# Solucionar problemas comuns com LWA em WLCs 9800

## Contents



## Introdução

Este documento descreve os problemas comuns com clientes que se conectam a uma WLAN com Autenticação Web Local (LWA).

## Pré-requisitos

### Requisitos

A Cisco recomenda que você tenha conhecimento básico de:

- Controladora de LAN sem fio (WLC) 9800 da Cisco.
- Compreensão geral da Autenticação da Web Local (LWA) e sua configuração.

### Componentes Utilizados

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

- WLC 9800-CL
- Access point Cisco 9120AXI
- 9800 WLC Cisco IOS® XE versão 17.9.3

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

LWA é um tipo de autenticação de WLAN que pode ser configurado na WLC onde o cliente final que tenta se conectar, depois de selecionar a WLAN na lista, apresenta um portal para o usuário. Neste portal, o usuário pode inserir um nome de usuário e uma senha (dependendo da configuração selecionada) para concluir a conexão com a WLAN.

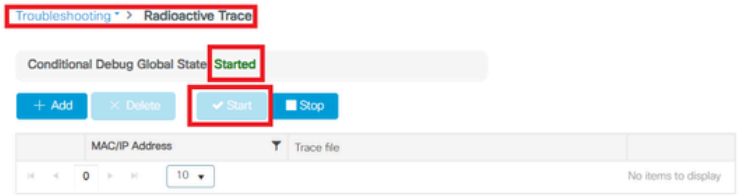
Consulte o guia de configuração de Configuração da Autenticação da Web Local para obter mais informações sobre como configurar o LWA na WLC 9800.

## Rastreamentos radioativos (RA) no 9800 WLC

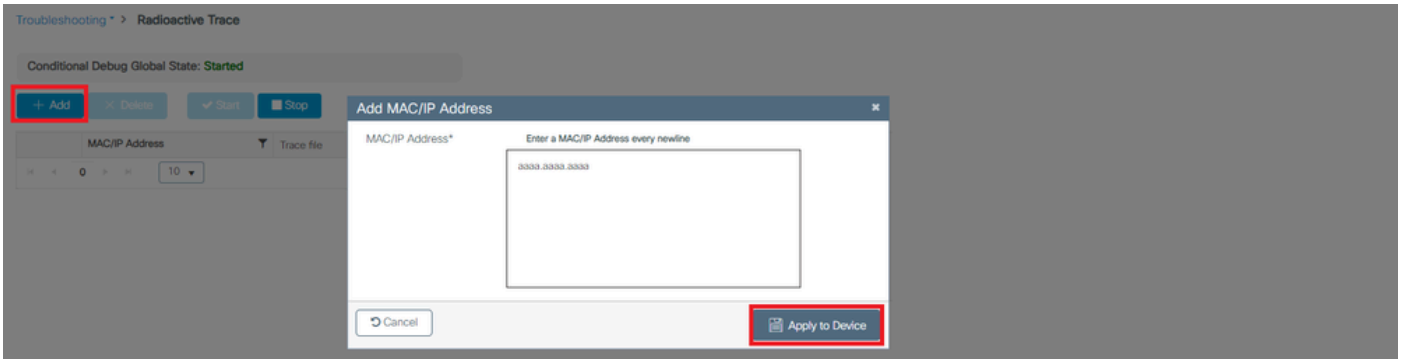
Os rastreamentos radioativos são uma excelente ferramenta de identificação e solução de problemas que pode ser usada ao solucionar vários problemas com a WLC e a conectividade do cliente. Para coletar rastreamentos de RA, siga estas etapas:

Na GUI:

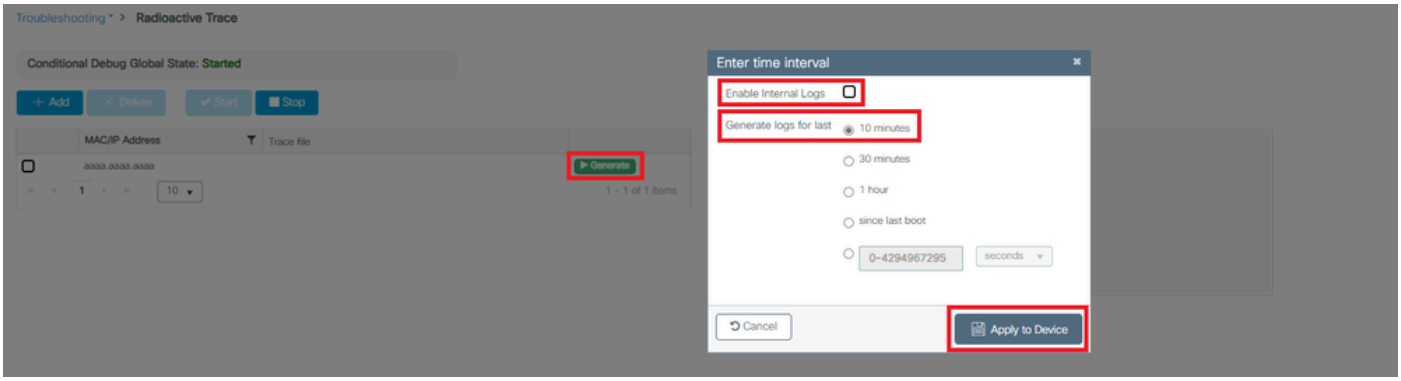
1. Vá para Troubleshooting > Radioative Trace.
2. Clique em Iniciar para habilitar o estado global de depuração condicional.
3. Clique em + Adicionar. Uma janela pop-up é aberta. Digite o endereço MAC do cliente. Qualquer formato de endereço MAC é aceito (aabb.ccdd.eeff, AABB.CCDD.EEEE, aa:bb:cc:dd:ee:ff ou AA:BB:CC:DD:EE:FF). Em seguida, clique em Apply to Device.
4. Faça com que o cliente reproduza o problema 3 ou 4 vezes.
5. Depois que o problema for reproduzido, clique em Generate (Gerar).
6. Uma nova janela pop-up será aberta. Gerar logs para os últimos 10 minutos. (Nesse caso, não é necessário ativar os logs internos). Clique em Apply to Device e aguarde o arquivo ser processado.
7. Depois que o arquivo tiver sido gerado, clique no ícone Download.



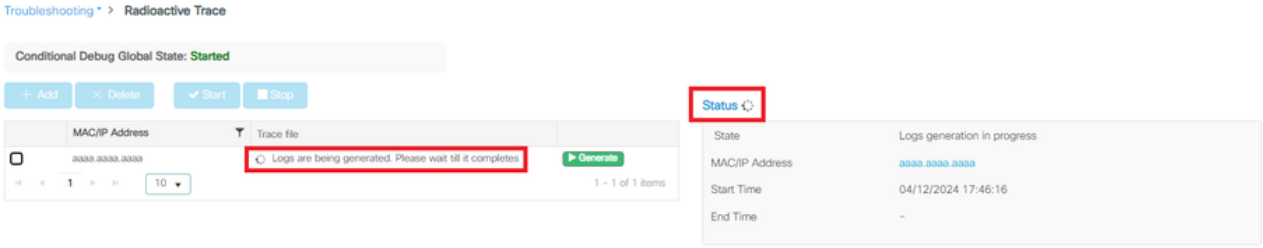

Habilitar depuração condicional



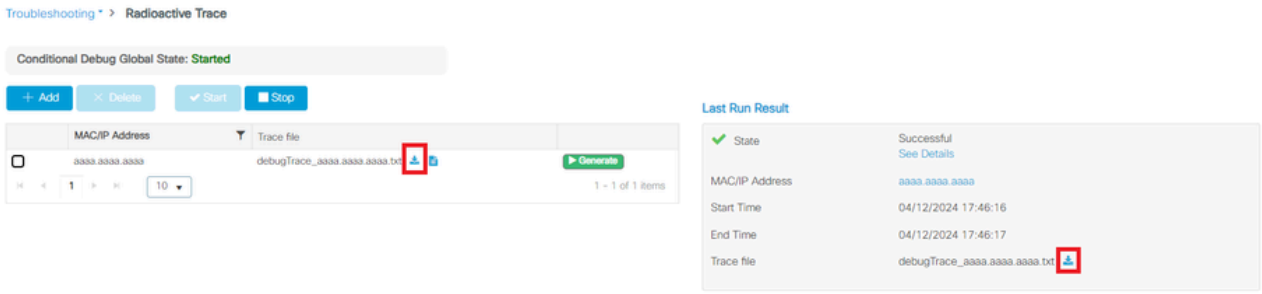

Adicionar um endereço MAC de cliente




Gerar Logs nos Últimos 10 Minutos




Aguarde até que o arquivo seja




geradoBaixe o arquivo

Na CLI:

<#root>

```
WLC# debug wireless mac
<mac-address>
 monitor-time 600
```

Um novo arquivo no flash de inicialização será gerado, chamado ra_trace_MAC_<mac-address>_HMMSS.XXX_timezone_DayWeek_Month_Day_year.log

<#root>

```
WLC# more bootflash:
ra_trace_MAC_<mac-address>_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log
```

Copiar o arquivo para um servidor externo para análise

<#root>

```
WLC# copy bootflash:
ra_trace_MAC_<mac-address>_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log
 ftp://username:password@<ftp-server-ip>/path/RATRACE_FILENAME.txt
```

Para obter mais informações sobre o rastreamento radioativo, consulte este link.

