Configurar e solucionar problemas de autenticação da Web externa no 9800 WLC

Contents

Introdução

Este documento descreve como configurar e solucionar problemas de autenticação da Web externa (EWA) em um Catalyst 9800 Wireless LAN Controller (WLC).

Pré-requisitos

Este documento pressupõe que o servidor Web está configurado corretamente para permitir a comunicação externa e que a página Web está configurada corretamente para enviar todos os parâmetros necessários para que a WLC autentique o usuário e mova as sessões do cliente para o estado RUN.

Observação: como o acesso a recursos externos é restrito pela WLC através de permissões de lista de acesso, todos os scripts, fontes, imagens e assim por diante. que são usados na

página da Web precisam ser baixados e permanecer locais ao servidor da Web.

Os parâmetros necessários para autenticação de usuário são:

- buttonClicked: esse parâmetro precisa ser definido com o valor "4" para que o WLC detecte a ação como uma tentativa de autenticação.
- redirectUrl: O valor neste parâmetro é usado pelo controlador para direcionar o cliente para um site específico após a autenticação bem-sucedida.
- err_flag: Esse parâmetro é usado para indicar algum erro, como informações incompletas ou credenciais incorretas; em autenticações bem-sucedidas, ele é definido como "0".
- username: este parâmetro é usado somente para mapas de parâmetro webauth; se o mapa de parâmetro estiver definido como consentimento, ele poderá ser ignorado. Ele deve ser preenchido com o nome de usuário do cliente sem fio.
- senha: este parâmetro é usado somente para mapas de parâmetro webauth; se o mapa de parâmetro estiver definido como consentimento, ele poderá ser ignorado. Ele deve ser preenchido com a senha do cliente sem fio.

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Desenvolvimento para Web em HTML (Hyper Text Markup Language)
- Recursos sem fio do Cisco IOS®-XE
- Ferramentas para desenvolvedores de navegadores da Web

Componentes Utilizados

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

- C9800-CL WLC Cisco IOS®-XE versão 17.3.3
- Microsoft Windows Server 2012 com recursos de Serviços de Informações da Internet (IIS)
- Pontos de acesso 2802 e 9117

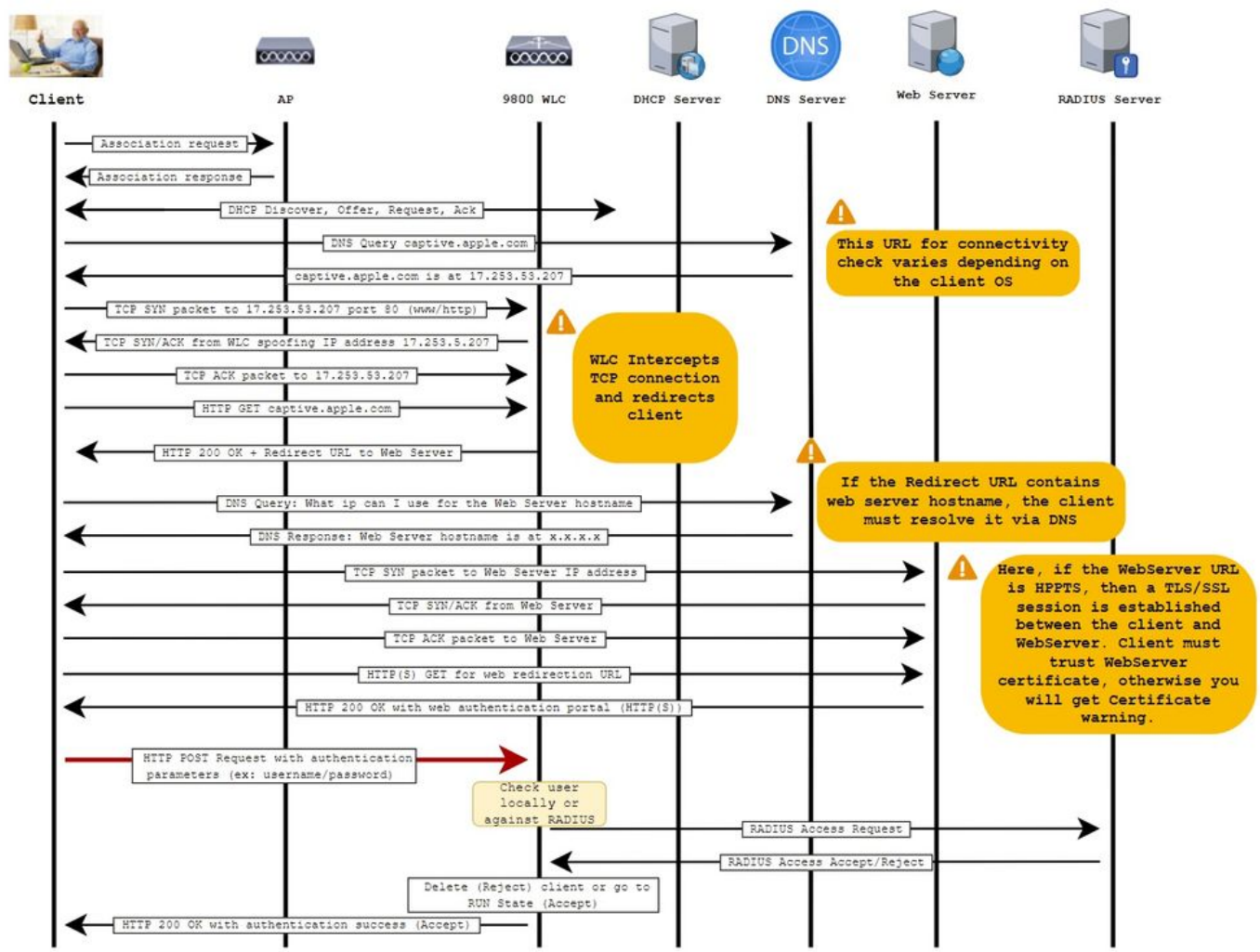
As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

A autenticação externa da Web aproveita um portal da Web hospedado fora da WLC em um servidor Web dedicado ou em servidores multifuncionais, como o Identity Services Engine (ISE), que permite o acesso granular e o gerenciamento de componentes da Web. O handshake envolvido para integrar com êxito um cliente a uma WLAN de autenticação da Web externa é renderizado na imagem. A imagem lista interações sequenciais entre cliente sem fio, WLC, servidor do Sistema de Nome de Domínio (DNS - Domain Name System) que resolve o Uniform

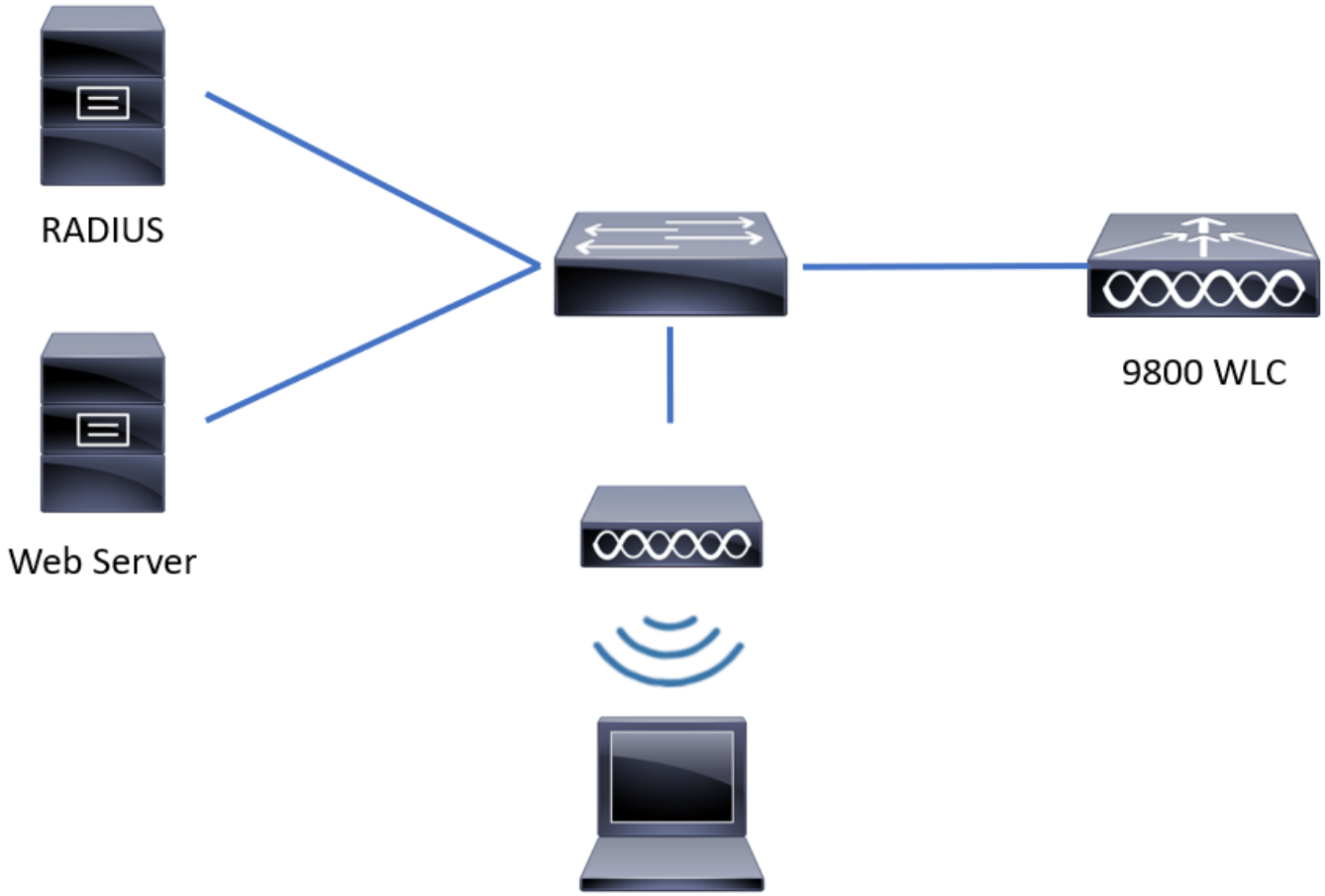
Resource Location (URL - Local de Recurso Uniforme) e servidor Web, onde o WLC valida as credenciais do usuário localmente. Esse fluxo de trabalho é útil para solucionar qualquer condição de falha.

Observação: antes da chamada POST HTTP do cliente para a WLC, se a autenticação da Web segura estiver habilitada no mapa de parâmetros e se a WLC não tiver um ponto confiável assinado por uma autoridade de certificação confiável, um alerta de segurança será exibido no navegador. O cliente precisa ignorar esse aviso e aceitar o reenvio do formulário para que o controlador coloque as sessões do cliente no estado RUN.



Configurar

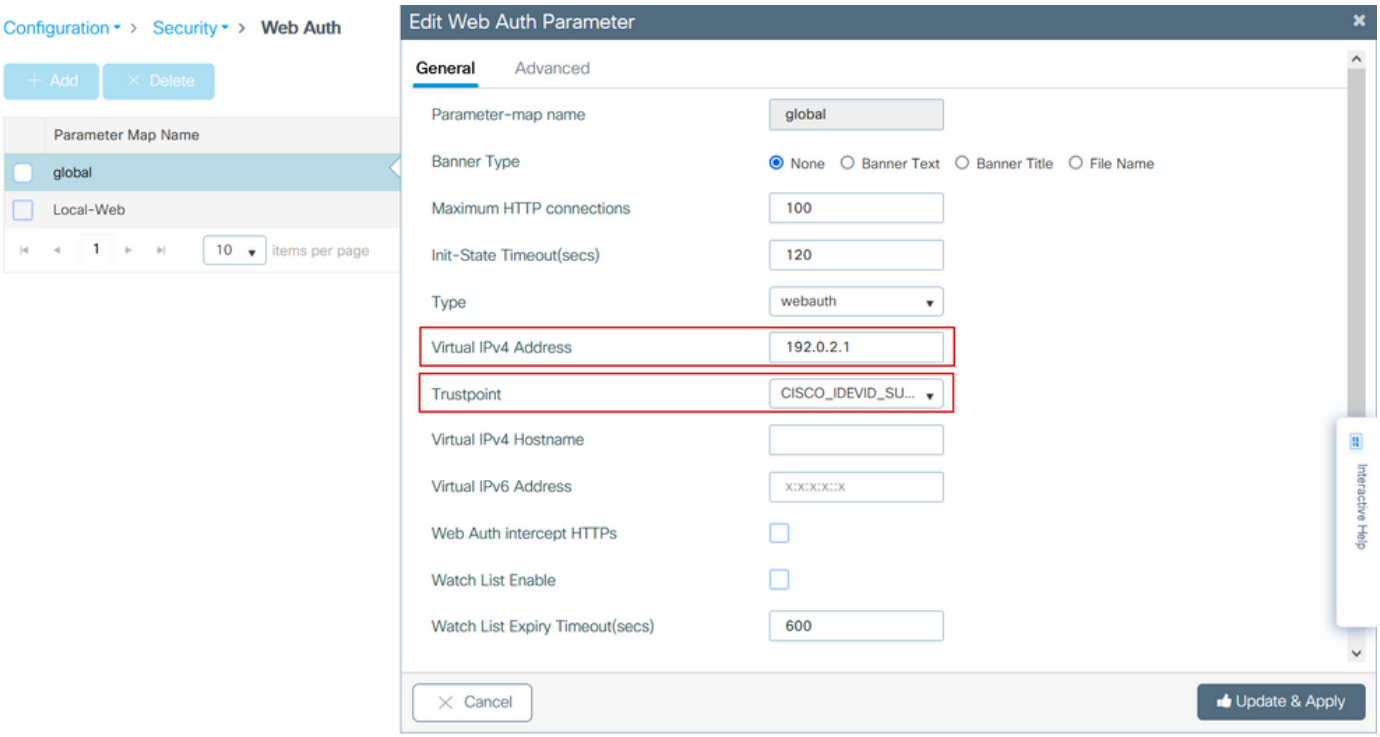
Diagrama de Rede



Definir Configurações de Parâmetros da Web

Etapa 1. Navegue para Configuration > Security > Web Auth e escolha o mapa de parâmetros globais. Verifique se o endereço IPv4 virtual e o ponto confiável estão configurados para fornecer recursos de redirecionamento apropriados.

Observação: por padrão, os navegadores usam um site HTTP para iniciar o processo de redirecionamento. Se o redirecionamento de HTTPS for necessário, será necessário verificar os HTTPs de interceptação de Web Auth; no entanto, essa configuração não é recomendada, pois aumenta o uso da CPU.

