使用SAML Integration with Duo SSO和Windows AD配置ISE 3.1 GUI管理员登录

目录

简介

本文档介绍如何配置Cisco ISE 3.1 SAML SSO与外部身份提供程序（如Cisco Duo SSO）的集成。

先决条件

要求

Cisco 建议您了解以下主题：

- 思科身份服务引擎(ISE) 3.1
- 有关安全断言标记语言(SAML)单点登录(SSO)部署(SAML 1.1)的基本知识

- Cisco DUO SSO知识
- Windows Active Directory知识

使用的组件

本文档中的信息基于以下软件和硬件版本：

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

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

身份提供程序(IdP)

在本例中，Duo SSO用于验证和声明用户身份以及对所请求资源（“服务提供商”）的访问权限。

双点SSO充当IdP，使用SAML 1.1或任何SAML 2.0 IdP（例如Microsoft Azure）的现有本地Active Directory (AD)对用户进行身份验证，并在允许访问服务提供商应用程序之前提示进行双因素身份验证。

配置要使用Duo SSO保护的应用时，必须将属性从Duo SSO发送到应用。Active Directory无需其他设置，但是如果使用SAML(2.0) IdP作为身份验证源，请验证是否已将其配置为发送正确的SAML属性。

服务提供商(SP)

用户想要访问的托管资源或服务；本例中为Cisco ISE应用服务器。

SAML

SAML是允许IdP将授权凭证传递到SP的开放标准。

SAML事务使用可扩展标记语言(XML)实现身份提供者和服务提供商之间的标准化通信。SAML是用户身份的身份验证与使用服务的授权之间的链接。

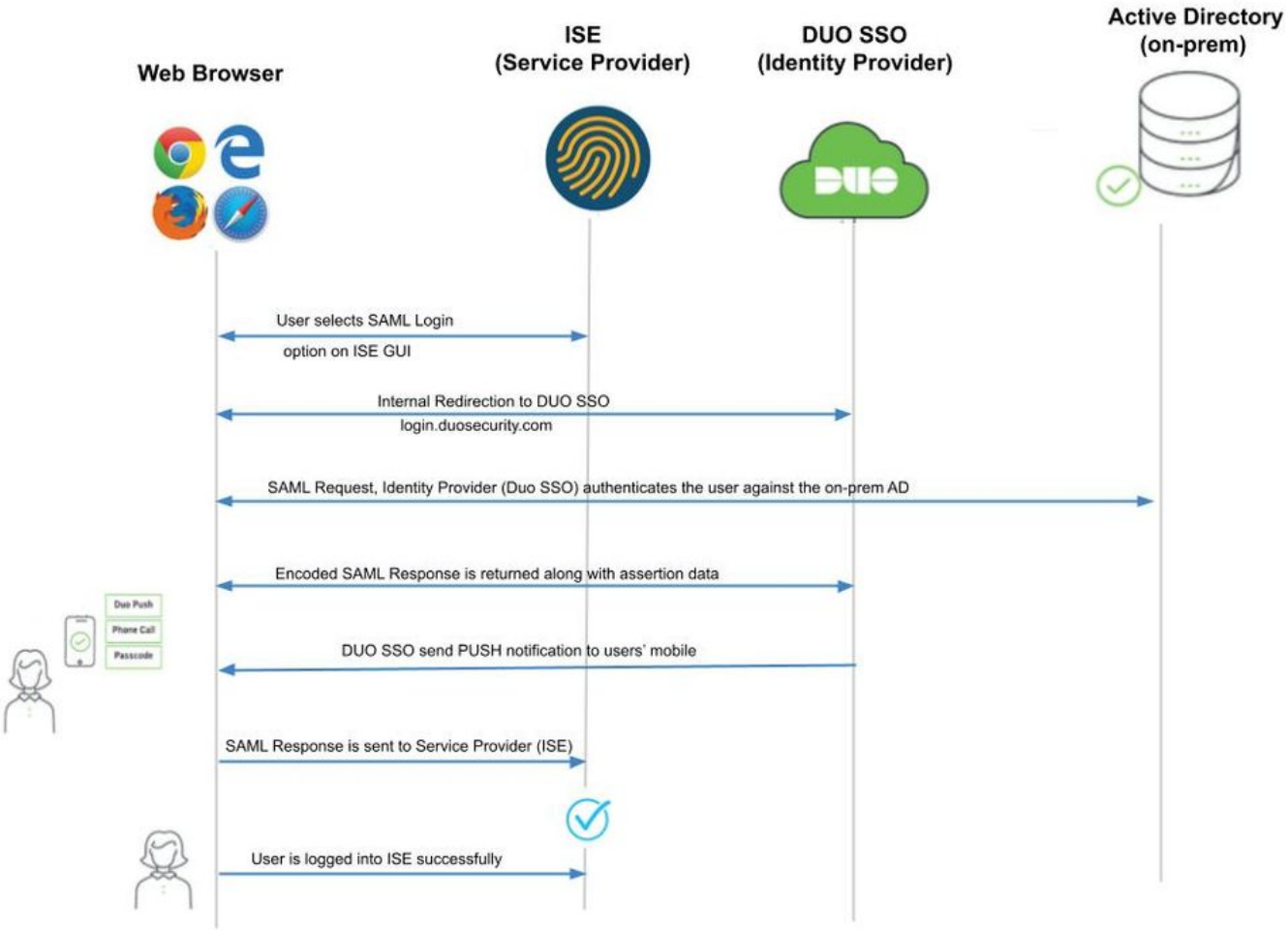
SAML断言

SAML断言是IdP发送到包含用户授权的服务提供商的XML文档。有三种不同类型的SAML断言-身份验证、属性和授权决策。

- 身份验证断言可证明用户的标识，并提供用户登录的时间以及他们使用的身份验证方法（例如，Kerberos、双因素等）。

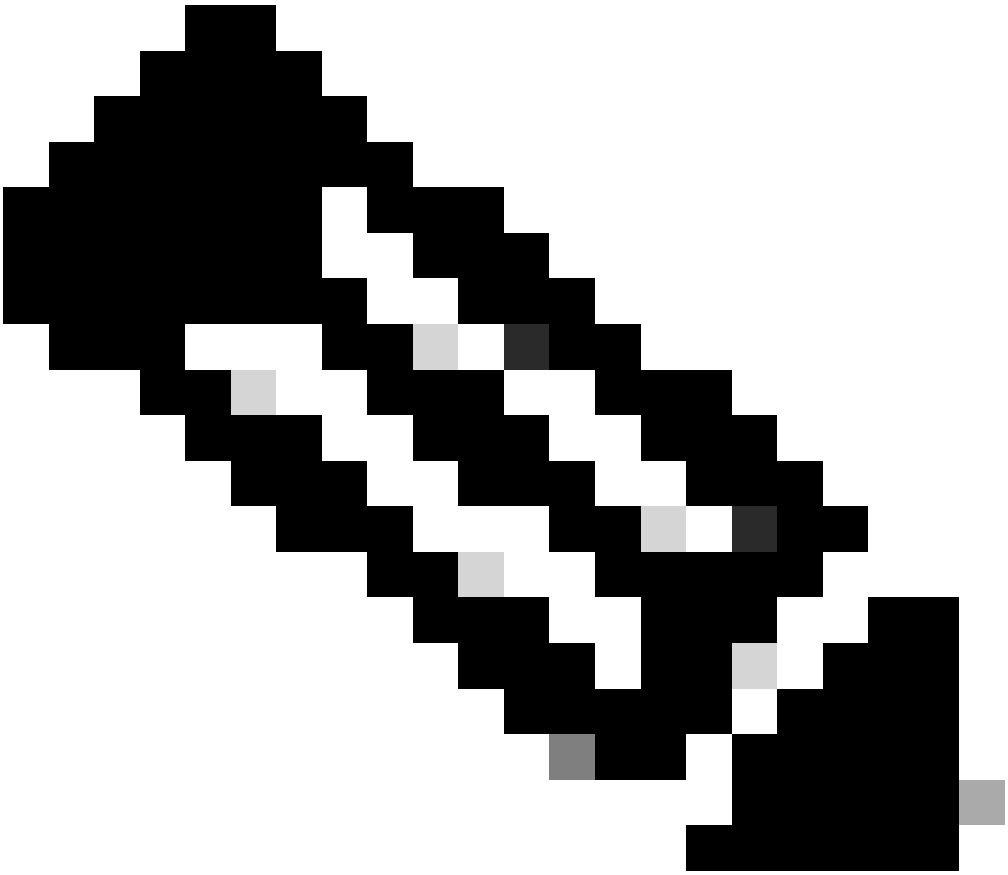
- 属性断言将SAML属性（提供有关用户信息的特定数据片段）传递给SP。
- 授权决定断言声明用户是否获得授权以便使用该服务，或者IdP是否由于密码失败或缺少对服务的权限而拒绝其请求。

高级流程图



流程：

1. 用户使用Login Via SAML选项登录到ISE。
2. ISE (SAML SP)使用SAML请求消息将用户的浏览器重定向至Duo SSO。



注意：在分布式环境中，您可能会收到“Invalid Certificate（无效证书）”错误，因此第3步现在可以执行。因此，对于分布式环境，步骤2.与此略有不同：
问题：ISE临时重定向至其中一个PSN节点的门户（在端口8443上）。
解决方案：为了确保ISE提供与管理员GUI证书相同的证书，请确保您信任的系统证书对所有PSN节点上的门户使用也是有效的。

3. 用户使用主AD凭证登录。
4. Duo SSO会将此消息转发到AD，AD会向Duo SSO返回响应。
5. 双点SSO要求用户在移动设备上发送PUSH来完成双因素身份验证。
6. 用户完成双因素身份验证。
7. Duo SSO将用户的浏览器重定向到SAML SP，并显示一条响应消息。
8. 用户现在能够登录到ISE。

