CHAPTER 12

その他のサービスの設定

この章では、無線ドメイン サービス（WDS）、クライアント デバイスの高速安全ローミング、無線管理、無線侵入検知サービス（WIDS）、およびその他のサービスのアクセス ポイントを設定する方法について説明します。

WDS の概要

ネットワークに WDS を設定すると、無線 LAN 上のアクセス ポイントは WDS デバイス（WDS デバイスとして設定されたアクセス ポイント、サービス統合型ルータのいずれか）を使用して、特定のサブネット内でクライアント デバイスに高速安全ローミングを提供し、無線管理に参加します。WDS デバイスとして設定されたアクセス ポイントは、最大 60 の参加アクセス ポイントをサポートします。WDS デバイスとして設定されたサービス統合型ルータ（ISR）は、最大 100 の参加アクセス ポイントサポートします。

（注） 単一のアクセス ポイントは、最大 16 個までのモビリティ グループをサポートします。

高速安全ローミングによって、クライアント デバイスがアクセス ポイント間をローミングする際の再認証が迅速化されるため、音声やその他の時間に敏感なアプリケーションにおける遅延を回避できます。

無線管理に参加しているアクセス ポイントは、無線環境に関する情報（潜在的な不正アクセス ポイント、クライアント アソシエーション、アソシエーション解除など）を WDS デバイスに転送します。

WDS デバイスの役割

WDS デバイスは無線 LAN 上で次のようないくつかの作業を実行します。

- WDS 機能をアドバタイズして、無線 LAN に最適な WDS デバイスの選択に参加します。WDS 用に無線 LAN を設定する場合は、1 つのデバイスをメインの WDS 候補として設定し、1 つ以上の追加デバイスをバックアップの WDS 候補として設定します。メインの WDS デバイスがオフラインになったら、バックアップの WDS デバイスの 1 つがその役割を引き継ぎます。
- 有線インターフェイスを使用して、サブネット内の全アクセス ポイントを認証し、それぞれのアクセス ポイントとセキュア通信チャネルを設定します。

- 参加しているアクセス ポイントにアソシエートされているすべての 802.1X 認証クライアント デバイスに対するパススルーとして機能します。
- 動的キーを使用するサブネット中の全クライアント デバイスを登録して、それらに対してセッション キーを設定し、セキュリティ クレデンシャルをキャッシュします。クライアントが WDS デバイスに登録された別のアクセス ポイントにローミングするときは、WDS デバイスがクライアントのセキュリティ クレデンシャルを新しいアクセス ポイントに転送します。

表 12-1 に、WDS デバイスとして設定できるプラットフォーム（アクセス ポイントまたは ISR）でサポートされる参加アクセス ポイント数をリストします。

表 12-1　WDS デバイスでサポートされる参加アクセス ポイント数

WDS デバイスとして設定されたユニット	サポートされる参加アクセス ポイント数
クライアント デバイスからも接続できるアクセス ポイント	30
無線インターフェイスが無効になっているアクセス ポイント	60
サービス統合型ルータ（ISR）	100（ISR プラットフォームに応じて異なる）

WDS デバイスを使用したアクセス ポイントの役割

無線 LAN 上のアクセス ポイントは、次の動作において WDS デバイスと対話します。

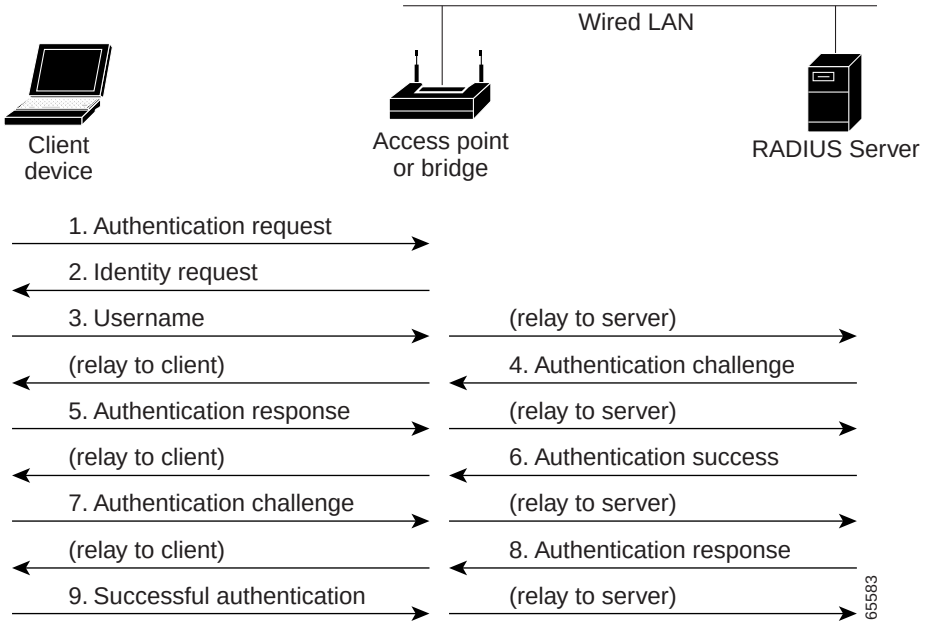
- 現在の WDS デバイスを検出、トラッキングし、WDS アドバタイズメントを無線 LAN に中継します。
- WDS デバイスを認証して、認証した WDS デバイスと安全な通信チャネルを確立します。
- WDS デバイスとアソシエートしたクライアント デバイスを登録します。
- 無線データを WDS デバイスに報告します。

高速安全ローミングの概要

多くの無線 LAN 内のアクセス ポイントは、システム全体においてアクセス ポイントからアクセス ポイントへローミングするモバイル クライアント デバイスに対応します。クライアント デバイスで稼働するアプリケーションの中には、異なるアクセス ポイントにローミングする場合に高速な再アソシエーションを必要とするものがあります。たとえば、音声アプリケーションでは、会話の遅延やギャップを防ぐために、シームレスなローミングが必要です。

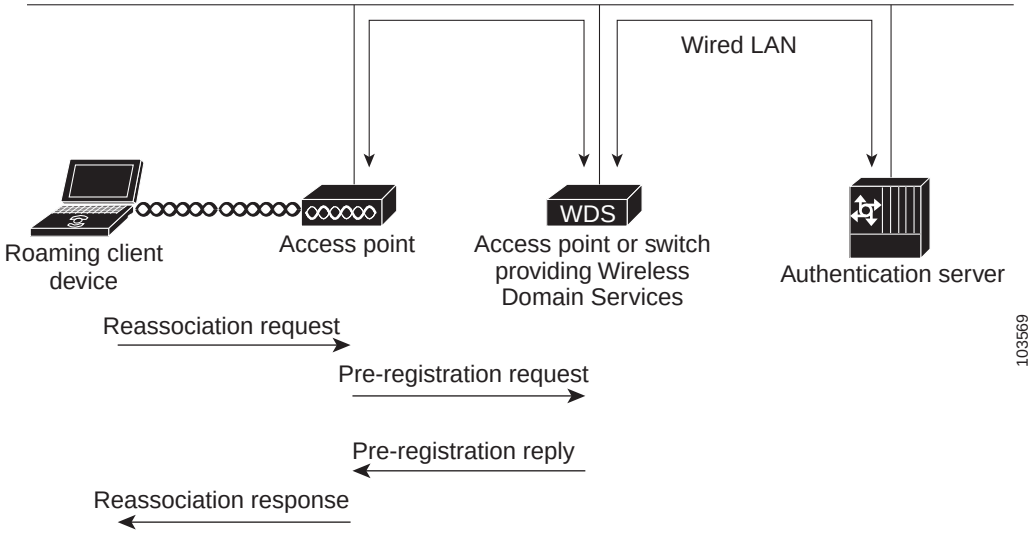
通常稼働時、EAP/802.1x 対応クライアント デバイスは、メイン RADIUS サーバとの通信を含む完全な EAP/802.1x 認証を実行することによって、新しいアクセス ポイントとの間で相互認証を行います（図 12-1 を参照）。

図 12-1　RADIUS サーバを使用したクライアント認証交換の例（LEAP の場合）



無線 LAN に高速安全ローミングを設定すれば、EAP/802.1x 対応のクライアント デバイスはメイン RADIUS サーバを利用することなく、あるアクセス ポイントから別のアクセス ポイントにローミングできるようになります。Cisco Centralized Key Management（CCKM）を使用すると、無線ドメイン サービス（WDS）を提供するように設定されているデバイスは、RADIUS サーバの代わりにクライアントを短時間で認証するため、音声などの時間が重要なアプリケーションでは知覚できるほどの遅延は発生しません。図 12-2 は、CCKM を使用したクライアント認証を示しています。

図 12-2　CCKM と WDS アクセス ポイントを使用するクライアント再アソシエーション



WDS デバイスは、無線 LAN 上の CCKM 利用可能クライアント デバイスに対するクレデンシャルのキャッシュを維持します。CCKM 利用可能クライアントが、1 つのアクセス ポイントから別のアクセス ポイントへローミングする場合、クライアントが新しいアクセス ポイントへ再アソシエーションの要求を送信し、新しいアクセス ポイントはその要求を WDS デバイスへ中継します。WDS デバイスはクライアントのクレデンシャルを新しいアクセス ポイントに転送し、新しいアクセス ポイントは再アソシエーション応答をクライアントに送信します。クライアントと新しいアクセス ポイントとの間で渡されるパケットは 2 つだけであるため、再アソシエーションの時間が大幅に短縮されます。クライアントは再アソシエーション応答をユニキャスト キーの生成にも使用します。高速安全ローミングをサポートするアクセス ポイントを設定する方法の詳細は、「高速安全ローミングの設定」セクション（12-17 ページ）を参照してください。

（注）　このメカニズムでは、クライアントが AP 間で受け渡しされるクレデンシャルを受け入れる必要もあります。必ず、アクセス ポイントで CCKM を有効にするとともに、ワイヤレス クライアントが、ネットワークで使用されている（CCX を使用する）認証メカニズムに対し CCKM をサポートしていることを確認してください。CCKM をサポートしていない場合、クライアントは高速ローミング メカニズムを拒否し、RADIUS サーバによる再認証を強制する場合があります。
各認証メカニズムに必要な CCX のバージョンを確認するには、次の URL にアクセスします。
http://www.cisco.com/web/partners/pr46/pr147/program_additional_information_new_release_features.html
各クライアント タイプでサポートされる CCX バージョンを確認するには、次の URL にアクセスします。
http://www.cisco.com/web/partners/pr46/pr147/partners_pgm_partners_0900aecd800a7907.html

