

Configurar o FlexConnect EWA no Catalyst 9800 WLC e ISE

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Configurar](#)

[Diagrama de Rede](#)

[Configurações](#)

[Verificar](#)

[Exemplo de rastreamento de RA de uma tentativa bem-sucedida](#)

[Informações Relacionadas](#)

Introdução

Este documento descreve como configurar um FlexConnect EWA no Catalyst 9800 WLC e ISE.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento da configuração de 9800 Wireless LAN Controllers (WLC).

Componentes Utilizados

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

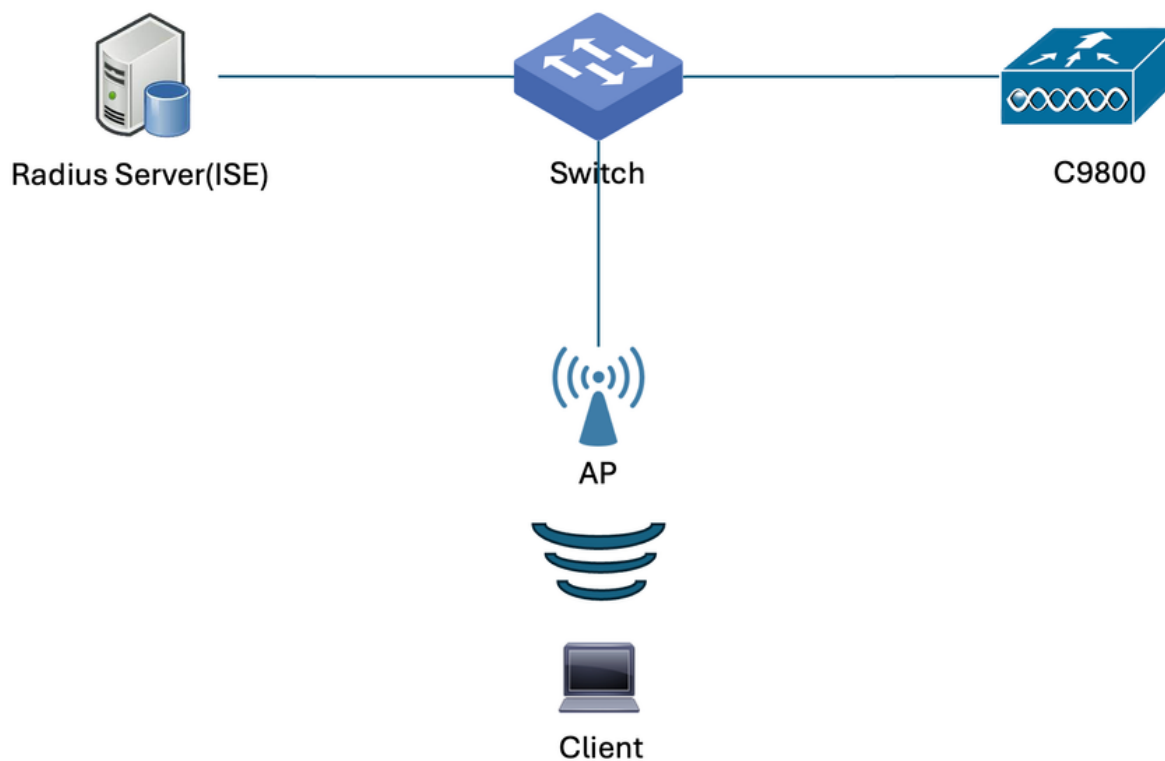
- Cisco Catalyst 9800 WLC Cisco IOS®XE versão 17.15.3
- Identity Service Engine (ISE) v3.4.0.608

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.

Configurar

Diagrama de Rede

Este documento é baseado nesta topologia:

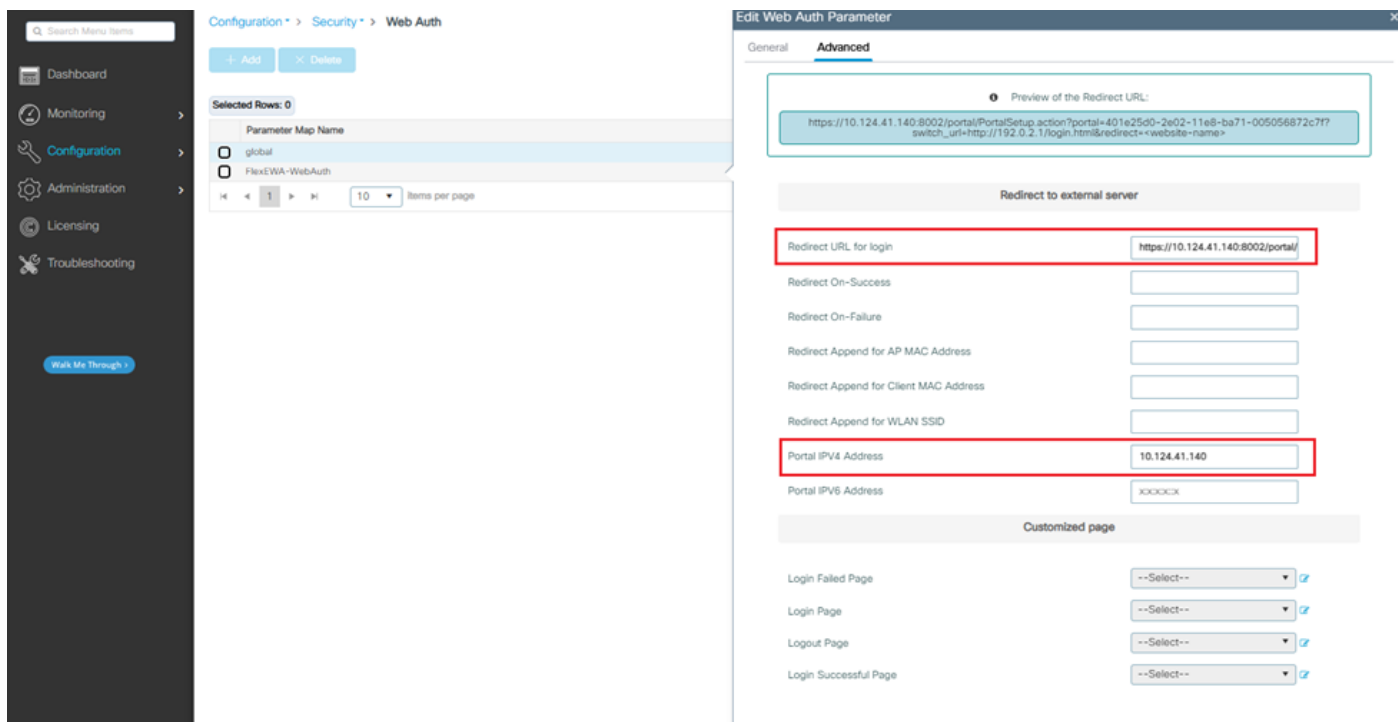


Configurações

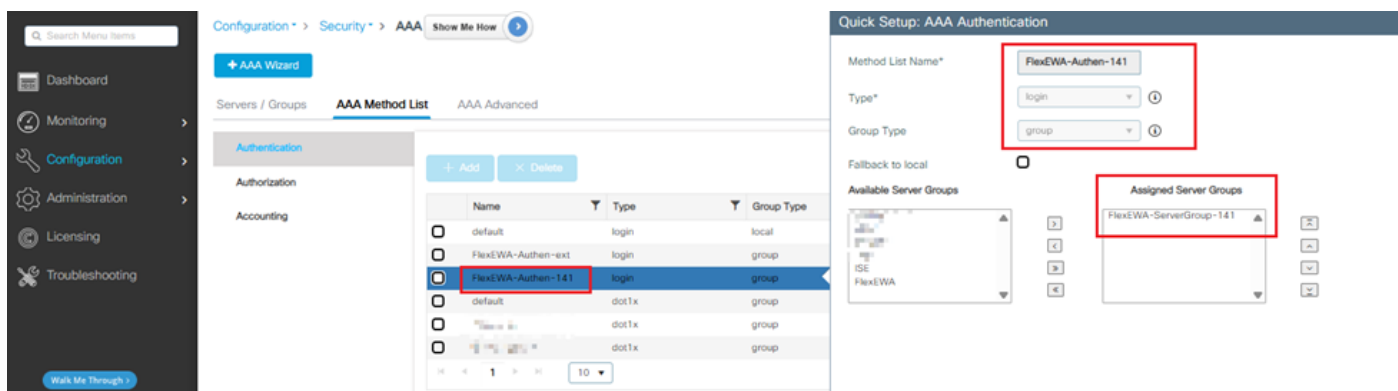
Etapa 1. Navegue até Configuration > Security > Web Auth > +Add a Web Auth Parameter Map.

The screenshot shows the Cisco ISE configuration interface. On the left is a navigation menu with options like Dashboard, Monitoring, Configuration, Administration, Licensing, and Troubleshooting. The main area displays the 'Configuration > Security > Web Auth' path. A table lists parameter maps: 'global', 'FlexEWA-WebAuth', and 'FlexEWA-WebAuth-141'. The 'FlexEWA-WebAuth-141' map is selected. On the right, the 'Edit Web Auth Parameter' window is open, showing the 'General' tab. The 'Parameter-map Name' is 'FlexEWA-WebAuth-141', and the 'Type' is 'webauth'. Other settings include 'Maximum HTTP connections' (100), 'Init-State Timeout(secs)' (120), and 'Banner Configuration' (Banner Title, Banner Type, and Read From File).

A URL do portal é gerada no ISE (etapa 7).



Etapa 2. Navegue até Configuration > Security > AAA > AAA Method List > Authentication > + Add an Authentication List.



Etapa 3. Suponha que a porta HTTPS seja 8002, consulte a ACL autogerada WA-sec-10.124.41.140 para adicionar uma nova ACL de pré-autenticação.

Configuration > Security > ACL

ACL Name: FlexEWA141-sec-ACL

ACL Type: IPv4 Extended

Rules:

Sequence	Action	Source IP	Source Wildcard	Destination IP	Destination Wildcard	Protocol	Source Port	Destination Port	DSCP	Log
10	permit	any		10.124.41.141		tcp	None	eq www	None	Disabled
15	permit	any		10.124.41.141		tcp	None	eq 8002	None	Disabled
20	permit	any		10.124.41.141		tcp	None	eq 443	None	Disabled
25	permit	10.124.41.141		any		tcp	eq 8002	None	None	Disabled
30	permit	10.124.41.141		any		tcp	eq www	None	None	Disabled
40	permit	10.124.41.141		any		tcp	eq 443	None	None	Disabled
50	permit	any		any		tcp	None	eq domain	None	Disabled
60	permit	any		any		udp	None	eq domain	None	Disabled
70	permit	any		any		udp	None	eq bootpc	None	Disabled
80	permit	any		any		udp	None	eq bootps	None	Disabled

Etapa 4. Verifique a ACL autogerada WA-v4-int 10.124.41.141.

Configuration > Security > ACL

ACL Name: WA-v4-int-10.124.41.141

ACL Type: IPv4 Extended

Rules:

Sequence	Action	Source IP	Source Wildcard	Destination IP	Destination Wildcard	Protocol	Source Port	Destination Port	DSCP	Log
10	deny	any		10.124.41.141		tcp	None	eq www	None	Disabled
20	permit	any		any		tcp	None	eq www	None	Disabled

Etapa 5. Aplique as duas ACLs a Configuration > Tags&Profiles > Flex > Flex Profile > Policy ACL.

