アドミニストレーション ガイド

Cisco WAP571 Wireless-AC/N Premium Dual Radio Access Point with PoE

Cisco WAP571E Wireless-AC/N Premium Dual Radio Outdoor Access Point

目次

1

作業の開始

ここでは、ワイヤレス アクセス ポイント（WAP）デバイスの Web ベースの設定ユーティリティの概要について説明します。具体的な内容は、次のとおりです。

- Web ベースの設定ユーティリティの開始
- アクセス ポイント セットアップ ウィザードの使用
- はじめに
- ウィンドウ ナビゲーション

Web ベースの設定ユーティリティの開始

ここでは、システム要件と Web ベースの設定ユーティリティ内の移動方法について説明します。

サポートされるブラウザ

- Internet Explorer 7.0 以上
- Chrome 5.0 以上
- Firefox 3.0 以上
- Safari 3.0 以上

ブラウザについての制約事項

- Internet Explorer 6 を使用している場合、IPv6 アドレスで直接アクセス ポイントにアクセスすることはできません。ただし、ドメイン ネーム シ ステム（DNS）サーバを使用して、IPv6 アドレスを含むドメイン名を作成し、そのドメイン名を IPv6 アドレスの代わりにアドレス バーに指定することはできます。
- Internet Explorer 8 を使用する場合は、Internet Explorer からセキュリティ設定を設定できます。[ツール]、[インターネット オプション] の順に選択し、[セキュリティ] タブを選択します。[ローカル イントラネット] を選択し、[サイト] を選択します。[詳細設定] を選択し、[追加] を選択します。アクセス ポイントの

イントラネット アドレス（http://*<ip-address>*）をローカル イントラネット ゾーンに追加します。IP アドレスはサブネット IPアドレスとして指定することもできます。これにより、サブネット内のすべてのアドレスをローカル イントラネット ゾーンに追加できます。

- 管理ステーションに複数の IPv6 インターフェイスがある場合、IPv6 ローカル アドレスではなく IPv6 グローバル アドレスを使用して、ブラウザからアクセス ポイントにアクセスしてください。

ログアウト

デフォルトで、Web ベースの AP 設定ユーティリティは 10 分間非アクティブな状態が続くとログアウトされるようになっています。デフォルトのタイムアウト時間を変更する手順については、「**HTTP/HTTPS サービス**」を参照してください。

ログアウトするには、Web ベースの AP 設定ユーティリティの右上隅の [ログアウト] をクリックします。

アクセス ポイント セットアップ ウィザードの使用

アクセス ポイントに初めてログインすると（または工場出荷時設定にリセットされた後にログインすると）、初期設定の実行を支援するアクセス ポイント セットアップ ウィザードが表示されます。ウィザードを完了するには、次の手順を実行します。

アクセス ポイント セットアップ ウィザードの使用

注 [キャンセル（Cancel）] をクリックしてウィザードをバイパスすると、[パスワードの変更（Change Password）] ページが表示されます。ログインするデフォルトのパスワードを変更できます。その他すべての設定については、工場出荷時設定が適用されますパスワードを変更した後に再びログインする必要があります。

ステップ 1 ウィザードの初期ページで [次へ（Next）] をクリックします。[デバイスの設定 - ファームウェアのアップグレード（Configure Device - Firmware Upgrade）] ウィンドウが表示されます。

ステップ 2 [参照（Browse）] ボタンをクリックして、ネットワーク上のファームウェア イメージ ファイルを選択します。

注 使用するファームウェア アップグレード ファイルは、tar ファイルである必要があります。bin ファイルまたはその他の形式のファイルをアップグレードに使用しないでください。これらのタイプのファイルは機能しません。

ステップ 3 [アップグレード(Upgrade)] をクリックして新しいファームウェア イメージを適用します。または [スキップ(Skip)] をクリックすると、[デバイスの設定 - 設定の復元(Configure Device - Configuration Restore)] ウィンドウが表示されます。

注 新しいファームウェアのアップロードには数分かかる場合があります。新しいファームウェアのアップロード中は、ページを更新したり、別のページに移動したりしないでください。ファームウェアのアップロードが中止されます。プロセスが完了すると、アクセス ポイントが再起動して通常の動作を再開します。

ステップ 4 [参照(Browse)] ボタンをクリックして、ネットワーク上の設定ファイルを選択します。

注 コンフィギュレーション ファイルは XML 形式であり、WAP デバイスに関するすべての情報を格納しています。

ステップ 5 [アップグレード(Upgrade)] をクリックして、選択したコンフィギュレーション ファイルを適用します。または [スキップ(Skip)] をクリックすると、[デバイスの設定 - IP アドレス(Configure Device - IP Address)] ウィンドウが表示されます。

注 コンフィギュレーション ファイルの復元には数分かかる場合があります。コンフィギュレーション ファイルの復元中は、ページを更新したり、別のページに移動したりしないでください。設定の復元が中止されます。プロセスが完了すると、アクセス ポイントが再起動して通常の動作を再開します。

ステップ 6 WAP デバイスに DHCP サーバから IP アドレスを受信させる場合は、[ダイナミック IPアドレス(DHCP)(Dynamic IP Address (DHCP))] をクリックします。[静的IPアドレス(Static IP Address)] を選択して、IP アドレスを手動で設定することもできます。これらのフィールドの説明については、「IPv4 設定」を参照してください。

ステップ 7 [次へ(Next)] をクリックします。[シングルポイント設定 - クラスタの設定(Single Point Setup-Set a Cluster)] ウィンドウが表示されます。シングル ポイント設定の説明については、「シングル ポイント設定の概要」を参照してください。

ステップ 8 WAP デバイスの新しいシングル ポイント設定を作成するには、[新しいクラスタの作成(Create a New Cluster)] を選択し、[新しいクラスタ名(New Cluster Name)] でクラスタ名を指定します。同じクラスタ名でデバイスを設定し、他の WAP デバイスでシングル ポイントセットアップ モードを有効にすると、それらは自動的にグループに参加します。

ネットワーク上にすでにクラスタがある場合は、[既存のクラスタに参加(Join an Existing Cluster)] をクリックし、[既存クラスタ名(Existing Cluster Name)] にクラスタ名を入力することにより、このデバイスをクラスタに追加できます。

このデバイスをこの時点でシングル ポイント設定に参加させない場合は、[シングルポイント設定を有効にしないでください(Do not Enable Single Point Setup)] をクリックします。

(オプション) WAP デバイスの物理的な位置を示すために [APの位置(AP Location)] フィールドにテキストを入力することができます。

ステップ 9 [次へ(Next)] をクリックします。[デバイスの構成 - システムの日付と時刻の設定(Configure Device - Set System Date)] ウィンドウが表示されます。

ステップ 10 タイム ゾーンを選択し、システム時刻を手動で設定するか、NTP サーバから時刻を取得するように WAP デバイスをセットアップします。これらのオプションの説明については、「時刻設定」を参照してください。

注 コンピュータの日時を設定する場合は、[システム時刻(System Time)] の横にある矢印を使用して現在のコンピュータから時刻を設定できます。

ステップ 11 [次へ(Next)] をクリックします。[セキュリティの有効化 - パスワードの設定(Enable Security - Set Password)] ウィンドウが表示されます。

ステップ 12 [新しいパスワード(New Password)] にパスワードを入力し、[パスワードの確認(Confirm Password)] フィールドにもう一度パスワードを入力します。[ユーザ名(Username)] フィールドでユーザ名を変更できます。パスワードの詳細については、「ユーザ アカウント」を参照してください。

注 パスワード セキュリティ ルールを無効にする場合は、[パスワードの複雑性(Password Complexity)] チェック ボックスをオフにできます。ただし、パスワード セキュリティ ルールは有効にしたままにすることを強くお勧めします。

ステップ 13 [次へ(Next)] をクリックします。無線 1 インターフェイスに関する [セキュリティの有効化 - ワイヤレスネットワークの命名(Enable Security - Name Your Wireless Network)] ウィンドウが表示されます。

注 このウィンドウとこの後の 2 つのウィンドウ([ワイヤレスセキュリティ(Wireless Security)] および [VLAN ID]) では、まず、無線 1 インターフェイスについて、次の設定値を設定します。次に、無線 2 についてこれらの設定値を設定できるウィンドウが再表示されます。

ステップ 14 [ネットワーク名(Network Name)] にネットワーク名を入力します。この名前は、デフォルト ワイヤレス ネットワークの SSID として使用されます。

ステップ 15 [次へ(Next)] をクリックします。[セキュリティの有効化 - ワイヤレスネットワークの保護(Enable Security - Secure Your Wireless Network)] ウィンドウが表示されます。

ステップ 16 セキュリティ暗号化タイプを選択し、セキュリティ キーを入力します。これらのオプションの説明については、「システム セキュリティ」を参照してください。

ステップ 17 [次へ(Next)] をクリックします。ウィザードに [セキュリティの有効化 - ワイヤレスネットワークのVLAN IDの割り当て(Enable Security- Assign the VLAN ID For Your Wireless Network)] ウィンドウが表示されます。

ステップ 18 ワイヤレス ネットワークで受信されるトラフィックの VLAN ID を入力します。

ワイヤレス トラフィックを VLAN 1 の管理トラフィックと分離するために、デフォルト(1) とは異なる VLAN ID をワイヤレス トラフィックに割り当てる必要があります。

ステップ 19 [次へ(Next)] をクリックします。

ステップ 20 WAP571/E デバイスの場合は、無線 2 の設定を可能にする [ネットワーク名(Network Name)]、[ワイヤレスセキュリティ(Wireless Security)]、および [VLAN ID] ページが表示されます。無線 2 の設定が完了したら、[次へ(Next)] をクリックします。

ウィザードに [キャプティブポータルの有効化 - ゲストネットワークの作成(Enable Captive Portal - Create Your Guest Network)] ウィンドウが表示されます。

ステップ 21 ネットワーク上のゲストの認証方式をセットアップするかどうかを選択し、[次へ(Next)] をクリックします。

[いいえ(No)] をクリックする場合は、ステップ 29 に進みます。

[はい(Yes)] をクリックすると、ウィザードに [キャプティブポータルの有効化 - ゲストネットワークの命名(Enable Captive Portal - Name Your Guest Network)] ウィンドウが表示されます。

ステップ 22 無線 1 について、[ゲストネットワーク名(Guest Network Name)] にゲスト ネットワーク名を指定します。WAP571/E デバイスの場合は、ゲスト ネットワークが**無線 1** または **無線 2** を使用するかどうかを選択します。

ステップ 23 [次へ(Next)] をクリックします。ウィザードに [キャプティブポータルの有効化 - ゲストネットワークの保護(Enable Captive Portal - Secure Your Guest Network)] ウィンドウが表示されます。

ステップ 24 ゲスト ネットワークのセキュリティ暗号化タイプを選択し、セキュリティ キーを入力します。これらのオプションの説明については、「システム セキュリティ」を参照してください。

ステップ 25 [次へ(Next)] をクリックします。ウィザードに [キャプティブポータルの有効化 - VLAN IDの割り当て(Enable Captive Portal - Assign the VLAN ID)] ウィンドウが表示されます。

ステップ 26 ゲスト ネットワークの VLAN ID を指定します。ゲスト ネットワークの VLAN ID は、管理 VLAN ID と異なっている必要があります。

ステップ 27 [次へ(Next)] をクリックします。ウィザードに [キャプティブポータルの有効化 - リダイレクトURLの有効化(Enable Captive Portal - Enable Redirect URL)] ウィンドウが表示されます。

ステップ 28 [リダイレクトURLを有効化(Enable Redirect URL)] を選択し、[リダイレクトURL(Redirect URL)] フィールドで完全修飾ドメイン名または IP アドレス(「http://」を含む)を指定します。指定すると、ゲスト ネットワーク ユーザが、認証後に、指定された URL にリダイレクトされるようになります。

ステップ 29 [次へ(Next)] をクリックします。ウィザードに [サマリ - 設定の確認(Summary - Confirm Your Settings)] ウィンドウが表示されます。

ステップ 30 設定した設定値を確認します。[戻る(Back)] をクリックして、1 つまたは複数の設定を再設定します。[キャンセル(Cancel)] をクリックすると、すべての設定が前の値またはデフォルト値に戻ります。

ステップ 31 修正したら、[送信(Submit)] をクリックします。WAP セットアップ設定が保存され、確認ウィンドウが表示されます。

ステップ 32 [完了(Finish)] をクリックします。変更したパスワードで AP にログインできる [ログイン(Login)] ウィンドウが表示されます。

はじめに

クイック ナビゲーションにより、簡単にデバイス設定を実行できるように、[はじめに] ページには、一般的なタスクを実行するためのリンクが用意されています。[はじめに] ページは、Web ベースの AP 設定ユーティリティにログインするたびに表示されるデフォルト ウィンドウです。

カテゴリ	リンク名(ページ上)	リンク ページ
初期セットアップ	セットアップ ウィザードの実行	アクセス ポイント セットアップ ウィザードの使用
	無線設定の構成	無線
	ワイヤレス ネットワーク設定の構成	ネットワーク
	LAN 設定の構成	LAN
	シングル ポイント設定の構成	シングル ポイント設定の概要
デバイス ステータス	システムの要約	システム概要
	ワイヤレス ステータス	ネットワーク インターフェイス
クイック アクセス	アカウント パスワードの変更	ユーザ アカウント
	デバイスのファームウェアのアップグレード	ファームウェアの管理
	構成のバックアップ/リストア	構成ファイルのダウンロード/バックアップ

ウィンドウ ナビゲーション

ナビゲーションを使用して Web ベースのユーティリティ内を移動します。

設定ユーティリティのヘッダー

設定ユーティリティのヘッダーには標準情報が含まれており、各ページの上部に表示されます。ヘッダーには次のボタンがあります。

ナビゲーション ウィンドウ/メイン メニュー

ボタン名	説明
(ユーザ)	AP にログインしているユーザのアカウント名 (Administrator または Guest) です。工場出荷時のユーザ名は **cisco** です。
ログアウト	クリックすると、Web ベースの AP 設定ユーティリティからログアウトします。
言語	ボタンの上にマウス ポインタを移動させ、言語を選択します。
バージョン情報	クリックすると、AP のタイプおよびバージョン番号が表示されます。
ヘルプ	クリックすると、オンライン ヘルプが表示されます。オンラインヘルプは、UTF-8 エンコーディングを使用するブラウザで表示されるように設計されています。オンライン ヘルプが文字化けする場合は、ブラウザのエンコーディング設定が UTF-8 に設定されていることを確認します。

ナビゲーション ウィンドウ (またはメイン メニュー) は、各ページの左側にあります。ナビゲーション ウィンドウは、WAP デバイスの最上位機能のリストです。メイン メニュー項目の前に矢印がある場合は、選択して展開すると、各グループのサブメニューが表示されます。その後、必要なサブメニュー項目を選択して、関連ページを開くことができます。

管理ボタン

さまざまなページに表示されるよく使用されるボタンを次の表に示します。

ボタン名	説明
追加	新しいエントリをテーブルまたはデータベースに追加します。
キャンセル	ページに加えた変更をキャンセルします。
すべてクリア	ログ テーブルのすべてのエントリを消去します。
バージョン情報	クリックすると、AP のタイプおよびバージョン番号が表示されます。
削除	テーブルのエントリを削除します。まずエントリを選択してください。
編集	既存のエントリを編集または修正します。まずエントリを選択してください。
更新	現在のページを最新のデータで再表示します。
保存	設定またはコンフィギュレーションを保存します。
更新	新しい情報でスタートアップ コンフィギュレーションを更新します。

2

ステータスと統計

ここでは、ステータスと統計の表示方法について説明します。具体的な内容は次のとおりです。

- システム概要
- ネットワーク インターフェイス
- トラフィック統計
- ワイヤレス マルチキャスト転送の統計
- ワークグループ ブリッジ送信/受信
- 関連付けられたクライアント
- TSPEC クライアント アソシエーション
- TSPEC ステータスと統計
- TSPEC AP 統計
- 無線統計
- 電子メール アラート ステータス
- ログ

システム概要

[システム概要] ページには、ハードウェア モデルの説明、ソフトウェア バージョン、最後の再起動から経過した時間などの基本情報が表示されます。

システム情報を表示するには、[ステータスと統計] > [システム概要] の順に選択します。[はじめに] ページの [デバイス ステータス] の下で、[システム概要] を選択することもできます。

[システム概要] ページには、次の情報が表示されます。

- [PID VID]: WAP ハードウェアのモデルおよびバージョン。
- [シリアル番号]: Cisco WAP デバイスのシリアル番号。
- [基本 MAC アドレス]: WAP の MAC アドレス。
- [ファームウェア バージョン(アクティブ イメージ)]: アクティブ イメージのファームウェア バージョン番号。
- [ファームウェアの MD5 チェックサム(アクティブイメージ)]: アクティブ イメージのチェックサム。
- [ファームウェア バージョン(非アクティブ)]: バックアップ イメージのファームウェア バージョン番号。
- [ファームウェア MD5 チェックサム(非アクティブ)]: バックアップ イメージのチェックサム。
- [ホスト名]: デバイスに割り当てられた名前。
- [システム稼働時間]: 最後の再起動から経過した時間。
- [システム時刻]: 現在のシステム時刻。
- [電源]: システムは、PoE Power-Sourcing Equipment (PSE; 給電側機器) から Power over Ethernet を受信します。

[TCP/UDP サービス] 表に、WAP で動作するプロトコルとサービスに関する基本情報が表示されます。

- [サービス]: サービスの名前(使用可能な場合)。
- [プロトコル]: サービスで使用される基本的な転送プロトコル(TCP または UDP)。
- [ローカル IP アドレス]: WAP デバイス上でこのサービスに接続されているリモート デバイスの IP アドレス(該当する場合)。[すべて] は、デバイス上のすべての IP アドレスでこのサービスを使用できることを示します。

- [ローカル ポート]: サービスのポート番号。
- [リモート IP アドレス]: このサービスを使用しているリモート ホストの IP アドレス（該当する場合）。[すべて] は、システムにアクセスするすべてのリモート ホストにサービスを使用できることを示します。
- [リモート ポート]: このサービスと通信するリモート デバイスのポート番号。
- [接続状態]: サービスの状態。UDP の場合、[アクティブ] または [確立済み] 状態の接続のみが表に表示されます。TCP の状態は次のとおりです。
  - [リスニング] : サービスは接続要求をリスニングしています。
  - [アクティブ] : 接続セッションが確立され、パケットが送信 / 受信されています。
  - [確立済み] : このプロトコルに関する各デバイスの役割に応じて、WAP デバイスとサーバまたはクライアント間で接続セッションが確立されています。
  - [Time Wait] : クロージング シーケンスが開始されていて、WAP は接続を終了するまでシステム定義のタイムアウト時間（通常は 60 秒）待機しています。

[更新] をクリックすると、画面を更新して、最新情報を表示できます。

ネットワーク インターフェイス

[ネットワーク インターフェイス] ページには、有線および無線インターフェイスの設定およびステータス情報が表示されます。ネットワーク インターフェイス情報を表示するには、[ステータスと統計] > [ネットワーク インターフェイス] の順に選択します。

次の情報が表示されます。

- [LAN ステータス]: 次の LAN インターフェイス情報が表示されます。
  - [MAC アドレス] : WAP デバイスの MAC アドレス。
  - [IP アドレス] : WAP デバイスの IP アドレス。
  - [サブネット マスク] : WAP デバイスのサブネット マスク。
  - [デフォルト ゲートウェイ] : WAP デバイスのデフォルト ゲートウェイ。

- [ドメイン ネーム サーバ -1] : WAP デバイスで使用されるドメイン ネーム サーバ 1 の IP アドレス。
- [ドメイン ネーム サーバ -2] : WAP デバイスで使用されるドメイン ネームサーバ 2 の IP アドレス。
- [IPv6 アドレス] : WAP デバイスの IPv6 アドレス。
- [IPv6 自動設定グローバル アドレス] : IPv6 の自動設定済みグローバル アドレス。
- [IPv6 リンク ローカル アドレス] : WAP デバイスの IPv6 リンク ローカル アドレス。
- [デフォルト IPv6 ゲートウェイ] : WAP デバイスのデフォルト IPv6 ゲートウェイ。
- [IPv6-DNS-1] : WAP デバイスで使用される IPv6 DNS サーバ 1 の IPv6 アドレス。
- [IPv6-DNS-2] : WAP デバイスで使用される IPv6 DNS サーバ 2 の IPv6 アドレス。

次の設定は、内部インターフェイスに適用されます。設定を変更するには、[編集] リンクをクリックします。[IPv4 設定] ページにリダイレクトされます。

- [ポート ステータス]:LAN インターフェイスのステータスが表示されます。
- [インターフェイス]:イーサネット インターフェイスの数。
  - [リンク ステータス] : イーサネット インターフェイスのステータス。
  - [ポート速度] : イーサネット インターフェイスの速度。
  - [デュプレックス モード] : イーサネット インターフェイスのデュプレックス モード。
  - [グリーン イーサネット ステータス] : イーサネット インターフェイスのステータス。

設定を変更するには、[編集] リンクをクリックします。[ポート設定] ページにリダイレクトされます。

- [VLAN ステータス]:次のすべての既存 VLAN の情報が表示されます。
  - [VLAN ID] : VLAN の ID。
  - [説明] : VLAN の説明。
  - [Eth] : このインターフェイスは、VLAN のタグ付きまたはタグなしメンバーです。

設定を変更するには、[編集] リンクをクリックします。[VLAN 設定] ページにリダイレクトされます。

- [無線ステータス]: 次のワイヤレス無線インターフェイスの情報が表示されます。
  - [ワイヤレス無線] : ワイヤレス無線モードが無線インターフェイスに対して有効または無効になっています。
  - [MAC アドレス] : 無線インターフェイスに関連付けられた MAC アドレス。
  - [モード] : 無線インターフェイスで使用される 802.11 モード（a/b/g/n/ac）。
  - [チャネル] : 無線インターフェイスで使用されるチャネル。
  - [動作帯域幅] : 無線インターフェイスで使用される動作帯域幅。

設定を変更するには、[編集] リンクをクリックします。[無線] ページにリダイレクトされます。

- [インターフェイス ステータス]: 各 Virtual Access Point（VAP; 仮想アクセス ポイント）および各 Wireless Distribution System（WDS; ワイヤレス ディストリビューション システム）インターフェイスの次のステータス情報が表示されます。
- [インターフェイス]: WAP デバイスのワイヤレス インターフェイス。
- [名前（SSID）]: ワイヤレス インターフェイス名。
- [ステータス]: VAP の管理ステータス（[動作中] または [停止]）。
- [MAC アドレス]: 無線インターフェイスの MAC アドレス。
- [VLAN ID]: 無線インターフェイスの VLAN ID。
- [プロファイル]: 関連するスケジューラ プロファイルの名前。
- [状態]: 現在の状態（[アクティブ] または [非アクティブ]）。この状態は、VAP がクライアントとデータをやり取りしているかどうかを示します。

[更新] をクリックして、画面を更新し、最新情報を表示します。

トラフィック統計

[トラフィック統計] ページを使用して、WAP の基本情報を表示します。イーサネット インターフェイス、Virtual Access Points（VAP; 仮想アクセス ポイント）およびすべての WDS インターフェイスの送信/受信統計もリアルタイムで表示されます。すべての送信/受信統計には、WAP が最後に起動されてからの合計数が反映されます。WAP を再起動すると、これらの数値は再起動後の送信/受信数の合計を示します。

[トラフィック統計] ページを表示するには、[ステータスと統計情報] > [トラフィック統計] の順に選択します。

[トラフィック統計] ページには、各方向のトラフィックの要約データと統計情報が表示されます。

- [ネットワーク インターフェイス]: イーサネット インターフェイスおよび各 VAP/WDS インターフェイスの名前。

  VAP インターフェイス名の前に WLAN0 および WLAN1 が付いていて、無線インターフェイスを示します（WLAN0 は無線 1 を表し、WLAN1 は無線 2 を表します）。

- [合計パケット数]: この WAP デバイスが送信（[送信] 表）または受信（[受信] 表）した合計パケット数。

- [合計バイト数]: この WAP デバイスが送信（[送信] 表）または受信（[受信] 表）した合計バイト数。

- [合計廃棄パケット数]: この WAP デバイスが送信（[送信] 表）または受信（[受信] 表）した合計廃棄パケット数。

- [合計廃棄バイト数]: この WAP デバイスが送信（[送信] 表）または受信（[受信] 表）した合計廃棄バイト数。

- [エラー]: この WAP デバイスでのデータの送信/受信に関連する合計エラー数。

[更新] をクリックすると、画面を更新して、最新情報を表示できます。

ワイヤレス マルチキャスト転送の統計

[ワイヤレス マルチキャスト転送の統計] ページには、現在の AP に関する基本情報の一部が表示され、AP のワイヤレス マルチキャスト トラフィック インターフェイスおよび両方の無線インターフェイスの VAP の送信/受信統計情報がリアルタイムに表示されます。表示されるすべての送信/受信統計情報は、AP が最後に起動されてからの合計数です。AP を再起動すると、これらの数値は再起動後の送信/受信数の合計を示します。

[ワイヤレス マルチキャスト転送の統計] ページを表示するには、ナビゲーション ペインで、[ステータスと統計情報] > [ワイヤレス マルチキャスト転送の統計] の順に選択します。

送信/受信統計

- [ネットワーク インターフェイス]:イーサネット インターフェイスおよび各 VAP/WDS インターフェイスの名前。

  VAP インターフェイス名の前に WLAN0 および WLAN1 が付いていて、無線インターフェイスを示します(WLAN0 は無線 1 を表し、WLAN1 は無線 2 を表します)。

- [Mcast-Data-Frames]:受信したマルチキャスト データ フレーム数が表示されます。
- [Mcast-Data-Fwd]:転送したマルチキャスト データ フレーム数が示されます。
- [Mcast-Data-Flooded]:フラッディングしたマルチキャスト データ フレーム数が示されます。
- [Mcast-Data-Sentup]:送信したマルチキャスト データ フレーム数が示されます。
- [Mcast-Data-Dropped]:廃棄したマルチキャスト データ フレーム数が示されます。
- [Mfdb-Cache Hits]:MFDB キャッシュ ミス数が表示されます。
- [Mfdb-Cache-MissesIndicates]:送信したマルチキャスト データ フレーム数。

IGMP 統計

- [ネットワーク インターフェイス]:イーサネット インターフェイスおよび各 VAP/WDS インターフェイスの名前。

  VAP インターフェイス名の前に WLAN0 および WLAN1 が付いていて、無線インターフェイスを示します(WLAN0 は無線 1 を表し、WLAN1 は無線 2 を表します)。

- [IGMP-Frames]:受信した IGMP フレーム数が表示されます。
- [IGMP-Frames-Fwd]:受信した IGMP メンバーシップ クエリー数が表示されます。
- [IGMP-Frames-Sentup]:送信した IGMP メンバーシップ レポート数が表示されます。
- [Mfdb-cache-Hits]:MFDB キャッシュ ヒット数が表示されます。
- [Mfdb-Cache-Misses]:MFDB キャッシュ ミス数が表示されます。

マルチキャスト グループ

- [ネットワーク インターフェイス]:イーサネット インターフェイスおよび各 VAP/WDS インターフェイスの名前。

  VAP インターフェイス名の前に WLAN0 および WLAN1 が付いていて、無線インターフェイスを示します(WLAN0 は無線 1 を表し、WLAN1 は無線 2 を表します)。
- [マルチキャスト グループ]:マルチキャスト グループの IP アドレスが表示されます。
- [ステーション]:マルチキャスト グループ ステーションの MAC アドレスが表示されます。
- [パケット]:受信したマルチキャスト グループ ステーションのパケット数が表示されます。

[更新] をクリックすると、画面を更新して、最新情報を表示できます。

ワークグループ ブリッジ送信/受信

[ワークグループ ブリッジ送信/受信] ページには、ワークグループ ブリッジ上のステーション間のトラフィックのパケット数とバイト数が表示されます。ワークグループ ブリッジの設定の詳細は、「ワークグループ ブリッジ」を参照してください。

[ワークグループ ブリッジ送信/受信] ページを表示するには、ナビゲーション ペインで [ステータスと統計情報] > [ワークグループ ブリッジ] の順に選択します。

ワークグループ ブリッジ インターフェイスとして設定されている各ネットワーク インターフェイスの次のフィールドが表示されます。

- [ネットワーク インターフェイス]:イーサネットまたは VAP インターフェイスの名前。WLAN0 は無線 1 を表し、WLAN1 は無線 2 を表します。

- [ステータスと統計情報]:インターフェイスが切断されているか、動作中または停止として管理上設定されているかどうかを示します。
- [VLAN ID]:仮想 LAN(VLAN)の ID。VLAN を使用すると、複数の内部ネットワークおよびゲスト ネットワークを同一 WAP デバイス上に確立できます。VLAN ID は、[VAP] タブで設定します。
- [名前(SSID)]:ワイヤレス ネットワーク名。SSID とも呼ばれます。この英数字のキーは、ワイヤレス ローカル エリア ネットワークを一意に識別します。SSID は、[VAP] タブで設定します。

各ワークグループ ブリッジ インターフェイスの送信/受信方向について、次のその他の情報が表示されます。

- [合計パケット数]:ワークグループ ブリッジの有線クライアントとワイヤレス ネットワーク間でブリッジされた合計パケット数。
- [合計バイト数]:ワークグループ ブリッジの有線クライアントとワイヤレス ネットワーク間でブリッジされた合計バイト数。

[更新] をクリックすると、画面を更新して、最新情報を表示できます。

関連付けられたクライアント

[関連付けられたクライアント] ページを使用して、特定のアクセス ポイントに関連付けられたクライアント ステーションを表示できます。

[関連付けられたクライアント] ページを表示するには、[ステータスと統計情報] > [関連付けられたクライアント] の順に選択します。

関連付けられたステーションは、各ステーションに対して送信/受信されたパケット トラフィックに関する情報とともに表示されます。

- [関連付けられたクライアントの合計数]:現在 AP に関連付けられているクライアントの合計数。
- [ネットワーク インターフェイス]:クライアントが関連付けられている VAP。VAP インターフェイス名の前に WLAN0 および WLAN1 が付いていて、無線インターフェイスを示します(WLAN0 は無線 1 を表し、WLAN1 は無線 2 を表します)。
- [ステーション]:関連付けられたワイヤレス クライアントの MAC アドレス。
- [ステータス]:[認証済み] および [関連付け] ステータスには、基本的な IEEE 802.11 認証および関連付けステータスが表示されます。クライアントが WAP

デバイスへの接続に使用するセキュリティ タイプは関係ありません。このステータスには、IEEE 802.1X 認証または関連付けステータスは表示されません。

このフィールドに関する考慮事項は、次のとおりです。

- WAP デバイスのセキュリティ モードがなしまたは静的 WEP の場合、クライアントの認証および関連付けステータスは期待どおりに表示されます。つまり、クライアントが WAP デバイスに対して認証済みと表示されている場合、データを送信 / 受信できます（静的 WEP では、IEEE 802.11 認証のみを使用するためです）。
- WAP デバイスが IEEE 802.1X または WPA セキュリティを使用する場合、実際はセキュリティの第 2 レイヤを介して認証されていませんが、クライアント アソシエーションを（IEEE 802.11 セキュリティによって）認証済みと表示できます。

- [ステーションから/ステーションへ]:[ステーションから] のカウンタは、ワイヤレス クライアントによって送信されるパケット数またはバイト数を示します。[ステーションへ] のカウンタは、WAP デバイスからワイヤレス クライアントに送信されるパケット数およびバイト数を示します。
  - [パケット数] : ワイヤレス クライアントから受信（送信）されたパケット数。
  - [バイト数] : ワイヤレス クライアントから受信（送信）されたバイト数。
  - [廃棄パケット数] 受信（送信）後に廃棄されたパケット数。
  - [廃棄バイト数] 受信（送信）後に廃棄されたバイト数。
  - [TS 違反パケット（ステーションから）] : アクティブなトラフィック ストリーム（TS）のアップリンク帯域幅を超過しているか、または、クライアント ステーションが許可されていないアドミッション制御が必要なアクセス カテゴリに対して、クライアント ステーションから WAP デバイスに送信されたパケット数。
  - [TS 違反パケット（ステーションへ）] : アクティブな TS ダウンリンク帯域幅を超過しているか、または、クライアント ステーションが許可されていないアドミッション制御が必要なアクセス カテゴリに対して、WAP デバイスからクライアント ステーションに送信されたパケット数。
- [アップ時間]: クライアントが WAP デバイスに関連付けられる時間。

[更新] をクリックすると、画面を更新して、最新情報を表示できます。

TSPEC クライアント アソシエーション

[TSPEC クライアント アソシエーション] ページには、このアクセス ポイントによって送信/受信される TSPEC クライアント データのリアルタイム情報が表示されます。[TSPEC クライアント アソシエーション] ページの表には、関連付けが開始された後に送信/受信された音声およびビデオ パケットがステータス情報とともに表示されます。

TSPEC は、QoS 対応ワイヤレス クライアントから WAP デバイスに送信されるトラフィックの仕様で、トラフィック ストリーム(TS)用に一定量のネットワーク アクセスを要求します。トラフィック ストリームは、ワイヤレス クライアントによって特定のユーザ プライオリティに属していると識別されるデータ パケットの集合です。音声トラフィック ストリームの例としては、コーデック生成されたデータ パケットを音声プライオリティ トラフィックとしてマークする Wi-Fi CERTIFIED の電話の受話器があります。ビデオ トラフィック ストリームの例としては、企業サーバからのビデオ会議フィードを優先するワイヤレス ノートパソコンのビデオ再生アプリケーションがあります。

TSPEC クライアント アソシエーションの統計情報を表示するには、ナビゲーション ペインで [ステータスと統計情報] > [TSPEC クライアント アソシエーション] の順に選択します。

[TSPEC クライアント アソシエーション] ページには次の情報が表示されます。

[ステータスと統計情報]:

- [ネットワーク インターフェイス]: クライアントが使用する無線インターフェイス。WLAN0 は無線 1 を表し、WLAN1 は無線 2 を表します。
- [SSID]: TS クライアントに関連付けられたサービス セット ID。
- [ステーション]: クライアント ステーションの MAC アドレス。
- [TS ID]: TSPEC トラフィック セッション ID(0 ～ 7 の範囲)。
- [アクセス カテゴリ]: TS アクセス カテゴリ(音声またはビデオ)。
- [方向]: この TS のトラフィックの方向。方向のオプションは、次のとおりです。
  - [アップリンク] : クライアントからデバイス。
  - [ダウンリンク] : デバイスからクライアント。
  - [双方向]

- [ユーザ プライオリティ]: この TS の User Priority（UP; ユーザ プライオリティ）。UP は、IP ヘッダーの UP 部分の各パケットともに送信されます。一般的な値は、次のとおりです。
  - 音声：6 ～ 7
  - ビデオ：4 ～ 5

  値は、他のプライオリティ トラフィック セッションに応じて変わる場合があります。
- [メディア時間]: TS トラフィックが伝送メディアを占有する時間。
- [使用超過イベント]: クライアントが TSPEC 用に確立されたメディア時間を超過した回数。些細な、数少ない違反は無視されます。
- [VAP MAC アドレス]: 仮想アクセス ポイントの MAC アドレス。

[統計情報]:

- [ネットワーク インターフェイス]: クライアントが使用する無線インターフェイス。
- [ステーション]: クライアント ステーションの MAC アドレス。
- [TS ID]: TSPEC トラフィック セッション ID（0 ～ 7 の範囲）。
- [アクセス カテゴリ]: TS アクセス カテゴリ（音声またはビデオ）。
- [方向]: この TS のトラフィックの方向。方向のオプションは、次のとおりです。
  - [アップリンク] : クライアントからデバイス。
  - [ダウンリンク] : デバイスからクライアント。
  - [双方向]
- [ステーションから]: ワイヤレス クライアントから受信したパケット数およびバイト数が表示されます。
  - [パケット数] : 許可された TSPEC を超過したパケット数。
  - [バイト数] : TSPEC が確立されておらず、WAP デバイスによるアドミッションが必要な場合のバイト数。
- [ステーションへ]: WAP デバイスからワイヤレス クライアントに送信されるパケット数およびバイト数。
  - [パケット数] : 許可された TSPEC を超過したパケット数。

- [バイト数]: WAP デバイスによるアドミッションが必要な場合に TSPEC が確立されていないバイト数。

[更新] をクリックすると、画面を更新して、最新情報を表示できます。

TSPEC ステータスと統計

[TSPEC ステータスと統計] ページには、次の情報が表示されます。

- 無線による TSPEC セッションの要約情報。
- VAP による TSPEC セッションの要約情報。
- 無線インターフェイスおよびネットワーク インターフェイスのリアルタイムの送信/受信統計。

表示されるすべての送信/受信統計は、WAP デバイスを最後に起動してからの合計数です。WAP デバイスを再起動すると、これらの数値は再起動後の送信/受信数の合計を示します。

TSPEC ステータスと統計を表示するには、ナビゲーション ペインで [ステータスと統計情報] > [TSPEC ステータスと統計] の順に選択します。

[TSPEC ステータスと統計] ページには、WLAN(無線)および VAP インターフェイスの次のステータス情報が表示されます。

- [ネットワーク インターフェイス]: 無線または VAP インターフェイスの名前。WLAN0 は無線 1 を表し、WLAN1 は無線 2 を表します。
- [アクセス カテゴリ]: このトラフィック ストリームに関連付けられた現在のアクセス カテゴリ(音声またはビデオ)。
- [ステータス]: TSPEC セッションが当該のアクセス カテゴリに対して有効(動作中)か無効(停止)かを示します。

注 ステータスは、設定ステータスです(必ずしも現在のセッションをアクティブに表しているわけではありません)。

- [アクティブなトラフィック ストリーム]: この無線およびアクセス カテゴリについて現在アクティブな TSPEC トラフィック ストリームの数。
- [トラフィック ストリーム クライアント]: この無線およびアクセス カテゴリに関連付けられたトラフィック ストリーム クライアントの数。

- [許可されたメディア時間]:データを送信するために、伝送メディアのこのアクセス カテゴリに割り当てられた時間。この値は、この TS のメディアに割り当てられた最大帯域幅よりも小さいか、これと等しい必要があります。
- [未割り当てのメディア時間]:このアクセス カテゴリに使用されていない帯域幅の時間。

次の統計情報は、ワイヤレス無線インターフェイスの送信/受信パスについて別々に表示されます。

- [アクセス カテゴリ]:このトラフィック ストリームに関連付けられたアクセス カテゴリ(音声またはビデオ)。
- [合計パケット数]:指定されたアクセス カテゴリについて、この無線が送信([送信] 表)または受信([受信] 表)した TS パケットの合計数。
- [合計バイト数]:指定されたアクセス カテゴリで受信した合計バイト数。

次の統計情報は、ネットワーク インターフェイス(VAP)の送信/受信パスについて別々に表示されます。

- [合計音声パケット数]:この VAP に対して、この WAP デバイスが送信([送信] 表)または受信([受信] 表)した合計 TS 音声パケット数。
- [合計音声バイト数]:この VAP に対して、この WAP デバイスが送信([送信] 表)または受信([受信] 表)した合計 TS 音声バイト数。
- [合計ビデオ パケット数]:この VAP に対して、この WAP デバイスが送信([送信] 表)または受信([受信] 表)した合計 TS ビデオ パケット数。
- [合計ビデオ バイト数]:この VAP に対して、この WAP デバイスが送信([送信] 表)または受信([受信] 表)した合計 TS ビデオ バイト数。

[更新] をクリックすると、画面を更新して、最新情報を表示できます。

TSPEC AP 統計

[TSPEC AP 統計] ページには、WAP デバイスに許可/拒否された音声およびビデオ トラフィック ストリームの情報が表示されます。[TSPEC AP 統計] ページを表示するには、ナビゲーション ペインで [ステータスと統計情報] > [TSPEC AP 統計] の順に選択します。

- [音声 ACM の TSPEC 統計の要約]:許可/拒否された音声トラフィック ストリームの合計数。

- [ビデオ ACM のTSPEC 統計の要約]:許可/拒否されたビデオ トラフィック ストリームの合計数。

[更新] をクリックすると、画面を更新して、最新情報を表示できます。

無線統計

[無線統計] ページを使用して、各ワイヤレス無線インターフェイスのパケットレベルおよびバイトレベルの統計情報を表示できます。[無線統計] ページを表示するには、ナビゲーション ペインで [ステータスと統計情報] > [無線統計] の順に選択します。

WAP571/E デバイスでは、統計情報を表示する無線を選択します。

- [受信パケット数]:WAP デバイスが受信した合計パケット数。
- [送信パケット数]:WAP デバイスが送信した合計パケット数。
- [受信バイト数]:WAP デバイスが受信した合計バイト数。
- [送信バイト数]:WAP デバイスが送信した合計バイト数。
- [廃棄された受信パケット数]:WAP デバイスが受信した中で廃棄されたパケット数。
- [廃棄された送信パケット数]:WAP デバイスが送信した中で廃棄されたパケット数。
- [廃棄された受信バイト数]:WAP デバイスが受信した中で廃棄されたバイト数の合計。
- [廃棄された送信バイト数]:WAP デバイスが送信した中で廃棄されたバイト数。
- [受信したフラグメント]:WAP デバイスが受信したフラグメント化されたフレーム数。
- [送信したフラグメント]:WAP デバイスが送信したフラグメント化されたフレーム数。
- [受信したマルチキャスト フレーム]:マルチキャスト ビットが宛先 MAC アドレスに設定されている、受信された MSDU フレームの数。
- [送信したマルチキャスト フレーム]:マルチキャスト ビットが宛先 MAC アドレスに設定されている、正常に送信された MSDU フレームの数。
- [重複フレーム数]:[シーケンス制御] フィールドで重複が示されたフレームを受信した回数。

- [送信失敗数]:送信の試行が短時間の再試行制限または長時間の再試行制限のいずれかを超過していたために MSDU が正常に送信されなかった回数。
- [FCS エラー数]:受信した MPDU フレームで検出された FCS エラーの数。
- [送信の再試行数]:1 回または複数回の再試行後に MSDU が正常に送信された回数。
- [ACK 障害数]:ACK フレームが期待どおりに受信されなかった回数。
- [RTS 障害数]:RTS フレームに応答して CTS フレームが受信されなかった回数。
- [複合化できなかった WEP 数]:無線で複合化できなかったために廃棄されたフレームの数。フレームが暗号化されなかったか、または WAP デバイスでサポートされていないプライバシー オプションで暗号化されたために、フレームが廃棄されることがあります。
- [RTS 成功数]:RTS フレームに応答して CTS フレームが受信された回数。
- [複数の再試行数]:1 回以上の再試行後に MSDU が正常に送信された回数。
- [フレーム送信数]:正常に送信された MSDU の数。

[更新] をクリックすると、画面を更新して、最新情報を表示できます。

電子メール アラート ステータス

[電子メール アラート ステータス] ページには、WAP デバイスで生成された syslog メッセージに基づいて送信される電子メール アラートに関する情報が表示されます。[電子メール アラート ステータス] ページを表示するには、ナビゲーション ペインで [ステータスと統計情報] > [電子メール アラート ステータス] の順に選択します。

- [電子メール アラート ステータス]:電子メール アラートの設定ステータス。ステータスは [有効] または [無効] のいずれかになります。デフォルトは [無効] です。
- [電子メール送信数]:送信した電子メールの合計数。範囲は、32 ビットの符号なし整数です。デフォルトは 0 です。
- [電子メール失敗数]:失敗した電子メールの合計数。範囲は、32 ビットの符号なし整数です。デフォルトは 0 です。
- [最終電子メール送信時間]:最後に電子メールを送信した日付、曜日、時刻。

[更新] をクリックすると、最新情報を表示できます。

ログ

[ログ] ページには、ログインの試行や設定変更などのログ エントリを生成したシステム イベントのリストが表示されます。ログは再起動時にクリアされます。管理者がクリアすることもできます。最大 512 個のイベントが表示されます。古いエントリは、新しいイベント用にスペースを空けるために、必要に応じてリストから削除されます。

[ログ] ページを表示するには、ナビゲーション ペインで [ステータスと統計情報] > [ログ] の順に選択します。

- [タイム スタンプ]:イベントが発生したシステム時間。
- [重要度]:イベントがエラー(err)によるものか、情報(info)なのかを示します。
- [サービス]:イベントに関連付けられたソフトウェア コンポーネント。
- [説明]:イベントの説明。

