Configurar a postura no Catalyst 9800 WLC e ISE

Contents

- Introdução
- Pré-requisitos
  - Requisitos
  - Componentes Utilizados
- Informações de Apoio
- Configurar
  - Diagrama de Rede
  - Configuração de AAA no 9800 WLC
  - Configuração de WLAN
  - Configuração de perfil de política
  - Configuração de marca de política
  - Atribuição de marca de política
  - Configuração de ACL de redirecionamento
  - Configuração da ACL de política
  - Configuração e postura de AAA no ISE
- Examples
- Verificar
- Troubleshooting
  - Lista de verificação
- Coletar depurações
- Referências

Introdução

Este documento descreve como configurar uma WLAN de postura em um Catalyst 9800 WLC e ISE através da Interface Gráfica do Usuário (GUI).

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Configuração geral da WLC 9800
- Configuração de políticas e perfis do ISE

Componentes Utilizados

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

- 9800 WLC Cisco IOS® XE Cupertino v17.9.5
- Identity Service Engine (ISE) v3.2
- Notebook Windows 10 Enterprise

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

Fluxo de recursos de NAC e CoA do controlador de LAN sem fio

1. O cliente autentica usando a autenticação dot1x.

2. RADIUS Access Accept transporta o URL redirecionado para a porta 80 e ACLs de pré-autorização que incluem a permissão de endereços IP e portas, ou VLAN de quarentena.

3. O cliente é redirecionado para a URL fornecida em aceitação de acesso e colocado em um novo estado até que a validação da postura seja feita. O cliente nesse estado se comunica com o servidor ISE e valida a si mesmo em relação às políticas configuradas no servidor ISE NAC.

4. O agente NAC no cliente inicia a validação da postura (tráfego para a porta 80): O agente envia a solicitação de descoberta HTTP para a porta 80, que é redirecionada pelo controlador para a URL fornecida na aceitação de acesso. O ISE sabe que o cliente está tentando alcançar e responde diretamente ao cliente. Dessa forma, o cliente aprende sobre o IP do servidor ISE e, a partir de agora, ele fala diretamente com o servidor ISE.

5. A WLC permite esse tráfego porque a ACL está configurada para permitir esse tráfego. Em caso de substituição de VLAN, o tráfego é ligado para que chegue ao servidor ISE.

6. Quando o cliente ISE concluir a avaliação, um RADIUS CoA-Req com serviço de reautenticação será enviado para a WLC. Isso inicia a reautenticação do cliente (enviando EAP-START). Depois que a reautenticação for bem-sucedida, o ISE enviará a aceitação de acesso com uma nova ACL (se houver) e nenhum redirecionamento de URL ou VLAN de acesso.

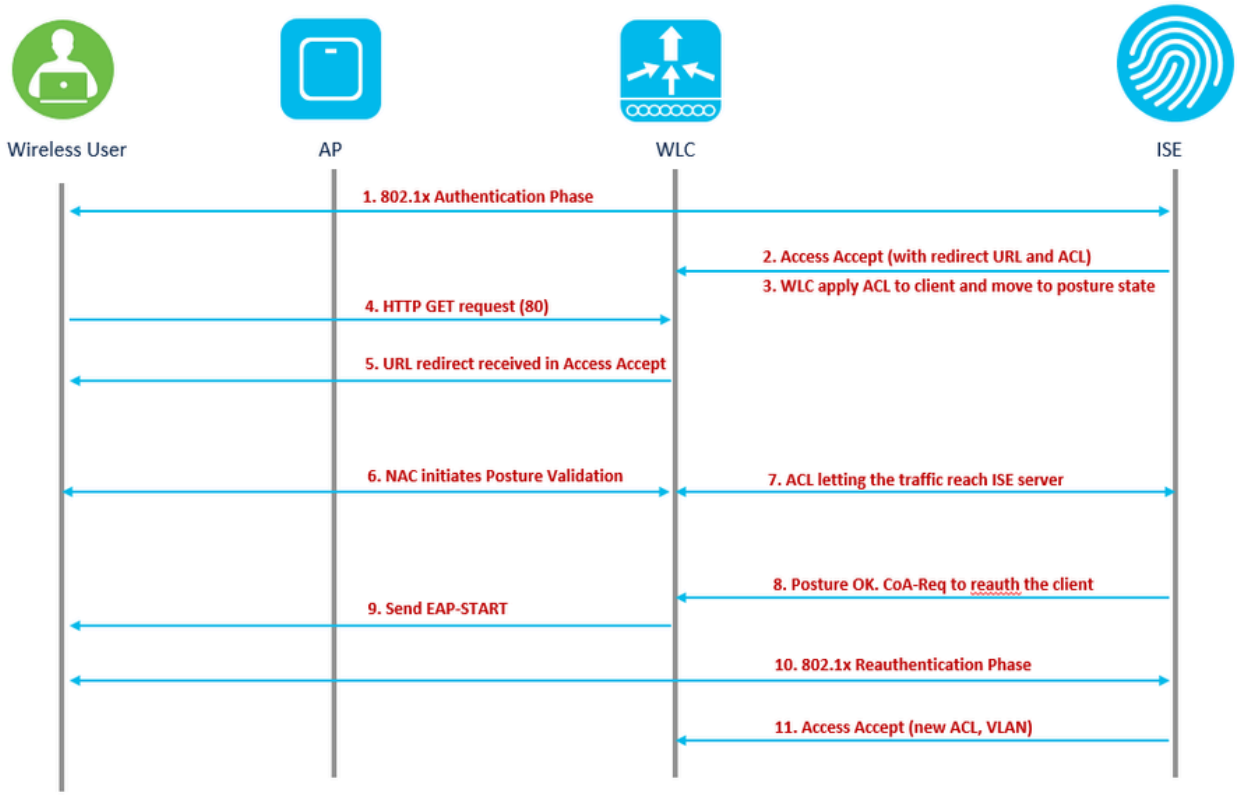
7. A WLC tem suporte para CoA-Req e Disconnect-Req conforme RFC 3576. A WLC precisa suportar CoA-Req para o serviço de reautenticação, de acordo com o RFC 5176.

8. Em vez das ACLs que podem ser baixadas, as ACLs pré-configuradas são usadas na WLC. O servidor ISE envia apenas o nome da ACL, que já está configurada no controlador.

9. Este design funciona para casos de VLAN e ACL. Em caso de substituição de VLAN, apenas redirecionamos a porta 80 que é redirecionada e permite (bridge) o resto do tráfego na VLAN de

quarentena. Para a ACL, a ACL de pré-autenticação recebida na aceitação de acesso é aplicada.

Esta figura fornece uma representação visual desse fluxo de recursos:



fluxo de trabalho de recurso

Neste caso de uso, um SSID que é usado apenas para usuários corporativos é habilitado para postura. Nenhum outro caso de uso, como BYOD, Convidado ou qualquer outro, existe neste SSID.

Quando um cliente sem fio se conecta ao SSID de postura pela primeira vez, ele deve baixar e instalar o módulo de postura no portal redirecionado do ISE e, finalmente, aplicar as ACLs relevantes com base no resultado da verificação de postura (compatível/não compatível).

Configurar

Diagrama de Rede

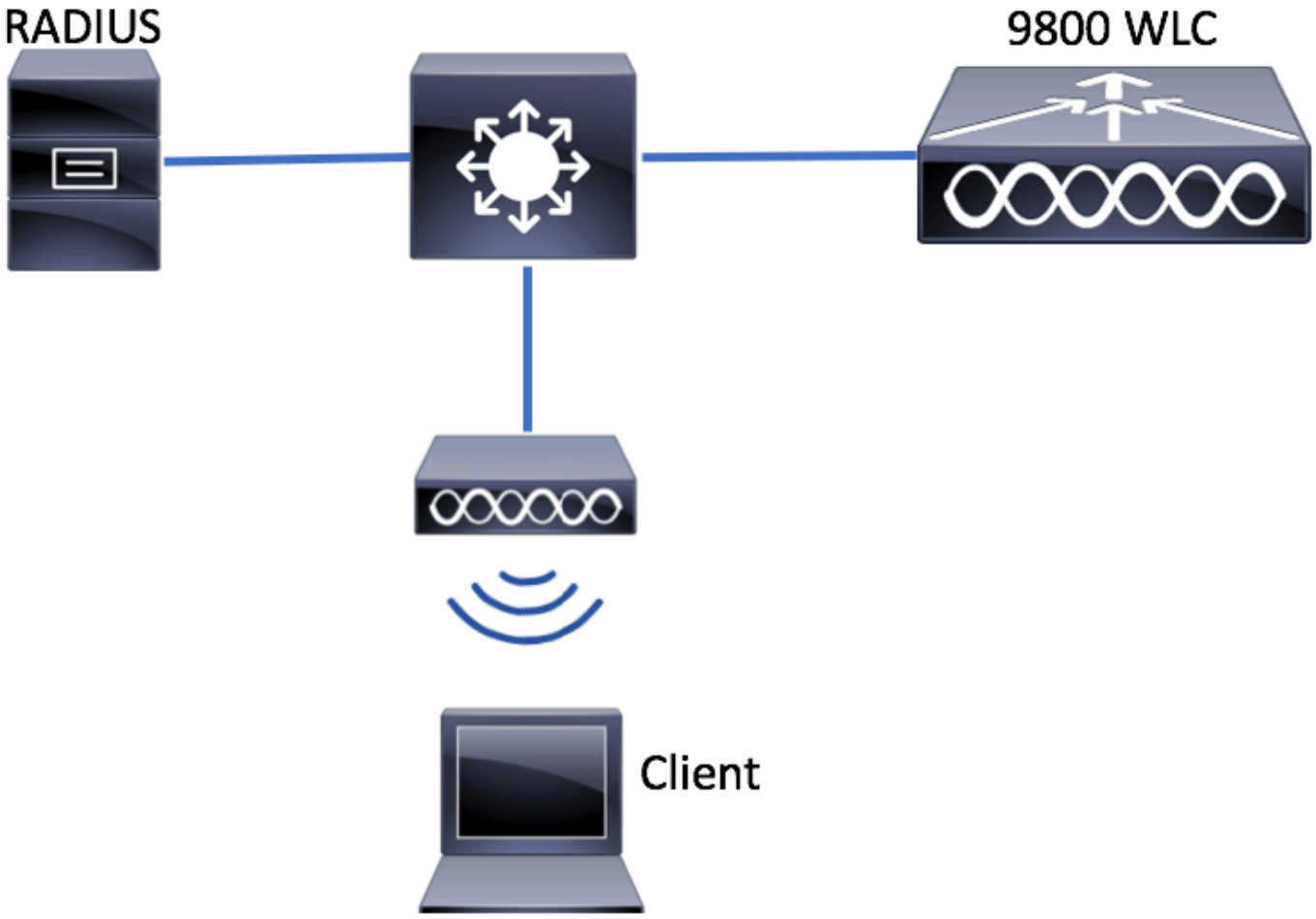
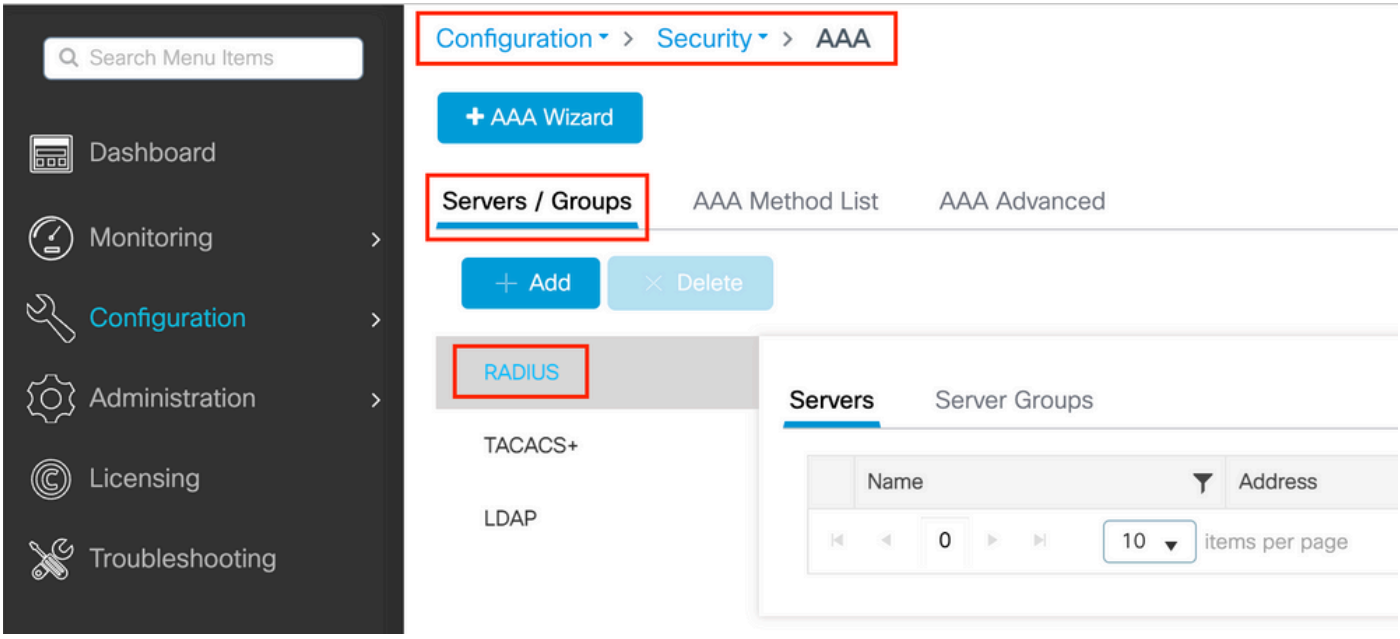


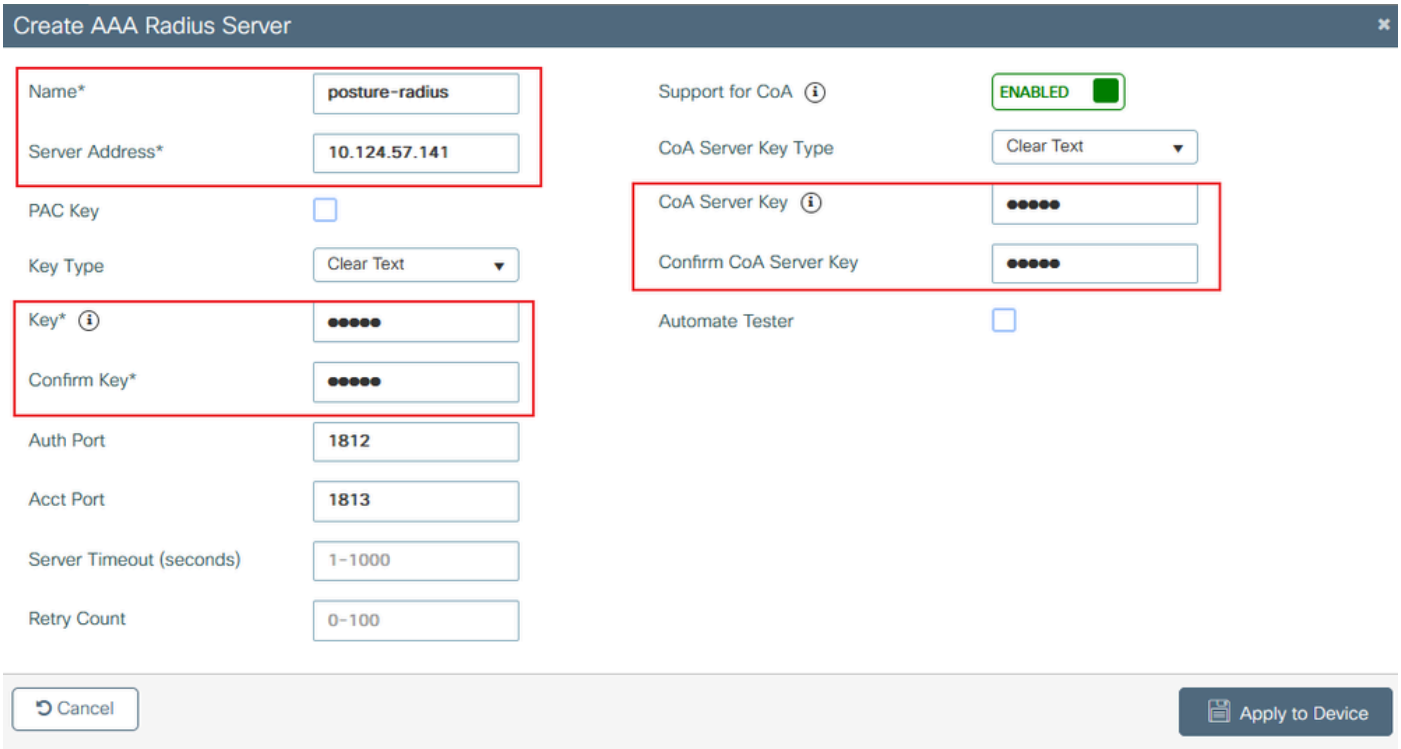
Diagrama de Rede

Configuração de AAA no 9800 WLC

Etapa 1. Adicionar o servidor ISE à configuração da WLC 9800. Navegue para Configuration > Security > AAA > Servers/Groups > RADIUS > Servers > + Add e insira as informações do servidor RADIUS como mostrado nas imagens. Verifique se o suporte para CoA está ativado para NAC de postura.

