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

Contents

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.

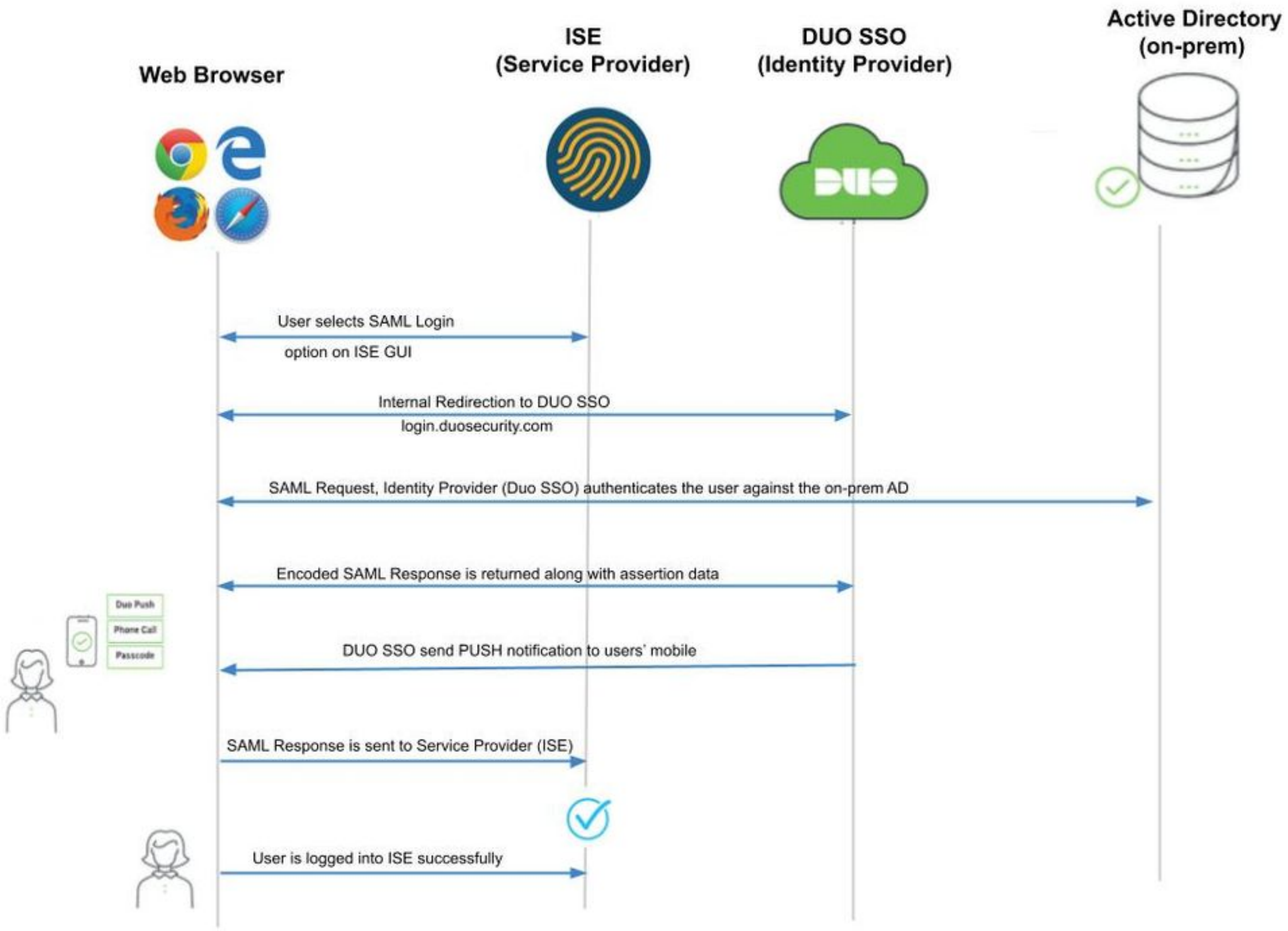
SAML Assertion

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


Web Browser
ISE
(Service Provider)
DUO SSO
(Identity Provider)
Active Directory
(on-prem)
DUO
User selects SAML Login
option on ISE GUI
Internal Redirection to DUO SSO
login.duosecurity.com
SAML Request, Identity Provider (Duo SSO) authenticates the user against the on-prem AD
Encoded SAML Response is returned along with assertion data
Duo Push
Phone Call
Passcode
DUO SSO send PUSH notification to users' mobile
SAML Response is sent to Service Provider (ISE)
User is logged into ISE successfully

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.

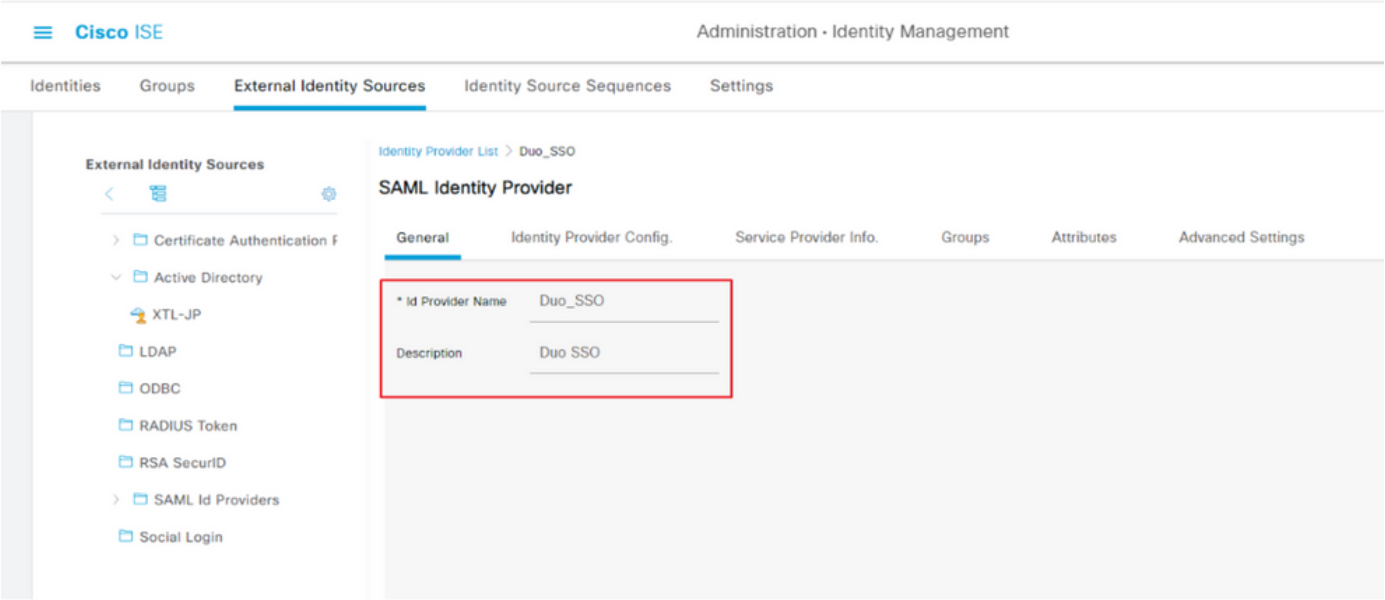
Configure SAML SSO Integration with Duo SSO

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:


Cisco ISE
Administration · Identity Management
Identities
Groups
External Identity Sources
Identity Source Sequences
Settings
External Identity Sources
Certificate Authentication F
Active Directory
XTL-JP
LDAP
ODBC
RADIUS Token
RSA SecurID
SAML Id Providers
Social Login
Identity Provider List > Duo_SSO
General
Identity Provider Config.
Service Provider Info.
Groups
Attributes
Advanced Settings

SAML Identity Provider

* Id Provider Name: Duo_SSO

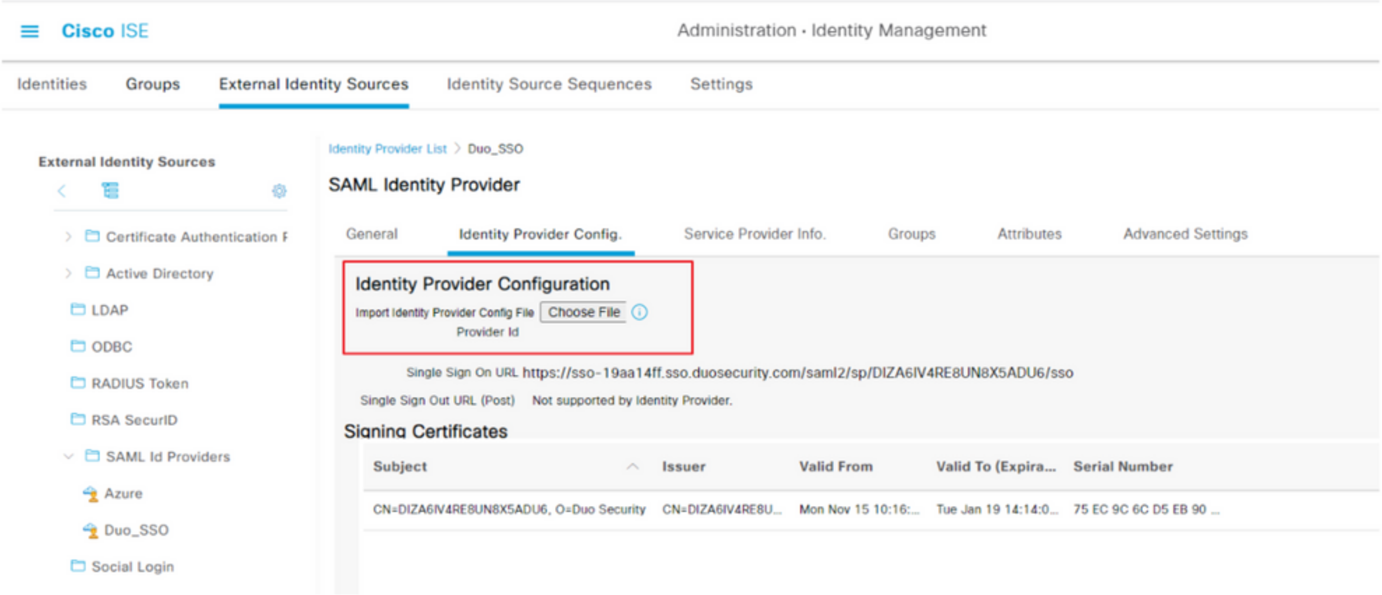
Description: Duo SSO

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:



