

使用與Duo SSO和Windows AD整合的SAML配置 ISE 3.1 GUI管理員登入

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[辨識提供者\(IdP\)](#)

[服務提供者\(SP\)](#)

[SAML](#)

[SAML斷言](#)

[概要流程圖](#)

[設定與Duo SSO整合的SAML SSO](#)

[步驟 1. 在ISE上配置SAML IdP](#)

[將Duo SSO配置為外部SAML身份源](#)

[從Duo管理門戶導入SAML後設資料XML檔案](#)

[配置ISE身份驗證方法](#)

[建立管理員組](#)

[為管理組建立RBAC策略](#)

[新增群組成員資格](#)

[導出SP資訊](#)

[步驟 2. 為ISE配置Duo SSO](#)

[步驟 3. 將Cisco ISE與Duo SSO整合為通用SP](#)

[驗證](#)

[測試與Duo SSO的整合](#)

[疑難排解](#)

簡介

本文檔介紹如何配置Cisco ISE 3.1 SAML SSO與外部身份提供者 (如Cisco Duo SSO) 的整合。

必要條件

需求

思科建議您瞭解以下主題：

- 思科身分辨識服務引擎(ISE) 3.1
- 安全宣告標籤語言(SAML)單一登入(SSO)部署的基本知識(SAML 1.1)

- Cisco DUO SSO知識
- 瞭解Windows Active Directory

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 思科ISE 3.1
- Cisco Duo SSO
- Windows Active Directory

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

辨識提供者(IdP)

在此案例中，Duo SSO會驗證並宣告使用者身分及對所要求資源（「服務提供者」）的存取許可權。

Duo SSO充當IdP，使用SAML 1.1或任何SAML 2.0 IdP（例如Microsoft Azure）的現有內部部署Active Directory (AD)驗證您的使用者，並在允許訪問服務提供商應用程式之前提示進行雙因素驗證。

當配置要使用Duo SSO保護的應用時，您必須將屬性從Duo SSO傳送到應用。Active Directory無需其他設定，但如果您使用SAML(2.0) IdP作為身份驗證源，請驗證您是否將其配置為傳送正確的SAML屬性。

服務提供者(SP)

使用者想要訪問的託管資源或服務；在此例中為Cisco ISE應用伺服器。

SAML

SAML是允許IdP向SP傳遞授權憑據的開放標準。

SAML事務使用可擴展標籤語言(XML)實現身份提供方和服務提供者之間的標準化通訊。SAML是使用者身份驗證與使用服務的授權之間的鏈路。

SAML斷言

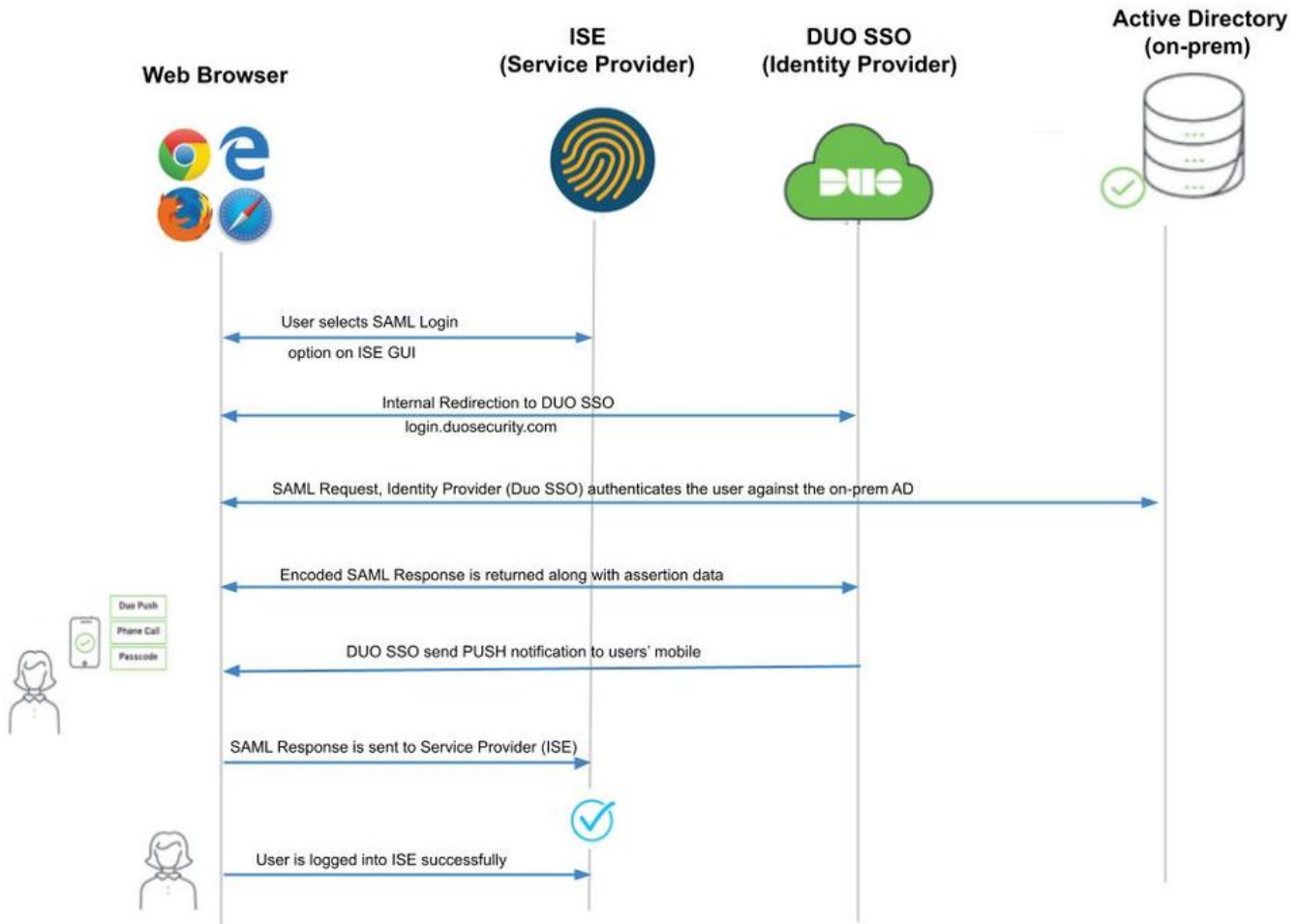
SAML Assertion是IdP傳送到包含使用者授權的服務提供者的XML文檔。有三種不同型別SAML斷言-身份驗證、屬性和授權決策。

