



Mobility Groups

- [Information About Mobility Groups, on page 1](#)
- [Prerequisites for Configuring Mobility Groups, on page 4](#)
- [Configuring Mobility Groups \(GUI\), on page 5](#)
- [Configuring Mobility Groups \(CLI\), on page 7](#)
- [Viewing Mobility Group Statistics \(GUI\), on page 8](#)
- [Viewing Mobility Group Statistics \(CLI\), on page 10](#)
- [Profile Name Matching for Mobility Anchor , on page 10](#)
- [Information about Inter-Release Controller Mobility, on page 11](#)

Information About Mobility Groups

A mobility group is a set of controllers, identified by the same mobility group name, that defines the realm of seamless roaming for wireless clients. By creating a mobility group, you can enable multiple controllers in a network to dynamically share information and forward data traffic when inter-controller or inter-subnet roaming occurs. Controllers in the same mobility group can share the context and state of client devices as well as their list of access points so that they do not consider each other's access points as rogue devices. With this information, the network can support inter-controller wireless LAN roaming and controller redundancy.

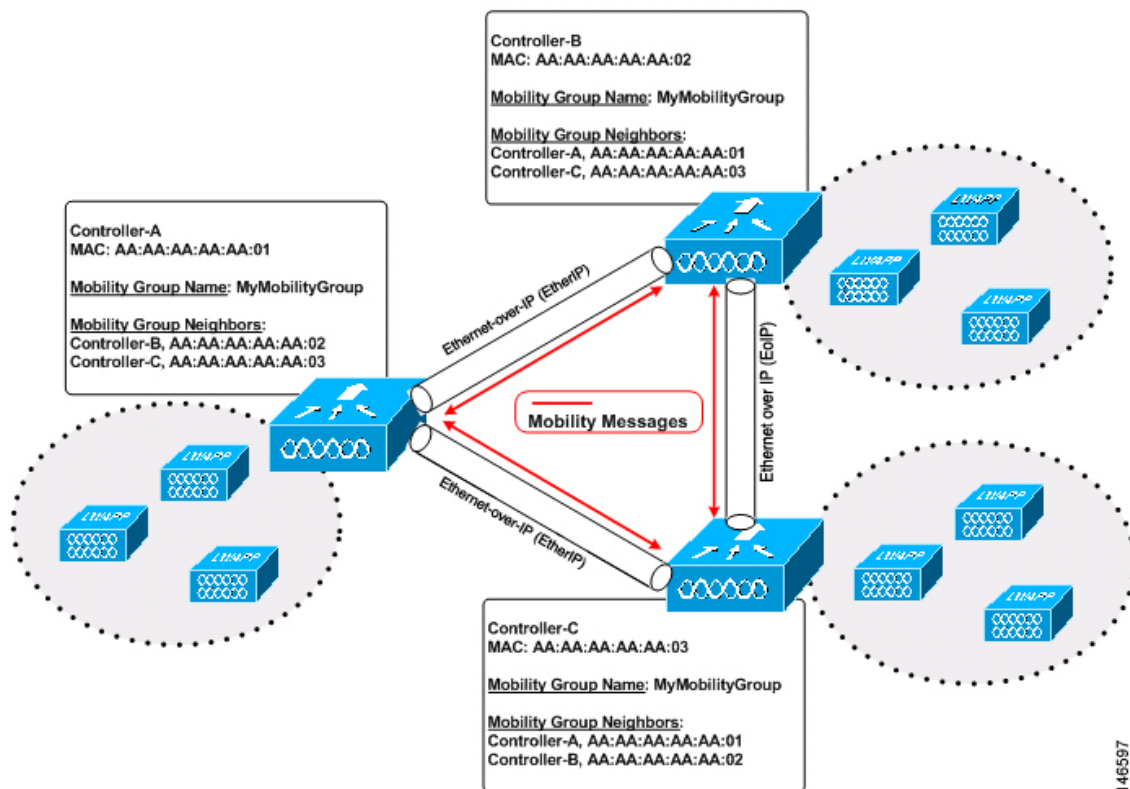


Note If migrating APs from one controller to another controller to decommission the old controller, clients that were associated with the first controller before the move might be anchored to the old controller after the move. As a workaround, you must disable the WLANs on the old controller before decommissioning it.



