

autenticação do 802.1x com o 2.1 PEAP, ISE e o WLC 8.3

Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Configurar](#)

[Diagrama de Rede](#)

[Configurações](#)

[Declare o servidor Radius no WLC](#)

[Crie o SSID](#)

[Declare o WLC no ISE](#)

[Crie um novo usuário no ISE](#)

[Crie a regra da autenticação](#)

[Crie o perfil da autorização](#)

[Crie a regra da autorização](#)

[Configuração do dispositivo final](#)

[Verificar](#)

[Processo de autenticação no WLC](#)

[Processo de autenticação no ISE](#)

Introdução

Isto documenta explica como estabelecer um WLAN (Wireless Local Area Network) com Segurança do 802.1x e ultrapassagem VLAN (rede de área local virtual) com PEAP (protocolo extensible authentication protegido) como EAP (protocolo extensible authentication).

Pré-requisitos

Cisco recomenda ter um conhecimento básico de:

- 802.1x
- PEAP
- Certification Authority (CA)
- Certificados

Requisitos

[Componentes Utilizados](#)

WLC v8.3.102.0

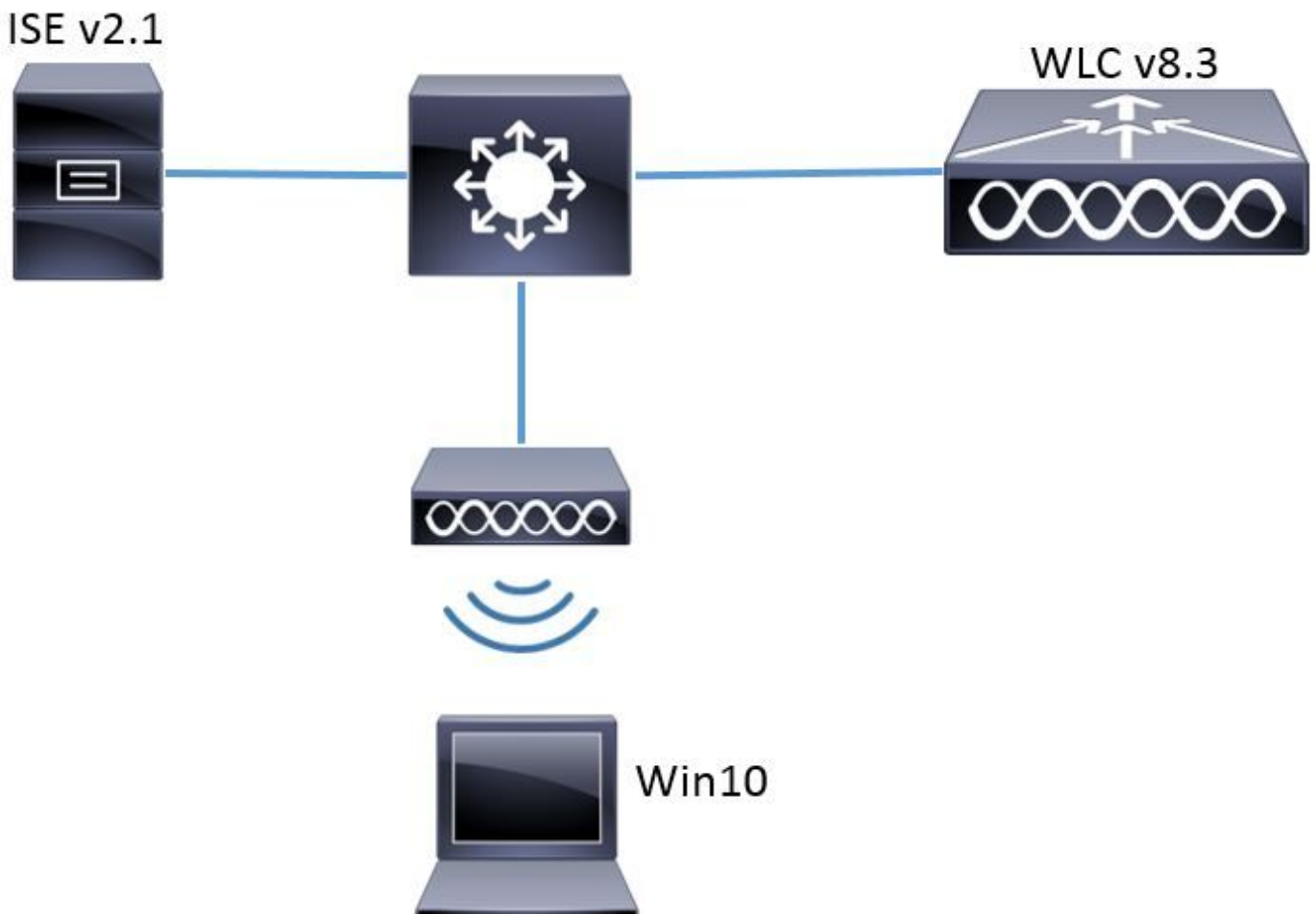
ISE v2.1

Portátil de Windows 10

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 sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Configurar

