CHAPTER 5

セキュリティ ソリューションの設定

この章では、無線 LAN のセキュリティ ソリューションについて説明します。この章の内容は、次のとおりです。

- 「Cisco UWN Solution のセキュリティ」（P.5-2）
- 「RADIUS の設定」（P.5-3）
- 「TACACS+ の設定」（P.5-19）
- 「最大ローカル データベース エントリの設定」（P.5-30）
- 「ローカル ネットワーク ユーザの設定」（P.5-32）
- 「LDAP の設定」（P.5-35）
- 「ローカル EAP の設定」（P.5-40）
- 「SpectraLink 社の NetLink 電話用システムの設定」（P.5-52）
- 「無線による管理機能の使用」（P.5-54）
- 「DHCP オプション 82 の設定」（P.5-55）
- 「アクセス コントロール リストの設定と適用」（P.5-57）
- 「管理フレーム保護の設定」（P.5-68）
- 「クライアント除外ポリシーの設定」（P.5-75）
- 「ID ネットワーキングの設定」（P.5-77）
- 「不正なデバイスの管理」（P.5-84）
- 「IDS の設定」（P.5-107）
- 「wIPS の設定」（P.5-124）
- 「意図的な悪用の検出」（P.5-127）

Cisco UWN Solution のセキュリティ

Cisco UWN Solution セキュリティの内容は、次のとおりです。

- 「セキュリティ概要」（P.5-2）
- 「レイヤ 1 ソリューション」（P.5-2）
- 「レイヤ 2 ソリューション」（P.5-2）
- 「レイヤ 3 ソリューション」（P.5-3）
- 「統合されたセキュリティ ソリューション」（P.5-3）

セキュリティ概要

Cisco UWN セキュリティ ソリューションは、802.11 アクセス ポイントのセキュリティを構成する潜在的に複雑なレイヤ 1、レイヤ 2、およびレイヤ 3 を 1 つのシンプルなポリシー マネージャにまとめたもので、システム全体のセキュリティ ポリシーを WLAN 単位でカスタマイズできます。Cisco UWN セキュリティ ソリューションは、シンプルで、統一された、体系的なセキュリティ管理ツールを提供します。

企業での WLAN 展開の最も大きな障害の 1 つが、脆弱な独立型の暗号化方式である Wired Equivalent Privacy（WEP）です。低価格のアクセス ポイントの登場も新たな問題であり、それらは企業ネットワークに接続して man-in-the-middle 攻撃や DoS 攻撃（サービス拒絶攻撃）に利用される可能性があります。また、次々に追加されるセキュリティ ソリューションの複雑さから、多くの IT マネージャが WLAN セキュリティの最新技術を採用することをためらっています。

レイヤ 1 ソリューション

Cisco UWN セキュリティ ソリューションによって、すべてのクライアントは、アクセスの試行回数をオペレータが設定した回数までに制限されます。クライアントがその制限回数内にアクセスできなかった場合、そのクライアントは、オペレータが設定したタイマーが切れるまで自動的に除外（アクセスをブロック）されます。オペレーティング システムでは、WLAN ごとに SSID ブロードキャストを無効にすることもできます。

レイヤ 2 ソリューション

上位レベルのセキュリティと暗号化が必要な場合、ネットワーク管理者は、Extensible Authentication Protocol（EAP; 拡張認証プロトコル）や Wi-Fi Protected Access（WPA）、および WPA2 など業界標準のセキュリティ ソリューションも実装できます。Cisco UWN Solution の WPA 実装には、Advanced Encryption Standard（AES）動的キー、Temporal Key Integrity Protocol + Message Integrity Code Checksum（TKIP + Michael）動的キー、WEP 静的キーが含まれます。無効化も使用され、オペレータが設定した回数だけ認証の試行に失敗すると、自動的にレイヤ 2 アクセスがブロックされます。

どの無線セキュリティ ソリューションを採用した場合も、コントローラと Lightweight アクセス ポイントとの間のすべてのレイヤ 2 有線通信は、Control and Provisioning of Wireless Access Points（CAPWAP）トンネルを使用してデータを渡すことにより保護されます。

レイヤ 3 ソリューション

WEP の問題は、パススルー Virtual Private Network（VPN; バーチャル プライベート ネットワーク）のような業界標準のレイヤ 3 セキュリティ ソリューションを使用すると、さらに進んだ解決が可能です。

Cisco UWN Solution では、ローカルおよび RADIUS Media Access Control（MAC; メディア アクセス制御）フィルタリングがサポートされています。このフィルタリングは、802.11 アクセス カード MAC アドレスの既知のリストがある小規模のクライアント グループに適しています。

さらに、Cisco UWN Solution では、ローカルおよび RADIUS ユーザおよびパスワード認証がサポートされています。この認証は、小規模から中規模のクライアント グループに適しています。

統合されたセキュリティ ソリューション

- Cisco UWN Solution オペレーティング システムのセキュリティは、堅牢な 802.1X AAA（認証、認可、アカウンティング）エンジンを中心に構築されており、オペレータは、Cisco UWN Solution 全体にわたってさまざまなセキュリティ ポリシーを迅速に設定および適用できます。
- コントローラおよび Lightweight アクセス ポイントには、システム全体の認証および認可プロトコルがすべてのポートおよびインターフェイスに装備され、最大限のシステム セキュリティが提供されています。
- オペレーティング システムのセキュリティ ポリシーは個別の WLAN に割り当てられ、Lightweight アクセス ポイントは設定されたすべての WLAN（最大 16）に同時にブロードキャストします。これにより、干渉を増加させ、システム スループットを低下させる可能性があるアクセス ポイントを追加する必要はなくなります。
- オペレーティング システム セキュリティは、RRM 機能を使用して、干渉およびセキュリティ侵犯がないか継続的に空間を監視し、それらを検出したときはオペレータに通知します。
- オペレーティング システム セキュリティは、業界標準の AAA サーバで動作し、システム統合が単純で簡単です。

RADIUS の設定

Remote Authentication Dial-In User Service（RADIUS）とは、ネットワークへの管理アクセス権を取得しようとするユーザに対して中央管理されたセキュリティ機能を提供する、クライアント/サーバ プロトコルです。このプロトコルは、ローカル認証や TACACS+ 認証と同様に、バックエンドのデータベースとして機能し、認証サービスおよびアカウンティング サービスを提供します。

- **認証**：コントローラにログインしようとするユーザを検証するプロセス。

  コントローラで RADIUS サーバに対してユーザが認証されるようにするには、ユーザは有効なユーザ名とパスワードを入力する必要があります。

  （注） 複数のデータベースを設定する場合、コントローラ GUI または CLI を使用して、バックエンド データベースが試行される順序を指定できます。

- **アカウンティング**：ユーザによる処理と変更を記録するプロセス。

ユーザによる処理が正常に実行される度に、RADIUS アカウンティング サーバでは、変更された属性、変更を行ったユーザのユーザ ID、ユーザがログインしたリモート ホスト、コマンドが実行された日付と時刻、ユーザの認可レベル、および実行された処理と入力された値の説明がログに記録されます。RADIUS アカウンティング サーバが接続不能になった場合、ユーザはセッションを続行できなくなります。

RADIUS では、転送に User Datagram Protocol（UDP; ユーザ データグラム プロトコル）を使用します。RADIUS では、1 つのデータベースが保持されます。そして、UDP ポート 1812 で受信認証要求がリッスンされ、UDP ポート 1813 で受信アカウンティング要求がリッスンされます。アクセス コントロールを要求するコントローラは、クライアントとして動作し、サーバから AAA サービスを要求します。コントローラとサーバ間のトラフィックは、プロトコルで定義されるアルゴリズムと、両方のデバイスにおいて設定される共有秘密キーによって暗号化されます。

RADIUS 認証サーバおよびアカウンティング サーバは、それぞれ最大 17 台まで設定できます。たとえば、1 台の RADIUS 認証サーバを中央に配置し、複数の RADIUS アカウンティング サーバを異なる地域に配置できます。同じタイプのサーバを複数設定すると、最初のサーバで障害が発生したり、接続不能になったりしても、コントローラは、必要に応じて 2 台目や 3 台目あるいはそれ以降のサーバへの接続を自動的に試行します。

（注） 冗長性を保つために複数の RADIUS サーバが設定されている場合、バックアップが適切に機能するようにするには、すべてのサーバでユーザ データベースを同一にする必要があります。

プライマリ RADIUS サーバ（最も低いサーバ インデックスを持つサーバ）は、コントローラの最優先サーバに想定されています。プライマリ サーバが応答しなくなると、コントローラは、次にアクティブなバックアップ サーバ（低い方から 2 番目のサーバ インデックスを持つサーバ）に切り替えます。コントローラは、プライマリ RADIUS サーバが回復して応答するようになったときにそのサーバにフォールバックするように設定されているか、使用可能なバックアップ サーバのうちのより優先されるサーバにフォールバックするように設定されていない限り、このバックアップ サーバを引き続き使用します。

CiscoSecure Access Control Server（ACS）とコントローラの両方で、RADIUS を設定する必要があります。コントローラは、GUI または CLI のいずれかを使用して設定できます。

ACS 上での RADIUS の設定

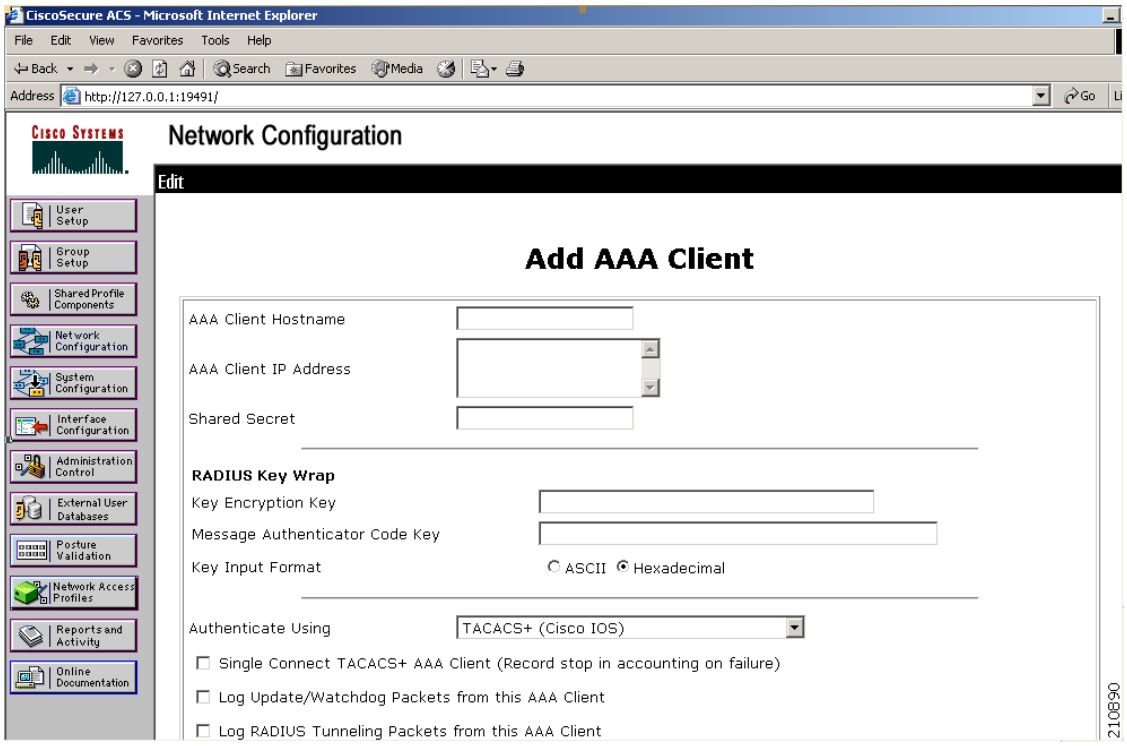
ACS 上で RADIUS を設定する手順は、次のとおりです。

（注） RADIUS は、CiscoSecure ACS バージョン 3.2 以上でサポートされます。この項に示される手順および図は、ACS バージョン 4.1 に関連するもので、他のバージョンでは異なる場合があります。実行しているバージョンの CiscoSecure ACS のマニュアルを参照してください。

ステップ 1　ACS のメイン ページで、[Network Configuration] を選択します。

ステップ 2　[AAA Clients] の下の [Add Entry] を選択し、使用しているコントローラをサーバに追加します。[Add AAA Client] ページが表示されます（図 5-1 を参照）。

図 5-1　CiscoSecure ACS の [Add AAA Client] ページ



ステップ 3　[AAA Client Hostname] フィールドに、コントローラの名前を入力します。

ステップ 4　[AAA Client IP Address] フィールドに、コントローラの IP アドレスを入力します。

ステップ 5　[Shared Secret] フィールドに、サーバとコントローラ間の認証に使用する共有秘密キーを入力します。

（注）　共有秘密キーは、サーバとコントローラの両方で同一である必要があります。

ステップ 6　[Authenticate Using] ドロップダウン ボックスから [RADIUS (Cisco Aironet)] を選択します。

ステップ 7　[Submit + Apply] をクリックして、変更内容を保存します。

ステップ 8　ACS のメイン ページで、[Interface Configuration] を選択します。

ステップ 9　[RADIUS (Cisco Aironet)] を選択します。[RADIUS (Cisco Aironet)] ページが表示されます。

ステップ 10　[User Group] の [Cisco-Aironet-Session-Timeout] チェックボックスをオンにします。

ステップ 11　[Submit] をクリックして、変更内容を保存します。

ステップ 12　ACS のメイン ページで、[System Configuration] を選択します。

ステップ 13　[Logging] を選択します。

ステップ 14　[Logging Configuration] ページが表示されたら、ログ記録するすべてのイベントを有効にし、変更内容を保存します。

ステップ 15　ACS のメイン ページで、[Group Setup] を選択します。

ステップ 16　[Group] ドロップダウン ボックスから、以前に作成したグループを選択します。

（注）　この手順では、ユーザが割り当てられることになるロールに基づいて、ACS のグループにすでにユーザが割り当てられていることを想定しています。

ステップ 17　[Edit Settings] をクリックします。[Group Setup] ページが表示されます。

ステップ 18　[Cisco Aironet Attributes] の [Cisco-Aironet-Session-Timeout] チェックボックスをオンにして、編集ボックスにセッション タイムアウト値を入力します。

ステップ 19　RADIUS 認証を使用したコントローラへの読み取り専用アクセスまたは読み取りと書き込みアクセスを指定するには、Service-Type 属性（006）を設定します。読み取り専用アクセスが必要な場合は、[Callback NAS Prompt] を設定し、読み取りと書き込みの両方の権限が必要な場合は [Administrative] を設定してください。この属性を設定しない場合、認証プロセスはコントローラ上での認可エラーなしで正常に完了しますが、認証を再試行するようにプロンプトが表示されることがあります。

（注）　ACS 上で Service-Type 属性を設定する場合は、コントローラの GUI の [RADIUS Authentication Servers] ページ上にある [Management] チェックボックスを必ずオンにします。詳細は、次の項のステップ 17 を参照してください。

（注）　「アクセス ポイントによって送信される RADIUS 認証属性」（P.5-15）には、RADIUS 属性の一覧が示されています。この属性は、Access-Request パケットおよび Access-Accept パケットで Lightweight アクセス ポイントからクライアントに送信されます。

ステップ 20　[Submit] をクリックして、変更内容を保存します。

GUI を使用した RADIUS の設定

コントローラの GUI を使用して RADIUS を設定する手順は、次のとおりです。

ステップ 1　[Security] > [AAA] > [RADIUS] の順に選択します。

ステップ 2　次のいずれかの操作を行います。

- RADIUS サーバを認証用に設定する場合は、[Authentication] を選択します。
- RADIUS サーバをアカウンティング用に設定する場合は、[Accounting] を選択します。

（注）　認証およびアカウンティングの設定に使用される GUI ページには、ほとんど同じフィールドが含まれています。そのため、ここでは [Authentication] ページを例にとって、設定の手順を一度だけ示します。同じ手順に従って、複数のサービスまたは複数のサーバを設定できます。

[RADIUS Authentication（または Accounting）Servers] ページが表示されます（図 5-2 を参照）。

図 5-2　[RADIUS Authentication Servers] ページ

このページには、これまでに設定されたすべての RADIUS サーバが表示されます。

- 既存のサーバを削除するには、そのサーバの青いドロップダウンの矢印の上にカーソルを置いて、[Remove] を選択します。
- コントローラが特定のサーバに接続されるようにするには、そのサーバの青いドロップダウンの矢印の上にカーソルを置いて、[Ping] を選択します。

ステップ 3　[Call Station ID Type] ドロップダウン ボックスから、[IP Address]、[System MAC Address]、または [AP MAC Address] を選択して、送信側の IP アドレス、システムの MAC アドレス、または AP MAC アドレスが Access-Request メッセージで RADIUS サーバに送信されるかどうかを指定します。

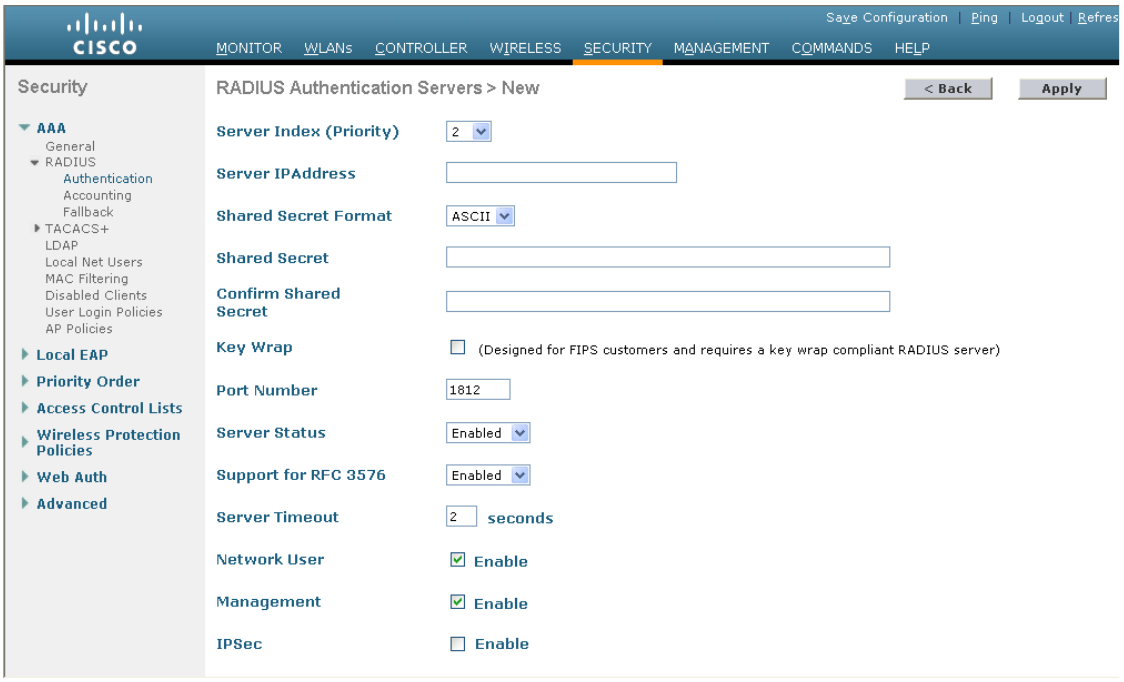
ステップ 4　AES キー ラップ保護を使用して RADIUS からコントローラへのキーの転送を有効にするには、[Use AES Key Wrap] チェックボックスをオンにします。デフォルトではオフになっています。この機能は、FIPS を使用するユーザにとって必要です。

ステップ 5　[Apply] をクリックして、変更を適用します。

ステップ 6　次のいずれかの操作を行います。

- 既存の RADIUS サーバを編集するには、そのサーバのサーバ インデックス番号をクリックします。[RADIUS Authentication（または Accounting）Servers > Edit] ページが表示されます。
- RADIUS サーバを追加するには、[New] をクリックします。[RADIUS Authentication（または Accounting）Servers > New] ページが表示されます（図 5-3 を参照）。

図 5-3　[RADIUS Authentication Servers > New] ページ



ステップ 7　新しいサーバを追加する場合、[Server Index (Priority)] ドロップダウン ボックスから数字を選択し、同じサービスを提供するその他の設定済みの RADIUS サーバに対するこのサーバの優先順位を指定します。最大 17 台のサーバを設定できます。コントローラは、最初のサーバに接続できない場合、必要に応じてリスト内の 2 番目や 3 番目あるいはそれ以降のサーバへの接続を試行します。

ステップ 8　新しいサーバを追加する場合は、[Server IP Address] フィールドに、RADIUS サーバの IP アドレスを入力します。

ステップ 9　[Shared Secret Format] ドロップダウン ボックスから、[ASCII] または [Hex] を選択し、コントローラと RADIUS サーバ間で使用される共有秘密キーの形式を指定します。デフォルト値は [ASCII] です。

ステップ 10　[Shared Secret] フィールドおよび [Confirm Shared Secret] フィールドに、コントローラとサーバ間の認証に使用する共有秘密キーを入力します。

（注）　共有秘密キーは、サーバとコントローラの両方で同一である必要があります。

ステップ 11　新しい RADIUS 認証サーバを設定して AES キー ラップを有効にすると、コントローラと RADIUS サーバ間の共有秘密キーの安全性を高めることができます。そのための手順は、次のとおりです。AES キー ラップは、Federal Information Processing Standards（FIPS）を使用するユーザのために設計されており、キー ラップ準拠の RADIUS 認証サーバを必要とします。

a. [Key Wrap] チェックボックスをオンにします。[Key Wrap Format] ドロップダウン ボックスから [ASCII] または [Hex] を選択して、Key Encryption Key（KEK）または Message Authentication Code Key（MACK）の AES キー ラップ キーの形式を指定します。

b. [Key Encryption Key (KEK)] フィールドに、16 バイトの KEK を入力します。

c. [Message Authentication Code Key (MACK)] フィールドに、20 バイトの KEK を入力します。

ステップ 12　新しいサーバを追加する場合は、[Port Number] フィールドに、インターフェイス プロトコルに対する RADIUS サーバの UDP ポート番号を入力します。有効な値の範囲は 1 ～ 65535 で、認証用のデフォルト値は 1812、アカウンティング用のデフォルト値は 1813 です。

ステップ 13　[Server Status] フィールドから [Enabled] を選択して、この RADIUS サーバを有効にするか、[Disabled] を選択して無効にします。デフォルト値は [Enabled] です。

ステップ 14　新しい RADIUS 認証サーバを設定する場合は、[Support for RFC 3576] ドロップダウン ボックスから [Enabled] を選択して RFC 3576 を有効にするか、[Disabled] を選択してこの機能を無効にします。RFC 3576 では、ユーザ セッションへの動的な変更を可能にするよう RADIUS プロトコルが拡張されています。デフォルト値は [Enabled] です。RFC 3576 では、ユーザの切断およびユーザ セッションに適用される認可の変更のほか、Disconnect メッセージと Change-of-Authorization（CoA）メッセージがサポートされています。Disconnect メッセージは、ユーザ セッションをただちに中断させる原因となります。一方、CoA メッセージでは、データ フィルタなどのセッション認可属性が変更されます。

ステップ 15　[Server Timeout] フィールドに、再送信の間隔（秒数）入力します。有効な範囲は 2 ～ 30 秒で、デフォルト値は 2 秒です。

（注）　再認証が繰り返し試行されたり、プライマリ サーバがアクティブで接続可能なときにコントローラがバックアップ サーバにフォールバックする場合には、タイムアウト値を増やすことをお勧めします。

ステップ 16　ネットワーク ユーザ認証（アカウンティング）を有効にする場合は [Network User] チェックボックスをオンにします。この機能を無効にする場合は、オフにします。デフォルト値はオンです。この機能を有効にすると、ここで設定するサーバはネットワーク ユーザの RADIUS 認証（アカウンティング）サーバと見なされます。WLAN 上の RADIUS サーバを設定しなかった場合は、ネットワーク ユーザに対してこのオプションを有効にする必要があります。

ステップ 17　RADIUS 認証サーバを設定するには、[Management] チェックボックスをオンにして管理認証を有効にします。この機能を無効にする場合は、オフにします。デフォルト値はオンです。この機能を有効にすると、ここで設定するサーバは管理ユーザの RADIUS 認証サーバと見なされ、認証要求が RADIUS サーバに送られます。

ステップ 18　IP セキュリティ メカニズムを有効にする場合は、[IPSec] チェックボックスをオンにします。この機能を無効にする場合は、オフにします。デフォルトではオフになっています。

（注）　[IPSec] オプションは、Crypto カードがコントローラに取り付けられている場合に限り表示されます。

ステップ 19　ステップ 18 で IPSec を有効にした場合は、次の手順に従って追加の IPSec パラメータを設定します。

a.　[IPSec] ドロップダウン ボックスから、IP セキュリティで使用する認証プロトコルとして、[HMAC MD5] または [HMAC SHA1] のいずれかのオプションを選択します。デフォルト値は [HMAC SHA1] です。

Message Authentication Code（MAC; メッセージ認証コード）は、秘密キーを共有する 2 者間で送信される情報を検証するために使用されます。Hash Message Authentication Code（HMAC）は、暗号ハッシュ関数に基づくメカニズムです。任意の反復暗号ハッシュ関数との組み合わせで使用できます。HMAC でハッシュ関数として MD5 を使用するのが HMAC MD5 であり、SHA1 を使用するのが HMAC SHA1 です。また、HMAC では、メッセージ認証値の計算と検証に秘密キーを使用します。

b.　[IPSec Encryption] ドロップダウン ボックスで次のオプションのいずれかを選択して、IP セキュリティ暗号化メカニズムを指定します。

- [DES]：Data Encryption Standard（DES; データ暗号化規格）は、プライベート（秘密）キーを使用するデータ暗号化の方法です。DES では、56 ビットのキーを 64 ビットのデータ ブロックごとに適用します。
- [3DES]：連続して 3 つのキーを適用するデータ暗号化規格です。これはデフォルト値です。

- [AES CBS]：Advanced Encryption Standard（AES）では、128、192、または 256 ビット長のキーを使用して 128、192、または 256 ビット長のデータ ブロックを暗号化します。AES 128 CBC では、Cipher Block Chaining（CBC; 暗号ブロック連鎖）モードで 128 ビットのデータ パスを使用します。

c. [IKE Phase 1] ドロップダウン ボックスから、[Aggressive] または [Main] のいずれかのオプションを選択して、Internet Key Exchange（IKE; インターネット キー エクスチェンジ）プロトコルを指定します。デフォルト値は [Aggressive] です。

IKE Phase 1 は、IKE の保護方法をネゴシエートするために使用されます。Aggressive モードでは、セキュリティ ゲートウェイの ID をクリアで送信するだけで、わずかに高速な接続が確立され、より少ないパケットでより多くの情報が渡されます。

d. [Lifetime] フィールドに、値（秒単位）を入力してセッションのタイムアウト間隔を指定します。有効な範囲は 1800 ～ 57600 秒で、デフォルト値は 1800 秒です。

e. [IKE Diffie Hellman Group] ドロップダウン ボックスから、[Group 1 (768 bits)]、[Group 2 (1024 bits)]、または [Group 5 (1536 bits)] のいずれかのオプションを選択して、IKE Diffie Hellman グループを指定します。デフォルト値は [Group 1 (768 bits)] です。

Diffie Hellman 技術を 2 つのデバイスで使用して共通キーを生成します。このキーを使用すると、値を公開された状態で交換して、同じ共通キーを生成することができます。3 つのグループのすべてで従来の攻撃に対するセキュリティが確保されますが、キーのサイズが大きいことから、Group 5 の安全性がより高くなります。ただし、Group 1 および Group 2 のキーを使用した計算は、素数サイズがより小さいために、多少高速に実行される可能性があります。

ステップ 20　[Apply] をクリックして、変更を適用します。

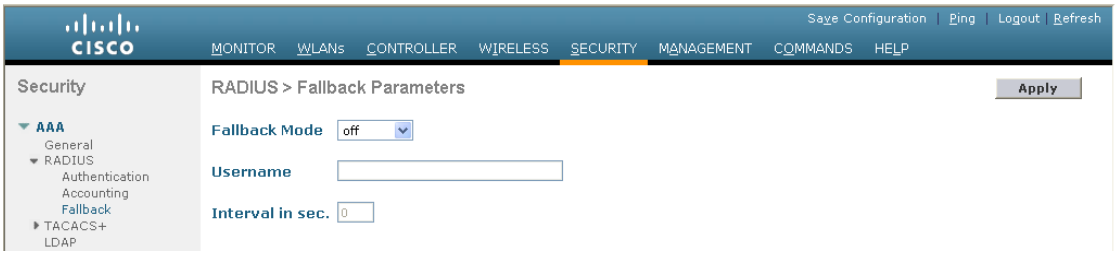
ステップ 21　[Save Configuration] をクリックして、変更を保存します。

ステップ 22　同じサーバ上または追加の RADIUS サーバ上で追加のサービスを設定する場合は、上記の手順を繰り返します。

ステップ 23　RADIUS サーバのフォールバック動作を指定する手順は、次のとおりです。

a. [Security] > [AAA] > [RADIUS] > [Fallback] の順に選択して、[RADIUS > Fallback Parameters] ページを開きます（図 5-4 を参照）。

図 5-4　[RADIUS > Fallback Parameters] ページ



b. [Fallback Mode] ドロップダウン ボックスから、次のいずれかのオプションを選択します。

- [Off]：RADIUS サーバのフォールバックを無効にします。これはデフォルト値です。
- [Passive]：コントローラが、関係のないプローブ メッセージを使用することなく、使用可能なバックアップ サーバからより低い優先順位を持つサーバへの復帰を実行するようにします。コントローラは、ある期間だけすべての非アクティブ サーバを無視し、後で RADIUS メッセージの送信が必要になったときに再試行します。
- [Active]：コントローラが、RADIUS プローブ メッセージを使用して、使用可能なバックアップ サーバからより低い優先順位を持つサーバへの復帰を実行し、非アクティブとマークされたサーバがオンラインに戻ったかどうかを判断するようにします。コントローラは、すべての

アクティブ RADIUS 要求に対して、すべての非アクティブ サーバを無視します。プライマリ サーバが回復した ACS サーバからの応答を一旦受信すると、アクティブ フォールバック RADIUS サーバは、アクティブ プローブ認証を要求しているサーバにプローブ メッセージを送信しなくなります。

c. ステップ b でフォールバック モードを [Active] にした場合は、非アクティブなサーバ プローブで送信される名前を [Username] フィールドに入力します。最大 16 文字の英数字を入力できます。デフォルト値は「cisco-probe」です。

d. ステップ b でフォールバック モードを [Active] にした場合は、[Interval in Sec] フィールドにプローブ間隔値（秒単位）を入力します。この間隔は、Passive モードでの非アクティブ時間、および Active モードでのプローブ間隔としての意味を持ちます。有効な範囲は 180 ～ 3600 秒で、デフォルト値は 300 秒です。

ステップ 24　複数のデータベースを設定する際の認証の順序を指定するには、[Security] > [Priority Order] > [Management User] の順に選択します。[Priority Order > Management User] ページが表示されます（図 5-5 を参照）。

図 5-5　[Priority Order > Management User] ページ

ステップ 25　[Order Used for Authentication] フィールドでは、コントローラによって管理ユーザの認証が試行される際に、どのサーバを優先するかを指定します。[Not Used] フィールドと [Order Used for Authentication] フィールドとの間でサーバを移動するには、[>] および [<] ボタンを使用します。[Order Used for Authentication] フィールドに希望するサーバが表示されたら、[Up] ボタンと [Down] ボタンを使用して優先するサーバをリストの先頭に移動します。

デフォルトで、ローカル データベースは常に最初に検索されます。ユーザ名が見つからない場合、コントローラは、RADIUS に設定されている場合は RADIUS サーバへの切り換え、TACACS+ に設定されている場合は TACACS+ サーバへの切り換えを行います。デフォルトの設定はローカル、RADIUS の順になっています。

ステップ 26　[Apply] をクリックして、変更を適用します。

ステップ 27　[Save Configuration] をクリックして、変更を保存します。

CLI を使用した RADIUS の設定

コントローラの CLI を使用して RADIUS を設定する手順は、次のとおりです。

（注）　CLI コマンドで使用されるパラメータの有効範囲およびデフォルト値については、「GUI を使用した RADIUS の設定」（P.5-6）を参照してください。

ステップ 1　送信側の IP アドレス、システムの MAC アドレス、または AP MAC アドレスが Access-Request メッセージで RADIUS サーバに送信されるかどうかを指定するには、次のコマンドを入力します。

config radius callStationIdType {*ip_address*, *mac_address*, *ap_mac_address*, *ap_macaddr_ssid*}

ステップ 2　Access-Request メッセージで RADIUS 認証サーバまたはアカウンティング サーバに送信される MAC アドレスにデリミタを指定するには、次のコマンドを入力します。

config radius {**auth** | **acct**} **mac-delimiter {colon** | **hyphen** | **single-hyphen** | **none**}

- **colon** はデリミタをコロンに設定します（書式は xx:xx:xx:xx:xx:xx となります）。
- **hyphen** はデリミタをハイフンに設定します（書式は xx-xx-xx-xx-xx-xx となります）。これはデフォルト値です。
- **single-hyphen** はデリミタを単一のハイフンに設定します（書式は xxxxxx-xxxxxx となります）。
- **none** はデリミタを無効にします（書式は xxxxxxxxxxxx となります）。

ステップ 3　RADIUS 認証サーバを設定するには、次のコマンドを使用します。

- **config radius auth add** *index server_ip_address port#* {**ascii** | **hex**} *shared_secret* : RADIUS 認証サーバを追加します。
- **config radius auth keywrap {enable** | **disable**} : AES キー ラップを有効にします。これによって、コントローラと RADIUS サーバ間の共有秘密キーの安全性が高まります。AES キー ラップは、Federal Information Processing Standards（FIPS）を使用するユーザのために設計されており、キー ラップ準拠の RADIUS 認証サーバを必要とします。
- **config radius auth keywrap add {ascii** | **hex**} *kek mack index* : AES キー ラップ属性を設定します。
  - *kek* では、16 バイトの Key Encryption Key（KEK）が指定されます。
  - *mack* では、20 バイトの Message Authentication Code Key（MACK）が指定されます。
  - *index* では、AES キー ラップを設定する RADIUS 認証サーバのインデックスが指定されます。
- **config radius auth rfc3576 {enable** | **disable**} ***index*** : RFC 3576 を有効または無効にします。RFC 3576 では、ユーザ セッションへの動的な変更を可能にするように RADIUS プロトコルが拡張されています。RFC 3576 では、ユーザの切断およびユーザ セッションに適用される認可の変更のほか、Disconnect メッセージと Change-of-Authorization（CoA）メッセージがサポートされています。Disconnect メッセージは、ユーザ セッションをただちに中断させる原因となります。一方、CoA メッセージでは、データ フィルタなどのセッション認可属性が変更されます。
- **config radius auth retransmit-timeout *index timeout*** : RADIUS 認証サーバの再送信のタイムアウト値を設定します。
- **config radius auth network** *index* **{enable** | **disable**} : ネットワーク ユーザ認証を有効または無効にします。この機能を有効にすると、ここで設定するサーバはネットワーク ユーザの RADIUS 認証サーバと見なされます。WLAN 上の RADIUS サーバを設定しなかった場合は、ネットワーク ユーザに対してこのオプションを有効にする必要があります。
- **config radius auth management** *index* **{enable** | **disable**} : 管理認証を有効または無効にします。この機能を有効にすると、ここで設定するサーバは管理ユーザの RADIUS 認証サーバと見なされ、認証要求が RADIUS サーバに送られます。
- **config radius auth ipsec** {**enable** | **disable**} ***index*** : IP セキュリティ メカニズムを有効または無効にします。
- **config radius auth ipsec authentication** {**hmac-md5** | **hmac-sha1**} ***index*** : IP セキュリティに使用する認証プロトコルを設定します。
- **config radius auth ipsec encryption** {**3des** | **aes** | **des** | **none**} ***index*** : IP セキュリティ暗号化メカニズムを設定します。

- **config radius auth ipsec ike dh-group** {**group-1** | **group-2** | **group-5**} ***index***：IKE Diffie Hellman グループを設定します。
- **config radius auth ipsec ike lifetime** *interval index*：セッションのタイムアウト間隔を設定します。
- **config radius auth ipsec ike phase1**{**aggressive** | **main**} ***index*** : Internet Key Exchange（IKE）プロトコルを設定します。
- **config radius auth** {**enable** | **disable**} *index* : RADIUS 認証サーバを有効または無効にします。
- **config radius auth delete** *index* : 以前に追加された RADIUS 認証サーバを削除します。

ステップ 4　RADIUS アカウンティング サーバを設定するには、次のコマンドを使用します。

- **config radius acct add** *index server_ip_address port#* {**ascii** | **hex**} *shared_secret* : RADIUS アカウンティング サーバを追加します。
- **config radius acct server-timeout** *index timeout*：RADIUS アカウンティング サーバの再送信のタイムアウト値を設定します。
- **config radius acct network** *index* {**enable** | **disable**}：ネットワーク ユーザ アカウンティングを有効または無効にします。この機能を有効にすると、ここで設定するサーバはネットワーク ユーザの RADIUS アカウンティング サーバと見なされます。WLAN 上の RADIUS サーバを設定しなかった場合は、ネットワーク ユーザに対してこのオプションを有効にする必要があります。
- **config radius acct ipsec** {**enable** | **disable**} ***index*** : IP セキュリティ メカニズムを有効または無効にします。
- **config radius acct ipsec authentication** {**hmac-md5** | **hmac-sha1**} ***index***：IP セキュリティに使用する認証プロトコルを設定します。
- **config radius acct ipsec encryption** {**3des** | **aes** | **des** | **none**} ***index***：IP セキュリティ暗号化メカニズムを設定します。
- **config radius acct ipsec ike dh-group** {**group-1** | **group-2** | **group-5**} ***index***：IKE Diffie Hellman グループを設定します。
- **config radius acct ipsec ike lifetime** *interval index*：セッションのタイムアウト間隔を設定します。
- **config radius acct ipsec ike phase1**{**aggressive** | **main**} ***index*** : Internet Key Exchange（IKE）プロトコルを設定します。
- **config radius acct** {**enable** | **disable**} *index* : RADIUS アカウンティング サーバを有効または無効にします。
- **config radius acct delete** *index* : 以前に追加された RADIUS アカウンティング サーバを削除します。

ステップ 5　RADIUS サーバのフォールバック動作を設定するには、次のコマンドを入力します。

config radius fallback-test mode {**off | passive | active**}

- **off** は、RADIUS サーバのフォールバックを無効にします。
- **passive** は、コントローラが、関係のないプローブ メッセージを使用することなく、使用可能なバックアップ サーバからより低い優先順位を持つサーバへの復帰を実行するようにします。コントローラは、ある期間だけすべての非アクティブ サーバを無視し、後で RADIUS メッセージの送信が必要になったときに再試行します。
- **active** は、コントローラが、RADIUS プローブ メッセージを使用して、使用可能なバックアップ サーバからより低い優先順位を持つサーバへの復帰を実行し、非アクティブとマークされたサーバがオンラインに戻ったかどうかを判断するようにします。コントローラは、すべてのアクティブ RADIUS 要求に対して、すべての非アクティブ サーバを無視します。プライマリ サーバが回復した ACS サーバからの応答を一旦受信すると、アクティブ フォールバック RADIUS サーバは、アクティブ プローブ認証を要求しているサーバにプローブ メッセージを送信しなくなります。

ステップ 6　ステップ 5 で Active モードを有効にした場合は、次のコマンドを入力して追加のフォールバック パラメータを設定します。

- **config radius fallback-test username** *username*：非アクティブなサーバ プローブで送信する名前を指定します。*username* パラメータには、最大 16 文字の英数字を入力できます。
- **config radius fallback-test interval** *interval*：プローブ間隔（秒単位）を指定します。

ステップ 7　変更を保存するには、次のコマンドを入力します。

save config

ステップ 8　複数のデータベースを設定する場合の認証の順序を設定するには、次のコマンドを入力します。

config aaa auth mgmt *AAA_server_type AAA_server_type*

ここで、*AAA_server_type* は **local**、**radius**、または **tacacs** となります。

現在の管理認証サーバの順序を表示するには、次のコマンドを入力します。

show aaa auth

次のような情報が表示されます。

```
Management authentication server order:
   1..................................... local
   2..................................... radius
```

ステップ 9　次のコマンドを使用して、RADIUS の統計情報を表示します。

- **show radius summary**：RADIUS サーバと統計情報の概要を表示します。
- **show radius auth statistics**：RADIUS 認証サーバの統計情報を表示します。
- **show radius acct statistics**：RADIUS アカウンティング サーバの統計情報を表示します。
- **show radius rfc3576 statistics**：RADIUS RFC 3576 サーバの概要を表示します。

show radius auth statistics コマンドに対しては、次のような情報が表示されます。

```
Authentication Servers:

Server Index..................................... 1
Server Address................................... 10.91.104.76
Msg Round Trip Time.............................. 0 (msec)
First Requests................................... 1
Retry Requests................................... 0
Accept Responses................................. 0
Reject Responses................................. 0
Challenge Responses.............................. 0
Malformed Msgs................................... 0
Bad Authenticator Msgs........................... 0
Pending Requests................................. 0
Timeout Requests................................. 0
Unknowntype Msgs................................. 0
Other Drops...................................... 0
```

show radius acct statistics コマンドに対しては、次のような情報が表示されます。

```
Accounting Servers:

Server Index..................................... 1
Server Address................................... 10.10.10.1
Msg Round Trip Time.............................. 0 (msec)
First Requests................................... 1
Retry Requests................................... 0
Accounting Responses............................. 0
Malformed Msgs................................... 0
Bad Authenticator Msgs........................... 0
```

```
Pending Requests.............................. 0
Timeout Requests.............................. 0
Unknowntype Msgs.............................. 0
Other Drops................................... 0
```

show radius rfc3576 statistics コマンドに対しては、次のような情報が表示されます。

```
RFC-3576 Servers:

Server Index.................................. 1
Server Address................................ 10.91.104.76
Disconnect-Requests........................... 0
COA-Requests.................................. 0
Retransmitted Requests........................ 0
Malformed Requests............................ 0
Bad Authenticator Requests.................... 0
Other Drops................................... 0
Sent Disconnect-Ack........................... 0
Sent Disconnect-Nak........................... 0
Sent CoA-Ack.................................. 0
Sent CoA-Nak.............................. 0
```

ステップ 10　次のコマンドを使用して、アクティブなセキュリティ アソシエーションを表示します。

- **show ike** {**brief** | **detailed**} *ip_or_mac_addr* : アクティブな Internet Key Exchange（IKE）セキュリティ アソシエーションの簡単な概要または詳しい要約を表示します。
- **show ipsec** {**brief** | **detailed**} *ip_or_mac_addr* : アクティブな Internet Protocol Security（IPSec）セキュリティ アソシエーションの簡単な概要または詳しい要約を表示します。

ステップ 11　1 台または複数台の RADIUS サーバの統計情報をクリアするには、次のコマンドを入力します。

clear stats radius {**auth** | **acct**} {*index* | **all**}

ステップ 12　コントローラが RADIUS サーバに接続できることを確認するには、次のコマンドを入力します。

ping *server_ip_address*

アクセス ポイントによって送信される RADIUS 認証属性

この項の表には、RADIUS 認証属性が示されています。この認証属性は、Access-Request パケットおよび Access-Accept パケットで Lightweight アクセス ポイントからクライアントに送信されます。

表 5-1　Access-Request パケットで送信される認証属性

属性 ID	説明
1	User-Name
2	Password
3	CHAP-Password
4	NAS-IP-Address
5	NAS-Port
6	Service-Type[1]
12	Framed-MTU
30	Called-Station-ID（MAC アドレス）
31	Calling-Station-ID（MAC アドレス）

表 5-1　Access-Request パケットで送信される認証属性

属性 ID	説明
32	NAS-Identifier
33	Proxy-State
60	CHAP-Challenge
61	NAS-Port-Type
79	EAP-Message
243	TPLUS-Role

1. RADIUS 認証を使用してコントローラへの読み取り専用アクセスまたは読み取りと書き込みアクセスを指定するには、RADIUS サーバで Service-Type 属性（6）を設定する必要があります。読み取り専用アクセスが必要な場合は [Callback NAS Prompt] を設定し、読み取りと書き込みの両方の権限が必要な場合は [Administrative] を設定してください。詳細については、「ACS 上での RADIUS の設定」の項のステップ 19 を参照してください。

