对9800 WLC上的LWA的常见问题进行故障排除

目录

简介

本文档介绍使用本地Web身份验证(LWA)连接到WLAN的客户端的常见问题。

先决条件

要求

思科建议您具备以下方面的基础知识：

- 思科无线局域网控制器(WLC) 9800系列。
- 对本地Web身份验证(LWA)及其配置的一般了解。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 9800-CL WLC
- 思科接入点9120AXI
- 9800 WLC Cisco IOS® XE版本17.9.3

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

LWA是一种WLAN身份验证，可在WLC上配置，其中尝试连接的终端客户端从列表中选择WLAN后，会向用户提供一个门户。在此门户中，用户可以输入用户名和密码（取决于所选的配置），以完成与WLAN的连接。

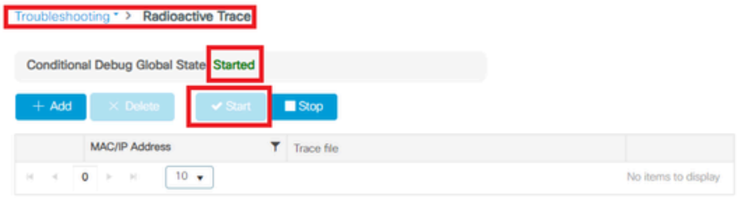
有关如何在9800 WLC上配置LWA的详细信息，请参阅配置本地Web身份验证配置指南。

9800 WLC上的放射性(RA)痕迹

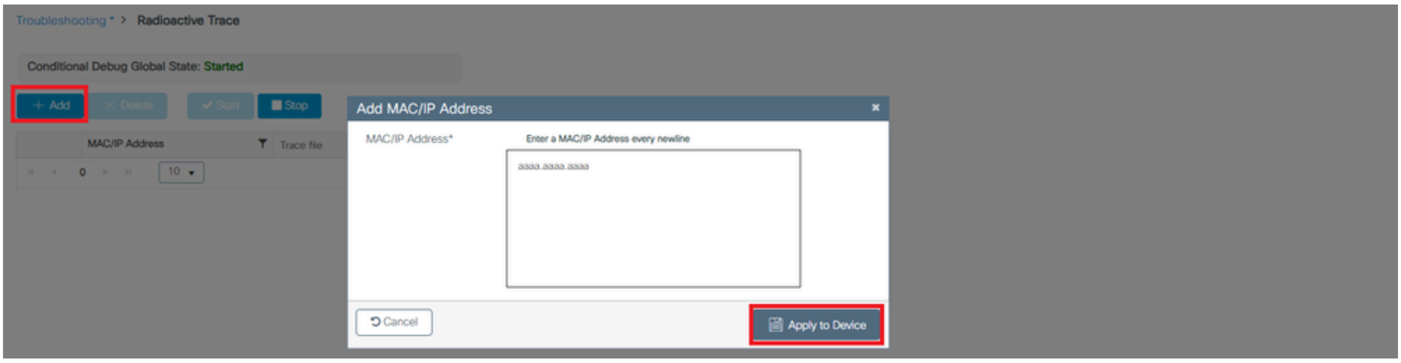
放射性踪迹是一种很好的故障排除工具，可用于排除WLC和客户端连接的各种问题。为了收集RA跟踪，请执行以下步骤：

从 GUI：

1. 转至故障排除 > 放射跟踪。
2. 点击Start以启用Conditional Debug Global State。
3. 单击+ Add。打开一个弹出窗口。输入客户机的 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)。然后单击Apply to Device。
4. 让客户端重现问题3或4次。
5. 重现问题后，单击“生成”。
6. 将打开一个新的弹出窗口。生成过去10分钟的日志。（在这种情况下，无需启用内部日志）。单击Apply to Device，并等待文件处理。
7. 生成文件后，单击Download图标。