Diagrama de Rede



Configurações

As etapas gerais são:

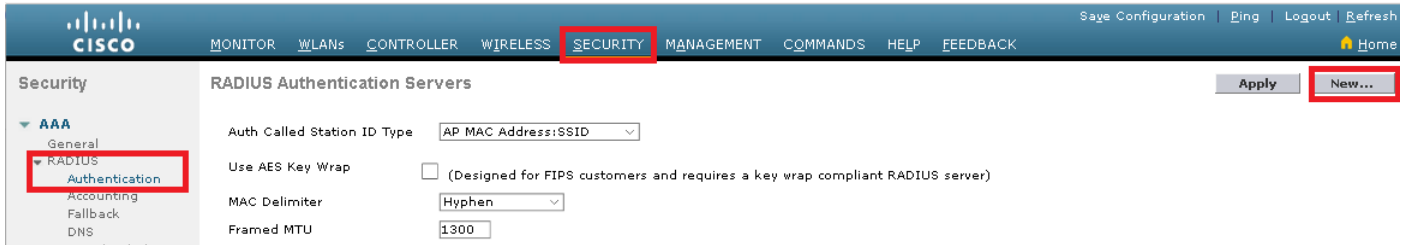
1. Declare o servidor Radius (ISE neste exemplo) no WLC e vice-versa para permitir um com o outro uma comunicação
2. Crie o SSID (Service Set Identifier) no WLC
3. Crie a regra da autenticação no ISE
4. Crie o perfil da autorização no ISE
5. Crie a regra da autorização no ISE
6. Configurar o valor-limite

Declare o servidor Radius no WLC

A fim permitir uma comunicação entre o servidor Radius e o WLC é precisado de registrar e vice-versa o servidor Radius no WLC.

GUI:

Etapa 1. Abra o GUI do WLC e navegue à **SEGURANÇA > ao RAIO > à autenticação > novo.**



Etapa 2. Encha a informação do servidor Radius.

RADIUS Authentication Servers > New

Server Index (Priority)

Server IP Address(Ipv4/Ipv6)

Shared Secret Format

Shared Secret

Confirm Shared Secret

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

Port Number

Server Status

Support for CoA

Server Timeout seconds

Network User Enable

Management Enable

Management Retransmit Timeout seconds

IPsec Enable

CLI:

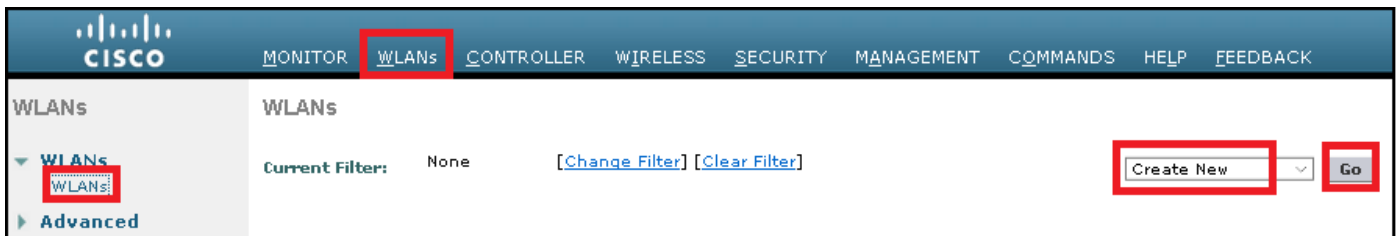
```
> config radius auth add <index> <a.b.c.d> 1812 ascii <shared-key>> config radius auth disable <index>> config radius auth retransmit-timeout <index> <timeout-seconds>> config radius auth enable <index>
```

