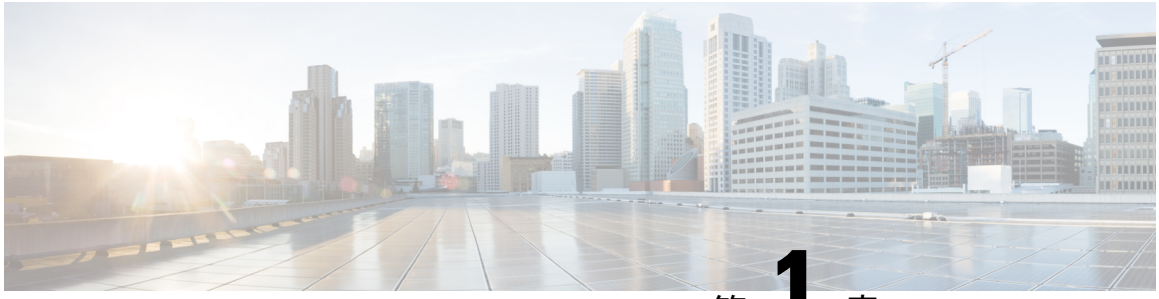
Cisco Mobility Express リリース 8.7 導入ガイド

初版：2018 年 4 月 18 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 の概要

ネットワークに接続するデバイスの数と、帯域幅を大量に消費するアプリケーションの数が増えることにより、モバイルの使用量が増加の一途をたどっています。IT スタッフの少ない、もしくは IT スタッフが存在しない中小企業はこのような予想外の成長にどう対処すればよいのでしょうか。

Cisco Mobility Express ソリューションは、中小規模のビジネスで簡単かつコスト効率よくエンタープライズクラスのワイヤレスアクセスを従業員や顧客の両方に提供できるよう特別に設計されています。これは、Cisco Aironet® 1560、1815W、1815I、1830、1850、2800、3800 シリーズ 802.11ac Wave 2 のアクセス ポイントに組み込まれている仮想ワイヤレス LAN コントローラ機能です。Cisco Mobility Express ソリューションを使用すれば、中小規模ネットワークで大企業と同じ品質のユーザ エクスペリエンスを体験できます。

Cisco Mobility Express ソリューションは、次のような特長を持つオンプレミス マネージド Wi-Fi ソリューションです。

- 最大 100 台のアクセス ポイントからなる中小規模の導入に最適です。
- 10 分以内での設定を可能にする、簡単な Over-the-Air 導入を装備しています。また、新しいサイトを起動するためにネットワーク プラグ アンド プレイを使用できます。
- 物理コントローラは不要で、シスコの高度な機能をサポートします。
- Cisco Aironet® 1560、1815W、1815I、1815M、1830、1850、2800、3800 シリーズ 802.11ac Wave 2 のアクセス ポイントでサポートされます。
- 1700、2700、3700 シリーズなどの他の Aironet® アクセス ポイントを制御できます。
- サイト サーベイの実行に使用できます。
- 次世代の Autonomous です。802.11ac Wave 2 アクセス ポイントは、従来の Autonomous モードをサポートしていません。
- 業界をリードするシスコのテクノロジーを使用すれば、中小規模ネットワークでエンタープライズグレードの Wi-Fi を利用するのに必要なデバイスの数を減らせます。ゲスト、BYOD、Cisco High Density Experience（HDX）などの高度な機能がデフォルトで有効化されているため、導入プロセスがさらに容易になります（互換性のあるアクセスポイントを

利用する場合）。CMX を追加してプレゼンスベースのサービスと詳細な分析を利用できます。

• サポートされる Cisco Aironet® アクセス ポイント （2 ページ）

サポートされる Cisco Aironet® アクセス ポイント

Cisco Mobility Express ソリューションは、次のコンポーネントで構成されます。

- マスター アクセス ポイント：仮想ワイヤレス LAN コントローラ機能を実行する Cisco Aironet® 1560、1815W、1815I、1815M、1830、1850、2800、3800 シリーズ 802.11ac Wave 2 アクセス ポイント。
- 従属アクセス ポイント：ワイヤレス LAN コントローラがアクセス ポイントを管理するのと同様にマスター アクセス ポイントによって管理される Cisco Aironet® アクセス ポイント。

（注） マスター アクセス ポイントは、ワイヤレス LAN コントローラとして機能し、従属アクセス ポイントを管理して、同時にクライアントの接続も提供します。

マスター アクセス ポイント

ワイヤレス LAN コントローラ機能をサポートし、マスター アクセス ポイントとして動作する Cisco Aironet® アクセス ポイントを、次の表に記載しています。

表 *1*：マスター アクセス ポイントとして動作可能な *Cisco Aironet*® アクセス ポイント

マスター アクセス ポイント	サポートされているモデル番号
Cisco Aironet® 1540 シリーズ	AIR-AP1540I-x-K9 AIR-AP1540D-x-K9
Cisco Aironet® 1560 シリーズ	AIR-AP1562I-x-K9 AIR-AP1562E-x-K9 AIR-AP1562D-x-K9
Cisco Aironet® 1815I シリーズ	AIR-AP1815I-x-K9C
Cisco Aironet® 1815M シリーズ	AIR-AP1815M-x-K9C
Cisco Aironet® 1815W シリーズ	AIR-AP1815W-x-K9C
Cisco Aironet® 1830 シリーズ	AIR-AP1832I-x-K9C

マスター アクセス ポイント	サポートされているモデル番号
Cisco Aironet® 1850 シリーズ	AIR-AP1852I-x-K9C AIR-AP1852E-x-K9C
Cisco Aironet® 2800 シリーズ	AIR-AP2802I-x-K9C AIR-AP2802E-x-K9C
Cisco Aironet® 3800 シリーズ	AIR-AP3802I-x-K9C AIR-AP3802E-x-K9C

（注） その他のモデル番号にある -x- は、モデルの規制ドメインを示す実際の文字のプレースホルダです。規制ドメインの詳細については、次を参照してください。 http://www.cisco.com/c/dam/assets/prod/wireless/wireless-compliance-tool/index.html

従属アクセス ポイント

従属アクセス ポイントおよびクライアントが接続するアクセス ポイントとして動作する Cisco Aironet® アクセス ポイントを、次の表に記載しています。

表 *2*：従属アクセス ポイントとして動作可能な *Cisco Aironet*® アクセス ポイント

従属アクセス ポイント	サポートされているモデル番号
Cisco Aironet® 700i シリーズ	AIR-CAP702I-x-K9
Cisco Aironet® 700w シリーズ	AIR-CAP702W-x-K9
Cisco Aironet® 1540 シリーズ	AIR-AP1540I-x-K9 AIR-AP1540D-x-K9
Cisco Aironet® 1560 シリーズ	AIR-AP1562I-x-K9 AIR-AP1562E-x-K9 AIR-AP1562D-x-K9
Cisco Aironet® 1700 シリーズ	AIR-CAP1702I-x-K9
Cisco Aironet® 1810 シリーズ	AIR-AP1810W-x-K9
Cisco Aironet® 1815I シリーズ	AIR-AP1815I-x-K9C
Cisco Aironet® 1815M シリーズ	AIR-AP1815M-x-K9C
Cisco Aironet® 1815W シリーズ	AIR-AP1815W-x-K9C
Cisco Aironet® 1830 シリーズ	AIR-AP1832I-x-K9C

従属アクセス ポイント	サポートされているモデル番号
Cisco Aironet® 1850 シリーズ	AIR-AP1852I-x-K9 AIR-AP1852E-x-K9C
Cisco Aironet® 2700 シリーズ	AIR-CAP2702I-x-K9 AIR-CAP2702E-x-K9
Cisco Aironet® 2800 シリーズ	AIR-AP2802I-x-K9C AIR-AP2802E-x-K9C
Cisco Aironet® 3700 シリーズ	AIR-CAP3702I-x-K9 AIR-CAP3702E-x-K9
Cisco Aironet® 3800 シリーズ	AIR-AP3802I-x-K9C AIR-AP3802E-x-K9C

（注） その他のモデル番号にある -x- は、モデルの規制ドメインを示す実際の文字のプレースホルダです。規制ドメインの詳細については、次を参照してください。 http://www.cisco.com/c/dam/assets/prod/wireless/wireless-compliance-tool/index.html

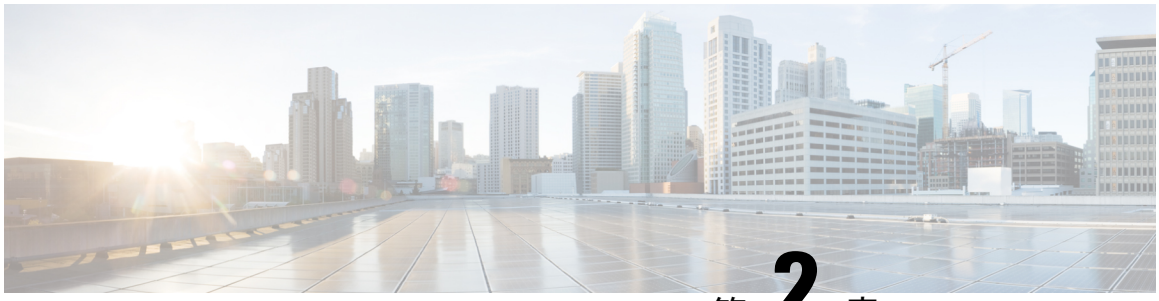
Cisco Mobility Express 規模の制限

Cisco Mobility Express は 1 つの導入で 100 アクセス ポイントと 2000 クライアントまでをサポートします。以下に、マスター アクセス ポイントごとの規模の制限を示します。

