Configure Guest Anchor for Guest Access Services with Catalyst 9800 and AireOS IRCM Controllers

The Wireless Guest Access model addresses the need to provide internet access to guests in a secure and accountable manner. While there can be many different deployments, this section focuses on the implementation of wireless guest networking using a combination of controllers that includes a Foreign Anchor solution. It has a mixed deployment where Catalyst 9800, Cisco AireOS 8.8.111 (or 8.5-based IRCM Image) and Cisco AireOS 8.2/8.3/8.5 controllers co-exist and have designated roles for anchor and foreign depending upon the setup. In addition to one controller being designated as a guest anchor, the guest deployment may or may not have additional controllers in the DMZ for load balancing.

Table 1: Workflow to promote mobility in guest deployment scenario using a guest anchor

Step	Configuration
Mandatory	Ensure that you have configured a VLAN and assigned an interface for guest traffic. See Configure VLAN for more information.

Step	Configuration
Mandatory	Ensure that you have configured a Guest WLAN. See Configure WLAN and Associated Settings for more information. The guest WLAN is configured on every foreign controller that manages APs where guest access is required. Even though the anchor controller(s) is not specifically used to manage APs associated with a guest WLAN, it must also be configured with the guest WLAN because the anchor controller is a logical extension of the WLAN where user traffic is ultimately bridged (using CAPWAP between the AP and the foreign controller, and Secure Mobility/ EoIP between the foreign controller and the anchor controller) to an interface/VLAN on the anchor controller. **Note** It is extremely important to note that all parameters defined in the WLAN Security, QoS, and Advanced settings tabs, must be configured identically in both the anchor and foreign controllers. See Ensure Identical Parameter Configuration on Peer Controllers for more information.

Step	Configuration
Mandatory	Ensure that you have set up mobility groups that will be part of this deployment. There can be many possible combinations, only some of the cases are detailed below. Configure the mobility group as per your requirement. **Note** It is important to configure peer controllers to tunnel the traffic from one controller to another. However, when you are trying to set up the guest controller in the DMZ as an anchor controller, the mobility group name with the peer controller does not have to match, as usually the anchor controller will not have APs attached and clients cannot roam from one controller to the other in a DMZ. Setting up the peers ensures that the client can access a guest WLAN throughout an enterprise but still be restricted to a specific subnet. See Configure Mobility Groups between Catalyst 9800 and Cisco AireOS (IRCM image) Controllers for Secure Mobility OR See Configure Mobility Groups between Catalyst 9800 and AireOS 8.8.111 (or 8.5-based IRCM Image) Controller for Secure Mobility
Mandatory	Configure the mobility anchor based on your deployment setup. Choose from the following available choices listed in this document. Configure Mobility Anchors using the CLI, on page 4 Configure Mobility Anchors using the GUI, on page 23 • Configure a Catalyst 9800 as Anchor with another Catalyst 9800 as Foreign Controller • Configure Catalyst 9800 as Anchor and AireOS Controller (IRCM image) as Foreign Controller • Configure AireOS (IRCM Image) Controller as Anchor with Catalyst 9800 as Foreign Controller • Configure AireOS Controller (IRCM image) as Anchor and AireOS as Foreign Controller

Step	Configuration
Optional	Configure load balancing if you have more than one Catalyst 9800 controller in the DMZ. OR Configure load balancing if you have more than one AireOS controller (IRCM image) in the DMZ.
Optional	Verify the configuration.

- Configure Mobility Anchors using the CLI, on page 4
- Configure Mobility Anchors using the GUI, on page 23

Configure Mobility Anchors using the CLI

Mobility Anchor, also referred to as Guest tunneling or Auto Anchor Mobility, is a feature where all the client traffic that belongs to a WLAN (specially Guest WLAN) is tunneled to a predefined controller or set of controllers that are configured as Anchor for that specific WLAN. This feature helps to restrict clients to a specific subnet and have more control over the user traffic.

Using a mobility anchor forces clients to be anchored to a controller other than the one they first associate with. This forces their traffic to be tunneled to the DMZ. Then it must pass through the firewall and its associated policies before getting anywhere. This is done on a per-WLAN basis.

- Anchor Controller - Refers to one or more controllers deployed in the enterprise DMZ that are used to perform guest mobility secure/EoIP tunnel termination, web redirection, and user authentication.
- Foreign Controller - Refers to one or more controllers deployed in the enterprise that are used to perform guest mobility secure tunnel termination, web redirection, and user authentication.

Configure a Catalyst 9800 as Anchor with another Catalyst 9800 as Foreign Controller

This task is required when you designate the Catalyst 9800 in the DMZ as Guest Anchor and the Catalyst 9800 in the enterprise as the Foreign Controller.

Before you begin

- Create a WLAN Profile for guests that defines the SSID name and profile and all the security settings on both the Catalyst 9800 controllers.
- Create a policy profile.
- Ensure that the above configurations match on the peer controllers.
- Build a mobility tunnel between the Foreign Catalyst 9800 controller and Anchor Catalyst 9800 controller.

First, log in to the foreign 9800 controller and define the anchor 9800 controller's ip address under the policy profile.

Step 1 **enable**

Example:

```
Device>enable
```

Enables privileged EXEC mode. Enter your password, if prompted.

Step 2 **configure terminal**

Example:

```
Device#configure terminal
```

Enters global configuration mode.

Step 3 **wireless profile policy** *name of anchor-policy*

Example:

```
Device(config)#wireless profile policy anchor-policy
```

Configures WLAN policy profile and enters the wireless policy configuration mode.

Step 4 **mobility anchor** *anchor-ip-address priority number*

Example:

```
Device(config-wireless-policy)#mobility anchor 10.88.173.49 priority 3
```

Defines anchor 9800 ip address on the foreign controller.

Step 5 **central switching**

Example:

```
Device(config-wireless-policy)#central switching
```

Enables Central switching.

Step 6 **vlan***vlan-id*

Example:

```
Device(config-wireless-policy)#vlan 16
```

Configures a VLAN name or VLAN ID.