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

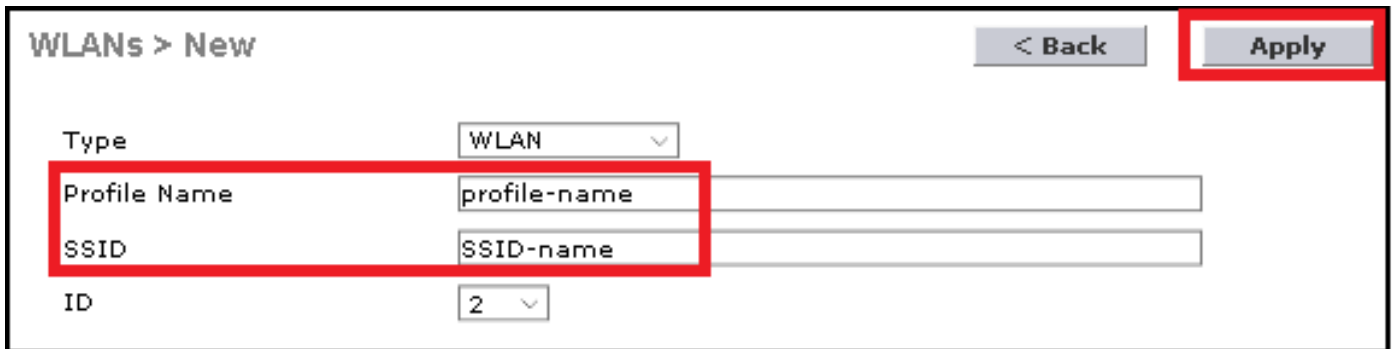
Crie o SSID

GUI:

Etapa 1. Abra o GUI do WLC e navegue a **WLAN > criam novo > vão.**



Etapa 2. Escolha um nome para o SSID e o perfil, a seguir clique-o **aplicam-se**.



CLI:

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

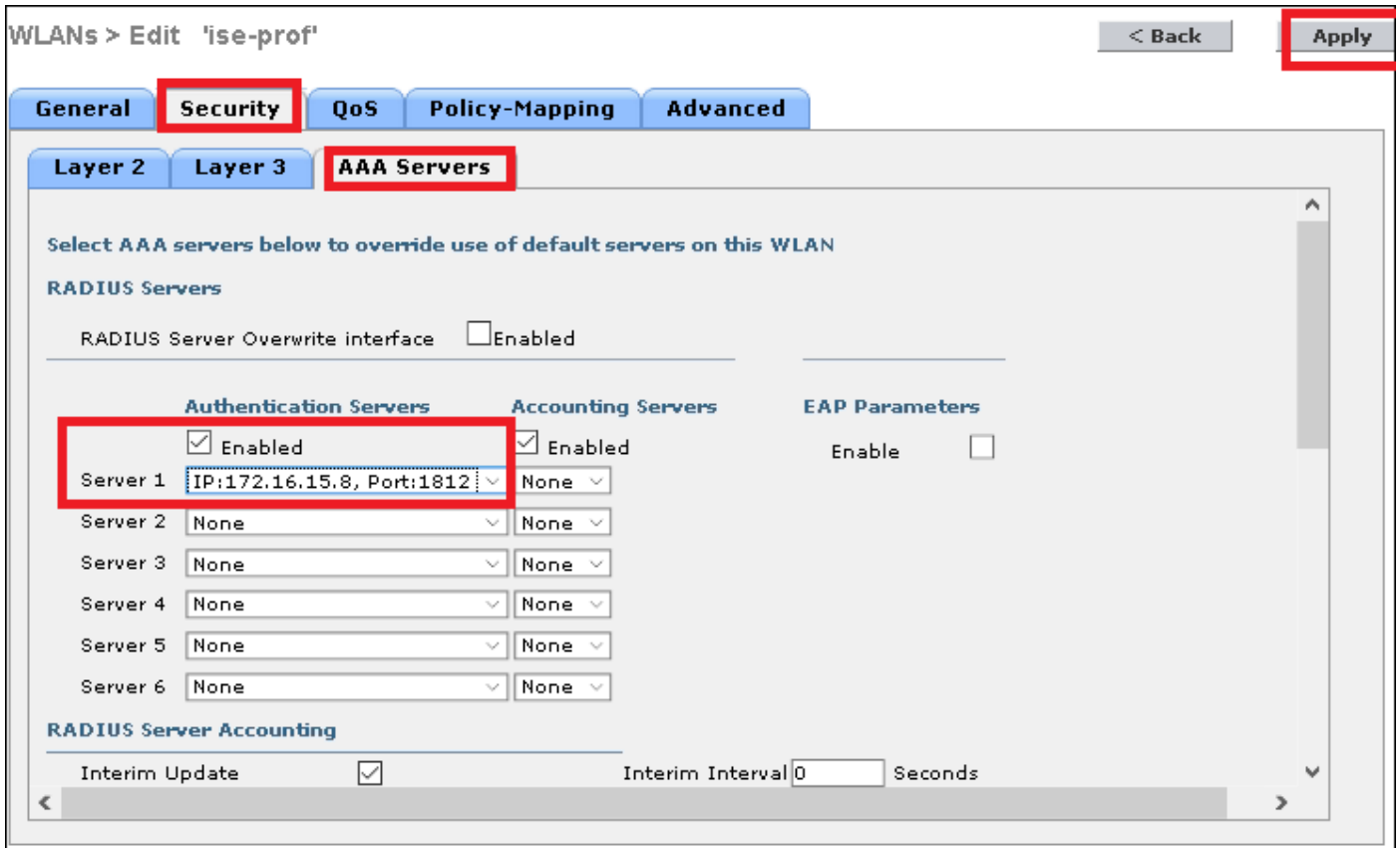
Etapa 3. Atribua o servidor Radius ao WLAN.

