تكوين سجل إدارة واجهة المستخدم الرسومية ISE 3.1 باستخدام تكامل SAML مع Duo SSO و Windows AD

المحتويات

المقدمة

يصف هذا وثيقة كيف أن يشكل Cisco ISE 3.1 SAML SSO تكامل مع معرف خارجي مثل Cisco Duo SSO.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- Cisco Identity Services Engine (ISE) 3.1
- معرفة أساسية بعمليات نشر تسجيل الدخول الأحادي (SSO) للغة تأكيد الأمان (SAML 1.1)
- معرفة Cisco Duo SSO
- معرفة Windows Active Directory

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

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

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

معلومات أساسية

موفر الهوية (IDp)

في هذه الحالة، يقوم Duo SSO بالتحقق من هوية المستخدم وامتيازات الوصول إلى المورد المطلوب ("مزود الخدمة") والتأكد من ذلك.

يعمل Duo SSO كمعرف، ويصادق المستخدمين باستخدام Active Directory (AD) المحلي (على سبيل المثال، Microsoft Azure) ويطلب مصادقة ثنائية المعامل قبل السماح بالوصول إلى تطبيق مزود الخدمة.

عند تكوين تطبيق ليتم حمايته باستخدام Duo SSO، يجب عليك إرسال سمات من Duo SSO إلى التطبيق. يعمل Active Directory بدون إعداد إضافي، ولكن إذا كنت تستخدم معرف SSO كمصدر مصادقة، فتحقق من تكوينه لإرسال سمات SAML الصحيحة.

مزود الخدمة (SP)

المورد المستضاف أو الخدمة التي ينوي المستخدم الوصول إليها، خادم تطبيق Cisco ISE في هذه الحالة.

سامل

SAML هو معيار مفتوح يسمح ب IDp لتمرير بيانات اعتماد التخويل إلى SP.

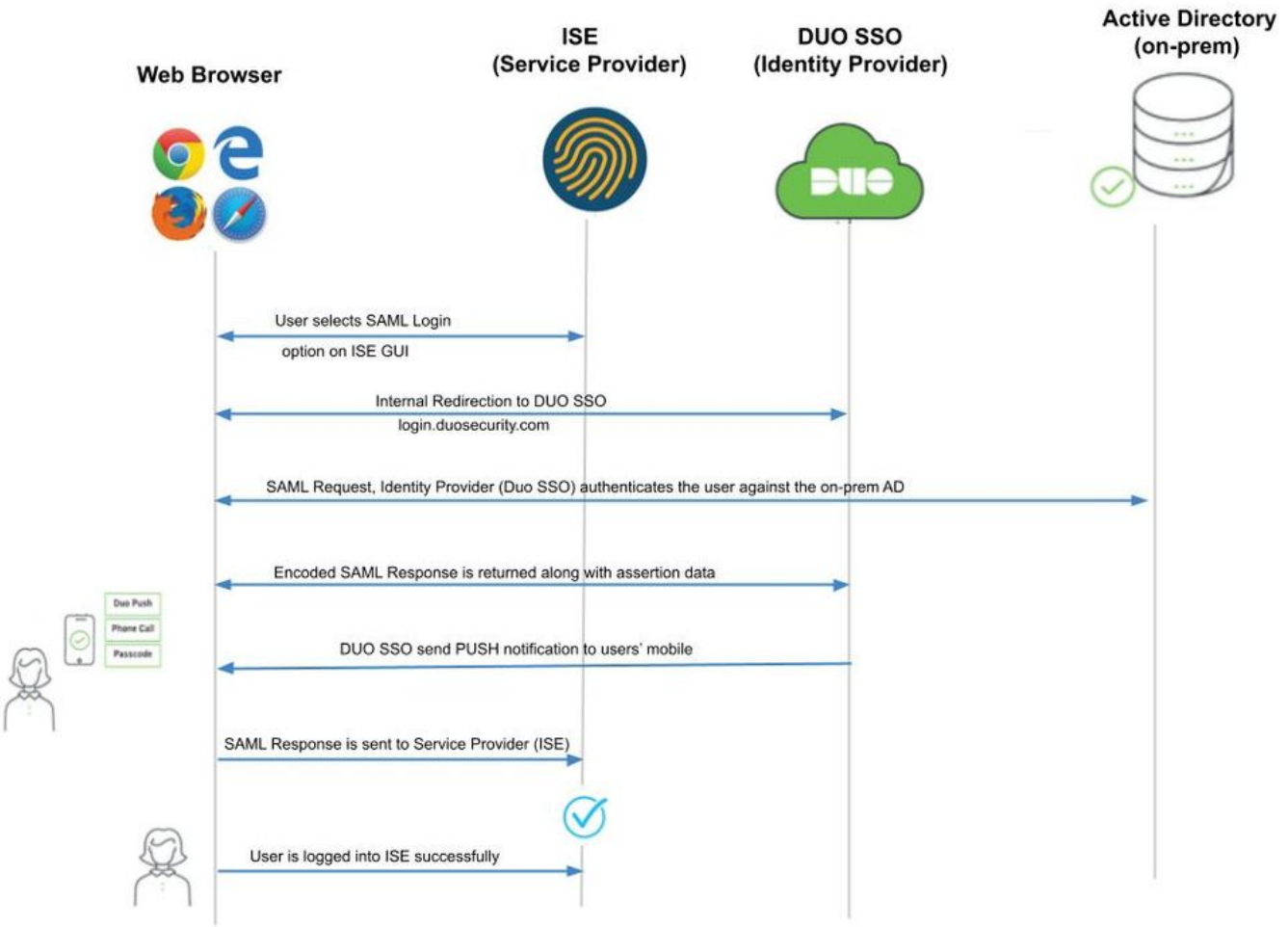
تستخدم حركات SAML لغة الترميز القابلة للتوسيع (XML) للاتصالات القياسية بين موفر الهوية ومزودي الخدمة. SAML هو الارتباط بين مصادقة هوية المستخدم والتفويض لاستخدام خدمة.

تأكيد SAML

تأكيد SAML وه مستند XML الذي يرسله IdP إلى موفر الخدمة الذي يحتوي على تفويض المستخدم. هناك ثلاثة أنواع مختلفة من تأكيدات SAML - المصادقة وتحديد السمة وقرار التفويض.

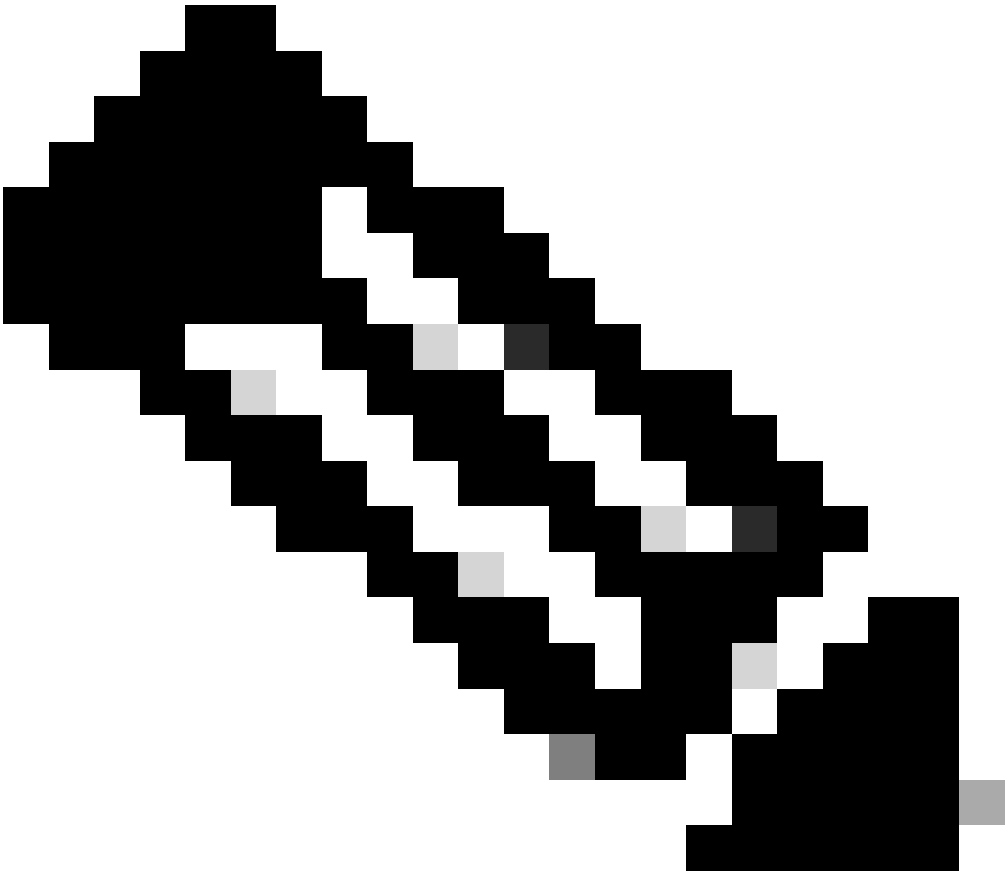
- تثبت تأكيدات المصادقة تعريف المستخدم وتوفر الوقت الذي قام المستخدم بتسجيل الدخول فيه وطريقة المصادقة التي استخدمها (على سبيل المثال، Kerberos، ثنائي العامل، وما إلى ذلك).
- يقوم تأكيد الإسناد بتمرير سمات SAML، وهي قطع بيانات محددة توفر معلومات حول المستخدم، إلى SP.
- يعلن تأكيد قرار التخويل ما إذا كان المستخدم مخولا لاستخدام الخدمة أو إذا رفض IdP طلبه بسبب فشل كلمة المرور أو عدم وجود حقوق للخدمة.

رسم تخطيطي للتدفق عالي المستوى



التدفق:

1. المستخدم يسجل الدخول إلى ISE باستخدام خيار تسجيل الدخول عبر SAML.
2. يقوم ISE (SAML SP) بإعادة توجيه المستعرض الخاص بالمستخدم إلى SSO ثنائي باستخدام رسالة طلب SAML.



3. خطوة غير صالحة أو خطأ شهادة: في بيئة موزعة، يمكن الحصول على شهادة غير صالحة أو خطأ في بيئة موزعة، فإن الخطوة 2 تختلف بالنسبة إلى بيئة موزعة، فإن الخطوة 2 تختلف. لذلك، يمكن أن تعمل الآن. لذلك، بالنسبة إلى بيئة موزعة، فإن الخطوة 2 تختلف قليلا بهذه الطريقة:
الإصدار: تتم إعادة توجيه ISE مؤقتا إلى بوابة إحدى عقد PSN (على المنفذ 8443).
الحل: لضمان أن ISE يقدم نفس الشهادة مثل شهادة واجهة المستخدم الرسومية (GUI) للمسؤول، تأكد من أن شهادة النظام التي تثق بها صالحة لاستخدام المدخل أيضا على جميع عقد PSN.

