Risoluzione dei problemi comuni con LWA sui WLC 9800

Sommario

Introduzione

In questo documento vengono descritti i problemi comuni dei client che si connettono a una WLAN con Autenticazione Web locale (LWA).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza base di:

- Cisco Wireless LAN Controller (WLC) serie 9800.
- Informazioni generali sull'autenticazione Web locale (LWA) e la relativa configurazione.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

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

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

LWA è un tipo di autenticazione WLAN che può essere configurato sul WLC in cui il client finale che tenta di connettersi, dopo aver selezionato la WLAN dall'elenco, presenta un portale all'utente. In questo portale, l'utente può immettere un nome utente e una password (a seconda della configurazione selezionata) per completare la connessione alla WLAN.

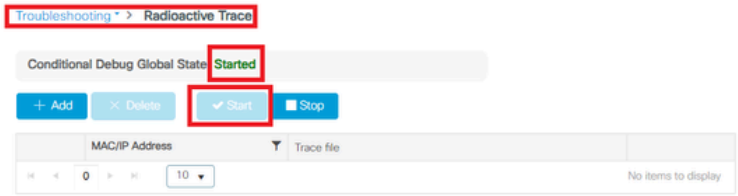
Per ulteriori informazioni su come configurare LWA sul WLC 9800, consultare la guida alla configurazione dell'autenticazione Web locale.

Tracce radioattive (RA) sul WLC 9800

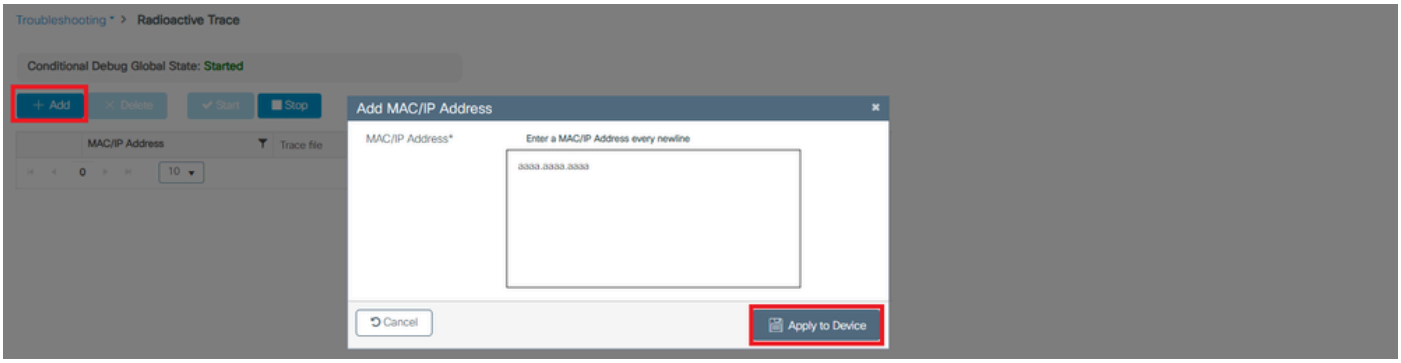
Le tracce radioattive sono un ottimo strumento di risoluzione dei problemi che può essere utilizzato per risolvere vari problemi relativi al WLC e alla connettività del client. Per raccogliere le tracce RA, eseguire le operazioni riportate di seguito.

Dall'interfaccia grafica:

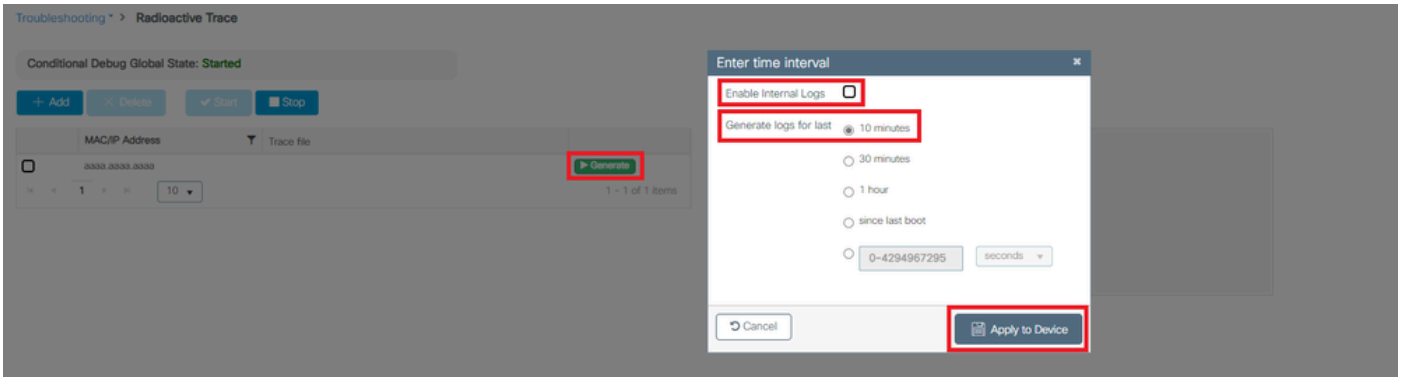
1. Selezionare Risoluzione dei problemi > Traccia radioattiva.
2. Fare clic su Start per abilitare lo stato globale di debug condizionale.
3. Fare clic su + Aggiungi. Viene aperta una finestra popup. Immettere l'indirizzo MAC del client. Qualsiasi formato di indirizzo MAC è accettato (aabb.ccdd.eeff, AABB.CCDD.EEEE, a:bb:cc:dd:ee:ff, o AA:BB:CC:DD:EE:FF). Quindi fare clic su Apply to Device (Applica al dispositivo).
4. Chiedere al client di riprodurre il problema 3 o 4 volte.
5. Una volta riprodotto il problema, fare clic su Generate.
6. Viene aperta una nuova finestra popup. Generare i registri per gli ultimi 10 minuti. (in questo caso non è necessario attivare i registri interni). Fare clic su Apply to Device (Applica alla periferica) e attendere l'elaborazione del file.
7. Una volta generato il file, fare clic sull'icona Download.