CLI:

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

GUI:

Navegue à **Segurança > aos servidores AAA** e escolha o servidor Radius desejado, a seguir a batida **aplica-se**.



Etapa 4. Aumente opcionalmente o timeout de sessão

CLI:

```
> config wlan session-timeout <wlan-id> <session-timeout-seconds>
```

GUI:

WLANs > Edit 'ise-prof' < Back Apply

General Security QoS Policy-Mapping **Advanced**

Allow AAA Override	<input type="checkbox"/> Enabled	DHCP	
Coverage Hole Detection	<input checked="" type="checkbox"/> Enabled	DHCP Server	<input type="checkbox"/> Override
Enable Session Timeout	<input checked="" type="checkbox"/> <input type="text" value="28800"/> Session Timeout (secs)	DHCP Addr. Assignment	<input type="checkbox"/> Required
Aironet IE	<input checked="" type="checkbox"/> Enabled	OEAP	
Diagnostic Channel	<input type="checkbox"/> Enabled	Split Tunnel	<input type="checkbox"/> Enabled
Override Interface ACL	IPv4 <input type="text" value="None"/> IPv6 <input type="text" value="None"/>	Management Frame Protection (MFP)	
Layer2 Ad	<input type="text" value="None"/>	MFP Client Protection	<input type="text" value="Optional"/>
URL ACL	<input type="text" value="None"/>	DTIM Period (in beacon intervals)	
P2P Blocking Action	<input type="text" value="Disabled"/>	802.11a/n (1 - 255)	<input type="text" value="1"/>
Client Exclusion	<input checked="" type="checkbox"/> Enabled <input type="text" value="60"/> Timeout Value (secs)	802.11b/g/n (1 - 255)	<input type="text" value="1"/>
Maximum Allowed Clients	<input type="text" value="0"/>	NAC	
Static IP Tunneling	<input type="checkbox"/>	NAC State	<input type="text" value="None"/>

Etapa 5. Permite o WLAN

CLI:

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

GUI:

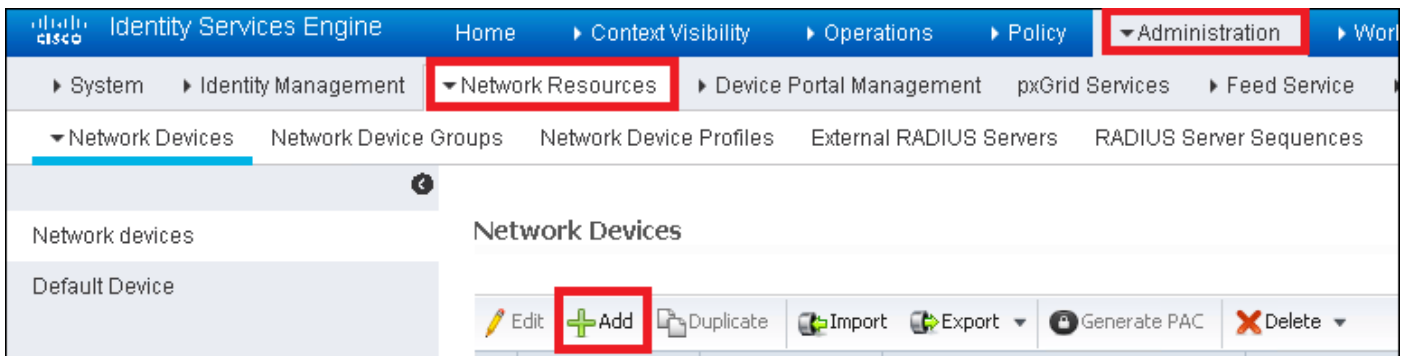
WLANs > Edit 'ise-prof' < Back Apply

General Security QoS Policy-Mapping **Advanced**

Profile Name	<input type="text" value="ise-prof"/>
Type	WLAN
SSID	<input type="text" value="ise-ssid"/>
Status	<input checked="" type="checkbox"/> Enabled
Security Policies	[WPA2][Auth(802.1X)] (Modifications done under security tab will appear after applying the changes.)
Radio Policy	<input type="text" value="All"/>
Interface/Interface Group(G)	<input type="text" value="management"/>
Multicast Vlan Feature	<input type="checkbox"/> Enabled
Broadcast SSID	<input checked="" type="checkbox"/> Enabled
NAS-ID	<input type="text" value="none"/>

Declare o WLC no ISE

Etapa 1. Abra o console ISE e navegue ao > **Add da administração > dos recursos de rede > dos dispositivos de rede.**



Etapa 2. Encha a informação

Opcionalmente pode ser especificada um nome modelo, versão de software, descrição e atribuir os grupos de dispositivo de rede baseados em tipos de dispositivo, em lugar ou em WLC.

a.b.c.d correspondem à relação do WLC que envia a autenticação pedida. À revelia é a interface de gerenciamento.

