Resolución de problemas comunes con LWA en los WLC 9800

Contenido

Introducción

Este documento describe los problemas comunes con los clientes que se conectan a una WLAN con autenticación Web local (LWA).

Prerequisites

Requirements

Cisco recomienda tener conocimientos básicos sobre:

- Cisco Wireless LAN Controller (WLC) serie 9800.
- Comprensión general de la autenticación Web local (LWA) y su configuración.

Componentes Utilizados

La información de este documento se basa en las siguientes versiones de software y hardware:

- WLC 9800-CL
- Punto de acceso Cisco 9120AXI
- 9800 WLC Cisco IOS® XE versión 17.9.3

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

LWA es un tipo de autenticación WLAN que se puede configurar en el WLC donde el cliente final que intenta conectar, después de que seleccionen el WLAN de la lista, presenta un portal al usuario. En este portal, el usuario puede introducir un nombre de usuario y una contraseña (dependiendo de la configuración seleccionada) para finalizar la conexión a la WLAN.

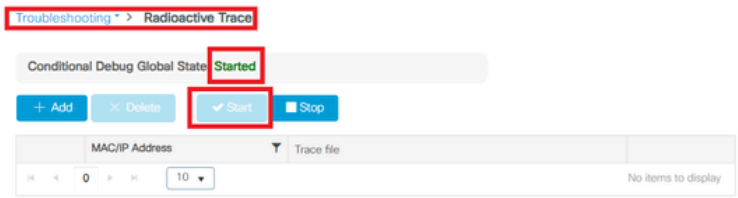
Consulte la guía de configuración Configure Local Web Authentication para obtener más información sobre cómo configurar LWA en el WLC 9800.

Rastreos radiactivos (RA) en el 9800 WLC

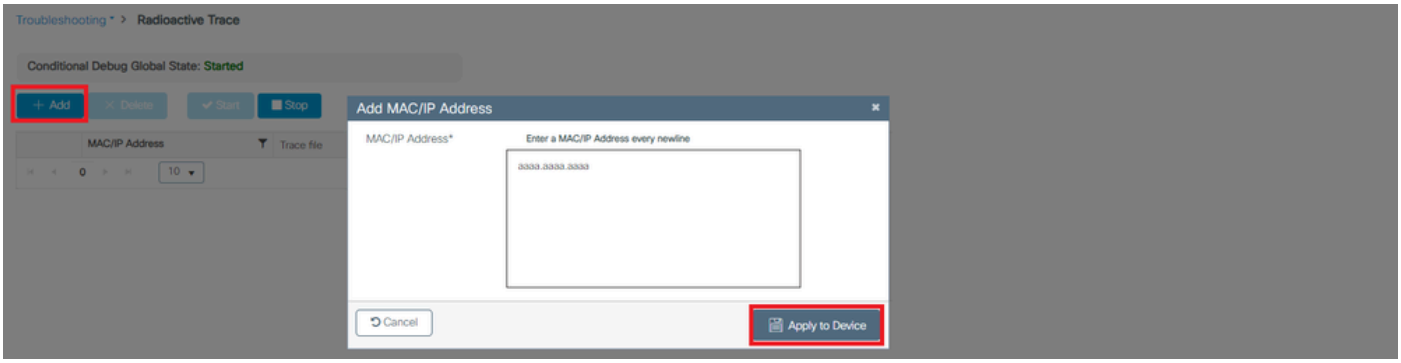
Los rastros radiactivos son una gran herramienta de troubleshooting que se puede utilizar cuando la troubleshooting de diversos problemas con el WLC y la conectividad del cliente. Para recolectar rastros de RA, siga estos pasos:

Desde la GUI:

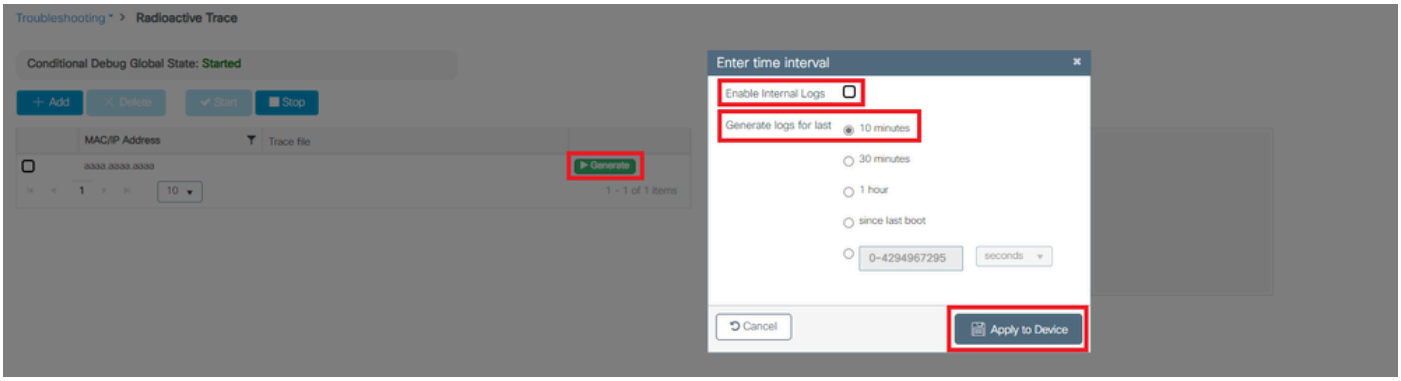
1. Vaya a Troubleshooting > Radioactive Trace.
2. Haga clic en Start para habilitar el estado global de depuración condicional.
3. Haga clic en + Agregar. Se abre una ventana emergente. Introduzca la dirección MAC del cliente. Se acepta cualquier formato de dirección MAC (aabb.ccdd.eeff, AABB.CCDD.EEEE, aa:bb:cc:dd:ee:ff, o AA:BB:CC:DD:EE:FF). A continuación, haga clic en Aplicar al dispositivo.
4. Haga que el cliente reproduzca el problema 3 ó 4 veces.
5. Una vez reproducido el problema, haga clic en Generar.
6. Se abre una nueva ventana emergente. Generar registros de los últimos 10 minutos. (En este caso, no es necesario activar los registros internos). Haga clic en Apply to Device y espere a que se procese el archivo.
7. Una vez generado el archivo, haga clic en el icono Download.



