Configuración del inicio de sesión de administrador de GUI de ISE 3.1 mediante la integración de SAML con Duo SSO y Windows AD

Contenido

Introducción

Este documento describe cómo configurar la integración de SSO SAML de Cisco ISE 3.1 con un proveedor de identidad externo como Cisco Duo SSO.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Cisco Identity Services Engine (ISE) 3.1
- Conocimientos básicos sobre implementaciones de Single Sign-On (SSO) mediante el lenguaje de marcado de aserción de seguridad (SAML) (SAML 1.1)
- Conocimientos de Cisco DUO SSO
- Conocimiento de Windows Active Directory

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

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

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

Proveedor de identidad (IdP)

En este caso, es el SSO doble el que verifica y afirma la identidad del usuario y los privilegios de acceso a un recurso solicitado (el "proveedor de servicios").

Duo SSO actúa como un IdP, autenticando a sus usuarios usando Active Directory (AD) existente en las instalaciones con SAML 1.1 o cualquier IdP de SAML 2.0 (por ejemplo, Microsoft Azure) y solicitando la autenticación de dos factores antes de permitir el acceso a su aplicación de proveedor de servicios.

Al configurar una aplicación para que esté protegida con Duo SSO, debe enviar atributos de Duo SSO a la aplicación. Active Directory funciona sin configuración adicional, pero si utilizó un IdP SAML(2.0) como origen de autenticación, verifique que lo configuró para enviar los atributos SAML correctos.

Proveedor de servicios (SP)

El recurso o servicio alojado al que el usuario pretende acceder; Cisco ISE Application Server en este caso.

SAML

SAML es un estándar abierto que permite el IdP para pasar las credenciales de autorización al

SP.

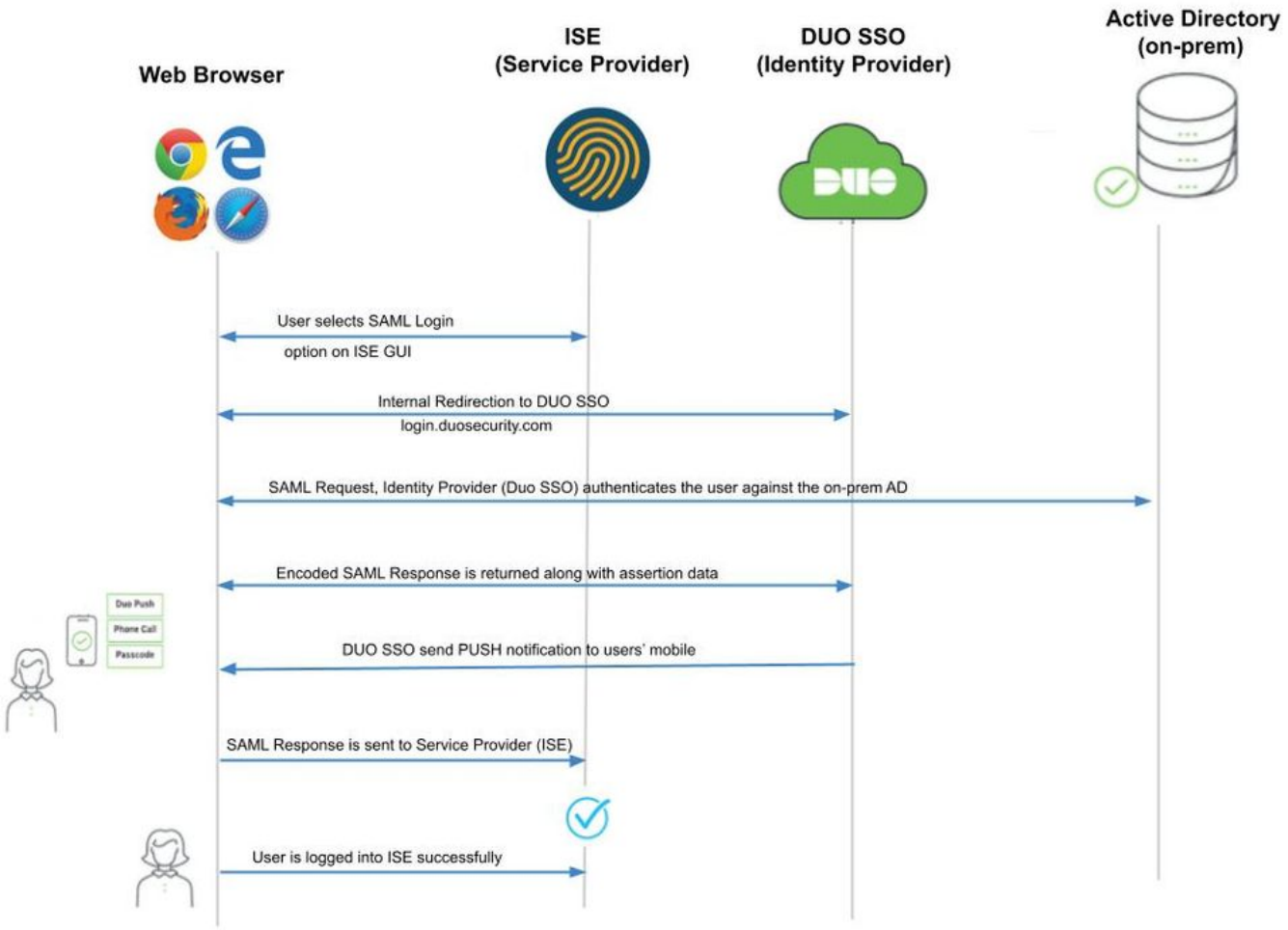
Las transacciones SAML utilizan lenguaje de marcado extensible (XML) para las comunicaciones estandarizadas entre el proveedor de identidad y los proveedores de servicios. SAML es el link entre la autenticación de la identidad del usuario y la autorización para utilizar un servicio.

Afirmación SAML

Una Afirmación SAML es el documento XML que el IdP envía al proveedor de servicios que contiene la autorización de usuario. Existen tres tipos diferentes de aserciones SAML: autenticación, atributo y decisión de autorización.

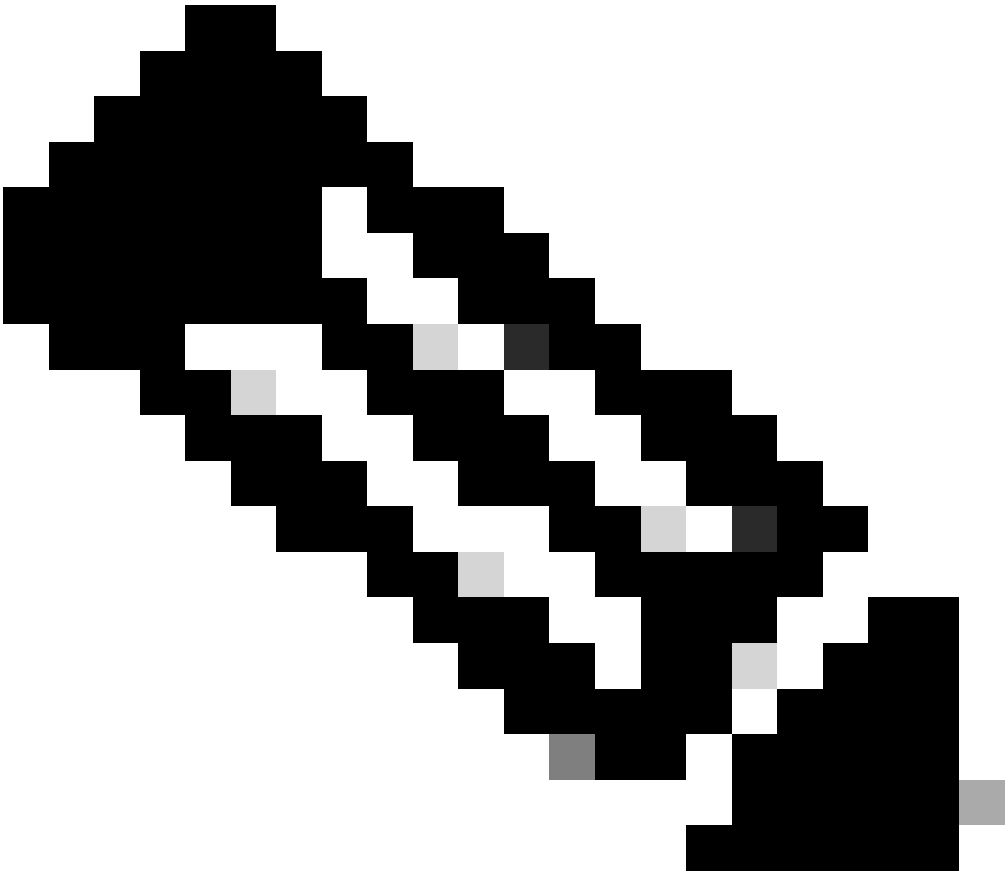
- Las aserciones de autenticación prueban la identificación del usuario y proporcionan la hora en que el usuario inició sesión y el método de autenticación que utilizaron (por ejemplo, Kerberos, de dos factores, etc.).
- La aserción de atribución pasa los atributos SAML, datos específicos que proporcionan información sobre el usuario, al SP.
- Una aserción de decisión de autorización declara si el usuario está autorizado para utilizar el servicio o si el IdP ha denegado su solicitud debido a un error de contraseña o a la falta de derechos para el servicio.

Diagrama de flujo de alto nivel



Flujo:

1. El usuario inicia sesión en ISE mediante la opción Iniciar sesión mediante SAML.
2. ISE (SAML SP) redirige el navegador del usuario a Duo SSO con un mensaje de solicitud SAML.



Nota: En un entorno distribuido, puede obtener un error de certificado no válido y el paso 3. ahora puede funcionar. Por lo tanto, para un entorno distribuido, el paso 2 difiere ligeramente de esta manera:
Problema: ISE redirige temporalmente al portal de uno de los nodos PSN (en el puerto 8443).
Solución: para asegurarse de que ISE presenta el mismo certificado que el certificado de la GUI de administración, asegúrese de que el certificado del sistema en el que confía también es válido para el uso del portal en todos los nodos PSN.

3. El usuario inicia sesión con las credenciales de AD principales.
4. Duo SSO lo reenvía a AD, lo que devuelve una respuesta a Duo SSO.
5. Duo SSO requiere que el usuario complete la autenticación de dos factores enviando un PUSH en el móvil.
6. El usuario completa la autenticación Duo de dos factores.
7. Duo SSO redirige el navegador del usuario al SP SAML con un mensaje de respuesta.
8. Ahora el usuario puede iniciar sesión en ISE.