表 5-2　Access-Accept パケットで受け付けられる認証属性（シスコ）

属性 ID	説明
1	Cisco-LEAP-Session-Key
2	Cisco-Keywrap-Msg-Auth-Code
3	Cisco-Keywrap-NonCE
4	Cisco-Keywrap-Key
5	Cisco-URL-Redirect
6	Cisco-URL-Redirect-ACL

（注）　シスコ固有の属性 Auth-Algo-Type および SSID はサポートされません。

表 5-3　Access-Accept パケットで受け付けられる認証属性（標準）

属性 ID	説明
6	Service-Type[1]
8	Framed-IP-Address
25	Class
26	Vendor-Specific
27	Timeout
29	Termination-Action
40	Acct-Status-Type
64	Tunnel-Type
79	EAP-Message
81	Tunnel-Group-ID

1. RADIUS 認証を使用してコントローラへの読み取り専用アクセスまたは読み取りと書き込みアクセスを指定するには、RADIUS サーバで Service-Type 属性（6）を設定する必要があります。読み取り専用アクセスが必要な場合は [Callback NAS Prompt] を設定し、読み取りと書き込みの両方の権限が必要な場合は [Administrative] を設定してください。詳細については、「ACS 上での RADIUS の設定」の項のステップ 19 を参照してください。

（注）　メッセージ オーセンティケータはサポートされていません。

表 5-4　Access-Accept パケットで受け付けられる認証属性（Microsoft）

属性 ID	説明
11	MS-CHAP-Challenge
16	MS-MPPE-Send-Key
17	MS-MPPE-Receive-Key
25	MS-MSCHAP2-Response
26	MS-MSCHAP2-Success

表 5-5　Access-Accept パケットで受け付けられる認証属性（Airespace）

属性 ID	説明
1	VAP-ID
2	QoS-Level
3	DSCP
4	8021P-Type
5	VLAN-Interface-Name
6	ACL-Name
7	Data-Bandwidth-Average-Contract
8	Real-Time-Bandwidth-Average-Contract
9	Data-Bandwidth-Burst-Contract
10	Real-Time-Bandwidth-Burst-Contract
11	Guest-Role-Name

RADIUS アカウンティング属性

表 5-6 に、コントローラから RADIUS サーバに送信されるアカウンティング要求の RADIUS アカウンティング属性を示します。表 5-7 には Accounting-Status-Type 属性（40）のさまざまな値の一覧を表示します。

表 5-6　アカウンティング要求のアカウンティング属性

属性 ID	説明
1	User-Name
4	NAS-IP-Address
5	NAS-Port
8	Framed-IP-Address
25	Class
30	Called-Station-ID（MAC アドレス）
31	Calling-Station-ID（MAC アドレス）
32	NAS-Identifier
40	Accounting-Status-Type
41	Accounting-Delay-Time（ストップおよび中間メッセージのみ）
42	Accounting-Input-Octets（ストップおよび中間メッセージのみ）
43	Accounting-Output-Octets（ストップおよび中間メッセージのみ）
44	Accounting-Session-ID
45	Accounting-Authentic
46	Accounting-Session-Time（ストップおよび中間メッセージのみ）
47	Accounting-Input-Packets（ストップおよび中間メッセージのみ）
48	Accounting-Output-Packets（ストップおよび中間メッセージのみ）
49	Accounting-Terminate-Cause（ストップおよび中間メッセージのみ）

表 5-6　アカウンティング要求のアカウンティング属性 （続き）

属性 ID	説明
64	Tunnel-Type
65	Tunnel-Medium-Type
81	Tunnel-Group-ID

表 5-7　Accounting-Status-Type 属性の値

属性 ID	説明
1	Start
2	Stop
3	Interim-Update
7	Accounting-On
8	Accounting-Off
9-14	トンネリングのアカウンティング用に予約
15	Failed 用に予約

TACACS+ の設定

Terminal Access Controller Access Control System Plus（TACACS+）は、コントローラへの管理アクセスを取得しようとするユーザに中央管理されたセキュリティを提供する、クライアント/サーバ プロトコルです。このプロトコルは、ローカルおよび RADIUS に類似したバックエンドのデータベースとして機能します。ただし、ローカルおよび RADIUS では、認証サポートと制限のある認可サポートしか提供されないのに対し、TACACS+ では、次の 3 つのサービスが提供されます。

- **認証**：コントローラにログインしようとするユーザを検証するプロセス。

  コントローラで TACACS+ サーバに対してユーザが認証されるようにするには、ユーザは有効なユーザ名とパスワードを入力する必要があります。認証サービスおよび認可サービスは、互いに密接に関連しています。たとえば、ローカルまたは RADIUS データベースを使用して認証が実行された場合、認可ではそのローカルまたは RADIUS データベース内のユーザに関連したアクセス権（read-only、read-write、lobby-admin のいずれか）が使用され、TACACS+ は使用されません。同様に、TACACS+ を使用して認証が実行されると、認可は TACACS+ に関連付けられます。

  （注） 複数のデータベースを設定する場合、コントローラ GUI または CLI を使用して、バックエンド データベースが試行される順序を指定できます。

- **認可**：ユーザのアクセス レベルに基づいて、ユーザがコントローラで実行できる処理を決定するプロセス。

  TACACS+ の場合、認可は特定の処理ではなく、権限（またはロール）に基づいて実行されます。利用可能なロールは、コントローラ GUI の 7 つのメニュー オプション（[MONITOR]、[WLAN]、[CONTROLLER]、[WIRELESS]、[SECURITY]、[MANAGEMENT]、および [COMMANDS]）に対応しています。ロビー アンバサダー権限のみを必要とするユーザは、追加のロールである LOBBY を使用できます。ユーザが割り当てられるロールは、TACACS+ サーバ上で設定されます。ユーザは 1 つまたは複数のロールに対して認可されます。最小の認可は MONITOR のみで、最大は ALL です。ALL では、ユーザは 7 つのメニュー オプションすべてに関連付けられた機能を実行できるよう認可されます。たとえば、SECURITY のロールを割り当てられたユーザは、

[Security] メニューに表示される（または CLI の場合はセキュリティ コマンドとして指定される）すべてのアイテムに対して変更を実行できます。ユーザが特定のロール（WLAN など）に対して認可されていない場合でも、そのユーザは読み取り専用モード（または関連する CLI の **show** コマンド）で、そのメニュー オプションにアクセスできます。TACACS+ 認可サーバが接続不能または認可不能になった場合、ユーザはコントローラにログインできません。

（注）　ユーザが割り当てられたロールでは許可されていないコントローラ GUI のページに変更を加えようとすると、十分な権限がないことを示すメッセージが表示されます。ユーザが割り当てられたロールでは許可されていないコントローラ CLI コマンドを入力すると、実際にはそのコマンドは実行されていないのに、正常に実行されたというメッセージが表示されます。この場合、「Insufficient Privilege!Cannot execute command!」という追加のメッセージが表示され、コマンドを実行するための十分な権限がないことがユーザに通知されます。

- **アカウンティング**：ユーザによる処理と変更を記録するプロセス。

  ユーザによる処理が正常に実行される度に、TACACS+ アカウンティング サーバでは、変更された属性、変更を行ったユーザのユーザ ID、ユーザがログインしたリモート ホスト、コマンドが実行された日付と時刻、ユーザの認可レベル、および実行された処理と入力された値の説明がログに記録されます。TACACS+ アカウンティング サーバが接続不能になった場合、ユーザはセッションを中断されずに続行できます。

RADIUS で User Datagram Protocol（UDP; ユーザ データグラム プロトコル）を使用するのとは異なり、TACACS+ では、転送に Transmission Control Protocol（TCP; 転送制御プロトコル）を使用します。1 つのデータベースを維持し、TCP ポート 49 で受信要求をリッスンします。アクセス コントロールを要求するコントローラは、クライアントとして動作し、サーバから AAA サービスを要求します。コントローラとサーバ間のトラフィックは、プロトコルで定義されるアルゴリズムと、両方のデバイスにおいて設定される共有秘密キーによって暗号化されます。

最大 3 台の TACACS+ 認証サーバ、認可サーバ、およびアカウンティング サーバをそれぞれ設定できます。たとえば、1 台の TACACS+ 認証サーバを中央に配置し、複数の TACACS+ 認可サーバを異なる地域に配置できます。同じタイプの複数のサーバを設定していると、最初のサーバで障害が発生したり、接続不能になっても、コントローラは自動的に 2 台目、および必要に応じて 3 台目のサーバを試行します。

（注）　複数の TACACS+ サーバが冗長性のために設定されている場合、バックアップが適切に機能するようにするには、すべてのサーバにおいてユーザ データベースを同一にする必要があります。

CiscoSecure Access Control Server（ACS）とコントローラの両方で、TACACS+ を設定する必要があります。コントローラは、GUI または CLI のいずれかを使用して設定できます。

ACS 上での TACACS+ の設定

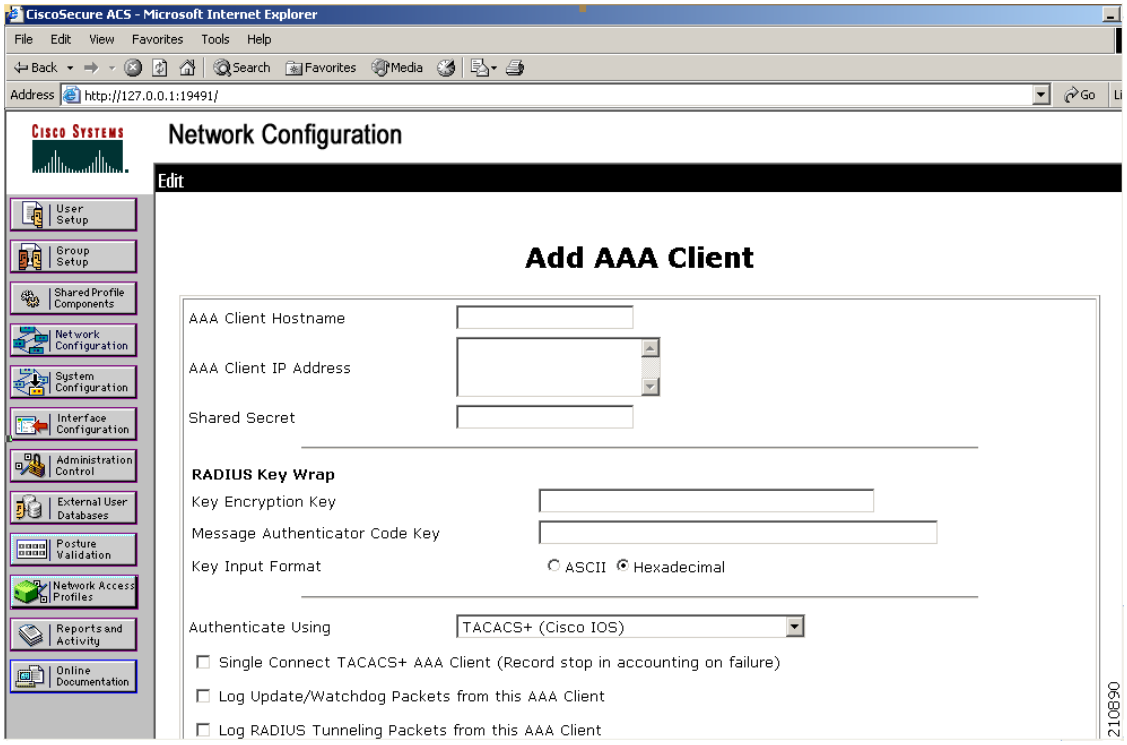
ACS 上で TACACS+ を設定する手順は、次のとおりです。

（注）　TACACS+ は、CiscoSecure ACS バージョン 3.2 以上でサポートされます。この項に示される手順および図は、ACS バージョン 4.1 に関連するもので、他のバージョンでは異なる場合があります。実行しているバージョンの CiscoSecure ACS のマニュアルを参照してください。

ステップ 1　ACS のメイン ページで、[Network Configuration] を選択します。

ステップ 2　[AAA Clients] の下の [Add Entry] を選択し、使用しているコントローラをサーバに追加します。[Add AAA Client] ページが表示されます（図 5-6 を参照）。

図 5-6　CiscoSecure ACS の [Add AAA Client] ページ



ステップ 3　[AAA Client Hostname] フィールドに、コントローラの名前を入力します。

ステップ 4　[AAA Client IP Address] フィールドに、コントローラの IP アドレスを入力します。

ステップ 5　[Shared Secret] フィールドに、サーバとコントローラ間の認証に使用する共有秘密キーを入力します。

（注）　共有秘密キーは、サーバとコントローラの両方で同一である必要があります。

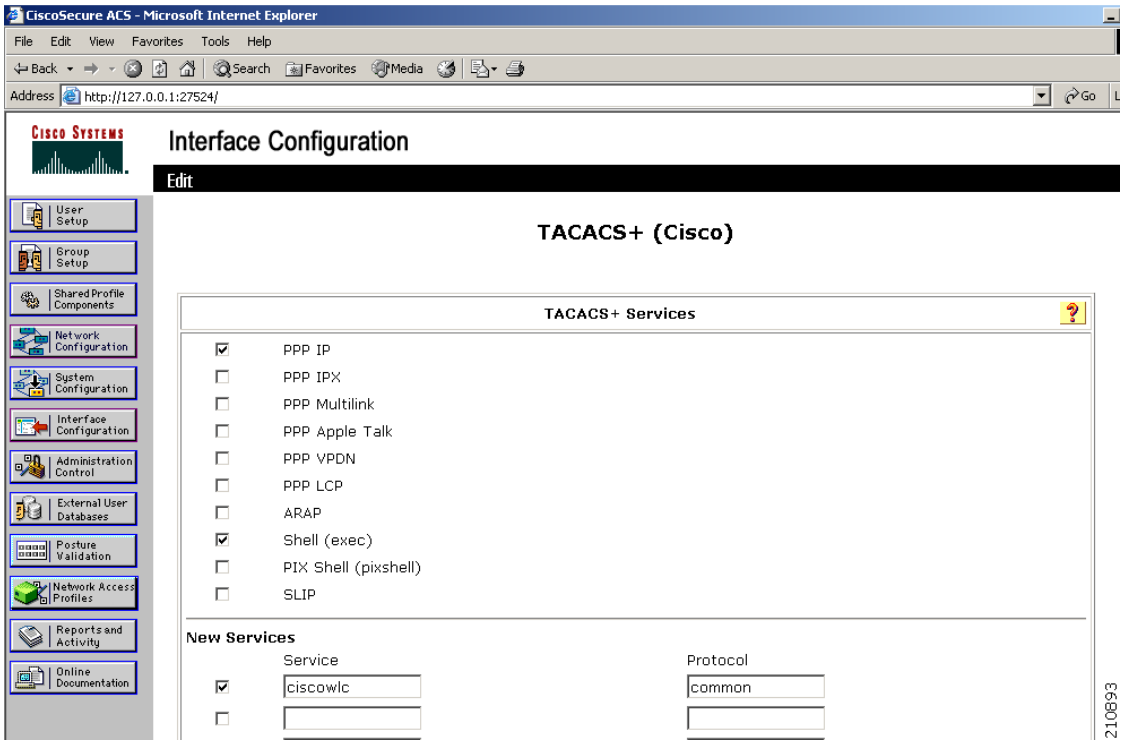
ステップ 6　[Authenticate Using] ドロップダウン ボックスから [TACACS+ (Cisco IOS)] を選択します。

ステップ 7　[Submit + Apply] をクリックして、変更内容を保存します。

ステップ 8　ACS のメイン ページで、[Interface Configuration] を選択します。

ステップ 9　[TACACS+ (Cisco IOS)] を選択します。[TACACS+ (Cisco)] ページが表示されます（図 5-7 を参照）。

図 5-7　CiscoSecure ACS の [TACACS+ (Cisco)] ページ



ステップ 10　[TACACS+ Services] で、[Shell (exec)] チェックボックスをオンにします。

ステップ 11　[New Services] で、最初のチェックボックスをオンにし、[Service] フィールドに **ciscowlc** と入力し、[Protocol] フィールドに **common** と入力します。

ステップ 12　[Advanced Configuration Options] で、[Advanced TACACS+ Features] チェックボックスをオンにします。

ステップ 13　[Submit] をクリックして、変更内容を保存します。

ステップ 14　ACS のメイン ページで、[System Configuration] を選択します。

ステップ 15　[Logging] を選択します。

ステップ 16　[Logging Configuration] ページが表示されたら、ログ記録するすべてのイベントを有効にし、変更内容を保存します。

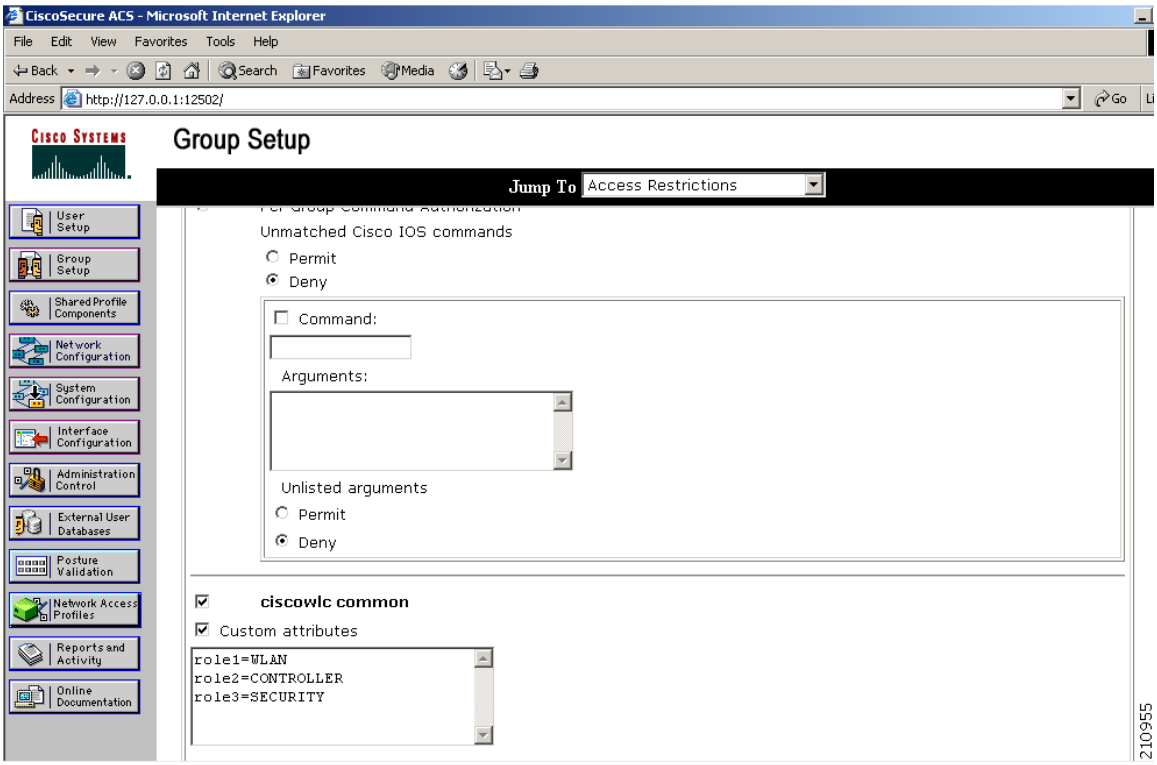
ステップ 17　ACS のメイン ページで、[Group Setup] を選択します。

ステップ 18　[Group] ドロップダウン ボックスから、以前に作成したグループを選択します。

（注）　この手順では、ユーザが割り当てられることになるロールに基づいて、ACS のグループにすでにユーザが割り当てられていることを想定しています。

ステップ 19　[Edit Settings] をクリックします。[Group Setup] ページが表示されます（図 5-8 を参照）。

図 5-8　CiscoSecure ACS の [Group Setup] ページ



ステップ 20　[TACACS+ Settings] の [ciscowlc common] チェックボックスをオンにします。

ステップ 21　[Custom Attributes] チェックボックスをオンにします。

ステップ 22　[Custom Attributes] の下のテキストボックスで、このグループに割り当てるロールを指定します。使用可能なロールは、MONITOR、WLAN、CONTROLLER、WIRELESS、SECURITY、MANAGEMENT、COMMANDS、ALL、および LOBBY です。前述のように、最初の 7 つのロールは、コントローラ GUI のメニュー オプションに対応しており、これら特定のコントローラ機能へのアクセスを許可します。グループでの必要性に応じて、1 つまたは複数のロールを入力できます。7 つのロールすべてを指定するには ALL を、ロビー アンバサダー ロールを指定するには LOBBY を使用します。次の形式を使用してロールを入力します。

role*x*=*ROLE*

たとえば、特定のユーザ グループに対して WLAN、CONTROLLER、および SECURITY のロールを指定するには、次のテキストを入力します。

```
role1=WLAN
role2=CONTROLLER
role3=SECURITY
```

あるユーザ グループに 7 つのロールすべてに対するアクセスを付与するには、次のテキストを入力します。

```
role1=ALL
```

（注）　必ず上記の形式を使用してロールを入力するようにしてください。ロールはすべて大文字で入力する必要があり、テキスト間にスペースは挿入できません。

（注）　MONITOR ロールまたは LOBBY ロールは、その他のロールと組み合わせることはできません。[Custom Attributes] テキストボックスにこれら 2 つのロールのどちらかを指定すると、追加のロールが指定された場合でも、ユーザには MONITOR または LOBBY 権限のみが付与されます。

ステップ 23　[Submit] をクリックして、変更内容を保存します。

GUI を使用した TACACS+ の設定

コントローラの GUI を使用して TACACS+ を設定する手順は、次のとおりです。

ステップ 1　[Security] > [AAA] > [TACACS+] の順に選択します。

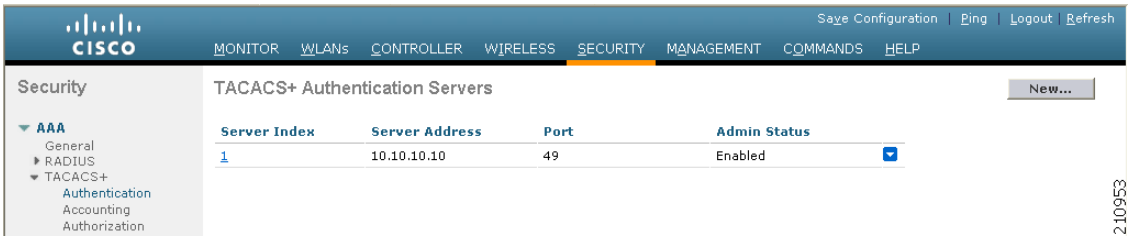
ステップ 2　次のいずれかの操作を行います。

- TACACS+ サーバを認証用に設定する場合は、[Authentication] を選択します。
- TACACS+ サーバを認可用に設定する場合は、[Authorization] を選択します。
- TACACS+ サーバをアカウンティング用に設定する場合、[Accounting] をクリックします。

（注）　認証、認可、アカウンティングの設定に使用される GUI ページには、すべて同じフィールドが含まれます。そのため、ここでは [Authentication] ページを例にとって、設定の手順を一度だけ示します。同じ手順に従って、複数のサービスまたは複数のサーバを設定できます。

[TACACS+（Authentication、Authorization、または Accounting）Servers] ページが表示されます（図 5-9 を参照）。

図 5-9　[TACACS+ Authentication Servers] ページ



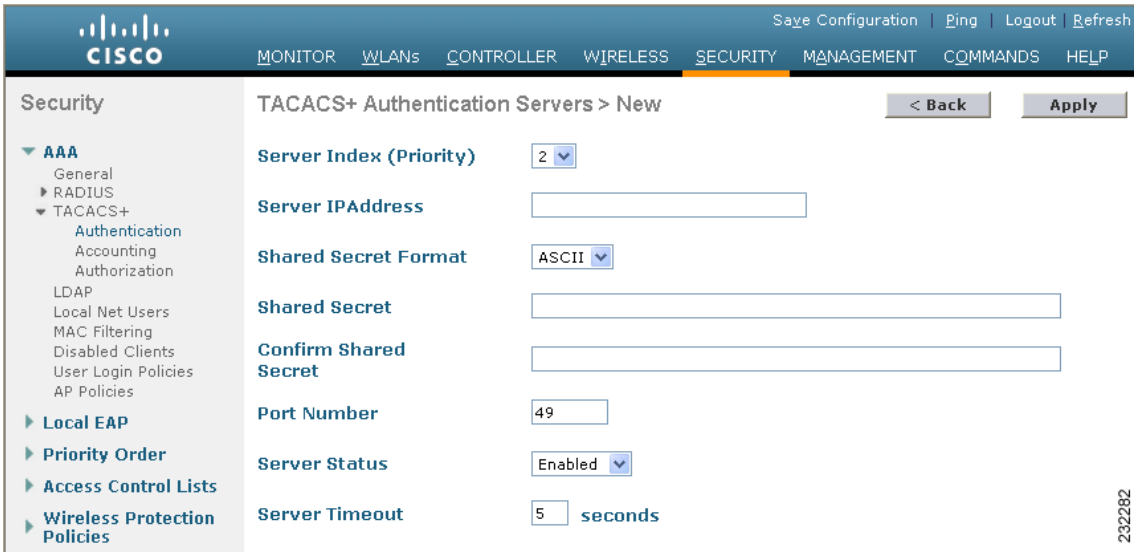
このページでは、これまでに設定されたすべての TACACS+ サーバが表示されます。

- 既存のサーバを削除するには、そのサーバの青いドロップダウンの矢印の上にカーソルを置いて、[Remove] を選択します。
- コントローラが特定のサーバに接続されるようにするには、そのサーバの青いドロップダウンの矢印の上にカーソルを置いて、[Ping] を選択します。

ステップ 3　次のいずれかの操作を行います。

- 既存の TACACS+ サーバを編集するには、そのサーバのサーバ インデックス番号をクリックします。[TACACS+（Authentication、Authorization、または Accounting）Servers > Edit] ページが表示されます。
- TACACS+ サーバを追加するには、[New] をクリックします。[TACACS+（Authentication、Authorization、または Accounting）Servers > New] ページが表示されます（図 5-10 を参照）。

図 5-10　[TACACS+ Authentication Servers >New] ページ



ステップ 4　新しいサーバを追加する場合、[Server Index (Priority)] ドロップダウン ボックスから数字を選択し、同じサービスを提供するその他の設定済みの TACACS+ サーバに対するこのサーバの優先順位を指定します。最大 3 台のサーバを設定できます。コントローラが最初のサーバに接続できない場合、リスト内の 2 番目および必要に応じて 3 番目のサーバへの接続を試行します。

ステップ 5　新しいサーバを追加する場合は、[Server IP Address] フィールドに、TACACS+ サーバの IP アドレスを入力します。

ステップ 6　[Shared Secret Format] ドロップダウン ボックスから、[ASCII] または [Hex] を選択し、コントローラと TACACS+ サーバ間で使用される共有秘密キーの形式を指定します。デフォルト値は [ASCII] です。

ステップ 7　[Shared Secret] フィールドおよび [Confirm Shared Secret] フィールドに、コントローラとサーバ間の認証に使用する共有秘密キーを入力します。

（注）　共有秘密キーは、サーバとコントローラの両方で同一である必要があります。

ステップ 8　新しいサーバを追加する場合は、[Port Number] フィールドに、インターフェイス プロトコルに対する TACACS+ サーバの TCP ポート番号を入力します。有効な範囲は 1 ～ 65535 で、デフォルト値は 49 です。

ステップ 9　[Server Status] フィールドから [Enabled] を選択して、この TACACS+ サーバを有効にするか、[Disabled] を選択して無効にします。デフォルト値は [Enabled] です。

ステップ 10　[Server Timeout] フィールドに、再送信の間隔（秒数）を入力します。有効な範囲は 5 ～ 30 秒で、デフォルト値は 5 秒です。

（注）　再認証が繰り返し試行されたり、プライマリ サーバがアクティブで接続可能なときにコントローラがバックアップ サーバにフォールバックする場合には、タイムアウト値を増やすことをお勧めします。

ステップ 11　[Apply] をクリックして、変更を適用します。

ステップ 12　[Save Configuration] をクリックして、変更を保存します。

ステップ 13　同じサーバ上で、または追加の TACACS+ サーバ上で追加のサービスを設定する場合は、上記の手順を繰り返します。

ステップ 14　複数のデータベースを設定する際の認証の順序を指定するには、[Security] > [Priority Order] > [Management User] の順に選択します。[Priority Order > Management User] ページが表示されます（図 5-11 を参照）。

図 5-11　[Priority Order > Management User] ページ

ステップ 15　[Order Used for Authentication] フィールドでは、コントローラによって管理ユーザの認証が試行される際に、どのサーバを優先するかを指定します。[Not Used] フィールドと [Order Used for Authentication] フィールドとの間でサーバを移動するには、[>] および [<] ボタンを使用します。[Order Used for Authentication] フィールドに希望するサーバが表示されたら、[Up] ボタンと [Down] ボタンを使用して優先するサーバをリストの先頭に移動します。

デフォルトで、ローカル データベースは常に最初に検索されます。ユーザ名が見つからない場合、コントローラは、RADIUS に設定されている場合は RADIUS サーバへの切り換え、TACACS+ に設定されている場合は TACACS+ サーバへの切り換えを行います。デフォルトの設定はローカル、RADIUS の順になっています。

ステップ 16　[Apply] をクリックして、変更を適用します。

ステップ 17　[Save Configuration] をクリックして、変更を保存します。

CLI を使用した TACACS+ の設定

コントローラ CLI を使用して TACACS+ を設定するには、この項のコマンドを使用します。

（注）　CLI コマンドで使用されるパラメータの有効範囲およびデフォルト値については、「GUI を使用した TACACS+ の設定」（P.5-24）を参照してください。

1. TACACS+ 認証サーバを設定するには、次のコマンドを使用します。
   - **config tacacs auth add** *index server_ip_address port#* {**ascii** | **hex**} *shared_secret*:TACACS+ 認証サーバを追加します。
   - **config tacacs auth delete** *index*：以前に追加された TACACS+ 認証サーバを削除します。
   - **config tacacs auth** {**enable** | **disable**} *index*：TACACS+ 認証サーバを有効または無効にします。
   - **config tacacs auth server-timeout** *index timeout*：TACACS+ 認証サーバの再送信のタイムアウト値を設定します。
2. TACACS+ 認可サーバを設定するには、次のコマンドを使用します。
   - **config tacacs athr add** *index server_ip_address port#* {**ascii** | **hex**} *shared_secret*:TACACS+ 認可サーバを追加します。
   - **config tacacs athr delete** *index*：以前に追加された TACACS+ 認可サーバを削除します。
   - **config tacacs athr** {**enable** | **disable**} *index*：TACACS+ 認可サーバを有効または無効にします。
   - **config tacacs athr server-timeout** *index timeout*：TACACS+ 認可サーバの再送信のタイムアウト値を設定します。
3. TACACS+ アカウンティング サーバを設定するには、次のコマンドを使用します。
   - **config tacacs acct add** *index server_ip_address port#* {**ascii** | **hex**} *shared_secret*:TACACS+ アカウンティング サーバを追加します。
   - **config tacacs acct delete** *index*:以前に追加された TACACS+ アカウンティング サーバを削除します。
   - **config tacacs acct** {**enable** | **disable**} *index*：TACACS+ アカウンティング サーバを有効または無効にします。
   - **config tacacs acct server-timeout** *index timeout*：TACACS+ アカウンティングの再送信のタイムアウト値を設定します。
4. 次のコマンドを使用して、TACACS+ の統計を表示します。
   - **show tacacs summary**：TACACS+ サーバと統計情報の概要を表示します。
   - **show tacacs auth stats**：TACACS+ 認証サーバの統計情報を表示します。
   - **show tacacs athr stats**：TACACS+ 認可サーバの統計情報を表示します。
   - **show tacacs acct stats**：TACACS+ アカウンティング サーバの統計情報を表示します。

   たとえば、**show tacacs summary** コマンドに対しては、次のような情報が表示されます。

```
Authentication Servers

Idx  Server Address     Port    State     Tout
---  ----------------  ------  --------  ----
1    11.11.12.2        49      Enabled   5
2    11.11.13.2        49      Enabled   5
3    11.11.14.2        49      Enabled   5
```

```
Authorization Servers

Idx  Server Address    Port    State     Tout
---  ----------------  ------  --------  ----
1    11.11.12.2        49      Enabled   5
2    11.11.13.2        49      Enabled   5
3    11.11.14.2        49      Enabled   5

Accounting Servers

Idx  Server Address    Port    State     Tout
---  ----------------  ------  --------  ----
1    11.11.12.2        49      Enabled   5
2    11.11.13.2        49      Enabled   5
3    11.11.14.2        49      Enabled   5
```

show tacacs auth stats コマンドに対しては、次のような情報が表示されます。

```
Server Index..................................... 1
Server Address................................... 10.10.10.10
Msg Round Trip Time.............................. 0 (msec)
First Requests................................... 0
Retry Requests................................... 0
Accept Responses................................. 0
Reject Responses................................. 0
Error Responses.................................. 0
Restart Responses................................ 0
Follow Responses................................. 0
GetData Responses................................ 0
Encrypt no secret Responses...................... 0
Challenge Responses.............................. 0
Malformed Msgs................................... 0
Bad Authenticator Msgs........................... 0
Pending Requests................................. 0
Timeout Requests................................. 0
Unknowntype Msgs................................. 0
Other Drops.....................................0
```

5. 1 台または複数台の TACACS+ サーバの統計をクリアするには、次のコマンドを入力します。

   clear stats tacacs [**auth** | **athr** | **acct**] {*index* | **all**}

6. 複数のデータベースを設定する場合の認証の順序を設定するには、次のコマンドを入力します。デフォルトの設定はローカル、radius の順になっています。

   config aaa auth mgmt [**radius** | **tacacs**]

   現在の管理認証サーバの順序を表示するには、次のコマンドを入力します。

   show aaa auth

   次のような情報が表示されます。

```
Management authentication server order:
   1..................................... local
   2..................................... tacacs
```

7. コントローラが確実に TACACS+ サーバに接続できるようにするには、次のコマンドを入力します。

   ping *server_ip_address*

8. TACACS+ のデバッグを有効または無効にするには、次のコマンドを入力します。

   debug aaa tacacs {**enable** | **disable**}

9. 変更を保存するには、次のコマンドを入力します。
   save config

TACACS+ 管理サーバのログの表示

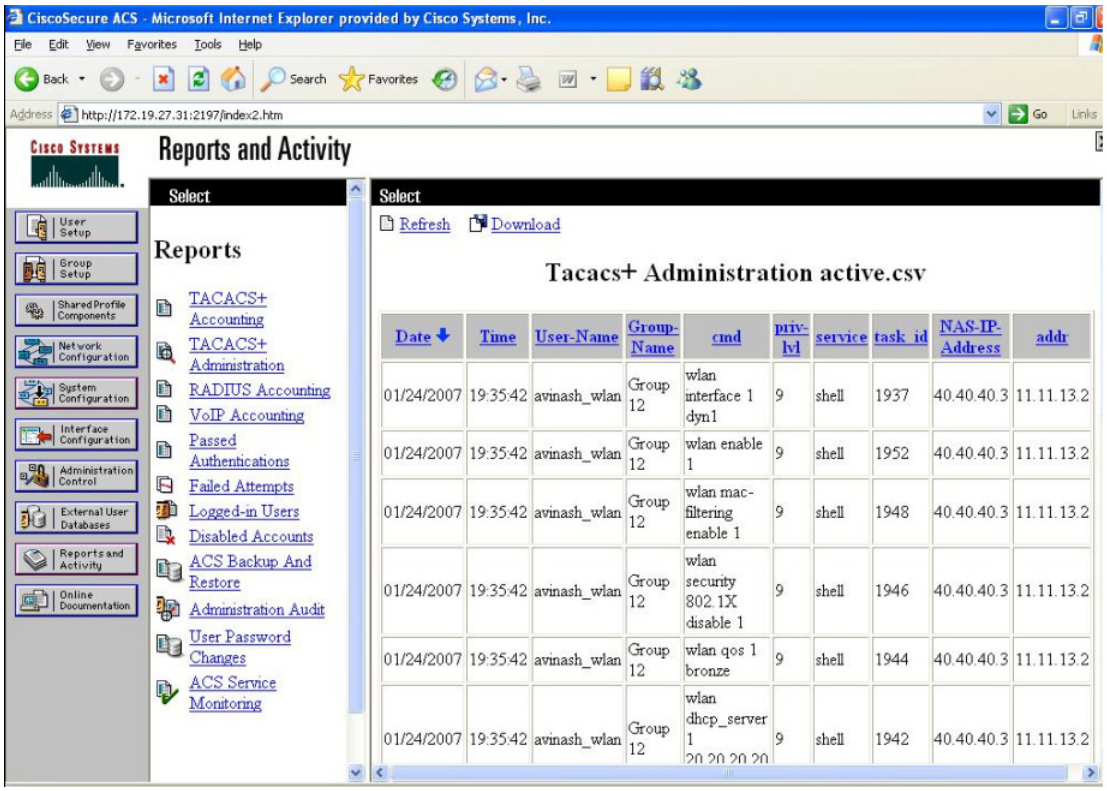
コントローラ上で TACACS+ アカウンティング サーバが設定されている場合、TACACS+ 管理サーバのログを表示する手順は、次のとおりです。

ステップ 1　ACS のメイン ページで、[Reports and Activity] を選択します。

ステップ 2　[TACACS+ Administration] を選択します。

ステップ 3　表示するログの日付に対応する .csv ファイルをクリックします。[TACACS+ Administration .csv] ページが表示されます（図 5-12 を参照）。

図 5-12　CiscoSecure ACS の [TACACS+ Administration .csv] ページ



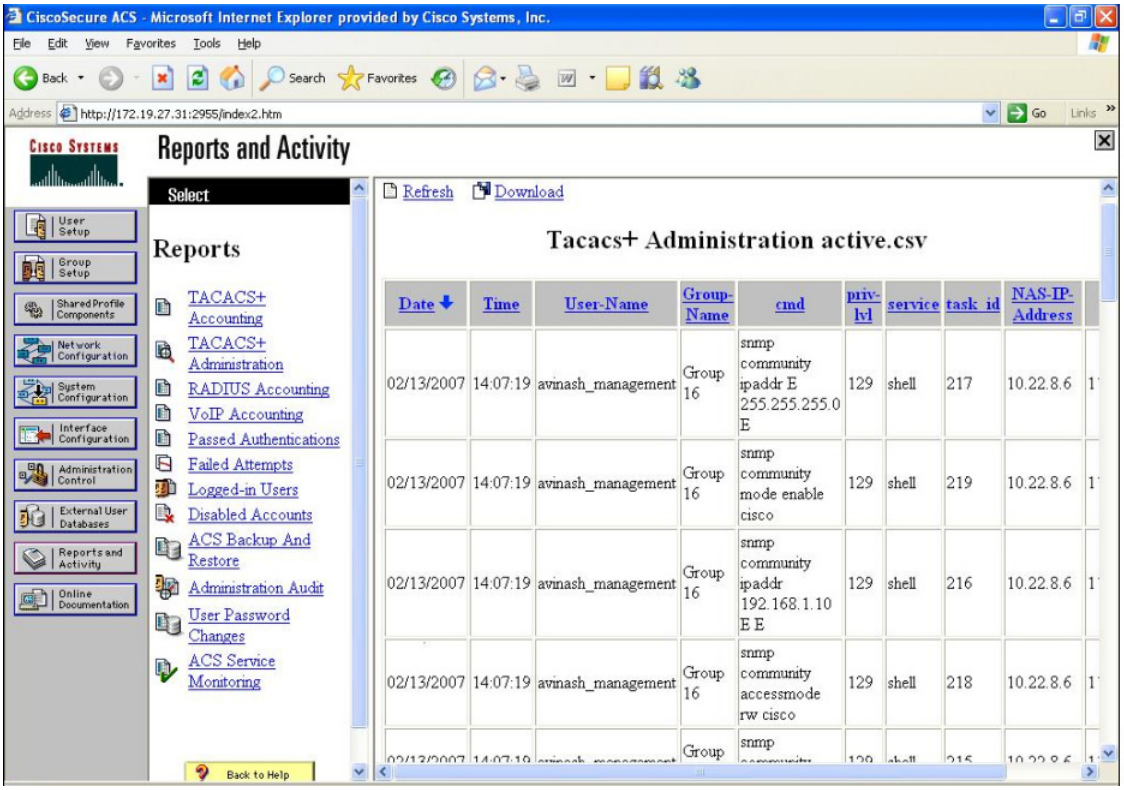
このページには、次の情報が表示されます。

- 処理が実行された日付と時刻
- 処理を実行したユーザの名前と割り当てられたロール
- ユーザが属するグループ
- ユーザが実行した特定の処理
- 処理を実行したユーザの権限レベル

- コントローラの IP アドレス
- 処理が実行されたノートパソコンまたはワークステーションの IP アドレス

単一の処理（またはコマンド）が、コマンド内のパラメータごとに、複数回ログ記録される場合があります。たとえば、ユーザが **snmp community ipaddr** *ip_address subnet_mask community_name* というコマンドを入力したとします。その場合、ある行では、IP アドレスはログに記録されても、サブネット マスクとコミュニティ名はログに「E」と記録されることがあります。また、別の行では、サブネット マスクはログに記録されても、IP アドレスとコミュニティ名はログに「E」と記録されることがあります。図 5-13 の例の最初の行と 3 番目の行を参照してください。

図 5-13　CiscoSecure ACS の [TACACS+ Administration .csv] ページ



（注）　[Refresh] をクリックすると、いつでもこのページを更新できます。

最大ローカル データベース エントリの設定

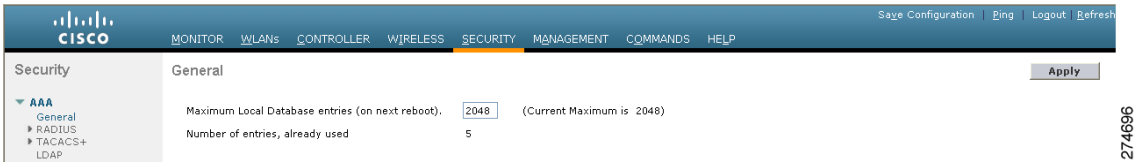
コントローラの GUI または CLI を使用して、ユーザ認証情報を格納するために使用するローカル データベース エントリの最大数を指定できます。データベース エントリには、ローカル管理ユーザ（ロビー アンバサダーを含む）、ローカル ネットワーク ユーザ（ゲスト ユーザを含む）、MAC フィルタ エントリ、除外リスト エントリ、およびアクセス ポイント認可リスト エントリが含まれます。これらを合わせて、設定されている最大値を超えることはできません。

GUI を使用した最大ローカル データベース エントリの設定

コントローラの GUI を使用して、ローカル データベース エントリの最大数を設定する手順は、次のとおりです。

ステップ 1　[Security] > [AAA] > [General] の順に選択して、[General] ページを開きます（図 5-14 を参照）。

図 5-14　[General] ページ



ステップ 2　[Maximum Local Database Entries] フィールドに、次回コントローラがリブートした際にローカル データベースに追加できる最大エントリ数を入力します。現在設定されている値が、フィールドの右側のカッコ内に表示されます。有効な範囲は 512 ～ 2048 で、デフォルトの設定は 2048 です。

[Number of Entries, Already Used] フィールドには、データベースに現存するエントリ数が表示されます。

ステップ 3　[Apply] をクリックして、変更を適用します。

ステップ 4　[Save Configuration] をクリックして、設定を保存します。

CLI を使用した最大ローカル データベース エントリの設定

ローカル データベース エントリの最大を設定するには、コントローラ CLI を使用して次の手順を実行します。

ステップ 1　次回コントローラがリブートした際にローカル データベースに追加できる最大エントリ数を指定するには、次のコマンドを入力します。

config database size *max_entries*

ステップ 2　変更を保存するには、次のコマンドを入力します。

save config

ステップ 3　データベース エントリの最大数およびデータベースの現在の内容を表示するには、次のコマンドを入力します。

show database summary

次のような情報が表示されます。

```
Maximum Database Entries..................... 2048
Maximum Database Entries On Next Reboot...... 2048
Database Contents
    MAC Filter Entries....................... 2
    Exclusion List Entries................... 0
    AP Authorization List Entries............ 1
    Management Users......................... 1
    Local Network Users...................... 1
        Local Users.......................... 1
        Guest Users.......................... 0
```

```
Total.................................... 5
```

