

Umbrella de integración con NetIQ para SSO con SAML

Contenido

[Introducción](#)

[Descripción general de Umbrella SAML Integration para NetIQ](#)

[Prerequisites](#)

[Importar metadatos y certificado de Cisco Umbrella](#)

[Creación de un grupo de atributos](#)

[Crear un nuevo proveedor de confianza](#)

Introducción

Este documento describe cómo integrar Cisco Umbrella con NetIQ para Single Sign-on (SSO) con SAML.

Descripción general de Umbrella SAML Integration para NetIQ

La configuración de SAML con NetIQ difiere de nuestras otras integraciones SAML ya que no es un proceso de un clic o dos en el asistente, pero requiere cambios en NetIQ para funcionar correctamente. Este documento describe las modificaciones detalladas que debe realizar para que SAML y NetIQ funcionen conjuntamente. Como tal, esta información se proporciona "tal cual" y se desarrolló en colaboración con los clientes existentes. La asistencia disponible para esta solución es limitada y la asistencia de Cisco Umbrella no puede superar el esquema general que se ofrece aquí.

Para obtener más información sobre cómo funciona la integración de SAML con Umbrella, lea nuestra reseña aquí: [Comience con el inicio de sesión único](#).

Identity Servers ►

IDP-Cluster

General

Local

Liberty

SAML 1.1

SAML 2.0

Trusted Providers

| Profiles

Prerequisites

Puede encontrar los pasos para pasar por la configuración inicial de SAML aquí: [Integraciones de identidad: Prerrequisitos](#). Una vez que haya completado los pasos que incluyen la descarga de los metadatos de Cisco Umbrella, puede seguir utilizando estas instrucciones específicas de NetIQ para completar la configuración.