Configuration > Tags & Profiles > Flex

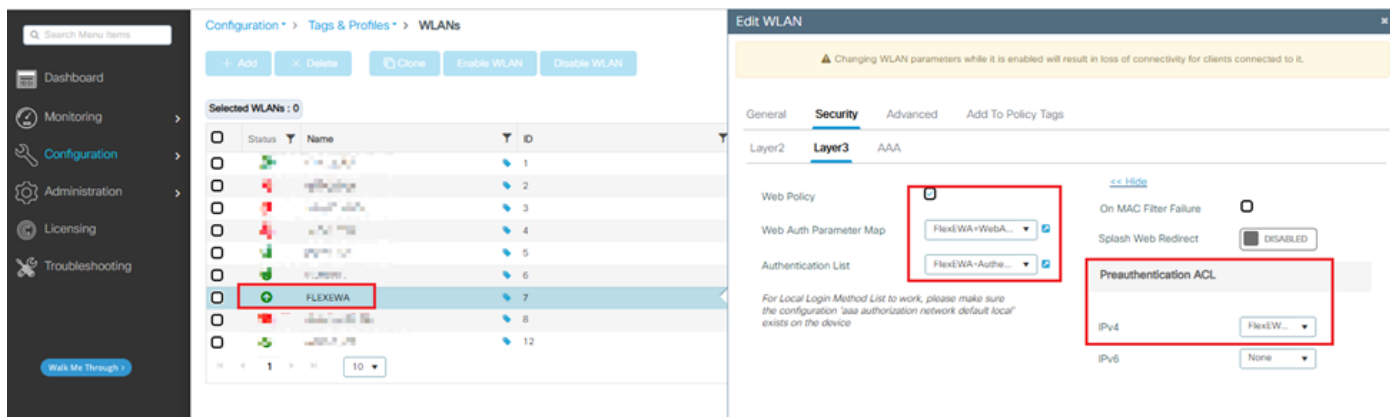
Selected Rows: 0

Flex Profile Name: default-flex-profile

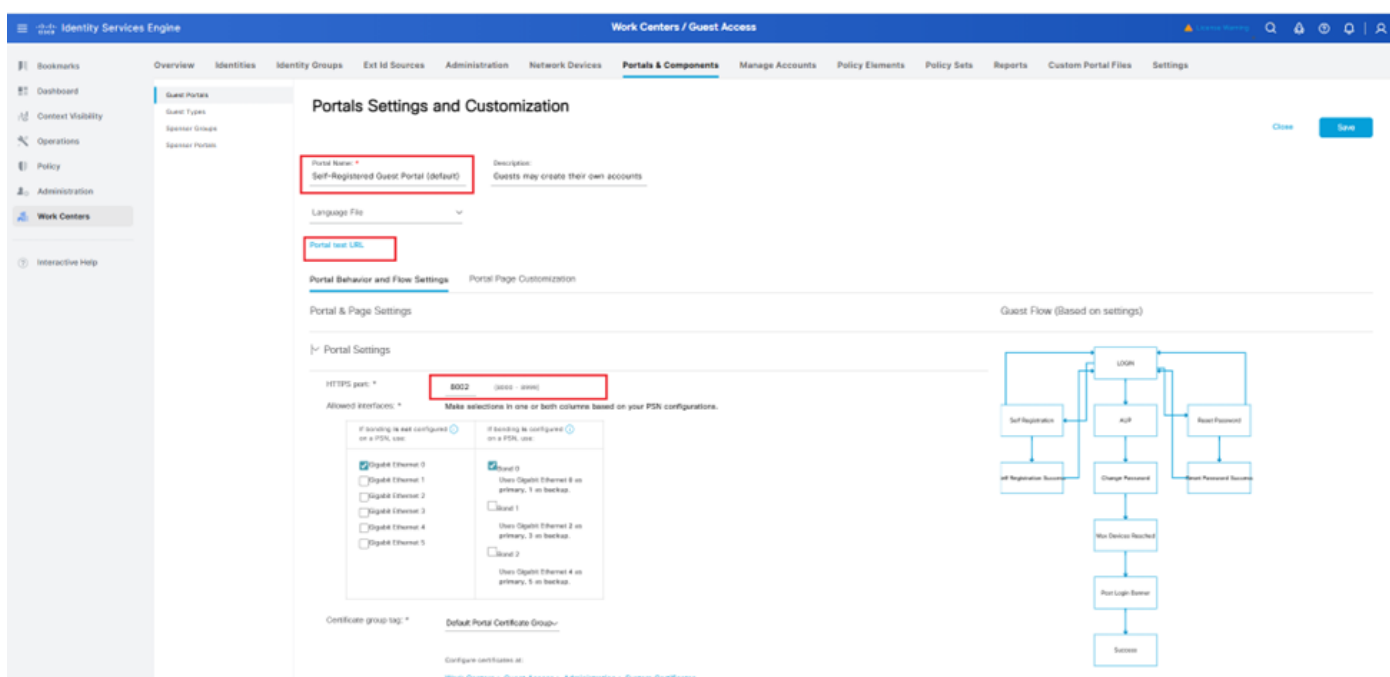
Policy ACL:

ACL Name	Central Web Auth	URL Filter
FlexEWA141-sec-ACL	Disabled	
WA-v4-int-10.124.41.141	Disabled	

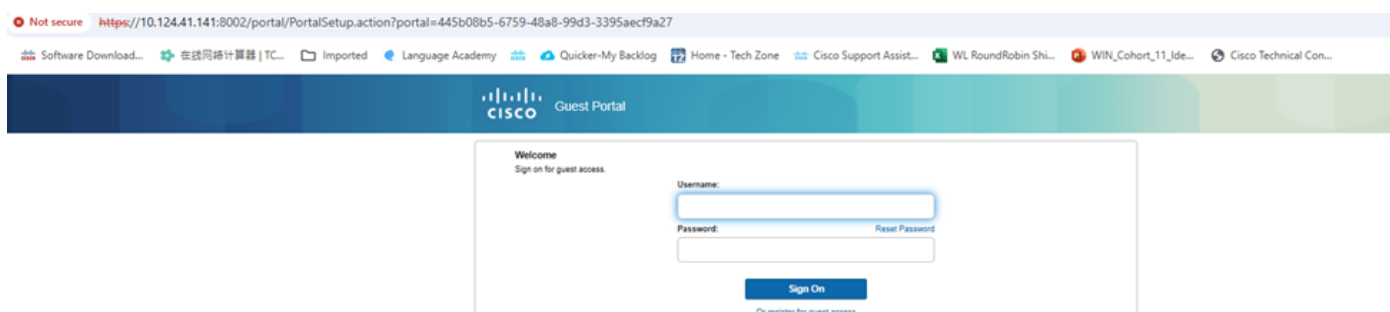
Etapa 6. Aplique o recém-criado Web Auth Parameter Map, Authentication List e Preauthentication ACL à WLAN.



Etapa 7. Navegue até Centros de trabalho > Portais e componentes > Portais de convidado > Configurações e personalização de portais > Nome do portal > Portal de convidado autorregistrado (padrão) para gerar o URL do portal do ISE.

