Configurar a autenticação da Web central no acesso SD

Contents

Introdução

Este documento descreve um guia passo a passo para configurar a Central Web Authentication (CWA) e descreve os procedimentos de verificação em todos os componentes.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Cisco Catalyst Center
- Cisco Identity Services Engine (ISE)
- Arquitetura do Catalyst 9800 Wireless Controller
- Autenticação, Autorização e Auditoria (AAA)

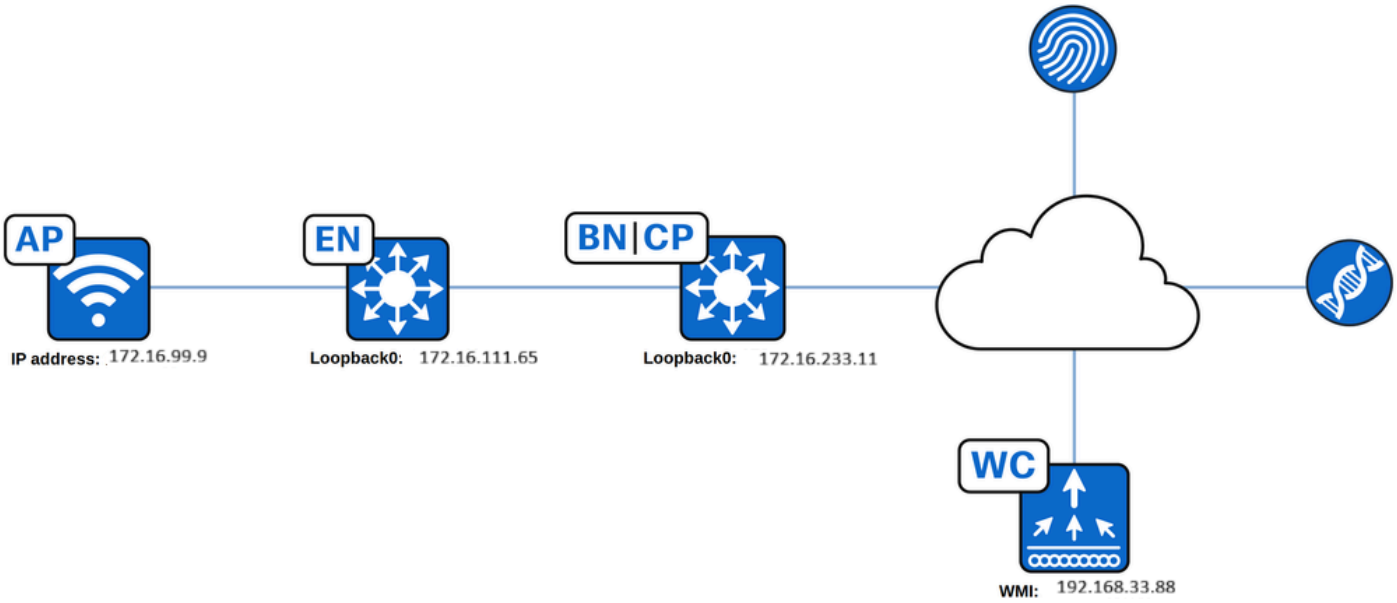
Componentes Utilizados

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

- Controladora de LAN sem fio (WLC) da Cisco - C9800-CL, Cisco IOS® XE 17.12.04
- Cisco Catalyst Center - Versão 2.3.7.7
- Cisco Identity Services Engine (ISE) - Versão 3.0.0.458
- Nó de borda SDA - C9300-48P, Cisco IOS® XE 17.12.05
- Nó de borda SDA/Plano de controle - C9500-48P, Cisco IOS® XE17.12.05
- Cisco Access Point - C9130AXI-A, versão 17.9.5.47

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.

Topologia



Overview

A Autenticação da Web Central (CWA) usa um SSID tipo convidado para redirecionar o navegador da Web do usuário para um portal cativo hospedado pelo Cisco ISE, usando uma ACL de redirecionamento configurada. O portal cativo permite que o usuário se registre e autentique e, após a autenticação bem-sucedida, a controladora Wireless LAN (WLC) aplica a autorização apropriada para conceder acesso total à rede. Este guia fornece instruções passo a passo para configurar o CWA usando o Cisco Catalyst Center.

Configurar o CWA no Cisco Catalyst Center

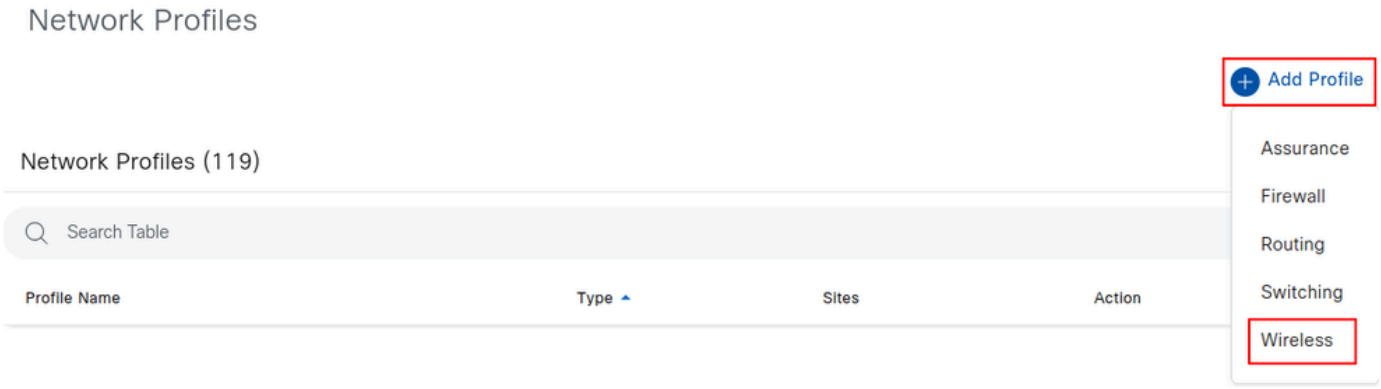
Criar o perfil de rede

Um perfil de rede permite definir as configurações que podem ser aplicadas a um local específico. Os perfis de rede podem ser criados para vários elementos no Cisco Catalyst Center, incluindo:

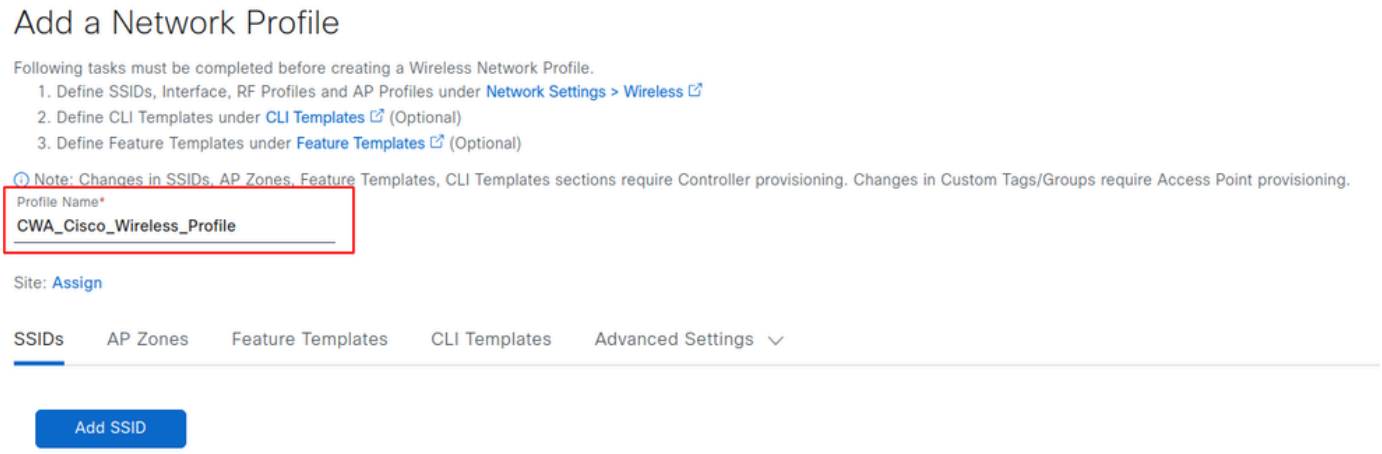
- Garantia
- Firewall
- Roteamento
- Comutação
- Dispositivo de telemetria
- Tecnologia Wireless

Para o CWA, um perfil sem fio deve ser configurado.

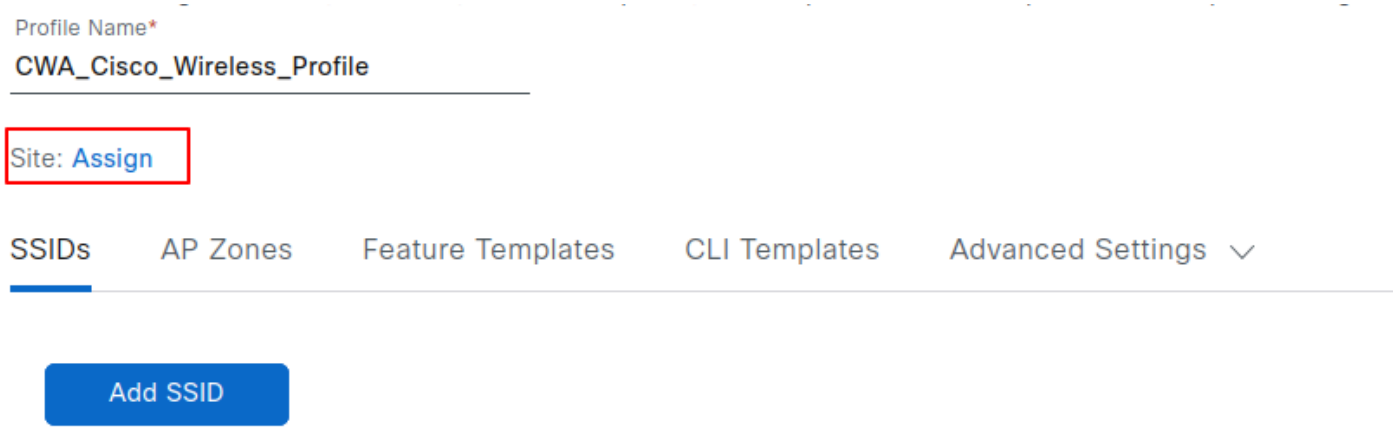
Para configurar um perfil sem fio, navegue para Design > Network Profiles, clique em Add Profile e selecione Wireless.



Nomeie o perfil conforme necessário. Neste exemplo, o perfil sem fio é chamado CWA_Cisco_Wireless_Profile. Você pode adicionar qualquer SSID existente a esse perfil selecionando Adicionar SSID. A criação de SSID é abordada na próxima seção.

