對9800 WLC上的LWA的常見問題進行故障排除

目錄

簡介

本檔案介紹使用本機Web驗證(LWA)連線到WLAN的使用者端常見問題。

必要條件

需求

思科建議您具備以下基本知識：

- 思科無線LAN控制器(WLC) 9800系列。
- 對本地Web身份驗證(LWA)及其配置的一般瞭解。

採用元件

本檔案中的資訊是根據以下軟體和硬體版本：

- 9800-CL WLC
- 思科存取點9120AXI
- 9800 WLC Cisco IOS® XE版本17.9.3

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

LWA是一種可在WLC上設定的WLAN驗證型別，嘗試連線的終端使用者端在自清單中選取WLAN後，會向使用者提供一個入口網站。在此門戶中，使用者可以輸入使用者名稱和密碼（取決於所選配置）以完成與WLAN的連線。

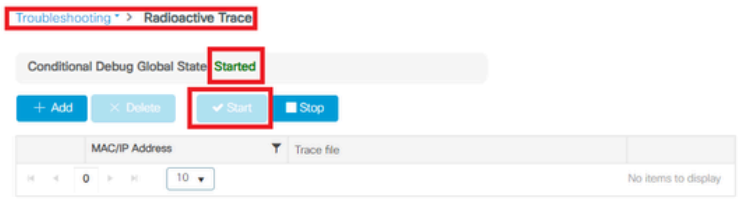
有關如何在9800 WLC上配置LWA的詳細資訊，請參閱配置本地Web身份驗證配置指南。

9800 WLC上的放射性(RA)痕跡

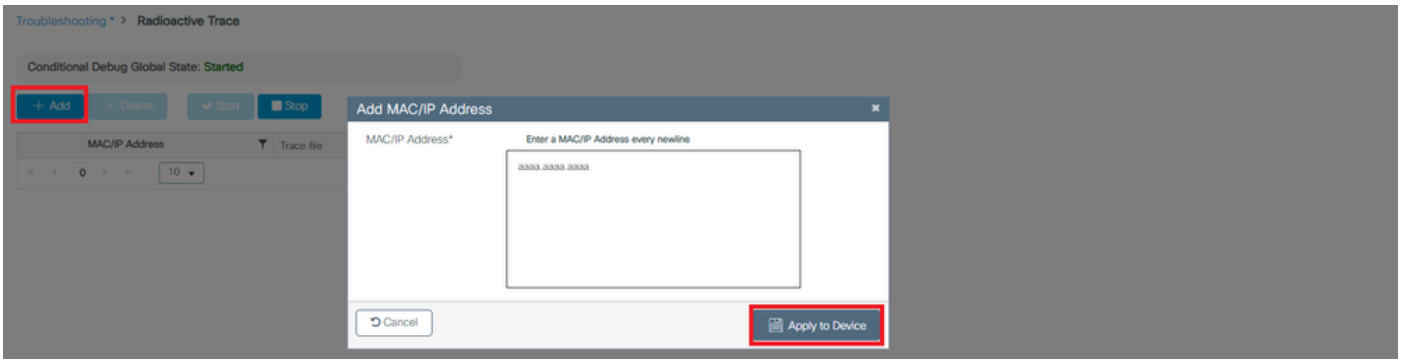
放射性跡線是一種非常好的故障排除工具，可用於排除WLC和客戶端連線方面的各種故障。為了收集RA追蹤，請執行下列步驟：

在 GUI 上：

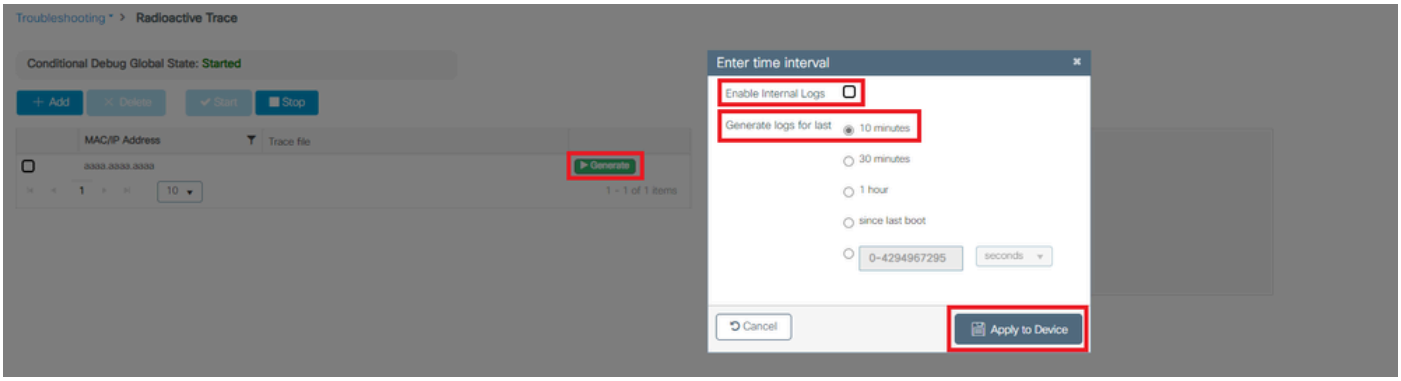
1. 轉至故障排除 > 放射跟蹤。
2. 按一下「開始」以啟用「條件式除錯全域狀態」。
3. 按一下+ Add。即會開啟一個快顯視窗。輸入客戶端的MAC地址。接受任何MAC地址格式(aabb.ccdd.eeff、AABB.CCDD.EEEE、aa：bb：cc：dd：ee：ff或AA：BB：CC：DD：EE：FF)。然後按一下Apply to Device。
4. 讓客戶端重現問題3或4次。
5. 重現問題後，按一下「生成」。
6. 即會開啟新的快顯視窗。生成過去10分鐘的日誌。（在這種情況下，不需要啟用內部日誌）。按一下Apply to Device，並等待檔案被處理。
7. 生成檔案後，按一下Download圖示。



