Configure Verify and Troubleshoot Web Auth on Mac Filter Failure

Contents

Introduction

This document describes to Configure, Troubleshoot and Verify Local Web Auth on “Mac Filter Failure” feature using ISE for external authentication.

Prerequisites

Configure ISE for MAC Authentication

Valid user credentials configured on ISE/Active Directory

Requirements

Cisco recommends that you have knowledge of these topics:

Basic understanding to navigate through controller Web UI

Policy, WLAN profile and Policy Tags configuration

Service policy configuration on ISE

Components Used

9800 WLC version 17.12.2

C9120 AXI AP

9300 switch

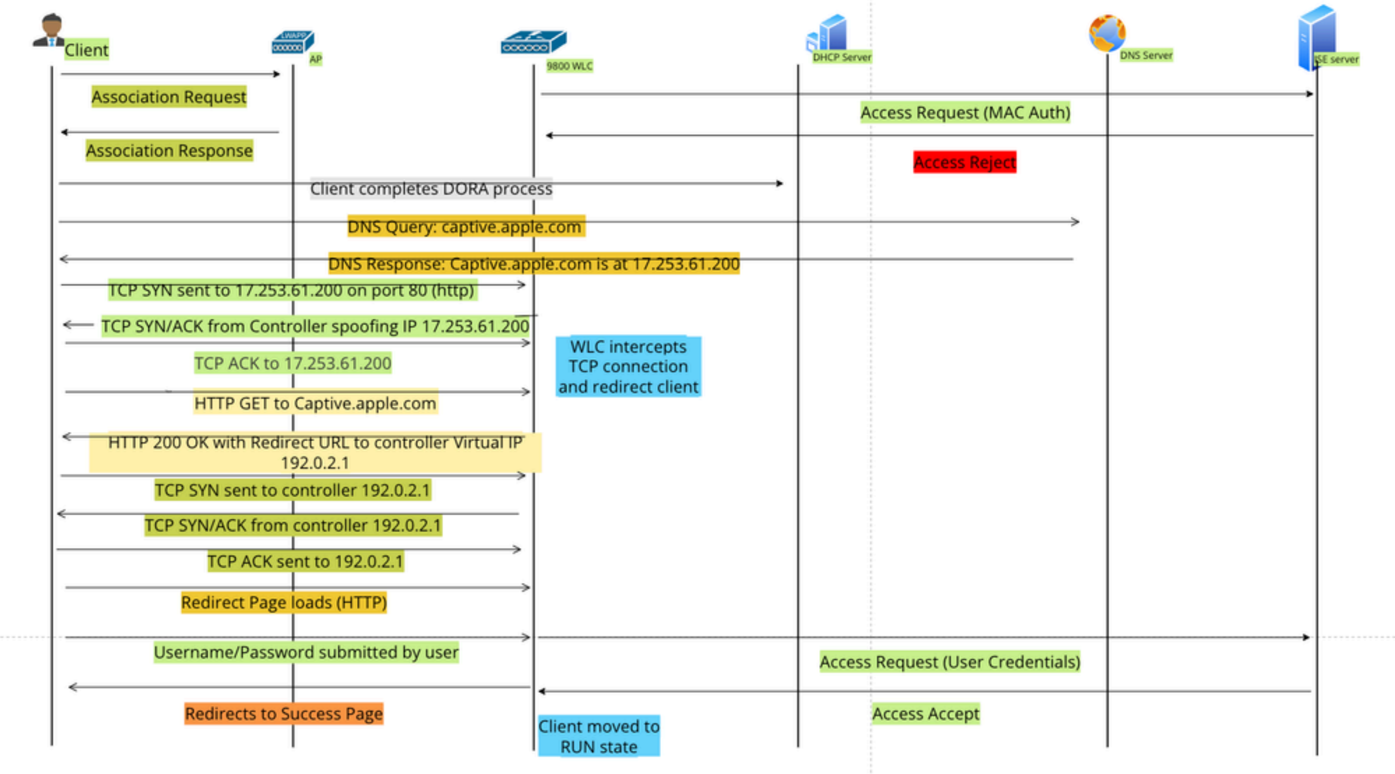
ISE version version 3.1.0.518

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

The Web Auth "On Mac Failure Filter" feature serves as a fallback mechanism in WLAN environments that use both MAC Authentication and Web Authentication.

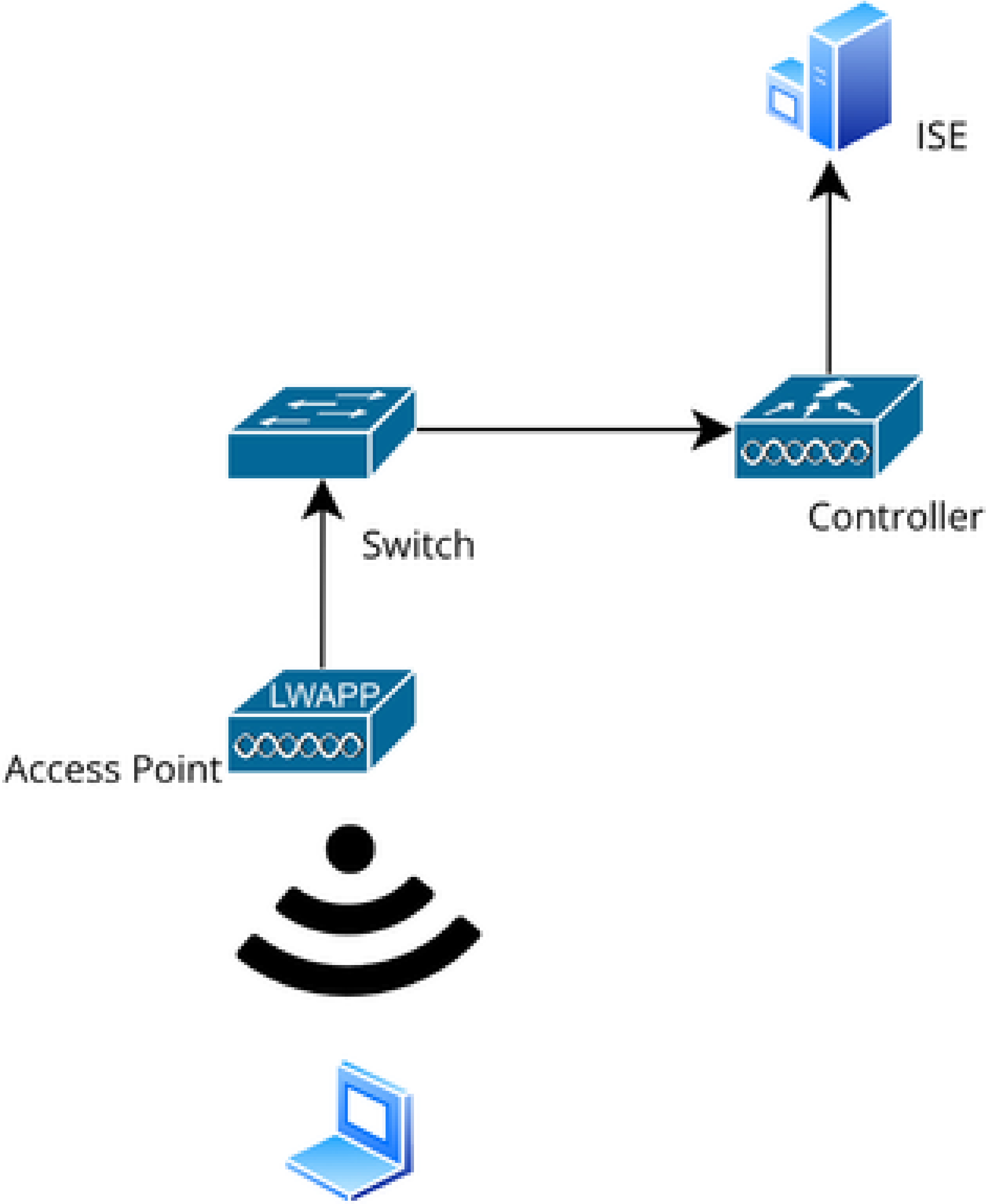
- **Fallback Mechanism:** When a client attempts to connect to a WLAN with MAC Filter against an external RADIUS server (ISE) or local server and fails to authenticate, this feature automatically initiates a Layer 3 Web Authentication.
- **Successful Authentication:** If a client successfully authenticates through the MAC Filter, Web Authentication is bypassed, allowing the client to connect directly to the WLAN.
- **Avoiding Disassociations:** This feature helps prevent disassociations that can otherwise occur due to MAC filter authentication failures.


Client
AP
9800 WLC
DHCP Server
DNS Server
ISE server
Association Request
Association Response
Access Request (MAC Auth)
Access Reject
Client completes DORA process
DNS Query: captive.apple.com
DNS Response: Captive.apple.com is at 17.253.61.200
TCP SYN sent to 17.253.61.200 on port 80 (http)
TCP SYN/ACK from Controller spoofing IP 17.253.61.200
WLC intercepts TCP connection and redirect client
TCP ACK to 17.253.61.200
HTTP GET to Captive.apple.com
HTTP 200 OK with Redirect URL to controller Virtual IP 192.0.2.1
TCP SYN sent to controller 192.0.2.1
TCP SYN/ACK from controller 192.0.2.1
TCP ACK sent to 192.0.2.1
Redirect Page loads (HTTP)
Username/Password submitted by user
Access Request (User Credentials)
Redirects to Success Page
Access Accept
Client moved to RUN state

Web Auth Flow

Configure

Network Diagram



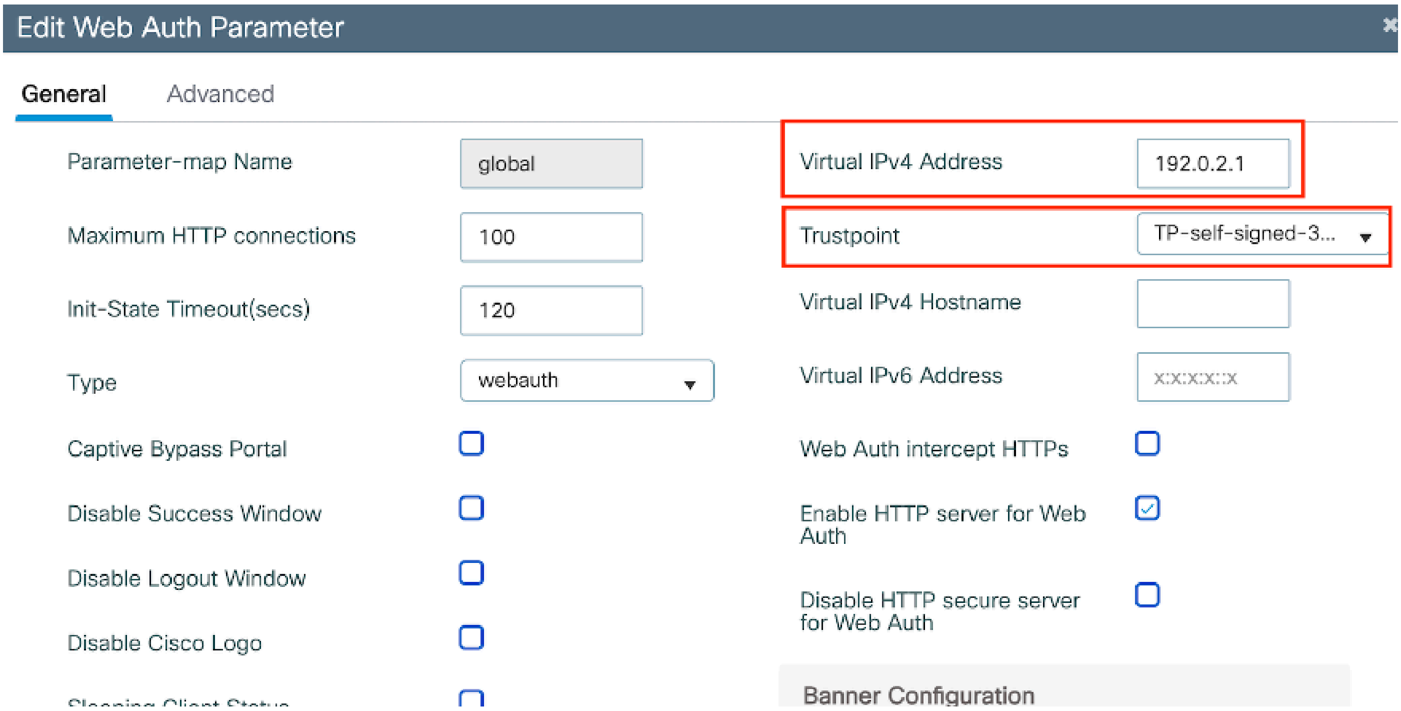
Network Topology

Configurations

Configure Web Parameters

Navigate to Configuration > Security > Web Auth and select the **Global** parameter map

Verify the **Virtual IP** and **Trustpoint** configuration from the Global Parameter Map. All custom Web Auth parameter profiles inherit the Virtual IP and Trustpoint configuration from the Global Parameter Map.

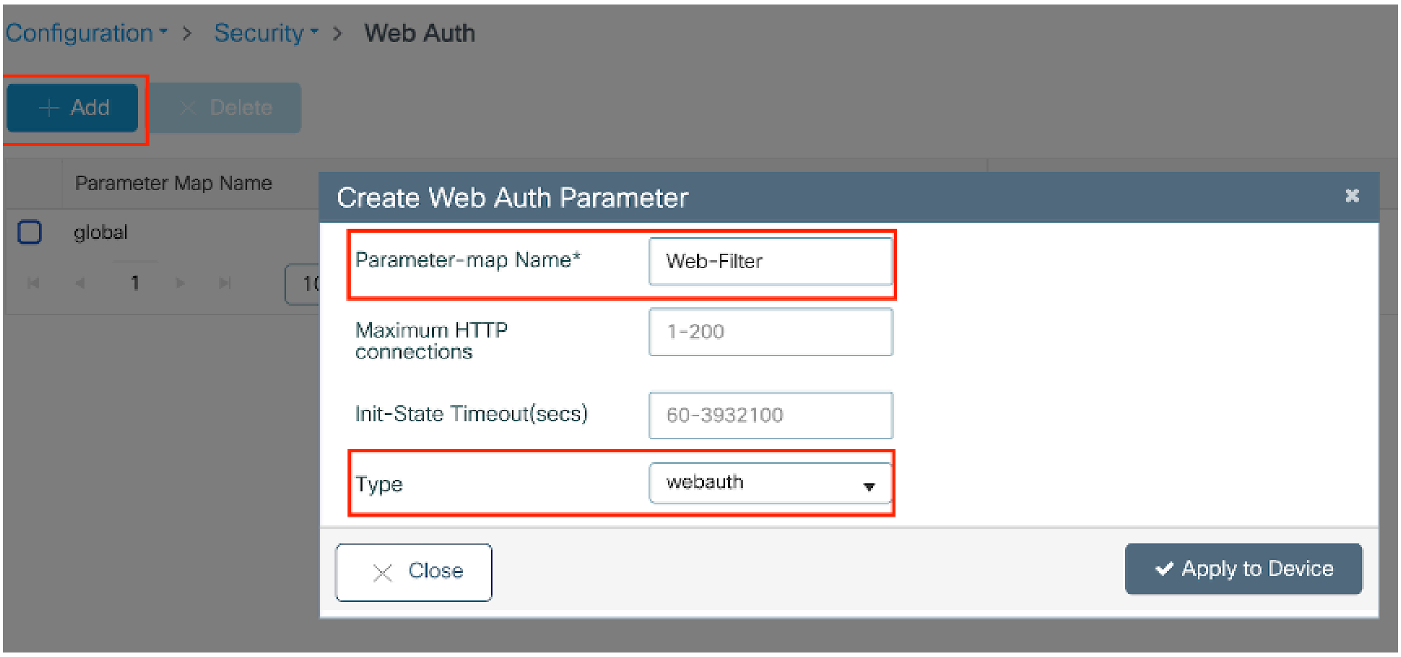


Edit Web Auth Parameter

Parameter-map Name	global	Virtual IPv4 Address	192.0.2.1
Maximum HTTP connections	100	Trustpoint	TP-self-signed-3...
Init-State Timeout(secs)	120	Virtual IPv4 Hostname	
Type	webauth	Virtual IPv6 Address	X:X:X:X::X
Captive Bypass Portal	□	Web Auth intercept HTTPs	□
Disable Success Window	□	Enable HTTP server for Web Auth	☑
Disable Logout Window	□	Disable HTTP secure server for Web Auth	□
Disable Cisco Logo	□	Banner Configuration	

Global Web Auth Parameter Profile

Step1: Select "Add" to create a custom web authentication parameter map. Enter Profile name and choose Type as "Webauth".



