

Configure Verify and Troubleshoot Wired Guest in Wireless LAN Controller

Contents

Introduction

This document describes how to configure, verify, and troubleshoot wired guest access in 9800 and IRCM with external web authentication.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

9800 WLC

AireOS WLC

Mobility Tunnel

ISE

It is assumed that a mobility tunnel between the two WLCs has been established prior to configuring wired guest access.

This aspect is outside the scope of this configuration example. For detailed instructions, please refer to the attached document titled [Configuring Mobility Topologies on 9800](#)

Components Used

9800 WLC version 17.12.1

5520 WLC version 8.10.185.0

ISE 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.

Configure Wired Guest on catalyst 9800 anchored to another catalyst 9800

Network Diagram



Network Topology

Configuration on Foreign 9800 WLC

Configure Web Parameter map

Step1: Navigate to **Configuration > Security > Web Auth**, select **Global**, verify the virtual IP address of the controller and Trustpoint mapping, and ensure the type is set to webauth.

Configuration > Security > Web Auth

Edit Web Auth Parameter

General Advanced

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	xxxxxx
Captive Bypass Portal	<input type="checkbox"/>	Web Auth intercept HTTPs	<input checked="" type="checkbox"/>
Disable Success Window	<input type="checkbox"/>	Enable HTTP server for Web Auth	<input checked="" type="checkbox"/>
Disable Logout Window	<input type="checkbox"/>	Disable HTTP secure server for Web Auth	<input type="checkbox"/>
Disable Cisco Logo	<input type="checkbox"/>	Banner Configuration	
Sleeping Client Status	<input type="checkbox"/>	Banner Title	
Sleeping Client Timeout (minutes)	720	Banner Type	<input checked="" type="radio"/> None <input type="radio"/> Banner Text

Global parameter map



Note: Web Auth intercept HTTPs is an optional setting. If HTTPS redirection is required, the Web Auth intercept HTTPS option must be enabled. However, this configuration is not recommended as it increases CPU usage.

Step2: Under the **Advanced** tab, configure the external web page URL for client redirection. Set "Redirect URL for Login" and "Redirect On-Failure"; "Redirect On-Success" is optional. Once configured, a preview of the redirect URL is displayed on the Web Auth profile.

i Preview of the Redirect URL:

http://10.127.196.171/webauth/login.html?switch_url=https://192.0.2.1/login.html&redirect=<website-name>

Redirect to external server

Redirect URL for login	http://10.127.196.171/w
Redirect On-Success	http://10.127.196.171/w
Redirect On-Failure	http://10.127.196.171/w
Redirect Append for AP MAC Address	<input type="text"/>
Redirect Append for Client MAC Address	<input type="text"/>
Redirect Append for WLAN SSID	<input type="text"/>
Portal IPV4 Address	10.127.196.171
Portal IPV6 Address	x::x::x::x

Advanced tab

CLI Configuration

```
parameter-map type webauth global
type webauth
virtual-ip ipv4 192.0.2.1
redirect for-login http://10.127.196.171/webauth/login.html
redirect on-success http://10.127.196.171/webauth/logout.html
redirect on-failure http://10.127.196.171/webauth/failed.html
redirect portal ipv4 10.127.196.171
intercept-https-enable
trustpoint TP-self-signed-3915430211
webauth-http-enable
```

Note: In this scenario, the global parameter map is used. As per requirement configure a custom web parameter map by selecting Add and, set the redirect URL under the Advanced tab. The Trustpoint and Virtual IP settings is inherited from the global profile.

AAA Settings:

Step1: Create a Radius Server:

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

The screenshot shows the 'Create AAA Radius Server' configuration page. The 'Servers' tab is selected and highlighted with a red box. The 'Add' button is also highlighted with a red box. The form contains the following fields and options:

- Name* (text input)
- Server Address* (text input with placeholder 'IPv4/IPv6/Hostname')
- PAC Key (checkbox, unchecked)
- Key Type (dropdown menu, 'Clear Text')
- Key* (text input)
- Confirm Key* (text input)
- Auth Port (text input, '1812')
- Acct Port (text input, '1813')
- Server Timeout (seconds) (text input, '1-1000')
- Retry Count (text input, '0-100')
- Support for CoA (toggle, 'ENABLED')
- CoA Server Key Type (dropdown menu, 'Clear Text')
- CoA Server Key (text input)
- Confirm CoA Server Key (text input)
- Automate Tester (checkbox, unchecked)

Buttons at the bottom: 'Cancel' and 'Apply to Device'.

Radius 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
```

Step 2: Create a RADIUS Server Group:

Select "Add" under the Server Groups section to define a server group and toggle the servers to be included in the group configuration.

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

[+ AAA Wizard](#)

Servers / Groups AAA Method List AAA Advanced

[+ Add](#) [× Delete](#)

RADIUS

Servers **Server Groups**

TACACS

LDAP

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

Available Servers Assigned Servers

ISE-Auth

Radius server group

CLI Configuration

```

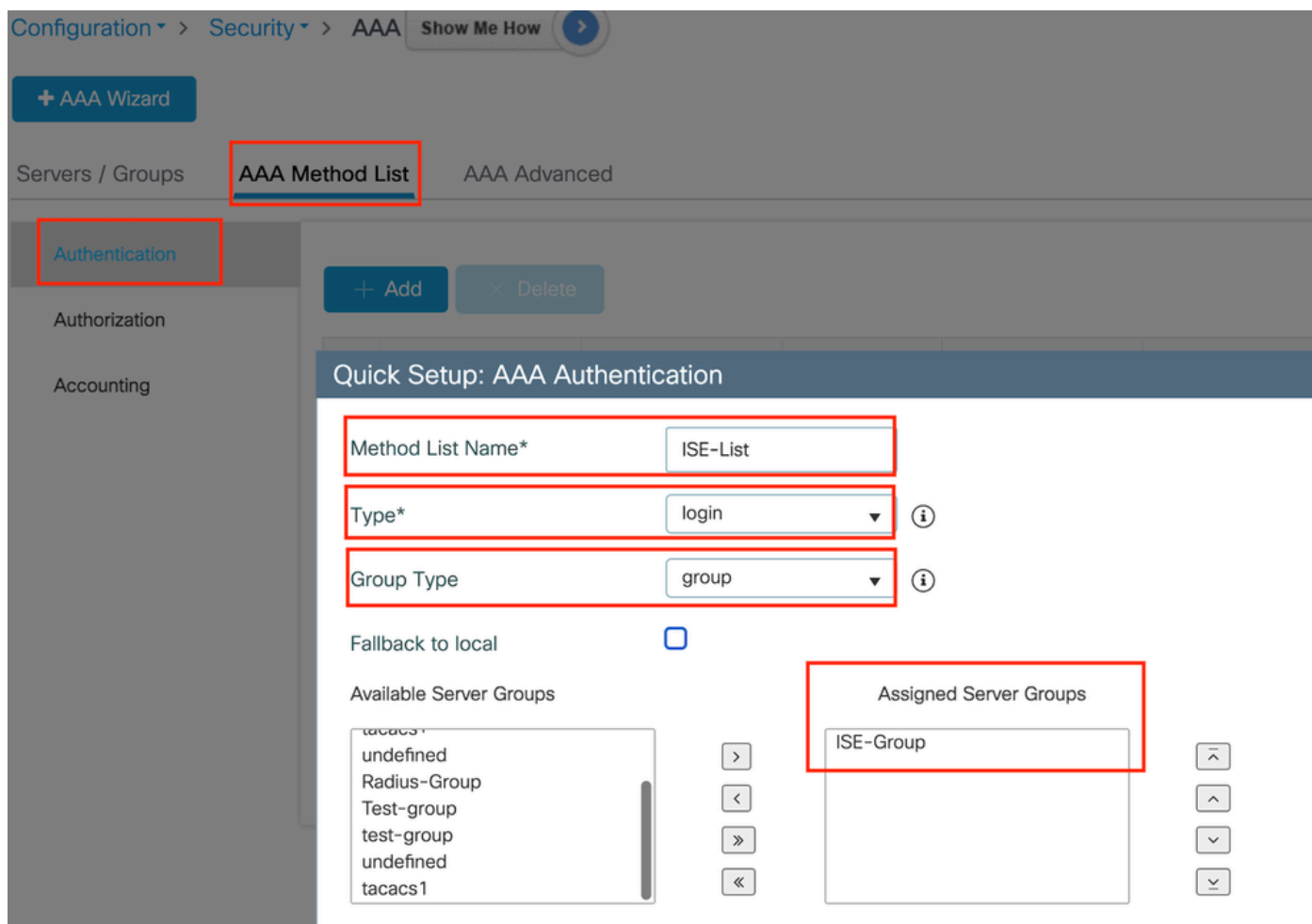
aaa group server radius ISE-Group
server name ISE-Auth
ip radius source-interface Vlan2074
deadtime 5

```

Step3: Configure AAA Method List:

Navigate to the AAA Method List tab, select Add under Authentication, define a method list name with Type as "login" and Group type as "Group," and map the configured authentication server group under the

Assigned Server Group section.



Authentication method list

CLI configuration

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

Configure Policy profile

Step1: Navigate to **Configuration > Tags & Profiles > Policy**, name your new profile in the **General** tab, and enable it using the status toggle.

+ Add

× Delete

Clone

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

General

Access Policies

QOS and AVC

Mobility

Advanced

Name*

GuestLANPolicy

Description

Enter Description

Status

ENABLED

Passive Client

DISABLED

IP MAC Binding

ENABLED

Encrypted Traffic Analytics

DISABLED

CTS Policy

Inline Tagging

SGACL Enforcement

Default SGT

2-65519

WLAN Switching Policy

Central Switching

ENABLED

Central Authentication

ENABLED

Central DHCP

ENABLED

Flex NAT/PAT

DISABLED

Policy Profile

Step2: Under the **Access Policies** tab, assign a random vlan as vlan mapping is completed on the anchor controller. In this example, vlan 1 is configured

General **Access Policies** QOS and AVC Mobility Advanced

RADIUS Profiling

HTTP TLV Caching

DHCP TLV Caching

WLAN Local Profiling

Global State of Device Classification Disabled ⓘ

Local Subscriber Policy Name ⓘ

VLAN

VLAN/VLAN Group ⓘ

Multicast VLAN

WLAN ACL

IPv4 ACL ⓘ

IPv6 ACL ⓘ

URL Filters ⓘ

Pre Auth ⓘ

Post Auth ⓘ

Access Policy tab

Step3: Under the **Mobility** tab, toggle the Anchor controller to Primary (1) and optionally configure Secondary and Tertiary mobility tunnels for redundancy requirements

General Access Policies QOS and AVC **Mobility** Advanced





Mobility Anchors

Export Anchor

Static IP Mobility DISABLED

Adding Mobility Anchors will cause the enabled WLANs to momentarily disable and may result in loss of connectivity for some clients.

Drag and Drop/double click/click on the arrow to add/remove Anchors

Available (3)	Selected (1)
Anchor IP	Anchor IP Anchor Priority
<div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;">  10.106.40.11 → </div> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;">  10.76.118.75 → </div> <div style="border: 1px solid #ccc; padding: 5px;">  10.76.118.74 → </div>	<div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;">  10.76.118.70 <input type="text" value="Primary (1)"/> ← </div>

Mobility map

CLI Configuration

```
wireless profile policy GuestLANPolicy
```

mobility anchor 10.76.118.70 priority 1
no shutdown

Configure Guest LAN profile

Step1: Navigate to **Configuration > Wireless > Guest LAN**, select **Add**, configure a unique profile name, enable Wired VLAN, enter the VLAN ID for wired guest users, and toggle the profile status to **Enabled**.

General	Security		
Profile Name*	<input type="text" value="Guest-Profile"/>	Client Association Limit	<input type="text" value="2000"/>
Guest LAN ID*	<input type="text" value="1"/>	Wired VLAN Status	<input checked="" type="checkbox"/> ENABLE
mDNS Mode	<input type="text" value="Bridging"/>	Wired VLAN ID*	<input type="text" value="2024"/>
Status	<input checked="" type="checkbox"/> ENABLE		

Guest LAN Profile

Step2: Under the Security tab, enable Web Auth, map the Web Auth parameter map, and select the Radius server from the Authentication drop-down list.

Edit Guest LAN Profile

General **Security**

Layer3

Web Auth

ENABLE

Web Auth Parameter Map

global

Authentication List

ISE-List

CLI Configuration