表 *3 : Cisco Mobility Express* 規模の制限

マスター アクセス ポイント	サポートされるアクセス ポイント数	サポートされるクライアント数
Cisco Aironet® 1540 シリーズ	50	1000
Cisco Aironet® 1560 シリーズ	100	2000
Cisco Aironet® 1815I シリーズ	50	1000
Cisco Aironet® 1815M シリーズ	50	1000
Cisco Aironet® 1815W シリーズ	50	1000
Cisco Aironet® 1830 シリーズ	50	1000
Cisco Aironet® 1850 シリーズ	50	1000
Cisco Aironet® 2800 シリーズ	100	2000
Cisco Aironet® 3800 シリーズ	100	2000

（注） Mobility Express ネットワークに 50 以上のアクセス ポイントがある場合、マスター AP（ワイヤレス LAN コントローラ機能を実行）は最大 20 クライアントに対応できます。この制限は、マスター AP にのみ適用され、Mobility Express ネットワークのその他のアクセス ポイントには適用されません。



第 2 章

Cisco Mobility Express の導入

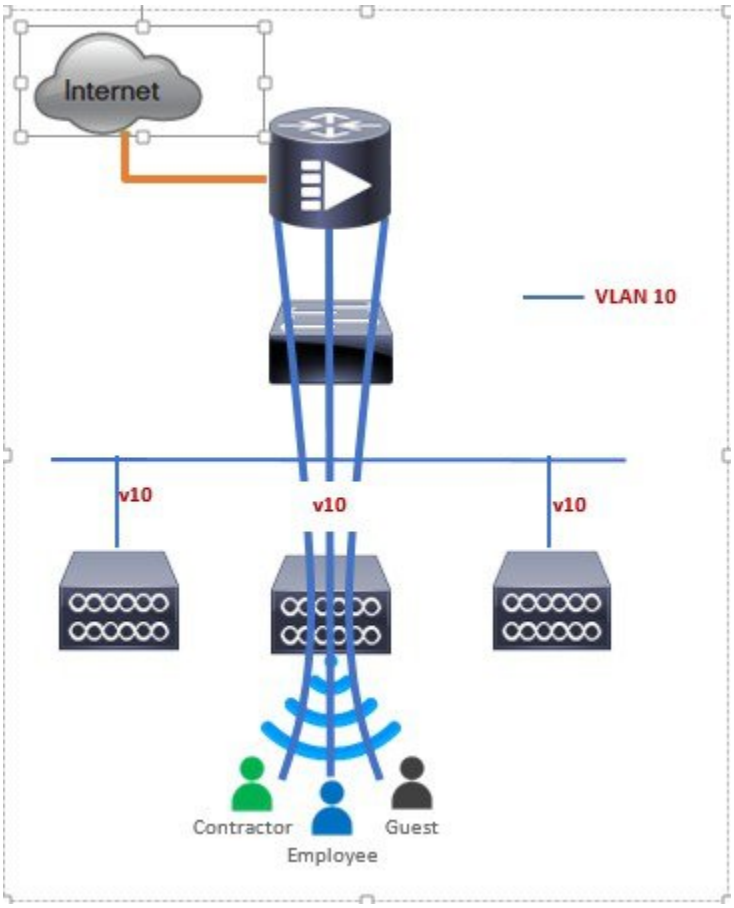
Mobility Express ソリューション導入の前提条件

1. Cisco Mobility Express ネットワークのセットアップまたは毎日の運用時に、同じネットワークにシスコの他のワイヤレス LAN コントローラ（アプライアンスも仮想も）が存在してはなりません。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 LAN 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。
2. マスター アクセス ポイントとして設定する最初のアクセス ポイントを決定します。このアクセス ポイントはワイヤレス LAN コントローラ機能をサポートしている必要があります。
3. DHCP サーバは、アクセス ポイントおよびクライアントが IP アドレスを取得できるように、ネットワーク上で使用可能である必要があります。AireOS® リリース 8.3.102.0 以降では、マスター アクセス ポイントでも同様に DHCP サーバを構成できますが、これは、主にサイト サーベイに使用されます。

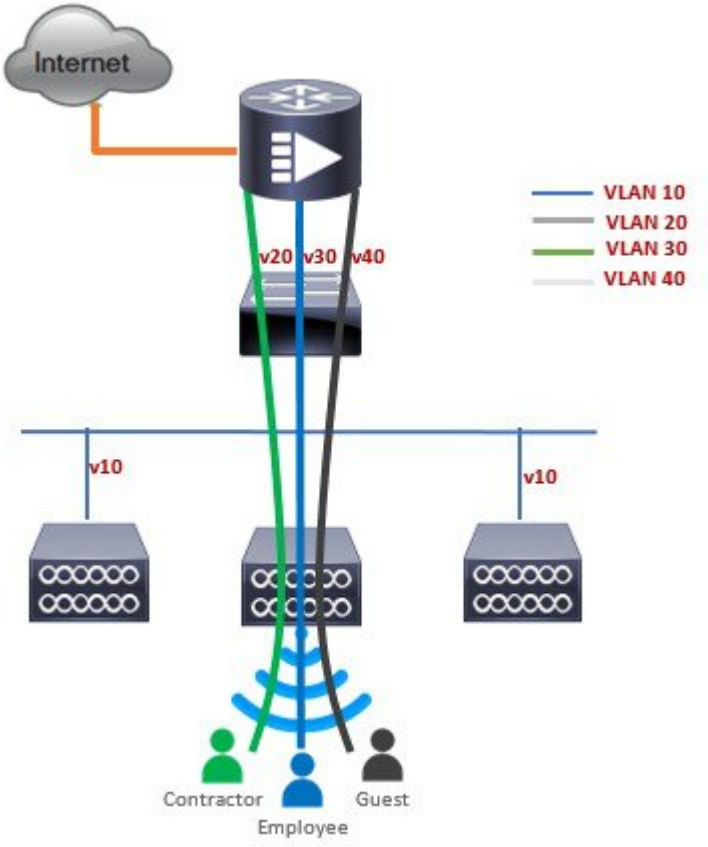
Mobility Express 対応アクセスポイントのネットワークへの接続

導入によっては、Mobility Express 対応アクセス ポイントをスイッチのアクセス ポートまたはトランク ポートに接続できます。

アクセス ポイントおよび WLAN が同じネットワーク上にある場合、Mobility Express 対応アクセス ポイントを、次に示すように、スイッチのアクセス ポートに接続できます。



Mobility Express の管理トラフィックはタグなしです。アクセス ポイントおよび WLAN がすべて異なる VLAN にある場合、Mobility Express 対応アクセス ポイントはスイッチのトランク ポートに接続し、個々の WLAN のトラフィックは個々の VLAN でローカルにスイッチングされます。下記は、異なる VLAN でアクセス ポイントと WLAN を使用した導入です。




```
interface GigabitEthernet1/0/37
description » Connected to Master AP «
switchport trunk native vlan 40
switchport trunk allowed vlan 10,20,30,40
switchport mode trunk
```

アクセス ポイントのイメージの決定

Cisco Aironet® 1540、1560、1815、1830、1850、2800、3800 シリーズのアクセス ポイントは、CAPWAP イメージ、または、アクセス ポイントで仮想ワイヤレス LAN コントローラ機能を実行できる Cisco Mobility Express イメージのどちらかに対応します。

アクセス ポイントのイメージと機能を判別するには、次の手順に従います。

手順

ステップ 1 コンソールを使用してアクセス ポイント CLI にログインし、**AP#show version** を入力し、show version の完全な出力を確認します。デフォルトのログイン クレデンシャルは、Username:cisco および Password:cisco です。

ステップ 2 ***show version*** 出力で、以下に強調表示されているような **AP イメージのタイプ**と **AP 設定**のパラメータを表示**しない**場合、AP は CAPWAP イメージを実行し、アクセス ポイントのコントローラの機能を実行する場合は Cisco Mobility Express への変換が必要なことを意味します。CAPWAP アクセス ポイントから Mobility Express に変換するには、このドキュメントの変換セクションを参照してください。

```
cisco AIR-AP1852E-UXK9 ARMv7 Processor rev 0 (v71) with 997184/525160K bytes of memory.

Processor board ID RFDP2BCR021
AP Running Image : 8.2.100.0
Primary Boot Image : 8.2.100.0
Backup Boot Image : 8.1.106.33
AP Image type : MOBILITY EXPRESS IMAGE
AP Configuration : MOBILITY EXPRESS CAPABLE
0 Gigabit Ethernet interfaces
0 802.11 Radios
Radio FW version . 1401b63d12113073a3C08aa67f0c039c0
NSS FW version : NSS.AK.1.0.c4-0Z026-E_cust C-1.24160
```

show version が、**AP Image Type: MOBILITY EXPRESS IMAGE** および **AP Configuration: NOT MOBILITY EXPRESS CAPABLE** を表示する場合は、アクセス ポイントに Cisco Mobility Express イメージがある場合でさえ、CAPWAP アクセス ポイントとして実行するように設定されていることを意味します。この場合、アクセスポイントは、コントローラの機能を実行せず、アクティブなマスター AP の障害の際はマスター選択プロセスには参加しません。

```
cisco AI R-AP1852E-UXK9 ARMv7 Processor rev 0 (v7I) with 997184/726252K bytes of memory.
 Processor board ID RFDP2BCR021
AP Running Image : 8.2.101.0
Primary Boot Image : 8.2.100.0
Backup Boot Image : 8.1.106.33
AP Image type : MOBILITY EXPRESS IMAGE
AP Configuration : NOT MOBILITY EXPRESS CAPABLE
```

