Encrypted Mobility Tunnel

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.

- Native IPv6 is not supported.

- Mobility Multicast infrastructure 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.

- Only MIC certificate is supported to create the tunnel.

Configuring Global Encrypted Mobility Tunnel (GUI)

Procedure

Step 1	Choose **Controller** > **Mobility Management** > **Mobility Configuration** to open the **Global Configuration** page.
Step 2	Check the **Mobility Encryption** check box to enable mobility encryption on the network.
Step 3	Save the configuration. Cisco WLC reboots to reflect the change in mobility encryption state.

Configuring Global Encrypted Mobility Tunnel (CLI)

Procedure

	Command or Action	Purpose
Step 1	[Optional] Disable the MIC certificate validation check by entering this command:	**config ap cert-expiry-ignore mic** { **enable | disable** } **Note** You must use this command only when there are mobility peers with expired MIC certificates in the network.
Step 2	Configure encrypted mobility tunnel by entering this command:	**config mobility encryption {enable | disable}** **Note** The WLC reboots after the feature is enabled or disabled.

Step 3	View the status of the encrypted mobility tunnel by entering this command:	lines
		
		 show mobility summary
		
		 Note DTLS Mode status is not displayed in the output when encrypted mobility tunnel feature is disabled.
		
		 Information similar to the following is displayed:
		
		 `(Cisco Controller) >show mobility summary`
		
		 `Mobility Protocol Port.......................... 16666` `Default Mobility Domain.......................... TestSpartan8500Dev1Group` `Multicast Mode`

Command or Action	Purpose

	``
	....
	Disabled
	DTLS Mode
	....
	 Enabled
	Mobility Domain ID for
	802.11r................... 0x209c
	Mobility Keepalive
	Interval..................... 10
	Mobility Keepalive
	Count........................ 3
	Mobility Group Members
	Configured................ 1
	Mobility Control Message DSCP
	Value.............. 0
	
	Controllers configured in the Mobility
	Group
	 MAC Address IP Address Group
	 Name Multicast IP
	            Status
	 f4:cf:e2:0a:ea:00 8.1.4.2
	Test8500Dev1Group 0.0.0.0
	                        Up
	``