ローカル ネットワーク ユーザの設定

この項では、コントローラ上のローカル ユーザ データベースにローカル ネットワーク ユーザを追加する方法について説明します。ローカル ユーザ データベースには、すべてのローカル ネットワーク ユーザの資格情報（ユーザ名とパスワード）が保存されます。これらの資格情報は、ユーザの認証に使用されます。たとえば、ローカル EAP では、ユーザの資格情報を取得するのに、バックエンド データベースとしてローカル ユーザ データベースを使用する場合があります。詳細は、「ローカル EAP の設定」（P.5-40）を参照してください。

（注） コントローラはクライアント情報をまず RADIUS 認証サーバに渡します。クライアント情報が RADIUS データベースのエントリに一致しない場合は、ローカル ユーザ データベースがポーリングされます。RADIUS 認証が失敗した場合、または存在しない場合は、このデータベースで見つかったクライアントがネットワーク サービスへのアクセスを付与されます。

ローカル ネットワーク ユーザは、GUI または CLI のいずれかを使用して設定できます。

GUI を使用したローカル ネットワーク ユーザの設定

コントローラ GUI を使用してローカル ネットワーク ユーザを設定する手順は、次のとおりです。

ステップ 1　[Security] > [AAA] > [Local Net Users] の順に選択して、[Local Net Users] ページを開きます（図 5-15 を参照）。

図 5-15　[Local Net Users] ページ

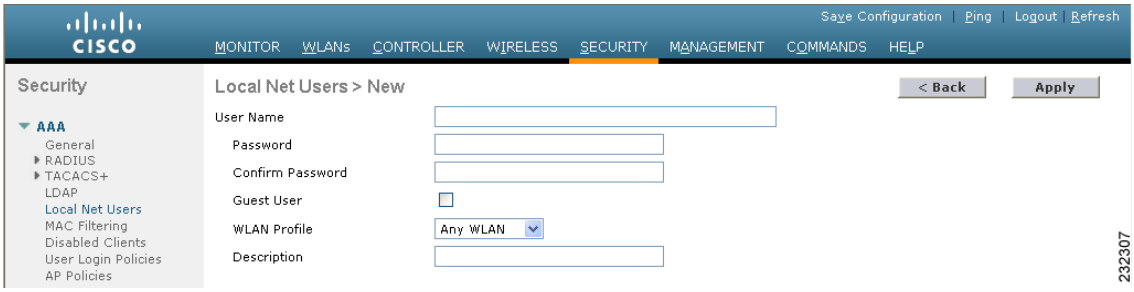
このページでは、これまでに設定されたすべてのローカル ネットワーク ユーザが表示されます。すべてのゲスト ユーザと、ゲスト ユーザに割り当てられている QoS ロール（該当する場合）も指定されます。QoS ロールの設定の詳細は、「Quality of Service ロールの設定」（P.4-70）を参照してください。

（注） 既存のユーザを削除するには、そのユーザの青いドロップダウンの矢印の上にカーソルを置いて、[Remove] を選択します。

ステップ 2　次のいずれかの操作を行います。

- 既存のローカル ネットワーク ユーザを編集するには、そのユーザのユーザ名をクリックします。[Local Net Users > Edit] ページが表示されます。
- ローカル ネットワーク ユーザを追加するには、[New] をクリックします。[Local Net Users > New] ページが表示されます（図 5-16 を参照）。

図 5-16　[Local Net Users > New] ページ



ステップ 3　新しいユーザを追加する場合は、[User Name] フィールドに、そのローカル ユーザのユーザ名を入力します。最大 24 文字の英数字を入力できます。

（注）　ローカル ネットワーク ユーザ名は、すべて同じデータベース内に保存されるため、一意である必要があります。

ステップ 4　[Password] フィールドおよび [Confirm Password] フィールドに、ローカル ユーザのパスワードを入力します。最大 24 文字の英数字を入力できます。

ステップ 5　新しいユーザを追加する場合、そのユーザがローカル ネットワークにアクセスできる時間を制限するには、[Guest User] チェックボックスをオンにします。デフォルトの設定は、オフになっています。

ステップ 6　新しいユーザを追加し、[Guest User] チェックボックスをオンにした場合は、[Lifetime] フィールドに、ゲスト ユーザ アカウントをアクティブにする時間（秒単位）を入力します。有効な範囲は 60 ～ 2,592,000（30 日間）秒（両端の値を含む）で、デフォルトの設定は 86,400 秒です。

ステップ 7　[Guest User] チェックボックスをオンにして新しいユーザを追加するときに、このゲスト ユーザに QoS ロールを割り当てるには、[Guest User Role] チェックボックスをオンにします。デフォルトの設定は、オフになっています。

（注）　ゲスト ユーザに QoS ロールを割り当てない場合、このユーザの帯域幅コントラクトは、WLAN の QoS プロファイルで定義されます。

ステップ 8　[Guest User Role] チェックボックスをオンにして新しいユーザを追加する場合は、このゲスト ユーザに割り当てる QoS ロールを [Role] ドロップダウン ボックスから選択します。

（注）　新しい QoS ロールを作成する手順については、「Quality of Service ロールの設定」（P.4-70）を参照してください。

ステップ 9　[WLAN Profile] ドロップダウン ボックスから、ローカル ユーザによってアクセスされる WLAN の名前を選択します。デフォルトの設定である [Any WLAN] を選択すると、ユーザは設定済みのどの WLAN にもアクセスできるようになります。

ステップ 10　[Description] フィールドに、ローカル ユーザを説明するタイトル（「ユーザ」など）を入力します。

ステップ 11　[Apply] をクリックして、変更を適用します。

ステップ 12　[Save Configuration] をクリックして、変更を保存します。

CLI を使用したローカル ネットワーク ユーザの設定

コントローラ CLI を使用してローカル ネットワーク ユーザを設定するには、この項のコマンドを使用します。

（注）　CLI コマンドで使用されるパラメータの有効範囲およびデフォルト値については、「GUI を使用したローカル ネットワーク ユーザの設定」（P.5-32）を参照してください。

1. ローカル ネットワーク ユーザを設定するには、次のコマンドを使用します。
   - **config netuser add** *username password* **wlan** *wlan_id* **userType permanent description** *description*：コントローラ上のローカル ユーザ データベースに永久ユーザを追加します。
   - **config netuser add** *username password* {**wlan** | **guestlan**} {*wlan_id* | *guest_lan_id*} **userType guest lifetime** *seconds* **description** *description*：WLAN または有線ゲスト LAN 上のゲスト ユーザを、コントローラのローカル ユーザ データベースに追加します。

   （注）　永久ユーザまたはゲスト ユーザをコントローラからローカル ユーザ データベースに追加する代わりに、RADIUS サーバ上にユーザに対するエントリを作成して Web 認証が実行される WLAN に対して RADIUS 認証を有効にするよう選択できます。

   - **config netuser delete** *username*：コントローラ上のローカル ユーザ データベースからユーザを削除します。

   （注）　ローカル ネットワーク ユーザ名は、すべて同じデータベース内に保存されるため、一意である必要があります。

2. 次のコマンドを使用して、コントローラで設定されたローカル ネットワーク ユーザに関連する情報を表示します。
   - **show netuser detail** *username*：ローカル ユーザ データベース内の特定のユーザの設定を表示します。
   - **show netuser summary**：ローカル ユーザ データベース内のすべてのユーザの一覧を表示します。

   たとえば、**show netuser detail** *username* コマンドに対しては、次のような情報が表示されます。

```
User Name.............................. abc
WLAN Id................................ Any
Lifetime............................... Permanent
Description............................ test user
```

3. 変更を保存するには、次のコマンドを入力します。

   save config

LDAP の設定

この項では、Lightweight Directory Access Protocol（LDAP）サーバを、RADIUS データベースやローカル ユーザ データベースに類似したバックエンド データベースとして設定する方法について説明します。LDAP バックエンド データベースを使用すると、コントローラで、特定のユーザの資格情報（ユーザ名およびパスワード）を LDAP サーバから検索できるようになります。これらの資格情報は、ユーザの認証に使用されます。たとえば、ローカル EAP では、ユーザの資格情報を取得するのに、バックエンド データベースとして LDAP を使用する場合があります。詳細は、「ローカル EAP の設定」（P.5-40）を参照してください。

（注）　LDAP バックエンド データベースでは、ローカル EAP 方式として、EAP-TLS、EAP-FAST/GTC、および PEAPv1/GTC がサポートされます。LEAP、EAP-FAST/MSCHAPv2、および PEAPv0/MSCHAPv2 もサポートされていますが、平文のパスワードを返すように LDAP サーバが設定されている場合にのみサポートされます。たとえば、Microsoft Active Directory は、平文のパスワードを返さないため、サポートされません。平文のパスワードを返すように LDAP サーバを設定できない場合、LEAP、EAP-FAST/MSCHAPv2、および PEAPv0/MSCHAPv2 はサポートされません。

LDAP は、GUI または CLI のいずれかを使用して設定できます。

GUI を使用した LDAP の設定

コントローラ GUI を使用して LDAP を設定する手順は、次のとおりです。

ステップ 1　[Security] > [AAA] > [LDAP] の順に選択して、[LDAP Servers] ページを開きます（図 5-17 を参照）。

図 5-17　[LDAP Servers] ページ

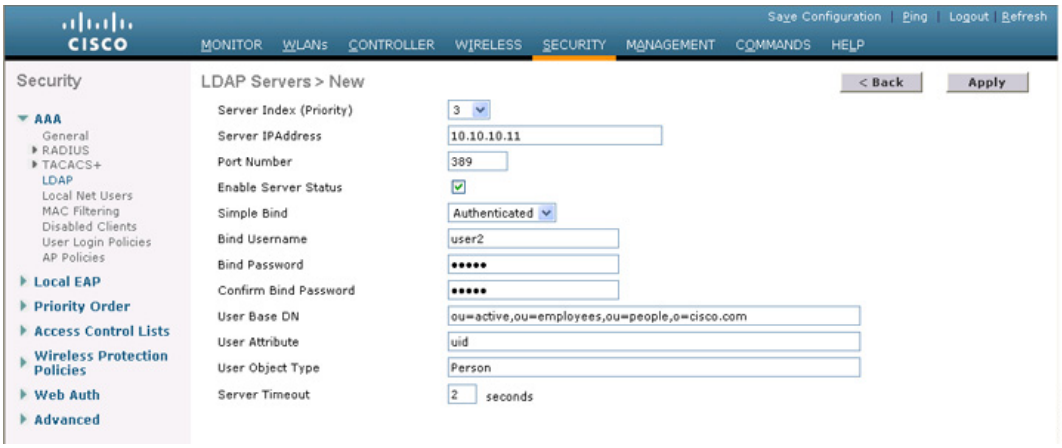
このページでは、これまでに設定されたすべての LDAP サーバが表示されます。

- 既存の LDAP サーバを削除するには、そのサーバの青いドロップダウンの矢印の上にカーソルを置いて、[Remove] を選択します。
- コントローラが特定のサーバに接続されるようにするには、そのサーバの青いドロップダウンの矢印の上にカーソルを置いて、[Ping] を選択します。

ステップ 2　次のいずれかの操作を行います。

- 既存の LDAP サーバを編集するには、そのサーバのインデックス番号をクリックします。[LDAP Servers > Edit] ページが表示されます。
- LDAP サーバを追加するには、[New] をクリックします。[LDAP Servers > New] ページが表示されます（図 5-18 を参照）。

図 5-18　[LDAP Servers >New] ページ



ステップ 3　新しいサーバを追加する場合は、[Server Index (Priority)] ドロップダウン ボックスから数字を選択し、その他の設定済みの LDAP サーバに対するこのサーバの優先順位を指定します。最大 17 台のサーバを設定できます。コントローラが最初のサーバに接続できない場合、リスト内の 2 番目のサーバへの接続を試行する、というようになります。

ステップ 4　新しいサーバを追加する場合は、[Server IP Address] フィールドに、LDAP サーバの IP アドレスを入力します。

ステップ 5　新しいサーバを追加する場合は、[Port Number] フィールドに、LDAP サーバの TCP ポート番号を入力します。有効な範囲は 1 ～ 65535 で、デフォルト値は 389 です。

ステップ 6　[Enable Server Status] チェックボックスをオンにしてこの LDAP サーバを有効にします。無効にする場合は、オフにします。デフォルト値は無効（disable）です。

ステップ 7　[Simple Bind] ドロップダウン ボックスから、[Anonymous] または [Authenticated] を選択して、LDAP サーバ用のローカル認証バインド方式を指定します。[Anonymous] 方式では、LDAP サーバへの匿名アクセスが可能です。しかし、[Authenticated] 方式では、ユーザ名とパスワードを入力してアクセスをセキュリティで保護する必要があります。デフォルトでは [Anonymous] になっています。

ステップ 8　ステップ 7 で [Authenticated] を選択した場合は、次の手順に従ってください。

a. [Bind Username] フィールドに、LDAP サーバに対するローカル認証に使用されるユーザ名を入力します。ユーザ名には、最大 80 文字を使用できます。

（注）　ユーザ名が「cn=」（小文字）で始まる場合、コントローラは、完全な LDAP データベース パスがユーザ名に含まれているとみなし、ユーザベースの DN を付加しません。この指定により、認証済みのバインド ユーザをユーザ ベース DN の外に置くことができます。

b. [Bind Password] フィールドおよび [Confirm Bind Password] フィールドには、LDAP サーバに対するローカル認証で使用されるパスワードを入力します。パスワードには、最大 32 文字を使用できます。

ステップ 9　[User Base DN] フィールドに、すべてのユーザの一覧を含む LDAP サーバ内のサブツリーの Distinguished Name（DN; 識別名）を入力します。たとえば、ou=organizational unit、.ou=next organizational unit、o=corporation.com のようになります。ユーザを含むツリーがベース DN である場合、**o=***corporation***.com** または **dc=***corporation***,dc=com** と入力します。

ステップ 10　[User Attribute] フィールドに、ユーザ名を含むユーザ レコード内の属性の名前を入力します。この属性はディレクトリ サーバから取得できます。

ステップ 11　[User Object Type] フィールドに、レコードをユーザとして識別する LDAP objectType 属性の値を入力します。多くの場合、ユーザ レコードには複数の objectType 属性の値が含まれています。そのユーザに一意の値と、他のオブジェクト タイプと共有する値があります。

ステップ 12　[Server Timeout] フィールドに、再送信の間隔（秒数）入力します。有効な範囲は 2 ～ 30 秒で、デフォルト値は 2 秒です。

ステップ 13　[Apply] をクリックして、変更を適用します。

ステップ 14　[Save Configuration] をクリックして、変更を保存します。

ステップ 15　LDAP をローカル EAP 認証のための優先バックエンド データベース サーバとして指定する手順は、次のとおりです。

a.　[Security] > [Local EAP] > [Authentication Priority] の順に選択して、[Priority Order > Local-Auth] ページを開きます（図 5-19 を参照）。

図 5-19　[Priority Order > Local-Auth] ページ

b.　[LOCAL] を強調表示して、[<] をクリックし、それを左の [User Credentials] ボックスに移動します。

c.　[LDAP] を強調表示して、[>] をクリックし、それを右の [User Credentials] ボックスに移動します。右側の [User Credentials] ボックスの上部に表示されるデータベースは、ユーザの資格情報を取得する際に使用されます。

（注）　[LDAP] と [LOCAL] の両方が右側の [User Credentials] ボックスに表示され、[LDAP] が上部で [LOCAL] が下部にある場合、ローカル EAP は LDAP バックエンド データベースを使用してクライアントの認証を試行し、LDAP サーバが接続不能である場合は、ローカル ユーザ データベースにフェールオーバーします。ユーザが見つからない場合、認証の試行は拒否されます。[LOCAL] が上部にある場合、ローカル EAP はローカル ユーザ データベースのみを使用して認証を試行します。LDAP バックエンド データベースへのフェールオーバーは行われません。

d.　[Apply] をクリックして、変更を適用します。

e.　[Save Configuration] をクリックして、変更を保存します。

ステップ 16　（オプション）特定の LDAP サーバを WLAN に割り当てる手順は、次のとおりです。

a.　[WLANs] を選択して、[WLANs] ページを開きます。

b.　必要な WLAN の ID 番号をクリックします。

c.　[WLANs > Edit] ページが表示されたら、[Security] > [AAA Servers] タブを選択し、[WLANs > Edit]（[Security] > [AAA Servers]）ページを開きます（図 5-20 を参照）。

図 5-20　[WLANs > Edit]（[Security] > [AAA Servers]）ページ

d. [LDAP Servers] ドロップダウン ボックスから、この WLAN に使用する LDAP サーバを選択します。最大 3 台の LDAP サーバを選択できます。これらのサーバは優先順位に従って試行されます。

（注）　これらの LDAP サーバは、Web 認証が有効になっている WLAN にのみ適用されます。ローカル EAP によって使用されません。

e. [Apply] をクリックして、変更を適用します。

f. [Save Configuration] をクリックして、変更を保存します。

CLI を使用した LDAP の設定

コントローラ CLI を使用して LDAP を設定するには、この項のコマンドを使用します。

（注）　CLI コマンドで使用されるパラメータの有効範囲およびデフォルト値については、「GUI を使用した LDAP の設定」（P.5-35）を参照してください。

1. LDAP サーバを設定するには、次のコマンドを使用します。
   - **config ldap add** *index server_ip_address port# user_base user_attr user_type* : LDAP サーバを追加します。
   - **config ldap delete** *index* : 以前に追加された LDAP サーバを削除します。
   - **config ldap** {**enable** | **disable**} *index* : LDAP サーバを有効または無効にします。
   - **config ldap simple-bind** {**anonymous** ***index*** | **authenticated** ***index*** **username** ***username*** **password** ***password***} : LDAP サーバ用のローカル認証バインド方式を指定します。匿名方式では LDAP サーバへの匿名アクセスが可能です。一方、認可方式ではユーザ名とパスワードを入力してアクセスをセキュリティで保護する必要があります。デフォルトでは匿名になっています。

（注）　ユーザ名には、最大 80 文字を使用できます。

（注）　ユーザ名が「cn=」（小文字）で始まる場合、コントローラは、完全な LDAP データベース パスがユーザ名に含まれているとみなし、ユーザベースの DN を付加しません。この指定により、認証済みのバインド ユーザをユーザ ベース DN の外に置くことができます。

- **config ldap retransmit-timeout** *index timeout*：LDAP サーバの再送信の間隔（秒数）を設定します。

2. 次のコマンドを使用すると、LDAP を優先バックエンド データベースとして指定できます。

   config local-auth user-credentials ldap

（注）　**config local-auth user-credentials ldap local** と入力すると、ローカル EAP は LDAP バックエンド データベースを使用してクライアントの認証を試行し、LDAP サーバが接続不能である場合は、ローカル ユーザ データベースにフェールオーバーします。ユーザが見つからない場合、認証の試行は拒否されます。**config local-auth user-credentials local ldap** と入力すると、ローカル EAP はローカル ユーザ データベースのみを使用して認証を試行します。LDAP バックエンド データベースへのフェールオーバーは行われません。

3. （オプション）特定の LDAP サーバを WLAN に割り当てるには、次のコマンドを使用します。

   - **config wlan ldap add** *wlan_id server_index*：設定済みの LDAP サーバを WLAN に接続します。

（注）　このコマンドで指定される LDAP サーバは、Web 認証が有効になっている WLAN にのみ適用されます。ローカル EAP によって使用されません。

   - **config wlan ldap delete** *wlan_id* **{all |** *index***}**：特定の、またはすべての設定済み LDAP サーバを WLAN から削除します。

4. 設定済みの LDAP サーバに関連する情報を表示するには、次のコマンドを使用します。

   - **show ldap summary**：設定済みの LDAP サーバの概要を表示します。
   - **show ldap** *index*：詳細な LDAP サーバ情報を表示します。
   - **show ldap statistics**：LDAP サーバの統計情報を表示します。
   - **show wlan** *wlan_id*：WLAN に適用される LDAP サーバを表示します。

   たとえば、**show ldap** *index* コマンドに対しては、次のような情報が表示されます。

```
Server Index.................................... 2
Address......................................... 10.10.20.22
Port............................................ 389
Enabled......................................... Yes
User DN......................................... ou=active,ou=employees,ou=people,
                                                 o=cisco.com
User Attribute.................................. uid
User Type....................................... Person
Retransmit Timeout.............................. 2 seconds
Bind Method .................................... Authenticated
Bind Username.................................. user1
```

show ldap summary コマンドに対しては、次のような情報が表示されます。

```
Idx  Server Address   Port  Enabled
---  ---------------  ----  -------
1    2.3.1.4          389  No
2    10.10.20.22     389   Yes
```

show ldap statistics コマンドに対しては、次のような情報が表示されます。

```
Server Index..................................... 1
Server statistics:
  Initialized OK................................. 0
  Initialization failed.......................... 0
  Initialization retries......................... 0
  Closed OK...................................... 0
Request statistics:
  Received....................................... 0
  Sent........................................... 0
  OK............................................. 0
  Success........................................ 0
  Authentication failed.......................... 0
  Server not found............................... 0
  No received attributes......................... 0
  No passed username............................. 0
  Not connected to server........................ 0
  Internal error................................. 0
  Retries........................................ 0

Server Index..................................... 2
...
```

5. コントローラが確実に LDAP サーバに接続できるようにするには、次のコマンドを入力します。

   ping *server_ip_address*

6. 変更を保存するには、次のコマンドを入力します。

   save config

7. LDAP のデバッグを有効または無効にするには、次のコマンドを入力します。

   debug aaa ldap {**enable** | **disable**}

ローカル EAP の設定

ローカル EAP は、ユーザおよび無線クライアントのローカル認証を可能にする認証方式です。この方式は、バックエンド システムが妨害されたり、外部認証サーバがダウンした場合でも、無線クライアントへの接続を維持できるように、リモート オフィスで使用する目的で設計されています。ローカル EAP を有効にすると、コントローラは認証サーバおよびローカル ユーザ データベースとして機能するため、外部認証サーバへの依存が排除されます。ローカル EAP は、ローカル ユーザ データベースまたは LDAP バックエンド データベースからユーザの資格情報を取得して、ユーザを認証します。ローカル EAP では、コントローラと無線クライアント間で、LEAP、EAP-FAST、EAP-TLS、PEAPv0/MSCHAPv2、および PEAPv1/GTC 認証方式をサポートします。

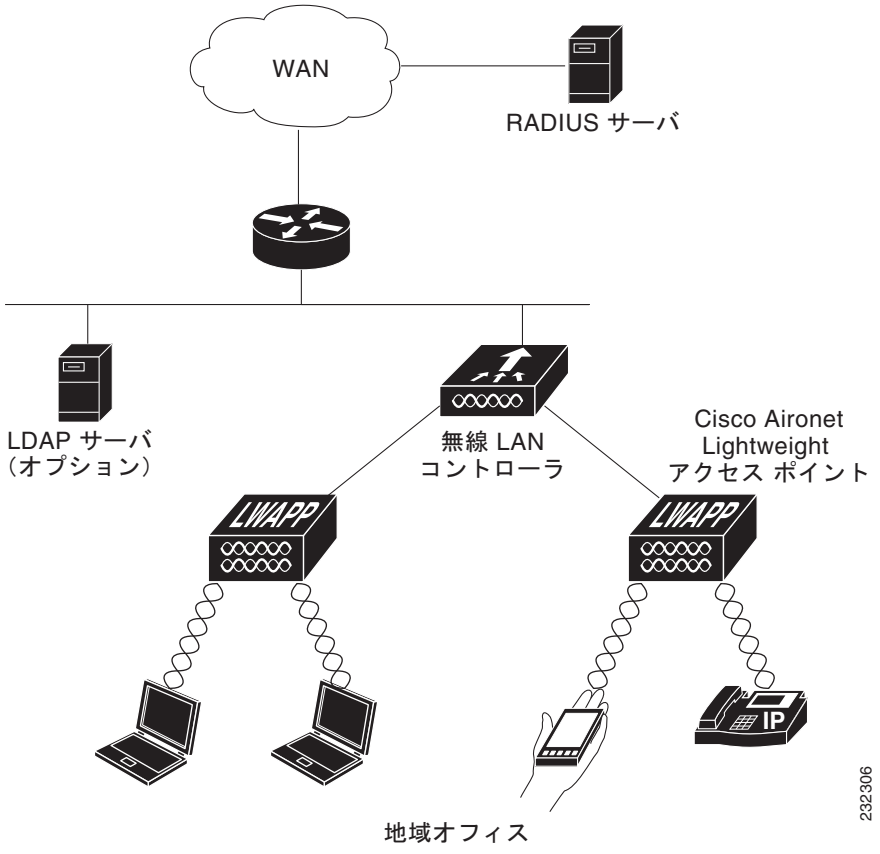
（注） LDAP バックエンド データベースでは、ローカル EAP 方式として、EAP-TLS、EAP-FAST/GTC、および PEAPv1/GTC がサポートされます。LEAP、EAP-FAST/MSCHAPv2、および PEAPv0/MSCHAPv2 もサポートされていますが、平文のパスワードを返すように LDAP サーバが設

定されている場合にのみサポートされます。たとえば、Microsoft Active Directory は、平文のパスワードを返さないため、サポートされません。平文のパスワードを返すように LDAP サーバを設定できない場合、LEAP、EAP-FAST/MSCHAPv2、および PEAPv0/MSCHAPv2 はサポートされません。

（注）　コントローラ上で RADIUS サーバが設定されている場合は、コントローラはまず RADIUS サーバを使用して無線クライアントを認証しようとします。ローカル EAP は、RADIUS サーバがタイムアウトしていたり、RADIUS サーバが設定されていない場合など、RADIUS サーバが見つからない場合にのみ試行されます。4 台の RADIUS サーバが設定されている場合、コントローラは最初の RADIUS サーバを使用してクライアントの認証を試行し、次に 2 番目の RADIUS サーバ、その次にローカル EAP を試行します。その後クライアントが手動で再認証を試みると、コントローラは 3 番目の RADIUS サーバを試行し、次に 4 番目の RADIUS サーバ、その次にローカル EAP を試行します。コントローラで外部 RADIUS サーバを使用してクライアントの認証を試行する場合は、次の CLI コマンドを次の順序で入力します。
config wlan disable *wlan_id*
config wlan radius_server auth disable *wlan_id*
config wlan enable *wlan_id*

図 5-21 は、ローカル EAP を使用したリモート オフィスの例を示しています。

図 5-21　ローカル EAP の例



ローカル EAP は、GUI または CLI のいずれかを使用して設定できます。

GUI を使用したローカル EAP の設定

コントローラの GUI を使用してローカル EAP を設定する手順は、次のとおりです。

ステップ 1　EAP-TLS、PEAPv0/MSCHAPv2、および PEAPv1/GTC は、認証に証明書を使用し、EAP-FAST は、証明書または PAC のいずれかを使用します。コントローラには、シスコによりインストールされたデバイスの証明書と、Certificate Authority（CA; 認証局）の証明書が同梱されています。ただし、お手持ちのベンダー固有の証明書を使用する場合は、それらの証明書をコントローラにインポートする必要があります。ローカル EAP でこれらのいずれかのタイプの EAP を使用するよう設定する場合は、適切な証明書と PAC（手動の PAC プロビジョニングを使用する場合）がコントローラにインポートされていることを確認してください。証明書と PAC のインポートの手順については、第 9 章を参照してください。

ステップ 2　コントローラでローカル ユーザ データベースからユーザの資格情報を取得するようにする場合は、そのコントローラ上でローカル ネットワーク ユーザを適切に設定していることを確認してください。手順については、「ローカル ネットワーク ユーザの設定」（P.5-32）を参照してください。

ステップ 3　コントローラで LDAP バックエンド データベースからユーザの資格情報を取得するようにする場合は、そのコントローラ上で LDAP サーバを適切に設定していることを確認してください。手順については、「LDAP の設定」（P.5-35）を参照してください。

ステップ 4　バックエンド データベース サーバからユーザの資格情報の取得順序を指定する手順は、次のとおりです。

a. [Security] > [Local EAP] > [Authentication Priority] の順に選択して、[Priority Order > Local-Auth] ページを開きます（図 5-22 を参照）。

図 5-22　[Priority Order > Local-Auth] ページ

b. ユーザの資格情報がローカルまたは LDAP データベースから取得される優先順位を決定します。たとえば、LDAP データベースがローカル ユーザ データベースよりも優先されるようにすることも、または LDAP データベースがまったく考慮されないようにすることもできます。

c. 優先順位を決定したら、目的のデータベースを強調表示します。次に、左と右の矢印および [Up] ボタンと [Down] ボタンを使用して、目的のデータベースを右側の [User Credentials] ボックスの上部に移動します。

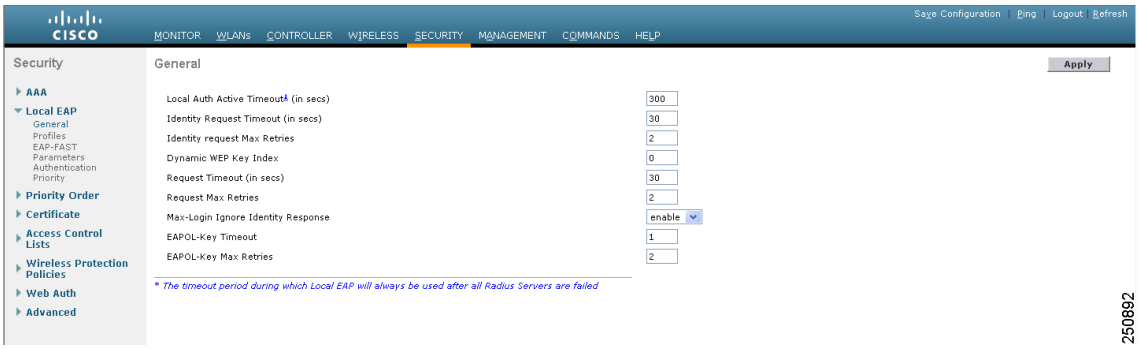
（注）　[LDAP] と [LOCAL] の両方が右側の [User Credentials] ボックスに表示され、[LDAP] が上部で [LOCAL] が下部にある場合、ローカル EAP は LDAP バックエンド データベースを使用してクライアントの認証を試行し、LDAP サーバが接続不能である場合は、ローカル ユーザ データベースにフェールオーバーします。ユーザが見つからない場合、認証の試行は拒否されます。[LOCAL] が上部にある場合、ローカル EAP はローカル ユーザ データベースのみを使用して認証を試行します。LDAP バックエンド データベースへのフェールオーバーは行われません。

d. [Apply] をクリックして、変更を適用します。

ステップ 5　ローカル EAP タイマーに値を指定する手順は、次のとおりです。

a. [Security] > [Local EAP] > [General] の順に選択して、[General] ページを開きます（図 5-23 を参照）。

図 5-23　[General] ページ



b. [Local Auth Active Timeout] フィールドに、設定済みの RADIUS サーバのペアによる認証が失敗したあとに、コントローラがローカル EAP を使用して無線クライアントを認証する際の試行時間（秒単位）を入力します。有効な範囲は 1 ～ 3600 秒で、デフォルトの設定は 100 秒です。

c. [Identity Request Timeout] フィールドに、コントローラがローカル EAP を使用して無線クライアントに EAP ID 要求を送信する際の試行時間（秒単位）を入力します。有効な範囲は 1 ～ 120 秒で、デフォルトの設定は 30 秒です。

d. [Identity Request Max Retries] フィールドに、コントローラがローカル EAP を使用して無線クライアントに EAP ID 要求を再送信する際の最大試行回数を入力します。有効な値の範囲は 1 ～ 20 回で、デフォルトの設定は 20 回です。

e. [Dynamic WEP Key Index] フィールドに、動的 Wired Equivalent Privacy（WEP）に使用するキーインデックスを入力します。デフォルトの設定は 0 です。

f. [Request Timeout] フィールドに、コントローラがローカル EAP を使用して無線クライアントに EAP 要求を送信する際の試行時間（秒単位）を入力します。有効な範囲は 1 ～ 120 秒で、デフォルトの設定は 30 秒です。

g. [Request Max Retries] フィールドに、コントローラがローカル EAP を使用して無線クライアントに EAP 要求を再送信する際の最大試行回数を入力します。有効な値の範囲は 1 ～ 120 回で、デフォルトの設定は 20 回です。

h. [Max-Login Ignore Identity Response] ドロップダウンボックスから、[Enable] を選択し、同じユーザ名を使用してコントローラに接続できるデバイスの数を制限できます。同じコントローラ上の異なるデバイス（PDA、ノートパソコン、IP 電話など）から最大 8 回ログインできます。デフォルト値は有効（enable）です。

i. [EAPOL-Key Timeout] フィールドで、コントローラがローカル EAP を使用して無線クライアントに LAN 経由で EAP キーを送信する際の試行時間（秒単位）を入力します。有効な値の範囲は 1 ～ 5 秒で、デフォルトの設定は 1 秒です。

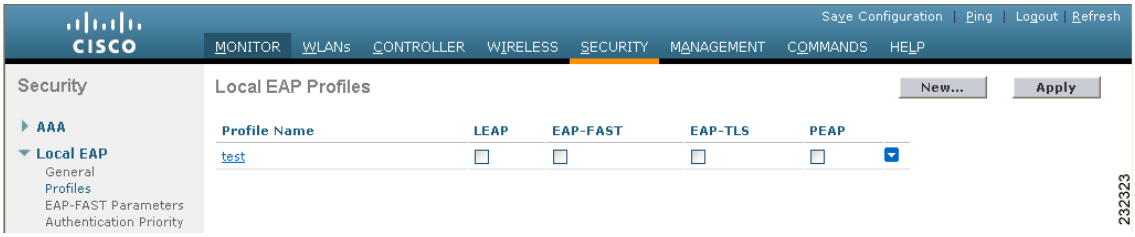
j. [EAPOL-Key Max Retries] フィールドで、コントローラがローカル EAP を使用して無線クライアントに LAN 経由で EAP キーを送信する際の最大試行回数を指定します。有効な値の範囲は 0 ～ 4 回で、デフォルトの設定は 2 回です。

k. [Apply] をクリックして、変更を適用します。

ステップ 6　無線クライアントでサポートされる EAP 認証タイプを指定する、ローカル EAP プロファイルを作成する手順は、次のとおりです。

a. [Security] > [Local EAP] > [Profiles] の順に選択して、[Local EAP Profiles] ページを開きます（図 5-24 を参照）。

図 5-24　[Local EAP Profiles] ページ



このページでは、これまでに設定されたすべてのローカル EAP プロファイルが表示され、その EAP タイプを指定します。最大 16 個のローカル EAP プロファイルを作成できます。

（注）　既存のプロファイルを削除するには、そのプロファイルの青いドロップダウンの矢印の上にカーソルを置いて、[Remove] を選択します。

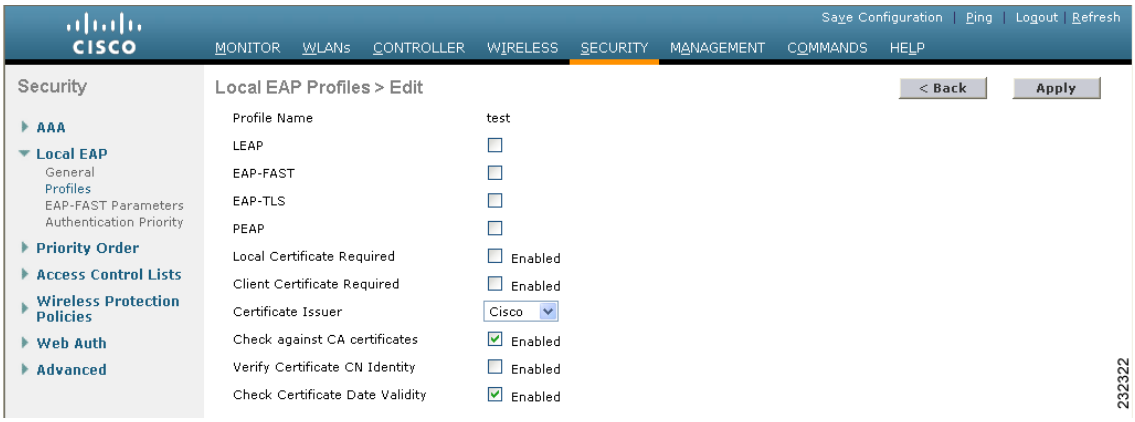
b. [New] をクリックして、[Local EAP Profiles > New] ページを開きます。

c. [Profile Name] フィールドに、新しいプロファイルの名前を入力し、[Apply] をクリックします。

（注）　プロファイル名には最大 63 文字の英数字を入力できます。スペースは含めないでください。

d. [Local EAP Profiles] ページが再度表示されたら、新しいプロファイルの名前をクリックします。[Local EAP Profiles > Edit] ページが表示されます（図 5-25 を参照）。

図 5-25　[Local EAP Profiles > Edit] ページ



e. [LEAP] チェックボックス、[EAP-FAST] チェックボックス、[EAP-TLS] チェックボックス、および/または [PEAP] チェックボックスをオンにし、ローカル認証に使用できる EAP タイプを指定します。

（注）　プロファイルごとに複数の EAP タイプを指定できます。ただし、証明書を使用する複数の EAP タイプ（証明書を使用する EAP-FAST、EAP-TLS、PEAPv0/MSCHAPv2、PEAPv1/GTC など）を選択する場合、すべての EAP タイプで同じ証明書（Cisco または他のベンダーが発行する）を使用する必要があります。

（注）　[PEAP] チェックボックスをオンにすると、コントローラ上で PEAPv0/MSCHAPv2 と PEAPv1/GTC の両方が有効になります。

f. EAP-FAST を選択し、コントローラ上のデバイスの証明書を認証に使用する場合は、[Local Certificate Required] チェックボックスをオンにします。証明書の代わりに PAC を使用する EAP-FAST を使用する場合は、このチェックボックスをオフのままにします。これがデフォルトの設定です。

（注）　デバイス証明書は LEAP と共に使用されず、EAP-TLS と PEAP には必須であるため、このオプションは EAP-FAST にのみ適用されます。

g. EAP-FAST を選択し、無線クライアントがデバイスの証明書を認証のためにコントローラに送信するようにするには、[Client Certificate Required] チェックボックスをオンにします。証明書の代わりに PAC を使用する EAP-FAST を使用する場合は、このチェックボックスをオフのままにします。これがデフォルトの設定です。

（注）　クライアント証明書は LEAP または PEAP と共に使用されず、EAP-TLS には必須であるため、このオプションは EAP-FAST にのみ適用されます。

h. 証明書を使用する EAP-FAST、EAP-TLS、または PEAP を選択する場合は、シスコが発行する証明書と別のベンダーが発行する証明書のどちらがクライアントに送信されるようにするかを選択します。[Cisco] または [Vendor] を [Certificate Issuer] ドロップダウン ボックスから選択してください。デフォルトの設定は、[Cisco] になっています。

i. 証明書を使用する EAP-FAST または EAP-TLS を選択し、クライアントから受信する証明書をコントローラ上の CA 証明書と照合して検証する場合は、[Check Against CA Certificates] チェックボックスをオンにします。デフォルトの設定は、有効になっています。

j. 証明書を使用する EAP-FAST または EAP-TLS を選択し、受信する証明書内の Common Name（CN; 通常名）をコントローラ上の CA 証明書の CN と照合して検証する場合は、[Verify Certificate CN Identity チェックボックスをオンにします。デフォルトの設定は、無効になっています。

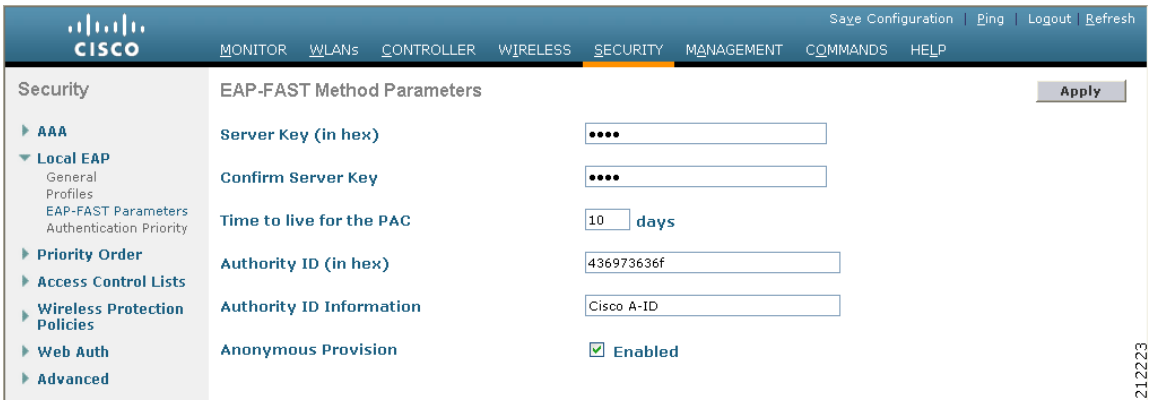
k. 証明書を使用する EAP-FAST または EAP-TLS を選択し、受信するデバイス証明書が現在有効で期限が切れていないことがコントローラで検証されるようにする場合は、[Check Certificate Date Validity] チェックボックスをオンにします。デフォルトの設定は、有効になっています。

l. [Apply] をクリックして、変更を適用します。

ステップ 7　EAP-FAST プロファイルを作成した場合、EAP-FAST パラメータを設定する手順は、次のとおりです。

a. [Security] > [Local EAP] > [EAP-FAST Parameters] の順に選択して、[EAP-FAST Method Parameters] ページを開きます（図 5-26 を参照）。

図 5-26　[EAP-FAST Method Parameters] ページ



b. [Server Key] フィールドおよび [Confirm Server Key] フィールドに、PAC の暗号化と暗号化解除に使用するキー（16 進数文字）を入力します。

c. [Time to Live for the PAC] フィールドに、PAC の有効日数を入力します。有効な範囲は 1 ～ 1000 日で、デフォルトの設定は 10 日です。

d. [Authority ID] フィールドに、ローカル EAP-FAST サーバの権限識別子を 16 進数文字で入力します。最大 32 文字の 16 進数文字を入力できますが、文字数は偶数である必要があります。

e. [Authority ID Information] フィールドに、ローカル EAP-FAST サーバの権限識別子をテキスト形式で入力します。

f. 匿名プロビジョニングを有効にするには、[Anonymous Provision] チェックボックスをオンにします。この機能を使用すると、PAC プロビジョニング中に、PAC がないクライアントに PAC が自動的に送信されるようになります。この機能を無効にする場合、PAC は手動でプロビジョニングされる必要があります。デフォルトの設定は、有効になっています。

（注）　ローカル証明書またはクライアント証明書、あるいはその両方が必要で、すべての EAP-FAST クライアントで証明書を使用するよう強制する場合は、[Anonymous Provision] チェックボックスをオフにしてください。

g. [Apply] をクリックして、変更を適用します。

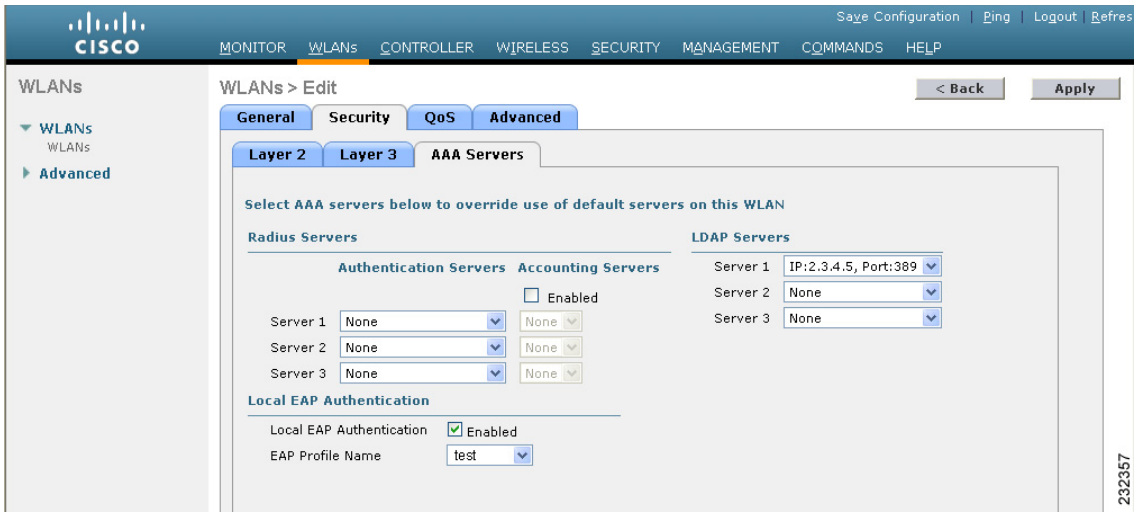
ステップ 8　WLAN 上でローカル EAP を有効にする手順は、次のとおりです。

a. [WLANs] を選択して、[WLANs] ページを開きます。

b. 必要な WLAN の ID 番号をクリックします。

c. [WLANs > Edit] ページが表示されたら、[Security] > [AAA Servers] タブを選択し、[WLANs > Edit]（[Security] > [AAA Servers]）ページを開きます（図 5-27 を参照）。

