

Configurar a autenticação da Web central no acesso SD

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Topologia](#)

[Overview](#)

[Configurar o CWA no Cisco Catalyst Center](#)

[Criar o perfil de rede](#)

[Criar o SSID](#)

[Provisionamento de estrutura](#)

[Revisar a configuração provisionada para o Cisco ISE](#)

[Perfil de Autorização](#)

[Conjuntos de políticas](#)

[Configuração do Portal do Convidado](#)

[Revisar a configuração provisionada para a WLC](#)

[Configuração de SSID](#)

[Configuração de Perfil de Diretiva sem Fio](#)

[Configuração de marca de política](#)

[Configuração de ACL de redirecionamento](#)

[Redirecionar ACL no ponto de acesso](#)

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)

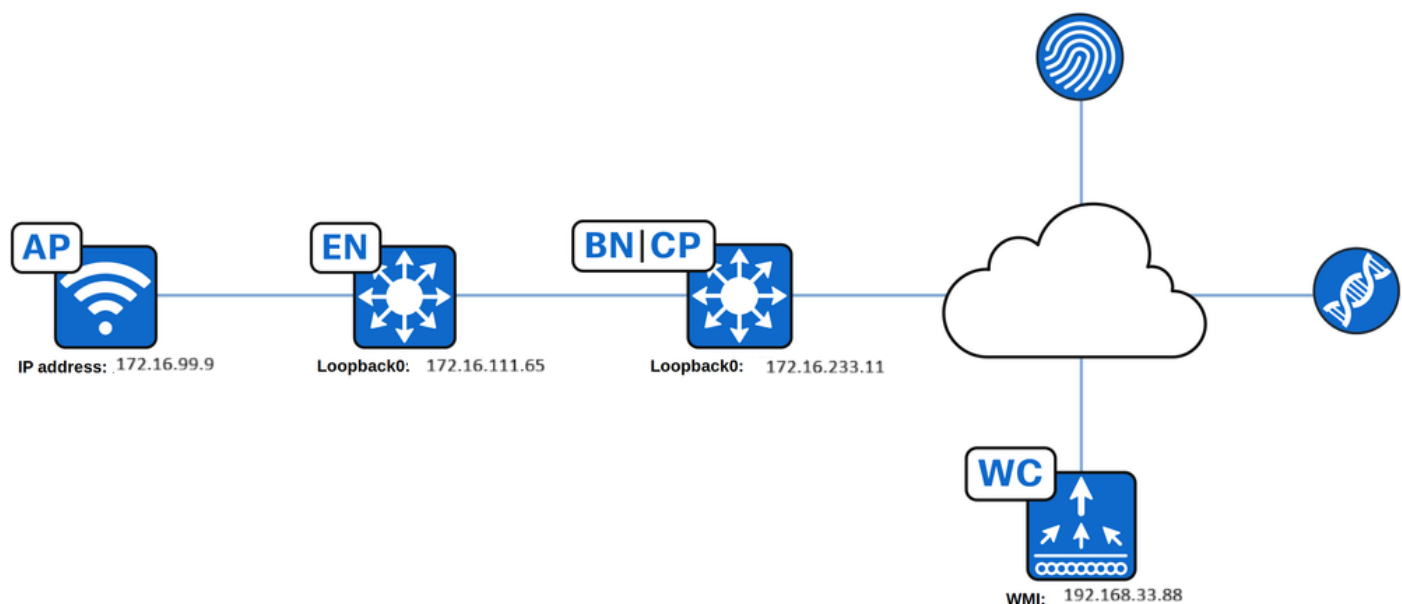
Componentes Utilizados

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® XE 17.12.05
- 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.

Network Profiles

Network Profiles (119)

Search Table

Profile Name	Type	Sites	Action
--------------	------	-------	--------

+ Add Profile

Assurance

Firewall

Routing

Switching

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.

Add a Network Profile

Following tasks must be completed before creating a Wireless Network Profile.

