Configurar a autenticação 802.1X com PEAP, ISE 2.1 e WLC 8.3

Contents

Introduction

Este documento descreve como configurar uma rede local sem fio (WLAN) com segurança 802.1x e substituição de rede local virtual (VLAN).

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- 802.1x
- Protocolo PEAP protegido
- Autoridade de Certificação (CA)
- Certificados

Componentes Utilizados

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

- WLC v8.3.102.0

- Identity Service Engine (ISE) v2.1
- Notebook Windows 10

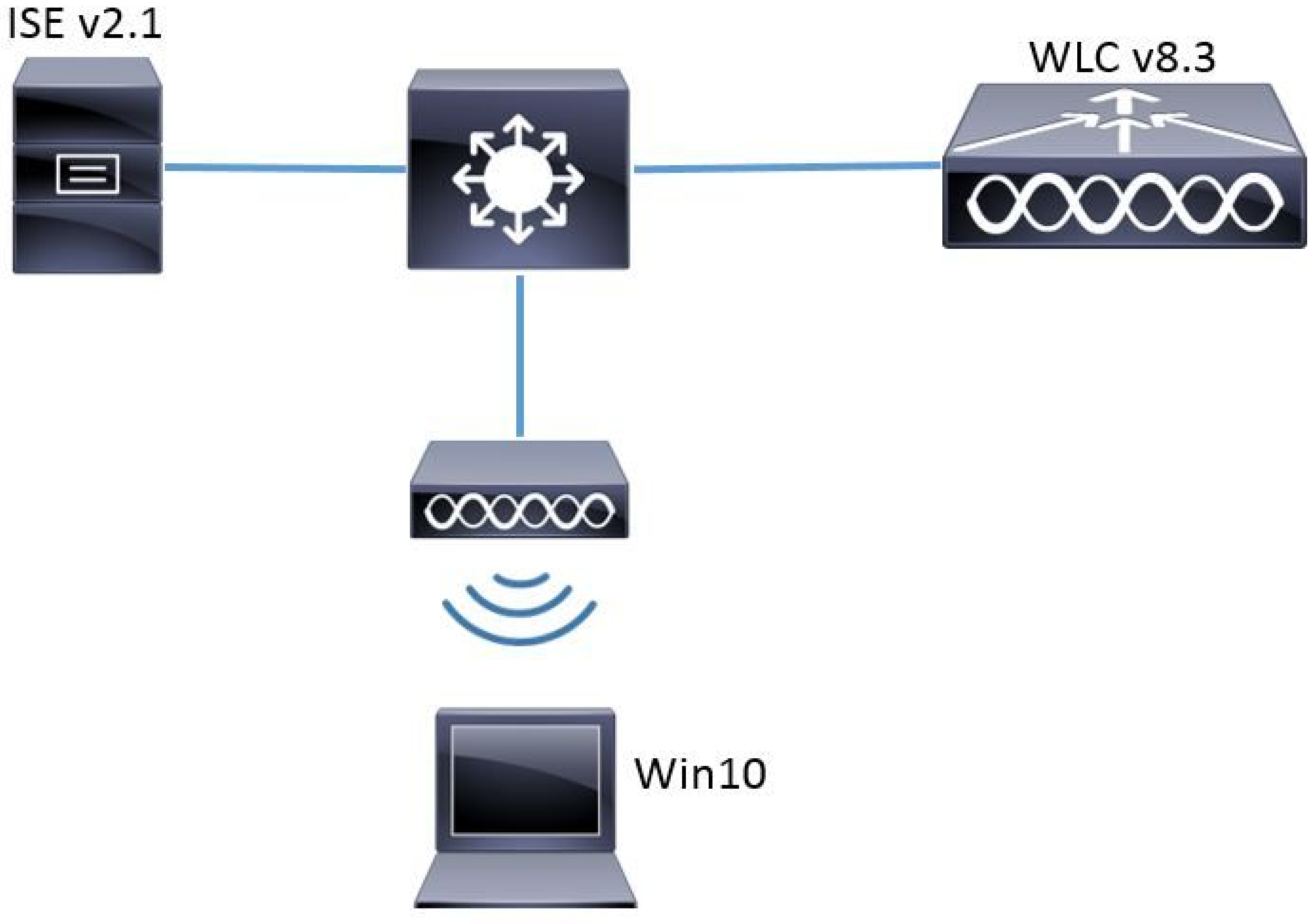
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

Ao configurar uma WLAN com segurança 802.1x e VLAN, você pode substituir o Protected Extensible Authentication Protocol como Extensible Authentication Protocol (EAP).

Configurar

Diagrama de Rede



Configuração

As etapas gerais são:

1. Declare o servidor RADIUS na WLC e vice-versa para permitir a comunicação entre si.
2. Crie o Service Set Identifier (SSID) no WLC.
3. Crie a regra de autenticação no ISE.
4. Crie o perfil de autorização no ISE.

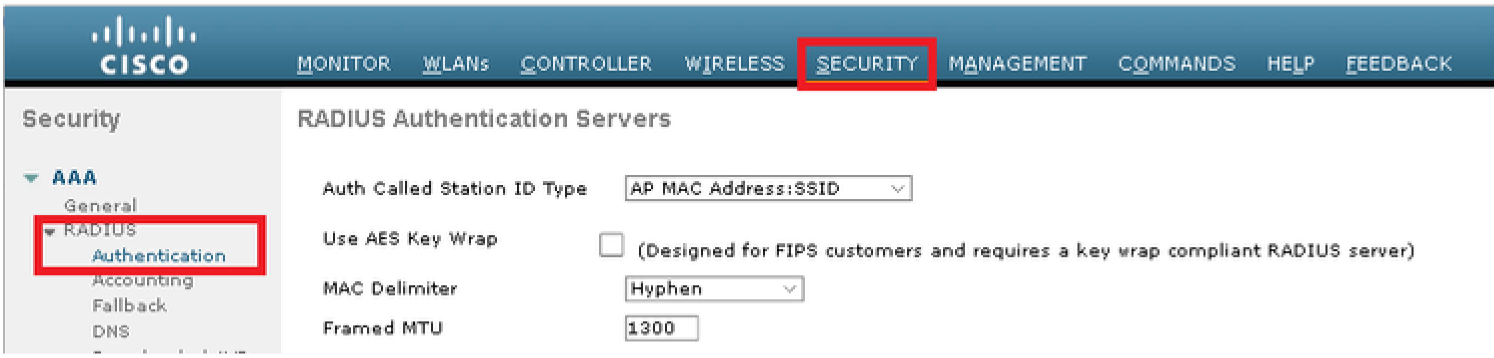
5. Crie a regra de autorização no ISE.
6. Configure o ponto final.

Declarar servidor RADIUS no WLC

Para permitir a comunicação entre o servidor RADIUS e a WLC, você precisa registrar o servidor RADIUS na WLC e vice-versa.

GUI:

Etapa 1. Abra a GUI do WLC e navegue para **SECURITY** > **RADIUS** > **Authentication** > **New** conforme mostrado na imagem.



RADIUS Authentication Servers

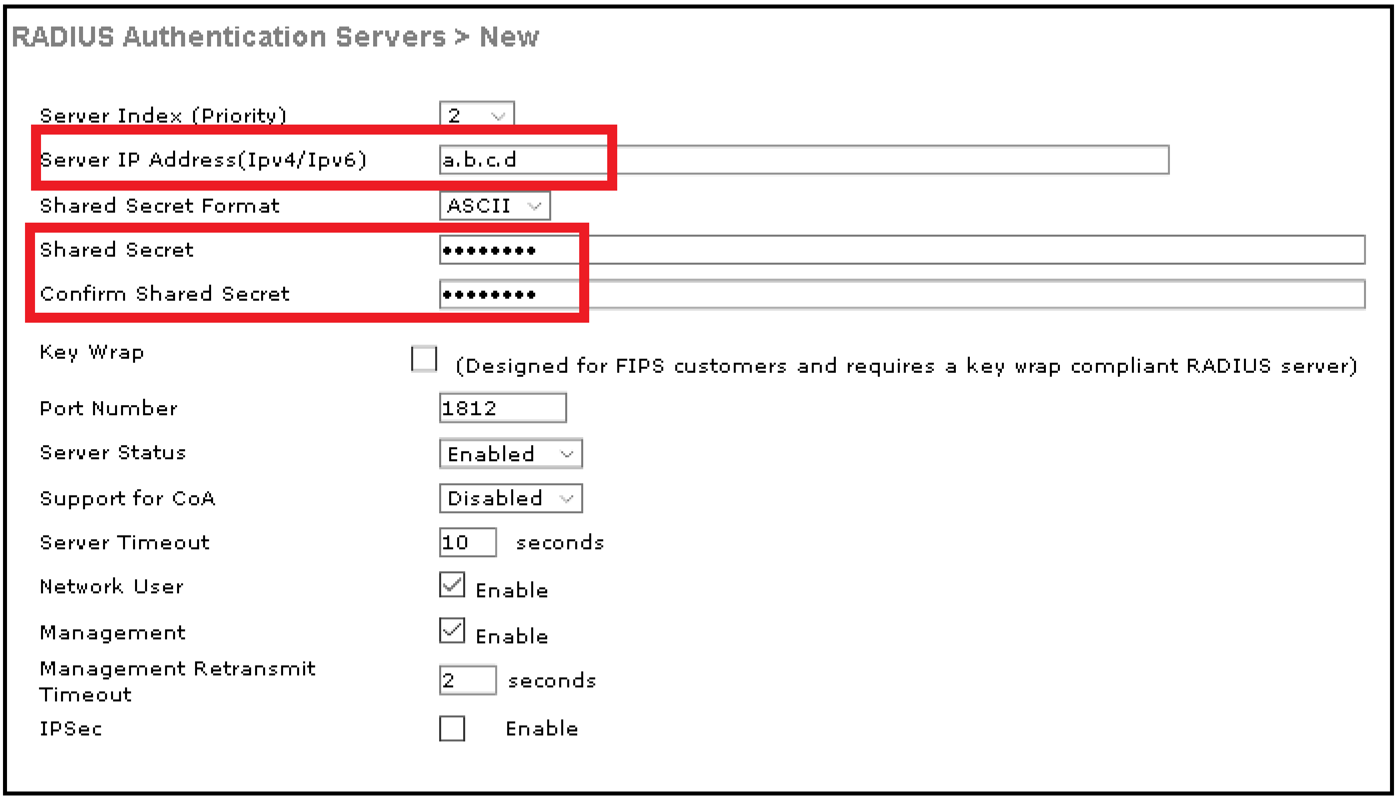
Auth Called Station ID Type: AP MAC Address:SSID

Use AES Key Wrap: □ (Designed for FIPS customers and requires a key wrap compliant RADIUS server)

MAC Delimiter: Hyphen

Framed MTU: 1300

Etapa 2. Insira as informações do servidor RADIUS conforme mostrado na imagem.



RADIUS Authentication Servers > New

Server Index (Priority): 2

Server IP Address(Ipv4/Ipv6): a.b.c.d

Shared Secret Format: ASCII

Shared Secret: ••••••••

Confirm Shared Secret: ••••••••

Key Wrap: □ (Designed for FIPS customers and requires a key wrap compliant RADIUS server)

Port Number: 1812

Server Status: Enabled

Support for CoA: Disabled

Server Timeout: 10 seconds

Network User: ☑ Enable

Management: ☑ Enable

Management Retransmit Timeout: 2 seconds

IPSec: □ Enable

CLI:

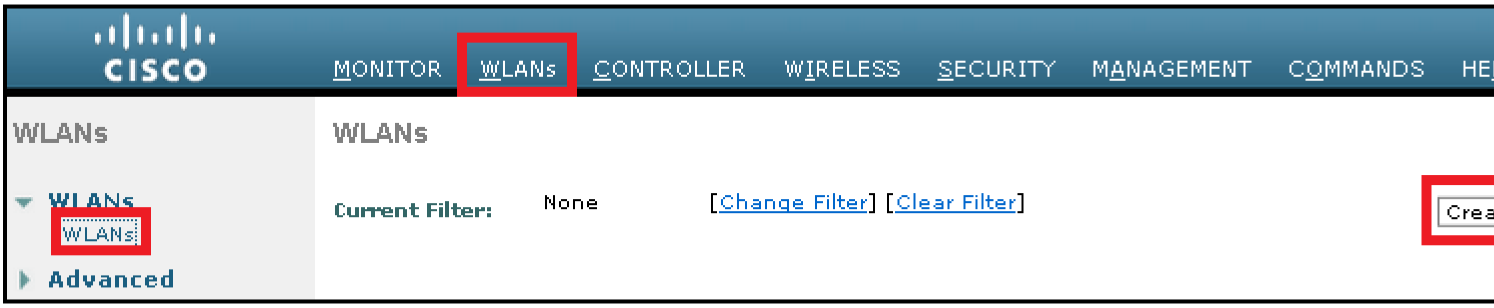
```
> config radius auth add <index> <a.b.c.d> 1812 ascii <shared-key>
> config radius auth disable <index>
> config radius auth retransmit-timeout <index> <timeout-seconds>
> config radius auth enable <index>
```

<a.b.c.d> corresponde ao servidor RADIUS.

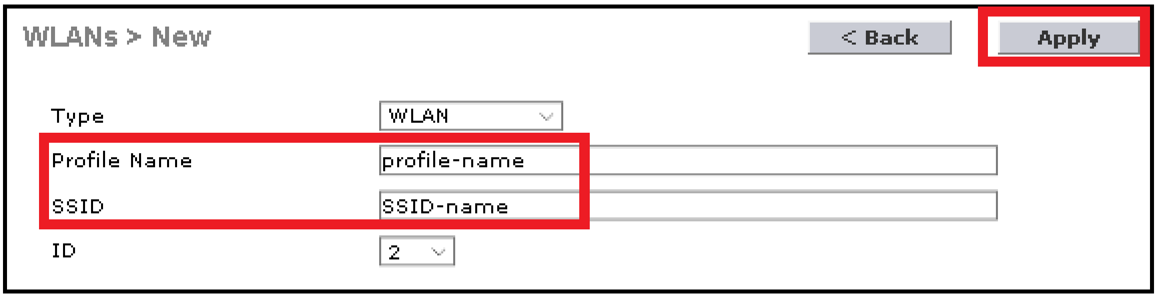
Criar SSID

GUI:

Etapa 1. Abra a GUI da WLC e navegue para **WLANs > Create New > Go** conforme mostrado na imagem.



Etapa 2. Escolha um nome para o SSID e o perfil e clique em **Aplicar**, conforme mostrado na imagem.



Type	WLAN
Profile Name	profile-name
SSID	SSID-name
ID	2

CLI:

```
> config wlan create <id> <profile-name> <ssid-name>
```

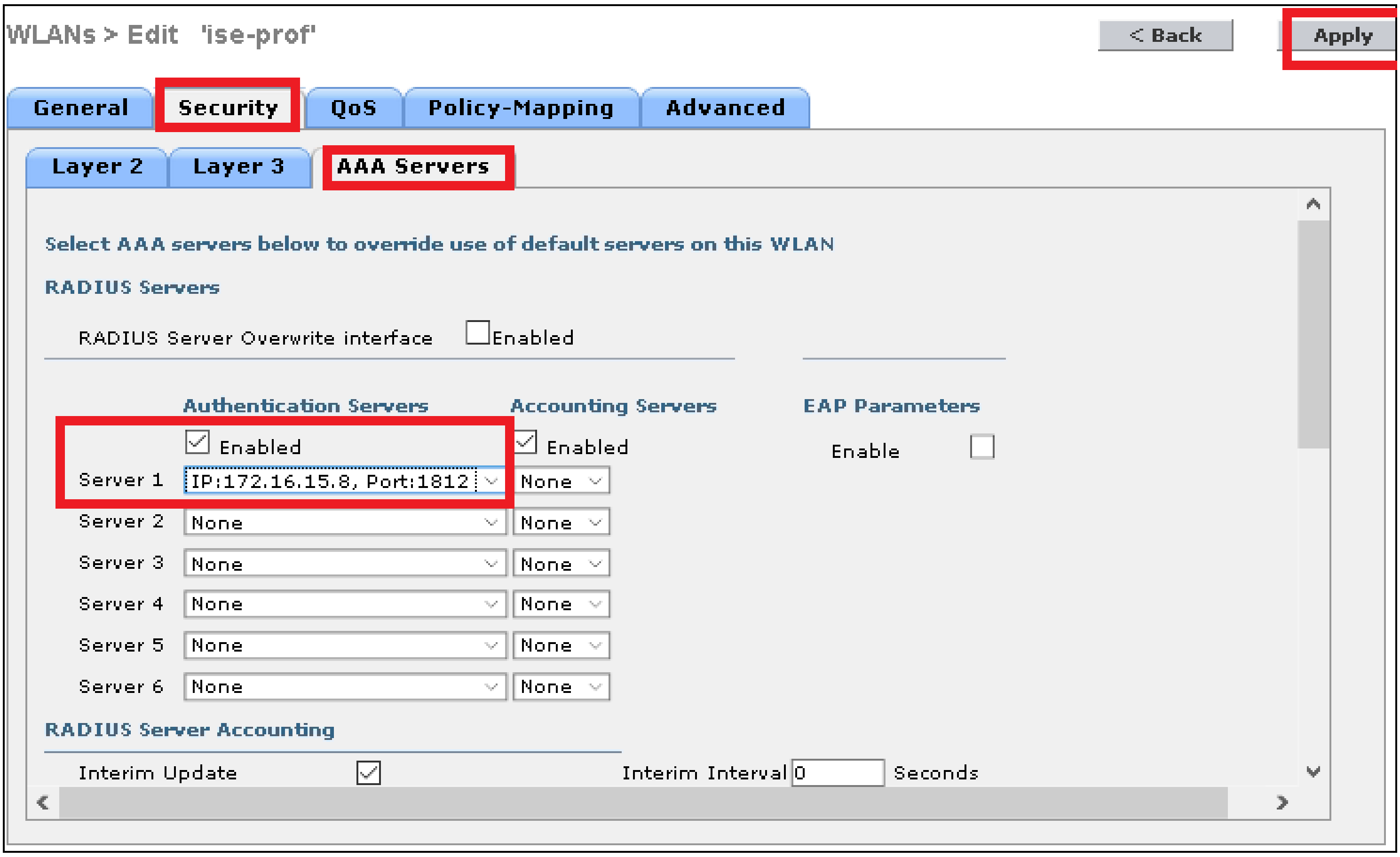
Etapa 3. Atribua o servidor RADIUS à WLAN.

