Cisco Mobility Express リリース 8.2 ユーザ ガイド

初版：2015 年 11 月 30 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

【注意】シスコ製品をご使用になる前に、安全上の注意（**www.cisco.com/jp/go/safety_warning/**）をご確認ください。本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

目 次

第 1 章

Cisco Mobility Express について

Cisco Mobility Express の概要

Cisco Mobility Express ワイヤレス ネットワーク ソリューションは、Cisco Aironet 1850 シリーズおよび 1830 シリーズのアクセス ポイント（AP）に現在バンドルされている仮想 WLC 機能を提供します。この機能により簡素化された Wi-Fi アーキテクチャは、エンタープライズレベルから中小規模の導入環境までの WLAN 機能に対応できるようになります。

Cisco Mobility Express ワイヤレス ネットワーク ソリューションでは、Cisco Mobility Express ワイヤレス コントローラを実行する 1 つの AP がマスター AP として指定されます。従属 AP と呼ばれる他の AP は、その AP 自身をこのマスター AP に関連付けます。

マスター AP は、WLC として動作して従属 AP を管理および制御するだけでなく、クライアントにサービスを提供する AP としても動作します。従属 AP は、クライアントにサービスを提供する通常の Lightweight AP として動作します。

サポートされる AP の一覧については、サポートされる Cisco Aironet アクセス ポイント，（2 ページ）を参照してください。

Cisco Mobility Express ソリューションは、WLC のほとんどの機能を提供し、以下とのインターフェイス接続機能があります。

- Cisco Prime Infrastructure：AP グループの管理など、簡素化されたネットワーク管理を行います。
- Cisco Identity Services Engine：高度なポリシーの適用を行います。
- Cisco Mobility Services Engine：プレゼンスレベルのデータおよび高度なスペクトル ソリューションを提供します。

サポートされる Cisco Aironet アクセス ポイント

Cisco Mobility Express リリースでは、次の AP がサポートされます。

マスターとしてサポートされる AP（統合 WLC 機能をサポート）	従属としてサポートされる AP
• Cisco Aironet 1850 シリーズ • Cisco Aironet 1830 シリーズ [1]	• Cisco Aironet 700i シリーズ • Cisco Aironet 700w シリーズ • Cisco Aironet 1600 シリーズ • Cisco Aironet 1700 シリーズ • Cisco Aironet 2600 シリーズ • Cisco Aironet 2700 シリーズ • Cisco Aironet 3500 シリーズ • Cisco Aironet 3600 シリーズ • Cisco Aironet 3700 シリーズ

[1] マスター AP としてサポートされる AP は、従属 AP としても機能できます。

サポートされるソフトウェア イメージ

マスターとしてサポートされる AP モデルは、次のいずれかの工場出荷時デフォルト ソフトウェア付きで発注できます。

- Cisco Mobility Express ソフトウェア イメージ。これらのモデルのモデル番号（または製品 ID）は *C* で終わります。
- Lightweight AP ソフトウェア イメージ。ワイヤレス コントローラに join するための Control And Provisioning of Wireless Access Points（CAPWAP）プロトコルに基づきます。これらのモデルは Cisco Mobility Express ソフトウェア イメージを含むようにオンサイトで手動で変換できます。この変換については、CAPWAP Lightweight AP 15.3.3-JBB5 以降から Cisco Mobility Express ソフトウェアへの変換, （14 ページ）を参照してください。

従属としてのみサポートされる AP モデルには、CAPWAP ベースの Lightweight AP ソフトウェア イメージが必要です。

AP モデルの Cisco Mobility Express ソフトウェアは、次の URL からダウンロードできます。

https://software.cisco.com/download/navigator.html

[Download Software] ウィンドウで AP モデルに移動し、[Mobility Express Software] を選択すると、現在使用可能なソフトウェアが最新版から順に表示されます。ソフトウェア リリースには、ダウンロードするリリースを判断する際に役立つように、次のようなラベルが付いています。

- Early Deployment (ED)：これらのソフトウェア リリースには、新機能、新しいハードウェア プラットフォーム サポート、およびバグ修正ファイルが付属しています。
- Maintenance Deployment (MD)：これらのソフトウェア リリースには、バグ修正ファイルおよび現時点のソフトウェア メンテナンスが付属しています。
- Deferred (DF)：これらは延期されたソフトウェア リリースです。アップグレードしたリリースに移行することを推奨します。

シスコ ワイヤレス用 Cisco Mobility Express ソフトウェア リリース 8.2 を次に示します。

ソフトウェアのタイプと目的	リリース	AP 1850 用	AP 1830 用
Lightweight アクセス ポイントからの変換のみに使用される Mobility Express コントローラ対応 AP ソフトウェア。	8.2.100.1	AIR-AP1850-K9-8.2.100.1.tar	AIR-AP1830-K9-8.2.100.1.tar
サポートされるアクセス ポイントの ME コントローラ ソフトウェアおよびイメージを更新するために使用されるアクセス ポイント イメージ バンドル。	8.2.100.1	AIR-AP1850-K9-ME-8-2-100-1.zip	AIR-AP1830-K9-ME-8-2-100-1.zip

第 2 章

使用する前に

Cisco Mobility Express の設定とアクセスの前提条件

- Cisco Mobility Express ネットワークのセットアップ中または日常的な動作中に、同じネットワーク上にシスコの他のワイヤレス コントローラ（アプライアンスまたは仮想）が存在してはなりません。

  Cisco Mobility Express コントローラを、同じネットワーク上の他のワイヤレス コントローラと相互運用または共存させることはできません。ネットワーク上に Cisco Mobility Express コントローラ以外のワイヤレス コントローラが存在しないことを確認してください。

- セットアップする最初のアクセス ポイント（AP）を決定します。セットアップする最初の AP は、Cisco Mobility Express ワイヤレス コントローラの機能をサポートする AP である必要があります。これは、この AP をマスター AP として動作させ、他の AP をその AP に接続す

るために必要です。これにより、事前定義された *CiscoAirProvision* サービス セット識別子（SSID）はマスター AP および他の AP によってのみアドバタイズされます。

- AP の『*Hardware Installation Guide*』に従って AP を正しくインストールしてください。
- DHCP サーバがネットワークに存在すること、およびネットワーク上でこのサーバにアクセスできることを確認します。Mobility Express コントローラは、アクセス ポイントとワイヤレス クライアントの IP アドレスの管理に外部 DHCP サーバを使用します。
- Cisco Mobility Express コントローラを初期設定するには、Wi-Fi 経由でコントローラ コンフィギュレーション ウィザードを使用します。

  マスター AP によってアドバタイズされる事前定義の *CiscoAirProvision* SSID に接続するためには、Wi-Fi 対応のラップトップが必要です。この SSID に有線ネットワークからアクセスすることはできません。
- ラップトップには、互換性のあるブラウザがインストールされている必要があります。Cisco Mobility Express ワイヤレス コントローラの Web インターフェイスおよび初期設定ウィザードと互換性のあるブラウザのリストについては、対応ブラウザ，（70 ページ）を参照してください。
- ネットワークでユニバーサル規制ドメインのアクセス ポイントを使用する場合は、AP がクライアントへのサービス提供を開始する前に、適切な規制ドメインへのアクセス ポイントを用意しておく必要があります。「*Cisco Aironet Universal AP Priming and Cisco AirProvision User Guide*」（URL：http://www.cisco.com/c/en/us/td/docs/wireless/access_point/ux-ap/guide/uxap-mobapp-g.html）を参照してください。

これらの前提条件を満たしていることを確認したら、初期設定ウィザードの起動，（6 ページ）に進みます。

（注） CLI ベースの初期設定ウィザードも使用可能ですが、上級ユーザのみに推奨されています。CLI 初期設定ウィザードの使用，（62 ページ）を参照してください。

初期設定ウィザードの起動

ステップ 1 コントローラ機能を持つ AP を起動します。この AP は、1850 または 1830 シリーズの AP である必要があります。
最初に AP の電源を入れてから *CiscoAirProvision* SSID がブロードキャスティングを開始するまでには、数分かかります。*CiscoAirProvision* SSID がブロードキャスティングを開始したら、AP のステータス LED が緑、赤、オレンジの順に循環して点灯します。

ステップ 2 Wi-Fi 対応のラップトップを、AP によってアドバタイズされる *CiscoAirProvision* SSID へ、Wi-Fi 経由で接続します。パスワードは password です。
ラップトップはサブネット 192.168.1.0/24 から IP アドレスを取得します。

ステップ 3 サポートされているブラウザを使用して、*http://192.168.1.1* に移動します。これにより、初期設定ウィザードにリダイレクトされます。
初期設定ウィザードの管理者アカウント ウィンドウがブラウザに表示されます。

次の作業

初期設定ウィザードの管理者アカウントウィンドウが表示されたら、初期設定ウィザードの使用, （7 ページ）に進みます。表示されない場合は、AP のソフトウェアが CAPWAP Lightweight AP であるか Cisco Mobility Express であるかの確認, （12 ページ）に進みます。

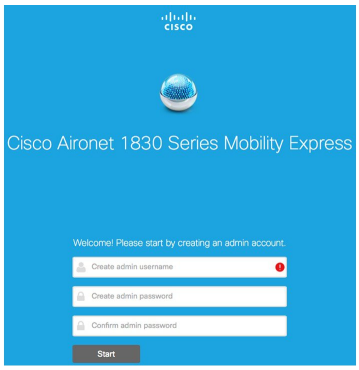
初期設定ウィザードの使用

初期設定ウィザードを使用すると、Cisco Mobility Express ワイヤレス LAN コントローラで特定の基本パラメータを設定でき、これにより Cisco Mobility Express ネットワークが動作します。

初期設定ウィザードで入力するデータについては、次のセクションを参照してください。

初期設定ウィザードで開いているウィンドウ

図 *1*：*Cisco Mobility Express* 初期設定ウィザードで開いているウィンドウ



このウィンドウのバナーには、Cisco Mobility Express ワイヤレス コントローラを設定している AP モデルの名前（たとえば、Cisco Aironet 1830 シリーズ Mobility Express など）が表示されます。

コントローラで管理者アカウントを作成するには、次のパラメータを指定し、[Start] をクリックします。

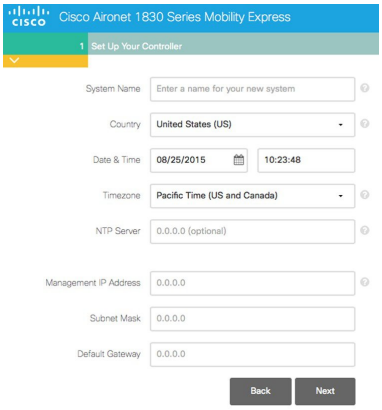
- 管理者のユーザ名を入力します。ASCII 文字を最大 24 文字入力できます。
- パスワードを入力します。ASCII 文字を最大 24 文字入力できます。

  パスワードを指定するときには、次のことを確認してください。

- パスワードには、小文字、大文字、数字、特殊文字のうち、3 つ以上の文字クラスが含まれる必要があります。
- パスワード内で同じ文字を連続して 4 回以上繰り返すことはできません。
- 新規のパスワードとして、関連するユーザ名と同じものやユーザ名を逆にしたものは使用できません。
- パスワードには、Cisco という語の大文字を小文字に変更したものや文字の順序を入れ替えたもの（cisco、ocsic など）は使用できません。また、i の代わりに 1、I、！を、o の代わりに 0 を、s の代わりに $ を使用することはできません。

ステップ 1：コントローラをセットアップする

図 *2*：コントローラの設定



コントローラを設定するには、次の基本パラメータを指定します。

- System Name：このコントローラに割り当てる名前を入力します。
- Country：この Cisco Mobility Express ネットワークが存在する国を入力します。
- Date and Time：日付を指定します。デフォルトでは、デバイスのシステム時刻が適用されます。必要に応じて時刻を手動で編集できます。
- Timezone：タイム ゾーンを選択します。
- NTP Server ：Network Time Protocol（NTP）サーバを使用して自動的に設定された日付と時刻を使用するために、NTP サーバの IPv4 アドレスまたは FQDN 名を入力できます。

  デフォルトで 3 つの NTP サーバが自動的に作成されます。NTP サーバのデフォルトの FQDN 名を次に示します。

  - 0.ciscome.pool.ntp.org（NTP のインデックス値 1）
  - 1.ciscome.pool.ntp.org（NTP のインデックス値 2）
  - 2.ciscome.pool.ntp.org（NTP のインデックス値 3）

ここで指定する IPv4 アドレスまたは FQDN 名は NTP インデックス 1 のサーバに適用され、これによりそのデフォルトの FQDN、*0.ciscome.pool.ntp.org* が上書きされます。NTP サーバの編集の詳細については、[Management] > [Time] に進みます。

- Management IP Address：コントローラを管理するための IP アドレスを入力します。
- Subnet Mask：コントローラのサブネット マスクを入力します。
- Default Gateway：コントローラのデフォルト ゲートウェイを入力します。

ステップ 2：ワイヤレス ネットワークを作成する

次の 2 つのネットワークをセットアップします。

- Employee Network：社員およびネットワークを日常的に使用する正規ユーザ向けの Wi-Fi ネットワーク。ゲスト用ではありません。
- Guest Network：ゲスト ユーザ向けの Wi-Fi ネットワーク。

[Employee Network] セクションで、次のパラメータを指定します。

- Network Name：社員ネットワーク用の SSID を指定します。
- Security：事前共有キー（PSK）認証を使用する [WPA2 Personal]、または認証に RADIUS サーバを必要とする [WPA2 Enterprise]（802.1x とも呼ばれる）を選択します。
- Pass Phrase：[WPA2 Personal] セキュリティを選択した場合は、PSK を指定します。
- Authentication Server IP Address：[WPA2 Enterprise] セキュリティを選択した場合は、RADIUS サーバの IP アドレスを入力します。
- Shared Secret：RADIUS サーバ用のパスワードを入力します。
- VLAN：[Management VLAN]（VLAN 0）を選択するか、[New VLAN] を選択して新規作成（1 ～ 4096 の VLAN ID を指定）します。
- VLAN ID：新規 VLAN の VLAN ID を指定します。