Step 7 **no shutdown**

Example:

```
Device(config-wireless-policy)#no shutdown
```

Enables the policy profile.

Step 8 **exit**

Example:

```
Device(config-wireless-policy)#exit
```

Exits the configuration mode and returns to privileged EXEC mode.

What to do next

Link the Policy Profile with the WLAN inside the Policy Tag , on page 6

Link the Policy Profile with the WLAN inside the Policy Tag

This task is required after you have created an anchor policy profile. Link the Policy Profile with the WLAN inside the Policy Tag assigned to the APs associated to the foreign controller that service this WLAN.

Before you begin

Ensure that you have created a anchor policy profile.

On the 9800 controller:

Step 1 **enable**

Example:

```
Device>enable
```

Enables privileged EXEC mode. Enter your password, if prompted.

Step 2 **configure terminal**

Example:

```
Device#configure terminal
```

Enters global configuration mode.

Step 3 **wireless tag policy** *name of policy tag*

Example:

```
Device(config)#wireless tag policy PT1
```

Configures the policy tag and enters the wireless policy configuration mode.

Step 4 **wlan** *name of WLAN profile* **policy** *name of policy profile*

Example:

```
Device(config-policy-tag)#wlan anchor-ssid policy anchor-policy
```

Creates a new policy tag or edits an existing one to link the Policy Profile with the WLAN inside the Policy Tag. This tag is assigned to the APs associated with the foreign controller that service this WLAN.

Step 5 **exit**

Exits the configuration mode and returns to privileged EXEC mode.

What to do next

Configure the AireOS controller as the guest anchor controller .

Configure settings on the 9800 Anchor Controller

This task is required after you have configured the anchor controller settings on the foreign 9800 controller. Now, log in to the 9800 anchor controller and configure the settings to match the 9800 foreign controller settings.

- Create the anchor policy profile - this name must match the name on the 9800 foreign controller.
- Enable the export anchor on the anchor controller. This instruct this 9800 controller that it is the anchor 9800 WLC for any WLAN that uses that Policy Profile. When the foreign 9800 controller sends the clients to the anchor 9800 WLC, it informs about the WLAN and the Policy Profile that the client is assigned to, so the anchor 9800 WLC knows which local Policy Profile to use.

Before you begin

- Create a WLAN Profile for guests that define the SSID name and profile and all the security settings on both the Catalyst 9800 controllers.
- Create a policy profile.
- Ensure that the above configurations match on the peer controllers.
- Build a mobility tunnel between the Foreign Catalyst 9800 controller and Anchor Catalyst 9800 controller.

Follow the steps below:

Step 1 **enable**

Example:

```
Device>enable
```

Enables privileged EXEC mode. Enter your password, if prompted.

Step 2 **configure terminal**

Example:

```
Device#configure terminal
```

Enters global configuration mode.

Step 3 **wireless profile policy***name of anchor-policy*

Example:

```
Device(config)#wireless profile policy anchor-policy
```

Configures WLAN policy profile and enters the wireless policy configuration mode.

Step 4 **mobility anchor**

Example:

```
Device(config-wireless-policy)#mobility anchor
```

Configures this 9800 controller as the anchor controller.

Step 5 **vlan***vlan-id*

Example:

```
Device(config-wireless-policy)#vlan 16
```

Configures a VLAN name or VLAN ID.

Step 6 **no shutdown**

Example:

```
Device(config-wireless-policy)#no shutdown
```

Enables the policy profile.

Step 7 **exit**

Example:

```
Device(config-wireless-policy)#exit
```

Exits the configuration mode and returns to privileged EXEC mode.

Step 8 **show wireless mobility summary**

Need sample output

Step 9 **show wireless client mac <> detail**

Need sample output

What to do next

On 9800 controllers, you can use the following commands to verify the configuration and the state of the wireless clients using a foreign/anchor SSID.

```
Device#show wireless client summary
```

Configure Catalyst 9800 Controller as Anchor and AireOS Controller (IRCM image) as Foreign Controller

This task is required when you are setting up the Catalyst 9800 controller as the guest anchor in the DMZ and the AireOS controller (IRCM image) as the foreign controller in the campus/enterprise.

Before you begin

Ensure that you have set up the Mobility Tunnel between the peer controllers.

On the Catalyst 9800 anchor controller do the following:

Step 1 **enable**

Example:

```
Device>enable
```

Enables privileged EXEC mode. Enter your password, if prompted.

Step 2 **configure terminal**

Example:

```
Device#configure terminal
```

Enters global configuration mode.

Step 3 **wireless profile policy** *name of anchor-policy*

Example:

```
Device(config)#wireless profile policy anchor policy
```

Configures WLAN policy profile and enters the wireless policy configuration mode. Creates the anchor policy profile on the 9800 anchor controller. This instructs this Catalyst 9800 controller that it is the anchor 9800 controller for any WLAN that uses that Policy Profile. When the foreign AireOS controller sends the clients to the anchor 9800 controller, it informs about the WLAN name that the client is assigned to, so the anchor 9800 controller knows which local WLAN configuration to use and it also uses this name to know which local Policy Profile to use.

Step 4 **mobility anchor**

Example:

```
Device(config-wireless-policy)#mobility anchor
```

Configures this 9800 controller as the anchor controller.

Step 5 **vlan***vlan-id*

Example:

```
Device(config-wireless-policy)#vlan 16
```

Configures a VLAN name or VLAN ID.

Step 6 **no shutdown**

Example:

```
Device(config-wireless-policy)#no shutdown
```

Enables the policy profile.

Step 7 **exit**

Example:

```
Device(config-wireless-policy)#exit
```

Exits the configuration mode and returns to privileged EXEC mode.

What to do next

Configure AireOS Controller (IRCM image) as Foreign Controller, on page 9

Configure AireOS Controller (IRCM image) as Foreign Controller

This task is required after you have configured the 9800 anchor controller. Now, log in to the AireOS foreign controller and configure the settings, so that when the foreign AireOS controller sends the clients to the anchor 9800 controller, it can inform about the WLAN name that the client is assigned to, for the anchor controller to know which local WLAN configuration to use.

