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

本文檔介紹如何配置Cisco ISE 3.1 SAML SSO與外部身份提供商（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。

服務提供商(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商之間的標準化通訊。SAML是使用者身份身份驗證與使用服務的授權之間的鏈路。

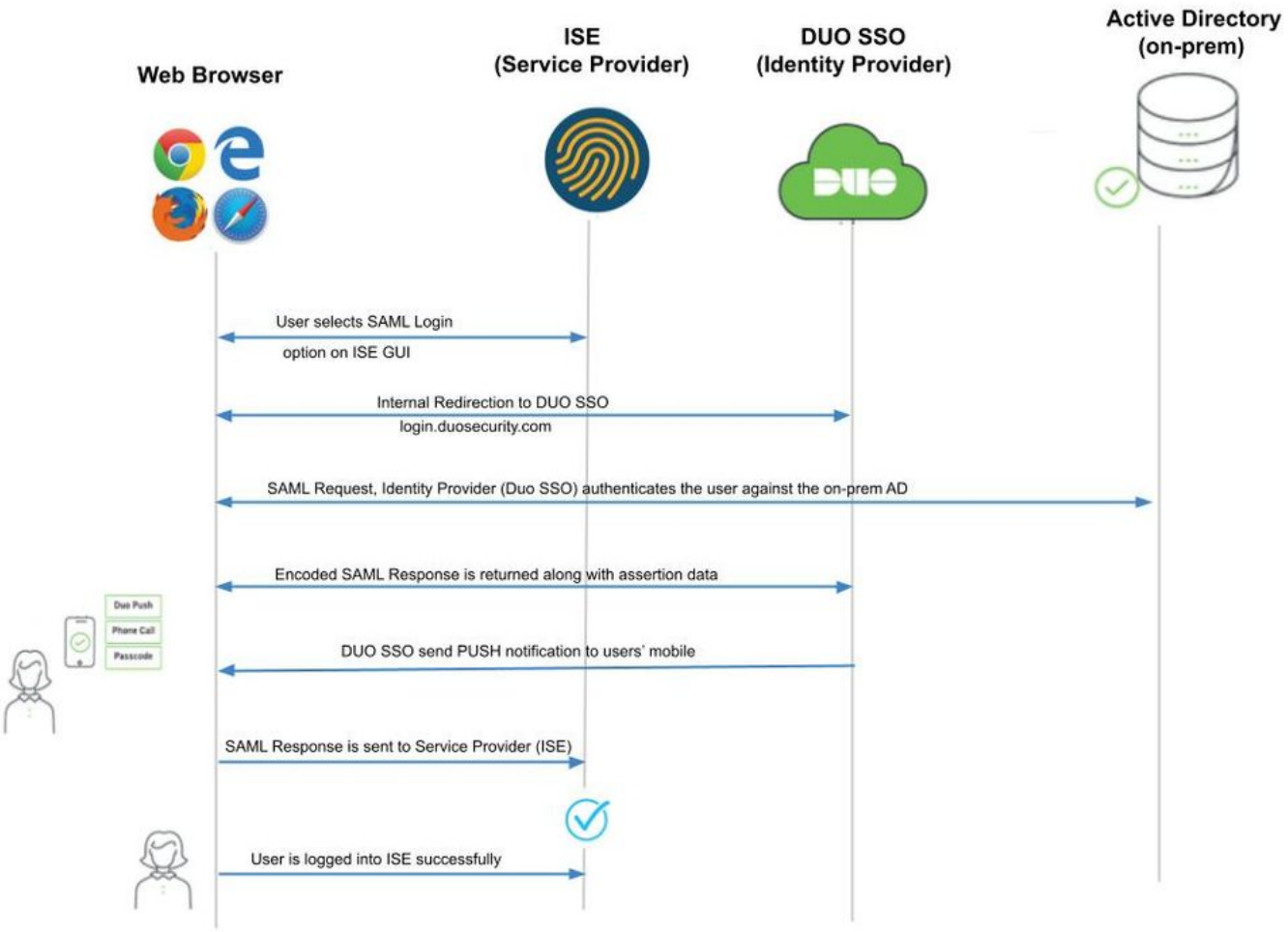
SAML斷言

SAML Assertion是IdP傳送到包含使用者授權的服務提供商的XML文檔。有三種不同型別的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

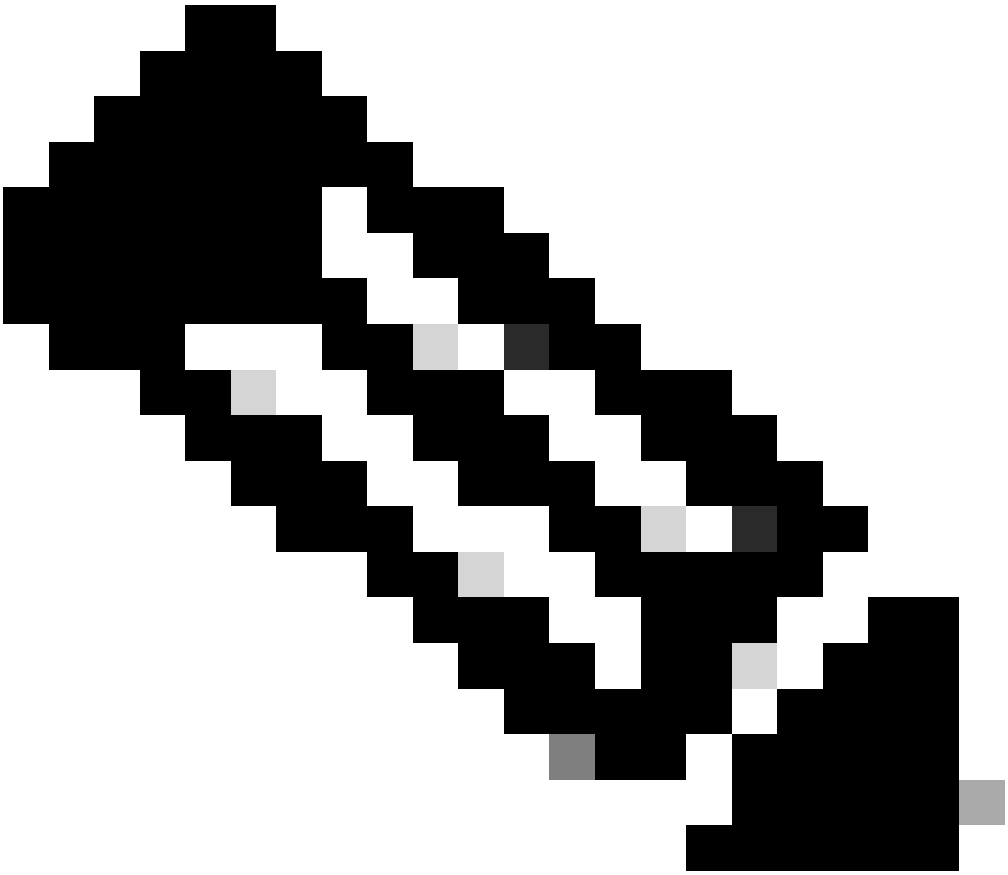
（例如，Kerberos、雙因素等）。
- 歸屬斷言將SAML屬性（提供有關使用者資訊的特定資料）傳遞給SP。
- 授權決策斷言宣告使用者是否獲得授權以便使用該服務，或者IdP是否由於密碼失敗或缺少對服務的許可權而拒絕其請求。

