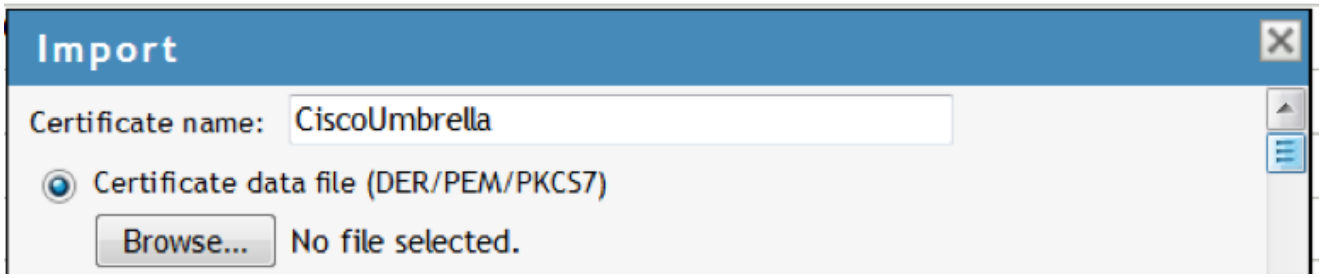
メタデータは、Cisco Umbrella SAMLセットアップウィザード(設定>認証> SAML)にあります。



115001332488

メタデータとCisco Umbrella証明書のインポート

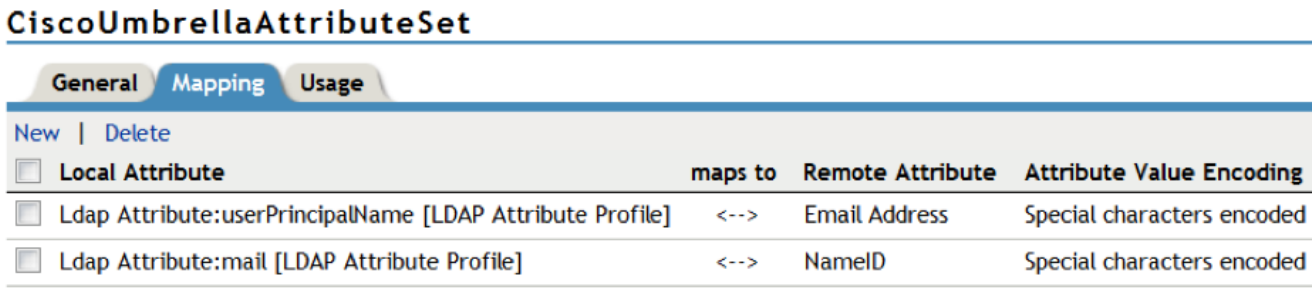
1. テキストエディタでCisco Umbrellaメタデータ（前提条件でダウンロード）を開き、X509証明書を抽出します。証明書はds:X509Certificateで始まり/ds:X509Certificateで終わります。最初から最後までコピーするだけです。
2. この新しいファイルをCiscoUmbrella.cerという名前で保存します。
3. x509証明書をPKCS7/PEMに変換します。これを行う方法はさまざまですが、このコマンドはテクニックを実行します。**openssl x509 -in CiscoUmbrella.cer -out CiscoUmbrella.pem -outform PEM**
4. NetIQで、Trusted Rootsの下でNAMを起動します。
5. New > Browseの順に選択し、CiscoUmbrella.pemをインポートします。