Identity Provider Configuration

Import Identity Provider Config File

Provider Id

Single Sign On URL https://sso-19aa14ff.sso.duosecurity.com/saml2/sp/DIZA6IV4RE8UN8X5ADU6/sso

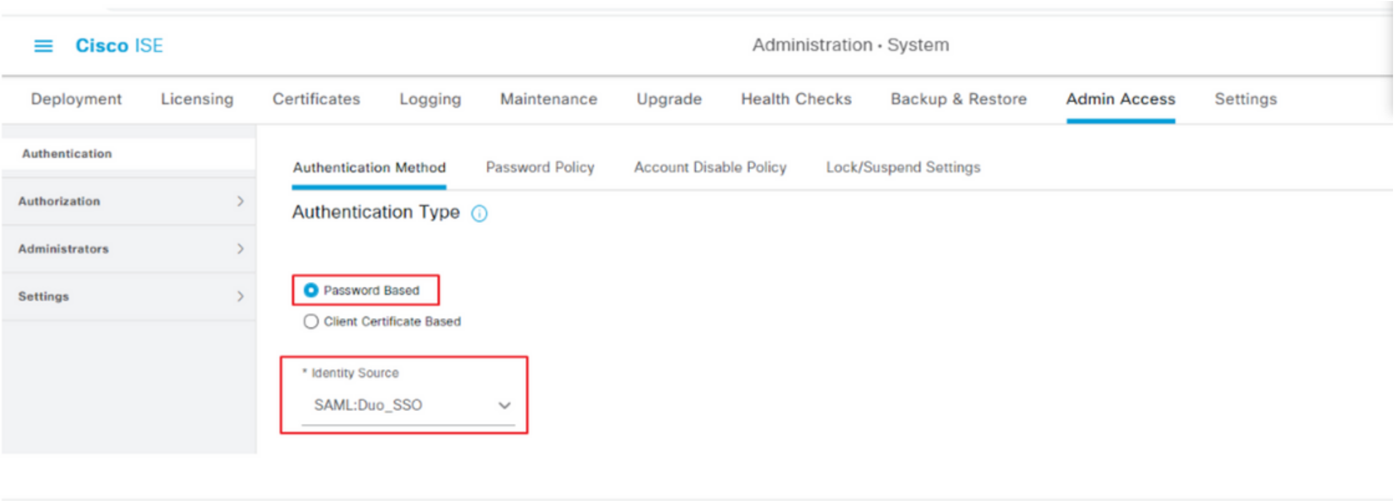
Single Sign Out URL (Post) Not supported by Identity Provider.

Signing Certificates

Subject	Issuer	Valid From	Valid To (Expira...	Serial Number
CN=DIZA6IV4RE8UN8X5ADU6, O=Duo Security	CN=DIZA6IV4RE8U...	Mon Nov 15 10:16:...	Tue Jan 19 14:14:0...	75 EC 9C 6C D5 EB 90 ...

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:



Authentication Type

● Password Based

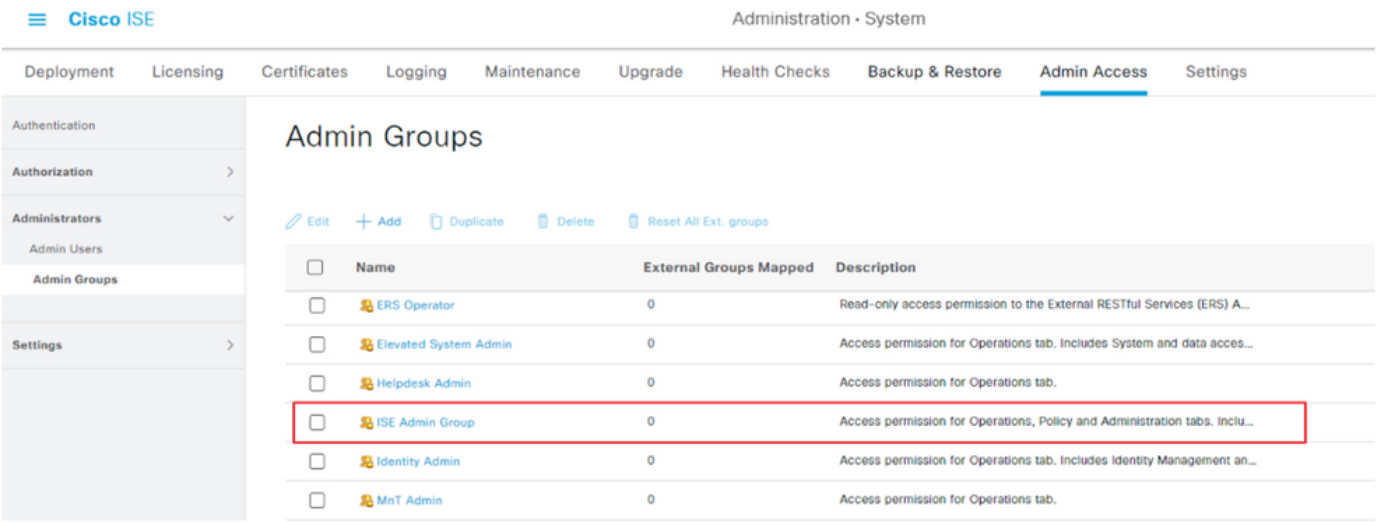
○ Client Certificate Based

* Identity Source: SAML:Duo_SSO

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.



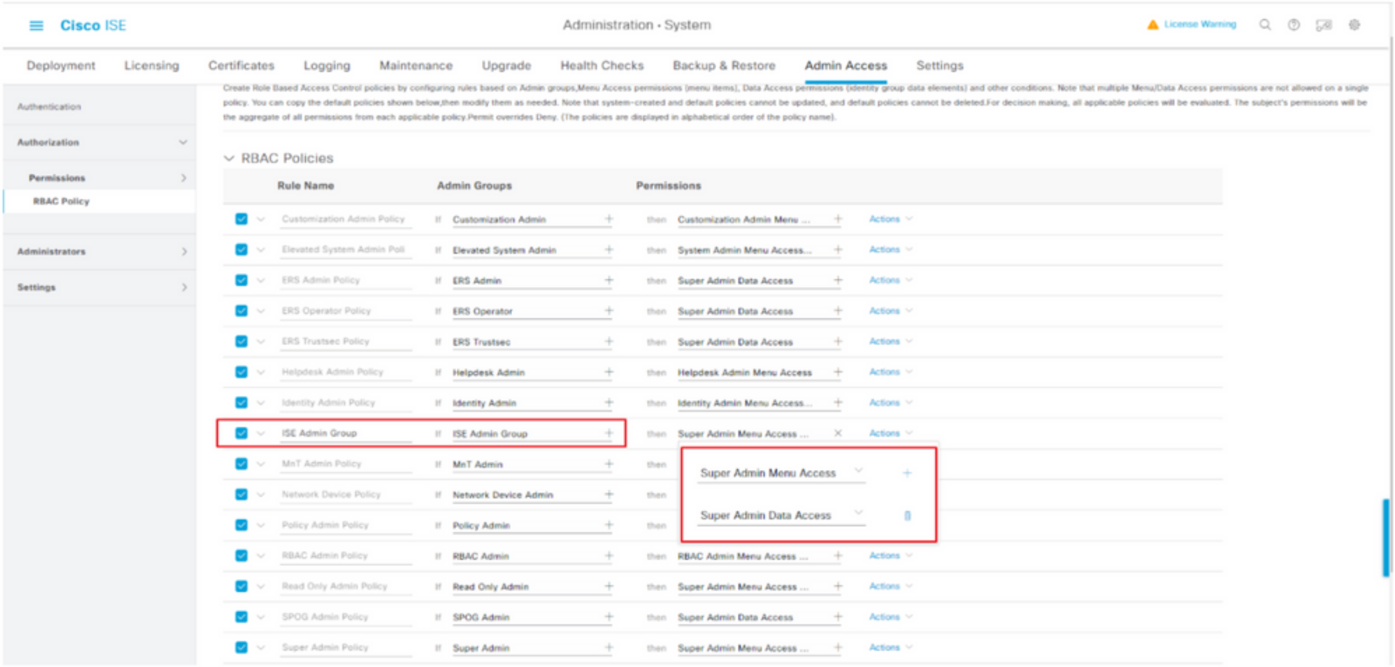
Admin Groups

□	Name	External Groups Mapped	Description
□	ERS Operator	0	Read-only access permission to the External RESTful Services (ERS) A...
□	Elevated System Admin	0	Access permission for Operations tab. Includes System and data acces...
□	Helpdesk Admin	0	Access permission for Operations tab.
□	ISE Admin Group	0	Access permission for Operations, Policy and Administration tabs. Inclu...
□	Identity Admin	0	Access permission for Operations tab. Includes Identity Management an...
□	MnT Admin	0	Access permission for Operations tab.

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.



Create Role Based Access Control policies by configuring rules based on Admin groups,Menu Access permissions (menu items), Data Access permissions (identity group data elements) and other conditions. Note that multiple Menu/Data Access permissions are not allowed on a single policy. You can copy the default policies shown below,then modify them as needed. Note that system-created and default policies cannot be updated, and default policies cannot be deleted.For decision making, all applicable policies will be evaluated. The subject's permissions will be the aggregate of all permissions from each applicable policy.Permit overrides Deny. (The policies are displayed in alphabetical order of the policy name).