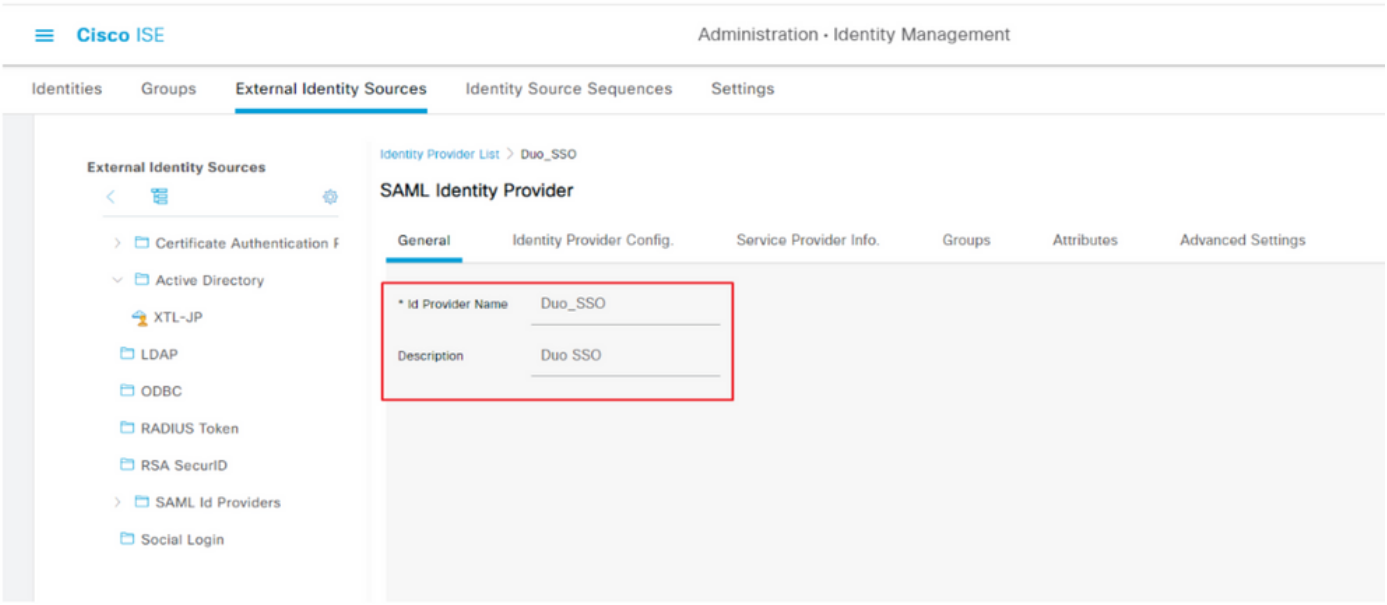
配置SAML SSO与Duo SSO的集成

步骤1:在ISE上配置SAML IdP

将Duo SSO配置为外部SAML身份源

在ISE上，导航至Administration > Identity Management > External Identity Sources > SAML Id Providers，然后点击**Add**按钮。

输入IdP的名称，然后单击**Submit**以保存它。IdP名称仅对ISE有效，如图所示：

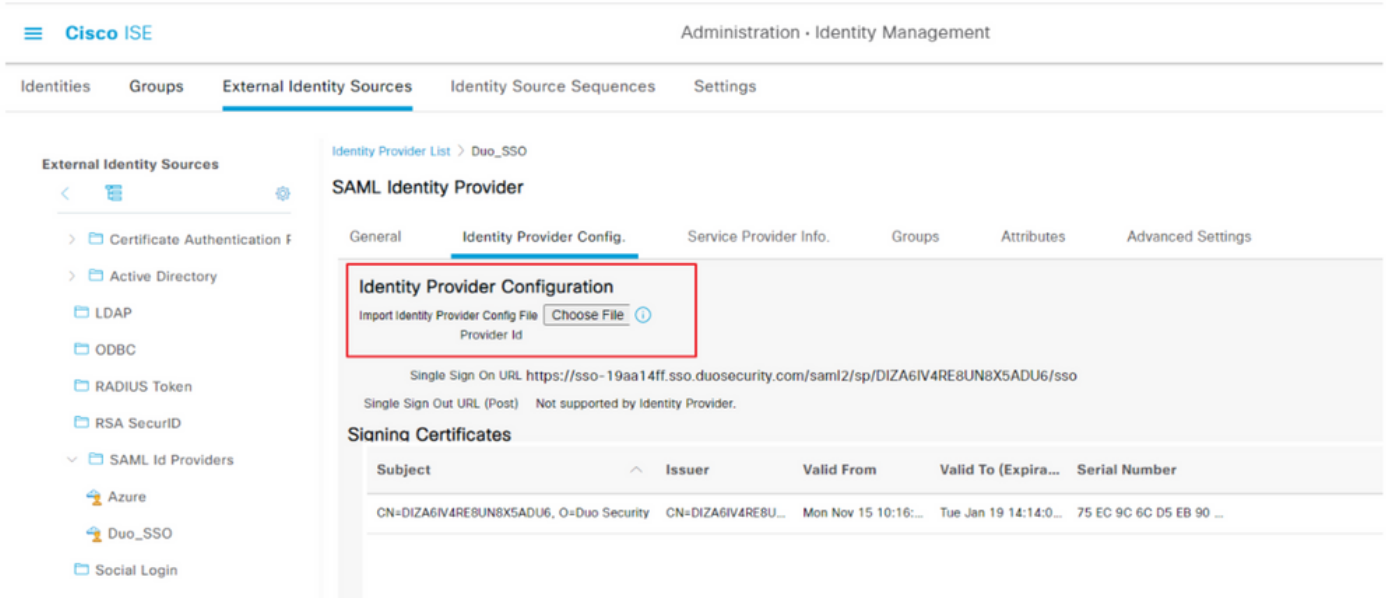


从Duo管理员门户导入SAML元数据XML文件

在ISE上，导航到Administration > Identity Management > External Identity Sources > SAML Id Providers.>选择您创建的SAML IdP，点击Identity Provider Configuration，然后点击选择文件按钮。

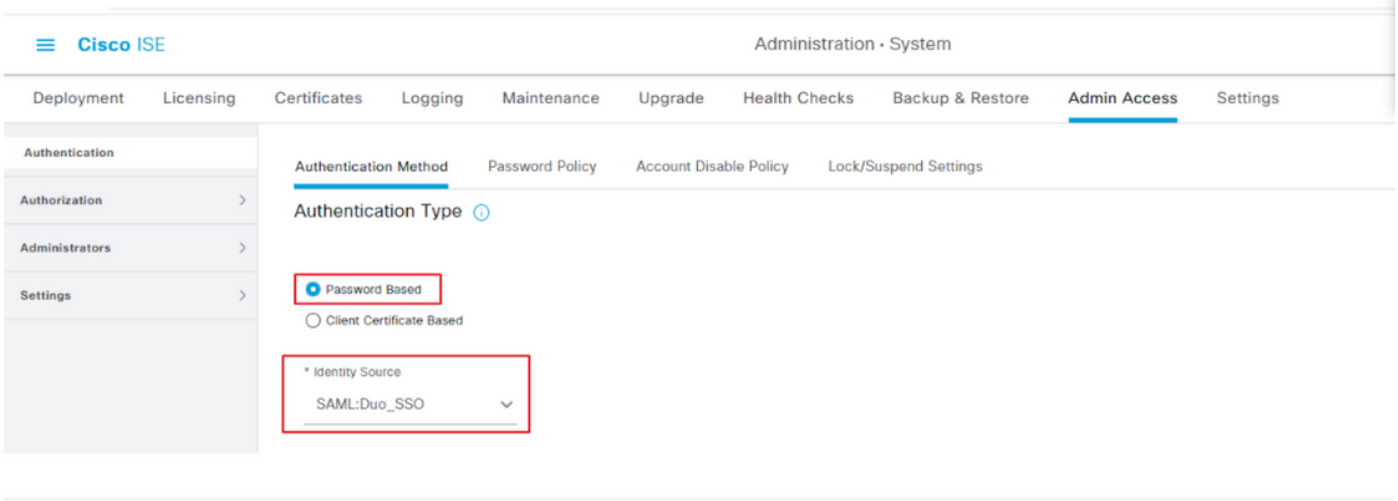
选择从Duo Admin门户导出的**SSO IDP元数据XML**文件，并单击**Open**以保存。（本文档的Duo部分也提到了此步骤。）

SSO URL和签名证书是：



配置ISE身份验证方法

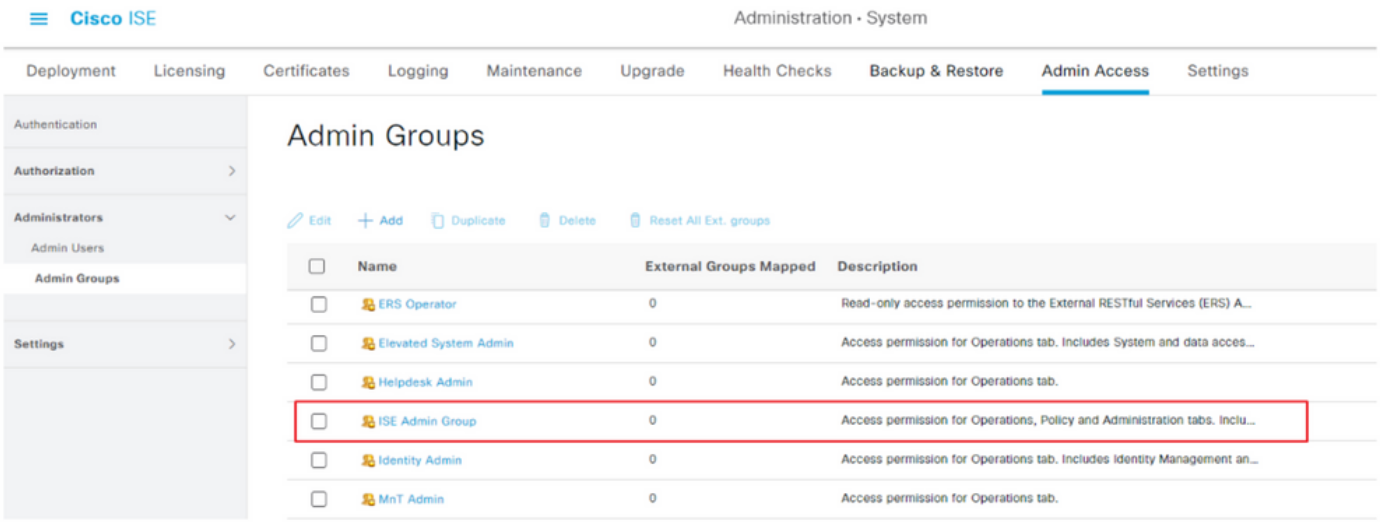
导航到Administration > System > Admin Access > Authentication > Authentication Method(或者)并选择Password-Based（基于密码）单选按钮。从身份源(Identity Source)下拉列表中选择之前创建的所需IdP名称，如图所示：