[更新] をクリックすると、画面を更新して、最新情報を表示できます。

[すべてクリア] をクリックすると、ログからすべてのエントリをクリアできます。

3

管理

ここでは、グローバルなシステム設定を設定し、診断を実施する方法を説明します。

次のトピックがあります。

- システム設定
- ユーザ アカウント
- 時間設定
- ログ設定
- 電子メール アラート
- LED ディスプレイ
- HTTP/HTTPS サービス
- 管理アクセス制御
- ファームウェアの管理
- 構成ファイルのダウンロード/バックアップ
- 構成ファイルのプロパティ
- 構成のコピー/保存
- 再起動
- ディスカバリ - Bonjour
- パケット キャプチャ
- サポート情報
- スパニング ツリー設定

システム設定

[システム設定] ページでは、ネットワーク内で WAP デバイスを識別する情報を設定できます。

システム設定の指定

システム設定を指定するには、次の手順を実行してください。

ステップ 1 [管理] > [システム設定] の順に選択します。

ステップ 2 パラメータを入力します。

- [ホスト名]: WAP デバイスに管理用に割り当てられた名前です。この名前はノードの完全修飾ドメイン名にするよう規定されています。デフォルト ホスト名は **wap** と、WAP デバイスの MAC アドレスの 16 進値末尾 6 桁を結合した文字列です。ホスト名ラベルに含めることができるのは、文字、数字、およびハイフンのみです。ホスト名ラベルの開始または終了はハイフンにできません。また、その他の記号、句読文字、スペースは使用できません。許可されるホスト名の長さは 1 ～ 63 文字です。
- [システム連絡先]: WAP デバイスに関する連絡担当者です。[システム連絡先] は 0 ～ 255 文字の長さで、スペースおよび特殊文字を含めることができます。
- [システム ロケーション]: WAP デバイスの物理的な場所の説明です。[システム ロケーション] は 0 ～ 255 文字の長さで、スペースおよび特殊文字を含めることができます。

ステップ 3 [保存] をクリックします。変更がスタートアップ コンフィギュレーションに保存されます。

ユーザ アカウント

デフォルトでは、1 人の管理ユーザが WAP デバイスに設定されています。

- ユーザ名 : **cisco**
- パスワード : **cisco**

[ユーザ アカウント] ページは、追加の最大 4 ユーザの設定とユーザ パスワードの変更に使用できます。

ユーザの追加

ユーザを新規に追加するには、次の手順を実行してください。

ステップ 1 ナビゲーション ウィンドウで [管理] > [ユーザ アカウント] の順に選択します。

[ユーザ アカウント] テーブルに現在設定されているユーザが表示されます。ユーザ **cisco** は読み取り/書き込み権限を持つようにシステムに事前設定されています。

その他のすべてのユーザは読み取り専用アクセス権を持つことはできますが、読み取り/書き込みアクセス権を持つことはできません。

ステップ 2 [追加] をクリックします。テキスト ボックスの新しい行が表示されます。

ステップ 3 新しいユーザのボックスをチェックし、[編集] を選択します。

ステップ 4 英数字 1 ～ 32 文字の [ユーザ名] を入力します。ユーザ名で使用できるのは 0 ～ 9 の数字と a ～ z の文字(大文字および小文字)のみです。

ステップ 5 1 ～ 64 文字の [新しいパスワード] を入力してから、同じパスワードを [新しいパスワードの確認] テキスト ボックスに入力します。

パスワードを入力していくと、垂直バーの数と色が次のように変化してパスワードの強度が示されます。

- **赤**:パスワードは複雑さの最小要件を満たしていません。
- **オレンジ**:パスワードは複雑さの最小要件を満たしていますが、パスワードの強度は脆弱です。
- **グリーン**:パスワードは堅牢です。

ステップ 6 [保存] をクリックします。変更がスタートアップ コンフィギュレーションに保存されます。

注 ユーザを削除するには、ユーザ名の横のチェック ボックスをオンにし、[削除] をクリックします。恒久的に削除するには、完了時に [保存] を選択します。

ユーザ パスワードの変更

ユーザ パスワードを変更するには、次の手順を実行してください。

ステップ 1 ナビゲーション ウィンドウで [管理] > [ユーザ アカウント] の順に選択します。

[ユーザ アカウント] テーブルに現在設定されているユーザが表示されます。ユーザ **cisco** は読み取り/書き込み権限を持つようにシステムに事前設定されています。ユーザ **cisco** のパスワードは変更できます。

ステップ 2 設定するユーザを選択し、[編集] をクリックします。

ステップ 3 1 ～ 64 文字の [新しいパスワード] を入力してから、同じパスワードを [新しいパスワードの確認] テキスト ボックスに入力します。

パスワードを入力していくと、垂直バーの数と色が次のように変化してパスワードの強度が示されます。

- **赤**:パスワードは複雑さの最小要件を満たしていません。
- **オレンジ**:パスワードは複雑さの最小要件を満たしていますが、パスワードの強度は脆弱です。
- **グリーン**:パスワードは堅牢です。

ステップ 4 [保存] をクリックします。変更がスタートアップ コンフィギュレーションに保存されます。

注 パスワードを変更する場合は、システムにログインし直す必要があります。

時間設定

システム クロックは、メッセージ ログなどのソフトウェア イベント用にネットワークと同期したタイムスタンプを付けるサービスを提供します。システム クロックを手動で設定することもできれば、サーバからクロック データを取得する Network Time Protocol（NTP）クライアントとして WAP デバイスを設定することもできます。

[時間設定] ページは、システム時刻を手動で設定するか、事前設定された NTP サーバから時間設定を取得するようにシステムを設定するために使用します。デフォルトでは、AP は、事前設定された NTP サーバのリストから時刻を取得するように設定されます。

現在のシステム時刻が [システム クロック ソース] オプションと合わせてページの先頭に表示されます。

WAP デバイスで時間設定を自動取得するように NTP を使用するには、次の手順を実行してください。

NTP を通じた時間設定の自動取得

NTP を通じて時間設定を自動取得するには、次の手順を実行してください。

ステップ 1 [システム クロック ソース] フィールドで [Network Time Protocol（NTP）] を選択します。

ステップ 2 次のパラメータを設定します。

- [NTP サーバ/IPv4/IPv6 アドレス名]：NTP サーバの IPv4 アドレス、IPv6 アドレス、またはホスト名を指定します。デフォルトの NTP サーバがリストされます。

  ホスト名は 1 個以上のラベルで構成できます。ラベルは最大 63 文字の英数字のセットです。ホスト名に複数のラベルが含まれている場合、それぞれはピリオド（.）で区切られます。一連のラベルとピリオドを合わせた許可される長さは最大 253 文字です。

- [タイムゾーン]：場所に応じたタイムゾーンを選択します。

ステップ 3 夏時間が適用されるタイムゾーンの場合は、[夏時間用に時刻を調整] を選択します。選択した場合は、次のフィールドを設定します。

- [夏時間の開始]：夏時間を開始する月、日、週、時間を選択します。
- [夏時間の終了]：夏時間を終了する月、日、週、時間を選択します。
- [夏時間オフセット]：夏時間の開始時にクロックを進め、終了時に戻す分数を指定します。

ステップ 4 [保存] をクリックします。変更がスタートアップ コンフィギュレーションに保存されます。

時間設定の手動指定

時間設定を手動で指定するには、次の手順を実行してください。

ステップ 1 [システム クロック ソース] フィールドで [手動] を選択します。

ステップ 2 次のパラメータを設定します。

- [システム日付]：ドロップダウンリストから現在の月、日、および 1 年の何日目かを選択します。
- [システム時刻]：24 時間表記で現在の時間と分を選択します。午後 10 時なら 22:00:00 です。

注 コンピュータの日時を使用する場合は、現在のコンピュータから時刻を設定するための矢印が [システム時刻] の横にあります。

- [タイムゾーン]: 場所に応じたタイムゾーンを選択します。

ステップ 3 夏時間が適用されるタイムゾーンの場合は、[夏時間用に時刻を調整] を選択します。選択した場合は、次のフィールドを設定します。

- [夏時間の開始]: 夏時間を開始する月、日、週、時間を選択します。
- [夏時間の終了]: 夏時間を終了する月、日、週、時間を選択します。
- [夏時間オフセット]: 夏時間の開始時にクロックを進め、終了時に戻す分数を指定します。

ステップ 4 [保存] をクリックします。変更がスタートアップ コンフィギュレーションに保存されます。

ログ設定

[ログ設定] ページを使用すると、永続的メモリへのログ メッセージの保存を有効化できます。リモート ホストにログを送信することもできます。

永続的ログの設定

システムが予期せずリブートする場合、ログ メッセージは原因の診断に役立つことがあります。ただし、永続的ロギングを有効にしていない場合は、システムがリブートするとログ メッセージは消去されます。

注意 永続的ロギングを有効にすると、フラッシュ（不揮発性）メモリが減り、ネットワーク パフォーマンスが低下することがあります。永続的ロギングを有効にするのは問題をデバッグするときだけにしてください。問題のデバッグの完了後は、永続的ロギングを必ず無効にしてください。

永続的ロギングの設定

永続的ロギングを設定するには、次の手順を実行してください。

ステップ 1 ナビゲーション ウィンドウで [管理] > [ログ設定] の順に選択します。

ステップ 2 次のパラメータを設定します。

- [永続化]:不揮発性メモリにシステム ログを保存して WAP デバイスのリブート時にログが維持されるようにするには、[有効化] をクリックします。不揮発性メモリに保存できるログ メッセージは最大 128 個です。128 個の制限に到達すると、最も古いログ メッセージが最新のメッセージによって上書きされます。揮発性メモリにシステム ログを保存するにはこのフィールドをクリアします。揮発性メモリに格納されたログはシステムがリブートすると削除されます。
- [重大度]:不揮発性メモリのログに書き込むために必要とされるイベントの最小重大度です。たとえば、2(重大)を指定した場合は、重大、アラート、およびエマージェンシーのイベントが不揮発性メモリに記録されます。重大度 3 ～ 7 のエラー メッセージは揮発性メモリに書き込まれます。
- [深度]:揮発性メモリに保管できるメッセージの最大数で、最大 512 個です。このフィールドに設定した数に到達すると、最も古いログ イベントが最新のログ イベントによって上書きされます。不揮発性メモリ(永続的ログ)に保管できるログ メッセージの最大数は 128 個であり、変更できないことに注意してください。

ステップ 3 [保存] をクリックします。変更がスタートアップ コンフィギュレーションに保存されます。

リモート ログ サーバ

[カーネル ログ] はシステム イベント([システム ログ] に表示)と、エラー状況などのカーネル メッセージを含む包括的なリストです。

カーネル ログ メッセージは、Web インターフェイスから直接表示できません。まず、ログを受信およびキャプチャするようにリモート ログ サーバを設定する必要があります。その後、リモート ログ サーバにログを記録するように WAP デバイスを設定できます。WAP デバイスでは最大 2 つのリモート ログ サーバをサポートします。

WAP デバイス syslog メッセージ用のリモート ログ サーバ収集は次の機能を提供します。

- 複数 AP からの syslog メッセージを集約可能
- 単独の WAP デバイスに保持するよりも長くメッセージの履歴を保管
- スクリプトによって管理操作およびアラートをトリガー

リモート ログ サーバとしてのホストの指定

ネットワーク上のホストをリモート ログ サーバとして動作するように指定するには、次の手順を実行してください。

ステップ 1 ナビゲーション ウィンドウで [管理] > [ログ設定] の順に選択します。

ステップ 2 [リモート ログ サーバ テーブル] で、次のパラメータを設定します。

- [リモート ログ サーバ]: リモート ログ サーバの IPv4/IPv6 アドレスまたはホスト名を入力します。

  ホスト名は、最大 63 文字の英数字のセットからなる 1 つ以上のラベルで構成できます。ホスト名に複数のラベルが含まれる場合、それぞれをピリオド(.)で区切ります。一連のラベルおよびピリオドの長さは、最大 253 文字にすることができます。

- [有効化]: オンにすると、このリモート ログ サーバが有効になります。その場合、ログの重大度および UDP ポートを定義します。

  [ログの重大度]: リモート ログ サーバに送信するために必要とされるイベントの重大度をオンにします。

- [UDP ポート]: リモート ホスト上の syslog プロセスの論理ポート番号です。範囲は 1 ～ 65535 です。デフォルト ポートは 514 です。

  デフォルト ポートの使用をお勧めします。ログ ポートをあえて設定し直す場合は、syslog に割り当てるポート番号が使用可能であることを確認してください。

ステップ 3 [保存] をクリックします。変更がスタートアップ コンフィギュレーションに保存されます。

[リモート ログ] ホストを有効にした場合は、[保存] をクリックするとリモート ロギングがアクティブになります。WAP デバイスでは、構成に応じて、リモート ログ サーバ モニタ、指定されたカーネル ログ ファイル、またはその他のストレージに表示するために、リアルタイムでカーネル メッセージを送信します。

[リモート ログ] ホストを無効にした場合は、[保存] をクリックするとリモート ロギングが無効になります。

注 新しい設定の保存後に、対応するプロセスが停止されて再開されることがあります。これが発生すると、WAP デバイスは接続性を失うことがあります。接続性を失ったときにワイヤレス クライアントへの影響が最小限になるように、WAP デバイスの設定を変更することをお勧めします。

電子メール アラート

電子メール アラート機能は、特定のシステム イベントが発生したときに、設定した電子メール アドレスにメッセージを送信するために使用します。

この機能では、メール サーバ構成、メッセージ重大度の構成、および最大 3 個の電子メール アドレスの構成を行って、エマージェンシーおよびエマージェンシーでない電子メール アラートを送信できます。

ヒント　個人所有の電子メール アドレスは使用しないでください。個人電子メールのログイン クレデンシャルを不要に公開することになりかねません。代わりに個別の電子メール アカウントを使用してください。多くの電子メール アカウントでは、送信されたすべてのメッセージのコピーを保持する動作がデフォルトであることにも留意してください。この電子メール アカウントにアクセスできる全員が、送信されたメッセージにアクセスできます。電子メール設定を調べて、会社のプライバシー ポリシーに準じていることを確認してください。

電子メール アラートを送信するための AP の設定

電子メール アラートを送信するように AP を設定するには、次の手順を実行してください。

ステップ 1　ナビゲーション ウィンドウで [管理] > [電子メール アラート] の順に選択します。

ステップ 2　[グローバル構成] 領域で、次のパラメータを設定します。

- [管理モード]: 電子メール アラート機能をグローバルに有効化する場合に選択します。
- [差出人電子メール アドレス]: 電子メールの送信者として表示するアドレスを入力します。このアドレスは、印字可能な文字のみによる 255 文字の文字列です。デフォルトではアドレスは設定されません。
- [ログ期間]: スケジュールされたメッセージの送信頻度を選択します。範囲は 30 ～ 1440 分です。デフォルトは 30 分です。
- [スケジュール済みメッセージの重大度]: この重大度以上のログ メッセージは、まとめられて、[ログ期間] で指定された頻度でコンフィギュレーション電子メール アドレスに送信されます。次の値から選択してください。[なし]、[エマージェンシー]、[アラート]、[重大]、[エラー]、[警告]、[通知]、[情報]、および [デバッグ]。[なし] に設定した場合は、スケジュールされた重大度メッセージは送信されません。デフォルトの重大度は [警告] です。
- [エマージェンシーメッセージ重大度]: この重大度以上のログ メッセージは、設定されている電子メール アドレスにただちに送信されます。次の値から選択してください。[なし]、[エマージェンシー]、[アラート]、[重大]、[エラー]、[警告]、[通知]、[情報]、および [デバッグ]。[なし] に設定した場合は、エマージェンシー重大度メッセージは送信されません。デフォルトは [アラート] です。

ステップ 3　[メール サーバ構成] 領域で、次のパラメータを設定します。

- [サーバの IPv4 アドレス/名前]：送信 SMTP サーバの IP アドレスまたはホスト名を入力します。（ホスト名は電子メール プロバイダーに問い合わせてください）。このサーバ アドレスは、有効な IPv4 アドレスまたはホスト名でなければなりません。IPv4 アドレスは xxx.xxx.xxx.xxx（192.0.2.10）のような形式である必要があります。

  ホスト名は 1 個以上のラベルで構成できます。ラベルは最大 63 文字の英数字のセットです。ホスト名に複数のラベルが含まれている場合、それぞれはピリオド（.）で区切られます。一連のラベルとピリオドを合わせた許可される長さは最大 253 文字です。

- [データ暗号化]：送信電子メール アラートのセキュリティのモードを入力します。このアラートは、セキュアな TLS プロトコルで送信することも、デフォルトのオープン プロトコルで送信することもできます。セキュアな TLSv1 プロトコルを使用すると、パブリック ネットワークをまたがった通信中の傍受および改ざんを防止できます。

- [ポート]：送信電子メールに使用する SMTP ポート番号を入力します。範囲は 0 ～ 65535 の有効なポート番号です。デフォルト ポートは 465 です。このポートは、通常、電子メール プロバイダーの使用するモードによって決まります。

- [ユーザ名]：これらのメールの送信に使用する電子メール アカウントのユーザ名を入力します。通常（常にではない）、このユーザ名はドメインを含む完全な電子メール アドレス（例：Name@example.com）です。指定したアカウントは送信者の電子メール アドレスとして使用されます。ユーザ名には 1 ～ 64 文字の英数字を使用できます。

- [パスワード]：これらのメールの送信に使用する電子メール アカウントのパスワードを入力します。パスワードには 1 ～ 64 個の文字を使用できます。

ステップ 4 電子メール アドレスおよび件名行を設定します。

- [宛先電子メール アドレス 1/2/3]：電子メール アラートを受信するアドレスを最大 3 個入力します。各電子メール アドレスは有効である必要があります。

- [電子メールの件名]：電子メールの件名行に表示されるテキストを入力します。最大 255 文字の英数字文字列を使用できます。

ステップ 5 [テスト メール] をクリックしてテスト電子メールを送信し、設定した電子メール アカウントを検証します。

ステップ 6 [保存] をクリックします。変更がスタートアップ コンフィギュレーションに保存されます。

電子メール アラートの例

次の例は、[メール サーバ構成] のパラメータを入力する方法を示しています。

```
Gmail
[サーバの IPv4 アドレス/名前] = smtp.gmail.com
[データ暗号化] = TLSv1
[ポート] = 465
[ユーザ名] = 上記のサーバに関連付けられている電子メール アカウントにログインするために使用できる完全な電子メール アドレス
[パスワード] = xxxxxxxx は有効な電子メール アカウントの有効なパスワード
[宛先電子メール アドレス 1] = myemail@gmail.com

Windows Live Hotmail
Windows Live Hotmail では次の設定を推奨しています。
[データ暗号化]:TLSv1
[SMTP サーバ]:smtp.live.com
[SMTP ポート]:587
ユーザ名:myName@hotmail.com、myName@myDomain.com などの完全な電子メール アドレス
パスワード:ご使用の Windows Live アカウントのパスワード

Yahoo!Mail
Yahoo では、この種のサービスでは有料アカウントが必要です。Yahoo では、次の設定を推奨しています。
[データ暗号化]:TLSv1
[SMTP サーバ]:plus.smtp.mail.yahoo.com
[SMTP ポート]:465 または 587
ユーザ名:myName(@yahoo.com は省く)など、ドメイン名を含まない電子メール アドレス
パスワード:ご使用の Yahoo アカウントのパスワード
```

次の例は、一般的なログ電子メールのフォーマット例を示しています。

```
From:AP-192.168.2.10@mailserver.com
Sent:Wednesday, September 09, 2009 11:16 AM
To: administrator@mailserver.com
Subject: log message from AP

TIME           Priority Process Id  Message
Sep 8 03:48:25 info login[1457]  root login on ttyp0
Sep 8 03:48:26 info mini_http-ssl[1175]  Max concurrent connections of 20
reached
```

LED ディスプレイ

WAP デバイスには LED が 1 個搭載されています。[LED ディスプレイ] ページは、LED を有効または無効にするためと、設定されているスケジューラ プロファイルと LED を関連付けるために使用します。

[LED ディスプレイ] はデフォルトで [有効] です。[LED ディスプレイ] が [無効化] の場合、LED はオフです。[LED ディスプレイ] 値が [スケジューラの関連付け] の場合は、スケジューラ プロファイルを選択するドロップダウン ボックスが表示されます。有効にした場合、LED は WAP デバイスの対応するステータスおよびアクティビティを示します。

LED ディスプレイの変更

LED ディスプレイを変更するには、次の手順を実行してください。

ステップ 1 ナビゲーション ウィンドウで [管理] > [LED ディスプレイ] の順に選択します。

ステップ 2 ドロップダウン選択から [有効化/無効化/スケジューラの関連付け] を選択します。

ステップ 3 [スケジューラの関連付け LED ディスプレイ] のドロップダウン選択リストから [プロファイル名] を選択します。デフォルトでは LED に関連付けられているプロファイルはありません。このドロップダウン選択には、[ワイヤレス] > [スケジューラ] ページと同様に、設定されている [スケジューラ プロファイル名] が表示されます。

LED がスケジューラ プロファイルと関連付けられている場合、このカラムには、該当時刻にアクティブ プロファイル ルールが存在しているのかどうかに応じたステータスが表示されます。

ステップ 4 [保存] をクリックします。変更がスタートアップ コンフィギュレーションに保存されます。

HTTP/HTTPS サービス

[HTTP/HTTPS サービス] ページは、Web ベースの管理接続を有効にするためと設定するために使用します。HTTPS を使用して管理セッションを保護する場合は、[HTTP/HTTPS サービス] ページも使用して必要な SSL 証明書を管理します。

HTTP サービスおよび HTTPS サービスの設定

HTTP サービスおよび HTTPS サービスを設定するには、次の手順を実行してください。

ステップ 1 ナビゲーション ウィンドウで [管理] > [HTTP/HTTPS サービス] の順に選択します。

ステップ 2 次のグローバル設定値を設定します。

- [最大セッション数]:HTTP と HTTPS の両方を含む、同時に使用できる Web セッションの数です。

ユーザが WAP デバイス コンフィギュレーション ユーティリティにログオンすると、セッションが作成されます。このセッションは、ユーザがログオフするか、[セッション タイムアウト] が満了するまで維持されます。範囲は 1 ～ 10 セッションです。デフォルトは 5 です。最大セッション数に到達すると、コンフィギュレーション ユーティリティへのログオンを次に試行したユーザには、セッション制限に関するエラー メッセージが表示されます。

- [セッション タイムアウト]:非アクティブなユーザが WAP デバイス構成ユーティリティに引き続きログオンしている最大時間(分単位)です。設定されているタイムアウトに到達すると、ユーザは自動でログオフされます。範囲は 1 ～ 60 分です。デフォルトは 10 分です。

ステップ 3　HTTP サービスおよび HTTPS サービスを設定します。

- [HTTP サーバ]:HTTP を通じてアクセスできるようにします。デフォルトでは、HTTP アクセスは有効です。無効にすると、このプロトコルを使用している現在の接続はすべて切断されます。
- [HTTP ポート]:HTTP 接続に使用する 1025 ～ 65535 の論理ポート番号です。HTTP 接続のデフォルト ポート番号は IANA のウェルノウン ポート番号の 80 です。
- [HTTPS サーバ]:セキュア HTTP を通じてアクセスできるようにします。デフォルトでは、HTTPS アクセスは有効です。無効にすると、このプロトコルを使用している現在の接続はすべて切断されます。
- [HTTPS ポート]:HTTPS 接続に使用する 1025 ～ 65535 の論理ポート番号です。HTTP 接続のデフォルト ポート番号は IANA のウェルノウン ポート番号の 443 です。
- [HTTP から HTTPS へリダイレクト]:HTTP ポートでの管理 HTTP アクセス試行を HTTPS ポートにリダイレクトします。このフィールドは HTTP アクセスが無効化されている場合のみ使用可能です。

ステップ 4　[保存] をクリックします。変更がスタートアップ コンフィギュレーションに保存されます。

SSL 証明書の管理

HTTPS サービスを使用するには、WAP デバイスは有効な SSL 証明書を保持している必要があります。WAP デバイスで証明書を生成することもできれば、ネットワークまたは TFTP サーバから証明書をダウンロードすることもできます。

WAP デバイスの証明書を生成するには、[SSL 証明書の生成] をクリックします。この操作は、AP が IP アドレスを取得してから実行して、証明書のコモン ネームと AP の IP アドレスが一致することを確認する必要があります。新しい SSL 証明書を生成すると、セキュア Web サーバが再起動します。セキュア接続は、新しい証明書がブラウザで受け入れられるまで機能しません。

[証明書ファイルのステータス] 領域で、WAP デバイスに現在証明書が存在しているかどうかと、証明書に関する次の情報を表示できます。

- 証明書ファイルあり
- 証明書の失効日
- 証明書発行者の共通名

SSL 証明書（拡張子 .pem）が WAP デバイスに存在している場合は、コンピュータにダウンロードしてバックアップにすることができます。[SSL 証明書のダウンロード（デバイスから PC）] 領域の [ダウンロード方法] で [HTTP] または [TFTP] を選択し、[ダウンロード] をクリックします。

- [HTTP] を選択した場合は、ダウンロードを確認してから、参照してネットワーク上のファイルを保存する場所を指定するようプロンプトが表示されます。
- [TFTP] を選択した場合は、ダウンロードしたファイルに割り当てる [ファイル名] とファイルをダウンロードする TFTP サーバのアドレスを入力するための追加のフィールドが表示されます。

ご使用のコンピュータから WAP デバイスに証明書ファイル（拡張子 .pem）をアップロードすることもできます。[SSL 証明書のアップロード（PC からデバイス）] 領域の [アップロード方法] で [HTTP] または [TFTP] を選択します。

- HTTP の場合は、ネットワークの場所を参照し、ファイルを選択して [アップロード] をクリックします。
- TFTP の場合は TFTP サーバ上の [ファイル名] および [TFTP サーバの IPv4 アドレス] を入力してから [アップロード] をクリックします。ファイル名には次の文字を含めることはできません。スペース、<、>、|、\、:、(、)、&、;、#、?、*、連続する 2 個以上のピリオド。

アップロードが成功すると確認メッセージが表示されます。

管理アクセス制御

WAP デバイス コンフィギュレーション ユーティリティへのアクセスを許可されている最大 5 台の IPv4 ホストと 5 台の IPv6 ホストをリストするアクセス コントロール リスト（ACL）を作成できます。この機能が無効化されている場合は、正しい WAP デバイス ユーザ名およびパスワードを入力することにより、誰もが任意のネットワーク クライアントからコンフィギュレーション ユーティリティにアクセスできます。

管理 ACL が有効化されている場合は、Web および SNMP を通じたアクセスは指定された IP ホストに制限されます。

注意 入力するすべての IP アドレスを検証します。管理コンピュータと一致しない IP アドレスを入力した場合は、コンフィギュレーション インターフェイスへのアクセスを失うことになります。管理コンピュータには静的 IP アドレスを割り当てて、アドレスが自動で変更されないようにすることを強くお勧めします。

アクセス リストの作成

アクセス リストを作成するには、次の手順を実行してください。

ステップ 1 ナビゲーション ウィンドウで [管理] > [管理アクセス制御] の順に選択します。

ステップ 2 [管理 ACL モード] で [有効化] を選択します。

ステップ 3 アクセスを許可する最大 5 個の IPv4 アドレスおよび 5 個の IPv6 アドレスを入力します。

ステップ 4 IP アドレスが正しいことを確認します。

ステップ 5 [保存] をクリックします。変更がスタートアップ コンフィギュレーションに保存されます。

ファームウェアの管理

WAP デバイスは 2 個のファームウェア イメージを維持しています。イメージの 1 つはアクティブでもう 1 つは非アクティブです。ブートアップ時にアクティブ イメージをロードできなかった場合は、非アクティブ イメージがロードされてアクティブ イメージになります。アクティブ イメージと非アクティブ イメージを切り替えることもできます。

新しいバージョンの AP ファームウェアが提供された場合は、デバイス上のファームウェアをアップグレードして新機能および拡張機能を利用できます。AP では、ファームウェア アップグレードに TFTP または HTTP クライアントを使用します。

新しいファームウェアをアップロードし、システムがリブートすると、新しく追加したファームウェアがプライマリ イメージになります。アップグレードが失敗した場合は、元のファームウェアが引き続きプライマリ イメージです。

注 ファームウェアをアップグレードする場合、アクセス ポイントでは既存のコンフィギュレーション情報を維持します。

ファームウェア イメージの切り替え

AP で実行されているファームウェア イメージを切り替えるには、次の手順を実行してください。

ステップ 1 ナビゲーション ウィンドウで [管理] > [ファームウェアの管理] の順に選択します。

ステップ 2 [アクティブ イメージのスワップ] をクリックします。

ファームウェア イメージの切り替えと、これに続くリブートを確認するダイアログボックスが表示されます。

ステップ 3 [OK] をクリックして続行します。

この処理は数分かかることがあり、この間アクセス ポイントは使用不能です。イメージの切り替えの進行中はアクセス ポイントの電源を切らないでください。イメージの切り替えが完了すると、アクセス ポイントが再起動します。AP はアップグレード前と同じ構成時の設定を使用して通常の動作を再開します。

TFTP アップグレード

TFTP を使用してアクセス ポイントのファームウェアをアップグレードするには、次の手順を実行してください。

ステップ 1 ナビゲーション ウィンドウで [管理] > [ファームウェアの管理] の順に選択します。

製品 ID（PID VID）およびアクティブと非アクティブのファームウェアのバージョンが表示されます。

ステップ 2 [TFTP で転送] を選択します。

ステップ 3 [送信元ファイル名] フィールドに、イメージ ファイルの名前（1 ～ 128 文字）を入力します。これには、アップロードするイメージを格納しているディレクトリのパスを含みます。

たとえば、/share/builds/ap ディレクトリにある ap_upgrade.tar イメージをアップロードするには、次のように入力します。*/share/builds/ap/ap_upgrade.tar*

使用するファームウェア アップグレード ファイルは tar ファイルである必要があります。bin ファイルまたはその他の形式のファイルをアップグレードに使用しないでください。これらのタイプのファイルは機能しません。

ファイル名には次の項目を含めることはできません。スペース、<、>、|、\、:、(、)、&、;、#、?、*、連続する 2 個以上のピリオド。

ステップ 4 [TFTP サーバの IPv4 アドレス] を入力し、[アップグレード] をクリックします。

新しいソフトウェアのアップロードには数分かかる場合があります。新しいソフトウェアのアップロード中は、ページを更新したり、別のページに移動したりしないでください。ソフトウェアのアップロードが中止されます。プロセスが完了すると、アクセス ポイントが再起動して通常の動作を再開します。

ステップ 5 ファームウェア アップグレードが正常に完了したことを確認するには、ユーザ インターフェイスにログインし、[ファームウェアのアップグレード] ページを表示してアクティブ ファームウェアのバージョンを参照します。

HTTP アップグレード

HTTP を使用してアップグレードするには、次の手順を実行してください。

ステップ 1 [HTTP で転送] を選択します。

ステップ 2 新しいファイルの名前とパスが分かっている場合は、[送信元ファイル名] フィールドに入力します。不明の場合は、[参照] ボタンをクリックして、ネットワーク上のファームウェア イメージ ファイルを選択します。

使用するファームウェア アップグレード ファイルは tar ファイルである必要があります。bin ファイルまたはその他の形式のファイルをアップグレードに使用しないでください。これらのタイプのファイルは機能しません。

ステップ 3 [アップグレード] をクリックして新しいファームウェア イメージを適用します。

新しいソフトウェアのアップロードには数分かかる場合があります。新しいソフトウェアのアップロード中は、ページを更新したり、別のページに移動したりしないでください。ソフトウェアのアップロードが中止されます。プロセスが完了すると、アクセス ポイントが再起動して通常の動作を再開します。

ステップ 4 ファームウェア アップグレードが正常に完了したことを確認するには、ユーザ インターフェイスにログインし、[ファームウェアのアップグレード] ページを表示してアクティブ ファームウェアのバージョンを参照します。

構成ファイルのダウンロード/バックアップ

AP コンフィギュレーション ファイルは XML 形式であり、WAP デバイスに関するすべての情報を格納しています。コンフィギュレーション ファイルはネットワーク ホストまたは TFTP サーバにバックアップ(アップロード)して、内容を手動で編集したり、バックアップを作成したりできます。バックアップしたコンフィギュレーション ファイルは、編集後にアクセス ポイントにダウンロードして、コンフィギュレーションを変更できます。

AP は、次のコンフィギュレーション ファイルを維持しています。

- **スタートアップ コンフィギュレーション**:フラッシュ メモリに保存されたコンフィギュレーション ファイルです。
- **バックアップ コンフィギュレーション**:バックアップとして使用するために WAP デバイスに保存された追加のコンフィギュレーション ファイルです。
- **ミラー コンフィギュレーション**:スタートアップ コンフィギュレーションが 24 時間以上変更されていない場合は、ミラー コンフィギュレーション ファイルに自動で保存されます。ミラー コンフィギュレーション ファイルは、過去のスタートアップ コンフィギュレーションのスナップショットです。ミラー コンフィギュレーションは出荷時設定へのリセットをまたがって保存されます。このため、ミラー コンフィギュレーションをスタートアップ コンフィギュレーションにコピーすることで、出荷時設定へのリセット後にシステム コンフィギュレーションを回復するために使用できます。

注 これらのファイルは別のシステムとのダウンロードおよびアップロードに加え、WAP デバイス上の異なるファイル タイプにコピーすることもできます。「構成のコピー/保存」を参照してください。

コンフィギュレーション ファイルのバックアップ

コンフィギュレーション ファイルをネットワーク ホストまたは TFTP サーバにバックアップ(アップロード)するには、次の手順を実行してください。

ステップ 1 ナビゲーション ウィンドウで [管理] > [構成ファイルのダウンロード/バックアップ] の順に選択します。

ステップ 2 [転送方法] として [TFTP 経由] または [HTTP/HTTPS 経由] を選択します。

ステップ 3 [アクションを保存] として [バックアップ(AP から PC)] を選択します。

ステップ 4 TFTP バックアップの場合に限り、拡張子 xml を付けて [宛先ファイル名] を入力します。サーバ上のファイルを配置するパスも含めてから、[TFTP サーバの IPv4 アドレス] を入力します。

ファイル名には次の文字を含めることはできません。スペース、<、>、|、\、:、(、)、&、;、#、?、*、連続する 2 個以上のピリオド。

ステップ 5 TFTP バックアップの場合に限り、[TFTP サーバの IPv4 アドレス] を入力します。

ステップ 6 バックアップするコンフィギュレーション ファイルを選択します。

- **スタートアップ コンフィギュレーション**：WAP デバイスの最後の起動で使用されたコンフィギュレーション ファイル タイプです。これには、適用されただけで WAP デバイスにはまだ保存されていないコンフィギュレーション変更は含まれていません。
- **バックアップ コンフィギュレーション**：WAP デバイスに保存されたバックアップ コンフィギュレーション ファイル タイプです。
- **ミラー コンフィギュレーション**：スタートアップ コンフィギュレーションが 24 時間以上変更されていない場合は、ミラー コンフィギュレーション ファイルに自動で保存されます。ミラー コンフィギュレーション ファイルは、過去のスタートアップ コンフィギュレーションのスナップショットです。ミラー コンフィギュレーションは出荷時設定へのリセットをまたがって保存されます。このため、ミラー コンフィギュレーションをスタートアップ コンフィギュレーションにコピーすることで、出荷時設定へのリセット後にシステム コンフィギュレーションを回復するために使用できます。

ステップ 7 [保存] をクリックしてバックアップを開始します。HTTP バックアップの場合は、ウィンドウが表示されて、ファイルを保存する目的の場所を参照して指定できます。

ファイルを AP にダウンロードすることにより、コンフィギュレーションを更新したり、以前バックアップしたコンフィギュレーションに AP を戻したりできます。

コンフィギュレーション ファイルのダウンロード

コンフィギュレーション ファイルを WAP デバイスにダウンロードするには、次の手順を実行してください。

ステップ 1 ナビゲーション ウィンドウで [管理] > [構成ファイルのダウンロード/バックアップ] の順に選択します。

ステップ 2 [転送方法] として [TFTP 経由] または [HTTP/HTTPS 経由] を選択します。

ステップ 3 [アクションを保存] として [ダウンロード(PC から AP)] を選択します。

ステップ 4 TFTP ダウンロードの場合に限り、拡張子 xml を付けて [送信元ファイル名] を入力します。サーバ上でファイルが存在しているパスも含めてから、[TFTP サーバの IPv4 アドレス] を入力します。

ファイル名には次の文字を含めることはできません。スペース、<、>、|、\、:、(、)、&、;、#、?、*、連続する 2 個以上のピリオド。

ステップ 5 ダウンロードしたファイルで置き換える AP 上のコンフィギュレーション ファイル([スタートアップ コンフィギュレーション] または [バックアップ コンフィギュレーション]) を選択します。

ダウンロードしたファイルによってスタートアップ コンフィギュレーション ファイルが上書きされ、このファイルが妥当性検査に合格すると、ダウンロードしたコンフィギュレーションは AP を次回リブートしたときに有効になります。

ステップ 6 [保存] をクリックしてアップグレードまたはバックアップを開始します。HTTP ダウンロードの場合は、ウィンドウが表示されて、ダウンロードするファイルを参照して選択できます。ダウンロードが完了すると、成功したことがウィンドウで示されます。

注意 コンフィギュレーション ファイルのダウンロード中は、AP への電力が遮断されていないことを確認してください。コンフィギュレーション ファイルのダウンロード中に電源異常が発生すると、ファイルは失われるため処理を再開する必要があります。

構成ファイルのプロパティ

[構成ファイルのプロパティ] ページでは、スタートアップまたはバックアップ コンフィギュレーション ファイルをクリアできます。スタートアップ コンフィギュレーション ファイルをクリアすると、AP を次回リブートしたときにバックアップ コンフィギュレーション ファイルがアクティブになります。

AP は、起動すると、スタートアップ コンフィギュレーションの適用を試行します。スタートアップ コンフィギュレーションに何らかの問題がある場合、AP はミラー コンフィギュレーションの適用を試行します。何らかの理由でミラー コンフィギュレーションを適用できない場合、AP はバックアップ コンフィギュレーションの適用を試行します。

スタートアップ コンフィギュレーション ファイルまたはバックアップ コンフィギュレーション ファイルの削除

スタートアップ コンフィギュレーション ファイルまたはバックアップ コンフィギュレーション ファイルを削除するには、次の手順を実行してください。

ステップ 1　ナビゲーション ウィンドウで [管理] > [構成ファイルのプロパティ] の順に選択します。

ステップ 2　[スタートアップ コンフィギュレーション] または [バックアップ コンフィギュレーション] ファイル タイプを選択します。

ステップ 3　[ファイルのクリア] をクリックします。

構成のコピー/保存

[構成のコピー/保存] ページでは、AP ファイル システム内でファイルをコピーできます。たとえば、バックアップ コンフィギュレーション ファイルをスタートアップ コンフィギュレーション ファイル タイプにコピーして、WAP デバイスの次回起動時に使用されるようにすることができます。

別のファイル タイプへのファイルのコピー

別のファイル タイプにファイルをコピーするには、次の手順を実行してください。

ステップ 1　ナビゲーション ウィンドウで [管理] > [構成のコピー/保存] の順に選択します。

ステップ 2　[送信元ファイル名] を選択します。

- **スタートアップ コンフィギュレーション**：WAP デバイスの最後の起動で使用されたコンフィギュレーション ファイル タイプです。これには、適用されただけで WAP デバイスにはまだ保存されていないコンフィギュレーション変更は含まれていません。
- **バックアップ コンフィギュレーション**：WAP デバイスに保存されたバックアップ コンフィギュレーション ファイル タイプです。
- **ミラー コンフィギュレーション**：スタートアップ コンフィギュレーションが 24 時間以上変更されていない場合は、ミラー コンフィギュレーション ファイルに自動で保存されます。ミラー コンフィギュレーション ファイルは、過去のスタートアップ コンフィギュレーションのスナップショットです。ミラー コンフィギュレーションは出荷時設定へのリセットをまたがって保存されます。このため、ミラー コンフィギュレーションをスタートアップ コンフィギュレーションにコピーすることで、出荷時設定へのリセット後にシステム コンフィギュレーションを回復するために使用できます。

ステップ 3　[宛先ファイル名] で、コピーするファイルで置き換えるファイル タイプを選択します。

ステップ 4 [保存] をクリックしてコピー処理を開始します。

完了すると、「コピー操作成功」というメッセージがウィンドウに表示されます。

再起動

AP の再起動

[再起動] ページを使用すると AP を再起動できます。

ステップ 1 WAP を再起動するには、ナビゲーション ウィンドウで [管理] > [再起動] の順に選択します。

ステップ 2 次のいずれかのオプションを選択します。

- [再起動]: スタートアップ コンフィギュレーションを使用して WAP を再起動します。
- [出荷時のデフォルトで再起動]: 工場出荷時のデフォルト コンフィギュレーション ファイルを使用して WAP を再起動します。カスタマイズしたすべての設定が失われます。

ウィンドウが表示されて、再起動を確認またはキャンセルできます。現行の管理セッションが終了されることがあります。

ステップ 3 [OK] をクリックして再起動します。

ディスカバリ - Bonjour

Bonjour を使用すると、マルチキャスト DNS（mDNS）を使用して AP および Bonjour のサービスを検出できます。Bonjour ではサービスをネットワークにアドバタイズし、サポートしているサービスの種類に関するクエリに答えることで、小規模なビジネス環境でのネットワーク構成を簡素化します。

AP では次のサービスの種類をアドバタイズします。

- **シスコ固有のデバイス記述**（csco-sb）: このサービスにより、クライアントでは、ビジネス ネットワークに展開されている Cisco WAP デバイスおよびその他の製品を検出できます。

- **管理ユーザ インターフェイス**: このサービスは WAP デバイスで使用可能な管理インターフェイス（HTTP、HTTPS、および SNMP）を識別します。

Bonjour 対応 WAP デバイスがネットワークに接続されたとき、すべての Bonjour クライアントでは、事前構成なしでコンフィギュレーション ユーティリティを検出および利用できます。

システム管理者はインストールされている Internet Explorer プラグインを使用して WAP デバイスを検出できます。この Web ベースのコンフィギュレーション ユーティリティはブラウザのタブとして表示されます。

Bonjour は IPv4 と IPv6 の両方のネットワークで機能します。

Bonjour はデフォルトで有効になっています。

管理ステータスの変更

管理ステータスを変更するには、次の手順を実行してください。

ステップ 1 ナビゲーション ウィンドウで [管理] > [ディスカバリ - Bonjour] の順に選択します。

ステップ 2 Bonjour を有効にするには [有効化] をオンにします。Bonjour を無効にするには [有効化] をオフにします。

ステップ 3 [保存] をクリックします。変更がスタートアップ コンフィギュレーションに保存されます。

パケット キャプチャ

ワイヤレス パケット キャプチャ機能を使用すると、WAP デバイスによって送受信されたパケットをキャプチャおよび保管できます。キャプチャされたパケットは、次に、トラブルシューティングやパフォーマンスの最適化のためにネットワーク プロトコル アナライザで分析できます。パケット キャプチャには 2 通りの方式があります。

- **ローカル キャプチャ方式**: キャプチャされたパケットは WAP デバイス上のファイルに保管されます。WAP デバイスでこのファイルを TFTP サーバに送信することも、HTTP または HTTPS によってコンピュータにダウンロードすることもできます。このファイルは pcap 形式でフォーマットされており、Wireshark、OmniPeek などのツールを使用して検査できます。

- [リモートキャプチャ(Remote capture)]:キャプチャされたパケットは Wireshark ツールを実行している外部コンピュータにリアルタイムでリダイレクトされます。
- [CloudSharkキャプチャ(CloudShark Capture)]:キャプチャされたパケットは、CloudShark アプライアンスにリアルタイムでアップロードされます。CloudShark アプライアンスでは、キャプチャに名前とタグを付け検索することができ、キャプチャが整理されます。

注 CloudShark は Web 用のネットワーク アナライザ ツールです。追加のユーティリティ、プラグイン、ダウンロードを必要とせず、任意の Web ブラウザからアクセスできます。

WAP デバイスでは次のタイプのパケットをキャプチャできます。

- 無線インターフェイスで送受信された 802.11 パケット。802.11 ヘッダーを含む、無線インターフェイスでキャプチャされたパケット。
- イーサネット インターフェイスで送受信された 802.3 パケット。
- VAP インターフェイス、WDS インターフェイスなどの内部論理インターフェイスで送受信された 802.3 パケット。