この AP でコントローラの機能を実行する場合、**AP Configuration** は **MOBILITY EXPRESS CAPABLE** に変更する必要があります。AP 設定を変更するには、AP CLI で次のコマンドを実行します。 **AP#ap-type mobility-express tftp://**

アクセスポイントが再起動し、起動後にコントローラの機能を実行することができます。***show version*** の出力を再度確認して、***AP Configuration*** が ***MOBILITY EXPRESS CAPABLE*** に変更されていることを確認することができます。

show version が **AP Image Type: MOBILITY EXPRESS IMAGE** および **AP Configuration: MOBILITY EXPRESS CAPABLE** を表示する場合、アクセス ポイントには Mobility Express イメージがあり、コントローラの機能を実行できることを意味します。このシナリオでは、**show version** の出力は次のように表示されます。

```
cisco AIR-AP3802I-B-K9 ARMv7 Processor rev 1 (v7l) with 1028384/255032K bytes of memory.
Processor board ID FCW2034NXAV
AP Running Image     : 8.4.2.66
Primary Boot Image   : 8.4.2.66
Backup Boot Image    : 8.4.2.34
AP Image type : MOBILITY EXPRESS IMAGE
AP Configuration : MOBILITY EXPRESS CAPABLE
1 Multigigabit Ethernet interfaces
1 Gigabit Ethernet interfaces
2 802.11 Radios
Radio Driver version : 9.0.5.5-W8964
```

```
Radio FW version : 9.1.8.1
NSS FW version : 2.4.18
```

変換

CAPWAP を実行するアクセス ポイントを Cisco Mobility Express に変換できます。またその逆も可能です。

CAPWAP から Cisco Mobility Express へのアクセス ポイントの変換

11ac Wave 2 アクセス ポイントでの Cisco Mobility Express の対応は、異なる AireOS リリースで導入されていますが、アクセス ポイントが Mobility Express に変換される前に、アクセス ポイントの Cisco Mobility Express の機能をサポートした最小の AireOS CAPWAP イメージが必要であることに注意してください。CAPWAP から Cisco Mobility Express への変換をサポートするアクセス ポイントの最小の AireOS リリースは次のとおりです。

表 *4 : Cisco Mobility Express* をサポートする最小の *AireOS* リリース

アクセス ポイント	**CAPWAP** イメージをサポートする最小の **AireOS** リリース
Cisco Aironet® 1540 シリーズ	リリース 8.5 以降
Cisco Aironet® 1560 シリーズ	リリース 8.4 以降
Cisco Aironet® 1815I シリーズ	リリース 8.4 以降
Cisco Aironet® 1815M シリーズ	リリース 8.5 以降
Cisco Aironet® 1815W シリーズ	リリース 8.4 以降
Cisco Aironet® 1830 シリーズ	リリース 8.1 MR2 以降
Cisco Aironet® 1850 シリーズ	リリース 8.1 MR2 以降
Cisco Aironet® 2800 シリーズ	リリース 8.3 以降
Cisco Aironet® 3800 シリーズ	リリース 8.3 以降

（注） アクセス ポイントの CAPWAP イメージが Cisco Mobility Express をサポートできる最小の AireOS リリースより古い場合、アクセス ポイントは最初に最小の AireOS リリース以上を実行する WLC に参加して CAPWAP イメージをアップグレードする必要があります。AP の CAPWAP イメージをアップグレードした後、CAPWAP から Mobility Express へ AP を変換できます。

CAPWAP を実行するアクセス ポイントで Mobility Express への変換を実行するには、次の手順に従います。

手順

ステップ 1 Cisco.com から TFTP サーバへアクセス ポイントの変換イメージをダウンロードします。これは tar ファイルです。このファイルは解凍しないでください。次の表に、Cisco Wireless Release **8.7.102.0** 向けの Cisco Mobility Express ソフトウェアを示します。

表 *5:* アクセス ポイントの変換 *tar* ファイル

マスター AP としてサポートされるアクセス ポイント	Unified Wireless Network Lightweight AP ソフトウェアから Cisco Mobility Express に変換する場合にのみ使用するソフトウェア
Cisco Aironet® 1540 シリーズ	AIR-AP1540-K9-8-7-102-0.tar
Cisco Aironet® 1560 シリーズ	AIR-AP1560-K9-8-7-102-0.tar
Cisco Aironet® 1815I シリーズ	AIR-AP1815-K9-8-7-102-0.tar
Cisco Aironet® 1815M シリーズ	AIR-AP1815-K9-8-7-102-0.tar
Cisco Aironet® 1815W シリーズ	AIR-AP1815-K9-8-7-102-0.tar
Cisco Aironet® 1830 シリーズ	AIR-AP1830-K9-8-7-102-0.tar
Cisco Aironet® 1850 シリーズ	AIR-AP1850-K9-8-7-102-0.tar
Cisco Aironet® 2800 シリーズ	AIR-AP2800-K9-8-7-102-0.tar
Cisco Aironet® 3800 シリーズ	AIR-AP3800-K9-8-7-102-0.tar

ステップ 2 アクセス ポイントにログインします。

ステップ 3 アクセス ポイントの CLI で **AP#show version** を実行します。show version の出力から、**AP Image type** と **AP Configuration** を判断できます。次に変換プロセスに進みます

ケース 1：**AP Image type** が **MOBILITY EXPRESS IMAGE** で **AP configuration** が **NOT MOBILITY EXPRESS CAPABLE** の場合、次のコマンドを入力して、**AP Configuration** を **MOBILITY EXPRESS CAPABLE** に変更します。

AP#ap-type mobility-express

（注） アクセス ポイントに **AP Image type: MOBILITY EXPRESS IMAGE** があるため、新しいイメージはダウンロードされません。コマンドを実行した後、アクセスポイントが再起動します。再起動後、**AP Configuration** は **MOBILITY EXPRESS CAPABLE** に変更されます。

ケース 2：**AP Image type** と **AP Configuration** が表示されない場合は、AP が CAPWAP イメージを実行していることを意味します。変換を行うには、次のコマンドを実行します。

AP#ap-type mobility-express tftp://<TFTP Server IP>/<path to tar file>

例：

```
AP#ap-type mobility-express tftp://10.18.22.34/AIR-AP1850-K9-8.7.102.0.tar
```

```
Starting the ME image download...
It may take few minutes to finish the download.

Image downloaded, writing to flash...
do PREDOWNLOAD, part1 is active part
sh: CHECK_ME: unknown operand
Image start 0x40355008 size 0x01dae41a file size 0x01dae7ca
Key start 0x42103422 size 0x00000230
Sinature start 0x42103652 size 0x00000180
Verify returns 0
btldr rel is 16 vs 16, does not need update
part to upgrade is part2
activate part2, set BOOT to part2
AP primary version: 8.1.105.37
Archive done.
Oe as AP needs to boot up with ME image

The system is going down Now!
sent SIGTERM to all processes
sent SIGKILL to all processes

Requesting system reboot79]
[07/24/2015 18:19:43.0887] Restarting system.
[07/24/2015 18:19:43.1257] Going down for restart now
```

（注） イメージのダウンロードが完了すると、イメージがフラッシュに書き込まれ、その後再起動されます。AP が起動すると、***AP Image type*** は ***MOBILITY EXPRESS IMAGE***、***AP Configuration*** は ***MOBILITY EXPRESS CAPABLE*** になります。

ステップ 4 これがネットワークで最初のアクセス ポイントの場合は、コントローラの機能が開始され、***CiscoAirProvison*** SSID をブロードキャストします。

Cisco Mobility Express から CAPWAP へのアクセス ポイントの変換

Mobility Express イメージを実行するアクセス ポイントを CAPWAP に変換する理由は主に 2 つあります。次のとおりです。

1. Mobility Express 導入でアクセス ポイントを維持したいが、マスター AP がフェールオーバーする際に、アクセス ポイントをマスター選択プロセスには参加させたくない。
2. 1 つ以上の Mobility Express 対応アクセス ポイントをアプライアンス WLC または vWLC に移行したい。

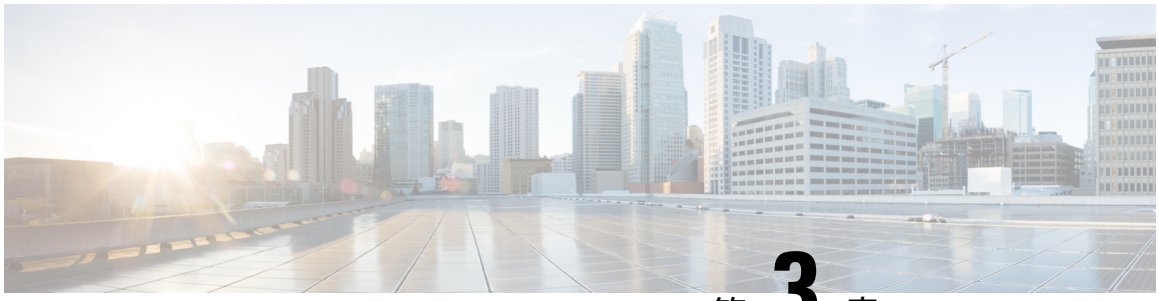
1. CAPWAP に変換する理由が上記の 1 の場合、以下の手順に従います。
    1. コンソールまたは ssh からアクセス ポイント CLI にログインし、EXEC モードにアクセスします。マスター AP を CAPWAP に変換する場合は、コンソールの接続によりコントローラ CLI にアクセスします。AP CLI を使用するには、コントローラのプロンプトで **apciscochell** と入力し、アクセス ポイント シェルにログインします。
    2. **ap#ap-type capwap** CLI を実行します。これにより、**AP Configuration** が **NOT MOBILITY EXPRESS** に変更され、アクセス ポイントはマスター選択プロセスには参加しません。