1. Define SSIDs, Interface, RF Profiles and AP Profiles under [Network Settings > Wireless](#)
2. Define CLI Templates under [CLI Templates](#) (Optional)
3. Define Feature Templates under [Feature Templates](#) (Optional)

Note: Changes in SSIDs, AP Zones, Feature Templates, CLI Templates sections require Controller provisioning. Changes in Custom Tags/Groups require Access Point provisioning.

Profile Name*

CWA_Cisco_Wireless_Profile

Site: Assign

SSIDs AP Zones Feature Templates CLI Templates Advanced Settings

Add SSID

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

Profile Name*

CWA_Cisco_Wireless_Profile

Site: [Assign](#)

SSIDs

AP Zones

Feature Templates

CLI Templates

Advanced Settings ▾

Add SSID

Criar o SSID

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

SSIDs

Configure SSIDs for enterprise and guest wireless networks. You can assign them to sites via Wireless Network Profiles.

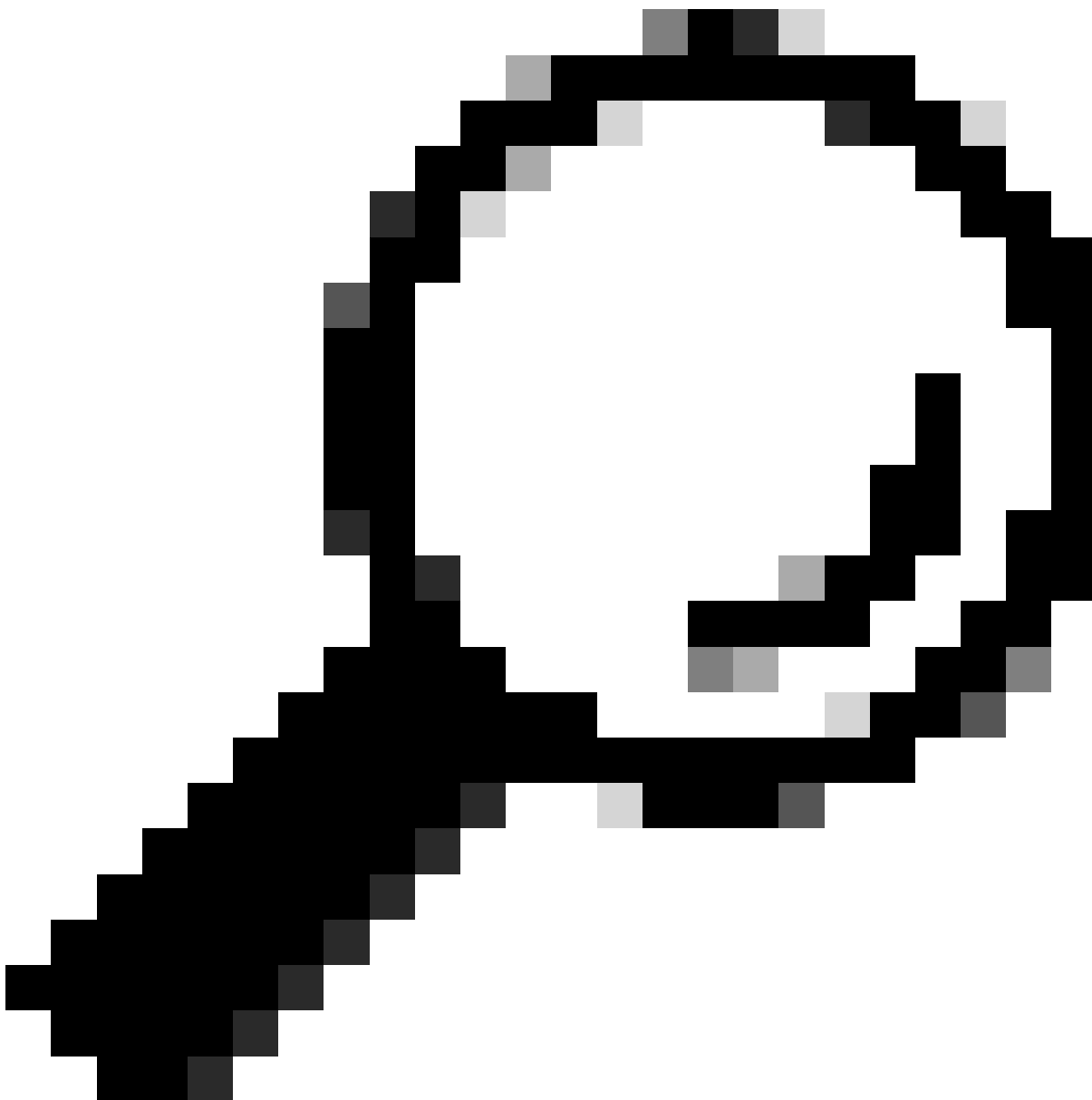
SSID (79)

