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

Índice

Introdução

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

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

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

Componentes Utilizados

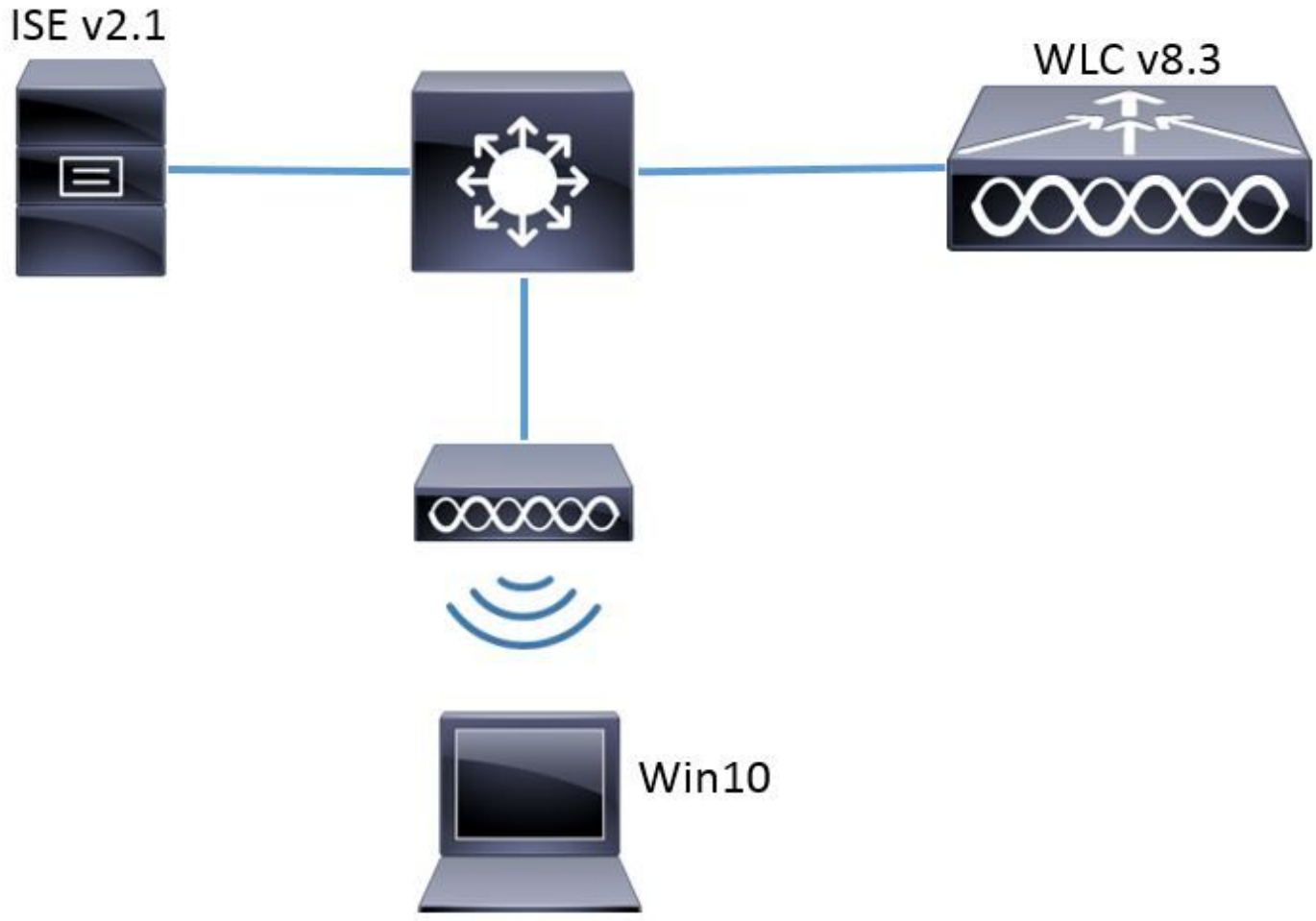
As informações neste documento são baseadas nestas versões de software e hardware:

- WLC v8.3.102.0
- Motor do serviço da identidade (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



Configuração

As etapas gerais são:

1. Declare o servidor Radius no WLC e vice-versa para permitir um com o otro uma comunicação.
2. Crie o Service Set Identifier (SSID) no WLC.

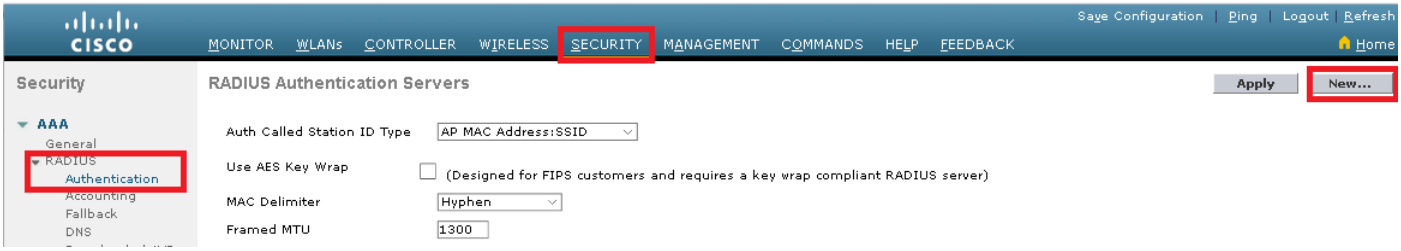
3. Crie a regra da autenticação no ISE.
4. Crie o perfil da autorização no ISE.
5. Crie a regra da autorização no ISE.
6. Configurar o valor-limite.

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** segundo as indicações da imagem.



Etapa 2. Incorpore a informação do servidor Radius segundo as indicações da imagem.