```
guest-lan profile-name Guest-Profile 1 wired-vlan 2024  
security web-auth authentication-list ISE-List  
security web-auth parameter-map global
```

Guest LAN MAP

Navigate to **Configuration > Wireless > Guest LAN**.

Under the **Guest LAN MAP** configuration section, select **Add** and map the Policy profile and Guest LAN profile

> Guest LAN Map Configuration

+ Add Map × Delete Map

Guest LAN Map: GuestMap

+ Add × Delete

Guest LAN Profile Name	Policy Name
No records available.	
10 items per page 0 - 0 of 0 items	

Profile Name: Guest-Profile

Policy Name: GuestLANPolicy

Save Cancel

Guest LAN MAP

CLI Configuration

```
wireless guest-lan map GuestMap  
guest-lan Guest-Profile policy GuestLANPolicy
```

Configuration on Anchor 9800 WLC

Configure Web Parameter map

Step1: Navigate to **Configuration > Security > Web Auth**, select **Global**, verify the virtual IP address of the controller and Trustpoint mapping, and ensure the type is set to webauth.

Configuration > Security > Web Auth

Edit Web Auth Parameter

General Advanced

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
Captive Bypass Portal	<input type="checkbox"/>	Web Auth intercept HTTPs	<input checked="" type="checkbox"/>
Disable Success Window	<input type="checkbox"/>	Enable HTTP server for Web Auth	<input checked="" type="checkbox"/>
Disable Logout Window	<input type="checkbox"/>	Disable HTTP secure server for Web Auth	<input type="checkbox"/>
Disable Cisco Logo	<input type="checkbox"/>	Banner Configuration	
Sleeping Client Status	<input type="checkbox"/>	Banner Title	
Sleeping Client Timeout (minutes)	720	Banner Type	<input checked="" type="radio"/> None <input type="radio"/> Banner Text

Global parameter map

Step2: Under the **Advanced** tab, configure the external web page URL for client redirection. Set "Redirect URL for Login" and "Redirect On-Failure"; "Redirect On-Success" is optional.

Once configured, a preview of the redirect URL is displayed on the Web Auth profile.

General **Advanced**

Preview of the Redirect URL:

`http://10.127.196.171/webauth/login.html?switch_url=https://192.0.2.1/login.html&redirect=<website-name>`

Redirect to external server

Redirect URL for login	http://10.127.196.171/w
Redirect On-Success	http://10.127.196.171/w
Redirect On-Failure	http://10.127.196.171/w
Redirect Append for AP MAC Address	
Redirect Append for Client MAC Address	
Redirect Append for WLAN SSID	
Portal IPV4 Address	10.127.196.171
Portal IPV6 Address	X::X::X::X

Advanced tab

CLI Configuration

```
parameter-map type webauth global
type webauth
virtual-ip ipv4 192.0.2.1
redirect for-login http://10.127.196.171/webauth/login.html
redirect on-success http://10.127.196.171/webauth/logout.html
redirect on-failure http://10.127.196.171/webauth/failed.html
redirect portal ipv4 10.127.196.171
intercept-https-enable.
trustpoint TP-self-signed-3915430211
webauth-http-enable
```

AAA Settings:

Step1: Create a Radius Server:

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

The screenshot displays the 'Create AAA Radius Server' configuration window. The 'Add' button is highlighted with a red box. The 'Name*' field is highlighted with a red box. The 'Server Address*' field is highlighted with a red box. The 'Key Type' dropdown is set to 'Clear Text'. The 'Key*' and 'Confirm Key*' fields are highlighted with a red box. The 'Support for CoA' checkbox is checked and labeled 'ENABLED'. The 'Automate Tester' checkbox is unchecked. The 'Auth Port' is set to 1812, 'Acct Port' is set to 1813, 'Server Timeout (seconds)' is set to 1-1000, and 'Retry Count' is set to 0-100. The 'Apply to Device' button is visible at the bottom right.

Radius 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
```

Step 2: Create a RADIUS Server Group:

Select **Add** under the Server Groups section to define a server group and toggle the servers to be included in the group configuration.

Name*	ISE-Group
Group Type	RADIUS
MAC-Delimiter	none
MAC-Filtering	none
Dead-Time (mins)	5
Load Balance	<input type="checkbox"/> DISABLED
Source Interface VLAN ID	2081

Available Servers



Assigned Servers

ISE-Auth

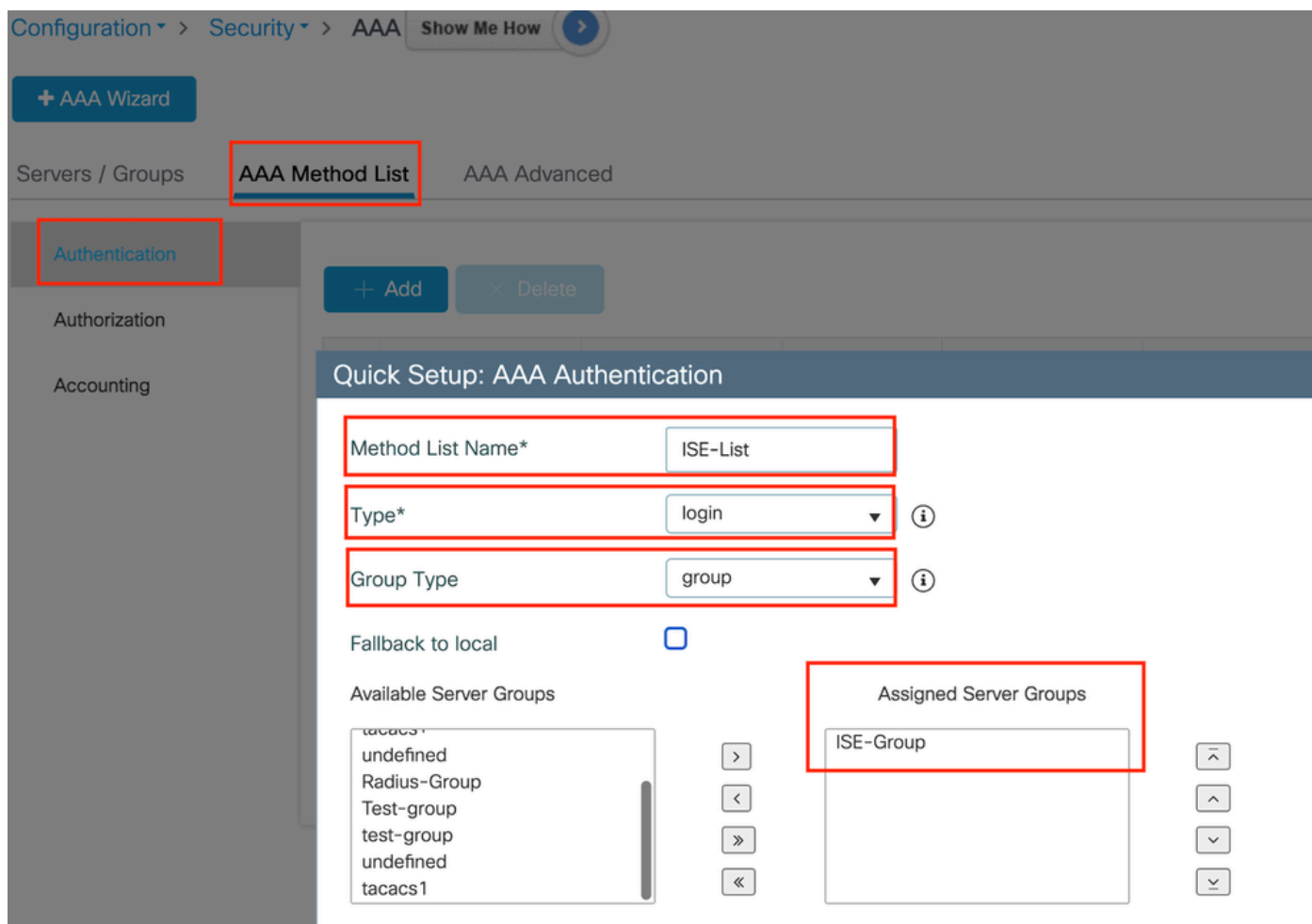
Anchor radius group

CLI Configuration

```
aaa group server radius ISE-Group
server name ISE-Auth
ip radius source-interface Vlan2081
deadtime 5
```

Step3: Configure AAA Method List:

Navigate to the **AAA Method List** tab, select **Add** under **Authentication**, define a method list name with Type as "login" and Group type as "Group," and map the configured authentication server group under the Assigned Server Group section.



Authentication method list

CLI configuration

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

Configure Policy profile

Step1: Navigate to **Configuration > Tag & Profiles > Policy**, configure the policy profile with the same name as on the foreign controller and enable the profile.

General

Access Policies

QOS and AVC

Mobility

Advanced

Name*	GuestLANPolicy
Description	Enter Description
Status	ENABLED <input checked="" type="checkbox"/>
Passive Client	<input type="checkbox"/> DISABLED
IP MAC Binding	ENABLED <input checked="" type="checkbox"/>
Encrypted Traffic Analytics	<input type="checkbox"/> DISABLED
CTS Policy	
Inline Tagging	<input type="checkbox"/>
SGACL Enforcement	<input type="checkbox"/>
Default SGT	2-65519

WLAN Switching Policy

Central Switching	ENABLED <input checked="" type="checkbox"/>
Central Authentication	ENABLED <input checked="" type="checkbox"/>
Central DHCP	ENABLED <input checked="" type="checkbox"/>
Flex NAT/PAT	<input type="checkbox"/> DISABLED

Anchor Policy Profile

Step2: Under the **Access Policies**, map the wired client vlan from the drop down list

General

Access Policies

QOS and AVC

Mobility

Advance

RADIUS Profiling

HTTP TLV Caching

DHCP TLV Caching

WLAN Local Profiling

Global State of Device
Classification

Disabled ⓘ

Local Subscriber Policy Name

Search or Select



VLAN

VLAN/VLAN Group

VLAN2024



Access Policies tab



Note: Configuration of the policy profile must match on both the Foreign and Anchor controllers, except for the VLAN.

Step3: Under the **Mobility** tab, check box **Export Anchor**.

Mobility Anchors

Export Anchor



Static IP Mobility



Adding Mobility Anchors will cause the enabled WLANs to momentarily disable and may result in loss of connectivity for some clients.

Drag and Drop/double click/click on the arrow to add/remove Anchors

Available (2)

Selected (0)

Anchor IP

Anchor IP

Anchor IP

Export Anchor



Note: This configuration designates the 9800 Wireless LAN Controller (WLC) as the anchor WLC for any WLAN associated with the specified Policy Profile. When a foreign 9800 WLC redirects clients to the anchor WLC, it provides details about the WLAN and the Policy Profile assigned to the client. This enables the anchor WLC to apply the appropriate local Policy Profile based on the received information.