Wireless Intrusion Detection Service の概要

無線 LAN 上に Wireless Intrusion Detection Service（WIDS）を実装すると、アクセス ポイント、およびオプションの（シスコ以外の）WIDS エンジンが同時に動作して、無線 LAN インフラストラクチャ、およびアソシエートされたクライアント デバイスに対する攻撃を探知および防止します。

（シスコ以外の）WIDS エンジンとともに動作する場合、アクセス ポイントは侵入を探知し、無線 LAN を防御するアクションを実行できます。

WIDS の機能は次のとおりです。

- スイッチ ポートのトレースと不正抑制：スイッチ ポートのトレースと抑制では、未知の無線（潜在的な不正デバイス）の無線 MAC アドレスを生成する RF 検出方法を使用します。（シスコ以外の）WIDS エンジンは、無線 MAC アドレスから有線側 MAC アドレスを取り出し、これを使用してスイッチの BRIDGE MIB を検索します。
- 過剰管理フレーム検出：過剰管理フレームは、無線 LAN が攻撃されたことを示します。攻撃者は、無線上で大量の管理フレームを注入し、そのフレームを処理する必要があるアクセス ポイントに大きな負荷を加えることにより、サービス拒絶攻撃を実行する場合があります。スキャン モードのアクセス ポイントとルート アクセス ポイントは、WIDS のフィーチャ セットの一部として無線信号をモニタして、過剰管理フレームを検出します。アクセス ポイントが過剰管理フレームを検出すると、障害を生成して、それを WDS を介して（シスコ以外の）WIDS エンジンに送信します。

- 認証/保護失敗検出：認証/保護失敗検出は、無線 LAN 上での最初の認証フェーズを回避するかまたは、進行中のリンク保護を侵害しようとする攻撃者を探します。これらの検出メカニズムは、次の特定の認証攻撃に対応します。
  - EAPOL フラッド検出
  - MIC/暗号化失敗検出
  - MAC スプーフィング検出
- フレーム キャプチャ モード：フレーム キャプチャ モードでは、スキャナ アクセス ポイントが 802.11 フレームを収集し、ネットワーク上の WIDS エンジンのアドレスに転送します。

（注）　アクセス ポイントの WIDS への参加の設定方法については、「WIDS に参加するようにアクセス ポイントを設定する」セクション（12-26 ページ）を、アクセス ポイントに対する Management Frame Protection（MFP; 管理フレーム保護）の設定方法については、管理フレーム保護の設定（12-21 ページ）を参照してください。

- 802.11 管理フレーム保護（MFP）：本質的に、無線は正規のデバイスか、不法デバイスであるかを問わず、あらゆるデバイスで傍受および参加が可能なブロードキャスト メディアです。制御/管理フレームは、クライアント ステーションが AP とのセッションを選択および開始する際に使用するため、これらのフレームはオープンである必要があります。管理フレームは暗号化できませんが、偽造から保護する必要があります。MFP は、802.11 管理フレームを完全に保護できる手段です。

WDS の設定

この項では、ネットワーク上で WDS を設定する方法について説明します。この項の構成は、次のとおりです。

WDS のガイドライン

WDS を設定する場合は、次のガイドラインに従います。

- クライアント デバイスも収容している WDS アクセス ポイントでは最大 30 個のアクセス ポイントの参加がサポートされますが、無線を無効にした WDS アクセス ポイントでは、最大 60 個までサポートされます。

  WDS 専用モードの場合、WDS では最大 60 個までのインフラストラクチャ アクセス ポイントと 1200 個のクライアントがサポートされます。

- リピータ アクセス ポイントは、WDS をサポートしません。リピータ アクセス ポイントを WDS 候補として設定しないでください。また WDS アクセス ポイントを、イーサネット障害時にリピータ モードに戻る（フォールバックする）設定はしないでください。

WDS の要件

WDS を設定するには、無線 LAN 上に次の項目を含める必要があります。

- 少なくとも 1 つのアクセス ポイントまたはサービス統合型ルータ（ISR）
- 認証サーバ（またはローカル認証サーバとして設定されたアクセス ポイントまたは ISR）

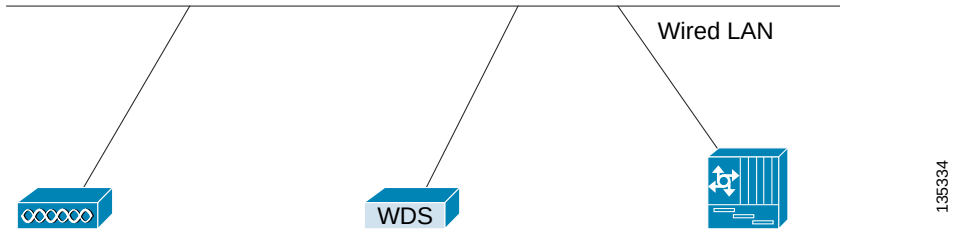
設定の概要

WDS および高速安全ローミングの設定には、次の 3 つの主要手順を完了する必要があります。

1. アクセス ポイント、ISR、またはスイッチを潜在的な WDS デバイスとして設定します。この項では、アクセス ポイントを WDS デバイスとして設定する方法について説明します。
2. 他のアクセス ポイントが、この WDS デバイスを使用するように設定します。
3. ネットワーク上の認証サーバが WDS デバイスと、WDS デバイスを使用するアクセス ポイントを認証するように設定します。

図 12-3 は、WDS に参加する各デバイスに必要な設定を示しています。

図 12-3　　WDS に参加するデバイスの設定



Access point:

- Wireless Services enabled
- Username and password for authentication to the server

WDS device:

- Configured as a WDS candidate
- If an access point serving client devices, username and password for authentication to the server

Authentication server

- WDS access point entered as an infra-structure device
- Access points that use the WDS entered on the server as client devices with usernames and passwords that match those configured on the access points

アクセス ポイントを潜在的な WDS デバイスとして設定する

(注) メインの WDS 候補用に、多数のクライアント デバイスを収容する必要のないアクセス ポイントを設定します。クライアント デバイスが WDS アクセス ポイントの起動時にアソシエートした場合、そのクライアントは認証のために数分待たされる可能性があります。

(注) リピータ アクセス ポイントは、WDS をサポートしません。リピータ アクセス ポイントを WDS 候補として設定しないでください。また、WDS アクセス ポイントを、イーサネット障害時にリピータ モードに戻るように設定しないでください。

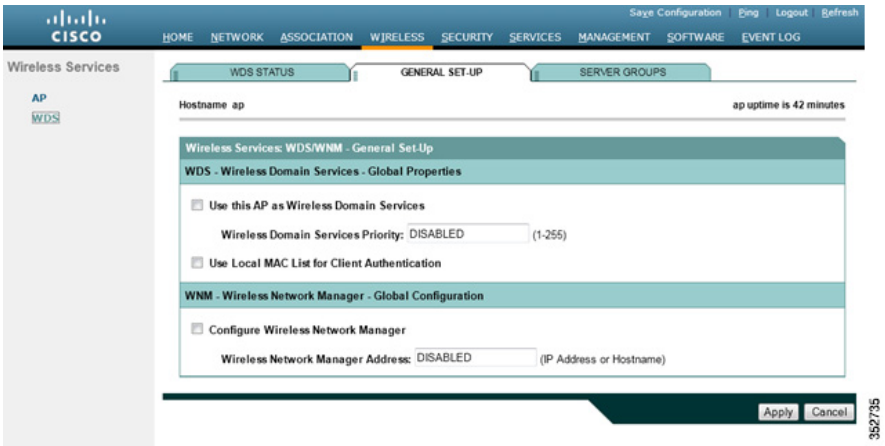
(注) WDS が有効な場合、WDS アクセス ポイントはすべての認証を実行、トラッキングします。したがって、WDS アクセス ポイントでは EAP セキュリティ設定を行う必要があります。アクセス ポイント上での EAP 設定の詳細は、第 11 章「認証タイプの設定」を参照してください。

プライマリ WDS アクセス ポイントとして設定するアクセス ポイント上で、次の手順に従ってメインの WDS 候補としてアクセス ポイントを設定します。

ステップ 1　[Wireless] > [WDS] の順に選択します。

ステップ 2　[General Set-Up] タブをクリックします。

図 12-4　[General Set-Up] の [Hostname ap] ページ



ステップ 3　[Use this AP as Wireless Domain Services] チェックボックスをオンにします。

ステップ 4　[Wireless Domain Services Priority] フィールドに 1 ～ 255 の優先順位数を入力して、WDS 候補の優先順位を設定します。
[Wireless Domain Services Priority] フィールド内の数字が最も大きい WDS アクセス ポイント候補が、WDS アクセス ポイントとして機能します。たとえば、1 つの WDS 候補には優先順位に 255 が割り当てられており、もう 1 つの候補には優先順位に 100 が割り当てられている場合は、優先順位が 255 の候補が WDS アクセス ポイントとして機能します。

ステップ 5　(WDS クライアントの場合のみ)WDS デバイスに設定されたローカル アドレス リストに含まれる MAC アドレスを使用してクライアント AP デバイスを認証する場合は、[Use Local MAC List for Client Authentication] チェックボックスをオンにします。
このチェックボックスをオンにしない場合、WDS デバイスは [Server Groups] ページで MAC アドレス認証用に指定したサーバを使用して、MAC アドレスに基づくクライアント認証を行います。

(注)　[Use Local MAC List for Client Authentication] チェックボックスをオンにしても、クライアント デバイスに対して MAC ベースの認証が強制されるわけではありません。サーバベースの MAC アドレス認証に対するローカルの代替方法が提供されるだけです。

