

Integrar Umbrella com NetIQ para SSO com SAML

Contents

[Introdução](#)

[Visão geral da integração do Umbrella SAML para NetIQ](#)

[Pré-requisitos](#)

[Importar metadados e certificado do Cisco Umbrella](#)

[Criar um Grupo de Atributos](#)

[Criar um Novo Provedor Confiável](#)

Introdução

Este documento descreve como integrar o Cisco Umbrella com NetIQ para Single Sign-on (SSO) com SAML.

Visão geral da integração do Umbrella SAML para NetIQ

A configuração do SAML com NetIQ difere de nossas outras integrações SAML, pois não é um processo de um ou dois cliques no assistente, mas requer alterações no NetIQ para funcionar corretamente. Este documento descreve as modificações detalhadas que você precisa fazer para fazer com que o SAML e o NetIQ trabalhem juntos. Como tal, essas informações são fornecidas "no estado em que se encontram" e foram desenvolvidas em conjunto com os clientes existentes. O suporte disponível para esta solução é limitado e o suporte do Cisco Umbrella não pode ajudar além do esboço geral fornecido aqui.

Para obter mais informações sobre como a integração SAML funciona com o Umbrella, leia nossa análise aqui: [Introdução ao Logon Único](#).

Identity Servers ►

IDP-Cluster

General

Local

Liberty

SAML 1.1

SAML 2.0

Trusted Providers

| Profiles

Pré-requisitos

Você pode encontrar as etapas para passar pela configuração inicial do SAML aqui: [Integrações de identidade: Pré-requisitos](#). Após concluir as etapas que incluem o download dos metadados do Cisco Umbrella, você poderá continuar usando essas instruções específicas do NetIQ para concluir a configuração.

Os metadados podem ser encontrados no assistente de configuração do Cisco Umbrella SAML (Configurações > Autenticação > 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+oYGgpIGdMIGaMQswCQYDVQGEwJVUzETMBEGA1UECBMkQ2FsaWZvcm5pYTEwMBQGA1UEBxMNU2FuIEZyYW5jaXNjbzEQMA4GA1UEChMHT3B1bKROUzEUMBIGA1UECnRlW5naW5lZXJpbmcxEzARBGNVBMATCk9wZW5ETlMgQ1gxITAFBgkqhkiG9w0BCQEWEmVuZy5jeEBvcGVuZG5zLmNvbYIJALzrHo0EBtfKMAwGA1UdEwQFMAMBAf8wDQYJKoZIhvcNAQEFBQADggEBAApp6PqcEMopitp65xloAiH0HQJsxePWF+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

Importar metadados e certificado do Cisco Umbrella

1. Abra os metadados do Cisco Umbrella (baixados nos pré-requisitos) em um editor de texto e extraia o certificado X509. O certificado começa com ds:X509Certificate e termina com /ds:X509Certificate - basta copiar do início ao fim.
2. Salve este novo arquivo como CiscoUmbrella.cer.
3. Converta o certificado x509 em PKCS7 / PEM. Os métodos para isso variam, mas esse comando faz o truque: `openssl x509 -in CiscoUmbrella.cer -out CiscoUmbrella.pem -outform PEM`
4. No NetIQ, inicie o NAM em Trusted Roots.
5. Selecione New > Browse e importe CiscoUmbrella.pem.

Import

Certificate name:

☒ Certificate data file (DER/PEM/PKCS7)

No file selected.

115000349367

Criar um Grupo de Atributos

1. Vá para Identity Servers > NetIQ NAM.
2. Clique em Conjuntos de Atributos.
3. Selecione New e mapeie os 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

Criar um Novo Provedor Confiável

1. Vá até a guia geral de IDP e selecione SAML 2.0.
2. Selecione Criar Novo Provedor de Confiança.

[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. Selecione o atributo que você acabou de criar e escolha Enviar com autenticação. Para a resposta de autenticação, escolha Pós-ligação, Persistente, Transitório e Não especificado.
4. Selecionar atributo LDAP: mail [LDAP Attribute Profile] e torne-o padrão.

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. Navegue até Configuration > Intersite Transfer Service. Dê a ele um nome como Cisco Umbrella SAML e adicione a URL de login do Cisco Umbrella SSO como um Destino (<https://login.umbrella.com/sso>).

CiscoUmbrella-SSO

Configuration Metadata

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

ID:

Target:

☐ Allow any target

115000356827

6. Vá para Configuration > Options e escolha Kerberos como os contratos selecionados:

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 o arquivo de metadados do Cisco Umbrella. Atualize o campo EntityDescription validUntil para uma data futura, como 2020-12-10T20:50:59Z (como mostrado na captura de tela).
8. Volte para NetIQ > Metadata e importe o arquivo de metadados atualizado.

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. Adicionar uma classe à asserção. A asserção do Cisco Umbrella requer que a turma `urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport`
10. Vá para Local > Contracts, selecione Secure Name/Password e adicione ao campo Allowable Class e adicione a classe acima:

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

Methods:

Secure Name/Password - Form

Available methods:

AD_Login

chgpwd

kerberosMethod

115000357247

11. Atualize o Identity Services e os gateways de acesso para garantir que sejam válidos e atualizados e faça o download dos metadados do NetIQ.
12. Use os metadados baixados para executar o assistente do Cisco Umbrella "Other" SAML. A etapa 3 é onde você é solicitado a fazer o upload dos metadados:

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

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.