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。

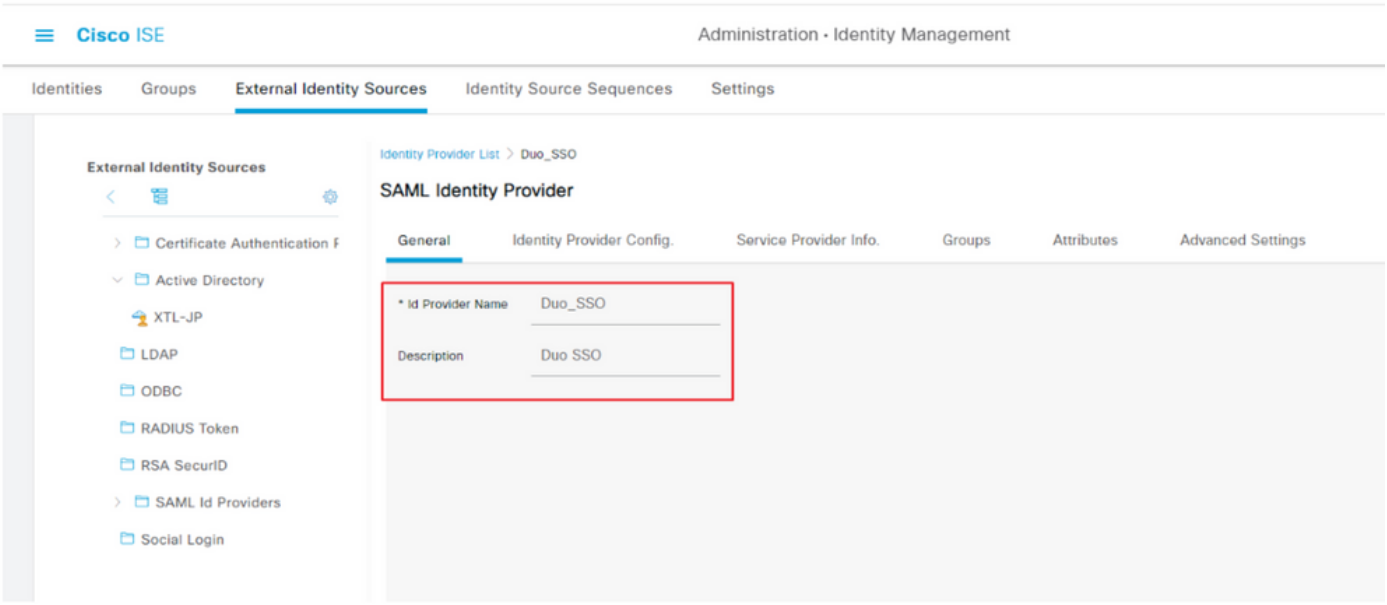
設定與Duo SSO整合的SAML SSO

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：

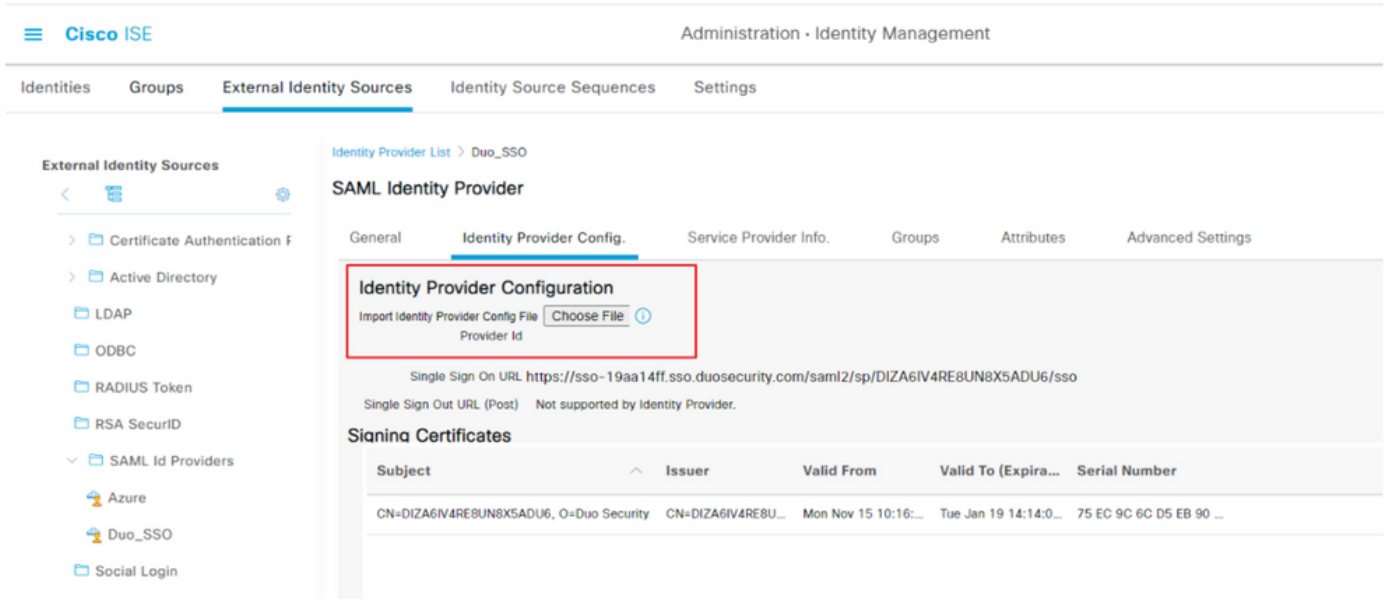


從Duo管理門戶導入SAML後設資料XML檔案

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。）

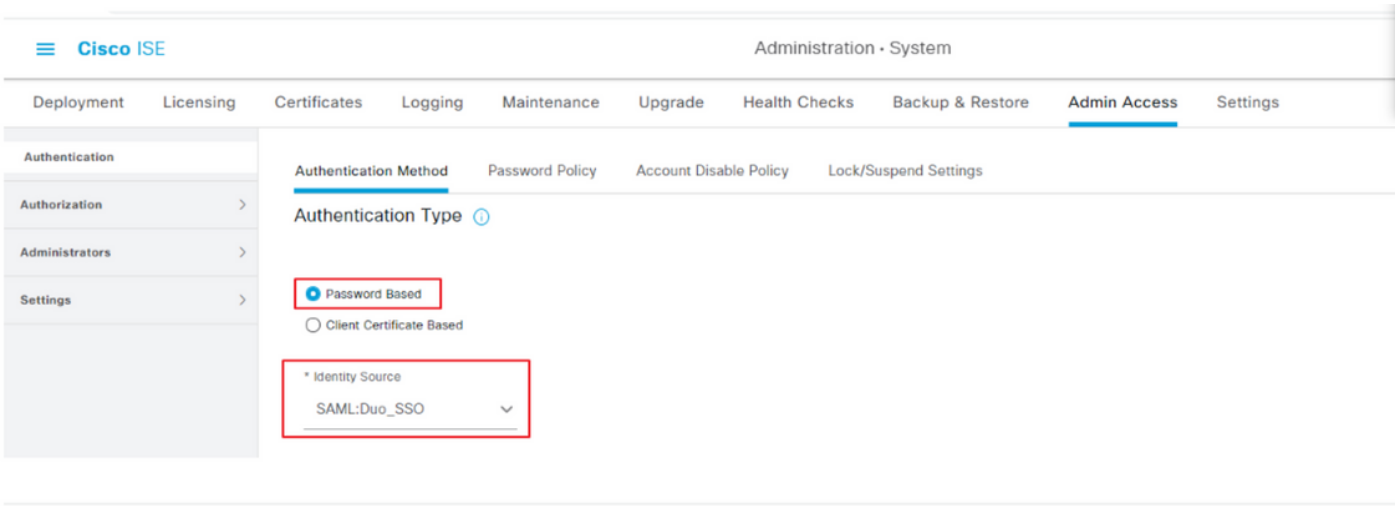
SSO URL和簽名證書包括：



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

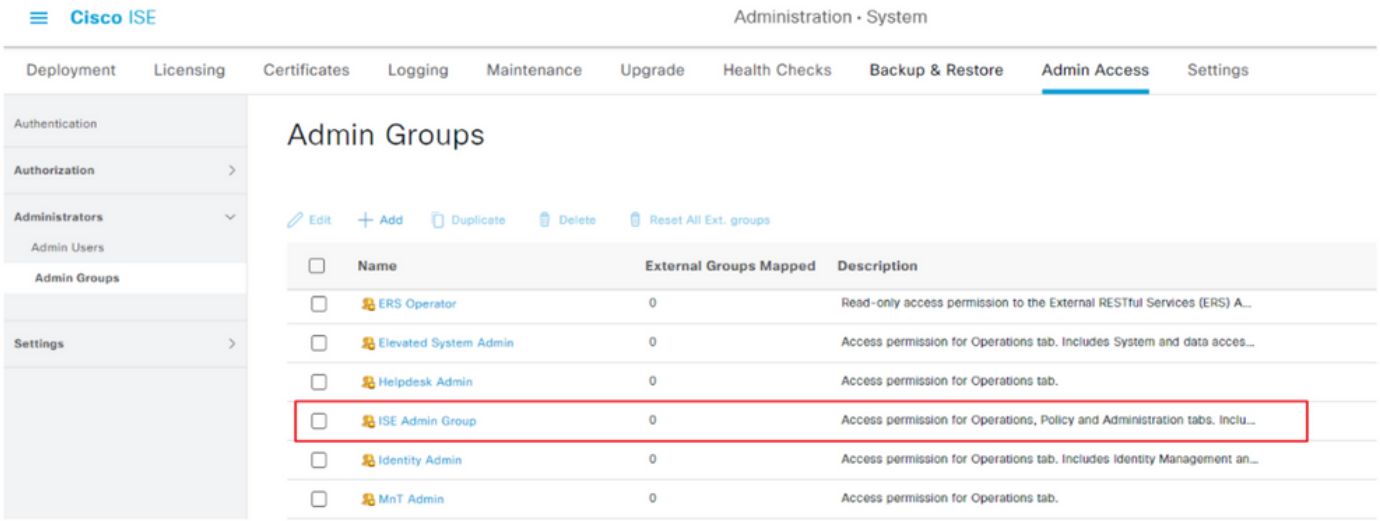
Identity Source下拉式清單中選擇先前建立的必要IdP名稱，如下圖所示：