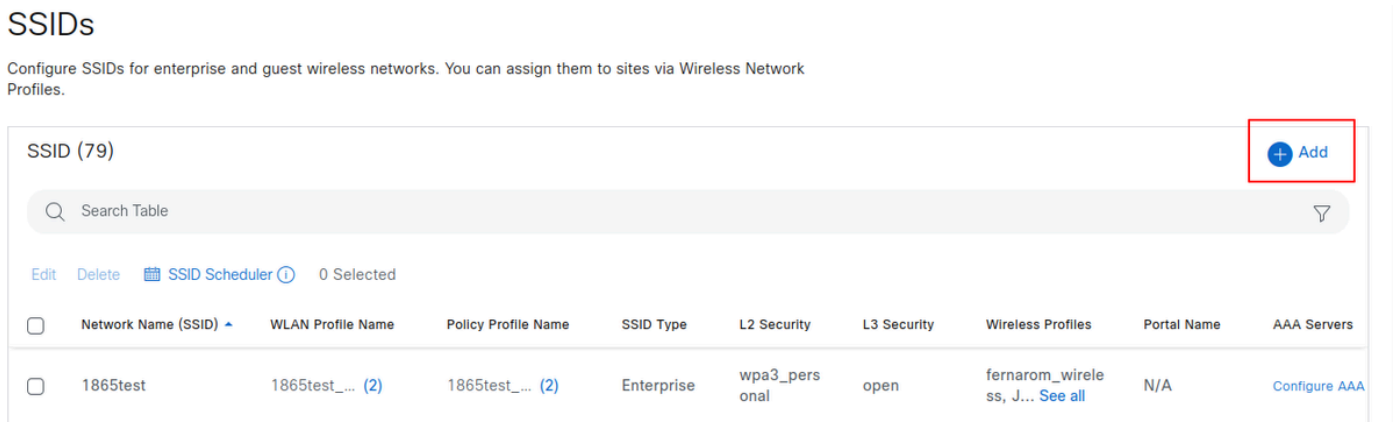


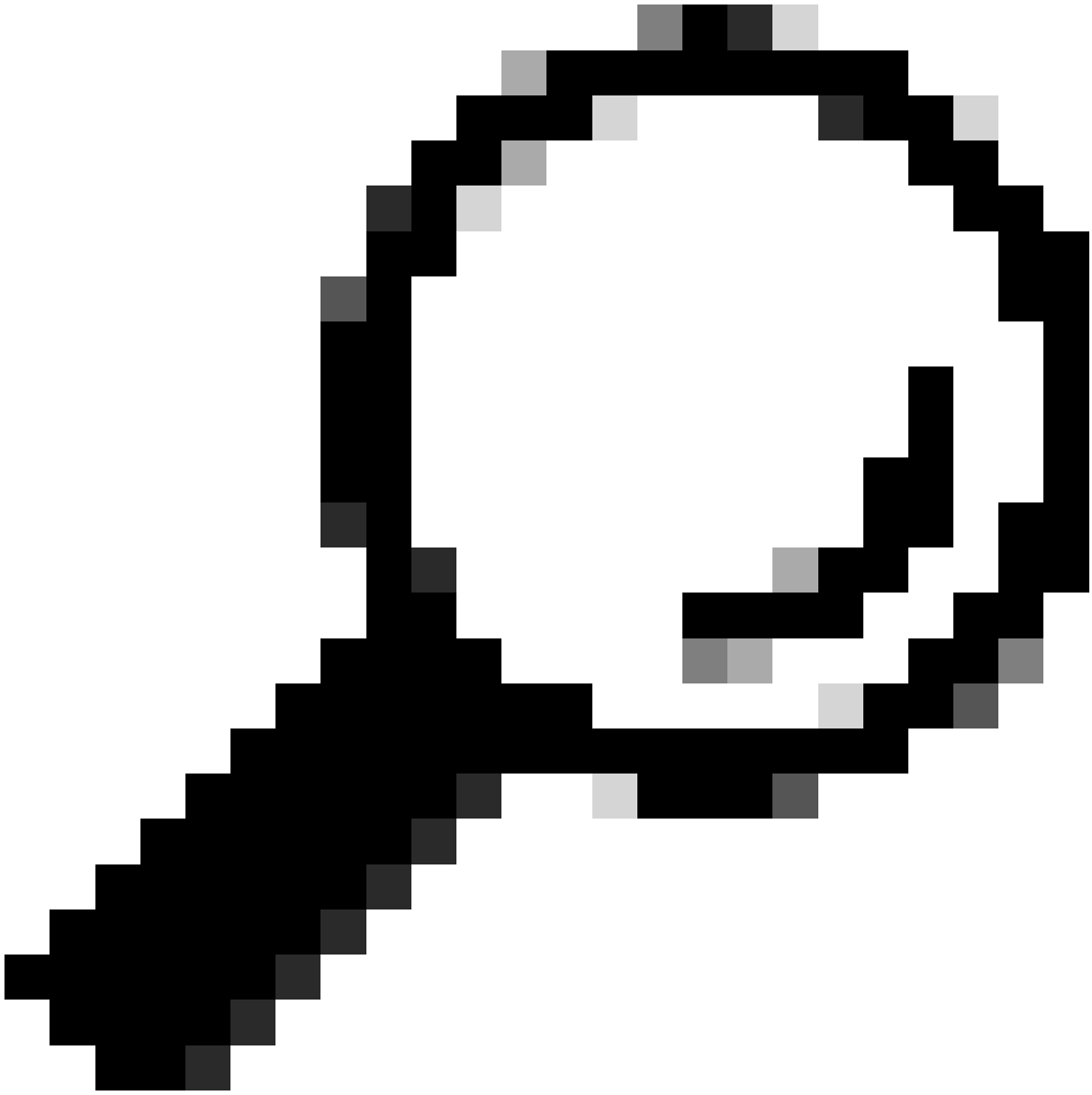
Selecione Atribuir para escolher o local onde esse perfil será aplicado e selecione o local desejado. Depois de selecionar os sites, clique em Salvar.



Criar o SSID

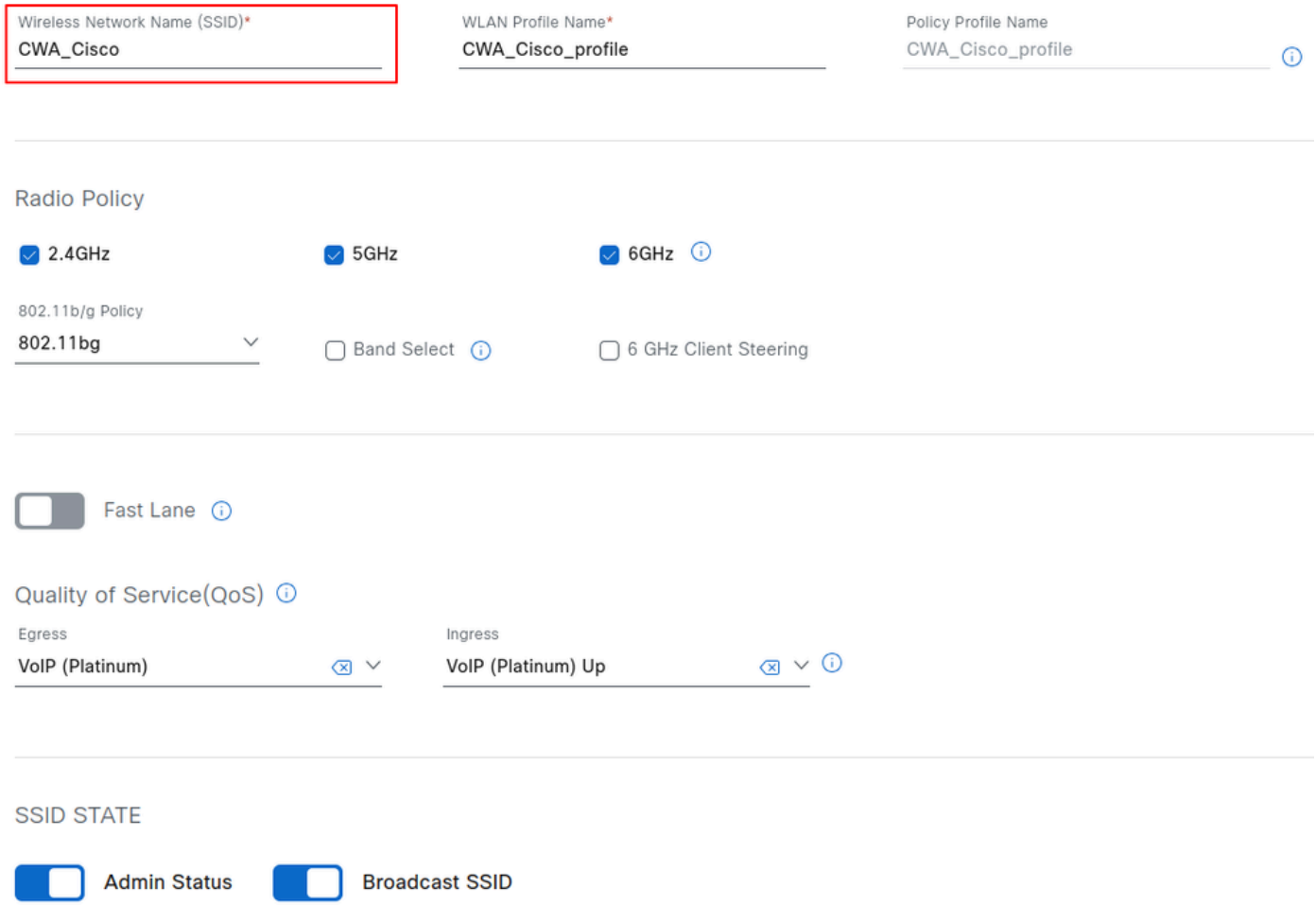
Navegue até Design > Network Settings > Wireless > SSIDs e clique em Add.



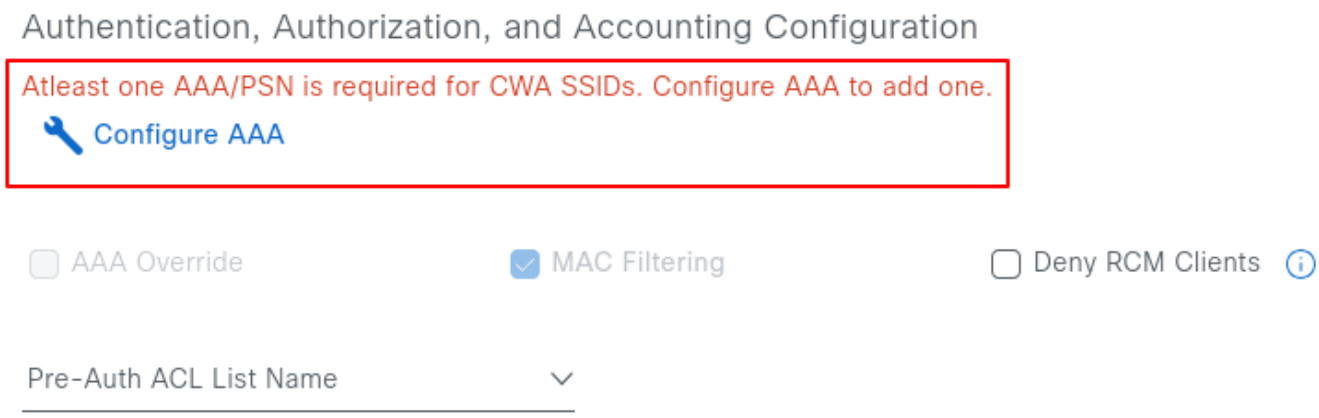


Tip: Ao criar um SSID para o CWA, é essencial selecionar o tipo de convidado. Essa seleção adiciona um comando ao perfil de política sem fio do SSID no WLC - o comando nac - que permite que o CoA seja usado para reautenticação depois que o usuário se registrar no portal cativo. Sem essa configuração, os usuários podem experimentar um loop infinito de registro e redirecionamento ao portal repetidamente.

Depois de selecionar Add, continue o fluxo de trabalho de configuração do SSID. Na primeira página, configure o nome do SSID, você também pode selecionar a faixa da política de rádio e definir o estado do SSID, incluindo as configurações de status administrativo e de broadcast . Para este guia de configuração, o SSID é chamado de CWA_Cisco.



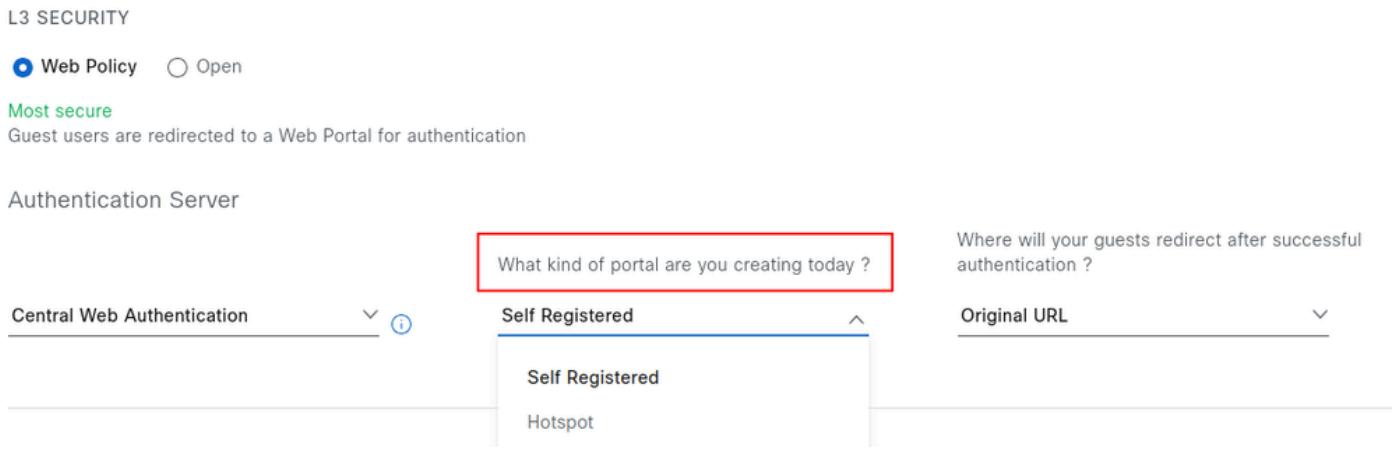
Após inserir o nome SSID, o nome do perfil da WLAN e o nome do perfil da política são gerados automaticamente. Selecione Avançar para continuar.
Pelo menos um AAA/PSN deve ser configurado para SSIDs do CWA. Se nenhum estiver configurado, selecione Configure AAA e escolha o endereço IP PSN na lista suspensa.