Before you begin

Ensure that you have set up the Mobility Tunnel between the peer controllers.

On the AireOS (IRCM image) controller,configure the following:

Step 1 **config wlan disable** *wlan-id*

Example:

```
Device >config wlan disable 2
```

Disables the SSID on the foreign AireOS controller. This clears up any associated configurations for this SSID/WLAN.

Step 2 **config wlan mobility anchor add** *wlan-id9800 controller's management interface*

Example:

```
Device >config wlan mobility anchor add 2 10.88.173.105
```

Adds the 9800 controller as the anchor for this SSID/WLAN.

Step 3 **config wlan enable** *wlan-id*

Example:

```
Device >wlan 2
```

Enables the WLAN ID to receive clients.

What to do next

On 9800 controllers, you can use the following commands to verify the configuration and the state of the wireless clients using a foreign/anchor SSID.

To show the wlan configuration information:

```
Device#show run wlan
wlan wlan1 1 wlan1
 dot11ax target-waketime
 dot11ax twt-broadcast-support
wlan wlan2 2 wlan2
 dot11ax target-waketime
 dot11ax twt-broadcast-support
```

To display a summary of all WLANs configured on the controller:

```
Device#show wlan summary

Number of WLANs: 2

ID   Profile Name                      SSID                              Status Security

-----------------------------------------------------------------------------------------------------

1    wlan1                             wlan1                             DOWN
[WPA2][802.1x][AES]

2    wlan2                             wlan2                             DOWN
[WPA2][802.1x][AES]
```

Verify the client state on the controller:

```
Device#show wireless client summary
Number of Clients: 1

MAC Address    AP Name                                        Type ID   State
Protocol Method     Role
------------------------------------------------------------------------------------------
6038.e00b.011a AP687D.B45C.1300                               WLAN 1    Run
11n(5)   None       Foreign

Number of Excluded Clients: 0

eWLC-IRCM-C1#
8520:  {'Number of Clients': '1', 'Number of Excluded Clients': '0'}
8521:  +++ eWLC-IRCM-C1 with alias 'a': executing command 'show wireless client summary'
+++
show wireless client summary
Number of Clients: 1

MAC Address    AP Name                                        Type ID   State
Protocol Method     Role
------------------------------------------------------------------------------------------
6038.e00b.011a AP687D.B45C.1300                               WLAN 1    Run
11n(5)   None       Foreign

Number of Excluded Clients: 0
```

```
Device#show wireless mobility summary
```

```
Device#show ap tag summary
```

```
show ap summary

Number of APs.................................... 2

Global AP User Name.............................. Cisco123
Global AP Dot1x User Name........................ Not Configured
Global AP Dot1x EAP Method....................... EAP-FAST

AP Name                         Slots  AP Model              Ethernet MAC       Location
            Country     IP Address       Clients  DSE Location
------------------------------  -----  --------------------  -----------------
--------------------  ----------  ---------------  -------  --------------
APA0B4.3969.ADA6                3      AIR-AP3802I-B-K9       a0:b4:39:69:ad:a6  default
location      US          10.14.117.201    0        [0 ,0 ,0 ]
AP00A2.8900.3660                3      AIR-AP1852I-B-K9       00:a2:89:00:36:60  default
location      US          10.14.117.202    0        [0 ,0 ,0 ]
```

```
Device#show ap <ap-name> tag detail
```

```
Device#show wlan { summary | id | name | all }
```

```
Device#show wireless tag policy detailed <policy-tag-name>
```

```
Device#show wireless profile policy detailed <policy-profile-name>
```

On AireOS controllers, you can use the following commands to verify the configuration and the state of the wireless clients using a foreign/anchor SSID.

To see the wlans and the details, configured on this controller:

```
Device >show wlan summary

Number of WLANs.................................. 4

WLAN ID  WLAN Profile Name / SSID                                                 Status
  Interface Name        PMIPv6 Mobility
```

```
-------  -----------------------------------------------------------------------  --------
  --------------------  ---------------
1        testlab1-mob / testlab1-mob                                              Enabled
  management            none
2        testlab1-anchor-108 / testlab1-anchor-108                                Disabled
  management            none
3        testlab1-anchor-109 / testlab1-anchor-109                                Disabled
  management            none
4        testlab1-mob-psk / testlab1-mob-psk                                      Enabled
  management            none
```

