

Configure o login do administrador da GUI do ISE 3.1 usando a integração SAML com o Duo SSO e o Windows AD

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Provedor de identidade \(IdP\)](#)

[Provedor de serviços \(SP\)](#)

[SAML](#)

[Asserção SAML](#)

[Diagrama de fluxo de alto nível](#)

[Configurar a Integração de SSO SAML com SSO Duo](#)

[Etapa 1. Configurar SAML IdP no ISE](#)

[Configurar o SSO Duo como uma fonte de identidade SAML externa](#)

[Importar o arquivo XML de metadados SAML do Duo Admin Portal](#)

[Configurar o método de autenticação do ISE](#)

[Criar um grupo de administradores](#)

[Criar uma Política RBAC para o Grupo Admin](#)

[Adicionar participação em grupos](#)

[Exportar informações da controladora](#)

[Etapa 2. Configurar o SSO Duo para ISE](#)

[Etapa 3. Integrar o Cisco ISE com o SSO Duo como um SP genérico](#)

[Verificar](#)

[Testando a integração com o SSO Duo](#)

[Troubleshooting](#)

Introdução

Este documento descreve como configurar a integração do Cisco ISE 3.1 SAML SSO com um provedor de identidade externo como o Cisco Duo SSO.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Cisco Identity Services Engine (ISE) 3.1
- Conhecimento básico sobre implantações de Security Assertion Markup Language (SAML) Single Sign-On (SSO) (SAML 1.1)
- Conhecimento do Cisco DUO SSO
- Conhecimento do Windows Active Directory

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

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

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

Provedor de identidade (IdP)

É o SSO Duo, neste caso, que verifica e declara uma identidade de usuário e privilégios de acesso a um recurso solicitado (o 'Provedor de serviços').

Duo SSO atua como um IdP, autenticando seus usuários usando o Active Directory (AD) local existente com SAML 1.1 ou qualquer SAML 2.0 IdP (por exemplo, Microsoft Azure) e solicitando autenticação de dois fatores antes de permitir o acesso ao aplicativo do provedor de serviços.

Ao configurar um aplicativo para ser protegido com o Duo SSO, você deve enviar atributos do Duo SSO para o aplicativo. O Active Directory funciona sem configuração adicional, mas se você usou um SAML(2.0) IdP como sua origem de autenticação, verifique se você o configurou para enviar os atributos SAML corretos.

Provedor de serviços (SP)

O recurso ou serviço hospedado que o usuário pretende acessar; neste caso, o servidor de aplicativos Cisco ISE.

SAML

O SAML é um padrão aberto que permite que o IdP passe credenciais de autorização para o SP.

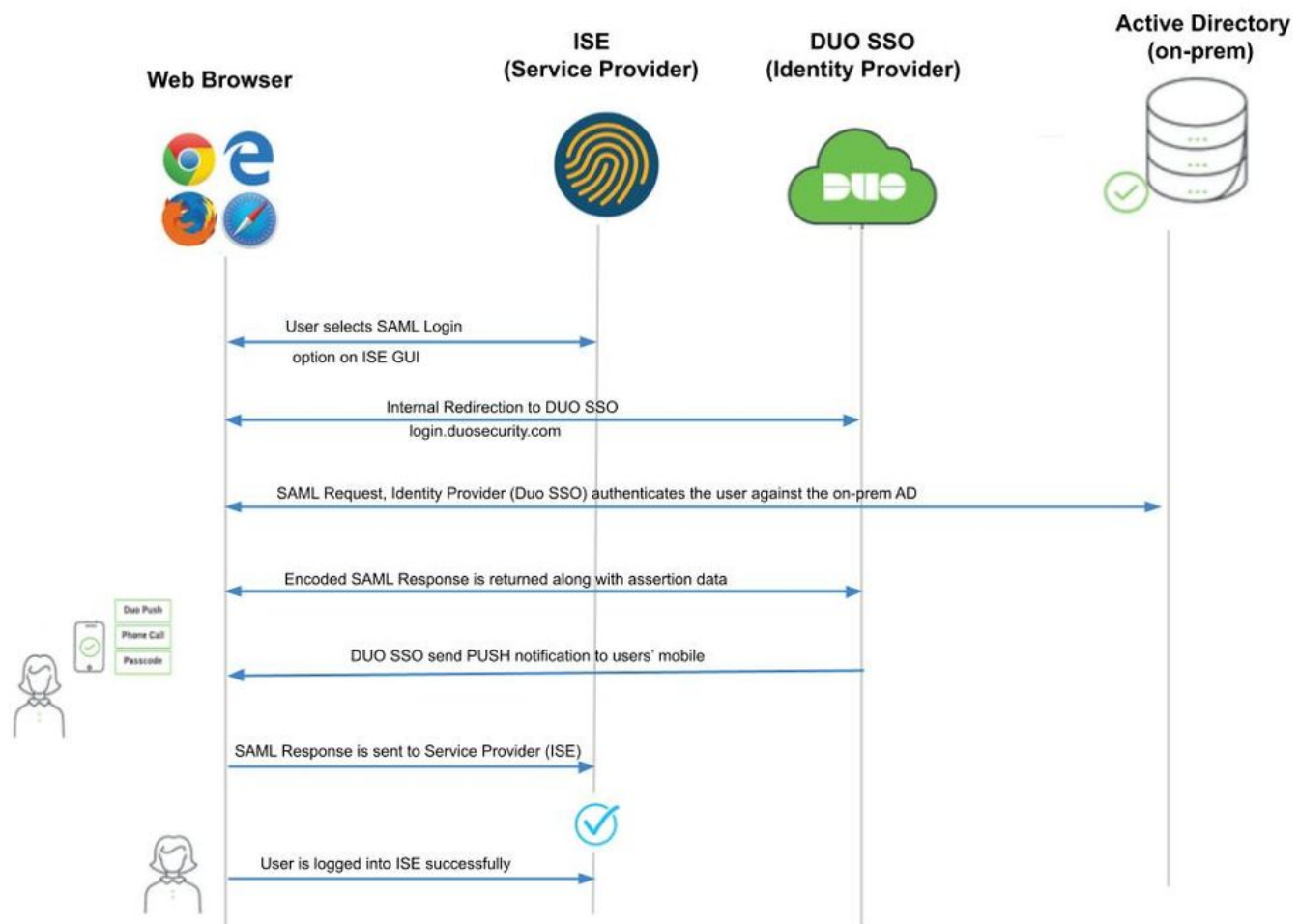
As transações SAML usam Extensible Markup Language (XML) para comunicações padronizadas entre o provedor de identidade e os provedores de serviços. O SAML é o link entre a autenticação da identidade do usuário e a autorização para usar um serviço.