# Fluxo esperado

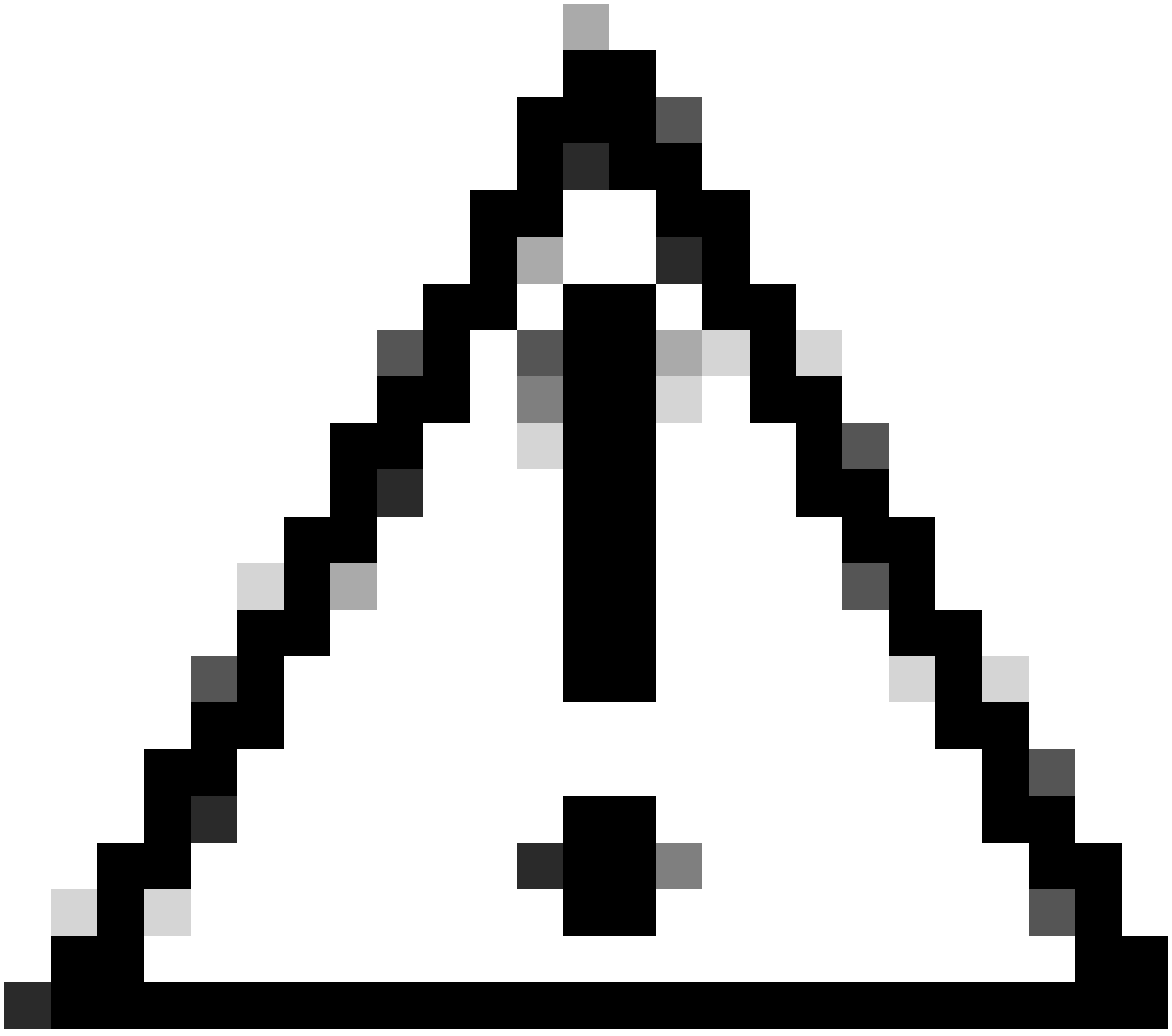
Consulte as informações para entender o cenário de trabalho para o LWA.

## Estágios pelos quais o Cliente Passa da Perspectiva do Cliente

1. O cliente final está associado à WLAN.
2. O cliente recebe um endereço IP atribuído.
3. O portal é apresentado ao cliente final.
4. O cliente final insere as credenciais de login.
5. O cliente final é autenticado.
6. O cliente final pode navegar na Internet.

## Estágios pelos quais o cliente passa da perspectiva da WLC

---



Cuidado: muitos registros do rastreamento de Radio Ative (RA) foram deixados de fora para fins de simplicidade.

---

O cliente final está associado à WLAN

<#root>

MAC: aaaa.bbbb.cccc

**Association received**

. BSSID d4e8.801a.3063, WLAN LWA-SSID, Slot 0 AP d4e8.801a.3060, APD4E8.8019.608C, old BSSID d4e8.801a.
MAC: aaaa.bbbb.cccc Received Dot11 association request. Processing started,SSID: LWA-SSID, Policy profi
MAC: aaaa.bbbb.cccc Client state transition: S_CO_L3_AUTH_IN_PROGRESS -> S_CO_L3_AUTH_IN_PROGRESS
MAC: aaaa.bbbb.cccc Dot11 ie validate ext/supp rates. Validation Passed for Supported rates radio_type
MAC: aaaa.bbbb.cccc WiFi direct: Dot11 validate P2P IE. P2P IE not present.
MAC: aaaa.bbbb.cccc dot11 send association response. Framing association response with resp_status_code
MAC: aaaa.bbbb.cccc Dot11 Capability info byte1 1, byte2: 14
MAC: aaaa.bbbb.cccc WiFi direct: skip build Assoc Resp with P2P IE: Wifi direct policy disabled
MAC: aaaa.bbbb.cccc Clearing old call info.
MAC: aaaa.bbbb.cccc dot11 send association response. Sending assoc response of length: 161 with resp_st
MAC: aaaa.bbbb.cccc

**Association success.**

 AID 1, Roaming = True, WGB = False, 11r = False, 11w = False Fast roam = False
MAC: aaaa.bbbb.cccc DOT11 state transition: S_DOT11_ASSOCIATED -> S_DOT11_ASSOCIATED

## Autenticação L2

<#root>

MAC: aaaa.bbbb.cccc Starting L2 authentication. Bssid in state machine:d4e8.801a.3063 Bssid in request
MAC: aaaa.bbbb.cccc Client state transition: S_CO_L3_AUTH_IN_PROGRESS -> S_CO_L2_AUTH_IN_PROGRESS
MAC: aaaa.bbbb.cccc L2 Authentication initiated. method WEBAUTH, Policy VLAN 0, AAA override = 1
[aaaa.bbbb.cccc:capwap_90400002] -

**authc_list: forwebauth**

[aaaa.bbbb.cccc:capwap_90400002] - authz_list: Not present under wlan configuration
MAC: aaaa.bbbb.cccc Client auth-interface state transition: S_AUTHIF_WEBAUTH_PENDING -> S_AUTHIF_WEBAUT
MAC: aaaa.bbbb.cccc IP-learn state transition: S_IPLEARN_COMPLETE -> S_IPLEARN_COMPLETE
MAC: aaaa.bbbb.cccc Client auth-interface state transition: S_AUTHIF_WEBAUTH_PENDING -> S_AUTHIF_WEBAUT
MAC: aaaa.bbbb.cccc

**L2 Authentication of station is successful.**

, L3 Authentication : 1

## O cliente recebe um endereço IP atribuído

<#root>

MAC: aaaa.bbbb.cccc Client state transition: S_CO_DPATH_PLUMB_IN_PROGRESS -> S_CO_IP_LEARN_IN_PROGRESS
MAC: aaaa.bbbb.cccc IP-learn state transition: S_IPLEARN_COMPLETE -> S_IPLEARN_COMPLETE
MAC: aaaa.bbbb.cccc

**Received ip learn response. method: IPLEARN_METHOD_DHCP**

Autenticação L3

<#root>

```
MAC: aaaa.bbbb.cccc Client state transition: S_CO_IP_LEARN_IN_PROGRESS -> S_CO_L3_AUTH_IN_PROGRESS
MAC: aaaa.bbbb.cccc
```

**L3 Authentication initiated. LWA**

```
MAC: aaaa.bbbb.cccc Client auth-interface state transition: S_AUTHIF_WEBAUTH_PENDING -> S_AUTHIF_WEBAUT
```

O cliente obtém um endereço IP

<#root>

```
RX: DHCPv4 from interface capwap_90400002 on vlan 100 Src MAC: aaaa.bbbb.cccc Dst MAC: ffff.ffff.ffff s
TX: DHCPv4 from interface capwap_90400002 on vlan 100 Src MAC: aaaa.bbbb.cccc Dst MAC: ffff.ffff.ffff s
RX: DHCPv4 from interface Gi2 on vlan 100 Src MAC: cccc.bbbb.aaaa Dst MAC: aaaa.bbbb.cccc src_ip: Y.Y.Y
TX: DHCPv4 from interface Gi2 on vlan 100 Src MAC: cccc.bbbb.aaaa Dst MAC: aaaa.bbbb.cccc src_ip: Y.Y.Y
RX: DHCPv4 from interface capwap_90400002 on vlan 100 Src MAC: aaaa.bbbb.cccc Dst MAC: ffff.ffff.ffff s
TX: DHCPv4 from interface capwap_90400002 on vlan 100 Src MAC: aaaa.bbbb.cccc Dst MAC: ffff.ffff.ffff s
RX: DHCPv4 from interface Gi2 on vlan 100 Src MAC: cccc.bbbb.aaaa Dst MAC: aaaa.bbbb.cccc src_ip: Y.Y.Y
TX: DHCPv4 from interface Gi2 on vlan 100 Src MAC: cccc.bbbb.aaaa Dst MAC: aaaa.bbbb.cccc src_ip: Y.Y.Y
MAC: aaaa.bbbb.cccc IP-learn state transition: S_IPLEARN_COMPLETE ->
```