Note Controllers do not have to be of the same model to be a member of a mobility group. Mobility groups can be comprised of any combination of controller platforms as long as the controllers are running compatible AireOS versions. For more information, see the "IRCM Compatibility Matrix for AireOS Releases" section in the [Cisco Wireless Solutions Software Compatibility Matrix](#) document.

Figure 1: Example of a Single Mobility Group



146597

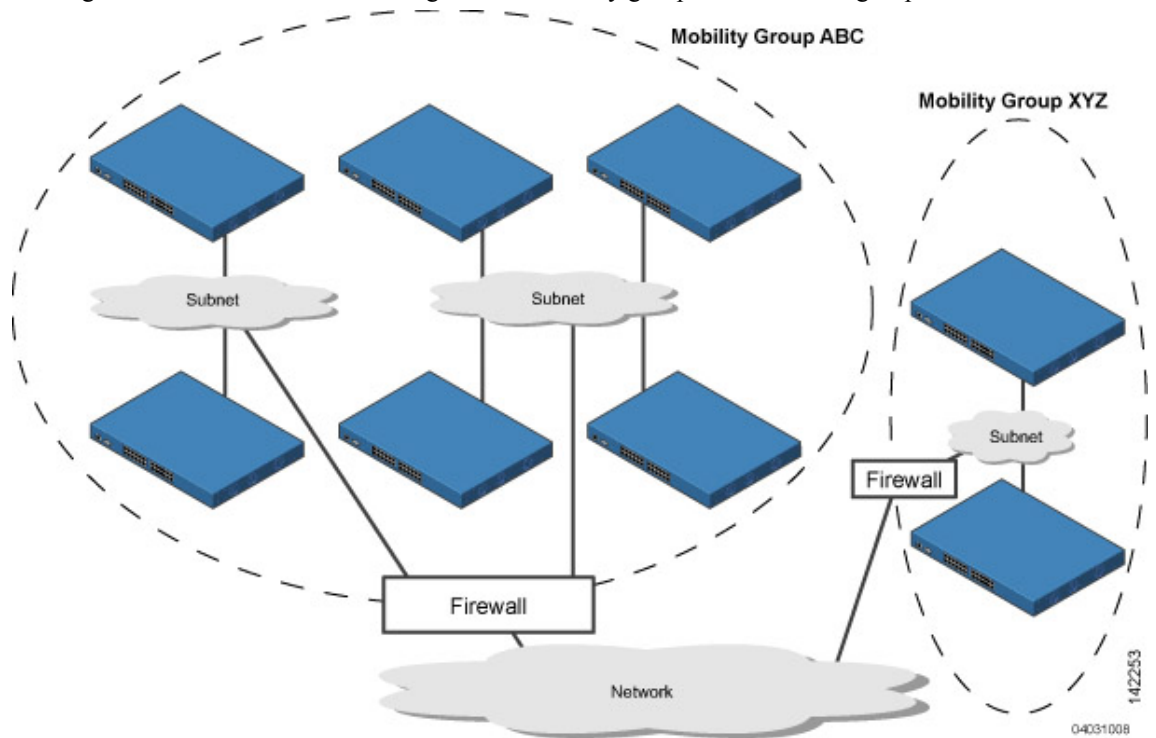
As shown above, each controller is configured with a list of the other members of the mobility group. In this example, client data traffic is tunneled between controllers in Ethernet-over-IP as mobility encryption is not configured. Whenever a new client joins a controller, the controller sends out a unicast message (or multicast message if mobility multicast is configured) to all of the controllers in the mobility group. The controller to which the client was previously connected passes on the status of the client. You can configure the controller to use multicast to send the Mobile Announce messages. This functionality enables the controller to send only one copy of the message to the network, which destines it to the multicast group that contains all the mobility members. To derive the maximum benefit from multicast messaging, we recommend that you enable multicast messaging for all group members.

