Configuring Management Frame Protection

Protected Management Frames (Management Frame Protection)

By default, 802.11 management frames are unauthenticated and hence not protected against spoofing. Infrastructure management frame protection (MFP) and 802.11w protected management frames (PMF) provide protection against such attacks.

Infrastructure MFP

Infrastructure MFP protects management frames by detecting adversaries that are invoking denial-of-service attacks, flooding the network with associations and probes, interjecting as rogue APs, and affecting network performance by attacking the QoS and radio measurement frames. Infrastructure MFP is a global setting that provides a quick and effective means to detect and report phishing incidents.

Specifically, infrastructure MFP protects 802.11 session management functions by adding message integrity check information elements (MIC IEs) to the management frames emitted by APs (and not those emitted by clients), which are then validated by other APs in the network. Infrastructure MFP is passive, can detect and report intrusions but has no means to stop them.

Infrastructure MFP consists of three main components:

- **Management frame protection**: The AP protects the management frames it transmits by adding a MIC IE to each frame. Any attempt to copy, alter, or replay the frame invalidates the MIC, causing any receiving AP configured to detect MFP frames to report the discrepancy. MFP is supported for use with Cisco Aironet lightweight APs.
- **Management frame validation**: In infrastructure MFP, the AP validates every management frame that it receives from other APs in the network. It ensures that the MIC IE is present (when the originator is configured to transmit MFP frames) and matches the content of the management frame. If it receives any frame that does not contain a valid MIC IE from a BSSID belonging to an AP that is configured to

transmit MFP frames, it reports the discrepancy to the network management system. In order for the timestamps to operate properly, all controllers must be Network Time Protocol (NTP) synchronized.

- **Event reporting**: The AP notifies the controller when it detects an anomaly, and the controller aggregates the received anomaly events and can report the results through SNMP traps to the network management system.

Infrastructure MFP is disabled by default, and you can enable it globally. When you upgrade from a previous software release, infrastructure MFP is disabled globally if you have enabled AP authentication because the two features are mutually exclusive. When you enable infrastructure MFP globally, signature generation (adding MICs to outbound frames) can be disabled for selected WLANs, and validation can be disabled for selected APs.

Note CCXv5 client MFP is no longer supported. Client MFP is enabled as optional by default on WLANs that are configured for WPA2. However, client MFP is not supported on Wave 2 APs or 802.11ax Wi-Fi6 APs, and there exist no clients that support CCXv5.

802.11w PMF

802.11w standard protects the transmission of control and management frames, between APs and clients, against forgery and replay attacks. The frame types protected include Disassociation, Deauthentication, and Robust Action frames such as:

- Spectrum Management
- Quality of Service (QoS)
- Block Ack
- Radio measurement
- Fast Basic Service Set (BSS) Transition

For information about 802.11w PMF, see the 802.11w section.

Additional Reference: Configure 802.11w Management Frame Protection on WLC

This section contains the following subsections:

Restrictions for Management Frame Protection

- Lightweight access points support infrastructure MFP in local and monitor modes and in FlexConnect mode when the access point is connected to a controller. They support client MFP in local, FlexConnect, and bridge modes.
- Client MFP is supported for use only with CCXv5 clients using WPA2 with TKIP or AES-CCMP.
- Non-CCXv5 clients may associate to a WLAN if client MFP is disabled or optional.
- Error reports generated on a FlexConnect access point in standalone mode cannot be forwarded to the controller and are dropped.

Configuring Infrastructure MFP (GUI)

Step 1 Choose **Security> Wireless Protection Policies > AP Authentication/MFP** to open the AP Authentication Policy page.

Step 2 Enable infrastructure MFP globally for the controller by choosing **Management Frame Protection** from the **Protection Type** drop-down list.

Step 3 Click **Apply** to commit your changes.

Note If more than one controller is included in the mobility group, you must configure an NTP/SNTP server on all controllers in the mobility group that are configured for infrastructure MFP.

Step 4 Configure client MFP for a particular WLAN after infrastructure MFP has been enabled globally for the controller as follows:

a) Choose **WLANs**.

b) Click the profile name of the desired **WLAN**. The **WLANs > Edit** page appears.

c) Choose **Advanced**. The **WLANs > Edit (Advanced) page** is displayed.

d) From the **MFP Client Protection** drop-down list, choose **Disabled**, **Optional**, or **Required** . The default value is **Optional**. If you choose **Required**, clients are allowed to associate only if MFP is negotiated (that is, if WPA2 is configured on the controller and the client supports CCXv5 MFP and is also configured for WPA2).

Note For Cisco OEAP 600, MFP is not supported. It should either be Disabled or Optional.

e) Click **Apply** to commit your changes.

Step 5 Save the configuration.

Viewing the Management Frame Protection Settings (GUI)

To see the controller's current global MFP settings, choose **Security** > **Wireless Protection Policies** > **Management Frame Protection**. The Management Frame Protection Settings page appears.

On this page, you can see the following MFP settings:

- The **Management Frame Protection** field shows if infrastructure MFP is enabled globally for the controller.
- The **Controller Time Source Valid** field indicates whether the controller time is set locally (by manually entering the time) or through an external source (such as the NTP/SNTP server). If the time is set by an external source, the value of this field is "True." If the time is set locally, the value is "False." The time source is used for validating the timestamp on management frames between access points of different controllers within a mobility group.
- The **Client Protection** field shows if client MFP is enabled for individual WLANs and whether it is optional or required.

Configuring Infrastructure MFP (CLI)

Procedure

- Enable or disable infrastructure MFP globally for the controller by entering this command:

  config wps mfp infrastructure {enable | disable}
- Enable or disable client MFP on a specific WLAN by entering this command:

  config wlan mfp client {**enable** | **disable**} *wlan_id* [**required**]

  If you enable client MFP and use the optional **required** parameter, clients are allowed to associate only if MFP is negotiated.

Viewing the Management Frame Protection Settings (CLI)

Procedure

- See the controller's current MFP settings by entering this command:

  show wps mfp summary
- See the current MFP configuration for a particular WLAN by entering this command:

  show wlan wlan_id
- See whether client MFP is enabled for a specific client by entering this command:

  show client detail *client_mac*
- See MFP statistics for the controller by entering this command:

  show wps mfp *statistics*

Note This report contains no data unless an active attack is in progress. This table is cleared every 5 minutes when the data is forwarded to any network management stations.

Debugging Management Frame Protection Issues (CLI)

Procedure

- Use this command if you experience any problems with MFP:

  debug wps mfp ? {**enable** | **disable**}

  where ? is one of the following:

  client—Configures debugging for client MFP messages.

capwap—Configures debugging for MFP messages between the controller and access points.

detail—Configures detailed debugging for MFP messages.

report—Configures debugging for MFP reporting.

mm—Configures debugging for MFP mobility (inter-controller) messages.