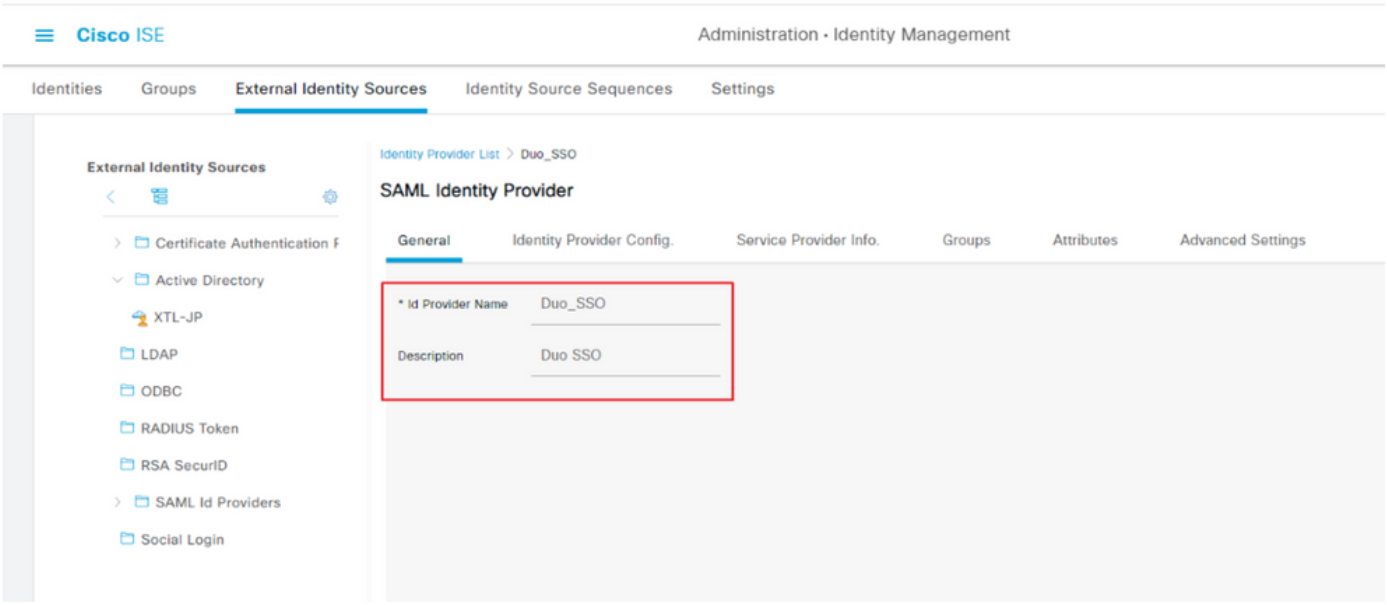
Configuración de la Integración de SSO de SAML con Duo SSO

Paso 1. Configuración de ID de SAML en ISE

Configuración de Duo SSO como fuente de identidad SAML externa

En ISE, desplácese hasta Administration > Identity Management > External Identity Sources > SAML Id Providers y haga clic en el botón **Agregar**.

Ingrese el nombre del IdP y haga clic en **Enviar** para guardarlo. El nombre del idP es significativo solo para ISE, como se muestra en la imagen:

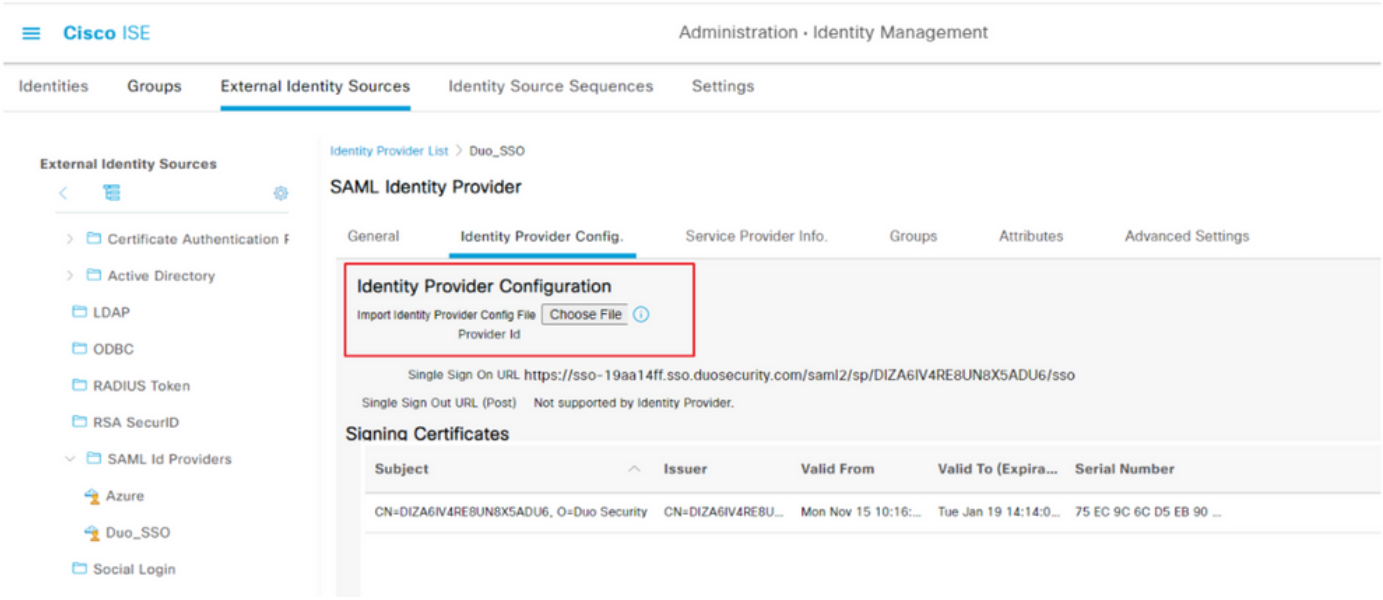


Importar el archivo XML de metadatos SAML desde Duo Admin Portal

En ISE, navegue hasta Administration > Identity Management > External Identity Sources > SAML Id Providers. > Choose the SAML IdP you created, haga clic en el botón **Choose File** Identity Provider Configuration y, a continuación, en el botón **Choose File**.

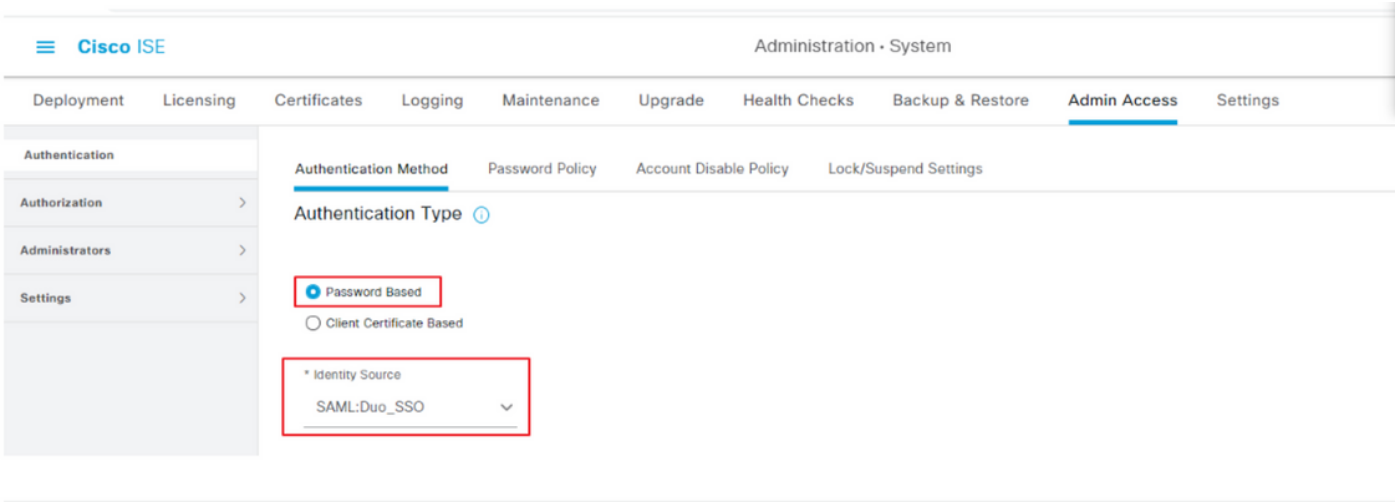
Elija el archivo **SSO IDP Metadata XML** exportado desde el portal Duo Admin y haga clic en **Open** para guardarlo. (Este paso también se menciona en la sección Duo de este documento.)

La URL de SSO y los certificados de firma son:



Configurar método de autenticación de ISE

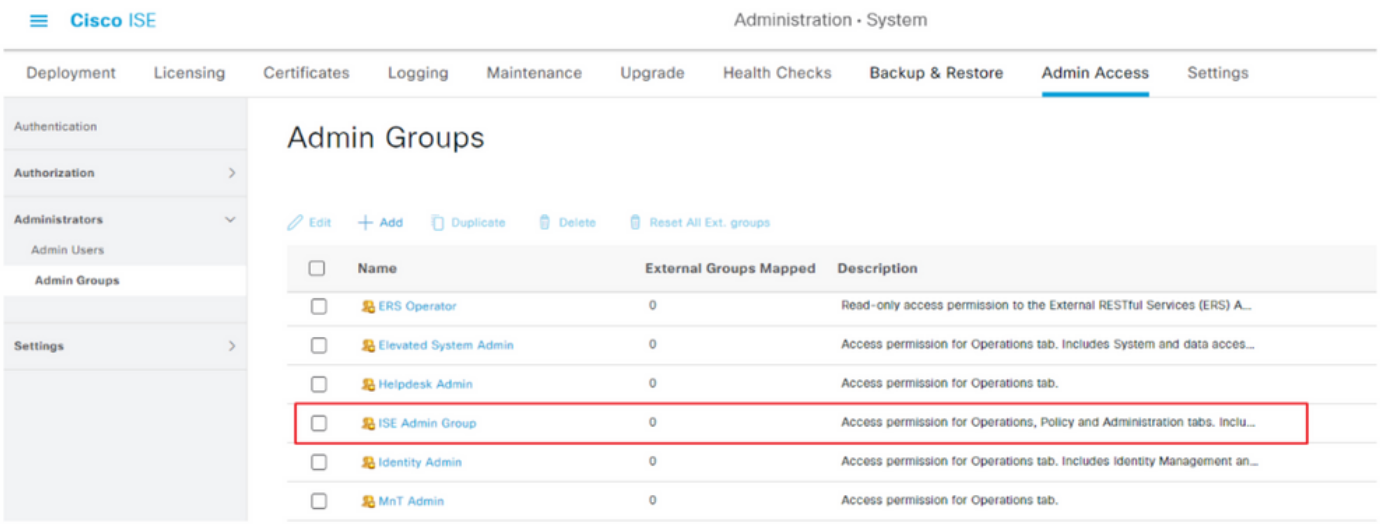
Desplácese hasta Administration > System > Admin Access > Authentication > Authentication Method y seleccione el botón de radio Password-Based (Basado en contraseña). Elija el nombre de IdP necesario creado anteriormente en la lista desplegable Origen de identidad, como se muestra en la imagen:



Crear un grupo de administradores

Desplácese hasta Administration > System > Admin Access > Authentication > Administrators > Admin Group y haga clic en el botón **Super Admin** y, a continuación, en el botón **Duplicar**. Ingrese el **Nombre del grupo de administradores** y haga clic en el botón **Enviar**.