- 身份驗證斷言可證明使用者的身份，並提供使用者登入的時間以及他們使用的身份驗證方法

(例如 , Kerberos、雙因素等)。

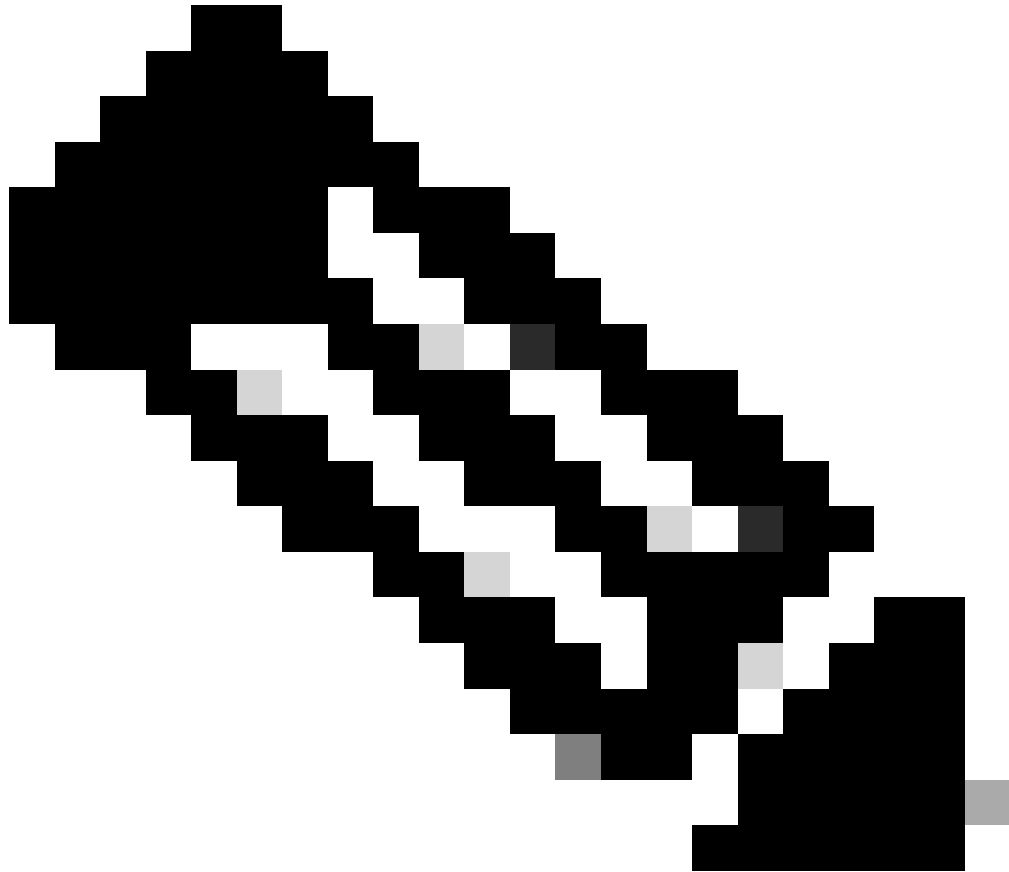
- 歸屬斷言將SAML屬性 (提供有關使用者資訊的特定資料) 傳遞給SP。
- 授權決策斷言宣告使用者是否獲得授權以便使用該服務 , 或者IdP是否由於密碼失敗或缺少對服務的許可權而拒絕其請求。

概要流程圖



流程 :

1. 使用者使用Login Via SAML選項登入到ISE。
2. ISE (SAML SP)使用SAML請求消息將使用者瀏覽器重定向到Duo SSO。



注意：在分散式環境中，可能會出現「Invalid Certificate」錯誤，並且第3步現在可以工作。因此，對於分散式環境，步驟2.與此稍有不同：

問題：ISE臨時重定向到其中一個PSN節點的門戶（在埠8443上）。

解決方案：為了確保ISE提供與管理員GUI證書相同的證書，請確保您信任的系統證書對所有PSN節點上的門戶使用有效。

3. 使用者使用主AD憑證登入。
4. Duo SSO將此消息轉發給AD，AD將響應返回給Duo SSO。
5. Duo SSO要求使用者透過在流動裝置上傳送PUSH來完成雙因素身份驗證。
6. 使用者完成Duo雙因素身份驗證。
7. Duo SSO將使用者瀏覽器重定向到SAML SP並返回一條響應消息。
8. 使用者現在能夠登入到ISE。

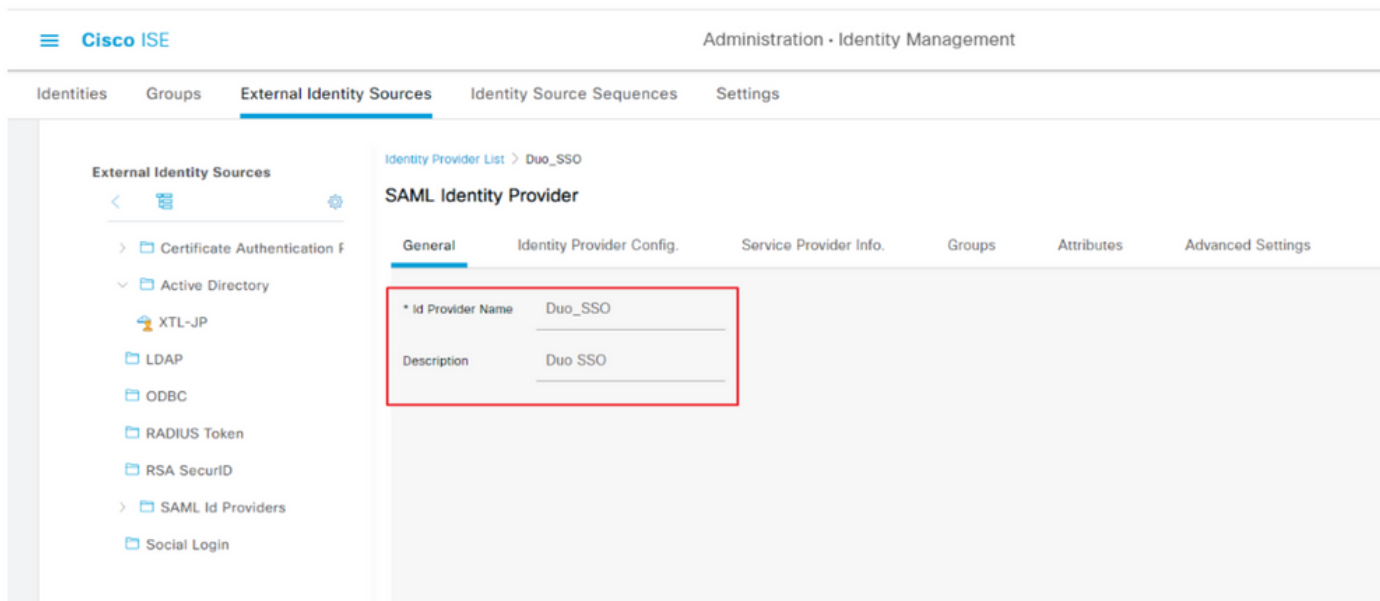
設定與Duo SSO整合的SAML SSO

步驟 1.在ISE上配置SAML IdP

將Duo SSO配置為外部SAML身份源

在ISE上，導航到Administration > Identity Management > External Identity Sources > SAML Id Providers，然後點選增加按鈕。