3. يقوم المستخدم بتسجيل الدخول باستخدام مسوغات AD الأساسية.
4. يقوم Duo SSO بإعادة هذا إلى AD الذي يرجع إستجابة إلى Duo SSO.
5. تتطلب Duo SSO من المستخدم إكمال مصادقة ثنائية العوامل عن طريق إرسال دفعة على الجوال.
6. يقوم المستخدم بإكمال مصادقة ثنائية العامل.
7. يقوم Duo SSO بإعادة توجيه مستعرض المستخدم إلى SAML SP برسالة إستجابة.
8. يمكن للمستخدم الآن تسجيل الدخول إلى ISE.

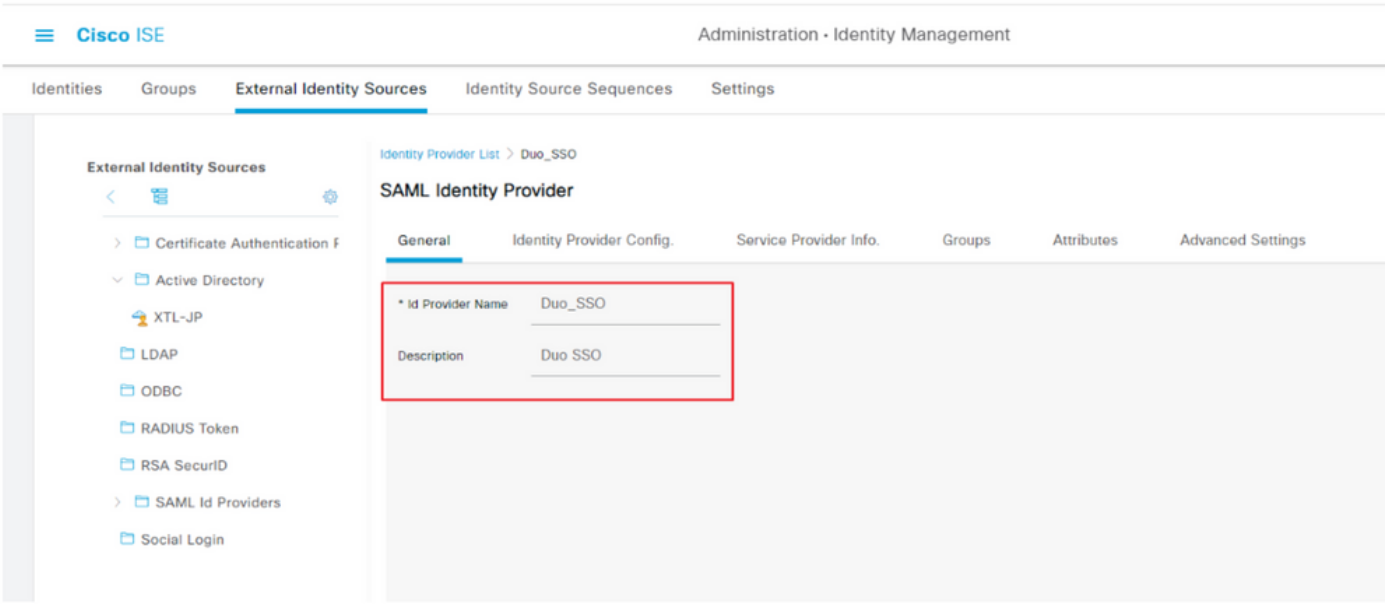
تكوين تكامل SAML SSO باستخدام Duo SSO

الخطوة 1. تكوين معرف SAML على ISE

تكوين SSO الثنائي كمصدر هوية SAML خارجي

على ISE، انتقل إلى Administration > Identity Management > External Identity Sources > SAML Id Providers وانقر فوق زر إضافة.

أدخل اسم معرف العملية وانقر فوق إرسال لحفظه. يكون اسم معرف P مهم فقط لـ ISE كما هو موضح في الصورة:

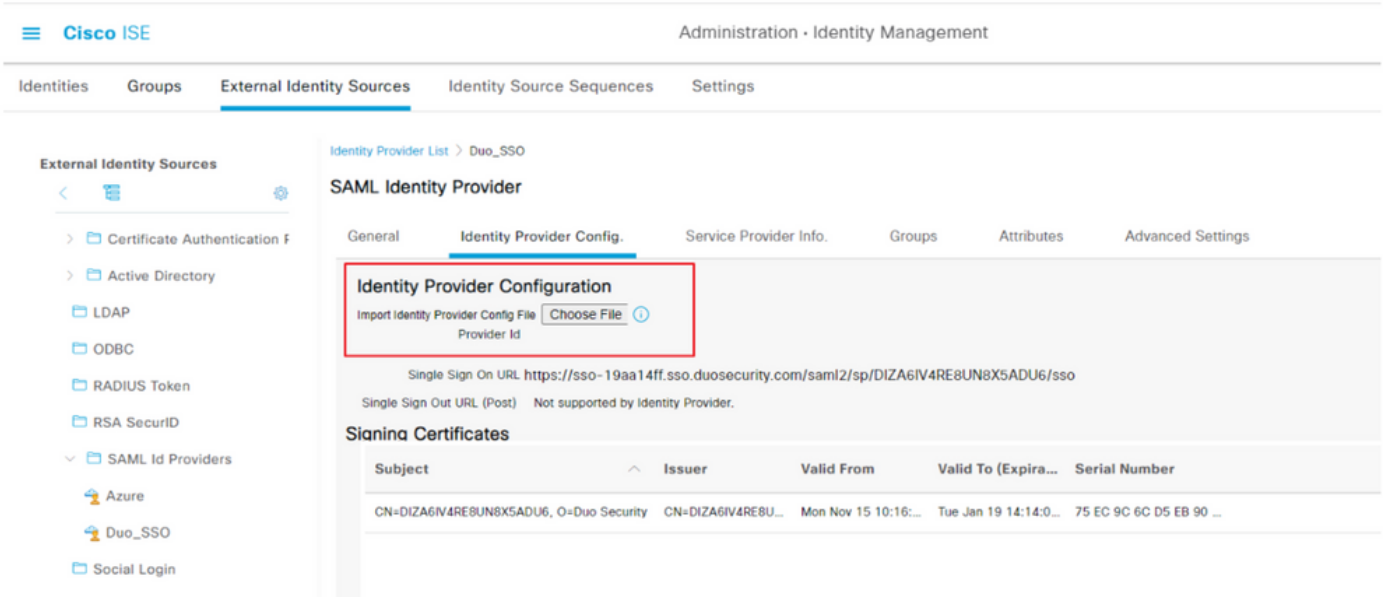


استيراد ملف XML لبيانات تعريف SAML من مدخل مسؤول Duo

على ISE، انتقل إلى Administration > Identity Management > External Identity Sources > SAML Id Providers. > أختر SAML IDp الذي أنشأته، Identity Provider Configuration ثم انقر زر إختيار ملف.

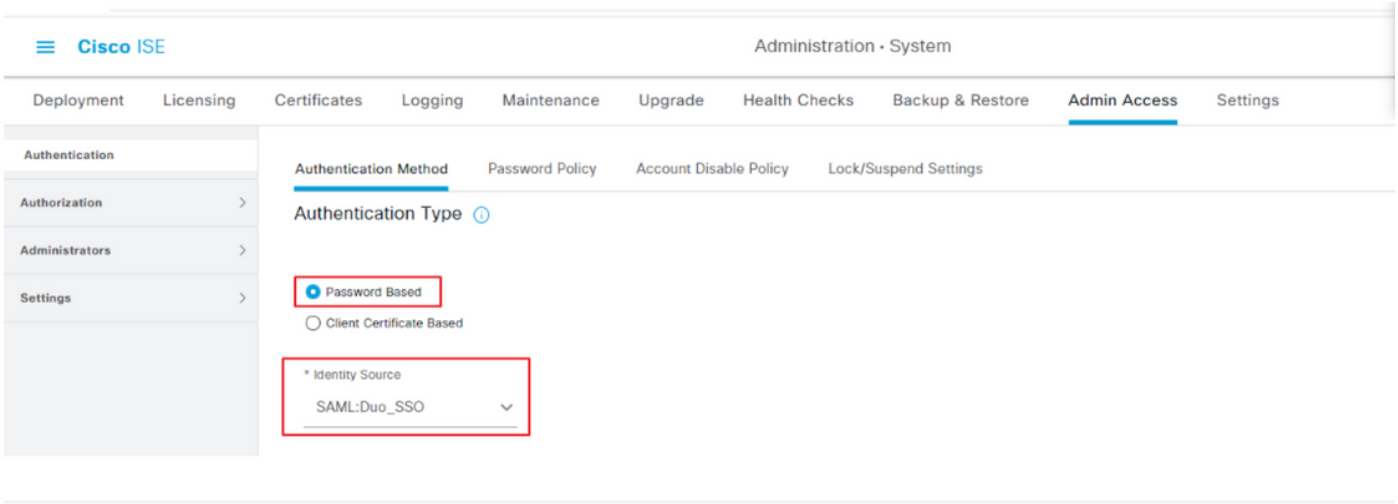
أختر ملف **SSO IDP Metadata XML** المصدر من مدخل Duo Admin وانقر فتح لحفظه. (يتم ذكر هذه الخطوة في قسم "الثنائي" في هذا المستند أيضا.)