[+ Add](#)

Search Table

[Edit](#) [Delete](#) [SSID Scheduler](#) ⓘ 0 Selected

☐	Network Name (SSID) ▾	WLAN Profile Name	Policy Profile Name	SSID Type	L2 Security	L3 Security	Wireless Profiles	Portal Name	AAA Servers
☐	1865test	1865test_... (2)	1865test_... (2)	Enterprise	wpa3_personal	open	fernarom_wireless, J... See all	N/A	Configure AAA



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`.

Wireless Network Name (SSID)* CWA_Cisco	WLAN Profile Name* CWA_Cisco_profile	Policy Profile Name CWA_Cisco_profile
---	--	---

Radio Policy

☒ 2.4GHz
 ☒ 5GHz
 ☒ 6GHz ⓘ

802.11b/g Policy
802.11bg ▼
 ☐ Band Select ⓘ
 ☐ 6 GHz Client Steering

☐ Fast Lane ⓘ

Quality of Service(QoS) ⓘ

Egress
VoIP (Platinum) ⓘ ▼
 Ingress
VoIP (Platinum) Up ⓘ ▼ ⓘ

SSID STATE

☒ Admin Status
 ☒ Broadcast SSID

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.

Authentication, Authorization, and Accounting Configuration

Atleast one AAA/PSN is required for CWA SSIDs. Configure AAA to add one.

 [Configure AAA](#)

☐ AAA Override

☒ MAC Filtering

☐ Deny RCM Clients ⓘ

Pre-Auth ACL List Name ▼

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.

L3 SECURITY

☒ Web Policy ☐ Open

Most secure

Guest users are redirected to a Web Portal for authentication

Authentication Server

Central Web Authentication	What kind of portal are you creating today ?	Where will your guests redirect after successful authentication ?
	Self Registered	Original URL
	Self Registered	
	Hotspot	

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.

Authentication Server

Central Web Authentication	What kind of portal are you creating today ?	Where will your guests redirect after successful authentication ?
	Self Registered	Original URL
		Success Page
		Original URL
		Custom URL

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.

Authentication, Authorization, and Accounting Configuration

 AAA Configured (1)

☒ AAA Override

☒ MAC Filtering

☐ Deny RCM Clients 

Pre-Auth ACL List Name 

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

Pre-Auth ACLs AP Authorization List AP Impersonation Configure DTLS Ciphersuites

Configure Pre-Auth Access Control Lists. You can assign them to SSIDs during SSID creation or modification.

Pre-Auth Access Control Lists (10)

 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.

New Pre-Auth ACL

Pre-Auth ACL List Name*
Name_on_Catalyst_Center 

Pre-Auth ACL Name*
DNAC_ACL_WEBAUTH_REDIRECT 

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.

Advanced Settings

Configure the advanced fields to complete SSID setup.

