Configure ISE 3.1 GUI Admin Log in Using SAML Integration with Duo SSO and Windows AD

Contents

Introduction

Prerequisites

- Requirements
- Components Used

Background Information

- Identity Provider (IdP)
- Service Provider (SP)
- SAML
- SAML Assertion

High-Level Flow Diagram

Configure SAML SSO Integration with Duo SSO

- Step 1. Configure SAML IdP on ISE
  - Configure Duo SSO as an External SAML Identity Source
  - Import the SAML Metadata XML file from the Duo Admin Portal
  - Configure ISE Authentication Method
  - Create an Admin Group
  - Create an RBAC Policy for the Admin Group
  - Add Groups Membership
  - Export SP Information
- Step 2. Configure Duo SSO for ISE
- Step 3. Integrate Cisco ISE with Duo SSO as a Generic SP

Verify

- Testing the Integration with Duo SSO

Troubleshoot

Introduction

This document describes how to configure Cisco ISE 3.1 SAML SSO integration with an External Identity Provider like Cisco Duo SSO.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco Identity Services Engine (ISE) 3.1
- Basic knowledge about Security Assertion Markup Language (SAML) Single Sign-On (SSO)

deployments (SAML 1.1)
- Knowledge of Cisco DUO SSO
- Knowledge of Windows Active Directory

Components Used

The information in this document is based on these software and hardware versions:

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

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

Identity Provider (IdP)

It is the Duo SSO in this case, that verifies and asserts a user identity and access privileges to a requested resource (the 'Service Provider').

Duo SSO acts as an IdP, authenticating your users using existing on-premises Active Directory (AD) with SAML 1.1 or any SAML 2.0 IdP (for example, Microsoft Azure) and prompting for two-factor authentication before permitting access to your service provider application.

When configuring an application to be protected with Duo SSO you must send attributes from Duo SSO to the application. Active Directory works with no additional setup, but if you used a SAML(2.0) IdP as your authentication source, verify that you configured it to send the correct SAML attributes.

Service Provider (SP)

The hosted resource or service that the user intends to access; Cisco ISE Application Server in this case.

SAML

SAML is an open standard that allows IdP in order to pass authorization credentials to SP.

SAML transactions use Extensible Markup Language (XML) for standardized communications between the identity provider and service providers. SAML is the link between the authentication of the identity of the user and the authorization in order to use a service.

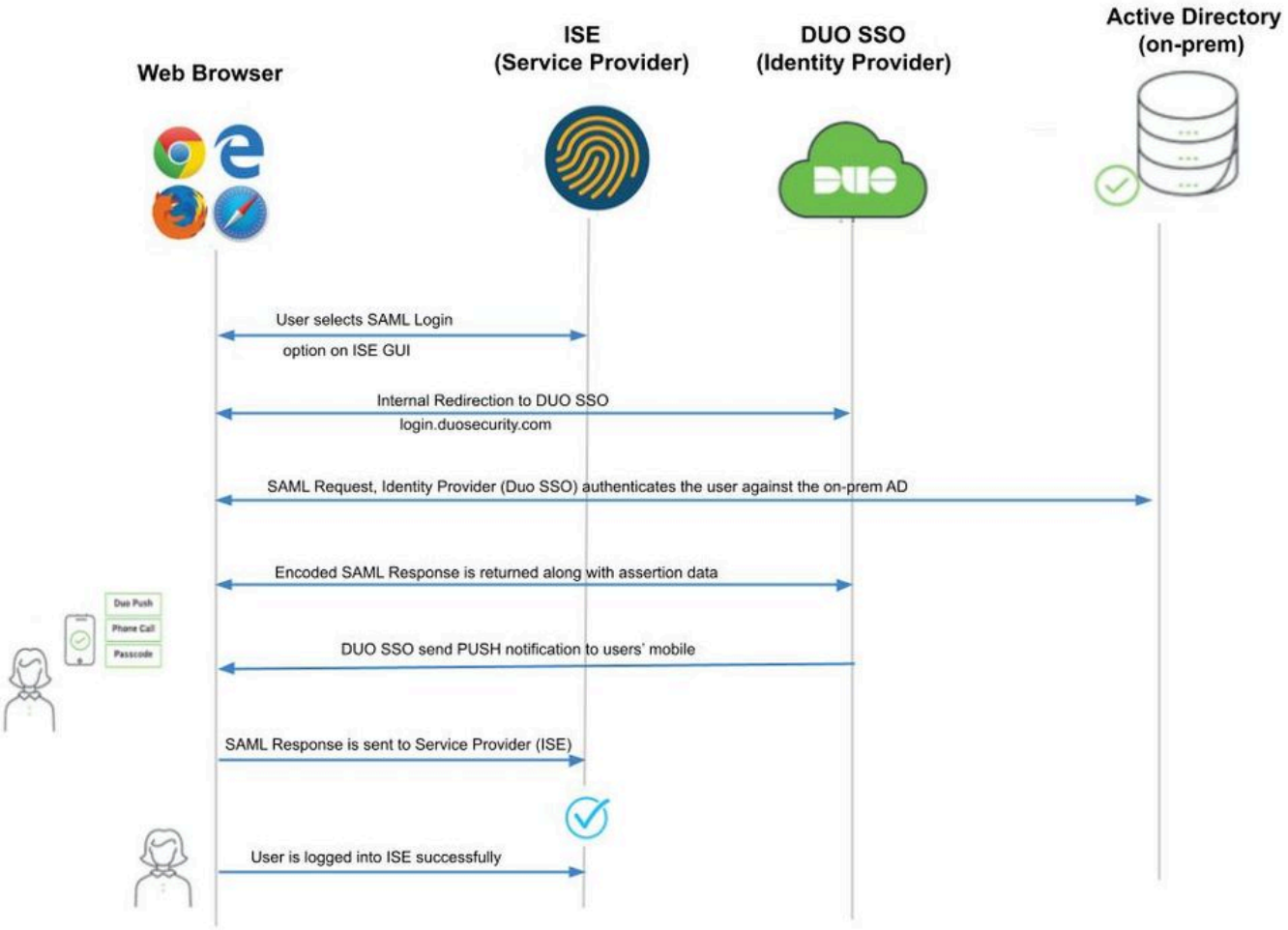
SAML Assertion

A SAML Assertion is the XML document that the IdP sends to the service provider that contains the user authorization. There are three different types of SAML Assertions – authentication, attribute, and authorization decision.

- Authentication assertions prove the identification of the user and provide the time the user logged in and what method of authentication they used (for example, Kerberos, two-factor, and so on).
- The attribution assertion passes the SAML attributes, specific pieces of data that provide information

about the user, to the SP.
- An authorization decision assertion declares if the user is authorized in order to use the service or if the IdP denied their request due to a password failure or lack of rights to the service.

High-Level Flow Diagram



Flow:

1. The user logs in to ISE using the Login Via SAML option.
2. ISE (SAML SP) redirects the browser of the user to Duo SSO with a SAML request message.

Note: In a distributed environment, you can get an Invalid Certificate error and Step 3. can now work. Hence, for a distributed environment, Step 2. differs slightly in this way:
Issue: ISE temporarily redirects to the Portal of one of the PSN nodes (on port 8443).
Solution: In order to ensure ISE presents the same certificate as the admin GUI certificate, ensure the System Certificate that you trust is valid for Portal usage too on all PSN nodes.

---

3. User logs in with primary AD credentials.
4. Duo SSO forwards this to AD which returns a response back to Duo SSO.
5. Duo SSO requires the user to complete two-factor authentication by sending a PUSH on the mobile.
6. The user completes Duo two-factor authentication.

7. Duo SSO redirects the browser of the user to the SAML SP with a response message.
8. The user is now able to log in to ISE.

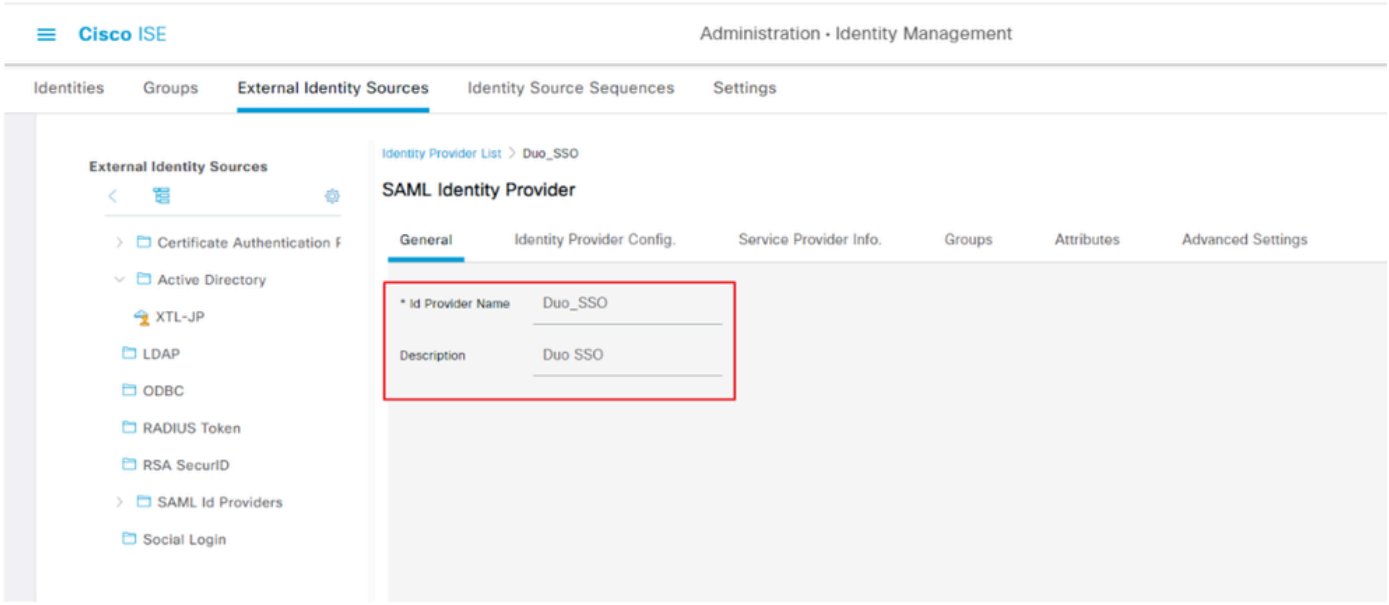
Configure SAML SSO Integration with Duo SSO

Step 1. Configure SAML IdP on ISE

Configure Duo SSO as an External SAML Identity Source

On ISE, navigate to Administration > Identity Management > External Identity Sources > SAML Id Providers and click the **Add** button.