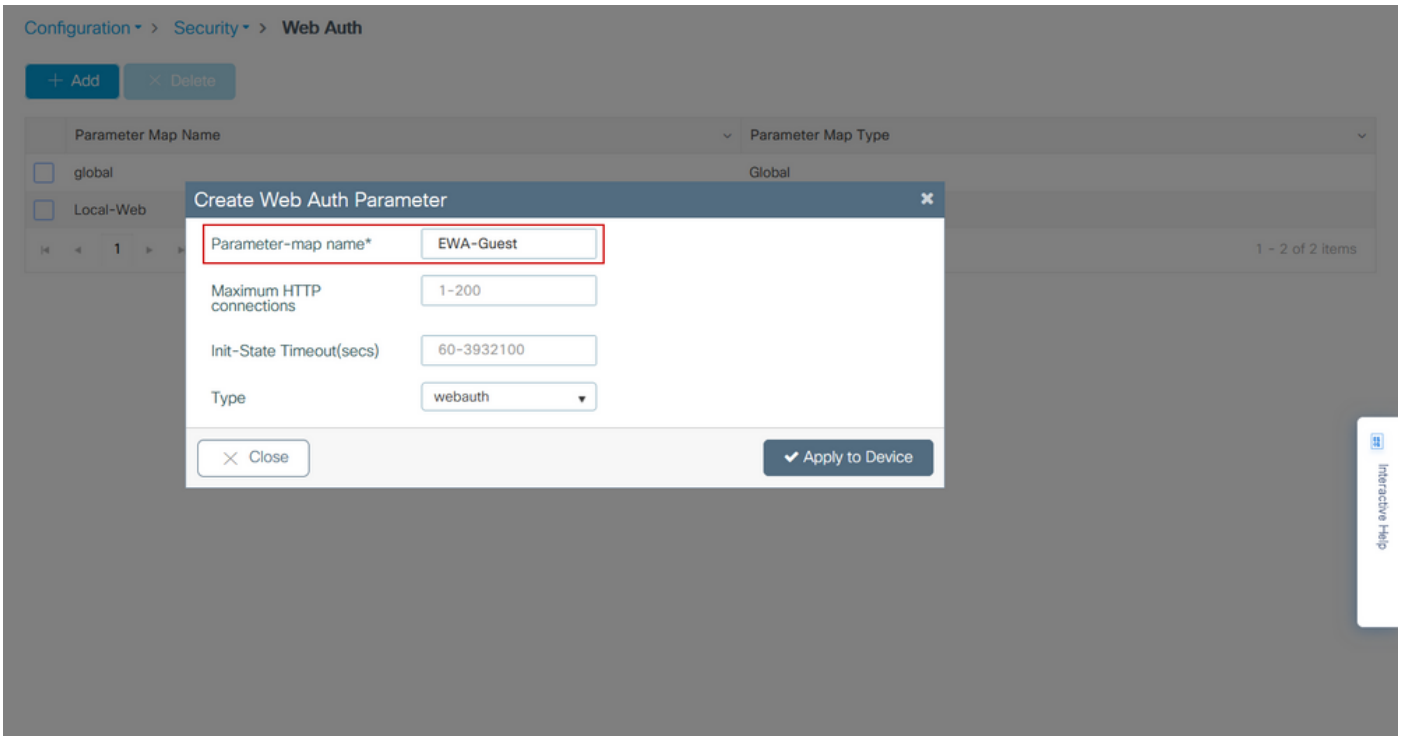


Configuração de CLI:

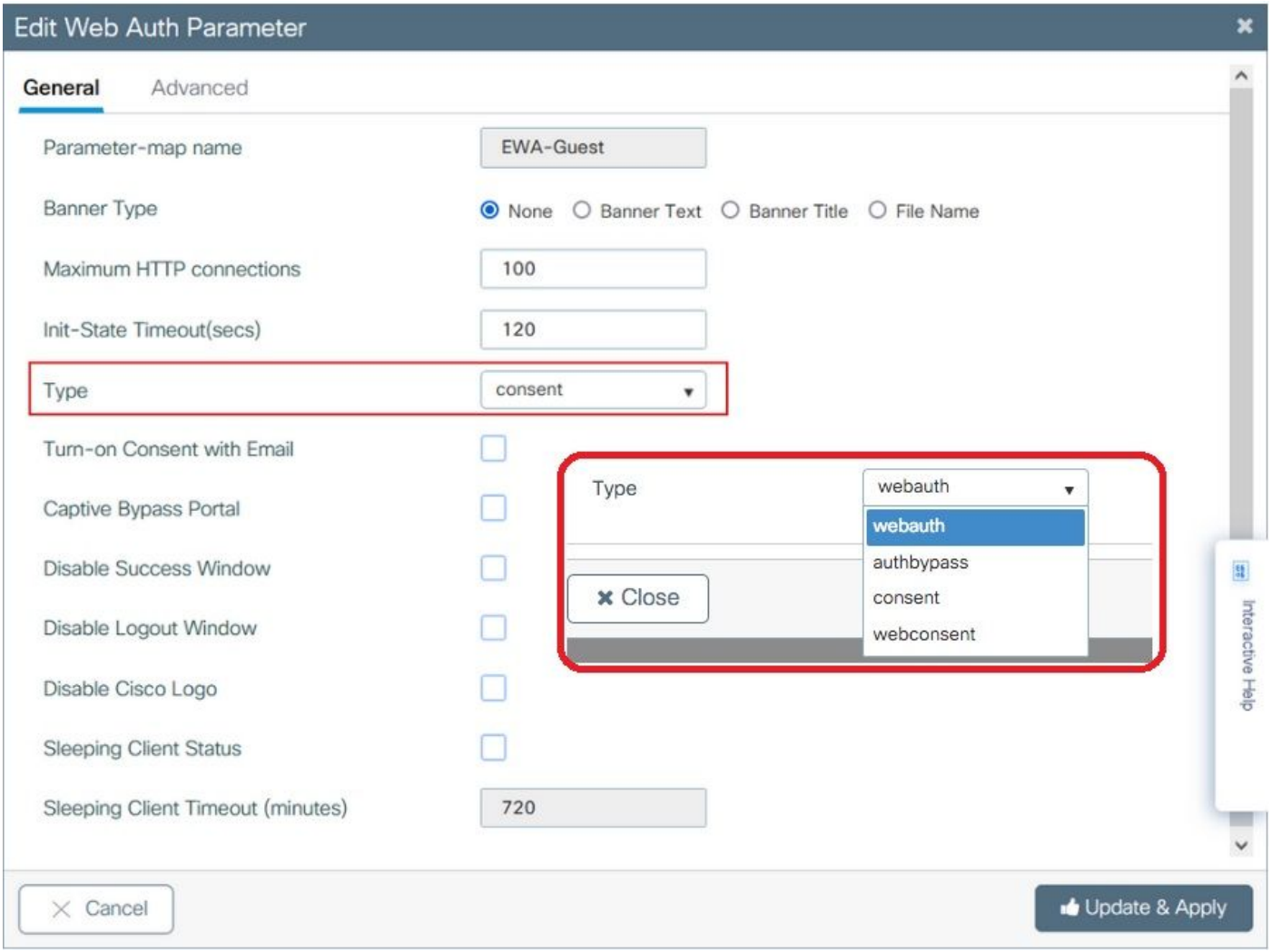
<#root>

```
9800#

configure terminal

9800(config)#

parameter-map type webauth global

9800(config-params-parameter-map)#

virtual-ip ipv4 192.0.2.1

9800(config-params-parameter-map)#

trustpoint CISCO_IDEVID_SUDI


9800(config-params-parameter-map)#

secure-webauth-disable


9800(config-params-parameter-map)#

webauth-http-enable
```

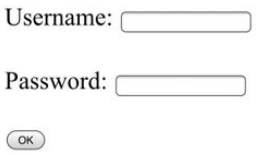
Etapa 2. Selecione + Adicionar e configure um nome para o novo mapa de parâmetros que aponte para o servidor externo. Opcionalmente, configure o número máximo de falhas de autenticação HTTP antes que o cliente seja excluído e o tempo (em segundos) que um cliente pode permanecer no estado de autenticação da Web.



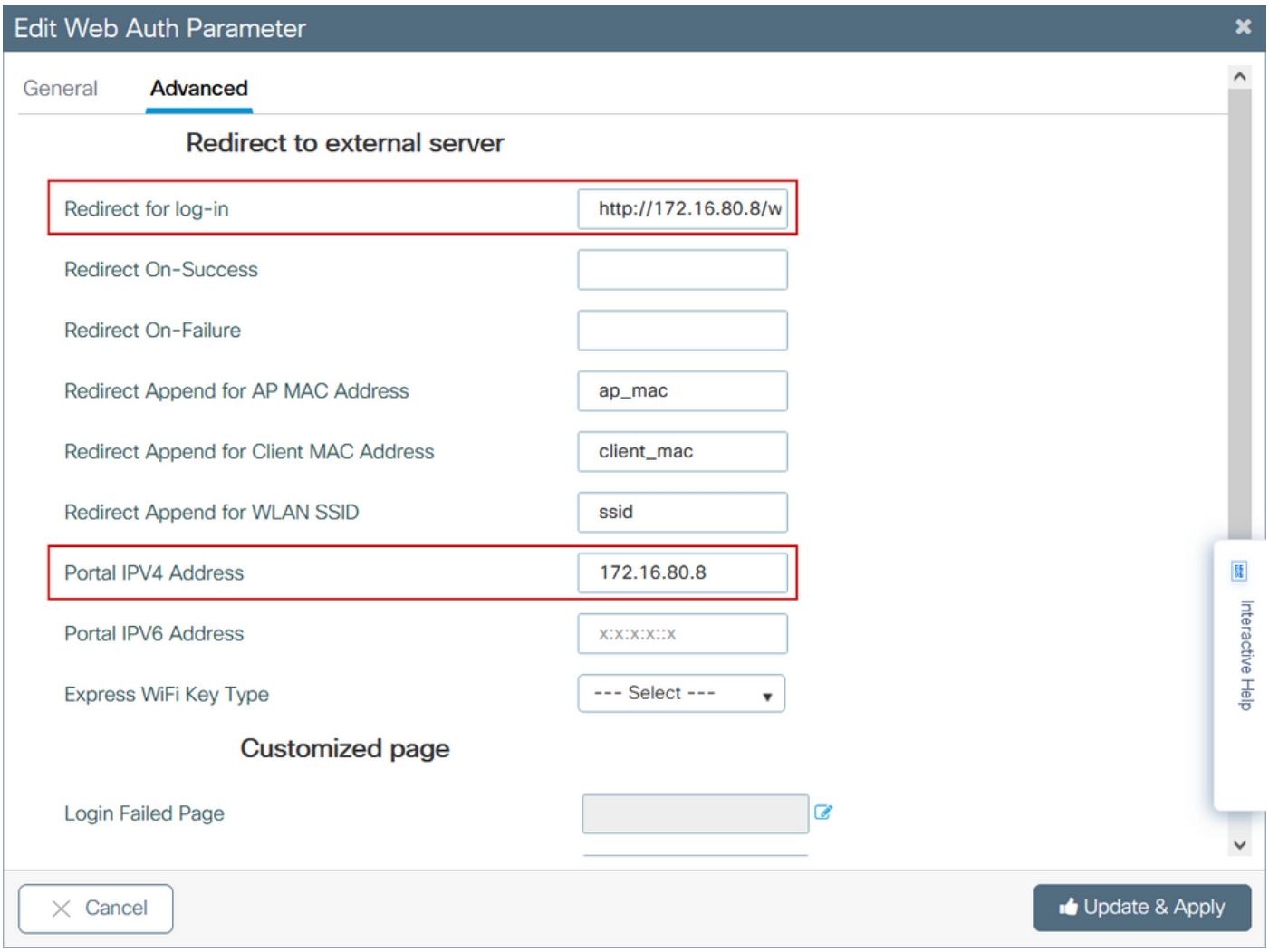
Etapa 3. Selecione o mapa de parâmetros recém-criado, na guia Geral configure o tipo de autenticação na lista suspensa Tipo.



- Nome do mapa de parâmetros = Nome atribuído ao mapa de parâmetros WebAuth
- Máximo de conexões HTTP = Número de falhas de autenticação antes que o cliente seja excluído
- Timeout de Estado de Inicialização (seg) = Segundos que um cliente pode ficar no status de autenticação da Web
- Tipo = Tipo de autenticação da Web

webauth	authbypass	consentimento	webconsent
	O cliente se conecta ao SSID e obtém um endereço IP, depois o WLC 9800 verifica se o endereço MAC tem permissão para entrar no rede, se sim, ela é movida para o estado EXECUTAR, se não for, é não tem permissão para ingressar. (Ele não se enquadra na autenticação da Web)		

Etapa 4. Na guia Advanced, configure o Redirect for login and Portal IPV4 Address com o URL e o endereço IP do site do servidor específicos, respectivamente.



Configuração da CLI para as Etapas 2, 3 e 4:

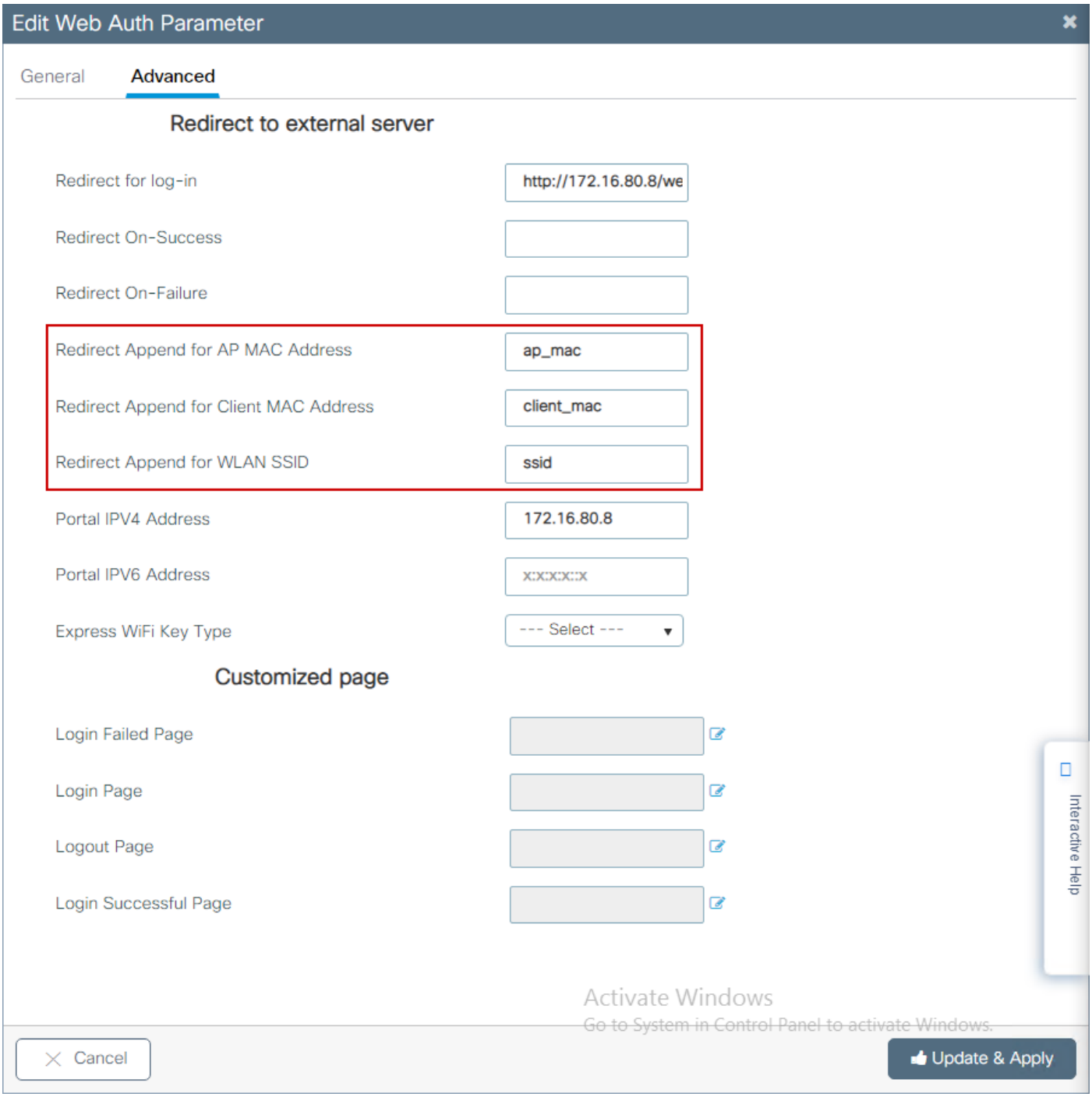
<#root>

```
9800(config)#

parameter-map type webauth EWA-Guest

9800(config-params-parameter-map)#

type consent

9800(config-params-parameter-map)#

redirect for-login http://172.16.80.8/webauth/login.html

9800(config-params-parameter-map)#

redirect portal ipv4 172.16.80.8
```

