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

Índice

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

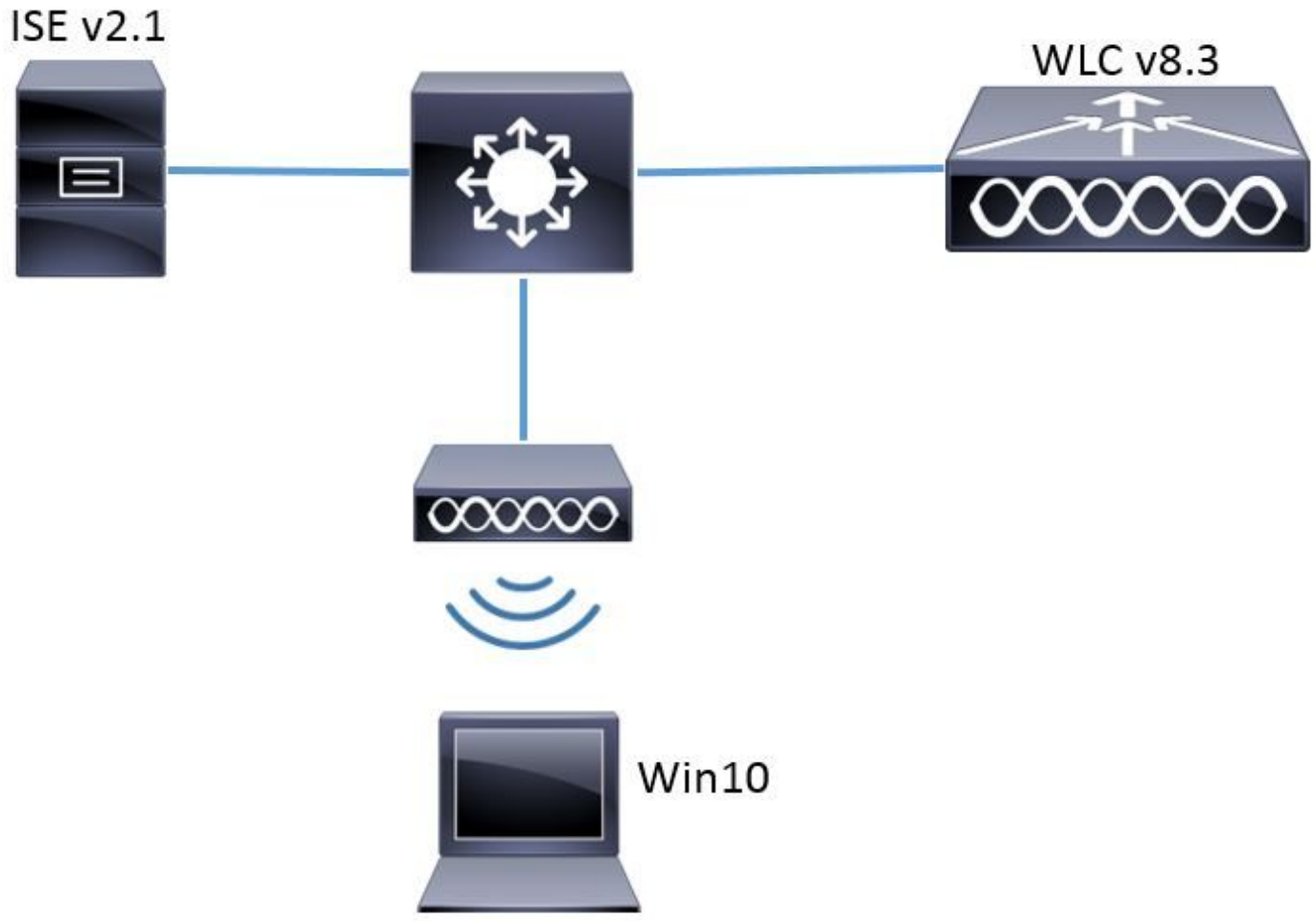
ISE v2.1

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:

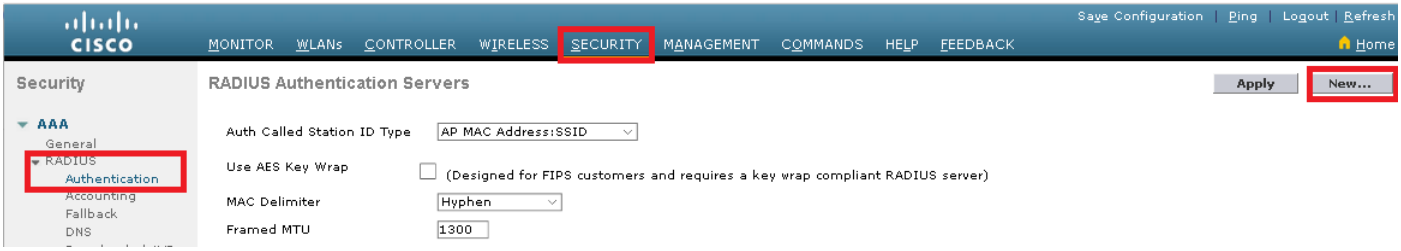
1. Declare o servidor Radius (ISE neste exemplo) no WLC e vice-versa para permitir um com o otro uma comunicação
2. Crie o SSID (Service Set Identifier) no WLC
3. Crie a regra da autenticação no ISE
4. Crie o perfil da autorização no ISE
5. Crie a regra da autorização no ISE
6. Configurar o valor-limite

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.

