Cisco Wireless リリース 8.10 向け Cisco Mobility Express ユーザガイド

初版：2019 年 10 月 18 日

最終更新：2020 年 3 月 19 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/

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 1

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 を介したマスター 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

マスター 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 ごとのクライアント数の制限 39
AP 無線あたりのクライアント数の制限 39
WLAN ユーザの表示と管理 40
双方向帯域幅レート制限 41
クライアントごとの双方向レートの制限 42
BSSID ごとの双方向レートの制限 42
WLAN ごとの双方向レートの制限 43
Cisco Mobility Express ネットワーク内のリモート LAN 44
リモート LAN の作成 44
関連付けられているアクセス ポイントの管理 46
アクセス ポイントの管理 46

外部アンテナの設定 49
WLAN ゲスト ユーザのログイン ページの設定 50
デフォルトのログイン ページの設定 51
カスタマイズされたログイン ページの設定 51
内部 DHCP サーバの管理 53
DHCP プールの追加 53
DHCP プールの編集 54
DHCP プールの削除 54
DHCP リースの詳細の表示 55
リース IP アドレスの詳細のエクスポート 55
リース IP アドレスの開放 55
認証キャッシング機能について 56
WPA/WPA2-Dot1x 認証の設定 56
RADIUS サーバでの MAC フィルタリングの設定 57
Identity PSK の設定 58
キャッシュされた認証ユーザの確認 59

第 5 章 ネットワークの管理 61
管理アクセス インターフェイスの設定 61
Admin アカウントの管理 62
管理者アカウントの追加 63
管理者アカウントの編集 64
管理者アカウントの削除 64
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 64
ゲスト ユーザ アカウントの作成 65
日時の設定 66
自動的に日時を設定するための NTP サーバの使用 66
NTP サーバの追加と編集 66
グローバル NTP サーバの設定（CLI） 67
NTP サーバ ステータスの更新 68
NTP サーバの削除と無効化 68

日時の手動設定 68
Cisco Mobility Express ソフトウェアの更新 69
異種ネットワークに対応するための AP の効率的な接続 70
AP の効率的な参加の設定 71
AP の効率的な参加のステータスを確認 71
HTTP を使用したソフトウェア アップデート 71
TFTP を使用したソフトウェア アップデート 73
SFTP を使用したソフトウェア アップデート 75
Cisco.com からのソフトウェア直接アップデート 76
設定管理 78
設定管理の拡張機能 78
注意事項および制約事項 79
設定の更新（GUI） 79
設定の更新（CLI） 80

第 6 章 メッシュおよび Flex + ブリッジモードの管理 83
Cisco Wave 2 屋内アクセスポイントに搭載されているメッシュ機能について 83
制限とガイドライン 83
Mobility Express Day 0 設定の Flex + ブリッジモードについて 84
Mobility Express の Flex + ブリッジモードに関する制限事項とガイドライン 84
ルートアクセスポイントでの Day 0 Flex + ブリッジの設定（GUI） 85
ルートアクセスポイントでの Day 0 Flex + ブリッジの設定（CLI） 86
ルートアクセスポイントでのソフトウェアのアップグレード（GUI） 86
複数の MAC アドレスのインポート（GUI） 87
ブリッジモードへのマッピングの設定（GUI） 87
FlexConnect グループの設定（CLI） 88
WLAN-VLAN マッピング（CLI）による FlexConnect グループの の設定 89
グローバルメッシュ設定のエキスパートビューの有効化（GUI） 89
アクセスポイントでのメッシュの設定（GUI） 90
トラブルシューティング 90

RAP を使用したメッシュツリーの場合、内部 RAP（ME）でバックホールを無効にすると、外部 RAP が ME モードになる/サイレント再起動する 90

第 7 章 サービスの使用 93

mDNS 93

マルチキャスト ドメイン ネーム システムについて 93

Location Specific Services（ロケーション固有サービス） 93

mDNS ポリシー 94

mDNS ポリシーのクライアント属性 94

mDNS AP 95

プライオリティ MAC サポート 95

Origin-Based Service Discovery 95

マルチキャスト DNS の設定の制限 96

マルチキャスト DNS の設定 96

mDNS ポリシーの設定 98

Cisco Umbrella 99

Cisco Mobility Express に搭載された Cisco Umbrella の概要 99

Cisco Mobility Express での Cisco Umbrella の設定（GUI） 100

Cisco Mobility Express（CLI）での Cisco Umbrella の設定 101

TLS 102

TLS セキュアトンネル 102

TLS トンネルの設定 104

第 8 章 詳細設定の使用と操作 105

SNMP の管理 105

SNMP アクセスの設定 105

SNMPv3 ユーザの追加 106

SNMPv3 ユーザの編集 107

SNMPv3 ユーザの削除 108

システム メッセージ ロギングの設定 108

RF パラメータの最適化 110

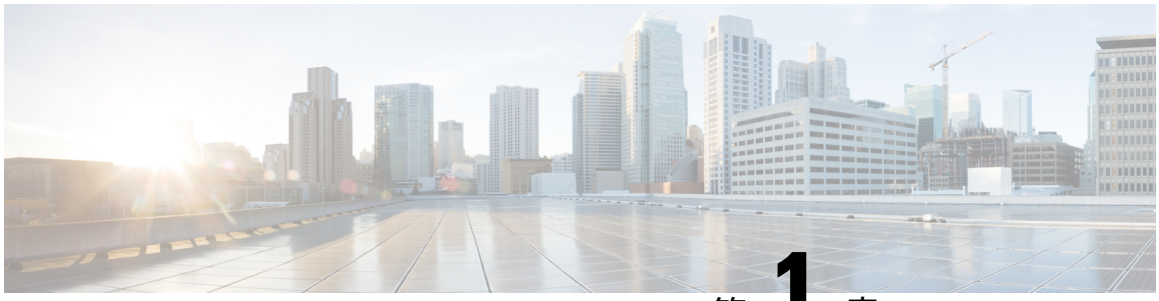
ローミングの最適化 110

ローミングの最適化について 110
ローミングの最適化の制約事項 111
設定の最適化されたローミング 111
コントローラ ツールの使用 112
コントローラの再起動 112
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 112
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 113
コントローラ コンフィギュレーションの保存 113
CMX クラウド プレゼンス分析の使用 114
CMX プレゼンス分析の前提条件 114
CMX プレゼンス分析の有効化 114
DNS アクセス制御リスト 115
DNS アクセス制御リスト（ACL）の設定 116
事前認証レベルで ACL を WLAN に適用 116
事後認証レベルで ACL を WLAN に適用 117
WLAN での AAA オーバーライドの設定 117

付録 A： コントローラ CLI コマンド 119
Cisco Mobility Express CLI 119
CLI 初期設定ウィザードの使用 119
CLI での手順 123
SNMPv3 ユーザのデフォルト値の変更 123
802.11r 高速移行の設定 124
CDP タイマーの設定 125
Cisco Mobility Express（CLI）での Cisco Umbrella の設定 125

付録 B： 概念、FAQ、および高度なユーザに関する情報 127
対応ブラウザ 127
Cisco Mobility Express コントローラのフェールオーバーとマスター AP の選定プロセス 128
VRID の設定 129
アクセス ポイントへのイメージのプレダウンロード 130

CAPWAP の Mobility Express 変換の代替手段 130
CAPWAP イメージの変換 131
Mobility Express から CAPWAP タイプへの AP の変換 132
DHCP オプションを介した Mobility Express AP の CAPWAP への変換 133
RF パラメータの最適化設定 133
アクセス ポイントでの RFID トラッキング 135
RFID トラッキングの設定 135
関連資料 135
よくある質問 136



第 1 章

Cisco Mobility Express について

- 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 （1 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 ヵ所以上と、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 として機能する AP をマスター AP といい、このマスター AP によって管理される Cisco Mobility Express ネットワーク内の他の AP を下位 AP といいます。

WLC として機能する他に、マスター AP は下位 AP 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）

- マスター 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。
- マスター 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 へと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*

マスター 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

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

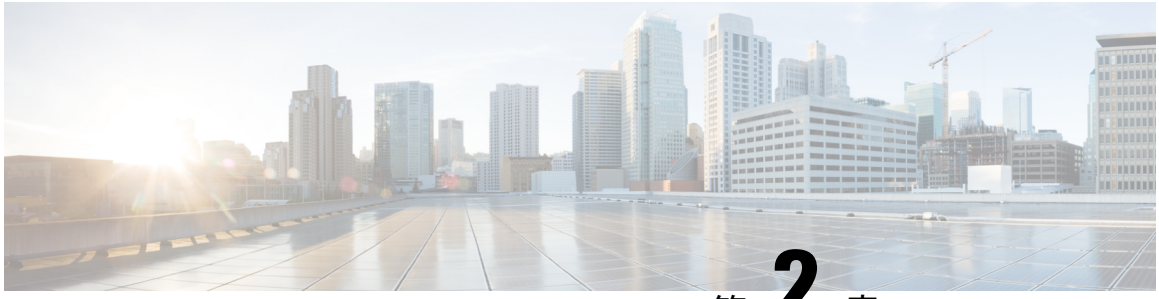
- Cisco Mobility Express ソフトウェア イメージ。これらのモデルのモデル番号（または製品 ID）は C で終わります。
- Lightweight AP ソフトウェア イメージ。ワイヤレス コントローラに join するための Control And Provisioning of Wireless Access Points（CAPWAP）プロトコルに基づきます。これらのモデルは Cisco Mobility Express ソフトウェア イメージを含むようにオンサイトで手動により変換できます。この変換については、CAPWAP Lightweight AP から Cisco 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 を介したマスター 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）
- マスター 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 をマスター AP として動作させ、他の AP をその AP に接続するために必要です。これにより、事前定義された *CiscoAirProvision* サービス セット識別子（SSID）はマスター AP によってのみアドバタイズされ、他の AP によっては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。

  マスター AP によってアドバタイズされる事前定義の CiscoAirProvision SSID に接続するためには、Wi-Fi 対応のラップトップが必要です。この SSID に有線ネットワークからアクセスすることはできません。

- ラップトップには、互換性のあるブラウザがインストールされている必要があります。Cisco Mobility Express ワイヤレス コントローラの Web インターフェイスおよび初期設定ウィザードと互換性のあるブラウザのリストについては、対応ブラウザ （127 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 （119 ページ）」を参照してください。

Cisco Plug and Play を介したマスター 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）サーバを介してマスター 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イ ゼロ時の初期設定の場合にのみ有効になります。

デイ ゼロ時に 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 の中からマスター AP を選択します。選択したこのマスター 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 ネットワーク内のマスター 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。
- マスター 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 がブロードキャスティングを開始するまでには、数分かかります。*CiscoAirProvision* SSID がブロードキャスティングを開始したら、AP のステータス LED が緑、赤、オレンジの順に循環して点灯します。

ステップ 2 Wi-Fi 対応のラップトップを、AP によってアドバタイズされる *CiscoAirProvision* SSID へ、Wi-Fi 経由で接続します。パスワードは password です。

ラップトップはサブネット 192.168.1.0/24 から IP アドレスを取得します。

ステップ 3 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 とも呼ばれる）を選択します。
- Pass Phrase：[WPA2 Personal] セキュリティを選択した場合は、PSK を指定します。
- Authentication Server IP Address：[WPA2 Enterprise] セキュリティを選択した場合は、RADIUS サーバの IP アドレスを入力します。
- Shared Secret：RADIUS サーバ用のパスワードを入力します。
- VLAN：[Management VLAN]（VLAN 0）を選択するか、[New VLAN] を選択して新規作成（1 ～ 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（133 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 （110 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

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`	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。 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、マスター 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。 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 ap-type mobility-express tftp コマンドを実行します。AP が再起動し、オンラインに戻り、マスター AP の選定プロセスに参加します。これがマスター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。

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、CiscoAirProvison SSID のブロードキャスティングを開始します。

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 （130 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 （132 ページ）を参照してください。

マスター AP に関連付ける AP の準備

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

始める前に

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

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

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

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

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

ステップ 4 ソフトウェア アップデートを実行します。。

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 （46 ページ）

Cisco Mobility Express へのログイン

ステップ 1 ブラウザを開き、ブラウザのアドレス バーに**`https://<ip address>`**と入力して、Cisco Mobility Express の [Wireless LAN Controller] ログイン ページにアクセスします。この IP アドレスは、Cisco Mobility Wireless Express コントローラを管理するために指定したアドレスです。

Cisco Mobility Express コントローラは、HTTPS に自己署名証明書を使用します。そのため、すべてのブラウザに警告が表示され、証明書がブラウザに表示されたときに例外の状態でも続行するかどうか尋ねられます。Mobility Express の [Wireless LAN Controller] ログイン ページにアクセスするためには、警告を受け入れます。

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

ステップ 2 [Login] をクリックします。

ステップ 3 管理者ユーザのクレデンシャルを入力してログインします。

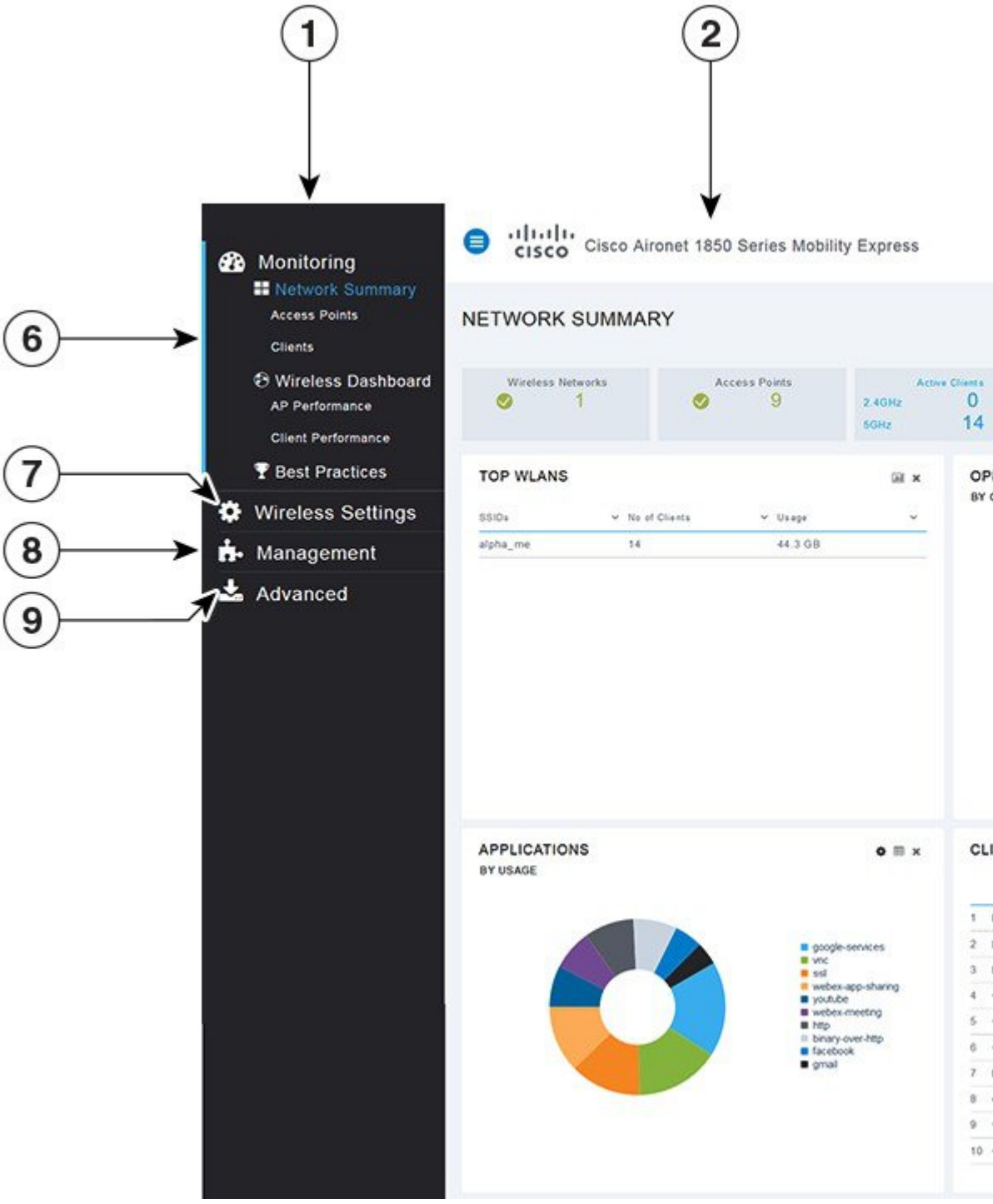
次のタスク

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。

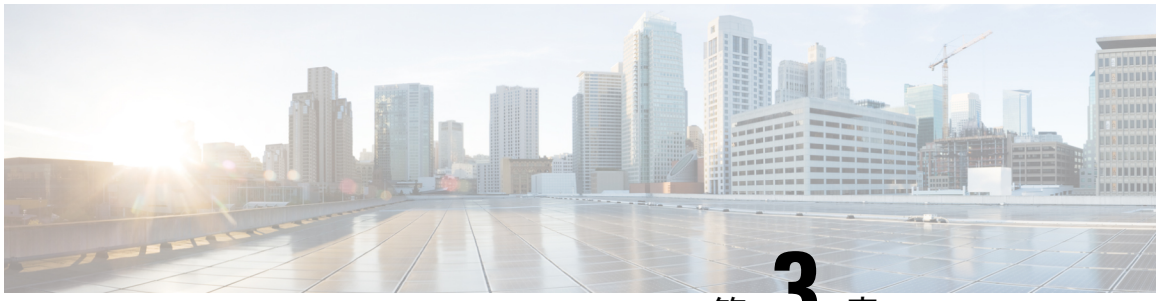
Mobility Express コントローラの Web インターフェイスについて