輸入IdP的名稱，然後按一下Submit以儲存它。IdP名稱僅對ISE有效，如圖所示：

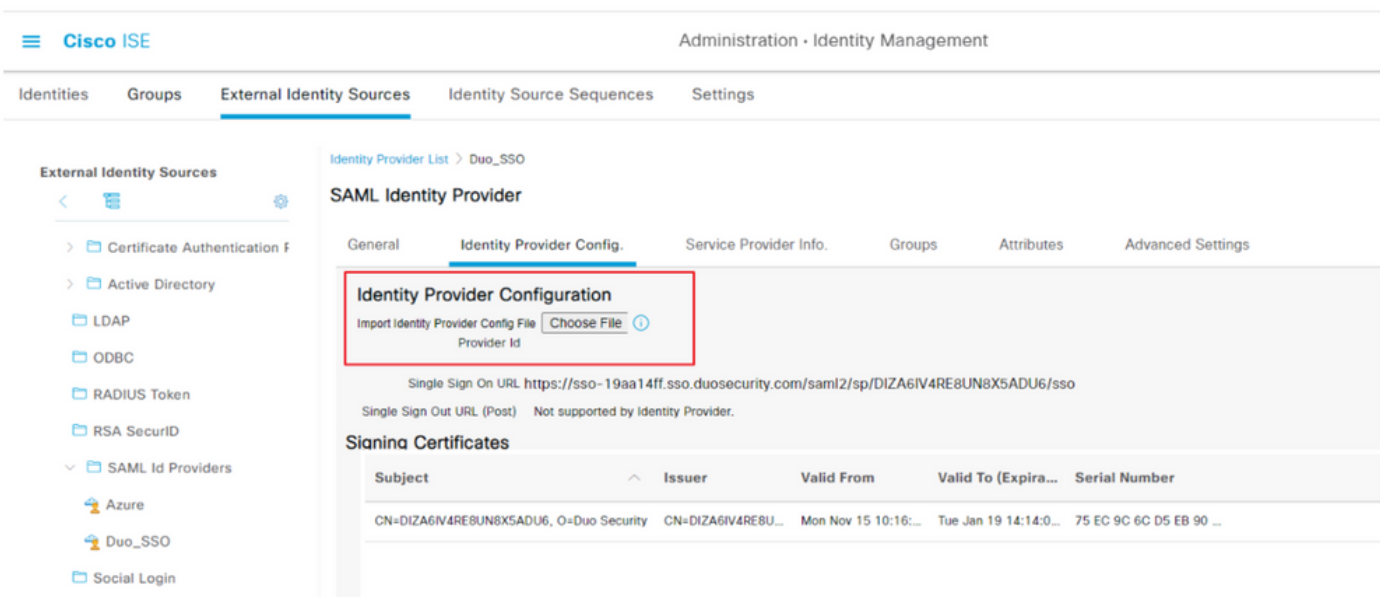


從Duo管理門戶導入SAML後設資料XML檔案

在ISE上，導航到Administration > Identity Management > External Identity Sources > SAML Id Providers.>選擇您建立的SAML IdP，點選Identity Provider Configuration，然後點選選擇檔案按鈕。

選擇從Duo Admin門戶導出的SSO IDP後設資料XML檔案，然後按一下Open以儲存該檔案。（此步驟也在本檔案的Duo一節中提及。）

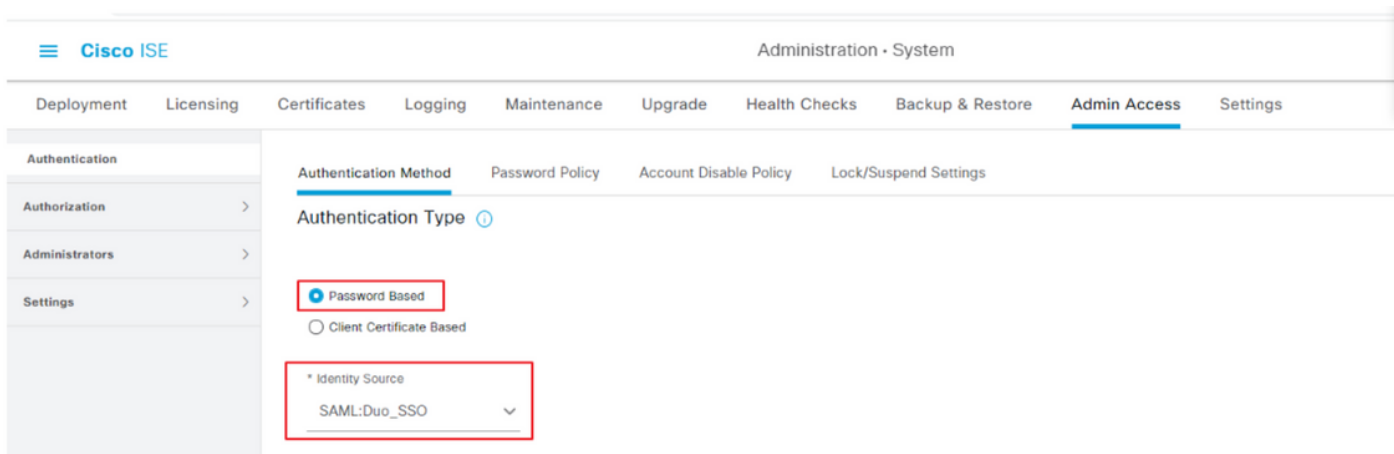
SSO URL和簽名證書包括：



配置ISE身份驗證方法

導航到Administration > System > Admin Access > Authentication > Authentication Method，然後選擇「Password-Based」單選按鈕。從

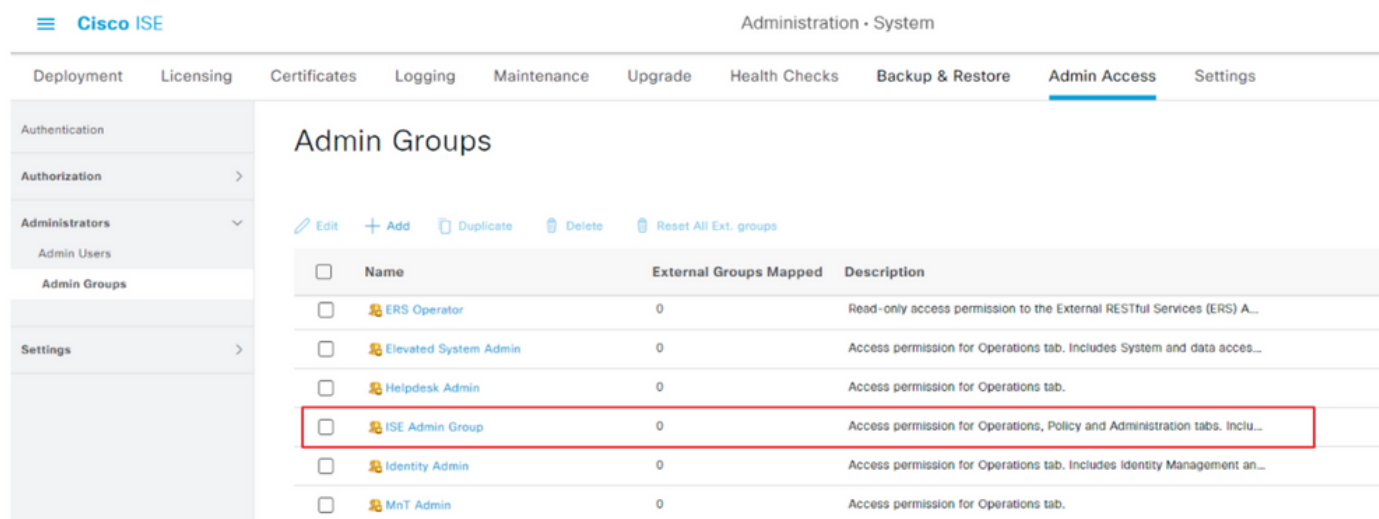
Identity Source 下拉式清單中選擇先前建立的必要IdP名稱，如下圖所示：



建立管理員組

導航到Administration > System > Admin Access > Authentication > Administrators > Admin Group，點選超級管理員，然後點選複製按鈕。輸入Admin group Name，然後按一下Submit按鈕。