Asserção SAML

Uma SAML Assertion é o documento XML que o IdP envia ao provedor de serviços que contém a autorização do usuário. Existem três tipos diferentes de Asserções SAML - autenticação, atributo e decisão de autorização.

- As asserções de autenticação comprovam a identificação do usuário e fornecem a hora em que o usuário se conectou e o método de autenticação usado (por exemplo, Kerberos, dois fatores, etc.).
- A asserção de atribuição passa os atributos SAML, pedaços específicos de dados que fornecem informações sobre o usuário, para o SP.
- Uma declaração de decisão de autorização declara se o usuário está autorizado a usar o serviço ou se o IdP negou sua solicitação devido a uma falha de senha ou à falta de direitos ao serviço.

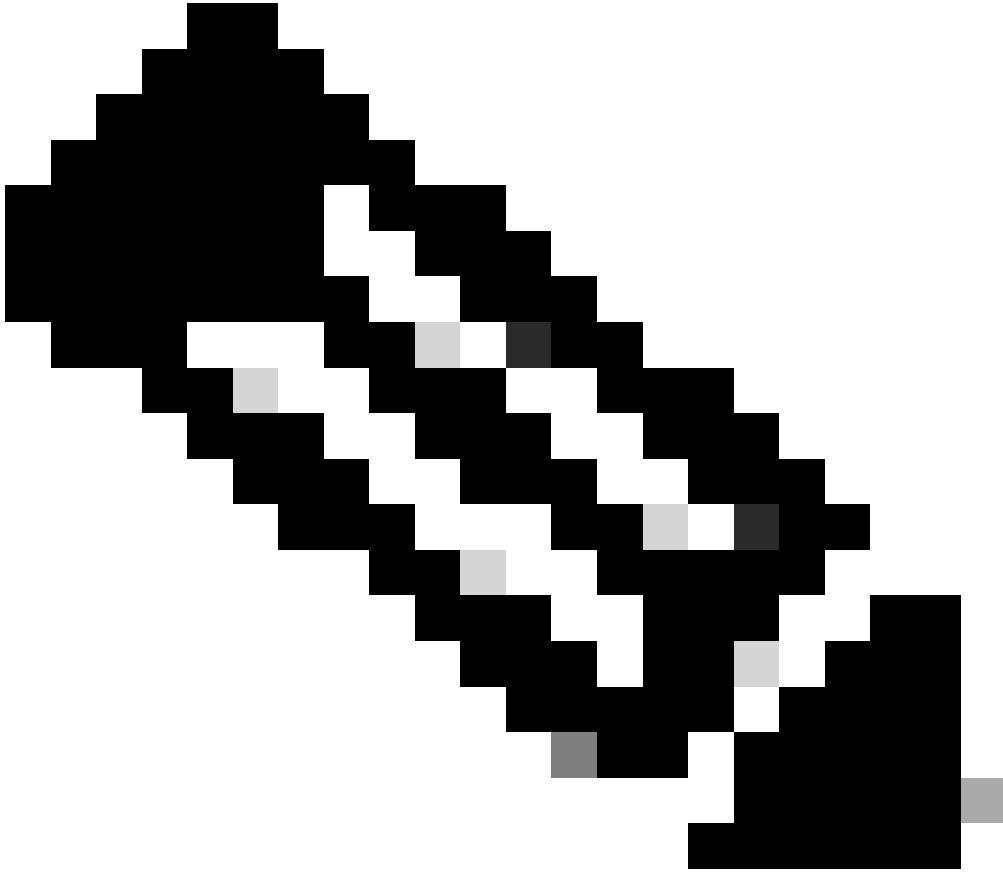
Diagrama de fluxo de alto nível



Fluxo:

1. O usuário faz login no ISE usando a opção Login via SAML.

2. O ISE (SAML SP) redireciona o navegador do usuário para o Duo SSO com uma mensagem de solicitação SAML.
-



Observação: em um ambiente distribuído, você pode obter um erro de certificado inválido e a Etapa 3. pode agora funcionar. Portanto, para um ambiente distribuído, a Etapa 2. difere um pouco dessa forma:

Problema: o ISE redireciona temporariamente para o portal de um dos nós PSN (na porta 8443).

Solução: para garantir que o ISE apresente o mesmo certificado que o certificado da GUI do administrador, certifique-se de que o certificado do sistema confiável seja válido para uso do portal também em todos os nós PSN.

