

Configurare ISE 3.1 GUI Admin Log in utilizzando l'integrazione SAML con Duo SSO e Windows AD

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Provider di identità \(IdP\)](#)

[Provider di servizi \(SP\)](#)

[SAML](#)

[Asserzione SAML](#)

[Diagramma di flusso ad alto livello](#)

[Configura integrazione SAML SSO con Duo SSO](#)

[Passaggio 1. Configurazione di SAML IdP su ISE](#)

[Configurazione di Duo SSO come origine di identità SAML esterna](#)

[Importare il file XML dei metadati SAML dal portale di amministrazione Duo](#)

[Configura metodo di autenticazione ISE](#)

[Crea un gruppo amministrativo](#)

[Creare un criterio RBAC per il gruppo Admin](#)

[Aggiungi appartenenza a gruppi](#)

[Esporta informazioni SP](#)

[Passaggio 2. Configurare Duo SSO per ISE](#)

[Passaggio 3. Integrazione di Cisco ISE con Duo SSO come SP generico](#)

[Verifica](#)

[Test dell'integrazione con Duo SSO](#)

[Risoluzione dei problemi](#)

Introduzione

Questo documento descrive come configurare l'integrazione di Cisco ISE 3.1 SAML SSO con un provider di identità esterno come Cisco Duo SSO.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Cisco Identity Services Engine (ISE) 3.1
- Conoscenze base delle distribuzioni SAML (Security Assertion Markup Language) Single Sign-On (SSO) (SAML 1.1)
- Conoscenza di Cisco DUO SSO
- Informazioni su Windows Active Directory

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

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

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Provider di identità (IdP)

In questo caso, è il Duo SSO che verifica e dichiara l'identità di un utente e i privilegi di accesso a una risorsa richiesta (il "Provider di servizi").

Duo SSO funge da provider di identità, autenticando gli utenti tramite Active Directory locale (AD) esistente con SAML 1.1 o un provider di identità SAML 2.0 (ad esempio, Microsoft Azure) e richiedendo l'autenticazione a due fattori prima di consentire l'accesso all'applicazione del provider di servizi.

Quando si configura un'applicazione da proteggere con Duo SSO, è necessario inviare gli attributi da Duo SSO all'applicazione. Active Directory funziona senza ulteriori impostazioni, ma se come origine di autenticazione è stato utilizzato un provider di identità SAML(2.0), verificare di averlo configurato per l'invio degli attributi SAML corretti.

Provider di servizi (SP)

La risorsa o il servizio ospitato a cui l'utente intende accedere; in questo caso, Cisco ISE Application Server.

SAML

SAML è uno standard aperto che consente a IdP di passare le credenziali di autorizzazione all'SP.

Le transazioni SAML utilizzano il linguaggio XML (Extensible Markup Language) per le

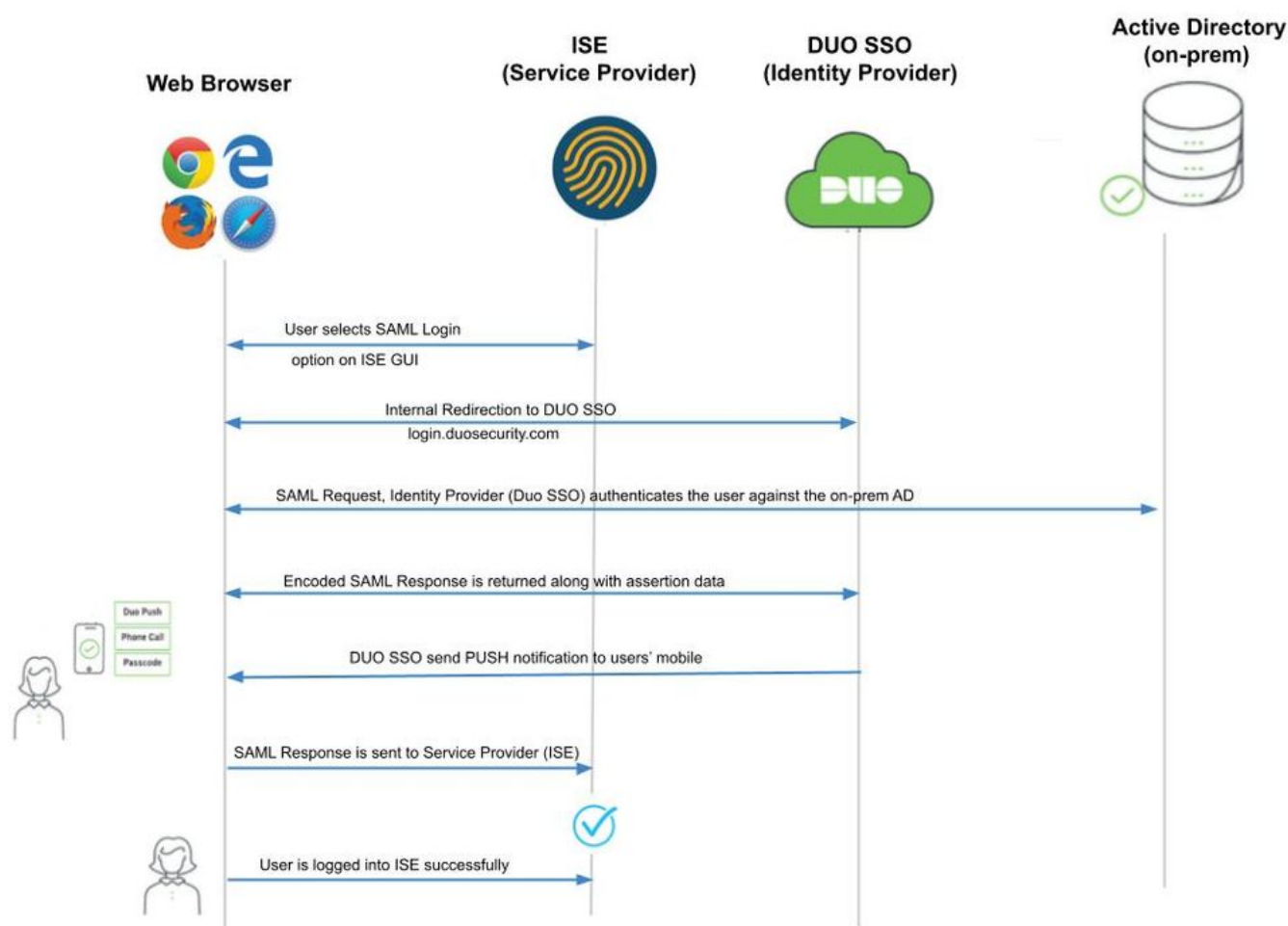
comunicazioni standardizzate tra provider di identità e provider di servizi. SAML è il collegamento tra l'autenticazione dell'identità dell'utente e l'autorizzazione per utilizzare un servizio.