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マスター AP の AP モデルを示します。
3	AP またはクライアントを、MAC アドレスを使用して検索します。
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 （113 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、マスター AP は、WLAN をモニタできるだけでなく、ネットワーク上のすべての接続デバイスと未接続デバイスをモニタできます。

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

- 設定された WLAN の詳細を表示する。
- トラフィックおよび関連するクライアントに基づいた上位 WLAN を一覧表示する。
- ネットワーク内の AP の詳細を表示する。
- 2.4 GHz または 5 GHz 帯でアクティブに動作するクライアントの詳細を表示する。
- これらのデバイスで稼働するクライアント デバイス オペレーティング システムとアプリケーションの概要を表示する。
- 不正なクライアントおよび AP の詳細なリストを表示する。

- 無線周波数が 2.4 GHz および 5 GHz であるネットワークに存在する各種干渉の詳細を表示する。
- ネットワーク内の AP のパフォーマンスをモニタする。
- ネットワーク内のクライアントのパフォーマンスをモニタする。

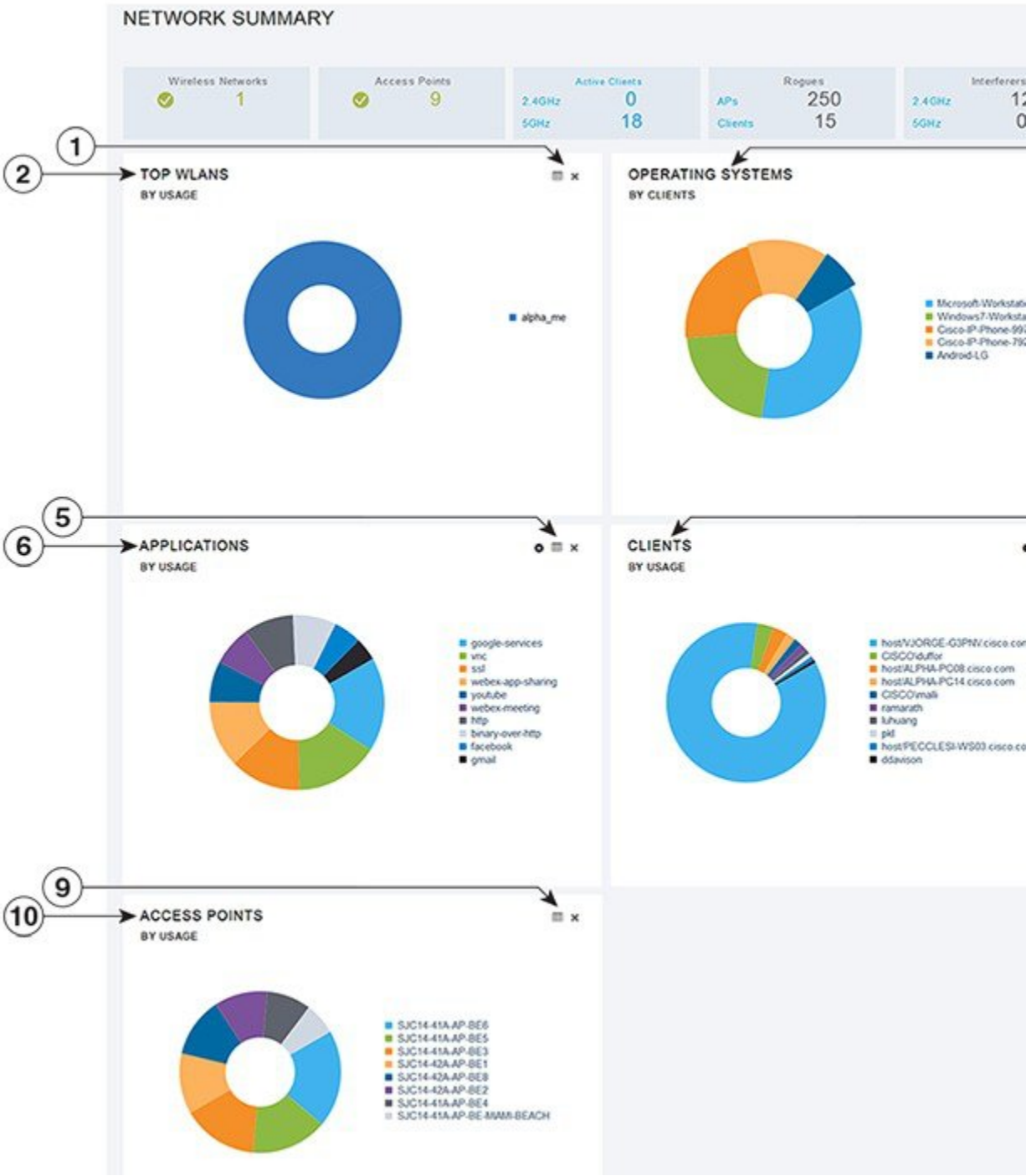
（注）
- [Network Summary] ウィンドウに表示されるパラメータはすべて読み取り専用です。
- このページは 30 秒ごとに自動的にリフレッシュされます。

[Network Summary] ビューのカスタマイズ

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

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

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



WLAN ユーザの表示と管理

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

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

WLAN の表示

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

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

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

設定済み WLAN の詳細の表示

ステップ 1　**[Monitoring]** > **[Network Summary]** の順に選択します。

[Wireless Networks] サマリー ウィンドウに、設定済み WLAN の数が表示されます。

ステップ 2　[Wireless Networks] サマリー ウィンドウで、ステータス アイコンまたはカウント表示アイコンをクリックすると、対応する WLAN の高度な詳細情報（[Active] ステータス、[Name]、[Security Policy]、[Radio Policy] など）が表示されます。

[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。

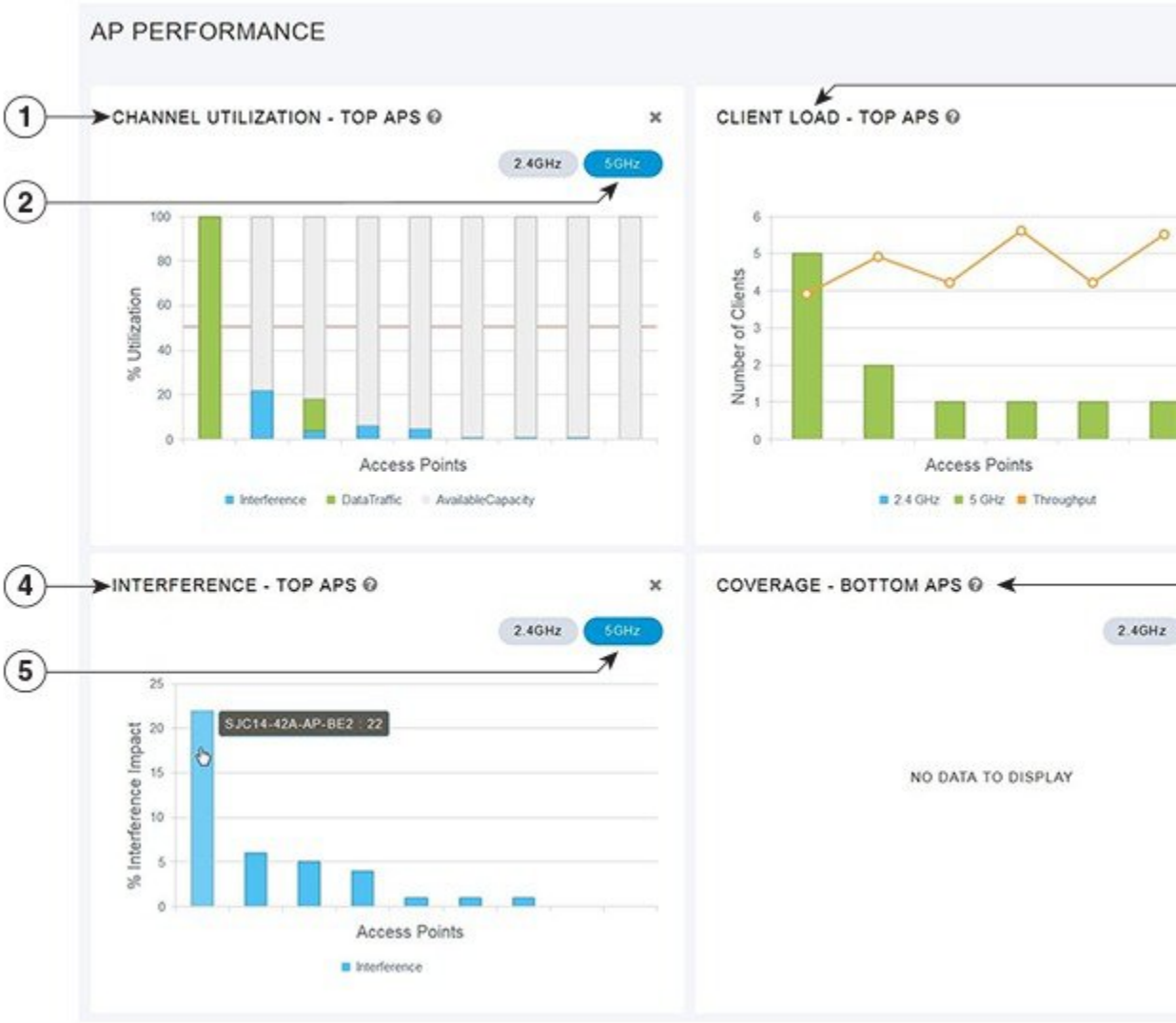
[Interferers Summary] ウィンドウに、すべての非 WiFi 干渉デバイスのサマリーが表示されます。これらの干渉は、2.4 GHz または 5 GHz で動作する可能性があります。

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。

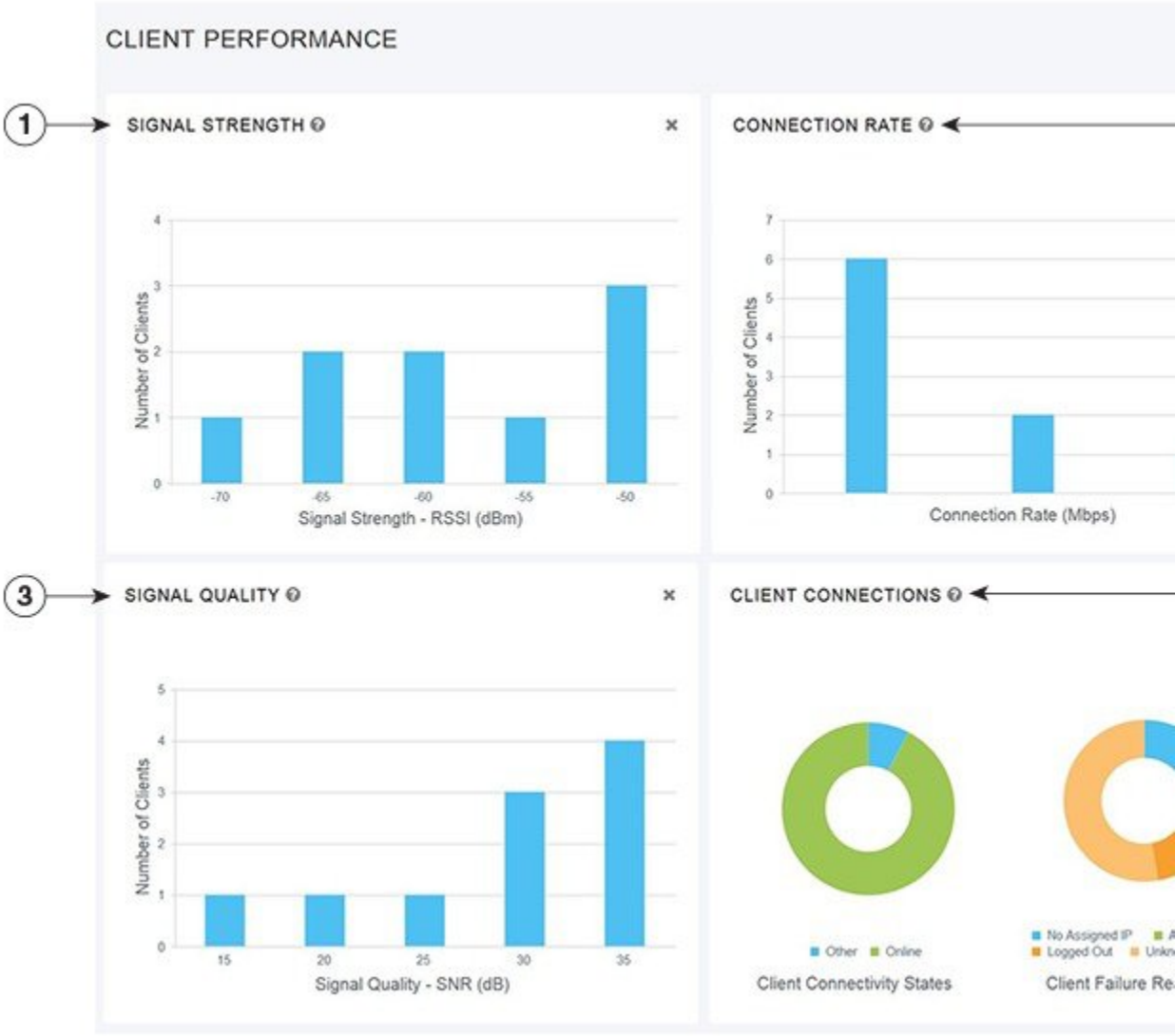
ステップ 2 削除するウィジェットの右上にある [Delete Widget] アイコンをクリックします。

[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。

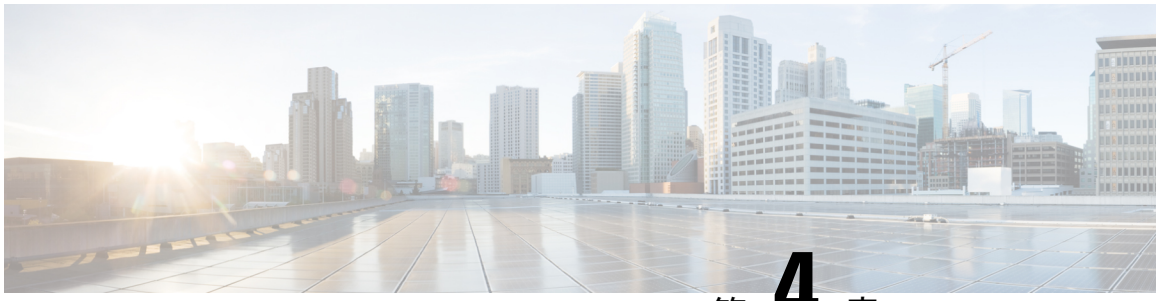
[Client Performance] ウィンドウがリフレッシュされ、新しいウィジェットが表示されます。

[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）
- Cisco Mobility Express ネットワーク内のリモート LAN （44 ページ）
- 関連付けられているアクセス ポイントの管理 （46 ページ）
- WLAN ゲスト ユーザのログイン ページの設定 （50 ページ）
- 内部 DHCP サーバの管理 （53 ページ）
- 認証キャッシング機能について （56 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、マスターAPのコントローラで現在設定されているすべてのWLANが一覧表示されます。この一覧には、各 WLAN に関する次の詳細情報が表示されます。