CLI:

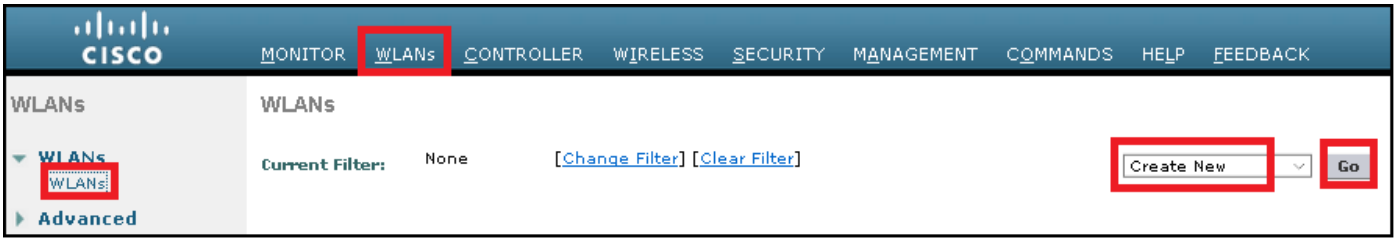
```
> config radius auth add <index> <a.b.c.d> 1812 ascii <shared-key>> config radius auth disable
<index>> config radius auth retransmit-timeout <index> <timeout-seconds>> config radius auth
enable <index>
```

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

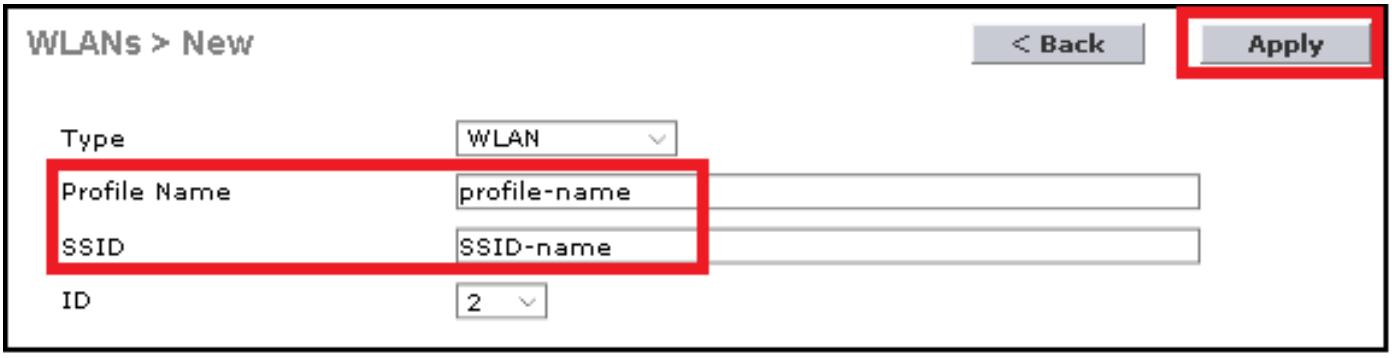
Crie o SSID

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>
```

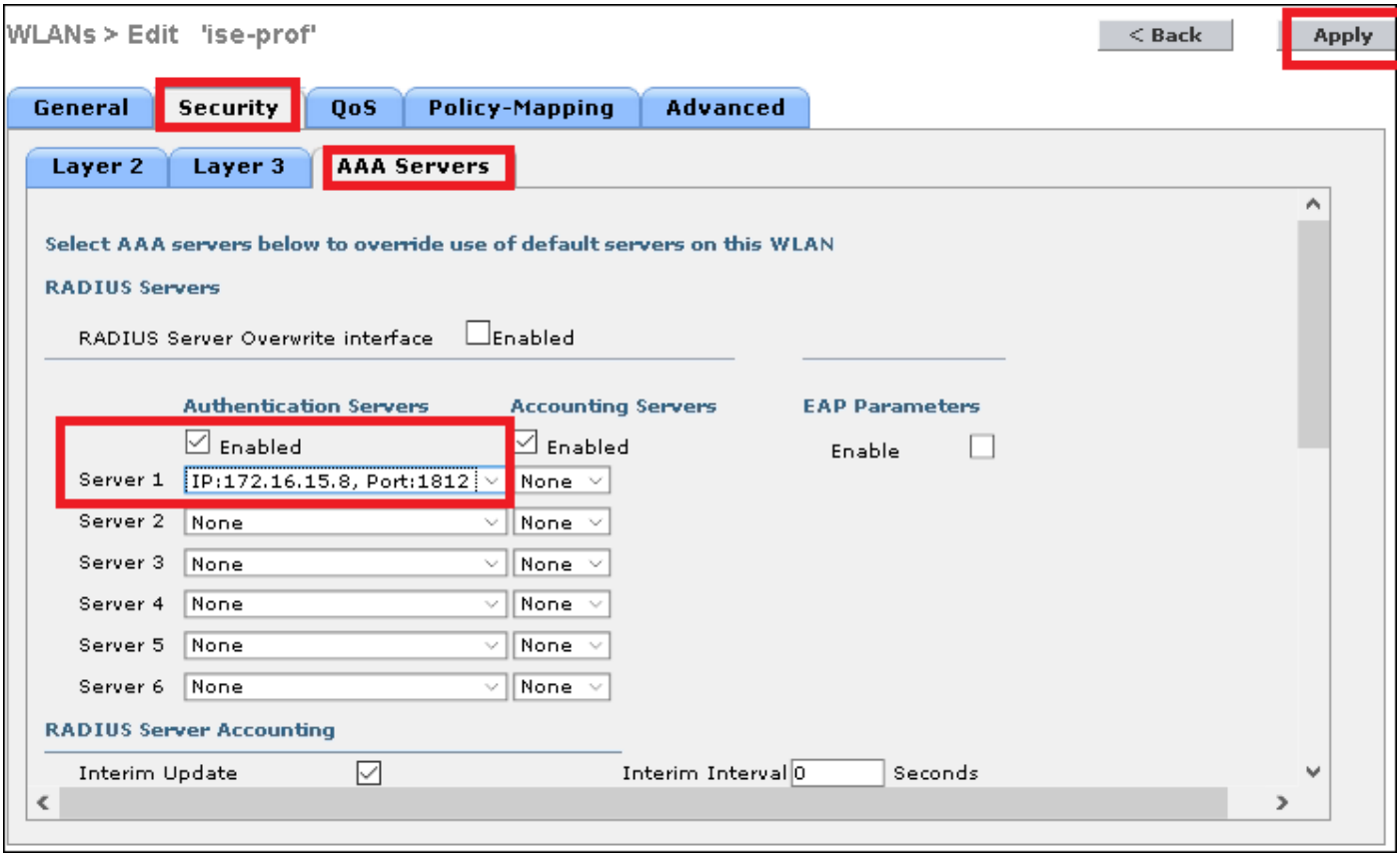
Etapa 3. Atribua o servidor Radius ao WLAN.