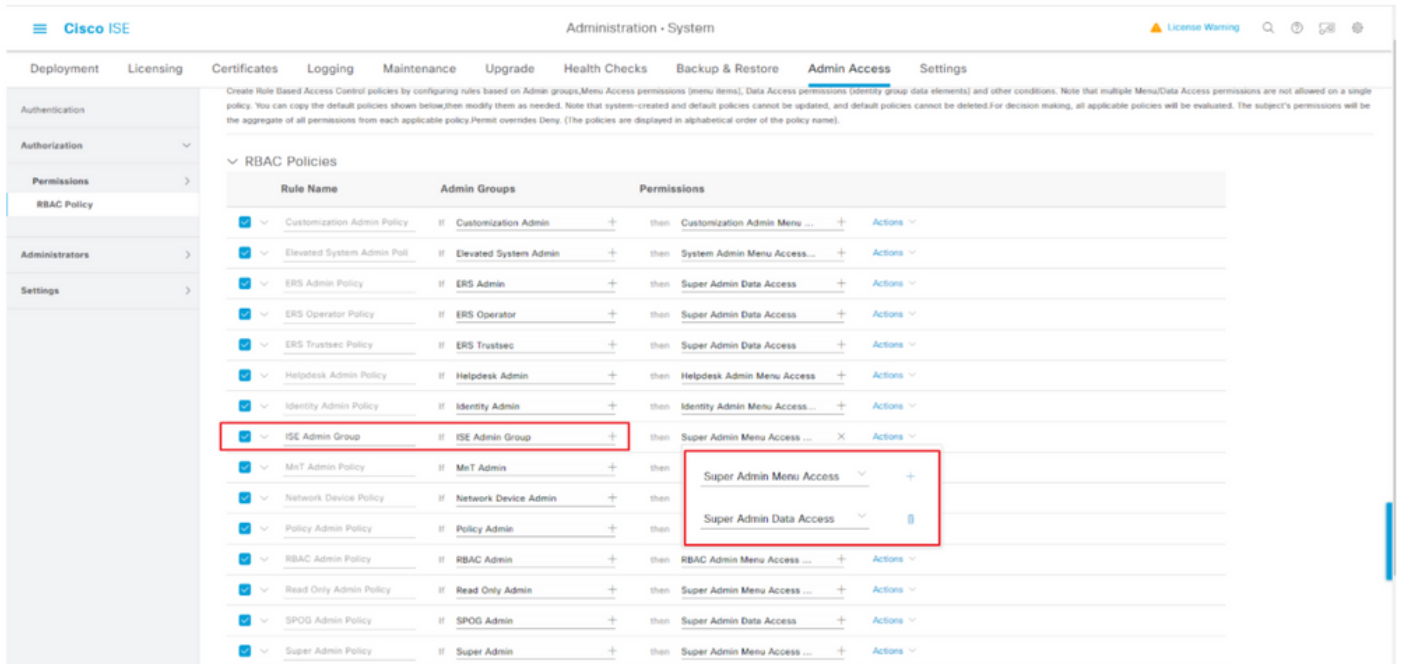
這會為Admin組提供Super Admin許可權。



為管理組建立RBAC策略

導航到Administration > System > Admin Access > Authorization > RBAC Policy，然後選擇與超級管理員策略相對應的操作。按一下Duplicate > Add the Name field > Save。

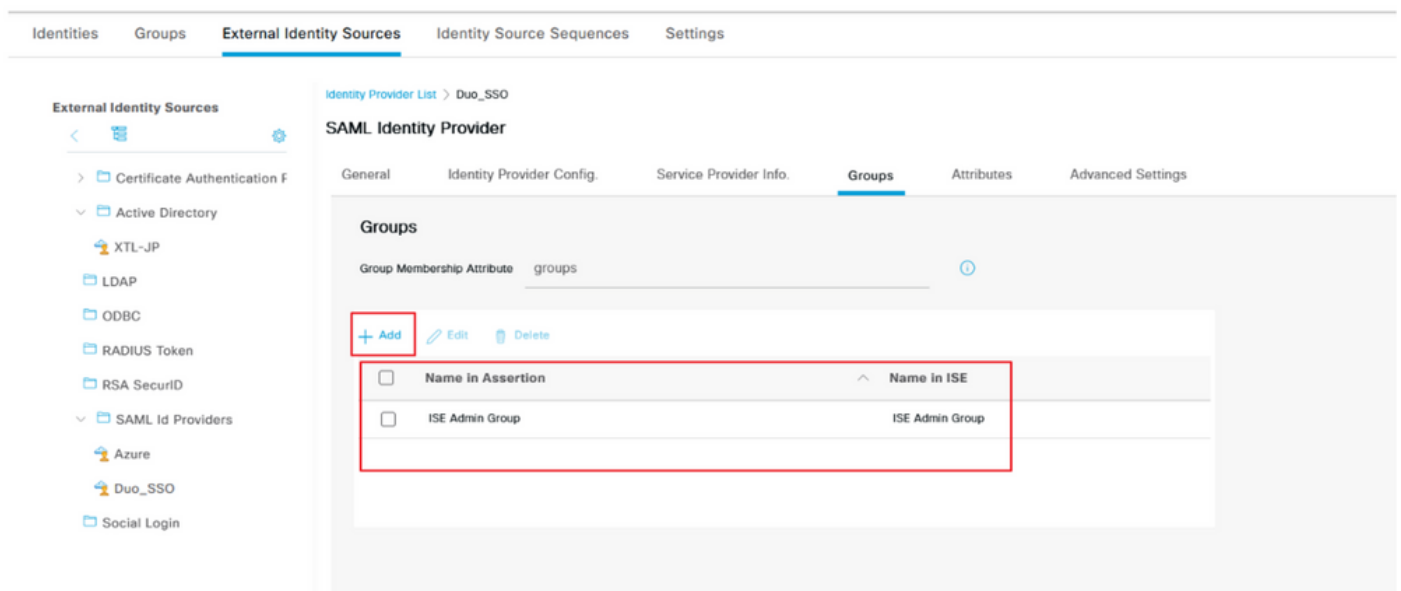
存取許可權與超級管理員原則相同。



新增群組成員資格

在ISE上，導航到Administration > Identity Management > External Identity Sources > SAML Id Providers，然後選擇您建立的SAML IdP。按一下Groups，然後按一下Add按鈕。

