使用WLC和LAP的基础设施管理帧保护(MFP)配置示例

目录

简介
先决条件
要求
使用的组件
规则
背景信息
基础架构 MFP 功能
客户端 MFP 功能
客户端 MFP 组件
密钥生成和分配
管理帧保护
错误报告
广播管理帧保护
支持的平台
支持的模式
混合信元支持
配置
在控制器上配置 MFP
在 WLAN 上配置 MFP
验证
相关信息

简介

本文档介绍了一种新的无线安全功能，称为管理帧保护 (MFP)。 本文档也描述了如何在基础架构设备中配置 MFP，例如轻量接入点 (LAP) 和无线 LAN 控制器 (WLC)。

先决条件

要求

- 了解如何配置 WLC 和 LAP 以进行基本操作
- 基本了解 IEEE 802.11 管理帧

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 运行固件版本 4.1 的 Cisco 2000 系列 WLC
- Cisco 1131AG LAP
- 运行固件版本 3.6 的 Cisco Aironet 802.11a/b/g 客户端适配器
- Cisco Aironet Desktop Utility 版本 3.6

注意：WLC版本4.0.155.5及更高版本支持MFP，但版本4.0.206.0使用MFP提供最佳性能。在版本4.1.171.0 及更高版本上支持客户端 MFP。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

背景信息

在 802.11 中，管理帧始终未认证且未加密，例如（取消）认证、（解除）关联、信标和探测。换句话说，802.11 管理帧始终在非安全的方式下进行发送，这与使用以下协议加密的数据流不同，如 WPA、WPA2，或至少 WEP 等等。

这允许攻击者伪装来自 AP 的管理帧攻击与 AP 关联的客户端。使用伪装的管理帧，攻击者可执行以下操作：

- 在 WLAN 上运行拒绝服务 (DOS)
- 当重新连接时，试图在客户端上进行中间人攻击
- 运行脱机字典攻击

当验证在无线网络基础架构中交换的 802.11 管理帧时，MFP 克服了这些缺陷。

注意：本文档重点介绍基**础设施和客户端MFP。**

注意：某些无线客户端与启用MFP的基础设施设备通信存在某些限制。MFP 将一组冗长的信息元素添加到每个探测请求或 SSID 信标。有些无线客户端具有有限内存和 CPU，例如 PDA、智能电话、条码扫描仪等等。因此，您不能处理这些请求或信标。因此，由于误解了 SSID 功能，您无法完全看到 SSID，或者您不能与这些基础架构设备关联。此问题不是 MFP 特有的问题。这还出现在具有多信息元素 (IE) 的任何 SSID 上。 在您实时部署之前，始终建议使用所有可用的客户端类型测试环境中*启用 MFP 的 SSID。*

注意：

这些是基础架构 MFP 的组件：

- **管理帧保护 — 当启用管理帧保护时，AP 将消息完整性检查信息元素 (MIC IE) 添加到其传输的每个管理帧。**任何试图复制、修改或者重播帧的操作均使 MIC 无效。配置用来验证 MFP 帧的一个 AP 接收到具有无效 MIC 的帧，并将其报告给 WLC。
- **管理帧验证— 当启用管理帧验证时，AP 验证其从网络中其他 AP 接收的每个管理帧。**这确保 MIC IE 存在（当配置发送方来传输 MFP 帧时）并与管理帧的内容匹配。如果它从属于 AP 的 BSSID 处接收了不包含有效 MIC IE 的任何帧（配置用来传输 MFP 帧），则向网络管理系统报

告这一差异。**注意：**要使时间戳正常运行，所有WLC必须同步网络时间协议(NTP)。
- **事件报告 — 当检测到异常情况时，接入点通知 WLC。**WLC 聚集了异常事件并通过 SNMP 陷阱向网络管理器报告。