-
3. O usuário faz logon com credenciais principais do AD.
 4. O SSO Duo encaminha isso para o AD, que retorna uma resposta para o SSO Duo.
 5. O SSO Duo exige que o usuário conclua a autenticação de dois fatores enviando um PUSH no celular.
 6. O usuário conclui a autenticação de dois fatores do Duo.
 7. Duo SSO redireciona o navegador do usuário para a controladora de armazenamento SAML

com uma mensagem de resposta.

8. O usuário agora pode fazer login no ISE.

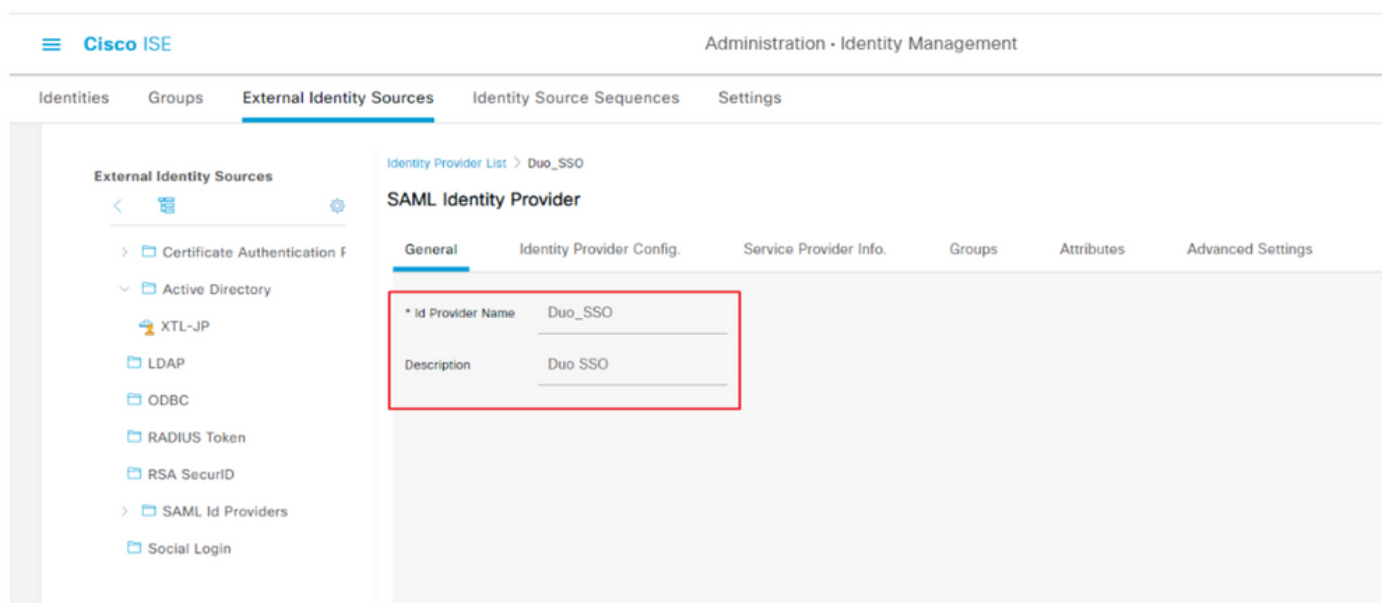
Configurar a Integração de SSO SAML com SSO Duo

Etapa 1. Configurar SAML IdP no ISE

Configurar o SSO Duo como uma fonte de identidade SAML externa

No ISE, navegue até **Administration > Identity Management > External Identity Sources > SAML Id Providers** e clique no botão **Adicionar**.

Insira o nome do IdP e clique em **Submit** para salvá-lo. O nome do IdP é significativo apenas para o ISE, como mostrado na imagem:



Importar o arquivo XML de metadados SAML do Duo Admin Portal

No ISE, navegue para **Administration > Identity Management > External Identity Sources > SAML Id Providers**. > Escolher o SAML IdP que você criou, clique no botão **Identity Provider Configuration** e, em seguida, no botão **Escolher arquivo**.

Escolha o arquivo **SSO IDP Metadata XML** exportado do portal Duo Admin e clique em **Open** para salvá-lo. (Esta etapa também é mencionada na seção Duo deste documento.)

O URL do SSO e os Certificados de Autenticação são:

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. Below this, there are fields for 'Single Sign On URL' (https://sso-19aa14ff.sso.duosecurity.com/saml2/sp/DIZA6IV4RE8UN8X5ADU6/sso) and 'Single Sign Out URL (Post)'. A 'SAML Certificates' table is also visible with columns for Subject, Issuer, Valid From, Valid To (Expires), and Serial Number.

Configurar o método de autenticação do ISE

Navegue até Administration > System > Admin Access > Authentication > Authentication Method e escolha o botão de opção Baseado em Senha. Escolha o Nome do IdP necessário criado anteriormente na lista suspensa Origem da identidade, conforme mostrado na imagem:

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 this is a dropdown menu for '* Identity Source' with 'SAML:Duo_SSO' selected.

Criar um grupo de administradores

Navegue até Administration > System > Admin Access > Authentication > Administrators > Admin Group e clique no botão **Super Admin** e depois no botão Duplicate. Insira o **Admin group Name** e clique no botão **Submit**.

Fornecer privilégios de Super Admin para o grupo Admin.