ステップ 6　[Apply] をクリックします。

ステップ 7　[Server Groups] タブをクリックして [WDS Server Groups] ページに移動します。

ステップ 8　WDS アクセス ポイントを使用するインフラストラクチャ デバイス(アクセス ポイント)の 802.1x 認証に使用するサーバ グループを作成します。[Server Group Name] フィールドにグループ名を入力します。

ステップ 9　[Priority 1] ドロップダウン リストからプライマリ サーバを選択します(グループに追加する必要のあるサーバが [Priority] ドロップダウン リストに表示されない場合は、[Define Servers] をクリックして、[Server Manager] ページを表示します。そのページでサーバを設定してから、[WDS Server Groups] ページに戻ります)。

(注)　ネットワーク上に認証サーバが存在しない場合、アクセス ポイントまたは ISR をローカル認証サーバとして設定できます。設定方法の詳細は、第 9 章「ローカル認証サーバとしてのアクセス ポイントの設定」を参照してください。

ステップ 10　(任意)[Priority 2] ドロップダウン リストおよび [Priority 3] ドロップダウン リストからバックアップ サーバを選択します。

ステップ 11　[Apply] をクリックします。

ステップ 12　ワイヤレス クライアント デバイス用の 802.1x 認証に使用するサーバのリストを設定します。特定のタイプの認証(EAP、LEAP、その他の EAP タイプ、または MAC ベースなど)を使用するクライアント用の別のリストを指定したり、任意のタイプの認証を使用するクライアント デバイス用のリストを指定したりできます。[Server Group Name] フィールドに、サーバのグループ名を入力します。

[LEAP Authentication] チェックボックスは、特に次に示すシスコ製クライアント向けに用意されています。

- LEAP を使用する Cisco 7920、7921、および 7925 電話
- ワイヤレス クライアント(ワークグループ ブリッジまたは非ルート ブリッジ)として設定され、LEAP 認証を使用する自律 AP

[LEAP Authentication] チェックボックスをオフにすると、これらのクライアント デバイスは、LEAP および WDS サービスを使用してワイヤレス ネットワークに対する認証を実行できなくなります。EAP オプションが選択されている場合、クライアントは他の任意の形式の EAP 認証を使用して接続できます。ただし、これによって、他のクライアント カードやサプリカントの組み合わせが接続できなくなるわけではありません。これらのクライアントは、LEAP を含め、あらゆる形式の EAP 認証に 802.1X 標準を使用するためです。この情報は、シスコ以外のクライアントには適用されません。

ステップ 13　[Priority 1] ドロップダウン リストからプライマリ サーバを選択します(グループに追加する必要のあるサーバが [Priority] ドロップダウン リストに表示されない場合は、[Define Servers] をクリックして、[Server Manager] ページを表示します。そのページでサーバを設定してから、[WDS Server Groups] ページに戻ります)。

ステップ 14　(任意)[Priority 2] ドロップダウン リストおよび [Priority 3] ドロップダウン リストからバックアップ サーバを選択します。

ステップ 15　(任意)[Restrict SSIDs] を選択すると、使用するサーバ グループを、特定の SSID を使用するクライアント デバイスに制限できます。[SSID] フィールドに SSID を入力して、[Add] をクリックします。SSID を削除するには、削除する SSID を [SSID] リスト内で選択して [Remove] をクリックします。

ステップ 16　[Apply] をクリックします。

ステップ 17　EAP 認証用に WDS アクセス ポイントを設定します。EAP の設定方法の詳細については、第 11 章「認証タイプの設定」を参照してください。

(注)　この認証では、デフォルトで LEAP を使用します。WDS サービスを使用するインフラストラクチャ アクセス ポイントは、WDS デバイスを介して認証される必要があります。WDS アクセス ポイントでクライアント デバイスを使用する場合は、「アクセス ポイントを WDS デバイスを使用するように設定する」セクション(12-10 ページ)の手順に従って、WDS アクセス ポイントが WDS を使用するように設定します。

CLI の設定例

次の例は、「アクセス ポイントを潜在的な WDS デバイスとして設定する」セクション（12-7 ページ）に記載された手順と同じ働きをする CLI コマンドを示しています。

```
AP# configure terminal
AP(config)# aaa new-model
AP(config)# wlccp wds priority 200 interface bvi1
AP(config)# wlccp authentication-server infrastructure infra_devices
AP(config)# wlccp authentication-server client any client_devices
AP(config-wlccp-auth)# ssid fred
AP(config-wlccp-auth)# ssid ginger
AP(config)# end
```

次の例では、サーバ グループ *infra_devices* を使用してインフラストラクチャ デバイスを認証しています。SSID *fred* または *ginger* を使用するクライアント デバイスは、サーバ グループ *client_devices* を使用して認証されます。SSID リストを指定しない場合、すべての SSID が対象になります。

この例で使用されているコマンドの詳細については、『*Cisco IOS Command Reference for Cisco Aironet Access Points and Bridges*』を参照してください。

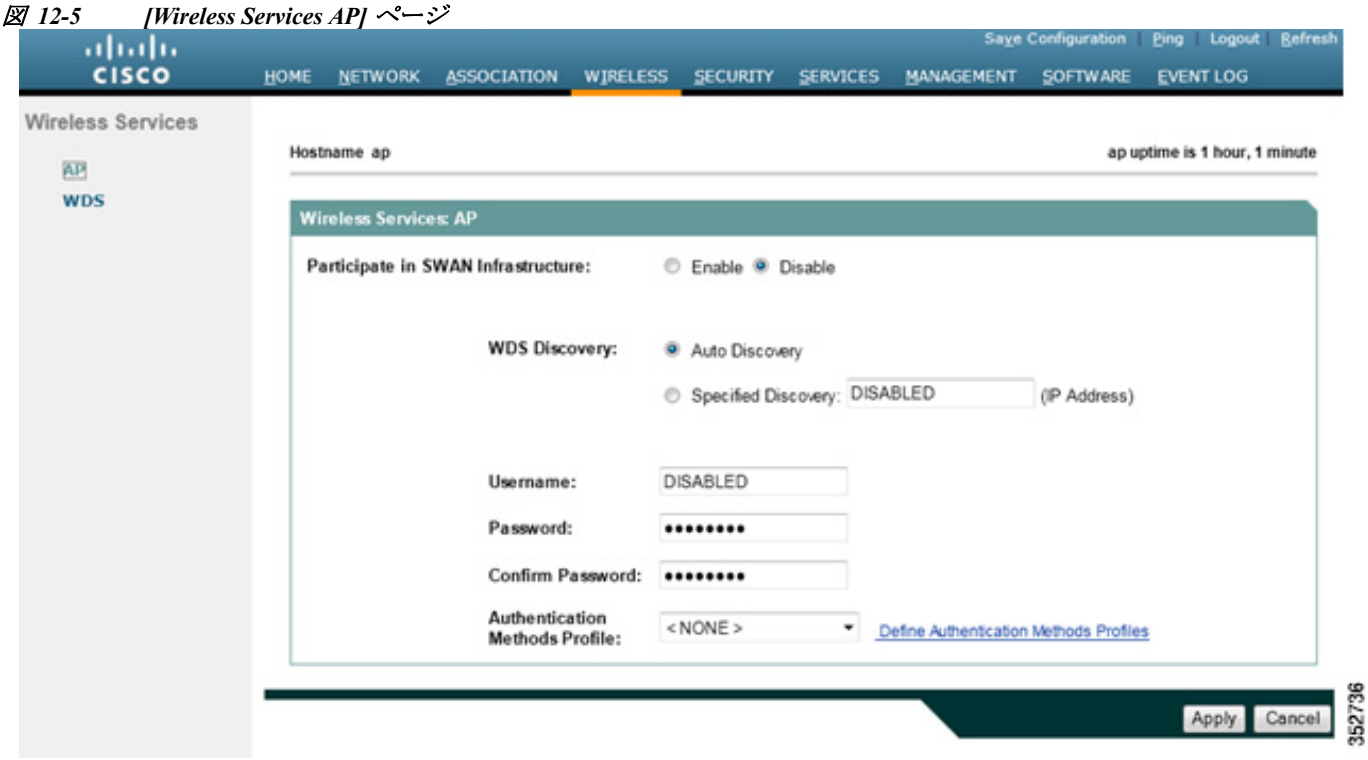
アクセス ポイントを WDS デバイスを使用するように設定する

WDS デバイスを通じて認証し、WDS 内に参加するようにアクセス ポイントを設定する手順は、次のとおりです。

（注）　インフラストラクチャ アクセス ポイントが WDS に参加するには、WDS が実行している IOS と同じバージョンを実行する必要があります。

ステップ 1　[Wireless] > [AP] の順に選択します。[Wireless Services AP] ページが表示されます。

図 12-5　[Wireless Services AP] ページ



ステップ 2　AP がクライアント認証で WDS サービスを使用できるように設定するには、[Participate in SWAN Infrastructure] 設定の [Enable] をクリックします。

ステップ 3　(任意)[Specified Discovery] を選択し、入力フィールドに WDS の IP アドレスを入力します。[Specified Discovery] を有効にすると、アクセス ポイントは WDS アドバタイズメントを待たずに、WDS デバイスを使用して即座に認証します。指定した WDS デバイスが応答しない場合、アクセス ポイントは WDS アドバタイズメントを待ちます。

ステップ 4　[Username] フィールドにアクセス ポイントのユーザ名を入力します。このユーザ名は、認証サーバ上でアクセス ポイント用に作成したユーザ名と一致していなければなりません。

ステップ 5　[Password] フィールドにアクセス ポイントのパスワードを入力し、[Confirm Password] フィールドに同じパスワードをもう一度入力します。このパスワード名は、認証サーバ上でアクセス ポイント用に作成したパスワードと一致していなければなりません。このページでユーザ名とパスワードを設定すると、AP は WDS サーバを介した認証に LEAP を使用します。

ステップ 6　(任意)インフラストラクチャ AP の認証を LEAP を使用した WDS で行わず、別の EAP 認証方式(EAP-FAST など)を使用する場合は、[Authentication Methods Profile] ドロップダウン リストから別の認証方式プロファイルを選択します。認証方式プロファイルをまだ定義していない場合は、[Define Authentication Method Profiles] リンクをクリックしてプロファイルを設定してから、[Wireless Services AP] 設定ページに戻ってプロファイルを選択します。新しいプロファイルの作成方法の詳細については、802.1X サプリカントの EAP 方式プロファイルの作成と適用 (11-17 ページ)を参照してください。