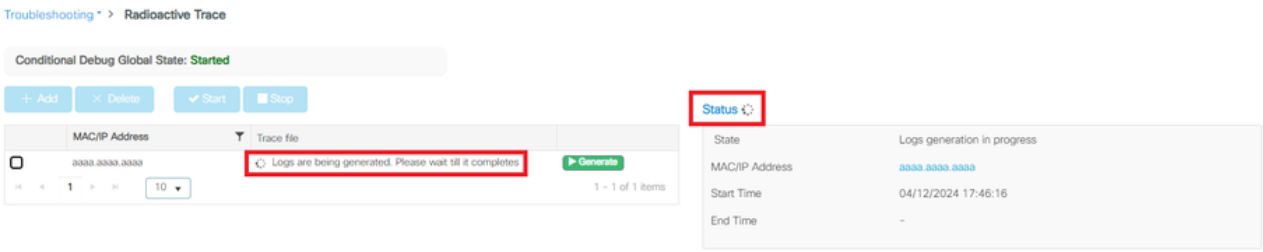
啟用條件式除錯



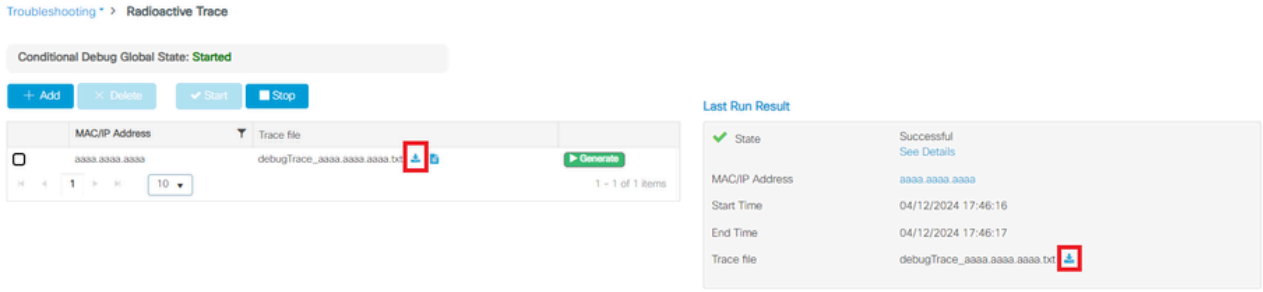
增加客戶端MAC地址



生成過去10分鐘的日誌



等待檔案產生



下載檔案

在CLI上：

<#root>

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

在bootflash中將生成名為ra_trace_MAC_<mac-address>_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log的新檔案

<#root>

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

將檔案複製到外部伺服器進行分析

<#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
```

有關放射性跟蹤的詳細資訊，請參閱此連結。

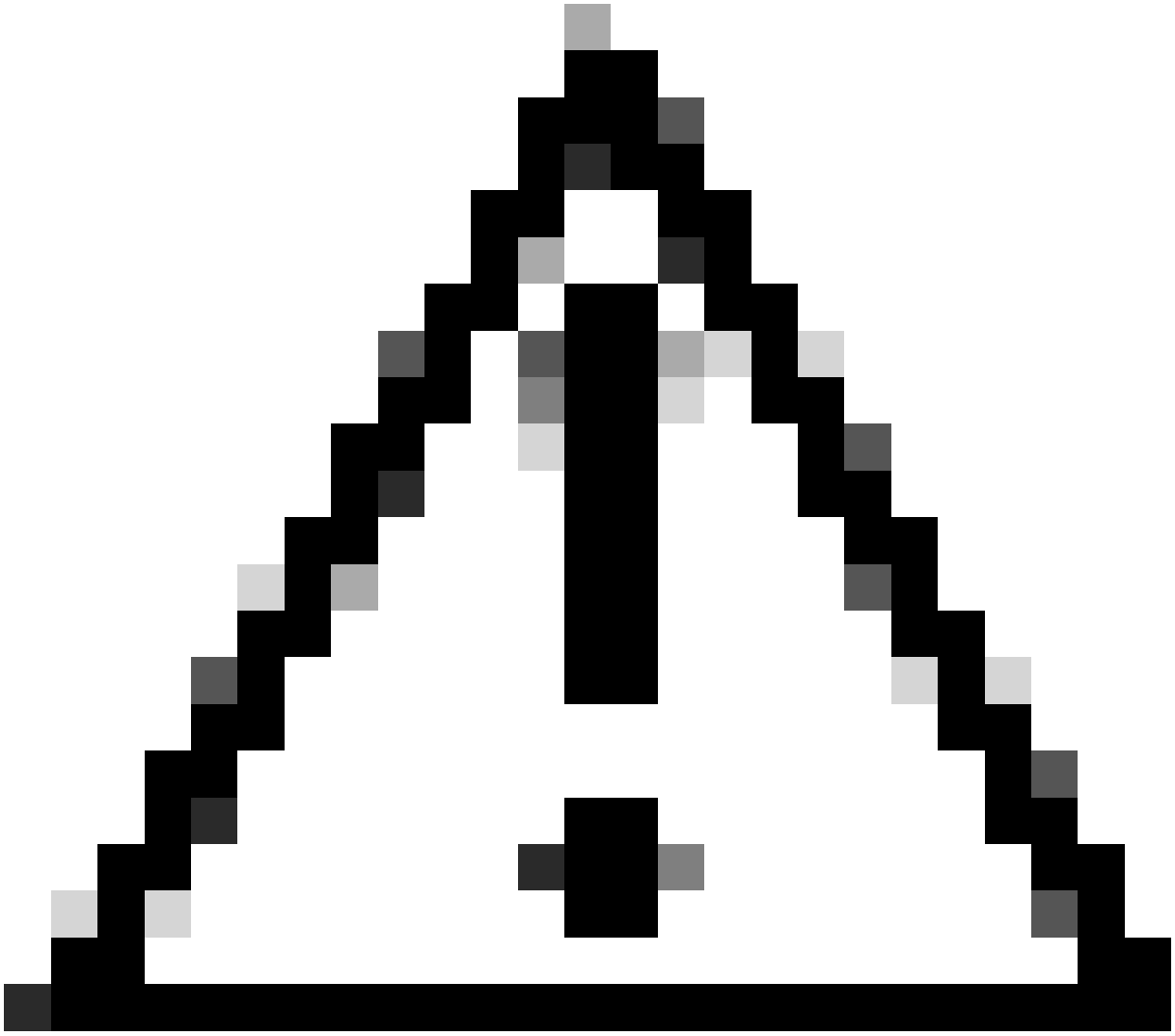
預期流量

請參考資訊以瞭解LWA的工作案例。

從使用者端角度分階段進行使用者端作業

1. 終端客戶端與WLAN關聯。
2. 客戶端獲得分配的IP地址。
3. 門戶向終端客戶端顯示。
4. 終端使用者端輸入登入認證。
5. 終端使用者端已經過驗證。
6. 終端使用者端可以瀏覽網際網路。

從WLC的角度分階段客戶端進行



注意：為簡單起見，未列出「無線電活動(RA)」跟蹤中的許多日誌。

最終客戶端與WLAN關聯

<#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
```

L2驗證

<#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
```

客戶端獲得分配的IP地址

<#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

L3身份驗證

<#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
```

