

Beheben gängiger Probleme mit LWA auf 9800 WLCs

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Radioaktive \(RA\) Spuren auf dem 9800 WLC](#)

[Erwarteter Datenfluss](#)

[Phasen, die der Kunde aus Client-Sicht durchläuft](#)

[Phasen, die der Client aus WLC-Sicht durchläuft](#)

[Häufige Fehlerbehebungsszenarien](#)

[Authentifizierungsfehler](#)

[Portal wird dem Benutzer nicht angezeigt, aber Client wird verbunden angezeigt](#)

[Portal wird dem Benutzer nicht angezeigt, und Client stellt keine Verbindung her](#)

[Endclients erhalten keine IP-Adresse](#)

[Dem Endkunden wird kein benutzerdefiniertes Portal angezeigt.](#)

[Das angepasste Portal wird dem Endkunden nicht richtig angezeigt.](#)

[Portal: "Ihre Verbindung ist nicht sicher/Überprüfung der Signatur fehlgeschlagen"](#)

[Zugehörige Informationen](#)

Einleitung

In diesem Dokument werden häufige Probleme bei Clients beschrieben, die sich mit einem WLAN mit lokaler Webauthentifizierung (LWA) verbinden.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Grundkenntnisse in folgenden Bereichen verfügen:

- Cisco Wireless LAN Controller (WLC) der Serie 9800
- Allgemeine Kenntnisse über die lokale Web-Authentifizierung (LWA) und deren Konfiguration

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und

Hardwareversionen:

- 9800-CL WLC
- Cisco Access Point 9120AXI
- 9800 WLC Cisco IOS® XE Version 17.9.3

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

LWA ist eine Art von WLAN-Authentifizierung, die auf dem WLC konfiguriert werden kann, wobei der Endclient, der versucht, eine Verbindung herzustellen, nachdem er das WLAN aus der Liste ausgewählt hat, dem Benutzer ein Portal präsentiert. In diesem Portal kann der Benutzer einen Benutzernamen und ein Kennwort (abhängig von der ausgewählten Konfiguration) eingeben, um die Verbindung mit dem WLAN abzuschließen.

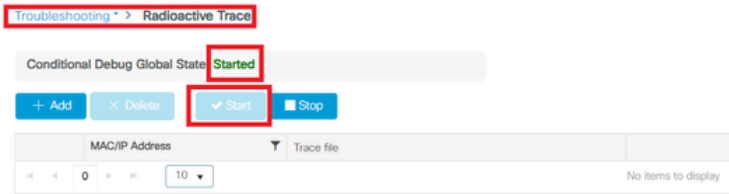
Weitere Informationen zur Konfiguration von LWA auf dem 9800 WLC finden Sie im Konfigurationsleitfaden [Configure Local Web Authentication \(Lokale Webauthentifizierung konfigurieren\)](#).

Radioaktive (RA) Spuren auf dem 9800 WLC

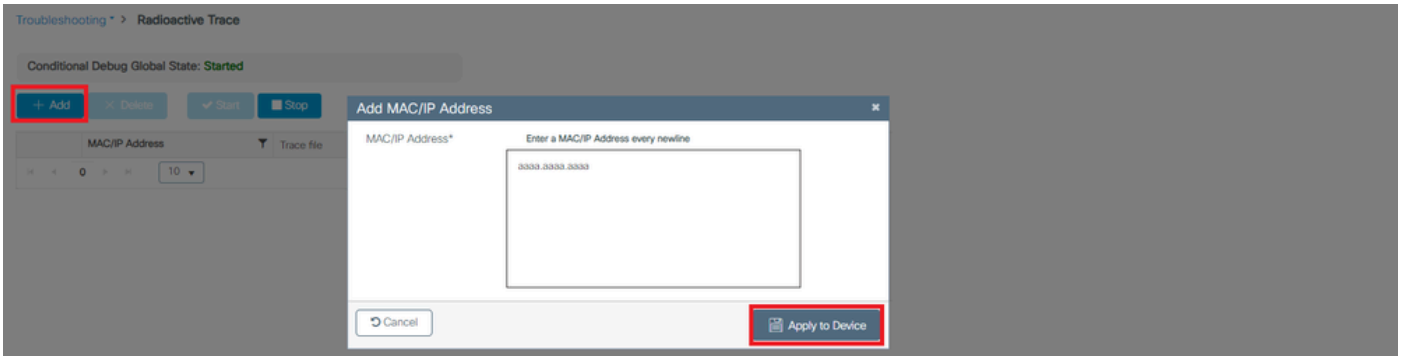
Radioactive Traces sind ein hervorragendes Tool zur Fehlerbehebung bei verschiedenen Problemen mit dem WLC und der Client-Verbindung. Um RA-Spuren zu sammeln, gehen Sie wie folgt vor:

Über die GUI:

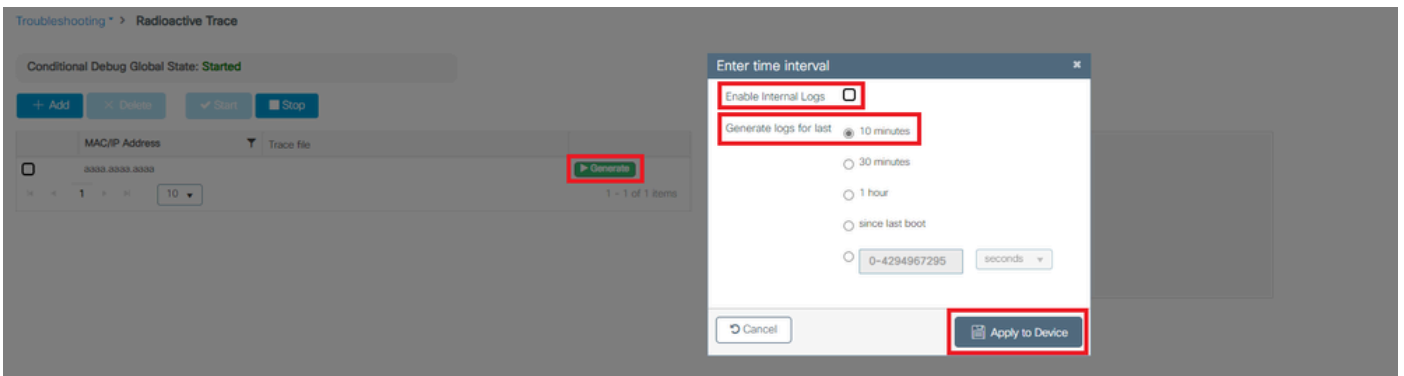
1. Gehen Sie zu Fehlerbehebung > Radioaktive Spur.
2. Klicken Sie auf Start, um den globalen Zustand für bedingtes Debuggen zu aktivieren.
3. Klicken Sie auf + Hinzufügen. Ein Popup-Fenster wird geöffnet. Geben Sie die MAC-Adresse des Clients ein. Es werden alle MAC-Adressformate akzeptiert (aabb.ccdd.eeff, AABB.CCDD.EEEE, aa:bb:cc:dd:ee:ff oder AA:BB:CC:DD:EE:FF). Klicken Sie dann auf Auf Gerät anwenden.
4. Lassen Sie den Kunden das Problem 3 oder 4 Mal reproduzieren.
5. Sobald das Problem reproduziert wurde, klicken Sie auf Generate (Erstellen).
6. Ein neues Popup-Fenster wird geöffnet. Erstellen Sie die Protokolle der letzten 10 Minuten. (In diesem Fall ist es nicht erforderlich, die internen Protokolle zu aktivieren). Klicken Sie auf Apply to Device (Auf Gerät anwenden), und warten Sie, bis die Datei verarbeitet wird.
7. Klicken Sie nach dem Erstellen der Datei auf das Symbol Download.