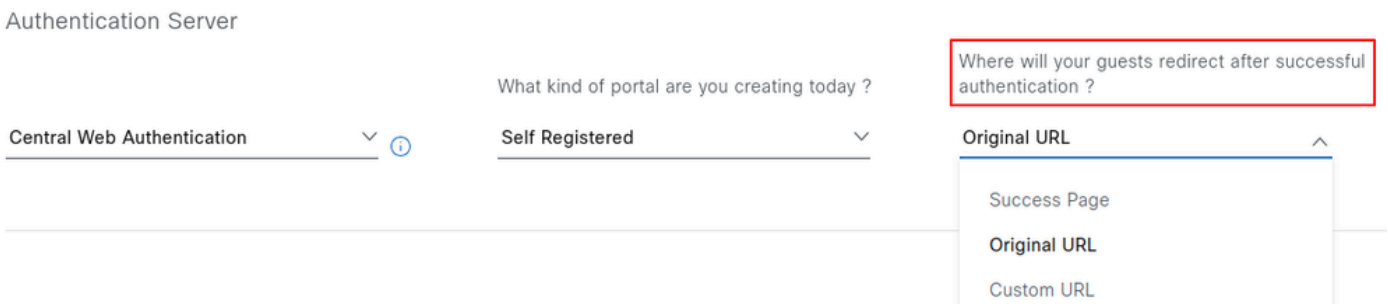
Depois de selecionar o servidor AAA, defina os parâmetros de segurança da Camada 3 e selecione o tipo de portal: Registrado automaticamente ou Hotspot.

Portais de convidados dos pontos de acesso: Um portal de hotspot para convidados fornece acesso à rede para convidados sem a necessidade de nomes de usuário e senhas. Aqui, os usuários devem aceitar uma Política de Uso Aceitável (AUP) para obter acesso à rede, levando a

um acesso subsequente à Internet. O acesso por meio de um portal de convidado credenciado requer que os convidados tenham um nome de usuário e uma senha.



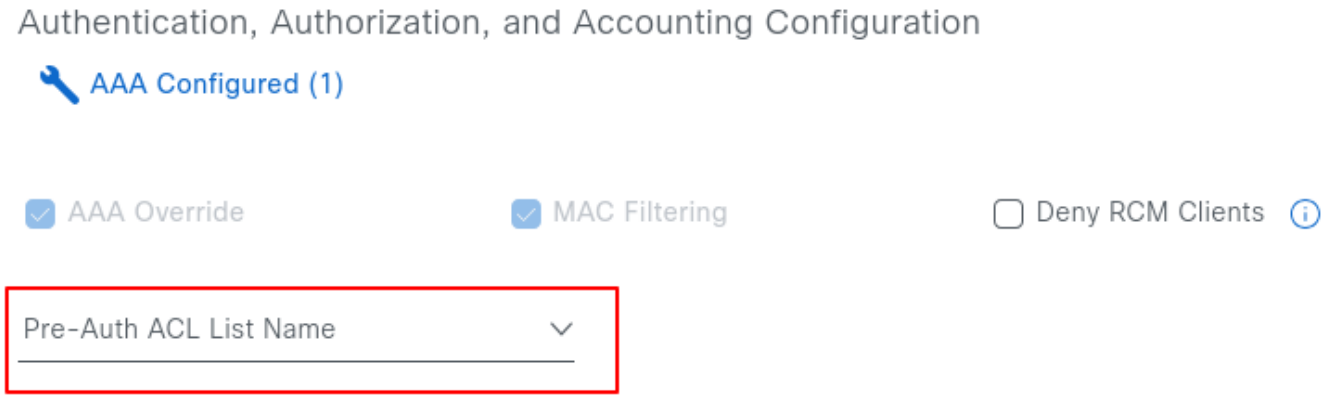
A ação que ocorre depois que o usuário se registra ou aceita a política de uso também pode ser configurada. Há três opções disponíveis: Página de sucesso, URL original e URL personalizada.



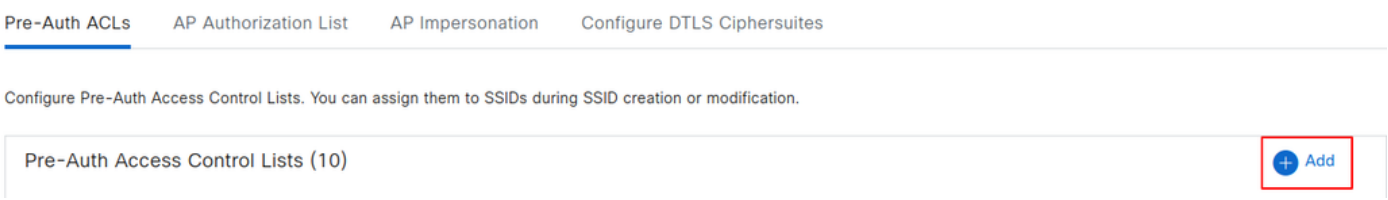
A seguir está uma descrição do comportamento de cada opção:

Página de sucesso: Redireciona o usuário para uma página de confirmação indicando que a autenticação teve êxito.
URL original: redireciona o usuário para o URL original que foi solicitado antes de ser interceptado pelo portal cativo.
URL personalizada: redireciona o usuário para um URL personalizado especificado. A seleção dessa opção habilita um campo adicional para definir a URL de destino

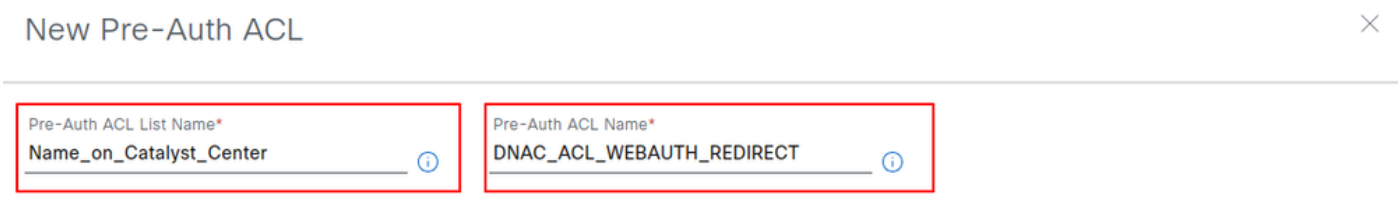
Na mesma página, em Authentication, Authorization, and Accounting Configuration, uma ACL de pré-autorização também pode ser configurada. Essa ACL permite a adição de entradas extras para protocolos além dos endereços IP DHCP, DNS ou PSN, que são obtidos das configurações de rede e anexados à ACL de redirecionamento durante o provisionamento. Esse recurso está disponível no Cisco Catalyst Center versão 2.3.3.x e posterior.



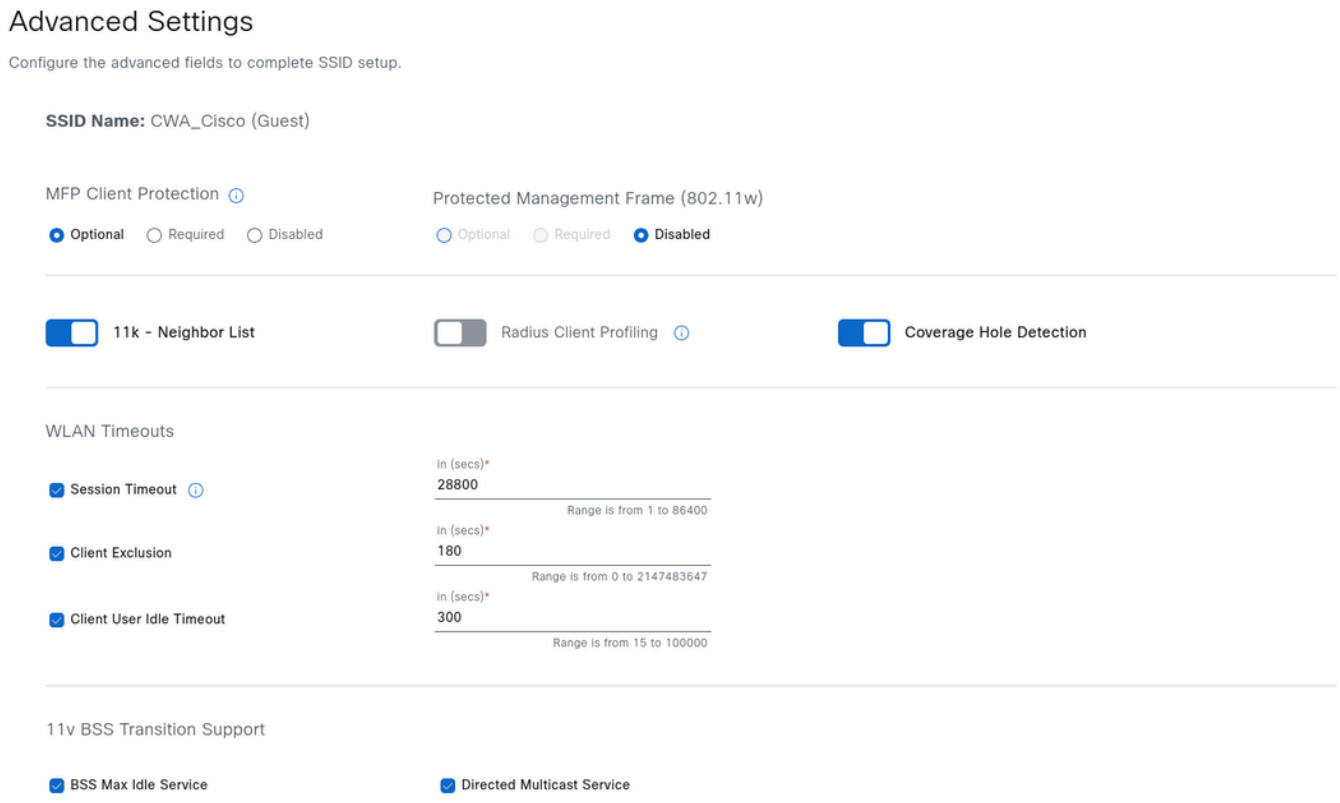
Para configurar uma ACL de pré-autenticação, navegue para Design > Network Settings > Wireless > Security Settings e clique em Add.



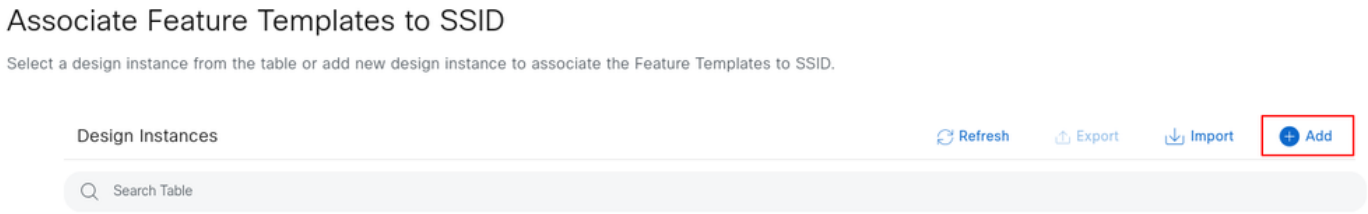
O primeiro nome identifica a ACL no Catalyst Center, enquanto o segundo nome corresponde ao nome da ACL no WLC. O segundo nome pode corresponder à ACL de redirecionamento existente configurada na WLC. Como referência, o Catalyst Center provisiona o nome Cisco DNA_ACL_WEBAUTH_REDIRECT para o WLC. As entradas da ACL de pré-autenticação são anexadas após as entradas existentes.