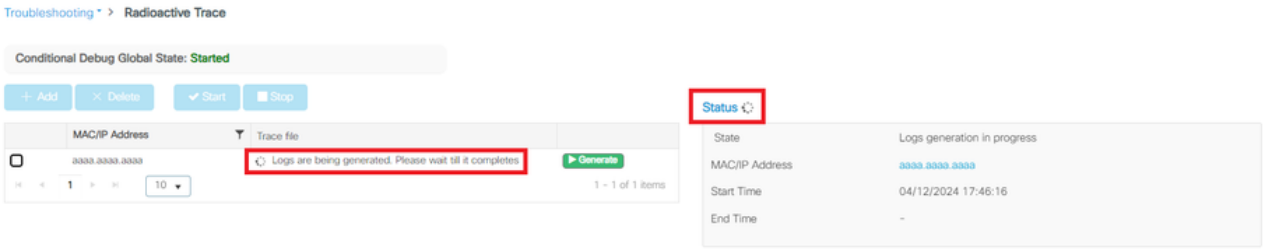
Abilita debug condizionale



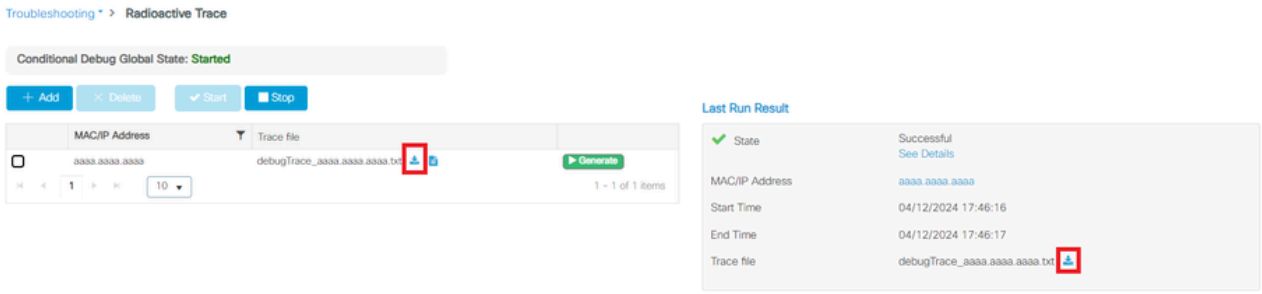
Aggiungi un indirizzo MAC client



Genera log per gli ultimi 10 minuti



Attendere la



generazioneScaricare il file

Dalla CLI:

<#root>

```
WLC# debug wireless mac
```

<mac-address>

```
 monitor-time 600
```

Viene generato un nuovo file in bootflash denominato 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

Copiare il file in un server esterno per l'analisi

<#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
```

Per ulteriori informazioni su Radioactive Tracing, fare riferimento a questo collegamento.

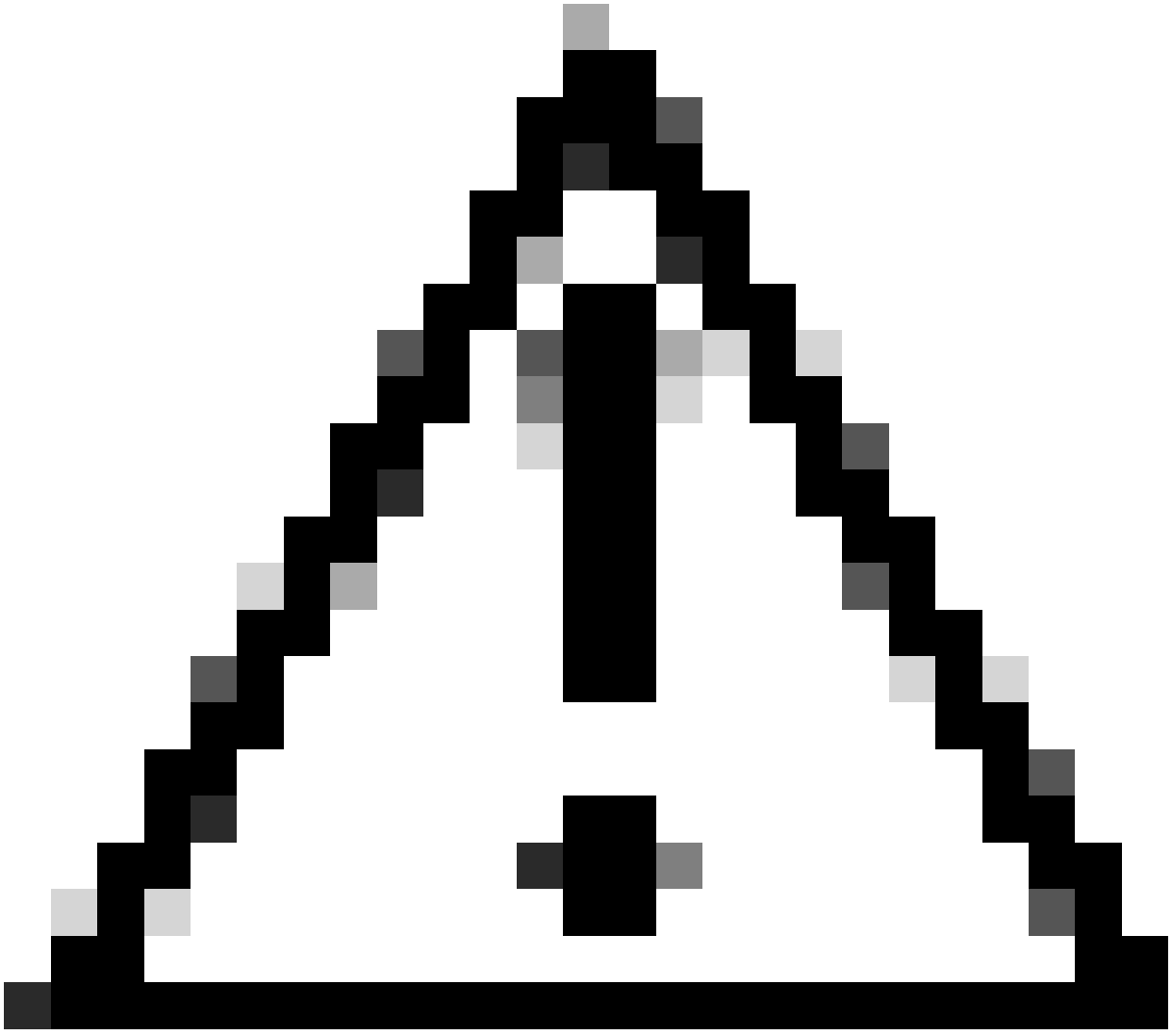
Flusso previsto

Consultare le informazioni per comprendere lo scenario di lavoro per LWA.

Fasi del client dal punto di vista del client

1. Il client finale viene associato alla WLAN.
2. Al client viene assegnato un indirizzo IP.
3. Il portale viene presentato al client finale.
4. Il client finale immette le credenziali di accesso.
5. Client finale autenticato.
6. Il client finale è in grado di esplorare Internet.

Fasi del client nella prospettiva WLC



Attenzione: molti log della traccia di Radio Active (RA) sono stati esclusi per motivi di semplicità.

Associazioni del client finale alla 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

Autenticazione 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

Il client riceve un indirizzo IP assegnato

<#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

Autenticazione 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
```

Il client ottiene un indirizzo 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

Elaborazione portale

<#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

Il WLC elabora le informazioni da applicare al client finale di connessione

<#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: applica il profilo utente al client finale connesso

<#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'

Autenticazione Web completata

<#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

Attributi AAA applicati al client finale

<#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

"]

Il client finale raggiunge lo stato di esecuzione

<#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

Scenari comuni di risoluzione dei problemi

Errori di autenticazione

Considerazioni

- Il portale visualizzato riporta "Autenticazione non riuscita" dopo l'immissione delle credenziali corrette.
- WLC visualizza Client in stato "Web Auth Pending" (Autenticazione Web in sospeso).
- La pagina iniziale viene visualizzata di nuovo.

