WLC と LAP でのインフラストラクチャ管理フレーム保護（MFP）設定例

内容

概要

このドキュメントでは、Management Frame Protection（MFP; 管理フレーム保護）と呼ばれるワイヤレスでの新しいセキュリティ機能を解説しています。 さらに、Lightweight Access Point（LAP; Lightweight アクセス ポイント）やワイヤレス LAN コントローラ（WLC）などのインフラストラクチャ デバイスで MFP を設定する方法についても説明しています。

前提条件

要件

- 基本動作用に WLC と LAP を設定する方法に関する知識
- IEEE 802.11 管理フレームに関する基本的な知識

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- ファームウェア リリース 4.1 が稼働する Cisco 2000 シリーズ WLC
- Cisco 1131AG LAP
- ファームウェア リリース 3.6 が稼働する Cisco Aironet 802.11a/b/g クライアント アダプタ
- Cisco Aironet Desktop Utility バージョン 3.6

注：MFPはWLCバージョン4.0.155.5以降でサポートされていますが、バージョン4.0.206.0ではMFPに最適なパフォーマンスが提供されます。クライアント MFP はバージョン 4.1.171.0 以降でサポートされています。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

背景説明

802.11 では、認証（およびその解除）、関連付け（およびその解除）、ビーコン、プローブなどの管理フレームは常に認証が行われず、暗号化もされません。つまり、802.11 の管理フレームは常にセキュリティ保護されていない方式で送信されます。これは、WPA、WPA2、または少なくとも WEP などのプロトコルで暗号化されるデータ トラフィックとは異なります。

このため、攻撃者は AP からの管理フレームをスプーフィングして、AP に関連付けられたクライアントを攻撃できます。スプーフィングされた管理フレームを使用すると、攻撃者は次のアクションを実行できます。

- WLAN での Denial of Service（DoS; サービス拒否攻撃）の実行
- クライアントが再接続する際にクライアントでの中間者攻撃の試行
- オフラインの辞書攻撃の実行

MFP は、ワイヤレス ネットワーク インフラストラクチャで交換される 802.11 の管理フレームを認証する際の、これらの欠点を克服します。

注：このドキュメントでは、インフラストラクチャとクライアントMFPに焦点を当てています。

注：一部の無線クライアントがMFP対応のインフラストラクチャデバイスと通信する場合には、一定の制限があります。MFP により、各プローブ要求または SSID ビーコンには、一連の長い情報要素が付加されます。PDA、スマートフォン、バーコード スキャナなどの一部のワイヤレス クライアントは、メモリと CPU が制限されています。そのため、ユーザはこれらの要求またはビーコンを処理できません。その結果、SSID 機能が正確に把握されないため、SSID を完全に確認できなかったり、これらのインフラストラクチャ デバイスとの関連付けができなくなります。この問題は MFP に特有なものではありません。これは、複数の Information Element（IE; 情報要素）を含むすべての SSID でも発生します。 リアルタイムで展開する前に、使用可能なすべてのクライアント タイプが実装された環境で MFP *対応*の SSID をテストすることが、常に推奨されます。

注：

インフラストラクチャ MFP のコンポーネントには次のものがあります。

- **管理フレーム保護**：管理フレーム保護が有効である場合、AP により、伝送される各管理フレームに Message Integrity Check Information Element（MIC IE; メッセージ完全性チェック情報要素）が付加されます。フレームのコピー、変更、または再生を試みると、MIC が無効となります。AP は、MFP フレームを検証するように設定されているため、無効な MIC の付いたフレームを受信すると、それを WLC に報告します。
- **管理フレーム検証**：管理フレーム検証が有効である場合、AP では、ネットワーク内の他の AP から受信されるすべての管理フレームが検証されます。これにより、MIC IE が存在していて（発信側が MFP フレームを送信するよう設定されている場合）、管理フレームの中身が一致していることが確認されます。MFP フレームを送信するよう設定されている AP に属する BSSID から有効な MIC IE が含まれていないフレームを受信した場合は、その矛盾がネットワーク管理システムに報告されます。**注：タイムスタ**ンプを正しく動作させるには、すべてのWLCがネットワークタイムプロトコル(NTP)同期されている必要があります。
- **イベント報告**：アクセス ポイントはは異常を検出すると WLC に通知します。WLC は異常イベントを集積して、SNMP トラップ経由でそれをネットワーク管理者に報告します。