Etapa 5. (Opcional) A WLC pode enviar os parâmetros adicionais por meio da Sequência de caracteres de consulta. Geralmente, isso é necessário para tornar o 9800 compatível com portais externos de terceiros. Os campos "Redirect Append for AP MAC Address", "Redirect Append for Client MAC Address" e "Redirect Append for WLAN SSID" permitem que parâmetros adicionais

sejam acrescentados à ACL de redirecionamento com um nome personalizado. Selecione o mapa de parâmetros recém-criado e navegue até a guia Avançado, configure o nome para os parâmetros necessários. Os parâmetros disponíveis são:

- Endereço MAC do AP (no formato aa:bb:cc:dd:ee:ff)
- Endereço MAC do cliente (no formato aa:bb:cc:dd:ee:ff)
- Nome do SSID



Configuração de CLI:

<#root>

```
9800(config)#
```

```
parameter-map type webauth EWA-Guest

9800(config-params-parameter-map)#
redirect append ap-mac tag ap_mac

9800(config-params-parameter-map)#
redirect append wlan-ssid tag ssid

9800(config-params-parameter-map)#
redirect append client-mac tag client_mac
```

Para este exemplo, a URL de redirecionamento enviada ao cliente resulta em:

```
http://172.16.80.8/webauth/consent.html?switch_url=http://192.0.2.1/login.html&ap_mac=&ssid=&client_mac
```

Observação: quando você adiciona as informações do Endereço IPV4 do portal, ele adiciona automaticamente uma ACL que permite o tráfego HTTP e HTTPS dos clientes sem fio para o servidor de autenticação da Web externo, para que você não tenha que configurar nenhuma ACL de pré-autenticação extra. Caso você queira permitir vários endereços IP ou URLs, a única opção é configurar um filtro de URL para que qualquer IP correspondente a determinado URL seja permitido antes da autenticação. Não é possível adicionar estaticamente mais de um endereço IP de portal, a menos que você use filtros de URL.

Observação: o mapa de parâmetros global é o único no qual você pode definir endereços IPv4 e IPv6 virtuais, HTTPs de interceptação de Webauth, portal de desvio cativo, habilitar lista de controle e configurações de tempo limite de expiração da lista de controle.

Resumo da configuração da CLI:

Servidor Web local

```
parameter-map type webauth <web-parameter-map-name>
 type { webauth | authbypass | consent | webconsent }
 timeout init-state sec 300
 banner text ^Cbanner login^C
```

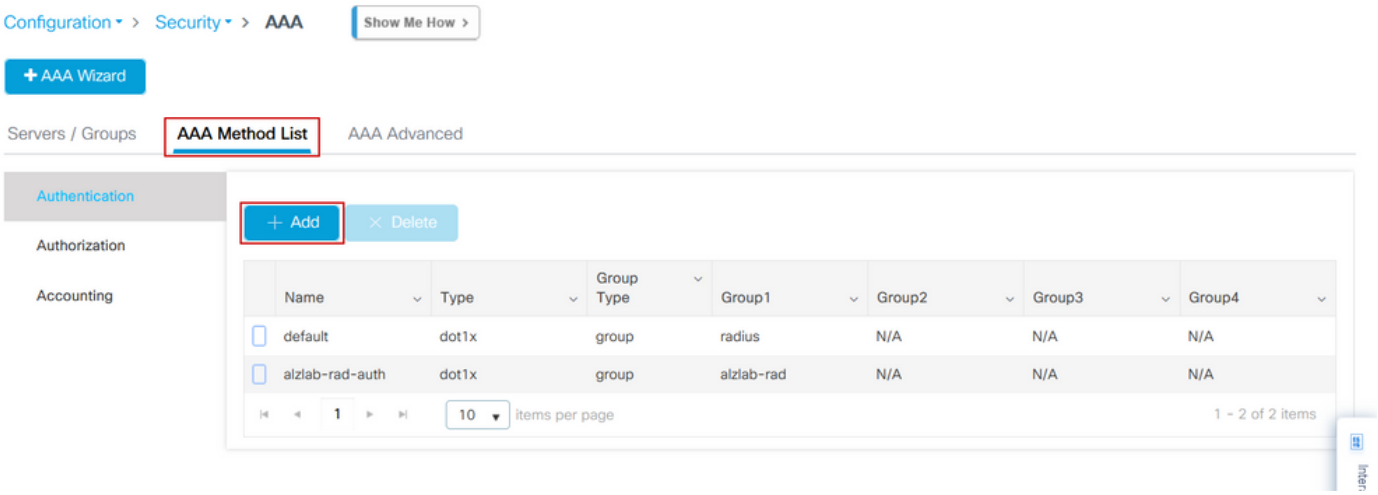
Servidor Web externo

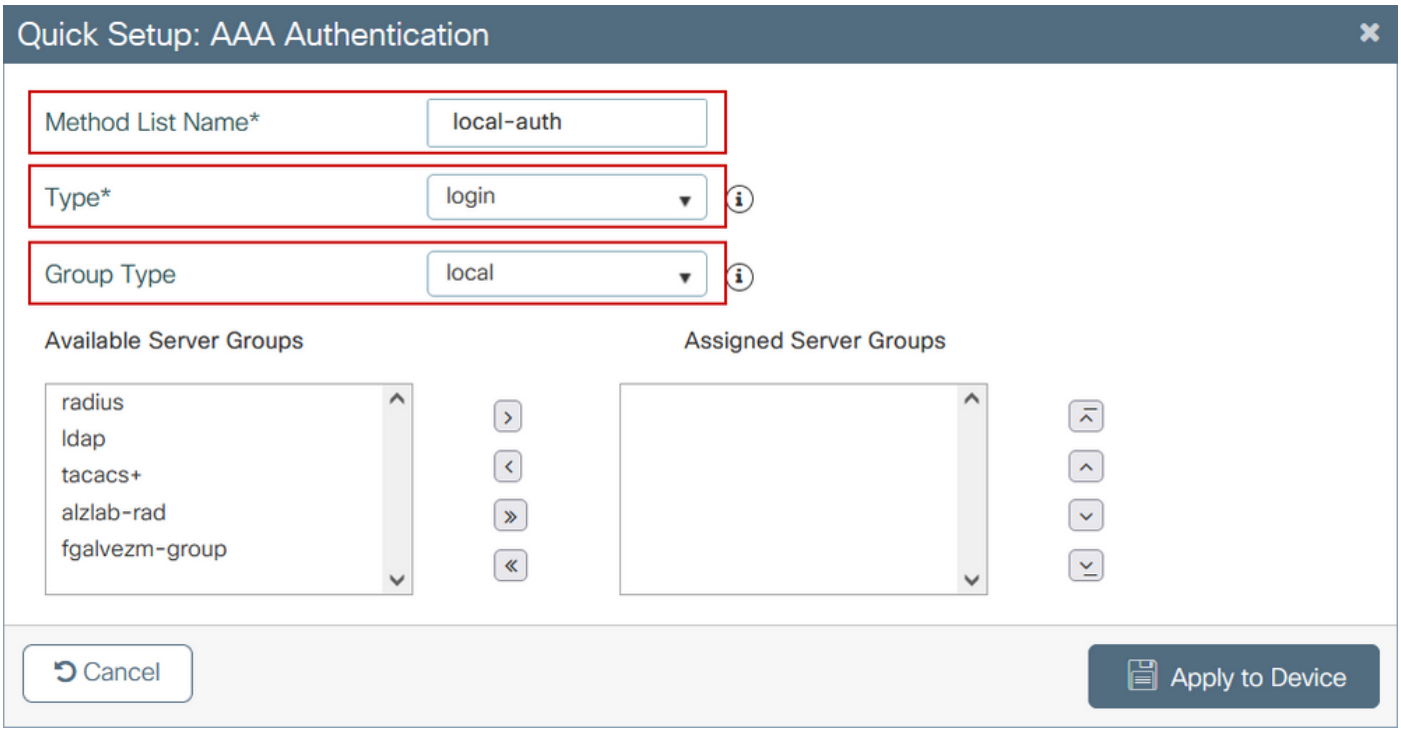
```
parameter-map type webauth <web-parameter-map-name>
 type webauth
 timeout init-state sec 300
 redirect for-login <URL-for-webauth>
 redirect portal ipv4 <external-server's-IP
 max-http-conns 10
```

Definir configurações de AAA

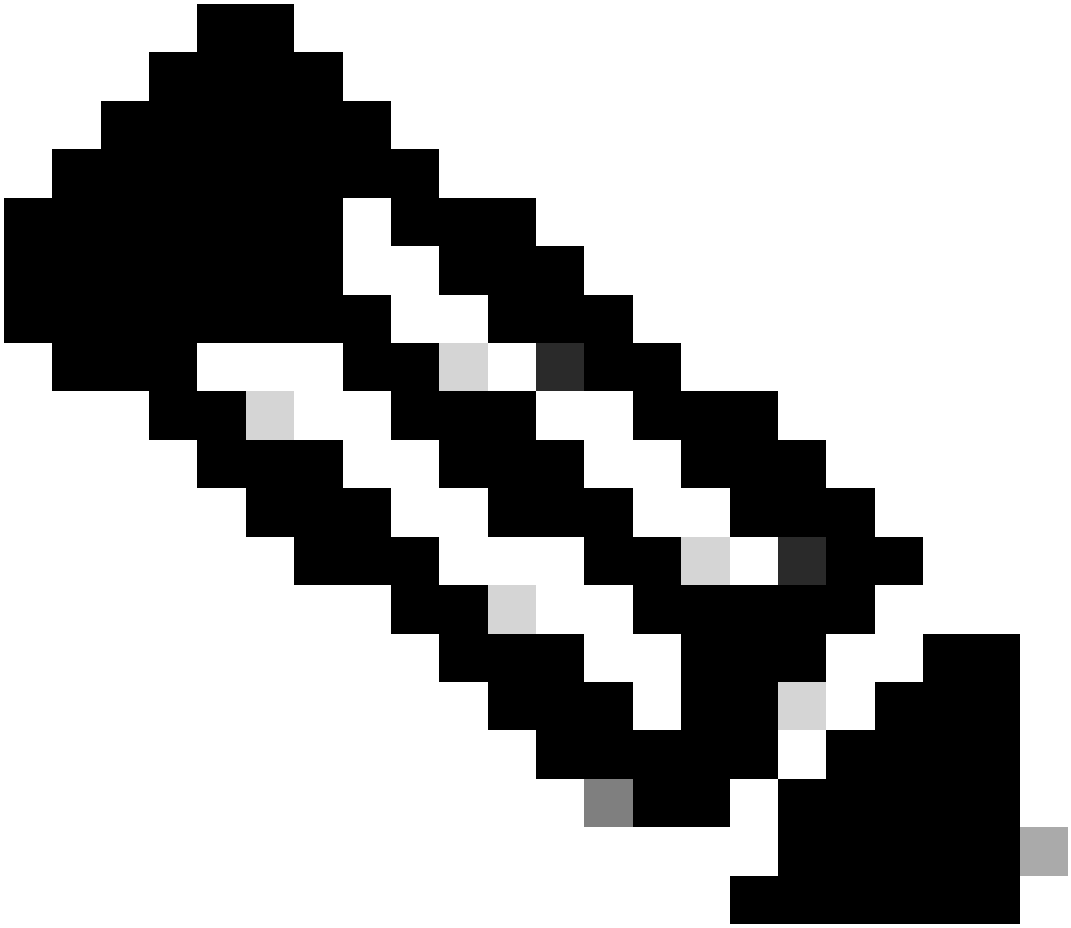
Esta seção de configuração só é necessária para mapas de parâmetros configurados para o tipo de autenticação webauth ou webconsent.

Etapa 1. Navegue para Configuration > Security > AAA e selecione AAA Method List. Configure uma nova lista de métodos, selecione + Adicionar e preencha os detalhes da lista; verifique se Tipo está definido como "login", como mostrado na imagem.

