Configuring Management Frame Protection

Information About Management Frame Protection

Management frame protection (MFP) provides security for the otherwise unprotected and unencrypted 802.11 management messages passed between access points and clients. MFP provides both infrastructure and client support.

- 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 access points, 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 access points (and not those emitted by clients), which are then validated by other access points in the network. Infrastructure MFP is passive. It can detect and report intrusions but has no means to stop them.

- Client MFP—Shields authenticated clients from spoofed frames, preventing many of the common attacks against wireless LANs from becoming effective. Most attacks, such as deauthentication attacks, revert to simply degrading performance by contending with valid clients.

  Specifically, client MFP encrypts management frames are sent between access points and CCXv5 clients so that both the access points and clients can take preventative action by dropping spoofed class 3 management frames (that is, management frames passed between an access point and a client that is authenticated and associated). Client MFP leverages the security mechanisms defined by IEEE 802.11i to protect the following types of class 3 unicast management frames: disassociation, deauthentication,

and QoS (WMM) action. Client MFP protects a client-access point session from the most common type of denial-of-service attack. It protects class 3 management frames by using the same encryption method used for the session's data frames. If a frame received by the access point or client fails decryption, it is dropped, and the event is reported to the controller.

To use client MFP, clients must support CCXv5 MFP and must negotiate WPA2 using either TKIP or AES-CCMP. EAP or PSK may be used to obtain the PMK. CCKM and controller mobility management are used to distribute session keys between access points for Layer 2 and Layer 3 fast roaming.

Note To prevent attacks using broadcast frames, access points supporting CCXv5 will not emit any broadcast class 3 management frames (such as disassociation, deauthentication, or action). CCXv5 clients and access points must discard broadcast class 3 management frames.

Client MFP supplements infrastructure MFP rather than replaces it because infrastructure MFP continues to detect and report invalid unicast frames sent to clients that are not client-MFP capable as well as invalid class 1 and 2 management frames. Infrastructure MFP is applied only to management frames that are not protected by client MFP.

Infrastructure MFP consists of three main components:

- Management frame protection—The access point 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 access point configured to detect MFP frames to report the discrepancy. MFP is supported for use with Cisco Aironet lightweight access points.
- Management frame validation—In infrastructure MFP, the access point validates every management frame that it receives from other access points 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 access point 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 access point 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.

Note Client MFP uses the same event reporting mechanisms as infrastructure MFP.

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

Client MFP is enabled by default on WLANs that are configured for WPA2. It can be disabled, or it can be made mandatory (in which case, only clients that negotiate MFP are allowed to associate) on selected WLANs.

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.
- OEAP 600 Series Access points do not support MFP.
- 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 Management Frame Protection (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 appears.

d) Choose **Disabled**, **Optional**, or **Required** from the MFP Client Protection drop-down list. 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 Click **Save Configuration** to save your settings.

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 Management Frame Protection (CLI)

- 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)

- 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)

- 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.