For example, if a controller supports 6000 access points, a mobility group that consists of 24 such controllers supports up to 144,000 access points (24 * 6000 = 144,000 access points).

Mobility messages among mobility group members can be transmitted in IPv4 or IPv6, as unicast or multicast. We recommend multicast messaging for large mobility groups.

Figure 2: Two Mobility Groups

This figure shows the results of creating distinct mobility group names for two groups of controllers.



The controllers in the ABC mobility group share access point and client information with each other. The controllers in the ABC mobility group do not share the access point or client information with the XYZ controllers, which are in a different mobility group, unless each mobility group member is configured with mobility list entries for the other mobility group members. Likewise, the controllers in the XYZ mobility group do not share access point or client information with the controllers in the ABC mobility group. This feature ensures mobility group isolation across the network.

Every controller maintains information about its peer controllers in a mobility list. Controllers can communicate across mobility groups and clients may roam between access points in different mobility groups if the controllers are included in each other's mobility lists.

A mobility group can have up to 24 members and a mobility list can have up to 72 members. For example, the following combinations are allowed:

- 3 mobility groups with 24 members in each group
- 12 mobility groups with 6 members in each group
- 24 mobility groups with 3 members in each group
- 72 mobility groups with 1 member in each group

The controller supports seamless roaming across multiple mobility groups. During seamless roaming, the client maintains its IP address across all mobility groups; however, Cisco Centralized Key Management (CCKM) and proactive key caching (PKC) are supported only for inter-mobility-group roaming. When a client crosses a mobility group boundary during a roam, the client is fully authenticated, but the IP address is maintained, and mobility tunneling is initiated for Layer 3 roaming.

Prerequisites for Configuring Mobility Groups

Before you add controllers to a mobility group, you must verify that the following requirements have been met for all controllers that are to be included in the group:

- IP connectivity must exist between the management interfaces of all controllers.



Note You can verify IP connectivity by pinging the controllers using the `mping` and `eping` commands.



Note Mobility control packets can use any interface address as the source, based on routing table. It is recommended that all controllers in the mobility group should have the management interface in the same subnet. A topology where one controller's management interface and other controller's dynamic interface are on same subnet not recommended for seamless mobility.

- If configuring mobility peers that run different software versions, see the "IRCM Compatibility Matrix for AireOS Releases" section in the [Cisco Wireless Solutions Software Compatibility Matrix](#) document.



Note If you inadvertently configure a controller with a failover controller that runs a different software release, the access point might take a long time to join the failover controller because the access point starts the discovery process in CAPWAP and then changes to LWAPP discovery.

- All controllers must be configured with the same virtual interface IP address.
- 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.



Note You can find the MAC and IP addresses of the other controllers to be included in the mobility group on the **Controller > Mobility Groups** page of each controller's GUI.

- If you have a firewall b/w your mobility group members, open UDP port 16666 and IP protocol 97. If you are using encrypted mobility, open UDP port 5246 and 5247.

For information about protocols and port numbers that must be used for management and operational purposes, see the [Cisco Unified Wireless Network Protocol and Port Matrix](#) document.



Note To view information on mobility support across controllers with different software versions, see <http://www.cisco.com/c/en/us/td/docs/wireless/compatibility/matrix/compatibility-matrix.html>.



Note You cannot perform port address translation (PAT) on the firewall. You must configure one-to-one network address translation (NAT).

Configuring Mobility Groups (GUI)

Procedure

Step 1 Choose **Controller > Mobility Management > Mobility Groups** to open the **Static Mobility Group Members** page.