インフラストラクチャ MFP の機能

MFP を使用すると、Message Integrity Check（MIC; メッセージ完全性チェック）を作成するためにすべての管理フレームは暗号ハッシュ化されます。 MIC はフレームの末尾（Frame Check Sequence（FCS; フレーム チェック シーケンス）の前）に付加されます。

- 中央集中型ワイヤレス アーキテクチャでは、インフラストラクチャ MFP は WLC 上で有効/無効が切り替えられます（グローバル設定）。 WLAN 単位で選択的に保護を無効にすることができ、AP 単位で選択的に検証を無効にすることができます。
- 余分の IE を処理できないデバイスにより使用される WLAN 上で、保護を無効にすることができます。
- 過負荷または過出力状態の AP では、検証を無効にする必要があります。

WLC で設定されている 1 つ以上の WLAN で MFP が有効である場合、WLC から、登録された各 AP 上の各無線に一意の鍵が送信されます。管理フレームは、MFP 対応の WLAN 経由で AP により送信されます。これらの AP には、フレーム保護 MIC IE のラベルが付けられます。フレームを変更しようとするとメッセージが無効になり、MFP フレームを検出するように設定されている受信側 AP が WLAN コントローラに不一致を報告します。

ローミング環境で実装されている場合、MFP の一連のプロセスは次のようになります。

1. MFP がグローバルに有効になっていると、WLC により、MFP 用に設定されているあらゆる AP/WLAN 用に一意の鍵が生成されます。WLC は相互間で通信を行うため、すべての WLC ではモビリティ ドメイン内のすべての AP/BSS の鍵が認識されます。**注：モビリ**ティ/RFグループ内のすべてのコントローラで、MFPが同じように設定されている必要があります。
2. AP で未知の BSS に関する MFP 保護フレームが受信されると、フレームのコピーがバッファリングされ、鍵を取得するために WLC に照会されます。
3. WLC で BSSID が未知のものである場合、AP にはメッセージ「Unknown BSSID」が返され、AP ではその BSSID から受信された管理フレームは廃棄されます。

4. WLC で BSSID が既知のものであっても、その BSSID で MFP が無効になっていると、WLC からは「Disabled BSSID」が返されます。 続いて AP では、その BSSID から受信されたすべての管理フレームには MFP MIC がないものと見なされます。
5. BSSID が既知のものであり、BSSID で MFP が有効である場合、（AES 暗号化 LWAPP 管理トンネル経由で）WLC から要求側 AP に MFP 鍵が返されます。
6. AP ではこのようにして受信された鍵がキャッシュ化されます。この鍵は、MIC IE の検証または追加に使用されます。

クライアント MFP の機能

クライアント MFP により、スプーフされたフレームから認証済みクライアントが保護されるので、ワイヤレス LAN に対する一般的な攻撃の多くが無力化されます。認証解除攻撃などの大多数の攻撃では、有効なクライアントと競合することにより、単にパフォーマンスが低下するだけです。

具体的には、アクセス ポイントとクライアントの両方が、スプーフされたクラス 3 管理フレーム（つまり、認証済みで関連付けされているクライアントとアクセス ポイント間で受け渡される管理フレーム）を廃棄して予防措置を講じることができるように、クライアント MFP ではアクセス ポイントと CCXv5 クライアント間で送信される管理フレームが暗号化されます。 クライアントMFPは、IEEE 802.11iで定義されたセキュリティメカニズムを利用して、次のタイプのクラス3ユニキャスト管理フレームを保護します。関連付け解除、認証解除、およびQoS(WMM)アクション。クライアント MFP では、最も一般的な DoS 攻撃から、クライアントアクセス ポイント セッションを保護できます。ここでは、セッションのデータ フレームで使用されるのと同じ暗号化方式を使用することにより、クラス 3 管理フレームが保護されます。アクセス ポイントやクライアントで受信されるフレームを復号化できない場合、フレームは廃棄され、このイベントがコントローラに報告されます。

クライアント MFP を使用するには、クライアントは CCXv5 MFP をサポートしている必要があり、TKIP または AES-CCMP のいずれかで WPA2 をネゴシエートする必要があります。PMK を取得するためには、EAP または PSK を使用できます。アクセス ポイント間で、またはレイヤ 2 とレイヤ 3 の高速ローミングでセッション鍵を配布するためには、CCKM およびコントローラ モビリティ管理が使用されます。

ブロードキャスト フレームに対する攻撃を防ぐために、CCXv5 をサポートしているアクセス ポイントでは、ブロードキャスト クラス 3 管理フレーム（関連付け解除、認証解除、またはアクションなど）は送信されません。CCXv5 クライアントとアクセス ポイントでは、ブロードキャスト クラス 3 管理フレームを破棄する必要があります。