115000349367

属性グループの作成

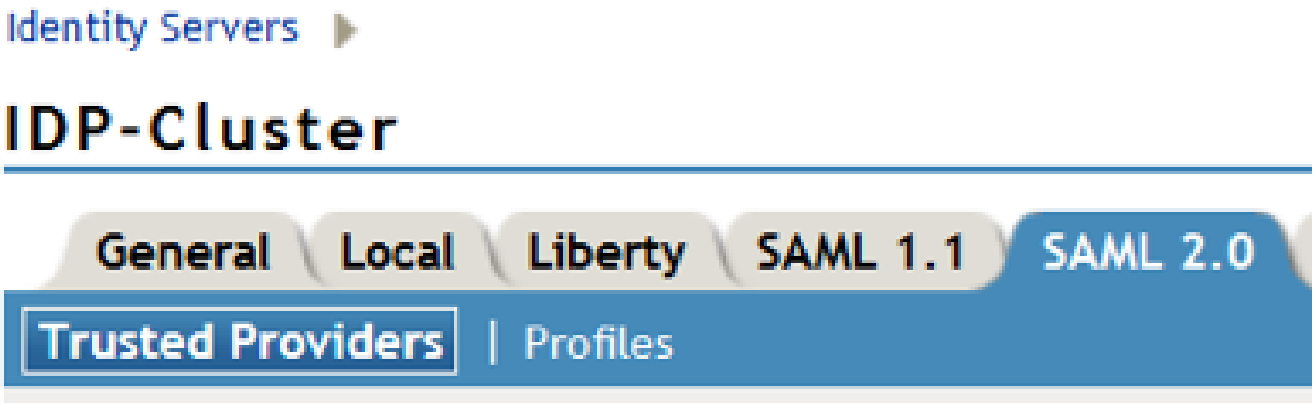
1. Identity Servers > NetIQ NAMの順に選択します。
2. Attribute Setsをクリックします。
3. Newを選択して、LDAP属性をマッピングします。