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

WLAN のセットアップに関する注意事項と制約事項

- Cisco Mobility Express コントローラには、最大 16 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。
- [Local Profiling]：

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。マスター AP のコントローラは、認証サーバおよびローカル ユーザ データベースとして機能するため、外部認証サーバに依存する必要がなくなります。

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

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

- Guest：コントローラは、ゲスト ユーザ専用の WLAN でゲスト ユーザ アクセスを提供できます。この WLAN をゲスト ユーザ アクセス専用に設定するには、[Security] に [Guest] を選択します。

  ゲスト ユーザの認証を設定するには、[Guest 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 （40 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、ネットワーキング スタックとのデータ送受信をするアプリケーションが使用できます。一部のポートは、Telnet、SSH、HTTP など特定のアプリケーション用に指定されています。
5. [DSCP] ドロップダウン リストから次のオプションのいずれかを選択して、この ACL の Differentiated Service Code Point（DSCP）値を指定します。[DSCP] は、インターネット上の QoS を定義するために使用できる IP ヘッダー テキスト ボックスです。次のオプションを選択できます。
   - [Any]：任意の DSCP（これは、デフォルト値です）

- [Specific]：DSCP 編集ボックスに入力する、0 ～ 63 の特定の DSCP

6. [Apply] アイコンをクリックして、変更を確定します。

ステップ 7 Quality of Service（QoS）とは、選択したネットワーク トラフィックにさまざまなテクノロジーに渡る優れたサービスを提供する、ネットワークの機能を意味します。QoS の主要な目的は、専用の帯域幅の確保、ジッターおよび遅延の制御（ある種のリアルタイム トラフィックや対話型トラフィックで必要）、および損失特性の改善などを優先的に処理することです。

Cisco Mobility Express コントローラでは次の 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 （40 ページ）」を参照してください。

WLAN の有効化と無効化

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

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

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

ステップ 4 [Apply] をクリックします。

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

WLAN の編集と削除

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

- WLAN を編集するには、その隣にある [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 ごとのクライアント数の制限

マスター AP に応じて、Cisco Mobility Express は WLAN ごとに最大 100 の AP と、2,000 の クライアントをサポートします。Cisco Mobility Express ネットワーク上のクライアント数を制限するには、次を実行します。

始める前に

ステップ 1 [Expert] ビューで、**[Wireless Settings]** > **[WLANs]** に移動します。

[WLAN/RLAN Configuration] ウィンドウが表示されます。

ステップ 2 [Add New WLAN/RLAN] をクリックします。

既存の WLAN のクライアントの制限を変更するには、[WLAN/RLAN] テーブルの特定の WLAN に移動し、[Edit] アイコンをクリックします。

[Add New WLAN/RLAN] ウィンドウが表示されます。

ステップ 3 [Advanced] タブで、[Maximum Allowed Clients] の特定の値を対応するドロップダウンリストから選択するか、または入力します。

ステップ 4 [Apply] をクリックして、変更内容を保存します。

[WLAN/RLAN Configuration] ウィンドウが表示されます。

選択した WLAN が、指定したクライアントの最大数で設定されています。

AP 無線あたりのクライアント数の制限

Cisco Mobility Express は、単一の AP 無線上で最大 200 の接続クライアントをサポートします。Cisco Wireless リリース 8.7 以降、この制限は以下を実行することによって変更できます。

始める前に

ステップ 1 [Expert] ビューで、**[Wireless Settings]** > **[WLANs]** に移動します。

[WLAN/RLAN Configuration] ウィンドウが表示されます。

ステップ 2 [Add New WLAN/RLAN] をクリックします。

既存の WLAN の AP 無線ごとの最大クライアント制限を変更するには、[WLAN/RLAN] テーブル内の特定の WLAN に移動し、[Edit] アイコンをクリックします。

[Add New WLAN/RLAN] ウィンドウが表示されます。

ステップ 3 [Advanced] タブで、[Maximum Allowed Clients Per AP Radio] の特定の値を対応するドロップダウンリストから選択するか、または入力します。

ステップ 4 [Apply] をクリックして、変更内容を保存します。

[WLAN/RLAN Configuration] ウィンドウが表示されます。

選択した WLAN が AP 無線に接続可能な改訂したクライアントの最大数で設定されます。

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。

双方向帯域幅レート制限

Cisco Mobility Express ネットワーク上でクライアント デバイス、WLAN、および BSSID のスループットの制限を定義できます。双方向レート制限によって、ネットワーク帯域幅がすべてのユーザに平等に分配されます。Cisco Mobility Express ネットワーク上のクライアント デバイス、WLAN、および BSSID に双方向帯域幅レート制限を設定するには、次の手順を実行します。

- クライアントごとの双方向レートの制限 （42 ページ）
- BSSID ごとの双方向レートの制限 （42 ページ）
- WLAN ごとの双方向レートの制限 （43 ページ）

クライアントごとの双方向レートの制限

ステップ 1 **[Wireless Settings]** > **[WLANs]** に移動します。

[WLAN/RLAN Configuration] ウィンドウが表示されます。

ステップ 2 [Add New WLAN/RLAN] をクリックします。

既存の WLAN の双方向レート制限を変更するには、テーブル内の特定の WLAN に移動し、[Edit] アイコンをクリックします。

[Add New WLAN/RLAN] ウィンドウが表示されます。

ステップ 3 [Traffic Shaping] タブで、クライアントごとのダウンストリームとアップストリームの制限に特定の値を選択するか、または入力します。

[Standard] ビューで、対応するスライダーを移動して、次のように特定の値を選択します（Mbps 単位）。

- **[Per-client downstream bandwidth limit]**
- **[Per-client upstream bandwidth limit]**

[Expert] ビューで、[Rate limits per client] セクションの下にある次のフィールドに特定の値を指定します（kbps 単位）。

- **[Average downstream bandwidth limit]**
- **[Average real-time downstream bandwidth limit]**
- **[Average upstream bandwidth limit]**
- **[Average real-time upstream bandwidth limit]**

ステップ 4 [Apply] をクリックして、変更内容を保存します。

[WLAN/RLAN Configuration] ウィンドウが表示されます。

新しい設定に従って、双方向帯域幅はクライアント デバイスごとに制限されています。

BSSID ごとの双方向レートの制限

ステップ 1 **[Wireless Settings]** > **[WLANs]** に移動します。

[WLAN/RLAN Configuration] ウィンドウが表示されます。

ステップ 2 [Add New WLAN/RLAN] をクリックします。

既存の WLAN の双方向レート制限を変更するには、テーブル内の特定の WLAN に移動し、[Edit] アイコンをクリックします。

[Add New WLAN/RLAN] ウィンドウが表示されます。

ステップ 3 [Traffic Shaping] タブで、BSSID ごとのダウンストリームとアップストリームの制限に特定の値を選択するか、または入力します。

[Standard] ビューで、対応するスライダーを移動して、次のように特定の値を選択します（Mbps 単位）。

- **[Per-BSSID downstream bandwidth limit]**
- **[Per-BSSID upstream bandwidth limit]**

[Expert] ビューで、[Rate limits per BSSID] セクションの下にある次のフィールドに特定の値を指定します（kbps 単位）。

- **[Average downstream bandwidth limit]**
- **[Average real-time downstream bandwidth limit]**
- **[Average upstream bandwidth limit]**
- **[Average real-time upstream bandwidth limit]**

ステップ 4 [Apply] をクリックして、変更内容を保存します。

[WLAN/RLAN Configuration] ウィンドウが表示されます。

新しい設定に従って、双方向帯域幅は BSSID ごとに制限されています。

WLAN ごとの双方向レートの制限

ステップ 1 **[Wireless Settings]** > **[WLANs]** に移動します。

[WLAN/RLAN Configuration] ウィンドウが表示されます。

ステップ 2 [Add New WLAN/RLAN] をクリックします。

既存の WLAN の双方向レート制限を変更するには、テーブル内の特定の WLAN に移動し、[Edit] アイコンをクリックします。

[Add New WLAN/RLAN] ウィンドウが表示されます。

ステップ 3 [Traffic Shaping] タブで、WLAN ごとのダウンストリームとアップストリームの制限に特定の値を選択するか、または入力します。

[Standard] ビューで、対応するスライダーを移動して、次のように特定の値を選択します（Mbps 単位）。

- **[Per-WLAN downstream bandwidth limit]**
- **[Per-WLAN upstream bandwidth limit]**

[Expert] ビューで、[Rate limits per WLAN] セクションの下にある次のフィールドに特定の値を指定します（kbps 単位）。

- **[Average downstream bandwidth limit]**

- **[Average real-time downstream bandwidth limit]**
- **[Average upstream bandwidth limit]**
- **[Average real-time upstream bandwidth limit]**

ステップ 4 [Apply] をクリックして、変更内容を保存します。

[WLAN/RLAN Configuration] ウィンドウが表示されます。

新たに指定された値に従って、双方向帯域幅は WLAN で制限されるようになります。

Cisco Mobility Express ネットワーク内のリモート LAN

[WLAN/RLAN Configuration] ウィンドウを通じてリモート ローカル エリア ネットワーク（RLAN）を作成し、管理できます。このウィンドウへは **[Wireless Settings]** > **[WLANs]** でアクセスできます。RLAN では、1810W や1815W のような Cisco AP 上で有線ポートを管理できます。

Cisco Mobility Express ネットワーク上で RLAN 機能を有効にするには、次のタスクを指定された順序で実行します。

- RLAN を作成します。
- AP グループを作成します。
- RLAN を AP グループに関連付けます。
- （管理する必要がある有線ポートを備えた）AP をAP グループに追加します
- 有線 ポートを RLAN に関連付けます。

リモート LAN の作成

ステップ 1 **[Wireless Settings]** > **[WLANs]** に移動します。

このウィンドウには、Cisco Mobility Express コントローラ上に設定されているすべての WLAN とリモート LAN のカウントが表示されます。また、設定された WLAN と RLAN の詳細を示すテーブルも表示されます。

各リモート LAN については、プロファイル**名**、管理状態、**タイプ**（RLAN）、および**セキュリティ ポリシー**を確認できます。WLAN およびリモート LAN を表示するテーブルが複数ページに及ぶ場合、ページ番号のリンクをクリックすると、それらのページにアクセスできます。

[WLAN/RLAN Configuration] ウィンドウが表示されます。

ステップ 2 [Add New WLAN/RLAN] をクリックします。

[Add New WLAN/RLAN] ウィンドウが表示されます。

ステップ 3 [WLANs] を選択して、[WLANs] ページを開きます。

このページでは、コントローラ上で現在設定されているすべての WLAN およびリモート LAN が表示されます。各 WLAN について、WLAN/リモート LAN ID、プロファイル名、タイプ、SSID、ステータス、およびセキュリティ ポリシーを表示できます。

WLAN/リモート LAN の合計数がページの右上隅に表示されます。WLAN/リモート LAN 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。

（注） リモート LAN を削除する場合は、カーソルを目的の WLAN の青いドロップダウン矢印の上に置いて、[Remove] を選択するか、または行の左側のチェックボックスをオンにして、ドロップダウン リストから [Remove Selected] を選択し、[Go] をクリックします。決定を確認するメッセージが表示されます。作業を続行すると、割り当てられているアクセス ポイント グループおよびアクセス ポイント無線からそのリモート LAN が削除されます。

ステップ 4 ドロップダウン リストから [Create New] を選択し、[Go] をクリックして新規の Remote-LAN を作成します。[WLANs > New] ページが表示されます。

ステップ 5 [Type] ドロップダウン リストから、[Remote LAN] を選択してリモート LAN を作成します。

ステップ 6 [Profile Name] テキスト ボックスに、このリモート WLAN に割り当てるプロファイル名に対する最大 32 文字の英数字を入力します。プロファイル名は固有である必要があります。

ステップ 7 [WLAN ID] ドロップダウン リストから、この WLAN の ID 番号を選択します。

ステップ 8 [Apply] をクリックして、変更を確定します。[WLANs > Edit] ページが表示されます。

（注） 編集する WLAN の ID 番号をクリックすることにより、[WLANs] ページから [WLANs > Edit] ページを開くこともできます。

ステップ 9 [General] タブ、[Security] タブ、および [Advanced] タブ上でパラメータを使用してこのリモート LAN を設定します。特定の機能を設定する手順については、この章の後の項を参照してください。

ステップ 10 [General] タブの [Status] チェックボックスをオンにして、このリモート LAN を有効にします。リモート LAN に対する設定変更が終了するまで、チェックボックスをオフにしておいてください。

（注） また、[WLANs] ページから、有効化または無効化する ID の左側のチェック ボックスをオンにして、ドロップダウンリストから [Enable Selected] または [Disable Selected] を選択し、[Go] をクリックすることでも、リモート LAN を有効化または無効化できます。

ステップ 11 [Apply] をクリックして、変更を確定します。

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

関連付けられているアクセス ポイントの管理

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

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

  図 *14*：プライマリ コントローラ（マスター *AP*）アイコン

  図 *15*：従属 *AP* アイコン

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

（注） AP が AP グループに参加するとき、または AP グループの RF プロファイルが変更されたときに AP の CAPWAP プロセスが再起動され、すべての AP の再起動が回避されます。新しい CAPWAP 再起動ペイロードが AP に送信され、CAPWAP プロセスのみが再起動されます。応答として、AP では新しい AP グループまたは RF プロファイルに固有の新しい設定を受信します。コントローラへの AP の接続が失われ、AP がネットワークをリロードして再度参加します。

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

- [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。	
[Channel]	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。 [Automatic] を選択すると、動的チャネル割り当てが有効になります。つまり、マスター AP の制御下にある各 AP にチャネルが動的に割り当てられます。これにより、隣接する AP が同じチャネル上でブロードキャストされることがなくなり、干渉などの通信の問題を回避できます。2.4 GHz 無線の場合、米国では 11 チャネルが提供され、米国以外の国や地域では最大 14 チャネルが提供されます。ただし、隣接する AP で使用される場合、非オーバーラップと見なすことができるのは、1-6-11 のみです。 特定の値を割り当てると、その AP にチャネルが静的に割り当てられます。	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。 5 GHz の無線の場合は、最大 23 の非オーバーラップ チャネルが提供されます。 特定の値を割り当てると、その AP にチャネルが静的に割り当てられます。
[Channel Width]	2.4 GHz のチャネル幅は 20 MHzにしか設定できません。	チャネル ボンディングを使用する場合、5 GHz のチャネル幅は [Automatic]、あるいは 20、40、または 80 MHz に設定できます。 チャネル ボンディングは、1 つの無線ストリーム用のチャネルを 2 つまたは 4 つのグループに分けます。これにより、速度とスループットが向上します。2.4 GHz のチャネル数が不十分である場合は、複数の非オーバーラップチャネルを有効にするためにチャネル ボンディングを使用することはできません。

パラメータ	説明
[Transmit Power]	[Automatic] に設定するか、または 1 ～ 8 の値を設定できます。 これは対数目盛の送信電力、つまり AP で使用される伝送エネルギーです。[1] が最高、[2] が [1] の半分、[3] が [1] の 1/4 となり、以下同様に減少していきます。 [Automatic] を選択すると、受信側の変動する信号レベルに基づいて、無線のトランスミッタ電力が調整されます。これによりトランスミッタは、フェーディング条件が発生した場合に、ほとんどの時間、最大電力未満で動作できるようになります。これが最大値に到達するまで、送信電力が必要に応じて増加します。

ステップ 6 [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。
        1. 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。
        2. 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 （40 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 （51 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 （51 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 1 MB 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。

認証キャッシング機能について

認証キャッシング機能により、認証に不可欠なクライアント情報が、RADIUS サーバとの認証に成功した時点でコントローラ上のキャッシュにローカル保存されます。RADIUS サーバへの接続が失われると、キャッシュに保存された情報がクライアントの認証に使用されます。

RADIUS サーバが稼働中は、キャッシュを設定することも可能です。クライアントの詳細がローカルに存在しない場合、認証要求は RADIUS サーバを介して送信されます。

サポートされるセキュリティタイプは、次のとおりです。

- RADIUS サーバを使用した MAC フィルタリング
- WPA/WPA2-Dot1x 認証
- MAC フィルタ障害時の Web 認証
- Identity PSK（iPSK）

WPA/WPA2-Dot1x 認証の設定

WPA/WPA2 Dot1x を設定するには、次の手順に従います。

ステップ 1 [Wireless Settings] > [WLANs] の順に選択します。
[WLAN/RLAN 構成（WLAN/RLAN Configuration）] ページが表示されます。