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.**

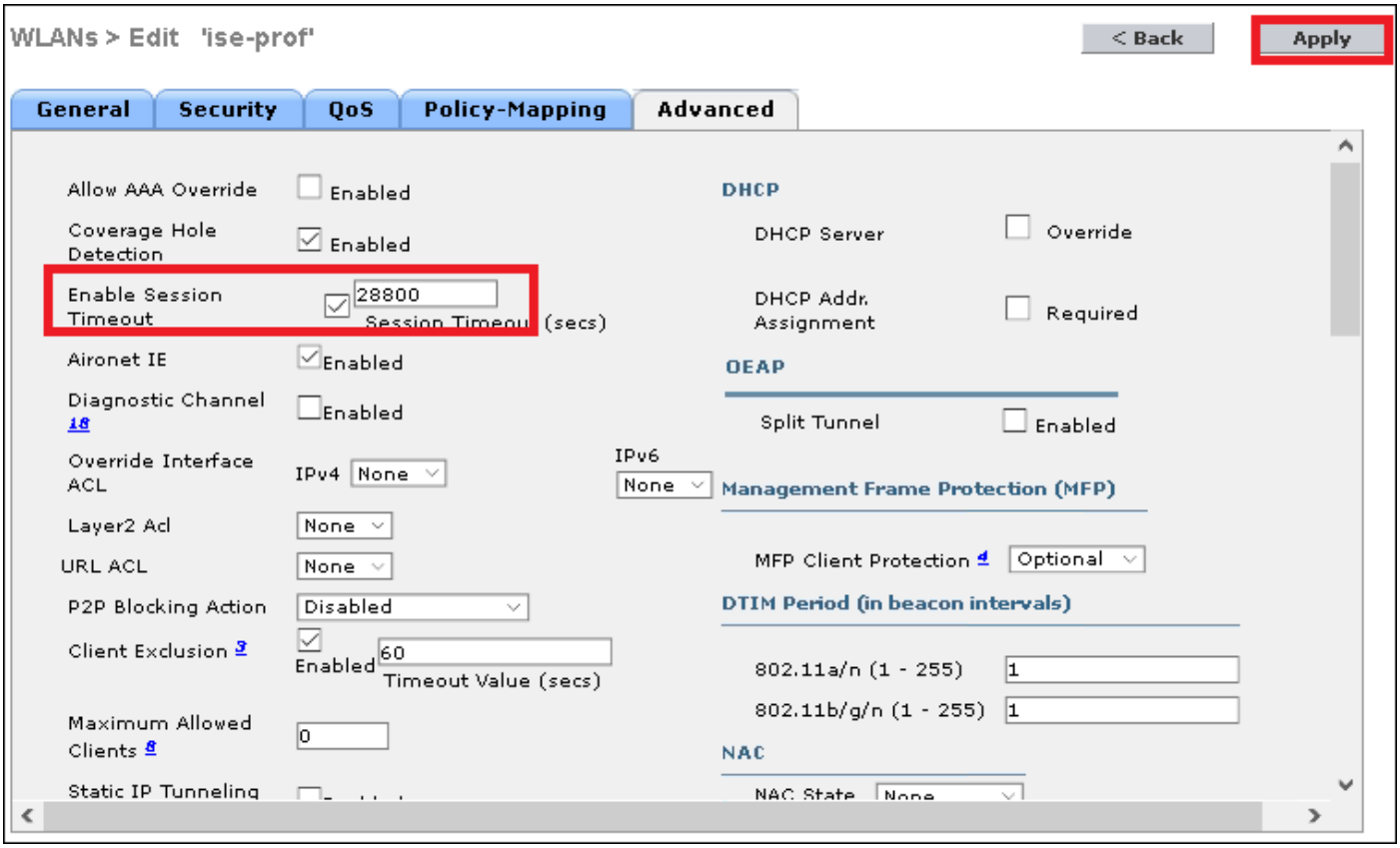


Etapa 4. Aumente opcionalmente o timeout de sessão

CLI:

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

GUI:

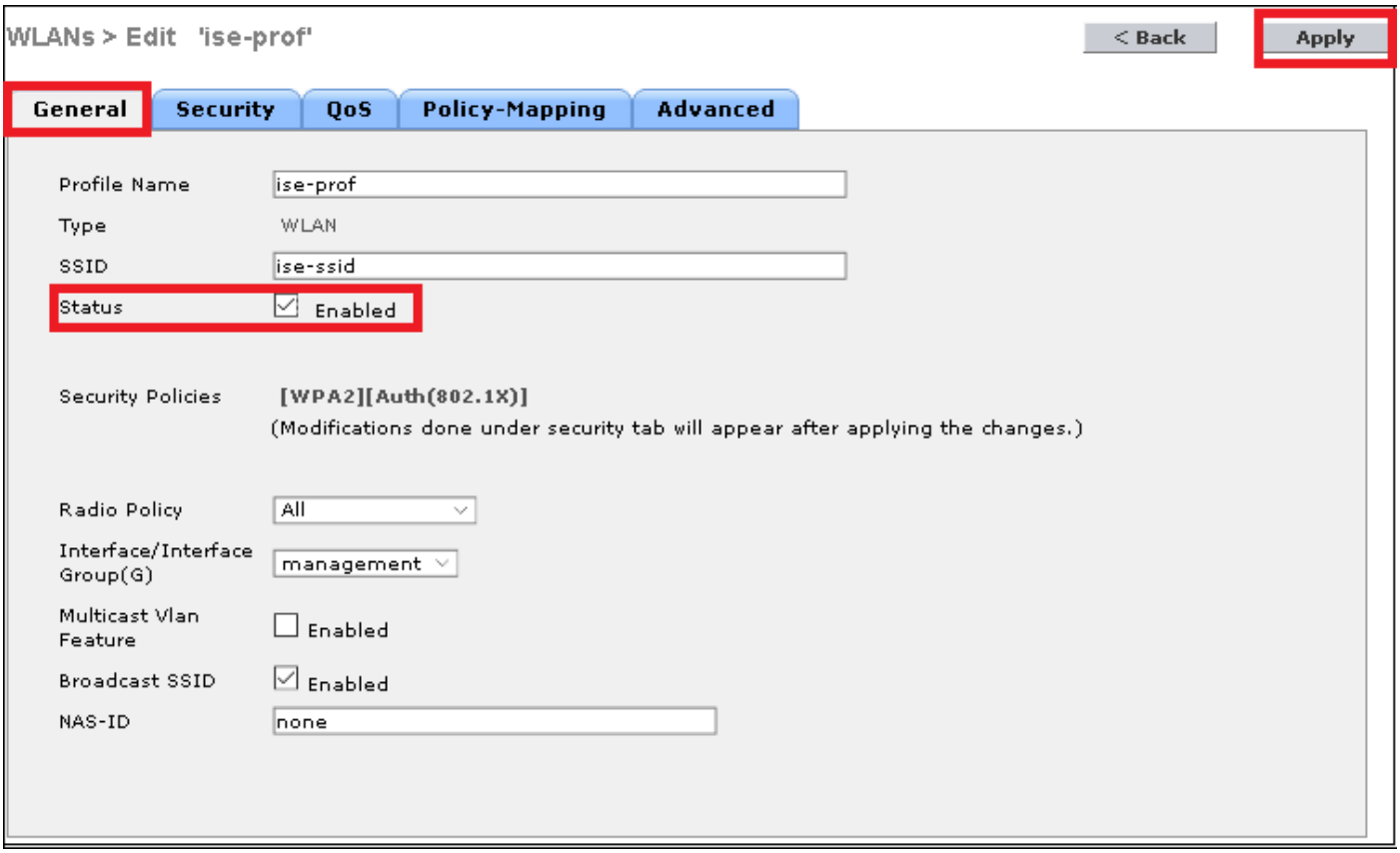


Etapa 5. Permita o WLAN