**S_IPLEARN_COMPLETE**

Processamento do portal

<#root>

```
[aaaa.bbbb.cccc][X.X.X.X]capwap_90400002
```

**HTTP GET request**

```
[aaaa.bbbb.cccc][X.X.X.X]capwap_90400002
```

**Parse GET, src [X.X.X.X] dst [Z.Z.Z.Z] url [http://connectivitycheck.gstatic.com/generate_204]**

```
[aaaa.bbbb.cccc][X.X.X.X]capwap_90400002 Read complete: parse_request return 8
[aaaa.bbbb.cccc][X.X.X.X]capwap_90400002 Param-map used: lwa-parameter_map
[aaaa.bbbb.cccc][X.X.X.X]capwap_90400002
```

**State GET_REDIRECT -> GET_REDIRECT**

```
[...]
```

```
[aaaa.bbbb.cccc][X.X.X.X]capwap_90400002
```

**GET rcvd when in GET_REDIRECT state**

[aaaa.bbbb.cccc][X.X.X.X]capwap_90400002

**HTTP GET request**

[aaaa.bbbb.cccc][X.X.X.X]capwap_90400002

**Parse GET, src [X.X.X.X] dst [192.0.2.1] url [https://<virtual-ip-address>:443/login.html?redirect=http:**

[aaaa.bbbb.cccc][X.X.X.X]capwap_90400002 Read complete: parse_request return 10

[aaaa.bbbb.cccc][X.X.X.X]capwap_90400002

**Param-map used: lwa-parameter_map**

[aaaa.bbbb.cccc][X.X.X.X]capwap_90400002

**State GET_REDIRECT -> LOGIN**

[aaaa.bbbb.cccc][X.X.X.X]capwap_90400002

**Sending Webauth login form**

, len 8076
[...]
[aaaa.bbbb.cccc][X.X.X.X]capwap_90400002

**POST rcvd when in LOGIN state**

[aaaa.bbbb.cccc][X.X.X.X]capwap_90400002 get url: /login.html
[aaaa.bbbb.cccc][X.X.X.X]capwap_90400002 Read complete: parse_request return 4
[aaaa.bbbb.cccc][X.X.X.X]capwap_90400002 Param-map used: lwa-parameter_map
[aaaa.bbbb.cccc][X.X.X.X]capwap_90400002 State LOGIN -> AUTHENTICATING
[aaaa.bbbb.cccc][X.X.X.X]capwap_90400002 45876/176 IO state READING -> AUTHENTICATING
[aaaa.bbbb.cccc][X.X.X.X]capwap_90400002 Param-map used: lwa-parameter_map
[aaaa.bbbb.cccc][X.X.X.X]capwap_90400002

**State AUTHENTICATING -> AUTHC_SUCCESS**

A WLC processa informações a serem aplicadas ao cliente final de conexão

<#root>

[aaaa.bbbb.cccc:capwap_90400002]

**Authc success from WebAuth, Auth event success**

[aaaa.bbbb.cccc:capwap_90400002] Raised event

**APPLY_USER_PROFILE**

(14)
[aaaa.bbbb.cccc:capwap_90400002] Raised event RX_METHOD_AUTHC_SUCCESS (3)
[aaaa.bbbb.cccc:capwap_90400002] SM will not send event Template Deactivated to PRE for 0xAE000012
[aaaa.bbbb.cccc:capwap_90400002] SM will not send event Template Deactivated to PRE for 0xAE000012

**Authentication Success.**

Resolved Policy bitmap:4 for client aaaa.bbbb.cccc

Applying Attribute :

**username 0 "cisco"**

Applying Attribute : aaa-author-type 0 1 (0x1)
Applying Attribute : aaa-author-service 0 16 (0x10)
Applying Attribute : clid-mac-addr 0 3a e6 3b 9a fc 4a
Applying Attribute : addr 0 0xac104206
Applying Attribute : addrv6 0 "þ€"
Applying Attribute : addrv6 0 " ?Ì??"
Applying Attribute : addrv6 0 " ?Ì??"
Applying Attribute : addrv6 0 " ?Ì??"
Applying Attribute : target-scope 0 0 [client]
Applying Attribute : audit-session-id 0 "1A4210AC0000001C5B12A51C"
Applying Attribute : aaa-unique-id 0 28 (0x1c)
Applying Attribute : client-iif-id 0 4261415483 (0xfe000a3b)
Applying Attribute :

**vlan-id 0 100 (0xa63)**

Applying Attribute : session-linksec-secured 0 False
Applying Attribute : nas-ip-address 0 0x0
Applying Attribute : nas-ipv6-Address 0 ""
Applying Attribute : interface 0 ""
Applying Attribute : port-type 0 19 [802.11 wireless]
Applying Attribute : nas-port 0 10014 (0x40eba)
Applying Attribute :

**cisco-wlan-ssid 0 "LWA-SSID"**

Applying Attribute :

**wlan-profile-name 0 "LWA-SSID"**

Applying Attribute : dnis 0 "d4-e8-80-1a-30-60:LWA-SSID"
Applying Attribute : formatted-clid 0 "3a-e6-3b-9a-fc-4a"
Applying Attribute : bsn-wlan-id 0 16 (0x10)
Applying Attribute : nas-identifier-wireless 0 "LWA-SSID"
Applying Attribute : timeout 0 86400 (0x15180)
Applying Attribute : priv-lvl 0 1 (0x1)
Applying Attribute : timeout 0 86400 (0x15180)
Applying Attribute :

**method 0 1 [webauth]**

Applying Attribute : clid-mac-addr 0 3a e6 3b 9a fc 4a
Applying Attribute : intf-id 0 2420113410 (0x90400002)
[aaaa.bbbb.cccc:capwap_90400002] auth mgr attr add/change notification is received for attr username(45
[aaaa.bbbb.cccc:capwap_90400002] SM Notified attribute

**Add/Update username cisco**

[aaaa.bbbb.cccc:capwap_90400002]

**Received User-Name cisco for client aaaa.bbbb.cccc**

[aaaa.bbbb.cccc:capwap_90400002] auth mgr attr add/change notification is received for attr auth-domain
[aaaa.bbbb.cccc:capwap_90400002] Method webauth changing state from 'Running' to 'Authc Success'
[aaaa.bbbb.cccc:capwap_90400002] Context changing state from 'Running' to 'Authc Success'

```
[aaaa.bbbb.cccc:capwap_90400002]
```

**Username cisco received**

```
[aaaa.bbbb.cccc:capwap_90400002]
```

**WLAN ID 16 received**

A WLC aplica o perfil de usuário ao cliente final conectado

<#root>

```
Applied User Profile: aaa-author-type 0 1 (0x1)
Applied User Profile: aaa-author-service 0 16 (0x10)
Applied User Profile: clid-mac-addr 0 3a e6 3b 9a fc 4a
Applied User Profile: target-scope 0 0 [client]
Applied User Profile: aaa-unique-id 0 28 (0x1c)
Applied User Profile: client-iif-id 0 4261415483 (0xfe000a3b)
Applied User Profile: vlan-id 0 100 (0xa63)
Applied User Profile:session-linksec-secured 0 False
Applied User Profile: nas-ip-address 0 0x0
Applied User Profile: nas-ipv6-Address 0 ""
Applied User Profile: interface 0 ""
Applied User Profile: port-type 0 19 [802.11 wireless]
Applied User Profile: nas-port 0 10014 (0x40eba)
Applied User Profile:
```

**cisco-wlan-ssid 0 "LWA-SSID"**

```
Applied User Profile:
```

**wlan-profile-name 0 "LWA-SSID"**

```
Applied User Profile:nas-identifier-wireless 0 "LWA-SSID"
Applied User Profile: priv-lvl 0 1 (0x1)
Applied User Profile: method 0 1 [webauth]
Applied User Profile:
```

**clid-mac-addr 0 3a e6 3b 9a fc 4a**

```
Applied User Profile: intf-id 0 2420113410 (0x90400002)
Applied User Profile:
```

**username 0 "cisco"**

```
Applied User Profile: bsn-wlan-id 0 16 (0x10)
Applied User Profile: timeout 0 86400 (0x15180)
Applied User Profile: timeout 0 86400 (0x15180)
MAC: aaaa.bbbb.cccc Link-local bridging not enabled for this client, not checking VLAN validity
[aaaa.bbbb.cccc:capwap_90400002]
```

**User Profile applied successfully - REPLACE**

```
[aaaa.bbbb.cccc:capwap_90400002] auth mgr attr add/change notification is received for attr method(757)
```

```
[aaaa.bbbb.cccc:capwap_90400002]
Raised event AUTHZ_SUCCESS (11)
[aaaa.bbbb.cccc:capwap_90400002]
Context changing state from 'Authc Success' to 'Authz Success'
```

Autenticação da Web Concluída

<#root>

```
MAC: aaaa.bbbb.cccc
L3 Authentication Successful.
 ACL:[]
MAC: aaaa.bbbb.cccc Client auth-interface state transition: S_AUTHIF_WEBAUTH_PENDING ->
S_AUTHIF_WEBAUTH_DONE
```

Atributos AAA Aplicados ao Cliente Final

<#root>

```
[ Applied attribute : username 0 "
cisco
" ]
[ Applied attribute : bsn-wlan-id 0 16 (0x10) ]
[ Applied attribute : timeout 0 86400 (0x15180) ]
[ Applied attribute : timeout 0 86400 (0x15180) ]
[ Applied attribute :bsn-vlan-interface-name 0 "
myvlan
" ]
```

O cliente final alcança o estado Run

<#root>

```
Managed client RUN state notification: aaaa.bbbb.cccc
MAC: aaaa.bbbb.cccc Client state transition: S_CO_L3_AUTH_IN_PROGRESS ->
S_CO_RUN
```

# Cenários comuns de solução de problemas

## Falhas de autenticação

### Considerações

- O portal mostrado diz "Authentication Failed" (Falha na autenticação) após inserir as credenciais corretas.
- A WLC mostra o cliente no estado "Web Auth Pending".
- A página inicial é exibida novamente para o usuário.