Asserzione SAML

Un'asserzione SAML è il documento XML che l'IdP invia al provider di servizi che contiene l'autorizzazione utente. Esistono tre tipi diversi di asserzioni SAML: autenticazione, attributo e decisione di autorizzazione.

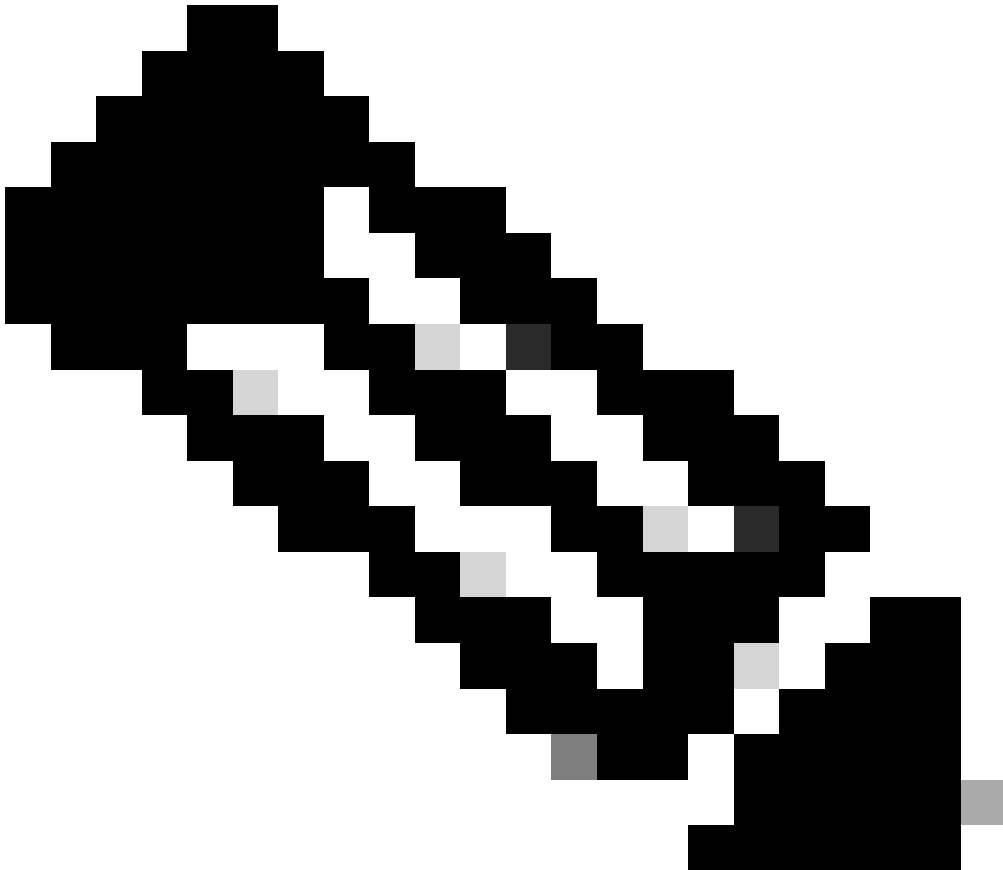
- Le asserzioni di autenticazione provano l'identificazione dell'utente e forniscono l'ora di accesso dell'utente e il metodo di autenticazione utilizzato, ad esempio Kerberos, a due fattori e così via.
- L'asserzione di attribuzione passa all'SP gli attributi SAML, parti specifiche di dati che forniscono informazioni sull'utente.
- Un'asserzione di decisione di autorizzazione dichiara se l'utente è autorizzato a utilizzare il servizio o se l'IdP ha negato la richiesta a causa di un errore della password o della mancanza di diritti per il servizio.

Diagramma di flusso ad alto livello



Flusso:

1. L'utente accede ad ISE usando l'opzione Login via SAML.
 2. ISE (SAML SP) reindirizza il browser dell'utente a Duo SSO con un messaggio di richiesta SAML.
-



Nota: in un ambiente distribuito, è possibile ottenere un errore di certificato non valido e il passo 3. ora può funzionare. Pertanto, per un ambiente distribuito, la Fase 2. differisce leggermente in questo modo:

Problema: ISE reindirizza temporaneamente il portale di uno dei nodi PSN (sulla porta 8443).

Soluzione: per garantire che ISE presenti lo stesso certificato dell'interfaccia utente grafica dell'amministratore, verificare che il certificato di sistema considerato attendibile sia valido anche per l'utilizzo del portale in tutti i nodi PSN.

-
3. L'utente accede con le credenziali di Active Directory primarie.
 4. Duo SSO inoltra questo messaggio ad AD che restituisce una risposta a Duo SSO.
 5. Duo SSO richiede all'utente di completare l'autenticazione a due fattori inviando un PUSH sul dispositivo mobile.

6. L'utente completa l'autenticazione a due fattori Duo.
7. Duo SSO reindirizza il browser dell'utente all'SP SAML con un messaggio di risposta.
8. A questo punto, l'utente può accedere ad ISE.