ステップ 7　[Apply] をクリックします。

WDS と対話するように設定したアクセス ポイントは、自動的に次の手順を実行します。

- 現在の WDS デバイスを検出、トラッキングし、WDS アドバタイズメントを無線 LAN に中継します。
- WDS デバイスを認証して、認証した WDS デバイスと安全な通信チャネルを確立します。
- WDS デバイスとアソシエートしたクライアント デバイスを登録します。

CLI の設定例

次の例は、「アクセス ポイントを WDS デバイスを使用するように設定する」セクション（12-10 ページ）に記載された手順と同じ働きをする CLI コマンドを示しています。

```
AP# configure terminal
AP(config)# wlccp ap username APWestWing password 0 wes7win8
AP(config)# wlccp ap eap profile Myfast
AP(config)# end
```

この例では、アクセス ポイントは WDS デバイスと対話できるように設定されており、ユーザ名に *APWestWing*、パスワードに *wes7win8* を使用して認証サーバに対する認証を行います。

オプションの Myfast EAP プロファイルは、LEAP 以外の方式を使用して認証を行うために呼び出されます。この例では、プロファイルは EAP-FAST を使用し、次のように設定されています。

```
ap(config)# eap profile myfast
ap(config-eap-profile)# method fast
ap(config-eap-profile)# end
```

認証サーバ上でクライアントとしてアクセス ポイントを設定するときには、同じユーザ名とパスワードの組み合わせで設定する必要があります。

この例で使用されているコマンドの詳細については、『*Cisco IOS Command Reference for Cisco Aironet Access Points and Bridges*』を参照してください。

認証サーバが WDS をサポートするように設定する

WDS デバイスと WDS に参加している全アクセス ポイントは、認証サーバに対する認証を行う必要があります。サーバ上で、アクセス ポイント用のユーザ名とパスワードと、WDS デバイス用のユーザ名とパスワードを設定します。

サーバが Cisco ACS を実行している場合は、次の手順に従ってサーバ上でアクセス ポイントを設定します。

ステップ 1　Cisco Identity Services Engine（ISE）にログインします。

ステップ 2　[Administration] > [Network Resources] > [Network devices] を選択します。
[Network Devices] ページが表示されます。
このページで、WDS を AAA クライアントとして追加できます。

図 12-6　Cisco ISE の [Network Devices] ページ

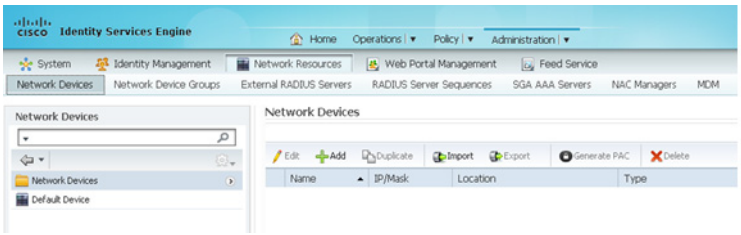
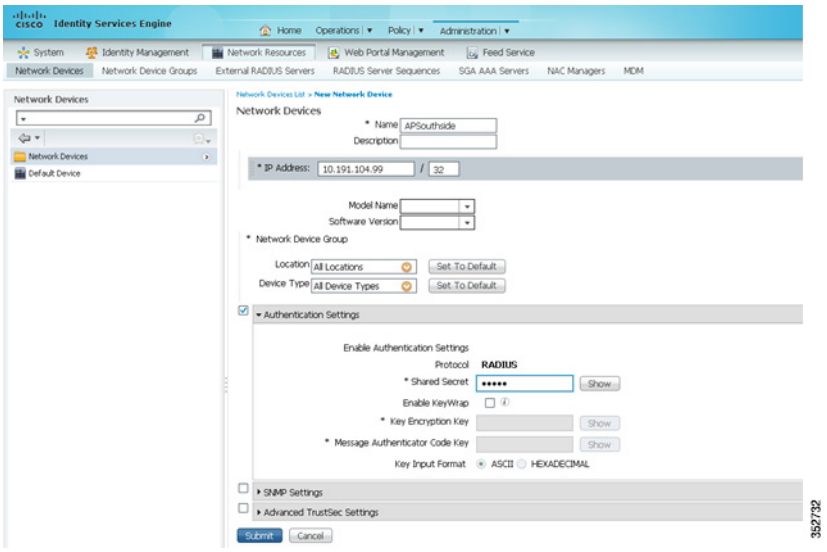


図 12-7　Cisco ISE の [Network Devices] ページの詳細



ステップ 3　[Add] をクリックし、WDS を新しい AAA クライアントとして追加します。

ステップ 4　[Name] フィールドに、WDS デバイス名を入力します。この名前はローカルでのみ有効です。オプションで、WDS デバイスの説明を入力します。

ステップ 5　[IP Address] フィールドに、WDS デバイスの IP アドレスを入力します。(任意)デバイスのロケーションとデバイス タイプを指定します(これらのカテゴリが ISE に設定されている場合のみ)。

ステップ 6　[Authentication Settings] チェックボックスをオンにします。[Authentication Settings] 領域のフィールドが有効になります。

ステップ 7　RADIUS プロトコルの場合、[Shared Secret] フィールドに共有秘密値を入力します。この値は、ISE を RARIUS サーバとして設定するときに、WDS デバイスでそのとおりに入力されます。

ステップ 8　[Submit] をクリックしてエントリを検証します。

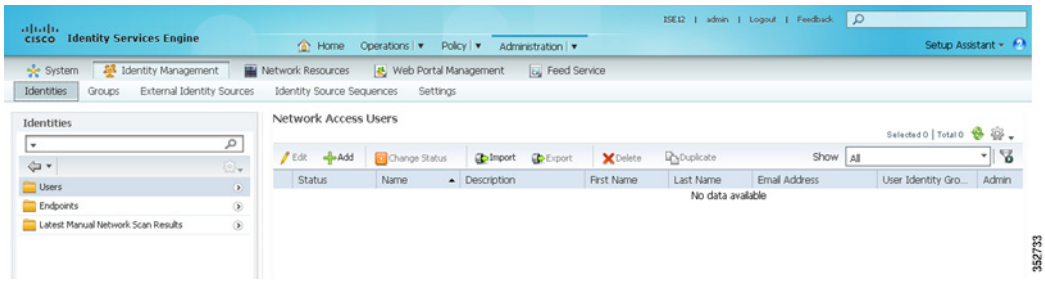
ステップ 9　WDS デバイス候補のそれぞれについて、ステップ 3 からステップ 8 の手順を繰り返します。

ステップ 10　[Administration] > [Identities Management] > [Identities] の順に選択します。[Network Access Users] ページが表示されます。

(注)　この手順では、ISE 内部データベースにユーザを設定する方法を説明します。ISE では、外部データベースも使用できます。詳細については、ISE ガイドを参照してください。

ステップ 11　[Add] をクリックして、新しいユーザを追加します。

図 12-8　[Network Access Users] ページ



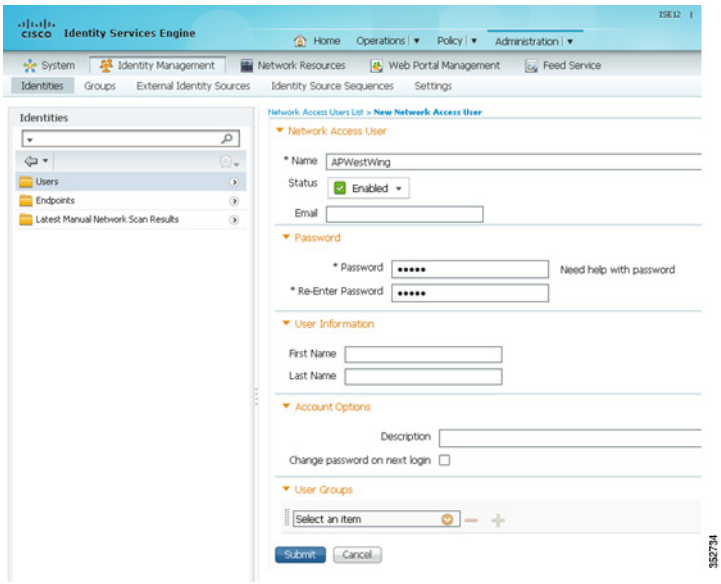
ステップ 12　[Name] フィールドに、WDS へのアクセス ポイント クライアントに設定したユーザ名を入力します。

ステップ 13　[Password] フィールドと [Confirm Password] フィールドに、[Wireless Services AP] ページでアクセス ポイントに対して入力したのとまったく同じパスワードを入力します。

ステップ 14　[Submit] をクリックします。

ステップ 15　WDS デバイスを使用するアクセス ポイントそれぞれに対して、ステップ 11 からステップ 14 の手順を繰り返します。

図 12-9　Cisco ISE の [Network Access Users] ページの詳細



WDS 専用モードの設定

WDS アクセス ポイントは、**wlccp wds mode wds-only** コマンドを使用すれば、WDS 専用モードで稼働できます。このコマンドを発行してリロードすると、アクセス ポイントは WDS 専用モードで機能を開始します。WDS 専用モードでは、dot11 サブシステムが初期化されず、dot11 インターフェイス関連のコマンドが設定できません。WDS 専用モードの場合、WDS では最大 60 個までのインフラストラクチャ アクセス ポイントと最大 1200 個のクライアントがサポートされます。このコマンドの **no** 形式を使用して、WDS 専用モードをオフにします。WDS アクセス ポイントの実行中モードを表示するには、**show wlccp wds** コマンドを使用します。

WDS アクセス ポイントが AP および WDS の両モードで稼働するように設定するには、**no wlccp wds mode wds-only** コマンドを使用し、さらに **write erase** コマンドを使用してアクセス ポイントをただちにリロードします。アクセス ポイントをリロードすると、dot11 無線サブシステムが初期化されます。アクセス ポイントと WDS は、無線クライアントに直接アソシエートします。このモードの場合、WDS では 20 個の無線クライアントの直接アソシエートに加え、30 個のインフラストラクチャ アクセス ポイントと 600 個のクライアントがサポートされます。