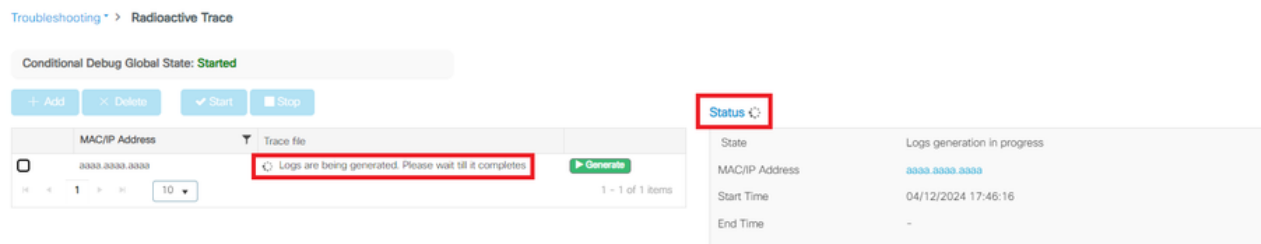
Bedingtes Debuggen aktivieren



Hinzufügen einer Client-MAC-Adresse




Erstellen von Protokollen für die letzten 10 Minuten



Warten Sie, bis die Datei

Conditional Debug Global State: **Started**

+ Add × Delete ▼ Start ■ Stop

MAC/IP Address	Trace file	
aaaa.aaaa.aaaa	debugTrace_aaaa.aaaa.aaaa.txt	

1 - 1 of 1 items

▶ Generate


Last Run Result

✓ 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 

generiert wurdeDatei heruntergeladen

Über die CLI:

<#root>

WLC# debug wireless mac

<mac-address>

monitor-time 600

Eine neue Datei im Bootflash wird generiert und heißt 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

Datei zur Analyse auf einen externen Server kopieren

<#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

Weitere Informationen zur radioaktiven Verfolgung finden Sie unter [diesem Link](#).

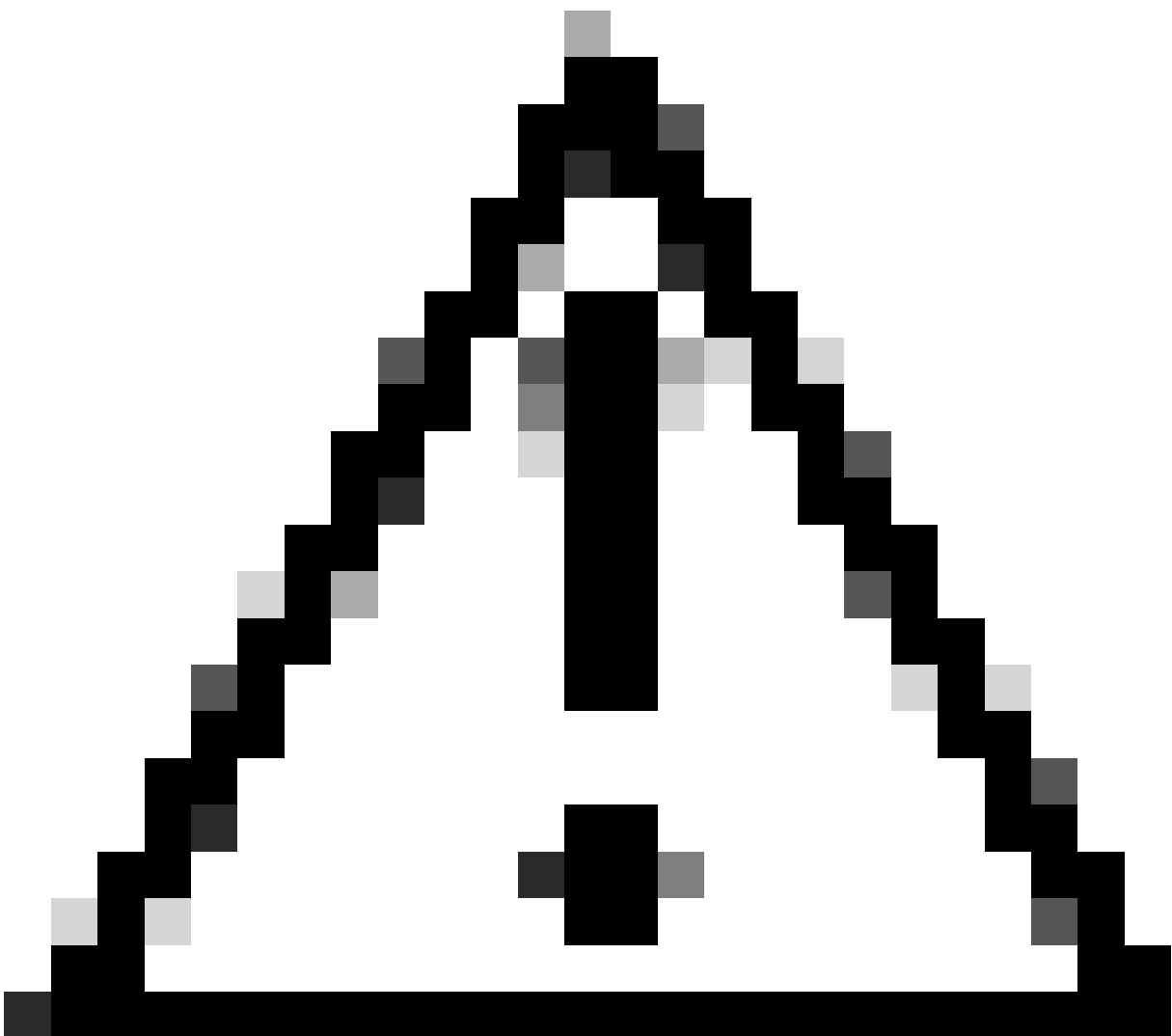
Erwarteter Datenfluss

Informationen zum Verständnis des Funktionsszenarios von LWA finden Sie in den .