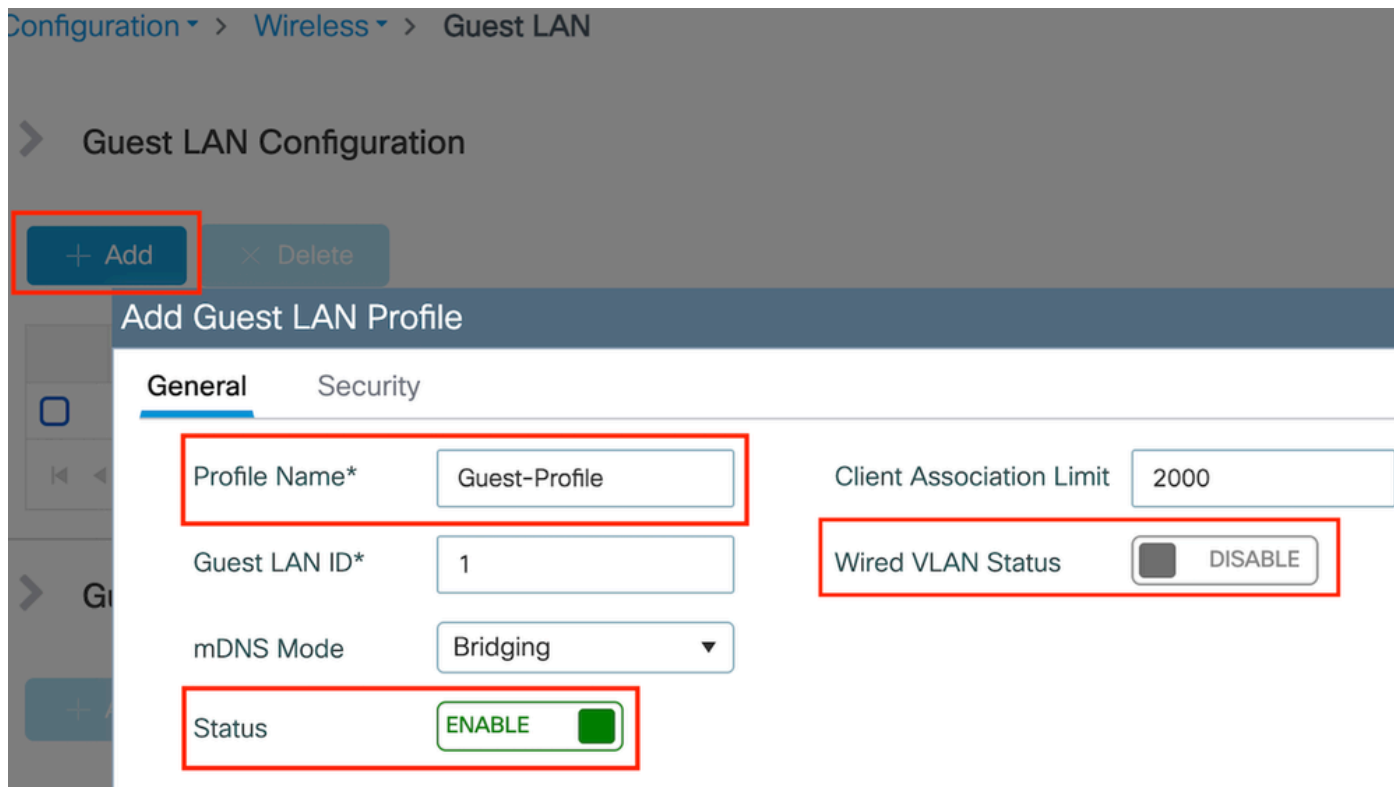
CLI Configuration

```
wireless profile policy GuestLANPolicy
mobility anchor
vlan VLAN2024
no shutdown
```

Configure Guest LAN Profile

Step1: Navigate to **Configuration > Wireless > Guest LAN**, then select **Add** to create and configure the Guest LAN profile. Ensure the profile name matches that of the foreign controller. Note that the Wired

VLAN must be disabled on the Anchor controller.



Guest LAN Profile

Step2: In the security settings, enable **Web Auth** and then configure the Web Auth parameter map and Authentication List.

Edit Guest LAN Profile

General

Security

Layer3

Web Auth

ENABLE



Web Auth Parameter Map

global



Authentication List

ISE-List





Note: The Guest LAN profile configuration must be identical between the Foreign and Anchor controllers except for the Wired VLAN status

CLI Configuration

```
guest-lan profile-name Guest-Profile 1
security web-auth authentication-list ISE-List
security web-auth parameter-map global
```

Guest LAN MAP

Step1: Navigate to **Configuration > Wireless > Guest LAN**. In the Guest LAN MAP configuration section, select **Add** and map the Policy Profile to the Guest LAN profile.

Guest LAN Map Configuration

+ Add Map × Delete Map

Guest LAN Map : GuestMap

+ Add × Delete

Guest LAN Profile Name	Policy Name
No records available.	

10 items per page 0 - 0 of 0 items

Profile Name: Guest-Profile

Policy Name: GuestLANPolicy

Save Cancel

Guest LAN MAP

wireless guest-lan map GuestMap
guest-lan Guest-Profile policy GuestLANPolicy

Configure Wired Guest on catalyst 9800 anchored to AireOS 5520 Controller



Network Topology

Configuration on Foreign 9800 WLC

Configure Web Parameter map

Step1: Navigate to **Configuration > Security > Web Auth** and select **Global**. Verify that the virtual IP address of the controller and the Trustpoint are correctly mapped on the profile, with the type set to **webauth**.

General		Advanced	
Parameter-map Name	<input type="text" value="global"/>	Virtual IPv4 Address	<input type="text" value="192.0.2.1"/>
Maximum HTTP connections	<input type="text" value="100"/>	Trustpoint	<input type="text" value="TP-self-signed-3..."/>
Init-State Timeout(secs)	<input type="text" value="120"/>	Virtual IPv4 Hostname	<input type="text"/>
Type	<input type="text" value="webauth"/>	Virtual IPv6 Address	<input type="text" value=":::XX:XX::X"/>
Captive Bypass Portal	<input type="checkbox"/>	Web Auth intercept HTTPs	<input type="checkbox"/>
Disable Success Window	<input type="checkbox"/>	Enable HTTP server for Web Auth	<input checked="" type="checkbox"/>
Disable Logout Window	<input type="checkbox"/>	Disable HTTP secure server for Web Auth	<input type="checkbox"/>
Disable Cisco Logo	<input type="checkbox"/>	Banner Configuration	
Sleeping Client Status	<input type="checkbox"/>	Banner Title	<input type="text"/>
Sleeping Client Timeout (minutes)	<input type="text" value="720"/>	Banner Type	<input checked="" type="radio"/> None <input type="radio"/> Banner Text <input type="radio"/> Read From File

Web Parameter map

Step2: Under the **Advanced** tab, specify the external web page URL to which clients must be redirected. Configure the **Redirect URL for Login** and **Redirect On-Failure**. The Redirect On-Success setting is an optional configuration.

Preview of the Redirect URL:

http://10.127.196.171/webauth/login.html?switch_url=https://192.0.2.1/login.html&redirect=<website-name>

Redirect to external server

Redirect URL for login	<input type="text" value="http://10.127.196.171/w"/>
Redirect On-Success	<input type="text" value="http://10.127.196.171/w"/>
Redirect On-Failure	<input type="text" value="http://10.127.196.171/w"/>
Redirect Append for AP MAC Address	<input type="text"/>
Redirect Append for Client MAC Address	<input type="text"/>
Redirect Append for WLAN SSID	<input type="text"/>
Portal IPV4 Address	<input type="text" value="10.127.196.171"/>
Portal IPV6 Address	<input type="text" value="X:X:X:X"/>

Advanced tab

CLI configuration

```
parameter-map type webauth global
type webauth
virtual-ip ipv4 192.0.2.1
redirect for-login http://10.127.196.171/webauth/login.html
redirect on-success http://10.127.196.171/webauth/logout.html
redirect on-failure http://10.127.196.171/webauth/failed.html
redirect portal ipv4 10.127.196.171
trustpoint TP-self-signed-3010594951
webauth-http-enable
```



Note: For AAA configuration, please refer to the configuration details provided in "" section for the Foreign 9800 WLC.

Configure Policy profile

Step1: Navigate to **Configuration > Tags & Profiles > Policy**. Select **Add**, and in the **General** tab, provide a name for the profile and enable the status toggle.

General

Access Policies

QOS and AVC

Mobility

Advanced

Name*

Guest

Description

Enter Description

Status

ENABLED

Passive Client

DISABLED

IP MAC Binding

ENABLED

Encrypted Traffic Analytics

DISABLED

CTS Policy

Inline Tagging

SGACL Enforcement

Default SGT

2-65519

WLAN Switching Policy

Central Switching

ENABLED

Central Authentication

ENABLED

Central DHCP

ENABLED

Flex NAT/PAT

DISABLED

Policy profile

Step2: In the Access Policies tab, assign a random VLAN.

General

Access Policies

QOS and AVC

Mobility

Advanced

RADIUS Profiling

HTTP TLV Caching

DHCP TLV Caching

WLAN Local Profiling

Global State of Device
Classification

Disabled ⓘ

Local Subscriber Policy Name

Search or Select



VLAN

VLAN/VLAN Group

1



Multicast VLAN

Enter Multicast VLAN

Access Policies

Step3: In the **Mobility** tab, toggle the Anchor controller and set its priority to **Primary (1)**

Mobility Anchors

Export Anchor



Static IP Mobility




Adding Mobility Anchors will cause the enabled WLANs to momentarily disable and may result in loss of connectivity for some clients.

Drag and Drop/double click/click on the arrow to add/remove Anchors

Available (1)



Anchor IP

 10.76.6.156 

Selected (1)

Anchor IP

Anchor Priority

 10.76.118.74	Primary (1) 
--	---

Mobility tab

Note: The Policy profile of the 9800 Foreign WLC must match with the Guest LAN profile of the 5520 Anchor WLC except for the vlan configuration

CLI Configuration

```
wireless profile policy Guest
no accounting-interim
exclusionlist timeout 180
no flex umbrella dhcp-dns-option
mobility anchor 10.76.118.74 priority 1
no shutdown
```

Configure Guest LAN profile

Step1: Navigate to **Configuration > Wireless > Guest LAN** and select **Add**. Configure a unique profile name and enable **Wired VLAN**, specifying the VLAN ID dedicated for wired guest users. Finally, toggle the profile status to **Enabled**.

General

Security

Profile Name* Guest

Guest LAN ID* 2

mDNS Mode Bridging

Status ENABLE

Client Association Limit 2000

Wired VLAN Status ENABLE

Wired VLAN ID* 11

Guest LAN Policy

Step2: Under the **Security** tab, enable **Web Auth**, map the Web Auth parameter map, and select the **RADIUS** server from the **Authentication** drop-down list.

General

Security

Layer3

Web Auth ENABLE

Web Auth Parameter Map global

Authentication List ISE-List

Security tab



Note: The Guest LAN profile name must be the same for the 9800 Foreign and 5520 Anchor controller

CLI Configuration

```
guest-lan profile-name Guest 2 wired-vlan 11
security web-auth authentication-list ISE-List
security web-auth parameter-map global
```

Guest LAN MAP

Step1: Navigate to **Configuration > Wireless > Guest LAN**. In the **Guest LAN MAP** configuration section, select **Add** and map the Policy Profile to the Guest LAN profile.

Guest LAN Map Configuration

+ Add Map × Delete Map

Guest LAN Map : GuestMap

+ Add × Delete

Guest LAN Profile Name	Policy Name
No records available.	

10 items per page 0 - 0 of 0 items

Profile Name: Guest

Policy Name: Guest

Save Cancel

Guest LAN MAP

CLI Configuration

```
wireless guest-lan map GuestMap
guest-lan Guest policy Guest
```

Configuration on Anchor 5520 WLC

Configure Web Authentication

Step1: Navigate to **Security > Web Auth > Web Login Page**. Set the Web Authentication type to **External (Redirect to external server)** and configure the external Web Auth URL. The **Redirect URL after login** is optional and can be configured if clients need to be redirected to a dedicated page after successful authentication.

Security > Web Login Page

Web Authentication Type: External (Redirect to external server)

Redirect URL after login: http://10.127.196.171/webauth/logout.html

Login Success Page Type: None

External Webauth URL: http://10.127.196.171/webauth/login.html

QrCode Scanning Bypass Timer: 0

QrCode Scanning Bypass Count: 0

Web Auth

Web Auth settings

AAA Settings:

Step1: Configure radius server

Navigate to **Security > Radius > Authentication > New**.



Radius Server

Step2: Configure the RADIUS server IP and shared secret on the controller. Toggle the server status to **Enabled** and check the **Network User** checkbox.

RADIUS Authentication Servers > New

Server Index (Priority)	4 ▾
Server IP Address(Ipv4/Ipv6)	<input type="text"/>
Shared Secret Format	ASCII ▾
Shared Secret	<input type="text"/>
Confirm Shared Secret	<input type="text"/>
Apply Cisco ISE Default settings	<input type="checkbox"/>
Apply Cisco ACA Default settings	<input type="checkbox"/>
Key Wrap	<input type="checkbox"/> (Designed for FIPS customers)
Port Number	1812
Server Status	Enabled ▾
Support for CoA	Disabled ▾
Server Timeout	5 seconds
Network User	<input checked="" type="checkbox"/> Enable
Management	<input checked="" type="checkbox"/> Enable
Management Retransmit Timeout	5 seconds
Tunnel Proxy	<input type="checkbox"/> Enable
PAC Provisioning	<input type="checkbox"/> Enable
IPSec	<input type="checkbox"/> Enable
Cisco ACA	<input type="checkbox"/> Enable

Server configuration

Configure Access Control List

Step1: Navigate to **Security > Access Control List** and select **New**. Create a Pre-Authentication ACL that permits traffic to DNS and the external web server.

