9800 WLCでのLWAに関する一般的な問題のトラブルシューティング

内容

はじめに

このドキュメントでは、ローカルWeb認証(LWA)を使用してWLANに接続するクライアントに関する一般的な問題について説明します。

前提条件

要件

次の項目に関する基本的な知識があることが推奨されます。

- Cisco Wireless LAN Controller(WLC)9800シリーズ
- ローカルWeb認証(LWA)とその設定に関する一般的な知識。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- 9800-CL WLC
- Ciscoアクセスポイント9120AXI
- 9800 WLC Cisco IOS® XEバージョン17.9.3

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

LWAは、接続を試みるエンドクライアントがリストからWLANを選択した後、ユーザにポータルを提供するWLCで設定できるWLAN認証のタイプです。このポータルでは、ユーザは（選択した設定に応じて）ユーザ名とパスワードを入力して、WLANへの接続を終了できます。

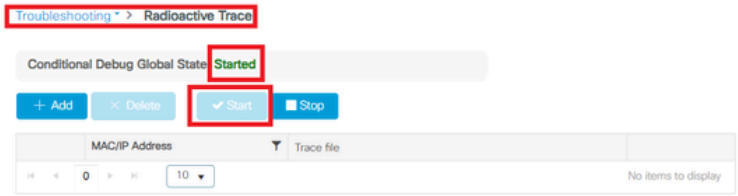
9800 WLCでLWAを設定する方法の詳細については、『ローカルWeb認証の設定』設定ガイドを参照してください。

9800 WLCでの放射性(RA)トレース

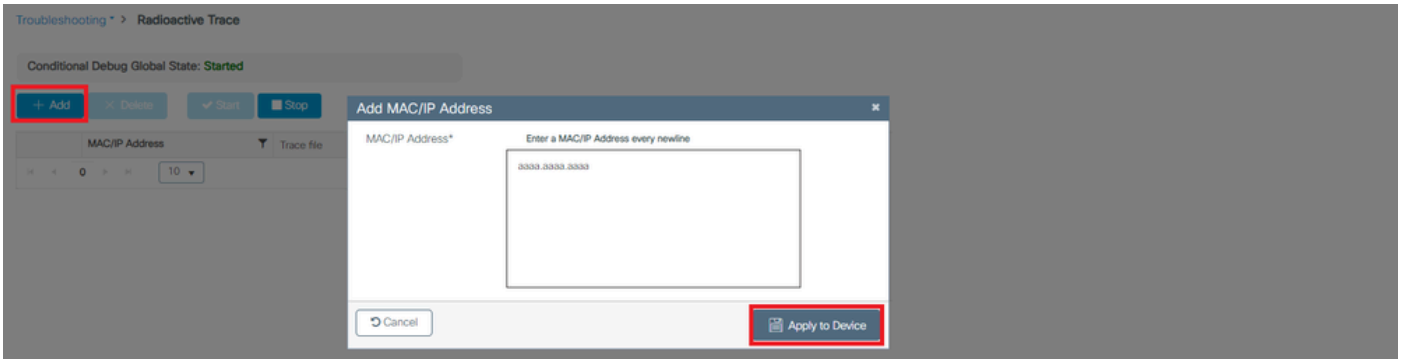
放射性トレースは、WLCおよびクライアント接続に関するさまざまな問題のトラブルシューティングを行う際に使用できる、優れたトラブルシューティングツールです。RAトレースを収集するには、次の手順を実行します。

GUI で次の手順を実行します。

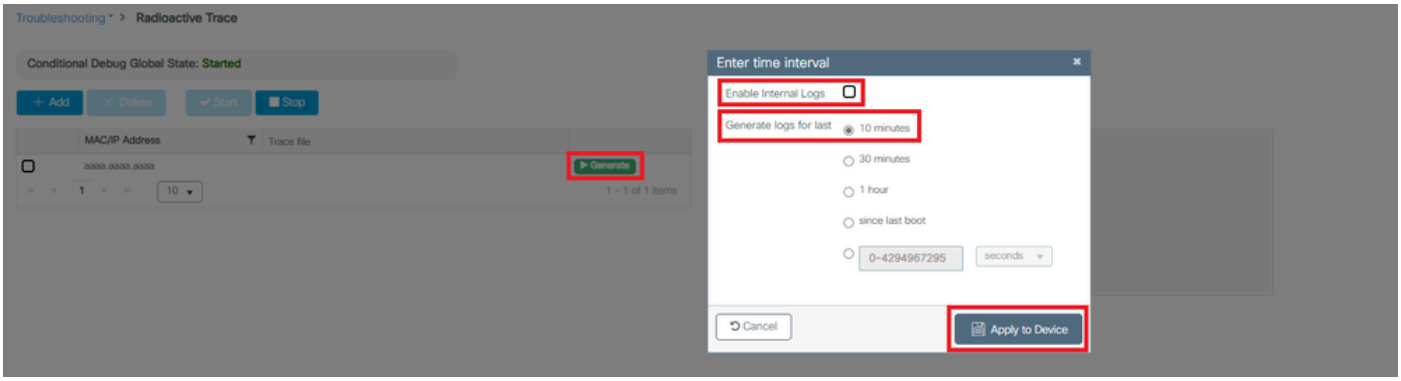
1. Troubleshooting > Radioactive Traceの順に進みます。
2. Startをクリックして、Conditional Debug Global Stateを有効にします。
3. +追加をクリックします。ポップアップウィンドウが開きます。クライアントのMACアドレスを入力します。任意のMACアドレス形式(aabb.ccdd.eeff、AABB.CCDD.EEEE、aa:bb:cc:dd:ee:ff、またはAA:BB:CC:DD:EE:FF)を使用できます。次に、Apply to Deviceをクリックします。
4. クライアントに問題を3回または4回再現させます。
5. 問題が再現されたら、Generateをクリックします。
6. 新しいポップアップウィンドウが開きます。過去10分間のログを生成します。（この場合、内部ログを有効にする必要はありません）。Apply to Deviceをクリックし、ファイルが処理されるまで待ちます。
7. ファイルが生成されたら、Downloadアイコンをクリックします。



