

Intégration d'Umbrella avec NetIQ pour SSO avec SAML

Table des matières

[Introduction](#)

[Présentation de l'intégration SAML Umbrella pour NetIQ](#)

[Conditions préalables](#)

[Importer les métadonnées et le certificat Cisco Umbrella](#)

[Créer un groupe d'attributs](#)

[Créer un nouveau fournisseur de confiance](#)

Introduction

Ce document décrit comment intégrer Cisco Umbrella avec NetIQ pour l'authentification unique (SSO) avec SAML.

Présentation de l'intégration SAML Umbrella pour NetIQ

La configuration de SAML avec NetIQ diffère de nos autres intégrations SAML car il ne s'agit pas d'un processus en un ou deux clics dans l'assistant, mais nécessite des modifications dans NetIQ pour fonctionner correctement. Ce document décrit les modifications détaillées que vous devez apporter pour que SAML et NetIQ fonctionnent ensemble. À ce titre, ces renseignements sont fournis « tels quels » et ont été élaborés de concert avec les clients existants. L'assistance disponible pour cette solution est limitée et l'assistance Cisco Umbrella n'est pas en mesure d'apporter une assistance au-delà de la description générale donnée ici.

Pour plus d'informations sur le fonctionnement de l'intégration SAML avec Umbrella, lisez notre article ici : [Premiers pas avec l'authentification unique](#).

Identity Servers ►

IDP-Cluster

General

Local

Liberty

SAML 1.1

SAML 2.0

Trusted Providers

| Profiles

Conditions préalables

Vous trouverez les étapes à suivre pour passer par la configuration SAML initiale ici : [Intégrations des identités : Conditions préalables](#). Une fois que vous avez terminé ces étapes, qui incluent le téléchargement des métadonnées Cisco Umbrella, vous pouvez continuer à utiliser ces instructions spécifiques à NetIQ pour terminer la configuration.

Les métadonnées sont disponibles dans l'assistant de configuration de Cisco Umbrella SAML (Paramètres > Authentification > SAML).

Security Type	Status
SAML	Disabled

1. Choose SAML provider

2. OpenDNS Metadata

3. Upload Metadata

OpenDNS Metadata
[For more information on how to do this, please view our SAML setup guides.](#)

Option A: Copy and Paste

Copy this into your SAML provider's configuration

```
CAQIwgf8wHQYDVR0BBYEFDrNbJTppCIqDDpLx6LxPqX8Uj+MIHPBgNVHSMGccwgcSAFDrNbJTppCIqDDpLx6LxPqX8Uj+oYGgpIGdMIGAMQswCQYDVQQGEwJVUzETMBEGA1UECBMkQ2FsaWZvcm5pYTEwMBQGA1UEBxMNU2FuIEZyYW5jaXNjbzEQMA4GA1UEChMT3B1bkrOUzEUMBIGA1UECnMxRW5naW5lZXJpbmcxEzARBGNVBAMTCk9wZW5ETlMgQ1gxITAFBgkqhkiG9w0BCQEWEmVuZy5jeEBvcGVuZG5zLmNvbYIJALzrHo0EBtfKMAwGA1UdEwQFMAMBAf8wDQYJKoZIhvcNAQEFBQADggEBAApp6PqcEMopitp65xloAiH0HQJsxePWF+T9kH8sNEi1AFCcRFVDIPQVqLVQfymadUfGRHB51Kr0sM+529nQqzkWXSnlR01RfFABGgAsbIXxVv26xr/Xi48yRPLyVNP6vxMaonU++Uot hxlcriZqX7ZYoxhRZXECPqVLXaskAAHn0preupeQz2w8qxv/s+2E0NeZ9ehH2fVIEhbKAY1TuC/RWkVfoN4VvDnzby5C56qJs4z1gTRlijpkg1tSTSixeFJ0P/JdLKWa1Y8SM3U5fnXcwWawMztKznE+/b3W+bvmISFYG3zi0zsCY4aj8GMTLGLhdk4BB2QVpCH0z/xNk=</ds:X509Certificate>
</ds:X509Data>
</ds:KeyInfo>
</md:KeyDescriptors>
```