SSID Name: CWA_Cisco (Guest)

MFP Client Protection ⓘ

☒ Optional ☐ Required ☐ Disabled

Protected Management Frame (802.11w)

☐ Optional ☐ Required ☒ Disabled

☒ 11k - Neighbor List

☐ Radius Client Profiling ⓘ

☒ Coverage Hole Detection

WLAN Timeouts

☒ Session Timeout ⓘ

In (secs)*
28800
Range is from 1 to 86400

☒ Client Exclusion

In (secs)*
180
Range is from 0 to 2147483647

☒ Client User Idle Timeout

In (secs)*
300
Range is from 15 to 100000

11v BSS Transition Support

☒ BSS Max Idle Service

☒ Directed Multicast Service

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.

Associate Feature Templates to SSID

Select a design instance from the table or add new design instance to associate the Feature Templates to SSID.

Design Instances

[Refresh](#)

[Export](#)

[Import](#)

[Add](#)

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.

SSID Name: CWA_Cisco (Guest)

[+ Add Profile](#)

100NG SOM RA

adortiz-test-profile

anarami-wireless

angel test

antvegaprofile

Cnicolet_Oeiras

CWA_Cisco_Wireless_P...

[Associate Profile](#)

[Cancel](#)

Profile Name

CWA_Cisco_Wireless_Profile

WLAN Profile Name

CWA_Cisco_profile ⓘ

Fabric

☒ Yes ☐ No

Policy Profile Name

CWA_Cisco_profile ⓘ

802.11be Profile Name

▼

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

No Self Registration Portal Available

Create Portal

Portal

CWA_Cisco_Portal

Login Page

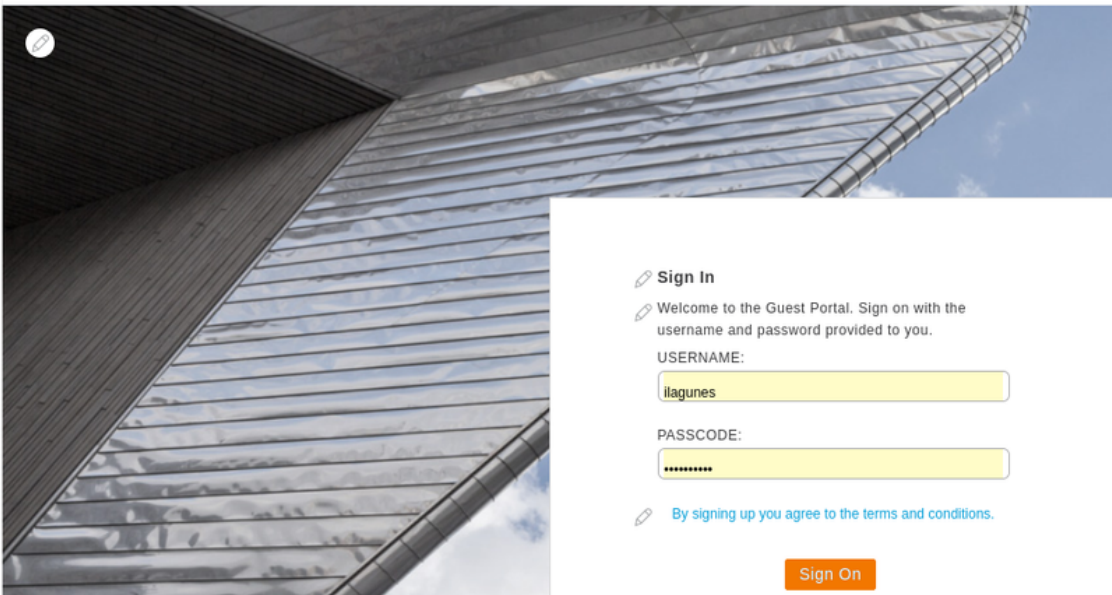
> Page Content

Access Code

Header Text



**HIGH-TECH CORPORATION**





Sign In

 Welcome to the Guest Portal. Sign on with the username and password provided to you.