2. CAPWAP に変換する理由が上記の 2 の場合、以下の手順に従います。
    1. コンソールまたは ssh からアクセス ポイント CLI にログインし、EXEC モードにアクセスします。
    2. 次の CLI を実行します。

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

<switch_name> and <switch_ip_address> is the name and IP address respectively of the WLC
 to which the APs need to be migrate.
```

（注） 上記のコマンドでは、**AP Configuration: MOBILITY EXPRESS CAPABLE** で稼働しているアクセス ポイントがすべて **AP Configuration: NOT MOBILITY EXPRESS CAPABLE** に変換されます。このコマンドが発行されると、AP が再起動され、コントローラ（switch_ip_address）を検索して参加します。



第 3 章

Cisco Mobility Express コントローラの設定

Cisco Mobility Express コントローラは複数の方法で設定できます。使用できる方法は次のとおりです。

1. CLI セットアップ ウィザード
2. Over–the–Air セットアップ ウィザード
3. ネットワーク プラグアンドプレイ

CLI セットアップ ウィザード

CLI からのセットアップ ウィザードを使用するには、アクセス ポイントのコンソール ポートに接続する必要があります。コンソール ポートのデフォルト パラメータは、9600 ボー、8 データ ビット、1 ストップ ビット、およびパリティなしです。コンソール ポートはハードウェア フロー制御をサポートしていません。

アクセス ポイントのコンソール ポートに接続した後、アクセス ポイントを起動します。しばらくすると、アクセス ポイントは内部のコントローラ機能を開始します。

Mobility Express コントローラを設定するには、次の例で示すような手順を実行します。

```
System Name [Cisco_2c:3a:40] (31 characters max): me-wlc
Enter Country Code list (enter 'help' for a list of countries) [US]:

Configure a NTP server now? [YES][no]: no
Configure the system time now? [YES][no]: no

Note! Default NTP servers will be used

Management Interface IP Address: 40.40.40.10
Management Interface Netmask: 255.255.255.0
Management Interface Default Router: 40.40.40.1
```

```
Cleaning up Provisioning SSID
Create Management DHCP Scope? [yes][NO]: yes
DHCP Network : 40.40.40.0
DHCP Netmask : 255.255.255.0
Router IP: 40.40.40.1
Start DHCP IP address: 40.40.40.11
Stop DHCP IP address: 40.40.40.254
DomainName :
DNS Server : [OPENDNS][user DNS]
Create Employee Network? [YES][no]: YES
Employee Network Name (SSID)?: WestAutoBody-Employee
Employee VLAN Identifier? [MGMT][1-4095]: MGMT
Employee Network Security? [PSK][enterprise]: PSK
Employee PSK Passphrase (8-38 characters)?: Cisco123
Re-enter Employee PSK Passphrase: Cisco123
Create Guest Network? [yes][NO]: YES
Guest Network Name (SSID)?: WestAutoBody-Guest
Guest VLAN Identifier? [EMPLOYEE][1-4095]: EMPLOYEE
Guest Network Security? [WEB-CONSENT][psk]: WEB-CONSENT
Create Guest DHCP Scope? [yes][NO]: NO
Enable RF Parameter Optimization? [YES][no]: YES
Client Density [TYPICAL][Low][High]: TYPICAL
Traffic with Voice [NO][Yes]: Yes