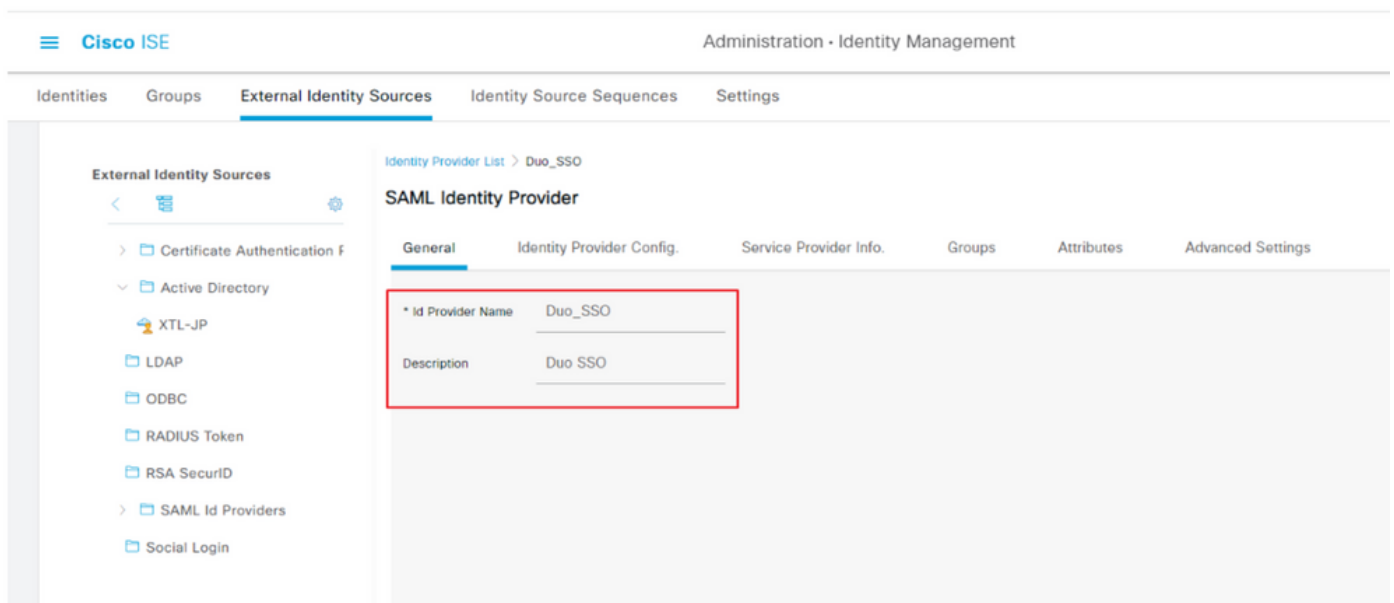
Configura integrazione SAML SSO con Duo SSO

Passaggio 1. Configurazione di SAML IdP su ISE

Configurazione di Duo SSO come origine di identità SAML esterna

Ad ISE, selezionare Administration > Identity Management > External Identity Sources > SAML Id Providers e fare clic sul pulsante **Add**.

Immettere il nome dell'IdP e fare clic su **Submit** (Invia) per salvarlo. Il nome del provider di identità è significativo solo per ISE, come mostrato nell'immagine:



Importare il file XML dei metadati SAML dal portale di amministrazione Duo

Ad ISE, selezionare Administration > Identity Management > External Identity Sources > SAML Id Providers. > Choose the SAML IdP you created (Scegli l'ID SAML creato), fare clic sul Identity Provider Configuration nome e quindi sul pulsante **Choose File** (Scegli file).

Scegliere il file **SSO IDP Metadata XML** esportato dal portale Duo Admin e fare clic su **Apri** per salvarlo. (questo passaggio è menzionato anche nella sezione Duo del presente documento).

L'URL SSO e i certificati di firma sono:

The screenshot shows the Cisco ISE Administration interface for Identity Management. The left sidebar lists 'External Identity Sources' with options like Certificate Authentication, Active Directory, LDAP, ODBC, RADIUS Token, RSA SecurID, SAML Id Providers, Azure, Duo_SSO, and Social Login. The main content area is titled 'SAML Identity Provider' and has tabs for 'General', 'Identity Provider Config.', 'Service Provider Info.', 'Groups', 'Attributes', and 'Advanced Settings'. The 'Identity Provider Config.' tab is active, showing an 'Identity Provider Configuration' section with a 'Choose File' button for importing a config file. Below this, the 'Single Sign On URL' is set to 'https://sso-19aa14ff.sso.duosecurity.com/saml2/sp/DIZA6IV4RE8UN8X5ADU6/sso'. The 'Single Sign Out URL (Post)' is 'Not supported by Identity Provider.'. A 'SAML Certificates' table is also visible with columns for Subject, Issuer, Valid From, Valid To, and Serial Number.

Configura metodo di autenticazione ISE

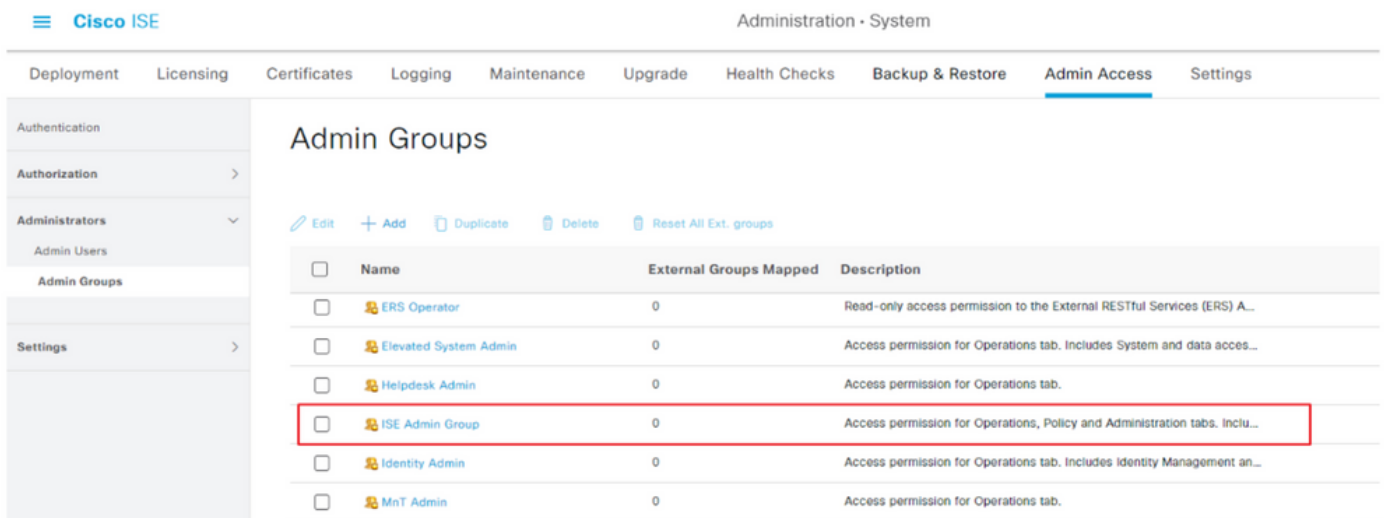
Individuare Administration > System > Admin Access > Authentication > Authentication Method e scegliere il pulsante di opzione Basato su password. Scegliere il Nome IdP richiesto creato in precedenza dall'elenco a discesa Origine identità come mostrato nell'immagine:

The screenshot shows the Cisco ISE Administration interface for System > Admin Access > Authentication > Authentication Method. The left sidebar shows 'Authentication', 'Authorization', 'Administrators', and 'Settings'. The main content area has tabs for 'Authentication Method', 'Password Policy', 'Account Disable Policy', and 'Lock/Suspend Settings'. The 'Authentication Method' tab is active, showing 'Authentication Type' with two radio button options: 'Password Based' (selected) and 'Client Certificate Based'. Below the radio buttons is an 'Identity Source' dropdown menu with 'SAML:Duo_SSO' selected.

Crea un gruppo amministrativo

Individuare Administration > System > Admin Access > Authentication > Administrators > Admin Group e fare clic su **Amministratore privilegiato** e quindi sul pulsante **Duplica**. Immettere il **nome del gruppo Amministratori** e fare clic sul pulsante **Invia**.

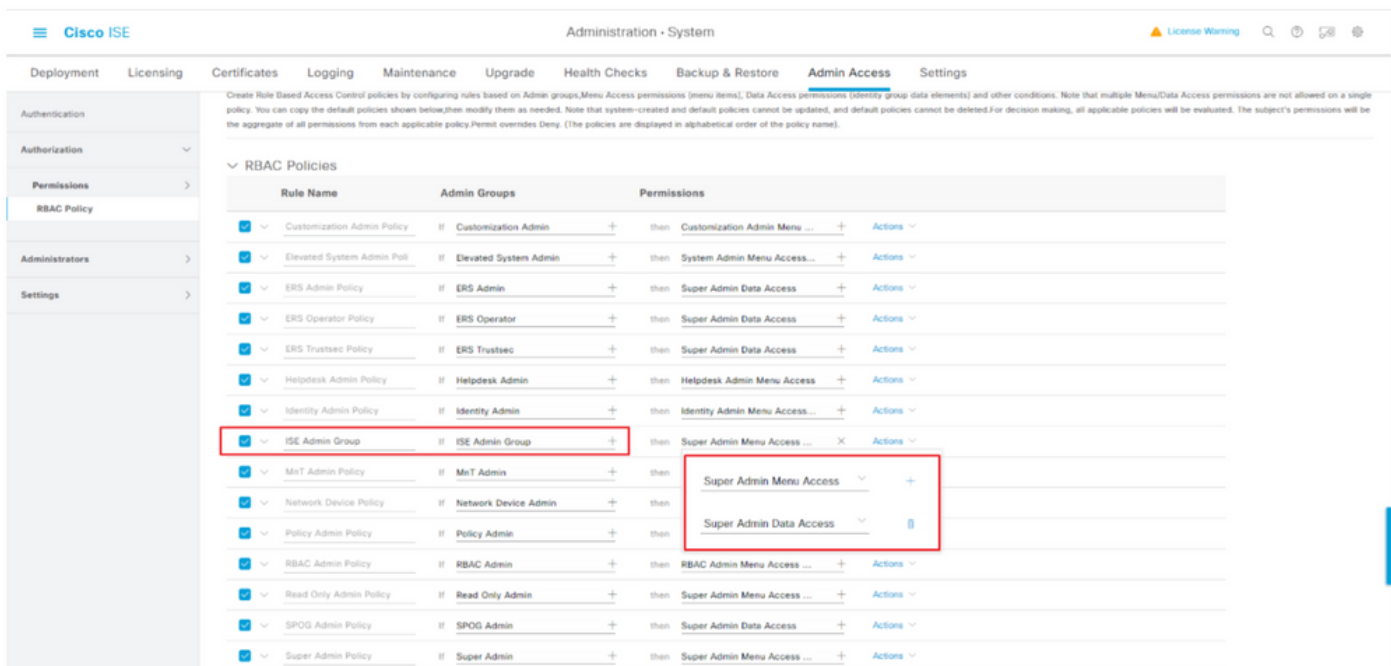
In questo modo vengono forniti i privilegi di amministratore privilegiato al gruppo Admin.



Creare un criterio RBAC per il gruppo Admin

Individuare Administration > System > Admin Access > Authorization > RBAC Policy e scegliere le **azioni** corrispondenti al **criterio di amministrazione avanzato**. Fare clic su .Duplicate > Add the Name field > Save