[管理] > [パケット キャプチャ] の順に選択して [パケット キャプチャ] ページを表示します。[パケット キャプチャ] ページでは次の操作が可能です。

- パケット キャプチャ パラメータを設定する。
- ローカルまたはリモート パケット キャプチャを開始する。
- 現在のパケット キャプチャ ステータスを表示する。
- パケット キャプチャ ファイルをダウンロードする。

[パケット キャプチャ構成] 領域では、パラメータを設定してパケット キャプチャを開始できます。

パケット キャプチャの設定

パケット キャプチャ設定を指定するには、次の手順を実行してください。

ステップ 1 次のパラメータを設定します。

- [ビーコンのキャプチャ]:無線によって検出または送信された 802.11 ビーコンのキャプチャを有効または無効にします。
- [無作為キャプチャ]:キャプチャがアクティブであるときの無差別モードを有効または無効にします。

無差別モードでは、この WAP デバイス宛てではないトラフィックを含め、チャネル上のすべてのトラフィックを無線機が受信します。無差別モードで動作中の無線機は、関連付けられたクライアントの処理を続行しています。この WAP デバイスを宛先としていないパケットは転送されません。

キャプチャが完了次第、無線機は非無差別モード動作に戻ります。

- [無線クライアント フィルタ]:指定した MAC アドレスの WLAN クライアントとの間で送受信されるフレームのみをキャプチャする WLAN クライアント フィルタを有効または無効にします。
- [クライアント フィルタ MAC アドレス]:WLAN クライアント フィルタリング用の MAC アドレスを指定します。

注 MAC フィルタは、802.11 インターフェイスのキャプチャを実施している場合に限りアクティブです。

- [パケット キャプチャ方式]:次のいずれかのオプションを選択します。
  - [ローカル ファイル]:キャプチャされたパケットは WAP デバイス上のファイルに保管されます。
  - [リモート]:キャプチャされたパケットは Wireshark ツールを実行している外部コンピュータにリアルタイムでリダイレクトされます。
  - [CloudShark]:キャプチャされたパケットは、CloudShark アプライアンスにリアルタイムでアップロードされます。

ステップ 2 選択した方式に応じて、「ローカル パケット キャプチャ」セクションまたは「リモート パケット キャプチャ」セクションを参照して続行してください。

注 パケット キャプチャ構成パラメータに対する変更は、パケット キャプチャの再開後に有効になります。パケット キャプチャの実行中にパラメータを変更しても現在のパケット キャプチャ セッションには影響を与えません。新しいパラメータ値の使用を開始するには、既存のパケット キャプチャ セッションを停止して再開する必要があります。

ローカル パケット キャプチャ

ローカル パケット キャプチャを開始するには、次の手順を実行してください。

ステップ 1 [パケット キャプチャ方式] で [ローカル ファイル] が選択されていることを確認します。

ステップ 2 次のパラメータを設定します。

- [キャプチャ インターフェイス]:パケット キャプチャのキャプチャ インターフェイス タイプを入力します。
  - **radio1**:無線インターフェイス Radio 1 上の 802.11 トラフィック。
  - **radio2**:Radio 2 上の 802.11 トラフィック。
  - **eth0**:イーサネット ポート上の 802.3 トラフィック。
  - **wlan0**:Radio 1 上の VAP0 トラフィック。
  - **wlan1**:Radio 2 上の VAP0 トラフィック
  - **wlan0vap1** ～ **wlan0vap7**:Radio 1 上の指定した VAP 上のトラフィック。
  - **wlan1vap1** ～ **wlan1vap7**:Radio 2 上の指定した VAP 上のトラフィック。
  - **wlan0wds0** ～ **wlan0wds3**:指定した WDS インターフェイス上のトラフィック。
  - **brtrunk**:WAP デバイスの Linux ブリッジ インターフェイス。
- [キャプチャ期間]:キャプチャの期間を秒数で入力します。範囲は 10 ～ 3600 です。デフォルトは 60 です。CloudShark を使用する無制限のパケット キャプチャ方式では、値を 0 秒にすることができます。
- [最大キャプチャ ファイル サイズ]:許可されるキャプチャ ファイルの最大サイズを KB 単位で入力しています。範囲は 64 ～ 4096 です。デフォルトは 1024 です。CloudShark を使用するパケット キャプチャ方式では、このオプションは有効になりません。

ステップ 3 [保存] をクリックします。変更がスタートアップ コンフィギュレーションに保存されます。

ステップ 4 [キャプチャ開始] をクリックします。

ローカル パケット キャプチャ モードでは、WAP デバイスはキャプチャしたパケットを RAM ファイル システムに保管します。有効化したパケット キャプチャは、次のいずれかのイベントが発生するまで持続します。

- キャプチャ時間が設定した期間に到達する。
- キャプチャ ファイルが最大サイズに到達する。
- 管理者がキャプチャを停止する。

WAP デバイスでアクティブなキャプチャがある場合は、このページの [パケット キャプチャ ステータス] 領域にパケット キャプチャ ステータスが表示されます。

- [現在のキャプチャ ステータス]:パケット キャプチャが実行中か停止しているか。
- [パケット キャプチャ時間]:経過したキャプチャ時間。
- [パケットキャプチャファイルサイズ(Packet Capture File Size)]:現在のキャプチャ ファイル サイズ。通常このサイズは、キャプチャ サイズが制限された無料の CloudShark アカウントを使用している場合には、CloudShark のキャプチャ サイズよりも大きくなります。
- [CloudSharkキャプチャファイルのアップロードステータス(CloudShark Capture File Upload Status)]:選択した CloudShark パケット キャプチャのアップロードが成功すると、ハイパーリンクが表示されます。[CloudSharkでキャプチャを表示(View Capture on CloudShark)] ハイパーリンクをクリックすると、ブラウザ ウィンドウが開き、CloudShark アプライアンスでキャプチャされたパケットが表示されます。

注 アップロードが失敗すると、エラー メッセージが表示されます。

WAP デバイスからの最新データを表示するには [更新] をクリックします。

注 パケット ファイル キャプチャを終了するには、[キャプチャの終了] をクリックします。

リモート パケット キャプチャ

リモート パケット キャプチャ機能では、パケット キャプチャの宛先としてリモート ポートを指定できます。この機能は Windows 用 Wireshark ネットワーク アナライザ ツールと連携して動作します。パケット キャプチャ サーバは WAP デバイス上で実行され、キャプチャしたパケットは TCP 接続を通じて Wireshark ツールに送信されます。Wireshark はオープン ソースのツールで、http://www.wireshark.org からダウンロードして無料で利用できます。

Wireshark ツールを実行している Microsoft Windows コンピュータでは、キャプチャしたトラフィックを表示、記録、および分析できます。リモート パケット キャプチャ機能は、Windows 用 Wireshark ツールの標準機能です。Linux バージョンは WAP デバイスに使用できません。

リモート キャプチャ モードを使用している場合、WAP デバイスでは、キャプチャしたデータをローカルのファイル システムに保管しません。

Wireshark コンピュータと WAP デバイスの間にファイアウォールが設置されている場合は、ファイアウォールを通過するように、該当ポートのトラフィックを許可する必要があります。ファイアウォールは、Wireshark コンピュータから WAP デバイスへの TCP 接続の開始を許可するように設定する必要もあります。

WAP デバイスでのリモート キャプチャの開始

WAP デバイスでリモート キャプチャを開始するには、次の手順を実行してください。

ステップ 1 [管理] > [パケット キャプチャ] の順に選択します。

ステップ 2 [無作為キャプチャ] を有効にします。

ステップ 3 [パケット キャプチャ方式] で [リモート] を選択します。

ステップ 4 [リモート キャプチャ ポート] でデフォルト ポート（2002）を使用するか、デフォルト以外のポートを使用している場合は、Wireshark を WAP デバイスに接続するために使用する、必要なポート番号を入力します。ポートの範囲は 1025 ～ 65530 です。

ステップ 5 別の機会に使用するために設定を保存するには、[保存] をクリックします。

ステップ 6 [キャプチャ開始] をクリックします。

ネットワーク アナライザ ツールの開始

Microsoft Windows 用 Wireshark ネットワーク アナライザ ツールを開始するには、次の手順を実行してください。

ステップ 1 同じコンピュータで Wireshark ツールを開始します。

ステップ 2 メニューで [Capture] > [Options] の順に選択します。ポップアップ ウィンドウが表示されます。

ステップ 3 [Interface] で [Remote] を選択します。ポップアップ ウィンドウが表示されます。

ステップ 4 [Host]：WAP デバイスの IP アドレスを入力します。

ステップ 5 [Port]：WAP のポート番号を入力します。たとえば、デフォルトを使用した場合は 2002 を入力し、デフォルト以外のポートを使用した場合は使用したポート番号を入力します。

ステップ 6 [OK] をクリックします。

ステップ 7 パケットをキャプチャする必要のあるインターフェイスを選択します。Wireshark ポップアップ ウィンドウの IP アドレスの横に、インターフェイスを選択するためのプルダウン リストがあります。インターフェイスは次のいずれかにすることができます。

WAP デバイスの Linux ブリッジ インターフェイス
--rpcap://[192.168.1.220]:2002/brtrunk
優先 LAN インターフェイス
-- rpcap://[192.168.1.220]:2002/eth0
Radio 1 上の VAP0 トラフィック
-- rpcap://[192.168.1.220]:2002/wlan0
802.11 トラフィック
-- rpcap://[192.168.1.220]:2002/radio1
WAP571/E の Radio 1 に対する VAP1 ～ VAP7 トラフィック
-- rpcap://[192.168.1.220]:2002/wlan0vap1 ~ wlan0vap7
WAP571/E の Radio 2 に対する VAP1 ～ VAP7 トラフィック
-- rpcap://[192.168.1.220]:2002/wlan1vap1 ~ wlan1vap7

WAP デバイス上の最大 4 個のインターフェイスを同時にトレースできます。ただし、インターフェイスごとに別々の Wireshark セッションを開始する必要があります。追加のリモート キャプチャ セッションを開始するには、Wireshark の構成手順を繰り返してください。WAP デバイスでの構成を実施する必要はありません。

注 システムでは、リモート パケット キャプチャ セッション用に設定されたポートから始まる連続する 4 個のポート番号を使用します。連続する 4 個のポート番号を使用できることを確認してください。デフォルト ポートを使用しない場合は、1024 よりも大きいポート番号を使用することをお勧めします。

無線インターフェイスのトラフィックをキャプチャする際、ビーコン キャプチャを無効化することはできますが、その他の 802.11 制御フレームは引き続き Wireshark に送信されます。次の情報のみを表示するように表示フィルタを設定できます。

- トレース内のデータ フレーム
- 特定の独立基本サービス セット ID（BSSID）上のトラフィック
- 2 台のクライアント間のトラフィック

次に有用な表示フィルタの例をいくつか示します。

- ビーコンおよび ACK/RTS/CTS フレームを除外：

  !(wlan.fc.type_subtype == 8 || wlan.fc.type == 1)

- データ フレーム限定：

  wlan.fc.type == 2

- 特定の BSSID 上のトラフィック：

  wlan.bssid == 00:02:bc:00:17:d0

- 特定のクライアントとの間の全トラフィック：

  wlan.addr == 00:00:e8:4e:5f:8e

リモート キャプチャ モードでは、トラフィックは、いずれかのネットワーク インターフェイスを通じて、Wireshark を実行しているコンピュータに送信されます。トラフィックは、Wireshark ツールの場所に応じて、イーサネット インターフェイスまたはいずれかの無線で送信できます。パケットをトレースしたためにトラフィックがフラッディングしないために、WAP デバイスでは、Wireshark アプリケーションを宛先とするすべてのパケットをフィルタ処理して除外するキャプチャ フィルタを自動で設定します。たとえば、Wireshark IP ポートが 58000 に設定されている場合は、次のキャプチャ フィルタが WAP デバイスに自動で設定されます。

not portrange 58000-58004

パフォーマンス上とセキュリティ上の問題から、パケット キャプチャ モードは WAP デバイス上の NVRAM に保存されません。WAP デバイスがリセットされるとキャプチャ モードは無効になるため、トラフィックのキャプチャを再開するには有効化し直す必要があります。パケット キャプチャ パラメータ（モードを除く）は NVRAM に保存されます。

パケット キャプチャ機能を有効化すると、次のセキュリティ上の問題が発生することがあります。権限を持たないクライアントが WAP デバイスに接続してユーザ データをトレースするおそれがあります。パケットのキャプチャ中は WAP デバイスのパフォーマンスにも悪影響があり、この影響はアクティブ Wireshark セッションがない場合でも、ある程度続くことがあります。トラフィック キャプチャ中に WAP デバイスでのパフォーマンスへの影響を最小限にするには、Wireshark ツールに送信されるトラフィックを制限するキャプチャ フィルタを設定します。802.11 トラフィックをキャプチャするとき、キャプチャしたフレームの大部分はビーコンになる傾向があります（通常は、すべての AP が 100 ミリ秒ごとに送信）。Wireshark ではビーコン フレームの表示フィルタをサポートしている一方で、WAP デバイスがキャプチャしたビーコン パケットを Wireshark ツールに転送しないようにするキャプチャ フィルタはサポートしていません。802.11 ビーコンのキャプチャ処理によるパフォーマンス上の影響を削減するには、キャプチャ ビーコン モードを無効にします。

キャプチャ ファイルは、TFTP を介して設定した TFTP サーバにダウンロードするか、HTTP または HTTPS を介してコンピュータにダウンロードできます。キャプチャ ファイルは RAM ファイル システムにあり、WAP デバイスがリセットされると消去されます。

TFTP を使用したパケット キャプチャ ファイルのダウンロード

TFTP を使用してパケット キャプチャ ファイルをダウンロードするには、次の手順を実行してください。

ステップ 1 [TFTP を使用してキャプチャ ファイルをダウンロード] を選択します。

ステップ 2 デフォルトと異なる場合は、ダウンロードする [TFTP サーバ ファイル名] を入力します。デフォルトでは、キャプチャされたパケットは WAP デバイスの /tmp/apcapture.pcap フォルダ ファイルに保管されます。

ステップ 3　提示されるフィールドに [TFTP サーバの IPv4 アドレス] を指定します。

ステップ 4　[ダウンロード] をクリックします。

HTTP を使用したパケット キャプチャ ファイルのダウンロード

HTTP を使用してパケット キャプチャ ファイルをダウンロードするには、次の手順を実行してください。

ステップ 1　[TFTP を使用してキャプチャ ファイルをダウンロード] をクリアします。

ステップ 2　[ダウンロード] をクリックします。確認ウィンドウが表示されます。

ステップ 3　[OK] をクリックします。ファイルを保存するネットワークの場所を選択できるダイアログボックスが表示されます。

サポート情報

[サポート情報] ページでは AP に関する詳細コンフィギュレーション情報を格納しているテキスト ファイルをダウンロードできます。このファイルには、ソフトウェアとハードウェアのバージョン情報、MAC アドレスと IP アドレス、機能の管理および運用のステータス、ユーザ設定された設定、トラフィックの統計情報などが格納されています。このテキスト ファイルはテクニカル サポート担当者に提供して、問題のトラブルシューティングに役立てることができます。

[サポート情報] ページを表示するには、[管理] > [サポート情報] の順に選択します。

[ダウンロード] をクリックして、現在のシステム設定に基づいてファイルを生成します。短い待ち時間の後でウィンドウが表示されて、ファイルをコンピュータに保存できます。

スパニング ツリー設定

[スパニング ツリー設定] ページは Cisco WAP571/E の STP 設定を指定するために使用します。

Cisco WAP571 の STP 設定の指定

Cisco WAP571 の STP 設定を指定するには、次の手順を実行してください。

ステップ 1　[管理] > [スパニング ツリー設定] の順に選択します。

ステップ 2　パラメータを設定します。

[STP ステータス]：Cisco WAP571/E での STP をグローバルに有効または無効にします。デフォルトでは、STP は有効です。

ステップ 3　[保存] をクリックします。変更がスタートアップ コンフィギュレーションに保存されます。

4

LAN

ここでは、WAP デバイスのポート、VLAN、IPv4、および IPv6 の設定方法について説明します。

具体的な内容は次のとおりです。

- ポート設定
- VLAN 設定
- IPv4 設定
- IPv6 設定
- IPv6 トンネル
- LLDP

ポート設定

[ポート設定] ページを使用して、WAP デバイスをローカル エリア ネットワークに物理的に接続するポートの設定を表示および実行します。

ポートを設定するには

ステップ 1 [LAN] > [ポート設定] の順に選択します。

[ポート設定] 表には、次の 2 つのインターフェイス（Eth0 から Eth1）のステータスと設定が表示されます。

- [リンク ステータス]: 現在のポートのリンク ステータスが表示されます。
- [ポート速度]: レビュー モードでは、現在のポート速度が表示されます。編集モードでは、自動ネゴシエーションが無効な場合、100 Mbps または 10 Mbps のポート速度を選択します。1000 Mbps の速度は、自動ネゴシエーションが有効な場合にのみサポートされます。

- [デュプレックス モード]: レビュー モードでは、現在のポートのデュプレックス モードが表示されます。編集モードでは、自動ネゴシエーションが無効な場合、[半二重] または [全二重] のいずれかを選択します。

[自動ネゴシエーション]: 有効な場合、ポートはリンク パートナーとネゴシエートして、最速のリンク速度と使用可能なデュプレックス モードを設定します。無効な場合、手動で [ポート速度] と [デュプレックス モード] を設定できます。

[グリーン イーサネット]: グリーン イーサネット モードでは、自動パワーダウン モードと Energy Efficient Ethernet（EEE、IEEE 802.3az）モードの両方がサポートされています。グリーン イーサネット モードは、ポートの自動ネゴシエーションが有効な場合にのみ機能します。自動パワーダウン モードでは、リンク パートナーからの信号が存在しない場合にチップ電力が低減されます。WAP デバイスは、回線上のエネルギーが失われると自動的に低電力モードになり、エネルギーが検出されると通常動作に戻ります。EEE モードでは、リンク使用量が少ないときの待機時間がサポートされます。これにより、リンクの両側で、各 PHY の動作回路の一部を無効にして電力を節約できます。

- [グリーン イーサネット ステータス]: 現在の EEE ステータスが表示されます。

ステップ 2 編集するインターフェイスをチェックしてから、[編集] ボタンをクリックして編集モードに入ります。その後、設定を入力します。

ステップ 3 [保存] をクリックします。変更が、スタートアップ コンフィギュレーションに保存されます。

注 WAP571/E は、リンク アグリゲーション モードにするために Eth0 および Eth1 の 2 つをバンドルします。リンク パートナーもリンク アグリゲーションをサポートしている必要があります。Eth1 は、常に Eth0 の設定に従います。

VLAN 設定

[VLAN 設定] ページを使用し、VLAN 設定を表示および実行します。

VLAN を設定するには

ステップ 1 [LAN] > [VLAN 設定] の順に選択します。

ステップ 2 [VLAN 設定] 表には、各 VLAN レコードに次のフィールドがあります。

- [VLAN ID]: VLAN の ID。各 VLAN ID は1 ～ 4094 の範囲で、同じ VLAN ID にすることはできません。

- [説明]：関連する VLAN の説明。64 文字以下で入力する必要があります。A-Z、a-z、0-9、_ を使用できます。

ステップ 3 [管理 VLAN]：Web GUI を通して WAP デバイスにアクセスするために使用する VLAN。管理 VLAN にすることができる VLAN は 1 つのみです。インターフェイス（有線または無線）が管理 VLAN に属していない場合、ユーザが設定ユーティリティへのアクセスに使用できるインターフェイスはありません。

- [Eth0 - Eth1]：各ポートには、最大 1 つのタグなし VLAN が必要です。次のオプションが用意されています。
  - [タグなし]：ポートは VLAN のメンバーです。ポートから送信された VLAN のパケットは、タグなしになります。ポートが受信したタグなしパケットは、VLAN（タグ付き）に分類されます。
  - [タグ付き]：ポートは、VLAN のメンバーです。ポートから送信された VLAN のパケットは、VLAN ヘッダーでタグ付けされます。
  - [除外]：ポートは VLAN に属していません。

注 VLAN ID 1 を削除することはできません。VLAN に関連付けられたポート（有線または無線）が削除されると、WAP デバイスはその VLAN ID を自動的に 1 に設定します。

注 新しい設定を保存すると、対応するプロセスが停止され、再起動されることがあります。この事態が発生すると、WAP デバイスが切断される可能性があります。切断によってワイヤレス クライアントが受ける影響が最も小さい場合に、WAP デバイスの設定を変更することをお勧めします。

IPv4 設定

[IPv4 設定] ページを使用して、スタティックまたはダイナミック IPv4 アドレス割り当てを設定します。

IPv4 アドレスを設定するには

ステップ 1 [LAN] > [IPv4 設定] の順に選択します。

ステップ 2 次の IPv4 設定を行います。

- [接続タイプ]：デフォルトでは、WAP デバイス上の DHCP クライアントが、ネットワーク情報の要求を自動的にブロードキャストします。スタティック IP アドレスを使用する場合は、DHCP クライアントを無効にして、手動で IP アドレスとその他のネットワーク情報を設定する必要があります。

次のオプションのいずれかを選択します。

- [DHCP]：WAP デバイスは、LAN 上の DHCP サーバから IP アドレスを取得します。
- [スタティック IP]：IPv4 アドレスを手動で設定します。IPv4 アドレスは、xxx.xxx.xxx.xxx（192.0.2.10）の形式にする必要があります。

- [スタティック IP アドレス]、[サブネット マスク]、[デフォルト ゲートウェイ]：スタティック IP アドレスを割り当てる場合は、これらのフィールドに IP 情報を入力します。
- [ドメイン ネーム サーバ]：次のいずれかのオプションを選択します。
  - [ダイナミック]：WAP デバイスは、LAN 上の DHCP サーバから DNS サーバ アドレスを取得します。
  - [手動]：1 つ以上の DNS サーバ アドレスを手動で設定します。指定のフィールドに最大 2 つの IP アドレスを入力します。

ステップ 3　IPv4 DHCP 自動コンフィギュレーションを次に示すように設定します。

- [DHCP 自動コンフィギュレーション オプション（DHCP Auto Configuration Options）]：デフォルトでは、[DHCP 自動コンフィギュレーション オプション（DHCP Auto Configuration Options）] が有効になっています。アクセス ポイントが工場出荷時の状態で起動される場合、最初に DHCP オプションを使用した自動コンフィギュレーションが試みられます。

  自動コンフィギュレーションの動作は次のとおりです。

  - イーサネット インターフェイスのみが有効にされて、WLAN インターフェイスはダウンした状態で、アクセス ポイントが起動します。
  - ユーザが利用できるサービスはありません（ユーザ インターフェイスは除きます）。

- [待機間隔(Wait Interval)] に指定された時間が経過した時点、またはコンフィギュレーション ファイルの TFTP アップロードが完了した時点(どちらか早い方)で、[DHCP 自動コンフィギュレーション オプション(DHCP Auto Configuration Options)] が自動的に無効になります。
- DHCP クライアントを無効にした場合(つまり、スタティック IP アドレスを使用するように設定した場合)や、[DHCP 自動コンフィギュレーション オプション(DHCP Auto Configuration Options)] を無効にした場合、自動コンフィギュレーションは即時に中止されます。

WAP デバイス上の DHCP クライアントは、DHCP オプション 66 および 67 の要求を自動的にブロードキャストします。[DHCP] と [DHCP 自動コンフィギュレーション オプション(DHCP Auto Configuration Options)] が有効である場合、アクセス ポイントは次のリブート時に、DHCP 要求に対して DHCP サーバが返した情報を使用して自動的に設定されます。

注 ユーザ/管理者がコンフィギュレーション ファイルをアップロードすると、自動コンフィギュレーションはオーバーライドされて、その選択されたコンフィギュレーション ファイルが優先されます。それ以外の場合にアクセス ポイントがリブートされる(ファームウェアをアップグレードした場合や、リブート操作を行ったなど)際は、既存の自動コンフィギュレーション設定が適用されます。

- [バックアップ TFTP サーバの IPv4 アドレス/ホスト名(Backup TFTP Server IPv4 address/Host Name)]: TFTP サーバのアドレスを設定すると、自動コンフィギュレーション中に DHCP サーバが指定する他の TFTP サーバからファイルを取得できなかった場合に、そのアドレスが使用されます。IPv4 アドレスまたはホスト名の情報を入力します。ホスト名の形式で入力する場合は、ホスト名を IP アドレスに変換するための DNS サーバが利用可能でなければなりません。

  この値は、次の起動時に自動コンフィギュレーション プロシージャで使用されます。

- [コンフィギュレーション ファイル名]: コンフィギュレーション ファイル名を指定すると、アクセス ポイントの自動コンフィギュレーション中に DHCP サーバからブート ファイル名を受信しない場合に、指定したコンフィギュレーション ファイルが TFTP サーバから取得されます。この値が指定されていない場合は、「config.xml」が使用されます。ファイルを指定する場合、拡張子は xml でなければなりません。

  この値は、次の起動時に自動コンフィギュレーション プロシージャで使用されます。

- [待機間隔(Wait Interval)]:待機間隔が設定されている場合、アクセス ポイントがローカル設定を使用して起動した後、待機間隔として設定された時間が経過してから、有効にされているサービスをユーザが利用できるようにします。指定された待機期間内に TFTP トランザクションが開始されなければ、アクセス ポイントは自動コンフィギュレーションを中止します。

  この値は、次の起動時に自動コンフィギュレーション プロシージャで使用されます。

- [ステータス ログ]:このフィールドには、自動コンフィギュレーションの完了または中止理由が表示されます。

ステップ 4 [保存] をクリックします。変更が、スタートアップ コンフィギュレーションに保存されます。

注 新しい設定を保存すると、対応するプロセスが停止され、再起動されることがあります。この事態が発生すると、WAP デバイスが切断される可能性があります。切断によってワイヤレス クライアントが受ける影響が最も小さい場合に、WAP デバイスの設定を変更することをお勧めします。

IPv6 設定

[IPv6 設定] ページを使用して、IPv6 アドレスを使用する WAP デバイスを設定します。

IPv6 アドレスを設定するには

ステップ 1 [LAN] > [IPv6 設定] の順に選択します。

ステップ 2 次のパラメータを設定します。

- [IPv6 接続タイプ]:WAP デバイスが IPv6 アドレスを取得する方法を選択します。
  - [DHCPv6]:DHCPv6 サーバによって IPv6 アドレスが割り当てられます。
  - [Static IPv6]:IPv6 アドレスを手動で設定します。IPv6 アドレスは、xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx(2001:DB8::CAD5:7D91)の形式にする必要があります。

注 スタティック IPv6 を設定すると、DHCPv6 は使用できなくなります。DHCPv6 を設定すると、設定が存在する場合にスタティック IPv6 を操作できます。

- [IPv6 管理モード]:IPv6 管理アクセスを有効または無効にします。

- [IPv6 自動設定管理モード]：WAP デバイス上の IPv6 自動アドレス設定を有効または無効にします。

  有効な場合、WAP デバイスは、LAN ポートで受信したルータ アドバタイズメントを処理することによって、IPv6 アドレスとゲートウェイを学習します。WAP デバイスは、自動設定された複数の IPv6 アドレスを持つことができます。

- [スタティック IPv6 アドレス]：スタティック IPv6 アドレス。WAP デバイスは、アドレスがすでに自動設定されていても、スタティック IPv6 アドレスを持つことができます。

- [スタティック IPv6 アドレスのプレフィクス長]：スタティック アドレスのプレフィクス長。0 ～ 128 の整数で指定します。デフォルトは 0 です。

- [スタティック IPv6 アドレスのステータス]：次のいずれかのオプションを選択します。

  - [稼働中]：IP アドレスは LAN 上で一意と確認され、インターフェイスでは使用できません。

  - [試行中]：WAP デバイスは、スタティック IP アドレスが割り当てられている場合に、Duplicate Address Detection（DAD; 重複アドレス検出）プロセスを自動的に開始します。IPv6 アドレスは、ネットワークで一意と確認された場合に試行中ステータスになります。このステータスでは、IPv6 アドレスを使用して通常のトラフィックを送受信することはできません。

  - [ブランク]（値なし）：IP アドレスが割り当てられていないか、割り当てられたアドレスが動作していません。

- [IPv6 自動設定グローバル アドレス]：WAP デバイスに 1 つ以上の IPv6 アドレスが自動的に割り当てられている場合、そのアドレスが表示されます。

- [IPv6 リンク ローカル アドレス]：ローカルの物理リンクに使用される IPv6 アドレス。リンク ローカル アドレスは設定できません。IPv6 ネイバー探索プロセスを使用することで割り当てられます。

- [デフォルト IPv6 ゲートウェイ]：静的に設定されたデフォルト IPv6 ゲートウェイ。

- [IPv6 ドメイン ネーム サーバ]：次のいずれかのオプションを選択します。

  - [ダイナミック]：DNS ネーム サーバは DHCPv6 を通して動的に学習されます。

  - [手動]：指定のフィールドに、最大 2 つの IPv6 DNS ネーム サーバを手動で指定します。

ステップ 3　[保存] をクリックします。変更が、スタートアップ コンフィギュレーションに保存されます。

注 新しい設定を保存すると、対応するプロセスが停止され、再起動されることがあります。この事態が発生すると、WAP デバイスが切断される可能性があります。切断によってワイヤレス クライアントが受ける影響が最も小さい場合に、WAP デバイスの設定を変更することをお勧めします。

IPv6 トンネル

WAP571/E デバイスは、Intra-Site Automatic Tunnel Addressing Protocol（ISATAP）をサポートしています。ISATAP によって、WAP デバイスは、IPv4 パケット内にカプセル化した IPv6 パケットを LAN を介して送信できます。このプロトコルによって、WAP デバイスは、接続する LAN が IPv6 をサポートしていなくても、リモートの IPv6 対応ホストと通信できます。

WAP デバイスは、ISATAP クライアントとして機能します。ISATAP が有効なホストまたはルータが、LAN 上に存在している必要があります。ルータの IP アドレスまたはホスト名は、WAP デバイスで設定されます（デフォルトでは isatap）。ホスト名として設定される場合、WAP デバイスは DNS サーバと通信して、名前を 1 つまたは複数の ISATAP ルータ アドレスに解決します。その後、WAP デバイスはルータに送信要求メッセージを送信します。ISATAP が有効なルータがアドバタイズメント メッセージで応答すると、WAP デバイスおよびルータがトンネルを確立します。トンネル インターフェイスは、リンク ローカル アドレスおよびグローバル IPv6 アドレスが割り当てられ、IPv4 ネットワーク上で仮想 IPv6 インターフェイスとして機能します。

IPv6 ホストが ISATAP ルータ経由で接続された WAP デバイスと通信を開始すると、ISATAP ルータによって IPv6 パケットは IPv4 パケットにカプセル化されます。

ISATAP を使用して IPv6 トンネルを設定するには

ステップ 1 ナビゲーション エリアで、[LAN] > [IPv6 トンネル] の順に選択します。

ステップ 2 次のパラメータを設定します。

- [ISATAP ステータス]：WAP デバイスでの ISATAP の管理モードを有効または無効にします。
- [ISATAP 対応ホスト]：ISATAP ルータの IP アドレスまたは DNS 名。デフォルト値は isatap です。
- [ISATAP クエリー間隔]：AP が DNS サーバにクエリーを送信して ISATAP ホスト名を IP アドレスに解決しようとする頻度を指定します。WAP は、ISATAP ルータの IP アドレスが不明な場合にのみ DNS クエリーを送信します。有効な範囲は、120 ～ 3600 秒です。デフォルト値は 120 秒です。

- [ISATAP 送信要求間隔]：WAP が、DNS クエリー メッセージを通して学習する ISATAP ルータにルータ送信要求メッセージを送信する頻度を指定します。WAP は、アクティブな ISATAP ルータがない場合にのみルータ送信要求メッセージを送信します。有効な範囲は、120 ～ 3600 秒です。デフォルト値は 120 秒です。

ステップ 3 [保存] をクリックします。設定が、スタートアップ コンフィギュレーションに保存されます。

トンネルが確立されると、[ISATAP IPv6 リンク ローカル アドレス] と [ISATAP IPv6 グローバル アドレス] がページに表示されます。これらは、IPv4 ネットワークに対する仮想 IPv6 インターフェイス アドレスです。

LLDP

Link Layer Discovery Protocol（LLDP; リンク層検出プロトコル）は、IEEE 802.1AB 標準によって定義されています。LLDP によって、UAP は、システム名、システム性能、および所要電力などの情報をアドバタイズできます。この情報によって、システム トポロジを特定したり、LAN 上の不適切な設定を検出したりすることができます。AP は、Link Layer Discovery Protocol for Media Endpoint Devices（LLDP-MED）もサポートしています。LLDP-MED は、ネットワーク管理を向上するためにデバイスが相互に渡す追加の情報エレメントを標準化します。

LLDP を設定するには

ステップ 1 ナビゲーション エリアで、[LAN] > [LLDP] の順に選択します。

ステップ 2 次のパラメータを設定します。

- [LLDP モード]：AP での LLDP の管理モード。LLDP が有効な場合、AP は LLDP プロトコル データ ユニットをネイバー デバイスに送信します。
- [TX 間隔]：LLDP メッセージ送信の間の秒数。有効な範囲は、5 ～ 32768 秒です。デフォルト値は 30 秒です。
- [POE プライオリティ]：拡張電力の情報要素を AP が送信する場合のプライオリティ レベル。PoE プライオリティ レベルによって、スイッチなどの Power Sourcing Equipment（PSE; 給電側機器）は、すべての接続デバイスに給電するだけの能力がない場合に、どの受電デバイスを優先して電力を割り当てるべきかを判断します。PoE プライオリティは、次のいずれかを選択できます。
  - 重要
  - 高

- 低
- 不明

ステップ 3 [保存] をクリックします。設定が、システムに保存されます。

5

ワイヤレス

ここでは、無線動作のプロパティの設定方法について説明します。

具体的な内容は次のとおりです。

- 無線
- 不正 AP 検出
- ネットワーク
- ワイヤレス マルチキャスト転送
- スケジューラ
- スケジューラ アソシエーション
- MAC フィルタリング
- ブリッジ
- QoS

無線

無線の設定は、WAP デバイスの無線の動作、および物理メディアとのやり取り、つまり WAP デバイスが発する信号の種類やその方法について直接制御します。

無線の設定

無線の設定方法:

ステップ 1 ナビゲーション ペインで、[ワイヤレス] > [無線] を選択します。

ステップ 2 [グローバル設定] エリアで、[TSPEC の違反間隔] を設定します。これは WAP デバイスが、必須アドミッション制御手順に従わなかった、関連付けられたクライアントを報告する時間間隔(秒)です。報告は、システム ログおよび SNMP トラップを介して行われます。0 ～ 900 秒の間の時間を入力します。デフォルトは 300 秒です。

ステップ 3　設定する [無線] インターフェイス（[無線 1] または [無線 2]）を選択します。

ステップ 4　[基本設定] エリアで次の設定を行います。

注 ローカルの規制により、特定の無線モードの使用を禁止されている場合があります。すべての国ですべてのモードが使用可能なわけではありません。

- [無線]：無線インターフェイスをオンまたはオフにします。デフォルトでは、オンになっています。

注 80 MHz の帯域幅を使用する 5 GHz 無線を有効にし、その無線上で大量のトラフィックが伝送される場合、WAP デバイスには IEEE 802.3af PoE 標準の規定（12.95 W）を上回る電力が必要となります。80 MHz チャネルを使用する場合は、WAP デバイスには 802.3at 電源装置（PSE）から電源を供給することを強くお勧めします。WAP デバイスで必要な電力が PSE の最大供給電力を上回った場合、WAP デバイスは再起動する場合があります。

- [MAC アドレス]：インターフェイスの Media Access Control（MAC; メディアアクセス制御）アドレス。MAC アドレスは製造業者が割り当てるもので、変更することはできません。
- [モード]：無線が使用する IEEE 802.11 標準および周波数。モードのデフォルト値は、無線 1 の場合は 802.11a/n/ac 、無線 2 の場合は 802.11b/g/n です。各無線について、選択可能なモードのうち 1 つを選択します。

  無線 1 は次の無線モードに対応しています。

  - 802.11a：802.11a クライアントのみがこの WAP デバイスに接続できます。
  - 802.11a/n/ac：5 GHz の周波数で動作する 802.11a クライアント、802.11n、および 802.11ac クライアントがこの WAP デバイスに接続できます。
  - 802.11n/ac：5 GHz の周波数で動作する 802.11n クライアント、および 802.11ac クライアントがこの WAP デバイスに接続できます。

  無線 2 は次の無線モードに対応しています。

  - 802.11b/g：802.11b および 802.11g クライアントがこの WAP デバイスに接続できます。
  - 802.11b/g/n（デフォルト）：2.4 GHz の周波数で動作する 802.11b、802.11g、および 802.11n クライアントがこの WAP デバイスに接続できます。
  - 802.11n 2.4 GHz：2.4 GHz の周波数で動作する 802.11n クライアントのみがこの WAP デバイスに接続できます。

- [チャネル帯域幅]（802.11n および 802.11ac モードのみ）：802.11n の仕様では、他のモードで使用可能なレガシー 20 MHz チャネルに加え、40 MHz 幅のチャネルも可能です。40 MHz チャネルはより高いデータ レートが使用可能ですが、他の 2.4 GHz および 5 GHz のデバイスで使用可能な少数のチャネルは残ります。

  802.11ac の仕様では、20 MHz および 40 MHz のチャネルに加え、80 MHz 幅のチャネルも可能です。

  20 MHz チャネルへのチャネル帯域幅の使用を制限するため、このフィールドには 20 MHz を設定します。802.11ac モードの場合、無線の 80 MHz チャネル帯域幅の使用を制限するため、このフィールドには 40 MHz を設定します。

- [プライマリ チャネル]（20 または 40 MHz 帯域幅の 802.11n モードのみ）：40 MHz のチャネルは、周波数領域で連続する 2 つの 20 MHz チャネルから構成されると考えられます。これら 2 つの 20 MHz チャネルは、多くの場合、プライマリ チャネルおよびセカンダリ チャネルと呼ばれます。プライマリ チャネルは、20 MHz チャネル帯域幅のみサポートする 802.11n クライアント、およびレガシー クライアントに使用します。

  次のいずれかのオプションを選択します。

  - [上方]：プライマリ チャネルを 40 MHz 帯域内の上方 20 MHz チャネルとして設定します。
  - [下方]：プライマリ チャネルを 40 MHz 帯域内の下方 20 MHz チャネルとして設定します。デフォルトでは [下方] が選択されています。

- [チャネル]：無線が送信および受信に使用する無線スペクトルの一部です。

  使用可能なチャネルの範囲は、無線インターフェイスのモードと国コードの設定により決まります。チャネル設定で [自動] を選択した場合、WAP デバイスは使用可能なチャネルをスキャンし、トラフィックの検出量が最も少なかったチャネルを選択します。

  各モードは、スペクトルが Federal Communications Commission（FCC; 米国連邦通信委員会）、または International Telecommunication Union（ITU-R; 国際電気通信連合）などの国内および国際機関により認可された方法に応じて、多くのチャネルを提供します。

- [スペクトラム解析モード]：スペクトラム解析モードのステータス。スペクトラム解析モードのステータスは、[無効]、[専用スペクトラム アナライザ]、または [ハイブリッド スペクトラム アナライザ（Hybrid Spectrum Analyzer）] のいずれかです。デフォルトは [無効] です。

ステップ 5　[詳細設定] エリアで次の設定を行います。

- [電波時間正常性(Air Time Fairness)]: 電波時間正常性を有効または無効にします。この機能は、低速のデータ転送によって高速のデータ転送が抑制されるという問題に対処します。
- [DFS サポート]: このフィールドは、選択された無線モードが 5 GHz の周波数で動作する場合のみ使用可能です。

  5 GHz 帯域の無線において、[DFS サポート] がオンで、規制ドメインがチャネル上でのレーダー検出を必要とする場合、802.11h の Dynamic Frequency Selection(DFS; 動的周波数選択)および Transmit Power Control(TPC; 送信電力制御)機能は有効になります。

  DFS は、5 GHz 帯域のレーダー システムとスペクトルを共有し、共同チャネル動作を回避するためにワイヤレス デバイスを必要とする機能です。DFS の要件は、AP の国コード設定によって決まる規制ドメインに応じて異なります。

  802.11h ワイヤレス モードを使用する場合、IEEE 802.11h 標準についていくつか重要なポイントがあります。

  - 802.11h は 5 GHz 帯域でのみ有効です。これは 2.4 GHz 帯域では必要ありません。
  - 802.11h が有効なドメインで動作している場合、AP は割り当てられたチャネルを使おうとします。前のレーダー検出によってチャネルがブロックされたり、AP がチャネル上でレーダーを検出した場合、AP は自動的に別のチャネルを選択します。
  - 802.11h が有効な場合、AP はレーダー スキャンのため、最低 60 秒間、5 GHz 帯域で動作しません。
  - 802.11h が動作する場合、WDS リンクを設定することが困難な場合があります。これは、WDS リンク上のこの 2 つの AP が動作するチャネルが、チャネルの使用状況およびレーダーの干渉に応じて、変化し続ける場合があるためです。WDS は、両方の AP が同じチャネルで動作する場合にのみ動作します。WDS の詳細については、ブリッジ をご覧ください。
- [サポートされるショート ガード インターバル]: このフィールドは、選択された無線モードに 802.11n が含まれている場合のみ有効です。

  このガード インターバルは OFDM シンボル間のデッドタイム(ナノ秒)です。このガード インターバルは、シンボル間およびキャリア間の干渉(ISI、ICI)を防ぎます。802.11n モードでは、a および g の定義から、ガード インターバルを 800 ナノ秒から 400 ナノ秒に減らすことができます。ガード インターバルを減らすことにより、データ スループットが 10 % 向上します。

WAP デバイスが通信しているクライアントもショート ガード インターバルに対応している必要があります。

次のいずれかのオプションを選択します。

- [はい]：WAP デバイスは、ショート ガード インターバルにも対応しているクライアントと通信する場合、400 ナノ秒のガード インターバルを使ってデータを送信します。デフォルトでは [はい] が選択されています。
- [いいえ]：WAP デバイスは、800 ナノ秒のガード インターバルを使ってデータを送信します。

- [保護]：この保護機能には、802.11 送信がレガシー ステーションやアプリケーションとの干渉を引き起こさないことを保証するためのルールが含まれます。デフォルトでは、保護は有効です（自動）。保護を有効にすると、レガシー デバイスが WAP デバイスの範囲内にある場合、保護が起動されます。

  保護を無効（オフ）にすることができます。ただし、範囲内のレガシー クライアントまたは WAP デバイスが 802.11n 送信により影響を受ける場合があります。また、保護はモードが 802.11b/g の場合にも有効です。このモードで保護が有効な場合、802.11b クライアントと WAP デバイスを 802.11g 送信から保護します。

注 この設定は、クライアントを WAP デバイスと関連付ける機能には影響を与えません。

- [ビーコンの間隔]：ビーコン フレームの送信間隔。WAP デバイスはワイヤレス ネットワークの存在を知らせるため、これらを通常の間隔で送信します。デフォルトの動作は、ビーコン フレームを 100 ミリ秒ごとに（または 1 秒間に 10 回）送信します。

  20 ～ 2000 ミリ秒の間の整数を入力します。デフォルトは 100 秒です。

- [DTIM 期間]：Delivery Traffic Information Map（DTIM; 配信トラフィック情報マップ）期間。1 ～ 255 ビーコンの間の整数を入力します。デフォルトは 2 ビーコンです。

  DTIM メッセージはビーコン フレームに含まれる要素です。これは、現在低電力モードでスリープ状態にあるクライアント ステーションのうち、どれがピックアップを待っている WAP デバイスにバッファされたデータを保有しているかを示します。

  ここで指定する DTIM 期間は、この WAP デバイスが提供するクライアントが、ピックアップを待っている WAP デバイスにバッファされたデータを、どの程度の頻度で確認するかを示します。

測定はビーコンで行います。たとえばこのフィールドに 1 を設定すると、クライアントは WAP デバイスにバッファされたデータをビーコンごとに確認します。このフィールドに 10 を設定すると、クライアントは 10 ビーコンごとに確認します。

- [フラグメンテーションしきい値]: フレーム サイズのしきい値(バイト)。有効な整数は偶数で、かつ 256 ～ 2346 の範囲内である必要があります。デフォルトは 2346 です。