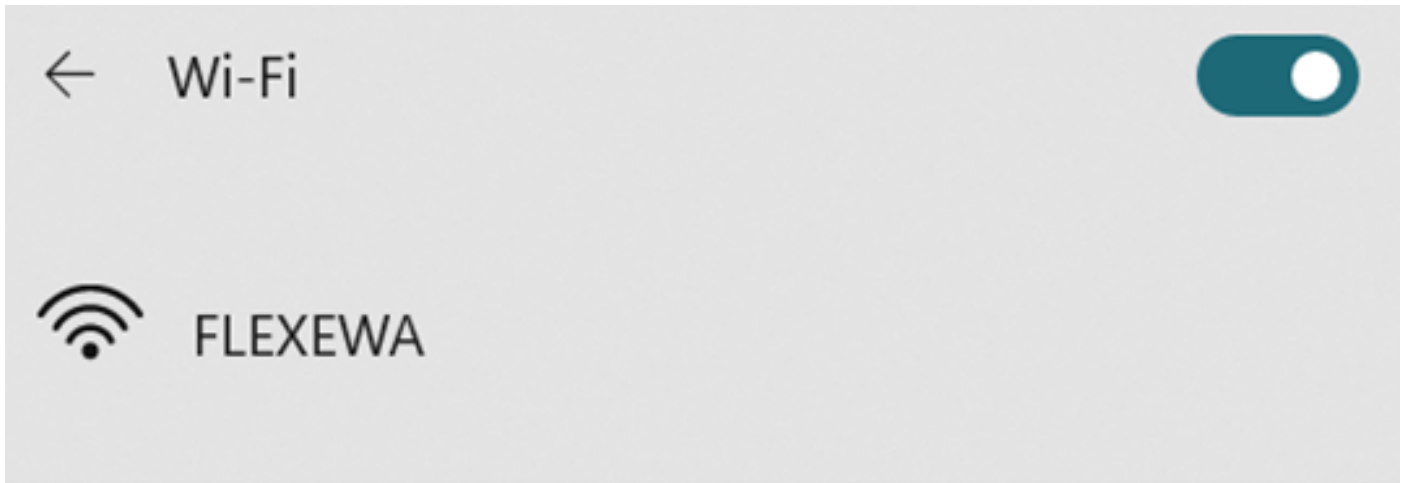


Este portal da Web listado é exibido após clicar em URL de teste do portal.

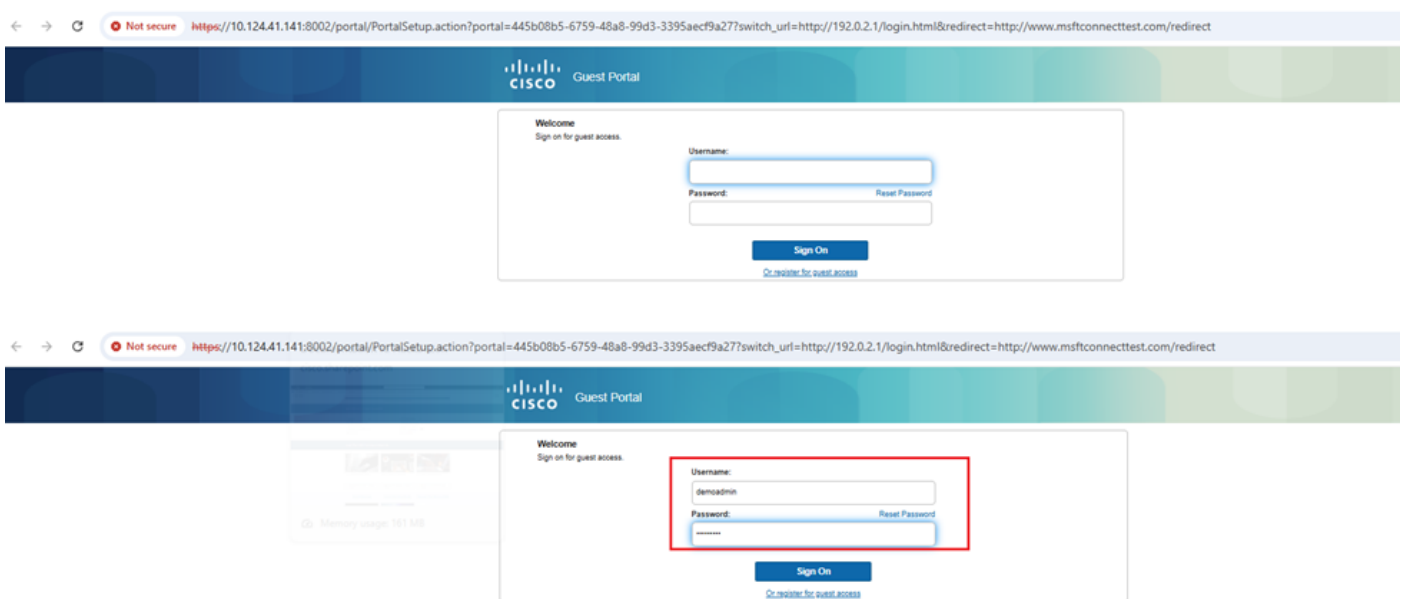


Verificar

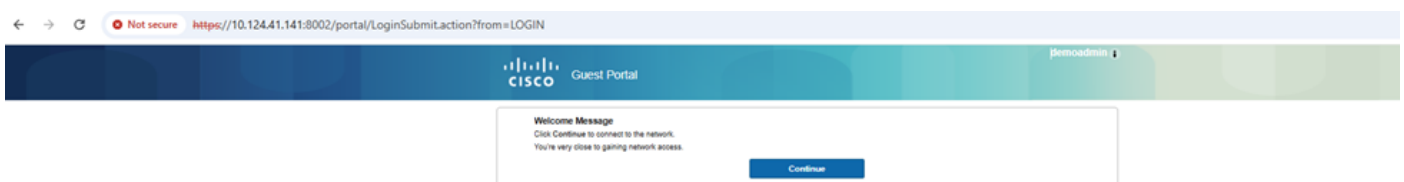
Etapa 1. Conectando o SSID FLEXEWA.



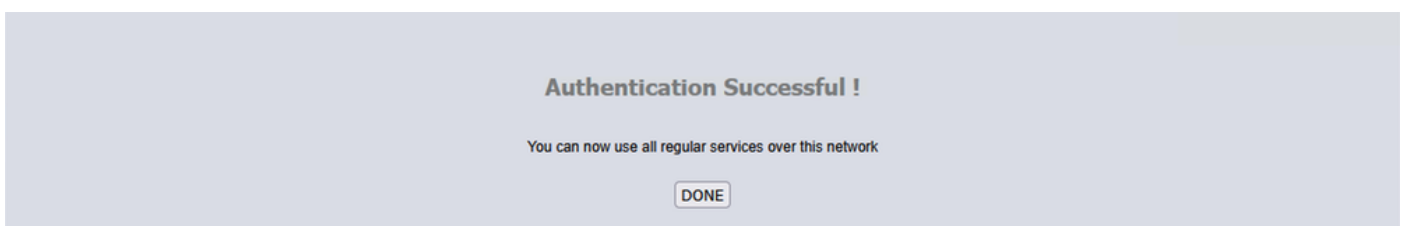
Etapa 2. Redirecionar para o portal e inserir o nome de usuário e a senha.



Etapa 3. O Portal do Convidado será exibido:



Etapa 4. Depois de clicar em Continuar, a autenticação é bem-sucedida:



Exemplo de rastreamento de RA de uma tentativa bem-sucedida

Esta é a saída de uma tentativa de conexão bem-sucedida da perspectiva de rastreamento de Rádio Ativo. Use-o como referência para identificar estágios de sessão de cliente para clientes que se conectam a um SSID de autenticação da Web de Camada 3.