客戶端獲得IP地址

<#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

入口網站處理

<#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

WLC處理要應用於連線的終端客戶端的資訊

<#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將使用者設定檔套用到連線的終端使用者端

<#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'
```

Web身份驗證已完成

<#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

應用於終端客戶端的AAA屬性

<#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

"]

終端客戶端到達Run狀態

<#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

常見故障排除方案

身份驗證失敗

考量

- 輸入正確的憑證後，顯示的門戶顯示「身份驗證失敗」。
- WLC顯示客戶端處於「Web Auth Pending」狀態。
- 初始啟動顯示頁面會再次顯示給使用者。

WLC RA跟蹤

<#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]

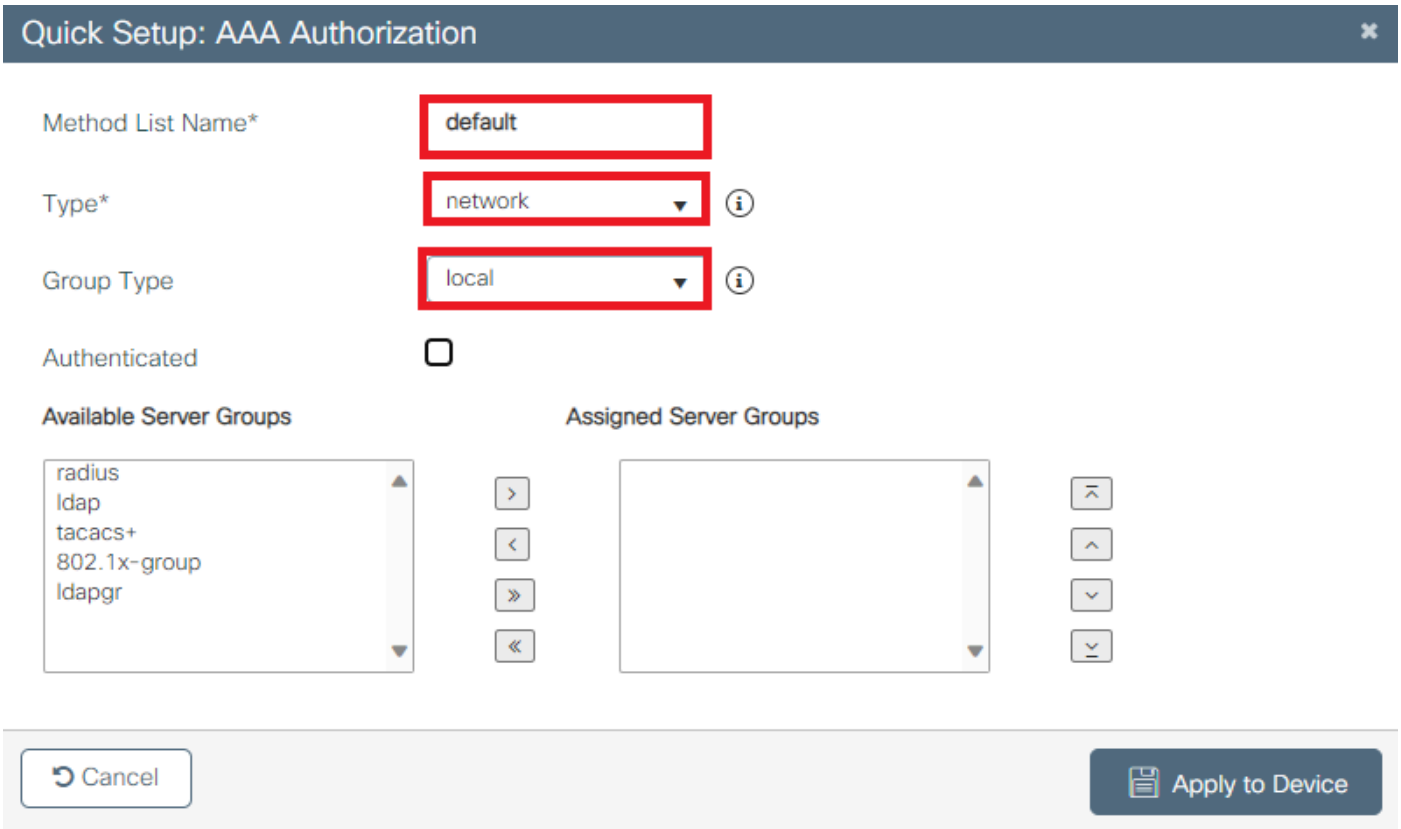
```
[aaaa.bbbb.cccc:capwap_90400002] Authc failure from WebAuth, Auth event fail
[aaaa.bbbb.cccc:capwap_90400002] (Re)try failed method WebAuth - aaaa.bbbb.cccc
[aaaa.bbbb.cccc:capwap_90400002] Method webauth changing state from 'Running' to 'Authc Failed'
```

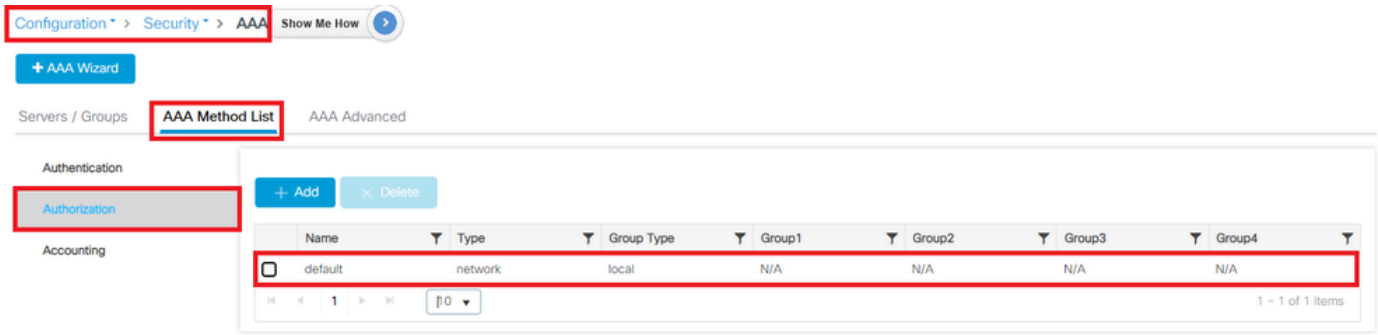
建議的解決方案

確保WLC配置中存在用於網路授權的預設AAA方法清單。

在 GUI 上：

1. 轉至Configuration > Security > AAA > AAA Method List > Authorization。 按一下+ Add。
2. 配置為：
    1. 方法清單名稱：預設
    2. 型別：網路
    3. 群組型別：本機
3. 點選應用到裝置。





在CLI上：

<#root>

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

門戶未顯示給使用者，但客戶端顯示為已連線

從最終客戶端可能發生的行為

- 終端客戶端將其裝置視為「已連線」。
- 最終客戶端看不到門戶。
- 終端使用者端未輸入任何認證。
- 已為最終客戶端分配IP地址。
- WLC顯示客戶端處於「運行」狀態。

WLC RA跟蹤

客戶端獲得分配的IP地址，然後立即在WLC上進入「運行」狀態。使用者屬性僅顯示分配給終端客戶端的VLAN。

<#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 "
```