To see more details of a particular wlan configured on this controller:

```
Device >show wlan 1


WLAN Identifier.................................. 1
Profile Name..................................... testlab1
Network Name (SSID).............................. testlab1
Status........................................... Enabled
MAC Filtering.................................... Disabled
Broadcast SSID................................... Enabled
AAA Policy Override.............................. Disabled
Network Admission Control
Client Profiling Status
    Radius Profiling ............................ Disabled
     DHCP ....................................... Disabled
     HTTP ....................................... Disabled
    Local Profiling ............................. Disabled
     DHCP ....................................... Disabled
     HTTP ....................................... Disabled
  Radius-NAC State............................... Disabled
  SNMP-NAC State................................. Disabled
  Quarantine VLAN................................ 0
Maximum Clients Allowed.......................... Unlimited
Security Group Tag............................... Unknown(0)
Maximum number of Clients per AP Radio........... 200
ATF Policy....................................... 0
Number of Active Clients......................... 0
Exclusionlist Timeout............................ 180 seconds
Session Timeout.................................. 86400 seconds
User Idle Timeout................................ Disabled
Sleep Client..................................... disable
Sleep Client Timeout............................. 720 minutes
Web Auth Captive Bypass Mode..................... None
User Idle Threshold.............................. 0 Bytes
NAS-identifier................................... none
CHD per WLAN..................................... Enabled
Webauth DHCP exclusion........................... Disabled
Interface........................................ management
Multicast Interface.............................. Not Configured
WLAN IPv4 ACL.................................... unconfigured
WLAN IPv6 ACL.................................... unconfigured
WLAN Layer2 ACL.................................. unconfigured
WLAN URL ACL..................................... unconfigured
mDNS Status...................................... Disabled
mDNS Profile Name................................ default-mdns-profile
DHCP Server...................................... Default
Central NAT Peer-Peer Blocking................... Unknown
DHCP Address Assignment Required................. Disabled
Static IP client tunneling....................... Disabled
Tunnel Profile................................... Unconfigured
PMIPv6 Mobility Type............................. none
    PMIPv6 MAG Profile........................... Unconfigured
    PMIPv6 Default Realm......................... Unconfigured
    PMIPv6 NAI Type.............................. Hexadecimal
    PMIPv6 MAG location.......................... WLC
Quality of Service............................... Silver
Per-SSID Rate Limits............................. Upstream Downstream
Average Data Rate................................   0    0
Average Realtime Data Rate.......................   0    0
Burst Data Rate..................................   0    0
Burst Realtime Data Rate.........................   0    0
Per-Client Rate Limits........................... Upstream Downstream
Average Data Rate................................   0    0
Average Realtime Data Rate.......................   0    0
Burst Data Rate..................................   0    0
Burst Realtime Data Rate.........................   0    0
Scan Defer Priority.............................. 4,5,6
Scan Defer Time.................................. 100 milliseconds
WMM.............................................. Allowed
WMM UAPSD Compliant Client Support............... Disabled
Media Stream Multicast-direct.................... Disabled
CCX - AironetIe Support.......................... Enabled
CCX - Gratuitous ProbeResponse (GPR)............. Disabled
CCX - Diagnostics Channel Capability............. Disabled
Dot11-Phone Mode (7920).......................... Disabled
Wired Protocol................................... 802.1P (Tag=0)
Passive Client Feature........................... Disabled
Peer-to-Peer Blocking Action..................... Disabled
Radio Policy..................................... All
DTIM period for 802.11a radio.................... 1
DTIM period for 802.11b radio.................... 1
Radius Servers
   Authentication................................ Global Servers
   Accounting.................................... Global Servers
      Interim Update............................. Enabled
      Interim Update Interval.................... 0
      Framed IPv6 Acct AVP ...................... Prefix
   Dynamic Interface............................. Disabled
   Dynamic Interface Priority.................... wlan
Local EAP Authentication......................... Disabled
Radius NAI-Realm................................. Disabled
Mu-Mimo.......................................... Enabled
Security
   802.11 Authentication:........................ Open System
   FT Support.................................... Disabled
   Static WEP Keys............................... Disabled
   802.1X........................................ Disabled
   Wi-Fi Protected Access (WPA/WPA2)............. Disabled
   Wi-Fi Direct policy configured................ Disabled
   EAP-Passthrough............................... Disabled
   CKIP ......................................... Disabled
   Web Based Authentication...................... Disabled
   Web Authentication Timeout.................... 300
   Web-Passthrough............................... Disabled
   Mac-auth-server............................... 0.0.0.0
   Web-portal-server............................. 0.0.0.0
   qrscan-des-key................................
   Conditional Web Redirect...................... Disabled
   Splash-Page Web Redirect...................... Disabled
   Auto Anchor................................... Enabled
   FlexConnect Local Switching................... Disabled
   FlexConnect Central Association............... Disabled
   flexconnect Central Dhcp Flag................. Disabled
   flexconnect nat-pat Flag...................... Disabled
   flexconnect Dns Override Flag................. Disabled
   flexconnect PPPoE pass-through................ Disabled
   flexconnect local-switching IP-source-guar.... Disabled
   FlexConnect Vlan based Central Switching ..... Disabled
   FlexConnect Local Authentication.............. Disabled
   FlexConnect Learn IP Address.................. Enabled
  Client MFP................................... Optional but inactive (WPA2 not configured)

   PMF........................................... Disabled
   PMF Association Comeback Time................. 1
   PMF SA Query RetryTimeout..................... 200
   Tkip MIC Countermeasure Hold-down Timer....... 60
   Eap-params.................................... Not Applicable
AVC Visibilty.................................... Disabled
AVC Profile Name................................. None
OpenDns Profile Name............................. None
OpenDns Wlan Mode................................ ignore
Flow Monitor Name................................ None
Split Tunnel Configuration
    Split Tunnel................................. Disabled
Call Snooping.................................... Disabled
Roamed Call Re-Anchor Policy..................... Disabled
SIP CAC Fail Send-486-Busy Policy................ Enabled
SIP CAC Fail Send Dis-Association Policy......... Disabled
KTS based CAC Policy............................. Disabled
Assisted Roaming Prediction Optimization......... Disabled
802.11k Neighbor List............................ Enabled
802.11k Neighbor List Dual Band.................. Disabled
802.11v Directed Multicast Service............... Enabled
802.11v BSS Max Idle Service..................... Enabled
802.11v BSS Transition Service................... Enabled
802.11v BSS Transition Disassoc Imminent......... Disabled
802.11v BSS Transition Disassoc Timer............ 200
802.11v BSS Transition OpRoam Disassoc Timer..... 40
DMS DB is empty
Band Select...................................... Disabled
Load Balancing................................... Disabled
Multicast Buffer................................. Disabled
Universal Ap Admin............................... Disabled
Broadcast Tagging................................ Disabled
PRP.............................................. Disabled

 Mobility Anchor List
 WLAN ID     IP Address           Status                               Priority
 -------     ---------------      ------                               --------
 1           9.11.41.108          Up                                    3


802.11u........................................ Disabled

MSAP Services.................................. Disabled

Local Policy
----------------
Priority  Policy Name
--------  ---------------

Lync State ...................................... Disabled
Audio QoS Policy................................. Silver
Video QoS Policy................................. Silver
App-Share QoS Policy............................. Silver
File Transfer QoS Policy......................... Silver
Lync State ...................................... Disabled
Audio QoS Policy................................. Silver
Video QoS Policy................................. Silver
App-Share QoS Policy............................. Silver
File Transfer QoS Policy......................... Silver
File Transfer QoS Policy........................ Silver
QoS Fastlane Status............................. Disable
Selective Reanchoring Status.................... Disable
Lobby Admin Access.............................. Disabled

 Fabric Status
--------------

Fabric status................................... Disable
Vnid Name.......................................
Vnid............................................ 0
Applied SGT Tag................................. 0
Peer Ip Address................................. 0.0.0.0
Flex Acl Name...................................
Flex Avc Policy Name............................

U3-Interface................................. Disable

U3-Reporting Interval......................... 30
```

Configure AireOS(withIRCM Image)Controller as Anchor with Catalyst 9800 as Foreign Controller

This task is required when you are setting up the AireOS controller as the guest anchor in the DMZ and the Catalyst 9800 as the foreign controller in the campus/enterprise. On the 9800 controller:

Before you begin

Ensure that you have set up the Mobility Tunnel between the peer controllers.