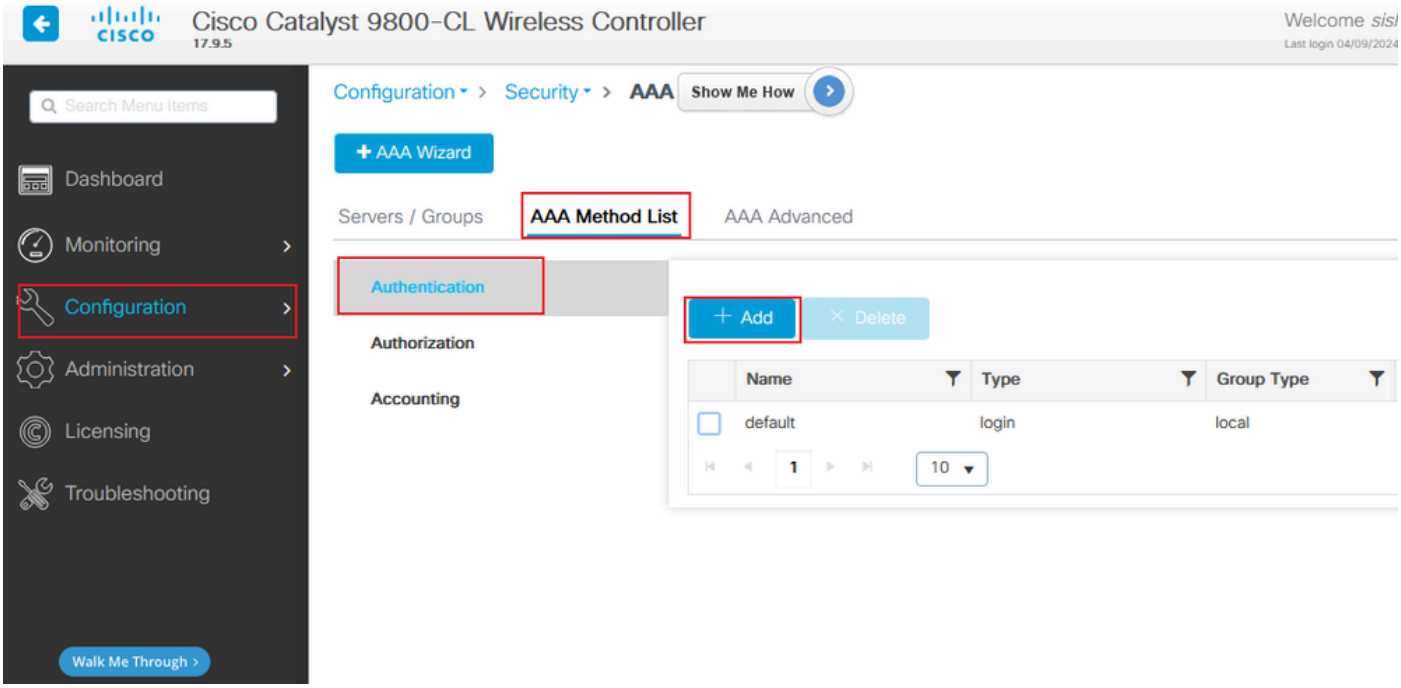


9800 criar servidor radius

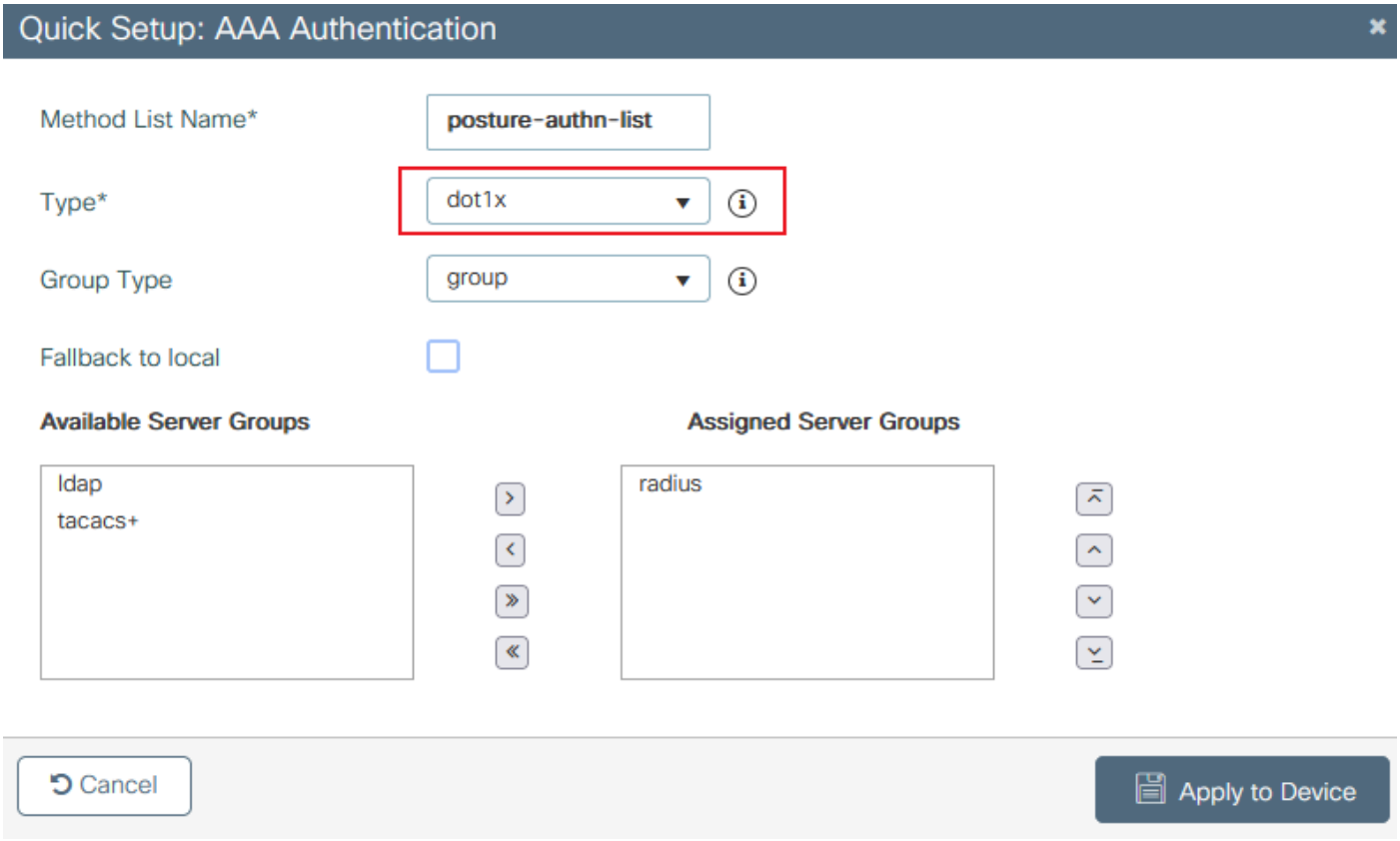


9800 criar detalhes de raio

Etapa 2. Criar uma lista de métodos de autenticação. Navegue para Configuration > Security > AAA > AAA Method List > Authentication > + Add conforme mostrado na imagem:

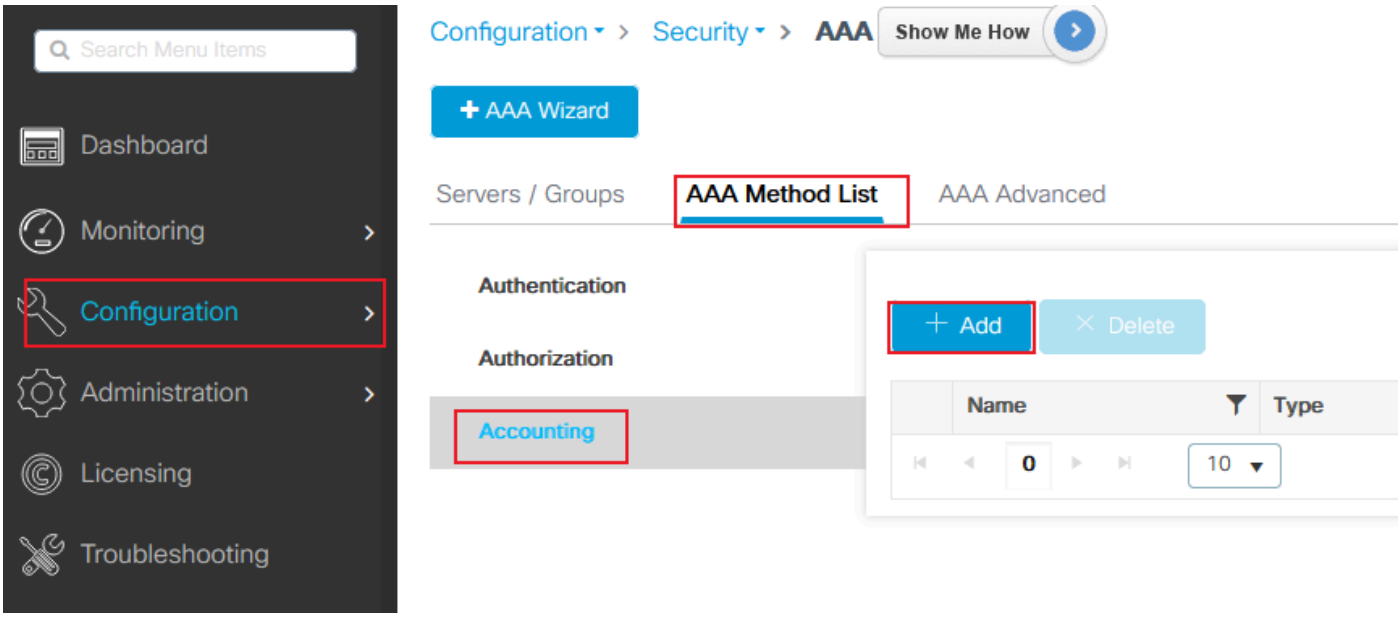


9800 add auth list

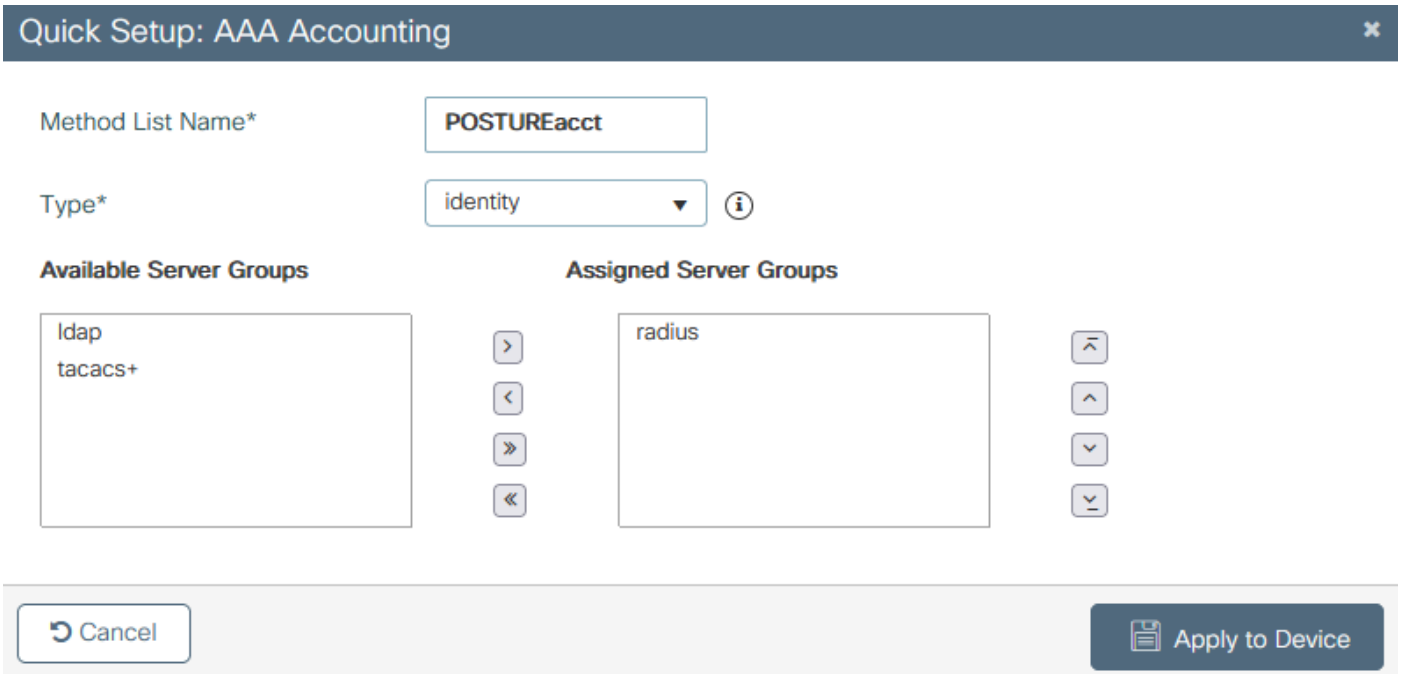


9800 criar detalhes da lista de autenticação

Etapa 3. (Opcional) Crie uma lista de métodos contábeis conforme mostrado na imagem:



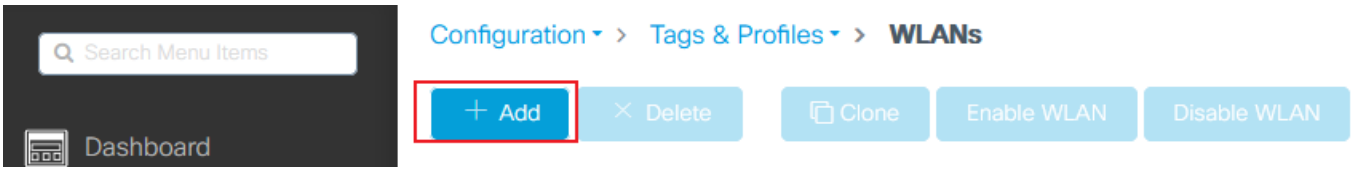
9800 adicionar lista de contas



9800 criar detalhes da lista de contas

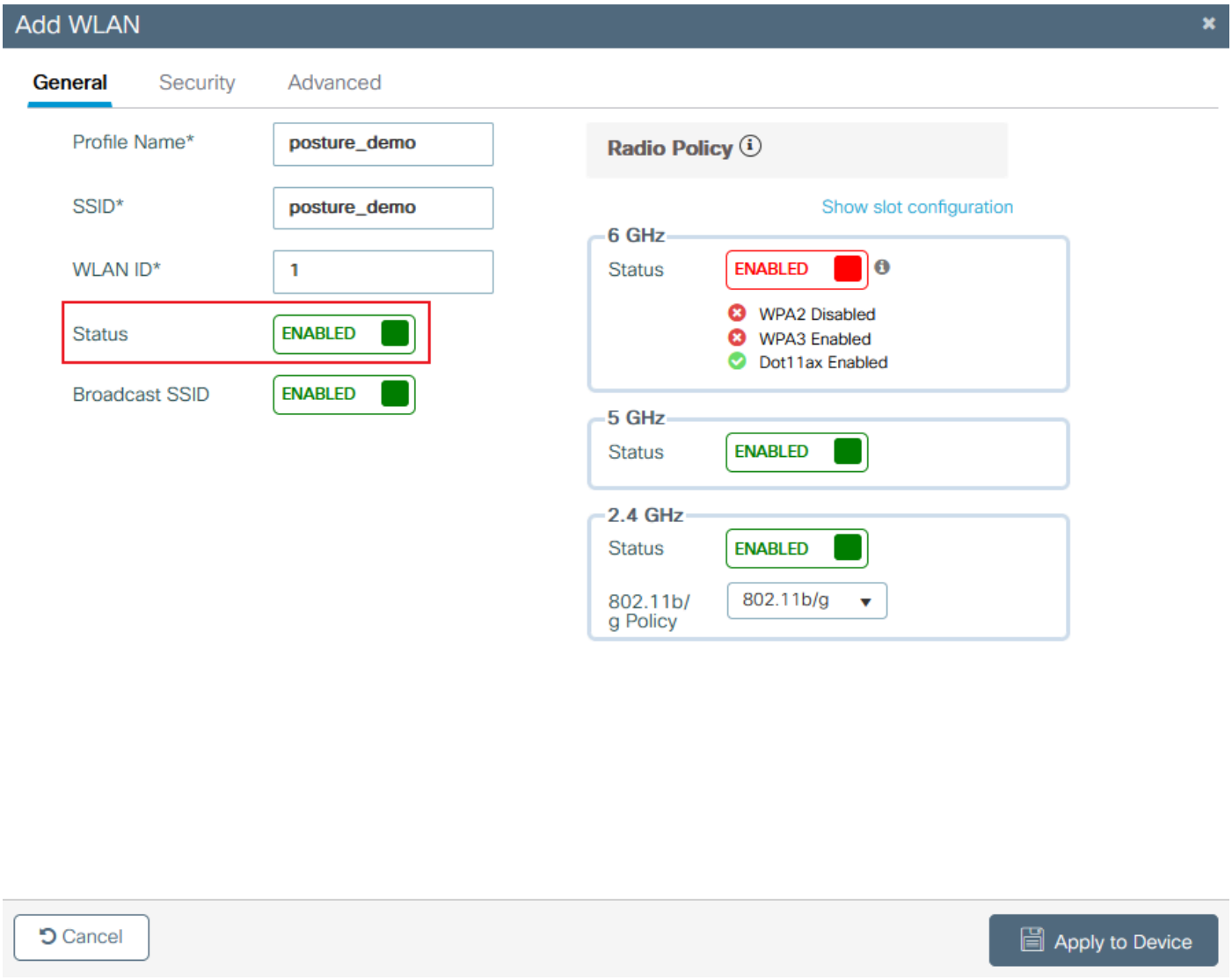
Configuração de WLAN

Etapa 1. Criar a WLAN. Navegue até Configuration > Tags & Profiles > WLANs > + Add e configure a rede conforme necessário:



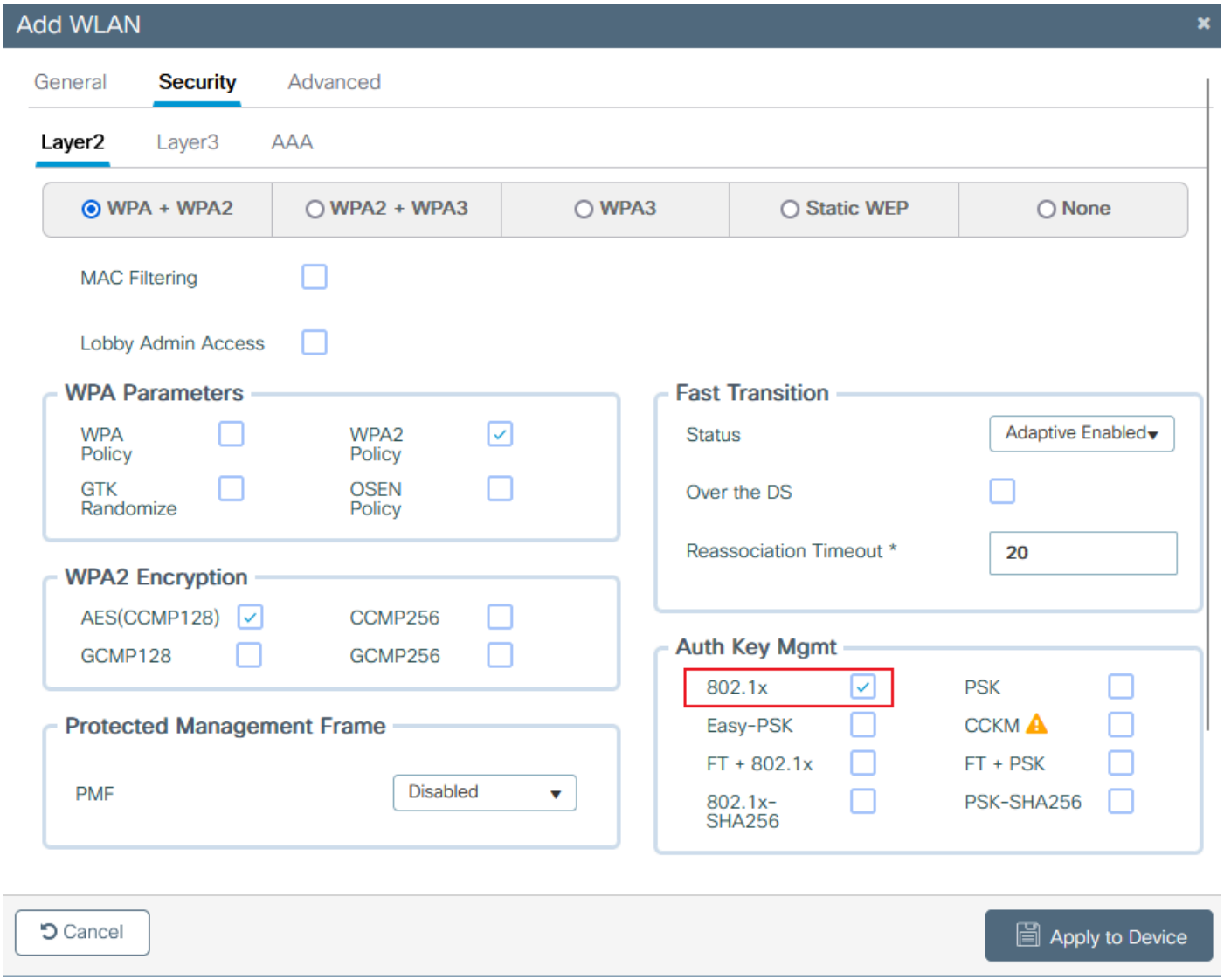
9800 WLAN add

Etapa 2. Inserir as informações gerais da WLAN.

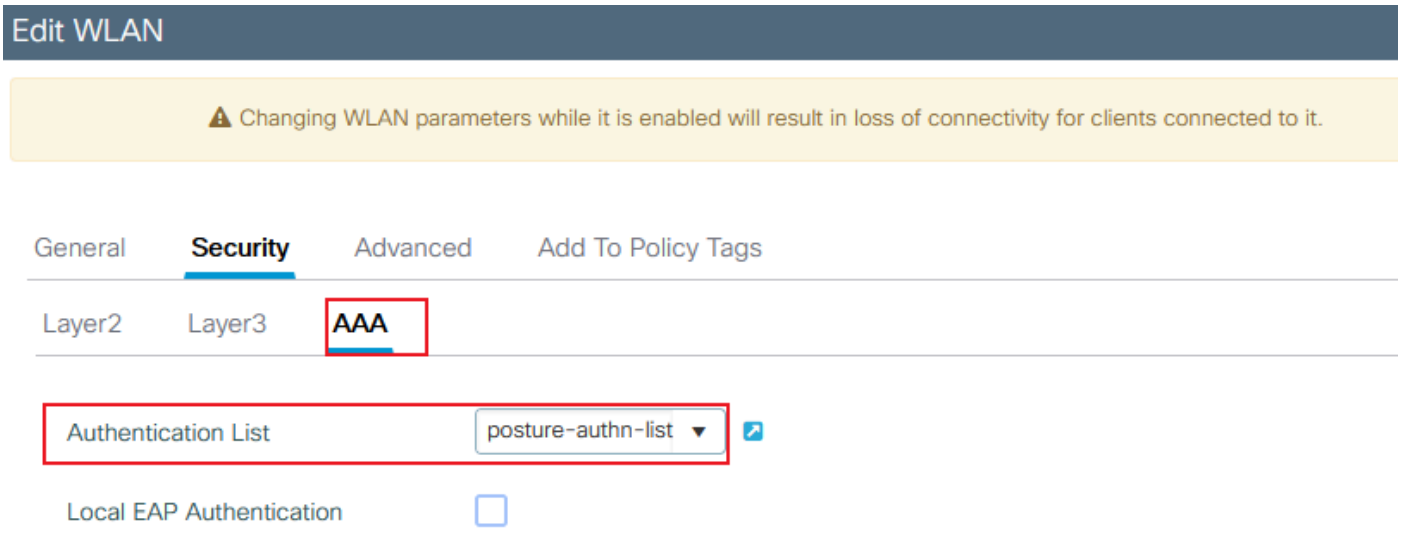


9800 criar WLAN geral

Etapa 3. Navegue até a guia Segurança e escolha o método de segurança necessário. Nesse caso, escolha '802.1x' e a lista de autenticação AAA (que você criou na Etapa 2. na seção Configuração AAA) será necessária:



9800 criar segurança de WLAN L2

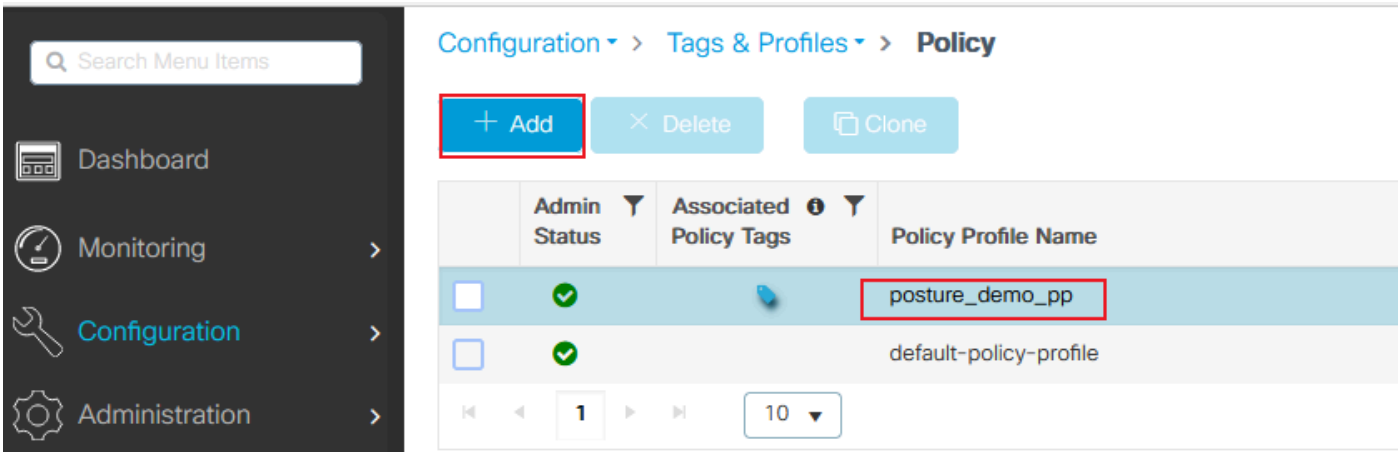


9800 criar segurança de WLAN AAA

Configuração de perfil de política

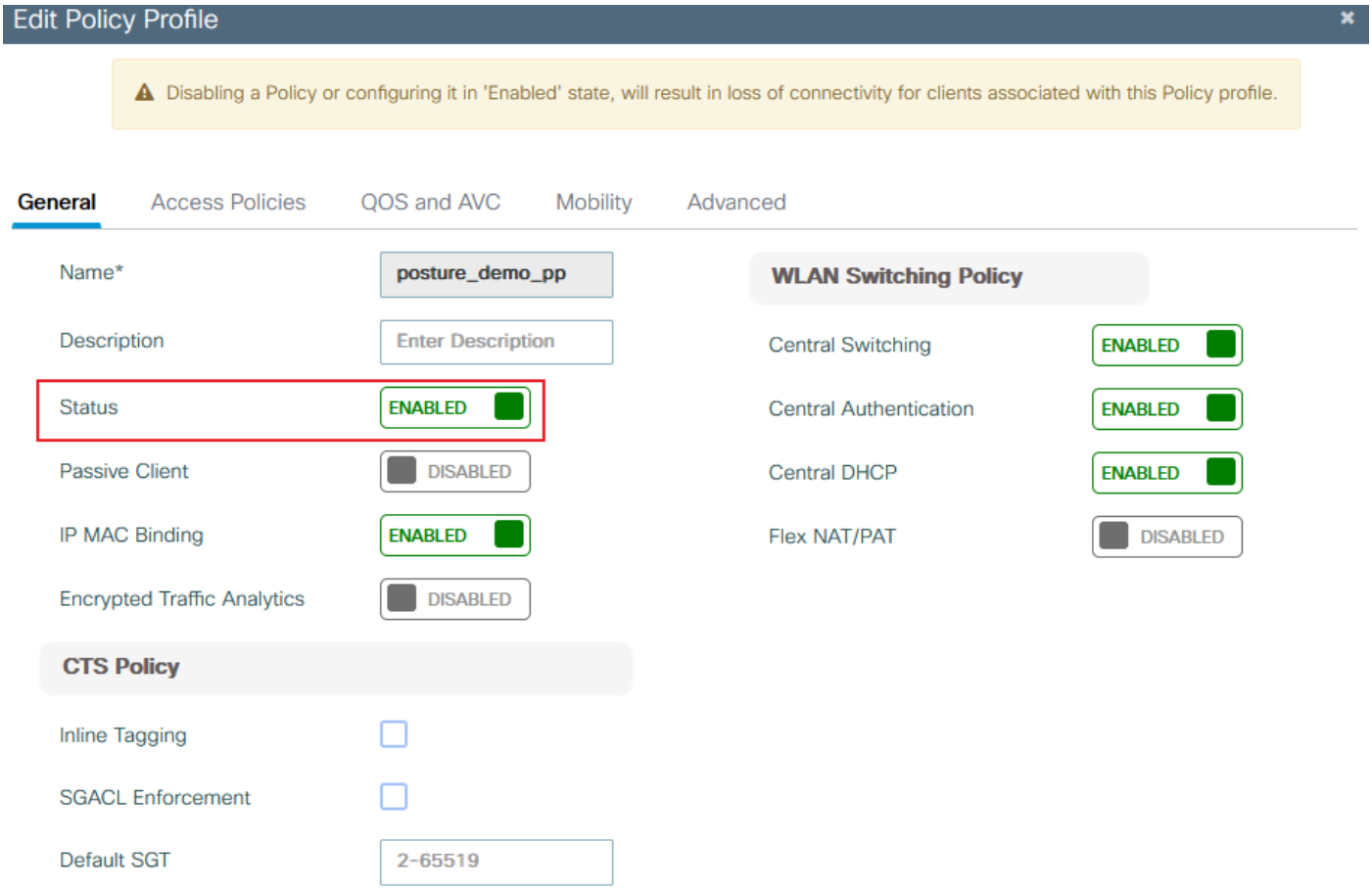
Dentro de um Perfil de política, você pode decidir atribuir os clientes a qual VLAN, entre outras configurações (como Lista de controles de acesso (ACLs), Qualidade de serviço (QoS), Âncora de mobilidade, Temporizadores, etc.). Você pode usar o perfil de política padrão ou criar um novo.

Etapa 1. Crie um novo Perfil de Política. Navegue até Configuration > Tags & Profiles > Policy e crie um novo:



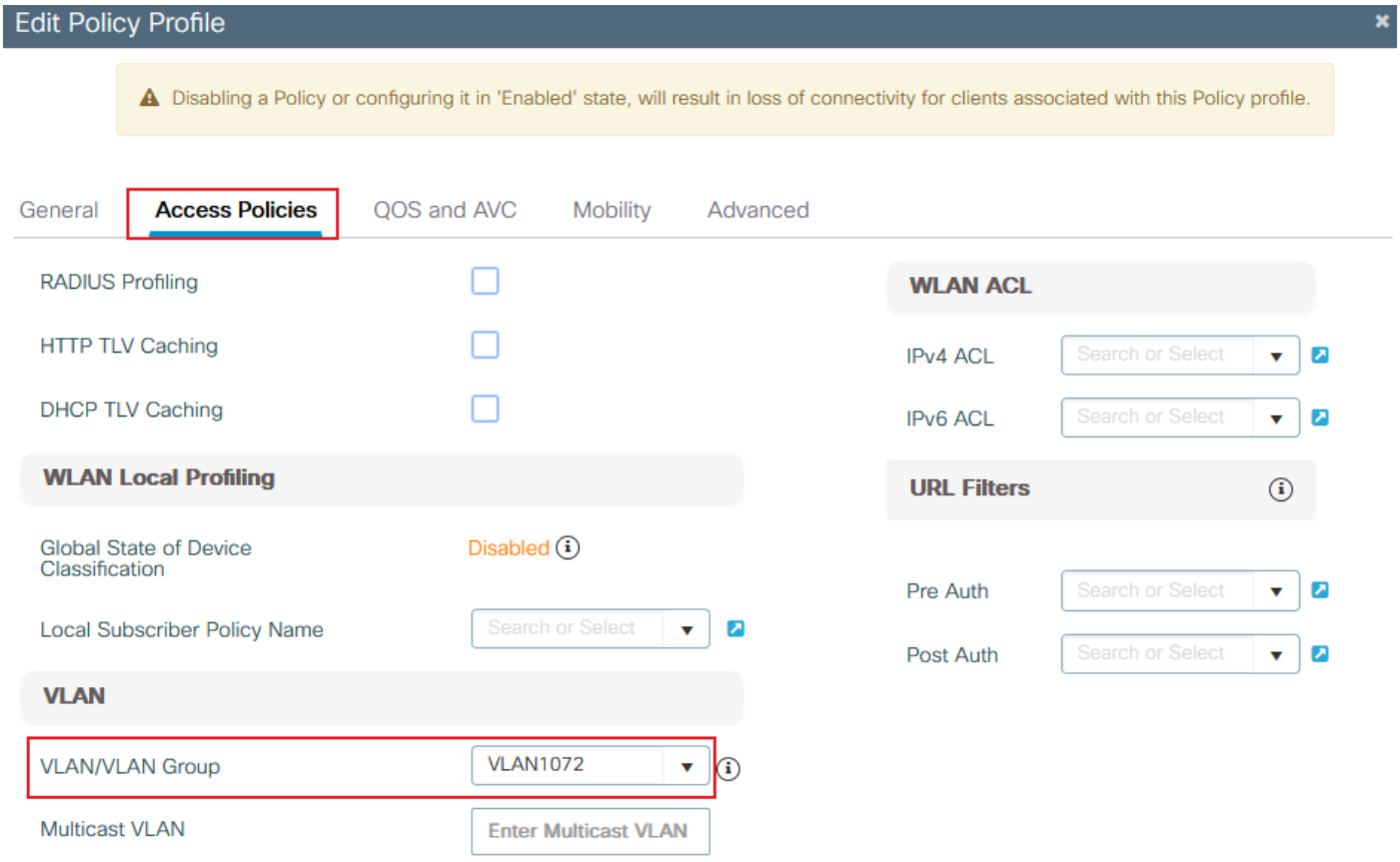
9800 adicionar perfil de política

Verifique se o perfil está ativado.