Create Web Auth Parameter

Parameter-map Name*	Web-Filter
Maximum HTTP connections	1-200
Init-State Timeout(secs)	60-3932100
Type	webauth

Web Auth Parameter Profile

If your clients are also getting an IPv6 address, you must also add a Virtual IPv6 address in the parameter map. Use an IP in the documentation range **2001:db8::/32**

If your clients obtained an IPv6 address, there is a good chance they try to get the HTTP web auth redirection in V6 and not V4, which is why you need the Virrtual IPv6 to be set also.

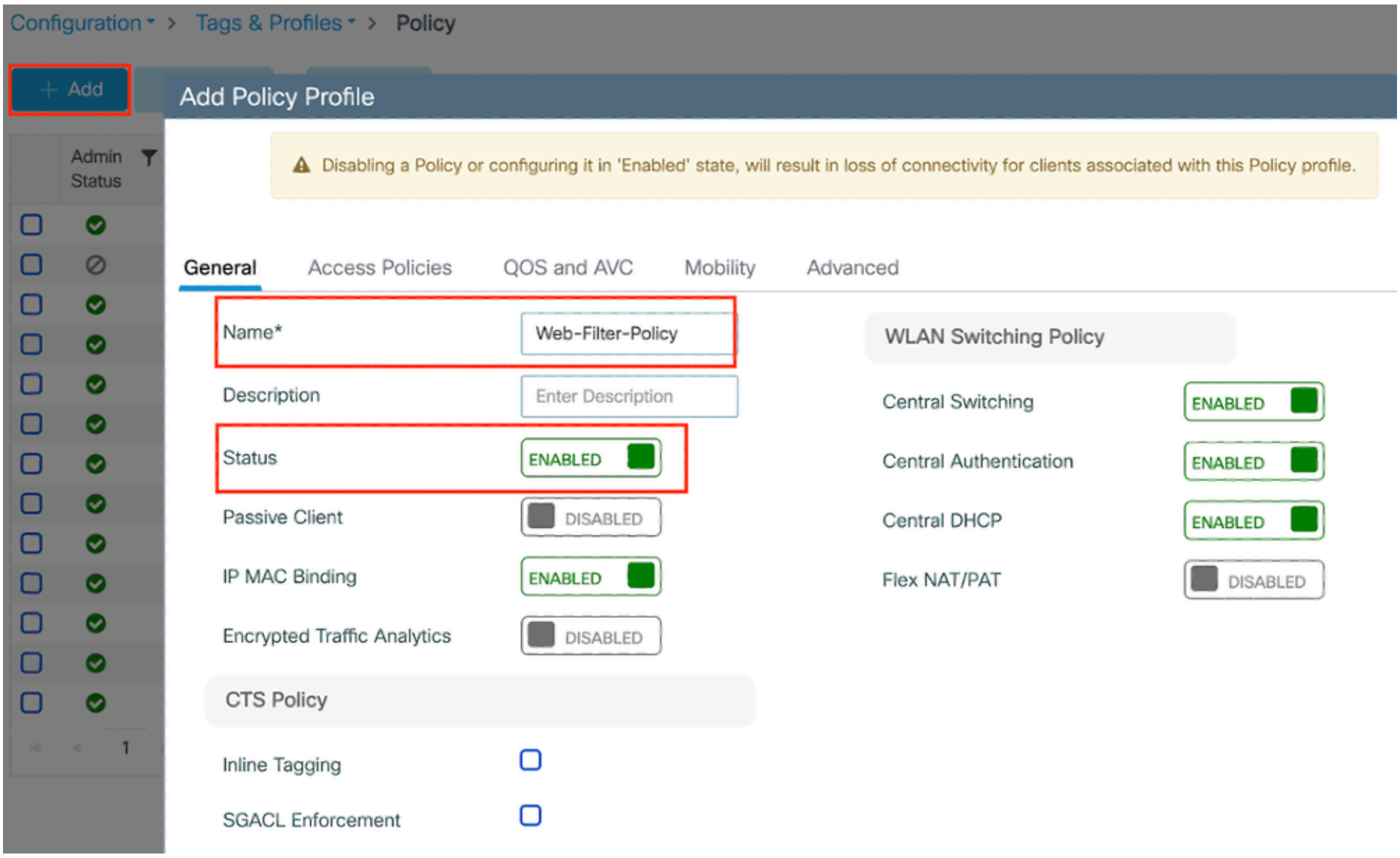
CLI Configuration:

```
parameter-map type webauth Web-Filter
 type webauth
```

Configure Policy Profile

Step1: Create a Policy Profile

Navigate to Configuration > Tags & Profiles > Policy. Select "Add". In the General tab, specify a name for the profile and enable the status toggle.



Add Policy Profile

⚠ Disabling a Policy or configuring it in 'Enabled' state, will result in loss of connectivity for clients associated with this Policy profile.

Name*	Web-Filter-Policy
Description	Enter Description
Status	ENABLED
Passive Client	DISABLED
IP MAC Binding	ENABLED
Encrypted Traffic Analytics	DISABLED

CTS Policy

Inline Tagging	□
SGACL Enforcement	□

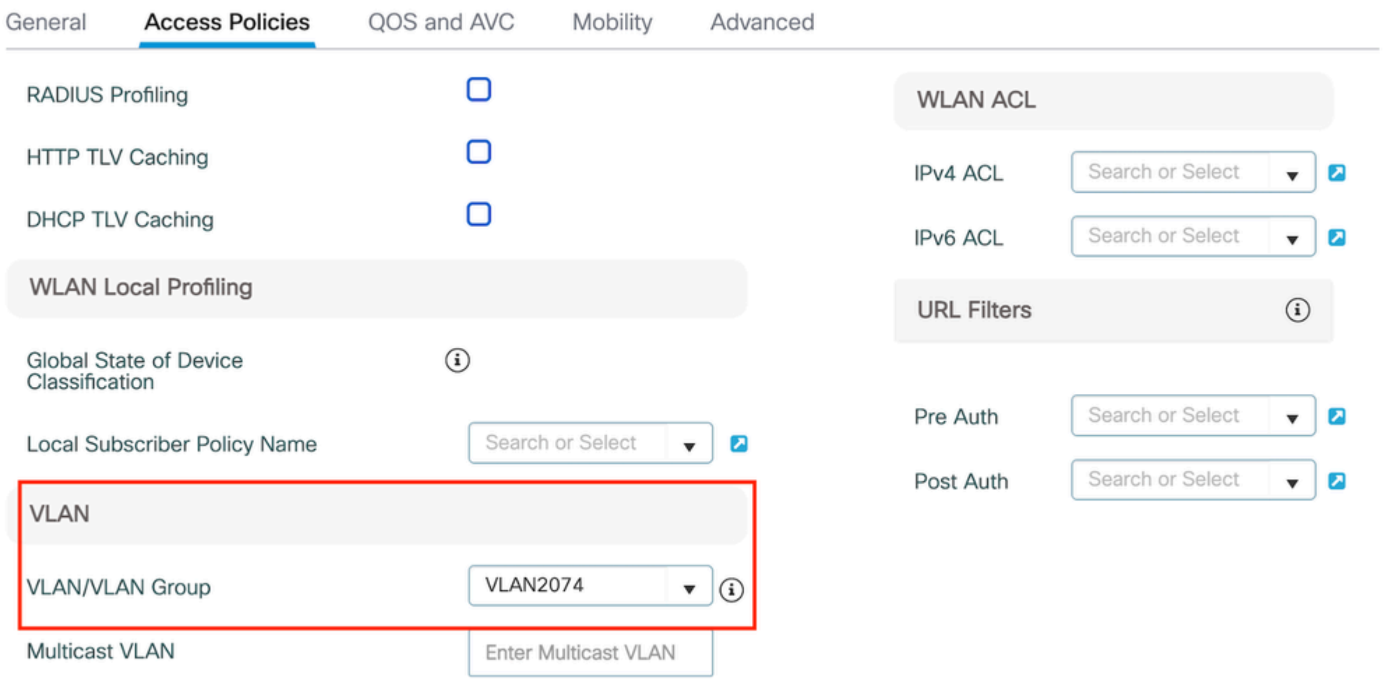
WLAN Switching Policy

Central Switching	ENABLED
Central Authentication	ENABLED
Central DHCP	ENABLED
Flex NAT/PAT	DISABLED

Policy Profile

Step2:

Under the Access Policies tab, choose the client VLAN from the VLAN section dropdown list.



RADIUS Profiling □

HTTP TLV Caching □

DHCP TLV Caching □

WLAN Local Profiling

Global State of Device Classification ⓘ

Local Subscriber Policy Name: Search or Select

VLAN

VLAN/VLAN Group: VLAN2074 ⓘ

Multicast VLAN: Enter Multicast VLAN

WLAN ACL

IPv4 ACL: Search or Select

IPv6 ACL: Search or Select

URL Filters ⓘ

Pre Auth: Search or Select

Post Auth: Search or Select

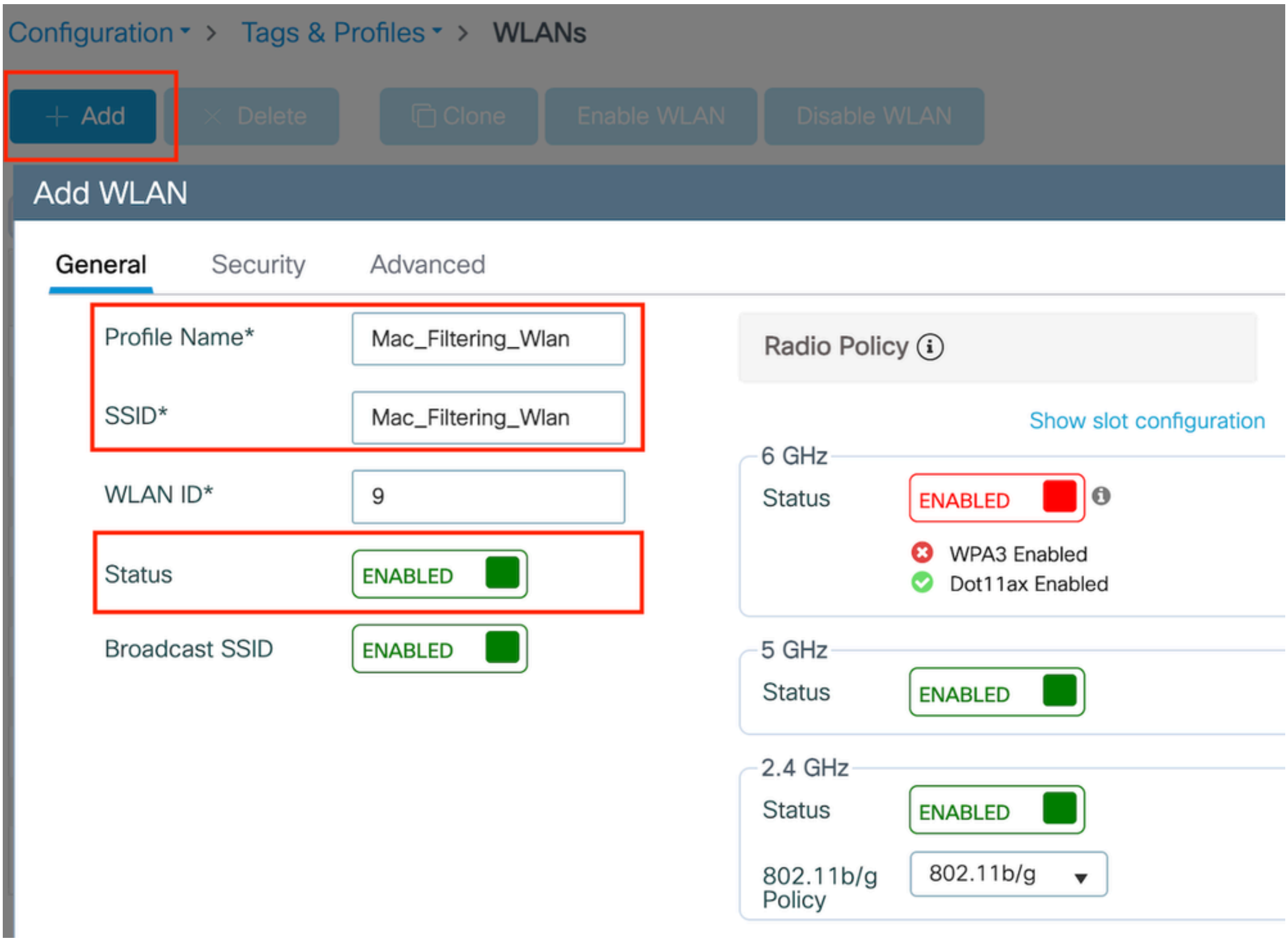
Access Policy tab

CLI Configuration:

```
wireless profile policy Web-Filter-Policy
 vlan VLAN2074
 no shutdown
```

Configure WLAN Profile

Step1: Navigate to Configuration > Tags and Profiles > WLANs. Select "Add" to create a new profile. Define a profile name and SSID name, and enable the status field.



Add WLAN

Profile Name* Mac_Filtering_Wlan

SSID* Mac_Filtering_Wlan

WLAN ID* 9

Status ENABLED

Broadcast SSID ENABLED

Radio Policy

Show slot configuration

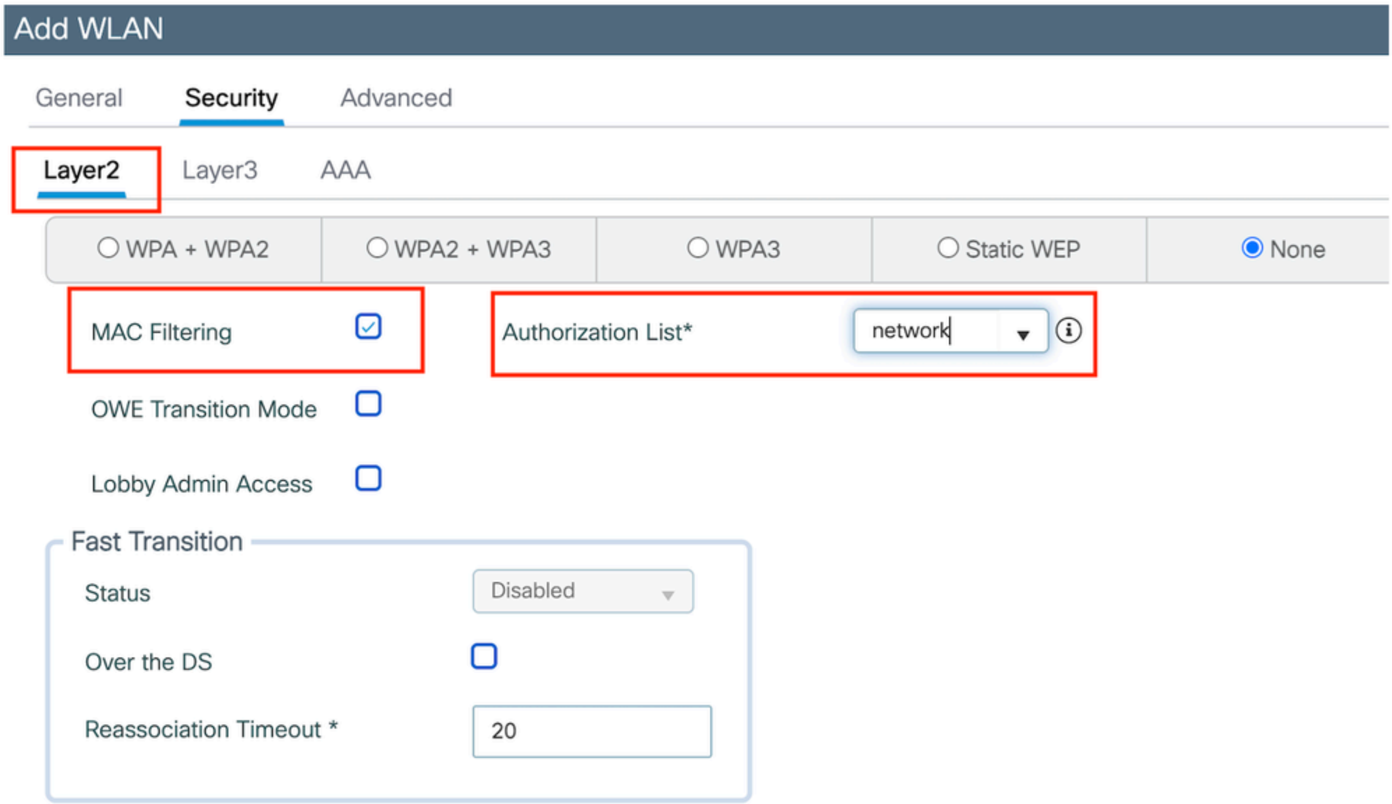
6 GHz
Status ENABLED
☒ WPA3 Enabled
✓ Dot11ax Enabled

5 GHz
Status ENABLED

2.4 GHz
Status ENABLED
802.11b/g Policy 802.11b/g ▾

WLAN Profile

Step2: Under the Security tab, enable the "Mac Filtering" checkbox and configure the RADIUS server in the Authorization List (ISE or local server). This setup utilizes ISE for both Mac Authentication and Web Authentication.