Enter the name of the IdP and click **Submit** in order to save it. The IdP name is significant only for ISE as shown in the image:

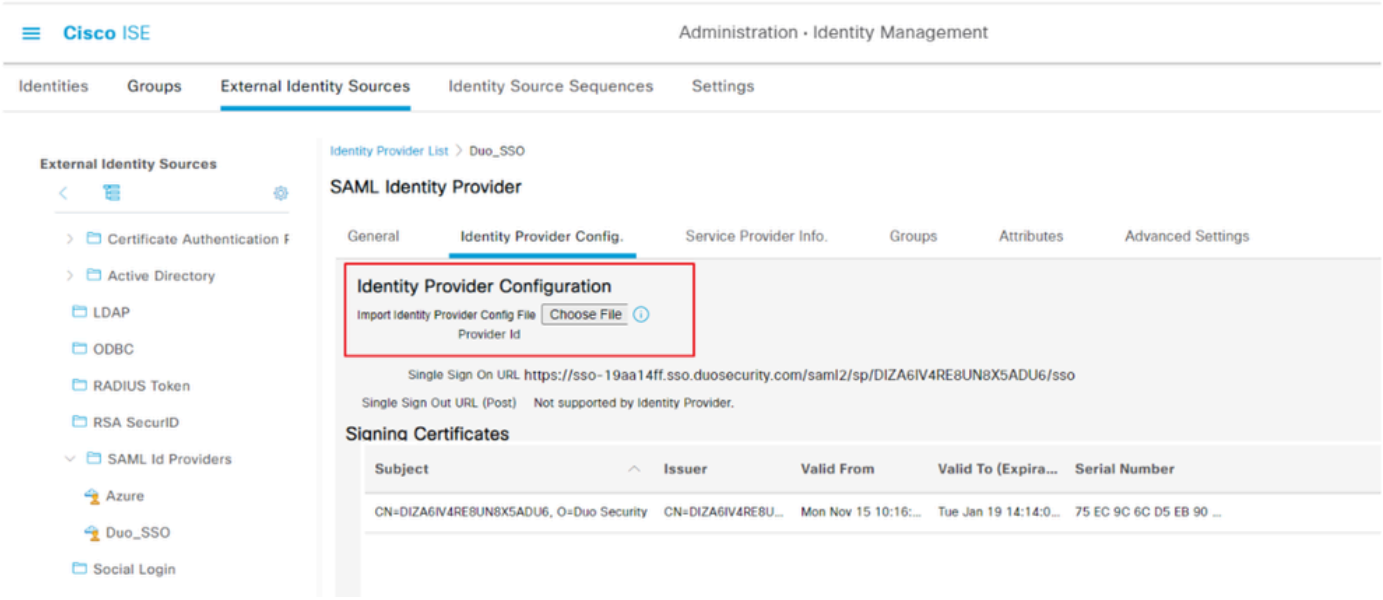


Import the SAML Metadata XML file from the Duo Admin Portal

On ISE, navigate to Administration > Identity Management > External Identity Sources > SAML Id Providers. > Choose the SAML IdP you created, click the Identity Provider Configuration and then the **Choose File** button.

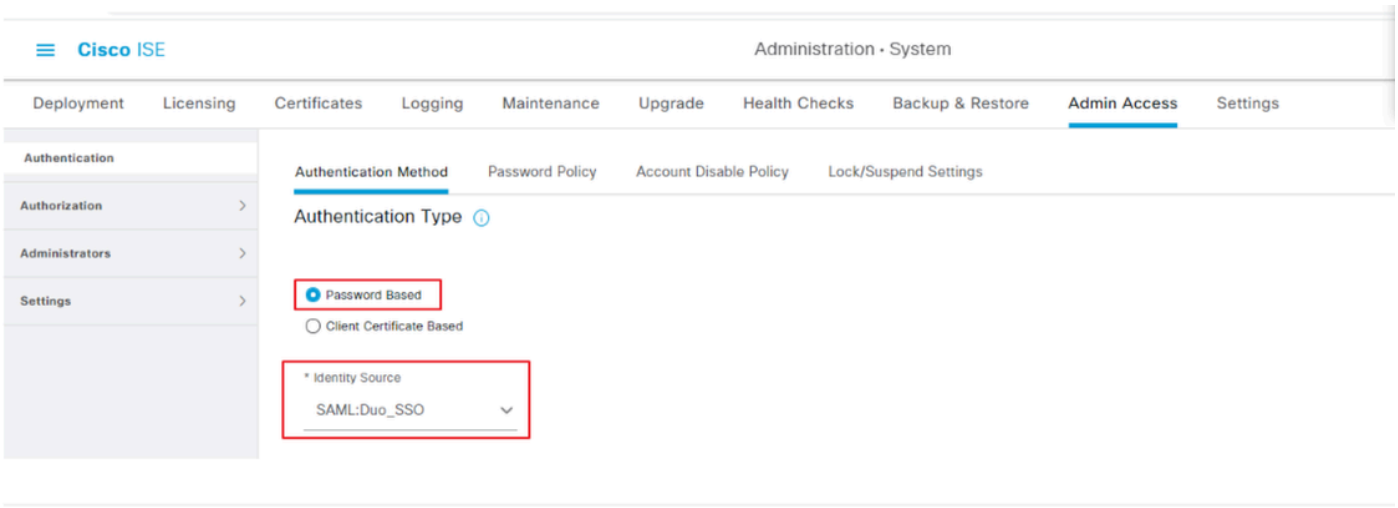
Choose the **SSO IDP Metadata XML** file exported from Duo Admin portal and click **Open** in order to save it. (This step is mentioned in the Duo section of this document as well.)

The SSO URL and Signing Certificates are:



Configure ISE Authentication Method

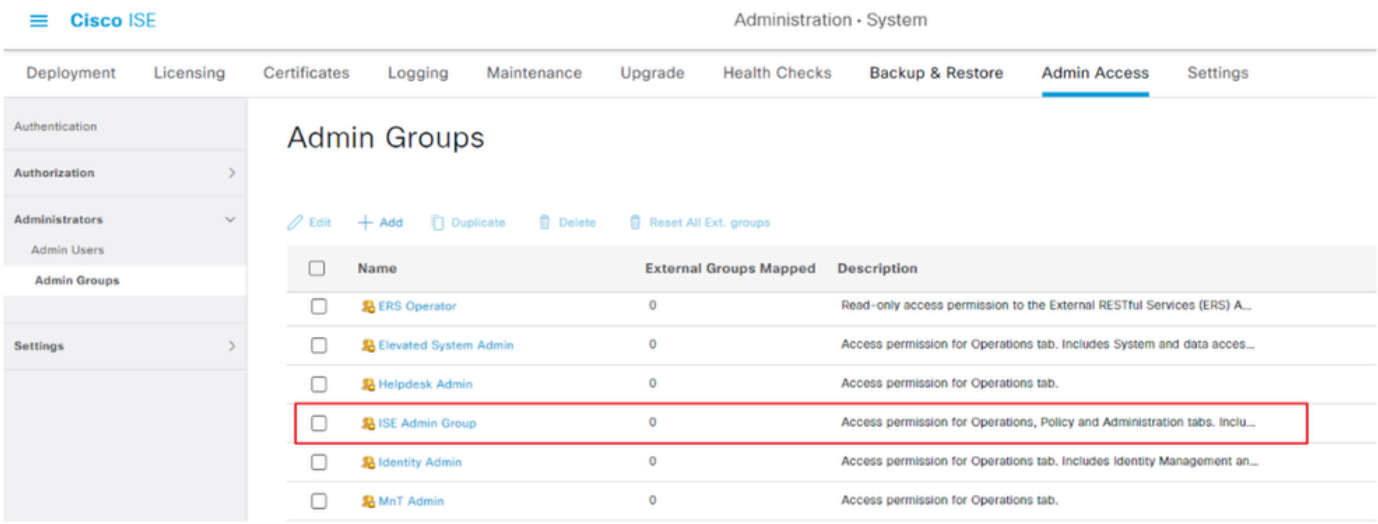
Navigate to Administration > System > Admin Access > Authentication > Authentication Method and choose the Password-Based radio button. Choose the required IdP Name created earlier from the Identity Source drop-down list as shown in the image:



Create an Admin Group

Navigate to Administration > System > Admin Access > Authentication > Administrators > Admin Group and click the **Super Admin** and then the **Duplicate** button. Enter the **Admin group Name** and click the **Submit** button.