创建管理员组

导航到Administration > System > Admin Access > Authentication > Administrators > Admin Group，点击**超级管理员**，然后点击**复制**按钮。输入**Admin group Name**，然后单击**Submit**按钮。

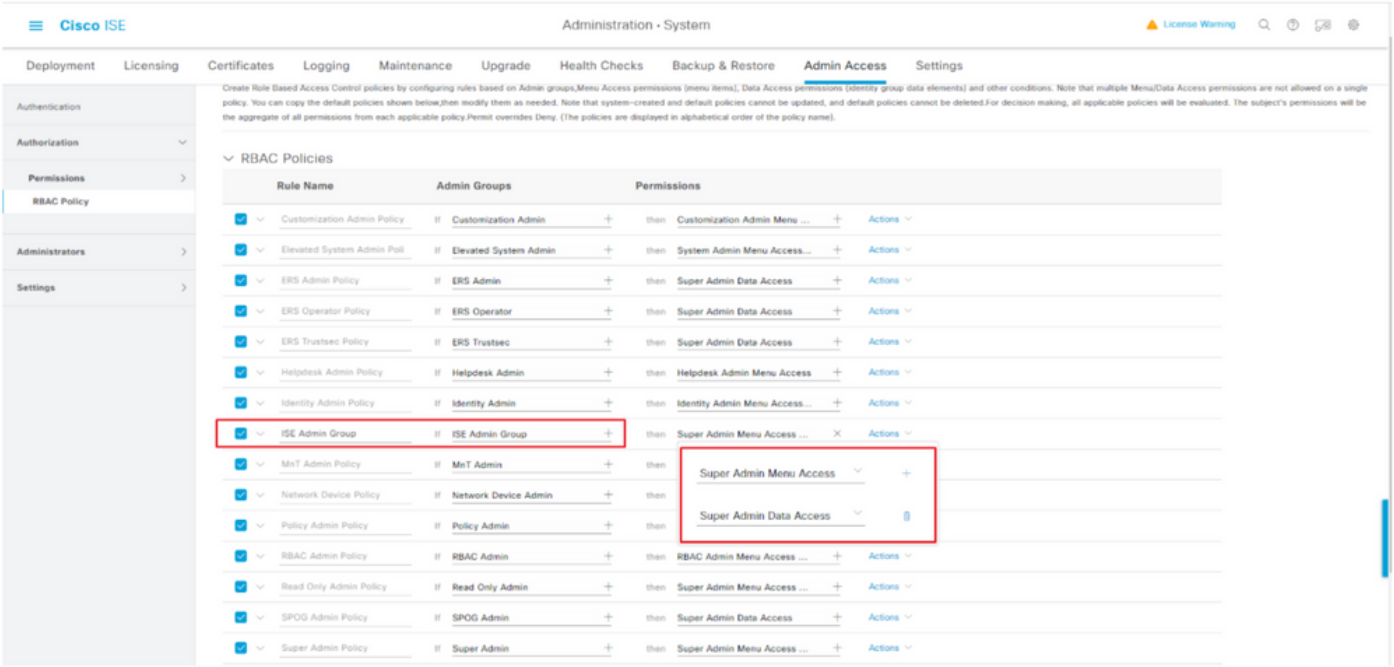
这将为管理员组提供超级管理员权限。



为管理员组创建RBAC策略

导航到Administration > System > Admin Access > Authorization > RBAC Policy，然后选择与**超级管理员策略**对应的**操作**。单击。Duplicate > Add the Name field > Save

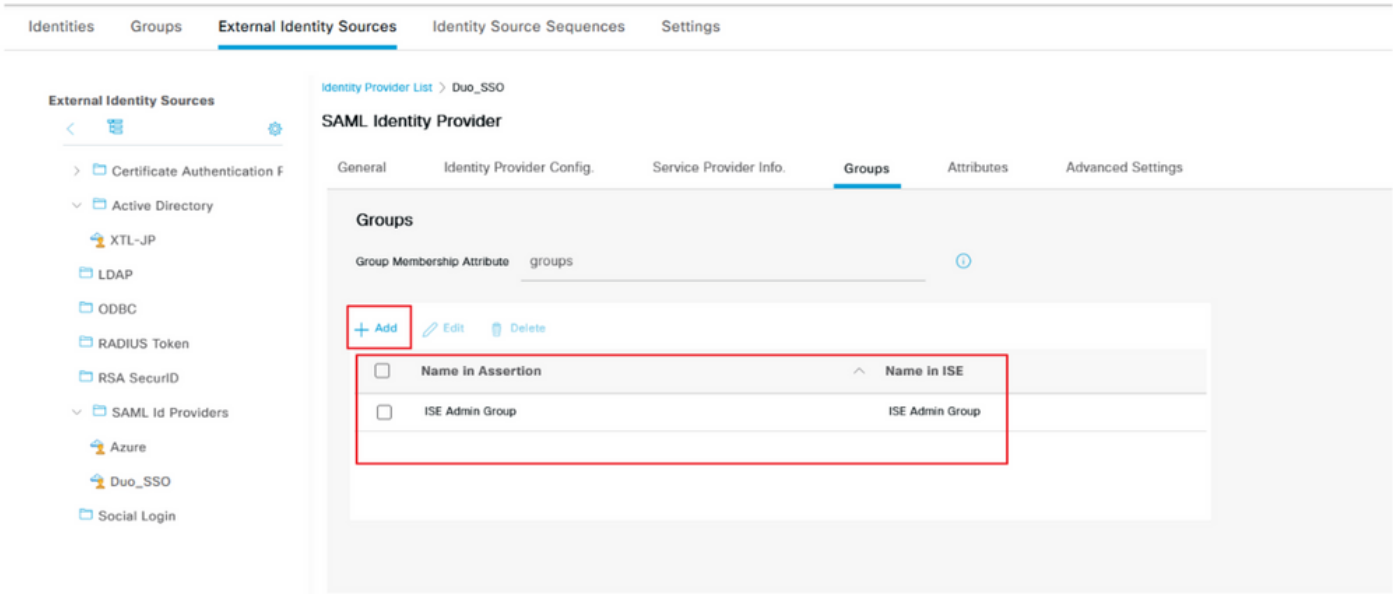
访问的权限与超级管理员策略相同。



添加组成员身份

在ISE上，导航至Administration > Identity Management > External Identity Sources > SAML Id Providers(SSID名称)并选择您创建的SAML IdP。单击**Groups**，然后单击Add按钮。

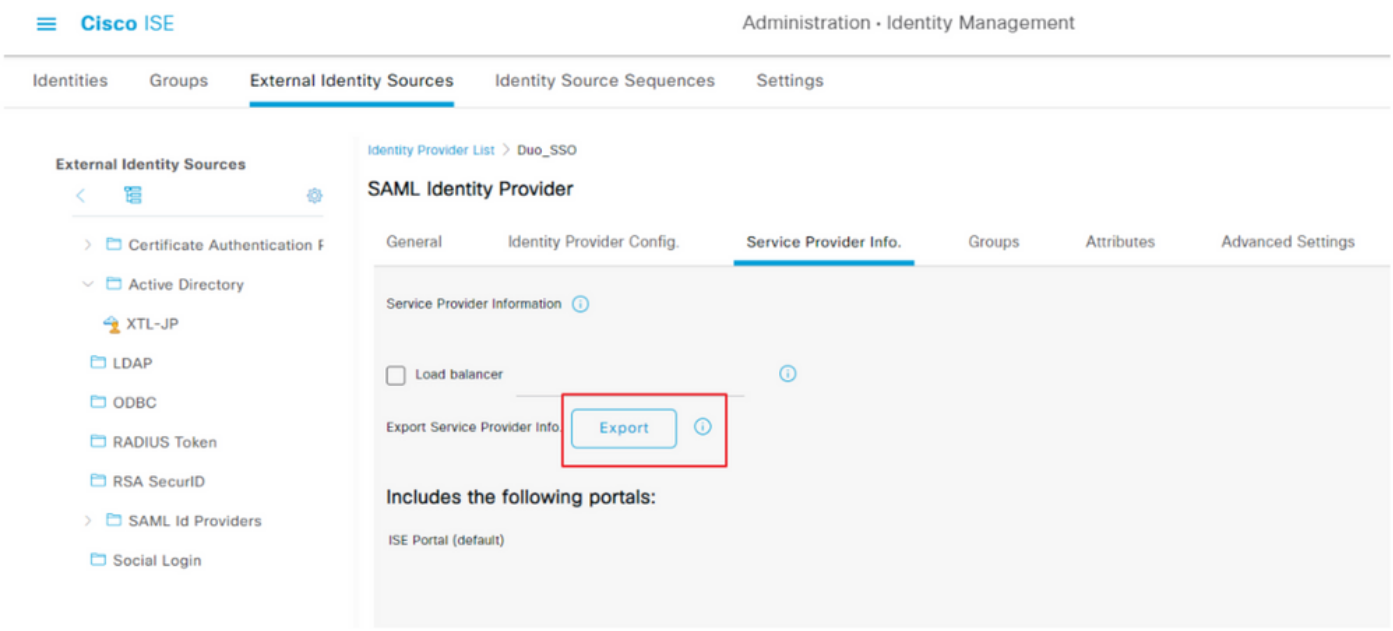
在断言中添加名称（ISE管理员组的名称），并从下拉列表中选择所创建的基于角色的访问控制(RBAC)组（第4步），然后单击**Open**以保存该组。系统将自动填充SSO URL和签名证书：



导出SP信息

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

将该选项卡切换到“SP信息”。然后单击导出按钮，如图所示：



下载.xml文件并保存。请记录AssertionConsumerServiceLocation URL and **entityID**值，因为这些详细信息在双核SSO门户中是必需的。