Add WLAN

General | Security | Advanced

Layer2 | Layer3 | AAA

○ WPA + WPA2 ○ WPA2 + WPA3 ○ WPA3 ○ Static WEP ● None

MAC Filtering ☑

Authorization List* network

OWE Transition Mode □

Lobby Admin Access □

Fast Transition

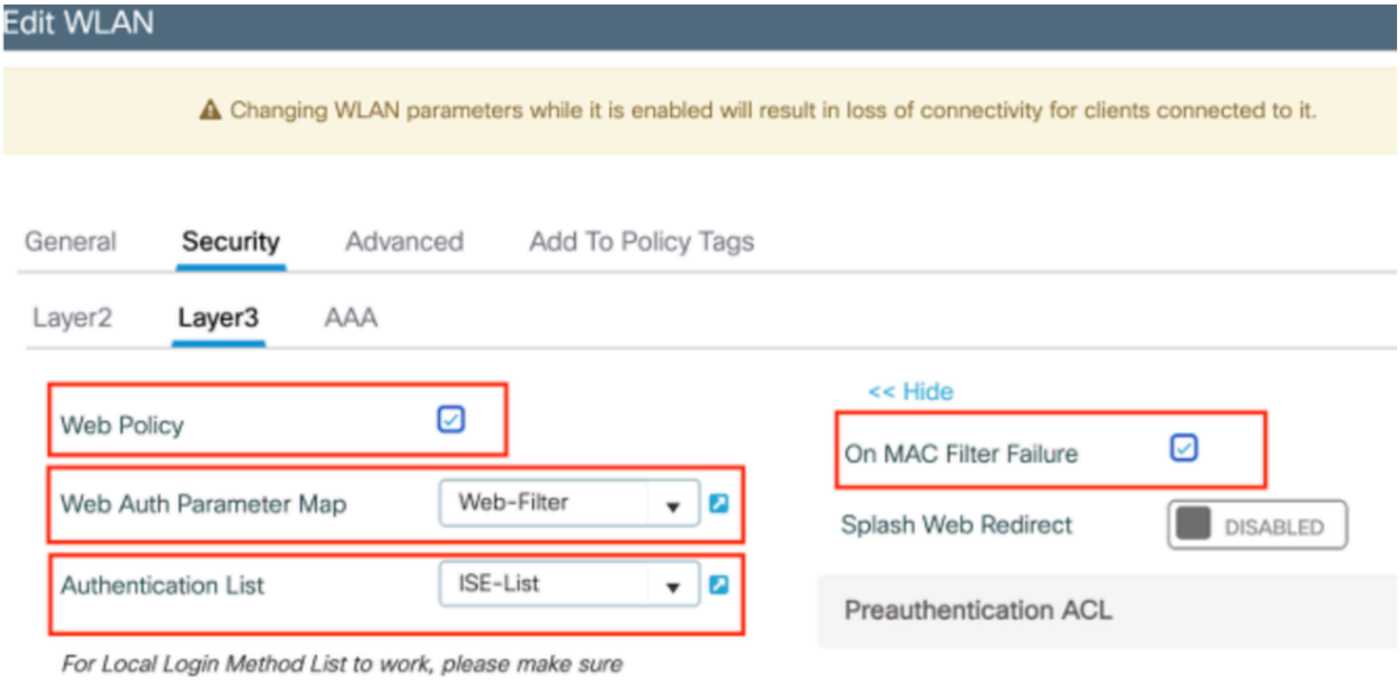
Status Disabled

Over the DS □

Reassociation Timeout * 20

WLAN Layer 2 security

Step3: Navigate to Security > Layer3. Enable Web Policy and associate it with the Web Authentication Parameter Map profile. Check the "On Mac Filter Failure" checkbox and choose the RADIUS server from the Authentication list dropdown.



Edit WLAN

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

General | Security | Advanced | Add To Policy Tags

Layer2 | Layer3 | AAA

Web Policy ☑

Web Auth Parameter Map Web-Filter

Authentication List ISE-List

For Local Login Method List to work, please make sure

<< Hide

On MAC Filter Failure ☑

Splash Web Redirect DISABLED

Preauthentication ACL

WLAN Layer3 security tab

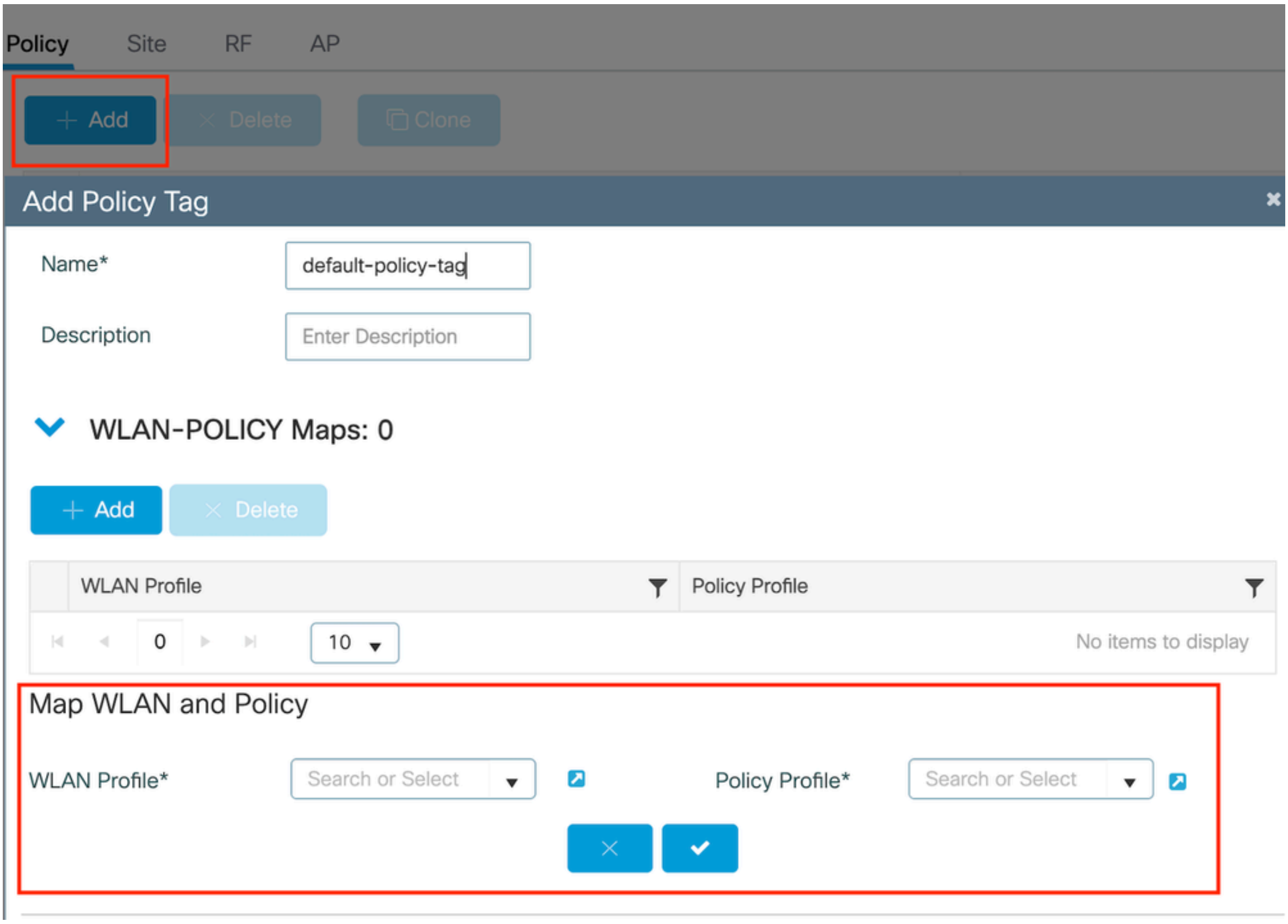
CLI Configuration

```
wlan Mac_Filtering_Wlan 9 Mac_Filtering_Wlan
```

```
 mac-filtering network
 radio policy dot11 24ghz
 radio policy dot11 5ghz
 no security ft adaptive
 no security wpa
 no security wpa wpa2
 no security wpa wpa2 ciphers aes
 no security wpa akm dot1x
 security web-auth
 security web-auth authentication-list ISE-List
 security web-auth on-macfilter-failure
 security web-auth parameter-map Web-Filter
 no shutdown
```

Step4: Configure Policy Tags, Create WLAN Profile, and Policy Profile Mapping

Navigate to Configuration > Tags & Profiles > Tags > Policy. Click "Add" to define a name for the Policy Tag. Under WLAN-Policy Maps, select "Add" to map the previously created WLAN and Policy profile.



Name* default-policy-tag

Description Enter Description

WLAN Profile	Policy Profile
0 10	No items to display

WLAN Profile* Search or Select

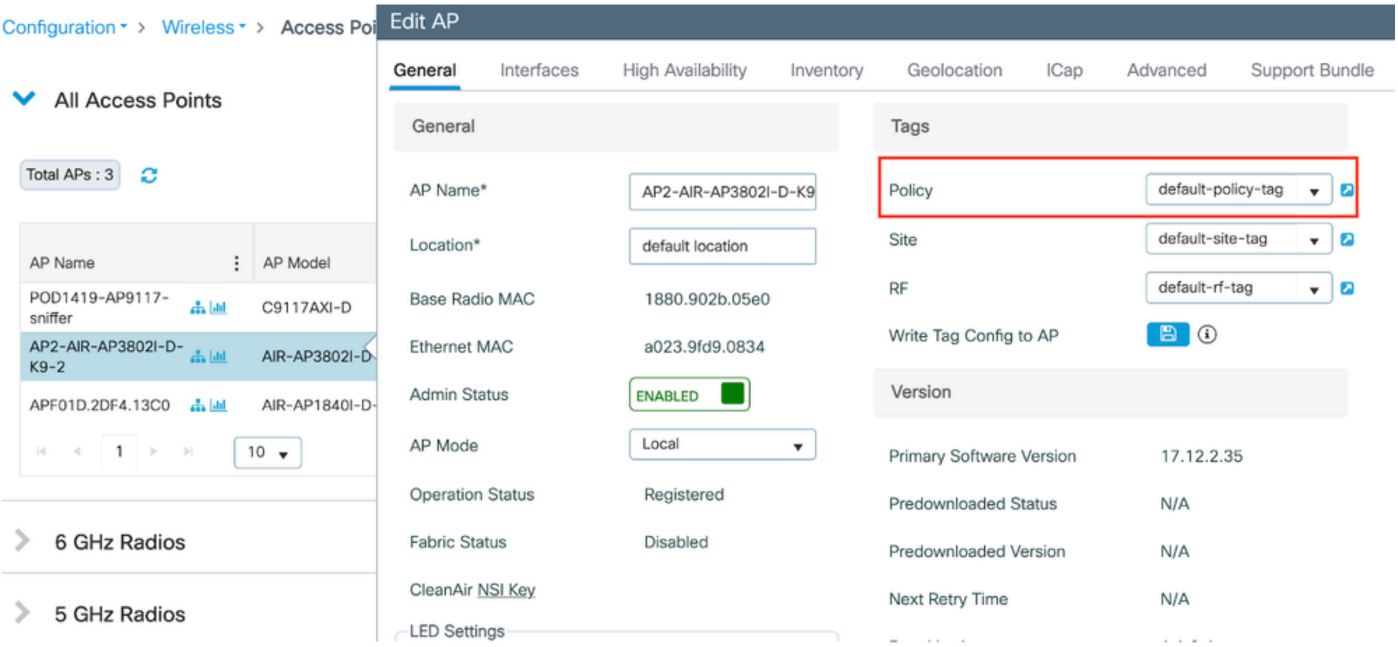
Policy Profile* Search or Select

Policy TAG map

CLI Configuration:

```
wireless tag policy default-policy-tag
 description "default policy-tag"
wlan Mac_Filtering_Wlan policy Web-Filter-Policy
```

Step 5: Navigate to Configuration > Wireless > Access Point. Select the access point responsible for broadcasting this SSID. Within the Edit AP menu, assign the created Policy Tag.



Configuration > Wireless > Access Poi

All Access Points

Total APs : 3

AP Name	AP Model
POD1419-AP9117-sniffer	C9117AXI-D
AP2-AIR-AP3802I-D-K9-2	AIR-AP3802I-D
APF01D.2DF4.13C0	AIR-AP1840I-D-

1 | 10

6 GHz Radios

5 GHz Radios

Edit AP

General | Interfaces | High Availability | Inventory | Geolocation | ICap | Advanced | Support Bundle

General

AP Name*	AP2-AIR-AP3802I-D-K9
Location*	default location
Base Radio MAC	1880.902b.05e0
Ethernet MAC	a023.9fd9.0834
Admin Status	ENABLED
AP Mode	Local
Operation Status	Registered
Fabric Status	Disabled
CleanAir NSI Key	

LED Settings

Tags

Policy	default-policy-tag
Site	default-site-tag
RF	default-rf-tag
Write Tag Config to AP	

Version

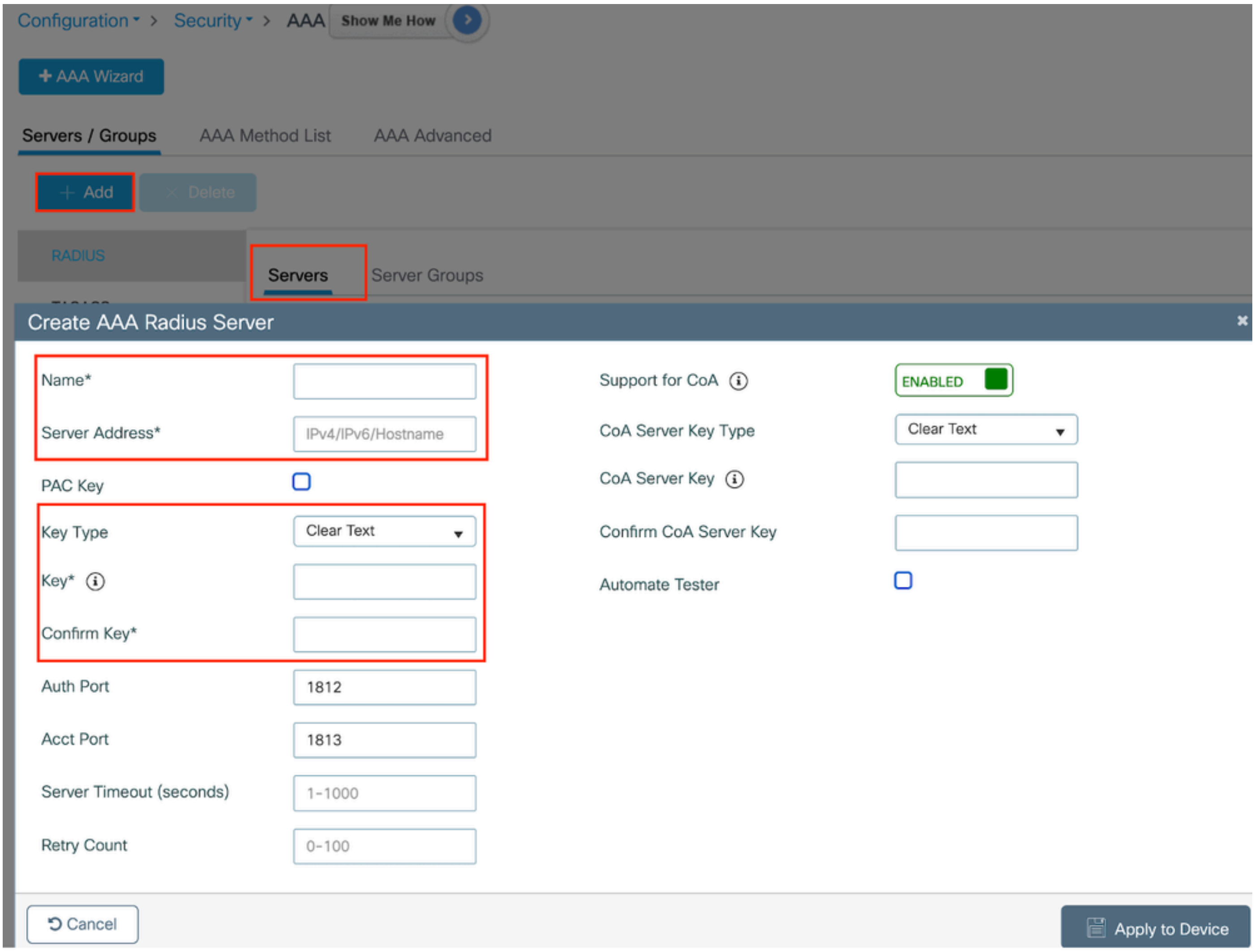
Primary Software Version	17.12.2.35
Predownloaded Status	N/A
Predownloaded Version	N/A
Next Retry Time	N/A

Mapping policy TAG to AP

Configure AAA Settings:

Step1: Create a Radius Server:

Navigate to Configuration > Security > AAA. Click the "Add" option under the Server/Group section. On the "Create AAA Radius Server" page, enter the server name, IP address, and Shared Secret.