CLI:

```
> config wlan radius_server auth add <wlan-id> <radius-index>
```

GUI:

Navegue para **Security > AAA Servers** e escolha o servidor RADIUS desejado, depois pressione **Apply** como mostrado na imagem.



Select AAA servers below to override use of default servers on this WLAN

RADIUS Servers

RADIUS Server Overwrite interface □ Enabled

	Authentication Servers	Accounting Servers	EAP Parameters
	☑ Enabled	☑ Enabled	Enable □
Server 1	IP:172.16.15.8, Port:1812	None	
Server 2	None	None	
Server 3	None	None	
Server 4	None	None	
Server 5	None	None	
Server 6	None	None	

RADIUS Server Accounting

Interim Update ☑ Interim Interval 0 Seconds

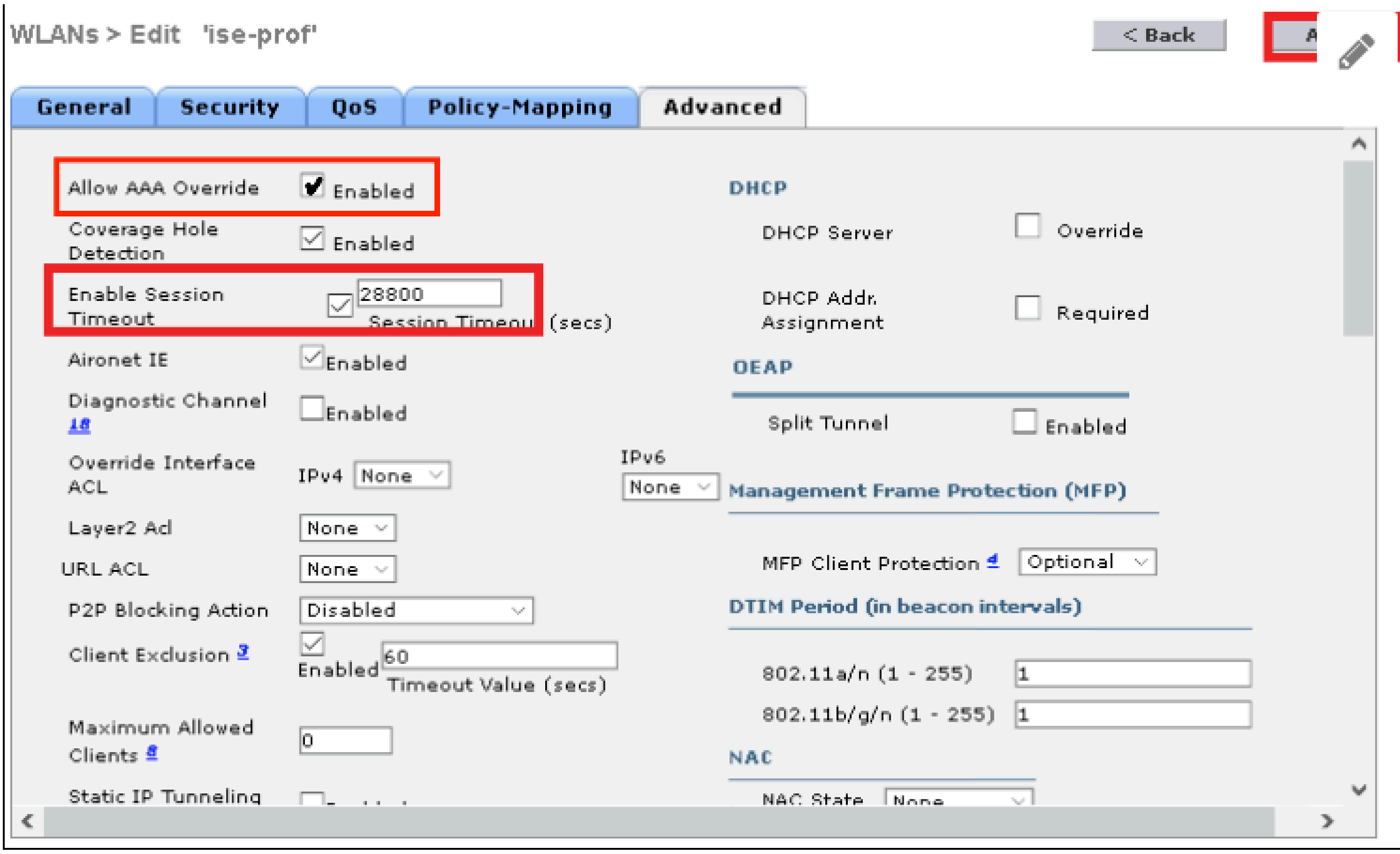
Etapa 4. Habilite **Allow AAA Override** e, opcionalmente, aumente o timeout da sessão

CLI:

```
> config wlan aaa-override enable <wlan-id>
> config wlan session-timeout <wlan-id> <session-timeout-seconds>
```

GUI:

Navegue até **WLANs > WLAN ID > Advanced** e habilite **Allow AAA Override**. Opcionalmente, especifique o Tempo Limite da Sessão conforme mostrado na imagem.



WLANs > Edit 'ise-prof'

Allow AAA Override ☑ Enabled

Coverage Hole Detection ☑ Enabled

Enable Session Timeout ☑ 28800 Session Timeout (secs)

Aironet IE ☑ Enabled

Diagnostic Channel 18 □ Enabled

Override Interface ACL IPv4 None IPv6 None

Layer2 Acl None

URL ACL None

P2P Blocking Action Disabled

Client Exclusion 3 ☑ Enabled 60 Timeout Value (secs)

Maximum Allowed Clients 8 0

Static IP Tunneling □

DHCP

DHCP Server □ Override

DHCP Addr. Assignment □ Required

OEAP

Split Tunnel □ Enabled

Management Frame Protection (MFP)

MFP Client Protection 4 Optional

DTIM Period (in beacon intervals)

802.11a/n (1 - 255) 1

802.11b/g/n (1 - 255) 1

NAC

NAC State None

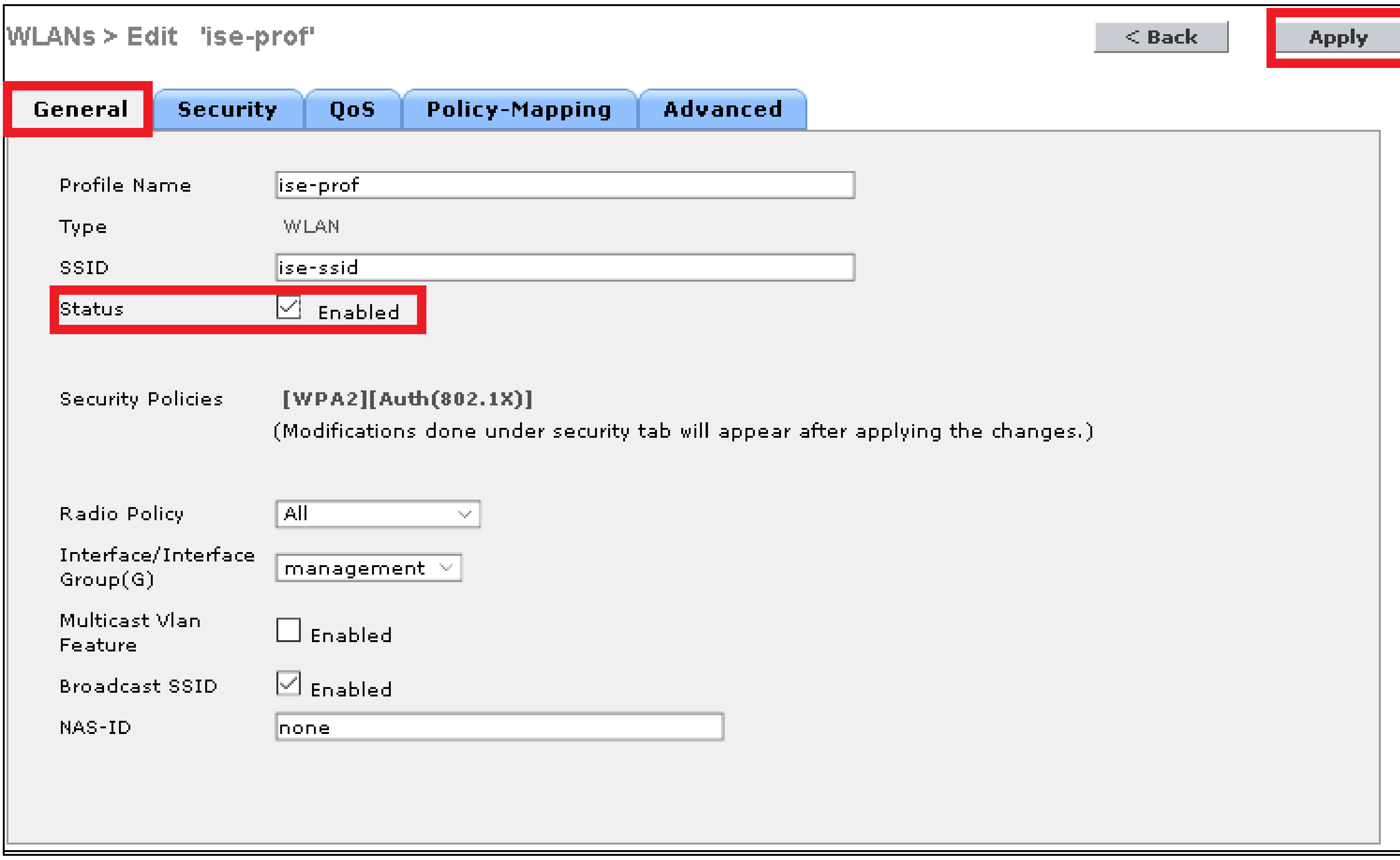
Etapa 5. Ativar a WLAN.

CLI:

```
> config wlan enable <wlan-id>
```

GUI:

Navegue até **WLANs > WLAN ID > General** e habilite o SSID como mostrado na imagem.



Profile Name: ise-prof

Type: WLAN

SSID: ise-ssid

Status: ☑ Enabled

Security Policies: [WPA2][Auth(802.1X)]
(Modifications done under security tab will appear after applying the changes.)

Radio Policy: All

Interface/Interface Group(G): management

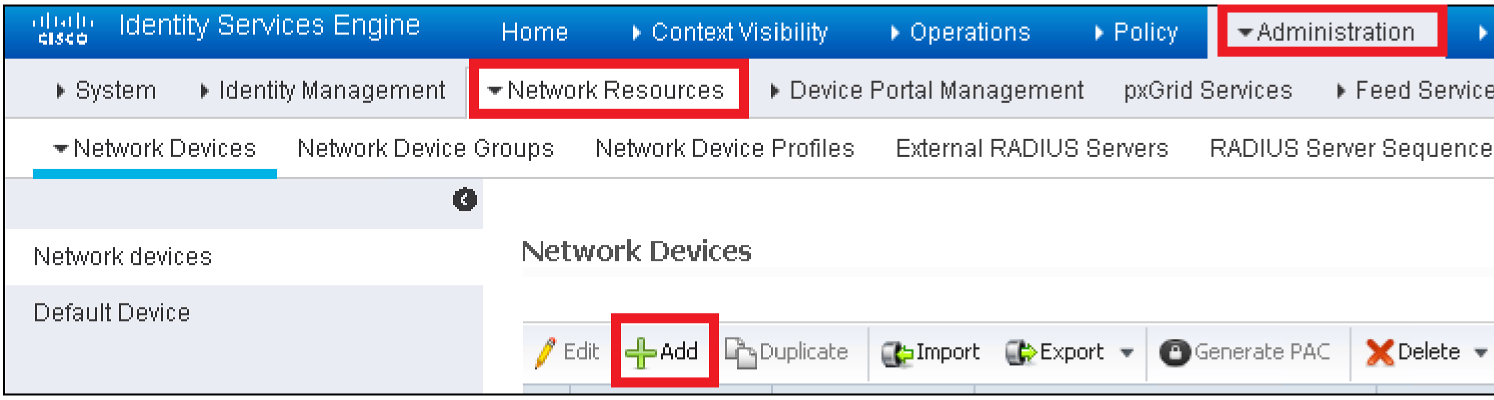
Multicast Vlan Feature: □ Enabled

Broadcast SSID: ☑ Enabled

NAS-ID: none

Declarar WLC no ISE

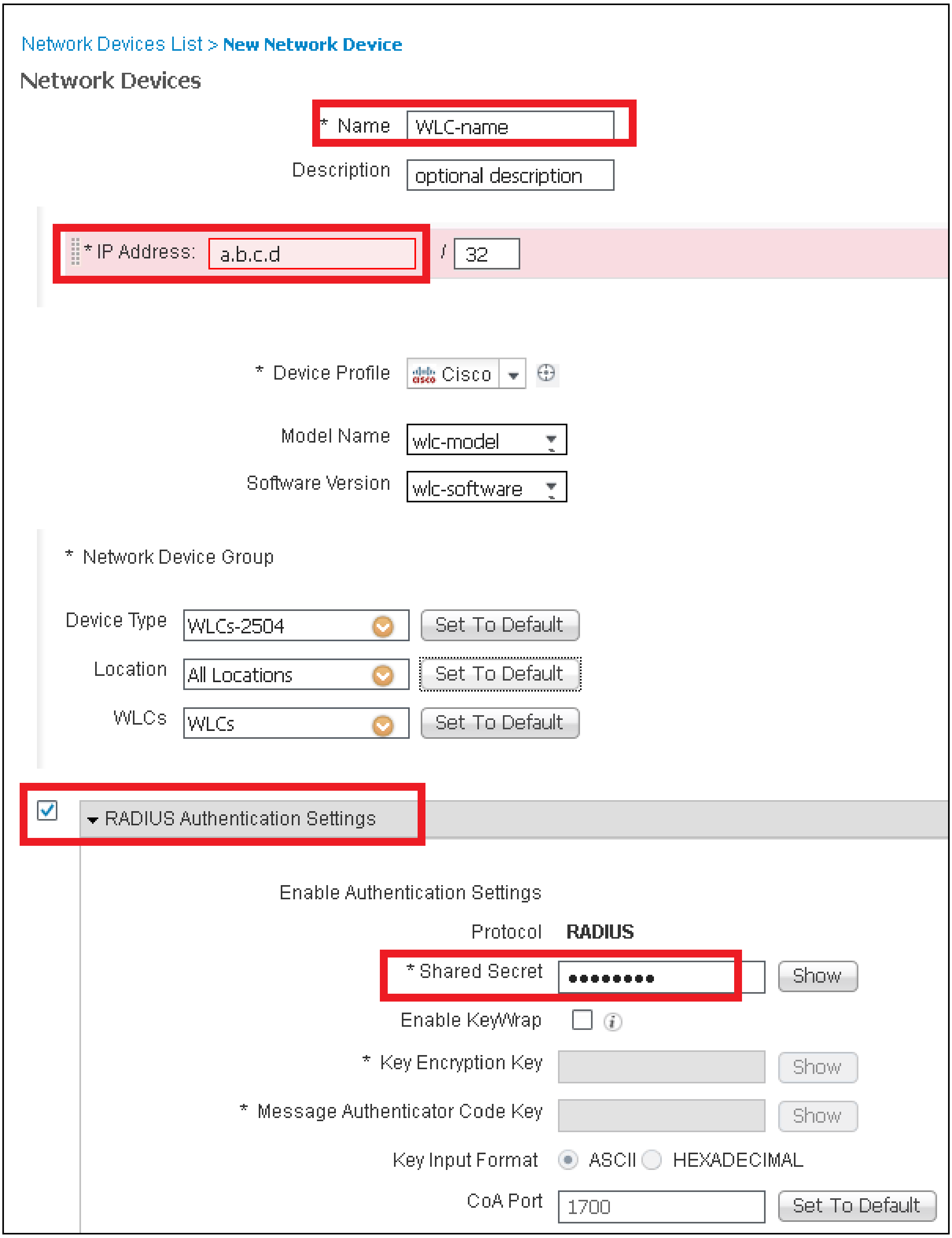
Etapa 1. Abra o console do ISE e navegue até **Administração** > **Recursos de rede** > **Dispositivos de rede** > **Adicionar** conforme mostrado na imagem.



