# 使用WLC和LAP的基礎設施管理幀保護(MFP)配置示例

## 目錄



## 簡介

本檔案介紹無線中一種稱為管理訊框保護(MFP)的新安全功能。 本檔案也說明如何在輕型存取點(LAP)和無線LAN控制器(WLC)等基礎架構裝置上設定MFP。

## 必要條件

### 需求

- 瞭解如何配置WLC和LAP以實現基本操作
- IEEE 802.11管理幀的基本知識

### 採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Cisco 2000系列WLC（執行韌體版本4.1）
- Cisco 1131AG LAP
- 運行韌體版本3.6的Cisco Aironet 802.11a/b/g客戶端介面卡
- Cisco Aironet案頭實用程式版本3.6

**注意**：WLC 4.0.155.5版及更高版本支援MFP，但4.0.206.0版通過MFP提供最佳效能。4.1.171.0及更高版本支援客戶端MFP。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

## 慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

# 背景資訊

在802.11中，(de)authentication、(dis)association、beacons和探測器等管理幀始終未經驗證且未加密。換句話說，802.11管理幀始終以不安全的方式傳送，與資料流量不同，資料流量使用WPA、WPA2（至少是WEP）等協定加密。

這使得攻擊者能夠偽裝來自AP的管理幀，以攻擊與AP關聯的客戶端。利用欺騙的管理幀，攻擊者可以執行以下操作：

- 在WLAN上運行拒絕服務(DOS)
- 重新連線客戶端時，嘗試中間人攻擊客戶端
- 運行離線字典攻擊

MFP在驗證在無線網路基礎設施中交換的802.11管理幀時克服了這些缺陷。

**注意：本**文檔重點介紹基**礎設施和客戶端MFP**。

**注意**：某些無線客戶端與支援MFP的基礎設施裝置通訊存在某些限制。MFP向每個探測請求或SSID信標新增一組長資訊元素。一些無線客戶端（如PDA、智慧手機、條形碼掃描器等）記憶體和CPU有限。因此，您無法處理這些請求或信標。因此，您完全看不到SSID，或者由於對SSID功能的誤解而無法與這些基礎設施裝置關聯。此問題並非特定於MFP。具有多個資訊元素(IE)的任何SSID也會出現這種情況。 在即時部署之前，建議使用所有可用的客戶端型別在環境中測試啟用了MFP的*SSID*。

**附註**：

以下是基礎架構MFP的元件：

- **管理幀保護** — 啟用管理幀保護時，AP將消息完整性檢查資訊元素(MIC IE)新增到其傳輸的每個管理幀。任何複製、更改或重播幀的嘗試都會使MIC失效。配置為驗證MFP幀的AP收到的MIC無效的幀，會將其報告給WLC。
- **管理幀驗證** — 啟用管理幀驗證後，AP會驗證從網路中的其他AP收到的每個管理幀。它確保MIC IE存在（當發起方被配置為傳輸MFP幀時），並且匹配管理幀的內容。如果它從屬於配置為傳輸MFP幀的AP的BSSID接收到不包含有效MIC IE的任何幀，則會向網路管理系統報告差異

。**注意**：為使時間戳正常運行，所有WLC必須同步網路時間協定(NTP)。
- **事件報**告 — 接入點檢測到異常時通知WLC。WLC聚合異常事件並通過SNMP陷阱將其報告給網路管理器。

## 基礎架構MFP功能

使用MFP時，所有管理幀都會以密碼方式雜湊以建立消息完整性檢查(MIC)。 MIC將新增到幀的末尾(在幀校驗序列(FCS)之前)。

- 在集中式無線架構中，基礎架構MFP在WLC上啟用/禁用（全域性配置）。 可以針對每個WLAN選擇性地禁用保護，也可以針對每個AP選擇性地禁用驗證。
- 在無法處理額外IE的裝置使用的WLAN上可以禁用保護。
- 必須在超載或超載的AP上禁用驗證。

在WLC中設定的一個或多個WLAN上啟用MFP時，WLC會向每個註冊AP上的每個無線電傳送唯一金鑰。AP通過啟用MFP的WLAN傳送管理幀。這些AP標有幀保護MIC IE。任何更改幀的嘗試都會使消息失效，從而導致配置為檢測MFP幀的接收AP向WLAN控制器報告差異。