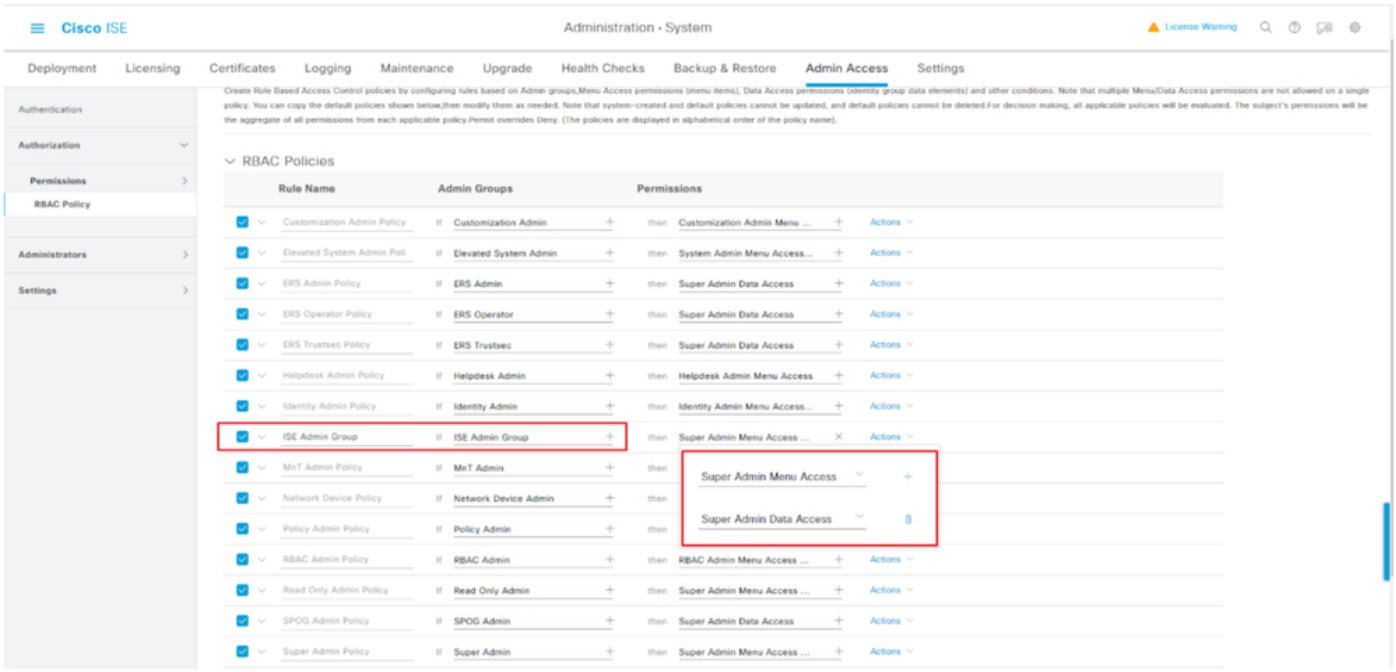
This provides Super Admin privileges to the Admin group.



Create an RBAC Policy for the Admin Group

Navigate to Administration > System > Admin Access > Authorization > RBAC Policy and choose the **Actions** corresponding to **Super Admin Policy**. Click Duplicate > Add the Name field > Save.

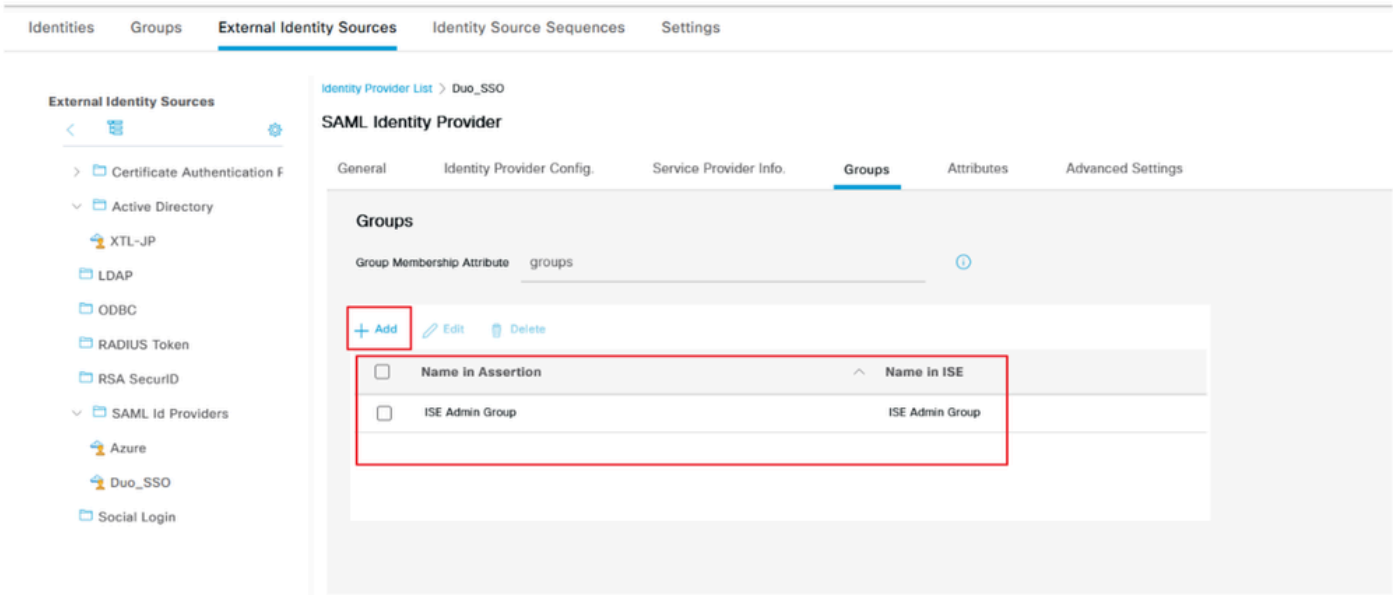
The Permissions for access are the same as the Super Admin Policy.



Add Groups Membership

On ISE, navigate to Administration > Identity Management > External Identity Sources > SAML Id Providers and choose the SAML IdP you created. Click **Groups** and then the Add button.

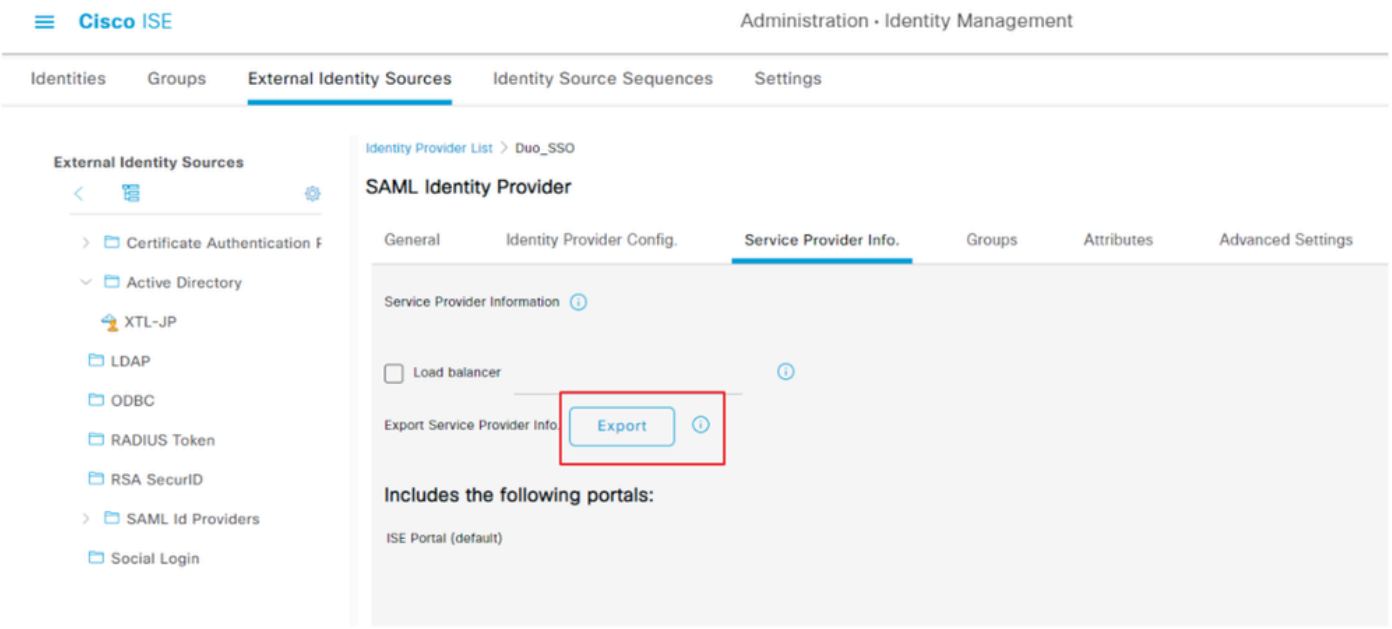
Add the Name in Assertion (Name of the ISE Admin group) and from dropdown choose the Role-Based Access Control (RBAC) Group created (Step 4.) and click **Open** in order to save it. The SSO URL and Signing Certificates are auto-populated:



Export SP Information

Navigate to Administration > Identity Management > External Identity Sources > SAML Id Providers > (Your SAML Provider) .