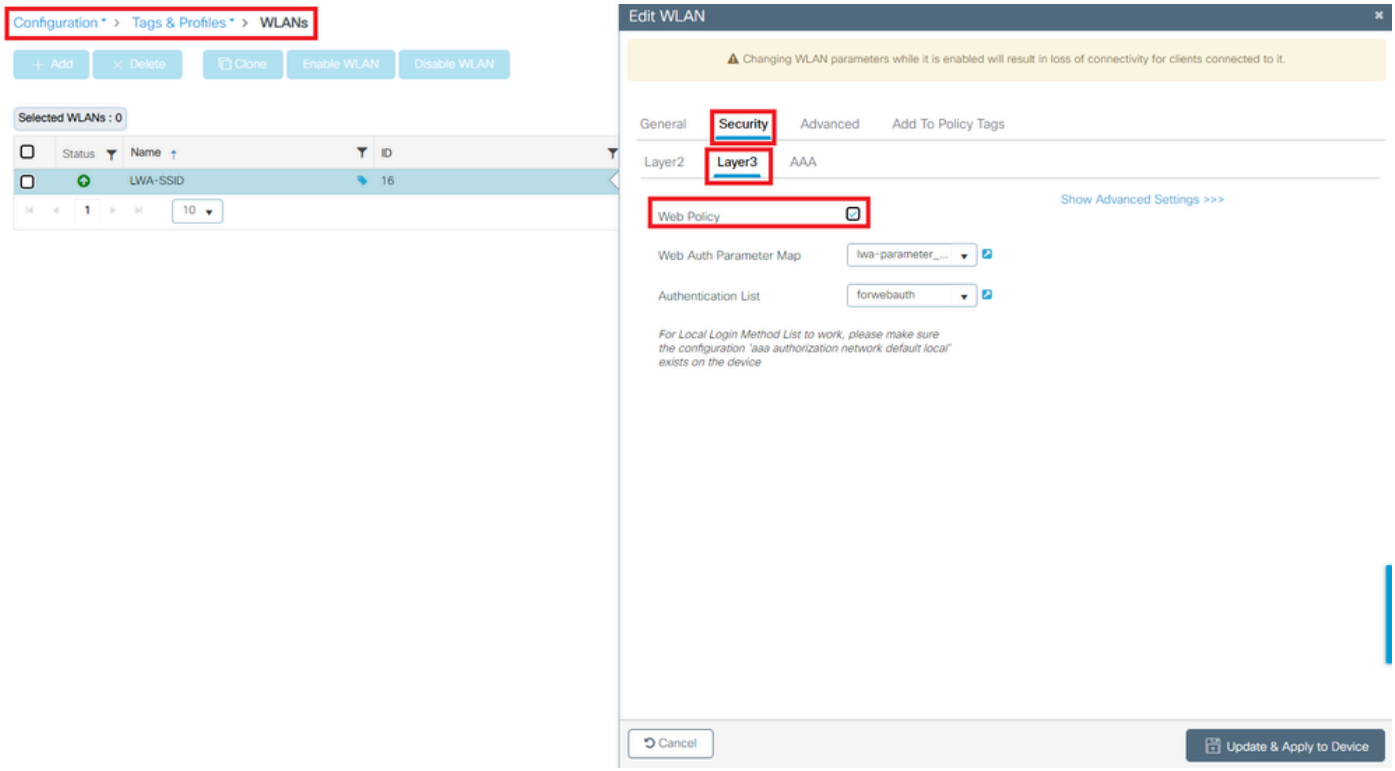
```
myvlan

" ]
[ 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
```

建議的解決方案

確保已在WLAN上啟用Web策略。

在 GUI 上：

1. 轉至Configuration > Tags & Profiles > WLANs。
2. 選擇LWA WLAN。
3. 轉至Security > Layer 3。
4. 確保啟用Web Policy覈取方塊。



需要啟用Web策略

在CLI上：

```
<#root>

WLC# configure terminal


WLC(config)# wlan

<wlan>
```

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

入口未顯示給使用者，客戶端未連線

從最終客戶端可能發生的行為

- 終端客戶端發現其裝置正在持續嘗試連線。

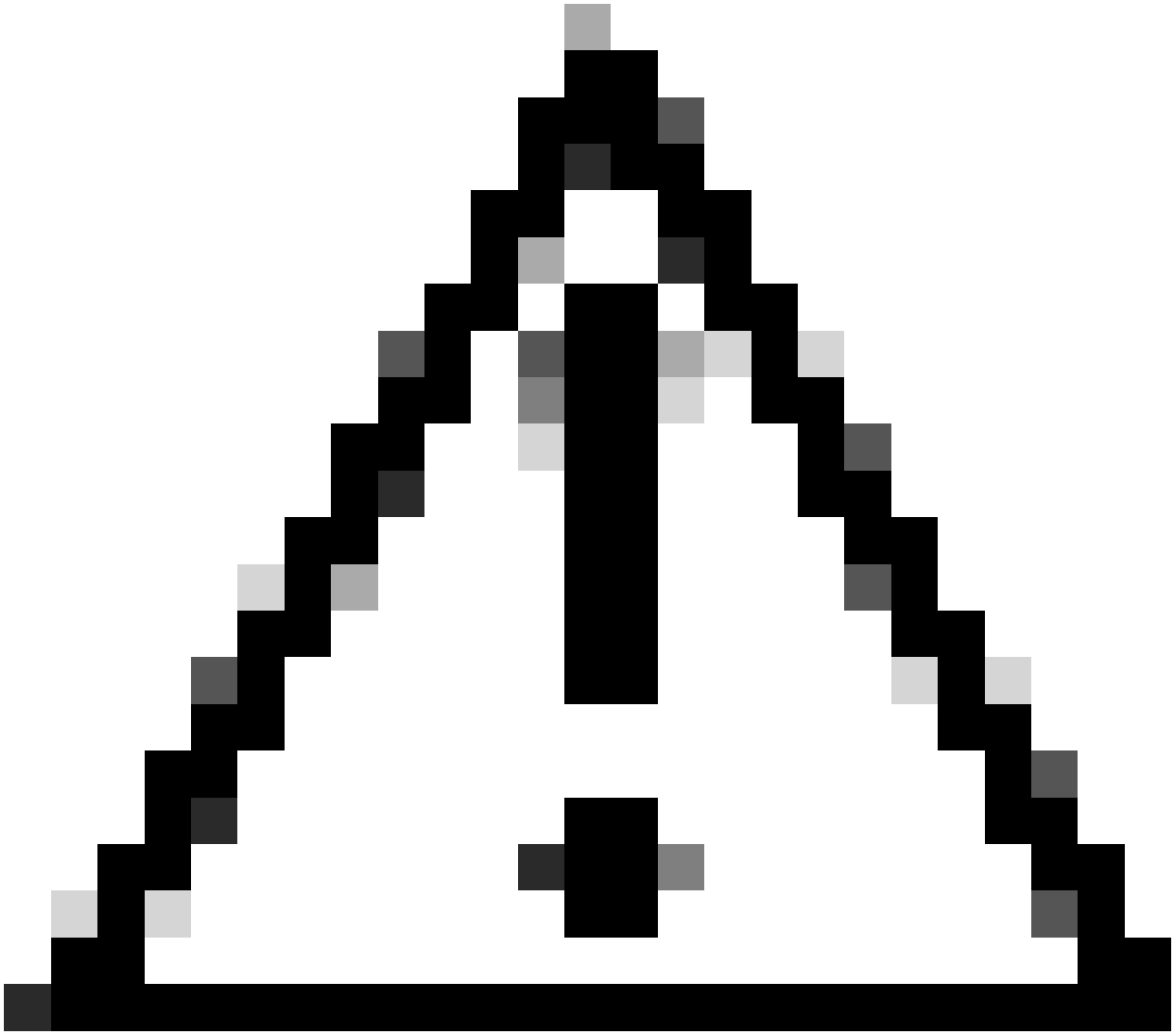
- 最終客戶端看不到門戶。
- 沒有為終端客戶端分配IP地址。
- WLC顯示使用者端處於「Webauth擱置中」狀態。