這是在漫遊環境中實現的MFP的逐步過程：

1. 全域性啟用MFP後，WLC將為為MFP配置的每個AP/WLAN生成唯一金鑰。WLC在自身內部通訊，以便所有WLC知道行動網域中所有AP/BSS的金鑰。**注意**：移動/RF組中的所有控制器都必須以相同方式配置MFP。
2. 當AP收到其不知道的BSS的MFP保護幀時，它會緩衝該幀的副本並查詢WLC以獲取金鑰。
3. 如果BSSID在WLC上未知，它將向AP返回消息「未知BSSID」，AP將丟棄從該BSSID接收的管理幀。
4. 如果WLC上已知BSSID，但該BSSID上禁用了MFP，則WLC返回「已禁用BSSID」。 然後AP假設從該BSSID接收的所有管理幀都不具有MFP MIC。
5. 如果BSSID已知且已啟用MFP，WLC會將MFP金鑰傳回提出要求的AP（透過AES加密的LWAPP管理通道）。
6. AP快取以這種方式接收的金鑰。此金鑰用於驗證或新增MIC IE。

## 客戶端MFP功能

客戶端MFP可保護經過身份驗證的客戶端免受偽裝幀的攻擊，從而阻止對無線LAN的許多常見攻擊的有效性。大多數攻擊（如取消身份驗證攻擊）在與有效客戶端競爭時恢復為效能降級。

具體來說，客戶端MFP加密在接入點和CCXv5客戶端之間傳送的管理幀，以便接入點和客戶端都可以採取預防措施並丟棄偽裝的第3類管理幀（即，在接入點與經過身份驗證和關聯的客戶端之間傳遞的管理幀）。 客戶端MFP利用IEEE 802.11i定義的安全機制來保護這些型別的3類單播管理幀：取消關聯、取消身份驗證和QoS(WMM)操作。客戶端MFP可以保護客戶端接入點會話免受最常見的拒絕服務攻擊。它使用與會話資料幀相同的加密方法來保護第3類管理幀。如果接入點或客戶端接收的幀解密失敗，則會丟棄該幀，並向控制器報告該事件。

要使用客戶端MFP，客戶端必須支援CCXv5 MFP並且必須使用TKIP或AES-CCMP協商WPA2。EAP或PSK可用於獲取PMK。CCKM和控制器移動性管理用於在接入點之間分配會話金鑰或第2層和第3層快速漫遊。

為了防止對廣播幀的攻擊，支援CCXv5的接入點不會發出任何廣播第3類管理幀（如取消關聯、取消身份驗證或操作）。CCXv5客戶端和接入點必須丟棄廣播第3類管理幀。

客戶端MFP補充了基礎架構MFP，而不是取代它，因為基礎架構MFP繼續檢測並報告傳送給不支援客戶端MFP的客戶端的無效單播幀以及無效的第1類和第2類管理幀。基礎架構MFP僅應用於不受客戶端MFP保護的管理幀。

## 客戶端MFP元件

客戶端MFP由以下元件組成：

- 金鑰生成和分發
- 管理框架的保護和驗證
- 錯誤報告

## 金鑰生成和分發

客戶端MFP不使用為基礎架構MFP派生的金鑰生成和分發機制。相反，客戶端MFP利用IEEE 802.11i定義的安全機制來保護第3類單播管理幀。站點必須支援CCXv5，並且必須協商TKIP或AES-CCMP才能使用客戶端MFP。EAP或PSK可用於獲取PMK。

## 保護管理幀

應用AES-CCMP或TKIP保護單播第3類管理幀，其方式與資料幀已使用的方式類似。幀報頭的部分被複製到每個幀的加密負載元件中，以增強保護，如下一節所述。

這些幀型別受到保護：

- 解除關聯
- 取消驗證
- QoS(WMM)操作幀

AES-CCMP和TKIP保護的資料幀在IV欄位中包括用於防止重放檢測的序列計數器。當前傳輸計數器用於資料幀和管理幀，但新的接收計數器用於管理幀。接收計數器經過測試，以確保每個幀的數量都高於最後一個接收的幀（以確保這些幀是唯一的，並且沒有被重放），因此該方案導致接收值不是連續的並不重要。