This page shows the mobility group name in the Default Mobility Group text box and lists the MAC address and IPv4/IPv6 address of each controller that is currently a member of the mobility group. The first entry is the local controller, which cannot be deleted.

Note If you want to delete any of the remote controllers from the mobility group, hover your cursor over the blue drop-down arrow for the desired controller and choose **Remove**.

Step 2 Perform one of the following to add controllers to a mobility group:

- If you are adding only one controller or want to individually add multiple controllers, click **New**.

OR

- If you are adding multiple controllers and want to add them in bulk, click **EditAll**.

Note The EditAll option enables you to enter the MAC and IPv4/IPv6 addresses of all the current mobility group members and then copy and paste all the entries from one controller to the other controllers in the mobility group.

Step 3 Click **New** to open the **Mobility Group Member > New** page.

Step 4 Add a controller to the mobility group as follows:

- a. In the Member IP Address text box, enter the management interface IPv4/IPv6 address of the controller to be added.

Note 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 **Member MAC Address** text box, enter the MAC address of the controller to be added.

- c. In the **Group Name** text box, enter the name of the mobility group.

Note The mobility group name is case sensitive.

- d. In the **Hash** text box, enter the hash key of the peer mobility controller, which should be a virtual controller in the same domain.

You must configure the hash only if the peer mobility controller is a virtual controller in the same domain.

Note Hash is not supported for IPv6 members.

- e. Click **Apply** to commit your changes. The new controller is added to the list of mobility group members on the **Static Mobility Group Members** page.
- f. Click **Save Configuration**.
- g. Repeat [Step a](#) through [Step e](#) to add all of the controllers in the mobility group.
- h. Repeat this procedure on every controller to be included in the mobility group. All controllers in the mobility group must be configured with the MAC address and IPv4/IPv6 address of all other mobility group members.

The **Mobility Group Members > Edit All** page lists the MAC address, IPv4/IPv6 address, and mobility group name (optional) of all the controllers currently in the mobility group. The controllers are listed one per line with the local controller at the top of the list.

Note If desired, you can edit or delete any of the controllers in the list.

Step 5

Add more controllers to the mobility group as follows:

- a. Click inside the edit box to start a new line.
- b. Enter the MAC address, the management interface IPv4/IPv6 address, and the name of the mobility group for the controller to be added.

Note You should enter these values on one line and separate each value with one or two spaces.

Note The mobility group name is case sensitive.

- c. Repeat [Step a](#) and [Step b](#) for each additional controller that you want to add to the mobility group.
- d. Highlight and copy the complete list of entries in the edit box.
- e. Click **Apply** to commit your changes. The new controllers are added to the list of mobility group members on the **Static Mobility Group Members** page.
- f. Click **Save Configuration** to save your changes.
- g. Paste the list into the text box on the Mobility Group Members > Edit All page of all the other controllers in the mobility group and click **Apply** and **Save Configuration**.

Step 6

Choose **Mobility Management > Multicast Messaging** to open the **Mobility Multicast Messaging** page.

The names of all the currently configured mobility groups appear in the middle of the page.

Step 7

On the **Mobility Multicast Messaging** page, check the **Enable Multicast Messaging** check box to enable the controller to use multicast mode to send Mobile Announce messages to the mobility members. If you leave it unselected, the controller uses unicast mode to send the Mobile Announce messages. The default value is unselected.

Step 8

If you enabled multicast messaging in the previous step, enter the multicast group IPv4 address for the local mobility group in the **Local Group Multicast IPv4 Address** text box. This address is used for multicast mobility messaging.

Note In order to use multicast messaging, you must configure the IPv4 address for the local mobility group.

Note IPv6 is not supported for mobility multicast.

Step 9 Click **Apply** to commit your changes.

Step 10 If desired, you can also configure the multicast group IPv4 address for non-local groups within the mobility list. To do so, click the name of a non-local mobility group to open the Mobility Multicast Messaging > Edit page, and enter the multicast group IPv4 address for the non-local mobility group in the Multicast IP Address text box.