محدد موقع معلومات SSO وشهادات التوقيع هي:



تكوين أسلوب مصادقة ISE

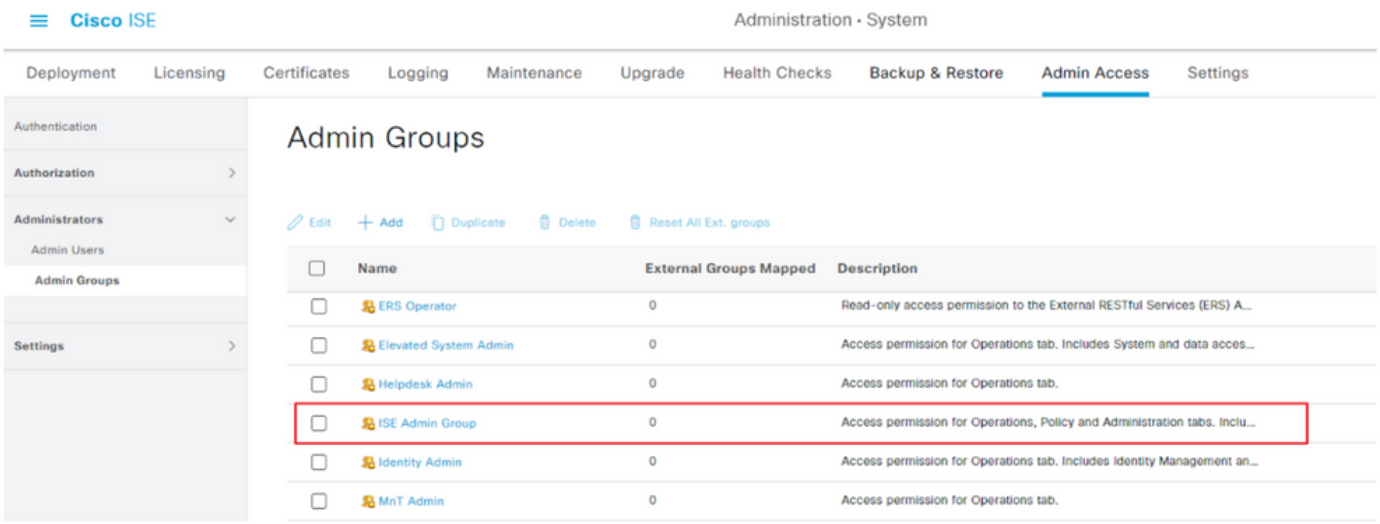
انتقل إلى Administration > System > Admin Access > Authentication > Authentication Method زر الاختيار المستند إلى كلمة المرور واختر هذا الزر. أختر اسم المعرف المطلوب الذي تم إنشاؤه مسبقا من القائمة المنسدلة مصدر الهوية كما هو موضح في الصورة:



إنشاء مجموعة إدارة

انتقل إلى Administration > System > Admin Access > Authentication > Administrators > Admin Group **Super Admin** ثم انقر فوق زر مضاعفة. أدخل اسم مجموعة الإدارة وانقر فوق الزر إرسال.

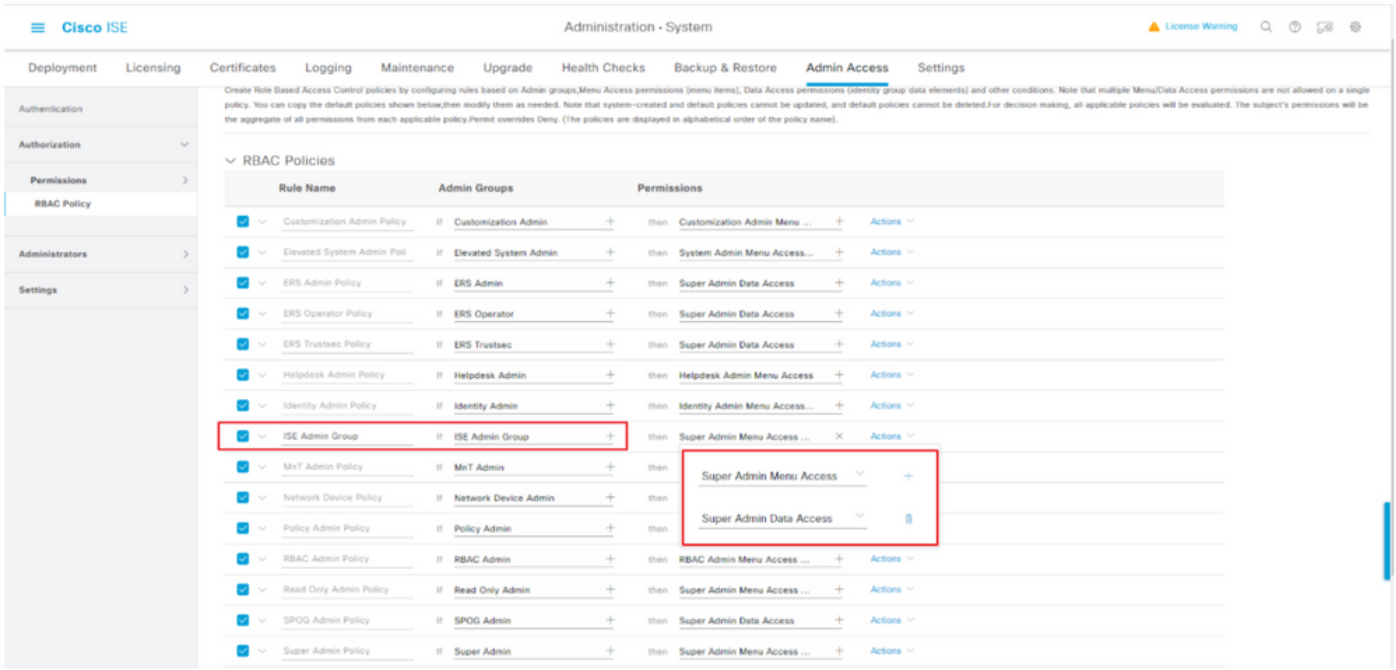
يوفر ذلك امتيازات المسؤول المتميز لمجموعة الإدارة.



إنشاء نهج RBAC لمجموعة الإدارة

انتقل إلى Administration > System > Admin Access > Authorization > RBAC Policy الإجراءات المتوافقة مع نهج **Super Admin** واختارها. انقر.Duplicate > Add the Name field > Save

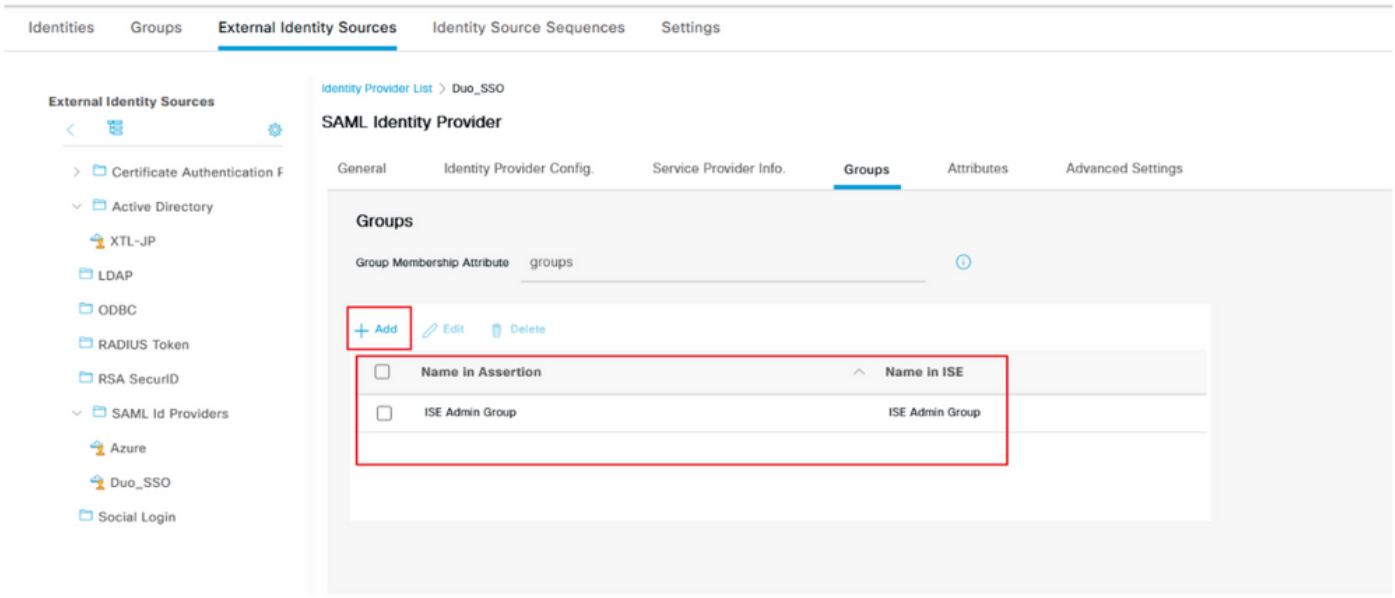
أذونات الوصول هي نفسها الخاصة بنهج Super Admin.



إضافة عضوية المجموعات

على ISE، انتقل إلى Administration > Identity Management > External Identity Sources > SAML Id Providers واختر SAML IDp الذي أنشأته. انقر فوق مجموعات ثم فوق الزر إضافة.

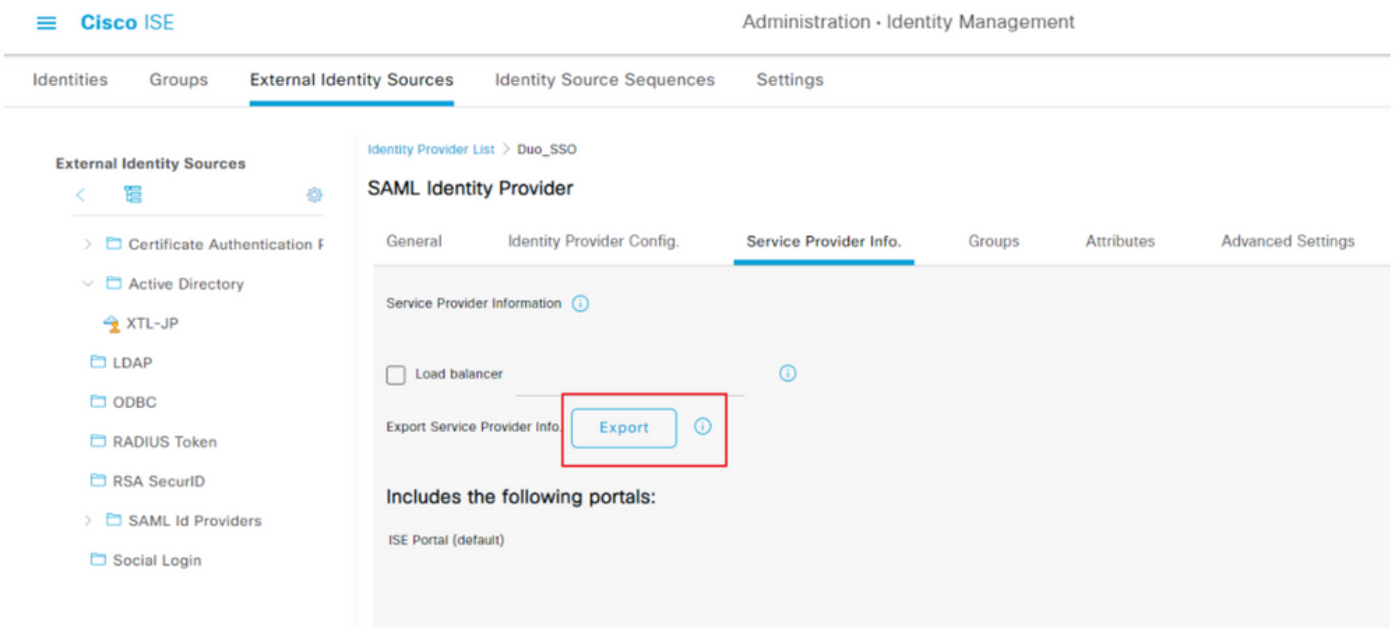
قم بإضافة الاسم في التأكيد (اسم مجموعة مسؤول ISE) ومن القائمة المنسدلة أختر مجموعة التحكم في الوصول المستندة إلى الأدوار (RBAC) التي تم إنشاؤها (الخطوة 4.) وانقر فوق فتح لحفظها. يتم علم عنوان URL الخاص ب SSO وشهادات التوقيع تلقائيا:



تصدير معلومات SP

انتقل إلى Administration > Identity Management > External Identity Sources > SAML Id Providers > (Your SAML Provider) .