Security

MONITOR **WLANs** CONTROLLER WIRELESS **SECURITY** MANAGEMENT COMMANDS HELP

Access Control Lists > Edit

General

Access List Name: Pre-Auth_ACL

Deny Counters: 0

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hits
1	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	Any	DNS	Any	Any	0
2	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	DNS	Any	Any	Any	0
3	Permit	0.0.0.0 / 0.0.0.0	10.127.196.171 / 255.255.255.255	TCP	Any	HTTP	Any	Any	0
4	Permit	10.127.196.171 / 255.255.255.255	0.0.0.0 / 0.0.0.0	TCP	HTTP	Any	Any	Any	0
5	Permit	0.0.0.0 / 0.0.0.0	10.127.196.171 / 255.255.255.255	TCP	Any	HTTPS	Any	Any	0
6	Permit	10.127.196.171 / 255.255.255.255	0.0.0.0 / 0.0.0.0	TCP	HTTPS	Any	Any	Any	0

Access list to permit traffic to web server

Configure Guest LAN profile

Step1: Navigate to **WLANs** > select **Create New** .

Select **Type** as **Guest LAN** and configure the same name as the policy profile of the 9800 Foreign controller.

MONITOR **WLANs** CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP

WLANs

Current Filter: None [Change Filter] [Clear Filter]

Create New [Go]

WLAN ID	Type	Profile Name	WLAN SSID	Admin Status	Security Policies
---------	------	--------------	-----------	--------------	-------------------

Create Guest LAN

MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP User:admin(ReadWrite) Home

WLANs > New

Type: Guest LAN

Profile Name: Guest

ID: 2

< Back Apply

Guest LAN Profile

Step2: Map the Ingress and Egress interfaces on the Guest LAN profile.

The Ingress interface in this case is none because the ingress interface is the EoIP tunnel from the Foreign controller.

The Egress interface is the VLAN where the wired client physically connects .

General **Security** **QoS** **Advanced**

Profile Name

Type Guest LAN

Status Enabled

Security Policies **Web-Auth**
(Modifications done under security tab will appear after applying the changes.)

Ingress Interface

Egress Interface

NAS-ID

Guest LAN profile

Step3: Under the Security tab, select Layer 3 security as **Web Authentication** and map the pre-authentication ACL.

WLANs > Edit 'Guest'

General **Security** **QoS** **Advanced**

Layer 2 **Layer 3** **AAA Servers**

Layer 3 Security

Preauthentication ACL IPv4 IPv6

Override Global Config²⁰ Enable

Guest LAN security tab

Step4: Navigate to **Security > AAA Server**.

Select the drop down and map the radius server to the Guest LAN profile.

General Security QoS Advanced

Layer 2 Layer 3 AAA Servers

Select AAA servers below to override use of default servers on this interface

RADIUS Servers

	Authentication Servers	Accounting Servers
Server 1	<input checked="" type="checkbox"/> Enabled IP:10.197.224.122, Port:1812	<input type="checkbox"/> Enabled None
Server 2	None	None
Server 3	None	None
Server 4	None	None

Map radius server to guest LAN profile

Step5: Navigate to **WLAN**. Hover over the drop down icon of the Guest LAN profile and select **Mobility Anchors**.

2 Guest LAN Guest ... Disabled Web-Auth

Remove
Mobility Anchors

Step6: Select **Mobility Anchor Create** to configure the controller as export anchor for this Guest LAN profile.

WLAN SSID Guest

Switch IP Address (Anchor)
local

Mobility Anchor Create

Data Path	Control Path
up	up

Mobility Anchor Create

Configure Wired Guest on AireOS 5520 anchored to catalyst 9800



Network Topology

Configuration on Foreign 5520 WLC

Controller Interface Configuration

Step1: Navigate to **Controller > Interfaces > New**. Configure an Interface name, VLAN ID and enable Guest LAN.

Wired Guest requires two dynamic interfaces.

First, create a Layer 2 dynamic interface and designate it as **Guest LAN**. This interface serves as the ingress interface for Guest LAN, where wired clients physically connect.

The screenshot shows the Cisco Controller configuration interface. The top navigation bar includes 'MONITOR', 'WLANS', 'CONTROLLER', 'WIRELESS', 'SECURITY', and 'MANA'. The left sidebar lists various configuration categories, with 'Interfaces' highlighted in red. The main content area is titled 'Interfaces > Edit' and is divided into several sections:

- General Information:** Interface Name is 'wired-guest' (highlighted in red), and MAC Address is 'a0:e0:af:32:d9:ba'.
- Configuration:** 'Guest Lan' is checked (highlighted in red), and NAS-ID is 'none'.
- Physical Information:** Port Number is '1', Backup Port is '0', and Active Port is '1'.
- Interface Address:** VLAN Identifier is '2020' (highlighted in red), DHCP Proxy Mode is 'Global', and 'Enable DHCP Option 82' is unchecked.

Ingress Interface

Step2: Navigate to **Controller > Interfaces > New**. Configure an Interface name, VLAN ID.

The second dynamic interface must be a Layer 3 interface on the controller, the wired clients receive IP address from this vlan subnet. This interface serves as the egress interface for the Guest LAN profile.

Controller

General

Icons

Inventory

Interfaces

Interface Groups

Multicast

Network Routes

Fabric Configuration

Redundancy

Mobility Management

Ports

NTP

CDP

PMIPv6

Tunneling

IPv6

mDNS

Advanced

Lawful Interception

Interfaces > Edit

General Information

Interface Name	vlan2024
MAC Address	a0:e0:af:32:d9:ba

Configuration

Guest Lan	<input type="checkbox"/>
Quarantine	<input type="checkbox"/>
Quarantine Vlan Id	0
NAS-ID	none

Physical Information

Port Number	1
Backup Port	0
Active Port	1
Enable Dynamic AP Management	<input type="checkbox"/>

Interface Address

VLAN Identifier	2024
IP Address	10.105.211.85
Netmask	255.255.255.128
Gateway	10.105.211.1

Egress Interface

Switch Port configuration

Wired Guest users connect to Access layer switch, these designated ports must be configured with VLAN in which **Guest LAN** is enabled on the controller

Access layer switch port configuration

```
interface gigabitEthernet <x/x/x>
```

```
description Wired Guest Access
```

```
switchport access vlan 2020
```

switchport mode access

end

Foreign controller uplink port configuration

interface TenGigabitEthernet<x/x/x>

description Trunk port to the Foreign WLC

switchport mode trunk

switchport trunk native vlan 2081

switchport trunk allowed vlan 2081,2020

end

Anchor controller uplink port configuration

interface TenGigabitEthernet<x/x/x>

description Trunk port to the Anchor WLC

switchport mode trunk

switchport trunk native vlan 2081

switchport trunk allowed vlan 2081,2024

end

Configure Web Authentication

Step1: Navigate to **Security > Web Auth > Web Login Page**. Set the Web Authentication type to **External (Redirect to external server)** and configure the external Web Auth URL. The **Redirect URL after login** is optional and can be configured if clients need to be redirected to a dedicated page after successful authentication.

The screenshot displays the Cisco Web Management Interface (WMI) for configuring Web Authentication. The navigation menu on the left shows the path: Security > Web Auth > Web Login Page. The main content area is titled "Web Login Page" and contains the following configuration fields:

Web Authentication Type	External (Redirect to external server)
Redirect URL after login	http://10.127.196.171/webauth/logout.html
Login Success Page Type	None
External Webauth URL	http://10.127.196.171/webauth/login.html

Below these fields are two numeric input fields for "QrCode Scanning Bypass Timer" and "QrCode Scanning Bypass Count", both set to 0. The interface includes a "Preview..." button and an "Apply" button. The "SECURITY" menu item in the top navigation bar and the "Web Auth" menu item in the left sidebar are highlighted with red boxes.

Web Auth settings

AAA Settings:

Step1: Configure radius server

Navigate to **Security > Radius > Authentication > New**.



Radius Server

Step2: Configure the RADIUS server IP and shared secret on the controller. Toggle the server status to **Enabled** and check the **Network User** checkbox.

RADIUS Authentication Servers > New

Server Index (Priority)	4 ▾
Server IP Address(Ipv4/Ipv6)	<input type="text"/>
Shared Secret Format	ASCII ▾
Shared Secret	<input type="text"/>
Confirm Shared Secret	<input type="text"/>
Apply Cisco ISE Default settings	<input type="checkbox"/>
Apply Cisco ACA Default settings	<input type="checkbox"/>
Key Wrap	<input type="checkbox"/> (Designed for FIPS customers)
Port Number	1812
Server Status	Enabled ▾
Support for CoA	Disabled ▾
Server Timeout	5 seconds
Network User	<input checked="" type="checkbox"/> Enable
Management	<input checked="" type="checkbox"/> Enable
Management Retransmit Timeout	5 seconds
Tunnel Proxy	<input type="checkbox"/> Enable
PAC Provisioning	<input type="checkbox"/> Enable
IPSec	<input type="checkbox"/> Enable
Cisco ACA	<input type="checkbox"/> Enable

Server configuration

Configure Access Control List

Step1: Navigate to **Security > Access Control List** and select **New**. Create a Pre-Authentication ACL that permits traffic to DNS and the external web server.

The screenshot shows the Cisco ISE Security page with the 'SECURITY' tab highlighted. The left sidebar shows the navigation menu with 'Access Control Lists' highlighted. The main content area is titled 'Access Control Lists > Edit' and shows the 'General' tab for an Access List named 'Pre-Auth_ACL'. The 'Deny Counters' are set to 0. A table lists six permit rules for various protocols and ports.

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hits
1	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	Any	DNS	Any	Any	0
2	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	DNS	Any	Any	Any	0
3	Permit	0.0.0.0 / 0.0.0.0	10.127.196.171 / 255.255.255.255	TCP	Any	HTTP	Any	Any	0
4	Permit	10.127.196.171 / 255.255.255.255	0.0.0.0 / 0.0.0.0	TCP	HTTP	Any	Any	Any	0
5	Permit	0.0.0.0 / 0.0.0.0	10.127.196.171 / 255.255.255.255	TCP	Any	HTTPS	Any	Any	0
6	Permit	10.127.196.171 / 255.255.255.255	0.0.0.0 / 0.0.0.0	TCP	HTTPS	Any	Any	Any	0

Access list to permit traffic to web server

Configure Guest LAN profile

Step1: Navigate to **WLAN > Create New > Go**.

The screenshot shows the Cisco ISE WLANs page with the 'WLANs' tab highlighted. The 'Current Filter' is set to 'None'. A 'Create New' button with a dropdown arrow and a 'Go' button are highlighted with a red box.

Guest LAN Profile

Select Type as Guest LAN and configure a profile name. The same name must be configured on the policy profile and Guest LAN profile of the 9800 Anchor controller.

The screenshot shows the 'WLANs > New' configuration page. The 'Type' dropdown is set to 'Guest LAN', the 'Profile Name' text field contains 'Guest-Profile', and the 'ID' dropdown is set to '3'. These three fields are highlighted with red boxes.

Guest LAN Profile

Step2: Under the General tab, Map the Ingress and Egress interface on the Guest LAN profile.

Ingress interface is the vlan to which the wired clients physically connect.

Egress interface is the vlan subnet that the clients request for IP address.

The screenshot shows the 'General' tab of the Guest LAN Profile configuration. The 'Profile Name' is 'Guest-Profile', 'Type' is 'Guest LAN', and 'Status' is 'Enabled'. Under 'Security Policies', 'Web-Auth' is selected. The 'Ingress Interface' is 'wired-guest' and the 'Egress Interface' is 'vlan2024'. 'NAS-ID' is set to 'none'. Red boxes highlight the 'Profile Name', 'Status', 'Ingress Interface', and 'Egress Interface' fields.

Guest LAN Profile

Step3: Navigate to **Security > Layer 3**.

Select **Layer 3 Security** as **Web Authentication** and map the Pre-Authentication ACL.

The screenshot shows the 'Security' tab, specifically the 'Layer 3' sub-tab. Under 'Layer 3 Security', 'Web Authentication' is selected. The 'Preauthentication ACL' is set to 'Pre-Auth_ACL' for IPv4 and 'None' for IPv6. The 'Override Global Config' checkbox is unchecked. Red boxes highlight the 'Web Authentication' dropdown, the 'Pre-Auth_ACL' dropdown, and the 'None' dropdown.

Layer 3 security tab

Step4:

Under AAA servers tab, map the Radius server and checkbox **Enabled**.