基础架构 MFP 功能

使用 MFP，所有管理帧被秘密地进行散列处理，以创建消息完整性检查 (MIC)。 MIC 被添加到帧的末端（在帧检查顺序 (FCS) 之前）。

- 在集中化无线体系结构中，在 WLC（全局配置）上启用/禁用基础架构 MFP。 可以选择性地禁用每个 WLAN 的保护，并且可以选择性地禁用每个 AP 的验证。
- 可以在 WLAN 上禁用保护，该 WLAN 由无法处理额外的 IE 的设备使用。
- 在过载或供电过量的 AP 上必须禁用验证。

当在 WLC 中配置的一个或多个 WLAN 上启用 MFP 时，WLC 将唯一的密钥发送到每个已注册 AP 上的每个无线电。AP 通过启用 MFP 的 WLAN 发送管理帧。这些 AP 标有帧保护 MIC IE。任何试图修改帧的操作均使消息无效，这导致配置用来检测 MFP 帧的接收 AP 向 WLAN 控制器报告这一差异。

这是在漫游环境中实施 MFP 的逐步过程：

1. 全局启用 MFP 时，WLC 生成为 MFP 配置的每个 AP/WLAN 的唯一密钥。WLC 在其自身内部进行通信，以便所有的 WLC 都了解移动域中所有 AP/BSS 的密钥。**注意：移**动/RF组中的所有控制器必须配置相同的MFP。
2. 当 AP 接收到其不了解的 BSS 的保护 MFP 帧时，它将缓冲该帧的副本，并查询 WLC 获得密钥。
3. 如果 BSSID 在 WLC 上未知，则向 AP 返回消息“未知 BSSID”，AP 丢弃从此 BSSID 接收的管理帧。
4. 如果 BSSID 在 WLC 上已知，但 MFP 在该 BSSID 上已禁用，则 WLC 返回“已禁用 BSSID”消息。 然后，AP 假设从该 BSSID 接收的所有管理帧都没有 MFP MIC。
5. 如果 BSSID 已知并且已启用 MFP，则 WLC 向请求的 AP 返回 MFP 密钥（通过 AES 加密的 LWAPP 管理隧道）。
6. AP 缓存以这种方式接收的密钥。此密钥用于验证或添加 MIC IE。

客户端 MFP 功能

客户端 MFP 屏蔽了来自伪装帧的已认证客户端，这阻止了对无线 LAN 的许多常见攻击的效果。当多数攻击（例如取消认证攻击）对付有效客户端时，它们开始性能下降。

具体而言，客户端 MFP 加密在接入点和 CCXv5 客户端之间发送的管理帧，以便接入点和客户端均能采取预防措施并丢弃伪装的第 3 类管理帧（即，管理帧在验证且关联的接入点和客户端之间通过）。 客户端 MFP 有效利用由 IEEE 802.11i 定义的安全机制来保护这些类型的第 3 类单播管理帧：解除关联、取消认证和 QoS (WMM) 操作。客户端 MFP 可以保护来自多数常见类型拒绝服务攻击的客户端接入点会话。它使用用于会话的数据帧的同一加密方法保护第 3 类管理帧。如果接入点或客户端接收的帧解密失败，则将其丢失，并将事件报告给控制器。

为了使用客户端 MFP，客户端必须支持 CCXv5 MFP，并且必须与 TKIP 或 AES-CCMP 协商 WPA2。EAP 或 PSK 可用于获取 PMK。CCKM 和控制器移动管理用于分配在接入点或第 2 层和第 3 层快速漫游之间的会话密钥。

为了阻止对广播帧的攻击，支持 CCXv5 的接入点不发出任何广播第 3 类管理帧（例如解除关联、取消认证或操作）。CCXv5 客户端和接入点必须丢弃广播第 3 类管理帧。

客户端 MFP 补充了基础架构 MFP，而不是将其替换，因为基础架构 MFP 继续检测和报告发送到不支持客户端 MFP 的客户端的无效单播帧，以及无效的第 1 类和第 2 类管理帧。基础架构 MFP 仅适用于未由客户端 MFP 保护的管理帧。