  フラグメンテーションしきい値は、ネットワーク上を送信されるパケット(フレーム)のサイズを制限する方法です。パケットが設定したフラグメンテーションしきい値を超えた場合、フラグメンテーション機能が有効化され、パケットは複数の 802.11 フレームとして送信されます。

  送信されるパケットがしきい値以下である場合、フラグメンテーションは使用されません。しきい値に最大値(デフォルトの 2,346 バイト)を設定すると、効果的にフラグメンテーションを無効にします。

  フラグメンテーションは、フレームを分割し再構築するという余分な作業が必要なため、またネットワーク上のメッセージ トラフィックを増やすため、より多くのオーバーヘッドを含みます。ただしフラグメンテーションを適切に設定すると、ネットワークのパフォーマンスと信頼性を高めることができます。

  より小さいフレームを送信(より低いフラグメンテーションしきい値を使用)することで、たとえば電子レンジとの干渉の問題解決に役立つ場合があります。

  集約された 802.11n または 802.11ac フレーム(AMPDU)はフラグメント化できません。フラグメンテーションは、レガシー無線モデル、802.11a または 802.11b/g にのみ適用可能です。

  デフォルトでは、フラグメンテーションはオフになっています。無線妨害が疑われる場合を除き、フラグメンテーションを使用しないことを推奨します。各フラグメントに適用される追加ヘッダーは、ネットワークのオーバーヘッドを増加させ、スループットを大幅に低下させる場合があります。

- [RTS しきい値]: Request to Send (RTS; 送信要求)のしきい値。有効な整数の範囲は 0 ～ 65535 です。デフォルトは 65535 オクテットです。

  RTS しきい値は MPDU 内のオクテット数を示し、この値以下の場合 RTS/CTS ハンドシェイクは実行されません。

  特に多くのクライアントがある場合、RTS しきい値を変更することで、WAP デバイスを通過するトラフィック フローを制御できます。低いしきい値を指定した場合、RTS パケットはより頻繁に送信され、より多くの帯域幅を消費し、パケットのスループットが低下します。ただし、より多くの RTS パケットを送信することで、ビジーなネットワーク、または電磁干渉を受けるネットワーク上で発生する干渉や衝突からのネットワーク回復を助けることができます。

RTS しきい値は、(802.11n または 802.11ac ではなく) レガシーな 802.11 データ フレームでのみ使用します。802.11n または 802.11ac の場合、AMPDU 送信はフレーム長に関わらず、RTS/CTS 交換によって保護されます。

- [帯域使用率]: WAP デバイスが新規クライアントの関連付けの許可を停止するまでに使用できる無線帯域幅。有効な整数の範囲は 0 ～ 100 %です。0 を設定すると、使用率に関わらず、新規関連付けが許可されます。デフォルトは 0 です。
- [関連付けられたクライアントの最大数]: この WAP デバイスの各無線に常にアクセスできるステーションの最大数。0 ～ 200 の間の整数を入力できます。デフォルトは 200 ステーションです。デュアル無線 WAP571/E デバイスは、合計で最大 400 クライアントまでサポートします。
- [送信電力]: この WAP デバイスの送信電力レベルのパーセント値。

  デフォルト値の 100 % は、WAP デバイスに最大のブロードキャスト範囲を与え、必要なアクセス ポイント数が減るため、低い % 値に比べてコスト効率が高くなります。

  ネットワークのキャパシティを増やすには、WAP デバイスを近くに配置し、送信電力を減らします。これにより、アクセス ポイント間のオーバーラップと干渉を減らすことができます。また、より弱いワイヤレス信号はネットワークの物理的な場所の外に伝播する可能性が低いため、より低い送信電力設定により、ネットワークをより安全な状態に維持できます。

  チャネル範囲と国コードの組み合わせによって、比較的低い最大送信電力の場合があります。送信電力を低い範囲 (たとえば 25 % または 12 %) に設定しようとした場合、パワー アンプによっては最低の送信電力要件があるため、期待する電力低下が発生しない場合があります。
- [フレーム バースト サポート]: 一般的に、フレーム バースト サポートを有効にすると、ダウンストリーム方向の無線性能が向上します。
- [固定マルチキャスト レート]: ブロードキャストおよびマルチキャスト パケットの送信レート (Mbps)。この設定は、ワイヤレス クライアントで設定レートを調整できる場合、ワイヤレス マルチキャスト ビデオ ストリーミングが発生する環境で役立ちます。

  [自動] が選択された場合、WAP デバイスは関連付けられたクライアントにとってのベスト レートを選択します。有効値の範囲は、設定された無線モードによって決まります。
- [レガシー レート設定]: レートはメガビット/秒で表されます。

サポートされるレート設定は、WAP デバイスがサポートするレートを表します。複数のレートにチェックを付けることができます(レートを選択/選択解除するにはボックスにチェックを付けます)。WAP デバイスは、エラー率や WAP デバイスからクライアント ステーションまでの距離などの要素に基づき、最も効率的なレートを自動的に選択します。

基本レート セットは、ネットワーク上の他のアクセス ポイントやクライアント ステーションとの通信を設定する目的で、WAP デバイスがネットワークにアドバタイズするレートを表します。WAP デバイスにサポートされたレート セットのサブセットをブロードキャストさせると、より効率的です。

- [ブロードキャスト/マルチキャスト レート上限]:マルチキャストおよびブロードキャストのレート上限は、ネットワーク上を送信されるパケット数を制限することで、ネットワーク全体のパフォーマンスを向上させることができます。

  デフォルトでは、マルチキャスト/ブロードキャスト レート上限オプションは無効になっています。マルチキャスト/ブロードキャスト レート上限を有効にするまで、次のフィールドは無効です。

  - [レート上限]:マルチキャストおよびブロードキャストのトラフィックのレート上限。上限は 1 より大きく、50 未満(パケット/秒)でなければなりません。このレート上限を下回るトラフィックは常に適合し、適切な宛先に送信されます。デフォルトでもある最大のレート上限は 50 パケット/秒です。

  - [レート上限バースト]:定義された最大レートを超えている場合でも、一時的なバーストとして通過することが許可されるトラフィックの量で、単位はバイト。デフォルトでもある最大のレート上限バーストは 75 パケット/秒です。

- [TSPEC モード]:WAP デバイスの全体的な TSPEC モードを規制します。デフォルトでは、TSPEC モードはオフです。次のオプションが用意されています。

  - [オン]:WAP デバイスは、[無線] ページで設定した TSPEC 設定に従い、TSPEC 要求を処理します。WAP デバイスが Wi-Fi CERTIFIED 電話などの QoS 対応デバイスからのトラフィックを処理する場合、この設定を使用します。

  - [オフ]:WAP デバイスはクライアント ステーションからの TSPEC 要求を無視します。QoS 対応デバイスが時間的制約のあるトラフィックを優先するために TSPEC を使用したくない場合、この設定を使用します。

- [TSPEC 音声 ACM モード]:音声アクセス カテゴリの必須アドミッション制御(ACM)を規制します。デフォルトでは、TSPEC 音声 ACM モードはオフです。次のオプションが用意されています。

- [オン]: ステーションは、音声トラフィック ストリームを送信または受信する前に、WAP デバイスに帯域幅の TSPEC 要求を送信する必要があります。WAP デバイスは、TSPEC が許可された場合、割り当てられたメディア時間を含む要求の結果と共に応答します。
- [オフ]: ステーションは、許可された TSPEC を要求せずに、音声のプライオリティ トラフィックを送受信できます。WAP デバイスは、クライアント ステーションからの音声 TSPEC 要求を無視します。

- [TSPEC 音声 ACM 上限]: WAP デバイスがアクセスを得るために音声 AC を使って、ワイヤレス メディア上で送信しようとするトラフィック量の上限。デフォルトの上限は、合計トラフィックの 20 % です。
- [TSPEC ビデオ ACM モード]: ビデオ アクセス カテゴリの必須アドミッション制御を規制します。デフォルトでは、TSPEC ビデオ ACM モードはオフです。次のオプションが用意されています。
  - [オン]: ステーションは、ビデオ トラフィック ストリームを送信または受信する前に、WAP デバイスに帯域幅の TSPEC 要求を送信する必要があります。WAP デバイスは、TSPEC が許可された場合、割り当てられたメディア時間を含む要求の結果と共に応答します。
  - [オフ]: ステーションは、許可された TSPEC を要求せずに、ビデオのプライオリティ トラフィックを送受信できます。WAP デバイスは、クライアント ステーションからのビデオ TSPEC 要求を無視します。
- [TSPEC ビデオ ACM 上限]: WAP デバイスがアクセスを得るためにビデオ AC を使って、ワイヤレス メディア上で送信しようとするトラフィック量の上限。デフォルトの上限は、合計トラフィックの 15 % です。
- [TSPEC AP 非アクティブ タイムアウト]: WAP デバイスがダウンリンク トラフィックの仕様をアイドルとして検出し、削除するまでの時間。有効な整数の範囲は 0 ～ 120 秒で、デフォルトは 30 秒です。
- [TSPEC ステーション 非アクティブ タイムアウト]: WAP デバイスがアップリンク トラフィックの仕様をアイドルとして検出し、削除するまでの時間。有効な整数の範囲は 0 ～ 120 秒で、デフォルトは 30 秒です。
- [TSPEC レガシー WMM キュー マップ モード]: ACM として動作するキューのレガシー トラフィックの混合を有効または無効にします。デフォルトでは、このモードはオフです。
- [TurboQAM]: この機能の目的は、Broadcom 固有の Broadcom-to-Broadcom リンクへの VHT 拡張を有効または無効にすることです。VHT 機能は、802.11ac のドラフトで指定されていない 256QAM VHT レートへの対応を有効にします。レートはすべて VHT LDPC モード、MCS 9 Nss 1 20Mhz、MCS 9 Nss 2 20Mhz、MCS 6 Nss 3 80Mhz です。VHT 機能は 802.11ac PHY のためにサポートされています。

ステップ 6 [保存] をクリックします。変更が、スタートアップ コンフィギュレーションに保存されます。

注意 新しい設定を保存すると、対応するプロセスが停止され、再起動されることがあります。この事態が発生すると、WAP デバイスが切断される可能性があります。切断によってワイヤレス クライアントが受ける影響が最も小さい場合に、WAP デバイスの設定を変更することをお勧めします。

不正 AP 検出

不正 AP は、システム管理者からの明示的な許可なく安全なネットワーク上にインストールされているアクセス ポイントです。ここにアクセスできる誰かが無意識に、または悪意を持って安価なワイヤレス AP をインストールすることにより、権限のない関係者がネットワークにアクセスできる可能性があるため、不正アクセス ポイントはセキュリティ上の脅威をもたらします。

AP は、ネットワークの近くにあるすべての AP を検出するため、各無線のすべてのチャネルで RF スキャンを行います。不正 AP が検出された場合、[不正 AP 検出] ページに表示されます。不正としてリストされている AP が正当なものである場合、それを [既知の AP リスト] に追加することができます。

注 [検出された不正 AP リスト] および [信頼できる AP リスト] は、必要なアクションをとるために使える情報を提供します。AP はそのリスト上の不正な AP を制御することはできず、また RF スキャンによって検出された AP にセキュリティ　ポリシーを適用することはできません。

不正 AP について詳細を確認するには、メインのナビゲーション ペインで、[ワイヤレス] > [不正 AP 検出] を選択します。

不正 AP について詳細を確認するには、[ワイヤレス] > [不正 AP 検出] を選択します。

AP 検出を有効にすると、無線は定期的に動作チャネルから同じ帯域内の他のチャネルのスキャンに切り替えます。

不正 AP リストの表示

不正 AP 検出は有効または無効にできます。無線が不正 AP についての情報を収集できるようにするには、無線 1 または無線 2 の [AP 検出] の隣の [有効化] をクリックし、次に [保存] をクリックします。

不正 AP 検出を更新する方法はなく、SSID は一度検出されるとデータベースに保存されます。

検出され信頼できる不正アクセス ポイントに関する情報が表示されます。画面を更新し、最新の情報を表示するには、[更新] をクリックします。

- [アクション]: AP が [検出された不正 AP リスト] にある場合、[信頼する] をクリックして、その AP を [信頼できる AP リスト] に移動することができます。

  AP が [信頼できる AP リスト] にある場合、[信頼しない] をクリックして、その AP を [検出された不正 AP リスト] に移動することができます。

注 [検出された不正 AP リスト] および [信頼できる AP リスト] が情報を提供します。AP はそのリスト上の AP を制御することはできず、また RF スキャンによって検出された AP にセキュリティ　ポリシーを適用することはできません。

- [MAC アドレス]: 不正 AP の MAC アドレス。
- [無線]: 不正 AP が無線 1（wlan0）または無線 2（wlan1）で検出されたかどうかを示します 。
- [ビーコンの間隔]: 不正 AP で使用されるビーコンの間隔。

  AP はワイヤレス ネットワークの存在を知らせるため、ビーコン フレームを通常の間隔で送信します。デフォルトの動作は、ビーコン フレームを 100 ミリ秒ごとに（または 1 秒間に 10 回）送信します。

注 ビーコンの間隔は、[無線] ページで設定します。

- [タイプ]: デバイスのタイプ。
  - AP は、その不正デバイスがインフラストラクチャ モードで IEEE802.11 ワイヤレス ネットワーキング フレームワークをサポートする AP であることを示します。
  - アドホックは、アドホック モードで実行されている不正ステーションを示します。アドホック モードに設定したステーションは、従来の AP を使用せずに互いに直接通信します。アドホック モードは IEEE802.11 ワイヤレス ネットワーキング フレームワークの 1 つで、ピアツーピア モード、または Independent Basic Service Set（IBSS; 独立した基本サービス セット）とも呼ばれます。
- [SSID]: WAP デバイスの Service Set Identifier（SSID）。

  SSID は、ワイヤレス ローカル エリア ネットワークを一意に識別する最大 32 文字の英数字の文字列です。これはネットワーク名とも呼ばれます。
- [プライバシー]: 不正デバイスにセキュリティがあるかどうかを示します。

- [オフ] は、不正デバイスのセキュリティ モードに [None]（セキュリティなし）が設定されていることを示します。
- [オン] は、不正デバイスに何らかのセキュリティがあることを示します。

注 [ネットワーク] ページを使って、AP 上のセキュリティを設定できます。

- [WPA]: WPA セキュリティがその不正 AP に対してオンかオフかを示します。
- [帯域]: 不正 AP で使用される IEEE 802.11 モード。（たとえば、IEEE 802.11a、IEEE 802.11b、IEEE 802.11g など）。

  ここに表示される数字がモードを示します。

  - 2.4 は IEEE 802.11b、802.11g、または 802.11n モード（またはこれらのモードの組み合わせ）を示します。
  - 5 は IEEE 802.11a、802.11n、または 802.11ac モード（またはこれらのモードの組み合わせ）を示します。
- [チャネル]: 不正 AP が現在ブロードキャストしているチャネル。

  チャネルは、無線が送信および受信に使用する無線スペクトルの一部を定義します。

注 [無線] ページを使って、チャネルを設定できます。

注 AP が DFS チャネルで動作している場合、スキャンは禁止されます。したがって、不正 AP は検出されません。

- [レート]: 不正 AP が現在送信しているレート（メガビット/秒）。

  現在のレートは常に、[サポートされるレート] に設定されているレートの 1 つです。

  報告されたレートは、AP からクライアントに送信された最後のパケットの速度です。この値は、AP とクライアント間の信号の品質、およびブロードキャストまたはマルチキャスト フレームが送信されるレートに基づき、アドバタイズされたレート セット内で変わることがあります。AP がデフォルト レートを使ってブロードキャスト フレームを STA に送信する場合、このフィールドは 2.4GHz の無線では 1 Mbps、5GHz の無線では 6 Mbps を報告します。アイドル状態のクライアントは、低いデフォルト レートを報告する確率が最も高くなります。
- [信号]: 不正 AP が発する無線信号の強度。マウスのカーソルをバーに重ねると、強度を示す数字（デシベル）が表示されます。
- [ビーコン]: 不正 AP が最初に検出されてから、そこから受信したビーコンの合計数。

- [最終ビーコン]: 不正 AP から受信した最後のビーコンの日付と時間。
- [レート]: 不正 AP のサポートされた基本の（アドバタイズされた）レート セット。レートはメガビット/秒（Mbps）で表示されます。

  すべてのサポートされるレートがリストされ、基本レートが太字で表示されます。レート セットは [無線] ページで設定します。

信頼できる AP リストの作成および保存

信頼できる AP リストを作成し、ファイルに保存する方法:

ステップ 1 [検出された不正 AP リスト] で、既知の AP について [信頼する] をクリックします。信頼された AP は [信頼できる AP リスト] に移動します。

ステップ 2 [信頼できる AP リストのダウンロード/バックアップ] のエリアで、[バックアップ（AP から PC）] を選択します。

ステップ 3 [保存] をクリックします。

リストには、[既知の AP リスト] に追加されたすべての AP の MAC アドレスが含まれます。デフォルトでは、ファイル名は Rogue2.cfg です。テキスト エディタまたは Web ブラウザを使ってファイルを開き、コンテンツを表示することができます。

信頼できる AP リストのインポート

保存されたリストから既知の AP リストをインポートできます。このリストは、別の AP から取得、またはテキスト ファイルから作成できます。AP の MAC アドレスが [信頼できる AP リスト] に表示される場合、それは不正として検出されていません。

AP リストをファイルからインポートする方法:

ステップ 1 [信頼できる AP リストのダウンロード/バックアップ] のエリアで、[ダウンロード（PC から AP）] を選択します。

ステップ 2 [ブラウズ] をクリックし、インポートするファイルを選択します。

インポートするファイルは、.text または .cfg 拡張子のプレーンテキスト ファイルでなければなりません。ファイルのエントリは、コロンで区切られた各オクテットの 16 進数表記の MAC アドレスです（例：00:11:22:33:44:55）。エントリはシングル スペースで分割する必要があります。AP がファイルを受け入れるためには、MAC アドレスのみを含める必要があります。

ステップ 3 既存の [信頼できる AP リスト] を置き換えるか、インポートしたファイルのエントリを [信頼できる AP リスト] に追加するかを選択します。

a. リストをインポートし、[既知の AP リスト] のコンテンツを置き換えるには、[リプレース] を選択します。

b. リストをインポートし、インポートしたファイルの AP を現在 [既知の AP リスト] に表示されている AP に追加するには、[マージ] を選択します。

ステップ 4 [保存] をクリックします。

インポートが完了したら、画面が更新され、インポートしたファイルの AP の MAC アドレスが [既知の AP リスト] に表示されます。

ネットワーク

Virtual Access Points（VAP; 仮想アクセスポイント）は、ワイヤレス LAN を、イーサネット VLAN と同等のワイヤレスの複数のブロードキャスト ドメインに分割します。VAP は、1つの物理 WAP デバイスの複数のアクセス ポイントをシミュレートします。AP は最大 16 VAP までサポートします。各 VAP は、VAP0 を除き、個別に有効または無効にすることができます。VAP0 は物理無線インターフェイスで、無線が有効なかぎり有効のままです。VAP0 の動作を無効にするには、無線自体を無効にする必要があります。

各 VAP は、ユーザが設定した Service Set Identifier（SSID）により識別できます。複数の VAP で同一の SSID 名を持つことはできません。SSID ブロードキャストは、各 VAP で個別に有効または無効にすることができます。SSID ブロードキャストは、デフォルトで有効になっています。

SSID 命名規則

VAP0 のデフォルトの SSID は ciscosb です。追加で作成された VAP の SSID 名はすべてブランクです。すべての VAP の SSID には他の値を設定できます。

SSID は大文字と小文字を区別し、2 ～ 32 文字の英数字のエントリが可能です。印刷可能な文字とスペース（ASCII 0x20）が指定可能です。

指定可能な文字は、

ASCII 0x20 から 0x7E です。

先頭および末尾にスペース（ASCII 0x20）は使用できません。

注 つまり、スペースは SSID 内で使用できますが、最初または最後の文字としては使用できません。またピリオド「.」（ASCII 0x2E）も使用できます。

VLAN ID

各 VAP は VLAN と関連付けられ、VLAN は VLAN ID（VID）により識別できます。VID は 1 ～ 4094 まで（1 と 4094 を含む）の任意の値を指定できます。WAP571/E デバイスは、33 のアクティブな VLAN（32 の WLAN と 1 つの管理 VLAN）をサポートします。

デフォルトでは、WAP デバイスの設定ユーティリティに割り当てられる VID は 1 です。これはデフォルトのタグなし VID でもあります。管理 VID が VAP に割り当てられた VID と同じである場合、この VAP に関連付けられた WLAN クライアントで WAP デバイスを管理できます。必要な場合は、Access Control List（ACL; アクセス制御リスト）を作成して WLAN クライアントからの管理を無効にできます。

VAP の設定

VAP の設定方法:

ステップ 1 ナビゲーション ペインで、[ワイヤレス] > [ネットワーク] を選択します。

ステップ 2 VAP を設定したい [無線] インターフェイス（[無線 1] または [無線 2]）を選択します。

ステップ 3 設定したい VAP の [有効] チェックボックスをオンにします。

または

VAP0 がシステムで設定されている唯一の VAP で、VAP を追加したい場合、[追加] をクリックします。次に、その VAP を選択し、[編集] をクリックします。

ステップ 4 次のパラメータを設定します。

- [VLAN ID]: VAP と関連付ける VLAN の VID。

注意 必ずネットワーク上で適切に設定された VLAN ID を入力してください。VAP がワイヤレス クライアントを不適切に設定した VLAN と関連付けると、ネットワークに問題が生じる可能性があります。
ワイヤレス クライアントがこの VAP を使って WAP デバイスに接続する場合、ポート VLAN ID を入力、またはワイヤレス クライアントを VLAN に割り当てるために

RADIUS サーバを使用しないかぎり、この WAP デバイスはこのワイヤレス クライアントからのすべてのトラフィックを、このフィールドで入力された VLAN ID とタグ付けします。VLAN ID の範囲は 1 ～ 4094 です。

注 VLAN ID を現在の管理 VLAN ID 以外の ID に変更した場合、この VAP に関連付けられた WLAN クライアントはこのデバイスを管理できません。[LAN] ページ上のタグなしの管理 VLAN ID の設定を確認してください。詳細については、[VLAN 設定]をご覧ください。

- [SSID 名]：ワイヤレス ネットワークの名前。SSIDは、最大 32 文字までの英数字の文字列です。各 VAP に対し、一意の SSID を選択します。

注 管理している WAP デバイスと同じ WAP デバイスにワイヤレス クライアントとして接続した場合、SSID をリセットすると、その WAP デバイスへの接続は失われます。この新しい設定を保存した後、新規 SSID に再接続する必要があります。

- [SSID ブロードキャスト]：SSID のブロードキャストを有効化および無効化します。

  WAP デバイスが このビーコン フレームの SSID をブロードキャストすることを許可するかどうかを指定します。ブロードキャスト SSID パラメータは、デフォルトで有効になっています。VAP が SSID をブロードキャストしない場合、そのネットワーク名はクライアント ステーションで使用可能なネットワークのリストには表示されません。代わりに、接続するには正確なネットワーク名をクライアントのワイヤレス接続ユーティリティに手で入力する必要があります。

  ブロードキャスト SSID の無効化は、誤ってネットワークに接続するクライアントを防止するには十分ですが、ハッカーによる暗号化されていないトラフィックへの接続または監視などの単純な試行でさえ防止できません。SSID ブロードキャストの抑制は、プライオリティによりクライアントの接続が容易になり、抑制しないと無防備なネットワーク（ゲスト ネットワークなど）、および入手可能な機密情報がないネットワークに対し、最低限レベルの保護を提供します。

- [セキュリティ]：VAP にアクセスするために必要な認証タイプ。
  - なし
  - 静的 WEP
  - 動的 WEP
  - WPA パーソナル
  - WPA エンタープライズ

[なし] 以外のセキュリティ モードを選択した場合、追加フィールドが表示されます。認証タイプとして、より強力なセキュリティ保護を提供する、[WPA パーソナル] または [WPA エンタープライズ] の使用を推奨します。[静的 WEP] または [動的 WEP] は、[WAP パーソナル] 、[WAP エンタープライズ] をサポートしていないレガシーのワイヤレス コンピュータまたはデバイスでのみ使用します。セキュリティに [静的 WEP] または [動的 WEP] を設定する必要がある場合、無線を 802.11a または 802.11b/g モードとして設定します(「無線」をご覧ください)。802.11n モードは、セキュリティ モードとして [静的 WEP] または [動的 WEP] を使用することを制限しています。

- [MAC フィルタリング]: この VAP にアクセスできるステーションが、設定された MAC アドレスのグローバル リストに制限されているかどうかを指定します(「MAC フィルタリング」をご覧ください)。次の MAC フィルタリングのタイプからいずれか 1 つを選択できます。
  - [無効]: MAC フィルタリングを使用しません。
  - [ローカル]:「MAC フィルタリング」ページで設定した MAC 認証リストを使用します。
  - [RADIUS]: 外部 RADIUS サーバの MAC 認証リストを使用します。
- [チャネル分離]: ステーションの分離を有効および無効にします。
- 無効にすると、ワイヤレス クライアントは通常、WAP デバイスを介してトラフィックを送信することにより、お互いに通信できます。
  - 有効にすると、WAP デバイスは、同じ VAP 上のワイヤレス クライアント間の通信をブロックします。この場合、WAP デバイスは、ネットワーク上のワイヤレス クライアントと有線デバイス間の WDS リンクを介した、データ トラフィック、および別の VAP に関連付けられた他のワイヤレス クライアントとのデータ トラフィックは許可しますが、ワイヤレス クライアントどうしは許可しません。

注 チャネル分離は単一 AP の同一 VAP に接続されたクライアントに適用可能ですが、別の AP の同一 VAP に接続されたクライアントには適用できません。そのため、単一 AP の同一 VAP に接続されたクライアントはお互いに ping に失敗し、別の AP の同一 VAP に接続されたクライアントはお互いに ping が成功します。

- [バンド ステア]: 両方の無線が動作する場合、バンド ステアを有効にします。無線の n 帯域幅はバンドステアリングとはみなされません。5 GHz 無線が偶然 20 MHz 帯域幅を使用しているときでも、一度バンドステアリングが設定されると、AP はクライアントを 5 GHz 無線にステアしようとします。

ステップ 5 [保存] をクリックします。変更が、スタートアップ コンフィギュレーションに保存されます。

注意 新しい設定を保存すると、対応するプロセスが停止され、再起動されることがあります。この事態が発生すると、WAP デバイスが切断される可能性があります。切断によってワイヤレス クライアントが受ける影響が最も小さい場合に、WAP デバイスの設定を変更することをお勧めします。

注 VAP を削除するには、削除する VAP を選択し、[削除] をクリックします。永久に削除を保存するには、削除が完了したときに [保存] をクリックします。

セキュリティの設定

この章では、[ネットワーク] ページのセキュリティ リストの選択に応じて設定する、セキュリティ設定について説明します。

なし(プレーンテキスト)

セキュリティ モードとして [なし] を選択した場合、AP 上で追加のセキュリティ設定を行うことはできません。このモードは、AP に転送または AP から転送されたデータはすべて暗号化されていないことを意味します。このセキュリティ モードは初期ネットワーク設定時または問題解決時には便利な場合がありますが、安全ではないため、社内ネットワークで日常的に使用することは推奨されません。

静的 WEP

有線と同等のプライバシー(WEP)は、802.11 ワイヤレス ネットワーク用のデータ暗号化プロトコルです。ネットワーク上のすべてのワイヤレス ステーションとアクセス ポイントは、静的な 64 ビット(40 ビットの秘密キー + 24 ビットの Initialization Vector(IV; 初期化ベクトル))、または 128 ビット(104 ビットの秘密キー + 24 ビットの IV)のデータ暗号化共有キーで構成されています。

[静的 WEP] は最も安全なモードではありませんが、部外者が暗号化されていないワイヤレス トラフィックを簡単に傍受することを防ぐことができるため、セキュリティ モードに [なし](プレーン テキスト)を設定するより安全な保護を提供します。

WEP は、静的キーに基づき、ワイヤレス ネットワークを通過するデータを暗号化します。(暗号化アルゴリズムは、RC4 と呼ばれるストリーム暗号です)。

次のパラメータを静的 WEP に設定します。

- [転送キーインデックス]: キーのインデックス リスト。キーのインデックスには 1 ～ 4 が設定できます。デフォルトは 1 です。

  [転送キーインデックス] は、WAP デバイスが送信するデータを暗号化するためにどの WEP キーを 使用するかを示します。

- [キー長]: キーの長さ。いずれか 1 つを選択します。
  - 64 ビット
  - 128 ビット
- [キー タイプ]: キーのタイプ。いずれか 1 つを選択します。
  - ASCII
  - 16 進
- [WEP キー]: 最大 4 つの WEP キーを指定できます。各テキストボックスに、各キーの文字列を入力します。入力するキーは、選択した次のキー タイプによって異なります。
  - ASCII：大文字と小文字のアルファベット、数字、および @ や # などの特殊記号が含まれます。
  - 16 進：0 ～ 9 の数字と A ～ F の文字が含まれます。

  [必要な文字数] フィールドで指定されているとおり、各キーにおいて同じ文字数を使用してください。これらは WAP デバイスを使ってステーションと共有される RC4 WEP キーです。

  各クライアント ステーションは、WAP デバイスに指定されているのと同じスロット内のこれらの同一 WEP キーのいずれかを使用するよう、設定する必要があります。
- [必要な文字数]: [WEP キー] フィールドに入力する文字数は、選択したキー長とキー タイプにより異なります。たとえば、128 ビット ASCII キーを使用する場合、[WEP キー] には 26 文字を入力する必要があります。必要な文字数は、設定したキー長とキー タイプに基づき自動的に更新されます。
- [802.1X 認証]: この認証アルゴリズムは、静的 WEP がセキュリティ モードの場合、クライアント ステーションが WAP デバイスと関連付けられるかどうかを判断するために使用する方法を定義します。

  次のいずれかのオプションを選択し、使用したい認証アルゴリズムを指定します。
  - [オープン システム] 認証は、クライアント ステーションが正確な WEP キーを持っているかどうかに関わらず、そのクライアント ステーションを WAP デバイスと関連付けることができます。このアルゴリズムは、プレーンテキスト、IEEE 802.1X、および WPA モードでも使用されます。認証アルゴリズムに [オープン システム] を設定した場合、どのクライアントも WAP デバイスと関連付けられます。

注 クライアント ステーションが関連付けられるかどうか不明だという理由だけで、WAP デバイスとトラフィックを交換できます。ステーションは、アクセスに成功し、WAP デバイスからのデータを暗号化し、読み取り可能なデータを WAP デバイスに送信するために、正確な WEP キーを持つ必要があります。

- [共有キー] 認証は、クライアント ステーションが WAP デバイスと関連付けられるには、正確な WEP キーを持つことを要求します。認証アルゴリズムに [共有キー] が設定された場合、不適切な WEP キーを持つステーションは、WAP デバイスと関連付けられません。
- [オープン システム] および [共有キー] の両方。両方の認証アルゴリズムを選択した場合、共有キー モードで WEP を使用するよう設定されたクライアント ステーションは、WAP デバイスに関連付けられるためには有効な WEP キーを持っている必要があります。またオープン システムとして WEP を使用するよう設定したクライアント ステーション（共有キー モードは無効）は、正確な WEP キーを持たない場合でも、WAP デバイスに関連付けることができます。

静的 WEP のルール

静的 WEP を使用する場合、次のルールが適用されます。

- すべてのクライアント ステーションは、ワイヤレス LAN（WLAN）のセキュリティに WEP を設定し、AP からステーションへのデータ送信を復号するため、すべてのクライアントが WAP デバイスで指定された WEP キーのいずれか 1 つを持っている必要があります。
- WAP デバイスは、クライアントがステーションから AP への送信に使用するすべてのキーを持つ必要があります。これにより、ステーションの送信を復号できます。
- 同一のキーは、すべてのノード（AP およびクライアント）において同一のスロットを占有する必要があります。たとえば、WAP デバイスが WEP key 3 として abc123 キーを指定する場合、クライアント ステーションは WEP key 3 として これと同じ文字列を指定する必要があります。
- クライアント ステーションはアクセス ポイントにデータを送信するために別のキーを使用できます（または同じキーを使用することもできますが、同じキーを使用すると、あるステーションが他のステーションから送信されたデータを復号できるため、安全性が低くなります）。
- 一部のワイヤレス クライアント ソフトウェアでは、複数の WEP キーを設定し、クライアント ステーションの転送キー インデックスを定義できます。これにより、異なるキーを使用して送信するデータを暗号化するよう、ステーションを設定できます。その結果、近隣のアクセス ポイントが他のアクセス ポイントの送信を復号することはできなくなります。

- アクセス ポイントとクライアント ステーション間で 64 ビットと 128 ビットの WEP キーを混合することはできません。

動的 WEP

動的 WEP は、802.1x 技術と Extensible Authentication Protocol（EAP; 拡張認証プロトコル）の組み合わせを参照します。動的 WEP のセキュリティにより、WEP キーは動的に変化します。

EAP メッセージは、EAP Encapsulation Over LANs（EAPOL; LAN 上での EAP カプセル化）と呼ばれるプロトコルを使用した IEEE802.11ワイヤレス ネットワークを介して送信されます。IEEE 802.1X は動的に作成されたキーを提供し、これは定期的に更新されます。RC4 ストリーム暗号は、各 802.11 フレームのフレーム ボディの暗号化と、Cyclic Redundancy Checkin（CRC; 巡回冗長検査）のために使用されます。

このモードでは、ユーザを認証するため、外部 RADIUS サーバを使用する必要があります。WAP デバイスは、Microsoft インターネット認証サーバなど、EAP をサポートする RADIUS サーバが必要です。Microsoft Windows クライアントで動作するよう、認証サーバは Protected EAP（PEAP; 保護 EAP）と MSCHAP V2 をサポートしている必要があります。

IEEE802.1X モードがサポートするさまざまな認証方法を使用でき、これには証明書やケルベロス認証、公開鍵認証が含まれます。クライアント ステーションは、WAP デバイスが使用する認証方法と同じものを使用するよう設定する必要があります。

次のパラメータを動的 WEP に設定します。

- [グローバル RADIUS サーバ設定を使用]: デフォルトでは、各 VAP は WAP デバイスで定義した RADIUS 設定を使用します（RADIUS サーバ をご覧ください）。ただし、RADIUS サーバの異なる設定を使用するよう、各 VAP を設定することができます。

  グローバル RADIUS サーバ設定を使用するには、チェックボックスが選択されていることを確認します。

  VAP に個別の RADIUS サーバを使用するには、チェックボックスをオフにして、次のフィールドに RADIUS サーバの IP アドレスとキーを入力します。

- [サーバの IP アドレス タイプ]: RADIUS サーバが使用する IP のバージョン。

  IPv4 と IPv6 のグローバル RADIUS アドレス設定を設定するアドレス タイプを切り替えることができますが、WAP デバイスは RADIUS サーバまたはこのフィールドで選択したアドレス タイプのサーバとのみコンタクトできます。

- [サーバの IP アドレス 1] または [サーバの IPv6 アドレス 1]: この VAP のプライマリ RADIUS サーバのアドレス。

最初のワイヤレス クライアントが WAP デバイスで認証しようとすると、その WAP デバイスはプライマリ サーバに認証要求を送信します。プライマリ サーバがこの認証要求に応答した場合、WAP デバイスはこの RADIUS サーバをプライマリ サーバとして使用し続け、認証要求は指定したアドレスに送信されます。

IPv4 アドレスは、xxx.xxx.xxx.xxx（192.0.2.10）の形式にする必要があります。IPv6 アドレスは、xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx（2001:DB8::CAD5:7D91）の形式にする必要があります。

- [サーバの IP アドレス 2] から [サーバの IP アドレス 4]、または [サーバの IPv6 アドレス 2] から [サーバの IPv6 アドレス 4]：最大 3 つまでの IPv4 または IPv6 バックアップ RADIUS サーバ アドレス。

  プライマリ サーバでの認証に失敗した場合、設定された各バックアップ サーバが順番に試行されます。

- [キー]：WAP デバイスがプライマリ RADIUS サーバの認証に使用する共有秘密キー。

  最大 63 の標準英数字と特殊文字を使用できます。キーは大文字と小文字が区別され、RADIUS サーバで設定されたキーと一致している必要があります。入力するテキストはアスタリスクとして表示されます。

- [キー 2] から [キー 4]：設定されたバックアップ RADIUS サーバに関連付けられた RADIUS キー。[サーバの IP（IPv6）アドレス 2] のサーバは [キー 2] を使用し、[サーバの IP（IPv6）アドレス 3] のサーバは [キー 3] を使用するなど。

- [RADIUS アカウンティングの有効化]：特定のユーザが消費したリソース（システム時刻や送受信されたデータ量など）の追跡および測定を可能にします。

  RADIUS アカウンティングを有効にすると、プライマリ RADIUS サーバとすべてのバックアップ サーバに対して有効になります。

- [アクティブ サーバ]：WAP デバイスが設定された各サーバに順番にコンタクトを試み、アップしている最初のサーバを選択するのではなく、管理上アクティブな RADIUS サーバの選択を可能にします。

- [ブロードキャスト キー更新レート]：この VAP に関連付けられているクライアントのブロードキャスト（グループ）キーが更新される間隔。

  デフォルトは 300 です。有効な範囲は 0 ～ 86400 秒です。値 0 は、ブロードキャスト キーが更新されないことを示します。

- [セッション キー更新レート]：WAP デバイスが VAP に関連付けられている各クライアントへのセッション（ユニキャスト）を更新する間隔。

有効な範囲は 30 ～ 86400 秒です。値 0 は、セッション キーが更新されないことを示します。

WPA パーソナル

WPA パーソナルは Wi-Fi アライアンス IEEE 802.11i 標準で、これには AES-CCMP および TKIP の暗号化が含まれます。WPA パーソナル バージョンは、エンタープライズ WPA セキュリティ モードで使用されているように、IEEE 802.1X および EAP を使用する代わりに Pre-Shared Key（PSK; 事前共有キー）を使用します。PSK はクレデンシャルの最初のチェックのみに使用されます。WPA パーソナルは、WPA-PSK とも呼ばれます。

このセキュリティ モードは、オリジナルの WPA をサポートするワイヤレス クライアント用に下位互換性があります。

WPA パーソナルは、次のパラメータで構成されます。

- [WPA バージョン]：サポートするクライアント ステーションのタイプ。
  - [WPA-TKIP]：ネットワークには、オリジナルの WPA および TKIP セキュリティ プロトコルのみをサポートしているクライアント ステーションがあります。アクセスポイントに WPA-TKIP のみ選択することは、最新の WiFi アライアンス要件では許可されていません。
  - [WPA2-AES]：ネットワーク上のすべてのクライアント ステーションは WPA2 バージョンおよび AES-CCMP 暗号 / セキュリティ プロトコルをサポートします。この WPA バージョンは、IEEE802.11i 標準ごとに最適なセキュリティを提供します。最新の WiFi アライアンス要件では、AP はこのモードを常にサポートする必要があります。

  ネットワークにクライアントが混在し、一部は WPA2 をサポートし、一部はオリジナルの WPA のみサポートする場合、両方のチェックボックスをオンにします。これにより、両方の WPA と WPA2 クライアント ステーションが関連付けし、認証しますが、それをサポートするクライアントにはより堅牢な WPA2 を使用します。この WPA の設定は、セキュリティの代わりにより多くの相互運用性を可能にします。

  WAP デバイスと関連付けられるよう、WPA クライアントは次のキーのいずれか 1 つを持つ必要があります。

  - 有効な TKIP キー
  - 有効な AES-CCMP キー
- [キー]：WPA パーソナル セキュリティ用共有秘密キー。8 文字以上 63 文字以下の文字列を入力します。使用できる文字には、大文字と小文字のアルファベット、数字、および @ や # などの特殊記号が含まれます。

- [キー強度計]: WAP デバイスは、使用される文字の種類（大文字と小文字のアルファベット、数字、特殊文字）や文字列の長さなどの複雑度の基準に照らしてキーをチェックします。WPA-PSK 複雑度チェック機能が有効な場合、最低限の基準を満たしていないかぎり、キーは受け入れられません。複雑度チェックの設定情報については、「WPA-PSK 複雑性」を参照してください。
- [ブロードキャスト キー更新レート]: この VAP に関連付けられているクライアントのブロードキャスト（グループ）キーが更新される間隔。

  デフォルトは 300 秒です。有効な範囲は 0 ～ 86400 秒です。値 0 は、ブロードキャスト キーが更新されないことを示します。

WPA エンタープライズ

RADIUS を使用した WPA エンタープライズは Wi-Fi アライアンス IEEE 802.11i 標準を実装したもので、これには CCMP（AES）および TKIP の暗号化が含まれます。このエンタープライズ モードでは、ユーザを認証するため、RADIUS サーバを使用する必要があります。

このセキュリティ モードは、オリジナルの WPA をサポートするワイヤレス クライアントと下位互換性があります。

WPA エンタープライズは、次のパラメータで構成されます。

- [WPA バージョン]: サポートするクライアント ステーションのタイプ。
  - [WPA-TKIP]：ネットワークには、オリジナルの WPA および TKIP セキュリティ プロトコルのみをサポートしているクライアント ステーションがあります。アクセスポイントに WPA-TKIP のみ選択することは、最新の WiFi アライアンス要件では許可されていません。
  - [WPA2-AES]：ネットワーク上のすべてのクライアント ステーションは WPA2 バージョンおよび AES-CCMP 暗号 / セキュリティ プロトコルをサポートします。この WPA バージョンは、IEEE802.11i 標準ごとに最適なセキュリティを提供します。最新の WiFi アライアンス要件では、AP はこのモードを常にサポートする必要があります。
- [MFP（管理フレーム保護）]: これ以外では保護されず、暗号化されない 802.11 管理フレームのセキュリティを提供します。このフィールドは、WPA2 セキュリティと CCMP フィールドが有効な場合のみ表示されます。次の 3 種類の値がチェックボックスで指定できます。デフォルトは対応です。
  - 不要
  - 対応
  - 必須

- [事前認証の有効化]:WPA バージョンに WPA2 のみ、または WPA および WPA2 を選択した場合、WPA2 クライアントの事前認証が可能です。

  WPA2 ワイヤレス クライアントに事前認証パケットを送信させるためには、[事前認証の有効化] をクリックします。事前認証情報は、クライアントが現在使用している WAP デバイスから対象の WAP デバイスに伝達されます。この機能を有効にすると、複数の AP に接続するクライアントがローミングするための認証を高速化できます。

  WPA バージョンに WPA を選択した場合、オリジナルの WPA はこの機能をサポートしていないため、このオプションは適用されません。

  RADIUS と共に WPA を使用するよう設定されたクライアント ステーションは、次のアドレスおよびキーのいずれか 1 つを持つ必要があります。

  - 有効な TKIP RADIUS IP アドレスと RADIUS キー
  - 有効な CCMP（AES）IP アドレスと RADIUS キー

- [グローバル RADIUS サーバ設定を使用]:デフォルトでは、各 VAP は WAP デバイスで定義した RADIUS 設定を使用します（**RADIUS サーバ** をご覧ください）。ただし、RADIUS サーバの異なる設定を使用するよう、各 VAP を設定することができます。

  グローバル RADIUS サーバ設定を使用するには、チェックボックスが選択されていることを確認します。

  VAP に個別の RADIUS サーバを使用するには、チェックボックスをオフにして、次のフィールドに RADIUS サーバの IP アドレスとキーを入力します。

- [サーバの IP アドレス タイプ]:RADIUS サーバが使用する IP のバージョン。

  IPv4 と IPv6 のグローバル RADIUS アドレス設定を設定するアドレス タイプを切り替えることができますが、WAP デバイスは RADIUS サーバまたはこのフィールドで選択したアドレス タイプのサーバとのみコンタクトできます。

- [サーバの IP アドレス 1] または [サーバの IPv6 アドレス 1]: この VAP のプライマリ RADIUS サーバのアドレス。

  [サーバの IP アドレス タイプ] として [IPv4] を選択した場合、すべての VAP がデフォルトで使用する RADIUS サーバの IP アドレス（例: 192.168.10.23）を入力します。[IPv6] を選択した場合、プライマリ グローバル RADIUS サーバの IPv6 アドレス（例: 2001:DB8:1234::abcd）を入力します。