図 5-27　[WLANs > Edit]（[Security] > [AAA Servers]）ページ



d. [Local EAP Authentication] チェックボックスをオンにして、この WLAN に対してローカル EAP を有効にします。

e. [EAP Profile Name] ドロップダウン ボックスから、この WLAN に使用する EAP プロファイルを選択します。

f. 必要に応じて、[LDAP Servers] ドロップダウン ボックスから、この WLAN でローカル EAP と共に使用する LDAP サーバを選択します。

g. [Apply] をクリックして、変更を適用します。

ステップ 9　[Save Configuration] をクリックして、変更を保存します。

CLI を使用したローカル EAP の設定

コントローラ CLI を使用してローカル EAP を設定する手順は、次のとおりです。

（注） CLI コマンドで使用されるパラメータの有効範囲およびデフォルト値については、「GUI を使用したローカル EAP の設定」（P.5-42）を参照してください。

ステップ 1　EAP-TLS、PEAPv0/MSCHAPv2、および PEAPv1/GTC は、認証に証明書を使用し、EAP-FAST は、証明書または PAC のいずれかを使用します。コントローラには、シスコによりインストールされたデバイスの証明書と、Certificate Authority（CA; 認証局）の証明書が付属しています。ただし、ご自身のベンダー固有の証明書を使用する場合は、それらの証明書をコントローラにインポートする必要があります。ローカル EAP でこれらのいずれかのタイプの EAP を使用するよう設定する場合は、適切な証明書と PAC（手動の PAC プロビジョニングを使用する場合）がコントローラにインポートされていることを確認してください。証明書と PAC のインポートの手順については、第 9 章を参照してください。

ステップ 2　コントローラでローカル ユーザ データベースからユーザの資格情報を取得するようにする場合は、そのコントローラ上でローカル ネットワーク ユーザを適切に設定していることを確認してください。手順については、「ローカル ネットワーク ユーザの設定」（P.5-32）を参照してください。

ステップ 3　コントローラで LDAP バックエンド データベースからユーザの資格情報を取得するようにする場合は、そのコントローラ上で LDAP サーバを適切に設定していることを確認してください。手順については、「LDAP の設定」（P.5-35）を参照してください。

ステップ 4　ユーザの資格情報がローカルまたは LDAP データベースから取得される優先順位を指定するには、次のコマンドを入力します。

config local-auth user-credentials {**local** | **ldap**}

（注）　**config local-auth user-credentials ldap local** と入力すると、ローカル EAP は LDAP バックエンド データベースを使用してクライアントの認証を試行し、LDAP サーバが接続不能である場合は、ローカル ユーザ データベースにフェールオーバーします。ユーザが見つからない場合、認証の試行は拒否されます。**config local-auth user-credentials local ldap** と入力すると、ローカル EAP はローカル ユーザ データベースのみを使用して認証を試行します。LDAP バックエンド データベースへのフェールオーバーは行われません。

ステップ 5　ローカル EAP タイマーに値を指定するには、次のコマンドを入力します。

- **config local-auth active-timeout** *timeout*：設定済みの RADIUS サーバのペアによる認証が失敗したあとに、コントローラがローカル EAP を使用して無線クライアントを認証する際の試行時間（秒単位）を指定します。有効な範囲は 1 ～ 3600 秒で、デフォルトの設定は 100 秒です。
- **config advanced eap identity-request-timeout** *timeout*：コントローラがローカル EAP を使用して無線クライアントに EAP ID 要求を送信する際の試行時間（秒単位）を指定します。有効な範囲は 1 ～ 120 秒で、デフォルトの設定は 30 秒です。
- **config advanced eap identity-request-retries** *retries*：コントローラがローカル EAP を使用して無線クライアントに EAP ID 要求を再送信する際の最大試行回数を指定します。有効な値の範囲は 1 ～ 20 回で、デフォルトの設定は 20 回です。
- **config advanced eap key-index** *index*：動的 Wired Equivalent Privacy（WEP）に使用するキー インデックスを指定します。デフォルトの設定は 0 です。
- **config advanced eap request-timeout** *timeout*：コントローラがローカル EAP を使用して無線クライアントに EAP 要求を送信する際の試行時間（秒単位）を指定します。有効な範囲は 1 ～ 120 秒で、デフォルトの設定は 30 秒です。
- **config advanced eap request-retries** *retries*：コントローラがローカル EAP を使用して無線クライアントに EAP 要求を再送信する際の最大試行回数を指定します。有効な値の範囲は 1 ～ 120 回で、デフォルトの設定は 20 回です。
- **config advanced eap eapol-key-timeout** *timeout*：コントローラがローカル EAP を使用して無線クライアントに LAN 経由で EAP キーを送信する際の試行時間（秒単位）を指定します。有効な値の範囲は 1 ～ 5 秒で、デフォルトの設定は 1 秒です。
- **config advanced eap eapol-key-retries** *retries*：コントローラがローカル EAP を使用して無線クライアントに LAN 経由で EAP キーを送信する際の最大試行回数を指定します。有効な値の範囲は 0 ～ 4 回で、デフォルトの設定は 2 回です。
- **config advanced eap max-login-ignore-identity-response** {**enable** | **disable**}：このコマンドを有効にすると、同じユーザ名を使用してコントローラに接続できるデバイスの数を制限できます。同じコントローラ上の異なるデバイス（PDA、ノートパソコン、IP 電話など）から最大 8 回ログインできます。デフォルト値は有効（enable）です。

ステップ 6　ローカル EAP プロファイルを作成するには、次のコマンドを入力します。

config local-auth eap-profile add *profile_name*

（注）　プロファイル名にスペースを含めないでください。

（注）　ローカル EAP プロファイルを削除するには、**config local-auth eap-profile delete** *profile_name* コマンドを入力します。

ステップ 7　ローカル EAP プロファイルに EAP 方式を追加するには、次のコマンドを入力します。

config local-auth eap-profile method add *method profile_name*

サポートされる方式は、leap、fast、tls、および peap です。

（注）　peap を選択する場合、コントローラ上で PEAPv0/MSCHAPv2 と PEAPv1/GTC の両方が有効になります。

（注）　プロファイルごとに複数の EAP タイプを指定できます。ただし、証明書を使用する複数の EAP タイプ（証明書を使用する EAP-FAST、EAP-TLS、PEAPv0/MSCHAPv2、および PEAPv1/GTC など）でプロファイルを作成する場合、すべての EAP タイプで同じ証明書（Cisco または他のベンダーが発行する）を使用する必要があります。

（注）　ローカル EAP プロファイルから EAP 方式を削除するには、**config local-auth eap-profile method delete** *method profile_name* コマンドを入力します。

ステップ 8　EAP-FAST プロファイルを作成した場合に、EAP-FAST パラメータを設定するには、次のコマンドを入力します。

config local-auth method fast *?*

ここで、*?* は、次のいずれかを示します。

- **anon-prov** {**enable** | **disable**}：コントローラで匿名プロビジョニングが許可されるように設定します。これにより、PAC プロビジョニング中に、PAC がないクライアントに PAC が自動的に送信されるようになります。
- **authority-id** *auth_id*：ローカル EAP-FAST サーバの権限識別子を指定します。
- **pac-ttl** *days*：PAC の有効日数を指定します。
- **server-key** *key*：PAC を暗号化および暗号化解除するために使用されるサーバ キーを指定します。

ステップ 9　プロファイルごとに証明書パラメータを設定するには、次のコマンドを入力します。

- **config local-auth eap-profile method fast local-cert** {**enable** | **disable**} *profile_name*：コントローラ上のデバイスの証明書が認証に必要とされるかどうかを指定します。

  （注）　デバイス証明書は LEAP と共に使用されず、EAP-TLS と PEAP には必須であるため、このコマンドは EAP-FAST にのみ適用されます。

- **config local-auth eap-profile method fast client-cert** {**enable** | **disable**} *profile_name*：無線クライアントから認証のためのデバイスの証明書をコントローラに送信する必要があるかどうかを指定します。

（注）　クライアント証明書は LEAP または PEAP と共に使用されず、EAP-TLS には必須であるため、このコマンドは EAP-FAST にのみ適用されます。

- **config local-auth eap-profile cert-issuer {cisco | vendor}** *profile_name*：証明書を使用する EAP-FAST、EAP-TLS、または PEAP を指定した場合は、クライアントに送信される証明書がシスコから発行されるものか、別のベンダーから発行されるものかを指定します。
- **config local-auth eap-profile cert-verify ca-issuer** {**enable** | **disable**} *profile_name*：証明書を使用する EAP-FAST または EAP-TLS を選択する場合は、クライアントから受信する証明書をコントローラ上の CA 証明書と照合して検証するかどうかを指定します。
- **config local-auth eap-profile cert-verify cn-verify** {**enable** | **disable**} *profile_name*：証明書を使用する EAP-FAST または EAP-TLS を選択する場合は、受信する証明書内の通常名（CN）をコントローラ上の CA 証明書の CN と照合して検証するかどうかを指定します。
- **config local-auth eap-profile cert-verify date-valid** {**enable** | **disable**} *profile_name*：証明書を使用する EAP-FAST または EAP-TLS を選択する場合は、受信するデバイスの証明書が現在も有効であり期限が切れていないことがコントローラで検証されるようにするかどうかを指定します。

ステップ 10　ローカル EAP を有効にし、EAP プロファイルを WLAN に接続するには、次のコマンドを入力します。

config wlan local-auth enable *profile_name wlan_id*

（注）　WLAN でローカル EAP を無効にするには、**config wlan local-auth disable** *wlan_id* コマンドを入力します。

ステップ 11　変更を保存するには、次のコマンドを入力します。

save config

ステップ 12　ローカル EAP に関連する情報を表示するには、次のコマンドを使用します。

- **show local-auth config**：コントローラ上のローカル EAP の設定を表示します。

  show local-auth config コマンドに対しては、次のような情報が表示されます。

```
User credentials database search order:
   Primary ..................................... Local DB

Timer:
    Active timeout ............................. 300

Configured EAP profiles:
   Name ........................................ fast-cert
     Certificate issuer ........................ vendor
     Peer verification options:
       Check against CA certificates ........... Enabled
       Verify certificate CN identity .......... Disabled
       Check certificate date validity ......... Enabled
     EAP-FAST configuration:
       Local certificate required .............. Yes
       Client certificate required ............. Yes
     Enabled methods ........................... fast
     Configured on WLANs ....................... 1

   Name ........................................ tls
     Certificate issuer ........................ vendor
     Peer verification options:
       Check against CA certificates ........... Enabled
       Verify certificate CN identity .......... Disabled
```

```
        Check certificate date validity ......... Enabled
      EAP-FAST configuration:
        Local certificate required .............. No
        Client certificate required ............. No
      Enabled methods ........................... tls
      Configured on WLANs ....................... 2

EAP Method configuration:
   EAP-FAST:
     Server key ................................ <hidden>
     TTL for the PAC ........................... 10
     Anonymous provision allowed ............... Yes
     Accept client on auth prov ................ No
     Authority ID .............................. 436973636f00000000000000000000000000
     Authority Information ..................... Cisco A-ID
```

- **show local-auth statistics**：ローカル EAP の統計情報を表示します。
- **show local-auth certificates**：ローカル EAP で使用可能な証明書を表示します。
- **show local-auth user-credentials**：コントローラがローカル データベースまたは LDAP データベースからユーザの資格情報を取得する際の優先順位を表示します。
- **show advanced eap**：ローカル EAP のタイマーの値を表示します。次のような情報が表示されます。

```
EAP-Identity-Request Timeout (seconds)..... 1
EAP-Identity-Request Max Retries........... 20
EAP Key-Index for Dynamic WEP.............. 0
EAP Max-Login Ignore Identity Response..... enable
EAP-Request Timeout (seconds).............. 20
EAP-Request Max Retries.................... 20
EAPOL-Key Timeout (seconds)................ 1
EAPOL-Key Max Retries...................... 2
```

- **show ap stats wlan *Cisco_AP***：各 WLAN の特定のアクセス ポイントにおける EAP タイムアウト回数および失敗回数を表示します。次のような情報が表示されます。

```
WLAN      1
   EAP Id Request Msg Timeouts................ 0
   EAP Id Request Msg Timeouts Failures....... 0
   EAP Request Msg Timeouts................... 2
   EAP Request Msg Timeouts Failures.......... 1
   EAP Key Msg Timeouts....................... 0
   EAP Key Msg Timeouts Failures.............. 0
WLAN      2
   EAP Id Request Msg Timeouts................ 1
   EAP Id Request Msg Timeouts Failures....... 0
   EAP Request Msg Timeouts................... 0
   EAP Request Msg Timeouts Failures.......... 0
   EAP Key Msg Timeouts....................... 3
   EAP Key Msg Timeouts Failures.............. 1
```

- **show client detail *client_mac***：アソシエートされた特定のクライアントについて、EAP タイムアウト回数および失敗回数を表示します。これらの統計は、クライアント アソシエーションの問題のトラブルシューティングを行う際に有用です。次のような情報が表示されます。

```
...
Client Statistics:
      Number of Bytes Received.................. 10
      Number of Bytes Sent...................... 10
      Number of Packets Received................ 2
      Number of Packets Sent.................... 2
      Number of EAP Id Request Msg Timeouts..... 0
```

```
        Number of EAP Id Request Msg Failures...... 0
        Number of EAP Request Msg Timeouts......... 2
        Number of EAP Request Msg Failures......... 1
        Number of EAP Key Msg Timeouts............. 0
        Number of EAP Key Msg Failures............. 0
        Number of Policy Errors.................... 0
        Radio Signal Strength Indicator............ Unavailable
        Signal to Noise Ratio...................... Unavailable
...
```

- **show wlan** *wlan_id*：特定の WLAN のローカル EAP のステータスを表示します。

ステップ 13　必要に応じて、次のコマンドを使用してローカル EAP セッションのトラブルシューティングを行います。

- **debug aaa local-auth eap method** {**all** | **errors** | **events** | **packets** | **sm**} {**enable** | **disable**}：ローカル EAP 方式のデバッグを有効または無効にします。
- **debug aaa local-auth eap framework** {**all** | **errors** | **events** | **packets** | **sm**} {**enable** | **disable**}：ローカル EAP フレームワークのデバッグを有効または無効にします。

（注）　上記の 2 つのコマンドでは、**sm** とはステート マシンを指します。

- **clear stats local-auth**：ローカル EAP のカウンタをクリアします。
- **clear stats ap wlan** *Cisco_AP*：各 WLAN の特定のアクセスポイントにおける EAP タイムアウト回数および失敗回数をクリアします。

SpectraLink 社の NetLink 電話用システムの設定

SpectraLink 社の NetLink 電話を Cisco UWN Solution と最適な形で統合するためには、長いプリアンブルを使用できるようにオペレーティング システムを設定する必要があります。無線プリアンブル（ヘッダーとも呼ばれる）とは、パケットの先頭部分のデータ セクションのことであり、ここには、無線デバイスでのパケットの送受信に必要な情報が格納されています。短いプリアンブルの方がスループット パフォーマンスが向上するため、デフォルトではこちらが有効になっています。ただし、SpectraLink 社の NetLink 電話などの一部の無線デバイスでは、長いプリアンブルを使用する必要があります。

長いプリアンブルを有効にするには、次のいずれかの方法を使用します。

- 「GUI を使用した 長いプリアンブルの有効化」（P.5-52）
- 「CLI を使用した 長いプリアンブルの有効化」（P.5-53）

GUI を使用した 長いプリアンブルの有効化

GUI を使用して長いプリアンブルを有効化し、無線 LAN 上にある SpectraLink 社の NetLink 電話の動作を最適化する手順は次のとおりです。

ステップ 1　[Wireless] > [802.11b/g/n] > [Network] の順に選択して、[802.11b/g Global Parameters] ページを開きます。

ステップ 2　[Short Preamble] チェックボックスがオンの場合は、これ以降の手順に進みます。[Short Preamble] チェックボックスがオフの場合（つまり長いプリアンブルが有効な場合）、コントローラはすでに SpectraLink 社の NetLink 電話用に最適化されているため、これ以降の手順を実行する必要はありません。

ステップ 3　[Short Preamble] チェックボックスをオフにして、長いプリアンブルを有効にします。

ステップ 4　[Apply] をクリックして、コントローラの設定を更新します。

（注）　コントローラへの CLI セッションがアクティブでない場合は、CLI セッションを開始してコントローラをリブートし、リブート プロセスを監視することをお勧めします。コントローラがリブートすると GUI が切断されるため、その意味でも CLI セッションは役に立ちます。

ステップ 5　[Commands] > [Reboot] > [Reboot] > [Save and Reboot] の順に選択して、コントローラをリブートします。次のプロンプトに対し [OK] をクリックします。

```
Configuration will be saved and the controller will be rebooted. Click ok to confirm.
```

コントローラがリブートします。

ステップ 6　コントローラの GUI にもう一度ログインし、コントローラが正しく設定されていることを確認します。

ステップ 7　[Wireless] > [802.11b/g/n] > [Network] の順に選択して、[802.11b/g Global Parameters] ページを開きます。[Short Preamble] チェックボックスがオフの場合、コントローラは SpectraLink 社の NetLink 電話用に最適化されています。

CLI を使用した 長いプリアンブルの有効化

CLI を使用して長いプリアンブルを有効化し、無線 LAN 上にある SpectraLink 社の NetLink 電話の動作を最適化する手順は次のとおりです。

ステップ 1　コントローラの CLI にログインします。

ステップ 2　**show 802.11b** と入力して Short preamble mandatory パラメータをチェックします。短いプリアンブルが有効になっている場合は、以降の手順に進みます。短いプリアンブルが有効な場合、次のように表示されます。

```
Short Preamble mandatory..................... Enabled
```

短いプリアンブルが無効になっている場合（つまり長いプリアンブルが有効な場合）、コントローラはすでに SpectraLink 社の NetLink 電話に対して最適化されているため、以降の手順を実行する必要はありません。長いプリアンブルが有効な場合、次のように表示されます。

```
Short Preamble mandatory..................... Disabled
```

ステップ 3　**config 802.11b disable network** と入力して 802.11b/g ネットワークを無効にします （802.11a ネットワーク上では、長いプリアンブルを有効化できません）。

ステップ 4　**config 802.11b preamble long** と入力して長いプリアンブルを有効にします。

ステップ 5　**config 802.11b enable network** と入力して 802.11b/g ネットワークを再度有効にします。

ステップ 6　**reset system** と入力して、コントローラをリブートします。次のプロンプトに対して **y** と入力します。

```
The system has unsaved changes. Would you like to save them now? (y/n)
```

コントローラがリブートします。

ステップ 7　もう一度 CLI にログインし、**show 802.11b** と入力して次のパラメータを表示し、コントローラが正しく設定されていることを確認します。

```
802.11b Network.............................. Enabled
Short Preamble mandatory..................... Disabled
```

上記のパラメータは、802.11b/g ネットワークが有効になっていて、短いプリアンブルが無効になっていることを示しています。

CLI を使用した Enhanced Distributed Channel Access の設定

次の CLI コマンドを使用すると、802.11 Enhanced Distributed Channel Access（EDCA; 拡張型分散チャネル アクセス）パラメータを設定して SpectraLink の電話をサポートできます。

config advanced edca-parameters {**svp-voice** | **wmm-default**}

svp-voice は SpectraLink Voice Priority（SVP）パラメータを有効にし、**wmm-default** は Wireless Multimedia（WMM）デフォルト パラメータを有効にします。

（注）　このコマンドをコントローラに接続されたすべてのアクセス ポイントに適用するには、このコマンドを入力した後、802.11b/g ネットワークを無効にし、その後再び有効にしてください。

無線による管理機能の使用

無線による管理機能を使用すると、オペレータは、無線クライアントを使用してローカル コントローラを監視および設定できます。この機能は、コントローラとの間のアップロードおよびダウンロード（転送）以外のすべての管理タスクに対して使用できます。

無線による管理機能を使用するには、次のいずれかの方法でコントローラを適切に設定しておく必要があります。

- 「GUI を使用した無線による管理の有効化」（P.5-54）
- 「CLI を使用した無線による管理の有効化」（P.5-55）

GUI を使用した無線による管理の有効化

ステップ 1　[Management] > [Mgmt Via Wireless] の順に選択して、[Management Via Wireless] ページを開きます。

ステップ 2　[Enable Controller Management to be accessible from Wireless Clients] チェックボックスをオンにして無線による WLAN の管理を有効にするか、オフにしてこの機能を無効にします。デフォルトではオフになっています。

ステップ 3　[Apply] をクリックして、変更を適用します。

ステップ 4　[Save Configuration] をクリックして、変更を保存します。

ステップ 5　無線クライアント Web ブラウザを使用して、コントローラ管理ポートまたはディストリビューション システム ポート IP アドレスに接続し、コントローラ GUI にログインして、無線クライアントを使用して WLAN を管理できていることを確認します。

CLI を使用した無線による管理の有効化

ステップ 1　CLI で、**show network** コマンドを使用して、management over wireless interface が enabled に設定されているか disabled に設定されているかを確認します。management over wireless interface が disabled の場合は、ステップ 2 に進みます。それ以外の場合は、ステップ 3 に進みます。

ステップ 2　無線による管理を有効にするには、**config network mgmt-via-wireless enable** と入力します。

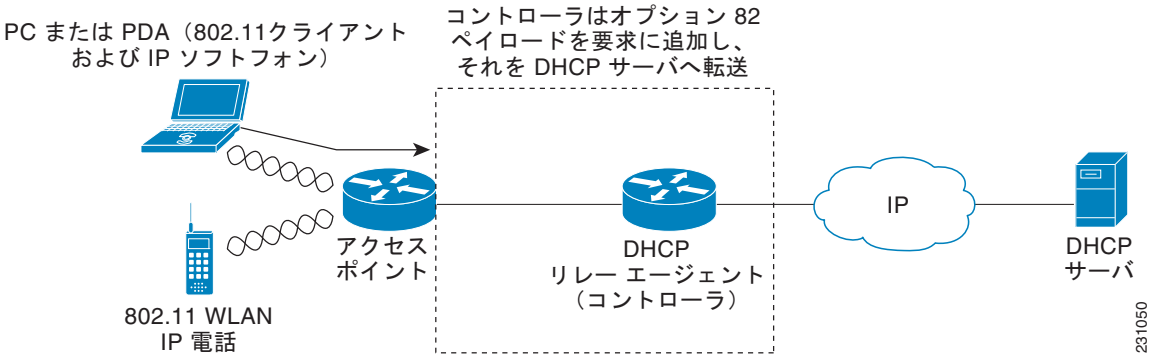
ステップ 3　無線クライアントを使用して、管理対象のコントローラに接続されているアクセス ポイントにアソシエートします。

ステップ 4　**telnet controller-ip-address** と入力して CLI にログインし、無線クライアントを使用して WLAN を管理できることを確認します。

DHCP オプション 82 の設定

DHCP オプション 82 では、DHCP を使用してネットワーク アドレスを割り当てる場合のセキュリティが強化されます。具体的には、コントローラが DHCP リレイ エージェントとして動作して、信頼できないソースからの DHCP クライアント要求を阻止できるようにします。DHCP 要求にオプション 82 情報を追加してから DHCP サーバに転送するように、コントローラを設定することができます。このプロセスを、図 5-28 に図示します。

図 5-28　DHCP オプション 82



アクセス ポイントは、クライアントからのすべての DHCP 要求をコントローラに転送します。コントローラは、DHCP オプション 82 ペイロードを追加してから要求を DHCP サーバに転送します。このオプションの設定方法によって、ペイロードには MAC アドレス、または MAC アドレスとアクセス ポイントの SSID が含まれます。コントローラ ソフトウェア リリース 4.0 以降では、コントローラ CLI を使用して DHCP オプション 82 を設定できます。コントローラ ソフトウェア リリース 6.0 では、GUI または CLI のいずれを使用しても、この機能を設定できます。

（注）　DHCP オプション 82 が正常に動作するためには、デフォルトで無効になっている DHCP プロキシを有効にする必要があります。DHCP プロキシを設定する方法については、「DHCP プロキシの設定」（P.4-41）を参照してください。

（注）　すでにリレー エージェント オプションが含まれている DHCP パケットは、コントローラでドロップされます。

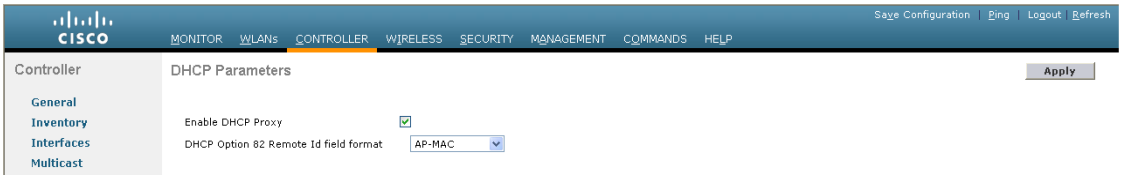
（注）　DHCP オプション 82 は、第 12 章で説明されている自動アンカー モビリティと共に使用することはできません。

GUI を使用した DHCP オプション 82 の設定

GUI を使用して DHCP オプション 82 をコントローラで設定する手順は、次のとおりです。

ステップ 1　[Controller] > [Advanced] > [DHCP] の順に選択して、[DHCP Parameters] ページを開きます（図 5-29 を参照）。

図 5-29　[DHCP Parameters] ページ



ステップ 2　[DHCP Option 82 Remote ID Field Format] ドロップダウン ボックスから次のオプションのいずれかを選択して、DHCP オプション 82 ペイロードの形式を指定します。

- [AP-MAC] : DHCP オプション 82 ペイロードにアクセス ポイントの MAC アドレスを追加します。これはデフォルト値です。
- [AP-MAC-SSID]:DHCP オプション 82 ペイロードにアクセス ポイントの MAC アドレスと SSID を追加します。

ステップ 3　[Apply] をクリックして、変更を適用します。

ステップ 4　[Save Configuration] をクリックして、変更を保存します。

CLI を使用した DHCP オプション 82 の設定

次の CLI コマンドを使用して DHCP オプション 82 をコントローラに設定できます。

1. DHCP オプション 82 ペイロードの形式を設定するには、次のコマンドの 1 つを入力します。
   - **config dhcp opt-82 remote-id** *ap_mac*

     このコマンドは DHCP オプション 82 ペイロードにアクセス ポイントの MAC アドレスを追加します。
   - **config dhcp opt-82 remote-id** *ap_mac*:*ssid*

     このコマンドは DHCP オプション 82 ペイロードにアクセス ポイントの MAC アドレスと SSID を追加します。

2. グローバル DHCP オプション 82 の設定を無効にし、コントローラの AP マネージャまたは管理インターフェイスに対してこの機能を無効（または有効）にするには、次のコマンドを入力します。

   config interface dhcp {**ap-manager** | **management**} **option-82** {**disable** | **enable**}

3. コントローラで DHCP オプション 82 のステータスを表示するには、次のコマンドを入力します。

   show interface detailed ap-manager

   次のような情報が表示されます。

```
Interface Name................................. ap-manager
MAC Address.................................... 00:0a:88:25:10:c4
IP Address..................................... 10.30.16.13
IP Netmask..................................... 255.255.248.0
IP Gateway..................................... 10.30.16.1
External NAT IP State.......................... Disabled
External NAT IP Address........................ 0.0.0.0
External NAT IP Netmask........................ 0.0.0.0
VLAN........................................... untagged
Active Physical Port........................... LAG (29)
Primary Physical Port.......................... LAG (29)
Backup Physical Port........................... Unconfigured
Primary DHCP Server............................ 10.1.0.10
Secondary DHCP Server.......................... Unconfigured
DHCP Option 82................................. Enabled
ACL............................................ Unconfigured
AP Manager..................................... Yes
Guest Interface................................ No
```

アクセス コントロール リストの設定と適用

アクセス コントロール リスト（ACL）は、特定のインターフェイスへのアクセスを制限するために使用される一連のルールです（たとえば、無線クライアントからコントローラの管理インターフェイスに ping が実行されるのを制限する場合などに使用されます。コントローラで設定した ACL は、管理インターフェイス、AP マネージャ インターフェイス、任意の動的インターフェイス、または無線クライアントとやり取りするデータ トラフィックの制御用の WLAN、あるいは Central Processing Unit（CPU; 中央処理装置）宛のすべてのトラフィックの制御用のコントローラ CPU に適用できます。

または、Web 認証用に事前認証 ACL を作成することもできます。事前認証 ACL を使用すると、認証が完了する前に、特定の種類のトラフィックを許可することができます。

（注） 5500 シリーズ コントローラ、2100 シリーズ コントローラ、またはコントローラ ネットワーク モジュールと共に外部の Web サーバを使用している場合は、WLAN 上で外部 Web サーバに対する事前認証 ACL を設定する必要があります。

最大で 64 の ACL を定義することができ、各 ACL に最大 64 のルール（またはフィルタ）を設定できます。各ルールには、ルールの処理に影響を与えるパラメータがあります。パケットが 1 つのルールの全パラメータと一致した場合、そのルールに設定された処理がそのパケットに適用されます。

（注） すべての ACL には、暗黙的に最後のルールとして「すべてのルールを拒否」が適用されます。パケットがどのルールとも一致しない場合、コントローラによってドロップされます。

（注）　CAPWAP が LWAPP と異なるポートを使用している場合は、ネットワーク内の ACL を変更する必要があります。

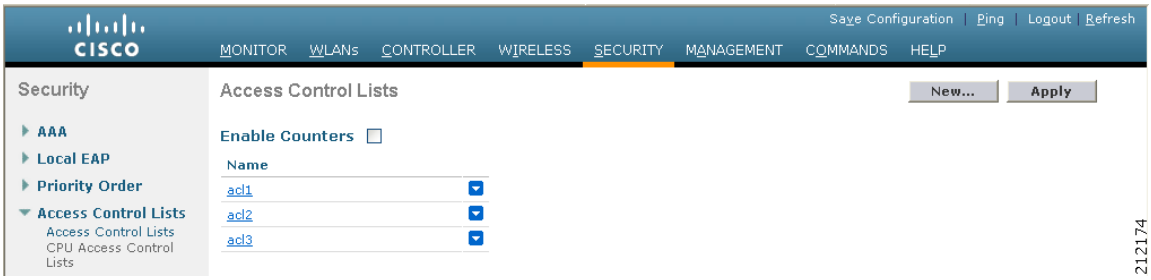
ACL は、GUI または CLI のいずれかを使用して設定および適用できます。

GUI を使用したアクセス コントロール リストの設定

コントローラ GUI を使用して ACL を設定する手順は、次のとおりです。

ステップ 1　[Security] > [Access Control Lists] > [Access Control Lists] の順に選択して、[Access Control Lists] ページを開きます（図 5-30 を参照）。

図 5-30　[Access Control Lists] ページ



このページでは、このコントローラに設定されたすべての ACL が表示されます。

（注）　既存の ACL を削除するには、その ACL の青いドロップダウンの矢印の上にカーソルを置いて、[Remove] を選択します。

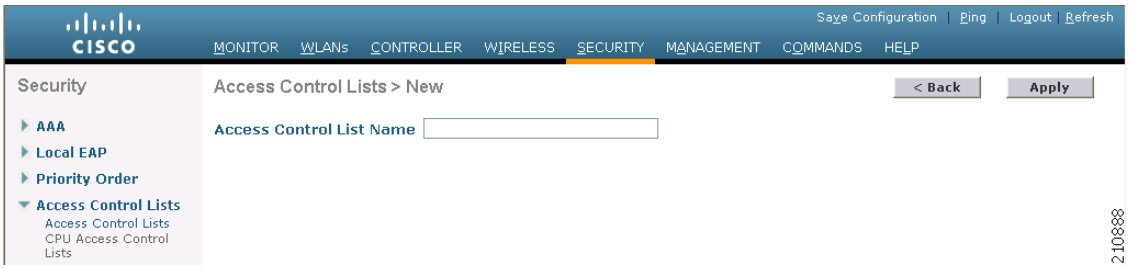
ステップ 2　パケットがコントローラ上で設定されている ACL のいずれかに一致しているかどうかを確認する場合は、[Enable Counters] チェックボックスをオンにして、[Apply] をクリックします。それ以外の場合は、このチェックボックスをオフのままにします（デフォルト値）。この機能は、システムのトラブルシューティングを実行する際に役立ちます。

（注）　ACL のカウンタをクリアするには、その ACL の青いドロップダウンの矢印の上にカーソルを置いて、[Clear Counters] を選択します。

（注）　ACL カウンタは、5500 シリーズ、4400 シリーズ、Cisco WiSM、および Catalyst 3750G 統合型無線 LAN コントローラ スイッチの各コントローラでのみ使用できます。

ステップ 3　新しい ACL を追加するには、[New] をクリックします。[Access Control Lists > New] ページが表示されます（図 5-31 を参照）。

図 5-31　[Access Control Lists > New] ページ

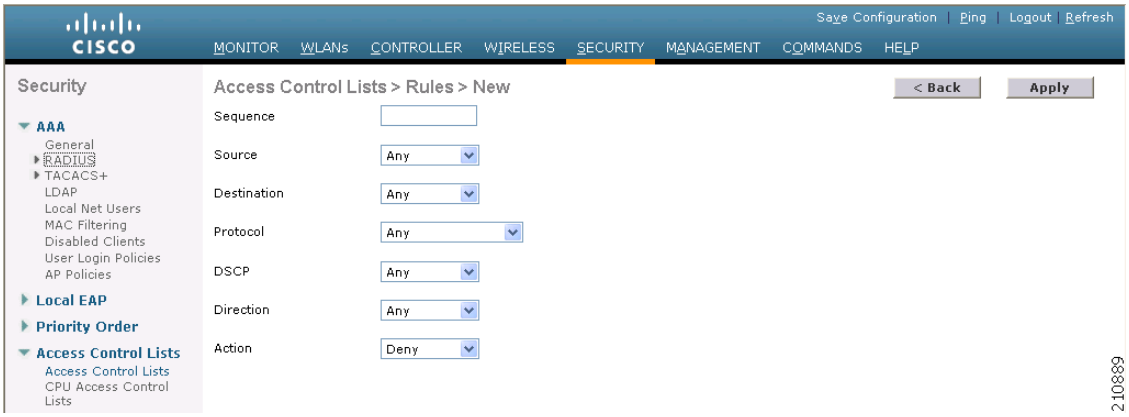


ステップ 4　[Access Control List Name] フィールドに新しい ACL の名前を入力します。最大 32 文字の英数字を入力できます。

ステップ 5　[Apply] をクリックします。[Access Control Lists] ページが再度表示されたら、新しい ACL の名前をクリックします。

ステップ 6　[Access Control Lists > Edit] ページが表示されたら、[Add New Rule] をクリックします。[Access Control Lists > Rules > New] ページが表示されます（図 5-32 を参照）。

図 5-32　[Access Control Lists > Rules > New] ページ



ステップ 7　この ACL にルールを設定する手順は、次のとおりです。

a.　コントローラは各 ACL について最大 64 のルールをサポートします。これらのルールは、1 から 64 の順にリストアップされます。[Sequence] フィールドで、値（1 ～ 64）を入力し、この ACL に定義されている他のルールに対してこのルールの順番を決定します。

（注）　ルール 1 ～ 4 がすでに定義されている場合にルール 29 を追加すると、これはルール 5 として追加されます。ルールのシーケンス番号を追加したり、変更した場合には、順序を維持するために他のルールのシーケンス番号が調整されます。たとえば、ルールのシーケンス番号を 7 から 5 に変更した場合、シーケンス番号 5 および 6 のルールはそれぞれ、自動的に 6 および 7 へと番号が変更されます。

b.　[Source] ドロップダウン ボックスから、次のオプションの 1 つを選択して、この ACL を適用するパケットの送信元を指定します。

- [Any]：任意の送信元（これは、デフォルト値です）。
- [IP Address]：特定の送信元。このオプションを選択した場合、編集ボックスに、送信元の IP アドレスとネットマスクを入力します。

c. [Destination] ドロップダウン ボックスから、次のオプションの 1 つを選択して、この ACL を適用するパケットの宛先を指定します。

- [Any] : 任意の宛先（これは、デフォルト値です）。
- [IP Address] : 特定の宛先。このオプションを選択した場合、編集ボックスに、宛先の IP アドレスとネットマスクを入力します。

d. [Protocol] ドロップダウン ボックスから、この ACL に使用する IP パケットのプロトコル ID を選択します。プロトコル オプションは次のとおりです。

- [Any] : 任意のプロトコル（これは、デフォルト値です）
- [TCP] : Transmission Control Protocol
- [UDP] : ユーザ データグラム プロトコル
- [ICMP] : インターネット制御メッセージ プロトコル
- [ESP] : IP Encapsulating Security Payload
- [AH] : 認証ヘッダー
- [GRE] : 総称ルーティング カプセル化
- [IP in IP] : Internet Protocol（IP; インターネット プロトコル）内 IP。IP-in-IP パケットを許可または拒否します。
- [Eth Over IP] : Ethernet-over-Internet プロトコル
- [OSPF] : Open Shortest Path First
- [Other] : その他の Internet Assigned Numbers Authority（IANA）プロトコル

（注） [Other] を選択する場合は、[Protocol] 編集ボックスに目的のプロトコルの番号を入力します。使用可能なプロトコルの一覧と対応する番号については、次の URL を参照してください。http://www.iana.org/assignments/protocol-numbers

（注） コントローラは ACL の IP パケットのみを許可または拒否できます。他のタイプのパケット（ARP パケットなど）は指定できません。

e. 前の手順で [TCP] または [UDP] を選択すると、[Source Port] および [Destination Port] の 2 つのパラメータも追加で表示されます。これらのパラメータを使用すれば、特定の送信元ポートと宛先ポート、またはポート範囲を選択することができます。ポート オプションは、ネットワーキング スタックとのデータ送受信をするアプリケーションによって使用されます。一部のポートは、telnet、ssh、http などの特定のアプリケーション用に指定されています。

f. [DSCP] ドロップダウン ボックスから、次のオプションの 1 つを選択して、この ACL の Differentiated Service Code Point（DSCP）値を指定します。DSCP は、インターネット上のサービスの質を定義するのに使用できる IP ヘッダー フィールドです。

- [Any] : 任意の DSCP（これは、デフォルト値です）
- [Specific] : DSCP 編集ボックスに入力する、0 ～ 63 の特定の DSCP

g. [Direction] ドロップダウン ボックスから、次のオプションの 1 つを選択して、この ACL を適用するトラフィックの方向を指定します。

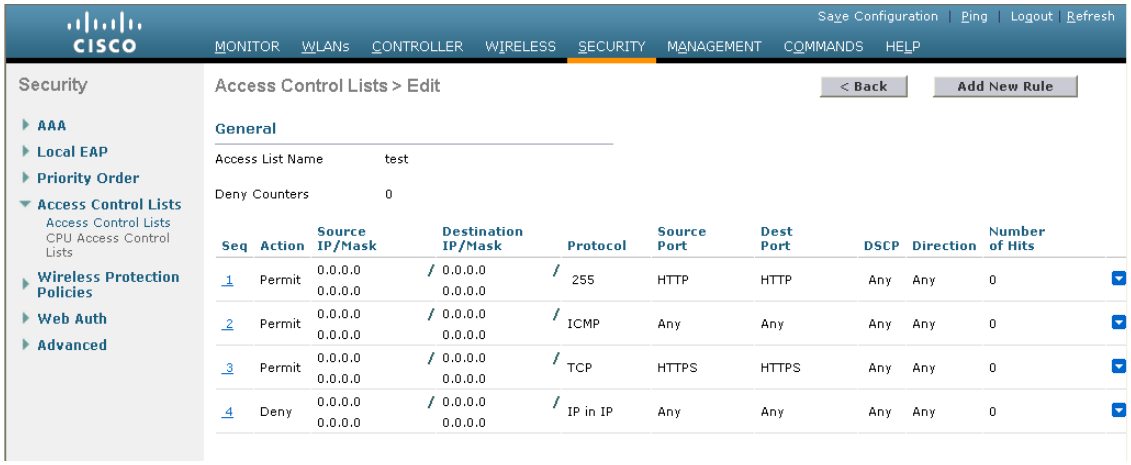
- [Any] : 任意の方向（これは、デフォルト値です）
- [Inbound] : クライアントから
- [Outbound] : クライアントへ

（注）　この ACL をコントローラ CPU に適用することを計画している場合は、[Any] または [Inbound] を選択してください。これは、CPU ACL は、CPU から送信されたパケットではなく、CPU に送信されたパケットのみに適用されるためです。

h. [Action] ドロップダウン ボックスから、[Deny] を選択してこの ACL でパケットがブロックされるようにするか、[Permit] を選択してこの ACL でパケットが許可されるようにします。デフォルト値は [Deny] です。

i. [Apply] をクリックして、変更を適用します。[Access Control Lists > Edit] ページが再表示され、この ACL のルールが示されます。図 5-33 を参照してください。

図 5-33　[Access Control Lists > Edit] ページ



[Deny Counters] フィールドには、パケットが明示的拒否 ACL ルールに一致した回数が表示されます。[Number of Hits] フィールドには、パケットが ACL ルールに一致した回数が表示されます。これらのフィールドを有効にするには、[Access Control Lists] ページ上で ACL カウンタを有効にする必要があります。

（注）　ルールを編集する場合は、希望のルールのシーケンス番号をクリックし、[Access Control Lists > Rules > Edit] ページを開きます。ルールを削除するには、目的のルールの青いドロップダウンの矢印の上にカーソルを置いて、[Remove] を選択します。

j. この ACL にさらにルールを追加するにはこの手順を繰り返します。

ステップ 8　[Save Configuration] をクリックして、変更を保存します。

ステップ 9　さらに ACL を追加するにはこの手順を繰り返します。

GUI を使用したアクセス コントロール リストの適用

コントローラ GUI を使用して ACL を適用するには、次の項の指示に従ってください。

- 「インターフェイスへのアクセス コントロール リストの適用」（P.5-62）
- 「コントローラ CPU へのアクセス コントロール リストの適用」（P.5-63）

- 「WLAN へのアクセス コントロール リストの適用」（P.5-63）
- 「WLAN への事前認証アクセス コントロール リストの適用」（P.5-64）

（注）　インターフェイスまたは WLAN に ACL を適用すると、1 Gbps ファイル サーバからのダウンロードの際にワイヤレス スループットが低下します。スループットを改善するには、インターフェイスまたは WLAN から ACL を削除するか、ポリシー レート制限制約を持つ隣接有線デバイスに ACL を移動するか、1 Gbps ではなく 100 Mbps を使用してファイル サーバを接続します。

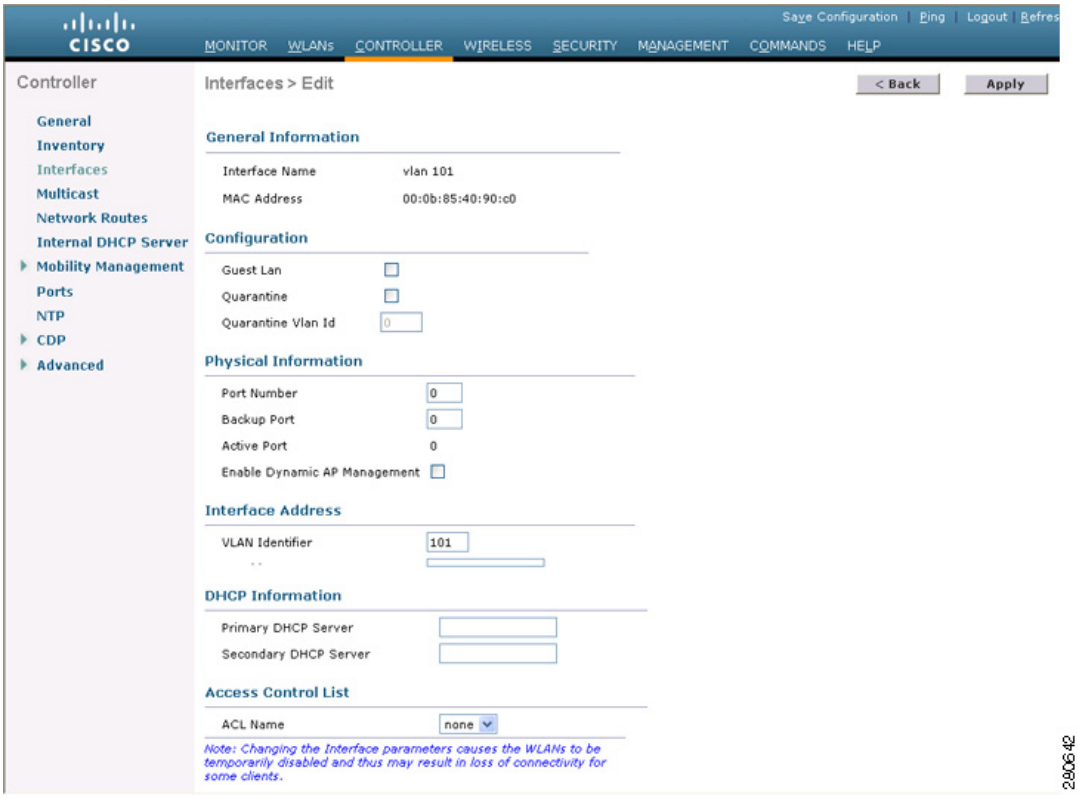
インターフェイスへのアクセス コントロール リストの適用

コントローラの GUI を使用して管理インターフェイス、AP マネージャ インターフェイス、または動的インターフェイスに ACL を適用する手順は、次のとおりです。