客户端 MFP 组件

客户端 MFP 包括以下组件：

- 密钥生成和分配
- 管理帧的保护和验证
- 错误报告

密钥生成和分配

客户端 MFP 不使用基础架构 MFP 派生的密钥生成和分配机制。相反，客户端 MFP 有效利用 IEEE 802.11i 定义的安全机制来保护第 3 类单播管理帧。站点必须支持 CCXv5，并且必须与 TKIP 或 AES-CCMP 协商以使用客户端 MFP。EAP 或 PSK 可用于获取 PMK。

管理帧保护

通过 AES-CCMP 或 TKIP 的应用，以用于数据帧的类似方式保护单播第 3 类管理帧。将帧报头的部分复制到附加保护的每个帧的加密有效负载组件中，如以下部分所述。

这些帧类型受到保护：

- 取消关联
- 取消身份验证
- QoS (WMM) 操作帧

受 AES-CCMP 和 TKIP 保护的数据帧包括 IV 字段中的顺序计数器，用于阻止重播检测。当前传输计数器用于数据和管理帧，但是一个新的接收计数器用于管理帧。测试接收计数器确保每个帧都有比最后接收的帧更高的编号（确保帧是唯一的并且未被重播），因此此方案造成已接收的值不连续并不重要。

错误报告

MFP-1 报告机制用于报告由接入点检测的管理帧解封装错误。即，WLC 收集 MFP 验证错误统计信息，并定期将整理的信息转发至 WCS。

客户端工作站检测的 MFP 违规错误由 CCXv5 漫游和实时诊断功能进行处理，且不在本文档的范围内。

广播管理帧保护

为了防止使用广播帧的攻击，支持 CCXv5 的 AP 不传输任何广播第 3 类（即解除关联、取消认证或操作）管理帧，除了恶意遏制的解除关联/取消认证帧。支持 CCXv5 的客户端站点必须丢弃广播第 3 类管理帧。假设 MFP 会话在一个适当保护的网络（强认证加上 TKIP 或 CCMP）中，因此对恶意遏制广播的忽略并不是问题。

同样，AP 丢弃入站广播管理帧。当前不支持入站广播管理帧，因此该操作不要求代码更改。

支持的平台

这些平台受到支持：

- WLAN 控制器200621064400WiSM具有嵌入式 440x 控制器的 375026/28/37/38xx 路由器
- LWAPP 接入点AP 1000AP 1100、1130AP 1200、1240、1250AP 1310
- 客户端软件ADU 3.6.4 及以上
- 网络管理系统WCS

该版本中不支持 1500 Mesh LWAPP AP。

支持的模式

这些模式中运行的基于 LWAPP 的接入点支持客户端 MFP：

支持的接入点模式	
模式	**客户端 MFP 支持**
本地	Yes
监控	无
嗅探器	无
恶意检测器	无
混合 REAP	Yes
REAP	无
根网桥	Yes
WGB	无

混合信元支持

不支持 CCXv5 的客户端站点可与 MFP-2 WLAN 进行关联。接入点记录哪些客户端支持 MFP-2，哪些不支持，以确定 MFP-2 安全措施是否适用于出站单播管理帧并预计适用于入站单播管理帧。