Configuration correct? If yes, system will save it and reset. [yes][NO]: yes
Cleaning up Provisioning SSID
```

（注） アクセス ポイントは、バックアップした後再起動します。Cisco Mobility Express コントローラは HTTPS の自己署名証明書を使用して、ブラウザの **https://<mangement_ip_address>** から WebUI にログインします。そのため、すべてのブラウザで警告メッセージが表示され、証明書がブラウザに提示される際に例外の状態でも続行するかどうかを確認されます。このリスクを受け入れて、Mobility Express のワイヤレス LAN コントローラのログイン ページへのアクセスに進みます。

Over-the-Air セットアップ ウィザード

Over-the-Air は、箱から取り出して Mobility Express を設定するための単純で簡単な方法です。OTA プロビジョニングは、WiFi 対応のデバイス、または iOS デバイス向けには App Store、Android デバイス向けには Play Store からダウンロードできる **Cisco Wireless** を使用して実施できます。**Cisco Wireless** app は、わずか数分で Mobility Express を導入するための最小セットの設定オプションを提供します。

手順

ステップ 1 アクセス ポイントの LED が**緑色になったら**、WiFi 対応ラップトップを **CiscoAirProvision** SSID に接続します。デフォルト 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。

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

ステップ 2 Webブラウザを起動し、**http://mobilityexpress.cisco**にアクセスします。これは設定ウィザードにリダイレクトされ、Admin アカウントのページが表示されます。

ステップ 3 次のパラメータを指定し、[Start]ボタンをクリックして、コントローラでAdminアカウントを作成します。

- admin のユーザ名を入力します。最大で 24 文字の ASCII 文字です。
- パスワードを入力します。最大で 24 文字の ASCII 文字です。パスワードを入力するときは、次のように設定してください。
  - 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 $ を使用することはできません。

ステップ 4 [Set Up Your Controller] セクションで、以下を設定します。

- システム名を入力します
- ドロップダウン リストから国を選択します
- 日付と時刻は自動的に入力されますが、手動で設定することもできます
- ドロップダウン リストからタイムゾーンを選択します
- すでに存在する場合は、NTPサーバのIPアドレスを入力します。空白にすると、NTPプールが自動的に構成されます
- コントローラの管理 IP アドレスを入力します
- サブネット マスクを入力します
- デフォルト ゲートウェイを入力します

ステップ 5 外部DHCPサーバを使用している場合、[Enable DHCP Server(Management Network)]を無効にします。Mobility Expressコントローラ上の内部DHCPサーバを使用する場合、DHCPサーバの関連情報を指定します。

ステップ 6 [Next] をクリックします。

ステップ 7 [Employee Network] の下の [Create Your Wireless Network] で、以下を設定します。

- ネットワーク名を入力します
- セキュリティを WPA2 パーソナルまたは WPA2 エンタープライズとしてドロップ ダウン リストから選択します

- WPA2 パーソナルを選択した場合は、パスフレーズを入力します

ステップ 8 [RF Parameter Optimization] を有効にして、以下を設定することもできます。

- 必要に応じて、[Client Density] スライダを動かします
- [Traffic Type] から、[Data] または [Data and Voice] を選択します

ステップ 9 [Next] をクリックします。

ステップ 10 ページで設定を確認し、[Apply] ボタンをクリックします。アクセス ポイントが再起動し、起動後にコントローラ機能を実行します。

（注） アクセス ポイントが再起動し、起動後に、**https:<management_ip_address>** を使用して、ブラウザから Mobility Express コントローラ WebUI にログインします。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、すべてのブラウザで警告メッセージが表示され、証明書がブラウザに提示される際に例外の状態でも続行するかどうかを確認されます。このリスクを受け入れて、Mobility Express のワイヤレス LAN コントローラのログイン ページへのアクセスに進みます。

ネットワーク プラグアンドプレイ

はじめに

シスコのネットワーク プラグ アンド プレイのソリューションは、エンタープライズ ネットワークを持つお客様に対し、シンプルでセキュアな統合サービスを提供し、Cisco Mobility Express をプロビジョニングするために新しいサイトのロールアウトを容易にします。このソリューションでは、クラウド リダイレクション サービス、オンプレミス、またはその組み合わせを使用して、Cisco Mobility Express、シスコ ルータ、スイッチで構成されるエンタープライズ ネットワークの統合されたプロビジョニングを、ほぼゼロ タッチの導入エクスペリエンスとして提供します。

シスコのネットワーク プラグ アンド プレイ アプリケーションを使用してサイトを事前プロビジョニングし、サイトに Cisco Mobility Express 対応のアクセス ポイントを追加できます。この作業には、アクセス ポイント情報の入力と Mobility Express 対応のアクセス ポイント上で実行する仮想コントローラのコントローラ設定ファイルのアップロードが含まれます。

作業者が Cisco Mobility Express 対応のアクセス ポイントを設置して電源を入れると、DHCP、DNS またはクラウド リダイレクション サービスを使用して Cisco APIC-EM コントローラを自動検出します。自動検出プロセスが完了した後、AP は、ローカル PnP サーバからコントローラ設定ファイルをダウンロードするか、またはターゲットとする PnP サーバにリダイレクトするクラウド リダイレクション サービスと通信します。

前提条件

1. シスコのネットワーク プラグ アンド プレイを使用する APIC-EM リリース 1.4 以降は、Cisco UCS または同等のサーバに仮想マシンとしてホストされます。