CLI:

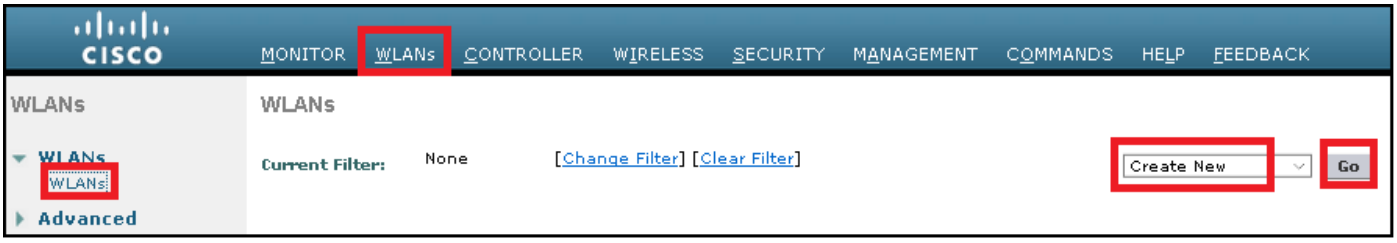
```
> config radius auth add <index> <a.b.c.d> 1812 ascii <shared-key>
> config radius auth disable <index>
> config radius auth retransmit-timeout <index> <timeout-seconds>
> config radius auth enable <index>
```

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

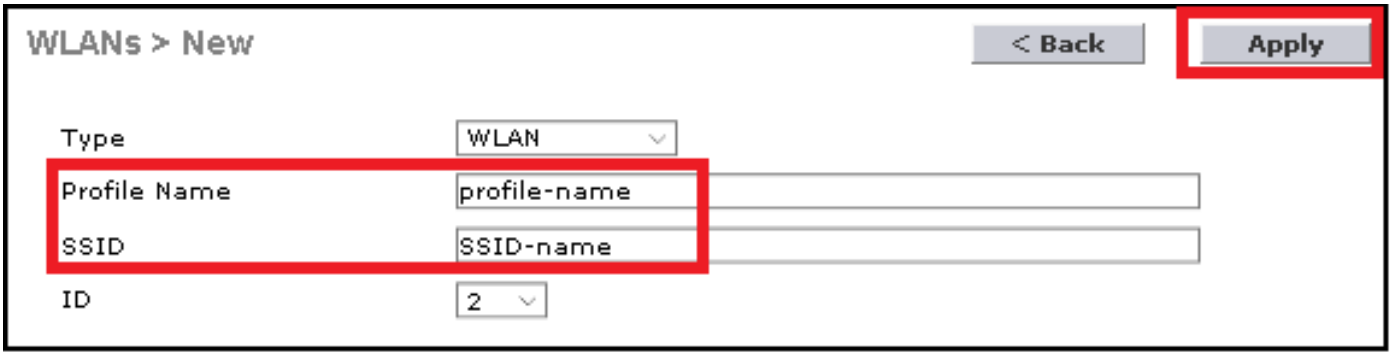
Crie o SSID

GUI:

Etapa 1. Abra o GUI do WLC e navegue a **WLAN > criam novo > vão** segundo as indicações da imagem.



Etapa 2. Escolha um nome para o SSID e o perfil, a seguir clique-o **aplicam-se** segundo as indicações da imagem.



CLI:

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

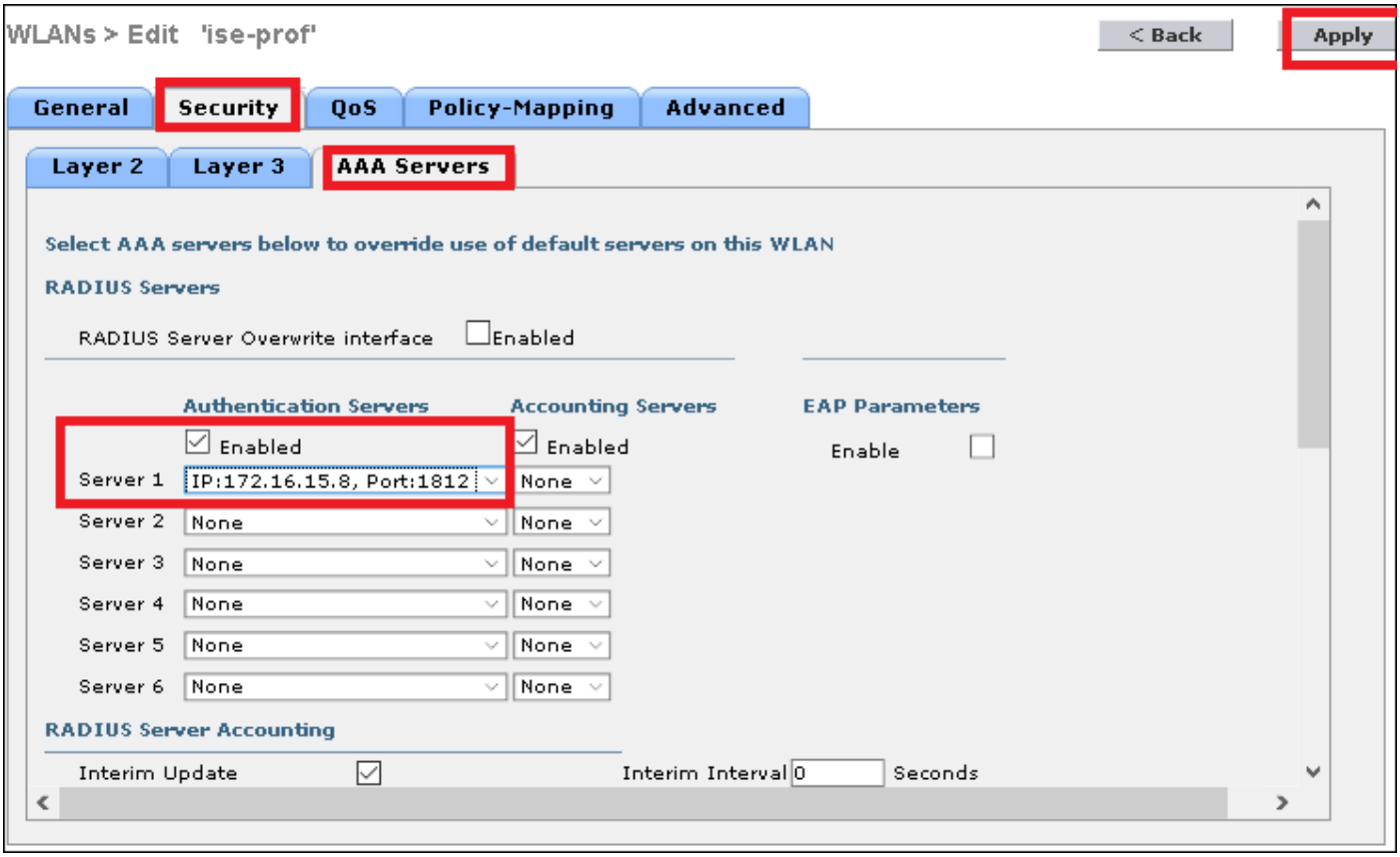
Etapa 3. Atribua o servidor Radius ao WLAN.