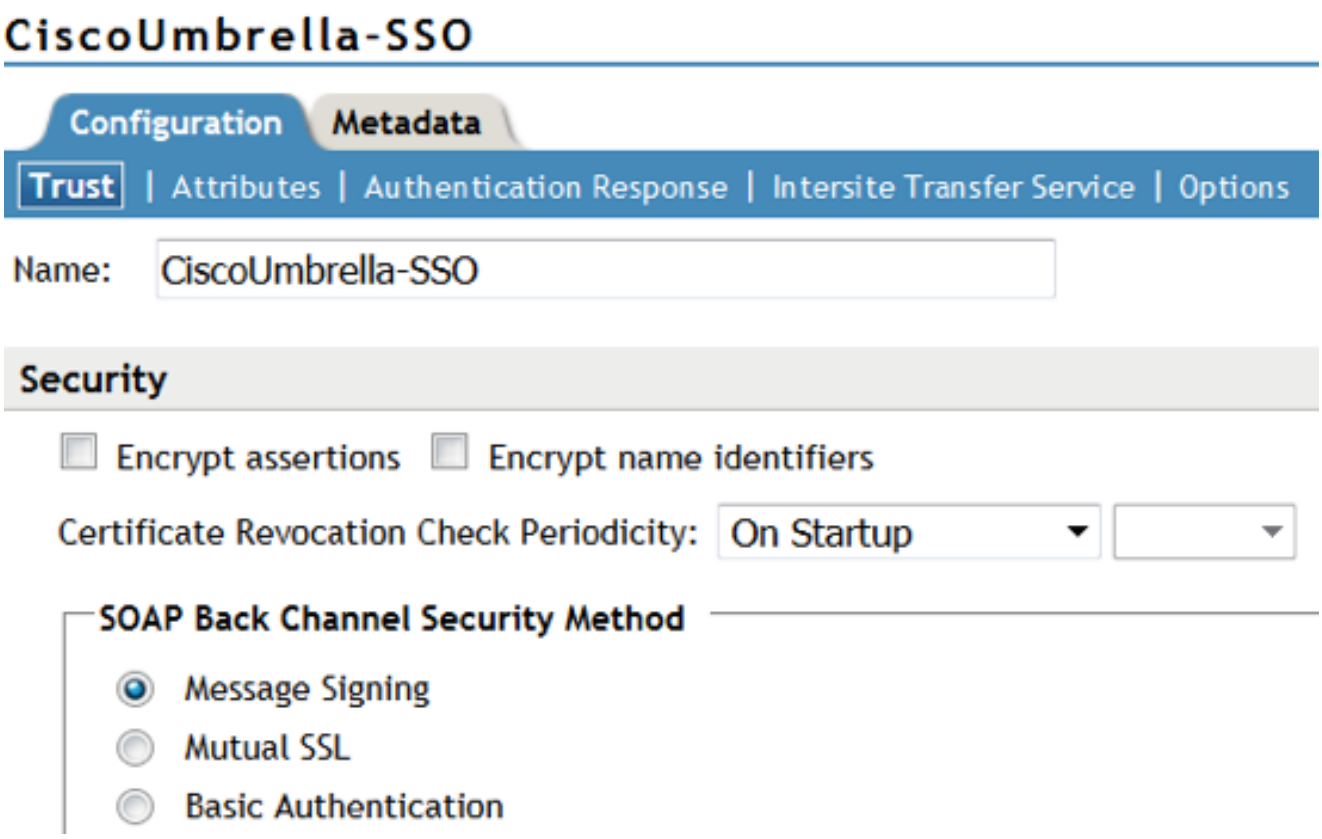
115000349567

新しい信頼プロバイダーの作成

1. IDP Generalタブに移動し、SAML 2.0を選択します。
2. Create New Trust Providerを選択します。

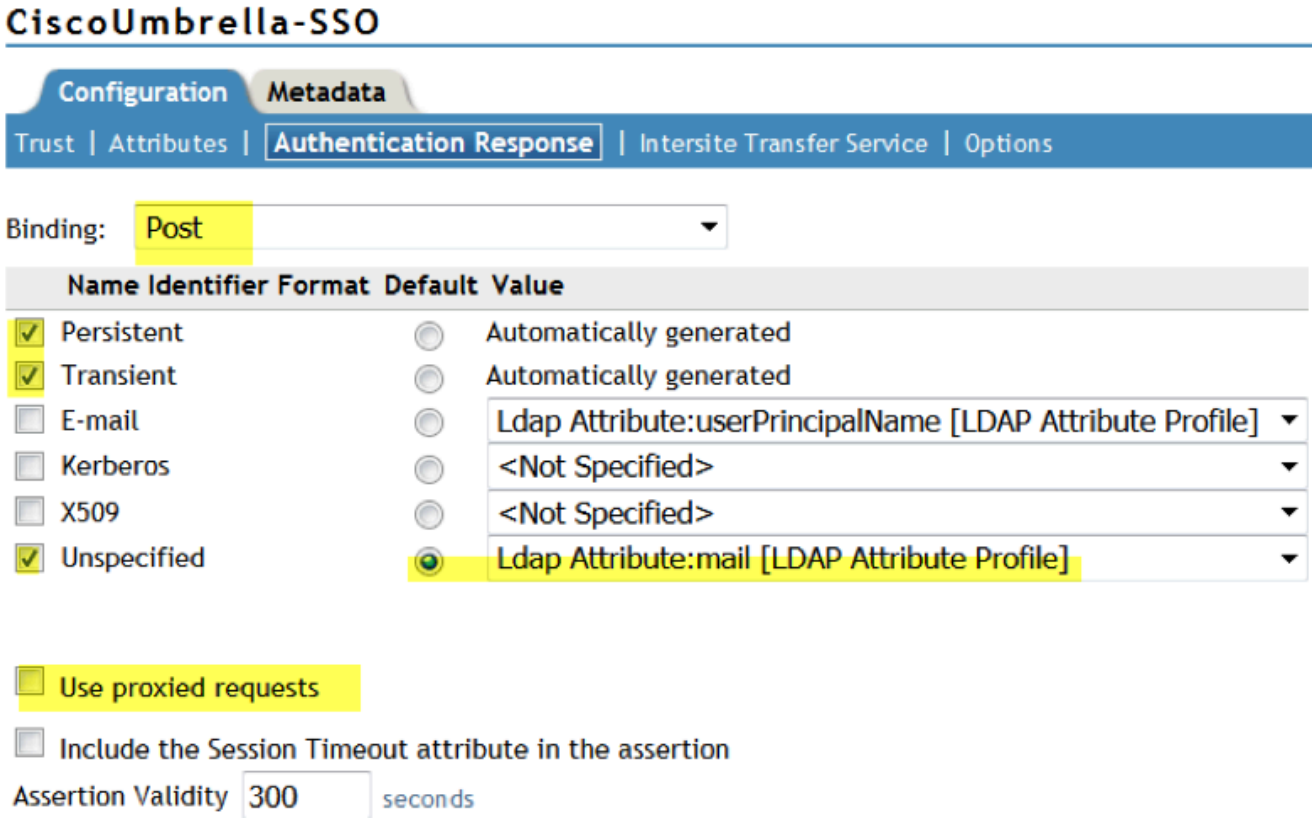


115000348788



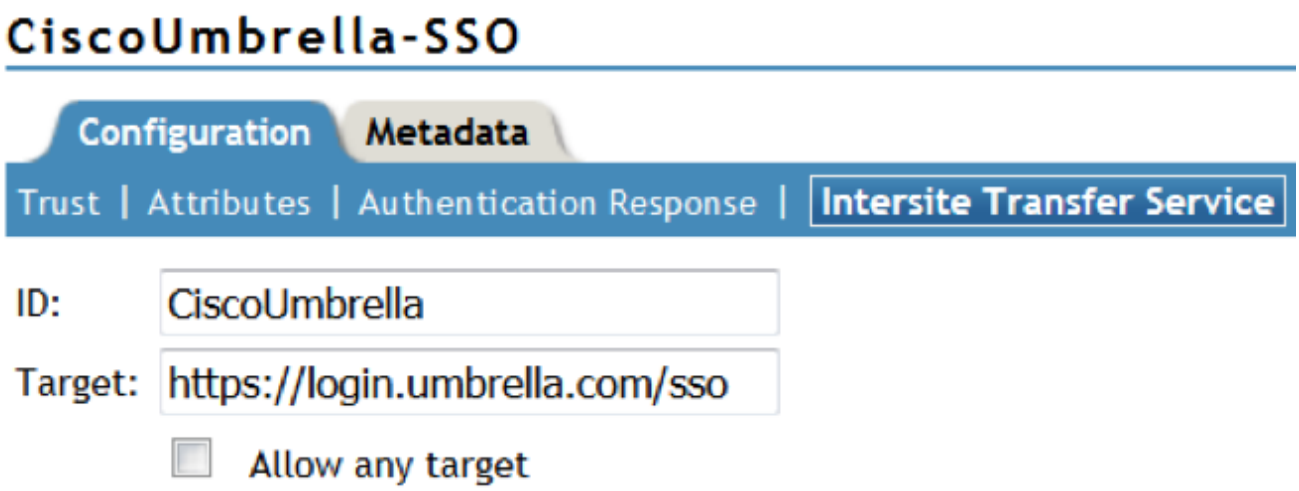
115000349827

3. 作成したばかりの属性を選択し、Send with Authenticationを選択します。Authentication Responseでは、Post Binding、Persistent、Transient、およびUnspecifiedを選択します。
4. LDAP Attribute: mail [LDAP Attribute Profile] を選択して、デフォルトにします。