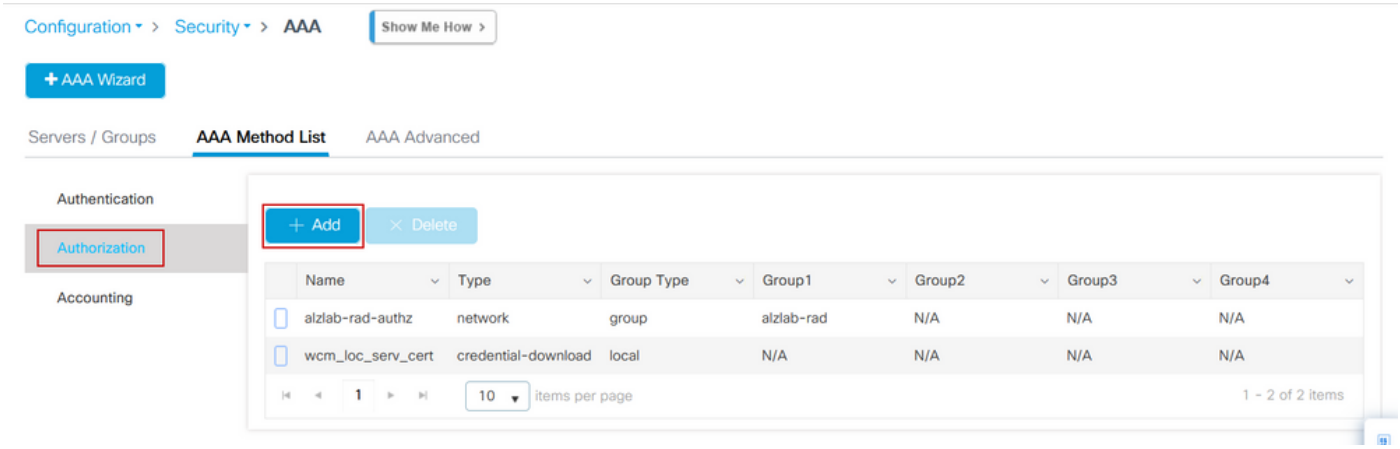


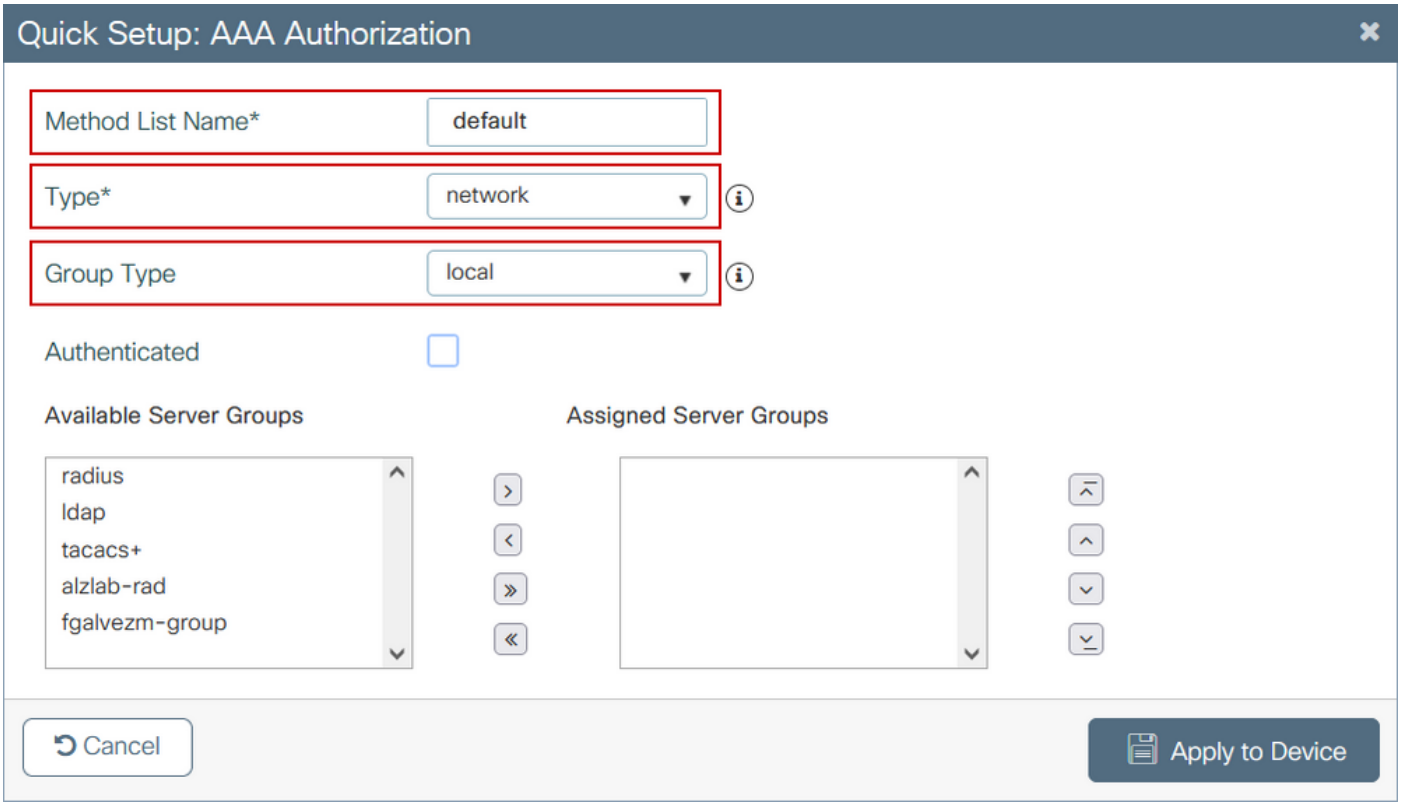


Etapa 2. Selecione Authorization e, em seguida, + Add para criar uma nova lista de métodos. Nomeie-o como padrão com Tipo como rede, conforme mostrado na imagem.



Observação: como é anunciado pelo controlador durante a configuração de segurança da camada 3 da WLAN: Para que a lista de métodos de logon local funcione, certifique-se de que a configuração 'aaa authorization network default local' exista no dispositivo. Isso significa que a lista de métodos de autorização com o nome default deve ser definida para configurar a autenticação da Web local corretamente. Nesta seção, esta lista de métodos de autorização específica é configurada.





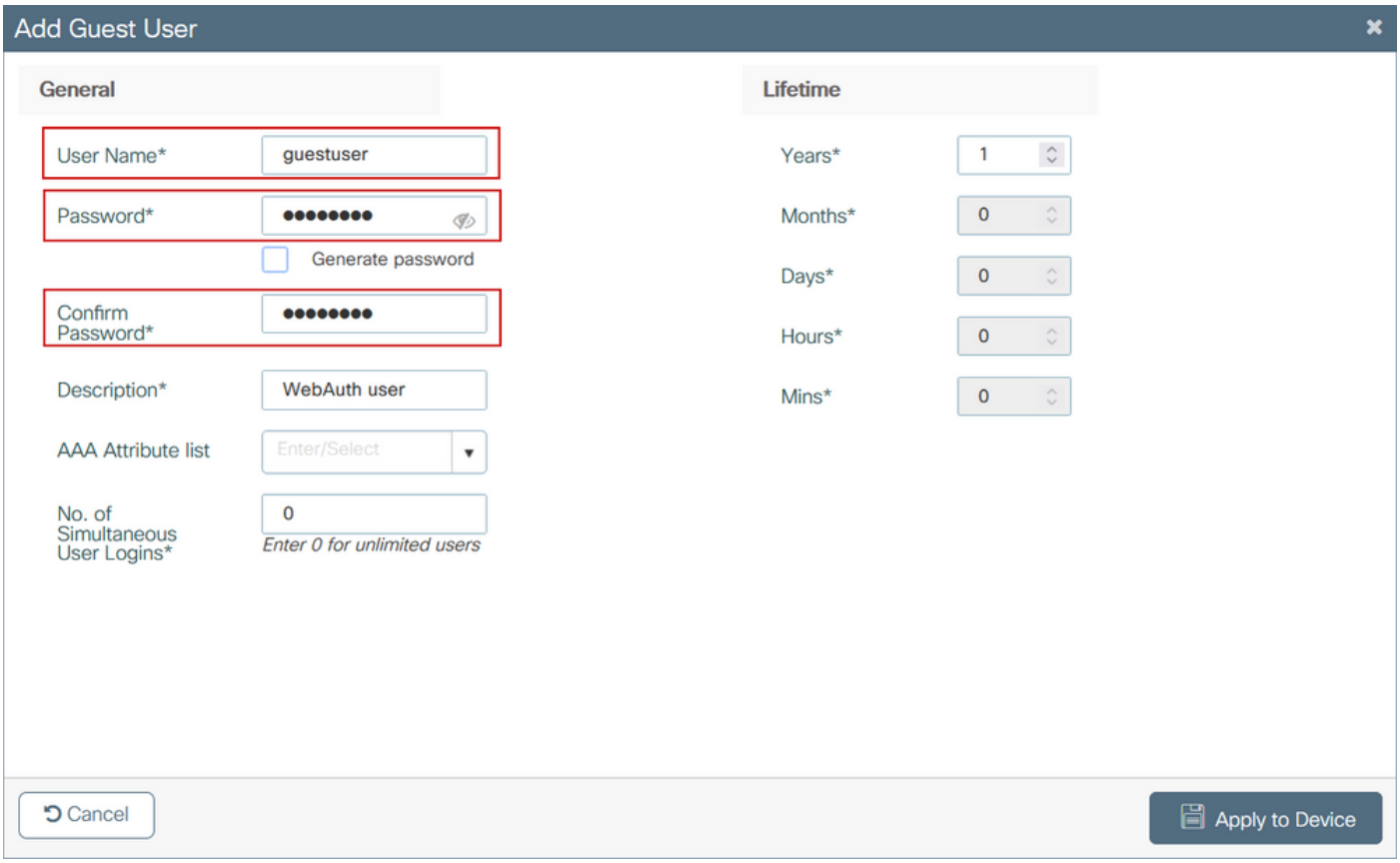
Configuração da CLI para as Etapas 1 e 2:

<#root>

```
9800(config)#
aaa new-model

9800(config)#
aaa authentication login local-auth local

9800(config)#
aaa authorization network default local
```

Observação: se a autenticação RADIUS externa for necessária, leia estas instruções relacionadas à configuração do servidor RADIUS em 9800 WLCs: AAA Config em 9800 WLC. Certifique-se de que a lista de métodos de autenticação tenha "login" definido como tipo em vez de dot1x.

Etapa 3. Navegue até Configuration > Security > Guest User. Selecione + Adicionar e configure os detalhes da conta de usuário convidado.



Configuração de CLI:

<#root>

```
9800(config)#

user-name guestuser

9800(config-user-name)#

description "WebAuth user"

9800(config-user-name)#

password 0 <password>

9800(config-user-name)#

type network-user description "WebAuth user" guest-user lifetime year 1
```

```
If permanent users are needed then use this command:
9800(config)#

username guestuserperm privilege 0 secret 0 <password>
```

Etapa 4. (Opcional) Na definição do mapa de parâmetros, algumas listas de controle de acesso (ACLs) são criadas automaticamente. Essas ACLs são usadas para definir qual tráfego dispara um redirecionamento para o servidor Web e qual tráfego tem permissão para passar. Se houver requisitos específicos, como vários endereços IP de servidor Web ou filtros de URL, navegue para Configuration > Security > ACL selecione + Add e defina as regras necessárias; as instruções permit são redirecionadas enquanto as instruções deny definem a passagem do tráfego.

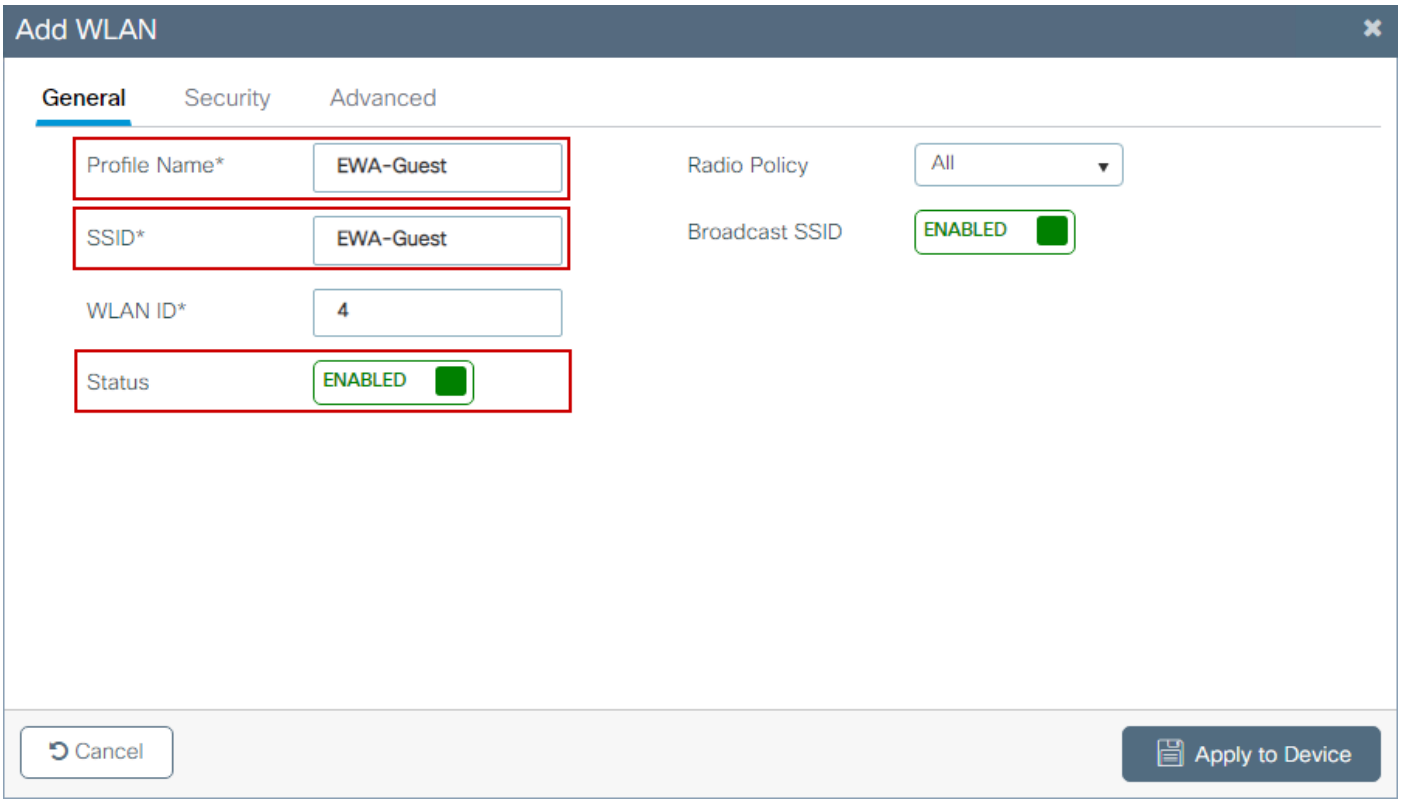
As regras de ACLs criadas automaticamente são:

<#root>

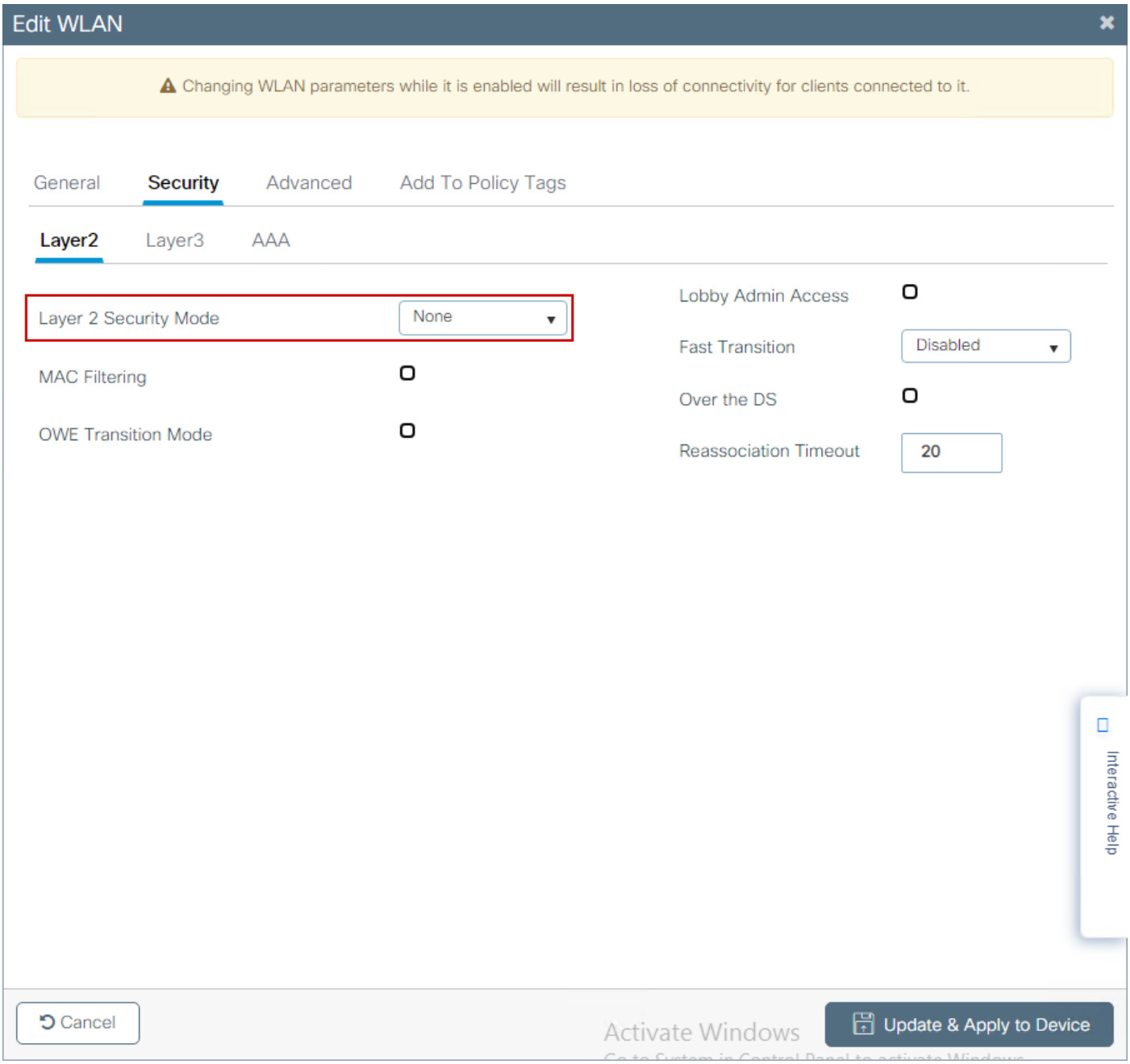
```
alz-9800#

show ip access-list


Extended IP access list WA-sec-172.16.80.8
10 permit tcp any host 172.16.80.8 eq www
20 permit tcp any host 172.16.80.8 eq 443
30 permit tcp host 172.16.80.8 eq www any
40 permit tcp host 172.16.80.8 eq 443 any
50 permit tcp any any eq domain
60 permit udp any any eq domain
70 permit udp any any eq bootpc
80 permit udp any any eq bootps
90 deny ip any any (1288 matches)
Extended IP access list WA-v4-int-172.16.80.8
10 deny tcp any host 172.16.80.8 eq www
20 deny tcp any host 172.16.80.8 eq 443
30 permit tcp any any eq www
40 permit tcp any host 192.0.2.1 eq 443
```