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。

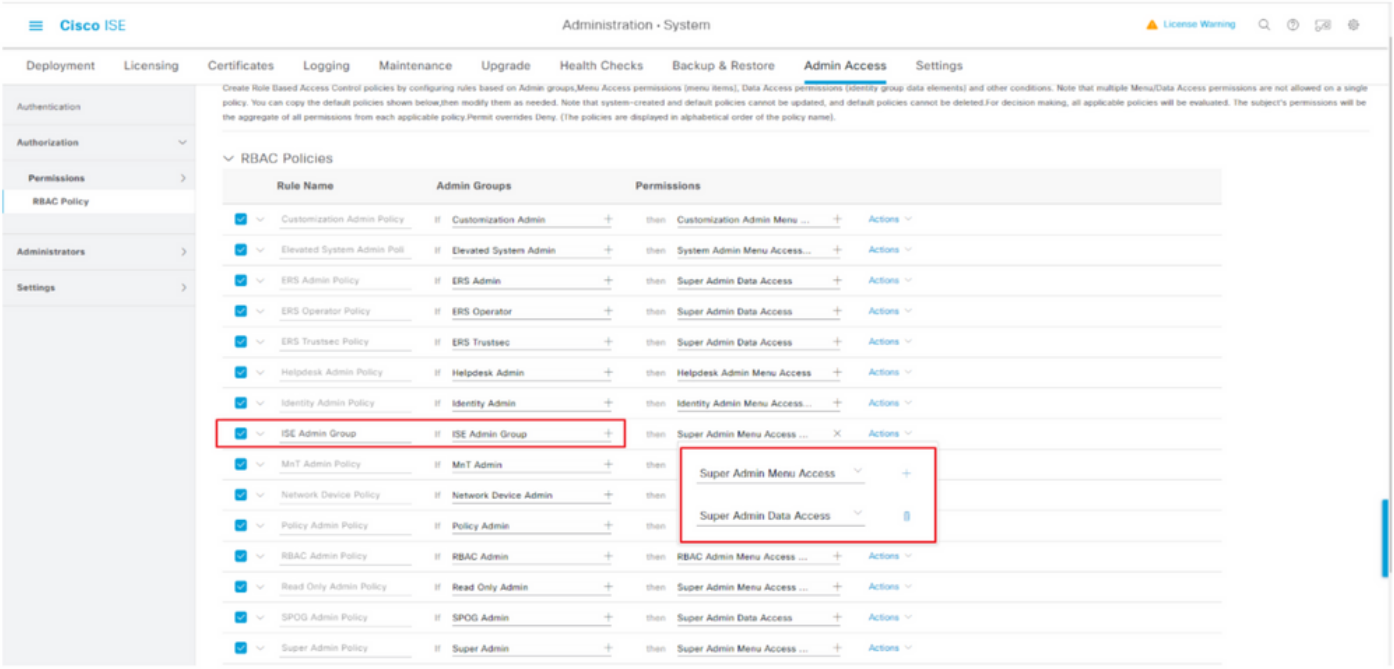
這會為Admin組提供Super Admin許可權。



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。

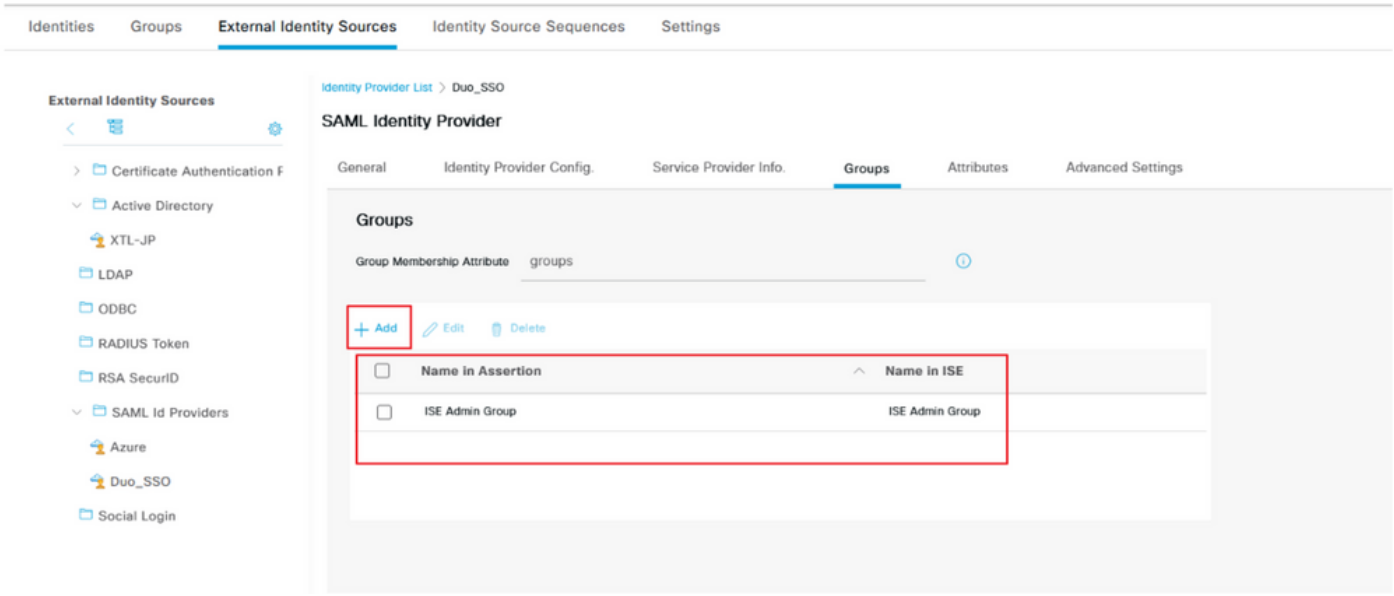
存取許可權與超級管理員原則相同。



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。

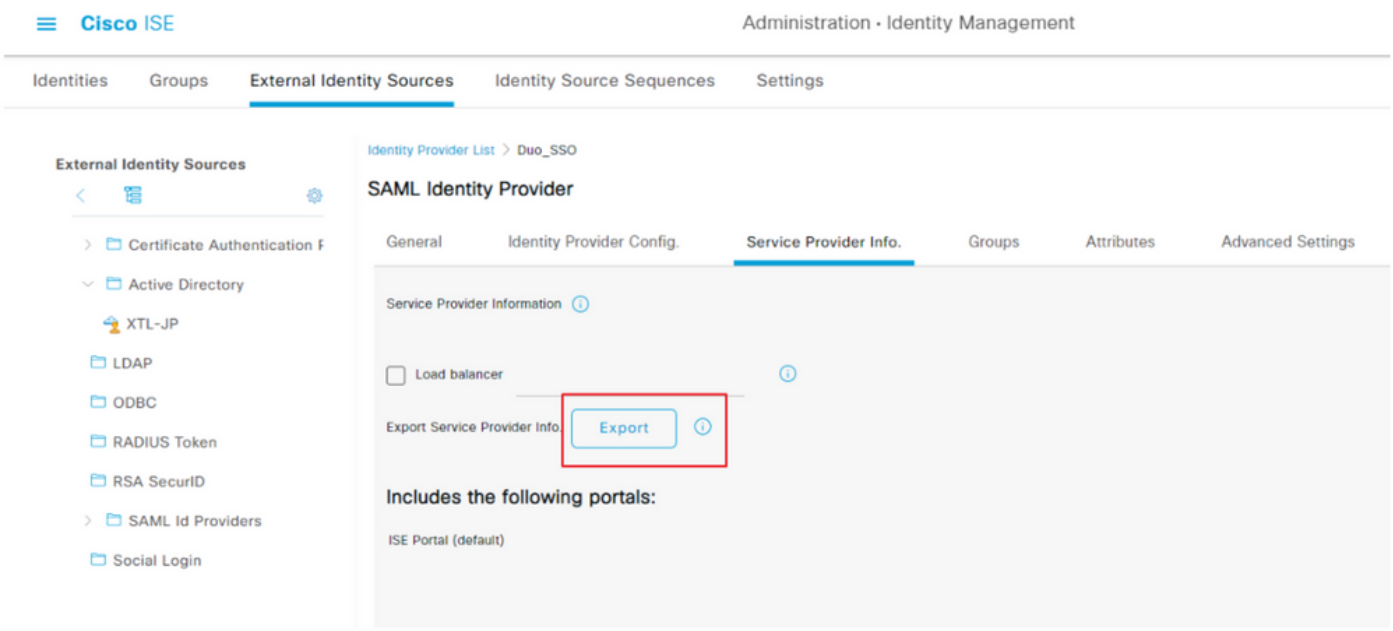
在斷言中增加名稱（ISE管理員組的名稱），然後從下拉選單中選擇所建立的基於角色的訪問控制(RBAC)組（第4步），然後按一下**Open**以儲存它。SSO URL和簽名證書會自動填充：



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

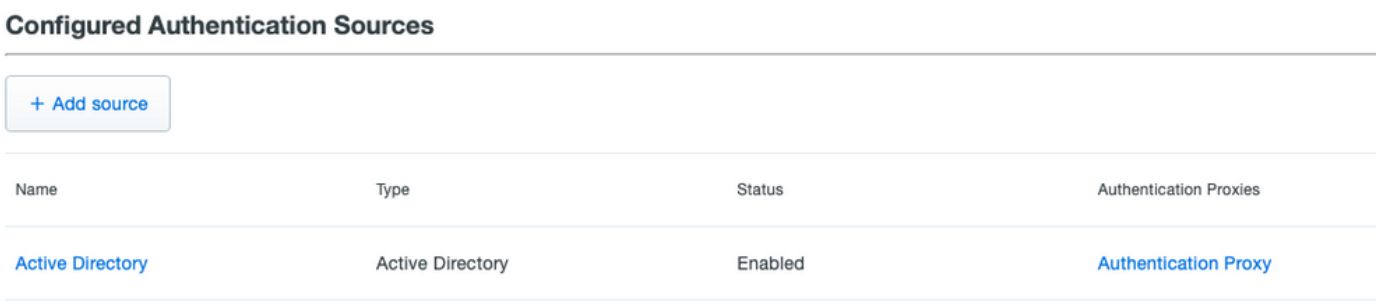
entityID = http://CiscoISE/7fdfc239-631e-439c-a3ab-f5e56429779d。

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。

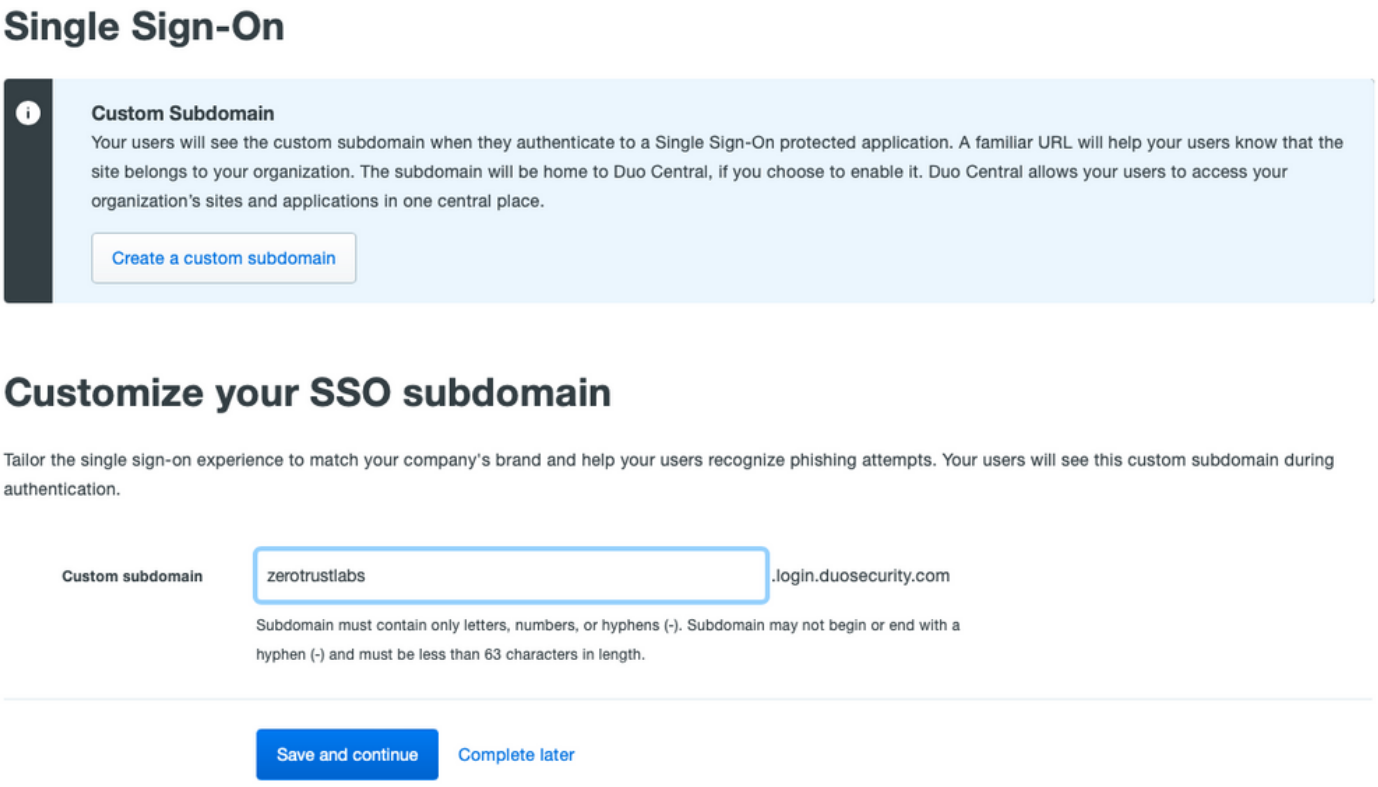
AssertionConsumerService位置= https://isenodename.com:8443/portal/SSOLoginResponse.action，其中isenodename是在XML檔案（位置）中找到的實際ISE FQDN名稱。

