Encrypted Tunnel Deployment Guide

Introduction 2
Pre-requisite 2
Product or Feature Overview 2
Configuring Encrypted Mobility Tunnel 3
Introduction

This document introduces the 8.7 Mobility Encrypted Tunnel and provides general guidelines for its deployment. The purpose of this document is to:

• Provide an overview of 8.7 Mobility Encrypted Tunnel Feature
• Highlight supported Key Features
• Provide details on deploying and managing the 8.7 Mobility Encrypted Tunnel Feature

Pre-requisite

You must have AireOS 8.0 or higher release on a Wireless LAN Controller in order to upgrade to the 8.5MR1 or 8.7 code.

Note

This feature is functional only in 8.5MR1 and 8.7 and above releases and is supported on 3504, 5520 and 8540 controllers.

Product or Feature Overview

The scope of the document is to provide a high level system description of support for End-to-End encryption of Mobility tunnel between Anchor and Foreign WLC. The document also describes the basic assumptions from the WLC perspective to support End-to-End encryption of Mobility tunnel between Anchor and Foreign WLC.

The architecture for End-to-End encryption of Mobility tunnel between Anchor and Foreign WLC is shown in the diagram below. In this architecture the WLCs are connected through CAPWAP based mobility tunnels which use DTLS encryption between the WLCs. The client data passes through secure DTLS encrypted CAPWAP tunnel between AP to WLC and between the Foreign and Anchor WLCs it passes through the CAPWAP based mobility tunnels which use DTLS encryption. Thus, through the entire data path from the client network to the Anchor WLC the client data is passing through encrypted tunnel with no scope for Man in the Middle snooping.
In release 8.7 end-to-end Tunnel encrypted between Anchor and Foreign Controllers

The encrypted tunnel passes through CAPWAP v4 with DTLS encryption

Old and New Mobility Architecture will be supported

Client SSO will be supported

Supported on 3504, 5520 and 8540 controllers

**Configuring Encrypted Mobility Tunnel**

To configure End to End Encrypted Mobility Tunnel in the release 8.7 follow the steps as indicated below.

**Procedure**

**Step 1**  Configure all the controllers that need to participate in the Mobility Group exchange. All controllers have to be configured with each other information.
Step 2
Enable Mobility Encryption on each controller.
After enabling Mobility Encryption, the controller will reboot.

(Cisco Controller) > config mobility group member add?
<IP addr> Member switch IP address

Step 3
Before rebooting, the controller will display the following message, hit OK and then Apply the change.

(Cisco Controller) > config mobility encryption?
enable Enables the encryption feature.

disable Disables the encryption feature.
Step 4  
After controllers that were configured with Encrypted Mobility Tunnel come up they will show with Status Up.

Figure 1:

```
(Cisco Controller) > show mobility summary
Mobility Protocol Port.............................. 16666
Default Mobility Domain............................. mxider
Multicast Mode.................................... Enabled
DT8 Mode ........................................... Enabled
Mobility Domain ID for 802.11s.................... 62911
Mobility Reappraisal Interval....................... 10
Mobility Reappraisal Count......................... 3
Mobility Group Members Configured................ 4
Mobility Control Message DSCP Value................ 0

Controllers configured in the Mobility Group
         MAC Address  IP Address   Status            Group Name  Multicast IP
00:12:97:0c:71:8b  10.90.39.28  Up     Control and Data Path Down  mxider  0.0.0.0
00:00:e0:1f:21:00  10.70.0.19  Up
00:00:e0:1f:21:00  10.70.0.17  Up
00:12:39:ee:62:db  10.70.0.16  Up
```

Step 5  
After the Mobility Encryption is enabled and Tunnel Link status shows as UP, one more check can be done to verify the encrypted connection is established. Perform MPING from one Controller to another Controller IP address over the Encrypted Tunnel and make sure MPING is successful.
<table>
<thead>
<tr>
<th>MAC Address</th>
<th>IP Address</th>
<th>Status</th>
<th>Group Name</th>
<th>Multicast IF</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:24:9f:71:9e:00</td>
<td>10.70.0.24</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>00:0b:4f:2a:00</td>
<td>10.70.0.19</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>00:0b:4f:2a:00</td>
<td>10.70.0.17</td>
<td>up</td>
<td></td>
<td></td>
</tr>
<tr>
<td>fc1b:39:1a:62:06</td>
<td>10.70.0.18</td>
<td>up</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

(Cisco Controller) >ping 10.70.0.17
Reply from 10.70.0.17: bytes=32 time=0ms TTL=64

Send count=5, Receive count=5 from 10.70.0.17

(Cisco Controller) >
Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).