## 錯誤報告

MFP-1報告機制用於報告接入點檢測到的管理幀解封裝錯誤。即，WLC收集MFP驗證錯誤統計資訊，並定期將整理的資訊轉發到WCS。

客戶端站點檢測到的MFP違規錯誤由CCXv5漫遊和即時診斷功能處理，不在本文檔的討論範圍內。

## 廣播管理訊框保護

為了防止使用廣播幀的攻擊，支援CCXv5的AP不會傳輸任何廣播類3（即，disassoc、deauth或action）管理幀，但惡意包含取消身份驗證/取消關聯幀除外。支援CCXv5的客戶端站點必須丟棄廣播第3類管理幀。假設MFP會話位於正確保護的網路中（強身份驗證加上TKIP或CCMP），因此忽略惡意遏制廣播不會造成問題。

同樣，AP會丟棄入站廣播管理幀。目前不支援任何傳入廣播管理訊框，因此不需要對此進行代碼變更。

## 支援的平台

支援以下平台：

- WLAN控制器200621064400WiSM含嵌入式440x控制器的375026/28/37/38xx路由器
- LWAPP存取點AP 1000AP 1100、1130AP 1200、1240、1250AP 1310
- 使用者端軟體ADU 3.6.4及更高版本
- 網路管理系統WCS

此版本不支援1500網狀LWAPP AP。

## 支援的模式

在這些模式下運行的基於LWAPP的接入點支援客戶端MFP:

| **支援的接入點模式** | |
|---|---|
| **模式** | **客戶端MFP支援** |
| 本地 | 是 |
| 監視 | 否 |
| 監聽器 | 否 |
| 惡意檢測器 | 否 |
| 混合REAP | 是 |
| REAP | 否 |
| 網橋根 | 是 |
| WGB | 否 |

## 混合單元支援

不支援CCXv5的客戶端工作站可以與MFP-2 WLAN關聯。接入點跟蹤哪些客戶端支援MFP-2，哪些客戶端不支援，以便確定MFP-2安全措施是否應用於出站單播管理幀以及入站單播管理幀中是否預期應用。

