



Cisco Wireless リリース 8.6 向け Cisco Mobility Express ユーザガイド

初版：2017年11月30日

最終更新：2021年2月16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。

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2018–2021 Cisco Systems, Inc. All rights reserved.



目次

第 1 章

Cisco Mobility Express について 1

- Cisco Mobility Express の概要 1
- サポートされているシスコのアクセス ポイント 2
- サポートされるソフトウェア イメージ 2

第 2 章

使用する前に 5

- Cisco Mobility Express の設定とアクセスの前提条件 5
- Cisco Plug and Play を介したプライマリ AP の自動プロビジョニング 6
- スイッチポートの設定 7
- 初期設定ウィザードの起動 7
- 初期設定ウィザードの使用 8
- 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 11
- CAPWAP Lightweight AP から Cisco Mobility Express ソフトウェアへの変換 13
- プライマリ AP に関連付ける AP の準備 14
- Cisco Mobility Express へのログイン 15
- Mobility Express コントローラの Web インターフェイスについて 16

第 3 章

Mobility Express ネットワークのモニタリング 19

- Cisco Mobility Express モニタリング サービスについて 19
- [Network Summary] ビューのカスタマイズ 20
 - WLAN ユーザの表示と管理 23
 - WLAN の表示 23
- 設定済み WLAN の詳細の表示 23

[Access Points] テーブル ビューのカスタマイズ	24
クライアントの詳細の表示	24
モビリティ状態のグラフィックについて	25
クライアントの ping テストの実行	25
クライアント パケットのキャプチャ	25
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	27
干渉源の詳細の表示	27
[Access Point Performance] ビューのカスタマイズ	28
[Access Point 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	28
[Access Point 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	29
[Client Performance] ビューのカスタマイズ	29
[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	30
[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	31

第 4 章

ワイヤレス設定の指定 33

WLAN と WLAN ユーザのセットアップ	33
Cisco Mobility Express ネットワーク内の WLAN について	33
WLAN の追加	34
WLAN の有効化と無効化	38
WLAN の編集と削除	39
WLAN ユーザの表示と管理	39
関連付けられているアクセス ポイントの管理	40
アクセス ポイントの管理	41
外部アンテナの設定	44
WLAN ゲスト ユーザのログイン ページの設定	45
デフォルトのログイン ページの設定	46
カスタマイズされたログイン ページの設定	46
内部 DHCP サーバの管理	48
DHCP プールの追加	48
DHCP プールの編集	49
DHCP プールの削除	49

DHCP リースの詳細の表示	50
リース IP アドレスの詳細のエクスポート	50
リース IP アドレスの開放	50

第 5 章
ネットワークの管理 53

管理アクセス インターフェイスの設定	53
Admin アカウントの管理	54
管理者アカウントの追加	55
管理者アカウントの編集	56
管理者アカウントの削除	56
ロビー管理者アカウントを使用したゲスト ユーザの管理	56
ゲスト ユーザ アカウントの作成	57
日時の設定	58
自動的に日時を設定するための NTP サーバの使用	58
NTP サーバの追加と編集	58
NTP サーバ ステータスの更新	59
NTP サーバの削除と無効化	59
日時の手動設定	59
Cisco Mobility Express ソフトウェアの更新	60
HTTP を使用したソフトウェア アップデート	61
TFTP を使用したソフトウェア アップデート	63
SFTP を使用したソフトウェア アップデート	65
Cisco.com からのソフトウェア直接アップデート	66

第 6 章
詳細設定の使用と操作 69

SNMP の管理	69
SNMP アクセスの設定	69
SNMPv3 ユーザの追加	70
SNMPv3 ユーザの編集	71
SNMPv3 ユーザの削除	72
システム メッセージ ロギングの設定	72

RF パラメータの最適化	74
コントローラ ツールの使用	74
コントローラの再起動	74
コントローラ コンフィギュレーションのクリアとコントローラのリセット	74
コントローラ コンフィギュレーションのエクスポートとインポート	75
コントローラ コンフィギュレーションの保存	75
CMX クラウドプレゼンス分析の使用	76
CMX プレゼンス分析の前提条件	76
CMX プレゼンス分析の有効化	77

付録 A :

コントローラ CLI コマンド	79
Cisco Mobility Express CLI	79
CLI 初期設定ウィザードの使用	79
CLI での手順	83
SNMPv3 ユーザのデフォルト値の変更	83
802.11r 高速移行の設定	84
CDP タイマーの設定	85
Cisco Mobility Express (CLI) での Cisco Umbrella の設定	85

付録 B :

概念、FAQ、および高度なユーザに関する情報	87
対応ブラウザ	87
Cisco Mobility Express コントローラのフェールオーバーとプライマリ AP の選定プロセス	88
アクセス ポイントへのイメージのプレダウンロード	89
CAPWAP の Mobility Express 変換の代替手段	90
Mobility Express から CAPWAP タイプへの AP の変換	91
RF パラメータの最適化設定	92
関連資料	93
よくある質問	94



第 1 章

Cisco Mobility Express について



(注) この製品のマニュアルセットは、偏向のない言語を使用するように配慮されています。このドキュメントセットでの偏向のない言語とは、年齢、障害、性別、人種的アイデンティティ、民族的アイデンティティ、性的指向、社会経済的地位、およびインターセクショナルリティに基づく差別を意味しない言語として定義されています。製品ソフトウェアのユーザインターフェイスにハードコードされている言語、RFPのドキュメントに基づいて使用されている言語、または参照されているサードパーティ製品で使用されている言語によりドキュメントに例外が存在する場合があります。

- [Cisco Mobility Express の概要 \(1 ページ\)](#)
- [サポートされているシスコのアクセス ポイント \(2 ページ\)](#)
- [サポートされるソフトウェア イメージ \(2 ページ\)](#)

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、802.11ac Wave 2 Cisco Aironet シリーズのアクセスポイント (AP) 1 ヶ所以上と、ネットワーク内の他の AP を管理する内蔵ソフトウェアベースのワイヤレス コントローラ (WLC) から構成されます。

WLC として機能している AP をプライマリ AP といい、このプライマリ AP によって管理される Cisco Mobility Express ネットワーク内のその他の AP を下位 AP といいます。

WLC として機能する他に、プライマリ AP は下位 AP と連動してクライアントとして機能する AP としても動作します。

Cisco Mobility Express は Cisco WLC のほとんどの機能を提供し、また、次とのインターフェイスとなる機能を備えています。

- 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。

- Connected Mobile Experiences (CMX) : Connect & Engage を使用してプレゼンス分析とゲストアクセスを提供します。

サポートされているシスコのアクセスポイント

次の Cisco Aironet シリーズの AP が Cisco Mobility Express ネットワークでサポートされています。



- (注)
- プライマリ AP の下にリストされている AP も下位 AP としても機能できます。
 - プライマリ AP の下にリストされているソフトウェアは、Cisco Mobility Express から CAPWAP Lightweight AP におよびその逆に変換できます。ご注文に際しては、『[Cisco Aironet Access Points Ordering Guide](#)』を参照してください。

表 1: Cisco Mobility Express でサポートされている Cisco AP

プライマリ AP	下位 AP
Cisco Aironet 1560 シリーズ	Cisco Aironet 700i シリーズ
Cisco Aironet 1815i	Cisco Aironet 700w シリーズ
Cisco Aironet 1815w	Cisco Aironet 1600 シリーズ
Cisco Aironet 1830 シリーズ	Cisco Aironet 1700 シリーズ
Cisco Aironet 1850 シリーズ	Cisco Aironet 1810W シリーズ
Cisco Aironet 2800 シリーズ	Cisco Aironet 2600 シリーズ
Cisco Aironet 3800 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

サポートされるソフトウェアイメージ

プライマリ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により変換できます。この変換については、[CAPWAP Lightweight AP から Cisco Mobility Express ソフトウェアへの変換 \(13 ページ\)](#) 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、<https://software.cisco.com/download/navigator.html> からダウンロードできます。

[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りリリースに移行することを推奨します。



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](#) (5 ページ)
- [Cisco Plug and Play を介したプライマリ AP の自動プロビジョニング](#) (6 ページ)
- [スイッチポートの設定](#) (7 ページ)
- [初期設定ウィザードの起動](#) (7 ページ)
- [初期設定ウィザードの使用](#) (8 ページ)
- [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](#) (11 ページ)
- [CAPWAP Lightweight AP から Cisco Mobility Express ソフトウェアへの変換](#) (13 ページ)
- [プライマリ AP に関連付ける AP の準備](#) (14 ページ)
- [Cisco Mobility Express へのログイン](#) (15 ページ)
- [Mobility Express コントローラの Web インターフェイスについて](#) (16 ページ)

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 をプライマリ 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）はプライマリ AP によってのみアドバタイズされ、他の AP によってアドバタイズされません。
- 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。
- Cisco Mobility Express は内部 DHCP サーバを提供しており、初期設定ウィザードを実行している間に必要に応じて設定できます。ただし、この代わりに外部 DHCP サーバを使用す

る場合は、DHCPサーバが存在し、ネットワーク内でアクセスできることを確認します。Cisco 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アドレスの管理にこの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。

プライマリ 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 \(87 ページ\)](#) 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、[スイッチポートの設定 \(7 ページ\)](#) 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 \(79 ページ\)」](#) を参照してください。

Cisco Plug and Play を介したプライマリ AP の自動プロビジョニング

Cisco Network Plug and Play (PnP) ソリューションを使用すると、リモートの Cisco Application Policy Infrastructure Controller エンタープライズモジュール (APIC-EM) サーバを介してプライマリ AP を自動的にプロビジョニングできます。PnP は Cisco Mobility Express ネットワーク展開のデフォルト時の初期設定の場合にのみ有効になります。

デフォルト時に Cisco Mobility Express 対応 AP が Cisco Mobility Express ネットワークに複数ある場合、VRRP を介してそれらの AP の中からプライマリ AP を選択します。選択したこのプライマリ AP は、次の方法のいずれかを通じ、PnP を介して APIC-EM サーバからプロビジョニングパラメータを受け取ります。

- シスコクラウドを介して APIC-EM にリダイレクト
- DHCP オプション 43 を介して

- DNS ディスカバリを介して

Cisco PnP を使用した自動プロビジョニングの前提条件および詳細な手順については、『[Cisco Network Plug and Play](#)』を参照してください。

スイッチポートの設定

アクセスポイントをスイッチに接続して電源を入れます。スイッチポートを設定する際に、次のことを確認します。

- Mobility Express ネットワーク内のプライマリ AP を含むすべてのアクセスポイントは、同じ L2 ブロードキャストドメインに存在する必要があります。管理トラフィックにタグを付けることはできません。
- プライマリ AP が接続されるスイッチポートはトランクポートまたはアクセスポートであり、また管理トラフィック用のネイティブ VLAN をトランキングするように設定する必要があります。データトラフィックは、ローカルスイッチング用の適切な VLAN とトランキングする必要もあります。

次に、スイッチポートの設定例を示します。

```
Interface GigabitEthernet1/0/37
description » Connected to Master AP «
switchport trunk native vlan 122
switchport trunk allowed vlan 10,20,122
switchport mode trunk
```

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。

最初に AP の電源を入れてから *CiscoAirProvision* SSID がブロードキャストを開始するまでには、数分かかります。*CiscoAirProvision* SSID がブロードキャストを開始したら、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 初期設定ウィザードにアクセスするために、サポートされている Web ブラウザを開き、URL として *mobilityexpress.cisco* を入力します。管理者アカウントを作成しようとすると、ウィザードが起動されます。

Apple クライアントでは、*CiscoAirProvision* SSID に接続後、初期設定ウィザードと一緒にキャプティブポータルウィンドウが自動的に開く場合があります。このウィンドウを使用して、Web ブラウザを開かずに初期設定を完了できます。

- (注) *CiscoAirProvision* SSID に接続した後で Web ブラウザを開いたら、自動的に *mobilityexpress.cisco* へリダイレクトされます。自動的にリダイレクトされない場合は、URL *mobilityexpress.cisco* または go to *http://192.168.1.1* を手動で入力します。これらはどちらも初期設定ウィザードにリダイレクトします。