クライアント MFP は、インフラストラクチャ MFP を置き換えるのではなく、補足します。これは、インフラストラクチャ MFP が、無効なクラス 1 管理フレームとクラス 2 管理フレームだけではなく、クライアント MFP 対応ではないクライアントに送信される無効なユニキャスト フレームを検出して報告し続けるためです。インフラストラクチャ MFP は、クライアント MFP によって保護されていない管理フレームにのみ適用されます。

クライアント MFP のコンポーネント

クライアント MFP は次のコンポーネントから構成されます。

- 鍵の生成と配布
- 管理フレームの保護と検証

- エラー レポート

鍵の生成と配布

クライアント MFP では、インフラストラクチャ MFP 向けに導出された鍵の生成と配布のメカニズムは使用されません。その代わりに、クライアント MFP では、クラス 3 ユニキャスト管理フレームを保護するために、IEEE 802.11i で定義されたセキュリティ メカニズムが利用されます。クライアント MFP を使用するには、ステーションで CCXv5 がサポートされている必要があり、TKIP と AES-CCMP のいずれかがネゴシエートされる必要があります。PMK を取得するためには、EAP または PSK を使用できます。

管理フレームの保護

すでにデータ フレームに使用されている方式に似た方式で AES-CCMP と TKIP のいずれかを適用することにより、ユニキャスト クラス 3 管理フレームは保護されます。以降で説明するように、フレーム ヘッダーの各部分は、保護を強化するために各フレームの暗号化されたペイロード コンポーネントにコピーされます。

次のフレームの種類が保護されます。

- 関連付け解除
- 認証解除
- QoS（WMM）アクション フレーム

AES-CCMP および TKIP により保護されたデータ フレームには IV フィールドにシーケンス カウンタが含まれます。このカウンタはリプレイ検出を防止するために使用されます。現在の送信カウンタはデータ フレームと管理フレームの両方に使用されますが、管理フレームには新しい受信カウンタが使用されます。受信カウンタは、各フレームが、最後に受信されたフレームよりも大きな数値を持つことを確認するため（フレームが一意であり、リプレイされていないことを確認するため）にテストされます。そのため、このスキームにより、受信された値が非連続になっても問題はありません。

エラー レポート

アクセス ポイントにより検出された管理フレーム カプセル化解除エラーを報告するために、MFP-1 レポート メカニズムが使用されます。つまり、WLC は MFP 検証エラー統計情報を収集し、定期的に照合情報を WCS に転送します。

クライアント ステーションにより検出された MFP 違反エラーは、CCXv5 のローミングおよびリアルタイム診断機能により処理されるため、このドキュメントでは取り扱いません。

ブロードキャスト管理フレーム保護

ブロードキャスト フレームを使用する攻撃を防止するために、CCXv5 をサポートする AP は、不正 AP 抑止認証解除/関連付け解除フレームを除き、ブロードキャスト クラス 3（つまり関連付け解除、認証解除、またはアクション）管理フレームを送信しません。CCXv5 対応クライアント ステーションは、ブロードキャスト クラス 3 管理フレームを廃棄する必要があります。MFP セッションは適切にセキュリティ保護されたネットワーク（強力な認証と TKIP または CCMP）内にあると想定されているため、不正 AP 抑止ブロードキャストを無視しても問題にはなりません。

同様に、AP では着信ブロードキャスト管理フレームが廃棄されます。現在、着信ブロードキャスト管理フレームはサポートされていないため、このためのコード変更は必要ありません。

対応プラットフォーム

次のプラットフォームがサポートされています。

- WLAN コントローラ2006210644400WISM組み込み 440x コントローラを搭載した 375026/28/37/38xx ルータ
- LWAPP アクセス ポイントAP 1000AP 1100、1130AP 1200、1240、1250AP 1310
- クライアント ソフトウェアADU 3.6.4 以降
- ネットワーク管理システムWCS

このリリースでは 1500 Mesh LWAPP AP はサポートされていません。

サポート対象モード

次のモードで動作する LWAPP ベースのアクセス ポイントでは、クライアント MFP がサポートされています。

サポート対象のアクセス ポイントのモード	
モード	**クライアント MFP のサポート**
Local	Yes
モニタ	No
スニファ	No
Rogue Detector	No
ハイブリッド REAP	Yes
REAP	No
ブリッジ ルート	Yes
WGB	No