قم بتبديل علامة التبويب إلى معلومات SP. وانقر فوق زر التصدير كما هو موضح في الصورة:



قم بتنزيل .xml الملف وحفظه. دون قيمة محدد موقع المعلومات (URLAssertionConsumerService) وقيمة EntityID فارجع وانظر هذه التفاصيل مطلوبة في مدخل SSO الثنائي.

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

فيما يلي التفاصيل/السمات موضع الاهتمام التي تم تجميعها من ملف التعريف والتي يجب تكوينها في دمج SAML العام الثنائي

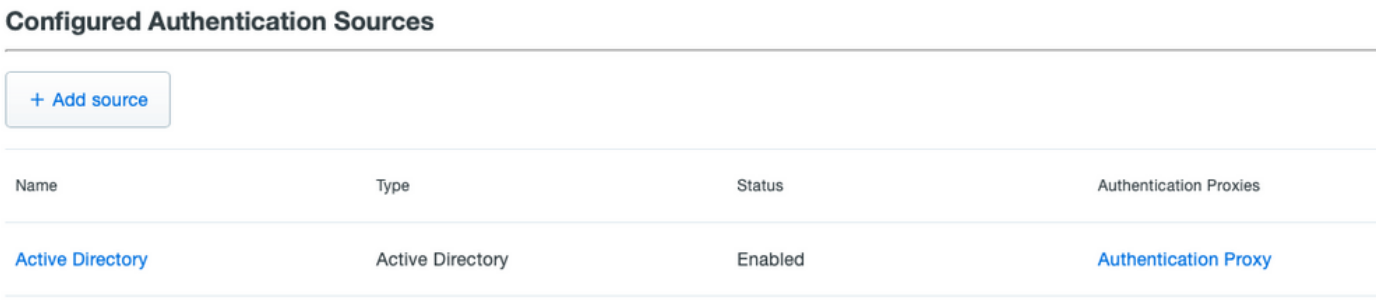
EntityID = http://CiscoISE/7fdfc239-631e-439c-a3ab-f5e56429779d.

موقع ConfirmationConsumerService = https://10.x.x.x:8443/portal/SSOLoginResponse.action حيث يمثل 10.x.x.x عنوان ISE IP الموجود على ملف XML (الموقع).

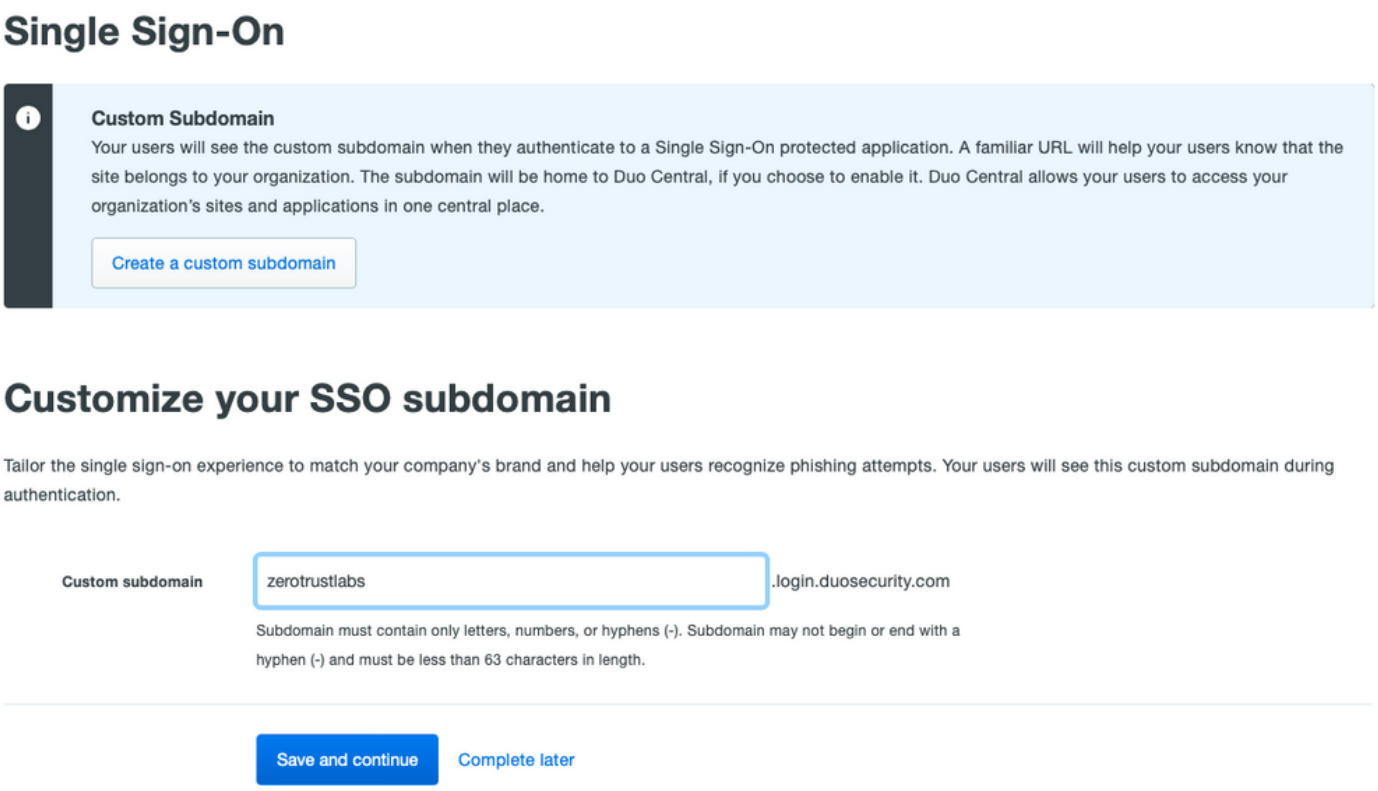
موقع ConfirmationConsumerService = https://isenodename.com:8443/portal/SSOLoginResponse.action حيثisenodename يكون اسم ISE FQDN الفعلي الموجود على ملف XML (الموقع).

الخطوة 2. تكوين SSO الثنائي ل ISE

تحقق من هذه كيلوبايت لتكوين Duo SSO باستخدام AD كمصدر مصادقة.



تحقق من هذه كيلوبايت لتمكين SSO باستخدام المجال المخصص.

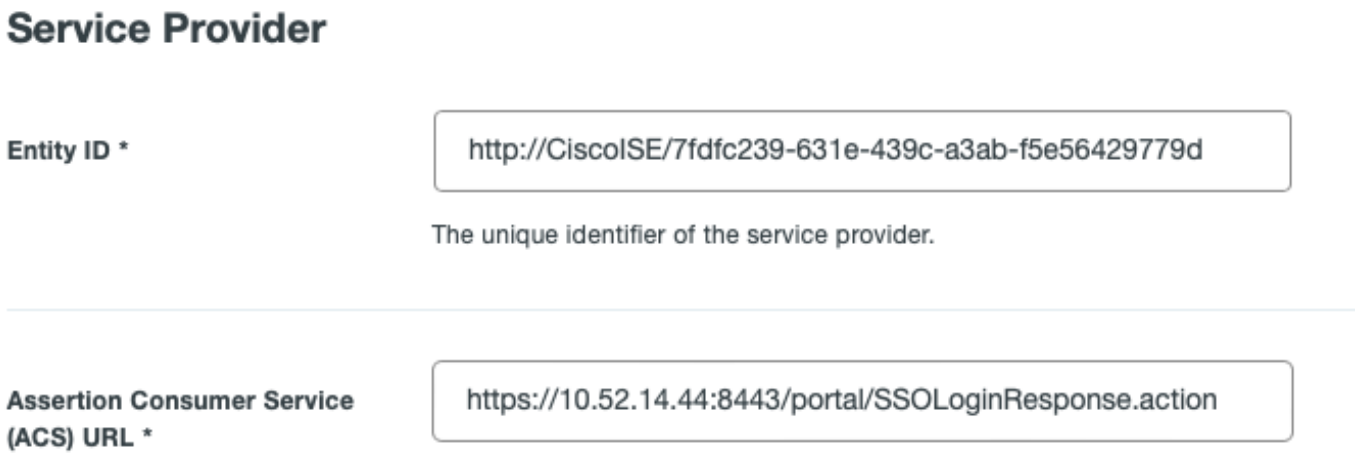


الخطوة 3. دمج Cisco ISE مع Duo SSO كمزود خدمة SP

تحقق من الخطوة 1. والخطوة 2. من هذه كيلوبايت من أجل دمج Cisco ISE مع Duo SSO كمزود خدمة رسومية.