ステップ 2 [Add new WLAN/RLAN] をクリックします。
[新規 WLAN/RLAN の追加（Add New WLAN/RLAN）] 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。

a) [Profile Name]：プロファイル名は一意であり、最大 32 文字までです。

b) [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。

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。

a) 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。

b) [RADIUS Servers] セクションで [Authentication Caching] を有効にし、[User Cache Timeout] を分単位で入力します。必要に応じて、[User Cache Reuse] を有効にします。デフォルトでは、[ユーザキャッシュの再利用（User Cache Reuse）] は無効になっています。

c) [Add RADIUS Authentication Server] をクリックします。サーバの詳細を入力して [適用（Apply）] をクリックします。

（注） RADIUS サーバに設定されている AV ペアを次に示します。

- **AC-Supported=yes**：ACCESS-REQUEST を使用してのみ送信され、認証キャッシュのサポートが有効になります。
- **AC-User-Name**：dot1x のユーザ名が ACCESS-ACCEPT の一部として送信されます。
- **AC-Credential-Hash**：ハッシュされたユーザパスワードが ACCESS-ACCEPT の一部として送信されます。

ステップ 5 [Advanced] タブを選択します。

ステップ 6 [AAA オーバーライドを許可（Allow AAA Override）] トグルボタンを使用して、AAA オーバーライドを有効にします。

ステップ 7 [Apply] をクリックします。

RADIUS サーバでの MAC フィルタリングの設定

次に示す手順に従って MAC フィルタリングを設定し、RADIUS サーバで [On MAC Filter Failure] を有効にします。

ステップ 1 [Wireless Settings] > [WLANs] の順に選択します。
[WLAN/RLAN Configuration] ページが表示されます。

ステップ 2 [Add new WLAN/RLAN] をクリックします。
[Add new WLAN/RLAN] 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。

a) [Profile Name]：プロファイル名は一意であり、最大 32 文字までです。

b) [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。

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

a) [Guest Network] を有効にします。

b) [MAC Filtering] を有効にします。

c) [Captive Portal] で [External Splash Page] を選択します。

d) [Captive Portal URL] フィールドに、Web サーバの URL を入力します。
e) [Access Type] で [RADIUS] を選択します。
f) [On MAC Filter Failure] を有効にします。
g) [RADIUS 認証サーバの追加（Add RADIUS Authentication Server）] をクリックします。サーバの詳細を入力して [適用（Apply）] をクリックします。

ステップ 5 [Advanced] タブを選択します。

ステップ 6 [AAA オーバーライドを許可（Allow AAA Override）] トグルボタンを使用して、AAA オーバーライドを有効にします。

ステップ 7 [Apply] をクリックします。

Identity PSK の設定

Identity PSK を設定するには、次の手順に従います。

ステップ 1 [Wireless Settings] > [WLANs] の順に選択します。
[WLAN/RLAN Configuration] ページが表示されます。

ステップ 2 [Add New WLAN/RLAN] をクリックします。
[新規 WLAN/RLAN の追加（Add New WLAN/RLAN）] 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。

a) [Profile Name]：プロファイル名は一意であり、最大 32 文字までです。
b) [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。

ステップ 4 [WLAN Security] タブで、次の設定を行います。

a) [MAC Filtering] を有効にします。
b) [Security Type] ドロップダウンリストで、[WPA2 Personal] のセキュリティ認証オプションを選択します。このオプションは、事前共有キー（PSK）を使用した Wi-Fi Protected Access 2 を意味します。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。
c) [Passphrase Format] では、[HEX] または [ASCII] を選択します。
d) [Passphrase] と [Confirm Passphrase] を入力します。
e) [RADIUS Servers] セクションで [Authentication Caching] を有効にし、[User Cache Timeout] を分単位で入力します。必要に応じて、[User Cache Reuse] を有効にします。デフォルトでは、[User Cache Reuse] は無効になっています。
f) [Add RADIUS Authentication Server] をクリックします。サーバの詳細を入力して、[Apply] をクリックします。

MAC 認証が成功すると、RADIUS サーバは次の Cisco AVPair 属性を返します。

- **psk-mode** の値は、**`ASCII`**、**`HEX`**、**`asciiEnc`**、**`hexEnc`** のいずれかになります。
- **psk**

（注） キーはMACアドレスとともにローカルキャッシュに保存され、後続の認証に使用されます。

（注） psk 値は単純に **ASCII** や **16 進数**の場合もあれば、**asciiEnc** や **hexEnc** の場合は暗号化されます。暗号化や復号化に使用されるアルゴリズムは、RFC2865（ユーザパスワードセクション：16 バイトのオーセンティケータの後に暗号化キーが続く）に準拠します。

ステップ 5 [Advanced] タブを選択します。

ステップ 6 [Allow AAA Override] トグルボタンを使用して、AAA オーバーライドを有効にします。

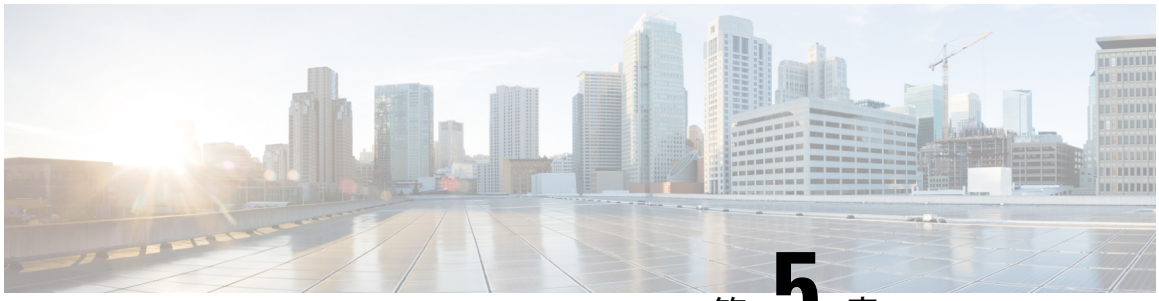
ステップ 7 [Apply] をクリックします。

キャッシュされた認証ユーザの確認

ステップ 1 キャッシュされた認証済みユーザを確認するには、[Management] > [Admin Accounts] を選択します。[Admin Accounts] ページが表示されます。

ステップ 2 [Admin Accounts] ページで、[Auth Cached Users] タブを選択します。
キャッシュされた認証済みユーザのサマリと詳細（MAC アドレス、ユーザ名、SSID、タイムアウト、残り時間など）が表示されます。

ステップ 3 リスト内のキャッシュされた認証ユーザをダブルクリックすると、キャッシュの詳細が表示されます。



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 （61 ページ）
- Admin アカウントの管理 （62 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 （64 ページ）
- 日時の設定 （66 ページ）
- Cisco Mobility Express ソフトウェアの更新 （69 ページ）
- 設定管理 （78 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て使用します。
  - 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 （63 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 （62 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 （63 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す。

[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められます。

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。現在の日時が [Set Time Manually] フィールドに表示されます。既存の NTP サーバがある場合、[NTP Index] 値の順に表示されます。

ステップ 2 [NTP Polling Interval] フィールドに、ポーリング間隔（秒単位）を指定します。

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。

c) すべての AP（内部と外部の両方）をコントローラが同期するのと同じ NTP サーバと同期させる場合は、[APに適用（Apply for APs）] オプションを有効にします。

- [Apply for APs] オプションでは、一度に 1 つの NTP サーバのみ設定できます。このオプションで 1 つの NTP サーバを設定すると、他のすべての設定済み NTP サーバは冗長になり、これらの冗長サーバへは接続されません。また、NTP サーバのフォールバックもありません。
- このオプションを有効にすると、NTP サービスがコントローラで再起動されます。
- [Apply for APs] オプションをサポートしていないリリースからサポートしているリリースにアップグレードすると、デフォルトでは [Apply for APs] オプションによって NTP サーバは設定されません。
- [Apply for APs] オプションをサポートしているリリースから、サポートしていない旧リリースにダウングレードすると、ダウングレード後に [Apply for APs] の設定は失われます。
- 高可用性シナリオでは、[Apply for APs] オプションの設定はスタンバイユニットと同期されます。

ステップ 5 [Apply] をクリックします。

グローバル NTP サーバの設定（CLI）

ステップ 1 次のコマンドを入力して、グローバル NTP サーバを設定します。この設定は、コントローラが時間に関する情報を取得して、外部 AP に送信するために使用します。

config advanced apgroup-global-ntp add *ntp-server-index*

ステップ 2 （任意）次のコマンドを入力して、グローバル NTP サーバを削除します。

config advanced apgroup-global-ntp delete

ステップ 3 次のコマンドを入力して、1 つまたはすべての AP のグローバル NTP サーバに関する情報を表示します。

show ap ntp-server-info {**all** | *cisco-ap*}

ステップ 4 次のコマンドを入力して、AP グループに設定されているグローバル NTP サーバに関する情報を表示します。

show advanced apgroup-global-ntp

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 日曜日から始まり、11 月の第 1 日曜日で終わります。

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

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

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

ステップ 6 [Apply] をクリックします。

Cisco Mobility Express ソフトウェアの更新

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

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

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

コントローラの Web インターフェイスを使用して Cisco Mobility Express コントローラ ソフトウェアを更新できます。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（71 ページ）を参照してください。
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（73 ページ）を参照してください。
SFTP を使用したソフトウェア アップデート	SFTP を使用したソフトウェア アップデート（75 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 （76 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マスター AP に

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

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。

異種ネットワークに対応するための AP の効率的な接続

効率的な AP の参加機能では、新しい AP がネットワークに参加すると、AP はネットワーク ファイル サーバからではなく、イメージ マスター AP からイメージをダウンロードします。新しい AP がネットワークに参加し、同じイメージ タイプの別の AP がすでにネットワークに存在している場合、新しい AP は既存の AP (イメージ マスター) からイメージをダウンロードします。その結果、WAN ネットワーク上のトラフィックが減少します。

効率的な AP 参加イメージのダウンロードのシーケンスは次のとおりです。

- 新しい AP（スレーブ AP）が Mobility Express（ME）ネットワークに参加すると、 ME はまず、効率的な AP の参加機能が有効であるか、AP のタイプが Cisco Wave 2 AP であるか、およびイメージのバージョンが 8.8 またはそれ以降であるかをチェックします。
- ME は、マスターおよびスレーブの設定メッセージを選択したマスターに送信します。トリガーのメッセージは、加入メッセージへの応答として、スレーブに送信されます。
- その後、スレーブ AP は、TFTP 経由でイメージをダウンロードするイメージのマスター AP を問い合わせます。イメージのマスター AP からの応答がないと、スレーブ AP はイメージ マスター AP に TFTP 要求を継続的に送信し、再試行回数を超過した場合、ディスカバリ モードに戻ります。
- スレーブ AP がイメージ マスターからイメージを正常にダウンロードすると、スレーブ AP は再起動し、新しいイメージで ME に参加します。

（注） システムに十分なメモリがない場合は、フォールバック機能により、外部サーバから新しく参加した AP にイメージがストリーミングされます。

転送モードを HTTP に設定している場合、このフォールバック機能はサポートされません。

AP の効率的な参加の設定

始める前に

効率的な AP の参加機能をサポートするには、Cisco Wireless リリースのバージョンは 8.8 以降である必要があります。

ステップ 1 [Management] > [Software Update] に移動します。

ステップ 2 [効率的な参加（Efficient Join）] オプションを有効にし、[適用（Apply）] ボタンをクリックします。

[効率的な参加（Efficient Join）] 機能を有効または無効にするには、次のコマンドを使用します。デフォルトでは、この機能は有効です。

```
(Cisco Controller) > config flexconnect group default-flexgroup efficient-join {enable | disable}
```

AP の効率的な参加のステータスを確認

ME での AP の効率的な参加機能のステータスを確認するには、次の **show** コマンドを使用します。

```
(Cisco Controller) > show flexconnect group detail default-flexgroup
```

ダウンロードの進捗状況を確認するには、次 **show** コマンドを使用します。

```
(Cisco Controller) > show ap image all
```

```
(Cisco Controller) > show flexconnect efficient-upgrade aps
```

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。

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) 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。次回のソフトウェア アップデート時に、これらのパラメータを再度入力する必要はありません。

ステップ 7 [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中止できます。

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（130 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中止できます。

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 サーバには、マスター AP 上にあるものと同じCisco Mobility Express ソフトウェア バンドルか、Cisco.com 上の最新のソフトウェア バンドルのいずれかが常に存在してい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 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 パスを入力します。

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中止できます。

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 （130 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中止できます。

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、マスター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 [IP Address (Ipv4)/Name] フィールドに、SFTP サーバの IP アドレスまたはドメイン名を入力します。

ステップ 5 [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 6 [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 7 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 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、[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 9 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 10 [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 11 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 （130 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中止できます。

ステップ 12 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

- マスター 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 アカウントの 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、更新が中止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中止できます。

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中止できます。

設定管理

設定管理の拡張機能

リリース 8.10 では、次の設定管理の拡張機能を使用できるようになりました。

- コンフィギュレーション ファイルのダウンロードのスケジューリング：リリース 8.10 では、コンフィギュレーション ファイルのダウンロードをスケジュールできます。1 回限りのダウンロードまたは定期的なダウンロードのスケジュールを設定できます。

  リリース 8.10 より前では、コンフィギュレーション ファイルの即時ダウンロードがサポートされていました。

この拡張機能には、次のオプションがあります。

- **1回限りのダウンロード**：コンフィギュレーション ファイルをダウンロードする絶対時間を設定できます。この設定は再起動後も保持されます。
- **定期的ダウンロード**：間隔（時間単位、週単位、月単位）を指定し、コンフィギュレーション ファイルの定期的ダウンロードをスケジュールできます。

- FQDN をサーバアドレスのオプションとして使用：リリース 8.10 より前では、即時ダウンロード機能を使用して、IP アドレスのみをサーバアドレスとして設定できました。リリース 8.10 では、FQDN をサーバアドレスとして設定し、コンフィギュレーション ファイルをダウンロードすることも可能です。
- コンフィギュレーション ファイルのダウンロード後にコントローラを再起動：リリース 8.10 より前は、コンフィギュレーション ファイルをダウンロードして ME に展開した後、ユーザが ME を再起動して新しい設定を有効にする必要がありました。ME の起動が完了するのに長い時間を要するため、ネットワークのダウンタイムが増加します。リリース 8.10 では、完全な ME プラットフォームを再起動する代わりに、ME 上で実行中のコントローラサービスのみが再起動されます。
- エラー発生時に以前の設定にロールバック：新しいコンフィギュレーション ファイルのダウンロードや展開プロセスで何らかのエラーが発生した場合、システムが自動的に以前のコンフィギュレーション ファイルにロールバックします。

注意事項および制約事項

- 1 つのダウンロードポリシーのみを設定すると、ポリシーをさらに強化できます。
- 設定データタイプに限定してダウンロードをスケジュールできます。
- 手動で設定したシステム時刻は再起動後に経過しないため、ダウンロードポリシーを設定する際に NTP を有効にすることをお勧めします。

設定の更新（GUI）

ステップ 1 Cisco Mobility Express コントローラの Web インターフェイスから、**[Advanced]** > **[Controller Tools]** を選択します。

ステップ 2 [Configuration Management] タブをクリックします。

ステップ 3 [Direction] ドロップダウンリストから、設定ファイルの [Upload] または [Download] を選択します。

- アップロード（Upload）：外部ソースからコントローラに設定を転送します。
- ダウンロード（Download）：コントローラから外部ソースに設定を転送します。

ステップ 4 [**Transfer Mode**] 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。

- FTP
- HTTP
- SFTP
- TFTP

ステップ 5 [IP Address(IPv4)/FQDN] ボックスに、サーバの完全修飾ドメイン名の IPv4 アドレスを入力します。

ステップ 6 [Port Number] ボックスで、ポート番号を指定します。

ステップ 7 [File Path] ボックスに、設定ファイルのパスを入力します。

（注） パスとファイル名には、\、:、*、?の文字は使用できません。また、"、<、>、|は、パスとファイル名には使用できません。スラッシュ「/」は、パス区切り記号として使用します。