Switch the tab to SP Info. and click the **Export** button as shown in the image:



Download the .xml file and save it. Make a note of the AssertionConsumerService Location URL and **entityID** value as these details are required in the Duo SSO Portal.


```
<?xml version="1.0" encoding="UTF-8"?><md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metada
TUxfaXNlMDIueGVyb3RydXN0bGFicy5jb20wHhcNMjExMTE1MjI1OTM0WhcNMjYxMTE0MjI1OTM0
WjAnMSUwIwYDVQQDExxTQU1MX2lzZTAyLnhlcm90cnVzdGxhYnMuY29tMIICIjANBgkqhkiG9w0B
AQEFAAOCAg8AMIICCgKCAgEAxw7scSLMH1ApI3O/7+vWsGP4schoJJHlVeJKHuJVgm19SXViW8Ab
WL9hQEXDr+U/zzp7fAq0YjckeNJg6VMhasao5tY4cutrAZK2F/kYvdVN+0N2cJUSTdJZNdKO+hcj
VmUgClUi6Xa4PJNw+1yhj8PwrDlpzfgXZLi3wlo5sMRGrg8NeSbShPJVakIEF2FoIOhXTOOSH4ZN
sD4q99dzrAv2m6y74vtUOGqwX4RRMOdvr7DIMNd2U/trh41QT85SY5c7Ol6fRWtY9omZBdUOS2JC
ihWnC9ug7FE0qdPm2h5KiZvxJck9OqVXDHvtRKctW5gwzfX8Hu7DQKqs9Oh04HRUxg2GEiuiXCQZ
```

5p63KfoRly5oW5OUKOLIMdyhDl+8uP+n+Jo3ufR8lKe42+/rws5Ct1hg4jozddutKkw2vyxMEg5/
ZpAz/goRIOmBN4r3n3FNGZV1uTfbb1Mz8yvY61ccGgTU1/Iynt9maNHxjbFtAP+HaiMPisfTKDRJ
OLx91v+xKpb+opcOxqVK1qOUs0yGVvfycaFNZ3jP5wBNBzSAi7cvXk7sIW9WM7DC84OjC/r9EbaX
Wll7MLV+16Z+FeDnzhzFVjq/cb61eNvXKKwDFryFqBnDLLJGmJuZQ/EgROwkvseR8tNE3qIYVhOe
qfCKZUpWtZ+lGLDD3r5Op9UCAwEAAaN/MHOwIgYDVR0RBBswGYIXaXNlMDIueGVyb3RydXN0bGFi
cy5jb20wDAYDVR0TBAUwAwEB/zALBgNVHQ8EBAMCAuwwHQYDVR0OBBYEFAoHeqyYR5rOXpOVXODT
WdpDycOoMBOGA1UdJQQWMBQGCCsGAQUFBwMBBggrBgEFBQcDAjANBgkqhkiG9w0BAQwFAAOCAgEA
aoIIkyS8slDwjQrRsUVyPi17LvlOTleCUQBrnr5WNUWlaXIB7Cb9qrG9D2ced72miH6vUcxine78
V4loTsgVu3tVlslQrOLW2eNLSbaN1XqbVUl1sCZkA4wGt8uLPXOt8UYysecEPFXDONiKGPoIMaFg
3pP5525cJpeLRkgHjw1Z2qT54lsGd8Gdq6V666kliAt73kPwfDiZf/uDsCI+euIHDywLdOad51kJ
RWAsZO7tgxK3tJO9z7JU4oY1fI26DUN43++Ap3KSaDiz9gYJ3fFjR9hP/nF/ywyOOHO5MgHqhsMo
+zBMADukmprYC8qd+Oz76+NQ6TLXgUer7NQMty68tQYP4riupvc26CEmgEZ592jBgDdt2tkY9An4
Fl/rqJPhX2RISLdUt50NcBbIZVOJ/IjkqHj9UG1E/U8qYy3krWvZV+VV5ChVNzwiVTWFCEOHNOTh
l/yYdAAsODUBbwTqgJL1G3hNo+dA3LAgg/XKENFr+tt3LQOkwPAtjKFQsIX/4sgMetV4KSqUI3HZ
qw5uOt9WT578SZ5p1u/qj2cfx2wdqRVk5vSij6TxOpXIaCuY2L5YfeIMP/K49K+DecMBxCrKygNT
vGXOPkVG/yqgQ9OIfQZ1OD3/NZxGyBJdzSSkjHxiUdWf4lWj1tVU+qav8M3imsCRvcZJppaKJNo=</ds:X509Certificate></ds:X

Here are the details/attributes of interest gathered from the meta file which needs to be configured in the Duo Generic SAML Integration

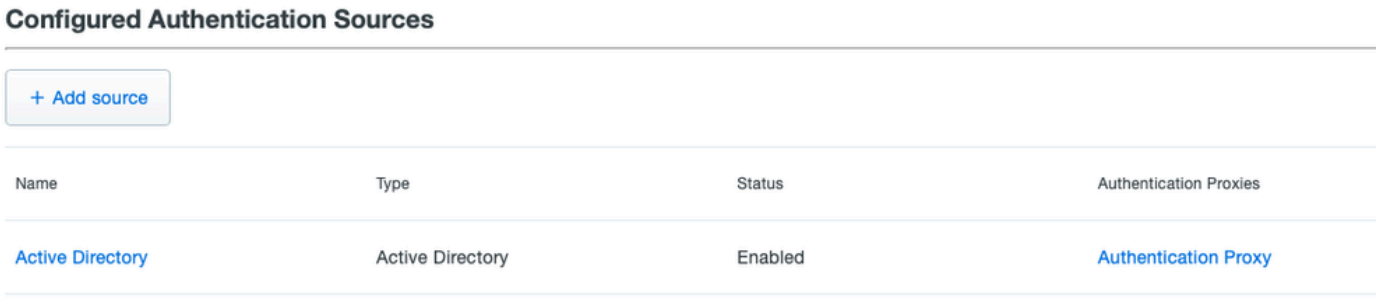
entityID = http://CiscoISE/7fdfc239-631e-439c-a3ab-f5e56429779d.

AssertionConsumerService Location = https://10.x.x.x:8443/portal/SSOLoginResponse.action where 10.x.x.x is the ISE IP found on the XML file (Location).

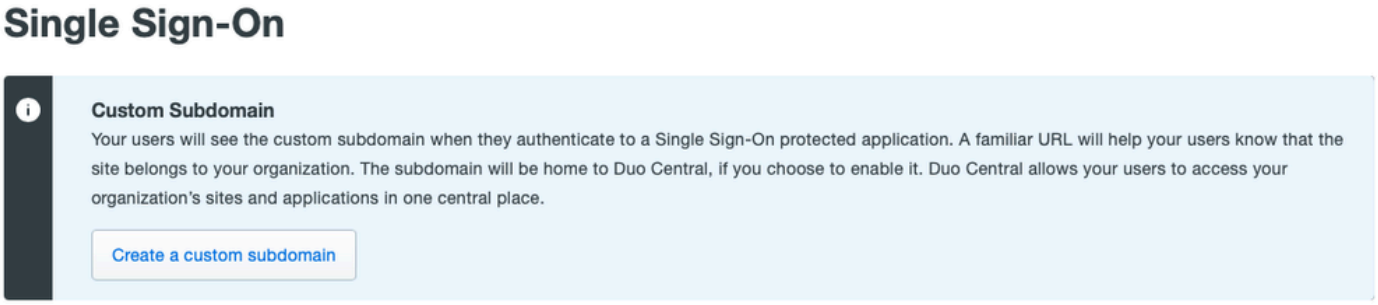
AssertionConsumerService Location = https://isenodename.com:8443/portal/SSOLoginResponse.action where isenodename is the actual ISE FQDN name found on the XML file (Location).

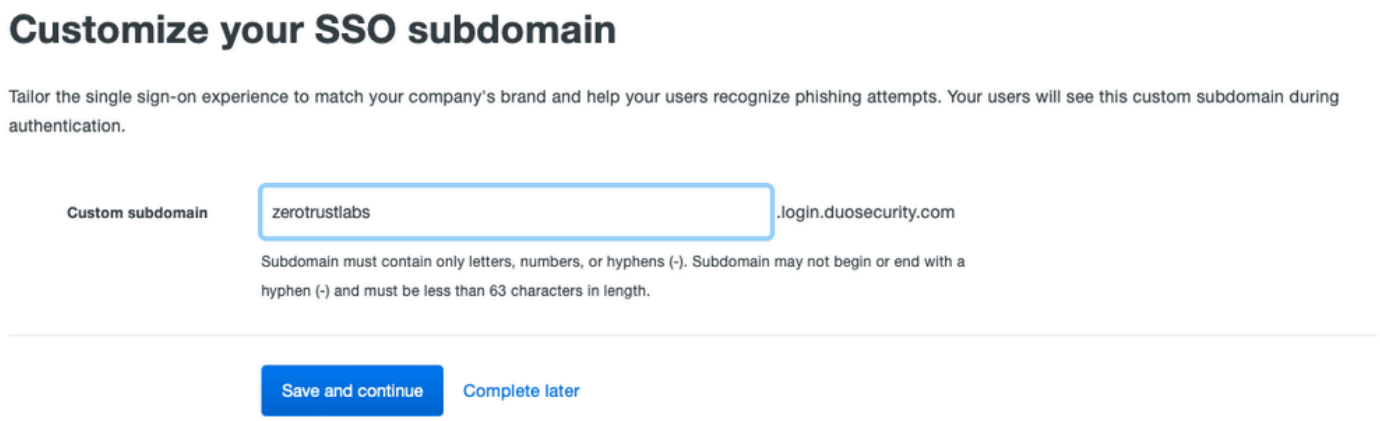
Step 2. Configure Duo SSO for ISE

Check this KB in order to configure Duo SSO with AD as an Authentication Source.



Check this KB in order to enable the SSO with your custom domain.



