

Integreer paraplu met NetIQ voor SSO met SAML

Inhoud

[Inleiding](#)

[Overzicht van Umbrella SAML Integration voor NetIQ](#)

[Voorwaarden](#)

[Metagegevens en Cisco-overkoepelend certificaat importeren](#)

[Een Attribuutgroep maken](#)

[Een nieuwe vertrouwensprovider maken](#)

Inleiding

In dit document wordt beschreven hoe Cisco Umbrella met NetIQ voor Single Sign-on (SSO) met SAML kan worden geïntegreerd.

Overzicht van Umbrella SAML Integration voor NetIQ

Het configureren van SAML met NetIQ verschilt van onze andere SAML-integraties, omdat het geen één- of tweeklikproces in de wizard is, maar wijzigingen in NetIQ vereist om correct te werken. Dit document beschrijft de gedetailleerde wijzigingen die u moet aanbrengen om SAML en NetIQ samen te laten werken. Als zodanig wordt deze informatie "as is" verstrekt en is deze ontwikkeld in samenwerking met bestaande klanten. De beschikbare ondersteuning voor deze oplossing is beperkt en Cisco Umbrella-ondersteuning kan niet verder gaan dan de algemene beschrijving die hier wordt gegeven.

Voor meer informatie over hoe SAML-integratie werkt met Umbrella, lees onze review hier: [Aan de slag met Single Sign-On](#).

Identity Servers ►

IDP-Cluster

General

Local

Liberty

SAML 1.1

SAML 2.0

Trusted Providers | Profiles

Voorwaarden

U kunt hier stappen vinden om door de initiële SAML-setup te komen: [Identiteits Integraties: Vereisten](#). Nadat u de stappen hebt voltooid die het downloaden van de metagegevens van Cisco Umbrella omvatten, kunt u deze specifieke NetIQ-instructies blijven gebruiken om de configuratie te voltooien.

De metagegevens zijn te vinden in de installatiewizard Cisco Umbrella SAML (Instellingen > Verificatie > 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+oYGgpIGdMIGaMQswCQYDVQQGEwJVUzETMBEGA1UECBMkQ2FsaWZvcm5pYTEwMBQGA1UEBxMNU2FuIEZyYW5jaXNjbzEQMA4GA1UEChMHT3B1bKROUzEUMBIGA1UECnRlbnR5bW51ZXJpbmcxEzARBgNVBAMTCk9wZW5ETlMgQ1gxITAFBgkqhkiG9w0BCQEWEmVuZy5jeEBvcGVuZG5zLmNvbYIJALzrHo0EBtFKMAwGA1UdEwQFMAMBAf8wDQYJKoZIhvcNAQEFBQADggEBAApp6PqcEMopitp65xloAiH0HQJsxePWF+T9kH8sNEi1AFCcRFVDIPQVqLVQfymadUfGRHB51Kr0sM+529nQqzkWXSnlR01RfFABGgAsbIXxVv26xr/Xi48yRPLyNP6vxMaonU++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

Metagegevens en Cisco-overkoepelend certificaat importeren

1. Open de Cisco Umbrella-metagegevens (gedownload in de voorwaarden) in een teksteditor en pak het X509-certificaat uit. Het certificaat begint met ds:X509Certificate en eindigt met ds:ds:X509Certificate - gewoon kopiëren van het begin tot het einde.
2. Dit nieuwe bestand opslaan als CiscoUmbrella.cer.
3. Converteer het x509 certificaat naar PKCS7 / PEM. Methoden hiervoor variëren, maar deze opdracht doet de truc: `openssl x509 -in CiscoUmbrella.cer -out CiscoUmbrella.pem -outform PEM`
4. In NetIQ lanceert NAM onder Trusted Roots.
5. Selecteer Nieuw > Bladeren en importeren CiscoUmbrella.pem.

Import

Certificate name:

☒ Certificate data file (DER/PEM/PKCS7)

No file selected.

115000349367

Een Attribuutgroep maken

1. Ga naar Identiteitservers > NetIQ NAM.
2. Klik op Attribuutsets.
3. Selecteer Nieuw en breng de LDAP-kenmerken in kaart:

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

Een nieuwe vertrouwensprovider maken

1. Ga naar het tabblad Algemeen van IDP en selecteer SAML 2.0.
2. Selecteer Nieuwe vertrouwensprovider maken.

[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

3. Selecteer het Attribuut dat u zojuist hebt gemaakt en kies Verzenden met verificatie. Kies Post Binding, Persistent, Transient en Unspecified voor Authentication Response.
4. Selecteer LDAP Attribuut: mail [LDAP Attribuutprofiel] en maak deze standaard.

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. Navigeer naar Configuratie > Intersite Transfer Service. Geef het een naam zoals Cisco Umbrella SAML en voeg de Cisco Umbrella SSO-inlog-URL toe als een doel (<https://login.umbrella.com/sso>).

CiscoUmbrella-SSO

Configuration Metadata

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

ID:

Target:

☐ Allow any target

115000356827

6. Ga naar Configuratie > Opties en kies Kerberos als de Geselecteerde contracten:

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:

Name/Password - Basic

Secure Name/Password - Basic

quickhelp

Secure Name/Password - Form

 

115000356068

7. Open het Cisco Umbrella Metadata-bestand. Werk het veld EntityDescription validUntil date bij naar toekomstige gegevens, zoals 2020-12-10T20:50:59Z (zoals weergegeven in de screenshot).
8. Ga terug naar NetIQ > Metagegevens en importeer het bijgewerkte metagegevensbestand.

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

- Voeg een klasse toe aan de bewering. De Cisco Umbrella-bewering vereist de klasse `urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport`
- Ga naar Lokaal > Contracten en selecteer Beveiligde naam/wachtwoord en voeg toe aan het veld Toegestane klasse en voeg de bovenstaande klasse toe:

Requested By

Allowable Class

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

Methods:

Secure Name/Password - Form

Available methods:

AD_Login
chgpwd
kerberosMethod

115000357247

- Update Identity Services en Access Gateways om ervoor te zorgen dat ze geldig en up-to-date zijn en download vervolgens de NetIQ-metagegevens.
- Gebruik de gedownloade metagegevens om door de SAML-wizard Cisco Umbrella "Other" te lopen. Stap 3 is waar u wordt gevraagd om de metadata te uploaden:

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

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.