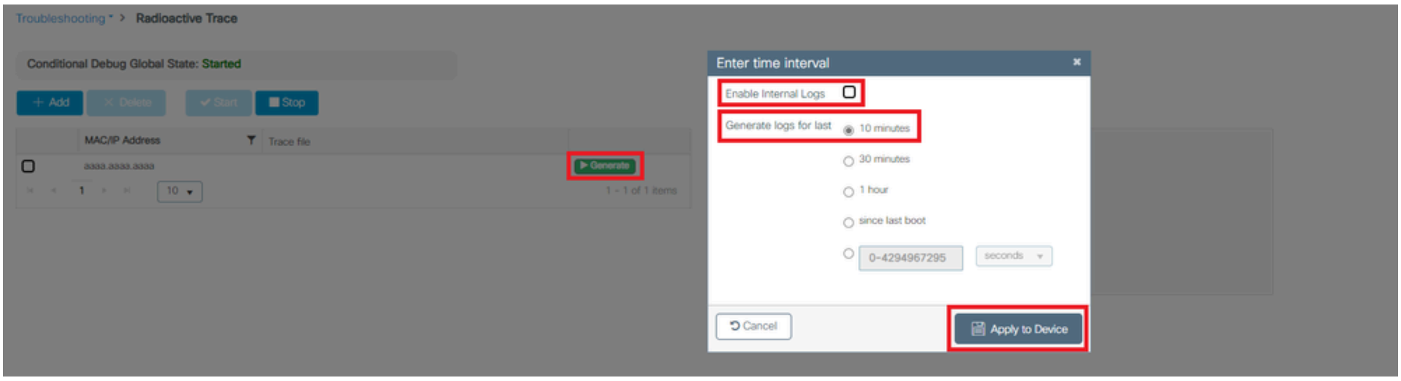
启用条件调试



MAC/IP Address* Enter a MAC/IP Address every newline

aaaa.aaaa.aaaa

添加客户端MAC地址



Enable Internal Logs □

Generate logs for last ● 10 minutes

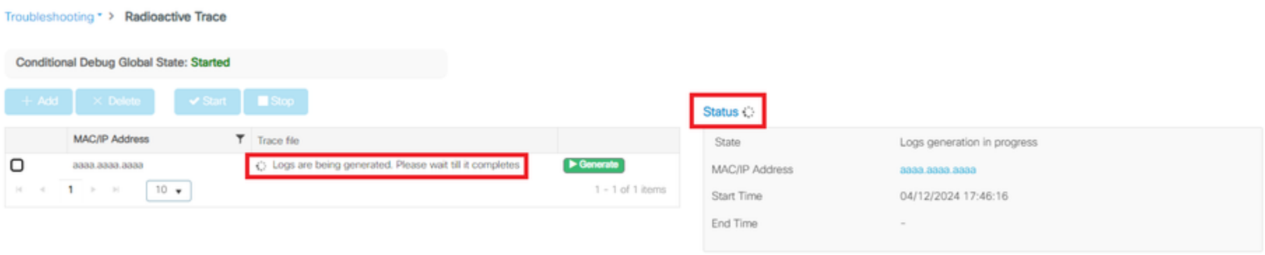
○ 30 minutes

○ 1 hour

○ since last boot

○ 0-4294967295 seconds

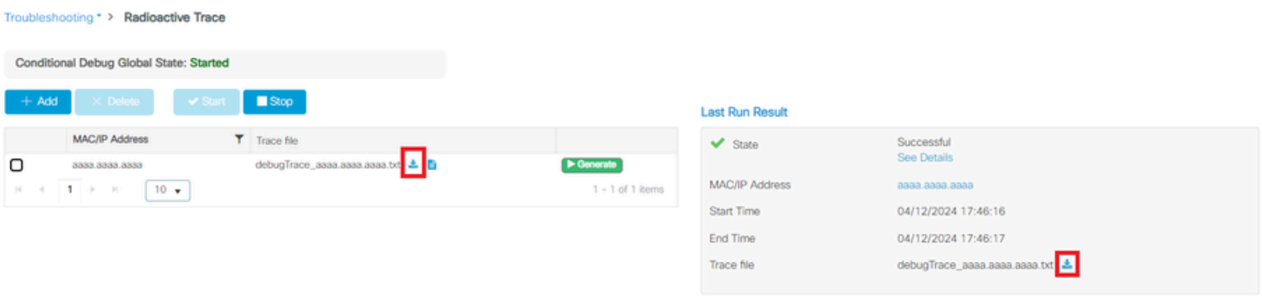
生成最近10分钟的日志



aaaa.aaaa.aaaa Logs are being generated. Please wait till it completes

State	Logs generation in progress
MAC/IP Address	aaaa.aaaa.aaaa
Start Time	04/12/2024 17:46:16
End Time	-

等待文件生成



aaaa.aaaa.aaaa debugTrace_aaaa.aaaa.aaaa.txt

✓ State	Successful See Details
MAC/IP Address	aaaa.aaaa.aaaa
Start Time	04/12/2024 17:46:16
End Time	04/12/2024 17:46:17
Trace file	debugTrace_aaaa.aaaa.aaaa.txt

下载文件

从CLI：

<#root>

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

在bootflash中生成一个名为ra_trace_MAC_<mac-address>_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log的新文件

<#root>

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

将文件复制到外部服务器进行分析

<#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
```

有关放射性示踪的详细信息，请参阅此链接。

预期流

请参阅信息以了解LWA的工作方案。

从客户端角度暂存客户端

1. 最终客户端与WLAN关联。
2. 客户端获得分配的IP地址。
3. 门户向最终客户端显示。
4. 终端客户端输入登录凭证。
5. 终端客户端通过身份验证。
6. 终端客户端可以浏览互联网。

从WLC的角度暂存客户端

注意：出于简单性考虑，保留了许多“无线电活动(RA)”跟踪日志。

最终客户端与WLAN关联

<#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身份验证

<#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
```

客户端获得分配的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身份验证

<#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
```

客户端获得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
```

门户处理

<#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处理要应用于连接终端客户端的信息

<#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将用户配置文件应用于连接的终端客户端

<#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身份验证已完成

<#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
```

应用于最终客户端的AAA属性

<#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

" ]
```