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

以下是从Duo Generic SAML Integration中需要配置的元文件中收集的相关详细信息/属性

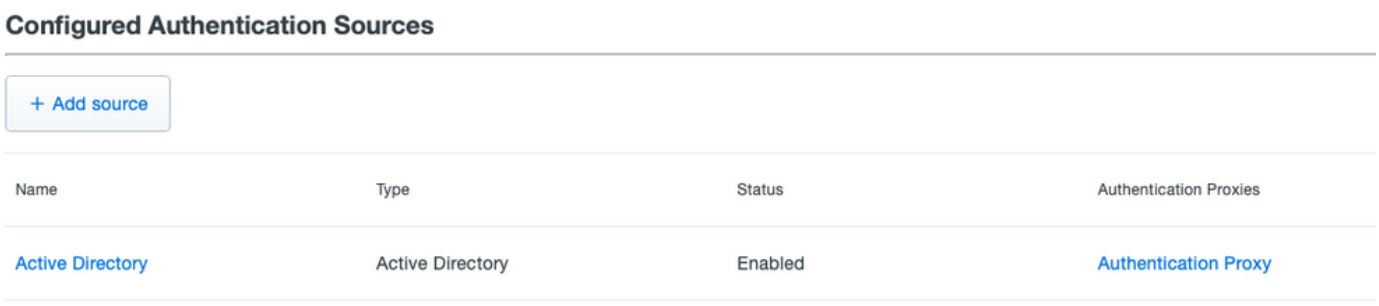
entityID = http://CiscoISE/7fdfc239-631e-439c-a3ab-f5e56429779d。

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

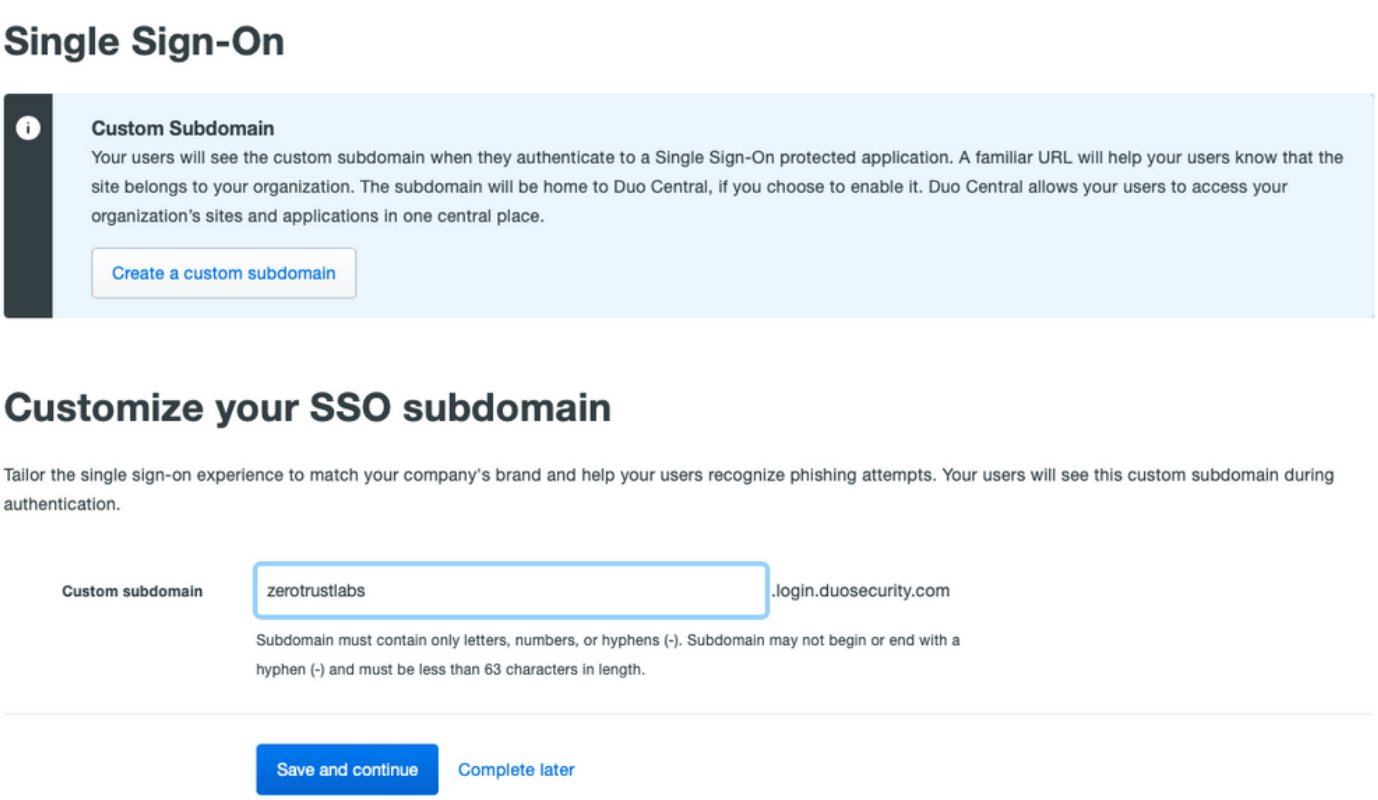
AssertionConsumerService位置= https://isenodename.com:8443/portal/SSOLoginResponse.action，其中isenodename是在XML文件（位置）中找到的实际ISE FQDN名称。

第二步：配置ISE的双核SSO

检查此KB以配置带AD的双核SSO作为身份验证源。



选中此KB以启用自定义域的SSO。

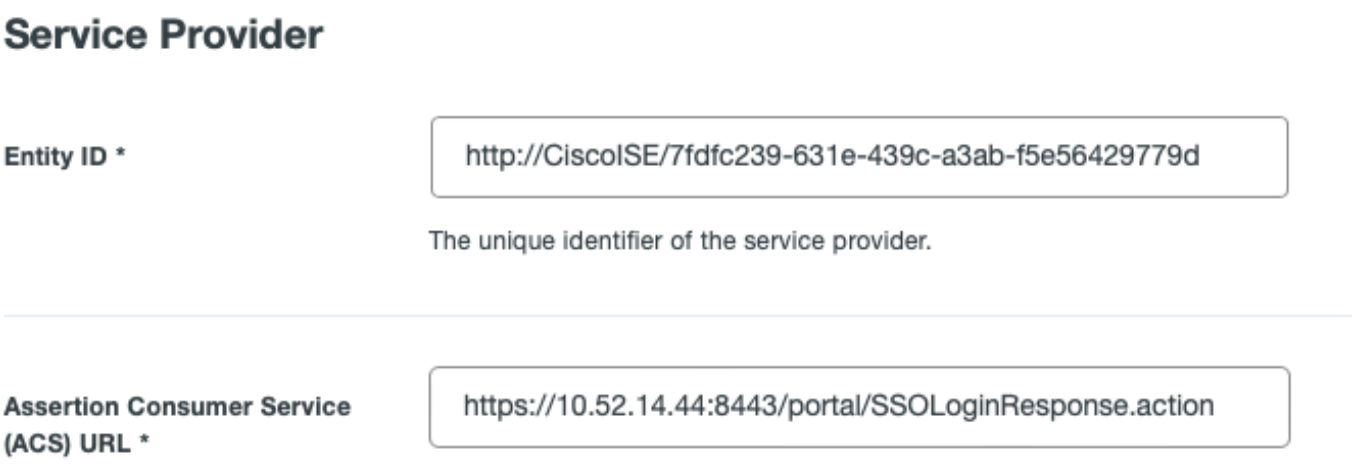


第三步：将Cisco ISE与Duo SSO集成为通用SP

检查此KB的第1步和第2步以将思科ISE与Duo SSO集成为通用SP。

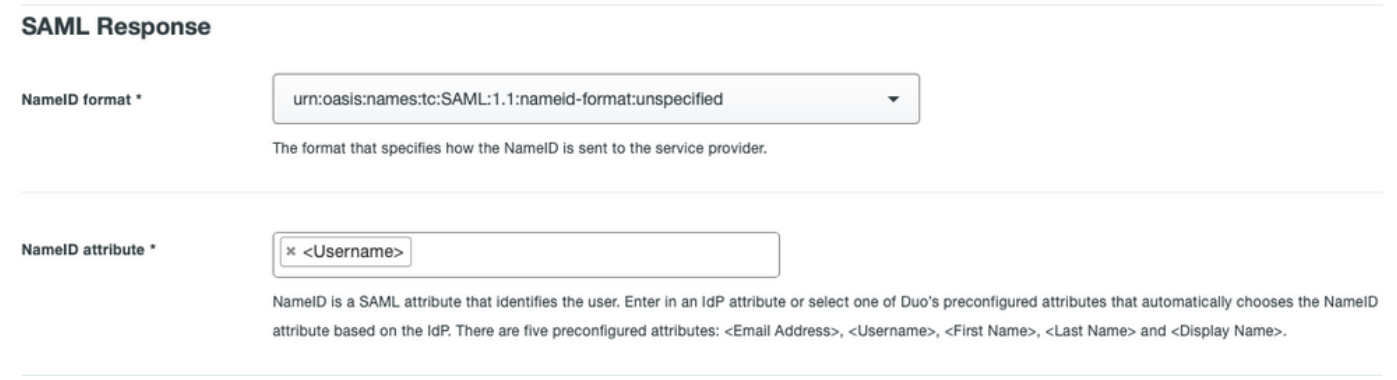
在双管理面板中配置通用SP的Cisco ISE SP详细信息：

名称	描述
实体Id	http://CiscoISE/7fdfc239-631e-439c-a3ab-f5e56429779d
断言消费者服务(ACS) URL	https://10.x.x.x:8443/portal/SSOLoginResponse.action