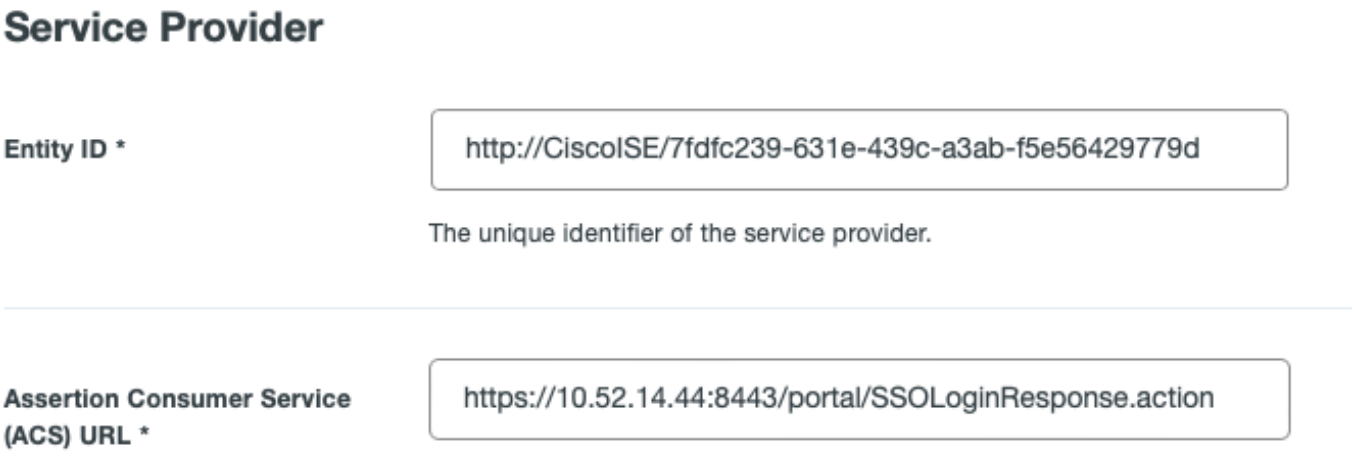


Step 3. Integrate Cisco ISE with Duo SSO as a Generic SP

Check Step 1. and Step 2. of this KB in order to integrate Cisco ISE with Duo SSO as a Genreic SP.

Configure Cisco ISE SP details in Duo Admin Panel for Generic SP:

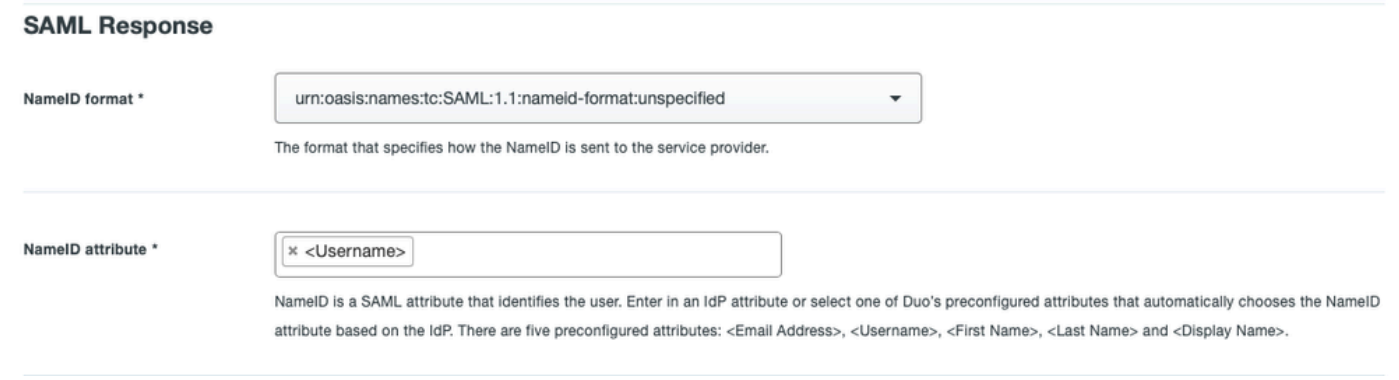
Name	Description
Entity ID	http://CiscoISE/7fdfc239-631e-439c-a3ab-f5e56429779d
Assertion Consumer Service (ACS) URL	https://10.x.x.x:8443/portal/SSOLoginResponse.action



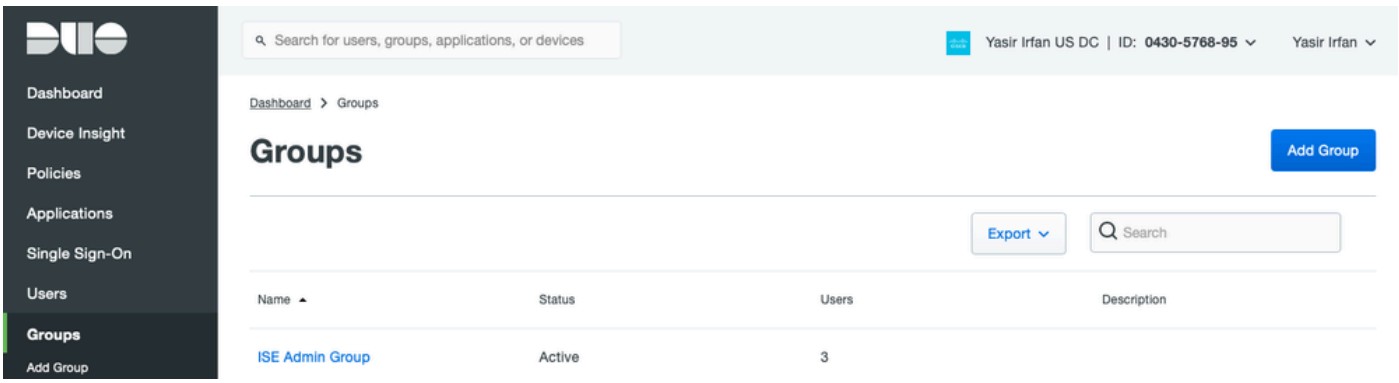
Configure SAML Response for Cisco ISE:

Name	Description
NameID format	urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified

NameID attribute	Username

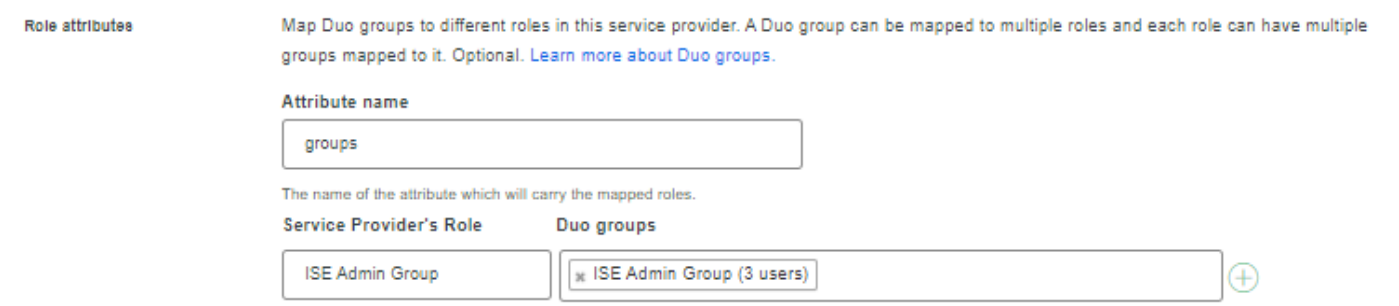


Create a group called Cisco Admin Group in the Duo Admin Panel and add the ISE users to this group or create a group in Windows AD and Sync the same to the Duo Admin panel using the directory Sync feature.

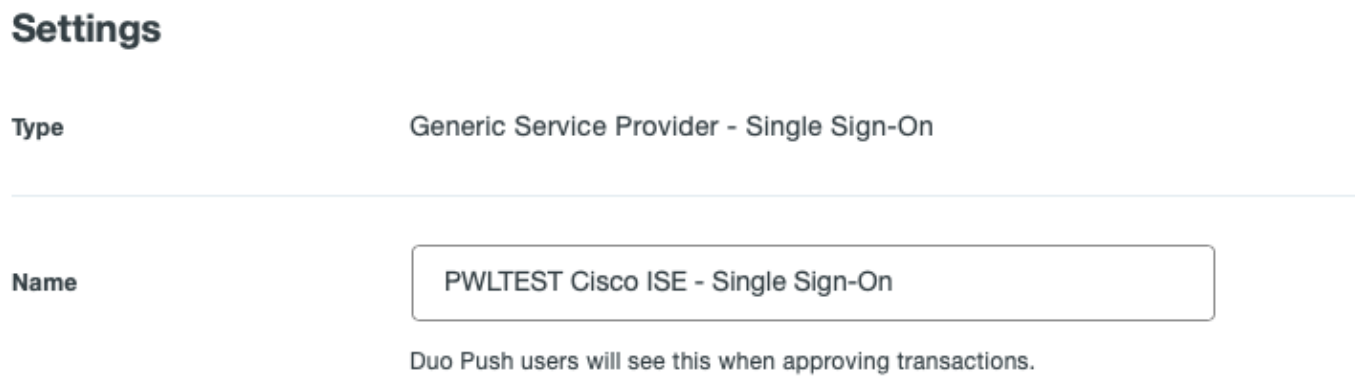


Configure Role attributes for Cisco ISE:

Name	Description
Attribute name	groups
SP Role	ISE Admin Group
Duo groups	ISE Admin Group

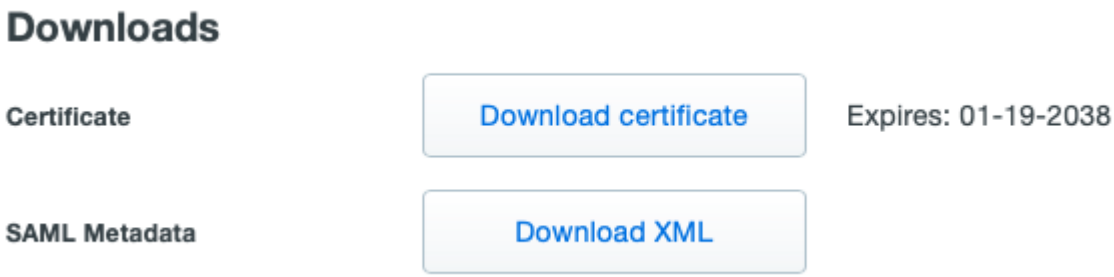


In the Settings section provide an appropriate name in the **Name** tab for this integration.