- DHCP Server Address：これはオプションです。

図 *3*：*[WPA2 Enterprise]* セキュリティを選択した社員ネットワーク

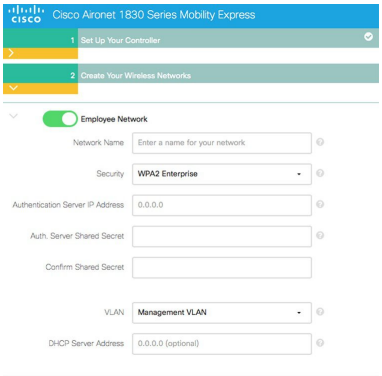
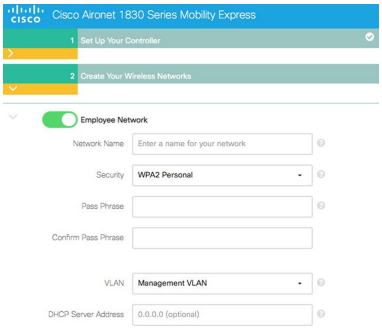


図 *4*：*[WPA2 Personal]* セキュリティを選択した社員ネットワーク



[Guest Network] セクションで、次のパラメータを指定します。

- Network Name：ゲスト ネットワーク用の SSID を指定します。
- Security：認証を必要としない [Web Consent]、または PSK 認証を必要とする [WPA2 Personal] を選択します。
- Pass Phrase：[WPA2 Personal] セキュリティを選択した場合は、PSK を指定します。
- VLAN：[Employee VLAN] を選択して社員ネットワークに定義したのと同じ VLAN を使用するか、[New VLAN] を選択して新規作成（1 ～ 4096 の VLAN ID を指定）します。
- VLAN ID：新規 VLAN の VLAN ID を指定します。

- DHCP Server Address：これはオプションです。

図 5：***[Web Consent]*** セキュリティを選択したゲスト ネットワーク

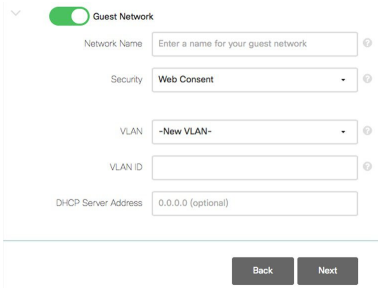
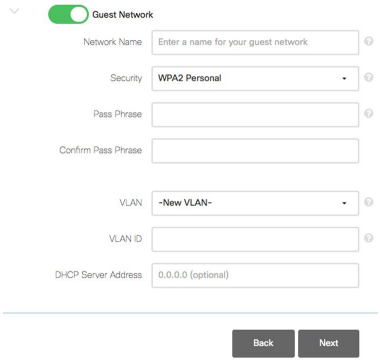


図 6：***[WPA2 Personal]*** セキュリティを選択したゲスト ネットワーク

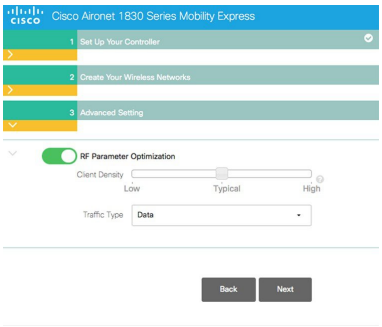


ステップ 3：詳細設定

ネットワークの無線周波数の信号のカバレッジと品質を最適化するため、ネットワークの予想されるクライアント密度とトラフィック タイプを指定します。低、標準または高密度のクライアント タイプが選択された場合に設定された値については、RF パラメータの最適化設定，（72 ページ） を参照してください。

（注） 初期化ウィザードで RF パラメータの最適化を有効にしない場合、クライアント密度は標準（デフォルト値）に設定され、RF トラフィック タイプはデータ（デフォルト値）に設定されます。

図 *7*：*RF* パラメータの最適化



これらの設定を適用すると、アクセス ポイントとコントローラが再起動します。次にCisco Mobility Express へのログイン，（16 ページ）に進みます。

AP のソフトウェアが CAPWAP Lightweight AP であるか Cisco Mobility Express であるかの確認

Cisco 1850 シリーズと 1830 シリーズの AP はどちらも、工場出荷時 CAPWAP Lightweight AP ソフトウェアまたは Cisco Mobility Express コントローラ ソフトウェア付きで発注できます。ただし、CAPWAP AP から Cisco Mobility Express ソフトウェアへの変換およびその逆方向の変換をオンサイトで実行できます。AP に Cisco Mobility Express イメージまたは CAPWAP Lightweight AP イメージが含まれているかどうかを判別するには、以下のステップに従います。

ステップ 1 RJ-45 ケーブルを使用して、AP のコンソール ポートに接続します。

ステップ 2 ユーザ名 Cisco とパスワード Cisco を使用して AP にログインします。どちらも大文字と小文字が区別されます。
これは、あらゆる Cisco Aironet AP の工場出荷時のユーザ名とパスワードです。

ステップ 3 AP コンソールで **sh version** コマンドを入力します。

ステップ 4 [AP Image Type] フィールドと [AP Configuration] フィールドのコマンド出力を確認します。次の表に示してある 3 つのシナリオが考えられます。

次の作業

出力のフィールドと値	次の作業
AP Image Type：`MOBILITY EXPRESS IMAGE` AP Configuration：`MOBILITY EXPRESS CAPABLE`	変換は不要です。APを再起動し、初期設定ウィザードの起動, （6 ページ）に進みます。
AP Image Type：`MOBILITY EXPRESS IMAGE` AP Configuration：`NOT MOBILITY EXPRESS CAPABLE`	これは、AP には Cisco Mobility Express ソフトウェアが含まれているが、CAPWAP Lightweight AP 構成で動作していることを表しています。CAPWAP Lightweight AP ソフトウェア リリース 15.3.3-JBB1 から 15.3.3-JBB5 以降へのアップグレード, （13 ページ）に進みます。
[AP Image Type] フィールドと [AP Configuration] フィールドが出力に存在しない	これは、AP に CAPWAP Lightweight AP は含まれているが、Cisco Mobility Express ソフトウェアは含まれていないことを表しています。CAPWAP Lightweight AP 15.3.3-JBB5 以降から Cisco Mobility Express ソフトウェアへの変換, （14 ページ）に進みます。

CAPWAP Lightweight AP ソフトウェア リリース 15.3.3-JBB1 から 15.3.3-JBB5 以降へのアップグレード

現在の AP は、Lightweight AP ソフトウェア リリース 15.3.3-JBB1（Cisco Wireless Controller ソフトウェア リリース 8.1.111.0 向け）を使用する 1850 シリーズ アクセス ポイントです。次の手順に従って、ソフトウェアを Lightweight AP ソフトウェア リリース 15.3.3-JBB5（Cisco Wireless Controller ソフトウェア リリース 8.1.122.0 向け）以降にアップグレードする必要があります。

（注） 次の手順では、8.1.122.0 リリースへのアップグレードについて説明するため、それに対応するソフトウェア ファイルを使用します。アップグレード後のリリースに応じて、必ず適切なソフトウェア ファイルを使用してください。

はじめる前に

- TFTP サーバと DHCP サーバを設定し、アクセス可能にする必要があります。

- このアップグレードの実行中に、AP がその AP 自体を既存の WLC に関連付けないようにしてください。

ステップ 1 Cisco.com から TFTP サーバへ *AIR-AP1850-K9-ME-8-1-122-0.zip* ファイルをダウンロードします。
ここでダウンロードされるファイルはアクセス ポイント イメージ バンドルであり、ソフトウェア アップデートやサポートされるアクセス ポイント イメージに使用されます。

ステップ 2 ファイルを解凍し、その内容を抽出します。

ステップ 3 AP のコンソール ポートに接続します。

ステップ 4 ユーザ名 Cisco とパスワード Cisco を使用して AP コンソールにログインします。どちらも大文字と小文字が区別されます。
これは、あらゆる Cisco Aironet AP の工場出荷時のユーザ名とパスワードです。

ステップ 5 AP コンソールのコマンドライン インターフェイスで、**enable** と入力します。

ステップ 6 **archive download-sw /reload tftp://**<*tftp server's ip address*>**/AIR-AP1850-K9-ME-8-1-122-0/ap1g4** と入力します。
または、**ap-type mobility-express tftp://**<*tftp server ip-address*>**/ap1g4** コマンドを使用します。

新しい Mobility Express ソフトウェア イメージから AP が再起動します。

次の作業

CAPWAP Lightweight AP 15.3.3-JBB5 以降から Cisco Mobility Express ソフトウェアへの変換, （14 ページ） に進みます。

CAPWAP Lightweight AP 15.3.3-JBB5 以降から Cisco Mobility Express ソフトウェアへの変換

現在の AP は、Lightweight AP ソフトウェア リリース 15.3.3-JBB5（Cisco WLC ソフトウェア リリース 8.1.122.0 向け）以降を使用する Cisco 1850 シリーズまたは 1830 シリーズ AP です。そのソフトウェアを Cisco Mobility Express 設定可能ソフトウェアに変換する必要があります。

（注） 次の手順では、8.1.122.0 Lightweight AP リリースから変換するため、それに対応するソフトウェア ファイルを使用します。変換元のリリースに応じて、必ず適切なソフトウェア ファイルを使用してください。

はじめる前に

- TFTP サーバと DHCP サーバを設定し、アクセス可能にする必要があります。

- このアップグレードの実行中に、ネットワーク内に Cisco WLC（物理または仮想）が存在しないことを確認してください。このアップグレードの実行中に、AP が他のワイヤレス コントローラとインターフェイス接続しないようにしてください。

ステップ 1 Cisco.com から TFTP サーバへ *AIR-AP1850-K9-ME-8-1-122-0.zip* ソフトウェア ファイルをダウンロードします。
ここでダウンロードされるファイルはアクセス ポイント イメージ バンドルであり、ソフトウェア アップデートやサポートされるアクセス ポイント イメージに使用されます。

ステップ 2 RJ-45 ケーブルを使用して、AP のコンソール ポートに接続します。

ステップ 3 ユーザ名 Cisco とパスワード Cisco を使用して AP にログインします。どちらも大文字と小文字が区別されます。
これは、あらゆる Cisco Aironet AP の工場出荷時のユーザ名とパスワードです。

ステップ 4 AP を CAPWAP Lightweight AP ソフトウェア リリース 15.3.3-JBB5 から Cisco Mobility Express ソフトウェアに変換するには、**ap-type mobility-express tftp://***<tftp server ip-address>/<filename with path from root on the TFTP server>* コマンドを使用します。
AP が再起動し、オンラインに戻り、コントローラに join しようとします（この処理に約 5 分かかります）。この後、AP は Mobility Express モードになり、*CiscoAirProvison* SSID のブロードキャストを開始します。

次の作業

初期設定ウィザードの起動, （6 ページ） に進みます。

マスター AP に関連付ける AP の準備

新しい AP をマスター AP 上の Cisco Mobility Express ワイヤレス コントローラに関連付けることができるようにするには、ここに示す手順に従ってください。これにより、Cisco Mobility Express ネットワークに join できるようになります。

はじめる前に

- Cisco Mobility Express ワイヤレス コントローラを使用するマスター AP は動作中である必要があります。
- マスター AP に関連付けるための準備をする AP がユニバーサル規制ドメイン AP である場合は、Cisco AirProvision モバイル アプリケーションを使用して用意する必要があります。詳細については、次の URL にある「*Cisco Aironet Universal AP Priming and Cisco AirProvision User Guide*」を参照してください：

http://www.cisco.com/c/en/us/td/docs/wireless/access_point/ux-ap/guide/uxap-mobapp-g.html

ステップ 1 Cisco.com から TFTP サーバに最新の Cisco Mobility Express バンドルをダウンロードします。このパックは .zip 形式（Windows の場合）または .tar 形式（Linux または Mac OSX の場合）で、サポートされているすべての AP のソフトウェア イメージが含まれています。

ステップ 2 TFTP サーバ上のフォルダにソフトウェア パックを解凍します。

ステップ 3 [Management] > [Software Update] > [File Path] フィールドにフォルダのパスを入力します。

ステップ 4 ソフトウェアアップデートを実行します。詳細については、ソフトウェアアップデートの実行, （54 ページ）を参照してください。

次の作業

関連付けられているアクセス ポイントの管理, （42 ページ）

Cisco Mobility Express へのログイン

ステップ 1 ブラウザを開き、ブラウザのアドレス バーに https://<*ip address*> と入力して、Cisco Mobility Express の [Wireless LAN Controller] ログイン ページにアクセスします。この IP アドレスは、Cisco Mobility Wireless Express コントローラを管理するために指定したアドレスです。
Cisco Mobility Express コントローラは、HTTPS に自己署名証明書を使用します。そのため、すべてのブラウザに警告が表示され、証明書がブラウザに表示されたときに例外の状態でも続行するかどうか尋ねられ

ます。Mobility Express の [Wireless LAN Controller] ログイン ページにアクセスするためには、警告を受け入れます。

図 *8*：*Cisco Mobility Express* ワイヤレス *LAN* コントローラの *Web* インターフェイスのログイン

ステップ 2 [Login] をクリックします。

ステップ 3 管理者ユーザのクレデンシャルを入力してログインします。

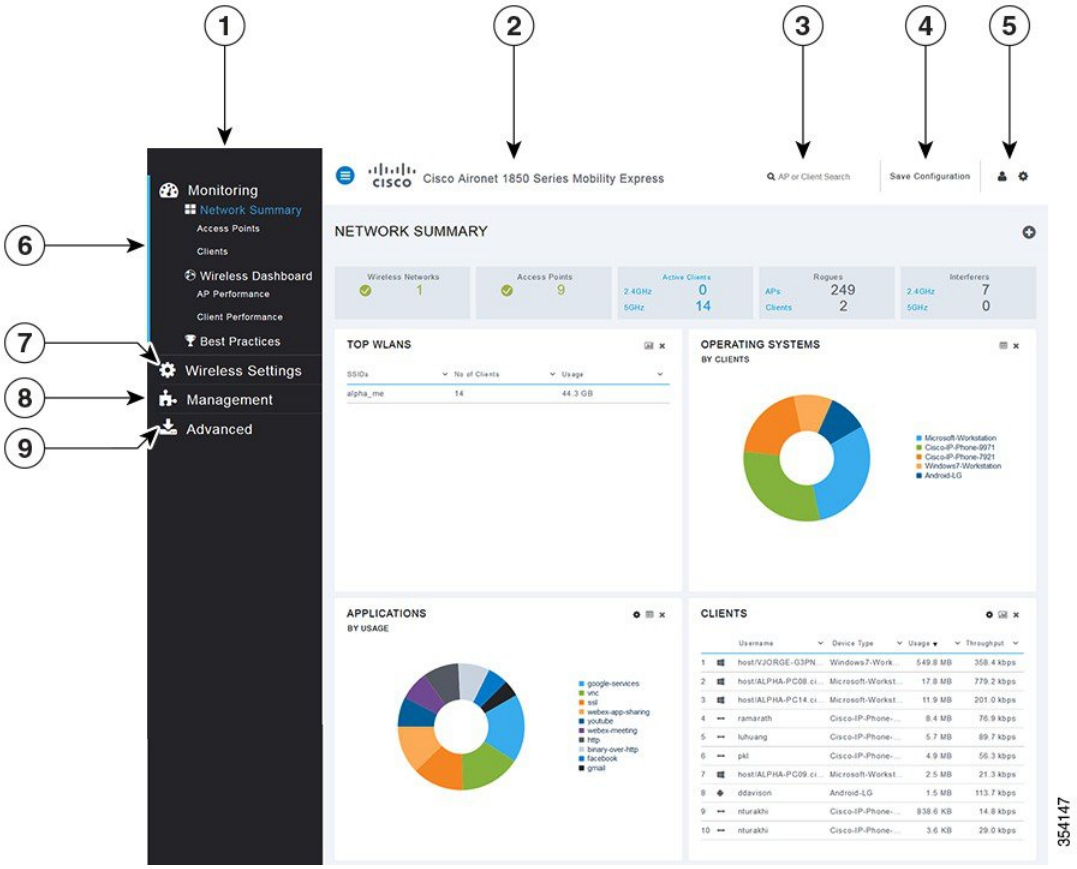
次の作業

ログインすると、デフォルトのランディング ページである [Network Summary] ウィンドウが表示されます。詳細については、Cisco Mobility Express モニタリング サービスについて，（21 ページ）を参照してください。

