Configure Enterprise Mobility using the GUI

The Brownfield deployment model assumes that the existing topology has a mix of Cisco AireOS 8.8.111 (or 8.5-based IRCM Image) and Cisco AireOS 8.2/8.3/8.5 controllers and that one or more Catalyst 9800 controllers are being deployed to replace the older AireOS controllers within the enterprise.

Note that the document assumes that you already have an understanding of the preliminary tasks required to set up your topology. However as a brief refresher, the following task list provides you with a checklist to ensure that your configurations are complete before you proceed to configure mobility groups to promote mobility for the wireless clients

Table 1: Preliminary Tasks

Have you completed?	Configurations
1	Configure VLAN, on page 2
2	Configure WLAN and Associated Settings, on page 3

Table 2: Mobility specific configurations

Step	Task
1	Ensure Identical Parameter Configuration on Peer Controllers
2	Configure Mobility Groups between Catalyst 9800 and AireOS 8.8.111 (or 8.5-based IRCM Image) Controller for Secure Mobility, on page 4

Once the above configurations are completed, the following types of roaming are possible between the controllers.

Note The following table is only illustrative of the possible combinations. Depending on the size of the enterprise, clients might roam between two-node or three- node setups. Accordingly, their roam might also be classified as Layer 2 or Layer 3 intercontroller roam with the client roaming between different vlans that are not discussed in detail.

Table 3:

Type of Roaming	Between	Associated VLAN Configuration
Layer 3	Catalyst 9800 and AireOS controllers 8.8.111 (or 8.5-based IRCM Image)	Controllers are on different VLAN ID or same VLAN ID.
	Catalyst 9800 and Catalyst 9800	Controllers are on different VLAN ID.
Layer 2	Two Catalyst 9800 controllers	Controllers are on same VLAN ID
Layer 2	Catalyst AireOS 8.8.111 (or 8.5-based IRCM Image) and AireOS controller 8.2/8.3/8.5	Controllers are on same VLAN ID and same subnet
Layer 3	Catalyst AireOS 8.8.111 (or 8.5-based IRCM Image) and Catalyst AireOS controller 8.2/8.3/8.5	Controllers are on different VLAN ID.

Depending on your requirement, follow the steps below to set up the controllers to enable roaming across the enterprise.

Most of the preliminary steps discussed below, are from the perspective of deploying Catalyst 9800 controllers to your existing setup. If you need help with deploying AireOS controllers with IRCM image, refer to the respective AireOS documents.

- Configure VLAN, on page 2
- Configure WLAN and Associated Settings, on page 3
- Configure Mobility Groups between Peer Controllers Using the GUI, on page 3
- Configure Mobility Groups between Catalyst 9800 and AireOS 8.8.111 (or 8.5-based IRCM Image) Controller for Secure Mobility, on page 4

Configure VLAN

A Virtual Local Area Network (VLAN) is a switched network that is logically segmented by function, area, or application without regard to the physical locations of the users. Before you start any configuration, you need to add the VLANs to which wireless clients will be assigned.

Step 1 Navigate to **Configuration** > **Layer2** > **VLAN** > **VLAN**

Click on the **Add** button to add a VLAN.

Step 2 Enter the details (VLAN ID and VLAN Name)

Repeat the steps to configure multiple VLANs for e.g. VLAN ID is **vlan 20** and VLAN name as **test 20**Alternatively, create a range of VLANs by entering a VLAN ID range. Note that the available VLAN ID range is 1 to 4094 and the recommended length for the VLAN Name is less than 20 characters.

Step 3 Click **Apply to Device**.

What to do next

Verify the VLAN/Interface Configuration on the GUI. The configured VLANs are listed on the page.

Configure WLAN and Associated Settings

WLAN is a network that allows devices to connect and communicate wirelessly.

Each WLAN has a separate WLAN ID, a separate profile name, and a WLAN SSID. All access points can advertise up to 16 WLANs. However, you can create up to 4096 WLANs and then selectively advertise these WLANs (using profiles and tags) to different access points for better manageability. You can configure WLANs with different SSIDs or with the same SSID. An SSID identifies the specific wireless network that you want the device to access.