ステップ 1　[Controller] > [Interfaces] の順に選択します。

ステップ 2　目的のインターフェイスの名前をクリックします。そのインターフェイスの [Interfaces > Edit] ページが表示されます（図 5-34 を参照）。

図 5-34　[Interfaces > Edit] ページ



ステップ 3　[ACL Name] ドロップダウン ボックスから必要な ACL を選択し、[Apply] をクリックします。デフォルト値は [none] です。

（注）　コントローラ インターフェイスの設定の詳細は、第 3 章を参照してください。

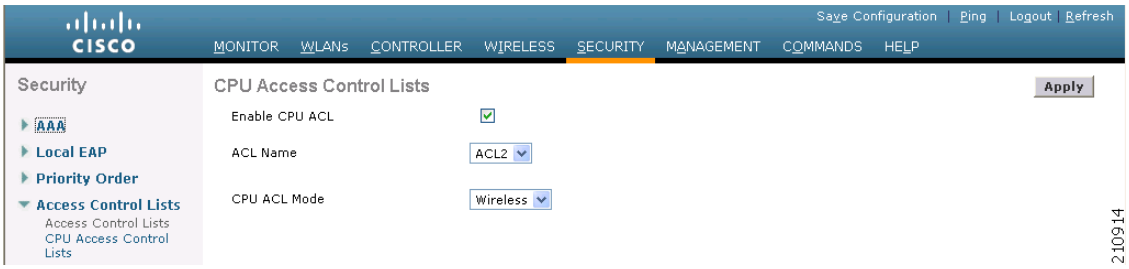
ステップ 4　[Save Configuration] をクリックして、変更を保存します。

コントローラ CPU へのアクセス コントロール リストの適用

コントローラの GUI を使用して、コントローラの CPU に ACL を適用し、CPU へのトラフィックを制御する手順は、次のとおりです。

ステップ 1　[Security] > [Access Control Lists] > [CPU] Access Control Lists] の順に選択します。[CPU Access Control Lists] ページが表示されます（図 5-35 を参照）。

図 5-35　[CPU Access Control Lists] ページ



ステップ 2　[Enable CPU ACL] チェックボックスをオンにして、指定した ACL でコントローラの CPU へのトラフィックを制御できるようにするか、チェックボックスをオフにして CPU ACL の機能を無効にし、CPU にすでに適用されている ACL をすべて削除します。デフォルトではオフになっています。

ステップ 3　[ACL Name] ドロップダウン ボックスから、コントローラの CPU へのトラフィックを制御する ACL を選択します。デフォルト値は [None] で、CPU ACL 機能は無効にされています。[CPU ACL Enable] チェックボックスをオンにして、[None] を選択すると、ACL を選択する必要があることを示すエラー メッセージが表示されます。

（注）　このパラメータは、[CPU ACL Enable] チェックボックスをオンにした場合のみ使用できます。

ステップ 4　[CPU ACL Mode] ドロップダウン ボックスから、コントローラの CPU への転送が制限されるトラフィックのタイプ（有線、無線、または両方）を選択します。デフォルト値は [Wired] です。

（注）　このパラメータは、[CPU ACL Enable] チェックボックスをオンにした場合のみ使用できます。

ステップ 5　[Apply] をクリックして、変更を適用します。

ステップ 6　[Save Configuration] をクリックして、変更を保存します。

WLAN へのアクセス コントロール リストの適用

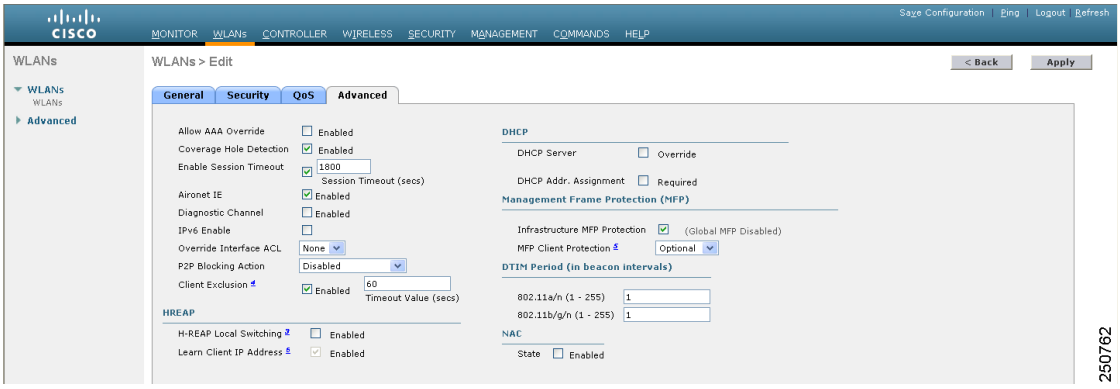
コントローラの GUI を使用して ACL を WLAN に適用する手順は、次のとおりです。

ステップ 1　[WLANs] を選択して、[WLANs] ページを開きます。

ステップ 2　必要な WLAN の ID 番号をクリックして、[WLANs > Edit] ページを開きます。

ステップ 3　[Advanced] タブを選択して、[WLANs > Edit] （[Advanced]）ページを開きます（図 5-36 を参照）。

図 5-36　[WLANs > Edit] （[Advanced]）ページ



ステップ 4　[Override Interface ACL] ドロップダウン ボックスから、この WLAN に適用する ACL を選択します。選択した ACL は、インターフェイスに設定されたすべての ACL を上書きします。デフォルト値は [none] です。

（注）　WLAN の設定の詳細は、第 6 章を参照してください。

ステップ 5　[Apply] をクリックして、変更を適用します。

ステップ 6　[Save Configuration] をクリックして、変更を保存します。

WLAN への事前認証アクセス コントロール リストの適用

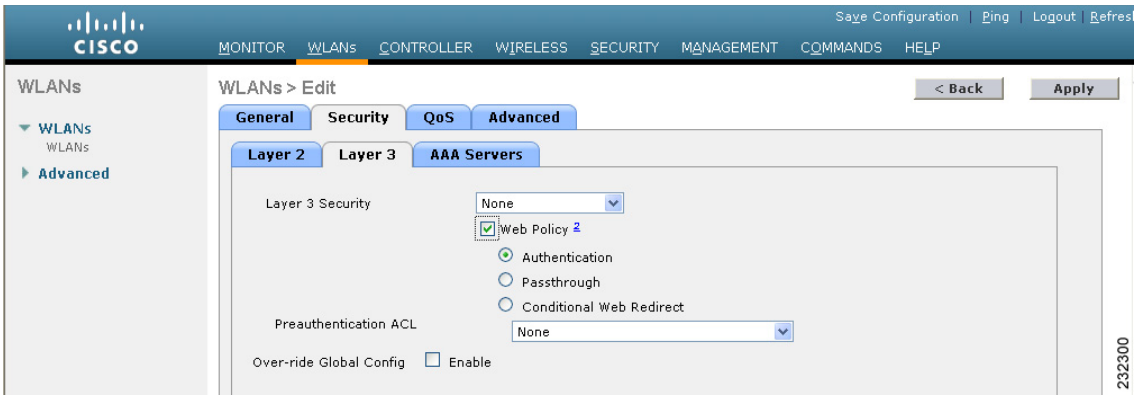
コントローラの GUI を使用して事前認証 ACL を WLAN に適用する手順は、次のとおりです。

ステップ 1　[WLANs] を選択して、[WLANs] ページを開きます。

ステップ 2　必要な WLAN の ID 番号をクリックして、[WLANs > Edit] ページを開きます。

ステップ 3　[Security] タブおよび [Layer 3] タブを選択して、[WLANs > Edit] （[Security] > [Layer 3]）ページを開きます（図 5-37 を参照）。

図 5-37　[WLANs > Edit]（[Security] > [Layer 3]）ページ



ステップ 4　[Web Policy] チェックボックスをオンにします。

ステップ 5　[Preauthentication ACL] ドロップダウン ボックスから目的の ACL を選択し、[Apply] をクリックします。デフォルト値は [none] です。

（注）　WLAN の設定の詳細は、第 6 章を参照してください。

ステップ 6　[Save Configuration] をクリックして、変更を保存します。

CLI を使用したアクセス コントロール リストの設定

コントローラ CLI を使用して ACL を設定する手順は、次のとおりです。

ステップ 1　コントローラ上に設定されているすべての ACL を表示するには、次のコマンドを入力します。

show acl summary

次のような情報が表示されます。

```
ACL Counter Status            Enabled
-------------------------------------
ACL Name                     Applied
------------------------- ------------
acl1                           Yes
acl2                           Yes
acl3                          Yes
```

ステップ 2　特定の ACL の詳細情報を表示するには、次のコマンドを入力します。

show acl detailed *acl_name*

次のような情報が表示されます。

```
                Source          Destination        Source Port Dest Port
I Dir IP Address/Netmask IP Address/Netmask Prot    Range Range    DSCP Action Counter
- --- ------------------ ------------------ ---- ----------- -------- ----- ------ -------
1 Any 0.0.0.0/0.0.0.0    0.0.0.0/0.0.0.0    Any    0-65535  0-65535  0     Deny     0
2 In  0.0.0.0/0.0.0.0    200.200.200.0/     6      80-80    0-65535  Any   Permit   0
                         255.255.255.0
```

```
DenyCounter :      0
```

Counter フィールドはパケットが ACL ルールに一致する場合に毎回増分され、DenyCounter フィールドはパケットがいずれのルールにも一致しない場合に毎回増分されます。

ステップ 3　コントローラの ACL カウンタを有効または無効にするには、次のコマンドを入力します。

config acl counter {**start** | **stop**}

（注）　ACL の現在のカウンタをクリアする場合は、次のコマンドを入力します。
clear acl counters *acl_name*

（注）　ACL カウンタは、5500 シリーズ、4400 シリーズ、Cisco WiSM、および Catalyst 3750G 統合型無線 LAN コントローラ スイッチの各コントローラでのみ使用できます。

ステップ 4　新しい ACL を追加するには、次のコマンドを入力します。

config acl create *acl_name*

acl_name パラメータには、最大 32 文字の英数字を入力できます。

ステップ 5　ACL に新しいルールを追加するには、次のコマンドを入力します。

config acl rule add *acl_name rule_index*

ステップ 6　ACL ルールを設定するには、次のコマンドを入力します。

config acl rule {

action *acl_name rule_index* {**permit** | **deny**} |

change index ***acl_name old_index new_index*** |

destination address *acl_name rule_index ip_address netmask* |

destination port range *acl_name rule_index start_port end_port* |

direction *acl_name rule_index* {**in** | **out** | **any**} |

dscp *acl_name rule_index dscp* |

protocol *acl_name rule_index protocol* |

source address *acl_name rule_index ip_address netmask* |

source port range *acl_name rule_index start_port end_port* |

swap index *acl_name index_1 index_2*}

ルール パラメータの説明については、「GUI を使用したアクセス コントロール リストの設定」（P.5-58）のステップ 7 を参照してください。

ステップ 7　設定を保存するには、次のコマンドを入力します。

save config

（注）　ACL を削除するには、**config acl delete *acl_name*** を入力します。ACL ルールを削除するには、**config acl rule delete *acl_name*** *rule_index* を入力します。

CLI を使用したアクセス コントロール リストの適用

コントローラ CLI を使用して ACL を適用する手順は、次のとおりです。

ステップ 1　次のいずれかの操作を行います。

- 管理インターフェイス、AP マネージャ インターフェイス、または動的インターフェイスに ACL を適用するには、次のコマンドを入力します。

  config interface acl {**management** | **ap-manager** | *dynamic_interface_name*} *acl_name*

  （注）　インターフェイスに適用されている ACL を表示するには、**show interface detailed** {**management** | **ap-manager** | *dynamic_interface_name*} と入力します。インターフェイスに適用されている ACL を削除するには、**config interface acl** {**management** | **ap-manager** | *dynamic_interface_name*} **none** と入力します。

  コントローラ インターフェイスの設定の詳細は、第 3 章を参照してください。

- ACL をデータ パスに適用するには、次のコマンドを入力します。

  config acl apply *acl_name*

- ACL をコントローラの CPU に適用して、CPU に転送されるトラフィックのタイプ（有線、無線、または両方）を制限するには、次のコマンドを入力します。

  config acl cpu *acl_name* {**wired** | **wireless** | **both**}

  （注）　コントローラ CPU に適用されている ACL を表示するには、**show acl cpu** と入力します。コントローラ CPU に適用されている ACL を削除するには、**config acl cpu none** と入力します。

- ACL を WLAN に適用するには、次のコマンドを入力します。

  config wlan acl *wlan_id acl_name*

  （注）　WLAN に適用されている ACL を表示するには、**show wlan** *wlan_id* と入力します。WLAN に適用されている ACL を削除するには、**config wlan acl** *wlan_id* **none** と入力します。

- 事前認証 ACL を WLAN に適用するには、次のコマンドを入力します。

  config wlan security web-auth acl *wlan_id acl_name*

  WLAN の設定の詳細は、第 6 章を参照してください。

ステップ 2　設定を保存するには、次のコマンドを入力します。

save config

管理フレーム保護の設定

Management Frame Protection（MFP; 管理フレーム保護）では、アクセス ポイントとクライアント間で送受信される 802.11 管理メッセージを保護および暗号化することにより、セキュリティが確保されます。MFP は、インフラストラクチャとクライアント サポートの両方を実現します。コントローラ ソフトウェア リリース 4.0 は、インフラストラクチャ MFP のみをサポートするのに対し、コントローラ ソフトウェア リリース 4.1 以降は、インフラストラクチャとクライアント MFP の両方をサポートします。

- **インフラストラクチャ MFP**：DoS 攻撃を引き起こしたり、ネットワーク上で過剰なアソシエーションやプローブを生じさせたり、不正なアクセス ポイントとして介入したり、QoS と無線測定フレームへの攻撃によりネットワーク パフォーマンスを低下させたりする敵対者を検出することにより、管理フレームを保護します。インフラストラクチャ MFP はまた、フィッシング インシデントの効果的かつ迅速な検出/報告手段を提供します。

  インフラストラクチャ MFP は特に、アクセス ポイントによって送信され（クライアントによって送信されたのではなく）、次にネットワーク内の他のアクセス ポイントによって検証される管理フレームに、Message Integrity Check Information Element（MIC IE; メッセージ整合性情報要素）を追加することによって、802.11 セッション管理機能を保護します。インフラストラクチャ MFP はパッシブです。侵入を検知し報告しますが、それを止めることはできません。

- **クライアント MFP**：認証されたクライアントをスプーフィング フレームから保護し、無線 LAN に対する多数の共通の攻撃が威力を発揮することのないようにします。認証解除攻撃などのほとんどの攻撃では、有効なクライアントとの競合により簡単にパフォーマンスを劣化させます。

  クライアント MFP は特に、アクセス ポイントと CCXv5 クライアント間で送受信される管理フレームを暗号化します。これにより、アクセス ポイントとクライアントの両方で、スプーフィングされたクラス 3 管理フレーム（つまり、アクセス ポイントと認証され関連付けられたクライアント間でやり取りされる管理フレーム）をドロップすることにより、予防措置をとることができます。クライアント MFP は、IEEE 802.11i によって定義されたセキュリティ メカニズムを利用し、アソシエーション解除、認証解除、および QoS（WMM）アクションといったタイプのクラス 3 ユニキャスト管理フレームを保護します。クライアント MFP は、最も一般的な種類のサービス拒否攻撃から、クライアントとアクセス ポイント間のセッションを保護します。また、セッションのデータ フレームに使用されているのと同じ暗号化方式を使用することにより、クラス 3 管理フレームを保護します。アクセス ポイントまたはクライアントにより受信されたフレームの暗号化解除に失敗すると、そのフレームはドロップされ、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 をサポートしており、TKIP または AES-CCMP のいずれかを使用して WPA2 をネゴシエートする必要があります。EAP または PSK は、PMK を取得するために使用されます。CCKM およびコントローラのモビリティ管理は、レイヤ 2 およびレイヤ 3 の高速ローミングのために、アクセス ポイント間でセッション キーを配布するのに使用されます。

（注） ブロードキャスト フレームを使用した攻撃を防ぐため、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（アソシエーション解除、認証解除、またはアクションなど）を送信しません。CCXv5 クライアントおよびアクセス ポイントは、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。

インフラストラクチャ MFP は、クライアント MFP 対応でないクライアントに送信された無効なユニキャスト フレームと、無効なクラス 1 およびクラス 2 管理フレームを引き続き検出および報告するため、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、補足するものであると言えます。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。

インフラストラクチャ MFP は次の 3 つの主要なコンポーネントで構成されます。

- **管理フレーム保護**：アクセス ポイントでは、送信される管理フレームが、各フレームに MIC IE を追加することによって保護されます。フレームのコピー、変更、リプレイが試みられた場合、MIC は無効となり、MFP フレームを検出するよう設定された受信アクセス ポイントは不具合を報告します。
- **管理フレーム検証**：アクセス ポイントでは、インフラストラクチャ MFP によって、ネットワークの他のアクセス ポイントから受信する各管理フレームが検証されます。MIC IE が存在しており（送信側が 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に一致していることを確認します。MFP フレームを送信するよう設定されているアクセス ポイントに属する BSSID からの有効な MIC IE が含まれていないフレームを受信した場合、不具合をネットワーク管理システムに報告します。タイムスタンプが適切に機能できるように、すべてのコントローラはネットワーク タイム プロトコル（NTP）で同期化されている必要があります。
- **イベント報告**：アクセス ポイントで異常が検出されるとコントローラに通知されます。コントローラでは、受信した異常イベントが集計され、その結果が SNMP トラップを使用してネットワーク管理システムに報告されます。

（注） スタンドアロン モードの Hybrid REAP アクセス ポイントで生成されるエラー レポートは、コントローラに転送することはできず、ドロップされます。

（注） クライアント MFP は、インフラストラクチャ MFP と同じイベント報告メカニズムを使用します。

インフラストラクチャ MFP は、デフォルトで有効にされ、グローバルに無効化できます。以前のソフトウェア リリースからアップグレードする場合、アクセス ポイント認証が有効になっているときは、これら 2 つの機能は相互に排他的であるため、インフラストラクチャ MFP はグローバルに無効になります。インフラストラクチャ MFP がグローバルに有効化されると、選択した WLAN に対してシグニチャの生成（MIC を送信フレームに追加する）を無効にでき、選択したアクセス ポイントに対して検証を無効にできます。

クライアント MFP は、WPA2 に対して設定された WLAN 上でデフォルトで有効にされています。選択した WLAN 上で、無効にすることも、必須にすることも（この場合 MFP をネゴシエートするクライアントのみがアソシエーションを許可されます）できます。

MFP は、GUI または CLI のいずれを使用しても設定できます。

MFP の使用に関するガイドライン

MFP を使用する際のガイドラインは次のとおりです。

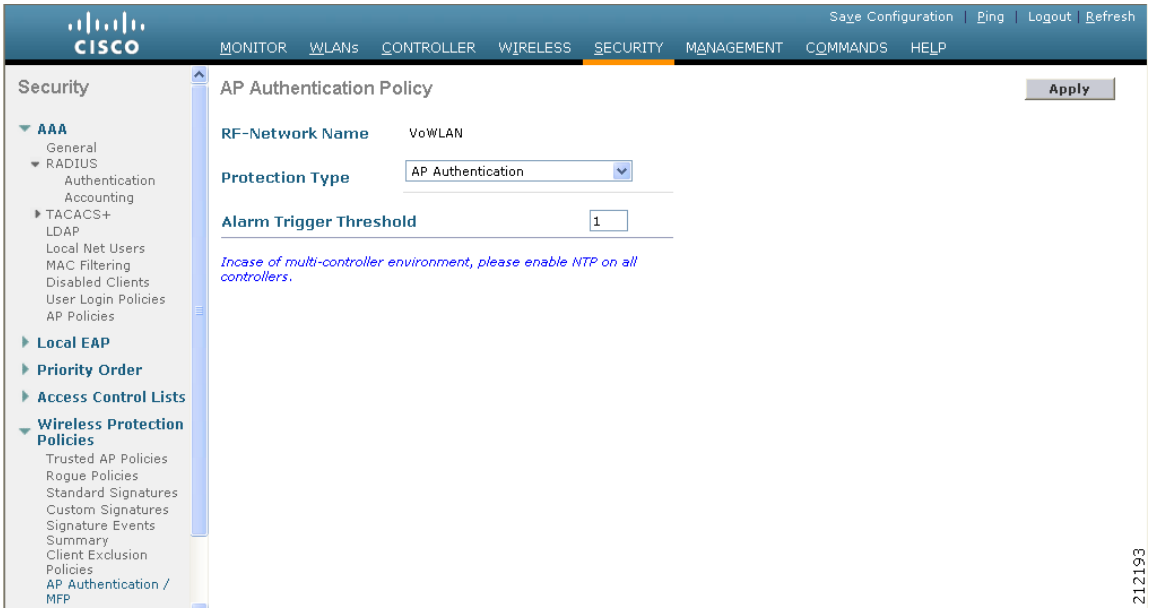
- MFP は、Cisco Aironet Lightweight アクセス ポイントでの使用がサポートされています。
- Lightweight アクセス ポイントでは、ローカル モードおよび監視モードで、およびアクセス ポイントがコントローラに接続されているときは Hybrid REAP モードで MFP がサポートされます。ローカル モード、Hybrid REAP モード、およびブリッジ モードで、MFP がサポートされます。
- クライアント MFP は、TKIP または AES-CCMP で WPA2 を使用する CCXv5 クライアントでの使用のみがサポートされています。
- クライアント MFP が無効にされているか、オプションである場合は、非 CCXv5 クライアントは WLAN にアソシエートできます。

GUI を使用した MFP の設定

コントローラ GUI を使用して MFP を設定する手順は、次のとおりです。

ステップ 1　[Security] > [Wireless Protection Policies] > [AP Authentication/MFP] の順に選択します。[AP Authentication Policy] ページが表示されます（図 5-38 を参照）。

図 5-38　[AP Authentication Policy] ページ



ステップ 2　コントローラでインフラストラクチャ MFP をグローバルに有効化するには、[Protection Type] ドロップダウン ボックスから [Management Frame Protection] を選択します。

ステップ 3　[Apply] をクリックして、変更を適用します。

（注）　複数のコントローラがモビリティ グループに含まれている場合は、インフラストラクチャ MFP に対して設定されているモビリティ グループ内のすべてのコントローラ上で、Network Time Protocol（NTP）サーバを設定する必要があります。

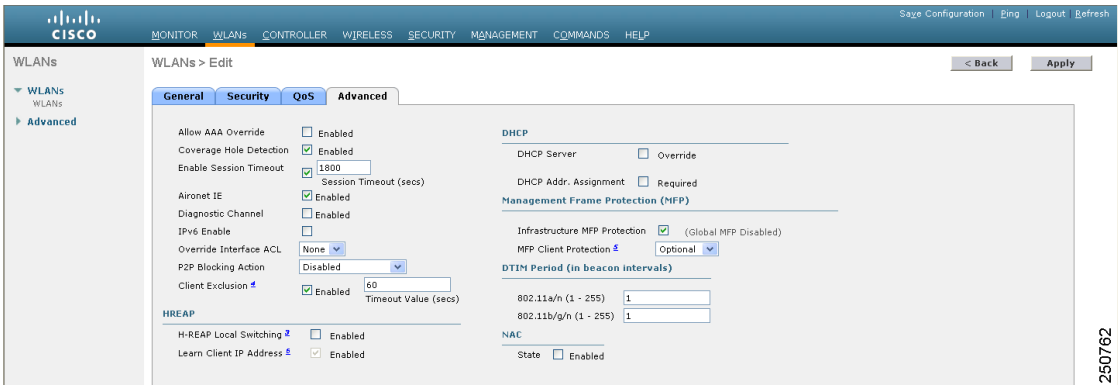
ステップ 4　コントローラで MFP をグローバルで有効化した後、特定の WLAN に対してインフラストラクチャ MFP 保護の無効化や再有効化を行う手順は、次のとおりです。

a.　[WLANs] を選択します。

b.　目的の WLAN のプロファイル名をクリックします。[WLANs > Edit] ページが表示されます。

c.　[Advanced] を選択します。[WLANs > Edit]（[Advanced]）ページが表示されます（図 5-39 を参照）。

図 5-39　[WLANs > Edit]（[Advanced]）ページ



d. [Infrastructure MFP Protection] チェックボックスをオフにしてこの WLAN に対して MFP を無効にするか、このチェックボックスをオンにしてこの WLAN に対して MFP を有効にします。デフォルト値は有効（enable）です。グローバル MFP が無効にされている場合、チェックボックスの右側のカッコ内に注意が表示されます。

e. [MFP Client Protection] ドロップダウン ボックスから、[Disabled]、[Optional]、または [Required] を選択します。デフォルト値は [Optional] です。[Required] を選択した場合、MFP がネゴシエートされている場合（つまり、WPA2 がコントローラ上で設定されており、クライアントが CCXv5 MFP をサポートしていて WPA2 に対して設定されている場合）のみ、クライアントはアソシエーションを許可されます。

f. [Apply] をクリックして、変更を適用します。

ステップ 5　コントローラでインフラストラクチャ MFP をグローバルで有効化した後、特定のアクセス ポイントに対してインフラストラクチャ MFP 検証の無効化や再有効化を行う手順は、次のとおりです。

a. [Wireless] > [Access Points] > [All APs] の順に選択して、[All APs] ページを開きます。

b. 目的のアクセス ポイントの名前をクリックします。

c. [Advanced] タブを選択します。[All APs > Details for]（[Advanced]）ページが表示されます。

d. [MFP Frame Validation] チェックボックスをオフにしてこのアクセス ポイントに対して MFP を無効にするか、このチェックボックスをオンにしてこのアクセス ポイントに対して MFP を有効にします。デフォルト値は有効（enable）です。グローバル MFP が無効にされている場合、チェックボックスの右側のカッコ内に注意が表示されます。

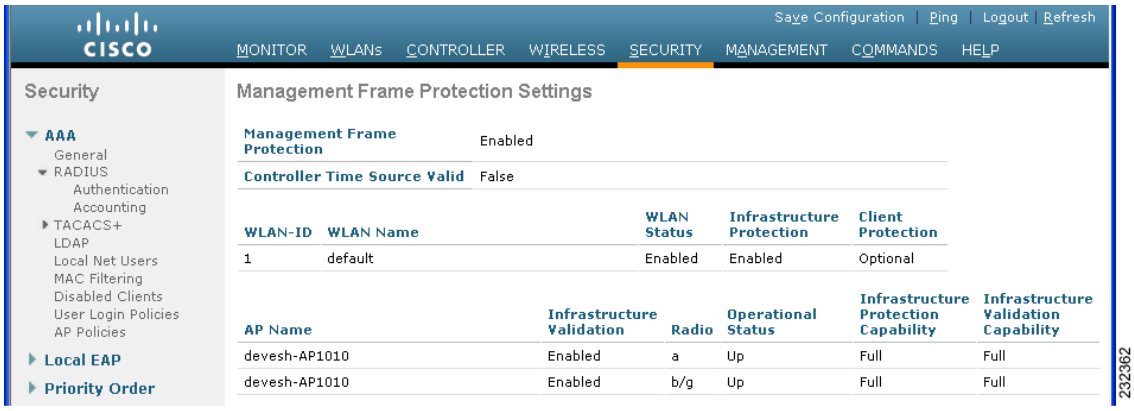
e. [Apply] をクリックして、変更を適用します。

ステップ 6　[Save Configuration] をクリックして、設定を保存します。

GUI を使用した MFP 設定の表示

コントローラの現在のグローバル MFP の設定を表示するには、[Security] > [Wireless Protection Policies] > [Management Frame Protection] の順に選択します。[Management Frame Protection Settings] ページが表示されます（図 5-40 を参照）。

図 5-40　[Management Frame Protection Settings] ページ



このページでは、次の MFP 設定が表示されます。

- [Management Frame Protection] フィールドは、インフラストラクチャ MFP がコントローラでグローバルに有効化されているかどうかを示します。
- [Controller Time Source Valid] フィールドは、コントローラの時刻が（時刻を手動で入力することにより）ローカルで設定されているか、外部ソース（NTP サーバなど）を通して設定されているかを示します。時刻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。時刻がローカルで設定されている場合、このフィールドの値は「False」です。時刻ソースは、モビリティ グループ内の複数のコントローラのアクセス ポイント間の管理フレーム上のタイムスタンプの検証に使用されます。
- [Infrastructure Protection] フィールドは、インフラストラクチャ MFP が個別の WLAN に対して有効化されているかどうかを示します。
- [Client Protection] フィールドは、クライアント MFP が個別の WLAN に対して有効化されているかどうかと、オプションまたは必須のいずれであるかを示します。
- [Infrastructure Validation] フィールドは、インフラストラクチャ MFP が個別のアクセス ポイントに対して有効化されているかどうかを示します。

CLI を使用した MFP の設定

コントローラ CLI を使用して MFP を設定するには、次のコマンドを使用します。

1. コントローラでインフラストラクチャ MFP をグローバルに有効または無効にするには、次のコマンドを入力します。

   config wps mfp infrastructure {**enable** | **disable**}

2. WLAN で MFP シグニチャの生成を有効または無効にするには、次のコマンドを入力します。

   config wlan mfp infrastructure protection {**enable** | **disable**} ***wlan_id***

   （注）　シグニチャの生成は、インフラストラクチャ MFP がグローバルに有効にされている場合のみ、アクティブ化されます。

3. アクセス ポイントでインフラストラクチャ MFP 検証を有効または無効にするには、次のコマンドを入力します。

   config ap mfp infrastructure validation {**enable** | **disable**} *Cisco_AP*

（注）　MFP 検証は、インフラストラクチャ MFP がグローバルに有効にされている場合のみ、アクティブ化されます。

4. 特定の WLAN でクライアント MFP シグニチャを有効または無効にするには、次のコマンドを入力します。

   config wlan mfp client {**enable** | **disable**} *wlan_id* [**required**]

   クライアント MFP を有効にしてオプションの **required** パラメータを使用すると、MFP がネゴシエートされている場合のみ、クライアントはアソシエーションを許可されます。

CLI を使用した MFP 設定の表示

コントローラの CLI を使用して MFP の設定を表示するには、次のコマンドを使用します。

1. コントローラの現在の MFP の設定を表示するには、次のコマンドを入力します。

   show wps mfp summary

   次のような情報が表示されます。

```
Global Infrastructure MFP state.... Enabled
Controller Time Source Valid....... False

                     WLAN       Infra.      Client
WLAN ID  WLAN Name Status     Protection  Protection
-------  ---------- -------- ----------  -----------
1        test1      Enabled   Disabled    Disabled
2        open       Enabled   Enabled     Required
3        testpsk    Enabled   *Enabled    Optional but inactive (WPA2 not configured)

         Infra.             Operational     --Infra. Capability--
AP Name  Validation  Radio  State            Protection  Validation
-------- ----------- -----  -----------  ----------- -----------
mapAP    Disabled    a      Up              Full        Full
                     b/g    Up              Full        Full
rootAP2  Enabled     a      Up              Full        Full
                     b/g    Up              Full        Full
HReap    *Enabled    b/g    Up             Full        Full
                     a      Down            Full        Full
```

2. 特定の WLAN の現在の MFP 設定を表示するには、次のコマンドを入力します。

   show wlan *wlan_id*

   次のような情報が表示されます。

```
WLAN Identifier.......................... 1
Profile Name............................. test1
Network Name (SSID)...................... test1
Status................................... Enabled
MAC Filtering............................ Disabled
Broadcast SSID........................... Enabled
...
Local EAP Authentication................. Enabled (Profile 'test')
Diagnostics Channel...................... Disabled
Security

   802.11 Authentication:................ Open System
   Static WEP Keys....................... Disabled
   802.1X................................ Enabled
```

```
     Encryption:.............................. 104-bit WEP
  Wi-Fi Protected Access (WPA/WPA2)...... Disabled
  CKIP .................................... Disabled
  IP Security.............................. Disabled
  IP Security Passthru..................... Disabled
  Web Based Authentication................. Disabled
  Web-Passthrough.......................... Disabled
  Conditional Web Redirect................. Disabled
  Auto Anchor.............................. Enabled
   H-REAP Local Switching.................. Disabled
  Infrastructure MFP protection.......... Enabled
  Client MFP............................... Required
...
```

3. 特定のアクセス ポイントの現在の MFP 設定を表示するには、次のコマンドを入力します。

   show ap config general ***AP_name***

   次のような情報が表示されます。

```
Cisco AP Identifier.............................. 0
Cisco AP Name.................................... ap:52:c5:c0
AP Regulatory Domain............................. 80211bg: -N 80211a: -N
Switch Port Number .............................. 1
MAC Address...................................... 00:0b:85:52:c5:c0
IP Address Configuration......................... Static IP assigned
IP Address....................................... 10.67.73.33
IP NetMask....................................... 255.255.255.192
...
AP Mode ......................................... Local
Remote AP Debug ................................. Disabled
S/W  Version .................................... 4.0.2.0
Boot  Version ................................... 2.1.78.0
Mini IOS Version .................................      --
Stats Reporting Period .......................... 180
LED State........................................ Enabled
ILP Pre Standard Switch.......................... Disabled
ILP Power Injector............................... Disabled
Number Of Slots.................................. 2
AP Model......................................... AP1020
AP Serial Number................................. WCN09260057
AP Certificate Type.............................. Manufacture Installed
Management Frame Protection Validation .......... Enabled
```

4. 特定のクライアントでクライアント MFP が有効にされているかどうかを表示するには、次のコマンドを入力します。

   show client detail *client_mac*

```
Client MAC Address............................... 00:14:1c:ed:34:72
...
Policy Type...................................... WPA2
Authentication Key Management.................... PSK
Encryption Cipher................................ CCMP (AES)
Management Frame Protection...................... Yes
...
```

5. コントローラの MFP 統計を表示するには、次のコマンドを入力します。

   show wps mfp statistics

   次のような情報が表示されます。

（注）　実際に攻撃が進行中でない限り、このレポートにデータは含まれません。ここに示すさまざまなエラーの種類の例は、図示のみを目的としています。この表は 5 分ごとにクリアされ、データはネットワーク管理ステーションに転送されます。

```
BSSID             Radio Validator AP Last Source Addr  Found  Error Type Count Frame Types
----------------- ----- ------------ ------------------ ------ ------------ ----- -------
00:0b:85:56:c1:a0  a    jatwo-1000b 00:01:02:03:04:05 Infra  Invalid MIC 183  Assoc Req
                                                                              Probe Req
                                                                              Beacon
                                                      Infra  Out of seq     4  Assoc Req
                                                      Infra  Unexpected MIC 85 Reassoc Req
                                                      Client Decrypt err  1974 Reassoc Req
                                                                              Disassoc
                                                      Client Replay err     74 Assoc Req
                                                                              Probe Req
                                                                              Beacon
                                                      Client Invalid ICV   174 Reassoc Req
                                                                              Disassoc
                                                      Client Invalid header174 Assoc Req
                                                                              Probe Req
                                                                              Beacon
                                                      Client Brdcst disass 174 Reassoc Req
                                                                              Disassoc
00:0b:85:56:c1:a0  b/g  jatwo-1000b 00:01:02:03:04:05 Infra  Out of seq  185 Reassoc Resp
                                                      Client Not encrypted 174 Assoc Resp
                                                                              Probe Resp
```

CLI を使用した MFP に関する問題のデバッグ

MFP に関する問題が発生した場合は、次のコマンドを使用します。

- **debug wps mfp *?*{enable | disable}**

  ここで、*?* は、次のいずれかを示します。

  client：クライアントの MFP メッセージのデバッグについて設定します。

  capwap：コントローラとアクセス ポイント間の MFP メッセージのデバッグについて設定します。

  detail：MFP メッセージの詳細なデバッグについて設定します。

  report：MFP レポートのデバッグについて設定します。

  mm：MFP モビリティ（コントローラ間）メッセージのデバッグについて設定します。

クライアント除外ポリシーの設定

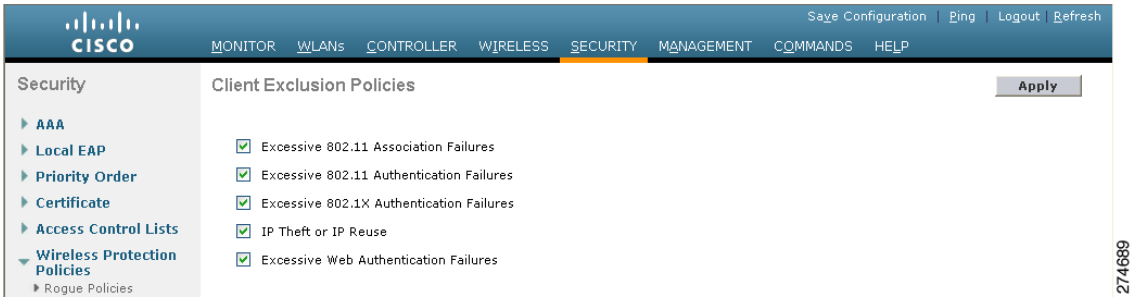
この項では、特定の条件下でコントローラ GUI または CLI を使用してクライアントを除外するようにコントローラを設定する方法を説明します。

GUI を使用したクライアント除外ポリシーの設定

コントローラの GUI を使用してクライアント除外ポリシーを設定する手順は、次のとおりです。

ステップ 1　[Security] > [Wireless Protection Policies] > [Client Exclusion Policies] の順に選択して、[Client Exclusion Policies] ページを開きます（図 5-41 を参照）。

図 5-41　[Client Exclusion Policies] ページ



ステップ 2　指定された条件においてコントローラでクライアントを除外するには、これらのいずれかのチェックボックスをオンにします。各除外ポリシーのデフォルトは有効です。

- [Excessive 802.11 Association Failures]：クライアントは、802.11 アソシエーションの試行に 5 回連続して失敗すると、6 回目の試行で除外されます。
- [Excessive 802.11 Authentication Failures]：クライアントは、802.11 認証の試行に 5 回連続して失敗すると、6 回目の試行で除外されます。
- [Excessive 802.1X Authentication Failures]：クライアントは、802.1X 認証の試行に 3 回連続して失敗すると、4 回目の試行で除外されます。
- [IP Theft or IP Reuse]：IP アドレスが他のデバイスにすでに割り当てられている場合、クライアントは除外されます。
- [Excessive Web Authentication Failures]：クライアントは、Web 認証の試行に 3 回連続して失敗すると、4 回目の試行で除外されます。

ステップ 3　[Apply] をクリックして、変更を適用します。

ステップ 4　[Save Configuration] をクリックして、変更を保存します。

CLI を使用したクライアント除外ポリシーの設定

コントローラの CLI を使用してクライアント除外ポリシーを設定する手順は、次のとおりです。

ステップ 1　802.11 アソシエーションを 5 回連続して失敗した後、6 回目の試行でコントローラがクライアントを除外することを有効または無効にするには、次のコマンドを入力します。

config wps client-exclusion 802.11-assoc {enable | disable}

ステップ 2　802.11 認証を 5 回連続して失敗した後、6 回目の試行でコントローラがクライアントを除外することを有効または無効にするには、次のコマンドを入力します。

config wps client-exclusion 802.11-auth {enable | disable}

ステップ 3　802.1X 認証を 3 回連続して失敗した後、4 回目の試行でコントローラがクライアントを除外することを有効または無効にするには、次のコマンドを入力します。

config wps client-exclusion 802.1x-auth {enable | disable}

ステップ 4　IP アドレスが別のデバイスにすでに割り当てられている場合に、クライアントを除外するようにコントローラを有効または無効にするには、次のコマンドを入力します。

config wps client-exclusion ip-theft {enable | disable}

ステップ 5　Web 認証を 3 回連続して失敗した後、4 回目の試行でコントローラがクライアントを除外することを有効または無効にするには、次のコマンドを入力します。

config wps client-exclusion web-auth {enable | disable}

ステップ 6　上記のすべての理由でコントローラがクライアントを除外することを有効または無効にするには、次のコマンドを入力します。

config wps client-exclusion all {enable | disable}

ステップ 7　変更を保存するには、次のコマンドを入力します。

save config

ステップ 8　クライアント除外ポリシー構成設定を表示するには、このコマンドを入力します。

show wps summary

次のような情報が表示されます。

```
Auto-Immune
  Auto-Immune.................................... Disabled

Client Exclusion Policy
  Excessive 802.11-association failures.......... Enabled
  Excessive 802.11-authentication failures....... Enabled
  Excessive 802.1x-authentication................ Enabled
  IP-theft....................................... Enabled
  Excessive Web authentication failure........... Enabled

Signature Policy
  Signature Processing........................... Enabled
```

ID ネットワーキングの設定

この項では、ID ネットワーキング機能とその設定方法、およびさまざまなセキュリティ ポリシーに対して予想される動作について説明します。

- 「ID ネットワーキングの概要」（P.5-77）
- 「ID ネットワーキングで使用される RADIUS 属性」（P.5-78）
- 「AAA Override の設定」（P.5-81）

ID ネットワーキングの概要

ほとんどの無線 LAN システムの場合、各 WLAN に静的なポリシーがあり、SSID が設定されているすべてのクライアントに適用されます。これは強力な方式ですが、クライアントに複数の Quality of Service（QoS）およびセキュリティ ポリシーを適用するには、そのクライアントに複数の SSID を設定する必要があるために、限界がありました。

これに対して Cisco Wireless LAN Solution は、ID ネットワーキングをサポートしています。これは、ネットワークが 1 つの SSID をアドバタイズできるようにすると同時に、特定のユーザに対して、ユーザ プロファイルに基づいて異なる QoS またはセキュリティ ポリシーの適用を可能にするものです。ID ネットワーキングを使用して制御できるポリシーには、次のものがあります。

- Quality of Service。RADIUS Access Accept に QoS-Level 値が指定されている場合、WLAN プロファイルで指定された QoS 値が上書きされます。
- ACL。RADIUS Access Accept に ACL 属性が指定されている場合、システムでは ACL-Name が認証後にクライアント ステーションに適用されます。これにより、そのインターフェイスに割り当てられている ACL がすべて上書きされます。
- VLAN。VLAN Interface-Name または VLAN-Tag が RADIUS Access Accept に存在する場合は、クライアントが特定のインターフェイス上に配置されます。

（注）　VLAN 機能は、MAC フィルタリング、802.1X、および WPA のみをサポートします。Web 認証または IPSec はサポートしません。

- トンネル属性。

（注）　この項で後述する他の RADIUS 属性（QoS-Level、ACL-Name、Interface-Name、または VLAN-Tag）のいずれかを返す場合、トンネル属性も返す必要があります。

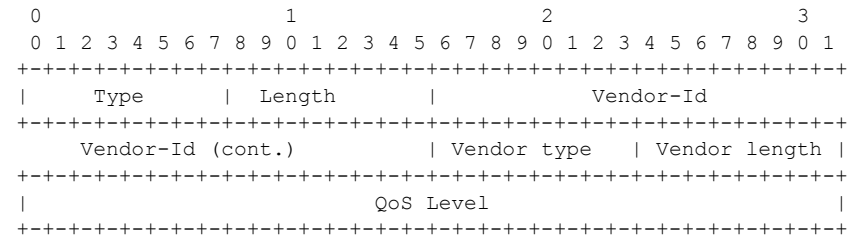
オペレーティング システムのローカル MAC フィルタ データベースは、インターフェイス名を含むように拡張され、ローカル MAC フィルタで、クライアントが割り当てられるインターフェイスを指定できるようになりました。別の RADIUS サーバも使用できますが、その RADIUS サーバは [Security] メニューを使用して定義する必要があります。