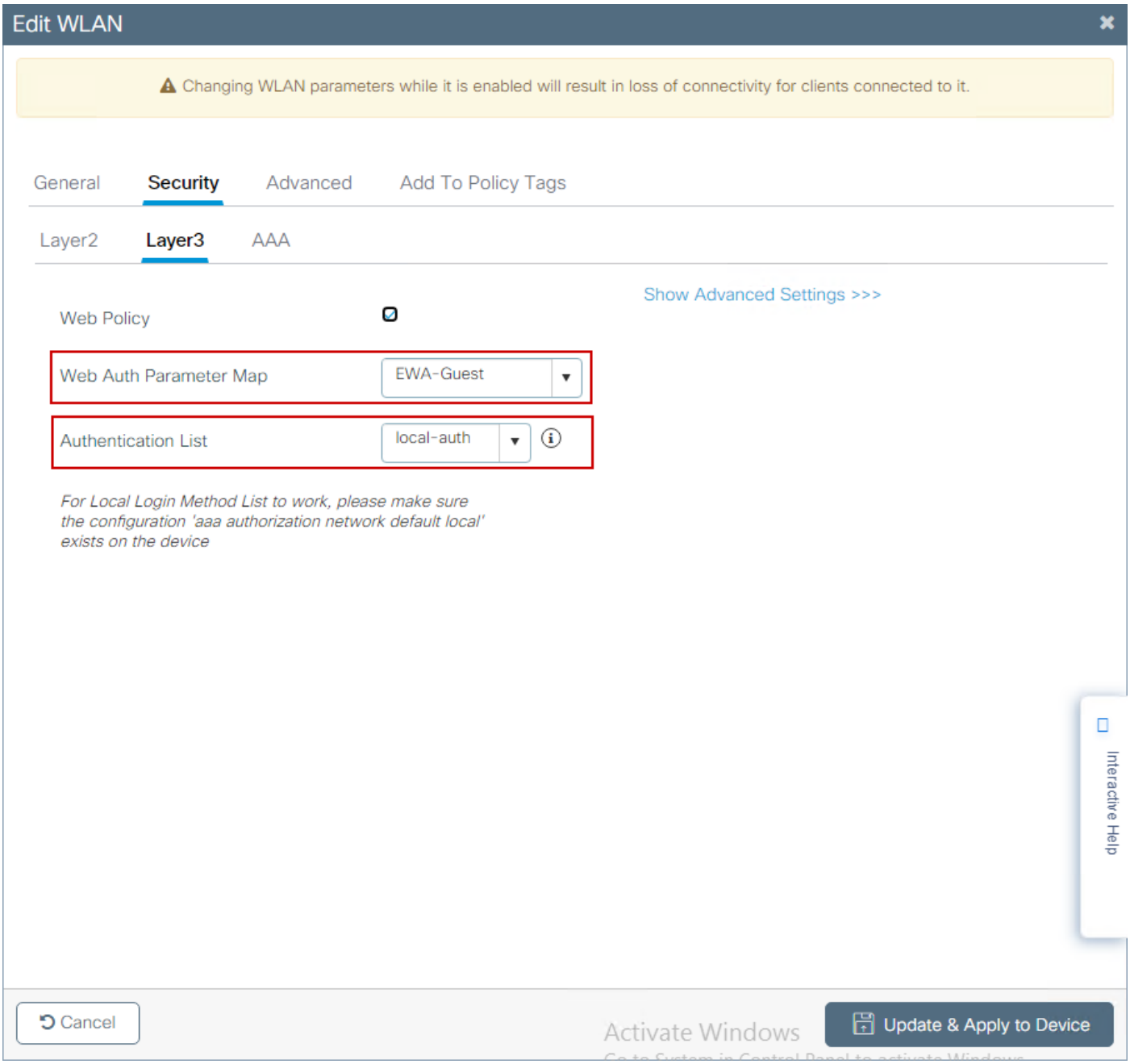
Configurar políticas e marcas

Etapa 1. Navegue até Configuration > Tags & Profiles > WLANs, selecione + Add para criar uma nova WLAN. Defina o perfil e o nome do SSID e o Status na guia Geral.



Etapa 2. Selecione a guia Security e defina a autenticação da camada 2 como None (Nenhuma) se não precisar de nenhum mecanismo de criptografia aérea. Na guia Layer 3 (Camada 3), marque a caixa Web Policy (Diretiva da Web), selecione o mapa de parâmetros no menu suspenso e escolha a lista de autenticação no menu suspenso. Opcionalmente, se uma ACL personalizada tiver sido definida anteriormente, selecione Show Advanced Settings e selecione a ACL apropriada no menu suspenso.


Edit WLAN
Changing WLAN parameters while it is enabled will result in loss of connectivity for clients connected to it.
General
Security
Advanced
Add To Policy Tags
Layer2
Layer3
AAA
Layer 2 Security Mode
None
MAC Filtering
OWE Transition Mode
Lobby Admin Access
Fast Transition
Disabled
Over the DS
Reassociation Timeout
20
Interactive Help
Cancel
Activate Windows
Update & Apply to Device



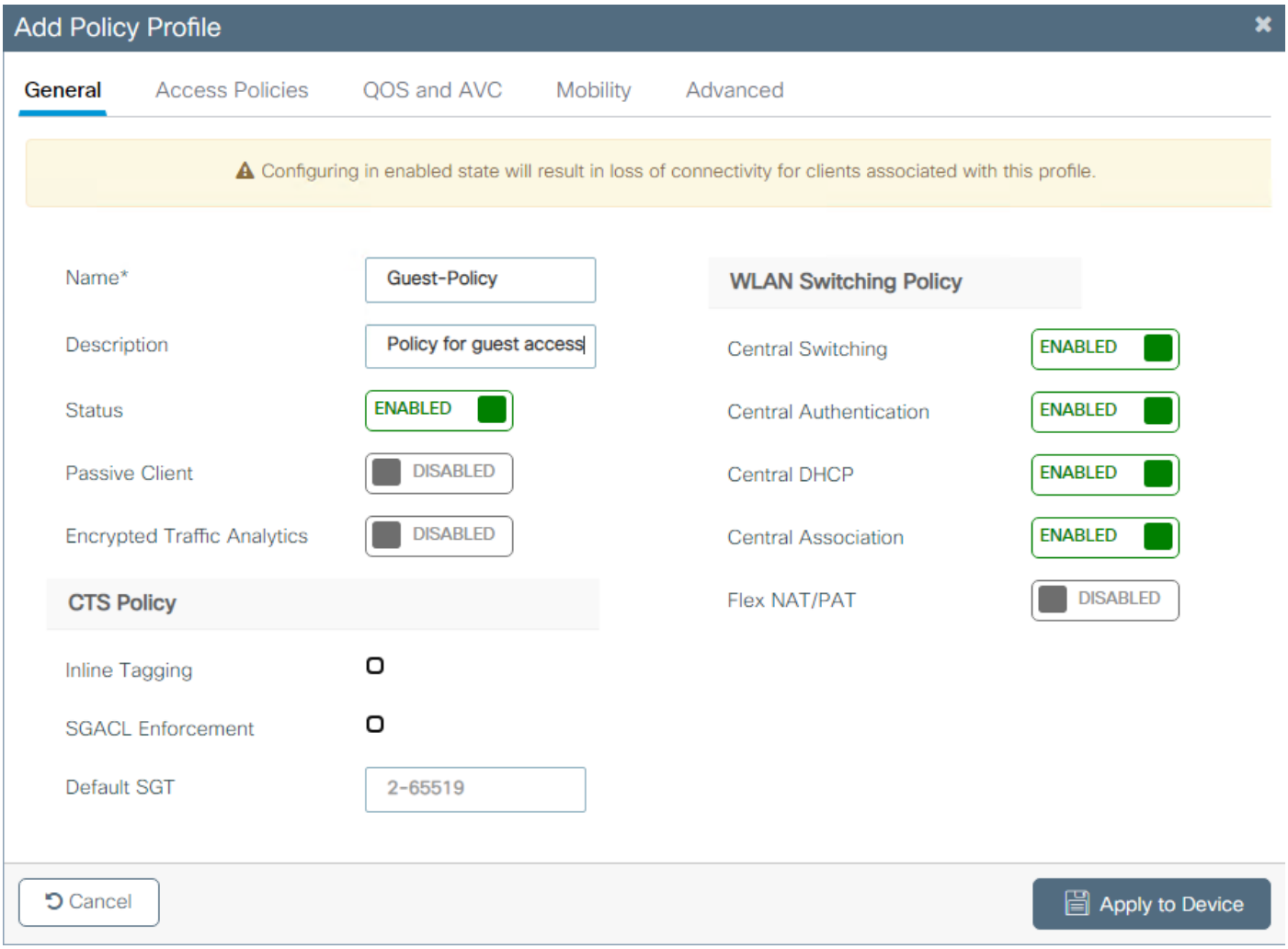
Configurações CLI:

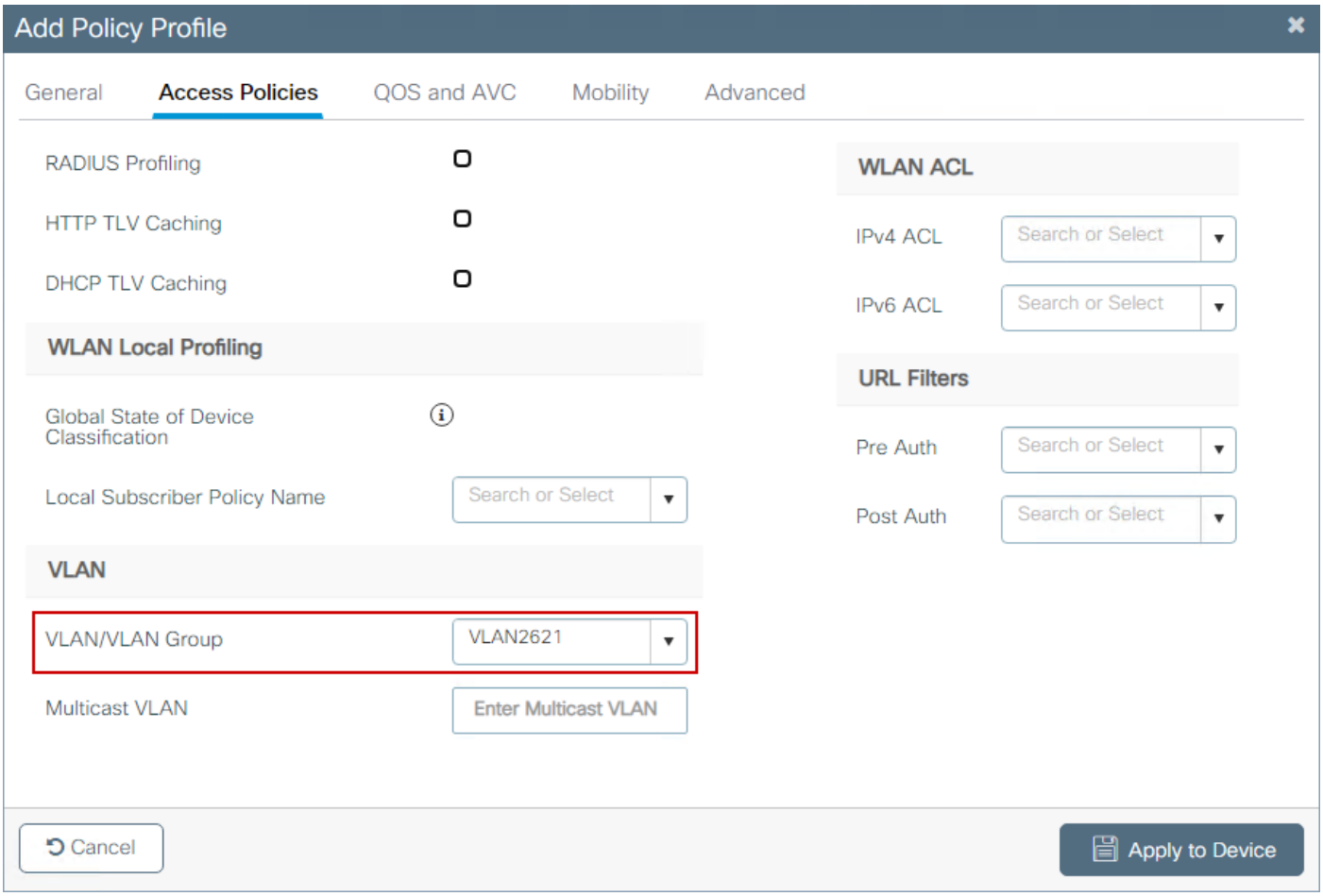
<#root>

```
9800(config)#
wlan EWA-Guest 4 EWA-Guest

9800(config-wlan)#
no security ft adaptive

9800(config-wlan)#
no security wpa

9800(config-wlan)#
```

```
no security wpa wpa2

9800(config-wlan)#
no security wpa wpa2 ciphers aes

9800(config-wlan)#
no security wpa akm dot1x

9800(config-wlan)#
security web-auth

9800(config-wlan)#
security web-auth authentication-list local-auth

9800(config-wlan)#
security web-auth parameter-map EWA-Guest

9800(config-wlan)#
 no shutdown
```

Etapa 3. Navegue até Configuration > Tags & Profiles > Policy e selecione + Add. Defina o nome e o status da política; certifique-se de que as configurações de Central em WLAN Switching Policy estejam Enabled for Local mode APs. Na guia Access Policies, selecione a VLAN correta no menu suspenso VLAN/VLAN Group, conforme mostrado na imagem.