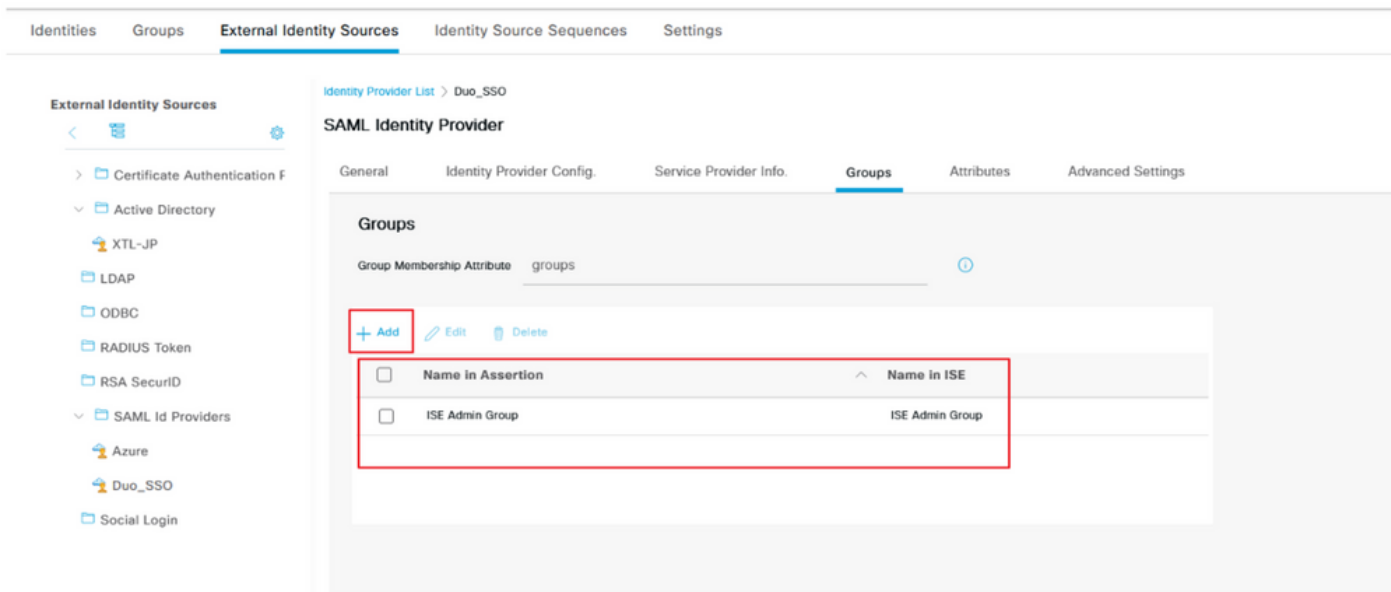
Le autorizzazioni per l'accesso sono le stesse del criterio di amministrazione avanzato.



Aggiungi appartenenza a gruppi

Ad ISE, selezionare Administration > Identity Management > External Identity Sources > SAML Id Providers e scegliere l'IdP SAML creato. Fare clic su **Gruppi**, quindi sul pulsante Aggiungi.

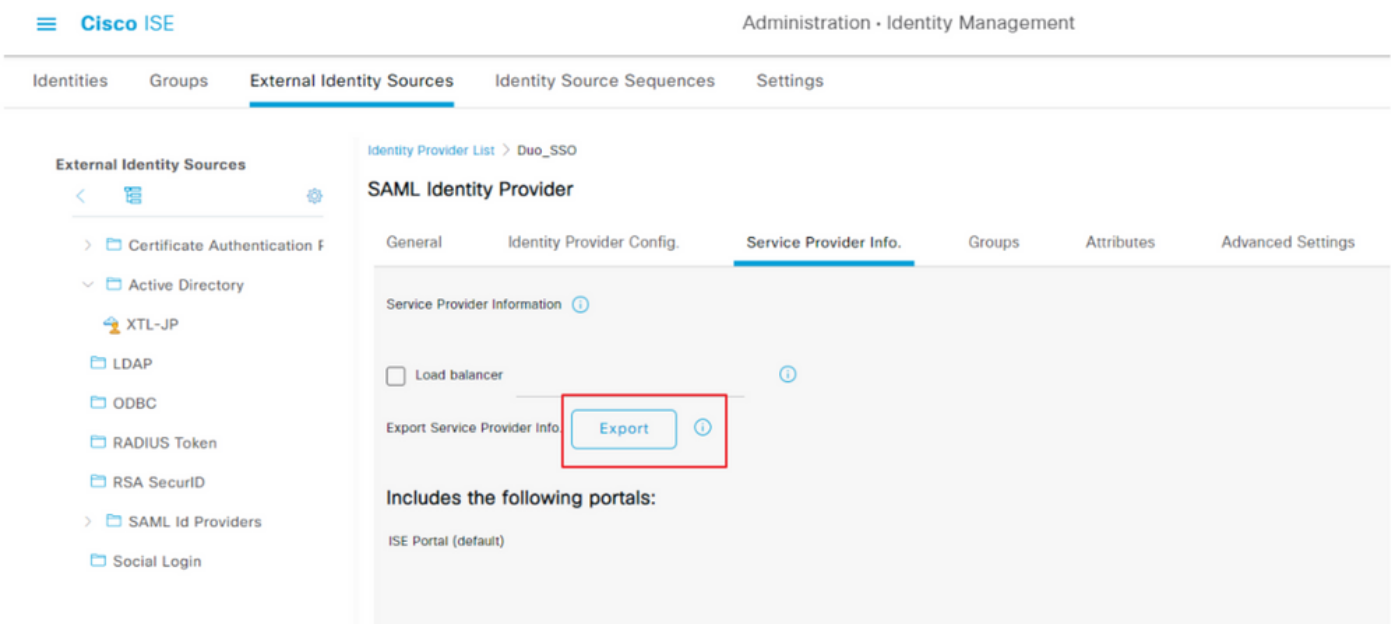
Aggiungere il nome in Asserzione (nome del gruppo ISE Admin) e dall'elenco a discesa scegliere il gruppo RBAC (Role-Based Access Control) creato (Passaggio 4.) e fare clic su **Apri** per salvarlo. L'URL SSO e i certificati di firma vengono popolati automaticamente:



Esporta informazioni SP

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

Passare alla scheda Informazioni SP e fare clic sul pulsante **Esporta**, come mostrato nell'immagine:



Scaricare il file.xml e salvarlo. AssertionConsumerService Prendere nota del valore Location URL (URL percorso) e **entityID (ID entità)**, in quanto questi dettagli sono richiesti nel portale Duo SSO.

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

Di seguito sono riportati i dettagli/attributi di interesse raccolti dal metafilere che devono essere configurati in Duo Generic SAML Integration

entityID = <http://CiscoISE/7fdcf239-631e-439c-a3ab-f5e56429779d>.

Posizione AssertionConsumerService = <https://10.x.x.x:8443/portal/SSOLoginResponse.action> dove 10.x.x.x è l'indirizzo IP ISE trovato nel file XML (Posizione).

AssertionConsumerService Location = <https://isenodename.com:8443/portal/SSOLoginResponse.action> dove isenodename è il nome FQDN ISE effettivo trovato nel file XML (Location).

Passaggio 2. Configurare Duo SSO per ISE

Selezionare questa [KB](#) per configurare Duo SSO con AD come origine di autenticazione.