Mobility Express コントローラの Web インターフェイスについて

次の図は、Mobility Express コントローラの Web インターフェイスの起動ページと一般的なレイアウトです。

図 *9* : ***Mobility Express*** コントローラの ***Web*** インターフェイス



番号	Web インターフェイスのセクションまたは機能
1	Web インターフェイスのサイド ペイン。これはメイン ナビゲーション ペインです。このページから、Web インターフェイスの各種サブセクションに移動できます。
2	Web インターフェイスのタイトル。統合されたコントローラ機能が現在動作しているマスター AP の AP モデルを示します。
3	AP またはクライアントを、MAC アドレスを使用して検索します。

番号	Web インターフェイスのセクションまたは機能
4	クリックすると、現在のコントローラ コンフィギュレーションが NVRAM に保存されます。詳細については、コントローラ コンフィギュレーションの保存, （60 ページ）を参照してください。
5	クリックすると、現在のシステム情報が表示されるか、コントローラの Web インターフェイスからログオフします。
6	Mobility Express ネットワークの [Monitoring] セクション。詳細については、Cisco Mobility Express モニタリング サービスについて, （21 ページ）を参照してください。
7	[Wireless Settings] セクション。関連付けられた AP、WLAN、WLAN ユーザ アカウント、およびゲスト ユーザ アカウントを管理できます。 詳細については、ワイヤレス設定の指定, （35 ページ）を参照してください。
8	[Management] セクション。管理アクセス パラメータの設定、管理者アカウントとネットワーク時間の管理、およびソフトウェア アップデートの実行ができます。 詳細については、ネットワークの管理, （47 ページ）を参照してください。
9	[Advanced] セクション。SNMP の設定、システム ログの設定、工場出荷時へのリセットを実行できます。詳細については、詳細設定の使用と操作, （57 ページ）を参照してください。

第 3 章

Mobility Express ネットワークのモニタリング

Cisco Mobility Express モニタリング サービスについて

Cisco Mobility Express モニタリング サービスを使用すると、マスター AP は、WLAN をモニタできるだけでなく、ネットワーク上のすべての接続デバイスと未接続デバイスをモニタできます。

モニタリング サービスは、[Network Summary] タブと [Wireless Dashboard] タブに以下の機能を提供します。

- 設定された WLAN の詳細を表示する。
- トラフィックおよび関連するクライアントに基づいた上位 WLAN を一覧表示する。
- ネットワーク内の AP の詳細を表示する。
- 2.4 GHz または 5 GHz 帯でアクティブに動作するクライアントの詳細を表示する。

- これらのデバイスで稼働するクライアントデバイス オペレーティング システムとアプリケーションの概要を表示する。
- 不正なクライアントおよび AP の詳細なリストを表示する。
- 無線周波数が 2.4 GHz および 5 GHz であるネットワークに存在する各種干渉の詳細を表示する。
- ネットワーク内の AP のパフォーマンスをモニタする。
- ネットワーク内のクライアントのパフォーマンスをモニタする。

（注）
- [Network Summary] ウィンドウに表示されるパラメータはすべて読み取り専用です。
- このページは 30 秒ごとに自動的にリフレッシュされます。

[Network Summary] ビューのカスタマイズ

[Network Summary] ビューをカスタマイズするには、ウィジェットを追加または削除します。各種ウィジェットに表示されるデータは、個々のウィジェットの右上にある表示アイコンを切り替えることによって、ドーナツ形式または表形式で表示できます。

図 *10* : *[Network Summary]* ウィジェット - 表形式ビュー

図 *11* : *[Network Summary]* ウィジェット - ドーナツ形式ビュー

WLAN ユーザの表示と管理

ローカル サーバ設定を使用して、WPA2 Enterprise のみの WLAN ユーザを表示および管理できます。ワイヤレス クライアントが Cisco Mobility Express ワイヤレス ネットワークを使用するには、ネットワーク内の WLAN に接続する必要があります。ワイヤレス クライアントが WLAN に接続するには、その WLAN に設定されたユーザ クレデンシャルを使用する必要があります。この WLAN で [Security Policy] として [WPA2 Personal] が使用されている場合、ユーザはコントローラ AP 上のその WLAN に設定された該当する WPA2 PSK を入力する必要があります。[Security Policy] が [WPA2-Enterprise] に設定されている場合、ユーザは、RADIUS ユーザ データベースで設定されている有効なユーザ アイデンティティとそれに対応するパスワードを入力する必要があります。

[WLAN Users] ウィンドウで、Cisco Mobility Express ワイヤレス ネットワーク内の各種 WLAN の各種ユーザ（およびユーザ クレデンシャル）をセットアップできます。これらは、WPA2-PSK を使用してマスター AP で認証されるローカル ユーザです。WPA2-Enterprise で認証されるユーザは [WLAN Users] データベースの一部ではないため、認証するためには、RADIUS データベースにそのユーザの有効なレコードが含まれている必要があります。

WLAN の表示

[WLAN Configuration] ウィンドウには、マスター AP で現在設定されているすべての WLAN がリストされるのに加えて、各 WLAN の次の詳細情報が表示されます。

- Active：WLAN が有効であるか、無効であるか。
- Name：WLAN の名前
- Security Policy
- Radio Policy

ヒント　アクティブ WLAN の総数がページの上部に表示されます。WLAN のリストが複数ページに渡る場合は、ページ番号のリンクまたは進む/戻るアイコンをクリックすることで、目的のページにアクセスできます。

設定済み WLAN の詳細の表示

ステップ 1　[Monitoring] > [Network Summary] の順に選択します。
[Wireless Networks] サマリー ウィンドウに、設定済み WLAN の数が表示されます。

ステップ 2　[Wireless Networks] サマリー ウィンドウで、ステータス アイコンまたはカウント表示アイコンをクリックすると、対応する WLAN の高度な詳細情報（[Active] ステータス、[Name]、[Security Policy]、[Radio Policy] など）が表示されます。
このページから新しい WLAN を追加することもできます。詳細については、WLAN の追加, （36 ページ）を参照してください。

[Access Points] テーブル ビューのカスタマイズ

ステップ 1 [Monitoring] > [Network Summary] > [Access Points] をクリックします。
[Access Points] ビュー ページが表示されます。

ステップ 2 [Access Points] ビュー ページで、[2.4GHz] タブと [5GHz] タブを切り替えると、それぞれの無線周波数で動作するアクセス ポイントが表形式でリストされます。

ステップ 3 （任意）カラム ヘッダーの右上にある下向き矢印をクリックして、テーブル ビューで表示または非表示にするカラムを選択します。

ステップ 4 （任意）カラムヘッダーの右上にある下向き矢印をクリックして、必要なパラメータに基づいてテーブル ビューをフィルタリングします。

クライアントの詳細の表示

ステップ 1 [Monitoring] > [Network Summary] をクリックします。
[Active Clients] サマリーセクションに、すべてのアクティブ クライアントのサマリーが表示されます。これらのクライアントは、2.4 GHz で動作する 802.11 b/g/n クライアント、または 5 GHz で動作する 802.11 a/n/ac クライアントです。

ステップ 2 [Active Clients] サマリーセクションで、カウント表示アイコンをクリックすると、クライアント デバイスの高度な詳細情報が表示されます。
表示される情報は次のとおりです。

- 一般的な詳細。
- 接続状態のグラフィック。
- ネットワーク接続を使用しているクライアントの上位アプリケーション。
- モビリティ状態のグラフィック。
- ネットワーク、QoS、セキュリティ、ポリシーの詳細。
- クライアントの ping およびパケット キャプチャ テスト。

カラムヘッダーの右上にある下向き矢印をクリックして、テーブルに表示される詳細情報をカスタマイズして、必要なカラムを表示または非表示にするか、または必要なパラメータに基づいてテーブル ビューをフィルタリングします。

モビリティ状態のグラフィックについて

クライアントのモビリティ状態のグラフィックには次の詳細が表示されます。

- ワイヤレス LAN コントローラの名前と、これを実行している AP の IP アドレスおよびモデル番号。
- クライアントがコントローラへの接続に使用している AP の名前と、接続のタイプ（たとえば、Flexconnect）、AP の IP アドレス、AP のモデル番号。
- AP とクライアント間の接続の特性。たとえば、無線 802.11n 5 GHz 接続。
- クライアントの名前、クライアントのタイプ（たとえば、Microsoft ワークステーション）、クライアントの VLAN ID、およびクライアントの IP アドレス。

クライアントの ping テストの実行

クライアントで ping テストを実行して、コントローラとクライアント間のレイテンシまたは遅延を確認できます。これは、Internet Control Message Protocol（ICMP）に基づくテストです。ping テストを使用して、コントローラとクライアント間の接続およびレイテンシを確認できます。

テストを開始するには、[Start] をクリックします。ミリ秒のレイテンシがグラフィカルに表示されます。

クライアント パケットのキャプチャ

クライアント パケット キャプチャ機能では、AP を正常に動作しながら、ネットワーク管理者が AP 宛て、AP 経由、および AP からのパケットをキャプチャすることができます。パケットは、キャプチャされて Wireshark などのツールを使用してオフライン分析を行うことができる FTP サーバにエクスポートされます。この機能により、パケットの形式、アプリケーションの分析、およびセキュリティに関する情報の収集を支援することでトラブルシューティングが容易になります。

注意点

- パケット キャプチャは、同時に 1 つのクライアントに対してのみ有効にできます。
- パケットは、ビーコンとプローブ応答を除き、パケットの到着順または送信順にキャプチャおよびダンプされます。パケット キャプチャには、チャネル、RSSI、データ レート、SNR およびタイムスタンプなどの情報が含まれています。各パケットは、AP からの追加情報に付加されます。
- ファイルは、AP 名、コントローラ名およびタイムスタンプに基づいて、各 AP の FTP サーバに作成されます。
- FTP 転送時間がパケット レートより遅い場合、一部のパケットがキャプチャ ファイルに表示されないことがあります。

- AP のバッファにパケットが含まれていない場合、接続を維持するために、ダミー パケットがダンプされます。
- FTP 転送が失敗した場合、または FTP 接続がパケット キャプチャ中に失われた場合、AP は、パケットのキャプチャを止め、エラー メッセージおよび SNMP トラップによって通知し、新しい FTP 接続が確立されます。
- 無線配信中にすべてのパケットがキャプチャされるわけではなく、無線ドライバに到達するものだけがキャプチャされます。
- FTP サーバがあることを確認する前に、AP によって到達可能になります。キャプチャされたパケットは、この FTP サーバにダンプされます。

パケット キャプチャの実行

1. [Monitoring] > [Network Summary] > [Clients] の順に選択します。
2. [Client View] ページで、[Client Test] の下の [Packet Capture] タブをクリックします。
3. [Capture Point] で、次の詳細情報を指定します。
   - AP Name ：キャプチャ ポイントになる AP の名前です。キャプチャ ポイントは、パケットがキャプチャされるトラフィック トランジット ポイントです。キャプチャ ポイントとして AP のみ指定できます
   - Time ：パケット キャプチャの期間を指定します。範囲は 1 ～ 60 分です。
4. [Capture Filters] で、キャプチャする必要のあるパケットのタイプを指定します。次のタイプがあります。
   - 制御パケット
   - データ パケット
   - Dot1x
   - IAPP
   - 管理パケット
   - ARP
   - マルチキャスト フレーム
   - ブロードキャスト フレーム
   - すべての IP
   - 一致するポート番号を持つ TCP
   - 一致するポート番号を持つ UDP
5. [FTP Details] で、キャプチャされたパケットをダンプする FTP サーバの次に示す詳細を指定します。

- IP アドレス
- パケットがダンプされる FTP サーバのフォルダのパス
- FTP サーバにアクセスするためのユーザ名とパスワード

6 [Start] をクリックします。

[Client Status] アイコンは、パケット キャプチャ中は緑色です。それ以外は赤色になります。

不正なデバイス（クライアントおよびアクセス ポイント）の詳細の表示

ステップ 1 [Monitoring] > [Network Summary] をクリックします。
[Rogues] サマリー ウィンドウに、不正な AP とクライアントのサマリーが表示されます。

ステップ 2 [Rogues] サマリー ウィンドウで、カウント表示アイコンをクリックすると、不正なデバイス（未管理の隣接する AP またはクライアント）の高度な詳細情報が表示されます。

干渉源の詳細の表示

ステップ 1 [Monitoring] > [Network Summary] をクリックします。
[Interferers Summary] ウィンドウに、すべての非 WiFi 干渉デバイスのサマリーが表示されます。これらの干渉は、2.4 GHz または 5 GHz で動作する可能性があります。