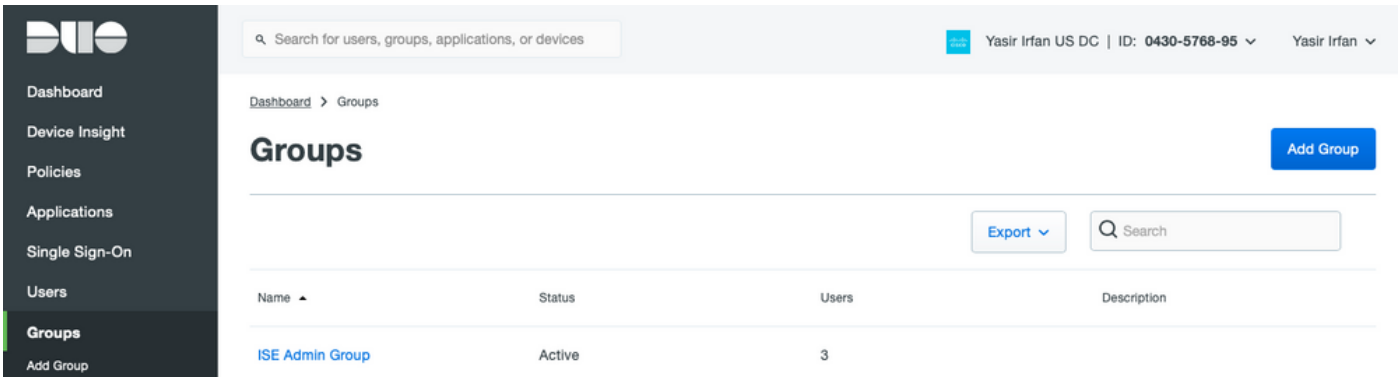


配置Cisco ISE的SAML响应：

名称	描述
NameID格式	urn：oasis：名称：tc：SAML：1.1：nameid-format：未指定
NameID属性	用户名

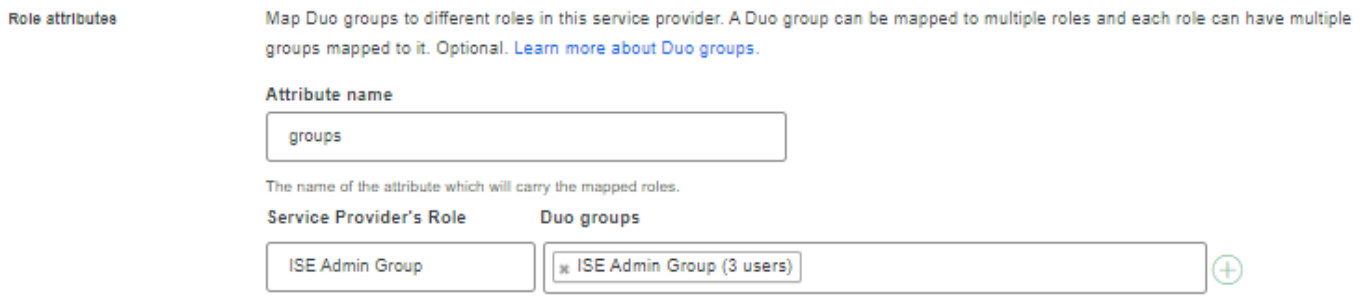


在Duo Admin Panel中创建名为Cisco Admin Group的组，并将ISE用户添加到此组，或在Windows AD中创建组，并使用目录同步功能将其同步到Duo Admin面板。

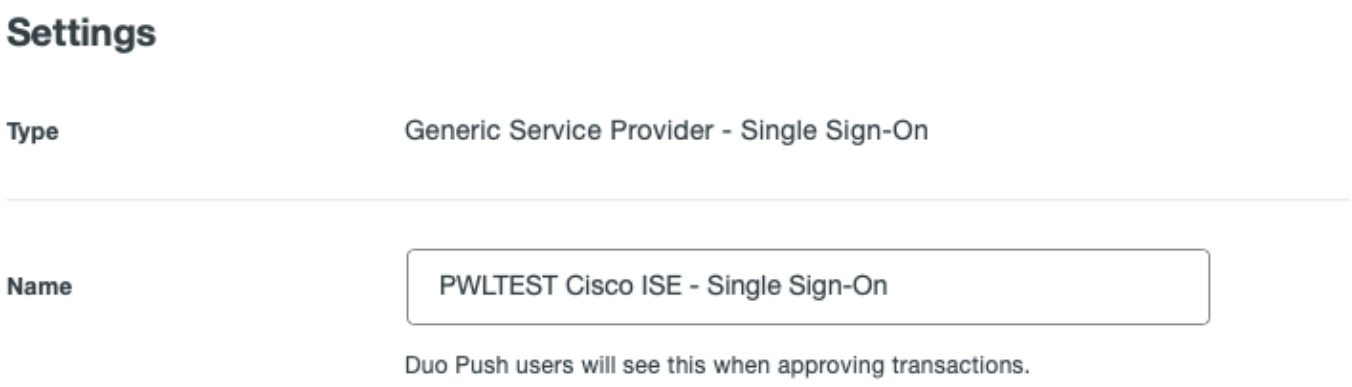


配置思科ISE的角色属性：

名称	描述
属性名称	组
SP角色	ISE管理员组
Duo组	ISE管理员组

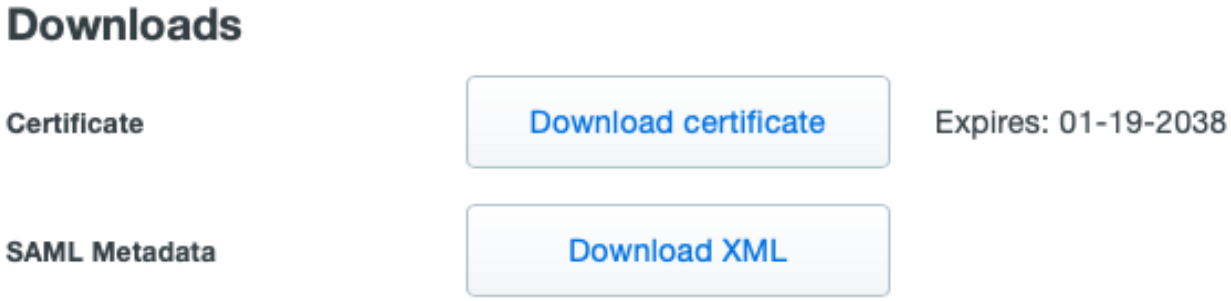


在Settings部分的**Name**选项卡中为此集成提供相应的名称。



单击**Save**按钮以保存配置，请参阅此KB以获取更多详细信息。

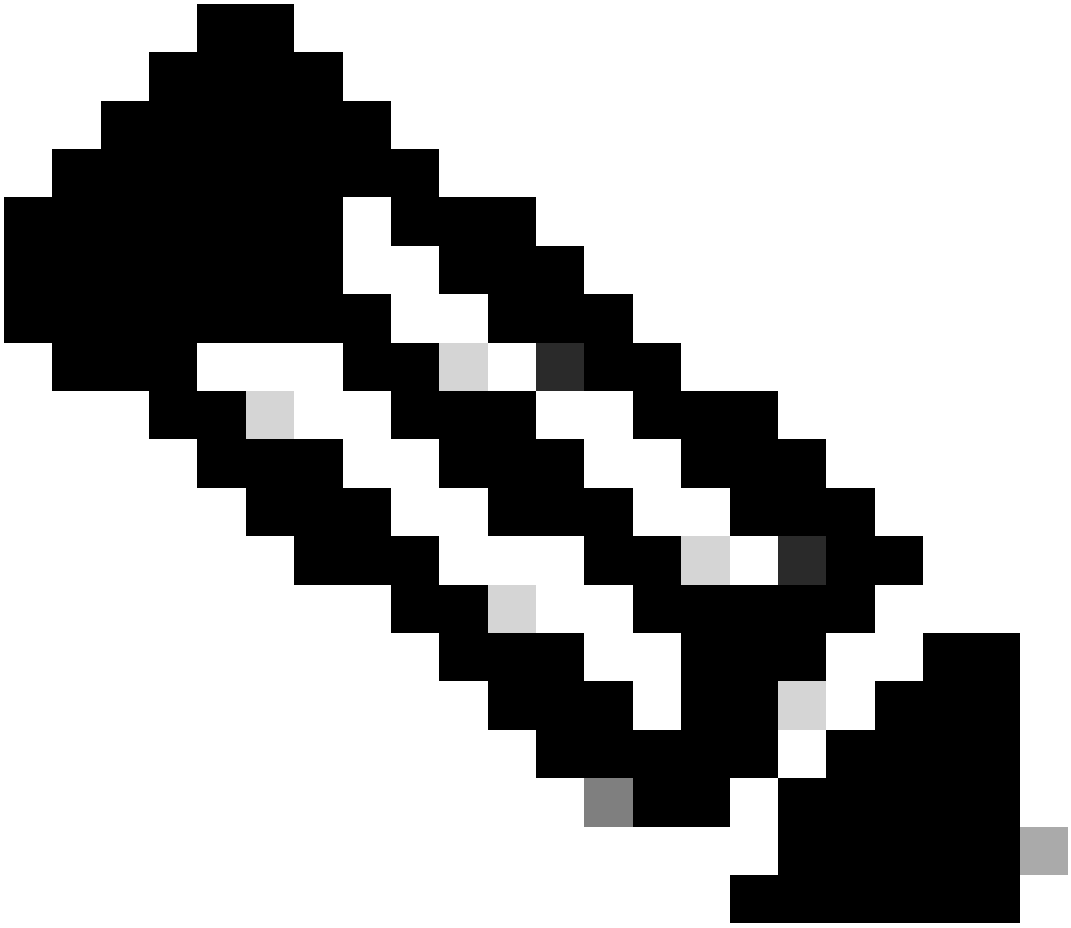
单击**Download XML**以下载SAML元数据。



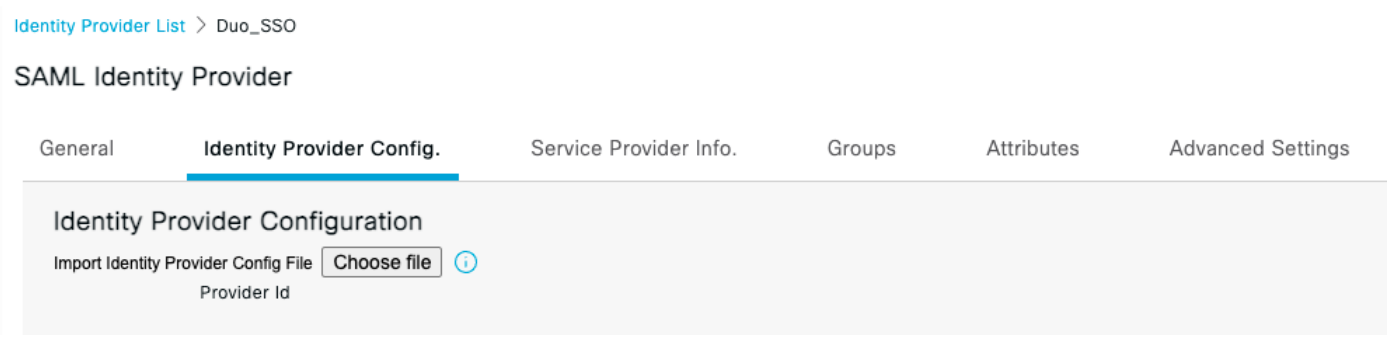
通过导航到Administration > Identity Management > External Identity Sources > SAML Id Providers > Duo_SSO将SAML元数据下载从双核Admin面板上传到Cisco ISE。