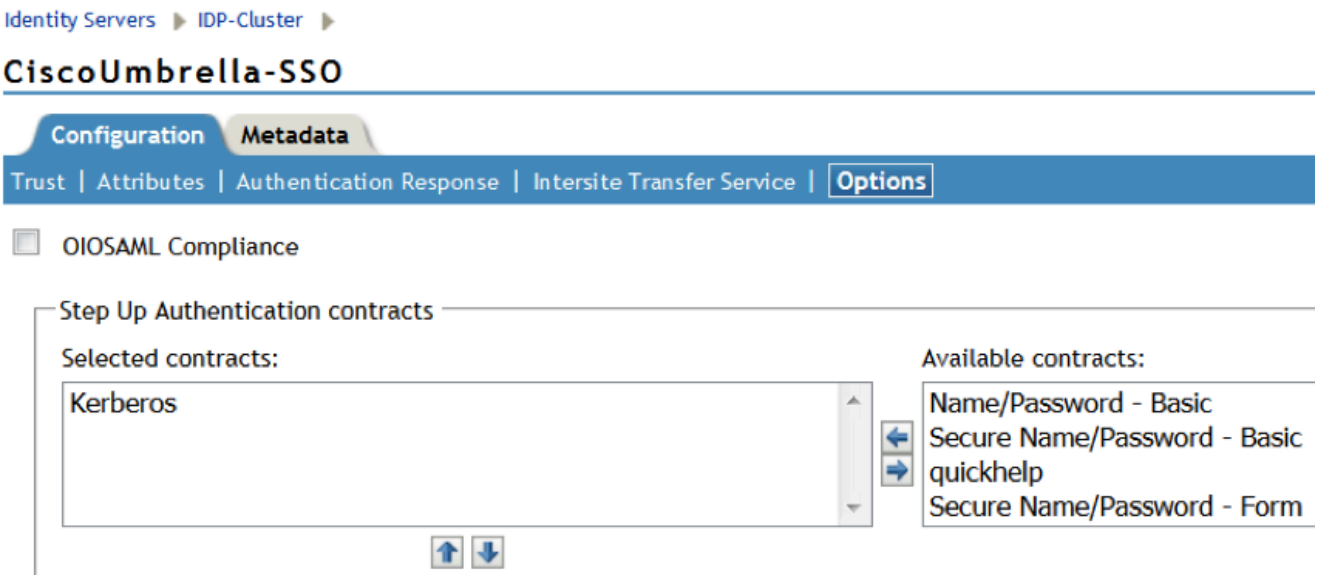
115000355688

5. Configuration > Intersite Transfer Serviceの順に移動します。Cisco Umbrella SAMLのような名前を付け、Cisco Umbrella SSOログインURLをターゲット(https://login.umbrella.com/sso)として追加します。