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。



選中此KB以啟用自定義域的SSO。

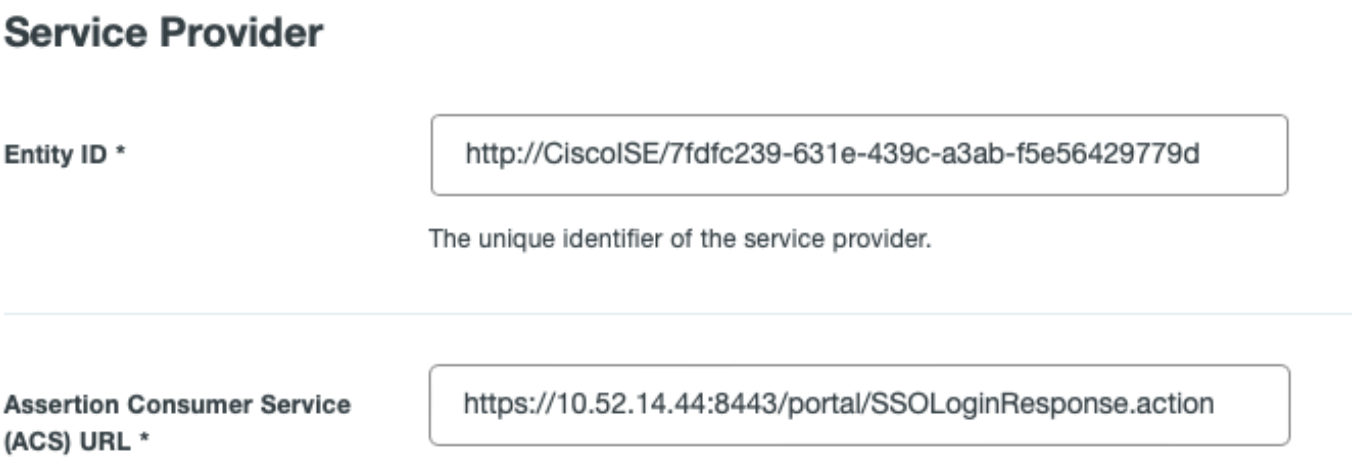


步驟 3.將Cisco ISE與Duo SSO整合為通用SP

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

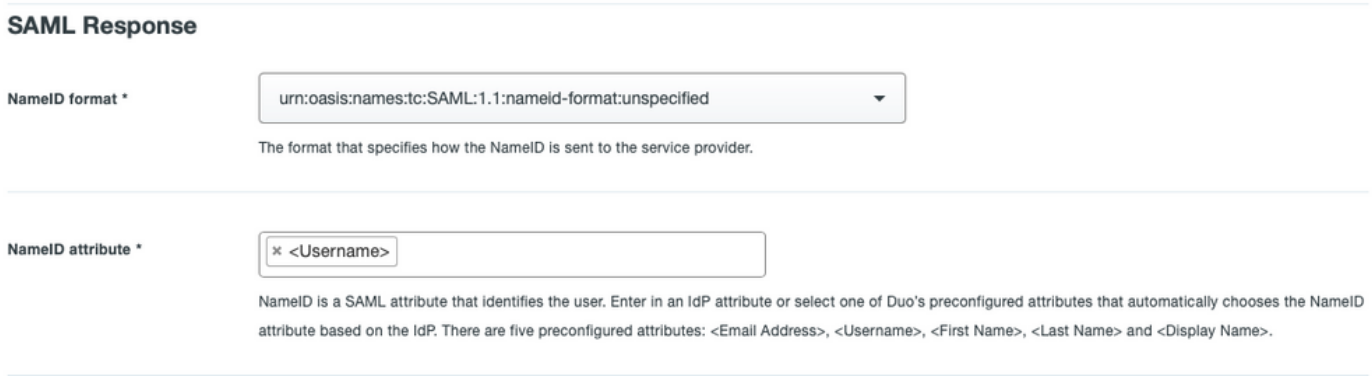
在Duo管理面板中配置通用SP的Cisco ISE SP詳細資訊：

名稱	說明
實體ID	http://CiscoISE/7fdfc239-631e-439c-a3ab-f5e56429779d
宣告使用者服務(ACS) URL	https://10.x.x.x:8443/portal/SSOLoginResponse.action

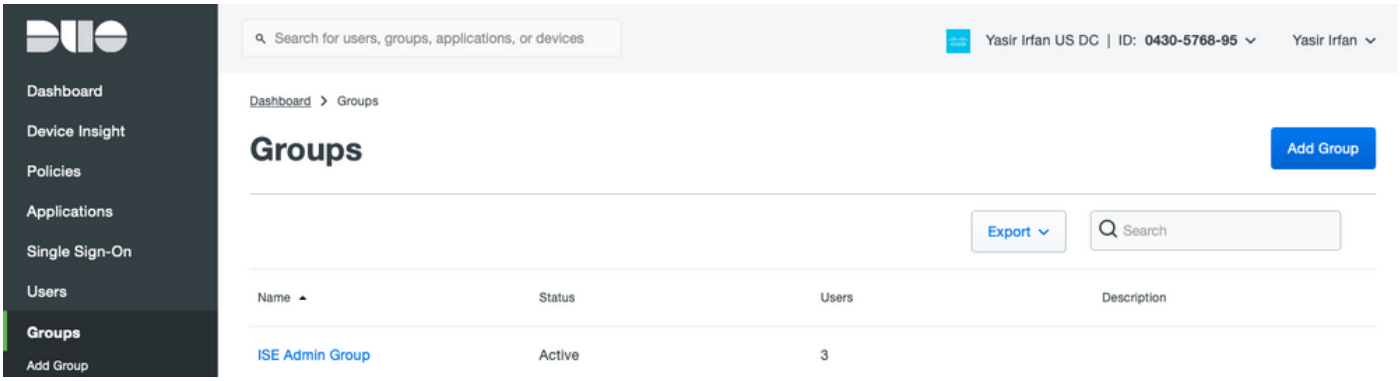


配置思科ISE的SAML響應：

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

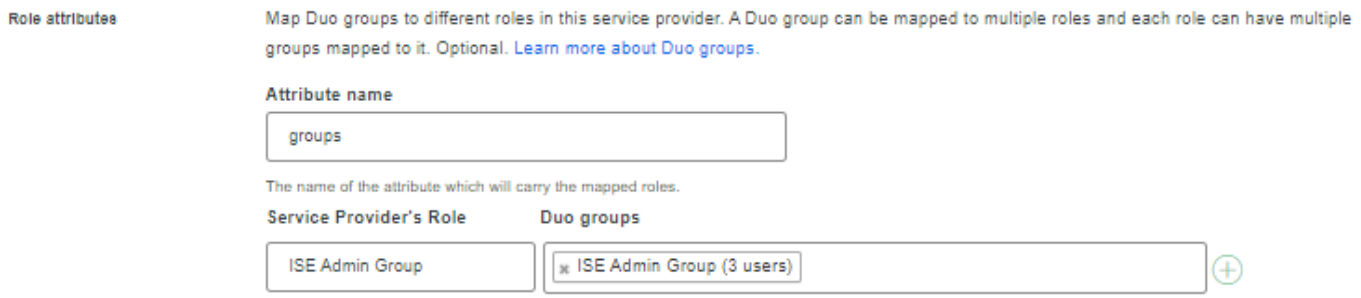


在Duo Admin Panel中建立名為Cisco Admin Group的組，並將ISE使用者增加到此組，或在Windows AD中建立組並使用目錄同步功能將其同步到Duo Admin面板。