General Security QoS Advanced

Layer 2 Layer 3 AAA Servers

Select AAA servers below to override use of default servers on the

RADIUS Servers

Authentication Servers		Accounting Servers	
Server 1	<input checked="" type="checkbox"/> Enabled IP:10.197.224.122, Port:1812	<input type="checkbox"/> Enabled	None
Server 2	None		None
Server 3	None		None
Server 4	None		None

Mapping radius servers to Guest LAN profile

Step5: Navigate to WLAN page and hover over the dropdown icon of Guest LAN profile and select Mobility Anchors.

WLAN SSID	Guest-Profile	Enabled	Auth
30	WLAN guest-1665	Disabled	[WPA + WPA2][Auth(PSK)]
1	Guest LAN Guest-Profile	Enabled	Web-Auth
2	Guest LAN Guest	Disabled	Web-Auth

Remove
Mobility Anchors

Mobility Anchors

Step6: Map the mobility Anchor from the drop down list to the Guest LAN Profile.

Mobility Anchors

WLAN SSID Guest-Profile

Switch IP Address (Anchor)

Mobility Anchor Create

Switch IP Address (Anchor)

Foot Notes

local
10.106.39.41
10.76.6.156
✓ 10.76.118.70

Data Path

Co

Mapping mobility anchor to Guest LAN

Configuration on Anchor 9800 WLC

Configure Web Parameter map

Step1: Navigate to **Configuration > Security > Web Auth** and select **Global**. Verify that the virtual IP address of the controller and the Trustpoint are correctly mapped on the profile, with the type set to **webauth**.

General		Advanced	
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	:::~::~:~::
Captive Bypass Portal	<input type="checkbox"/>	Web Auth intercept HTTPs	<input type="checkbox"/>
Disable Success Window	<input type="checkbox"/>	Enable HTTP server for Web Auth	<input checked="" type="checkbox"/>
Disable Logout Window	<input type="checkbox"/>	Disable HTTP secure server for Web Auth	<input type="checkbox"/>
Disable Cisco Logo	<input type="checkbox"/>	Banner Configuration	
Sleeping Client Status	<input type="checkbox"/>	Banner Title	
Sleeping Client Timeout (minutes)	720	Banner Type	<input checked="" type="radio"/> None <input type="radio"/> Banner Text <input type="radio"/> Read From File

Web Parameter map

Step2: Under the **Advanced** tab, specify the external web page URL to which clients must be redirected. Configure the **Redirect URL for Login** and **Redirect On-Failure**. The Redirect On-Success setting is an optional configuration.

Preview of the Redirect URL:

http://10.127.196.171/webauth/login.html?switch_url=https://192.0.2.1/login.html&redirect=<website-name>

Redirect to external server

Redirect URL for login	<input type="text" value="http://10.127.196.171/w"/>
Redirect On-Success	<input type="text" value="http://10.127.196.171/w"/>
Redirect On-Failure	<input type="text" value="http://10.127.196.171/w"/>
Redirect Append for AP MAC Address	<input type="text"/>
Redirect Append for Client MAC Address	<input type="text"/>
Redirect Append for WLAN SSID	<input type="text"/>
Portal IPV4 Address	<input type="text" value="10.127.196.171"/>
Portal IPV6 Address	<input type="text" value="X:X:X:X"/>

Advanced tab

CLI configuration

```
parameter-map type webauth global
type webauth
virtual-ip ipv4 192.0.2.1
redirect for-login http://10.127.196.171/webauth/login.html
redirect on-success http://10.127.196.171/webauth/logout.html
redirect on-failure http://10.127.196.171/webauth/failed.html
redirect portal ipv4 10.127.196.171
trustpoint TP-self-signed-3010594951
webauth-http-enable
```



Note: For AAA configuration, please refer to the configuration details provided in "Configure Wired Guest on catalyst 9800 anchored to another catalyst 9800" section for the Foreign 9800 WLC.

Configure Policy profile

Step1: Navigate to **Configuration > Tags & Profiles > Policy**. Configure the policy profile with the same name used for the Guest LAN profile of the Foreign controller.

General

Access Policies

QOS and AVC

Mobility

Advanced

Name*

Guest-Profile

Description

Enter Description

Status

ENABLED

Passive Client

DISABLED

IP MAC Binding

ENABLED

Encrypted Traffic Analytics

DISABLED

CTS Policy

Inline Tagging

SGACL Enforcement

Default SGT

2-65519

WLAN Switching Policy

Central Switching

ENABLED

Central Authentication

ENABLED

Central DHCP

ENABLED

Flex NAT/PAT

DISABLED

Policy Profile

Step2: Under the Access Policies tab, map the wired client vlan from the drop down list

General

Access Policies

QOS and AVC

Mobility

Advanced

RADIUS Profiling

HTTP TLV Caching

DHCP TLV Caching

WLAN Local Profiling

Global State of Device
Classification

Disabled ⓘ

Local Subscriber Policy Name

Search or Select



VLAN

VLAN/VLAN Group

VLAN2024



Multicast VLAN

Enter Multicast VLAN

Access Policies

Step3: Under the **Mobility** tab, check box **Export Anchor**.

Mobility Anchors

Export Anchor



Static IP Mobility



Adding Mobility Anchors will cause the enabled WLANs to momentarily disable and may result in loss of connectivity for some clients.

Drag and Drop/double click/click on the arrow to add/remove Anchors

Mobility Tab

CLI Configuration

```
wireless profile policy Guest-Profile
no accounting-interim
exclusionlist timeout 180
no flex umbrella dhcp-dns-option
mobility anchor
vlan VLAN2024
no shutdown
```

Configure Guest LAN profile

Step1: Navigate to **Configuration > Wireless > Guest LAN** and select **Add** to configure the Guest LAN profile and disable Wired VLAN status.

Guest LAN profile name on Anchor must be same as the Guest LAN profile on Foreign WLC.

General Security

Profile Name*	Guest-Profile	Client Association Limit	2000
Guest LAN ID*	1	Wired VLAN Status	<input type="checkbox"/> DISABLE
mDNS Mode	Bridging		
Status	ENABLE <input checked="" type="checkbox"/>		

Guest LAN Profile

Step2: Under the **Security** tab, enable **Web Auth**. Select the Web Auth parameter map and Authentication List from the drop down list

Edit Guest LAN Profile

General **Security**

Layer3

Web Auth	ENABLE <input checked="" type="checkbox"/>
Web Auth Parameter Map	global
Authentication List	ISE-List

Guest LAN Security tab

CLI Configuration

```
guest-lan profile-name Guest-Profile 1  
security web-auth authentication-list ISE-List
```

security web-auth parameter-map global

Guest LAN MAP

Step1: Navigate to **Configuration > Wireless > Guest LAN**. In the **Guest LAN MAP** configuration section, select **Add** and map the Policy Profile to the Guest LAN profile.

> Guest LAN Map Configuration

+ Add Map × Delete Map

Guest LAN Map: GuestMap

+ Add × Delete

Guest LAN Profile Name	Policy Name
No records available.	
10 items per page 0 - 0 of 0 items	

Profile Name:

Policy Name:

Save Cancel

Guest LAN MAP

Verify

Validate controller Configuration

#show guest-lan summary

GLAN	GLAN Profile Name	Status
1	Guest-Profile	UP
2	Guest	UP

#show guest-lan id 1

<#root>

```
Guest-LAN Profile Name      : Guest
=====
Guest-LAN ID                : 2
Wired-Vlan                  :
11
Status                       :
Enabled
Number of Active Clients    : 0
```



```

Max Associated Clients           : 2000
Security
  WebAuth                       :
Enabled
  Webauth Parameter Map        : global
  Webauth Authentication List  :
ISE-List
  Webauth Authorization List   : Not configured
mDNS Gateway Status            : Bridge

```

#show parameter-map type webauth global

```

<#root>
Parameter Map Name             : global
  Type                         :
webauth
  Redirect:
    For Login                   :
http://10.127.196.171/webauth/login.html
    On Success                  :
http://10.127.196.171/webauth/logout.html
    On Failure                  :
http://10.127.196.171/webauth/failed.html
  Portal ipv4                  :
10.127.196.171
    Virtual-ipv4                :
192.0.2.1

```

#show parameter-map type webauth name <profile name> (If custom web parameter profile is used)

#show wireless guest-lan-map summary

GLAN Profile Name	Policy Name
Guest	Guest

#show wireless mobility summary

IP	Public Ip	MAC Address
----	-----------	-------------

10.76.118.70

10.76.118.70

f4bd.9e59.314b

#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 secure server capability: Present
HTTP secure server status: Enabled
HTTP secure server port: 443
HTTP secure server trustpoint: TP-self-signed-3010594951

>show guest-lan summary

Number of Guest LANs..... 1

GLAN ID	GLAN Profile Name	Status	Interface Name
2	Guest	Enabled	wired-vlan-11

>show guest-lan 2

Guest LAN Identifier..... 2
Profile Name..... Guest
Status..... Enabled
Interface..... wired-vlan-11
Radius Servers
 Authentication..... 10.197.224.122 1812 *
 Web Based Authentication..... Enabled
 Web Authentication Timeout..... 300
 IPv4 ACL..... Pre-Auth_ACL
 Mobility Anchor List
 GLAN ID IP Address Status

 2 10.76.118.74 Up

>show custom-web all

Radius Authentication Method..... PAP
Cisco Logo..... Enabled
CustomLogo..... None
Custom Title..... None
Custom Message..... None

```
Custom Redirect URL..... http://10.127.196.171/webauth/logout.html
Web Authentication Login Success Page Mode..... None
Web Authentication Type..... External
Logout-popup..... Enabled
External Web Authentication URL..... http://10.127.196.171/webauth/login.html
QR Code Scanning Bypass Timer..... 0
QR Code Scanning Bypass Count..... 0
```

>show custom-web guest-lan 2

```
Guest LAN Status..... Enabled
Web Security Policy..... Web Based Authentication
WebAuth Type..... External
Global Status..... Enabled
```

Validate client Policy state

On Foreign,

#show wireless client summary

Client policy manager state on the Foreign controller is RUN after the client associates successfully.

<#root>

MAC Address	AP Name	Type ID	State	Protocol	Method
a0ce.c8c3.a9b5	N/A				
GLAN 1					
			Run		
802.3					
			Web Auth		
Export Foreign					

>show client detail a0ce.c8c3.a9b5

<#root>

```
Client MAC Address..... a0:ce:c8:c3:a9:b5
Client Username ..... N/A
Client Webauth Username ..... N/A
Client State..... Associated
User Authenticated by ..... None
Client User Group.....
Client NAC OOB State..... Access
guest-lan..... 1
Wireless LAN Profile Name..... Guest-Profile
Mobility State.....
```

Export Foreign

Mobility Anchor IP Address.....
10.76.118.70

Security Policy Completed.....
Yes

Policy Manager State.....
RUN

Pre-auth IPv4 ACL Name..... Pre-Auth_ACL
EAP Type..... Unknown
Interface.....

wired-guest-egress

VLAN..... 2024
Quarantine VLAN..... 0

On Anchor,

Client state transistion must be monitored on the Anchor controller.

Client policy manager state is in Web Auth pending .

<#root>

MAC Address	AP Name	Type ID	State	Protocol	Method
a0ce.c8c3.a9b5	10.76.6.156				

GLAN 1

Webauth Pending

802.3

Web Auth

Export Anchor

Once the client authenticates, the policy manager state transitions to RUN state.