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** segundo as indicações da imagem.



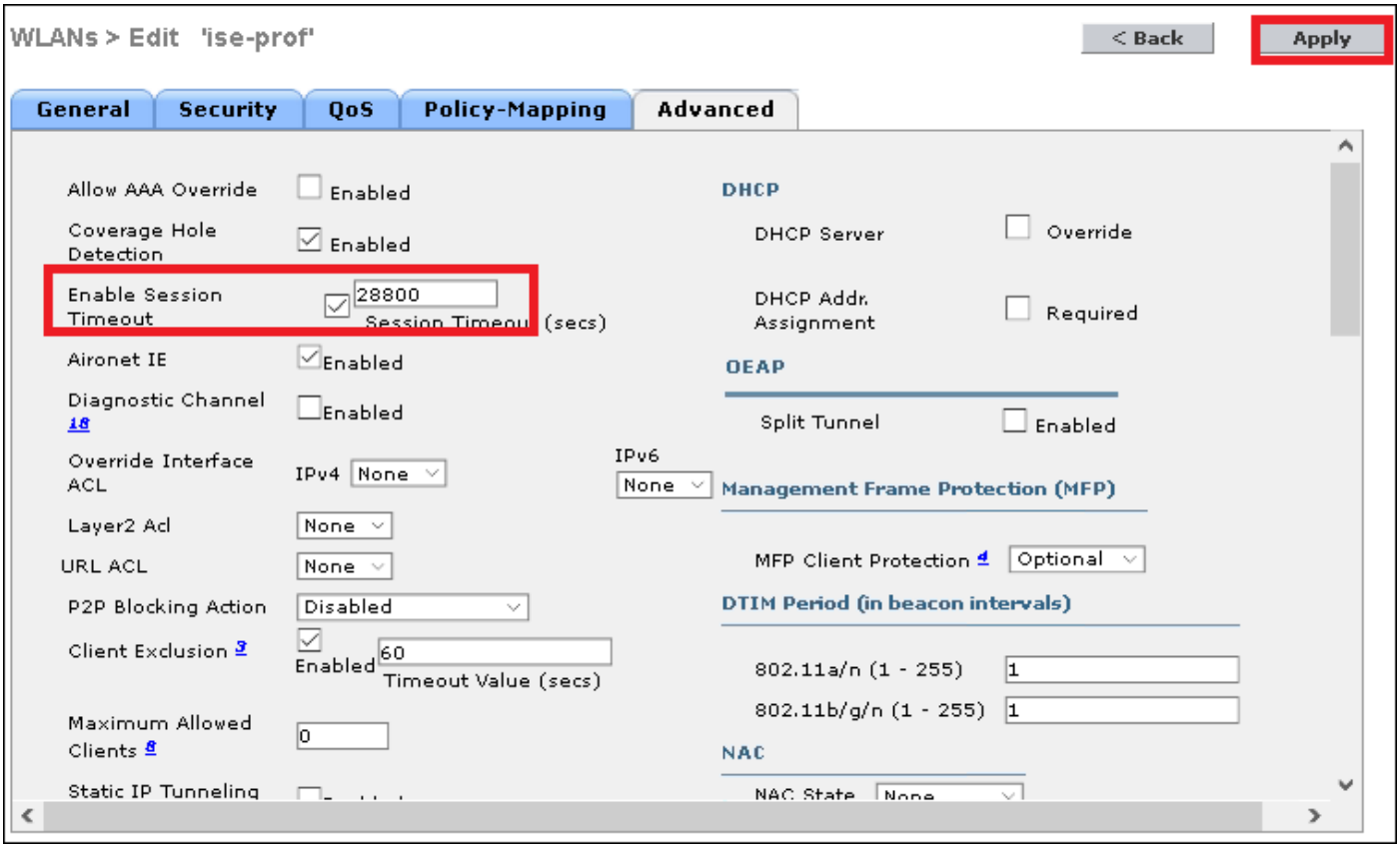
Etapa 4. Aumente opcionalmente o timeout de sessão

CLI:

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

GUI:

Navegue a **WLAN > ID de WLAN > avançou** e especificam o timeout de sessão segundo as indicações da imagem.