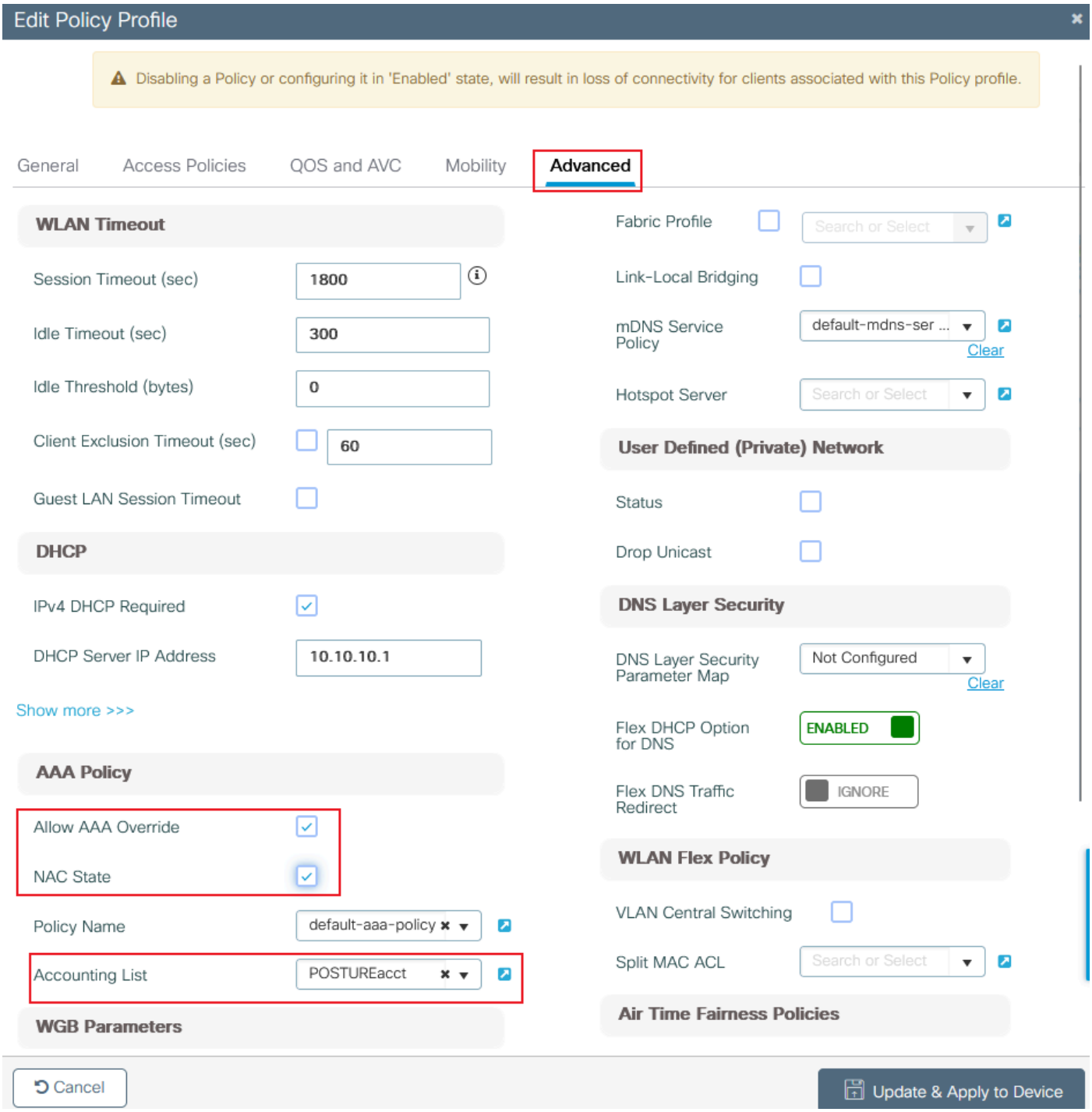
9800 criar perfil de política geral

Etapa 2. Escolher a VLAN. Navegue até a guia Access Policies e escolha o nome da VLAN na lista suspensa ou digite manualmente a VLAN-ID. Não configure uma ACL no perfil de política:



9800 criar VLAN de perfil de política

Etapa 3. Configurar o perfil de política para aceitar substituições ISE (permitir substituição de AAA) e Alteração de Autorização (CoA) (Estado NAC). Como opção, você também pode especificar um método de auditoria:

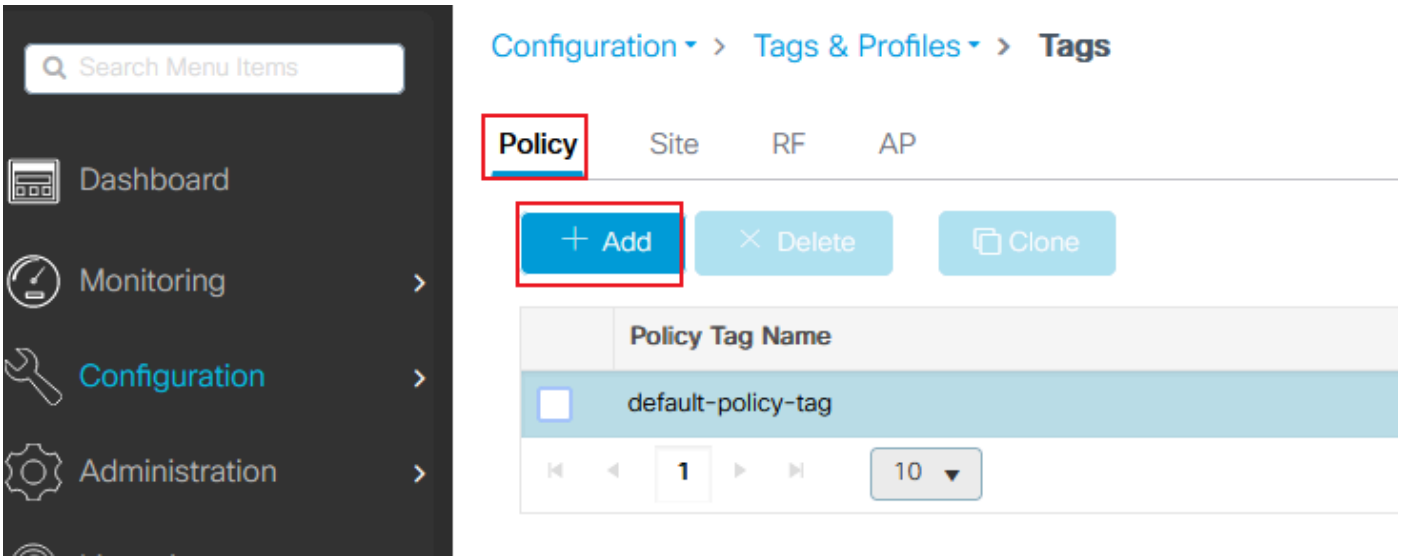


9800 criar perfil de política Avançado

Configuração de marca de política

Dentro da marca de política, você vincula a SSID ao perfil de política. Você pode criar uma nova marca de política ou usar a marca default-policy.

Navegue para Configuration > Tags & Profiles > Tags > Policy e adicione um novo se necessário, como mostrado na imagem:



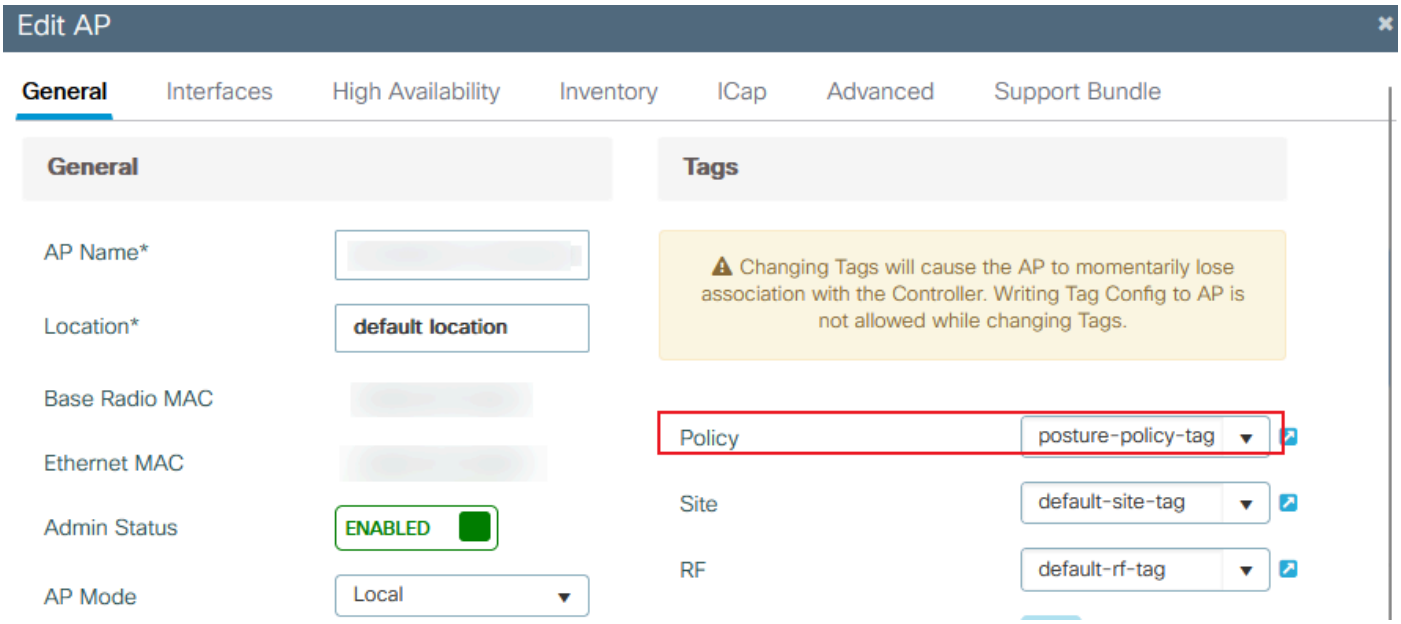
9800 policy tag add

Vincule o perfil de WLAN ao perfil de política desejado:

Detalhes da etiqueta de política do 9800

Atribuição de marca de política

Atribua a marca de política aos APs necessários. Navegue para Configuration > Wireless > Access Points > AP Name > General Tags , faça a atribuição necessária e clique em Update & Apply to Device .



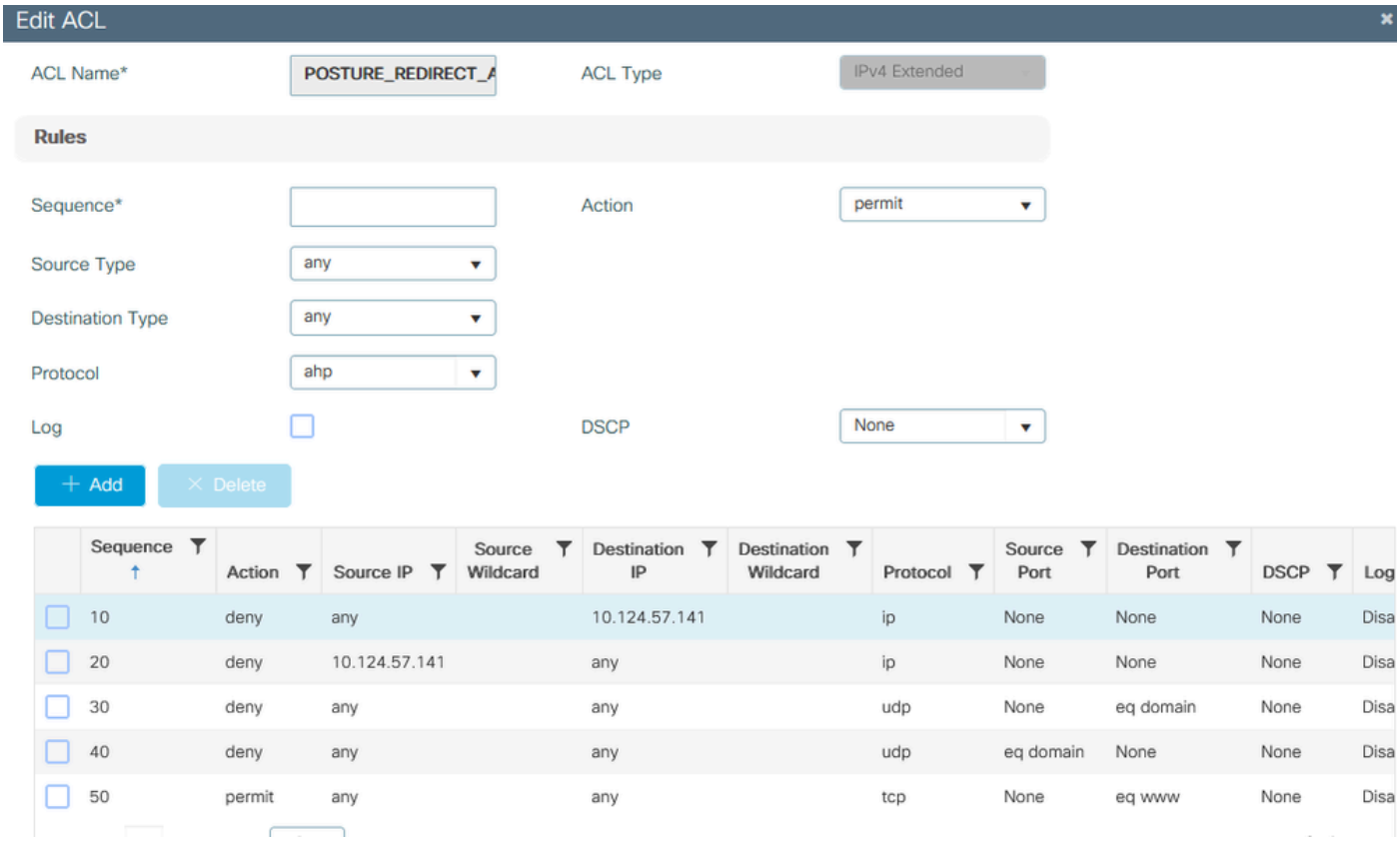
Atribuição de tag de política 9800

Configuração de ACL de redirecionamento

Navegue até Configuração > Segurança > ACL > + Adicionar para criar uma nova ACL.

A ACL usada para o redirecionamento do portal de postura tem os mesmos requisitos que o CWA (autenticação da Web central).

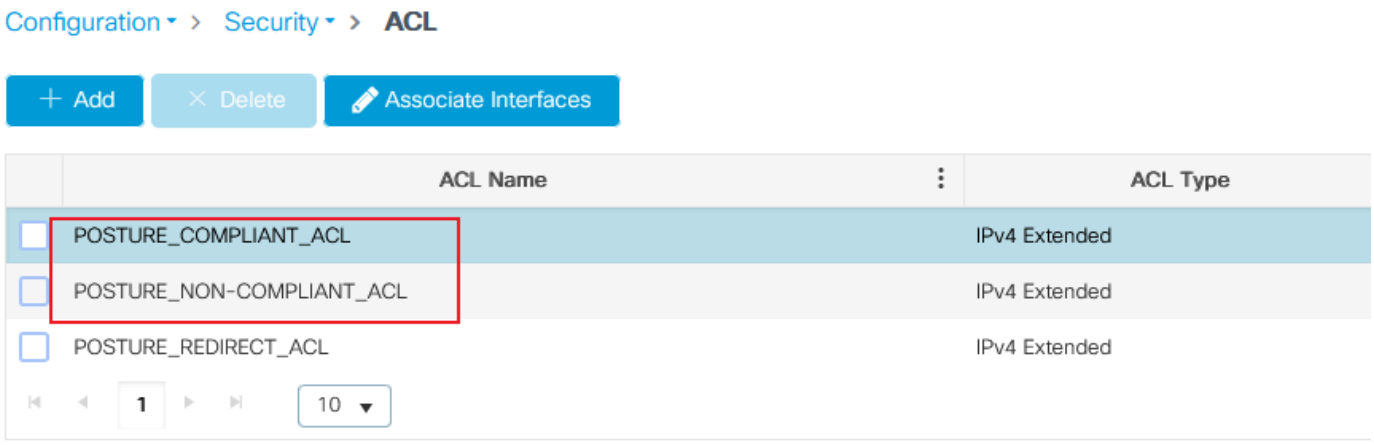
Você precisa negar o tráfego para os nós de ISE PSNs, bem como negar o DNS e permitir todo o restante. Essa ACL de redirecionamento não é uma ACL de segurança, mas uma ACL de punt que define qual tráfego vai para a CPU (em permissões) para tratamento posterior (como redirecionamento) e qual tráfego permanece no plano de dados (em negação) e evita o redirecionamento. A ACL deve ser semelhante a esta (substitua 10.124.57.141 pelo endereço IP do ISE neste exemplo):



Detalhes da ACL de redirecionamento 9800

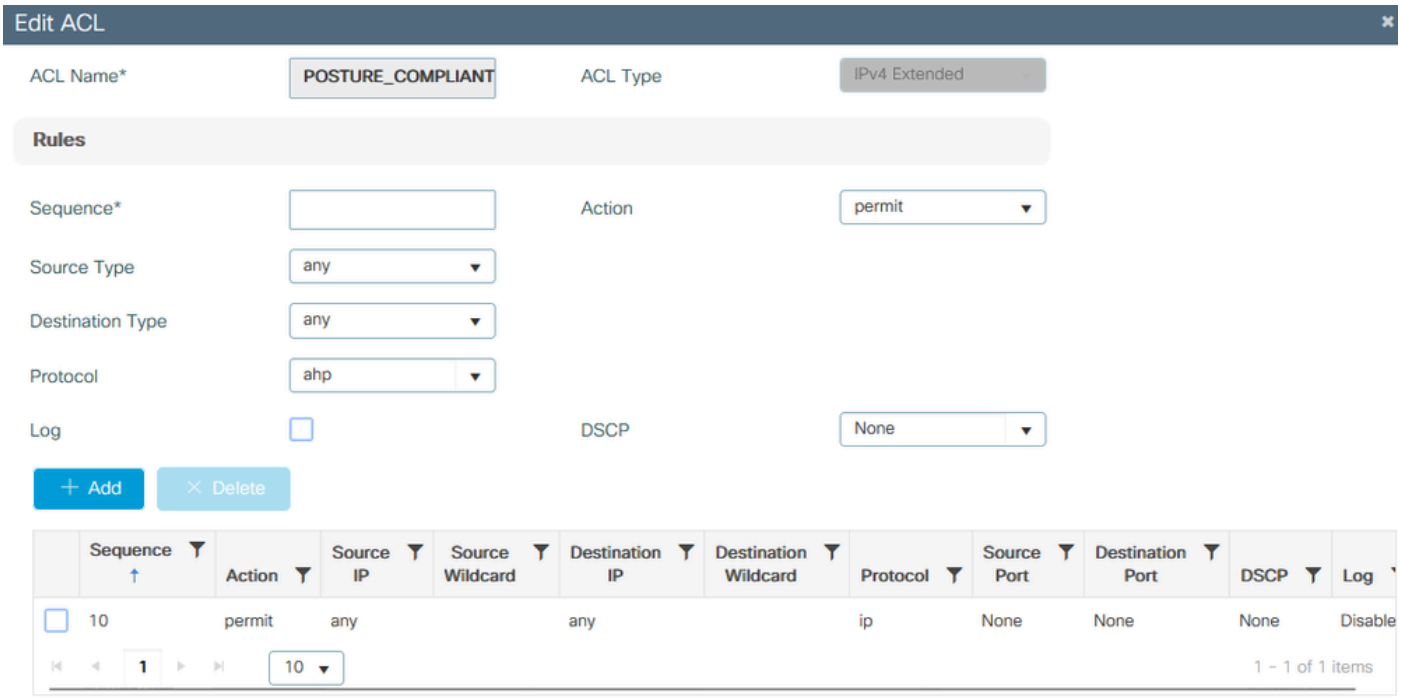
Configuração da ACL de política

Nesse caso, você precisa definir ACLs separadas no 9800 WLC para que o ISE autorize os cenários Compatível e Não Compatível com base no resultado da verificação de violação.