ステップ 8 [File Name] ボックスに、設定ファイル名を入力します。

ステップ 9 ユーザ名とパスワードを指定します。

ステップ 10 コンフィギュレーション ファイルのダウンロードをスケジュールするには、[Schedule Update] を有効に設定します。

ステップ 11 コンフィギュレーション ファイルのダウンロードのスケジューリングを有効にするには、[Active] を有効に設定します。

ステップ 12 コンフィギュレーション ファイルのダウンロード頻度を指定します。

ステップ 13 コンフィギュレーション ファイルをダウンロードする日時を指定します。

ステップ 14 [Schedule Window] ボックスには、転送スケジュールの間隔を設定します。有効な範囲は 5 ～ 180 分です。

ステップ 15 [Apply] をクリックします。

設定の更新（CLI）

ステップ 1 次のコマンドを入力して、新しいダウンロードポリシーを作成するか、またはコンフィギュレーションファイルをダウンロードするために既存のポリシーを削除します。

transfer schedule {**create** | **delete**} *policy-name*

ステップ 2 次のコマンドを入力して、ダウンロードポリシーをアクティブ化または非アクティブ化します。

transfer schedule {**start** | **stop**} *policy-name*

ステップ 3 次のコマンドを入力して、特定のプロファイルに対して転送ダウンロード関連の各種パラメータを設定します。

transfer schedule parameter *policy-name*

次のパラメータオプションを使用できます。

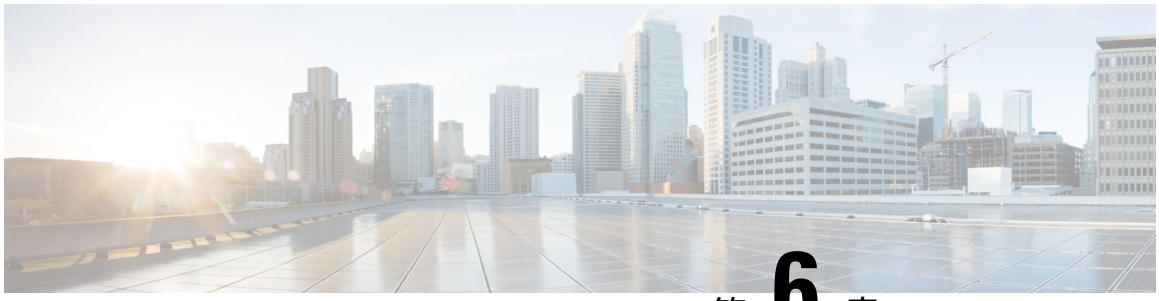
パラメータ	説明
datatype	ファイルタイプを設定
direction	スケジュールポリシーの方向を設定
filename	サーバ上のファイル名を設定
mode	転送モードを設定
password	サーバのログインパスワードを設定
path	サーバ上のファイルパスを設定
port	デフォルトのサーバポートを変更
serverIP	サーバの IP アドレスまたは FQDN を設定
tftpMaxRetries	許可される TFTP パケットの最大再試行回数。有効な範囲は 1 ～ 254 です。
tftpPktTimeout	TFTP パケットのタイムアウト（秒単位）。有効な範囲は 1 ～ 254 です。
username	サーバのログインユーザ名を設定
window	転送スケジュールの間隔を設定
frequency	ダウンロードポリシーの頻度を設定。時間単位、日単位、週単位、月単位で設定できます。

ステップ 4 次のコマンドを入力して、スケジュール済みポリシーの概要（ポリシー名、データタイプ、スケジュールステータスなど）を表示します。

show transfer-schedule summary

ステップ 5 次のコマンドを入力して、ダウンロードポリシーの詳細情報を表示します。

show transfer-schedule detailed *policy-name*



第 6 章

メッシュおよびFlex+ブリッジモードの管理

- Cisco Wave 2 屋内アクセスポイントに搭載されているメッシュ機能について （83 ページ）
- 制限とガイドライン （83 ページ）
- Mobility Express Day 0 設定の Flex + ブリッジモードについて （84 ページ）
- Mobility Express の Flex + ブリッジモードに関する制限事項とガイドライン （84 ページ）
- ルートアクセスポイントでの Day 0 Flex + ブリッジの設定（GUI） （85 ページ）
- ルートアクセスポイントでの Day 0 Flex + ブリッジの設定（CLI） （86 ページ）
- ルートアクセスポイントでのソフトウェアのアップグレード（GUI） （86 ページ）
- 複数の MAC アドレスのインポート（GUI） （87 ページ）
- ブリッジモードへのマッピングの設定（GUI） （87 ページ）
- FlexConnect グループの設定（CLI） （88 ページ）
- WLAN-VLAN マッピング（CLI）による FlexConnect グループの の設定 （89 ページ）
- グローバルメッシュ設定のエキスパートビューの有効化（GUI） （89 ページ）
- アクセスポイントでのメッシュの設定（GUI） （90 ページ）
- トラブルシューティング （90 ページ）

CiscoWave2屋内アクセスポイントに搭載されているメッシュ機能について

AP の取り付けおよび電源供給を除き、構造を変更しないでワイヤレスカバレッジを提供します。

制限とガイドライン

- 旧型の屋内 AP の一部は、メッシュネットワークをサポートしていません。

（注） サポートされていない AP の CLI モードには、「**無線 MAC が不適切または連続していないため、この AP はメッシュモードをサポートしていません（This AP does not support Mesh mode due to misaligned or non-contiguous radio MAC）**」というメッセージが表示されます。

Mobility Express Day 0 設定の Flex + ブリッジモードについて

この機能により、Mobility Express にメッシュサポートが追加され、屋内および屋外 AP の Flex + ブリッジモードに対応します。メッシュ AP を使用する利点は、メッシュ AP がコントローラの役割を果たし、別のコントローラが不要になるため、ネットワークのセットアップコストが削減されることです。

ME に搭載されているメッシュ機能は、デフォルトの FlexConnect グループのみをサポートします。FlexConnect グループを追加作成することはできません。

このリリースでは、ME GUI を使用して、MAC アドレスを CSV ファイルフォーマットで一括インポートできます。

Mobility Express の Flex + ブリッジモードに関する制限事項とガイドライン

- AP タイプの Mobility Express モードは、MAP ロールを持つ外部 AP ではサポートされていないため、MAP が無応答状態になるのを防ぐことができます。
- サポートされる AP は、次のとおりです。
  - **RAP-ME**：Cisco AireOS 1542、1562、1815s、3802s Ap
  - **MAP**: Cisco AireOS 1542、1562、1815s、3802s AP
  - **MAP の背後にある FlexConnect AP**：シスコの屋内および屋外用アクセスポイント

ルートアクセスポイントでの Day 0 Flex + ブリッジの設定（GUI）

ステップ 1 選択した RAP の電源を入れます。

ステップ 2 Wi-Fi 対応 PC で **CiscoAirProvision** SSID に接続します。

デフォルトのパスワード「password」を入力します。

（注） **CiscoAirProvision** SSID は 2.4GHz バンドでブロードキャストされます。

ステップ 3 ブラウザで Web アドレス **http://192.168.1.1** を開きます。

このページは、初期設定ウィザードにリダイレクトされます。

ステップ 4 次のパラメータを指定して、[Start] をクリックし、コントローラで管理者アカウントを作成します。

1. 管理者ユーザ名を入力します。最大で 24 文字の ASCII 文字を指定できます。
2. パスワードを入力します。最大で 24 文字の ASCII 文字を指定できます。

   パスワードを入力するときには、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の文字が含まれている必要があります。
   - 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、関連した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 $ を使用することもできません。

ステップ 5 各値を指定して、コントローラをセットアップします。

[Set Up Your Controller] 画面では、チェックリストを使用して、『*Cisco Mobility Express* 導入ガイド』の「Over-the-Air セットアップウィザードを使用した Mobility Express の設定」に記載されたステップ 4 の手順に従います。

[Mesh] オプションをスライドさせて [Enable] にします。

（注） メッシュを有効にすると、AP は Flex + ブリッジモードに設定されます。無効にすると、AP は FlexConnect モードに設定されます。

ステップ 6 GUI を使用して AP を起動すると、Mobility Express が設定されます。

ルートアクセスポイントでの Day 0 Flex + ブリッジの設定（CLI）

ステップ 1 選択した RAP の電源を入れます。

ステップ 2 プロンプトが表示されたら、次のパラメータを入力します。

1. [ユーザ名（Username）]
2. パスワード
3. システム名
4. 国コード（Country Code）

ステップ 3 Flex + ブリッジモードで RAP を設定します。

「Set the internal AP to Flex+Bridge mode」プロンプトで 「Yes」 と入力します。

（注） 「No」と入力すると、AP は FlexConnect モードで以前の Mobility Express イメージをロードします。デフォルトは [いいえ（No）] です。

ルートアクセスポイントでのソフトウェアのアップグレード（GUI）

ステップ 1 **[Management]** > **[Software Update]** を選択し、[Software Update] ページを開きます。

ステップ 2 AP タイプの自動変換オプションを無効にします。

ステップ 3 使用されている MAP と RAP が同じモデルでない場合は、[Efficient Join] を無効にします。

ステップ 4 [Apply] をクリックします。

ステップ 5 [Transfer Mode] ドロップダウンリストから、[TFTP] または [FTP] モードを選択します。

ステップ 6 [IP Address]（IPv4）フィールドにサーバの IP アドレスを入力します。

ステップ 7 [File Path] フィールドに、ソフトウェアファイルの TFTP/SFTP サーバディレクトリパスを入力します。

ステップ 8 次の 2 つのアップデートオプションのいずれかを選択します。

- ソフトウェアをすぐに更新するには、[Update] をクリックします。
- アップデートを実行するスケジュールを設定することも可能です。

1. [Schedule Update] を有効にします。

2. [Set Update Time] フィールドで日付と時刻を選択します。

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、手動でコントローラを再起動できます。アップグレード後に、**[Advanced]** > **[Controller Tools]** を選択し、[Restart Controller] をクリックします。

複数の MAC アドレスのインポート（GUI）

ステップ 1 **[Wireless]** > **[WLAN Users]** を選択して、[WLAN Users] ページを開きます。

ステップ 2 [LOCAL MAC Addresses] タブを選択します。

ステップ 3 [Import] をクリックして、CSV ファイルをインポートします。

[Import Mac ID File] ウィンドウが表示されます。

ステップ 4 [Import Mac ID File] ウィンドウで、カンマ区切り値（CSV）ファイルをアップロードします。

[Choose File] ボタンをクリックして、MAC アドレスが保存されている CSV ファイルを参照し、[OK] を選択します。

（注） CSV ファイルのフォーマットが例として表示されます。

```
MAC ID,Type,WLAN ID,Description
00:73:ee:4a:31:00,b,0,MAP1562
00:42:ec:4a:5v:80,w,0, RAP1562E
```

ステップ 5 [Yes] を選択して、CSV ファイルをインポートします。

ファイルがインポートされると、サマリーが表示されます。[Click Here] オプションをクリックすると、インポートに失敗した MAC ID と失敗の原因の一覧を確認できます。

ブリッジモードへのマッピングの設定（GUI）

ステップ 1 **[Wireless Settings]** > **[Access Points]** > を選択し、[Access Points Administration] ページを開きます。

ステップ 2 対象の AP に設定されている現在のタイプを確認します。

AP が ME 対応のタイプの場合は、CAPWAP に変換します。

1. [AP] チェックボックスをオンにします。
2. [Convert TO CAPWAP] を選択して、AP を CAPWAP モードに変換します。

タイプが CAPWAP に正しく変更されたら、次の手順に進みます。

ステップ 3 AP の設定を編集するには、[AP Edit] ボタンを選択します。

[AP Edit] ダイアログが表示されたら、[Yes] を選択します。

ステップ 4 **[AutoAP (Active Controller)]** > **[General]** タブで、ドロップダウンリストから [Operating Mode] を [Bridge] に変更します。

チャネルおよび Tx 電力設定に関するメッセージが記載されたウィンドウが表示されます。[OK] をクリックします。

ステップ 5 [Radio 2 (5GHz)] タブを選択します。

1. [Channel] ドロップダウンリストから該当するチャネルを選択します。
2. [Transmit Power] ドロップダウンリストから該当する電力値を選択します。

ステップ 6 [Apply] をクリックします。

ステップ 7 コントローラで次のコマンドを入力して、AP がメッシュネットワークの一部であるかどうかを確認します。

show mesh ap tree

FlexConnect グループの設定（CLI）

ステップ 1 次のコマンドを入力して、FlexConnect グループの VLAN サポートを有効にします。

config flexconnect group *group-name***vlan** {**enable** | **disable**}

ステップ 2 次のコマンドを入力して、default-flexgroup のネイティブ VLAN を設定します。

config flexconnect group *group-name* **vlan native** *vlan-id*

ステップ 3 次のコマンドを入力して、FlexConnect グループで VLAN override-ap を有効にします。

config flexconnect group *group-name***vlan override-ap** {**enable** | **disable**}

```
Warning! This might result in clearing AP specific wlan-vlan mappings and vlan acl mappings.
Are you sure ? (y/n) Y
```

WLAN-VLAN マッピング（CLI）による FlexConnect グループの の設定

ステップ 1 次のコマンドを入力して、FlexConnect グループに WLAN-VLAN マッピングを作成します。

config flexconnect group *group-name* **wlan-vlan wlan** *wlan-id* {**add** | **delete**} **vlan** *vlan-id*

ステップ 2 次のコマンドを入力して、FlexConnect グループの詳細を表示します。

show flexconnect group detail *group-name*

ステップ 3 次のコマンドを入力して、Flexconnect WLAN-VLAN の詳細を表示します。

show flexconnect wlan vlan

グローバルメッシュ設定のエキスパートビューの有効化（GUI）

ステップ 1 メインページの右上にある緑色の両向き矢印アイコンを選択します。

確認ウィンドウが表示されます。[OK] をクリックします。

ステップ 2 **[Wireless Settings]** > **[Mesh]** を選択して、[Mesh settings] ページを開きます。

ステップ 3 次のタブでメッシュを設定します。

1. [General]：AireOS コントローラの設定と同様
2. [Mesh RAP Downlink backhaul]；2.4 GHz または 5 GHz でグローバル RAP バックホールを設定します。
3. [Convergence]：モードを設定します。
4. [Ethernet Bridging]：VLAN を透過的に設定します
5. [Security]：セキュリティパラメータを設定します。

ステップ 4 設定を保存します。

アクセスポイントでのメッシュの設定（GUI）

ステップ 1 **[Wireless Settings]** > **[Access Points]** を選択し、[Access Points Administration] ページを開きます。

ステップ 2 対象の AP で [Edit] オプションを選択します。

AP の設定ウィンドウが表示されます。[Mesh] タブを選択します。

ステップ 3 AP にメッシュを設定します。

ステップ 4 設定を保存します。

トラブルシューティング

この項の内容は、次のとおりです。

RAPを使用したメッシュツリーの場合、内部RAP（ME）でバックホールを無効にすると、外部RAPがMEモードになる/サイレント再起動する

このシナリオでは、MAPの背後にあるスイッチがルートブリッジとして選択されたため、RAPのいずれかに接続されているスイッチポートが、ポート転送のルートブリッジになりました。メッシュネットワークでは、メイン RAP に接続するスイッチはルートブリッジにする必要があるため、このシナリオはサポートされません。

以下では、正しくない設定を確認できます。

```
Device#show spanning-tree vlan 56

VLAN0056
  Spanning tree enabled protocol ieee
  Root ID    Priority    32824
             Address     001e.7a3f.0580
             Cost        4
             Port        37 (GigabitEthernet1/0/37)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32824  (priority 32768 sys-id-ext 56)
             Address     00cc.fc7e.b980
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  300 sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Gi1/0/1             Desg FWD 4         128.1    P2p
Gi1/0/3             Desg FWD 4         128.3    P2p
Gi1/0/13            Desg FWD 4         128.13   P2p
Gi1/0/19            Desg FWD 4         128.19   P2p
```

```
Gi1/0/21            Desg FWD 4         128.21   P2p
Gi1/0/22            Desg FWD 4         128.22   P2p
Gi1/0/23            Desg FWD 4         128.23   P2p

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------

Gi1/0/24            Desg FWD 4         128.24   P2p
Gi1/0/37            Root FWD 4         128.37   P2p ==>>> Result of incorrect default
config
Gi1/0/41            Desg FWD 4         128.41   P2p
Gi1/0/43            Desg FWD 4         128.43   P2p
Gi1/0/48            Desg FWD 4         128.48   P2p
```

上記のような場合、トポロジの変更（イーサネット ブリッジング スイッチの背後でのマップローミングなど）によって、ポートは一時的にブロックされ、ループを検出するためにリスニングモードに移行します。