Tracce RA WLC

<#root>

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

Param-map used: lwa-parameter_map

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

AUTHC_FAIL [INVALID CREDENTIALS]

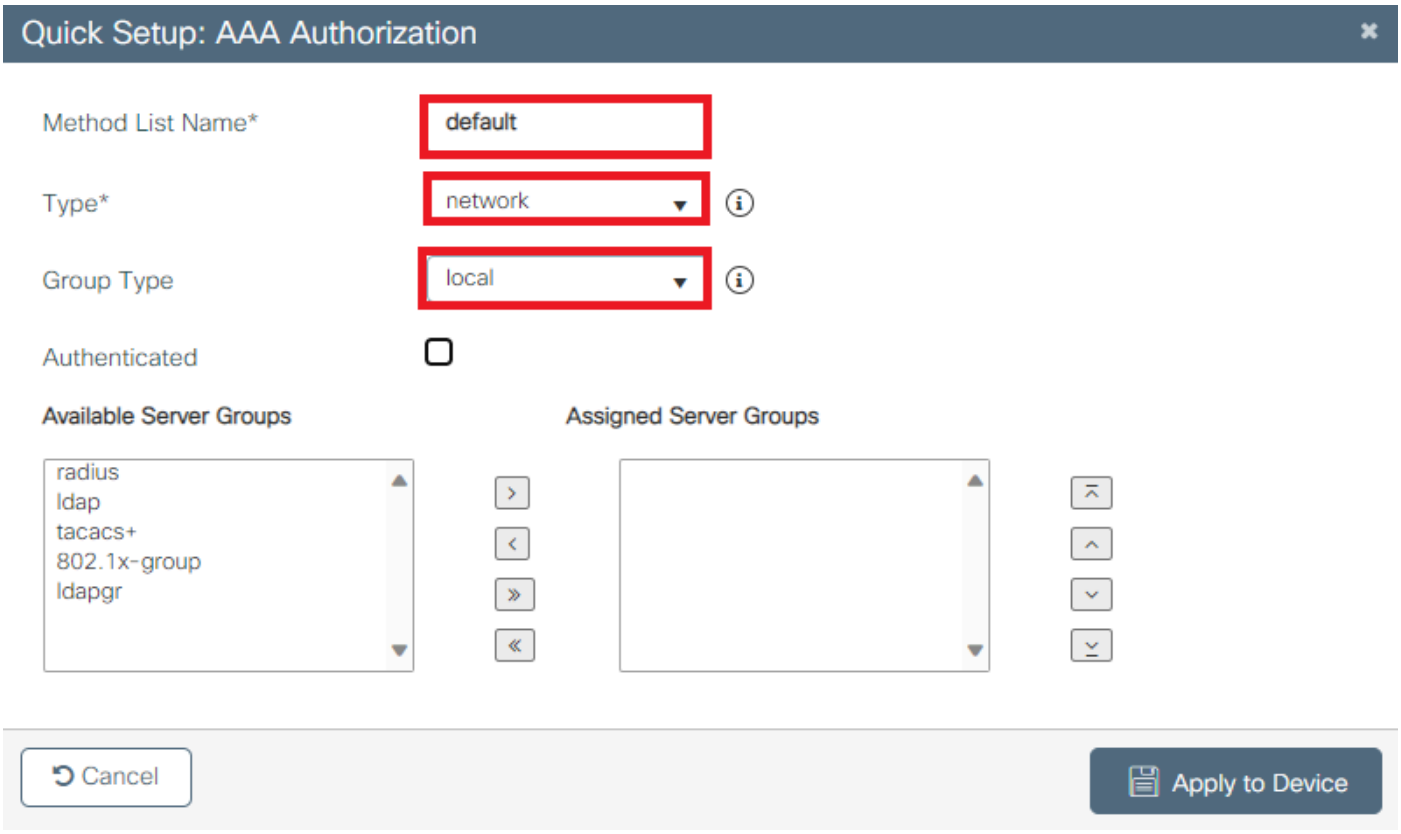
```
[aaaa.bbbb.cccc:capwap_90400002] Authc failure from WebAuth, Auth event fail
[aaaa.bbbb.cccc:capwap_90400002] (Re)try failed method WebAuth - aaaa.bbbb.cccc
[aaaa.bbbb.cccc:capwap_90400002] Method webauth changing state from 'Running' to 'Authc Failed'
```

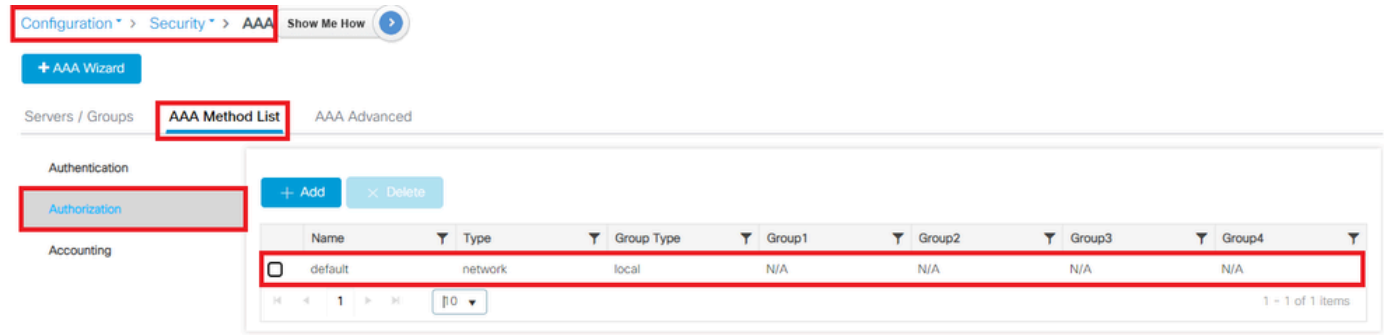
Soluzioni consigliate

Verificare che l'elenco dei metodi AAA predefinito per l'autorizzazione di rete sia presente nella configurazione WLC.

Dall'interfaccia grafica:

1. Selezionare Configurazione > Sicurezza > AAA > Elenco metodi AAA > Autorizzazione. Fare clic su + Aggiungi.
2. Configura come:
    1. Nome elenco metodi: predefinito
    2. Tipo: rete
    3. Tipo di gruppo: locale
3. Fare clic su Applica a dispositivo.





Dalla CLI:

<#root>

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

Il portale non viene visualizzato all'utente ma il client risulta connesso

Comportamento possibile riscontrato dal client finale

- Il client finale vede il proprio dispositivo come "Connesso".
- Il client finale non visualizza il portale.

- Il client finale non immette credenziali.
- Al client finale è assegnato un indirizzo IP.
- Il WLC mostra il client in stato "Run" (Esegui).

Tracce RA WLC

Al client viene assegnato un indirizzo IP che viene immediatamente spostato sullo stato "Run" sul WLC. Gli attributi utente mostrano solo la VLAN assegnata al client finale.