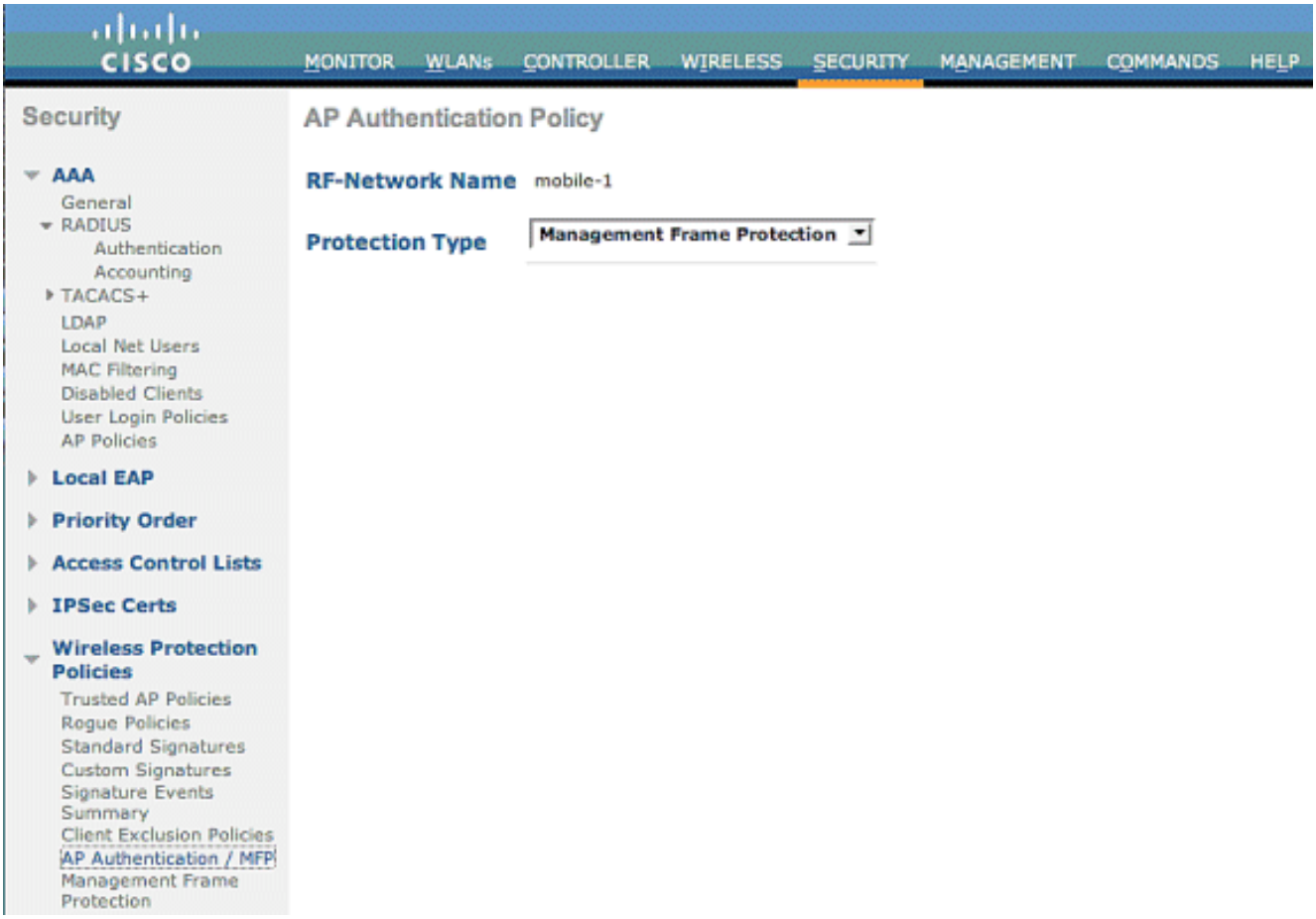
# 設定

## 在控制器上配置MFP

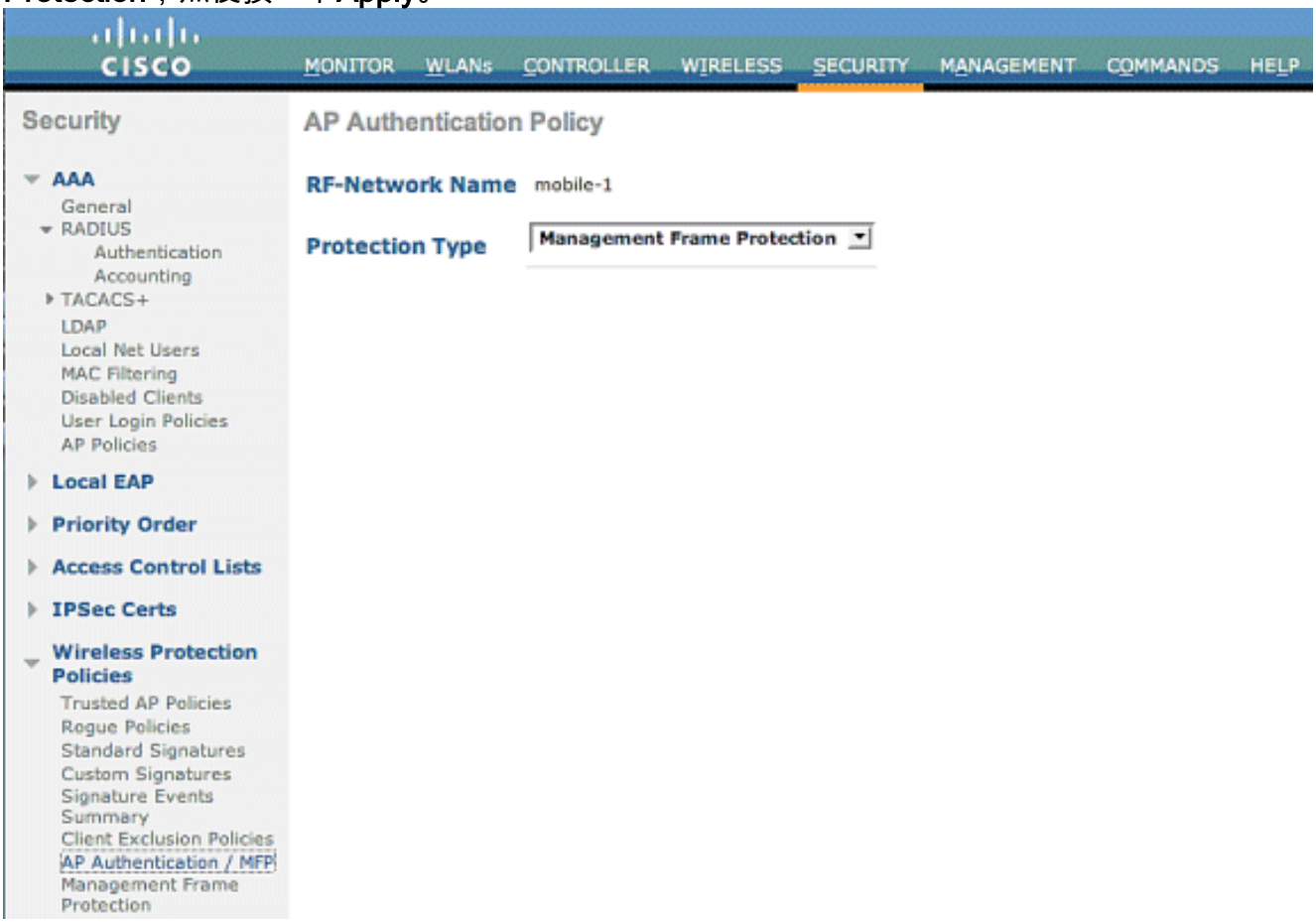
您可以在控制器上全域性配置MFP。執行此操作時，**預設情況下會為每個加入的接入點啟用管理幀保護和驗**證，並且自動禁用接入點身份驗證。