以下は、このような一時ブロックの例です。

```
Device#sh spanning-tree vlan 56

VLAN0056
  Spanning tree enabled protocol ieee
  Root ID    Priority    32824
             Address     001e.7a3f.0580
             Cost        4
             Port        37 (GigabitEthernet1/0/37)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32824  (priority 32768 sys-id-ext 56)
             Address     00cc.fc7e.b980
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  300 sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Gi1/0/1             Desg FWD 4         128.1    P2p
Gi1/0/3             Desg FWD 4         128.3    P2p
Gi1/0/13            Desg FWD 4         128.13   P2p
Gi1/0/19            Desg FWD 4         128.19   P2p
Gi1/0/21            Desg FWD 4         128.21   P2p
Gi1/0/22            Desg FWD 4         128.22   P2p
Gi1/0/23            Desg FWD 4         128.23   P2p

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------

Gi1/0/24            Desg FWD 4         128.24   P2p
Gi1/0/37            Root FWD 4         128.37   P2p
Gi1/0/41            Desg FWD 4         128.41   P2p
Gi1/0/43            Altn BLK 4         128.43   P2p ===>>> Temporary block
Gi1/0/48            Desg FWD 4         128.48   P2p
```

次の例は、ポートがループを検出するためにリスニングモードになっていることを示しています。

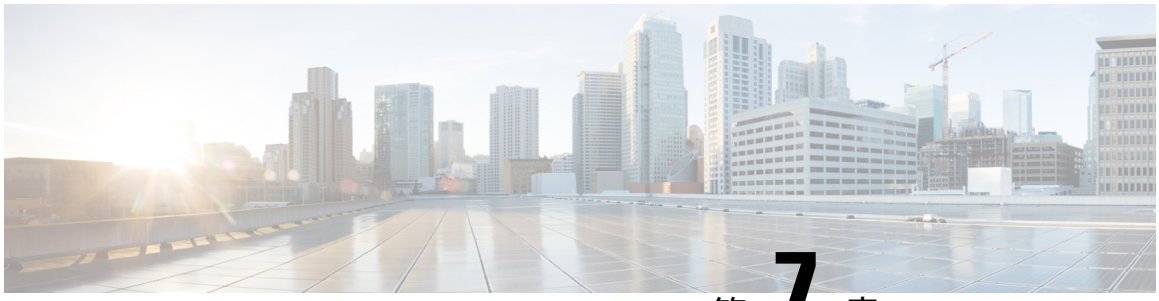
```
Device#sh spanning-tree vlan 56

VLAN0056
  Spanning tree enabled protocol ieee
  Root ID    Priority    32824
             Address     001e.7a3f.0580
             Cost        4
```

```
            Port        43 (GigabitEthernet1/0/43)
            Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32824  (priority 32768 sys-id-ext 56)
             Address     00cc.fc7e.b980
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  15  sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Gi1/0/1             Desg FWD 4         128.1    P2p
Gi1/0/3             Desg FWD 4         128.3    P2p
Gi1/0/13            Desg FWD 4         128.13   P2p
Gi1/0/19            Desg FWD 4         128.19   P2p
Gi1/0/21            Desg FWD 4         128.21   P2p
Gi1/0/22            Desg FWD 4         128.22   P2p
Gi1/0/23            Desg FWD 4         128.23   P2p

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------

Gi1/0/24            Desg FWD 4         128.24   P2p
Gi1/0/37            Desg FWD 4         128.37   P2p
Gi1/0/41            Desg FWD 4         128.41   P2p
Gi1/0/43            Root LIS 4         128.43   P2p ===>>>>>> Listen for loops
Gi1/0/48            Desg FWD 4         128.48   P2p
```

この段階では、Mobility Express の Virtual Router Redundancy Protocol（VRRP）が外部 RAP に到達していないため、ME 対応 の RAP が switchdrvr の独自のインスタンスを開始します。ポートが再び開かれると、VRRP は重複する ME を検出し、AP をただちにシャットダウンして switchdrvr をダウンさせます（サイレントリブート）。

複数のスイッチとデフォルト設定を持つトポロジでは、デバイスの MAC アドレスに基づいてルートブリッジが選択されます。これは、メッシュネットワークでは推奨されません。RAP に接続されているスイッチが、常にプライマリルートブリッジに設定されていることを確認します。確認を行うには、**spanning-tree vlan** *vlan id* **root primary** コマンドを使用します。

ルートブリッジを選択すると、RAP に接続されているすべてのポートが指定された転送ポートになり、このスイッチではブロックされません。代わりに、マップの背後にあるスイッチがルートポートになり、トポロジの変更時にポートをブロックするか、ループを検出するためにリスニングモードに移行します。



第 7 章

サービスの使用

- mDNS （93 ページ）
- Cisco Umbrella （99 ページ）
- TLS （102 ページ）

mDNS

マルチキャスト ドメイン ネーム システムについて

マルチキャスト ドメイン ネーム システム（mDNS）サービス ディスカバリは、ローカル ネットワークでサービスを通知し、検出する手段を提供します。mDNS サービス ディスカバリを使用すれば、ワイヤレス クライアントは、別のレイヤ 3 ネットワーク上でアドバタイズされた Apple プリンタや Apple TV などの Apple サービスにアクセスすることができます。mDNS は IP マルチキャスト経由で DNS クエリを実行します。また、mDNS は 0 設定 IP ネットワーキングをサポートします。通常どおり、mDNS は宛先アドレスとしてマルチキャスト IP アドレス 224.0.0.251 を使用し、UDP 宛先ポートとして 5353 を使用します。

Location Specific Services（ロケーション固有サービス）

mDNS サービス アドバタイズメントおよび mDNS クエリ パケットの処理では、ロケーション固有サービス（LSS）をサポートしています。コントローラが受信するすべての有効な mDNS サービス アドバタイズメントは、新しいエントリをサービス プロバイダーのデータベースに挿入する際に、サービス プロバイダーからのサービス アドバタイズメントに関連付けられた AP の MAC アドレスにタグ付けされます。クライアント クエリーに対する応答記述では、クエリー送信するクライアントに関連付けられた AP の MAC アドレスを使用して SP-DB のワイヤレス エントリをフィルタリングします。ワイヤレス サービス プロバイダーのデータベース エントリは、LSS がサービスに対して有効になっている場合、AP-NEIGHBOR-LIST に基づいてフィルタリングされます。LSS がサービスに対して無効になっている場合、ワイヤレス サービス プロバイダーのデータベース エントリは、そのサービスに対するワイヤレス クライアントからのクエリに応答する場合、フィルタリング対象ではありません。

LSS は、ワイヤレス サービス プロバイダーのデータベース エントリだけに適用されます。有線サービス プロバイダー デバイスのロケーションは認識されません。

LSS の状態は、ORIGIN が有線に設定されているサービスに対して有効にすることはできません。この逆も同じです。

mDNS ポリシー

ここでは、特定のサービスプロバイダーにアクセスするためのポリシーの定義方法について説明します。アクセスポリシーでは、クライアント属性、構造、およびポリシーを構成するルール要素（ルールとポリシーの評価方法）が定義されます。これは、mDNS クエリを作成したクライアントに対する mDNS 応答に、特定のサービスプロバイダーを含める必要があるかどうかを判断する際に役立ちます。

LSS が有効になっている場合、近隣するサービスプロバイダーに関する情報だけが提供されますが、MDNS ポリシーでは、さらに詳細なポリシーを定義できます。

mDNS ポリシーは、次の情報に基づいてフレーム化できます。

- ユーザ
- Role
- AP 名
- AP Location
- [AP グループ（AP Group）]

mDNS ポリシーの制限事項

MDNS ポリシーの制限事項は次のとおりです。

- LSS は、mDNS ポリシーと組み合わせて適用できません。
- ロールとユーザ情報は、ISE サーバから提供されます。
- キーワード **Any** がルールパラメータ値として使用されている場合、チェックはバイパスされます。
- ルールはサービスプロバイダーの MAC アドレスに基づいて適用されるため、サービスプロバイダーによってアドバタイズされるすべてのサービスに対してルールが評価されます。
- mDNS ポリシーは、mDNS サービスに基づくものではなく、サービスプロバイダーの MAC アドレスに基づいて適用されます。
- mDNS ポリシーは、mDNS スヌーピングが有効になっている場合にのみアクティブになります。
- MAC アドレスごとに設定できるポリシーの最大数は、5 つです。

mDNS ポリシーのクライアント属性

mDNS クエリを開始するクライアントは、クライアントのコンテキストを表す一連の属性に関連付けられます。属性として使用できるのは、ロール、ユーザ ID、関連付けられた AP 名、関

連付けられた AP の場所、および関連付けられた AP グループです。アクセスポリシールールを明確化するために、ここに列挙された属性のみを使用します。

たとえば属性が場所の場合、クライアントが異なる場所に移動すると動的に変更されます。ユーザは、論理 OR 演算を使用してこれらの属性を組み合わせてルールを定式化し、そのルールをポリシーにアタッチできます。

サービスグループには、1 つまたは複数のルールを設定できます。

mDNS AP

mDNS AP 機能により、コントローラは VLAN 上の有線サービス プロバイダーの可視性を獲得できます。すべての AP で VLAN を設定する必要があります。コントローラの VLAN の可視性は、AP が mDNS アドバタイズメントをコントローラに転送することで実現されます。

内部 AP による mDNS パケット転送を開始または停止するには、コントローラで提供される設定可能なノブを使用します。また、この設定を使用して、AP が有線側から mDNS アドバタイズメントをスヌープする必要のある VLAN を指定できます。AP がスヌープできる VLAN の最大数は 10 です。

（注） デフォルトでは、mDNS AP は VLAN をスヌーピングしないため、管理 VLAN を指定して mDNS パケットをスヌーピングする必要があります。

mDNS AP 設定は、グローバル mDNs スヌーピングを無効にしてもそれぞれの mDNS AP で保持されます。

プライオリティ MAC サポート

サービスごとに最大 50 の MAC アドレスを設定できます。これらの MAC アドレスは、プライオリティを必要とするサービス プロバイダーの MAC アドレスです。これによって、サービス プロバイダーのデータベースがフルであっても、サービス プロバイダー数が最多であるサービスから最新の非プライオリティ サービス プロバイダーを削除することによって、設定されたサービスの MAC アドレスから発信されるあらゆるサービス アドバタイズメントが学習されることが保証されます。サービスのプライオリティ MAC アドレスを設定する場合は、**ap-group** と呼ばれるオプションのパラメータがあります。これは有線サービスプロバイダーにのみ適用され、有線サービスプロバイダーのデバイスにロケーションの検知を関連付けます。クライアントの mDNS クエリがこの **ap-group** から発信されると、プライオリティ MAC アドレスおよび **ap-group** による有線エントリが検索されて、集約応答の最初に表示されます。

Origin-Based Service Discovery

発信元（有線または無線）に基づいて着信トラフィックをフィルタするようにサービスを設定できます。mDNS AP から学習されたすべてのサービスは有線として扱われます。認識元が有線である場合、LSS は無線サービスにのみ適用されるため、LSS サービスに対して有効にすることはできません。

LSS ステータスがサービスに対して有効である場合、LSS は無線サービスプロバイダーのデータベースのみに適用されるため、発信元が無線に設定されたサービスを有線に変更することはできません。発信元を有線と無線で変更した場合、変更前の発信元タイプを持つサービスプロバイダーのデータベースエントリは削除されます。

マルチキャスト DNS の設定の制限

- IPv6 を介した mDNS はサポートされません。
- ローカル側で切り替えられた WLAN およびメッシュ アクセス ポイントでは、FlexConnect モードのアクセス ポイントで mDNS はサポートされていません。
- mDNS はリモート LAN ではサポートされません。
- サードパーティの mDNS サーバまたはアプリケーションは mDNS 機能を使用するコントローラではサポートされていません。サードパーティのサーバまたはアプリケーションによってアドバタイズされるデバイスは、コントローラで mDNS のサービスまたはデバイス テーブルに正しく入力されません。
- レイヤ 2 ネットワークで Apple のサーバとクライアントが同じサブネット内に存在する場合、コントローラでの mDNS スヌーピングは不要です。ただし、これはスイッチング ネットワークの動作に依存します。使用しているスイッチが mDNS スヌーピングと想定どおりに連動しない場合は、コントローラで mDNS を有効にする必要があります。
- ビデオは、WMM が有効な状態の Apple iOS 6 ではサポートされていません。
- mDNS AP は同じサービスまたは VLAN に対して同じトラフィックを複製することはできません。
- LSS フィルタリングはワイヤレス サービスのみに制限されます。
- LSS、mDNS AP、プライオリティ MAC アドレスおよび送信元ベースの検出機能は、コントローラの GUI を使用して設定できません。
- mDNS AP 機能は CAPWAP V6 ではサポートされません。
- mDNS のユーザ プロファイル モビリティは、ゲスト アンカーではサポートされません。
- iPad、iPhone などの Apple デバイスは、Bluetooth を使用して Apple TV を検出できます。このため、Apple TV がエンド ユーザに表示されることがあります。

マルチキャスト DNS の設定

ステップ 1 次の手順に従って、グローバル mDNS パラメータおよびマスター サービス データベースを設定します。

a) [Switch to Expert View] アイコンをクリックします。エキスパート ビューに切り替えるかどうかを確認するメッセージが表示されます。[Yes] をクリックします。

b) [Services] > [mDNS] を選択します。

c) [mDNS Global Snooping] トグル ボタンを使用して、mDNS パケットのスヌーピングを有効または無効にします。
d) 分単位で mDNS クエリー間隔を入力します。クエリー間隔はコントローラがサービスを検索する頻度です。デフォルトは 15 分です。
e) [Add VLAN Id] ボタンをクリックして内部 AP スヌーピング用の VLAN のリストを追加します。

（注）
- ME の GUI から追加された VLAN は、すべての AP（内部および外部）に設定されます。**config mdns ap vlan add vlan-id ap-name** コマンドを実行するだけで、個々の AP VLAN を設定できます。
- GUI の [mDNS VLAN Mapping] テーブルには、内部 AP に設定されている VLAN のみが表示されます。**config mdns ap vlan add vlan-id ap-name** コマンドを実行するだけで、外部 AP に具体的に VLAN を設定できるので、**show ap summary** コマンドを実行すれば、すべての AP（内部と外部の両方）に追加された VLAN を表示できます。外部 AP に VLAN が設定されていても、GUI には表示されません。

f) 次のタブで詳細を入力します。

1. [Master Services Database]：マスター データベースに記載されているサービスを表示します。コントローラは、マスター サービス データベースで mDNS サービスが利用できる場合にのみ、このサービスのアドバタイズメントをスヌーピングおよび学習します。コントローラは、最大 64 のサービスをスヌープおよび学習できます。
   - [Add Service] ボタンをクリックしてマスター データベースに新しいサービスを追加します。
   - [Add/Edit mDNS Service] ウィンドウで、[Service Name]、[Service String]、[Query Status]、[Location Services]、および [Origin] を指定します。
   - [Update] をクリックします。
2. [mDNS Profiles]：mDNS プロファイルのリストを表示します。
   - [Add Profile] ボタンをクリックして新しいプロファイルを追加します。
   - [Add/Edit mDNS] ウィンドウで、後で WLAN にマッピングする可能性があるプロファイル名を入力します。
3. [Domain Names]：ドメイン名を表示し、検出されたリストからドメイン名を追加します。
4. [mDNS Browser]：実行している mDNS サービスの数を表示します。

g) [Apply] をクリックします。

ステップ 2 次の手順に従って、WLAN に mDNS プロファイルをマッピングします。

a) [Wireless Settings] > [WLANs] の順に選択します。
b) [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。
c) [Add new WLAN] ウィンドウで [Advanced] タブを選択します。
d) [mDNS] トグル ボタンを使用して、mDNS を有効または無効にします。
e) [mDNS Profile] ドロップダウン リストから、プロファイルを選択します。

f) [Passive Client] トグル ボタンを使用してパッシブ クライアントを有効にします。[Services] > [Media Stream] で [Global Multicast] が有効になっていることを確認してください。パッシブ クライアントは [Global Multicast] が無効になっていると機能しません。
g) [Multicast IP] アドレスを入力します。
h) [Multicast Direct] トグルを使用してマルチキャスト ダイレクトを有効にします。
i) [Apply] をクリックします。