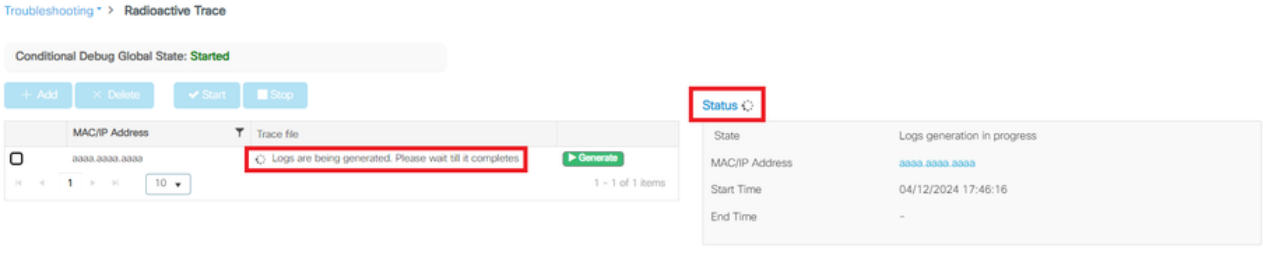
Habilitar depuración condicional



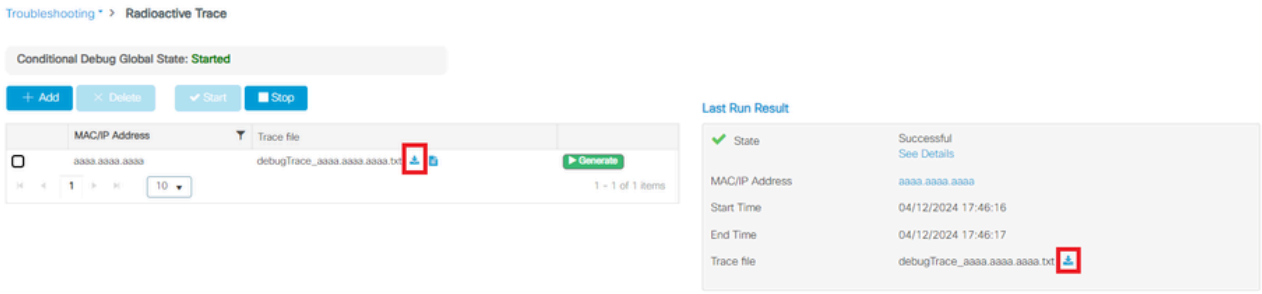
Agregar una dirección MAC de cliente



Generar registros de los últimos 10 minutos



Espere a que se genere el archivo



Descargar el archivo

Desde la CLI:

<#root>

```
WLC# debug wireless mac
```

<mac-address>

```
 monitor-time 600
```

Se generará un nuevo archivo en la memoria de inicialización llamado ra_trace_MAC_<mac-address>_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log

<#root>

```
WLC# more bootflash:
```

ra_trace_MAC_<mac-address>_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log

Copie el archivo en un servidor externo para su análisis

<#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 obtener más información sobre Radioactive Tracing, consulte este enlace.

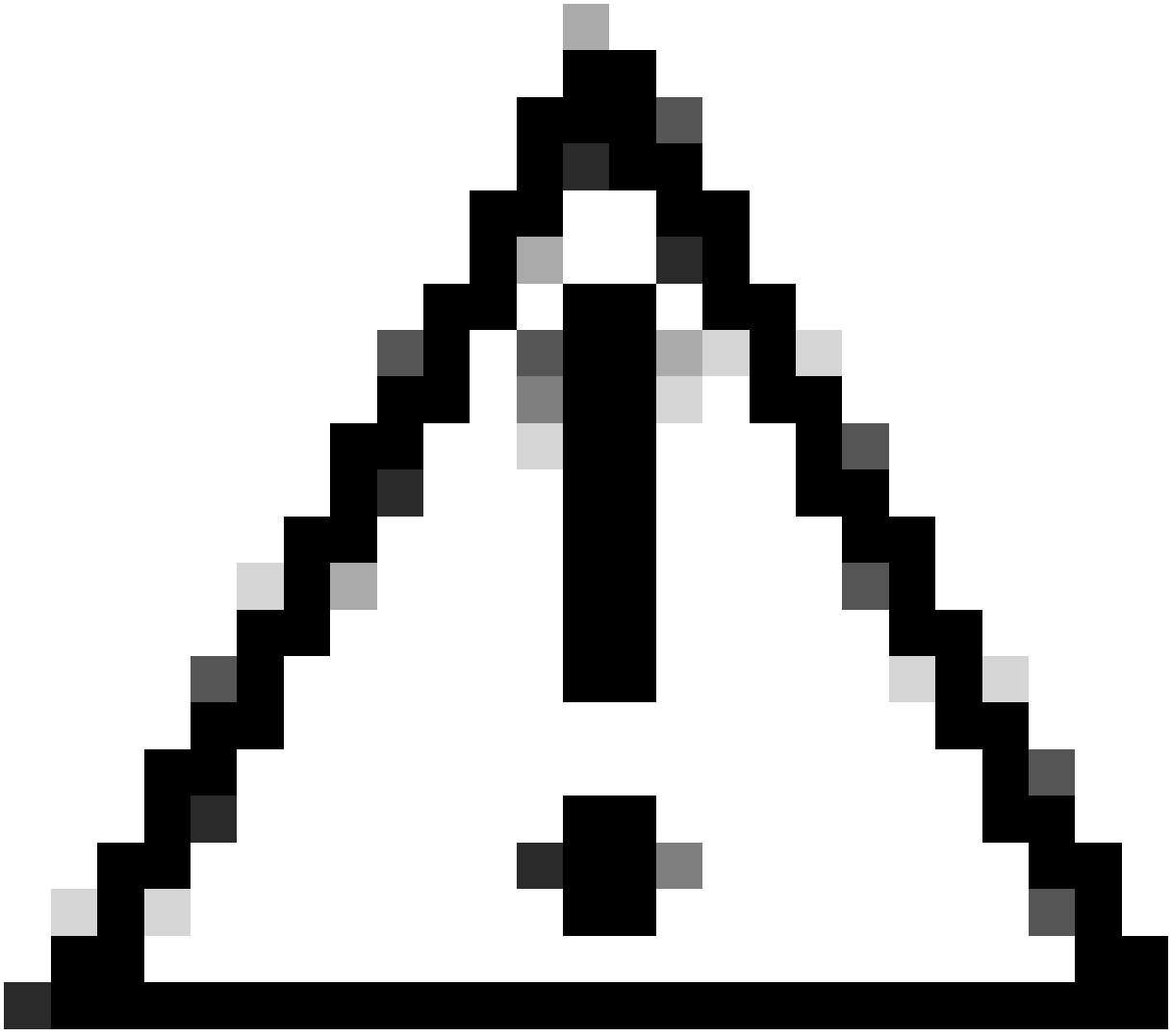
Flujo esperado

Consulte la información para comprender el escenario de trabajo de LWA.

Etapas por las que pasa el cliente desde la perspectiva del cliente

1. El cliente final se asocia a la WLAN.
2. El cliente obtiene una dirección IP asignada.
3. El portal se presenta al cliente final.
4. El cliente final introduce las credenciales de inicio de sesión.
5. El cliente final está autenticado.
6. El cliente final puede navegar por Internet.

Etapas por las que pasa el cliente desde la perspectiva del WLC



Precaución: muchos registros del seguimiento de Radio Active (RA) se omitieron por motivos de simplicidad.