MAC Address	AP Name	Type ID	State	Protocol	Method
a0ce.c8c3.a9b5	10.76.6.156	GLAN 1	Run	802.3	Web

#show wireless client mac-address a0ce.c8c3.a9b5 detail

<#root>

Client MAC Address : a0ce.c8c3.a9b5
Client MAC Type : Universally Administered Address
Client DUID: NA
Client IPv4 Address :

10.105.211.69

Client State : Associated
Policy Profile : Guest-Profile
Flex Profile : N/A
Guest Lan:
GLAN Id: 1
GLAN Name: Guest-Profile

Mobility:

Foreign IP Address :

10.76.118.74

Point of Attachment : 0xA0000003
Point of Presence : 0
Move Count : 1
Mobility Role :

Export Anchor

Mobility Roam Type :

L3 Requested

Policy Manager State:

Webauth Pending

Last Policy Manager State :

IP Learn Complete

Client Entry Create Time : 35 seconds

VLAN : VLAN2024

Session Manager:

Point of Attachment : mobility_a0000003
IIF ID : 0xA0000003
Authorized : FALSE
Session timeout : 28800
Common Session ID: 4a764c0a0000008ea0285466
Acct Session ID : 0x00000000
Auth Method Status List
Method : Web Auth
Webauth State :

Login

Webauth Method :

Webauth

Server Policies:

Resultant Policies:
URL Redirect ACL :

WA-v4-int-10.127.196.171

```
Preauth ACL      :
WA-sec-10.127.196.171
VLAN Name       : VLAN2024
VLAN            :
2024
Absolute-Timer  : 28800
```

Client moves to RUN state after successful web authentication.

show wireless client mac-address a0ce.c8c3.a9b5 detail

<#root>

```
Client MAC Address : a0ce.c8c3.a9b5
Client MAC Type   : Universally Administered Address
Client DUID       : NA
Client IPv4 Address :
10.105.211.69
Client Username   :
testuser
```

```
Client State : Associated
Policy Profile : Guest-Profile
Flex Profile  : N/A
Guest Lan:
  GLAN Id: 1
  GLAN Name: Guest-Profile
Wireless LAN Network Name (SSID) : N/A
BSSID : N/A
Connected For : 81 seconds
Protocol : 802.3
```

Policy Manager State:

Run

Last Policy Manager State :

Webauth Pending

```
Client Entry Create Time : 81 seconds
VLAN : VLAN2024
```

Last Tried Aaa Server Details:

Server IP :

10.197.224.122

Auth Method Status List

Method : Web Auth

Webauth State : Authz

Webauth Method : Webauth

Resultant Policies:

URL Redirect ACL :

IP-Adm-V4-LOGOUT-ACL

VLAN Name : VLAN2024
VLAN :

2024

Absolute-Timer : 28800

>show client detail a0:ce:c8:c3:a9:b5

<#root>

Client MAC Address..... a0:ce:c8:c3:a9:b5
Client Username N/A
Client Webauth Username N/A
Client State..... Associated
Wireless LAN Profile Name..... Guest
WLAN Profile check for roaming..... Disabled
Hotspot (802.11u)..... Not Supported
Connected For 90 secs
IP Address..... 10.105.211.75
Gateway Address..... 10.105.211.1
Netmask..... 255.255.255.128
Mobility State.....

Export Anchor

Mobility Foreign IP Address.....
10.76.118.70

Security Policy Completed..... No
Policy Manager State.....

WEBAUTH_REQD

Pre-auth IPv4 ACL Name.....

Pre-Auth_ACLPre-auth

IPv4 ACL Applied Status..... Yes
Pre-auth IPv4 ACL Applied Status.....

Yes

After Authentication client transistions to RUN state.

<#root>

show client detail a0:ce:c8:c3:a9:b5
Client MAC Address..... a0:ce:c8:c3:a9:b5
Client Username

testuser

Client Webauth Username

testuser

Client State.....

Associated

User Authenticated by

RADIUS Server

Client User Group..... testuser

Client NAC OOB State..... Access

Connected For 37 secs

IP Address.....

10.105.211.75

Gateway Address..... 10.105.211.1

Netmask..... 255.255.255.128

Mobility State.....

Export Anchor

Mobility Foreign IP Address..... 10.76.118.70

Security Policy Completed..... Yes

Policy Manager State.....

RUN

Pre-auth IPv4 ACL Name..... Pre-Auth_ACL

Pre-auth IPv4 ACL Applied Status..... Yes

EAP Type..... Unknown

Interface.....

wired-vlan-11

VLAN.....

11

Quarantine VLAN..... 0

Troubleshoot

AireOS Controller debug

Enable client debug

>debug client <H.H.H>

To verify if debugging is enabled

>show debugging

To disable debug

debug disable-all

9800 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 in 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's bootflash.

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

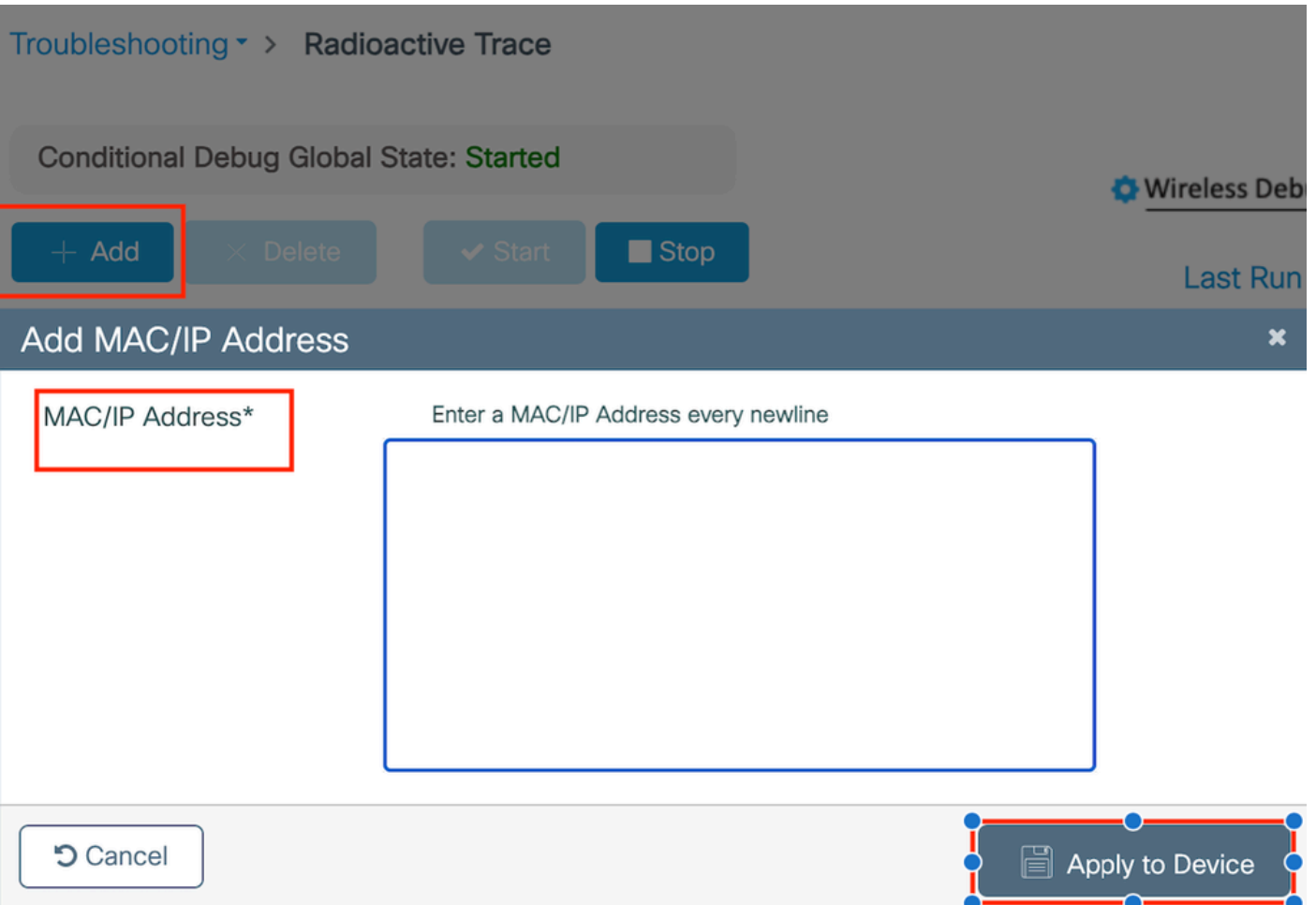
Copy the file to an external server.

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

Display the debug log:

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

Enable RA trace in GUI,



Enable RA trace on WebUI

Embedded Packet Capture

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

+ Add × Delete

Create Packet Capture

Capture Name* TestPCap

Filter* any

Monitor Control Plane

Inner Filter Protocol DHCP

Inner Filter MAC

Buffer Size (MB)* 100

Limit by* Duration 3600 secs ≈ 1.00 hour

Available (12) Search

- Tw0/0/1
- Tw0/0/2
- Tw0/0/3
- Te0/1/0

Selected (1)

- Tw0/0/0



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

Navigate to **Troubleshooting > Packet Capture** and select **Start** to capture packets.

Capture Name	Interface	Monitor Control Plane	Buffer Size	Filter by	Limit	Status	Action
<input type="checkbox"/> TestPCap	TwoGigabitEthernet0/0/0	No	0%	any	3600 secs	Inactive	▶ Start