執行以下步驟在控制器上全域性配置MFP。

1. 在控制器GUI上，按一下「Security」。在出現的螢幕中，按一下Wireless Protection Policies下的AP Authentication/MFP。



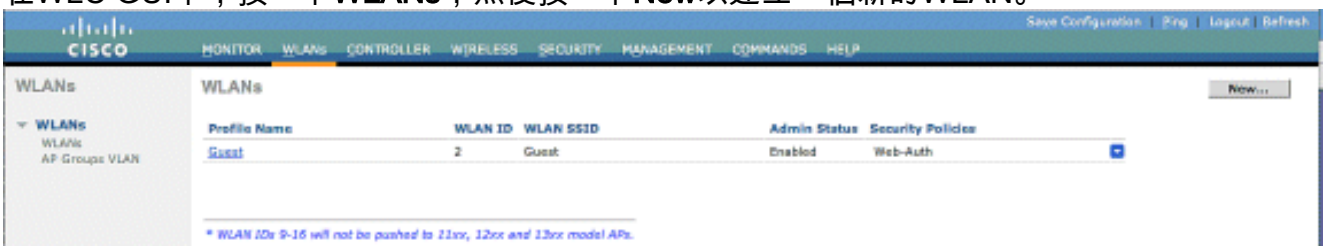

2. 在AP Authentication Policy中，從**Protection Type**下拉選單中選擇**Management Frame Protection**，然後按一下**Apply**。