Phasen, die der Kunde aus Client-Sicht durchläuft

1. Dem WLAN zugewiesener Endclient.
2. Dem Client wird eine IP-Adresse zugewiesen.
3. Das Portal wird dem Endkunden angezeigt.
4. Der Endclient gibt Anmeldeinformationen ein.
5. Der Endclient ist authentifiziert.
6. Der Endclient kann im Internet surfen.

Phasen, die der Client aus WLC-Sicht durchläuft



Vorsicht: Viele Protokolle der Radio Active (RA)-Spur wurden der Einfachheit halber weggelassen.

Dem WLAN zugewiesener Endclient

<#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-Authentifizierung

<#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_WEBAUTH
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_WEBAUTH
MAC: aaaa.bbbb.cccc

L2 Authentication of station is successful.

, L3 Authentication : 1

Client erhält zugewiesene IP-Adresse

<#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-Authentifizierung

<#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_WEBAUTH
```

Client erhält IP-Adresse

<#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
```

Portalverarbeitung

<#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 verarbeitet Informationen, die auf den verbindenden Endkunden angewendet werden sollen

<#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 "p€"

Applying Attribute : addrv6 0 " ?İ??"

Applying Attribute : addrv6 0 " ?İ??"

Applying Attribute : addrv6 0 " ?İ??"

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 wendet Benutzerprofil auf den verbundenen Endkunden an

<#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-Authentifizierung ist abgeschlossen

```
<#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
```

AAA-Attribute auf Endkunden angewendet

```
<#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
```

```
" ]
```

Endkunde erreicht Ausführungszustand.

```
<#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
```

Häufige Fehlerbehebungsszenarien

Authentifizierungsfehler

Überlegungen

- Das angezeigte Portal besagt nach Eingabe der richtigen Anmeldeinformationen "Authentifizierung fehlgeschlagen".
- WLC zeigt Client im Status "Web Auth Pending" (Webauthentifizierung ausstehend) an.
- Die erste Splash-Seite wird dem Benutzer erneut angezeigt.

WLC RA-Ablaufverfolgungen

<#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'
```

Empfohlene Lösungen

Stellen Sie sicher, dass die standardmäßige AAA-Methodenliste für die Netzwerkautorisierung in der WLC-Konfiguration vorhanden ist.

Über die GUI:

1. Gehen Sie zu Configuration > Security > AAA > AAA Method List > Authorization. Klicken Sie auf + Hinzufügen.
2. Konfigurieren Sie es als:
 1. Methodenlistenname: default
 2. Typ: Netzwerk
 3. Gruppentyp: lokal
3. Klicken Sie auf Auf Gerät anwenden.

Quick Setup: AAA Authorization

Method List Name*

Type* ⓘ

Group Type ⓘ

Authenticated

Available Server Groups

radius
ldap
tacacs+
802.1x-group
ldapgr

>
<
>>
<<

Assigned Server Groups

⬆
⬆
⬇
⬇

Cancel

Apply to Device

Configuration > Security > AAA [Show Me How](#)

+ AAA Wizard

Servers / Groups **AAA Method List** AAA Advanced

Authentication

Authorization

Accounting

+ Add × Delete

	Name	Type	Group Type	Group1	Group2	Group3	Group4
<input type="checkbox"/>	default	network	local	N/A	N/A	N/A	N/A

Über die CLI:

<#root>

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

Portal wird dem Benutzer nicht angezeigt, aber Client wird verbunden angezeigt

Mögliches Verhalten des Endkunden

- Der Endkunde sieht sein Gerät als "verbunden".
- Das Portal wird dem Endkunden nicht angezeigt.

- Der Endclient gibt keine Anmeldeinformationen ein.
- Dem Endclient wurde eine IP-Adresse zugewiesen.
- WLC zeigt den Client im Status "Run" an.

WLC RA-Ablaufverfolgungen

Dem Client wird eine IP-Adresse zugewiesen, und er wird auf dem WLC sofort in den Status "Run" versetzt. Benutzerattribute zeigen nur das dem Endclient zugewiesene VLAN an.