Network Devices

* Name

Description

* IP Address: /

* Device Profile

Model Name

Software Version

* Network Device Group

Device Type

Location

WLCs

Enable Authentication Settings

Protocol **RADIUS**

* Shared Secret

Enable KeyWrap

* Key Encryption Key

* Message Authenticator Code Key

Key Input Format ASCII HEXADECIMAL

CoA Port

Para obter mais informações sobre dos grupos de dispositivo de rede reveja este link:

[ISE - Grupos de dispositivo de rede](#)

Crie um novo usuário no ISE

Etapa 1. Navegue ao > Add da administração > do Gerenciamento de identidades > das identidades > dos usuários

The screenshot displays the Cisco Identity Services Engine (ISE) Administration interface. The breadcrumb trail is: Home > Context Visibility > Operations > Policy > Administration > System > Identity Management > Network Resources > Device Portal Management > pxGrid > Identities > Users. The 'Users' link is highlighted in red. The main content area shows 'Network Access Users' with a table header containing 'Status', 'Name', and 'Description'. Above the table are buttons for 'Edit', 'Add', 'Change Status', 'Import', and 'Export'. The 'Add' button is highlighted with a red dashed box. A sidebar on the right contains a menu with 'Administration' at the top, followed by 'System' and 'Identity Management'. Under 'Identity Management', 'Identities' is highlighted in red.

Etapa 2. Encha a informação

Neste exemplo este usuário pertence a um grupo chamado ALL_ACCOUNTS mas pode ser ajustado como necessário.