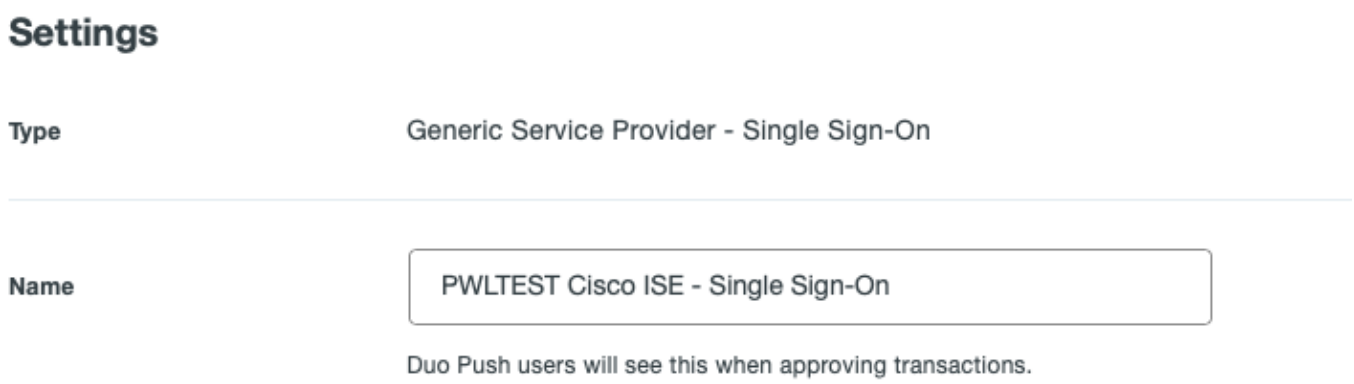


配置思科ISE的角色屬性：

名稱	說明
屬性名稱	群組
SP角色	ISE管理組
Duo組	ISE管理組

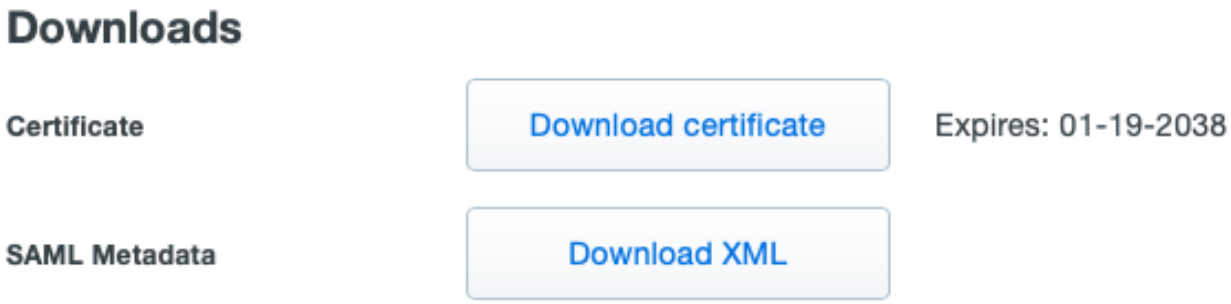


在Settings部分的**Name**頁籤中，為此整合提供相應的名稱。



按一下**Save**按鈕儲存配置，並參閱此KB以瞭解更多詳細資訊。

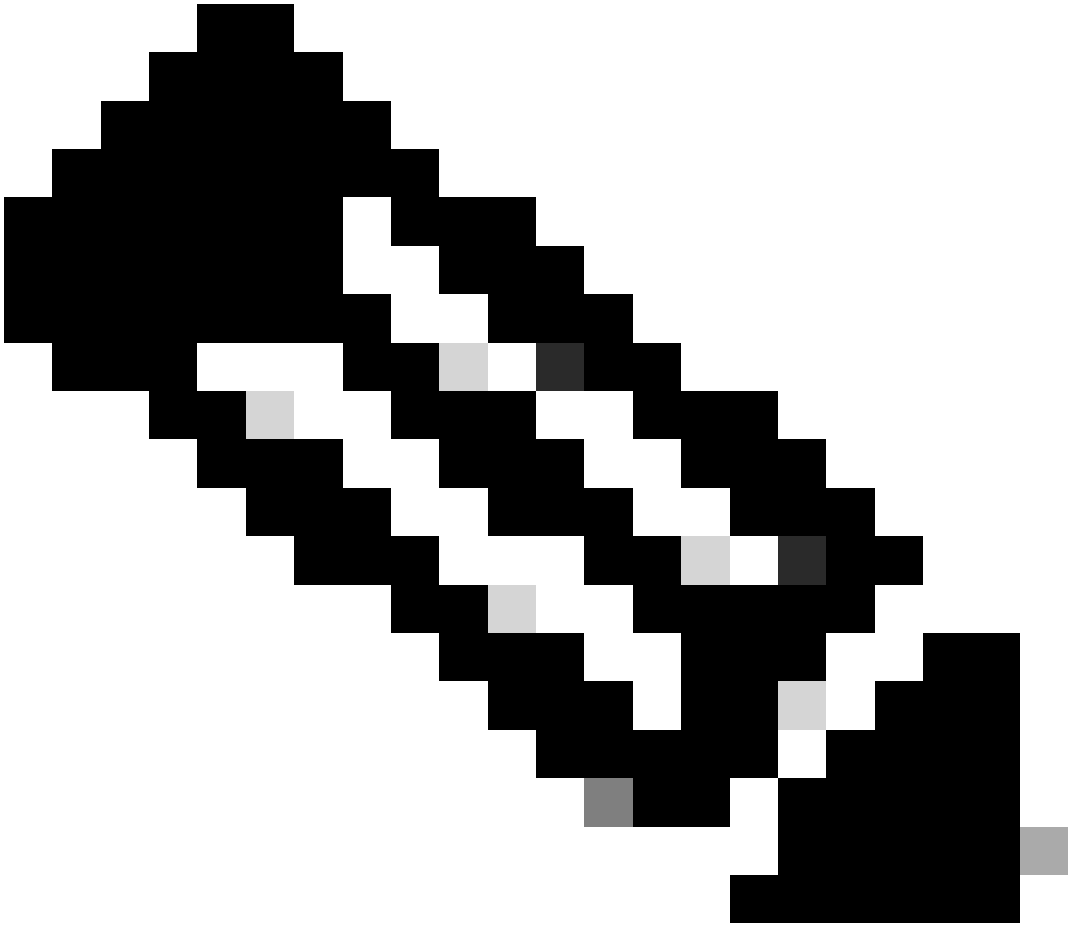
按一下**Download XML**以下載SAML後設資料。



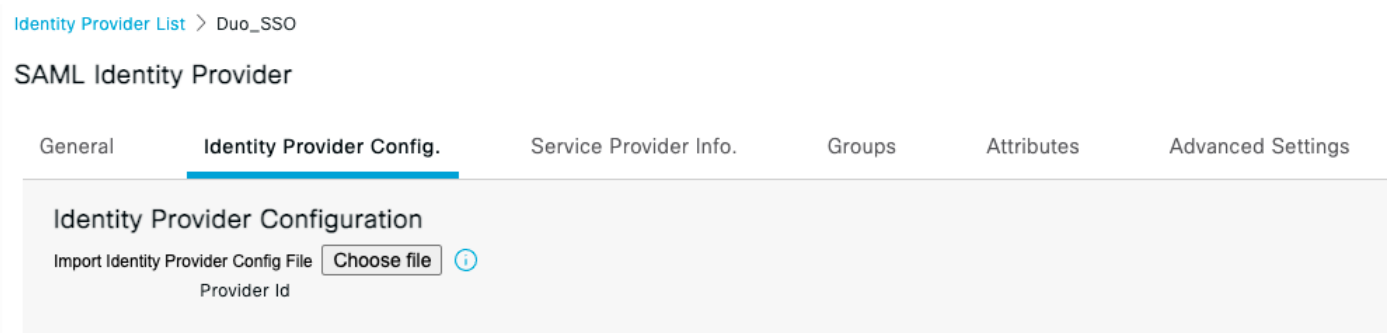
導航至Administration > Identity Management > External Identity Sources > SAML Id Providers > Duo_SSO，將SAML MetaData下載從Duo管理面板上傳到Cisco ISE。

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**。



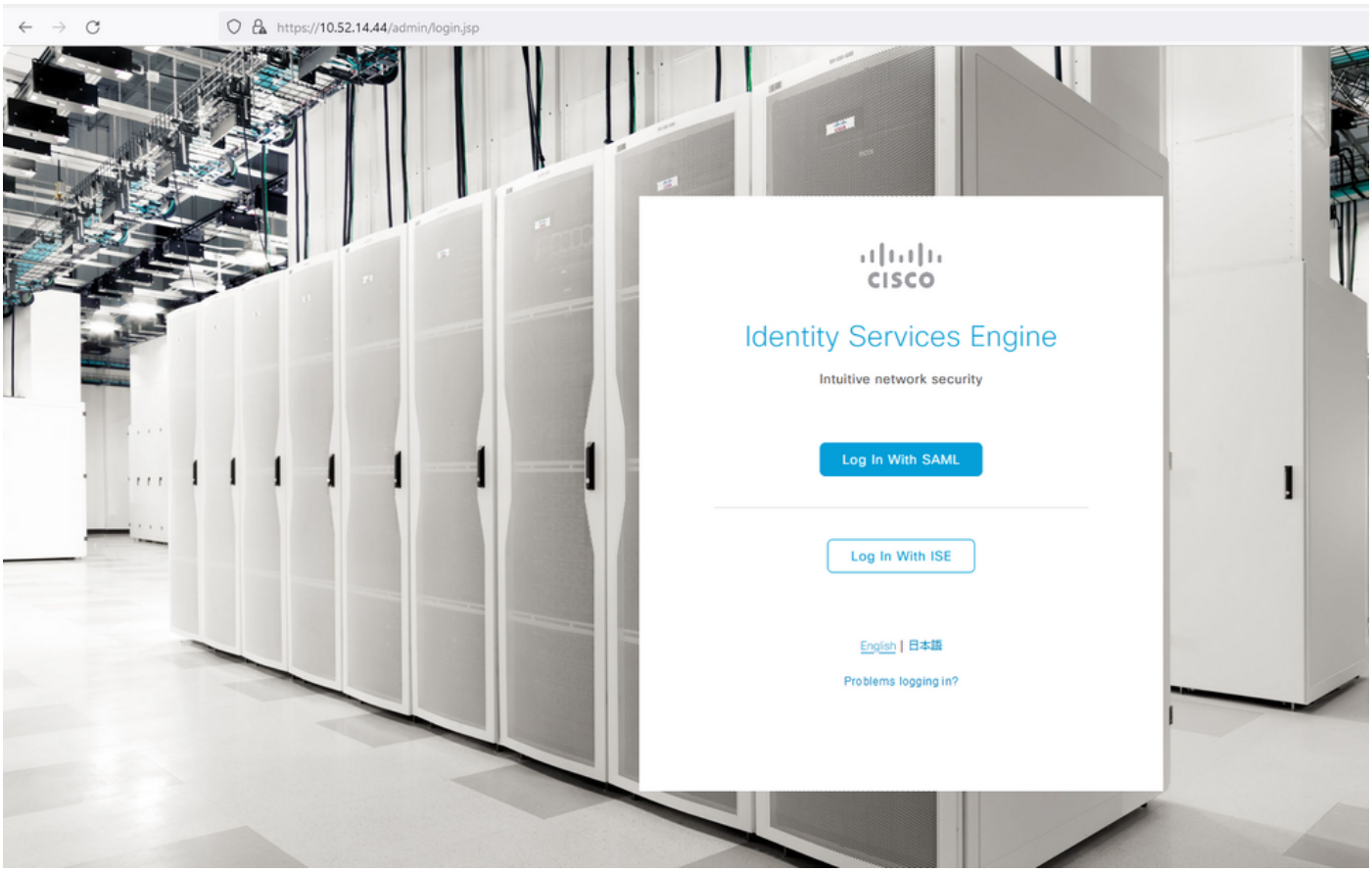
注意：此步驟在配置SAML SSO與Duo SSO整合的部分中提到；第2步。從Duo Admin門戶導入**SAML後設資料XML檔案。**