<#root>

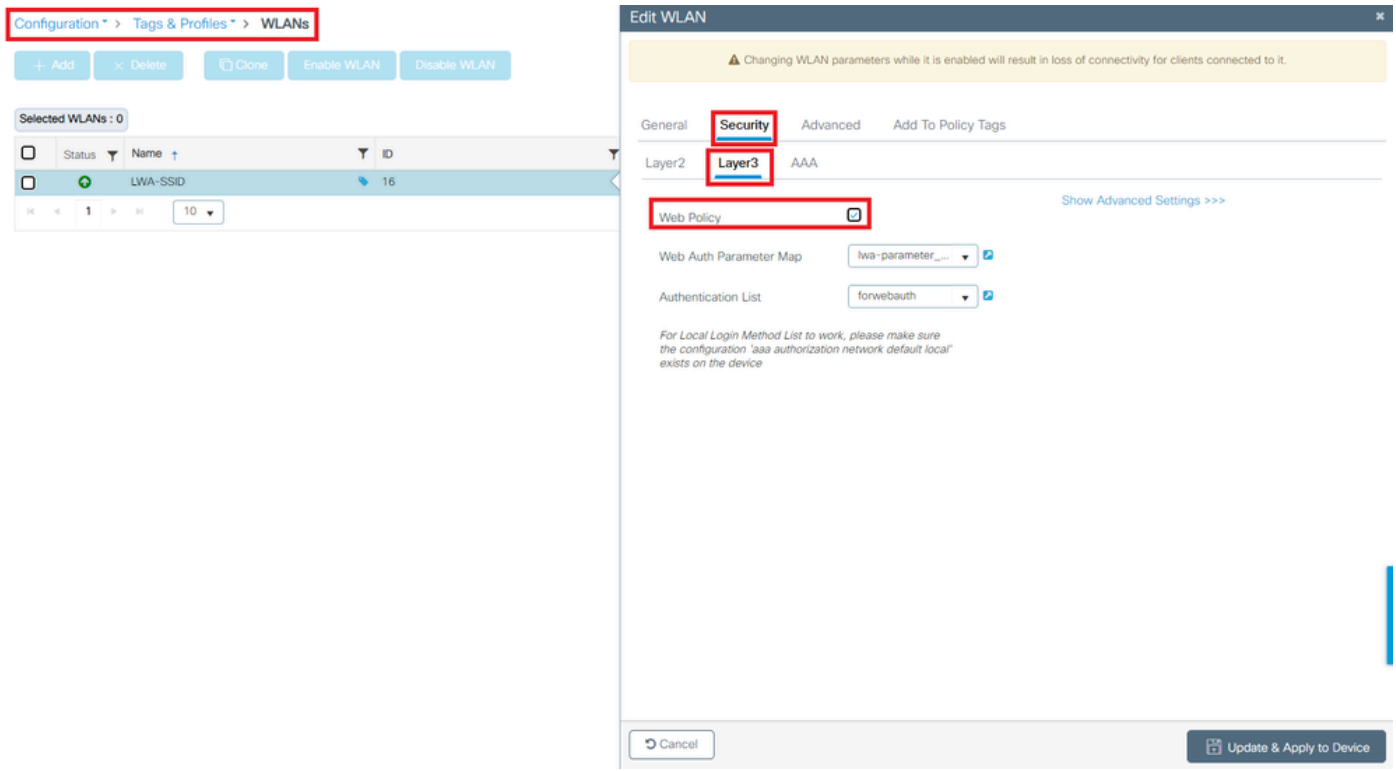
```
MAC: aaaa.bbbb.cccc

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
```

Soluzioni consigliate

Verificare che il criterio Web sia abilitato sulla WLAN.

Dall'interfaccia grafica:

1. Selezionare Configurazione > Tag e profili > WLAN.
2. Selezionare le WLAN LWA.
3. Selezionare Sicurezza > Layer 3.
4. Verificare che la casella di controllo Criteri Web sia attivata.



È necessario abilitare i criteri Web

Dalla CLI:

<#root>

```
WLC# configure terminal
```

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

<wlan>

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

Il portale non è visibile all'utente e il client non si connette

Comportamento possibile riscontrato dal client finale

- Il client finale rileva che il dispositivo sta tentando continuamente di connettersi.
- Il client finale non visualizza il portale.
- Al client finale non è assegnato un indirizzo IP.
- WLC visualizza il client nello stato "Webauth in sospeso".

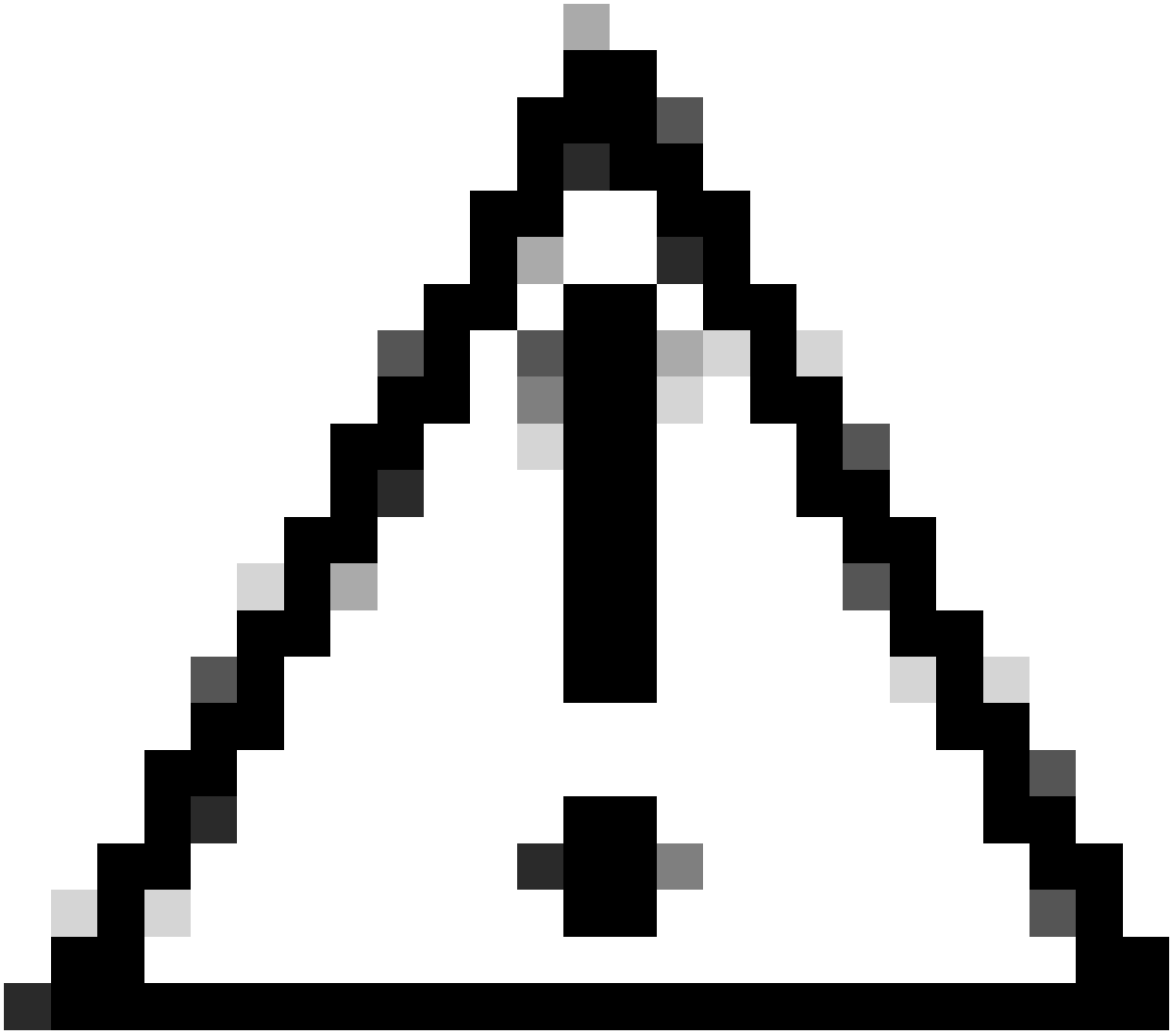
Soluzioni consigliate

Abilitare i server HTTP/HTTPS necessari. È ora possibile avere un maggiore controllo su quali

server HTTP/HTTPS devono essere abilitati per adattarsi completamente alle esigenze della rete. Fare riferimento a questo collegamento per ulteriori informazioni sulla configurazione delle richieste HTTP e HTTPS per l'autenticazione Web poiché sono supportate diverse combinazioni HTTP; ad esempio, è possibile utilizzare HTTP solo per webadmin e HTTP per webauth.