- [サーバの IP アドレス 2] から [サーバの IP アドレス 4]、または [サーバの IPv6 アドレス 2] から [サーバの IPv6 アドレス 4]: この VAP のバックアップ RADIUS サーバとして使用する、最大 3 つまでの IPv4 および（または）IPv6 アドレス。

プライマリ サーバでの認証に失敗した場合、設定された各バックアップ サーバが順番に試行されます。

- [キー 1]: グローバル RADIUS サーバの共有秘密キー。最大 63 の標準英数字と特殊文字を使用できます。このキーは大文字と小文字を区別し、WAP デバイスおよび RADIUS サーバで設定されているものと同じキーを設定しなければなりません。入力時に RADIUS キーを他者から見られるのを防ぐため、入力するテキストはアスタリスクで表示されます。
- [キー 2] から [キー 4]: 設定されたバックアップ RADIUS サーバに関連付けられた RADIUS キー。[サーバの IP(IPv6)アドレス 2] のサーバは [キー 2] を使用し、[サーバの IP(IPv6)アドレス 3] のサーバは [キー 3] を使用するなど。
- [RADIUS アカウンティングの有効化]: 特定のユーザが消費したリソース(システム時刻や送受信されたデータ量など)を追跡および測定します。

  RADIUS アカウンティングを有効にすると、プライマリ RADIUS サーバとすべてのバックアップ サーバに対して有効になります。
- [アクティブ サーバ]: WAP デバイスが設定された各サーバに順番にコンタクトを試み、アップしている最初のサーバを選択するのではなく、アクティブな RADIUS サーバの管理上の選択を可能にします。
- [ブロードキャスト キー更新レート]: この VAP に関連付けられているクライアントのブロードキャスト(グループ)キーが更新される間隔。

  デフォルトは 300 秒です。有効な範囲は 0 ～ 86400 秒です。値 0 は、ブロードキャスト キーが更新されないことを示します。
- [セッション キー更新レート]: WAP デバイスが VAP に関連付けられている各クライアントへのセッション(ユニキャスト)を更新する間隔。

  有効な範囲は 30 ～ 86400 秒です。値 0 は、セッション キーが更新されないことを示します。

ワイヤレス マルチキャスト転送

ワイヤレス マルチキャスト転送は、ワイヤレス メディア上のマルチキャスト トラフィックを転送するための効率的な方法を提供し、マルチキャスト フレームのユニキャストを繰り返し使用する WLAN 上のマルチキャスト送信の問題を解決します。

これは参加グループ メンバーを追跡し続けるために IGMP フレームを使用し、マルチキャスト パケットはユニキャスト MAC 変換後に、関係するメンバーにのみ送信されます。

WMF を使用すると、フレームがユニキャストとして送信されるため、データ転送の信頼性が高くなります。またリンク エラーやノイズ条件に基づき、ステーションごとに動的なレート制御が可能なため、堅牢な送信が可能になります。

マルチキャスト グループ メンバーは、STA の終点にもなります。STA デバイス間のストリーミングもサポートされます。マルチキャスト ストリーミング サーバはどの LAN ポートにも接続できます。

ワイヤレス マルチキャスト転送の設定

ワイヤレス マルチキャスト転送の設定方法:

ステップ 1 ナビゲーション ペインで、[ワイヤレス] > [ワイヤレス マルチキャスト転送] を選択します。

ステップ 2 パラメータを設定します。

- [ワイヤレス マルチキャスト転送]: Cisco WAP571/E 上でグローバルなワイヤレス マルチキャスト転送を有効または無効にします。

注 新しい設定を保存すると、対応するプロセスが停止され、再起動されることがあります。この事態が発生すると、WAP デバイスが切断される可能性があります。切断によってワイヤレス クライアントが受ける影響が最も小さい場合に、WAP デバイスの設定を変更することをお勧めします。

スケジューラ

無線と VAP スケジューラにより、VAP または無線を動作可能にするための特定の時間間隔のルールを設定でき、VAP と無線の有効化または無効化を自動化します。

この機能を使用する 1 つの方法として、セキュリティを高め、消費電力を低減するため、無線を勤務時間内のみ動作するようスケジューリングします。またスケジューラを使用し、一日の特定の時間のみ、ワイヤレス クライアントが VAP にアクセス可能にすることもできます。

AP は最大 16 プロファイルまでサポートします。有効なルールのみこのプロファイルに追加されます。最大 16 までのルールが、スケジューリング プロファイルを作成するためグループ化されます。同じプロファイルに属する定期的な時間のエントリが重複することはできません。

最大 16 のスケジューラ プロファイル名を作成できます。デフォルトでは、プロファイルは何も作成されません。

スケジューラ プロファイルの追加

スケジューラのステータスを表示し、スケジューラ プロファイルを追加する方法:

ステップ 1 ナビゲーション ペインで、[ワイヤレス] > [スケジューラ] を選択します。

ステップ 2 [管理モード] が有効であることを確認します。デフォルトでは無効です。

[スケジューラ動作ステータス] 領域には、スケジューラの現在の動作ステータスが表示されます。

- [ステータス]: スケジューラの動作ステータス。指定できるのは、[有効] または [無効] です。デフォルトは [無効] です。
- [理由]: スケジューラの動作ステータスの理由。選択項目は次のとおりです。
  - [IsActive]: スケジューラは管理上有効です。
  - [管理モードが無効]: グローバル構成が無効のため、動作ステータスがダウンしています。
  - [システム時刻が古い]: システム時刻が同期していません。

ステップ 3 プロファイルを追加するには、[スケジューラのプロファイル設定] テキストボックスにプロファイル名を入力し、[追加] をクリックします。プロファイル名は最大 32 文字の英数字です。

スケジューラ ルールの設定

プロファイルには最大 16 のルールを設定できます。各ルールでは、無線または VAP が動作可能な開始時刻、終了時刻、および曜日（または日）を指定します。ルールは本来定期的なものであり、毎週繰り返されます。有効なルールであるためには、開始時刻と終了時刻においてすべてのパラメータ（曜日、時刻、分）が含まれている必要があります。競合するルールは設定できません。たとえば、あるルールを各平日に開始するよう設定し、各週末に開始する別のルールを設定することはできますが、あるルールを毎日開始するよう設定し、週末に開始する別のルールを設定することはできません。

プロファイルのルールの設定

プロファイルのルールの設定方法:

ステップ 1 [プロファイル名の選択] リストからプロファイルを選択します。

ステップ 2 [ルールの追加] をクリックします。

新しいルールがルールの表に表示されます。

ステップ 3 [プロファイル名] の隣のチェックボックスをオンにし、[編集] をクリックします。

ステップ 4 [曜日] メニューからそのルールの定期的なスケジュールを選択します。ルールは、毎日、各平日、各週末（土曜日と日曜日）、またはある曜日に実行されるよう設定できます。

ステップ 5 開始および終了時刻を設定します。

- [開始時刻]：無線または VAP の動作が有効になる時刻。時刻はHH:MM（24時間）形式で設定します。範囲 は <00 ～ 23>:<00 ～ 59> です。デフォルトは 00:00 です。
- [終了時刻]：無線または VAP の動作が無効になる時刻。時刻はHH:MM（24時間）形式で設定します。範囲 は <00 ～ 23>:<00 ～ 59> です。デフォルトは 00:00 です。

ステップ 6 [保存] をクリックします。変更が、スタートアップ コンフィギュレーションに保存されます。

注 スケジューラ プロファイルを有効にするには、無線インターフェイスまたは VAP インターフェイスと関連付ける必要があります。[スケジューラ アソシエーション] ページを参照してください。

注 ルールを削除するには、[プロファイル名] カラムから対象のプロファイルを選択し、[削除] をクリックします。

スケジューラ ルールの範囲

ここでは、スケジューラ ルールの範囲について説明します。

- 特定の日に対してのみ設定したルールは、他の日には影響を与えません。
- 「毎日」、「平日」、または「週末」などのグループを使用するルールは、複数の日に影響を与えます。
- 「週末」に設定したルールは、土曜日と日曜日に影響を与えますが、他の日には影響を与えません。デフォルトのスケジューラの動作は、その日に無線が有効な期間を制御する明示的なルールがない場合、無線が有効になります。
- スケジューラ機能の設計は、無線や VAP が有効な場合に各ルールが境界を設定するようなものです。
- 「曜日」エントリにより、ルールの範囲を作成します。ルールは定義した範囲に対してのみ影響を与えます。週末とは土曜日と日曜日のみを指します。「毎日」とはすべての日など。ルールを設定するとき、「曜日」GUI エントリがルールの範囲（週末、毎日、平日、日曜日、月曜日など）を定義します。

- これにより、詳細なルールが可能になります。範囲に週のすべての日が含まれない場合、作成されたすべてのルールに暗黙の拒否はありません。適切な範囲をわずか 1 分に設定することで、「拒否」または「無効」ルールを作成します。明示的に許可された時刻を除き、常に無線または VAP を無効にするには、夜中から 12:01 までのわずか 1 分間だけアクティブになる「毎日」のルールが必要です。これは、無線が毎日 1 分間だけオンになることを意味します。次に、無線をアクティブにしたい時間ごとに例外を追加できます。

一般的な事例を次に示します。

- 無線を月曜日から金曜日の午前9時から午後5時まで有効にする
- 週末に有効な無線はない

2 つのルールを使用してプロファイルを作成します。

平日：開始時刻：9:00 終了時刻：17:00

週末の開始時刻：0:00 終了時刻：0:01

スケジューラ アソシエーション

スケジューラ プロファイルを有効にするには、WLAN インターフェイスまたは VAP インターフェイスと関連付ける必要があります。デフォルトでは、作成されたスケジューラ プロファイルはなく、無線または VAP と関連付けられたプロファイルもありません。

1 つのスケジューラ プロファイルのみ、WLAN インターフェイスまたは各 VAP と関連付けることができます。1 つのプロファイルを複数の VAP と関連付けることができます。VAP または WLAN インターフェイスと関連付けられたスケジューラ プロファイルを削除すると、その関連付けは削除されます。

スケジューラ プロファイルと WLAN インターフェイスまたは VAP との関連付け

スケジューラ プロファイルを WLAN インターフェイスまたは VAP と関連付ける方法：

ステップ 1 ナビゲーション ペインで、[ワイヤレス] > [スケジューラ アソシエーション] を選択します。スケジューラ プロファイルを関連付けたい [無線] インターフェイス（[無線 1] または [無線 2]）を選択します。

ステップ 2 WLAN インターフェイスまたは VAP において、[プロファイル名] リストからプロファイルを選択します。

[インターフェイスの動作ステータス] カラムに、現在インターフェイスが有効か無効かが表示されます。

ステップ 3 [保存] をクリックします。変更が、スタートアップ コンフィギュレーションに保存されます。

MAC フィルタリング

Media Access Control（MAC; メディア アクセス制御）フィルタリングを使用して、リストされたクライアント ステーションのみ、アクセス ポイントでの認証を除外または許可することができます。MAC 認証は [ネットワーク] ページの VAP ごとに有効または無効にします。VAP の設定により、WAP デバイスは、外部 RADIUS サーバに保存された MAC フィルタ リストを参照するか、WAP デバイスにローカルで保存された MAC フィルタ リストを参照します。

MAC フィルタ リストを WAP デバイスにローカルで設定

WAP デバイスは 1 つのローカル MAC フィルタのみサポートします。つまり、ローカル リストの使用が有効になっているすべての VAP に同一のリストが適用されます。フィルタは、リスト上の MAC アドレスのみアクセスを許可する、またはリスト上のアドレスのみアクセスを拒否するよう、設定できます。

フィルタ リストには最大 512 の MAC アドレスを追加できます。

MAC フィルタリングの設定

MAC フィルタリングの設定方法:

ステップ 1 ナビゲーション ペインで、[ワイヤレス] > [MAC フィルタリング] を選択します。

ステップ 2 WAP デバイスのフィルタ リストの使用方法を選択します。

- [リスト上のステーションのみ許可]: ステーション リストにないステーションはすべて、WAP デバイスを介したネットワークへのアクセスを拒否されます。
- [リスト上のステーションをブロック]: リストにあるステーションのみ、WAP デバイスを介したネットワークへのアクセスを拒否されます。その他のステーションはアクセスを許可されます。

注 フィルタ設定は、RADIUS サーバ（存在する場合）上に保存された MAC フィルタリング リストにも適用されます。

ステップ 3 [MAC アドレス] フィールドに許可またはブロックする MAC アドレスを入力し、[追加] をクリックします。

その MAC アドレスが [ステーション リスト] に表示されます。

ステップ 4 リストが完成するまで MAC アドレスの入力を続け、[保存] をクリックします。変更が、スタートアップ コンフィギュレーションに保存されます。

注 MAC アドレスをステーション リストから削除するには、対象をを選択し、[削除] をクリックします。

注 新しい設定を保存すると、対応するプロセスが停止され、再起動されることがあります。この事態が発生すると、WAP デバイスが切断される可能性があります。切断によってワイヤレス クライアントが受ける影響が最も小さい場合に、WAP デバイスの設定を変更することをお勧めします。

RADIUS サーバ上での MAC 認証の設定

1 つ以上の VAP において、RADIUS 認証サーバに保存された MAC フィルタを使用するよう設定する場合、その RADIUS サーバにステーション リストを設定する必要があります。リストの形式は次の表に示すとおりです。

RADIUS サーバ認証	説明	値
User-Name (1)	クライアント ステーションの MAC アドレス。	有効なイーサネット MAC アドレス。
User-Password (2)	クライアント MAC エントリを検索するために使用する固定のグローバル パスワード。	NOPASSWORD

ブリッジ

ここでは、2 種類のブリッジについて説明します。具体的な内容は次のとおりです。

WDS ブリッジ

Wireless Distribution System（WDS; ワイヤレス配信システム）は複数の WAP571/E デバイスの接続を可能にします。WDS を使用すると、アクセス ポイントは無線で互いに通信できます。この機能は、ローミング クライアントにシームレスな体験を提供するため、また複数のワイヤレス ネットワークを管理するために重要です。また必要なケーブリング量を減らすことで、ネットワーク インフラストラクチャを簡素化できます。WAP デバイスを、接続するリンクの数に基づき、ポイントツーポイントまたはポイントツーマルチポイントのブリッジ モードで設定できます。

ポイントツーポイント モードでは、WAP デバイスはクライアントの関連付けを受け入れ、ワイヤレス クライアントや他のリピータと通信します。WAP デバイスは、アクセス ポイント間に確立されたトンネルを介した他のネットワーク向けのすべてのトラフィックを転送します。ブリッジはホップ カウントには追加されません。これはシンプルな OSI レイヤ 2 ネットワーク デバイスとして動作します。

ポイントツーマルチポイントのブリッジ モードでは、WAP デバイスは複数のアクセス ポイント間の共通リンクとして機能します。このモードでは、中央の WAP デバイスはクライアントの関連付けを受け入れ、クライアントや他のリピータと通信します。他のすべてのアクセス ポイントは、ルーティング目的でパケットを適切なワイヤレス ブリッジに転送する中央の WAP デバイスとのみ関連付けられます。

AP はリピータとしても機能します。このモードでは、AP はセル範囲内で非常に離れている 2 つの AP 間の接続として機能します。リピータとして機能する場合、AP は LAN への有線接続を持たず、ワイヤレス接続を使用して信号を繰り返します。AP がリピータとして機能するために必要な特別な設定はなく、リピータ モードの設定もありません。それでもワイヤレス クライアントは、リピータとして動作している WAP デバイスに接続することができます。

WAP デバイス上で WDS を設定する前に、次のガイドラインに注意してください。

- クライアントの関連付けを許可しない純粋なブリッジング モードでは、VAP0 に曖昧な WPA キーを使用するか、SSID ブロードキャストを無効にすることを推奨します。
- WDS リンクに参加するすべての Cisco WAP デバイスでは、次の同一の設定をする必要があります。
  - 無線
  - IEEE 802.11 モード
  - チャネル帯域幅
  - チャネル（自動を推奨）

注 802.11n 2.4 GHz 帯域でブリッジングが動作する場合、チャネル帯域幅をデフォルトの 20/40 MHz ではなく、20 MHz に設定します。2.4 GHz 20/40 MHz 帯域の場合、そのエリアで 20 MHz WAP デバイスが検出された場合、動作帯域幅が 40 MHz から 20 MHz に変化する場合があります。チャネル帯域幅の不一致は、リンクが切断される原因となります。

これらの設定情報については、「無線」(基本設定)を参照してください。

- WDS を使用する場合、WDS リンクに参加する両方の WAP デバイスに WDS を設定してください。
- WDS リンクは、WAP デバイスのいずれかのペア間でただ 1 つだけ設定できます。つまりリモート MAC アドレスは、ある WAP デバイスの WDS ページに 1 度だけ表示されます。

WDS ブリッジの設定方法:

ステップ 1 ナビゲーション ペインで、[ワイヤレス] > [ブリッジ] を選択します。

ステップ 2 ドロップダウンの選択肢から WDS ブリッジを選択します。

ステップ 3 設定したい [WDS インターフェイス] において、[有効化] にチェックします。

ステップ 4 その他のパラメータの設定:

- [リモート MAC アドレス]:宛先 WAP デバイスの MAC アドレス、つまりデータが送信または中継される宛先、またはデータ送信元の WDS リンクのもう一端の WAP デバイスを指定します。

ヒント [ステータスと統計] > [ネットワーク インターフェイス] ページで MAC アドレスを検索できます。

- [暗号化]:WDS リンクで使用する暗号化のタイプで、ブリッジングする VAP と一致させる必要はありません。WDS 暗号化設定は WDS ブリッジにおいて一意です。オプションは、なし、WEP、WPA パーソナルです。WPA2-PSK は WDS リンクの暗号化および VAP セキュリティのオプションの 1 つです。それらを実行するには、管理者がそれらのオプションを選択する必要があります。

  WDS リンク上のセキュリティ問題について懸念がない場合、いずれのタイプの暗号化も設定しないことも可能です。またはセキュリティ上の懸念がある場合、静的 WEP または WPA パーソナルを選択できます。WPA パーソナル モードでは、WAP デバイスは、WDS リンク上で CCMP(AES)暗号化と共に WPA2-PSK を使用します。この手順に続き、暗号化オプションの詳細については、**WDS リンク上の WEP** または **WDS リンク上の WPA/PSK** を参照してください。

注 静的 WEP は、無線がレガシー モード(5 GHz 無線の場合 802.11a および 2.4 GHz 無線の場合 802.11b/g)で動作する場合のみ適用できます。

ステップ 5 [保存] をクリックします。変更が、スタートアップ コンフィギュレーションに保存されます。

ステップ 6 他のデバイスまたはこのブリッジに接続されているデバイスについても、この手順を繰り返します。

ヒント [ステータスと統計] > [ネットワーク インターフェイス] ページで、ブリッジ リンクがアップしていることを確認できます。インターフェイス ステータス表では、WLAN0:WDS(x) ステータスには、ステータスがアップと表示されます。

注 リモート ネットワークのパートナー WDS AP は、WDS リンクが切断された場合でも、その管理 IP アドレスをメイン ネットワーク内の WDS AP に接続された DHCP サーバから取得し、保持します。WDS インターフェイスが管理上ダウンすると、IP アドレスは解放されます。

注意 新しい設定を保存すると、対応するプロセスが停止され、再起動されることがあります。この事態が発生すると、WAP デバイスが切断される可能性があります。切断によってワイヤレス クライアントが受ける影響が最も小さい場合に、WAP デバイスの設定を変更することをお勧めします。

WDS リンク上の WEP

暗号化タイプとして WEP を選択すると、これらの追加のフィールドが表示されます。

- [キー長]: WEP が有効な場合、WEP キーの長さを **64 ビット** または **128 ビット** で指定します。
- [キー タイプ]: WEP が有効な場合、WEP キーのタイプを指定します（[ASCII] または [Hex:]）。
- [WEP キー]: [ASCII] を選択した場合、0 から 9、a から z、および A から Z の任意の組み合わせを入力します。[Hex] を選択した場合、16進数（0 から 9、および A から F の任意の組み合わせ）を入力します。これらは WAP デバイスを使ってステーションと共有される RC4 暗号化キーです。

  必要な文字数がこのフィールドの右側に表示され、選択した [キータイプ] および [キー長] フィールドに基づき変化します。

WDS リンク上の WPA/PSK

暗号化タイプとして WPA/PSK を選択すると、これらの追加のフィールドが表示されます。

- [WDS ID]: 作成した新規 WDS リンクに適切な名前を入力します。WDS リンクの他端にも同じ WDS ID が入力されていることが重要です。この WDS ID が

WDS リンク上の両方の WAP デバイスで同じでない場合、お互いに通信し、データを交換することはできません。

WDS ID は任意の英数字の組み合わせを指定できます。

- [キー]:WDS ブリッジの一意の共有キーを入力します。この一意の共有キーは、WDS リンクの他端の WAP デバイスにも入力する必要があります。このキーが両方の WAP で同じでない場合、お互いに通信し、データを交換することはできません。

  WPA-PSK キーは、8 文字以上 63 文字以下の文字列です。使用できる文字には、大文字と小文字のアルファベット、数字、および @ や # などの特殊記号が含まれます。

ワークグループ ブリッジ

AP ワークグループ ブリッジ機能は、WAP デバイスがリモート ネットワークのアクセシビリティを拡張できるようにします。ワークグループ ブリッジ モードでは、AP はワイヤレス LAN 上のワイヤレス ステーション(STA)として機能します。これにより、リモートの有線ネットワークと、ワークグループ ブリッジ モードで接続されているワイヤレス LAN 間のトラフィックをブリッジすることができます。

ワークグループ ブリッジ機能は STA モードのサポートを可能にします。WAP デバイスは、Basic Service Set(BSS; 基本サービスセット)上で STA デバイスとして動作することができます。ワークグループ ブリッジ モードを有効にすると、AP は、AP がワイヤレス クライアントとして関連付ける 1 つの BSS のみサポートします。

ワークグループ ブリッジ モードは、WDS ブリッジ機能がピア AP で動作できない場合にのみ使用することを推奨します。WDS はより優れたソリューションであり、ワークグループ ブリッジ ソリューションよりも推奨されます。Cisco WAP571/E デバイスをブリッジングする場合、WDS を使用します。それ以外の場合、ワークグループ ブリッジを検討します。ワークグループ ブリッジ機能を有効にすると、VAP 設定は適用されず、ワークグループ ブリッジの設定のみが適用されます。

注 ワークグループ ブリッジ モードが AP で有効になっている場合、WDS 機能は動作しません。

ワークグループ ブリッジ モードでは、WPA デバイスによって管理される BSS(つまり WAP デバイスが STA として関連付けるもの)はインフラストラクチャ クライアント インターフェイスと呼ばれ、他の WAP デバイスはアップストリーム AP と呼ばれます。

WAP デバイスの有線インターフェイスに接続されたデバイスは、インフラストラクチャ クライアント インターフェイスによって接続されたネットワークにアクセスすることができます。

WAP デバイス上でワークグループ ブリッジを設定する前に、次のガイドラインに注意してください。

- ワークグループ ブリッジに参加するすべての WAP デバイスでは、次の同一の設定をする必要があります。
  - 無線
  - IEEE 802.11 モード
  - チャネル帯域幅
  - チャネル（自動を推奨）

  これらの設定情報については、「無線」(基本設定)を参照してください。
- ワークグループ ブリッジは現在、IPv4 トラフィックのみサポートしています。
- ワークグループ ブリッジ モードはシングル ポイント設定ではサポートされていません。

ワークグループ ブリッジ モードの設定方法:

ステップ 1 ナビゲーション ペインで、[ワイヤレス] > [ブリッジ] を選択します。

ステップ 2 ドロップダウンの選択肢から [ワークグループ ブリッジ モード] を選択します。

ステップ 3 [ワークグループ ブリッジ モード] において [有効化] を選択します。

ステップ 4 ワークグループ ブリッジ モードを設定したい無線インターフェイス([無線 1] または [無線 2])を選択します。

ステップ 5 次のパラメータをインフラストラクチャ クライアント インターフェイス(アップストリーム)に設定します。

- [SSID]:BSS の SSID。

注 SSID スキャニング用に [SSID] の隣に矢印があります。この機能はデフォルトでは無効になっていて、[不正 AP 検出](これもデフォルトでは無効)で [AP 検出] が有効になっている場合のみ有効になります。

- [セキュリティ]:アップストリーム WAP デバイスのクライアント ステーションとしての認証に使用するセキュリティのタイプ。次のいずれかから選択します。
  - なし
  - 静的 WEP
  - WPA パーソナル

- WPA エンタープライズ

- [VLAN ID]：BSS に関連付けられる VLAN。

注 インフラストラクチャ クライアント インターフェイスは、設定されたクレデンシャルと共に、アップストリーム WAP デバイスに関連付けられます。WAP デバイスは、アップストリーム リンク上の DHCP サーバから IP アドレスを取得できます。または、静的 IP アドレスを割り当てることができます。[接続ステータス] フィールドには、WAP がアップストリーム WAP デバイスに接続されているかどうかを示します。[更新] ボタンをクリックし、最新の接続ステータスを表示できます。

WGB AP（AP がアップストリーム AP へのクライアントとして動作）は、アップストリーム AP から関連付けを解除された場合でも、その管理 IP アドレスをアップストリーム DHCP サーバから取得し、保持します。

注 静的 WEP は、無線がレガシー モード（5 GHz 無線の場合 802.11a および 2.4 GHz 無線の場合 802.11b/g ）で動作する場合のみ適用できます。

QoS

サービス品質（QoS）設定は、Voice-over-IP（VoIP）やその他のタイプのオーディオ、ビデオ、ストリーミング メディア、従来の IP データなどの差別化されたワイヤレス トラフィックを処理する際に、最適化されたスループットとより良いパフォーマンスを実現する送信キューを設定する機能を提供します。

AP に QoS を設定するには、送信キューにさまざまなタイプのワイヤレス トラフィックのパラメータを設定し、（コンテンション ウィンドウを介した）送信時の最小待機時間および最大待機時間を指定します。

WAP Enhanced Distributed Channel Access（EDCA; 改善された分散型チャネルアクセス）パラメータは、WAP デバイスからクライアント ステーションへのトラフィックの流れに影響を与えます。

静的 EDCA パラメータは、クライアント ステーションから WAP デバイスへのトラフィックの流れに影響を与えます。

通常の使用では、WAP デバイスとステーション EDCA のデフォルト値は変更する必要はありません。これらの値を変更すると、提供される QoS に影響を与えます。

WAP デバイスとステーション EDCA パラメータの設定

WAP デバイスとステーション EDCA パラメータの設定方法:

ステップ 1 **ナビゲーション ペインで、[ワイヤレス] > [QoS] を選択します。**QoS を設定する無線インターフェイス([無線 1] または [無線 2])を選択します。

ステップ 2 [EDCA テンプレート] リストからオプションを 1 つ選択します。

- [WFA デフォルト]:WAP デバイスとステーション EDCA パラメータを WiFi アライアンスのデフォルト値(通常の混合トラフィックでは最適)と共にポピュレートします。
- [音声用に最適化]:WAP デバイスとステーション EDCA パラメータを音声トラフィックに最適な値と共にポピュレートします。
- [カスタム]:カスタム EDCA パラメータの選択を可能にします。

これらの 4 つのキューは、WAP からステーションに送信されるさまざまなデータ タイプ用に定義されています。[カスタム] テンプレートを選択した場合、キューを定義するパラメータは設定可能です。それ以外の場合、選択に合わせた、事前に定義された値が設定されます。4 つのキューは以下のとおりです。

- [データ 0(音声)]:優先度の高いキューで遅延は最小。VoIP やストリーミング メディアなどの時間的制約のあるデータは、自動的にこのキューに送信されます。
- [データ 1(ビデオ)]:優先度の高いキューで遅延は最小。時間的制約のあるビデオ データは、自動的にこのキューに送信されます。
- [データ 2(ベスト エフォート)]:中程度の優先度のキューで、中程度のスループットと遅延。従来の IP データのほとんどは、このキューに送信されます。
- [データ 3(バックグラウンド)]:優先度の最も低いキューで、高いスループット。最大のスループットを必要とし、時間的制約のないバルク データ(FTP データなど)は、このキューに送信されます。

ステップ 3 次の EDCA およびステーション EDCA パラメータを設定します。

注 これらのパラメータは、前の手順で [カスタム] を選択した場合のみ設定可能です。

- [調停フレーム間スペース]:データ フレームの待機時間。待機時間はスロットで測定します。AIFS の有効な値は 1 ～ 255 です。
- [最小コンテンション ウィンドウ]:送信を再試行するための初期のランダム バックオフ待機時間(ウィンドウ)を定義するアルゴリズムへの入力。

  この値は、初期のランダム バックオフ待機時間の定義範囲の上限(ミリ秒)です。

  最初に生成されるランダムな数字は、0 とここで指定する数字の間の数字です。

データ フレームが送信される前に、ランダム バックオフ待機時間が期限切れになった場合、リトライ カウンタが増え、ランダム バックオフ値（ウィンドウ）が倍になります。ランダム バックオフ値が [最大コンテンション ウィンドウ] で定義された数に達するまで、倍増され続けます。

有効な値は、1、3、7、15、31、63、127、255、511、または 1023 です。この値は、[最大コンテンション ウィンドウ] の値よりも小さくなければなりません。

- [最大コンテンション ウィンドウ]: ランダム バックオフ値の倍増の上限（ミリ秒）。この倍増は、データ フレームが送信されるか、[最大コンテンション ウィンドウ] の上限に達するまで継続されます。

  [最大コンテンション ウィンドウ] の上限に達すると、最大再試行可能回数に達するまで再試行を続行します。

  有効な値は、1、3、7、15、31、63、127、255、511、または 1023 です。この値は、[最小コンテンション ウィンドウ] の値よりも大きくなければなりません。

- [最大バースト]（WAP のみ）: WAP からクライアント ステーションに流れるトラフィックのみに適用される WAP EDCAパラメータ。

  この値は、ワイヤレス ネットワーク上で可能なパケット バーストの最大バースト長（ミリ秒）を指定します。パケットバーストは、ヘッダー情報なしで送信される複数のフレームの集合体です。オーバーヘッドの低減によって、より高いスループットとより優れたパフォーマンスを実現します。

  有効な値は 0.0 ～ 999 です。

- [Wi-Fi マルチメディア（WMM）]: Wi-Fi MultiMedia（WMM; Wi-Fi マルチメディア）拡張を有効にするには、[有効化] を選択します。このフィールドはデフォルトで有効になっています。WMM を有効にすると、QoS の優先順位付けとワイヤレス メディア アクセスの整合がオンになります。WMM を有効にすると、AP 上の QoS 設定は、WAP デバイスからクライアント ステーションに流れるダウンストリーム トラフィック（AP EDCA パラメータ）、およびステーションから AP に流れるアップストリーム トラフィック（ステーション EDCA パラメータ）を制御します。

  WMM を無効にすると、QoS は、ステーションから WAP デバイスに流れるアップストリーム トラフィックのステーション EDCA パラメータを制御します。WMM を無効にしても、WAP デバイスからクライアント ステーションに流れるダウンストリーム トラフィックのパラメータ（AP EDCA パラメータ）を設定できます。

- [TXOP 制限]（ステーションのみ）: TXOP 制限はステーション EDCA パラメータで、クライアント ステーションから WAP デバイスに流れるトラフィックにのみ適用されます。Transmission Opportunity（TXOP; 送信機会）は、WME クラ

イアント ステーションが WAP デバイス向けの Wireless Medium（WM; ワイヤレス メディア）への送信を開始する権限を持っている場合の時間間隔（ミリ秒）です。TXOP 制限の最大値は 65535 です。

ステップ 4 次の追加設定を行います。

- [確認応答なし]: サービス クラス値として QosNoAck を持つフレームに WAP デバイスが確認応答すべきでないことを指定するには、[有効化] を選択します。
- [スケジュールされていない自動節電配信]: 電力管理方法である APSD を有効にするには、[有効化] を選択します。APSD は、VoIP 電話が WAP デバイスを介してネットワークにアクセスする場合に、推奨します。

ステップ 5 [保存] をクリックします。変更が、スタートアップ コンフィギュレーションに保存されます。

注意 新しい設定を保存すると、対応するプロセスが停止され、再起動されることがあります。この事態が発生すると、WAP デバイスが切断される可能性があります。切断によってワイヤレス クライアントが受ける影響が最も小さい場合に、WAP デバイスの設定を変更することをお勧めします。

6

スペクトラム アナライザ

ここでは、AP デバイスのスペクトラム アナライザ機能について説明します。

スペクトラム アナライザ

スペクトラム解析機能によって、ワイヤレス ネットワークのリアルタイム管理で、無線周波数(RF)環境を広範囲にモニタリングできるようになります。また、ワイヤレス ネットワーク管理者は、RF 環境に関するリアルタイムの情報と過去の情報の両方を確認できます。

スペクトラム解析では、非 Wi-Fi 干渉について 2.4 GHz および 5 GHz 周波数帯ですべての IEEE 802.11 チャネルをスキャンしたり、干渉を分類したり、ネットワークの末端でローカル イベント ログに干渉イベントを記録したりすることができます。

注 スペクトラム アナライザは、アナログ コードレス電話、ワイヤレス ビデオ カメラ、電子レンジ、S バンド モーション ディレクタ、ナローバンド ジャマー、ワイドバンド ジャマー、不明干渉源などの干渉を記録できます。

[スペクトラム アナライザ] ページには、スペクトラム アナライザ機能のステータスとスペクトラム データを表示するためのリンクが示されます。

スペクトラム アナライザの設定

スペクトラム アナライザを設定するには

ステップ 1 ナビゲーション ペインで、[スペクトラム アナライザ] を選択します。

ステップ 2 スペクトラム解析モードのステータス。このステータスは、[専用スペクトラム アナライザ]、[ハイブリッド スペクトラム アナライザ(Hybrid Spectrum Analyzer)]、または

[無効] のいずれかです。デフォルトは [無効] です。スペクトラム アナライザが一度にサポートする無線は 1 つのみです。

注 専用モードでは、10 % 以上の時間でスペクトラム解析に無線が使用されるため、クライアント接続は機能するとしても保証はされません。ハイブリッド モードでは、クライアント接続が保証されますが、スループットの低下が予想されます。

ステップ 3 [保存] をクリックします。変更が、スタートアップ コンフィギュレーションに保存されます。

ステップ 4 スキャン モードが [専用スペクトラム アナライザ] または [ハイブリッド スペクトラム アナライザ(Hybrid Spectrum Analyzer)] に設定されている場合、[スペクトラム データの表示(View Spectrum Data)] ボタンをクリックしてスペクトラム ビューアを起動します。

注 スペクトラム ビューアには、IPv4 アドレスでのみアクセスできます。

7

システム セキュリティ

ここでは、AP デバイスのセキュリティ設定方法について説明します。

具体的な内容は次のとおりです。

- RADIUS サーバ
- 802.1X サプリカント
- パスワードの複雑性
- WPA-PSK 複雑性

RADIUS サーバ

複数の機能で、RADIUS 認証サーバと通信する必要があります。たとえば、AP の Virtual Access Point（VAP; 仮想アクセス ポイント）を設定すると、ワイヤレス クライアント アクセスを制御するセキュリティ方法を設定できます（[無線] ページを参照）。ダイナミック WEP および WPA エンタープライズのセキュリティ方法では、外部の RADIUS サーバを使用してクライアントを認証します。クライアント アクセスがリストに限定されている場合、RADIUS サーバを使用してアクセスを制御するように MAC アドレス フィルタリング機能を設定することもできます。キャプティブ ポータル機能もクライアントの認証に RADIUS を使用します。

[RADIUS サーバ] ページを使用して、これらの機能で使用する RADIUS サーバを設定できます。グローバルに使用可能な IPv4 または IPv6 RADIUS サーバを最大 4 つ設定できます。ただし、グローバル サーバに対して RADIUS クライアントが IPv4 または IPv6 モードのどちらで動作するのかを選択する必要があります。1 台のサーバは必ずプライマリとして機能し、その他はバックアップ サーバとして機能します。

注 グローバル RADIUS サーバを使用する以外に、特定の RADIUS サーバ セットを使用するように各 VAP を設定することもできます。[ネットワーク]ページを参照してください。

グローバル RADIUS サーバの設定

グローバル RADIUS サーバを設定するには

ステップ 1 ナビゲーション ペインで、[システム セキュリティ] > [RADIUS サーバ] の順に選択します。

ステップ 2 パラメータを入力します。

- [サーバの IP アドレス タイプ]:RADIUS サーバが使用する IP のバージョン。

  アドレス タイプを切り替えて IPv4 および IPv6 グローバル RADIUS アドレスを設定できますが、WAP デバイスはこのフィールドで選択したアドレス タイプの RADIUS サーバにのみアクセスします。

- [サーバの IP アドレス 1] または [サーバの IPv6 アドレス 1]:プライマリ グローバル RADIUS サーバのアドレス。

  最初のワイヤレス クライアントが WAP デバイスで認証を試行するときに、デバイスはプライマリ サーバに認証要求を送信します。プライマリ サーバが認証要求に応答する場合、WAP デバイスは引き続きこの RADIUS サーバをプライマリ サーバとして使用し、認証要求は指定アドレスに送信されます。

- [サーバの IP アドレス(2 ～ 4)] または [サーバの IPv6 アドレス(2 ～ 4)]:最大 3 つのバックアップ IPv4 または IPv6 RADIUS サーバ アドレス。

  プライマリ サーバでの認証に失敗した場合、設定された各バックアップ サーバが順番に試行されます。

- [キー 1]:WAP デバイスがプライマリ RADIUS サーバでの認証に使用する共有秘密キー。

  1 ～ 64 文字の標準的な英数字と特殊文字を使用できます。キーは大文字と小文字が区別され、RADIUS サーバで設定されたキーと一致している必要があります。入力したテキストは、アスタリスクで表示されます。

- [キー(2 ～ 4)] :設定済みのバックアップ RADIUS サーバに関連付けられた RADIUS キー。[サーバの IP(IPv6)アドレス 2] のサーバは [キー 2] を使用し、[サーバの IP (IPv6)アドレス 3] のサーバは [キー 3] を使用します。以降も同様です。

- [RADIUS アカウンティングの有効化]:特定のユーザが消費したリソース(システム時刻や送受信されたデータ量など)の追跡および測定を可能にします。

  RADIUS アカウンティングを有効にすると、プライマリ RADIUS サーバとすべてのバックアップ サーバに対して有効になります。

ステップ 3 [保存] をクリックします。変更が、スタートアップ コンフィギュレーションに保存されます。

802.1X サプリカント

IEEE 802.1X 認証によって、アクセス ポイントは安全な有線ネットワークにアクセスできるようになります。アクセス ポイントを有線ネットワーク上で 802.1X サプリカント（クライアント）として有効化できます。アクセス ポイントが 802.1X を使用して認証できるように、MD5 アルゴリズムを使用して暗号化されたユーザ名とパスワードを設定できます。

IEEE 802.1X ポートベースのネットワーク アクセス制御を使用するネットワークでは、802.1X オーセンティケータがアクセスを許可するまでサプリカントはネットワークにアクセスできません。ネットワークで 802.1X が使用されている場合は、オーセンティケータに提供できるように、WAP デバイスで 802.1X 認証情報を設定する必要があります。

[802.1X サプリカント] ページは、[サプリカント設定]、[証明書ファイルのステータス]、[証明書ファイルのアップロード] の 3 つのエリアに分かれています。

[サプリカント設定] エリアでは、802.1X の動作ステータスの設定と基本設定を行うことができます。

802.1X サプリカントの設定

802.1X サプリカントを設定するには

ステップ 1 ナビゲーション ペインで、[システム セキュリティ] > [802.1X サプリカント] の順に選択します。

ステップ 2 [更新] をクリックして、証明書ファイルのステータスを更新します。

ステップ 3 パラメータを入力します。

- [管理モード]：802.1X サプリカント機能を有効にします。
- [EAP 方法]：認証ユーザ名とパスワードの暗号化に使用するアルゴリズム。
  - [MD5]：基本的なセキュリティを提供する RFC 3748 で定義されたハッシュ関数。
  - [PEAP]：Protected Extensible Authentication Protocol（保護された拡張認証プロトコル）。TLS トンネル内で暗号化することで、MD5 よりも高いレベルのセキュリティを提供します。
  - [TLS]：Transport Layer Security（トランスポート レイヤ セキュリティ）。RFC 5216 で定義されているように、高レベルのセキュリティを提供するオープン標準です。

- [ユーザ名]：WAP デバイスは、802.1X オーセンティケータからの要求に応答する際にこのユーザ名を使用します。ユーザ名の長さは、1 ～ 64 文字にすることができます。大文字および小文字のアルファベット、数字、および引用符を除くすべての特殊文字を含む、ASCII 印刷可能文字を使用できます。
- [パスワード]：WAP デバイスは、802.1X オーセンティケータからの要求に応答する際にこの MD5 パスワードを使用します。パスワードの長さは、1 ～ 64 文字にすることができます。大文字および小文字のアルファベット、数字、および引用符を除くすべての特殊文字を含む、ASCII 印刷可能文字を使用できます。

注 EAP-TLS モードでは、WAP デバイスは、802.1X オーセンティケータからの要求に応答する際にこの ID を使用します。WAP デバイスは PEM 形式の証明書ファイルをサポートしています。証明書ファイルには、秘密キーとルート証明書が含まれている必要があります。WAP デバイスでは、この証明書ファイルはパスワードで保護されたファイルでなければなりません。WAP デバイスは、秘密キー パスワードを使用してこの証明書ファイルのロックを解除します。

ステップ 4 [保存] をクリックします。変更が、スタートアップ コンフィギュレーションに保存されます。

注 新しい設定を保存すると、対応するプロセスが停止され、再起動されることがあります。この事態が発生すると、WAP デバイスが切断される可能性があります。切断によってワイヤレス クライアントが受ける影響が最も小さい場合に、WAP デバイスの設定を変更することをお勧めします。

[証明書ファイルのステータス] エリアに、現在、証明書が存在するかどうかが表示されます。

- [証明書ファイルあり]：HTTP SSL 証明書ファイルが存在するかどうかが表示されます。存在する場合は [あり] と表示されます。デフォルト設定は [なし] です。
- [証明書の失効日]：HTTP SSL 証明書ファイルの有効期限が表示されます。範囲は有効日です。

AP への証明書ファイルのアップロード

[証明書ファイルのアップロード] エリアで、AP に証明書ファイルをアップロードできます。

ステップ 1 [転送方法] で、[HTTP] または [TFTP] のいずれかを選択します。

ステップ 2 [HTTP] を選択した場合は、[参照] をクリックしてファイルを選択します。

注 HTTP サーバおよび HTTPS サーバを設定するには、「**HTTP/HTTPS サービス**」を参照してください。

[TFTP] を選択した場合は、[ファイル名] と [TFTP サーバの IPv4 アドレス] を入力します。ファイル名に、スペース、<、>、|、\、:、(、)、&、;、#、?、*、および 2 つ以上の連続したピリオドを使用することはできません。

ステップ 3 [アップロード] をクリックします。

確認ウィンドウが表示され、経過表示バーでアップロードのステータスが示されます。

パスワードの複雑性

WAP デバイスの設定ユーティリティへのアクセスに使用するパスワードの複雑性要件を設定できます。パスワードを複雑にするとセキュリティが向上します。

パスワードの複雑性要件の設定

パスワードの複雑性要件を設定するには

ステップ 1 ナビゲーション ペインで、[システム セキュリティ] > [パスワードの複雑性] の順に選択します。

ステップ 2 [パスワードの複雑性] 設定で、[有効] を選択します。

ステップ 3 次のパラメータを設定します。

- [パスワードの最小文字クラス]: パスワード文字列で表す必要がある文字クラスの最小数。使用可能な 4 つの文字クラスは、大文字、小文字、数字、標準キーボードで使用可能な特殊文字です。
- [現在とは別のパスワード]: 現在のパスワードの有効期限が切れたときに、別のパスワードを入力するために選択します。選択しなければ、有効期限が切れたときに同じパスワードを再入力できます。
- [最大パスワード長]: パスワード文字数の最大長は、64 ～ 80 の範囲です。デフォルトは 64 です。
- [最小パスワード長]: パスワード文字数の最小長は、0 ～ 32 の範囲です。デフォルトは 8 です。
- [パスワード エージングのサポート]: 設定した期間後にパスワードの有効期限が切れるようにする場合に選択します。
- [パスワード エージング時間]: 新しく作成したパスワードの有効期限が切れるまでの日数（1 ～ 365）。デフォルトは 180 日です。