Cliente associado com êxito:

09/2025/09 15:21:48.617769958 {wncd_x_R0-0}{1}: [client-orch-sm] [17842]: (nota): MAC: f0b6.1e39.9ce8 Associação recebida. BSSID c418.fc82.bb0b, WLAN FLEXEWA, Slot 1 AP c418.fc82.bb00, 9178_1, Site tag HK, Policy tag default-policy-tag, Policy profile default-policy-profile, Switching Central, Socket delay 0ms, AP BSSID MAC c418.fc82.bb0b

09/2025/09 15:21:48.617813534 {wncd_x_R0-0}{1}: [client-orch-sm] [17842]: (depurar): MAC: f0b6.1e39.9ce8 Recebeu solicitação de associação Dot11. Processamento iniciado,SSID: FLEXEWA, Perfil da política: default-policy-profile, Nome do AP: 9178_1, Endereço Mac Do Ap: c418.fc82.bb00BSSID MAC0000.0000.0000wlan ID: 7RSSI: -30, SNR: 67

09/2025/09 15:21:48.618002570 {wncd_x_R0-0}{1}: [client-orch-state] [17842]: (nota): MAC: f0b6.1e39.9ce8 Transição de estado do cliente: S_CO_INIT -> S_CO_ASSOCIATING

09/2025/09 15:21:48.618017149 {wncd_x_R0-0}{1}: [client-orch-sm] [17842]: (ERRO): MAC: f0b6.1e39.9ce8 Falha ao obter registro dot11

09/2025/09 15:21:48.618301251 {wncd_x_R0-0}{1}: [dot11-validate] [17842]: (informações): MAC: f0b6.1e39.9ce8 Dot11 ie validar taxas de texto/suporte. Validação Aprovada para taxas com suporte radio_type 2

09/2025/09 15:21:48.618320304 {wncd_x_R0-0}{1}: [dot11-validate] [17842]: (depurar): MAC: f0b6.1e39.9ce8 Dot11 ie validar rsnx, cliente não usando sae, ignorar verificação

09/2025/09 15:21:48.618339230 {wncd_x_R0-0}{1}: [dot11-validate] [17842]: (informações): MAC: f0b6.1e39.9ce8 WiFi direto: Dot11 valida IE P2P. IE P2P ausente.

09/2025/09 15:21:48.618598747 {wncd_x_R0-0}{1}: [ponto11] [17842]: (depurar): MAC: f0b6.1e39.9ce8 dot11 envia resposta de associação. Resposta de associação de enquadramento com resp_status_code: 0

09/2025/09 15:21:48.618604733 {wncd_x_R0-0}{1}: [ponto11] [17842]: (depurar): MAC: f0b6.1e39.9ce8 Dot11 Informações de capacidade byte1 1, byte2: 11

09/2025/09 15:21:48.618696034 {wncd_x_R0-0}{1}: [quadro dot11] [17842]: (informações): MAC: f0b6.1e39.9ce8 WiFi direto: ignorar compilação de Assoc Resp com IE P2P: Política de WiFi Direct desabilitada

09/2025/09 15:21:48.618785409 {wncd_x_R0-0}{1}: [ponto11] [17842]: (informações): MAC: f0b6.1e39.9ce8 dot11 envia resposta de associação. Enviando resposta assoc de comprimento: 177 com resp_status_code: 0, STATUS_DOT11: DOT11_STATUS_SUCCESS

09/2025/09 15:21:48.618791096 {wncd_x_R0-0}{1}: [ponto11] [17842]: (nota): MAC: f0b6.1e39.9ce8 Sucesso da associação. AID 33, Roaming = False, WGB = False, 11r = False, 11w = False Fast roam = False

09/2025/09 15:21:48.618806595 {wncd_x_R0-0}{1}: [ponto11] [17842]: (informações): MAC: f0b6.1e39.9ce8 transição de estado DOT11: S_DOT11_INIT -> S_DOT11_ASSOCIATED

09/2025/09 15:21:48.618855282 {wncd_x_R0-0}{1}: [client-orch-sm] [17842]: (depurar): MAC: A associação f0b6.1e39.9ce8 Estação Dot11 foi bem-sucedida.

Autenticação da camada 2 ignorada:

09/2025/09 15:21:48.618992721 {wncd_x_R0-0}{1}: [client-orch-sm] [17842]: (depurar): MAC:

f0b6.1e39.9ce8 Iniciando a autenticação L2. Bssid na máquina de estado:c418.fc82.bb0b Bssid na solicitação é:c418.fc82.bb0b

09/2025/09 15:21:48.619006036 {wncd_x_R0-0}{1}: [client-orch-state] [17842]: (nota): MAC: f0b6.1e39.9ce8 Transição de estado do cliente: S_CO_ASSOCIATING -> S_CO_L2_AUTH_IN_PROGRESS

09/2025/09 15:21:48.619093387 {wncd_x_R0-0}{1}: [client-auth] [17842]: (nota): MAC: f0b6.1e39.9ce8 Autenticação L2 iniciada. método WEBAUTH, Política VLAN 0, substituição de AAA = 0

[...]

09/2025/09 15:21:48.623839337 {wncd_x_R0-0}{1}: [client-auth] [17842]: (informações): MAC: f0b6.1e39.9ce8 Transição de estado da interface de autenticação do cliente: S_AUTHIF_L2_WEBAUTH_PENDING -> S_AUTHIF_L2_WEBAUTH_DONE

09/2025/09 15:21:48.623863687 {wncd_x_R0-0}{1}: [auth-mgr] [17842]: (informações): [f0b6.1e39.9ce8:capwap_90000008] O tipo de dispositivo para a sessão é detectado como Dispositivo Intel e o nome antigo do Dispositivo Intel e do Dispositivo para a sessão é detectado como INTEL CORPORATE e o antigo mapa de protocolo INTEL CORPORATE e o antigo mapa de protocolo 1 e o novo é 1

09/2025/09 15:21:48.623873529 {wncd_x_R0-0}{1}: [auth-mgr] [17842]: (informações): [f0b6.1e39.9ce8:capwap_90000008] a notificação de adição/alteração de attr do auth mgr é recebida para attr dc-profile-name(1130)

09/2025/09 15:21:48.623911035 {wncd_x_R0-0}{1}: [client-orch-sm] [17842]: (depurar): MAC: f0b6.1e39.9ce8 L2 A autenticação da estação foi bem-sucedida., L3 Autenticação: 1

Placa ACL:

09/2025/09 15:21:48.620896754 {wncd_x_R0-0}{1}: [webauth-sm] [17842]: (informações): [0.0.0.0]Starting Webauth, mac [f0:b6:1e:39:9c:e8],IIF 0 , ID de auditoria D1257C0A000000CA2D54F867

09/2025/09 15:21:48.620927053 {wncd_x_R0-0}{1}: [webauth-state] [17842]: (informações): [f0b6.1e39.9ce8][0.0.0.0]Mapa de parâmetros usado: global

09/2025/09 15:21:48.620935005 {wncd_x_R0-0}{1}: [webauth-state] [17842]: (informações): [f0b6.1e39.9ce8][0.0.0.0]Estado Inválido Estado -> INIT

09/2025/09 15:21:48.620942683 {wncd_x_R0-0}{1}: [webauth-sess] [17842]: (informações): capwap_90000008[f0b6.1e39.9ce8][0.0.0.0]Criar sessão, Adicionar endereço 0.0.0.0

09/2025/09 15:21:48.620946808 {wncd_x_R0-0}{1}: [auth-mgr-feat_wireless] [17842]: (informações): [0000.0000.0000:desconhecido] ID da zona 0x0 recuperada para 12364632846638254486 bssid

09/2025/09 15:21:48.620958619 {wncd_x_R0-0}{1}: [webauth-state] [17842]: (informações): capwap_90000008[f0b6.1e39.9ce8][0.0.0.0]Param-map usado: FlexEWA=WebAuth-141

09/2025/09 15:21:48.620962048 {wncd_x_R0-0}{1}: [webauth-state] [17842]: (informações): capwap_90000008[f0b6.1e39.9ce8][0.0.0.0]State INIT -> INIT

09/2025/09 15:21:48.620978097 {wncd_x_R0-0}{1}: [webauth-sm] [17842]: (informações): capwap_90000008[f0b6.1e39.9ce8][0.0.0.0]Iniciar sessão, encaminhar estado para 0 IF 0x90000008 mac [f0b6.1e39.9ce8]

09/2025/09 15:21:48.620981018 {wncd_x_R0-0}{1}: [webauth-sm] [17842]: (informações): capwap_90000008[f0b6.1e39.9ce8][0.0.0.0]Iniciar sessão, Sessões SM init 5

09/2025/09 15:21:48.620988217 {wncd_x_R0-0}{1}: [webauth-state] [17842]: (informações): capwap_90000008[f0b6.1e39.9ce8][0.0.0.0]Param-map usado: FlexEWA=WebAuth-141

09/2025/09 15:21:48.620991618 {wncd_x_R0-0}{1}: [webauth-state] [17842]: (informações): capwap_90000008[f0b6.1e39.9ce8][0.0.0.0]State INIT -> INIT

09/2025/09 15:21:48.621023019 {wncd_x_R0-0}{1}: [webauth-acl] [17842]: (informações): capwap_90000008[f0b6.1e39.9ce8][0.0.0.0]Aplicando ACL de interceptação IPv4 via SVM, nome: WA-v4-int-10.124.41.141-7, prioridade: 50, IIF-ID: 0

09/2025/09 15:21:48.621032776 {wncd_x_R0-0}{1}: [svm] [17842]: (informações): SVM_INFO: Aplicando Svc Templ WA-v4-int-10.124.41.141-7 (ML:NONE)

09/2025/09 15:21:48.621786262 {wncd_x_R0-0}{1}: [epm] [17842]: (informações): [f0b6.1e39.9ce8:capwap_90000008] O Recurso (PLUG-IN de URL do EPM) foi iniciado (status Êxito)

09/2025/09 15:21:48.621804034 {wncd_x_R0-0}{1}: [epm-acl] [17842]: (informações): [f0b6.1e39.9ce8:capwap_90000008] Id Do Filtro: FlexEWA141-sec-ACL recebida

09/2025/09 15:21:48.622151544 {wncd_x_R0-0}{1}: [epm] [17842]: (informações): [f0b6.1e39.9ce8:capwap_90000008] O recurso (PLUG-IN de ACL do EPM) foi iniciado (status Êxito)

09/2025/09 15:21:48.622187815 {wncd_x_R0-0}{1}: [svm] [17842]: (informações): SVM_INFO: A resposta do epm é SYNC com o código de retorno Success

09/2025/09 15:21:48.622226011 {wncd_x_R0-0}{1}: [auth-mgr] [17842]: (informações): [f0b6.1e39.9ce8:capwap_90000008] Modelo de evento de elevação ativado (9) nesta sessão, cliente (desconhecido) (0)

09/2025/09 15:21:48.622265240 {wncd_x_R0-0}{1}: [webauth-acl] [17842]: (informações): capwap_90000008[f0b6.1e39.9ce8][0.0.0.0]Aplicando ACL de interceptação IPv6 via SVM, nome: IP-Adm-V6-Int-ACL-global-7, prioridade: 52, IIF-ID: 0

09/2025/09 15:21:48.622270327 {wncd_x_R0-0}{1}: [svm] [17842]: (informações): SVM_INFO: Aplicando Svc Templ IP-Adm-V6-Int-ACL-global-7 (ML:NONE)

09/2025/09 15:21:48.622898831 {wncd_x_R0-0}{1}: [epm] [17842]: (informações): [f0b6.1e39.9ce8:capwap_90000008] O Recurso (PLUG-IN de URL do EPM) foi iniciado (status Êxito)

09/2025/09 15:21:48.622932973 {wncd_x_R0-0}{1}: [svm] [17842]: (informações): SVM_INFO: A resposta do epm é SYNC com o código de retorno Success

09/2025/09 15:21:48.622957784 {wncd_x_R0-0}{1}: [auth-mgr] [17842]: (informações): [f0b6.1e39.9ce8:capwap_90000008] Modelo de evento de elevação ativado (9) nesta sessão, cliente (desconhecido) (0)

09/2025/09 15:21:48.623119047 {wncd_x_R0-0}{1}: [ponto11] [17842]: (depurar): MAC: f0b6.1e39.9ce8 Dot11 SAE encontra o progresso da ipsk como 0, não no estado pendente

09/2025/09 15:21:48.623126095 {wncd_x_R0-0}{1}: [llbridge-main] [17842]: (depurar): MAC: f0b6.1e39.9ce8 O Link-local Bridging não está ativado para este cliente, não verificando a validade da VLAN

09/2025/09 15:21:48.623205421 {wncd_x_R0-0}{1}: [auth-mgr] [17842]: (informações): [f0b6.1e39.9ce8:capwap_90000008] Contexto alterando estado de 'Ocioso' para 'Em Execução'