终端客户端到达运行状态

<#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
```

常见故障排除场景

验证失败次数

考虑事项

- 输入正确的凭证后，显示的门户显示“身份验证失败”。
- WLC显示客户端处于“Web Auth Pending”状态。
- 初始启动页再次向用户显示。

WLC RA跟踪

<#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]

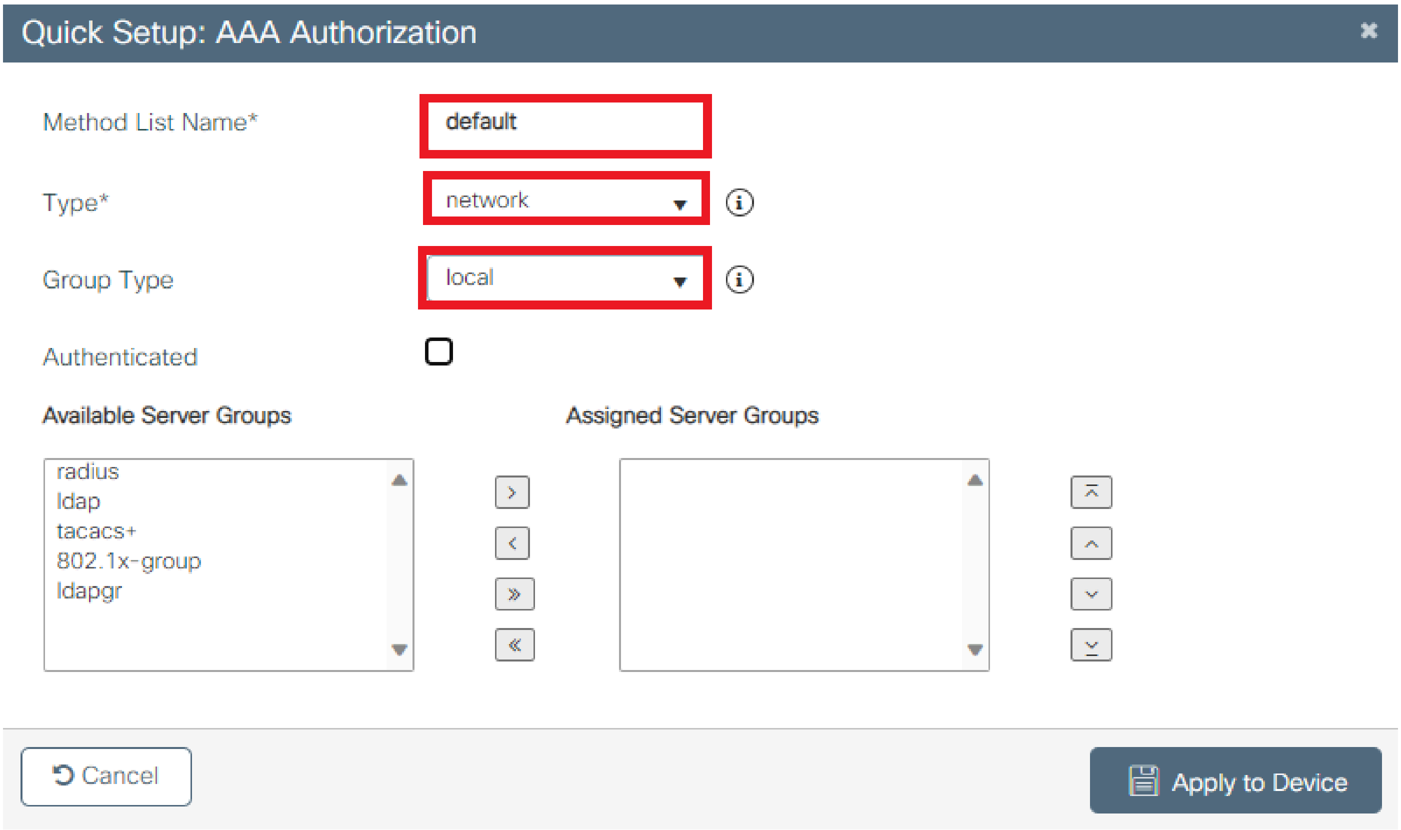
```
[aaaa.bbbb.cccc:capwap_90400002] Authc failure from WebAuth, Auth event fail
[aaaa.bbbb.cccc:capwap_90400002] (Re)try failed method WebAuth - aaaa.bbbb.cccc
[aaaa.bbbb.cccc:capwap_90400002] Method webauth changing state from 'Running' to 'Authc Failed'
```

推荐的解决方案

确保WLC配置中存在网络授权的默认AAA方法列表。

从 GUI：

1. 转至Configuration > Security > AAA > AAA Method List > Authorization。 点击+ Add。
2. 配置为：
   1. 方法列表名称：默认
   2. 类型：网络
   3. 组类型：本地
3. 单击Apply to Device。

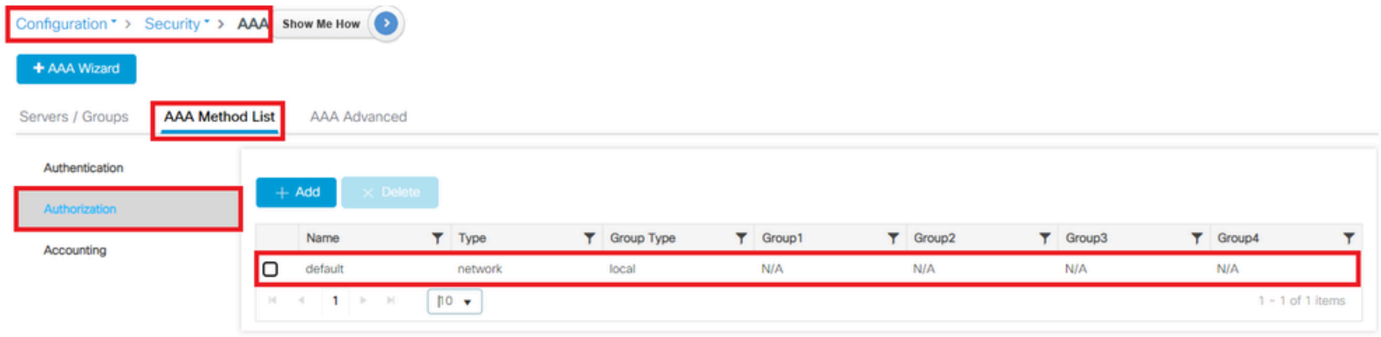

Quick Setup: AAA Authorization

Method List Name*: default

Type*: network

Group Type: local

Authenticated: □



	Name	Type	Group Type	Group1	Group2	Group3	Group4
□	default	network	local	N/A	N/A	N/A	N/A

从CLI：

<#root>

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

门户未向用户显示，但客户端显示为已连接

从最终客户端经历的可能行为

- 最终客户端将其设备视为“已连接”。

- 最终客户端看不到门户。
- 终端客户端不输入任何凭证。
- 已为最终客户端分配IP地址。
- WLC显示客户端处于“运行”状态。

WLC RA跟踪

为客户端分配一个IP地址，然后它立即在WLC上变为“运行”状态。用户属性仅显示分配给终端客户端的VLAN。

<#root>

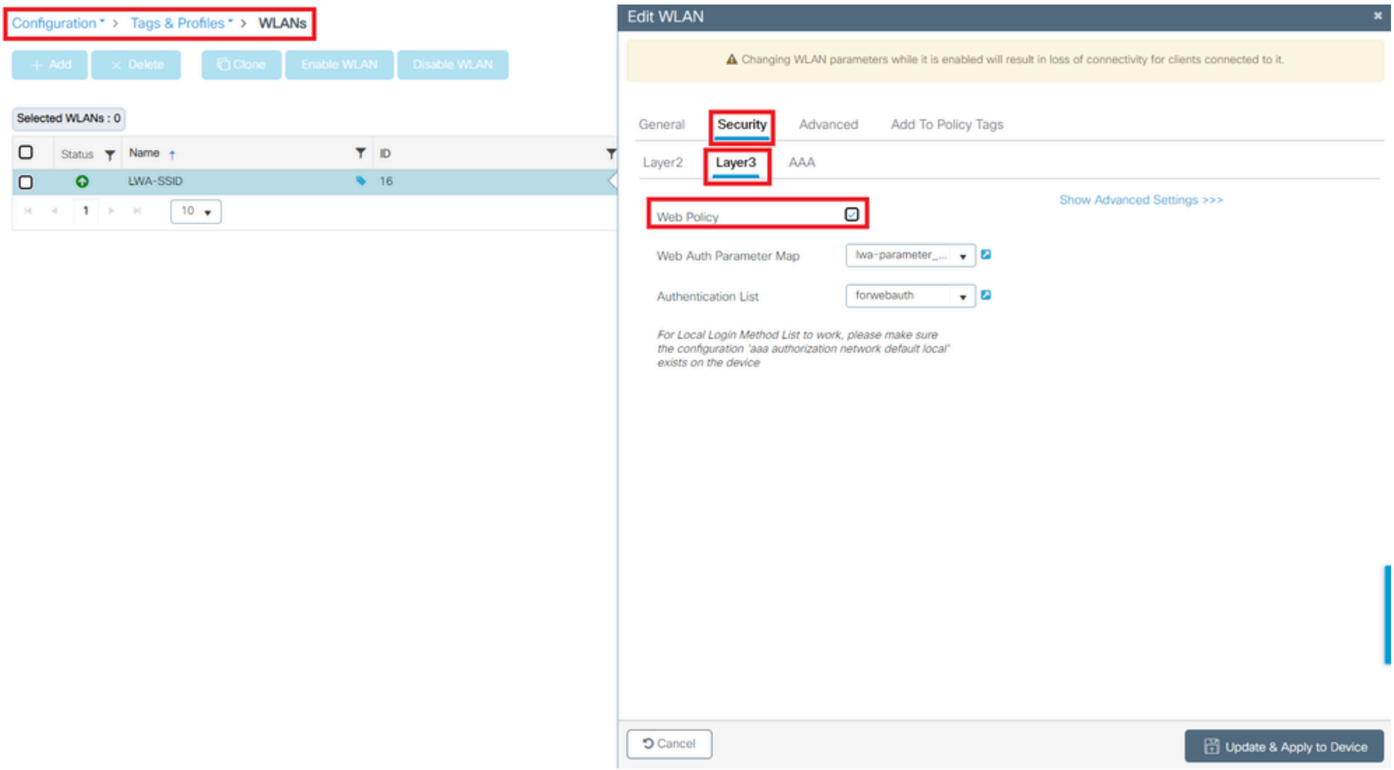
```
MAC: aaaa.bbbb.cccc