USERNAME:

PASSCODE:

 [By signing up you agree to the terms and conditions.](#)

Sign On

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

Summary

Review all changes

SSID Name: CWA_Cisco (Guest)

> Basic Settings [Edit](#)

> Security Settings [Edit](#)

> Advanced Settings [Edit](#)

∨ Associate Feature Templates to SSID [Edit](#)

Design Instance	N/A
-----------------	-----

∨ Network Profile Settings [Edit](#)

CWA_Cisco_Wireless_Profile	Fabric (Associated)
----------------------------	-------------------------------------

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

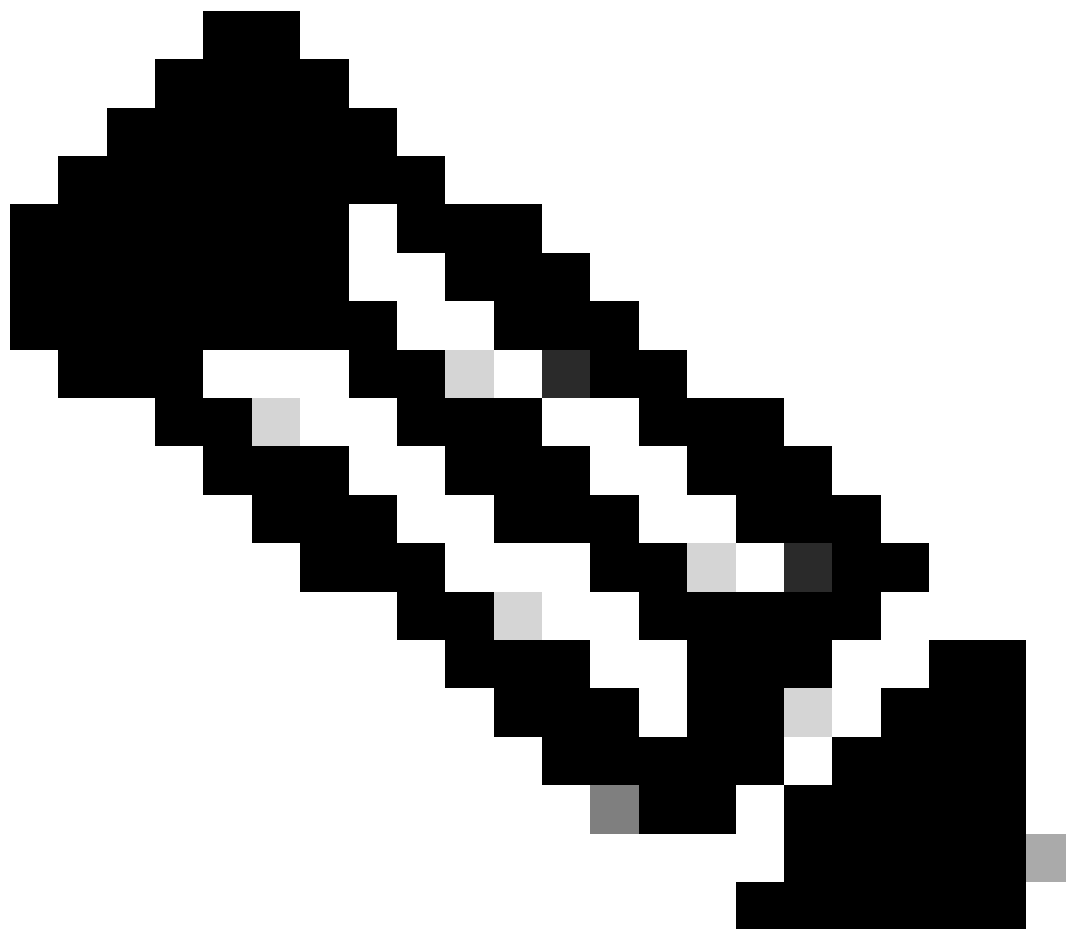
Escolha o pool SSID, opcionalmente associe uma Tag de grupo de segurança e clique em Implantar. O SSID é transmitido por pontos de acesso somente se um pool for atribuído.