建議的解決方案

啟用必要的HTTP/HTTPS伺服器。現在，可以更好地控制需要啟用哪些HTTP/HTTPS伺服器來完全適應網路的需求。有關為Web身份驗證配置HTTP和HTTPS請求的詳細資訊，請參閱此連結，因為支援多種HTTP組合；例如，HTTP僅可用於Webadmin，HTTP用於webauth。

要允許透過HTTP和HTTPS訪問進行管理裝置管理和Web身份驗證，請從CLI執行以下操作：

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



注意：如果這兩個伺服器都已停用，就無法存取WLC的圖形使用者介面(GUI)。

終端客戶端未獲取IP地址

從最終客戶端可能發生的行為

- 終端客戶端看到其裝置不斷嘗試獲取IP地址。
- WLC顯示客戶端處於「IP Learning」狀態。

WLC RA跟蹤

不回約的派遣請求。

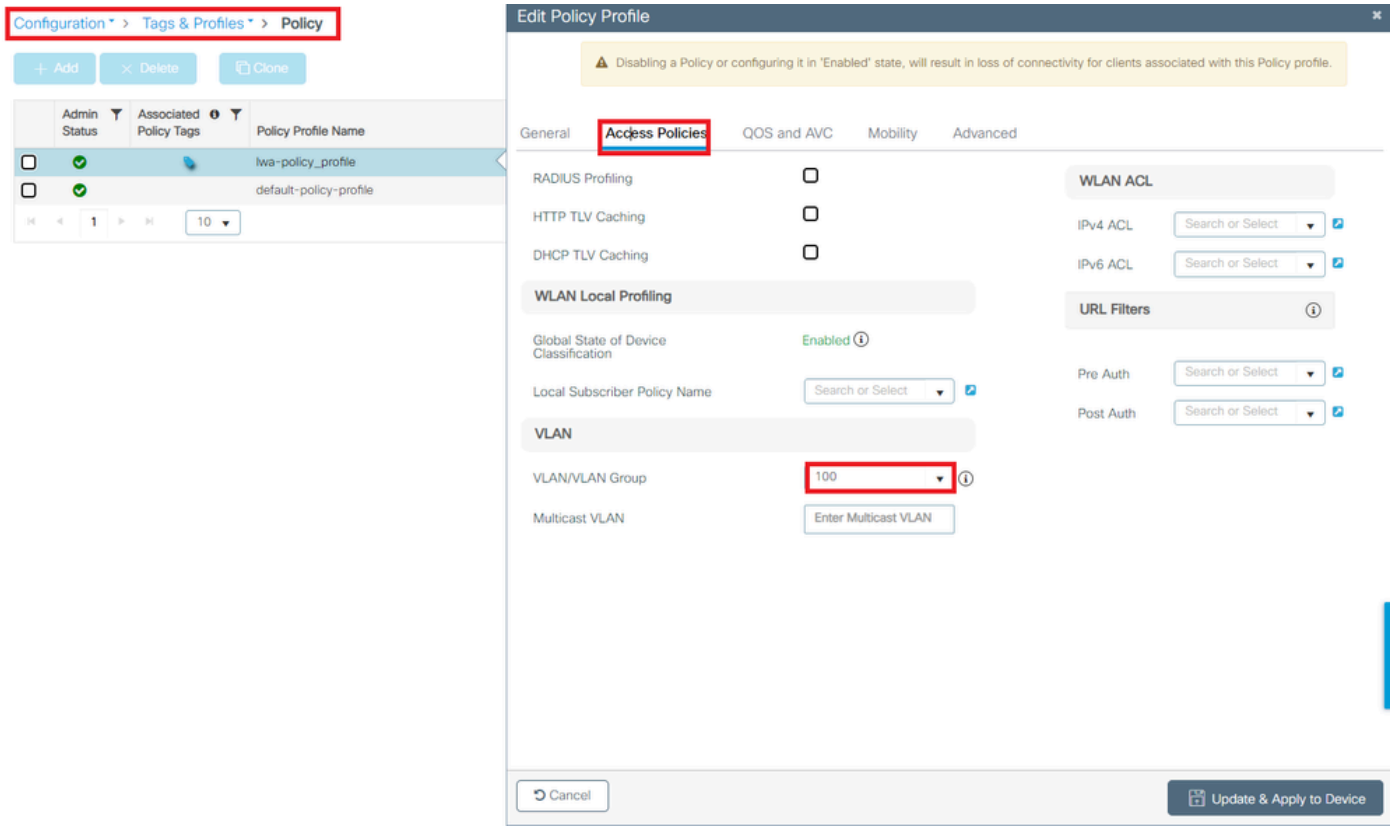
```
RX: DHCPv4 from interface capwap_90400002 on vlan 100 Src MAC: aaaa.bbbb.cccc Dst MAC: ffff.ffff.ffff s
TX: DHCPv4 from interface capwap_90400002 on vlan 100 Src MAC: aaaa.bbbb.cccc Dst MAC: ffff.ffff.ffff s
```

建議的解決方案

首先：確保為策略配置檔案分配了正確的VLAN。

在 GUI 上：

1. 轉至Configuration > Tags & Profiles > Policy。
2. 選擇使用的策略配置檔案。
3. 轉至Access Policies。
4. 選擇正確的VLAN。



在CLI上：

<#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>
```

第二：確保某個位置為使用者提供了DHCP池。檢查其配置和可達性。RA跟蹤顯示正在經歷的VLAN DHCP DORA進程。確保此VLAN為正確的VLAN。