```
<#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
```

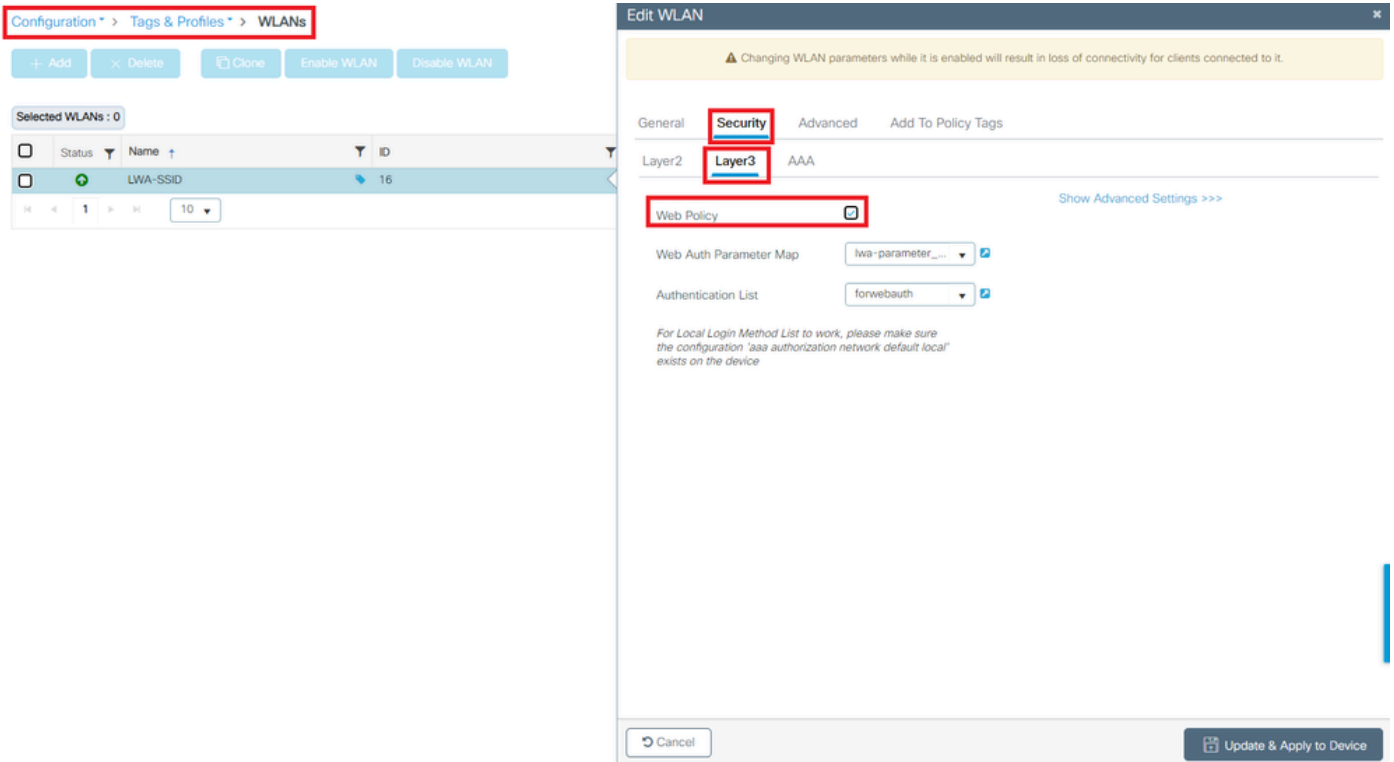
```
MAC: aaaa.bbbb.cccc Client state transition: S_CO_IP_LEARN_IN_PROGRESS -> S_CO_RUN
```

Empfohlene Lösungen

Stellen Sie sicher, dass die Webrichtlinie im WLAN aktiviert ist.

Über die GUI:

1. Gehen Sie zu Configuration > Tags & Profiles > WLANs.
2. Wählen Sie die LWA-WLANs aus.
3. Gehen Sie zu Security > Layer 3.
4. Stellen Sie sicher, dass das Kontrollkästchen Webrichtlinie aktiviert ist.



Web-Richtlinie muss aktiviert werden

Über die CLI:

```
<#root>
```

```
WLC# configure terminal
```

```
WLC(config)# wlan
```

```
<wlan>
```

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

Portal wird dem Benutzer nicht angezeigt, und Client stellt keine Verbindung her

Mögliches Verhalten des Endkunden

- Der Endkunde erkennt, dass sein Gerät ständig versucht, eine Verbindung herzustellen.
- Das Portal wird dem Endkunden nicht angezeigt.
- Dem Endclient wurde keine IP-Adresse zugewiesen.
- WLC zeigt den Client im Zustand "Webauth Pending" (Webauth ausstehend) an.

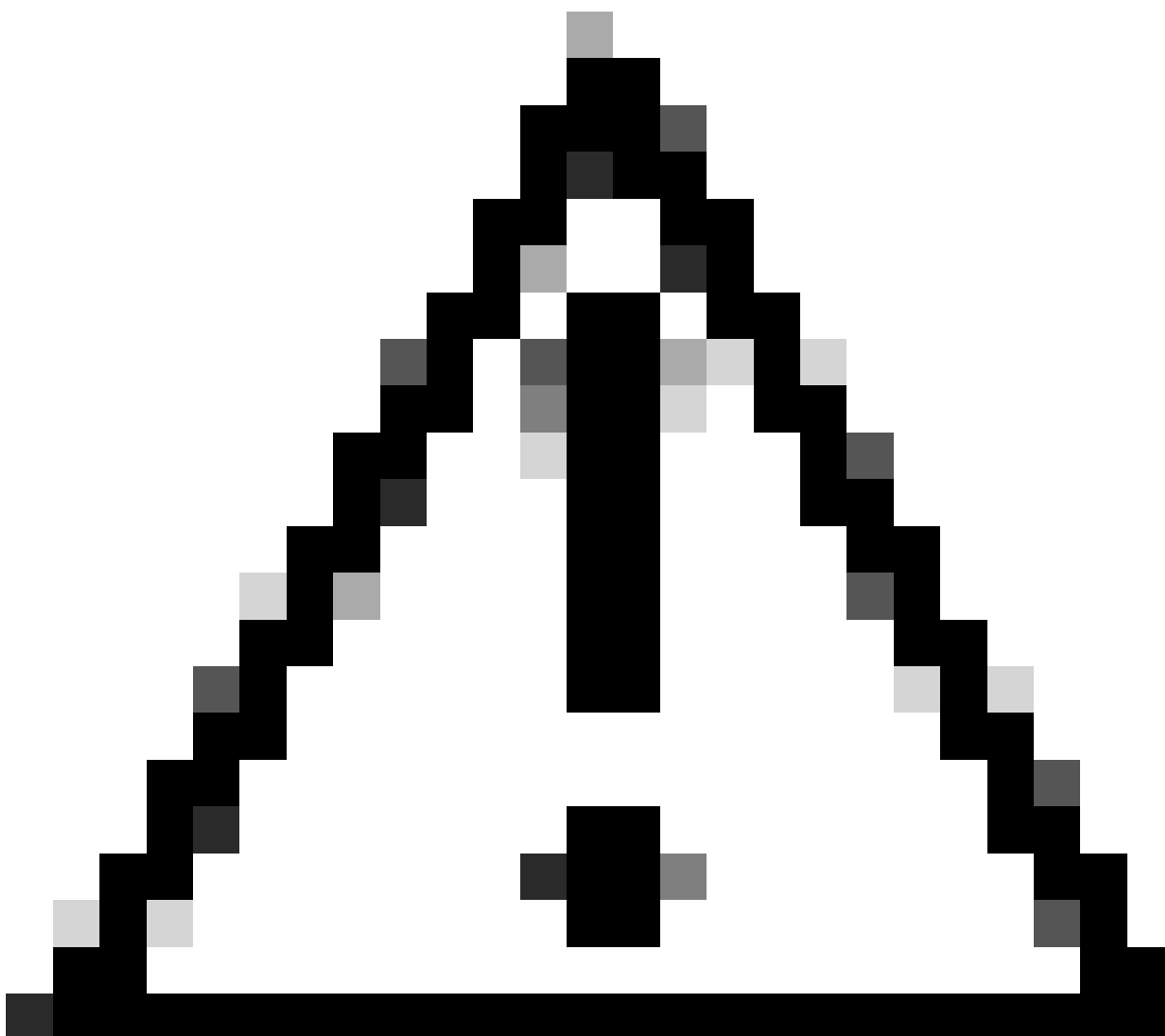
Empfohlene Lösungen

Aktivieren Sie die erforderlichen HTTP-/HTTPS-Server. Es ist jetzt möglich, mehr Kontrolle

darüber zu haben, welche HTTP-/HTTPS-Server aktiviert werden müssen, um sich vollständig an die Anforderungen des Netzwerks anzupassen. Weitere Informationen zur Konfiguration von HTTP- und HTTPS-Anforderungen für die Webauthentifizierung finden Sie unter [diesem Link](#), da mehrere HTTP-Kombinationen unterstützt werden. Beispielsweise können HTTPSs nur für Webadmin und HTTP für Webauth verwendet werden.

So ermöglichen Sie über die Kommandozeile eine administrative Geräteverwaltung und Webauthentifizierung mit HTTP- und HTTPS-Zugriff:

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



Achtung: Wenn beide Server deaktiviert sind, besteht kein Zugriff auf die grafische Benutzeroberfläche (GUI) des WLC.

Endclients erhalten keine IP-Adresse

Mögliches Verhalten des Endkunden

- Endkunden sehen, dass ihr Gerät ununterbrochen versucht, eine IP-Adresse zu erhalten.
- WLC zeigt den Client im Status "IP Learning" an.

WLC RA-Ablaufverfolgungen

Entdeckungsanfragen ohne Angebot zurück.