☒ Enable Wireless Multicast ⓘ

SSID Name	Type	Security	Traffic Type	Address Pool	Security Group
CWA_Cisco	Guest	Open	Voice + Data	Choose Pool test 	Assign SGT 

1 Record(s) Show Records: 25 ▾ 1 - 1 < ⓘ >

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.

Standard Authorization Profiles

For Policy Export go to [Administration > System > Backup & Restore > Policy Export Page](#)

Selected 0 Total 18

[Edit](#) [+ Add](#) [Duplicate](#) [Delete](#)

All [Filter](#)

☐	Name	Profile	Description
☐	AuthProfile-DNAC	Cisco	SGT Authentication Profile para DNACtl
☐	Block_Wireless_Access	Cisco	Default profile used to block wireless devices. Ensure that you configure a NULL RC
☐	CWA_Cisco_Portal_Profile	Cisco	DNA generated Authorization Profile for 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.

Common Tasks

☒ Web Redirection (CWA, MDM, NSP, CPP)

Centralized Web Auth

ACL

DNAC_ACL_WEBAUTH_RE...

Value

CWA_Cisco_Portal

☒ Display Certificates Renewal Message

☐ Static IP/Host name/FQDN

☐ Suppress Profiler CoA for endpoints in Logical Profile

Conjuntos de políticas

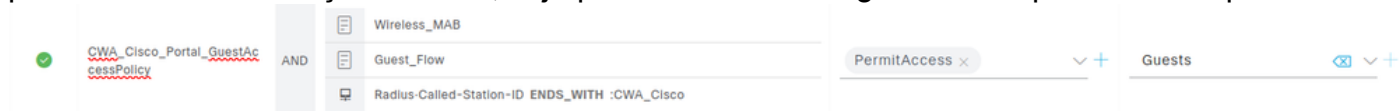
Navegue até Policy > Policy Sets > Default > Authorization Policy para exibir os dois conjuntos de políticas criados para o portal chamado CWA_Cisco_Portal. Esses conjuntos de políticas são:

- CWA_Cisco_Portal_GuestAccessPolicy
- CWA_Cisco_Portal_RedirectPolicy

☒	CWA_Cisco_Portal_GuestAccessPolicy	AND	Wireless_MAB Guest_Flow Radius-Called-Station-ID ENDS_WITH :CWA_Cisco	PermitAccess x	Guests
☒	CWA_Cisco_Portal_RedirectPolicy	AND	Wireless_MAB Radius-Called-Station-ID ENDS_WITH :CWA_Cisco	CWA_Cisco_Portal_Pr... x	Select from list

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.



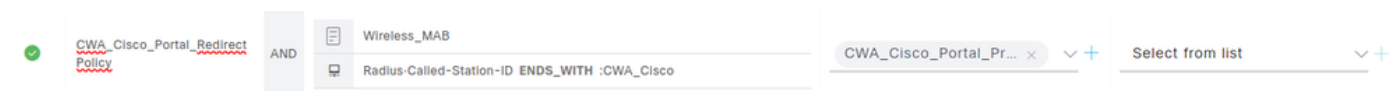
Esse conjunto de políticas atende a três critérios:

- **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.

Guest Portals

Choose one of the three pre-defined portal types, which you can edit, customize, and authorize for guest access.

Create Edit Duplicate Delete

CWA_Cisco_Portal
Wireless Setup Self-Registration Guest Portal
✔ Used in 1 rules in the Authorization policy

Deadpool_Site
Wireless Setup Self-Registration Guest Portal
✔ Used in 1 rules in the Authorization policy

Hotspot Guest Portal (default)
Guests do not require username and password credentials to access the network, but you can optionally require an access code
⚠ Authorization setup required

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.

Selected WLANs : 0

☐	Status	Name	ID	SSID	2.4/5 GHz Security
☐		CWA_Cisco_profile	21	CWA_Cisco	[open], MAC Filtering
		1		10	

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.