▼ **Network Access User**

* Name

Status Enabled ▼

Email

▼ **Passwords**

Password Type: ▼

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

▼ **User Groups**

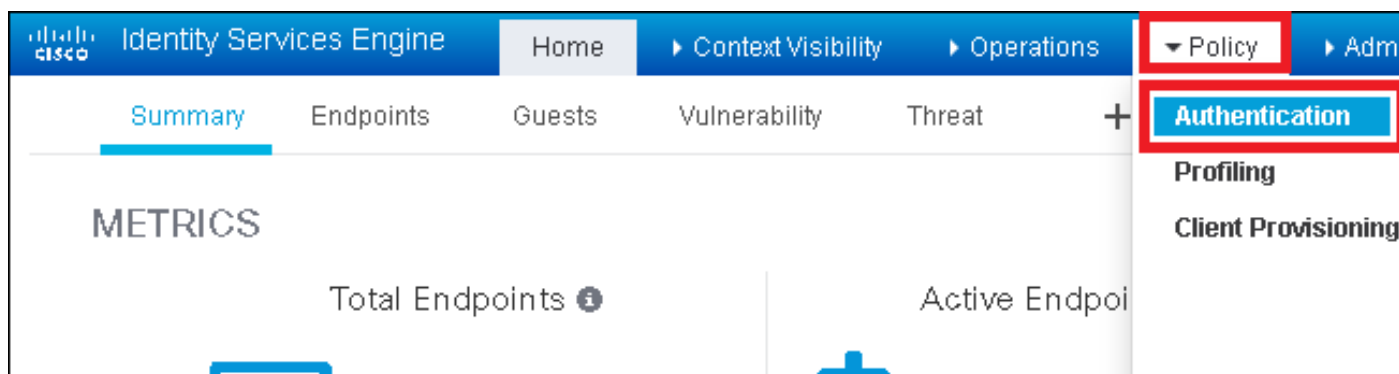
+

Crie a regra da autenticação

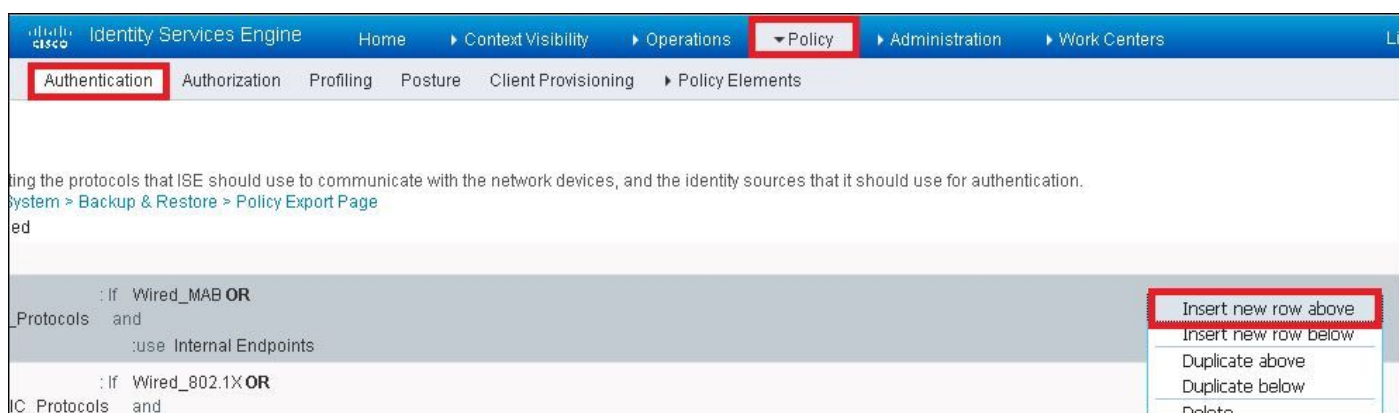
As regras da autenticação estão usadas para verificar se as credenciais dos usuários são direito (verifique se o usuário é realmente quem diz que é) e para limitar os métodos de

autenticação que estão permitidos ser usados por ele.

Etapa 1. Navegue à política > à autenticação.

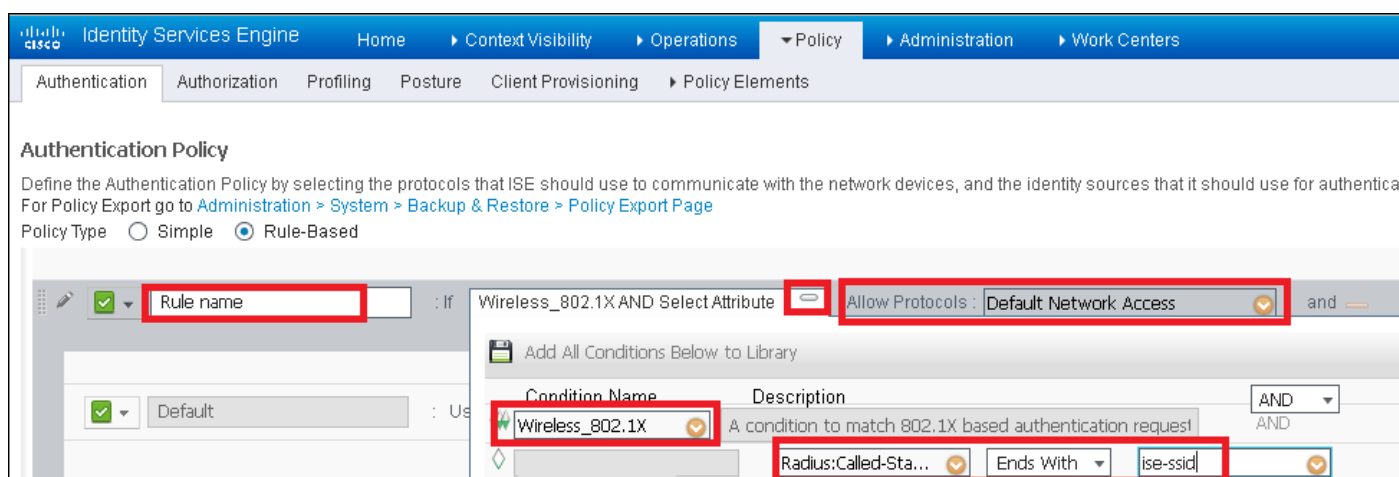


Etapa 2. Introduza uma regra nova da autenticação.