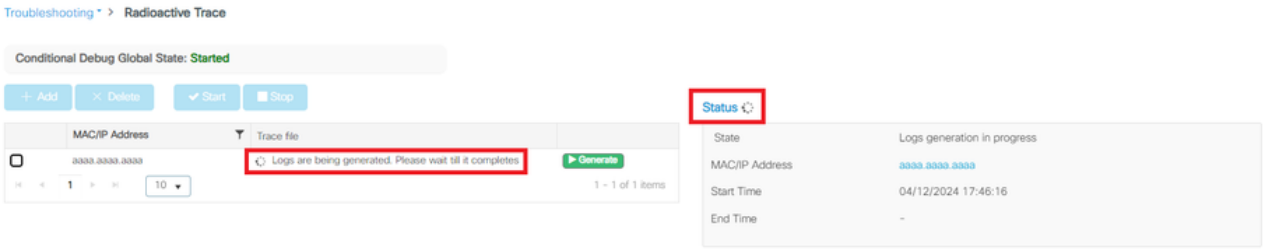
条件付きデバッグの有効化



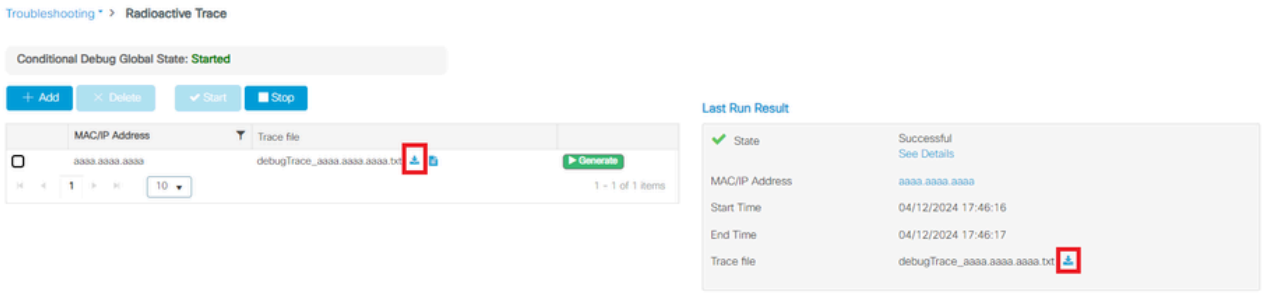
クライアントのMACアドレスを追加する



過去10分間のログの生成



ファイルが



生成されるのを待つファイルをダウンロードする

CLI から、

<#root>

```
WLC# debug wireless mac
```

<mac-address>

```
 monitor-time 600
```

ブートフラッシュにra_trace_MAC_<mac-address>_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.logという名前の新しいファイルが生成されます。

<#root>

```
WLC# more bootflash:
```

ra_trace_MAC_<mac-address>_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log

分析のためにファイルを外部サーバにコピーする

<#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
```

放射性トレースの詳細については、このリンクを参照してください。

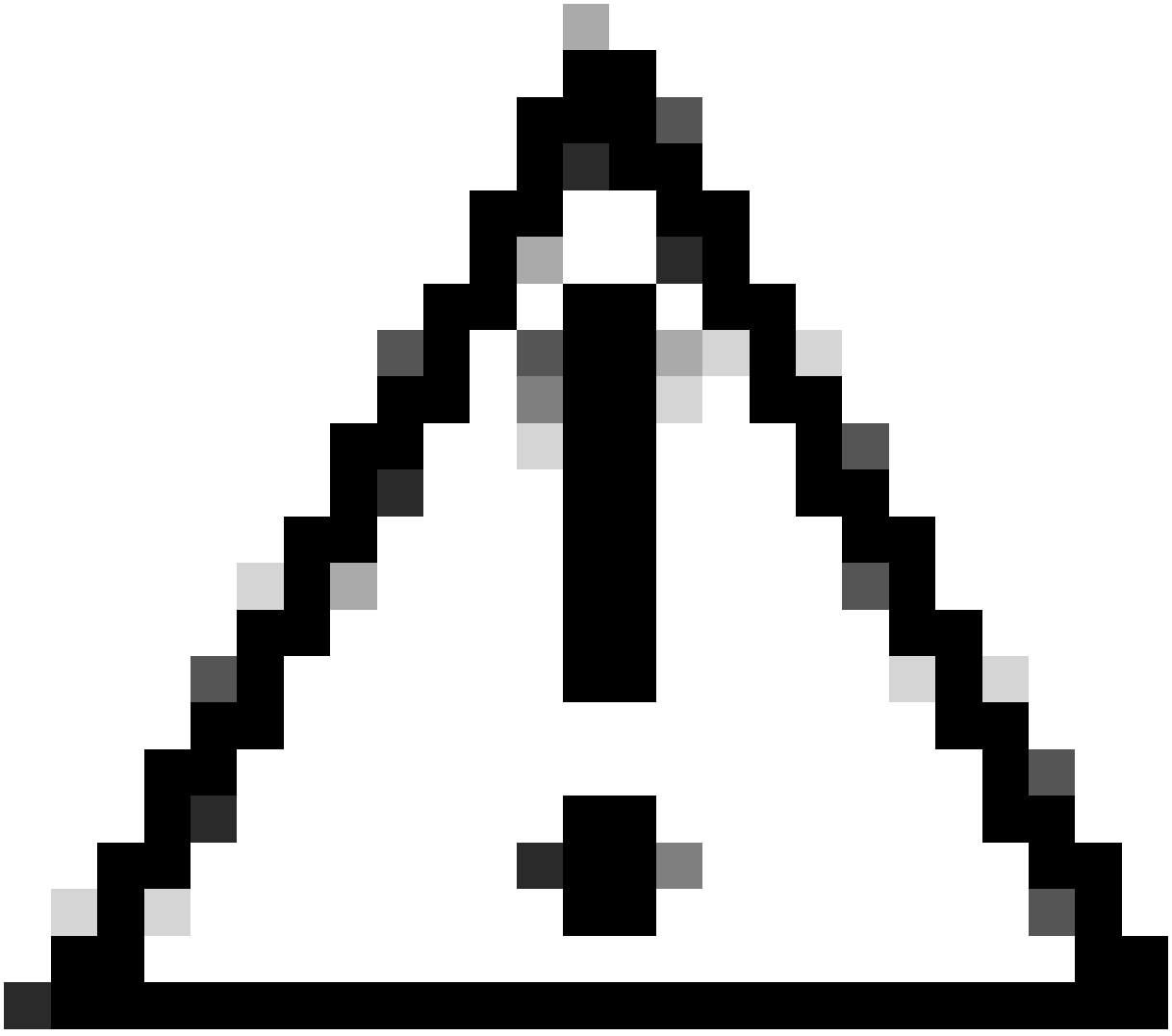
予想されるフロー

LWAの動作シナリオについては、この情報を参照してください。

クライアント側から見たクライアントのステージ

1. エンドクライアントがWLANに関連付けられます。
2. クライアントがIPアドレスを割り当てられる。
3. ポータルがエンドクライアントに表示されます。
4. エンドクライアントがログインクレデンシャルを入力します。
5. エンドクライアントが認証されます。
6. エンドクライアントがインターネットをブラウズできる。

WLCの観点からクライアントが受けるステージ



注意：わかりやすくするために、無線アクティブ(RA)トレースの多くのログが省略されています。

エンドクライアントがWLANに関連付けられている

<#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認証

<#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

クライアントがIPアドレスを割り当てられる

<#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認証

<#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
```

クライアントがIPアドレスを取得する

<#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

ポータル処理

<#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が接続エンドクライアントに適用される情報を処理する

<#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が接続されたエンドクライアントにユーザプロファイルを適用する

<#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認証が完了しました

<#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

エンドクライアントに適用される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

"]

エンドクライアントがRun状態になる

<#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

一般的なトラブルシューティングのシナリオ

Authentication failures

考慮事項

- 表示されているポータルで、正しいクレデンシャルを入力すると「Authentication Failed」と表示される。
- WLCに「Web Auth Pending」状態のクライアントが表示されています。
- 最初のスプラッシュページが再びユーザに表示されます。

WLC RAトレース

<#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]