### Rastreamentos RA de WLC

<#root>

```
[aaaa.bbbb.cccc][X.X.X.X]capwap_90400002 Param-map used: lwa-parameter_map
[aaaa.bbbb.cccc][X.X.X.X]capwap_90400002 State LOGIN -> AUTHENTICATING
[aaaa.bbbb.cccc][X.X.X.X]capwap_90400002 40828/176 IO state READING -> AUTHENTICATING
[aaaa.bbbb.cccc][X.X.X.X]capwap_90400002
```

**Param-map used: lwa-parameter_map**

```
[aaaa.bbbb.cccc][X.X.X.X]capwap_90400002 State AUTHENTICATING ->
```

**AUTHC_FAIL [INVALID CREDENTIALS]**

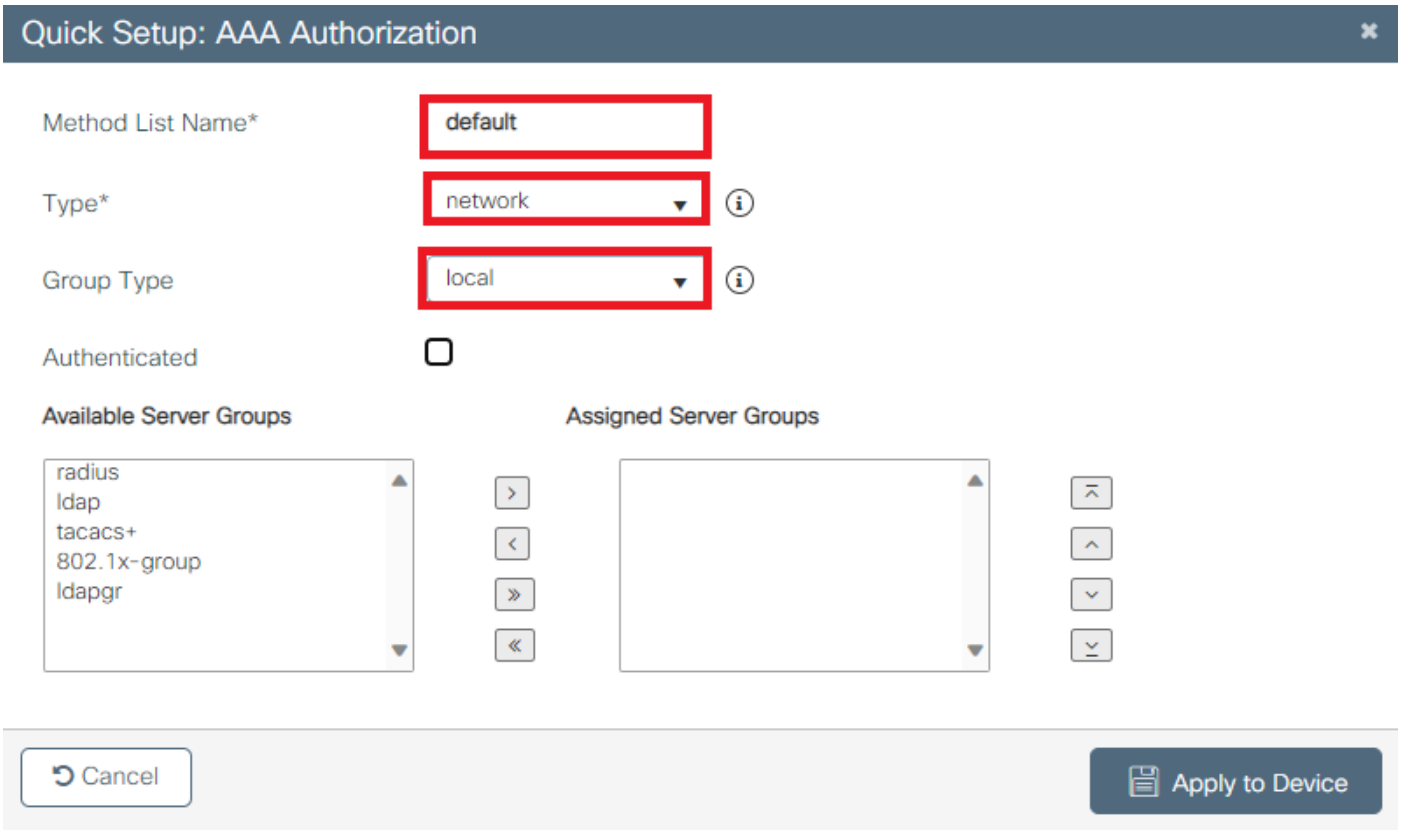
```
[aaaa.bbbb.cccc:capwap_90400002] Authc failure from WebAuth, Auth event fail
[aaaa.bbbb.cccc:capwap_90400002] (Re)try failed method WebAuth - aaaa.bbbb.cccc
[aaaa.bbbb.cccc:capwap_90400002] Method webauth changing state from 'Running' to 'Authc Failed'
```

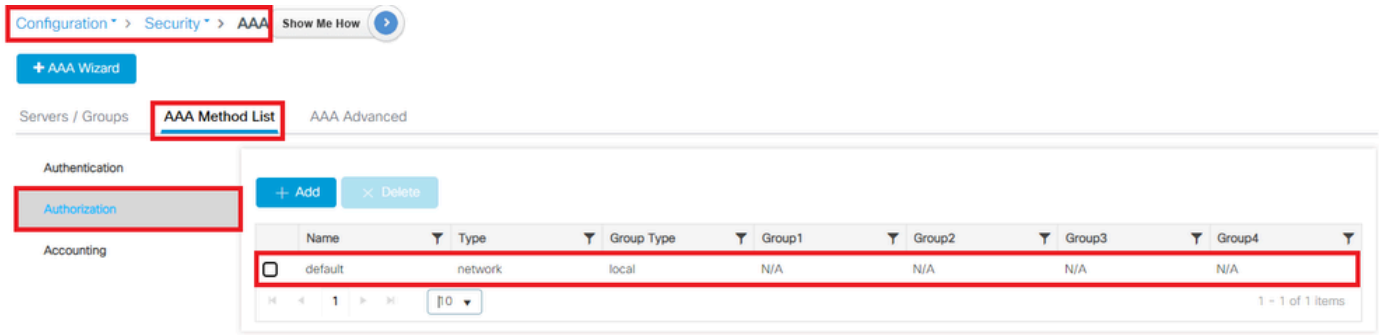
### Soluções recomendadas

Certifique-se de que a lista de métodos AAA padrão para autorização de rede exista na configuração da WLC.

Na GUI:

1. Vá para Configuration > Security > AAA > AAA Method List > Authorization. Clique em + Adicionar.
2. Configure-o como:
    1. Nome da lista de métodos: padrão
    2. Tipo: rede
    3. Tipo de grupo: local
3. Clique em Aplicar ao dispositivo.




Na CLI:

<#root>

```
WLC# configure terminal
WLC(config)# aaa authorization default network local
```

## O portal não é exibido para o usuário, mas o cliente parece conectado

Possível comportamento observado do cliente final

- O cliente final vê seu dispositivo como "Conectado".
- O cliente final não vê o portal.

- O cliente final não insere credenciais.
- O cliente final tem um endereço IP atribuído.
- A WLC mostra o cliente no estado "Run".

Rastreamentos RA de WLC

O cliente recebe um endereço IP atribuído e é imediatamente movido para o estado "Executar" na WLC. Os atributos do usuário mostram apenas a VLAN atribuída ao cliente final.