Step 1 Navigate to **Configuration** > **Wireless** > **WLANs** and click on the **Add** button to add a WLAN.

Step 2 Enter all the needed information (SSID name, security type and so on) and once done, click **Save &Apply to Device**. In this example the SSID name is **`IRCM1014_WLAN_OPENAUTH1`**.

Step 3 Navigate to **Configuration** > **Tags & Profiles** > **Policy**. Select the name of a pre-existing policy or click **+Add** to create a new policy. Enable the policy, set the needed VLAN and any other parameter you want to customize and click **Save & Apply to Device** .

Step 4 Next, create or modify a Policy Tag. To do so, go to **Configuration** > **Tags & Profiles** > **Tags** > **Policy**. Select a pre-existing policy tag or click **+ Add** to add a new one.

Step 5 Inside the Policy Tag, click **+ Add** . From the drop-down list select the **WLAN Profile** name you want to add to the Policy Tag and to which you want to link it. To complete the task, click **Save & Apply to Device** .

Step 6 Repeat the above for all the WLANs that you want to add. Click **Save & Apply to Device**once the task is complete.

What to do next

Ensure Identical Parameter Configuration on Peer Controllers and Configure Mobility Groups between Peer Controllers Using the GUI, on page 3.

Configure Mobility Groups between Peer Controllers Using the GUI

A Mobility Group is a group of Wireless LAN Controllers (WLCs or controllers) in a network with the same Mobility Group name. These controllers can dynamically share context and state of client devices, controller load information, and can also forward data traffic among them, which enables inter-controller wireless LAN roam and controller redundancy.

Each controller in a mobility group is configured with a list of the other members of the mobility group. Each controller device builds a neighbor relationship with every other member of the group.

The configuration comprises of the following tasks:

Table 4:

Step	Task
1	Create a mobility group on Catalyst 9800 and on the AireOS 8.8.111 (or 8.5-based IRCM Image) controller.
2	Configure peer information on Catalyst 9800 and AireOS 8.8.111 (or 8.5-based IRCM Image) controller and set up tunnel between them.
3	Verify the tunnel.

Before you begin:

- You must have gathered the MAC address and IP address of every controller that is to be included in the mobility group. This information is necessary because you will be configuring all controllers with the MAC address and IP address of all the other mobility group members.
- Each controller must be manually configured with the MAC address and IP address of all the other mobility group members.
- Ensure that there is IP connectivity between the management interfaces of all controller devices; verify by pinging between them.
- The controllers need unrestricted access through any firewalls or access control lists (ACL) to use UDP port 16666 (unencrypted) or UDP port 16667 (encrypted) for message exchange between them.
- All controllers must be configured with the same mobility group name; the mobility group name is case-sensitive.
- All controllers must be configured to use the same virtual interface IP address.

Configure Mobility Groups between Catalyst 9800 and AireOS 8.8.111 (or 8.5-based IRCM Image) Controller for Secure Mobility

This configuration is required when you are creating a mobility group and setting up Catalyst 9800 and Cisco AireOS (IRCM image) as mobility peers.

Follow the steps to setup the tunnel between the peer controllers:

Step 1 Configure Mobility Group on the Catalyst 9800 controller. To do so, on the Catalyst 9800's GUI , go to **Configuration** > **Mobility** and in the **Global Configuration** tab, perform the following tasks:

a) Enter a name for the mobility group.
b) Enter the multicast IP address for the mobility group.
c) n the **Keep Alive Interval** field, specify the number of times a ping request is sent to a mobility list member before the member is considered to be unreachable. The valid range is 3 to 20, and the default value is 3.

d) Specify the **Mobility Keep Alive Count** amount of time (in seconds) between each ping request sent to a mobility list member. The valid range is 1 to 30 seconds.
e) (Optional) Enter the DSCP value for the mobility group.
f) Enter the mobility MAC address.
g) (Optional) Enable the **DTLS High Cipher Only** button to advertise higher cipher suites during DTLS handshakes. This is disabled, by default.
h) Click **Apply**.