混合セルのサポート

CCXv5 対応ではないクライアント ステーションは、MFP-2 WLAN と関連付けを行うことができます。MFP-2 セキュリティ対策が、発信ユニキャスト管理フレームに適用され、着信ユニキャスト管理フレームで想定されているかどうかを判断するために、アクセス ポイントでは、どのクライアントが MFP-2 対応で、どのクライアントが MFP-2 非対応であるかのトラッキングが継続されます。

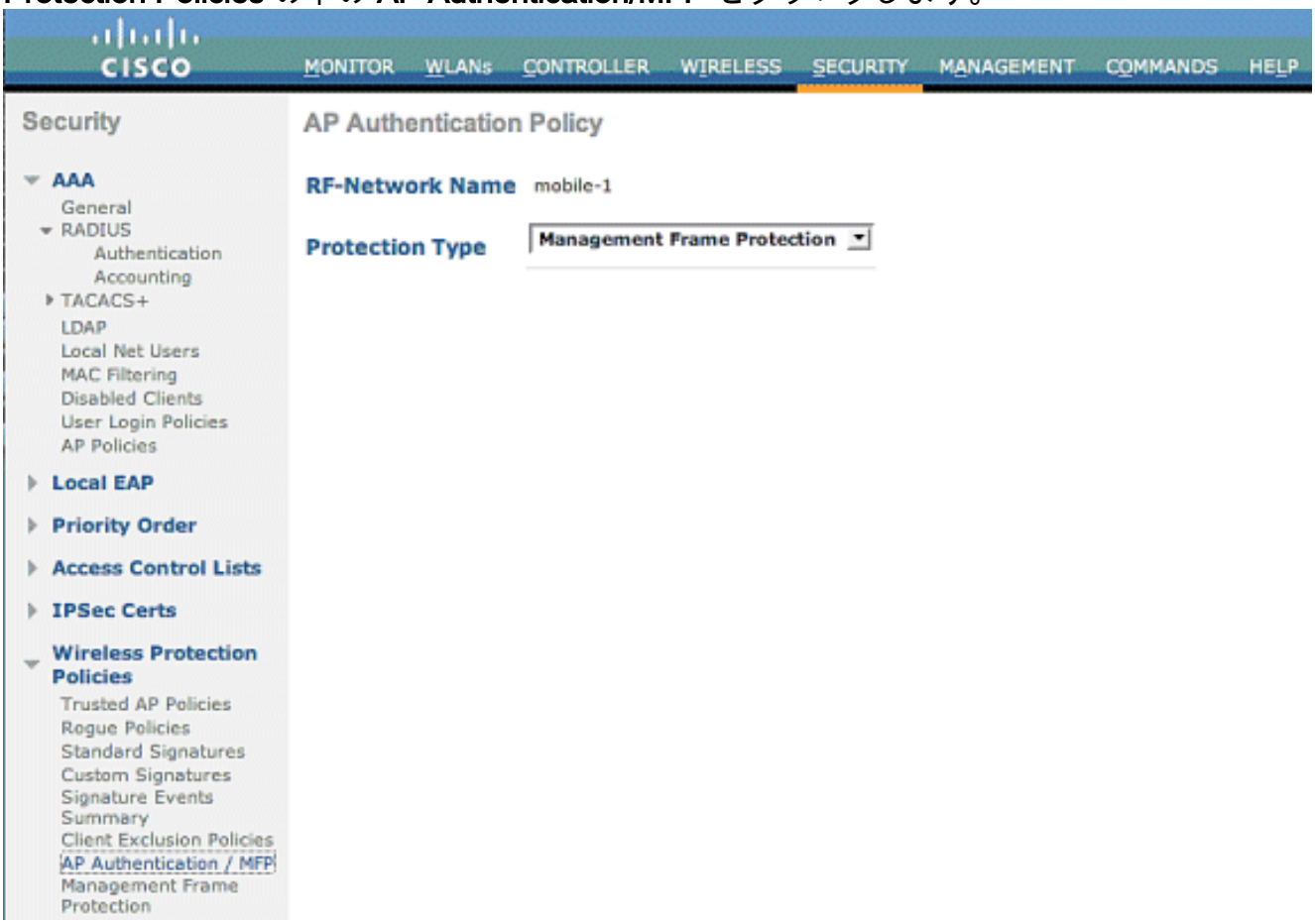
設定

コントローラでの MFP の設定

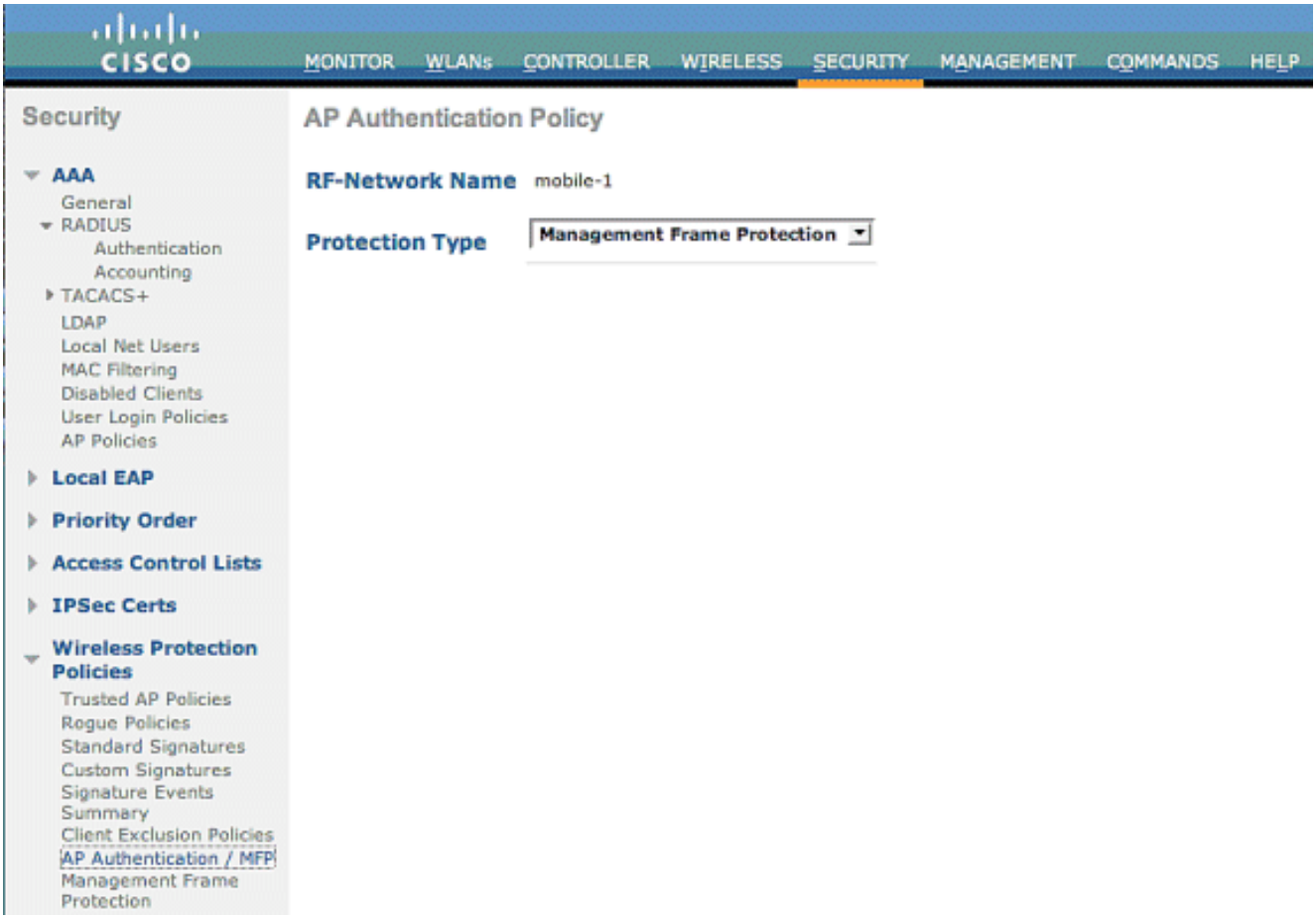
MFP はコントローラ上でグローバルに設定できます。このようにした場合、**加入している各アクセス ポイントに対して、管理フレームの保護と検証はデフォルトで有効であり**、アクセス ポイント認証は自動的に無効になります。

コントローラでグローバルに MFP を設定するには、次の手順を実行します。

1. コントローラの GUI で、[Security] をクリックします。表示された画面で、**Wireless Protection Policies** の下の **AP Authentication/MFP** をクリックします。