El cliente final se asocia a la 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

Autenticación 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

El cliente obtiene una dirección IP asignada

<#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

Autenticación 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
```

El cliente obtiene una dirección 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

Procesamiento del 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

El WLC procesa la información que se aplicará al cliente final que se conecta

<#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

WLC aplica el perfil de usuario al 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'

La autenticación web ha finalizado

<#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 al 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

"]

El cliente final alcanza el estado de ejecución

<#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

Escenarios comunes de solución de problemas

Errores de autenticación

Consideraciones

- El portal mostrado indica "Error de autenticación" después de introducir las credenciales correctas.
- El WLC muestra al cliente en el estado "Pendiente de la autenticación Web".
- La página inicial de bienvenida se muestra de nuevo al usuario.

WLC RA Traces

<#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]

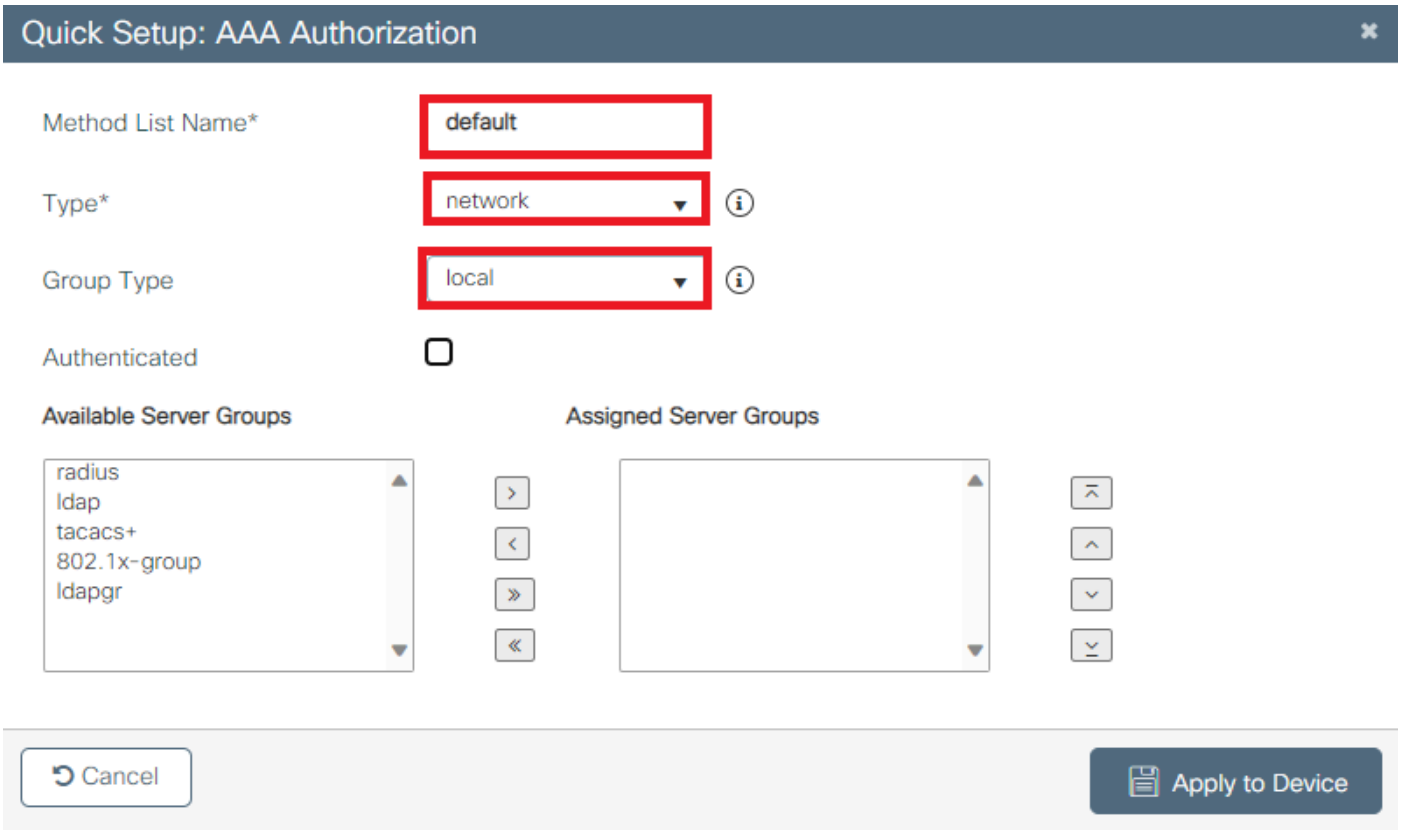