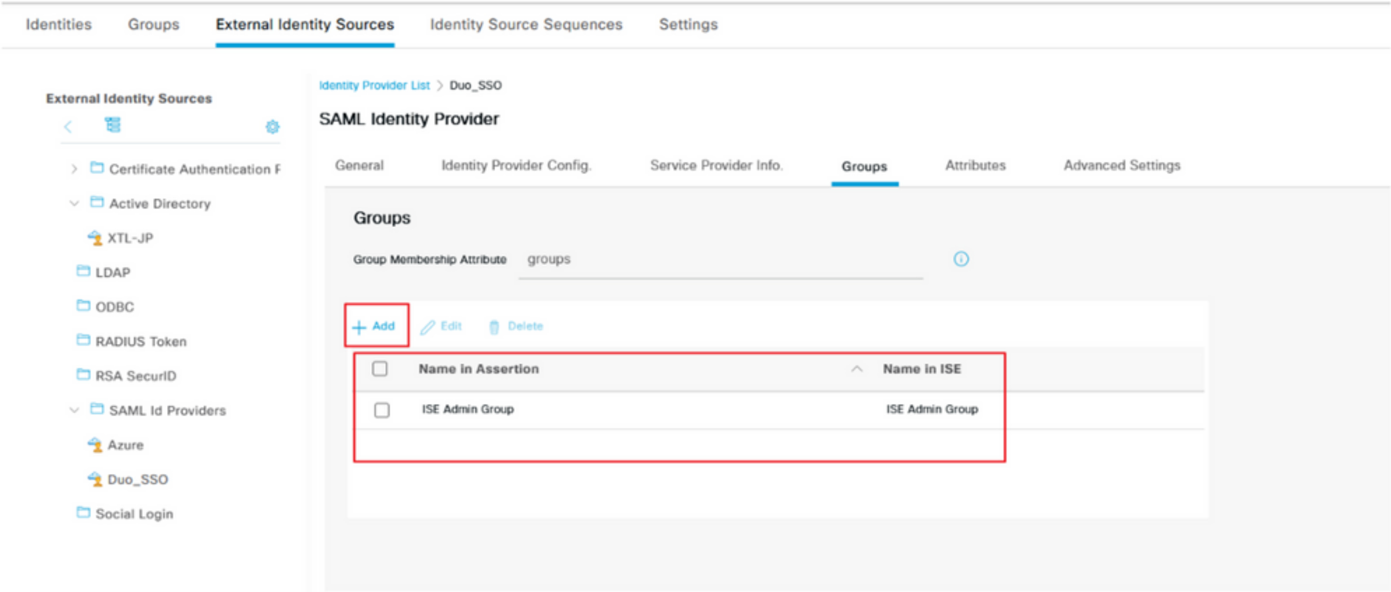
RBAC Policies

	Rule Name		Admin Groups		Permissions	
☑	Customization Admin Policy	If	Customization Admin	then	Customization Admin Menu ...	Actions
☑	Elevated System Admin Poli	If	Elevated System Admin	then	System Admin Menu Access...	Actions
☑	ERS Admin Policy	If	ERS Admin	then	Super Admin Data Access	Actions
☑	ERS Operator Policy	If	ERS Operator	then	Super Admin Data Access	Actions
☑	ERS Trustsec Policy	If	ERS Trustsec	then	Super Admin Data Access	Actions
☑	Helpdesk Admin Policy	If	Helpdesk Admin	then	Helpdesk Admin Menu Access	Actions
☑	Identity Admin Policy	If	Identity Admin	then	Identity Admin Menu Access...	Actions
☑	ISE Admin Group	If	ISE Admin Group	then	Super Admin Menu Access ... Super Admin Menu Access Super Admin Data Access	Actions
☑	MnT Admin Policy	If	MnT Admin	then		
☑	Network Device Policy	If	Network Device Admin	then		
☑	Policy Admin Policy	If	Policy Admin	then		
☑	RBAC Admin Policy	If	RBAC Admin	then	RBAC Admin Menu Access ...	Actions
☑	Read Only Admin Policy	If	Read Only Admin	then	Super Admin Menu Access ...	Actions
☑	SPOG Admin Policy	If	SPOG Admin	then	Super Admin Data Access	Actions
☑	Super Admin Policy	If	Super Admin	then	Super Admin Menu Access ...	Actions

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:



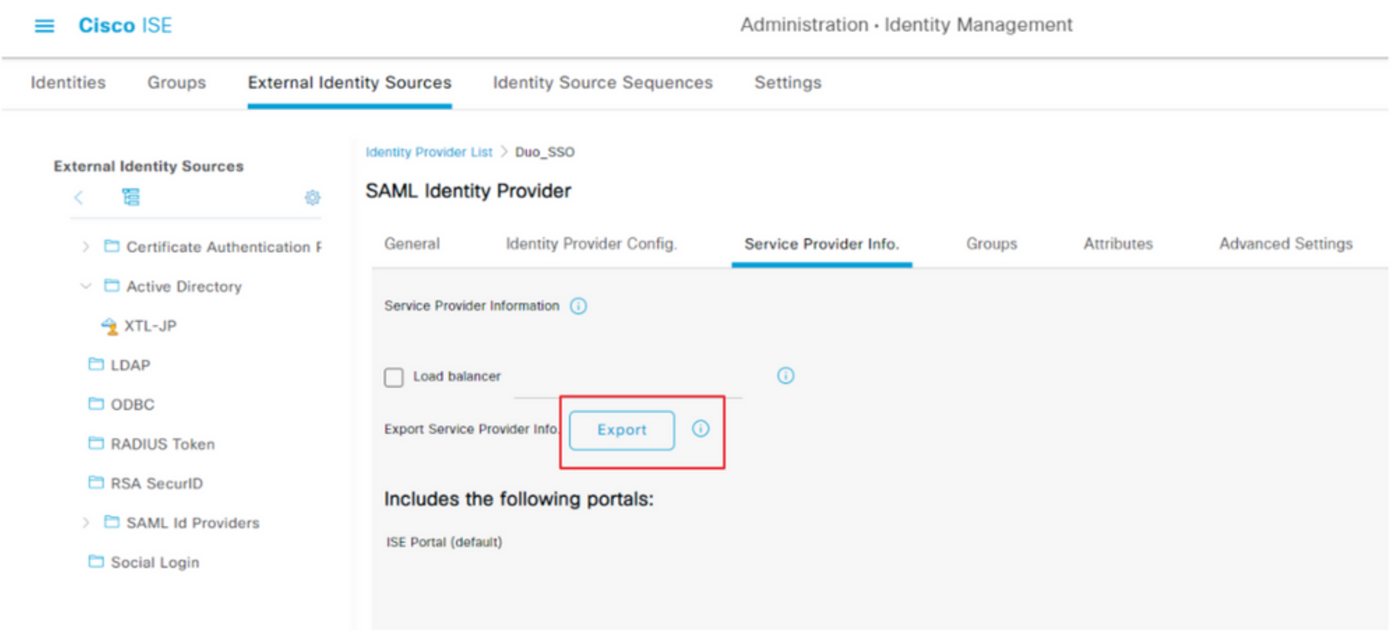
Group Membership Attribute: groups

□	Name in Assertion	Name in ISE
□	ISE Admin Group	ISE Admin Group

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:


Cisco ISE
Administration · Identity Management
Identities
Groups
External Identity Sources
Identity Source Sequences
Settings
External Identity Sources
Certificate Authentication P
Active Directory
XTL-JP
LDAP
ODBC
RADIUS Token
RSA SecurID
SAML Id Providers
Social Login
Identity Provider List > Duo_SSO
SAML Identity Provider
General
Identity Provider Config.
Service Provider Info.
Groups
Attributes
Advanced Settings
Service Provider Information
Load balancer
Export Service Provider Info.
Export
Includes the following portals:
ISE Portal (default)

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+1yhj8PwrDlpzfgXZLi3wlo5sMRGrg8NeSbShPJVakIEF2FoI0hXTOOSH4ZN
sD4q99dzrAv2m6y74vtU0GqwX4RRMOdvr7DIMNd2U/trh41QT85SY5c7Ol6fRWtY9omZBdU0S2JC
ihWnC9ug7FE0qdPm2h5KiZvxJck9OqVXDHvtRKctW5gwzfX8Hu7DQKqs90h04HRUxg2GEiuiXCQZ
5p63KfoRly5oW50UKOLIMdyhDl+8uP+n+Jo3ufR8lKe42+/rws5Ct1hg4jozddutKkw2vyxMEg5/
ZpAz/goRIOmBN4r3n3FNGZV1uTfbb1Mz8yvY61ccGgTU1/Iynt9maNHxjbFtAP+HaiMPisfTKDRJ
OLx91v+xKpb+opcOxqVK1q0Us0yGVvfycaFNZ3jP5wBNBzSAi7cvXk7sIW9WM7DC84OjC/r9EbaX
Wll7MLV+16Z+FeDnzhzFVjq/cb61eNvXKKwDFryFqBnDLLJGmJuZQ/EgR0wkvseR8tNE3qIYVh0e
qfCKZUpWtZ+lGLDD3r50p9UCAwEAAaN/MH0wIgYDVR0RBBswGYIXaXNlMDIueGVyb3RydXN0bGFi
cy5jb20wDAYDVR0TBAUwAwEB/zALBgNVHQ8EBAMCAuwwHQYDVR0OBBYEFAoHeqyYR5r0XpOVXODT
WdpDycOoMB0GA1UdJQQWMBQGCCsGAQUFBwMBBggrBgEFBQcDAjANBgkqhkiG9w0BAQwFAAOCAgEA
aoIIkyS8slDwjQrRsUVyPi17Lvl0TleCUQBrnr5WNUWlaXIB7Cb9qrG9D2ced72miH6vUcxine78
V4loTsgVu3tVlslQrOLW2eNLSbaN1XqbVUl1sCZkA4wGt8uLPX0t8UYysecEPFXD0NiKGPoIMaFg
3pP5525cJpeLRkgHjw1Z2qT54lsGd8Gdq6V666kliAt73kPwfDiZf/uDsCI+euIHDywLdOad51kJ
RWAsZO7tgxK3tJO9z7JU4oY1fI26DUN43++Ap3KSaDiz9gYJ3fFjR9hP/nF/ywyOOHO5MgHqhsMo
+zBMADukmprYC8qd+Oz76+NQ6TLXgUer7NQMty68tQYP4riupvc26CEmgEZ592jBgDdt2tkY9An4
Fl/rqJPhX2RISLdUt50NcBbIZVOJ/IjkqHj9UG1E/U8qYy3krWvZV+VV5ChVNzwiVTWFCEOHNOTh
l/yYdAAsODUBbwTqgJL1G3hNo+dA3LAgg/XKENFr+tt3LQ0kwPAtjKFQsIX/4sgMetV4KSqUI3HZ
qw5u0t9WT578SZ5p1u/qj2cfx2wdqRVk5vSij6TxOpXIaCuY2L5YfeIMP/K49K+DecMBxCrKygNT
vGX0PkVG/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

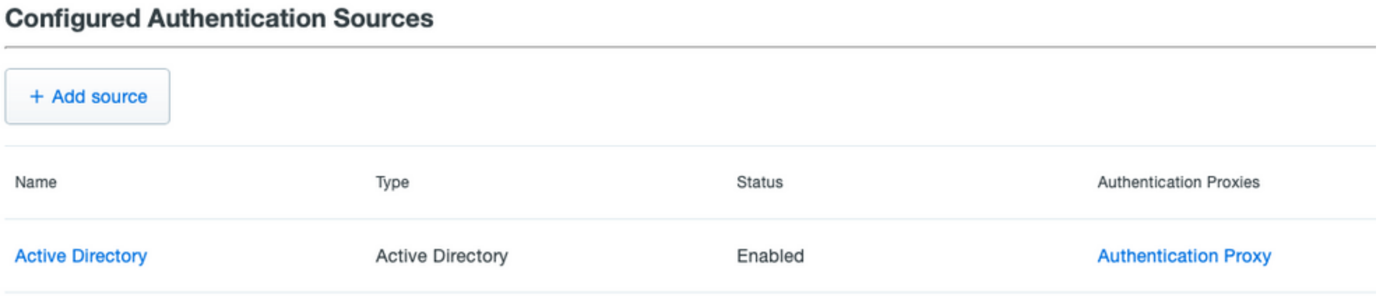
entityID = http://CiscoISE/7fdfc239-631e-439c-a3ab-f5e56429779d.