Cisco ISE Administration - System

Deployment Licensing Certificates Logging Maintenance Upgrade Health Checks Backup & Restore **Admin Access** Settings

Authentication

Authorization >

Administrators >

Admin Users

Admin Groups

Settings >

Admin Groups

[Edit](#) [+ Add](#) [Duplicate](#) [Delete](#) [Reset All Ext. groups](#)

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

Criar uma Política RBAC para o Grupo Admin

Navegue até Administration > System > Admin Access > Authorization > RBAC Policy e escolha as **Ações** correspondentes à Política de Super Admin. Clique em Duplicate > Add the Name field > Save.

As permissões de acesso são as mesmas da política de Super Admin.

Cisco ISE Administration - System License Warning

Deployment Licensing Certificates Logging Maintenance Upgrade Health Checks Backup & Restore **Admin Access** Settings

Authentication

Authorization >

Permissions >

RBAC Policy

Administrators >

Settings >

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).

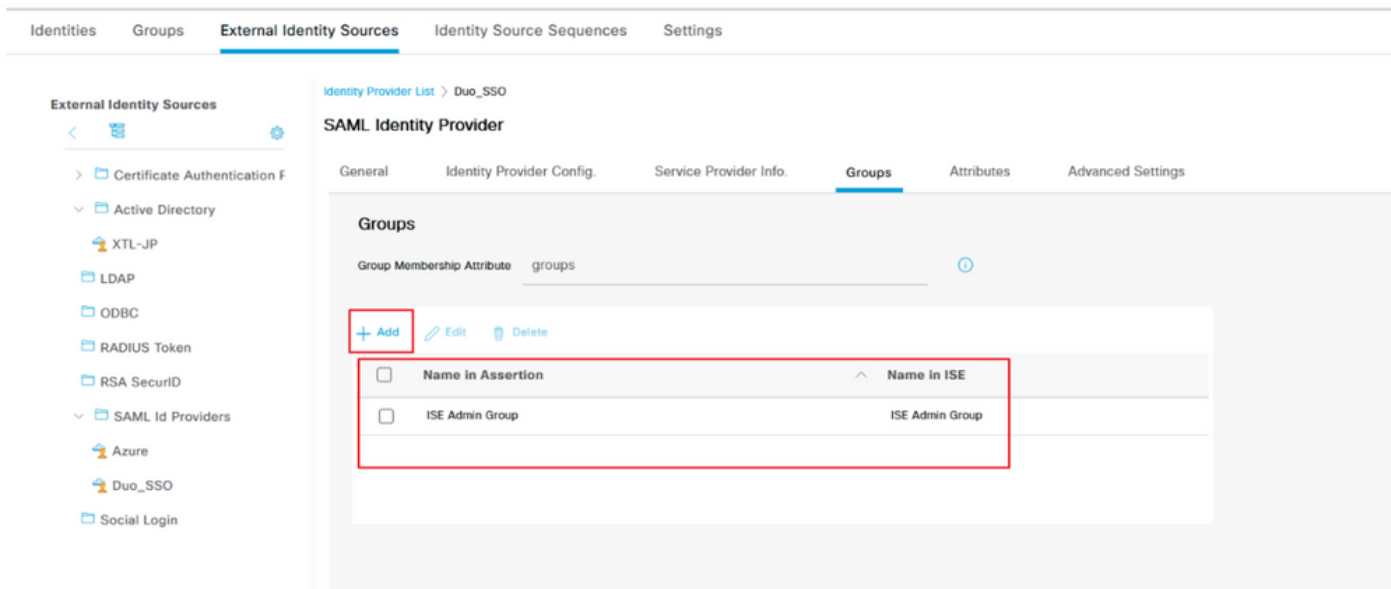
RBAC Policies

Rule Name	Admin Groups	Permissions
<input checked="" type="checkbox"/> Customization Admin Policy	Customization Admin	Customization Admin Menu ...
<input checked="" type="checkbox"/> Elevated System Admin Pol...	Elevated System Admin	System Admin Menu Access...
<input checked="" type="checkbox"/> ERS Admin Policy	ERS Admin	Super Admin Data Access
<input checked="" type="checkbox"/> ERS Operator Policy	ERS Operator	Super Admin Data Access
<input checked="" type="checkbox"/> ERS Trustee Policy	ERS Trustee	Super Admin Data Access
<input checked="" type="checkbox"/> Helpdesk Admin Policy	Helpdesk Admin	Helpdesk Admin Menu Access
<input checked="" type="checkbox"/> Identity Admin Policy	Identity Admin	Identity Admin Menu Access...
<input checked="" type="checkbox"/> ISE Admin Group	ISE Admin Group	Super Admin Menu Access ...
<input checked="" type="checkbox"/> MnT Admin Policy	MnT Admin	Super Admin Menu Access
<input checked="" type="checkbox"/> Network Device Policy	Network Device Admin	Super Admin Data Access
<input checked="" type="checkbox"/> Policy Admin Policy	Policy Admin	RBAC Admin Menu Access ...
<input checked="" type="checkbox"/> RBAC Admin Policy	RBAC Admin	RBAC Admin Menu Access ...
<input checked="" type="checkbox"/> Read Only Admin Policy	Read Only Admin	Super Admin Menu Access ...
<input checked="" type="checkbox"/> SPOG Admin Policy	SPOG Admin	Super Admin Data Access
<input checked="" type="checkbox"/> Super Admin Policy	Super Admin	Super Admin Menu Access ...

Adicionar participação em grupos

No ISE, navegue até Administration > Identity Management > External Identity Sources > SAML Id Providers e escolha o SAML IdP que você criou. Clique em **Groups** e, em seguida, no botão Add.