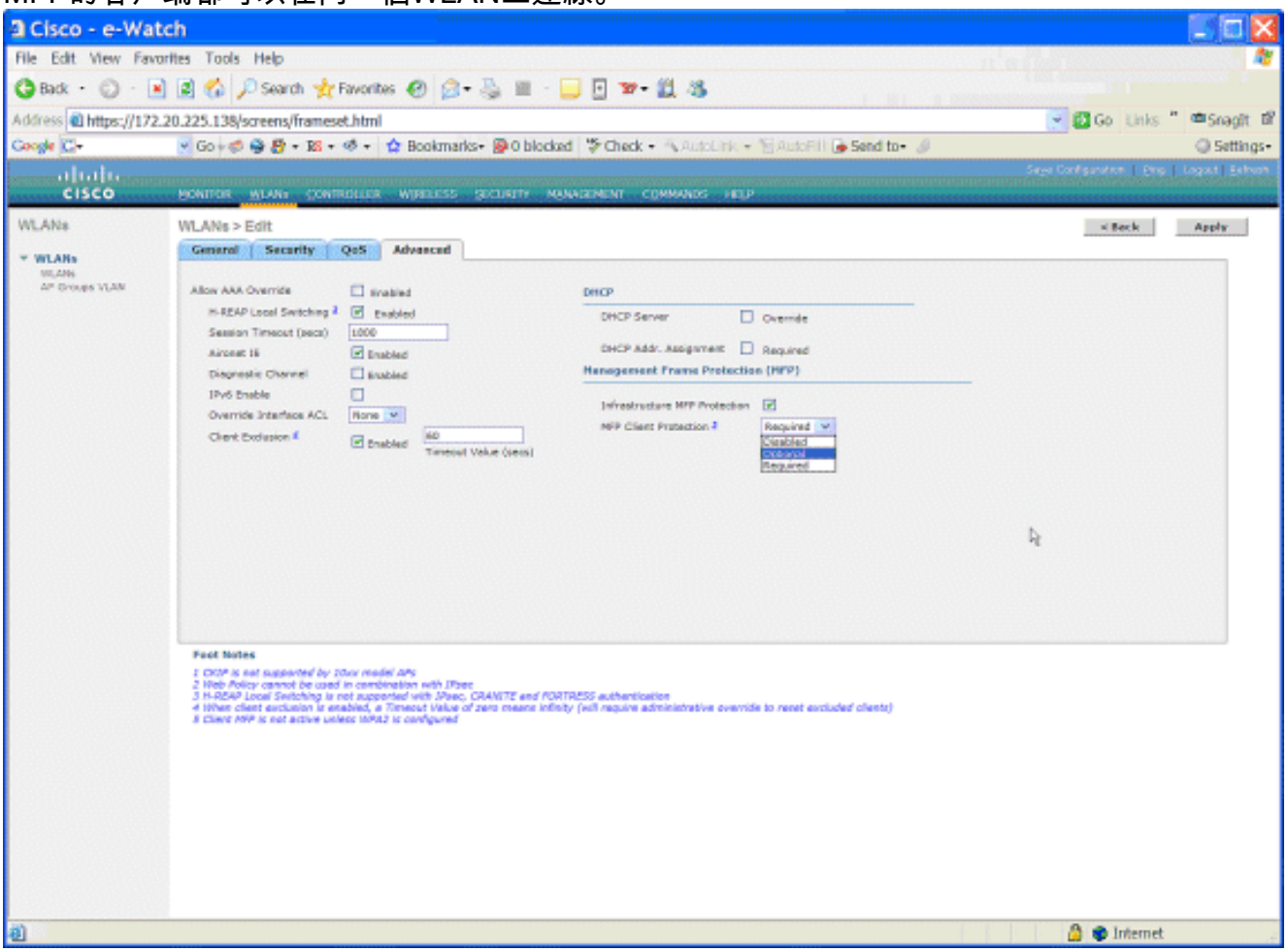

## 在WLAN上配置MFP

您還可以在WLC上配置的每個WLAN上啟用/禁用基礎架構MFP保護和客戶端MFP。通過基礎設施MFP保護（僅在全域性啟用時啟用）預設啟用這兩個功能，而客戶端MFP僅在為WLAN配置WPA2安全性時啟用。若要在WLAN上啟用MFP，請執行以下步驟：