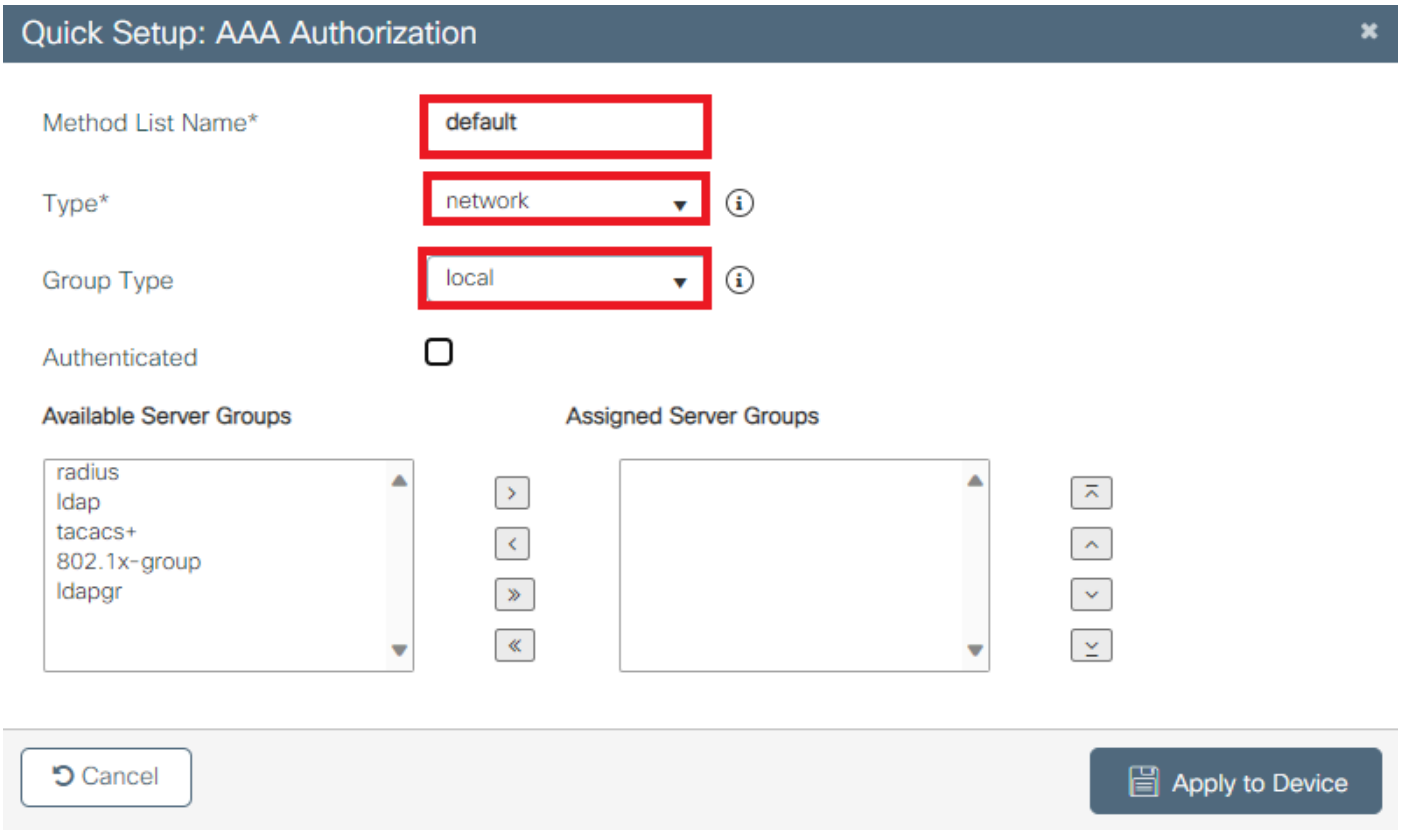
```
[aaaa.bbbb.cccc:capwap_90400002] Authc failure from WebAuth, Auth event fail
[aaaa.bbbb.cccc:capwap_90400002] (Re)try failed method WebAuth - aaaa.bbbb.cccc
[aaaa.bbbb.cccc:capwap_90400002] Method webauth changing state from 'Running' to 'Authc Failed'
```

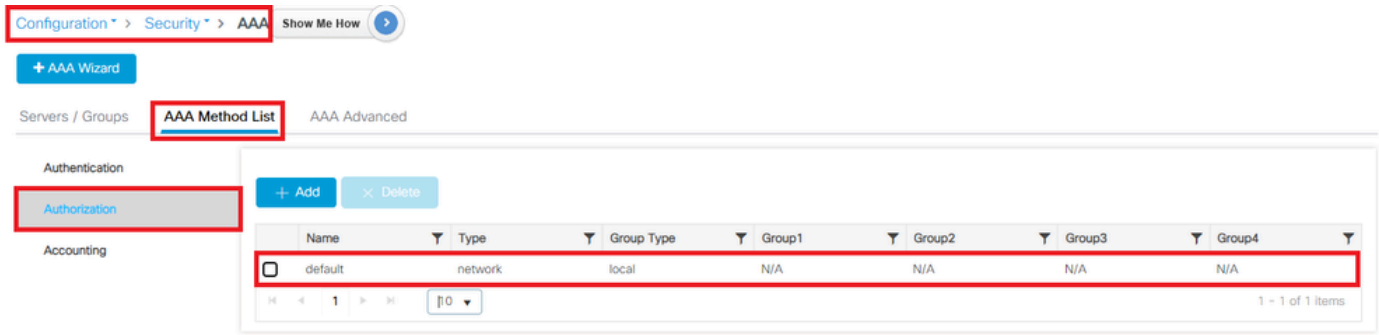
推奨ソリューション

ネットワーク認証用のデフォルトのAAA方式リストがWLC設定に存在することを確認します。

GUI で次の手順を実行します。

1. Configuration > Security > AAA > AAA Method List > Authorizationの順に選択します。 + Addをクリックします。
2. 次のように設定します。
    1. 方式リスト名：デフォルト
    2. タイプ：network
    3. グループタイプ：ローカル
3. Apply to Deviceをクリックします。





CLI から、

<#root>

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

ポータルはユーザには表示されないが、クライアントは接続されているように見える

エンドクライアントから発生する可能性のある動作

- エンドクライアントはデバイスを「接続済み」として認識します。

- エンドクライアントにポータルが表示されない。
- エンドクライアントはクレデンシャルを入力しません。
- エンドクライアントにIPアドレスが割り当てられている。
- WLCに「Run」状態のクライアントが表示されます。

WLC RAトレース

クライアントは割り当てられたIPアドレスを取得し、WLC上ですぐに「Run」状態に移行します。ユーザ属性は、エンドクライアントに割り当てられたVLANのみを表示します。