```
[aaaa.bbbb.cccc:capwap_90400002] Authc failure from WebAuth, Auth event fail
[aaaa.bbbb.cccc:capwap_90400002] (Re)try failed method WebAuth - aaaa.bbbb.cccc
[aaaa.bbbb.cccc:capwap_90400002] Method webauth changing state from 'Running' to 'Authc Failed'
```

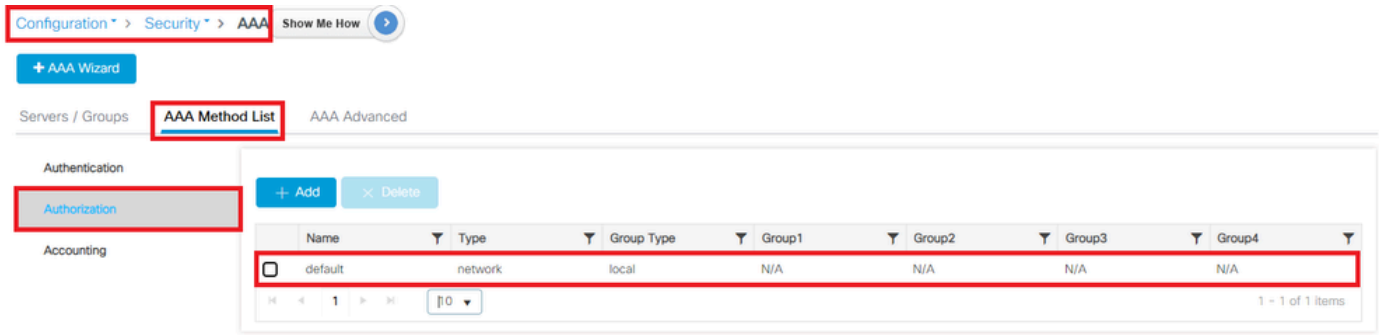
Soluciones recomendadas

Asegúrese de que la lista de métodos AAA predeterminada para la autorización de red exista en la configuración del WLC.

Desde la GUI:

1. Vaya a Configuration > Security > AAA > AAA Method List > Authorization . Haga clic en + Agregar.
2. Configúrelo como:
    1. Nombre de lista de métodos: predeterminado
    2. Tipo: red
    3. Tipo de grupo: local
3. Haga clic en Aplicar al dispositivo.





Desde la CLI:

<#root>

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

El portal no se muestra al usuario, pero el cliente aparece conectado

Comportamiento posible experimentado por el cliente final

- El cliente final ve su dispositivo como "conectado".
- El cliente final no ve el portal.

- El cliente final no introduce credenciales.
- El cliente final tiene una dirección IP asignada.
- El WLC muestra al cliente en el estado "Run".

WLC RA Traces

El cliente obtiene una dirección IP asignada y se mueve inmediatamente al estado "Run" en el WLC. Los atributos de usuario solo muestran la VLAN asignada al cliente final.

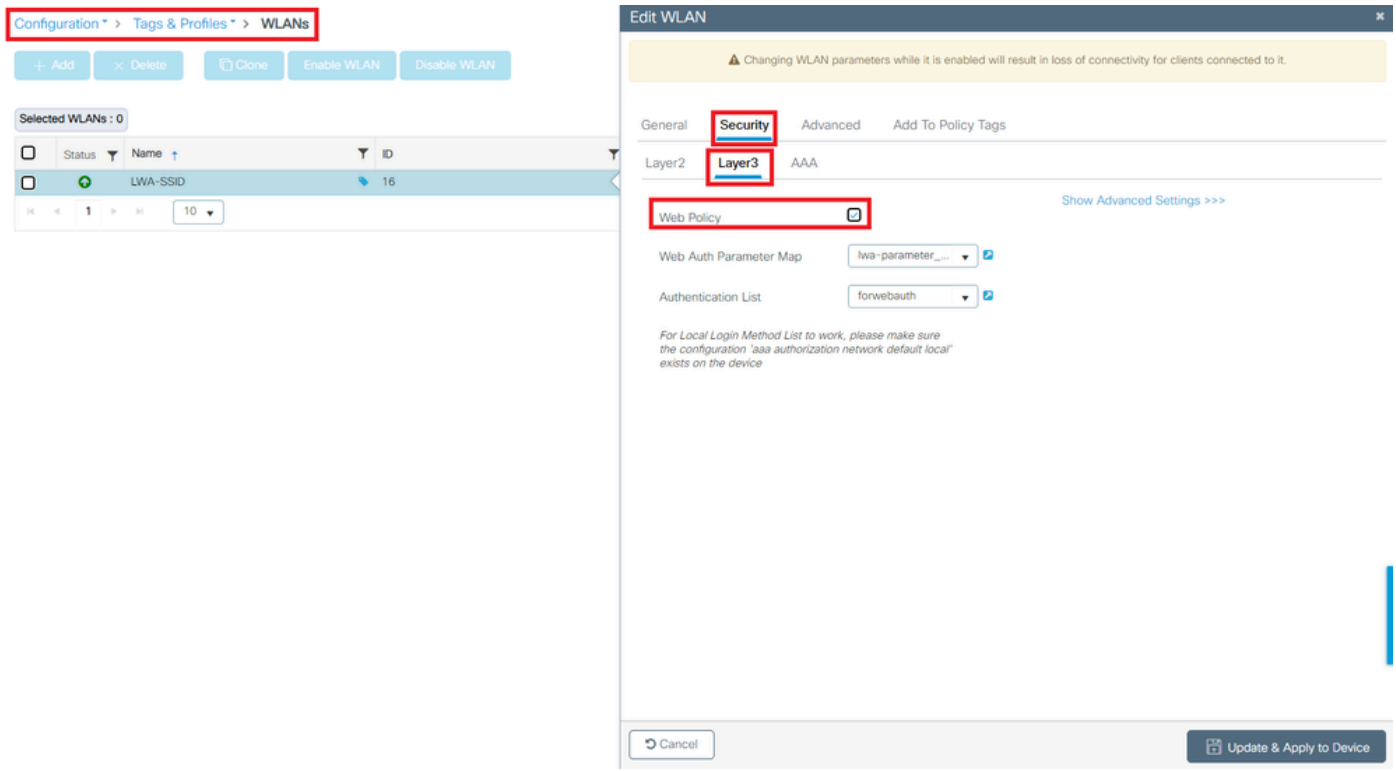
```
<#root>