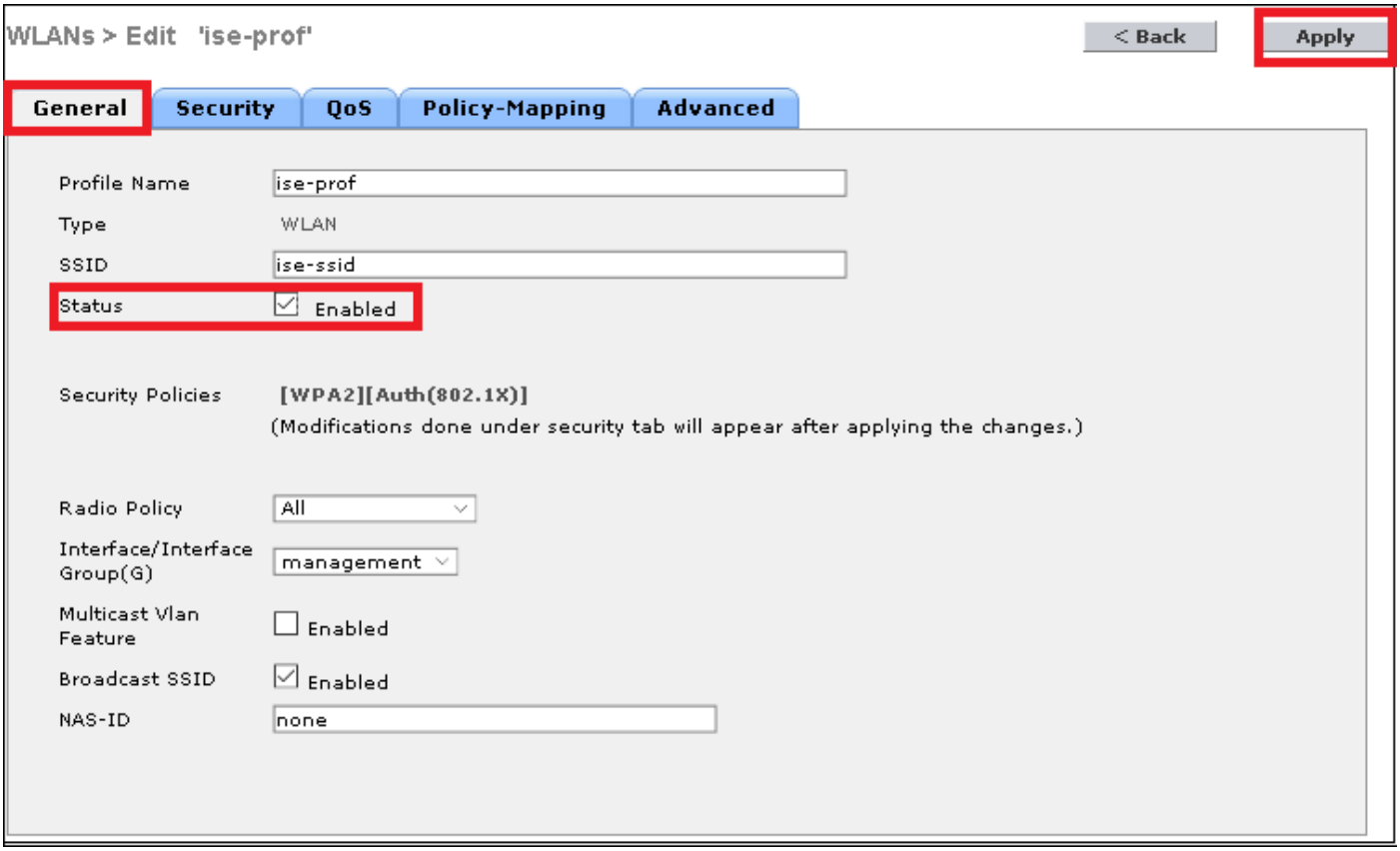
Etapa 5. Permita o WLAN.

CLI:

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

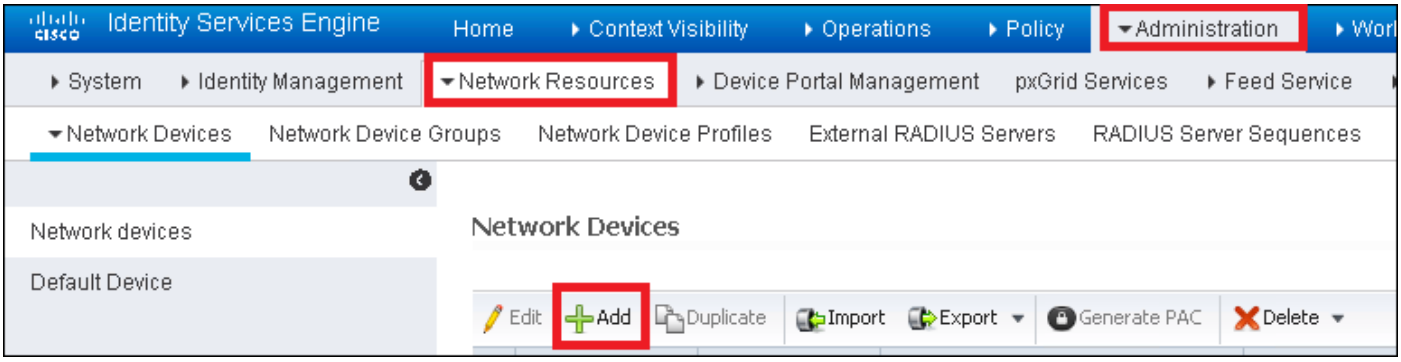
GUI:

Navegue a **WLAN > ID de WLAN > general** e permita o SSID segundo as indicações da imagem.