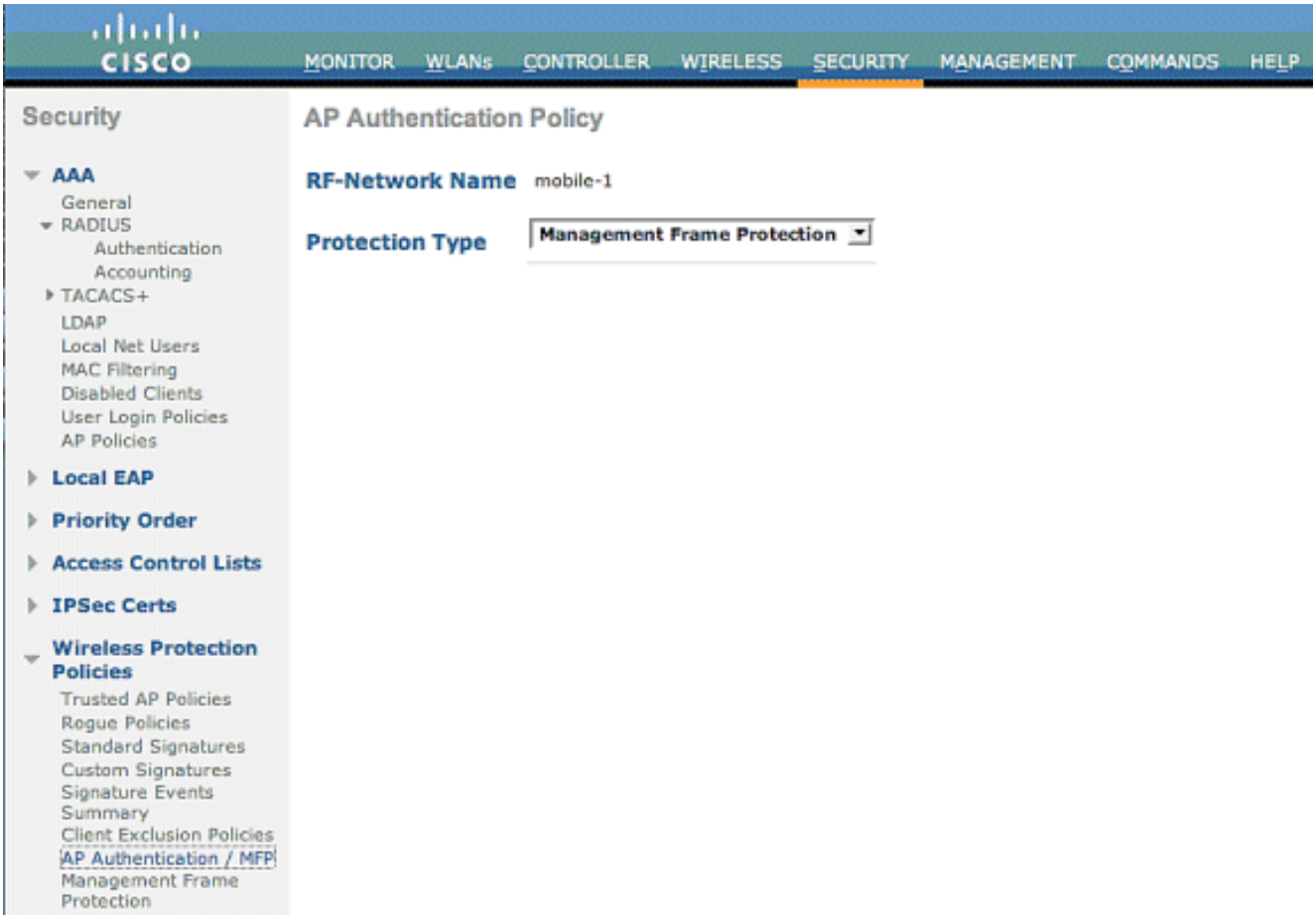
配置

在控制器上配置 MFP

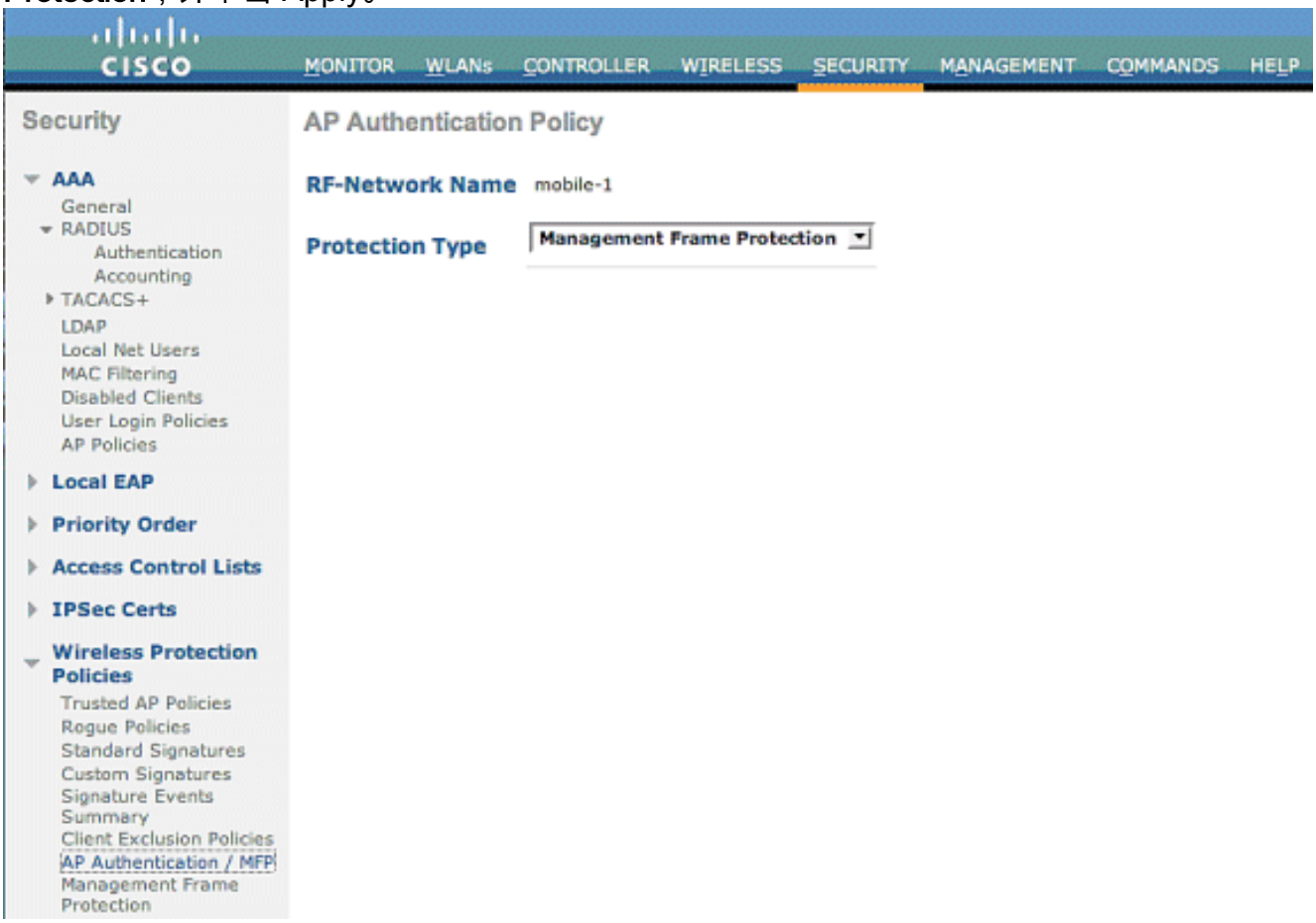
您可以在控制器上全局配置 MFP。进行此操作时，**每个加入的接入点管理帧的保护和验证默认启用**，并且自动禁用接入点认证。

执行这些步骤，以在控制器上全局配置 MFP。