Add Policy Profile
General
Access Policies
QOS and AVC
Mobility
Advanced
Configuring in enabled state will result in loss of connectivity for clients associated with this profile.
Name*
Guest-Policy
Description
Policy for guest access
Status
ENABLED
Passive Client
DISABLED
Encrypted Traffic Analytics
DISABLED
CTS Policy
Inline Tagging
SGACL Enforcement
Default SGT
2-65519
WLAN Switching Policy
Central Switching
ENABLED
Central Authentication
ENABLED
Central DHCP
ENABLED
Central Association
ENABLED
Flex NAT/PAT
DISABLED
Cancel
Apply to Device

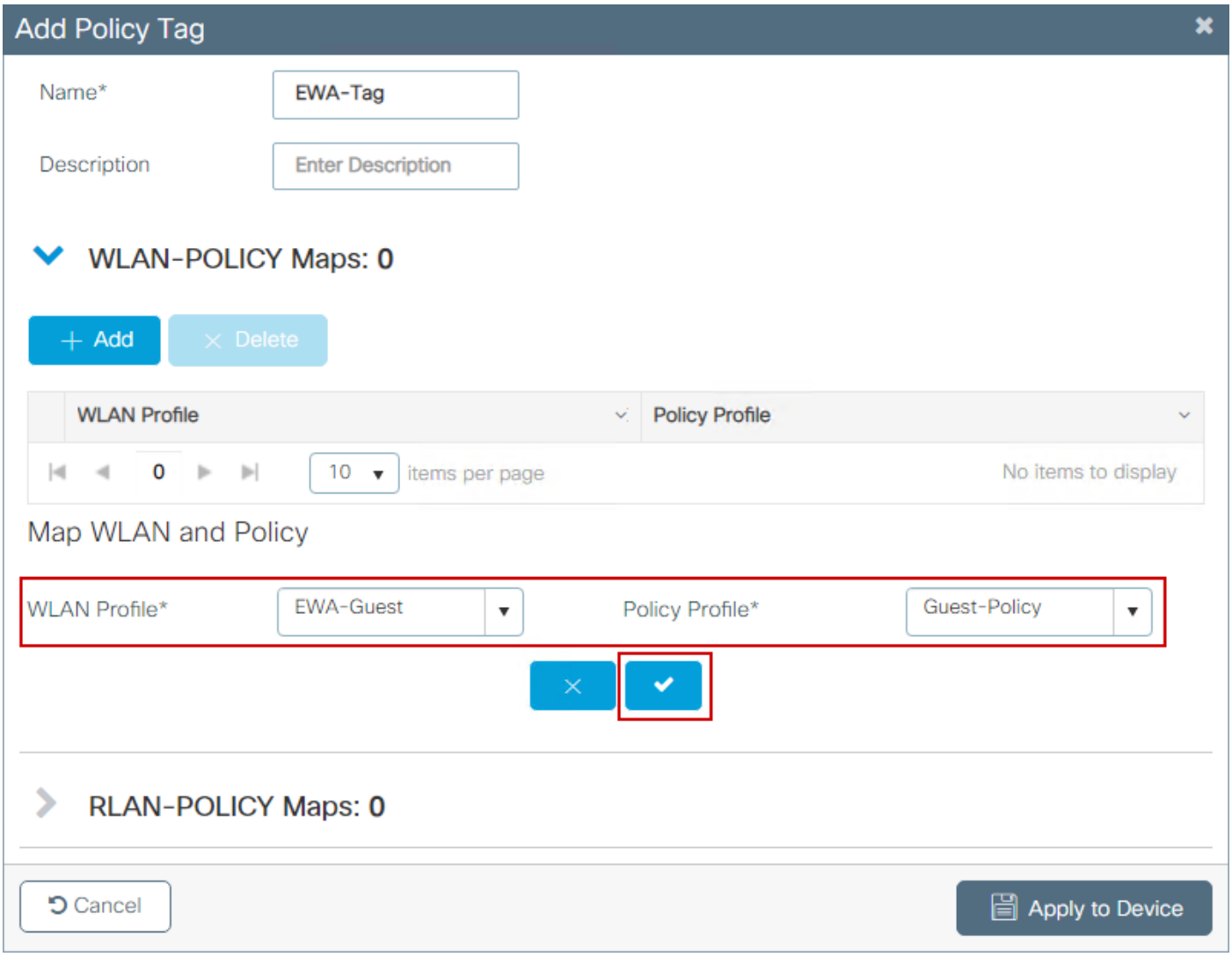


Configuração de CLI:

<#root>

```
9800(config)#

wireless profile policy Guest-Policy

9800(config-wireless-policy)#

description "Policy for guest access"

9800(config-wireless-policy)#

vlan VLAN2621

9800(config-wireless-policy)#

no shutdown
```

Etapa 4. Navegue até Configuration > Tags & Profiles > Tags, na guia Policy selecione + Add. Defina um nome de marca e, em Mapas de WLAN-POLICY, selecione + Adicionar e adicione o Perfil de WLAN e Política criado anteriormente.

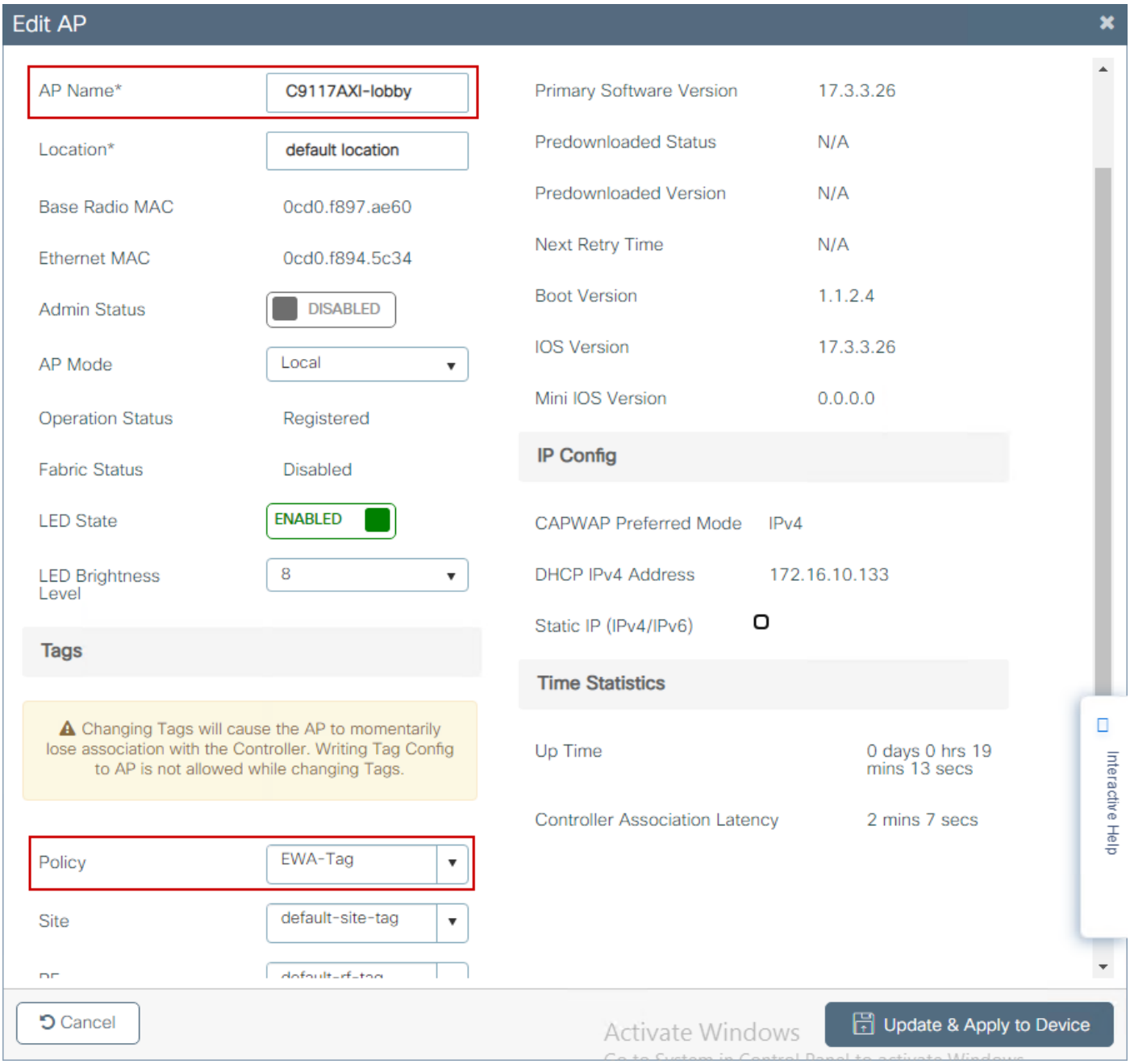


Configuração de CLI:

<#root>

```
9800(config)#

wireless tag policy EWA-Tag


9800(config-policy-tag)#

wlan EWA-Guest policy Guest-Policy
```

Etapa 5. Navegue até Configuration > Wireless > Access Points e selecione o AP que é usado para transmitir este SSID. No menu Edit AP, selecione a tag recém-criada no menu suspenso Policy.



Se vários APs precisarem ser marcados ao mesmo tempo, há duas opções disponíveis:

Opção A. Navegue até Configuration > Wireless Setup > Advanced e selecione Start Now para exibir a lista do menu de configuração. Selecione o ícone de lista ao lado de Tag APs, ele exibe a lista de todos os APs no estado Join, verifique os APs necessários e, em seguida, selecione + Tag APs, selecione a Policy Tag criada no menu suspenso.

Wireless Setup Flow Overview

This screen allows you to design Wireless LAN Configuration. It involves creating Policies and Tags. Once the design is completed, they can be deployed to the Access Points right here.

DESIGN PHASE

Tags & Profiles

WLAN Policy (Mandatory)	Site Policy (Optional)	Radio Policy (Optional)
WLAN Profile	AP Join Profile	RF Profile
Policy Profile	Flex Profile	RF Tag
Policy Tag	Site Tag	

DEPLOY PHASE

Apply to APs

(Mandatory)

Tag APs

Select APs and push configuration to them

TERMINOLOGY

Tag

WLAN Policy, Policy Profile

Site Policy - AP Profile, Site Profile

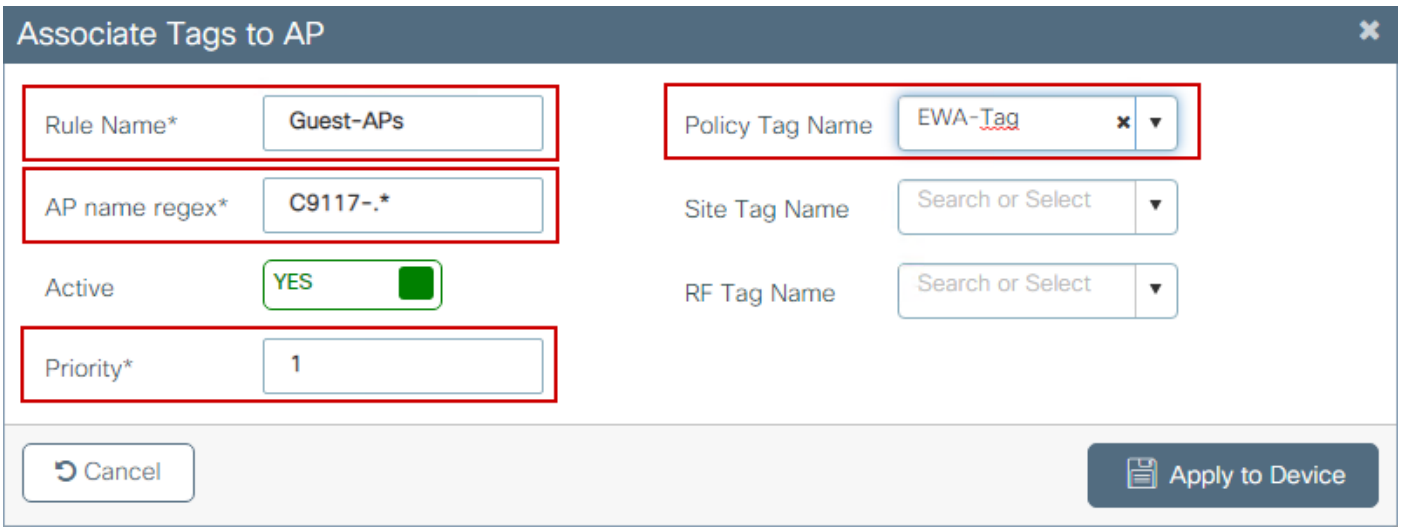
Radio Policy - Radio Characteristics

ACTIONS

Go to List View

Create New

. Defina o nome da regra, o nome do AP regex (essa configuração permite que a controladora defina quais APs serão marcados), a prioridade (números menores têm maior prioridade) e as marcas necessárias.



Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente:

<#root>

9800#

show running-config wlan

9800#

show running-config aaa

9800#

show aaa servers

9800#

show ap tag summary

9800#

show ap name <ap-name> config general

9800#

show ap name <ap-name> tag detail

9800#

show wlan [summary | id | name | all]

9800#

show wireless tag policy detailed <policy-tag name>

9800#

show wireless profile policy detailed <policy-profile name>

Verifique o status e a disponibilidade do servidor http com show ip http server status:

<#root>

9800#

show ip http server status

HTTP server status: Enabled

HTTP server port: 80

HTTP server active supplementary listener ports: 21111
HTTP server authentication method: local
HTTP server auth-retry 0 time-window 0
HTTP server digest algorithm: md5
HTTP server access class: 0

HTTP server IPv4 access class: None

HTTP server IPv6 access class: None

[...]
HTTP server active session modules: ALL
HTTP secure server capability: Present

HTTP secure server status: Enabled

HTTP secure server port: 443

HTTP secure server ciphersuite: rsa-aes-cbc-sha2 rsa-aes-gcm-sha2
dhe-aes-cbc-sha2 dhe-aes-gcm-sha2 ecdhe-rsa-aes-cbc-sha2
ecdhe-rsa-aes-gcm-sha2 ecdhe-ecdsa-aes-gcm-sha2
HTTP secure server TLS version: TLSv1.2 TLSv1.1
HTTP secure server client authentication: Disabled
HTTP secure server PIV authentication: Disabled
HTTP secure server PIV authorization only: Disabled

HTTP secure server trustpoint: CISCO_IDEVID_SUDI

HTTP secure server peer validation trustpoint:
HTTP secure server ECDHE curve: secp256r1
HTTP secure server active session modules: ALL

Verifique a conexão da ACL à sessão do cliente com estes comandos:

<#root>

9800#

show platform software wireless-client chassis active R0 mac-address <Client mac in aaaa.bbbb.cccc forma

ID : 0xa0000002
MAC address : aaaa.bbbb.cccc
Type : Normal
Global WLAN ID : 4

SSID : EWA-Guest

Client index : 0
Mobility state : Local

Authentication state : L3 Authentication

VLAN ID : 2621
[...]
Disable IPv6 traffic : No

Dynamic policy template : 0x7b 0x73 0x0b 0x1e 0x46 0x2a 0xd7 0x8f 0x23 0xf3 0xfe 0x9e 0x5c 0xb0 0xeb 0xf

9800#

show platform software cgacl chassis active F0

Template ID

Group Index

Lookup ID Number of clients

0x7B 0x73 0x0B 0x1E 0x46 0x2A 0xD7 0x8F 0x23 0xF3 0xFE 0x9E 0x5C 0xB0 0xEB 0xF8 0x0000000a

0x0000001a 1

9800#

show platform software cgacl chassis active F0 group-idx <group index> acl

Acl ID Acl Name CGACL Type Protocol Direction Sequence
---
16 IP-Adm-V6-Int-ACL-global Punt IPv6 IN 1

25 WA-sec-172.16.80.8 Security IPv4 IN 2

```
26 WA-v4-int-172.16.80.8 Punt IPv4 IN 1


19 implicit_deny Security IPv4 IN 3
21 implicit_deny_v6 Security IPv6 IN 3
18 preauth_v6 Security IPv6 IN 2
```

Troubleshooting

Rastreamento Sempre Ativo

A WLC 9800 fornece recursos de rastreamento SEMPRE ATIVOS. Isso garante que todos os erros relacionados à conectividade do cliente, avisos e mensagens de nível de aviso sejam constantemente registrados e que você possa exibir registros de uma condição de incidente ou falha após sua ocorrência.