CLI:

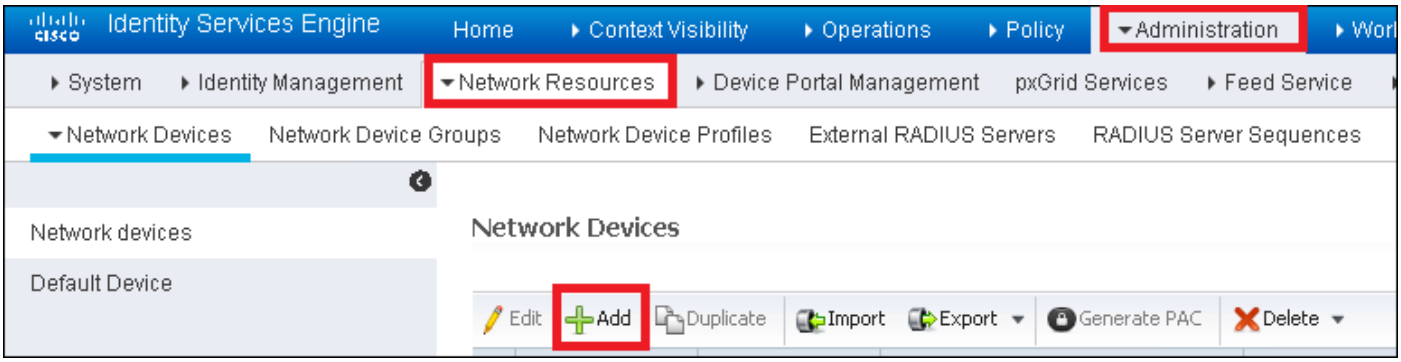
```
> config wlan enable <wlan-id>
```

GUI:



Declare o WLC no ISE

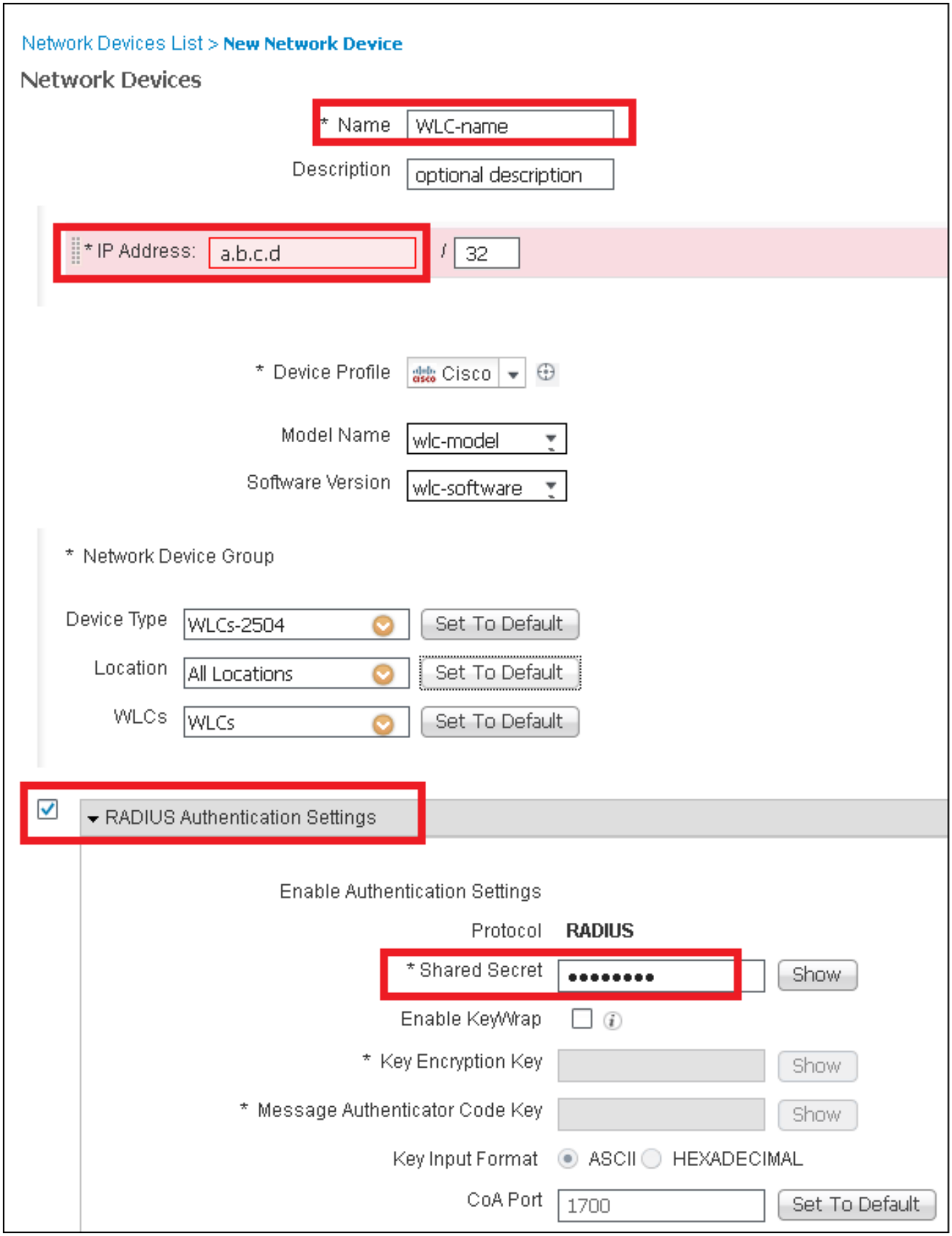
Etapa 1. Abra o console ISE e navegue ao **> Add da administração > dos recursos de rede > dos dispositivos de rede.**