09/2025/09 15:21:48.623209350 {wncd_x_R0-0}{1}: [auth-mgr] [17842]: (informações): [f0b6.1e39.9ce8:capwap_90000008] Método webauth alterando estado de 'Não executado' para 'Em execução'

09/2025/09 15:21:48.623572855 {wncd_x_R0-0}{1}: [auth-mgr] [17842]: (informações):

[f0b6.1e39.9ce8:capwap_90000008] O SM não pode enviar o Modelo de evento Ativado para PRE para 0x8D000C0

09/2025/09 15:21:48.623680228 {wncd_x_R0-0}{1}: [client-auth] [17842]: (informações): MAC: f0b6.1e39.9ce8 Transição de estado da interface de autenticação do cliente: S_AUTHIF_AWAIT_L2_WEBAUTH_START_RESP -> S_AUTHIF_L2_WEBAUTH_PENDING

Processo de aprendizado de IP:

09/2025/09 15:21:51.628124695 {wncd_x_R0-0}{1}: [client-orch-state] [17842]: (nota): MAC: f0b6.1e39.9ce8 Transição de estado do cliente: S_CO_DPATH_PLUMB_IN_PROGRESS -> S_CO_IP_LEARN_IN_PROGRESS

09/2025/09 15:21:51.628463813 {wncd_x_R0-0}{1}: [cliente-aluno] [17842]: (informações): MAC: f0b6.1e39.9ce8 Transição de estado de aprendizagem IP: S_IPLEARN_INIT -> S_IPLEARN_IN_PROGRESS

09/2025/09 15:21:51.632284534 {wncd_x_R0-0}{1}: [client-auth] [17842]: (informações): MAC: f0b6.1e39.9ce8 Transição de estado da interface de autenticação do cliente: S_AUTHIF_L2_WEBAUTH_DONE -> S_AUTHIF_L2_WEBAUTH_DONE

09/2025/09 15:21:51.676501288 {wncd_x_R0-0}{1}: [pacote sisf] [17842]: (informações): RX: DHCP IPv6 de intf capwap_90000008 na vlan 174 Src MAC: f0b6.1e39.9ce8 Dst MAC: 333.0001.0002 Ipv6 SRC: fe80::3f83:2848:d30:7aea, Ipv6 Horário de Verão: ff02::1:2, digite: tipo de mensagem: DHCPV6_MSG_SOLICIT xid: 14443573

09/2025/09 15:21:51.676541447 {wncd_x_R0-0}{1}: [pacote sisf] [17842]: (informações): TX: DHCP IPv6 de intf capwap_90000008 na vlan 174 Src MAC: f0b6.1e39.9ce8 Dst MAC: 333.0001.0002 Ipv6 SRC: fe80::3f83:2848:d30:7aea, Ipv6 Horário de Verão: ff02::1:2, digite: tipo de mensagem: DHCPV6_MSG_SOLICIT xid: 14443573

09/2025/09 15:21:51.706187097 {wncd_x_R0-0}{1}: [pacote sisf] [17842]: (informações): RX: ARP da interface capwap_90000008 no MAC de origem da vlan 174: f0b6.1e39.9ce8 MAC de Destino: ffff.ffff.ffff SOLICITAÇÃO ARP, MAC do remetente ARP: f0b6.1e39.9ce8 MAC de destino ARP: 0000.0000.0000 IP do remetente ARP: 169.254.137.222, IP de destino ARP: 169.254.137.222, [...]

09/2025/09 15:21:52.686190945 {wncd_x_R0-0}{1}: [cliente-aluno] [17842]: (nota): MAC: f0b6.1e39.9ce8 Aprendizado do IP do cliente bem-sucedido. Método: IP DHCP: 10.124.37.251

09/2025/09 15:21:52.686244192 {wncd_x_R0-0}{1}: [auth-mgr] [17842]: (informações): [f0b6.1e39.9ce8:capwap_90000008] notificação de adição/alteração de attr de auth mgr recebida para attr addr(8)

09/2025/09 15:21:52.686285422 {wncd_x_R0-0}{1}: [webauth-sess] [17842]: (informações): capwap_90000008[f0b6.1e39.9ce8][0.0.0.0]Altere notif CB, Adicione o endereço 10.124.37.251 [f0b6.1e39.9ce8]

09/2025/09 15:21:52.686289265 {wncd_x_R0-0}{1}: [auth-mgr-feat_wireless] [17842]: (informações): [0000.0000.0000:desconhecido] ID da zona 0x0 recuperada para 12364632846638254486 bssid

09/2025/09 15:21:52.686291647 {wncd_x_R0-0}{1}: [webauth-sess] [17842]: (informações): adicionando sessão de webauth à tabela de hash ipv4 para id 0 de vrf, id 0 da tabela vrf ipv4

09/2025/09 15:21:52.686430038 {wncd_x_R0-0}{1}: [auth-mgr-feat_acct] [17842]: (informações): [f0b6.1e39.9ce8:capwap_90000008] SM Atributo notificado Adicionar/Atualizar endereço 10.124.37.251

09/2025/09 15:21:52.686456653 {wncd_x_R0-0}{1}: [epm] [17842]: (informações):
[0000.0000.0000:desconhecido] HDL = 0x0 vlan 174 contagem de falhas 0 dirty_counter 0 is_dirty
0

09/2025/09 15:21:52.686710209 {wncd_x_R0-0}{1}: [cliente-aluno] [17842]: (informações): MAC:
f0b6.1e39.9ce8 Transição de estado de aprendizagem IP: S_IPLEARN_IN_PROGRESS ->
S_IPLEARN_COMPLETE

Processo de autenticação e redirecionamento da camada 3:

09/2025/09 15:21:52.687395906 {wncd_x_R0-0}{1}: [client-auth] [17842]: (nota): MAC:
f0b6.1e39.9ce8 Autenticação L3 iniciada. LWA

09/2025/09 15:21:52.687472722 {wncd_x_R0-0}{1}: [client-auth] [17842]: (informações): MAC:
f0b6.1e39.9ce8 Transição de estado da interface de autenticação do cliente:
S_AUTHIF_L2_WEBAUTH_DONE -> S_AUTHIF_WEBAUTH_PENDING

09/2025/09 15:21:52.687723489 {wncd_x_R0-0}{1}: [pacote sisf] [17842]: (informações): RX:
DHCPv4 da interface Po1 na VLAN 174 Src MAC: 4006.d589.4e78 Dst MAC: ffff.ffff.ffff src_ip:
10.124.37.242, dst_ip: 255.255.255.255, BOOTPREPLY, SIFS_DHCPACK, giaddr: 0.0.0.0,
yiaddr: 10.124.37.251, CMAC: f0b6.1e39.9ce8

09/2025/09 15:21:52.687992316 {wncd_x_R0-0}{1}: [pacote sisf] [17842]: (informações): TX:
DHCPv4 da interface Po1 na VLAN 174 Src MAC: 4006.d589.4e78 Dst MAC: f0b6.1e39.9ce8
src_ip: 10.124.37.242, dst_ip: 255.255.255.255, BOOTPREPLY, SIFS_DHCPACK, giaddr: 0.0.0.0,
yiaddr: 10.124.37.251, CMAC: f0b6.1e39.9ce8

09/2025/09 15:21:52.688020475 {wncd_x_R0-0}{1}: [ewlc-infra-evq] [17842]: (detalhado):
Digite:EWLC_CAPWAP_HDR_AP, Id:23277
[...]