```
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,
```

自定義門戶未顯示給最終客戶端

從最終客戶端可能發生的行為

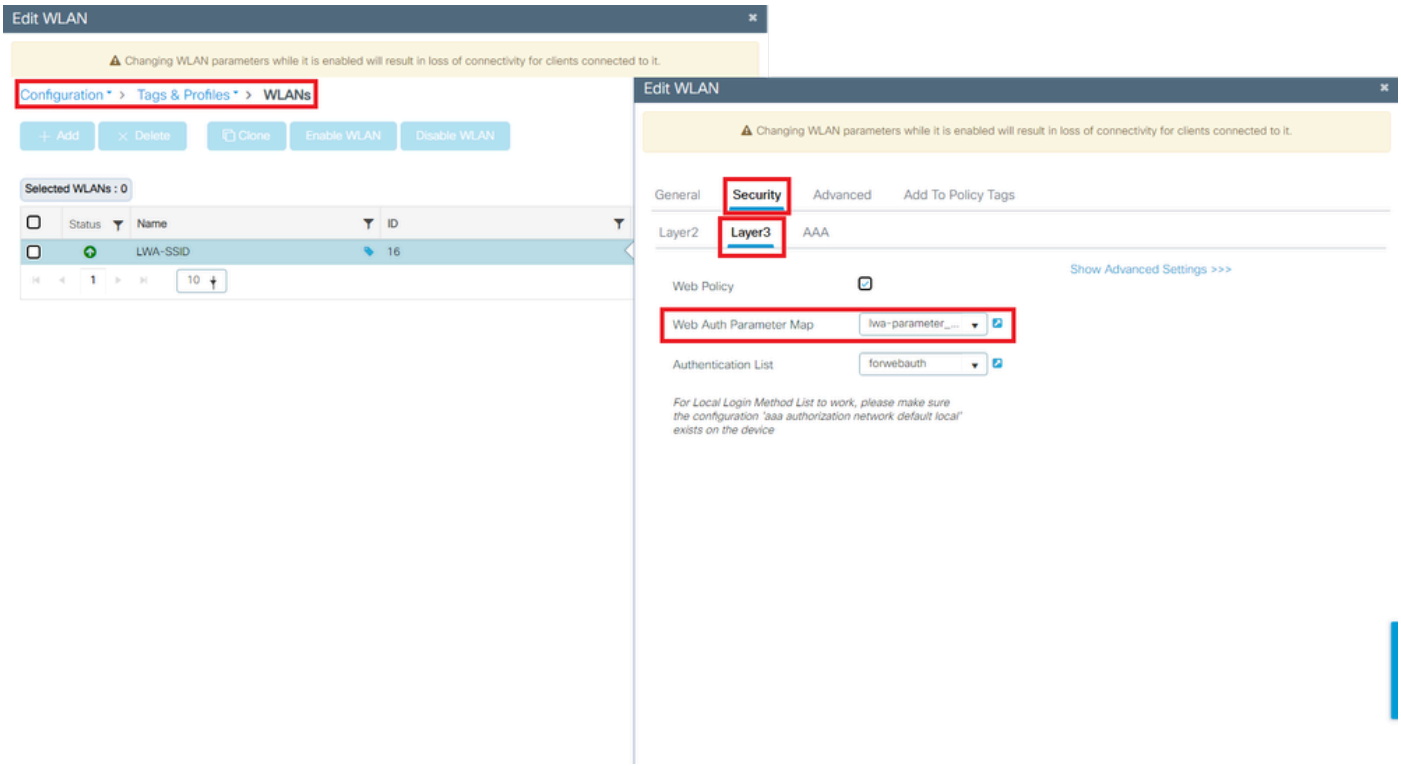
- 會看到預設的WLC輸入網站。

建議的解決方案

首先：確保WLAN使用的是自定義Web身份驗證引數對映。

在 GUI 上：

1. 轉至Configuration > Tags & Profiles > WLANs。
2. 從清單中選擇WLAN。
3. 轉至Security > Layer 3。
4. 選擇自定義的Web身份驗證引數對映。



已選取自訂引數對應

在CLI上：

<#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>

第二：必須注意的是，從Cisco.com Web門戶下載的自定義內容無法與非常堅固和複雜的程式設計介面一起使用。通常，建議只在CSS級別進行更改，並且可能增加或刪除映像。不支援Applet、PHP、修改變數、React.js等。如果自訂入口網站沒有顯示給使用者端，請嘗試使用預設的WLC頁面，然後檢視是否可複製問題。如果成功看到入口，則應該使用的自定義頁面上存在不受支援的內容。

第三：如果使用EWC(嵌入式無線控制器)，建議使用CLI增加自定義頁面，以確保其正確顯示：

<#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
```