1. 在WLC GUI中，按一下**WLANs**，然後按一下**New**以建立一個新的WLAN。

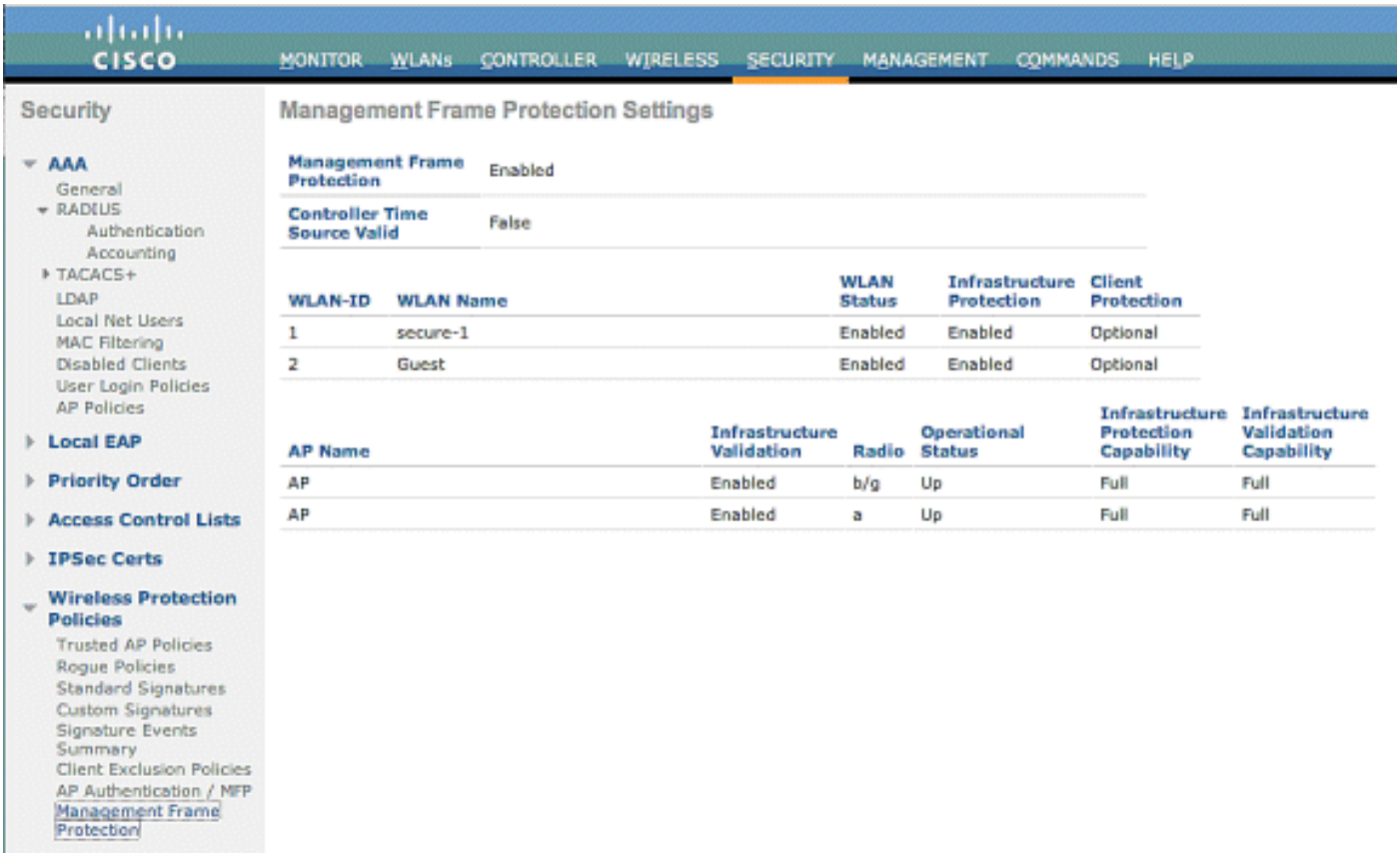



2. 在WLAN編輯頁面上，轉至*Advanced*頁籤，然後選中**Infrastructure MFP Protection**覈取方塊以啟用此WLAN上的基礎架構MFP。若要停用此WLAN的基礎架構MFP保護，請取消選中此覈取方塊。要啟用客戶端MFP，請從下拉選單中選擇必需或可選選項。如果選擇Client MFP= Required，請確保所有客戶端都支援MFP-2或它們無法連線。如果選擇可選，則啟用MFP和非MFP的客戶端都可以在同一個WLAN上連線。




## 驗證

要從GUI驗證MFP配置，請在「安全」頁面的「無線保護策略」下按一下**管理**幀保護。這會將您帶到MFP設定頁面。




在MFP Settings頁面中，您可以檢視WLC、LAP和WLAN上的MFP配置。範例如下。

- Management Frame Protection欄位顯示WLC是否已全域性啟用MFP。
- Controller Time Source Valid欄位指示WLC時間是本地設定（通過手動輸入時間）還是通過外部源（例如NTP伺服器）設定。 如果時間由外部源設定，則此欄位的值為「True」。 如果時間在本地設定，則值為「False」。 時間來源用於驗證同時配置了移動性的不同WLC的接入點之間的管理幀。**注意：**如果在移動/RF組中的所有WLC上啟用MFP，則始終建議您使用NTP伺服器來設定移動組中的WLC時間。
- **MFP Protection**欄位顯示是否為單個WLAN啟用MFP。
- **MFP驗證**欄位顯示是否為單個接入點啟用MFP。