1. 从控制器 GUI 中，单击 **Security**。在由此产生的屏幕上单击 **Wireless Protection Policies 之下的 AP Authentication/MFP**。



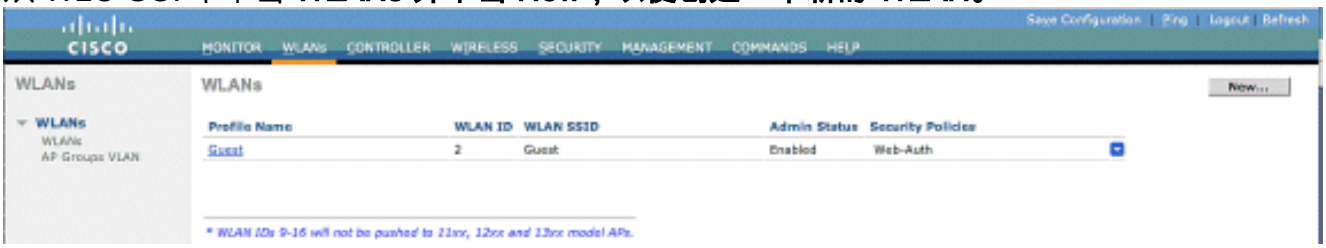
2. 在 AP 认证策略中，请从 **Protection Type 下拉菜单中选择 Management Frame Protection**，并单击 Apply。