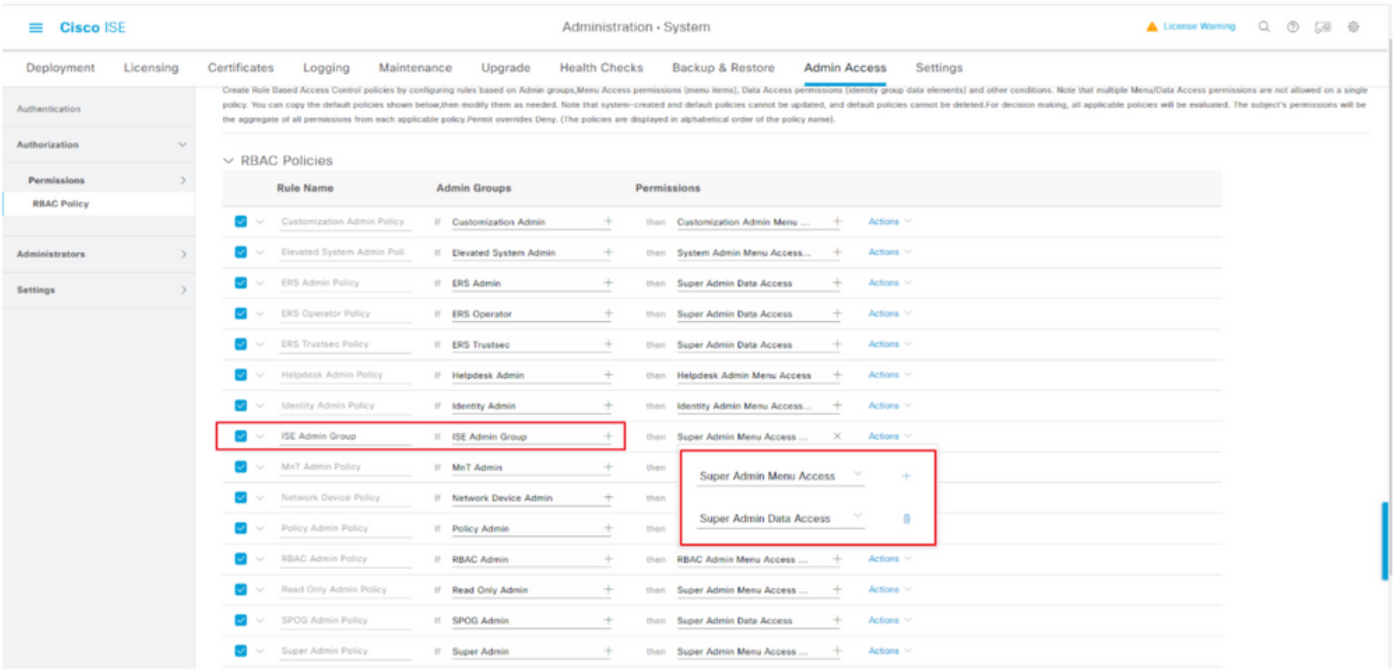
Esto proporciona privilegios de superadministrador al grupo de administradores.



Crear una política RBAC para el grupo de administradores

Desplácese hasta Administration > System > Admin Access > Authorization > RBAC Policy y elija las **acciones** correspondientes a la **política de superadministración**. Haga clic en Duplicate > Add the Name field > Save.

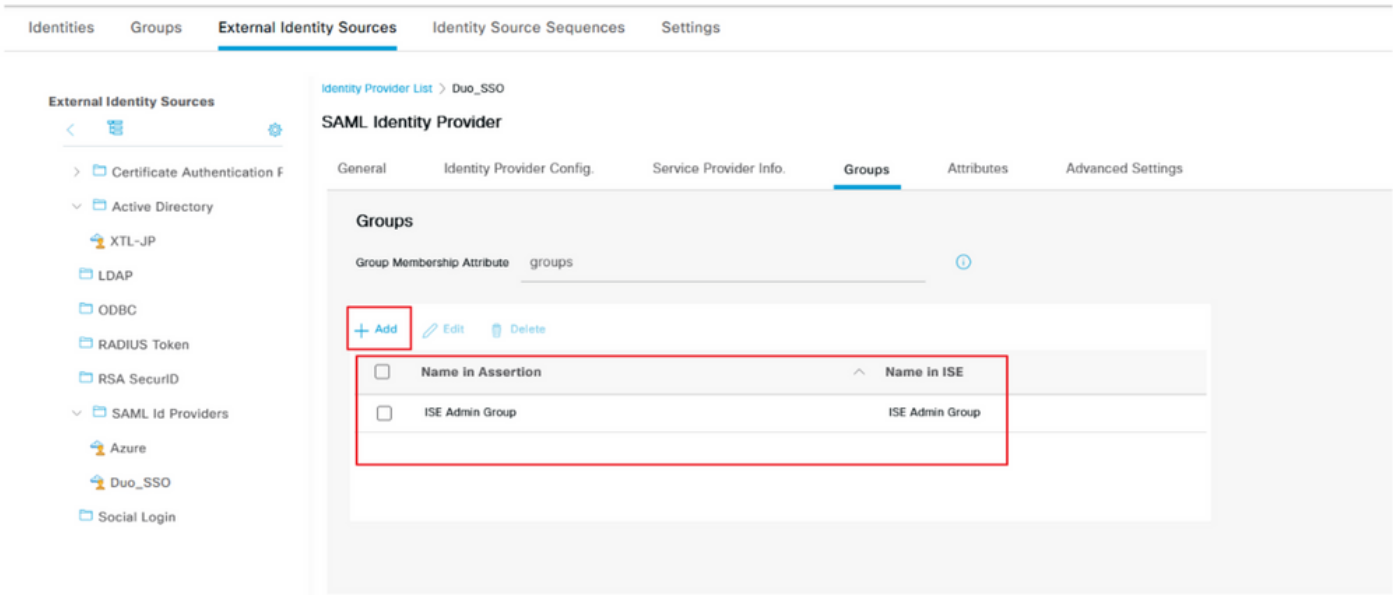
Los permisos de acceso son los mismos que los de la directiva de superadministrador.



Agregar pertenencia a grupos

En ISE, desplácese hasta Administration > Identity Management > External Identity Sources > SAML Id Providers y elija el IDP de SAML que ha creado. Haga clic en **Grupos** y, a continuación, en el botón Agregar.

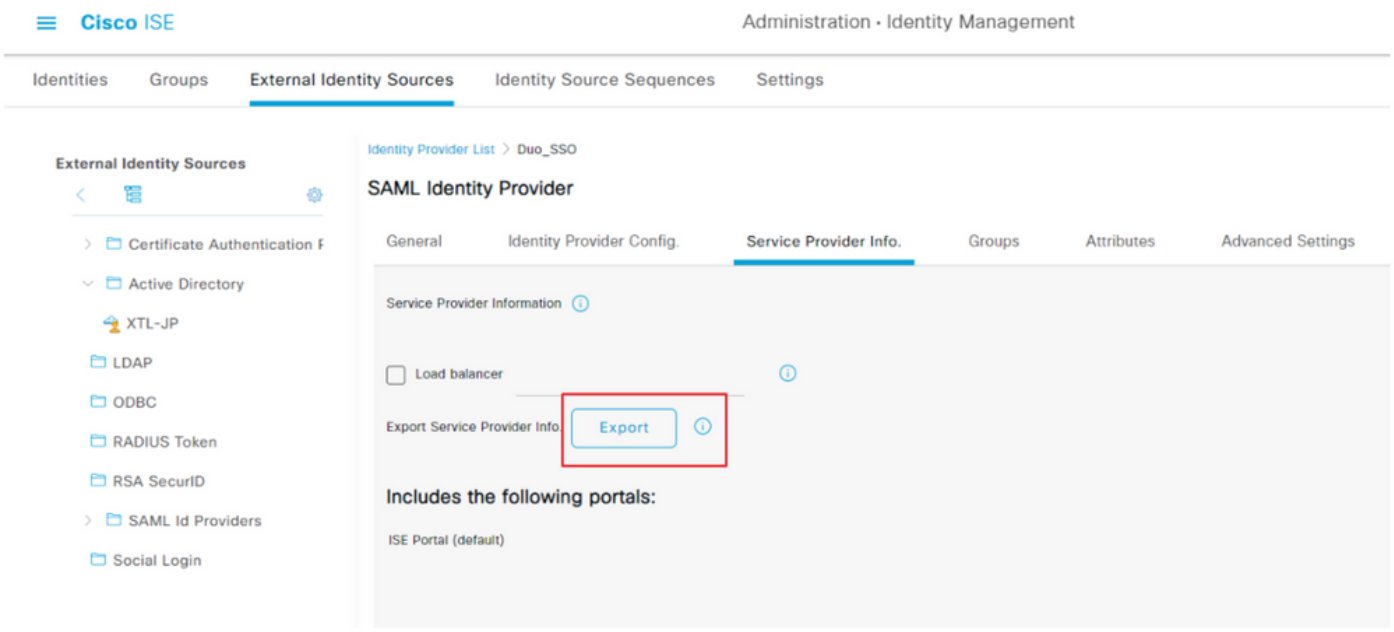
Agregue el nombre en la aserción (nombre del grupo de administradores de ISE) y en el menú desplegable elija el grupo de control de acceso basado en roles (RBAC) creado (paso 4) y haga clic en **Abrir** para guardarlo. La URL de SSO y los certificados de firma se rellenan automáticamente:



Exportar información SP

Vaya a Administration > Identity Management > External Identity Sources > SAML Id Providers > (Your SAML Provider) .

