Management Frame Protection

Information About 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.

Supported Access Point Models

Cisco MFP is supported on the following AP models:

- Cisco Aironet 2802, 3802, and 4802 series access points
- Cisco Aironet 2800, 3800, 4800, and 1560 series access points

Unsupported Access Point Models

Cisco MFP is not supported on the following AP models:

- Cisco Aironet 1800 and 1900 series access points
- Cisco 802.11ax access points
- All Cisco IOS access points

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.
- Client MFP is supported for use only with CCXv5 clients using WPA2 with TKIP or AES-CCMP.
- Client MFP is not supported on Cisco Wave 1 APs and Cisco Wave 2 APs.
- OEAP 600 series access points do not support MFP.
- 802.11ax access points do not support MFP.
- 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.
- Keys are generated using random number generator but you can improve the keys by changing to SHA.

- MFP key for each BSSID is not supported.

Configuring Management Frame Protection (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless wps mfp** **Example:** `Device(config)# wireless wps mfp`	Configures a management frame protection.

Step 3	**wireless wps mfp** {**ap-impersonation** | **key-refresh-interval**}
	Example:
	`Device(config)# wireless wps mfp ap-impersonation`
	`Device(config)# wireless wps mfp key-refresh-interval`
		Configures ap impersonation detection (or) MFP key refresh interval in hours.
		key-refresh-interval—Refers to the MFP key refresh interval in hours. The valid range is from 1 to 24. Default value is 24.

Step 4	**end** **Example:** `Device(config)# end`	Saves the configuration and exits configuration mode and returns to privileged **EXEC** mode.

Verifying Management Frame Protection Settings

To verify if the Management Frame Protection (MFP) feature is enabled or not, use the following command:

```
Device# show wireless wps summary
Client Exclusion Policy
  Excessive 802.11-association failures   : unknown
  Excessive 802.11-authentication failures: unknown
  Excessive 802.1x-authentication         : unknown
  IP-theft                                : unknown
  Excessive Web authentication failure    : unknown
  Failed Qos Policy                       : unknown

Management Frame Protection
  Global Infrastructure MFP state : Enabled
  AP Impersonation detection      : Disabled
  Key refresh interval            : 15
```

To view the MFP details, use the following command:

```
Device# show wireless wps mfp summary
Management Frame Protection
  Global Infrastructure MFP state : Enabled
  AP Impersonation detection      : Disabled
  Key refresh interval            : 15
```

To view the MFP statistics details, use the following command:

```
Device# show wireless wps mfp statistics
BSSID          Radio DetectorAP                       LastSourceAddr Error           Count
     FrameTypes

aabb.ccdd.eeff a     AP3800                           aabb.ccdd.eeff Invalid MIC     10
     Beacon, Probe Response
                                                                     Invalid MIC     20
     Beacon, Probe Response
```

To verify if access points support MFP validation and protection, use the following command:

```
Device# show wireless wps mfp ap summary
AP Name                          Radio MAC               Validation            Protection
-------------------------------------------------------------------------------------------
AP002A.1087.CBF4                 00a2.eefd.bdc0          Enabled               Enabled
AP58AC.78DE.9946                 00a2.eeb8.4ae0          Enabled               Enabled
APb4de.3196.caac                 4c77.6d83.6b90          Enabled               Enabled
```