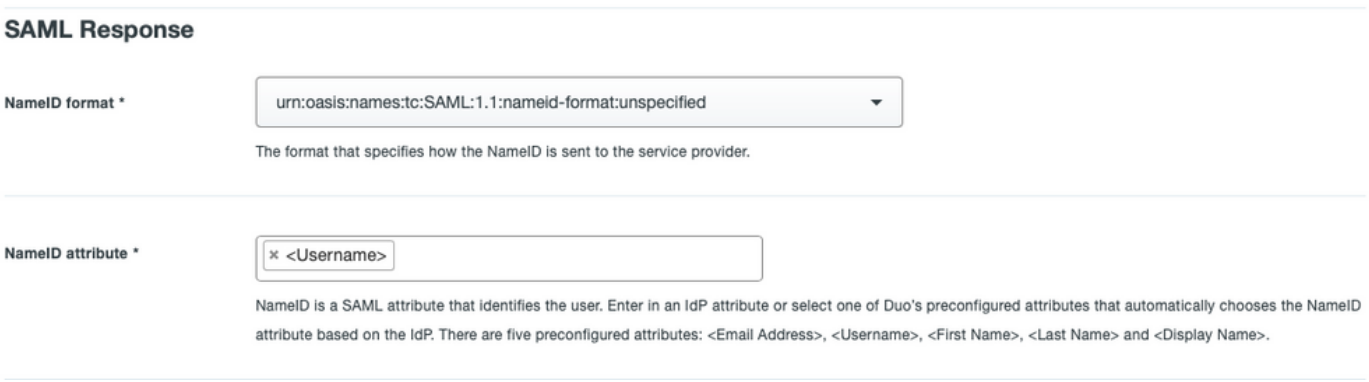
تكوين تفاصيل Cisco ISE SP في لوحة مسؤول Duo ل SP عام:

الوصف	الاسم
http://CiscoISE/7fdfc239-631e-439c-a3ab-f5e56429779d	معرف الكيان
https://10.x.x.x:8443/portal/SSOLoginResponse.action	عنوان URL لخدمة المستهلك لتأكيد البيانات (ACS)

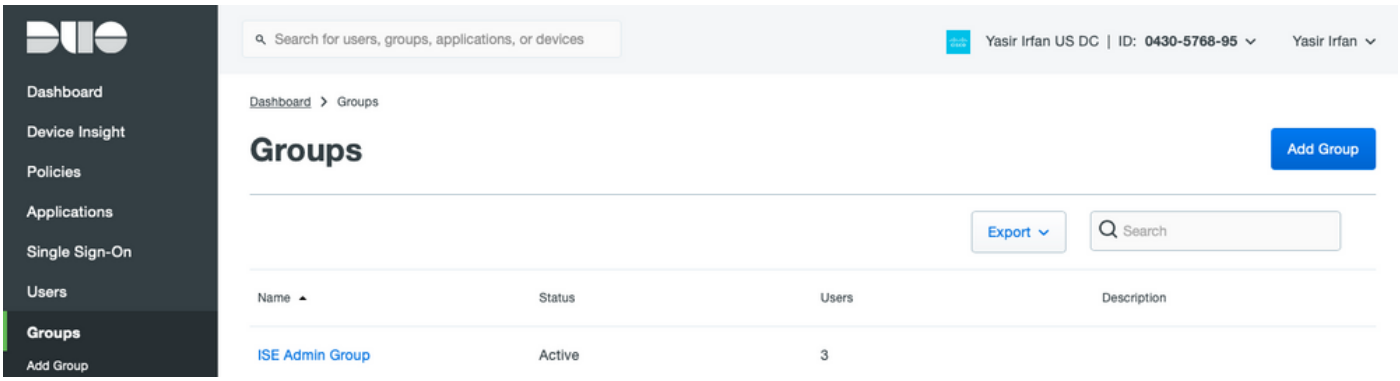


تكوين إستجابة SAML ل Cisco ISE:

الوصف	الاسم
urn:oasis:الأسماء:tc:saml:1.1:nameid-format:غير محدد	تنسيق NameID
Username	سمة NameID

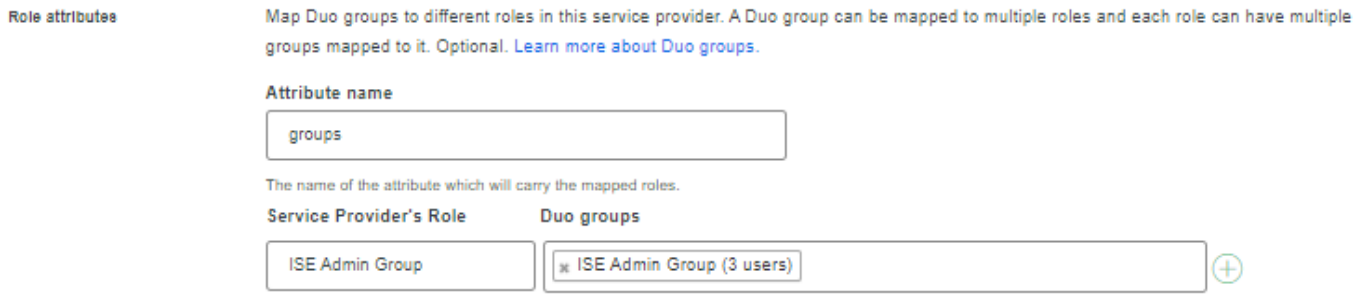


قم بإنشاء مجموعة تسمى مجموعة مسؤول Cisco في لوحة مسؤول Duo وأضف مستخدمي ISE إلى هذه المجموعة أو قم بإنشاء مجموعة في Windows AD وقم بمزامنة نفس المجموعة إلى لوحة مسؤول Duo باستخدام ميزة مزامنة الدليل.

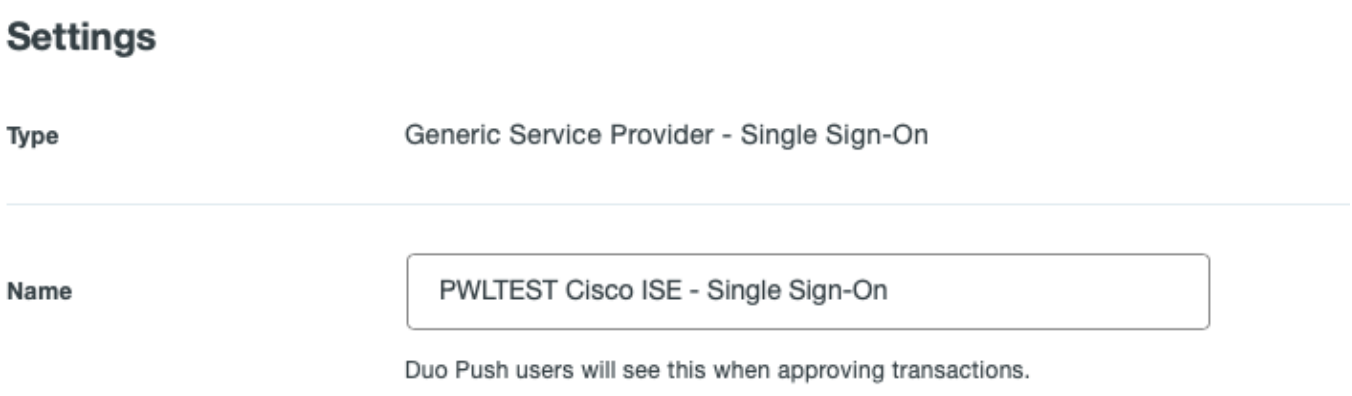


تكوين سمات الدور ل Cisco ISE:

الاسم	الوصف
اسم السمة	مجموعات
دور SP	مجموعة مسؤول ISE
ثنائي المجموعات	مجموعة مسؤول ISE

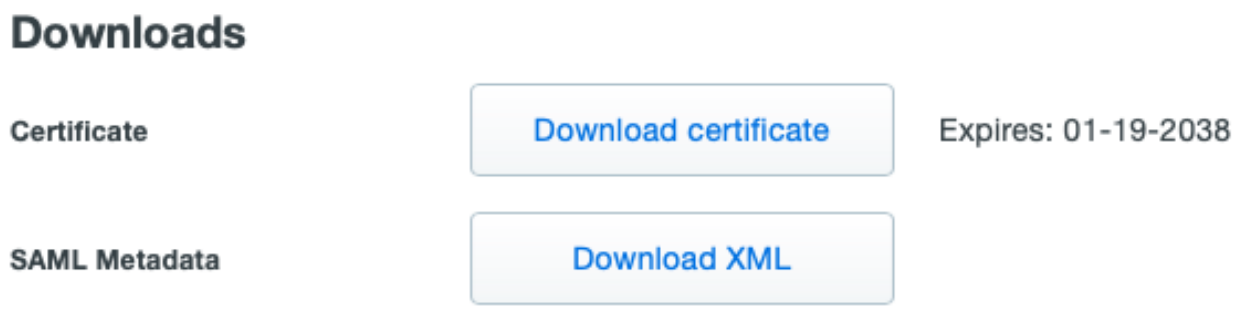


في قسم الإعدادات قم بتوفير اسم مناسب في علامة التبويب الاسم لهذا التكامل.

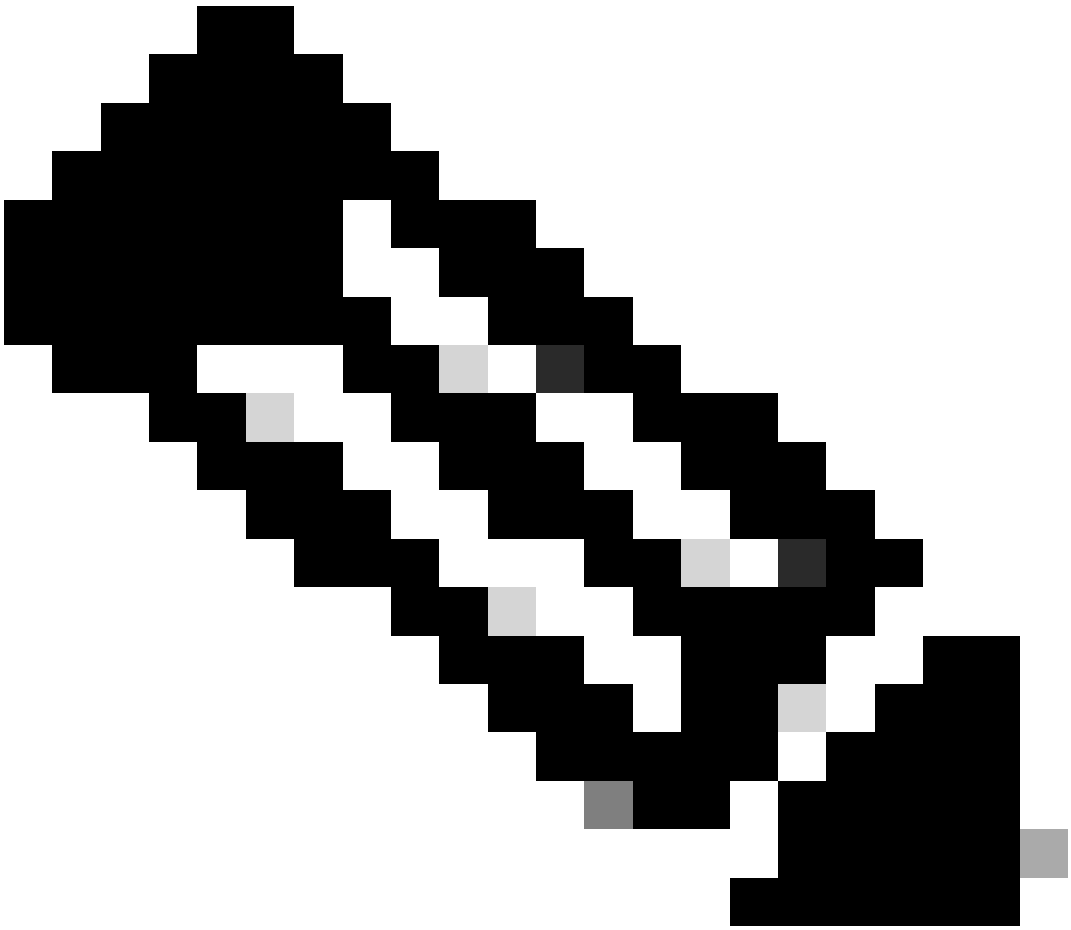


طقطقت لا **save** زر in order to أنقذت التشكيل وأرجعت هذه ك ب ل كثير معلومة.