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
```

推荐的解决方案

确保在WLAN上启用了Web策略。

从 GUI：

1. 转至Configuration > Tags & Profiles > WLANs。
2. 选择LWA WLANs。
3. 转至Security > Layer 3。
4. 确保启用Web Policy复选框。



□	Status	Name	ID
□	●	LWA-SSID	16

Changing WLAN parameters while it is enabled will result in loss of connectivity for clients connected to it.

Web Policy ☑

Web Auth Parameter Map: lwa-parameter_...

Authentication List: forwebauth

For Local Login Method List to work, please make sure the configuration 'aaa authorization network default local' exists on the device

需要启用Web策略

从CLI：

<#root>

```
WLC# configure terminal
```

```
WLC(config)# wlan
<wlan>
```

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

门户未显示给用户，客户端未连接

从最终客户端经历的可能行为

- 终端客户端看到其设备不断尝试连接。

- 最终客户端看不到门户。
- 没有为终端客户端分配IP地址。
- WLC显示客户端处于“Webauth Pending”状态。

推荐的解决方案

启用必要的HTTP/HTTPS服务器。现在，可以更好地控制需要启用哪些HTTP/HTTPS服务器来完全适应网络的需求。有关为Web身份验证配置HTTP和HTTPS请求的详细信息，请参阅此链接，因为支持几种HTTP组合；例如，HTTP仅可用于webadmin，HTTP用于webauth。

要通过HTTP和HTTPS访问允许管理设备管理和Web身份验证，请从CLI执行以下操作：

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

发现请求。

注意：如果这两个服务器都禁用，则无法访问图形用户界面(GUI)的WLC。

终端客户端未获得IP地址

从最终客户端经历的可能行为

- 终端客户端看到其设备不断尝试获取IP地址。
- WLC显示客户端处于“IP学习”状态。

WLC RA跟踪

发现请求，但无返款。

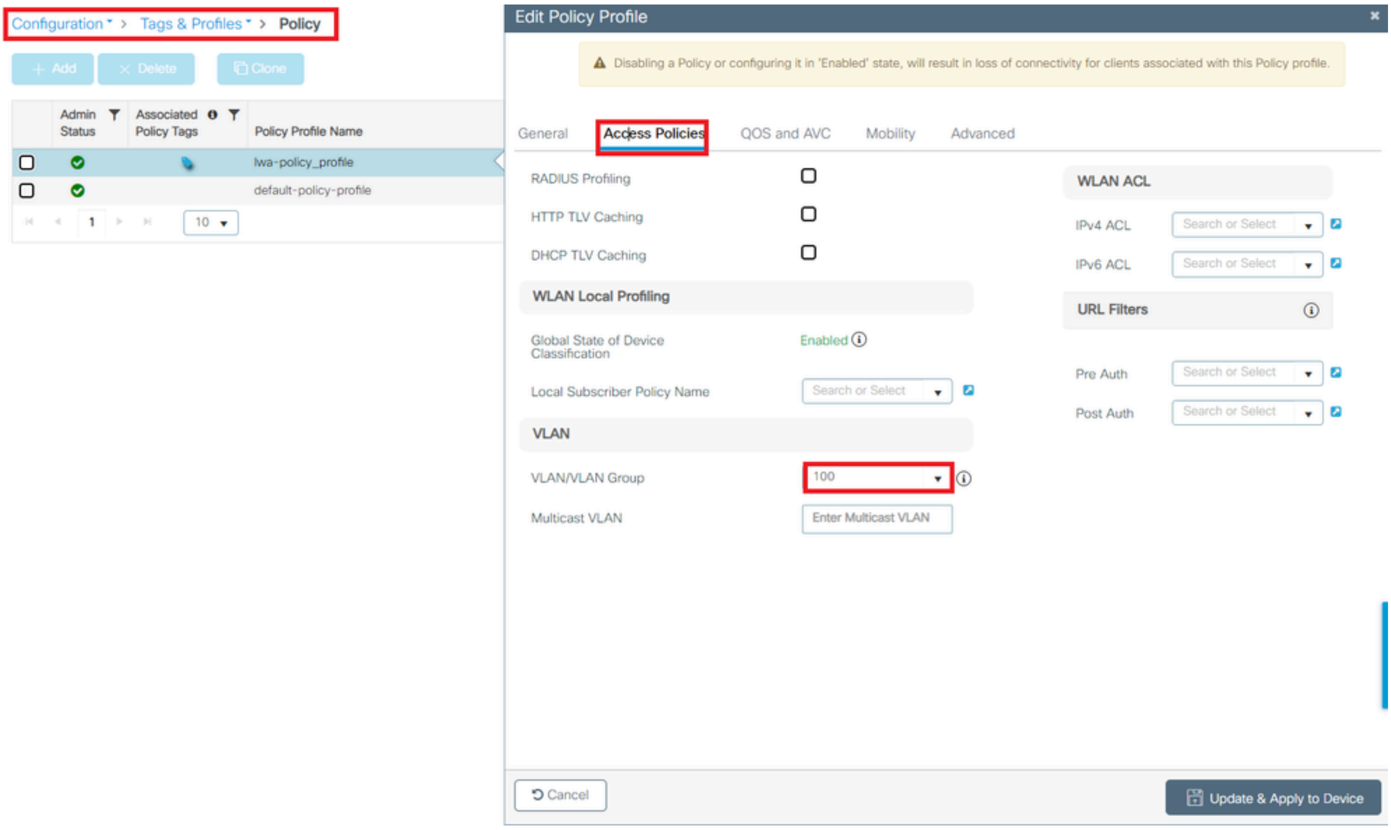
```
RX: DHCPv4 from interface capwap_90400002 on vlan 100 Src MAC: aaaa.bbbb.cccc Dst MAC: ffff.ffff.ffff s
TX: DHCPv4 from interface capwap_90400002 on vlan 100 Src MAC: aaaa.bbbb.cccc Dst MAC: ffff.ffff.ffff s
```

推荐的解决方案

首先：确保为策略配置文件分配正确的VLAN。

从 GUI：

1. 转至Configuration > Tags & Profiles > Policy。
2. 选择使用的策略配置文件。
3. 转到Access Policies。
4. 选择正确的VLAN。



从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>
```