Start Packet 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
```

<Reproduce the issue>

monitor capture TestPCap stop

show monitor capture TestPCap

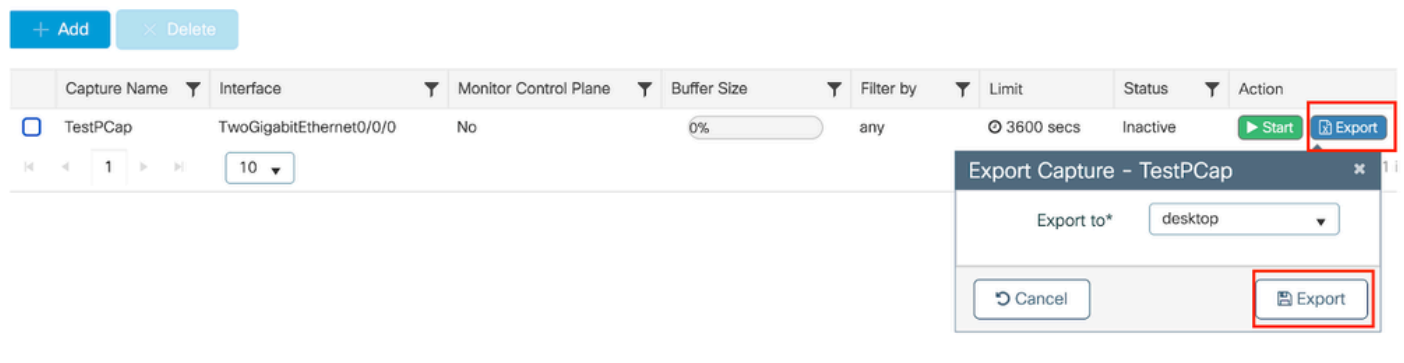
Status Information for Capture TestPCap

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

Navigate to **Troubleshooting > Packet Capture** and select **Export** to download the capture file on the local machine.



Download EPC

Working log snippets

AireOS Foreign Controller client debug log

Wired packet received from wired client

*apfReceiveTask: May 27 12:00:55.127: a0:ce:c8:c3:a9:b5 Wired Guest packet from 10.105.211.69 on mobi

Foreign controller building export anchor request

*apfReceiveTask: May 27 12:00:56.083: a0:ce:c8:c3:a9:b5 Attempting anchor export for mobile a0:ce:c8:c3

*apfReceiveTask: May 27 12:00:56.083: a0:ce:c8:c3:a9:b5 mmAnchorExportSend: Building ExportForeignLradM

*apfReceiveTask: May 27 12:00:56.083: a0:ce:c8:c3:a9:b5 SGT Payload built in Export Anchor Req 0

Foreign controller sends Export anchor request to the anchor controller.

*apfReceiveTask: May 27 12:00:56.083: a0:ce:c8:c3:a9:b5 Export Anchor request sent to 10.76.118.70

Anchor controller sends acknowledgement for the Anchor request for client

*Dot1x_NW_MsgTask_5: May 27 12:00:56.091: a0:ce:c8:c3:a9:b5 Recvd Exp Anchor Ack for mobile a0:ce:c8:c

Mobility role for the clients on the Foreign controller is updated to export Foreign.

*apfReceiveTask: May 27 12:00:56.091: a0:ce:c8:c3:a9:b5 0.0.0.0 DHCP_REQD (7) mobility role update requ
Peer = 10.76.118.70, Old Anchor = 10.76.118.70, New Anchor = 10.76.118.70

Client transitioned into RUN state.

*apfReceiveTask: May 27 12:00:56.091: a0:ce:c8:c3:a9:b5 0.0.0.0 DHCP_REQD (7) State Update from Mobilit

*apfReceiveTask: May 27 12:00:56.091: a0:ce:c8:c3:a9:b5 Stopping deletion of Mobile Station: (callerId:

*apfReceiveTask: May 27 12:00:56.091: a0:ce:c8:c3:a9:b5 Moving client to run state

9800 Foreign controller radioactive trace

Client associates to the controller.

2024/07/15 04:10:29.087608331 {wncd_x_R0-0}{1}: [client-orch-state] [17765]: (note): MAC: a0ce.c8c3.a9b

Mobility discovery is in progress after association.

2024/07/15 04:10:29.091585813 {wncd_x_R0-0}{1}: [client-orch-state] [17765]: (note): MAC: a0ce.c8c3.a9b5
2024/07/15 04:10:29.091605761 {wncd_x_R0-0}{1}: [client-orch-state] [17765]: (note): MAC: a0ce.c8c3.a9b5

Once Mobility discovery is processed, client roam type is updates to L3 requested.

2024/07/15 04:10:29.091664605 {wncd_x_R0-0}{1}: [mm-transition] [17765]: (info): MAC: a0ce.c8c3.a9b5 MM
2024/07/15 04:10:29.091693445 {wncd_x_R0-0}{1}: [mm-client] [17765]: (info): MAC: a0ce.c8c3.a9b5 Roam t

Foreign controller is sending the export anchor request to the Anchor WLC.

2024/07/15 04:10:32.093245394 {mobilityd_R0-0}{1}: [mm-client] [18316]: (debug): MAC: a0ce.c8c3.a9b5 Ex
2024/07/15 04:10:32.093253788 {mobilityd_R0-0}{1}: [mm-client] [18316]: (debug): MAC: a0ce.c8c3.a9b5 Fo
2024/07/15 04:10:32.093274405 {mobilityd_R0-0}{1}: [mm-client] [18316]: (info): MAC: a0ce.c8c3.a9b5 For

Export Anchor response is received from the Anchor controller and vlan is applied from the user profile.

2024/07/15 04:10:32.106775213 {mobilityd_R0-0}{1}: [mm-transition] [18316]: (info): MAC: a0ce.c8c3.a9b5
2024/07/15 04:10:32.106811183 {mobilityd_R0-0}{1}: [mm-client] [18316]: (debug): MAC: a0ce.c8c3.a9b5 Ex
2024/07/15 04:10:32.107183692 {wncd_x_R0-0}{1}: [epm-misc] [17765]: (info): [a0ce.c8c3.a9b5:Tw0/0/0] An
2024/07/15 04:10:32.107247304 {wncd_x_R0-0}{1}: [svm] [17765]: (info): [a0ce.c8c3.a9b5] Applied User Pr
2024/07/15 04:10:32.107250258 {wncd_x_R0-0}{1}: [aaa-attr-inf] [17765]: (info): Applied User Profile:

Once the Export Anchor request is processed, client mobility role is updated to Export Foreign.

2024/07/15 04:10:32.107490972 {wncd_x_R0-0}{1}: [mm-client] [17765]: (debug): MAC: a0ce.c8c3.a9b5 Proce
2024/07/15 04:10:32.107502336 {wncd_x_R0-0}{1}: [mm-client] [17765]: (info): MAC: a0ce.c8c3.a9b5 Mobili
2024/07/15 04:10:32.107533732 {wncd_x_R0-0}{1}: [sanet-shim-translate] [17765]: (info): Anchor Vlan: 20
2024/07/15 04:10:32.107592251 {wncd_x_R0-0}{1}: [mm-client] [17765]: (note): MAC: a0ce.c8c3.a9b5 Mobili

Client transitions into IP learn state.

2024/07/15 04:10:32.108210365 {wncd_x_R0-0}{1}: [client-orch-state] [17765]: (note): MAC: a0ce.c8c3.a9b5
2024/07/15 04:10:32.108293096 {wncd_x_R0-0}{1}: [client-orch-sm] [17765]: (debug): MAC: a0ce.c8c3.a9b5

After IP learn, client moves to RUN state on the Foreign WLC.

2024/07/15 04:10:32.108521618 {wncd_x_R0-0}{1}: [client-orch-state] [17765]: (note): MAC: a0ce.c8c3.a9b5

AireOS Anchor controller client debug log

Export Anchor request received from the Foreign controller.

```
*Dot1x_NW_MsgTask_5: May 28 10:46:27.831: a0:ce:c8:c3:a9:b5 Anchor Export Request Recvd for mobile a0:c
*Dot1x_NW_MsgTask_5: May 28 10:46:27.831: a0:ce:c8:c3:a9:b5 mmAnchorExportRcv: Extracting mmPayloadExpo
*Dot1x_NW_MsgTask_5: May 28 10:46:27.831: a0:ce:c8:c3:a9:b5 mmAnchorExportRcv Ssid=Guest useProfileName
```

Local bridging vlan is applied for the client.

```
*Dot1x_NW_MsgTask_5: May 28 10:46:27.831: a0:ce:c8:c3:a9:b5 Updated local bridging VLAN to 11 while app
*Dot1x_NW_MsgTask_5: May 28 10:46:27.831: a0:ce:c8:c3:a9:b5 Applying Interface(wired-vlan-11) policy on
*Dot1x_NW_MsgTask_5: May 28 10:46:27.831: a0:ce:c8:c3:a9:b5 After applying Interface(wired-vlan-11) pol
```

Mobility role is updated to Export Anchor and client state transitioned Associated.

```
*Dot1x_NW_MsgTask_5: May 28 10:46:27.831: a0:ce:c8:c3:a9:b5 0.0.0.0 START (0) mobility role update requ
Peer = 10.76.118.70, Old Anchor = 0.0.0.0, New Anchor = 10.76.118.74
Dot1x_NW_MsgTask_5: May 28 10:46:27.831: a0:ce:c8:c3:a9:b5
add client MAC a0:ce:c8:c3:a9:b5 IP 10.76.1
*Dot1x_NW_MsgTask_5: May 28 10:46:27.831: a0:ce:c8:c3:a9:b5
Sent message to add a0:ce:c8:c3:a9:b5 on me
*Dot1x_NW_MsgTask_5: May 28 10:46:27.832: a0:ce:c8:c3:a9:b5 mmAnchorExportRcv (mm_listen.c:7933) Changi
```

Mobility is completed, client state is associated and mobility role is Export Anchor.

```
*Dot1x_NW_MsgTask_5: May 28 10:46:27.832: a0:ce:c8:c3:a9:b5 0.0.0.0 DHCP_REQD (7) State Update from Mob
```

Client IP address is learnt on the controller and state transitioned from DHCP required to Web auth required.

```
*dtlArpTask: May 28 10:46:58.356: a0:ce:c8:c3:a9:b5 Static IP client associated to interface wired-vlan
*dtlArpTask: May 28 10:46:58.356: a0:ce:c8:c3:a9:b5 dtlArpSetType: Changing ARP Type from 0 ---> 1 for
*dtlArpTask: May 28 10:46:58.356: a0:ce:c8:c3:a9:b5 10.105.211.75 DHCP_REQD (7) Change state to WEBAUTH
```

Webauth URL is being formulated by adding the external redirect url and controller Virtual ip address.

```
*webauthRedirect: May 28 10:46:58.500: a0:ce:c8:c3:a9:b5- Preparing redirect URL according to configure
*webauthRedirect: May 28 10:46:58.500: a0:ce:c8:c3:a9:b5- Web-auth type External, using URL:http://10.1
*webauthRedirect: May 28 10:46:58.500: a0:ce:c8:c3:a9:b5- Added switch_url, redirect URL is now http://
```


Added Client mac address and WLAN to the URL.

```
*webauthRedirect: May 28 10:46:58.500: a0:ce:c8:c3:a9:b5- Added client_mac , redirect URL is now http://
*webauthRedirect: May 28 10:46:58.500: a0:ce:c8:c3:a9:b5- Added wlan, redirect URL is now
*webauthRedirect: May 28 10:46:58.500: a0:ce:c8:c3:a9:b5- Added wlan, redirect URL is now http://10.127
```

Final URL after parsing the HTTP GET for host 10.105.211.1

```
*webauthRedirect: May 28 10:46:58.500: a0:ce:c8:c3:a9:b5- parser host is 10.105.211.1
*webauthRedirect: May 28 10:46:58.500: a0:ce:c8:c3:a9:b5- parser path is /auth/discovery
*webauthRedirect: May 28 10:46:58.500: a0:ce:c8:c3:a9:b5-added redirect=, URL is now http://10.127.196.
```

Redirect URL is sent to the client in the 200 OK response packet.

```
*webauthRedirect: May 28 10:46:58.500: a0:ce:c8:c3:a9:b5- 200 send_data =HTTP/1.1 200 OK
Location:http://10.127.196.171/webauth/login.html?switch_url=https://192.0.2.1/login.html&client_mac=a0
```

Client establishes a TCP connection with redirect url host. Once the clients submit the login username and password on the portal a radius request is sent by the controller to radius server

Once the controller receives an Access-Accept, the client closed the TCP session and is moved to RUN state.

```
*aaaQueueReader: May 28 10:46:59:077: a0:ce:c8:c3:a9:b5 Sending the packet to v4 host 10.197.224.122:18
*aaaQueueReader: May 28 10:46:59:077: a0:ce:c8:c3:a9:b5 Successful transmission of Authentication Packe
*aaaQueueReader: May 28 10:46:59:077: AVP[01] User-Name.....testuser
*aaaQueueReader: May 28 10:46:59:077: AVP[03] Calling-Station-Id.....a0-ce-c8
*aaaQueueReader: May 28 10:46:59:077: AVP[04] Nas-Port.....0x000000
*aaaQueueReader: May 28 10:46:59:077: AVP[05] Nas-Ip-Address.....0x0a4c76
*aaaQueueReader: May 28 10:46:59:077: AVP[06] NAS-Identifier.....POD1586-
*aaaQueueReader: May 28 10:46:59:500: a0:ce:c8:c3:a9:b5 radiusServerFallbackPassiveStateUpdate: RADIUS
*radiusTransportThread: May 28 10:46:59:500: a0:ce:c8:c3:a9:b5 Access-Accept received from RADIUS serv
*Dot1x_NW_MsgTask_5: May 28 10:46:59:500: a0:ce:c8:c3:a9:b5 Processing Access-Accept for mobile a0:ce:c
*apfReceiveTask: May 28 10:46:59:500: a0:ce:c8:c3:a9:b5 Moving client to run state
```

9800 Anchor controller radioactive trace

Mobility announce message for the client from the Foreign controller.

2024/07/15 15:10:20.614677358 {mobilityd_R0-0}{1}: [mm-client] [15259]: (debug): MAC: a0ce.c8c3.a9b5 Re

Export anchor request received from the foreign controller when the client is associating for which Export anchor response is sent by the Anchor controller which can be verified on the Foreign controller RA trace.

2024/07/15 15:10:22.615246594 {mobilityd_R0-0}{1}: [mm-transition] [15259]: (info): MAC: a0ce.c8c3.a9b5

Client is moved to associating state and mobility role is transitioned to Export Anchor.

2024/07/15 15:10:22.616156811 {wncd_x_R0-0}{1}: [client-orch-state] [14709]: (note): MAC: a0ce.c8c3.a9b5
2024/07/15 15:10:22.627358367 {wncd_x_R0-0}{1}: [mm-client] [14709]: (note): MAC: a0ce.c8c3.a9b5 Mobili

2024/07/15 15:10:22.627462963 {wncd_x_R0-0}{1}: [dot11] [14709]: (note): MAC: a0ce.c8c3.a9b5 Client da
2024/07/15 15:10:22.627490485 {mobilityd_R0-0}{1}: [mm-client] [15259]: (debug): MAC: a0ce.c8c3.a9b5 Ex
2024/07/15 15:10:22.627494963 {mobilityd_R0-0}{1}: [mm-client] [15259]: (debug): MAC: a0ce.c8c3.a9b5 Fo

IP learn is completed, client IP learnt through ARP .

2024/07/15 15:10:22.628124206 {wncd_x_R0-0}{1}: [client-iplearn] [14709]: (info): MAC: a0ce.c8c3.a9b5
2024/07/15 15:10:23.627064171 {wncd_x_R0-0}{1}: [sisf-packet] [14709]: (info): RX: ARP from interface m
2024/07/15 15:10:24.469704913 {wncd_x_R0-0}{1}: [client-iplearn] [14709]: (note): MAC: a0ce.c8c3.a9b5
2024/07/15 15:10:24.470527056 {wncd_x_R0-0}{1}: [client-iplearn] [14709]: (info): MAC: a0ce.c8c3.a9b5
2024/07/15 15:10:24.470587596 {wncd_x_R0-0}{1}: [client-orch-sm] [14709]: (debug): MAC: a0ce.c8c3.a9b5
2024/07/15 15:10:24.470613094 {wncd_x_R0-0}{1}: [client-orch-sm] [14709]: (debug): MAC: a0ce.c8c3.a9b5

Client policy state is in web auth pending.

2024/07/15 15:10:24.470748350 {wncd_x_R0-0}{1}: [client-auth] [14709]: (info): MAC: a0ce.c8c3.a9b5 Cli

TCP handshake is spoofed by the controller. When the client sends a HTTP GET, a 200 OK response frame is sent which contains the redirect URL.

The client must establish a TCP handshake with the redirect URL and load the page.

2024/07/15 15:11:37.579177010 {wncd_x_R0-0}{1}: [webauth-httpd] [14709]: (info): mobility_a0000001[a0ce
2024/07/15 15:11:37.579190912 {wncd_x_R0-0}{1}: [webauth-httpd] [14709]: (info): mobility_a0000001[a0ce
2024/07/15 15:11:37.579226658 {wncd_x_R0-0}{1}: [webauth-state] [14709]: (info): mobility_a0000001[a0ce
2024/07/15 15:11:37.579230650 {wncd_x_R0-0}{1}: [webauth-state] [14709]: (info): mobility_a0000001[a0ce
2024/07/15 15:11:47.123072893 {wncd_x_R0-0}{1}: [webauth-httpd] [14709]: (info): mobility_a0000001[a0ce

2024/07/15 15:11:47.123082753 {wncd_x_R0-0}{1}: [webauth-httpd] [1470

When the client submits the login credentials on the web portal page, an Access-Request packet is sent to the radius server for authentication.