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
```

Soluciones recomendadas

Asegúrese de que la política web esté habilitada en la WLAN.

Desde la GUI:

1. Vaya a Configuration > Tags & Profiles > WLANs.
2. Seleccione las WLANs LWA.
3. Vaya a Seguridad > Capa 3.
4. Asegúrese de que la casilla de verificación Web Policy esté habilitada.



La política web debe estar habilitada

Desde la CLI:

<#root>

```
WLC# configure terminal


WLC(config)# wlan
```

<wlan>

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

El portal no se muestra al usuario y el cliente no se conecta

Comportamiento posible experimentado por el cliente final

- El cliente final ve que su dispositivo está intentando conectarse continuamente.

- El cliente final no ve el portal.
- El cliente final no tiene una dirección IP asignada.
- El WLC muestra al cliente en el estado "Webauth pendiente".

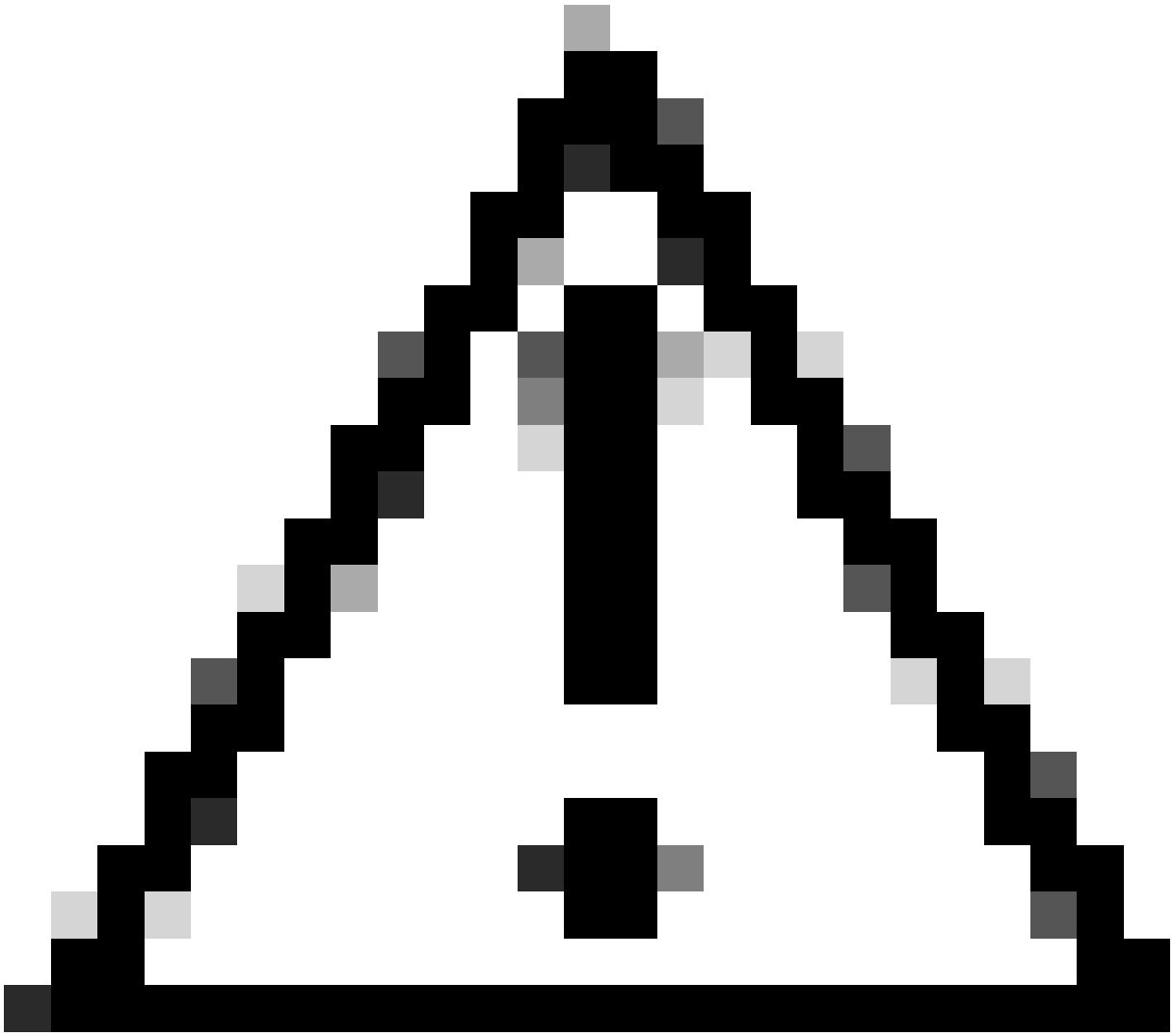
Soluciones recomendadas

Active los servidores HTTP/HTTPS necesarios. Ahora es posible tener un mayor control sobre

qué servidores HTTP/HTTPS deben activarse para adaptarse completamente a las necesidades de la red. Consulte este enlace para obtener más información sobre la configuración de solicitudes HTTP y HTTPS para la autenticación web, ya que se admiten varias combinaciones HTTP; por ejemplo, los HTTP se pueden utilizar solo para webadmin y los HTTP se pueden utilizar para webauth.

Para permitir la administración de dispositivos y la autenticación web con acceso HTTP y HTTPS, desde la CLI:

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



Precaución: Si ambos servidores están inhabilitados, no hay acceso a la interfaz gráfica de usuario (GUI) del WLC.

Los clientes finales no obtienen una dirección IP

Comportamiento posible experimentado por el cliente final

- Los clientes finales ven que su dispositivo está intentando continuamente obtener una dirección IP.
- El WLC muestra al cliente en el estado "IP Learning".

WLC RA Traces

Solicitudes de descubrimiento sin devolución de oferta.

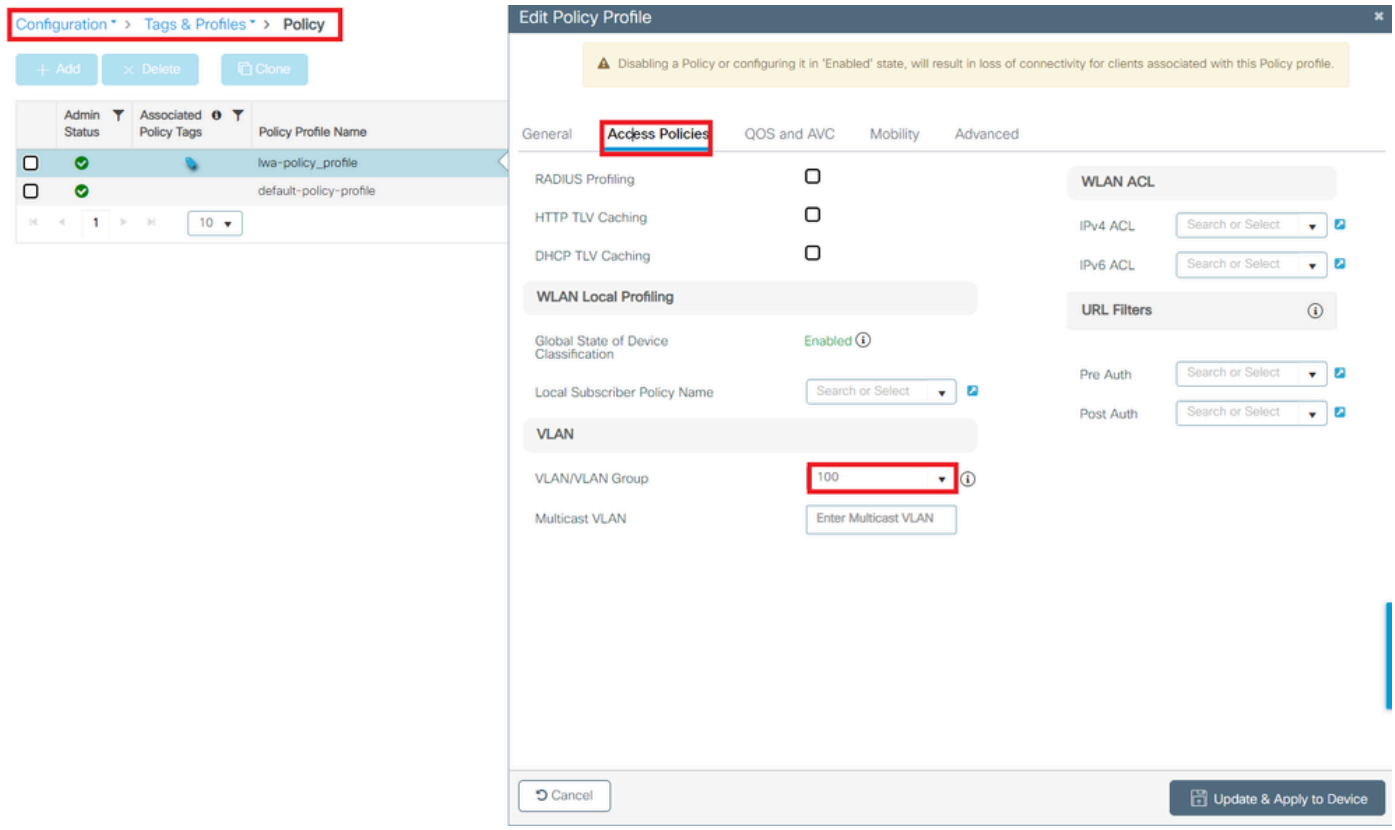
```
RX: DHCPv4 from interface capwap_90400002 on vlan 100 Src MAC: aaaa.bbbb.cccc Dst MAC: ffff.ffff.ffff s
TX: DHCPv4 from interface capwap_90400002 on vlan 100 Src MAC: aaaa.bbbb.cccc Dst MAC: ffff.ffff.ffff s
```

Soluciones recomendadas

Primero: Asegúrese de que el perfil de política tenga asignada la VLAN correcta.

Desde la GUI:

1. Vaya a Configuración > Etiquetas y perfiles > Política.
2. Seleccione el perfil de directiva utilizado.
3. Vaya a Políticas de acceso.
4. Seleccione la VLAN adecuada.



Desde la 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: Asegúrese de que haya un conjunto DHCP disponible para el usuario en algún lugar. Compruebe su configuración y su disponibilidad. Los seguimientos de RA muestran bajo qué proceso DORA DHCP de VLAN está pasando. Asegúrese de que esta VLAN sea la VLAN correcta.