第二：确保某个位置有可供用户使用的DHCP池。检查其配置和可达性。RA跟踪显示VLAN DHCP DORA进程正在经历的哪个VLAN。确保此VLAN为正确的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,
```

自定义门户未显示给最终客户端

从最终客户端经历的可能行为

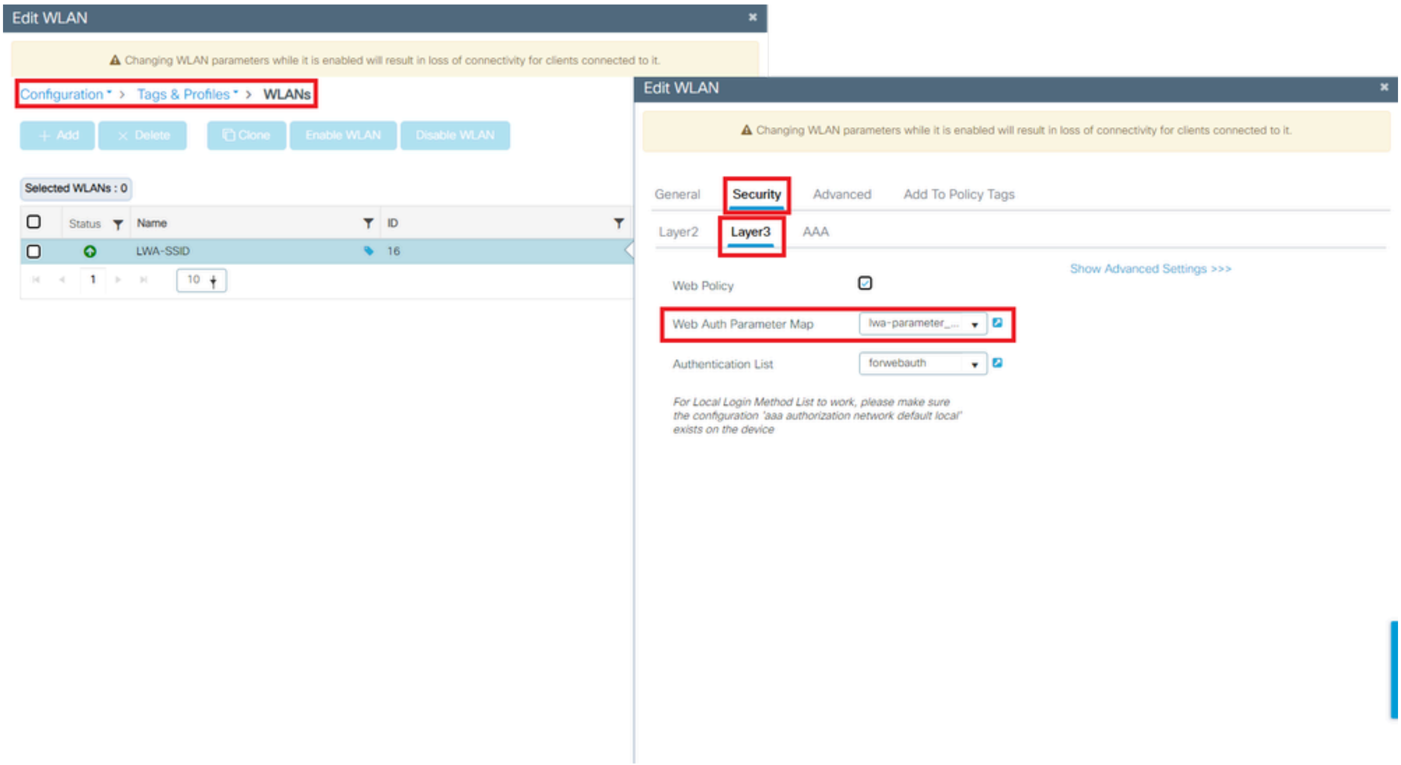
- 可看到WLC的默认门户。

推荐的解决方案

首先：确保WLAN使用自定义的Web身份验证参数映射。

从 GUI：

1. 转至Configuration > Tags & Profiles > WLANs。
2. 从列表中选择WLAN。
3. 转至Security > Layer 3。
4. 选择自定义Web身份验证参数映射。



Changing WLAN parameters while it is enabled will result in loss of connectivity for clients connected to it.

Configuration > Tags & Profiles > WLANs

Selected WLANs : 0

□	Status	Name	ID
□	●	LWA-SSID	16

1 10

Changing WLAN parameters while it is enabled will result in loss of connectivity for clients connected to it.

Web Policy ☑

Web Auth Parameter Map lwa-parameter_...

Authentication List forwebauth

For Local Login Method List to work, please make sure the configuration 'aaa authorization network default local' exists on the device

已选择自定义参数映射

从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>

第二：请注意，从Cisco.com Web门户下载的自定义下载无法与非常坚固和复杂的编程接口配合使用。通常，建议只在CSS级别进行更改，可能添加或删除映像。不支持Applet、PHP、修改变量、React.js等。如果未向客户端显示自定义门户，请尝试使用默认WLC页面并查看是否可以复制问题。如果成功看到门户，则说明在要使用的自定义页面上存在不受支持的内容。

第三：如果使用EWC(嵌入式无线控制器)，建议使用CLI添加自定义页面，以确保其正确显示：

<#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
```