次のタスク

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、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 (11 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。



- (注) 工場出荷時の Cisco Mobility Express 対応 AP のユーザ名とパスワードを変更します。デフォルトのクレデンシャルである [cisco] (大文字と小文字は区別されません) を使用する場合は、これらの AP では SSH が無効になります。

- 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 サーバの詳細を編集するには、**[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。
- **[Enable DHCP Server (Management Network)]** : これはオプションです。内部 DHCP サーバを有効にする場合は、次のパラメータを指定します。
 - ネットワーク
 - マスク
 - 管理 VLAN ID
 - 開始 IP

- 終了 IP
- ドメイン名
- ネーム サーバ

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。これにより、ゲスト ネットワーク アクセスよりも多くの権限が提供されます。
- **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 ~ 4094 の VLAN ID を指定) します。
- **VLAN ID** : 新規 VLAN の VLAN ID を指定します。
- **[Enable DHCP Server (Employee Network)]** : これはオプションです。[Employee Network] で IP アドレスを割り当てるために内部 DHCP サーバを有効にする場合は、次のパラメータを指定します。
 - ネットワーク
 - マスク
 - 開始 IP
 - 終了 IP
 - デフォルト ゲートウェイ
 - ドメイン名
 - ネーム サーバ
 - ネーム サーバ IP1

• ネーム サーバ IP2

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 ~ 4094 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 \(92 ページ\)](#) 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。これを後で変更するには、[RF パラメータの最適化 \(74 ページ\)](#) を参照してください。

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 \(15 ページ\)](#) 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

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 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。

次のタスク

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 Image Type : MOBILITY EXPRESS IMAGE AP Configuration : NOT MOBILITY EXPRESS CAPABLE	<p>これは、APにCisco Mobility Express ソフトウェアが含まれているものの、APがCAPWAP Lightweight APとして動作していることを表しています。</p> <p>このAPは、現在、Mobility Express コントローラとして動作するように設定されていません。また、プライマリ APの選定プロセスにも参加していません。したがって、CiscoAirProvision SSIDをブロードキャストしません。ただし、このAPは、Mobility Express ネットワークの下位 APとして機能できます。</p> <p>このAPのMobility Express コントローラ機能を有効にするには、AP コンソールで <code>ap-type mobility-express tftp</code> コマンドを実行します。APが再起動し、オンラインに戻り、プライマリ APの選定プロセスに参加します。これがプライマリとして選定されると、その時点でCiscoAirProvision SSIDをブロードキャストするようになります。</p>

出力のフィールドと値	次の作業
[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 から Cisco Mobility Express ソフトウェアへの変換 (13 ページ) に進みます。

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

AP 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には、次の手順に従います。

note



ヒント AP ソフトウェアから Cisco Mobility Express ソフトウェアへの変換で問題が発生した場合、AP CAPWAP ソフトウェアを最新の AP ソフトウェア バージョンの ap3g3-k9w8-tar.153-3.JD.tar にアップグレードします。CAPWAP ソフトウェアを Cisco Mobility Express ソフトウェア AIR-AP2800-K9-ME-8-3-102-0.tar に変換できるようになりました。

この問題は、デフォルトのイメージで出荷されるか、または Cisco Wireless リリース 8.3 より前のバージョンの Mobility Express 対応 AP で発生します。これは AP のメモリに十分なスペースがないか、または AP が U ブートモードで起動してもイメージがフラッシュで見つからないために発生します。



(注) 次の手順では、1850 シリーズの AP 上の 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、および AP モデルに応じて、必ず適切なソフトウェア ファイルを使用してください。

始める前に

- 現在の AP は、Lightweight AP ソフトウェアリリース 15.3.3-JBB5 (Cisco ワイヤレス コントローラ 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。
- 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。

- `capwap ap erase all` コマンドを使用して、AP のプライミング設定を削除してください。

ステップ 1 Cisco.com から TFTP サーバへ AIR-AP1850-K9-8.1.122.0.tar ソフトウェア ファイルをダウンロードします。ソフトウェア ダウンロード ページで、対象リリースのこの .tar ファイルは、「Lightweight アクセス ポイントからの変換にのみ使用されるソフトウェア (Software to be used for conversion from Lightweight Access Points only)」というラベルが付けられています。

ステップ 2 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 of TAR file with path from root on the TFTP server>` コマンドを使用します。

ソフトウェア ファイルが AP にダウンロードされ、AP のフラッシュ メモリに書き込まれます。AP は Mobility Express 対応の構成でリブートし、CiscoAirProvision SSID のブロードキャストを開始します。

次のタスク

上記の変換プロセスの .zip ファイルを使用する代替手段については、[CAPWAP の Mobility Express 変換の代替手段 \(90 ページ\)](#) を参照してください。

Mobility Express タイプから CAPWAP タイプに AP を変換する方法については、[Mobility Express から CAPWAP タイプへの AP の変換 \(91 ページ\)](#) を参照してください。

プライマリ AP に関連付ける AP の準備

新しい AP をプライマリ 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。

始める前に

- Cisco Mobility Express ワイヤレスコントローラを使用するプライマリ AP は動作中である必要があります。
- プライマリ 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。。
-

次のタスク

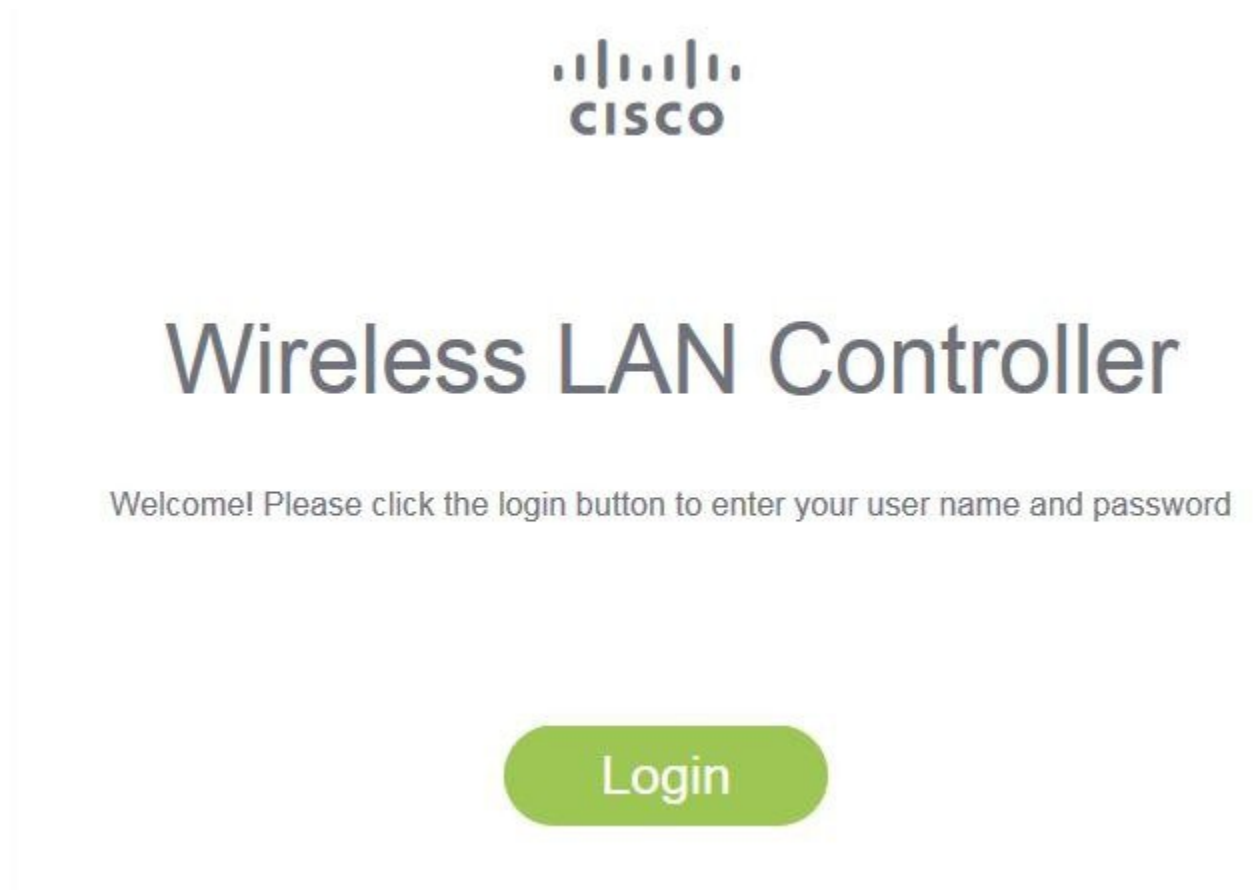
[関連付けられているアクセス ポイントの管理 \(40 ページ\)](#)

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。Cisco 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。

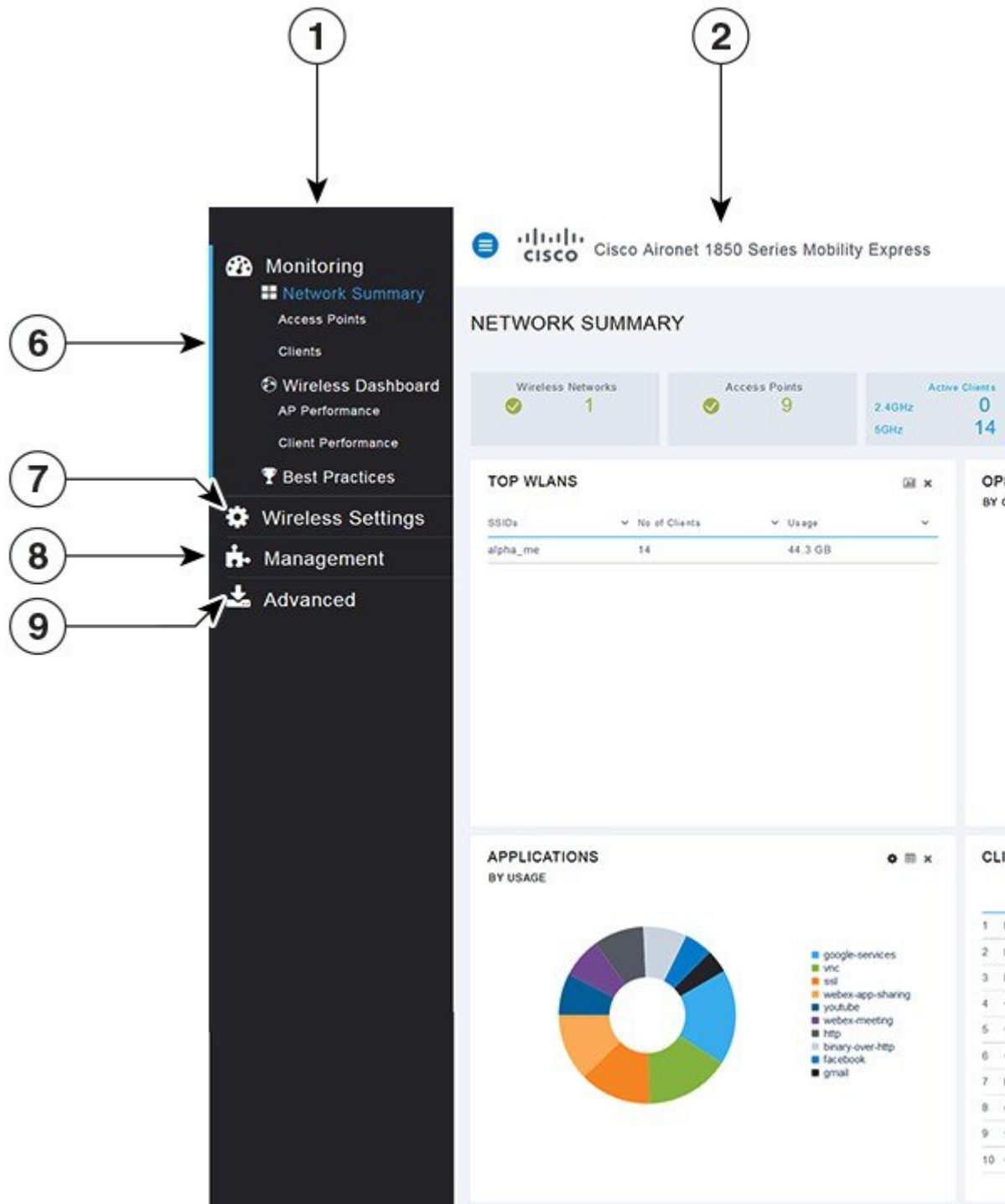
次のタスク

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 \(19 ページ\)](#) 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プライマリ 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。
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 (75 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 (19 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 (33 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。
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。