ID ネットワーキングで使用される RADIUS 属性

この項では、ID ネットワーキングで使用される RADIUS 属性について説明します。

QoS-Level

この属性は、スイッチング ファブリック内および空間経由のモバイル クライアントのトラフィックに適用される Quality of Service レベルを示します。この例は、QoS-Level 属性フォーマットの要約を示しています。フィールドは左から右に伝送されます。

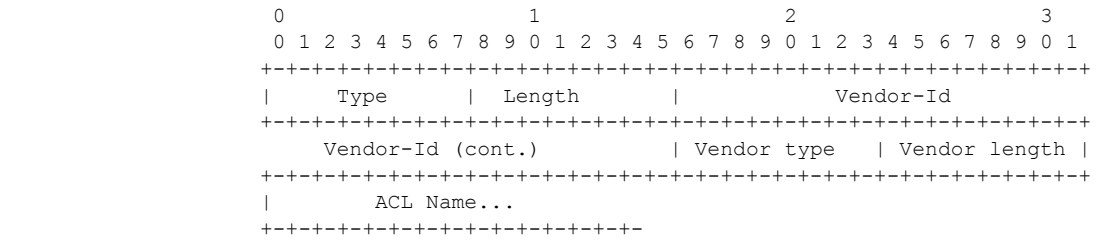


- Type - 26（ベンダー固有）
- Length – 10
- Vendor-Id – 14179
- Vendor type – 2

- Vendor length – 4
- Value – 3 オクテット：
  - 0 – Bronze（バックグラウンド）
  - 1 - Silver（ベストエフォート）
  - 2 – Gold（ビデオ）
  - 3 – Platinum（音声）

ACL-Name

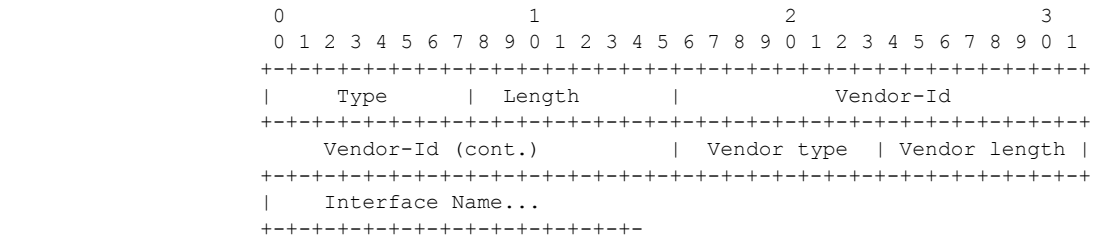
この属性は、クライアントに適用される ACL 名を示します。ACL-Name 属性形式の要約を次に示します。フィールドは左から右に伝送されます。



- Type - 26（ベンダー固有）
- Length – >7
- Vendor-Id – 14179
- Vendor type – 6
- Vendor length – >0
- Value - クライアントに対して使用する ACL の名前を含む文字列

Interface-Name

この属性は、クライアントが関連付けられる VLAN インターフェイスを示します。Interface-Name 属性形式の要約を次に示します。フィールドは左から右に伝送されます。



- Type - 26（ベンダー固有）
- Length – >7
- Vendor-Id – 14179
- Vendor type – 5
- Vendor length – >0
- Value - クライアントが割り当てられるインターフェイスの名前を含む文字列

（注）　この属性は、MAC フィルタリングが有効になっている場合、またはセキュリティ ポリシーとして 802.1X または WPA が使用されている場合にのみ機能します。

VLAN-Tag

この属性は、特定のトンネル セッションのグループ ID を示し、Tunnel-Private-Group-ID 属性とも呼ばれます。

この属性は、トンネルの発信側が、特定の接続からグループを事前に判別できる場合は Access-Request パケットに含めることができ、このトンネル セッションを特定のプライベート グループに属するものとして処理する場合は Access-Accept パケットに含める必要があります。プライベート グループは、トンネル セッションを特定のユーザのグループと関連付けるために使用できます。たとえば、未登録の IP アドレスが特定のインターフェイスを通過するようにするルーティングを容易にするために使用できます。Start と Stop のいずれかの値を持つ Acct-Status-Type 属性を含み、かつトンネル セッションに関連する Accounting-Request パケットには、プライベート グループを含める必要があります。

Tunnel-Private-Group-ID 属性形式の要約を次に示します。フィールドは左から右に伝送されます。

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|      Type     |    Length     |     Tag       |   String...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

- Type - 81（Tunnel-Private-Group-ID 用）
- Length – >= 3
- Tag - Tag フィールドは、長さが 1 オクテットで、同じパケット内の、同じトンネルを示す属性をグループ化するために使用されます。Tag フィールドの値が 0x00 より大きく、0x1F 以下である場合、（いくつかの選択肢のうちの）この属性が属するトンネルを示すと解釈されます。Tag フィールドが 0x1F より大きい場合、後続の String フィールドの最初のバイトとして解釈されます。
- String - このフィールドは必須です。グループはこの String フィールドによって表されます。グループ ID の形式に制約はありません。

トンネル属性

（注）　この項の他の RADIUS 属性（QoS-Level、ACL-Name、Interface-Name、または VLAN-Tag）のいずれかを返す場合、トンネル属性も返す必要があります。

RFC2868 では、認証と認可に使用される RADIUS トンネル属性が定義されています。RFC2867 では、アカウンティングに使用されるトンネル属性が定義されています。IEEE 802.1X Authenticator がトンネリングをサポートしている場合は、認証の結果としてサプリカントに対して強制的なトンネルをセットアップできます。

これは、特に、認証の結果に基づいて IEEE8021Q で定義されている特定のバーチャル LAN（VLAN）にポートを配置できるようにする場合に適しています。たとえば、これを使用すると、無線ホストが大学のネットワーク内で移動するときに同じ VLAN 上にとどまれるようになります。

RADIUS サーバは、一般的に、Access-Accept 内にトンネル属性を含めることによって目的の VLAN を示します。ただし、IEEE 802.1X Authenticator も、Access- Request 内にトンネル属性を含めることによってサプリカントに割り当てる VLAN に関するヒントを提供できます。

VLAN 割り当てのために、次のトンネル属性が使用されます。

- Tunnel-Type=VLAN（13）
- Tunnel-Medium-Type=802
- Tunnel-Private-Group-ID=VLANID

VLANID は 12 ビットであり、1 ～ 4094（両端の値を含む）の値をとることに注意してください。Tunnel-Private-Group-ID は、RFC2868 で定義されているように String 型なので、IEEE 802.1X で使用するために VLANID 整数値は文字列としてエンコードされます。

トンネル属性が送信されるときは、Tag フィールドに値が含まれている必要があります。RFC2868 の第 3.1 項には次のように明記されています。

- この Tag フィールドは長さが 1 オクテットであり、同じパケット内で同じトンネルを示す属性をグループ化する方法を提供することを目的としています。このフィールドの有効な値は、0x01 ～ 0x1F（両端の値を含む）です。この Tag フィールドが使用されない場合は、ゼロ（0x00）である必要があります。
- Tunnel-Client-Endpoint、Tunnel-Server-Endpoint、Tunnel-Private-Group-ID、Tunnel-Assignment-ID、Tunnel-Client-Auth-ID、または Tunnel-Server-Auth-ID 属性（ただし Tunnel-Type、Tunnel-Medium-Type、Tunnel-Password、Tunnel-Preference は含まない）で使用する場合、0x1F より大きい Tag フィールドは、次のフィールドの最初のオクテットと解釈されます。
- 代替トンネル タイプが提供されない場合（たとえば、トンネリングはサポートしているが VLAN はサポートしていない IEEE 802.1X Authenticator の場合）、トンネル属性に必要なのは 1 つのトンネルを指定することのみです。したがって、VLANID を指定することのみが目的の場合、すべてのトンネル属性の Tag フィールドをゼロ（0x00）に設定する必要があります。代替トンネル タイプが提供される場合は、0x01 ～ 0x1F のタグ値を選択する必要があります。

AAA Override の設定

WLAN の Allow AAA Override オプションを使用すると、WLAN で ID ネットワーキングを設定できます。これにより、AAA サーバから返される RADIUS 属性に基づいて、個々のクライアントに VLAN タギング、QoS、および ACL を適用できます。

（注） AAA Override のためにクライアントが新しいインターフェイスに移動したあと、そのインターフェイスに ACL を適用しても、クライアントが再認証されるまで ACL は有効になりません。この問題を回避するには、インターフェイス上ですでに設定された ACL にすべてのクライアントが接続するように、ACL を適用してから WLAN を有効にするか、クライアントが再認証されるように、インターフェイスを適用した後で WLAN を一旦無効にし、再び有効にします。

AAA Override を許可する設定の多くは、RADIUS サーバで実行されます。RADIUS サーバでは、コントローラに返すようにする上書きプロパティで、Access Control Server（ACS）を設定する必要があります。

コントローラでは、GUI または CLI を使用して、Allow AAA Override 設定パラメータを有効にするだけです。このパラメータを有効にすることにより、コントローラで RADIUS サーバから返される属性を受け入れるようになります。次にコントローラはそれらの属性をクライアントに適用します。

正しい QoS 値を取得するための RADIUS サーバ ディクショナリ ファイルの更新

Steel-Belted RADIUS（SBR）、FreeRadius、または同等の RADIUS サーバを使用している場合、AAA Override 機能を有効化した後、クライアントが正しい QoS 値を取得できないことがあります。ディクショナリ ファイルの編集を可能にするこれらのサーバについて、正しい QoS 値（Silver = 0、Gold = 1、Platinum = 2、Bronze = 3）を反映させてファイルを更新する必要があります。そのための手順は、次のとおりです。

（注）　この問題は、Cisco Secure Access Control Server（ACS）には適用されません。

ステップ 1　SBR サービス（または他の RADIUS サービス）を停止します。

ステップ 2　次のテキストを、ciscowlan.dct として Radius_Install_Directory¥Service フォルダに保存します。

```
################################################################################
# CiscoWLAN.dct- Cisco Wireless Lan Controllers
#
# (See README.DCT for more details on the format of this file)
################################################################################

# Dictionary - Cisco WLAN Controllers
#
# Start with the standard Radius specification attributes
#
@radius.dct
#
# Standard attributes supported by Airespace
#
# Define additional vendor specific attributes (VSAs)
#

MACRO Airespace-VSA(t,s) 26 [vid=14179 type1=%t% len1=+2 data=%s%]

ATTRIBUTE   WLAN-Id                 Airespace-VSA(1, integer)     cr
ATTRIBUTE   Aire-QoS-Level         Airespace-VSA(2, integer)     r
VALUE Aire-QoS-Level Bronze  3
VALUE Aire-QoS-Level Silver   0
VALUE Aire-QoS-Level Gold     1
VALUE Aire-QoS-Level Platinum 2

ATTRIBUTE   DSCP                    Airespace-VSA(3, integer)     r
ATTRIBUTE   802.1P-Tag              Airespace-VSA(4, integer)     r
ATTRIBUTE   Interface-Name          Airespace-VSA(5, string)      r
ATTRIBUTE   ACL-Name                Airespace-VSA(6, string)      r

# This should be last.

################################################################################
# CiscoWLAN.dct - Cisco WLC dictionary
################################################################################
```

ステップ 3　dictiona.dcm ファイルを（同じディレクトリに）開いて、行「@ciscowlan.dct.」を追加します。

ステップ 4　dictiona.dcm ファイルを保存して閉じます。

ステップ 5　vendor.ini ファイルを（同じでディレクトリに）開いて、次のテキストを追加します。

```
vendor-product       = Cisco WLAN Controller
dictionary           = ciscowlan
ignore-ports         = no
port-number-usage    = per-port-type
```

```
help-id              =
```

ステップ 6　vendor.ini ファイルを保存して閉じます。

ステップ 7　SBR サービス（または他の RADIUS サービス）を起動します。

ステップ 8　SBR アドミニストレータ（または他の RADIUS アドミニストレータ）を起動します。

ステップ 9　RADIUS クライアントを追加します（まだ追加されていない場合）。[Make/Model] ドロップダウン ボックスから [Cisco WLAN Controller] を選択します。

GUI を使用した AAA Override の設定

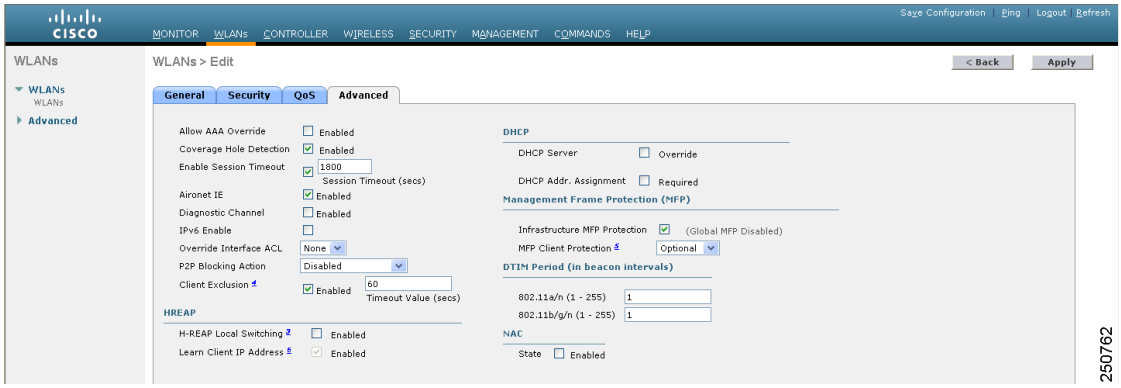
コントローラ GUI を使用して AAA Override を設定する手順は、次のとおりです。

ステップ 1　[WLANs] を選択して、[WLANs] ページを開きます。

ステップ 2　設定する WLAN の ID 番号をクリックします。[WLANs > Edit] ページが表示されます。

ステップ 3　[Advanced] タブを選択して、[WLANs > Edit] （[Advanced]）ページを開きます（図 5-42 を参照）。

図 5-42　[WLANs > Edit] （[Advanced]）ページ



ステップ 4　AAA Override の検証を有効にする場合は [Allow AAA Override] チェックボックスをオンにします。この機能を無効にする場合は、オフにします。デフォルト値は無効（disable）です。

ステップ 5　[Apply] をクリックして、変更を適用します。

ステップ 6　[Save Configuration] をクリックして、変更を保存します。

CLI を使用した AAA Override の設定

コントローラ CLI を使用して AAA Override を有効または無効にするには、次のコマンドを使用します。

config wlan aaa-override {**enable** | **disable**} *wlan_id*

wlan_id には、1 ～ 16 の ID を入力します。

不正なデバイスの管理

この項では、不正なデバイスに対するセキュリティ ソリューションについて説明します。不正なデバイスとは、ネットワーク内で管理対象のアクセス ポイントによって検出される、システムに属していない不明なアクセス ポイントまたはクライアントのことです。

問題

不正なアクセス ポイントは、正規のクライアントをハイジャックし、プレーンテキストまたは他の DoS 攻撃や man-in-the-middle 攻撃を使用して無線 LAN の運用を妨害する可能性があります。つまり、ハッカーは、不正なアクセス ポイントを使用することで、ユーザ名やパスワードなどの機密情報を入手することができます。すると、ハッカーは一連の Clear To Send（CTS; クリア ツー センド）フレームを送信できるようになります。アクセス ポイントになりすましてこの CTS フレームが送信され、特定のクライアントには伝送を許可し、他のすべてのクライアントには待機するように指示が送られると、正規のクライアントは、ネットワーク リソースに接続できなくなってしまいます。したがって、無線 LAN サービス プロバイダーは、境域からの不正なアクセス ポイントの締め出しに強い関心を持っています。

不正なアクセス ポイントは安価で簡単に利用できることから、企業の従業員は、IT 部門に報告して同意を得ることなく、許可されていない不正なアクセス ポイントを既存の LAN に接続し、アドホック無線ネットワークを確立することがあります。これらの不正なアクセス ポイントは、企業のファイアウォールの背後にあるネットワーク ポートに接続可能であるため、重大なネットワーク セキュリティ侵犯につながる恐れがあります。通常、従業員は不正なアクセス ポイントのセキュリティ設定を有効にしないので、権限のないユーザがこのアクセス ポイントを使って、ネットワーク トラフィックを傍受し、クライアント セッションをハイジャックすることは簡単です。さらに警戒すべきことは、セキュリティで保護されていないアクセス ポイントの場所が無線ユーザにより頻繁に公開されるため、企業のセキュリティが侵害される可能性も増大します。

不正なデバイスの検出

コントローラでは、すべての近隣のアクセス ポイントが継続的に監視されます。また、不正なアクセス ポイントおよびクライアントが自動的に検出されて、それらの情報が収集されます。コントローラで不正なアクセス ポイントが検出されると、Rogue Location Discovery Protocol （RLDP; 不正ロケーション検出プロトコル）を使用して、不正なアクセス ポイントがネットワークに接続されているかどうかが判定されます。

コントローラは、すべてのアクセス ポイント上で、または monitor（リッスン専用）モードに設定されたアクセス ポイント上でのみ RLDP を使用できるように設定できます。この後者のオプションでは、輻輳している RF 空間での不正なアクセス ポイントを簡単に自動検出できるようになります。そして、不要な干渉を生じさせたり、一定のデータ アクセス ポイント機能に影響を与えたりすることなく、監視を行えるようになります。すべてのアクセス ポイントで RLDP を使用するようにコントローラを設定した場合、モニタ アクセス ポイントとローカル（データ）アクセス ポイントの両方が近くにあると、コントローラでは常に RLDP 動作に対してモニタ アクセス ポイントが選択されます。ネットワーク上に不正があると RLDP で判断された場合は、検出された不正を手動で阻止することも、自動的に阻止することもできます。

不正なアクセス ポイントの分類

コントローラ ソフトウェア リリース 5.0 以降では、不正なアクセス ポイントの分類および報告機能が強化されており、不正なアクセス ポイントがユーザ定義のルールに従って特定の不正の状態に分類され、ある状態から別の状態に自動的に移行できるようになっています。以前のリリースでは、MAC アドレスまたは BSSID によってソートされた不正なアクセス ポイントが 1 ページにまとめてコントローラに表示されていました。このリリースでは、不正なアクセス ポイントを Friendly、Malicious、または Unclassified に分類してコントローラに表示するルールを作成できます。

デフォルトでは、いずれの分類ルールも有効になっていません。したがって、すべての不明なアクセス ポイントは Unclassified に分類されます。ルールを作成し、その条件を設定して、ルールを有効にすると、未分類のアクセス ポイントは分類し直されます。ルールを変更するたびに、Alert 状態のみのすべてのアクセス ポイント（Friendly、Malicious、および Unclassified）にそのルールが適用されます。

（注） ルール ベースの分類は、アドホック不正クライアントおよび不正クライアントには適用されません。

（注） 5500 シリーズ コントローラは最大で 2000 個の不正（確認応答の不正など）に対応します。4400 シリーズ コントローラ、Cisco WiSM、および Catalyst 3750G 統合型無線 LAN コントローラ スイッチは最大で 625 個の不正に対応します。2100 シリーズ コントローラおよびサービス統合型ルータのコントローラ ネットワーク モジュールは最大で 125 個の不正に対応します。各コントローラは、不正阻止数を無線あたり 3 つに（または監視モードのアクセス ポイントでは無線あたり 6 つに）制限します。

コントローラは、管理対象のアクセス ポイントの 1 つから不正レポートを受信すると、次のように応答します。

1. コントローラは不明なアクセス ポイントが危険性のない MAC アドレスのリストに含まれているか確認します。そのリストに含まれている場合、コントローラはアクセス ポイントを Friendly として分類します。
2. 不明なアクセス ポイントが危険性のない MAC アドレスのリストに含まれていない場合、コントローラは、不正の状態の分類ルールを適用します。
3. 不正なアクセス ポイントが Malicious、Alert または Friendly、Internal または External にすでに分類されている場合は、コントローラはそのアクセス ポイントを自動的に分類しません。不正なアクセス ポイントがそれ以外に分類されており、Alert 状態にある場合に限り、コントローラはそのアクセス ポイントを自動的に分類し直します。
4. コントローラは、優先度の一番高いルールを適用します。不正なアクセス ポイントがルールで指定された条件に一致すると、コントローラはそのアクセス ポイントをルールに設定された分類タイプに基づいて分類します。
5. 不正なアクセス ポイントが設定されたルールのいずれにも一致しないと、コントローラはそのアクセス ポイントを Unclassified に分類します。
6. コントローラは、すべての不正なアクセス ポイントに対して上記の手順を繰り返します。
7. 不正なアクセス ポイントがネットワーク上にあると RLDP で判断されると、ルールが設定されていない場合でも、コントローラは不正の状態を Threat とマークし、そのアクセス ポイントを自動的に Malicious に分類します。その後、不正なアクセス ポイントを手動で阻止することができますが（不正を自動的に阻止するよう RLDP が設定されていない限り）、その場合は不正の状態が Contained に変更されます。不正なアクセス ポイントがネットワーク上にないと、コントローラによって不正の状態が Alert とマークされ、そのセス ポイントを手動で阻止できるようになります。
8. アクセス ポイントは、必要に応じて、異なる分類タイプや不正の状態に手動で移動できます。

表 5-8 に、特定の分類タイプの不正なアクセス ポイントに適用される不正の状態を示します。

表 5-8　　分類マッピング

ルール ベースの分類タイプ	不正の状態
Friendly	• Internal：不明なアクセス ポイントがネットワーク内に存在し、WLAN のセキュリティに脅威を与えない場合、手動で Friendly、Internal に設定します。たとえば、ラボ ネットワーク内のアクセス ポイントなどです。 • External：不明なアクセス ポイントがネットワーク外に存在し、WLAN のセキュリティに脅威を与えない場合、手動で Friendly、External に設定します。たとえば、近所のコーヒーショップ設置されているアクセス ポイントなどです。 • Alert：不明なアクセス ポイントがネイバー リストまたはユーザが設定した危険性のない MAC のリストに記載されていない場合、そのアクセス ポイントは Alert に移動されます。
Malicious	• Alert：不明なアクセス ポイントがネイバー リストまたはユーザが設定した危険性のない MAC のリストに記載されていない場合、そのアクセス ポイントは Alert に移動されます。 • Threat：不明なアクセス ポイントがネットワーク上に発見され、WLAN のセキュリティに脅威を与えています。 • Contained：不明なアクセス ポイントが阻止されています。 • Contained Pending：不明なアクセス ポイントが Contained とマークされましたが、リソースを使用できないため対処が遅れています。
Unclassified	• Pending：最初の検出で、不明なアクセス ポイントは 3 分間 Pending 状態に置かれます。この間に、管理対象のアクセス ポイントでは、不明なアクセス ポイントがネイバー アクセス ポイントであるかどうかが判定されます。 • Alert：不明なアクセス ポイントがネイバー リストまたはユーザが設定した危険性のない MAC のリストに記載されていない場合、そのアクセス ポイントは Alert に移動されます。 • Contained：不明なアクセス ポイントが阻止されています。 • Contained Pending：不明なアクセス ポイントが Contained とマークされましたが、リソースを使用できないため対処が遅れています。

コントローラ ソフトウェア リリース 5.0 にアップグレードした場合は、不正なアクセス ポイントの分類と状態は次のように再設定されます。

- Known から Friendly、Internal
- Acknowledged から Friendly、External
- Contained から Malicious、Contained

前述のように、コントローラでは、ユーザ定義のルールに基づいて不明なアクセス ポイントの分類タイプと不正の状態が自動的に変更されます。または、不明なアクセス ポイントを異なる分類タイプと不正の状態に手動で移動できます。表 5-9 に、不明なアクセス ポイントに設定できる分類タイプや不正の状態の推移を示します。

表 5-9　設定可能な分類タイプ/不正の状態の推移

推移前	推移後
Friendly（Internal、External、Alert）	Malicious（Alert）
Friendly（Internal、External、Alert）	Unclassified（Alert）
Friendly（Alert）	Friendly（Internal、External）
Malicious（Alert、Threat）	Friendly（Internal、External）
Malicious（Contained、Contained Pending）	Malicious（Alert）
Unclassified（Alert、Threat）	Friendly（Internal、External）
Unclassified（Contained、Contained Pending）	Unclassified（Alert）
Unclassified（Alert）	Malicious（Alert）

不正の状態が Contained の場合、不正なアクセス ポイントの分類タイプを変更する前に、そのアクセス ポイントが阻止されないようにする必要があります。不正なアクセス ポイントを Malicious から Unclassified に移動する場合は、そのアクセス ポイントを削除して、コントローラで分類し直せるようにする必要があります。

WCS 相互作用

WCS ソフトウェア リリース 5.0 以降でも、ルール ベースの分類がサポートされています。WCS では、コントローラ上で設定された分類ルールが使用されます。次のイベント後に、コントローラから WCS にトラップが送信されます。

- 最初に不明なアクセス ポイントが Friendly に移動した場合に、不正の状態が Alert であると、コントローラから WCS にトラップが送信されます。不正の状態が Internal または External であると、トラップは送信されません。
- タイムアウトの経過後に不正なエントリが移動した場合、Malicious（Alert、Threat）または Unclassified（Alert）に分類された不正なアクセス ポイントに関して、コントローラから WCS にトラップが送信されます。コントローラでは、不正の状態が Contained、Contained Pending、Internal、および External である不正なエントリは削除されません。

RLDP の設定

コントローラの GUI または CLI を使用して、不正なデバイスを自動的に検出および阻止するように RLDP を設定できます。

GUI を使用した RLDP の設定

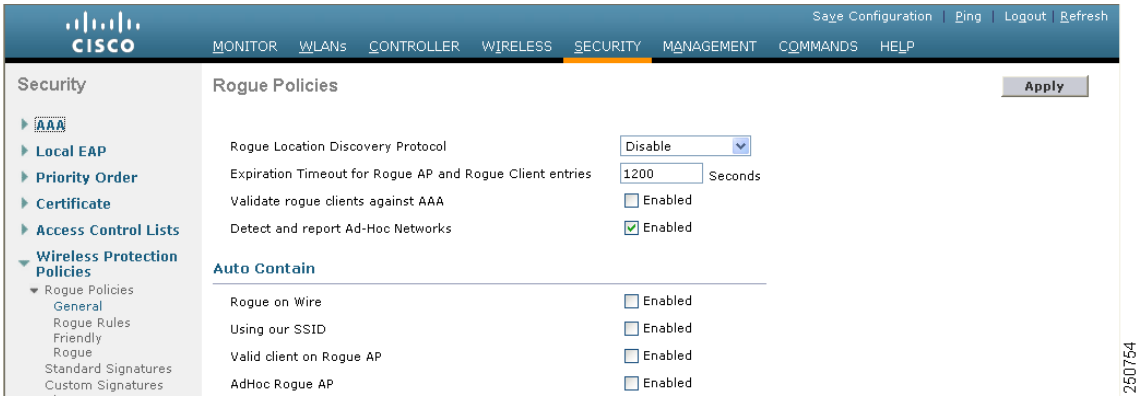
コントローラの GUI を使用して RLDP を設定する手順は、次のとおりです。

ステップ 1　必要なアクセス ポイントで不正検出が有効になっていることを確認します。コントローラに接続されたすべてのアクセス ポイントに対し、不正の検出がデフォルトで有効にされます（OfficeExtend アクセス ポイントを除く）。ただし、コントローラ ソフトウェア リリース 6.0 では、個々のアクセス ポイントについて不正の検出を有効または無効にすることができます。それには、[All APs > Details for]（[Advanced]）ページで [Rogue Detection] チェックボックスをオンまたはオフにします。

（注）　家庭の環境で展開されるアクセス ポイントは大量の不正デバイスを検出する可能性が高いため、OfficeExtend アクセス ポイントでは不正検出はデフォルトでは無効です。

ステップ 2　[Security] > [Wireless Protection Policies] > [Rogue Policies] > [General] を順に選択して、[Rogue Policies] ページを開きます（図 5-43 を参照）。

図 5-43　[Rogue Policie] ページ



ステップ 3　[Rogue Location Discovery Protocol] ドロップダウン ボックスから、次のオプションのいずれかを選択します。

- [Disable]：すべてのアクセス ポイント上で RLDP を無効にします。これはデフォルト値です。
- [All APs]：すべてのアクセス ポイント上で RLDP を有効にします。
- [Monitor Mode APs]：監視モードのアクセス ポイント上でのみ RLDP を有効にします。

ステップ 4　[Expiration Timeout for Rogue AP and Rogue Client Entries] フィールドに、不正なアクセス ポイントとクライアント エントリの期限が切れてリストから削除されるまでの秒数を入力します。有効な範囲は 240 ～ 3600 秒で、デフォルト値は 1200 秒です。

（注）　不正なアクセス ポイントまたはクライアントのエントリがタイムアウトすると、その不正の状態がいずれの分類タイプに対しても Alert または Threat である場合には、コントローラから削除されます。

ステップ 5　必要に応じて、[Validate Rogue Clients Against AAA] チェックボックスをオンにし、AAA サーバまたはローカル データベースを使用して、不正なクライアントが有効なクライアントかどうかを検証します。デフォルトではオフになっています。

ステップ 6　必要に応じて、[Detect and Report Ad-Hoc Networks] チェックボックスをオンにして、アドホック不正検出および報告を有効にします。デフォルト値はオンです。

ステップ 7　特定の不正なデバイスをコントローラで自動的に阻止するには、次のチェックボックスをオンにします。それ以外の場合は、このチェックボックスをオフのままにします（デフォルト値）。

注意　次のパラメータのいずれかを有効にすると、「Using this feature may have legal consequences. Do you want to continue?」という警告メッセージが表示されます。工業、科学、医療用（ISM）帯域の 2.4 GHz および 5 GHz の周波数は一般に解放されているので、ライセンスなしで使用できます。したがって、別の関係者のネットワーク上のデバイスを阻止することには、法的責任が発生する場合があります。

- [Rogue on Wire]：有線ネットワークで検出された不正を自動的に阻止します。
- [Using Our SSID]：ネットワークの SSID をアドバタイズする不正を自動的に阻止します。このパラメータをオフにしておくと、該当する不正が検出されても警告が生成されるだけです。
- [Valid Client on Rogue AP]：信頼できるクライアントのアソシエート先の不正なアクセス ポイントを自動的に阻止します。このパラメータをオフにしておくと、該当する不正が検出されても警告が生成されるだけです。
- [AdHoc Rogue AP]：コントローラによって検出されたアドホック ネットワークを自動的に阻止します。このパラメータをオフにしておくと、該当するネットワークが検出されても警告が生成されるだけです。

ステップ 8　[Apply] をクリックして、変更を適用します。

ステップ 9　[Save Configuration] をクリックして、変更を保存します。

CLI を使用した RLDP の設定

コントローラの CLI を使用して RLDP を設定する手順は、次のとおりです。

ステップ 1　必要なアクセス ポイントで不正検出が有効になっていることを確認します。コントローラに接続されたすべてのアクセス ポイントに対し、不正の検出がデフォルトで有効にされます（OfficeExtend アクセス ポイントを除く）。ただし、コントローラ ソフトウェア リリース 6.0 では、**config rogue detection** {**enable** | **disable**} *Cisco_AP* コマンドを入力することにより、個々のアクセス ポイントに対して設定を有効または無効にすることができます。

（注）　特定のアクセス ポイントについて、不正検出の現在の設定状態を確認するには、**show ap config general** *Cisco_AP* コマンドを入力します。

（注）　家庭の環境で展開されるアクセス ポイントは大量の不正デバイスを検出する可能性が高いため、OfficeExtend アクセス ポイントでは不正検出はデフォルトでは無効です。

ステップ 2　RLDP を有効、無効、または開始するには、次のコマンドを入力します。

- **config rogue ap rldp enable alarm-only**:すべてのアクセス ポイント上で RLDP を有効にします。
- **config rogue ap rldp enable alarm-only** *monitor_ap_only*：監視モードのアクセス ポイント上でのみ RLDP を有効にします。
- **config rogue ap rldp initiate** *rogue_mac_address*：特定の不正なアクセス ポイント上で RLDP を開始します。
- **config rogue ap rldp disable**：すべてのアクセス ポイント上で RLDP を無効にします。

ステップ 3　不正なアクセス ポイントとクライアント エントリの期限が切れてリストから削除されるまでの秒数を指定するには、次のコマンドを入力します。

config rogue ap timeout *seconds*

seconds の有効な値の範囲は 240 ～ 3600 秒（両端の値を含む）で、デフォルト値は 1200 秒です。

（注）　不正なアクセス ポイントまたはクライアントのエントリがタイムアウトになると、その不正の状態がいずれの分類タイプに対しても Alert または Threat である場合には、コントローラから削除されます。

ステップ 4　アドホック不正検出および報告を有効または無効にするには、次のコマンドを入力します。

config rogue adhoc {**enable** | **disable**}

ステップ 5　AAA サーバまたはローカル データベースを有効または無効して、不正なクライアントが有効なクライアントかどうかを検証するには、次のコマンドを入力します。

config rogue client aaa {**enable** | **disable**}

ステップ 6　特定の不正なデバイスをコントローラで自動的に阻止するには、次のコマンドを入力します。

注意　次のコマンドのいずれかを入力すると、「Using this feature may have legal consequences. Do you want to continue?」という警告メッセージが表示されます。工業、科学、医療用（ISM）帯域の 2.4 GHz および 5 GHz の周波数は一般に解放されているので、ライセンスなしで使用できます。したがって、別の関係者のネットワーク上のデバイスを阻止することには、法的責任が発生する場合があります。

- **config rogue ap rldp enable auto-contain**：有線ネットワークで検出された不正を自動的に阻止します。
- **config rogue ap ssid auto-contain**：ネットワークの SSID をアドバタイズする不正を自動的に阻止します。

  （注）　該当する不正が検出されたときに警告だけが生成されるようにするには、**config rogue ap ssid alarm** コマンドを入力します。

- **config rogue ap valid-client auto-contain**：信頼できるクライアントのアソシエート先の不正なアクセス ポイントを自動的に阻止します。

  （注）　該当する不正が検出されたときに警告だけが生成されるようにするには、**config rogue ap valid-client alarm** コマンドを入力します。

- **config rogue adhoc auto-contain**：コントローラによって検出されたアドホック ネットワークを自動的に阻止します。

  （注）　該当する不正が検出されたときに警告だけが生成されるようにするには、**config rogue adhoc alert** コマンドを入力します。

ステップ 7　変更を保存するには、次のコマンドを入力します。

save config

不正分類ルールの設定

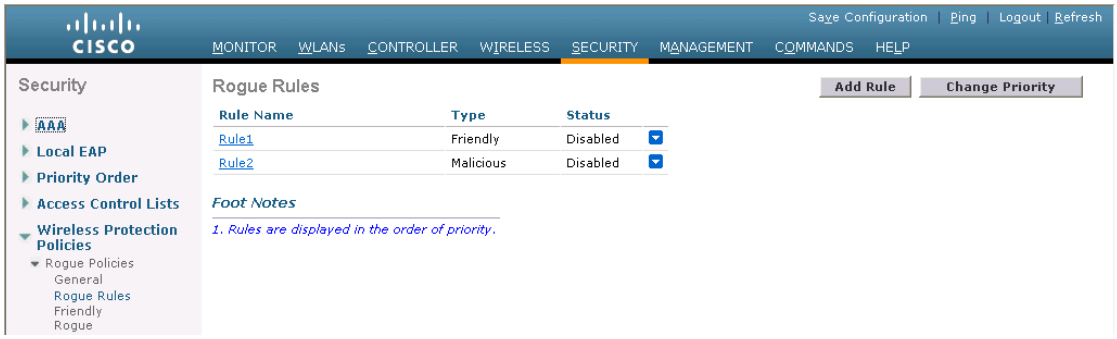
コントローラの GUI または CLI を使用して、1 つのコントローラにつき最大 64 の不正分類ルールを設定できます。

GUI を使用した不正分類ルールの設定

コントローラの GUI を使用して不正分類ルールを設定する手順は、次のとおりです。

ステップ 1　[Security] > [Wireless Protection Policies] > [Rogue Policies] > [Rogue Rules] を選択して、[Rogue Rules] ページを開きます（図 5-44 を参照）。

図 5-44　[Rogue Rules] ページ



すでに作成されているすべてのルールが優先順位に従って一覧表示されます。各ルールの名前、タイプ、およびステータスが表示されます。

（注）　ルールを削除するには、そのルールの青いドロップダウンの矢印の上にカーソルを置いて、[Remove] をクリックします。

ステップ 2　新しいルールを作成する手順は、次のとおりです。

a. [Add Rule] をクリックします。[Add Rule] セクションがページ上部に表示されます。

b. [Rule Name] フィールドに、新しいルールの名前を入力します。名前にはスペースを含めないでください。

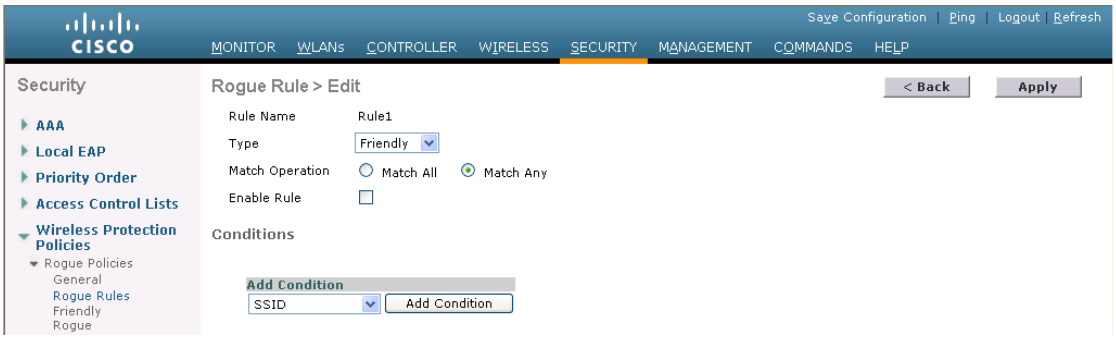
c. [Rule Type] ドロップダウン ボックスで、[Friendly] または [Malicious] を選択して、このルールと一致する不正なアクセス ポイントを Friendly または Malicious に分類します。

d. [Add] をクリックして既存のルール リストにこのルールを追加するか、[Cancel] をクリックしてこの新しいルールを破棄します。

ステップ 3　ルールを編集する手順は、次のとおりです。

a. 編集するルールの名前をクリックします。[Rogue Rule > Edit] ページが表示されます（図 5-45 を参照）。

図 5-45　[Rogue Rule > Edit] ページ



b. [Type] ドロップダウン ボックスで、[Friendly] または [Malicious] を選択して、このルールと一致する不正なアクセス ポイントを Friendly または Malicious に分類します。

c. [Match Operation] フィールドで、次のいずれかを選択します。

- [Match All]：このルールが有効な場合、検出された不正なアクセス ポイントは、ルールで指定されたすべての条件を満たしている場合にルールと一致し、ルールの分類タイプが不正なアクセス ポイントに適用されます。
- [Match Any]：このルールが有効な場合、検出された不正なアクセス ポイントは、ルールで指定された条件のいずれかを満たす場合にルールと一致し、ルールの分類タイプが不正なアクセス ポイントに適用されます。これはデフォルト値です。

d. このルールを有効にするには、[Enable Rule] チェックボックスをオンにします。デフォルトではオフになっています。

e. [Add Condition] ドロップダウン ボックスで、不正なアクセス ポイントが満たす必要がある次の条件から 1 つまたは複数を選択し、[Add Condition] をクリックします。

- [SSID]：不正なアクセス ポイントには、特定のユーザ設定 SSID が必要です。このオプションを選択する場合は、[User Configured SSID] フィールドに SSID を入力して、[Add SSID] をクリックします。

（注）　SSID を削除するには、SSID を強調表示して [Remove] をクリックします。

- [RSSI]：不正なアクセス ポイントには、最小の Received Signal Strength Indicator（RSSI; 受信信号強度インジケータ）値が必要です。たとえば、不正なアクセス ポイントが設定値より大きい RSSI を持つ場合、そのアクセス ポイントは Malicious に分類されます。このオプションを選択する場合は、[Minimum RSSI] フィールドに最小 RSSI 値を入力します。有効な値の範囲は -95 ～ -50 dBm（両端の値を含む）で、デフォルト値は 0 dBm です。
- [Duration]：不正なアクセス ポイントが最小期間検出される必要があります。このオプションを選択する場合は、[Time Duration] フィールドに最小検出期間の値を入力します。有効な値の範囲は 0 ～ 3600 秒（両端の値を含む）で、デフォルト値は 0 秒です。
- [Client Count]：不正なアクセス ポイントに最小数のクライアントがアソシエートされている必要があります。たとえば、不正なアクセス ポイントにアソシエートされたクライアントの数が設定値以上の場合、アクセス ポイントは Malicious に分類されます。このオプションを選択する場合は、[Minimum Number of Rogue Clients] フィールドに不正なアクセス ポイントにアソシエートされたクライアントの最小数を入力します。有効な値の範囲は 1 ～ 10（両端の値を含む）で、デフォルト値は 0 です。

- [No Encryption]：不正なアクセス ポイントのアドバタイズされた WLAN で暗号化が無効になっている必要があります。不正なアクセス ポイントの暗号化が無効になっている場合、より多くのクライアントがそのアクセス ポイントに対してアソシエートを試行します。このオプションに関して、これ以外の設定を行う必要はありません。

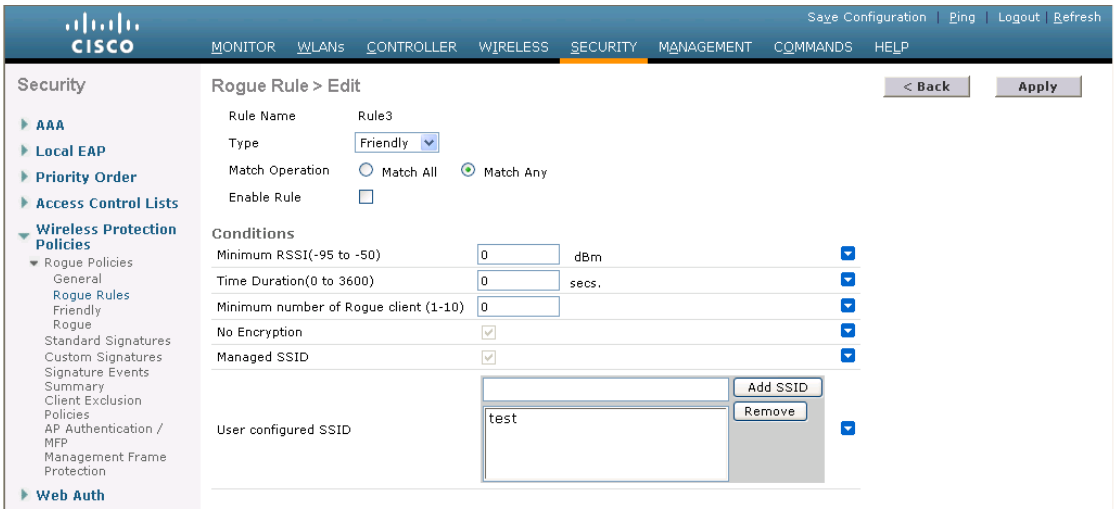
（注）　WCS では、このオプションは「オープン認証」と呼ばれます。

- [Managed SSID]：不正なアクセス ポイントの管理対象 SSID（WLAN に対して設定された SSID）がコントローラで認識されている必要があります。このオプションに関して、これ以外の設定を行う必要はありません。

（注）　SSID および管理対象 SSID の 2 つのリストは相互に排他的であるため、[SSID] および [Managed SSID] の条件を [Match All] 操作で使用することはできません。[Match All] を使用してルールを定義し、これら 2 つの条件を設定した場合は、いずれかの条件が満たされないので、不正なアクセス ポイントが Friendly または Malicious に分類されることはありません。