<#root>

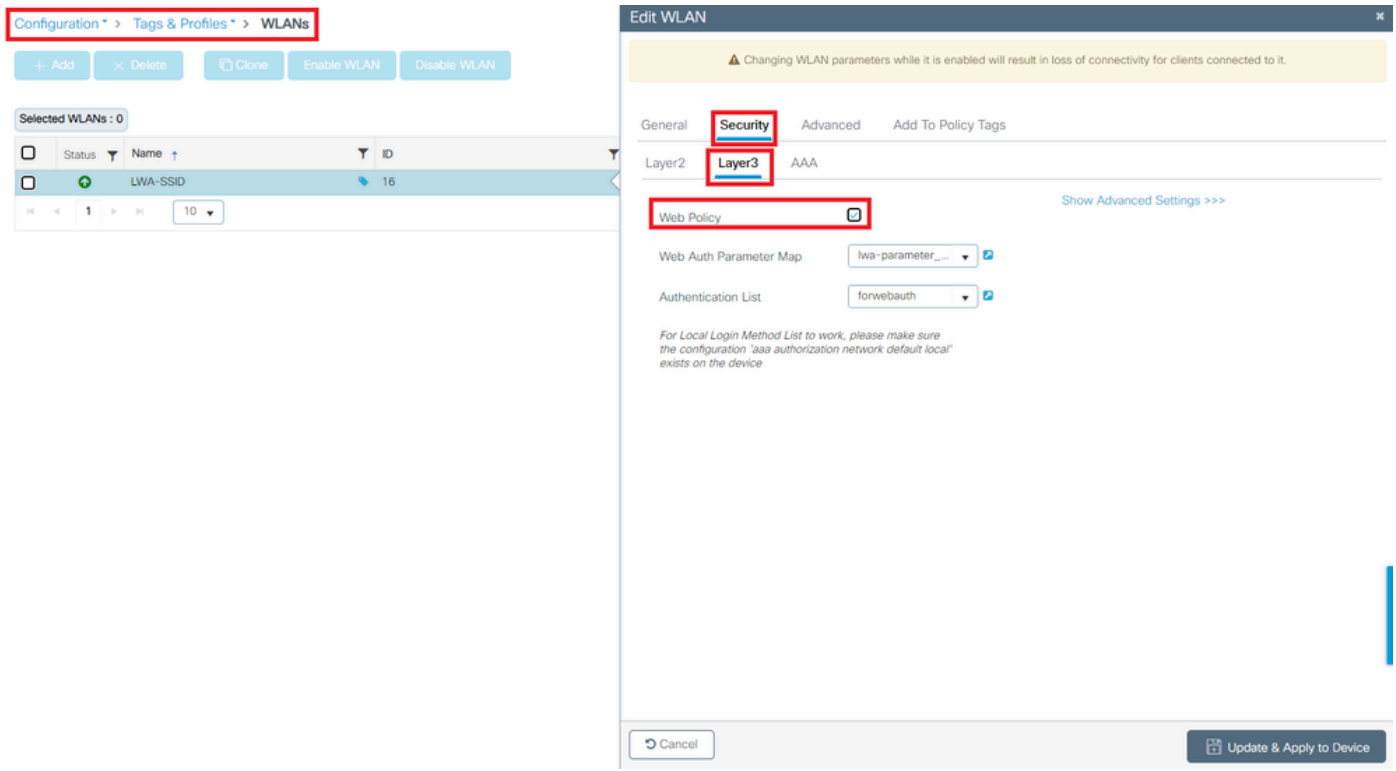
```
MAC: aaaa.bbbb.cccc

Client IP learn successful. Method: DHCP IP: X.X.X.X


[aaaa.bbbb.cccc:capwap_90400002] auth mgr attr add/change notification is received for attr addr(8)
[aaaa.bbbb.cccc:capwap_90400002] SM Notified attribute Add/Update addr X.X.X.X
MAC: aaaa.bbbb.cccc IP-learn state transition:

 S_IPLEARN_IN_PROGRESS -> S_IPLEARN_COMPLETE


MAC: aaaa.bbbb.cccc Received ip learn response. method: IPLEARN_METHOD_DHCP
[ Applied attribute :bsn-vlan-interface-name 0 "

myvlan

" ]
[ Applied attribute : timeout 0 1800 (0x708) ]
MAC: aaaa.bbbb.cccc Client QoS run state handler
Managed client RUN state notification: aaaa.bbbb.cccc
MAC: aaaa.bbbb.cccc Client state transition: S_CO_IP_LEARN_IN_PROGRESS -> S_CO_RUN
```

Soluções recomendadas

Certifique-se de que a política da Web esteja habilitada na WLAN.

Na GUI:

1. Vá para Configuration > Tags & Profiles > WLANs.
2. Selecione as WLANs LWA.
3. Vá para Segurança > Camada 3.
4. Verifique se a caixa de seleção Web Policy está habilitada.




A política da Web precisa ser habilitada

Na CLI:

<#root>

```
WLC# configure terminal


WLC(config)# wlan
```

**<wlan>**

```
WLC(config-wlan)# shutdown
WLC(config-wlan)# security webauth
WLC(config-wlan)# no shutdown
```

## O portal não é exibido para o usuário e o cliente não se conecta

Possível comportamento observado do cliente final

- O cliente final vê que o dispositivo está tentando se conectar continuamente.
- O cliente final não vê o portal.
- O cliente final não tem um endereço IP atribuído.
- A WLC mostra o cliente no estado "Webauth Pending".

Soluções recomendadas

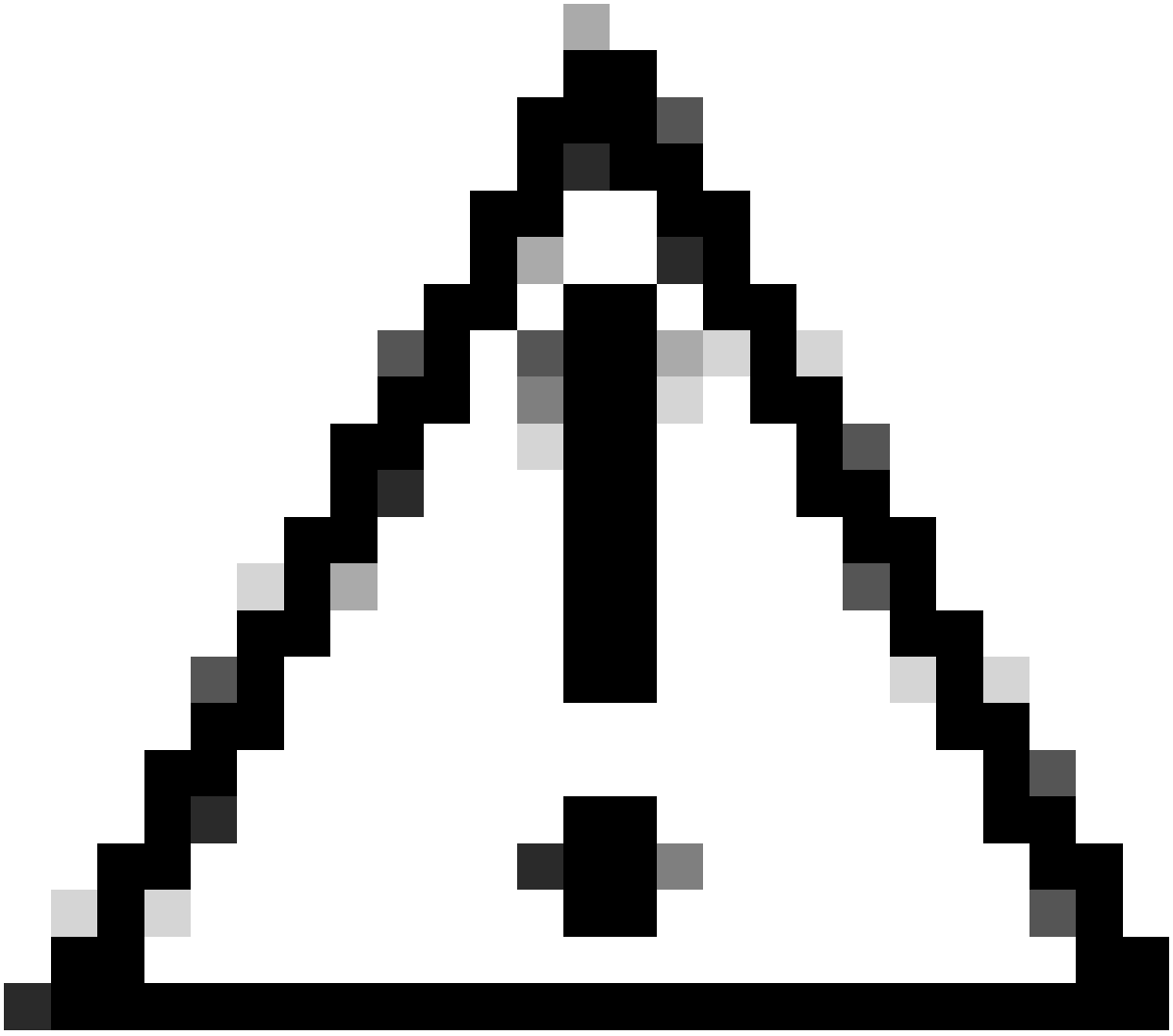
Ative os servidores HTTP/HTTPS necessários. Agora é possível ter mais controle sobre quais

servidores HTTP/HTTPS precisam ser habilitados para se adaptarem totalmente às necessidades da rede. Consulte este link para obter mais informações sobre como configurar solicitações HTTP e HTTPS para autenticação da Web, pois há várias combinações de HTTP suportadas; por exemplo, HTTPs podem ser usados somente para webadmin e HTTP usado para webauth.

Para permitir o gerenciamento administrativo de dispositivos e a autenticação da Web com acesso HTTP e HTTPS, na CLI:

```
WLC# configure terminal
WLC(config)# ip http server
WLC(config)# ip http secure-server
```

---



Cuidado: se ambos os servidores estiverem desativados, não haverá acesso à Interface Gráfica do Usuário (GUI) da WLC.

---

## Os clientes finais não estão obtendo um endereço IP

Possível comportamento observado do cliente final

- Os clientes finais veem que seus dispositivos estão continuamente tentando obter um endereço IP.
- A WLC mostra o cliente no estado "IP Learning".

Rastreamentos RA de WLC

Solicitações de descoberta sem retorno da oferta.