Observação: com base no volume de logs gerados, você pode voltar de algumas horas para vários dias.

Para visualizar os rastreamentos que a WLC 9800 coletou por padrão, você pode se conectar via SSH/Telnet à WLC 9800 e ler essas etapas (certifique-se de registrar a sessão em um arquivo de texto).

Etapa 1. Verifique a hora atual do controlador para que você possa acompanhar os registros no tempo de volta até quando o problema ocorreu.

```
<#root>

9800#

show clock
```

Etapa 2. Colete syslogs do buffer do controlador ou do syslog externo, conforme ditado pela configuração do sistema. Isso fornece uma visão rápida da integridade do sistema e dos erros, se houver.

```
<#root>

9800#

show logging
```

Etapa 3. Verifique se as condições de depuração estão ativadas.

<#root>

9800#

show debugging

```
IOSXE Conditional Debug Configs:
Conditional Debug Global State: Stop
IOSXE Packet Tracing Configs:
Packet Infra debugs:
Ip Address                                              Port
------------------------------------------------------|----------
```

Observação: se você vir qualquer condição listada, isso significa que os rastreamentos são registrados no nível de depuração para todos os processos que encontram as condições ativadas (endereço mac, endereço IP e assim por diante). Isso aumentaria o volume de registros. Portanto, recomenda-se limpar todas as condições quando não estiver depurando ativamente.

Etapa 4. Supondo que o endereço mac em teste não foi listado como uma condição na Etapa 3. Colete os rastreamentos de nível de aviso sempre ativo para o endereço mac específico.

<#root>

9800#

show logging profile wireless filter [mac | ip] [<aaaa.bbbb.cccc> | <a.b.c.d>] to-file always-on-<FILENA

Você pode exibir o conteúdo da sessão ou copiar o arquivo para um servidor TFTP externo.

<#root>

9800#

more bootflash:always-on-<FILENAME.txt>

or
9800#

copy bootflash:always-on-<FILENAME.txt> tftp://<a.b.c.d>/<path>/always-on-<FILENAME.txt>

Depuração condicional e rastreamento radioativo

Se os rastreamentos sempre ativos não fornecerem informações suficientes para determinar o disparador do problema sob investigação, você poderá habilitar a depuração condicional e capturar o rastreamento de Radio Ative (RA), que fornece rastreamentos no nível de depuração para todos os processos que interagem com a condição especificada (endereço mac do cliente, neste caso). Para habilitar a depuração condicional, leia estas etapas.

Etapa 1. Verifique se não há condições de depuração ativadas.

<#root>

9800#

clear platform condition all

Etapa 2. Ative a condição de depuração para o endereço MAC do cliente sem fio que você deseja monitorar.

Estes comandos começam a monitorar o endereço MAC fornecido por 30 minutos (1.800 segundos). Como alternativa, você pode aumentar esse tempo para até 2.085.978.494 segundos.

<#root>

9800#

debug wireless mac <aaaa.bbbb.cccc> {monitor-time <seconds>}

Observação: para monitorar mais de um cliente por vez, execute o comando debug wireless mac por endereço mac.

Observação: a atividade do cliente sem fio não é exibida na sessão do terminal, pois todos os logs são armazenados em buffer internamente para serem exibidos posteriormente.

Etapa 3. Reproduza o problema ou comportamento que você deseja monitorar.

Etapa 4. Interrompa as depurações se o problema for reproduzido antes que o tempo de monitoramento padrão ou configurado acabe.

<#root>

9800#

no debug wireless mac <aaaa.bbbb.cccc>

Depois que o monitor-time tiver passado ou a conexão sem fio de depuração for interrompida, o 9800 WLC gerará um arquivo local com o nome:

ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log

Etapa 5. Colete o arquivo da atividade do endereço MAC. Você pode copiar o registro de rastreamento de RA para um servidor externo ou exibir a saída diretamente na tela.

Verifique o nome do arquivo de rastreamentos de RA.

<#root>

9800#

dir bootflash: | inc ra_trace

Copie o arquivo para um servidor externo:

<#root>

9800#

copy bootflash:ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log tftp://<a.b.c.d>

Mostre o conteúdo:

<#root>

9800#

more bootflash:ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log

Etapa 6. Se a causa do problema ainda não for evidente, colete os registros internos, que são uma visualização mais detalhada dos registros de nível de depuração. Você não precisa depurar o cliente novamente, pois o comando fornece logs de depuração que já foram coletados e armazenados internamente.

<#root>

9800#

show logging profile wireless internal filter [mac | ip] [<aaaa.bbbb.cccc> | <a.b.c.d>] to-file ra-inter

---

Observação: a saída desse comando retorna rastros para todos os níveis de registro de todos os processos e é bastante volumosa. Entre em contato com o TAC da Cisco para ajudar a analisar esses rastreamentos.

<#root>

9800#

copy bootflash:ra-internal-<FILENAME>.txt tftp://<a.b.c.d>/ra-internal-<FILENAME>.txt

Mostre o conteúdo:

<#root>

```
9800#

more bootflash:ra-internal-<FILENAME>.txt
```

Passo 7. Remova as condições de depuração.

Observação: certifique-se de sempre remover as condições de depuração após uma sessão de solução de problemas.

Capturas de pacotes incorporadas

Os controladores 9800 podem farejar pacotes nativamente; isso permite uma solução de problemas mais fácil como visibilidade de processamento de pacote de plano de controle.

Etapa 1. Defina uma ACL para filtrar o tráfego de interesse. Para a autenticação da Web, é recomendável permitir o tráfego de e para o servidor Web, bem como o tráfego de e para alguns APs onde os clientes estão conectados.

<#root>

```
9800(config)#

ip access-list extended EWA-pcap


9800(config-ext-nacl)#

permit ip any host <web server IP>


9800(config-ext-nacl)#

permit ip host <web server IP> any


9800(config-ext-nacl)#

permit ip any host <AP IP>


9800(config-ext-nacl)#

permit ip host <AP IP> any
```

Etapa 2. Defina os parâmetros de captura do monitor. Certifique-se de que o tráfego do plano de controle esteja habilitado em ambas as direções, a interface se refere ao uplink físico do seu

controlador.

<#root>

```
9800#

monitor capture EWA buffer size <buffer size in MB>


9800#

monitor capture EWA access-list EWA-pcap


9800#

monitor capture EWA control-plane both interface <uplink interface> both
```

<#root>

```
9800#

show monitor capture EWA


Status Information for Capture EWA
Target Type:
Interface: Control Plane, Direction: BOTH

Interface: TenGigabitEthernet0/1/0, Direction: BOTH


Status : Inactive
Filter Details:

Access-list: EWA-pcap


Inner Filter Details:
Buffer Details:
Buffer Type: LINEAR (default)

Buffer Size (in MB): 100


Limit Details:
Number of Packets to capture: 0 (no limit)
Packet Capture duration: 0 (no limit)
Packet Size to capture: 0 (no limit)
Packet sampling rate: 0 (no sampling)
```

Etapa 3. Inicie a captura do monitor e reproduza o problema.

<#root>

```
9800#

monitor capture EWA start
```

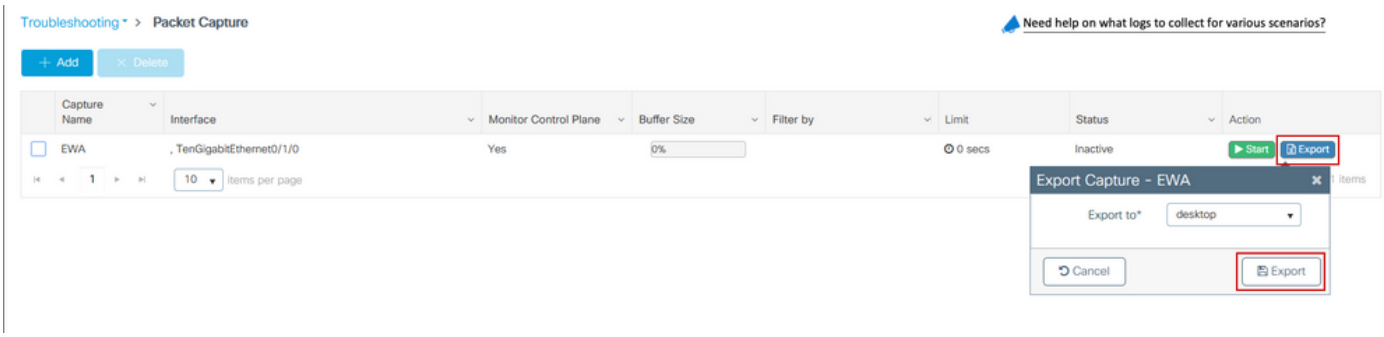
```
Started capture point : EWA
```

Etapa 4. Pare a captura do monitor e exporte-a.

<#root>

```
9800#
monitor capture EWA stop

Stopped capture point : EWA
9800#monitor capture EWA export tftp://<a.b.c.d>/EWA.pcap
```

Como alternativa, a captura pode ser baixada da GUI, navegue para Troubleshooting > Packet Capture e selecione Export na captura configurada. Selecione desktop no menu suspenso para fazer download da captura por meio de HTTP para a pasta desejada.



Solução de problemas do lado do cliente

As WLANs de autenticação da Web dependem do comportamento do cliente. Dessa forma, o conhecimento e as informações sobre o comportamento do cliente são fundamentais para identificar a causa raiz dos comportamentos incorretos de autenticação da Web.

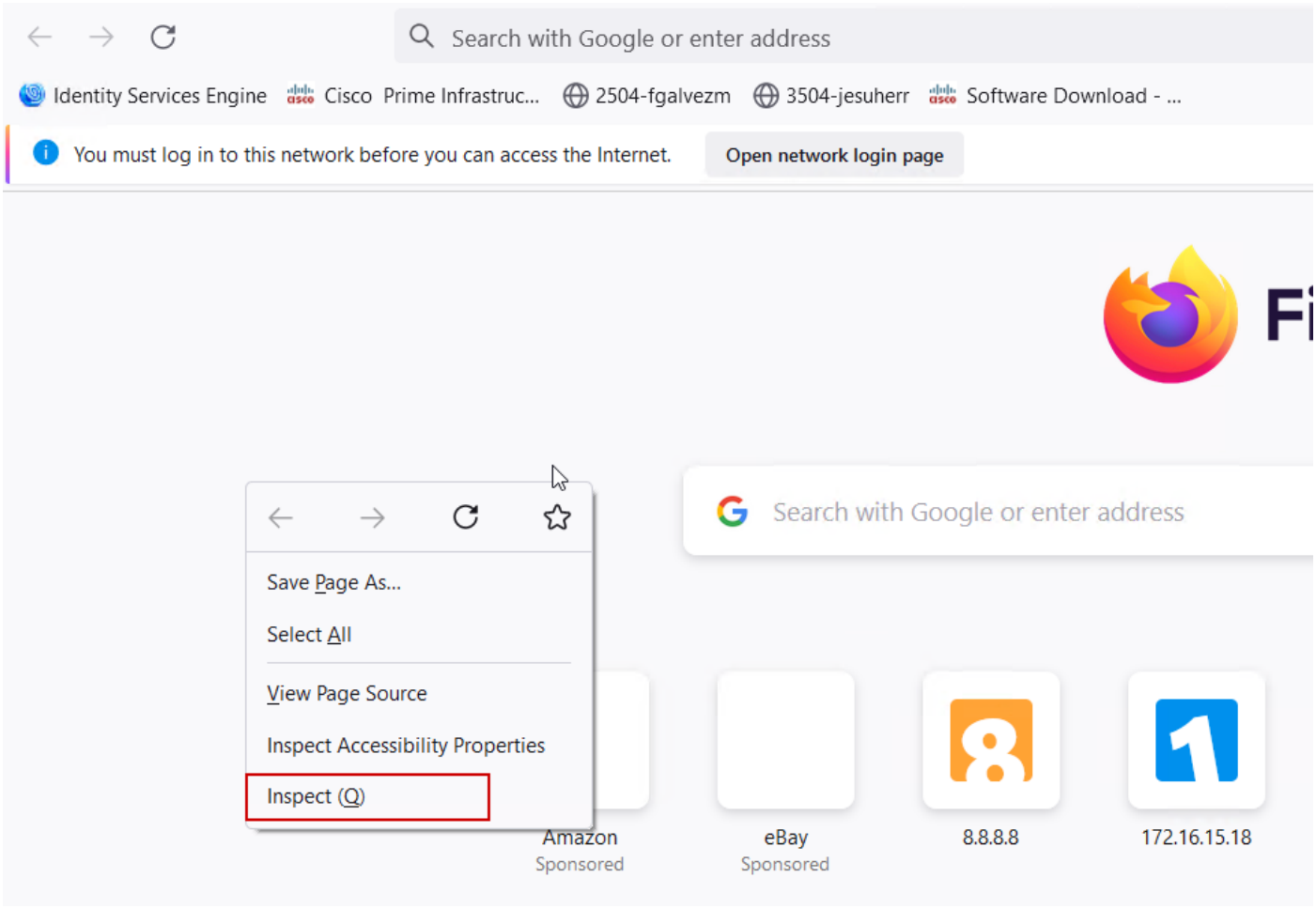
Solução de problemas do navegador HAR

Muitos navegadores modernos, como o Mozilla Firefox e o Google Chrome, fornecem ferramentas de desenvolvedor de console para depurar interações de aplicativos da Web. Os arquivos HAR são registros de interações cliente-servidor e fornecem um cronograma de interações HTTP juntamente com informações de solicitação e resposta (cabeçalhos, código de status, parâmetros, etc.).

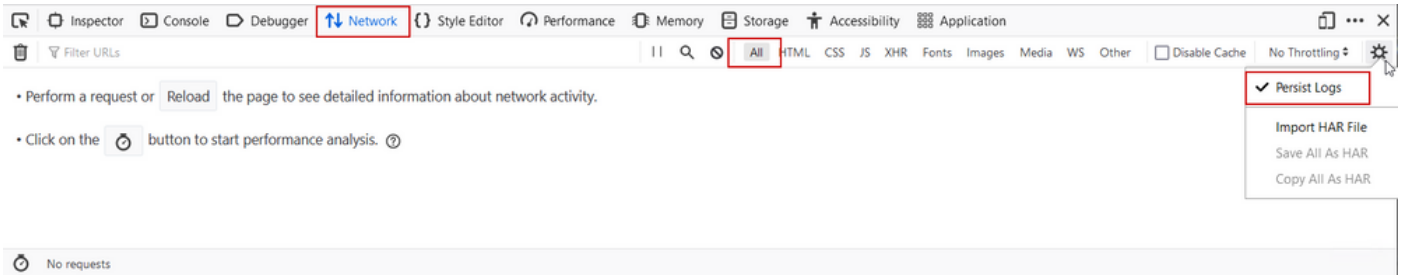
Os arquivos HAR podem ser exportados do navegador do cliente e importados em um navegador diferente para análise posterior. Este documento descreve como coletar o arquivo HAR do Mozilla Firefox.