2. アクセス ポイント：Cisco Mobility Express ソフトウェアを実行する Cisco 802.11ac Wave 2 アクセス ポイント。
3. コントローラ設定：ネットワーク PnP にアップロードするための Cisco Mobility Express コントローラ設定ファイル。

APIC-EM ディスカバリ オプション

1. オプション 43 を使用して DHCP サーバを設定し、Cisco Mobility Express 対応アクセス ポイントでAPIC-EMコントローラを自動検出できるようにします（クラウドリダイレクションをテストしているだけの場合はオプション 43 は必要ありません）。DHCP オプション 43 は、設定されている DHCP サーバ文字列（オプション 43 ascii 「5A1N;B2;K4;I192.168.1.123;J80」）を構成します。

（注） 192.168.1.123 は APCI-EM サーバの IP アドレスです。

2. オンプレミス PnP サーバは「pnpserver.yourlocal.domain」を使用して DNS に追加できます。（オプション 43 が設定されていないなどの理由で）DHCP ディスカバリが、APIC-EM コントローラの IP アドレスの取得に失敗した場合、シスコのプラグ アンド プレイ エージェントは、DNS ルックアップ方式を利用しようとします。DHCP サーバから返されたネットワーク ドメイン名に基づき、事前設定されたホスト名「pnpserver」を使用して、APIC-EM コントローラの完全修飾ドメイン名（FQDN）を作成します。たとえば、DHCP サーバからドメイン名「customer.com」が返された場合、シスコのプラグ アンド プレイ IOS エージェントは「pnpserver.customer.com」という FQDN を作成します。次に、この FQDN の IP アドレスを解決するために、ローカル ネーム サーバを使用します。
3. クラウド リダイレクション サービスには、インターネットへの接続と、「devicehelper.cisco.com」を解決できる有効な DNS サーバが必要です。クラウド リダイレクション サービスは Cisco Mobility Express アクセスポイントを APIC-EM にリダイレクトします。

APIC-EM/ネットワーク PnP サーバの設定

サイトの事前プロビジョニングのワークフロー

シスコのネットワーク プラグ アンド プレイによって新規サイトの事前プロビジョニングおよび計画ができます。新しいサイトを作成するときに、シスコのネットワーク プラグ アンド プレイで選択した Cisco Mobility Express コントローラ、設定ファイル、製品 ID および製品シリ

アル番号を事前プロビジョニングできます。これは、サイトが完全に機能するためにかかる時間を簡素化および迅速化します。

その他の機能や PnP 設定の詳細については、次のリンクを参照してください。
http://www.cisco.com/c/en/us/support/cloud-systems-management/one-enterprise-network-controller/products-installation-and-configuration-guides-list.html

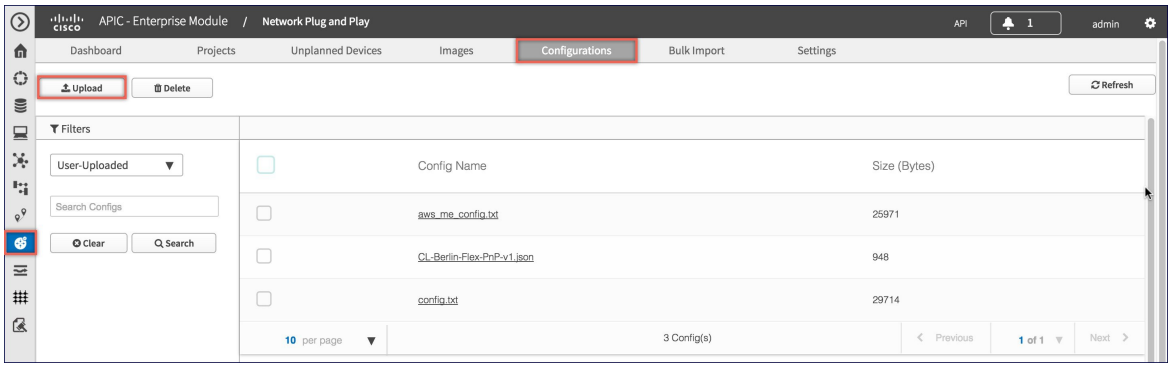
ネットワークにサイトを事前プロビジョニングするには、次の手順を実行します。

1. ネットワーク PnP に Cisco Mobility Express コントローラの設定ファイルをインポート
2. プロジェクトの作成
3. プロジェクトに Cisco Mobility Express 対応アクセス ポイントを追加しコントローラ設定を関連付ける

ネットワーク PnP への Cisco Mobility Express 設定ファイルのインポート

手順

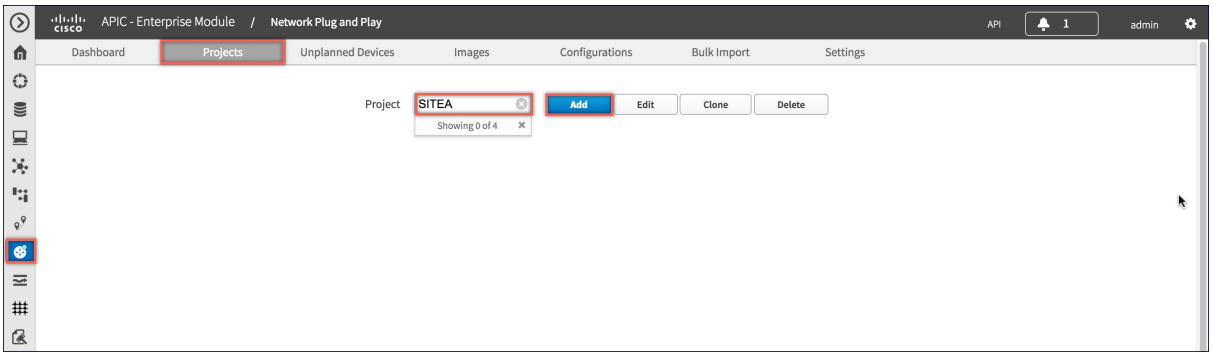
ステップ 1 APIC-EM コントローラにログインし、[Network Plug and Play] > [Configurations] に移動します。
ステップ 2 [Upload] をクリックして、コントローラ設定をアップロードします。
ステップ 3 ローカル マシンからコントローラの設定ファイルを選択します。



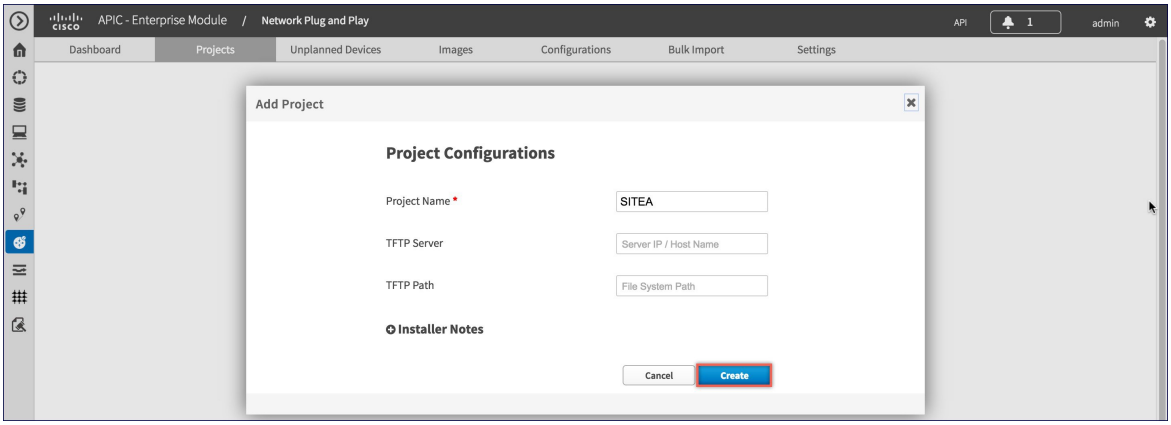
プロジェクトの作成

手順

ステップ 1 [Network Plug and Play] > [Projects] に移動します。
ステップ 2 プロジェクトの名前を入力し、[Add] ボタンをクリックします。



ステップ 3 [Create] ボタンをクリックして、プロジェクトを作成します。



プロジェクトへの Cisco Mobility Express 対応アクセス ポイントの追加とコントローラ設定の関連付け

手順

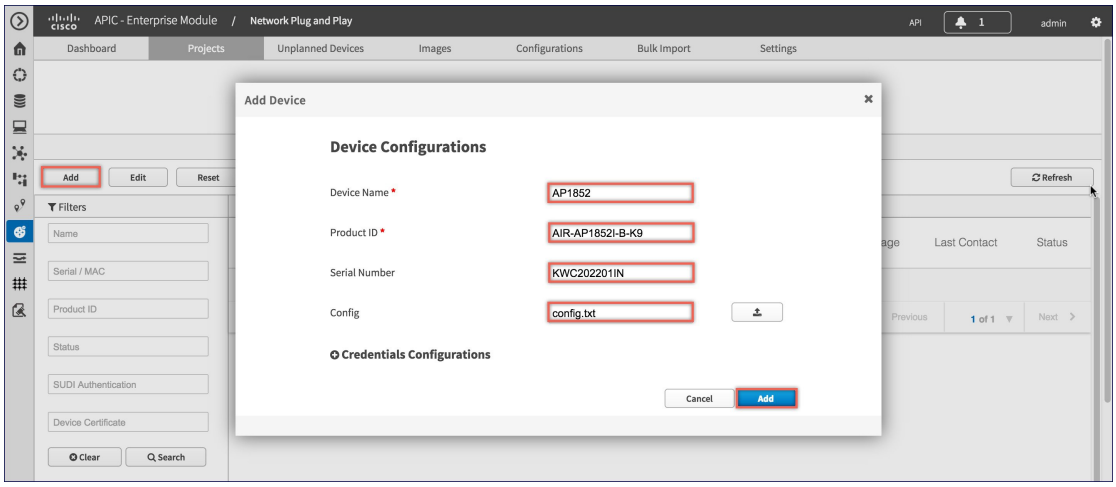
ステップ 1 [Network Plug and Play] > [Projects] に移動します。

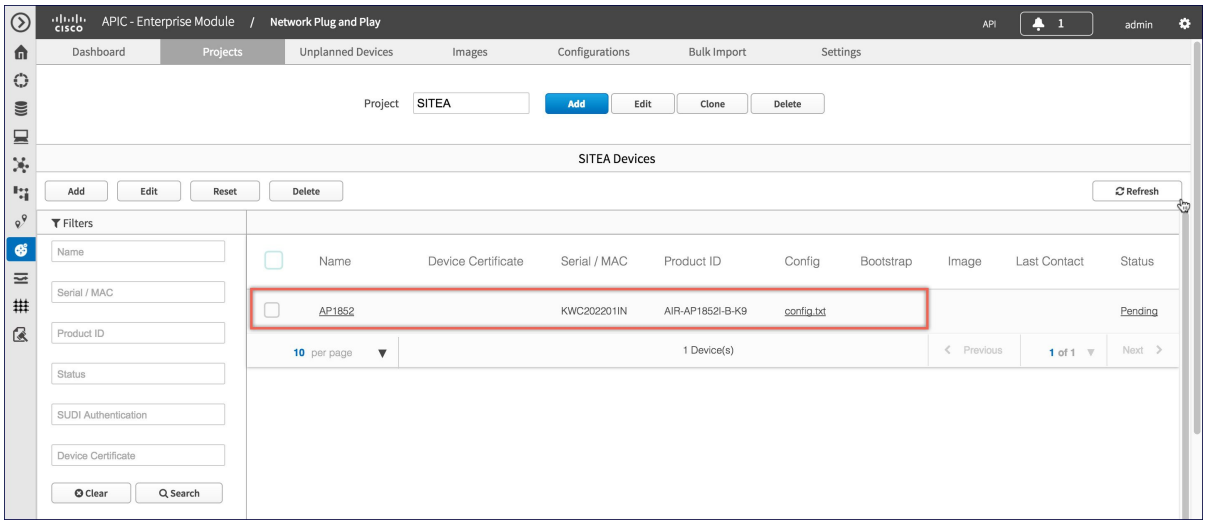
ステップ 2 [Project Devices] の下にある [Add] ボタンをクリックします。

ステップ 3 [Add Device] ウィンドウで、次の情報を入力します。

- Device Name：（各サイトに一意の名前で）デバイス名を入力します
- Product ID：ドロップダウン リストからアクセス ポイントのデバイス ID を選択します。
- Serial Number：Mobility Express アクセス ポイントのシリアル番号を入力します。
- Config：新しい設定をアップロードするか、以前に追加した設定ファイルを選択できます。

ステップ 4 [Add] ボタンをクリックします。





Cisco Mobility Express を使用した APIC-EM ネットワーク プラグ アンド プレイ導入オプション

ネットワーク プラグ アンド プレイを使用した Cisco Mobility Express の導入では、2 つの導入オプションがサポートされています。

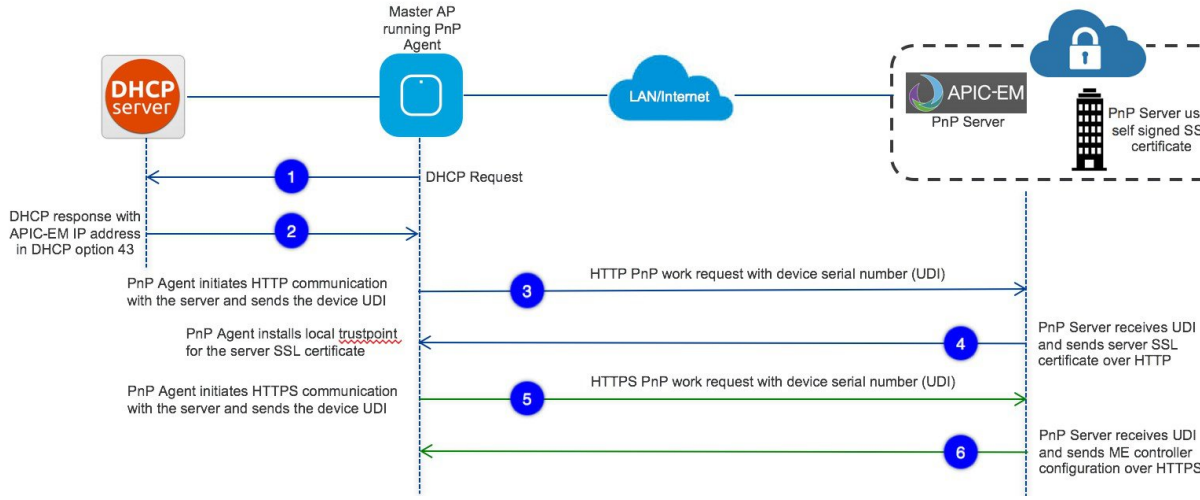
プライベート クラウドの APIC-EM コントローラ

APIC-EM コントローラへのクラウド プラグ アンド プレイ接続によるリダイレクト

プライベート クラウドの APIC-EM コントローラ

この導入オプションには、オプション 43 または DNS ディスカバリを使用して、Cisco Mobility Express アクセス ポイントによって検出できるオンプレミス APIC-EM コントローラが必要です。

図 *1*: プライベート クラウド フローの *APIC-EM* コントローラ



オプション 43 は、APIC-EM コントローラの IP アドレスを指示しています。オプション 43 で DHCP スコープを設定するには、以下に示す形式に従うことが重要です。以下の例で、192.168.1.123 は、APIC-EM コントローラの IP アドレスです。