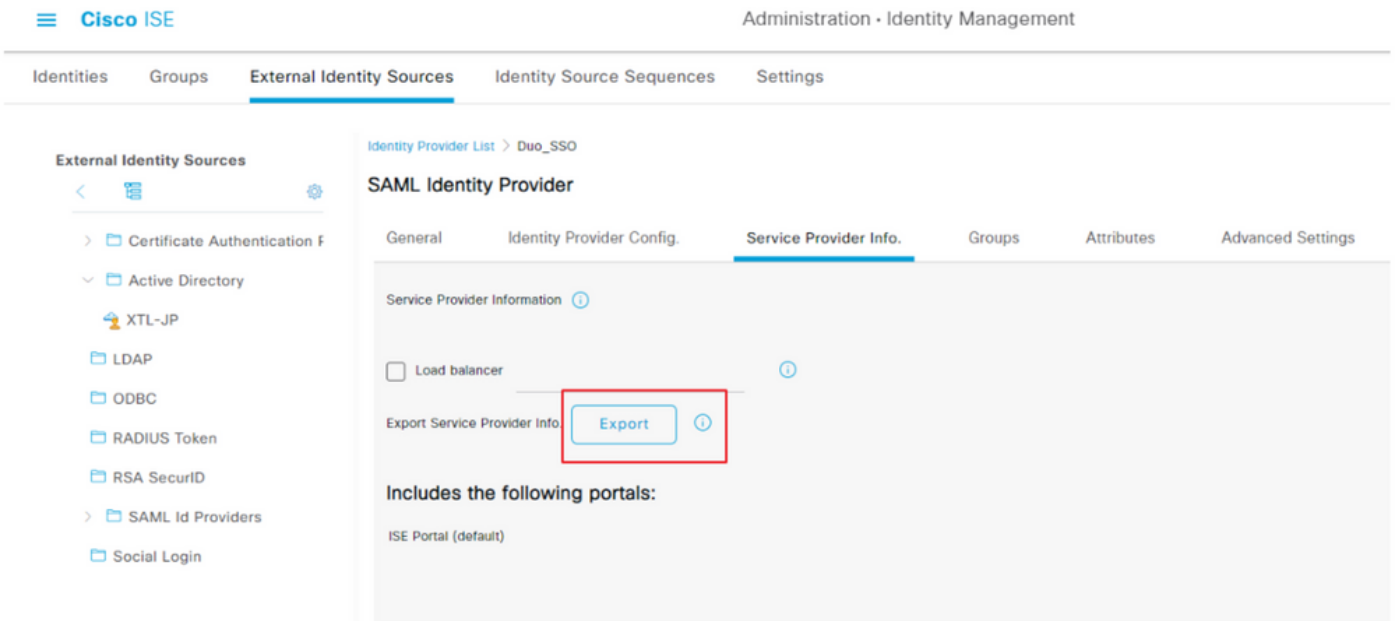
在斷言中增加名稱（ISE管理員組的名稱），然後從下拉選單中選擇所建立的基於角色的訪問控制(RBAC)組（第4步），然後按一下Open以儲存它。SSO URL和簽名證書會自動填充：



導出SP資訊

導航到Administration > Identity Management > External Identity Sources > SAML Id Providers > (Your SAML Provider)。

將該頁籤切換到「SP資訊」。然後按一下導出按鈕，如圖所示：



下載.xml檔案並儲存。記下AssertionConsumerServiceLocation URL和entityID值，因為Duo SSO門戶中需要這些詳細資訊。

```
<?xml version="1.0" encoding="UTF-8"?><md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metada
```

以下是從Duo Generic SAML Integration中需要配置的meta檔案中收集的相關詳細資訊/屬性

entityID = <http://CiscoISE/7fdcf239-631e-439c-a3ab-f5e56429779d>。

AssertionConsumerService位置 = <https://10.x.x.x:8443/portal/SSOLoginResponse.action>，其中10.x.x.x是在XML檔案 (位置) 中找到的ISE IP。

AssertionConsumerService位置 = <https://isenodename.com:8443/portal/SSOLoginResponse.action>，其中isenodename是在XML檔案 (位置) 中找到的實際ISE FQDN名稱。

步驟 2. 為ISE配置Duo SSO

檢查此[KB](#)以配置帶AD的Duo SSO作為身份驗證源。

Configured Authentication Sources

Name	Type	Status	Authentication Proxies
+ Add source			
Active Directory	Active Directory	Enabled	Authentication Proxy

選中此[KB](#)以啟用自定義域的SSO。

Single Sign-On

i

Custom Subdomain

Your users will see the custom subdomain when they authenticate to a Single Sign-On protected application. A familiar URL will help your users know that the site belongs to your organization. The subdomain will be home to Duo Central, if you choose to enable it. Duo Central allows your users to access your organization's sites and applications in one central place.

[Create a custom subdomain](#)

Customize your SSO subdomain

Tailor the single sign-on experience to match your company's brand and help your users recognize phishing attempts. Your users will see this custom subdomain during authentication.

Custom subdomain

zerotrustlabs

.login.duosecurity.com

Subdomain must contain only letters, numbers, or hyphens (-). Subdomain may not begin or end with a hyphen (-) and must be less than 63 characters in length.

[Save and continue](#)

[Complete later](#)

步驟 3.將Cisco ISE與Duo SSO整合為通用SP

檢查此[KB](#)的第1步和第2步，將Cisco ISE與Duo SSO整合為通用SP。

在Duo管理面板中配置通用SP的Cisco ISE SP詳細資訊：

名稱	說明
實體ID	http://CiscoISE/7fdcf239-631e-439c-a3ab-f5e56429779d
宣告使用者服務(ACS) URL	https://10.x.x.x:8443/portal/SSOLoginResponse.action

Service Provider

Entity ID *

<http://CiscoISE/7fdcf239-631e-439c-a3ab-f5e56429779d>

The unique identifier of the service provider.

Assertion Consumer Service
(ACS) URL *

<https://10.52.14.44:8443/portal/SSOLoginResponse.action>

配置思科ISE的SAML響應：

名稱	說明
NameID格式	urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified
NameID屬性	使用者名稱

SAML Response

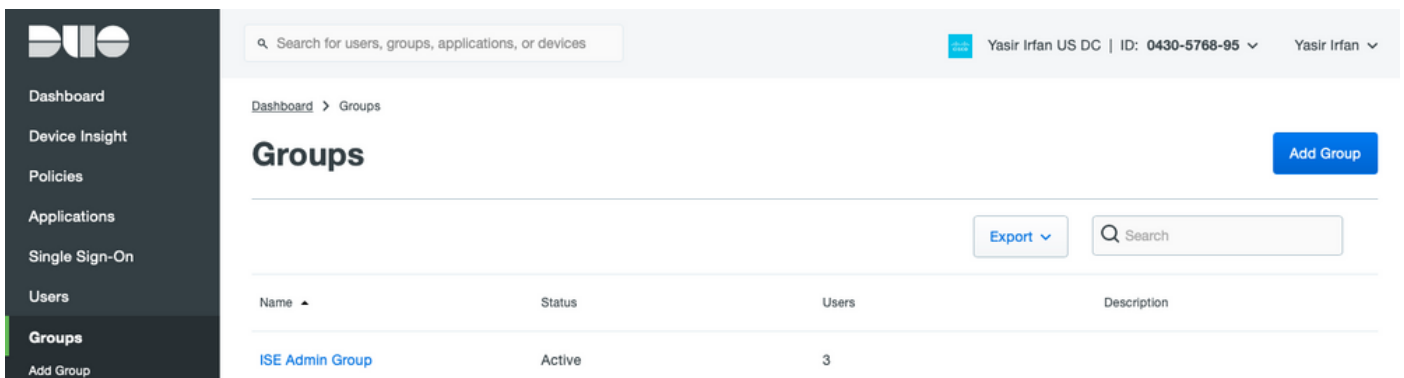
NameID format *

The format that specifies how the NameID is sent to the service provider.

NameID attribute *

NameID is a SAML attribute that identifies the user. Enter in an IdP attribute or select one of Duo's preconfigured attributes that automatically chooses the NameID attribute based on the IdP. There are five preconfigured attributes: <Email Address>, <Username>, <First Name>, <Last Name> and <Display Name>.

在Duo Admin Panel中建立名為Cisco Admin Group的組，並將ISE使用者增加到此組，或在Windows AD中建立組並使用目錄同步功能將其同步到Duo Admin面板。



配置思科ISE的角色屬性：

名稱	說明
屬性名稱	群組
SP角色	ISE管理組
Duo組	ISE管理組

Role attributes

Map Duo groups to different roles in this service provider. A Duo group can be mapped to multiple roles and each role can have multiple groups mapped to it. Optional. [Learn more about Duo groups](#).

Attribute name

The name of the attribute which will carry the mapped roles.