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 \(19 ページ\)](#)
- [\[Network Summary\] ビューのカスタマイズ \(20 ページ\)](#)
- [設定済み WLAN の詳細の表示 \(23 ページ\)](#)
- [\[Access Points\] テーブル ビューのカスタマイズ \(24 ページ\)](#)
- [クライアントの詳細の表示 \(24 ページ\)](#)
- [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 \(27 ページ\)](#)
- [干渉源の詳細の表示 \(27 ページ\)](#)
- [\[Access Point Performance\] ビューのカスタマイズ \(28 ページ\)](#)
- [\[Client Performance\] ビューのカスタマイズ \(29 ページ\)](#)

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、プライマリ 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。



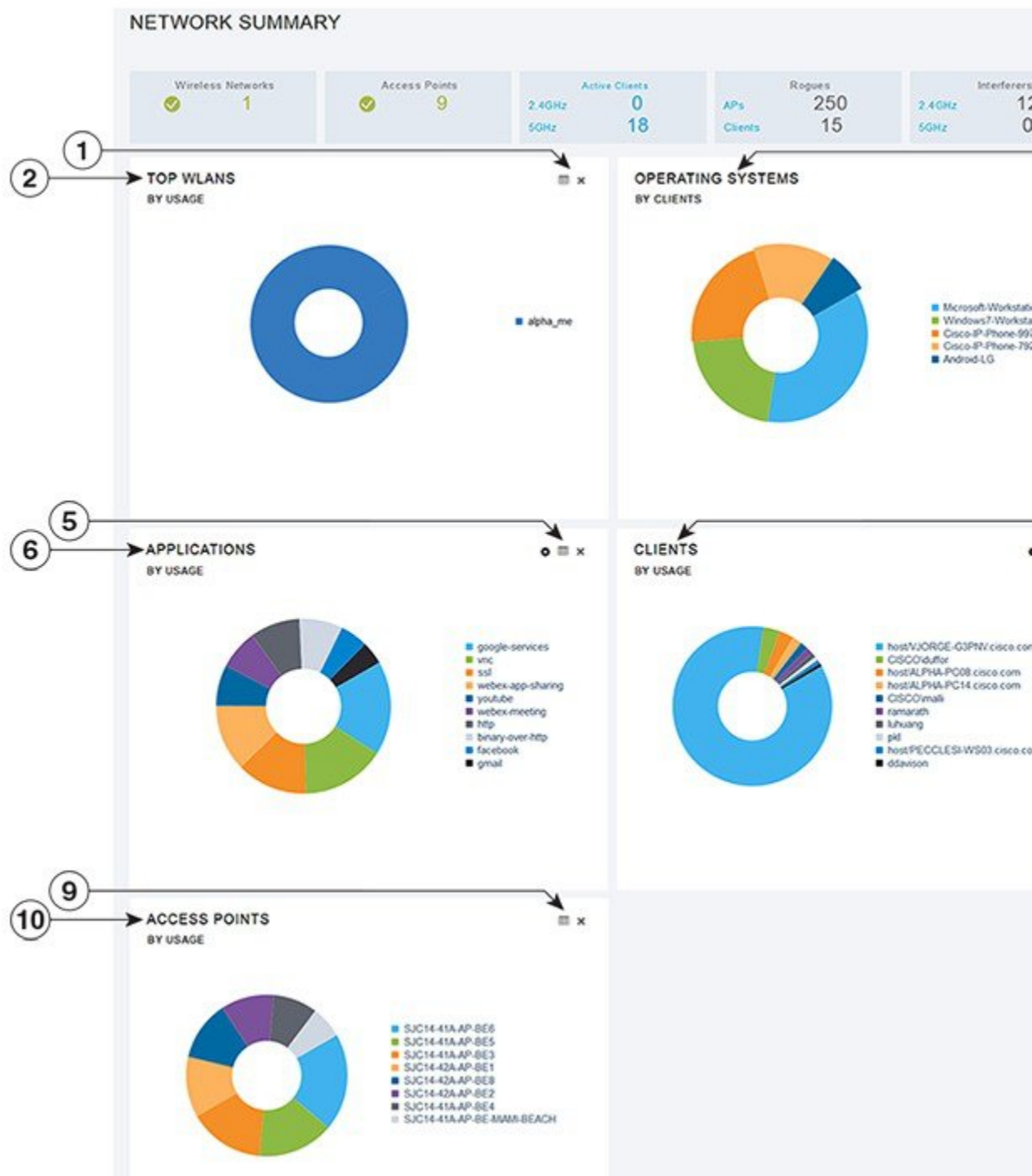
- (注)
- [Network Summary] ウィンドウに表示されるパラメータはすべて読み取り専用です。
 - このページは 30 秒ごとに自動的にリフレッシュされます。

[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 を使用してプライマリ 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、プライマリ 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。

[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



- (注) この機能は、Cisco AP-OS を備えた下位の AP 上、つまり、Cisco Aironet 1810W, 1830、1850、2800、および 3800 シリーズのアクセス ポイントでは動作しません。

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 \(33 ページ\)](#)
- [関連付けられているアクセス ポイントの管理 \(40 ページ\)](#)
- [WLAN ゲスト ユーザのログイン ページの設定 \(45 ページ\)](#)
- [内部 DHCP サーバの管理 \(48 ページ\)](#)

WLAN と WLAN ユーザのセットアップ

Cisco Mobility Express ネットワーク内の 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] > [WLANs] を選択します。

[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、プライマリ 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 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。

- 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 [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] : プロファイル名は一意であり、最大 32 文字までです。
- [SSID] : プロファイル名も SSID として機能します。WLAN プロファイル名とは異なる SSID を指定することができます。プロファイル名と同様に、SSID も 32 文字までとし、一意である必要があります。
- [Admin State] : ドロップダウンリストから [Enabled] を選択してこの WLAN を有効にするか、または [Disabled] を選択します。
デフォルトは [Enabled] です。
- [Radio Policy] : ドロップダウンリストで、次のオプションから選択します。
 - [All] : デュアルバンド (2.4 GHz と 5 GHz) 対応のクライアントをサポートするように WLAN を設定します。
 - [2.4 GHz only] : 802.11b/g/n 対応のクライアントのみをサポートするように WLAN を設定します。
 - [5 GHz only] : 802.11a/n/ac 対応のクライアントのみをサポートするように WLAN を設定します。

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、つまり、2.5 GHz または 5 GHz、あるいはその両方を指定します。

- [Broadcast SSID] : デフォルトは [Enabled] です。切り替えると、SSID が検出可能になります。それ以外の場合は、SSID は表示されません。
- ローカル プロファイリング

ステップ 4 [WLAN Security] タブで、[Security] ドロップダウンリスト リストから次のセキュリティ認証オプションのいずれかを設定します。

- **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は、[Shared Key] フィールドに PSK を指定し、[Confirm Shared Key] フィールドにもう一度指定して確認します。セキュリティ上の理由により、入力する PSK はアスタリスクで隠されます。表示するには、[Show Shared Key] チェックボックスをオンにします。

- **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。プライマリ 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。
- **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を設定するには、[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 Type] 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。

 - **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は、[Passphrase] フィールドに PSK を指定し、[Confirm Passphrase] フィールドにもう一度指定して確認します。セキュリティ上の理由により、入力する PSK はアスタリスクで隠されます。表示するには、[Show Passphrase] チェックボックスをオンにします。

- [Captive Portal (AP)] : 次の **キャプティブポータルタイプ** のいずれかをユーザに提示するキャプティブポータルを設定するには、こ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 \(39 ページ\)](#) を参照してください。
 - [Web Consent] : 表示された利用規約をゲストが受け入れたときに、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。
- [Captive Portal (External Web Server)] : ネットワーク外の Web サーバを使用して外部キャプティブポータル認証を取得するには、このオプションを選択します。また、[Site URL] フィールドにサーバの URL を指定します。
- [CMX Guest Connect] : Cisco CMX Connect を使用してゲストを認証するには、このオプションを選択します。また、[Site URL] フィールドに CMX クラウドサイトの URL を指定します。

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 : Internet Control Message Protocol (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. [宛先 IP / Mask (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、ネットワーク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 コントローラでは次の4つの QoS レベルがサポートされています。[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。

次のタスク

この時点で、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 \(39 ページ\)](#)」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。
- **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 (プライマリ 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 (プライマリ 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。

- [Operating Mode] および [Make me Controller] : プライマリ AP の場合、[Operating Mode] フィールドに AP とコントローラが表示されます。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。
[Make me Controller] ボタンは、プライマリの選定プロセスに含めることができる下位 AP に対してのみ使用できます。この AP をプライマリ AP にするには、このボタンをクリックします。
- 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。

- 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 (プライマリ 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。

- [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。
- [サブネット マスク (Subnet Mask)]
- [Country Code]

ステップ 5 [Radio 1] タブおよび [Radio 2] タブでは、次のパラメータを設定できます。

(注) [Radio 1] タブは、Cisco Aironet 3800 シリーズと 2800 シリーズの AP を除き、すべての AP の 2.4 GHz (802.11 b/g/n) 無線に相当します。これらの AP では、2.4 GHz (802.11 b/g/n) または 5 GHz (802.11a/n/ac) のいずれかに設定できます。[Radio 2] タブはすべての AP の 5 GHz (802.11a/n/ac) 無線のみに相当します。

また、無線タブ名は、カッコ内に運用無線帯域も示しています。

パラメータ	説明
[Admin Mode]	AP 上で対応する無線を有効または無効にします。
[Band]	[Radio 1] にのみ表示されます。デフォルトでは、2.4 GHz に設定されています。3800 シリーズと 2800 シリーズの AP の場合は、5 GHz に変更できます。

パラメータ	説明	
[Channel]	<p>2.4 GHz の場合、これを [Automatic] に設定するか、1 ~ 11 の値を設定します。</p> <p>[Automatic] を選択すると、動的チャンネル割り当てが有効になります。つまり、プライマリ AP の制御下にある各 AP にチャンネルが動的に割り当てられます。これにより、隣接する AP が同じチャン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 チャンネルが提供され、米国以外の国や地域では最大 14 チャン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。</p> <p>特定の値を割り当てると、その AP にチャンネルが静的に割り当てられます。</p>	<p>5 GHz の場合、これは [Automatic]、36、40、44、48、52、56、60、64、100、104、108、112、116、132、136、140、149、153、157、161、または 165 に設定できます。</p> <p>5 GHz の無線の場合は、最大 23 の非オーバーラップチャンネルが提供されます。</p> <p>特定の値を割り当てると、その AP にチャンネルが静的に割り当てられます。</p>
[Channel Width]	<p>2.4 GHz のチャンネル幅は 20 MHz にしか設定できません。</p>	<p>チャンネルボンディングを使用する場合、5 GHz のチャンネル幅は [Automatic]、あるいは 20、40、または 80 MHz に設定できます。</p> <p>チャンネルボンディングは、1 つの無線ストリーム用のチャンネルを 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 のチャン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ンネルを有効にするためにチャンネルボンディングを使用することはできません。</p>