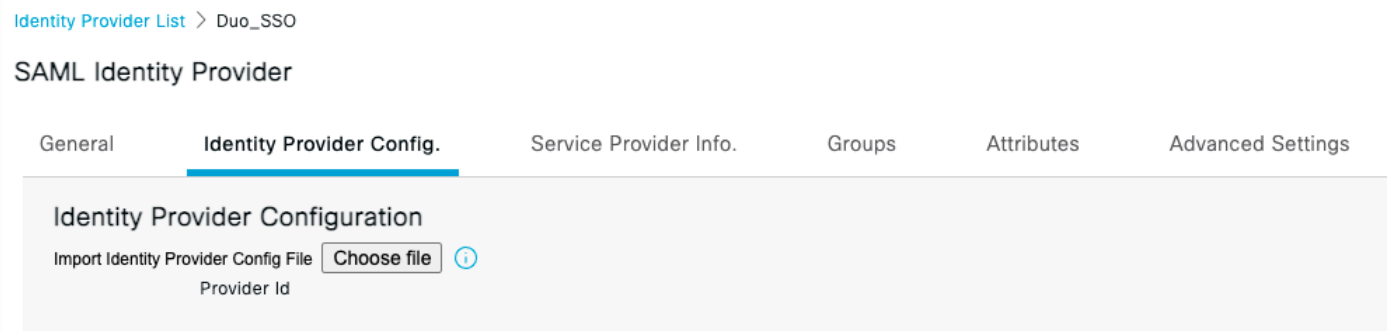
انقر فوق **تنزيل XML** لتنزيل بيانات تعريف SAML.



قم بتحميل SAML MetaData Download من لوحة إدارة Duo إلى Cisco ISE بالتنقل إلى Administration > Identity Management > External Identity Sources > SAML Id Providers > Duo_SSO.
قم بتبديل علامة التبويب إلى **تكوين موفر الهوية**. وانقر فوق الزر **إختيار الملف**.
أختر ملف بيانات التعريف **XML** الذي تم تنزيله في الخطوة 8. وانقر **حفظ**.



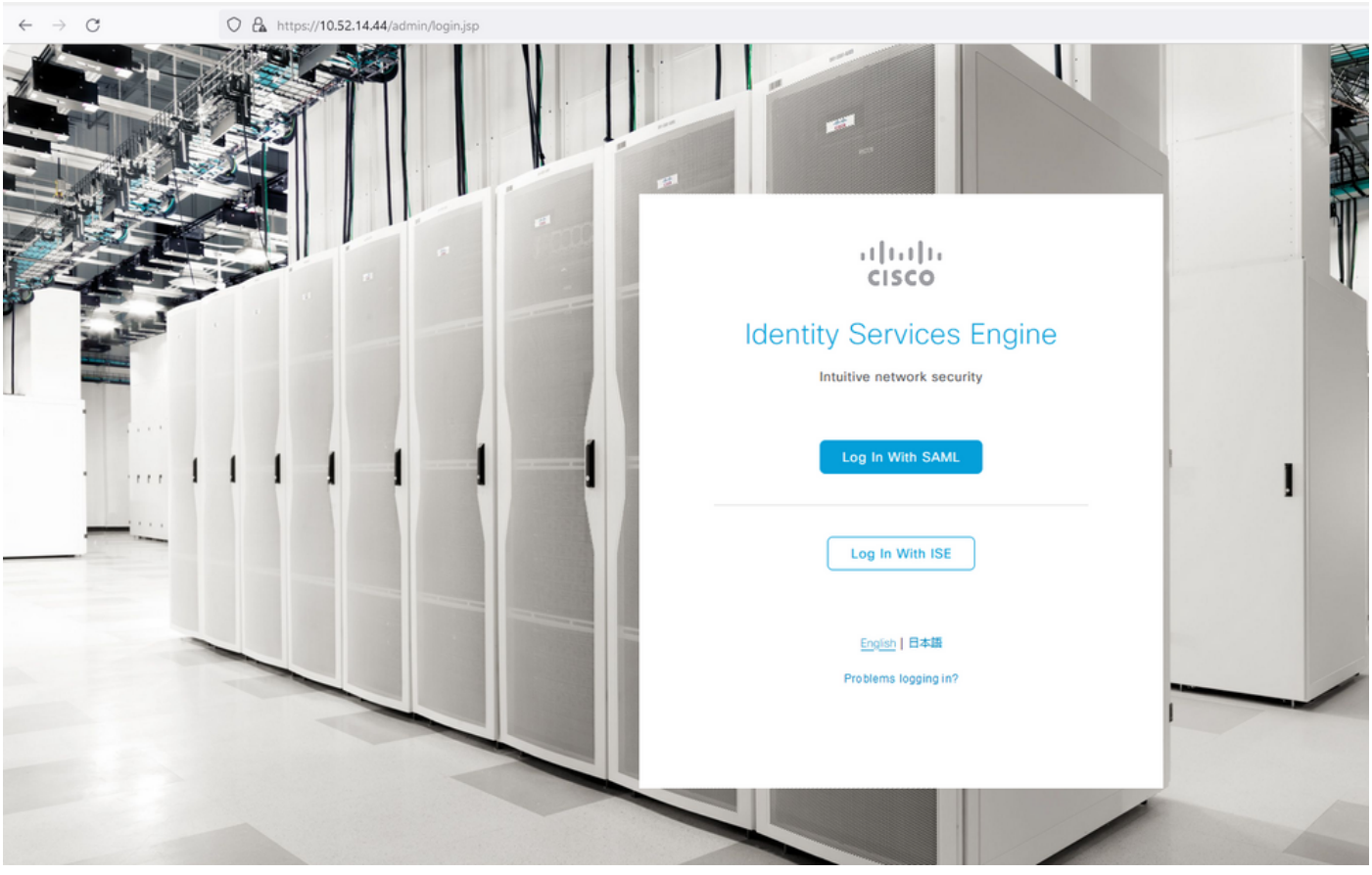
ملاحظة: تمت الإشارة إلى هذه الخطوة هنا ضمن القسم تكوين تكامل SAML SSO مع Duo SSO؛ الخطوة 2. استيراد ملف **SAML Metadata XML** من مدخل Duo Admin.