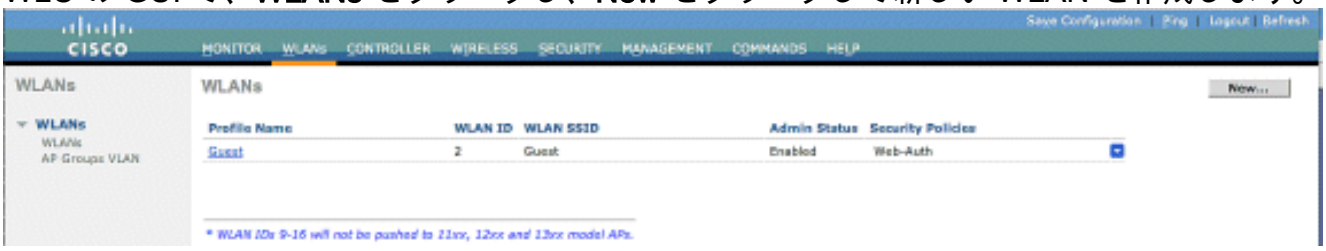
2. AP Authentication Policy で、**Protection Type** ドロップダウン メニューから Management Frame Protection を選択し、Apply をクリックします。



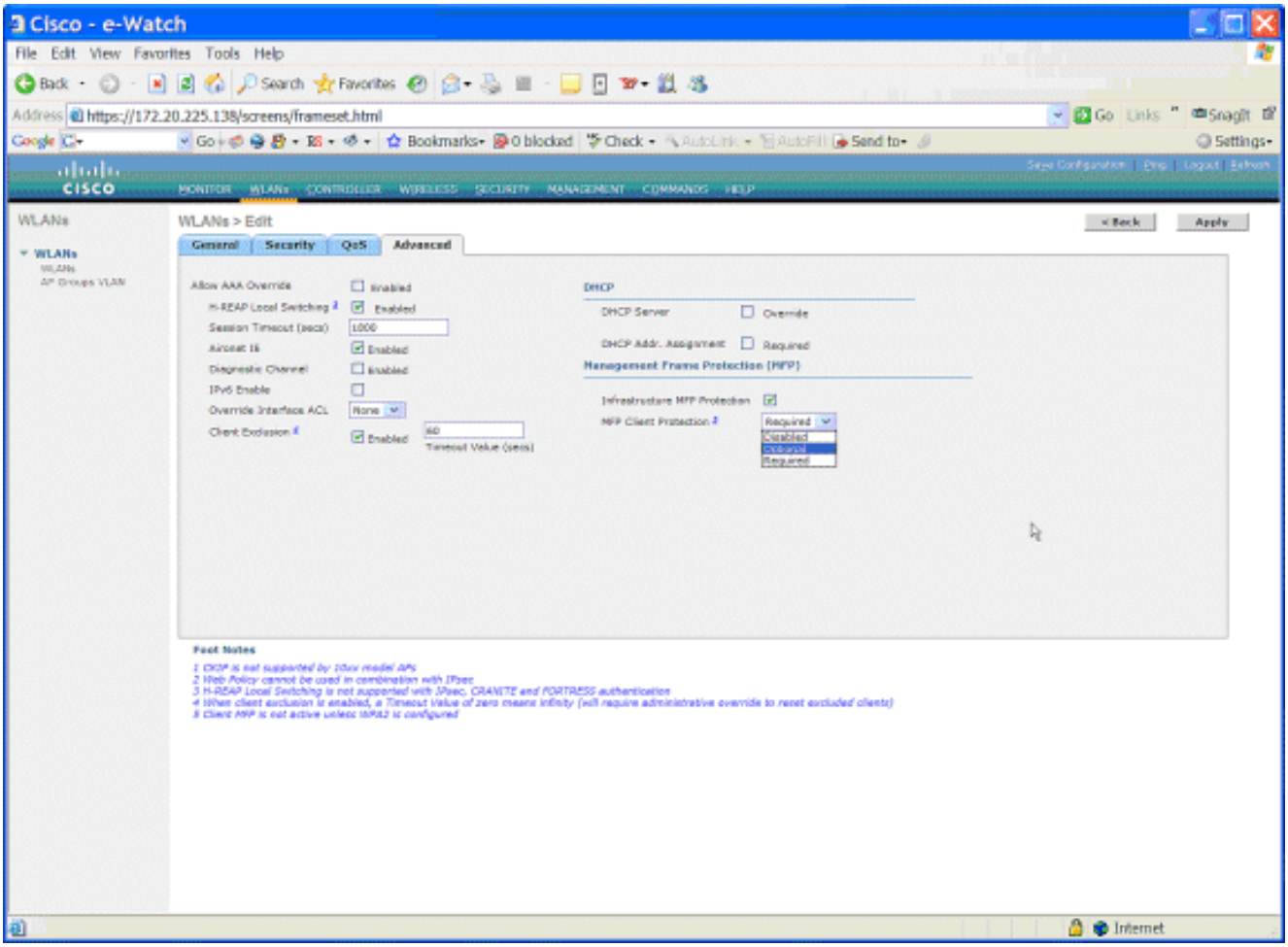
WLAN での MFP の設定

WLC 上で設定された各 WLAN 上で、インフラストラクチャ MFP 保護およびクライアント MFP を有効にしたり、無効にしたりできます。デフォルトでは両方とも有効になっていますが、インフラストラクチャ MFP 保護はグローバルに有効である場合にのみアクティブです。クライアント MFP がアクティブであるのは WPA2 セキュリティを使用して WLAN が設定されている場合のみです。WLAN で MFP を有効にするには、次の手順に従います。