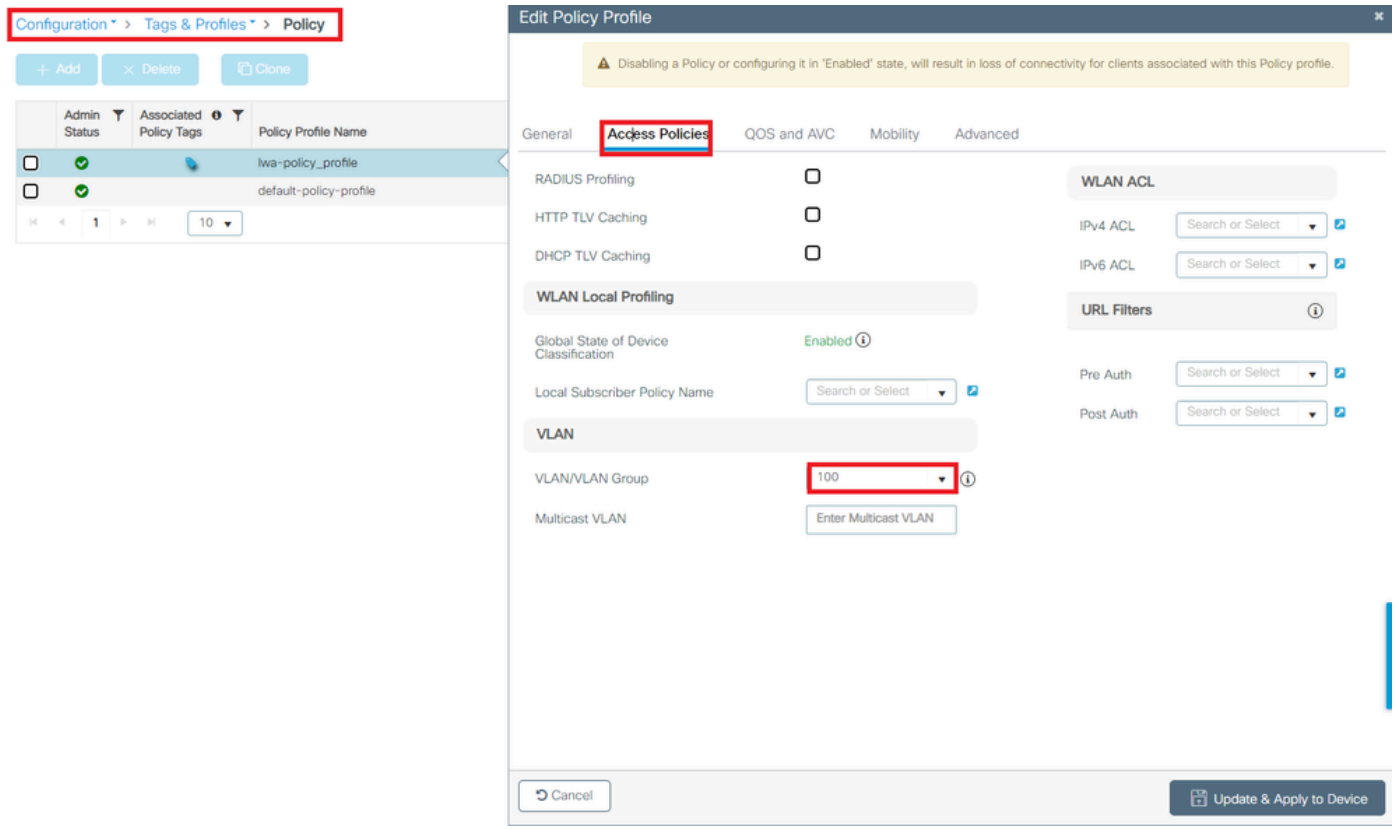
```
RX: DHCPv4 from interface capwap_90400002 on vlan 100 Src MAC: aaaa.bbbb.cccc Dst MAC: ffff.ffff.ffff s
TX: DHCPv4 from interface capwap_90400002 on vlan 100 Src MAC: aaaa.bbbb.cccc Dst MAC: ffff.ffff.ffff s
```

Soluções recomendadas

Primeiro: certifique-se de que o perfil de política tenha a VLAN correta atribuída.

Na GUI:

1. Vá para Configuration > Tags & Profiles > Policy.
2. Selecione o perfil de diretiva usado.
3. Vá para Access Policies (Políticas de acesso).
4. Selecione a VLAN correta.




Na CLI:

<#root>

```
WLC# show wireless profile policy detailed
```

**<policy-profile>**

```
Policy Profile Name :
```

**<policy-profile>**

```
Description :
```

**<policy-profile>**

```
Status : ENABLED
VLAN :
```

***VLAN-selected***

```
[...]

WLC# configure terminal
WLC(config)# wireless profile policy
```

**<policy-profile>**

```
WLC(config-wireless-policy)#
```

**vlan <correct-vlan>**

Segundo: verifique se há um pool DHCP disponível para o usuário em algum lugar. Verifique sua configuração e sua acessibilidade. Os rastreamentos de RA mostram por qual VLAN o processo DHCP DORA está passando. Verifique se essa VLAN é a VLAN correta.

```
DHCPv4 from interface capwap_90400002 on vlan 100 Src MAC: aaaa.bbbb.cccc Dst MAC: ffff.ffff.ffff src_i
DHCPv4 from interface Gi2 on vlan 100 Src MAC: cccc.bbbb.aaaa Dst MAC: aaaa.bbbb.cccc src_ip: Y.Y.Y.Y,
DHCPv4 from interface capwap_90400002 on vlan 100 Src MAC: aaaa.bbbb.cccc Dst MAC: ffff.ffff.ffff src_i
DHCPv4 from interface Gi2 on vlan 100 Src MAC: cccc.bbbb.aaaa Dst MAC: aaaa.bbbb.cccc src_ip: Y.Y.Y.Y,
```

## O portal personalizado não é mostrado ao cliente final

Possível comportamento observado do cliente final

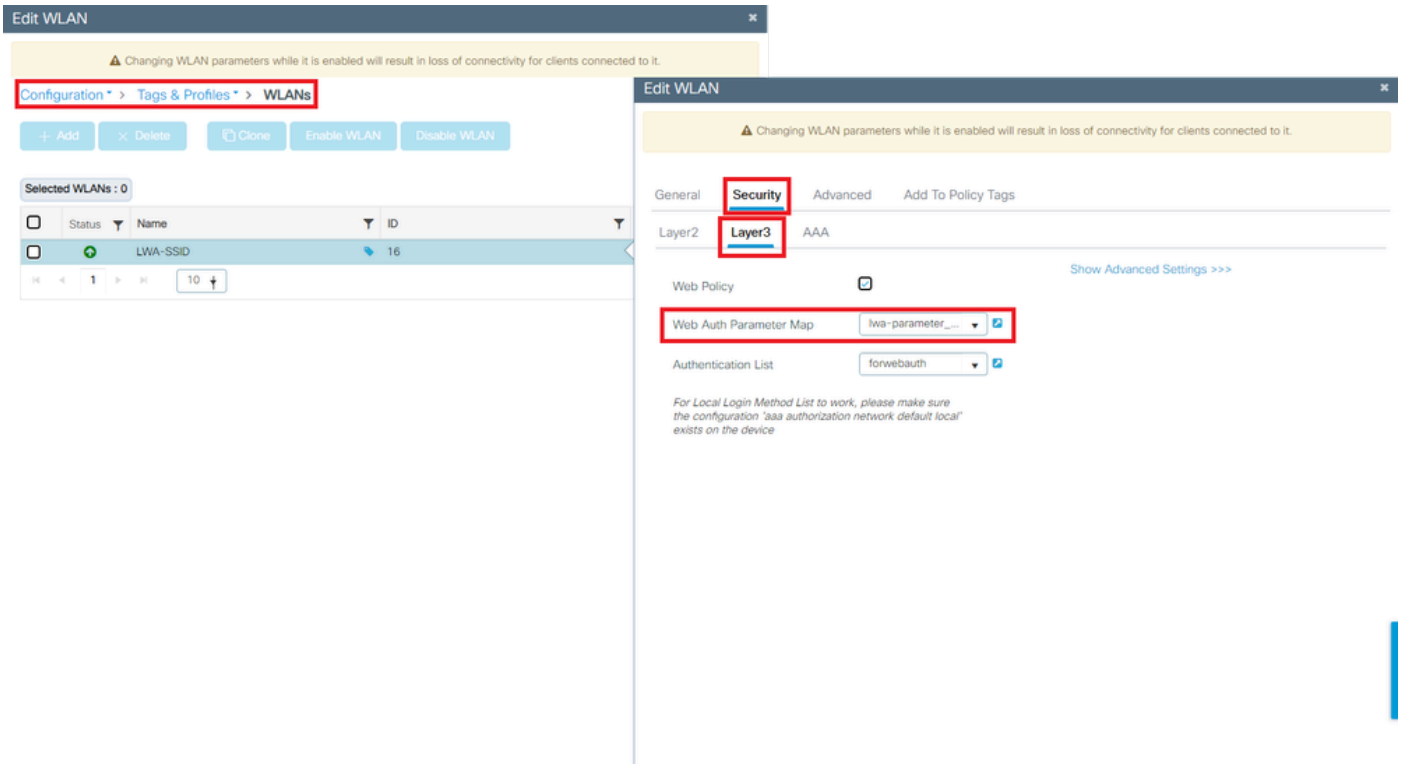
- O portal padrão da WLC é visto.

Soluções recomendadas

Primeiro: verifique se a WLAN está usando o Mapa de Parâmetros de Autenticação da Web personalizado.

Na GUI:

1. Vá para Configuration > Tags & Profiles > WLANs.
2. Selecione a WLAN na lista.
3. Vá para Segurança > Camada 3.
4. Selecione o mapa personalizado do Parâmetro de Autenticação da Web.