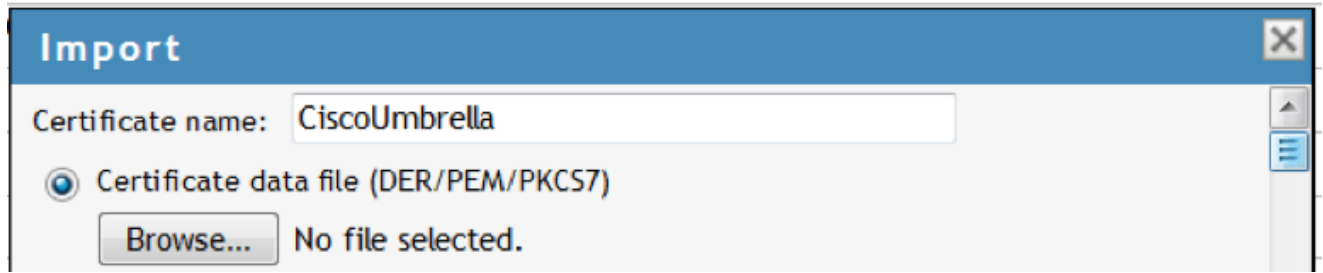
Option B: Download XML File

[DOWNLOAD XML FILE](#)

115001332488

Importer les métadonnées et le certificat Cisco Umbrella

1. Ouvrez les métadonnées Cisco Umbrella (téléchargées dans les conditions préalables) dans un éditeur de texte et extrayez le certificat X509. Le certificat commence par ds : X509Certificate et se termine par /ds : X509Certificate - il suffit de copier du début à la fin.
2. Enregistrez ce nouveau fichier sous le nom CiscoUmbrella.cer.
3. Convertissez le certificat x509 en PKCS7 / PEM. Les méthodes pour cela varient, mais cette commande fait l'affaire : `openssl x509 -in CiscoUmbrella.cer -out CiscoUmbrella.pem -outform PEM`
4. Dans NetIQ, lancez NAM sous Trusted Roots.
5. Sélectionnez Nouveau > Parcourir et importez CiscoUmbrella.pem.



Import

Certificate name:

☒ Certificate data file (DER/PEM/PKCS7)

No file selected.

115000349367

Créer un groupe d'attributs

1. Accédez à Identity Servers > NetIQ NAM.
2. Cliquez sur Jeux d'attributs.
3. Sélectionnez New et mappez les attributs LDAP :

CiscoUmbrellaAttributeSet

General Mapping Usage			
New Delete			
☐ Local Attribute	maps to	Remote Attribute	Attribute Value Encoding
☐ Ldap Attribute:userPrincipalName [LDAP Attribute Profile]	<-->	Email Address	Special characters encoded
☐ Ldap Attribute:mail [LDAP Attribute Profile]	<-->	NameID	Special characters encoded