```
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
```

Empfohlene Lösungen

Erstens: Stellen Sie sicher, dass dem Richtlinienprofil das richtige VLAN zugewiesen ist.

Über die GUI:

1. Gehen Sie zu Konfiguration > Tags & Profile > Richtlinie.
2. Wählen Sie das verwendete Richtlinienprofil aus.
3. Gehen Sie zu Zugriffsrichtlinien.
4. Wählen Sie das richtige VLAN aus.

The screenshot shows the Cisco WLC GUI configuration page for a Policy Profile. The breadcrumb navigation at the top left is "Configuration > Tags & Profiles > Policy". The main content area is titled "Edit Policy Profile" and has a warning message: "Disabling a Policy or configuring it in 'Enabled' state, will result in loss of connectivity for clients associated with this Policy profile." The "Access Policies" tab is selected and highlighted with a red box. Under the "VLAN" section, the "VLAN/VLAN Group" is set to "100", also highlighted with a red box. Other sections include "WLAN Local Profiling" (Global State of Device Classification: Enabled), "WLAN ACL" (IPv4 and IPv6 ACLs), and "URL Filters" (Pre and Post Auth).

Über die 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>
```

Zweitens: Stellen Sie sicher, dass dem Benutzer irgendwo ein DHCP-Pool zur Verfügung steht. Überprüfen Sie die Konfiguration und die Erreichbarkeit. RA-Traces zeigen, welches VLAN der DHCP DORA-Prozess durchläuft. Stellen Sie sicher, dass dieses VLAN das richtige VLAN ist.

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

Dem Endkunden wird kein benutzerdefiniertes Portal angezeigt.

Mögliches Verhalten des Endkunden

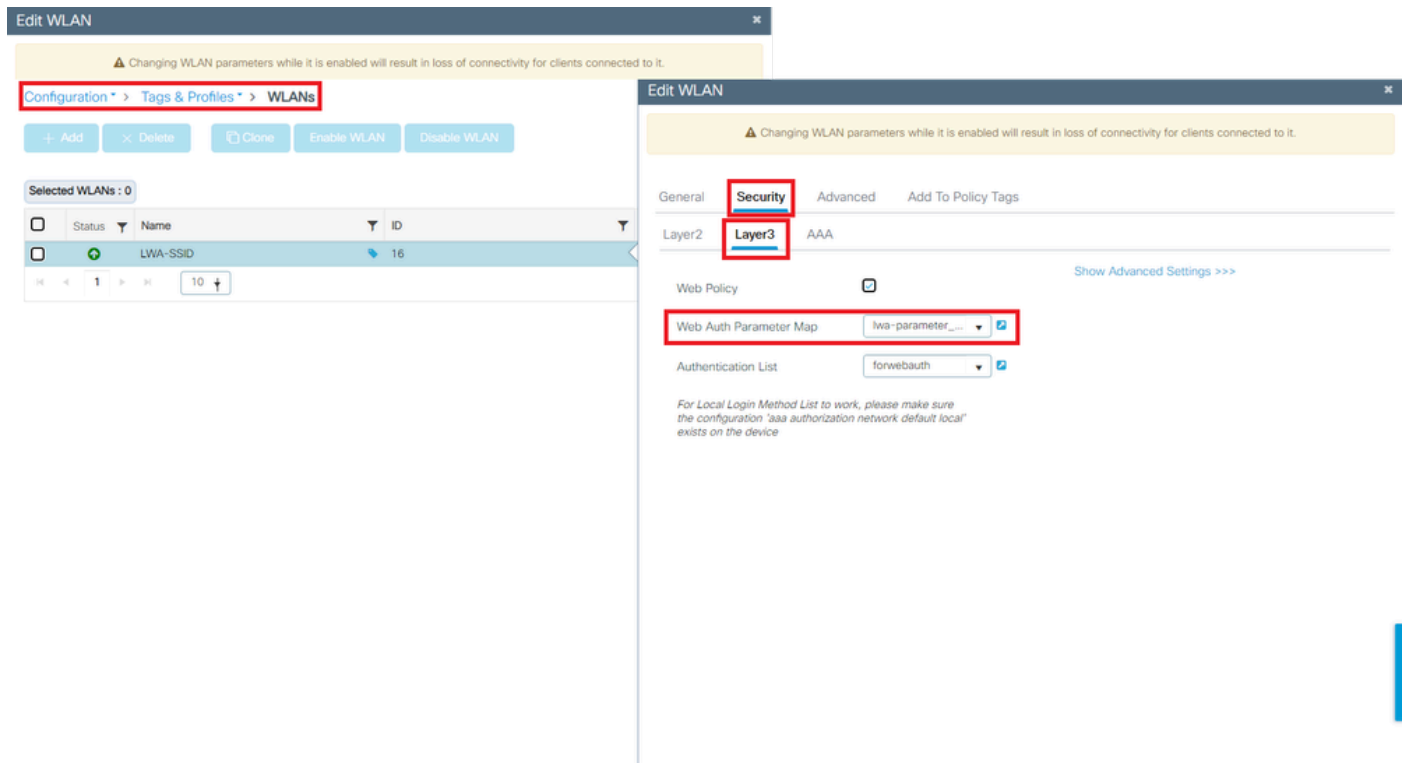
- Das Standardportal des WLC wird angezeigt.