Mapa de Parâmetros Personalizado Selecionado

Na CLI:

<#root>

```
WLC# show wlan name LWA-SSID
WLAN Profile Name : LWA-SSID
================================================
[...]
Security:
     Webauth Parameter Map :
```

**<parameter-map>**

```
WLC# configure terminal
WLC(config)# wlan
```

**<wlan>**

```
WLC(config-wlan)# security web-auth parameter-map
```

**<parameter-map>**

Segundo: É importante observar que o download personalizado do portal da Web Cisco.com não funciona com uma interface de programação muito robusta e complicada. Em geral, é recomendável fazer alterações apenas em um nível CSS e talvez adicionar ou remover imagens. Miniaplicativos, PHP, variáveis de modificação, React.js e assim por diante, não são suportados. Se um portal personalizado não for mostrado ao cliente, tente usar as páginas WLC padrão e veja se o problema pode ser replicado. Se o portal for visto com êxito, há algo que não é suportado

nas páginas personalizadas que devem ser usadas.

Terceiro: Se estiver usando um EWC (Controlador sem fio incorporado), é recomendável usar a CLI para adicionar as páginas personalizadas para garantir que sejam exibidas corretamente:

<#root>

```
EWC# configure terminal
EWC(config)# parameter-map type
```

**<parameter-map>**

```
EWC(config-params-parameter-map)# custom-page login device flash:loginsantosh.html
EWC(config-params-parameter-map)# custom-page login expired device flash:loginexpire.html
EWC(config-params-parameter-map)# custom-page failure device flash:loginfail.html
EWC(config-params-parameter-map)# custom-page success device flash:loginsucess.html
EWC(config-params-parameter-map)# end
```

## O portal personalizado não é mostrado corretamente ao cliente final

Possível comportamento observado do cliente final

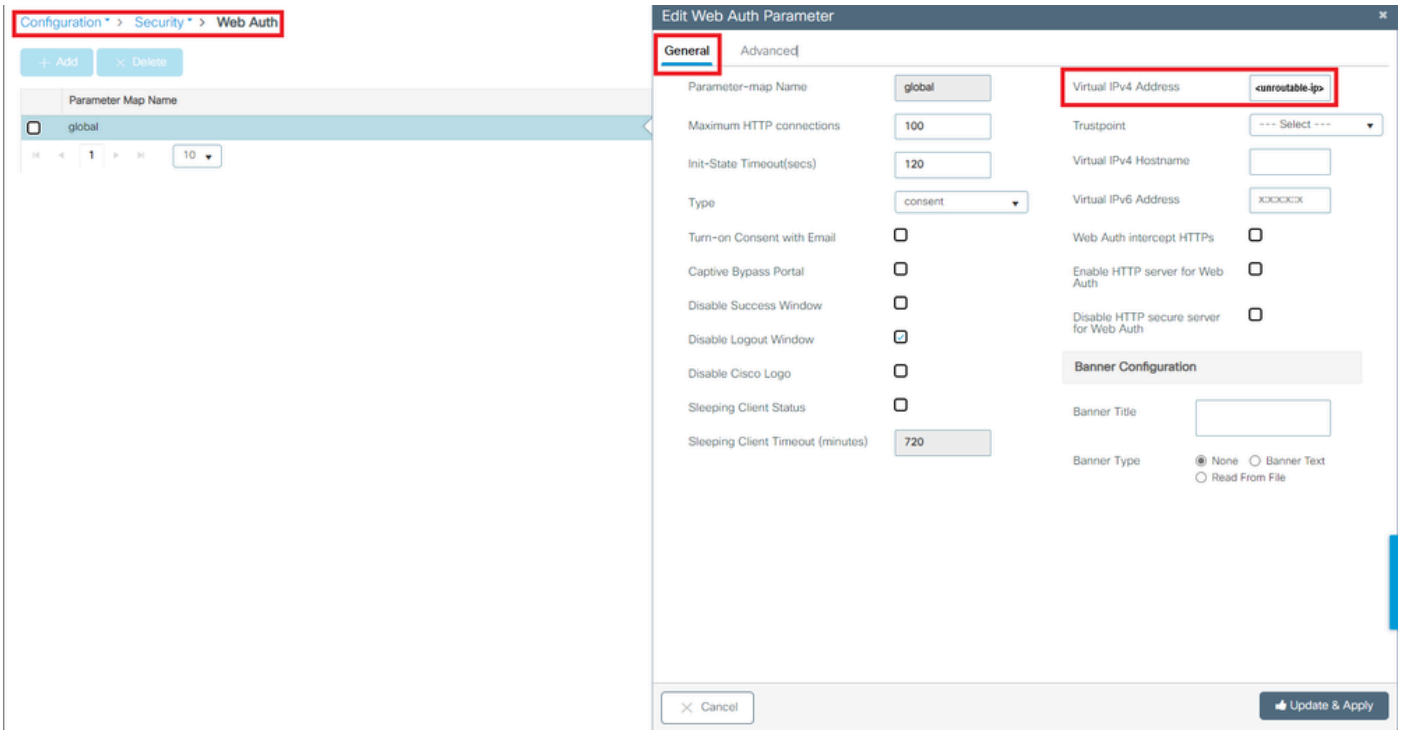
- O portal personalizado não é renderizado corretamente (ou seja, as imagens não são exibidas).

Soluções recomendadas

Certifique-se de que o mapa de parâmetros globais tenha um endereço IP virtual atribuído.

Na GUI:

1. Vá para Configuration > Security > Web Auth.
2. Selecione o mapa de parâmetros global na lista.
3. Adicione um endereço IP virtual não roteável.




Endereço IP Virtual no Mapa de Parâmetros Globais Definido como um Endereço IP Não Roteável

## Na CLI:

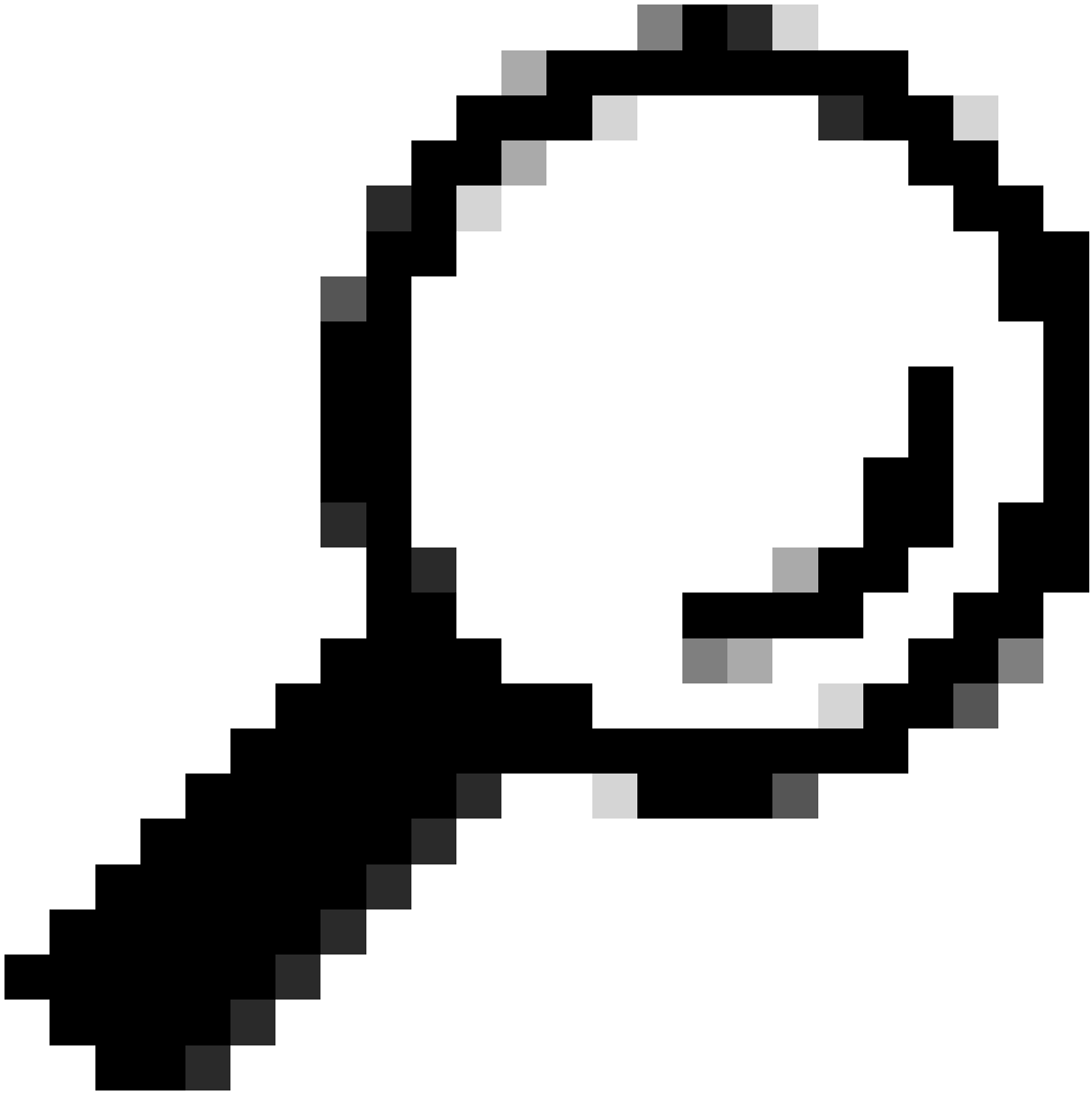
### <#root>

```
WLC# show parameter-map type webauth global
Parameter Map Name : global
[...]
Virtual-ipv4 :
```

**<unroutable-ip>**

```
[...]

WLC# configure terminal
WLC(config)# parameter-map type webauth global
WLC(config-params-parameter-map)# virtual-ip ipv4
```

**<unroutable-ip>**



Dica: o endereço IP virtual serve como o endereço de redirecionamento para a página de login da autenticação da Web. Nenhum outro dispositivo na rede deve ter o mesmo IP, ele não deve ser mapeado para uma porta física, nem existir em qualquer tabela de roteamento. Portanto, é recomendável configurar o IP virtual como um endereço IP não roteável, somente aqueles que estão no RFC5737 podem ser usados.