（注） ワイヤレスコントローラは、次の場合にVLAN経由で学習した有線デバイス（Apple TV など）からサービスをアドバタイズします。

- [WLAN Advanced] オプションで mDNS スヌーピングが有効になっている。
- インターフェイスまたは WLAN で mDNS プロファイルが有効になっている。

mDNS ポリシーの設定

次の手順に従って、mDNS ポリシーを設定します。

a) [Switch to Expert View] アイコンをクリックします。エキスパート ビューに切り替えるかどうかを確認するメッセージが表示されます。[Yes] をクリックします。
b) [Services] > [mDNS] を選択します。
c) [mDNS Global Snooping] トグル ボタンを使用して、mDNS パケットのスヌーピングを有効または無効にします。
d) [mDNS Policy] トグルボタンを使用して、mDNS ポリシーをそれぞれ有効または無効にします。
e) 分単位で mDNS クエリー間隔を入力します。クエリー間隔はコントローラがサービスを検索する頻度です。デフォルトは 15 分です。
f) [mDNS Policy] タブをクリックします。
mDNS ポリシー数が表示されます。
g) [Add mDNS Policy] ボタンをクリックします。
[Add mDNS Policy] ウィンドウで、最初に mDNS サービスグループを追加する必要があります。

1. [DNS Service Group Name] と [Description] を入力します。
2. [Add Service Instance] ボタンをクリックします。[Add Service Instance] ウィンドウが表示されます。サービスインスタンスを追加するには、次の詳細情報を入力します。
   - **Mac Address**
   - **Name**
   - [Location Type]：AP グループ、AP 名、または AP ロケーションでロケーションタイプを選択します。
   - [Location]：選択したロケーションタイプに基づきます。
3. [Apply] をクリックします。

[mDNS Policy] ウィンドウに作成されたサービスインスタンスが表示されます。

h) [Profile Name] を入力して、[Apply] をクリックします。

Cisco Umbrella

Cisco Mobility Express に搭載された Cisco Umbrella の概要

Cisco Umbrellaプラットフォームは、クラウドで提供されるネットワークセキュリティソリューションです。ドメインネームシステム（DNS）レベルでは、マルウェアや侵害からデバイスを保護するのに役立つリアルタイムの洞察を提供します。Cisco Mobility Express リリース 8.8 以降では、Cisco Umbrella マッピングは WLAN レベルでのみサポートされます。

Cisco Umbrella は、Cisco Mobiliry Express で次のように動作します。

- ワイヤレスクライアントがワイヤレスコントローラに接続すると、インターネットへのトラフィックを開始するときに DNS クエリを送信します。Cisco Umbrella は、DNS トラフィックを透過的に代行受信し、DNS クエリを Cisco Umbrella クラウドサーバにリダイレクトします。
- DNS クエリの完全修飾ドメイン名（FQDN）に基づくセキュリティポリシーは、Cisco Umbrella クラウドサーバで定義されます。
- Cisco Umbrella は、DNS クエリの FQDN に基づいて次のいずれかの応答を返します。
  - 悪意のある FQDN：Cisco Umbrella がブロックしたページの IP を対応するクライアントに返します。
  - 安全な FQDN：宛先 IP アドレスを返します。

Cisco Mobility Express に搭載された Cisco Umbrella のサポート内容

- 最大 10 個の異なる Cisco Umbrella プロファイルがサポートされます。各プロファイルには、固有のデバイス ID が割り当てられます。
- Cisco Umbrella プロファイルやデバイス ID のワイヤレスエンティティへのマッピングについては、WLAN レベルのマッピングのみがサポートされます。
- AP へのデバイス ID のプロビジョニングについては、AP が DNS パケットをスヌーピングし、EDNS タグを適用します。
- 強制や無視オープンモードがサポートされます。
- 新規の DHCP-6 オーバーライドオプションは、WLAN レベルでサポートされます。

制限事項

Cisco Umbrella は、次では機能しません。

- Cisco Umbrella は、次では機能しません。
  - Cisco IOS AP
  - ローカル認証
  - IPv6 アドレス
-
- アプリケーションまたはホストが、DNS を使用する代わりに IP アドレスを直接使用してドメイン名をクエリしている場合。
- クライアントが Web プロキシに接続されていて、サーバ アドレスを解決するための DNS クエリを送信しない場合。
- ワークグループブリッジ（WGB）の背後にある有線ゲストとクライアント。
- 仮想ワイヤレス LAN コントローラ（WLC）
- WLAN などのワイヤレスエンティティで、設定によるワイヤレス Cisco Umbrella プロファイルの適用が、デバイスの登録が成功したかどうかによって決まる場合。
- Cisco Umbrella クラウドが 2 つの IPv4 アドレスを提供している場合。WLC/AP では、最初に設定されたサーバアドレスが使用されます。サーバ間でロードバランシングは行われません。

Cisco Mobility Express での Cisco Umbrella の設定（GUI）

次の手順を実行して、Cisco Mobility Express で Cisco Umbrella を設定します。

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 [Switch to Expert View] アイコンをクリックします。
エキスパート ビューに切り替えるかどうかを確認するメッセージが表示されます。[OK] をクリックします。

ステップ 2 [Services] > [Umbrella] を選択します。

ステップ 3 [Umbrella Global Status] トグルボタンを使用して、Umbrella ステータスをそれぞれ有効または無効にします。

ステップ 4 Cisco Umbrella から取得した **Umbrella API トークン**を入力します。

ステップ 5 [Apply] をクリックして Cisco Umbrella を有効にします。

ステップ 6 [Add Profile] をクリックして新しいプロファイルを作成します。

[Add Profile Name] ウィンドウが表示されます。

ステップ 7 [Profile Name] を入力して、[Apply] をクリックします。

新しいプロファイルが作成されます。

ステップ 8 次の手順に従って、WLAN に Cisco Umbrella プロファイルをマッピングします。

a) [Wireless Settings] > [WLANs] を選択します。
b) [Add new WLAN/RLAN] をクリックします。[Add new WLAN/RLAN] ウィンドウが表示されます。
c) [Add new WLAN] ウィンドウで [Advanced] タブを選択します。
d) [Umbrella Profile] ドロップダウンリストから、プロファイルを選択します。
e) [Umbrellaモード] ドロップダウンリストで、[Ignore] または [強制（Forced）] を選択します。
f) [Umbrella DHCP Override] トグルボタンを使用して、Cisco Umbrella DHCP オーバーライドを有効にします。
g) [Apply] をクリックします。

次のタスク

1. [Cisco Umbrella] ダッシュボードで、[Device Name] の下に、Cisco WLC とその ID が表示されていることを確認します。
2. ユーザ ロールの分類ルール（従業員のルールや従業員以外のルールなど）を作成します。
3. Cisco Umbrella サーバでポリシーを設定します。

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。

TLS

TLS セキュアトンネル

Transport Layer Security（TLS）はセキュア ポートと証明書交換を使用して、2 つのシステム間またはデバイス間でセキュアで信頼できるシグナリングとデータ転送を実現します。マルチサイト展開の課題を克服するために、Cisco Mobility Express は、TLS セキュアトンネルを使用して、Cisco Mobility Express から中央のデータセンターへのセキュアな接続を確立します。インバウンドトラフィックには、SSH、SNMP、Ping、HTTP、HTTPS、および TFTP が含まれ、アウトバウンドトラフィックには、SNMP、RADIUS、および TFTP が含まれます。

TLS トンネルには 2 つのコンポーネントがあります。

- TLS クライアント：Cisco Mobility Express コードに組み込まれ、マスター AP 上で実行されます。

- TLS ゲートウェイ：中央サイトで展開されて TLS トンネルを確立するための仮想マシンです。TLS ゲートウェイは、2 つのネットワークインターフェイス（パブリックネットワークとプライベートネットワーク）を備えています。

TLS クライアントの機能は次のとおりです。

- PnP でゼロタッチプロビジョニングをサポート
- TLS ゲートウェイ向け FQDN をサポート
- PSK ベースの認証
- Dead Peer Detection（DPD）
- トラフィックトンネリングの暗黙的および明示的設定
- NAT およびファイアウォール トラバーサルをサポート
- デバイスパラメータのシステム情報（シリアル番号、MAC アドレス、システム名）をサポート

TLS ゲートウェイの機能は次のとおりです。

- VMware を基盤とした仮想セキュリティソリューション
- TLS クライアントに対するダイナミック IP 割り当て：TLS ゲートウェイの 内部 DHCP サーバを使用した静的プールベースの IP 割り当て。
- デッドピア検出（DPD）と定期的なキー再生成：DPD とキー再生成間隔の設定、DPD と NAT タイムアウトの同期化。
- PSK 認証：事前共有キー（PSK）ベースの認証、複数の PSK 設定、およびゲートウェイでの PSK の暗号化ストレージ。
- 内部 DNS サーバ：DNS 解決用に設定可能な TLS クライアントの DNS サーバ。
- 接続レート制限：接続レート制限（1 秒あたり 50 接続）。
- スケール特性：インスタンスごとに 1 万トンネルのスケール制限。
- IP イベント通知：TLS クライアントトンネルの接続、切断、再接続（キー再生成）イベント時の通知（サーバ [syslog サーバ] Netconf/Restconf に通知）
- 有用性：設定 CLI、デバッグ統計情報（ゲートウェイレベルとデバイスレベル）、およびロギングをサポート。
- SSH ログイン制御：TLS ゲートウェイ VM への SSH ログインの有効化と無効化をサポート（プライベート インターフェイスのみ対象）。

Cisco Mobility Express セキュアトンネルは、次をサポートしています。

- アウトバウンド：SNMP トラップ、RADIUS（認証/アカウンティング）
- インバウンド：SNMP、SSH、Ping、HTTPS、HTTP

- TLS ゲートウェイ FQDN
- PSK ベースの認証
- インバウンドトラフィック：TFTP、SFTP、FTP
- キー再生成メカニズム
- トラフィックトンネリングの暗黙的および明示的な設定方法。暗黙的トンネリングにより、アプリケーションのトンネリングが可能になります。たとえば、SNMP トラップや RADIUS などです。また、明示的トンネリングにより、トンネリング用のホストやネットワークが追加されます。たとえば、SSH、PI/SNMP、DNAC などです。

Cisco Mobility Express に TLS セキュアトンネルを設定する際の一連の手順を以下に示します。

1. TLS ゲートウェイの展開：中央サイトで TLS ゲートウェイを展開するには、ここに記載されている手順に従います。
2. CLI の設定：詳細については、「Mobility Express コントローラのコマンド」のセクションを参照してください。
3. TLS の設定（GUI）：詳細については、「TLS トンネルの設定」を参照してください。

TLS トンネルの設定

TLS トンネルを設定するには、次の手順を実行します。

ステップ 1 [Switch to Expert View] アイコンをクリックします。
エキスパート ビューに切り替えるかどうかを確認するメッセージが表示されます。[Yes] をクリックします。

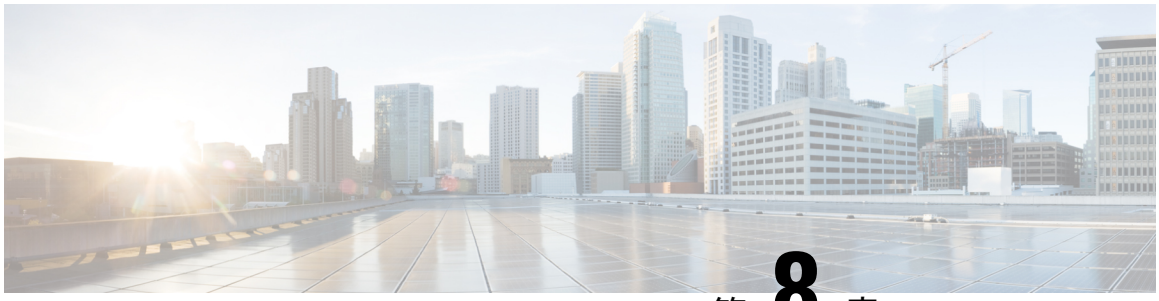
ステップ 2 [Services] > [TLS] の順に選択します。
[TLS Tunnel Settings] ページが表示されます。

ステップ 3 [TLS Tunnel] トグルボタンを使用して、TLS トンネルを有効または無効にします。

ステップ 4 [TLS Tunnel Settings] ページで、次のパラメータを設定します。

- [TLS Gateway URL/IP Address] を入力します。
- PSK ID を入力します。
- PSK キーを入力します。
- RADIUS と SNMP を有効にします。

ステップ 5 [Apply] をクリックします。



第 8 章

詳細設定の使用と操作

- SNMP の管理 （105 ページ）
- システム メッセージ ロギングの設定 （108 ページ）
- RF パラメータの最適化 （110 ページ）
- コントローラ ツールの使用 （112 ページ）
- コントローラ コンフィギュレーションの保存 （113 ページ）
- CMX クラウド プレゼンス分析の使用 （114 ページ）
- DNS アクセス制御リスト （115 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 マスター 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 を設定できます。

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 （133 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。

ローミングの最適化

ローミングの最適化について

ローミングの最適化は、遠隔地のアクセスポイントに長時間アソシエートし続けているクライアントや、接続が不安定な Wi-Fi ネットワークに接続を試みるアウトバウンド クライアントの問題を解決します。最適化されたローミングでは、クライアントのデータ パケットとデータ レートに基づいて、クライアントの関連付けを解除することができます。クライアントは、RSSI アラーム条件が満たされ、現在のデータ レートが最適化ローミング データ レートのしきい値を下回っている場合にアソシエート解除されます。データ レート オプションを無効にして、RSSI のみをクライアントのアソシエート解除に使用するようにできます。

また、最適化されたローミングは、着信クライアントの RSSI を RSSI しきい値と照合して、クライアントの RSSI が低いときのクライアント関連付けも防ぎます。このチェックで、クライアントに有効な接続がない限り、クライアントの Wi-Fi ネットワークへの接続が阻止されます。クライアントはビーコンを受信して Wi-Fi ネットワークに接続できても、信号が弱いために安定した接続をサポートできない場合がよくあります。

ローミングの最適化を使用することによって、無線に対してクライアント カバレッジ レポート間隔を設定することもできます。

最適化されたローミングは、次のシナリオに有益です。

- クライアントを積極的に切断することによってスティッキー クライアントの問題に対処する。
- データ RSSI パケットを積極的に監視する。
- 設定されたしきい値よりも RSSI が低い場合はクライアントの関連付けを解除する。

ローミングの最適化の制約事項

- 802.11a/b ネットワークを無効にするまで、ローミングの最適化の間隔を設定できません。
- BSS 遷移が 802.11v 対応クライアントに送信され、切断タイマーの期限が切れる前にそのクライアントが他の BSS に遷移していない場合、そのクライアントは強制的に切断されます。802.11v 対応クライアントのデフォルトにより、BSS 遷移が有効になります。

設定の最適化されたローミング

始める前に

- GUI を介して最適化されたローミングを設定できるようにするには、[Expert View] に切り替えていることを確認します。
- 802.11a/b ネットワークを無効にするまで、ローミングの最適化の間隔を設定できません。

ステップ 1 **[Advanced]** > **[RF Optimization]** を選択します。

[RF Optimization] ページが表示されます。

ステップ 2 [Optimized Roaming] ノブを有効にします。

最適化されたローミングを設定するためのさまざまなオプションが表示されます。これには、データ レート チェックやカバレッジ ホール検出と緩和（CHDM）から取得したデフォルトの RSSI しきい値などが含まれています。

ステップ 3 [2.4 GHz Interval] テキスト ボックスと [5.0 GHz Interval] テキスト ボックスに、アクセス ポイントがマスター AP にクライアント カバレッジ統計を報告する間隔の値を指定します。

間隔の範囲は 5 ～ 90 秒（デフォルト）です。報告間隔を小さく設定すると、ネットワークはカバレッジ レポート メッセージによって過負荷になることがあります。

クライアント カバレッジの統計情報には、データ パケット RSSI、カバレッジ ホールの検出および軽減（CHDM）の事前アラーム障害、再送信要求と現在のデータ レートが含まれます。

（注） アクセス ポイントは、次の条件に基づいてクライアント統計情報をマスター AP に送信します。

- 間隔がデフォルトで 90 秒に設定されている場合。
- カバレッジホールの検出（CHD）の赤色アラームにより、最適化されたローミングに障害が発生している間のみに間隔が設定されている場合（たとえば、10 秒）。

ステップ 4 [2.4 GHz Data Rates] スライダーと [5.0 GHz Data Rates] スライダーを操作して、クライアントのしきい値データ レートを設定します。