09/2025/09 15:21:55.663715832 {wncd_x_R0-0}{1}: [webauth-io] [17842]: (informações):
capwap_90000008[f0b6.1e39.9ce8][10.124.37.251]54129/197 Estado de ES NOVO -> LEITURA

09/2025/09 15:21:55.664060604 {wncd_x_R0-0}{1}: [webauth-io] [17842]: (informações):
capwap_90000008[f0b6.1e39.9ce8][10.124.37.251]54129/197 Ler evento, Mensagem pronta

09/2025/09 15:21:55.664071121 {wncd_x_R0-0}{1}: [webauth-httpd] [17842]: (informações):
capwap_90000008[f0b6.1e39.9ce8][10.124.37.251]GET rcvd quando no estado INIT

09/2025/09 15:21:55.664077798 {wncd_x_R0-0}{1}: [webauth-httpd] [17842]: (informações):
capwap_90000008[f0b6.1e39.9ce8][10.124.37.251]HTTP GET request

09/2025/09 15:21:55.664094019 {wncd_x_R0-0}{1}: [webauth-httpd] [17842]: (informações):
capwap_90000008[f0b6.1e39.9ce8][10.124.37.251]Analisar GET, src [10.124.37.251] dst
[23.5.165.82] url [<http://www.msftconnecttest.com/connecttest.txt>]

[...]

09/2025/09 15:22:16.420792303 {wncd_x_R0-0}{1}: [webauth-httpd] [17842]: (informações):
capwap_90000008[f0b6.1e39.9ce8][10.124.37.251]POST recebido quando em estado LOGIN

09/2025/09 15:22:32.375197748 {wncd_x_R0-0}{1}: [webauth-acl] [17842]: (informações):
capwap_90000008[f0b6.1e39.9ce8][10.124.37.251]Desaplique a ACL IPv4, exceto pela SVM,
nome "WA-v4-int-10.124.41.141-7", pri 50, IIF 0

09/2025/09 15:22:32.376230716 {wncd_x_R0-0}{1}: [auth-mgr] [17842]: (informações):
[f0b6.1e39.9ce8:capwap_90000008] Modelo de ramal de saída desativado (11) nesta sessão,

cliente (desconhecido) (0)

09/2025/09 15:22:32.376262689 {wncd_x_R0-0}{1}: [webauth-acl] [17842]: (informações):
capwap_90000008[f0b6.1e39.9ce8][10.124.37.251]Não aplicar a ACL de exceção IPv6 via SVM,
nome "IP-Adm-V6-Int-ACL-global", pri 52, IIF 0

09/2025/09 15:22:32.376734374 {wncd_x_R0-0}{1}: [auth-mgr] [17842]: (informações):
[f0b6.1e39.9ce8:capwap_90000008] Modelo de ramal de saída desativado (11) nesta sessão,
cliente (desconhecido) (0)

09/2025/09 15:22:32.376865998 {wncd_x_R0-0}{1}: [ponto11] [17842]: (depurar): MAC:
f0b6.1e39.9ce8 Dot11 SAE encontra o progresso da ipsk como 0, não no estado pendente

09/2025/09 15:22:32.376870611 {wncd_x_R0-0}{1}: [llbridge-main] [17842]: (depurar): MAC:
f0b6.1e39.9ce8 O Link-local Bridging não está ativado para este cliente, não verificando a
validade da VLAN

09/2025/09 15:22:32.376949875 {wncd_x_R0-0}{1}: [auth-mgr] [17842]: (informações):
[f0b6.1e39.9ce8:capwap_90000008] Êxito na autenticação a partir do WebAuth, êxito no evento
de autenticação

Transição para o estado RUN:

09/2025/09 15:22:32.379351256 {wncd_x_R0-0}{1}: [client-auth] [17842]: (nota): MAC:
f0b6.1e39.9ce8 ADD MOBILE enviado. Sinalizadores de estado do cliente: 0x38 BSSID: MAC:
c418.fc82.bb0b capwap IFID: 0x90000008, Adicionar celulares enviados: 1

09/2025/09 15:22:32.379583842 {wncd_x_R0-0}{1}: [errmsg] [17842]: (informações):
%CLIENT_ORCH_LOG-6-CLIENT_ADDED_TO_RUN_STATE: R0/0: wcd: Entrada de nome de
usuário (demoadmin) unida com ssid (FLEXEWA) para dispositivo com MAC: f0b6.1e39.9ce8 no
canal (100)

09/2025/09 15:22:32.379671775 {wncd_x_R0-0}{1}: [aaa-attr-inf] [17842]: (informações): [Atributo
aplicado :bsn-vlan-interface-name 0 "wlc-management"]

09/2025/09 15:22:32.379673695 {wncd_x_R0-0}{1}: [aaa-attr-inf] [17842]: (informações): [Atributo
aplicado: timeout 0 28800 (0x7080)]

09/2025/09 15:22:32.379683417 {wncd_x_R0-0}{1}: [aaa-attr-inf] [17842]: (informações): [Atributo
aplicado: url-redirect-acl 0 "IP-Adm-V4-LOGOUT-ACL"]

09/2025/09 15:22:32.379727993 {wncd_x_R0-0}{1}: [ewlc-qos-client] [17842]: (informações):
MAC: f0b6.1e39.9ce8 QoS do cliente executam manipulador de estado

09/2025/09 15:22:32.379756610 {wncd_x_R0-0}{1}: [rog-proxy-capwap] [17842]: (depurar):
Notificação de estado de execução de cliente gerenciado: f0b6.1e39.9ce8

09/2025/09 15:22:32.379810670 {wncd_x_R0-0}{1}: [client-orch-state] [17842]: (nota): MAC:
f0b6.1e39.9ce8 Transição de estado do cliente: S_CO_L3_AUTH_IN_PROGRESS -> S_CO_RUN

Informações Relacionadas

- [Configurar e solucionar problemas de autenticação da Web externa no 9800 WLC](#)

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.