Etapa 2. Insira os valores.

Opcionalmente, pode ser um nome de Modelo, versão de software, descrição e atribuir grupos de Dispositivos de Rede com base em tipos de dispositivo, localização ou WLCs.

a.b.c.d corresponde à interface da WLC que envia a autenticação solicitada. Por padrão, é a interface de gerenciamento, como mostrado na imagem.



Network Devices List > New Network Device

Network Devices

* Name: WLC-name

Description: optional description

* IP Address: a.b.c.d / 32

* Device Profile: Cisco

Model Name: wlc-model

Software Version: wlc-software

* Network Device Group

Device Type: WLCs-2504

Location: All Locations

WLCs: WLCs

☑ RADIUS Authentication Settings

Enable Authentication Settings

Protocol: RADIUS

* Shared Secret: ●●●●●●●●●

Enable KeyWrap: □

* Key Encryption Key

* Message Authenticator Code Key

Key Input Format: ● ASCII ○ HEXADECIMAL

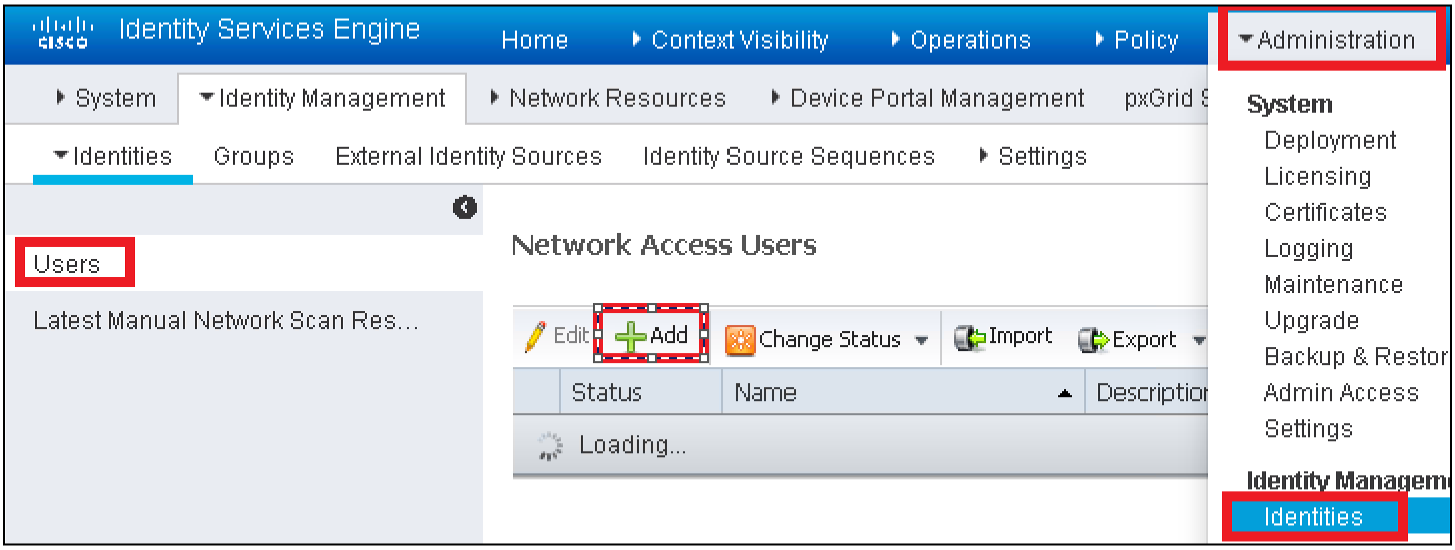
CoA Port: 1700

Para obter mais informações sobre Grupos de dispositivos de rede:

[ISE â€“ Grupos de dispositivos de rede]

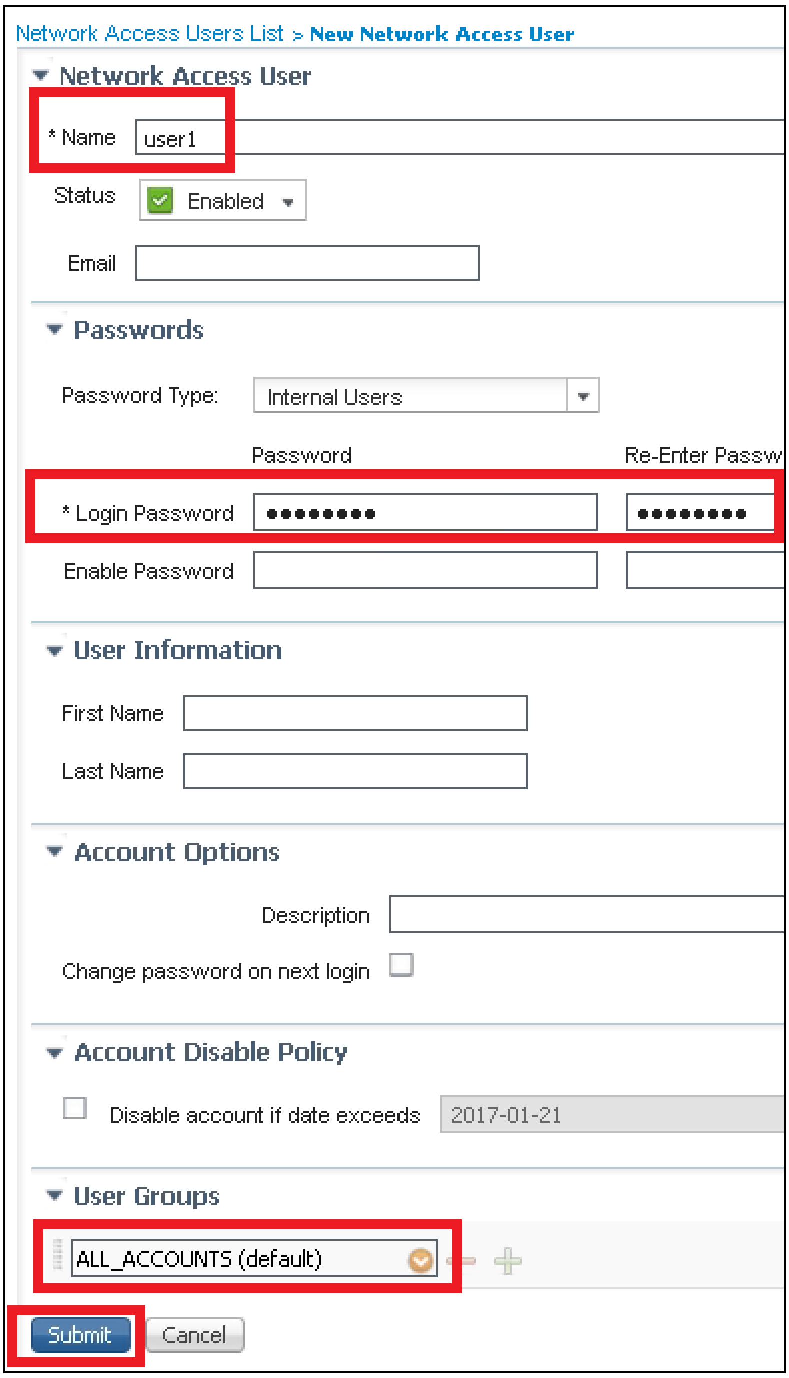
Criar novo usuário no ISE

Etapa 1. Navegue até Administração > Gerenciamento de identidade > Identidades > Usuários > Adicionar , conforme mostrado na imagem.



Etapa 2. Inserir informações.

Neste exemplo, este usuário pertence a um grupo chamado ALL_ACCOUNTS, mas pode ser ajustado conforme necessário, como mostrado na imagem.



Network Access Users List > New Network Access User

Network Access User

* Name: user1

Status: ✓ Enabled

Email:

Passwords

Password Type: Internal Users

	Password	Re-Enter Passw
* Login Password	●●●●●●●●●	●●●●●●●●●
Enable Password		

User Information

First Name:

Last Name:

Account Options

Description:

Change password on next login □

Account Disable Policy

□ Disable account if date exceeds 2017-01-21

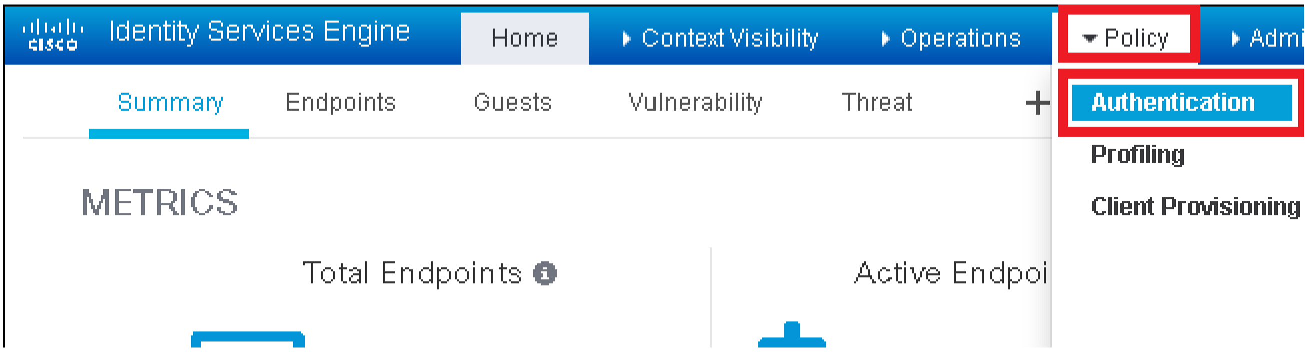
User Groups

ALL_ACCOUNTS (default)

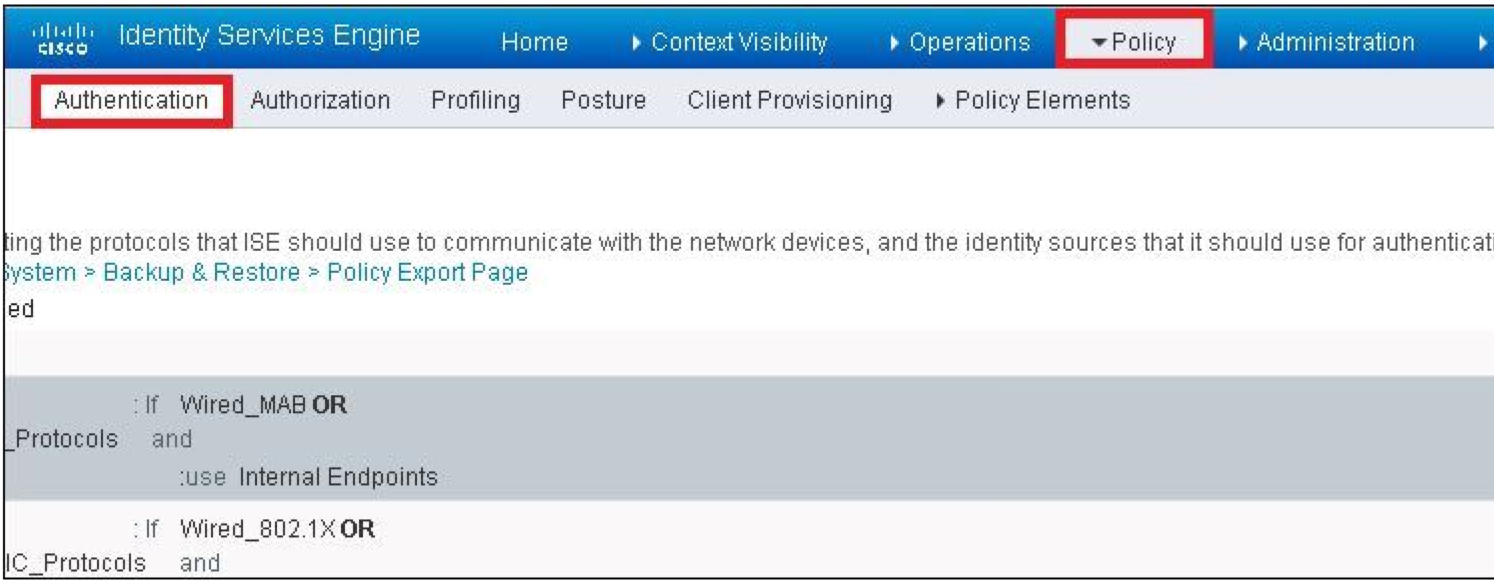
Criar Regra de Autenticação

As regras de autenticação são usadas para verificar se as credenciais dos usuários estão corretas (verificar se o usuário realmente é quem diz ser) e limitar os métodos de autenticação que podem ser usados por ele.

Etapa 1. Navegue para **Política** > **Autenticação** como mostrado na imagem.



Etapa 2. Insira uma nova regra de autenticação, conforme mostrado na imagem.



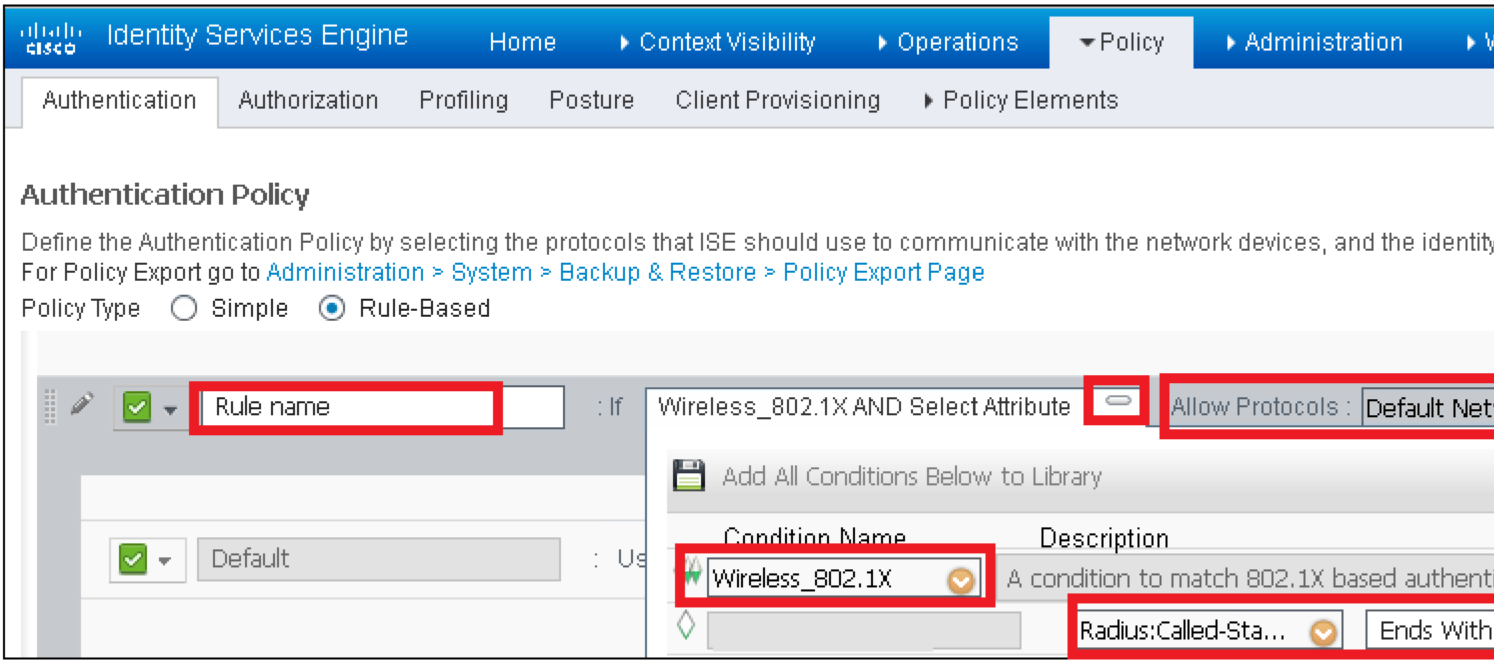
ting the protocols that ISE should use to communicate with the network devices, and the identity sources that it should use for authenticat
System > Backup & Restore > Policy Export Page
ed

: If Wired_MAB **OR**
_Protocols and
:use Internal Endpoints

: If Wired_802.1X **OR**
IC_Protocols and

Etapa 3. Insira os valores.

Esta regra de autenticação permite todos os protocolos listados na lista Acesso de rede padrão. Isso se aplica à solicitação de autenticação para clientes Wireless 802.1x e com ID de estação chamada, e termina com ise-ssid, como mostrado na imagem.