ステップ 2 [Interferers] サマリー ウィンドウで、カウント表示アイコンをクリックすると、干渉デバイスの高度な詳細情報が表示されます。

[Access Point Performance] ビューのカスタマイズ

[AP Performance] ビューをカスタマイズするには、ウィジェットを追加または削除します。

図 *12*：*[Wireless Dashboard] - [AP Performance]*

[AccessPointPerformance]ビューをカスタマイズするためのウィジェットの追加

ステップ 1 [Monitoring] > [Wireless Dashboard] > [AP Performance] の順に選択します。

ステップ 2 [AP Performance] ウィンドウの右上にある [Add Widget] アイコンをクリックします。

ステップ 3 追加するウィジェットをクリックして選択します。

- Channel Utilization：上位の AP
- Interference：上位の AP
- Client Load：上位の AP
- Coverage：下位の AP

ステップ 4 [Close] をクリックします。
[AP Performance] ウィンドウがリフレッシュされ、新しいウィジェットが表示されます。

[AccessPointPerformance]ビューをカスタマイズするためのウィジェットの削除

ステップ 1 [Monitoring] > [Wireless Dashboard] > [AP Performance] の順に選択します。

ステップ 2 削除するウィジェットの右上にある [Delete Widget] アイコンをクリックします。
[AP Performance] ウィンドウに、削除したウィジェットが表示されなくなります。

[Client Performance] ビューのカスタマイズ

[Client Performance] ビューをカスタマイズするには、ウィジェットを追加または削除します。

図 *13*：*[Wireless Dashboard] - [Client Performance]*

[Client Performance] ビューをカスタマイズするためのウィジェットの追加

ステップ 1 [Monitoring] > [Wireless Dashboard] > [Client Performance] の順に選択します。

ステップ 2 [Client Performance] ウィンドウの右上にある [Add Widget] アイコンをクリックします。

ステップ 3 追加するウィジェットをクリックして選択します。

- Signal Strength
- Signal Quality
- Connection Rate
- Client Connections

ステップ 4 [Close] をクリックします。
[Client Performance] ウィンドウがリフレッシュされ、新しいウィジェットが表示されます。

[Client Performance] ビューをカスタマイズするためのウィジェットの削除

ステップ 1 [Monitoring] > [Wireless Dashboard] > [Client Performance] の順に選択します。

ステップ 2 削除するウィジェットの右上にある [Delete Widget] アイコンをクリックします。
[Client Performance] ウィンドウに、削除したウィジェットが表示されなくなります。

第 4 章

ワイヤレス設定の指定

WLAN と WLAN ユーザのセットアップ

Cisco Mobility Express ネットワークの WLAN について

ワイヤレス ローカル エリア ネットワーク（WLAN）を作成および管理するには、[WLAN Configuration] ウィンドウを使用します。[Wireless Settings] > [WLAN Users] の順に選択します。

[WLAN Configuration] ウィンドウの上部に、アクティブな WLAN の総数が表示されるとともに、マスター AP のコントローラで現在設定されているすべての WLAN が一覧表示されます。この一覧には、各 WLAN に関する次の詳細情報が表示されます。

- WLAN が有効であるか、無効であるか。
- WLAN の名前。
- WLAN のセキュリティ ポリシー。
- WLAN の無線ポリシー。

WLAN のセットアップに関する注意事項と制約事項

- Cisco Mobility Express コントローラには、最大 16 個の WLAN を関連付けることができます。ただし、推奨されるのは最大 4 個までです。コントローラは、設定されたすべての WLAN を、接続されているすべての AP に割り当てます。
- 各 WLAN には一意の WLAN ID、一意のプロファイル名、および SSID があります。

- WLAN 名と SSID は 32 文字以内にする必要があります。スペースは WLAN プロファイル名と SSID では許可されません。
- 接続されている各 AP は、[Enabled] 状態の WLAN のみをアドバタイズします。AP は、無効化された WLAN はアドバタイズしません。
- コントローラでは、同じ SSID の WLAN を区別するために、異なる属性が使用されます。
- ピアツーピア ブロッキングは、マルチキャスト トラフィックには適用されません。
- WLAN から VLAN0 へのマッピング、VLAN 1002～1006 のマッピングはできません。
- スタティック IPv4 アドレスを使用するデュアルスタック クライアントはサポートされていません。
- 同じ SSID を使用する複数の WLAN を作成するときには、WLAN ごとに一意のプロファイル名を作成します。

WLAN の追加

ステップ 1 [Wireless Settings] > [WLANs] の順に選択します。
[WLAN Configuration] ウィンドウが表示されます。

ステップ 2 WLAN を新規作成するには、[Add New WLAN] をクリックします。
[Add New WLAN] ウィンドウが表示されます。

ステップ 3 [General] タブで、次のパラメータを設定します。

- WLAN ID：ドロップダウン リストから、この WLAN 用の ID 番号を選択します。
- Profile Name：この WLAN に割り当てるプロファイル名を 32 文字以内で入力します。プロファイル名は固有である必要があります。
- SSID：この WLAN に割り当てる SSID を 32 文字以内で入力します。
- Admin State：ドロップダウン リストから [Enabled] を選択して、この WLAN を有効にします。有効にしない場合は、[Disabled] を選択します。デフォルトは [Enabled] です。
- Radio Policy：無線ポリシーを使用すると、WLAN に関連付けられているすべての AP の RF 設定を最適化できます。選択した無線ポリシーは、802.11 無線に適用されます。各無線ポリシーでは、WLAN をアドバタイズするスペクトルの部分を指定するのに加えて、それが 2.4 GHz（802.11b モードまたは 802.11g モード）であるか 5 GHz（802.11a モード）であるか、あるいはその両方であるかを指定します。

  コントローラに関連付けられている AP の RF プロファイルを設定します。[Radio Policy] ドロップダウン リストから次のいずれかを選択します。

  - All（デフォルト）
  - 802.11a only

- 802.11a/g
- 802.11g only
- 802.11b/g

ステップ 4　[WLAN Security] タブで、次のパラメータを設定します。

- Security：このドロップダウン リストから次のいずれかのセキュリティ認証オプションを選択します。
  - Guest：コントローラは、ゲスト ユーザ専用の WLAN でゲスト ユーザ アクセスを提供できます。この WLAN をゲスト ユーザ アクセス専用に設定するには、[Security] に [Guest] を選択します。

    ゲスト ユーザの認証を設定するには、[Guest Authentication] ドロップダウン リストで次のいずれかのオプションを選択します。

    - Require Username and Password：これはデフォルト オプションです。この WLAN のゲスト ユーザに指定できるユーザ名とパスワードを使用してゲストを認証するには、[Wireless Settings] > [WLAN Users] でこのオプションを選択します。詳細については、WLAN ユーザの表示と管理, （40 ページ）を参照してください。
    - Display Terms & Conditions：表示された利用規約をゲストが受け入れたら、WLAN へのアクセスを許可するには、このオプションを選択します。これでユーザは、ユーザ名とパスワードを入力しなくても WLAN にアクセスできます。
    - Require Email Address：ゲスト ユーザが WLAN にアクセスしようとしたときに、電子メール アドレスの入力を求めるには、このオプションを選択します。有効な電子メール アドレスが入力されたら、アクセス権を付与します。これでユーザは、ユーザ名とパスワードを入力しなくても WLAN にアクセスできます。

  - Open：このオプションはオープン認証です。オープン認証では、あらゆるデバイスが認証でき、AP との通信を試行できます。オープン認証を使用すると、あらゆるワイヤレス デバイスが AP に対して認証を実行できます。
  - WPA2 Personal：このオプションは、事前共有キー（PSK）を使用する Wi-Fi Protected Access 2 です。WPA2 Personal は、PSK 認証を使用してネットワークを保護するために使用されるメソッドです。PSK は、WLAN セキュリティ ポリシー下のコントローラ AP で設定するだけでなく、クライアントでも設定します。WPA2 Personal は、ネットワーク上の認証サーバを信頼しません。このオプションは、エンタープライズ認証サーバがない場合に使用します。このオプションを選択した場合、[Shared Key] フィールドに PSK を指定します。
  - WPA2 Enterprise：このオプションは、ローカル認証サーバまたは RADIUS サーバを使用する Wi-Fi Protected Access 2 です。これがデフォルトのオプションです。

    ローカル認証方式を使用するには、[Authentication Server] ドロップダウン リストで [AP] を選択します。このオプションはローカル EAP 認証方式です。この認証方式では、ユーザとワイヤレス クライアントをローカルで認証できます。マスター AP のコントローラは、認証サーバおよびローカル ユーザ データベースとして機能するため、外部認証サーバに依存する必要がなくなります。

RADIUS サーバ ベースの認証方式を使用するには、[Authentication Server] ドロップダウン リストで [External Radius] を選択します。RADIUS は、中央管理サーバとの通信を行って、ユーザの認証と WLAN へのアクセス許可を可能にするクライアント/サーバ プロトコルです。RADIUS 認証サーバは最大 2 つまで指定できます。サーバごとに次の詳細を指定する必要があります。

- RADIUS IP：RADIUS サーバの IPv4 アドレス。
- RADIUS Port：RADIUS サーバの通信ポートを入力します。デフォルト値は 1812 です。
- Shared Secret：RADIUS サーバで使用する秘密キーを ASCII 形式で入力します。

ステップ 5 [VLAN & Firewall] タブで [Use VLAN Tagging] ドロップダウン リストから [Yes] を選択し、パケットの VLAN タギングを有効にします。その後、タギングに使用する [VLAN ID] をドロップダウン リストから選択します。デフォルトでは VLAN タギングは無効です。
VLAN タギングを有効にすると、パケットが属する VLAN（仮想ローカル エリア ネットワーク）を識別するために、選択した VLAN ID がパケット ヘッダーに挿入されます。これによりコントローラは、VLAN ID を使用して、ブロードキャスト パケットの送信先 VLAN を判別できるため、VLAN 間でトラフィックが分離されます。

ステップ 6 VLAN タギングを有効にするように選択した場合は、アクセス コントロール リスト（ACL）に基づいて WLAN のファイアウォールを有効にするためのオプションを選択できます。ACL は次のいずれかの目的で使用されるルール セットです。1 つの目的は、特定の WLAN へのアクセスを制限して、ワイヤレス クライアントとの間で送受信されるデータ トラフィックを制御すること、もう 1 つの目的は、コントローラ CPU へのアクセスを制限して、CPU を宛先とするすべてのトラフィックを制御することです。
ACL ベースのファイアウォールを有効にするには、次の手順に従います。

1. [Enable Firewall] ドロップダウン リストで [Yes] を選択します。
2. [ACL Name] フィールドに、新しい ACL の名前を入力します。最大 32 文字の英数字を入力できます。ACL 名は固有の名前でなければなりません。
3. [Apply] をクリックします。
4. ACL のルールを設定するには、[Add Rule] をクリックします。

ACL ルールは VLAN に適用されることに注意してください。複数の WLAN で同じ VLAN を使用できるので、VLAN に適用されている ACL ルールがあればそれが継承されます。

この ACL のルールを次のように設定します。

1. [Action] ドロップダウン リストから、この ACL によってパケットがブロックされるようにする場合は [Deny] を選択し、この ACL によってパケットが許可されるようにする場合は [Permit] を選択します。デフォルトの設定は [Permit] です。コントローラは ACL の IP パケットのみを許可または拒否できます。他のタイプのパケット（ARP パケットなど）は指定できません。
2. [Protocol] ドロップダウン リストから、この ACL に使用する IP パケットのプロトコル ID を選択します。プロトコル オプションは次のとおりです。
   - Any：任意のプロトコル（これはデフォルト値です）

- TCP：トランスミッション コントロール プロトコル
- UDP：ユーザ データグラム プロトコル
- ICMP：インターネット制御メッセージ プロトコル

  ESP：IP カプセル化セキュリティ ペイロード
- AH：認証ヘッダー
- GRE：Generic Routing Encapsulation
- IP in IP：Internet Protocol（IP）in IP（IP-in-IP パケットのみを許可または拒否）
- Eth Over IP：Ethernet-over-Internet プロトコル
- OSPF：Open Shortest Path First
- Other：その他の Internet Assigned Numbers Authority（IANA）プロトコル。[Other] を選択する場合は、[Protocol]テキストボックスに目的のプロトコルの番号を入力します。使用可能なプロトコルのリストは IANA Web サイトで確認できます。

3 [Dest. IP/Mask] フィールドに、特定の宛先の IP アドレスとネットマスクを入力します。

4 [TCP] または [UDP] を選択した場合は、[Destination Port] を指定する必要があります。この宛先ポートは、ネットワーキング スタックとのデータ送受信をするアプリケーションが使用できます。一部のポートは、Telnet、SSH、HTTP など特定のアプリケーション用に指定されています。

5 [DSCP] ドロップダウン リストから次のオプションのいずれかを選択して、この ACL の Differentiated Service Code Point（DSCP）値を指定します。[DSCP] は、インターネット上の QoS を定義するために使用できる IP ヘッダー テキスト ボックスです。次のオプションを選択できます。

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

6 [Apply] アイコンをクリックして、変更を確定します。

ステップ 7 Quality of Service（QoS）とは、選択したネットワーク トラフィックにさまざまなテクノロジーに渡る優れたサービスを提供する、ネットワークの機能を意味します。QoS の主要な目的は、専用の帯域幅の確保、ジッターおよび遅延の制御（ある種のリアルタイム トラフィックや対話型トラフィックで必要）、および損失特性の改善などを優先的に処理することです。
Cisco Mobility Express コントローラは、次の 4 つの QoS レベルをサポートします。[QoS] タブの [QoS] ドロップダウン リストで、次のいずれかの QoS レベルを選択します。

- Platinum (Voice)：無線を介して転送される音声のために高品質のサービスを保証します。
- Gold (Video)：高品質のビデオ アプリケーションをサポートします。
- Silver (Best Effort)：クライアントの通常の帯域幅をサポートします。
- Bronze (Background)：ゲスト サービス用の最小の帯域幅を提供します。

ステップ 8 [Application Visibility] は、Network-Based Application Recognition（NBAR2）エンジンを使用してアプリケーションを分類し、ワイヤレス ネットワークにアプリケーションレベルの可視性を提供します。[Application Visibility] により、コントローラは 1000 個を超えるアプリケーションの検出と認識、リアルタイム分析の実行、ネットワークの輻輳とネットワーク リンクの使用状況のモニタができます。この機能は、[Monitoring] > [Network Summary] にある [Applications By Usage] 統計を提供します。
[Application Visibility] を有効にするには、[Application Visibility] ドロップダウン リストから [Enabled]（デフォルト オプション）を選択します。有効にしない場合は、[Disabled] を選択します。

