



# Management Frame Protection

---

This document describes how to configure Management Frame Protection (MFP).

## Understanding Management Frame Protection

Management Frame Protection provides security for the management messages passed between access point (AP) and Client stations. MFP consists of two functional components: Infrastructure MFP and Client MFP.

Infrastructure MFP provides infrastructure support. Infrastructure MFP utilizes a message integrity check (MIC) across broadcast and directed management frames. This check assists in detecting of rogue devices and denial-of-service attacks. Client MFP provides client support.

Client MFP protects authenticated clients from spoofed frames, by preventing many of the common attacks against WLANs from becoming effective.

Management Frame Protection operation requires a wireless domain service (WDS). MFP is configured at the wireless LAN solution engine (WLSE), but you can manually configure MFP on an AP and WDS.



**Note**

---

If a WLSE is not present, then MFP cannot report detected intrusions and thus has limited effectiveness. If a WLSE is present, you should perform the configuration from the WLSE.

---

For complete protection, you should also configure an MFP AP for Simple Network Time Protocol (SNTP).

Client MFP encrypts class 3 management frames sent between APs and Cisco Compatible Extension version 5 (CCXv5)—capable client stations, so that both AP and client can take preventive action by dropping spoofed class 3 management frames (management frames) that are passed between an AP and a client station that is authenticated and associated). Client MFP leverages the security mechanisms defined by IEEE 802.11i to protect class 3 unicast management frames. The unicast cipher suite that is negotiated by the STA in the reassociation request's Robust Security Network Information Element (RSNIE) is used to protect both unicast data and class 3 management frames. An AP in workgroup bridge mode, repeater mode, or no-root bridge mode must negotiate either Temporal Key Integrity Protocol (TKIP) or Advanced Encryption Standard-Cipher Block Chaining Message Authentication Code Protocol (AES-CCMP) to use Client MFP.



---

**Americas Headquarters:**  
**Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA**

© 2008 Cisco Systems, Inc. All rights reserved.

## Protection of Unicast Management Frames

Unicast class 3 management frames are protected by applying either AES-CCMP or TKIP in a manner that is similar to that used for data frames. Client MFP is enabled for autonomous APs only if the encryption is AES-CCMP or TKIP and key management is Wi-Fi Protected Access version 2 (WPA2).

## Protection of Broadcast Management Frames

To prevent attacks using broadcast frames, APs that support CCXv5 do not emit any broadcast class 3 management frames. An AP in workgroup bridge mode, repeater mode, or non-root bridge mode discards broadcast class 3 management frames if Client MFP is enabled.

Client MFP is enabled for autonomous APs only if the encryption is AES-CCMP or TKIP and key management is WPA2.

## Client MFP For Access Points in Root mode

Autonomous APs in root mode support mixed-mode clients. Clients capable of CCXv5 with negotiated cipher suite AES or TKIP with WPA2 are Client MFP enabled. Client MFP is disabled for clients that are not CCXv5 capable. By default, Client MFP is optional for a particular service set identifier (SSID) on the AP. Client MFP can be enabled or disabled by using the command-line interface (CLI) in SSID configuration mode.

Client MFP can be configured as either required or optional for a particular SSID. To configure Client MFP as required, you must configure the SSID with key management WPA2 mandatory. If the key management is not WPA2 mandatory, an error message is displayed and your CLI command is rejected. If you attempt to change the key management with Client MFP configured as required and key management WPA2, an error message is displayed and your CLI command is rejected. When configured as optional, Client MFP is enabled if the SSID is capable of WPA2; otherwise, Client MFP is disabled.

## Configuring Client MFP

The following CLI commands are used to configure Client MFP for APs in root mode.

- **ids mfp client required**

This SSID configuration command enables Client MFP as required on a particular SSID. The dot11radio interface is reset when the command is executed. The command also assumes that the SSID is configured with WPA2 mandatory. If the SSID is not configured with WPAv2 mandatory, an error message is displayed and the command is rejected.

- **no ids mfp client**

This SSID configuration command disables Client MFP on a particular SSID. The dot11radio interface is reset when the command is executed.

- **ids mfp client optional**

This SSID configuration command enables Client MFP as optional on a particular SSID. The dot11radio interface is reset when the command is executed. Client MFP is enabled for this particular SSID if the SSID is WPA2 capable; otherwise, Client MFP is disabled.

- **show dot11 ids mfp client statistics**

Use this command to display Client MFP statistics on the AP console for a dot11radio interface.

- **clear dot11 ids mfp client statistics**  
Use this command to clear the Client MFP statistics.
- **authentication key management wpa version {1 | 2}**  
Use this command to explicitly specify which WPA version to use for WPA key management for a particular SSID.

## Configuring Infrastructure MFP

To configure infrastructure MFP, follow these step, beginning in privileged EXEC mode:

	Command	Description
Step 1	<b>configure terminal</b>	Enters global configuration mode.
Step 2	<b>dot11 ids mfp generator</b>	Configures the AP as an MFP generator. When enabled, the AP protects the management frames it transmits by adding a Message Integrity Check Information Element (MIC IE) to each frame. Any attempt to copy, alter, or replay the frame will invalidate the MIC, causing any receiving AP that is configured to detect (validate) MFP frames to report the discrepancy. The AP must be a member of a WDS.
Step 3	<b>dot11 ids mfp detector</b>	Configures the AP as an MFP detector. When enabled, the AP validates management frames it receives from other APs. If the AP receives any frame that does not contain a valid, and expected, MIC IE, it will report the discrepancy to the WDS. The AP must be a member of a WDS.
Step 4	<b>sntp server <i>server IP address</i></b>	Enters the name or IP address of the SNTP server.
Step 5	<b>end</b>	Returns to the privileged EXEC mode.
Step 6	<b>copy running-config startup-config</b>	(Optional) Saves your entries in the configuration file.

To configure the WDS, follow these steps, beginning in privileged EXEC mode WDS:

	Command	Description
Step 1	<b>configure terminal</b>	Enters global configuration mode.
Step 2	<b>dot11 ids mfp distributor</b>	Configures the WDS as an MFP distributor. When enabled, the WDS manages signature keys that are used to create the MIC IEs, and the WDS securely transfers them between generators and detectors.
Step 3	<b>end</b>	Returns to the privileged EXEC mode.
Step 4	<b>copy running-config startup-config</b>	(Optional) Saves your entries in the configuration file.