Name*	
Server Address*	IPv4/IPv6/Hostname
PAC Key	□
Key Type	Clear Text
Key*	
Confirm Key*	
Auth Port	1812
Acct Port	1813
Server Timeout (seconds)	1-1000
Retry Count	0-100
Support for CoA	ENABLED
CoA Server Key Type	Clear Text
CoA Server Key	
Confirm CoA Server Key	
Automate Tester	□

Server Configuration

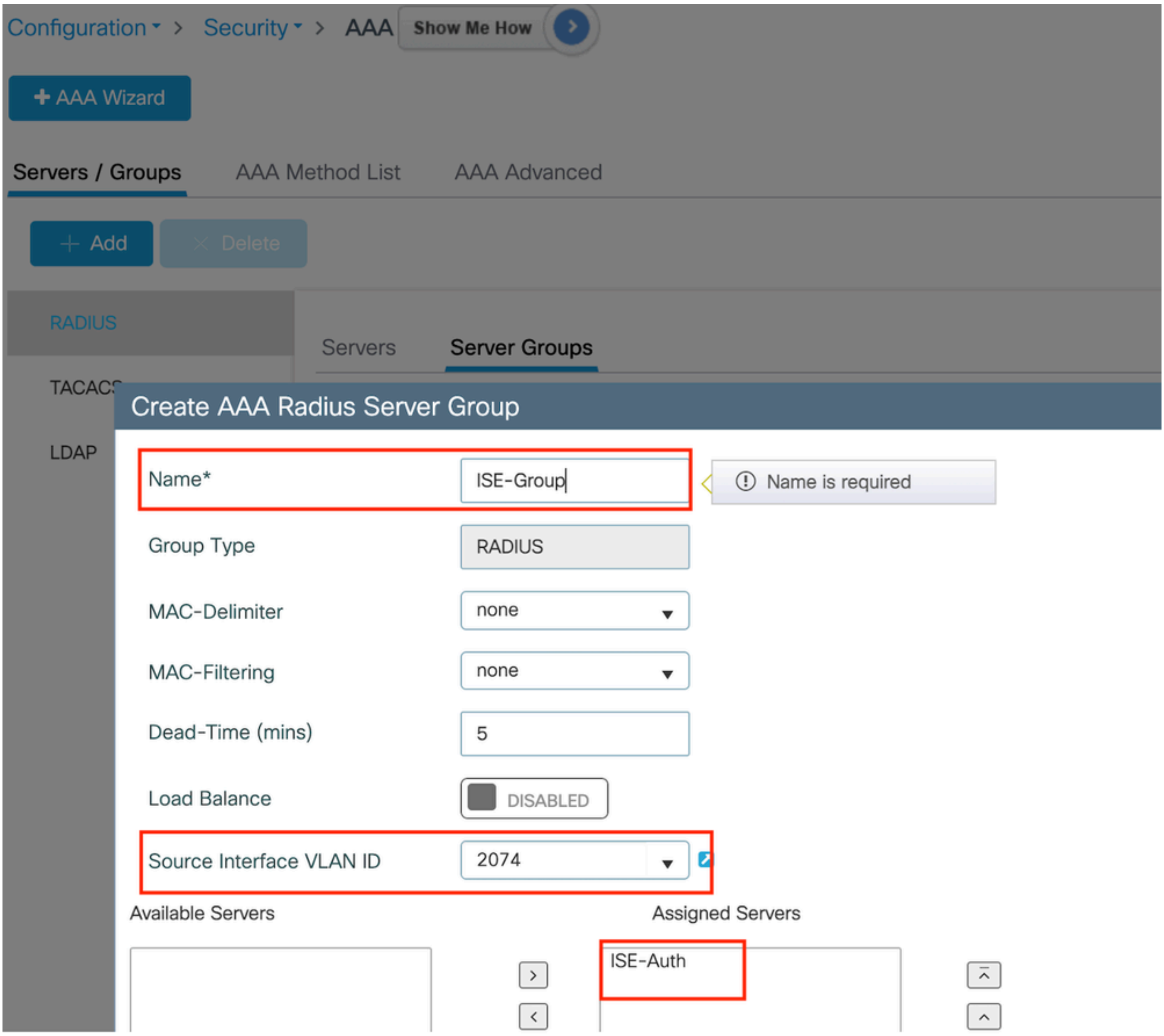
CLI Configuration

```
radius server ISE-Auth
 address ipv4 10.197.224.122 auth-port 1812 acct-port 1813
 key *****
 server name ISE-Auth
```

Step2: Create a Radius Server Group:

Select the "Add" option under the Server Groups section to define a server group. Toggle the servers to be included within the same group configuration.

It is not required to set the source interface. By default, the 9800 uses its routing table to figure out the interface to use to reach the RADIUS server and typically uses the default gateway.



Create AAA Radius Server Group

Name* ISE-Group

Name is required

Group Type RADIUS

MAC-Delimiter none

MAC-Filtering none

Dead-Time (mins) 5

Load Balance DISABLED

Source Interface VLAN ID 2074

Assigned Servers: ISE-Auth

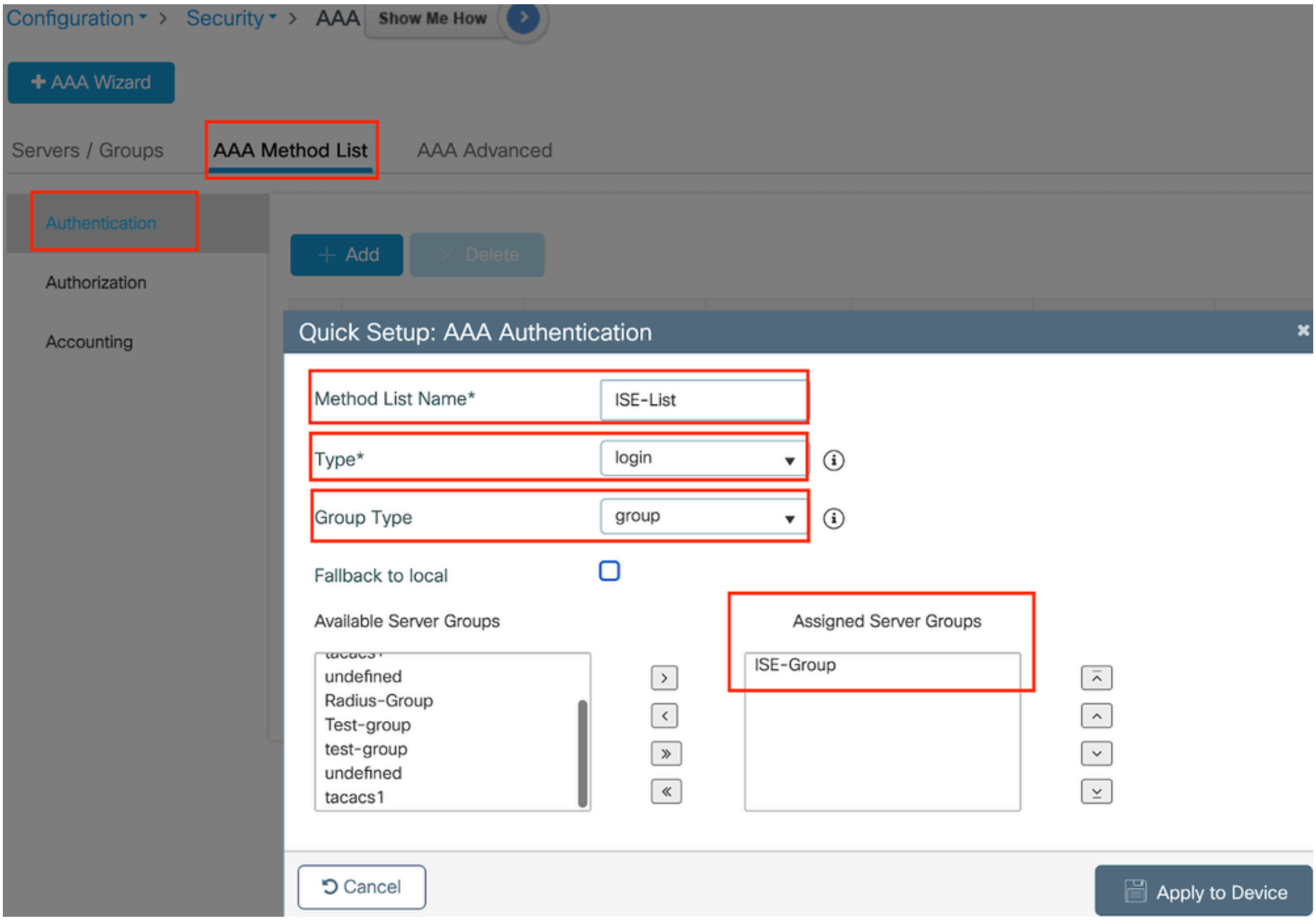
Server Group

CLI Configuration

```
aaa group server radius ISE-Group
 server name ISE-Auth
 ip radius source-interface Vlan2074
 deadtime 5
```

Step3: Configure AAA Method List:

Navigate to the AAA Method List tab. Under Authentication, click Add. Define a method list name with Type as "login" and Group type as "Group". Map the configured authentication server group under the Assigned Server Group section.



Quick Setup: AAA Authentication

Method List Name* ISE-List

Type* login

Group Type group

Fallback to local □

Available Server Groups

tacacs+
undefined
Radius-Group
Test-group
test-group
undefined
tacacs1

Assigned Server Groups

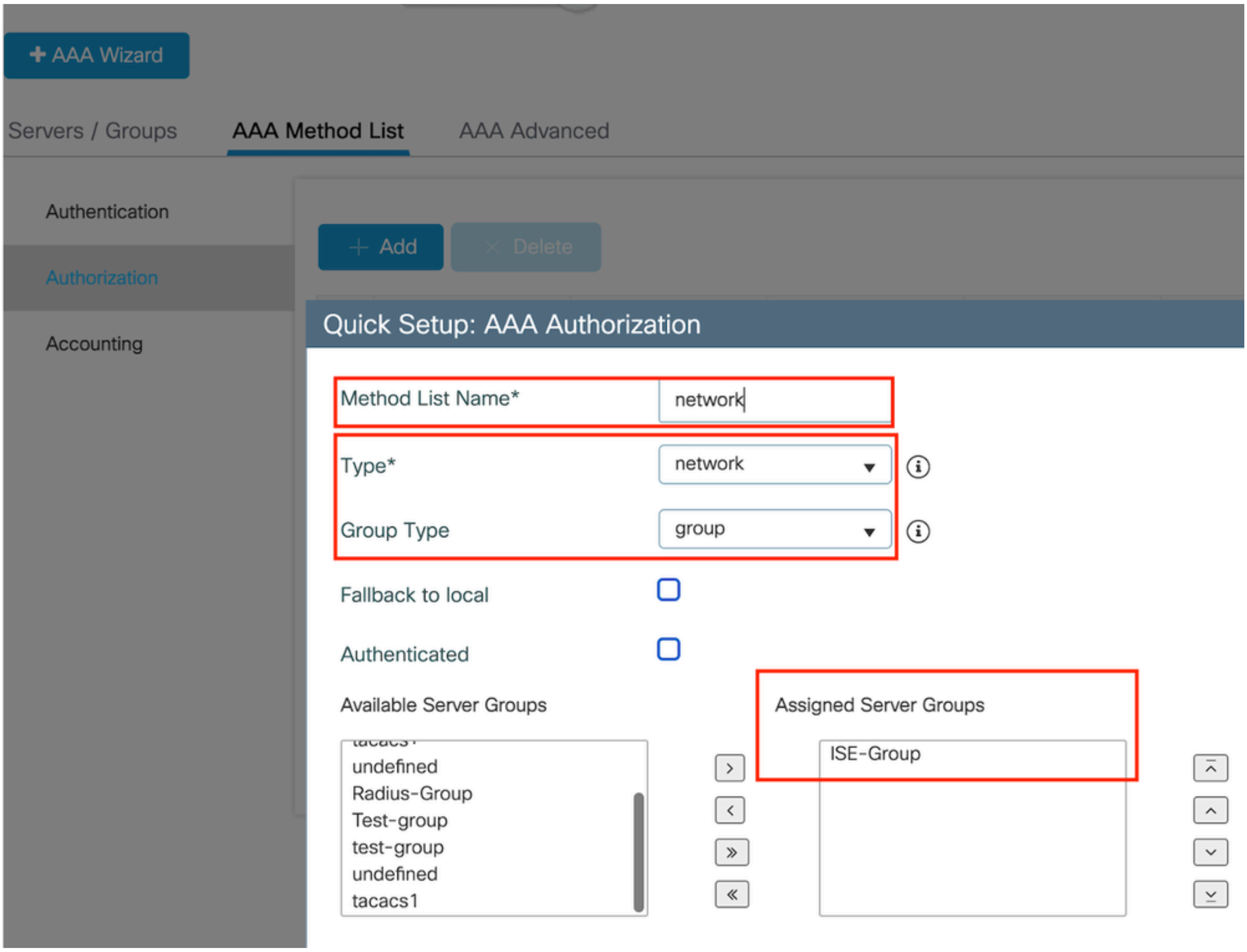
ISE-Group

Authentication Method list

CLI Configuration

```
aaa authentication login ISE-List group ISE-Group
```

Navigate to the Authorization Method List section and click "Add". Define a method list name and set the type to "network" with Group type as "Group". Toggle the configured RADIUS server to the Assigned Server Groups section.



Method List Name* network

Type* network

Group Type group

Fallback to local ☐

Authenticated ☐

Available Server Groups

- tacacs1
- undefined
- Radius-Group
- Test-group
- test-group
- undefined
- tacacs1

Assigned Server Groups

- ISE-Group

Authorization method list

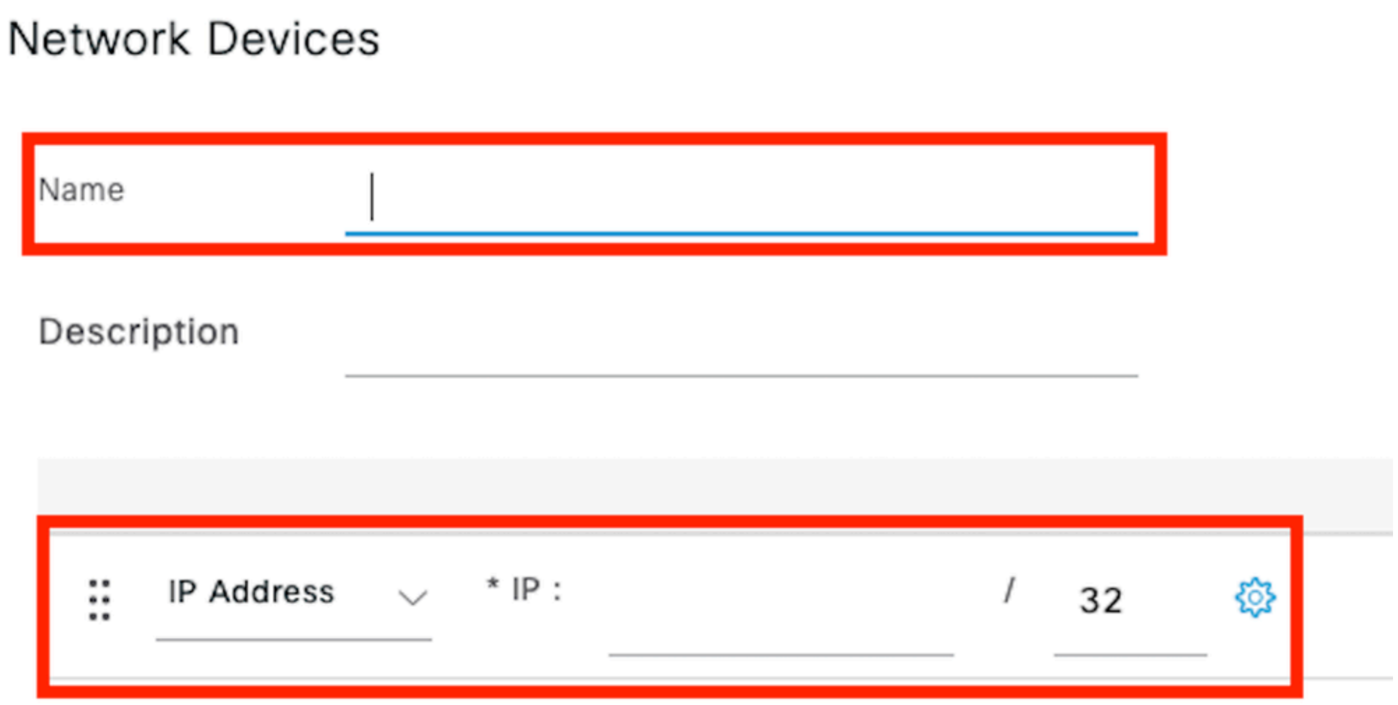
CLI Configuration

```
aaa authorization network network group ISE-Group
```