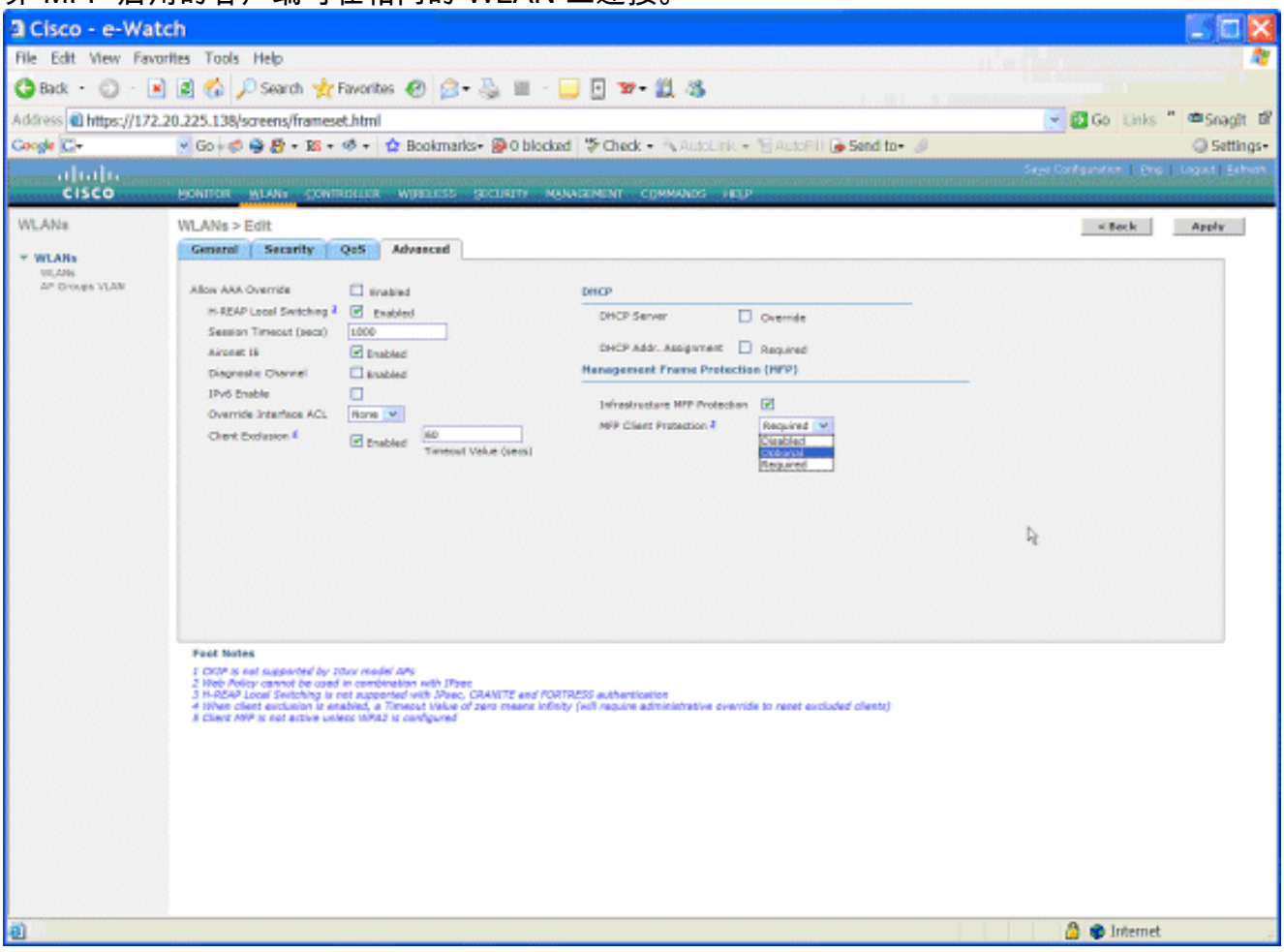
在 WLAN 上配置 MFP

您也可以在 WLC 上配置的每个 WLAN 上启用/禁用基础架构 MFP 保护和客户端 MFP。在默认情况下两者都已通过基础架构 MFP 保护启用，这仅在全局启用时有效，而且客户端 MFP 仅在 WLAN 配置了 WPA2 安全时有效。执行下列步骤以便在 WLAN 上启用 MFP：