General Security Advanced Add To Policy Tags

Profile Name*

CWA_Cisco_profile

SSID*

CWA_Cisco

WLAN ID*

21

Status

ENABLED

Broadcast SSID

ENABLED

Radio Policy ⓘ

Show slot configuration

6 GHz

Status

DISABLED

5 GHz

Status

ENABLED

2.4 GHz

Status

ENABLED

802.11b/g Policy

802.11b/g

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.

Layer2 Layer3 AAA

☐ WPA + WPA2

☐ WPA2 + WPA3

☐ WPA3

☐ Static WEP

☒ None

MAC Filtering☒

OWE Transition Mode☐

Lobby Admin Access☐

Fast Transition

Status

Disabled

Over the DS☐

Reassociation Timeout *

20

Authorization List*

co-0044d514

default

dnac-cts-

CWA_Cisco-

0044d514

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.

Servers / Groups AAA Method List AAA Advanced

Authentication

Authorization

Accounting

+ Add

× Delete

	Name	Type	Group Type	Group1	Group2	Group3	Group4
☐	default	exec	local	N/A	N/A	N/A	N/A
☐	default	network	local	N/A	N/A	N/A	N/A
☐	dnac-cts-CWA_Traini-6a20f88c	network	group	dnac-rGrp-CWA_Traini-6a20f88c	N/A	N/A	N/A
☐	dnac-cts-Guest_pers-6fc56a40	network	group	dnac-rGrp-Guest_pers-6fc56a40	N/A	N/A	N/A
☐	dnac-cts-CWA_Cisco-0044d514	network	group	dnac-rGrp-CWA_Cisco-0044d514	N/A	N/A	N/A

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.

Servers Server Groups

	Name	Server 1	Server 2	Server 3
☐	dnac-rGrp-CWA_Cisco-0044d514	dnac-radius_10.88.244.180	N/A	N/A

1 - 1 of 1 items

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.

Servers Server Groups

	Name	Address	Auth Port	Acct Port
☐	dnac-radius_10.88.244.180	10.88.244.180	1812	1813

1 - 1 of 1 items

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

Name*	dnac-radius_10.88.244.	Support for CoA ⓘ	ENABLED 
Server Address*	10.88.244.180	CoA Server Key Type	Hidden ▼
Set New Key	☐	CoA Server Key ⓘ	
Auth Port	1812	Automate Tester	☐
Acct Port	1813		
Server Timeout (seconds)	4		
Retry Count	3		

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.

	Admin Status	Associated Policy Tags	Policy Profile Name	Description
☐	✓		CWA_Cisco_profile	CWA_Cisco_profile
☐	✓		default-policy-profile	default policy profile

Clique no nome da política para exibir sua configuração.

Name* CWA_Cisco_profile

Description CWA_Cisco_profile

Status **ENABLED** 

Passive Client  DISABLED

IP MAC Binding **ENABLED** 

Encrypted Traffic Analytics  DISABLED

CTS Policy

Inline Tagging ☐

SGACL Enforcement ☐

Default SGT 2-65519

WLAN Switching Policy

Central Switching  DISABLED

Central Authentication **ENABLED** 

Central DHCP  DISABLED

Flex NAT/PAT  DISABLED

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.

AAA Policy

Allow AAA Override ☒

NAC State ☒

Policy Name default-aaa-policy x 

Accounting List Search or Select 

Interim Accounting **ENABLED** 

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.

+ Add		× Delete	
☐	Policy Tag	Policy Profile	
☐	PT_ilagu_TOYOT_Foor6_a5548	CWA_Cisco_profile	
1		10	1 - 1 of 1 items

Para o SSID CWA_Cisco_profile, a tag de política PT_ilagu_TOYOT_Foor6_a5548 é usada para verificar essa configuração, vá até Configuration > Tags & Profiles > Tags > Policy.

Policy Tag Name	Description
☐ default-policy-tag	default policy-tag
☐ PT_ilagu_TOYOT_Foor6_a5548	PolicyTagName PT_ilagu_TOYOT_Foor6_a55

Clique no nome para exibir seus detalhes. A tag de política PT_ilagu_TOYOT_Foor6_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.