Authentication Policy

Define the Authentication Policy by selecting the protocols that ISE should use to communicate with the network devices, and the identity
For Policy Export go to Administration > System > Backup & Restore > Policy Export Page

Policy Type ○ Simple ● Rule-Based

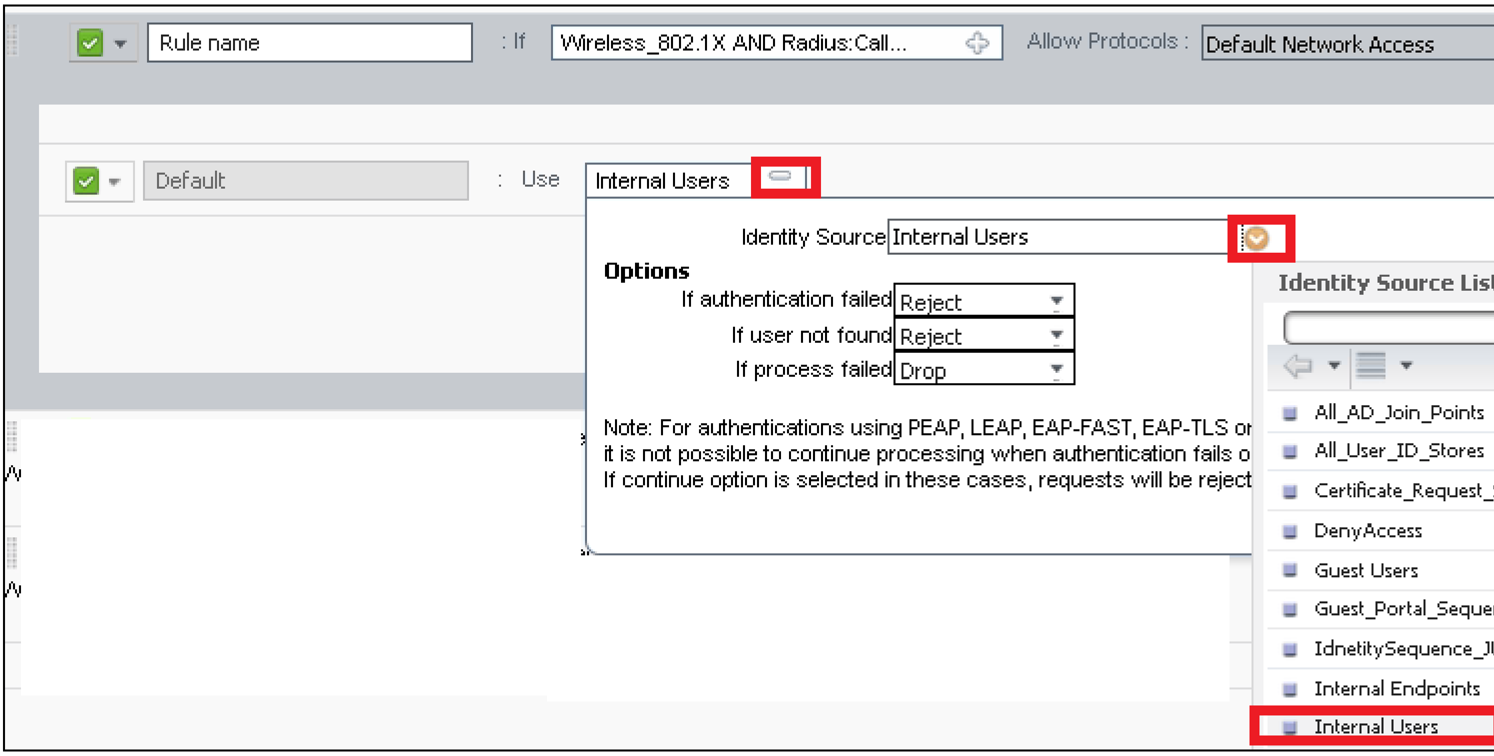
☑ Rule name : If Wireless_802.1X AND Select Attribute Allow Protocols : Default Net

Add All Conditions Below to Library

Condition Name	Description
Wireless_802.1X	A condition to match 802.1X based authent
	Radius:Called-Sta... Ends With

☑ Default : Us

Além disso, escolha a fonte de identidade para os clientes que correspondem a esta regra de autenticação. Este exemplo usa a lista de origem de identidade de usuários internos como mostrado na imagem.



Rule name : If Wireless_802.1X AND Radius:Call... Allow Protocols : Default Network Access

Default : Use Internal Users

Identity Source Internal Users

Options

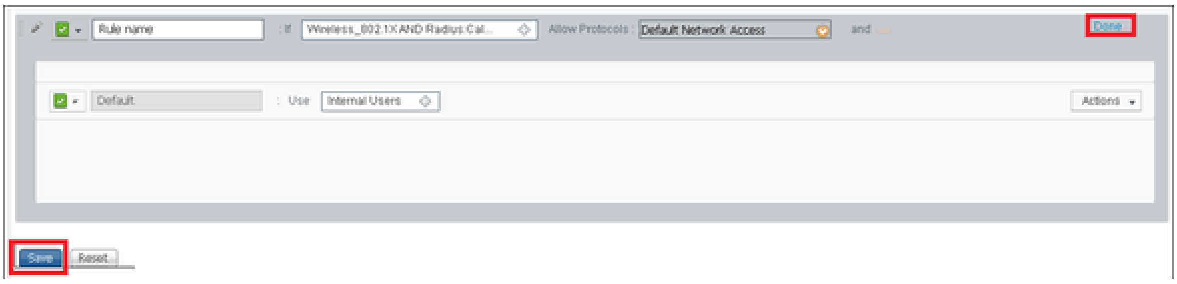
If authentication failed Reject

If user not found Reject

If process failed Drop

Note: For authentications using PEAP, LEAP, EAP-FAST, EAP-TLS or
it is not possible to continue processing when authentication fails o
If continue option is selected in these cases, requests will be reject

Quando terminar, clique em **Concluído** e em **Salvar** como mostrado na imagem.



Rule name : If Wireless_802.1X AND Radius:Cal... Allow Protocols : Default Network Access and

Default : Use Internal Users

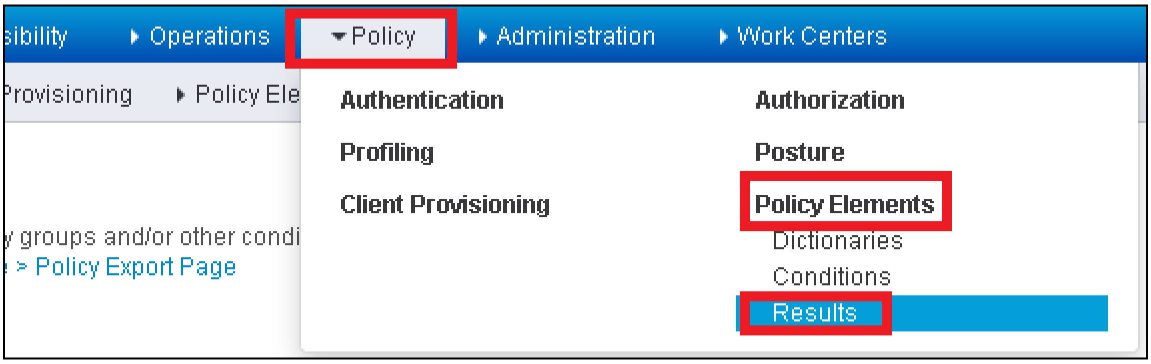
Para obter mais informações sobre fontes de identidade, consulte este link:

[Criar um grupo de identidade de usuário]

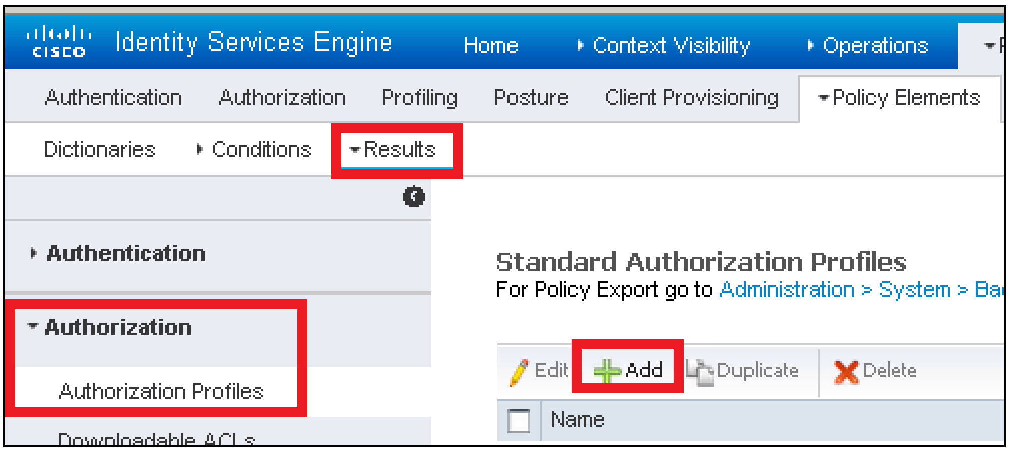
Criar perfil de autorização

O perfil de autorização determina se você tem ou não acesso à rede. Listas de Controle de Acesso (ACLs - Access Control Lists), substituição de VLAN ou qualquer outro parâmetro. O perfil de autorização mostrado neste exemplo envia uma aceitação de acesso para você e atribui a VLAN 2404.

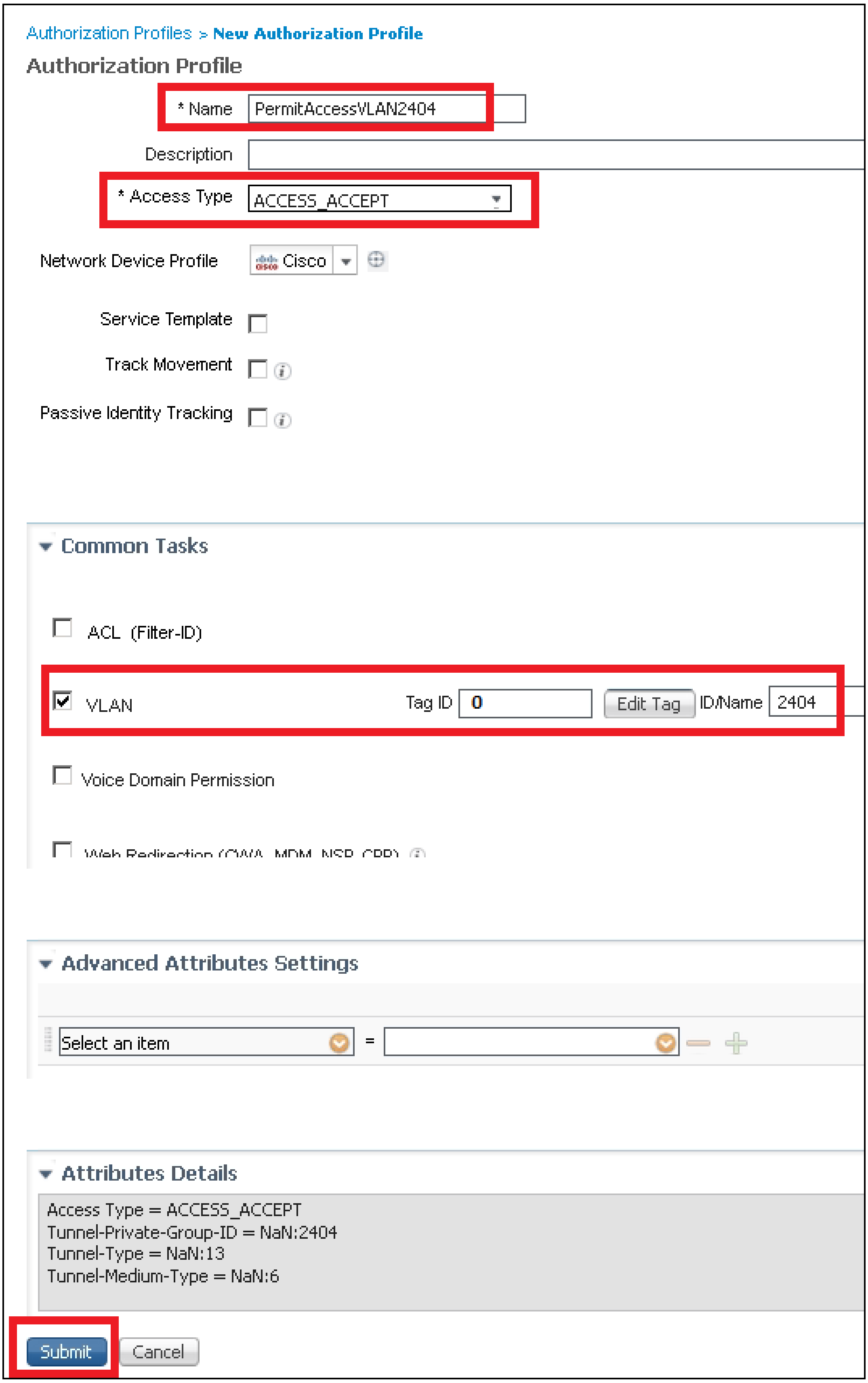
Etapa 1. Navegue para **Política** > **Elementos de política** > **Resultados** como mostrado na imagem.



Etapa 2. Adicione um novo perfil de autorização. Navegue até **Authorization** > **Authorization Profiles** > **Add** conforme mostrado na imagem.



Etapa 3. Insira os valores conforme mostrado na imagem.


Authorization Profiles > New Authorization Profile
Common Tasks
Advanced Attributes Settings
Attributes Details
Edit Tag
Submit
Cancel

Authorization Profile

* Name PermitAccessVLAN2404

Description

* Access Type ACCESS_ACCEPT

Network Device Profile Cisco

Service Template □

Track Movement □

Passive Identity Tracking □

□ ACL (Filter-ID)

☑ VLAN Tag ID 0 ID/Name 2404

□ Voice Domain Permission

□ Web Redirection (CWA, MDM, NSP, CPP)

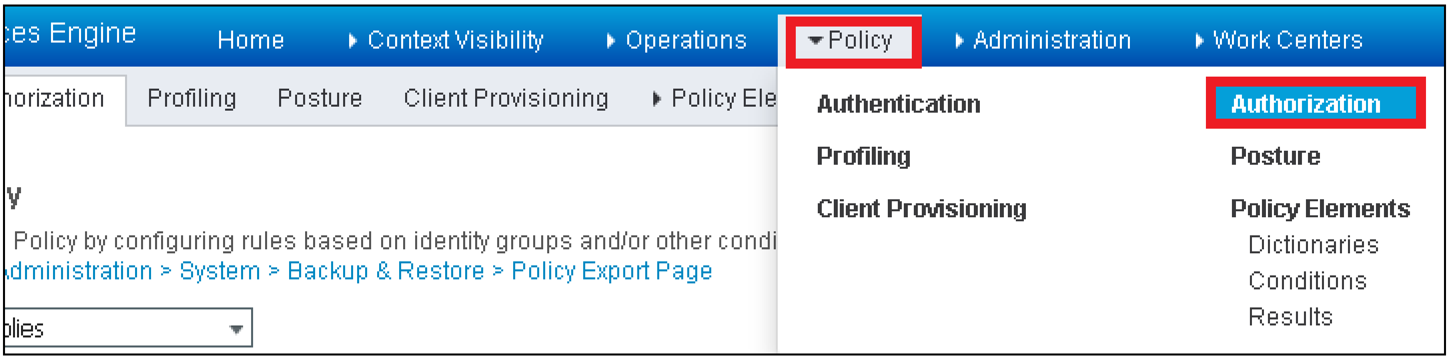
Select an item =

Access Type = ACCESS_ACCEPT
Tunnel-Private-Group-ID = NaN:2404
Tunnel-Type = NaN:13
Tunnel-Medium-Type = NaN:6

Criar Regra de Autorização

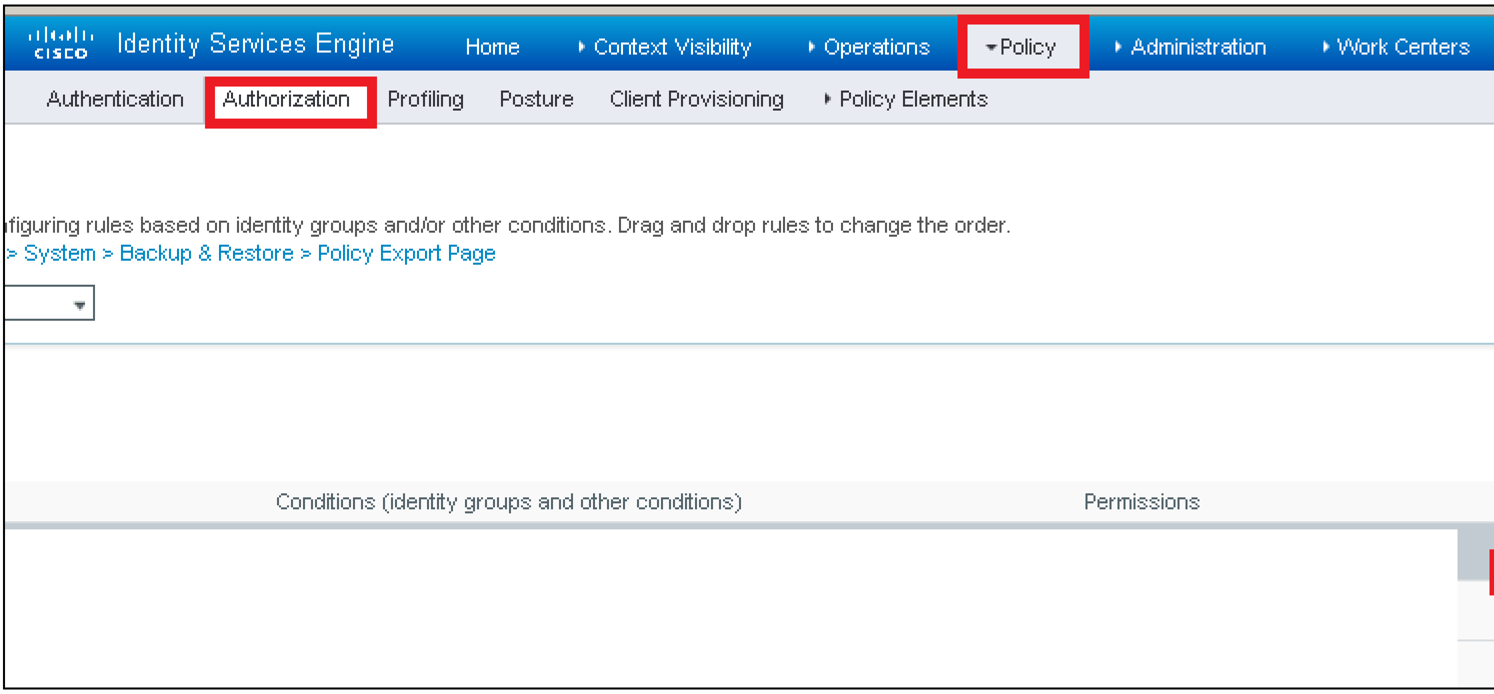
A regra de autorização é a responsável por determinar quais permissões (qual perfil de autorização) o resultado será aplicado a você.