パラメータ	説明
[Transmit Power]	<p>[Automatic] に設定するか、または 1 ~ 8 の値を設定できます。</p> <p>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。</p> <p>[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。</p>

ステップ 6 [Apply] をクリックして変更を保存し、終了します。

外部アンテナの設定

始める前に

アンテナの設定は、アクセスポイント用に設定されている外部アンテナに対して行います。アンテナの設定は、電波の受信状況を改善するのに重要です。アクセスポイント (AP) に外部アンテナが設定されている場合にのみ、[AP Edit] ウィンドウに [Antenna Configuration] タブが表示されます。

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。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 数が表示されます。

ステップ 2 設定する外部アンテナの横にある [Edit] アイコンをクリックします。

(注) AP に外部アンテナが設定されている場合にのみ、[Antenna Configuration] タブが表示されます。

[Antenna Configuration] タブのある [Edit] ウィンドウが表示されます。

ステップ 3 [Antenna Configuration] タブで、次のパラメータを設定します。

1. [Radio 2 (5GHz)] の下に次のパラメータを入力します。

1. [Diversity] では、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。

- 有効 (Enable) : ダイバーシティモードで左右のアンテナが動作するように設定するには、[Enable] を選択します。左右のアンテナの両方が、信号を送受信できるようになります。
- 右 (Right) : 右側のアンテナが信号を送受信するように設定するには、[Right] オプションを選択します。

3. 左 (Left) : 左側のアンテナが信号を送受信するように設定するには、[Left] オプションを選択します。
2. 送受信には、次のアンテナの組み合わせを選択します。
 1. A : アンテナ A を使用
 2. AB ; アンテナ A および B を使用
 3. ABC : アンテナ A、B、および C を使用
 4. ABCD : アンテナ A、B、C、および D を使用

(注) 無効な組み合わせを選択すると、エラーメッセージが表示されます。
3. [Antenna Gain] には、デバイスに接続されたアンテナの結果のゲインを指定します。-128 ~ 128 dB の値を入力します。必要に応じて、1.5 などの小数値を使用できます。
2. [Apply] をクリックして変更を適用します。

WLAN ゲストユーザのログイン ページの設定

開始する前に、次の手順を実行してゲストユーザにネットワークへのアクセスを提供します。

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 \(34 ページ\)](#) 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 \(39 ページ\)](#) を参照してください。

WLAN のゲストユーザには、次のログイン ページ オプションを表示できます。

- わずかな変更オプションを備えたシンプルで必要最低限のデフォルトのログイン ページ。これを設定するには、[デフォルトのログイン ページの設定 \(46 ページ\)](#) を参照してください。
- コントローラにアップロードされたカスタマイズされたログイン ページ。これを設定するには、[カスタマイズされたログイン ページの設定 \(46 ページ\)](#) を参照してください。

デフォルトのログイン ページの設定

設定が不要なデフォルトのログインページにはシスコロゴとシスコ独自のテキストが含まれています。このデフォルトのログイン ページをここで説明するように変更できます。

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 デフォルトのログイン ページを使用するには、[Page Type] ドロップダウンリストで [Internal] を選択します。

ステップ 3 次のパラメータを設定して、デフォルトの内部ログイン ページを変更します。

- [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。
- [ページ メッセージ (Page Message)] : デフォルトのメッセージは「シスコはお客様のネットワークに無線 LAN インフラストラクチャを提供します。を開始するにはログインしてエアスペースを入力してください。(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 4 [Apply] をクリックします。

カスタマイズされたログイン ページの設定

コンピュータにカスタム ログイン ページを作成し、そのページとイメージ ファイルを .TAR ファイルに圧縮した後、コントローラにアップロードすることができます。アップロードは HTTP を介して行われます。



- (注) コントローラの設定を保存する時点では、コントローラにダウンロードし、保存した Web 認証バンドルなどの余分なファイルやコンポーネントは含まれません。そのため、そのようなファイルのコピーを手動で外部にバックアップします。



(注) Cisco TAC はカスタム Web 認証バンドルを作成する責任を負いません。

始める前に

- コンピュータ上でカスタム ログイン ページを作成して、以下を確認します。
 - ログイン ページの名前を **login.html** とします。コントローラは、この名前に基づいて Web 認証 URL を作成します。Web 認証バンドルの展開後にこのファイルが見つからない場合、そのバンドルは破棄され、エラー メッセージが表示されます。
 - このページには 6 つ以上のエレメント (HTML、CSS、およびイメージ) を含めないでください。これは、内部コントローラの Web サーバが実装する DoS 保護メカニズムにより、各クライアントが開く同時 TCP 接続が負荷に応じて最大 5 つに制限されるためです。ページに多くの要素が含まれていて、ブラウザによる DoS 保護の処理方法によっては、ページのロードが遅くなることがある場合、一部のブラウザでは、同時に 5 つを超える TCP セッションが開かれようとしています。
 - ユーザ名とパスワード用のテキスト ボックスを含めます。
 - 元の URL からアクション URL を抽出して、ページに設定する。
 - リターン ステータス コードをデコードするスクリプトを提供する。
 - メインページで使用されるすべてのパス (たとえば、イメージへの参照など) が相対パスであること。
 - バンドル内のすべてのファイル名が 30 文字以内であること。

- ページとイメージファイルを TAR ファイルに圧縮します。ファイルの最大許容サイズは、非圧縮の状態です。

シスコは、GNU 標準に準拠しているアプリケーションを使用して .TAR ファイル (Web 認証バンドルとも呼ばれる) を圧縮することをお勧めします。GNU に準拠していない .TAR 圧縮アプリケーションで Web 認証バンドルをロードすると、コントローラはバンドル内のファイルを抽出できません。

.TAR ファイルはコントローラのファイルシステムに未展開ファイルとして入力されます。



(注) 前述の前提要件に準拠していないカスタマイズされた複雑な Web 認証バンドルがある場合、シスコは外部 Web サーバでそれをホストすることをお勧めします。(..)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** カスタマイズしたログインページをコントローラにアップロードするには、[Page Type] ドロップダウンリストで [Customized] を選択します。
- ステップ 3** [Upload] をクリックし、カスタマイズした Web 認証バンドルの .TAR ファイルを参照してアップロードします。
- ステップ 4** ログイン後にユーザを特定の URL（会社の URL など）にダイレクトさせる場合、[Redirect URL After Login] テキストボックスにその URL を入力します。最大 254 文字を入力することができます。
- ステップ 5** [Apply] をクリックします。
- [Preview] をクリックして、カスタマイズされた Web 認証ログイン ページを表示します。

内部 DHCP サーバの管理

Cisco Mobility Express コントローラには、内部 DHCP サーバが含まれています。このサーバは、それに関連付けられているネットワーク デバイスに割り当てられた DHCP アドレスを管理します。クライアントデバイスに割り当てられた IP アドレスはリブートすると失われます。これにより、複数のクライアントデバイスで IP アドレスを再利用できるようになります。IP アドレスの競合を解決するには、クライアントデバイスが既存の IP アドレスを解放し、新しいアドレスを要求する必要があります。

Cisco Wireless リリース 8.3 以降、Cisco Mobility Express の Web インターフェイスを使用して内部 DHCP サーバを設定できます。

DHCP プールの追加

- ステップ 1** [Wireless Settings] > [DHCP Server] を選択します。
- [DHCP Configuration] ウィンドウが表示されます。
- ステップ 2** [Add New Pool] をクリックします。
- [Add DHCP Pool] ウィンドウが表示されます。
- ステップ 3** [Pool Name] フィールドに、特定の名前を入力します。
- DHCP プール名は、次の条件を満たしている必要があります。
- ステップ 4** [Active] ドロップダウンリストから [Enabled] または [Disabled] のいずれかを選択します。
- デフォルト設定では [Disabled] になっています。
- ステップ 5** [VLAN ID] フィールドに、DHCP プールの VLAN ID を入力します。
- (注) [Management Network] チェックボックスを選択し、Cisco Mobility Express コントローラの管理インターフェイス IP アドレスを DHCP サーバの IP アドレスとして設定します。

- ステップ 6** [Network/Mask] フィールドに、ネットワークの IP アドレスとサブネットマスクを指定します。
- ステップ 7** [Start IP] フィールドに、ネットワークの開始 IP アドレスを指定します。
- ステップ 8** [End IP] フィールドに、ネットワークの終了 IP アドレスを指定します。
- ステップ 9** [Default Gateway] フィールドに、ネットワークへのデフォルト ゲートウェイの IP アドレスを指定します。
- (注) デフォルトのゲスト、開始 IP アドレス、および終了 IP アドレスは同じサブネット内にある必要があります。
- ステップ 10** [Domain Name] フィールドに、特定の名前を入力します。
- ドメイン名は、次の条件を満たしている必要があります。
- ステップ 11** [Name Servers] ドロップダウンリストから、[OpenDNS] または [User Defined] のいずれかを選択します。
- デフォルトの設定は [OpenDNS] です。
- ステップ 12** 表示されたフィールドにネーム サーバの IP アドレスを入力します。
-

DHCP プールの編集

- ステップ 1** [Wireless Settings] > [DHCP Server] を選択します。
- [DHCP Configuration] ウィンドウが表示されます。
- ステップ 2** 詳細を変更する DHCP プールが含まれている行で [edit_icon.gif] アイコンをクリックします。
- DHCP プール テーブル内の特定の行が編集可能になります (または、[Edit DHCP Pool] ウィンドウが表示されます)。
- ステップ 3** [DHCP Pool] テーブルで、特定の変更をインラインします (または、[Edit DHCP Pool] ウィンドウに表示します)。
- ステップ 4** [Apply] をクリックします。
- [DHCP Pool] テーブルが更新され、更新したエントリがこのテーブルに表示されます。
-

DHCP プールの削除

- ステップ 1** [Wireless Settings] > [DHCP Server] を選択します。
- [DHCP Configuration] ウィンドウが表示されます。
- ステップ 2** 削除する DHCP プールが含まれている行で [X] アイコンをクリックします。

警告メッセージが表示されます。

ステップ 3 ポップアップ ウィンドウで [Yes] をクリックします。

[DHCP Pool] テーブルが更新され、削除したエントリがこのテーブルから削除されます。

DHCP リースの詳細の表示

ステップ 1 [Wireless Settings] > [DHCP Server] を選択します。

[DHCP Configuration] ウィンドウが表示されます。

ステップ 2 [DHCP Pool] テーブルに下にある [DHCP Leases] をクリックします。

[DHCP Pool Information] ウィンドウが表示されます。このウィンドウでは、ホスト名、その MAC アドレス、割り当てられている IP アドレス、リースの有効期限の詳細など、詳細情報を表示できます。

(注) [DHCP Pool Information] テーブルの対応するエントリでホストへのリースを削除することで、特定の IP アドレスを開放できます。

リース IP アドレスの詳細のエクスポート

ステップ 1 [Wireless Settings] > [DHCP Server] を選択します。

[DHCP Configuration] ウィンドウが表示されます。

ステップ 2 [DHCP Pool] テーブルに下にある [DHCP Leases] をクリックします。

[DHCP Pool Information] ウィンドウが表示されます。

ステップ 3 [DHCP Pool Information] テーブルに下にある [Export] をクリックします。

ステップ 4 リース IP アドレスと対応するホストの詳細をエクスポートする形式を選択します。

リース IP アドレスの開放

ステップ 1 [Wireless Settings] > [DHCP Server] を選択します。

[DHCP Configuration] ウィンドウが表示されます。

ステップ 2 [DHCP Pool] テーブルに下にある [DHCP Leases] をクリックします。

[DHCP Pool Information] ウィンドウが表示されます。

ステップ 3 削除するリース IP アドレスが割り当てられたホストを含む行で、[release_icon.gif] アイコンをクリックします。

警告メッセージが表示されます。

ステップ 4 [DHCP Pool Information] テーブルの対応するエントリでリースを削除することで、特定の IP アドレスを開放できます。

ステップ 5 ポップアップ ウィンドウで [Yes] をクリックします。

[DHCP Pool Information] テーブルが更新され、削除したエントリがこのテーブルから削除されます。



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 \(53 ページ\)](#)
- [Admin アカウントの管理 \(54 ページ\)](#)
- [ロビー管理者アカウントを使用したゲスト ユーザの管理 \(56 ページ\)](#)
- [日時の設定 \(58 ページ\)](#)
- [Cisco Mobility Express ソフトウェアの更新 \(60 ページ\)](#)