未向最终客户端正确显示自定义门户

从最终客户端经历的可能行为

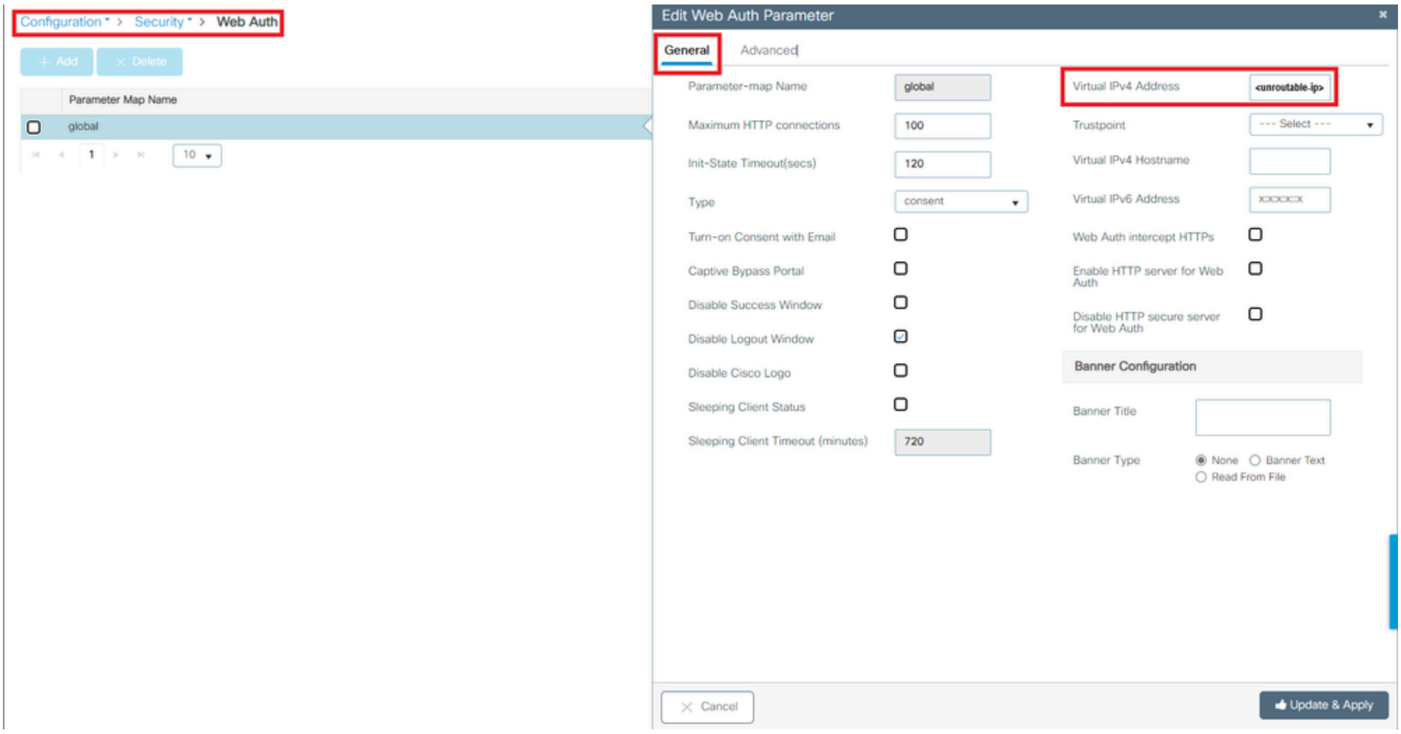
- 未正确呈现自定义门户（即不显示图像）。

推荐的解决方案

确保为全局参数映射分配了虚拟IP地址。

从 GUI：

1. 转至Configuration > Security > Web Auth。
2. 从列表中选择global参数映射。
3. 添加无法路由的虚拟IP地址。



☐	global

Parameter-map Name	global	Virtual IPv4 Address	<unroutable-ip>
Maximum HTTP connections	100	Trustpoint	--- Select ---
Init-State Timeout(secs)	120	Virtual IPv4 Hostname	
Type	consent	Virtual IPv6 Address	X:X:X:X::X
Turn-on Consent with Email	☐	Web Auth intercept HTTPs	☐
Captive Bypass Portal	☐	Enable HTTP server for Web Auth	☐
Disable Success Window	☐	Disable HTTP secure server for Web Auth	☐
Disable Logout Window	☑		
Disable Cisco Logo	☐	Banner Title	
Sleeping Client Status	☐	Banner Type	● None ○ Banner Text ○ Read From File
Sleeping Client Timeout (minutes)	720		