Etapa 1. Navegue para **Política** > **Autorização** como mostrado na imagem.



Policy by configuring rules based on identity groups and/or other condi

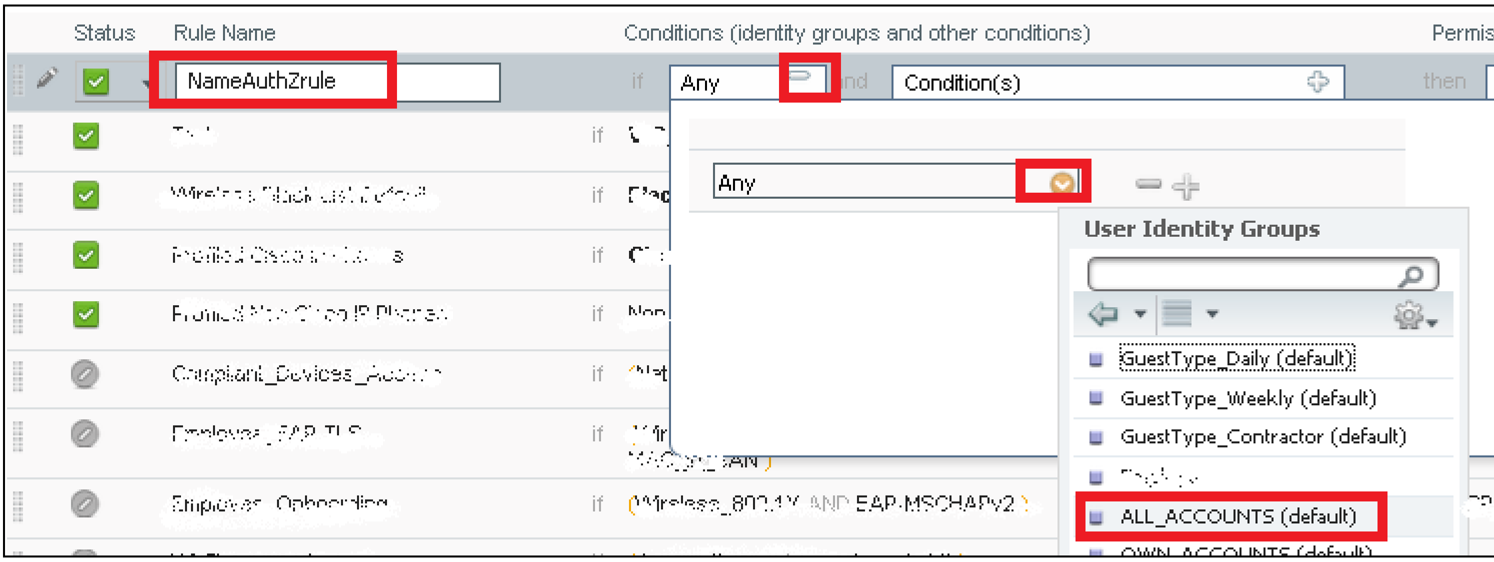
Etapa 2. Inserir uma nova regra conforme mostrado na imagem.



figuring rules based on identity groups and/or other conditions. Drag and drop rules to change the order.

Etapa 3. Insira os valores.

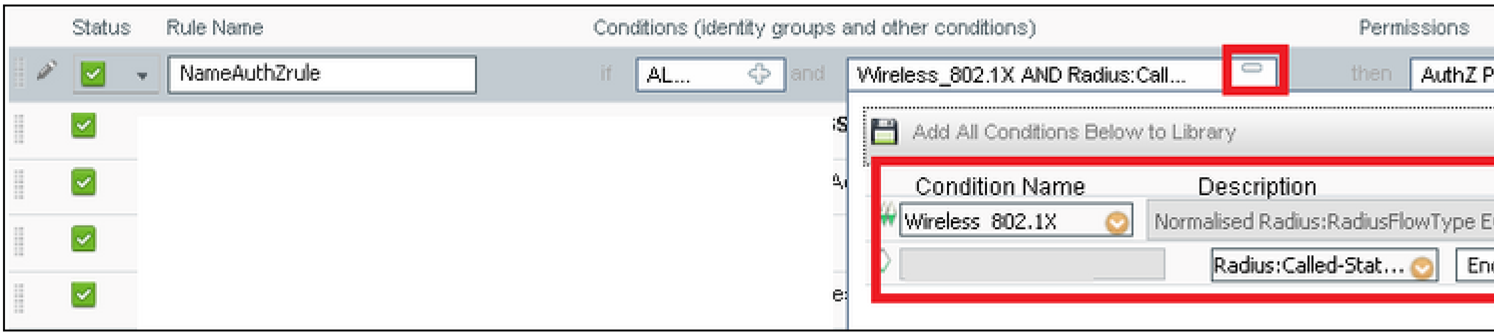
Primeiro, selecione um nome para a regra e o grupo de identidade onde o usuário está armazenado (ALL_ACCOUNTS), como mostrado na imagem.



Status
Rule Name
Conditions (identity groups and other conditions)
Permis
if
Any
and
Condition(s)
then
Compliant_Devices_Acc
Employee_Onboarding
(Wireless_802.1X AND EAP-MSCHAPv2)
Any
User Identity Groups
GuestType_Daily (default)
GuestType_Weekly (default)
GuestType_Contractor (default)
ALL_ACCOUNTS (default)
OWN_ACCOUNTS (default)

Rule Name: NameAuthZrule

Depois disso, selecione outras condições que façam com que o processo de autorização se encaixe nessa regra. Neste exemplo, o processo de autorização atingirá essa regra se usar 802.1x Wireless e sua ID de estação chamada terminar com ise-ssid, como mostrado na imagem.

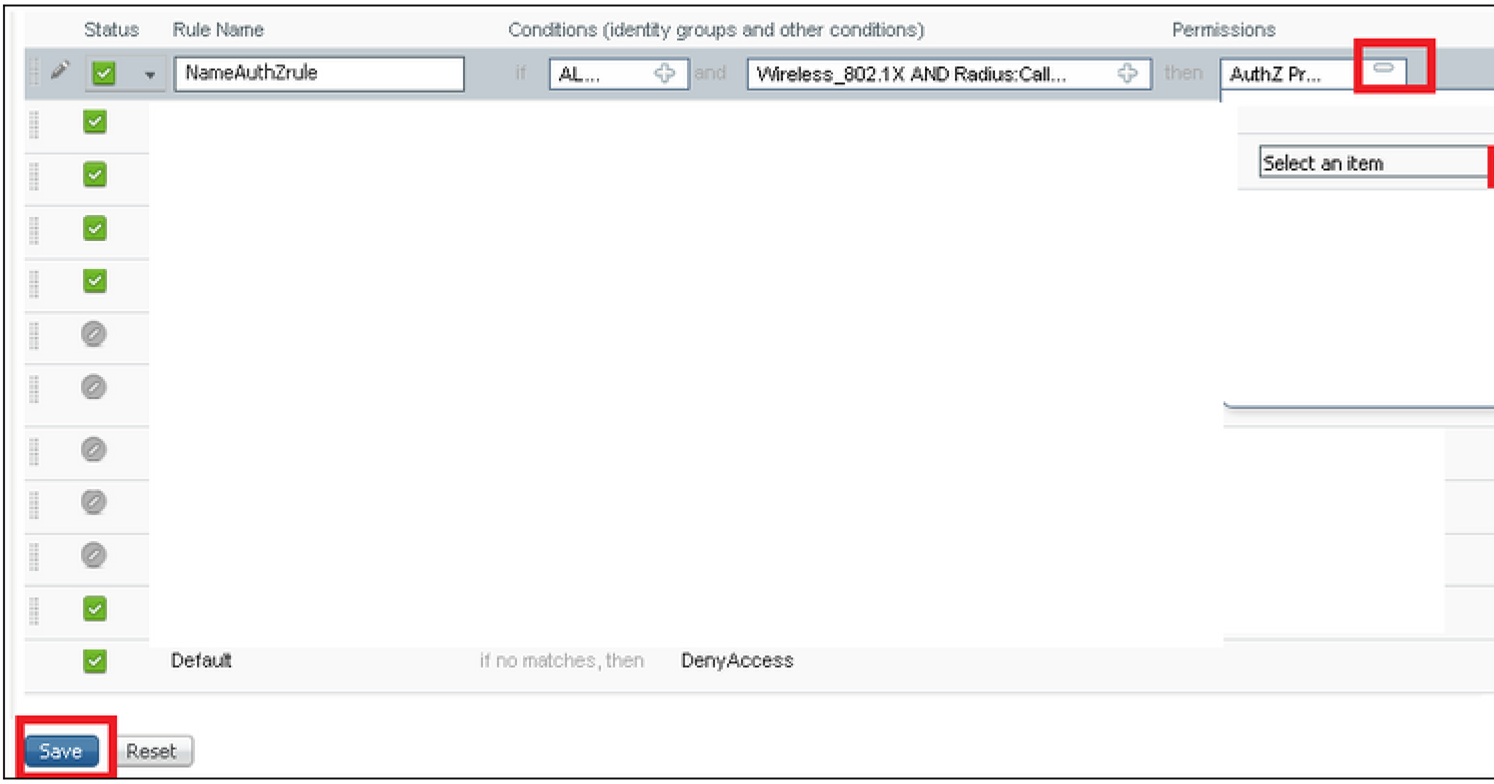

Status
Rule Name
Conditions (identity groups and other conditions)
Permissions
if
and
then
Add All Conditions Below to Library
Condition Name
Description

Rule Name: NameAuthZrule

if AL... and Wireless_802.1X AND Radius:Call... then AuthZ P

Condition Name	Description	
Wireless_802.1X	Normalised Radius:RadiusFlowType E	
	Radius:Called-Stat...	En

Por fim, selecione o perfil de Autorização atribuído a você que atinge essa regra. Clique em **Done** e **Save** como mostrado na imagem.



Rule Name: NameAuthZrule

if AL... and Wireless_802.1X AND Radius:Call... then AuthZ Pr...

Default — if no matches, then DenyAccess

Configuração do dispositivo final

Configure uma máquina Windows 10 laptop para se conectar a um SSID com Autenticação 802.1x e PEAP/MS-CHAPv2 (versão da Microsoft do Challenge-Handshake Authentication Protocol) Versão 2.

Neste exemplo de configuração, o ISE usa seu certificado autoassinado para executar a autenticação.

Para criar o perfil WLAN na máquina com Windows, há duas opções:

1. Instale o certificado autoassinado no computador para validar e confie no servidor ISE para concluir a autenticação.
2. Ignore a validação do servidor RADIUS e confie em qualquer servidor RADIUS usado para executar a autenticação (não recomendado, pois pode se tornar um problema de segurança).

A configuração dessas opções é explicada em Configuração do dispositivo final - Criar o perfil de WLAN -

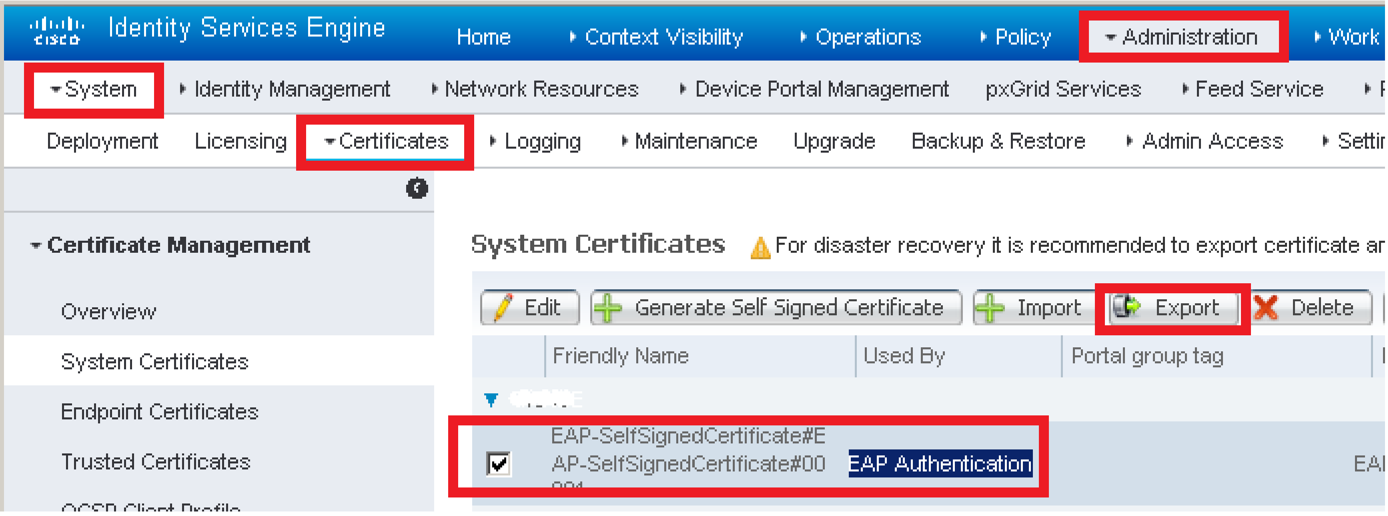
Etapa 7.

Configuração do dispositivo final - Instalar certificado autoassinado ISE

Etapa 1. Exportar certificado autoassinado.

Faça login no ISE e navegue até **Administration** > **System** > **Certificates** > **System Certificates**.

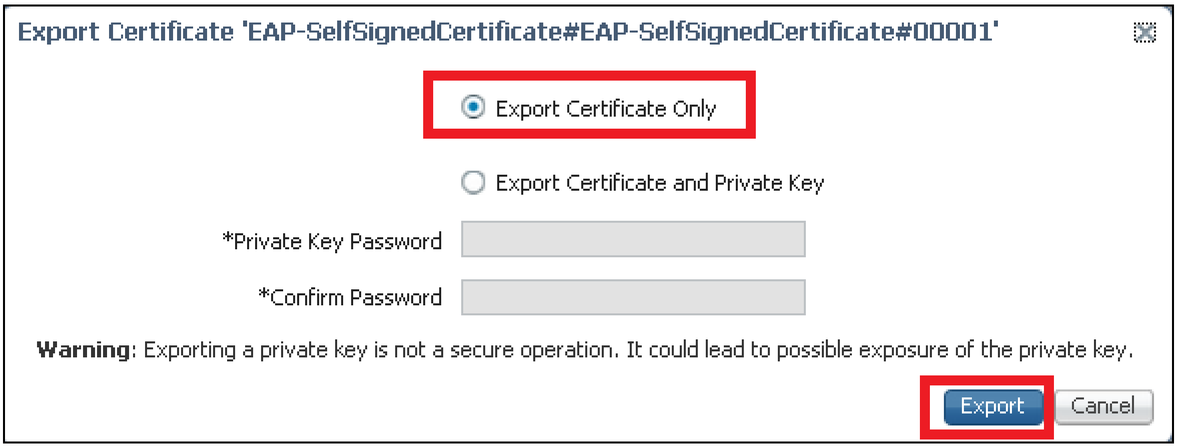
Em seguida, escolha o certificado usado para a **Autenticação EAP** e clique em **Exportar** como mostrado na imagem.



System Certificates ⚠ For disaster recovery it is recommended to export certificate ar

	Friendly Name	Used By	Portal group tag	
▼ [redacted]				
☑	EAP-SelfSignedCertificate#EAP-SelfSignedCertificate#00001	EAP Authentication		EAI

Salve o certificado no local necessário. Esse certificado deve ser instalado na máquina com Windows, como mostrado na imagem.