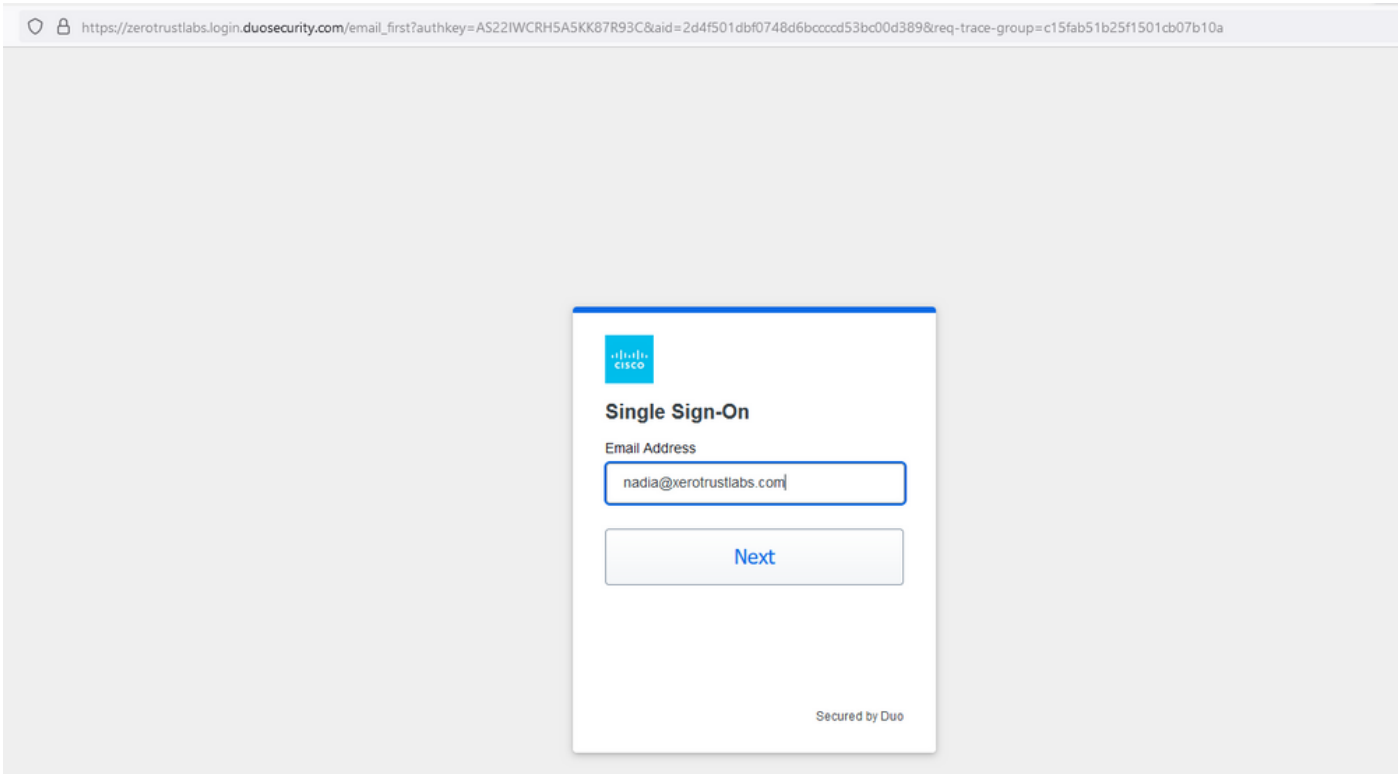
التحقق من الصحة

اختبار الدمج مع Duo SSO

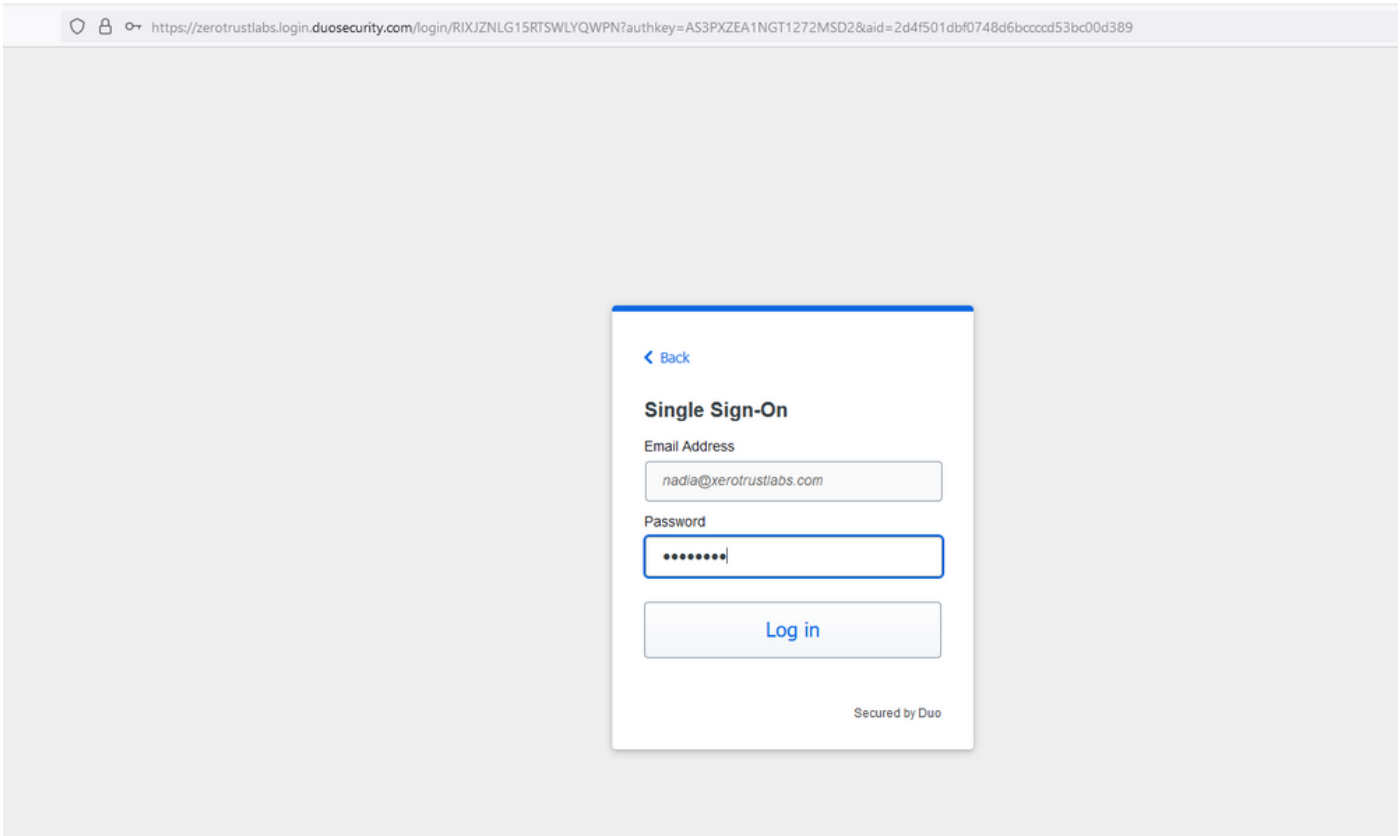
1. قم بتسجيل الدخول إلى لوحة إدارة **Cisco ISE** وانقر فوق تسجيل الدخول باستخدام **SAML**.



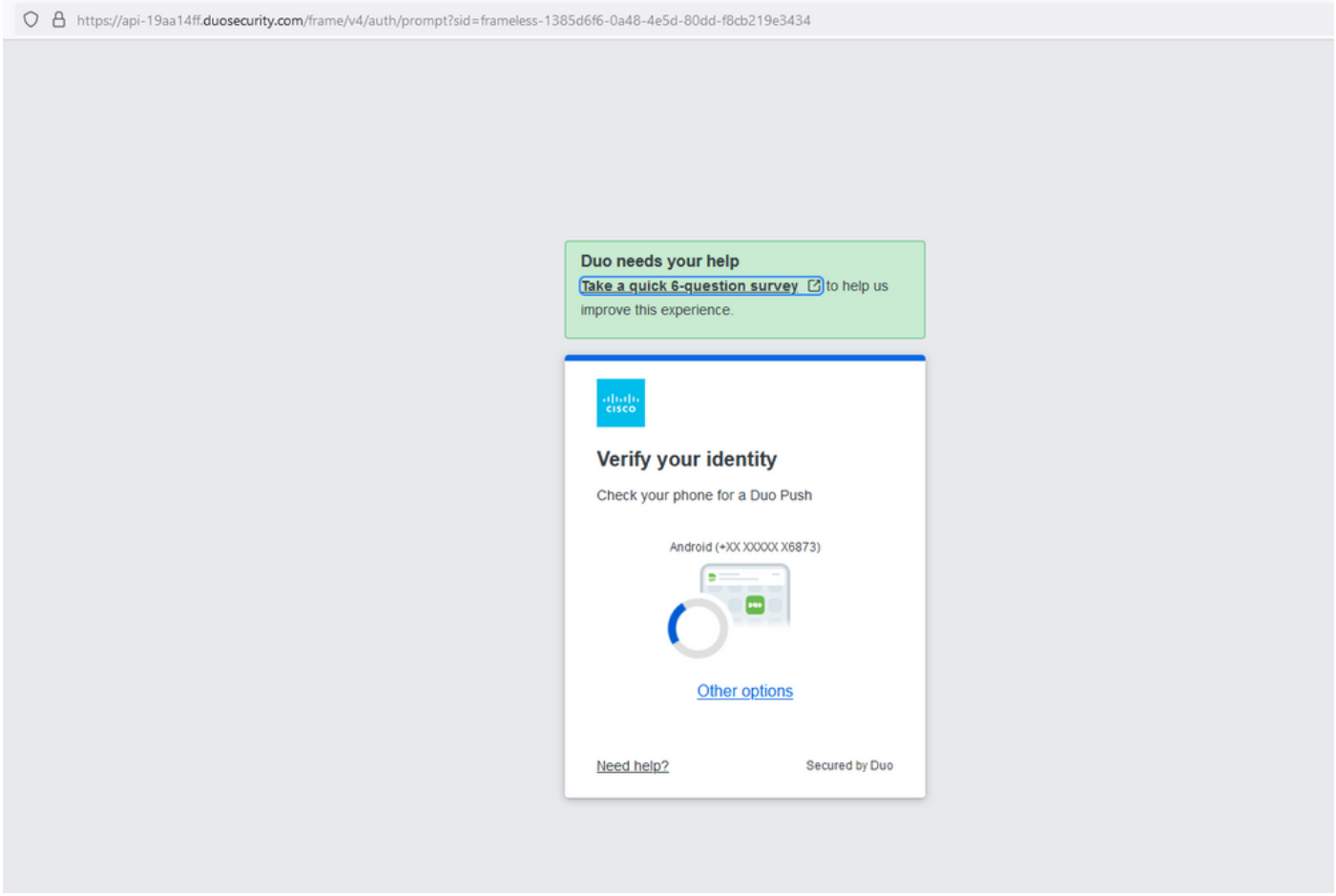
2. تتم إعادة التوجيه إلى صفحة SSO، فأدخل عنوان البريد الإلكتروني وانقر فوق التالي.



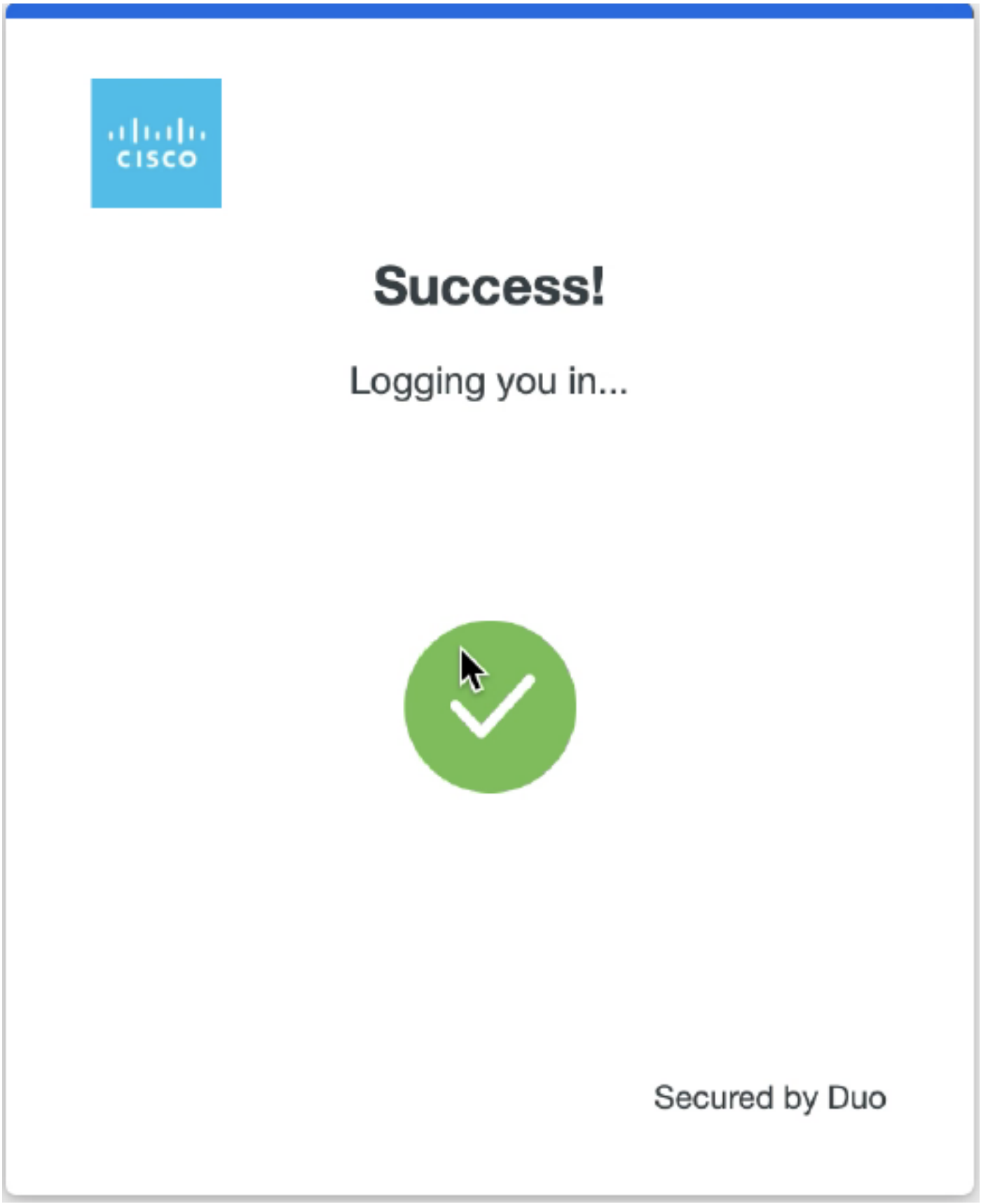
3. أدخل كلمة المرور وانقر فوق تسجيل الدخول.