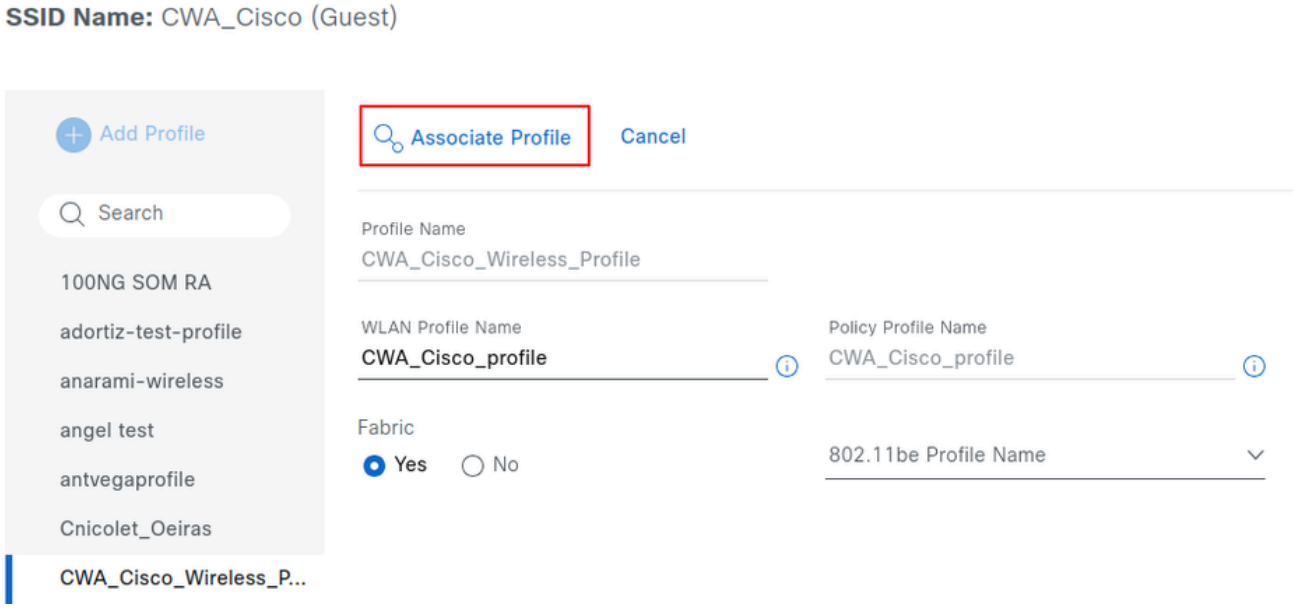
Retornando ao fluxo de trabalho de criação de SSID, selecione Avançar para exibir as configurações avançadas, incluindo transição rápida, tempo limite de sessão, tempo limite de usuário cliente e limitação de taxa. Ajuste os parâmetros conforme necessário e selecione Next para continuar. Para os fins deste guia de configuração, o exemplo mantém as configurações padrão.



Depois de selecionar Next, um prompt aparece para associar qualquer modelo de recurso ao SSID. Se aplicável, selecione os modelos desejados clicando em Adicionar e, quando terminar, clique em Avançar.

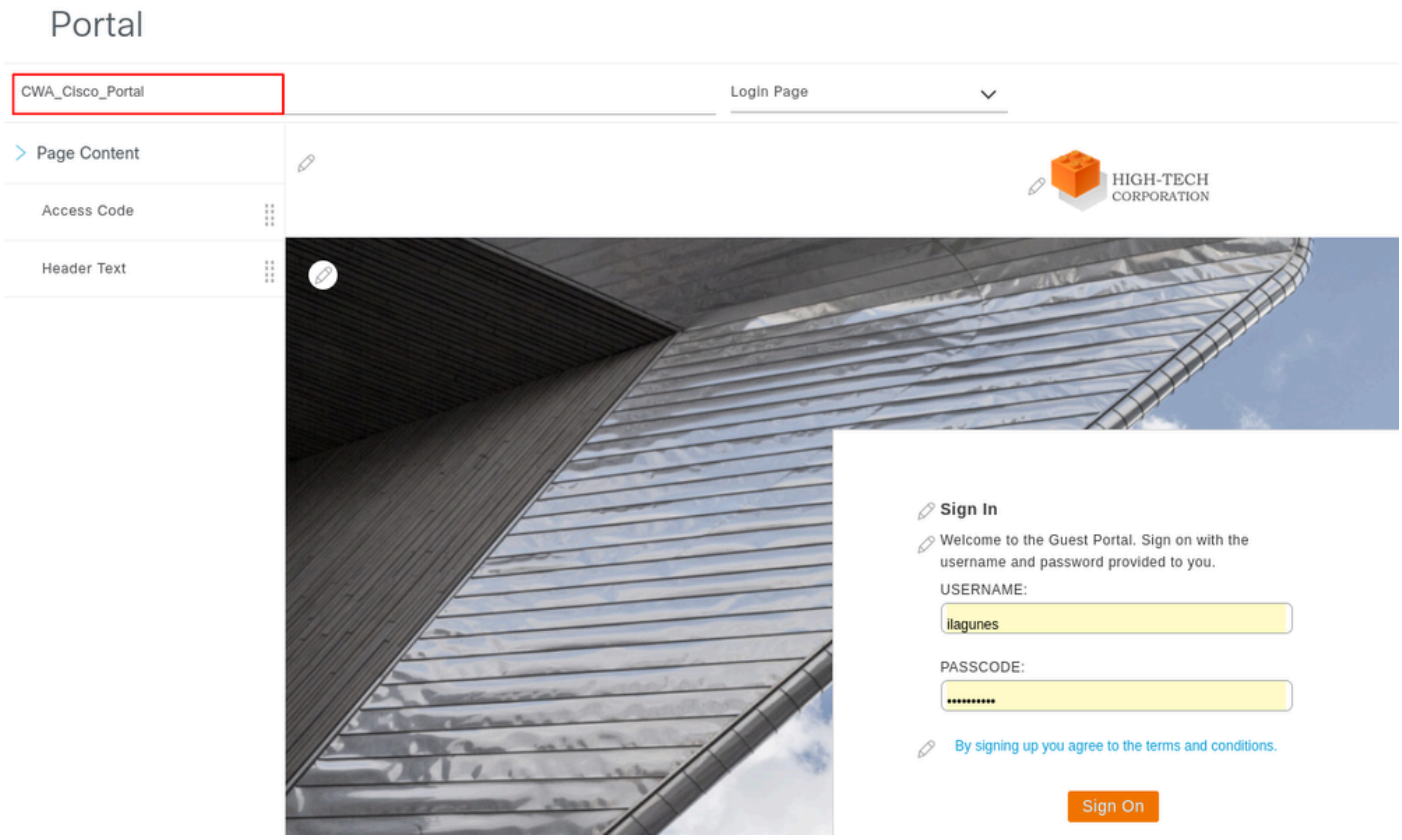


Associe o SSID ao perfil sem fio criado anteriormente. Para referência, consulte a seção Criar o perfil de rede sem fio. Nessa seção, você também pode selecionar se o SSID está habilitado para matriz ou não. Depois de concluir, clique em Associar perfil.

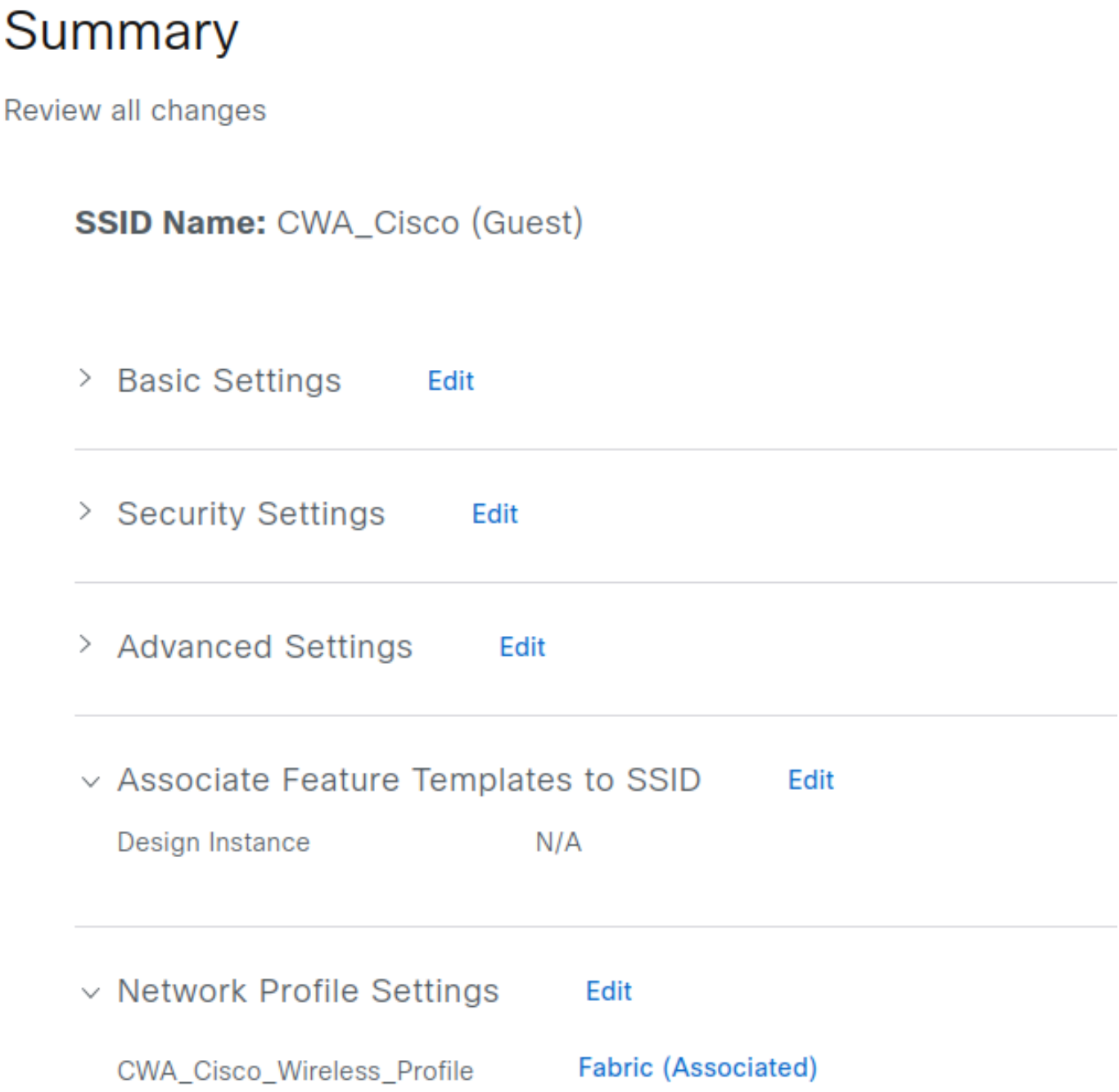


show wireless management trustpoint
Quando o perfil estiver associado ao SSID, clique em Avançar para criar e projetar o portal cativo. Para iniciar, clique em Criar portal.

O nome do portal define o nome de domínio no FQDN e o nome do conjunto de políticas no ISE. Clique em Save quando terminar. O portal permanece editável e pode ser excluído, se necessário.



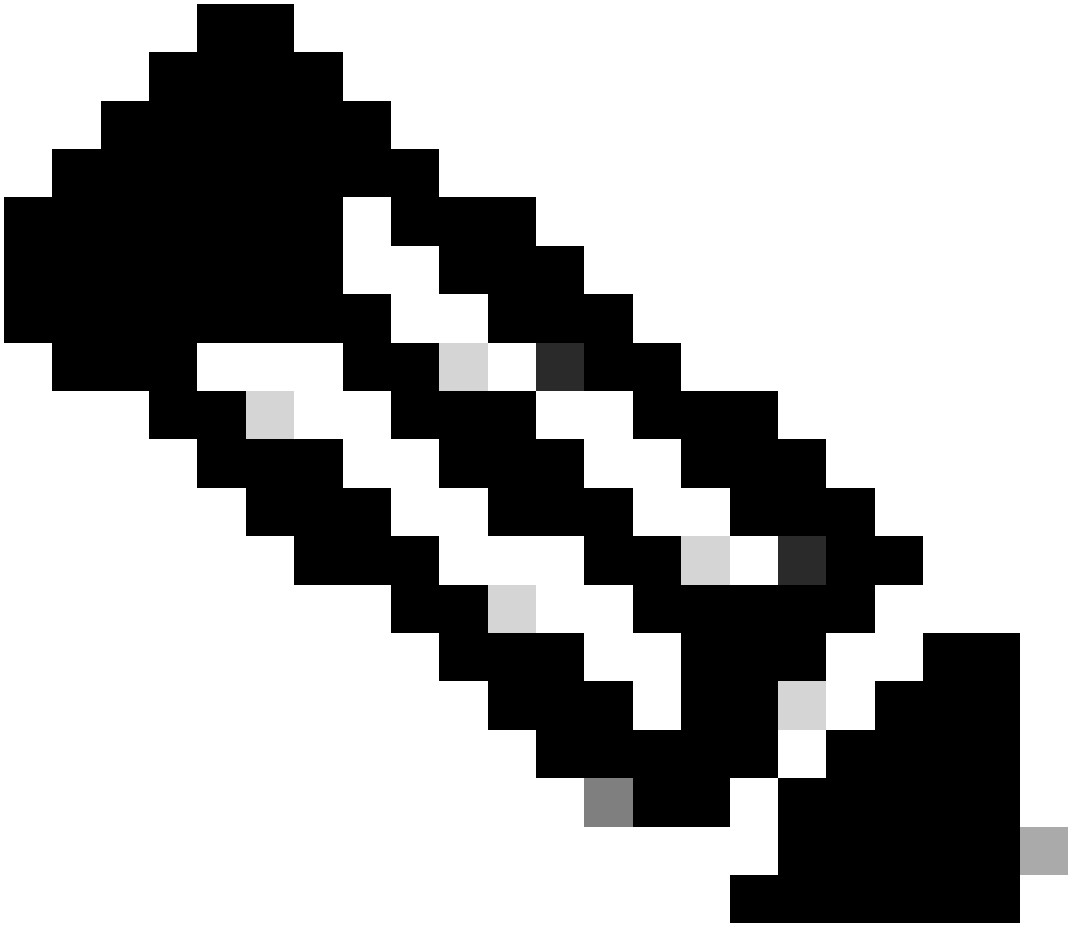
Selecione Próximo para exibir um resumo de todos os parâmetros de configuração definidos nas etapas anteriores.