1 つのルールにつき最大 6 つの条件を追加できます。条件を追加すると、[Conditions] セクションに表示されます（図 5-46 を参照）。

図 5-46　[Rogue Rule > Edit] ページ



（注）　条件を削除するには、その条件の青いドロップダウンの矢印の上にカーソルを置いて、[Remove] をクリックします。

f. [Apply] をクリックして、変更を適用します。

ステップ 4　[Save Configuration] をクリックして、変更を保存します。

ステップ 5　不正分類ルールを適用する順序を変更する場合の手順は、次のとおりです。

a. [Back] をクリックして、[Rogue Rules] ページに戻ります。

b. [Change Priority] をクリックして、[Rogue Rules > Priority] ページにアクセスします（図 5-47 を参照）。

図 5-47　[Rogue Rules > Priority] ページ

不正ルールが優先順位に従って [Change Rules Priority] 編集ボックスに表示されます。

c. 優先順位を変更するルールを強調表示し、[Up] をクリックしてリスト内の順位を上げるか、[Down] をクリックしてリスト内の順位を下げます。

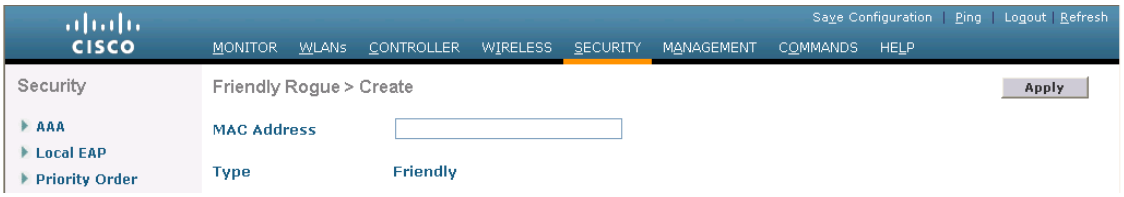
d. 目的の順位になるまで、ルールを上または下に移動します。

e. [Apply] をクリックして、変更を適用します。

ステップ 6　不正なアクセス ポイントを Friendly に分類して危険性のない MAC アドレスのリストに追加する場合の手順は、次のとおりです。

a. [Security] > [Wireless Protection Policies] > [Rogue Policies] > [Friendly Rogue] の順に選択して、[Friendly Rogue > Create] ページにアクセスします（図 5-48 を参照）。

図 5-48　[Friendly Rogue > Create] ページ



b. [MAC Address] フィールドに、危険性のない不正なアクセス ポイントの MAC アドレスを入力します。

c. [Apply] をクリックして、変更を適用します。

d. [Save Configuration] をクリックして、変更を保存します。このアクセス ポイントは、コントローラの、危険性のないアクセス ポイントのリストに追加され、[Friendly Rogue APs] ページに表示されます。

CLI を使用した不正分類ルールの設定

コントローラの CLI を使用して不正分類ルールを設定する手順は、次のとおりです。

ステップ 1　ルールを作成するには、次のコマンドを入力します。

config rogue rule add ap priority *priority* **classify** {**friendly** | **malicious**} *rule_name*

（注）　後からこのルールの優先順位を変更し、それに伴ってリスト内の他のルールの順番を変更する場合は、**config rogue rule priority** *priority rule_name* コマンドを入力します。後からこのルールの分類を変更する場合は、**config rogue rule classify** {**friendly** | **malicious**} *rule_name* コマンドを入力します。

（注）　すべての不正分類ルール、または特定のルールを削除するには、**config rogue rule delete** {**all** | *rule_name*} コマンドを入力します。

ステップ 2　すべてのルールまたは特定のルールを無効にするには、次のコマンドを入力します。

config rogue rule disable {**all** | *rule_name*}

（注）　ルールの属性を変更する前にルールを無効にする必要があります。

ステップ 3　不正なアクセス ポイントが満たす必要があるルールに条件を追加するには、次のコマンドを入力します。

config rogue rule condition ap set *condition_type condition_value rule_name*

condition_type は、次のいずれかです。

- **ssid**：不正なアクセス ポイントには、特定の SSID が必要です。コントローラによって管理されない SSID を追加する必要があります。このオプションを選択する場合は、*condition_value* パラメータに SSID を入力します。SSID はユーザ設定の SSID リストに追加されます。

  （注）　ユーザ設定の SSID リストからすべての SSID または特定の SSID を削除するには、**config rogue rule condition ap delete ssid** {**all** | *ssid*} *rule_name* コマンドを入力します。

- **rssi**：不正なアクセス ポイントには、最小の RSSI 値が必要です。たとえば、不正なアクセス ポイントが設定値より大きい RSSI を持つ場合、そのアクセス ポイントは Malicious に分類されます。このオプションを選択する場合は、*condition_value* パラメータに最小 RSSI 値を入力します。有効な値の範囲は -95 ～ -50 dBm（両端の値を含む）で、デフォルト値は 0 dBm です。
- **duration**：不正なアクセス ポイントが最小期間検出される必要があります。このオプションを選択する場合は、*condition_value* パラメータに最小検出期間の値を入力します。有効な値の範囲は 0 ～ 3600 秒（両端の値を含む）で、デフォルト値は 0 秒です。
- **client-count**：不正なアクセス ポイントに最小数のクライアントがアソシエートされている必要があります。たとえば、不正なアクセス ポイントにアソシエートされたクライアントの数が設定値以上の場合、アクセス ポイントは Malicious に分類されます。このオプションを選択する場合は、*condition_value* パラメータに不正なアクセス ポイントにアソシエートされたクライアントの最小数を入力します。有効な値の範囲は 1 ～ 10（両端の値を含む）で、デフォルト値は 0 です。
- **no-encryption**：不正なアクセス ポイントのアドバタイズされた WLAN で暗号化が無効になっている必要があります。このオプションには *condition_value* パラメータは必要ありません。
- **managed-ssid**：不正なアクセス ポイントの SSID がコントローラで認識されている必要があります。このオプションには *condition_value* パラメータは必要ありません。

（注）　1 つのルールにつき最大 6 つの条件を追加できます。ルールからすべての条件または特定の条件を削除するには、**config rogue rule condition ap delete** {**all** | *condition_type*} *condition_value rule_name* コマンドを入力します。

ステップ 4　検出された不正なアクセス ポイントで、そのルールで指定された条件のすべてまたはいずれかが満たされた場合にルールと一致したことになるよう指定し、そのアクセス ポイントにルールの分類タイプが適用されるようにするには、次のコマンドを入力します。

config rogue rule match {**all** | **any**} *rule_name*

ステップ 5　すべてのルールまたは特定のルールを有効にするには、次のコマンドを入力します。

config rogue rule enable {**all** | *rule_name*}

（注）　変更を有効にするには、ルールを有効にする必要があります。

ステップ 6　新しい危険性のないアクセス ポイント エントリを危険性のない MAC アドレスのリストに追加したり、リストから既存の危険性のないアクセス ポイント エントリを削除したりするには、次のコマンドを入力します。

config rogue ap friendly {**add** | **delete**} *ap_mac_address*

ステップ 7　変更を保存するには、次のコマンドを入力します。

save config

ステップ 8　コントローラ上に設定されている不正分類ルールを表示するには、次のコマンドを入力します。

show rogue rule summary

次のような情報が表示されます。

```
Priority Rule Name  State      Type        Match  Hit Count
-------- ---------- -------- ------------ ------ ---------
1        Rule1      Disabled   Friendly      Any   0
2        Rule2      Enabled    Malicious     Any  339
3       Rule3      Disabled   Friendly     Any   0
```

ステップ 9　特定の不正分類ルールの詳細情報を表示するには、次のコマンドを入力します。

show rogue rule detailed *rule_name*

次のような情報が表示されます。

```
Priority..................................... 2
Rule Name.................................... Rule2
State........................................ Enabled
Type......................................... Malicious
Match Operation.............................. Any
Hit Count.................................... 352
Total Conditions............................. 6
Condition 1
    type..................................... Client-count
    value.................................... 10
Condition 2
    type..................................... Duration
    value (seconds).......................... 2000
Condition 3
    type..................................... Managed-ssid
    value.................................... Enabled
Condition 4
    type..................................... No-encryption
```

```
    value..................................... Enabled
Condition 5
    type...................................... Rssi
    value (dBm)............................... -50
Condition 6
    type...................................... Ssid
    SSID Count................................ 1
    SSID 1.................................... test
```

不正なデバイスの表示および分類

コントローラの GUI または CLI を使用して、不正なデバイスを表示し、コントローラによって実行されるべき処理を決定することができます。

注意　不正なデバイスを阻止することを選択すると、「There may be legal issues following this containment. Are you sure you want to continue?」という警告メッセージが表示されます。工業、科学、医療用（ISM）帯域の 2.4 GHz および 5 GHz の周波数は一般に解放されているので、ライセンスなしで使用できます。したがって、別の関係者のネットワーク上のデバイスを阻止することには、法的責任が発生する場合があります。

GUI を使用した不正なデバイスの表示および分類

コントローラの GUI を使用して、不正なデバイスを表示および分類する手順は、次のとおりです。

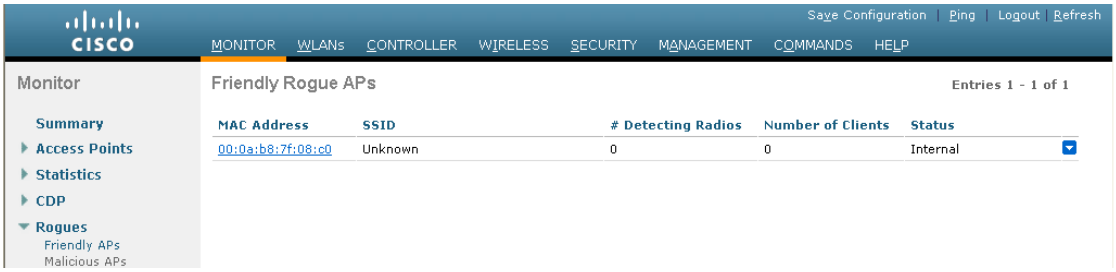
ステップ 1　[Monitor] > [Rogues] の順に選択します。

ステップ 2　次のオプションを選択すると、コントローラで検出された各タイプの不正なアクセス ポイントを表示できます。

- [Friendly APs]
- [Malicious APs]
- [Unclassified APs]

次のようなページが表示されます（図 5-49 を参照）。

図 5-49　[Friendly Rogue APs] ページ



[Friendly Rogue APs] ページ、[Malicious Rogue APs] ページ、および [Unclassified Rogue APs] ページには、不正なアクセス ポイントの MAC アドレスと SSID、不正なアクセス ポイントに接続されたクライアント数、不正なアクセス ポイントが検出された無線の数、および不正なアクセス ポイントの現在のステータスといった情報が表示されます。

（注）　これらのいずれかのページから不正なアクセス ポイントを削除するには、青いドロップダウンの矢印の上にカーソルを置いて、[Remove] をクリックします。

ステップ 3　不正なアクセス ポイントの詳細を取得するには、アクセス ポイントの MAC アドレスをクリックします。[Rogue AP Detail] ページが表示されます（図 5-50 を参照）。

図 5-50　[Rogue AP Detail] ページ

このページには、不正なデバイスの MAC アドレス、不正なデバイスのタイプ（アクセス ポイントなど）、不正なデバイスが有線ネットワーク上にあるかどうか、不正なデバイスが最初および最後に報告された日時、デバイスの現在のステータスといった情報が表示されます。

ステップ 4　[Class Type] フィールドには、この不正なアクセス ポイントの現在の分類が表示されます。

- [Friendly]：ユーザ定義の Friendly ルールと一致した不明なアクセス ポイント、または既知の不正なアクセス ポイント。危険性のないアクセス ポイントは阻止することができません。
- [Malicious]：ユーザ定義の Malicious ルールと一致した不明なアクセス ポイント、またはユーザが Friendly または Unclassified 分類タイプから手動で移動した不明なアクセス ポイント。

（注）　アクセス ポイントが Malicious に分類されると、その後でそのアクセス ポイントにルールを適用することはできなくなります。また、別の分類タイプに移動することもできません。危険性のあるアクセス ポイントを Unclassified 分類タイプに移動する場合は、そのアクセス ポイントを削除して、コントローラで分類し直せるようにする必要があります。

- [Unclassified]：ユーザ定義の Friendly または Malicious ルールと一致しない不明なアクセス ポイント。未分類のアクセス ポイントは阻止することができます。また、このアクセス ポイントは、ユーザ定義のルールに従って自動的に、またはユーザが手動で、Friendly または Malicious 分類タイプに移動できます。

このデバイスの分類を変更するには、[Class Type] ドロップダウン ボックスから別の分類を選択します。

（注）　不正なアクセス ポイントの現在の状態が [Contain] である場合、そのアクセス ポイントは移動できません。

ステップ 5　[Update Status] ドロップダウン ボックスから、次のオプションの 1 つを選択して、この不正なアクセス ポイントに対するコントローラの応答方法を指定します。

- [Internal]：コントローラはこの不正なアクセス ポイントを信頼します。このオプションは、[Class Type] が [Friendly] に設定されている場合に使用できます。
- [External]：コントローラはこの不正なアクセス ポイントの存在を認識します。このオプションは、[Class Type] が [Friendly] に設定されている場合に使用できます。
- [Contain]：コントローラによって危険性のあるデバイスが阻止され、そのデバイスの信号が、認証されたクライアントに干渉しないようになります。このオプションは、[Class Type] が [Malicious] または [Unclassified] に設定されている場合に使用できます。
- [Alert]：コントローラからシステム管理者に、さらなる処理を行うよう即時に警告が転送されます。このオプションは、[Class Type] が [Malicious] または [Unclassified] に設定されている場合に使用できます。

ページの下部には、この不正なアクセス ポイントが検出されたアクセス ポイントと、不正なアクセス ポイントにアソシエートされたすべてのクライアントの両方に関する情報が提供されます。クライアントの詳細を表示するには、[Edit] をクリックして [Rogue Client Detail] ページを開きます。

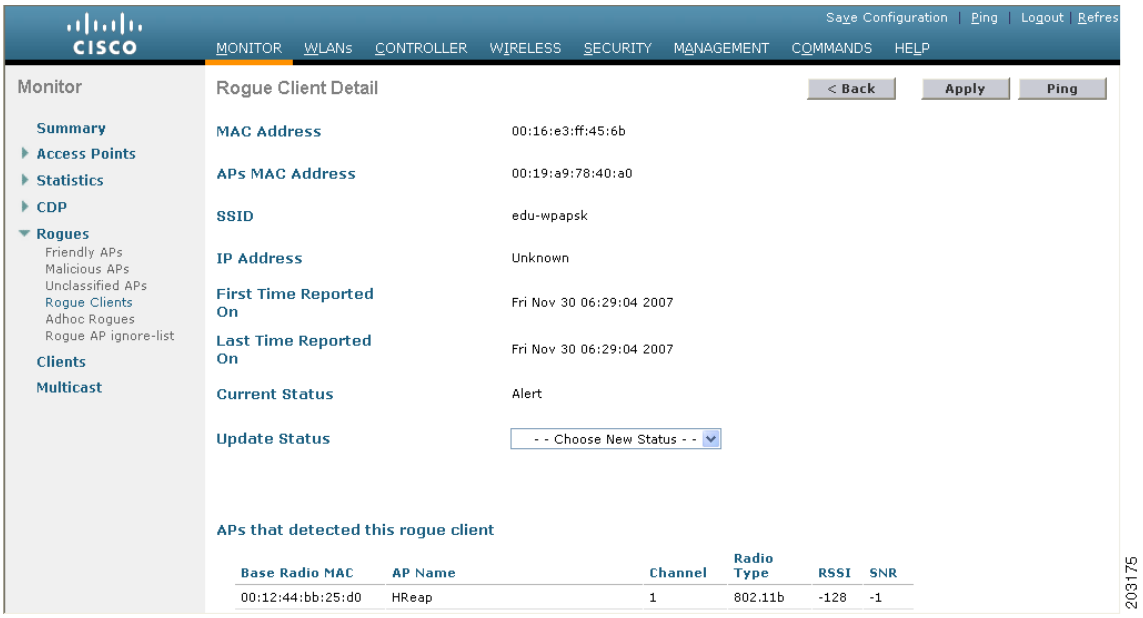
ステップ 6　[Apply] をクリックして、変更を適用します。

ステップ 7　[Save Configuration] をクリックして、変更を保存します。

ステップ 8　コントローラに接続された不正なクライアントを表示するには、[Rogue Clients] を選択します。[Rogue Clients] ページが表示されます。このページには、不正なクライアントの MAC アドレス、不正なクライアントがアソシエートされているアクセス ポイントの MAC アドレス、不正なクライアントの SSID、不正なクライアントが検出された無線の数、不正なクライアントが最後に報告された日時、不正なクライアントの現在のステータスといった情報が表示されます。

ステップ 9　不正なクライアントの詳細情報を参照するには、そのクライアントの MAC アドレスをクリックします。[Rogue Client Detail] ページが表示されます（図 5-51 を参照）。

図 5-51　[Rogue Client Detail] ページ



このページには、不正なクライアントの MAC アドレス、このクライアントがアソシエートされているアクセス ポイントの MAC アドレス、不正なクライアントの SSID および IP アドレス、不正なクライアントが最初および最後に報告された日時、不正なクライアントの現在のステータスといった情報が表示されます。

ステップ 10　[Update Status] ドロップダウン ボックスから、次のオプションの 1 つを選択して、この不正なクライアントに対するコントローラの応答方法を指定します。

- [Contain]：コントローラによって危険性のあるデバイスが阻止され、そのデバイスの信号が、認証されたクライアントに干渉しないようになります。
- [Alert]：コントローラからシステム管理者に、さらなる処理を行うよう即時に警告が転送されます。

ページの下部には、この不正なクライアントが検出されたアクセス ポイントに関する情報が提供されます。

ステップ 11　[Apply] をクリックして、変更を適用します。

ステップ 12　必要に応じて、[Ping] をクリックすることによって、このクライアントへのコントローラの接続をテストできます。

ステップ 13　[Save Configuration] をクリックして、変更を保存します。

ステップ 14　コントローラによって検出されたアドホック不正を表示するには、[Adhoc Rogues] を選択します。[Adhoc Rogues] ページが表示されます（図 5-52 を参照）。

図 5-52　[Adhoc Rogues] ページ

このページには、MAC アドレス、BSSID、アドホック不正の SSID、アドホック不正が検出された無線の数、アドホック不正の現在のステータスといった情報が表示されます。

ステップ 15　アドホック不正の詳細情報を参照するには、その不正の MAC アドレスをクリックします。[Adhoc Rogue Detail] ページが表示されます（図 5-53 を参照）。

図 5-53　[Adhoc Rogue Detail] ページ

このページには、アドホック不正の MAC アドレスおよび BSSID、不正が最初および最後に報告された日時、不正の現在のステータスといった情報が表示されます。

ステップ 16　[Update Status] ドロップダウン ボックスから、次のオプションの 1 つを選択して、このアドホック不正に対するコントローラの応答方法を指定します。

- [Contain]：コントローラによって危険性のあるデバイスが阻止され、そのデバイスの信号が、認証されたクライアントに干渉しないようになります。
- [Alert]：コントローラからシステム管理者に、さらなる処理を行うよう即時に警告が転送されます。
- [Internal]：コントローラはこの不正なアクセス ポイントを信頼します。
- [External]：コントローラはこの不正なアクセス ポイントの存在を認識します。

ステップ 17　[Maximum Number of APs to Contain the Rogue] ドロップダウン ボックスから、[1]、[2]、[3]、または [4] のオプションの 1 つを選択して、このアドホック不正を阻止するために使用するアクセス ポイントの最大数を指定します。

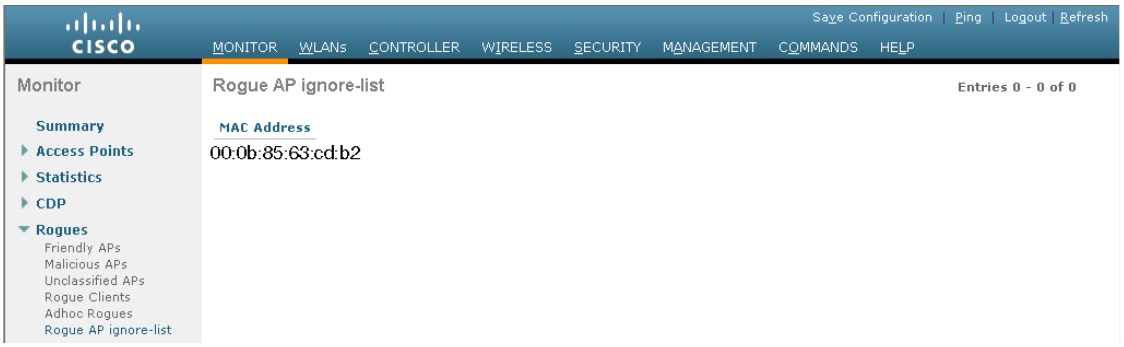
ページの下部には、このアドホック不正が検出されたアクセス ポイントに関する情報が提供されます。

ステップ 18　[Apply] をクリックして、変更を適用します。

ステップ 19　[Save Configuration] をクリックして、変更を保存します。

ステップ 20　無視するように設定された任意のアクセス ポイントを表示するには、[Rogue AP Ignore-List] を選択します。[Rogue AP Ignore-List] ページが表示されます（図 5-54 を参照）。

図 5-54　[Rogue AP Ignore-List] ページ



このページには、無視するように設定されている任意のアクセス ポイントの MAC アドレスが表示されます。不正無視リストには、WCS ユーザが WCS マップに手動で追加した任意の Autonomous アクセス ポイントのリストが含まれています。コントローラでは、これらの Autonomous アクセス ポイントが、WCS によって管理されていても不正と見なされます。不正無視リストを使用すると、コントローラでこれらのアクセス ポイントを無視できます。このリストは次のように更新されます。

- コントローラは、不正レポートを受信すると、不明なアクセス ポイントが不正無視アクセス ポイント リストに存在するかどうかを確認します。
- 不明なアクセス ポイントが不正無視リストに存在する場合、コントローラはこのアクセス ポイントを無視して他の不正なアクセス ポイントの処理を続けます。
- 不明なアクセス ポイントが不正無視リストにない場合、コントローラは WCS にトラップを送信します。WCS は、Autonomous アクセス ポイント リストでこのアクセス ポイントを発見すると、このアクセス ポイントを不正無視リストに追加するようコントローラにコマンドを送信します。このアクセス ポイントは、今後の不正レポートで無視されるようになります。
- ユーザが WCS から Autonomous アクセス ポイントを削除すると、WCS はこのアクセス ポイントを不正無視リストから削除するようにコントローラにコマンドを送信します。

CLI を使用した不正デバイスの表示および分類

コントローラの CLI を使用して、不正デバイスを表示および分類するには、次のコマンドを入力します。

1. コントローラによって検出されたすべての不正なアクセス ポイントのリストを表示するには、次のコマンドを入力します。

   show rogue ap summary

次のような情報が表示されます。

```
Rogue Location Discovery Protocol..... Enabled
Rogue AP timeout..... 1200

MAC Address        Classification     # APs # Clients Last Heard
-----------------  ------------------ ----- --------- -----------------------
00:0a:b8:7f:08:c0  Friendly           0     0         Not Heard
00:0b:85:01:30:3f  Malicious          1     0         Fri Nov 30 11:30:59 2007
00:0b:85:63:70:6f  Malicious          1     0         Fri Nov 30 11:20:14 2007
00:0b:85:63:cd:bf Malicious         1        0       Fri Nov 30 11:23:12 2007
...
```

2. コントローラによって検出された危険性のない不正なアクセス ポイントのリストを表示するには、次のコマンドを入力します。

   show rogue ap friendly summary

   次のような情報が表示されます。

```
Number of APs..... 1

MAC Address        State              # APs # Clients Last Heard
-----------------  ------------------ ----- --------- --------------------------
00:0a:b8:7f:08:c0  Internal           1   0        Tue Nov 27 13:52:04 2007
```

3. コントローラによって検出された危険性のある不正なアクセス ポイントのリストを表示するには、次のコマンドを入力します。

   show rogue ap malicious summary

   次のような情報が表示されます。

```
Number of APs..... 264

MAC Address        State              # APs # Clients Last Heard
-----------------  ------------------ ----- --------- -----------------------
00:0b:85:01:30:3f  Alert              1     0         Fri Nov 30 11:20:01 2007
00:0b:85:63:70:6f  Alert              1     0         Fri Nov 30 11:20:14 2007
00:0b:85:63:cd:bf  Alert              1     0         Fri Nov 30 11:23:12 2007
00:0b:85:63:cd:dd  Alert              1     0         Fri Nov 30 11:27:03 2007
00:0b:85:63:cd:de  Alert              1     0         Fri Nov 30 11:26:23 2007
00:0b:85:63:cd:df Alert           1     0        Fri Nov 30 11:26:50 2007
...
```

4. コントローラによって検出された未分類の不正なアクセス ポイントのリストを表示するには、次のコマンドを入力します。

   show rogue ap unclassified summary

   次のような情報が表示されます。

```
Number of APs..... 164

MAC Address        State              # APs # Clients Last Heard
-----------------  ------------------ ----- --------- -----------------------
00:0b:85:63:cd:bd  Alert              1     0         Fri Nov 30 11:12:52 2007
00:0b:85:63:cd:e7  Alert              1     0         Fri Nov 30 11:29:01 2007
00:0b:85:63:ce:05  Alert              1     0         Fri Nov 30 11:26:23 2007
00:0b:85:63:ce:07  Alert               1     0         Fri Nov 30 11:26:23 2007
...
```

5. 特定の不正なアクセス ポイントの詳細情報を表示するには、次のコマンドを入力します。

   show rogue ap detailed *ap_mac_address*

   次のような情報が表示されます。

```
Rogue BSSID..................................... 00:0b:85:63:d1:94
Is Rogue on Wired Network....................... No
Classification.................................. Unclassified
State........................................... Alert
First Time Rogue was Reported................... Fri Nov 30 11:24:56 2007
Last Time Rogue was Reported.................... Fri Nov 30 11:24:56 2007
Reported By
    AP 1
        MAC Address............................. 00:12:44:bb:25:d0
        Name.................................... HReap
        Radio Type.............................. 802.11g
        SSID.................................... edu-eap
        Channel................................. 6
        RSSI.................................... -61 dBm
        SNR..................................... -1 dB
        Encryption.............................. Enabled
        ShortPreamble........................... Enabled
        WPA Support............................. Disabled
        Last reported by this AP.............. Fri Nov 30 11:24:56 2007
```

6. 特定の 802.11a/n 無線に関する不正レポート（各種チャネル幅で検出された不正なデバイスの数を示す）を確認するには、次のコマンドを入力します。

   show ap auto-rf 802.11a *Cisco_AP*

   次のような情報が表示されます。

```
Number Of Slots................................. 2
AP Name......................................... AP2
MAC Address..................................... 00:1b:d5:13:39:74
  Radio Type.................................... RADIO_TYPE_80211a
  Noise Information
    Noise Profile............................... PASSED
    Channel 36.................................   -80 dBm
    Channel 40.................................   -78 dBm
    ...
  Interference Information
    Interference Profile........................ PASSED
    Channel 36.................................   -81 dBm @  8 % busy
    Channel 40.................................   -66 dBm @  4 % busy
   ...
Rogue Histogram (20/40_ABOVE/40_BELOW)
    Channel 36.................................. 21/ 1/ 0
    Channel 40..................................  7/ 0/ 0
    ...
```

7. 不正なアクセス ポイントにアソシエートされているすべての不正なクライアントのリストを表示するには、次のコマンドを入力します。

   show rogue ap clients *ap_mac_address*

   次のような情報が表示されます。

```
MAC Address        State              # APs  Last Heard
-----------------  -----------------  -----  -------------------------
00:bb:cd:12:ab:ff  Alert               1     Fri Nov 30 11:26:23 2007
```

8. コントローラによって検出されたすべての不正なクライアントのリストを表示するには、次のコマンドを入力します。

   show rogue client summary

   次のような情報が表示されます。

```
Validate rogue clients against AAA.............. Disabled

MAC Address        State              # APs Last Heard
-----------------  ------------------ ----- -----------------------
00:0a:8a:7d:f5:f5  Alert              1     Mon Dec  3 21:56:36 2007
00:18:ba:78:c4:44  Alert              1     Mon Dec  3 21:59:36 2007
00:18:ba:78:c4:d1  Alert              1     Mon Dec  3 21:47:36 2007
00:18:ba:78:ca:f8 Alert            1     Mon Dec  3 22:02:36 2007
...
```

9. 特定の不正なクライアントの詳細情報を表示するには、次のコマンドを入力します。

   show rogue client detailed *client_mac_address*

   次のような情報が表示されます。

```
Rogue BSSID..................................... 00:0b:85:23:ea:d1
State........................................... Alert
First Time Rogue was Reported................... Mon Dec  3 21:50:36 2007
Last Time Rogue was Reported.................... Mon Dec  3 21:50:36 2007
Rogue Client IP address......................... Not known
Reported By
    AP 1
        MAC Address............................. 00:15:c7:82:b6:b0
        Name.................................... AP0016.47b2.31ea
        Radio Type.............................. 802.11a
        RSSI.................................... -71 dBm
        SNR..................................... 23 dB
        Channel................................. 149
        Last reported by this AP.............. Mon Dec  3 21:50:36 2007
```

10. コントローラによって検出されたすべてのアドホック不正のリストを表示するには、次のコマンドを入力します。

    show rogue adhoc summary

    次のような情報が表示されます。

```
Detect and report Ad-Hoc Networks............... Enabled

Client MAC Address  Adhoc BSSID         State    # APs   Last Heard
------------------  ------------------  ---------- -------  -----------------------
00:bb:cd:12:ab:ff  super              Alert       1      Fri Nov 30 11:26:23 2007
```

11. 特定のアドホック不正の詳細情報を表示するには、次のコマンドを入力します。

    show rogue adhoc detailed *rogue_mac_address*

    次のような情報が表示されます。

```
Adhoc Rogue MAC address......................... 02:61:ce:8e:a8:8c
Adhoc Rogue BSSID............................... 02:61:ce:8e:a8:8c
State........................................... Alert
First Time Adhoc Rogue was Reported............. Tue Dec 11 20:45:45 2007
Last Time Adhoc Rogue was Reported.............. Tue Dec 11 20:45:45 2007
Reported By
    AP 1
        MAC Address............................. 00:14:1b:58:4a:e0
        Name.................................... AP0014.1ced.2a60
        Radio Type.............................. 802.11b
```

```
SSID..................................... rf4k3ap
Channel.................................. 3
RSSI..................................... -56 dBm
SNR...................................... 15 dB
Encryption............................... Disabled
ShortPreamble............................ Disabled
WPA Support.............................. Disabled
Last reported by this AP.............. Tue Dec 11 20:45:45 2007
```

12. 無視するように設定されている不正なアクセス ポイントのリストを表示するには、次のコマンドを入力します。

    show rogue ignore-list

    次のような情報が表示されます。

```
MAC Address
------------------
10:bb:17:cc:01:ef
```

    （注）　不正無視アクセス ポイントのリストの詳細については、「GUI を使用した不正なデバイスの表示および分類」（P.5-97）のステップ 20 を参照してください。

13. 不正なアクセス ポイントを Friendly に分類するには、次のコマンドを入力します。

    config rogue ap classify friendly state {**internal** | **external**} *ap_mac_address*

    - **internal** は、コントローラがこの不正なアクセス ポイントを信頼することを表しています。
    - **external** は、コントローラがこの不正なアクセス ポイントの存在を認識することを表しています。

    （注）　不正なアクセス ポイントの現在の状態が Contain である場合、そのアクセス ポイントを Friendly クラスに移動することはできません。

14. 不正なアクセス ポイントに Malicious のマークを付けるには、次のコマンドを入力します。

    config rogue ap classify malicious state {**alert** | **contain**} *ap_mac_address*

    - **contain** は、コントローラによって危険性のあるデバイスが阻止され、そのデバイスの信号が、認証されたクライアントに干渉しないようになることを表しています。
    - **alert** は、コントローラからシステム管理者に、更なる処理を行うよう即時に警告が転送されることを表しています。

    （注）　不正なアクセス ポイントの現在の状態が Contain である場合、そのアクセス ポイントを Malicious クラスに移動することはできません。

15. 不正なアクセス ポイントに Unclassified のマークを付けるには、次のコマンドを入力します。

    config rogue ap classify unclassified state {**alert** | **contain**} *ap_mac_address*

    （注）　不正なアクセス ポイントの現在の状態が Contain である場合、そのアクセス ポイントを Unclassified クラスに移動することはできません。

16. 不正なクライアントに対するコントローラの応答方法を指定するには、次のコマンドを入力します。

- **config rogue client alert** *client_mac_address*：コントローラからシステム管理者に、さらなる処理を行うよう即時に警告が転送されます。
- **config rogue client contain** *client_mac_address*：コントローラによって危険性のあるデバイスが阻止され、そのデバイスの信号が、認証されたクライアントに干渉しないようになります。

17. アドホック不正に対するコントローラの応答方法を指定するには、次のコマンドを入力します。
    - **config rogue adhoc alert** *rogue_mac_address*：コントローラからシステム管理者に、さらなる処理を行うよう即時に警告が転送されます。
    - **config rogue adhoc contain** *rogue_mac_address*：コントローラによって危険性のあるデバイスが阻止され、そのデバイスの信号が、認証されたクライアントに干渉しないようになります。
    - **config rogue adhoc external** *rogue_mac_address*：コントローラによって、このアドホック不正の存在が認識されます。
18. 変更を保存するには、次のコマンドを入力します。

    save config

IDS の設定

Cisco Intrusion Detection System/Intrusion Prevention System（CIDS/IPS; シスコ侵入検知システム/侵入防御システム）は、特定のクライアントに関わる攻撃がレイヤ 3 ～ レイヤ 7 で検出されたとき、これらのクライアントによる無線ネットワークへのアクセスをブロックするよう、コントローラに指示します。このシステムは、ワーム、スパイウェア/アドウェア、ネットワーク ウィルス、およびアプリケーションの不正使用などの脅威の検出、分類、阻止を支援することにより、強力なネットワーク保護を提供します。潜在的な攻撃を検出するには 2 つの方法があります。

- IDS センサー。次の項を参照してください。
- IDS シグニチャ。IDS シグニチャの設定（P.5-112）を参照してください。

（注）　コントローラでは WCS を介して Cisco Wireless Intrusion Prevention System（wIPS）もサポートされています。詳細は、「wIPS の設定」（P.5-124）を参照してください。

IDS センサーの設定

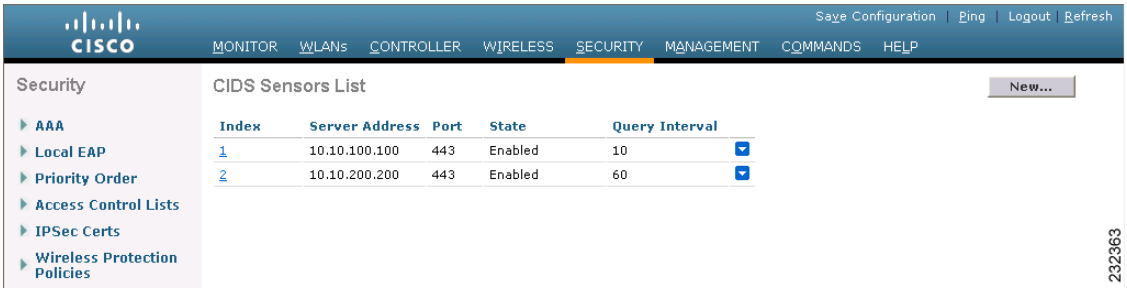
ネットワークのさまざまなタイプの IP レベル攻撃を検出するように、IDS センサーを設定することができます。センサーで攻撃が特定されたら、違反クライアントを回避するよう、コントローラに警告することができます。新しく IDS センサーを追加したときは、コントローラをその IDS センサーに登録し、回避クライアントのリストをセンサーから取得できるようにします。IDS センサー登録は、GUI または CLI のいずれかを使用して設定できます。

GUI を使用した IDS センサーの設定

コントローラの GUI を使用して IDS センサーを設定する手順は、次のとおりです。

ステップ 1　[Security] > [Advanced] > [CIDs] > [Sensors] の順に選択して、[CIDS Sensors List] ページを開きます（図 5-55 を参照）。

図 5-55　[CIDS Sensors List] ページ

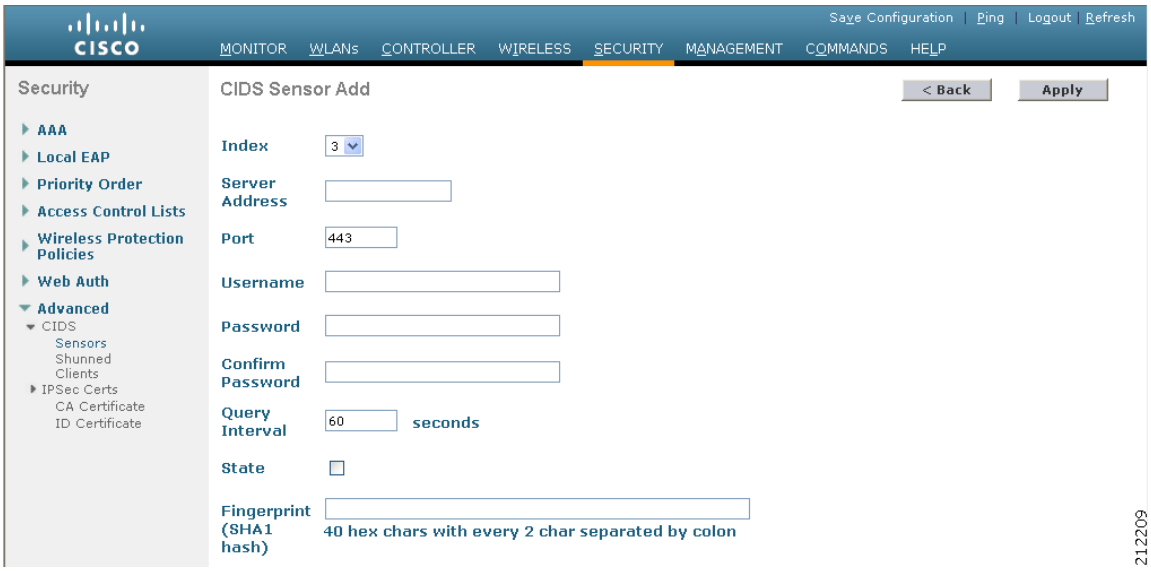


このページでは、このコントローラに設定されたすべての IDS センサーが表示されます。

（注）　既存のセンサーを削除するには、そのセンサーの青いドロップダウンの矢印の上にカーソルを置いて、[Remove] を選択します。

ステップ 2　IDS センサーをリストに追加するには、[New] をクリックします。[CIDS Sensor Add] ページが表示されます（図 5-56 を参照）。

図 5-56　[CIDS Sensor Add] ページ



ステップ 3　コントローラでは最大 5 つの IDS センサーをサポートします。[Index] ドロップダウン ボックスから数字（1 ～ 5）を選択し、コントローラで IDS センサーが検索される順序を決定します。たとえば、1 を選択した場合には、コントローラは最初にこの IDS センサーを検索します。

ステップ 4　[Server Address] フィールドに、IDS サーバの IP アドレスを入力します。

ステップ 5　[Port] フィールドには、コントローラと IDS センサーとの通信に使用される HTTPS ポートの番号が設定されます。センサーはデフォルトで 443 を使用して通信するので、このパラメータを 443 に設定することをお勧めします。

デフォルト：443

範囲：1 ～ 65535

ステップ 6　[Username] フィールドで、コントローラが IDS センサーの認証に使用するユーザ名を入力します。

（注）　このユーザ名は IDS センサーに設定されており、少なくとも読み取り専用権限を持っている必要があります。

ステップ 7　[Password] フィールドと [Confirm Password] フィールドに、コントローラが IDS センサーの認証に使用するパスワードを入力します。

ステップ 8　[Query Interval] フィールドに、コントローラが IDS サーバで IDS イベントを検索する間隔（秒単位）を入力します。

デフォルト：60 秒

範囲：10 ～ 3600 秒

ステップ 9　[State] チェックボックスをオンにしてコントローラをこの IDS センサーに登録するか、このチェックボックスをオフにして登録を解除します。デフォルト値は無効（disable）です。

ステップ 10　[Fingerprint] フィールドに、40 桁の 16 進数文字のセキュリティ キーを入力します。このキーは、センサーの有効性の確認、およびセキュリティ攻撃の防止に使用されます。

（注）　キー内に 2 バイト間隔で表記されるコロン（:）を含めないようにしてください。たとえば、AA:BB:CC:DD の代わりに、AABBCCDD と入力します。

ステップ 11　[Apply] をクリックします。[CIDS Sensors List] ページのセンサーのリストに新しい IDS センサーが表示されます。

ステップ 12　[Save Configuration] をクリックして、変更を保存します。

CLI を使用した IDS センサーの設定

コントローラの CLI を使用して IDS センサーを設定する手順は、次のとおりです。

ステップ 1　IDS センサーを追加するには、次のコマンドを入力します。

config wps cids-sensor add *index ids_ip_address username password*

index パラメータは、コントローラで IDS センサーが検索される順序を決定します。コントローラでは最大 5 つの IDS センサーをサポートします。数字（1 ～ 5）を入力してこのセンサーの優先順位を決定します。たとえば、1 を入力した場合には、コントローラは最初にこの IDS センサーを検索します。

（注）　ユーザ名は IDS センサーに設定されており、少なくとも読み取り専用権限を持っている必要があります。

ステップ 2　（オプション）コントローラが IDS センサーとの通信に使用する HTTPS ポートの番号を指定するには、次のコマンドを入力します。

config wps cids-sensor port *index port_number*

port-number パラメータには、1 ～ 65535 の値を入力することができます。デフォルト値は 443 です。この手順は任意であり、デフォルト値の 443 の使用をお勧めします。デフォルトでは、センサーはこの値を使用して通信します。

ステップ 3　コントローラが IDS イベントについて IDS センサーを検索する間隔を指定するには、次のコマンドを入力します。

config wps cids-sensor interval *index interval*

interval パラメータには、10 ～ 3600 秒の値を入力することができます。デフォルト値は 60 秒です。

ステップ 4　センサーの有効性の確認に使用する 40 桁の 16 進数文字のセキュリティ キーを入力するには、次のコマンドを入力します。

config wps cids-sensor fingerprint *index* **sha1** *fingerprint*

センサーのコンソール上で、**show tls fingerprint** と入力することにより、フィンガープリントの値を取得できます。

（注）　キー内にコロン（:）が 2 バイト間隔で表記されるようにしてください（たとえば、AA:BB:CC:DD）。

ステップ 5　IDS センサーへのこのコントローラの登録を有効または無効にするには、次のコマンドを入力します。

config wps cids-sensor {**enable** | **disable**} *index*

ステップ 6　DoS 攻撃からの保護を有効または無効にするには、次のコマンドを入力します。

config wps auto-immune {**enable** | **disable**}

デフォルト値は無効（disable）です。

（注）　潜在的な攻撃者は、特殊な細工が施されたパケットを使用することにより、正規のクライアントを攻撃者として扱うように IDS の判断を誤らせます。これにより、誤ってコントローラから正規のクライアントが切断され、DoS 攻撃が開始されます。自動免疫機能が有効の場合、そのような攻撃に対抗できるよう設計されています。ただし、自動免疫機能を有効にすると、Cisco 792x 電話を使用した会話が断続的に途切れる場合があります。792x 電話の使用時に会話が頻繁に中断する場合は、自動免疫機能を無効にすることもできます。

ステップ 7　設定を保存するには、次のコマンドを入力します。

save config

ステップ 8　IDS センサー設定を表示するには、次のコマンドの 1 つを入力します。

- **show wps cids-sensor summary**
- **show wps cids-sensor detail** *index*

2 つ目のコマンドは、1 つ目のコマンドよりも詳細な情報を提供します。

ステップ 9　自動免疫設定の情報を確認するには、次のコマンドを入力します。

show wps summary

次のような情報が表示されます。

```
Auto-Immune
  Auto-Immune..................................... Disabled

Client Exclusion Policy
  Excessive 802.11-association failures.......... Enabled
  Excessive 802.11-authentication failures....... Enabled
```

```
  Excessive 802.1x-authentication.............. Enabled
  IP-theft..................................... Enabled
  Excessive Web authentication failure.......... Enabled

Signature Policy
  Signature Processing......................... Enabled
```

ステップ 10　IDS センサー設定に関連したデバッグ情報を取得するには、次のコマンドを入力します。

debug wps cids enable

（注）　センサーの設定を削除または変更するには、まず、**config wps cids-sensor disable** *index* と入力して設定を無効にする必要があります。その後、センサーを削除するには、**config wps cids-sensor delete** *index* と入力します。

回避クライアントの表示

IDS センサーは、疑わしいクライアントを検出すると、コントローラにこのクライアントを回避するよう警告します。回避エントリは、同じモビリティ グループ内のすべてのコントローラに配信されます。回避すべきクライアントが現在、このモビリティ グループ内のコントローラに接続されている場合、アンカー コントローラはこのクライアントを動的除外リストに追加し、外部コントローラはクライアントを切り離します。次回、このクライアントがコントローラに接続を試みた場合、アンカー コントローラはハンドオフを拒否し、外部コントローラにクライアントを除外することを通知します。モビリティ グループの詳細については、第 12 章を参照してください。