Cambie la ficha a SP Info. y haga clic en el botón **Export** como se muestra en la imagen:



Descargue el .xml archivo y guárdelo. Anote el valor de AssertionConsumerService Location URL y **entityID**, ya que estos detalles son obligatorios en el portal Duo SSO.

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

Aquí están los detalles/atributos de interés recopilados del archivo meta que debe configurarse en la integración SAML genérica Duo

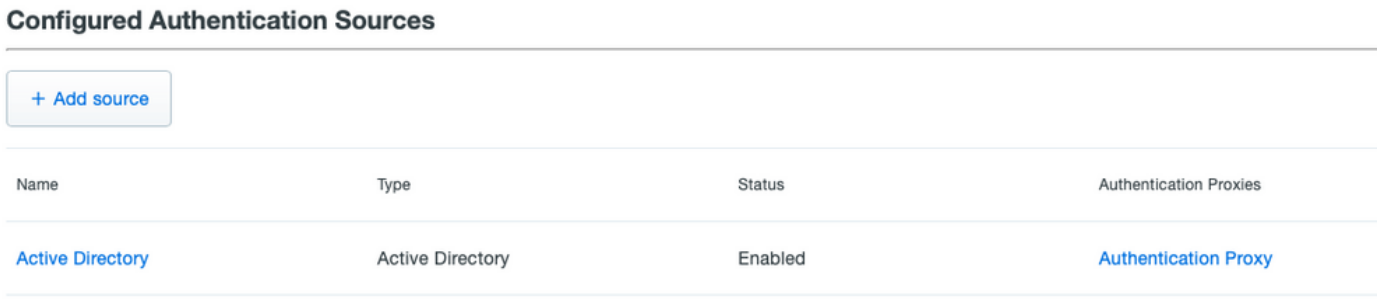
entityID = http://CiscoISE/7fdfc239-631e-439c-a3ab-f5e56429779d.

AssertionConsumerService Location = https://10.x.x.x:8443/portal/SSOLoginResponse.action donde 10.x.x.x es la IP de ISE que se encuentra en el archivo XML (Location).

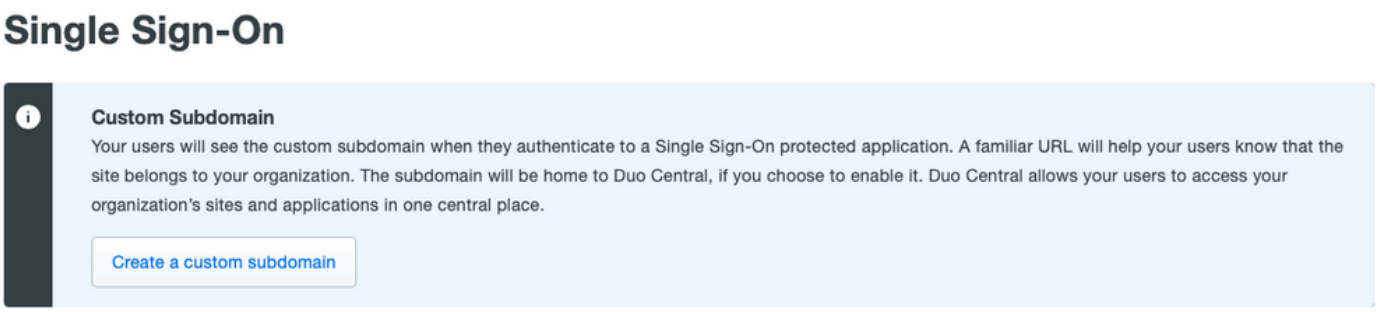
AssertionConsumerService Location = https://isenodename.com:8443/portal/SSOLoginResponse.action donde isenodename es el nombre FQDN de ISE real que se encuentra en el archivo XML (Ubicación).

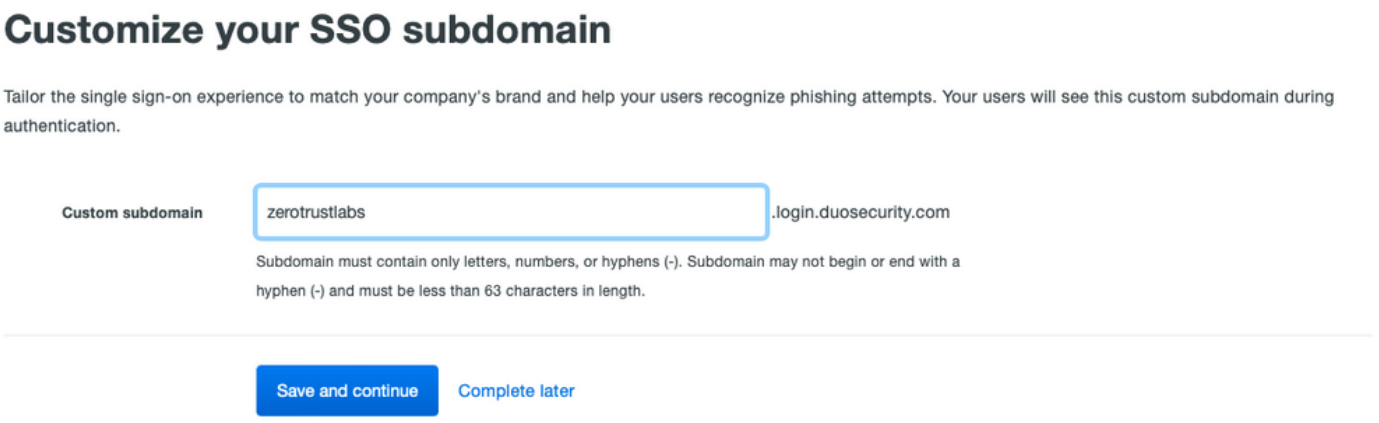
Paso 2. Configuración de Duo SSO para ISE

Verifique este KB para configurar Duo SSO con AD como fuente de autenticación.



Marque este KB para habilitar el SSO con su dominio personalizado.



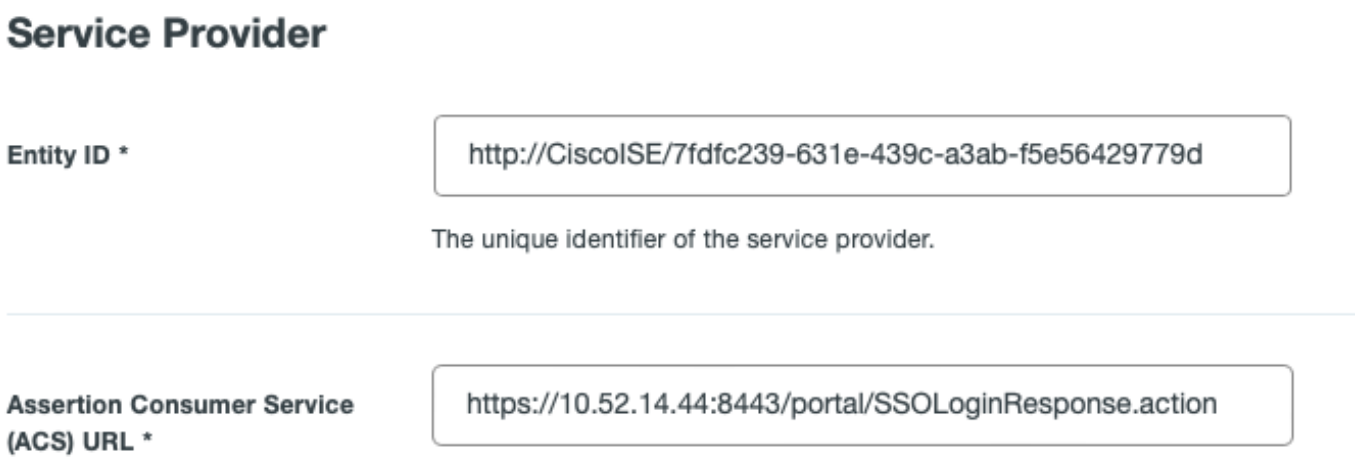


Paso 3. Integre Cisco ISE con Duo SSO como SP genérico

Verifique el Paso 1. y el Paso 2. de este KB para integrar Cisco ISE con Duo SSO como SP genérico.

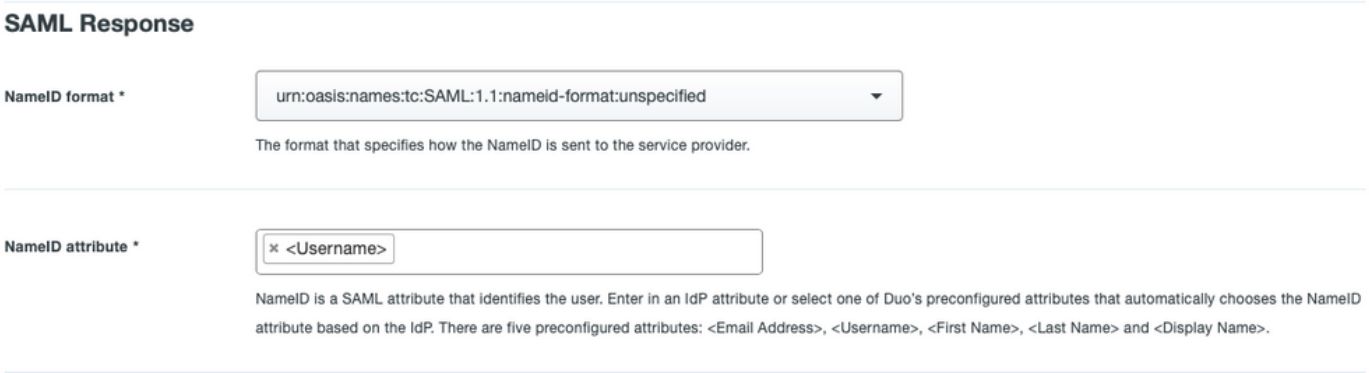
Configure los detalles de Cisco ISE SP en el panel Duo Admin para Generic SP:

Nombre	Descripción
ID de entidad	http://CiscoISE/7fdfc239-631e-439c-a3ab-f5e56429779d
URL de servicio de consumidor de afirmación (ACS)	https://10.x.x.x:8443/portal/SSOLoginResponse.action

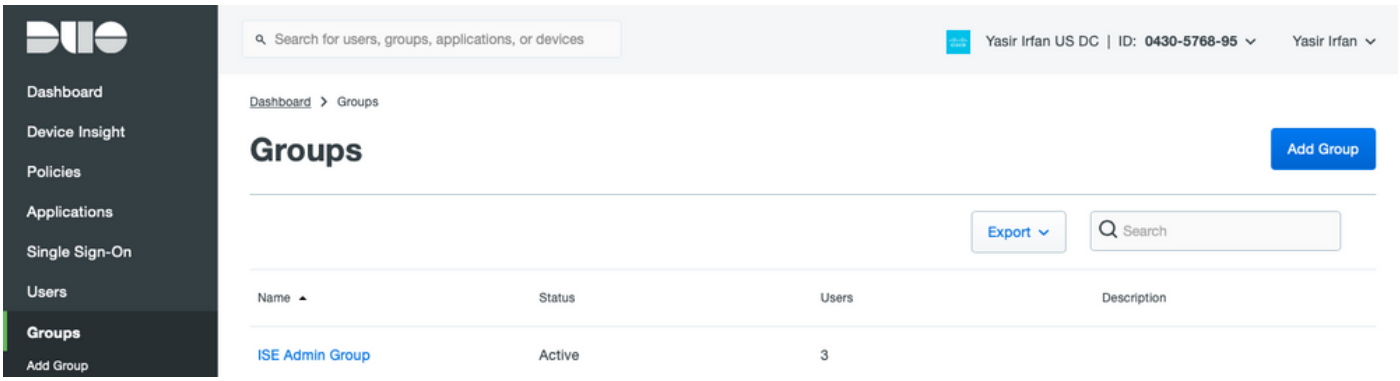


Configuración de la respuesta SAML para Cisco ISE:

Nombre	Descripción
Formato NameID	urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified
Atributo NameID	Nombre de usuario

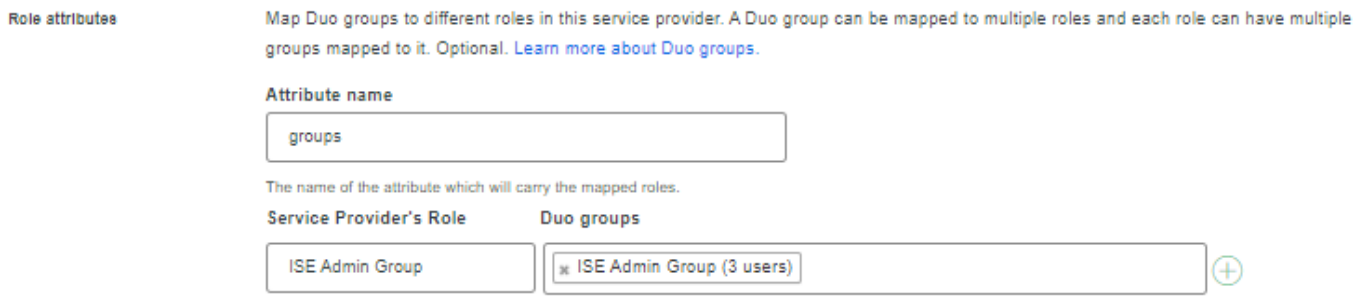


Cree un grupo llamado Grupo de administradores de Cisco en el Panel de administración de Duo y agregue los usuarios de ISE a este grupo o cree un grupo en Windows AD y sincronice el mismo con el panel de administradores de Duo mediante la función de sincronización de directorios.

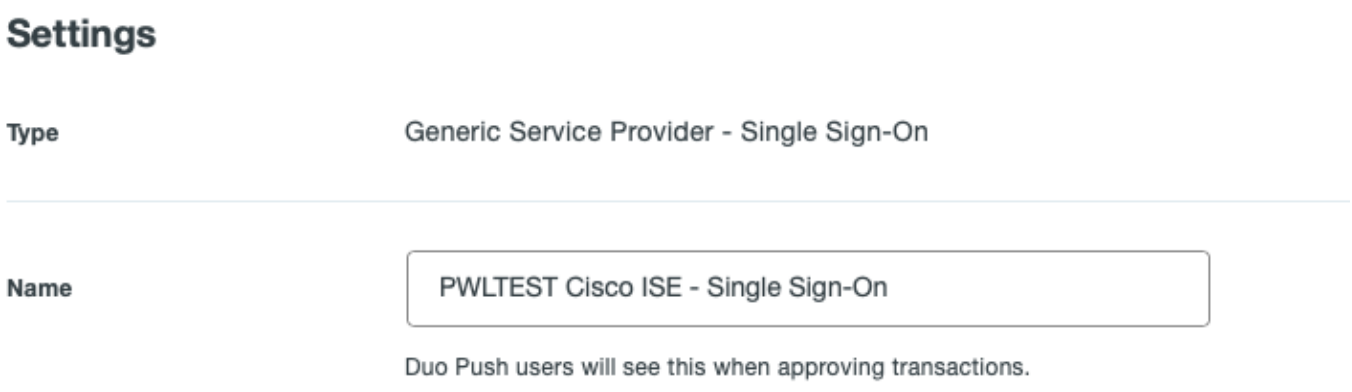


Configurar atributos de rol para Cisco ISE:

Nombre	Descripción
Nombre del atributo	grupos
Función SP	Grupo de administradores de ISE
Grupos duales	Grupo de administradores de ISE

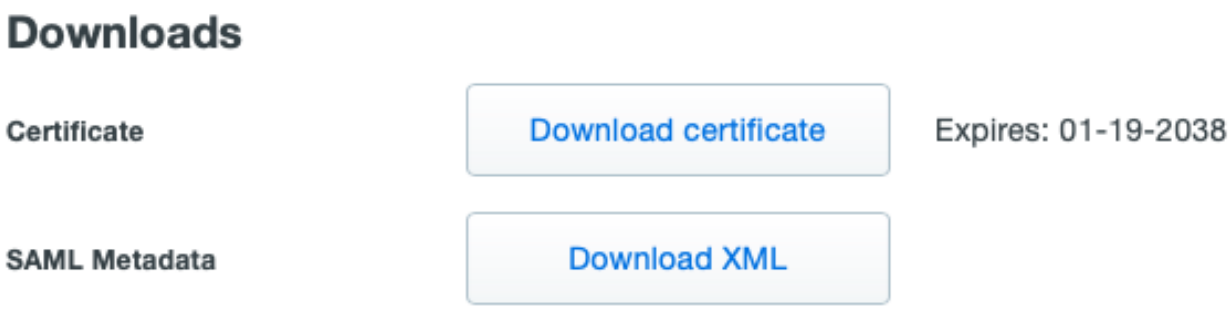


En la sección Configuración, proporcione un nombre adecuado en la ficha **Nombre** para esta integración.



Haga clic en el botón **Save** para guardar la configuración y consulte este KB para obtener más detalles.

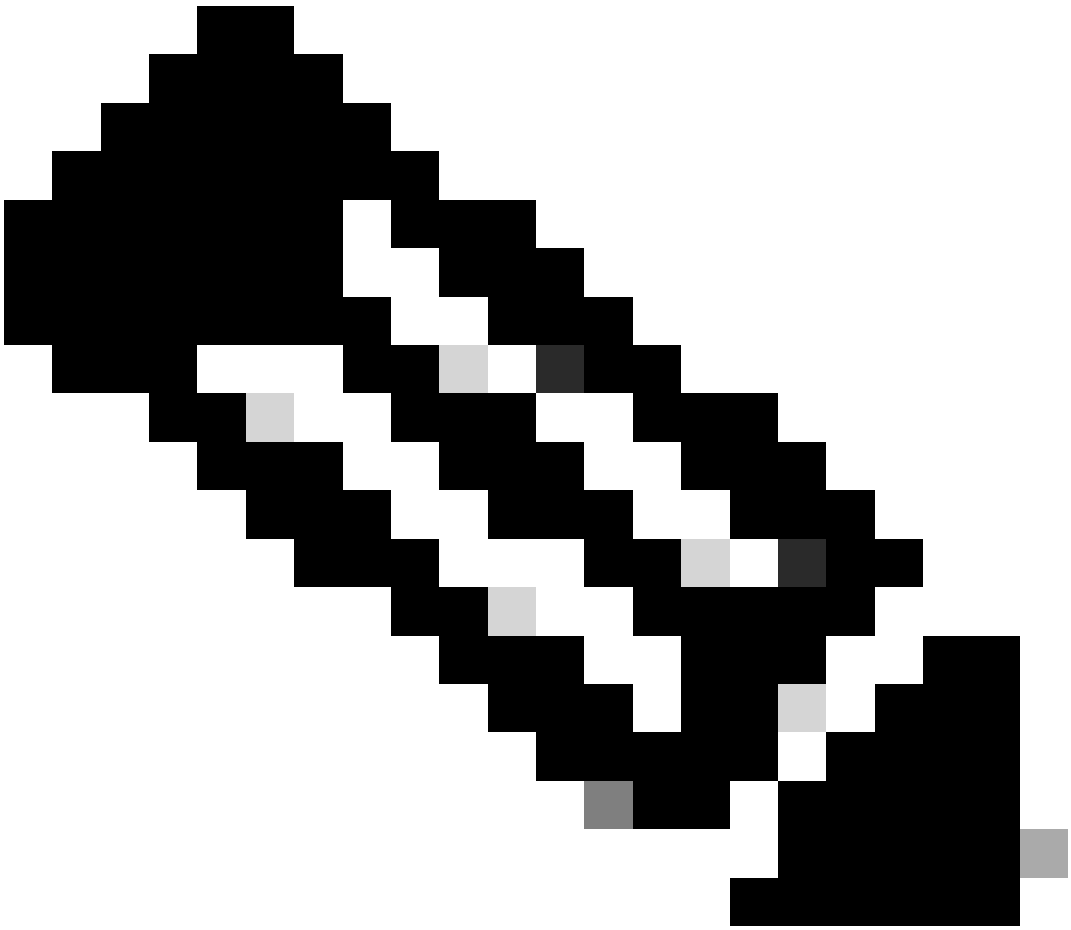
Haga clic en **Download XML** para descargar los metadatos SAML.