全局参数映射上的虚拟IP地址设置为无法路由的IP地址

从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>
```

提示：虚拟IP地址用作Web身份验证登录页的重定向地址。网络上的其他设备不能具有相同的IP，不能映射到物理端口，也不能存在于任何路由表中。因此，建议您将虚拟IP配置为不可路由的IP地址，但只能使用RFC5737上的地址。

门户显示“您的连接不安全/验证签名失败”

从最终客户端经历的可能行为

- 打开该门户时，客户端会看到指示连接不安全的错误。
- 门户需要使用证书。

要了解的事项

如果门户预期显示在HTTPS下，则意味着它需要使用SSL（安全套接字层）证书。所述证书必须由第三方证书颁发机构(CA)颁发，以验证域是真实的；在输入凭证和/或查看门户时，向终端客户端提供信任。要将证书上传到WLC，请参阅本文档。

推荐的解决方案

首先：重新启动所需的HTTP/HTTPS服务。现在，可以更好地控制需要启用哪些HTTP/HTTPS服务器来完全适应网络的需求。有关为Web身份验证配置HTTP和HTTPS请求的详细信息，请参阅此链接。

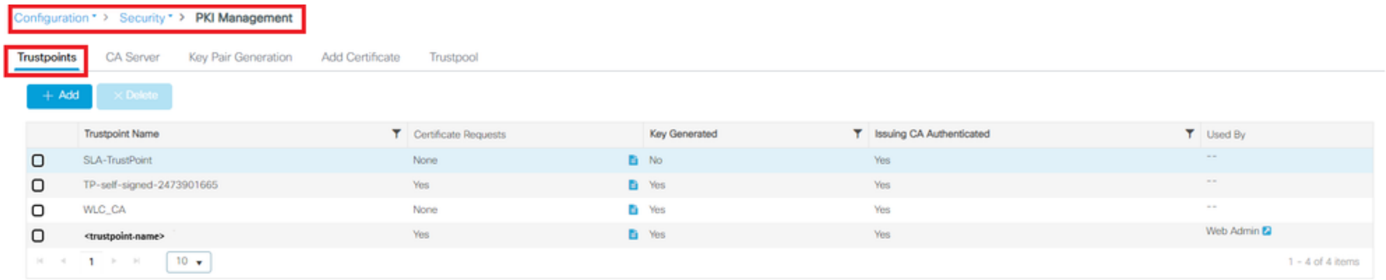
从CLI：

```
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
```

第二：确保证书已正确上传到WLC并且其有效日期正确。

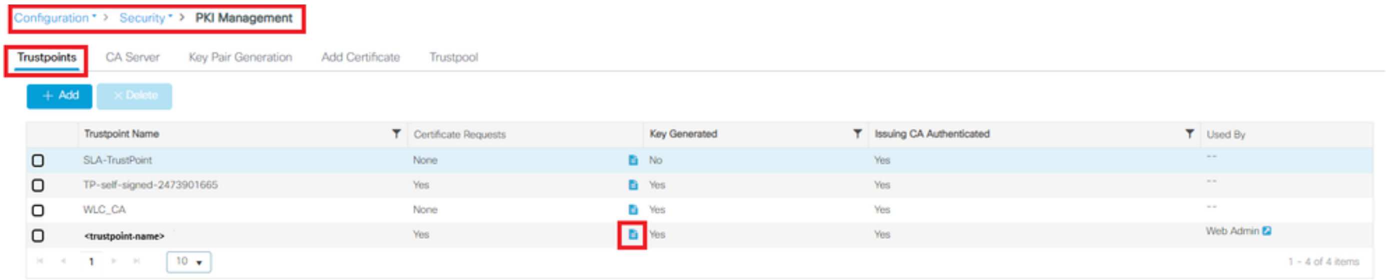
从 GUI：

1. 转至Configuration > Security > PKI Management
2. 在列表中搜索信任点
3. 查看其详细信息



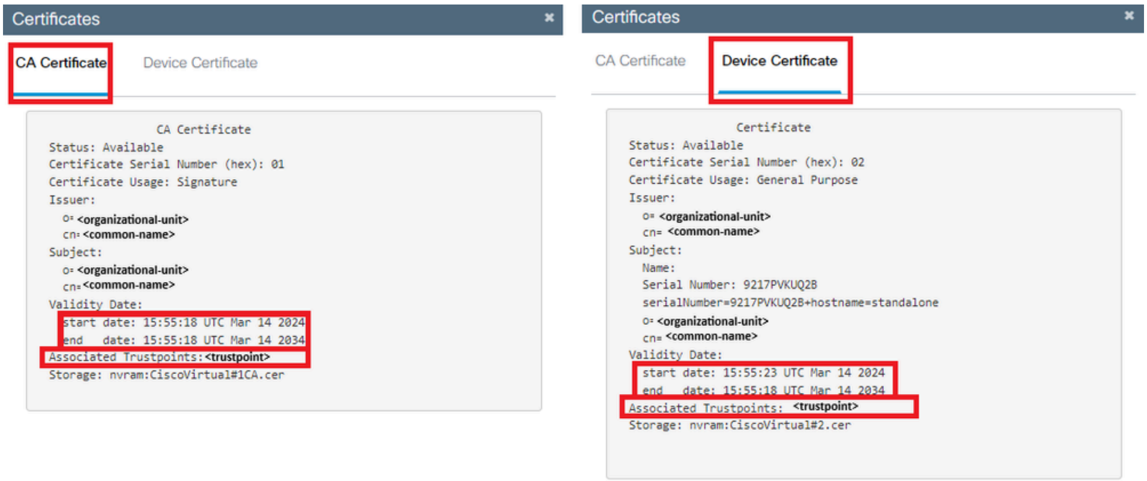
	Trustpoint Name	Certificate Requests	Key Generated	Issuing CA Authenticated	Used By
□	SLA-TrustPoint	None	No	Yes	--
□	TP-self-signed-2473901665	Yes	Yes	Yes	--
□	WLC_CA	None	Yes	Yes	--
□	<trustpoint-name>	Yes	Yes	Yes	Web Admin

检查信任点



	Trustpoint Name	Certificate Requests	Key Generated	Issuing CA Authenticated	Used By
□	SLA-TrustPoint	None	No	Yes	--
□	TP-self-signed-2473901665	Yes	Yes	Yes	--
□	WLC_CA	None	Yes	Yes	--
□	<trustpoint-name>	Yes	Yes	Yes	Web Admin

ExistsCheck Trustpoint