Empfohlene Lösungen

Erstens: Stellen Sie sicher, dass das WLAN die angepasste Web Auth Parameter Map verwendet.

Über die GUI:

1. Gehen Sie zu Configuration > Tags & Profiles > WLANs.
2. Wählen Sie das WLAN aus der Liste aus.
3. Gehen Sie zu Security > Layer 3.
4. Wählen Sie die benutzerdefinierte Zuordnung von Web Auth-Parametern aus.



Benutzerdefinierte Parameterzuordnung ausgewählt

Über die 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>
```

Zweitens: Es ist wichtig zu beachten, dass die angepassten Downloads über das Webportal [Cisco.com](https://www.cisco.com) nicht mit einer sehr robusten und komplizierten Programmierschnittstelle funktionieren. Es wird generell empfohlen, Änderungen nur auf CSS-Ebene vorzunehmen und möglicherweise Bilder hinzuzufügen oder zu entfernen. Applets, PHP, modifizierte Variablen, React.js usw. werden nicht unterstützt. Wenn dem Client kein benutzerdefiniertes Portal angezeigt wird, verwenden Sie die WLC-Standardseiten, um festzustellen, ob das Problem repliziert werden kann. Wenn das Portal erfolgreich gesehen wird, dann gibt es etwas, das auf den angepassten Seiten, die verwendet werden sollen, nicht unterstützt wird.

Drittens: Bei Verwendung eines EWC ([Embedded Wireless Controller](#)) wird empfohlen, die angepassten Seiten über die CLI hinzuzufügen, um sicherzustellen, dass sie ordnungsgemäß angezeigt werden:

```
<#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:loginsuccess.html
```

```
EWC(config-params-parameter-map)# end
```

Das angepasste Portal wird dem Endkunden nicht richtig angezeigt.

Mögliches Verhalten des Endkunden

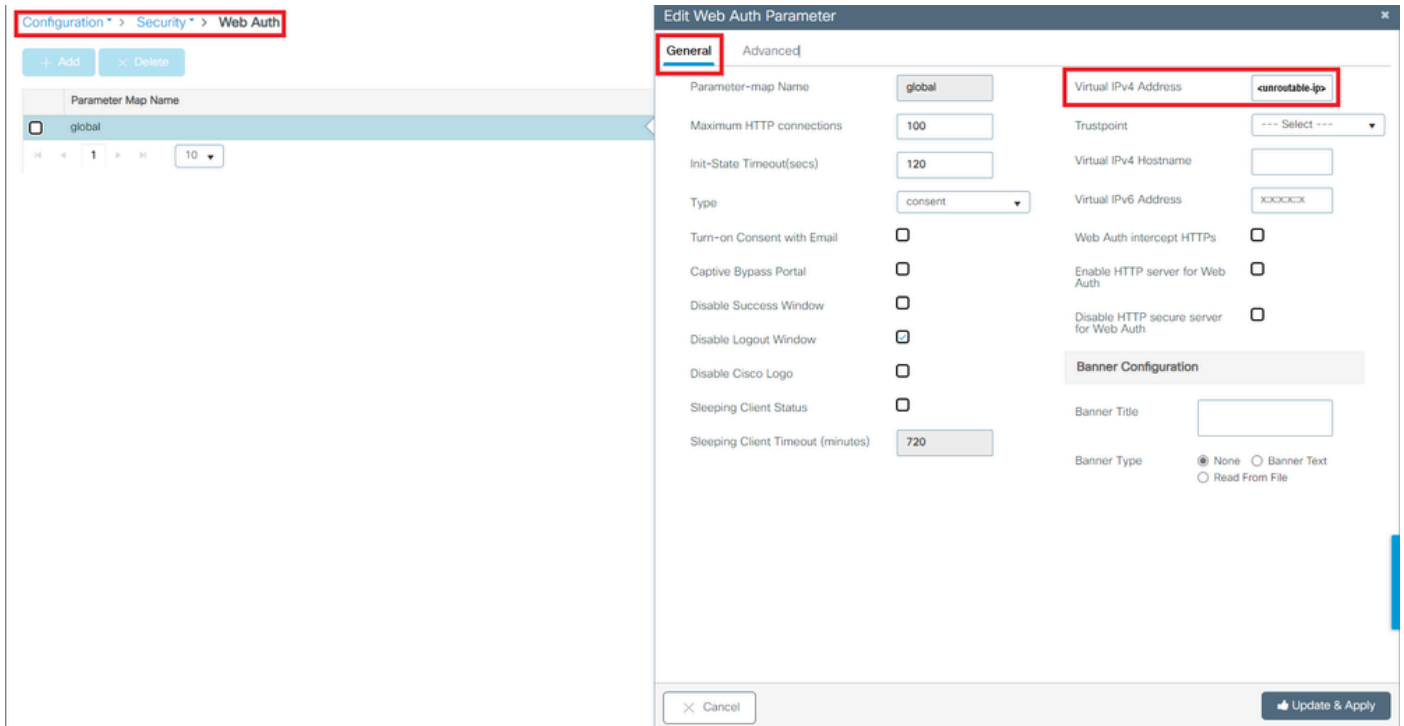
- Das angepasste Portal wird nicht korrekt wiedergegeben (d. h. Bilder werden nicht angezeigt).

Empfohlene Lösungen

Stellen Sie sicher, dass der globalen Parameterzuordnung eine virtuelle IP-Adresse zugewiesen ist.

Über die GUI:

1. Gehen Sie zu Configuration > Security > Web Auth.
2. Wählen Sie die globale Parameterzuordnung aus der Liste aus.
3. Hinzufügen einer nicht routbaren virtuellen IP-Adresse



Virtuelle IP-Adresse in globaler Parameterzuordnung Festlegen auf eine nicht routbare IP-Adresse

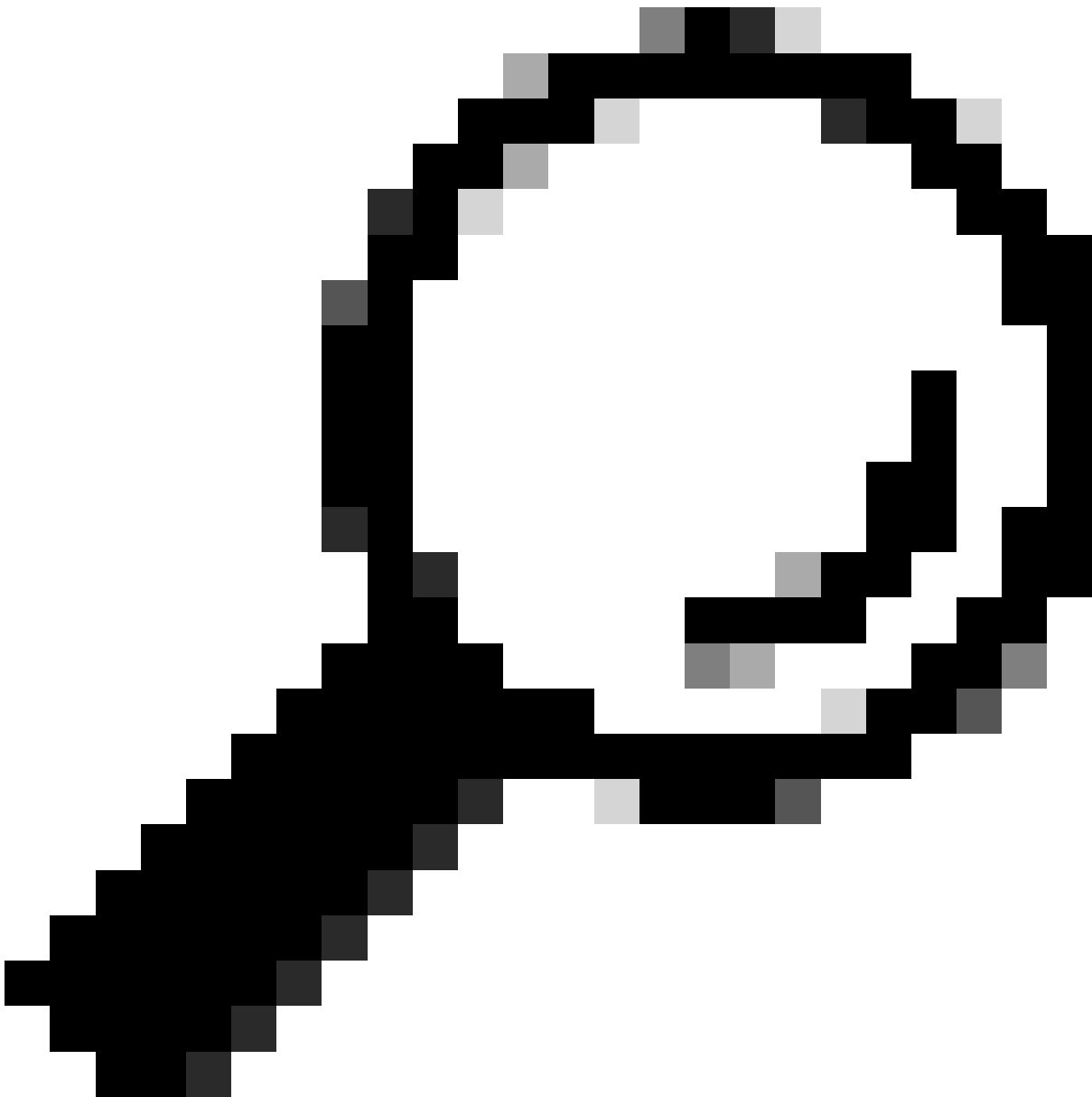
Über die CLI:

<#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>
```