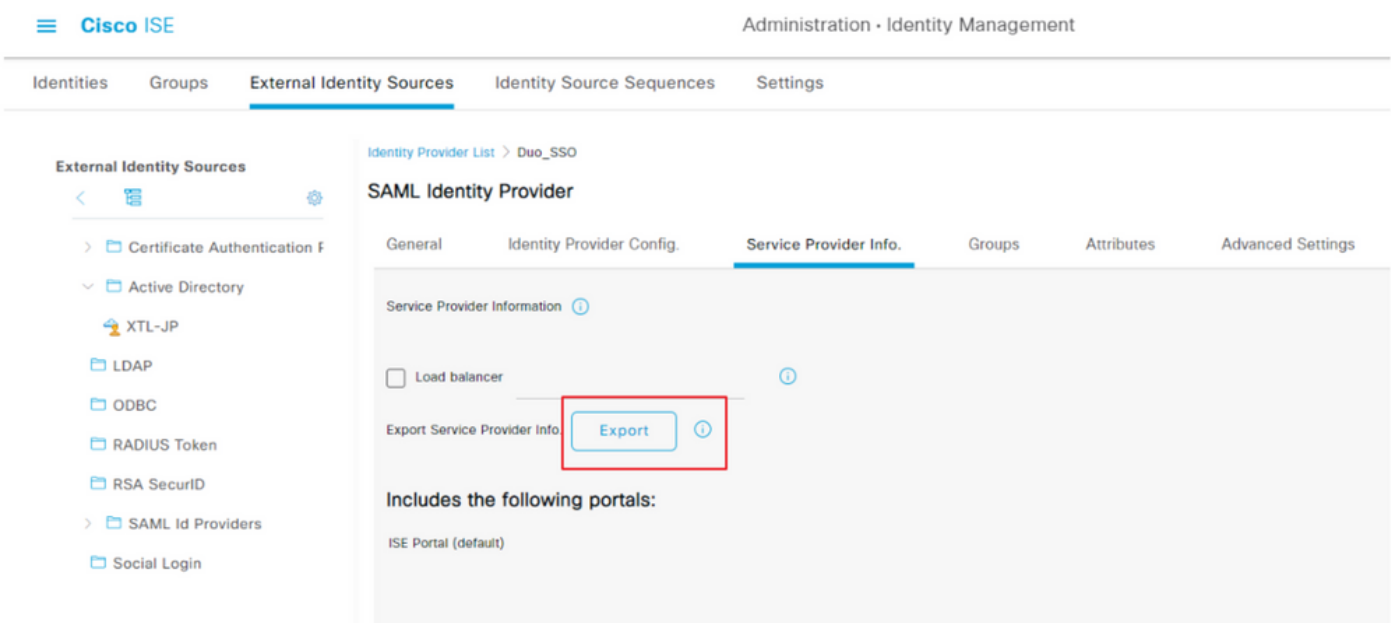
Adicione o nome em Asserção (nome do grupo de administradores do ISE) e, no menu suspenso, escolha o grupo de controle de acesso baseado em função (RBAC) criado (Etapa 4) e clique em **Abrir** para salvá-lo. O URL do SSO e os Certificados de Autenticação são preenchidos automaticamente:



Exportar informações da controladora

Navegue até Administration > Identity Management > External Identity Sources > SAML Id Providers > (Your SAML Provider) .

Altere a guia para SP Info. e clique no botão **Export**, conforme mostrado na imagem:



Faça o download do arquivo.xml e salve-o. Anote o URL do localAssertionConsumerService e o valor **entityID**, pois esses detalhes são necessários no Portal Duo SSO.

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

Aqui estão os detalhes/atributos de interesse reunidos a partir do meta arquivo que precisa ser configurado na Integração SAML Genérica Duo

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

AssertionConsumerService Location = <https://10.x.x.x:8443/portal/SSOLoginResponse.action> onde 10.x.x.x é o IP do ISE encontrado no arquivo XML (Location).

AssertionConsumerService Location = <https://isenodename.com:8443/portal/SSOLoginResponse.action> onde isenodename é o nome real do FQDN do ISE encontrado no arquivo XML (Location).

Etapa 2. Configurar o SSO Duo para ISE

Verifique este [KB](#) para configurar o SSO Duo com AD como uma Origem de autenticação.

Configured Authentication Sources

[+ Add source](#)

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

Verifique este [KB](#) para habilitar o SSO com seu domínio personalizado.

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](#)

Etapa 3. Integrar o Cisco ISE com o SSO Duo como um SP genérico

Verifique as Etapas 1 e 2 deste [KB](#) para integrar o Cisco ISE com o SSO Duo como um SP Genérico.

Configure os detalhes do SP do Cisco ISE no painel de administração do Duo para o SP genérico:

Nome	Descrição
ID da entidade	http://CiscoISE/7fdcf239-631e-439c-a3ab-f5e56429779d
URL do Serviço de Consumidor de Asserção (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>

Configurar resposta SAML para Cisco ISE:

Nome	Descrição
Formato NameID	urn:oasis:names:tc:SAML:1.1:nameid-format:não especificado
atributo NameID	Nome de usuário

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>.

Crie um grupo chamado Grupo de administração Cisco no painel de administração do Duo e adicione os usuários do ISE a esse grupo ou crie um grupo no Windows AD e sincronize o mesmo com o painel de administração do Duo usando o recurso de sincronização de diretório.

