

Integration von Umbrella mit NetIQ für SSO mit SAML

Inhalt

[Einleitung](#)

[Überblick über die Umbrella SAML Integration für NetIQ](#)

[Voraussetzungen](#)

[Metadaten und Cisco Umbrella Certificate importieren](#)

[Attributgruppe erstellen](#)

[Erstellen eines neuen Vertrauensanbieters](#)

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](#).

Identity Servers ►

IDP-Cluster

General

Local

Liberty

SAML 1.1

SAML 2.0

Trusted Providers | Profiles

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).

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+oYGgpIGdMIGaMQswCQYDVQGEwJVUzETMBEGA1UECBMkQ2FsaWZvcm5pYTEwMBQGA1UEBxMNU2FuIEZyYW5jaXNjbzEQMA4GA1UEChMT3B1bkrOUzEUMBIGA1UECxlRW5naW5lZXJpbmcxEzARBGNVBAMTCk9wZW5ETlMgQ1gxITAFBgkqhkiG9w0BCQEWEmVuZy5jeEBvcGVuZG5zLmNvbYIJALzrHo0EBtfKMAwGA1UdEwQFMAMBAf8wDQYJKoZIhvcNAQEFBQADggEBAApp6PqcEMopitp65xloAiH0HQJsxePWF+T9kH8sNEi1AFCcRFVDIPQVqLVQfymadUfGRHB51Kr0sM+529nQqzkWXSnlR01RfFABGgAsbIXxVv26xr/Xi48yRPLyVNP6vxMaonU++Uot  
hxlcriZqX7ZYoxhRZXECPqVLXaskAAHn0preupeQz2w8qxv/s+2E0NeZ9ehH2fVIEhbKAY1TuC/RWkVfoN4VvDnzby5C56qJs4z1gTR  
lijpkg1tSTSixeFJ0P/JdLKWa1Y8SM3U5fnXcwWawMztKznE+/b3W+bvmISFYG3zi0zsCY4aj8GMLGLhdk4BB2QVpCH0z/xNk=  
</ds:X509Certificate>  
    </ds:X509Data>  
  </ds:KeyInfo>  
</md:KeyDescriptors>
```

Option B: Download XML File
[DOWNLOAD XML FILE](#)

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.

Import

Certificate name:

☒ Certificate data file (DER/PEM/PKCS7)

No file selected.

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:

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

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.

[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. 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.

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. 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>).

CiscoUmbrella-SSO

Configuration Metadata

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

ID:

Target:

☐ Allow any target

115000356827

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

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. Öffnen Sie die Cisco Umbrella-Metadatendatei. Aktualisieren Sie das Feld EntityDescription validUntil 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.

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

- Fügen Sie der Assertion eine Klasse hinzu. Die Cisco Umbrella Assertion erfordert die Klasse `urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport`
- 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:

Requested By

Allowable Class

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

Methods:

Available methods:

115000357247

- 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.
- Verwenden Sie die heruntergeladenen Metadaten, um den Cisco Umbrella "Other" SAML-Assistenten auszuführen. In Schritt 3 werden Sie aufgefordert, die Metadaten hochzuladen:

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

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.