Export Certificate 'EAP-SelfSignedCertificate#EAP-SelfSignedCertificate#00001'

● Export Certificate Only

○ Export Certificate and Private Key

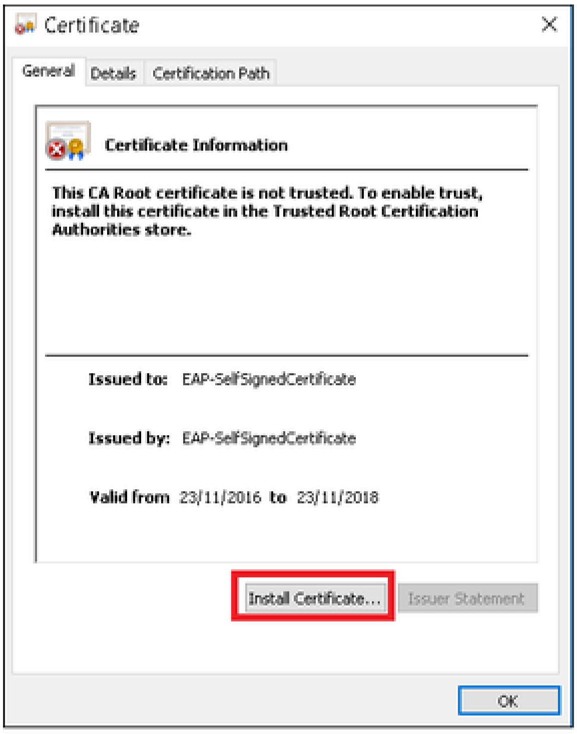
*Private Key Password

*Confirm Password

Warning: Exporting a private key is not a secure operation. It could lead to possible exposure of the private key.

Etapa 2. Instale o certificado na máquina Windows.

Copie o certificado exportado do ISE para a máquina Windows, altere a extensão do arquivo de .pem para .crt e, depois disso, clique duas vezes para instalá-lo como mostrado na imagem.



Certificate

General | Details | Certification Path

Certificate Information

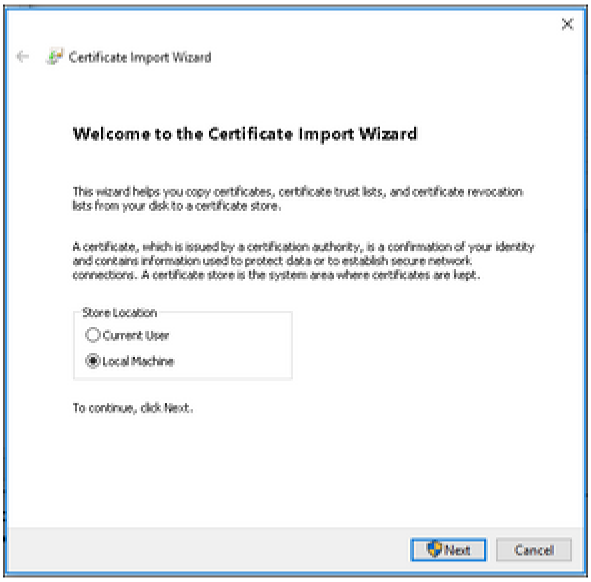
This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.

Issued to: EAP-SelfSignedCertificate

Issued by: EAP-SelfSignedCertificate

Valid from 23/11/2016 to 23/11/2018

Etapa 3. Selecione instalá-lo na **máquina local** e clique em **Avançar** como mostrado na imagem.



Certificate Import Wizard

Welcome to the Certificate Import Wizard

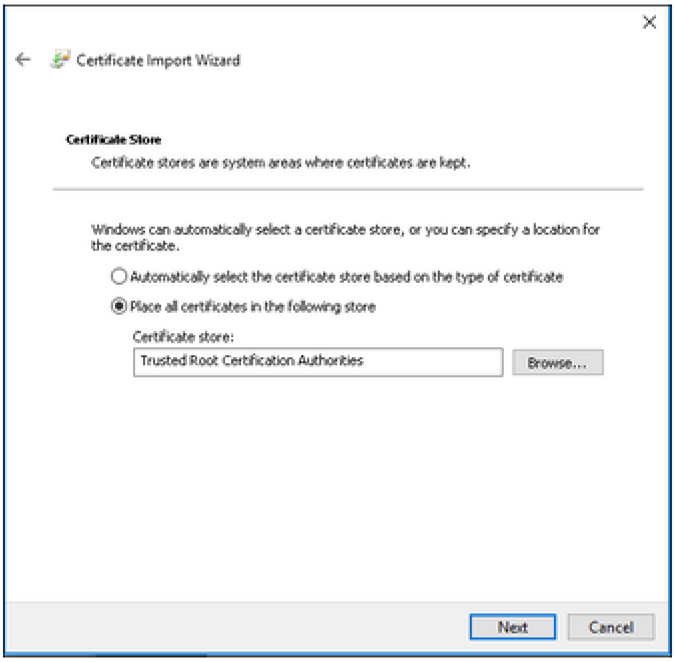
This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

Store Location
○ Current User
● Local Machine

To continue, click Next.

Etapa 4. Selecione **Place all certificates in this store**, depois procure e selecione **Trusted Root Certification Authorities.** Depois disso, clique em **Avançar** conforme mostrado na imagem.



Certificate Store

Certificate stores are system areas where certificates are kept.

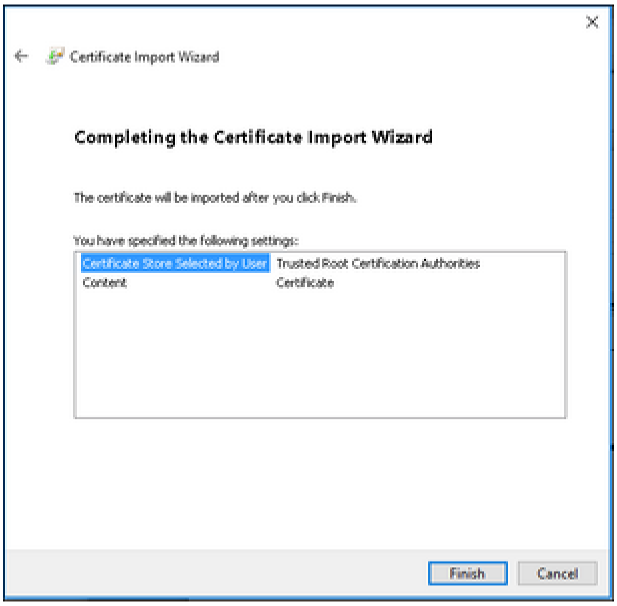
Windows can automatically select a certificate store, or you can specify a location for the certificate.

○ Automatically select the certificate store based on the type of certificate

● Place all certificates in the following store

Certificate store: Trusted Root Certification Authorities

Etapa 5. Em seguida, clique em **Finish** conforme mostrado na imagem.



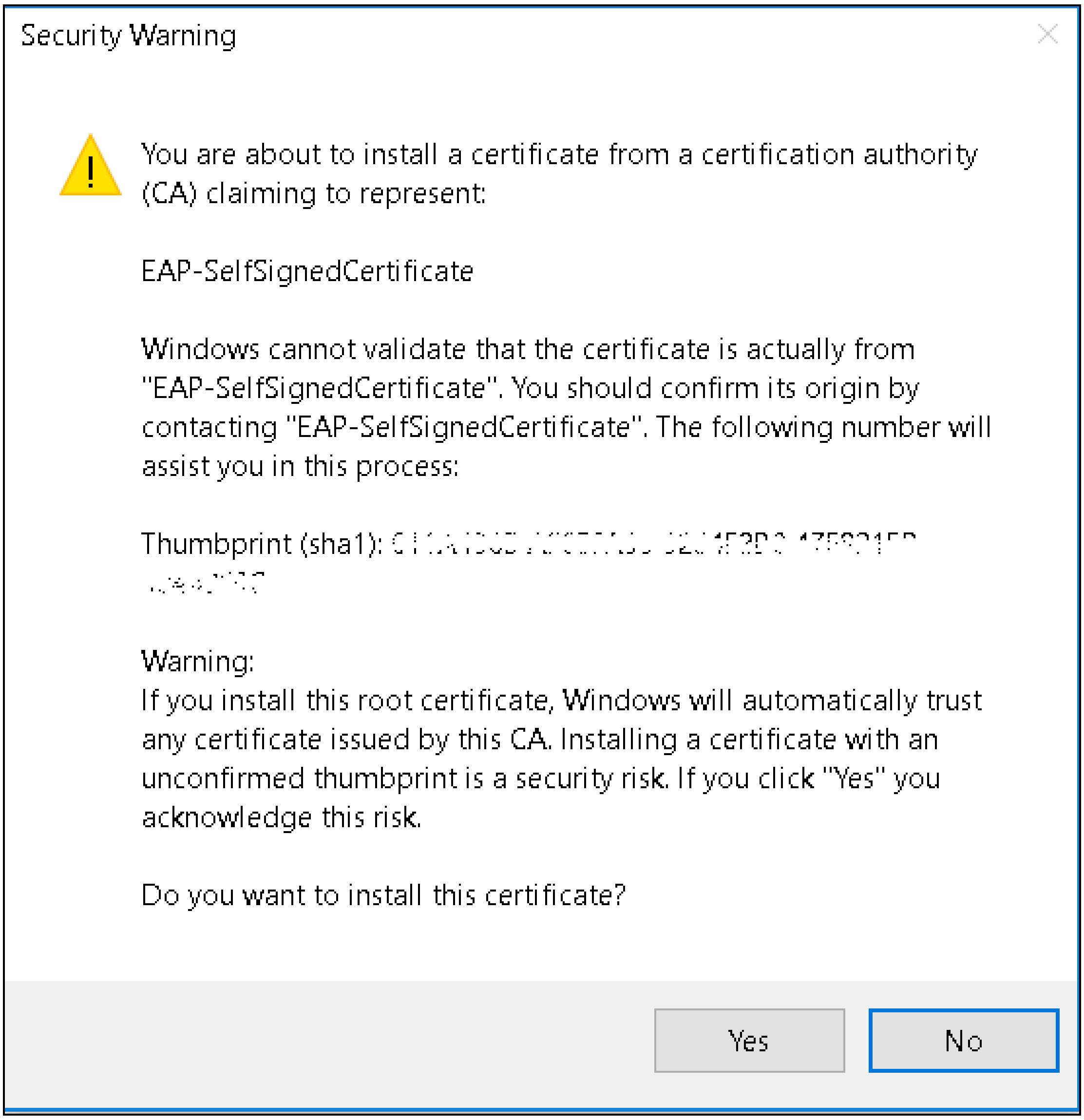
Completing the Certificate Import Wizard

The certificate will be imported after you click Finish.

You have specified the following settings:

Certificate Store Selected by User	Trusted Root Certification Authorities
Content	Certificate

Etapa 6. Confirme a instalação do certificado. Clique em **Sim** como mostrado na imagem.



Security Warning

You are about to install a certificate from a certification authority (CA) claiming to represent:

EAP-SelfSignedCertificate

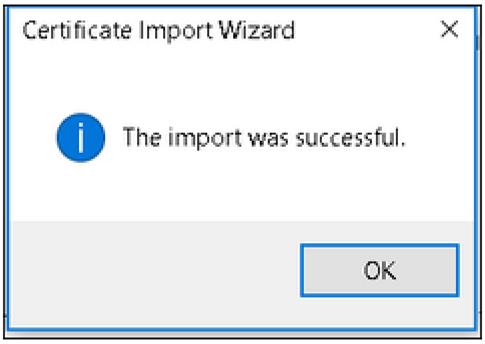
Windows cannot validate that the certificate is actually from "EAP-SelfSignedCertificate". You should confirm its origin by contacting "EAP-SelfSignedCertificate". The following number will assist you in this process:

Thumbprint (sha1): [redacted]

Warning:
If you install this root certificate, Windows will automatically trust any certificate issued by this CA. Installing a certificate with an unconfirmed thumbprint is a security risk. If you click "Yes" you acknowledge this risk.

Do you want to install this certificate?

Passo 7. Finalmente, clique em **OK** conforme mostrado na imagem.

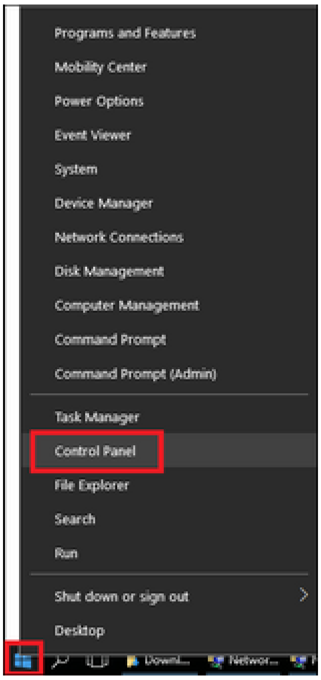


Certificate Import Wizard

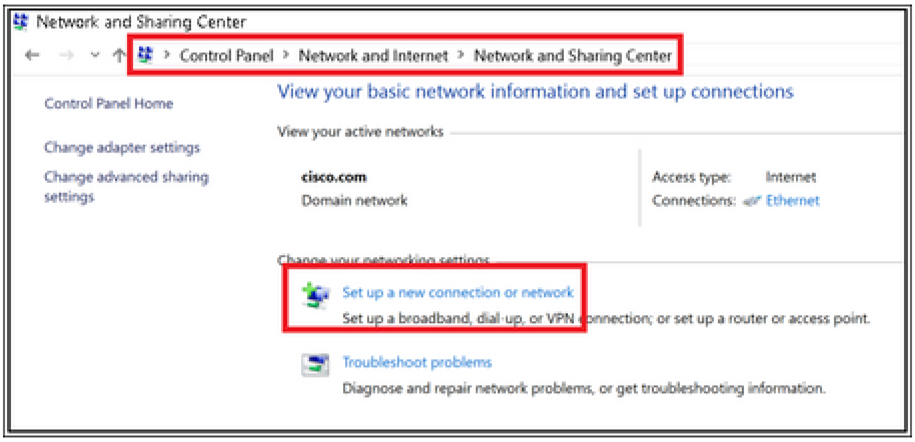
The import was successful.

Configuração do dispositivo final - Criar o perfil da WLAN

Etapa 1. Clique com o botão direito do mouse no ícone **Iniciar** e selecione **Painel de Controle** como mostrado na imagem.



Etapa 2. Navegue até **Rede e Internet** e depois navegue até **Central de Rede e Compartilhamento** e clique em **Configurar uma nova conexão ou rede** como mostrado na imagem.


Network and Sharing Center
Control Panel > Network and Internet > Network and Sharing Center
Control Panel Home
Change adapter settings
Change advanced sharing settings

View your basic network information and set up connections

View your active networks

cisco.com
Domain network

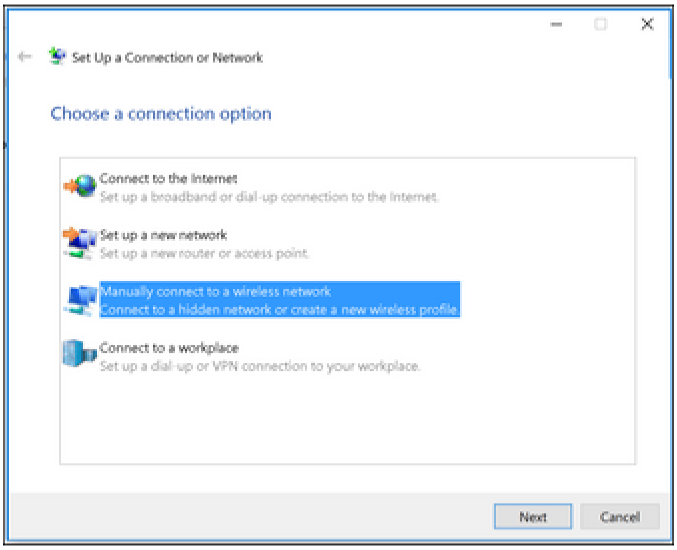
Access type: Internet
Connections: Ethernet

Change your networking settings

Set up a new connection or network
Set up a broadband, dial-up, or VPN connection; or set up a router or access point.

Troubleshoot problems
Diagnose and repair network problems, or get troubleshooting information.

Etapa 3. Selecione **Conectar manualmente a uma rede sem fio** e clique em **Avançar** conforme mostrado na imagem.



Choose a connection option

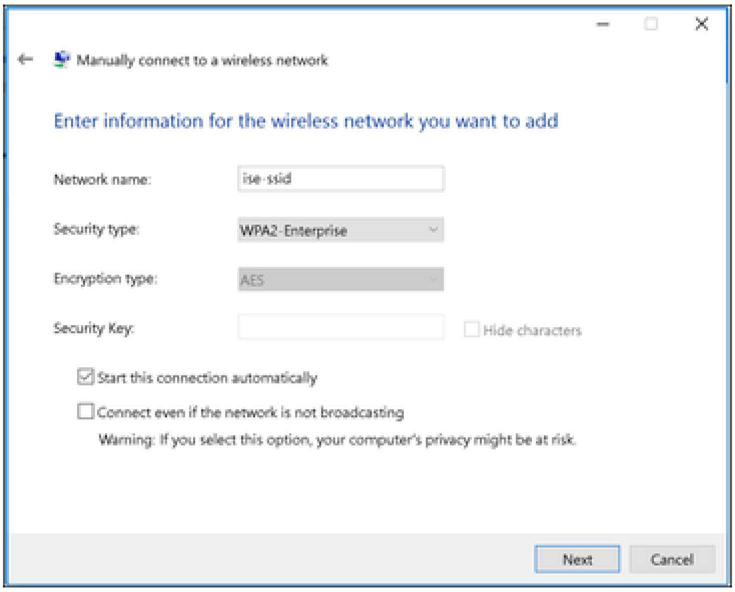
Connect to the Internet
Set up a broadband or dial-up connection to the Internet.

Set up a new network
Set up a new router or access point.