Note If you do not configure the multicast IPv4 address for non-local groups, the controller uses unicast mode to send mobility messages to those members.

Step 11 Click **Apply**.

Step 12 Click **Save Configuration**.

Configuring Mobility Groups (CLI)

Procedure

Step 1 Check the current mobility settings by entering this command:

Step 2 Create a mobility group by entering this command:

config mobility group domain *domain_name*

Note Enter up to 31 case-sensitive ASCII characters for the group name. Spaces are not allowed in mobility group names.

Step 3 Add a group member by entering this command:

config mobility group member add *mac_address ip_address*

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

Note Enter the **config mobility group member delete** *mac_address* command if you want to delete a group member.

Step 4 To configure the hash key of a peer mobility controller, which is a virtual controller in the same domain, enter this command:

config mobility group member hash *peer-ip-address key*

Step 5 Enable or disable multicast mobility mode by entering this command:

config mobility multicast-mode {**enable** | **disable**} *local_group_multicast_address*

where *local_group_multicast_address* is the multicast group IPv4 address for the local mobility group. This address is used for multicast mobility messaging.

Note In order to use multicast messaging, you must configure the IPv4 address for the local mobility group.

Note IPv6 is not supported for mobility multicast.

If you enable multicast mobility mode, the controller uses multicast mode to send Mobile Announce messages to the local group. If you disable multicast mobility mode, the controller uses unicast mode to send the Mobile Announce messages to the local group. The default value is disabled.

Step 6 (Optional) You can also configure the multicast group IPv4 address for non-local groups within the mobility list. To do so, enter this command:

config mobility group multicast-address *group_name IP_address*

If you do not configure the multicast IPv4 address for non-local groups, the controller uses unicast mode to send mobility messages to those members.

Step 7 Verify the mobility configuration by entering this command:

show mobility summary

Step 8 To see the hash key of mobility group members in the same domain, enter this command:

show mobility group member hash

Step 9 Save your changes by entering this command:

save config

Step 10 Repeat this procedure on every controller to be included in the mobility group. All controllers in the mobility group must be configured with the MAC address and IP address of all other mobility group members.

Step 11 Enable or disable debugging of multicast usage for mobility messages by entering this command:

debug mobility multicast {enable | disable}

Viewing Mobility Group Statistics (GUI)

Procedure

Step 1 Choose **Monitor > Statistics > Mobility Statistics** to open the Mobility Statistics page.

This page contains the following fields

- Global Mobility Statistics
 - Rx Errors—Generic protocol packet receive errors, such as packet too short or format incorrect.
 - Tx Errors—Generic protocol packet transmit errors, such as packet transmission fail.
 - Responses Retransmitted—Mobility protocol that uses UDP and resends requests several times if it does not receive a response. Because of network or processing delays, the responder may receive

one or more retry requests after it initially responds to a request. This text box shows a count of the response resends.