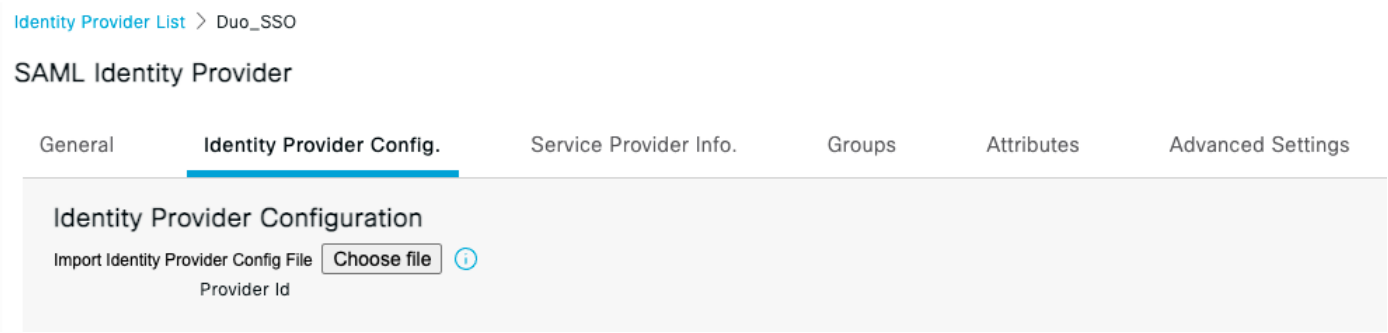
Cargue la descarga de MetaData de SAML desde el panel de administración de Duo a Cisco ISE accediendo a Administration > Identity Management > External Identity Sources > SAML Id Providers > Duo_SSO.

Cambie la ficha a **Identity Provider Config.** y haga clic en el botón **Choose** file (**Elegir** archivo).

Elija el archivo **XML de metadatos** descargado en el paso 8 y haga clic en **Guardar**.



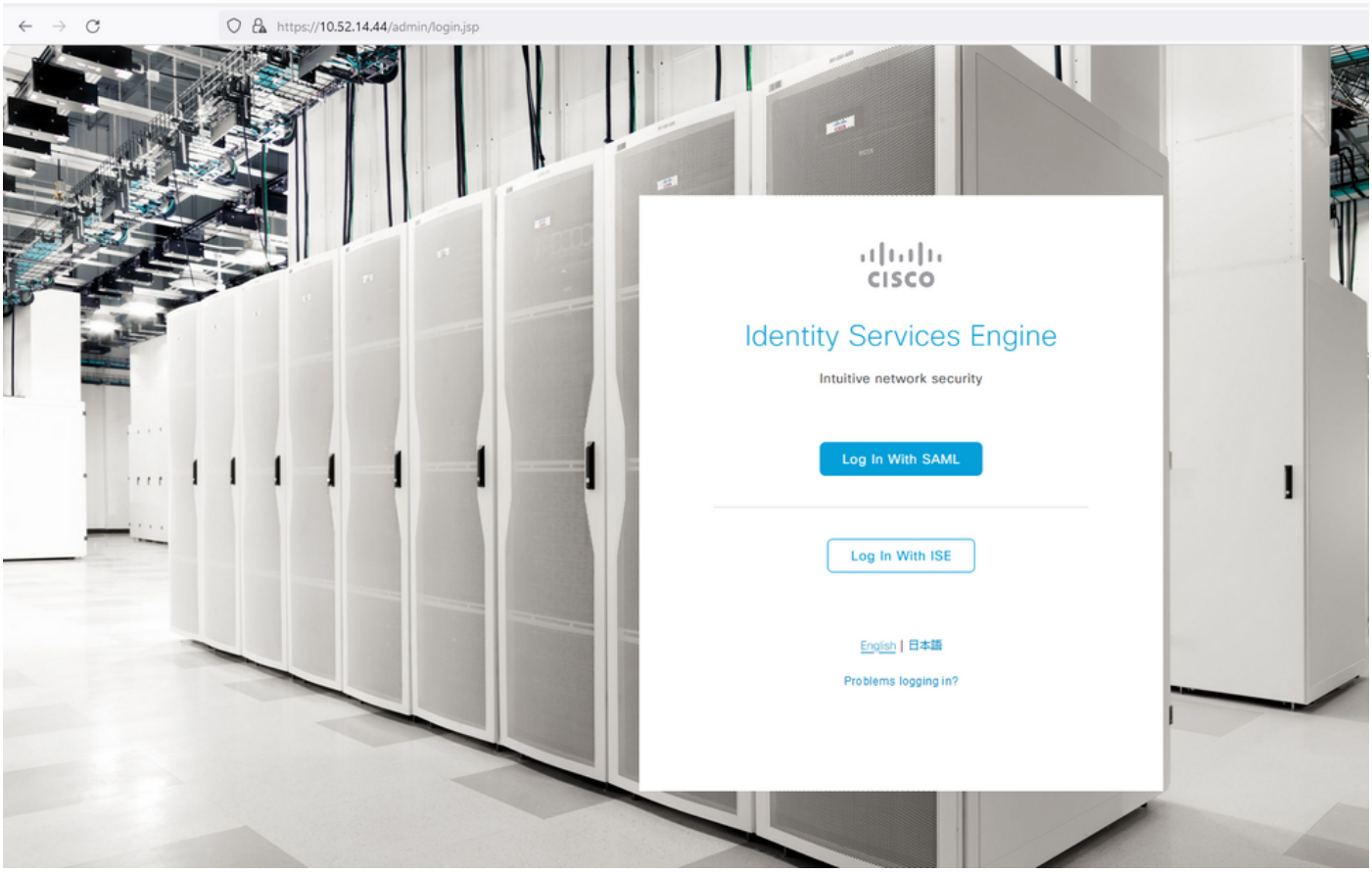
Nota: Este paso se menciona aquí en la sección Configure SAML SSO Integration with Duo SSO; Paso 2. Importe el archivo **XML de metadatos SAML** desde el portal Duo Admin.