Per consentire la gestione amministrativa dei dispositivi e l'autenticazione Web con accesso sia HTTP che HTTPS, dalla CLI:

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



Attenzione: se entrambi i server sono disabilitati, non sarà possibile accedere all'interfaccia grafica dell'utente (GUI) del WLC.

I client finali non ricevono un indirizzo IP

Comportamento possibile riscontrato dal client finale

- I client finali rilevano che il dispositivo sta tentando continuamente di ottenere un indirizzo IP.
- Il WLC mostra il client in stato "IP Learning".

Tracce RA WLC

Richieste di individuazione senza offerta inviata.

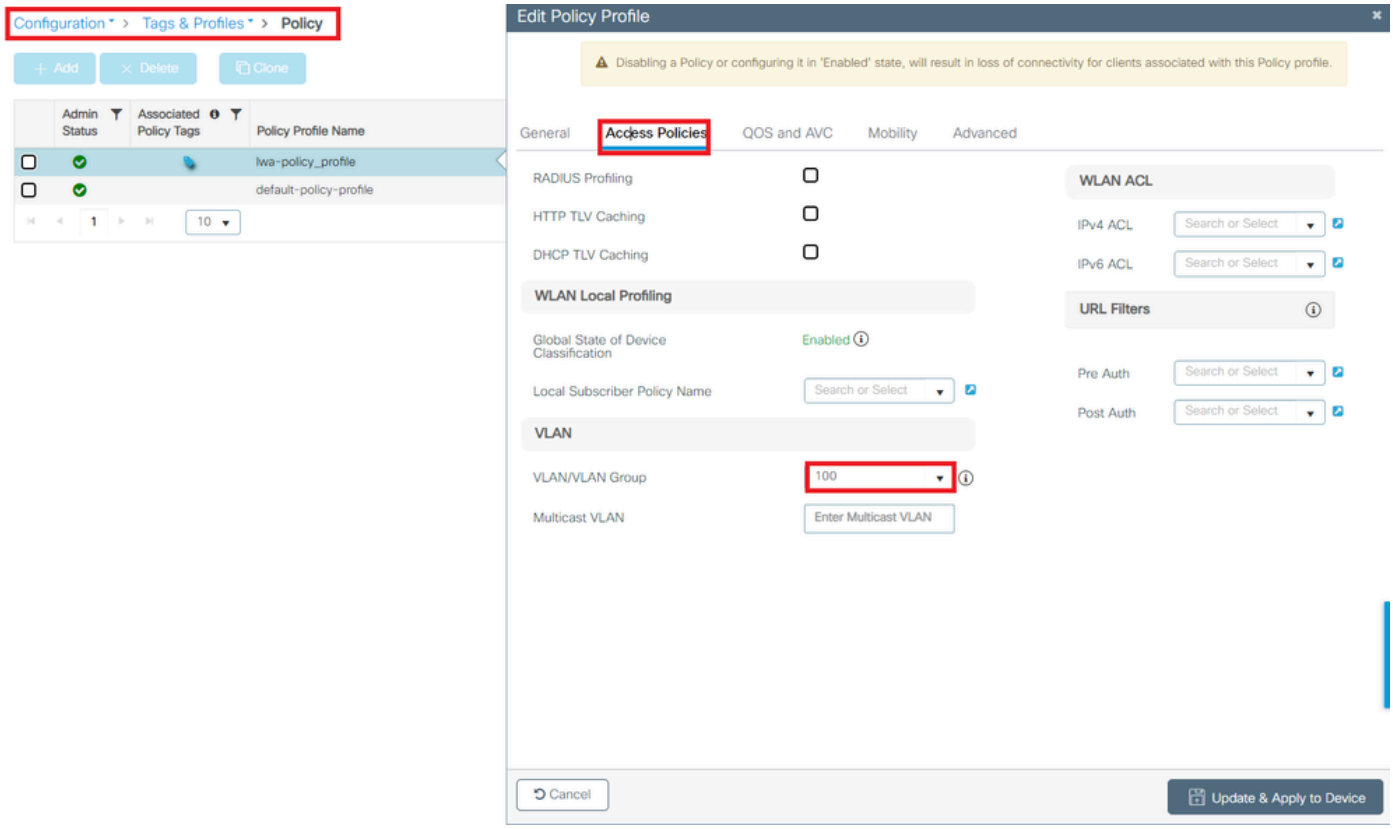
```
RX: DHCPv4 from interface capwap_90400002 on vlan 100 Src MAC: aaaa.bbbb.cccc Dst MAC: ffff.ffff.ffff s
TX: DHCPv4 from interface capwap_90400002 on vlan 100 Src MAC: aaaa.bbbb.cccc Dst MAC: ffff.ffff.ffff s
```

Soluzioni consigliate

Primo: verificare che al profilo della policy sia stata assegnata la VLAN corretta.

Dall'interfaccia grafica:

1. Selezionare Configurazione > Tag e profili > Criterio.
2. Selezionare il profilo criteri utilizzato.
3. Andare a Criteri di accesso.
4. Selezionare la VLAN corretta.



Dalla 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>

Secondo: verificare che sia disponibile un pool DHCP per l'utente. verificarne la configurazione e la raggiungibilità. Le tracce RSA mostrano il percorso del processo DORA DHCP VLAN. Verificare che la VLAN sia la VLAN corretta.

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

Il portale personalizzato non è visibile al client finale

Comportamento possibile riscontrato dal client finale

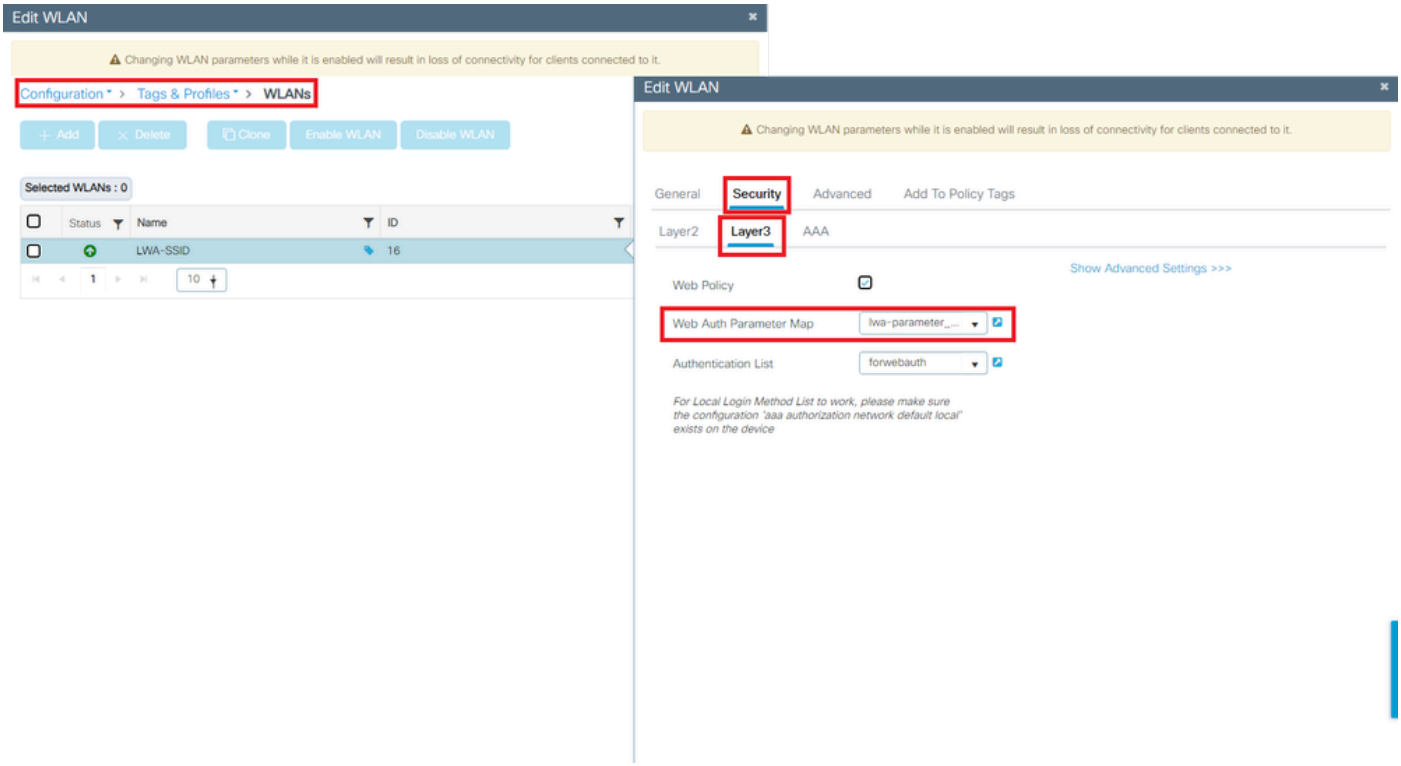
- Viene visualizzato il portale predefinito del WLC.