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

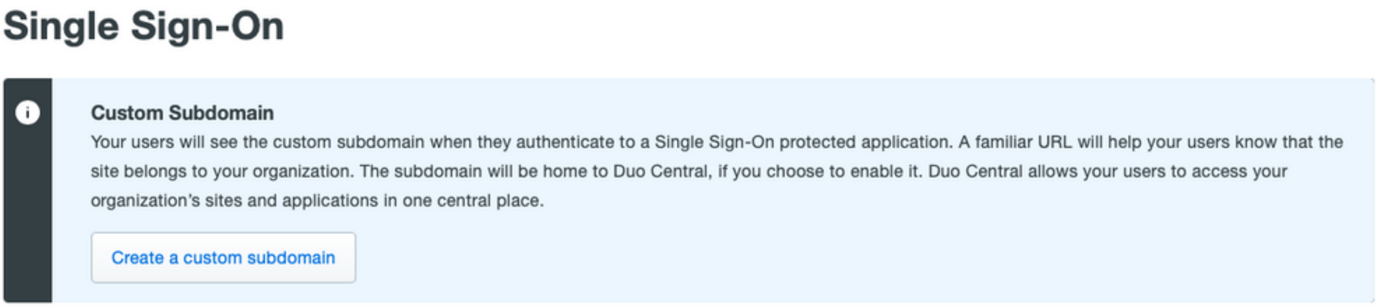
Check this KB in order to configure Duo SSO with AD as an Authentication Source.



Configured Authentication Sources

Name	Type	Status	Authentication Proxies
Active Directory	Active Directory	Enabled	Authentication Proxy

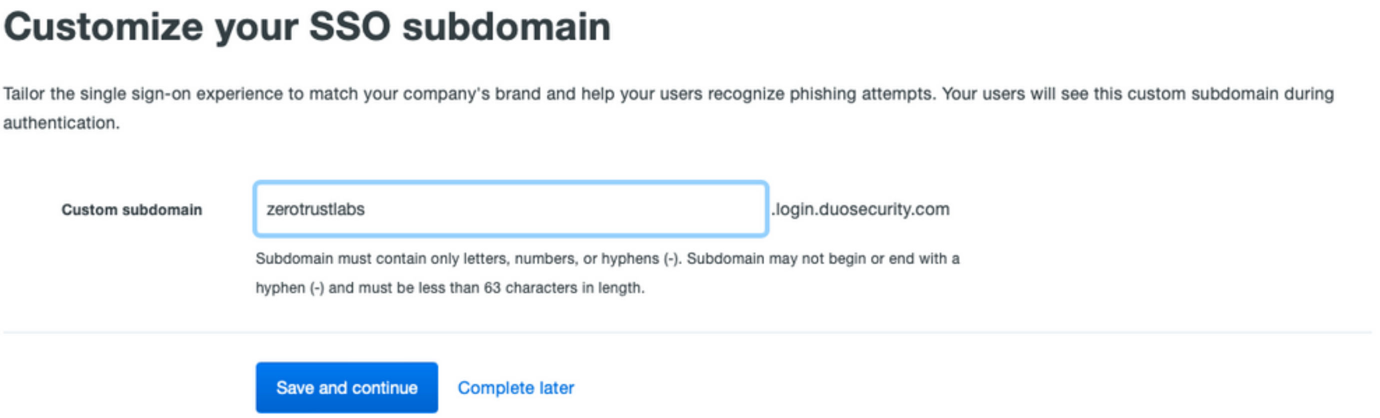
Check this KB in order to enable the SSO with your custom domain.



Single Sign-On

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.



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.

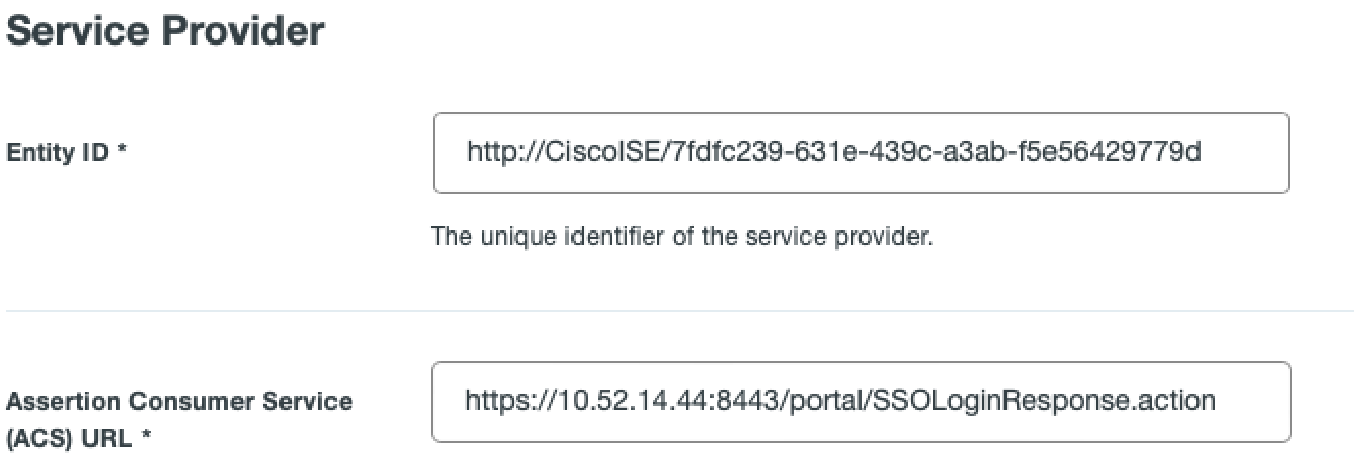
Step 3. Integrate Cisco ISE with Duo SSO as a Generic SP

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



Service Provider

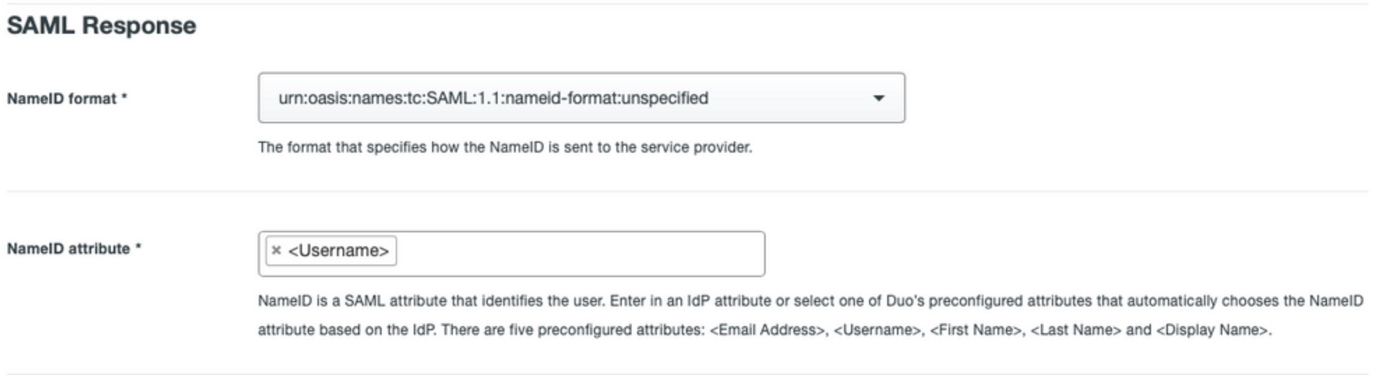
Entity ID * http://CiscoISE/7fdfc239-631e-439c-a3ab-f5e56429779d

The unique identifier of the service provider.

Assertion Consumer Service (ACS) URL * https://10.52.14.44:8443/portal/SSOLoginResponse.action

Configure SAML Response for Cisco ISE:

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



SAML Response

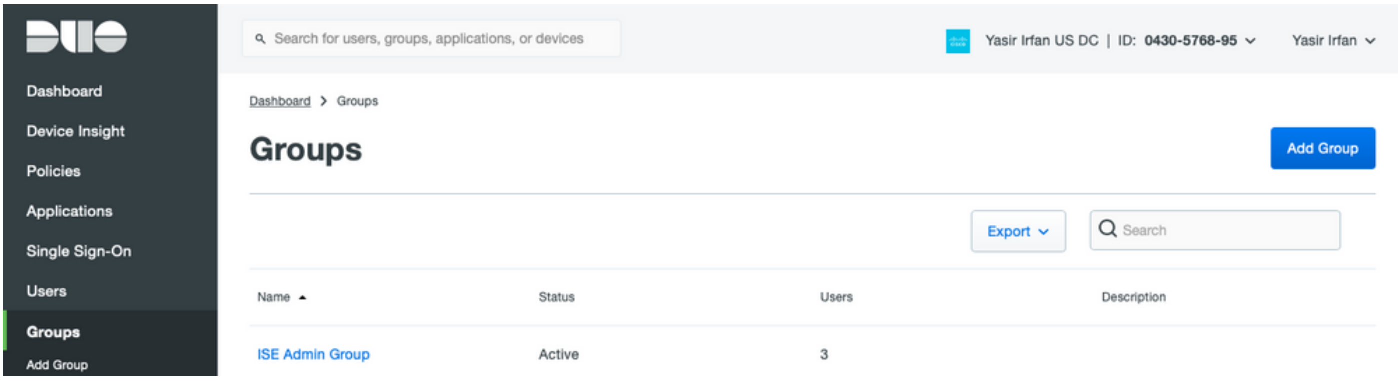
NameID format * urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified

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

NameID attribute * × <Username>

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>.

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.