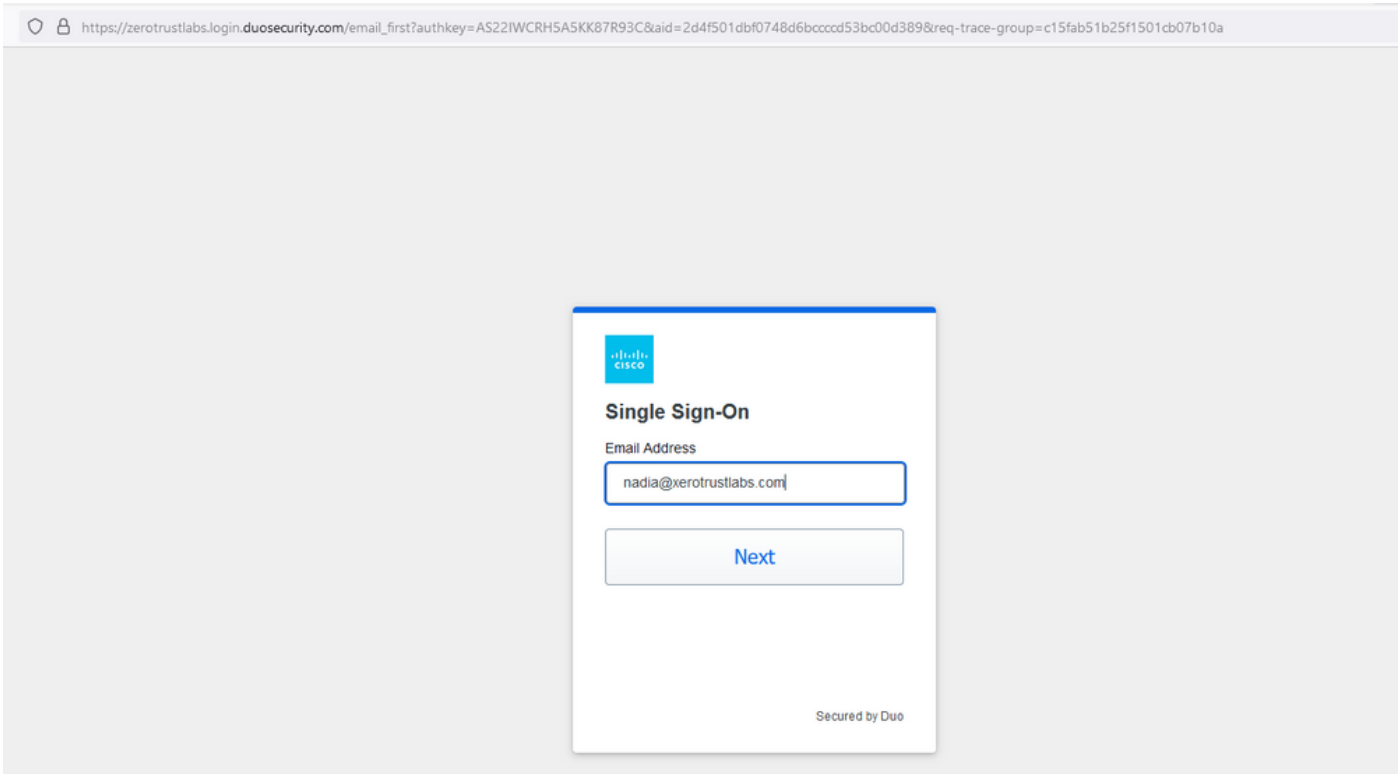
Verificación

Prueba de la integración con Duo SSO

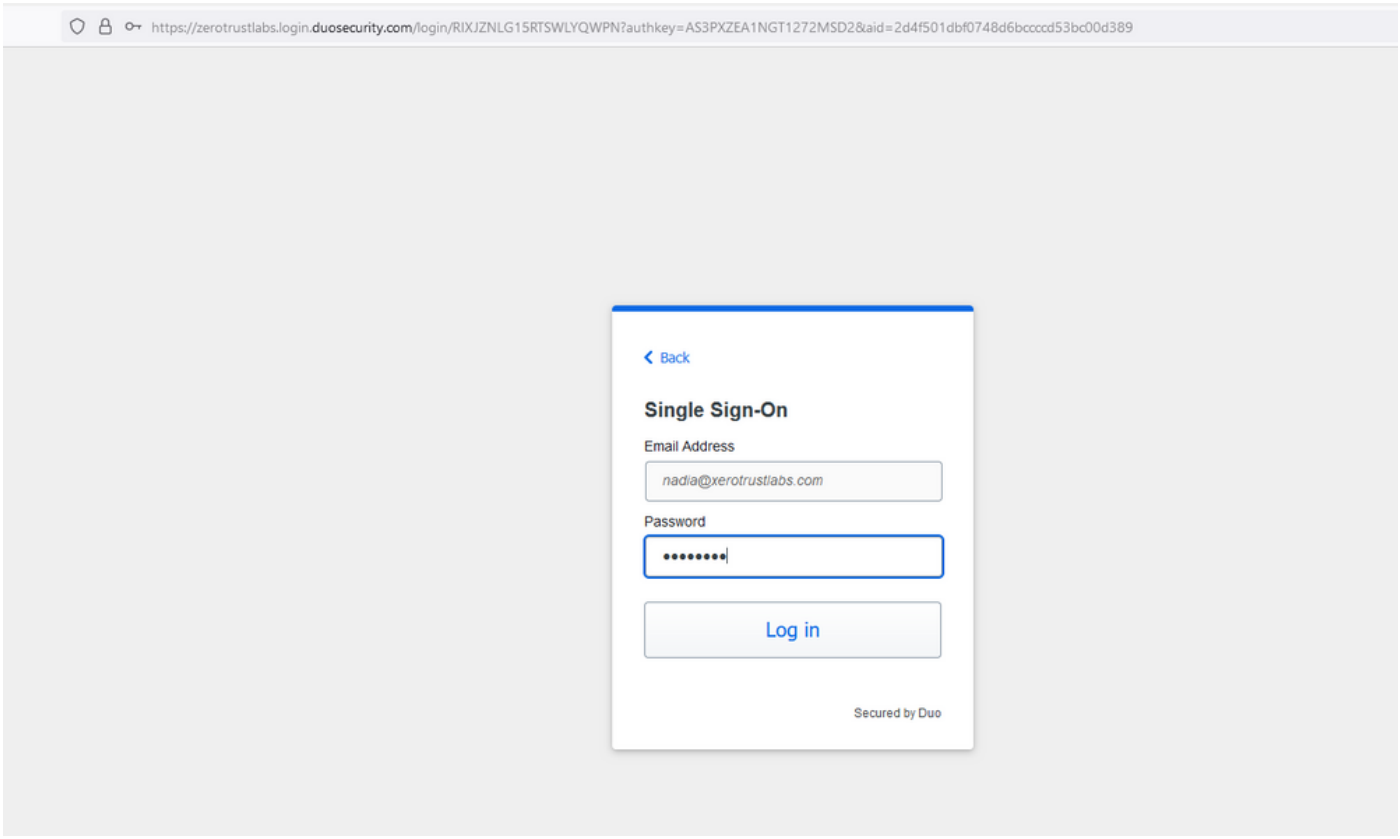
1. Inicie sesión en el **Panel de administración de Cisco ISE** y haga clic en **Iniciar sesión** con SAML.



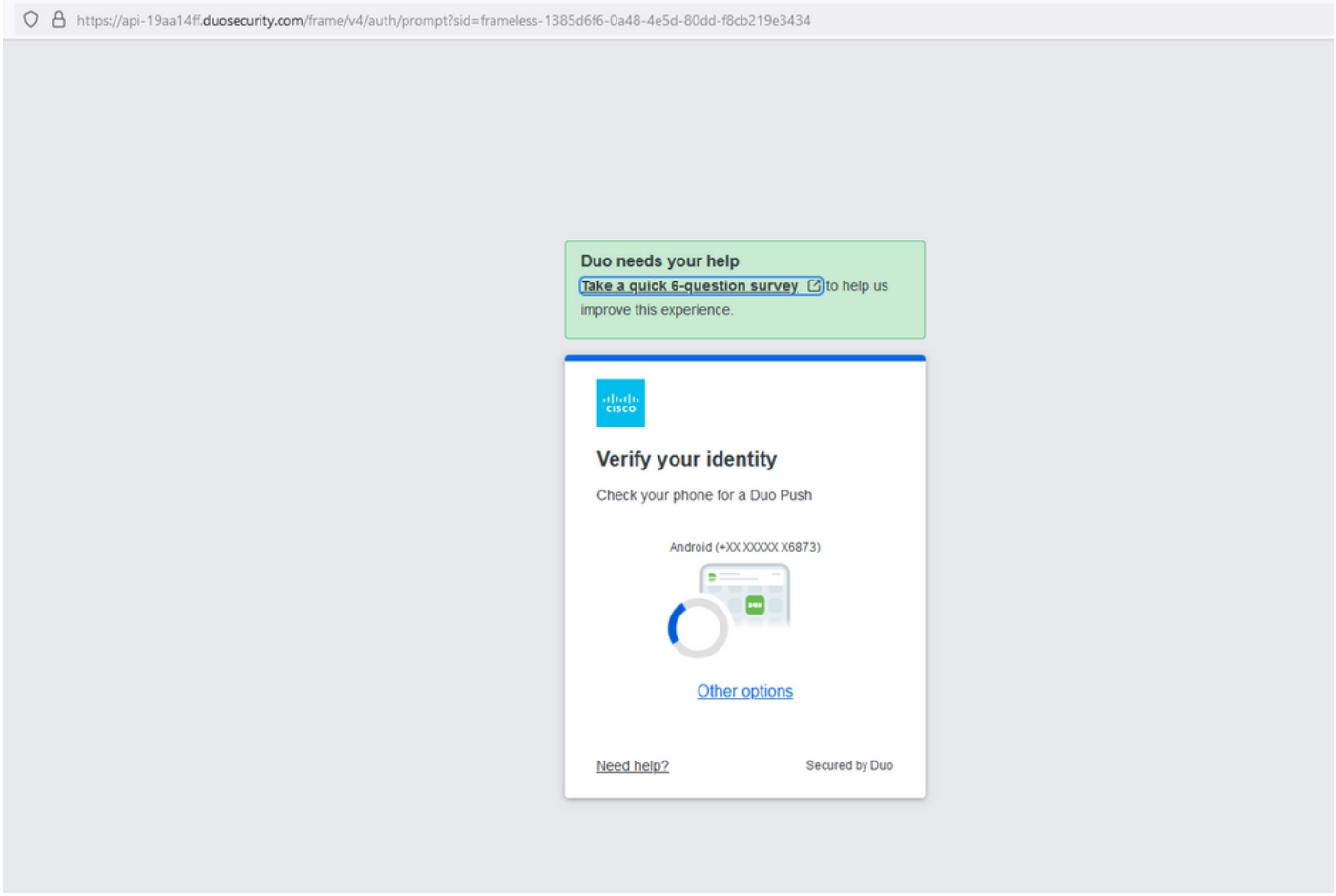
2. Redirigido a la página SSO, introduzca la **dirección de correo electrónico** y haga clic en **Siguiente**.



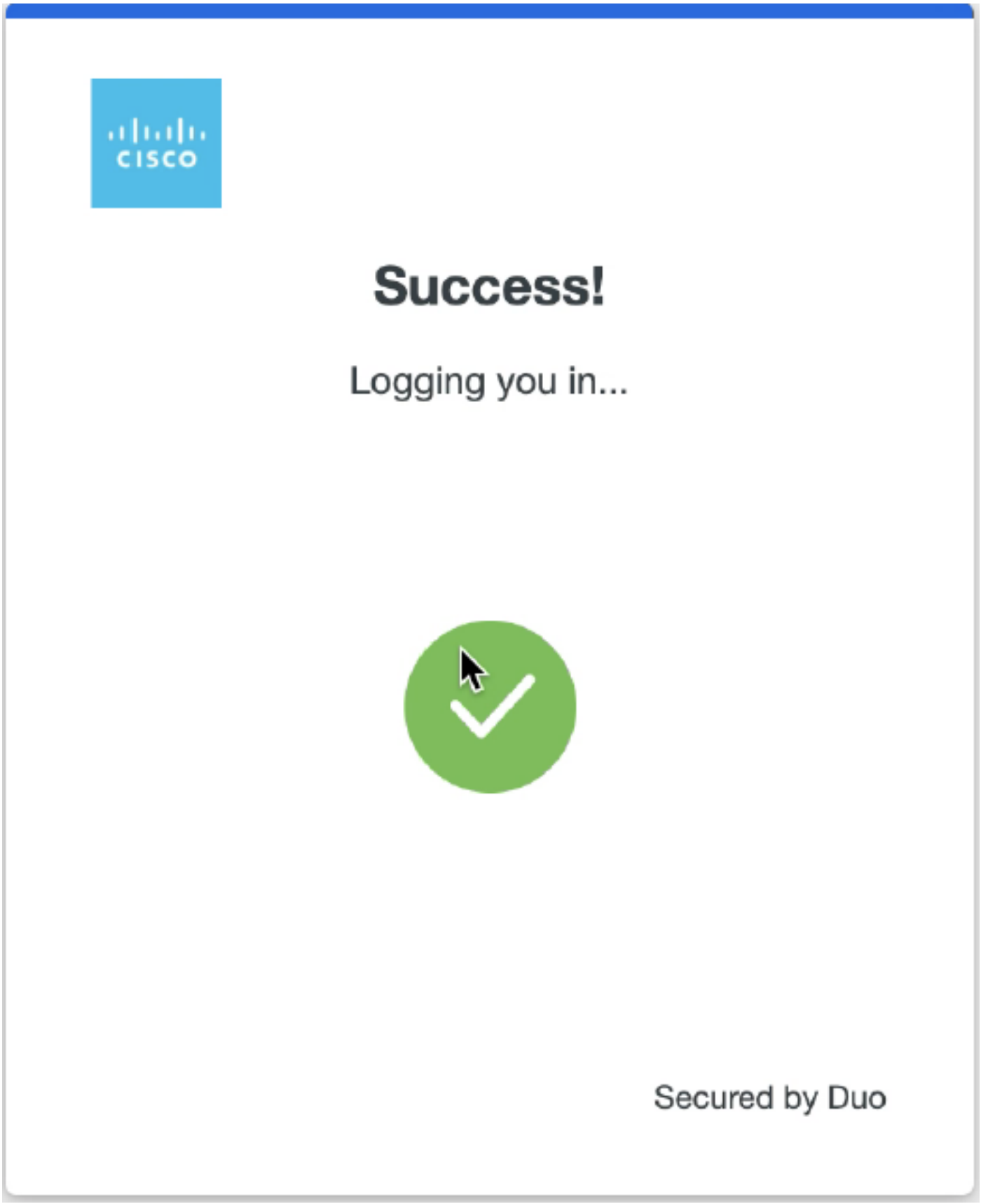
3. Introduzca la contraseña y haga clic en **Iniciar sesión**.