WDS 情報の表示

Web ブラウザのインターフェイスでは、[Wireless Services Summary] ページを使って WDS ステータスの概要を表示します。

特権 EXEC モードの CLI では、次のコマンドを使って、現在の WDS デバイスと CCKM に参加している他のアクセス ポイントについての情報を表示します。

コマンド（Command）	説明
show wlccp ap	CCKM に参加する任意のアクセス ポイント上で、このコマンドを使用して、WDS デバイスの MAC アドレス、WDS デバイスの IP アドレス、アクセス ポイントのステート（認証中、認証済み、登録済み）、インフラストラクチャ認証サーバの IP アドレス、クライアント デバイス（MN）認証サーバの IP アドレスを表示できます。
show wlccp wds ap [**cdp-neighbor** | **mac-address** *mac-address* | **order ip**]	WDS デバイスに限り、このコマンドを使って、CCKM に参加するアクセス ポイントに関するキャッシュ情報を表示できます。 • cdp-neighbor：WDS で認証された各 AP によってレポートされた CDP ネイバーを表示します。 • mac-address *mac-address*：入力された MAC アドレスで指定された AP に関する情報のみを表示します。 • order ip：AP の表示順を、AP MAC アドレスによる昇順から AP IP アドレスによる昇順に変更します。

コマンド(Command)	説明
show wlccp wds mn [**detail**] [**mac-addr** *mac-address*]	このコマンドを使用して、クライアント デバイスや呼び出されたモバイル ノードに関するキャッシュ情報を表示します。このコマンドは、各クライアントの MAC アドレス、IP アドレス、クライアントがアソシエートされているアクセス ポイント(cur-AP)、および状態(認証中、認証済み、または登録済み)を表示します。detail オプションを使用して、クライアントの有効期間(クライアントが再認証を必要とするまでの残りの秒数)、SSID、および VLAN ID を表示します。 特定のクライアント デバイスに関する情報を表示するには、**mac-address** オプションを使用します。
show wlccp wds	このコマンドを使用して、アクセス ポイントの IP アドレス、MAC アドレス、優先順位、インターフェイスの状態(管理上スタンドアロン、アクティブ、バックアップ、候補、または WDS 専用)を表示します。 状態がバックアップの場合、コマンドは現在の WDS デバイスの IP アドレス、MAC アドレス、および優先順位も表示します。
show wlccp wds nm	このコマンドを使用して、設定済みのすべてのネットワーク管理プラットフォームと統計情報(送受信メッセージ数、再送信数、ドロップされたメッセージ数)のリストを表示します。
show wlccp wds statistics	このコマンドを使用して、WDS に関する統計情報を表示します。統計情報には、現在の AP カウント、接続された AP での現在のクライアント カウント、AAA 認証試行カウント、AAA 認証成功カウント、AAA 認証失敗カウント、MAC スプーフィング ブロック カウント、AAA 認証なしのローミング カウント(事前共有キーと Open ネットワーク)、完全な AAA 認証を使用したローミング カウント(高速安全ローミングをサポートしていない非 CCX デバイスの場合)、高速安全ローミング カウント、MSC 失敗カウント、KSC 失敗カウントMIC 失敗カウント(WPA/WPA2 リプレイ攻撃の検出)、および RN 不一致カウント(WPA2 不一致の検出)が含まれます。
show wlccp wds aggregator statistics	このコマンドを使用して、参加 AP から収集された無線測定情報(送受信された更新)に関する統計を表示します。

デバッグ メッセージの使用

特権 EXEC モードでは、デバッグ コマンドを使用して、WDS デバイスと対話するデバイス用のデバッグ メッセージの表示を制御します。

コマンド（Command）	説明
debug wlccp ap {mn | nm | wds-discovery | state}	このコマンドを使用して、クライアント デバイス（**mn**）、設定済み管理プラットフォーム（**nm**）、WDS 検出プロセス、WDS デバイス（**state**）に対するアクセス ポイントの認証に関連するデバッグ メッセージの表示を有効にします。
debug wlccp dump	このコマンドを使用して、バイナリ形式で送受信された WLCCP パケットのダンプを実行します。
debug wlccp packet	このコマンドを使用して、WDS デバイスとやり取りするパケットの表示をオンにします。
debug wlccp rmlib { errors | packets }	このコマンドを使用して、AP と WDS の間、および（該当する場合は）WDS とネットワーク管理プラットフォームの間で交換された無線測定メッセージのデバッグを有効にします。
debug wlccp wds [aggregator | all | ap | authenticator | mn | nm | recovery | state | statistics]	このコマンドとそのオプションを使用して、WDS デバッグ メッセージの表示をオンにします。 すべての AP の WDS イベントをデバッグするには、**ap** オプションを使用します。オプションで mac-address を指定して、その特定の AP のイベントをデバッグすることもできます。 すべての WDS イベントをデバッグするには、**all** オプションを使用します。 必要に応じて、**nm** オプションを使用して、ネットワーク管理プラットフォームと交換されたメッセージをデバッグします。 WDS フェールオーバー（正常回復）プロセスをデバッグするには、**recovery** オプションを使用します。 **statistics** オプションを使用して、障害統計情報の表示をオンにします。
debug wlccp wds authenticator {all | dispatcher | mac-authen | process | rxdata | state-machine | txdata}	このコマンドとそのオプションを使用して、認証に関連する WDS デバッグ メッセージの表示をオンにします。

高速安全ローミングの設定

WDS を設定すると、CCKM 用に設定したアクセス ポイントは、アソシエートされたクライアント デバイスに高速安全ローミングを提供できます。この項では、高速で安全なローミングを無線 LAN 上で設定する方法を説明します。この項の構成は、次のとおりです。

- 高速安全ローミングの要件
- 高速安全ローミングをサポートするアクセス ポイントの設定

高速安全ローミングの要件

高速安全ローミングを設定するには、無線 LAN で次の項目が必要となります。

- WDS デバイスとして設定された 1 つ以上のアクセス ポイントまたは ISR
- WDS に参加するように設定されたアクセス ポイント
- 高速安全ローミング用に設定されたアクセス ポイント
- 認証サーバ（またはローカル認証サーバとして設定されたアクセス ポイントまたは ISR）
- Cisco Aironet クライアント デバイス、または Cisco Compatible Extensions（CCX）バージョン 2 以降と互換性のあるシスコ互換のクライアント デバイス

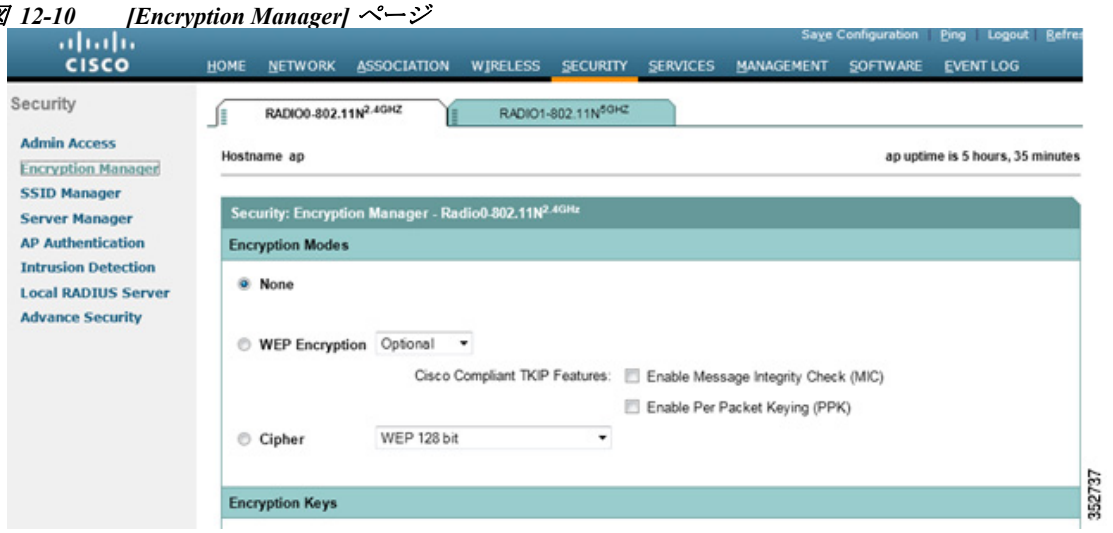
WDS の設定方法については、「WDS の設定」セクション（12-5 ページ）を参照してください。

高速安全ローミングをサポートするアクセス ポイントの設定

高速安全ローミングをサポートするには、WDS に参加するように無線 LAN 上のアクセス ポイントを設定し、それらのアクセス ポイントでターゲット SSID の CCKM 認証済みキー管理を許可する必要があります。SSID に CCKM を設定する手順は、次のとおりです。

ステップ 1　アクセス ポイント GUI で [Encryption Manager] ページを表示します。図 12-10 は、[Encryption Manager] ページの上部を示しています。

図 12-10　[Encryption Manager] ページ



ステップ 2　[Cipher] ボタンをクリックします。

ステップ 3　任意の暗号化メカニズムを設定します。シスコでは WPA2 の使用を推奨しています（WPA2 をサポートしていないレガシー クライアントをサポートする必要がある場合を除く）。暗号化メカニズムを WPA2 に設定するには、[Cipher] ドロップダウン リストから [AES CCMP] を選択します。