Etapa 1. Abra as Ferramentas de Desenvolvedor da Web com Ctrl + Shift + I ou clique com o

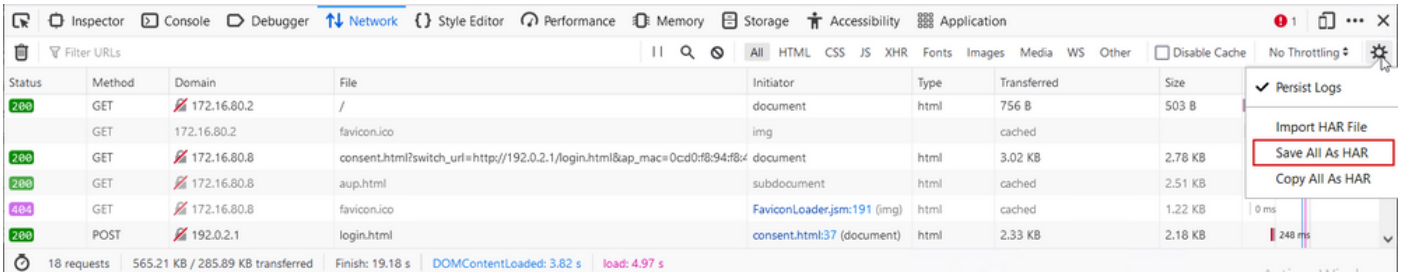
botão direito do mouse no conteúdo do navegador e selecione Inspecionar.



Etapa 2. Navegue até Rede, certifique-se de que "Todos" esteja selecionado para capturar todos os tipos de solicitação. Selecione o ícone de engrenagem e certifique-se de que Persist Logs tenha uma seta ao lado dele, caso contrário, as solicitações de logs são limpas sempre que uma alteração de domínio é disparada.



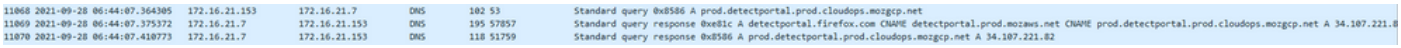
Etapa 3. Reproduza o problema, certifique-se de que o navegador registre todas as solicitações. Uma vez reproduzido o problema, pare o registro da rede, selecione no ícone da engrenagem e selecione Save All As HAR.



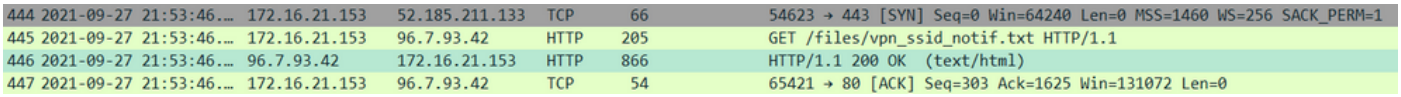
Captura de pacotes do lado do cliente

Clientes sem fio com SO como Windows ou MacOS podem farejar pacotes em seu adaptador de placa sem fio. Embora não sejam uma substituição direta de capturas de pacotes pelo ar, eles podem fornecer uma visão geral do fluxo de autenticação da Web geral.

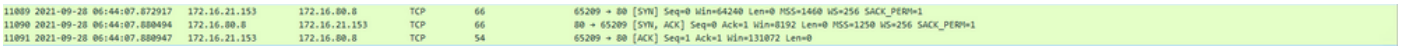
Solicitação DNS:



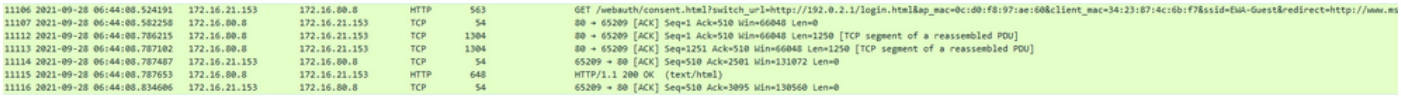
Handshake TCP inicial e GET HTTP para redirecionamento:



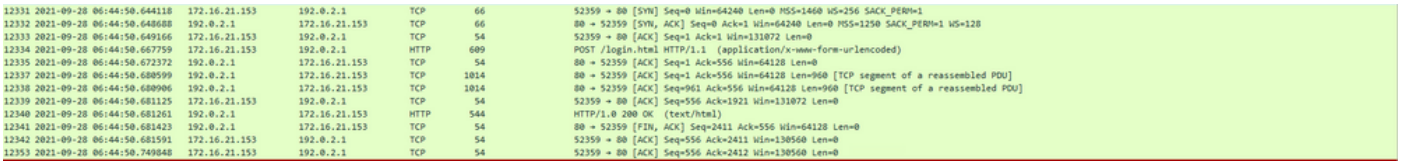
Handshake TCP com servidor externo:



HTTP GET para servidor externo (solicitação de portal cativo):



HTTP POST para IP virtual para autenticação:



Exemplo de uma tentativa bem-sucedida

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

Autenticação e associação 802.11:

<#root>

```
2021/09/28 12:59:51.781967 {wncd_x_R0-0}{1}: [client-orch-sm] [26328]: (note): MAC: 3423.874c.6bf7 Asso
2021/09/28 12:59:51.782009 {wncd_x_R0-0}{1}: [client-orch-sm] [26328]: (debug): MAC: 3423.874c.6bf7
```

Received Dot11 association request.

```
 Processing started,
```

SSID: EWA-Guest, Policy profile: Guest-Policy

```
, AP Name: C9117AXI-lobby, Ap Mac Address: 0cd0.f897.ae60 BSSID MAC0000.0000.0000 wlan ID: 4RSSI: -39,
2021/09/28 12:59:51.782152 {wncd_x_R0-0}{1}: [client-orch-state] [26328]: (note): MAC: 3423.874c.6bf7 C
2021/09/28 12:59:51.782357 {wncd_x_R0-0}{1}: [dot11-validate] [26328]: (info): MAC: 3423.874c.6bf7 WiFi
2021/09/28 12:59:51.782480 {wncd_x_R0-0}{1}: [dot11] [26328]: (debug): MAC: 3423.874c.6bf7 dot11 send a
```

Sending association response with resp_status_code: 0

```
2021/09/28 12:59:51.782483 {wncd_x_R0-0}{1}: [dot11] [26328]: (debug): MAC: 3423.874c.6bf7 Dot11 Capabi
2021/09/28 12:59:51.782509 {wncd_x_R0-0}{1}: [dot11-frame] [26328]: (info): MAC: 3423.874c.6bf7 WiFi di
2021/09/28 12:59:51.782519 {wncd_x_R0-0}{1}: [dot11] [26328]: (info): MAC: 3423.874c.6bf7 dot11 send as
2021/09/28 12:59:51.782611 {wncd_x_R0-0}{1}: [dot11] [26328]: (note): MAC: 3423.874c.6bf7
```

Association success. AID 1

```
, Roaming = False, WGB = False, 11r = False, 11w = False
2021/09/28 12:59:51.782626 {wncd_x_R0-0}{1}: [dot11] [26328]: (info): MAC: 3423.874c.6bf7 DOT11 state t
2021/09/28 12:59:51.782676 {wncd_x_R0-0}{1}: [client-orch-sm] [26328]: (debug): MAC: 3423.874c.6bf7
```

Station Dot11 association is successful.

Autenticação da camada 2 ignorada:

<#root>

```
2021/09/28 12:59:51.782727 {wncd_x_R0-0}{1}: [client-orch-sm] [26328]: (debug): MAC: 3423.874c.6bf7 Sta
2021/09/28 12:59:51.782745 {wncd_x_R0-0}{1}: [client-orch-state] [26328]: (note): MAC: 3423.874c.6bf7 C
2021/09/28 12:59:51.782785 {wncd_x_R0-0}{1}: [client-auth] [26328]: (note): MAC: 3423.874c.6bf7
```

L2 Authentication initiated. method WEBAUTH

```
, Policy VLAN 2621,AAA override = 0
2021/09/28 12:59:51.782803 {wncd_x_R0-0}{1}: [sanet-shim-translate] [26328]: (ERR): 3423.874c.6bf7 wlan
[...]
2021/09/28 12:59:51.787912 {wncd_x_R0-0}{1}: [client-auth] [26328]: (info): MAC: 3423.874c.6bf7 Client
2021/09/28 12:59:51.787953 {wncd_x_R0-0}{1}: [client-auth] [26328]: (info): MAC: 3423.874c.6bf7 Client
2021/09/28 12:59:51.787966 {wncd_x_R0-0}{1}: [client-orch-sm] [26328]: (debug): MAC: 3423.874c.6bf7
```

L2 Authentication of station is successful., L3 Authentication : 1

Placa ACL:

<#root>

```
2021/09/28 12:59:51.785227 {wncd_x_R0-0}{1}: [webauth-sm] [26328]: (info): [ 0.0.0.0]Starting Webauth,
2021/09/28 12:59:51.785307 {wncd_x_R0-0}{1}: [auth-mgr-feat_wireless] [26328]: (info): [0000.0000.0000:
2021/09/28 12:59:51.785378 {wncd_x_R0-0}{1}: [webauth-acl] [26328]: (info): capwap_9000000b[3423.874c.6
```

Applying IPv4 intercept ACL via SVM, name: WA-v4-int-172.16.80.8

```
, priority: 50, IIF-ID: 0
2021/09/28 12:59:51.785738 {wncd_x_R0-0}{1}: [epm-redirect] [26328]: (info): [0000.0000.0000:unknown]
```

URL-Redirect-ACL = WA-v4-int-172.16.80.8

```
2021/09/28 12:59:51.786324 {wncd_x_R0-0}{1}: [webauth-acl] [26328]: (info): capwap_9000000b[3423.874c.6
```

Applying IPv6 intercept ACL via SVM, name: IP-Adm-V6-Int-ACL-global, priority: 52

```
, IIF-ID: 0
2021/09/28 12:59:51.786598 {wncd_x_R0-0}{1}: [epm-redirect] [26328]: (info): [0000.0000.0000:unknown]
```

URL-Redirect-ACL = IP-Adm-V6-Int-ACL-global

```
2021/09/28 12:59:51.787904 {wncd_x_R0-0}{1}: [client-auth] [26328]: (info): MAC: 3423.874c.6bf7 Client
```

Processo de aprendizado de IP:

<#root>

```
2021/09/28 12:59:51.799515 {wncd_x_R0-0}{1}: [client-orch-state] [26328]: (note): MAC: 3423.874c.6bf7 C
2021/09/28 12:59:51.799716 {wncd_x_R0-0}{1}: [client-iplearn] [26328]: (info): MAC: 3423.874c.6bf7
```

IP-learn state transition: S_IPLEARN_INIT -> S_IPLEARN_IN_PROGRESS

```
2021/09/28 12:59:51.802213 {wncd_x_R0-0}{1}: [client-auth] [26328]: (info): MAC: 3423.874c.6bf7 Client
2021/09/28 12:59:51.916777 {wncd_x_R0-0}{1}: [sisf-packet] [26328]: (debug): RX: ARP from interface cap
[...]
2021/09/28 12:59:52.810136 {wncd_x_R0-0}{1}: [client-iplearn] [26328]: (note): MAC: 3423.874c.6bf7
```

Client IP learn successful. Method: ARP IP: 172.16.21.153

```
2021/09/28 12:59:52.810185 {wncd_x_R0-0}{1}: [epm] [26328]: (info): [0000.0000.0000:unknown] HDL = 0x0
2021/09/28 12:59:52.810404 {wncd_x_R0-0}{1}: [auth-mgr] [26328]: (info): [3423.874c.6bf7:capwap_900000
2021/09/28 12:59:52.810794 {wncd_x_R0-0}{1}: [auth-mgr-feat_wireless] [26328]: (info): [0000.0000.0000:
2021/09/28 12:59:52.810863 {wncd_x_R0-0}{1}: [client-iplearn] [26328]: (info): MAC: 3423.874c.6bf7
```

IP-learn state transition: S_IPLEARN_IN_PROGRESS -> S_IPLEARN_COMPLETE

Processo de autenticação e redirecionamento da camada 3:

<#root>

```
2021/09/28 12:59:52.811141 {wncd_x_R0-0}{1}: [client-auth] [26328]: (note): MAC: 3423.874c.6bf7
```

L3 Authentication initiated. LWA

```
2021/09/28 12:59:52.811154 {wncd_x_R0-0}{1}: [client-auth] [26328]: (info): MAC: 3423.874c.6bf7 Client
2021/09/28 12:59:55.324550 {wncd_x_R0-0}{1}: [webauth-httpd] [26328]: (info): capwap_9000000b[3423.874c
2021/09/28 12:59:55.324565 {wncd_x_R0-0}{1}: [webauth-httpd] [26328]: (info): capwap_9000000b[3423.874c
```

HTTP GET request

```
2021/09/28 12:59:55.324588 {wncd_x_R0-0}{1}: [webauth-httpd] [26328]: (info): capwap_9000000b[3423.874c
[...]
2021/09/28 13:01:29.859434 {wncd_x_R0-0}{1}: [webauth-httpd] [26328]: (info): capwap_9000000b[3423.874c
```

POST rcvd when in LOGIN state

```
2021/09/28 13:01:29.859636 {wncd_x_R0-0}{1}: [webauth-acl] [26328]: (info): capwap_9000000b[3423.874c.6
2021/09/28 13:01:29.860335 {wncd_x_R0-0}{1}: [webauth-acl] [26328]: (info): capwap_9000000b[3423.874c.6
2021/09/28 13:01:29.861092 {wncd_x_R0-0}{1}: [auth-mgr] [26328]: (info): [3423.874c.6bf7:capwap_900000
```

Authc success from WebAuth, Auth event success

```
2021/09/28 13:01:29.861151 {wncd_x_R0-0}{1}: [ewlc-infra-evq] [26328]: (note): Authentication Success.
2021/09/28 13:01:29.862867 {wncd_x_R0-0}{1}: [client-auth] [26328]: (note): MAC: 3423.874c.6bf7
```

L3 Authentication Successful.

```
 ACL:[]
2021/09/28 13:01:29.862871 {wncd_x_R0-0}{1}: [client-auth] [26328]: (info): MAC: 3423.874c.6bf7
```

Client auth-interface state transition: S_AUTHIF_WEBAUTH_PENDING -> S_AUTHIF_WEBAUTH_DONE

Transição para o estado RUN:

<#root>

```
2021/09/28 13:01:29.863176 {wncd_x_R0-0}{1}: [client-auth] [26328]: (note): MAC: 3423.874c.6bf7 ADD MOB
2021/09/28 13:01:29.863272 {wncd_x_R0-0}{1}: [errmsg] [26328]: (info): %CLIENT_ORCH_LOG-6-CLIENT_ADDED_
```

Username entry (3423.874C.6BF7) joined with ssid (EWA-Guest) for device with MAC: 3423.874c.6bf7

```
2021/09/28 13:01:29.863334 {wncd_x_R0-0}{1}: [aaa-attr-inf] [26328]: (info): [ Applied attribute :bsn-v
2021/09/28 13:01:29.863336 {wncd_x_R0-0}{1}: [aaa-attr-inf] [26328]: (info): [ Applied attribute : time
2021/09/28 13:01:29.863343 {wncd_x_R0-0}{1}: [aaa-attr-inf] [26328]: (info): [ Applied attribute : url-
2021/09/28 13:01:29.863387 {wncd_x_R0-0}{1}: [ewlc-qos-client] [26328]: (info): MAC: 3423.874c.6bf7 Cli
2021/09/28 13:01:29.863409 {wncd_x_R0-0}{1}: [rog-proxy-capwap] [26328]: (debug):
```

Managed client RUN state notification

```
: 3423.874c.6bf7
2021/09/28 13:01:29.863451 {wncd_x_R0-0}{1}: [client-orch-state] [26328]: (note): MAC: 3423.874c.6bf7
```

Client state transition: S_CO_L3_AUTH_IN_PROGRESS -> S_CO_RUN

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.