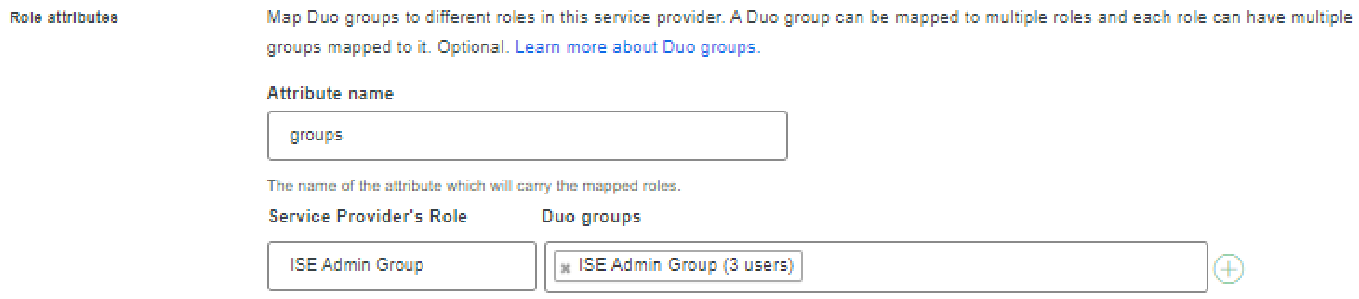


Groups

Name	Status	Users	Description
ISE Admin Group	Active	3	

Configure Role attributes for Cisco ISE:

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



Role attributes

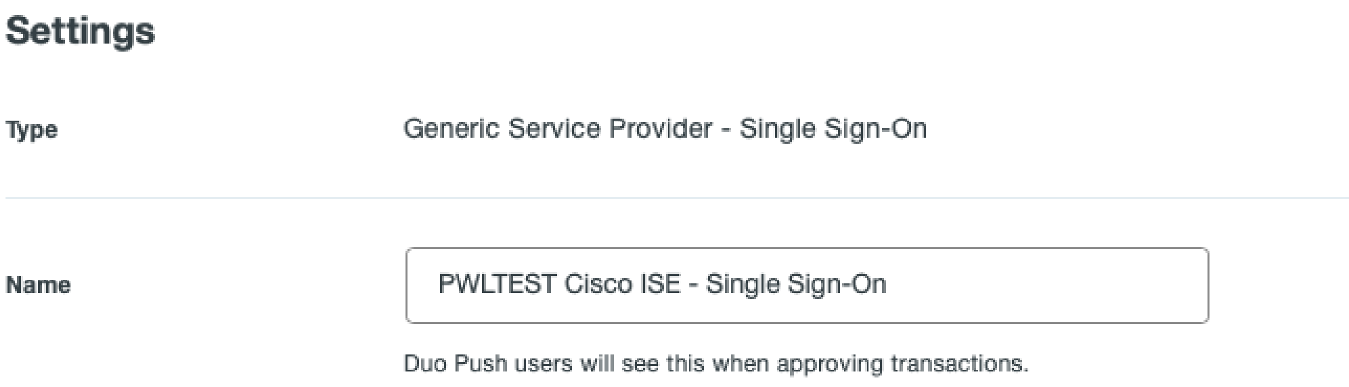
Map Duo groups to different roles in this service provider. A Duo group can be mapped to multiple roles and each role can have multiple groups mapped to it. Optional. Learn more about Duo groups.

Attribute name: groups

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

Service Provider's Role	Duo groups
ISE Admin Group	ISE Admin Group (3 users)

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



Settings

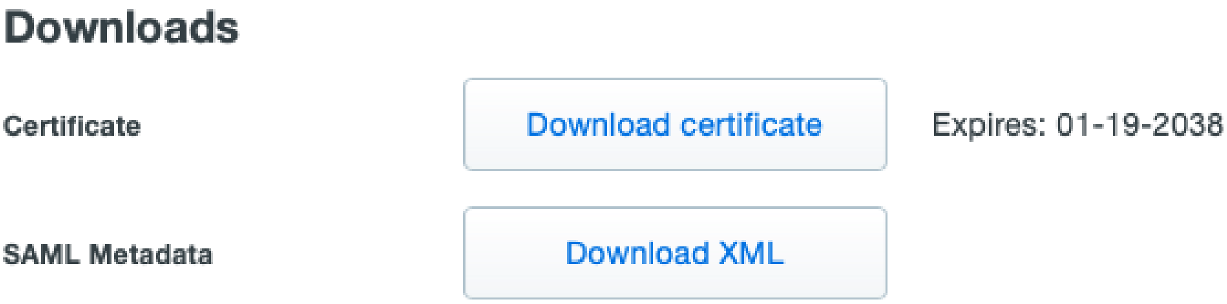
Type: Generic Service Provider - Single Sign-On

Name: PWLTEST Cisco ISE - Single Sign-On

Duo Push users will see this when approving transactions.

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.

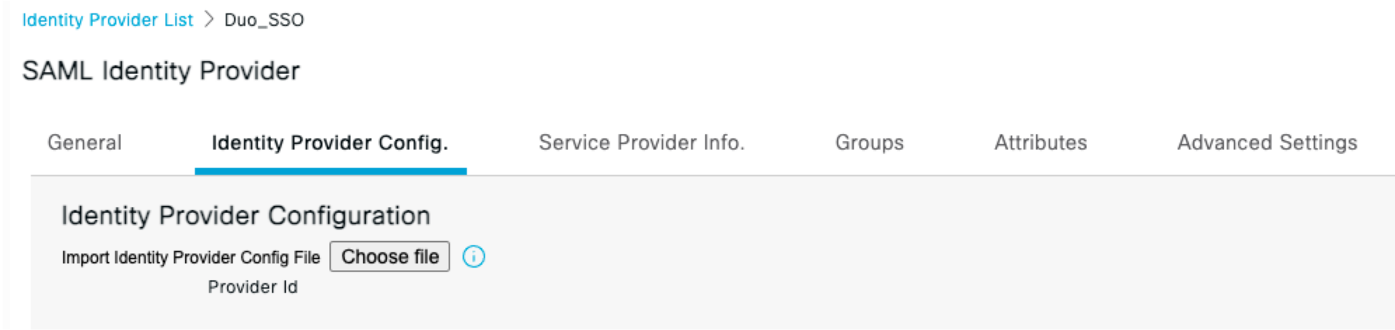


Downloads

Certificate	Download certificate	Expires: 01-19-2038
SAML Metadata	Download XML	

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.



Identity Provider List > Duo_SSO

SAML Identity Provider

Identity Provider Configuration

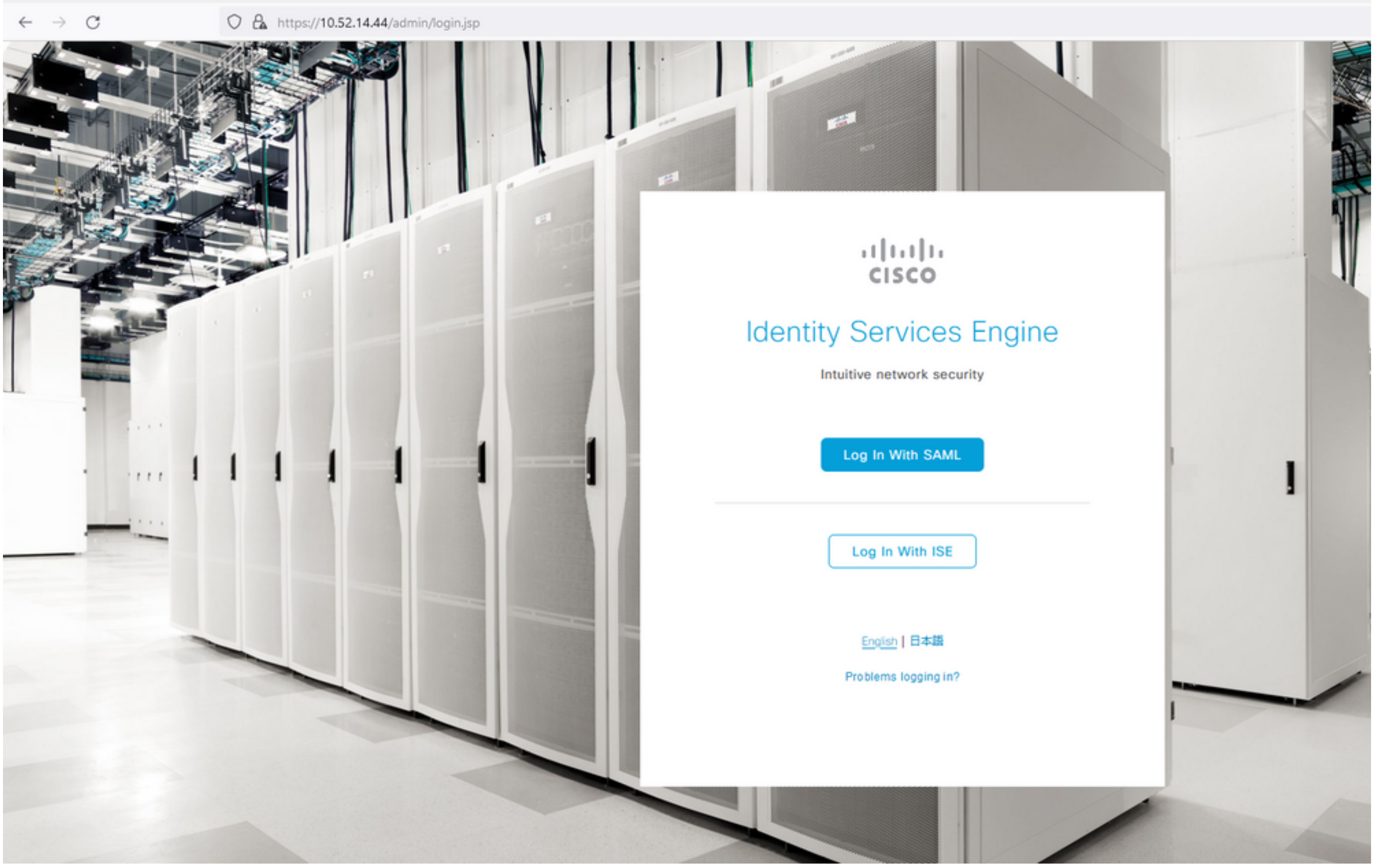
Import Identity Provider Config File Choose file