<#root>

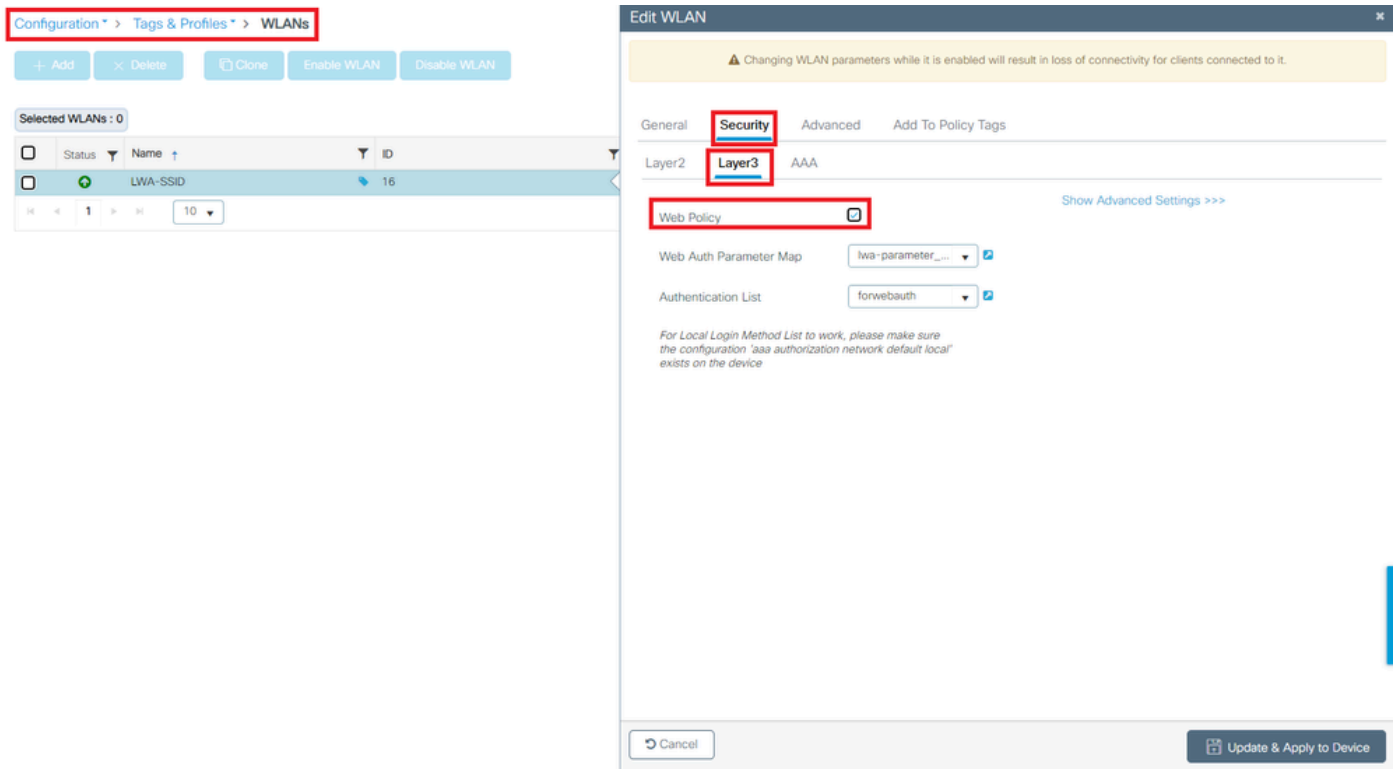
```
MAC: aaaa.bbbb.cccc

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
```

推奨ソリューション

WebポリシーがWLANで有効になっていることを確認します。

GUI で次の手順を実行します。

1. Configuration > Tags & Profiles > WLANsの順に選択します。
2. LWA WLANを選択します。
3. Security > Layer 3の順に選択します。
4. Web Policyチェックボックスが有効になっていることを確認します。



Webポリシーを有効にする必要がある

CLI から、

<#root>

```
WLC# configure terminal
```

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

<wlan>

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

ポータルがユーザに表示されず、クライアントが接続しない

エンドクライアントから発生する可能性のある動作

- エンドクライアントは、デバイスが絶えず接続を試みていることを認識します。

- エンドクライアントにポータルが表示されない。
- エンドクライアントにIPアドレスが割り当てられていない
- WLCに「Webauth Pending」状態のクライアントが表示されます。

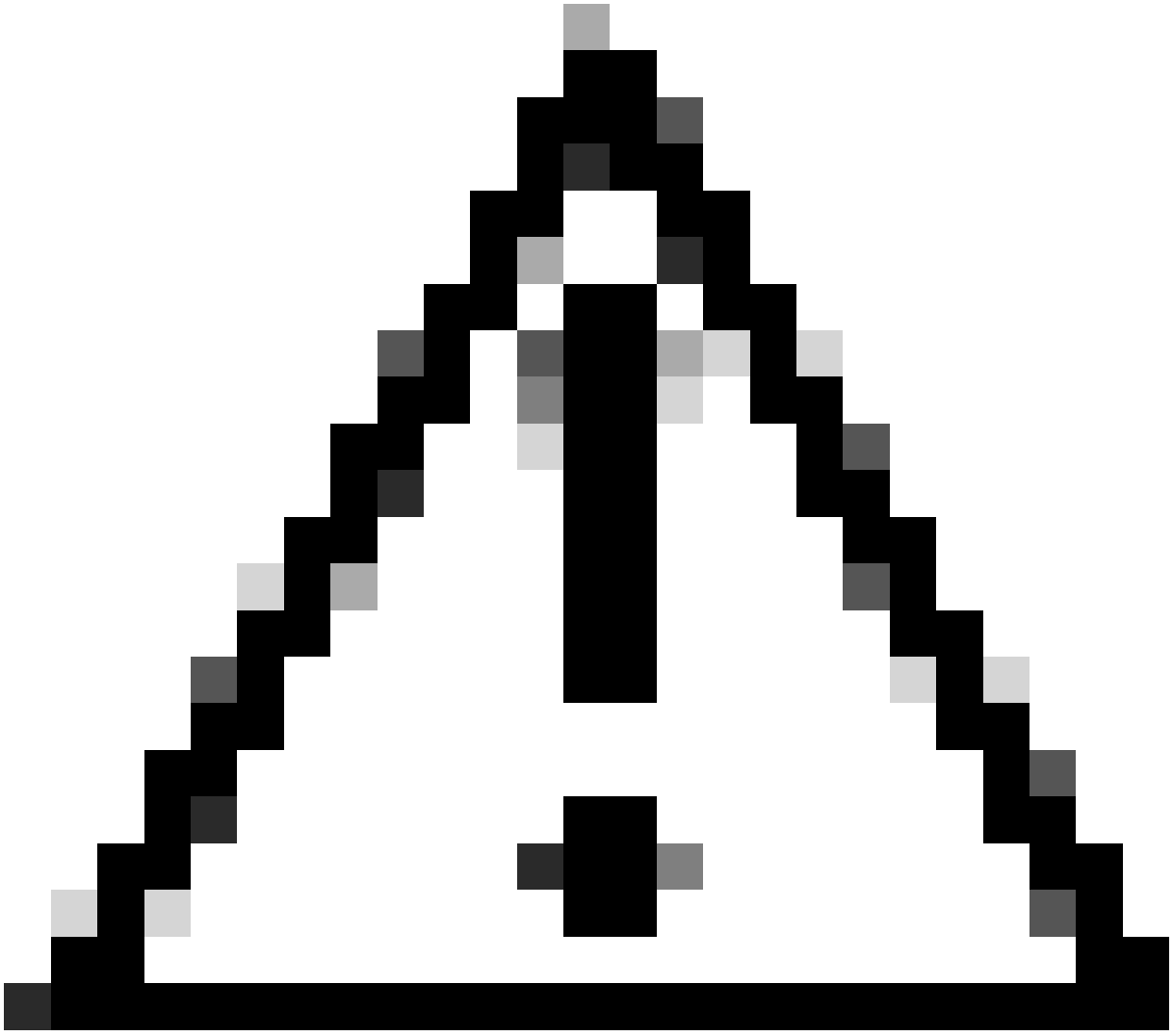
推奨ソリューション

必要なHTTP/HTTPSサーバを有効にします。ネットワークのニーズに完全に対応するために、ど

のHTTP/HTTPSサーバを有効にする必要があるのかをより細かく制御できるようになりました。HTTPの組み合わせがいくつかサポートされているため、Web認証のHTTPおよびHTTPS要求の設定の詳細については、このリンクを参照してください。たとえば、HTTPはwebadminにのみ使用でき、HTTPはwebauthに使用できます。