- Handoff Requests Received—Total number of handoff requests received, ignored, or responded to.
 - Handoff End Requests Received—Total number of handoff end requests received. These requests are sent by the anchor or foreign controller to notify the other about the close of a client session.
 - State Transitions Disallowed—Policy enforcement module (PEM) that has denied a client state transition, usually resulting in the handoff being terminated.
 - Resource Unavailable—Necessary resource, such as a buffer, was unavailable, resulting in the handoff being terminated.
- Mobility Initiator Statistics
 - Handoff Requests Sent—Number of clients that have associated to the controller and have been announced to the mobility group.
 - Handoff Replies Received—Number of handoff replies that have been received in response to the requests sent.
 - Handoff as Local Received—Number of handoffs in which the entire client session has been transferred.
 - Handoff as Foreign Received—Number of handoffs in which the client session was anchored elsewhere.
 - Handoff Denys Received—Number of handoffs that were denied.
 - Anchor Request Sent—Number of anchor requests that were sent for a three-party (foreign-to-foreign) handoff. The handoff was received from another foreign controller, and the new controller is requesting the anchor to move the client.
 - Anchor Deny Received—Number of anchor requests that were denied by the current anchor.
 - Anchor Grant Received—Number of anchor requests that were approved by the current anchor.
 - Anchor Transfer Received—Number of anchor requests that closed the session on the current anchor and transferred the anchor back to the requestor.
 - Mobility Responder Statistics
 - Handoff Requests Ignored—Number of handoff requests or client announcements that were ignored because the controller had no knowledge of that client.
 - Ping Pong Handoff Requests Dropped—Number of handoff requests that were denied because the handoff period was too short (3 seconds).
 - Handoff Requests Dropped—Number of handoff requests that were dropped due to either an incomplete knowledge of the client or a problem with the packet.
 - Handoff Requests Denied—Number of handoff requests that were denied.
 - Client Handoff as Local—Number of handoff responses sent while the client is in the local role.
 - Client Handoff as Foreign—Number of handoff responses sent while the client is in the foreign role.

- Anchor Requests Received—Number of anchor requests received.
- Anchor Requests Denied—Number of anchor requests denied.
- Anchor Requests Granted—Number of anchor requests granted.
- Anchor Transferred—Number of anchors transferred because the client has moved from a foreign controller to a controller on the same subnet as the current anchor.

Step 2 If you want to clear the current mobility statistics, click **Clear Stats**.

Viewing Mobility Group Statistics (CLI)

Procedure

Step 1 See mobility group statistics by entering this command:

show mobility statistics

Step 2 Clear the current mobility statistics by entering this command:

clear stats mobility

Profile Name Matching for Mobility Anchor

Currently AireOS controller can have two different WLANs with same SSID, so if on the anchor controller, there are 2 or more WLANs configured with the same SSID name, there is a possibility that, the anchor may pick a wrong WLAN corresponding to the SSID name it received from the (export) foreign controller for roaming and guest anchor client association scenarios and it will result in roaming and client association failures. With this feature enabled, profile name associated with the SSID will be used in place of SSID as profile name is unique across the controllers.

However to retain the existing functionality, SSID name and its length are sent along with profile name and its length from foreign controller.

This feature, by default, is in disabled state. You must explicitly enable it as required.

Configuring Profile Name Matching for Mobility Anchor (CLI)

Procedure

- Enable or disable the profile name check on the mobility anchor by entering this command:

config mobility use-profile-name {enable | disable }

The profile name matching feature is applied globally on the controller. Default value is disabled.

- View the profile name check status by entering this command:

show mobility summary

Example

```
(Cisco Controller) >show mobility summary

Mobility Protocol Port..... 1636
Default Mobility Domain..... jk332
Multicast Mode ..... Disabled
DTLS Mode ..... Disabled
Mobility Domain ID for 802.11r..... 0x711d
Mobility Keepalive Interval..... 10
Mobility Keepalive Count..... 3
Mobility Group Members Configured..... 1
Mobility Control Message DSCP Value..... 0
Mobility Use Profile Name..... Disabled
```

Information about Inter-Release Controller Mobility

Inter-Release Controller Mobility (IRCM) supports seamless mobility and services across different wireless LAN controllers that runs on different software and controllers.

IRCM supports controller deployment combinations such as:

- Existing Cisco Aireos controllers in the network and additional Cisco Catalyst 9800 wireless controllers is added (Brownfield).
- Cisco Aireos controllers deployed as Guest anchor and additional Cisco Catalyst 9800 wireless controllers added.
- Multiple Cisco Catalyst 9800 wireless controllers deployed (Green field).

A secure link in which data is encrypted using CAPWAP DTLS protocol can be established between two controllers. This secured link is called Encrypted Mobility Tunnel.

If encrypted mobility tunnel is in enabled state, the data traffic is encrypted and the controller uses UDP port 16667, instead of EoIP, to send the data traffic.