ステップ 9 [Apply] をクリックします。

次の作業

この時点で、この WLAN のユーザ アカウントを作成または編集できます。WLAN ユーザの表示と管理, （40 ページ）を参照してください。

WLAN の有効化と無効化

ステップ 1 [Wireless Settings] > [WLANs] の順に選択します。
[WLAN Configuration] ウィンドウが表示されます。

ステップ 2 有効または無効にする WLAN の横にある [Edit] アイコンをクリックします。
[Edit WLAN] ウィンドウが表示されます。

ステップ 3 [General] > [Admin State] の順に選択し、必要に応じて [Enabled] または [Disabled] を選択します。

ステップ 4 [Apply] をクリックします。

（注） WLAN を新規作成または既存の WLAN を編集した後で [Apply] をクリックすると、以前有効だったか無効だったかに関係なく、必ず WLAN が有効になります。

WLAN の編集と削除

[Wireless Settings] > [WLANs] の順に選択します。表示されるウィンドウで、次のいずれかの操作を実行します。

- WLAN を編集するには、その隣りにある [Edit] アイコンをクリックします。
- WLAN を削除するには、その隣りにある [Delete] アイコンをクリックします。

WLAN ユーザの表示と管理

WLAN ユーザを表示、管理するには、[Wireless Settings] > [WLAN Users] の順に選択します。

[WLAN Users] ウィンドウが表示され、コントローラ上で構成されている WLAN ユーザの総数が表示されます。さらに、ネットワーク上のすべてのWLANユーザおよび各ユーザに関する次の詳細情報が表示されます。

- User name：WLAN ユーザの名前。
- Guest user：このチェックボックスをオンにした場合、ユーザは作成時から 86400 秒間（24 時間）のみ有効となるゲスト ユーザ アカウントとなります。
- WLAN Profile：このユーザが接続できる WLAN。
- Password：WLAN への接続時に使用するパスワード。
- Description：ユーザに関する詳細またはコメント。

ローカル サーバ設定を使用して、WPA2 Enterprise のみの WLAN ユーザを表示および管理できます。ワイヤレス クライアントが Cisco Mobility Express ワイヤレス ネットワークを使用するには、ネットワーク内の WLAN に接続する必要があります。ワイヤレス クライアントが WLAN に接続するには、その WLAN に設定されたユーザ クレデンシャルを使用する必要があります。この WLAN で [Security Policy] として [WPA2 Personal] が使用されている場合、ユーザはコントローラ AP 上のその WLAN に設定された該当する WPA2 PSK を入力する必要があります。[Security Policy] が [WPA2-Enterprise] に設定されている場合、ユーザは、RADIUS ユーザ データベースで設定されている有効なユーザ アイデンティティとそれに対応するパスワードを入力する必要があります。

WLAN ユーザの追加

WLAN ユーザを追加するには、[Add WLAN User] をクリックしてから、次の詳細情報を入力します。

- User name：WLAN ユーザ アカウントの名前を指定します。
- Guest user：ゲスト WLAN ユーザ アカウントにする場合は、このチェックボックスをオンにします。さらに [Lifetime] フィールドに、このアカウントが有効であり続ける時間数を作成時からの秒数で指定できます。デフォルト値は 86400 秒（24 時間）です。ライフタイム値は 60 秒～ 31536000 秒（つまり 1 分~ 1 年）の範囲内で指定できます。
- WLAN Profile：このユーザが接続できる WLAN を選択します。ドロップダウン リストから特定の WLAN から選択するか、[Any WLAN] を選択して、コントローラ上にセットアップされているすべての WLAN 用にこのアカウントを適用します。

  このドロップダウン リストには、[Wireless Settings] > [WLANs] で設定した WLAN が表示されます。WLAN の追加の詳細については、WLAN の追加, （36 ページ）を参照してください。
- Password：WLAN への接続時に使用するパスワード。
- Description：ユーザに関する詳細またはコメント。

WLAN ユーザの編集

WLANユーザを編集するには、詳細を編集する WLANユーザの横にある [Edit] アイコンをクリックし、必要な変更を加えます。

WLAN ユーザの削除

WLAN ユーザを削除するには、削除する WLAN ユーザの横にある [Delete] アイコンをクリックしてから、確認ダイアログボックスで [Ok] をクリックします。

関連付けられているアクセス ポイントの管理

[Wireless Settings] > [Access Points] の順に選択します。[Access Points Administration] ウィンドウが表示されます。ウィンドウの上部には、コントローラに関連付けられている AP の数とともに、次の詳細情報が表示されます。

- Manage：次のアイコンが表示され、AP がプライマリ コントローラ（マスター AP）として動作しているのか、従属 AP として動作しているのかが示されます。

図 *14*：プライマリ コントローラ（マスター *AP*）アイコン

図 *15*：従属 *AP* アイコン

- Location：AP の場所。
- Name：AP の名前。
- IP Address：AP の IP アドレス。
- AP MAC：AP の MAC アドレス。
- Up Time：AP がコントローラに関連付けられている時間の長さ。
- AP Model：アクセス ポイントのモデル番号。

アクセス ポイントの管理

ステップ 1 [Wireless Settings] > [Access Points] の順に選択します。
[Access Points Administration] ウィンドウが表示されます。コントローラに関連付けられている AP のみを管理できます。

ステップ 2 管理する AP の横にある [Edit] アイコンをクリックします。

[Edit] ウィンドウが表示され、[General] タブが表示されます。

ステップ 3 [General] タブでは、次の AP パラメータを編集できます。

- IP Configuration：AP の IP アドレスがネットワーク上の DHCP サーバによって割り当てられるようにするには、[Obtain from DHCP] を選択します。静的 IP アドレスを使用する場合は、[Static IP] を選択します。静的 IP アドレスを使用する選択をした場合は、[IP Address]、[Subnet Mask]、および [Gateway] フィールドを編集できます。
- AP Name：AP の名前を編集します。これはフリー テキスト フィールドです。
- Location：AP の場所を編集します。これはフリー テキスト フィールドです。

[General] タブには次の編集できない AP パラメータも表示されます。

- Operating Mode：マスター AP の場合、このフィールドには [AP & Controller] と表示されます。関連付けられている他の AP の場合、このフィールドには [AP Only] と表示されます。
- AP MAC address
- AP Model number
- アクセス ポイントの [IP Address]（[Obtain from DHCP] を選択した場合のみ編集不可）。
- [Subnet mask]（[Obtain from DHCP] を選択した場合のみ編集不可）。
- [Gateway]（[Obtain from DHCP] を選択した場合のみ編集不可）。

ステップ 4 （マスター AP の場合のみ）[Controller] タブでは、統合された Mobility Express ワイヤレス LAN コントローラの次のコントローラ パラメータを手動で編集できます。

- System Name：このコントローラに割り当てた名前を編集します。 ASCII 文字を最大 31 文字入力できます。システム名は、初期設定ウィザード中に最初に指定されます。
- IP Address：この IP アドレスは、コントローラの Web インターフェイスへのログイン URL を決定します。URL の形式は *https://<ip address>* です。この IP アドレスを変更すると、ログイン URL も変更されます。
- Subnet Mask
- Country Code：このドロップダウン リストを使用してコントローラおよび関連するすべての AP の国番号を設定できます。 変更を適用すると、すべての下位 AP の国番号が自動的に変更され、AP がリブートして新しい国番号でオンラインに戻り、コントローラに再接続されます。ただしマスター AP を手動でリブートするまで、変更はコントローラおよびマスター AP には適用されません。

ステップ 5 [802.11 b/g/n] タブで、次のパラメータを設定できます。

- Admin Mode：[Enabled] または [Disabled]。これにより、AP の対応する無線（802.11 b/g/n の場合は 2.4 GHz）が有効または無効になります。
- Channel：[Automatic]、[1] 〜 [11]。

[Automatic] を選択すると、動的チャネル割り当てが有効になります。つまり、マスターAPの制御下にある各 AP にチャネルが動的に割り当てられます。これにより、隣接する AP が同じチャネル上でブロードキャストされることがなくなり、干渉などの通信の問題を回避できます。2.4 GHz 無線の場合、米国では11チャネルが提供され、米国以外の国や地域では最大14チャネルが提供されます。ただし、隣接する AP で使用される場合、非オーバーラップと見なすことができるのは、1-6-11 のみです。

特定の値を割り当てると、その AP にチャネルが静的に割り当てられます。

- Channel Width：20 MHz

  2.4 GHz のチャネル幅は 20 MHz にしか設定できません。

  チャネル ボンディングは、1 つの無線ストリーム用のチャネルを 2 つまたは 4 つのグループに分けます。これにより、速度とスループットが向上します。2.4 GHz のチャネル数が不十分である場合は、複数の非オーバーラップ チャネルを有効にするためにチャネル ボンディングを使用することはできません。

- Transmit Power：[Automatic]、[1] ～ [8]。

  これは対数目盛の送信電力、つまり AP で使用される伝送エネルギーです。[1] が最高、[2] が [1] の半分、[3] が [1] の 1/4 となり、以下同様に減少していきます。

  [Automatic] を選択すると、受信側の変動する信号レベルに基づいて、無線のトランスミッタ電力が調整されます。これによりトランスミッタは、フェーディング条件が発生した場合に、ほとんどの時間、最大電力未満で動作できるようになります。これが最大値に到達するまで、送信電力が必要に応じて増加します。

ステップ 6 [802.11 a/n/ac] タブで、次のパラメータを設定できます。

- Admin Mode：[Enabled] または [Disabled]。これにより、AP の対応する無線（802.11a/n/ac の場合は 5 GHz）が有効または無効になります。
- Channel：[Automatic]、[36]、[40]、[44]、[48]、[52]、[56]、[60]、[64]、[100]、[104]、[108]、[112]、[116]、[132]、[136]、[140]、[149]、[153]、[157]、[161]、[165]。

  5 GHz の無線の場合は、最大 23 の非オーバーラップ チャネルが提供されます。

  特定の値を割り当てると、その AP にチャネルが静的に割り当てられます。

- Channel Width：20、40、80 MHz

  チャネル ボンディングを使用する場合、5 GHz のチャネル幅は 20、40、または 80 MHz に設定できます。

- Transmit Power：[1] ～ [8]。

  これは対数目盛の送信電力、つまり AP で使用される伝送エネルギーです。[1] が最高、[2] が [1] の半分、[3] が [1] の 1/4 となり、以下同様に減少していきます。

  [Automatic] を選択すると、受信側の変動する信号レベルに基づいて、無線のトランスミッタ電力が調整されます。これによりトランスミッタは、フェーディング条件が発生した場合に、ほとんどの時

間、最大電力未満で動作できるようになります。これが最大値に到達するまで、送信電力が必要に応じて増加します。

ステップ 7 [Apply] をクリックして変更を保存し、終了します。

ゲスト WLAN ユーザ用にカスタマイズしたログイン ページの作成

前述の前提条件を満たした後で、すべてのゲストユーザ用にカスタマイズしたログインページを作成するには、以下のステップに従います。

はじめる前に

以下の操作を行って、ゲスト ユーザにネットワークへのアクセスを許可します。

1. ゲストユーザにアクセスを提供する新しい WLAN をセットアップするか、既存の WLAN を選択します。

   また、特定の WLAN をゲスト アクセス専用としてセットアップすることもできます。これを行うには、その WLAN の [WLAN Security] を [Guest] に設定します。詳細については、WLAN の追加, （36 ページ）を参照してください。

2. ゲスト ユーザ アカウントをセットアップします。[Wireless Settings] > [WLAN Users] の順に選択し、[Guest User] チェックボックスをオンにしてアカウントをセットアップします。詳細については、WLAN ユーザの表示と管理, （40 ページ）を参照してください。

ステップ 1 [Wireless Settings] > [Guest WLAN] の順に選択します。
[Guest WLAN] ページが表示されます。ネットワーク上にセットアップ済みのゲスト WLAN の数がページ上部に表示されます。

ステップ 2 表示された ウィンドウで、以下のパラメータを設定します。

- Display Cisco Logo：このフィールドはデフォルトで [Yes] に設定されています。デフォルト ウィンドウの右上に表示されるシスコのロゴを非表示にするには、[No] を選択します。このフィールドはデフォルトで [Yes] に設定されています。ただし、他のロゴを表示するためのオプションはありません。
- Redirect URL After Login：ログイン後にゲスト ユーザを特定の URL（企業 URL など）にリダイレクトする場合は、このフィールドにリダイレクト先の URL を入力します。最大 254 文字を入力することができます。

- Page Headline：デフォルトのヘッドラインは「*Welcome to the Cisco Wireless Network*」です。ログイン ページに独自のヘッドラインを表示するには、このフィールドにヘッドライン文字列を入力します。最大 127 文字を入力することができます。
- Page Message：デフォルトのメッセージは「*Cisco is pleased to provide the Wireless LAN infrastructure for your network. Please login and put your air space to work*」です。ログイン ページに独自のメッセージを表示するには、このフィールドにメッセージ（2047 文字まで）を入力します。

ステップ 3 [Apply] をクリックします。

第 5 章

ネットワークの管理

管理アクセス インターフェイスの設定

管理アクセスインターフェイスは、コントローラのインバンド管理やエンタープライズサービスへの接続に使用されるデフォルトインターフェイスです。また、コントローラとアクセスポイント（AP）間の通信にも使用されます。管理インターフェイスには、唯一常時 ping 可能な、コントローラのインバンド インターフェイス IP アドレスが設定されています。コントローラの Web インターフェイスにアクセスするには、ブラウザのアドレス バーに、コントローラの管理インターフェイスの IP アドレスを入力します。

AP の場合、ポートの数に関係なく、このコントローラには、コントローラ間の全通信を制御する管理インターフェイスが 1 つと、コントローラとアクセス ポイント間の全通信を制御する AP マネージャ インターフェイスが 1 つ必要です。

以下の操作を行って、コントローラへの管理アクセスのタイプを有効または無効にします。

ステップ 1 [Management] > [Access] の順に選択します。
[Management Access] ウィンドウが表示されます。有効にした管理タイプの数が、ウィンドウの上部に表示されます。