HTTPアクセスとHTTPSアクセスの両方で管理デバイス管理とWeb認証を許可するには、CLIから次の手順を実行します。

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



注意：これらのサーバの両方を無効にしても、WLCのグラフィカルユーザインターフェイス(GUI)にアクセスできません。

エンドクライアントがIPアドレスを取得していない

エンドクライアントから発生する可能性のある動作

- エンドクライアントは、デバイスがIPアドレスの取得を継続的に試みていることを認識します。
- WLCに「IPラーニング」状態のクライアントが表示されます。

WLC RAトレース

オファーなしのディスカバリ要求。

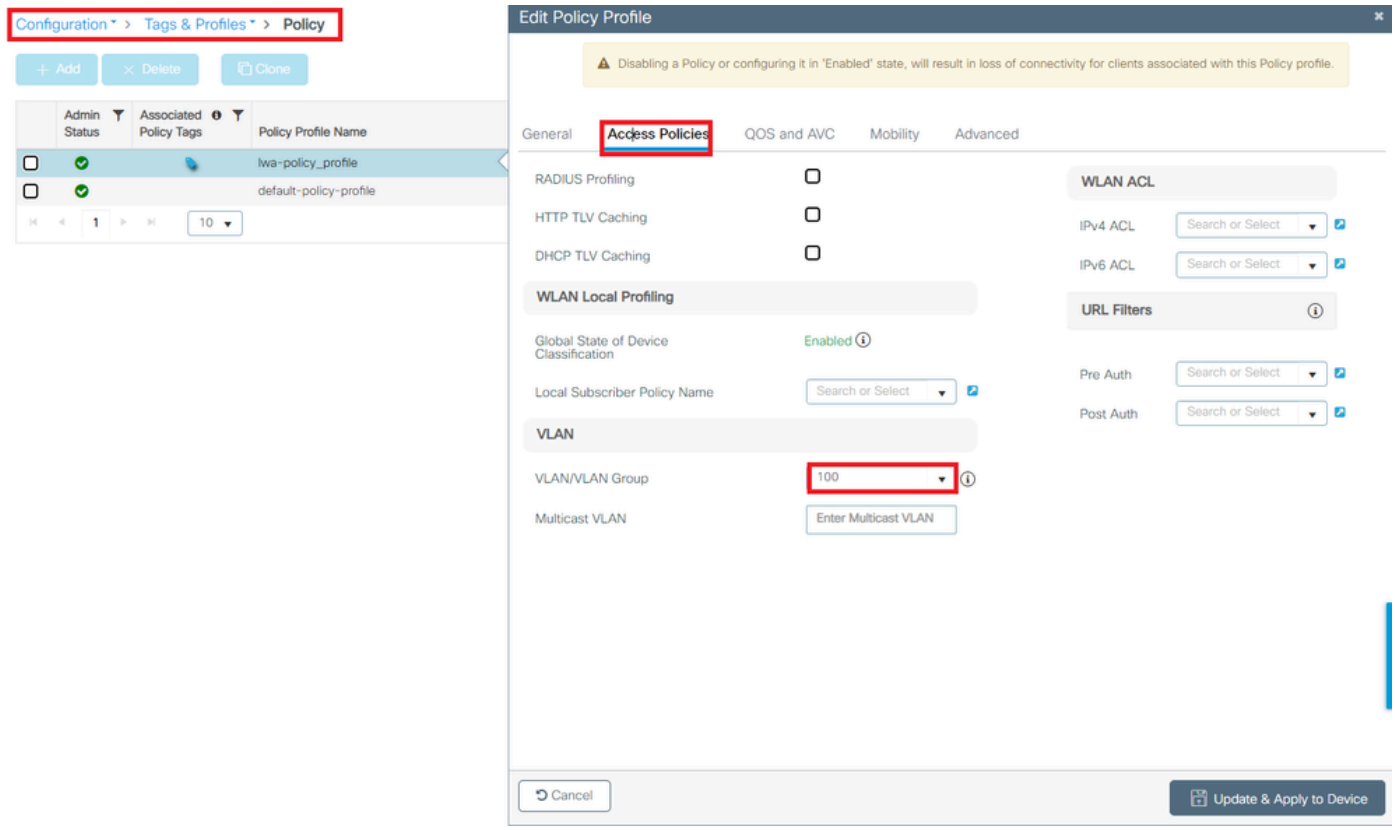
```
RX: DHCPv4 from interface capwap_90400002 on vlan 100 Src MAC: aaaa.bbbb.cccc Dst MAC: ffff.ffff.ffff s
TX: DHCPv4 from interface capwap_90400002 on vlan 100 Src MAC: aaaa.bbbb.cccc Dst MAC: ffff.ffff.ffff s
```

推奨ソリューション

最初：ポリシープロファイルに正しいVLANが割り当てられていることを確認します。

GUI で次の手順を実行します。

1. Configuration > Tags & Profiles > Policyの順に選択します。
2. 使用するポリシープロファイルを選択します。
3. Access Policiesに移動します。
4. 適切なVLANを選択します。



CLI から、

<#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>

2番目：ユーザが使用できるDHCPプールが存在することを確認します。その設定と到達可能性を確認します。RAトレースは、どのVLAN DHCP DORAプロセスが実行されているかを示します。このVLANが正しいVLANであることを確認します。

```
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,
```