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] を選択します。

[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。

Admin アカウントの管理

Cisco Mobility Express は、ユーザアカウントに割り当てられている権限に基づいて、Cisco Mobility Express コントローラの GUI から管理できます。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。

Cisco Mobility Express の GUI へは、次のアクセスタイプのいずれかを持つ管理者アカウントを使用してログインできます。

- **読み取り/書き込み** : この管理アカウントには、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するためのすべてのアクセス権があります。
- **読み取り専用** : この制限付きアクセスの管理アカウントでは、ユーザはコントローラ コンフィギュレーションの表示のみを行えます。このユーザは、設定に変更を加えることはできません。
- **ロビー アンバサダー** : この制限付きの管理アカウントでは、ユーザはゲスト ユーザアカウントの作成および管理のみを行なえます。また、ロビー アンバサダーはゲスト ユーザアカウントのクレデンシャルを印刷または電子メールすることができます。

ゲストユーザアカウントの作成については、「[ゲストユーザアカウントの作成](#)」を参照してください。

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。

Cisco Mobility Express コントローラの管理者アカウントの総カウントがこのウィンドウの上部に表示され、利用可能なすべての管理者アカウントの詳細なリストがテーブルに表示されます。

[Admin Accounts] ウィンドウが表示されます。

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。

新しい編集可能な行エントリがテーブルに表示されます。

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**
 - **Read/Write**
 - **Lobby Ambassador**
- **[Password]** : パスワードは大文字と小文字が区別され、次のガイドラインに基づいて作成する必要があります。
 - 8 文字以上で、大文字および小文字と、数字、特殊文字を組み合わせで使用します。
 - Cisco という語や管理ユーザ名を含めることはできず、次の方法で取得したこれらの語の変形も使用できません。
 - これらの語の文字を反転させる
 - 文字の大文字と小文字を変更する
 - 次のように置き換える
 - i の代わりに 1、|、または!
 - o の代わりに 0
 - s の代わりに \$
 - パスワード内で同じ文字を 4 回以上続けて繰り返すことはできません。

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 \(55 ページ\)](#) 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。

ロビー管理者アカウントを使用したゲストユーザの管理

ネットワークに一時的にアクセスできるようにするためにゲスト ユーザ アカウントを作成します。このネットワーク アクセスは、ゲスト アカウントのクレデンシャルが正常に認証された後に与えられます。

ロビー アンバサダー管理者アカウントを使用して、ゲスト ユーザ アカウントを作成、管理できます。ロビー アンバサダー アカウントの詳細については、[Admin アカウントの管理 \(54 ページ\)](#) を参照してください。

ゲストユーザアカウントの作成

始める前に

ゲストユーザアカウントを作成する前に、1つ以上のロビーアンバサダーユーザアカウントを所有している必要があります。ロビーアンバサダーアカウントの作成については、[管理者アカウントの追加 \(55 ページ\)](#) を参照してください。

ステップ 1 ブラウザで Cisco Mobility Express の GUI まで移動します。

ステップ 2 ロビーアンバサダー クレデンシャルを使用してログインします。

[Lobby Ambassador Guest Management] ウィンドウが表示されます。

ステップ 3 [Add Guest User] をクリックします。

[Add Guest User] ダイアログボックスが表示されます。

ステップ 4 ゲストユーザアカウントの次の詳細を入力します。

- **[ユーザ名 (User Name)]**

- **[Wireless Network]** : ネットワークへのゲストアクセス用にすでに設定されている特定のゲスト WLAN を選択します。ゲスト WLAN が設定されていないか、またはゲスト WLAN を選択しなかった場合は、デフォルトで [All Guest WLANs] が選択されます。

(注) ゲスト WLAN の作成の詳細については、[WLAN の追加 \(34 ページ\)](#) を参照してください。

- **[Permanent User]** : このゲストユーザアカウントが時間制限なくネットワークにアクセスできるようにするには、このチェックボックスを選択します。

- **[Expiry Date & Time]** : カレンダーとクロックアイコンをそれぞれクリックして、日時を指定します。ゲストユーザアカウントは指定した日時に無効になり、ゲストネットワークへのアクセスを防ぎます。

(注) [Permanent User] チェックボックスがオンになっている場合は、このフィールドはダイアログボックスに表示されません。

- **[Generate Password]** : 作成中のゲストユーザアカウントにパスワードを自動的に生成するには、このオプションボタンをクリックします。

ゲストユーザアカウントのパスワードを手動で指定する場合は、[Password] フィールドと [Confirm Password] フィールドにそのパスワードを入力します。

- **Password**

(注) [Generate Password] オプションボタンをクリックすると、このフィールドはダイアログボックスに表示されなくなります。

- **[Confirm Password]** : このエントリが [Password] フィールドの入力と一致していることを確認します。

- **Description**

ステップ 5 [Update] をクリックします。

アカウントのクレデンシャルは電子メールを介して、または印刷することでゲスト ユーザと共有できません。

[Guest User Credentials] ポップアップが表示されるとともに、[Guest Users List] テーブルが更新され、この新しいゲスト ユーザ アカウントのエントリが含まれます。

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完全修飾ドメイン名 (FQDN) は次のとおりです。

- 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 サーバの詳細を追加および編集するには、[Management] > [Time] に進みます。これにより、[Time Settings] ページが開きます。

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。現在の日時は [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。

ステップ 3 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。新しい NTP サーバを追加するには、[Add NTP Server] をクリックします。

ステップ 4 NTP サーバの次の値を追加、編集できます。

- a) NTP サーバのプライオリティを設定するには、[NTP Index] ボックスで 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。
- b) [NTP Server] ボックスで、NTP サーバの IP 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 5 [Apply] をクリックします。

NTP サーバステータスの更新

[Time Settings] ページの NTP サーバテーブルの [NTP Status] 列には、各 NTP サーバへの接続のステータスが表示されます。ステータスは次のいずれかになります。

- [Not Tried] : 同期はまだ試行されていません。
- [In Sync] : コントローラの時間は NTP サーバと同期されている状態です。
- [Not Synched] : コントローラの時間は NTP サーバと同期されていません。
- [In Progress] : 現在、同期の試行中です。

[Refresh] をクリックすると、更新された NTP の状態をいつでも確認することができます。

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。Cisco Mobility Express コントローラ上の現在の設定は削除されません。

次の表に、利用可能なソフトウェア アップデート方法を示します。

方法	方法へのリンク
HTTP を使用したソフトウェア アップデート (注) この方法は (ap1g4 および ap3g3 イメージをサポートする) Cisco Aironet 1830、1850、2800、および 3800 アクセス ポイントだけでネットワークが構成されている場合にのみ使用できます。	HTTP を使用したソフトウェア アップデート (61 ページ) を参照してください。

方法	方法へのリンク
TFTP を使用したソフトウェア アップデート	TFTP を使用したソフトウェア アップデート (63 ページ) を参照してください。
Cisco.com からのソフトウェア直接アップデート	Cisco.com からのソフトウェア直接アップデート (66 ページ) を参照してください。

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プライマリ 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プライマリ 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。プライマリ AP が、TFTP サーバまたは HTTP バスから新しい AP への新しいソフトウェアの転送を支援します。

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。

HTTP を使用したソフトウェア アップデート

始める前に

ネットワークが (ap1g4 および ap3g3 イメージをサポートする) 1830、1850、2800、および 3800 アクセス ポイントのみで構成されている場合にのみ、HTTP を介してソフトウェア アップデートを実行できます。ネットワーク内にサポートされている他の AP モデルがある場合は、TFTP を使用するか、または Cisco.com から直接更新します。

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。

- 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。
- 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。
- ソフトウェア リリース番号を選択します。
- ZIP ファイルに対応する [Download] をクリックします。

- e) 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。
- f) ZIP ファイルをコンピュータのハードドライブに保存し、その内容をコンピュータのディレクトリに抽出します。

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] を選択します。

[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から [HTTP] を選択します。

ステップ 4 [File] フィールドの横にある [Browse] ボタンをクリックし、展開された ZIP ファイルの内容が含まれているフォルダを参照し、次の表に示すようにソフトウェアファイルを選択します。

Cisco Mobility Express コントローラの Cisco AP シリーズ	選択するソフトウェアファイル
1830、1850	ap1g4
2800、3800	ap3g3

(注) ここで開くファイルエクスプローラは、オペレーティングシステム固有のエクスプローラで、コンピュータの OS によって異なります。

ステップ 5 イメージの事前ダウンロードの完了後にコントローラを自動的にリブートするように設定するには、[Auto Restart] チェック ボックスをオンにします。

また、[Advanced] > [Controller Tools] を選択し、[Restart Controller] を選択することで、アップグレード後にコントローラを手動でリブートできます。

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 [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 [Image Pre-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ライマリーイメージのステータスが表示されます。

進行中のソフトウェアアップデートは、コントローラがリブートを完了するまではいつでも [Abort] をクリックすることでキャンセルできます。

ステップ 8 イメージの事前ダウンロードの完了後、ソフトウェアアップグレードを完了するにはコントローラを再起動（またはリブート）する必要があります。[Auto Restart] チェック ボックスをオンにしていない場合は、アップグレード後に [Advanced] > [Controller Tools] を選択し、[Restart Controller] をクリックすることで、コントローラを手動でリブートできます。

イメージの事前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 \(89 ページ\)](#) を参照してください。

進行中のソフトウェアアップデートは、コントローラがリブートを完了するまではいつでも [Abort] をクリックすることでキャンセルできます。

ステップ 9 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。

TFTP を使用したソフトウェア アップデート

始める前に

- Cisco Mobility Express ソフトウェアファイルをホストするために、次のガイドラインに従って TFTP サーバを準備します。
 - 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、`TFTP failure while storing in flash` というエラーメッセージが表示されます。
 - ディストリビューション システム ネットワーク ポートを経由して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。
- 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。



(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。

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) ZIP ファイルに対応する [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、解凍してコンテンツ全体を TFTP サーバ上のデフォルト ディレクトリに抽出します。

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] を選択します。

[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から [TFTP] を選択します。

ステップ 4 [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。

ステップ 5 [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 6 イメージの事前ダウンロードの完了後にコントローラを自動的にリブートするように設定するには、[Auto Restart] チェック ボックスをオンにします。

また、[Advanced] > [Controller Tools] を選択し、[Restart Controller] を選択することで、アップグレード後にコントローラを手動でリブートできます。

ステップ 7 [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 8 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。
- 更新を後から実行するには、[Set Update 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 Update] 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 [Image Pre-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。

進行中のソフトウェアアップデートは、コントローラがリブートを完了するまではいつでも [Abort] をクリックすることでキャンセルできます。

ステップ 9 イメージの事前ダウンロードの完了後、ソフトウェア アップグレードを完了するにはコントローラを再起動（またはリブート）する必要があります。[Auto Restart] チェック ボックスをオンにしていない場合は、アップグレード後に [Advanced] > [Controller Tools] を選択し、[Restart Controller] をクリックすることで、コントローラを手動でリブートできます。

イメージの事前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 \(89 ページ\)](#) を参照してください。

進行中のソフトウェアアップデートは、コントローラがリブートを完了するまではいつでも [Abort] をクリックすることでキャンセルできます。

ステップ 10 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。

SFTP を使用したソフトウェア アップデート

SFTP 転送モードによるソフトウェア アップデートは、Cisco Mobility Express 導入でサポートされているすべてのアクセスポイントに有効です。このアップグレード方法を使用するには、プライマリアクセスポイントと通信できる SFTP サーバが必要です。この更新方法はコントローラ WebUI および CLI からサポートされます。