Tipp: Die virtuelle IP-Adresse dient als Umleitungsadresse für die Anmeldeseite für die Webauthentifizierung. Kein anderes Gerät im Netzwerk muss die gleiche IP-Adresse haben. Es darf keinem physischen Port zugeordnet sein und keine Routing-Tabelle enthalten. Es wird daher empfohlen, die virtuelle IP als nicht routbare IP-Adresse zu konfigurieren. Es können nur die IP-Adressen verwendet werden, die sich im [RFC 5737](#) befinden.

Portal sagt, dass "Ihre Verbindung nicht sicher ist/die Signatur fehlgeschlagen ist"

Mögliches Verhalten des Endkunden

- Beim Öffnen des Portals sieht der Client einen Fehler, der besagt, dass die Verbindung nicht sicher ist.
- Es wird erwartet, dass das Portal ein Zertifikat verwendet.

Wissenswertes

Wenn das Portal unter HTTPS angezeigt werden soll, bedeutet dies, dass ein SSL-Zertifikat (Secure Socket Layer) verwendet werden muss. Dieses Zertifikat muss von einer Zertifizierungsstelle (Certificate Authority, CA) eines Drittanbieters ausgestellt werden, um zu überprüfen, ob die Domain tatsächlich existiert; um Endkunden Vertrauen zu gewähren, wenn sie ihre Anmeldeinformationen eingeben und/oder das Portal besuchen. Informationen zum Hochladen eines Zertifikats auf den WLC finden Sie in [diesem Dokument](#).

Empfohlene Lösungen

Erstens: Starten Sie die gewünschten HTTP/HTTPS-Dienste neu. Es ist jetzt möglich, mehr Kontrolle darüber zu haben, welche HTTP-/HTTPS-Server aktiviert werden müssen, um sich vollständig an die Anforderungen des Netzwerks anzupassen. Weitere Informationen zum Konfigurieren von HTTP- und HTTPS-Anforderungen für die Webauthentifizierung finden Sie unter [diesem Link](#).