カスタマイズされたポータルがエンドクライアントに表示されない

エンドクライアントから発生する可能性のある動作

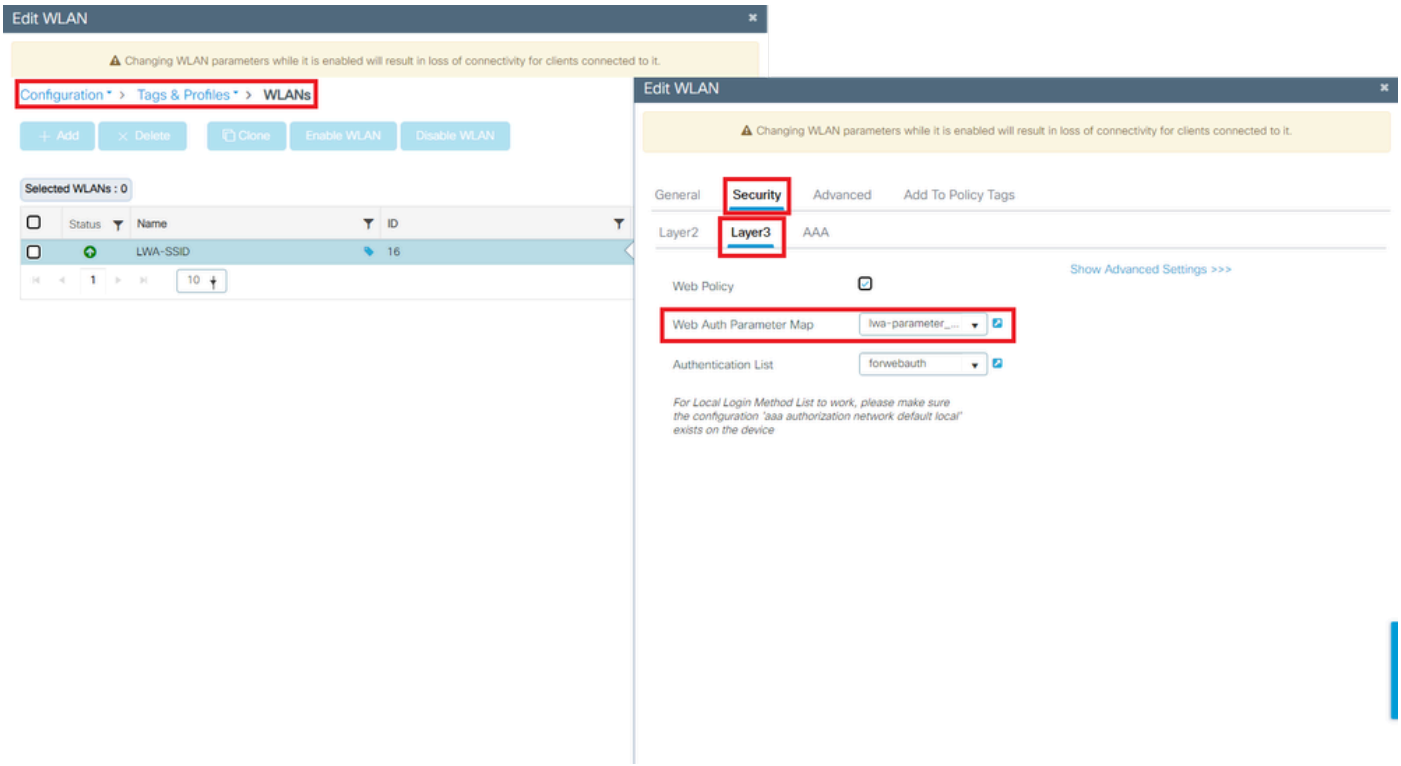
- WLCのデフォルトポータルが表示されます。

推奨ソリューション

最初：カスタマイズされたWeb認証パラメータマップをWLANが使用していることを確認します。

GUI で次の手順を実行します。

1. Configuration > Tags & Profiles > WLANsの順に選択します。
2. リストからWLANを選択します。
3. Security > Layer 3の順に選択します。
4. カスタマイズされたWeb認証パラメータマップを選択します。



カスタムパラメータマップが選択されました

CLI から、

<#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>

2つ目:Cisco.com Webポータルからダウンロードするカスタマイズされたダウンロードは、非常に堅牢で複雑なプログラミングインターフェイスでは動作しないことに注意してください。一般に、変更はCSSレベルだけを行い、イメージの追加や削除を行うことをお勧めします。アプレット、PHP、変数の変更、React.jsなどはサポートされていません。カスタマイズされたポータルがクライアントに表示されない場合は、デフォルトのWLCページを使用して、問題が再現されるかどうかを確認してください。ポータルが正常に表示された場合、使用することになっている力

スタマイズされたページでサポートされていないものがあります。

3:EWC(組み込みワイヤレスコントローラ)を使用する場合は、カスタマイズされたページが正しく表示されるように、CLIを使用してカスタマイズされたページを追加することをお勧めします。

<#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
```

カスタマイズされたポータルがエンドクライアントに正しく表示されない

エンドクライアントから発生する可能性のある動作

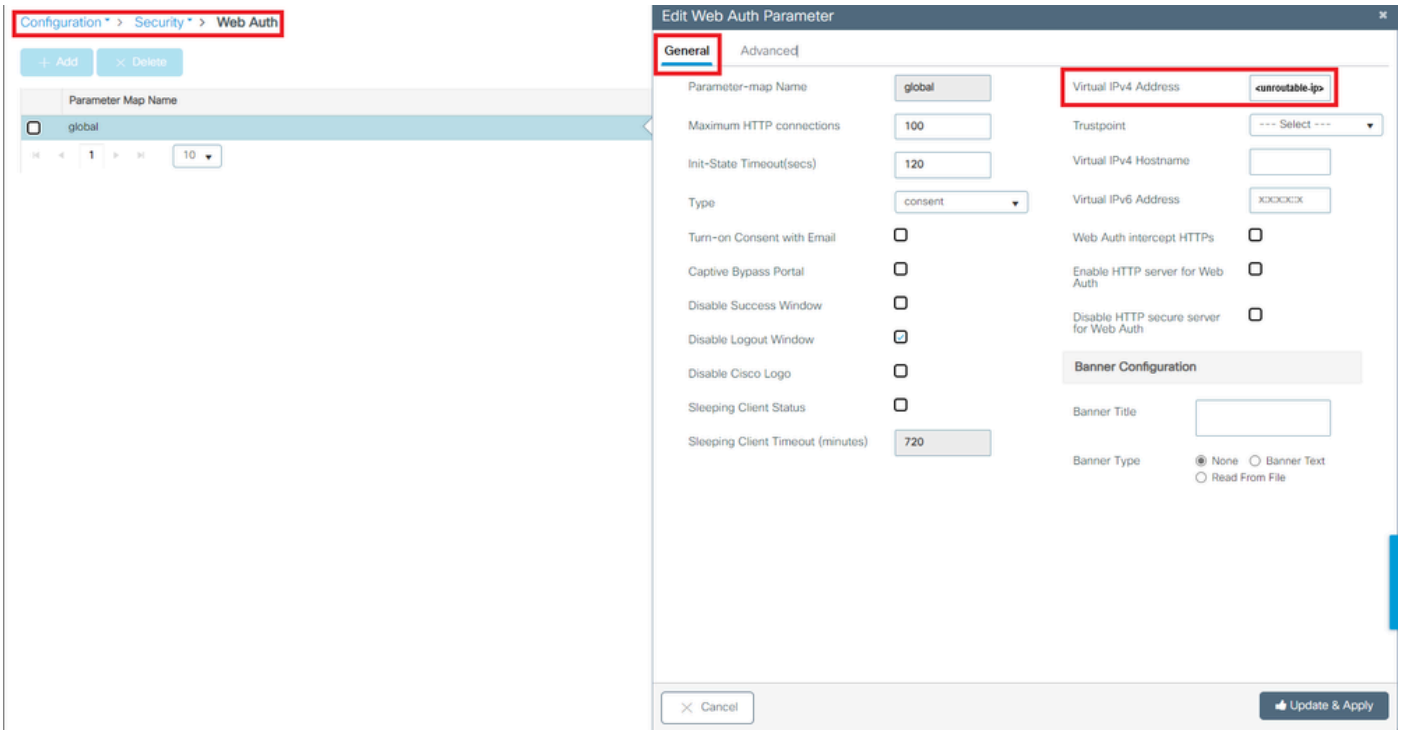
- カスタマイズされたポータルが正しくレンダリングされない（つまり、イメージが表示されない）。

推奨ソリューション

グローバルパラメータマップに仮想IPアドレスが割り当てられていることを確認します。

GUI で次の手順を実行します。

1. Configuration > Security > Web Authの順に選択します。
2. リストからグローバルパラメータマップを選択します。
3. ルーティングできない仮想IPアドレスを追加します。



グローバルパラメータマップの仮想IPアドレスをルーティング不能IPアドレスに設定

CLI から、

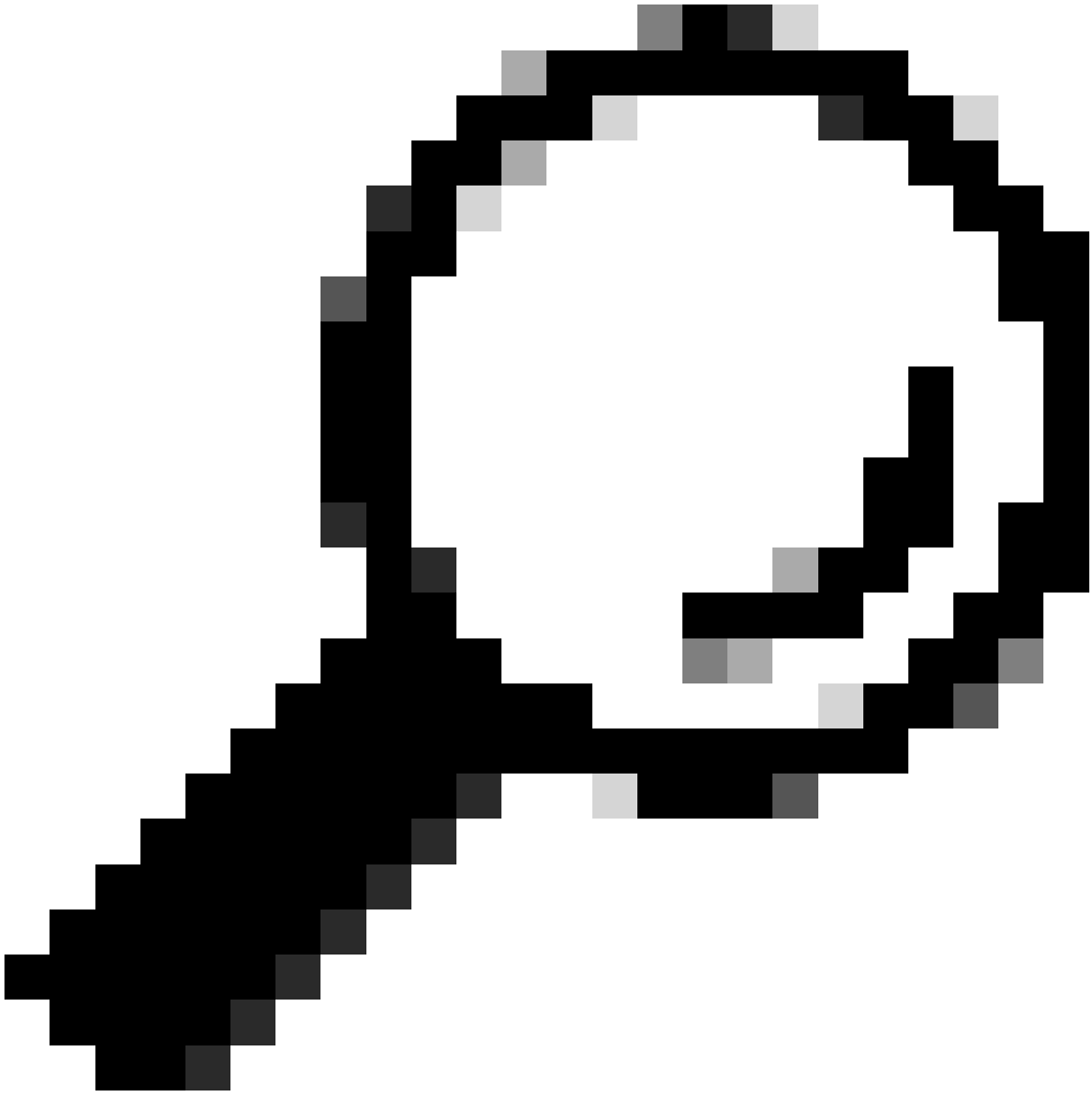
<#root>