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.

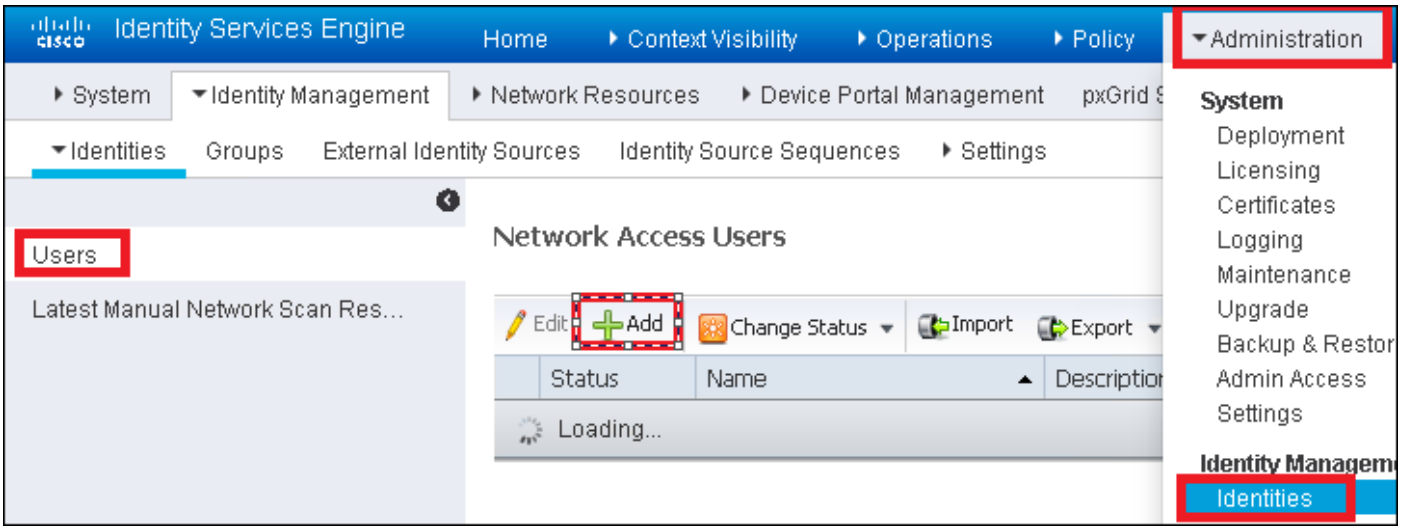


Para obter mais informações sobre dos grupos de dispositivo de rede reveja este link:

[ISE - Grupos de dispositivo de rede]

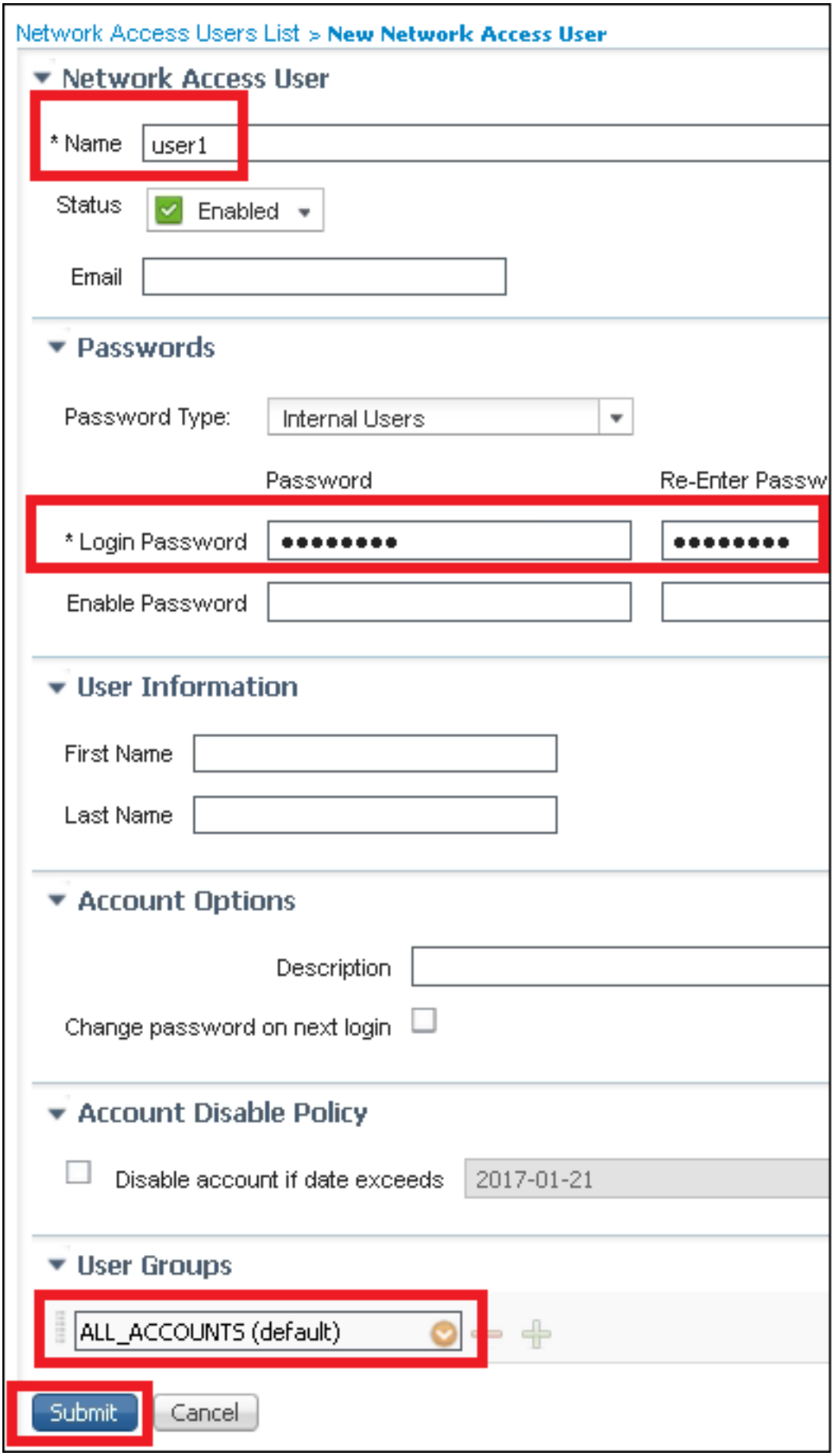
Crie um novo usuário no ISE