```
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,
```

El portal personalizado no se muestra al cliente final

Comportamiento posible experimentado por el cliente final

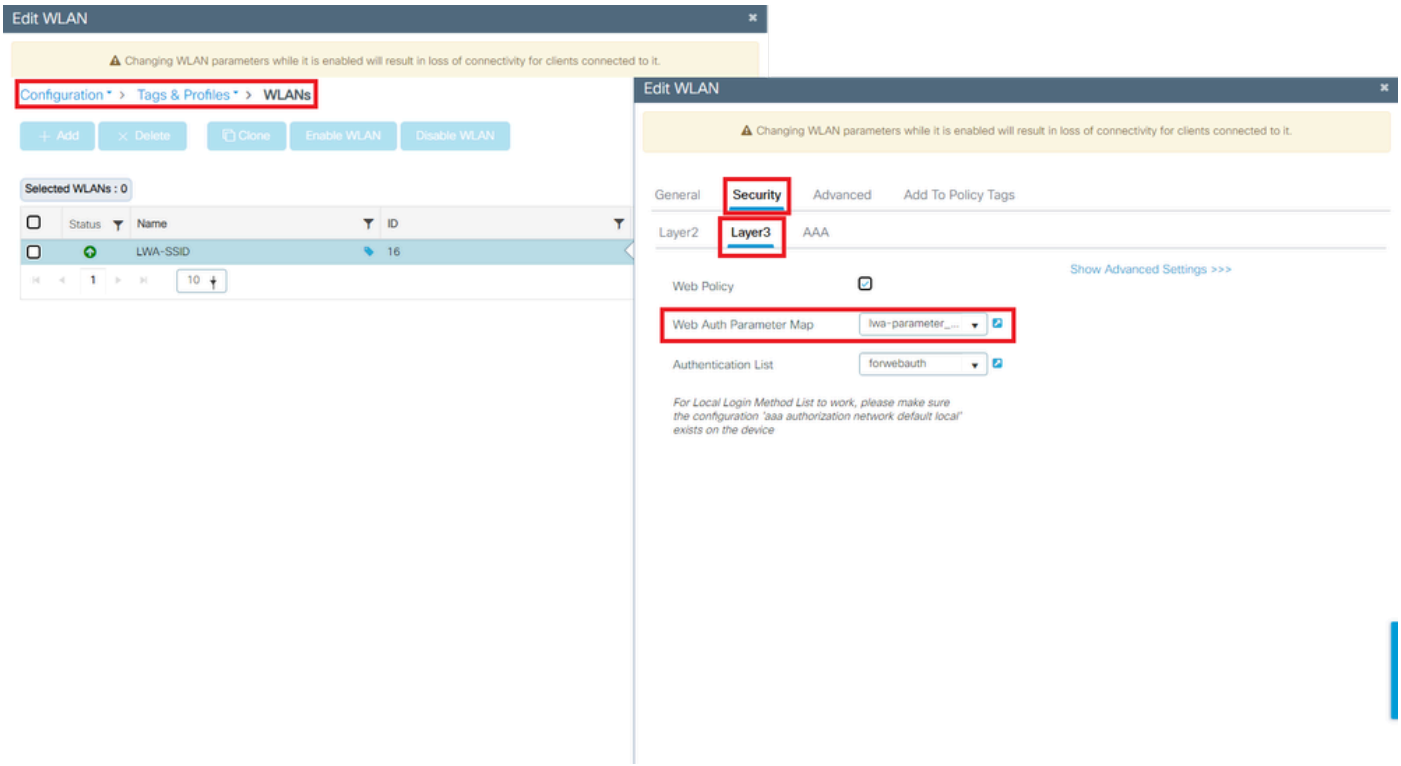
- Se ve el portal predeterminado del WLC.

Soluciones recomendadas

Primero: Asegúrese de que la WLAN esté utilizando el mapa de parámetro de autenticación Web personalizado.

Desde la GUI:

1. Vaya a Configuration > Tags & Profiles > WLANs.
2. Seleccione la WLAN en la lista.
3. Vaya a Seguridad > Capa 3.
4. Seleccione el mapa de parámetro de autenticación Web personalizado.



Mapa de parámetro personalizado seleccionado

Desde la 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: Es importante tener en cuenta que la descarga personalizada desde el portal web de Cisco.com no funciona con una interfaz de programación muy sólida y complicada. Generalmente se recomienda hacer cambios solamente en un nivel CSS y quizás agregar o quitar imágenes. No se admiten applets, PHP, variables de modificación, React.js, etc. Si un portal personalizado no se muestra al cliente, intente utilizar las páginas WLC predeterminadas y vea si el problema se puede replicar. Si el portal se ve con éxito, entonces hay algo que no se soporta en las páginas

personalizadas que se supone que se deben utilizar.

Tercero: Si utiliza un EWC (Controlador Inalámbrico Integrado) se sugiere utilizar la CLI para agregar las páginas personalizadas para asegurarse de que se muestran correctamente:

<#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
```

El portal personalizado no se muestra correctamente al cliente final

Comportamiento posible experimentado por el cliente final

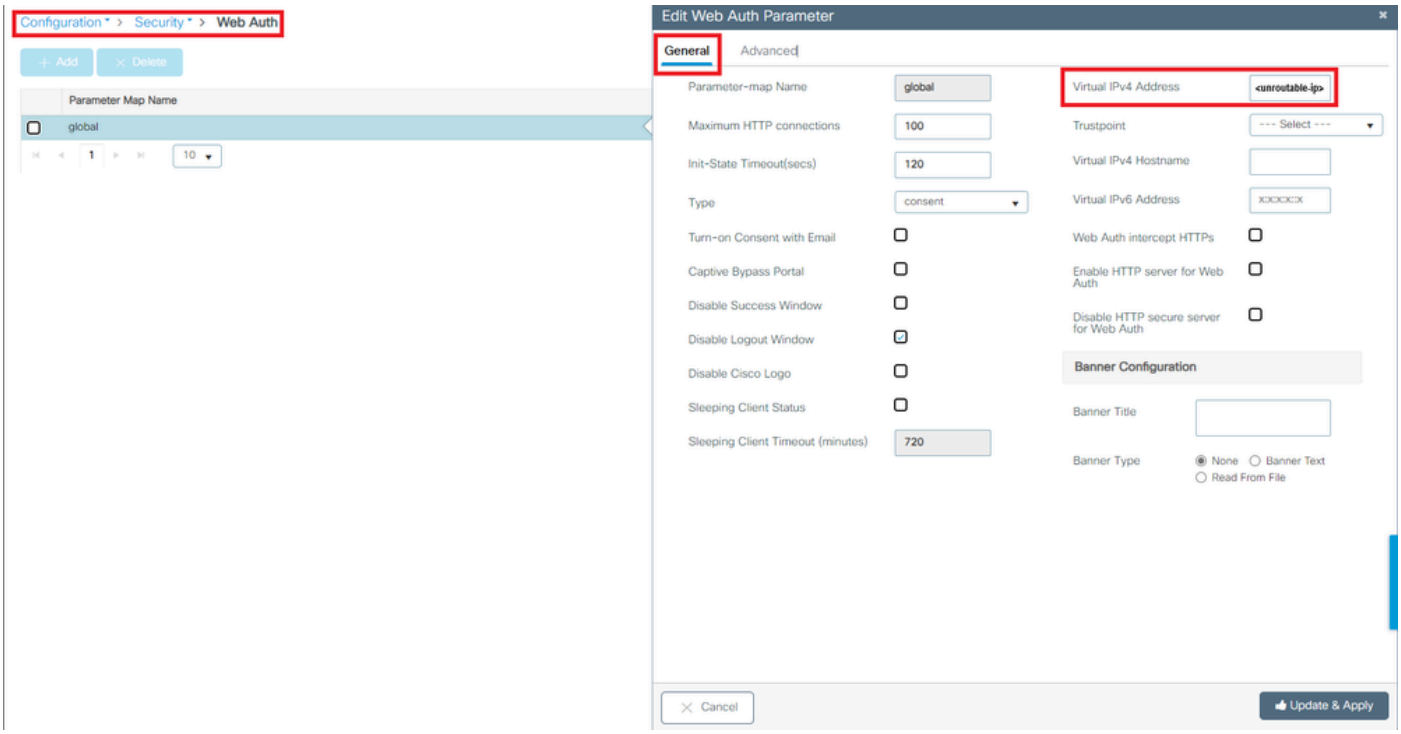
- El portal personalizado no se representa correctamente (es decir, las imágenes no se muestran).

Soluciones recomendadas

Asegúrese de que el mapa de parámetro global tenga asignada una dirección IP virtual.

Desde la GUI:

1. Vaya a Configuration > Security > Web Auth.
2. Seleccione el mapa de parámetro global de la lista.
3. Agregue una dirección IP virtual no enrutable.