Soluzioni consigliate

In primo luogo: verificare che la WLAN utilizzi la mappa dei parametri di autenticazione Web personalizzata.

Dall'interfaccia grafica:

1. Selezionare Configurazione > Tag e profili > WLAN.
2. Selezionare la WLAN dall'elenco.
3. Selezionare Sicurezza > Layer 3.
4. Selezionare la mappa dei parametri di autenticazione Web personalizzata.



Mappa parametri personalizzata selezionata

Dalla 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>

Secondo: è importante notare che il download personalizzato dal portale Web Cisco.com non funziona con un'interfaccia di programmazione molto robusta e complicata. In genere, si consiglia di apportare modifiche solo a un livello CSS e magari aggiungere o rimuovere immagini. Applet, PHP, variabili di modifica, React.js e così via non sono supportati. Se un portale personalizzato non viene visualizzato al client, provare a utilizzare le pagine WLC predefinite e verificare se il problema può essere replicato. Se il portale viene visualizzato correttamente, è presente un elemento non supportato nelle pagine personalizzate che si prevede di utilizzare.

Terzo: se si utilizza un EWC (Embedded Wireless Controller), si consiglia di utilizzare la CLI per aggiungere le pagine personalizzate in modo da assicurare che vengano visualizzate correttamente:

<#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
```

Il portale personalizzato non viene visualizzato correttamente sul client finale

Comportamento possibile riscontrato dal client finale

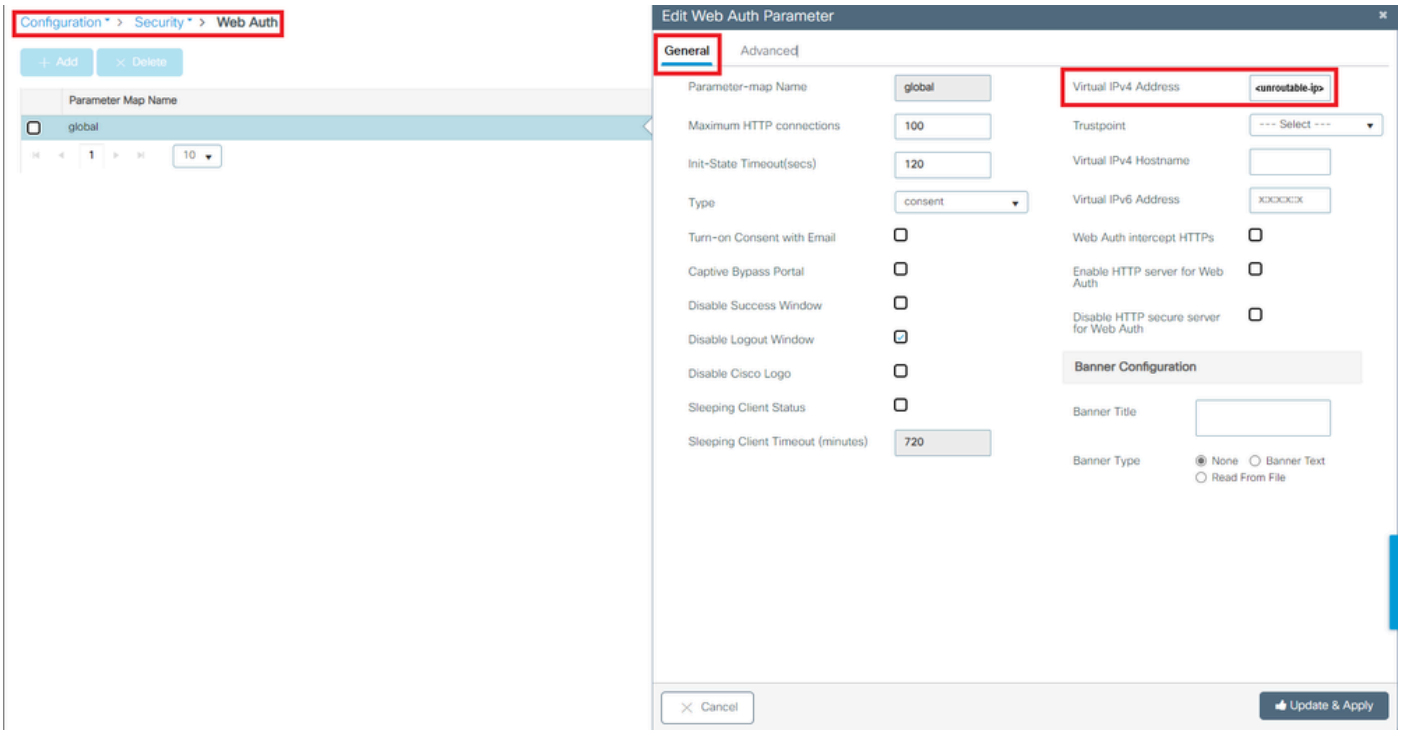
- Il rendering del portale personalizzato non viene eseguito correttamente, ovvero le immagini non vengono visualizzate.

Soluzioni consigliate

Verificare che alla mappa dei parametri globali sia assegnato un indirizzo IP virtuale.

Dall'interfaccia grafica:

1. Selezionare Configurazione > Protezione > Autenticazione Web.
2. Selezionare la mappa dei parametri globali dall'elenco.
3. Aggiungere un indirizzo IP virtuale non instradabile.



Indirizzo IP virtuale nella mappa dei parametri globali impostato su un indirizzo IP non instradabile

Dalla CLI:

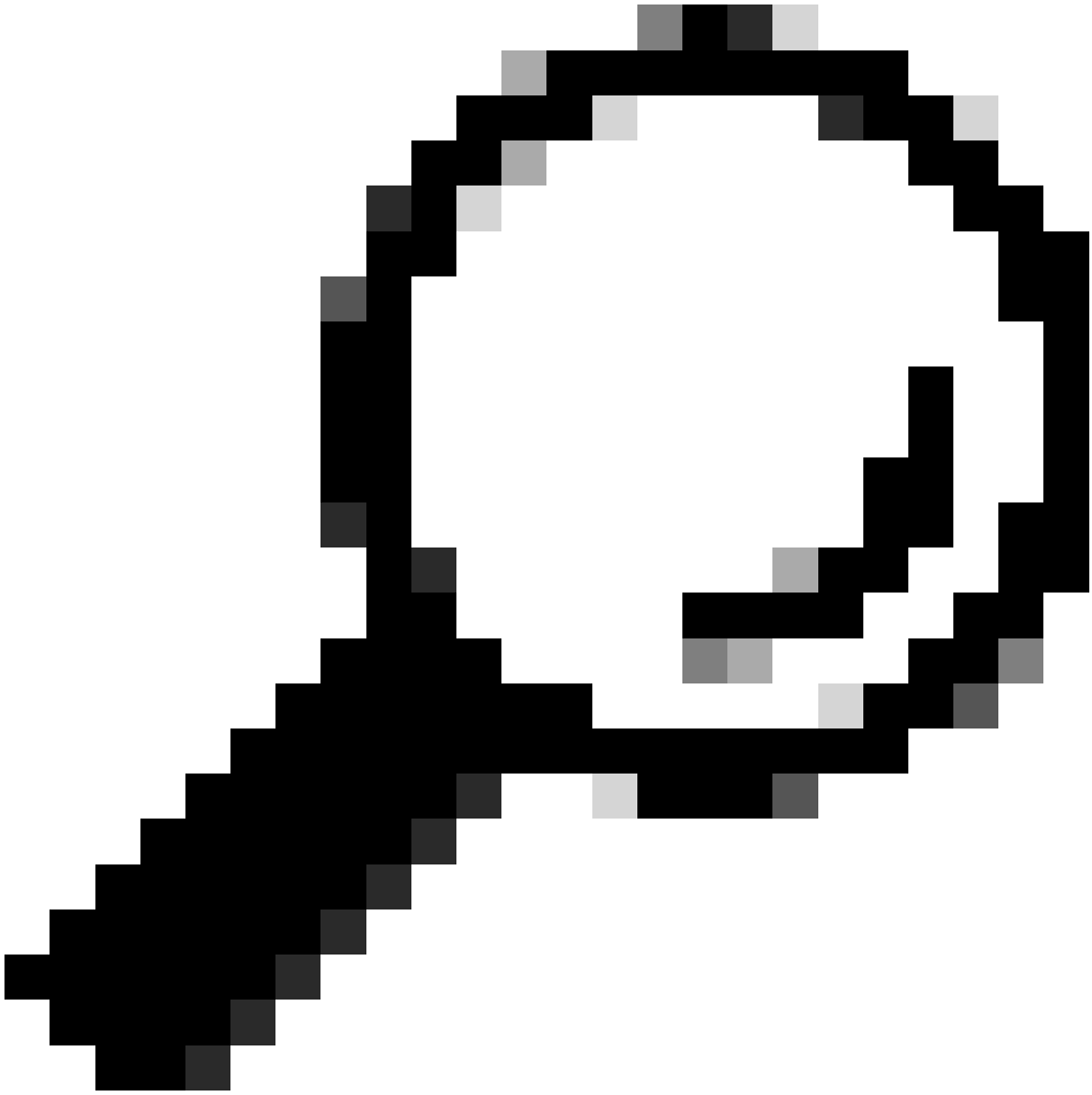
<#root>