将选项卡切换到**Identity Provider Config.**，然后单击**Choose** file按钮。

选择步骤8中下载的**元数据XML**文件，然后单击**保存**。



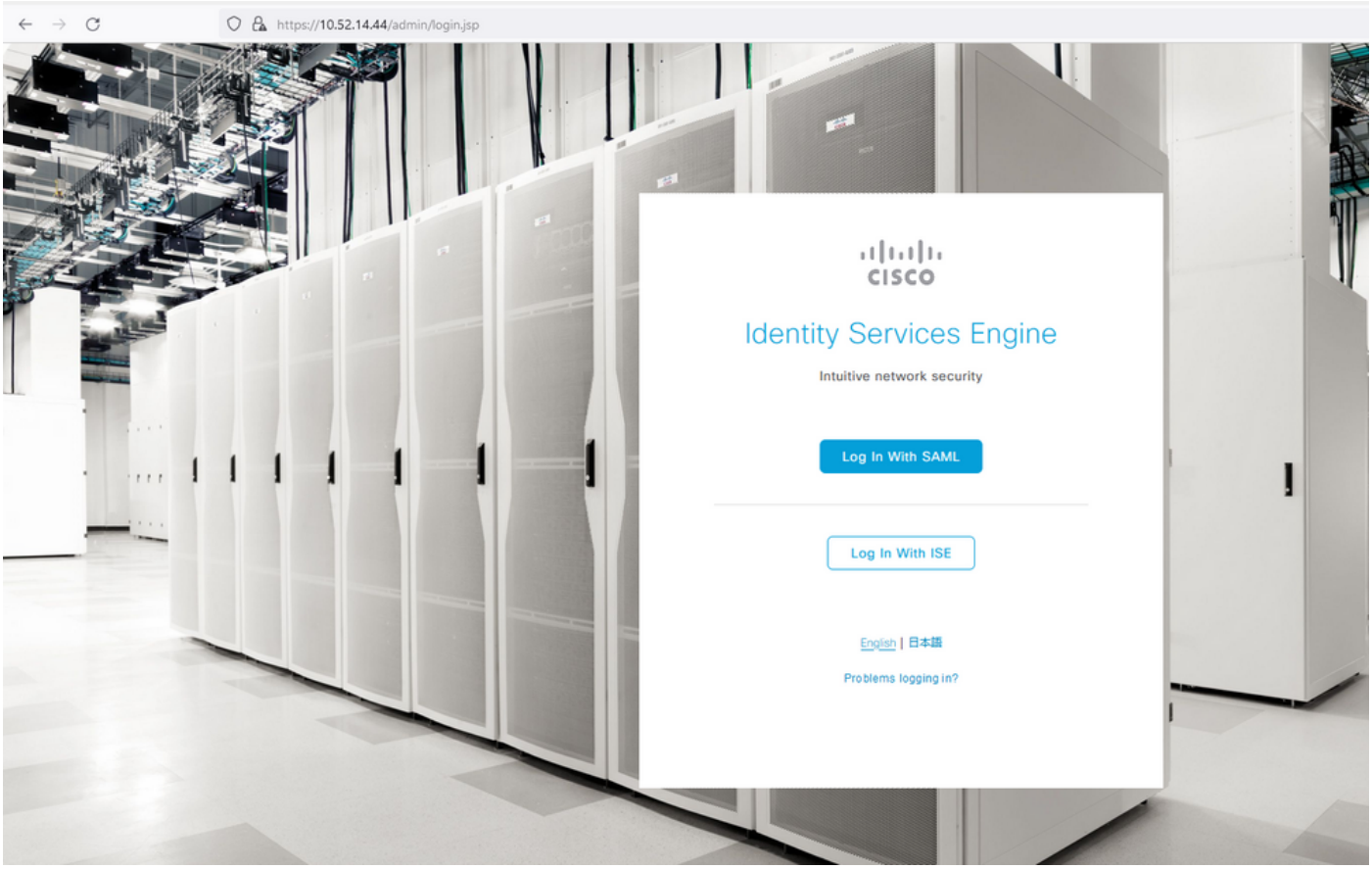
注意：此步骤在配置SAML SSO与Duo SSO集成部分（第2步）下提到。从Duo Admin门户导入**SAML元数据XML**文件。