```
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>



ヒント：仮想IPアドレスは、Web認証ログインページのリダイレクトアドレスとして機能します。ネットワーク上の他のデバイスは同じIPを持つことはできず、物理ポートにマッピングすることも、ルーティングテーブルに存在することもできません。したがって、仮想IPはルーティング不能IPアドレスとして設定することを推奨します。RFC5737に記載されているものだけを使用できます。

ポータルに「Your connection is not secure/verify signature failed」と表示される

エンドクライアントから発生する可能性のある動作

- ポータルを開くと、接続が安全でないことを示すエラーがクライアントに表示されます。
- ポータルは証明書を使用することが想定されています。

知っておくべき事柄

ポータルがHTTPSの下に表示されることが予想される場合は、SSL(Secure Socket Layer)証明書を使用する必要があることを意味します。この証明書は、ドメインが実際に存在することを検証するために、サードパーティの認証局(CA)によって発行される必要があります。エンドクライアントがクレデンシャルを入力したり、ポータルを表示したりするときに、信頼を提供します。WLCに証明書をアップロードするには、このドキュメントを参照してください。

推奨ソリューション

最初に、必要なHTTP/HTTPSサービスを再起動します。ネットワークのニーズに完全に対応するために、どのHTTP/HTTPSサーバを有効にする必要があるのかをより細かく制御できるようになりました。Web認証用のHTTPおよびHTTPS要求の設定の詳細については、このリンクを参照してください。

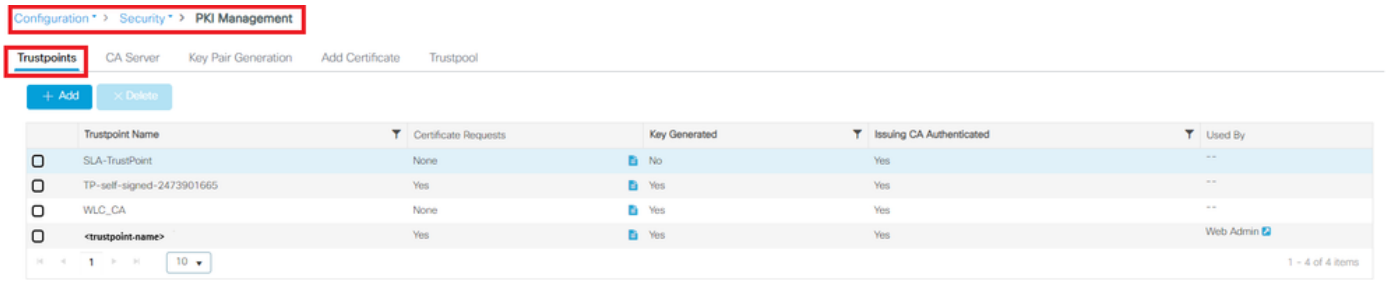
CLI から、

```
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
```