Service Provider's Role

Duo groups



在Settings部分的Name頁籤中，為此整合提供相應的名稱。

Settings

Type

Generic Service Provider - Single Sign-On

Name

Duo Push users will see this when approving transactions.

按一下Save按鈕儲存配置，並參閱此[KB](#)以瞭解更多詳細資訊。

按一下Download XML以下載SAML後設資料。

Downloads

Certificate

[Download certificate](#)

Expires: 01-19-2038

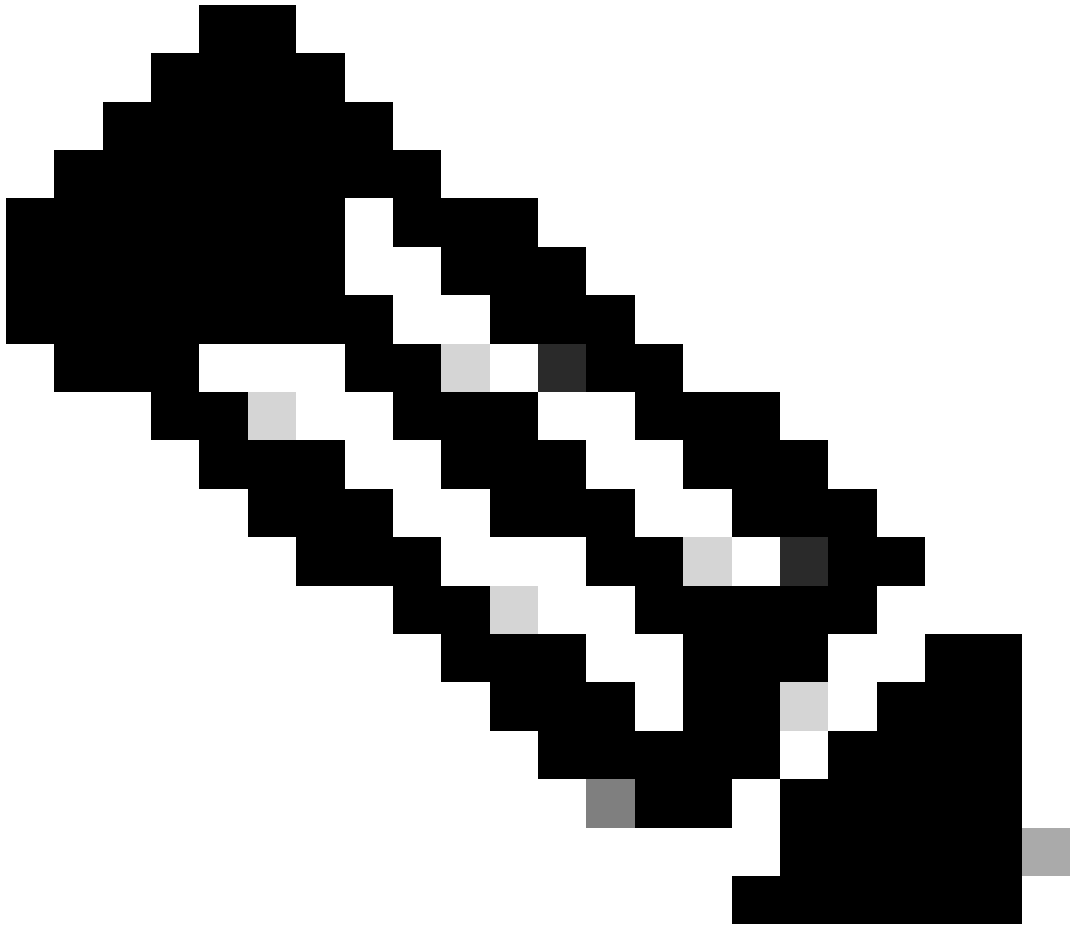
SAML Metadata

[Download XML](#)

導航至Administration > Identity Management > External Identity Sources > SAML Id Providers > Duo_SSO，將SAML MetaData下載從Duo管理面板上傳到Cisco ISE。

將頁籤切換到Identity Provider Config，然後按一下Choose檔案按鈕。

選擇在步驟8中下載的後設資料XML檔案，然後按一下儲存。



注意：此步驟在配置SAML SSO與Duo SSO整合的部分中提到；第2步。從Duo Admin門戶導入SAML後設資料XML檔案。

[Identity Provider List](#) > Duo_SSO

SAML Identity Provider

General

Identity Provider Config.

Service Provider Info.