Search for users, groups, applications, or devices

Yasir Irfan US DC | ID: 0430-5768-95

Yasir Irfan

Dashboard > Groups

Groups

Add Group

Export

Search

Name	Status	Users	Description
ISE Admin Group	Active	3	

Configurar atributos de função para o Cisco ISE:

Nome	Descrição
Nome do atributo	grupos
Função SP	Grupo de administração do ISE
Grupos Duo	Grupo de administração do ISE

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



Na seção Configurações, forneça um nome apropriado na guia **Nome** para essa integração.

Settings

Type

Generic Service Provider - Single Sign-On

Name

Duo Push users will see this when approving transactions.

Clique no botão **Save** para salvar a configuração e consulte este [KB](#) para obter mais detalhes.

Clique em **Download XML** para baixar os Metadados SAML.

Downloads

Certificate

[Download certificate](#)

Expires: 01-19-2038

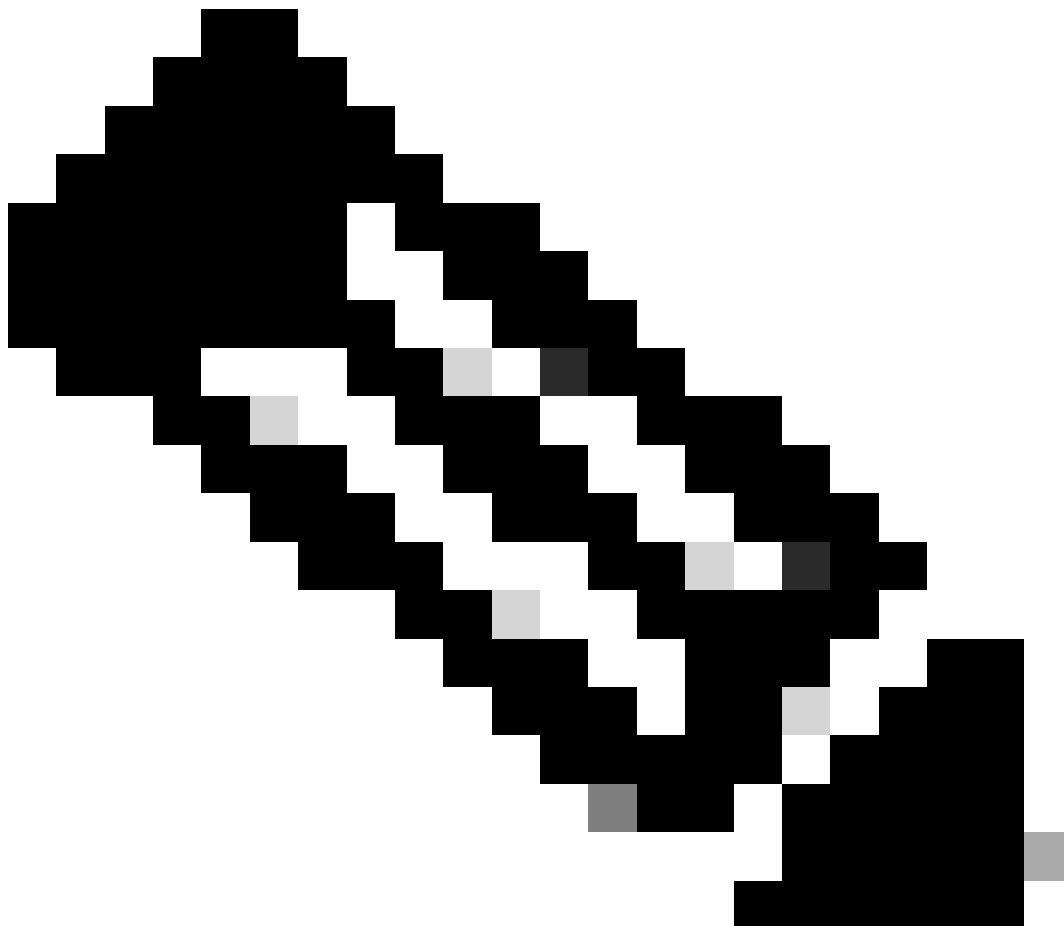
SAML Metadata

[Download XML](#)

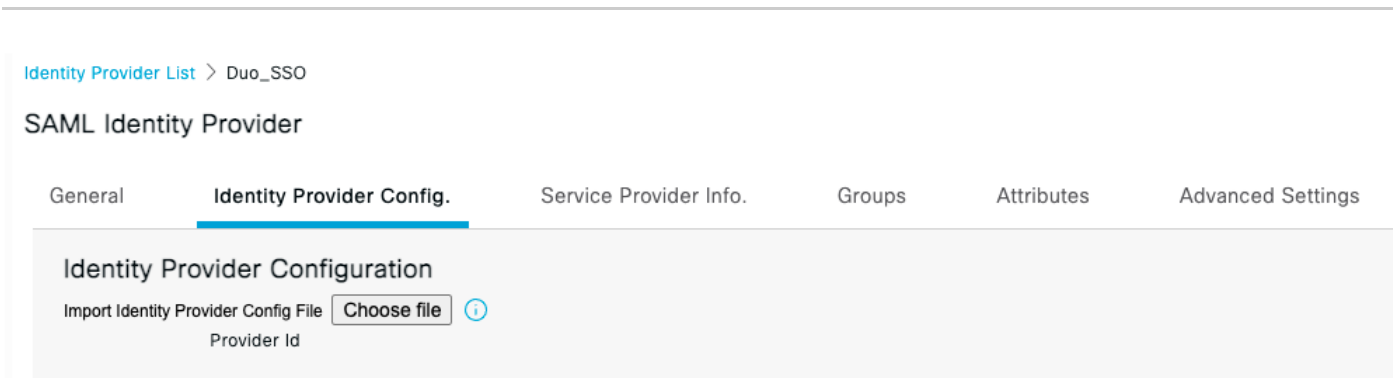
Faça o download de Metadados SAML do Painel de administração do Duo para o Cisco ISE navegando para Administration > Identity Management > External Identity Sources > SAML Id Providers > Duo_SSO.