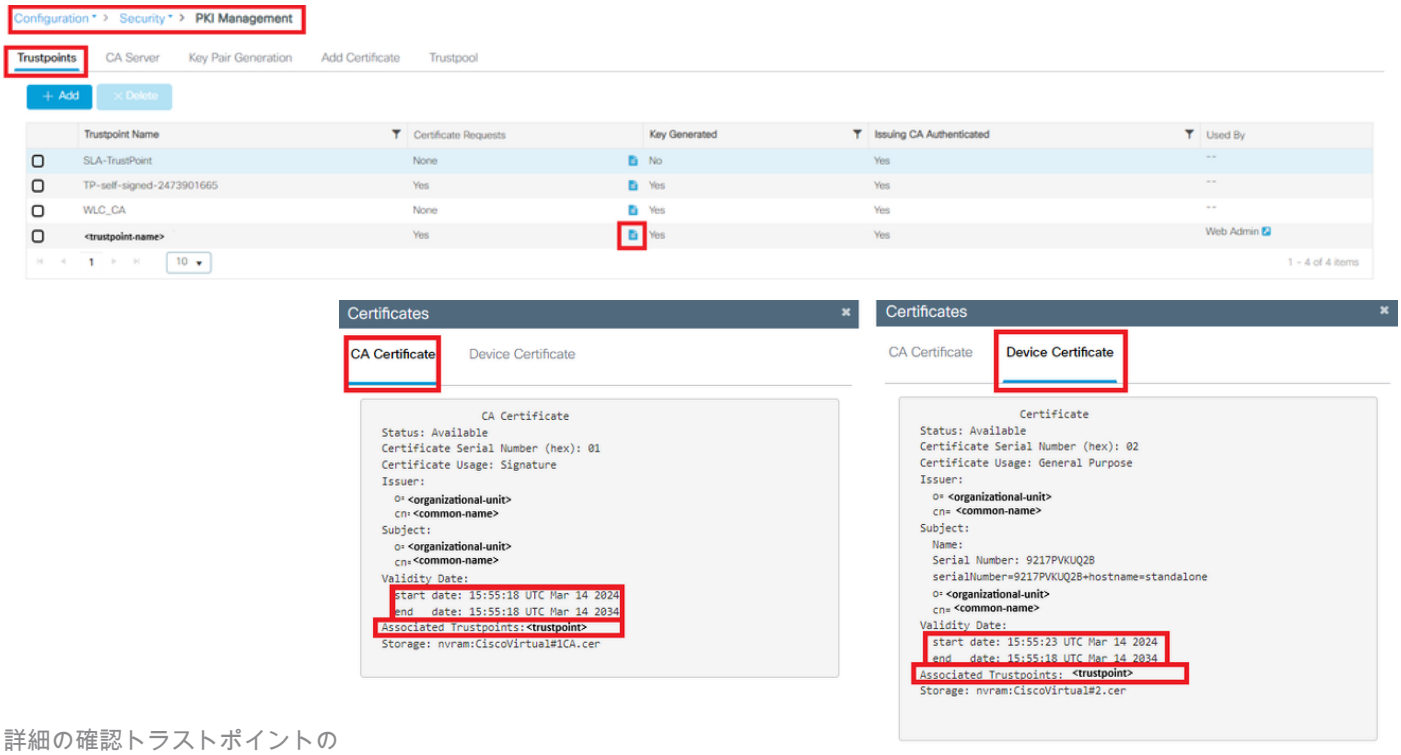
2番目：証明書がWLCに正しくアップロードされていること、およびその有効期間の日付が正しいことを確認します。

GUI で次の手順を実行します。

1. Configuration > Security > PKI Managementの順に選択します。
2. リストでトラストポイントを検索します
3. 詳細を確認する



トラストポイントの存在の確認トラストポイントの



詳細の確認トラストポイントの
有効性の確認

CLI から、

<#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>

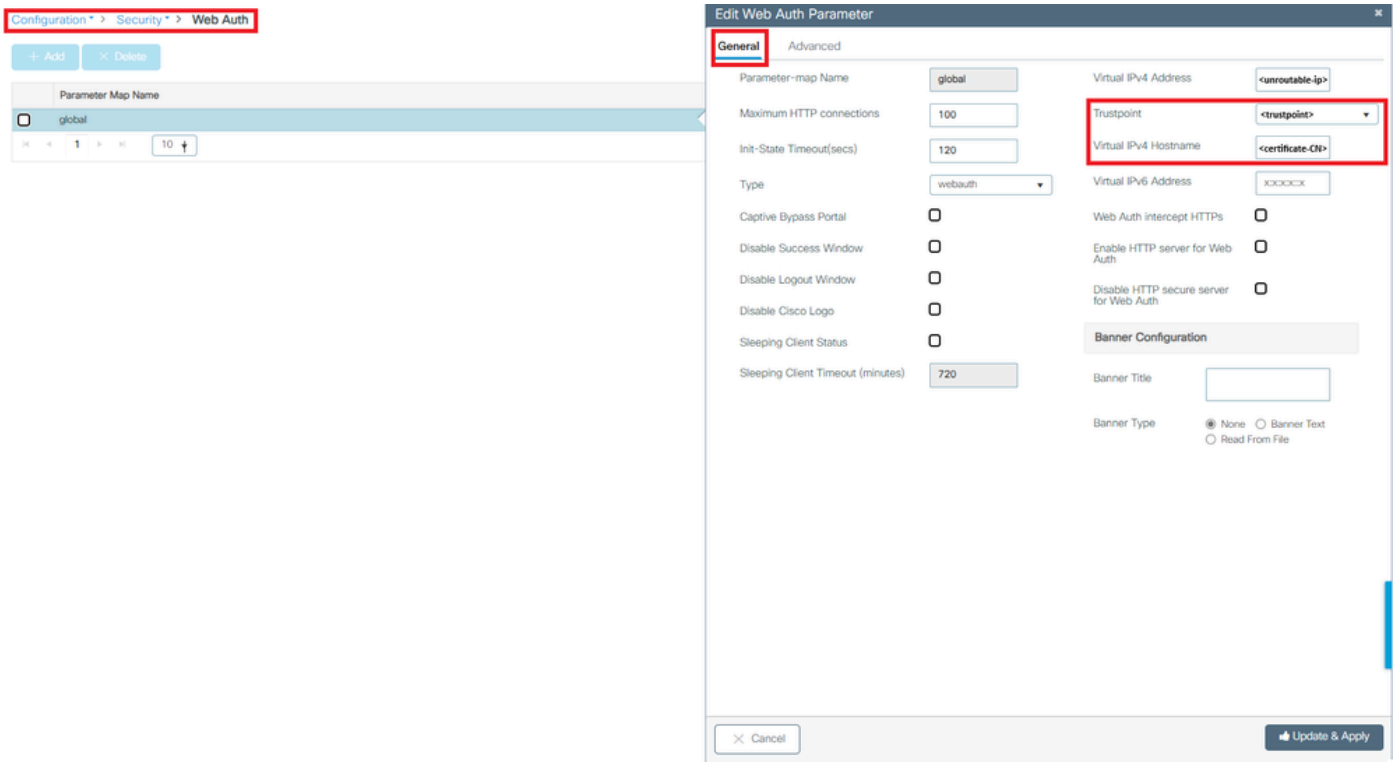
Associated Trustpoints: <trustpoint>

3:WebAuthパラメータマップで使用するために正しい証明書が選択されていること、および仮想

IPv4ホスト名が証明書内の共通名(CN)と一致することを確認します。

GUI で次の手順を実行します。

1. Configuration > Security > Web Authの順に選択します。
2. 使用するパラメータマップをリストから選択します。
3. トラストポイントと仮想IPv4ホスト名が正しいことを確認します。



トラストポイントと仮想IPv4ホスト名の確認

CLI から、

<#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>

関連情報

- ローカルWeb認証の設定
- Webベース認証(EWC)
- Catalyst 9800 WLCでのWeb認証ポータルのカスタマイズ
- Catalyst 9800 WLCでのCSR証明書の生成とダウンロード
- 仮想インターフェイスの設定

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。