Step 1 **enable**

Example:

```
Device>enable
```

Enables privileged EXEC mode. Enter your password, if prompted.

Step 2 **configure terminal**

Example:

```
Device#configure terminal
```

Enters global configuration mode.

Step 3 **wireless profile policy** *name of anchor-policy*

Example:

```
Device(config)#wireless profile policy policy_anchored_t6
```

Creates the anchor policy profile and enters the wireless policy configuration mode.

Step 4 **mobility anchor** *anchor-ip-address priority number*

Example:

```
Device(config-wireless-policy)#mobility anchor 192.168.5.56 priority 3
```

Defines AireOS ip address as anchor on the foreign controller. Now, the 9800 controller forwards the traffic of the SSID associated with this Policy Profile to the selected AireOS anchor.

Step 5 **no shutdown**

Enables the interface.

Step 6 **exit**

Exits the configuration mode and returns to privileged EXEC mode.

What to do next

Link the Policy Profile with the WLAN inside the Policy Tag , on page 16

Link the Policy Profile with the WLAN inside the Policy Tag

This task is required after you have created an anchor policy profile. Link the Policy Profile with the WLAN inside the Policy Tag assigned to the APs associated to the foreign controller that service this WLAN. On the 9800 controller:

Before you begin

Ensure that you have created a anchor policy profile.

Step 1 **enable**

Example:

```
Device>enable
```

Enables privileged EXEC mode. Enter your password, if prompted.

Step 2 **configure terminal**

Example:

```
Device#configure terminal
```

Enters global configuration mode.

Step 3 **wireless tag policy** *name of policy tag*

Example:

```
Device(config)#wireless tag policy PT2
```

Configures the policy tag and enters the wireless policy configuration mode.

Step 4 **wlan** *name of WLAN profile* **policy** *name of policy profile*

Example:

```
Device(config-policy-tag)#wlan ANCHOR_IRCM policy policy_anchored_t6
```

Creates a new policy tag or edits an existing one to link the Policy Profile with the WLAN inside the Policy Tag. This tag is assigned to the APs associated with the foreign controller that service this WLAN.

Step 5 **exit**

Exits the configuration mode and returns to privileged EXEC mode.

What to do next

Configure AireOS Controller (with IRCM image) as Guest Anchor Controller, on page 17

Configure AireOS Controller (with IRCM image) as Guest Anchor Controller

This task is required when you are setting up the AireOS controller controller as the guest anchor in the DMZ and the Catalyst 9800 as the foreign controller in the campus/enterprise. After you have configured the anchor policy profile on 9800, on the AireOS controller:

Before you begin

Ensure that you have set up the Mobility Tunnel between the peer controllers.

Step 1 **config wlan mobility anchor add** *wlan_id aireos anchor_controller_ip_address* **priority** *priority-number*

Example:

```
Device >config wlan mobility anchor add 27 192.168.5.56 priority 3
```

Configures the AireOS controller as anchor controller and assigns it a priority number for load balancing.

Step 2 **save config**

Example:

```
Device >save config
```

Step 3 **show mobility anchor {wlan | guest-lan}** *{wlan_id | guest_lan_id}*

Example:

```
Device >show mobility anchor

Mobility Anchor Export List


 Priority number, 1=Highest priority and 3=Lowest priority(default).

 WLAN ID     IP Address           Status                              Priority
 -------     ---------------      ------                              --------
 1           9.11.41.108          Up                                    1

 2           9.11.41.108          Up                                    2

 27          192.168.5.56         Up                                    3


 GLAN ID     IP Address           Status
 -------     ---------------      ------
```

What to do next

Verify the configuration on the 9800 controller.

```
# show run wlan
# show wlan summary
# show wireless client summary
# show wireless mobility summary
# show ap tag summary
# show ap <ap-name> tag detail
# show wlan { summary | id | name | all }
# show wireless tag policy detailed <policy-tag-name>
# show wireless profile policy detailed <policy-profile-name>
```

The client summary status on the 9800 foreign controller

```
Device#sh wireless client summary
Load for five secs: 1%/0%; one minute: 0%; five minutes: 0%
Time source is NTP, 10:53:13.762 CET Fri Dec 3 2021
Number of Clients: 3

MAC Address    AP Name                          Type ID   State          Protocol Method     Role
------------------------------------------------------------------------------------------------------------------------
08cc.68bc.15ae AP9120-2-r3-sw2-Gi1-0-39                 WLAN 1    Run            11n(5)   None      Local
6c40.0899.0466 AP9120-2-r3-sw2-Gi1-0-39                 WLAN 27   Run            11ac     None      Export Foreign

6c41.6a0d.2e90 AP9120-2-r3-sw2-Gi1-0-39                 WLAN 1    IP Learn       11n(5)   None      Local
```

The client summary status on the AireOS anchor controller

```
Device >show client summary

Number of Clients................................ 1

Number of PMIPV6 Clients......................... 0

Number of EoGRE Clients.......................... 0

                                                                GLAN/
                                                                RLAN/
MAC Address       AP Name                        Slot Status        WLAN  Auth Protocol
      Port Wired Tunnel  Role
----------------- ----------------------------- ---- ------------- ----- ----
---------------- ---- ----- ------- ----------------
6c:40:08:99:04:66 192.168.25.41                  N/A Associated     27   Yes  Mobile
      13   No    No      Export Anchor
```