1. WLC の GUI で、**WLANs** をクリックし、**New** をクリックして新しい WLAN を作成します。

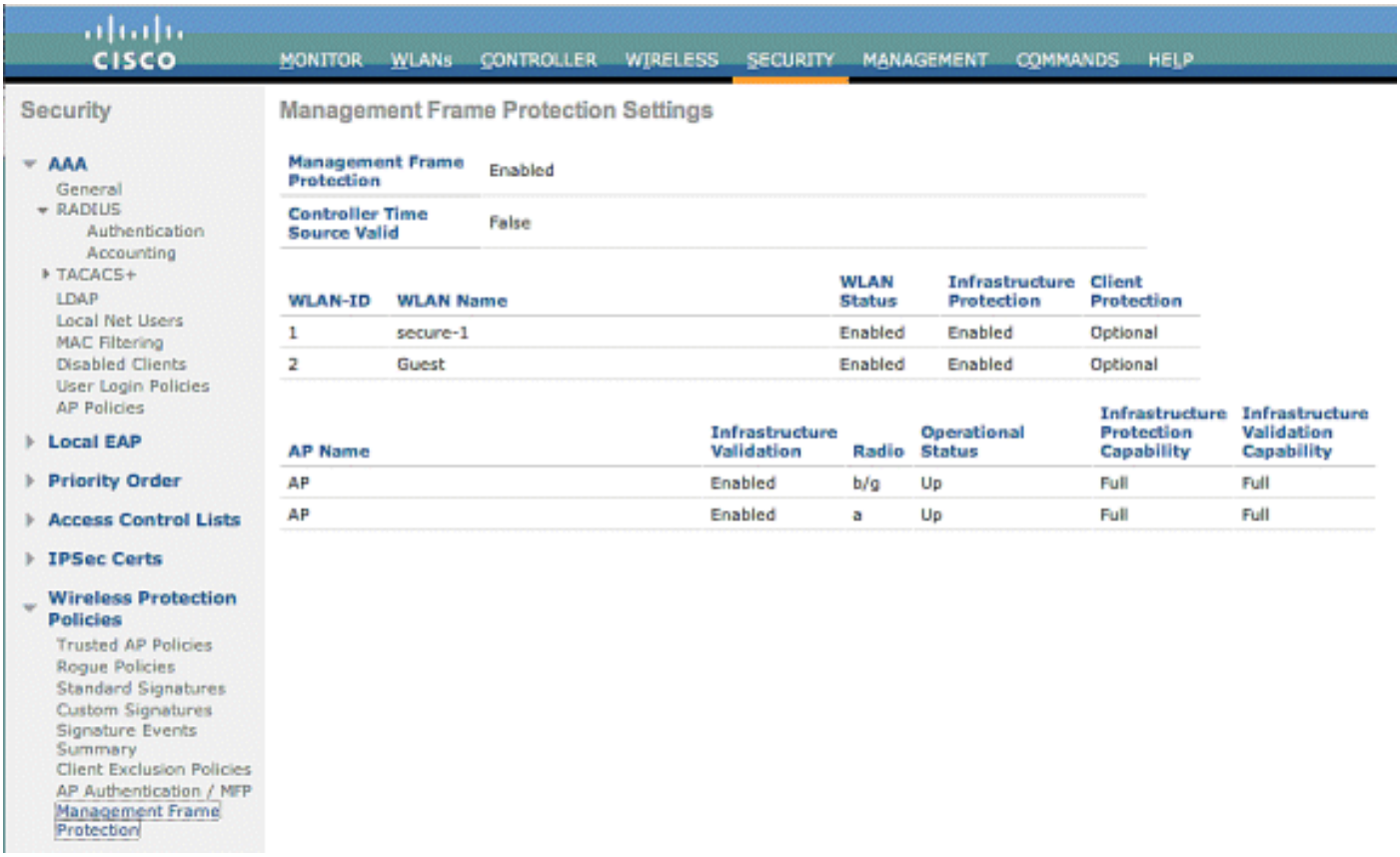


2. WLANs edit ページで、*Advanced* タブに移動し、**Infrastructure MFP Protection** チェック ボックスにチェックマークを入れて、この WLAN 上でインフラストラクチャ MFP を有効にします。この WLAN のインフラストラクチャ MFP 保護を無効にするには、このチェック ボックスのチェックマークを外します。クライアント MFP を有効にするには、ドロップダウン メニューから required オプションか optional オプションを選択します。Client MFP= Required を選択した場合、すべてのクライアントが MFP-2 をサポートしていることを確認してください。サポートしていない場合は接続できません。optional を選択した場合、MFP 対応および MFP 非対応クライアントが同じ WLAN 上で接続できます。



確認

GUI から MFP 設定を確認するには、Wireless Protection Policies from the Security ページで **Management Frame Protection** をクリックします。これにより、MFP Settings ページに移動します。



MFP Settings ページでは、WLC、LAP、および WLAN 上の MFP 設定を確認できます。次に例を示します。

- Management Frame Protection フィールドには、WLC に対して MFP がグローバルに有効であるかどうかが示されます。
- Controller Time Source Valid フィールドには、WLC 時間が（時間の手動入力により）ローカルに設定されているのか、外部ソース（NTP サーバなど）を通じて設定されているのかが示されます。 時間が外部ソースにより設定されている場合、このフィールドの値は「True」です。 時間がローカルに設定されている場合、値は「False」です。 モビリティも設定されているさまざまな WLC のアクセス ポイント間での管理フレームの検証に、時間ソースが使用されます。**注：モビリティ**/RFグループ内のすべてのWLCでMFPが有効になっている場合は、常にNTPサーバを使用してモビリティグループ内のWLC時刻を設定することをお勧めします。
- **MFP Protection** フィールドには、個別の WLAN に対して MFP が有効であるかどうかが示されます。
- **MFP Validation** フィールドには、個別のアクセス ポイントに対して MFP が有効であるかどうかが示されます。