```
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>



Suggerimento: l'indirizzo IP virtuale funge da indirizzo di reindirizzamento per la pagina di accesso per l'autenticazione Web. Nessun altro dispositivo nella rete deve avere lo stesso IP, non deve essere mappato a una porta fisica né esistere su alcuna tabella di routing. Pertanto, si consiglia di configurare l'IP virtuale come indirizzo IP non instradabile. È possibile utilizzare solo gli indirizzi presenti nella RFC5737.

Il portale afferma che "La connessione non è protetta/verifica firma non riuscita"

Comportamento possibile riscontrato dal client finale

- All'apertura del portale il client visualizza un errore che indica che la connessione non è protetta.
- Il portale deve utilizzare un certificato.

Cose da sapere

Se è previsto che il portale venga visualizzato in HTTPS, è necessario che utilizzi un certificato SSL (Secure Sockets Layer). Tale certificato deve essere rilasciato da un'Autorità di certificazione (CA) di terze parti per verificare che il dominio sia effettivamente reale; fornisce la fiducia ai client finali quando immettono le proprie credenziali e/o visualizzano il portale. Per caricare un certificato sul WLC, fare riferimento a questo documento.

Soluzioni consigliate

Primo: riavviare i servizi HTTP/HTTPS desiderati. È ora possibile avere un maggiore controllo su quali server HTTP/HTTPS devono essere abilitati per adattarsi completamente alle esigenze della rete. Fare riferimento a questo collegamento per ulteriori informazioni sulla configurazione delle richieste HTTP e HTTPS per l'autenticazione Web.

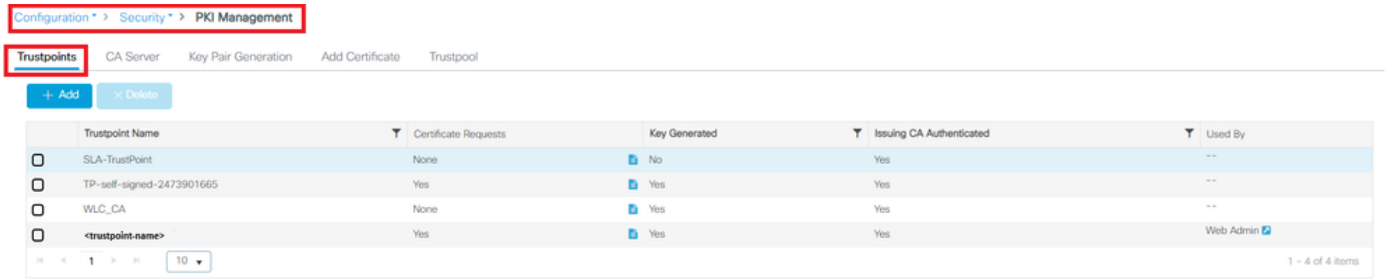
Dalla CLI:

```
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
```