Declare o WLC no ISE

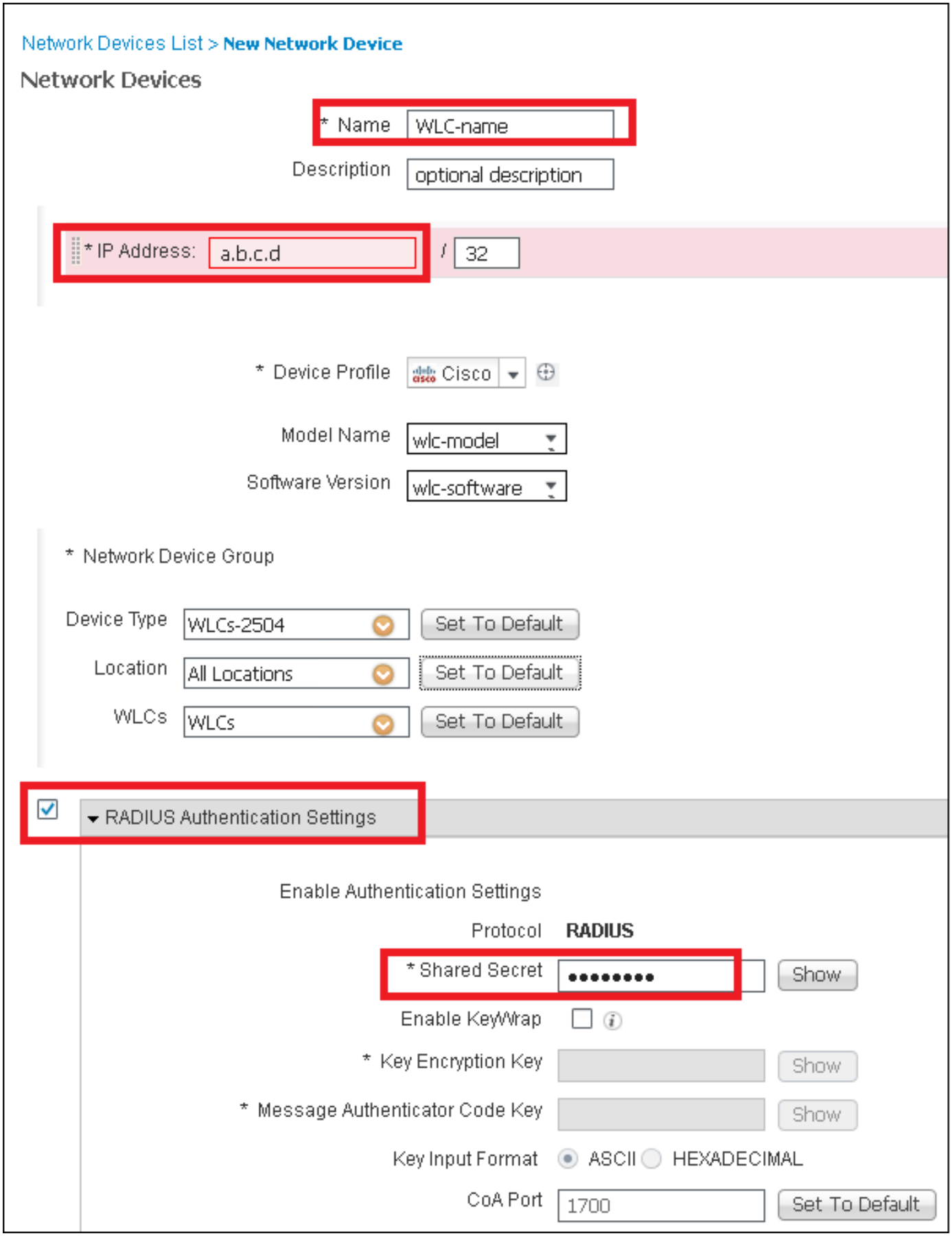
Etapa 1. Abra o console ISE e navegue ao **> Add da administração > dos recursos de rede > dos dispositivos de rede** segundo as indicações da imagem.



Etapa 2. Incorpore os valores.

Opcionalmente, pode ser um nome modelo especificado, 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 segundo as indicações da imagem.

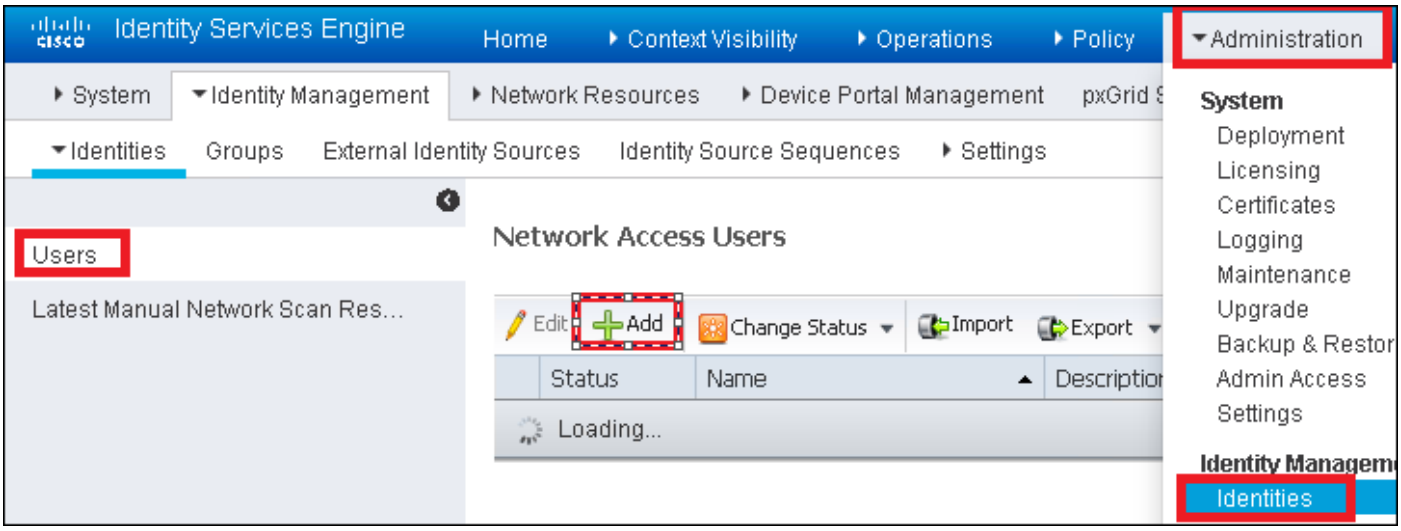


Para obter mais informações sobre dos **grupos de dispositivo de rede** reveja este link:

[ISE - Grupos de dispositivo de rede]