Step 2 Configure the mobility peer on Catalyst 9800. This information can be collected from an AireOS controller by navigating to the AireOS GUI's **CONTROLLER** > **Mobility Management** > **Mobility Groups** and noting the MAC Address, IP Address and Group Name of the AireOS controller.

Step 3 Add the AireOS controller information into the Cisco Catalyst controller.On the Catalyst 9800's GUI , go to **Configuration** > **Mobility** and in the **Peer Configuration** tab, perform the following tasks:

a) In the **Mobility Peer Configuration** section, click **Add**.
b) In the **Add Mobility Peer** window that is displayed, enter the MAC Address and the IP address for the mobility peer.
c) Additionally, when NAT is used, enter the optional public IP address to enter the mobility peer's NATed address. When NAT is not used, the public IP address is not used and the device displays the mobility peer's direct IP address.
d) Enter the mobility group to which you want to add the mobility peer.
e) Select the required status for Data Link Encryption.
f) Specify the SSC Hash as required.

SSC hash is required if the peer is a Cisco Catalyst 9800-CL Wireless Controller, which uses self-signed certificate and hence SSC hash is used as an additional validation. SSC hash is not required if peer is an appliance, which will have manufacturing installed certificates (MIC) or device certificates burned in the hardware.

g) Click **Apply to Device**.
h) (Optional) In the **Non-Local Mobility Group Multicast Configuration** section, click **Add** if you want the mobility messages to use multicast. This enables the controller to send only one copy of the message to the network, which in turn goes to the multicast group that contains all the mobility members.
i) Enter the mobility group name.
j) Enter the multicast IP (v4/v6) address for the mobility group.
k) Click Save.

Note On the Catalyst 9800 controller, control plane encryption is always enabled, which means that you need to have secure mobility enabled on the AireOS side. However, data link encryption is optional. If you enable it on the 9800 side, you will need to enable it on AireOS.

Step 4 Configure the mobility peer on the AireOS 8.8.111 (or 8.5-based IRCM Image) controller. To do so, collect the Catalyst 9800 controller mobility information. On the Catalyst 9800 GUI, navigate to **Configuration** > **Wireless** > **Mobility** > **Global Configuration** and note the **Mobility Group Name** and **Mobility MAC Address**. Collect the Hash value from the Catalyst 9800 controller if this is a virtual controller.

Step 5 Add the Catalyst 9800 controller information into the AireOS controller. To do so, navigate to **CONTROLLER** > **Mobility Management** > **Mobility Groups** > **New**, enter the values.

a) Enter the management interface IPv4/IPv6 address and the MAC address of the controller to be added in the respective text boxes.

If you are configuring the mobility group in a network where network address translation (NAT) is enabled, enter the IPv4/IPv6 address that is sent to the controller from the NAT device rather than the controller’s management interface IPv4/IPv6 address. Otherwise, mobility will fail among controllers in the mobility group.

b) In the **Group Name** text box, enter the name of the mobility group.

Note The mobility group name is case sensitive.

c) From the Secure Mobility drop-down list, choose **Enabled**.

d) From the **Data Tunnel Encryption** drop-down list, choose **Disabled** or **Enabled** based on what was configured on the peer Catalyst 9800 controller .

e) From the **High Cipher** drop-down list, choose **Enabled** You must enable **High Cipher** only if you require DTLS v1.2 encryption. The default value is **Disabled**. In disabled state, DTLS v1.0 encryption is enabled.

Note Note that this configuration must match the configuration on Catalyst 9800.

f) Enter the hash key of the peer mobility controller, which should be a virtual controller in the same domain.

Note Hash is only required in case of the virtual Catalyst 9800 -CL controller that uses a self-signed certificate. Appliances have a MIC certificate and don't need a hash.

Note Hash is not supported for IPv6 members.

g) Click **Apply** to commit your changes. The new controller is added to the list of mobility group members on the AireOS controller's **Static Mobility Group Members** page. Save the configuration by clicking the appropriate button.

Step 6 Verify the mobility tunnel between the peers is up and runnning. To do so, in the Catalyst 9800 controller's **Mobility Peer Configuration** section, view the list of devices that are part of this peer configuration. Ensure that the **Status** is **Up** .