The client details for a particular client on the Catalyst 9800 controller

```
Device#sh wi cli mac 6c40.0899.0466 detail
Load for five secs: 0%/0%; one minute: 0%; five minutes: 0%
Time source is NTP, 10:53:59.778 CET Fri Dec 3 2021


Client MAC Address : 6c40.0899.0466
Client MAC Type : Universally Administered Address
Client IPv4 Address : 4.41.0.46
Client IPv6 Addresses : fe80::6e40:8ff:fe99:466
                        2001:4:4:4:cc8:ce83:d5e6:12f6
                        2001:4:4:4:6e40:8ff:fe99:466
Client Username: N/A
AP MAC Address : d4e8.8019.f140
AP Name: AP9120-2-r3-sw2-Gi1-0-39
AP slot : 1
Client State : Associated
Policy Profile : policy_anchored_t6
Flex Profile : N/A
Wireless LAN Id: 27
WLAN Profile Name: ANCHOR_IRCM
Wireless LAN Network Name (SSID): ANCHOR_IRCM
BSSID : d4e8.8019.f14d
Connected For : 58 seconds
Protocol : 802.11ac
Channel : 60
Client IIF-ID : 0xa0000002
Association Id : 1
Authentication Algorithm : Open System
Idle state timeout : N/A
Session Timeout : 1800 sec (Remaining time: 1747 sec)
Session Warning Time : Timer not running
Input Policy Name  : None
Input Policy State : None
Input Policy Source : None
Output Policy Name  : None
Output Policy State : None
Output Policy Source : None
WMM Support : Enabled
U-APSD Support : Enabled
  U-APSD value : 0
  APSD ACs    : BK, BE, VI, VO
Fastlane Support : Disabled
Client Active State : Active
Power Save : ON
Current Rate : m9 ss3
Supported Rates : 18.0,36.0,48.0,54.0
AAA QoS Rate Limit Parameters:
  QoS Average Data Rate Upstream             : 0 (kbps)
  QoS Realtime Average Data Rate Upstream    : 0 (kbps)
  QoS Burst Data Rate Upstream               : 0 (kbps)
  QoS Realtime Burst Data Rate Upstream      : 0 (kbps)
  QoS Average Data Rate Downstream           : 0 (kbps)
  QoS Realtime Average Data Rate Downstream  : 0 (kbps)
  QoS Burst Data Rate Downstream             : 0 (kbps)
  QoS Realtime Burst Data Rate Downstream    : 0 (kbps)
Mobility:
  Anchor IP Address           : 192.168.5.56
  Point of Attachment         : 0x9000000F
  Point of Presence           : 0xA0000001
  AuthC status                : False
  Move Count                  : 0
  Mobility Role               : Export Foreign
  Mobility Roam Type          : L3 Requested
  Mobility Complete Timestamp : 12/03/2021 10:53:05 CET
Client Join Time:
  Join Time Of Client : 12/03/2021 10:53:02 CET
Client State Servers : None
Client ACLs : None
Policy Manager State: Run
Last Policy Manager State : IP Learn Complete
Client Entry Create Time : 55 seconds
Policy Type : WPA2
Encryption Cipher : CCMP (AES)
Authentication Key Management : PSK
```

```
AAA override passphrase : No
User Defined (Private) Network : Disabled
User Defined (Private) Network Drop Unicast : Disabled
Encrypted Traffic Analytics : No
Protected Management Frame - 802.11w : No
EAP Type : Not Applicable
VLAN Override after Webauth : No
VLAN : 169
Multicast VLAN : 0
Anchor VLAN : 504
WiFi Direct Capabilities:
  WiFi Direct Capable           : No
Central NAT : DISABLED
Session Manager:
  Point of Attachment : capwap_9000000f
  IIF ID             : 0x9000000F
  Authorized         : TRUE
  Session timeout    : 1800
  Common Session ID: 2919A8C00000000B7FB6204E
  Acct Session ID  : 0x00000000
  Auth Method Status List
        Method : None
  Local Policies:
        Service Template : wlan_svc_policy_anchored_t6_local (priority 254)
                VLAN             : 169
                Absolute-Timer   : 1800
  Server Policies:
  Resultant Policies:
                VLAN Name        : VLAN0169
                VLAN             : 169
                Absolute-Timer   : 1800
DNS Snooped IPv4 Addresses : None
DNS Snooped IPv6 Addresses : None
Client Capabilities
  CF Pollable : Not implemented
  CF Poll Request : Not implemented
  Short Preamble : Not implemented
  PBCC : Not implemented
  Channel Agility : Not implemented
  Listen Interval : 0
Fast BSS Transition Details :
  Reassociation Timeout : 20
11v BSS Transition : Not implemented
11v DMS Capable : No
QoS Map Capable : No
FlexConnect Data Switching : N/A
FlexConnect Dhcp Status : N/A
FlexConnect Authentication : N/A
FlexConnect Central Association : N/A
Client Statistics:
  Number of Bytes Received : 24115
  Number of Bytes Sent : 8301
  Number of Packets Received : 102
  Number of Packets Sent : 33
  Number of Policy Errors : 0
  Radio Signal Strength Indicator : -40 dBm
  Signal to Noise Ratio : 49 dB
Fabric status : Disabled
Radio Measurement Enabled Capabilities
  Capabilities: None
Client Scan Report Time : Timer not running
Client Scan Reports
Assisted Roaming Neighbor List
Nearby AP Statistics:
```

```
EoGRE : Pending Classification
Device Type      : Apple-Device
Device Name      : APPLE, INC.
Protocol Map     : 0x000001  (OUI)
Max Client Protocol Capability: 802.11ac Wave 2
Cellular Capability : N/A
```