Confirme os detalhes da configuração e selecione Save para aplicar as alterações.

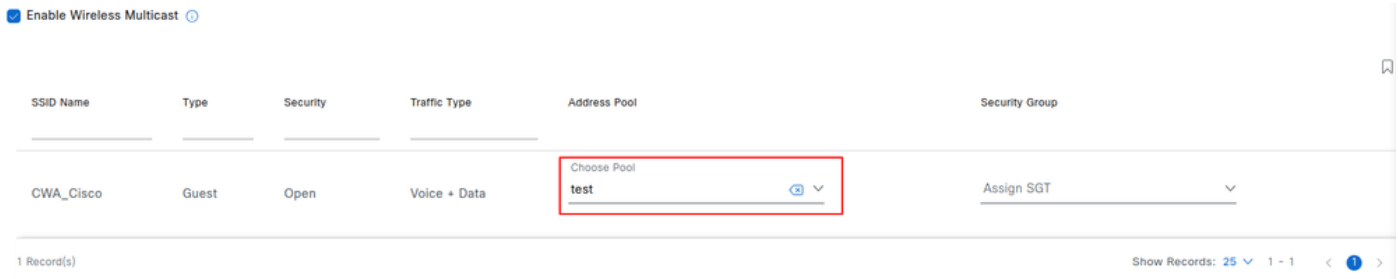
Provisionamento de estrutura

Após associar o perfil de rede sem fio ao site de estrutura, o SSID é exibido em Provisionar > Sites de estrutura > (Seu site) > SSIDs sem fio.

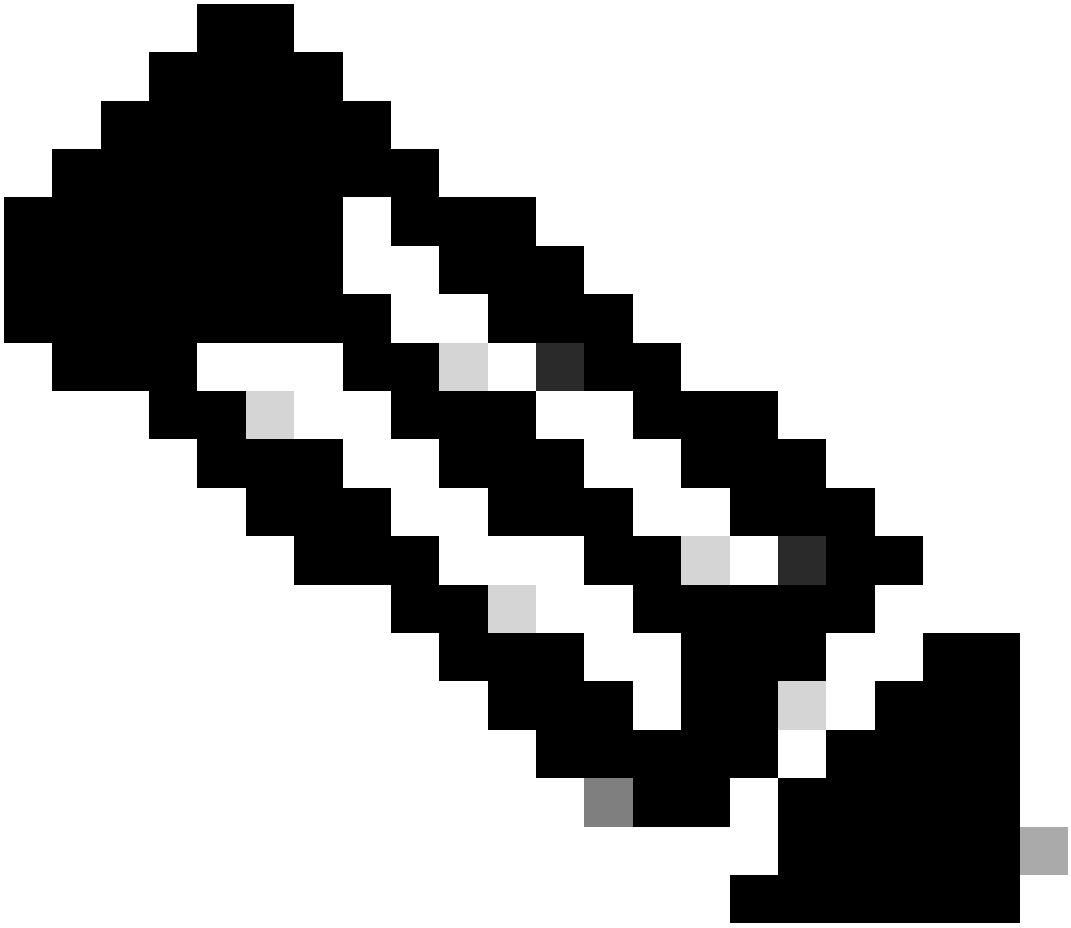


Note: Você precisa provisionar o Controlador de LAN sem fio para o site para que os SSIDs sejam exibidos em SSIDs sem fio

Escolha o pool SSID, opcionalmente associe uma Tag de grupo de segurança e clique em Implantar. O SSID é transmitido por pontos de acesso somente se um pool for atribuído.



Nos controladores AireOS e Catalyst 9800, reprovisione o Controller de LAN Wireless após qualquer alteração de configuração de SSID em Configurações de Rede.



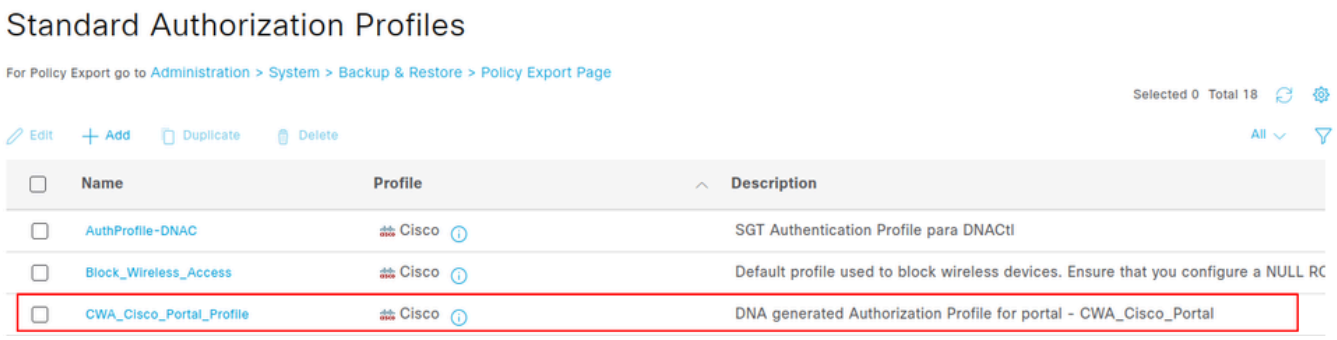
Note: Se nenhum pool for atribuído ao SSID, espera-se que os APs não o transmitam. O SSID é transmitido somente depois que um pool é atribuído. Depois que o pool é atribuído, o controlador não precisa ser provisionado novamente.

Reveja a configuração provisionada para Cisco ISE

Esta seção examina a configuração provisionada pelo Catalyst Center para o Cisco ISE.

Perfil de Autorização

Parte da configuração que o Catalyst Center provisiona no Cisco ISE é um perfil de autorização. Esse perfil define o resultado atribuído a um cliente com base em seus parâmetros e pode incluir configurações específicas, como atribuição de VLAN, ACLs ou redirecionamentos de URL.
Para exibir o perfil de autorização no ISE, navegue para Política > Elementos de política > Resultados. Se o nome do portal for CWA_Cisco_Portal, o nome do perfil será CWA_Cisco_Portal_Profile. O campo de descrição exibe o texto: Perfil de autorização gerado pelo DNA para o portal - CWA_Cisco_Portal.



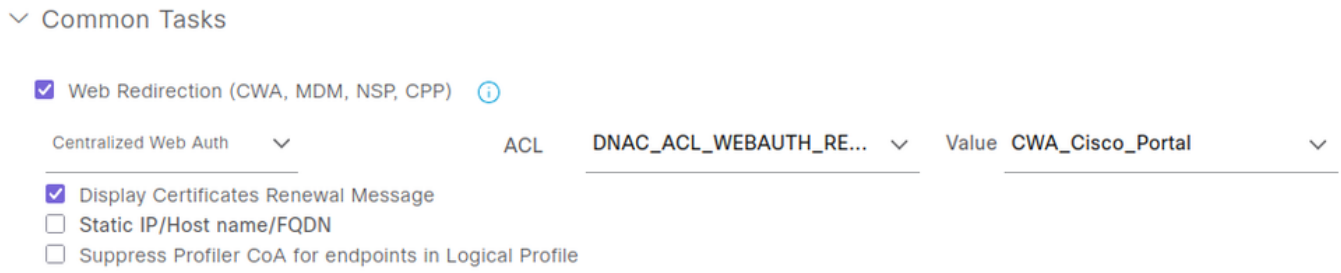
Para visualizar os atributos enviados à controladora Wireless LAN por este perfil de autorização, clique no nome do perfil de autorização e consulte a seção Tarefas comuns.
Este perfil de autorização fornece a ACL de redirecionamento e a URL de redirecionamento.

O atributo Redirecionamento da Web inclui dois parâmetros:

1. Nome da ACL: definido como Cisco DNA_ACL_WEBAUTH_REDIRECT.
2. Valor: refere-se ao nome do portal cativo, neste exemplo CWA_Cisco_Portal.

A opção Exibir Mensagem de Renovação de Certificados permite que o portal seja usado para renovar certificados que o endpoint está usando no momento.

Uma opção adicional, Static IP/Host Name/FQDN, está disponível em Display Certificates Renewal Message. Esse recurso permite a entrega do endereço IP do portal em vez do FQDN, que é útil quando o portal cativo falha ao carregar devido à incapacidade de acessar o servidor DNS.



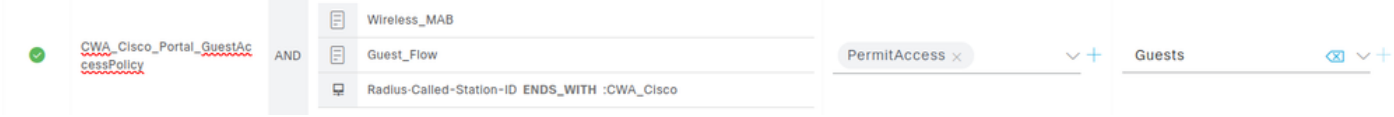
Conjuntos de políticas

Navegue até Policy > Policy Sets > Default > Authorization Policy para exibir os dois conjuntos de políticas criados para o portal chamado CWA_Cisco_Portal. Esses conjuntos de políticas são:

- CWA_Cisco_Portal_GuestAccessPolicy
- CWA_Cisco_Portal_RedirectPolicy

A política CWA_Cisco_Portal_GuestAccessPolicy é aplicada quando o cliente já concluiu o

processo de autenticação da Web, seja por meio do autorregistro ou do portal do hotspot.