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



Etapa 2. Encha a informação

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

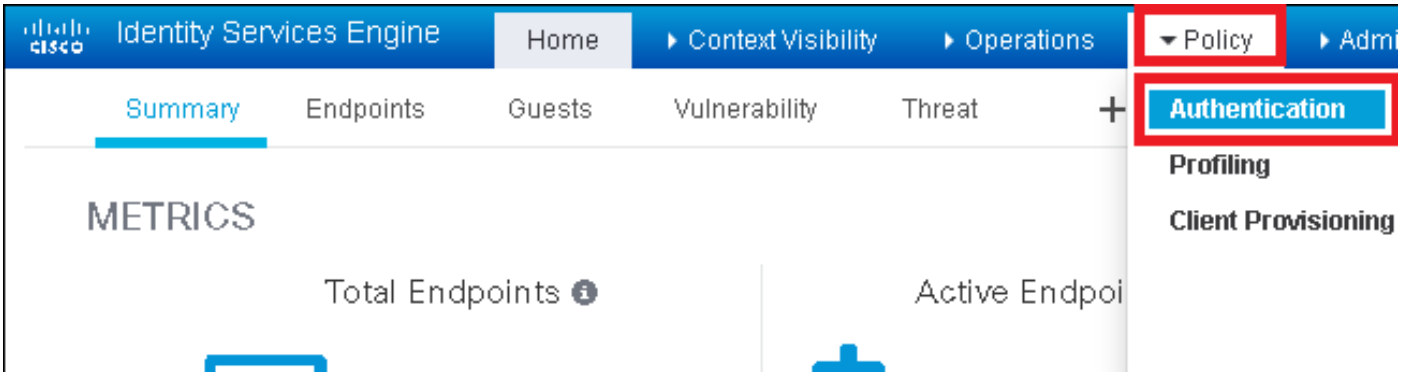


Crie a regra da autenticação

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.