Provider Id

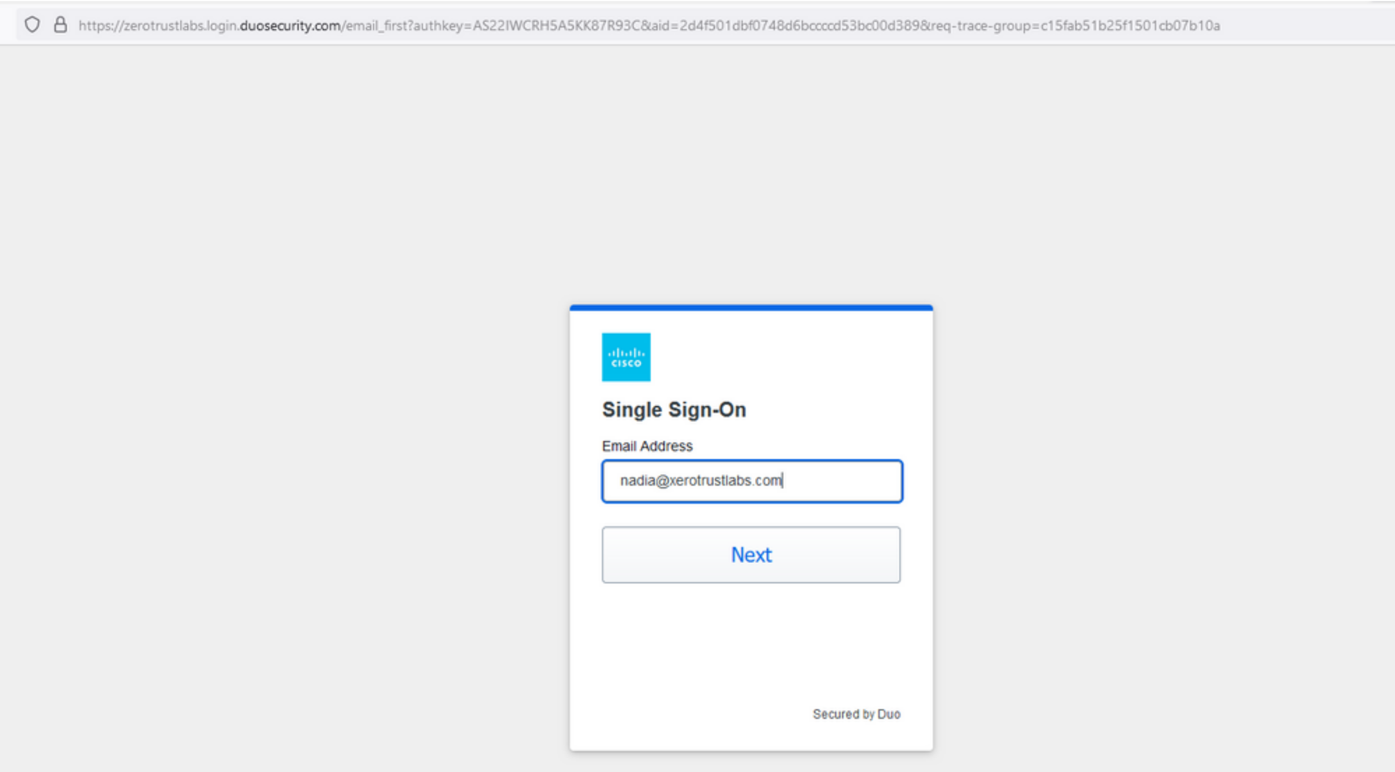
Verify

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**.



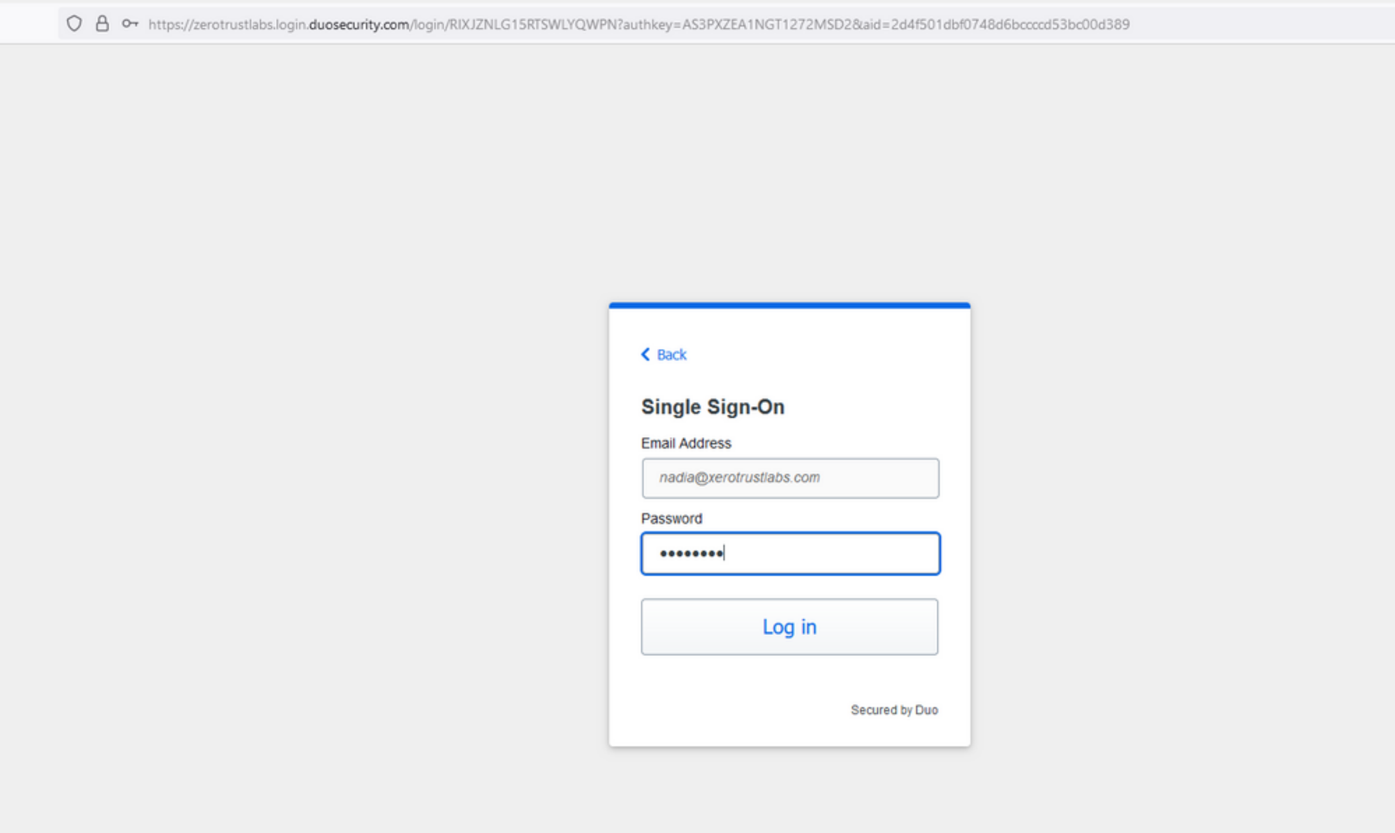
https://zerotrustlabs.login.duosecurity.com/email_first?authkey=AS22IWCRH5A5KK87R93C&aid=2d4f501dbf0748d6bccccd53bc00d389&req-trace-group=c15fab51b25f1501cb07b10a

Single Sign-On

Email Address

nadia@xerotrustlabs.com

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



https://zerotrustlabs.login.duosecurity.com/login/RIXJZNLG15RTSWLYQWPN?authkey=AS3PXZEA1NGT1272MSD2&aid=2d4f501dbf0748d6bccccd53bc00d389

Single Sign-On

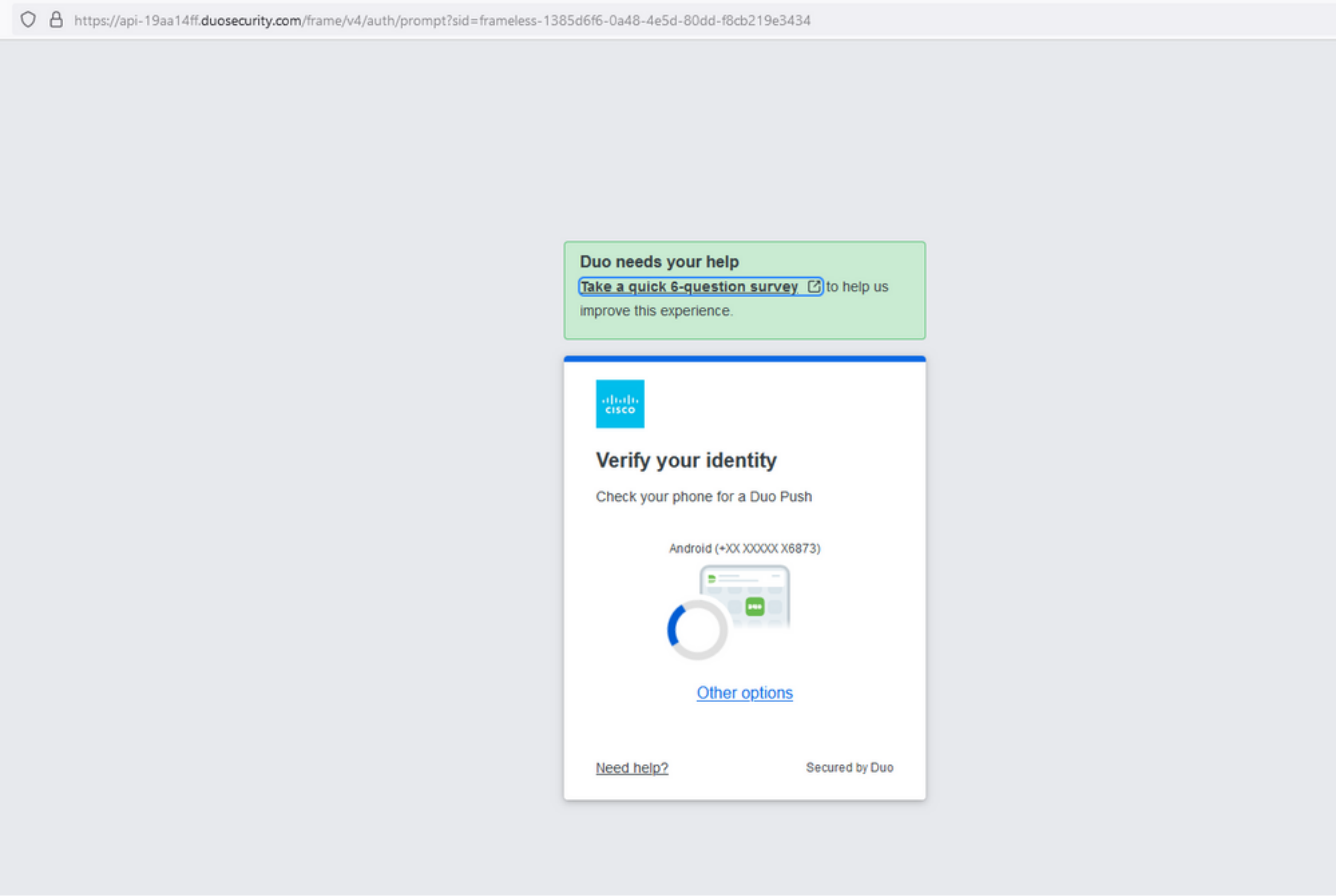
Email Address

nadia@xerotrustlabs.com

Password

••••••••

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



https://api-19aa14ff.duosecurity.com/frame/v4/auth/prompt?sid=frameless-1385d6f6-0a48-4e5d-80dd-f8cb219e3434