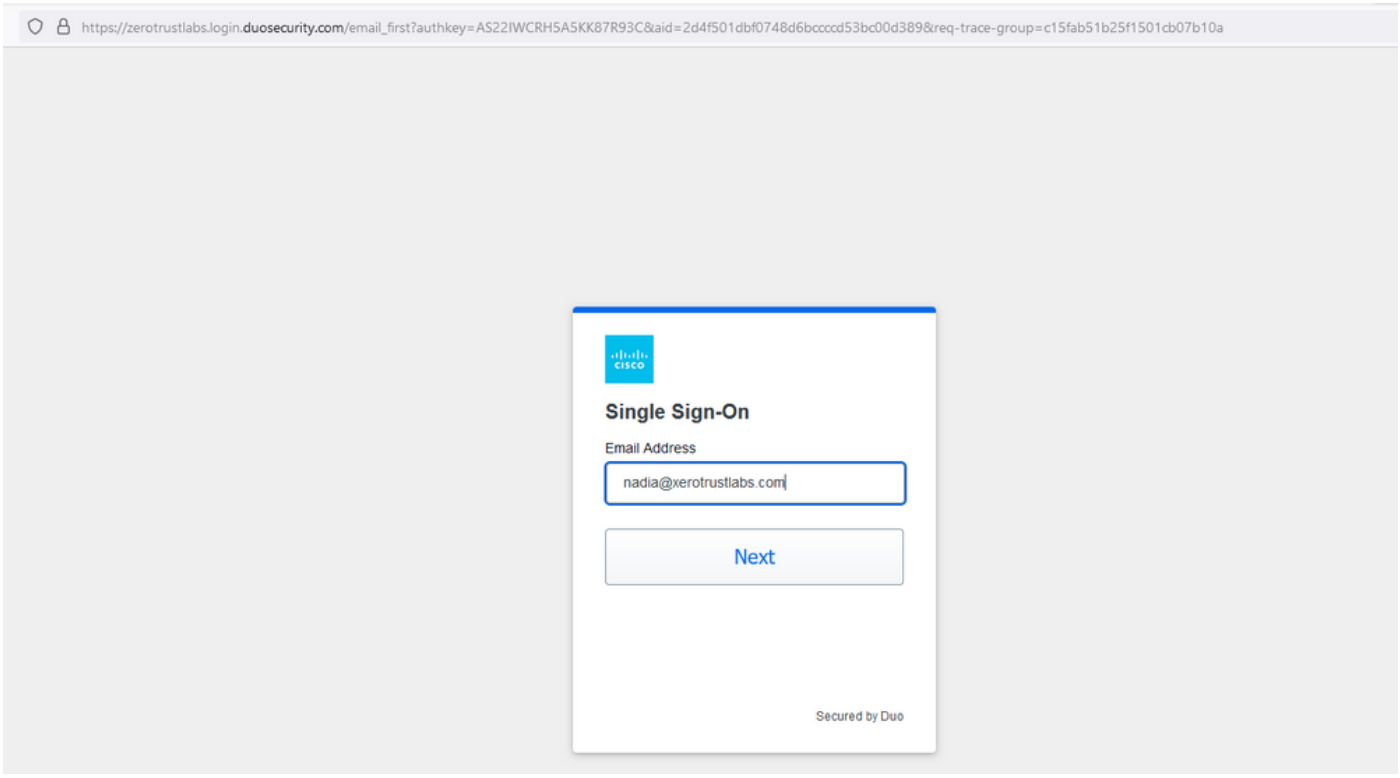
验证

测试与Duo SSO的集成

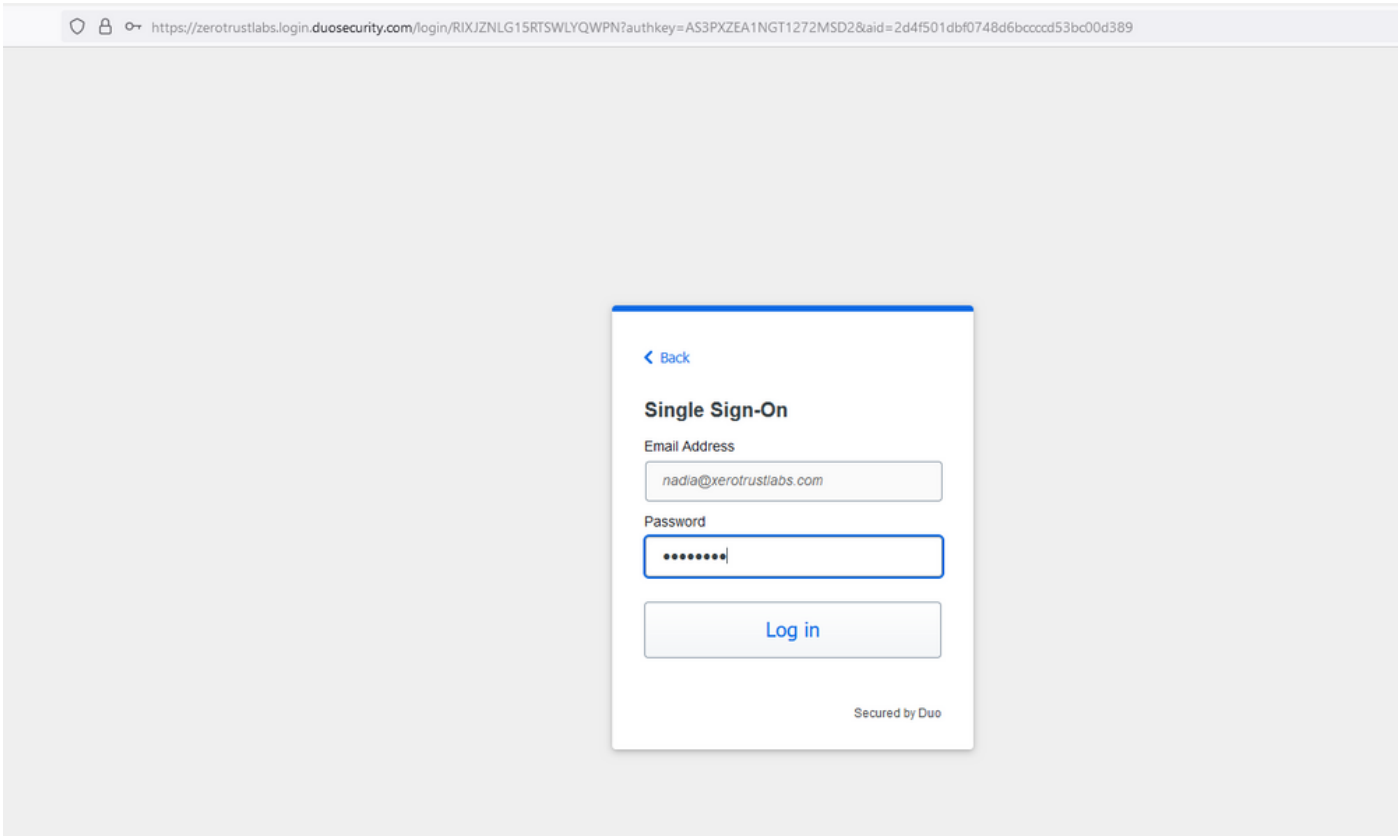
1. 登录**Cisco ISE管理面板**并单击**Log In With SAML**。