Über die 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
```

Zweitens: Stellen Sie sicher, dass das Zertifikat korrekt in den WLC hochgeladen wurde und dass das Gültigkeitsdatum korrekt ist.

Über die GUI:

1. Gehen Sie zu Konfiguration > Sicherheit > PKI-Verwaltung
2. Nach dem Vertrauenspunkt in der Liste suchen
3. Details überprüfen

Configuration * > Security * > PKI Management

Trustpoints CA Server Key Pair Generation Add Certificate Trustpool

+ Add - Delete

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

1 - 4 of 4 items

Überprüfen Sie, ob der Vertrauenspunkt

Configuration * > Security * > PKI Management

Trustpoints CA Server Key Pair Generation Add Certificate Trustpool

Trustpoint Name	Certificate Requests	Key Generated	Issuing CA Authenticated	Used By
<input type="checkbox"/> SLA-TrustPoint	None	<input type="checkbox"/> No	Yes	--
<input type="checkbox"/> TP-self-signed-2473901665	Yes	<input type="checkbox"/> Yes	Yes	--
<input type="checkbox"/> WLC_CA	None	<input type="checkbox"/> Yes	Yes	--
<input type="checkbox"/> <trustpoint-name>	Yes	<input checked="" type="checkbox"/> Yes	Yes	Web Admin <input checked="" type="checkbox"/>

Certificates 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 2024
Associated Trustpoints: <trustpoint>
Storage: mwanCiscoVirtualCA.cer

Certificates Device Certificate

Status: Available
Certificate Serial Number (hex): 02
Certificate Usage: General Purpose
Issuer:
o= <organizational-unit>
cn= <common-name>
Subject:
Name:
Serial Number: 9217PVUQ2B
serialNumber=9217PVUQ2B+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 2024
Associated Trustpoints: <trustpoint>
Storage: mwanCiscoVirtualCA.cer

vorhanden ist Überprüfen Sie die Vertrauenspunktdetails Überprüfen Sie die Vertrauenspunktvalidität.

Über die 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>

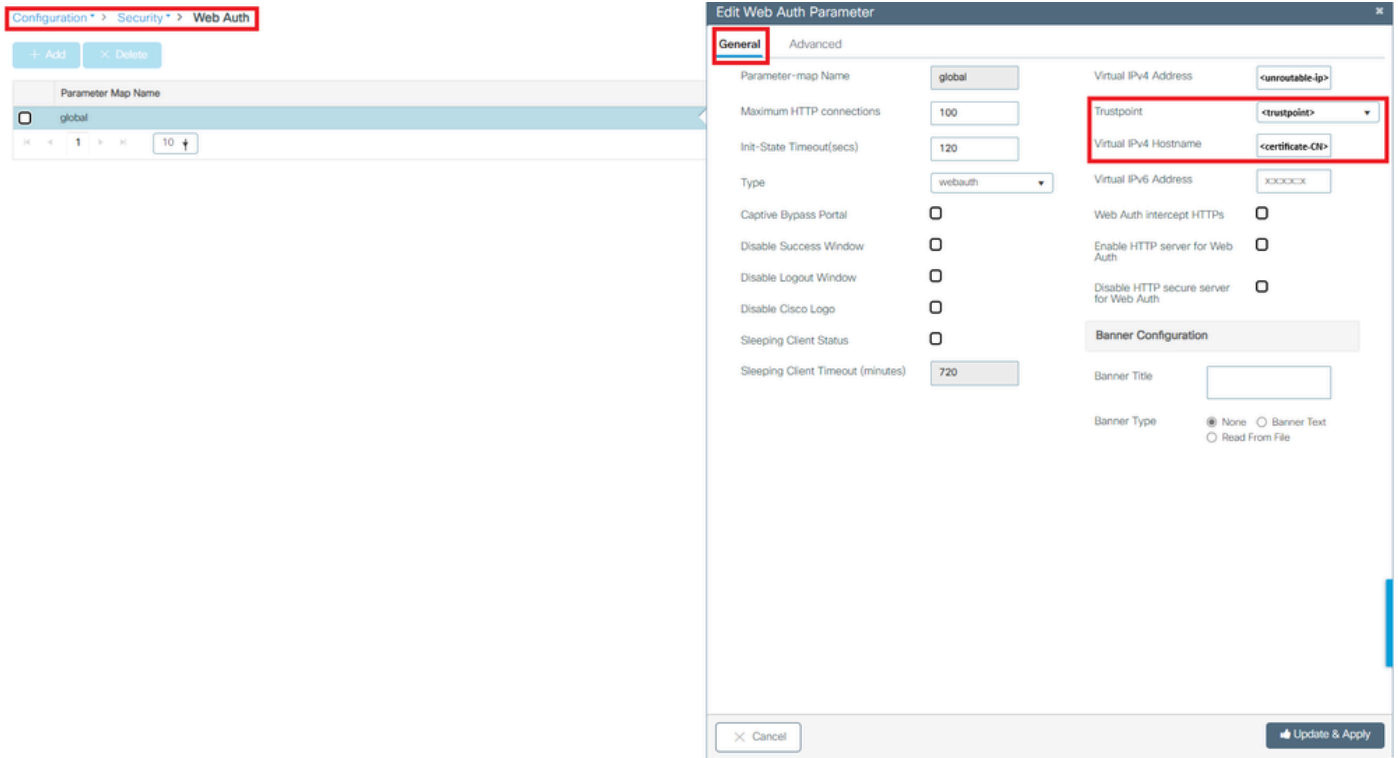
end date: <end-date>

Associated Trustpoints: <trustpoint>

Drittens: Stellen Sie sicher, dass das richtige Zertifikat, das für die Verwendung in der WebAuth-Parameterzuordnung ausgewählt wurde, und dass der virtuelle IPv4-Hostname mit dem Common Name (CN) im Zertifikat übereinstimmt.

Über die GUI:

1. Gehen Sie zu Configuration > Security > Web Auth.
2. Wählen Sie die verwendete Parameterzuordnung aus der Liste aus.
3. Überprüfen Sie, ob der Vertrauenspunkt und der virtuelle IPv4-Hostname richtig sind.



Überprüfen des Trustpoint- und Virtual IPv4-Hostnamens

Über die CLI:

```
<#root>
```

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

```
<type> <name>
```

```
parameter-map type
```

```
<type> <name>
```

```
[...]
```

```
virtual-ip ipv4
```

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

```
trustpoint
```

```
<trustpoint>
```

Zugehörige Informationen

- [Lokale Webauthentifizierung konfigurieren](#)

- [Webbasierte Authentifizierung \(EWC\)](#)
- [Anpassen des Web Authentication-Portals auf dem Catalyst 9800 WLC](#)
- [Erstellen und Herunterladen von CSR-Zertifikaten auf Catalyst 9800 WLCs](#)
- [Konfigurieren virtueller Schnittstellen](#)

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.