ISE configuration:

Add WLC as a network device on ISE

Step1: Navigate to Administration > Network Devices and click Add. Enter the controller IP address, Hostname and shared secret under the Radius Authentication Settings



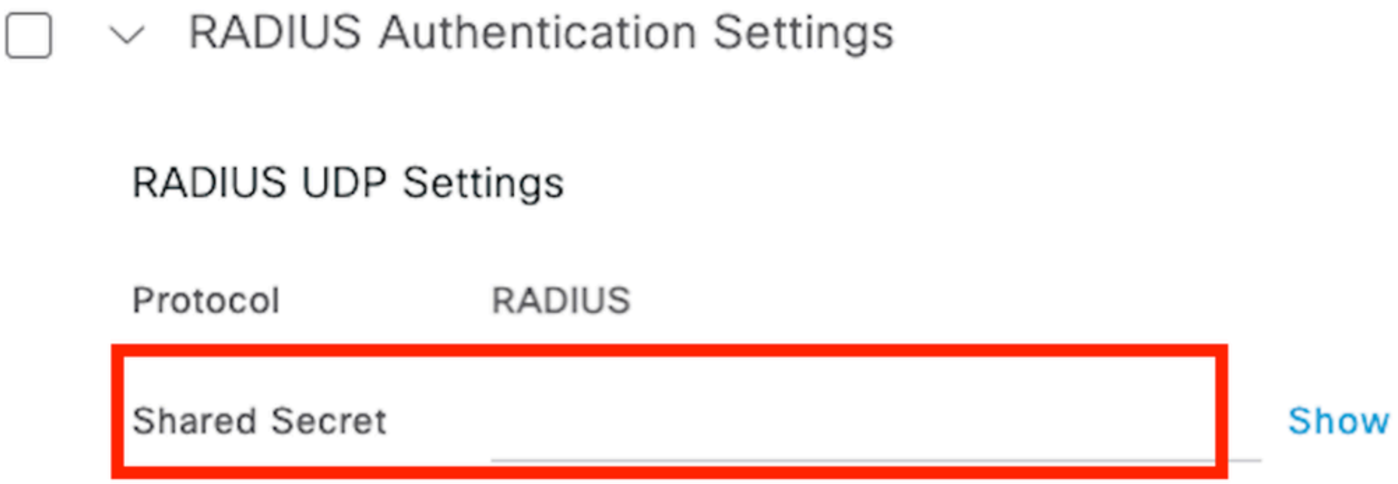
Network Devices

Name

Description

IP Address * IP : / 32

Add Network device



□ RADIUS Authentication Settings

RADIUS UDP Settings

Protocol RADIUS

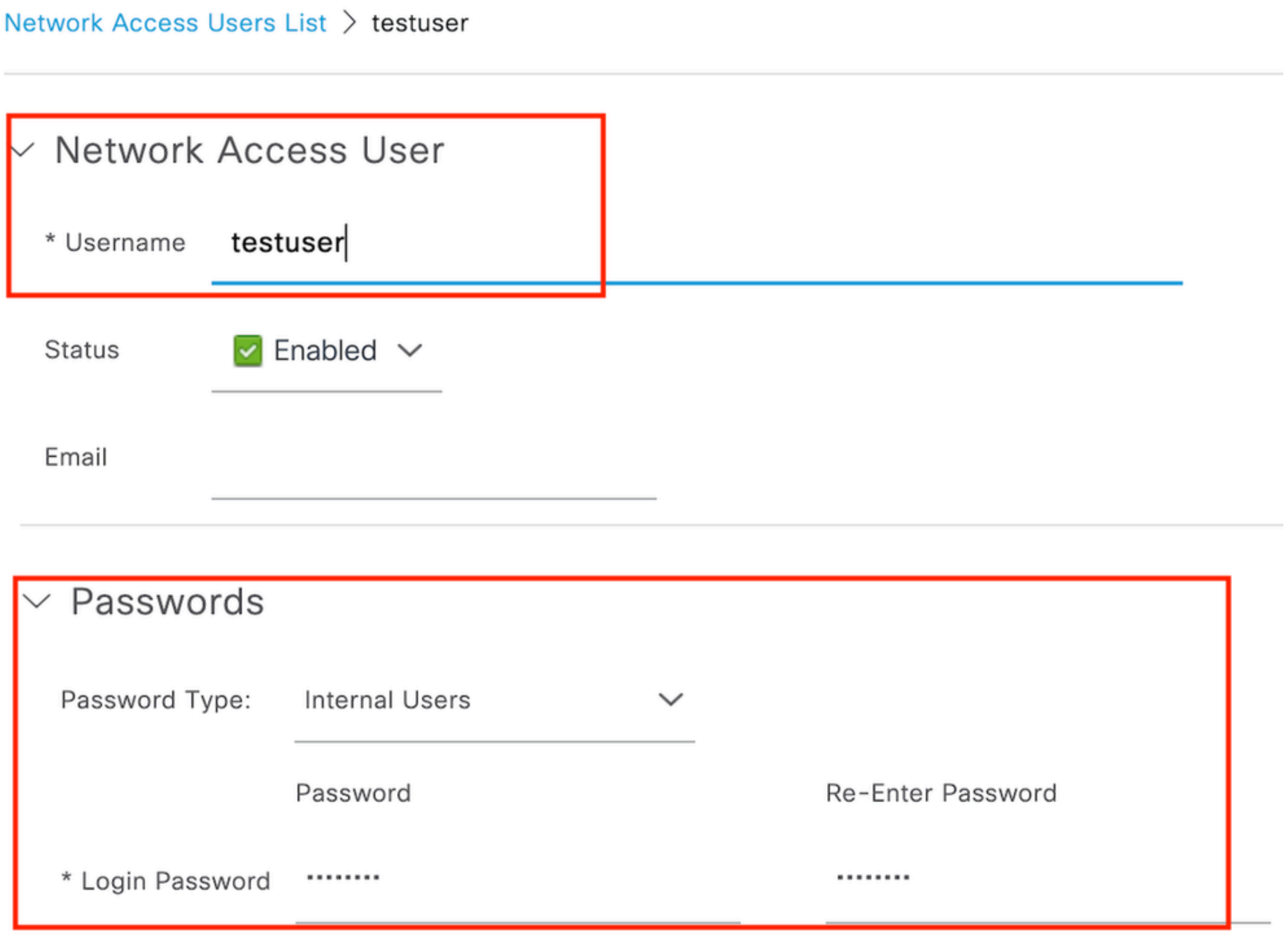
Shared Secret

Shared Secret

Step2: Create User entry

Under the Identity Management > Identities, select the Add option.

Configure the username and password which the client must use to web authentication



Network Access Users List > testuser

Network Access User

* Username testuser

Status ☑ Enabled

Email

Passwords

Password Type: Internal Users

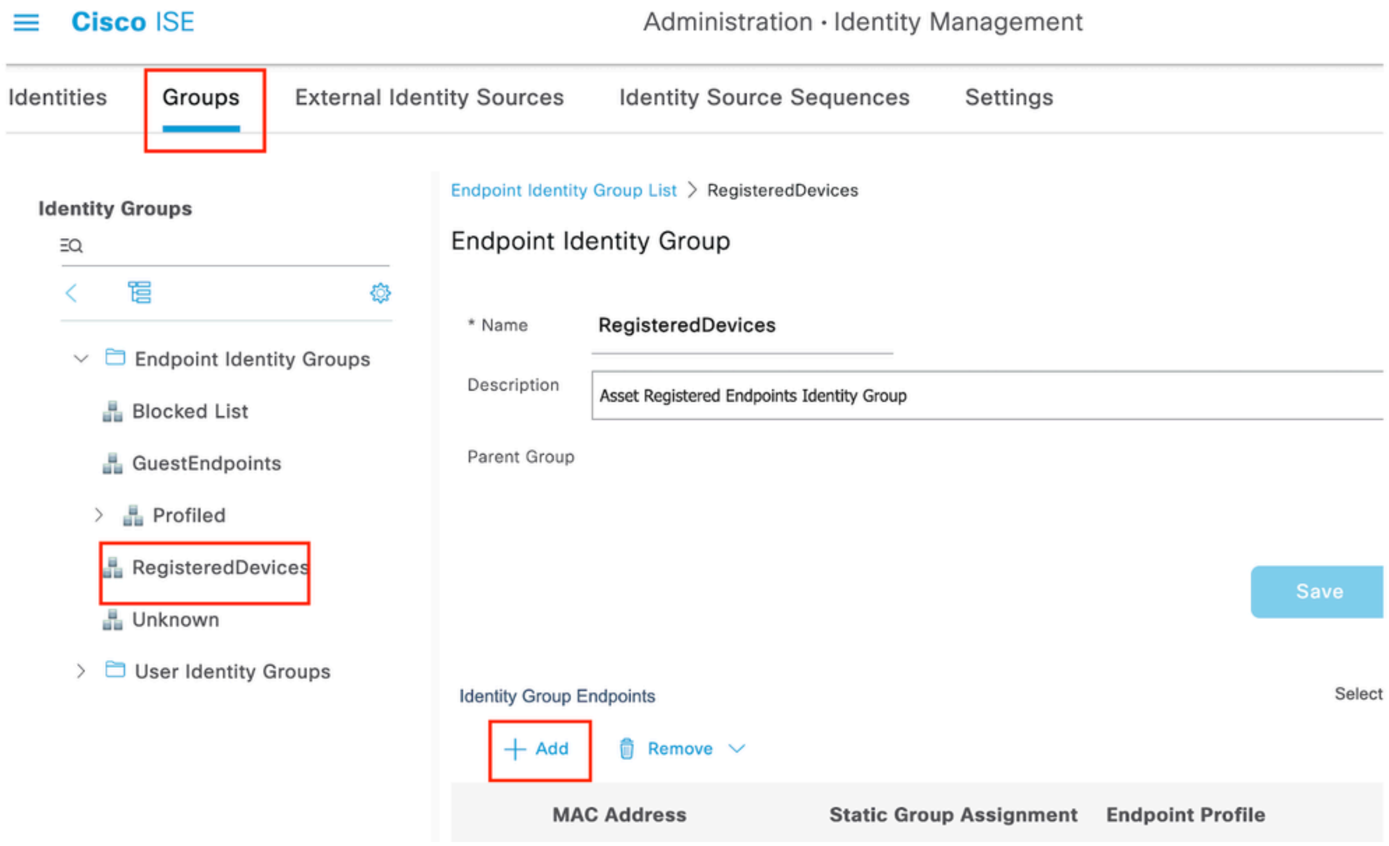
Password Re-Enter Password

* Login Password ········· ·········

Add user credentials

Step3: Navigate to Administration > Identity Management > Groups > Registered Devices and click Add.

Enter device mac address to create an entry on the server.



Endpoint Identity Group

* Name: RegisteredDevices

Description: Asset Registered Endpoints Identity Group

Parent Group

Identity Group Endpoints

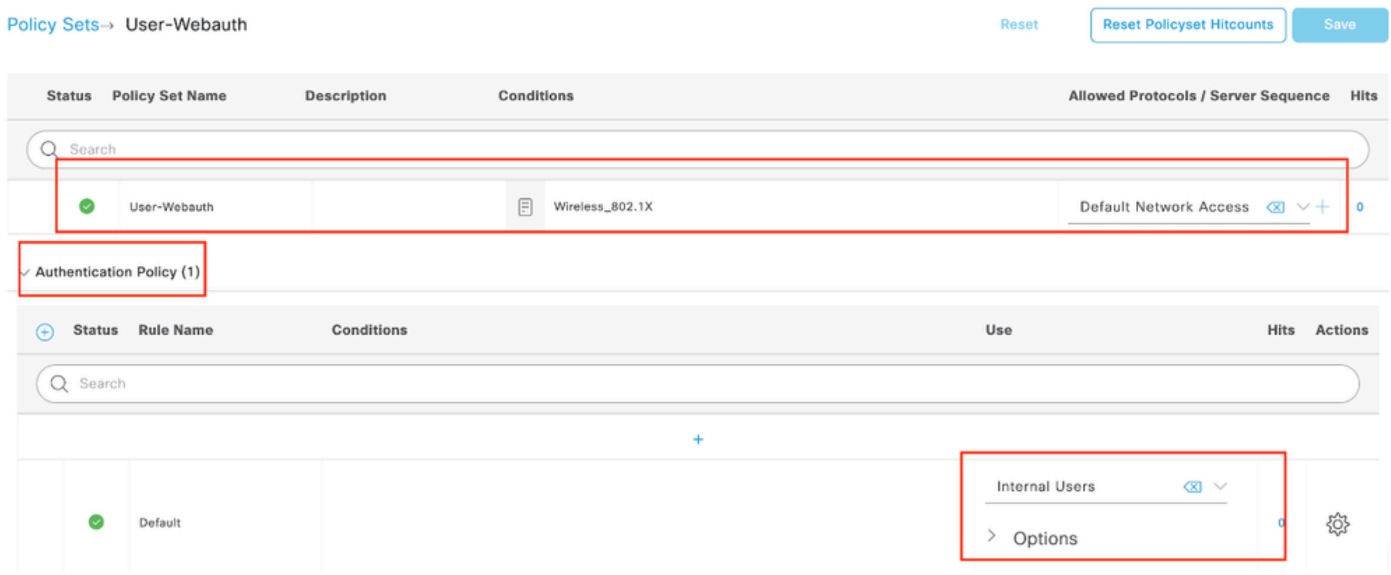
MAC Address	Static Group Assignment	Endpoint Profile

Add device mac address

Step4: Create Service Policy

Navigate to Policy > Policy sets and select “+” sign to create a new policy set

This policy set is for user web authentication, where a username and password for the client is created in Identity Management



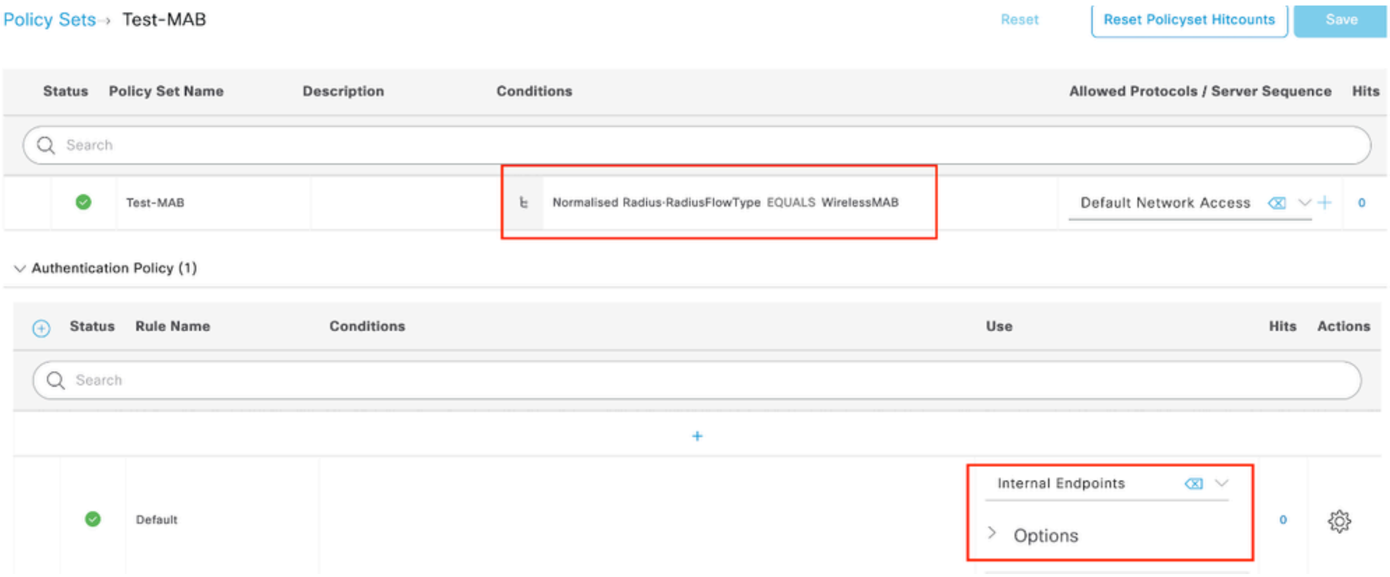
Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
✓	User-Webauth		Wireless_802.1X	Default Network Access	0

Authentication Policy (1)

Status	Rule Name	Conditions	Use	Hits	Actions
✓	Default		Internal Users	0	

Web Authentication Service policy

Similarly, create a MAB service policy and map internal endpoints under authentication policy.



Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
✓	Test-MAB		Normalised Radius·RadiusFlowType EQUALS WirelessMAB	Default Network Access	0

Authentication Policy (1)

Status	Rule Name	Conditions	Use	Hits	Actions
✓	Default		Internal Endpoints	0	⚙

MAB Authentication service policy

Verify

Controller configuration

<#root>

```
show wireless tag policy detailed

default-policy-tag

Policy Tag Name : default-policy-tag
Description     : default policy-tag
Number of WLAN-POLICY maps: 1
WLAN Profile Name                  Policy Name
------------------------------------------------------------------------

Mac_Filtering_Wlan



Web-Filter-Policy
```

<#root>

```
show wireless profile policy detailed

Web-Filter-Policy


Policy Profile Name                 :

Web-Filter-Policy

Description                         :
Status                              :
```

```
ENABLED

VLAN                                :

2074

Multicast VLAN                      : 0
```

<#root>

```
show wlan name

Mac_Filtering_Wlan


WLAN Profile Name     :

Mac_Filtering_Wlan

================================================
Identifier                                     : 9
Description                                    :
Network Name (SSID)                            :

Mac_Filtering_Wlan

Status                                         :

Enabled

Broadcast SSID                                 :

Enabled

Mac Filter Authorization list name             :

network

Webauth On-mac-filter Failure              :

Enabled

    Webauth Authentication List Name           :

ISE-List

    Webauth Authorization List Name            : Disabled
    Webauth Parameter Map                      :

Web-Filter
```

<#root>

```
show parameter-map type webauth name Web-Filter
Parameter Map Name               :

Web-Filter

  Type                           :

webauth

  Auth-proxy Init State time     : 120 sec
  Webauth max-http connection    : 100
  Webauth logout-window          :

Enabled

  Webauth success-window         :

Enabled

  Consent Email                  : Disabled
  Activation Mode                : Replace
  Sleeping-Client                : Disabled
  Webauth login-auth-bypass:
```

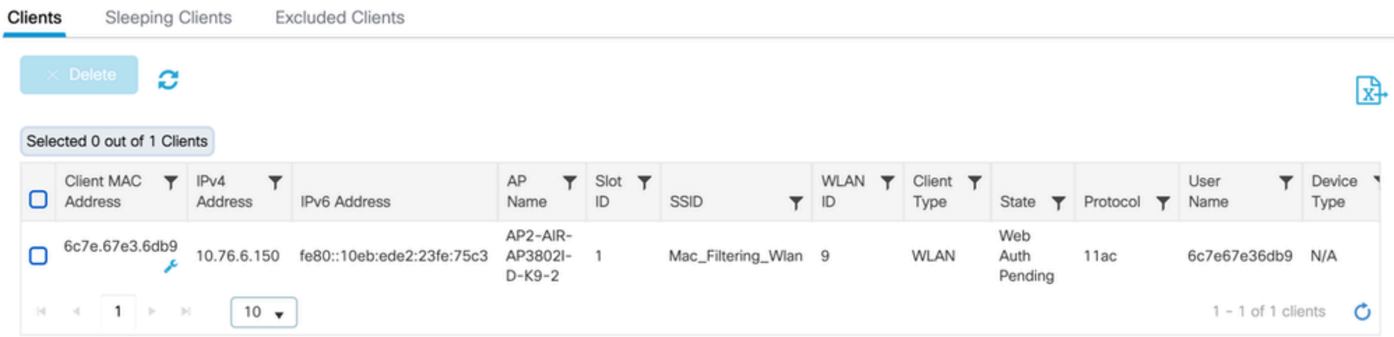
<#root>

```
show ip http server status

HTTP server status:

Enabled

HTTP server port:

80

HTTP server active supplementary listener ports: 21111
HTTP server authentication method: local
HTTP server auth-retry 0 time-window 0
HTTP server digest algorithm: md5
HTTP server access class: 0
HTTP server IPv4 access class: None
HTTP server IPv6 access class: None
HTTP server base path:
HTTP File Upload status: Disabled
HTTP server upload path:
HTTP server help root:
Maximum number of concurrent server connections allowed: 300
Maximum number of secondary server connections allowed: 50
Server idle time-out: 180 seconds
Server life time-out: 180 seconds
Server session idle time-out: 600 seconds
Maximum number of requests allowed on a connection: 25
Server linger time : 60 seconds
HTTP server active session modules: ALL
HTTP secure server capability: Present
HTTP secure server status:

Enabled

HTTP secure server port:

443
```

```
show ap name AP2-AIR-AP3802I-D-K9-2 tag detail

Policy tag mapping
------------------
WLAN Profile Name                Policy Name                      VLAN                             Flex
------------------------------------------------------------------------------------------------------------
Mac_Filtering_Wlan               Web-Filter-Policy                2074                             ENAB
```

Client policy state on controller

Navigate to the Dashboard > Clients section to confirm the status of connected clients.
Client is currently in Web Auth pending state



Client MAC Address	IPv4 Address	IPv6 Address	AP Name	Slot ID	SSID	WLAN ID	Client Type	State	Protocol	User Name	Device Type
6c7e.67e3.6db9	10.76.6.150	fe80::10eb:ede2:23fe:75c3	AP2-AIR-AP3802I-D-K9-2	1	Mac_Filtering_Wlan	9	WLAN	Web Auth Pending	11ac	6c7e67e36db9	N/A

Client detail

```
show wireless client summary
Number of Clients: 1
MAC Address    AP Name                                        Type ID   State             Protocol Meth
-------------------------------------------------------------------------------------------------------
6c7e.67e3.6db9 AP2-AIR-AP3802I-D-K9-2                         WLAN 9    Webauth Pending   11ac     Web
```

<#root>

```
show wireless client mac-address 6c7e.67e3.6db9 detail
Client MAC Address :

6c7e.67e3.6db9

Client MAC Type : Universally Administered Address
Client DUID: NA
Client IPv4 Address :

10.76.6.150

Client IPv6 Addresses : fe80::10eb:ede2:23fe:75c3
Client Username :

6c7e67e36db9

AP MAC Address : 1880.902b.05e0
AP Name: AP2-AIR-AP3802I-D-K9-2
AP slot : 1
Client State : Associated
Policy Profile :

Web-Filter-Policy

Flex Profile : N/A
Wireless LAN Id: 9
WLAN Profile Name:

Mac_Filtering_Wlan

Wireless LAN Network Name (SSID): Mac_Filtering_Wlan
```

```
BSSID : 1880.902b.05eb

Client ACLs : None
Mac authentication :

Failed

Policy Manager State:

Webauth Pending

Last Policy Manager State :

IP Learn Complete

Client Entry Create Time : 88 seconds
Policy Type : N/A
Encryption Cipher : None

Auth Method Status List
        Method : Web Auth
                Webauth State    :

Get Redirect

                Webauth Method   :

Webauth
```

After successful Web-Authentication, client policy manager state transitions to RUN

<#root>

```
show wireless client mac-address 6c7e.67e3.6db9 detail

Client ACLs : None
Mac authentication : Failed
Policy Manager State:

Run

Last Policy Manager State :

Webauth Pending

Client Entry Create Time : 131 seconds
Policy Type : N/A
```

Troubleshoot

The functionality of the Web Auth on MAC Failure feature relies on the controller capability to trigger web authentication upon MAB failure. Our primary aim is to gather RA traces efficiently from the controller for troubleshooting and analysis.

Collecting Radioactive trace

Activate Radio Active Tracing to generate client debug traces for the specified MAC address in the CLI.

Steps to enable Radioactive Tracing:

Ensure all the conditional debugs are disabled

```
clear platform condition all
```

Enable debug for specified mac address

```
debug wireless mac <H.H.H> monitor-time <Time is seconds>
```

After reproducing the issue, disable debugging to halt the RA trace collection.

```
no debug wireless mac <H.H.H>
```

Once the RA trace is stopped, the debug file is generated in the controller bootflash.

```
show bootflash: | include ra_trace
2728        179 Jul 17 2024 15:13:54.0000000000 +00:00 ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_Day
```

Copy the file to an external server.

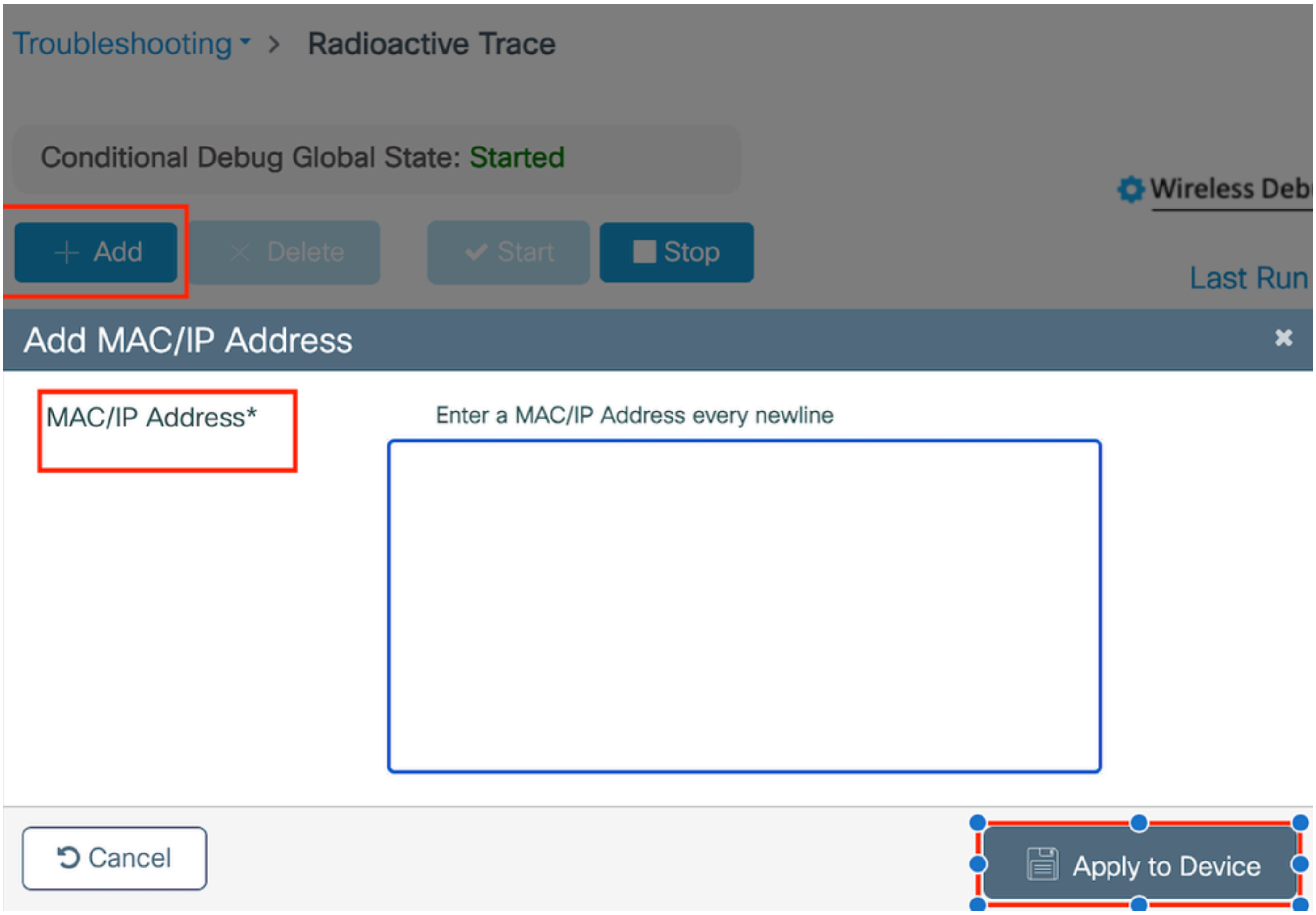
```
copy bootflash:ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log tftp://<IP addre
```

Display the debug log:

```
more bootflash:ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log
```

Enable RA trace in GUI,

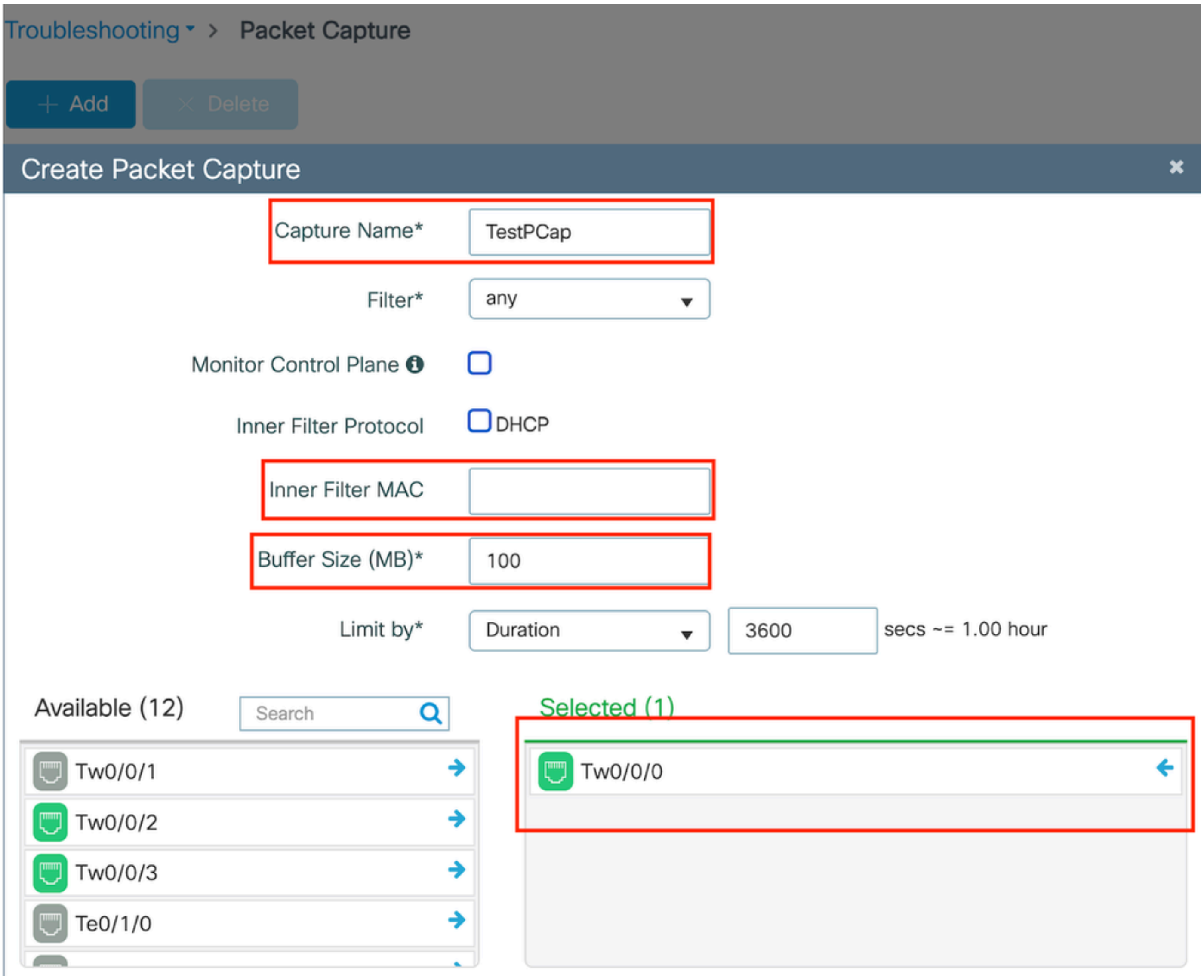
Step1: Navigate to Troubleshooting > Radioactive Trace. Select the option to add a new entry, then enter the client MAC address in the designated Add MAC/IP Address tab.


Troubleshooting > Radioactive Trace
Conditional Debug Global State: Started
Wireless Deb
+ Add
× Delete
✔ Start
Stop
Last Run
Add MAC/IP Address
MAC/IP Address*
Enter a MAC/IP Address every newline
Cancel
Apply to Device

Radioactive trace

Embedded Packet Captures:

Navigate to Troubleshooting > Packet Capture. Enter the capture name and specify the client MAC address as the inner filter MAC. Set the buffer size to 100 and choose the uplink interface to monitor incoming and outgoing packets.



Create Packet Capture

Capture Name* TestPCap

Filter* any ▾

Monitor Control Plane ℹ □

Inner Filter Protocol □ DHCP

Inner Filter MAC

Buffer Size (MB)* 100

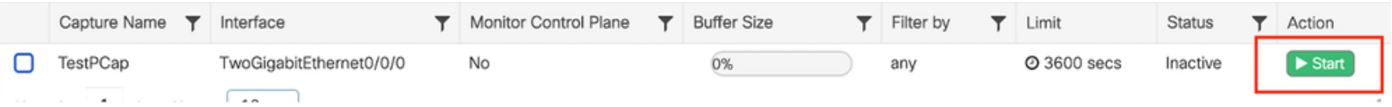
Limit by* Duration ▾ 3600 secs ~= 1.00 hour

Available (12)	Selected (1)
Tw0/0/1 →	Tw0/0/0 ←
Tw0/0/2 →	
Tw0/0/3 →	
Te0/1/0 →	

Embedded packet capture

Note: Select the "Monitor Control Traffic" option to view traffic redirected to the system CPU and reinjected into the data plane.