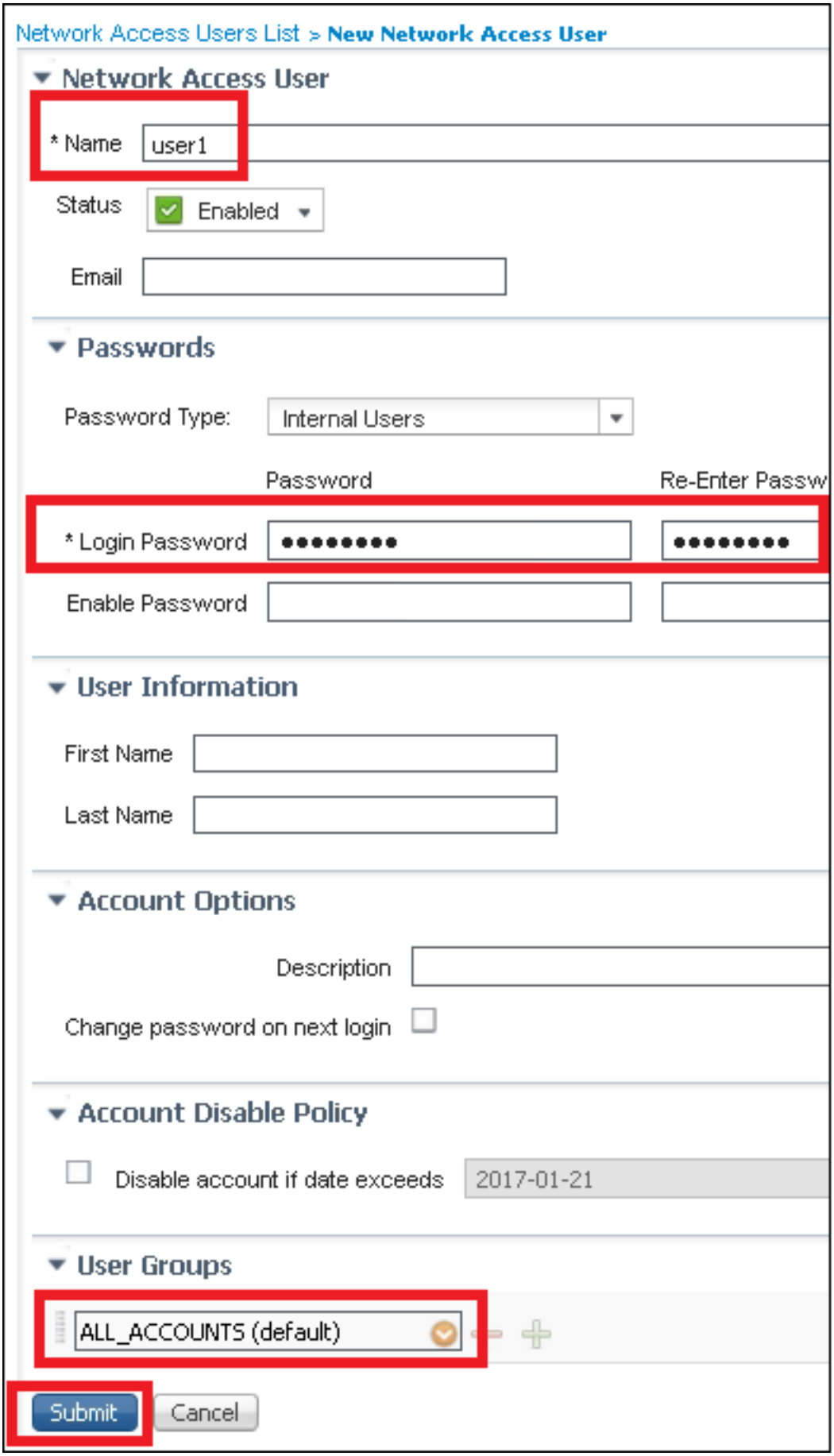
Crie o novo usuário no ISE

Etapa 1. Navegue ao **> Add da administração > do Gerenciamento de identidades > das identidades > dos usuários** segundo as indicações da imagem.



Etapa 2. Incorpore a informação.

Neste exemplo, este usuário pertence a um grupo chamado ALL_ACCOUNTS mas pode ser ajustado como necessário segundo as indicações da imagem.

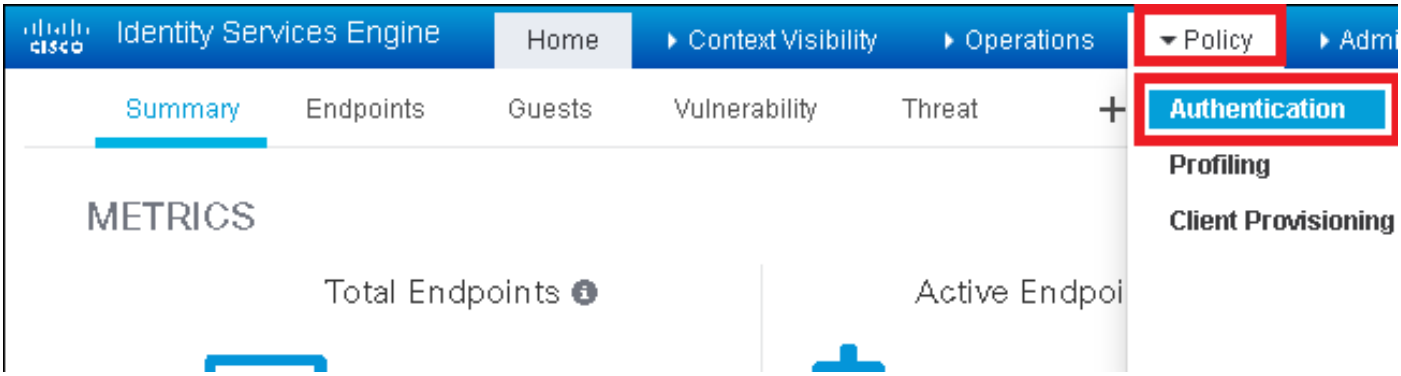


Crie a regra da autenticação

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.