1. 从 WLC GUI 中单击 **WLANs 并单击 New，以便创建一个新的 WLAN。**

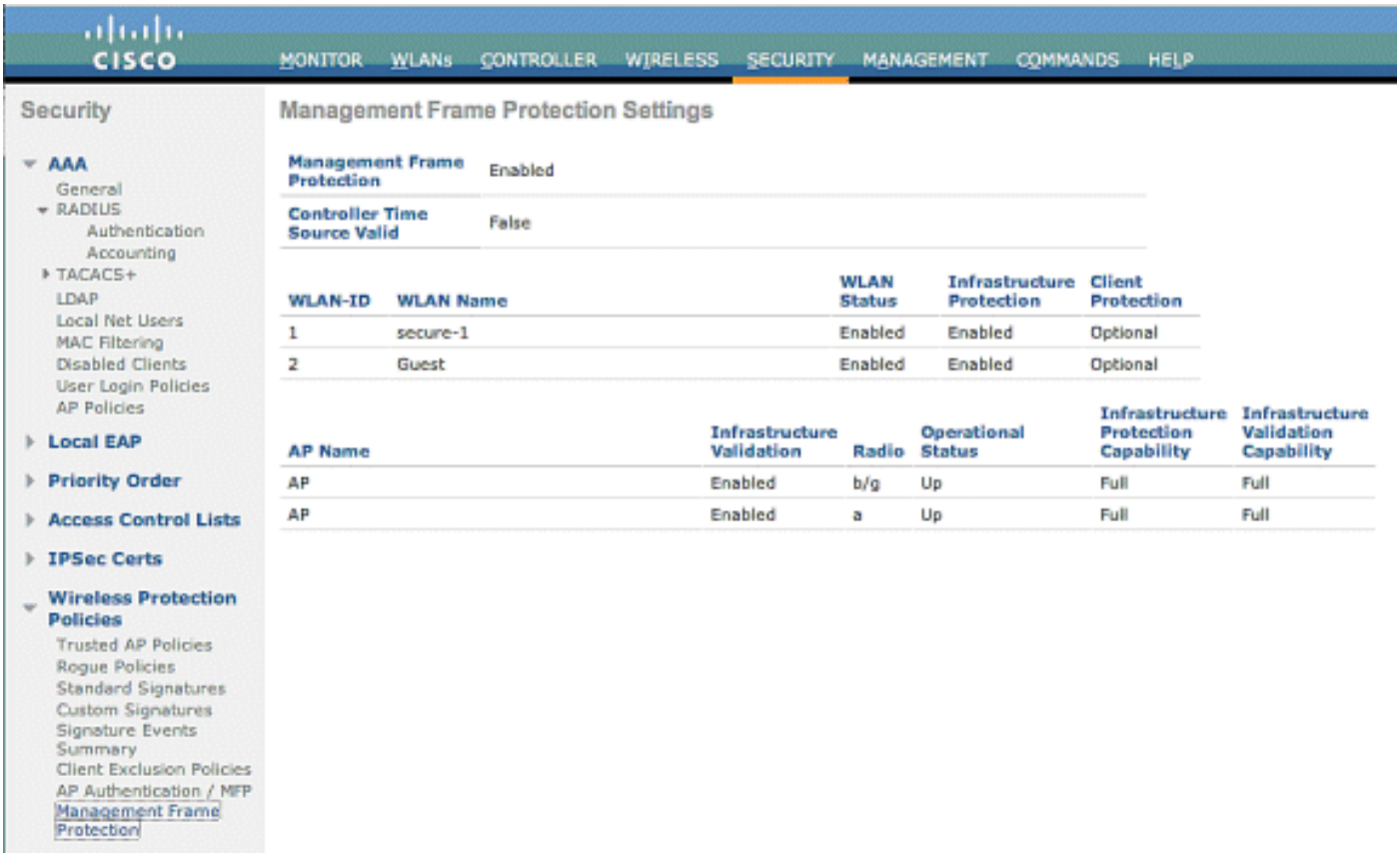


2. 在 WLANs 编辑页面，转到 *Advanced 选项卡 并选中* **Infrastructure MFP Protection 复选框，以在此 WLAN 上启用基础架构 MFP。**为了禁用此 WLAN 的基础架构 MFP 保护，取消选中此复选框。为了启用客户端 MFP，从下拉菜单中选择所需的或可选选项。如果您选择 Client MFP= Required，请确保所有的客户端可支持 MFP-2 或无法连接。如果您选择可选，MFP 和非 MFP 启用的客户端可在相同的 WLAN 上连接。



验证

为了从 GUI 验证 MFP 配置，请单击 Security 页面的 Wireless Protection Policies 之下的 **Management Frame Protection。**此操作将带您进入 MFP Settings 页面。



在 MFP Settings 页面中，您可以在 WLC、LAP 和 WLAN 上看到 MFP 配置。示例如下。

- 如果为 WLC 全局启用 MFP，将显示管理帧保护字段。
- 控制器时间源有效字段指示是否在本地（通过手动时间输入）或通过外部源（例如 NTP 服务器）对 WLC 时间进行设置。 如果由外部源设置时间，此字段的值为“True”。 如果是本地设置时间，则值为“False”。 时间源用于验证也配置有移动性的不同 WLC 的接入点之间的管理帧。**注意：**如果在移动/RF组中的所有WLC上启用了MFP，则始终建议使用NTP服务器在移动组中设置WLC时间。
- 如果启用单个 WLAN 的 MFP，则显示 **MFP 保护字段。**
- 如果启用单个接入点的 MFP，则显示 **MFP 验证字段。**

这些显示命令可用于以下操作：

- **show wps summary** — 使用此命令，以便查看 WLC 的当前无线保护策略（包括 MFP）的汇总。