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] ページにアクセスします。
- b) 特定の 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) 特定のソフトウェア 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) ZIP ファイルに対応する [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、解凍してコンテンツ全体を SFTP サーバ上のデフォルト ディレクトリに抽出します。

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] を選択します。

[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から [SFTP] を選択します。

ステップ 4 [ポート (Port)] フィールドにポート番号を入力します。デフォルトは 22 です。

ステップ 5 [File Path] フィールドに、ソフトウェア ファイルの SFTP サーバ ディレクトリ パスを入力します。

ステップ 6 SFTP サーバにログインする [ユーザ名 (Username)] と [パスワード (Password)] を入力します。

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、[更新 (Update)] をクリックし、確認ダイアログで [OK] をクリックします。
- 更新を後から実行するには、[更新時間の設定 (Set Update Time)] フィールドで現在の日付から 5 日間以内の日時を指定してから、[更新をスケジュール (Schedule Update)] をクリックします。

ステップ 8 イメージの事前ダウンロードの完了後にコントローラを自動的にリブートするように設定するには、[Auto Restart] チェック ボックスをオンにします。

また、[Advanced] > [Controller Tools] を選択し、[Restart Controller] を選択することで、アップグレード後にコントローラを手動でリブートできます。

ステップ 9 [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 10 イメージの事前ダウンロードの完了後、ソフトウェア アップグレードを完了するにはコントローラを再起動（またはリブート）する必要があります。[Auto Restart] チェック ボックスをオンにしていない場合は、アップグレード後に [Advanced] > [Controller Tools] を選択し、[Restart Controller] をクリックすることで、コントローラを手動でリブートできます。

イメージの事前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 \(89 ページ\)](#) を参照してください。

進行中のソフトウェアアップデートは、コントローラがリブートを完了するまではいつでも [Abort] をクリックすることでキャンセルできます。

ステップ 11 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。

Cisco.com からのソフトウェア直接アップデート

始める前に

- プライマリ AP のシリアル番号は、サービス契約に記載されているものである必要があります。これは、Cisco.com サイトからは実行できません。シスコカスタマーサービスに連絡し、シリアル番号をサービス契約に追加する必要があります。

ただし、返品保証 (Return to Manufacturer Authorization : RMA) を行っている場合、シリアル番号はデバイスを交換するチームによってサービス契約に追加されます。また、Cisco Services Contract Center データベースへのアクセスを持つ特定のシスコパートナーも、サービス契約にシリアル番号を追加できます。

- 有効な Cisco.com ユーザ クレデンシャルが必要です。
- Cisco Mobility Express コントローラが Cisco.com に到達できる必要があります。

ステップ 1 [Software Update Mode] ドロップダウンリストから [Cisco.com] を選択します。

ステップ 2 Cisco.com アカунトの Cisco.com ユーザ名とパスワードを入力します。

以前使用していた既存のクレデンシャルをクリアするには、新しいクレデンシャルを入力する前に [Clear Credentials] をクリックします。

ステップ3 ソフトウェア アップデートを自動的に確認するようにコントローラを設定するには、[Automatically Check for Updates] ドロップダウンリストの [Enabled] を選択します。この設定はデフォルトでイネーブルになっています。

ソフトウェアの確認が実行され、新しい最新のソフトウェアアップデートまたは推奨ソフトウェアアップデートが Cisco.com で入手できる場合は、次のようになります。

- GUI の右上隅にある [Software Update Alert] アイコンが緑色になります（それ以外の場合はグレー）。このアイコンをクリックすると [Software Update] ページが表示されます。
- [Software Update] ページの下部にある [Update] ボタンが有効になります

ステップ4 [Apply] をクリックします。

これにより、ソフトウェア アップデート モード、Cisco.com のクレデンシャル、[Automatically Check For Updates] のフィールドで行ったエントリまたは変更が保存されます。

コントローラは30日ごとに自動確認を実行し、Cisco.comでのダウンロードに利用可能な最新のソフトウェアや推奨ソフトウェアバージョンをチェックします。この情報は、[Latest Software Release] フィールドと [Recommended Software Release] フィールドに表示されます。表示されたリリースのリリース ノートを表示するには、横にある [?] をクリックします。

[Last Software Check] フィールドには、ソフトウェアを最後に自動または手動で確認したときのタイムスタンプが表示されます。

Cisco.com のユーザ名かパスワードまたはその両方が有効でない場合、ソフトウェアの確認は失敗してソフトウェア アップデートを実行できなくなります。

ステップ5 [Check Now] をクリックし、ソフトウェア確認を手動で実行します。

ソフトウェア確認は、[Check Now] をクリックすることでいつでも手動で実行できます。

ステップ6 ソフトウェア アップデートを進めるには、[Update] をクリックします。

[Software Update] ウィザードが表示されます。このウィザードは、次の3つのタブでの作業を順次実行します。

- [Release] タブ：推奨ソフトウェア リリースか、または最新ソフトウェア リリースのどちらにアップデートするかを指定します。
- [Update] タブ：APをいつリセットするかを指定します。すぐに実行するか、後から実行するためにスケジュールを設定するかを選択できます。
イメージの事前ダウンロードの完了後にコントローラを自動的にリブートするように設定するには、[Auto Restart] チェック ボックスをオンにします。
- [Confirm] タブ：選択を確認します。

ウィザードの指示に従います。[Confirm] をクリックするまでは、どのタブにもいつでも戻ることができます。[Confirm] をクリックすると、**シスコ ソフトウェア使用許諾契約書 (EULA)** が表示されます。

ステップ7 EULA に同意して更新を開始するには、[Agree] をクリックします。EULA に同意しないと、更新がキャンセルされてエラーが表示されます。

進行中のソフトウェアアップデートは、コントローラがリブートを完了するまではいつでも [Abort] をクリックすることでキャンセルできます。

次のタスク

更新のステータスおよび進捗状況は [Software Update] ページでモニタできます。更新が進むにつれて、次のデータが表示されます。

- ネットワーク内の AP の総数
- 次の AP の数
 - 現在更新中
 - 更新待機中
 - リブート中
 - 更新失敗

さらに、各 AP について、次のデータを使用して更新の進捗状況も表示されます。

- [AP Name]
- [State] : [Waiting to be updated] (更新待機中)、[Pre-downloading software] (ソフトウェアの事前ダウンロード中)、[Rebooting] (リブート中)、[Failed] (失敗)
- ダウンロード率の色分け
- 更新試行
- 最終更新エラー

進行中のソフトウェアアップデートは、コントローラがリブートを完了するまではいつでも [Abort] をクリックすることでキャンセルできます。



第 6 章

詳細設定の使用と操作

- [SNMP の管理 \(69 ページ\)](#)
- [システム メッセージ ロギング の設定 \(72 ページ\)](#)
- [RF パラメータ の最適化 \(74 ページ\)](#)
- [コントローラ ツール の使用 \(74 ページ\)](#)
- [コントローラ コンフィギュレーション の保存 \(75 ページ\)](#)
- [CMX クラウド プレゼンス分析 の使用 \(76 ページ\)](#)

SNMP の管理

Simple Network Management Protocol 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、これらのデバイスを設定して管理するために使用される一般的なネットワーク管理プロトコルです。

Cisco Wireless リリース 8.3 以降、Cisco Mobility Express の Web インターフェイスを使用して SNMPv2c および SNMPv3 の両方を設定できます。

SNMP アクセスの設定

Cisco Mobility Express プライマリ AP の次の SNMP アクセスモードを設定できます。

- SNMPv2c のみ
- SNMPv3 のみ
- SNMPv2c と NMPv3 の両方
- SNMPv2c も SNMPv3 もアクセス不可



(注) Cisco Mobility Express CLI を使用しても、SNMPv1、SNMPv2c、および SNMPv3 を設定できません。

ステップ 1 [Advanced] > [SNMP] を選択します。

[SNMP Setup] ウィンドウが表示されます。

ステップ 2 次に、[SNMP Access] に移動し、適切なチェック ボックスをオンにして、特定の SNMP モードを有効にします。

デフォルト モードは v2c です（あるいはデフォルトで SNMP モードの両方が選択されているか、またはいずれも選択されていないこともあります）。

選択した SNMP アクセス モードが有効になります。

(注) Cisco Mobility Express を使用した SNMPv3 ユーザの設定については、「SNMPv3 ユーザの設定」の項を参照してください。

ステップ 3 [Read Only Community] フィールドに、特定のコミュニティ名を入力します。

デフォルト名は *public* です。

ステップ 4 [Read-Write Community] フィールドに、特定のコミュニティ名を入力します。

デフォルト名は *private* です。

ステップ 5 [SNMP Trap] ドロップダウンリストから、[Enabled] または [Disabled] を選択して SNMP トラップの受信者を設定します。このツールはログを受信し、ネットワーク デバイスから送信された SNMP トラップを表示します。

デフォルト設定では [Disabled] になっています。

ステップ 6 [SNMP Server IP] フィールドで、接続するサーバの IP アドレスを指定します。

SNMPv3 ユーザの追加

ステップ 1 [Advanced] > [SNMP] を選択します。

[SNMP Setup] ウィンドウが表示されます。

ステップ 2 [SNMP v3 Users] セクションで、[Add New SNMP v3 User] ボタンをクリックします。

[Add SNMP v3 User] ウィンドウが表示されます。

ステップ 3 [User Name] フィールドに、新しい SNMPv3 ユーザのユーザ名を入力します。

ユーザ名は次の条件を満たしている必要があります。

-
-

ステップ 4 [Access Mode] ドロップダウンリストで、[Read Only] と [Read/Write] から必要なモードを選択します。

デフォルトは [Read Only] です。

ステップ 5 [Authentication Protocol] ドロップダウンリストから、[HMAC-MD5]、[HMAC-SHA]、または [None] のいずれかを選択します。

デフォルトの認証プロトコルは **HMAC-SHA** です。

ステップ 6 [Authentication Password] フィールドと [Confirm Authentication Password] フィールドに、次のパスワードポリシーに従って特定の認証パスワードを入力します。

(注) [Show Password] チェック ボックスを選択し、[Authentication Password] フィールドと [Confirm Authentication Password] フィールドのエントリを表示して一致していることを確認することができます。

ステップ 7 [Privacy Protocol] ドロップダウンリストで、[CBC-DES]、[CFB-AES-128]、または [None] のいずれかを選択します。

デフォルトのプライバシー プロトコルは [CFB-AES-128] です。

ステップ 8 [Privacy Password] フィールドと [Confirm Privacy Password] フィールドに、次のパスワードポリシーに従って特定のプライバシー パスワードを入力します。

(注) [Show Password] チェック ボックスを選択し、[Privacy Password] フィールドと [Confirm Privacy Password] フィールドのエントリを表示して一致していることを確認することができます。

ステップ 9 [Apply] をクリックして新しい SNMPv3 ユーザを作成します。

新たに追加した SNMP v3 ユーザが [SNMP Setup] ウィンドウの [SNMP v3 Users] テーブルに表示されます。

(注) 最大 7 つの SNMPv3 ユーザを追加できます。

SNMPv3 ユーザの編集

ステップ 1 [Advanced] > [SNMP] を選択します。

[SNMP Setup] ウィンドウが表示されます。

ステップ 2 詳細を変更する SNMPv3 ユーザが含まれている行で [edit_icon.gif] アイコンをクリックします。

[SNMPv3 Users] テーブル内の特定の行が編集可能になります (または、[Edit SNMPv3 User] ウィンドウが表示されます)。

ステップ 3 [SNMPv3 Users] テーブルで、特定の変更をインラインします (または、[Edit SNMPv3 Users] ウィンドウに表示します)。

ステップ 4 [Apply] をクリックします。

[SNMP v3 Users] テーブルが更新され、更新したエントリがこのテーブルに表示されます。

SNMPv3 ユーザの削除

ステップ 1 [Advanced] > [SNMP] を選択します。

[SNMP Setup] ウィンドウが表示されます。

ステップ 2 削除する SNMPv3 ユーザが含まれている行で [X] アイコンをクリックします。

警告メッセージが表示されます。

ステップ 3 ポップアップ ウィンドウで [Yes] をクリックします。

[SNMP v3 Users] テーブルが更新され、削除したエントリがこのテーブルから削除されます。

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。

始める前に

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)]
- [アラート (Alerts)]
- [Critical]