To ensure that controllers with expired MIC certificates are able to join the encrypted mobility tunnel enabled network, an existing CLI is used to disable the MIC certificate date validation.



Note This command disables the date validation check during Cisco AP join and encrypted mobility tunnel creation. When the **config ap cert-expiry-ignore** CLI is enabled, the lifetime check is disabled.

Restrictions for Inter-Release Controller Mobility

- This feature is supported on Cisco 3504, 5520, and 8540 controllers only.



Note The Cisco 5508 and 8510 Wireless Controllers do not support tunnel encryption protocols. They support IRCM with unencrypted mobility tunnels only.

- Native IPv6 is not supported.
- Mobility Multicast for an encrypted tunnel is not supported.
- The Encrypted Mobility Tunnel feature should be enabled on all the mobility peers in the network to have the tunnel created. The default state is set to disabled.
- If the packets passing through the controller after L3 roaming are greater than the MTU size of the controller in secure mobility, along with secure mobility, data encryption functionality must be enabled for the fragmented packets to be forwarded through a secure mobility tunnel.
- In AireOS controller, L3 override is not supported in guest VLAN. Hence, the client does not trigger DHCP Discovery on the new VLAN automatically.
- Only MIC certificate is supported to create the tunnel.
- When using Cisco 3504 controller as an anchor, we recommend reducing the client load by 30% of the controller's maximum load capability.

Configuring Mobility Groups for Inter-Release Controller Mobility (IRCM) (GUI)

Procedure

Step 1 Choose **Controller > Mobility Management > Mobility Groups** to open the **Static Mobility Group Members** page.

Note If you want to delete any of the remote controllers from the mobility group, hover your cursor over the blue drop-down arrow for the desired controller and choose **Remove**.

Step 2 Click **New** to open the **Mobility Group Member > New** page.

Step 3 Add a controller to the mobility group as follows:

a. In the **Member IP Address** text box, enter the management interface IPv4 address of the controller to be added.

Note IPv6 address is not supported.

b. In the **Member MAC Address** text box, enter the MAC address of the controller to be added.

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

Note The mobility group name is case sensitive.

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

e. From the **Data Tunnel Encryption** drop-down list, choose **Enabled**.

f. 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.

- g.** In the **Hash** text box, enter the virtual controller's hash key of the peer mobility controller.
You must configure the hash only if the peer mobility controller is a virtual controller.
- h.** Click **Apply** to commit your changes. The new controller is added to the list of mobility group members on the **Static Mobility Group Members** page.

Configuring Mobility Groups for Inter-Release Controller Mobility (IRCM) (CLI)

Procedure

- Step 1** Add a peer controller in the mobility group by entering this command:
config mobility group member add *peer-mac-addr peer-ip-addr group-name encrypt {enable | disable}*
 - Step 2** (Optional) Configure the peer controller data traffic encryption by entering this command:
config mobility group member data-dtls *peer-mac-addr {enable | disable}*
Default value is Enabled.
 - Step 3** (Optional) Configure high cipher encryption to enable DTLS 1.2 protocol by entering this command:
config mobility group member add *member-switch-mac-addr member-switch-ip-addr grp-name encrypt enable high-cipher-option enable*
Default value is Disabled.
 - Step 4** Configure the SSC hash of the Cisco Catalyst 9800 Series Wireless Controllers by entering this command:
config mobility group member hash *peer-ip-addr 40-digit-ssc-hash-key*
Note SSC hash is needed on for peers that do not use a MIC certificate. For example: Cisco Catalyst 9800-CL Wireless Controllers.
 - Step 5** View the peer to peer mobility encryption status by entering this command:
show mobility summary encryption
 - Step 6** To see the hash key of mobility group members in the same domain, enter this command:
show mobility group member hash
 - Step 7** View mobility DTLS connection status by entering this command:
show mobility dtls connections
 - Step 8** View mobility statistics by entering this command:
show mobility statistics
-