```
2024/07/15 15:12:04.281076844 {wncd_x_R0-0}{1}: [radius] [14709]: (info): RADIUS: Send Access-Request t
2024/07/15 15:12:04.281087672 {wncd_x_R0-0}{1}: [radius] [14709]: (info): RADIUS: authenticator e3 01
2024/07/15 15:12:04.281093278 {wncd_x_R0-0}{1}: [radius] [14709]: (info): RADIUS: Calling-Station-Id
2024/07/15 15:12:04.281097034 {wncd_x_R0-0}{1}: [radius] [14709]: (info): RADIUS: User-Name
2024/07/15 15:12:04.281148298 {wncd_x_R0-0}{1}: [radius] [14709]: (info): RADIUS: Cisco AVpair
```

Access-Accept is received from the radius server, webauth is successful.

```
2024/07/15 15:12:04.683597101 {wncd_x_R0-0}{1}: [radius] [14709]: (info): RADIUS: Received from id 1812
2024/07/15 15:12:04.683607762 {wncd_x_R0-0}{1}: [radius] [14709]: (info): RADIUS: authenticator 52 3e
2024/07/15 15:12:04.683614780 {wncd_x_R0-0}{1}: [radius] [14709]: (info): RADIUS: User-Name
```

Authentication is successful and client policy state is at RUN.

```
2024/07/15 15:12:04.683901842 {wncd_x_R0-0}{1}: [webauth-state] [14709]: (info): mobility_a0000001[a0ce
2024/07/15 15:12:04.690643388 {wncd_x_R0-0}{1}: [errmsg] [14709]: (info): %CLIENT_ORCH_LOG-6-CLIENT_ADD
2024/07/15 15:12:04.690726966 {wncd_x_R0-0}{1}: [aaa-attr-inf] [14709]: (info): [ Applied attribute :bs
2024/07/15 15:12:04.691064276 {wncd_x_R0-0}{1}: [client-orch-state] [14709]: (note): MAC: a0ce.c8c3.a9b
```

Embedded packet capture analysis

No.	Time	Source	Destination	Length	Protocol	Info
804	15:10:24.826953	10.105.211.69	10.105.211.1		HTTP	GET /auth/discovery?architecture=9 HTTP/1.1
806	15:10:24.826953	10.105.211.1	10.105.211.69		HTTP	HTTP/1.1 200 OK (text/html)

> Frame 806: 863 bytes on wire (6904 bits), 863 bytes captured (6904 bits)

- > Ethernet II, Src: Cisco_59:31:4b (f4:bd:9e:59:31:4b), Dst: Cisco_34:90:cb (6c:5e:3b:34:90:cb)
- > Internet Protocol Version 4, Src: 10.76.118.70, Dst: 10.76.6.156
- > User Datagram Protocol, Src Port: 16667, Dst Port: 16667
- > Control And Provisioning of Wireless Access Points - Data
- > Ethernet II, Src: Cisco_34:90:d4 (6c:5e:3b:34:90:d4), Dst: CeLink_c3:a9:b5 (a0:ce:c8:c3:a9:b5)
- > 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 4095
- > Internet Protocol Version 4, Src: 10.105.211.1, Dst: 10.105.211.69
- > Transmission Control Protocol, Src Port: 80, Dst Port: 54351, Seq: 1, Ack: 108, Len: 743

> Hypertext Transfer Protocol

- > HTTP/1.1 200 OK\r\n
- Location: http://10.127.196.171/webauth/login.html?switch_url=https://192.0.2.1/login.html&redirect=http://10.105.211.1/auth/discovery?architecture=9\r\n
- Content-Type: text/html\r\n
- Content-Length: 527\r\n
- \r\n
- [HTTP response 1/1]
- [Time since request: 0.000000000 seconds]
- [Request in frame: 804]
- [Request URI: http://10.105.211.1/auth/discovery?architecture=9]
- File Data: 527 bytes

Client is redirected to the portal page

Session is closed after receiving the redirect URL.

804	15:10:24.826953	10.105.211.69	10.105.211.1	HTTP	GET /auth/discovery?architecture=9 HTTP/1.1
805	15:10:24.826953	10.105.211.1	10.105.211.69	TCP	80 → 54351 [ACK] Seq=1 Ack=108 Win=65152 Len=0 TSval=2124108437 TSecr=2231352500
806	15:10:24.826953	10.105.211.1	10.105.211.69	HTTP	HTTP/1.1 200 OK (text/html)
807	15:10:24.826953	10.105.211.69	10.105.211.1	TCP	54351 → 80 [ACK] Seq=108 Ack=744 Win=131008 Len=0 TSval=2231352500 TSecr=2124108437
812	15:10:24.835955	10.105.211.69	10.105.211.1	TCP	54351 → 80 [FIN, ACK] Seq=108 Ack=744 Win=131072 Len=0 TSval=2231352510 TSecr=2124108437
813	15:10:24.836947	10.105.211.1	10.105.211.69	TCP	80 → 54351 [FIN, ACK] Seq=744 Ack=109 Win=65152 Len=0 TSval=2124108447 TSecr=2231352510
814	15:10:24.836947	10.105.211.69	10.105.211.1	TCP	54351 → 80 [ACK] Seq=109 Ack=745 Win=131072 Len=0 TSval=2231352510 TSecr=2124108447

TCP session is closed after receiving the redirect URL

Client initiates TCP 3 way handshake to the redirect URL host and sends a HTTP GET request.

Once the page loads, the login credentials are submitted on the portal, the controller sends a Access Request to the radius server to authenticate the client.

After successful authentication, the TCP session to the web server is closed and on the controller, the client policy manager state is transitioned to RUN.

2348	15:11:38.598968	10.105.211.69	10.127.196.171	TCP	54381 → 80 [SYN, ECE, CWR] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=2678067533 TSecr=0
2349	15:11:38.599959	10.127.196.171	10.105.211.69	TCP	80 → 54381 [SYN, ACK, ECE] Seq=0 Ack=1 Win=65535 Len=0 MSS=1380 WS=256 SACK_PERM
2350	15:11:38.599959	10.105.211.69	10.127.196.171	TCP	54381 → 80 [ACK] Seq=1 Ack=1 Win=262144 Len=0
2351	15:11:38.600966	10.105.211.69	10.127.196.171	HTTP	GET /webauth/login.html?switch_url=https://192.0.2.1/login.html&redirect=http://3.3.3.3/
2352	15:11:38.602965	10.127.196.171	10.105.211.69	HTTP	[TCP Previous segment not captured] Continuation
2354	15:11:38.602965	10.127.196.171	10.105.211.69	TCP	[TCP Out-Of-Order] 80 → 54381 [ACK] Seq=1 Ack=485 Win=2097408 Len=1380
2355	15:11:38.603957	10.105.211.69	10.127.196.171	TCP	[TCP Dup ACK 2350#1] 54381 → 80 [ACK] Seq=485 Ack=1 Win=262144 Len=0 SLE=1381 SRE=1737
2356	15:11:38.603957	10.105.211.69	10.127.196.171	TCP	54381 → 80 [ACK] Seq=485 Ack=1737 Win=260352 Len=0
2358	15:11:38.615965	10.105.211.69	10.127.196.171	HTTP	GET /webauth/yourlogo.jpg HTTP/1.1
2359	15:11:38.616957	10.127.196.171	10.105.211.69	HTTP	HTTP/1.1 304 Not Modified
2360	15:11:38.616957	10.105.211.69	10.127.196.171	TCP	54381 → 80 [ACK] Seq=1113 Ack=1880 Win=261952 Len=0
2362	15:11:38.621961	10.105.211.69	10.127.196.171	HTTP	GET /webauth/aup.html HTTP/1.1
2363	15:11:38.623960	10.127.196.171	10.105.211.69	HTTP	HTTP/1.1 304 Not Modified
2364	15:11:38.623960	10.105.211.69	10.127.196.171	TCP	54381 → 80 [ACK] Seq=1706 Ack=2023 Win=261952 Len=0
2747	15:12:04.280976	10.76.118.70	10.197.224.122	RADIUS	Access-Request id=0
2751	15:12:04.682963	10.197.224.122	10.76.118.70	RADIUS	Access-Accept id=0
2836	15:12:09.729957	10.105.211.69	10.127.196.171	HTTP	GET /webauth/logout.html HTTP/1.1
2837	15:12:09.731956	10.127.196.171	10.105.211.69	HTTP	HTTP/1.1 304 Not Modified
2838	15:12:09.731956	10.105.211.69	10.127.196.171	TCP	54381 → 80 [ACK] Seq=2186 Ack=2166 Win=261952 Len=0
4496	15:13:07.964946	10.105.211.69	10.127.196.171	TCP	54381 → 80 [FIN, ACK] Seq=2186 Ack=2166 Win=262144 Len=0
4497	15:13:07.964946	10.127.196.171	10.105.211.69	TCP	80 → 54381 [FIN, ACK] Seq=2166 Ack=2187 Win=2097408 Len=0
4498	15:13:07.965938	10.105.211.69	10.127.196.171	TCP	54381 → 80 [ACK] Seq=2187 Ack=2167 Win=262144 Len=0

Client sends a HTTP GET request to the portal page and completes the authentication successfully

Radius Access Request packet

2747	15:12:04.280976	10.76.118.70	10.197.224.122	RADIUS	Access-Request id=0
------	-----------------	--------------	----------------	--------	---------------------

```

> Frame 2747: 405 bytes on wire (3240 bits), 405 bytes captured (3240 bits)
> Ethernet II, Src: Cisco_59:31:4b (f4:bd:9e:59:31:4b), Dst: Cisco_34:90:cb (6c:5e:3b:34:90:cb)
> Internet Protocol Version 4, Src: 10.76.118.70, Dst: 10.197.224.122
> User Datagram Protocol, Src Port: 60222, Dst Port: 1812
√ RADIUS Protocol
  Code: Access-Request (1)
  Packet identifier: 0x0 (0)
  Length: 363
  Authenticator: e3018f5d8e52fccbe0d703da1a209e6
  [The response to this request is in frame 2751]
  Attribute Value Pairs
    > AVP: t=Calling-Station-Id(31) l=19 val=a0-ce-c8-c3-a9-b5
    > 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=10.105.211.69
    > AVP: t=Message-Authenticator(80) l=18 val=6f469fa30834350d2aed4e4b226cddf7
    > 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
    > AVP: t=Vendor-Specific(26) l=32 vnd=ciscoSystems(9)
    > AVP: t=Vendor-Specific(26) l=20 vnd=ciscoSystems(9)
    > AVP: t=NAS-IP-Address(4) l=6 val=10.76.118.70
    > AVP: t=NAS-Port-Type(61) l=6 val=Virtual(5)

```

Access Request Packet

Radius Access Accept Packet