ステップ 4 [保存] をクリックします。変更が、スタートアップ コンフィギュレーションに保存されます。

WPA-PSK 複雑性

WAP デバイスで VAP を設定すると、クライアントを安全に認証する方法を選択できます。VAP のセキュリティ方法として WPA Personal プロトコル（WPA 事前共有キーまたは WPA-PSK とも呼ばれる）を選択すると、[WPA-PSK 複雑性] ページを使用して認証プロセスで使用するキーの複雑性要件を設定できます。キーを複雑にするほどセキュリティが向上します。

WPA-PSK 複雑性の設定

WPA-PSK 複雑性を設定するには

ステップ 1 ナビゲーション ペインで、[システム セキュリティ] > [WPA-PSK 複雑性] の順に選択します。

ステップ 2 [WPA-PSK 複雑性] 設定の [有効] をクリックして、設定した基準に対して WAP デバイスが WPA-PSK キーを確認するようにします。このボックスを選択しなければ、次の設定は使用されません。[WPA-PSK 複雑性] は、デフォルトでは無効です。

ステップ 3 次のパラメータを設定します。

- [WPA-PSK の最小文字クラス]: キー文字列で表す必要がある文字クラスの最小数。使用可能な 4 つの文字クラスは、大文字、小文字、数字、標準キーボードで使用可能な特殊文字です。デフォルトは 3 です。
- [現在とは別の WPA-PSK]: 次のいずれかのオプションを選択します。
  - [有効]: 現在のキーの有効期限が切れた後に別のキーを設定する必要があります。
  - [無効]: 現在のキーの有効期限が切れた後に古いキーまたは以前のキーを使用できます。
- [WPA-PSK の最大長]: キーの文字数の最大長は 32 ～ 63 です。デフォルトは 63 です。
- [WPA-PSK の最小長]: キーの文字数の最小長は 8 ～ 16 です。デフォルトは 8 です。ボックスを選択すると、フィールドが編集可能になり、この要件が有効になります。

ステップ 4 [保存] をクリックします。変更が、スタートアップ コンフィギュレーションに保存されます。

8

クライアント QoS

ここでは、クライアント サービス品質（QoS）の概要と、クライアント QoS メニューから使用できる QoS 機能について説明します。具体的な内容は次のとおりです。

- グローバル設定
- クラス マップ
- ポリシー マップ
- クライアント QoS アソシエーション
- クライアント QoS ステータス

グローバル設定

クライアント QoS の [グローバル設定] ページを使用して、WAP デバイスのサービス品質を有効または無効にすることができます。

[クライアント QoS] を無効にすると、レート制限および DiffServ 設定はグローバルに無効になります。

このモードを有効にすると、特定の VAP またはイーサネットでもクライアント QoS モードを有効または無効にすることができます。[クライアント QoS アソシエーション] ページの [クライアント QoS モード] 設定を参照してください。

クラス マップ

QoS 機能には、差別化サービス（DiffServ）のサポートが含まれていて、トラフィックをストリームに分類したり、定義済みの Per-Hop Behavior に従って特定の QoS 処理を指定したりすることができます。

標準の IP ベース ネットワークは、ベストエフォート型のデータ配信サービスを提供するように設計されています。ベストエフォート型サービスでは、保証はされませんが、ネットワークによってタイミング良くデータが配信されます。輻輳が発生している場合、パケットが遅延したり、散発的に送信されたり、ドロップしたりすることがあります。電子メールやファイル転送などの一般的なインターネット アプリケーションでは、サービスのわずかな低下は許容範囲内であり、たいていの場合は気づきません。ただし、音声やマルチメディアなどのタイミング要件が厳しいアプリケーションでは、サービスの低下が望ましくない影響を及ぼします。

DiffServ 設定は、IP プロトコルやその他の基準に従ってトラフィックを分類するクラス マップを定義することから始まります。その後、各クラス マップをトラフィック クラスの処理方法を定義するポリシー マップに関連付けることができます。時間的に制約があるトラフィックを含むクラスには、その他のトラフィックに優先するポリシー マップを割り当てることができます。

[クラス マップ] ページを使用して、トラフィックのクラスを定義できます。[ポリシー マップ] ページを使用して、ポリシーを定義し、それらにクラス マップを関連付けます。

IPv4 クラス マップの設定

IPv4 クラス マップを追加して設定するには

ステップ 1 [クライアント QoS] > [クラス マップ] の順に選択します。

ステップ 2 [クラス マップ名] フィールドに、新しいクラス マップの名前を入力します。名前には、1 ～ 31 文字の英数字と特殊文字を使用できます。スペースは使用できません。

ステップ 3 [クラス マップ タイプ] リストから、クラス マップのタイプとして IPv4 を選択します。IPv4 クラス マップは、WAP デバイスの IPv4 トラフィックにのみ適用されます。

ステップ 4 [一致基準の設定] エリアで、パケットとクラスを照合するためのパラメータを設定します。

- [クラス マップ名]: リストから IPv4 クラス マップを選択します。
- [すべてのパケットの照合]: この一致条件は、レイヤ 3 パケットのすべてのパラメータに適用されます。有効にすると、すべてのレイヤ 3 パケットが条件を照合します。

- [プロトコル]:IPv4 パケットの IP プロトコル フィールドまたは IPv6 パケットのネクスト ヘッダー フィールドの値に基づく、レイヤ 3 またはレイヤ 4 プロトコルの一致条件を使用します。照合するプロトコルをキーワードで選択するか、プロトコル ID を入力します。
  - [リストから選択]:選択したプロトコルを照合します(IP、ICMP、IGMP、TCP、UDP)。
  - [値と照合]:名前でリストされていないプロトコルを照合します。プロトコル ID を入力します。プロトコル ID は、IANA によって割り当てられた標準値です。数値の範囲は 0 ～ 255 です。
- [送信元 IP]:パケットの送信元 IPv4 アドレスと適切なフィールドで定義された IPv4 アドレスを一致させる必要があります。
  - [送信元 IP アドレス]:この基準を適用する IPv4 アドレスを入力します。
  - [送信元 IP マスク]:送信元 IPv4 アドレス マスクを入力します。DiffServ のマスクは、ドット付き 10 進表記の IP のネットワーク方式ビット マスクです。宛先 IP アドレスのどの部分を使用してパケット コンテンツと照合するのかを示します。

255.255.255.255 の DiffServ マスクはすべてのビットが重要で、0.0.0.0 のマスクは重要なマスクがないことを示します。ACL ワイルド カード マスクでは反対になります。たとえば、基準と単一ホスト アドレスを照合するには、255.255.255.255 のマスクを使用します。基準を 24 ビット サブネット(192.168.10.0/24 など)と照合するには、255.255.255.0 のマスクを使用します。

- [送信元ポート]:ルールの一致条件に送信元ポートを含めます。送信元ポートは、データグラム ヘッダーで識別されます。
  - [リストから選択]:送信元ポートに関連付けられたキーワード(ftp、ftpdata、http、smtp、snmp、telnet、tftp、www)を照合します。これらの各キーワードは、同等のポート番号に変換されます。
  - [ポートと照合]:データグラム ヘッダーの送信元ポート番号と指定した IANA ポート番号を照合します。ポートの範囲は 0 ～ 65535 で、3 つの異なるポート タイプが含まれます。

    0 ～ 1023:ウェルノウン ポート

    1024 ～ 49151:登録済みポート

    49152 ～ 65535:ダイナミック ポート/プライベート ポート
  - [マスク]:ポート マスク。マスクで、使用するビットと無視するビットを決定します。16 進数(0 ～ 0xFFFF)のみ使用できます。1 はそのビットが重要なこと、0 はそのビットが無視されることを意味します。

- [宛先 IP]:パケットの宛先 IPv4 アドレスと適切なフィールドで定義された IPv4 アドレスを一致させる必要があります。
  - [宛先 IP アドレス]:この基準を適用する IPv4 アドレスを入力します。
  - [宛先 IP マスク]:宛先 IP アドレス マスクを入力します。
- [宛先ポート]:ルールの一致条件に宛先ポートを含めます。宛先ポートは、データグラム ヘッダーで識別されます。
  - [リストから選択]:データグラム ヘッダーの宛先ポートと選択したキーワード(ftp、ftpdata、http、smtp、snmp、telnet、tftp、www)を照合します。これらの各キーワードは、同等のポート番号に変換されます。
  - [ポートと照合]:データグラム ヘッダーの宛先ポートと指定した IANA ポート番号を照合します。ポートの範囲は 0 ～ 65535 で、3 つの異なるポートタイプが含まれます。

    0 ～ 1023:ウェルノウン ポート

    1024 ～ 49151:登録済みポート

    49152 ～ 65535:ダイナミック ポート/プライベート ポート
  - [マスク]:ポート マスク。マスクで、使用するビットと無視するビットを決定します。16 進数(0 ～ 0xFFFF)のみ使用できます。1 はそのビットが重要なこと、0 はそのビットが無視されることを意味します。
- [サービス タイプ]:パケットとクラス基準の照合に使用するサービスのタイプを指定します。
  - [IP DSCP] [リストから選択]:一致基準として使用する DSCP 値を選択します。
  - [IP DSCP] [値と照合]:0 ～ 63 のカスタム DSCP 値を入力します。
  - [IP プレシデンス]:パケットの IP プレシデンス値とこのフィールドで定義した IP プレシデンス値を照合します。IP プレシデンスの範囲は 0 ～ 7 です。
  - [IP ToS ビット]:一致基準として、IP ヘッダー内のパケットのタイプ オブ サービス(ToS)ビットを使用します。IP ToS ビット値の範囲は、00 ～ FF です。上位 3 ビットは、IP プレシデンス値を表します。上位 6 ビットは、IP DSCP 値を表します。

- [IP ToS マスク]：IP ToS マスク値を入力します。この値によって、パケットの IP ToS フィールドとの比較に使用される IP ToS ビット値のビット位置が識別されます。

  IP ToS マスク値は、00 ～ FF の 2 桁の 16 進数で、反転マスク（ワイルドカード）を表します。IP ToS マスクの値が 0 のビットは、パケットの IP ToS フィールドとの比較に使用される IP ToS ビット値のビット位置を示します。たとえば、IP ToS 値でビット 7 および 5 が設定されていてビット 1 がクリアなことを確認するには、ビット 7 が最も重要な場合、IP ToS ビット値 0 と IP ToS マスク 00 を使用します。

ステップ 5 [保存] をクリックします。変更が、スタートアップ コンフィギュレーションに保存されます。

注 クラス マップを削除するには、[クラス マップ名] リストから選択して [削除] をクリックします。ポリシーに割り当てられている場合は、そのクラス マップを削除することはできません。

IPv6 クラス マップの設定

IPv6 クラス マップを追加して設定するには

ステップ 1 [クライアント QoS] > [クラス マップ] の順に選択します。

ステップ 2 [クラス マップ名] フィールドに、新しいクラス マップの名前を入力します。名前には、1 ～ 31 文字の英数字と特殊文字を使用できます。スペースは使用できません。

ステップ 3 [クラス マップ タイプ] リストから、クラス マップのタイプとして IPv6 を選択します。IPv6 クラス マップは、WAP デバイスの IPv6 トラフィックにのみ適用されます。

ステップ 4 [一致基準の設定] エリアで、パケットとクラスを照合するためのパラメータを設定します。

- [クラス マップ名]：リストから IPv6 クラス マップを選択します。
- [すべてのパケットの照合]：この一致条件は、レイヤ 3 パケットのすべてのパラメータに適用されます。有効にすると、すべてのレイヤ 3 パケットが条件を照合します。
- [プロトコル]：IPv4 パケットの IP プロトコル フィールドまたは IPv6 パケットのネクスト ヘッダー フィールドの値に基づく、レイヤ 3 またはレイヤ 4 プロトコルの一致条件を使用します。照合するプロトコルをキーワードで選択するか、プロトコル ID を入力します。
  - [リストから選択]：選択したプロトコルを照合します（IPv6、ICMPv6、TCP、UDP）。

- [値と照合]:名前でリストされていないプロトコルを照合します。プロトコル ID を入力します。プロトコル ID は、IANA によって割り当てられた標準値です。数値の範囲は 0 ～ 255 です。

- [送信元 IPv6]:パケットの送信元 IPv6 アドレスと適切なフィールドで定義された IPv6 アドレスを一致させる必要があります。
  - [送信元 IPv6 アドレス]:この基準を適用する IPv6 アドレスを入力します。
  - [送信元 IPv6 のプレフィクス長]:送信元 IPv6 アドレスのプレフィクス長を入力します。
- [送信元ポート]:ルールの一致条件に送信元ポートを含めます。送信元ポートは、データグラム ヘッダーで識別されます。
  - [リストから選択]:送信元ポートに関連付けられたキーワード(ftp、ftpdata、http、smtp、snmp、telnet、tftp、www)を照合します。これらの各キーワードは、同等のポート番号に変換されます。
  - [ポートと照合]:データグラム ヘッダーの送信元ポート番号と指定した IANA ポート番号を照合します。ポートの範囲は 0 ～ 65535 で、3 つの異なるポート タイプが含まれます。

    0 ～ 1023:ウェルノウン ポート

    1024 ～ 49151:登録済みポート

    49152 ～ 65535:ダイナミック ポート/プライベート ポート
  - [マスク]:ポート マスク。マスクで、使用するビットと無視するビットを決定します。16 進数(0 ～ 0xFFFF)のみ使用できます。1 はそのビットが重要なこと、0 はそのビットが無視されることを意味します。
- [宛先 IPv6]:パケットの宛先 IPv6 アドレスと適切なフィールドで定義された IPv6 アドレスを一致させる必要があります。
  - [宛先 IPv6 アドレス]:この基準を適用する IPv6 アドレスを入力します。
  - [宛先 IPv6 のプレフィクス長]:宛先 IPv6 アドレスのプレフィクス長を入力します。
- [宛先ポート]:ルールの一致条件に宛先ポートを含めます。宛先ポートは、データグラム ヘッダーで識別されます。
  - [リストから選択]:データグラム ヘッダーの宛先ポートと選択したキーワード(ftp、ftpdata、http、smtp、snmp、telnet、tftp、www)を照合します。これらの各キーワードは、同等のポート番号に変換されます。

- [ポートと照合]:データグラム ヘッダーの宛先ポートと指定した IANA ポート番号を照合します。ポートの範囲は 0 ～ 65535 で、3 つの異なるポート タイプが含まれます。

  0 ～ 1023:ウェルノウン ポート

  1024 ～ 49151:登録済みポート

  49152 ～ 65535:ダイナミック ポート/プライベート ポート

- [マスク]:ポート マスク。マスクで、使用するビットと無視するビットを決定します。16 進数(0 ～ 0xFFFF)のみ使用できます。1 はそのビットが重要なこと、0 はそのビットが無視されることを意味します。

▪ [IPv6 フロー レベル]:IPv6 パケットに一意の 20 ビットの数値を入力します。ルータでの QoS 処理を表すためにエンド ステーションで使用されます(0 ～ 1048575 の範囲)。

▪ [IP DSCP]:DSCP 値を一致基準として使用します。

- [リストから選択]:リストから DSCP タイプを選択します。
- [値と照合]:0 ～ 63 のカスタム DSCP 値を入力します。

ステップ 5 [保存] をクリックします。変更が、スタートアップ コンフィギュレーションに保存されます。

注 クラス マップを削除するには、[クラス マップ名] リストから選択して [削除] をクリックします。ポリシーに割り当てられている場合は、そのクラス マップを削除することはできません。

MAC クラス マップの設定

MAC クラス マップを設定するには

ステップ 1 [クライアント QoS] > [クラス マップ] の順に選択します。

ステップ 2 [クラス マップ名] フィールドに、新しいクラス マップの名前を入力します。名前には、1 ～ 31 文字の英数字と特殊文字を使用できます。スペースは使用できません。

ステップ 3 [クラス マップ タイプ] リストから、クラス マップのタイプとして MAC を選択します。MAC クラス マップは、レイヤ 2 基準に適用されます。

ステップ 4 [一致基準の設定] エリアで、パケットとクラスを照合するためのパラメータを設定します。

▪ [クラス マップ名]:リストから MAC クラス マップを選択します。

- [すべてのパケットの照合]:有効にすると、すべてのレイヤ 2 パケットが条件を照合します。
- [EtherType]:一致基準とイーサネット フレームのヘッダーにある値を比較します。EtherType のキーワードを選択するか、EtherType の値を入力して、一致基準を指定します。
  - [リストから選択]:ダイアグラム ヘッダーの Ethertype と選択したプロトコル タイプ(appletalk、arp、ipv4、ipv6、ipx、netbios、pppoe)を照合します。
  - [値と照合]:データグラム ヘッダーの Ethertype と指定したカスタム プロトコル識別子を照合します。値は、0600 ～ FFFF の範囲の 4 桁の 16 進数を使用できます。
- [クラス オブ サービス]:パケットを照合するためのクラス オブ サービス 802.1p のユーザ プライオリティ値を指定します。有効な範囲は 0 ～ 7 です。
- [送信元 MAC]:ルールの一致条件に送信元 MAC アドレスを含めます。
  - [送信元 MAC アドレス]:イーサネット フレームと比較するための送信元 MAC アドレスを入力します。
  - [送信元 MAC マスク]:送信元 MAC アドレス マスクを入力して、宛先 MAC アドレスのどのビットをイーサネット フレームと比較するのかを指定します。

MAC マスクのそれぞれのビット位置について、0 は対応するアドレス ビットが有効なことを示し、1 はアドレス ビットが無視されることを示します。たとえば、MAC アドレスの最初の 4 オクテットのみをチェックするには、MAC マスク 00:00:00:00:ff:ff を使用します。MAC マスク 00:00:00:00:00:00 は、すべてのアドレス ビットをチェックします。また、単一の

MAC アドレスの照合に使用されます。

- [宛先 MAC]:ルールの一致条件に宛先 MAC アドレスを含めます。
  - [宛先 MAC アドレス]:イーサネット フレームと比較するための宛先 MAC アドレスを入力します。
  - [宛先 MAC マスク]:宛先 MAC アドレス マスクを入力して、宛先 MAC アドレスのどのビットをイーサネット フレームと比較するのかを指定します。
- [VLAN ID]:パケットを照合する VLAN ID を指定します。VLAN ID の範囲は 0 ～ 4095 です。

ステップ 5 [保存] をクリックします。変更が、スタートアップ コンフィギュレーションに保存されます。

注 クラス マップを削除するには、[クラス マップ名] リストから選択して [削除] をクリックします。ポリシーに割り当てられている場合は、そのクラス マップを削除することはできません。

ポリシー マップ

パケットは、定義された基準に基づいて分類および処理されます。分類基準は、[クラス マップ] ページのクラスで定義されます。処理は、[ポリシー マップ] ページのポリシー属性で定義されます。ポリシー属性は、クラスごとのインスタンス ベースで分類され、クラス基準と照合するトラフィックの処理方法を決定します。

WAP デバイスは、最大 50 個のポリシー マップをサポートします。ポリシー マップには、最大 10 個のクラス マップを含めることができます。

ポリシー マップの追加および設定

ポリシー マップを追加および設定するには

ステップ 1 [クライアント QoS] > [ポリシー マップ] の順に選択します。

ステップ 2 [ポリシー マップ名] フィールドに、ポリシー マップの名前を入力します。名前には、1 ～ 31 文字の英数字と特殊文字を使用できます。スペースは使用できません。

ステップ 3 [ポリシー マップの追加] をクリックします。

ステップ 4 [ポリシー クラスの定義] エリアで、ポリシー マップの次のパラメータを設定します。

- [ポリシー マップ名]: 設定するポリシー マップを選択します。
- [クラス マップ名]: このポリシーを適用するクラス マップを選択します。
- [簡易ポリシング]: クラスのトラフィック ポリシング方式を確立します。単純な形のポリシング方式では、単一のデータ レートとバースト サイズを使用します。適合と不適合の 2 つの結果が生じます。

  この機能を有効にする場合は、次のいずれかのフィールドを設定します。

  - [認定レート]: トラフィックが準拠する必要がある認定レート（Kbps 単位）。範囲は 1 ～ 1000000 Kbps です。
  - [認定バースト]: トラフィックが準拠する必要がある認定バースト サイズ（バイト単位）。範囲は 1 ～ 204800000 バイトです。

- [送信]: クラス マップ基準を満たした場合に、関連するトラフィック ストリームのすべてのパケットを転送するよう指定します。
- [ドロップ]: クラス マップ基準を満たした場合に、関連するトラフィック ストリームのすべてのパケットをドロップするよう指定します。
- [クラス オブ サービスのマーク]: 802.1p ヘッダーのプライオリティ フィールドで指定したクラス オブ サービス値で、関連するトラフィック ストリームのすべてのパケットをマークします。パケットにこのヘッダーが含まれていない場合は、ヘッダーを挿入します。CoS 値は、0 ～ 7 の整数です。
- [IP DSCP のマーク]: リストから選択した IP DSCP 値で、関連するトラフィック ストリームのすべてのパケットをマークします。
  - [リストから選択]: DSCP タイプのリスト。
- [IP プレシデンスのマーク]: 指定した IP プレシデンス値で、関連するトラフィック ストリームのすべてのパケットをマークします。IP プレシデンス値は、0 ～ 7 の整数です。
- [クラス マップの関連付け解除]: [クラス マップ名] リストで選択したクラスを [ポリシー マップ名] リストで選択したポリシーから削除します。
- [メンバー クラス]: 選択したポリシーのメンバーとして現在定義されているすべての DiffServ クラスをリストします。クラスがポリシーに関連付けられていない場合は、このフィールドは空になります。

ステップ 5 [保存] をクリックします。変更が、スタートアップ コンフィギュレーションに保存されます。

注 ポリシー マップを削除するには、[ポリシー マップ名] リストから選択して [削除] をクリックします。

注 ポリシー マップは、VAP に関連付けられていない場合にのみ削除できます。

注 [クラス オブ サービスのマーク]、[IP DSCP のマーク]、[IP プレシデンスのマーク] などのポリシーをマークするパラメータは、IPV6 クラス マップではサポートされていません。

クライアント QoS アソシエーション

[QoS アソシエーション] ページでは、ワイヤレスおよびイーサネット インターフェイスの QoS の特定の側面に対する制御を提供します。また、個々のクライアントが送受信できる帯域幅の量の制御も提供します。

一般的なトラフィック カテゴリの制御に加えて、QoS によって、差別化サービス（DiffServ）を通してさまざまなマイクロフローをクライアントごとに調整できます。DiffServ ポリシーは、一般的なマイクロフローの定義や処理の特徴を確立するのに便利なツールです。ネットワーク上で認証されている場合は、送受信両方のワイヤレス クライアントに適用できます。

QoS アソシエーション パラメータの設定

QoS アソシエーション パラメータを設定するには

ステップ 1 [クライアント QoS] > [クライアント QoS アソシエーション] の順に選択します。

ステップ 2 [インターフェイス] フィールドで、QoS パラメータを設定する無線またはイーサネット インターフェイスを選択します。

ステップ 3 **選択したインターフェイス**の [有効] を選択します。

ステップ 4 選択したインターフェイスの次のパラメータを選択します。

- [帯域幅制限（ダウン ストリーム）]：WAP デバイスからクライアントへの最大許容伝送レートを 1 秒あたりのビット数（bps）で入力します。有効範囲は 0 ～ 1300 Mbps です。
- [帯域幅制限（アップ ストリーム）]：クライアントから WAP デバイスへの最大許容伝送レートを 1 秒あたりのビット数（bps）で入力します。有効範囲は 0 ～ 1300 Mbps です。
- [DiffServ ポリシー]：選択したインターフェイスについて、WAP デバイスに送信されるトラフィックに適用する DiffServ ポリシーを選択します。

ステップ 5 [保存] をクリックします。変更が、スタートアップ コンフィギュレーションに保存されます。

クライアント QoS ステータス

[クライアント QoS ステータス] ページには、ポリシー マップに含まれるクラス マップやポリシー マップがバインドされているインターフェイスなど、ポリシー マップおよびクラス マップの詳細が表示されます。

IPv4 QoS、IPv6 QoS、および MAC QoS の表には、[クラス マップ] ページで定義したクラス マップに関する次の情報が表示されます。

- [メンバー クラス]: クラス マップ名。
- [すべて照合]: このマップがすべてのパケットを照合するかどうかが表示されます。

[ルール フィールド]: このクラス マップの詳細な定義が表示されます。詳細については、「クラス マップ」を参照してください。

[ポリシー マップ] 表には、[ポリシー マップ] ページで定義されたポリシー マップに関する次の情報が表示されます。

- [ポリシー マップ名]: ポリシー マップ名。
- [バインドされたインターフェイス]: このポリシー マップが関連付けられているインターフェイスが表示されます。
- [クラス マップ名]: このポリシー マップに含まれるクラス マップがリストされます。

[ポリシー]: このクラス マップのポリシーの詳細が表示されます。詳細については、「ポリシー マップ」を参照してください。

[更新] をクリックすると、画面を更新して、最新情報を表示できます。

9

ACL

ここでは、WAP デバイスで ACL 機能を設定する方法について説明します。次のトピックがあります。

- ACL ルール
- ACL アソシエーション
- ACL ステータス

ACL ルール

ACL は、ルールと呼ばれる許可条件および拒否条件を集めたものであり、権限を持たないユーザをブロックし、権限を持つユーザに特定のリソースへのアクセスを許可することによってセキュリティを提供します。ACL では、ネットワーク リソースに到達しようとする是認されていないすべての試行をブロックできます。

WAP デバイスは、最大 50 個の IPv4、IPv6、および MAC ACL ルールをサポートしています。

IPv4 と IPv6 の ACL

IP ACL はレイヤ 3 および 4 用にトラフィックを分類します。

各 ACL は WAP デバイスが受信するトラフィックに適用されるルールのセットです。各ルールは、所定のフィールドの内容によって、ネットワークへのアクセスを許可するのか拒否するのかを指定します。さまざまな基準に基づいたルールを設定でき、それらを送信元または宛先の IP アドレス、送信元または宛先のポート、パケットで伝送されているプロトコルなど、パケット内の 1 個以上のフィールドに適用できます。

注 作成するすべてのルールの終わりに暗黙の拒否があります。すべて拒否することのないよう、ACL 内に許可ルールを追加して、トラフィックを許可することを強くお勧めします。

MAC ACL

MAC ACL はレイヤ 2 ACL です。送信元または宛先の MAC アドレス、VLAN ID、Class of Service など、フレームのフィールドを検査するルールを設定できます。フレームが WAP デバイスのポートに入ると、WAP デバイスはフレームを検査して、ACL ルールをフレームの内容と照合します。内容と一致するルールがあった場合、許可アクションまたは拒否アクションがフレームに対して実行されます。

ACL を設定するためのワークフロー

[ACL ルール] ページを使用して ACL およびルールを設定してから、指定したインターフェイスにルールを適用します。

ACL の設定

ACL を設定するには、次の手順を実行してください。

ステップ 1 [ACL] > [ACL ルール] の順に選択します。

ステップ 2 ACL の名前を指定します。

ステップ 3 追加する ACL のタイプを選択します。

ステップ 4 ACL を追加します。

ステップ 5 ACL に新規ルールを追加します。

ステップ 6 ルールの一致基準を設定します。

ステップ 7 [ACL アソシエーション] ページを使用して、ACL を 1 つ以上のインターフェイスに適用します。

IPv4 ACL の設定

IPv4 ACL の設定

IPv4 ACL を設定するには、次の手順を実行してください。

ステップ 1 [ACL] > [ACL ルール] の順に選択します。

ステップ 2 [ACL 名] フィールドに ACL を識別する名前を入力します。この名前には、1 ～ 31 文字の英数字および特殊文字を使用することができます。スペースは使用できません。

ステップ 3 [ACL タイプ] リストから、ACL のタイプとして [IPv4] を選択します。IPv4 ACL は、レイヤ 3 およびレイヤ 4 基準に基づいてネットワーク リソースへのアクセスを制御します。

ステップ 4 [ACL の追加] をクリックします。

ステップ 5　[ACL ルール設定] 領域で、次の ACL ルール パラメータを設定します。

- [ACL 名 - ACL タイプ]: 新規ルールを設定する ACL を選択します。
- [ルール]: 選択した ACL の新規ルールを設定するために [新規ルール] を選択します。ACL に複数のルールがある場合、ルールは、ACL に追加した順序でパケットまたはフレームに適用されます。最後のルールとして暗黙のすべて拒否ルールがあります。
- [アクション]: この ACL ルールがアクションを許可するのか拒否するのかを選択します。
- [許可する] を選択した場合、このルールは、ルール基準を満たすすべてのトラフィックが WAP デバイスに入ることを許可します。基準を満たさないトラフィックはドロップされます。
- [拒否する] を選択した場合、このルールは、ルール基準を満たすトラフィックが WAP デバイスに入ることを必ずブロックします。基準を満たさないトラフィックは、このルールが最後のルールでなければ転送されます。すべての ACL の最後に暗黙のすべて拒否ルールがあるため、明示的に許可されないトラフィックはすべてドロップされます。
- [各パケットを一致させる]: 有効にした場合、許可アクションまたは拒否アクションを持つこのルールは、内容に関係なくフレームまたはパケットと一致します。この機能を有効にした場合、追加の一致条件は設定できません。新規ルールでは、このオプションがデフォルトで選択されています。他の一致フィールドを設定するにはこのオプションを無効にする必要があります。
- [プロトコル]: IPv4 パケットの IP Protocol フィールドまたは IPv6 パケットの Next Header フィールドの値に基づいてレイヤ 3 またはレイヤ 4 プロトコル一致基準を使用します。次のいずれかのオプションか [任意] を選択できます。
  - [リストから選択]: 次のプロトコルから選択します。IP、ICMP、IGMP、TCP、または UDP。
  - [値に一致させる]: IANA によって割り当てられた標準プロトコル ID 0 ～ 255 を入力します。[リストから選択] に名前がリストされていないプロトコルを指定する場合にこの方法を選択します。
- [送信元 IP]: パケットの送信元 IP アドレスは、該当するフィールドに定義されているアドレスと一致する必要があります。
  - [送信元 IP アドレス]: この基準に適用する IP アドレスを入力します。
  - [ワイルド カード マスク]: 送信元 IP アドレスのワイルド カード マスクを入力します。ワイルド カード マスクによって使用するビットおよび無視するビットが決まります。ワイルド カード マスク 255.255.255.255 は、どのビットも検査しないことを示します。ワイルドカード 0.0.0.0 はすべての

ビットを検査することを示します。このフィールドは [送信元 IP アドレス] をオンにする場合は必須です。

ワイルド カード マスクは基本的にはサブネット マスクの逆です。たとえば、単一のホスト アドレスと一致する基準の場合は、ワイルド カード マスク 0.0.0.0 を使用します。24 ビットのサブネット（例：192.168.10.0/24）と一致する基準の場合は、ワイルド カード マスク 0.0.0.255 を使用します。

- [送信元ポート]：ルールの一致基準に送信元ポートを含めます。送信元ポートはデータグラム ヘッダーで識別されます。
  - [リストから選択]：照合する送信元ポートと関連付けるキーワード（ftp、ftpdata、http、smtp、snmp、telnet、tftp、www）を選択します。この各キーワードは相当するポート番号に変換されます。
  - [ポートに一致させる]：データグラム ヘッダーで識別された送信元ポートに一致させる IANA ポート番号を入力します。ポートの範囲は 0 ～ 65535 で、3 種類のポートが含まれます。

    0 ～ 1023：ウェルノウン ポート

    1024 ～ 49151：登録済みポート

    49152 ～ 65535：動的ポートおよび/またはプライベート ポート
  - [マスク]：ポート マスクを入力します。マスクによって使用するビットおよび無視するビットが決まります。16 進数の値（0 ～ 0xFFFF）のみ使用できます。0 はこのビットを検査することを意味し、1 はこのビットを無視することを意味します。
- [宛先 IP]：パケットの宛先 IP アドレスは、該当するフィールドに定義されているアドレスと一致する必要があります。
  - [宛先 IP アドレス]：この基準に適用する IP アドレスを入力します。

    [ワイルド カード マスク]：宛先 IP アドレスのワイルド カード マスクを入力します。ワイルド カード マスクによって使用するビットおよび無視するビットが決まります。ワイルド カード マスク 255.255.255.255 は、どのビットも検査しないことを示します。ワイルドカード 0.0.0.0 はすべてのビットを検査することを示します。このフィールドは [送信元 IP アドレス] を選択する場合は必須です。

    ワイルド カード マスクは基本的にはサブネット マスクの逆です。たとえば、単一のホスト アドレスと一致する基準の場合は、ワイルド カード マスク 0.0.0.0 を使用します。24 ビットのサブネット（例：192.168.10.0/24）と一致する基準の場合は、ワイルド カード マスク 0.0.0.255 を使用します。

- [宛先ポート]:ルールの一致基準に宛先ポートを含めます。宛先ポートはデータグラム ヘッダーで識別されます。
  - [リストから選択]:照合する宛先ポートと関連付けるキーワード(ftp、ftpdata、http、smtp、snmp、telnet、tftp、www)を選択します。この各キーワードは相当するポート番号に変換されます。
  - [ポートに一致させる]:データグラム ヘッダーで識別された宛先ポートに一致させる IANA ポート番号を入力します。ポートの範囲は 0 ～ 65535 で、3 種類のポートが含まれます。

    0 ～ 1023:ウェルノウン ポート

    1024 ～ 49151:登録済みポート

    49152 ～ 65535:動的ポートおよび/またはプライベート ポート
  - [マスク]:ポート マスクを入力します。マスクによって使用するビットおよび無視するビットが決まります。16 進数の値(0 ～ 0xFFFF)のみ使用できます。0 はこのビットを検査することを意味し、1 はこのビットを無視することを意味します。
- [サービスの種類]:サービスの種類に基づいてパケットを照合します。
  - [IP DSCP リストから選択]:DSCP Assured Forwarding(AS)、Class of Service(CS)、または Expedited Forwarding(EF)の値に基づいてパケットを照合します。
  - [IP DSCP を値に一致させる]:カスタム DSCP 値に基づいてパケットを照合します。選択した場合は、0 ～ 63 の値をこのフィールドに入力してください。
  - [IP プレシデンス]:IP プレシデンス値に基づいてパケットを照合します。選択した場合は、0 ～ 7 の IP プレシデンス値を入力してください。
  - [IP ToS ビット]:一致基準としてパケットの IP ヘッダーの ToS ビットに使用する値を指定します。

    パケットの IP ToS フィールドは、IP ヘッダーの Service Type オクテットの全 8 ビットとして定義されています。IP ToS ビット値は 00 ～ ff の 2 桁の 16 進数です。上位 3 ビットは IP プレシデンス値を表します。上位 6 ビットは IP Differentiated Services Code Point(DSCP)値を表します。

- [IP ToS マスク]:パケットの IP ToS フィールドとの比較に使用する IP ToS ビット値内のビット位置を識別する IP ToS マスク値を入力します。

  IP ToS マスク値は 00 ～ FF の 2 桁の 16 進数であり、反転(ワイルドカード)マスクを表します。IP ToS マスク内の値ゼロは、パケットの IP ToS フィールドとの比較に使用する IP ToS ビット内のビット位置を示します。たとえば、ビット 7 および 5 が設定されており、ビット 1 がクリアされている IP ToS 値(ビット 7 が最上位)を検査するには、IP ToS ビット値 0 および IP ToS マスク 00 を使用します。

ステップ 6 [保存] をクリックします。変更がスタートアップ コンフィギュレーションに保存されます。

注 ACL を削除するには、[ACL 名 - ACL タイプ] リストで選択されていることを確認し、[ACL の削除] を選択してから [保存] をクリックします。

IPv6 ACL の設定

IPv6 ACL の設定

IPv6 ACL を設定するには、次の手順を実行してください。

ステップ 1 [ACL] > [ACL ルール] の順に選択します。

ステップ 2 [ACL 名] フィールドに ACL を識別する名前を入力します。

ステップ 3 [ACL タイプ] リストから ACL のタイプとして [IPv6] を選択します。IPv6 ACL はレイヤ 3 およびレイヤ 4 基準に基づいてネットワークへのアクセスを制御します。

ステップ 4 [ACL の追加] をクリックします。

ステップ 5 [ACL ルール設定] 領域で、次の ACL ルール パラメータを設定します。

- [ACL 名 - ACL タイプ]:新規ルールを設定する ACL を選択します。
- [ルール]:選択した ACL の新規ルールを設定するために [新規ルール] を選択します。ACL に複数のルールがある場合、ルールは、ACL に追加した順序でパケットまたはフレームに適用されます。最後のルールとして暗黙のすべて拒否ルールがあります。
- [アクション]:この ACL ルールがアクションを許可するのか拒否するのかを選択します。
- [許可する] を選択した場合、このルールは、ルール基準を満たすすべてのトラフィックが WAP デバイスに入ることを許可します。基準を満たさないトラフィックはドロップされます。

- [拒否する] を選択した場合、このルールは、ルール基準を満たすトラフィックが WAP デバイスに入ることを必ずブロックします。基準を満たさないトラフィックは、このルールが最後のルールでなければ転送されます。すべての ACL の最後に暗黙のすべて拒否ルールがあるため、明示的に許可されないトラフィックはすべてドロップされます。
- [各パケットを一致させる]: 有効にした場合、許可アクションまたは拒否アクションを持つこのルールは、内容に関係なくフレームまたはパケットと一致します。この機能を有効にした場合、追加の一致条件は設定できません。新規ルールでは、このオプションがデフォルトで選択されています。他の一致フィールドを設定するにはこのオプションを無効にする必要があります。
- [プロトコル]: 照合するプロトコルをキーワードまたはプロトコル ID で選択します。
- [送信元 IPv6]: パケットの送信元 IPv6 アドレスは、該当するフィールドに定義されている IPv6 アドレスと一致する必要があります。
  - [送信元 IPv6 アドレス]: この基準に適用する IPv6 アドレスを入力します。
  - [送信元 IPv6 プレフィックス長]: 送信元 IPv6 アドレスのプレフィックス長を入力します。
- [送信元ポート]: ルールの一致基準に送信元ポートを含めます。送信元ポートはデータグラム ヘッダーで識別されます。
  - [リストから選択]: 選択する場合は、リストからポート名を選択します。
  - [ポートに一致させる]: データグラム ヘッダーで識別された送信元ポートに一致させる IANA ポート番号を入力します。ポートの範囲は 0 ～ 65535 で、3 種類のポートが含まれます。

    0 ～ 1023: ウェルノウン ポート

    1024 ～ 49151: 登録済みポート

    49152 ～ 65535: 動的ポートおよび/またはプライベート ポート
  - [マスク]: ポート マスクを入力します。マスクによって使用するビットおよび無視するビットが決まります。16 進数の値（0 ～ 0xFFFF）のみ使用できます。0 はこのビットを検査することを意味し、1 はこのビットを無視することを意味します。
- [宛先 IPv6]: パケットの宛先 IPv6 アドレスは、該当するフィールドに定義されている IPv6 アドレスと一致する必要があります。
  - [宛先 IPv6 アドレス]: この基準に適用する IPv6 アドレスを入力します。

- [宛先 IPv6 プレフィックス長]:宛先 IPv6 アドレスのプレフィックス長を入力します。

- [宛先ポート]:ルールの一致基準に宛先ポートを含めます。宛先ポートはデータグラム ヘッダーで識別されます。
  - [リストから選択]:選択する場合は、リストからポート名を選択します。
  - [ポートに一致させる]:データグラム ヘッダーで識別された送信元ポートに一致させる IANA ポート番号を入力します。ポートの範囲は 0 ～ 65535 で、3 種類のポートが含まれます。

    0 ～ 1023:ウェルノウン ポート

    1024 ～ 49151:登録済みポート

    49152 ～ 65535:動的ポートおよび/またはプライベート ポート
  - [マスク]:ポート マスクを入力します。マスクによって使用するビットおよび無視するビットが決まります。16 進数の値(0 ～ 0xFFFF)のみ使用できます。0 はこのビットを検査することを意味し、1 はこのビットを無視することを意味します。

- [IPv6 フロー ラベル]:IPv6 パケット固有の 20 ビット値を指定します。ルータでの QoS 処理を示すためにエンド ステーションで使用されます(0 ～ 1048575 の範囲)。

- [IPv6 DSCP]:IP DSCP 値に基づいてパケットを照合します。選択する場合は、一致基準として次のいずれかのオプションを選択してください。
  - [リストから選択]:次の値から選択します。DSCP Assured Forwarding (AS)、Class of Service (CS)、または Expedited Forwarding (EF)。
  - [値に一致させる]:カスタム DSCP 値 0 ～ 63 を入力します。

ステップ 6 [保存] をクリックします。変更がスタートアップ コンフィギュレーションに保存されます。

注 ACL を削除するには、[ACL 名 - ACL タイプ] リストで選択されていることを確認し、[ACL の削除] をオンにしてから [保存] をクリックします。

MAC ACL の設定

MAC ACL ???