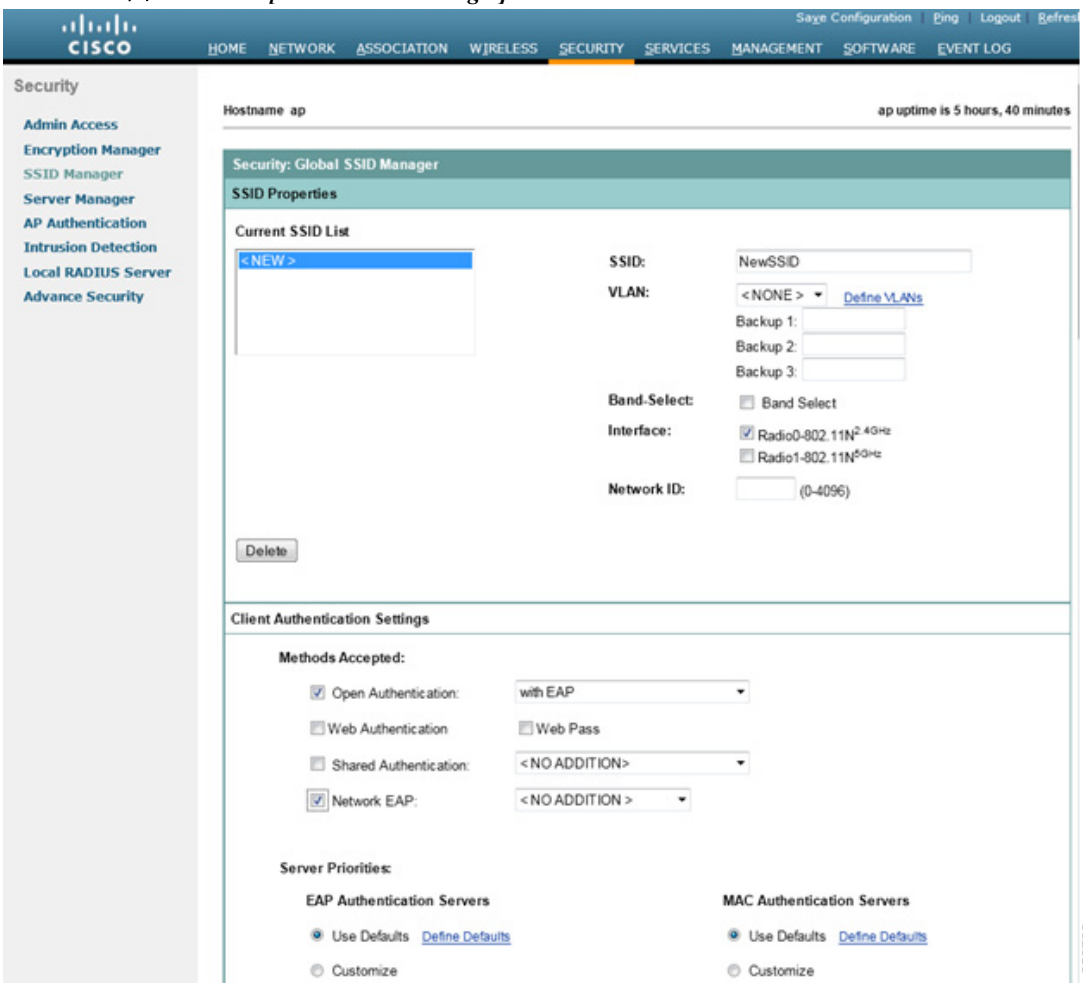
（注）　シスコでは、混合モード（AES CCMP と TKIP または WEP）の設定を推奨していません。これらのモードはネットワークのセキュリティを弱めるため、非推奨となっています。

ステップ 4　[Cipher] ドロップダウン リストから、[CKIP + CMIC] を選択します。

ステップ 5　[Apply] をクリックします。

ステップ 6　[Global SSID Manager] ページを表示します。図 12-11 は、[Global SSID Manager] ページの上部を示しています。

図 12-11　[Global SSID Manager] ページ



ステップ 7　CCKM（高速安全ローミング）をサポートする必要があるターゲット SSID で、次の設定を選択します。

a. アクセス ポイントに複数の無線インターフェイスが含まれている場合は、SSID が適用されるインターフェイスを選択します。

b. ネットワーク設定で、サポートする 802.1X/EAP 方式を選択します。Cisco IP 電話 7920、7921、7925、および 7926 で LAP をサポートする場合、およびクライアント アクセス ポイントには [Network EAP] を選択する必要があります。その他すべての EAP タイプ（PEAP、EAP-FAST、または EAP-TLS など）、およびその他すべてのクライアントのすべての EAP タイプ（LEAP を含む）には、[Open Authentication with EAP] を選択する必要があります。

c. [Key Management] 領域の [Key Management] ドロップダウン リストから、必要に応じて [Mandatory] または [Optional] を選択します。[Mandatory] を選択した場合、CCKM をサポートするクライアントだけが、SSID を使用してアソシエートできます。[Optional] を選択した場合、CCKM クライアントと CCKM をサポートしないクライアントの両方が、SSID を使用してアソシエートできます。

d. [CCKM] チェックボックスをオンにします。

e. AES CCMP 暗号を選択した場合、[Enable WPA] チェックボックスをオンにして、ドロップダウン リストから [WPAv2] オプションを選択します。

ステップ 8　[Apply] をクリックします。

CLI の設定例

次の例は、「高速安全ローミングをサポートするアクセス ポイントの設定」セクション（12-18 ページ）に記載された手順と同じ働きをする CLI コマンドを示しています。

```
AP# configure terminal
AP(config)# dot11 ssid NewSSID
AP(config-ssid)# authentication open eap eap_methods
AP(config-ssid)# authentication key-management wpa version 2 cckm
AP(config-ssid)# exit
AP(config)# interface dot11radio0
AP(config-if)# encryption mode ciphers aes-ccm
AP(config-if)# ssid NewSSID
AP(config-if)# exit
AP(config)# end
```

この例では、SSID *NewSSID* が CCKM で EAP をサポートするように設定され、AES CCMP 暗号スイートが 2.4 GHz 無線インターフェイスで有効にされます。SSID *NewSSID* は、2.4 GHz 無線インターフェイスで有効にされます。

この例で使用されているコマンドの詳細については、『*Cisco IOS Command Reference for Cisco Aironet Access Points and Bridges*』を参照してください。

802.11r のサポート

802.11r のサポートは、自律アクセス ポイントで提供されます。WGB、非ルート ブリッジ、およびリピータは、802.11r ではサポートされません。これは、クライアントのみをサポートします。

無線ドメイン サービスでは、次のタイプのローミングをサポートします。

- 分散システム（DS）上の Fast Transition
- 無線経由の Fast Transition

802.11r は、Cisco Centralized Key Management（CCKM）および Pairwise Master Key Identifier（PMKID）のローミングとは次のように異なります。

- ローミングする前に最初の認証が行われる
- 無線経由または DS を使用したターゲット AP との認証に既存アクセス ポイントの通信チャネルを使用する

802.11r の有効化

802.11r を有効にするには、次の手順を実行します。

ステップ 1　[Network] > [Network interface] を選択します。

ステップ 2　[Settings] タブをクリックします。

ステップ 3　[Radio0-802.11n 2G.Hz] または [Radio0-802.11n 5G.Hz] を選択します。

ステップ 4　11r 設定の [enable] オプション ボタンをクリックします。

ステップ 5　[over-air] または [over-ds] オプション ボタンをクリックします。

ステップ 6　再アソシエーションの時間を入力します。

値の範囲は 20 ～ 1200 です。

ステップ 7　[Apply] をクリックします。

アクセス ポイントの CLI で 802.11r を設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**dot11 ssid** <*ssid*>	SSID を設定します。
ステップ 3	**authentication key-management wpa version 2 dot11r**	アクセス ポイントに 802.11r を設定します。
ステップ 4	**interface dot11radio** {*0* | *1*}	無線インターフェイスのインターフェイス コンフィギュレーション モードを開始します。2.4 GHz 無線は Radio 0、5 GHz 無線は Radio 1 です。
ステップ 5	**dot11 dot11r pre-authentication {over-air | over-ds}**	[over-air] または [over-ds] の移行を有効または無効にします。
ステップ 6	**dot11 dot11r re-association timer** <*value*>	再アソシエーション タイマーを設定します。

管理フレーム保護の設定

管理フレーム保護の動作には WDS が必要です。MFP は、アクセス ポイントおよび WDS で手動で設定できます。

(注)　管理プラットフォームを使用しなければ、MFP は検出した侵入をレポートできないため、有効性が限定されます。

完全に保護するには、MFP アクセス ポイントで Simple Network Transfer Protocol（SNTP）も設定します。

管理フレーム保護

管理フレーム保護は、アクセス ポイントとクライアント ステーション間で転送される管理メッセージにセキュリティ機能を提供します。MFP は、インフラストラクチャ MFP とクライアント MFP の 2 つの機能コンポーネントで構成されます。

インフラストラクチャ MFP は、インフラストラクチャ サポートを提供します。インフラストラクチャ MFP は、不正デバイスおよびサービス拒絶攻撃の検出に有益なブロードキャストおよび誘導された管理フレームに対する Message Integrity Check（MIC; メッセージ完全性チェック）を利用します。クライアント MFP はクライアントをサポートします。クライアント MFP は、WLAN に対する一般的な攻撃の多くを無力化することによって、認証されたクライアントをスプーフィングされたフレームから保護します。

クライアント MFP の概要

クライアント MFP は、アクセス ポイントと CCXv5 対応クライアント ステーション間で送信されるクラス 3 管理フレームを暗号化し、スプーフィングされたクラス 3 管理フレーム（AP と認証およびアソシエートされたクライアント ステーション間で送信される管理フレーム）をドロップすることによって AP とクライアントの両方が予防措置を実行できるようにします。クライアント MFP は、IEEE 802.11i に規定されたセキュリティ メカニズムを使用して、クラス 3 ユニキャスト管理フレームを保護します。再アソシエーション要求の RSNIE で STA によって決定されたユニキャスト暗号スイートによって、ユニキャスト データとクラス 3 管理フレームの両方が保護されます。ワークグループ ブリッジ、リピータ、または非ルート ブリッジ モードのアクセス ポイントでクライアント MFP を使用するには、TKIP または AES-CCMP のいずれかのネゴシエーションが必要です。

ユニキャスト クラス 3 管理フレームは、すでにデータ フレームに使用されている方法と同様にして AES-CCMP または TKIP のいずれかを適用することによって保護されます。クライアント MFP は、暗号化が AES-CCMP または TKIP で、キー管理 WPA バージョン 2 の場合に限り、自律アクセス ポイントで有効化されます。