The client details for a particular client on the AireOS controller after the L3 roam.

```
Device >show client detail 6c:40:08:99:04:66
Client MAC Address............................... 6c:40:08:99:04:66
Client Username ................................. N/A
AP MAC Address................................... d4:e8:80:19:f1:40
AP Name.......................................... N/A
AP radio slot Id................................. N/A
Client State..................................... Associated
Client User Group................................
Client NAC OOB State............................. Access
Wireless LAN Id.................................. 27
Wireless LAN Network Name (SSID)................. ANCHOR_IRCM
Wireless LAN Profile Name........................ ANCHOR_IRCM
Hotspot (802.11u)................................ Not Supported
BSSID............................................ 00:00:00:00:00:ff
Connected For ................................... 73 secs
Channel.......................................... N/A
IP Address....................................... 4.41.0.46
Gateway Address.................................. 4.0.0.1
Netmask.......................................... 255.0.0.0
IPv6 Address..................................... fe80::6e40:8ff:fe99:466
IPv6 Address..................................... 2001:4:4:4:cc8:ce83:d5e6:12f6
IPv6 Address..................................... 2001:4:4:4:6e40:8ff:fe99:466
Association Id................................... 0
Authentication Algorithm......................... Open System
Reason Code...................................... 1
Status Code...................................... 0
Session Timeout.................................. 1800
Client CCX version............................... No CCX support
QoS Level........................................ Silver
Avg data Rate.................................... 0
Burst data Rate.................................. 0
Avg Real time data Rate.......................... 0
Burst Real Time data Rate........................ 0
Avg Uplink data Rate............................. 0
Burst Uplink data Rate........................... 0
Avg Uplink Real time data Rate................... 0
Burst Uplink Real Time data Rate................. 0
802.1P Priority Tag.............................. disabled
Security Group Tag............................... Unknown(0)
KTS CAC Capability............................... No
Qos Map Capability............................... No
WMM Support...................................... Disabled
Supported Rates..................................
Mobility State................................... Export Anchor
Mobility Foreign IP Address...................... 192.168.25.41
Mobility Move Count.............................. 1
Security Policy Completed........................ Yes
Policy Manager State............................. RUN
Audit Session ID................................. 2919A8C00000000B7FB6204E
AAA Role Type.................................... none
Acct Interim Interval............................ 0
Local Policy Applied............................. none
IPv4 ACL Name.................................... none
AAA FlexConnect ACL Applied Status............... Unavailable
IPv4 ACL Applied Status.......................... Unavailable
IPv6 ACL Name.................................... none
```

```
IPv6 ACL Applied Status.......................... Unavailable
Layer2 ACL Name.................................. none
Layer2 ACL Applied Status........................ Unavailable
Client Type...................................... SimpleIP
mDNS Status...................................... Disabled
mDNS Profile Name................................ none
No. of mDNS Services Advertised.................. 0
Policy Type...................................... N/A
Encryption Cipher................................ None
Protected Management Frame ...................... No
Management Frame Protection...................... No
EAP Type......................................... Unknown
Interface........................................ vlan4
VLAN............................................. 504
Quarantine VLAN.................................. 0
Access VLAN...................................... 504
Local Bridging VLAN.............................. 504
Client Capabilities:
      CF Pollable................................ Not implemented
      CF Poll Request............................ Not implemented
      Short Preamble............................. Not implemented
      PBCC....................................... Not implemented
      Channel Agility............................ Not implemented
      Listen Interval............................ 0
      Fast BSS Transition........................ Not implemented
      11v BSS Transition......................... Not implemented
Client Wifi Direct Capabilities:
      WFD capable................................ No
      Manged WFD capable......................... No
      Cross Connection Capable................... No
      Support Concurrent Operation............... No
Fast BSS Transition Details:
DNS Server details:
      DNS server IP ............................. 0.0.0.0
      DNS server IP ............................. 0.0.0.0
Assisted Roaming Prediction List details:


 Client Dhcp Required:     True
Allowed (URL)IP Addresses
-------------------------

AVC Profile Name: ............................... none
OpenDns Profile Name: ........................... none
Fastlane Client: ................................ No
Max DSCP: ....................................... 0
Client Statistics:
      Number of Bytes Received................... 0
      Number of Bytes Sent....................... 0
      Total Number of Bytes Sent................. 0
      Total Number of Bytes Recv................. 0
      Number of Bytes Sent (last 90s)............ 0
      Number of Bytes Recv (last 90s)............ 0
      Number of Packets Received................. 0
      Number of Packets Sent..................... 0
      Number of Interim-Update Sent.............. 0
      Number of EAP Id Request Msg Timeouts...... 0
      Number of EAP Id Request Msg Failures...... 0
      Number of EAP Request Msg Timeouts......... 0
      Number of EAP Request Msg Failures......... 0
      Number of EAP Key Msg Timeouts............. 0
      Number of EAP Key Msg Failures............. 0
      Number of Policy Errors.................... 0
      Radio Signal Strength Indicator............ 0 dBm
      Signal to Noise Ratio..................... 0 dB
Client RBACL Statistics:
      Number of RBACL Allowed Packets........... 0
      Number of RBACL Denied Packets............ 0
Nearby AP Statistics:
```

Configure Mobility Anchors using the GUI

Mobility Anchor, also referred to as Guest tunneling or Auto Anchor Mobility, is a feature where all the client traffic that belongs to a WLAN (specially Guest WLAN) is tunneled to a predefined controller or set of controllers that are configured as Anchor for that specific WLAN. This feature helps to restrict clients to a specific subnet and have more control over the user traffic.

Using a mobility anchor forces clients to be anchored to a controller other than the one they first associate with. This forces their traffic to be tunneled to the DMZ. Then it must pass through the firewall and its associated policies before getting anywhere. This is done on a per-WLAN basis.

- Foreign WLC—Refers to the one or more WLCs deployed throughout an enterprise campus or at branch location that are used for managing and controlling a group of APs. Foreign controllers map a guest WLAN into a guest mobility secure/EoIP tunnel.
- Anchor WLC - Refers to one or more WLCs deployed in the enterprise DMZ that are used to perform guest mobility secure tunnel termination, web redirection, and user authentication.

Configure Mobility Anchor on Catalyst 9800 as Guest Anchor Controller with another Catalyst 9800 as Guest Foreign Controller

Before you begin

- Create a WLAN Profile for guests that define the SSID name and profile and all the security settings on both the Catalyst 9800 controllers.
- Create a policy profile.
- Ensure that the WLAN profile name and policy profile name match between the anchor and foreign controllers
- Build a mobility tunnel between the foreign Catalyst 9800 controller and anchor Catalyst 9800 controller.