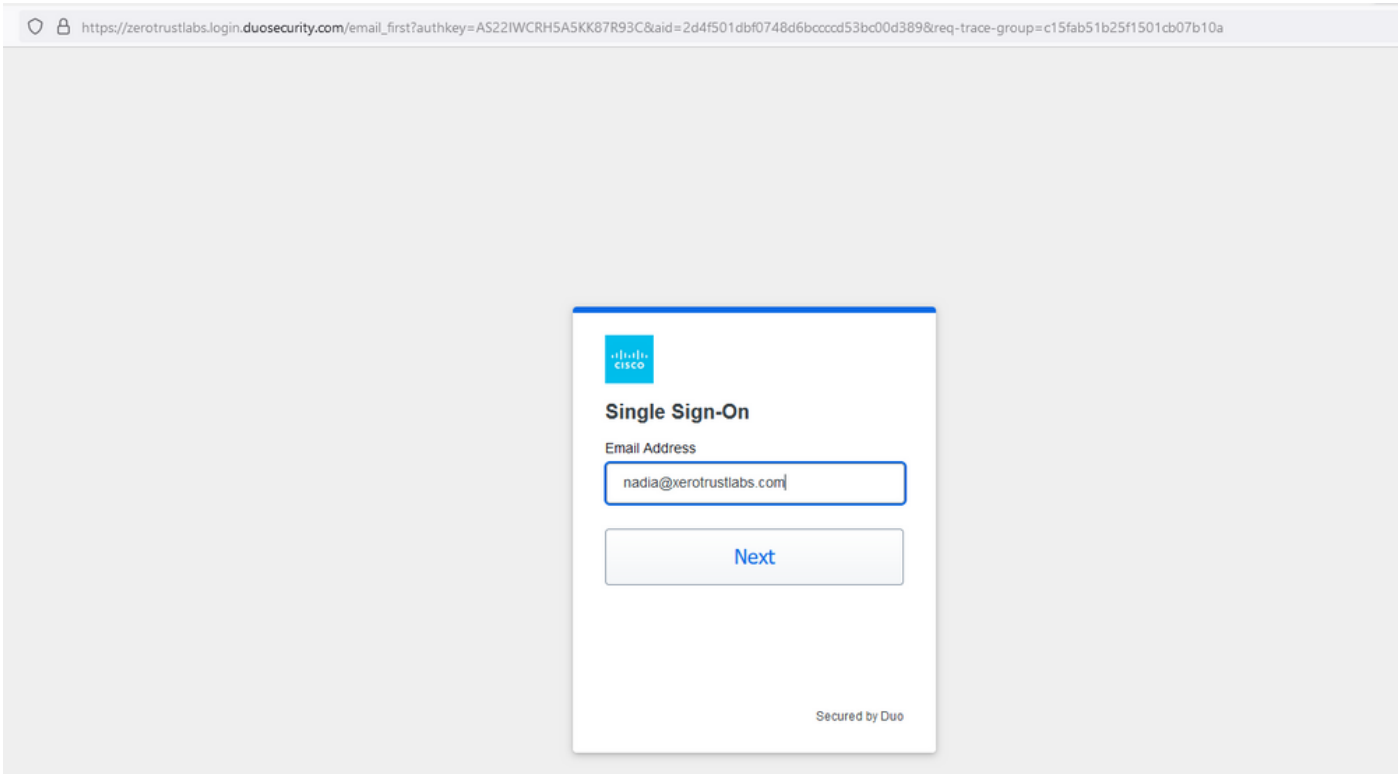
驗證

測試與Duo SSO的整合

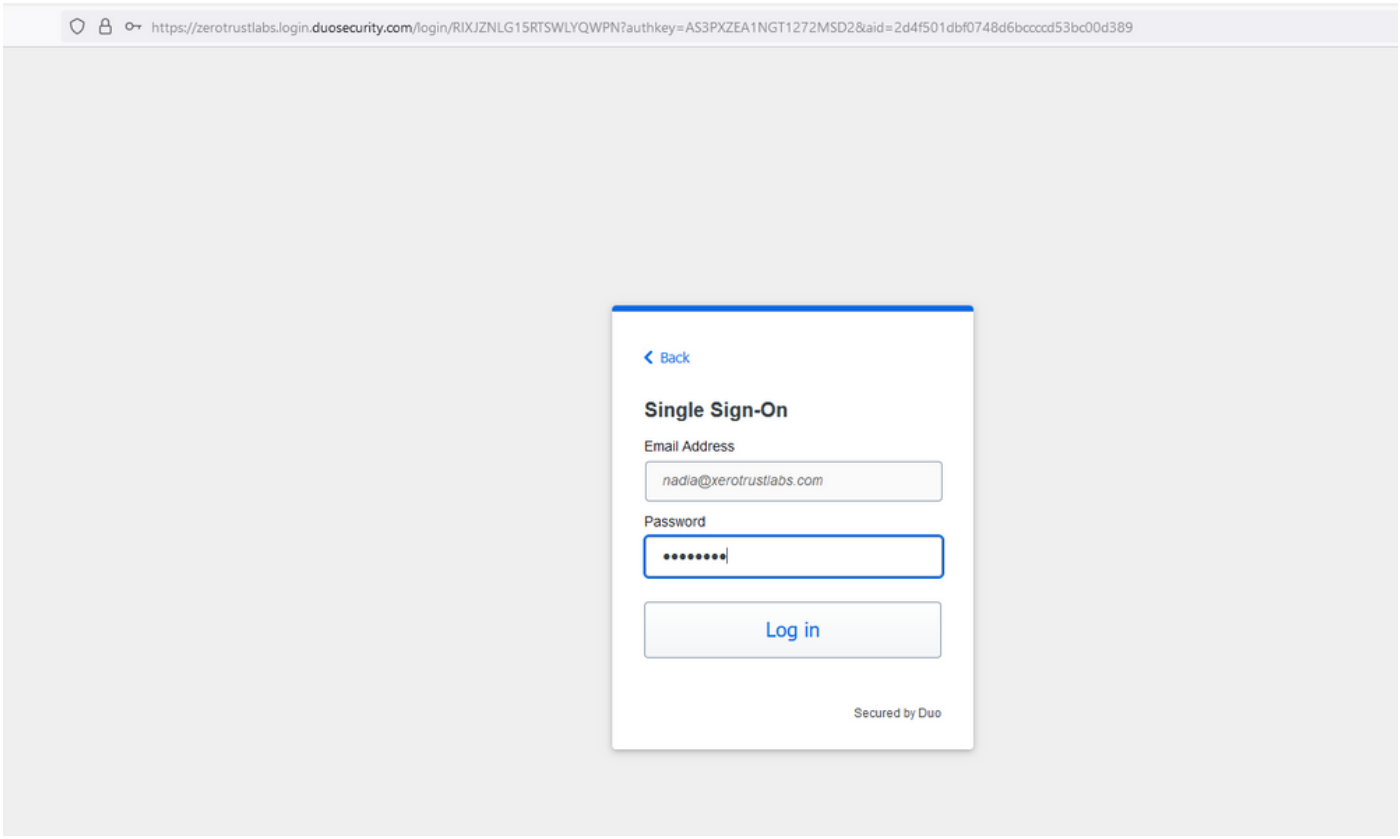
1. 登入到**Cisco ISE管理面板**，然後按一下**Log In** With SAML。