Duo needs your help

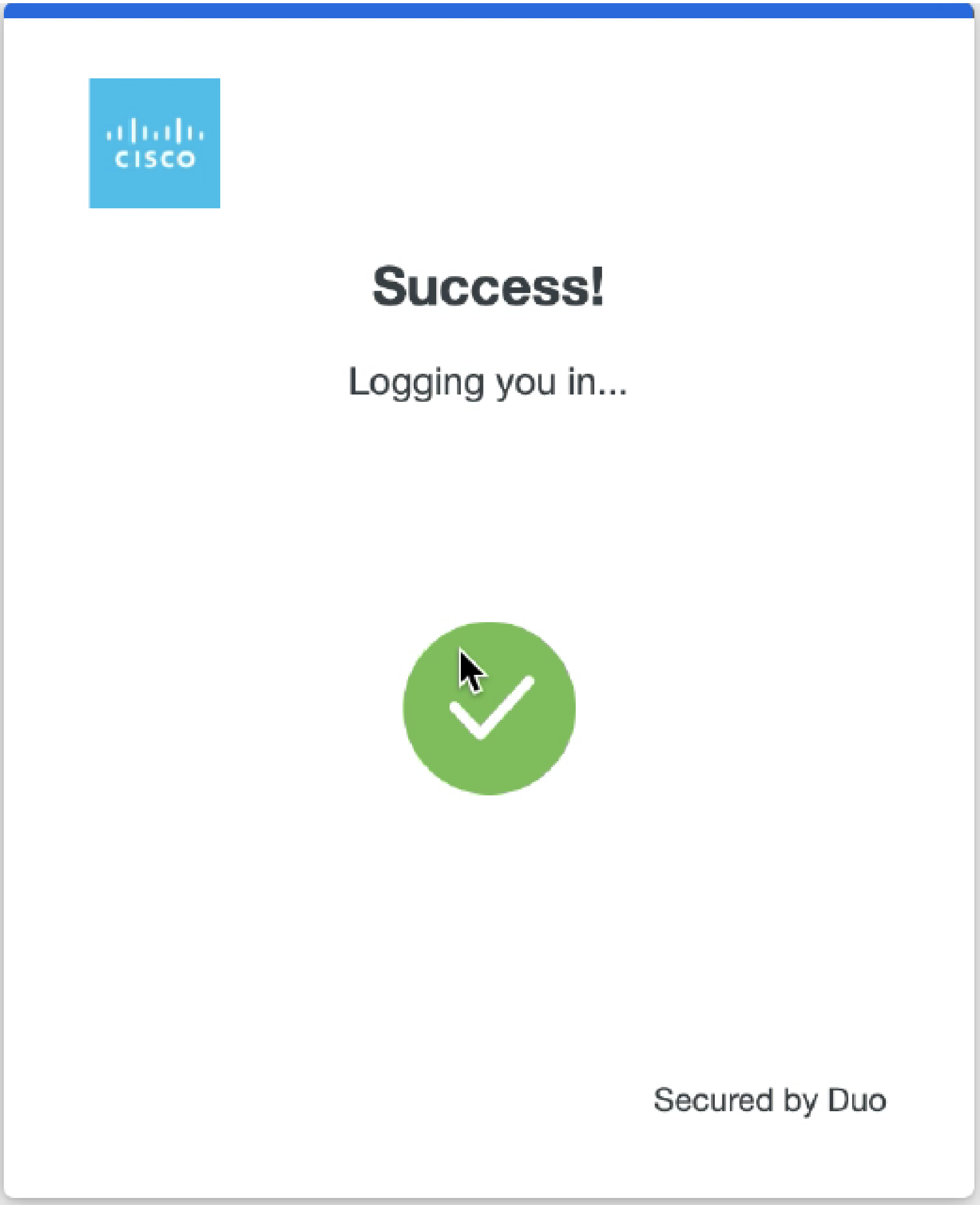
Take a quick 6-question survey to help us improve this experience.

Verify your identity

Check your phone for a Duo Push

Android (+XX XXXXX X6873)

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

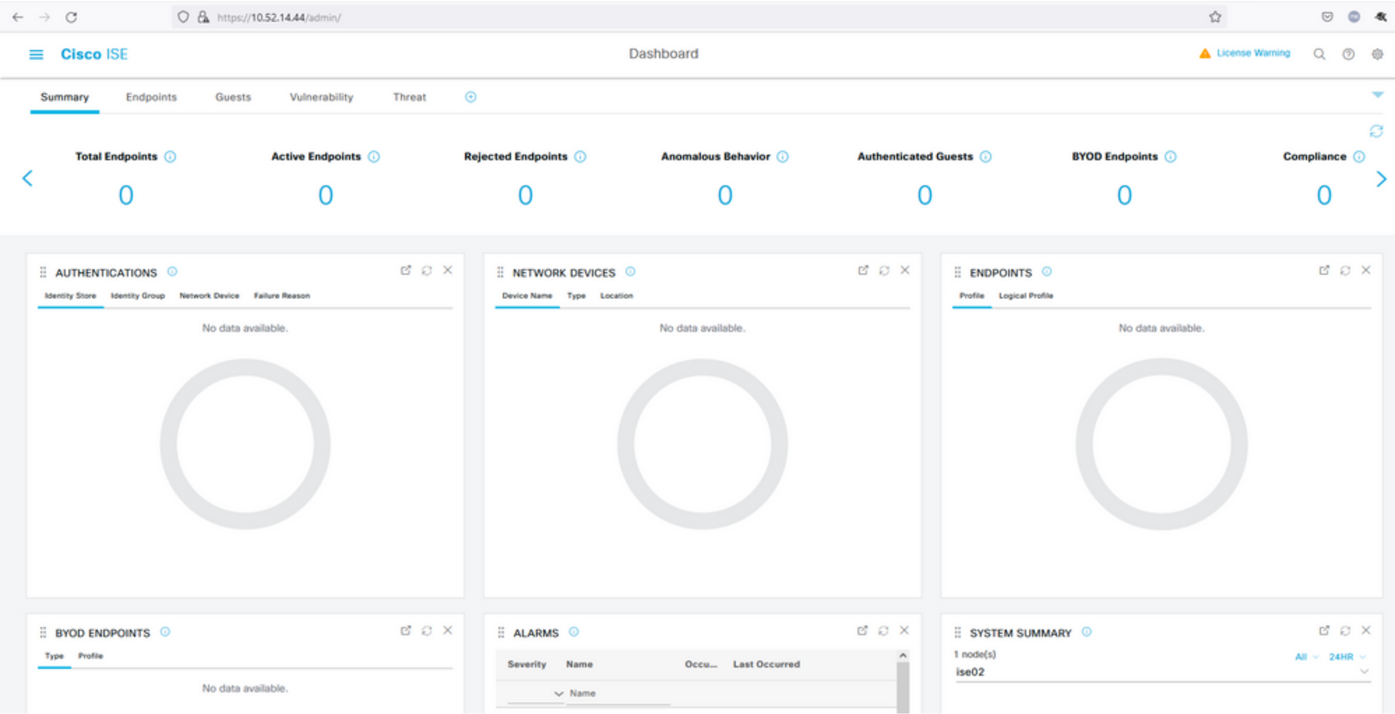


Success!

Logging you in...

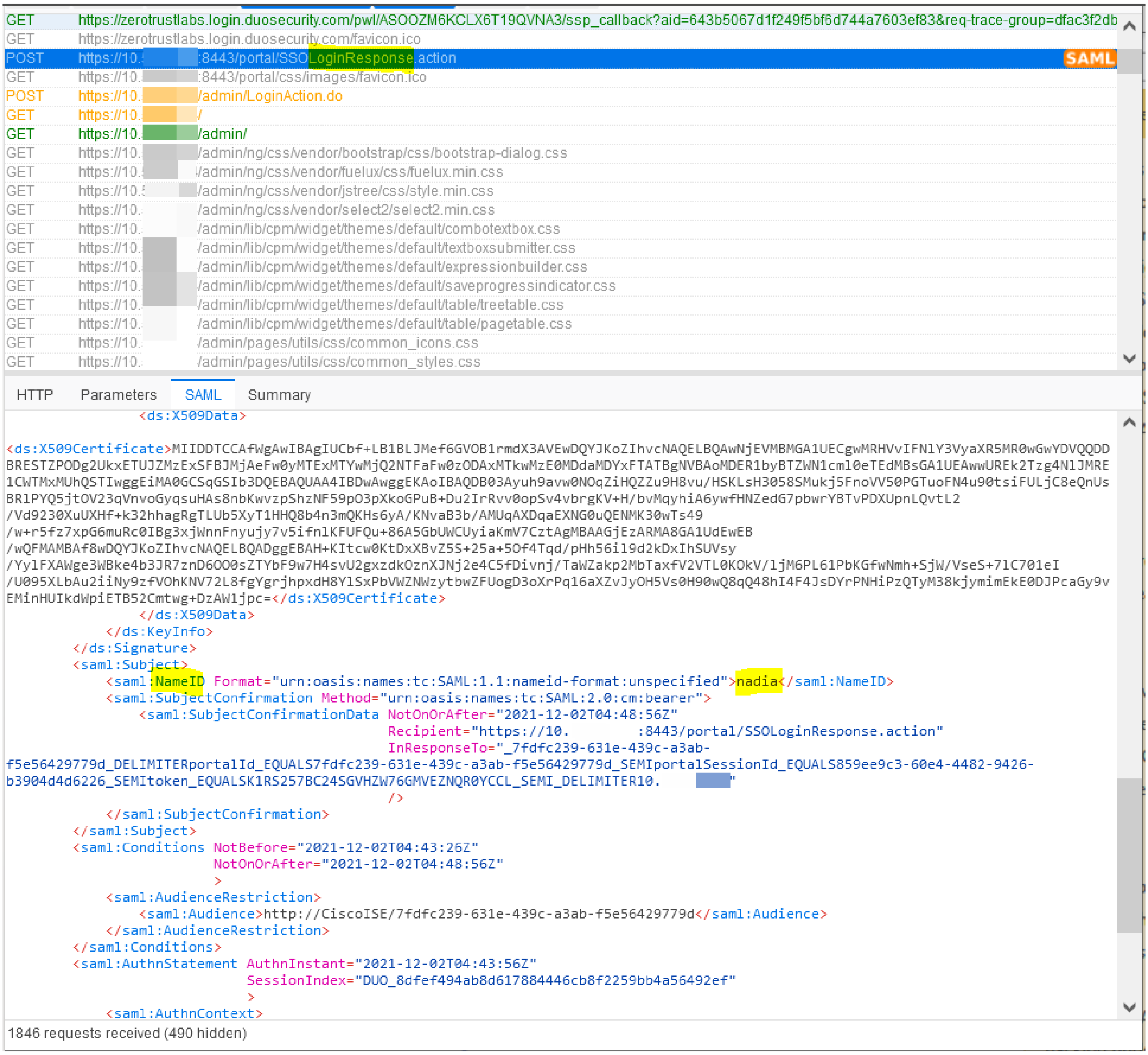
Secured by Duo

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).