Groups

Attributes

Advanced Settings

Identity Provider Configuration

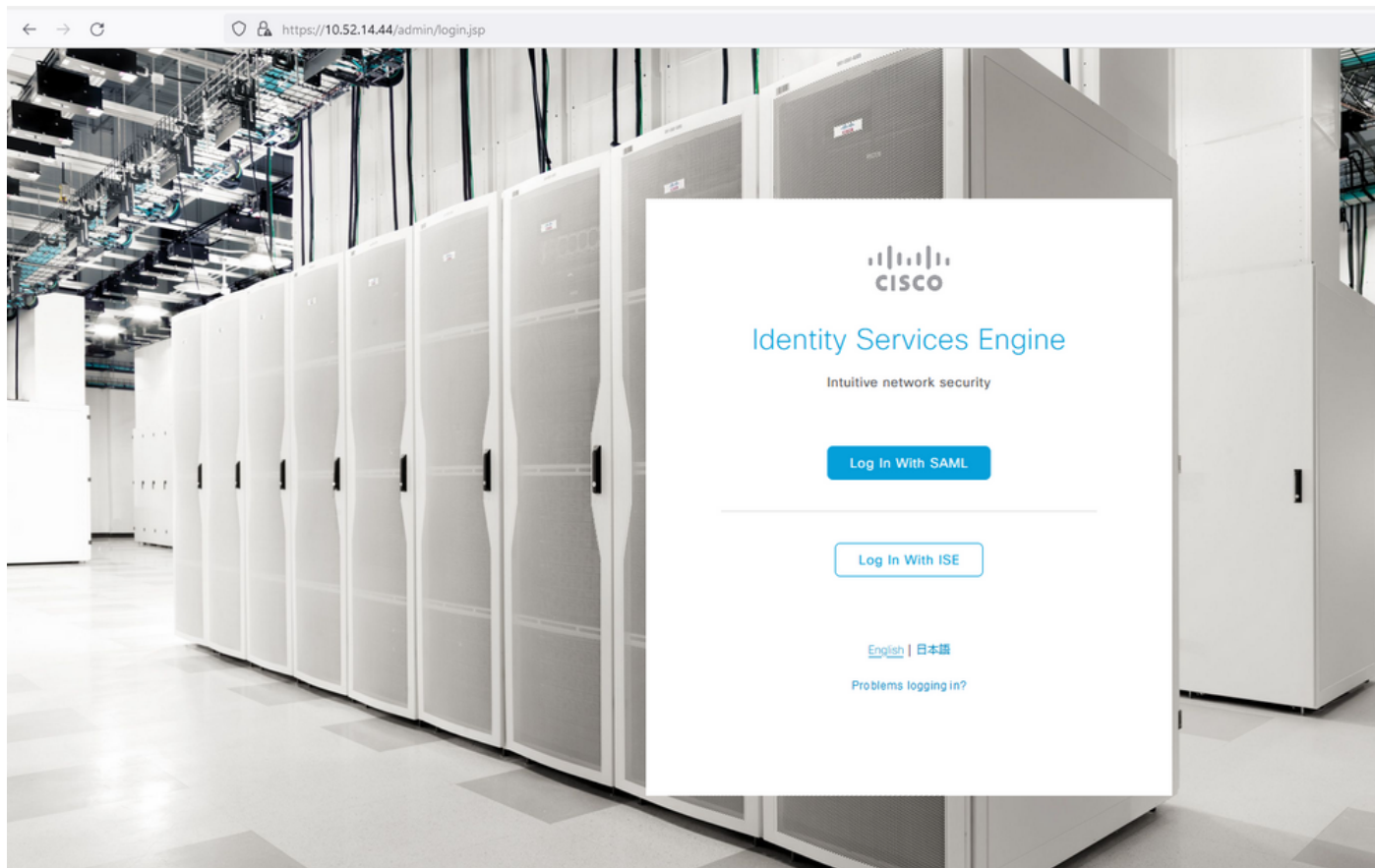
Import Identity Provider Config File ⓘ

Provider Id

驗證

測試與Duo SSO的整合

1. 登入到Cisco ISE管理面板，然後按一下**Log In With SAML**。

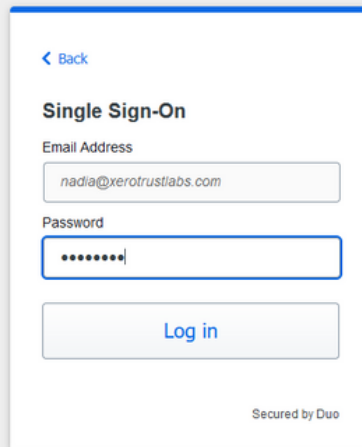


2. 已重定向到「SSO」頁，輸入電子郵件地址並按一下下一步。



The image shows a web browser window displaying a Cisco Single Sign-On page. At the top left is the Cisco logo. Below it, the text "Single Sign-On" is displayed. Underneath, there is a label "Email Address" followed by a text input field containing the email address "nadia@zerotrustlabs.com". Below the input field is a button labeled "Next". At the bottom right of the form, it says "Secured by Duo".

3. 輸入口令並按一下**Log in**。

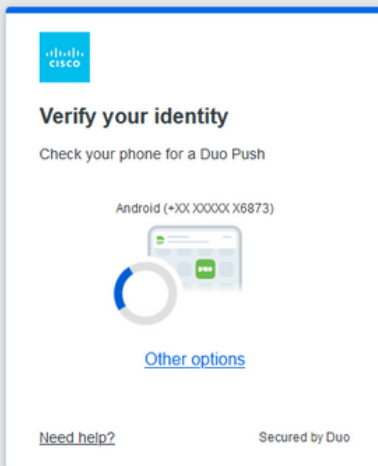


The image shows a web browser window displaying a Cisco Single Sign-On page. At the top left is a blue arrow pointing left with the text "Back". Below it, the text "Single Sign-On" is displayed. Underneath, there is a label "Email Address" followed by a text input field containing the email address "nadia@zerotrustlabs.com". Below that is a label "Password" followed by a password input field with masked characters "*****". Below the password field is a button labeled "Log in". At the bottom right of the form, it says "Secured by Duo".

4. 您的行動裝置上會出現Duo Push提示。

Duo needs your help

[Take a quick 6-question survey](#) to help us improve this experience.



The image shows a white rectangular box with a blue border, representing a Duo authentication prompt. At the top left is the Cisco Duo logo. The main heading is "Verify your identity" in bold. Below it, the instruction "Check your phone for a Duo Push" is displayed. A phone number "Android (+XX XXXXX X6873)" is shown above an illustration of a smartphone with a Duo push notification. Below the phone illustration is a blue circular progress indicator and a link for "Other options". At the bottom left is a "Need help?" link, and at the bottom right is the text "Secured by Duo".

5. 接受提示後，您將獲得一個窗口，並自動重定向到ISE管理員頁面。

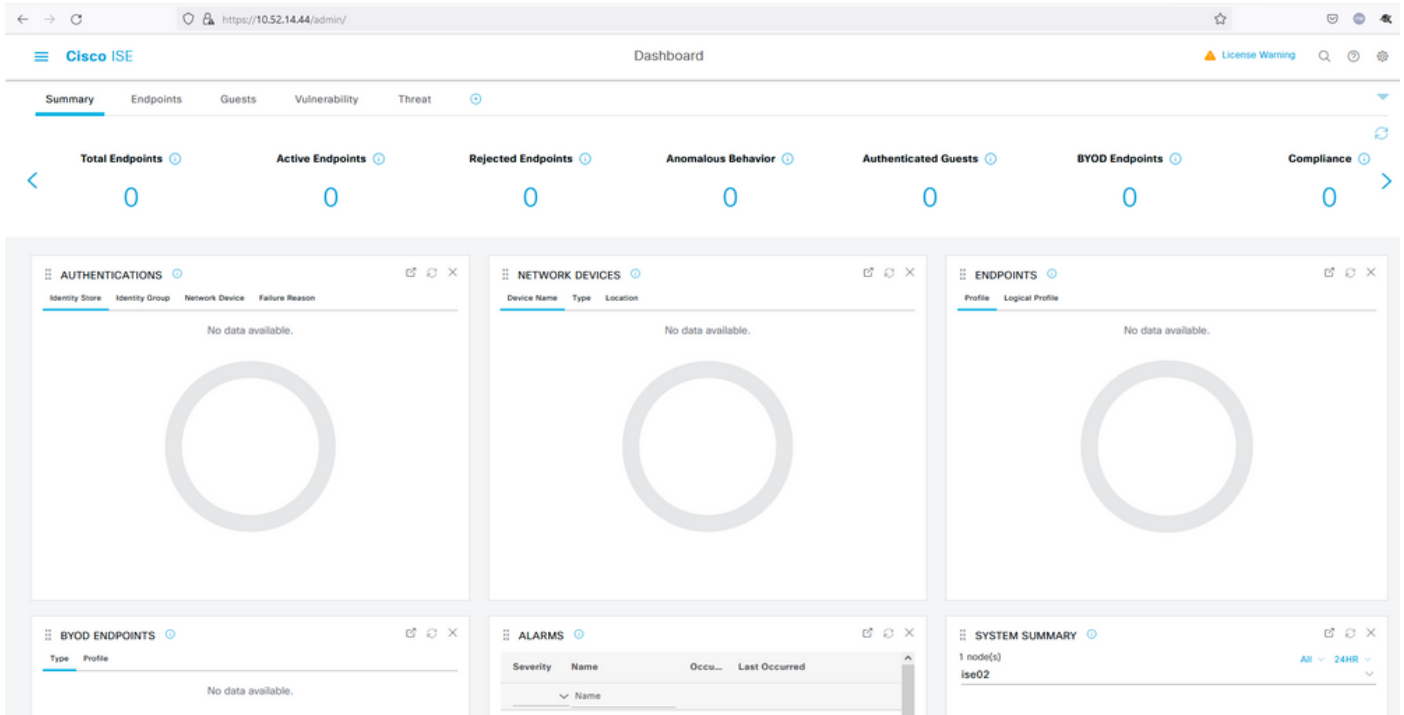


Success!

Logging you in...