Dirección IP virtual en mapa de parámetro global establecida en una dirección IP no enrutable

Desde la CLI:

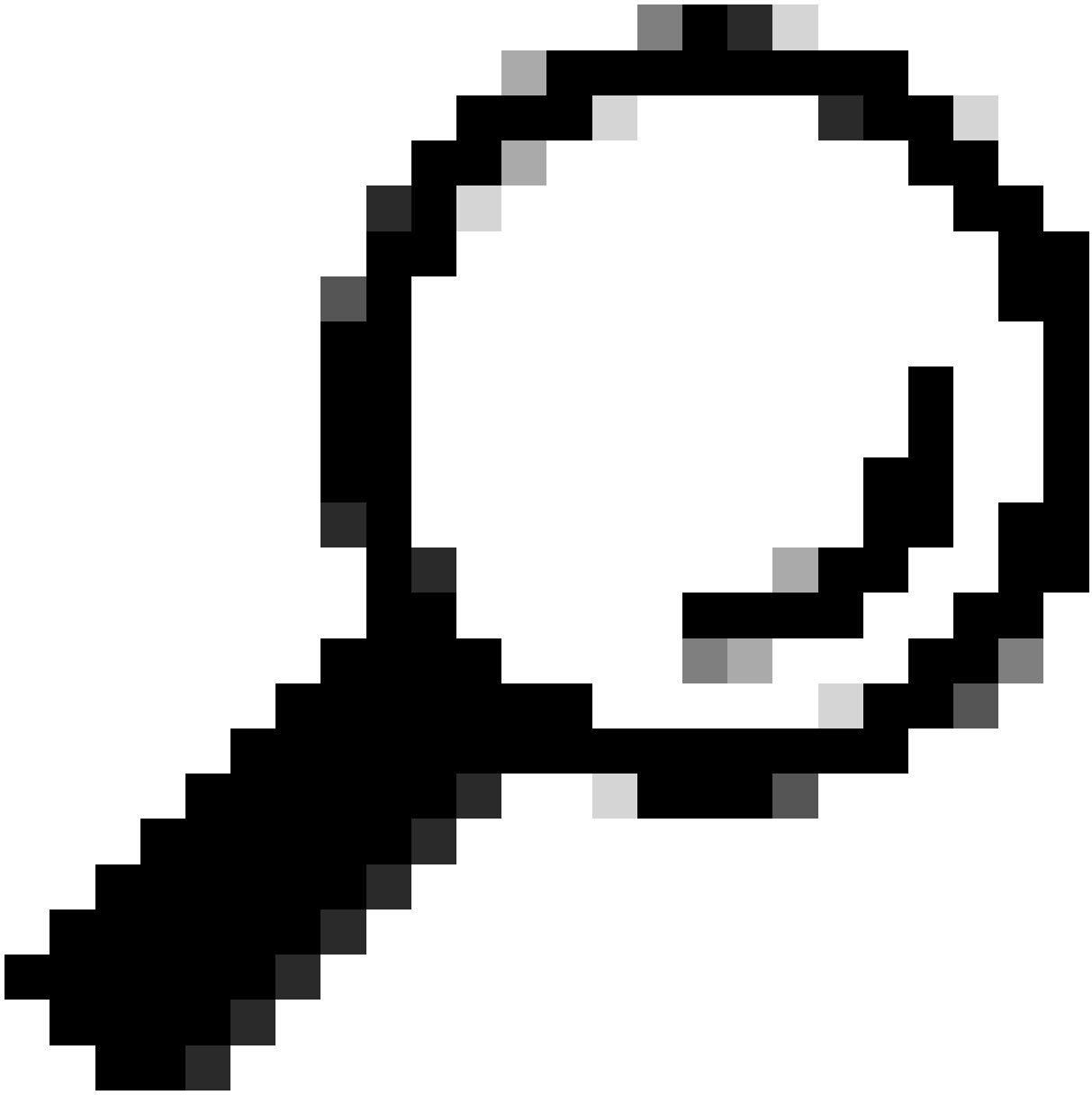
<#root>

```
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>



Sugerencia: la dirección IP virtual sirve como dirección de redirección para la página de inicio de sesión de autenticación Web. Ningún otro dispositivo en la red debe tener la misma IP, no debe ser mapeado a un puerto físico, ni existir en ninguna tabla de ruteo. Por lo tanto, se recomienda configurar la IP virtual como una dirección IP no ruteable, sólo se pueden utilizar las que están en el RFC5737.

El portal dice que "su conexión no es segura/ha fallado la firma de verificación"

Comportamiento posible experimentado por el cliente final

- Al abrir el portal, el cliente ve un error que indica que la conexión no es segura.
- Se espera que el portal utilice un certificado.

Cosas que debe saber

Si se espera que el portal se muestre en HTTPS, significa que necesita utilizar un certificado SSL (Secure Socket Layer). Dicho certificado debe ser emitido por una autoridad de certificación (CA) de terceros para validar que el dominio es real y proporcionar confianza a los clientes finales al introducir sus credenciales o ver el portal. Para cargar un certificado al WLC, consulte este documento.

Soluciones recomendadas

Primero: Reinicie los servicios HTTP/HTTPS que desee. Ahora es posible tener un mayor control sobre qué servidores HTTP/HTTPS deben activarse para adaptarse completamente a las necesidades de la red. Consulte este enlace para obtener más información sobre la configuración de solicitudes HTTP y HTTPS para la autenticación Web.

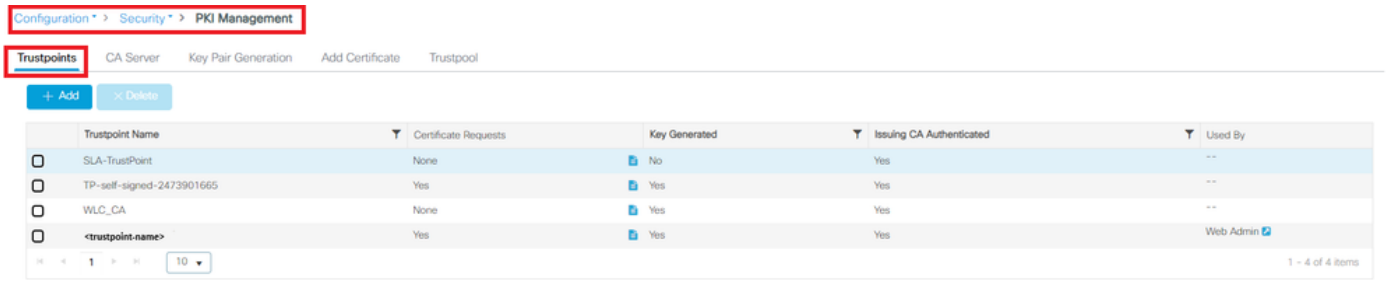
Desde la CLI:

```
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
```

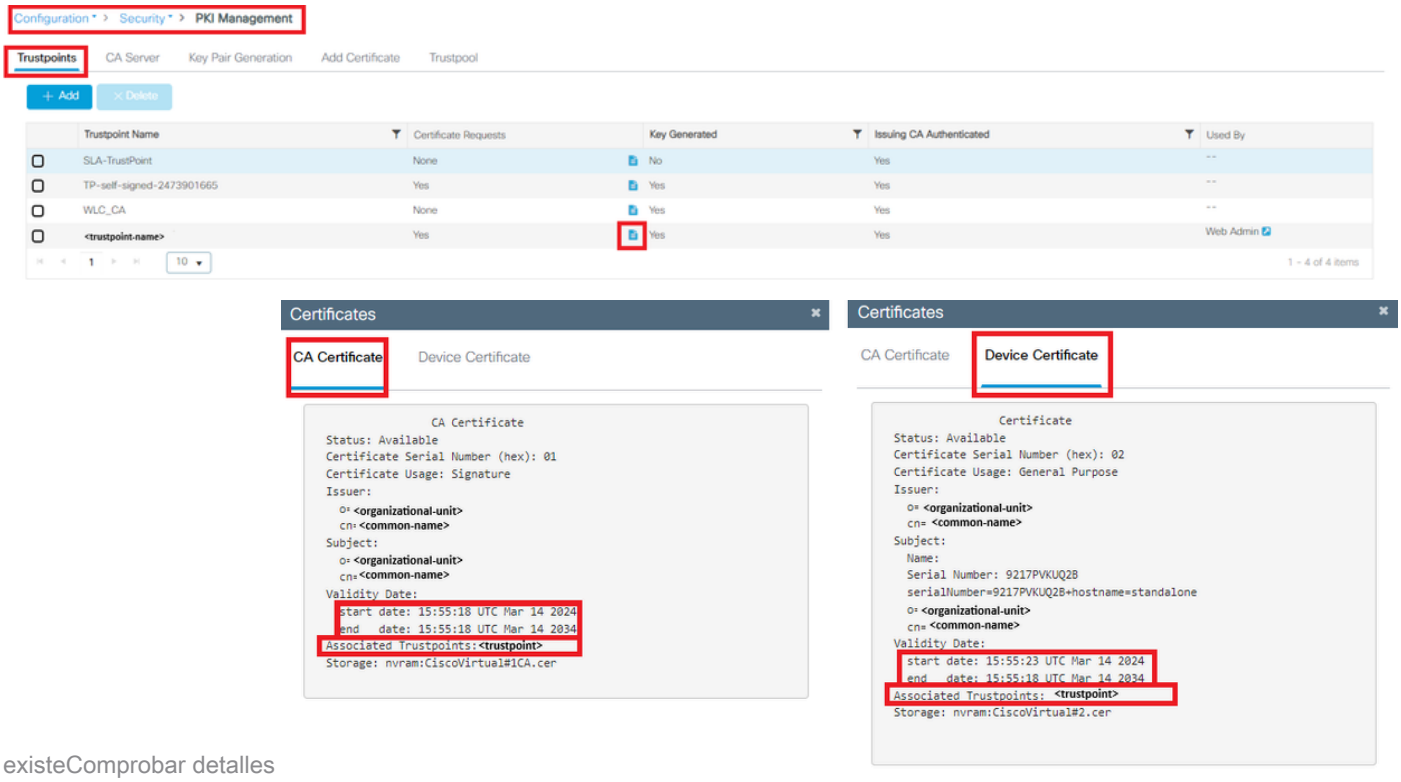
Segundo: Asegúrese de que el certificado esté correctamente cargado en el WLC y que su fecha de validez sea correcta.

Desde la GUI:

1. Vaya a Configuration > Security > PKI Management .
2. Buscar el punto de confianza en la lista
3. Compruebe sus detalles



Comprobar si el punto de confianza



existeComprobar detalles
del punto de confianzaComprobar validez del punto de confianza

Desde la 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>

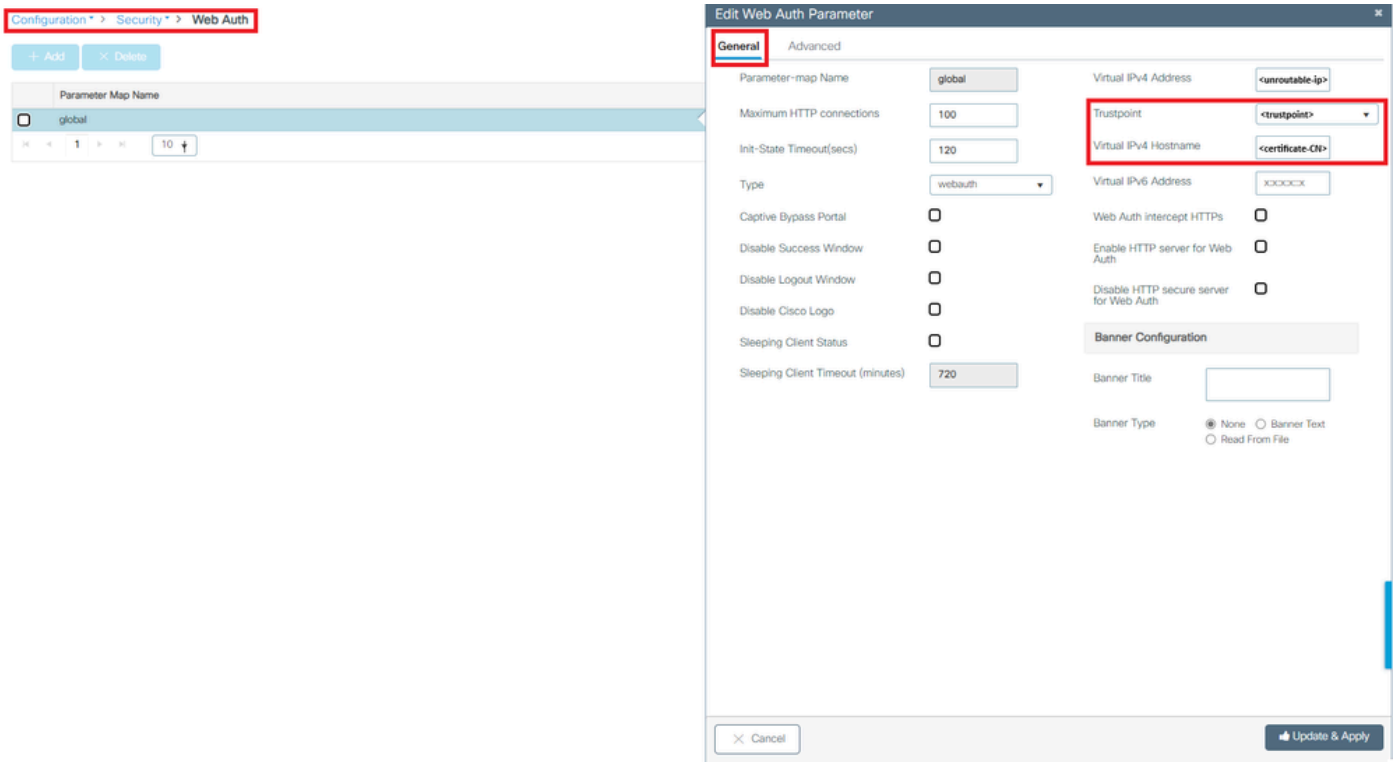
end date: <end-date>

Associated Trustpoints: <trustpoint>

Tercero: Asegúrese de que el certificado seleccionado correctamente para su uso en el mapa de parámetro WebAuth y que el nombre de host IPv4 virtual coincida con el nombre común (CN) del certificado.

Desde la GUI:

1. Vaya a Configuration > Security > Web Auth.
2. Seleccione el mapa de parámetro utilizado de la lista.
3. Compruebe que el punto de confianza y el nombre de host IPv4 virtual son correctos.



Comprobar el nombre de host IPv4 virtual y de punto de confianza

Desde la 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>

Información Relacionada

- Configurar autenticación Web local
- Autenticación basada en Web (EWC)
- Personalice el Portal de autenticación Web en el WLC de Catalyst 9800
- Generar y descargar certificados CSR en WLC Catalyst 9800
- Configuración de interfaces virtuales

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).