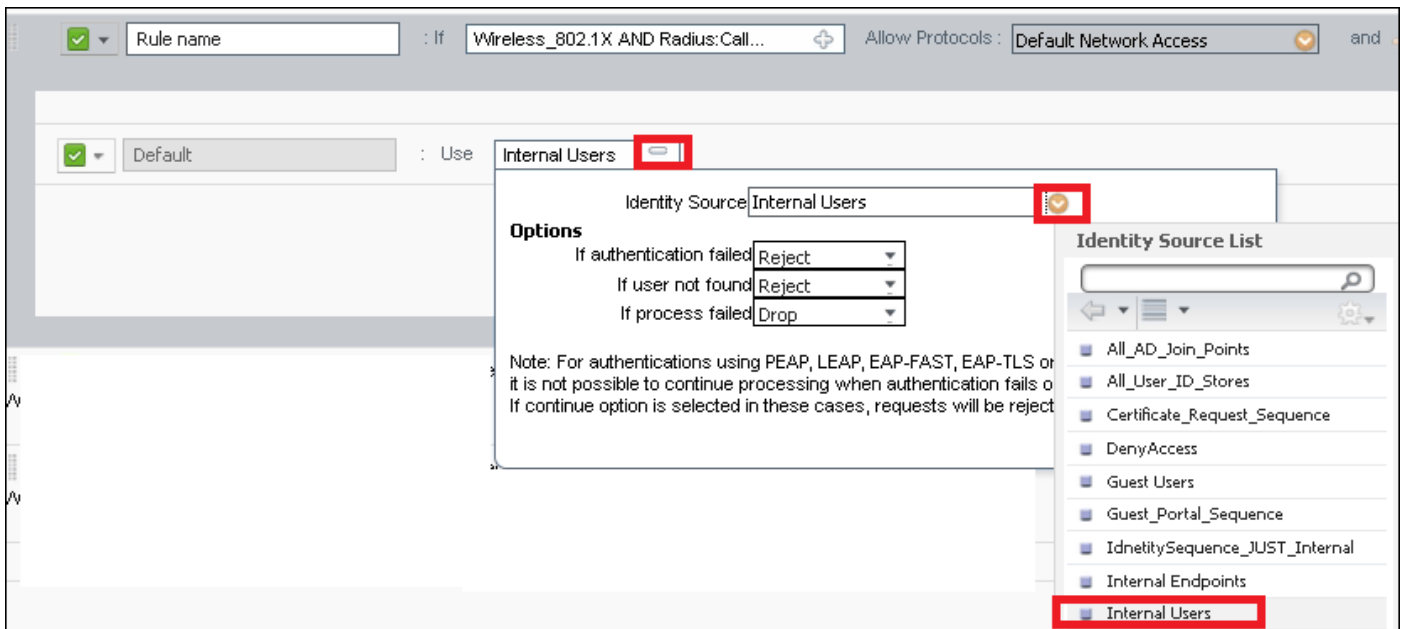


Etapa 3. Incorpore os valores.

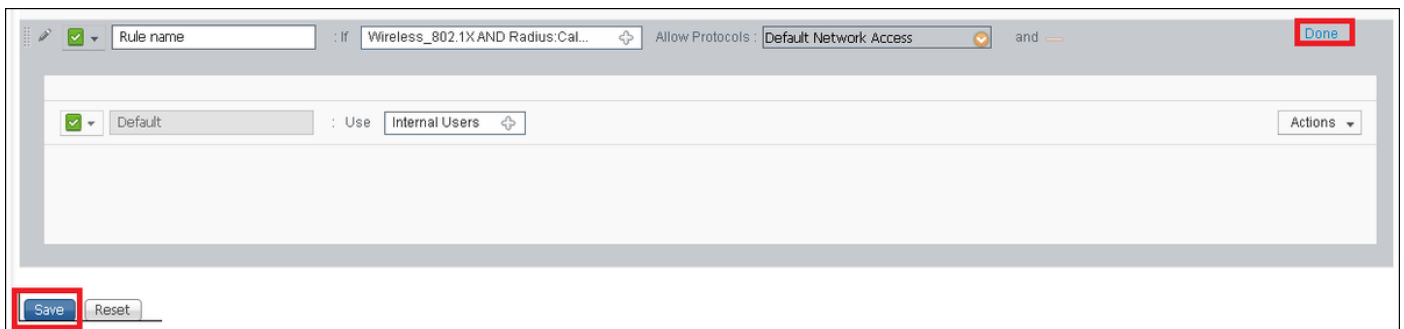
Esta regra da autenticação permite todos os protocolos alistados sob a lista de acessos da rede padrão, esta aplica-se ao pedido de autenticação para clientes wireless do 802.1x e com Chamar-Estação-ID e extremidades com ISE-SSID.



Igualmente escolha a fonte da identidade para os clientes que combina esta regra da autenticação, esta lista de origem da identidade dos usuários internos dos usos do exemplo



Uma vez que é clique terminado **feito e salvaguarda**



Para obter mais informações sobre de permita protocolos que as políticas consultam este link:

[Serviço permitido dos protocolos](#)