- **[Errors (Default)]**
- 警告
- 通知
- **[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。

RF パラメータの最適化

ネットワークの Wi-Fi のパフォーマンスを最大化するため、無線周波の信号のカバレッジと品質を最適化できます。

ステップ 1 [RF Optimization] ドロップダウンリストから [Enabled] を選択します。

ステップ 2 ネットワークの予想される [Client Density] と [Traffic Type] が表示されます。

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 \(92 ページ\)](#) を参照してください。

ステップ 3 [Apply] をクリックします。

コントローラ ツールの使用



(注) この機能は、読み込み/書き込み権限を持つ管理ユーザアカウントのみで利用できます。

[Controller Tools] ページでは、コントローラの次の操作を実行できます。

- コントローラの再起動。
[コントローラの再起動 \(74 ページ\)](#) を参照してください。
- コントローラ コンフィギュレーションのクリアと工場出荷時状態へのコントローラのリセット。[コントローラ コンフィギュレーションのクリアとコントローラのリセット \(74 ページ\)](#) を参照してください。
- コントローラ コンフィギュレーションのエクスポートとインポート。「[コントローラ コンフィギュレーションのエクスポートとインポート \(75 ページ\)](#)」を参照してください。

コントローラの再起動

コントローラは、[Advanced] > [Controller Tools] を選択し、[Restart Controller] をクリックすることで、いつでも再起動（またはリブート）できます。

コントローラ コンフィギュレーションのクリアとコントローラのリセット

この手順によって、Cisco Mobility Express ワイヤレス LAN コントローラは工場出荷時の設定にリセットされます。

ステップ 1 [Advanced] > [Controller Tools] を選択します。

これにより、[Controller Tools] ページが開きます。

ステップ 2 [Clear Candidate Configuration] をクリックします。

これにより、現在の Cisco Mobility Express コントローラ設定が消去され、工場出荷時の値に設定がリセットされて、Cisco Mobility Express ワイヤレス LAN コントローラがリブートします。

次のタスク

Cisco Mobility Express コントローラがリブートしたら、[初期設定ウィザードの起動 \(7 ページ\)](#) に進みます。

コントローラ コンフィギュレーションのエクスポートとインポート

コントローラ設定のエクスポート

現在のコントローラ設定は、いつでも .TXT ファイル形式にエクスポートできます。

現在の設定をエクスポートするには、[Advanced] > [Controller Tools] を選択し、[Configuration File] の下にある [Export Configuration] をクリックします。

設定ファイルは HTTPS を介し、Mobility Express の UI が表示されているデバイス上に保存されます。デフォルトでは、ダウンロードフォルダ内に *configuration.txt* として保存されます。

コントローラ設定のインポート

以前に .TXT ファイル形式で保存した設定ファイルから設定をインポートできます。これを行うには、[Advanced] > [Controller Tools] を選択し、[Configuration File] の下にある [Import Configuration] をクリックして必要なファイルを参照し、選択します。

インポートによって、ネットワーク内のコントローラ対応のすべての AP がリブートします。AP がオンラインに戻ると、プライマリ AP 選定プロセスが開始され、プライマリ AP は新たにインポートされたコントローラ構成でオンラインになります。

プライマリ AP 選定プロセスの詳細については、[Cisco Mobility Express コントローラのフェールオーバーとプライマリ AP の選定プロセス \(88 ページ\)](#) を参照してください。

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構成は、プライマリ 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 コントローラの構成は、プライマリ 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。

CMX クラウド プレゼンス分析の使用

Cisco Connected Mobile Experiences Cloud (Cisco CMX Cloud) は現場での分析を実現する Software as a Service (SaaS) 製品です。Cisco Mobility Express の Web インターフェイスを使用して、Cisco CMX Cloud ソリューションを設定できます。

Cisco Mobility Express と統合された Cisco CMX Cloud ソリューションは、次の機能を提供します。

- カスタム ポータルを通じ、訪問者のための安全なゲスト アクセス ソリューションの設定を可能にします。



(注) CMX Connect 設定はゲスト アクセス用の WLAN レベルで実行されます。

- すべての Wi-Fi のデバイスの検出を容易にします。
- 滞留時間、新規訪問者とリピーター訪問者、ピーク タイムなど、Wi-Fi デバイスのプレゼンスに関する分析を提供します。
- ロケーションベースのコンテンツを提供するゲストポータルページやモバイルアプリケーションに訪問者を直接取り込むこともできます。

CMX プレゼンス分析の前提条件

- 有効な CMX サーバ URL と対応する CMX サーバ トークンが必要です。CMX クラウドアカウントを登録するには、www.cmxcisco.com にアクセスしてください。詳細については、<http://support.cmxcisco.com/hc/en-us> を参照してください。



(注) サーバ URL フィールドの URL に `/visitor/login` が追加されていることを確認します。

- CMX クラウド用の WLAN が作成されます。詳細については、「ワイヤレス設定の指定」の章の「WLAN の追加」の項を参照してください。

CMX プレゼンス分析の有効化

始める前に

有効な CMX サーバの URL と対応するトークンが必要です。

ステップ 1 [Advanced] > [CMX] を選択します。

[CMX] ウィンドウが表示されます。

ステップ 2 [CMX Status] ドロップダウン ボックスで、[Enabled] を選択します。

ステップ 3 [CMX Server URL] フィールドに有効な CMX サーバの URL を入力します。

ステップ 4 [CMX Server Token] フィールドに有効な CMX サーバのトークンを入力します。

ステップ 5 [Apply] をクリックします。



付録 **A**

コントローラ CLI コマンド

- Cisco Mobility Express CLI (79 ページ)
- CLI 初期設定ウィザードの使用 (79 ページ)
- CLI での手順 (83 ページ)

Cisco Mobility Express CLI

特定のCisco Mobility Express ソフトウェア リリースでサポートされている機能については、Cisco Mobility Express コントローラ ソフトウェアが 同じ Cisco Unified Wireless Network ソフトウェア リリース バージョン内の Cisco WLC によってサポートされているほとんどのコマンドをサポートしています。ただし、Cisco Mobility Express コントローラに特有の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。これらの手順は、以降の各項で説明します。

Cisco Mobility Express コントローラ CLI でサポートされているコマンドの詳細なリストについては、<https://www.cisco.com/c/en/us/support/wireless/mobility-express/products-command-reference-list.html> に示されている特定のリリースの『Cisco Mobility Express Command Reference』を参照してください。Cisco Mobility Express は、このドキュメントに記載されている AireOS コマンドのみをサポートしています。

WLC CLI 上で利用可能なコマンドについては、次の URL に記載されている Cisco Unified Wireless Network ソフトウェア リリース用の『Cisco Wireless Controller Command Reference』ガイドを参照してください。<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

始める前に

- 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 IP アドレスとサブネット マスクを入力します。

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 管理 DHCP スコープを有効にし、設定するには、「**yes**」と入力します。それ以外の場合は、「**No**」と入力します。

「**YES**」と入力した場合は、次を入力する必要があります。

1. DHCP Network IP address (DHCP ネットワーク IP アドレス)
2. DHCP Netmask (DHCP ネットマスク)
3. Router IP Address (ルータ IP アドレス)
4. IP アドレス範囲の [Start DHCP IP address] (開始 DHCP IP アドレス) と [Stop DHCP IP address] (終了 DHCP IP アドレス)
5. Domain Name (ドメイン名)
6. OpenDNS かユーザ DNS かの指定

ステップ 11 [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 12 従業員 DHCP スコープを有効にし、設定するには「**yes**」と入力します。それ以外の場合は、「**No**」と入力します。

「**YES**」と入力した場合は、次を入力する必要があります。

1. DHCP Network IP address (DHCP ネットワーク IP アドレス)
2. DHCP Netmask (DHCP ネットマスク)
3. Router IP Address (ルータ IP アドレス)
4. IP アドレス範囲の [Start DHCP IP address] (開始 DHCP IP アドレス) と [Stop DHCP IP address] (終了 DHCP IP アドレス)
5. Domain Name (ドメイン名)
6. OpenDNS かユーザ DNS かの指定

ステップ 13 [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 14 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 15 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ポートし、ログオンプロンプトが表示されます。

CLI での手順

SNMPv3 ユーザのデフォルト値の変更

SNMPv3 ユーザのユーザ名、認証パスワード、およびプライバシーパスワードに対するコントローラのデフォルト値は、「default」が使用されています。これらの標準値を使用すると、セキュリティ上のリスクが発生します。したがって、これらの値を変更することを強く推奨します。

始める前に

SNMPv3 は時間に依存しています。コントローラの時間および時間帯を正確に設定してください。

ステップ 1 次のコマンドを入力して、このコントローラに対する SNMPv3 ユーザの最新のリストを表示します。

```
show snmpv3user
```

ステップ 2 [SNMPv3 User Name] カラムに「default」と表示されている場合は、次のコマンドを入力してこのユーザを削除します。

```
config snmp v3user delete username
```

username パラメータが SNMPv3 ユーザ名です（この場合は「default」）。

ステップ 3 次のコマンドを入力して、新しい SNMPv3 ユーザを作成します。

```
config snmp v3user createusername {ro |rw} {none |hmacmd5 |hmacsha} {none |des |aesfb128} auth_key encrypt_key
```

値は次のとおりです。

- *username* は、SNMPv3 ユーザ名です。
- **ro** は読み取り専用モード、**rw** は読み取り/書き込みモードです。
- **none**、**hmacmd5**、**hmacsha** は、認証プロトコル オプションです。
- **none**、**des**、**aesfb128** は、プライバシープロトコル オプションです。
- *auth_key* は、認証用の共有秘密キーです。
- *encrypt_key* は、暗号化用の共有秘密キーです。

username、*auth_key*、および *encrypt_key* の各パラメータに「default」と入力しないでください。

ステップ 4 **save config** コマンドを入力します。

ステップ 5 追加した SNMPv3 ユーザを有効にするために、**reset system** コマンドを入力して、コントローラを再起動します。

802.11r 高速移行の設定

- ステップ 1 802.11r 高速移行パラメータを有効または無効にするには、**config wlan security ft {enable | disable} wlan-id** コマンドを使用します。
- デフォルトで、高速移行は無効です。
- ステップ 2 分散システム上の 802.11r 高速移行パラメータを有効または無効にするには、**config wlan security ft over-the-ds {enable | disable} wlan-id** コマンドを使用します。
- デフォルトで、分散システム上の高速移行は無効です。
- ステップ 3 事前共有キー (PSK) を使用した高速移行の認証キー管理を有効または無効にするには、**config wlan security wpa akm ft-psk {enable | disable} wlan-id** コマンドを使用します。
- デフォルトで、PSK を使用した認証キー管理は無効です。
- ステップ 4 802.1X を使用した高速移行の認証キー管理を有効または無効にするには、**config wlan security wpa akm ft-802.1X {enable | disable} wlan-id** コマンドを使用します。
- デフォルトで、802.1X を使用した認証キー管理は無効です。
- ステップ 5 802.11r Fast Transition の再アソシエーション タイムアウトを有効または無効にするには、**config wlan security ft reassociation-timeout timeout-in-seconds wlan-id** コマンドを使用します。
- 有効範囲は 1 ~ 100 秒です。再アソシエーション タイムアウトのデフォルト値は 20 秒です。
- ステップ 6 分散システム上の高速移行の認証キー管理を有効または無効にするには、**config wlan security wpa akm ft over-the-ds {enable | disable} wlan-id** コマンドを使用します。
- デフォルトで、分散システム上の高速移行の認証キー管理は無効です。
- ステップ 7 クライアントの高速移行の設定を表示するには、**show client detailed client-mac** コマンドを使用します。
- ステップ 8 WLAN の高速移行の設定を表示するには、**show wlan wlan-id** コマンドを使用します。
- ステップ 9 高速移行イベントのデバッグを有効または無効にするには、**debug ft events {enable | disable}** コマンドを使用します。
- ステップ 10 高速移行のキー生成のデバッグを有効または無効にするには、**debug ft keys {enable | disable}** コマンドを使用します。
-