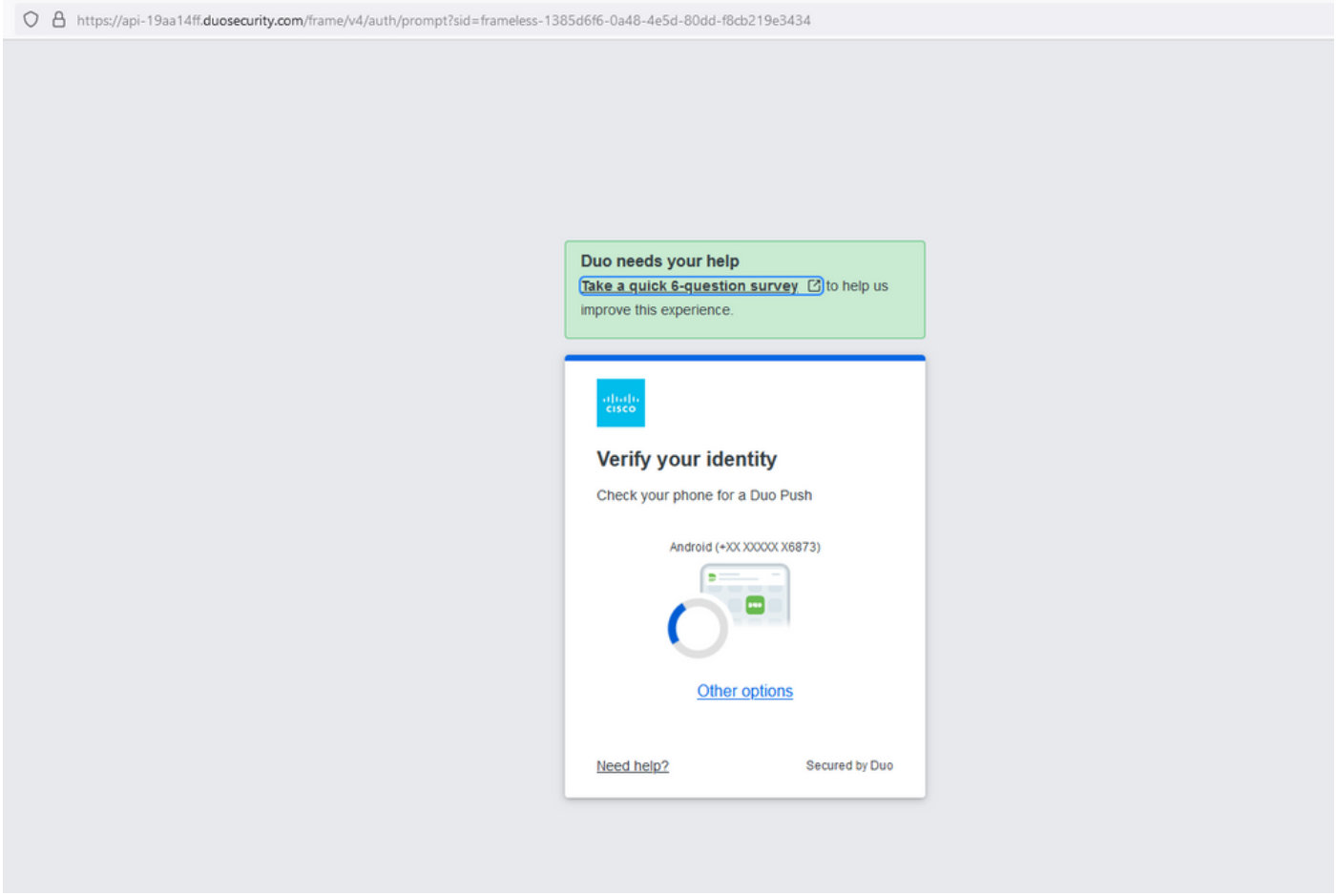
2. 已重定向到“SSO”页，输入电子邮件地址并单击**下一步**。



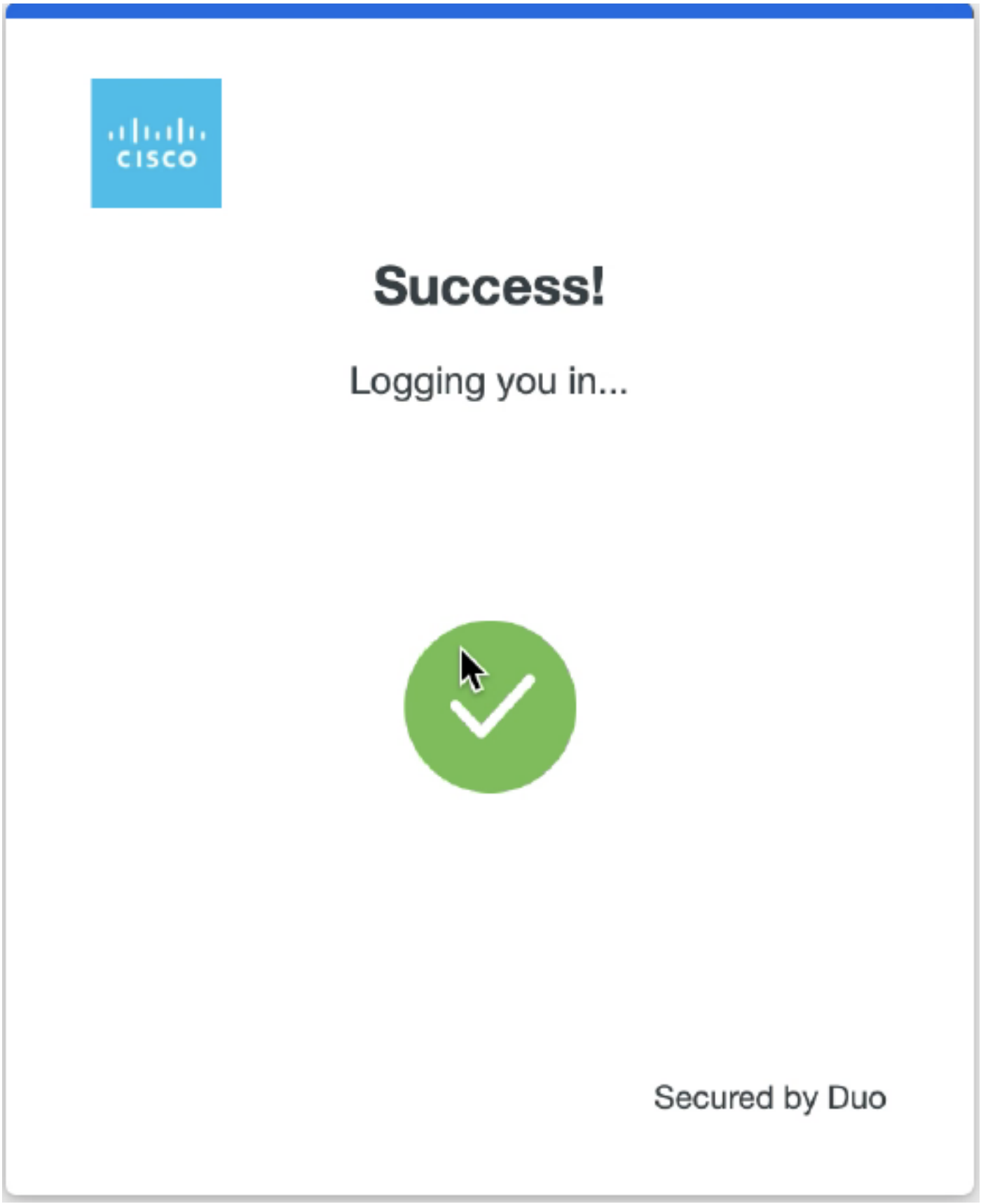
3. 输入口令，然后单击**Log in**。



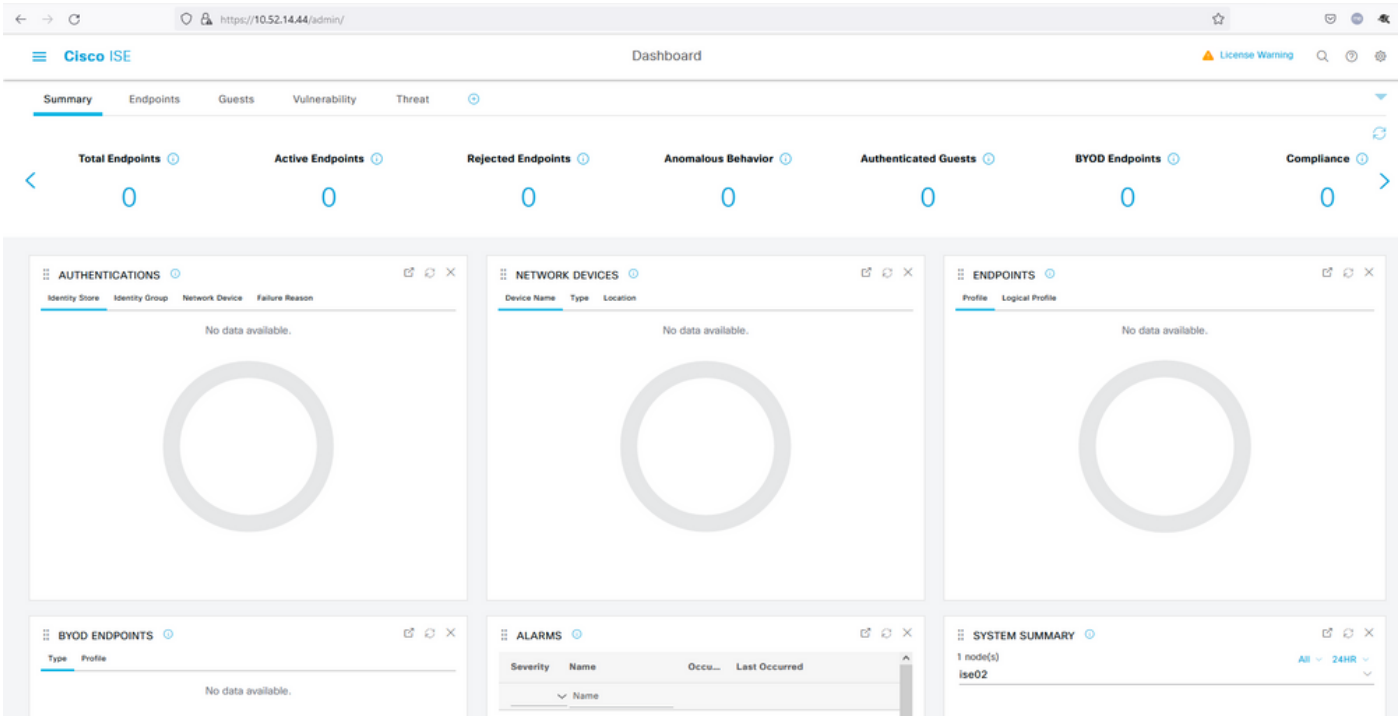
4. 您的移动设备上将显示Duo Push提示。



5. 接受提示后，您会获得一个窗口并自动重定向到ISE Admin页面。



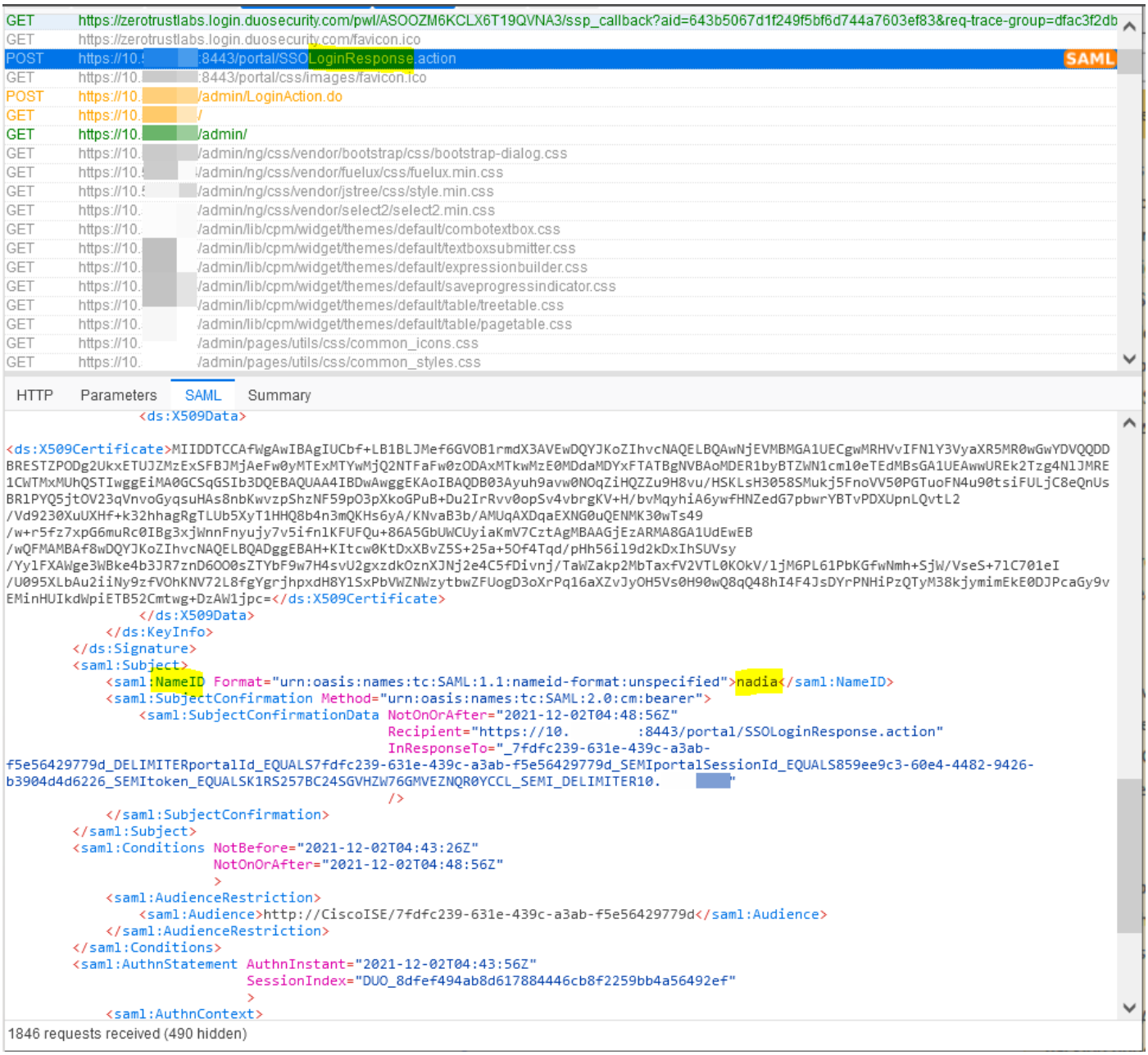
6. ISE管理员GUI访问权限页面。



故障排除

- 下载Mozilla FF的SAML Tracer扩展插件https://addons.mozilla.org/en-US/firefox/addon/saml-tracer/。

- 滚动到SSOLoginResponse.action数据包。在**SAML**选项卡下，您可以看到多个从双人SAML发送的属性：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+LB1BLJMef6GVOB1rmdX3AVEwDQYJKoZIhvcNAQELBQAwNjEVMBMGA1UECgwMRHVvIFNlY3VyaXR5MR0wGwYDVQQDDBRESTZPODg2UkxETUJZMzExSFBJMjAeFw0yMTExMTYwMjQ2NTFaFw0zODAxMTkwMzE0MDdaMDYxFTATBgNVBAoMDER1byBTZWN1cml0eTEdMBsGA1UEAwwUREk2Tzg4N1JMRE1CWTMxMUhQSTIwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDB03Ayuh9avw0NOqZiHQZZu9H8vu/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上的实时日志：

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

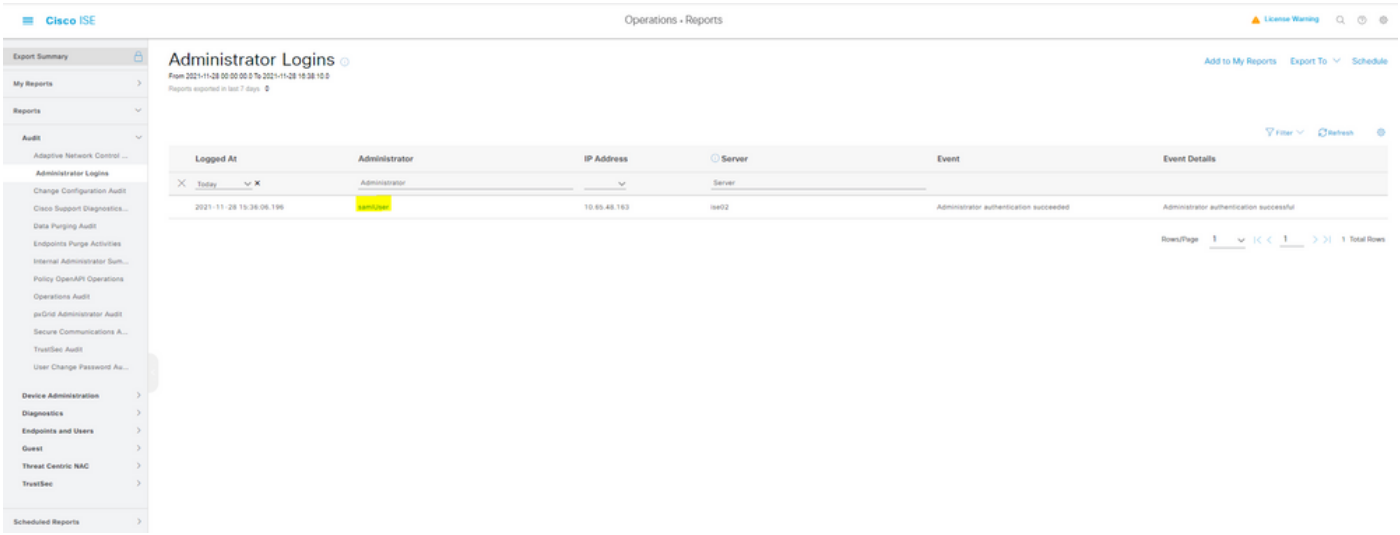
Other Attributes

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

Steps

5231	Guest Authentication Passed

- ISE上的管理登录日志：用户名：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

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。