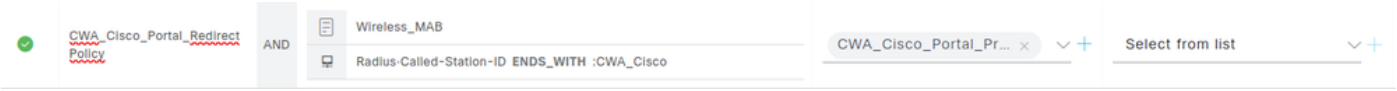


Esse conjunto de políticas atende a três critérios:

- Wireless_MAB: usado quando o Cisco ISE recebe uma solicitação de autenticação MAB (MAC Authentication Bypass, desvio de autenticação de MAC) de uma controladora Wireless LAN.
- Fluxo_Convidado: Refere-se à verificação do ISE do endereço MAC do ponto final em relação ao grupo de identidade GuestEndpoints. Se o endereço MAC do ponto final não estiver presente nesse grupo, a política não será aplicada.
- RADIUS Called-Station-ID ENDS_WITH :CWA_Cisco: O Called-Station-ID é um atributo RADIUS no ISE que armazena o endereço MAC da ponte ou do Ponto de Acesso no formato ASCII e anexa o SSID que está sendo acessado, separado por um ponto-e-vírgula (:). Neste exemplo, CWA_Cisco representa o nome SSID.

Nos perfis de coluna que você vê o nome PermitAccess, esse é um perfil de autorização reservado que não pode ser editado, que dá acesso total à rede e você também pode atribuir um SGT sob a coluna Grupos de segurança, que, nesse caso, é Convidados.

O perfil PermitAccess é usado. Este é um perfil de autorização reservado que não pode ser editado e concede acesso total à rede. Um SGT também pode ser atribuído na coluna Grupos de segurança; nesse caso, o SGT é definido como Convidados.
A próxima política a ser analisada é CWA_Cisco_Portal_RedirectPolicy.



Esse conjunto de políticas atende aos dois critérios a seguir:

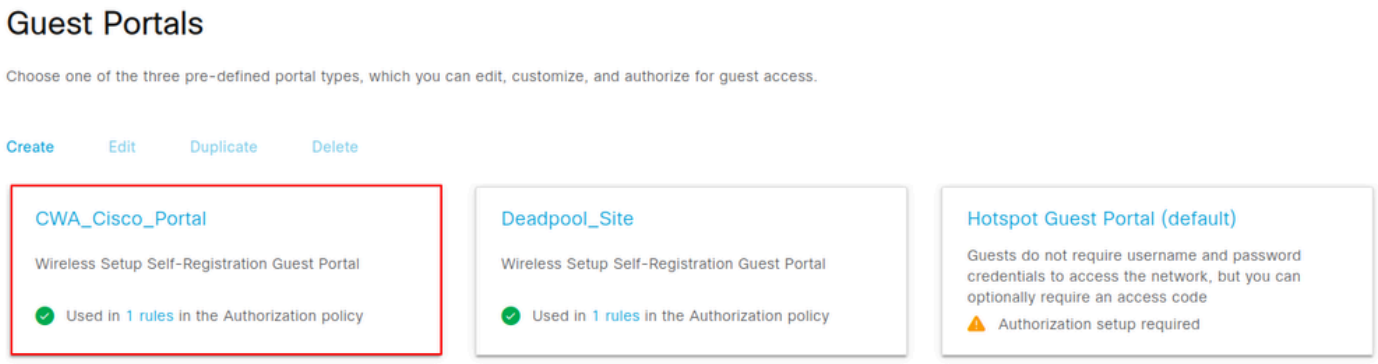
- Wireless_MAB: usado quando o Cisco ISE recebe uma solicitação de autenticação MAB de uma controladora Wireless LAN.
- RADIUS Called-Station-ID ENDS_WITH :CWA_Cisco: O Called-Station-ID é um atributo RADIUS no ISE que armazena o endereço MAC da ponte ou do Ponto de Acesso no formato ASCII e anexa o SSID que está sendo acessado, separado por um ponto-e-vírgula (:). Neste exemplo, :CWA_Cisco representa o nome SSID.

A ordem dessas políticas é fundamental. Se CWA_Cisco_Portal_RedirectPolicy for exibido primeiro na lista, ele corresponderá somente à autenticação MAB e ao nome SSID usando o atributo RADIUS Called-Station-ID ENDS_WITH :CWA_Training. Nessa configuração, mesmo que o endpoint já tenha sido autenticado pelo portal, ele continuará a corresponder a essa política indefinidamente. Como resultado, o acesso completo nunca é concedido através do perfil PermitAccess, e o cliente permanece preso em um loop contínuo de autenticação e redirecionamento para o portal.

Configuração do Portal do Convidado

Navegue até Centros de trabalho > Acesso de convidado > Portais e componentes para exibir o

portal.
O Portal do convidado criado aqui usa o mesmo nome do CWA_Cisco_Portal do Catalyst Center.
Selecione o nome do portal para se desejar exibir detalhes adicionais.

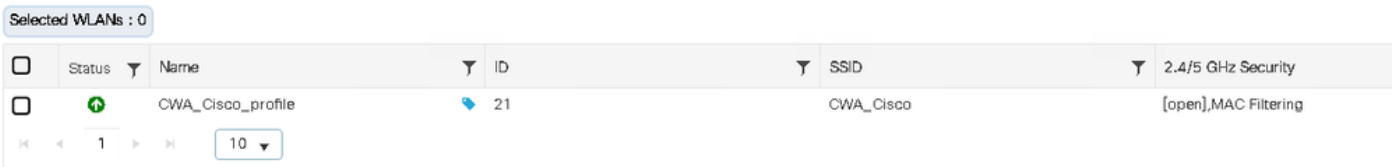


Reveja a configuração provisionada para a WLC

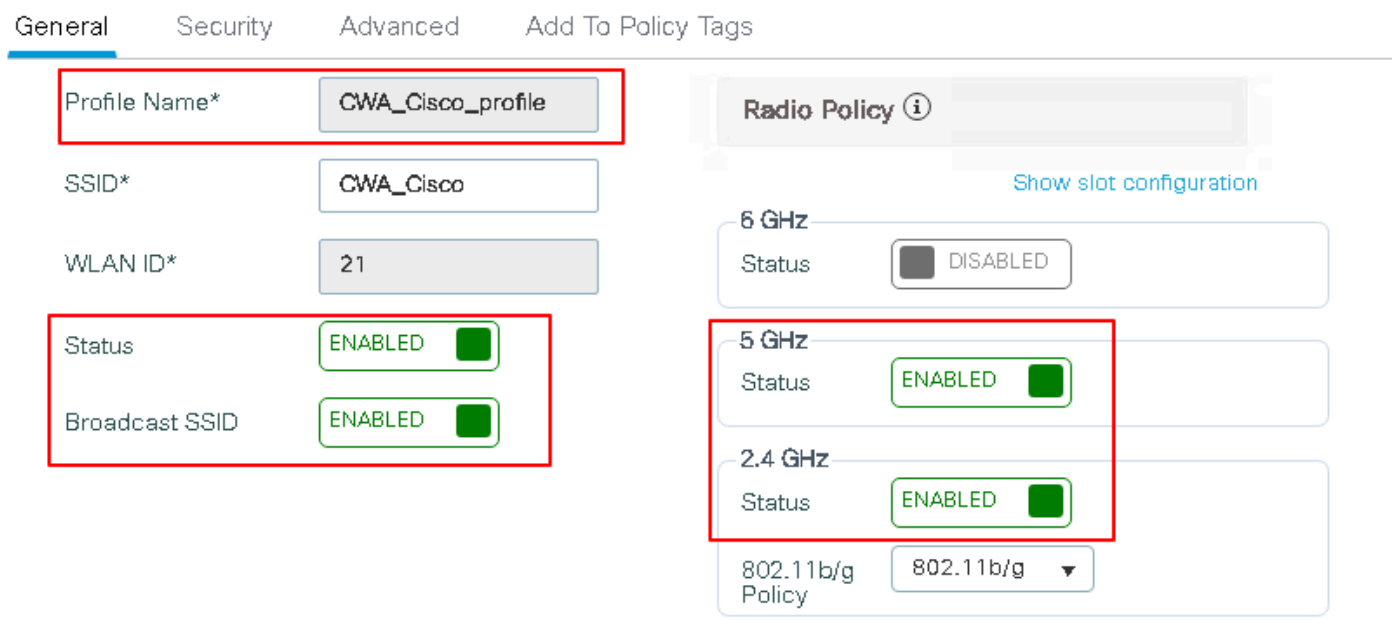
Esta seção examina a configuração provisionada pelo Catalyst Center para o Wireless LAN Controller.

Configuração de SSID

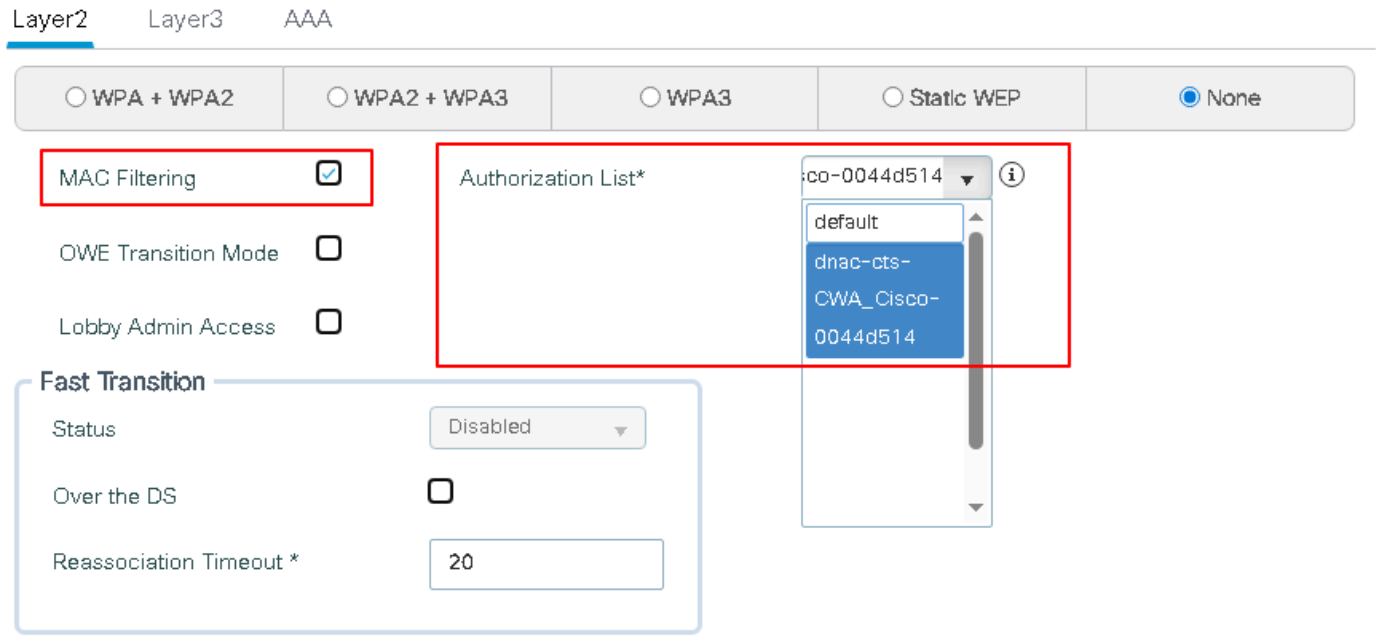
Na GUI da WLC, navegue para Configuration > Tags & Profiles > WLANs para exibir a configuração do SSID.