CDP タイマーの設定



(注) CDP 保留時間の設定は、プライマリ AP のコントローラコンソールからは行えません。コントローラの保留時間構成は無視されます。これは、Cisco Mobility Express のプライマリ AP 上のコントローラと内部 AP がスイッチ上の同じインターフェイスを共有しているためです。

Cisco Mobility Express (CLI) での Cisco Umbrella の設定

ここでは、Cisco Mobility Express で Cisco Umbrella を設定する手順について説明します。

始める前に

- Cisco Umbrella のアカウントが必要です。
- Cisco Umbrella からの API トークンが必要です。

ステップ 1 Cisco Umbrella を有効または無効にするには、**config opendns {enable | disable}** を使用します。

例：

```
(Cisco Controller) > config opendns enable
```

Cisco Umbrella のグローバル設定を有効または無効にします。

ステップ 2 **config opendns api-token api-token**

例：

```
(Cisco Controller) > config opendns api-token D0986C18DC334FB2E3AA46148D600A4001E5997
```

ネットワークに Cisco Umbrella の API トークンを登録します。

ステップ 3 **config opendns profile {create | delete | refresh} profilename**

例：

```
(Cisco Controller) > config opendns profile create profile1
```

WLAN 経由で適用できる Cisco Umbrella プロファイルを作成、削除、または更新します。

ステップ 4 **config wlan opendns-profile wlan-id profile-name {enable | disable}**

例：

```
(Cisco Controller) > config wlan opendns-profile 1 profile-name enable
```

Cisco Umbrella プロファイル ID を WLAN にマッピングします。

ステップ 5 **config wlan opendns-dhcp-opt6 wlan-id {enable | disable}**

例：

```
(Cisco Controller) > config wlan opendns-dhcp-opt6 1 enable
```

WLAN ごとに DHCP オプション 6 を有効または無効にします。

ステップ 6 `config wlan.opendns-mode wlan-id {ignore | forced}`

例 :

```
(Cisco Controller) >config wlan.opendns-mode 1 forced
```

WLAN で Cisco Umbrella モードを無視するかまたは適用します。



付録 **B**

概念、FAQ、および高度なユーザに関する情報

- [対応ブラウザ](#) (87 ページ)
- [Cisco Mobility Express コントローラのフェールオーバーとプライマリ AP の選定プロセス](#) (88 ページ)
- [アクセス ポイントへのイメージのプレダウロード](#) (89 ページ)
- [CAPWAP の Mobility Express 変換の代替手段](#) (90 ページ)
- [Mobility Express から CAPWAP タイプへの AP の変換](#) (91 ページ)
- [RF パラメータの最適化設定](#) (92 ページ)
- [関連資料](#) (93 ページ)
- [よくある質問](#) (94 ページ)

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	<ul style="list-style-type: none">• Internet Explorer 10 以降• Mozilla Firefox 33 以降• Google Chrome 38 以降
Apple MAC OS	<ul style="list-style-type: none">• 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プライマリ 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、すべての AP にプライマリ AP として機能する能力があるわけではありません。プライマリ AP として機能できる AP モデルについては、[サポートされているシスコのアクセスポイント \(2 ページ\)](#) 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、プライマリ AP として機能できるアクティブな AP がネットワークに複数必要です。フェールオーバーの発生時に、これらの AP の 1 つが自動的にプライマリとして選定されます。新しく選定されたプライマリは、元のプライマリと同じ IP および構成になります。管理者にとっては、フェールオーバー発生時、元のプライマリと新しく選定されたプライマリに違いはありません。



(注) プライマリ 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。

Mobility Express コントローラの強制フェールオーバー

Cisco Mobility Express ネットワークには、すべての AP にプライマリ AP として機能する能力があるわけではありません。プライマリ AP として機能できる AP モデルについては、[サポートされているシスコのアクセスポイント \(2 ページ\)](#) を参照してください。

プライマリ AP として機能できる任意の AP を手動で強制的にプライマリ AP にすることができます。プライマリとして機能できる AP を選択し、その AP にプライマリ AP の強制フェールオーバーを実行する場合、GUI と CLI の両方を使用できます。

GUI を使用して強制フェールオーバーを実行するには、以下の手順に従います。

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。
2. プライマリとして設定する 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。
3. [General] タブで、[Operating Mode] フィールドの横にある [Make me Controller] をクリックします。



- (注) プライマリ AP では、[Operating Mode] 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。[Make me Controller] ボタンは、プライマリの選定プロセスに含めることができる下位 AP に対してのみ使用できます。

CLI を使用して強制フェールオーバーを実行するには、次のコマンドを使用します。

```
config ap next-preferred-master cisco-ap-name forced-failover
```

GUI 方式または CLI 方式を使用して、選択した AP へのプライマリのフェールオーバーを強制すると、現在のプライマリ AP はリブートし、新しい AP が以前のプライマリの IP アドレスと構成を使用してコントローラとして継承します。以前のプライマリは、リブート後、オンラインに戻り、下位 AP として新しいプライマリ AP に join します。



- (注) 他のフェールオーバーと同様に、この強制フェールオーバーは、Cisco Mobility Express ネットワークにダウンタイムを引き起こします。このダウンタイム中に、スタンドアロン機能を有効にした AP に関連付けられたクライアントでサービスの中断が発生することはありません。スタンドアロン機能を有効になっていない AP のクライアントが影響を受けます。

プライマリ AP の選定プロセス

Cisco Mobility Express ネットワークでプライマリ AP がシャットダウンすると、この導入環境でプライマリとして機能できる他の AP の 1 つが自動的にプライマリ AP に指定されます。内部のプライマリ自動選定プロセスにより、Cisco Mobility Express 対応の AP からプライマリ 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 つはプライマリ AP の障害を検出すること、もう 1 つはプライマリとして機能できる AP から新しいプライマリ 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プライマリ AP を決定します。

- 他の Cisco Mobility Express 対応の AP と比べて最も高いコントローラ稼働時間を持つ AP
- 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 プライマリとして設定された 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。

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クバリ要求に自身のディスク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。

CAPWAP の Mobility Express 変換の代替手段



- (注)
- 推奨方法は、[CAPWAP Lightweight AP から Cisco Mobility Express ソフトウェアへの変換 \(13 ページ\)](#) のとおりです。推奨方法で動作しない場合にのみ選択する代替手段を次に示します。
 - 次の手順では、1850 シリーズの AP 上の 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、および AP モデルに応じて、必ず適切なソフトウェアファイルを使用してください。



ヒント AP ソフトウェアから Cisco Mobility Express ソフトウェアへの変換で問題が発生した場合、AP CAPWAP ソフトウェアを最新の AP ソフトウェアバージョンの `ap3g3-k9w8-tar.153-3.JD.tar` にアップグレードします。CAPWAP ソフトウェアを Cisco Mobility Express ソフトウェア `AIR-AP2800-K9-ME-8-3-102-0.tar` に変換できるようになりました。

この問題は、デフォルトのイメージで出荷されるか、または Cisco Wireless リリース 8.3 より前のバージョンの Mobility Express 対応 AP で発生します。これは AP のメモリに十分なスペースがないか、または AP が U ブートモードで起動してもイメージがフラッシュで見つからないために発生します。

ステップ 1 Cisco.com から TFTP サーバへ `AIR-API1850-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。

ソフトウェアダウンロードページで、対象リリースのこの .zip ファイルは、「アクセスポイントイメージバンドル、ソフトウェアのアップデートおよびサポートされているアクセスポイントイメージに使用 (*Access point image bundle, to be used for software update and/or supported access points images*) 」というラベルが付けられています。

ステップ 2 TFTP サーバのディレクトリに zip ファイルの内容を解凍します。

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 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-type mobility-express tftp://<tftp server ip address>/<filename of ap1g4 TAR file 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、*CiscoAirProvision* SSID のブロードキャストを開始します。

Mobility Express から CAPWAP タイプへの AP の変換

Mobility Express AP を CAPWAP AP に変換するには、この手順に示すように CLI で Mobility Express AP の AP タイプを Mobility Express から CAPWAP に変更する必要があります。

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。

AP タイプを CAPWAP にすると、AP はそれ自体の Mobility Express コントローラ機能を開始せず、Mobility Express プライマリ AP の選定プロセスにも参加しません。この AP は物理ワイヤレス コントローラベースのネットワーク（つまり Mobility Express 以外のネットワーク）に配置できます。ここで、そのコントローラに join する AP は、AP 上のイメージとコントローラ上のイメージは異なるので、コントローラから CAPWAP イメージを要求し、再起動し、CAPWAP AP としてコントローラに再度 join します。

Mobility Express コントローラの CLI から、Mobility Express イメージが実行されている複数のアクセス ポイントを CAPWAP に同時に変換するには、次のコマンドを実行します。

```
(Cisco Controller) > config ap unifiedmode <switch_name> <switch_ip_address>
```

引数の `<switch_name>` と `<switch_ip_address>` は、それぞれ AP が移行する必要がある移行先の WLC の名前と IP アドレスです。

上記のコマンドでは、すべての AP が *AP Configuration: NOT MOBILITY EXPRESS CAPABLE* に変換されます。AP はリロードされ、ローカル モードで再起動されます。

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	高い	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： <ul style="list-style-type: none"> 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： <ul style="list-style-type: none"> 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
受信感度	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)

	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)
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](#)
- [Cisco Mobility Express Command References](#)
- [Cisco Aironet Access Points Ordering Guide](#)
- [Cisco Aironet Universal AP Priming and Cisco AirProvision User Guide](#)
- [Cisco Aironet AP Hardware Guides](#)
 - [Cisco Aironet 1560 Access Point Hardware Guide](#)
 - [Cisco Aironet 1815i Access Point Hardware Guide](#)
 - [Cisco Aironet 1815w Access Point Hardware Guide](#)
 - [Cisco Aironet 1830 Series Access Points Hardware Guide](#)
 - [Cisco Aironet 1850 Series Access Points Hardware Guide](#)
 - [Cisco Aironet 2800 Series Access Points Hardware Guide](#)
 - [Cisco Aironet 3800 Series Access Points Hardware Guide](#)

よくある質問

Cisco 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。

[サポートされているシスコのアクセスポイント \(2 ページ\) #unique_106](#)を参照してください。

Cisco 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。

Cisco 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。

Cisco Mobility Express のライセンス要件はどうなっていますか。

Cisco Mobility Express にアクセスポイント用のライセンスは必要ありません。

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。AP 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 タイプへの AP の変換 \(91 ページ\)](#) 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 **Cisco Mobility Express** に変換することはできますか。

はい。導入環境に Cisco Mobility Express コントローラの機能をホストできる ([サポートされているシスコのアクセスポイント \(2 ページ\) #unique_106](#) にプライマリ AP としてリストされている) AP がある限り、ワイヤレスコントローラベースの導入環境を Cisco Mobility Express に変換できます。

プライマリ AP に接続されている AP 数が 25 台以下の場合、内部 AP 用のクライアント数は最大 20 台に制限されます。効率性を高めてトラフィックの輻輳を軽減するための回避策にはどのようなものがありますか。

Cisco Mobility Express を負荷が低い別の AP に移動させることが回避策になります。Cisco Mobility Express を別の AP に移動させるには、次の手順を実行します。

1. **show ap summary** コマンドを入力します。AP の一覧が表示されます。
2. クライアント数が最も少ない AP を確認します。

3. **config ap next-preferred-master <new_ap_name> forced-failover** コマンドを入力します。このコマンドを実行すると、Cisco Mobility Express コントローラは新しい AP に移動し、現在の AP はクライアントとして機能します。

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。