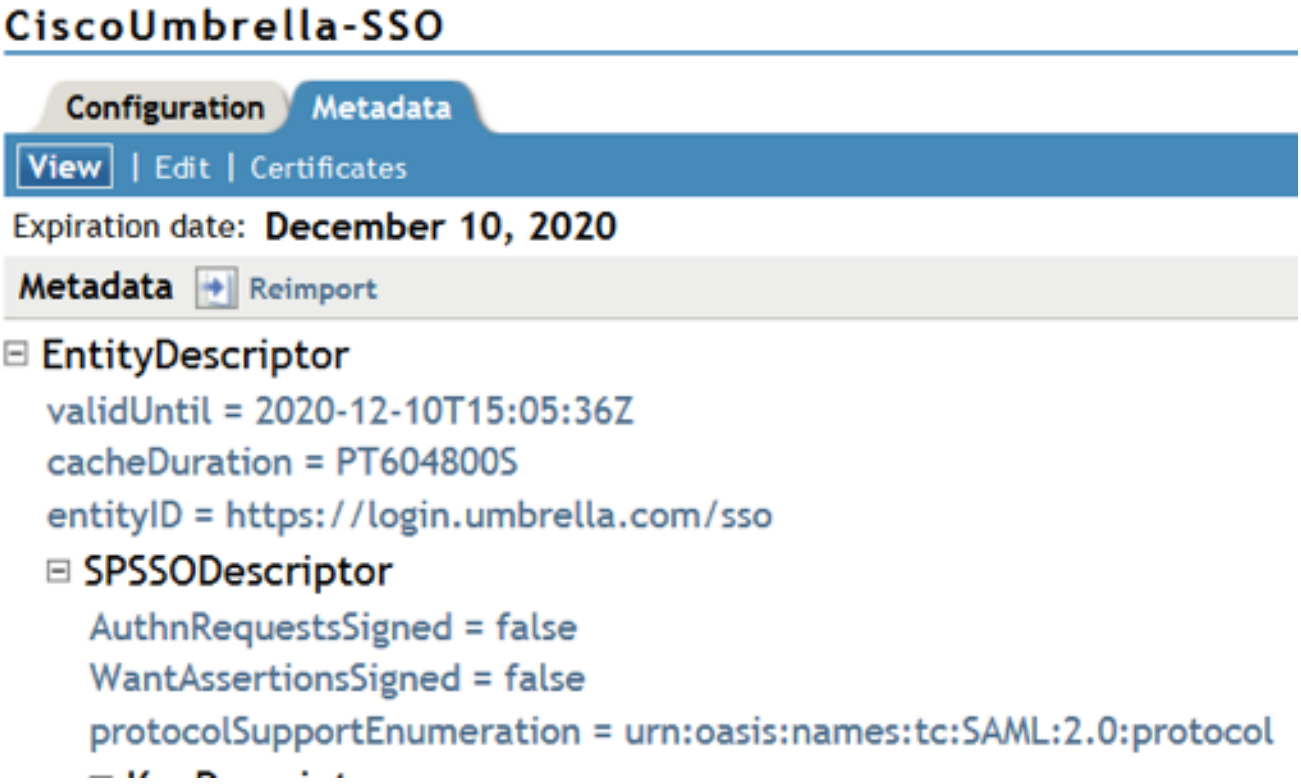
115000356827

6. Configuration > Optionsの順に移動し、Selected contracts:



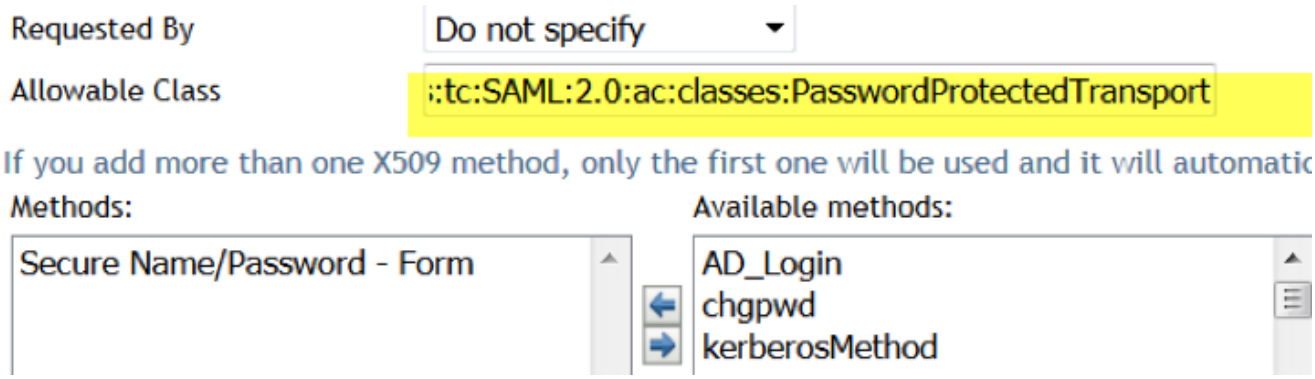
115000356068

7. Cisco Umbrellaメタデータファイルを開きます。EntityDescriptionフィールドvaildUntilの日付を、2020-12-10T20:50:59Zなどの将来のデータに更新します（スクリーンショットを参照）。
8. NetIQ > Metadataに戻り、更新されたメタデータファイルをインポートします。



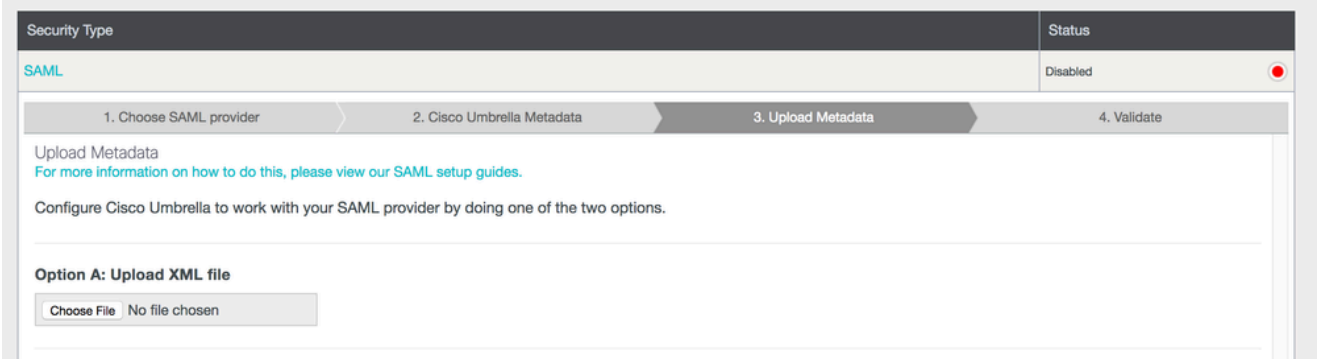
115000357147

9. アサーションにクラスを追加します。Cisco Umbrellaアサーションには、クラス **urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport**が必要です。
10. Local > Contractsの順に選択し、Secure Name/Passwordを選択して、Allowable Classフィールドに追加してから、上記のクラスを追加します。



115000357247

11. Identity Servicesとアクセスゲートウェイを更新して有効かつ最新であることを確認し、NetIQメタデータをダウンロードします。
12. ダウンロードしたメタデータを使用して、Cisco Umbrellaの「その他」のSAMLウィザードを実行します。手順3では、メタデータのアップロードを求められます。



115001186107

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。