MAC ACL を設定するには、次の手順を実行してください。

ステップ 1 [ACL] > [ACL ルール] の順に選択します。

ステップ 2 [ACL 名] フィールドに ACL を識別する名前を入力します。

ステップ 3 [ACL タイプ] リストから ACL のタイプとして [MAC] を選択します。MAC ACL は、レイヤ 2 基準に基づいてアクセスを制御します。

ステップ 4 [ACL の追加] をクリックします。

ステップ 5 [ACL ルール設定] 領域で、次の ACL ルール パラメータを設定します。

- [ACL 名 - ACL タイプ]: 新規ルールを設定する ACL を選択します。
- [ルール]: 選択した ACL の新規ルールを設定するために [新規ルール] を選択します。ACL に複数のルールがある場合、ルールは、ACL に追加した順序でパケットまたはフレームに適用されます。最後のルールとして暗黙のすべて拒否ルールがあります。
- [アクション]: この ACL ルールがアクションを許可するのか拒否するのかを選択します。
- [許可する] を選択した場合、このルールは、ルール基準を満たすすべてのトラフィックが WAP デバイスに入ることを許可します。基準を満たさないトラフィックはドロップされます。
- [拒否する] を選択した場合、このルールは、ルール基準を満たすトラフィックが WAP デバイスに入ることを必ずブロックします。基準を満たさないトラフィックは、このルールが最後のルールでなければ転送されます。すべての ACL の最後に暗黙のすべて拒否ルールがあるため、明示的に許可されないトラフィックはすべてドロップされます。
- [各パケットを一致させる]: 有効にした場合、許可アクションまたは拒否アクションを持つこのルールは、内容に関係なくフレームまたはパケットと一致します。この機能を有効にした場合、追加の一致条件は設定できません。新規ルールでは、このオプションがデフォルトで選択されています。他の一致フィールドを設定するにはこのオプションを無効にする必要があります。
- [EtherType]: イーサネット フレームのヘッダーにある値と比較する一致基準を選択します。EtherType キーワードを選択するか、EtherType 値を入力して一致基準を指定できます。
  - [リストから選択]: 単一のプロトコル タイプを appletalk、arp、ipv4、ipv6、ipx、netbios、pppoe から選択します。

- [値に一致させる]:パケットを照合するカスタム プロトコル識別子を入力します。この値は、0600 ～ FFFF の範囲の 4 桁の 16 進数です。

- [Class of Service]:イーサネット フレームと比較する 802.1p ユーザ プライオリティを入力します。有効な範囲は 0 ～ 7 です。このフィールドは最初または唯一の 802.1Q VLAN タグのみにあります。
- [送信元 MAC]:パケットの送信元 MAC アドレスは、該当するフィールドに定義されているアドレスと一致する必要があります。
  - [送信元 MAC アドレス]:イーサネット フレームと比較する送信元 MAC アドレスを入力します。
  - [送信元 MAC マスク]:イーサネット フレームと比較する送信元 MAC のビットを指定する送信元 MAC アドレス マスクを入力します。

    MAC マスクのビット位置ごとに、0 は対応するアドレス ビットを検査することを示し、1 はアドレス ビットを無視することを示します。たとえば、MAC アドレスの先頭 4 オクテットのみをチェックする場合は、MAC マスク 00:00:00:00:ff:ff を使用します。MAC マスク 00:00:00:00:00:00 ではすべてのアドレス ビットがチェックされるため、単一の MAC アドレスを照合する場合に使用します。
- [宛先 MAC]:パケットの宛先 MAC アドレスは、該当するフィールドに定義されているアドレスと一致する必要があります。
  - [宛先 MAC アドレス]:イーサネット フレームと比較する宛先 MAC アドレスを入力します。
  - [宛先 MAC マスク]:イーサネット フレームと比較する宛先 MAC のビットを指定する宛先 MAC アドレス マスクを入力します。
- [VLAN ID]:イーサネット フレームと比較する具体的な VLAN ID を入力します。

  このフィールドは最初または唯一の 802.1Q VLAN タグのみにあります。

ステップ 6 [保存] をクリックします。変更がスタートアップ コンフィギュレーションに保存されます。

注 ACL を削除するには、[ACL 名 - ACL タイプ] リストで選択されていることを確認し、[ACL の削除] をオンにしてから [保存] をクリックします。

ACL アソシエーション

[ACL アソシエーション] ページには、ワイヤレス インターフェイスおよびイーサネット インターフェイスとバインドされた ACL リストが表示されます。HTTP トラフィックや、特定のサブネットからのトラフィックなど、一般的なトラフィックのカテゴリを制御するために、ACL を設定して 1 つ以上のインターフェイスに割り当てることができます。

ACL のインターフェイスへの関連付け

ACL をインターフェイスに関連付けるには、次の手順を実行してください。

ステップ 1 [ACL] > [ACL アソシエーション] の順に選択します。

ステップ 2 [インターフェイス] フィールドで、ACL パラメータを設定する無線またはイーサネット インターフェイスをクリックします。

ステップ 3 選択したインターフェイスに関する次のパラメータを設定します。

- [ACL タイプ]：WAP デバイスに入るトラフィックに適用される ACL のタイプを選択します。次のいずれかのオプションを使用できます。
  - [IPv4]：ACL ルールと一致する IPv4 パケットを検査します。
  - [IPv6]：ACL ルールと一致する IPv6 パケットを検査します。
  - [MAC]：ACL ルールと一致するレイヤ 2 フレームを検査します。
  - [なし]：WAP デバイスに入るトラフィックを検査しません。
- [ACL 名]：WAP デバイスに入るトラフィックに適用される ACL の名前を選択します。

  パケットまたはフレームを WAP デバイスが受信すると、ACL ルールが一致するかどうかがチェックされます。許可される場合はパケットまたはフレームが処理され、拒否される場合は廃棄されます。

ステップ 4 [保存] をクリックします。変更がスタートアップ コンフィギュレーションに保存されます。

ACL ステータス

[ACL ステータス] ページには、さまざまなタイプの ACL ルールの詳細が表示されます。

ACL ステータスを表示するには、[ACL] > [ACL ステータス] の順に選択します。

次の情報が表示されます。

- [ACL 名]: ACL の名前。
- [インターフェイス バウンド]: ACL が関連付けられているインターフェイスです。
- [ルール番号]: ACL に含まれるルールの番号です。
- [アクション]: ACL によって実行されるアクションです。
- [各パケットを一致させる]: この ACL ルールが各パケットと一致するかどうかを示します。

[ルール フィールド]: ACL の詳細設定を表示します。詳細については、「ACL ルール」を参照してください。

[更新] をクリックして画面を更新することで、最新の情報を参照できます。

10

SNMP

ここでは、Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）を構成および統計情報収集タスクを実行するように設定する方法について説明します。

具体的な内容は次のとおりです。

- 全般
- ビュー
- グループ
- ユーザ
- ターゲット

全般

[全般] ページを使用して、SNMP を有効にしたり、基本的なプロトコル設定を行ったりすることができます。

SNMP の全般設定

SNMP の全般設定を行うには

ステップ 1　ナビゲーション ペインで、[SNMP] > [全般] の順に選択します。

ステップ 2　[SNMP] 設定で [有効] を選択します。SNMP は、デフォルトでは無効になっています。

ステップ 3　SNMP トラフィックの [UDP ポート] を指定します。

デフォルトでは、SNMP エージェントはポート 161 からの要求のみをリッスンします。ただし、エージェントが別のポートの要求をリッスンするように設定できます。有効な範囲は 1025 ～ 65535 です。

ステップ 4　SNMPv2 設定を行います。

- [読み取り専用コミュニティ]:SNMPv2 アクセス用の読み取り専用コミュニティの名前。有効な範囲は、1 ～ 256 文字の英数字と特殊文字です。

  コミュニティ名は、SNMP エージェントへのデータを要求できるネットワーク上のマシンを制限するための単純な認証機能としての役割を果たします。名前はパスワードとして機能します。送信者がパスワードを知っている場合に、要求は信頼できるものとみなされます。

- [読み書きコミュニティ]:SNMP SET 要求に使用される読み書きコミュニティ名。有効な範囲は、1 ～ 256 文字の英数字と特殊文字です。

  コミュニティ名の設定は、パスワードの設定と同じです。このコミュニティ名と同じ名前のマシンからの要求のみが許可されます。

- [管理ステーション]:SNMP を介して WAP デバイスにアクセスできるステーションを特定します。次のいずれかのオプションを選択します。

  - [すべて]:SNMP を介して WAP デバイスにアクセスできる一連のステーションは制限されません。
  - [ユーザ定義]:許可される SNMP 要求は、指定されたものに制限されます。

- [NMS IPv4 アドレス/名前]:Network Management System（NMS; ネットワーク管理システム）、または管理対象デバイスに GET 要求および SET 要求を実行できる一連のマシンの IPv4 IP アドレス、DNS ホスト名、またはサブネット。

  DNS ホスト名は、1 つ以上のラベルで構成できます。ラベルは、最大 63 文字の英数字で構成されます。ホスト名に複数のラベルが含まれる場合、それぞれをピリオド(.) で区切ります。一連のラベルおよびピリオドの長さは、最大 253 文字にすることができます。

  コミュニティ名と同様に、この設定で SNMP 設定にある程度のセキュリティが提供されます。SNMP エージェントは、ここに指定した IP アドレス、ホスト名、またはサブネットからの要求のみを受け入れます。

  サブネットを指定するには、*address/mask_length* の形式で 1 つ以上のサブネットワーク アドレス範囲を入力します。ここの *address* は IP アドレス、*mask_length* はマスク ビット数です。*address/mask* および *address/mask_length* の両方の形式がサポートされます。たとえば、192.168.1.0/24 の範囲を入力すると、アドレスが 192.168.1.0 でサブネットマスクが 255.255.255.0 のサブネットワークを指定します。

  アドレス範囲は、指定された NMS のサブネットを指定するために使用します。この範囲内の IP アドレスを持つマシンのみが、管理対象デバイスで GET 要求および SET 要求を実行できます。上記の例からすると、192.168.1.1 から 192.168.1.254 のアドレスを持つマシンが、デバイスで SNMP コマンドを実行

できます(サブネットワーク範囲で接尾辞 .0 で識別されるアドレスは、常にサブネット アドレス用に予約され、範囲で.255 で識別されるアドレスは、常にブロードキャスト アドレス用に予約されます)。

別の例としては、10.10.1.128/25 の範囲を入力すると、10.10.1.129 から 10.10.1.254 の IP アドレスを持つマシンが、管理対象デバイスで SNMP 要求を実行できます。この例では、10.10.1.128 はネットワーク アドレスで、10.10.1.255 はブロードキャスト アドレスです。合計 126 個のアドレスが指定されます。

- [NMS IPv6 アドレス/名前]:管理対象デバイスに GET 要求および SET 要求を実行できるマシンの IPv6 IP アドレス、DNS ホスト名、またはサブネット。IPv6 アドレスは、xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx (2001:DB8::CAD5:7D91) の形式にする必要があります。

  ホスト名は、最大 63 文字の英数字のセットからなる 1 つ以上のラベルで構成できます。ホスト名に複数のラベルが含まれる場合、それぞれをピリオド(.)で区切ります。一連のラベルおよびピリオドの長さは、最大 253 文字にすることができます。

ステップ 5 SNMPv2 トラップ設定を行います。

- [トラップ コミュニティ]:SNMP トラップに関連付けられるグローバルなコミュニティ文字列。デバイスから送信されたトラップは、コミュニティ名としてこの文字列を提供します。有効な範囲は、1 ～ 60 文字の英数字と特殊文字です。
- [トラップ宛先テーブル]:SNMP トラップを受信する最大 3 つの IP アドレスまたはホスト名のリスト。ボックスを選択して [ホスト IP アドレス タイプ](IPv4 または IPv6)を選択してから、[ホスト名/IP アドレス] を追加します。

  DNS ホスト名の例は、snmptraps.foo.com です。SNMP トラップは SNMP エージェントからランダムに送信されるため、トラップの送信先を正確に指定することは重要です。最大 3 つの DNS ホスト名を指定できます。必ず、[有効] チェックボックスを選択してから適切な [ホスト IP アドレス タイプ] を選択してください。

  前述の手順のホスト名に関する注意も参照してください。

ステップ 6 [保存] をクリックします。変更が、スタートアップ コンフィギュレーションに保存されます。

注 新しい設定を保存すると、対応するプロセスが停止され、再起動されることがあります。この事態が発生すると、WAP デバイスが切断される可能性があります。切断によってワイヤレス クライアントが受ける影響が最も小さい場合に、WAP デバイスの設定を変更することをお勧めします。

ビュー

SNMP MIB ビューは、MIB 階層のビュー サブツリーのファミリです。ビュー サブツリーは、Object Identifier（OID; オブジェクト ID）サブツリーの値とビット文字列のマスク値のペアリングによって識別されます。各 MIB ビューは、MIB ビューに含まれるものまたは MIB ビューから除外されるものの 2 セットのビュー サブツリーで定義されます。MIB ビュー を作成して、SNMPv3 ユーザがアクセスできる OID 範囲を制御できます。

AP は、最大 16 個のビューをサポートしています。

次の注意は、SNMPv3 ビューの設定に関するいくつかの重要なガイドラインの要約です。すべての注意を読んでから先に進んでください。

注 「すべて」が付く MIB ビューは、システムでデフォルトで作成されています。このビューには、システムでサポートされるすべての管理オブジェクトが含まれます。

注 デフォルトでは、「ビュー - すべて」および「ビュー - なし」の SNMPv3 ビューは WAP デバイスで作成されます。これらのビューを削除したり変更したりすることはできません。

SNMP ビューの追加および設定

SNMP ビューを追加および設定するには

ステップ 1 ナビゲーション ペインで、[SNMP] > [ビュー] の順に選択します。

ステップ 2 [追加] をクリックして、[SNMPv3 ビュー] 表に新しい行を作成します。

ステップ 3 新しい行のボックスを選択して、[編集] をクリックします。

- [ビュー名]: MIB ビューを識別する名前を入力します。ビュー名には最大で 32 文字の英数字を含めることができます。
- [タイプ]: ビューのサブツリーまたはサブツリーのファミリを MIB ビューに含めるか、MIB ビューから除外するかを選択します。
- [OID]: ビューに含めるまたはビューから除外するサブツリーの OID 文字列を入力します。

  たとえば、システムのサブツリーは OID 文字列 .3.6.1.2.1.1 で指定されます。
- [マスク]: OID マスクを入力します。マスクの長さは 47 文字です。OID マスクの形式は、xx.xx.xx (.)... または xx:xx:xx....(:) で、長さは 16 オクテットです。各オクテットは、ピリオド（.）またはコロン（:）のいずれかで区切られた 2 つの 16 進数文字です。このフィールドには、16 進数文字のみを使用できます。

たとえば、OID マスク FA.80 は、11111010.10000000 です。

ファミリ マスクは、ビュー サブツリーのファミリの定義に使用されます。ファミリ マスクは、関連するファミリ OID 文字列のサブ ID がファミリの定義に有効なことを示します。ビュー サブツリーのファミリによって、表内の 1 行に対して効果的なコントロール アクセスが可能になります。

ステップ 4 [保存] をクリックします。ビューが [SNMPv3 ビュー] リストに追加され、変更がスタートアップ コンフィギュレーションに保存されます。

注 ビューを削除するには、リストでビューを選択して [削除] を選択します。

グループ

SNMPv3 グループによって、異なる認証およびアクセス権限のグループにユーザをまとめることができます。各グループは、次の 3 つのセキュリティ レベルのいずれかに関連付けられます。

- noAuthNoPriv
- authNoPriv
- authPriv

各グループの MIB へのアクセスは、MIB ビューを読み取りまたは書き込みアクセス用のグループに別々に関連付けることによって制御されます。

デフォルトでは、AP には次の 2 つのグループがあります。

- **RO**：認証およびデータ暗号化を使用する読み取り専用グループ。このグループのユーザは、認証に MD5 キー/パスワードを使用し、暗号化に DES キー/パスワードを使用します。MD5 および DES キー/パスワードの両方を定義する必要があります。デフォルトで、このグループのユーザには、デフォルトのすべての MIB ビューに対する読み取りアクセス権があります。
- **RW**：認証およびデータ暗号化を使用する読み取り/書き込みグループ。このグループのユーザは、認証に MD5 キー/パスワードを使用し、暗号化に DES キー/パスワードを使用します。MD5 および DES キー/パスワードの両方を定義する必要があります。デフォルトで、このグループのユーザには、デフォルトのすべての MIB ビューに対する読み取りおよび書き込みアクセス権があります。

注 デフォルト グループの RO および RW を削除することはできません。

注 AP は、最大 8 個のグループをサポートしています。

SNMP グループの追加および設定

SNMP グループを追加および設定するには

ステップ 1 ナビゲーション ペインで、[SNMP] > [グループ] の順に選択します。

ステップ 2 [追加] をクリックして、[SNMPv3 グループ] 表に新しい行を作成します。

ステップ 3 新しいグループのボックスを選択して、[編集] をクリックします。

ステップ 4 次のパラメータを設定します。

- [グループ名]: グループを識別する名前。デフォルトのグループ名は RO および RW です。

  グループ名には最大で 32 文字の英数字を含めることができます。

- [セキュリティ レベル]: グループのセキュリティ レベルを設定します。オプションは次のとおりです。

  - [noAuthentication-noPrivacy]: 認証なし、データ暗号化なし（セキュリティなし）。

  - [Authentication-noPrivacy]: 認証あり、データ暗号化なし。このセキュリティ レベルでは、認証に MD5 キー/パスワードを使用しますが、暗号化に DES キー/パスワードは使用せずに SNMP メッセージを送信します。

  - [Authentication-Privacy]: 認証あり、データ暗号化あり。このセキュリティ レベルでは、認証用に MD5 キー/パスワードを送信し、暗号化用に DES キー/パスワードを送信します。

    認証、暗号化、または両方が必要なグループでは、[SNMP ユーザ] ページで MD5 および DES キー/パスワードを定義する必要があります。

- [書き込みビュー]: グループの MIB への書き込みアクセス。オプションは次のとおりです。

  - [ビュー - すべて]: グループは、MIB を作成、変更、および削除できます。

  - [ビュー - なし]: グループは、MIB を作成、変更、または削除できません。

- [読み取りビュー]: グループの MIB への読み取りアクセス。

  - [ビュー - すべて]: グループは、すべての MIB を表示および読み取りできます。

  - [ビュー - なし]: グループは、MIB を表示または読み取りできません。

ステップ 5 [保存] をクリックします。グループが [SNMPv3 グループ] リストに追加され、変更がスタートアップ コンフィギュレーションに保存されます。

注 グループを削除するには、リストでグループを選択して [削除] を選択します。

ユーザ

[SNMP ユーザ] ページを使用して、ユーザを定義したり、セキュリティ レベルを各ユーザに関連付けたり、ユーザごとにセキュリティ キーを設定したりすることができます。

各ユーザは、定義済みグループまたはユーザ定義グループのいずれかから SNMPv3 グループにマップされ、任意で認証および暗号化向けに設定されます。認証では、MD5 タイプのみがサポートされます。暗号化では、DES タイプのみがサポートされます。AP にデフォルトの SNMPv3 ユーザが存在しない場合は、最大 8 つのユーザを追加できます。

SNMP ユーザの追加

SNMP ユーザを追加するには

ステップ 1 ナビゲーション ペインで、[SNMP] > [ユーザ] の順に選択します。

ステップ 2 [追加] をクリックして、[SNMPv3 ユーザ] 表に新しい行を作成します。

ステップ 3 新しい行のボックスを選択して、[編集] をクリックします。

ステップ 4 次のパラメータを設定します。

- [ユーザ名]: SNMPv3 ユーザを識別する名前。ユーザ名には最大で 32 文字の英数字を含めることができます。
- [グループ]: ユーザがマップされるグループ。デフォルト グループは RW および RO です。[SNMP グループ] ページで追加グループを定義できます。
- [認証タイプ]: ユーザからの SNMPv3 要求に使用する認証タイプ。オプションは次のとおりです。
  - [MD5]: ユーザからの SNMP 要求に MD5 認証が必要です。
  - [なし]: このユーザ からの SNMPv3 要求に認証は必要ありません。
- [認証パス フレーズ]: (認証タイプに MD5 を指定している場合) SNMP エージェントがユーザから送信された要求を認証できるようにするためのパス フレーズ。パス フレーズの長さは 8 ～ 32 文字にする必要があります。

- [暗号化タイプ]:ユーザからの SNMP 要求に使用するプライバシーのタイプ。オプションは次のとおりです。
  - [DES]:ユーザからの SNMPv3 要求に DES 暗号化を使用します。
  - [なし]:このユーザ からの SNMPv3 要求にプライバシーは必要ありません。
- [暗号化パス フレーズ]:(プライバシー タイプに DES を指定している場合) SNMP 要求の暗号化に使用するパス フレーズ。パス フレーズの長さは 8 ～ 32 文字にする必要があります。

ステップ 5 [保存] をクリックします。ユーザが [SNMPv3 ユーザ] リストに追加され、変更がスタートアップ コンフィギュレーションに保存されます。

注 ユーザを削除するには、リストでユーザを選択して [削除] を選択します。

ターゲット

SNMPv3 ターゲットは、Inform メッセージを使用して SNMP 通知を SNMP マネージャに送信します。SNMPv3 ターゲットでは、Informs のみが送信され、トラップは送信されません。SNMP バージョン 1 および 2 では、トラップが送信されます。各ターゲットは、ターゲット IP アドレス、UDP ポート、および SNMPv3 ユーザ名で定義されます。

注 SNMPv3 ユーザ設定([ユーザ] ページを参照)を完了してから、SNMPv3 ターゲットを設定する必要があります。

注 AP は、最大 8 個のターゲットをサポートしています。

SNMP ターゲットの追加

SNMP ターゲットを追加するには

ステップ 1 ナビゲーション ペインで、[SNMP] > [ターゲット] の順に選択します。

ステップ 2 [追加] をクリックします。新しい行が表に作成されます。

ステップ 3 新しい行のボックスを選択して、[編集] をクリックします。

ステップ 4 次のパラメータを設定します。

- [IP アドレス]:ターゲットを受信するリモート SNMP マネージャの IPv4 アドレスを入力します。

- [UDP ポート]: SNMPv3 ターゲットの送信に使用する UDP ポートを入力します。
- [ユーザ]: ターゲットと関連付ける SNMP ユーザの名前を入力します。SNMP ユーザを設定するには、[ユーザ] ページを参照してください。

ステップ 5 [保存] をクリックします。ユーザが [SNMPv3 ターゲット] リストに追加され、変更がスタートアップ コンフィギュレーションに保存されます。

注 SNMP ターゲットを削除するには、リストでユーザを選択して [削除] を選択します。

11

キャプティブ ポータル

ここでは、キャプティブ ポータル（CP）機能について説明します。この機能により、ユーザの検証が完了するまでワイヤレス クライアントがネットワークにアクセスすることを防止できます。CP 検証は、ゲスト ユーザと認証済みユーザの両方についてアクセスを許可するように設定できます。

認証済みユーザは、アクセスが許可される前に、認可された CP グループまたはユーザのデータベースに対して検証される必要があります。このデータベースは、WAP デバイスにローカルに保存するか RADIUS サーバに保存することができます。

キャプティブ ポータルは 2 つの CP インスタンスで構成されます。各インスタンスは、各 VAP または SSID 用の異なる検証方式によって、個別に設定することができます。Cisco WAP571/E デバイスは、CP 認証用に設定されたいくつかの VAP および通常のワイヤレス認証方法（WPA、WPA Enterprise など）用に設定されたその他の VAP と同時に動作します。

具体的な内容は、次のとおりです。

- グローバル設定
- ローカル グループ/ユーザ
- インスタンス設定
- インスタンス アソシエーション
- Web ポータルのカスタマイズ
- 認証済みクライアント

グローバル設定

[グローバル CP 設定] ページでは、キャプティブ ポータル機能の管理状態を制御し、WAP デバイスで設定されているすべての CP インスタンスに影響するグローバル設定値を設定できます。

CP グローバル設定値の設定

CP グローバル設定値を設定するには、次の手順を実行してください。

ステップ 1 [キャプティブ ポータル]、[グローバル設定] の順に選択します。

ステップ 2 次のパラメータを設定します。

- [キャプティブ ポータル モード]:WAP デバイスでのキャプティブ ポータル動作を有効または無効にします。
- [認証タイムアウト]:ポータルを介してネットワークにアクセスする場合、クライアントは、まず、認証 Web ページに認証情報を入力する必要があります。このフィールドでは、WAP デバイスが、関連付けられたワイヤレス クライアントとの認証セッションを開いたままにする時間を秒単位で指定します。許可されたタイムアウト時間内に認証資格情報を入力できなかったクライアントは、認証 Web ページの表示を更新しなければならない場合があります。デフォルトの認証タイムアウトは 300 秒です。60 ～ 600 秒の範囲で入力します。
- [追加の HTTP ポート]:HTTP トラフィックでは HTTP 管理ポート(デフォルトでは 80)が使用されます。HTTP トラフィック用の追加のポートを設定できます。ポート番号(1025 ～ 65535 または 80)を入力します。HTTP ポートと HTTPS ポートを同じにすることはできません。
- [追加の HTTPS ポート]:SSL を介した HTTP トラフィック(HTTPS)では HTTPS 管理ポート(デフォルトでは 443)が使用されます。HTTPS トラフィック用の追加のポートを設定できます。ポート番号(1025 ～ 65535 または 443)を入力します。HTTP ポートと HTTPS ポートを同じにすることはできません。

ステップ 3 [キャプティブ ポータル設定カウンタ] エリアには、次の読み取り専用 CP 情報が表示されます。

- [インスタンス数]:WAP デバイスで現在設定されている CP インスタンスの数です。最大 2 つのインスタンスを設定できます。
- [グループ数]:WAP デバイスで現在設定されている CP グループの数です。最大 2 つのグループを設定できます。Default Group はデフォルトで存在し、削除できません。
- [ユーザ数]:WAP デバイスで現在設定されている CP グループの数です。最大 128 のユーザを設定できます。

ステップ 4 [保存] をクリックします。変更がスタートアップ コンフィギュレーションに保存されます。

ローカル グループ/ユーザ

[ローカル グループ/ユーザ] ページでは、ローカル グループおよびユーザを管理できます。

ローカル グループ

各ローカル ユーザはユーザ グループに割り当てられます。各グループは CP インスタンスに割り当てられます。このグループにより、CP インスタンスへのユーザ割り当ての管理が容易になります。

「Default」という名前のユーザ グループが組み込まれており、削除できません。最大 2 つの追加のユーザ グループを作成できます。

ローカル ユーザ グループを追加するには、次の手順を実行してください。

ステップ 1 [キャプティブ ポータル]、[ローカル グループ/ユーザ] の順に選択します。

ステップ 2 [ローカル グループ設定] エリアで、次のパラメータを設定します。

- [キャプティブ ポータル グループ]:[作成] を選択して新しいグループを作成します。
- [グループ名]:新しいグループの名前を入力します。

ステップ 3 [グループの追加] をクリックします。変更がスタートアップ コンフィギュレーションに保存されます。

ローカル ユーザ グループを追加するには、次の手順を実行してください。

ステップ 1 [キャプティブ ポータル]、[ローカル グループ/ユーザ] の順に選択します。

ステップ 2 [ローカル グループ設定] エリアで、削除するグループを選択します。

ステップ 3 [グループの削除] オプションをオンにします。

ステップ 4 [グループの削除] をクリックします。変更がスタートアップ コンフィギュレーションに保存されます。

ローカル ユーザ

ゲスト ユーザと認可済みユーザのいずれかに対応するように CP インスタンスを設定できます。ゲスト ユーザは、割り当てられたユーザ名およびパスワードを持ちません。

認可済みユーザは、最初にローカル データベースまたは RADIUS サーバに対して検証する必要のある有効なユーザ名およびパスワードを入力します。認可済みユーザは、通常、ゲスト ユーザとは異なる VAP と関連付けられた CP インスタンスに割り当てられます。

ローカル データベースで最大 128 の認可済みユーザを設定できます。

ローカル ユーザを追加および設定するには、次の手順を実行してください。

ステップ 1 [キャプティブ ポータル]、[ローカル グループ/ユーザ] の順に選択します。

ステップ 2 [ローカル ユーザ設定] エリアで、次のパラメータを設定します。

- [キャプティブ ポータル ユーザ]:[作成] を選択して新しいユーザを作成します。
- [ユーザ名]:新しいユーザの名前を入力します。

ステップ 3 [ユーザの追加] をクリックします。

ステップ 4 [ローカル ユーザ設定] エリアが、追加のオプションとともに再表示されます。次のパラメータを設定します。

- [ユーザ パスワード]:8 ～ 64 文字の英数字および特殊文字によるパスワードを入力します。ユーザは、キャプティブ ポータルを介してネットワークにログインするためにこのパスワードを入力する必要があります。
- [パスワードをクリア テキストで表示]:有効になっている場合は、入力するテキストが表示されます。無効になっている場合、入力時にテキストはマスクされません。
- [退席中タイムアウト]:クライアントの WAP デバイスとの関連付けが解除された後にユーザが CP 認証済みクライアント リストに保持される時間を入力します。クライアントが再認証を試みる前に、このフィールドで指定された時間が経過すると、クライアント エントリが認証済みクライアント リストから削除されます。0 ～ 1440 分の範囲で入力します。デフォルト値は 60 です。ここで設定したタイムアウト値は、ユーザ値が 0 に設定されないかぎり、CP インスタンスに関して設定された値よりも優先されます。0 に設定されている場合は、CP インスタンスに関して設定されているタイムアウト値が使用されます。
- [グループ名]:割り当てられているユーザ グループを選択します。各 CP インスタンスは、ユーザの特定のグループをサポートするように設定されます。

- [最大帯域幅アップストリーム]:キャプティブ ポータルを使用する場合にクライアントがトラフィックを送信できる最大アップロード速度を Mbps 単位で入力します。この設定により、ネットワークにデータを送信するために使用される帯域幅が制限されます。0 ～ 1300 Mbpsの範囲で入力します。デフォルトは 0 です。
- [最大帯域幅ダウンストリーム]:キャプティブ ポータルを使用する場合にクライアントがトラフィックを受信できる最大ダウンロード速度を Mbps 単位で入力します。この設定により、ネットワークからデータを受信するために使用される帯域幅が制限されます。0 ～ 1300 Mbpsの範囲で入力します。デフォルトは 0 です。

ステップ 5 [ユーザの保存] をクリックします。変更がスタートアップ コンフィギュレーションに保存されます。

ローカル ユーザを削除するには、次の手順を実行してください。

ステップ 1 [キャプティブ ポータル]、[ローカル グループ/ユーザ] の順に選択します。

ステップ 2 [ローカル ユーザ設定] エリアで、削除するユーザを選択します。

ステップ 3 [ユーザの削除] オプションをオンにします。

ステップ 4 [ユーザの削除] をクリックします。変更がスタートアップ コンフィギュレーションに保存されます。

インスタンス設定

最大 2 つの CP インスタンスを作成できます。各 CP インスタンスは、一連の定義済みインスタンス パラメータです。インスタンスは、1 つまたは複数の VAP と関連付けることができます。異なるインスタンスを設定することにより、関連付けられた VAP にユーザがアクセスを試みる場合に異なる応答をすることができます。

注 インスタンスを作成する前に、まず、次の項目を確認してください。

- 新しい VAP を追加する必要がありますか。必要がある場合は、[ネットワーク] ページにアクセスして VAP を追加します。

新しいグループまたは新しいユーザを追加する必要がありますか。必要がある場合は、[ローカル グループ/ユーザ] ページにアクセスしてグループまたはユーザを追加します。

CP インスタンスの作成およびその設定値の設定

CP インスタンスを作成し、その設定値を設定するには、次の手順を実行してください。

ステップ 1 [キャプティブ ポータル]、[インスタンス設定] の順に選択します。

ステップ 2 [キャプティブ ポート インスタンス] リストから [作成] を選択します。

ステップ 3 CP インスタンスの名前を [インスタンス名] フィールドに 1 ～ 32 文字の英数字で入力します。

ステップ 4 [保存] をクリックします。

ステップ 5 [キャプティブ ポータル インスタンス パラメータ] エリアが、追加のオプションとともに再表示されます。次のパラメータを設定します。

- [インスタンス ID]: インスタンス ID が表示されます。このフィールドは設定できません。
- [管理モード]: CP インスタンスを有効および無効にします。
- [プロトコル]: 検証プロセスで使用する CP インスタンスのプロトコルとして、HTTP または HTTPS を選択します。
  - [HTTP]: 検証時に暗号化を使用しません。
  - [HTTPS]: 暗号化を実現するために証明書が必要なセキュア ソケット レイヤ（SSL）を使用します。証明書は、接続時にユーザに提示されます。
- [検証]: CP でクライアントを検証するために使用する認証方式を選択します。
  - [ゲスト]: このユーザは、データベースによって認証される必要がありません。
  - [ローカル]: この WAP デバイスは、ローカル データベースを使用してユーザを認証します。
  - [RADIUS]: この WAP デバイスは、リモート RADIUS サーバ上のデータベースを使用してユーザを認証します。
  - [Active Directoryサーバ（Active Directory Server）]: WAP デバイスは、`starttls` コマンドを通じて SSL\TLS を使用し、セキュアな LDAP バインドを実行して、Active Directory で sAMAccountName 属性によってユーザを認証します。
  - [サードパーティクレデンシャル（3rd Party Credentials）]: WAP デバイスは、Facebook または Google のアカウントによってユーザを認証できます。

- [ソーシャルログイン方式(Social Login Method)]:WAP デバイスは OAuth プロトコルを使用して、Facebook または Google アカウントによってユーザを認証できます。
  - [Facebook]:クライアントの認証に Facebook アカウントを使用する、ソーシャル ログインを有効または無効にします。
  - [Google]:クライアントの認証に Google アカウントを使用する、ソーシャル ログインを有効または無効にします。
- [Active Directoryサーバ Host1(Active Directory Server Host1)]:サーバを追加し、ドメイン コントローラの IP アドレスを入力します。
- [Active Directoryサーバ Host2(Active Directory Server Host1)]:サーバを追加し、ドメイン コントローラの IP アドレスを入力します。
- [Active Directoryサーバ Host3(Active Directory Server Host1)]:サーバを追加し、ドメイン コントローラの IP アドレスを入力します。

注
- 複数のサーバを追加することができます。AP では、host1 から host3 の順序でサーバをテストします。

- [ウォールドガーデンの範囲(Walled Garden Range]:Web ポータル ページを通過するまでにユーザがアクセスできるドメインのリストを指定します。リスト内の項目はカンマで区切ります。ドメインにはアスタリスク(*)の形式でワイルドカードを含めることができます。

注
- シスコでは、データ保護、プライバシー、およびセキュリティ要件を、新商品のコンセプト考案から発売までの製品設計および開発手法に統合します。詳細については、https://www.cisco.com/c/en/us/about/trust-center/gdpr.html を参照してください。

- Facebook または Google ログインを有効にすると、ウォールド ガーデン機能の自動的にアクティブになり、認証のためのリストに次のドメインが追加されます。ドメインのリストは Facebook または Google に応じて変わる可能性があり、また最新でない場合があります。ドメインは手動で追加することができます。
  - **Facebook**:*.facebook.com、*.facebook.net、*.fbcdn.net
  - **Google**:*.googleapis.com、apis.google.com、accounts.google.com、*.googleusercontent.com、ssl.gstatic.com、fonts.gstatic.com
  - **Windows 10**: ww.msftconnecttest.com
  - [リダイレクト(Redirect)]:有効になっている場合。キャプティブ ポータルは、新しく認証されたクライアントを、設定された URL にリダイレクトする必要があります。このオプションがオフになっている場合、ユーザが検証に合格すると、ロケール固有の初期ページが表示されます

- [リダイレクト]:有効になっている場合。キャプティブ ポータルは、新しく認証されたクライアントを、設定された URL にリダイレクトする必要があります。このオプションがオフになっている場合、ユーザが検証に合格すると、ロケール固有の初期ページが表示されます。
- [リダイレクト URL]:リダイレクト モードが有効になっている場合は、新しく認証されたクライアントがリダイレクトされる URL(「http://」を含む)を入力します。0 ～ 256 文字で入力します。
- [退席中タイムアウト]:クライアントの WAP デバイスとの関連付けが解除された後にユーザが CP 認証済みクライアント リストに保持される時間を入力します。クライアントが再認証を試みる前に、このフィールドで指定された時間が経過すると、クライアント エントリが認証済みクライアント リストから削除されます。0 ～ 1440 分の範囲で入力します。デフォルト値は 60 分です。

退席中タイムアウト値はユーザごとに設定することもできます。[ローカル グループ/ユーザ] ページを参照してください。[ローカル ユーザ] ページで設定されている退席中タイムアウト値は、値が 0(デフォルト)に設定されないかぎり、ここで設定された値よりも優先されます。値が 0 の場合は、インスタンスのタイムアウト値が使用されます。

- [セッション タイムアウト]:CP セッションが有効であるための残り時間を秒単位で入力します。この時間が 0 に達すると、クライアントの認証が解除されます。0 ～ 1440 分の範囲で入力します。デフォルト値は 0 です。
- [最大帯域幅アップストリーム]:キャプティブ ポータルを使用する場合にクライアントがトラフィックを送信できる最大アップロード速度を Mbps 単位で入力します。この設定により、クライアントがネットワークにデータを送信できる帯域幅が制限されます。0 ～ 1300 Mbpsの範囲で入力します。デフォルト値は 0 です。
- [最大帯域幅ダウンストリーム]:キャプティブ ポータルを使用する場合にクライアントがトラフィックを受信できる最大ダウンロード速度を Mbps 単位で入力します。この設定により、クライアントがネットワークからデータを受信できる帯域幅が制限されます。0 ～ 1300 Mbpsの範囲で入力します。デフォルト値は 0 です。
- [ユーザ グループ名]:検証モードがローカルまたは RADIUS に設定されている場合、既存のユーザ グループを CP インスタンスに割り当てます。このグループに属しているすべてのユーザは、このポータルを介してネットワークにアクセスすることが許可されます。
- [RADIUS IP ネットワーク]:WAP RADIUS クライアントが、設定済みの IPv4 または IPv6 の RADIUS サーバ アドレスを使用するかどうかを選択します。

- [グローバル RADIUS]:検証モードが RADIUS に設定されている場合、デフォルトのグローバル RADIUS サーバ リストを使用してクライアントを認証するときは、[有効化] をオンにします(グローバル RADIUS サーバの設定については、「RADIUS サーバ」を参照してください)。CP 機能に異なる一連の RADIUS サーバを使用させる場合は、このチェック ボックスをオフにして、このページのフィールドでサーバを設定します。
- [RADIUS アカウンティング]:特定のユーザが消費したリソース(システム時刻、送受信データ量など)を追跡および測定するには、[有効化] をオンにします。RADIUS アカウンティングは、有効にすると、プライマリ RADIUS サーバ、すべてのバックアップ サーバ、およびグローバルまたはローカルに設定されているサーバに関して有効になります。
- [サーバの IP アドレス 1] または [サーバの IPv6 アドレス 1]:この VAP のプライマリ RADIUS サーバの IPv4 または IPv6 アドレスを入力します。IPv4 アドレスは、xxx.xxx.xxx.xxx(192.0.2.10)のような形式である必要があります。IPv6 アドレスは、xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx (2001:DB8::CAD5:7D91)のような形式である必要があります。

  最初のワイヤレス クライアントが VAP による認証を試みると、WAP デバイスは認証要求をプライマリ サーバに送信します。プライマリ サーバが認証要求に応答すると、WAP デバイスはこの RADIUS サーバを引き続きプライマリ サーバとして使用し、認証要求が指定されたアドレスに送信されます。
- [サーバの IP アドレス 2 ～ 4] または [サーバの IPv6 アドレス 2 ～ 4]:最大 3 つの IPv4 または IPv6 のバックアップ RADIUS サーバ アドレスを入力します。プライマリ サーバによる認証に失敗すると、設定済みの各バックアップ サーバが順に試みられます。
- [キー 1]:WAP デバイスが認証のためにプライマリ RADIUS サーバに対して使用する共有秘密キーを入力します。最大 63 文字の標準英数字および特殊文字を使用できます。このキーは、大文字と小文字が区別され、RADIUS サーバで設定されているキーと一致する必要があります。入力するテキストはアスタリスクとして表示されます。
- [キー 2 ～ 4]:設定済みのバックアップ RADIUS サーバに関連付けられている RADIUS キーを入力します。サーバの IP(IPv6)アドレス 1 のサーバはキー 1 を使用し、サーバの IP(IPv6)アドレス 2 のサーバはキー 2 を使用し、以降同様になります。
- [ロケール数]:インスタンスに関連付けられているロケールの数です。[Web カスタマイズ] ページから、3 つの異なるロケールを作成して 各 CP インスタンスに割り当てることができます。
- [インスタンスの削除]:現在のインスタンスを削除する場合はオンにします。

ステップ 6 [保存] をクリックします。変更がスタートアップ コンフィギュレーションに保存されます。

インスタンス アソシエーション

インスタンスを作成したら、[インスタンス アソシエーション] ページを使用して CP インスタンスを VAP に関連付けます。関連付けられた CP インスタンス設定は、VAP で認証を試みるユーザに適用されます。

VAP へのインスタンスの関連付け

インスタンスを VAP に関連付けるには

ステップ 1 [キャプティブ ポータル]、[インスタンス アソシエーション] の順に選択します。

ステップ 2 設定する無線を選択します。

ステップ 3 インスタンスを関連付ける VAP ごとに、インスタンス名を選択します。

ステップ 4 [保存] をクリックします。変更がスタートアップ コンフィギュレーションに保存されます。

Web ポータルのカスタマイズ

CP インスタンスを VAP に関連付けたら、ロケール（認証 Web ページ）を作成して、それを CP インスタンスにマッピングする必要があります。CP インスタンスに関連付けられた VAP にユーザがアクセスすると、認証ページが表示されます。

[Web ポータルのカスタマイズ] ページを使用して、ネットワーク上の異なるロケールに一意のページを作成し、ページのテキストとイメージをカスタマイズします。

CP 認証ページの設定

CP 認証ページの作成およびカスタマイズ

CP 認証ページを作成およびカスタマイズするには、次の手順を実行してください。

ステップ 1 [キャプティブ ポータル]、[Web ポータルのカスタマイズ] の順に選択します。

ステップ 2 [キャプティブ ポータル Web ロケール] リストから [作成] を選択します。

ネットワーク上の異なるロケールによって最大 3 つの異なる認証ページを作成できます。

ステップ 3 [キャプティブ ポータル Web ロケール パラメータ] エリアで、次のパラメータを設定します。

- [Web ロケール名]: ページに割り当てる Web ロケールの名前を入力します。この名前は 1 ～ 32 文字の英数字で指定できます。
- [キャプティブ ポータル インスタンス]: このロケールが関連付けられる CP インスタンスを選択します。1 つのインスタンスに複数のロケールを関連付けることができます。CP インスタンスに関連付けられた特定の VAP にユーザがアクセスを試みると、そのインスタンスに関連付けられたロケールが認証ページがリンクとして表示されます。ユーザは、リンクを選択してそのロケールに切り替えることができます。

ステップ 4 [保存] をクリックします。変更がスタートアップ コンフィギュレーションに保存されます。

ステップ 5 [キャプティブ ポータル Web ロケール パラメータ] エリアが、ロケールを変更するための追加のオプションとともに再表示されます。[ロケール ID] フィールドと [インスタンス名] フィールドは編集できません。編集可能なフィールドにはデフォルト値が表示されます。

ステップ 6 次のパラメータを設定します。

- [背景イメージ名]: ページの背景として表示されるイメージを選択します。[カスタムイメージのアップロード/削除] をクリックして、CP インスタンス用のイメージをアップロードできます。詳細については、「イメージのアップロードおよび削除」を参照してください。
- [ロゴイメージ名]: ページの左上隅に表示されるイメージファイルを選択します。このイメージは、ブランディング（企業のロゴなど）のために使用されます。カスタム ロゴイメージを WAP デバイスにアップロードする場合、それをリストから選択できます。
- [前景の色]: 前景の色の HTML コードを 6 桁の 16 進数の形式で入力します。1 ～ 32 文字で入力します。デフォルトは #999999 です。
- [背景の色]: 背景の色の HTML コードを 6 桁の 16 進数の形式で入力します。1 ～ 32 文字で入力します。デフォルトは #BFBFBF です。
- [セパレータ]: ページの見出し部とページの本文部を区切る太い横線の色の HTML コードを 6 桁の 16 進数の形式で入力します。1 ～ 32 文字で入力します。デフォルトは #BFBFBF です。

- [ロケール ラベル]:ロケールを説明するラベルを 1 ～ 32 文字で入力します。デフォルトのロケールは English です。
- [ロケール]:ロケールの略語を 1 ～ 32 文字で入力します。デフォルトは en です。
- [アカウントイメージ]:認証されたログインを示すためにログイン フィールドの上に表示されるイメージファイルを選択します。
- [アカウント ラベル]:ユーザ名の入力をユーザに指示するテキストです。1 ～ 32 文字で入力します。
- [ユーザ ラベル]:ユーザ名テキスト ボックスのラベルです。1 ～ 32 文字で入力します。
- [パスワード ラベル]:ユーザ パスワード テキスト ボックスのラベルです。1 ～ 64 文字で入力します。
- [ボタン ラベル]:認証のためにユーザがユーザ名とパスワードを送信する際にクリックするボタンのラベルです。2 ～ 32 文字で入力します。デフォルトは Connect です。
- [フォント]:CP ページのすべてのテキストに使用されるフォントの名前です。各フォントをカンマで区切ることにより複数のフォントを入力できます。最初のフォントをクライアント システムで使用できない場合は次のフォントが使用され、以降同様です。スペースが含まれるフォント名については、名前全体を引用符で囲みます。1 ～ 512 文字で入力します。デフォルトは MS UI ゴシック、Arial、sans-serif です。
- [ブラウザ タイトル]:ブラウザのタイトル バーに表示されるテキストです。1 ～ 128 文字で入力します。デフォルトは Captive Portal です。
- [ブラウザ コンテンツ]:ページ見出し部のロゴの右に表示されるテキストです。1 ～ 128 文字で入力します。デフォルトは Welcome to the Wireless Network です。
- [コンテンツ]:ページ本文部のユーザ名とパスワードのテキスト ボックスの下に表示される指示的なテキストです。1 ～ 256 文字で入力します。デフォルトは To start using this service, enter your credentials and click the connect button. です。
- [利用規約]:[利用規約] ボックスに表示されるテキストです。1 ～ 4096 文字で入力します。デフォルトは [利用規約] です。
- [同意ラベル]:利用規約を読んで同意したことを確認するためにチェック ボックスをオンにすることをユーザに指示するテキストです。1 ～ 128 文字で入力します。

- [同意なしテキスト]:ユーザが [利用規約] チェック ボックスをオンにしないでログイン資格情報を送信する場合にポップアップ ウィンドウに表示されるテキストです。1 ～ 128 文字で入力します。
- [処理中作業テキスト]:認証時に表示されるテキストです。1 ～ 128 文字で入力します。
- [拒否テキスト]:ユーザが認証に失敗したときに表示されるテキストです。1 ～ 128 文字で入力します。
- [ウェルカム タイトル]:クライアントが VAP に対して認証されたときに表示されるテキストです。1 ～ 128 文字で入力します。
- [ウェルカム コンテンツ]:クライアントがネットワークに接続されたときに表示されるテキストです。1 ～ 256 文字で入力します。
- [ロケールの削除]:現在のロケールを削除します。

ステップ 7 [保存] をクリックします。変更がスタートアップ コンフィギュレーションに保存されます。

ステップ 8 [プレビュー] をクリックすると、更新されたページが表示されます。

注 [プレビュー] をクリックすると、すでにスタートアップ コンフィギュレーションに保存されているテキストとイメージが表示されます。変更を加えた場合、変更を確認するには、[プレビュー] をクリックする前に [保存] をクリックしてください。

