

# Encrypted Mobility Tunnel


- Information about Encrypted Mobility Tunnel, on page 1


# Information about Encrypted Mobility Tunnel

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 Encrypted Mobility Tunnel

- 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.

- 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**