ステップ 2 コントローラへの管理アクセスのタイプを有効または無効にするには、ドロップダウン リストから該当するオプションを選択します。

- HTTP Access：HTTP アクセス モードを有効にして、Web ブラウザで *http://<ip-address>* を使用してコントローラの GUI にアクセスできるようにするには、[HTTP Access] ドロップダウン リストから [Enabled] を選択します。有効にしない場合は、[Disabled] を選択します。

  デフォルト値は [Disabled] です。

  （注） HTTP アクセス モードの接続は、セキュリティで保護されません。

- HTTPS Access：HTTPS アクセス モードを有効にして、Web ブラウザで *http://ip-address* を使用してコントローラの GUI にアクセスできるようにするには、[HTTPS Access] ドロップダウン リストから [Enabled] を選択します。有効にしない場合は、[Disabled] を選択します。

  デフォルト値は [Enabled] です。

  （注） HTTPS アクセス モードの接続は、セキュリティで保護されます。

- Telnet Access：Telnet アクセス モードを有効にして、ラップトップのコマンド プロンプトを使用してコントローラの CLI へのリモート アクセスを可能にするには、[Telnet Access] ドロップダウン リストから [Enabled] を選択します。有効にしない場合は、[Disabled] を選択します。

  デフォルト値は [Disabled] です。

  （注） Telnet アクセス モードの接続は、セキュリティで保護されません。

- SSHv2 Access：Secure Shell バージョン 2（SSHv2）アクセス モードを有効にするには、[SSHv2 Access] ドロップダウン リストから [Enabled] を選択します。このアクセス モードは、Telnet のセキュリティを強化したもので、データ暗号化およびセキュア チャネルを使用してデータを転送します。有効にしない場合は、[Disabled] を選択します。

  デフォルト値は [Enabled] です。

  （注） SSHv2 アクセス モードの接続は、セキュリティで保護されます。

ステップ 3 [Apply] をクリックして変更内容を保存します。

管理者アカウントの管理

コントローラのユーザ インターフェイスにログインしたり、コントローラを設定したり、設定情報を表示したりするには、管理用（つまり管理者）ユーザ アカウントが必要です。これにより、権限のないユーザがコントローラにアクセスしたり、コントローラを設定したりするのを防ぐことができます。

管理者アカウントの追加

ステップ 1 [Management] > [Admin Accounts] の順に選択します。
[Admin Accounts] ウィンドウが表示され、Cisco Mobility Express コントローラ上のすべての管理者アカウントがリストされます。コントローラ上の管理者アカウントの総数がウィンドウの上部に表示されます。

ステップ 2 [Add New User] をクリックして、新規管理者ユーザを追加します。

ステップ 3 必要に応じて、次のパラメータを設定します。

- Account name：管理者ユーザが使用するログインユーザ名。管理者アカウント名は一意でなければなりません。
- Access：管理者のアクセス権限を次のいずれかに設定します。
  - Read-Only：このオプションを選択すると、読み取り専用権限を持つ管理者アカウントが作成されます。管理者ユーザは、コントローラ コンフィギュレーションを表示できますが、設定を変更することはできません。
  - Read-Write：このオプションを選択すると、読み取り/書き込み権限を持つ管理者アカウントが作成されます。管理者ユーザは、コントローラ コンフィギュレーションを表示および変更できます。
- Password：次のルールに基づく管理者ユーザ アカウントのパスワードを入力します。
  - パスワードは大文字と小文字が区別されます。
  - パスワードは、小文字、大文字、数字、特殊文字のうち、3つ以上の文字クラスを含んだ8文字以上である必要があります。
  - パスワード内で同じ文字を連続して 4 回以上繰り返すことはできません。
  - パスワードに、Cisco という語または管理者ユーザ名を使用することはできません。さらに、これらの語の文字を逆順にしたもの、大文字を小文字に変更したもの、i を 1、|、または ! に置き換えたもの、o を 0 に置き換えたもの、s を $ に置き換えたものを使用することはできません。

ステップ 4 [Apply] をクリックして変更内容を保存します。

管理者アカウントの編集

ステップ 1 [Management] > [Admin Accounts] の順に選択します。

[Admin Accounts] ページが表示され、Cisco Mobility Express コントローラ上のすべての管理者アカウントがリストされます。コントローラ上の管理者アカウントの総数がページの上部に表示されます。

ステップ 2 編集するアカウントの横にある [Edit] アイコンをクリックします。

ステップ 3 管理者アカウントパラメータを必要に応じて変更します。これらのパラメータの詳細については、管理者アカウントの追加, （49 ページ）を参照してください。

ステップ 4 [Apply] をクリックします。

管理者アカウントの削除

ステップ 1 [Management] > [Admin Accounts] の順に選択します。
[Admin Accounts] ウィンドウが表示され、Cisco Mobility Express コントローラ上のすべての管理者アカウントがリストされます。コントローラ上の管理者アカウントの総数がページの上部に表示されます。

ステップ 2 削除するアカウントの横にある [Delete] アイコンをクリックします。

ステップ 3 確認ダイアログ ボックス内の [Ok] をクリックします。

日時の設定

Cisco Mobility Express コントローラの日時は最初、コントローラの初期設定セットアップ ウィザードを実行したときに設定されます。日時は手動で入力することも、日時を設定する Network Time Protocol（NTP）サーバを指定することもできます。

自動的に日時を設定するための NTP サーバの使用

コントローラが自動的に同期して日時を設定するための Network Time Protocol（NTP）サーバを 3 つまで指定できます。

デフォルトで 3 つの NTP サーバが自動的に作成されます。NTP サーバのデフォルトの FQDN 名を次に示します。

- 0.ciscome.pool.ntp.org（NTP のインデックス値 1）
- 1.ciscome.pool.ntp.org（NTP のインデックス値 2）
- 2.ciscome.pool.ntp.org（NTP のインデックス値 3）

初期設定ウィザードで NTP サーバの IPv4 アドレスまたは FQDN 名を指定できます。これは NTP インデックス 1 を持つサーバに適用されてそのデフォルトの FQDN である *0.ciscome.pool.ntp.org* を上書きします。NTP サーバの編集の詳細については、[Management] > [Time] に進みます。

NTP サーバの追加と編集

コントローラが自動的に日時を設定するための Network Time Protocol（NTP）サーバを 3 つまで指定できます。

ステップ 1 [Management] > [Time] の順に選択します。
[Time Settings] ウィンドウが表示され、設定されているタイム ゾーンがページ上部に表示されます。現在の日時が [Set Time Manually] フィールドに表示されます。既存の NTP サーバがある場合、[NTP Index] 値の順に表示されます。

ステップ 2 [NTP Polling Interval] フィールドに、ポーリング間隔（秒単位）を指定します。既存の NTP サーバを編集するには、その隣の [Edit] アイコンをクリックします。

ステップ 3 NTP サーバの次の値を追加、編集できます。

- NTP Index ：NTP サーバのプライオリティを設定するために、NTP のインデックス値を指定します。NTP のインデックス値は、プライオリティが高いものから順に 1 から 3 まで設定できます。コントローラは、最初にプライオリティが最も高いものから、指定されたポーリング間隔の時間の終わりまで NTP サーバと同期を試みます。同期が完了すると、コントローラは続けて残りの NTP サーバとの同期を試みます。同期が失敗した場合、コントローラは次の NTP サーバとの同期を試みます。
- NTP Server ：NTP サーバの IPv4 アドレスまたは完全修飾ドメイン名（FQDN）を指定します。FQDN を指定すると、DNS ルックアップが実行されます。ルックアップに失敗すると、エラーのログが syslog サーバに記録されます。コントローラは、NTP の設定を変更するかまたは有効な FQDN を指定するまでこの FQDN の解決を継続し、エラーがログに記録されます。

ステップ 4 [Apply] をクリックします。

NTP サーバの削除と無効化

NTP サーバを削除するには、[Management] > [Time] の順に選択します。表示される [Time Settings] ページで、削除する NTP サーバの隣の [Delete] アイコンをクリックします。確認ダイアログで [OK] をクリックし、次に [Apply] をクリックします。

NTP サーバによる日時の設定を無効にするには、上記の手順に従って、すべての設定済み NTP サーバを削除する必要があります。

日時の手動設定

ステップ 1 [Management] > [Time] の順に選択します。
[Time Settings] ウィンドウが表示され、設定されているタイム ゾーンがページ上部に表示されます。現在の日時が [Set Time Manually] フィールドに表示されます。
（注） これらのフィールドは、[NTP State] が [Enable] に設定されている場合は編集できません。

ステップ 2 [NTP State] ドロップダウン リストから [Disable] を選択します。

ステップ 3 [Time Zone] ドロップダウン リストからローカル タイム ゾーンを選択します。
Daylight Saving Time（DST; 夏時間）を使用する時間帯を選択すると、DST の発生時の時間変更を反映してコントローラが自動的にそのシステム クロックを設定します。米国では、DST は 3 月の第 2 日曜日から始まり、11 月の第 1 日曜日で終わります。

ステップ 4 [Set Time Automatically from Current Location] チェックボックスをオンにして、指定したタイム ゾーンに基づいて時刻を設定します。

ステップ 5 [Set Time Manually] フィールドで次の操作を行います。

- カレンダー アイコンをクリックし、月、日、年を選択します。
- 時計アイコンをクリックし、時刻（時と分）を指定します。

ステップ 6 [Apply] をクリックします。

Cisco Mobility Express ソフトウェアの更新

以下の操作を行って、Cisco Mobility Express コントローラの現在のソフトウェア バージョンを表示します。

- Web インターフェイスの右上隅にある歯車アイコンをクリックしてから、[System Information] をクリックします。
- [Management] > [Software Update] の順に選択します。

  これにより [Software Update] ウィンドウが表示され、その上部に現在のソフトウェアのバージョン番号が表示されます。

コントローラの Web インターフェイスを使用して Cisco Mobility Express コントローラ ソフトウェアを更新できます。これにより Cisco Mobility Express コントローラの現在の設定が削除されることはありません。

ソフトウェアを更新すると、内部コントローラ ソフトウェアが更新されるだけでなく、関連付けられているすべての AP 上の AP ソフトウェアも更新されます。AP 上の Cisco Mobility Express AP

ソフトウェアのバージョンが古い場合、ソフトウェア アップグレード後にマスター AP に join すると、Cisco Mobility Express AP ソフトウェアが自動的にアップグレードされて、最新のソフトウェアになります。これは、ソフトウェアのアップデート プロセス中に、コントローラに関連付けられているすべての Cisco Mobility Express サポート対象 AP 用の最新の Cisco Mobility Express ソフトウェアもダウンロードされるためです。コントローラに join する AP が、Cisco Mobility Express ソフトウェアのバージョンとマスター AP 上のバージョンを比較し、不一致が検出されると、新しい AP がソフトウェアのアップグレードを要求します。マスター AP が、TFTP サーバまたは HTTP パスから新しい AP への新しいソフトウェアの転送を支援します。

アップグレードが必要な Cisco Mobility Express ネットワークへ TFTP サーバから Cisco Mobility Express ソフトウェア イメージの新バージョンをダウンロードするには、AP ごとに約 5 分程度かかります。ソフトウェアのダウンロードはバックグラウンドで実行されるため、ネットワークには影響がありません。ソフトウェア アップデートがネットワークのパフォーマンスに影響しないようにするため、アップグレードは自動的に順次実行されます。

（注） 5 つまでのアクセス ポイントのソフトウェアを同時に更新できます。

TFTP サーバを準備するためのガイドライン

Cisco Mobility Express ソフトウェア ファイルをホストするために TFTP サーバを準備するときには、次のガイドラインに従ってください。

- TFTP サーバが 32 MB より大きいサイズのファイルに対して拡張 TFTP をサポートすることを確認します。このサイズのファイルをサポートする TFTP サーバには、tftpd32 や Cisco Prime Infrastructure 内の TFTP サーバがあります。
- コントローラ ソフトウェアをダウンロードするときに TFTP サーバでこのサイズのファイルがサポートされていないと、次のエラー メッセージが表示されます。

  「TFTP failure while storing in flash.」

- ディストリビューション システム ネットワーク ポートを経由してアップグレードする場合、ディストリビューション システム ポートはルーティング可能であるため、TFTP サーバは同じサブネット上にあっても、別のサブネット上にあってもかまいません。

（注） TFTP サーバに Cisco Mobility Express コントローラと同じ Cisco Mobility Express ソフトウェア バンドルまたは最新のソフトウェア バンドルが常に存在することを確認します。

ソフトウェア アップデートの実行

はじめる前に

- ソフトウェア アップデートに TFTP または HTTP を使用しているかどうかを判断します。

  ネットワークが、（ap1g4 イメージをサポートする）アクセス ポイントの 1850、1830、または両方のモデルで構成されている場合、TFTP または HTTP を介してアップデートを実行できます。ネットワークに他のサポートされている AP がある場合、更新には TFTP のみ使用できます。

- ソフトウェア アップデートに TFTP サーバを使用している場合、TFTP サーバが設定済みでアクセス可能である必要があります。TFTP サーバを準備するためのガイドライン，（53 ページ）を参照してください。

- Cisco.com および TFTP サーバにアクセスできるコンピュータを利用可能にしておきます。

ステップ 1 以下のステップに従って、コントローラ ソフトウェアのイメージを入手します。

a) コンピュータを使用して、[Cisco Download Software] ページ（URL：http://www.cisco.com/cisco/software/navigator.html）にアクセスします。
b) AP モデルに移動し、[Mobility Express Software] をクリックすると、現在使用可能なソフトウェアのリストが最新リリースから順に表示されます。
c) ソフトウェア リリース番号を選択します。
d) ファイル名をクリックします。
e) [Download] をクリックします。
f) シスコのエンド ユーザ ソフトウェアのライセンス契約を読み、[Agree] をクリックします。
g) ファイルをコンピュータのハード ドライブに保存します。
h) コンピュータのハード ドライブからファイルをコピーし、TFTP サーバ上のデフォルト ディレクトリに解凍します。

ステップ 2 Cisco Mobility Express コントローラの Web インターフェイスから [Management] > [Software Update] の順に選択します。
[Software Update] ウィンドウが表示され、現在のソフトウェアのバージョン番号が表示されます。

ステップ 3 [Transfer Mode] ドロップダウン リストで、必要に応じて TFTP または HTTP を選択します。

ステップ 4 転送モードとして [TFTP] を選択した場合は次の手順を行います。

a) [IP Address (Ipv4)] フィールドに、TFTP サーバの IP アドレスを入力します。
b) [File Path] フィールドに、ソフトウェア ファイルの TFTP サーバ ディレクトリのパスとファイル名を入力します。

