

將Umbrella與NetIQ整合，以便使用SAML進行SSO

目錄

[簡介](#)

[適用於NetIQ的Umbrella SAML整合概述](#)

[必要條件](#)

[匯入後設資料和Cisco Umbrella證書](#)

[建立屬性組](#)

[建立新的信任提供程式](#)

簡介

本文檔介紹如何將Cisco Umbrella與NetIQ整合，以實現單點登入(SSO)和SAML。

適用於NetIQ的Umbrella SAML整合概述

使用NetIQ配置SAML不同於其他SAML整合，因為它不是嚮導中一兩次按一下的過程，但需要對NetIQ進行更改才能正常工作。本文檔介紹了為使SAML和NetIQ協同工作而需要進行的詳細修改。因此，此資訊按「原樣」提供，並與現有客戶一起開發。對此解決方案的可用支援有限，思科Umbrella支援無法提供此處提供的總大綱之外的幫助。

有關SAML整合如何與Umbrella配合使用的詳細資訊，請在此處閱讀我們的評論：[開始單一登入](#)。

Identity Servers ►

IDP-Cluster



115000348788

必要條件

您可以在以下找到完成初始SAML設定的步驟：[身份整合：必要條件](#)。完成包括下載Cisco Umbrella後設資料的這些步驟後，您可以繼續使用這些NetIQ特定說明完成配置。

可在Cisco Umbrella SAML安裝嚮導(「設定」>「身份驗證」>「SAML」)中找到後設資料。

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

```
CAQIwgf8wHQYDVR0BBYEFDrNbJTxxpCIqDDpLx6LxPqX8Uj+MIHPBgNVHSMGccwgcSAFDrNbJTxxpCIqDDpLx6LxPqX8Uj+oYGgpIGdMIGaMQswCQYDVQQGEwJVUzETMBEGA1UECBMkQ2FsaWZvcm5pYTEwMBQGA1UEBxMNU2FuIEZyYW5jaXNjbzEQMA4GA1UEChMT3B1bkROUzEUMBIGA1UECjMLRW5naW5lZXJpbmcxEzARBgNVBAMTCk9wZW5ETLMgQ1gxITAFBgkqhkiG9w0BCQEWEmVuZy5jeEBvcGVuZG5zLmNvbYIJALzrHo0EBtFKMAwGA1UdEwQFMAMBAF8wDQYJKoZIhvcNAQEFBQADggEBAAppc6PqcEMopitp65x1oAiH0HQJsxePWF+T9kH8sNei1AFCcRFVDIPQVqLVQfymadUfGRHB51Kr0sM+529nQqzkWXSnlR01RfFABGgAsbIXxVv26xr/Xi48yRPLyVNP6vxMaonU++Uot  
hxlcriZqX7ZYoxhRZXEcpqVLXaskAAHn0preupeQz2w8qxv/s+2E0NeZ9ehH2fVieHbKAY1TuC/RWkVfoN4VvDnzby5C56qJs4z1gTR  
lijpkg1tSTSixeFJ0P/JdLKWa1Y8SM3U5fnXcwWawMztKznE+/b3W+bvmISFYG3zi0zsCY4aj8GMTLGlhdK4BB2QVpCH0z/xNk=  
</ds:X509Certificate>  
    </ds:X509Data>  
</ds:KeyInfo>  
</md:KeyDescriptors>
```

Option B: Download XML File

[Download XML File](#)

115001332488

匯入後設資料和Cisco Umbrella證書

- 在文本編輯器中開啟Cisco Umbrella後設資料 (在先決條件中下載) 並提取X509證書。證書以ds:X509Certificate開頭，以ds:X509Certificate結尾 — 僅從開始到結束進行複製。
- 將此新檔案另存為CiscoUmbrella.cer。
- 將x509證書轉換為PKCS7 / PEM。執行此命令的方法各不相同，但此命令可以執行此操作：
openssl x509 -in CiscoUmbrella.cer -out CiscoUmbrella.pem -outform PEM
- 在NetIQ中，在Trusted Root下啟動NAM。
- 選擇New > Browse並匯入CiscoUmbrella.pem。

Import

Certificate name: CiscoUmbrella

☒ Certificate data file (DER/PEM/PKCS7)

Browse...

No file selected.

115000349367

建立屬性組

1. 轉到身份伺服器> NetIQ NAM。
2. 按一下屬性集。
3. 選擇New並對映LDAP屬性：

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

建立新的信任提供程式

1. 轉到IDP General頁籤，然後選擇SAML 2.0。
2. 選擇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

- 選擇您剛剛建立的屬性，然後選擇Send with Authentication。對於身份驗證響應，請選擇Post Binding、Persistent、Transient和Unspecified。
- 選擇LDAP屬性：郵件[LDAP屬性配置檔案]並將其設為預設值。

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. 導航到Configuration > Intersite Transfer Service。為其指定類似於Cisco Umbrella SAML的名稱，並將Cisco Umbrella SSO登入URL新增為目標(<https://login.umbrella.com/sso>)。

CiscoUmbrella-SSO

Configuration Metadata

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

ID:

Target:

☐ Allow any target

115000356827

6. 前往Configuration > Options，然後選擇Kerberos作為所選合約：

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. 開啟Cisco Umbrella Metadata檔案。將EntityDescription欄位valdUntil日期更新為將來資料，例如2020-12-10T20:50:59Z（如螢幕截圖所示）。
8. 返回到NetIQ > Metadata並匯入更新的後設資料檔案。

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. 向斷言新增類。Cisco Umbrella斷言需要該類

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

10. 轉至Local > Contracts，選擇Secure Name/Password並新增到Allowable Class欄位，然後新增上述類：

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:

Secure Name/Password - Form

Available methods:

AD_Login

chgpwd

kerberosMethod

115000357247

11. 更新身份服務和訪問網關以確保它們有效且是最新的，然後下載NetIQ後設資料。

12. 使用下載的後設資料通過Cisco Umbrella「其他」SAML嚮導運行。第3步是要求您上傳後設資料的位置：

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

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。