GUI または CLI により、IDS センサーが回避すべきと特定したクライアントのリストを表示できます。

GUI を使用した回避クライアントの表示

コントローラの GUI を使用し、IDS センサーによって回避すべきであると判断されたクライアントのリストを表示する手順は、次のとおりです。

ステップ 1　[Security] > [Advanced] > [CIDS] > [Shunned Clients] の順に選択します。[CIDS Shun List] ページが表示されます（図 5-57 を参照）。

図 5-57　[CIDS Shun List] ページ

このページには、各回避クライアントの IP アドレスと MAC アドレス、IDS センサーの要求に応じてコントローラがクライアントのデータ パケットをブロックする期間、およびクライアントを検出した IDS センサーの IP アドレスが表示されます。

ステップ 2　必要に応じてリストを削除、およびリセットするには、[Re-sync] をクリックします。

CLI を使用した回避クライアントの表示

コントローラの CLI を使用し、IDS センサーによって回避すべきであると判断されたクライアントのリストを表示する手順は、次のとおりです。

ステップ 1　回避すべきクライアントのリストを表示するには、次のコマンドを入力します。

show wps shun-list

ステップ 2　コントローラに対し、このモビリティ グループ内の他のコントローラの回避リストと同期をとるよう強制するには、次のコマンドを入力します。

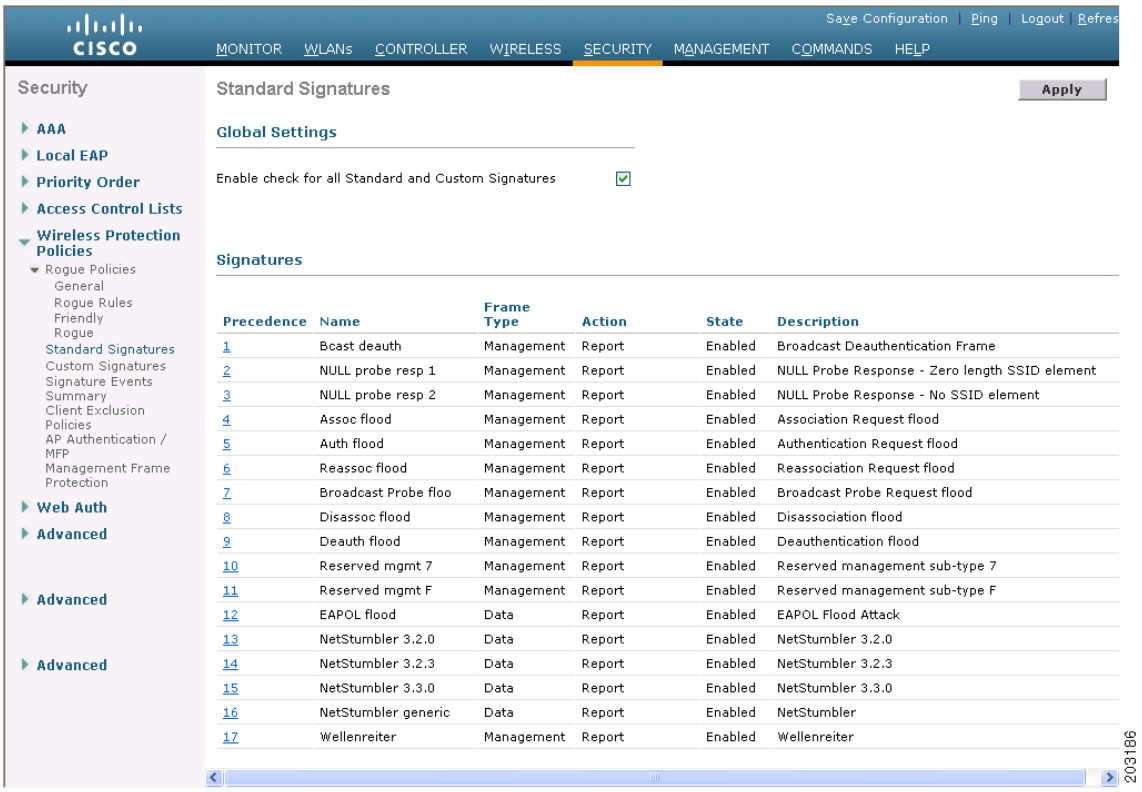
config wps shun-list re-sync

IDS シグニチャの設定

コントローラ上で、IDS シグニチャ、すなわち、受信 802.11 パケットにおけるさまざまなタイプの攻撃を特定するのに使用されるビット パターンのマッチング ルールを設定することができます。シグニチャが有効化されると、コントローラに接続されたアクセス ポイントでは、受信した 802.11 データまたは管理フレーム上でシグニチャ分析が行われ、整合性がない場合はコントローラに報告されます。攻撃が検出されると、適切な緩和措置が開始されます。

[Standard Signatures] ページに示すように、シスコでは、コントローラ上で 17 の標準シグニチャをサポートしています（図 5-58 を参照）。

図 5-58　[Standard Signatures] ページ



これらのシグニチャは 6 つの主要なグループに分かれます。初めの 4 つのグループには管理シグニチャが含まれており、後の 2 つのグループにはデータ シグニチャが含まれます。

- **ブロードキャスト認証解除フレーム シグニチャ**：ブロードキャスト認証解除フレーム攻撃において、ハッカーは別のクライアントのブロードキャスト MAC 宛先アドレスに対して 802.11 認証解除フレームを送信します。この攻撃は、宛先クライアントをアクセス ポイントからアソシエート解除および切断する原因となります。この処理が繰り返されると、クライアントでサービスが拒絶されます。ブロードキャスト認証解除フレーム シグニチャ（優先 1）を使用してそのような攻撃を検出する場合、アクセス ポイントでは、シグニチャの特性と一致するクライアント送信ブロードキャスト認証解除フレームがリッスンされます。アクセス ポイントは、そのような攻撃を検出すると、コントローラに警告を送ります。システムの設定に応じて、危険性のあるデバイスが阻止されて、そのデバイスの信号が認証されたクライアントに干渉しないようにされるか、コントローラからシステム管理者に、さらなる処理を行うよう即時に警告が転送されるか、または、その両方が実行されます。
- **NULL プローブ応答シグニチャ**：NULL プローブ応答攻撃において、ハッカーは無線クライアント アダプタに NULL プローブ応答を送信します。結果として、クライアント アダプタがロックされます。NULL プローブ応答シグニチャを使用してそのような攻撃が検出されると、アクセス ポイントは無線クライアントを特定し、コントローラに警告を送ります。NULL プローブ応答には、次のものがあります。
  - NULL probe resp 1（優先 2）
  - NULL probe resp 2（優先 3）
- **管理フレーム フラッドシグニチャ**：管理フレーム フラッド攻撃において、ハッカーはアクセス ポイントに大量の 802.11 管理フレームを送り付けます。その結果、アソシエートされたすべてのクライアントに対するサービスが拒絶されるか、アクセス ポイントへのアソシエートが試行され続

けます。この攻撃は、アソシエーション要求、認証要求、再アソシエーション要求、プローブ要求、アソシエーション解除要求、認証解除要求、予約管理サブタイプなど、さまざまなタイプの管理フレームを使用して実行されます。

管理フレーム フラッド シグニチャを使用してそのような攻撃が検出されると、アクセス ポイントによって、シグニチャのすべての特性と一致する管理フレームが特定されます。これらのフレームの頻度が、シグニチャで設定された頻度の値より大きくなると、これらのフレームを受信するアクセス ポイントによってアラームがトリガーされます。コントローラではトラップが生成され、WCS に転送されます。

管理フレーム フラッド シグニチャには、次のものがあります。

- Assoc flood（優先順位 4）
- Auth flood（優先順位 5）
- Reassoc flood（優先順位 6）
- Broadcast probe flood（優先順位 7）
- Disassoc flood（優先順位 8）
- Deauth flood（優先順位 9）
- Reserved mgmt 7（優先順位 10）
- Reserved mgmt F（優先順位 11）

予約管理フレーム シグニチャ 7 および F は、将来使用するために予約されています。

- **Wellenreiter シグニチャ**：Wellenreiter は、無線 LAN スキャンおよびディスカバリ ユーティリティです。これを使用すると、アクセス ポイントおよびクライアントに関する情報が漏洩してしまう可能性があります。Wellenreiter シグニチャ（優先順位 17）を使用してそのような攻撃が検出されると、アクセス ポイントは危険性のあるデバイスを特定し、コントローラに警告を送ります。
- **EAPOL フラッド シグニチャ**：EAPOL フラッド攻撃において、ハッカーは 802.1X 認証要求を含む EAPOL フレームを大量に発生させます。結果として、802.1X 認証サーバはすべての要求に応答できなくなり、有効なクライアントに正常な認証応答を送信できなくなります。そして、その影響を受けるすべてのクライアントに対するサービスが拒絶されます。EAPOL フラッド シグニチャ（優先順位 12）を使用してそのような攻撃が検出されると、アクセス ポイントは EAPOL パケットの最大許容数を超えるまで待機します。次に、コントローラに警告を送り、適切な緩和措置を実行します。
- **NetStumbler シグニチャ**：NetStumbler は、無線 LAN スキャン ユーティリティです。これによって、アクセス ポイントのブロードキャスト関連情報（動作チャネル、RSSI 情報、アダプタ製造業者名、SSID、WEP ステータス、GPS が接続された NetStumbler を実行するデバイスの経度と緯度など）が報告されます。NetStumbler は、アクセス ポイントに対する認証とアソシエーションを正常に完了すると、次の文字列のデータ フレーム（NetStumbler のバージョンによって異なる）を送信します。

バージョン	文字列
3.2.0	「Flurble gronk bloopit, bnip Frundletrune」
3.2.3	「All your 802.11b are belong to us」
3.3.0	ホワイト スペースを送信

NetStumbler シグニチャを使用してそのような攻撃が検出されると、アクセス ポイントは危険性のあるデバイスを特定してコントローラに警告を送ります。NetStumbler シグニチャには、次のものがあります。

- NetStumbler 3.2.0（優先順位 13）

- NetStumbler 3.2.3（優先順位 14）
- NetStumbler 3.3.0（優先順位 15）
- NetStumbler generic（優先順位 16）

コントローラ上にはデフォルトで標準シグニチャ ファイルが存在します。このシグニチャ ファイルをコントローラからアップロードすることも、カスタム シグニチャ ファイルを作成してコントローラにダウンロードすることも、または標準シグニチャ ファイルを修正してカスタム シグニチャ ファイルを作成することもできます。シグニチャは、GUI または CLI のいずれかを使用して設定できます。

GUI を使用した IDS シグニチャの設定

コントローラ GUI を使用してシグニチャを設定する手順は、次のとおりです。

- IDS シグニチャのアップロードまたはダウンロード：GUI を使用した IDS シグニチャのアップロードまたはダウンロード（P.5-115）
- IDS シグニチャの有効化または無効化：GUI を使用した IDS シグニチャの有効化または無効化（P.5-117）
- IDS シグニチャ イベントの表示：GUI を使用した IDS シグニチャ イベントの表示（P.5-119）

GUI を使用した IDS シグニチャのアップロードまたはダウンロード

コントローラの GUI を使用して IDS シグニチャをアップロードまたはダウンロードする手順は、次のとおりです。

ステップ 1　必要に応じて、独自のカスタム シグニチャ ファイルを作成します。

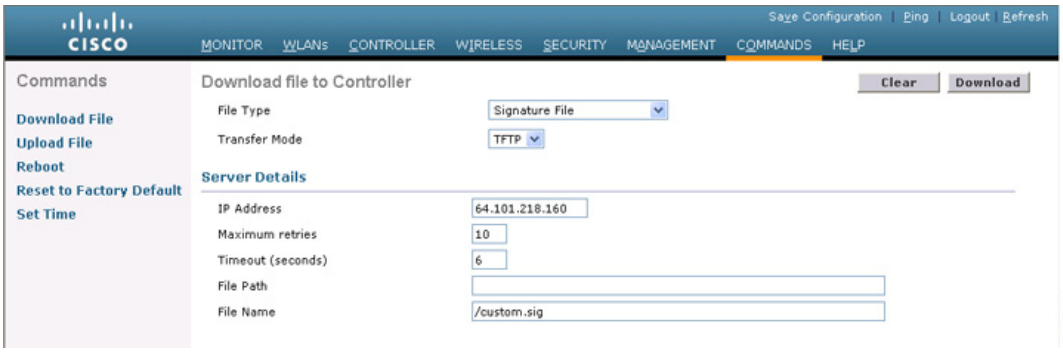
ステップ 2　Trivial File Transfer Protocol（TFTP）サーバが使用可能であることを確認します。TFTP サーバをセットアップする際の注意事項は次のとおりです。

- サービス ポート経由でダウンロードする場合、サービス ポートはルーティングできないため、TFTP サーバはサービス ポートと同じサブネット上になければなりません。そうでない場合は、コントローラ上に静的ルートを作成する必要があります。
- ディストリビューション システム ネットワーク ポートを経由してダウンロードする場合、ディストリビューション システム ポートはルーティング可能なので、TFTP サーバは同じサブネット上にあっても、別のサブネット上にあってもかまいません。
- サードパーティの TFTP サーバと WCS 内蔵型 TFTP サーバは同じ通信ポートを使用するため、サードパーティの TFTP サーバは Cisco WCS と同じコンピュータ上で実行できません。

ステップ 3　カスタム シグニチャ ファイル（*.sig）をダウンロードする場合は、ファイルを TFTP サーバ上のデフォルト ディレクトリに移動します。

ステップ 4　[Commands] を選択して、[Download File to Controller] ページを開きます（図 5-59 を参照）。

図 5-59　[Download File to Controller] ページ



ステップ 5　次のいずれかの操作を行います。

- カスタム シグニチャ ファイルをコントローラにダウンロードする場合は、[Download File to Controller] ページの [File Type] ドロップダウン ボックスから [Signature File] を選択します。
- 標準シグニチャ ファイルをコントローラからアップロードする場合は、[Upload File] を選択してから、[Upload File from Controller] ページの [File Type] ドロップダウン ボックスから [Signature File] を選択します。

ステップ 6　[Transfer Mode] ドロップダウン ボックスから、[TFTP] または [FTP] を選択します。

ステップ 7　[IP Address] フィールドに、TFTP または FTP サーバの IP アドレスを入力します。

ステップ 8　TFTP サーバを使用してシグニチャ ファイルをダウンロードする場合は、[Maximum Retries] フィールドにコントローラによるシグニチャ ファイルのダウンロードの最大試行回数を入力します。

範囲：1 ～ 254

デフォルト：10

ステップ 9　TFTP サーバを使用してシグニチャ ファイルをダウンロードする場合は、シグニチャ ファイルのダウンロードの試行時にコントローラがタイムアウトするまでの時間（秒単位）を [Timeout] フィールドに入力します。

範囲：1 ～ 254 秒

デフォルト：6 秒

ステップ 10　[File Path] フィールドに、ダウンロードまたはアップロードするシグニチャ ファイルのパスを入力します。デフォルト値は「/」です。

ステップ 11　[File Name] フィールドに、ダウンロードまたはアップロードするシグニチャ ファイルの名前を入力します。

（注）　コントローラは、シグニチャのアップロード時に、ユーザが指定した基本名に「_std.sig」および「_custom.sig」を追加したファイル名を使用して、標準シグニチャ ファイルとカスタム シグニチャ ファイルの*両方*を TFTP サーバにアップロードします。たとえば、「ids1」という名前のシグニチャ ファイルをアップロードする場合、コントローラは自動的に ids1_std.sig と ids1_custom.sig を生成して TFTP サーバにアップロードします。その後、必要に応じて TFTP サーバ上で ids1_custom.sig を変更し（必ず「Revision = custom」を設定してください）、自動的にダウンロードすることもできます。

ステップ 12　FTP サーバを使用している場合は、次の手順に従います。

a.　[Server Login Username] フィールドにユーザ名を入力し、FTP サーバにログインします。

b.　[Server Login Password] フィールドにパスワードを入力し、FTP サーバにログインします。

c. [Server Port Number] フィールドに、ダウンロードが発生する FTP サーバのポート番号を入力します。デフォルト値は 21 です。

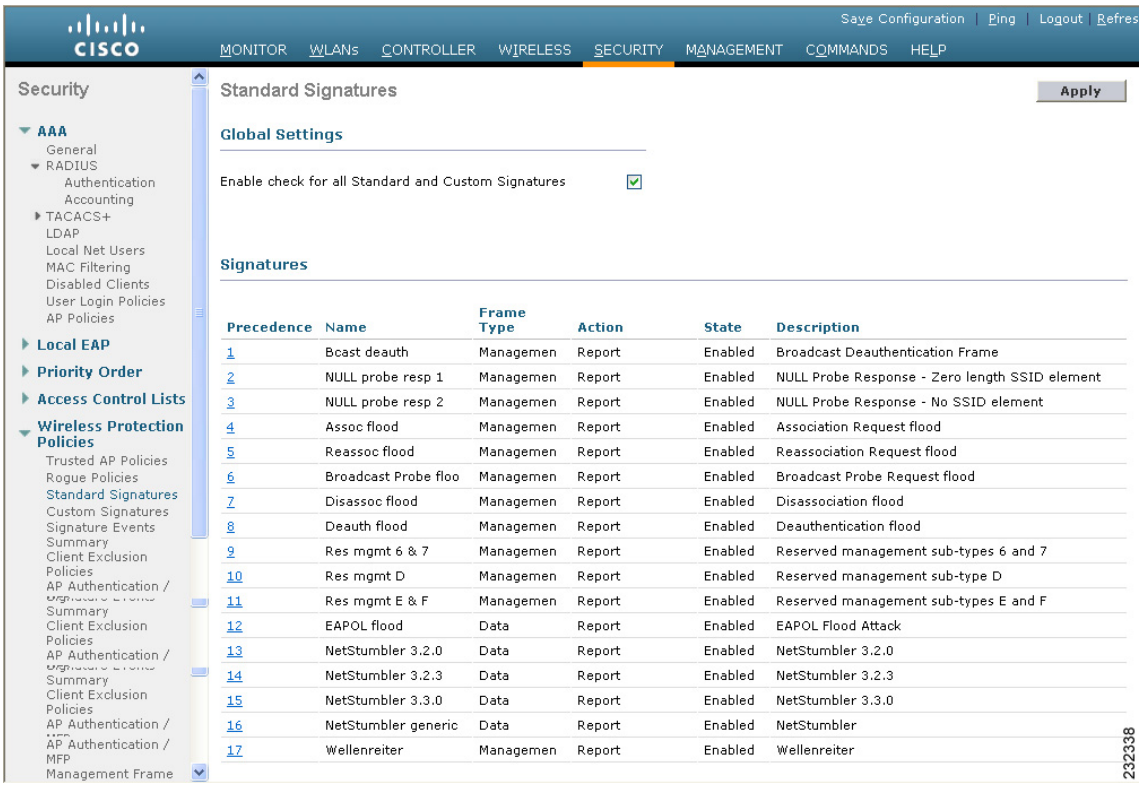
ステップ 13　[Download] を選択してシグニチャ ファイルをコントローラにダウンロードするか、[Upload] を選択してシグニチャ ファイルをコントローラからアップロードします。

GUI を使用した IDS シグニチャの有効化または無効化

コントローラ GUI を使用して IDS シグニチャを有効化または無効化する手順は、次のとおりです。

ステップ 1　[Security] > [Wireless Protection Policies] > [Standard Signatures] または [Custom Signatures] の順に選択します。[Standard Signatures] ページ（図 5-60 を参照）、または [Custom Signatures] ページが表示されます。

図 5-60　[Standard Signatures] ページ



[Standard Signatures] ページには、現在コントローラ上に存在するシスコ提供のシグニチャのリストが表示されます。[Custom Signatures] ページには、現在コントローラ上に存在する、ユーザ提供のシグニチャのリストが表示されます。このページには、各シグニチャについて次の情報が表示されます。

- コントローラがシグニチャ チェックを行う順序、または優先順位。
- シグニチャ名。シグニチャが検出しようとする攻撃タイプを明示するもの。
- シグニチャがセキュリティ攻撃を検出するフレーム タイプ。フレーム タイプとしては、データおよび管理があります。
- シグニチャが攻撃を検出したとき、コントローラが行うべき処理。処理としては、「None」と「Report」があります。

- シグニチャの状態。セキュリティ攻撃を検出するために、シグニチャが有効化されているかどうかを示すもの。
- シグニチャが検出しようとする攻撃のタイプの説明。

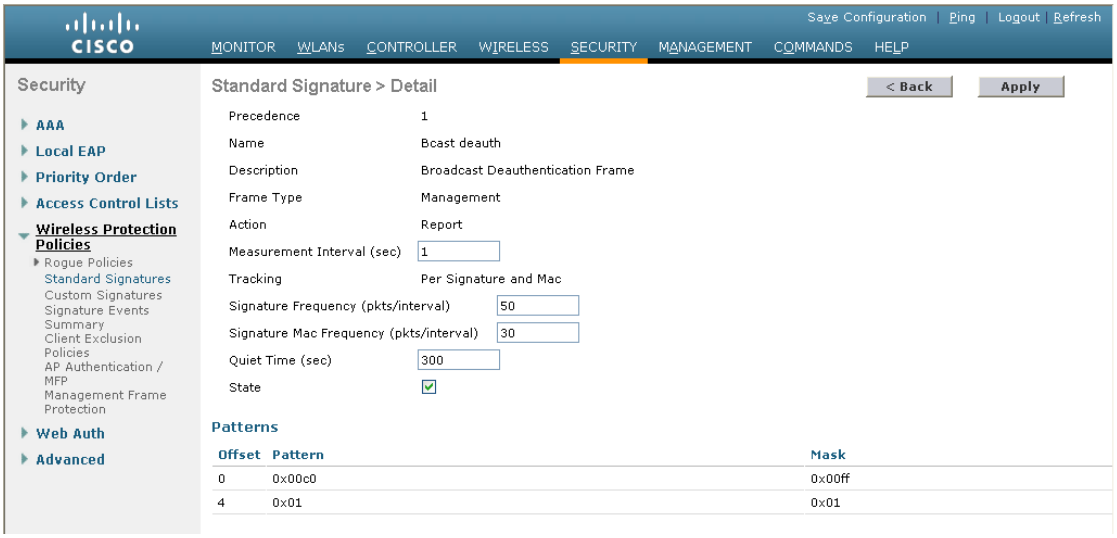
ステップ 2　次のいずれかの操作を行います。

- すべてのシグニチャ（標準およびカスタムの両方）について、それぞれ状態を「Enabled」に設定して有効にしておく場合には、[Standard Signatures] ページまたは [Custom Signatures] ページの上部の [Enable Check for All Standard and Custom Signatures] チェックボックスをオンにします。デフォルト値は、有効になっています（オンになっています）。シグニチャが有効化されると、コントローラに接続されたアクセス ポイントでは、受信した 802.11 データまたは管理フレーム上でシグニチャ分析が行われ、整合性がない場合はコントローラに報告されます。
- コントローラ上のすべてのシグニチャ（標準およびカスタムの両方）を無効にしておく場合には、[Enable Check for All Standard and Custom Signatures] チェックボックスをオフにします。このチェックボックスをオフにすると、たとえ個別のシグニチャの状態が「Enabled」に設定されている場合でも、すべてのシグニチャが無効になります。

ステップ 3　[Apply] をクリックして、変更を適用します。

ステップ 4　個別のシグニチャを有効化または無効化するには、そのシグニチャの優先順位番号をクリックします。[Standard Signature（または Custom Signature）> Detail] ページが表示されます（図 5-61 を参照）。

図 5-61　[Standard Signature > Detail] ページ



このページには、[Standard Signatures] ページおよび [Custom Signatures] ページとほぼ同じ情報が表示されますが、次のような詳細も表示されます。

- アクセス ポイントによるシグニチャ分析およびコントローラへの結果報告に使用される追跡方法。次の値が設定可能です。
  - [Per Signature]：シグニチャ分析とパターン マッチングにおける追跡および報告は、シグニチャ別およびチャネル別に実行されます。
  - [Per MAC]：シグニチャ分析とパターン マッチングにおける追跡と報告は、チャネルごとに個々のクライアント MAC アドレス別に実行されます。
  - [Per Signature and MAC]：シグニチャ分析とパターン マッチングにおける追跡と報告は、シグニチャ別/チャネル別、および MAC アドレス別/チャネル別の両方で実行されます。
- セキュリティ攻撃の検出に使用されるパターン。

ステップ 5　[Measurement Interval] フィールドに、シグニチャ頻度が設定された間隔内でしきい値に達するまでの経過時間（秒数）を入力します。有効な値の範囲は 1 ～ 3600 秒で、デフォルト値はシグニチャによって異なります。

ステップ 6　[Signature Frequency] フィールドに、個々のアクセス ポイント レベルで特定されるべき、1 間隔あたりの一致パケット数を入力します。この値に達すると攻撃が検出されたと判断されます。有効な値の範囲は 1 間隔あたり 1 ～ 32,000 パケットで、デフォルト値はシグニチャによって異なります。

ステップ 7　[Signature MAC Frequency] フィールドに、個々のアクセス ポイントでクライアント別に特定されるべき、1 間隔あたりの一致パケット数を入力します。この値に達すると攻撃が検出されたと判断されます。有効な値の範囲は 1 間隔あたり 1 ～ 32,000 パケットで、デフォルト値はシグニチャによって異なります。

ステップ 8　[Quiet Time] フィールドに、個々のアクセス ポイント レベルで攻撃が検出されない状態が経過して、アラームを停止できるようになるまでの時間（秒単位）を入力します。有効な値の範囲は 60 ～ 32,000 秒で、デフォルト値はシグニチャによって異なります。

ステップ 9　[State] チェックボックスをオンにし、このシグニチャを有効にしてセキュリティ攻撃を検出するか、オフにしてこのシグニチャを無効にします。デフォルト値は、有効になっています（オンになっています）。

ステップ 10　[Apply] をクリックして、変更を適用します。[Standard Signatures] ページまたは [Custom Signatures] ページに、シグニチャの更新された状態が反映されます。

ステップ 11　[Save Configuration] をクリックして、変更を保存します。

GUI を使用した IDS シグニチャ イベントの表示

コントローラ GUI を使用してシグニチャ イベントを表示する手順は、次のとおりです。

ステップ 1　[Security] > [Wireless Protection Policies] > [Signature Events Summary] の順に選択します。[Signature Events Summary] ページが表示されます（図 5-62 を参照）。

図 5-62　[Signature Events Summary] ページ

このページには有効化されたシグニチャによって検出された攻撃の数が表示されます。

ステップ 2　特定のシグニチャによって検出された攻撃の詳細を表示するには、そのシグニチャのシグニチャ タイプのリンクをクリックします。[Signature Events Detail] ページが表示されます（図 5-63 を参照）。

図 5-63　[Signature Events Detail] ページ

このページには、次の情報が表示されます。

- 攻撃者として特定されたクライアントの MAC アドレス
- アクセス ポイントが攻撃の追跡に使用する方法
- 攻撃が検出されるまでに特定された 1 秒当たりの一致パケットの数
- 攻撃が検出されたチャネル上のアクセス ポイント数
- アクセス ポイントが攻撃を検出した日時

ステップ 3　特定の攻撃の詳細を表示するには、その攻撃の [Detail] リンクをクリックします。[Signature Events Track Detail] ページが表示されます（図 5-64 を参照）。

図 5-64　[Signature Events Track Detail] ページ

このページには、次の情報が表示されます。

- 攻撃を検出したアクセス ポイントの MAC アドレス
- 攻撃を検出したアクセス ポイントの名前
- アクセス ポイントが攻撃の検出に使用した無線のタイプ（802.11a または 802.11b/g）
- 攻撃が検出された無線チャネル
- アクセス ポイントから攻撃が報告された日時

CLI を使用した IDS シグニチャの設定

コントローラの CLI を使用して IDS シグニチャを設定する手順は、次のとおりです。

ステップ 1　必要に応じて、独自のカスタム シグニチャ ファイルを作成します。

ステップ 2　TFTP サーバが使用可能であることを確認します。「GUI を使用した IDS シグニチャのアップロードまたはダウンロード」（P.5-115）のステップ 2 にある TFTP サーバのセットアップのガイドラインを参照してください。

ステップ 3　カスタム シグニチャ ファイル（*.sig）を TFTP サーバ上のデフォルト ディレクトリに移動します。

ステップ 4　ダウンロード モードまたはアップロード モードを指定するには、**transfer** {**download** | **upload**} **mode tftp** と入力します。

ステップ 5　ダウンロードまたはアップロードするファイルのタイプを指定するには、**transfer** {**download** | **upload**} **datatype signature** と入力します。

ステップ 6　TFTP サーバの IP アドレスを指定するには、**transfer** {**download** | **upload**} **serverip** *tftp-server-ip-address* と入力します。

（注）　TFTP サーバによっては、TFTP サーバ IP アドレスにスラッシュ（/）を入力するだけで、自動的に適切なディレクトリへのパスが判別されるものもあります。

ステップ 7　ダウンロードまたはアップロードのパスを指定するには、**transfer** {**download** | **upload**} **path** *absolute-tftp-server-path-to-file* と入力します。

ステップ 8　ダウンロードまたはアップロードするファイルを指定するには、**transfer** {**download** | **upload**} **filename** *filename.sig* と入力します。

（注）　コントローラは、シグニチャのアップロード時に、ユーザが指定した基本名に「_std.sig」および「_custom.sig」を追加したファイル名を使用して、標準シグニチャ ファイルとカスタム シグニチャ ファイルの*両方*を TFTP サーバにアップロードします。たとえば、「ids1」という名前のシグニチャ ファイルをアップロードする場合、コントローラは自動的に ids1_std.sig と ids1_custom.sig を生成して TFTP サーバにアップロードします。その後、必要に応じて TFTP サーバ上で ids1_custom.sig を変更し（必ず「Revision = custom」を設定してください）、自動的にダウンロードすることもできます。

ステップ 9　**transfer** {**download** | **upload**} **start** と入力し、プロンプトに **y** と応答して現在の設定を確認し、ダウンロードまたはアップロードを開始します。

ステップ 10　シグニチャ頻度が設定された間隔内でしきい値に達するまでの経過時間（秒数）を指定するには、次のコマンドを入力します。

config wps signature interval *signature_id interval*

ここで、*signature_id* は、シグニチャを一意に識別するために使用する数字です。有効な値の範囲は 1 ～ 3600 秒で、デフォルト値はシグニチャによって異なります。

ステップ 11　個々のアクセス ポイント レベルで特定されるべき、1 間隔あたりの一致パケット数を指定するには、次のコマンドを入力します。この値に達すると攻撃が検出されたと判断されます。

config wps signature frequency ***signature_id frequency***

有効な値の範囲は 1 間隔あたり 1 ～ 32,000 パケットで、デフォルト値はシグニチャによって異なります。

ステップ 12　個々のアクセス ポイントでクライアント別に特定されるべき、1 間隔あたりの一致パケット数を指定するには、次のコマンドを入力します。この値に達すると攻撃が検出されたと判断されます。

config wps signature mac-frequency *signature_id mac_frequency*

有効な値の範囲は 1 間隔あたり 1 ～ 32,000 パケットで、デフォルト値はシグニチャによって異なります。

ステップ 13　個々のアクセス ポイント レベルで攻撃が検出されない状態が経過して、アラームを停止できるようになるまでの時間（秒単位）を指定するには、次のコマンドを入力します。

config wps signature quiet-time *signature_id quiet_time*

有効な値の範囲は 60 ～ 32,000 秒で、デフォルト値はシグニチャによって異なります。

ステップ 14　IDS シグニチャを有効または無効にするには、次のいずれかを実行します。

- 個々の IDS シグニチャを有効または無効にするには、次のコマンドを入力します。

  config wps signature {**standard** | **custom**} **state** *signature_id* {**enable** | **disable**}

- IDS シグニチャ処理を有効または無効（すべての IDS シグニチャの処理を有効または無効）にするには、次のコマンドを入力します。

  config wps signature {**enable** | **disable**}

（注）　IDS シグニチャ処理を無効にすると、個々のシグニチャの設定状態に関係なく、すべてのシグニチャが無効になります。

ステップ 15　変更を保存するには、次のコマンドを入力します。

save config

ステップ 16　必要に応じて、特定のシグニチャまたはすべてのシグニチャをデフォルト値にリセットできます。そのためには、次のコマンドを入力します。

config wps signature reset {*signature_id* | **all**}

（注）　シグニチャをデフォルト値にリセットするには、コントローラの CLI しか使用できません。

CLI を使用した IDS シグニチャ イベントの表示

コントローラの CLI を使用してシグニチャ イベントを表示するには、次のコマンドを使用します。

1. コントローラで IDS シグニチャ処理が有効になっているか無効になっているかを確認するには、次のコマンドを入力します。

   show wps summary

   次のような情報が表示されます。

```
Auto-Immune
  Auto-Immune................................... Disabled

Client Exclusion Policy
  Excessive 802.11-association failures......... Enabled
  Excessive 802.11-authentication failures...... Enabled
  Excessive 802.1x-authentication............... Enabled
  IP-theft...................................... Enabled
  Excessive Web authentication failure.......... Enabled

Signature Policy
  Signature Processing.......................... Enabled
```

（注）　IDS シグニチャ処理を無効にすると、個々のシグニチャの設定状態に関係なく、すべてのシグニチャが無効になります。

2. コントローラにインストールされているすべての標準シグニチャとカスタム シグニチャの要約を個々に表示するには、次のコマンドを入力します。

   show wps signature summary

   次のような情報が表示されます。

```
Signature-ID..................................... 1
Precedence....................................... 1
Signature Name................................... Bcast deauth
Type............................................. standard
FrameType........................................ management
State............................................ enabled
Action........................................... report
Tracking......................................... per Signature and Mac
Signature Frequency.............................. 50 pkts/interval
Signature Mac Frequency.......................... 30 pkts/interval
Interval......................................... 1 sec
Quiet Time....................................... 300 sec
Description...................................... Broadcast Deauthentication Frame
Patterns:
                0(Header):0x00c0:0x00ff
               4(Header):0x01:0x01
```

3. 有効化されたシグニチャによって検出された攻撃の数を表示するには、次のコマンドを入力します。

   show wps signature events summary

   次のような情報が表示されます。

```
Precedence Signature Name     Type     # Events
---------- ------------------ -----    -----------
1          Bcast deauth       Standard    2
2          NULL probe resp 1  Standard    1
```

4. 特定の標準シグニチャまたはカスタム シグニチャによって検出された攻撃の詳細を表示するには、次のコマンドを入力します。

   show wps signature events {**standard** | **custom**} *precedence#* **summary**

   次のような情報が表示されます。

```
Precedence....................................... 1
Signature Name................................... Bcast deauth
Type............................................. Standard
Number of active events.......................... 2

Source MAC Addr   Track Method  Frequency No. APs Last Heard
----------------- ------------  --------- -------- ------------------------
00:01:02:03:04:01 Per Signature   4          3    Tue Dec 6 00:17:44 2005
00:01:02:03:04:01 Per Mac         6          2    Tue Dec 6 00:30:04 2005
```

5. アクセス ポイントによってシグニチャ別/チャネル別に追跡される攻撃の詳細を表示するには、次のコマンドを入力します。

   show wps signature events {**standard** | **custom**} *precedence#* ***detailed per-signature*** *source_mac*

6. アクセス ポイントによって個別クライアント ベース（MAC アドレス）で追跡される攻撃の詳細を表示するには、次のコマンドを入力します。

show wps signature events {**standard** | **custom**} *precedence#* ***detailed per-mac*** *source_mac*

次のような情報が表示されます。

```
Source MAC.................................... 00:01:02:03:04:01
Precedence.................................... 1
Signature Name................................ Bcast deauth
Type.......................................... Standard
Track......................................... Per Mac
Frequency..................................... 6
Reported By
    AP 1
        MAC Address........................... 00:0b:85:01:4d:80
        Name.................................. Test_AP_1
        Radio Type............................ 802.11bg
        Channel............................... 4
        Last reported by this AP.............. Tue Dec 6 00:17:49 2005
    AP 2
        MAC Address........................... 00:0b:85:26:91:52
        Name.................................. Test_AP_2
        Radio Type............................ 802.11bg
        Channel............................... 6
         Last reported by this AP.............. Tue Dec 6 00:30:04 2005
```

wIPS の設定

シスコの適応型 Wireless Intrusion Prevention System（wIPS）は、無線の脅威の検出およびパフォーマンスの管理のための高度な手法です。この手法では、ネットワーク トラフィック分析、ネットワーク デバイス / トポロジに関する情報、シグニチャベースの技法、および異常検出を組み合わせることにより、非常に正確で全面的な無線の脅威防御を実現できます。インフラストラクチャに完全に統合されたソリューションを採用すると、有線ネットワークと無線ネットワークの両方で無線トラフィックを継続的に監視し、ネットワークインテリジェンスを使用してさまざまなソースからの攻撃を分析することにより、損害または漏洩が発生する前に、攻撃をより正確に特定し事前に防止することができます。

シスコの適合型 wIPS の実装には Cisco 3300 シリーズ Mobility Services Engine（MSE）が必要です。MSE はアプライアンスベースのソリューションであり、Cisco Aironet アクセス ポイントの継続的な監視によって収集された情報の処理を集中化します。シスコの適応型 wIPS の機能と、MSE への WCS の統合により、wIPS サービスで wIPS ポリシーとアラームの設定、監視、およびレポートを行うことができます。

シスコの適応型 wIPS はコントローラに設定されていません。その代わり、プロファイル設定が WCS から wIPS サービスに転送され、wIPS サービスによってそのプロファイルがコントローラに転送されます。プロファイルはコントローラのフラッシュメモリに格納され、アクセス ポイントとコントローラが接続するとアクセス ポイントへ送信されます。アクセス ポイントのアソシエートが解除され、別のコントローラへ接続すると、アクセス ポイントは新しいコントローラから wIPS プロファイルを受信します。

監視モードのアクセス ポイントは、ポリシー プロファイルに基づいて、wIPS サービスへコントローラを介して定期的にアラームを送信します。wIPS サービスはアラームを格納および処理して、SNMP トラップを生成します。WCS は自身の IP アドレスをトラップの宛先として設定し、SNMP トラップを MSE から受信します。

（注）　上記のすべてのケースで、コントローラは単なる転送デバイスとして機能します。

（注）　シスコの適応型 wIPS の詳細については、『*Cisco Wireless Control System Configuration Guide, Release 6.0*』および『*Cisco 3300 Series Mobility Services Engine Configuration Guide, Release 6.0*』を参照してください。

アクセス ポイントでの wIPS の設定

コントローラの CLI を使用して、アクセス ポイント上で wIPS を設定する手順は、次のとおりです。wIPS を有効にするには、次の手順を実行する必要があります。

ステップ 1　監視モード用のアクセス ポイントを設定にするには、次のコマンドを入力します。

config ap mode monitor *Cisco_AP*

ステップ 2　アクセス ポイントがリブートされるが操作を続行するかどうかをたずねる警告が表示されたら、**Y** と入力します。

ステップ 3　変更を保存するには、次のコマンドを入力します。

save config

ステップ 4　アクセス ポイント無線を無効にするには、次のコマンドを入力します。

config {**802.11a** | **802.11b**} **disable** *Cisco_AP*

ステップ 5　アクセス ポイントで wIPS サブモードを設定するには、次のコマンドを入力します。

config ap mode monitor submode wips *Cisco_AP*

（注）　アクセス ポイントで wIPS を無効にするには、**config ap mode monitor submode none** *Cisco_AP* コマンドを入力します。

ステップ 6　アクセス ポイントに対して、wIPS に最適化されたチャネル スキャンを有効にするには、次のコマンドを入力します。

config ap monitor-mode wips-optimized *Cisco_AP*

アクセス ポイントは、250 ミリ秒の間、各チャネルをスキャンします。監視設定に基づいてスキャンされるチャネルの一覧が取得されます。次の 3 つのチャネル セットが利用できます。

- **All**：アクセス ポイントの無線でサポートされているすべてのチャネル
- **Country**：アクセス ポイントの使用国でサポートされているすべてのチャネルのみ
- **DCA**：チャネルの動的割り当て（DCA）アルゴリズムによって使用されるチャネル セットのみ（デフォルトでは、アクセス ポイントの使用国で許可された、オーバーラップしないすべてのチャネルを含む）。

show advanced {**802.11a** | **802.11b**} **monitor** コマンドの出力の 802.11a または 802.11b Monitor Channels フィールドに、監視設定チャネル セットが表示されます。

```
Default 802.11b AP monitoring
  802.11b Monitor Mode..................................... enable
  802.11b Monitor Channels................................. Country channels
  802.11b AP Coverage Interval............................. 180 seconds
  802.11b AP Load Interval................................. 60 seconds
  802.11b AP Noise Interval................................ 180 seconds
  802.11b AP Signal Strength Interval...................... 60 seconds
```

ステップ 7　アクセス ポイント無線を再度有効にするには、次のコマンドを入力します。

config {802.11a | 802.11b} enable *Cisco_AP*

ステップ 8　変更を保存するには、次のコマンドを入力します。

save config

wIPS 情報の表示

コントローラの CLI を使用して wIPS 情報を確認するには、次のコマンドを入力します。

（注） コントローラ GUI からアクセス ポイント サブモードを表示することもできます。そのためには、[Wireless] > [Access Points] > [All APs] > アクセスポイント名 > [Advanced] タブを選択します。アクセス ポイントが監視モードで、アクセス ポイントで wIPS サブモードが設定されている場合、[AP Sub Mode] フィールドに *wIPS* と表示されます。アクセス ポイントが監視モードではなく、アクセス ポイントで wIPS サブモードが設定されていない場合、[AP Sub Mode] フィールドには *None* と表示されます。

1. アクセス ポイントで wIPS サブモードを表示するには、次のコマンドを入力します。

   show ap config general *Cisco_AP*

   次のような情報が表示されます。

```
Cisco AP Identifier.............................. 3
Cisco AP Name.................................... AP1131:46f2.98ac
...
AP Mode ......................................... Monitor
Public Safety ................................... Disabled  Disabled
AP SubMode ...................................... WIPS
...
```

2. アクセス ポイントに設定された、wIPS に最適化されたチャネル スキャンを表示するには、次のコマンドを入力します。

   show ap monitor-mode summary

   次のような情報が表示されます。

```
AP Name             Ethernet MAC         Status      Scanning Channel List
------------------ -------------------- ----------  ------------------------
AP1131:46f2.98ac    00:16:46:f2:98:ac     wIPS          1, 6, NA, NA
```

3. WCS によってコントローラに転送される wIPS 設定を表示するには、次のコマンドを入力します。

   show wps wips summary

   次のような情報が表示されます。

```
Policy Name.............. Default
Policy Version.......... 3
```

4. コントローラでの wIPS 動作の現在の状態を表示するには、次のコマンドを入力します。

   show wps wips statistics

   次のような情報が表示されます。

```
Policy Assignment Requests............ 1
Policy Assignment Responses........... 1
Policy Update Requests................ 0
Policy Update Responses............... 0
```

```
Policy Delete Requests.............. 0
Policy Delete Responses............. 0
Alarm Updates....................... 13572
Device Updates...................... 8376
Device Update Requests.............. 0
Device Update Responses............. 0
Forensic Updates.................... 1001
Invalid WIPS Payloads............... 0
Invalid Messages Received........... 0
NMSP Transmitted Packets............ 22950
NMSP Transmit Packets Dropped....... 0
NMSP Largest Packet................. 1377
```

5. コントローラ上の wIPS 統計情報をクリアするには、次のコマンドを入力します。

   clear stats wps wips

意図的な悪用の検出

コントローラでは、潜在的な脅威を知らせる役割を果たす 3 つの意図的な悪用に関するアラームをサポートしています。これらはデフォルトで有効になっているため、コントローラ上での設定は不要です。

- **ASLEAP 検出**：コントローラは、攻撃者が LEAP クラック ツールを起動した場合にトラップを生成します。トラップ メッセージは、コントローラのトラップ ログで表示可能です。
- **擬似アクセス ポイント検出**：高密度アクセス ポイント環境でのアクセス ポイント アラームの誤作動を回避するために、コントローラは擬似アクセス ポイント検出ロジックを調整します。
- **ハニーポット アクセス ポイント検出**：コントローラは、不正なアクセス ポイントが管理対象 SSID を使用している場合にトラップ イベントを生成します（コントローラで設定された WLAN）。トラップ メッセージは、コントローラのトラップ ログで表示可能です。