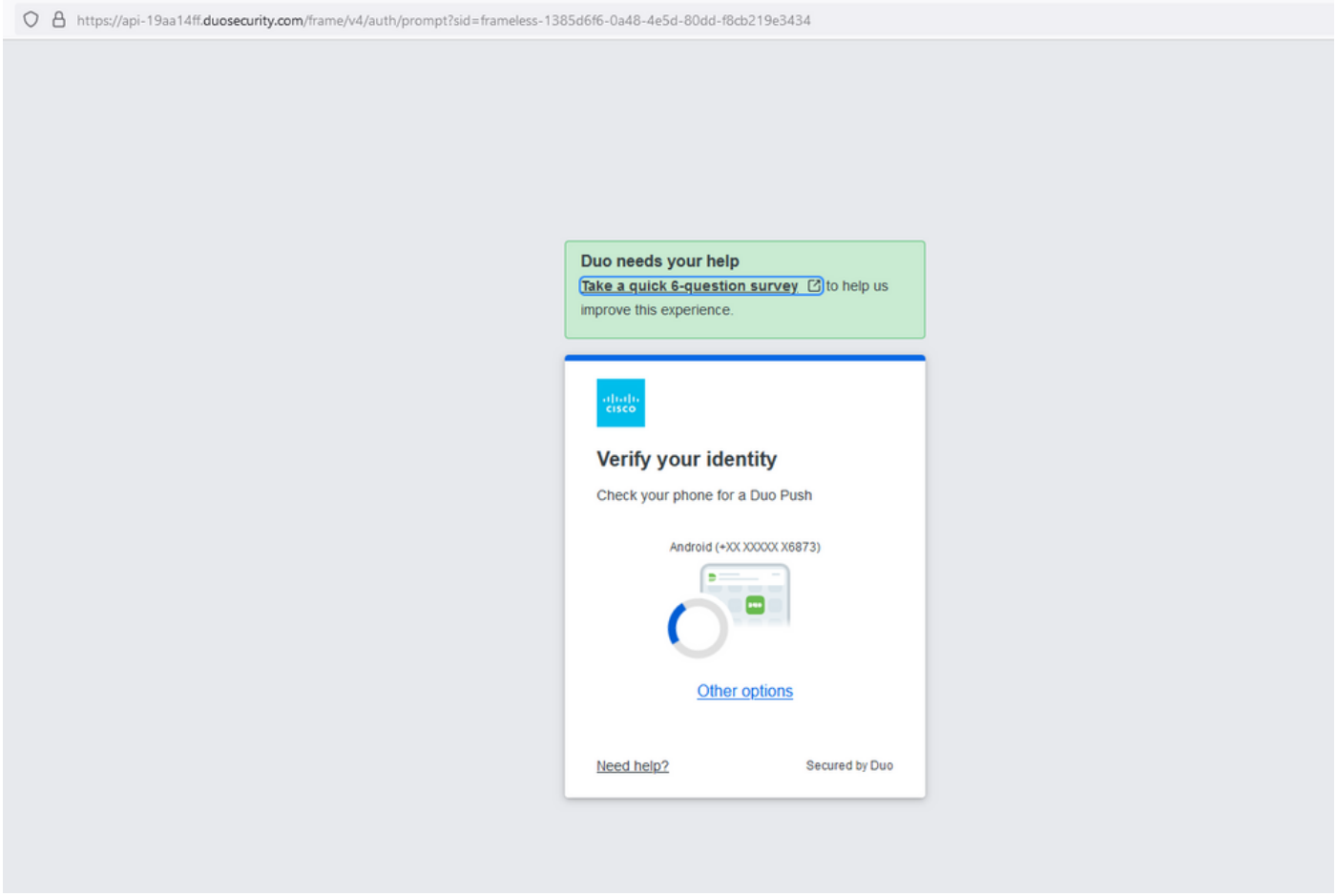
2. 已重定向到「SSO」頁，輸入**電子郵件地址**並按一下**下一步**。



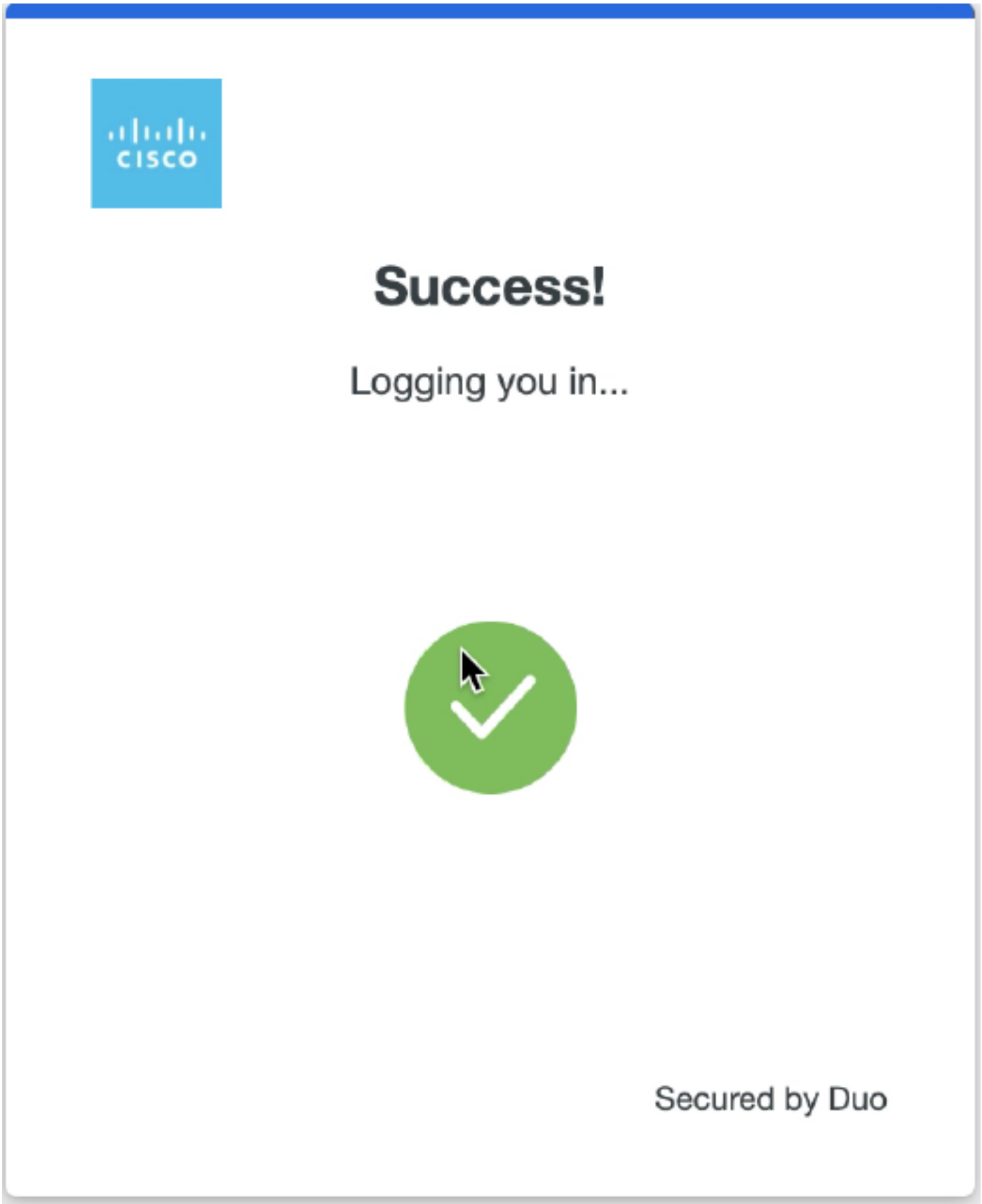
3. 輸入口令並按一下**Log in**。



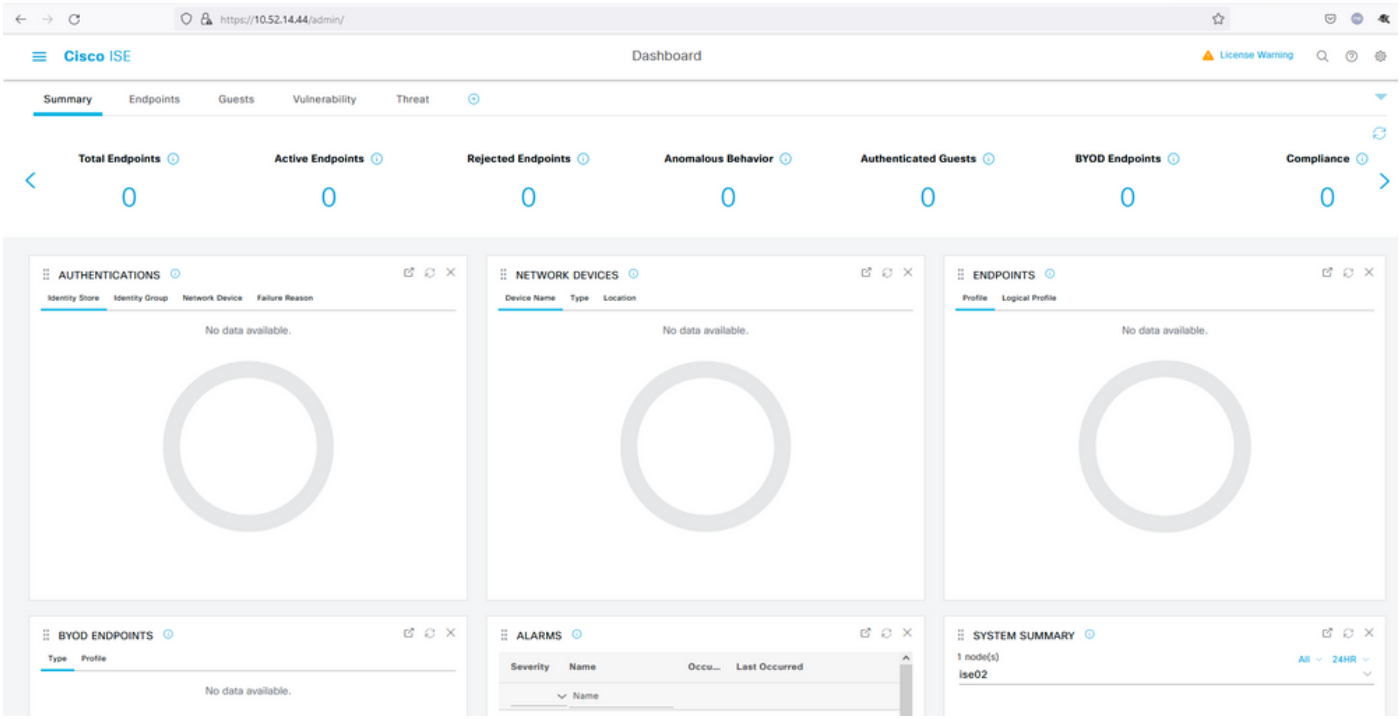
4. 您的行動裝置上會出現Duo Push提示。



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。



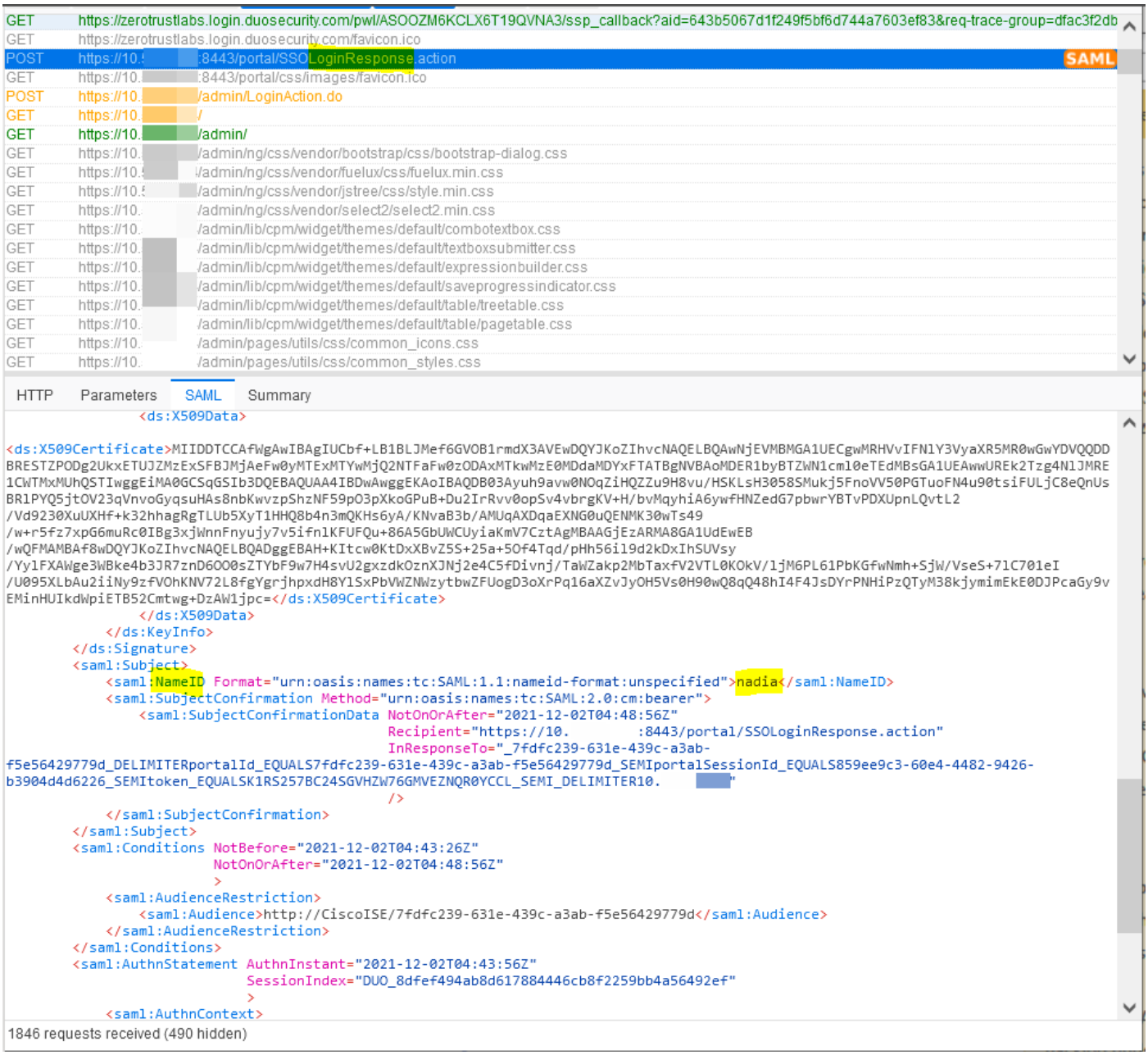
6. ISE管理員GUI訪問頁面。



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/pwl/ASOOZM6KCLX6T19QVNA3/ssp_callback?aid=643b5067d1f249f5bf6d744a7603ef83&req-trace-group=dfac3f2db
GET https://zerotrustlabs.login.duosecurity.com/favicon.ico
POST https://10.[redacted]:8443/portal/SSOLoginResponse.action SAML
GET https://10.[redacted]:8443/portal/css/images/favicon.ico
POST https://10.[redacted]/admin/LoginAction.do
GET https://10.[redacted]/
GET https://10.[redacted]/admin/
GET https://10.[redacted]/admin/ng/css/vendor/bootstrap/css/bootstrap-dialog.css
GET https://10.[redacted]/admin/ng/css/vendor/fuelux/css/fuelux.min.css
GET https://10.[redacted]/admin/ng/css/vendor/jstree/css/style.min.css
GET https://10.[redacted]/admin/ng/css/vendor/select2/select2.min.css
GET https://10.[redacted]/admin/lib/cpm/widget/themes/default/combotextbox.css
GET https://10.[redacted]/admin/lib/cpm/widget/themes/default/textboxsubmitter.css
GET https://10.[redacted]/admin/lib/cpm/widget/themes/default/expressionbuilder.css
GET https://10.[redacted]/admin/lib/cpm/widget/themes/default/saveprogressindicator.css
GET https://10.[redacted]/admin/lib/cpm/widget/themes/default/table/treetable.css
GET https://10.[redacted]/admin/lib/cpm/widget/themes/default/table/pagetable.css
GET https://10.[redacted]/admin/pages/utils/css/common_icons.css
GET https://10.[redacted]/admin/pages/utils/css/common_styles.css
HTTP Parameters SAML Summary
<ds:X509Data>
<ds:X509Certificate>MIIDDTCCAfWgAwIBAgIUCbf+LB1BLJMef6GVOB1rmdX3AVEwDQYJKoZIhvcNAQELBQAwNjEVMBMGA1UECgwMRHVvIFN1Y3VyaXR5MR0wGwYDVQQDDBRESTZPODg2UkxETUJZMzExSFBJMjAeFw0yMTExMTYwMjQ2NTFaFw0zODAxMTkwMzE0MDdaMDYxFTATBgNVBAoMDER1byBTZWN1cml0eTEdMBsGA1UEAwwUREk2Tzg4N1JMRE1CWTMxMUhQSTIwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDB03Ayuh9avw0NOqZiHQZZu9H8vu/HSKLsH3058SMukj5FnoVV50PGTuoFN4u90tsiFULjC8eQnUsBR1PYQ5jtOV23qVnvoGyqsuHAs8nbKwvzpShzNF59pO3pXkoGPuB+Du2IrRvv0opSv4vbrgKV+H/bvMqyhiA6ywfHNZedG7pbwrYBTvPDXUpnLQvtL2/Vd