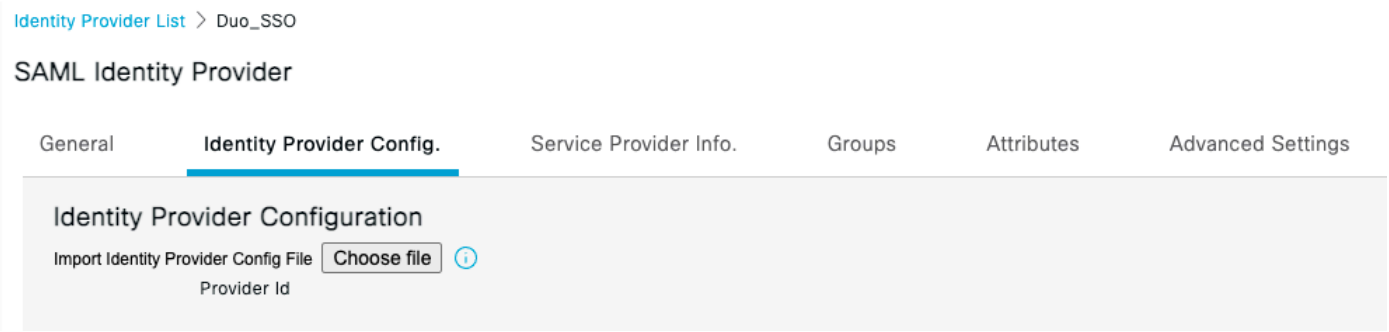
Click the **Save** button in order to save the configuration and refer to this KB for more details.

Click **Download XML** in order to download the SAML Metadata.



Upload SAML MetaData download from Duo Admin Panel to Cisco ISE by navigating to Administration > Identity Management > External Identity Sources > SAML Id Providers > Duo_SSO.
Switch the tab to **Identity Provider Config.** and click the **Choose** file button.
Choose the **Metadata XML** file downloaded in Step 8. and click **Save**.

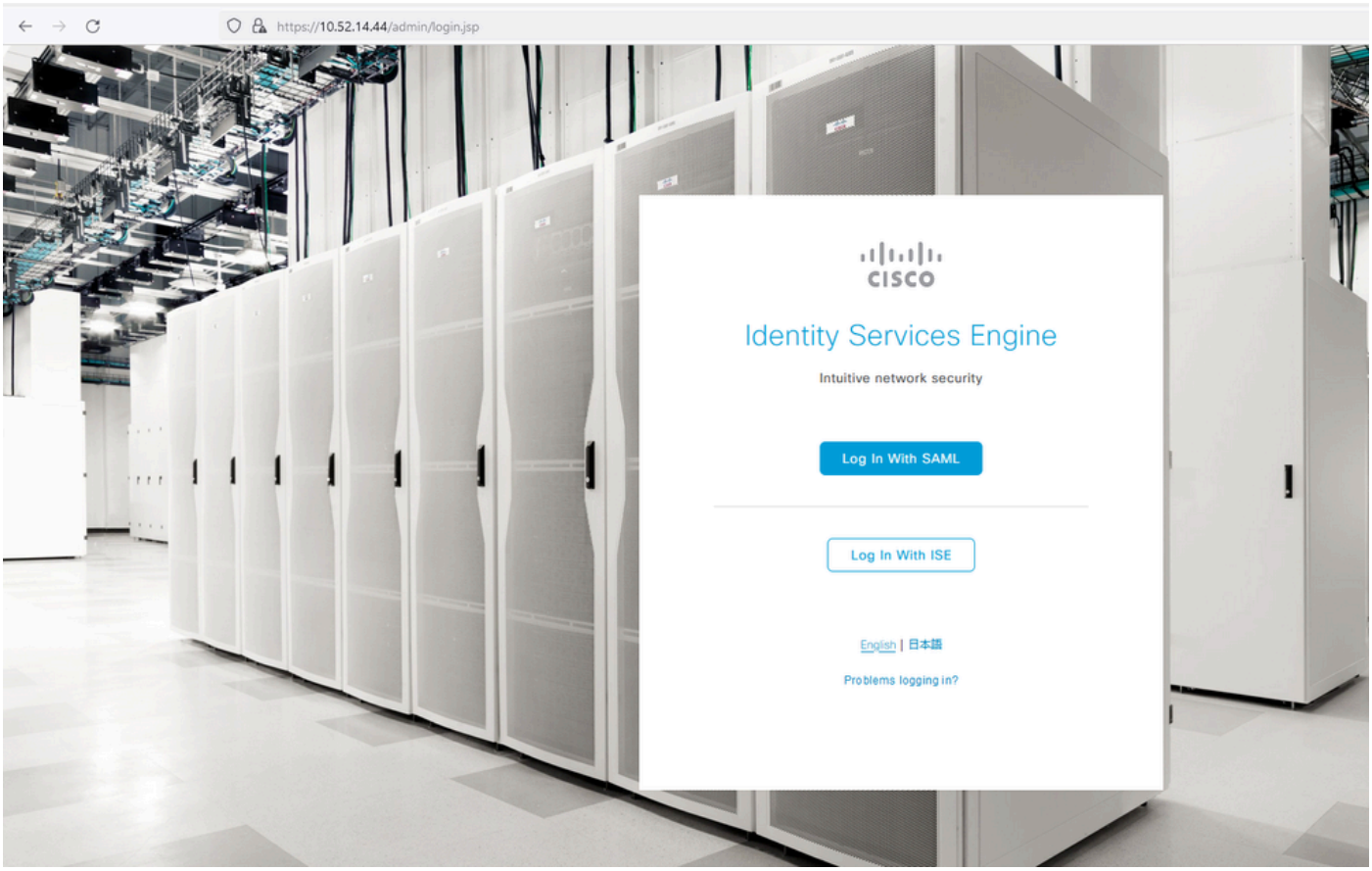
Note: This step is mentioned here under the section Configure SAML SSO Integration with Duo SSO; Step 2. Import the **SAML Metadata XML** file from the Duo Admin portal.