Los metadatos se pueden encontrar en el asistente de configuración de Cisco Umbrella SAML (Configuración > Autenticación > 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+oYGgpIGdMIGaMQswCQYDVQGEwJVUzETMBEGA1UECBMkQ2FsaWZvcm5pYTEwMBQGA1UEBxMNU2FuIEZyYW5jaXNjbzEQMA4GA1UEChMHT3B1bkrOUzEUMBIGA1UECnRlZXR5bmcxEzARBgNVBAMTCk9wZW5ETlMgQ1gxITAFBgkqhkiG9w0BCQEWEmVuZy5jeEBvcGVuZG5zLmNvbYIJALzrHo0EBtfKMAwGA1UdEwQFMAMBAf8wDQYJKoZIhvcNAQEFBQADggEBAApp6PqcEMopitp65xloAiH0HQJsxePWF+T9kH8sNEi1AFCcRFVDIPQVqLVQfymadUfGRHB51Kr0sM+529nQqzkWXSnlR01RfFABGgAsbIXxVv26xr/Xi48yRPLyNP6vxMaonU++Uot hxlcriZqX7ZYoxhRZXECPqVLXaskAAHn0preupeQz2w8qxv/s+2E0NeZ9ehH2fVIEhbKAY1TuC/RWkVfoN4VvDnzby5C56qJs4z1gTRlijpgltSTSixeFJ0P/JdLKWa1Y8SM3U5fnXcwWawMztKznE+/b3W+bvmISFYG3zi0zsCY4aj8GMTLGLhdk4BB2QVpCH0z/xNk=</ds:X509Certificate>
</ds:X509Data>
</ds:KeyInfo>
</md:KeyDescriptors>
```

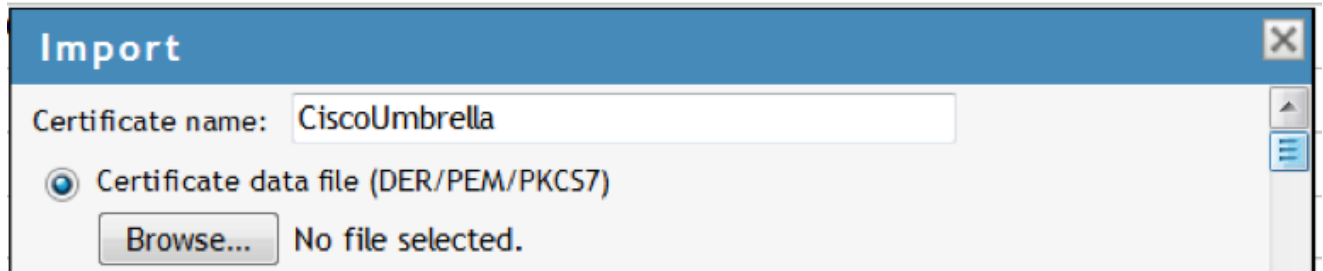
Option B: Download XML File

[DOWNLOAD XML FILE](#)

115001332488

Importar metadatos y certificado de Cisco Umbrella

1. Abra los metadatos de Cisco Umbrella (descargados en los requisitos previos) en un editor de texto y extraiga el certificado X509. El certificado comienza con ds:X509Certificate y termina con </ds:X509Certificate - sólo copia desde el principio hasta el final.
2. Guarde este nuevo archivo como CiscoUmbrella.cer.
3. Convierta el certificado x509 en PKCS7 / PEM. Los métodos para esto varían, pero este comando hace el truco: `openssl x509 -in CiscoUmbrella.cer -out CiscoUmbrella.pem -outform PEM`
4. En NetIQ, inicie NAM bajo Raíces de confianza.
5. Seleccione Nuevo > Examinar e importe CiscoUmbrella.pem.



Import

Certificate name:

☒ Certificate data file (DER/PEM/PKCS7)

No file selected.

115000349367

Creación de un grupo de atributos

1. Vaya a Identity Servers > NetIQ NAM.
2. Haga clic en Conjuntos de atributos.
3. Seleccione New y asigne los atributos 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

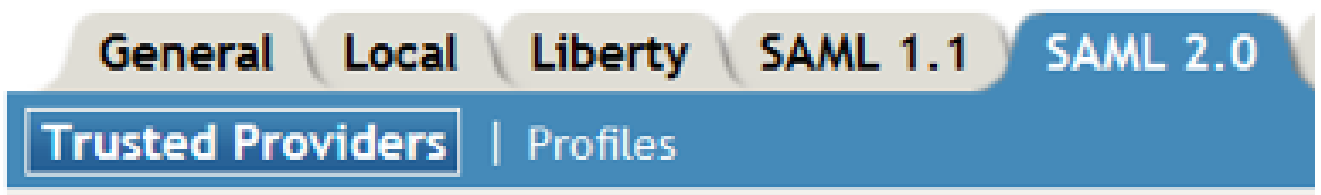
115000349567

Crear un nuevo proveedor de confianza

1. Vaya a la ficha General IDP y seleccione SAML 2.0.
2. Seleccione Create New Trust Provider.

[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. Seleccione el Atributo que acaba de crear y elija Enviar con Autenticación. Para la respuesta de autenticación elija Post Binding, Persistent, Transient y Unspecified.
4. Seleccione Atributo LDAP: mail [Perfil de atributo LDAP] y conviértalo en predeterminado.

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. Vaya a Configuration > Intersite Transfer Service. Asigne un nombre como Cisco Umbrella SAML y agregue la URL de inicio de sesión de Cisco Umbrella SSO como destino (<https://login.umbrella.com/sso>).

CiscoUmbrella-SSO

Configuration Metadata

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

ID:

Target:

☐ Allow any target

115000356827

6. Vaya a Configuration > Options y elija Kerberos como los contratos seleccionados:

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. Abra el archivo de metadatos de Cisco Umbrella. Actualice el campo EntityDescription validUntil a datos futuros, como 2020-12-10T20:50:59Z (como se muestra en la captura de pantalla).
8. Vuelva a NetIQ > Metadatos e importe el archivo de metadatos actualizado.

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. Agregue una clase a la afirmación. La afirmación de Cisco Umbrella requiere la clase `urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport`
10. Vaya a Local > Contracts y seleccione Secure Name/Password y agregue al campo Allowable Class, luego agregue la clase anterior:

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 automatically be used.

Methods:

Available methods:

Secure Name/Password - Form

AD_Login

chgpwd

kerberosMethod

115000357247

11. Actualice los servicios de identidad y los gateways de acceso para asegurarse de que son válidos y están actualizados y, a continuación, descargue los metadatos de NetIQ.
12. Utilice los metadatos descargados para ejecutar el asistente de SAML "Otros" de Cisco Umbrella. En el paso 3 se le solicita que cargue los metadatos:

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

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).