Select Start to capture packets



	Capture Name	Interface	Monitor Control Plane	Buffer Size	Filter by	Limit	Status	Action
□	TestPCap	TwoGigabitEthernet0/0/0	No	0%	any	3600 secs	Inactive	▶ Start

Start capture

CLI configuration

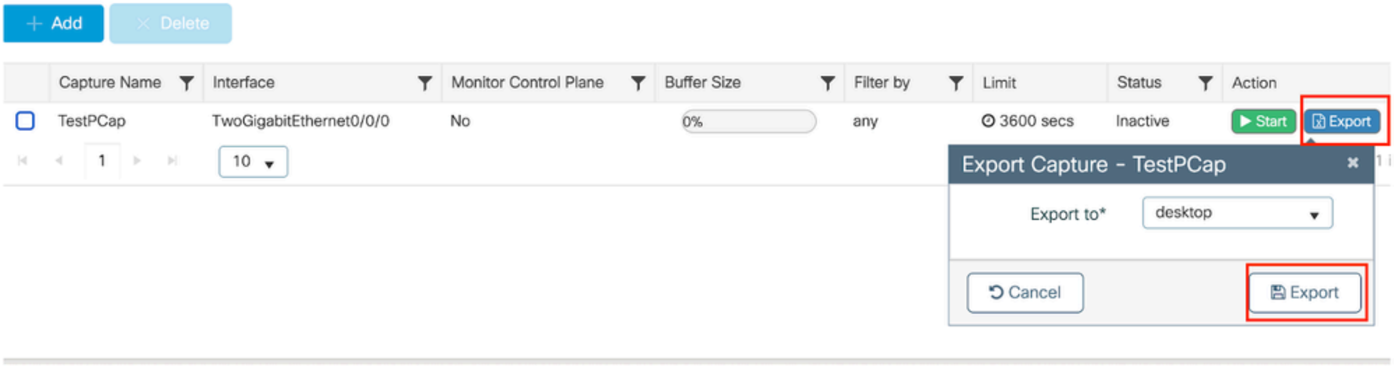
```
monitor capture TestPCap inner mac <H.H.H>
monitor capture TestPCap buffer size 100
monitor capture TestPCap interface twoGigabitEthernet 0/0/0 both
monitor capture TestPCap start

<Reporduce the issue>
```

```
monitor capture TestPCap stop
```

```
show monitor capture TestPCap

Status Information for Capture TestPCap
  Target Type:
 Interface: TwoGigabitEthernet0/0/0, Direction: BOTH
  Status : Inactive
  Filter Details:
  Capture all packets
  Inner Filter Details:
  Mac: 6c7e.67e3.6db9
  Continuous capture: disabled
  Buffer Details:
  Buffer Type: LINEAR (default)
  Buffer Size (in MB): 100
  Limit Details:
  Number of Packets to capture: 0 (no limit)
  Packet Capture duration: 3600
  Packet Size to capture: 0 (no limit)
  Maximum number of packets to capture per second: 1000
  Packet sampling rate: 0 (no sampling)
```

Export packet capture to external TFTP server

```
monitor capture TestPCap export tftp://<IP address>/ TestPCap.pcap
```



Capture Name	Interface	Monitor Control Plane	Buffer Size	Filter by	Limit	Status	Action
TestPCap	TwoGigabitEthernet0/0/0	No	0%	any	3600 secs	Inactive	▶ Start Export

Export Capture - TestPCap

Export to*: desktop

Export packet capture

Example scenario during successful MAC authentication, a client device connects to the network, its MAC address is validated by the RADIUS server through configured policies, and upon verification, access is granted by the network access device, allowing network connectivity.

Once client associates, controller sends a Access-Request to ISE server,

User name is the mac address of the client as this is MAB authentication

```
2024/07/16 21:12:52.711298748 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS: Send Access-Request t
2024/07/16 21:12:52.711310730 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS:  authenticator 19 c6
2024/07/16 21:12:52.711326401 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS:  User-Name
2024/07/16 21:12:52.711329615 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS:  User-Password
2024/07/16 21:12:52.711337331 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS:  Service-Type
2024/07/16 21:12:52.711340443 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS:  Vendor, Cisco
2024/07/16 21:12:52.711344513 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS:   Cisco AVpair
2024/07/16 21:12:52.711349087 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS:  Framed-MTU
2024/07/16 21:12:52.711351935 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS:  Message-Authenticato
2024/07/16 21:12:52.711377387 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS:  EAP-Key-Name
2024/07/16 21:12:52.711382613 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS:  Vendor, Cisco
2024/07/16 21:12:52.711385989 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS:   Cisco AVpair
```

ISE sends Access-Accept as we have a valid user entry

```
2024/07/16 21:12:52.779147404 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS: Received from id 1812
2024/07/16 21:12:52.779156117 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS:  authenticator 5d dc
2024/07/16 21:12:52.779161793 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS:  User-Name
2024/07/16 21:12:52.779165183 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS:  Class
2024/07/16 21:12:52.779219803 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS:  Message-Authenticato
```

```
2024/07/16 21:12:52.779417578 {wncd_x_R0-0}{1}: [mab] [17765]: (info): [6c7e.67b7.2d29:capwap_90000005]
2024/07/16 21:12:52.779436247 {wncd_x_R0-0}{1}: [mab] [17765]: (info): [6c7e.67b7.2d29:capwap_90000005]
```

Client policy state transistioned to Mac Auth completed

```
2024/07/16 21:12:52.780181486 {wncd_x_R0-0}{1}: [client-auth] [17765]: (info): MAC: 6c7e.67b7.2d29  Cli
2024/07/16 21:12:52.780238297 {wncd_x_R0-0}{1}: [client-orch-sm] [17765]: (debug): MAC: 6c7e.67b7.2d29
```

Client is in IP learn state after successful MAB authentication

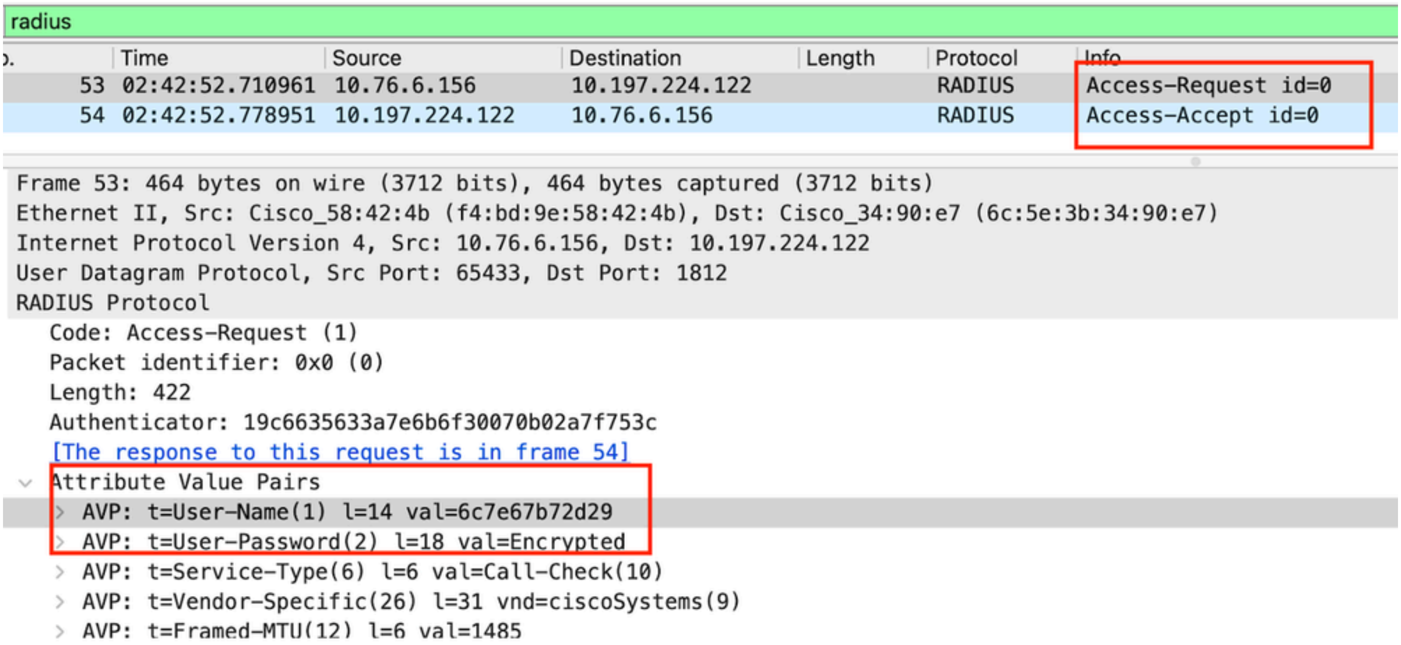
```
2024/07/16 21:12:55.791404789 {wncd_x_R0-0}{1}: [client-orch-state] [17765]: (note): MAC: 6c7e.67b7.2d2
2024/07/16 21:12:55.791739386 {wncd_x_R0-0}{1}: [client-iplearn] [17765]: (info): MAC: 6c7e.67b7.2d29
```

```
2024/07/16 21:12:55.794130301 {iosrp_R0-0}{1}: [buginf] [4440]: (debug): AUTH-FEAT-SISF-EVENT: IP updat
```

Client policy manager state updated to RUN, Web Authentication is skipped for the client which completes MAB authentication

```
2024/07/16 21:13:11.210786952 {wncd_x_R0-0}{1}: [errmsg] [17765]: (info): %CLIENT_ORCH_LOG-6-CLIENT_ADD
```

Verification using Embedded Packet Capture



```
radius
).      Time             Source          Destination     Length  Protocol  Info
    53  02:42:52.710961  10.76.6.156     10.197.224.122          RADIUS    Access-Request id=0
    54  02:42:52.778951  10.197.224.122  10.76.6.156             RADIUS    Access-Accept id=0

Frame 53: 464 bytes on wire (3712 bits), 464 bytes captured (3712 bits)
Ethernet II, Src: Cisco_58:42:4b (f4:bd:9e:58:42:4b), Dst: Cisco_34:90:e7 (6c:5e:3b:34:90:e7)
Internet Protocol Version 4, Src: 10.76.6.156, Dst: 10.197.224.122
User Datagram Protocol, Src Port: 65433, Dst Port: 1812
RADIUS Protocol
    Code: Access-Request (1)
    Packet identifier: 0x0 (0)
    Length: 422
    Authenticator: 19c6635633a7e6b6f30070b02a7f753c
    [The response to this request is in frame 54]
  ⌄ Attribute Value Pairs
    › AVP: t=User-Name(1) l=14 val=6c7e67b72d29
    › AVP: t=User-Password(2) l=18 val=Encrypted
    › AVP: t=Service-Type(6) l=6 val=Call-Check(10)
    › AVP: t=Vendor-Specific(26) l=31 vnd=ciscoSystems(9)
    › AVP: t=Framed-MTU(12) l=6 val=1485
```

Radius Packet

Example where MAC authentication failure for a client device

Mac Authentication initaited for a client after successful association

```
2024/07/17 03:20:59.842211775 {wncd_x_R0-0}{1}: [mab] [17765]: (info): [6c7e.67e3.6db9:capwap_90000005]
2024/07/17 03:20:59.842280253 {wncd_x_R0-0}{1}: [ewlc-infra-evq] [17765]: (note): Authentication Succes
2024/07/17 03:20:59.842284313 {wncd_x_R0-0}{1}: [client-auth] [17765]: (info): MAC: 6c7e.67e3.6db9  Cli
2024/07/17 03:20:59.842320572 {wncd_x_R0-0}{1}: [mab] [17765]: (info): [6c7e.67e3.6db9:capwap_90000005]
```

ISE would send Access-Reject as this device entry is not present in ISE

```
2024/07/17 03:20:59.842678322 {wncd_x_R0-0}{1}: [mab] [17765]: (info): [6c7e.67e3.6db9:capwap_90000005]
2024/07/17 03:20:59.842877636 {wncd_x_R0-0}{1}: [auth-mgr] [17765]: (info): [6c7e.67e3.6db9:capwap_9000
```

Web-Auth initiated for client device as MAB failed

```
2024/07/17 03:20:59.843728206 {wncd_x_R0-0}{1}: [client-auth] [17765]: (info): MAC: 6c7e.67e3.6db9  Cli
```

Once the Client initiates a HTTP GET request, Redirect URL is pushed to the client device as the corresponding TCP session is spoofed by the controller.

```
2024/07/17 03:21:37.817434046 {wncd_x_R0-0}{1}: [webauth-httpd] [17765]: (info): capwap_90000005[6c7e.6
```

```
2024/07/17 03:21:37.817459639 {wncd_x_R0-0}{1}: [webauth-httpd] [17765]: (debug): capwap_90000005[6c7e.
2024/07/17 03:21:37.817466483 {wncd_x_R0-0}{1}: [webauth-httpd] [17765]: (debug): capwap_90000005[6c7e.
2024/07/17 03:21:37.817482231 {wncd_x_R0-0}{1}: [webauth-state] [17765]: (info): capwap_90000005[6c7e.6
```

Client initiates a HTTP Get to the redirect URL and once the page loads the login credentials is submitted.

The controller sends a Access Request to ISE

This is a web autnentication as a valid user name is observed in Access-Accept packet

```
2024/07/17 03:22:51.132347799 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS: Send Access-Request t
2024/07/17 03:22:51.132362949 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS:  authenticator fd 40
2024/07/17 03:22:51.132368737 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS:  Calling-Station-Id
2024/07/17 03:22:51.132372791 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS:  User-Name
2024/07/17 03:22:51.132376569 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS:  Vendor, Cisco
```

Access-Accept received from ISE

```
2024/07/17 03:22:51.187040709 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS: Received from id 1812
2024/07/17 03:22:51.187050061 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS:  authenticator d3 ac
2024/07/17 03:22:51.187055731 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS:  User-Name
2024/07/17 03:22:51.187059053 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS:  Class
2024/07/17 03:22:51.187102553 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS:  Message-Authenticato
```

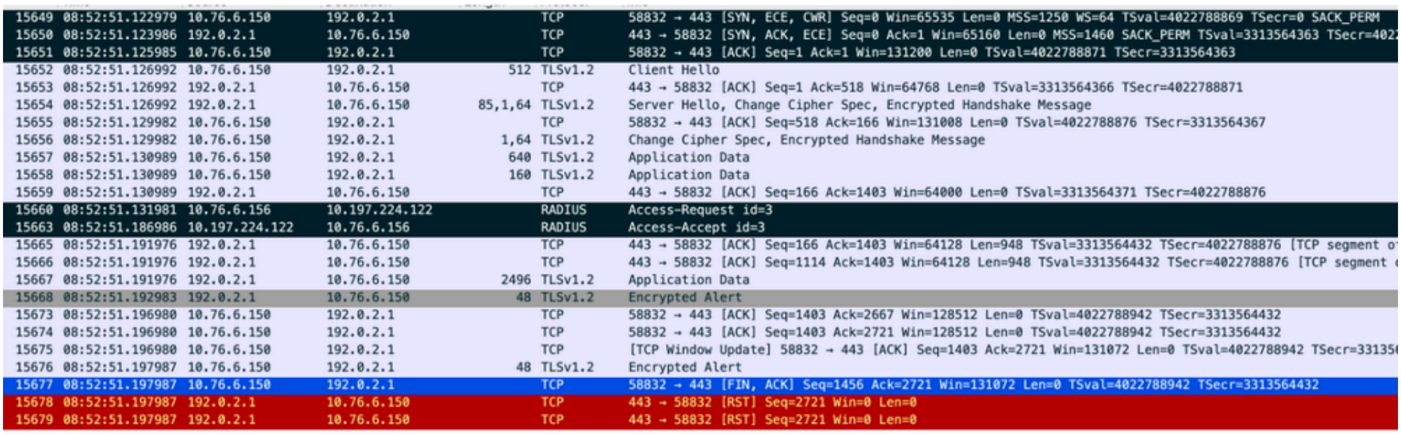
Web Authentication is successful and client state transistion to RUN state

```
2024/07/17 03:22:51.193775717 {wncd_x_R0-0}{1}: [errmsg] [17765]: (info): %CLIENT_ORCH_LOG-6-CLIENT_ADD
2024/07/17 03:22:51.194009423 {wncd_x_R0-0}{1}: [client-orch-state] [17765]: (note): MAC: 6c7e.67e3.6db
```

