Encrypted Mobility Tunnel

• Information About Encrypted Mobility Tunnel, on page 1
• Configuring Mobility Groups for Inter-Release Controller Mobility (IRCM) (GUI), on page 2
• Configuring Mobility Groups for Inter-Release Controller Mobility (IRCM) (CLI), on page 2

Information About Encrypted Mobility Tunnel

A secure link in which data is encrypted using CAPWAP DTLS protocol can be established between an anchor and a foreign controller. 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 Cisco WLCs 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 on Encrypted Mobility Tunnel

• Native IPv6 is not supported.

• Mobility Multicast infrastructure for an encrypted tunnel is not supported.

• Not supported on Cisco 2500, vWLC and WiSM2 controllers.
  This feature is supported on Cisco 3504, 5520, and 8540 Controllers only.

• 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.

• Only MIC certificate is supported to create the tunnel.
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:

1. 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.

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

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

Note
The mobility group name is case sensitive.

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

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

6. 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.

7. 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  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. All traffic is encrypted between mobility peers.

Step 3  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 4  View the peer to peer mobility encryption status by entering this command:
```
show mobility summary encryption
```

Step 5  To see the hash key of mobility group members in the same domain, enter this command:
```
show mobility group member hash
```

Step 6  View mobility DTLS connection status by entering this command:
```
show mobility dtls connections
```

Step 7  View mobility statistics by entering this command:
```
show mobility statistics
```