未正確向最終客戶端顯示自定義門戶

從最終客戶端可能發生的行為

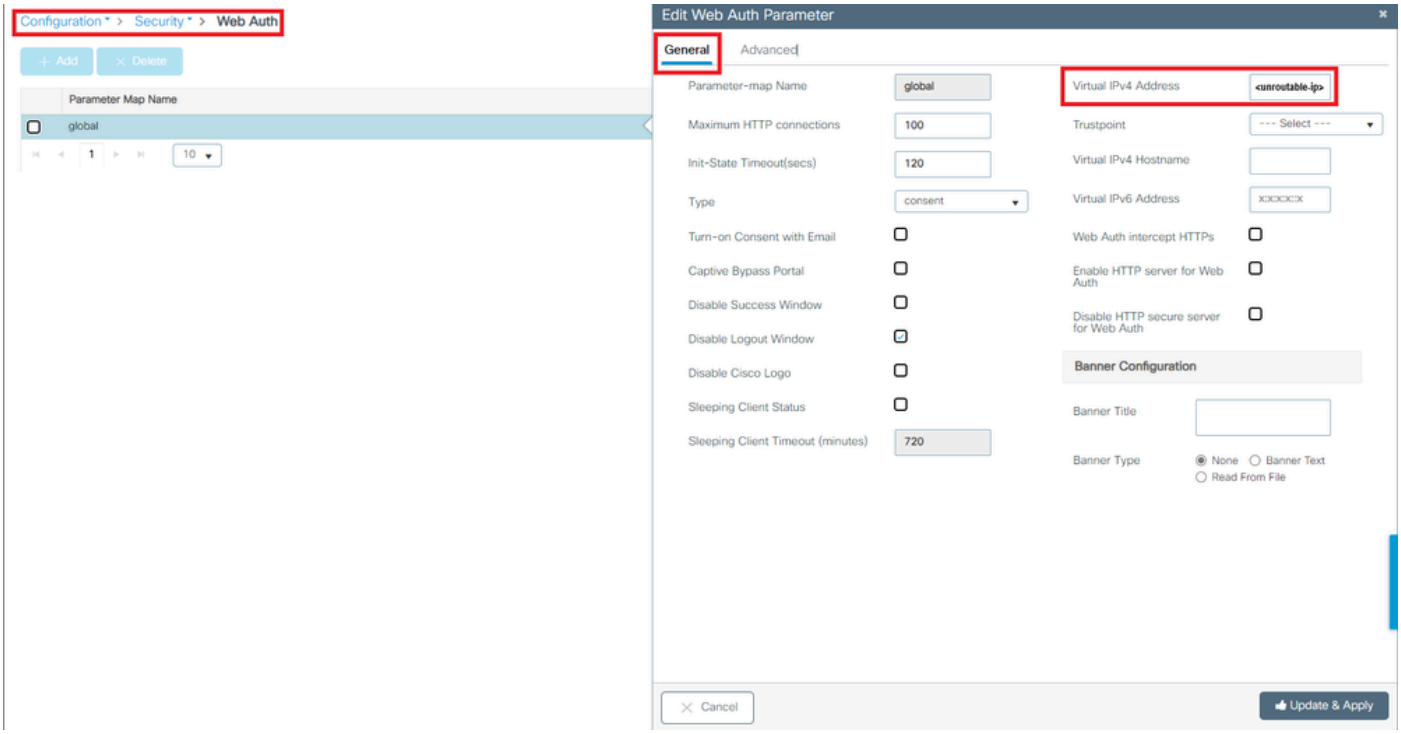
- 未正確呈現自定義門戶（即影象未顯示）。

建議的解決方案

確保為全局引數對映分配了虛擬IP地址。

在 GUI 上：

1. 轉到Configuration > Security > Web Auth。
2. 從清單中選擇global引數對映。
3. 增加不可路由的虛擬IP地址。



全局引數對映上的虛擬IP地址設定為不可路由的IP地址

在CLI上：

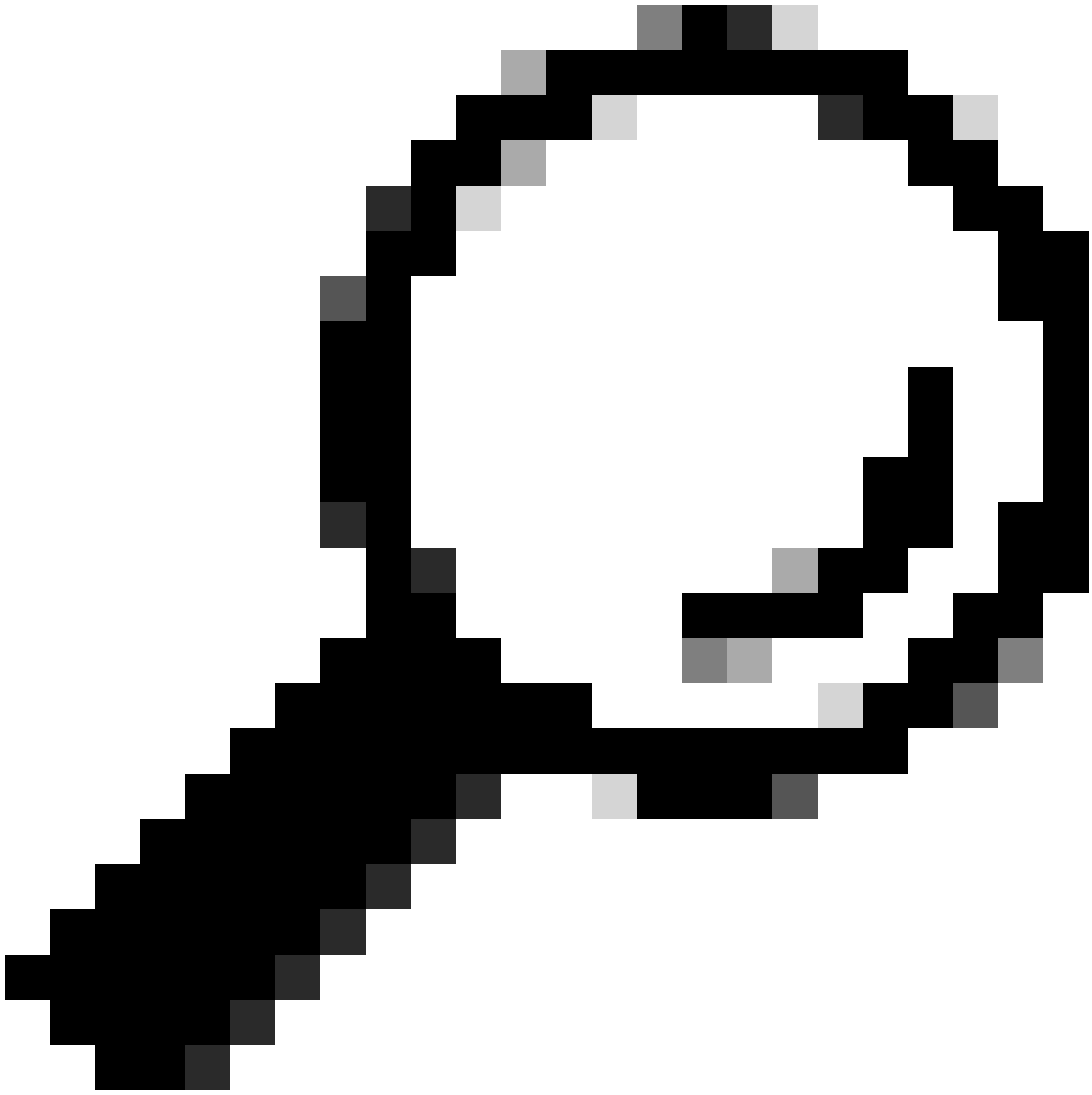
<#root>

```
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>



提示：虛擬IP地址用作Web身份驗證登入頁的重定向地址。網路中的任何其他裝置都不必須具有相同的IP，它不能對映到物理埠，也不能存在於任何路由表中。因此，建議將虛擬IP配置為不可路由的IP地址，但只能使用RFC5737上的那些地址。

門戶顯示「連線不安全/驗證簽名失敗」

從最終客戶端可能發生的行為

- 打開入口時，客戶端發現一個錯誤，表明連線不安全。
- 入口應該使用憑證。

須知事項

如果預期入口會顯示在HTTPS之下，則表示它需要使用SSL（安全通訊端層）憑證。該證書必須由

第三方證書頒發機構(CA)頒發，以驗證域是真實的；在輸入憑據和/或檢視門戶時，向終端客戶端提供信任。若要將憑證上傳到WLC，請參閱本檔案。

建議的解決方案

首先：重新啟動所需的HTTP/HTTPS服務。現在，可以更好地控制需要啟用哪些HTTP/HTTPS伺服器來完全適應網路的需求。有關為Web身份驗證配置HTTP和HTTPS請求的詳細資訊，請參閱此連結。

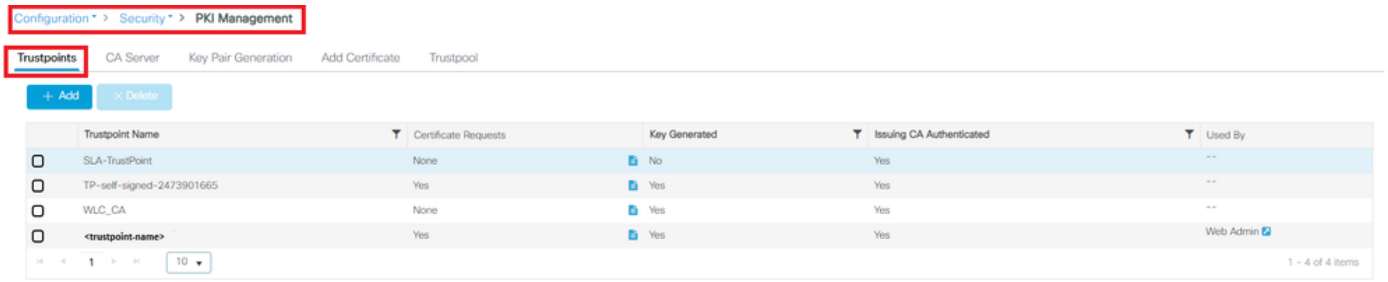
在CLI上：