Verification through EPC captures

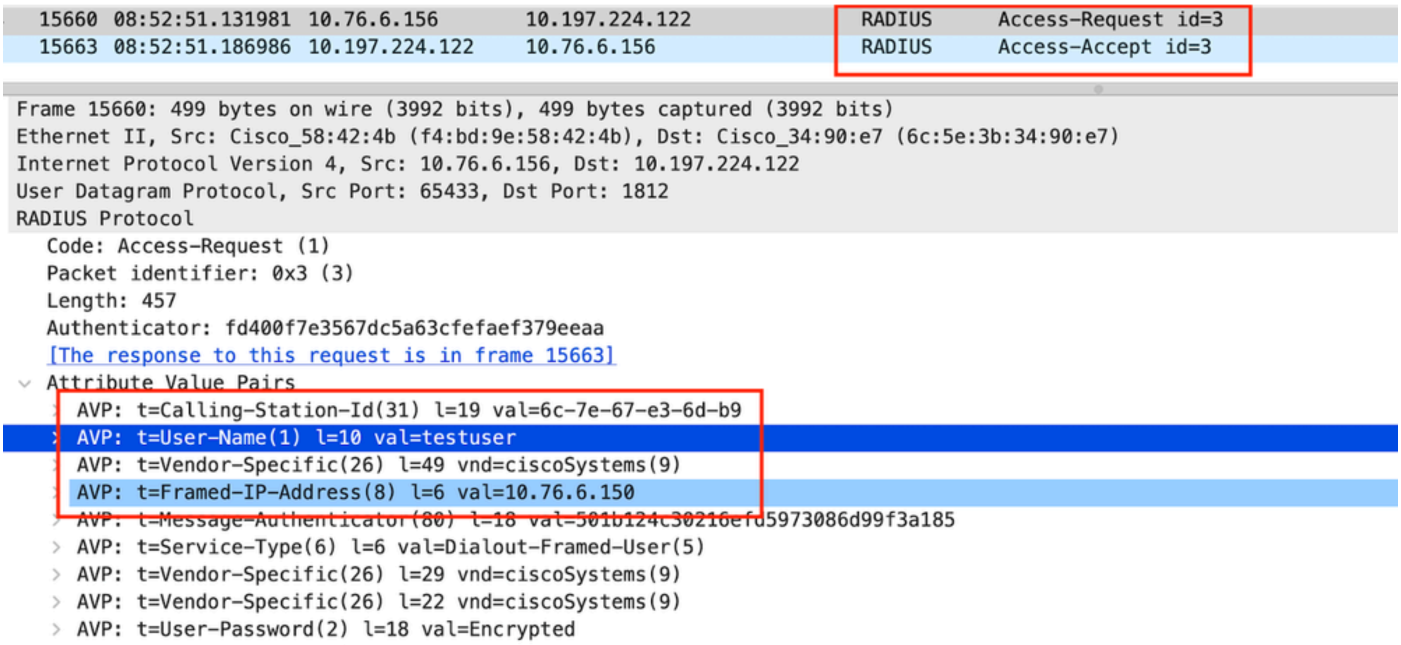
The client completes TCP handshake with the controller virtual IP address and the client loads the redirect portal page. Once the user submits username and password, we can observe a radius access-request from the controller management IP address.

After successful authentication, the client TCP session is closed and on the controller the client transitions into RUN state.



```
15649 08:52:51.122979 10.76.6.150     192.0.2.1                TCP      58832 → 443 [SYN, ECE, CWR] Seq=0 Win=65535 Len=0 MSS=1250 WS=64 TSval=4022788869 TSecr=0 SACK_PERM
15650 08:52:51.123986 192.0.2.1       10.76.6.150              TCP      443 → 58832 [SYN, ACK, ECE] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM TSval=3313564363 TSecr=402
15651 08:52:51.125985 10.76.6.150     192.0.2.1                TCP      58832 → 443 [ACK] Seq=1 Ack=1 Win=131200 Len=0 TSval=4022788871 TSecr=3313564363
15652 08:52:51.126992 10.76.6.150     192.0.2.1            512 TLSv1.2  Client Hello
15653 08:52:51.126992 192.0.2.1       10.76.6.150              TCP      443 → 58832 [ACK] Seq=1 Ack=518 Win=64768 Len=0 TSval=3313564366 TSecr=4022788871
15654 08:52:51.126992 192.0.2.1       10.76.6.150      85,1,64 TLSv1.2  Server Hello, Change Cipher Spec, Encrypted Handshake Message
15655 08:52:51.129982 10.76.6.150     192.0.2.1                TCP      58832 → 443 [ACK] Seq=518 Ack=166 Win=131008 Len=0 TSval=4022788876 TSecr=3313564367
15656 08:52:51.129982 10.76.6.150     192.0.2.1           1,64 TLSv1.2  Change Cipher Spec, Encrypted Handshake Message
15657 08:52:51.130989 10.76.6.150     192.0.2.1            640 TLSv1.2  Application Data
15658 08:52:51.130989 10.76.6.150     192.0.2.1            160 TLSv1.2  Application Data
15659 08:52:51.130989 192.0.2.1       10.76.6.150              TCP      443 → 58832 [ACK] Seq=166 Ack=1403 Win=64000 Len=0 TSval=3313564371 TSecr=4022788876
15660 08:52:51.131981 10.76.6.156     10.197.224.122           RADIUS   Access-Request id=3
15663 08:52:51.186986 10.197.224.122  10.76.6.156              RADIUS   Access-Accept id=3
15665 08:52:51.191976 192.0.2.1       10.76.6.150              TCP      443 → 58832 [ACK] Seq=166 Ack=1403 Win=64128 Len=948 TSval=3313564432 TSecr=4022788876 [TCP segment o
15666 08:52:51.191976 192.0.2.1       10.76.6.150              TCP      443 → 58832 [ACK] Seq=1114 Ack=1403 Win=64128 Len=948 TSval=3313564432 TSecr=4022788876 [TCP segment
15667 08:52:51.191976 192.0.2.1       10.76.6.150         2496 TLSv1.2  Application Data
15668 08:52:51.192983 192.0.2.1       10.76.6.150           48 TLSv1.2  Encrypted Alert
15673 08:52:51.196980 10.76.6.150     192.0.2.1                TCP      58832 → 443 [ACK] Seq=1403 Ack=2667 Win=128512 Len=0 TSval=4022788942 TSecr=3313564432
15674 08:52:51.196980 10.76.6.150     192.0.2.1                TCP      58832 → 443 [ACK] Seq=1403 Ack=2721 Win=128512 Len=0 TSval=4022788942 TSecr=3313564432
15675 08:52:51.196980 10.76.6.150     192.0.2.1                TCP      [TCP Window Update] 58832 → 443 [ACK] Seq=1403 Ack=2721 Win=131072 Len=0 TSval=4022788942 TSecr=33135
15676 08:52:51.197987 10.76.6.150     192.0.2.1             48 TLSv1.2  Encrypted Alert
15677 08:52:51.197987 10.76.6.150     192.0.2.1                TCP      58832 → 443 [FIN, ACK] Seq=1456 Ack=2721 Win=131072 Len=0 TSval=4022788942 TSecr=3313564432
15678 08:52:51.197987 192.0.2.1       10.76.6.150              TCP      443 → 58832 [RST] Seq=2721 Win=0 Len=0
15679 08:52:51.197987 192.0.2.1       10.76.6.150              TCP      443 → 58832 [RST] Seq=2721 Win=0 Len=0
```

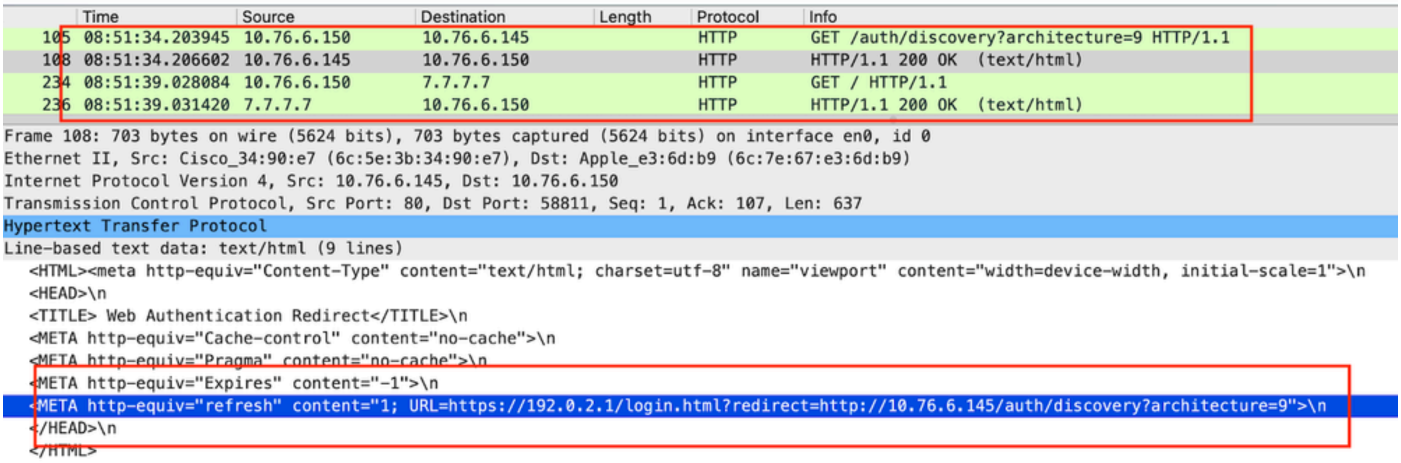
TCP flow with radius packet



```
 15660  08:52:51.131981  10.76.6.156      10.197.224.122     RADIUS    Access-Request id=3
 15663  08:52:51.186986  10.197.224.122   10.76.6.156        RADIUS    Access-Accept id=3

Frame 15660: 499 bytes on wire (3992 bits), 499 bytes captured (3992 bits)
Ethernet II, Src: Cisco_58:42:4b (f4:bd:9e:58:42:4b), Dst: Cisco_34:90:e7 (6c:5e:3b:34:90:e7)
Internet Protocol Version 4, Src: 10.76.6.156, Dst: 10.197.224.122
User Datagram Protocol, Src Port: 65433, Dst Port: 1812
RADIUS Protocol
    Code: Access-Request (1)
    Packet identifier: 0x3 (3)
    Length: 457
    Authenticator: fd400f7e3567dc5a63cfefaef379eeaa
    [The response to this request is in frame 15663]
  ⌄ Attribute Value Pairs
    › AVP: t=Calling-Station-Id(31) l=19 val=6c-7e-67-e3-6d-b9
    › AVP: t=User-Name(1) l=10 val=testuser
    › AVP: t=Vendor-Specific(26) l=49 vnd=ciscoSystems(9)
    › AVP: t=Framed-IP-Address(8) l=6 val=10.76.6.150
    › AVP: t=Message-Authenticator(80) l=18 val=501b124c30216efd5973086d99f3a185
    › AVP: t=Service-Type(6) l=6 val=Dialout-Framed-User(5)
    › AVP: t=Vendor-Specific(26) l=29 vnd=ciscoSystems(9)
    › AVP: t=Vendor-Specific(26) l=22 vnd=ciscoSystems(9)
    › AVP: t=User-Password(2) l=18 val=Encrypted
```

Radius packet sent to ISE with user credentials

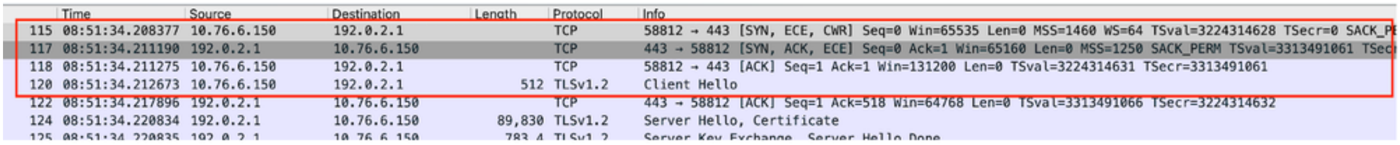
Client-side wireshark capture to validate the client traffic is getting redirected to the portal page and validate the TCP handshake to controller virtual ip address/ web server



```
      Time             Source         Destination     Length   Protocol   Info
  105 08:51:34.203945  10.76.6.150    10.76.6.145              HTTP       GET /auth/discovery?architecture=9 HTTP/1.1
  108 08:51:34.206602  10.76.6.145    10.76.6.150              HTTP       HTTP/1.1 200 OK  (text/html)
  234 08:51:39.028084  10.76.6.150    7.7.7.7                  HTTP       GET / HTTP/1.1
  236 08:51:39.031420  7.7.7.7        10.76.6.150              HTTP       HTTP/1.1 200 OK  (text/html)
Frame 108: 703 bytes on wire (5624 bits), 703 bytes captured (5624 bits) on interface en0, id 0
Ethernet II, Src: Cisco_34:90:e7 (6c:5e:3b:34:90:e7), Dst: Apple_e3:6d:b9 (6c:7e:67:e3:6d:b9)
Internet Protocol Version 4, Src: 10.76.6.145, Dst: 10.76.6.150
Transmission Control Protocol, Src Port: 80, Dst Port: 58811, Seq: 1, Ack: 107, Len: 637
Hypertext Transfer Protocol
Line-based text data: text/html (9 lines)
    <HTML><meta http-equiv="Content-Type" content="text/html; charset=utf-8" name="viewport" content="width=device-width, initial-scale=1">\n
    <HEAD>\n
    <TITLE> Web Authentication Redirect</TITLE>\n
    <META http-equiv="Cache-control" content="no-cache">\n
    <META http-equiv="Pragma" content="no-cache">\n
    <META http-equiv="Expires" content="-1">\n
    <META http-equiv="refresh" content="1; URL=https://192.0.2.1/login.html?redirect=http://10.76.6.145/auth/discovery?architecture=9">\n
    </HEAD>\n
    </HTML>
```

Client side capture to validate the redirect url

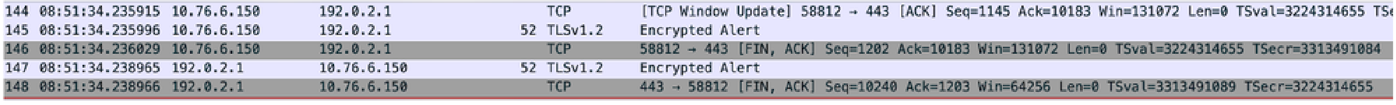
Client establishes TCP handshake to the virtual IP address of the controller



```
     Time             Source         Destination     Length  Protocol  Info
115  08:51:34.208377  10.76.6.150    192.0.2.1               TCP       58812 → 443 [SYN, ECE, CWR] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=3224314628 TSecr=0 SACK_PE
117  08:51:34.211190  192.0.2.1      10.76.6.150             TCP       443 → 58812 [SYN, ACK, ECE] Seq=0 Ack=1 Win=65160 Len=0 MSS=1250 SACK_PERM TSval=3313491061 TSecr
118  08:51:34.211275  10.76.6.150    192.0.2.1               TCP       58812 → 443 [ACK] Seq=1 Ack=1 Win=131200 Len=0 TSval=3224314631 TSecr=3313491061
120  08:51:34.212673  10.76.6.150    192.0.2.1           512 TLSv1.2   Client Hello
122  08:51:34.217896  192.0.2.1      10.76.6.150             TCP       443 → 58812 [ACK] Seq=1 Ack=518 Win=64768 Len=0 TSval=3313491066 TSecr=3224314632
124  08:51:34.220834  192.0.2.1      10.76.6.150      89,830 TLSv1.2   Server Hello, Certificate
125  08:51:34.220835  192.0.2.1      10.76.6.150       783,4 TLSv1.2   Server Key Exchange, Server Hello Done
```

TCP handshake between the client and webserver

Session is closed after successful web authentication,



```
144  08:51:34.235915  10.76.6.150        192.0.2.1                 TCP      [TCP Window Update] 58812 → 443 [ACK] Seq=1145 Ack=10183 Win=131072 Len=0 TSval=3224314655 TSe
145  08:51:34.235996  10.76.6.150        192.0.2.1              52 TLSv1.2  Encrypted Alert
146  08:51:34.236029  10.76.6.150        192.0.2.1                 TCP      58812 → 443 [FIN, ACK] Seq=1202 Ack=10183 Win=131072 Len=0 TSval=3224314655 TSecr=3313491084
147  08:51:34.238965  192.0.2.1          10.76.6.150            52 TLSv1.2  Encrypted Alert
148  08:51:34.238966  192.0.2.1          10.76.6.150               TCP      443 → 58812 [FIN, ACK] Seq=10240 Ack=1203 Win=64256 Len=0 TSval=3313491089 TSecr=3224314655
```

TCP session closed after client completes web authentication

Related Article

Understand Wireless Debugs and Log Collection on Catalyst 9800 Wireless LAN Controllers

Web based authentication on 9800

Configure local web authentication on 9800