Altere a guia para **Config. do provedor de identidade** e clique no botão **Escolher** arquivo.

Escolha o arquivo **Metadata XML** baixado na Etapa 8. e clique em **Save**.



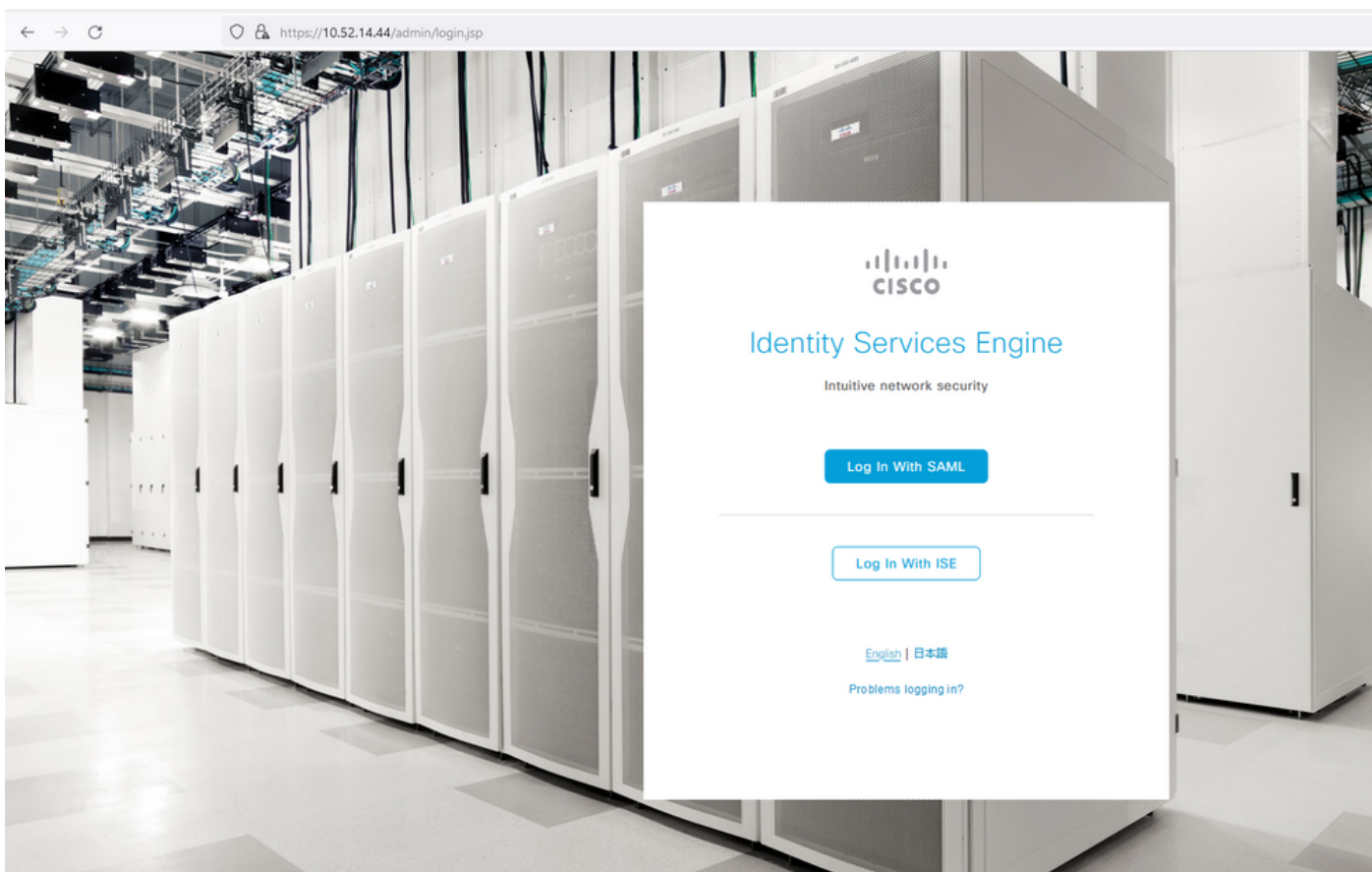
Observação: esta etapa é mencionada aqui na seção Configurar a Integração de SSO SAML com SSO Duo; Etapa 2. Importe o arquivo **SAML Metadata XML** do portal Duo Admin.



Verificar

Testando a integração com o SSO Duo

1. Faça login no **painel de administração do Cisco ISE** e clique em **Log In With SAML**.

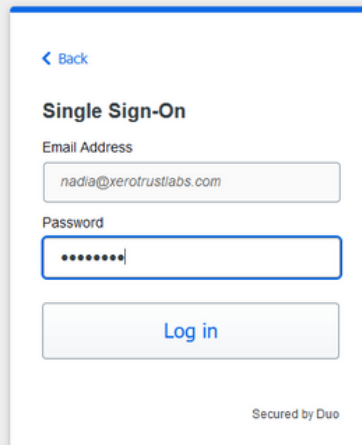


2. Redirecionado para a página SSO, informe o **Endereço de E-mail** e clique em **Próximo**.



The image shows a web browser window displaying a "Single Sign-On" form. At the top left of the form 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. Insira a senha e clique em **Login**.