Configured Authentication Sources

[+ Add source](#)

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

Selezionare questa [KB](#) per abilitare l'SSO con il dominio personalizzato.

Single Sign-On

1 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.

[Create a custom subdomain](#)

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 .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.

[Save and continue](#) [Complete later](#)

Passaggio 3. Integrazione di Cisco ISE con Duo SSO come SP generico

Controllare i passaggi 1 e 2 di questo [KB](#) per integrare Cisco ISE con Duo SSO come SP generico.

Configurare i dettagli dell'SP Cisco ISE nel pannello di amministrazione Duo per l'SP generico:

Nome	Descrizione
ID entità	http://CiscoISE/7fdcf239-631e-439c-a3ab-f5e56429779d
URL Assertion Consumer Service (ACS)	https://10.x.x.x:8443/portal/SSOLoginResponse.action

Service Provider

Entity ID *

<http://CiscoISE/7fdcf239-631e-439c-a3ab-f5e56429779d>

The unique identifier of the service provider.

Assertion Consumer Service (ACS) URL *

<https://10.52.14.44:8443/portal/SSOLoginResponse.action>

Configurare la risposta SAML per Cisco ISE:

Nome	Descrizione
Formato NameID	urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified
attributo NameID	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>.

Creare un gruppo denominato Cisco Admin Group nel pannello Duo Admin e aggiungere gli utenti ISE a questo gruppo oppure creare un gruppo in Windows AD e sincronizzare lo stesso con il pannello Duo Admin utilizzando la funzionalità di sincronizzazione della directory.

Configurare gli attributi del ruolo per Cisco ISE:

Nome	Descrizione
Nome attributo	gruppi
Ruolo SP	ISE Admin Group
Gruppi Duo	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

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

Service Provider's Role **Duo groups**

Nella sezione Impostazioni specificare un nome appropriato nella scheda **Nome** per l'integrazione.

Settings

Type Generic Service Provider - Single Sign-On

Name

Duo Push users will see this when approving transactions.

Fare clic sul pulsante **Save** (Salva) per salvare la configurazione e consultare questa [KB](#) per ulteriori dettagli.

Per scaricare i metadati SAML, fare clic su **Download XML**.

Downloads

Certificate

[Download certificate](#)

Expires: 01-19-2038

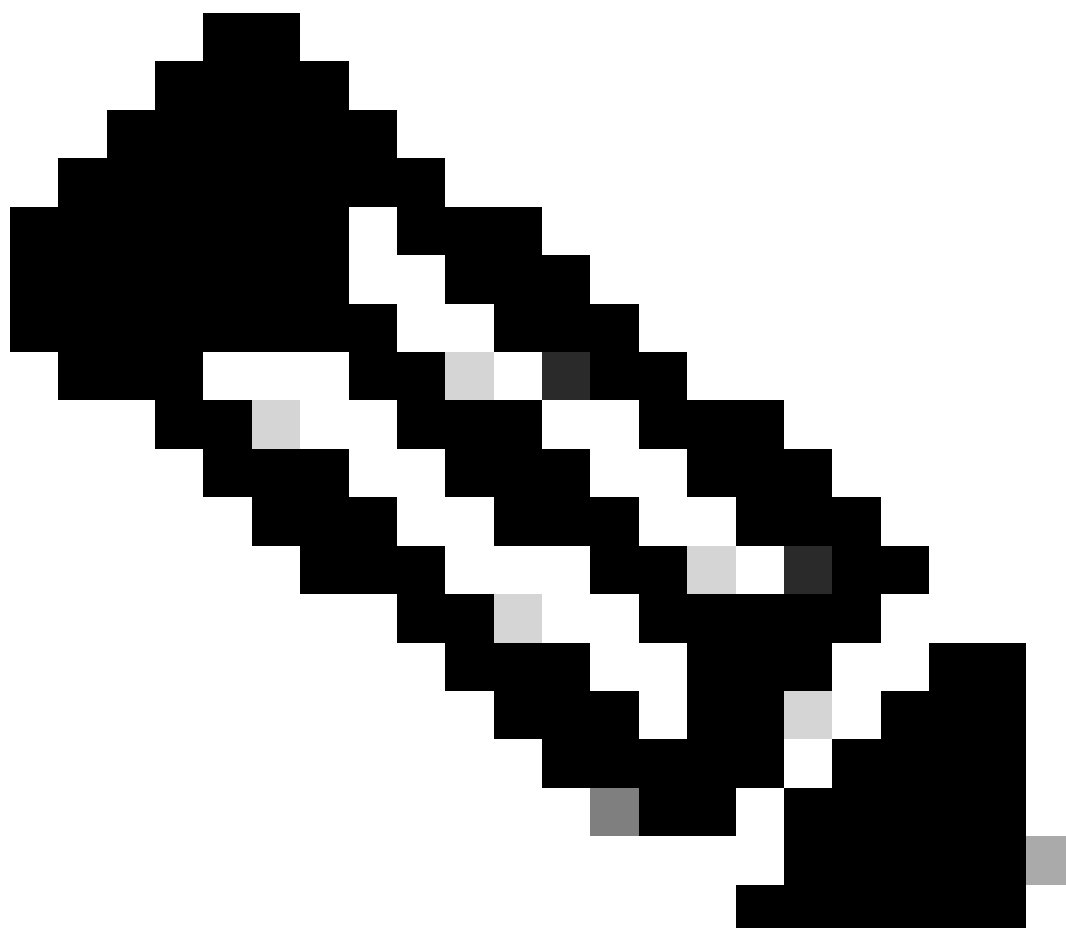
SAML Metadata

[Download XML](#)