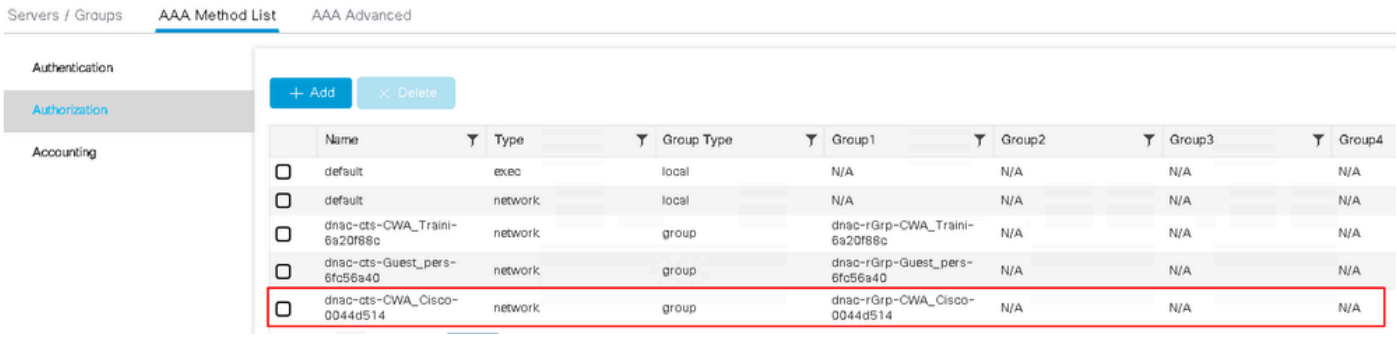
O SSID CWA_Cisco tem o nome CWA_Cisco_profile no WLC, com ID 21 e um tipo de segurança Open usando filtragem MAC. Clique duas vezes no SSID para visualizar sua configuração.



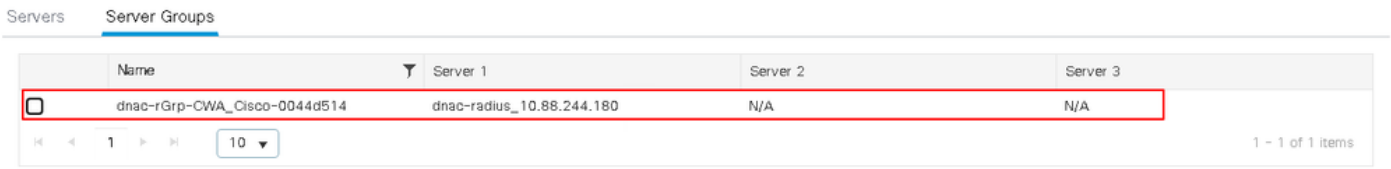
O SSID é UP e transmite em canais de 5 GHz e 2,4 GHz e está anexado ao perfil de política CWA_CIsco_Profile. Clique na guia Segurança para exibir as configurações.



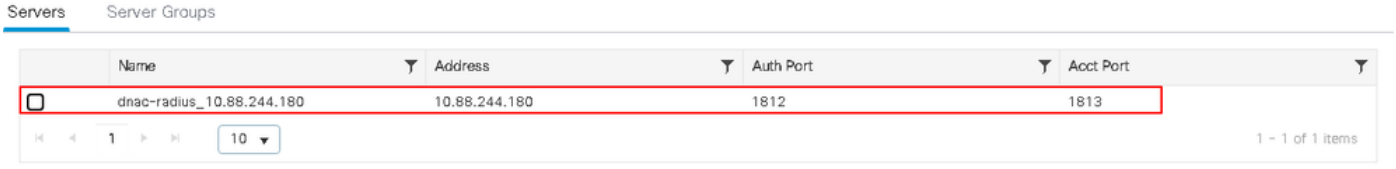
As principais configurações incluem o método de segurança de Camada 2 (Filtragem MAC) e a lista de autorização AAA (Cisco DNA-cts-CWA_Cisco-0044d514). Para revisar sua configuração, navegue para Configuration > Security > AAA > AAA Method List > Authorization.



A lista de métodos aponta para o grupo RADIUS Cisco DNA-Grp-CWA_Cisco-0044d514na coluna Group1. Para exibir sua configuração, navegue para Configuration > Security > AAA > Server/Groups > Server Groups.



O grupo de servidores Cisco DNA-Grp-CWA_Cisco-0044d514 aponta para Cisco DNA-radius_10.88.244.180 na coluna Servidor 1. Visualize sua configuração na guia Servers.



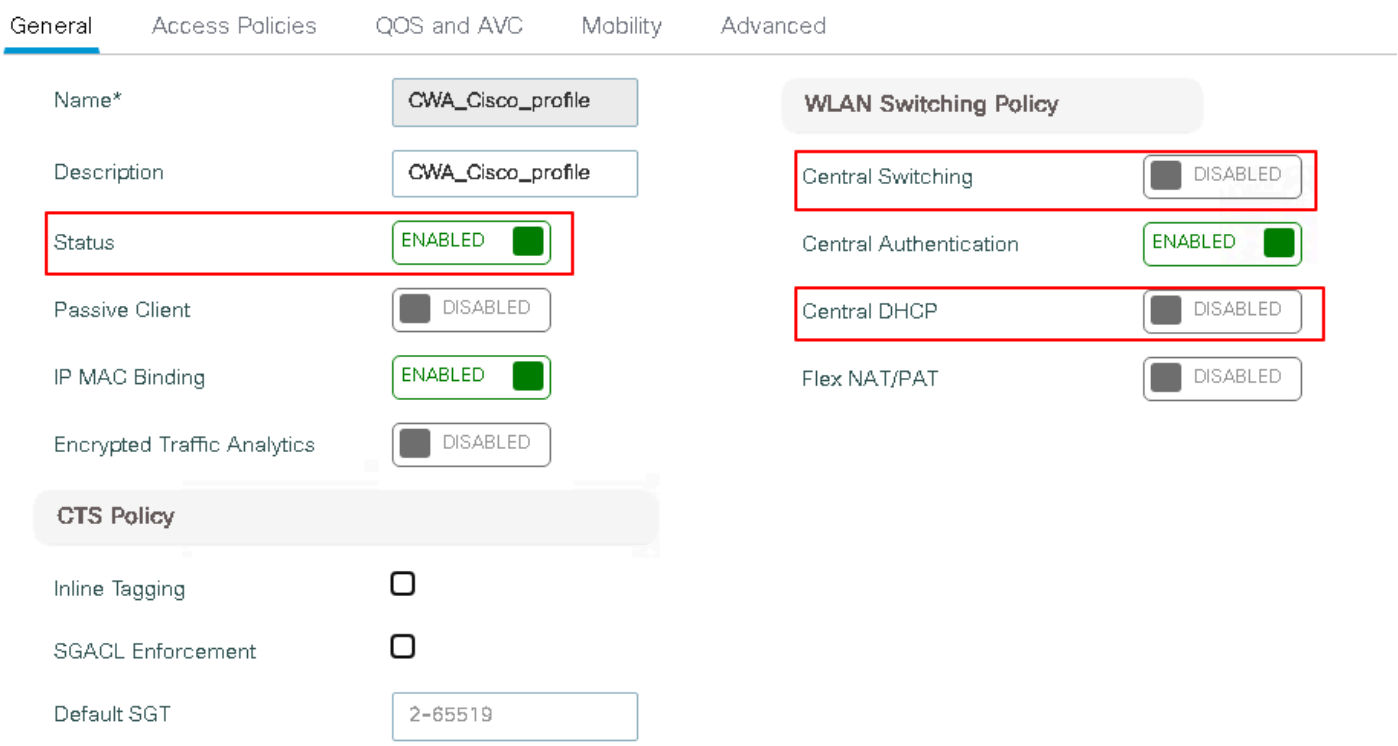
O servidor Cisco DNA-radius_10.88.244.180 tem o endereço IP 10.88.244.180. Clique em seu nome para exibir sua configuração

Uma configuração crítica é a mudança de autorização (CoA), que fornece um mecanismo para modificar os atributos de uma sessão de autenticação, autorização e contabilização (AAA) depois de ter sido autenticada no portal cativo. Sem esse recurso, o endpoint permanece em um estado web-auth pending mesmo após concluir o registro no portal.

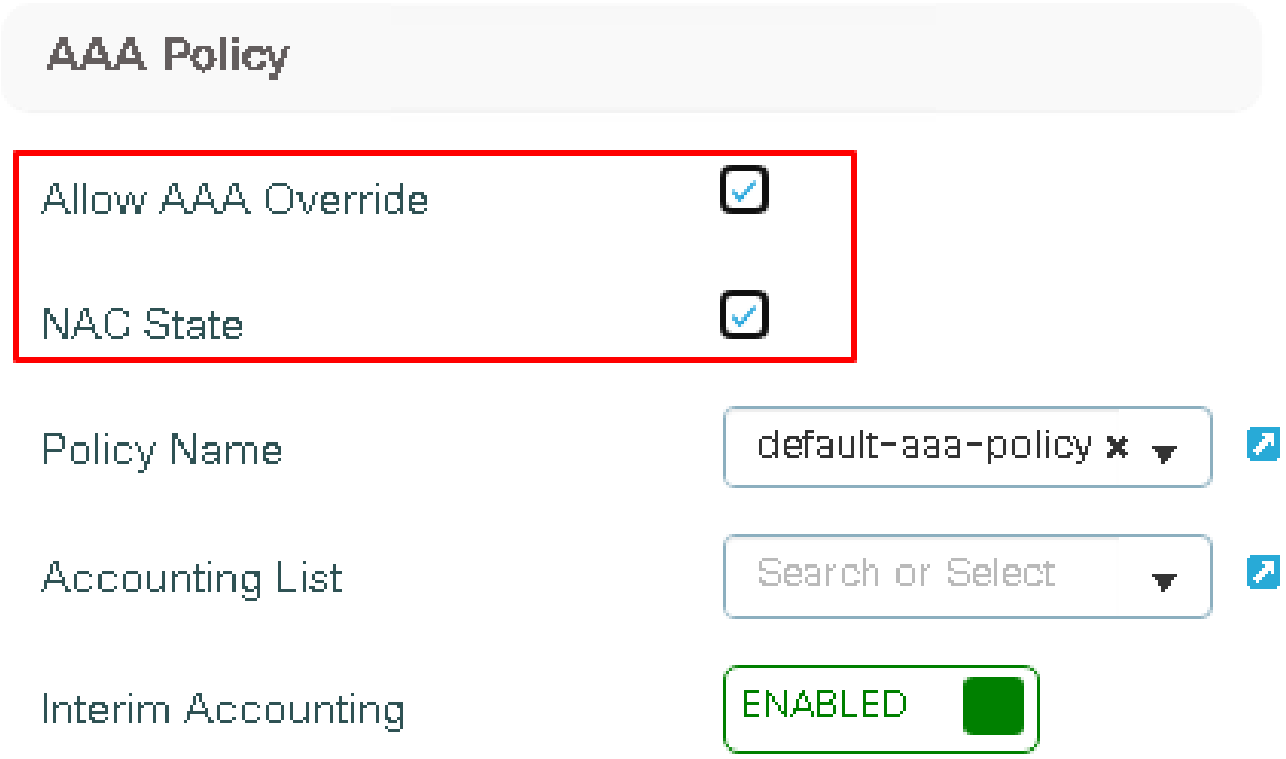
Configuração de Perfil de Diretiva sem Fio

Dentro do Policy Profile, os clientes podem receber configurações como VLAN, ACLs, QoS, Mobility Anchor e temporizadores. Para exibir a configuração do perfil de política, navegue até Configuração > Marcas e perfis > Política.

Clique no nome da política para exibir sua configuração.



O status da política é Enabled e como com qualquer SSID de estrutura, a comutação central e o DHCP central estão desabilitados. Clique na guia Advanced e navegue para a seção AAA Policy para exibir detalhes de configuração adicionais.



É possível habilitar o AAA Override e o Network Access Control (NAC). AAA Override permite que o controlador aceite atributos retornados pelo servidor RADIUS, como ACLs ou URLs, e aplique esses atributos aos clientes. O NAC habilita a alteração de autorização (CoA) depois que o cliente se registra no portal.
Essa configuração também pode ser visualizada através da CLI no WLC.