以下show命令可能很有用：

- **show wps summary** — 使用此命令可檢視WLC的當前無線保護策略（包括MFP）的摘要。
- **show wps mfp summary** — 若要檢視WLC的當前全域性MFP設定，請輸入以下命令。
- show ap config general *AP_name* — ***要檢視特定接入點的當前MFP狀態，請輸入以下命令。***

以下是**show ap config general *AP_name*** 命令輸出的範例：

```
(Cisco Controller) >show ap config general AP

Cisco AP Identifier.............................. 4
Cisco AP Name.................................... AP
Country code..................................... US  - United States
Regulatory Domain allowed by Country............. 802.11bg:-AB    802.11a:-AB
AP Country code.................................. US  - United States
AP Regulatory Domain............................. 802.11bg:-A    802.11a:-A
Switch Port Number .............................. 29
MAC Address...................................... 00:19:2f:7e:3a:30
IP Address Configuration......................... DHCP
IP Address....................................... 172.20.225.142
IP NetMask....................................... 255.255.255.248
```

```
Gateway IP Addr.............................. 172.20.225.137
Cisco AP Location............................ default location
Cisco AP Group Name.......................... default-group
Primary Cisco Switch.........................
Secondary Cisco Switch.......................
Tertiary Cisco Switch........................
Administrative State ........................ ADMIN_ENABLED
Operation State ............................. REGISTERED
Mirroring Mode .............................. Disabled
AP Mode ..................................... H-Reap
Public Safety ............................... Global: Disabled, Local: Disabled
Remote AP Debug ............................. Disabled
S/W  Version ................................ 4.1.169.24
Boot  Version ............................... 12.3.7.1
Mini IOS Version ............................ 3.0.51.0
Stats Reporting Period ...................... 180
LED State.................................... Enabled
PoE Pre-Standard Switch...................... Disabled
PoE Power Injector MAC Addr.................. Disabled
Number Of Slots.............................. 2
AP Model..................................... AIR-LAP1242AG-A-K9
IOS Version.................................. 12.4(20070414:021809)
Reset Button................................. Enabled
AP Serial Number............................. FTX1035B3QX
AP Certificate Type.......................... Manufacture Installed
H-REAP Vlan mode :........................... Disabled
Management Frame Protection Validation....... Enabled
Console Login Name...........................
Console Login State.......................... Unknown
Ethernet Port Duplex......................... Auto
Ethernet Port Speed.......................... Auto
```

以下是**show wps mfp summary**命令的輸出示例：

```
(Cisco Controller) >show wps mfp summary

Global MFP state.............................. enabled
Controller Time Source Valid.................. false


                                    WLAN       Infra.      Client
WLAN ID  WLAN Name                  Status     Protection  Protection
-------  -------------------------  ---------  ----------  ----------
1        secure-1                   Enabled    Enabled     Optional
2        Guest                      Enabled    Enabled     Optional but inactive (WPA2 not
configured)

                     Infra.             Operational     --Infra. Capability--
AP Name              Validation  Radio  State           Protection  Validation
-------------------  ----------  -----  --------------  ----------  ----------
AP                   Enabled     b/g    Up              Full        Full
```

以下debug指令可能很有用；

- **debug wps mfp lwapp** — 顯示MFP消息的調試資訊。
- **debug wps mfp detail** — 顯示MFP消息的詳細調試資訊。

- **debug wps mfp report** — 顯示MFP報告的調試資訊。
- **debug wps mfp mm** — 顯示MFP移動（控制器間）消息的調試資訊。

**注意**：Internet上還提供了幾個免費的無線資料包嗅探器，可用於捕獲和分析802.11管理幀。某些封包監聽器範例是Omnipeek和Wireshark。

## 相關資訊

- 配置安全解決方案：WLC組態設定指南
- 在WCS中配置安全解決方案
- 使用WLAN控制器(WLC)的EAP驗證組態範例
- 無線LAN控制器上的ACL組態範例
- 使用無線 LAN 控制器的外部 Web 驗證組態範例
- 使用RADIUS伺服器和無線LAN控制器進行動態VLAN分配配置示例
- 採用EAP-FAST驗證的Cisco安全服務使用者端
- WLC常見問題
- 無線支援頁面
- 技術支援與文件 - Cisco Systems