9230XuUXHf+k32hhagRgTLUb5XyT1HHQ8b4n3mQKHs6yA/KNvaB3b/AMUqAXDqaEXNG0uQENMK30wTs49/w+r5fz7xpG6muRc0IBg3xjWnnFnyujy7v5ifnlKFUFQu+86A5GbUWCUyiaKmV7CztAgMBAAGjEzARMA8GA1UdEwEB/wQFMAMBAf8wDQYJKoZIhvcNAQELBQADggEBAH+KItcw0KtDxXBvZ5S+25a+5Of4Tqd/pHh56il9d2kDxIhSUVsy/Yy1FXAWge3WBke4b3JR7znD6OO0sZTYbF9w7H4svU2gxzdkOznXJNj2e4C5fDivnj/TaWZakp2MbTaxfV2VTL0KOkV/1jM6PL61PbKGfwNmh+SjW/VseS+71C701eI/U095XLbAu2iiNy9zfVOhKNV72L8fgYgrjhpxdH8Y1SxPbVWZNWzytbwZFUogD3oXrPq16aXZvJyOH5Vs0H90wQ8qQ48hI4F4JsDYrPNHiPzQTyM38kjymimEkE0DJPcaGy9vEMinHUIkdWpiETB52Cmtwg+DzAW1jpc=</ds:X509Certificate>
</ds:X509Data>
</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. :8443/portal/SSOLoginResponse.action"
InResponseTo="_7fdfc239-631e-439c-a3ab-f5e56429779d_DELIMITERportalId_EQUALS7fdfc239-631e-439c-a3ab-f5e56429779d_SEMIportalSessionId_EQUALS859ee9c3-60e4-4482-9426-b3904d4d6226_SEMItoken_EQUALSK1RS257BC24SGVHZW76GMVEZNQR0YCCL_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_8dfef494ab8d617884446cb8f2259bb4a56492ef"
>
<saml:AuthnContext>
1846 requests received (490 hidden)

- ISE即時登入：

Cisco ISE

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

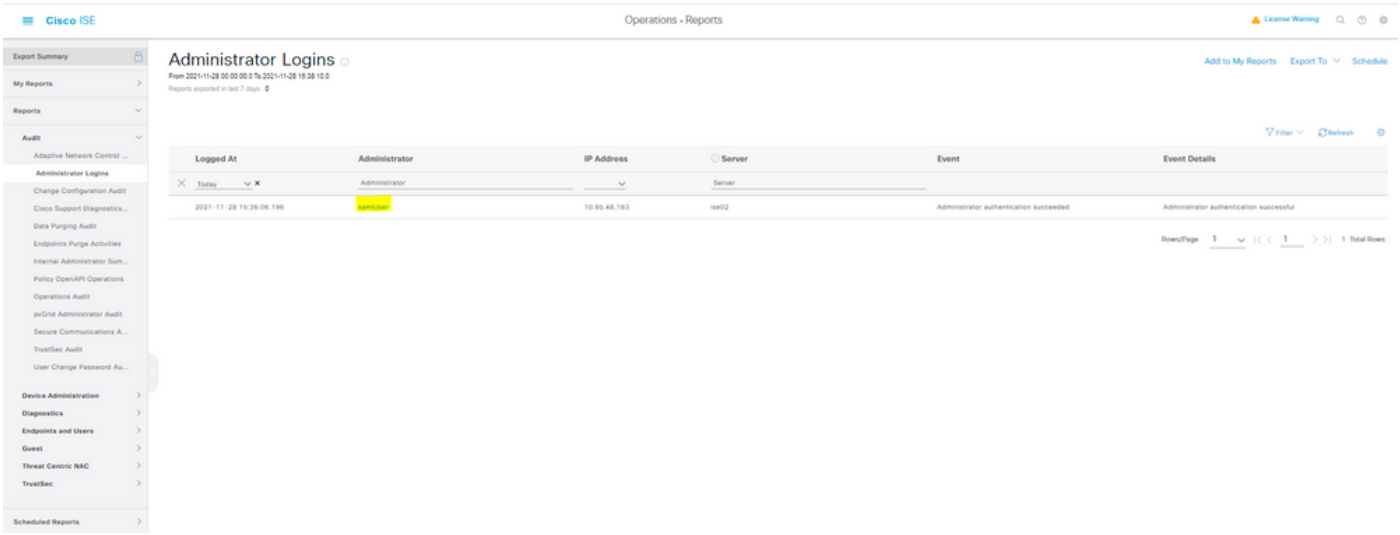
Other Attributes

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

Steps

5231	Guest Authentication Passed

- ISE上的管理登入日誌：使用者名稱：samlUser。


Cisco ISE
Operations · Reports
License Warning
Export Summary
My Reports
Reports
Audit
Adaptive Network Control ...
Administrator Logins
Change Configuration Audit
Cisco Support Diagnostics...
Data Purging Audit
Endpoints Purge Activities
Internal Administrator Sum...
Policy OpenAPI Operations
Operations Audit
pxGrid Administrator Audit
Secure Communications A...
TrustSec Audit
User Change Password Au...
Device Administration
Diagnostics
Endpoints and Users
Guest
Threat Centric NAC
TrustSec
Scheduled Reports
Administrator Logins
From 2021-11-28 00:00:00.0 To 2021-11-28 16:38:10.0
Reports exported in last 7 days
Add to My Reports
Export To
Schedule
Filter
Refresh
Logged At
Administrator
IP Address
Server
Event
Event Details
Today
Administrator
Server
2021-11-28 15:36:06.196
samlUser
10.65.48.163
ise02
Administrator authentication succeeded
Administrator authentication successful
Rows/Page
1
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）。