ステップ 5 次に転送モードとして [HTTP] を選択した場合は、[File Path] フィールドの隣の [Browse] ボタンをクリックし、ソフトウェア ファイルを参照して選択します。

ソフトウェア ファイルの名前は [File Path] フィールドに表示されます。

ステップ 6 [Apply] をクリックして、指定したパラメータを保存します。
これらのパラメータは、今後変更しない限り、保存されたままになります。次回のソフトウェア アップデート時に、これらのパラメータを再度入力する必要はありません。

ステップ 7 更新を即時に実行するか、後から実行するようにスケジュールします。

- 更新をただちに実行するには、[Update Now] をクリックし、確認ダイアログで [OK] をクリックします。

  ページ トップのセクションに、ダウンロードのステータスが表示されます。このプロセスの実行中に、コントローラまたは AP の電源を手動で切ったり、リセットしたりしないでください。電源を切ったり、リセットしたりすると、ソフトウェア イメージが破損する場合があります。

  ページの [Preimage Download Status] セクションに、ネットワーク内の AP にダウンロードされるプリイメージのステータスが表示されます。

  プリイメージのダウンロードが完了したら、[Reboot] をクリックしてコントローラを再起動します。

- 更新を後から実行するには、[Set Reboot Time] フィールドに現在の日付から 5 日間以内の日時を指定してから、[Schedule Later] をクリックします。プリイメージ ダウンロードが完了すると、コントローラは自動的に再起動します。

プリイメージ ダウンロード機能の詳細については、アクセス ポイントへのイメージのプレダウンロード, （71 ページ）を参照してください。

ステップ 8 コントローラにログインし、[Software Update] ウィンドウでコントローラ ソフトウェアのバージョンを確認します。

第 6 章

詳細設定の使用と操作

SNMP の管理

Simple Network Management Protocol バージョン 2（SNMPv2）は、ネットワーク管理用プロトコルです。これは、ネットワーク内のすべてのデバイスから情報を収集したり、それらのデバイスを設定、管理するために使用します。

SNMPv2 アクセスを有効にするには、[SNMPv2 Access] ドロップダウン リストから [Enabled] を選択します。有効にしない場合は、[Disabled] を選択します。デフォルトでは無効になっています。

SNMP コミュニティに読み取り専用権限を設定するには、[Read-Only Community] フィールドにコミュニティ名を入力します。デフォルトは [Public] です。

SNMP コミュニティに読み取り/書き込み権限を設定するには、[Read-Write Community] フィールドにコミュニティ名を入力します。デフォルトは [Private] です。

ネットワーク デバイスから送信される SNMP トラップを受信、ログ記録、および表示する SNMP トラップ レシーバ ツールを有効にするには、[SNMP Trap] ドロップダウン リストから [Enabled] を選択します。デフォルトでは無効になっています。

SNMP サーバに接続するには、[SNMP Server IP] フィールドにサーバの IP アドレスを指定します。

システム メッセージ ロギングの設定

システム メッセージ ロギング機能は、syslog サーバと呼ばれるリモート サーバにシステム イベントのログを記録します。各システム イベントは、イベントの詳細を含む Syslog メッセージをトリガーします。

システム メッセージ ロギング機能が有効な場合、コントローラは、コントローラに設定された syslog サーバに syslog メッセージを送信します。

はじめる前に

次の手順を開始する前に、ネットワークで syslog サーバをセットアップします。

ステップ 1 [Advanced] > [Logging] の順に選択します。
[Logging Setup] ウィンドウが表示されます。

ステップ 2 [Syslog Logging] ドロップダウン リストから [Enable] を選択します。デフォルトでは無効になっています。システム メッセージ ロギング機能が有効になります。

ステップ 3 [Syslog Server IP] フィールドに、syslog メッセージの送信先サーバの IPv4 アドレスを入力します。

ステップ 4 syslog サーバに対する syslog メッセージのフィルタリングの重大度レベルを設定します。[Logging Level] ドロップダウン リストから、次のいずれかの重大度レベル（重大度が高い順）を設定します。

- Emergencies (Highest severity)
- Alerts
- Critical
- Errors (Default)
- Warnings
- Notifications
- Informational
- Debugging (Lowest severity)

syslog レベルを設定すると、重大度がそのレベル以上であるメッセージのみが、syslog サーバに送信されます。

ステップ 5 syslog サーバに送信する syslog メッセージのファシリティを設定するには、[Syslog Facility] ドロップダウン リストから次のいずれかのオプションを選択します。

- [Kernel] = ファシリティ レベル 0
- [User Process] = ファシリティ レベル 1
- [Mail] = ファシリティ レベル 2
- [System Daemons] = ファシリティ レベル 3

- [Authorization System] = ファシリティ レベル 4
- [Syslog] = ファシリティ レベル 5（デフォルト値）
- [Line Printer] = ファシリティ レベル 6
- [USENET] = ファシリティ レベル 7
- [Unix-to-Unix Copy] = ファシリティ レベル 8
- [Cron] = ファシリティ レベル 9
- [FTP Daemon] = ファシリティ レベル 11
- [System Use 12] = ファシリティ レベル 12
- [System Use 13] = ファシリティ レベル 13
- [System Use 14] = ファシリティ レベル 14
- [System Use 15] = ファシリティ レベル 15
- [Local Use 0] = ファシリティ レベル 16
- [Local Use 1] = ファシリティ レベル 17
- [Local Use 2] = ファシリティ レベル 18
- [Local Use 3] = ファシリティ レベル 19
- [Local Use 4] = ファシリティ レベル 20
- [Local Use 5] = ファシリティ レベル 21
- [Local Use 6] = ファシリティ レベル 22
- [Local Use 7] = ファシリティ レベル 23
- [Authorization System (Private)] = ファシリティ レベル 24

ステップ 6 [Apply] をクリックします。

Mobility Express コントローラのリセット

この操作は、管理者ユーザのみが実行できます。

以下の操作を行って、Cisco Mobility Express ワイヤレス LAN コントローラを工場出荷時のデフォルト パラメータにリセットします。

1 [Advanced] > [Reset to Factory Default] の順に選択します。
これにより、[RESET MOBILITY EXPRESS CONTROLLER TO FACTORY DEFAULT] ウィンドウが開きます。

2 [Continue] をクリックして、次の操作を行います。

- Cisco Mobility Express コントローラ コンフィギュレーション パラメータを消去して工場出荷時の値に設定し、Cisco Mobility Express ワイヤレス LAN コントローラを再起動します。
- マスター AP を工場出荷時のデフォルト設定にリセットし、再起動します。

Mobility Express コントローラが再起動したら、初期設定ウィザードの起動, （6 ページ）に進みます。

Mobility Express コントローラの再起動

コントローラは随時再起動できます。再起動するには、[Management] > [Software Update] の順に選択してから、[Restart] をクリックします。

コントローラ コンフィギュレーションの保存

アクセス ポイントには、揮発性のあるアクティブな RAM と不揮発性の RAM（NVRAM）の 2 種類のメモリがあります。通常動作時は、Cisco Mobility Express コントローラの現在の設定は、マスター AP の RAM 上にあります。再起動時には、揮発性 RAM は完全に消去されますが、NVRAM 上のデータは保持されます。

RAM 上にある Cisco Mobility Express コントローラの設定は、マスター AP の NVRAM にいつでも保存できます。これにより、最後に保存した設定を使用してコントローラを再起動できます。

RAM 上にあるコントローラの現在の設定を NVRAM に保存するには、Cisco Mobility Express Web インターフェイスの右上にある [Save Configuration] をクリックし、[Ok] をクリックします。

設定が正常に保存されたら、同一であることを伝えるメッセージが表示されます。

付 録 A

コントローラ CLI コマンド

サポートされる CLI コマンドについて

Mobility Express のリリースでサポートされる機能について、Mobility Express コントローラのソフトウェアでは、同じ Cisco Unified Wireless Network ソフトウェア リリースのワイヤレス LAN コントローラでサポートされるほとんどの CLI コマンドをサポートします。ただし、Mobility Express コントローラに特有の CLI コマンドおよび手順や、異なる動作をするものがいくつかあります。これらのコマンドと手順については、次の各項で説明します。

「Cisco Wireless Controller Command Reference guides, for Cisco Unified Wireless Network Software Releases」は、次の URL に掲載されています。 http://www.cisco.com/c/en/us/support/wireless/wireless-lan-controller-software/products-command-reference-list.html

CLI 初期設定ウィザードの使用

はじめる前に

- アクセス ポイントのコンソール ポートに接続して次の手順を実行します。
- 利用可能なオプションは、各設定パラメータの後の括弧内に示されます。デフォルト値は、すべて大文字で示されます。
- 入力した応答が正しくない場合は、「Invalid Response」などのエラー メッセージが表示され、ウィザードのプロンプトが再び表示されます。
- 前のコマンド ラインに戻る必要があるときは、**ハイフン** キーを押してください。

ステップ 1 自動インストールプロセス（CLI初期設定ウィザード）を終了するよう求められたら、30秒待機します。CLI 初期設定ウィザードは 30 秒後に開始されます。
プロセスを終了するには、**yes** を入力します。

ウィザードが設定ファイルを TFTP サーバからダウンロードして、設定を自動的にコントローラにロードします。

ステップ 2 このコントローラに割り当てる**管理者のユーザ名**および**パスワード**を入力します。それぞれ、24 文字までの ASCII 文字を入力できます。
パスワード ポリシーは次の通りです。

- パスワードには、次の中から少なくとも 3 つのクラスの文字を含める必要があります。
  - 小文字の英字
  - 大文字の英字
  - 数字
  - 特殊文字
- パスワードには同じ文字を連続して 4 回以上繰り返すことはできません。
- 新規のパスワードとして、関連するユーザ名と同じものやユーザ名を逆にしたものは使用できません。
- パスワードには、Cisco という語の大文字を小文字に変更したものや文字の順序を入れ替えたもの（cisco、ocsic など）を使用できません。また、i の代わりに 1、I、! を、o の代わりに 0 を、s の代わりに $ を使用することはできません。

ステップ 3 **システム名**を入力します。これは、コントローラに割り当てる名前です。ASCII 文字を最大 31 文字入力できます。

ステップ 4 Mobility Express ネットワークが置かれる国のコードを入力します。

（注） 使用可能な Country Code の一覧を表示するには、**help** と入力します。

ステップ 5 電源投入時にコントローラの時間設定が外部ネットワーク タイム プロトコル（NTP）サーバから受信されるようにするには、「YES」と入力して NTP サーバを設定します。それ以外の場合は、**no** と入力します。

YES を入力した場合は、NTP サーバの IP アドレスを入力します。

no を入力した場合は、次に従って入力し、手動で日時を設定します。

- 日付を MM/DD/YY の形式で入力します。
- 時刻を HH:MM:SS の形式で入力します。

ステップ 6 ゾーンの場所のインデックスを入力してタイムゾーンを設定します。**help** を入力するとインデックス別のタイム ゾーンのリストが表示されます。

ステップ 7 管理インターフェイスの IP アドレスを入力します。

（注） 管理インターフェイスは、コントローラのインバンド管理やエンタープライズ サービスへの接続に使用されるデフォルト インターフェイスです。

ステップ 8 管理インターフェイスのサブネット マスクの IP アドレスを入力します。

ステップ 9 デフォルト ゲートウェイ ルータの IP アドレスを入力します。

ステップ 10 [Employee Network] を有効にするには、**YES** を入力します。それ以外の場合は、**no** と入力します。

YES を入力した場合は、次のように入力します。

1. 社員ネットワーク名（SSID）
2. 社員 VLAN ID（0 = タグなし）
3. 社員ネットワーク セキュリティ。**PSK** または **enterprise** を入力できます。
4. 社員ネットワーク セキュリティを **enterprise** と入力した場合は、次を指定します。
   - RADIUS サーバのアドレス。
   - RADIUS サーバのポート。
   - RADIUS サーバのシークレット（パスワード）。
5. 社員ネットワーク セキュリティを **PSK** と入力した場合は、次を指定します。
   - PSK パス フレーズ（8 ~ 38 文字）を入力します。
   - PSK パス フレーズ（8 ~ 38 文字）を再入力します。

ステップ 11 [Guest Network] を有効にするには、**YES** を入力します。それ以外の場合は、**no** と入力します。

YES を入力した場合は、次のように入力します。

1. ゲスト ネットワーク名（SSID）。
2. ゲスト VLAN ID（0 = タグなし）。

3 ゲスト ネットワーク セキュリティ。**WEB_CONSENT** または **psk** を入力できます。

4 ゲスト ネットワーク セキュリティを **PSK** と入力した場合は、次を指定します。

- ゲスト パス フレーズ（8 ~ 38 文字）を入力します。
- ゲスト パス フレーズ（8 ~ 38 文字）を再入力します。

ステップ 12 RF パラメータの最適化を有効にするには、**YES** を入力します。それ以外の場合は、**no** と入力します。**YES** を入力した場合は、次のように入力します。

1 クライアント密度。必要に合わせて **TYPICAL**、**Low**、または **High** を入力できます。

2 音声を含むトラフィック。必要に合わせて **NO** または **yes** を入力できます。

ステップ 13 設定が正しいかどうかをたずねるプロンプトが表示されたら、**yes** または **NO** と入力します。**yes** と入力すると、コントローラは設定を保存してリブートし、ログオン プロンプトが表示されます。

アプリケーションの可視性コマンド

次のコマンドは、Mobility Express コントローラのアプリケーションの可視性の設定に使用されます。

コマンド	説明	本リリースでの追加
config flexconnect group default-flexgroup avc 1 visibility { enable | disable }	WLAN のアプリケーションの可視性を有効化または無効化します	8.1.122.0
show flexconnect group detail default-flexgroup	各 WLAN のアプリケーションの可視性のステータスを表示します	8.1.122.0
show flexconnect avc statistics group default-flexgroup	FlexConnect グループに基づいたアプリケーション可視性の統計情報を表示します	8.1.122.0
how flexconnect avc statistics client *client_MAC*	各クライアントに基づいたアプリケーションの可視性の統計情報を表示します	8.1.122.0

CleanAir コマンド

コマンド	説明	本リリースでの追加
config 802.11b cleanair enable *ap_MAC*	関連する AP で CleanAir を有効化します。1850 および 1830 シリーズ AP には適用されません。	8.1.122.0
show 802.11b cleanair device ap *ap_MAC*	AP に接続しているすべての干渉デバイスを表示します。	8.1.122.0
show 802.11b cleanair device type jammer	特定の干渉デバイスを電波妨害します。	8.1.122.0