## O portal diz que "Sua conexão não é segura/verificar assinatura falhou"

Possível comportamento observado do cliente final

- Ao abrir o portal, o cliente vê um erro dizendo que a conexão não é segura.
- Espera-se que o portal use um certificado.

O que você precisa saber

Se for esperado que o portal seja exibido em HTTPS, isso significa que ele precisa usar um certificado SSL (Secure Socket Layer). Esse certificado deve ser emitido por uma Autoridade de Certificação (CA) de terceiros para validar que o domínio é de fato real; fornecendo confiança aos clientes finais ao inserir suas credenciais e/ou visualizar o portal. Para carregar um certificado para a WLC, consulte este documento.

Soluções recomendadas

Primeiro: reinicie os serviços HTTP/HTTPS desejados. Agora é possível ter mais controle sobre quais servidores HTTP/HTTPS precisam ser habilitados para se adaptarem totalmente às necessidades da rede. Consulte este link para obter mais informações sobre como configurar solicitações HTTP e HTTPS para autenticação da Web.

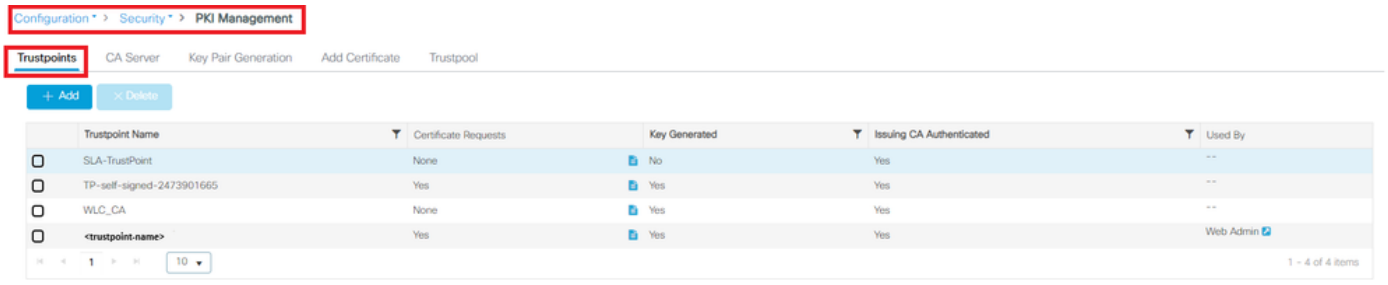
Na CLI:

```
WLC# configure terminal
WLC(config)# no ip http server
WLC(config)# no ip http secure-server
WLC(config)# ip http server
WLC(config)# ip http secure-server
```

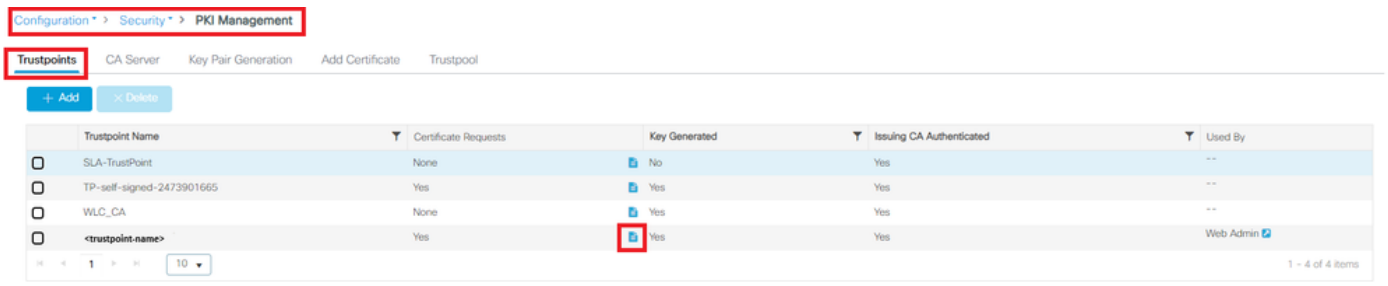
Segundo: verifique se o certificado foi carregado corretamente para a WLC e se sua data de validade está correta.

Na GUI:

1. Vá para Configuration > Security > PKI Management
2. Procurar o ponto de confiança na lista
3. Verificar seus detalhes




Verifique se o ponto de confiança



existeVerifique o ponto de confiança



DetailsCheckTrustpoint Validade

Na CLI:

<#root>

```
WLC# show crypto pki certificate
```

**[<certificate>]**

```
CA Certificate
  Status: Available
  Certificate Serial Number (hex): 01
  Certificate Usage: Signature
  Issuer:
    cn=<Common Name>
    o=<Organizational Unit>
  Subject:
    cn=<Common Name>
    o=<Organizational Unit>
  Validity Date:
```

**start date: <start-date>**

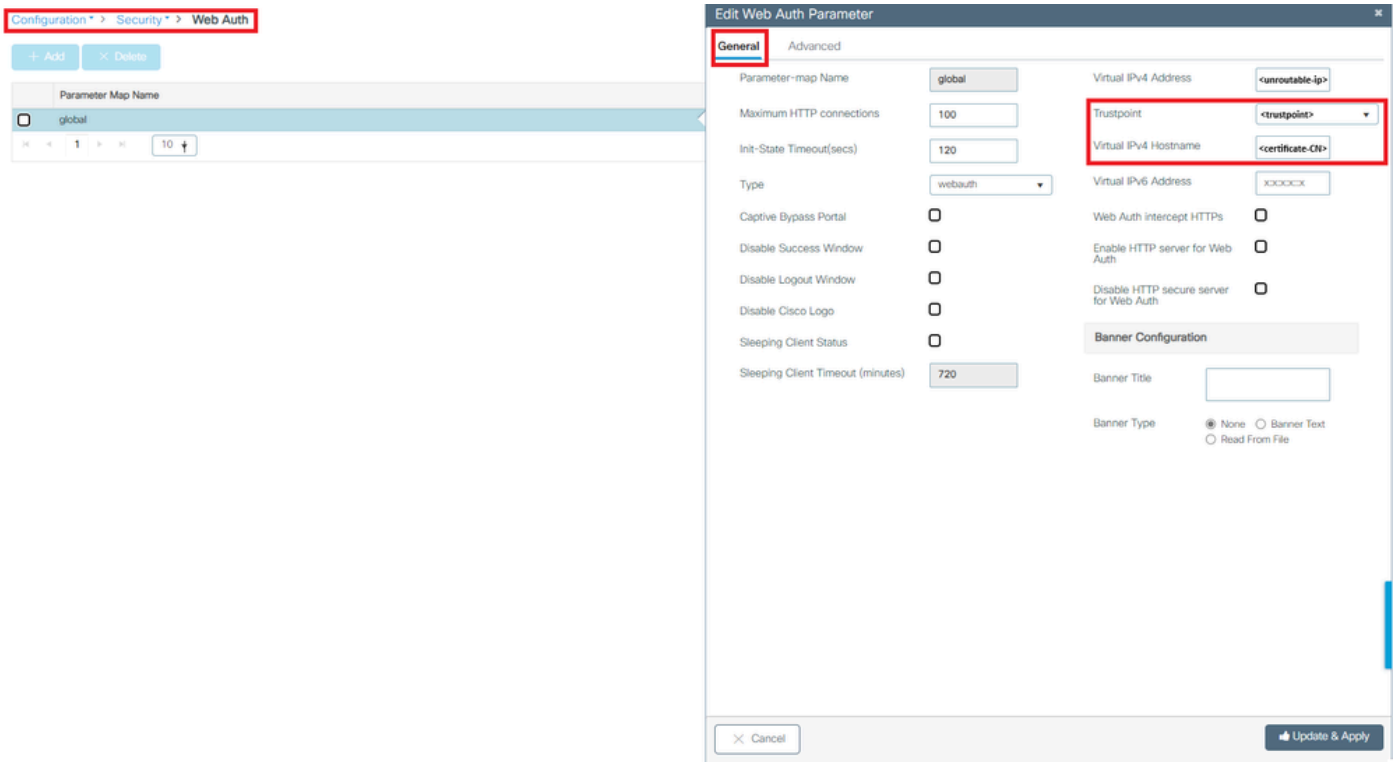
**end date: <end-date>**

**Associated Trustpoints: <trustpoint>**

Terceiro: certifique-se de que o certificado correto selecionado para uso no mapa de parâmetros WebAuth e que o nome de host IPv4 virtual corresponda ao nome comum (CN) no certificado.

Na GUI:

1. Vá para Configuration > Security > Web Auth.
2. Selecione o mapa de parâmetros usado na lista.
3. Verifique se o ponto confiável e o nome de host IPv4 virtual estão corretos.




Verifique o ponto de confiança e o nome de host IPv4 virtual

Na CLI:

<#root>

```
WLC# show run | section paramter-map type
```

**<type> <name>**

```
parameter-map type
```

**<type> <name>**

```
[...]
virtual-ip ipv4
```

**<unroutable-ip> <certificate-common-name>**

```
trustpoint
```

**<trustpoint>**

# Informações Relacionadas

- Configurar Autenticação da Web Local
- Autenticação baseada na Web (EWC)
- Personalizar o portal de autenticação da Web no Catalyst 9800 WLC
- Gerar e fazer download de certificados CSR em WLCs Catalyst 9800
- Configurando interfaces virtuais

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.