Secured by Duo



疑難排解

- 下載Mozilla FF <https://addons.mozilla.org/en-US/firefox/addon/saml-tracer/>的SAML Tracer副檔名。
- 捲動至SSOLoginResponse.action封包。在SAML頁籤下，您將看到從Duo SAML傳送的一些屬性：NameID、Recipient (AssertionConsumerService Location URL)和Audience(EntityID)。

```

GET https://zerotrustlabs.login.duosecurity.com/pw/ASOOZM6KCLX6T19QVNA3/ssp_callback?aid=643b5067d1f249f5bf6d744a7603ef83&req-trace-group=dfac3f2db
GET https://zerotrustlabs.login.duosecurity.com/favicon.ico
POST https://10.10.10.10:8443/portal/SSOLoginResponse.action SAML
GET https://10.10.10.10:8443/portal/css/images/favicon.ico
POST https://10.10.10.10:8443/admin/LoginAction.do
GET https://10.10.10.10:8443/admin/
GET https://10.10.10.10:8443/admin/ng/css/vendor/bootstrap/css/bootstrap-dialog.css
GET https://10.10.10.10:8443/admin/ng/css/vendor/fuelux/css/fuelux.min.css
GET https://10.10.10.10:8443/admin/ng/css/vendor/jstree/css/style.min.css
GET https://10.10.10.10:8443/admin/ng/css/vendor/select2/select2.min.css
GET https://10.10.10.10:8443/admin/lib/cpm/widget/themes/default/combobox.css
GET https://10.10.10.10:8443/admin/lib/cpm/widget/themes/default/textboxsubmitter.css
GET https://10.10.10.10:8443/admin/lib/cpm/widget/themes/default/expressionbuilder.css
GET https://10.10.10.10:8443/admin/lib/cpm/widget/themes/default/saveprogressindicator.css
GET https://10.10.10.10:8443/admin/lib/cpm/widget/themes/default/table/treetable.css
GET https://10.10.10.10:8443/admin/lib/cpm/widget/themes/default/table/pagetable.css
GET https://10.10.10.10:8443/admin/pages/utills/css/common_icons.css
GET https://10.10.10.10:8443/admin/pages/utills/css/common_styles.css

```

HTTP Parameters SAML Summary

```

<ds:X509Data>
<ds:X509Certificate>MIIDDTCCAfwAwIBAgIUCbf+LB1BLJMeF6GVOB1rmdX3AVEwDQYJKoZIhvcNAQELBQAwNjEVMGMGA1UECgwMRHRVIFN1Y3VyaXR5MR0wGwYDVQDD
BRESTZPODg2UkxETUJZMzExSFBJMjEwFw0zODAxMTkwMzE0MDdaMDYxFTATBgNVBAoMMDER1byBTZWN1cm10eTEdMBsGA1UEAwwUREk2Tzg4N1JMRE
1CWTMxMuhQSTIwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDB03Ayuh9avw0NoQzIhQZzu9H8vu/HSKLSH30585Mukj5FnoVV50PGTuoFN4u90t
sIFULjC8eQnUsBR1PYQ5jt0V23qVnvoGyqsuHAs8nbKwvzpzShzNF59p03pXkoGPuB+Du2Irrvv0opSv4vbrgKV+H/bvMqyhIA6ywfHNZedG7pbwrYBtVPDXUpnLQvtL2
/Vd9230XuXHF+k32hagRgTLub5XyT1HHQ8b4n3mQKHs6yA/KNvaB3b/AMUqAXDqaEXNG0uQENMK30wTs49
/w+r5fz7xp66muRc0IBg3xjWnnFnyujy7v5ifn1KFUFQu+86A5GbuUWUyiaKmV7CztAgMBAAGjEzARMA8GA1UdEwEB
/wQFMAMBAf8wDQYJKoZIhvcNAQELBQADggEBAH+KItcw0KtDxXBvZ5S+25a+50F4Tqd/pHh56i19d2kDxInSUVsy
/Yy1FXAWge3WBke4b3JR7znD6000sZTYbF9w7H4svU2gxzdk0znXJNj2e4C5fDivnj/TawZakp2MbTaxfV2VTL0K0kV/1jM6PL61PbKGFwNmh+SjW/VseS+71C701eI
/U095XLbAu2iIny9zfv0hKNV72L8fgYgrjhpdxH8Y1SxPbVWZMwzytbwZFUogD30XrPq16aXZvJyOH5Vs0H90wQ8Qq48hI4F4J3DyRPNH1PzQTYM38kjymEkE0DJPcaGy9v
EMinHUkdwpiETB52Cmtwg+DzAw1jpc=</ds:X509Certificate>
</ds:X509Data>
<ds:KeyInfo>
</ds:KeyInfo>
</ds:Signature>
<saml:Subject>
<saml:NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified">nadia</saml:NameID>
<saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
<saml:SubjectConfirmationData NotOnOrAfter="2021-12-02T04:48:56Z"
Recipient="https://10.10.10.10:8443/portal/SSOLoginResponse.action"
InResponseTo="_7fdfc239-631e-439c-a3ab-f5e56429779d_SEMIportalSessionId_EQUALS859ee9c3-60e4-4482-9426-
b3904d4d6226_SEMItoken_EQUALS1RS257BC24SGVHZW76GMVEZNR0YCCCL_SEMI_DELIMITER10."/>
</saml:SubjectConfirmation>
</saml:Subject>
<saml:Conditions NotBefore="2021-12-02T04:43:26Z"
NotOnOrAfter="2021-12-02T04:48:56Z"
>
<saml:AudienceRestriction>
<saml:Audience>http://CiscoISE/7fdfc239-631e-439c-a3ab-f5e56429779d</saml:Audience>
</saml:AudienceRestriction>
</saml:Conditions>
<saml:AuthnStatement AuthnInstant="2021-12-02T04:43:56Z"
SessionIndex="DUO_8dfe494ab8d617884446cb8f2259bb4a56492ef"
>
</saml:AuthnStatement>
</saml:AuthnContext>

```

1846 requests received (490 hidden)

- ISE即時登入：

Steps

5231 Guest Authentication Passed

Overview

Event	5231 Guest Authentication Passed
Username	nadia
Endpoint Id	
Endpoint Profile	
Authorization Result	

Authentication Details

Source Timestamp	2021-11-28 15:36:03.59
Received Timestamp	2021-11-28 15:36:03.59
Policy Server	ise02
Event	5231 Guest Authentication Passed
Username	nadia
User Type	NON_GUEST
Authentication Identity Store	Duo_SSO
Identity Group	Any
Authentication Method	PAP_ASCII
Authentication Protocol	PAP_ASCII

Other Attributes

ConfigVersionId	79
IpAddress	10.65.48.163
PortalName	ISE Portal (default)
PsnHostName	ise02.xerotrustlabs.com
GuestUserName	nadia

- ISE上的管理登入日誌：使用者名稱：samlUser。

- Export Summary
- My Reports
- Reports
- Audit
 - Adaptive Network Control
 - Administrator Logins
 - Change Configuration Audit
 - Cisco Support Diagnostics
 - Data Purging Audit
 - Endpoint Purge Activities
 - Internal Administrator Sum...
 - Policy OpenAPI Operations
 - Operations Audit
 - psGrid Administrator Audit
 - Secure Communications A...
 - TrustSec Audit
 - User Change Password Au...
- Device Administration
- Diagnostics
- Endpoints and Users
- Guest
- Threat Control NAC
- TrustSec
- Scheduled Reports

Administrator Logins

From 2021-11-28 00:00:00 To 2021-11-28 18:38:10

Reports reported in last 7 days

Add to My Reports Export To Schedule

Logged At	Administrator	IP Address	Server	Event	Event Details
Today	Administrator		Server		
2021-11-28 18:38:08.199		10.85.48.183	18492	Administrator authentication succeeded	Administrator authentication successful

Rows/Page 1 1 Total Rows

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）。