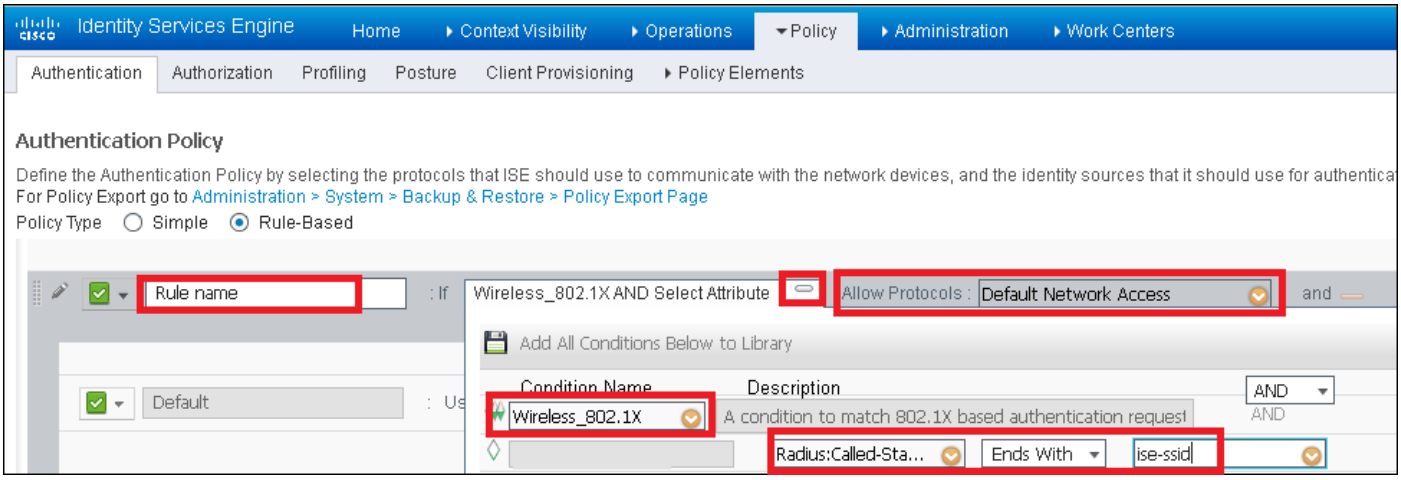
Etapa 1. Navegue à **política > à autenticação** segundo as indicações da imagem.



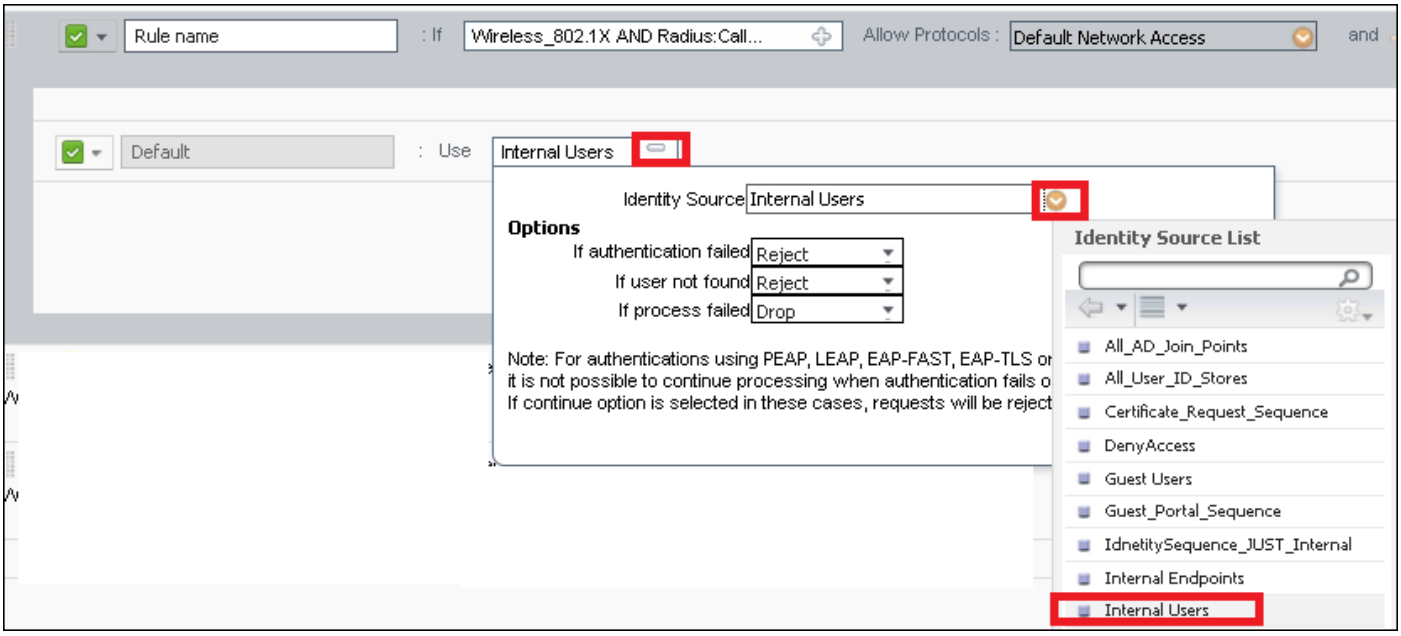
Etapa 2. Introduza uma regra nova da autenticação segundo as indicações da imagem.

Etapa 3. Incorpore os valores.

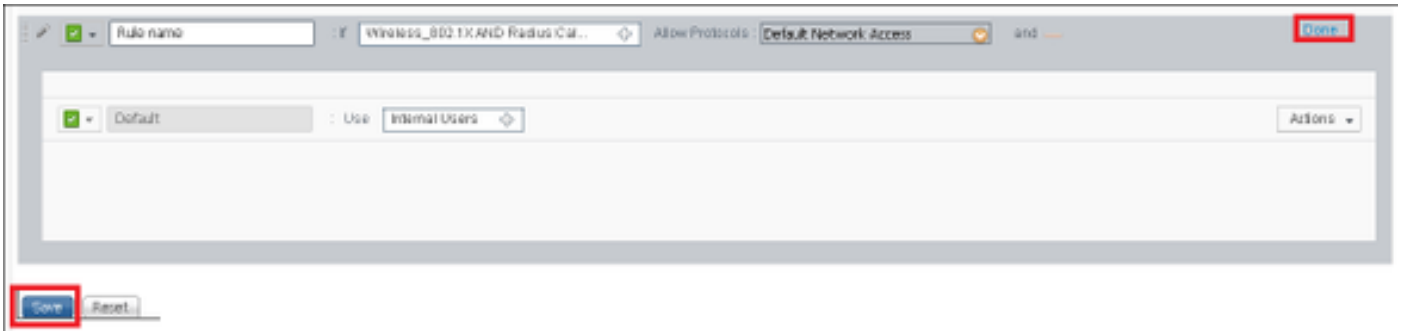
Esta regra da autenticação permite todos os protocolos alistados sob a **lista de acessos da rede padrão**, esta aplica-se ao pedido de autenticação para clientes wireless do 802.1x e com Chamar-Estação-ID e extremidades com o ISE-**SSID** segundo as indicações da imagem.