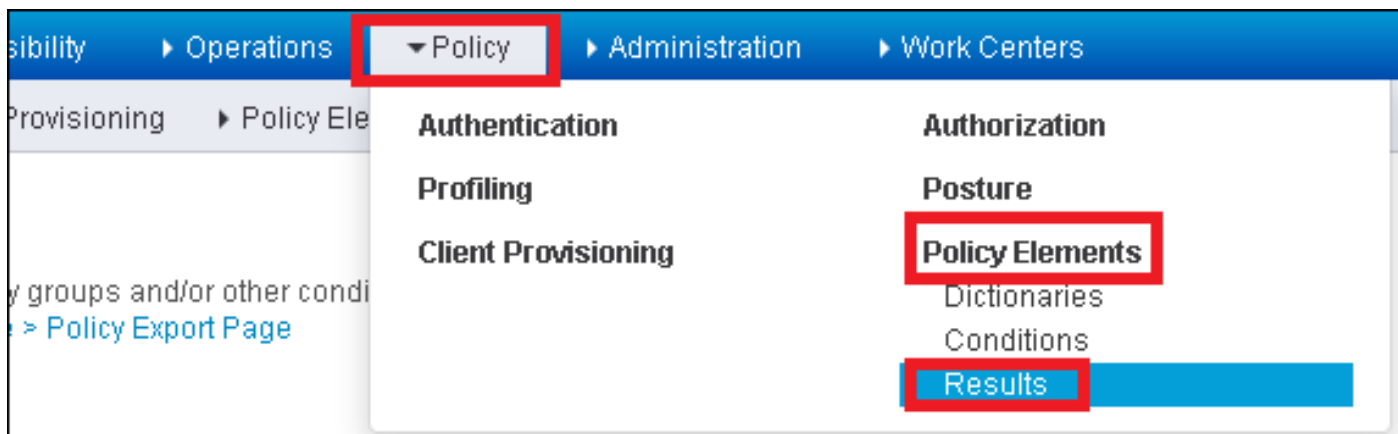
Para obter mais informações sobre da identidade as fontes consultam este link:

[Crie um grupo da identidade do usuário](#)

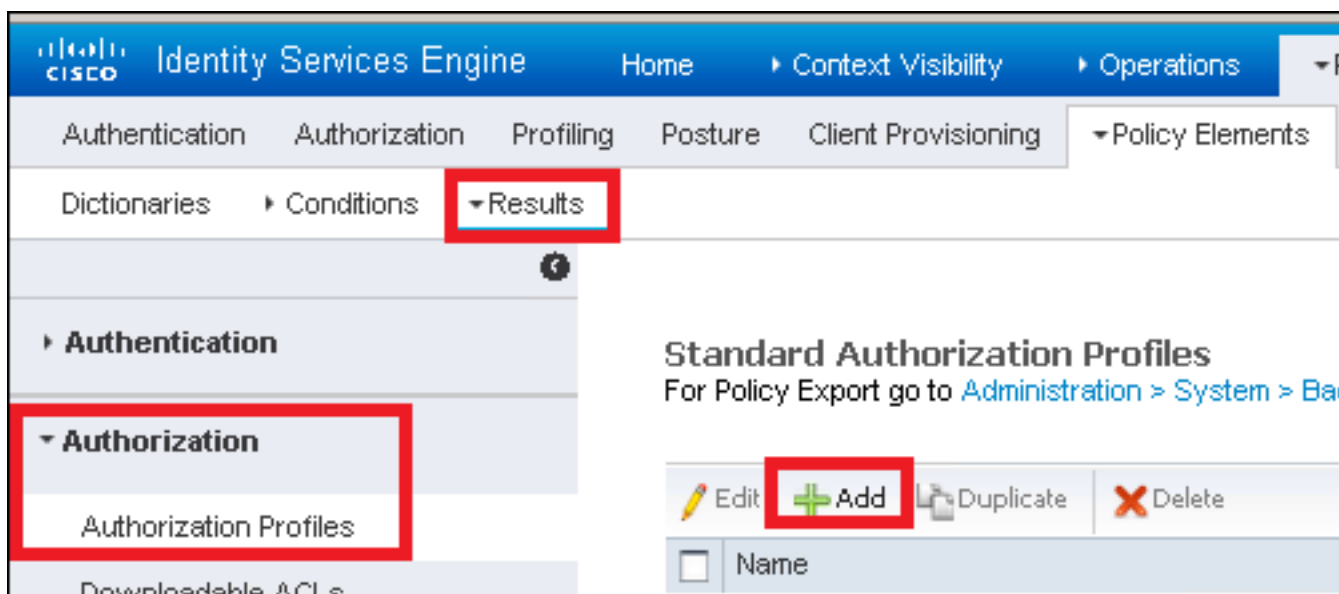
Crie o perfil da autorização

O perfil da autorização determina se o cliente tem o acesso ou não à rede, ao impulso ACL (listas de controle de acesso), à ultrapassagem VLAN (rede de área local virtual) ou ao todo o outro parâmetro. O perfil da autorização mostrado neste exemplo envia um acesso aceita para o cliente e atribui o cliente a VLAN 2404.

Etapa 1. Navegue à política > aos elementos > aos resultados da política



Etapa 2. Adicionar um perfil novo da autorização. Navegue ao > **Add da autorização** > dos perfis da autorização



Etapa 3. Encha os valores.