Manually connect to a wireless network
Connect to a hidden network or create a new wireless profile

Connect to a workplace
Set up a dial-up or VPN connection to your workplace.

Etapa 4. Insira as informações com o nome do SSID e o tipo de segurança WPA2-Enterprise e clique em **Avançar**, como mostrado na imagem.



Manually connect to a wireless network

Enter information for the wireless network you want to add

Network name: ise-ssid

Security type: WPA2-Enterprise

Encryption type: AES

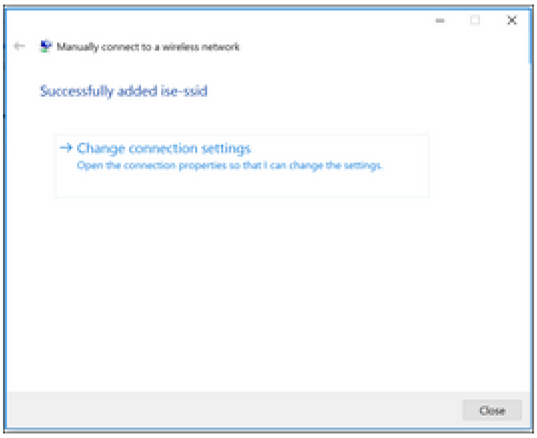
Security Key: □ Hide characters

☑ Start this connection automatically

□ Connect even if the network is not broadcasting

Warning: If you select this option, your computer's privacy might be at risk.

Etapa 5. Selecione **Change connection settings** para personalizar a configuração do perfil de WLAN conforme mostrado na imagem.

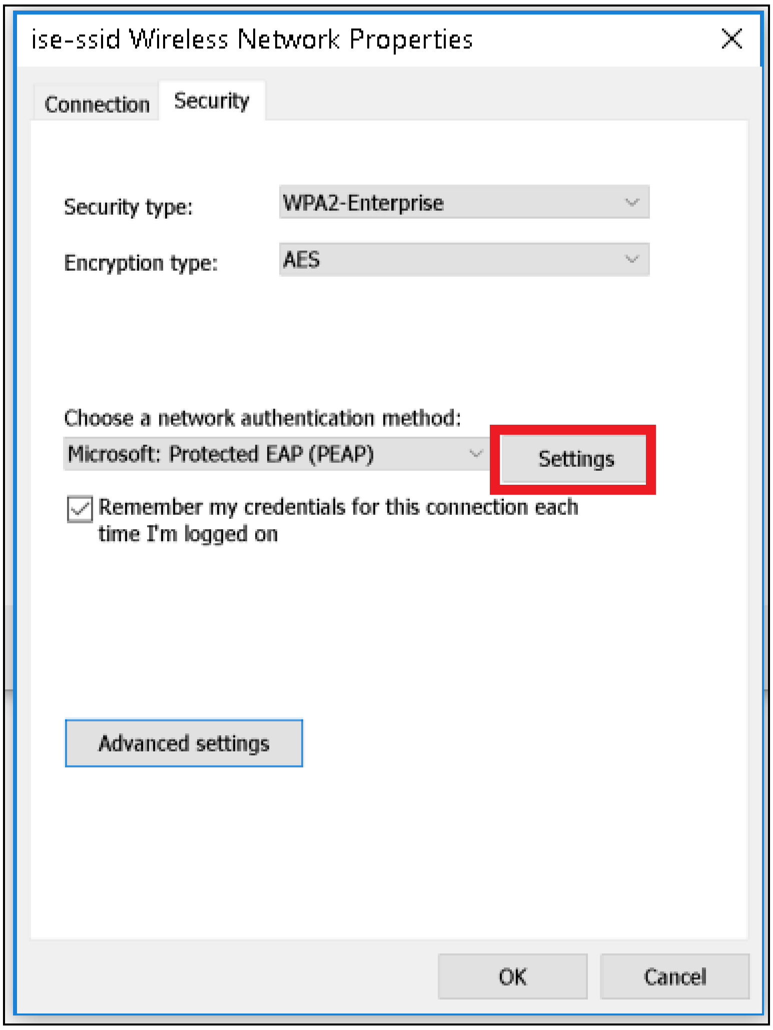


Manually connect to a wireless network

Successfully added ise-ssid

→ Change connection settings
Open the connection properties so that I can change the settings.

Etapa 6. Navegue até a guia **Segurança** e clique em **Configurações** conforme mostrado na imagem.



ise-ssid Wireless Network Properties

Security type: WPA2-Enterprise

Encryption type: AES

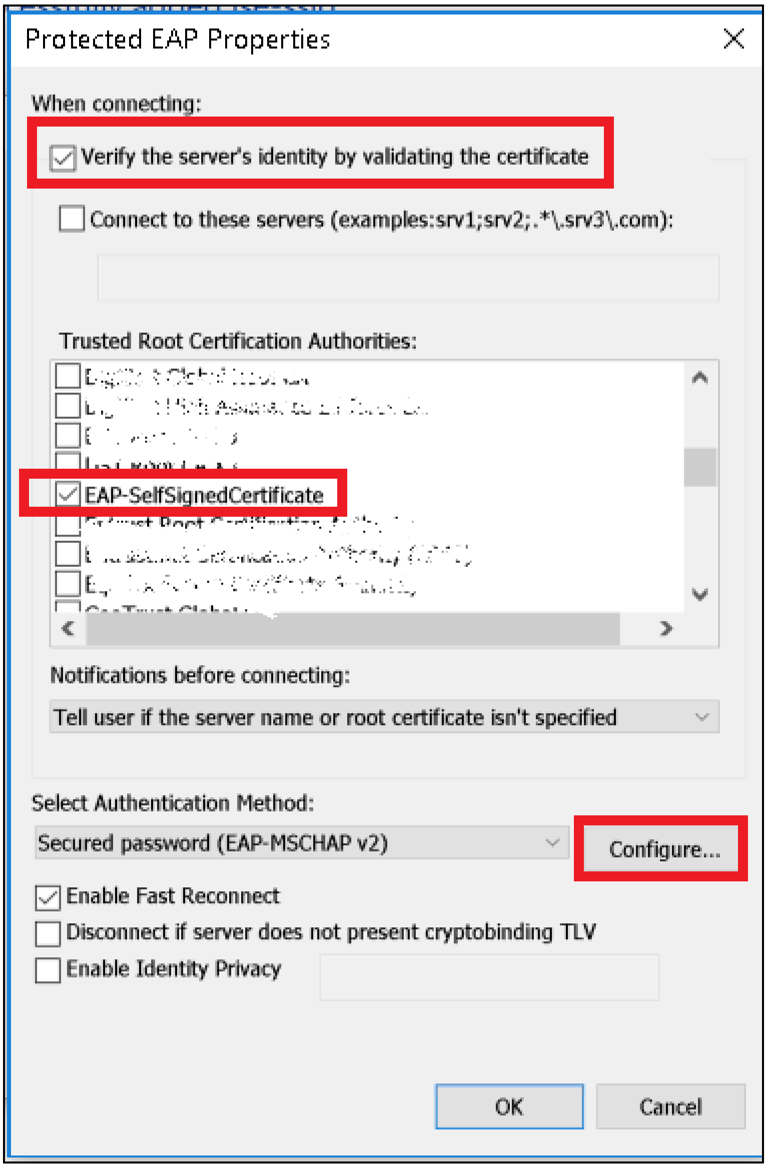
Choose a network authentication method: Microsoft: Protected EAP (PEAP)

☑ Remember my credentials for this connection each time I'm logged on

Passo 7. Selecione se o servidor RADIUS está validado ou não.

Em caso afirmativo, habilite **Verificar a identidade do servidor validando o certificado** e na lista **Autoridades de certificação raiz confiáveis:** selecione o certificado autoassinado do ISE.

Depois disso, selecione **Configurar** e desabilitar **Usar automaticamente meu nome e senha de login do Windows...** e clique em **OK** conforme mostrado nas imagens.



Protected EAP Properties

When connecting:

☑ Verify the server's identity by validating the certificate

□ Connect to these servers (examples:srv1;srv2;.*\.srv3\.com):

Trusted Root Certification Authorities:

□ [illegible]
□ [illegible]
□ [illegible]
□ [illegible]
☑ EAP-SelfSignedCertificate
□ [illegible]
□ [illegible]
□ [illegible]
□ [illegible]

Notifications before connecting:

Tell user if the server name or root certificate isn't specified

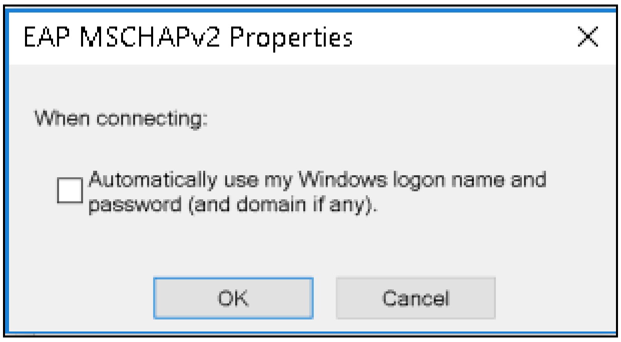
Select Authentication Method:

Secured password (EAP-MSCHAP v2)

☑ Enable Fast Reconnect

□ Disconnect if server does not present cryptobinding TLV

□ Enable Identity Privacy



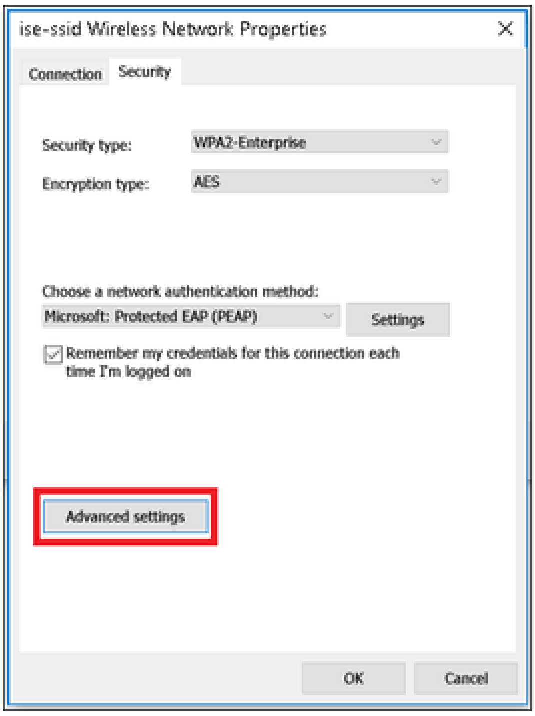
EAP MSCHAPv2 Properties

When connecting:

□ Automatically use my Windows logon name and password (and domain if any).

Etapa 8. Configure as credenciais do usuário.

Voltando à guia **Security**, selecione **Advanced settings**, especifique o modo de autenticação como User authentication e **save** as credenciais que foram configuradas no ISE para autenticar o usuário como mostrado nas imagens.



ise-ssid Wireless Network Properties

Connection | Security

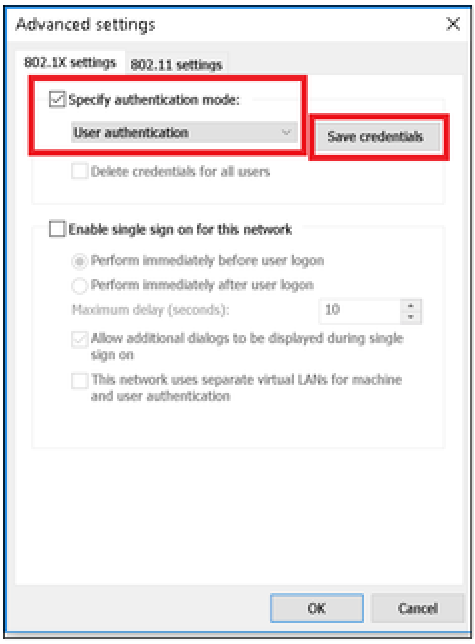
Security type: WPA2-Enterprise

Encryption type: AES

Choose a network authentication method:

Microsoft: Protected EAP (PEAP)

☑ Remember my credentials for this connection each time I'm logged on



Advanced settings

802.1X settings | 802.11 settings

☑ Specify authentication mode:

User authentication

☐ Delete credentials for all users

☐ Enable single sign on for this network

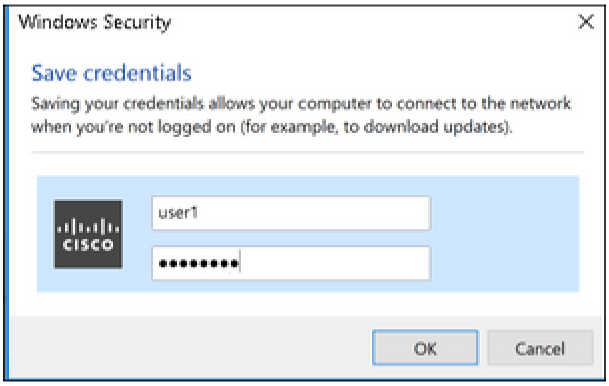
● Perform immediately before user logon

○ Perform immediately after user logon

Maximum delay (seconds): 10

☑ Allow additional dialogs to be displayed during single sign on

☐ This network uses separate virtual LANs for machine and user authentication



Windows Security

Save credentials

Saving your credentials allows your computer to connect to the network when you're not logged on (for example, to download updates).

user1

•••••••••

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

O fluxo de autenticação pode ser verificado da WLC ou da perspectiva do ISE.

Processo de autenticação no WLC

Execute os próximos comandos para monitorar o processo de autenticação para um usuário específico:

```
> debug client <mac-add-client>
> debug dot1x event enable
> debug dot1x aaa enable
```

Exemplo de uma autenticação bem-sucedida (parte da saída foi omitida):

<#root>

```
*apfMsConnTask_1: Nov 24 04:30:44.317:

e4:b3:18:7c:30:58 Processing assoc-req station:e4:b3:18:7c:30:58 AP:00:c8:8b:26:2c:d0-00

 thread:1a5cc288
*apfMsConnTask_1: Nov 24 04:30:44.317: e4:b3:18:7c:30:58 Reassociation received from mobile on BSSID 00:
*apfMsConnTask_1: Nov 24 04:30:44.318: e4:b3:18:7c:30:58 Applying Interface(management) policy on Mobile
*apfMsConnTask_1: Nov 24 04:30:44.318: e4:b3:18:7c:30:58 Applying site-specific Local Bridging override
*apfMsConnTask_1: Nov 24 04:30:44.318: e4:b3:18:7c:30:58 Applying Local Bridging Interface Policy for st
*apfMsConnTask_1: Nov 24 04:30:44.318: e4:b3:18:7c:30:58 RSN Capabilities:  60
*apfMsConnTask_1: Nov 24 04:30:44.318: e4:b3:18:7c:30:58 Marking Mobile as non-

e4:b3:18:7c:30:58 Received 802.11i 802.1X key management suite, enabling dot1x Authentication

11w Capable
*apfMsConnTask_1: Nov 24 04:30:44.318: e4:b3:18:7c:30:58 Received RSN IE with 1 PMKIDs from mobile e4:b3
*apfMsConnTask_1: Nov 24 04:30:44.319: Received PMKID:  (16)
*apfMsConnTask_1: Nov 24 04:30:44.319: e4:b3:18:7c:30:58 Searching for PMKID in MSCB PMKID cache for mob
*apfMsConnTask_1: Nov 24 04:30:44.319: e4:b3:18:7c:30:58 No valid PMKID found in the MSCB PMKID cache fo
*apfMsConnTask_1: Nov 24 04:30:44.319: e4:b3:18:7c:30:58 0.0.0.0 START (0) Initializing policy
*apfMsConnTask_1: Nov 24 04:30:44.319:

e4:b3:18:7c:30:58 0.0.0.0 START (0) Change state to AUTHCHECK (2) last state START (0)

*apfMsConnTask_1: Nov 24 04:30:44.319:

e4:b3:18:7c:30:58 0.0.0.0 AUTHCHECK (2) Change state to 8021X_REQD (3) last state AUTHCHECK (2)

*apfMsConnTask_1: Nov 24 04:30:44.319: e4:b3:18:7c:30:58 0.0.0.0 8021X_REQD (3) Plumbed mobile LWAPP rul
*apfMsConnTask_1: Nov 24 04:30:44.319: e4:b3:18:7c:30:58 apfMsAssoStateInc
*apfMsConnTask_1: Nov 24 04:30:44.319: e4:b3:18:7c:30:58 apfPemAddUser2 (apf_policy.c:437) Changing stat
*apfMsConnTask_1: Nov 24 04:30:44.319: e4:b3:18:7c:30:58 apfPemAddUser2:session timeout forstation e4:b3
*apfMsConnTask_1: Nov 24 04:30:44.319: e4:b3:18:7c:30:58 Stopping deletion of Mobile Station: (callerId:
*apfMsConnTask_1: Nov 24 04:30:44.319: e4:b3:18:7c:30:58 Func: apfPemAddUser2, Ms Timeout = 0, Session T
*apfMsConnTask_1: Nov 24 04:30:44.320: e4:b3:18:7c:30:58 Sending Assoc Response to station on BSSID 00:c
*spamApTask2: Nov 24 04:30:44.323: e4:b3:18:7c:30:58 Successful transmission of LWAPP Add-Mobile to AP 0
*spamApTask2: Nov 24 04:30:44.325: e4:b3:18:7c:30:58 Received ADD_MOBILE ack - Initiating 1x to STA e4:b
*spamApTask2: Nov 24 04:30:44.325: e4:b3:18:7c:30:58

Sent dot1x auth initiate message for mobile e4:b3:18:7c:30:58

*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.326: e4:b3:18:7c:30:58 reauth_sm state transition 0 ---> 1 for mobi
```

```
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.326: e4:b3:18:7c:30:58 EAP-PARAM Debug - eap-params for Wlan-Id :2
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.326: e4:b3:18:7c:30:58 Disable re-auth, use PMK lifetime.
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.326: e4:b3:18:7c:30:58 Station e4:b3:18:7c:30:58 setting dot1x reau
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.326: e4:b3:18:7c:30:58 Stopping reauth timeout for e4:b3:18:7c:30:5
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.326: e4:b3:18:7c:30:58 dot1x - moving mobile e4:b3:18:7c:30:58 into
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.326:
```