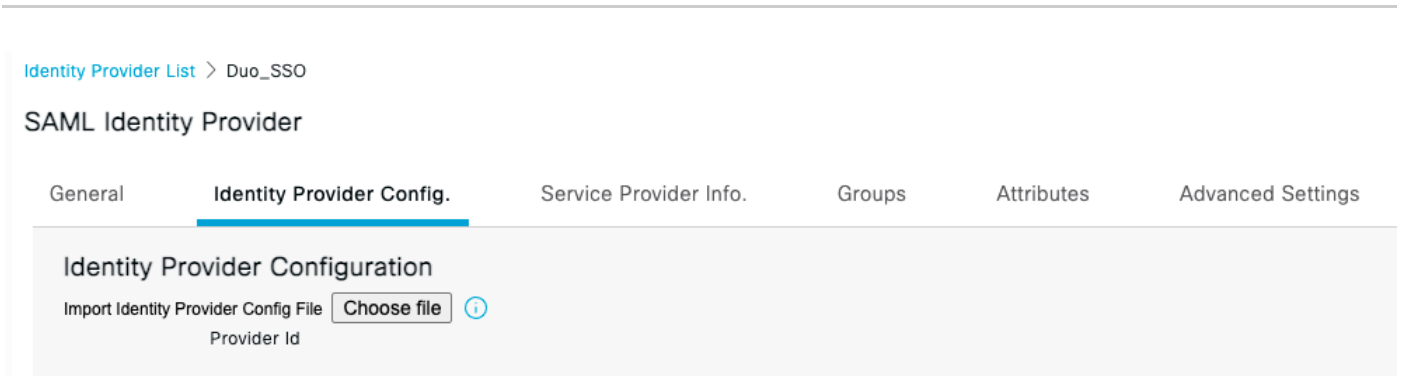
Caricare i metadati SAML dal pannello di amministrazione Duo a Cisco ISE passando a Administration > Identity Management > External Identity Sources > SAML Id Providers > Duo_SSO.

Passare alla scheda **Configurazione provider di identità** e fare clic sul pulsante **Scegli file**.

Scegliere il file **XML dei metadati** scaricato nel passaggio 8 e fare clic su **Salva**.



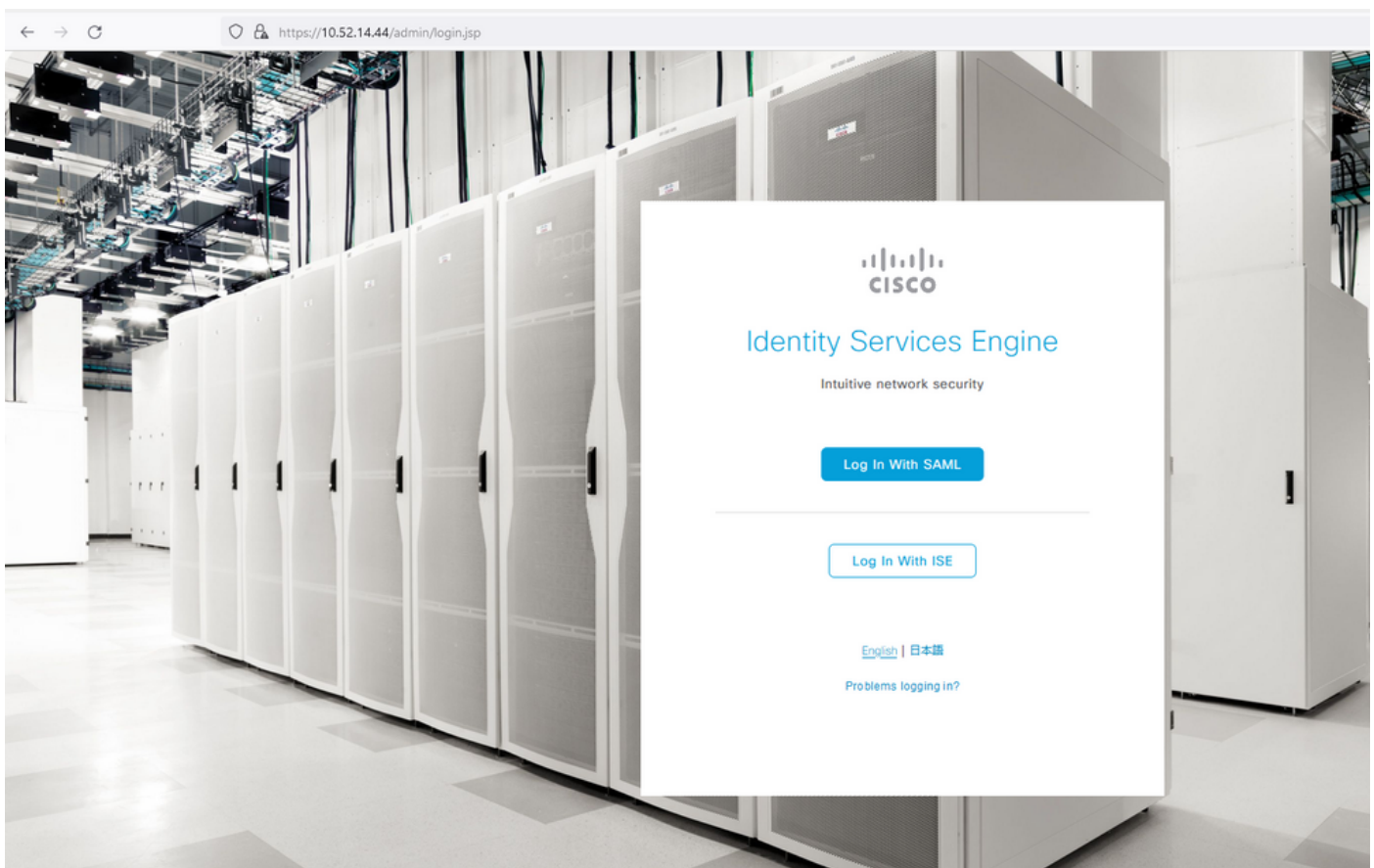
Nota: questo passaggio è menzionato nella sezione Configurazione dell'integrazione di SAML SSO con Duo SSO; passaggio 2. Importare il file **SAML Metadata XML** dal portale Duo Admin.



Verifica

Test dell'integrazione con Duo SSO

1. Accedere al **pannello di amministrazione di Cisco ISE** e fare clic su **Log In With SAML**.

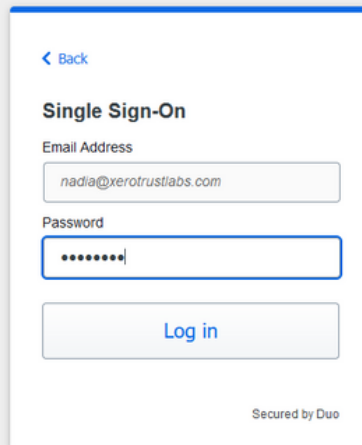


2. Reindirizzato alla pagina SSO, immettere l'**indirizzo e-mail** e fare clic su **Avanti**.



The image shows a web browser window displaying a Cisco Single Sign-On page. At the top left is the Cisco logo. Below it, the text "Single Sign-On" is displayed. Underneath, there is a label "Email Address" followed by a text input field containing the email address "nadia@zerotrustlabs.com". Below the input field is a button labeled "Next". At the bottom right of the form, it says "Secured by Duo".