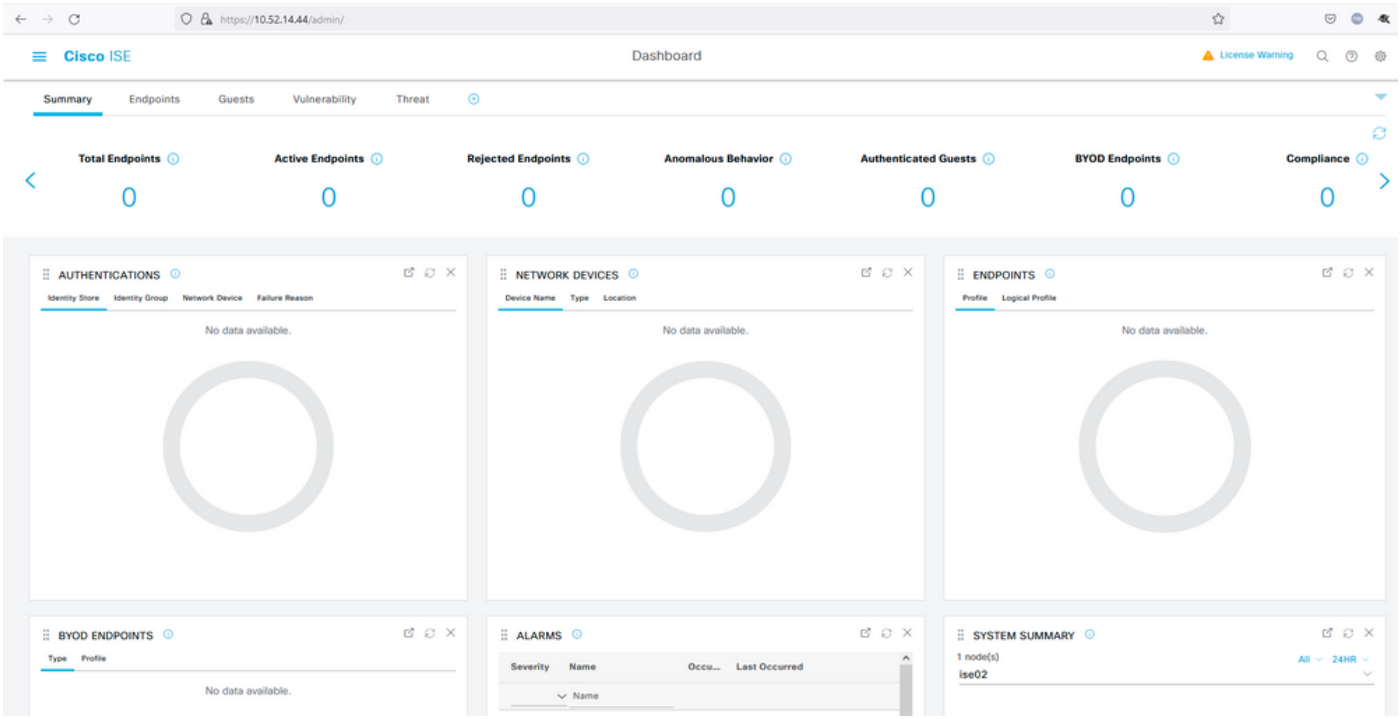
4. Usted recibe un mensaje Duo Push en su dispositivo móvil.



5. Una vez que acepta el mensaje, aparece una ventana y se le redirige automáticamente a la página ISE Admin.



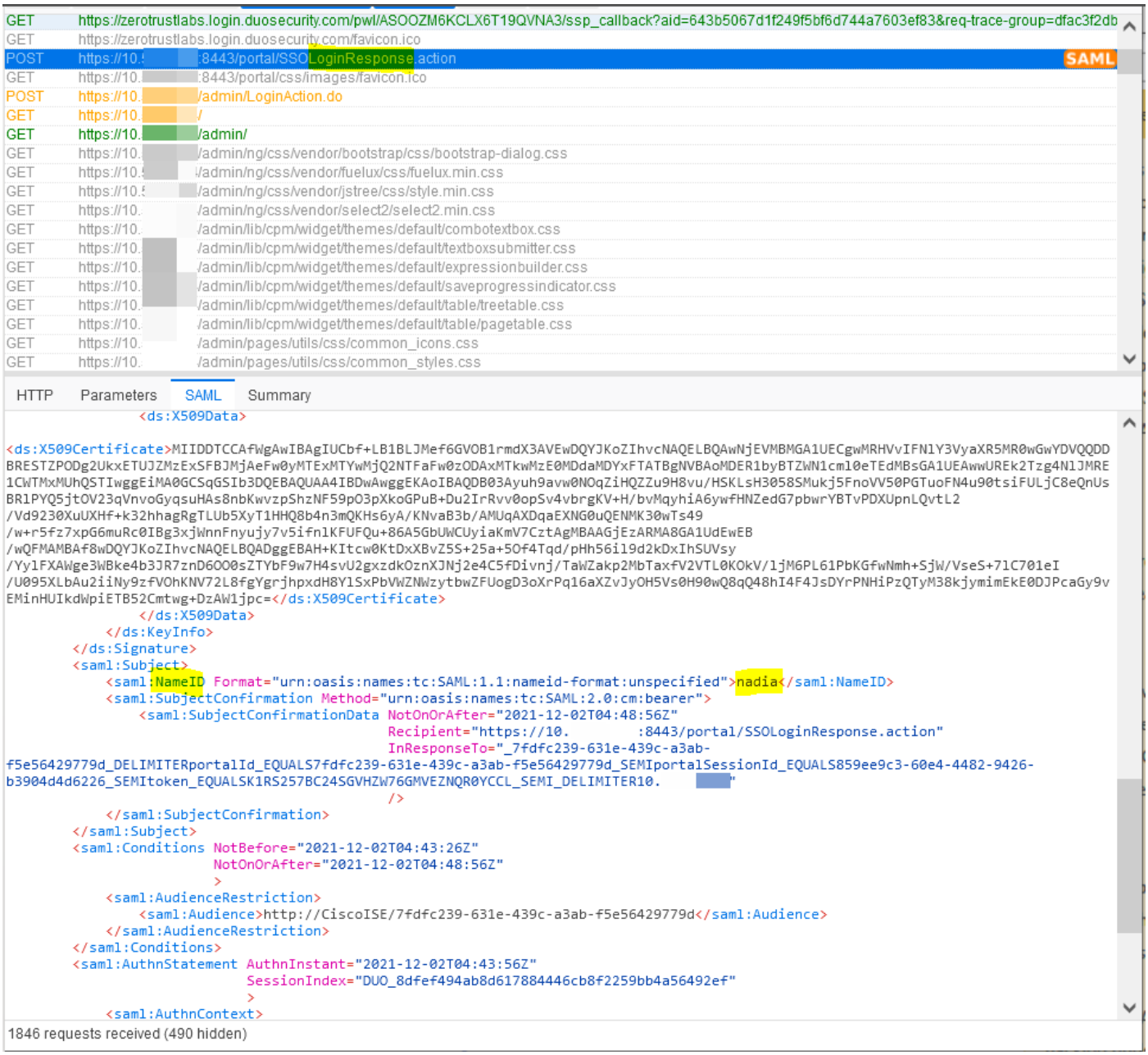
6. Página de acceso a la GUI de ISE Admin.



Troubleshoot

- Descargue la extensión del rastreador SAML para Mozilla FF https://addons.mozilla.org/en-US/firefox/addon/saml-tracer/.

- Desplácese hasta el SSOLoginResponse.action paquete. En la pestaña **SAML**, verá una serie de atributos enviados desde Duo SAML: NameID, Recipient (URL de ubicación de AssertionConsumerService) y Audience(EntityID).



- Inicio de sesión en directo en ISE:

Cisco ISE

Overview

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

Steps

5231	Guest Authentication Passed

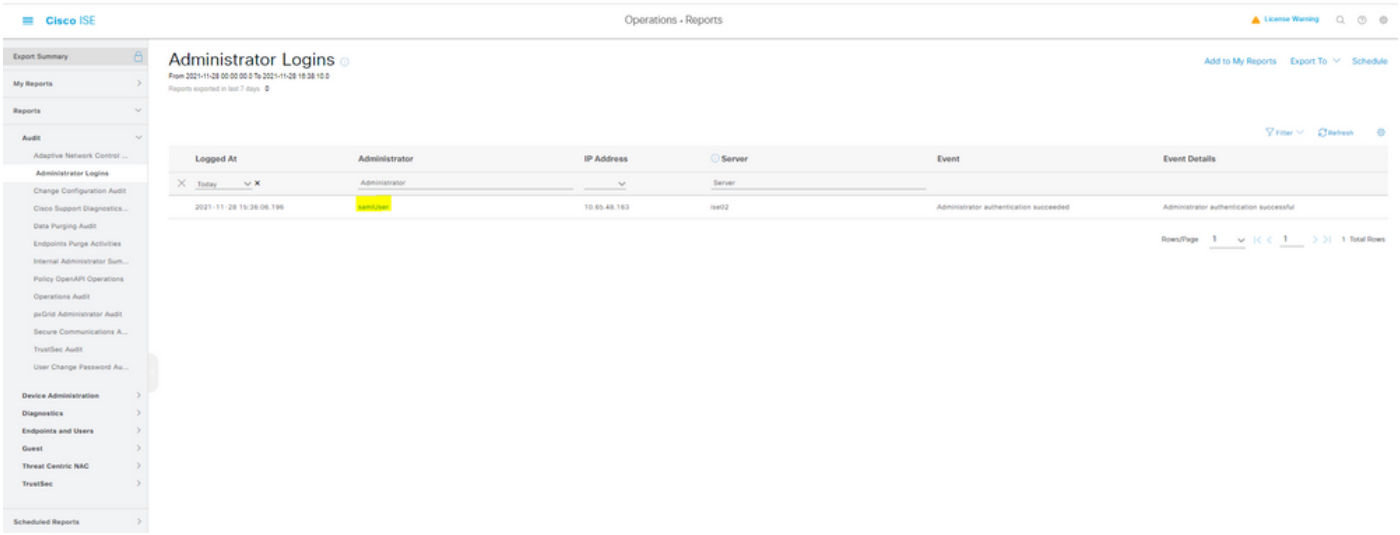
Authentication Details

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

- Inicio de sesión administrativo en ISE: nombre de usuario: 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

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).