Para verificar o perfil da diretiva, o SSID é anexado para executar o comando:

<#root>

```
WLC#show fabric wlan summary


Number of Fabric wlan : 1

WLAN  Profile Name       SSID       Status
------------------------------------------------------------------------------
21
CWA_Cisco_profile
  CWA_Cisco  UP
```

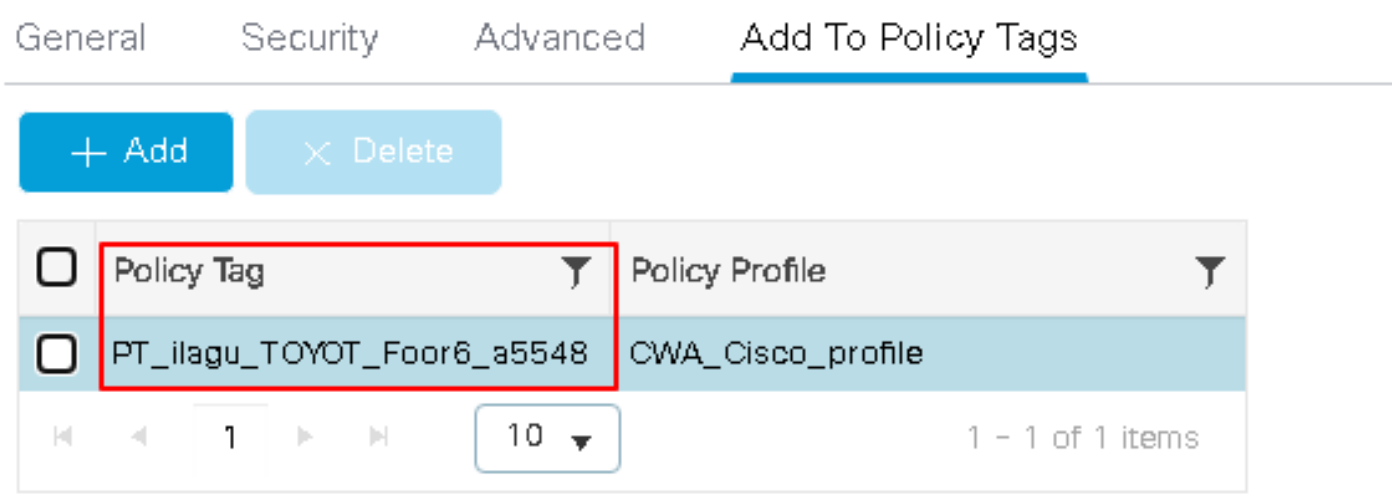
Para exibir a configuração do perfil de política CWA_Cisco_profile, execute o comando:

<#root>

```
WLC#show running-config | section policy CWA_Cisco_profile


wireless profile policy CWA_Cisco_profile
 aaa-override


 no central dhcp


 no central switching


 description CWA_Cisco_profile
 dhcp-tlv-caching
 exclusionlist timeout 180
 fabric CWA_Cisco_profile
 http-tlv-caching
 nac


 service-policy input platinum-up
 service-policy output platinum
 no shutdown
```

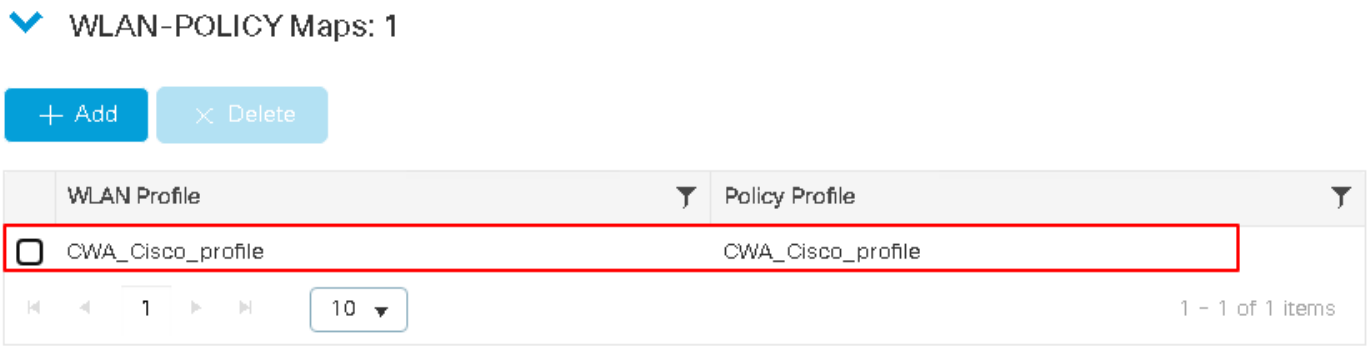
Configuração de marca de política

A tag de política é a maneira como você vincula a WLAN ao Perfil de política, navega para Configuration > Tags & Profiles > WLANs, clica no nome da WLAN e navega para Add to Policy Tags para identificar a tag de política atribuída ao SSID.



Para o SSID CWA_Cisco_profile, a tag de política PT_ilagu_TOYOT_For6_a5548 é usada para verificar essa configuração, vá até Configuration > Tags & Profiles > Tags > Policy.

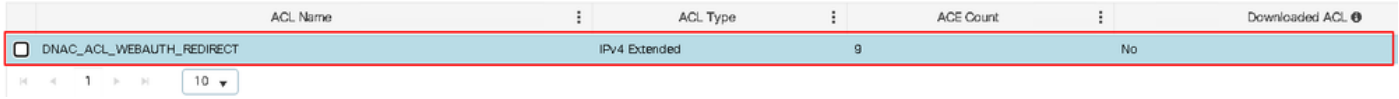
Clique no nome para exibir seus detalhes. A tag de política PT_ilagu_TOYOT_For6_a5548 vincula a WLAN CWA_Cisco que está associada ao nome CWA_Cisco_profile na WLC (consulte a página WLANs para referência) ao Perfil de política CWA_Cisco_profile.



O nome da WLAN CWA_Cisco_profile faz referência à WLAN CWA_Cisco.

Configuração de ACL de redirecionamento

No CWA, uma lista de controle de acesso de redirecionamento define qual tráfego é redirecionado para o WLC para processamento posterior e qual tráfego ignora o redirecionamento Essa configuração é enviada para a WLC após a criação do SSID e o provisionamento da WLC a partir do inventário. Para visualizá-la, navegue até Configuration > Security >ACL, O nome da ACL que o Catalyst Center usa para a ACL de redirecionamento é Cisco DNA_ACL_WEBAUTH_REDIRECT.



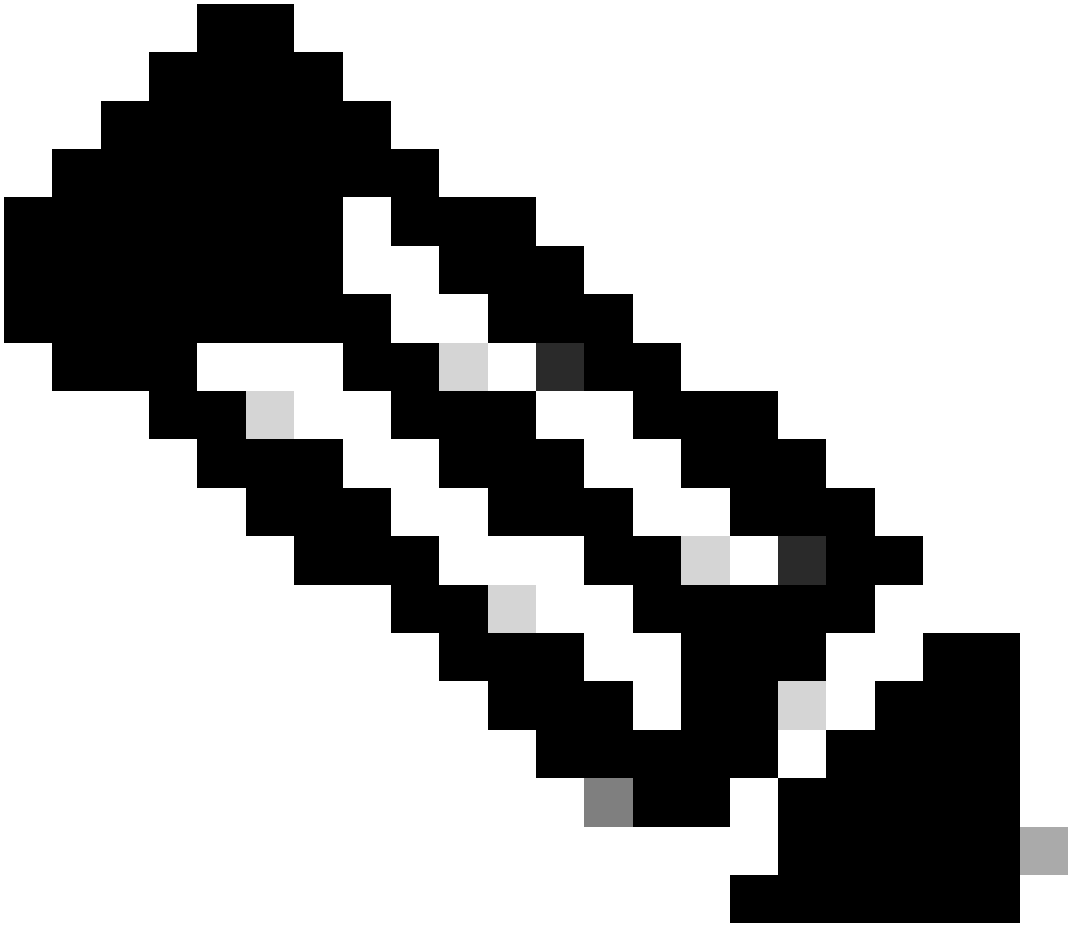
ACL Name	ACL Type	ACE Count	Downloaded ACL
DNAC_ACL_WEBAUTH_REDIRECT	IPv4 Extended	9	No

1 10

Clique no nome para visualizar sua configuração. Os valores são derivados das configurações de rede das configurações de rede do site no Catalyst Center.

Sequence	Action	Source IP	Source Wildcard	Destination IP	Destination Wildcard	Protocol	Source Port	Destination Port	DSCP	Log
1	deny	8.8.8.8		any		udp	eq bootps	eq bootpc	None	Disable
2	deny	any		8.8.8.8		udp	eq bootpc	eq bootps	None	Disable
3	deny	1.1.1.1		any		udp	eq bootps	eq bootpc	None	Disable
4	deny	any		1.1.1.1		udp	eq bootpc	eq bootps	None	Disable
5	deny	9.9.9.9		any		udp	eq bootps	eq bootpc	None	Disable
6	deny	any		9.9.9.9		udp	eq bootpc	eq bootps	None	Disable
7	deny	10.88.244.180		any		ip	None	None	None	Disable
8	deny	any		10.88.244.180		ip	None	None	None	Disable
9	permit	any		any		tcp	0 - 65535	eq www	None	Disable

1 10



Note: Esses valores são obtidos das configurações de rede do site configuradas no Catalyst Center, e os valores DHCP/DNS são originados do pool configurado na WLAN. O endereço IP PSN do ISE é referenciado na configuração AAA dentro do fluxo de trabalho do SSID.

Para visualizar a ACL de redirecionamento na CLI da WLC, execute este comando:

<#root>

```
WLC#show ip access-lists Cisco DNA_ACL_WEBAUTH_REDIRECT


Extended IP access list Cisco DNA_ACL_WEBAUTH_REDIRECT
1 deny udp host 8.8.8.8 eq bootps any eq bootpc
2 deny udp any eq bootpc host 8.8.8.8 eq bootps
3 deny udp host 1.1.1.1 eq bootps any eq bootpc
4 deny udp any eq bootpc host 1.1.1.1 eq bootps
5 deny udp host 9.9.9.9 eq bootps any eq bootpc
6 deny udp any eq bootpc host 9.9.9.9 eq bootps
7 deny ip host 10.88.244.180 any
8 deny ip any host 10.88.244.180
9 permit tcp any range 0 65535 any eq www
```

A ACL de redirecionamento pode ser aplicada ao perfil Flex para que possa ser enviada aos pontos de acesso. Execute este comando para confirmar esta configuração

<#root>

```
WLC#show running-config | section flex


wireless profile flex default-flex-profile

 acl-policy Cisco DNA_ACL_WEBAUTH_REDIRECT



central-webauth



urlfilter list Cisco DNA_ACL_WEBAUTH_REDIRECT
```

Redirecionar ACL no ponto de acesso

No access point, os valores de permissão e negação são invertidos: permit indica o tráfego de encaminhamento e deny indica o redirecionamento. Para revisar a configuração da ACL de redirecionamento no AP, execute este comando:

<#root>

```
AP#sh ip access-lists


Extended IP access list Cisco DNA_ACL_WEBAUTH_REDIRECT
1 permit udp 8.8.8.8 0.0.0.0 dhcp_server any eq 68
2 permit udp any dhcp_client 8.8.8.8 0.0.0.0 eq 67
3 permit udp 1.1.1.1 0.0.0.0 dhcp_server any eq 68
4 permit udp any dhcp_client 1.1.1.1 0.0.0.0 eq 67
5 permit udp 9.9.9.9 0.0.0.0 dhcp_server any eq 68
6 permit udp any dhcp_client 9.9.9.9 0.0.0.0 eq 67
7 permit ip 10.88.244.180 0.0.0.0 any
8 permit ip any 10.88.244.180 0.0.0.0
9 deny tcp any range 0 65535 any eq 80
```

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.