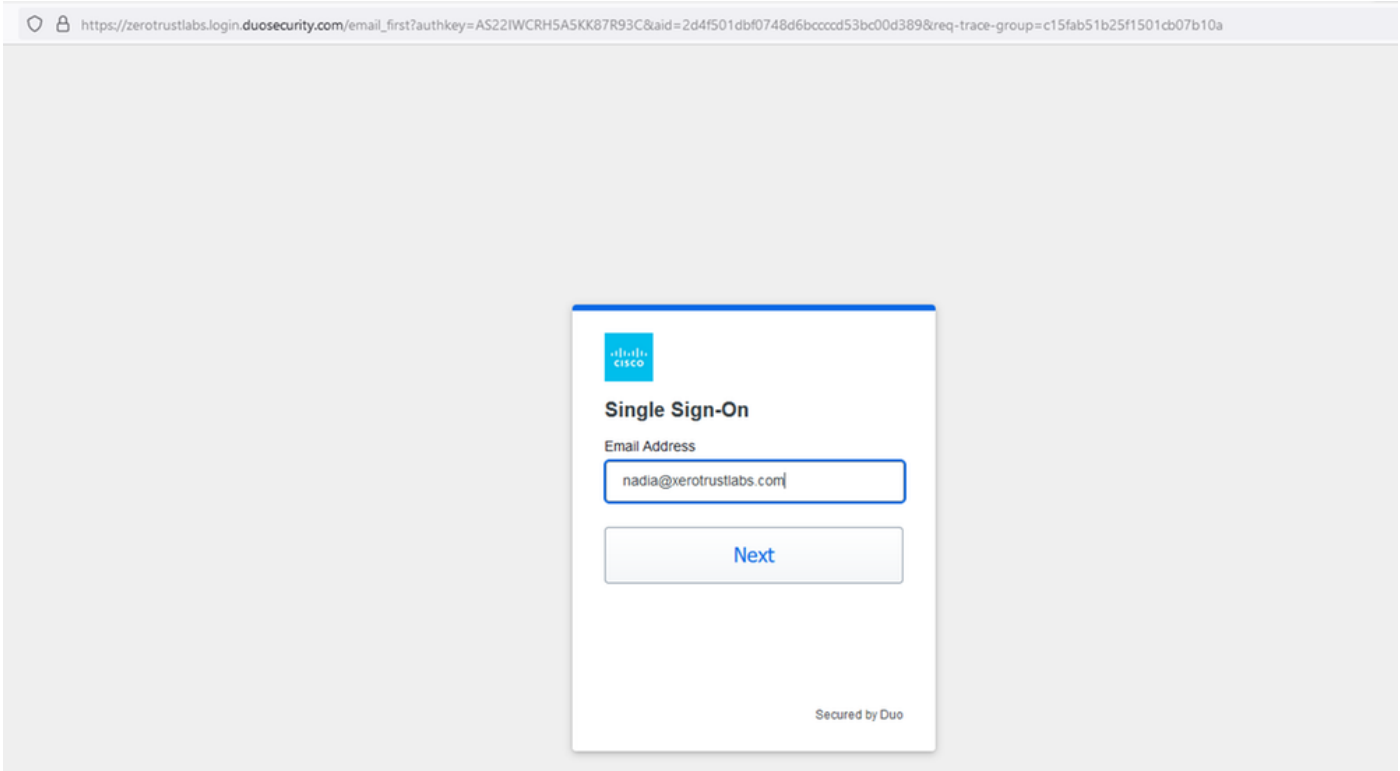
Verify

Testing the Integration with Duo SSO

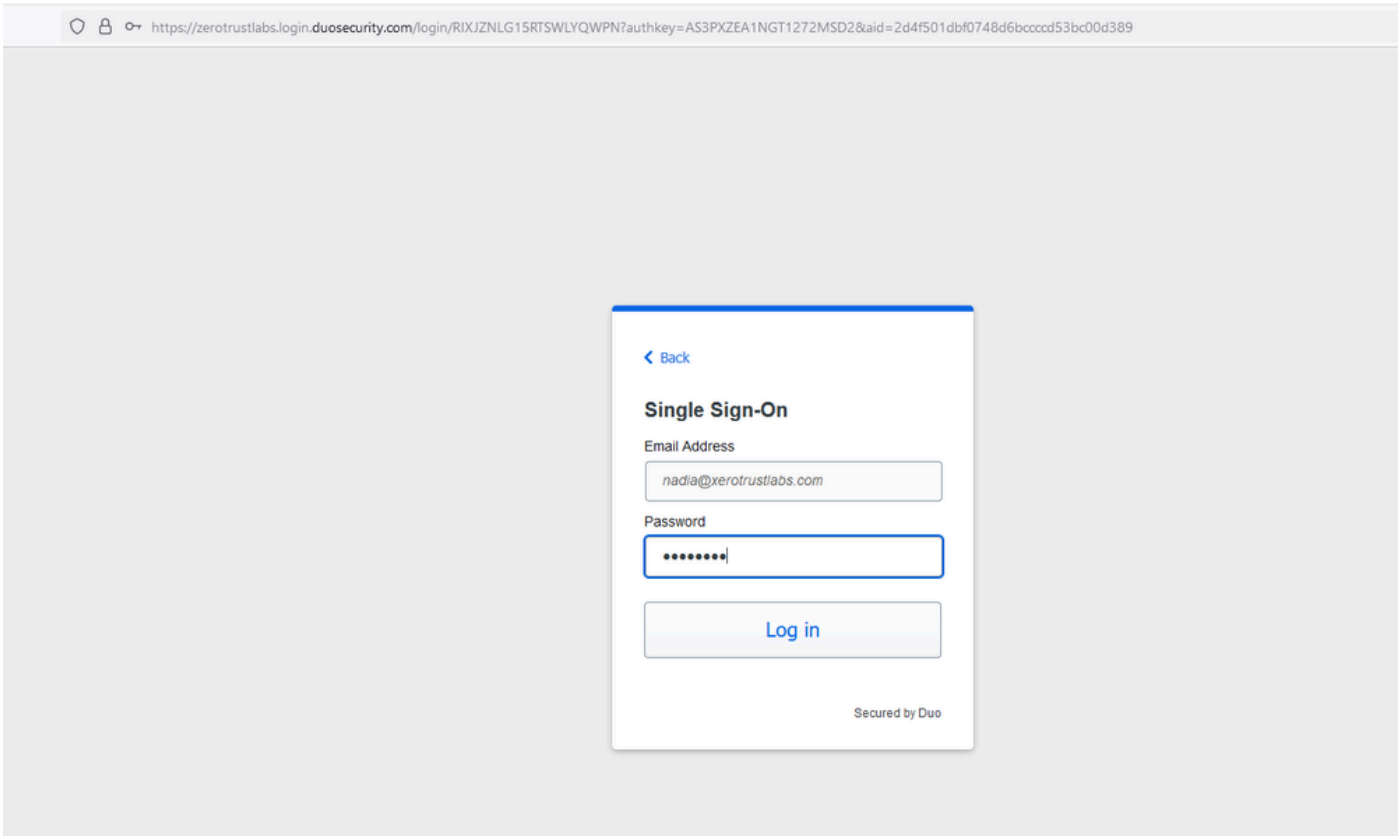
1. Login to the **Cisco ISE Admin Panel** and click **Log In With SAML**.



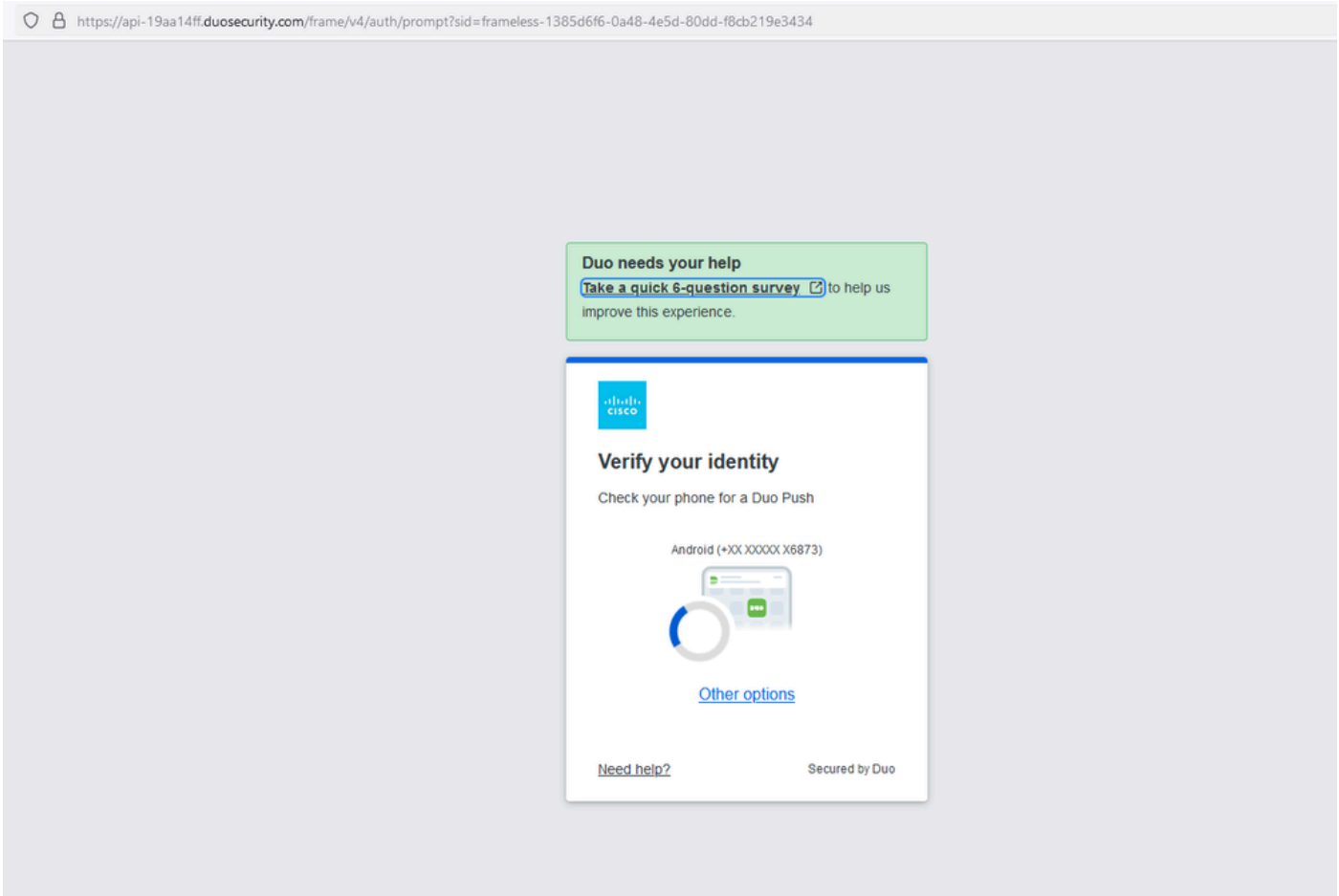
2. Redirected to the SSO page, enter the **Email Address** and click **Next**.