e4:b3:18:7c:30:58 Sending EAP-Request/Identity to mobile e4:b3:18:7c:30:58 (EAP Id 1)

```
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.380: e4:b3:18:7c:30:58 Received EAPOL EAPPKT from mobile e4:b3:18:7
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.380: e4:b3:18:7c:30:58 Received Identity Response (count=1) from mo
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.380: e4:b3:18:7c:30:58 Resetting reauth count 1 to 0 for mobile e4:
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.380: e4:b3:18:7c:30:58 EAP State update from Connecting to Authenti
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.380: e4:b3:18:7c:30:58 dot1x - moving mobile e4:b3:18:7c:30:58 into
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.380: e4:b3:18:7c:30:58 Entering Backend Auth Response state for mob
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.380: e4:b3:18:7c:30:58 Created Acct-Session-ID (58366cf4/e4:b3:18:7
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.386: e4:b3:18:7c:30:58 Processing Access-Challenge for mobile e4:b3
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.387: e4:b3:18:7c:30:58 Entering Backend Auth Req state (id=215) for
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.387: e4:b3:18:7c:30:58 WARNING: updated EAP-Identifier 1 ===> 215 f
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.387: e4:b3:18:7c:30:58 Sending EAP Request from AAA to mobile e4:b3
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.387: e4:b3:18:7c:30:58 Allocating EAP Pkt for retransmission to mob
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.390: e4:b3:18:7c:30:58 Received EAPOL EAPPKT from mobile e4:b3:18:7
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.390: e4:b3:18:7c:30:58 Received EAP Response from mobile e4:b3:18:7
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.390: e4:b3:18:7c:30:58 Resetting reauth count 0 to 0 for mobile e4:
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.390: e4:b3:18:7c:30:58 Entering Backend Auth Response state for mob
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.393: e4:b3:18:7c:30:58 Processing Access-Challenge for mobile e4:b3
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.393: e4:b3:18:7c:30:58 Entering Backend Auth Req state (id=216) for
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.393: e4:b3:18:7c:30:58 Sending EAP Request from AAA to mobile e4:b3
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.393: e4:b3:18:7c:30:58 Reusing allocated memory for  EAP Pkt for re
.
.
.
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.530:
```

e4:b3:18:7c:30:58 Processing Access-Accept for mobile e4:b3:18:7c:30:58

```
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.530: e4:b3:18:7c:30:58 Resetting web IPv4 acl from 255 to 255
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.530: e4:b3:18:7c:30:58 Resetting web IPv4 Flex acl from 65535 to 65
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.530:
```

e4:b3:18:7c:30:58 Username entry (user1) created for mobile, length = 253

```
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.530:
```

e4:b3:18:7c:30:58 Found an interface name:'vlan2404' corresponds to interface name received: vlan2404

```
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.530: e4:b3:18:7c:30:58 override for default ap group, marking intgr
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.530: e4:b3:18:7c:30:58 Applying Interface(management) policy on Mob
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.530: e4:b3:18:7c:30:58 Re-applying interface policy for client
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 apfApplyWlanPolicy: Apply WLAN Policy over P
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531:
```

e4:b3:18:7c:30:58 Inserting AAA Override struct for mobile

```
        MAC: e4:b3:18:7c:30:58, source 4
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 Applying override policy from source Overrid
*Dot1x_NW_MsgTask_0: Nov 24
```

04:30:44.531: e4:b3:18:7c:30:58 Found an interface name:'vlan2404' corresponds to interface name receive

```
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 Applying Interface(vlan2404) policy on Mobil
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 Re-applying interface policy for client
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 Setting re-auth timeout to 0 seconds, got fr
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 Station e4:b3:18:7c:30:58 setting dot1x reau
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 Stopping reauth timeout for e4:b3:18:7c:30:5
```

```
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 Creating a PKC PMKID Cache entry for station
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 Resetting MSCB PMK Cache Entry 0 for station
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 Adding BSSID 00:c8:8b:26:2c:d1 to PMKID cach
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531: New PMKID: (16)
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531:      [0000] cc 3a 3d 26 80 17 8b f1 2d c5 cd fd a0 8a c4 39
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 unsetting PmkIdValidatedByAp
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 Updating AAA Overrides from local for statio
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 Adding Audit session ID payload in Mobility
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 0 PMK-update groupcast messages sent
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 PMK sent to mobility group
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 Disabling re-auth since PMK lifetime can tak
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 Sending EAP-Success to mobile e4:b3:18:7c:30
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.532: e4:b3:18:7c:30:58 Freeing AAACB from Dot1xCB as AAA auth is do
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.532: e4:b3:18:7c:30:58 key Desc Version FT - 0
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.532: e4:b3:18:7c:30:58 Found an cache entry for BSSID 00:c8:8b:26:2
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.532: Including PMKID in M1  (16)
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.532:      [0000] cc 3a 3d 26 80 17 8b f1 2d c5 cd fd a0 8a c4 39
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.532: M1 - Key Data: (22)
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.532:      [0000] dd 14 00 0f ac 04 cc 3a 3d 26 80 17 8b f1 2d c5
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.532:      [0016] cd fd a0 8a c4 39
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.532:
```

e4:b3:18:7c:30:58 Starting key exchange to mobile e4:b3:18:7c:30:58, data packets will be dropped

```
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.532:
```

e4:b3:18:7c:30:58 Sending EAPOL-Key Message to mobile e4:b3:18:7c:30:58

```
state INITPMK (message 1), replay counter 00.00.00.00.00.00.00.00
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.532: e4:b3:18:7c:30:58 Reusing allocated memory for  EAP Pkt for re
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.532: e4:b3:18:7c:30:58 Entering Backend Auth Success state (id=223)
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.532: e4:b3:18:7c:30:58 Received Auth Success while in Authenticatin
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.532: e4:b3:18:7c:30:58 dot1x - moving mobile e4:b3:18:7c:30:58 into
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.547: e4:b3:18:7c:30:58 Received EAPOL-Key from mobile e4:b3:18:7c:3
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.547: e4:b3:18:7c:30:58 Ignoring invalid EAPOL version (1) in EAPOL-
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.547: e4:b3:18:7c:30:58 key Desc Version FT - 0
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.547:
```

e4:b3:18:7c:30:58 Received EAPOL-key in PTK_START state (message 2) from mobile

```
 e4:b3:18:7c:30:58
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.548: e4:b3:18:7c:30:58 Successfully computed PTK from PMK!!!
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.548: e4:b3:18:7c:30:58 Received valid MIC in EAPOL Key Message M2!!
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.548: e4:b3:18:7c:30:58 Not Flex client. Do not distribute PMK Key c
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.548: e4:b3:18:7c:30:58 Stopping retransmission timer for mobile e4:
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.548: e4:b3:18:7c:30:58 key Desc Version FT - 0
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.548: e4:b3:18:7c:30:58 Sending EAPOL-Key Message to mobile e4:b3:18
state PTKINITNEGOTIATING (message 3), replay counter 00.00.00.00.00.00.00.01
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.548: e4:b3:18:7c:30:58 Reusing allocated memory for  EAP Pkt for re
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.555: e4:b3:18:7c:30:58 Received EAPOL-Key from mobile e4:b3:18:7c:3
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.555: e4:b3:18:7c:30:58 Ignoring invalid EAPOL version (1) in EAPOL-
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.555: e4:b3:18:7c:30:58 key Desc Version FT - 0
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.555:
```

e4:b3:18:7c:30:58 Received EAPOL-key in PTKINITNEGOTIATING state (message 4)

```
 from mobile e4:b3:18:7c:30:58
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.555: e4:b3:18:7c:30:58 Stopping retransmission timer for mobile e4:
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.555: e4:b3:18:7c:30:58 Freeing EAP Retransmit Bufer for mobile e4:b
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.555: e4:b3:18:7c:30:58 apfMs1xStateInc
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.555: e4:b3:18:7c:30:58 apfMsPeapSimReqCntInc
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.555: e4:b3:18:7c:30:58 apfMsPeapSimReqSuccessCntInc
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.555:
```

e4:b3:18:7c:30:58 0.0.0.0 8021X_REQD (3) Change state to L2AUTHCOMPLETE (4) last state 8021X_REQD (3)

```
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.555: e4:b3:18:7c:30:58 Mobility query, PEM State: L2AUTHCOMPLETE
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.555: e4:b3:18:7c:30:58 Building Mobile Announce :
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.556: e4:b3:18:7c:30:58   Building Client Payload:
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.556: e4:b3:18:7c:30:58     Client Ip: 0.0.0.0
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.556: e4:b3:18:7c:30:58     Client Vlan Ip: 172.16.0.134, Vlan mask
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.556: e4:b3:18:7c:30:58     Client Vap Security: 16384
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.556: e4:b3:18:7c:30:58     Virtual Ip: 10.10.10.10
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.556: e4:b3:18:7c:30:58     ssid: ise-ssid
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.556: e4:b3:18:7c:30:58   Building VlanIpPayload.
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.556: e4:b3:18:7c:30:58 Not Using WMM Compliance code qosCap 00
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.556: e4:b3:18:7c:30:58 0.0.0.0 L2AUTHCOMPLETE (4) Plumbed mobile LW
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.556:
```

e4:b3:18:7c:30:58 0.0.0.0 L2AUTHCOMPLETE (4) Change state to DHCP_REQD (7) last state L2AUTHCOMPLETE (4)

```
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.556: e4:b3:18:7c:30:58 0.0.0.0 DHCP_REQD (7) pemAdvanceState2 6677,
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.556: e4:b3:18:7c:30:58 0.0.0.0 DHCP_REQD (7) Adding Fast Path rule
  type = Airespace AP - Learn IP address
  on AP 00:c8:8b:26:2c:d0, slot 0, interface = 1, QOS = 0
  IPv4 ACL ID = 255, IPv
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.556: e4:b3:18:7c:30:58 0.0.0.0 DHCP_REQD (7) Fast Path rule (contd.
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.556: e4:b3:18:7c:30:58 0.0.0.0 DHCP_REQD (7) Fast Path rule (contd.
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.556: e4:b3:18:7c:30:58 0.0.0.0 DHCP_REQD (7) Successfully plumbed m
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.556: e4:b3:18:7c:30:58 Successfully Plumbed PTK session Keysfor mob
*spamApTask2: Nov 24 04:30:44.556: e4:b3:18:7c:30:58 Successful transmission of LWAPP Add-Mobile to AP 0
*pemReceiveTask: Nov 24 04:30:44.557: e4:b3:18:7c:30:58 0.0.0.0 Added NPU entry of type 9, dtlFlags 0x0
*apfReceiveTask: Nov 24 04:30:44.557: e4:b3:18:7c:30:58 0.0.0.0 DHCP_REQD (7) mobility role update reque
  Peer = 0.0.0.0, Old Anchor = 0.0.0.0, New Anchor = 172.16.0.3
*apfReceiveTask: Nov 24 04:30:44.557: e4:b3:18:7c:30:58 0.0.0.0 DHCP_REQD (7) State Update from Mobility
*apfReceiveTask: Nov 24 04:30:44.557: e4:b3:18:7c:30:58 0.0.0.0 DHCP_REQD (7) pemAdvanceState2 6315, Add
*apfReceiveTask: Nov 24 04:30:44.557: e4:b3:18:7c:30:58 0.0.0.0 DHCP_REQD (7) Replacing Fast Path rule
  IPv4 ACL ID = 255,
*apfReceiveTask: Nov 24 04:30:44.557: e4:b3:18:7c:30:58 0.0.0.0 DHCP_REQD (7) Fast Path rule (contd...)
*apfReceiveTask: Nov 24 04:30:44.557: e4:b3:18:7c:30:58 0.0.0.0 DHCP_REQD (7) Fast Path rule (contd...)
*apfReceiveTask: Nov 24 04:30:44.557: e4:b3:18:7c:30:58 0.0.0.0 DHCP_REQD (7) Successfully plumbed mobil
*pemReceiveTask: Nov 24 04:30:44.557: e4:b3:18:7c:30:58 Sent an XID frame
*dtlArpTask: Nov 24 04:30:47.932: e4:b3:18:7c:30:58 Static IP client associated to interface vlan2404 wh
*dtlArpTask: Nov 24 04:30:47.933: e4:b3:18:7c:30:58 apfMsRunStateInc
*dtlArpTask: Nov 24 04:30:47.933:
```

e4:b3:18:7c:30:58 172.16.0.151 DHCP_REQD (7) Change state to RUN (20)

```
 last state DHCP_REQD (7)
```

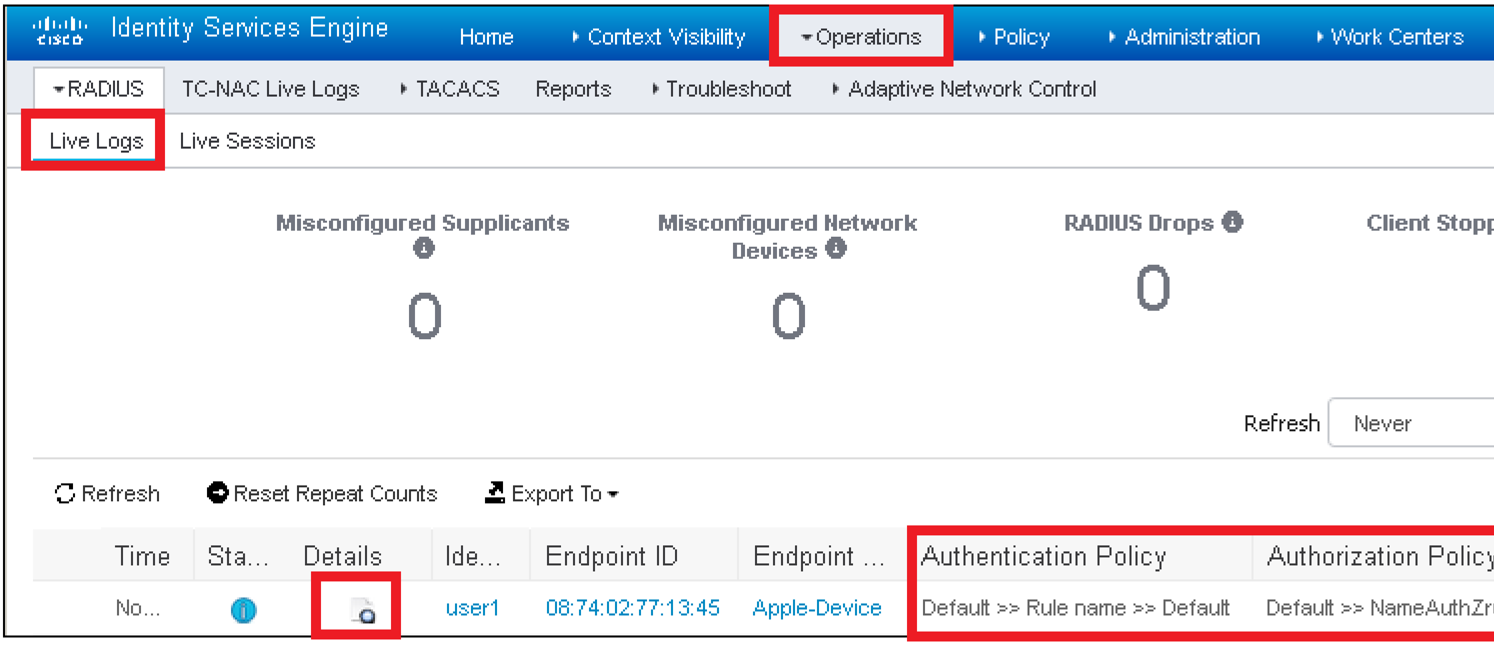
Para obter uma maneira fácil de ler as saídas do cliente de depuração, use a ferramenta de análise de depuração sem fio:

Wireless Debug Analyzer

Processo de autenticação no ISE

Navegue para **Operations** > **RADIUS** > **Live Logs** para ver qual política de autenticação, política de autorização e perfil de autorização foi atribuído ao usuário.

Para obter mais informações, clique em **Details** para ver um processo de autenticação mais detalhado, como mostrado na imagem.



Time	Sta...	Details	Ide...	Endpoint ID	Endpoint ...	Authentication Policy	Authorization Policy
No...			user1	08:74:02:77:13:45	Apple-Device	Default >> Rule name >> Default	Default >> NameAuthZr

Troubleshoot

No momento, não há informações específicas disponíveis para solucionar esse problema de configuração.

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.