イメージのアップロードおよび削除

CP インスタンスに関連付けられた VAP へのアクセスをユーザが開始すると、認証ページが表示されます。この認証ページは、独自のロゴまたはその他のイメージでカスタマイズできます。

最大 18 のイメージをアップロードできます(それぞれが 3 つのイメージを持つ 6 つのロケールを前提としています)。すべてのイメージは、5 KB 以下で、GIF または JPG 形式である必要があります。

イメージは、指定された寸法に適合するようにサイズが変更されます。最良の結果を得るには、ロゴおよびアカウントイメージは、次のように、デフォルトのイメージと似た比率である必要があります。

イメージタイプ	目的	デフォルトの幅 X 高さ
背景	ページの背景として表示されます。	10 X 800 ピクセル
ロゴ	ブランディング情報を提供するためにページの左上に表示されます。	168 X 78 ピクセル
アカウント	認証されたログインを示すためにログイン フィールドの上に表示されます。	295 X 55 ピクセル

WAP デバイスへのバイナリ グラフィック ファイルのアップロード

バイナリ グラフィック ファイルを WAP デバイスにアップロードするには

ステップ 1 [Web ポータルのカスタマイズ] ページで、[背景イメージ名]、[ロゴイメージ名]、または [アカウントイメージ] フィールドの横にある [カスタムイメージのアップロード/削除] をクリックします。

[Web ポータル カスタムイメージ] ページが表示されます。

ステップ 2 [参照] をクリックしてイメージを選択します。

ステップ 3 [アップロード] をクリックします。

ステップ 4 [戻る] をクリックして [Web ポータル カスタムイメージ] ページに戻ります。

ステップ 5 [キャプティブ ポータル Web ロケール] で、設定するロケールを選択します。

ステップ 6 [背景イメージ名]、[ロゴイメージ名]、または [アカウントイメージ] フィールドで、新しくアップロードされたイメージを選択します。

ステップ 7 [保存] をクリックします。

ステップ 8 イメージを削除するには、[Web ポータル カスタムイメージ] ページで、[Web カスタマイズイメージを削除] リストからイメージを選択し、[削除] をクリックします。デフォルトのイメージは削除できません。

認証済みクライアント

[認証済みクライアント] ページには 2 つのテーブルが表示されます。一つは、いずれかのキャプティブ ポータル インスタンスで認証済みのクライアントに関する [認証済みクライアント] テーブルです。もう一つは、キャプティブ ポータルで認証を試みて失敗したクライアントに関する情報を示す [認証に失敗したクライアント] テーブルです。

認証済みクライアントまたは認証に失敗したクライアントのリストを表示するには、[キャプティブ ポータル]、[認証済みクライアント] の順に選択します。次の情報が表示されます。

- [MAC アドレス]: クライアントの MAC アドレスです。
- [IP アドレス]: クライアントの IP アドレスです。
- [ユーザ名]: クライアントのキャプティブ ポータル ユーザ名です。
- [プロトコル]: ユーザが接続を確立するために使用したプロトコル（HTTP または HTTPS）です。
- [検証]: キャプティブ ポータルでのユーザ認証に使用される方式で、値は次のいずれかです。
  - [ゲスト]: このユーザは、データベースによって認証される必要がありません。
  - [ローカル]: この WAP デバイスは、ローカル データベースを使用してユーザを認証します。
  - [RADIUS]: この WAP デバイスは、リモート RADIUS サーバ上のデータベースを使用してユーザを認証します。
- [VAP ID]: ユーザが関連付けられている VAP です。
- [無線 ID]: 無線 ID です。
- [キャプティブ ポータル ID]: ユーザが関連付けられているキャプティブ ポータル インスタンスの ID です。
- [セッション タイムアウト]: CP セッションが有効であるための残り時間（秒単位）です。この時間が 0 に達すると、クライアントの認証が解除されます。
- [退席中タイムアウト]: クライアント エントリが有効であるための残り時間（秒単位）です。クライアントの CP との関連付けが解除されると、タイマーが起動します。この時間が 0 に達すると、クライアントの認証が解除されます。

- [受信パケット数]:WAP デバイスによってユーザ ステーションから受信された IP パケットの数です。
- [送信パケット数]:WAP デバイスからユーザ ステーションに送信された IP パケットの数です。
- [受信バイト数]:WAP デバイスによってユーザ ステーションから受信されたバイト数です。
- [送信バイト数]:WAP デバイスからユーザ ステーションに送信されたバイト数です。
- [障害時刻]:認証障害が発生した時間です。障害の時刻を示すタイムスタンプが含まれています。

[更新] をクリックすると、WAP デバイスからの最新データが表示されます。

12

シングル ポイント設定

ここでは、複数の WAP デバイスにわたるシングル ポイント設定を設定する方法について説明します。

具体的な内容は、次のとおりです。

- シングル ポイント設定の概要
- アクセス ポイント
- セッション
- チャネル管理
- ワイヤレス ネイバーフッド
- クラスタ ファームウェアのアップグレード

シングル ポイント設定の概要

シングル ポイント設定は、複数のデバイスにわたってワイヤレス サービスを管理および制御するための一元化された方法を提供します。シングル ポイント設定を使用すると、ワイヤレス デバイスの単一のグループ（クラスタ）を作成することができます。WAP デバイスをクラスタ化すると、ワイヤレス ネットワークを単一のエンティティとして表示、展開、設定、および保護することができます。ワイヤレス クラスタの作成後は、シングル ポイント設定により、無線干渉を削減し、ワイヤレス ネットワーク上の帯域幅を最大化するためのワイヤレス サービス全体にわたるチャネル計画も容易になります。

WAP デバイスの初期セットアップ時には、セットアップ ウィザードを使用してシングル ポイント設定を設定するか既存のシングル ポイント設定に参加させることができます。セットアップ ウィザードを使用せずに、Web ベースの設定ユーティリティを使用することもできます。

複数のアクセス ポイントにわたるシングル ポイント設定の管理

シングル ポイント設定により、ネットワークの同じサブネット内に存在する WAP デバイスの動的な設定認識型クラスタ（グループ）が作成されます。1 つのクラスタは最大 16 台の設定済み WAP571/E デバイスのグループをサポートします。ただし、同じクラスタでは、WAP571/E 以外のモデルの他のデバイスはサポートされません。

シングル ポイント設定では、同じサブネットまたはネットワーク内の複数のクラスタを管理できますが、それらは単一の独立したエンティティとして管理されます。次の表に、シングル ポイント設定のワイヤレス サービスの制限を示します。

グループ/クラスタ タイプ	シングル ポイント設定あたりの WAP デバイス数	シングル ポイント設定あたりのアクティブ クライアント数	クライアントの最大数（アクティブおよびアイドル）
WAP571/E	16	960（WAP571/E、デュアル無線）	2048（WAP571/E、デュアル無線）

クラスタは、VAP 設定、QoS キュー パラメータ、無線パラメータなどの設定情報を伝達できます。あるデバイスでシングル ポイント設定を設定すると、そのデバイスの設定（手動設定であってもデフォルト設定であっても）は、他のデバイスがクラスタに参加する場合にそれらのデバイスに伝達されます。

クラスタ形成の前提手順および条件

クラスタを形成するには、次の前提手順または条件が満たされていることを確認する必要があります。

ステップ 1 シングル ポイント設定クラスタを計画します。クラスタ化する複数の WAP デバイスについて、相互に互換性があることを確認してください。たとえば、Cisco WAP571/E デバイスは他の Cisco WAP571/E デバイスとのみクラスタ化できます。

注 クラスタ化されたすべての WAP デバイスで最新バージョンのファームウェアを実行することを強くお勧めします。ファームウェアのアップグレードは、クラスタ内のすべての WAP デバイスに伝達されません。そのため、各デバイスを個別にアップグレードする必要があります。

ステップ 2 同じ IP サブネット上でクラスタ化する WAP デバイスをセットアップし、それらが相互に接続されていることとスイッチド LAN ネットワーク全体でアクセス可能であることを確認します。

ステップ 3 すべての WAP デバイスでシングル ポイント設定を有効にします。「アクセス ポイント」を参照してください。

ステップ 4　すべての WAP デバイスが同じシングル ポイント設定名を参照することを確認します。「アクセス ポイント」を参照してください。

シングル ポイント設定のネゴシエーション

シングル ポイント設定に関して AP を有効にして設定すると、AP は、そのプレゼンスを通知する定期的なアドバタイズメントの送信（10 秒間隔）を開始します。クラスタの基準に合致する他の WAP デバイスが存在する場合、調停が開始され、どの WAP デバイスがクラスタの残りのメンバーにマスター設定を配信するかが決定されます。

シングル ポイント設定のクラスタ形成および調停には次のルールが適用されます。

- 既存のシングル ポイント設定クラスタについては、管理者がクラスタのいずれかのメンバーの設定を更新するたびに、その設定変更がクラスタのすべてのメンバーに伝達され、設定された WAP デバイスがクラスタの制御を担当するようになります。
- 2 つの個別のシングル ポイント設定クラスタを単一のクラスタに参加させると、最後に変更されたクラスタが設定の調停において優先され、クラスタ化されたすべての WAP デバイスの設定を上書きし、更新します。
- クラスタ内の WAP デバイスが別のある WAP デバイスから 60 秒以上にわたってアドバタイズメントを受信しない場合（そのデバイスがクラスタ内の他のデバイスとの接続を失っている場合など）、そのデバイスはクラスタから削除されます。
- シングル ポイント設定モードの WAP デバイスは、接続を失ってもすぐにはクラスタからドロップされません。デバイスが接続を回復し、ドロップされずにクラスタに再参加する場合、接続を失っている間にそのデバイスに対して設定変更が行われると、接続の再開時にその変更が他のクラスタ メンバーに伝達されます。
- クラスタ内の WAP デバイスが接続を失い、ドロップされた後にクラスタに再参加する場合、接続を失っている間に設定変更が行われると、再参加時にそのデバイスに変更が伝達されます。接続を失ったデバイスとクラスタの両方で設定変更が行われた場合、最も変更数の多いデバイス（副次的な条件として最後に変更されたデバイス）が選択され、その変更がクラスタに伝達されます（たとえば、WAP1 の変更数が最も多いが WAP2 が最後に変更された場合は WAP1 が選択され、これらの変更数が同じであるが WAP2 が最後に変更された場合は WAP2 が選択されます）。

シングル ポイント設定からドロップされたデバイスの動作

以前にクラスタのメンバーだった WAP デバイスがクラスタから切断された場合は、次のガイドラインが適用されます。

- クラスタとのコンタクトを失うと、WAP デバイスは、最新の動作設定を受け取れなくなります。この切断により、実稼働ネットワーク全体にわたる厳密な意味でのシームレスなワイヤレス サービスが停止します。
- WAP デバイスは、クラスタから最後に受け取ったワイヤレス パラメータで機能しつづけます。
- このクラスタ化されていない WAP デバイスに関連付けられているワイヤレス クライアントは、引き続きこのデバイスに関連付けられ、ワイヤレス接続が中断されることはありません。つまり、クラスタとの接続を失っても、その WAP デバイスに関連付けられたワイヤレス クライアントは、必ずしも引き続きネットワーク リソースにアクセスすることが不可能になるわけではありません。
- クラスタとの接続を失った原因が LAN インフラストラクチャとの物理的または論理的接続の切断である場合は、障害の性質に応じて、そのワイヤレス クライアントに対するネットワーク サービスが影響を受ける可能性があります。

次の表に、クラスタ化されたすべての WAP デバイス間で共有され、伝達される設定を示します。

シングル ポイント設定アクセス ポイントに伝達される設定パラメータと伝達されない設定パラメータ

シングル ポイント設定で伝達される一般設定およびパラメータ	
キャプティブ ポータル	パスワードの複雑性
クライアント QoS	ユーザ アカウント
電子メール アラート	QoS
HTTP/HTTPサービス（SSL 証明書設定を除く）	TSpec設定を含む無線設定（一部例外あり）
ログ設定	不正 AP 検出
MAC フィルタリング	スケジューラ
管理アクセス制御	SNMP 全般および SNMPv3
ネットワーク	WPA-PSK 複雑性
時間設定	ワイヤレス マルチキャスト転送
LED ディスプレイ	
LLDP（POE プライオリティ設定を除く）	
Umbrella	

シングル ポイント設定で伝達される無線設定およびパラメータ
モード
フラグメンテーションしきい値
RTS しきい値
レート セット
プライマリ チャネル
保護
固定マルチキャスト レート
ブロードキャストまたはマルチキャスト レート上限
チャネル帯域幅
サポートされるショート ガード インターバル

シングル ポイント設定で伝達されない無線設定およびパラメータ
チャネル
ビーコンの間隔
DTIM 期間
最大ステーション数
送信電力

シングル ポイント設定で伝達されないその他の設定およびパラメータ	
帯域使用率	ポート設定
Bonjour	VLAN および IPv4
IPv6 アドレス	WDS ブリッジ
IPv6 トンネル	
パケット キャプチャ	ワークグループ ブリッジ

アクセス ポイント

[アクセス ポイント] ページでは、WAP デバイスでのシングル ポイント設定を有効または無効にしたり、クラスタ メンバーを表示したり、メンバーの場所やクラスタ名を設定したりすることができます。また、メンバーの IPアドレスをクリックして、そのデバイス上のデータを設定および表示することができます。

シングル ポイント設定に関する WAP デバイスの設定

シングル ポイント設定クラスタの個々のメンバーの場所および名前を設定するには、次の手順を実行してください。

ステップ 1 ナビゲーション ウィンドウで、[シングル ポイント設定]、[アクセス ポイント] の順に選択します。

AP ではシングル ポイント設定はデフォルトで無効になっています。無効になっている場合は、[シングル ポイント設定の有効化] ボタンが表示されます。シングル ポイント設定が有効になっている場合は、[シングル ポイント設定の無効化] ボタンが表示されます。シングル ポイント設定が無効のときにのみシングル ポイント設定のオプションを編集できます。

このページの右側にあるアイコンは、シングル ポイント設定が有効かどうかを示し、有効になっている場合は、現在クラスタに参加している WAP デバイスの番号も示します。

ステップ 2 シングル ポイント設定が無効の状態で、シングル ポイント設定 クラスタの個別のメンバーごとに次の情報を設定します。

- [場所]:「Reception」(待合室)などのように、アクセスポイントが配置されている物理的な場所の説明を入力します。この場所を入力するフィールドはオプションです。
- [クラスタ名]:「Reception_Cluster」などのように、WAP デバイスが参加するクラスタの名前を入力します。

  このクラスタ名は、他の WAP デバイスには送信されません。メンバーになっている各デバイスで同じ名前を設定する必要があります。クラスタ名は、ネットワークで設定するシングル ポイント設定ごとに一意である必要があります。デフォルトは ciscosb-cluster です。
- [クラスタリング IP バージョン]: クラスタ内の WAP デバイスがクラスタの他のメンバーと通信するために使用する IP バージョンを指定します。デフォルトは IPv4 です。

IPv6 を選択する場合、シングル ポイント設定は、リンクローカル アドレス、自動設定される IPv6 グローバル アドレス、および静的に設定される IPv6 グローバル アドレスを使用できます。IPv6 を使用する場合は、クラスタ内のすべての WAP デバイスがリンクローカル アドレスのみを使用するかグローバル アドレスのみを使用するかのいずれかであることを確認してください。

シングル ポイント設定は、同じタイプの IP アドレッシングを使用するデバイスでのみ機能します。一部のデバイスが IPv4 アドレスを持ち、一部のデバイスが IPv6 アドレスを持つ WAP デバイスのグループでは機能しません。

ステップ 3 [シングル ポイント設定の有効化] をクリックします。

WAP デバイスが、サブネット内の同じクラスタ名と IP バージョンが設定されている他の WAP デバイスの検索を開始します。潜在的なクラスタ メンバーは、そのプレゼンスを通知するアドバタイズメントを 10 秒間隔で送信します。

他のクラスタ メンバーの検索中は、設定を適用中であることがステータスによって示されます。ページを更新して新しい設定を確認します。

1 台または複数の WAP デバイスが同じクラスタ設定ですでに設定されている場合、その WAP デバイスはクラスタに参加し、各メンバーに関する情報がテーブルにされます。

ステップ 4 シングル ポイント設定に参加させる追加の WAP デバイスについて、上記の手順を繰り返します。

シングル ポイント設定情報の表示

シングル ポイント設定が有効になっている場合、AP は、同じ設定の他の WAP デバイスと自動的にクラスタを形成します。[アクセス ポイント] ページに、検出された WAP デバイスのリストがテーブルに表示され、次の情報が示されます。

- [場所]: アクセスポイントが配置されている物理的な場所の説明です。
- [MAC アドレス]: アクセス ポイントの Media Access Control（MAC）アドレスです。このアドレスは、ブリッジ（br0）の MAC アドレスです。WAP デバイスは、このアドレスによって外部（他のネットワーク）から認識されます。
- [IP アドレス]: アクセス ポイントの IPアドレスです。

シングル ポイント設定のステータスと WAP デバイス数がページの右側にグラフィカルに表示されることに注意してください。

シングル ポイント設定へのアクセス ポイントの追加

現在スタンドアロン モードになっている新しいアクセス ポイントをシングル ポイント設定に追加するには

ステップ 1 スタンドアロン アクセス ポイントの Web ベースの設定ユーティリティにアクセスします。

ステップ 2 ナビゲーション ウィンドウで、[シングル ポイント設定]、[アクセス ポイント] の順に選択します。

ステップ 3 [クラスタ名] をクラスタのメンバーに対して設定されている名前に設定します。

ステップ 4 (オプション) [場所] フィールドに、「Reception」(待合室) などのように、アクセスポイントが配置されている物理的な場所の説明を入力します。

ステップ 5 [シングル ポイント設定の有効化] をクリックします。

アクセス ポイントが自動的にシングル ポイント設定に参加します。

シングル ポイント設定からのアクセス ポイントの削除

シングル ポイント設定クラスタからアクセス ポイントを削除するには

ステップ 1 検出されたデバイスが表示されたテーブルで、削除するクラスタ化された WAP デバイスの IPアドレスをクリックします。

その WAP デバイス用の Web ベースの設定ユーティリティが表示されます。

ステップ 2 ナビゲーション ウィンドウで、[シングル ポイント設定]、[アクセス ポイント] の順に選択します。

ステップ 3 [シングル ポイント設定の無効化] をクリックします。

そのアクセス ポイントの [シングル ポイント設定] ステータス フィールドに [無効] と表示されるようになります。

特定デバイスの設定情報へのアクセス

シングル ポイント設定クラスタ内のすべての WAP デバイスには同じ設定が反映されます (設定項目が伝達可能である場合)。管理のためにどの WAP デバイスに接続しているかは問題ではありません。クラスタ内のどの WAP デバイスでの設定変更も他のメンバーに伝達されます。

ただし、特定の WAP デバイスの情報を表示または管理したい場合もある可能性があります。たとえば、あるアクセス ポイントのクライアント関連付けまたはイベントなどのステータス情報を確認したい場合などです。そのようなときは、[アクセス ポイント] ページのテーブルの IPアドレスをクリックして、特定のアクセス ポイント用の Web ベースの設定ユーティリティを表示することができます。

IPアドレスを使用した URL によるデバイスへのアクセス

特定のアクセス ポイントの IPアドレスを次の形式で URL として Webブラウザのアドレス バーに直接入力することによって、その WAP デバイスの Web ベースの設定ユーティリティにアクセスすることもできます。

http://IPAddressOfAccessPoint（HTTP を使用する場合）

https://IPAddressofAccessPoint（HTTPS を使用する場合）

セッション

[セッション] ページには、シングル ポイント設定クラスタの WAP デバイスに関連付けられた WLAN クライアントに関する情報が表示されます。各 WLAN クライアントは、その MAC アドレスと、そのクライアントが現在接続されているデバイスの場所によって識別されます。

注 [セッション] ページには、クラスタ化された WAP デバイス上の無線あたり最大 20 のクライアントが表示されます。特定の WAP デバイスに関連付けられたすべての WLAN クライアントを確認するには、直接そのデバイスで [ステータス]、[関連付けられたクライアント] ページの順に選択します。

WLAN クライアント セッションの特定の統計情報を表示するには、[表示] リストから項目を選択して、[開始] をクリックします。アイドル時間、データ レート、および信号強度に関する情報を表示できます。

この文脈での「セッション」とは、一意の MAC アドレスを持つクライアントデバイス（ステーション）上のユーザがワイヤレス ネットワークとの接続を維持する期間を指します。セッションは、WLAN クライアントがネットワークにログオンすると開始され、その WLAN クライアントが意図的にログオフするか何らかの他の理由によって接続を失うと終了します。

注 「セッション」は、特定のアクセス ポイントへの WLAN クライアント接続を指す「関連付け」とは異なります。WLAN クライアントの関連付けは、同じセッション内で、あるクラスタ化されたアクセス ポイントから別のクラスタ化されたアクセス ポイントへと移行できます。

クラスタに関連付けられたセッションを表示するには、[シングル ポイント設定]、[セッション] の順に選択します。

シングル ポイント設定による WLAN クライアント セッションごとに次のデータが表示されます。

- [AP の場所]: アクセス ポイントの場所です。

  この場所は、[管理]、[システム設定] の順に選択すると表示されるページで指定した場所から取得されます。

- [ユーザ MAC]: ワイヤレス クライアントの MAC アドレスです。

  MAC アドレスは、ネットワークの各ノードを一意に識別するハードウェア アドレスです。

- [アイドル]: この WLAN クライアントが非アクティブ状態になっていた時間の合計です。

  WLAN クライアントは、データを送受信していないときは非アクティブになっていると見なされます。

- [レート]: ネゴシエーションされたデータ レートです。実際の転送レートはオーバーヘッドによって異なる場合があります。

  データ転送レートは、メガビット/秒（Mbps）単位で測定されます。この値は、アクセス ポイントで使用されているモードに関して設定されているアドバタイズ レートの範囲内になります。たとえば、802.11a の場合は 6～54 Mbps です。

  レポートされるレートは、AP からクライアントに最後に送信されたパケットの速度です。この値は、AP とクライアント間の信号品質およびブロードキャストまたはマルチキャスト フレームが送信されるレートに基づいて設定されるアドバタイズ レート内で変化する可能性があります。AP がデフォルトのレートで STA にブロードキャスト フレームを送信する場合、このフィールドでは 1 Mbps（2.4Ghz 無線の場合）および 6 Mbps（5 GHz 無線の場合）とレポートされます。アイドル状態のクライアントについては、ほとんどの場合、低いデフォルト レートがレポートされます。

- [信号]: WLAN クライアントがアクセス ポイントから受信する無線周波数（RF）信号の強度です。この測定値は「受信信号強度表示（RSSI）」と呼ばれ、0～100の値になります。

- [総受信量]: 現在のセッション中に WLAN クライアントによって受信されたパケットの総数です。

- [総送信量]: 現在のセッション中に WLAN クライアントによって送信されたパケットの総数です。

- [エラー レート]: このアクセス ポイントで転送中にドロップしたタイム フレームのパーセンテージです。

テーブルに示される情報を特定のインジケータによってソートするには、ソートする列のラベルをクリックします。たとえば、信号強度の順にテーブルの行を並べ替えるには、[信号] 列のラベルをクリックします。

チャネル管理

[チャネル管理] ページには、シングル ポイント設定クラスタの WAP デバイスに関する現在のチャネル割り当てと計画されているチャネル割り当てが表示されます。

チャネル管理が有効になっている場合、シングル ポイント設定クラスタの WAP デバイスによって使用される無線チャネルを自動的に割り当てます。自動チャネル割り当てにより、相互干渉（またはクラスタ外部の他の WAP デバイスとの干渉）が軽減され、Wi-Fi の帯域幅が最大化されるため、ワイヤレス ネットワーク経由の効率的な通信を維持するために役立ちます。

自動チャネル割り当て機能はデフォルトで無効になっています。チャネル管理の状態（有効または無効）は、シングル ポイント設定クラスタの他のデバイスに伝達されます。

チャネル マネージャ（つまり、クラスタに設定を提供するデバイス）は、指定された間隔で、すべてのクラスタ化された WAP デバイスを異なるチャネルにマッピングし、クラスタ メンバーの干渉レベルを測定します。重大なチャネル干渉が検出された場合、チャネルマネージャは、効率性アルゴリズム（または自動チャネル計画）に従って一部またはすべてのデバイスの新しいチャネルへの再割り当てを自動的に行います。変更が必要であるとチャネル マネージャが判断した場合、再割り当て情報がクラスタのすべてのメンバーに送信されます。送信デバイスと新旧のチャネル割り当てを示す syslog メッセージも生成されます。

シングル ポイント設定メンバーのチャネル割り当ての設定および表示

シングル ポイント設定メンバーのチャネル割り当てを設定および表示するには

ステップ 1 ナビゲーション ウィンドウで、[シングル ポイント設定]、[チャネル管理] の順に選択します。

[チャネル管理] ページでは、クラスタ内のすべての WAP デバイスのチャネル割り当てを表示し、自動チャネル管理を停止または開始することができます。また、詳細設定を使用して、チャネル再割り当てをトリガーする干渉軽減のレベルを修正したり、自動更新のスケジュールを変更したり、割り当てに使用されるチャネルセットを再設定したりすることもできます。

ステップ 2 自動チャネル割り当てを開始するには、[開始] をクリックします。

チャネル管理は、クラスタに含まれるすべての WAP デバイスの無線チャネルを同期させるデフォルトのクラスタ動作よりも優先されます。チャネル管理が有効になっている場合、無線チャネルは、クラスタ全体にわたって他のデバイスと同期されません。

自動チャネル割り当てが有効になっている場合、チャネルマネージャは、シングル ポイント設定クラスタの WAP デバイスによって使用される無線チャネルを定期的にマッピングし、必要であれば、チャネルの再割り当てを行って、クラスタ メンバーまたはクラスタ外部のデバイスとの干渉を軽減します。無線のチャネル ポリシーは自動的に静的モードに設定されます。また、[ワイヤレス]、[無線] の順に選択すると表示されるページの [チャネル] フィールドについては、[自動] オプションを使用できません。

現在のチャネル割り当ておよび推奨チャネル割り当てについては、[チャネル割り当ての表示およびロックの設定] を参照してください。

ステップ 3 自動チャネル割り当てを停止するには、[停止] をクリックします。

チャネル使用のマッピングまたはチャネルの再割り当ては行われなくなります。手動での更新のみがチャネルの割り当てに影響します。

[チャネル割り当ての表示およびロックの設定]

チャネル管理が有効になっている場合、このページには、[現在のチャネル割り当て] テーブル と[推奨チャネル割り当て] テーブルが表示されます。

[現在のチャネル割り当て] テーブル

[現在のチャネル割り当て] テーブルには、シングル ポイント設定クラスタの WAP デバイスの IPアドレスごとのリストが表示されます。

このテーブルには、現在のチャネル割り当てに関する次の詳細情報が示されます。

- [場所]: デバイスの物理的な場所です。
- [IP アドレス]: アクセス ポイントの IPアドレスです。
- [ワイヤレス無線]: 無線の MAC アドレスです。
- [帯域]: アクセス ポイントがブロードキャストしている帯域です。
- [チャネル]: このアクセス ポイントが現在ブロードキャストしている無線チャネルです。
- [ロック済み]: アクセス ポイントが強制的に現在のチャネルに固定されます。
- [ステータス]: デバイスのワイヤレス無線のステータスを示します（一部の WAP デバイスが持つことのできる複数のワイヤレス無線は、それぞれテーブルの個別の行に表示されます）。無線のステータスは、アップ（稼働している）またはダウン（稼働していない）です。

アクセス ポイントに関して、自動チャネル管理計画が選択されている場合、最適化戦略の一環として WAP デバイスの異なるチャネルへの再割り当てが行われることはありませんが、チャネルにロックされている WAP デバイスは計画の要件として考慮に入れられます。

ロック設定を更新するには [保存] をクリックします。ロックされているデバイスでは、[現在のチャネル割り当て]テーブルと[推奨チャネル割り当て] テーブルに同じチャネルが表示されます。ロックされているデバイスについては、現在のチャネルが維持されます。

[推奨チャネル割り当て] テーブル

[推奨チャネル割り当て] テーブルには、次回の更新時に各 WAP デバイスに割り当てられる予定の推奨チャネルが表示されます。ロックされたチャネルの再割り当ては行われず、デバイス間のチャネル分配の最適化では、ロックされたデバイスが現在のチャネルに留まる必要があることが考慮されます。ロックされていない WAP デバイスは、計画の結果に応じて、それらのデバイスが使用していたものとは異なるチャネルに割り当てられる場合があります。

[推奨チャネル割り当て] テーブルには、[現在のチャネル割り当て] テーブルと同様に、シングル ポイント設定の各 WAP デバイスの場所、IPアドレス、およびワイヤレス無線が示されます。また、推奨チャネル（チャネル計画が適用されるとこの WAP デバイスが割り当てられる無線チャネル）も示されます。

詳細設定の設定

[詳細設定] エリアでは、シングル ポイント設定のチャネル計画のカスタマイズおよびスケジュール設定を行うことができます。

デフォルトでは、干渉を 25% 以上軽減できる場合にのみ、チャネルの再割り当てが 1 時間ごとに自動的に行われます。チャネルの再割り当ては、ネットワークがビジー状態の場合にも行われます。デフォルト設定は、チャネル管理を実装する必要があるほとんどのシナリオに適合するように設計されています。

詳細設定を変更することにより、次の設定を設定できます。

- [干渉が最低でも以下に減った場合にチャネルを変更します]: 推奨計画が適用されるために達成する必要のある干渉軽減の最小パーセンテージです。デフォルトは 75 % です。ドロップダウン メニューを使用して、5～75 % の範囲でパーセンテージを選択します。この設定を使用すると、わずかな効率性の改善のためにネットワークが継続的に中断されることを防止するために、チャネルの再割り当てに関する効率性改善のしきい値を設定できます。

  たとえば、チャネル干渉が 75 %以上軽減される必要があり、推奨チャネル割り当てでは30%しか干渉が軽減されない場合、チャネルの再割り当てが行われません。ただし、最小チャネル干渉軽減を 25 % に再設定し、[保存] をクリックすると、推奨チャネル計画が実装され、必要に応じてチャネルの再割り当てが行われます。

- [次の時間ごとにチャネルの改善が可能か確認する]: 自動更新のスケジュールです。この間隔は、30 分～6 ヵ月の範囲で指定されます。

  デフォルトは 1 時間です。つまり、1 時間ごとにチャネルの使用率が再評価され、その結果として生成されたチャネル計画が適用されます。

これらの設定を変更する場合は、[保存] をクリックしてください。変更がアクティブなコンフィギュレーションとスタートアップ コンフィギュレーションに保存されます。

ワイヤレス ネイバーフッド

[ワイヤレス ネイバーフッド] ページには、クラスタの各ワイヤレス無線の範囲に含まれる無線ごとに最大 20 台のデバイスが表示されます（たとえば、WAP デバイスに 2 つのワイヤレス無線がある場合、このデバイスに関して 40 台のデバイスが表示されます）。[ワイヤレス ネイバーフッド] ページでは、クラスタのメンバーと非メンバーも区別されます。

[ワイヤレス ネイバーフッド] ビューは、次の作業に役立ちます。

- ワイヤレス ドメイン内の予期しない（または不正な）デバイスを検出して、位置を特定することにより、関連するリスクを制限するための措置を講じることを可能にします。
- 期待できるカバレッジを確認します。認識可能な WAP デバイスや、他のデバイスからの信号強度を評価することにより、展開によって計画の目標が達成されることを確認できます。
- 障害を検出します。カバレッジ パターンの予期しない変化を、色分けされたテーブルによって一目で明瞭に確認できます。

近接するデバイスを表示するには、[シングル ポイント設定]、[ワイヤレス ネイバーフッド] の順に選択します。特定のシングル ポイント設定で検出されたすべてのデバイスを表示するには、メンバーの Web インターフェイスにアクセスして、ナビゲーション ウィンドウで [ワイヤレス]、[不正 AP 検出] の順に選択します。

近接するアクセス ポイントごとに、次の情報が表示されます。

- [近接する AP の表示]: 次のいずれかのラジオ ボタンを選択してビューを切り替えます。
  - [クラスタ内] : クラスタのメンバーになっている近接 WAP デバイスのみが表示されます。
  - [クラスタ内にない] : クラスタのメンバーになっていない近接 WAP デバイスのみが表示されます。

- [両方] : すべての近接 WAP デバイス（クラスタのメンバーおよび非メンバー）が表示されます。

注 検出された AP がクラスタ メンバーでもある場合は、デフォルト VAP（VAP0）の SSID のみが [クラスタ内] として表示されます。AP 上の非デフォルト VAP は、[クラスタ内にない] として表示されます。

- [クラスタ]:テーブル上部のリストに、同じクラスタに含まれるすべての WAP デバイスの IP アドレスが表示されます（このリストは、[シングル ポイント設定]、[アクセス ポイント] の順に選択すると表示されるページに示されるメンバー リストと同じです）。

  クラスタに WAP デバイスが 1 台しか含まれていない場合は、WAP デバイスがそれ自体とグループ化されていることを示す 1 つの IPアドレスの列のみが表示されます。

  IP アドレスをクリックすると、特定の WAP デバイスの詳細が表示されます。

- [ネイバー]:SSID（ネットワーク名）ごとに左の列に表示される 1 台または複数のクラスタ化されたデバイスに近接するデバイスです。

ネイバーとして検出されるデバイスには、クラスタ メンバー自体が含まれる場合もあります。ネイバーがクラスタ メンバーでもある場合は、常にリストの上部に表示され、上の線が太くなり、位置を示すインジケータが含まれます。

[ネイバー] リストの各 WAP デバイスの右に表示される色付きのバーは、その列の上部に表示されている IPアドレスを持つクラスタ メンバーによって検出された、各ネイバー WAP デバイスの信号強度を示しています。これらのバーの上にマウス ポインタを移動させると、デシベル（dB）単位の信号強度を表す数字が表示されます。

シングル ポイント設定メンバーの詳細の表示

クラスタ メンバーの詳細を表示するには、ページ上部のメンバーの IP アドレスをクリックします。

[ネイバー] リストには、デバイスの次の詳細情報が表示されます。

- [SSID]:近接するアクセス ポイントのサービス セット識別子です。
- [MAC アドレス]:近接するアクセス ポイントの MAC アドレスです。
- [チャネル]:アクセス ポイントが現在ブロードキャストしているチャネルです。
- [レート]:このアクセス ポイントの現在の送信レート（Mbps 単位）です。現在のレートは、常に、[サポートされるレート] に表示されるレートのいずれかです。
- [信号]:アクセス ポイントから検出される無線信号の強度（dB 単位）です。
- [ビーコンの間隔]:アクセス ポイントによって使用されるビーコンの間隔です。

- [ビーコン日時]: このアクセス ポイントからビーコンが最後に受信された日時です。

クラスタ ファームウェアのアップグレード

クラスタは、一元化されたクラスタ ファームウェアのアップグレード機能を提供します。これにより、クラスタ内のすべての AP をドミナント AP（クラスタ コントローラ）からアップグレードできます。クラスタ ファームウェアのアップグレードは、ドミナント AP からのみ実行できます。

クラスタ ファームウェアのアップグレードのページでは、検出された WAP デバイスのリストがテーブルに表示され、次の情報が示されます。

- [場所]: アクセスポイントが配置されている物理的な場所の説明です。
- [IP アドレス]: アクセス ポイントの IPアドレスです。
- [MAC アドレス]: アクセス ポイントの Media Access Control（MAC）アドレスです。このアドレスは、ブリッジ（br0）の MAC アドレスです。WAP デバイスは、このアドレスによって外部（他のネットワーク）から認識されます。
- [現在のファームウェアのバージョン]: アクセス ポイントに関して現在実行されているファームウェアのバージョンです。
- [ファームウェアの転送ステータス]: ファームウェアのダウンロードおよび検証のステータス（None/Started/Downloaded/Success/Fail/Abort_admin/Abort_local/Dap_resigned）が示されます。
- [ファームウェアの転送進捗バー]: ファームウェアのダウンロードの経過表示バーが表示されます。

アップグレードするクラスタ メンバーの選択

アップグレードするクラスタ メンバーを選択するには、次の手順を実行してください。

ステップ 1 ナビゲーション ウィンドウで、[シングル ポイント設定]、[クラスタ ファームウェアのアップグレード] の順に選択します。

ステップ 2 アップグレードする AP のチェック ボックスをオンにします。

ステップ 3 [保存] をクリックします。

クラスタ ファームウェアのアップグレードの最新のステータスを取得するには、次の手順を実行してください。

[更新] をクリックします。

TFTP によるクラスタ メンバー上のファームウェアのアップグレード

TFTP を使用してクラスタ メンバー上のファームウェアをアップグレードするには、次の手順を実行してください。

ステップ 1 [TFTP で転送] を選択します。

ステップ 2 [送信元ファイル名] フィールドに、イメージ ファイルの名前（1 ～ 128 文字）を入力します。これには、アップロードするイメージを格納しているディレクトリのパスを含みます。

たとえば、/share/builds/ap ディレクトリにある ap_upgrade.tar イメージをアップロードするには、次のように入力します。/share/builds/ap/ap_upgrade.tar

使用するファームウェア アップグレード ファイルは、tar ファイルである必要があります。bin ファイルまたはその他の形式のファイルをアップグレードに使用しないでください。これらのタイプのファイルは機能しません。

ファイル名には、スペースや、<、>、|、\、:、(、)、&、;、#、?、*、および複数の連続するピリオドを使用できません。

ステップ 3 [TFTP サーバの IPv4 アドレス] にサーバのアドレスを入力して、[アップグレードの開始] をクリックします。

HTTP によるアップグレード

HTTP を使用してアップグレードするには、次の手順を実行してください。

ステップ 1 [HTTP で転送] を選択します。

ステップ 2 新しいファイルの名前とパスが分かっている場合は、それを [新しいファームウェア イメージ] フィールドに入力します。不明の場合は、[参照] ボタンをクリックして、ネットワーク上のファームウェア イメージ ファイルを選択します。

使用するファームウェア アップグレード ファイルは、tar ファイルである必要があります。bin ファイルまたはその他の形式のファイルをアップグレードに使用しないでください。これらのタイプのファイルは機能しません。

ステップ 3 [アップグレードの開始] をクリックして新しいファームウェア イメージを適用します。

注 [全体的なアップグレード ステータス] に、すべてのクラスタ メンバーの複合アップグレード ステータス（Not Initialized/In Progress/Completed/Fail/Abort_admin/None）が表示されます。

ドミナント AP からのクラスタ メンバーのアップグレードを停止するには、次の手順を実行してください。

[アップグレードの停止] をクリックします。

13

Umbrella

この章では、WAP デバイスの Umbrella 機能を設定する方法について説明します。

具体的な内容は次のとおりです。

- Cisco Umbrella の概要
- Umbrella の設定

Cisco Umbrella の概要

Cisco Umbrella はクラウドで提供されるネットワーク セキュリティ サービスです。マルウェアからデバイスを保護し、侵害をリアルタイムに防御するためのインサイトが得られます。進化するビッグ データおよびデータ マイニング方法によって、攻撃をプロアクティブに予測し、カテゴリ ベースのフィルタリングも行います。

Cisco Umbrella サーバは DNS クエリを解決し、ID ごとに事前設定済みのセキュリティ フィルタリング ルールを適用します。悪意があるドメインとしてマークされた場合は、ブロックされたページがクライアントに返され、安全であるとマークされた場合は解決された IP アドレスがクライアントに返されます。

Umbrella の設定

Umbrella を設定するには、次の手順を実行します。

ステップ 1 ナビゲーション ペインで [Umbrella] を選択します。

ステップ 2 次のパラメータを設定します。

- [有効(Enable)]: WAP デバイスで Umbrella 機能を有効または無効にします。
- [APIキー(API Key)]: Umbrella ダッシュボードから API キーを取得します。[管理(Admin)] -> [APIキー(API Keys)]。

- [APIキーの暗号(API Key's Secret)]:[APIキーの暗号(API Key's Secret)] は、Umbrella ダッシュボードで API キー作成したときに 1 回だけ表示されます。

注

- [APIキー(API Key)]、[APIキーの暗号(API Key's Secret)]、[デバイスタグ(Device Tag)] を変更すると、再登録によってネットワーク デバイスが作成されます。
- [デバイスタグ(オプション)(Device Tag (optional))]:デバイスまたはデバイスに割り当てられた特定の発信元を示すテキスト タグです。組織に固有であることを確認してください。
- [バイパスするローカルドメイン(オプション)(Local Domains to Bypass (optional))]:AP が、リスト内にある DNS クエリを転送します。リスト内の項目はカンマで区切ります。ドメインにはアスタリスク(*)の形式でワイルドカードを含めることができます。例:*.cisco.com.*.
- [DNSCrypt]:DNSCrypt 機能を有効にするかどうかを指定します。
- [登録状況(Registration Status)]:登録情報が表示されます。このステータスは[成功(Successful)]、[登録中(Registering)]、[失敗(Failed)] のいずれかになります。

A

認証解除メッセージの理由コード

クライアントが WAP デバイスから認証解除されると、メッセージがシステム ログに送られます。このメッセージには、クライアントが認証解除された原因を特定するために役立つことのある理由コードが含まれています。[ステータスと統計情報] > [ログ] をクリックするとログ メッセージを表示できます。

詳細については、次を参照してください。

- 認証解除理由コード表

認証解除理由コード表

次の表に、認証解除理由コードを示します。

理由コード	意味
0	予約済み
1	理由の指定なし
2	直前の認証が有効ではなくなった
3	送信側ステーション(STA)が独立基本サービス セット(IBSS)または ESS を去ろうとしているか去ったため認証解除されました
4	非アクティブであるため認証解除されました
5	WAP デバイスで現在関連付けられている STA の一部を処理できないため認証解除されました
6	関連付けられていない STA からクラス 2 フレームを受信しました
7	関連付けられていない STA からクラス 3 フレームを受信しました
8	送信側 STA が基本サービス セット(BSS)を去ろうとしているか去ったため認証解除されました

理由コード	意味
9	関連付け（または再関連付け）を要求している STA は応答側 STA で認証されていません
10	Power Capability 要素に含まれている情報が許容されないため認証解除されました
11	Supported Channels 要素に含まれている情報が許容されないため認証解除されました
12	BSS 移行管理が原因で認証解除されました
13	無効な要素（この標準規格に定義されており、内容が Clause 8 の指定を満たさない要素）
14	メッセージ完全性符号（MIC）エラー
15	4 ウェイ ハンドシェイク タイムアウト
16	グループ鍵ハンドシェイク タイムアウト
17	4 ウェイ ハンドシェイクに含まれている要素が Association Request/Reassociation Request/Probe Response/Beacon フレーム内の要素と異なる
18	無効なグループ暗号方式
19	無効なペアワイズ暗号方式
20	無効な AKMP
21	サポートされていない RSNE バージョン
22	無効な RSNE 機能
23	IEEE 802.1X 認証失敗
24	セキュリティ ポリシーによって暗号スイートが拒否されました

B

関連情報

シスコでは、WAP571/E をお客様が最大限に活用できるように、さまざまなリソースを提供しています。

サポート	
シスコ サポート コミュニティ	www.cisco.com/go/smallbizsupport
サポート センター（SBSC）の電話サポート連絡先	www.cisco.com/go/sbsc
ビジネス サポートとリソース	www.cisco.com/go/smallbizhelp
サポート サービス情報	www.cisco.com/go/sbs www.cisco.com/go/software（登録およびログインが必要）。
シスコ ファームウェアのダウンロード	www.cisco.com/go/smallbizfirmware リンクを選択して、シスコ製品のファームウェアをダウンロードできます。ログインは不要です。 その他のあらゆるシスコ製品のソフトウェアとファームウェアのダウンロードは、Cisco.com（www.cisco.com/go/software）の [ダウンロード] 領域で可能です（登録およびログインが必要）。
シスコ オープン ソース リクエスト	www.cisco.com/go/smallbiz_opensource_request

シスコ パートナー セントラル(パートナー ログインが必要です)	www.cisco.com/web/partners/sell/smb
製品マニュアル	
Cisco WAP571 Wireless-AC/N Premium Dual Radio Access Point with PoE のクイック スタート ガイドおよび管理ガイド	http://www.cisco.com/go/500_wap_resources