

UmbrellaとNetIQを統合してSAMLでSSOを実現

内容

[はじめに](#)

[NetIQ向けUmbrella SAML統合の概要](#)

[前提条件](#)

[メタデータとCisco Umbrella証明書のインポート](#)

[属性グループの作成](#)

[新しい信頼プロバイダーの作成](#)

はじめに

このドキュメントでは、Cisco UmbrellaとNetIQ for Single Sign-on(SSO)をSAMLと統合する方法について説明します。

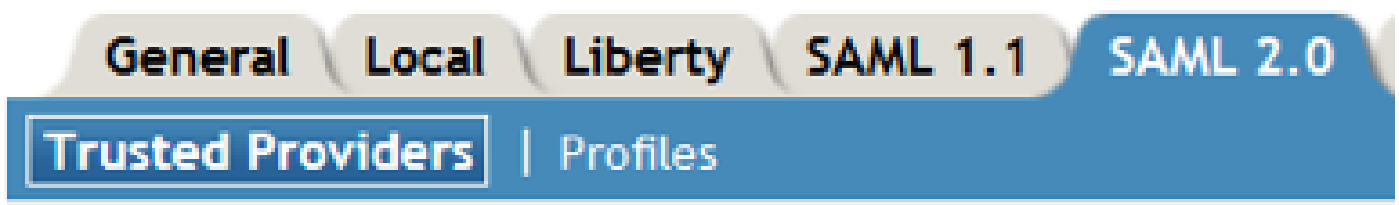
NetIQ向けUmbrella SAML統合の概要

NetIQによるSAMLの設定は、ウィザードでの1回または2回のクリックではなく、NetIQの変更が正しく動作する必要があるため、他のSAML統合とは異なります。このドキュメントでは、SAMLとNetIQを連携させるために必要な変更の詳細について説明します。そのため、この情報は「現状のまま」提供され、既存のお客様と共同で開発されました。このソリューションで利用可能なサポートは限られており、Cisco Umbrellaのサポートでは、ここで説明する一般的な概要を超えたサポートは提供できません。

SAML統合とUmbrellaの連携の詳細については、こちらのレビュー「[シングルサインオンを開始する](#)」を参照してください。

[Identity Servers](#) ▶

IDP-Cluster



115000348788

前提条件

SAMLの初期設定の手順については、[Identity Integrations: Prerequisites](#)を参照してください。

Cisco Umbrellaメタデータのダウンロードを含むこれらの手順を完了したら、次のNetIQ固有の手順を使用して設定を完了できます。

メタデータは、Cisco Umbrella SAMLセットアップウィザード(設定>認証> SAML)にあります。

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+MIHPBgNVHSEgcccwgcSAFDrNbJTppCIqDDpLx6LxPqX8Uj+oYGgpIGdMIGaMQswCQYDVQGEwJVUzETMBEGA1UECBMkQ2FsaWZvcm5pYTEwMBQGA1UEBxMNU2FuIEZyYW5jaXNjbzEQMA4GA1UEChMHT3B1bkrOUzEUMBIGA1UECxlRWSnaW5lZXJpbmcxEzARBGNVBAMTCk9wZW5ETlMgQ1gxITAfBgkqhkiG9w0BCQEWEmVuZy5jeEBvcGVuZG5zLmNvbYIJALzrHo0EBtfKMAwGA1UdEwQFMAMBAf8wDQYJKoZIhvcNAQEFBQADggEBAAppc6PqcEMopitp65xloAiH0HQJsxePWF+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

メタデータとCisco Umbrella証明書のインポート

1. テキストエディタでCisco Umbrellaメタデータ（前提条件でダウンロード）を開き、X509証明書を抽出します。証明書はds:X509Certificateで始まりds:X509Certificateで終わります。最初から最後までコピーするだけです。
2. この新しいファイルをCiscoUmbrella.cerという名前で保存します。
3. x509証明書をPKCS7/PEMに変換します。これを行う方法はさまざまですが、このコマンドはテクニクを実行します。openssl x509 -in CiscoUmbrella.cer -out CiscoUmbrella.pem -outform PEM
4. NetIQで、Trusted Rootsの下でNAMを起動します。
5. New > Browseの順に選択し、CiscoUmbrella.pemをインポートします。

Import

Certificate name: CiscoUmbrella

☒ Certificate data file (DER/PEM/PKCS7)

Browse...

No file selected.

115000349367

属性グループの作成

1. Identity Servers > NetIQ NAMの順に選択します。
2. Attribute Setsをクリックします。
3. Newを選択して、LDAP属性をマッピングします。

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

新しい信頼プロバイダーの作成

1. IDP Generalタブに移動し、SAML 2.0を選択します。
2. Create New Trust Providerを選択します。

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

- 作成したばかりの属性を選択し、Send with Authenticationを選択します。Authentication Responseでは、Post Binding、Persistent、Transient、およびUnspecifiedを選択します。
- LDAP Attribute: mail [LDAP Attribute Profile] を選択して、デフォルトにします。

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. Configuration > Intersite Transfer Serviceの順に移動します。Cisco Umbrella SAMLのような名前を付け、Cisco Umbrella SSOログインURLをターゲット (<https://login.umbrella.com/sso>)として追加します。

CiscoUmbrella-SSO

Configuration Metadata

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

ID:

Target:

☐ Allow any target

115000356827

6. Configuration > Optionsの順に移動し、Selected contracts:

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. Cisco Umbrellaメタデータファイルを開きます。EntityDescriptionフィールドvalidUntilの日付を、2020-12-10T20:50:59Zなどの将来のデータに更新します (スクリーンショットを参照)。
8. NetIQ > Metadataに戻り、更新されたメタデータファイルをインポートします。

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. アサーションにクラスを追加します。Cisco Umbrellaアサーションには、クラス `urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport` が必要です。
10. Local > Contractsの順に選択し、Secure Name/Passwordを選択して、Allowable Classフィールドに追加してから、上記のクラスを追加します。

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 automatic

Methods:

Available methods:

Secure Name/Password - Form

AD_Login

chgpwd

kerberosMethod

115000357247

11. Identity Servicesとアクセスゲートウェイを更新して有効かつ最新であることを確認し、NetIQメタデータをダウンロードします。
12. ダウンロードしたメタデータを使用して、Cisco Umbrellaの「その他」のSAMLウィザードを実行します。手順3では、メタデータのアップロードを求められます。

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

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。