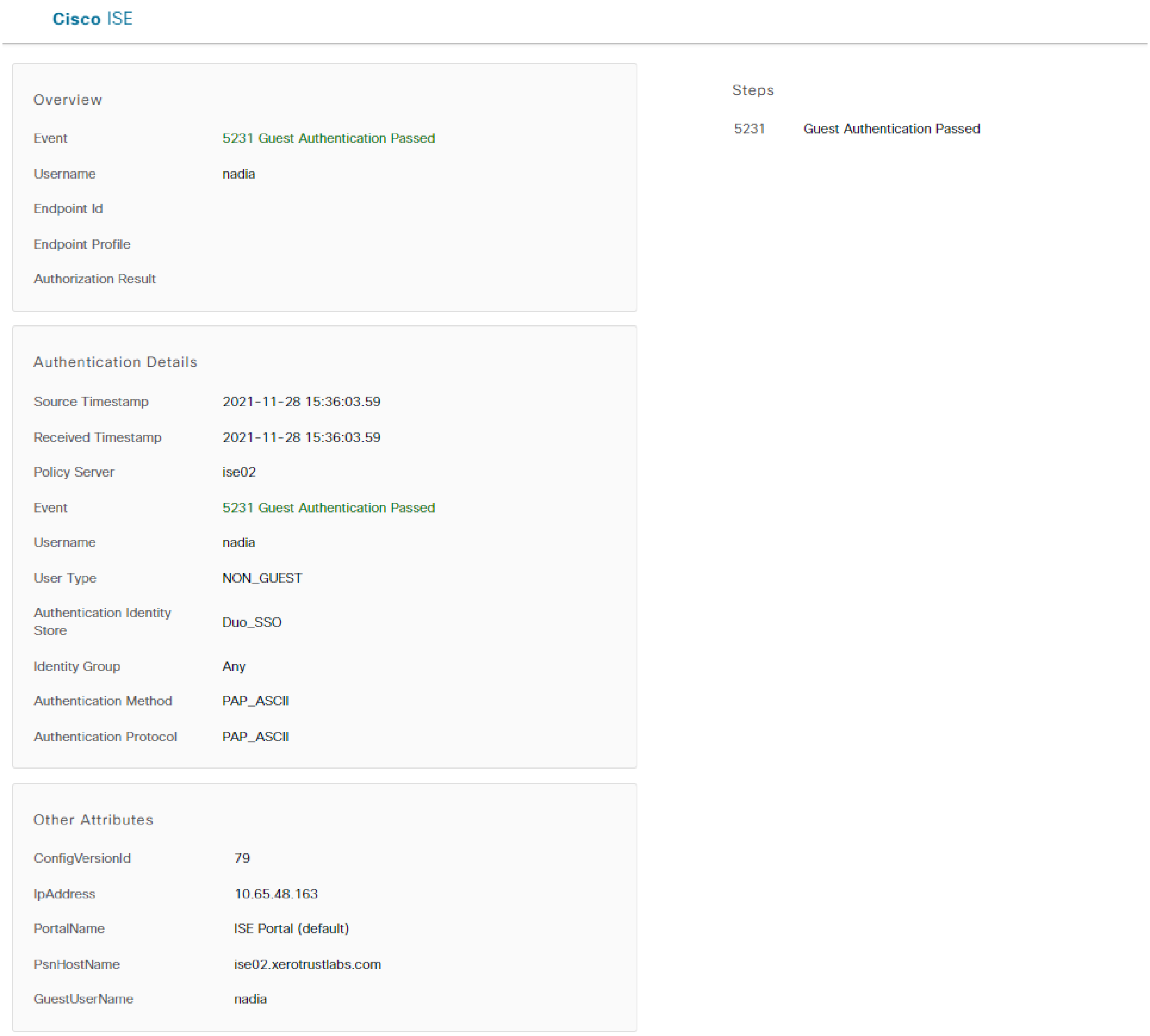
```
GET   https://zerotrustlabs.login.duosecurity.com/pwl/ASOOZM6KCLX6T19QVNA3/ssp_callback?aid=643b5067d1f249f5bf6d744a7603ef83&req-trace-group=dfac3f2db
GET   https://zerotrustlabs.login.duosecurity.com/favicon.ico
POST  https://10.[redacted]:8443/portal/SSOLoginResponse.action                                                    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
```

```
                <ds:X509Data>

<ds:X509Certificate>MIIDDTCCAfWgAwIBAgIUCbf+LB1BLJMef6GVOB1rmdX3AVEwDQYJKoZIhvcNAQELBQAwNjEVMBMGA1UECgwMRHVvIFN1Y3VyaXR5MR0wGwYDVQQDD
BRESTZPODg2UkxETUJZMzExSFBJMjAeFw0yMTExMTYwMjQ2NTFaFw0zODAxMTkwMzE0MDdaMDYxFTATBgNVBAoMDER1byBTZWN1cml0eTEdMBsGA1UEAwwUREk2Tzg4N1JMRE
1CWTMxMUhQSTIwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDB03Ayuh9avw0NOqZiHQZZu9H8vu/HSKLsH3058SMukj5FnoVV50PGTuoFN4u90tsiFULjC8eQnUs
BR1PYQ5jtOV23qVnvoGyqsuHAs8nbKwvzpShzNF59pO3pXkoGPuB+Du2IrRvv0opSv4vbrgKV+H/bvMqyhiA6ywfHNZedG7pbwrYBTvPDXUpnLQvtL2
/Vd9230XuUXHf+k32hhagRgTLUb5XyT1HHQ8b4n3mQKHs6yA/KNvaB3b/AMUqAXDqaEXNG0uQENMK30wTs49
/w+r5fz7xpG6muRc0IBg3xjWnnFnyujy7v5ifnlKFUFQu+86A5GbUWCUyiaKmV7CztAgMBAAGjEzARMA8GA1UdEwEB
/wQFMAMBAf8wDQYJKoZIhvcNAQELBQADggEBAH+KItcw0KtDxXBvZ5S+25a+5Of4Tqd/pHh56il9d2kDxIhSUVsy
/Yy1FXAWge3WBke4b3JR7znD6OO0sZTYbF9w7H4svU2gxzdkOznXJNj2e4C5fDivnj/TaWZakp2MbTaxfV2VTL0KOkV/ljM6PL61PbKGfwNmh+SjW/VseS+71C701eI
/U095XLbAu2iiNy9zfVOhKNV72L8fgYgrjhpxdH8Y1SxPbVWZNWzytbwZFUogD3oXrPq16aXZvJyOH5Vs0H90wQ8qQ48hI4F4JsDYrPNHiPzQTyM38kjymimEkE0DJPcaGy9v
EMinHUIkdWpiETB52Cmtwg+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.[redacted]: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.[redacted]"
                                              />
            </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)

- Live Log on ISE:



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

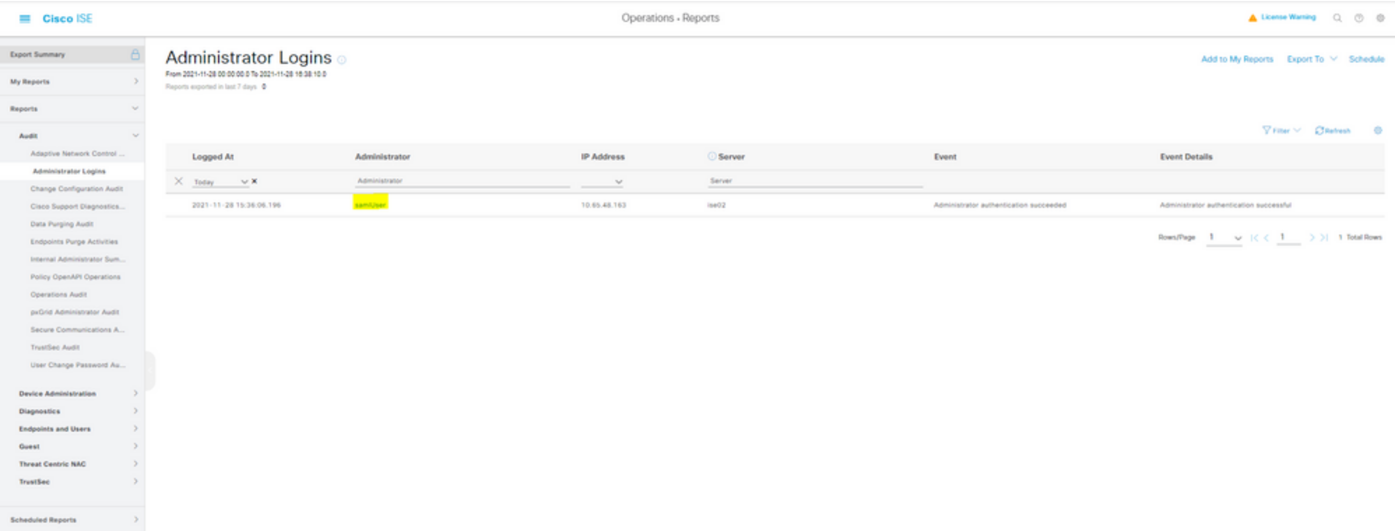
Other Attributes

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

Steps

5231	Guest Authentication Passed

- Administrative Login log on ISE: username: samlUser.



Administrator Logins

From 2021-11-28 00:00:00.0 To 2021-11-28 16:38:10.0

Reports exported in last 7 days 0

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