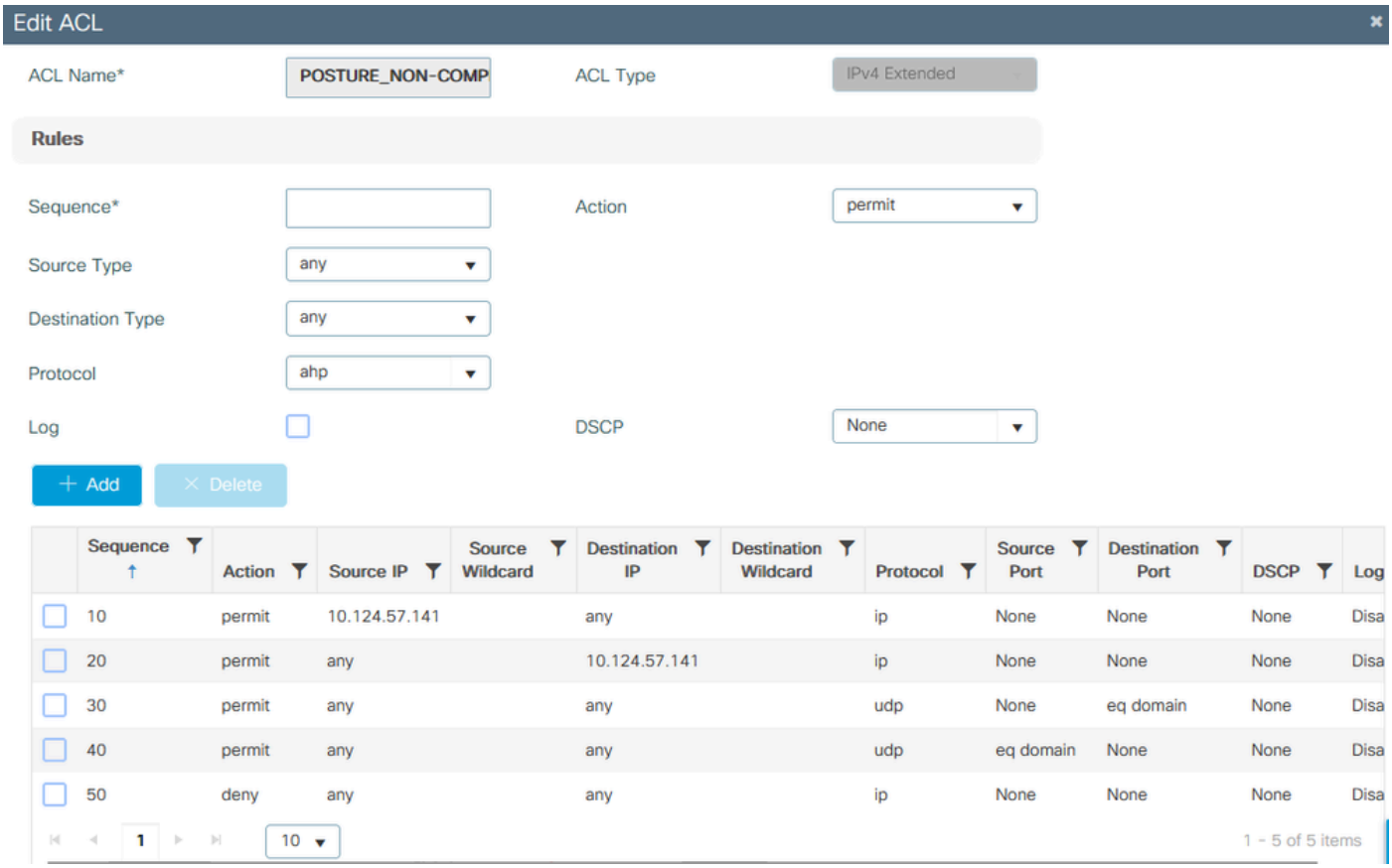
ACL 9800 geral

Para um cenário em conformidade, basta usar permit all nesse caso. Como outra configuração comum, você também pode fazer com que o ISE não autorize nenhuma ACL no resultado compatível, que é equivalente a permitir tudo no lado do 9800:



ACL 9800 - Compatível

Para um cenário não compatível, o cliente permite acesso apenas a determinadas redes, geralmente o servidor de remediação (o próprio ISE, neste caso):

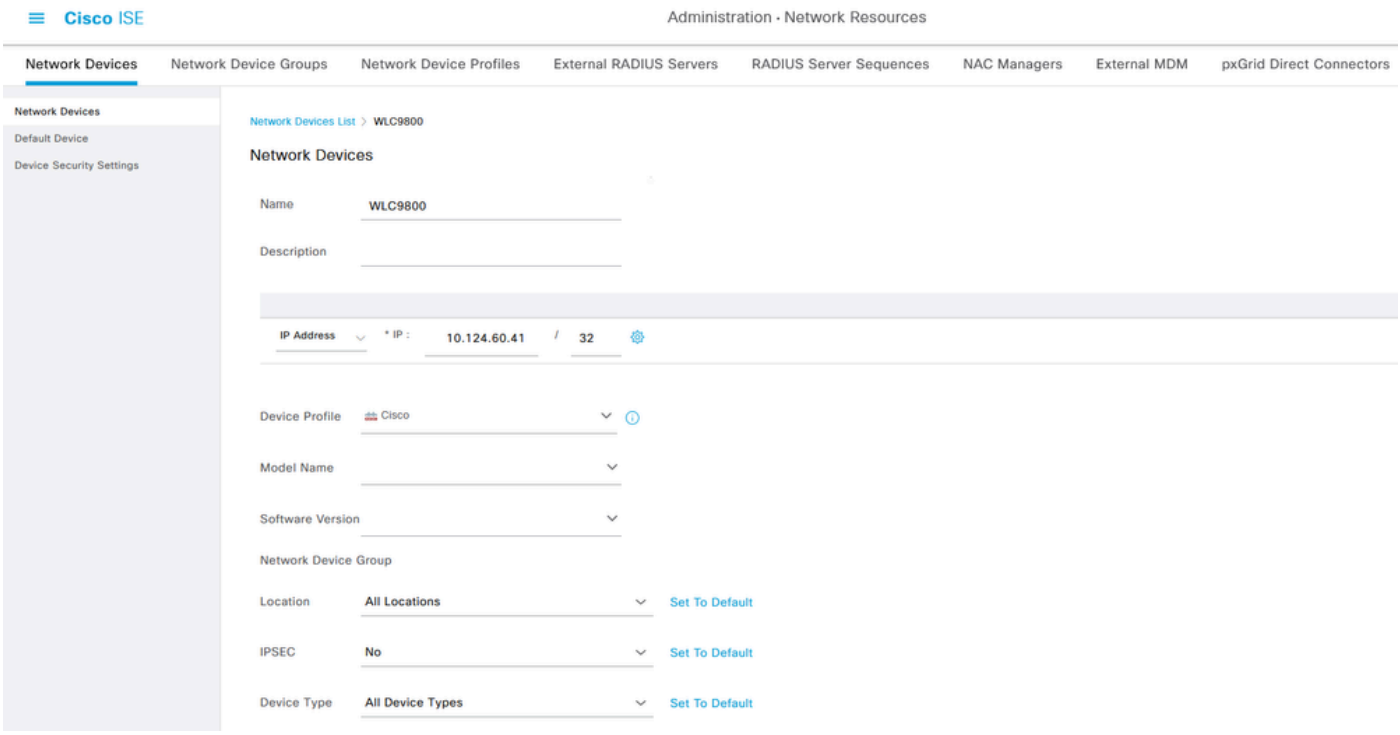


ACL 9800 - Não compatível

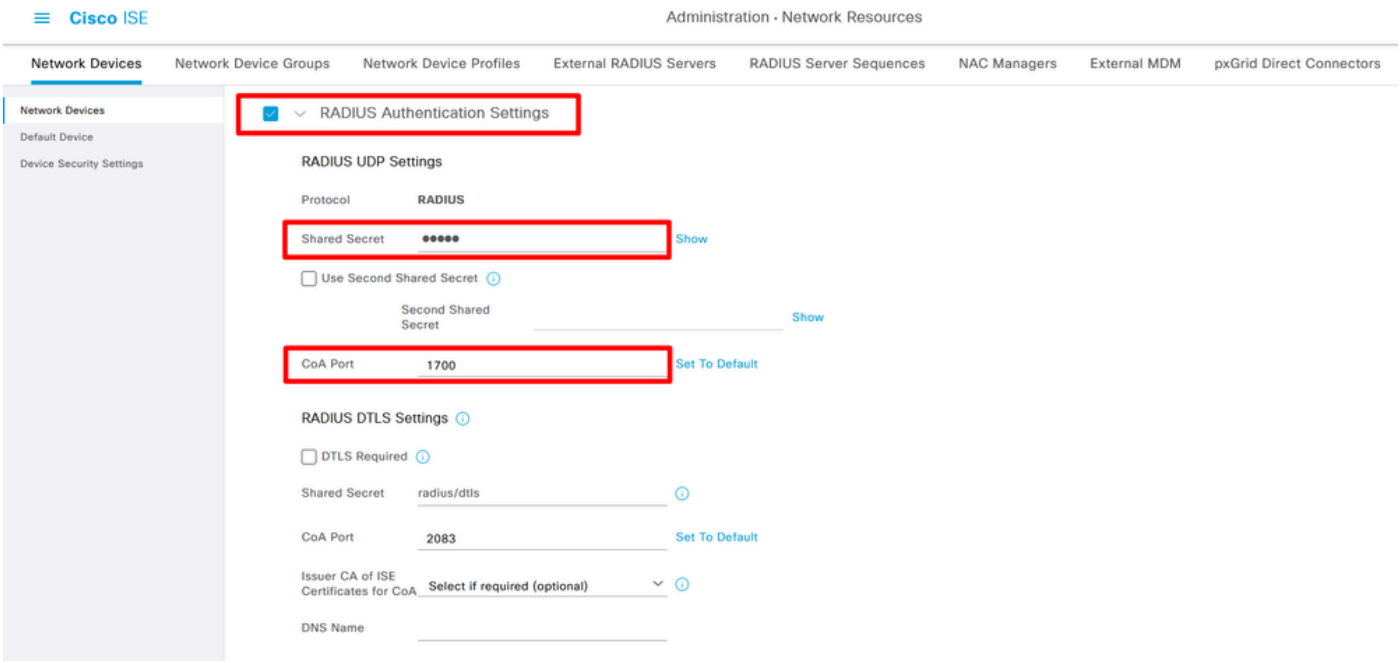
Configuração e postura de AAA no ISE

Requisito de postura: Neste exemplo, o requisito para determinar a conformidade é detectar se um arquivo de teste específico existe na área de trabalho usada para testar o PC com Windows.

Etapa 1. Adicione a WLC 9800 como NAD no ISE. Navegue até Administração> Recursos de rede> Dispositivos de rede> Adicionar:



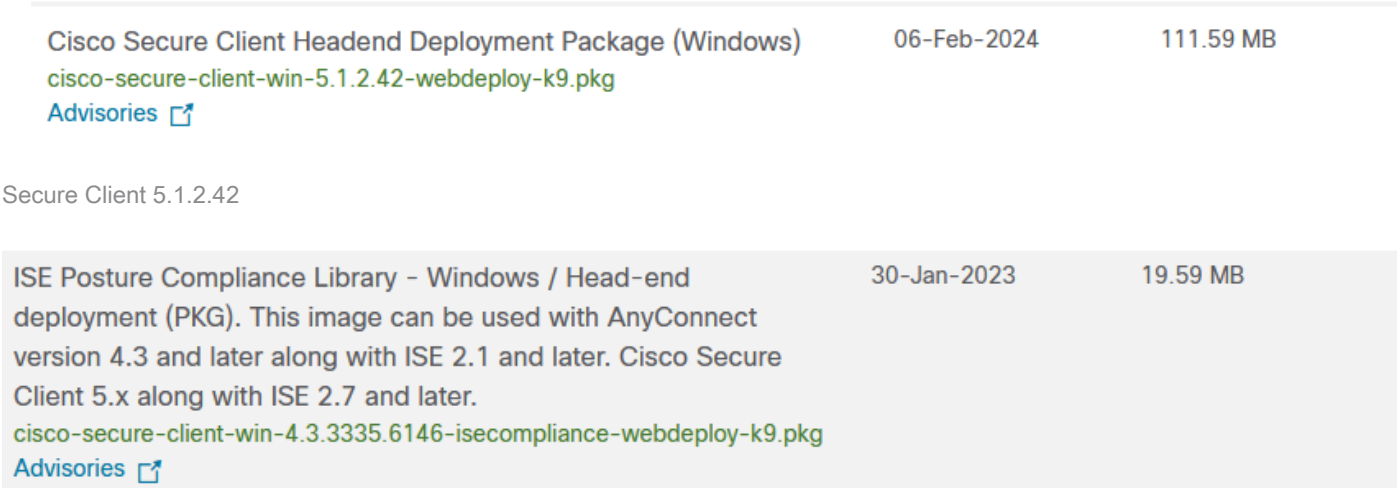
Adicionar dispositivo de rede 01



Adicionar dispositivo de rede 02

Etapa 2. Faça o download do pacote de implantação e do módulo de conformidade do Cisco Secure Client Headend no site do Cisco Software CCO.

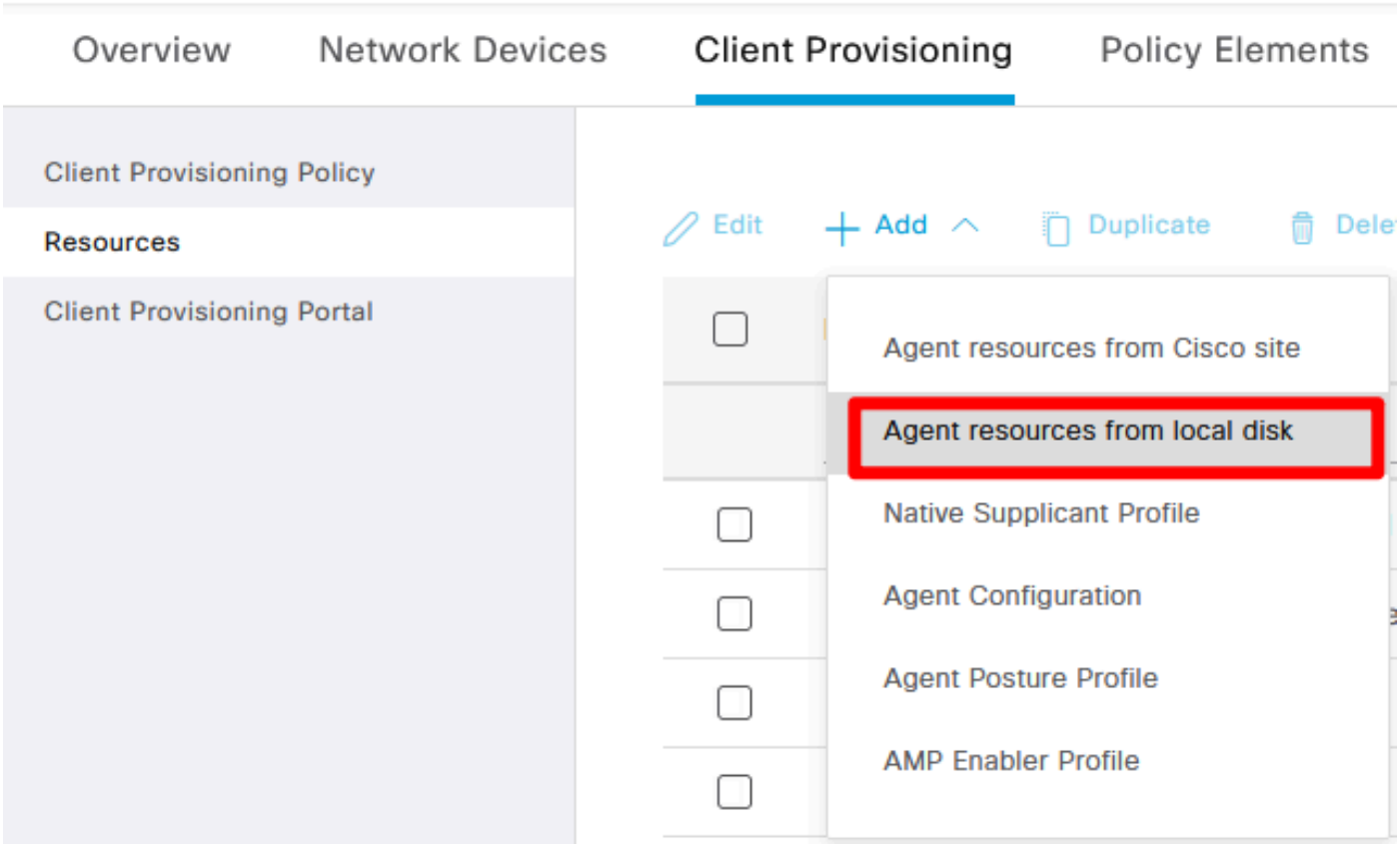
Acessar e pesquisar o Cisco Secure Client:



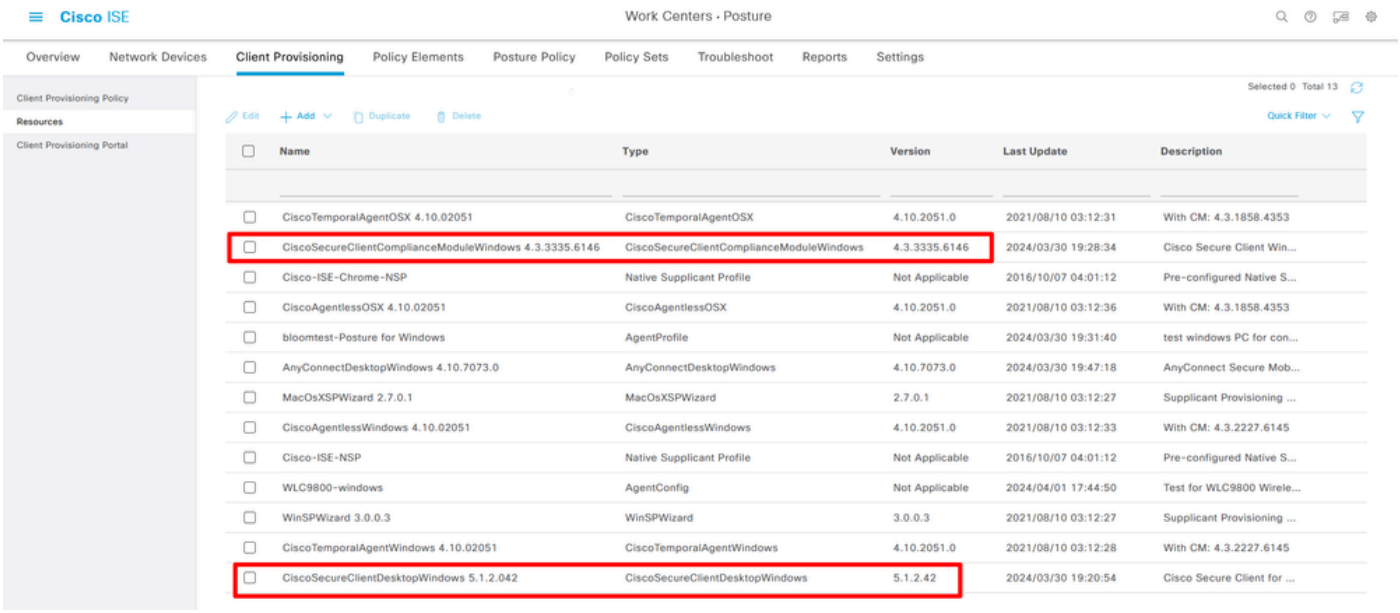
Secure Client 5.1.2.42

Módulo 4.3 de conformidade com ISE

Etapa 3. Carregar o pacote do módulo de implantação e conformidade do Cisco Secure Client Headend para o provisionamento do cliente ISE. Navegue até Centros de trabalho> Postura> Provisionamento do cliente> Recursos . Clique em Adicionar, Escolher Recursos do agente do disco local na caixa suspensa:

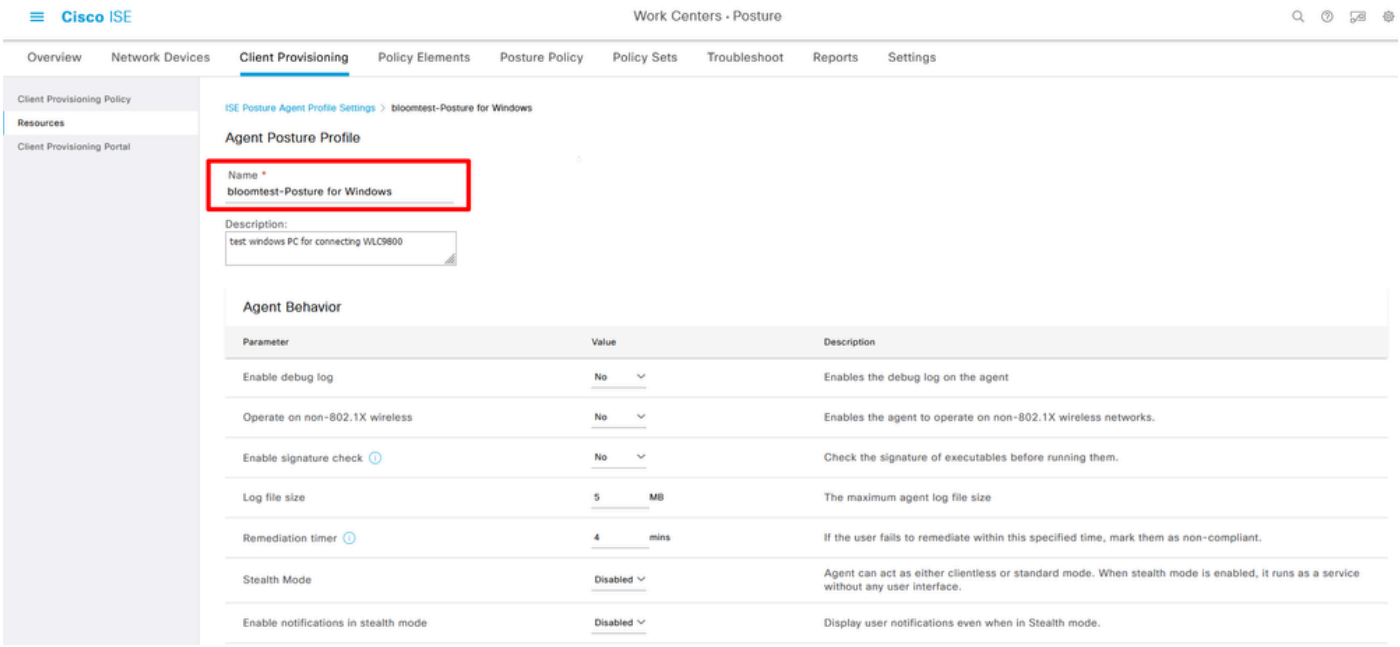


Carregar cliente seguro



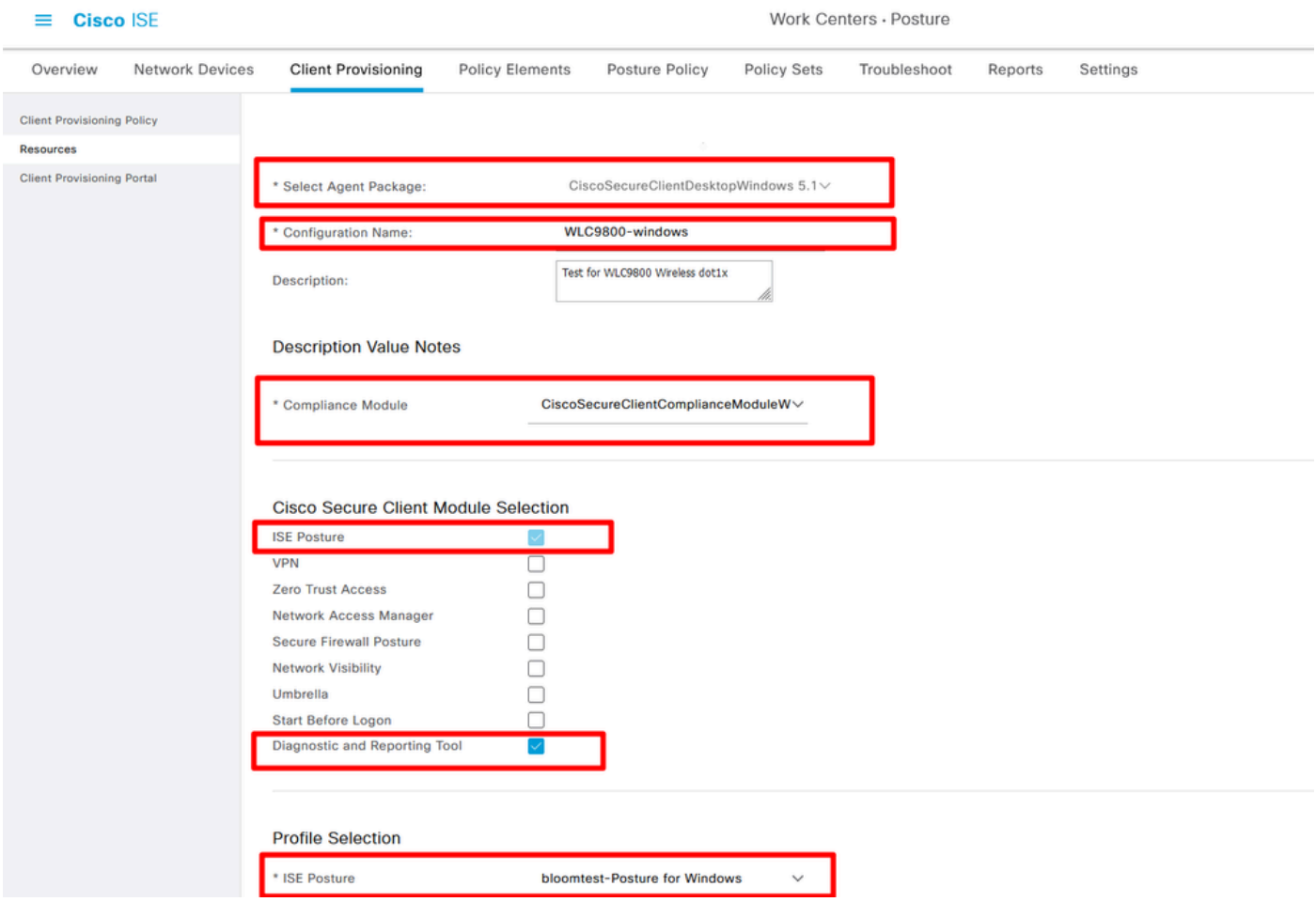
Carregamento do Cliente Seguro e do Módulo de Conformidade com êxito

Etapa 4. Criar Perfil de Situação do Agente Navegue até Centros de Trabalho> Postura> Provisionamento do Cliente> Recursos> Adicionar> Perfil de Situação do Agente:



Perfil de postura do agente

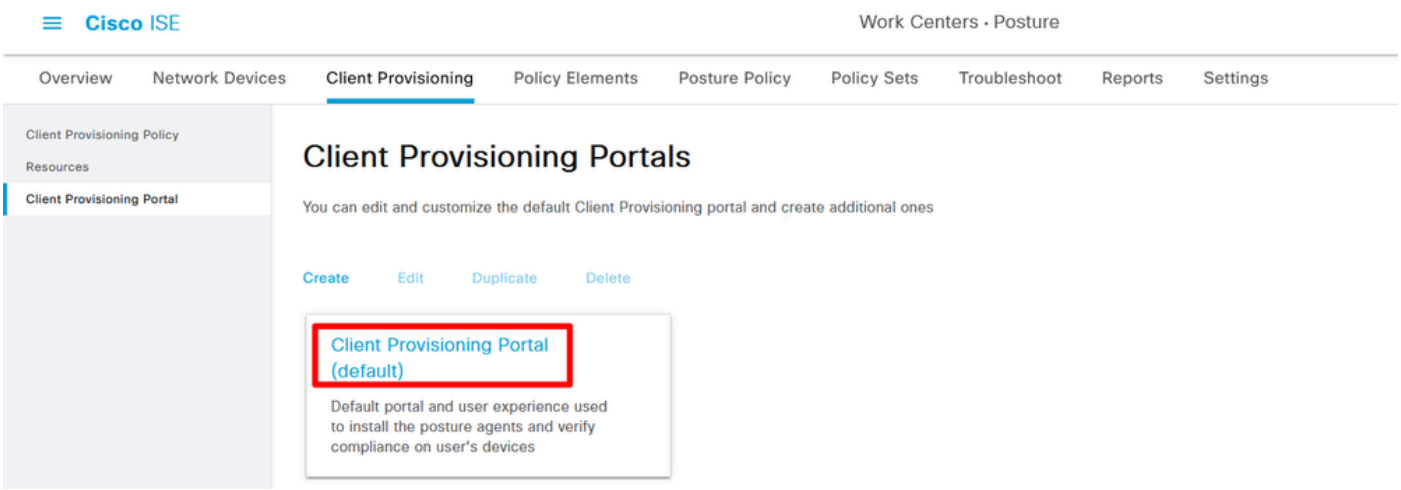
Etapa 5. Criar configuração do agente Navegue até Centros de trabalho> Postura> Provisionamento de cliente> Recursos> Adicionar> Configuração do agente:



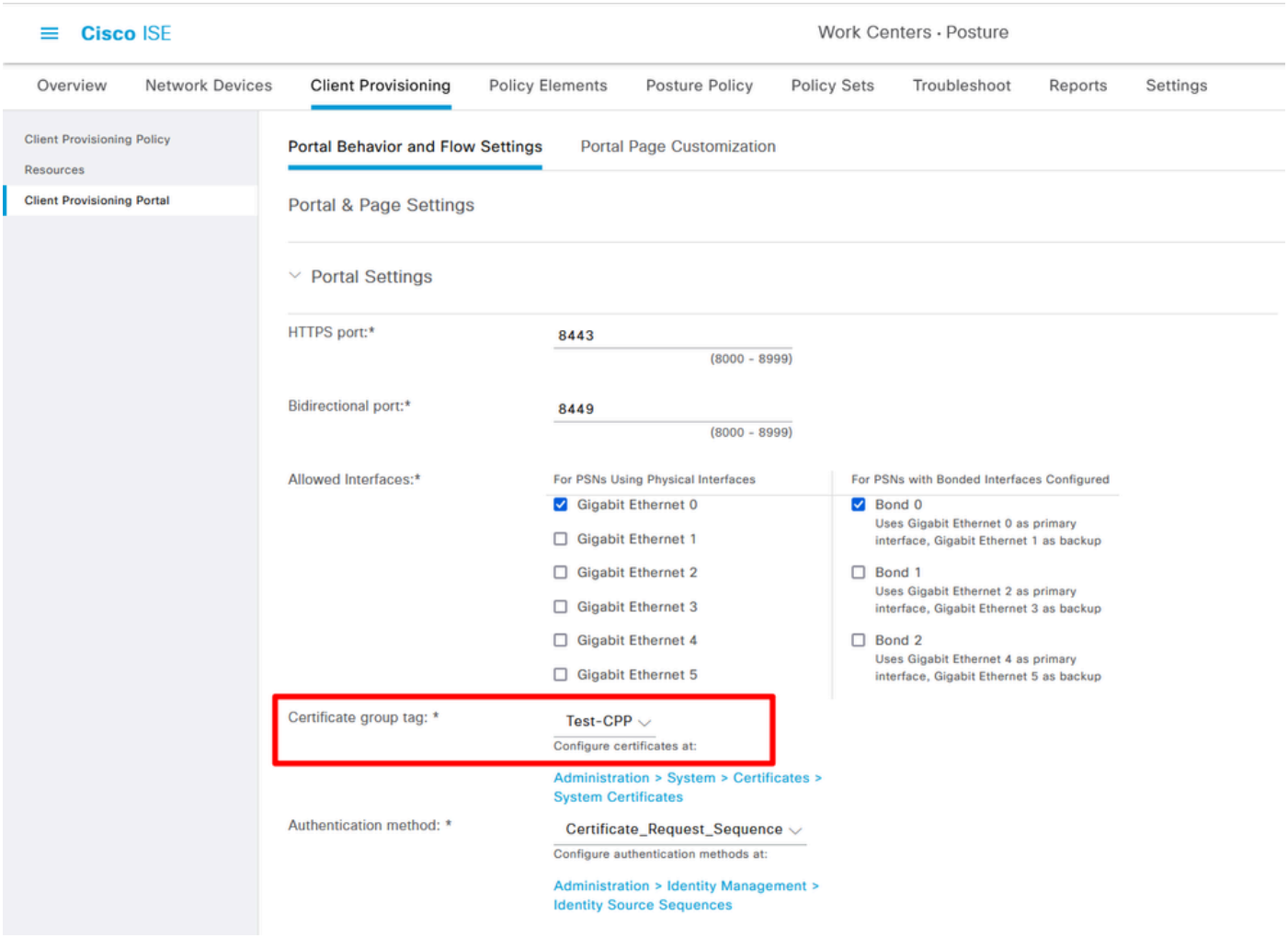
Adicionar configuração de agente

Etapa 6. Confirme o portal de Provisionamento de Cliente, use o portal padrão para teste se estiver OK. (Gere CSR e Solicite um certificado SSL do servidor de CA e substitua a marca Grupo de Certificados nas Configurações deste portal. Caso contrário, um aviso de certificado não confiável ocorrerá durante o processo de teste.)