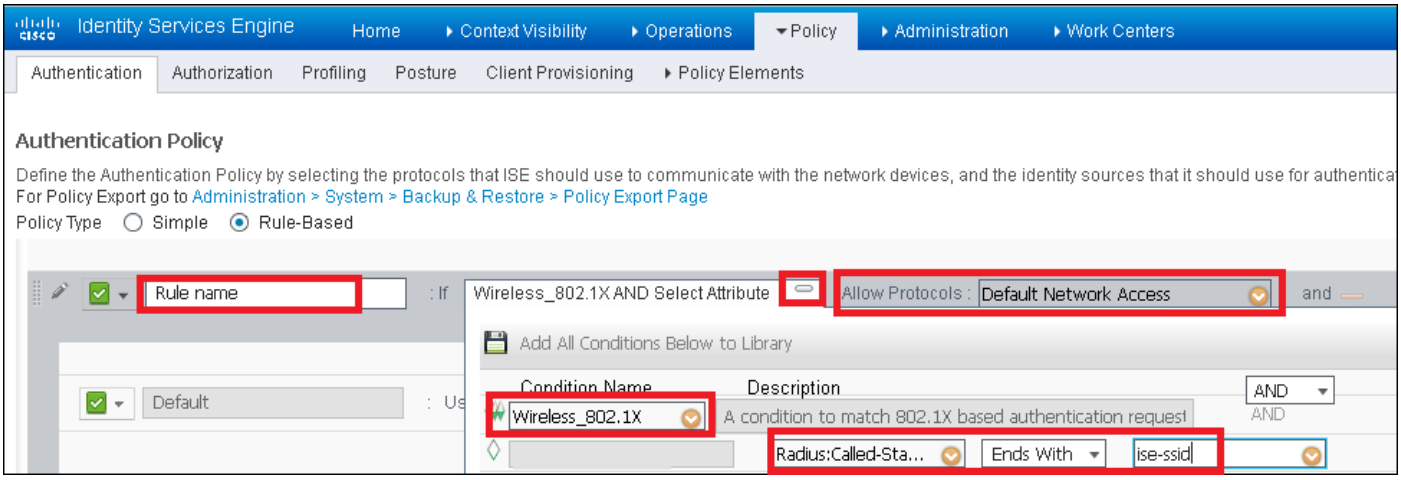
Etapa 1. Navegue à **política > à autenticação.**



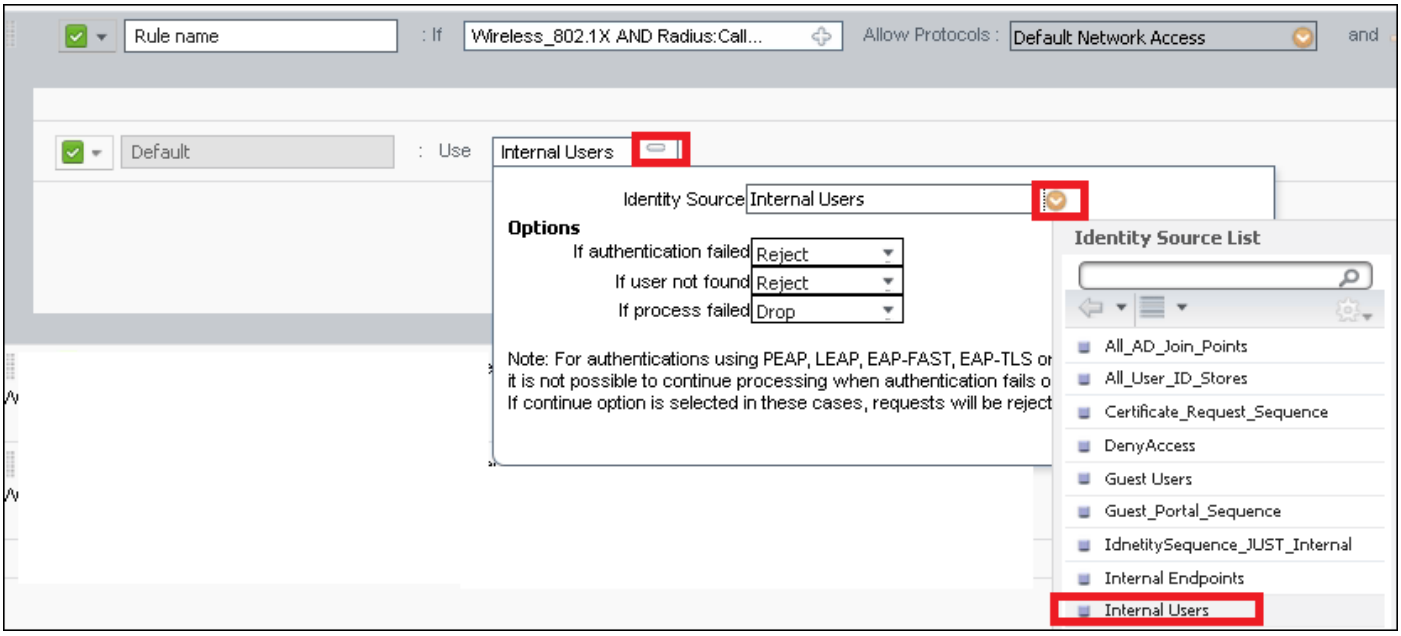
Etapa 2. Introduza uma regra nova da autenticação.

Etapa 3. Incorpore os valores.