- **show wps mfp summary — 为查看 WLC 的当前全局 MFP 设置，请输入此命令。**
- **show ap config general *AP_name*** — 为查看特定接入点的当前 MFP 状态，请输入此命令。

这是 **show ap config general *AP_name*** 命令的输出示例：

```
(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
```

这是 show wps mfp summary 命令的输出示例：

```
(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
```

这些 debug 命令可能很有帮助；

- debug wps mfp lwapp — 显示 MFP 消息的调试信息。

- debug wps mfp detail — 显示 MFP 消息的详细调试信息。
- debug wps mfp report — 显示 MFP 报告的调试信息。
- debug wps mfp mm — 显示 MFP 移动性（控制器之间）消息的调试信息。

注意：Internet上还提供几个免费无线数据包嗅探器，可用于捕获和分析802.11管理帧。一些示例数据包嗅探器为 Omnipeek 和 Wireshark。

相关信息

- 配置安全解决方案：WLC 配置指南
- 在 WCS 中配置安全解决方案
- WLAN 控制器 (WLC) 中 EAP 身份验证的配置示例
- 无线 LAN 控制器中的 ACL 配置示例
- 使用无线局域网控制器的外部 Web 身份验证配置示例
- 带有RADIUS服务器的动态VLAN分配和无线局域网控制器的配置示例
- 使用 EAP-FAST 身份验证的 Cisco 安全服务客户端
- WLC 常见问题解答
- 无线支持页
- 技术支持和文档 - Cisco Systems