Navegue até Centros de trabalho> Postura> Provisionamento de clientes> Portais de provisionamento de clientes:

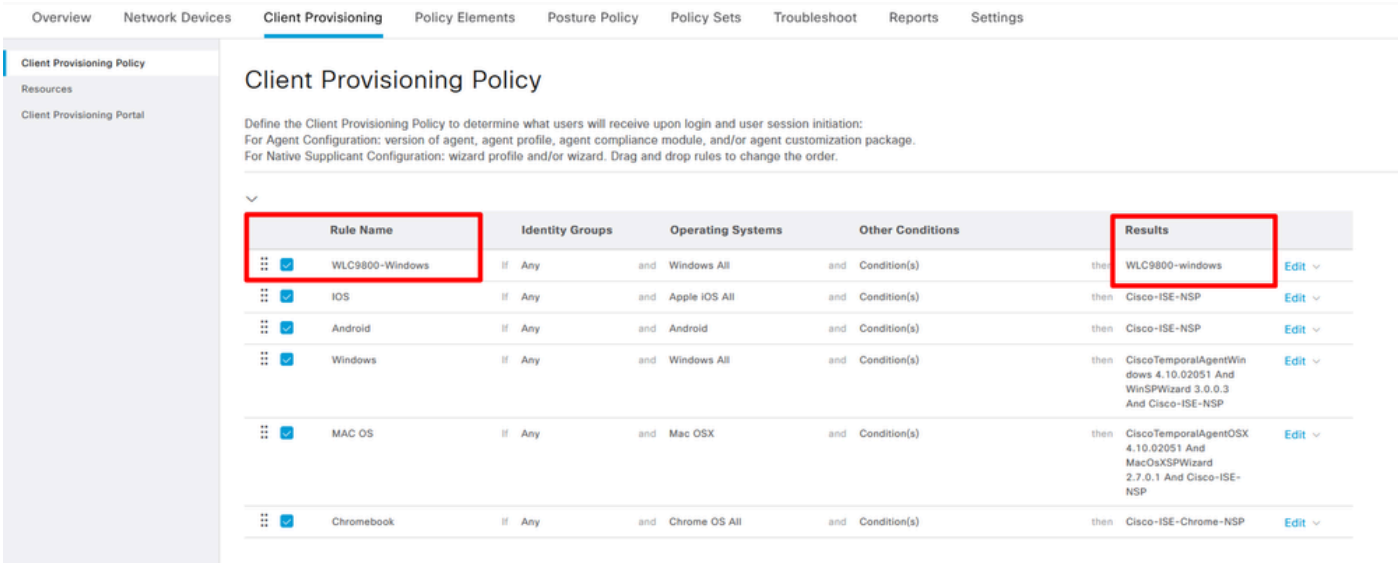


Escolher Portal de Provisionamento do Cliente 01



Escolher Portal de Provisionamento do Cliente 02

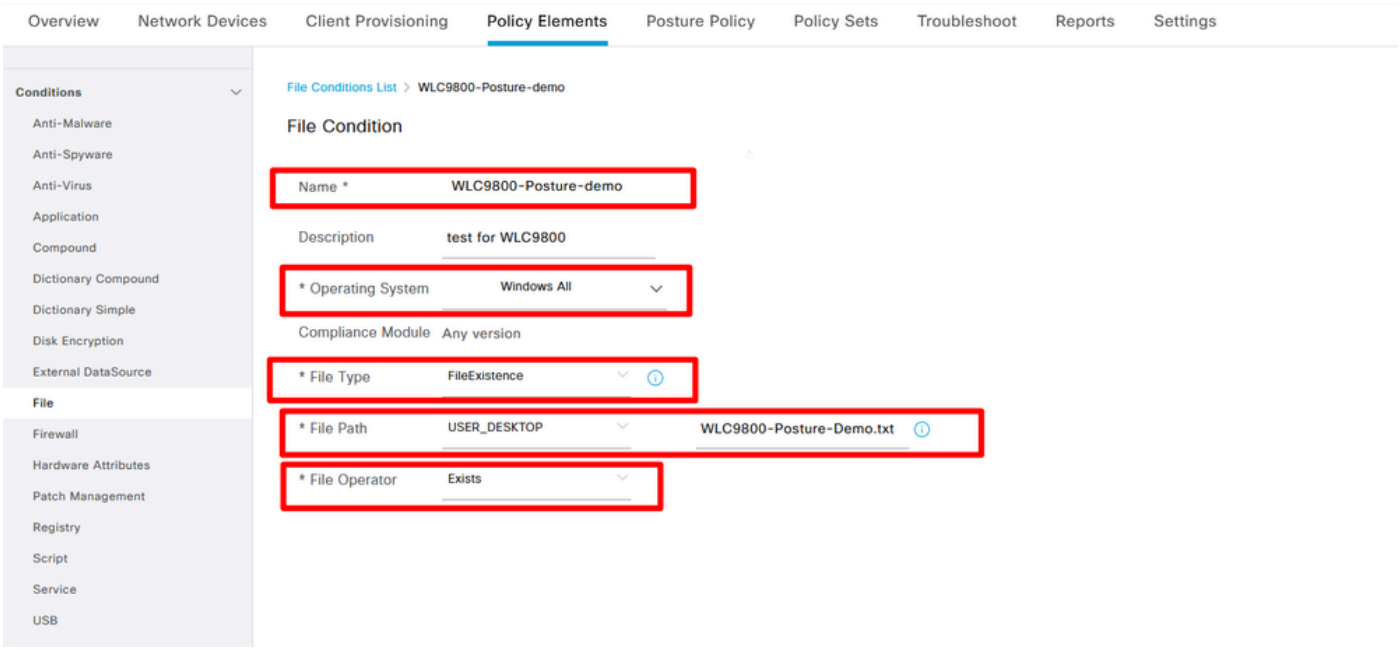
Etapa 7. Criar Política de Provisionamento do Cliente. Navegue até Centros de trabalho> Postura> Provisionamento de cliente> Política de provisionamento de cliente > Editar> inserir nova política acima.



Criar Política de Provisionamento de Cliente

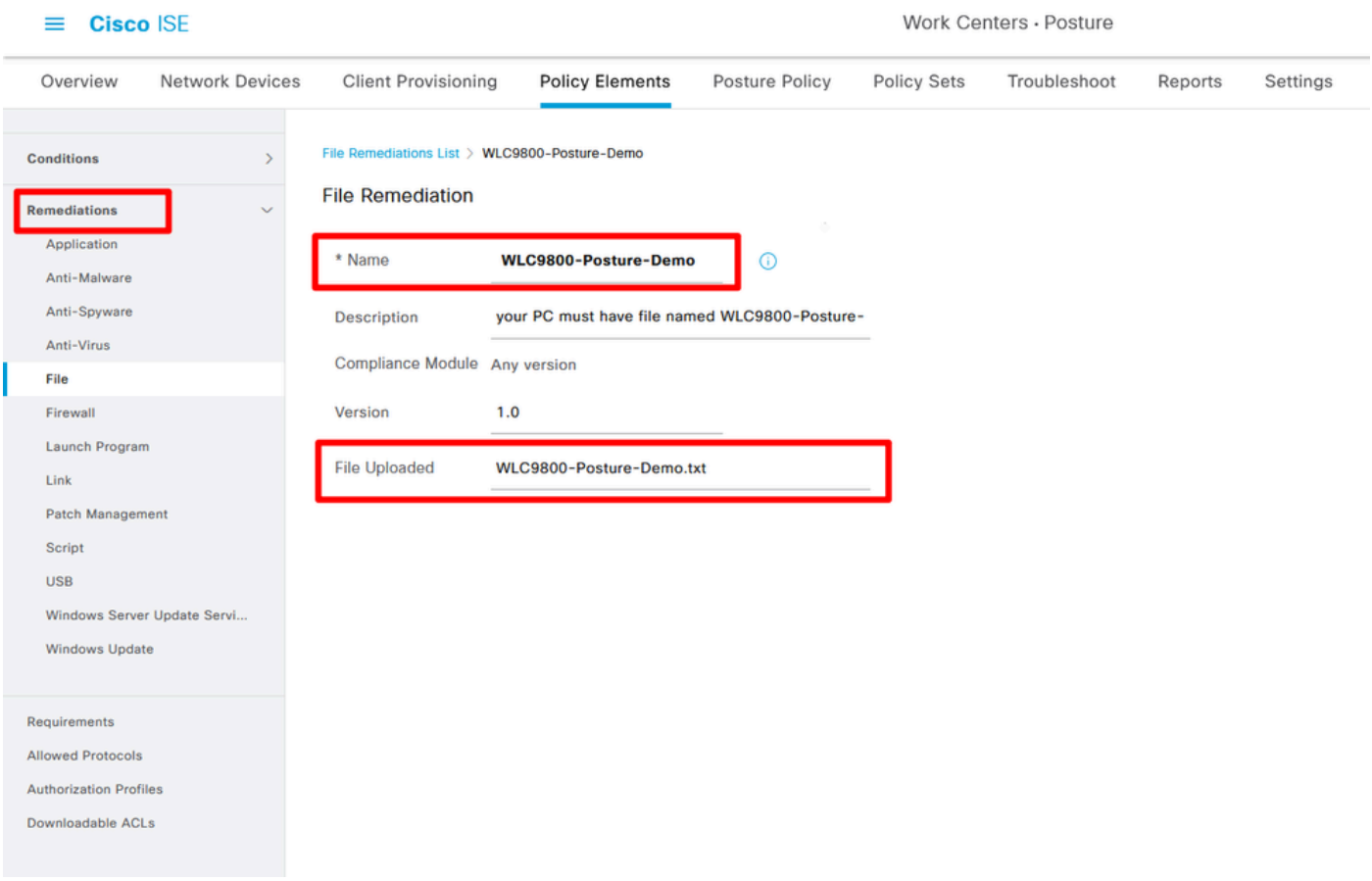
Etapa 8. Criar Condições de Arquivo. Navegue até Centros de trabalho> Postura> Elementos de

política> Condições> Arquivo> Condições do arquivo> Adicionar:



Criar condição de arquivo

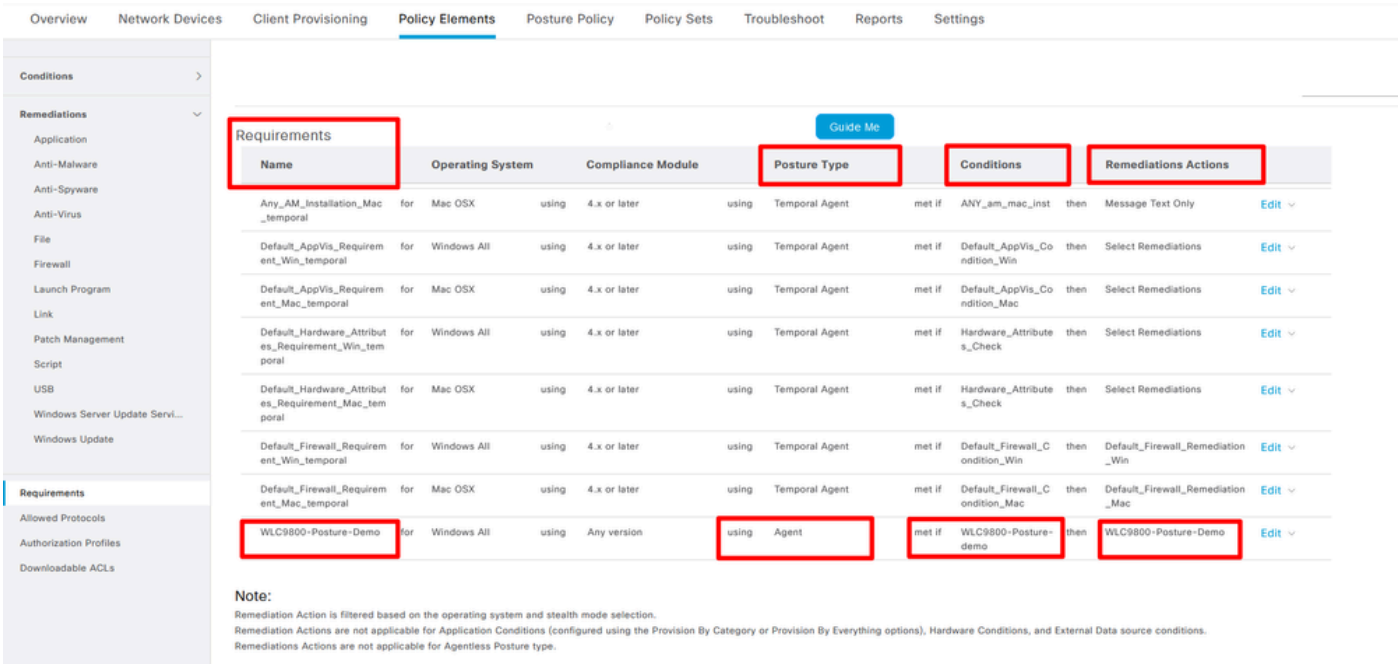
Etapa 9. Criar Remediações Navegue até Centros de Trabalho> Postura> Elementos de Política> Remediações > Arquivo> Adicionar:



Criar correção de arquivo

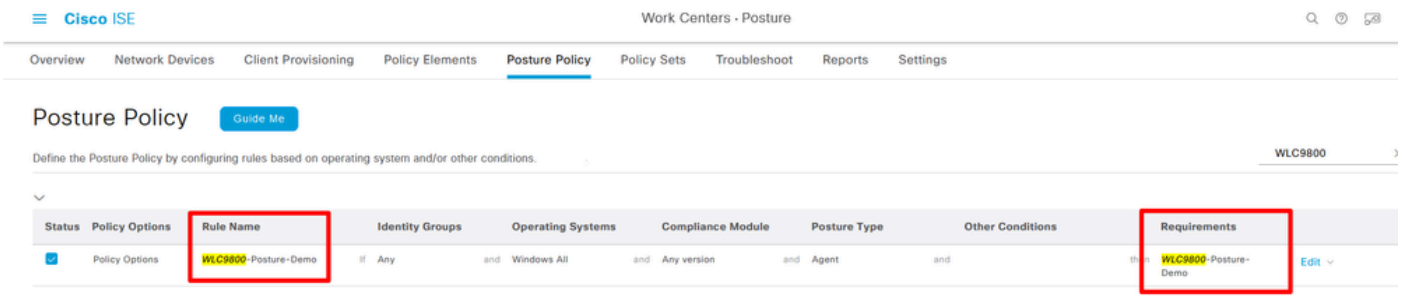
Etapa 10. Criar Requisito. Navegue até Centros de trabalho> Postura> Elementos de política>

Requisitos> Inserir novo requisito:



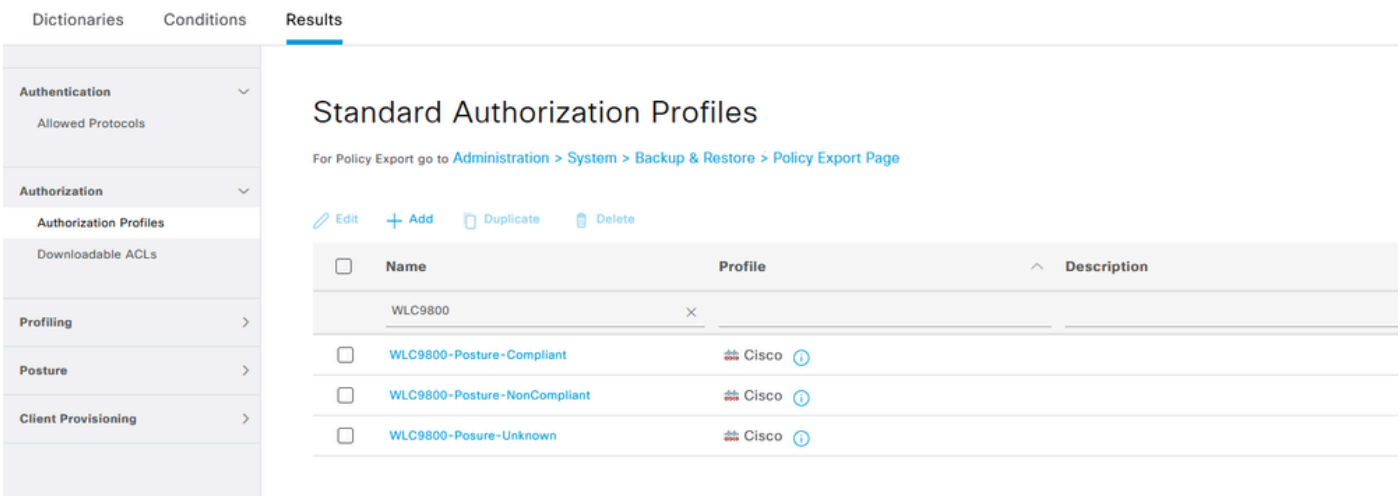
Criar Requisito de Situação

Etapa 11. Criar Política de Postura. Navegue até Centros de trabalho> Postura> Inserir nova política:

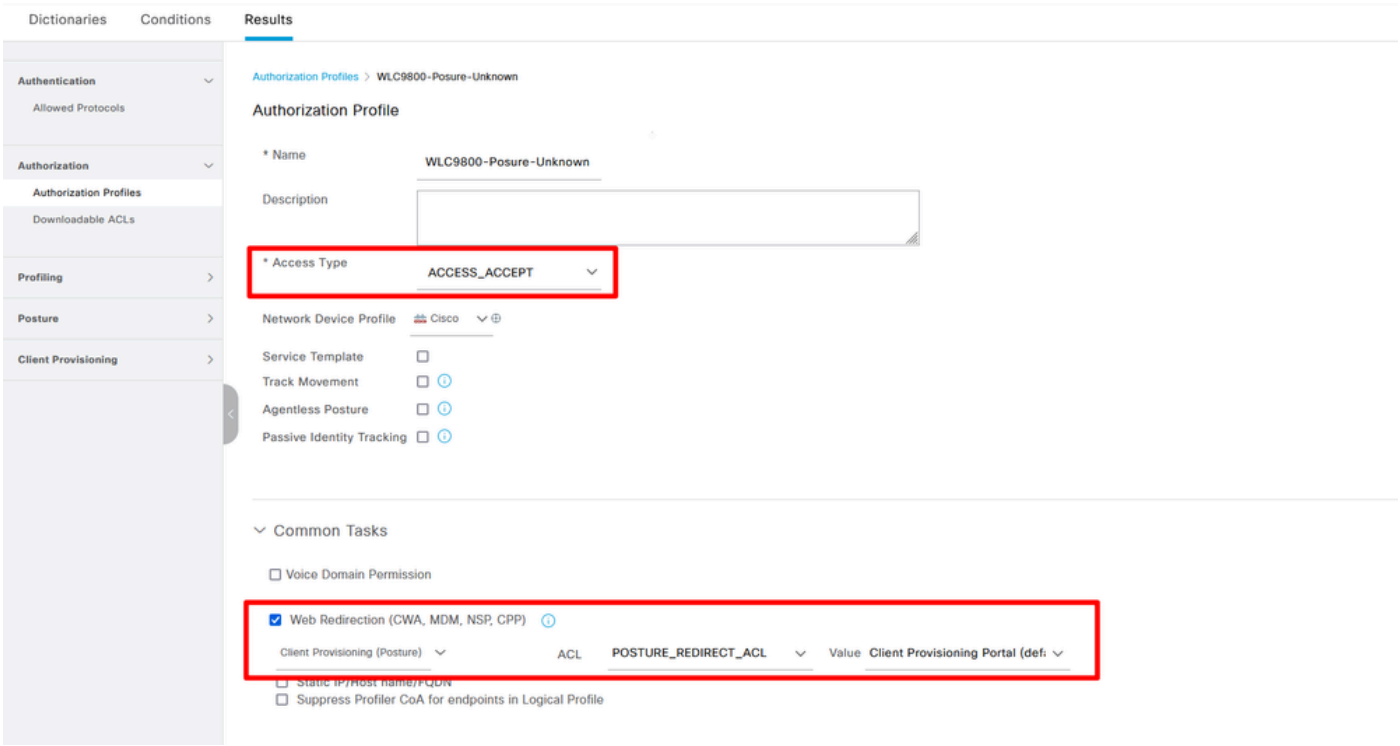


Criar política de postura

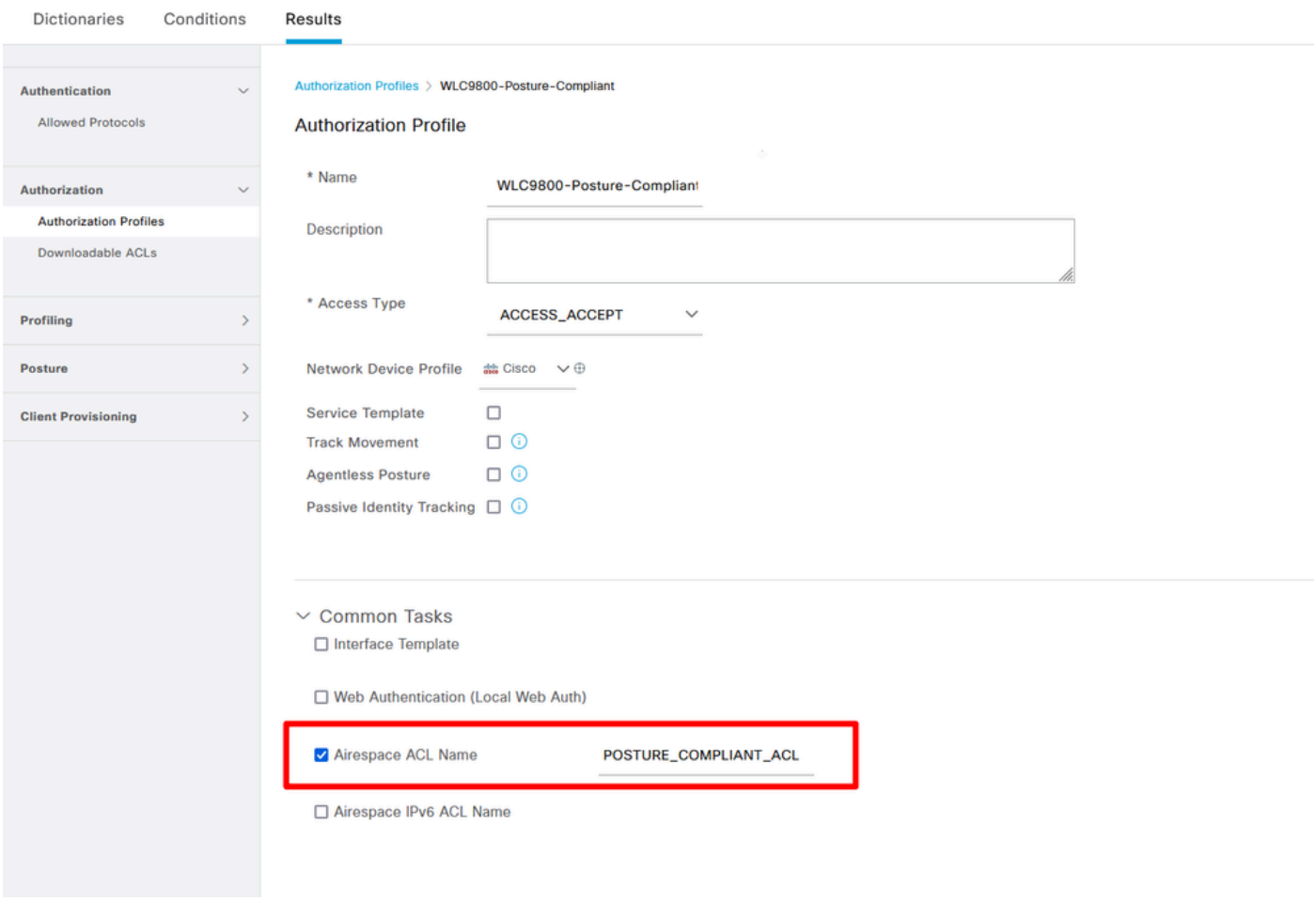
Etapa 12. Criar três Perfis de Autorização: O estado da postura é Desconhecido; O estado da postura não é conforme; O status da postura é compatível. Navegue até Política> Elementos de política> Resultados> Autorização> Perfis de autorização> Adicionar:



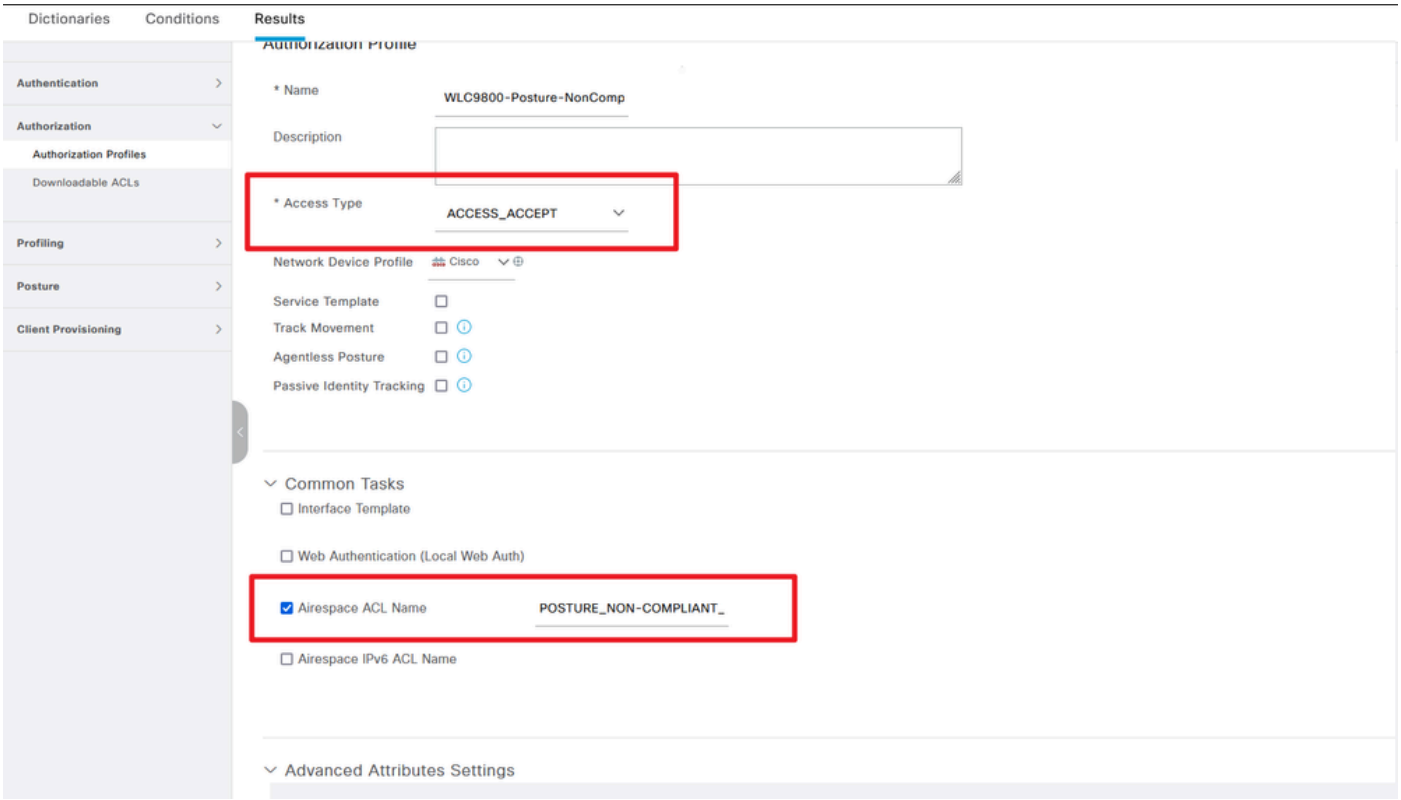
Criar perfis de autorização 01



Criar perfis de autorização 02



Criar perfis de autorização 03

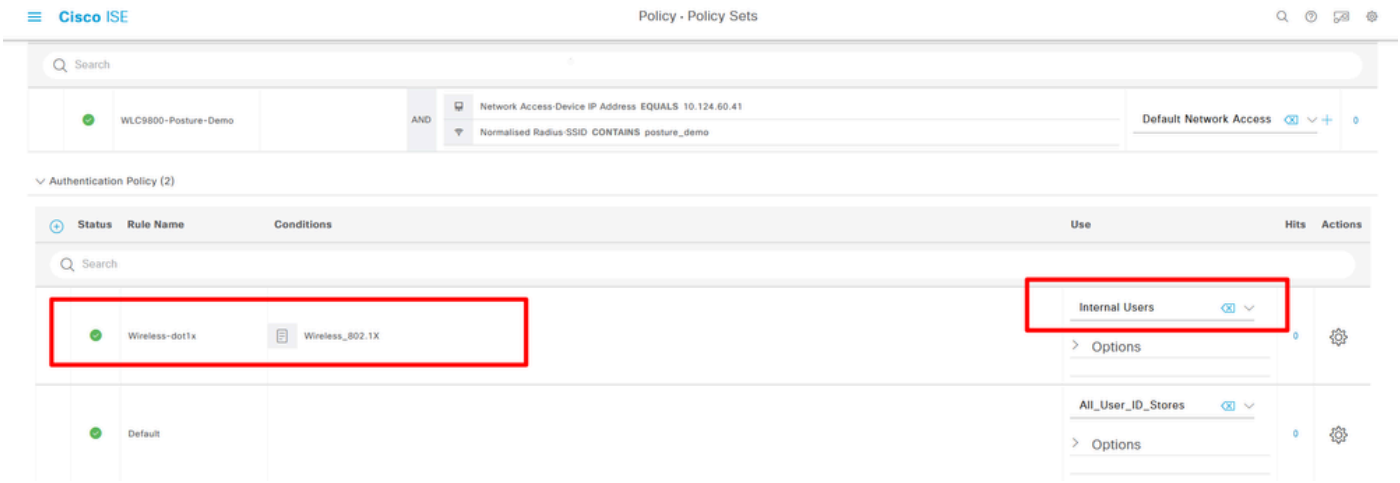


Etapa 13. Criar Conjuntos de Políticas. Navegue até Política> Política

Criar Conjuntos de Políticas

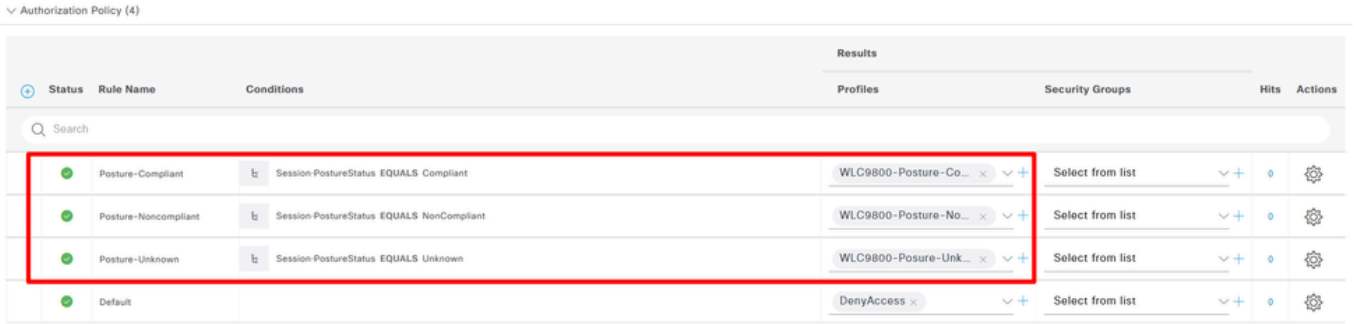
Sets> Adicionar ícone:

Etapa 14. Criar política de autenticação Navegue até Política> Conjuntos de políticas> Expanda "WLC9800-Posture-Demo"> Política de autenticação> Adicionar:



Criar Política de Autenticação

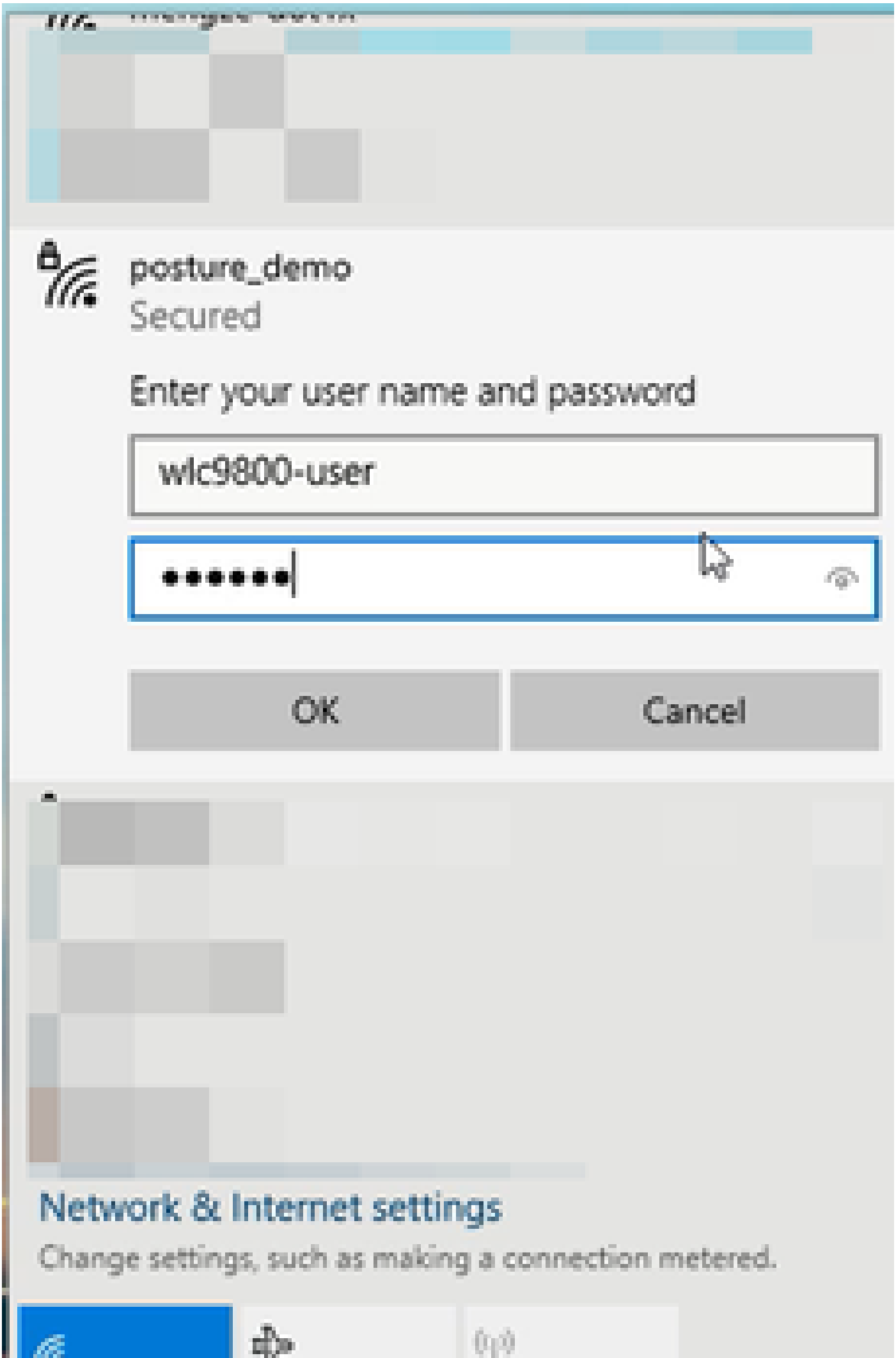
Etapa 15. Criar política de autorização Navegue até Política> Conjuntos de políticas> Expanda "WLC9800-Posture-Demo"> Política de autorização> Adicionar:



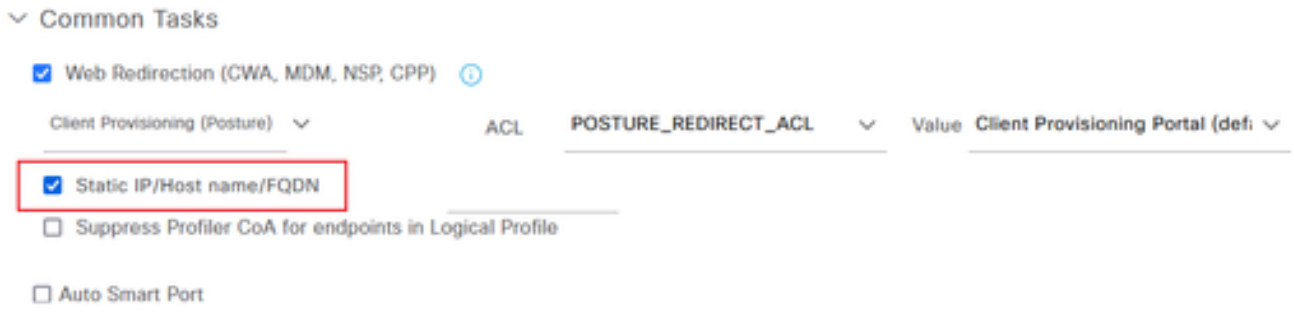
Criar Política de Autorização

Examples

1. Teste conectado SSID posture_demo com credenciais 802.1X corretas.


posture_demo
Secured
Enter your user name and password
wlc9800-user
OK
Cancel
Network & Internet settings
Change settings, such as making a connection metered.

- Se o navegador tiver sido redirecionado para a URL do portal do ISE, mas a página não puder ser carregada, verifique se o nome de domínio do ISE não foi adicionado ao servidor DNS e, portanto, o cliente não pode resolver a URL do portal. Para resolver rapidamente esse problema, verifique o IP estático/nome do host/FQDN no perfil de autorização para fornecer o endereço IP na URL de redirecionamento. No entanto, isso pode ser um problema de segurança, pois expõe o endereço IP do ISE.



Coletar depurações

Ative as depurações no C9800

Habilitar depurações no ISE

Referências

- Configurar o CWA no Catalyst 9800 WLC e ISE - Cisco
- BYOD sem fio com Identity Services Engine
- Implante a postura do ISE
- Solucionar problemas de gerenciamento e postura de sessão do ISE
- Comparar o fluxo de redirecionamento de postura do ISE com o fluxo sem redirecionamento de postura do ISE

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.