次の show コマンドを使用できます。

- **show wps summary：WLC の現在のワイヤレス保護ポリシー（MFP を含む）の概要を表示するには、このコマンドを使用します。**
- **show wps mfp summary**：WLC の現在のグローバル MFP 設定を表示するには、このコマンドを入力します。
- **show ap config general *AP_name*：特定のアクセス ポイントの現在の MFP 状態を表示するには、このコマンドを入力します。**

次に、**show ap config general *AP_name* コマンドの出力例を示します。**

```
(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
```

次に、**show wps mfp summary** コマンドの出力例を示します。

```
(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
```

次の debug コマンドを使用できます。

- **debug wps mfp lwapp**：MFP メッセージに関するデバッグ情報が表示されます。
- **debug wps mfp detail**：MFP メッセージに関する詳細なデバッグ情報が表示されます。
- **debug wps mfp report**：MFP レポートに関するデバッグ情報が表示されます。
- **debug wps mfp mm**：MFP モビリティ（コントローラ間）メッセージに関するデバッグ情報が表示されます。

注：インターネットから利用可能な複数の無料ワイヤレスパケットスニファも存在します。これらは、802.11管理フレームのキャプチャと分析に使用できます。パケット スニファの例には Omnipeek や Wireshark があります。

関連情報

- セキュリティ ソリューションの設定：WLC 設定ガイド
- WCS でのセキュリティ ソリューションの設定
- EAP 認証と WLAN コントローラ（WLC）の設定例
- Wireless LAN Controller での ACL の設定例
- ワイヤレス LAN コントローラを使用した外部 Web 認証の設定例
- RADIUS サーバおよびワイヤレス LAN コントローラを使用したダイナミック VLAN 割り当ての設定例
- EAP-FAST 認証を使用する Cisco Secure Services Client
- ワイヤレス LAN コントローラ（WLC）に関する FAQ
- ワイヤレスに関するサポート ページ
- テクニカル サポートとドキュメント – Cisco Systems

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。