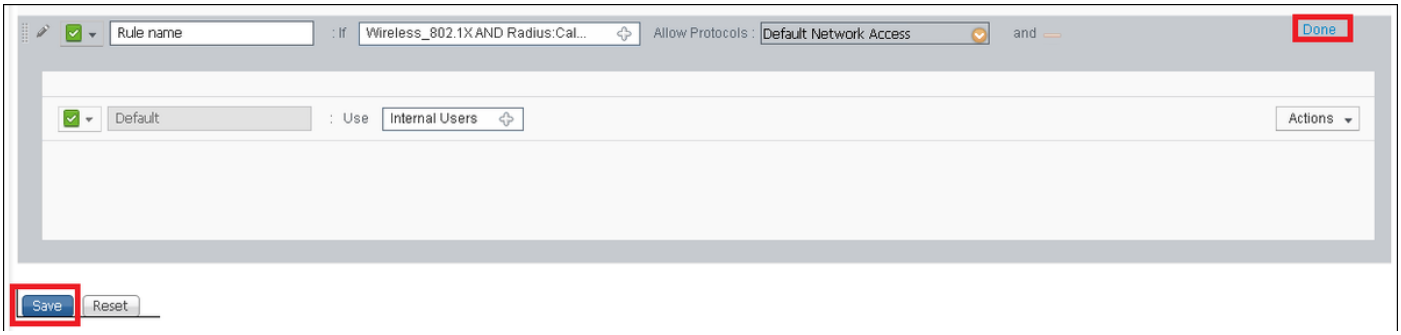
Esta regra da autenticação permite todos os protocolos alistados sob a **lista de acessos da rede padrão**, esta aplica-se ao pedido de autenticação para clientes wireless do 802.1x e com Chamar-Estação-ID e extremidades com ISE-**SSID**.



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

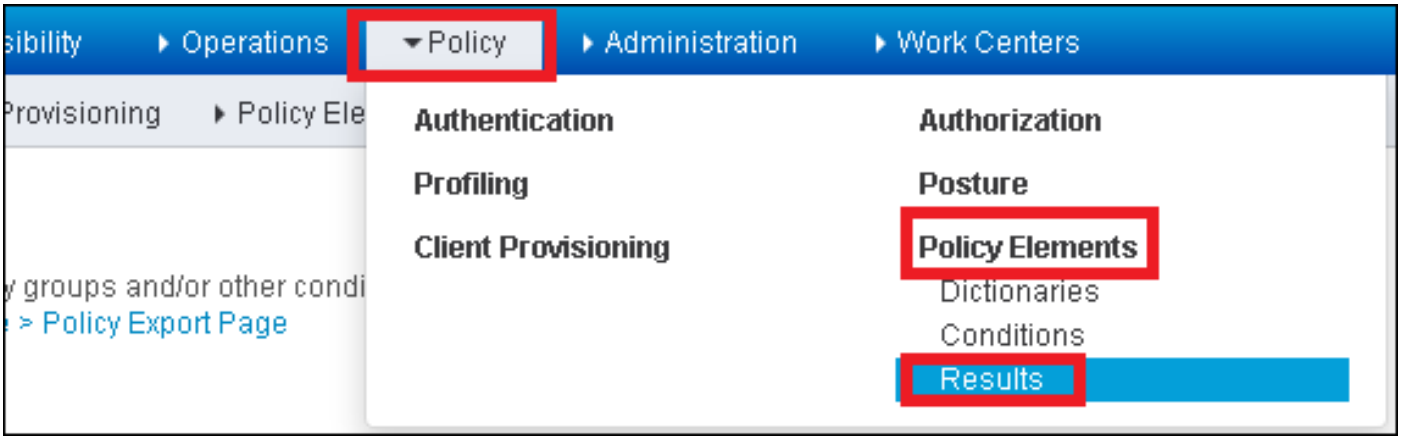
Para obter mais informações sobre da identidade as fontes consultam este link:

Crie um grupo da identidade do usuário

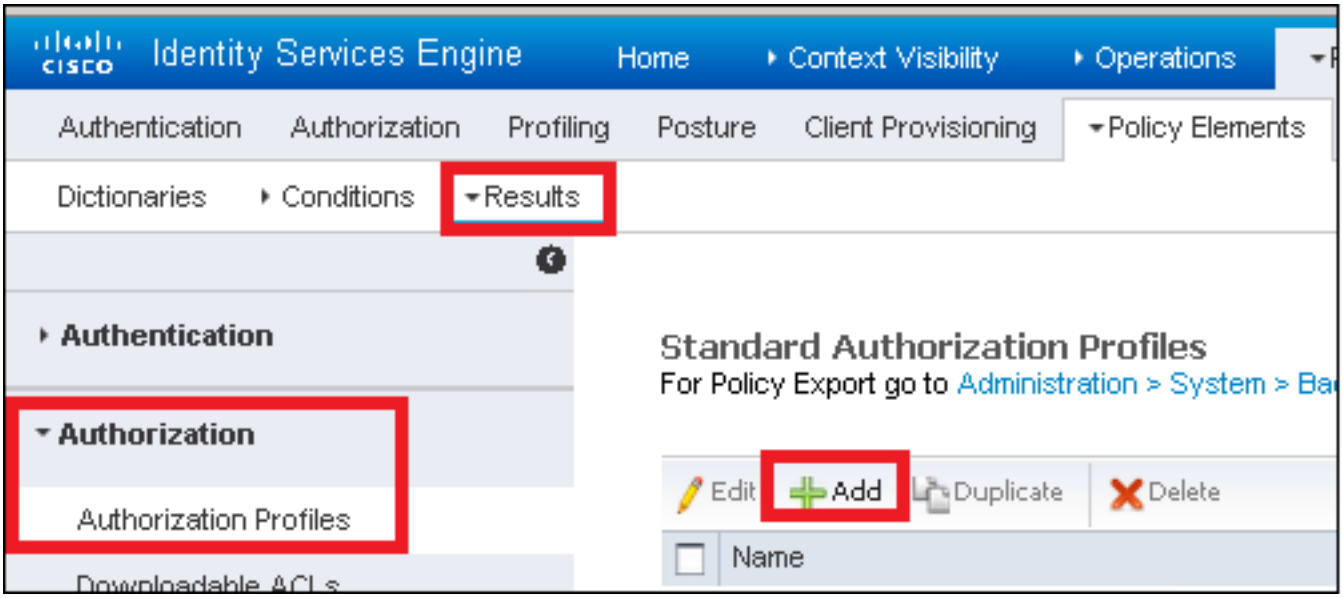
Crie o perfil da autorização

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.