```
                CA Certificate
Status: Available
Certificate Serial Number (hex): 01
Certificate Usage: Signature
Issuer:
   o: <organizational-unit>
   cn: <common-name>
Subject:
   o: <organizational-unit>
   cn: <common-name>
Validity Date:
   start date: 15:55:18 UTC Mar 14 2024
   end   date: 15:55:18 UTC Mar 14 2034
Associated Trustpoints:<trustpoint>
Storage: nvram:CiscoVirtual#1CA.cer
```

```
                Certificate
Status: Available
Certificate Serial Number (hex): 02
Certificate Usage: General Purpose
Issuer:
   o= <organizational-unit>
   cn= <common-name>
Subject:
   Name:
   Serial Number: 9217PVKUQ2B
   serialNumber=9217PVKUQ2B+hostname=standalone
   o= <organizational-unit>
   cn= <common-name>
Validity Date:
   start date: 15:55:23 UTC Mar 14 2024
   end   date: 15:55:18 UTC Mar 14 2034
Associated Trustpoints:  <trustpoint>
Storage: nvram:CiscoVirtual#2.cer
```

DetailsCheckTrustpoint Validity

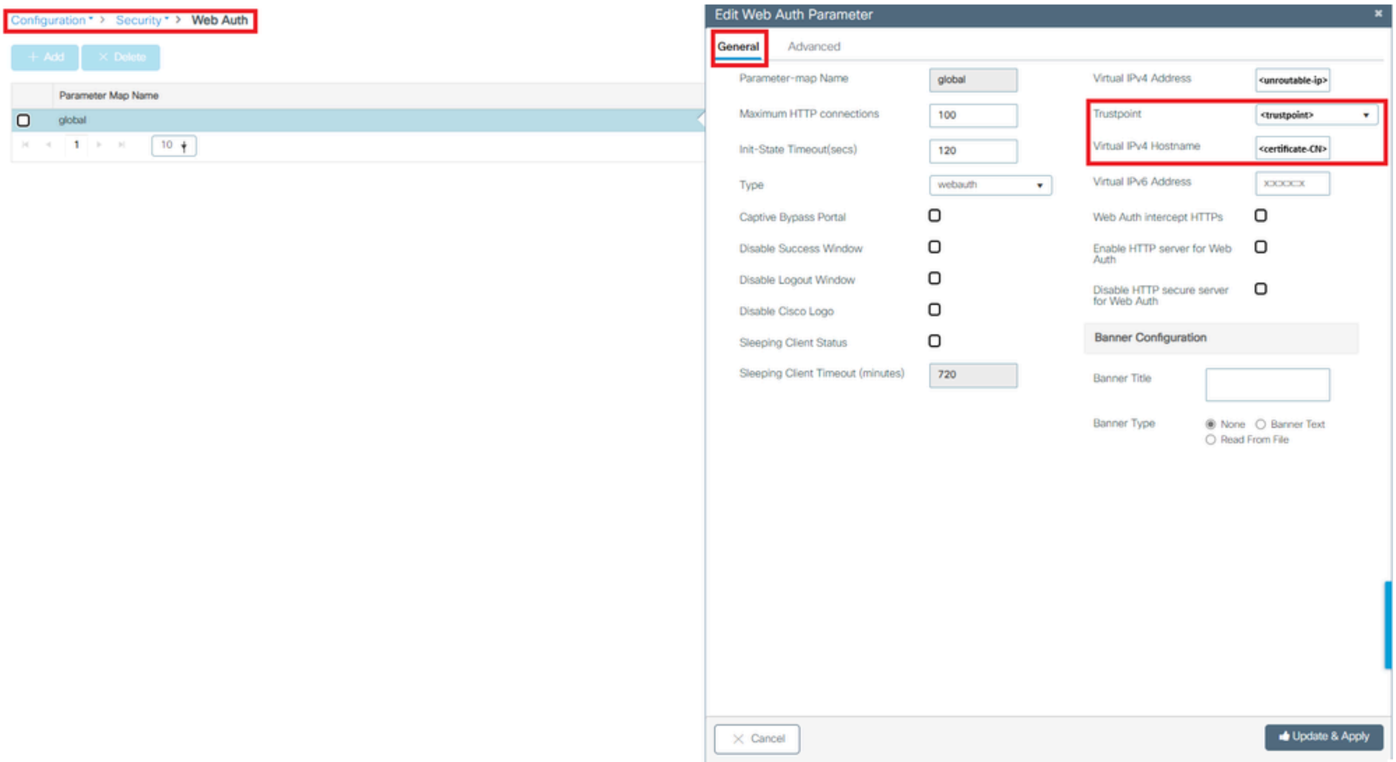
从CLI：

```
<#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>
```

第三：确保在WebAuth参数映射上选择要使用的正确证书，以及虚拟IPv4主机名与证书中的公用名(CN)匹配。

从 GUI：

1. 转至Configuration > Security > Web Auth。
2. 从列表中选择使用的参数映射。
3. 检查信任点和虚拟IPv4主机名是否正确。



Parameter-map Name: global
Maximum HTTP connections: 100
Init-State Timeout(secs): 120
Type: webauth
Captive Bypass Portal □
Disable Success Window □
Disable Logout Window □
Disable Cisco Logo □
Sleeping Client Status □
Sleeping Client Timeout (minutes): 720
Virtual IPv4 Address: <unroutable-ip>
Trustpoint: <trustpoint>
Virtual IPv4 Hostname: <certificate-CN>
Virtual IPv6 Address: XXXXX
Web Auth intercept HTTPs □
Enable HTTP server for Web Auth □
Disable HTTP secure server for Web Auth □
Banner Title:
Banner Type: ● None ○ Banner Text ○ Read From File

检查信任点和虚拟IPv4主机名

从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>
```

相关信息

- 配置本地Web身份验证
- 基于Web的身份验证(EWC)
- 自定义Catalyst 9800 WLC上的Web身份验证门户
- 在Catalyst 9800 WLC上生成和下载CSR证书
- 配置虚拟接口

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。