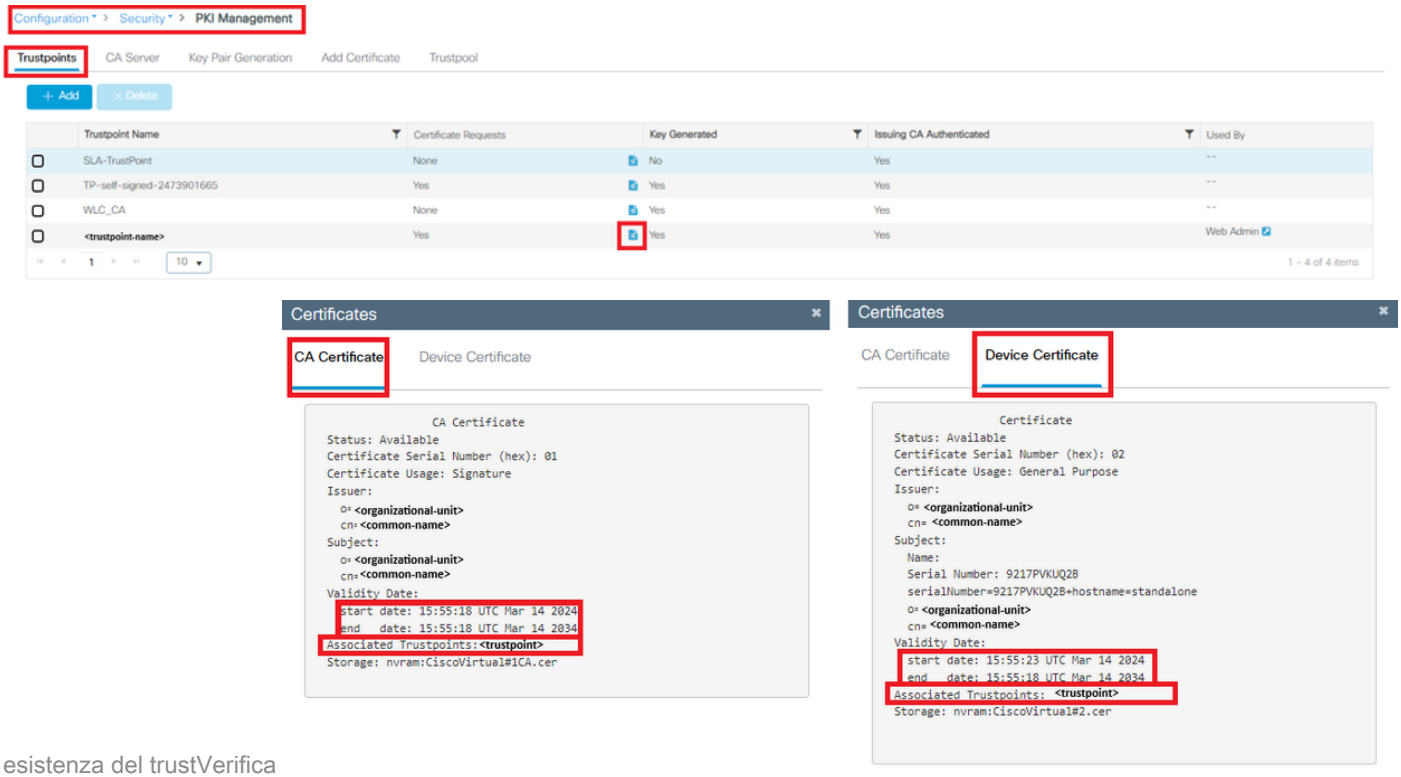
Secondo: verificare che il certificato sia caricato correttamente nel WLC e che la data di validità sia corretta.

Dall'interfaccia grafica:

1. Selezionare Configurazione > Sicurezza > Gestione PKI
2. Cercare il punto di trust nell'elenco
3. Controllarne i dettagli



Verifica l'



esistenza del trustVerifica
dettagliControlloValidità del trust

Dalla 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>

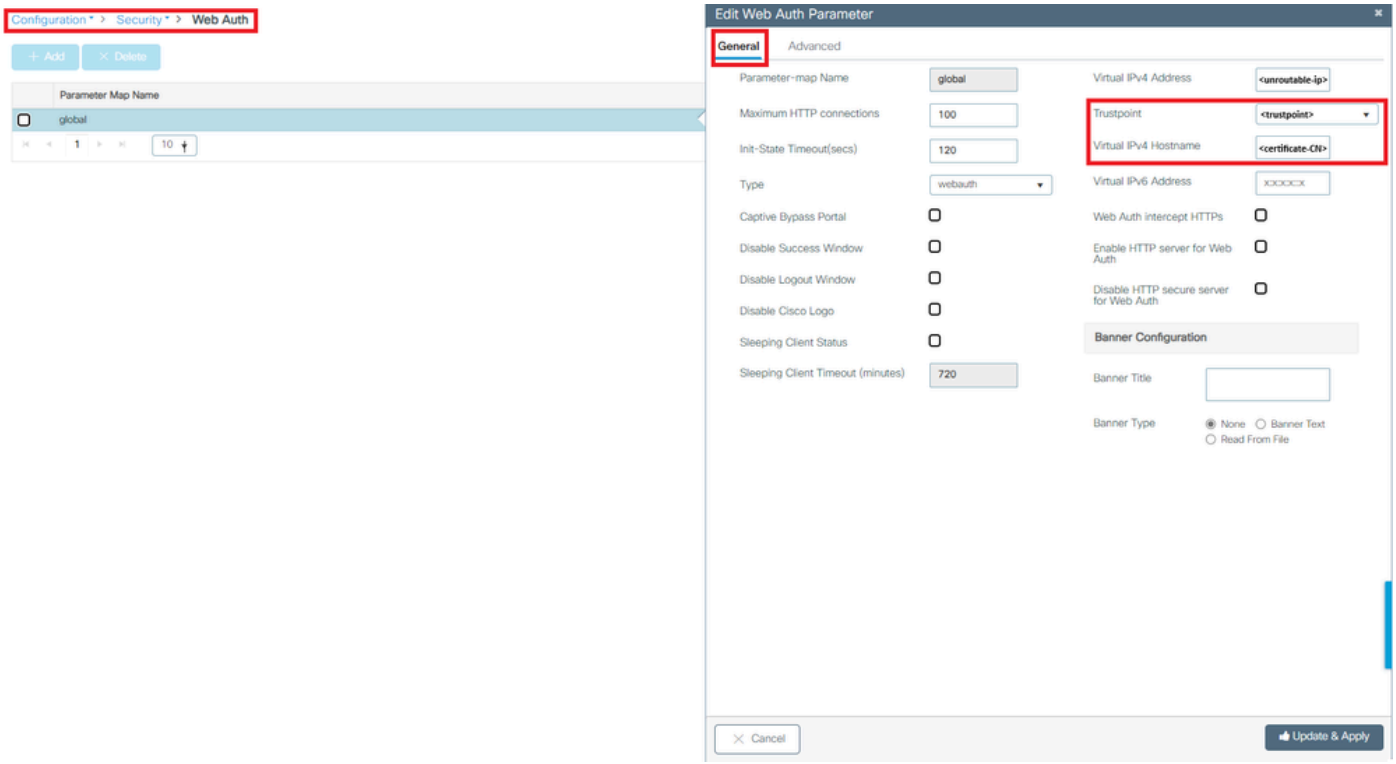
end date: <end-date>

Associated Trustpoints: <trustpoint>

Terzo: verificare che il certificato selezionato per l'utilizzo nella mappa dei parametri WebAuth sia corretto e che il nome host IPv4 virtuale corrisponda al nome comune (CN) nel certificato.

Dall'interfaccia grafica:

1. Selezionare Configurazione > Protezione > Autenticazione Web.
2. Selezionate la mappa dei parametri utilizzata dall'elenco.
3. Verificare che il trust point e il nome host IPv4 virtuale siano corretti.



Controllare il Trustpoint e il nome host IPv4 virtuale

Dalla 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>

Informazioni correlate

- Configura autenticazione Web locale
- Autenticazione basata sul Web (EWC)
- Personalizzazione del portale di autenticazione Web su Catalyst 9800 WLC
- Generazione e download dei certificati CSR sui WLC di Catalyst 9800
- Configurazione delle interfacce virtuali

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).