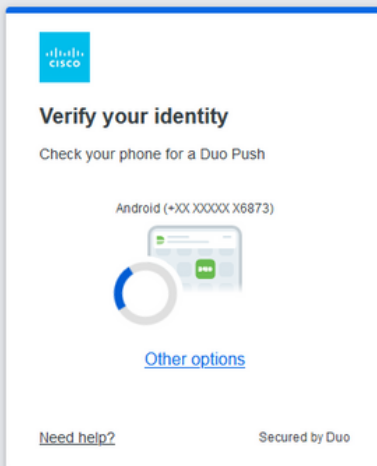


The image shows a web browser window displaying a "Single Sign-On" form. At the top left of the form is a blue arrow pointing left with the text "Back". Below it, the text "Single Sign-On" is displayed. Underneath, there is a label "Email Address" followed by a text input field containing the email address "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. Você recebe um prompt Duo Push no seu dispositivo móvel.

Duo needs your help

[Take a quick 6-question survey](#) to help us improve this experience.



The image shows a white rectangular box with a blue border, representing a Duo authentication prompt. At the top left is the Cisco Duo logo. The main heading is "Verify your identity" in bold. Below it, the text says "Check your phone for a Duo Push". A phone number is displayed: "Android (+XX XXXXX X6873)". In the center, there is a graphic of a smartphone with a green push notification icon and a blue circular progress indicator. Below the phone number is a blue link "Other options". At the bottom left is a link "Need help?" and at the bottom right is the text "Secured by Duo".

5. Depois de aceitar o prompt, você obterá uma janela e será redirecionado automaticamente para a página de administração do ISE.

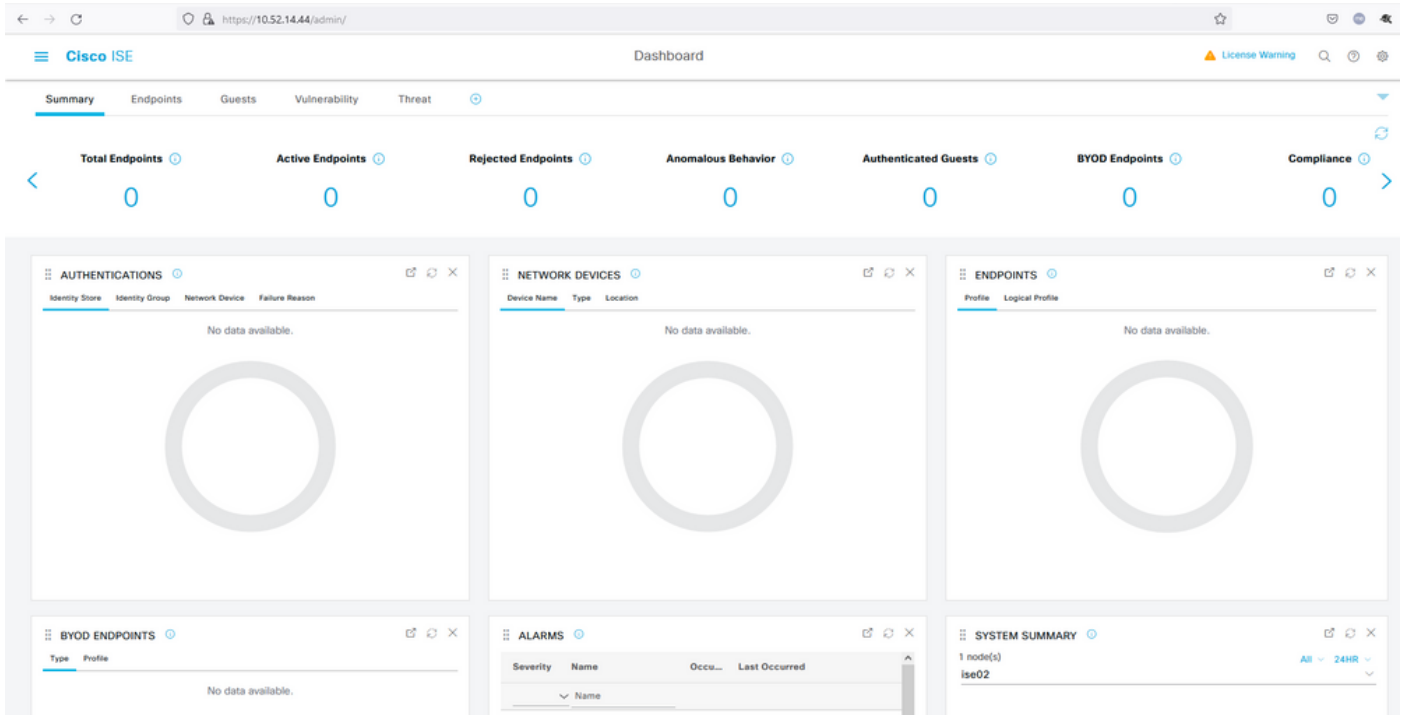


Success!

Logging you in...



Secured by Duo



Troubleshooting

- Baixe a extensão do rastreador SAML para o Mozilla FF <https://addons.mozilla.org/en-US/firefox/addon/saml-tracer/>.
- Role até o pacoteSSOLoginResponse.action. Na guia **SAML**, você vê vários atributos enviados do 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

- Logon administrativo no ISE: nome de usuário: samUser.

- 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 exported 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		10.85.48.183	18492	Administrator authentication succeeded	Administrator authentication successful

Rows/Page 1 1 Total Rows

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.