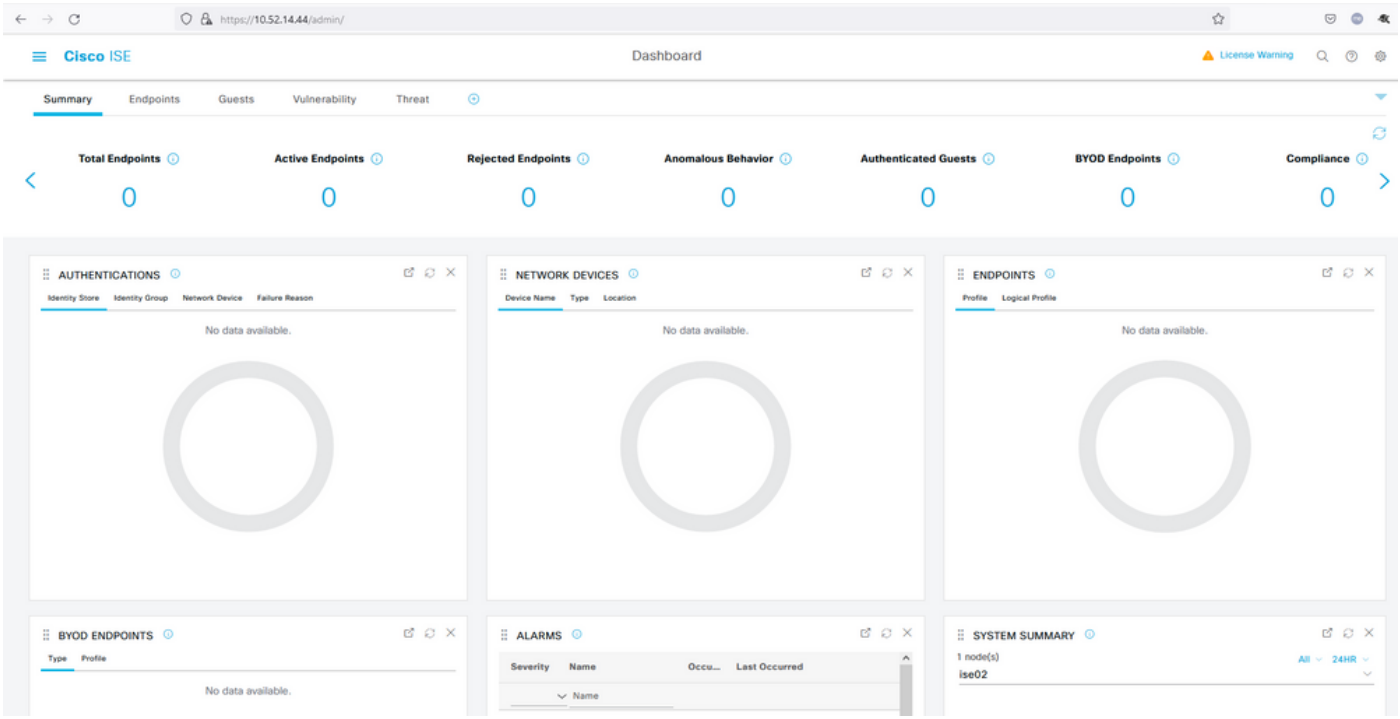
4. يمكنك الحصول على موجه دفع ثنائي على جهازك المحمول.



5. بمجرد قبول المطالبة، تحصل علىى نافذة ويتم إعادة توجيهها تلقائيا إلى صفحة مسؤول ISE.



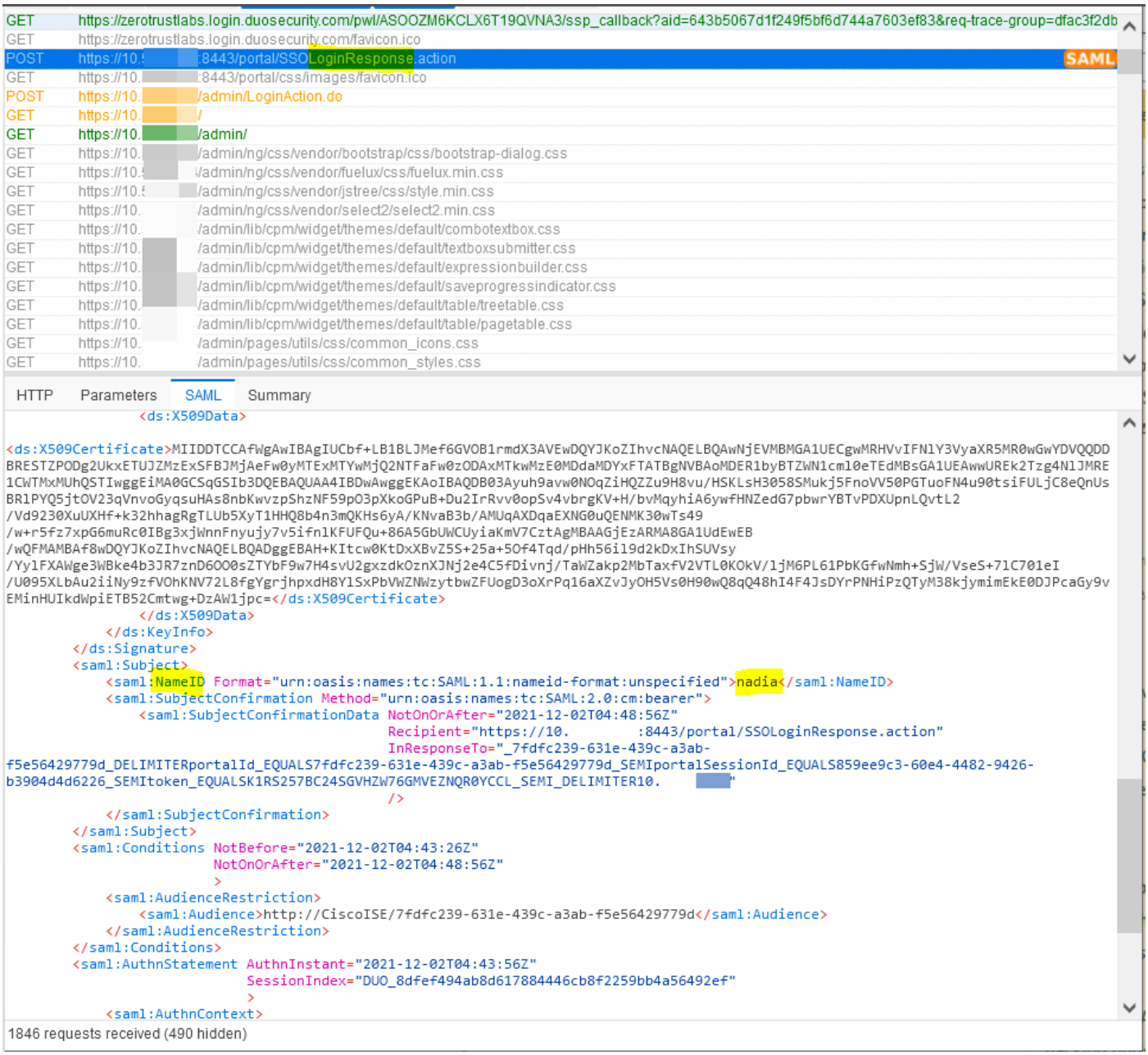
6. صفحة الوصول إلى واجهة المستخدم الرسومية (GUI) الخاصة بإدارة ISE.



استكشاف الأخطاء وإصلاحها

- قم بتنزيل ملحق SAML Tracer ل Mozilla FF https://addons.mozilla.org/en-US/firefox/addon/saml-tracer/.

- قم بالتمرير إلى SSOLoginResponse.action الحزمة. تحت علامة التبويب **SAML**، ترى عدد من السمات المرسلة من Duo SAML: NameID، المستلم (عنوان URL لموقع ConfirmationConsumerService)، والجمهور(EntityID).



- Live Log on ISE:

Cisco ISE

Overview

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

Steps

5231	Guest Authentication Passed

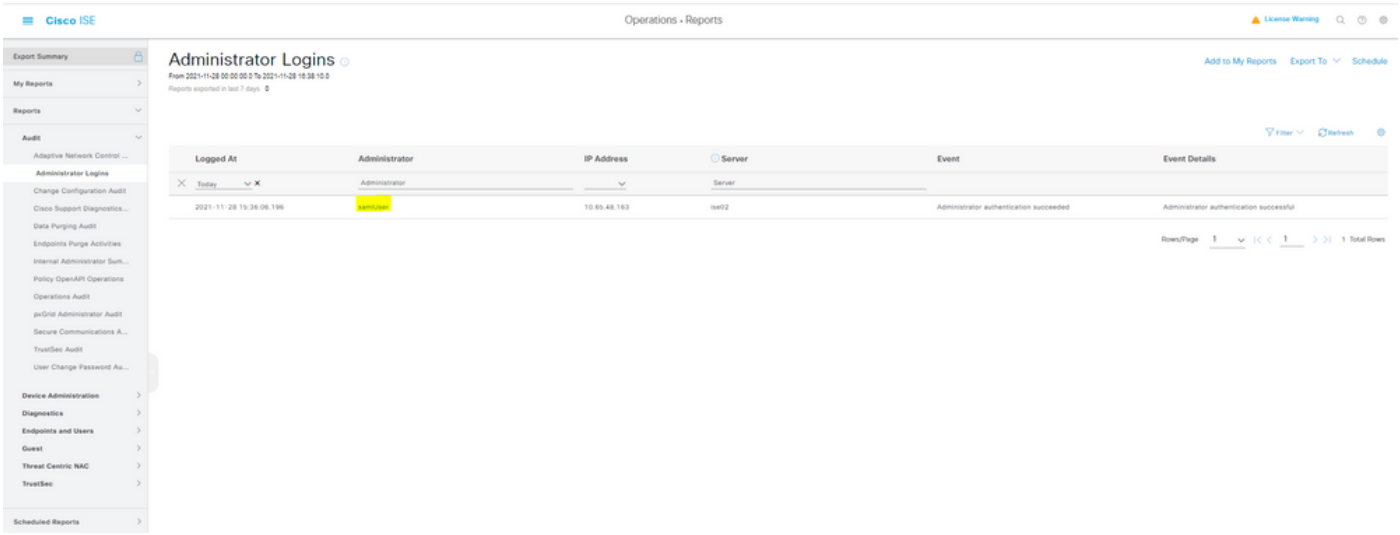
Authentication Details

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

- تسجيل الدخول الإداري إلى ISE: username: 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

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).