ブロードキャスト フレームを使用した攻撃を防ぐため、クライアント MFP 用に設定された CCXv5 をサポートするアクセス ポイントでは、ブロードキャスト クラス 3 管理フレームをいっさい送信しません。クライアント MFP が有効化されている場合、ワークグループ ブリッジ、リピータ、または非ルート ブリッジ モードのアクセス ポイントでは、ブロードキャスト クラス 3 の管理フレームが廃棄されます。

クライアント MFP は、暗号化が AES-CCMP または TKIP で、キー管理 WPA バージョン 2 の場合に限り、自律アクセス ポイントで有効化されます。

（注）　シスコでは、WPA2 を使用すること、および WPA バージョン 2 では TKIP を実装しないことを推奨しています。このモードは非推奨となっているためです。

ルート モードのアクセス ポイントのクライアント MFP

ルート モードの自律アクセス ポイントでは、混合モードのクライアントがサポートされます。CCXv5 に対応し、WPAv2 の暗号スイート AES または TKIP が決定されているクライアントでは、クライアント MFP は有効です。CCXv5 に対応していないクライアントでは、クライアント MFP は無効です。デフォルトでは、クライアント MFP はアクセス ポイント上の特定の SSID に対するオプションで、SSID コンフィギュレーション モードで CLI を使用して有効と無効を切り替えることができます。

特定の SSID に、クライアント MFP を必須とするか、オプションとするかを設定できます。クライアント MFP を必須に設定するには、SSID でキー管理 WPA バージョン 2 を必須に設定します。キー管理が WPAv2 必須に設定されていない場合、エラー メッセージが表示され、CLI コマンドが拒否されます。クライアント MFP を必須として設定したキー管理およびキー管理 WPAv2 を変更しようとすると、エラー メッセージが表示され、CLI コマンドが拒否されます。オプションとして設定されている場合、クライアント MFP は SSID で WPAv2 に対応している場合に限り有効化され、対応していない場合にはクライアント MFP は無効化されます。

クライアント MFP の設定

コマンド（Command）	説明
ids mfp client required	この SSID コンフィギュレーション コマンドは、特定の SSID でクライアント MFP を必須として有効化します。このコマンドの実行時に SSID が Dot11Radio インターフェイスにバインドされている場合は、Dot11Radio インターフェイスがリセットされます。また、このコマンドでは、SSID で WPA バージョン 2 が必須として設定されていることが要求されます。SSID で WPAv2 が必須として設定されていない場合、エラーメッセージが表示され、コマンドが拒否されます。 このコマンドの **no** 形式は、特定の SSID でクライアント MFP を無効にします。このコマンドの実行時に SSID が Dot11Radio インターフェイスにバインドされている場合は、Dot11Radio インターフェイスがリセットされます。
ids mfp client optional	この SSID コンフィギュレーション コマンドは、特定の SSID でクライアント MFP をオプションとして有効化します。このコマンドの実行時に SSID が Dot11Radio インターフェイスにバインドされている場合は、Dot11Radio インターフェイスがリセットされます。クライアント MFP は SSID で WPAv2 に対応している場合に限り、特定の SSID に対して有効化され、対応していない場合にはクライアント MFP は無効化されます。
authentication key management wpa version {1|2}	このコマンドを使用すると、特定の SSID の WPA キー管理に使用される WPA バージョンが明示的に指定されます。
dot11 ids mfp {generator | detector}	アクセス ポイントを MFP ジェネレータとして設定します。有効にすると、アクセス ポイントは Message Integrity Check Information Element（MIC IE; メッセージ完全性チェック情報エレメント）を各フレームに追加して、送信する管理フレームを保護します。フレームのコピー、改変、またはリプレイなどの攻撃が仕掛けられた場合、フレームは MIC を無効にし、MFP フレームを検出（検証）するように設定された受信アクセス ポイントのすべてで不一致がレポートされます。アクセス ポイントは、WDS のメンバーである必要があります。 アクセス ポイントを MFP ディテクタとして設定します。有効にすると、アクセス ポイントで他のアクセス ポイントから受信した管理フレームが検証されます。有効および予測された MIC IE が含まれないフレームを受信すると、WDS に不一致がレポートされます。アクセス ポイントは、WDS のメンバーである必要があります。

コマンド(Command)	説明
sntp server *server IP address*	SNTP サーバの名前または IP アドレスを入力します。
dot11 ids mfp distributor	グローバル コンフィギュレーション モードで、このコマンドを使用して WDS を MFP ディストリビュータとして設定します。有効にすると、WDS では署名キーが管理されます。このキーは MIC IE の作成に使用され、ジェネレータとディストリビュータ間で安全に転送されます。

Dot11Radio インターフェイスで以下の CLI コマンドを使用することで、アクセス ポイント コンソールのクライアント MFP に関する統計情報を表示およびクリアできます。

コマンド(Command)	説明
show dot11 ids mfp client statistics	このコマンドを使用すると、Dot11Radio インターフェイスのアクセス ポイント コンソールにクライアント MFP 統計が表示されます。
clear dot11 ids mfp client statistics	このコマンドを使用すると、クライアント MFP 統計がクリアされます。

802.11w による管理フレームの保護

現在の 802.11 標準は、無線リンクの管理および制御に使用するフレーム タイプを定義します。802.11 プロトコルに含まれる管理フレームは、WLAN に最高レベルのセキュリティが使用されている場合でも、認証も暗号化もされません。802.11w は、IEEE 802.11 標準ファミリの管理フレーム保護標準です。

802.11w は 3 種類の新しいセキュリティを提供することにより、管理フレームのセキュリティを向上します。

- データ送信元の信頼性
- リプレイ検出
- 堅牢な管理フレーム保護。

保護できる管理フレームは次のとおりです。

- ディスアソシエーション
- 認証解除
- パブリック アクション フレームを除くロバスト アクション フレーム

802.11w を使用して、アソシエーション要求のリプレイ攻撃を防ぐこともできます。802.11w が提供する保護は、Cisco クライアント MFP が提供する保護とある程度同等です。ただし、802.11w では Cisco インフラストラクチャ MFP と同等のメカニズムを提供していません。

Cisco クライアント MFP を有効にするには、保護対象のクライアントが CCXv5 をサポートすることを確認する必要があります。802.11w を有効にするには、保護対象のクライアントが 802.11w をサポートすることを確認する必要があります。

同じ SSID で Cisco インフラストラクチャ MFP と 802.11w の両方を有効にすることができます。ただし、同じ SSID と同じ無線の両方で Cisco クライアント MFP と 802.11w を有効にすることはできません。

802.11w を有効にするには、次の手順を実行します。

ステップ 1　アクセス ポイントの GUI で [Secuirty] ページを表示します。

ステップ 2　[SSID Manager] を選択します。

ステップ 3　[Client Authenticated Key Management] ページでは、次の操作を実行できます。

- 802.11w をサポートするクライアントだけが SSID に参加できるようにするには、[11w Configuration Required] オプション ボタンをクリックします。
- 802.11w をサポートするクライアントと 802.11w をサポートしないクライアントの両方が SSID に参加できるようにするには、[11w Configuration Optional] オプション ボタンをクリックします。

ステップ 4　[11w Association-comeback] の時間を入力します。

ステップ 5　[11w Saquery-retry] の時間を入力します。

次の CLI コマンドは、アクセス ポイントの 802.11w を有効にするために使用されます。

ap(config-ssid)# **11w-pmf client** *required/optional*

次の CLI コマンドは、アソシエーションのタイム アウトと saquery の再試行間隔を設定するために使用されます。

ap(config-ssid)# **11w-pmf association-comeback** *1000-20000ms*

ap(config-ssid)# **11w-pmf saquery-retry** *100-500ms*

これらのコマンドは任意です。これらのコマンドを使用しない場合、デフォルトの間隔が設定されます。アクセス ポイントに 802.11w を設定するには、MFP クライアントを無効にする必要があります。

(注)　WPAv2/AES は 802.11w では必須です。

(注)　802.11r を有効にすると、CCKM、11r 高速ローミング、DLS、無線測定、およびデュアル パブリック アクション フレーム保護はサポートされなくなります。

無線管理の設定

WDS を使用するように無線 LAN 上のアクセス ポイントを設定すると、アクセス ポイントは WDS デバイスと対話するときに自動的に無線管理における役割を果たします。無線管理の設定を行うには、ネットワーク上の管理プラットフォームと対話するように WDS デバイスを設定します。

WDS デバイスとして設定されたアクセス ポイント上の無線管理を有効にする手順は、次のとおりです。

ステップ 1　[Wireless Services Summary] ページを表示します。

ステップ 2　[WDS] をクリックして [General Setup] ページを表示します。

ステップ 3　[Configure Wireless Network Manager] チェックボックスをオンにします。

ステップ 4　[Wireless Network Manager IP Address] フィールドに、ネットワーク上の 管理プラットフォームの IP アドレスを入力します。

ステップ 5　[Apply] をクリックします。WDS アクセス ポイントが管理プラットフォームと対話するように設定されます。

CLI の設定例

次の例は、「無線管理の設定」セクション（12-25 ページ）に記載された手順と同じ働きをする CLI コマンドを示しています。

```
AP# configure terminal
AP(config)# wlccp wnm ip address 192.250.0.5
AP(config)# end
```

この例では、WDS アクセス ポイントは、IP アドレスが 192.250.0.5 の管理プラットフォームと対話できるようになります。

この例で使用されているコマンドの詳細については、『*Cisco IOS Command Reference for Cisco Aironet Access Points and Bridges*』を参照してください。

WIDS に参加するようにアクセス ポイントを設定する

WIDS に参加するには、WDS と無線管理に参加するようにアクセス ポイントを設定する必要があります。WDS と無線管理に参加するようにアクセス ポイントを設定するには、「アクセス ポイントを WDS デバイスを使用するように設定する」セクション（12-10 ページ）と「無線管理の設定」セクション（12-25 ページ）の手順を実行します。

アクセス ポイントをスキャナ モードに設定する

スキャナ モードの場合、アクセス ポイントは無線活動のチャネルをすべてスキャンし、その活動をネットワーク上の WDS デバイスに報告します。スキャナ アクセス ポイントは、クライアント アソシエーションを受け付けません。