次のデータ レートが使用可能です。

- 2.4 GHz：1、2、5.5、6、9、11、12,、18、24、36、48、54

• 5 GHz：6、9、12、18、24、36、48、54

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 （112 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 （112 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 （113 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、マスター AP 選定プロセスが開始され、マスター AP は新たにインポートされたコントローラ コンフィギュレーションでオンラインになります。

マスター 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マスター AP の選定プロセス （128 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設定は、マスター AP の RAM 上にあります。再起動時には、揮発性 RAM は完全に消去されますが、NVRAM 上のデータは保持されます。

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

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

設定が正常に保存されたら、同一であることを伝えるメッセージが表示されます。

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ト訪問者、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。

DNS アクセス制御リスト

DNS アクセス制御リスト（ACL）機能が Cisco Mobility Express でサポートされるようになりました。これにより、ドメインベースのフィルタリングが Flex モードで実行可能になります。今後は承認なしに URL を選択して許可できるようになります。この機能により、事前認証と事後認証の両方を対象に、URL ルールで設定された FQDN に対応する複数の IP を学習できます。

この機能は次のように URL リストをサポートします。

- IPv4 および IPv6
- ワイルドカード照合：32 個 の URL ルールから、最大 20 文字のワイルドカード照合が可能。
- 事後認証に対応した許可/拒否ルール。
- FQDN を使用した ACL の設定。
- ACL 名ごとに設定可能な 32 個の URL ルール。

（注） この機能拡張により、上記の機能は事後認証にも適用できます。

コントローラは、WLAN、AP グループ、AP ごとに ACL 名で設定するか、AAA サーバから返される名前で設定します。AP データパスは DNS 要求や応答をモニタし、設定された DNS 名の IP アドレスを学習し、学習した IP アドレスのトラフィックを許可します。

ACL アクションが DNS 応答を**許可**すると、IP アドレスはスヌーピングされたリストに追加されます。認証後の ACL では、URL アクションが**拒否**の場合、AP は DNS 応答を変更し、IP アドレス 0.0.0.0 をクライアントに送信します。

Wave 2 AP でサポートされている DNS ACL には、次の 2 つのタイプがあります。

- 事前認証または Web 認証 DNS ACL：これらの ACL の URL は、クライアント認証フェーズの前に**許可**に設定されています。クライアントの URL ルールが**許可**に設定されている

場合、クライアントデータはローカルに切り替えられます。URL が一致するルールがない場合、すべてのパケットがコントローラに転送されます。デフォルトでは、クライアントデータが AP に設定されているどのルールにも一致しない場合、トラフィックはコントローラに送信されて、L3 認証の対象になります。

- 事後認証 DNS ACL：これらの ACL は、クライアント実行中に適用されます。事後認証の ACL 名は WLAN で設定できます。また、特定のクライアントの AAA サーバで設定されている ACL 名で上書きできます。ACL ルールアクションが**拒否**に設定されて URL は、DNS 応答で IP アドレスを取得しません。AP は DNS 応答を 0.0.0.0 で上書きしてからクライアントに送信します。

DNS アクセス制御リスト（ACL）の設定

事前認証用に DNS ACL を設定する手順が変更されました。DNS ACL を設定するには、次の手順に従います。

ステップ 1 [Advanced] > [Security Settings] の順に選択します。
[Security Settings] ページが表示されます。

ステップ 2 [新Add new ACL] をクリックします。
[Add ACL Rule] ウィンドウが表示されます。

ステップ 3 新しい ACL ルールを追加するには、次の手順に従います。

a) [ACL Type] で [IPv4] または [IPv6] を選択します。
b) [ACL Name] を入力します。
c) ポリシー ACL を有効または無効にするには、[Policy ACL] トグルボタンを使用します。
d) [Add IP Rule] ボタンをクリックします。
[Add/Edit IP ACLs] ウィンドウが表示されます。
e) [Add/Edit IP ACL] ウィンドウでは、[Action]、[Protocol]、[Source IP/Mask]、[Source Port]、[Dest. IP Address/Mask]、[Dest. Port]、[DSCP] などの詳細を入力し、[Apply] をクリックします。
f) [Add URL Rules] ボタンをクリックします。
[Add/Edit URL ACLs] ウィンドウが表示されます。
g) [Add/Edit URL ACL] ウィンドウで、[URL] と [Action] を入力します。

（注） IPv4 と IPv6 で同じ URL を追加できません。

h) [Apply] をクリックします。

[Security Settings] ページに、ACL タイプ、ACL 名、およびポリシー名が一覧表示されます。また、ポリシー名がマッピングされているかどうかも確認できます。

事前認証レベルで ACL を WLAN に適用

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 [WLAN Security] タブで、[Guest Network] を有効にします。

ステップ 4 [Rule Name(IPv4)] および [Rule Name(IPv6)] ドロップダウンリストで値を選択します。

ステップ 5 [Apply] をクリックします。

事後認証レベルで ACL を WLAN に適用

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 [VLAN & Firewall] タブの [Enable Firewall] フィールドで、[Yes] を選択してファイアウォールを有効にします。

ステップ 4 [WLAN Post-auth ACL] セクションで、[ACL Name(IPv4)] 、[ACL Name(IPv6)] の一方または両方を選択します。

ステップ 5 [Apply] をクリックします。

WLAN での AAA オーバーライドの設定

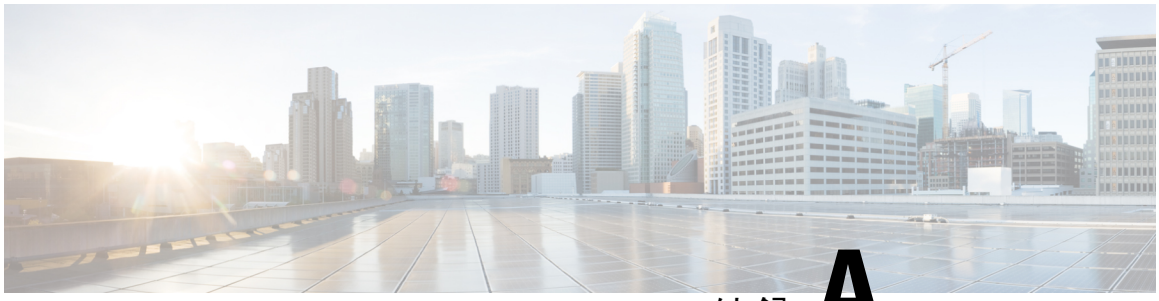
ステップ 1 現在標準ビューになっている場合は、**エキスパートビュー**に切り替えます。

ステップ 2 [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 3 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 4 [Advanced] タブを選択し、[Allow the AAA Override] トグルボタンを有効にします。

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 （119 ページ）
- CLI 初期設定ウィザードの使用 （119 ページ）
- CLI での手順 （123 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ブートし、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 create*username*{**ro** |**rw**} {**none** |**hmacmd5** |**hmacsha**} {**none** |**des | aescfb128**\\ *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**、**aescfb128** 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、マスター 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の設定は無視されます。これは、Cisco Mobility Express のマスター 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
```

コントローラ CLI コマンド

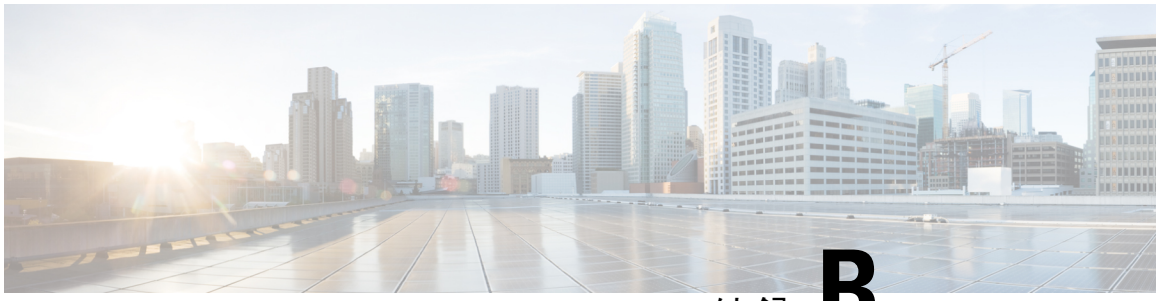
WLAN ごとに DHCP オプション 6 を有効または無効にします。

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 （127 ページ）
- Cisco Mobility Express コントローラのフェールオーバーとマスター AP の選定プロセス （128 ページ）
- アクセス ポイントへのイメージのプレダウンロード （130 ページ）
- CAPWAP の Mobility Express 変換の代替手段 （130 ページ）
- Mobility Express から CAPWAP タイプへの AP の変換 （132 ページ）
- RF パラメータの最適化設定 （133 ページ）
- アクセス ポイントでの RFID トラッキング （135 ページ）
- 関連資料 （135 ページ）
- よくある質問 （136 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	• Internet Explorer 10 以降 • Mozilla Firefox 33 以降 • Google Chrome 38 以降
Apple MAC OS	• Safari 7 以降 • Mozilla Firefox 33 以降 • Google Chrome 38 以降

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

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

Cisco Mobility Express ネットワークには、すべての AP にマスター AP として機能する能力があるわけではありません。マスター AP として機能できる AP モデルについては、サポートされているシスコのアクセス ポイント （1 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、マスター 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 つが自動的にマスターとして選定されます。新しく選定されたマスターは、元のマスターと同じ IP および設定になります。管理者にとっては、フェールオーバー発生時、元のマスターと新しく選定されたマスターに違いはありません。

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

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 にマスター AP として機能する能力があるわけではありません。マスター AP として機能できる AP モデルについては、サポートされているシスコのアクセス ポイント （1 ページ）を参照してください。

マスター AP として機能できる任意の AP を手動で強制的にマスター AP にすることができます。マスターとして機能できる AP を選択し、その AP にマスター 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. マスターとして設定する 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） マスター 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、マスター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 へのマスターのフェールオーバーを強制すると、現在のマスター AP はリブートし、新しい AP が以前のマスターの IP アドレスと設定を使用してコントローラとして継承します。以前のマスターは、リブート後、オンラインに戻り、下位 AP として新しいマスター 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。

マスター AP の選定プロセス

Cisco Mobility Express ネットワークでマスター AP がシャットダウンすると、この導入環境でマスターとして機能できる他の AP の 1 つが自動的にマスター AP に指定されます。内部のマスター自動選定プロセスにより、Cisco Mobility Express 対応の AP からマスター AP が自動的に選択されます。このプロセスは 2 つの目的で使用されます。1 つはマスター AP の障害を検出すること、もう 1 つはマスターとして機能できる AP から新しいマスター AP を指定することです。このプロセスは Virtual Router Redundancy Protocol（VRRP）に基づいており、優先順位の降順でリストしてある次のパラメータを基にアルゴリズムで次のマスター AP を決定します。

- 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 マスターとして設定された AP。
- 関連付けられているクライアント数を基準に負荷が最小である AP。
- クライアントの負荷が同程度の AP の中で、MAC アドレスが最小である AP。

VRID の設定

仮想ルータを識別するには、仮想ルータ識別子（VRID）を使用します。Cisco Wireless リリース 8.8 よりも前、Cisco Mobility Express の VRID は **01** 固定されていました。これは、00:00:5e:00:01:*VRID* に基づく固定 VRRP MAC によるものです。これは、同じ VRID を使用し

た場合の Cisco Mobility Express ネットワーク上の VRRP MAC の競合問題が原因です。Cisco Wireless リリース 8.8 以降、VRRP MAC の競合が検出された場合はマスター AP 上の VRID を変更できます。この新しい VRRP MAC は VRRP メッセージを介してスレーブに送信されます。次のコマンドは、VRID の設定や VRID または VRRP MAC の表示に利用できます。

ステップ 1 VRID を設定または変更するには、**config mob-exp vrid** *new_vrid* コマンドを使用します。

new_vrid の範囲は 1 ～ 255 で、デフォルトは 1 です。

ステップ 2 VRID を表示するには、**show mob-exp vrrp vrid** コマンドを使用します。

ステップ 3 VRRP MAC を表示するには、**show mob-exp vrrp mac** コマンドを使用します。

次のタスク

アクセス ポイントへのイメージのプレダウンロード

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

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-AP1850-K9-ME-8-1-122-0.zip* ソフトウェア ファイルをダウンロードします。

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、*CiscoAirProvison* SSID のブロードキャストを開始します。

CAPWAP イメージの変換

CAPWAP イメージの変換機能が強化されたことにより、AP が Mobility Express（ME）からイメージをダウンロードし、ME イメージを AP にフラッシュして、ビルド バージョンが同じであっても ME 対応にすることができます。

（注）

- AP のイメージ タイプがマスター AP と同じ CAPWAP である場合、新しいイメージ情報がダウンロードされます。
- AP のイメージのタイプが異なる CAPWAP イメージである場合、イメージのタイプの不一致にかかわらず、新しい ME イメージがダウンロードされます。
- ソフトウェア ダウンロードの SFTP サポート モードは、 CAPWAP COS AP を Mobility Express AP に変換するため、新しく追加されます。
- 新しい ME イメージがイメージ マスターからダウンロードされます。イメージ マスターがない場合は、TFTP または SFTPサーバ経由で新しいイメージが AP にダウンロードされます。

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 マスター 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。

DHCP オプションを介した Mobility Express AP の CAPWAP への変換

この機能では、DHCPオプション 43 を使用して、ME AP を ME モードから CAPWAP モードに変換することができますこれを行うには、最初に DHCPオプション 43 の DHCP サーバで特定の値を設定する必要があります。APがこのオプションのDHCPの値を受信すると、APのタイプは ME から CAPWAP に変更されます。

DHCP オプション 43

DHCPオプション 43 は、ワイヤレス LAN コントローラの IP アドレスを AP に提供するために使用されるオプションです。DHCPオプション 43 は、CAPWAP AP に変換することを AP に通知するために使用されます。

```
ip dhcp pool vlan177
network <wlc IP>
option 43 hex f205.0907.b10a.01
```

AP が DHCP サーバから IP の詳細をダウンロードして取得すると、16 進数の F205 で構成されるオプション 43 の値を ME-WLC IP とともに受信して AP を CAPWAP モードに変換し、AP が AireOS WLC に参加できるようになります。

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

概念、FAQ、および高度なユーザに関する情報

	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）
TPC しきい値、TPC最小値およびTPC 最大値 （これらのパラメータは、TX 電力と同じです）	帯域ごとに特定のRF プロファイル	TPC 最小値：デフォルトは-10 dB TPC 最大値：デフォルトは 30 dB	TPC しきい値： • 5 GHz の場合 -65 dB • 2.4 GHz の場合 -70 dB TPC 最小値：+7 dB TPC 最大値：デフォルトは 30 dB	TPC しきい値： • 5 GHz の場合 -60 dB • 2.4 GHz の場合 -65 dB TPC 最小値：-10 dB TPC 最大値：デフォルトは 30 dB
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）
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）

	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）
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

アクセス ポイントでの RFID トラッキング

Cisco Wireless リリース 8.8 以降、Cisco Mobility Express は、RFID で適切にタグ付けされたアセットのトラッキングをサポートしています。最大 2,000 のアクティブな RFID をトラッキングできるようになりました。

アクティブな RFID が範囲内にある場合、マスター AP はそれ自体のデータベースに RFID 関連情報を追加します。RFID トラッキングは Cisco Mobility Express ネットワーク内のマスターまたは下位を含むすべての AP 上に設定できます。RFID トラッキングは、マスター AP の CLI からのみ、Cisco Mobility Express ネットワーク内のすべての AP 上で設定できます。

RFID トラッキングの設定

ステップ 1 **config rfid {ccx | rate-limit | timeout}** コマンドを使用して、カスタム CCX マルチキャスト アドレス、メッセージ レートの制限またはタイムアウトのような RFID パラメータを設定します。

ステップ 2 RFID タグ データの収集を有効または無効にするには、**config rfid status {enable | disable}** コマンドを使用します。

ステップ 3 デフォルトの RFID 設定を表示するには、**show rfid config** コマンドを使用します。

ステップ 4 RFID タグや至近の AP のサマリーを表示するには、**show rfid summary** コマンドを使用します。

ステップ 5 RFID タグの詳細を表示するには、**show rfid detail** *mac-id* コマンドを使用します。

ステップ 6 RFID 統計を表示するには、**show rfid stats** コマンドを使用します。

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 （1 ページ）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 （132 ページ）を参照してください。

概念、FAQ、および高度なユーザに関する情報

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 （1 ページ） にマスター 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。

マスター 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。

概念、FAQ、および高度なユーザに関する情報