3. Inserire la password e fare clic su **Log in**.



The image shows a web browser window displaying a Cisco Single Sign-On page. At the top left is a blue back arrow icon labeled "Back". Below it, the text "Single Sign-On" is displayed. Underneath, there is a label "Email Address" followed by a text input field containing the email address "nadia@zerotrustlabs.com". Below that is a label "Password" followed by a password input field with masked characters "••••••••". Below the password field is a button labeled "Log in". At the bottom right of the form, it says "Secured by Duo".

4. Viene visualizzato il prompt Duo Push sul dispositivo mobile.

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)



[Other options](#)

[Need help?](#)

Secured by Duo

5. Una volta accettata la richiesta, si apre una finestra e si viene automaticamente reindirizzati alla pagina ISE Admin.

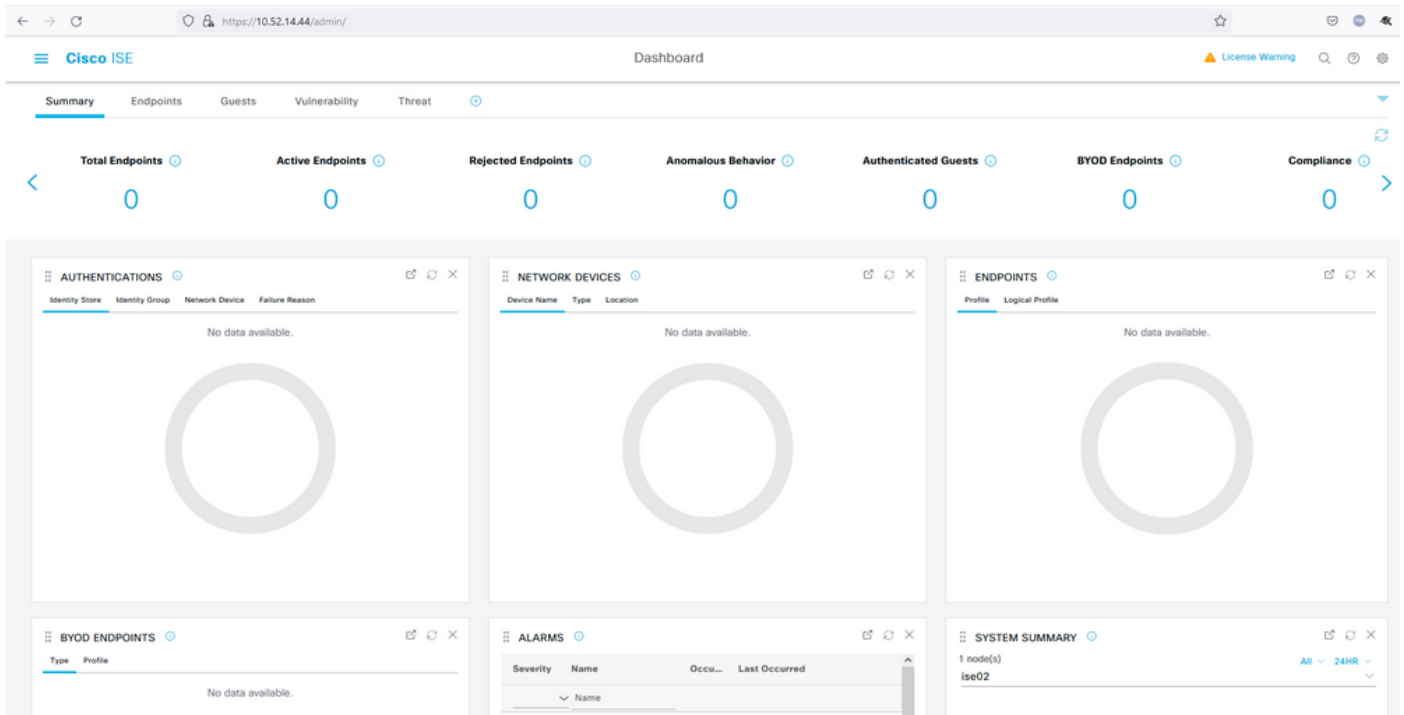


Success!

Logging you in...



Secured by Duo



Risoluzione dei problemi

- Scaricare l'estensione del tracer SAML per Mozilla FF <https://addons.mozilla.org/en-US/firefox/addon/saml-tracer/>.
- Scorrere fino al SSOLoginResponse.action pacchetto. Nella scheda **SAML** vengono visualizzati alcuni attributi inviati da Duo SAML: NameID, Recipient (AssertionConsumerService Location URL) e Audience(EntityID).

Steps

5231 Guest Authentication Passed

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

- Accesso amministrativo ad ISE: username: samlUser.

- Export Summary
- My Reports
- Reports
- Audit
 - Adaptive Network Control
 - Administrator Logins
 - Change Configuration Audit
 - Cisco Support Diagnostics
 - Data Purging Audit
 - Endpoint Purge Activities
 - Internal Administrator Sum...
 - Policy OpenAPI Operations
 - Operations Audit
 - psGrid Administrator Audit
 - Secure Communications A...
 - TrustSec Audit
 - User Change Password Au...
- Device Administration
- Diagnostics
- Endpoints and Users
- Guest
- Threat Control NAC
- TrustSec
- Scheduled Reports

Administrator Logins

From 2021-11-28 00:00:00 To 2021-11-28 18:38:10

Reports reported in last 7 days

Add to My Reports Export To Schedule

Logged At	Administrator	IP Address	Server	Event	Event Details
Today	Administrator		Server		
2021-11-28 18:38:08.199		10.65.48.163	16402	Administrator authentication succeeded	Administrator authentication successful

Rows/Page 1 1 Total Rows

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).