```
ip dhcp pool pnp_device_pool
network 192.168.1.0 255.255.255.0
default-router 192.168.1.1
option 43 ascii "5A1N;B2;K4;I192.168.1.123;J80"
```

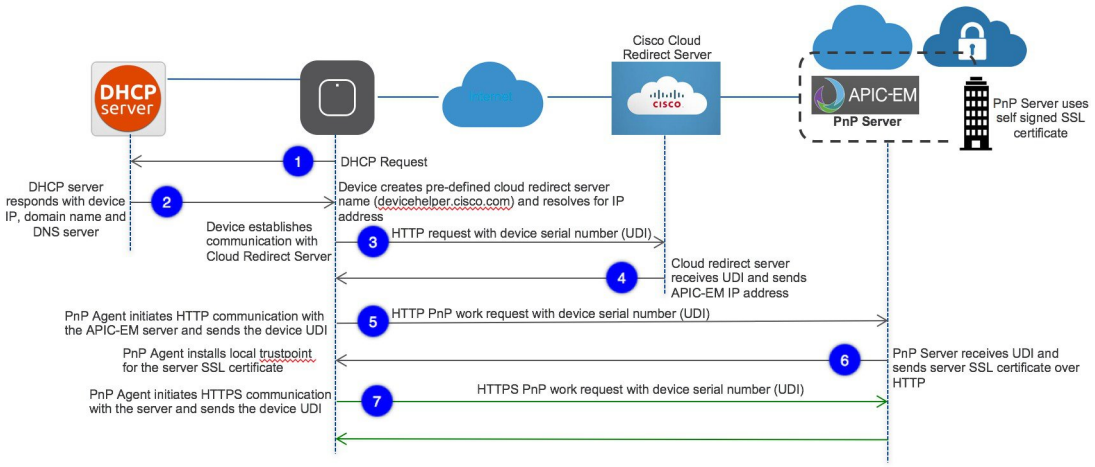
DNS ディスカバリ オプションを使用して APIC-EM コントローラを検出するには、DHCP スコープの DNS サーバとドメイン名を設定します。