Step 1 On the **Configuration** > **Tags & Profiles** > **Policy** page, click the **Add** button and define the anchor Catalyst 9800 controller's ip address under the policy profile. To do so, on the **Mobility** tab, select the IP address of the anchor 9800 controller and move it to the **Selected** list of Anchors.

Step 2 Navigate to **ConfigurationTags & ProfilesTags** and create a policy tag that will link the policy profile to the WLAN profile and might be assigned to the APs associated to the foreign controller that service this WLAN.

Step 3 Ensure you select **Update & Apply to Device** to apply the changes to the Policy Tag.

Step 4 (Optional) Assign the Policy Tag to an AP or verify that it already has it. Navigate to **Configuration** > **Wireless** > **Access Points** > **AP Name** > **General** > **.**

Step 5 Log in to anchor Catalyst 9800 controller and create the anchor policy profile. Ensure it has the exact same name that you used on the foreign 9800 controller. Navigate to **Configuration > Tags & Profiles > Policy > + Add**

Step 6 Navigate to Mobility tab and enable Export Anchor. This instructs this 9800 controller that it is the anchor 9800 controller for any WLAN that uses that Policy Profile. When the foreign 9800 controller sends the clients to the anchor 9800 controller , it informs about the WLAN and the Policy Profile that the client is assigned to, so the anchor 9800 controller knows which local Policy Profile to use.

Note Ensure you use this policy profile exclusively to receive the traffic from the foreign controllers. If you link this policy profile to an SSID (inside a Policy Tag), the SSID won't be broadcast by the APs.

Configure Mobility Anchor on Catalyst 9800 as Guest Anchor Controller and AireOS Controller (IRCM image) as Foreign Controller

This task is required when you are setting up the Catalyst 9800 controller as the guest anchor in the DMZ and the AireOS controller as the foreign controller in the campus/enterprise.

First go to the Catalyst 9800 controller's GUI and next go to the AireOS controller's GUI to do the following:

Before you begin

- You must have created the mobility tunnel between the foreign controller and the anchor controller. Follow the procedure outlined above to create the mobility group.
- You must have created a WLAN Profile, Policy Profile and Policy Tag on both the 9800 controllers. Create a WLAN Profile. Enter the Profile Name, SSID and assign a WLAN ID and enable Status and Broadcast SSID once all configurations are complete and ready for deployment. Depending on what range of clients you want this SSID to be discovered, choose the Radio Frequency. Logically you should create a WLAN profile (the WLAN profile has the Profile name, the SSID name and WLAN ID and also the security type for the WLAN and advanced protocols). Next you should create a policy profile that will specify Virtual Local Area Network (VLAN) ID, If traffic is central or local switching, Mobiliy Anchors, Quality of Service(QoS), timers, among other settings. The WLAN profile and the policy profile can be linked together using the Policy tag.

Step 1 Log in to the Catalyst 9800 anchor controller and navigate to **Configuration** > **Tags & Profiles** > **Policy** and click **+Add** to create the anchor policy profile. Ensure that the name of the policy profile is the exact same name of the SSID configured on the AireOS controller, otherwise it will not work.

Step 2 Navigate to the **Mobility** tab and enable **Export Anchor**.

This instructs this 9800 controller that it is the anchor 9800 controller for any WLAN that uses that policy profile. When the foreign AireOS controller sends the clients to the anchor 9800 controller, it informs about the WLAN name that the client is assigned to, so the anchor 9800 controller knows which local WLAN configuration to use and it also uses this name to know which local policy profile to use.

Note Ensure you use this policy profile exclusively to receive the traffic from the foreign controllers. If you link this policy profile to an SSID (inside a Policy Tag), the SSID won't be broadcast by the APs.

Step 3 Configure the AireOS controller as foreign. To do so, log in to the AireOS controller and navigate to **WLANs** > **WLANs**. Select the SSID configured earlier. Ensure that it matches the SSID configured on the Catalyst 9800 anchor controller. Navigate to the arrow at the end of the WLAN's row and select **Mobility Anchor**.

Step 4 Click the mobility anchor and navigate to **WLANs** > **Mobility Anchors** page. Click the **Mobility Anchor Create** button and select the IP address of the Catalyst 9800 controller to set the Catalyst 9800 controller as anchor for this SSID.

What to do next

Verify the configuration.

Configure Mobility Anchor on AireOS(IRCM Image) as Guest Anchor Controller and Catalyst 9800 as Foreign Controller

This task is required when you are setting up the Catalyst 9800 controller as the guest anchor in the DMZ and the AireOS controller as the foreign controller in the campus/enterprise.

Before you begin

Ensure that you have set up the Mobility Tunnel between the peer controllers.

Step 1 Log in to the Foreign 9800 controller and define the Anchor 9800 controller's ip address under the policy profile. To do so, navigate to **Configuration > Tags & Profiles > Policy > + Add** > **Tags & Profiles** > **Policy** and click **Add** to create a new Policy Profile. In the **General** tab, enter the Name and enable the **Central Switching** toggle button. Next, on the **Mobility** tab, select the IP address of the Anchor 9800 controller and move it to the **Selected** list of Anchors.

Step 2 Link the Policy Profile with the WLAN inside the Policy Tag assigned (or that will be assigned) to the APs associated to the foreign controller that service this WLAN. Navigate to **Configuration** > **Tags & Profiles** > **Tags**and either create a new one or use an existing one.

Step 3 Ensure you select **Update & Apply to Device** to apply the changes to the Policy Tag.

Step 4 (Optional) Assign the Site to an AP or verify that it already has it. Navigate to **Configuration > Wireless > Access Points > AP name > General**.

Step 5 Configure the AireOS controller as anchor. Log in to the AireOS controller and navigate to **WLANs** > **WLANs**. Navigate to the drop down menu by clicking on the arrow to the right end of the WLAN's row and select **Mobility Anchor** from the drop-downn list to set it as the local anchor. Navigate to **WLAN** > **Mobility Anchor** > **WLAN SSID**, select the **Switch IP Address** and select the local to make it an anchor.