Também, escolha a fonte da identidade para os clientes que combina esta regra da autenticação. Este exemplo usa a lista de origem da identidade dos **usuários internos** segundo as indicações da imagem.



Uma vez que terminado, clique **feito** e **salvar** segundo as indicações da imagem.



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

[Serviço permitido dos protocolos]

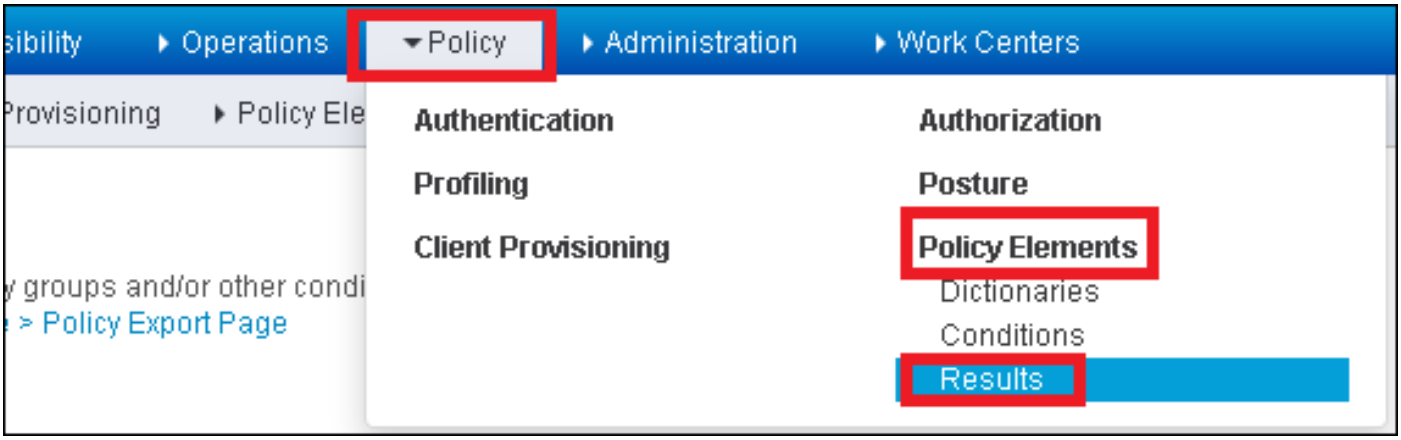
Para obter mais informações sobre da identidade as fontes consultam este link:

[Crie um grupo da identidade do usuário]

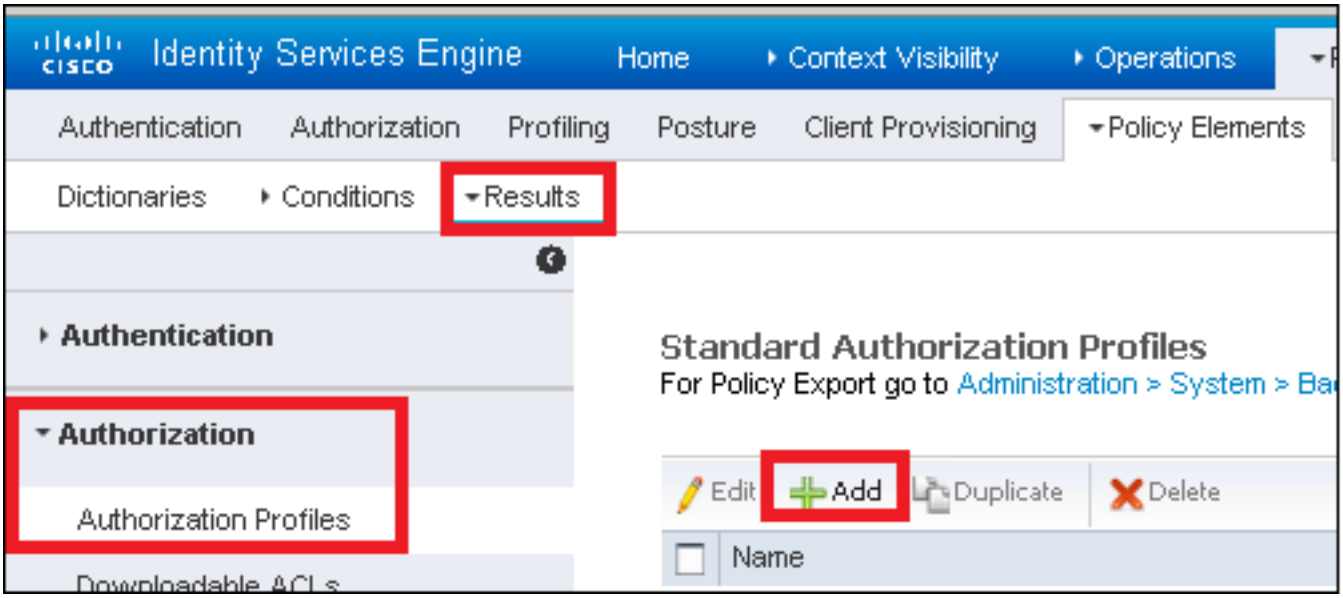
Crie o perfil da autorização

O perfil da autorização determina se o cliente tem o acesso ou não à rede, ao Access Control Lists (ACLs) do impulso, à ultrapassagem VLAN ou ao qualquer 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** segundo as indicações da imagem.



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



Etapa 3. Incorpore os valores segundo as indicações da imagem.