```
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
```

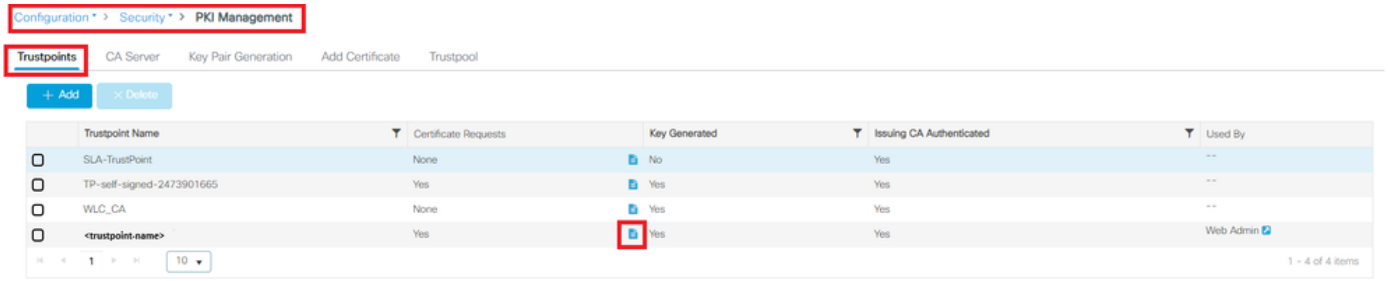
第二：確保已將證書正確上傳到WLC並且其有效日期正確。

在 GUI 上：

1. 轉至Configuration > Security > PKI Management
2. 在清單中搜尋信任點
3. 檢查其詳細資訊



檢查信任點



ExistsCheck信任點

DetailsCheckTrustpoint有效性

在CLI上：

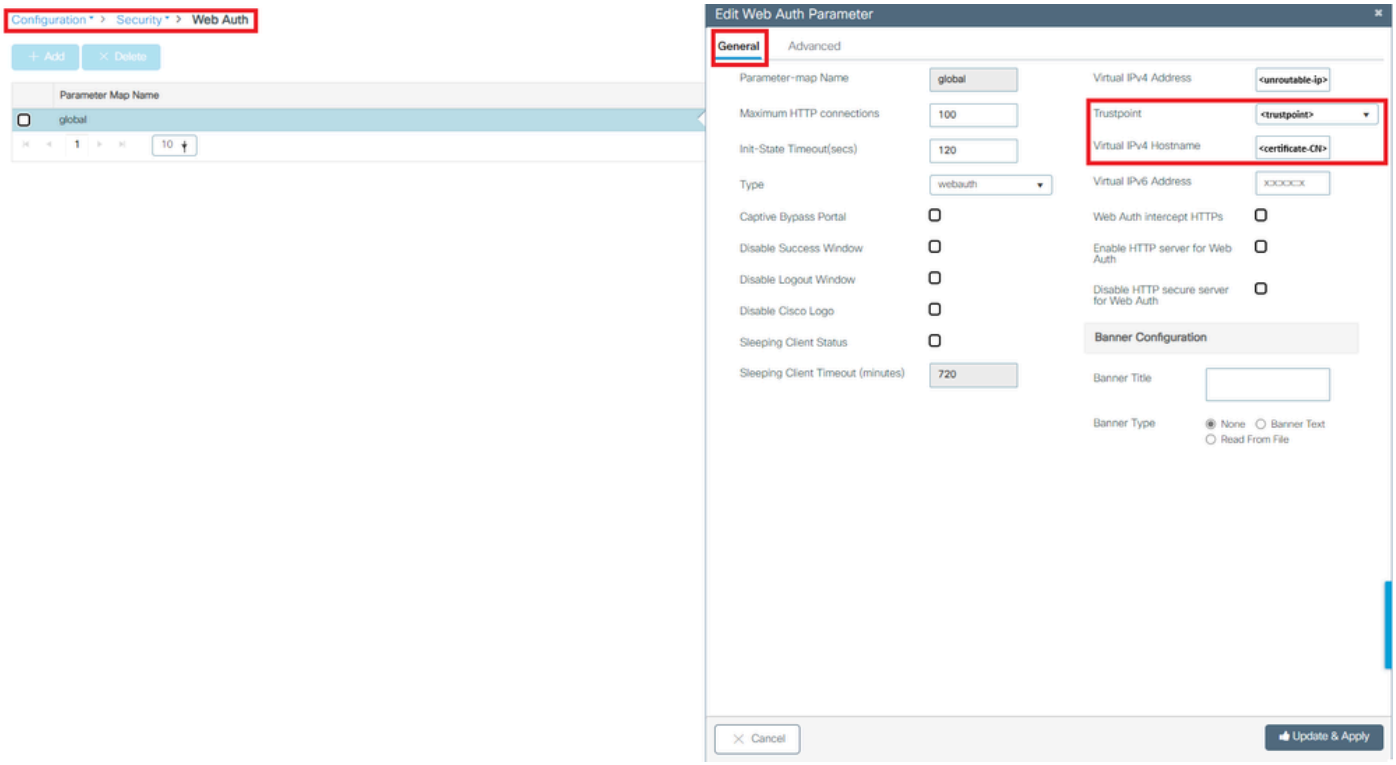
<#root>

```
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>
```

第三：確保在WebAuth引數對映中選擇了要使用的正確證書，以及虛擬IPv4主機名與證書中的公用名(CN)匹配。

在 GUI 上：

1. 轉到Configuration > Security > Web Auth。
2. 從清單中選取使用的引數對映。
3. 檢查信任點和虛擬IPv4主機名是否正確。



檢查信任點和虛擬IPv4主機名

在CLI上：

<#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>

相關資訊

- 設定本機Web驗證

- Web型驗證(EWC)
- 在Catalyst 9800 WLC上自定義Web身份驗證門戶
- 在Catalyst 9800 WLC上產生和下載CSR憑證
- 配置虛擬介面

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。