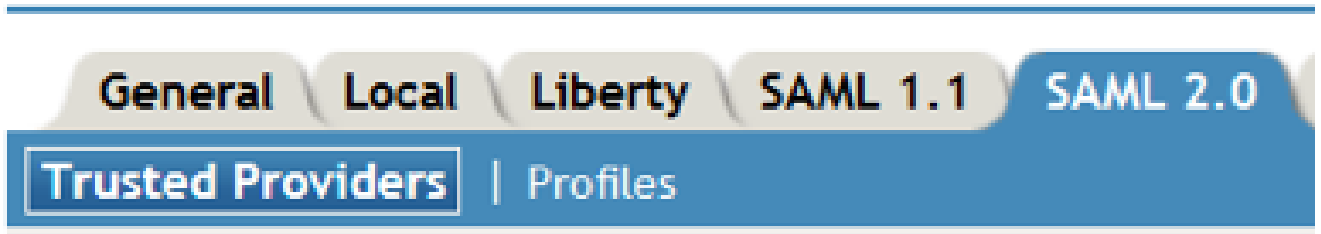
115000349567

Créer un nouveau fournisseur de confiance

1. Accédez à l'onglet IDP General et sélectionnez SAML 2.0.
2. Sélectionnez Créer un nouveau fournisseur de confiance.

[Identity Servers](#) ►

IDP-Cluster



General Local Liberty SAML 1.1 SAML 2.0

Trusted Providers | Profiles

115000348788

CiscoUmbrella-SSO

Configuration

Metadata

Trust

Attributes

Authentication Response

Intersite Transfer Service

Options

Name: CiscoUmbrella-SSO

Security

☐ Encrypt assertions ☐ Encrypt name identifiers

Certificate Revocation Check Periodicity: On Startup

SOAP Back Channel Security Method

- ☒ Message Signing
☐ Mutual SSL
☐ Basic Authentication

115000349827

- Sélectionnez l'attribut que vous venez de créer et choisissez Envoyer avec authentification. Pour Réponse d'authentification, choisissez Post Binding, Persistent, Transient et Unspecified.
- Sélectionner un attribut LDAP : mail [Profil d'attribut LDAP] et définissez-le par défaut.

CiscoUmbrella-SSO

Configuration

Metadata

Trust

Attributes

Authentication Response

Intersite Transfer Service

Options

Binding: Post

Name Identifier Format Default Value

☒	Persistent	☐	Automatically generated
☒	Transient	☐	Automatically generated
☐	E-mail	☐	Ldap Attribute:userPrincipalName [LDAP Attribute Profile]
☐	Kerberos	☐	<Not Specified>
☐	X509	☐	<Not Specified>
☒	Unspecified	☒	Ldap Attribute:mail [LDAP Attribute Profile]

☐ Use proxied requests

☐ Include the Session Timeout attribute in the assertion

Assertion Validity 300 seconds

115000355688

5. Accédez à Configuration > Intersite Transfer Service. Donnez-lui un nom comme Cisco Umbrella SAML et ajoutez l'URL de connexion SSO Cisco Umbrella comme cible (<https://login.umbrella.com/sso>).

CiscoUmbrella-SSO

Configuration Metadata

Trust | Attributes | Authentication Response | **Intersite Transfer Service**

ID:

Target:

☐ Allow any target

115000356827

6. Accédez à Configuration > Options et choisissez Kerberos comme contrats sélectionnés :

Identity Servers > IDP-Cluster >

CiscoUmbrella-SSO

Configuration Metadata

Trust | Attributes | Authentication Response | Intersite Transfer Service | **Options**

☐ OIOSAML Compliance

Step Up Authentication contracts

Selected contracts:

Available contracts:

115000356068

7. Ouvrez le fichier de métadonnées Cisco Umbrella. Mettez à jour le champ EntityDescription validUntil avec des données futures, telles que 2020-12-10T20:50:59Z (comme indiqué dans la capture d'écran).
8. Revenez à NetIQ > Metadata et importez le fichier de métadonnées mis à jour.

CiscoUmbrella-SSO

Configuration Metadata

View | Edit | Certificates

Expiration date: **December 10, 2020**

Metadata  Reimport

EntityDescriptor

validUntil = 2020-12-10T15:05:36Z

cacheDuration = PT604800S

entityID = https://login.umbrella.com/sso

SPSSODescriptor

AuthnRequestsSigned = false

WantAssertionsSigned = false

protocolSupportEnumeration = urn:oasis:names:tc:SAML:2.0:protocol

115000357147

9. Ajoutez une classe à l'assertion. L'assertion Cisco Umbrella nécessite la classe

`urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport`

10. Accédez à Local > Contracts et sélectionnez Secure Name/Password et ajoutez au champ Allowable Class, puis ajoutez la classe ci-dessus :

Requested By

Do not specify

Allowable Class

`urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport`

If you add more than one X509 method, only the first one will be used and it will automatic

Methods:

Available methods:

Secure Name/Password - Form

AD_Login

chgpwd

kerberosMethod

115000357247

11. Mettez à jour les services d'identité et les passerelles d'accès pour vous assurer qu'ils sont valides et à jour, puis téléchargez les métadonnées NetIQ.

12. Utilisez les métadonnées téléchargées pour exécuter l'assistant SAML Cisco Umbrella « Other ». L'étape 3 vous invite à télécharger les métadonnées :

Security Type	Status
SAML	Disabled 
1. Choose SAML provider2. Cisco Umbrella Metadata3. Upload Metadata4. Validate Upload Metadata For more information on how to do this, please view our SAML setup guides. Configure Cisco Umbrella to work with your SAML provider by doing one of the two options. Option A: Upload XML file Choose File No file chosen	

115001186107

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.