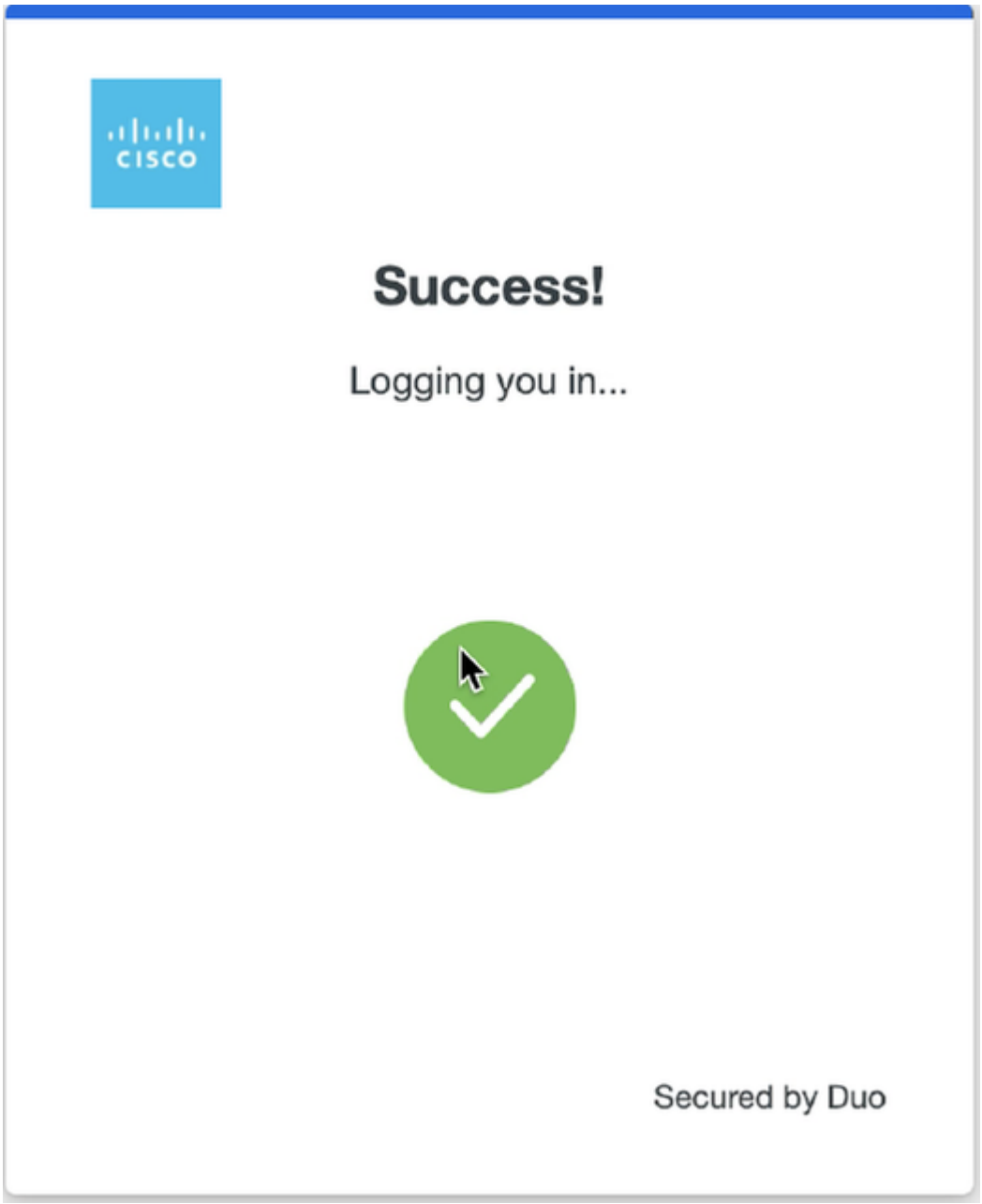
3. Enter the password and click **Log in**.



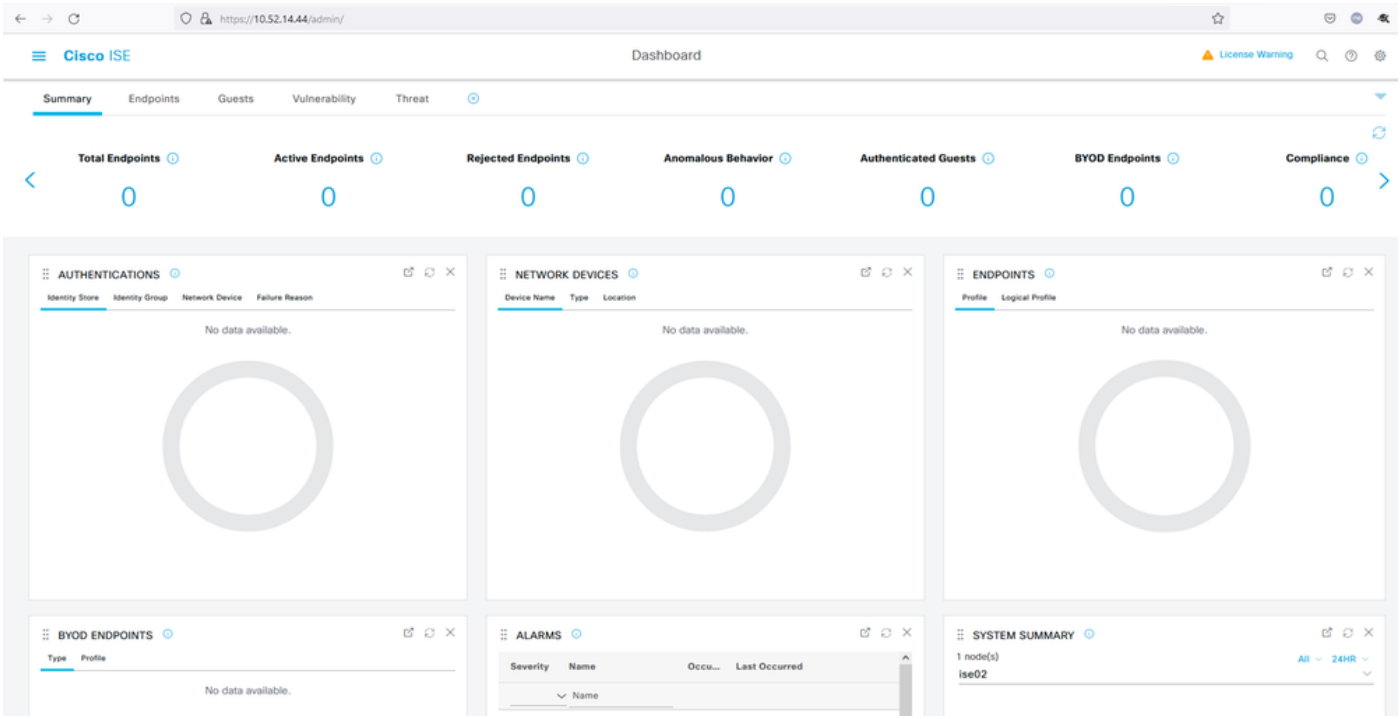
4. You get a Duo Push prompt on your mobile device.



5. Once you accept the prompt, you get a window and are automatically redirected to the ISE Admin page.

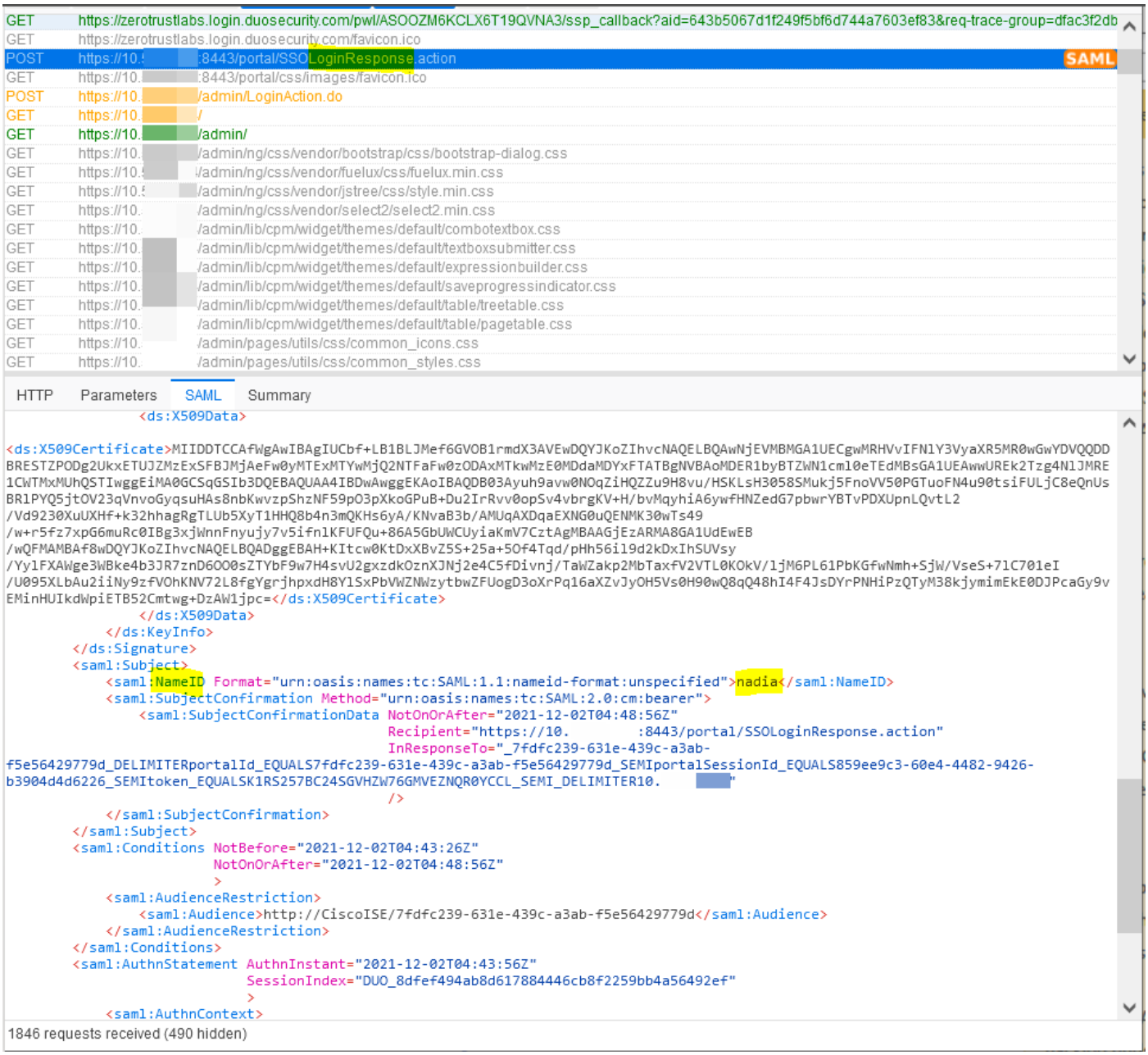


6. ISE Admin GUI Access Page.



Troubleshoot

- Download the SAML tracer extension for Mozilla FF https://addons.mozilla.org/en-US/firefox/addon/saml-tracer/.
- Scroll to the SSOLoginResponse.action packet. Under the **SAML** tab, you see a number of attributes sent from Duo SAML: NameID, Recipient (AssertionConsumerService Location URL), and Audience(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

- Administrative Login log on ISE: username: samlUser.

