

将Umbrella与NetIQ集成，用于使用SAML的SSO

目录

[简介](#)

[面向NetIQ的Umbrella SAML集成概述](#)

[先决条件](#)

[导入元数据和Cisco Umbrella证书](#)

[创建属性组](#)

[创建新的信任提供程序](#)

简介

本文档介绍如何将Cisco Umbrella与NetIQ集成以实现单点登录(SSO)和SAML。

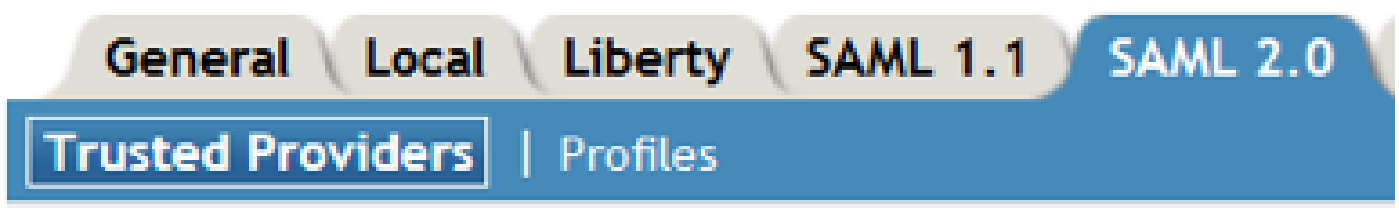
面向NetIQ的Umbrella SAML集成概述

使用NetIQ配置SAML不同于其他SAML集成，因为它不是向导中的一两次点击过程，但需要在NetIQ中进行更改才能正常工作。本文档介绍为了使SAML和NetIQ协同工作而需要进行的详细修改。因此，此信息按“原样”提供，并与现有客户共同开发。对此解决方案的可用支持有限，Cisco Umbrella支持无法提供除此处提供的一般大纲之外的其他帮助。

有关SAML集成如何与Umbrella配合使用的详细信息，请在此处阅读我们的评论：[开始单点登录](#)。

Identity Servers ►

IDP-Cluster



115000348788

先决条件

您可以在此处找到完成初始SAML设置的步骤：[身份集成：先决条件](#)。完成包括下载Cisco Umbrella元数据的这些步骤后，您可以继续使用这些NetIQ特定说明完成配置。

可以在Cisco Umbrella SAML设置向导（“设置”>“身份验证”>“SAML”）中找到该元数据。

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

```
CAQIwgf8wHQYDVR0BBYEFDzNbJTppCIqDDpLx6LxPqX8Uj+MIHPBgNVHSMegccwgcSAFDrNbJTppCIqDDpLx6LxPqX8Uj+oYGgpIGdMIGaMQswCQYDVQGEwJVUzETMBEGA1UECBMkQ2FsaWZvcm5pYTEwMBQGA1UEBxMNU2FuIEZyYW5jaXNjbzEQMA4GA1UEChMHT3B1b
kROUzEUMBIGA1UECxlRWSnaW5lZXJpbmcxEzARBgNVBAMTCk9wZW5ETlMgQ1gxITAFBgkqhkiG9w0BCQEWEmVuZy5jeEBvcGVuZG5z
LmNvbYIJALzrHo0EBtfKMAwGA1UdEwQFMAMBAF8wDQYJKoZIhvcNAQEFBQADggEBAApp6PqcEMopitp65xloAiH0HQJsxePWF+T9kH
8sNEi1AFCcRFVDIPQVqLVQfymadUfGRHB51Kr0sM+529nQqzkWXSnlR01RffABGgAsbIXxVv26xr/Xi48yRPLYvNP6vxMaonU++Uot
hxlcriZqX7ZYoxhRZXECPqVLXaskAAHn0preupeQz2w8qxv/s+2E0NeZ9ehH2fVIEHbKAY1TuC/RWkVfoN4VvDnzby5C56qJs4z1gTR
lijpkgltSTSixeFJ0P/JdLKWa1Y8SM3U5fnXcwWawMztKznE+/b3W+bvmISFYG3zi0zsCY4aj8GMTLGLhdk4BB2QVpCH0z/xNk=
</ds:X509Certificate>
</ds:X509Data>
</ds:KeyInfo>
</md:KeyDescriptors>
```

Option B: Download XML File

[Download XML File](#)

115001332488

导入元数据和Cisco Umbrella证书

1. 在文本编辑器中打开Cisco Umbrella元数据（在先决条件中下载）并提取X509证书。证书以ds:X509Certificate开头，以ds:X509Certificate结尾 — 只是从最开始到末尾进行复制。
2. 将此新文件另存为CiscoUmbrella.cer。
3. 将x509证书转换为PKCS7 / PEM。此命令的方法各不相同，但此命令可以达到目的：`openssl x509 -in CiscoUmbrella.cer -out CiscoUmbrella.pem -outform PEM`
4. 在NetIQ中，在Trusted Root下启动NAM。
5. 选择New > Browse并导入CiscoUmbrella.pem。

Import
Certificate name: CiscoUmbrella
Certificate data file (DER/PEM/PKCS7)
Browse... No file selected.

115000349367

创建属性组

1. 转至身份服务器> NetIQ NAM。
2. 单击属性集。

3. 选择New并映射LDAP属性：

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

创建新的信任提供程序

- 1. 转到IDP General选项卡，然后选择SAML 2.0。
- 2. 选择创建新信任提供程序。

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

- 选择刚创建的属性，然后选择Send with Authentication(使用身份验证发送)。对于 Authentication Response，请选择Post Binding、Persistent、Transient和Unspecified。
- 选择LDAP属性：邮件[LDAP属性配置文件]，并将其设为默认值。

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. 导航到配置>站点间传输服务。为其指定类似于Cisco Umbrella SAML的名称，并将Cisco Umbrella SSO登录URL添加为目标(<https://login.umbrella.com/sso>)。

CiscoUmbrella-SSO

Configuration Metadata

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

ID:

Target:

☐ Allow any target

115000356827

6. 转至Configuration > Options，然后选择Kerberos作为所选合同：

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. 打开Cisco Umbrella元数据文件。将EntityDescription字段vaildUntil日期更新为将来数据，例如2020-12-10T20:50:59Z（如屏幕截图所示）。
8. 返回NetIQ > Metadata并导入更新的元数据文件。

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. 将类添加到断言。Cisco Umbrella断言需要该类

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

10. 转至Local > Contracts，选择Secure Name/Password并添加到Allowable Class字段，然后添加上述类：

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:

Secure Name/Password - Form

Available methods:

AD_Login

chgpwd

kerberosMethod

115000357247

11. 更新身份服务和访问网关以确保它们有效且是最新的，然后下载NetIQ元数据。
12. 使用下载的元数据通过Cisco Umbrella“其他” SAML向导运行。第3步是要求您上传元数据的位置：

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

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。