特権 EXEC モードから、次の手順に従ってアクセス ポイントに無線ネットワークの役割をスキャナに設定します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface dot11radio { 0 | 1 }**	無線インターフェイスのインターフェイス コンフィギュレーション モードを開始します。 2.4 GHz 無線および 2.4 GHz 802.11n 無線は 0 です。 5 GHz 無線および 5 GHz 802.11n 無線は 1 です。
ステップ 3	**station role scanner**	アクセス ポイントの役割をスキャナに設定します。
ステップ 4	**end**	特権 EXEC モードに戻ります。

アクセス ポイントをモニタ モードに設定する

アクセス ポイントをスキャナとして設定すると、モニタ モードでフレームのキャプチャも可能になります。モニタ モードでは、アクセス ポイントは 802.11 フレームをキャプチャし、これをネットワーク上で WIDS エンジンに転送します。アクセス ポイントは、転送するすべての 802.11 フレームに 28 バイトのキャプチャ ヘッダーを追加します。ネットワーク上の WIDS エンジンは、このヘッダー情報を分析に使用します。アクセス ポイントは、キャプチャしたフレームの転送に UDP パケットを使用します。ネットワーク帯域幅を節約するため、複数のキャプチャしたフレームを 1 つの UDP パケットに結合できます。

スキャナ モードでは、アクセス ポイントは無線活動のすべてのチャネルをスキャンします。ただし、モニタ モードの場合、アクセス ポイントは、アクセス ポイント無線が設定されているチャネルだけをモニタします。

(注) アクセス ポイントに 2 つ無線が含まれている場合、インターフェイス上でモニタ モードを設定するには、無線が両方ともスキャナ モードに設定されている必要があります。

特権 EXEC モードから、次の手順に従って 802.11 フレームをキャプチャして転送するようにアクセス ポイントを設定します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface dot11radio** {**0** | **1**}	無線インターフェイスのインターフェイス コンフィギュレーション モードを開始します。 2.4 GHz 無線および 2.4 GHz 802.11n 無線は 0 です。 5 GHz 無線および 5 GHz 802.11n 無線は 1 です。
ステップ 3	**monitor frames endpoint ip address** *IP-address* **port** *UDP-port* [**truncate** *truncation-length*]	モニタ モードに無線を設定します。ネットワーク上の WIDS エンジン上で、IP アドレスと UDP ポートを入力します。 • (任意)転送したフレームごとに、バイト単位で最大長を設定します。アクセス ポイントは、この値より長いフレームを切り捨てます。デフォルトの長さは 128 バイトです。
ステップ 4	**end**	特権 EXEC モードに戻ります。

モニタ モード統計の表示

show wlccp ap rm monitor statistics グローバル コンフィギュレーション コマンドを使用して、キャプチャしたフレームの統計を表示します。

次に、コマンドの出力例を示します。

```
ap# show wlccp ap rm monitor statistics

Dot11Radio 0
====================
WLAN Monitoring           : Enabled
Endpoint IP address       : 10.91.107.19
Endpoint port             : 2000
Frame Truncation Length   : 535 bytes
```

```
Dot11Radio 1
====================
WLAN Monitoring           : Disabled

WLAN Monitor Statistics
=========================
Total No. of frames rx by DOT11 driver      : 58475
Total No. of Dot11 no buffers               : 361
Total No. of Frames Q Failed                : 0
Current No. of frames in SCAN Q             : 0

Total No. of frames captured                : 0
Total No. of data frames captured           : 425
Total No. of control frames captured        : 1957
Total No. of Mgmt frames captured           : 20287
Total No. of CRC errored frames captured: 0

Total No. of captured frames forwarded      : 23179
Total No. of captured frames forward failed : 0
```

clear wlccp ap rm statistics コマンドを使用して、モニタ モード統計を消去します。

モニタ モード制限の設定

モニタ モードでアクセス ポイントが使用するしきい値を設定できます。しきい値を超えると、アクセス ポイントは、情報をログに記録するかまたは警告を送信します。

認証失敗制限の設定

認証失敗制限を設定すると、*EAPOL フラッディング*と呼ばれるサービス拒絶攻撃からネットワークを保護できます。クライアントとアクセス ポイントとの間で発生する 802.1X 認証により、アクセス ポイント、オーセンティケータ、および EAPOL メッセージングを使用する認証サーバの間に、一連のメッセージが表示されます。通常、RADIUS サーバである認証サーバは、過度に認証が試みられるとすぐに負荷に耐えられなくなります。規制されていない場合、1 台のクライアントからネットワークに影響を与えるほどの認証要求が発生する可能性があります。

モニタ モードでは、アクセス ポイントは 802.1X クライアントがアクセス ポイントを通じて認証を試みる割合をトラッキングします。過度な認証の試みによってネットワークが攻撃される場合、アクセス ポイントは、認証しきい値を超えると警告を発します。

これらの制限はアクセス ポイント上で設定できます。

- アクセス ポイントからの 802.1X の試みの回数
- アクセス ポイント上の秒単位での EAPOL フラッドの期間

アクセス ポイントは、過度の認証の試みを検出すると、この情報を示すための MIB 変数を設定します。

- EAPOL フラッドが検出されました
- 認証の試みの回数
- 認証の試みの回数が最も多いクライアントの MAC アドレス

特権 EXEC モードから、次の手順に従って、アクセス ポイント上の失敗をトリガーする認証制限を設定します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**dot11 ids eap attempts** *number* **period** *seconds*	認証の試みの回数と、アクセス ポイント上で失敗をトリガーする EAPOL フラッドの秒数を設定します。
ステップ 3	**end**	特権 EXEC モードに戻ります。

802.11u Hotspot および Hotspot 2.0 の設定

802.11u Hotspot 機能により、IEEE 802.11 デバイスは外部ネットワークと対話できます。この機能はホットスポットやその他のパブリック ネットワークで、サービスがサブスクリプション ベースであるか無料であるかを問わずに使用されます。

Wi-Fi Certified Passpoint（Hotspot 2.0 とも呼ばれる）は、ホットスポットでのネットワーク アクセスを効率化し、ユーザが接続するたびにネットワークを見つけて認証を行う必要を排除します。Passpoint をサポートしていない Wi-Fi ネットワークでは、ユーザは毎回ネットワークを検索して選択し、アクセス ポイントへの接続を要求する必要があります。また多くの場合、認証クレデンシャルを再入力する必要もあります。Passpoint はそのプロセス全体を自動化し、ホットスポット ネットワークとモバイル デバイスとの間で、最高レベルの WPA2 セキュリティを適用したシームレスな接続を実現します。

802.11u Hotspot 機能は、ネットワークの検出や選択を支援し、外部ネットワークから情報を転送できるようにします。アソシエーション前にネットワークに関する情報をステーションに提供します。インターワーキングは、家、企業、およびパブリック アクセスのユーザに役立つだけでなく、製造業者やオペレータが IEEE 802.11 カスタマーに共通のコンポーネントおよびサービスを提供するのにも役立ちます。

802.11u Hotspot を設定する前に、次の条件が満たされていることを確認してください。

- WPA キー管理
- 複数の基本 SSID

802.11u Hotspot および Hotspot 2.0 を設定するには、次の手順に従います。

ステップ 1　ap(config-ssid)# モードを開始します。

ステップ 2　以下のコマンドを入力して、802.11u Hotspot を有効にして、設定します。

a. hotspot dot11u enable

b. hotspot dot11u domain *index domain_name*

c. hotspot dot11u network-type *network_type internet_availabily_status(0 or 1)*

d. hotspot dot11u auth-type *auth_type*

e. hotspot dot11u ipaddr-type *ipv4type ipv6type*

f. hotspot dot11u hessid *h.h.h*

g. hotspot dot11u nai-realm *index* realm-name *name_string*

h. hotspot dot11u nai-realm *index* eap-method *eap-index eap_method*

i. hotspot dot11u nai-realm *index* auth-method *eap-index auth-index auth_type auth_subtype*

j. hotspot dot11u roam-oi *index hex-string isbeacon*

k. hotspot dot11u 3gpp-info *index mobile_country_code mobile_network_code*

例:802.11u Hotspot の有効化

```
ap(config-ssid)# hotspot dot11u enable
ap(config-ssid)# hotspot dot11u domain 1 cisco
ap(config-ssid)# hotspot dot11u network-type  2   1
ap(config-ssid)# hotspot dot11u auth-type  1
ap(config-ssid)# hotspot dot11u ipaddr-type 2 2
ap(config-ssid)# hotspot dot11u hessid 1234.5678.1234
ap(config-ssid)# hotspot dot11u nai-realm 1 realm-name cisco
ap(config-ssid)# hotspot dot11u nai-realm 1 eap-method 1 17
ap(config-ssid)# hotspot dot11u nai-realm 1 auth-method  1 1 1 2
ap(config-ssid)# hotspot dot11u roam-oi 1 004096 1
ap(config-ssid)# hotspot dot11u 3gpp-info 1 123 123
```

ステップ 3　以下のコマンドを入力して、802.11u Hotspot 2.0 を有効にして、設定します。

a. hotspot hs2 enable

b. hotspot hs2 operator-name *index language_code operator_name*

c. hotspot hs2 wan-metrics *link_status symmetric_link_status uplink_speed downlink_speed*

d. hotspot hs2 port-config *ip_protocol port_number port_status*

例:802.11u Hotspot 2.0 の有効化

```
ap(config-ssid)# hotspot hs2 enable
ap(config-ssid)# hotspot hs2 operator-name 1 eng cisco
ap(config-ssid)# hotspot hs2 wan-metrics 1 1 2345 3434
ap(config-ssid)# hotspot hs2 port-config 1 23 34 2
```

ステップ 4　次のグローバル コンフィギュレーション コマンドを入力します。

a. dot11 dot11u ap-venue name *name_string*

b. dot11 dot11u ap-venue type *venue_group venue_type*

例:グローバル コンフィギュレーション コマンド:

```
ap(config)# dot11 dot11u ap-venue name cisco_odc
ap(config)# dot11 dot11u ap-venue type 2 2
```

802.11u Hotspot および Hotspot 2.0 の設定をデバッグするには、コマンド **debug dot11 dot11u** を使用します。

GUI を使用して 802.11u Hotspot や Hotspot 2.0 を有効にして設定するには、[Security] > [Dot11u Manager] に移動します。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。