WLAN-POLICY Maps: 1

+ Add		× Delete	
	WLAN Profile	Policy Profile	
☐	CWA_Cisco_profile	CWA_Cisco_profile	
1		10	1 - 1 of 1 items

O nome da WLAN CWA_Cisco_profile faz referência à WLAN CWA_Cisco.

☐	Status	Name	ID	SSID
☐		CWA_Cisco_profile	21	CWA_Cisco

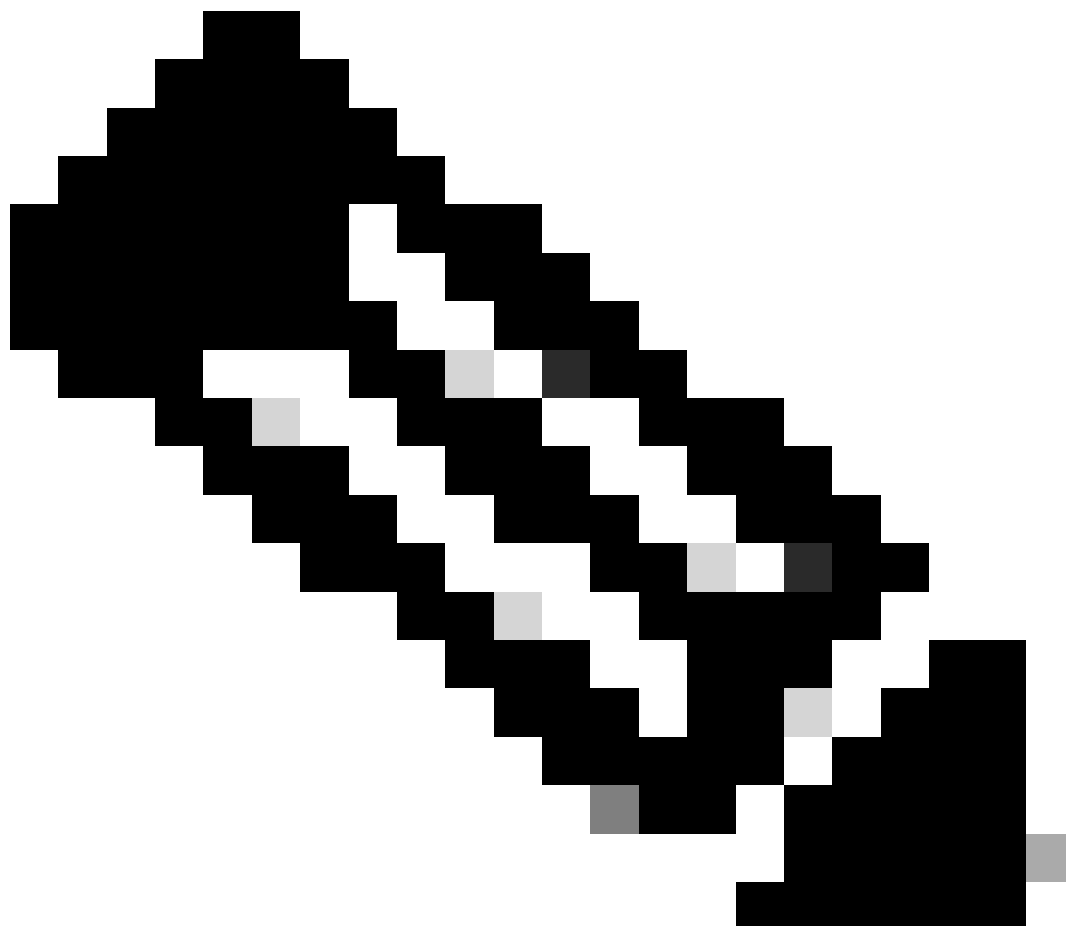
Configuração de ACL de redirecionamento

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

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



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.