コントローラ イメージのアップグレード コマンド

次のコマンドは、Mobility Express コントローラ ソフトウェア イメージのアップグレードを実行する場合に使用されます。

コマンド	説明	本リリースでの追加
transfer download ap-images imagePath *image_path*	TFTP サーバのソフトウェア イメージのパスを設定します	8.1.122.0
transfer download ap-images mode tftp	ファイル転送モードを TFTP に設定します	8.1.122.0
transfer download ap-images serverIp *ipv4_address*	TFTP サーバの IP アドレスを指定します	8.1.122.0
transfer download start	設定を保存し、イメージのダウンロードを開始します	8.1.122.0
debug transfer all { enable | disable }	有効になっているすべてのサブ コマンドを使用して転送とダウンロードをデバッグします	8.1.122.0
debug transfer tftp { enable | disable }	TFTP の転送ダウンロードをデバッグします	8.1.122.0

コマンド	説明	本リリースでの追加
debug transfer trace { enable | disable }	転送トレースをデバッグします	8.1.122.0

DNS コマンド

コマンド	説明	本リリースでの追加
config network dns default	デフォルト DNS サーバを設定します。	8.2.100.1
show network summary	デフォルト DNS サーバ（有効の場合）がリストされているネットワーク概要を表示します。	8.2.100.1

移行コマンド

次のコマンドは、Mobility Express ソフトウェア イメージから Lightweight CAPWAP AP ソフトウェア イメージに AP を変換する場合、およびその反対に変換する場合に使用されます。

コマンド	説明	本リリースでの追加
ap-type capwap	Mobility Express から CAPWAP に AP タイプを変換します	8.1.122.0
ap-type mobilityexpress tftp://*tftp_server*/*file_name*	Mobility Express ソフトウェア イメージの実行時に CAPWAP から Mobility Express に AP タイプを変換します	8.1.122.0
config ap unifiedmode *switch_nameswitch_IP_address*	すべての AP をスイッチから CAPWAP にタイプを同時に変換します	8.1.122.0

NTP コマンド

コマンド	説明	本リリースでの追加
config time ntp server 1 *FQDN_of_server*	NTP サーバ（ここでは例として、NTP インデックス 1 を持つ）の完全修飾ドメイン名を設定します。	8.2.100.1
config time ntp server 2 *NTP_Server_IP_address*	NTP サーバ（ここでは例として、NTP インデックス 2 を持つ）の IP アドレスを設定します。	8.2.100.1

UX 規制ドメイン コマンド

コマンド	説明	本リリースでの追加
config wlan disable 1	WLAN 1 を無効にします	8.1.122.0
config wlan universal-ap-admin enable 1	WLAN 1 のユニバーサル AP 管理者として有効化します	8.1.122.0
config wlan enable 1	WLAN 1 を有効にします	8.1.122.0
show ap summary	UX ではない場合、設定されている現在の国（US、IN など）を表示します	8.1.122.0

VRRP コマンド

次の Virtual Router Redundancy Protocol（VRRP）コマンドは、Mobility Express コントローラのフェールオーバー時にマスター AP のために使用されます。

コマンド	説明	本リリースでの追加
config ap next-preferred-master	新しいマスター AP として引き継ぐために選択されたマスター AP を設定します	8.1.122.0

コマンド	説明	本リリースでの追加
show ap next-preferred-master	マスター AP の状態を表示します	8.1.122.0
clear ap next-preferred-master	マスター AP の設定をクリアします	8.1.122.0

WGB コマンド

次の show コマンドはワークグループ ブリッジ（WGB）の詳細を表示するために使用できます。

コマンド	説明	本リリースでの追加
show wgb summary	ワークグループ ブリッジの概要を表示します	8.1.122.0
show wgb detail *WGB_MAC*	特定のワークグループ ブリッジの詳細を表示します	8.1.122.0

付 録 B

付録

Cisco Mobility Express ソリューションの機能と仕様

Cisco Mobility Express ソリューションの技術仕様、サポートされる機能とサポートされない機能、および相互運用性情報の詳細なリストについては、次の URL にある「*Release Notes for Cisco Wireless Controllers and Lightweight Access Points for Cisco Wireless Release 8.1.120.0*」を参照してください。
http://www.cisco.com/c/en/us/td/docs/wireless/controller/release/notes/crn81mr2.html

対応ブラウザ

オペレーティング システム	サポートされるブラウザとバージョン
Microsoft Windows	• Internet Explorer 10 以降 • Mozilla Firefox 33 以降 • Google Chrome 38 以降
Apple MAC OS	• Safari 7 以降 • Mozilla Firefox 33 以降 • Google Chrome 38 以降

Cisco Mobility Express コントローラのフェールオーバーとマスター AP の選定プロセス

Mobility Express コントローラのフェールオーバーのための冗長性

Cisco Mobility Express ネットワークには、マスター AP として機能できない AP が存在することがあります。マスター AP として機能できる AP モデルについては、サポートされる Cisco Aironet アクセス ポイント，（2 ページ）を参照してください。

フェールオーバーを可能にする冗長性を Cisco Mobility Express コントローラに持たせるには、ネットワークに、マスター AP として機能できるアクティブな AP が複数必要です。フェールオーバーの発生時に、これらの AP の 1 つが自動的にマスターとして選定されます。新しく選定されたマスターは、元のマスターと同じ IP および設定になります。管理者にとっては、フェールオーバー発生時、元のマスターと新しく選定されたマスターに違いはありません。

（注） マスター AP に接続されているクライアントは、フェールオーバー時に切断されます。

マスター AP の選定プロセス

Cisco Mobility Express AP ネットワークでマスター AP がシャットダウンすると、この導入環境でマスターとして機能できる他の AP の 1 つが自動的にマスター AP に指定されます。内部のマスター自動選定プロセスにより、Cisco Mobility Express 対応の AP からマスター AP が自動的に選択されます。このプロセスは 2 つの目的で使用されます。1 つはマスター AP の障害を検出すること、もう 1 つはマスターとして機能できる AP から新しいマスター AP を指定することです。この

プロセスは Virtual Router Redundancy Protocol（VRRP）に基づいており、優先順位の降順でリストしてある次のパラメータを基にアルゴリズムで次のマスター AP を決定します。

- コントローラの CLI で VRRP コマンド **config ap next-preferred-master** を使用して VRRP マスターとして設定された AP。
- 関連付けられているクライアント数を基準に負荷が最小である AP。
- クライアントの負荷が同程度の AP の中で、MAC アドレスが最小である AP。

Cisco Mobility Express ネットワークにアクセス ポイントを追加する方法

CAPWAP Lightweight AP ソフトウェアを実行しているサポート対象の AP を Cisco Mobility Express ネットワークに追加すると、起動時に CAPWAP の状態が Discover advertisements on boot up になります。マスター AP で動作する Cisco Mobility Express コントローラはこのアドバタイズメントに応答し、新しい AP は Cisco Mobility Express コントローラの join プロセスを実行します。追加される AP が同じバージョンを実行している場合は、すぐに Cisco Mobility Express ネットワークに join します。ただし、AP が Cisco Mobility Express で実行されているイメージより古いイメージを実行している場合は、対応する Cisco Mobility Express 対応 AP イメージをコントローラが TFTP サーバからダウンロードします。

ソフトウェア アップデートの実施方法については、Cisco Mobility Express ソフトウェアの更新, （52 ページ）を参照してください。

アクセス ポイントへのイメージのプレダウンロード

コントローラからアクセス ポイントへアップグレード ソフトウェア イメージをダウンロードするときには、アクセス ポイントをリセットしたり、ネットワーク接続を切断したりする必要はないため、ネットワークの停止を最小限に抑えることができます。つまり、アップグレード イメージは最初にコントローラにダウンロードされ、その後アクセス ポイントにダウンロードされます。その際、ネットワークは稼働したままになります。コントローラを再起動すると、アクセス ポイントの関連付けが解除され、アクセス ポイントが再起動します。コントローラが最初に起動し、その後で、イメージがアップグレードされたすべてのアクセス ポイントが起動します。コントローラがアクセス ポイントから送信されたディスカバリ要求に自身のディスカバリ応答パケットで応答すると、アクセス ポイントから join 要求が送信されます。

Mobility Express から CAPWAP Lightweight ソフトウェアへの AP の変換

Mobility Express コントローラを実行している AP を CAPWAP Lightweight 導入環境（つまり、Unified Wireless Network）用に変換するには、以下のステップに従います。

1. コンソール ポート、Telnet、または SSH を AP に接続します。
2. Mobility Express コントローラ コンソールにログインします。
3. Mobility Express コントローラ コンソールで **apciscoshell** コマンドを使用して、AP コンソールに接続します。
4. ユーザ名 *Cisco* とパスワード *Cisco* を使用して AP コンソールにログインします。どちらも大文字と小文字が区別されます。
5. **enable** と入力します。
6. **ap-type capwap** コマンドを入力し、確認します。

   これにより、AP が設定完了済みの CAPWAP Lightweight に変換されます。この AP は、変換し直して元に戻さない限り、Mobility Express マスター AP として機能できません。

RF パラメータの最適化設定

RF パラメータの最適化設定を初期化ウィザード中に行う場合は、次の表の情報を使用して導入に適切な設定を選択します。次の表は、低、標準、または高密度のクライアントのタイプが選択された場合のデフォルト値を示します。

（注） 初期化ウィザードで RF パラメータの最適化を有効にしない場合、クライアント密度は標準（デフォルト値）に設定され、RF トラフィック タイプはデータ（デフォルト値）に設定されます。

	依存関係	標準（企業向けの導入。デフォルトのプロファイル。）	高密度（スループットが最も重要な場合）	低密度（オープンスペースのカバレッジの場合）
TX 電力	帯域ごとにグローバル	デフォルト	高	最高
TPC しきい値、TPC 最小値および TPC 最大値 （これらのパラメータは、TX 電力と同じです）	帯域ごとに特定の RF プロファイル	TPC 最小値：デフォルトは -10 dB TPC 最大値：デフォルトは 30 dB	TPC しきい値： • 5 GHz の場合 -65 dB • 2.4 GHz の場合 -70 dB TPC 最小値：+7 dB TPC 最大値：デフォルトは 30 dB	TPC しきい値： • 5 GHz の場合 -60 dB • 2.4 GHz の場合 -65 dB TPC 最小値：-10 dB TPC 最大値：デフォルトは 30 dB

	依存関係	標準（企業向けの導入。デフォルトのプロファイル。）	高密度（スループットが最も重要な場合）	低密度（オープンスペースのカバレッジの場合）
Rx 感度	帯域ごとにグローバル（Advanced RX-SOP） RF プロファイル	デフォルト（自動）	中程度（RX-SOP）	低
CCA しきい値	帯域ごとにグローバル 802.11a のみ（非表示） RF プロファイル	デフォルト（0）	デフォルト（0）	デフォルト（0）
カバレッジ RSSI しきい値	帯域ごとにグローバル データと音声 RSSI RF プロファイル	デフォルト（データ：-80、音声：-80）	デフォルト（データ：-80、音声：-80）	高（データ：-90、音声：-90）
カバレッジクライアント数	帯域ごとにグローバル（カバレッジ例外） RF プロファイル（カバレッジホール検出）	デフォルト（3）	デフォルト（3）	低（2） 低（1 ～ 3）
データ レート	帯域ごとにグローバル（ネットワーク） RF プロファイル	12 Mbp（必須） 9 Mbp をサポート 1、2、5.5、6、11 Mbp は無効	12 Mbp（必須） 9 Mbp をサポート 1、2、5.5、6、11 Mbp は無効	CCK レートは有効 1、2、5.5、6、9、11、12 Mbp は有効

関連資料

Cisco Mobility Express Release Notes

http://www.cisco.com/c/en/us/td/docs/wireless/controller/release/notes/crn81mr2.html

Cisco Wireless Controller Command Reference, Release 8.1

http://www.cisco.com/c/en/us/td/docs/wireless/controller/8-1/cmd-ref/b_cr81.html

Cisco Aironet 1850 Series Access Points Hardware Installation Guide

http://www.cisco.com/c/en/us/td/docs/wireless/access_point/1850/hardware/guide/ap1850hwguide.html

Cisco Aironet 1830 Series Access Points Getting Started Guide

http://www.cisco.com/c/en/us/td/docs/wireless/access_point/1830/quick/guide/ap1830getstart.html

Cisco Aironet Universal AP Priming and Cisco AirProvision User Guide

http://www.cisco.com/c/en/us/td/docs/wireless/access_point/ux-ap/guide/uxap-mobapp-g.html

よくある質問

Mobility Express ワイヤレス LAN コントローラ機能をホストできるアクセス ポイント、およびそれによって管理できるアクセス ポイントはどれですか。

サポートされる Cisco Aironet アクセス ポイント, （2 ページ）を参照してください。

Mobility Express ワイヤレス LAN コントローラ機能でサポートされるコントローラベースのモードは何ですか。

Mobility Express ソリューションによって管理されるアクセス ポイントは、AireOS FlexConnect モードと同様に、集中型コントロールプレーン モードと分散型データ プレーン モードで動作します。

Mobility Express のライセンス要件はどうなっていますか。

Cisco Mobility Express ソリューションにはアクセス ポイント用のライセンスが必要ありません。

アクセス ポイントのスケールを拡大し、ワイヤレス コントローラ導入環境用に変換できますか。

はい。アクセス ポイントにプライマリ コントローラとして WLAN コントローラの IP アドレスを指し示すだけで実現できます。これはモードに依存しません。WLAN コントローラは、適切な AP イメージとそれぞれの設定をプッシュします。詳細については、Mobility Express から CAPWAP Lightweight ソフトウェアへの AP の変換, （71 ページ）を参照してください。

導入環境を縮小してアクセス ポイント数を 25 以下にする必要がある場合、既存のコントローラベースの導入環境から Mobility Express に変換することはできますか。

はい。導入環境に含まれるアクセス ポイントが Mobility Express コントローラ機能をホストできる場合は（Cisco Aironet 1850 または 1830 シリーズのアクセス ポイントなど）、ワイヤレス コントローラベースの導入環境を Mobility Express に変換できます。

Cisco Mobility Express ソリューションの詳細はどこで確認できますか。

http://www.cisco.com/go/mobilityexpress に進みます。