```
ip dhcp pool pnp_device_pool
network 192.168.1.0 255.255.255.0
default-router 192.168.1.1
domain-name cisco.com
dns-server 172.20.229.8
```

APIC-EM コントローラへのクラウド プラグ アンド プレイ接続によるリダイレクト

クラウド リダイレクション サービスは、APIC-EM コントローラに Cisco Mobility Express 対応アクセス ポイントをリダイレクトするために、シスコのパブリック ホステッド クラウドを使用します。最小要件は、Mobility Express アクセス ポイント ネットワークに、シスコのパブリック クラウドに到達可能な DHCP、DNS、接続があることです。この導入オプションでは、DHCP スコープのオプション 43 を設定する必要はありません。簡易テストでは、DHCP アドレスを取得し、展開されている Mobility Express AP から [devicehelper.cisco.com] に ping を送信します。

図 *2 : APIC-EM* コントローラ フローへのクラウド プラグ アンド プレイ デバイス リダイレクト



クラウド プラグ アンド プレイ デバイス リダイレクト プロビジョニングのワークフロー

このセクションでは、クラウド プラグ アンド プレイ接続サービスを使用して APIC-EM コントローラに Cisco Mobility Express のアクセス ポイントをリダイレクトするための手順について説明します。

クラウドプラグ アンドプレイ接続によるリダイレクト サービスを設定するには、次の手順に従います。

1. スマート アカウントを取得する
2. APIC-EM コントローラ プロファイルを作成する
3. デバイス リストに Mobility Express 対応アクセス ポイントを追加する
4. APIC-EM コントローラ プロファイルに Mobility Express 対応アクセス ポイントを関連付ける

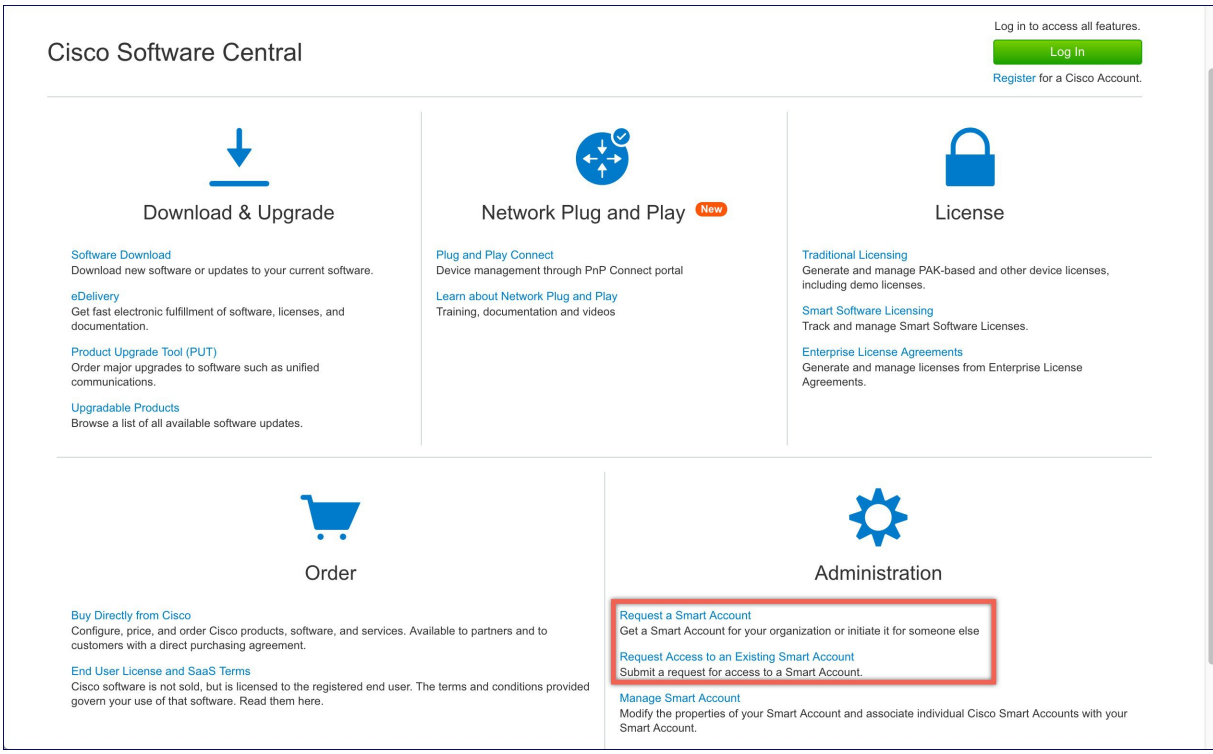
その他の機能や PnP 設定の詳細については、次のリンクを参照してください。
https://www.cisco.com/c/en/us/support/cloud-systems-management/one-enterprise-network-controller/products-installation-and-configuration-guides-list.html

スマート アカウントを取得する

手順

ステップ 1 http://software.cisco.com に移動します。

ステップ 2 スマート アカウントを申請するか、既存のスマート アカウントにログインします。

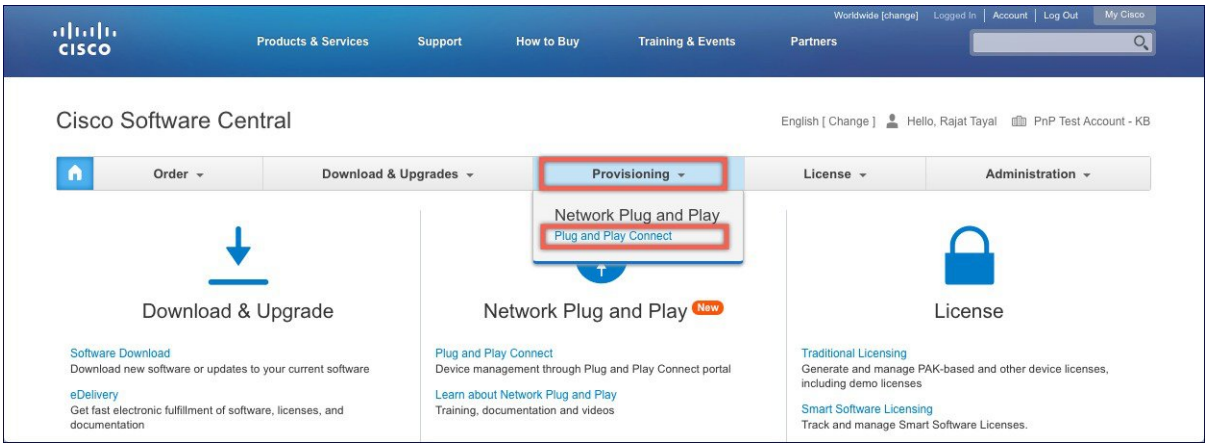


APIC-EM コントローラ プロファイルを作成する

手順

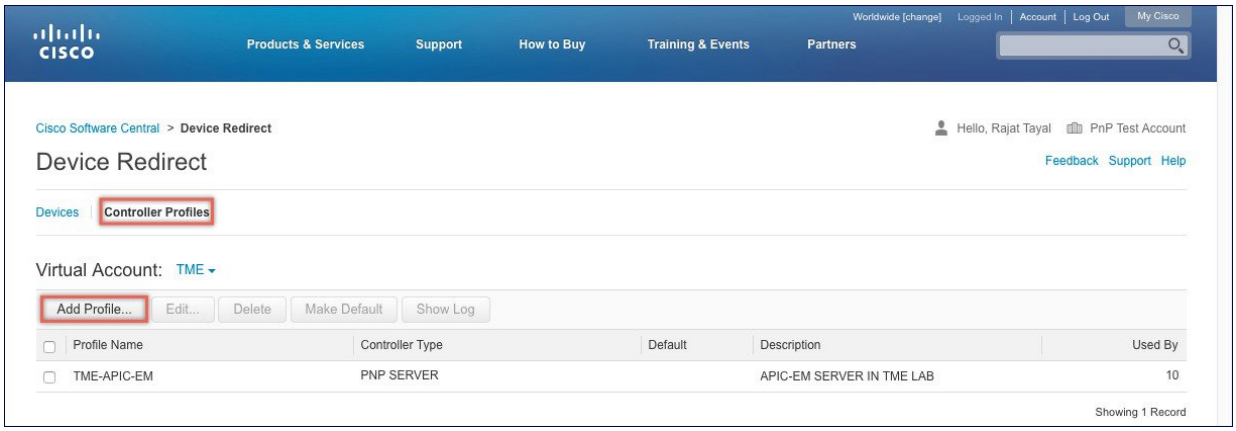
ステップ 1 http://software.cisco.com に移動して、ログインします。

ステップ 2 [Provisioning] > [Plug and Play Connect] に移動します。

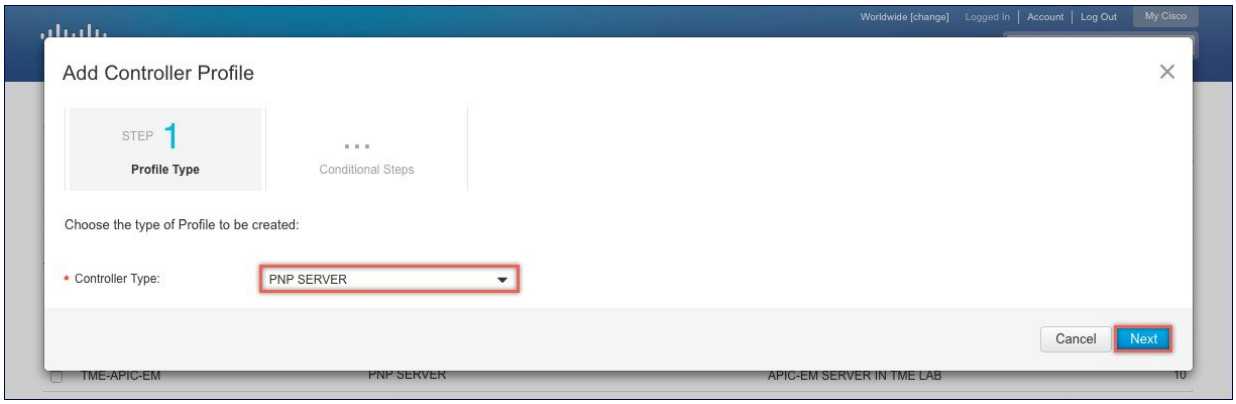


ステップ 3 [Controller Profiles] をクリックします。バーチャル アカウントを選択します。持っていない場合は、まずバーチャル アカウントを作成します。

ステップ 4 [Add Profile] をクリックして、新しいコントローラ プロファイルを作成します。



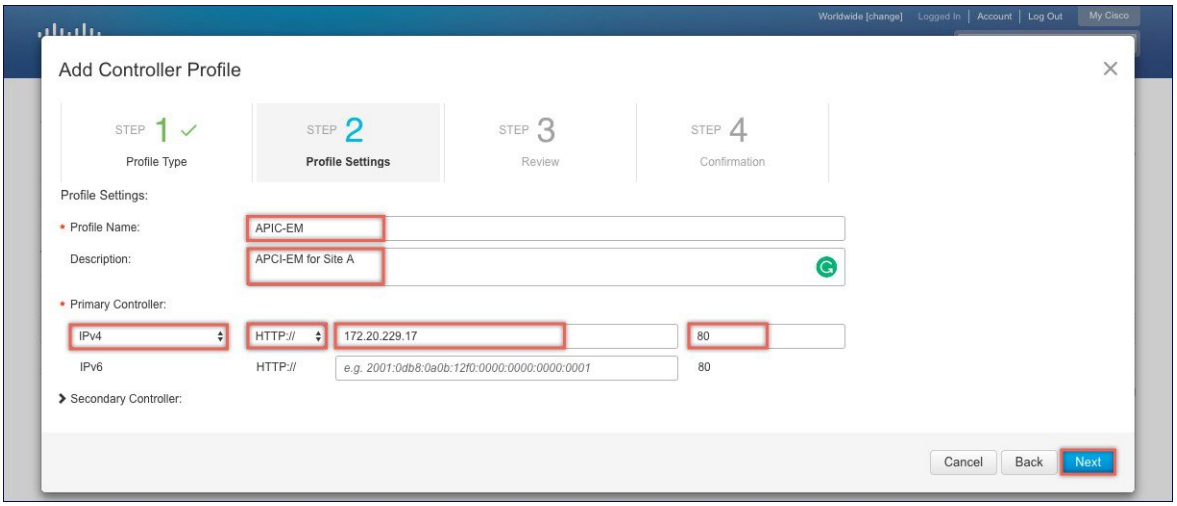
ステップ 5 [Controller Type] を PNP サーバとしてドロップダウン リストから選択し、[Next] をクリックします。



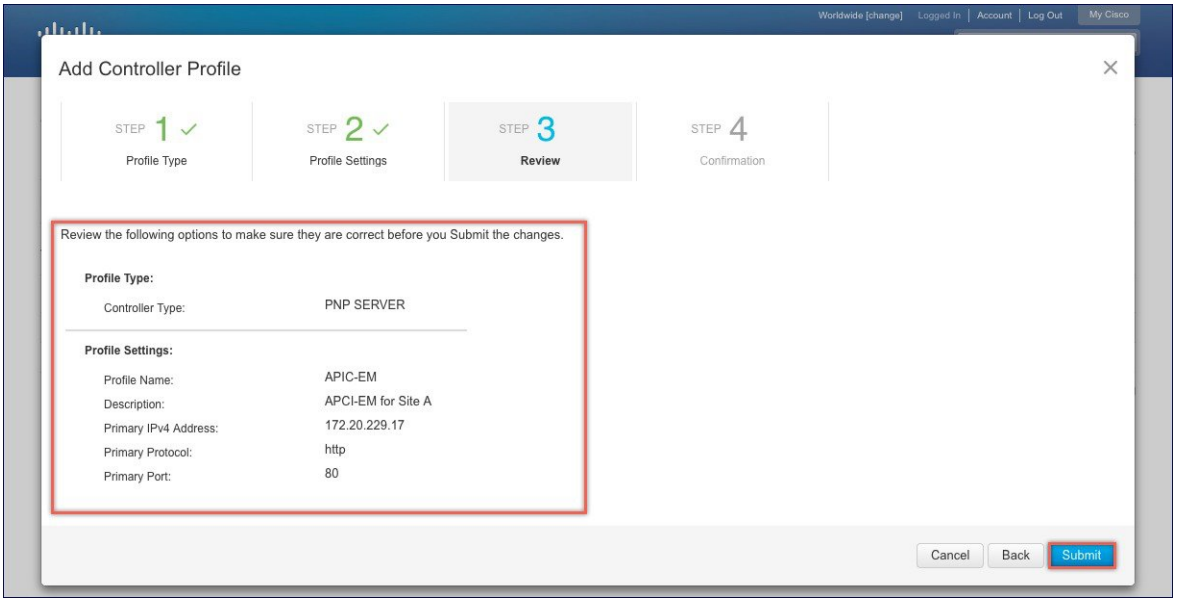
ステップ 6 次の情報を入力して [Next] をクリックします。

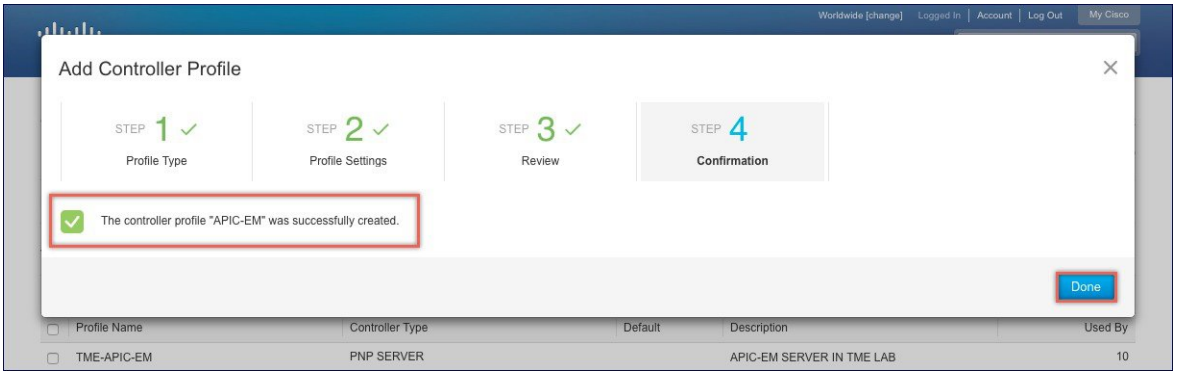
1. プロファイル名
2. 説明
3. IPv4、IPv6、HTTP、または HTTPS を選択し、PNP サーバの場合は、IP アドレスを入力します。

（注） HTTPS を選択する場合は、SSL 証明書をインポートします。また、必要に応じて、セカンダリ コントローラの情報を入力できます。



ステップ 7 エントリを確認して、コントローラ プロファイルを追加するために [Submit] ボタンをクリックし、最後に [Done] をクリックします。





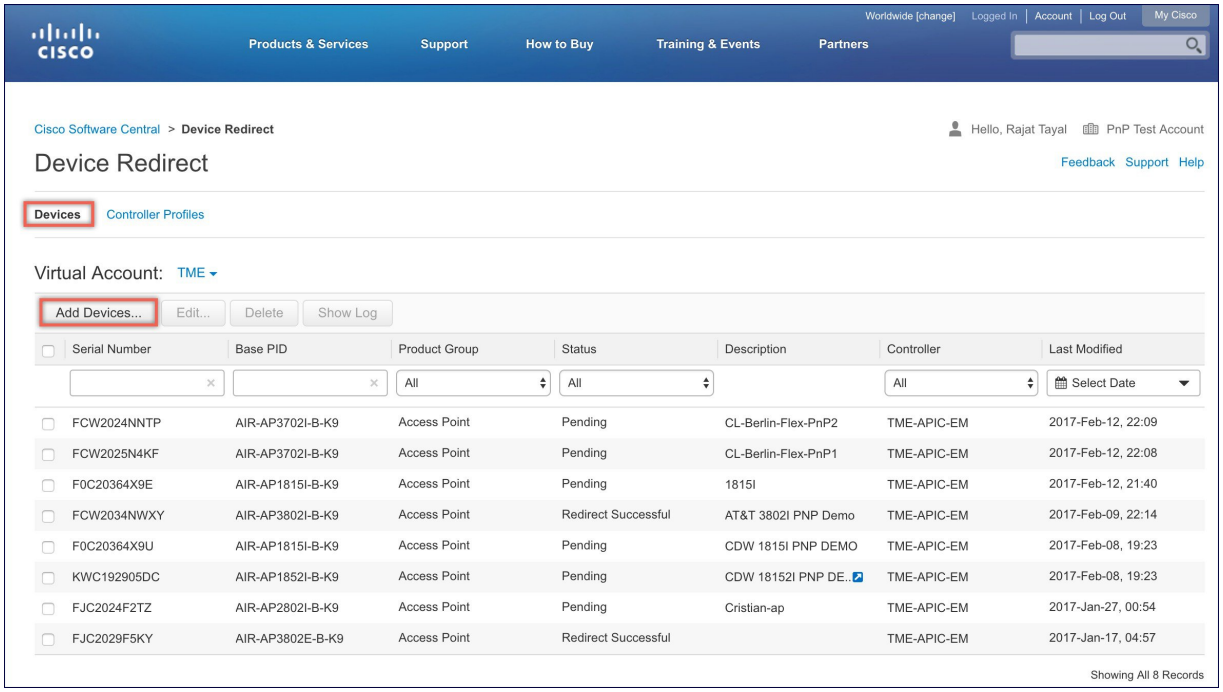
デバイス リストに Cisco Mobility Express 対応アクセス ポイントを追加する

手順

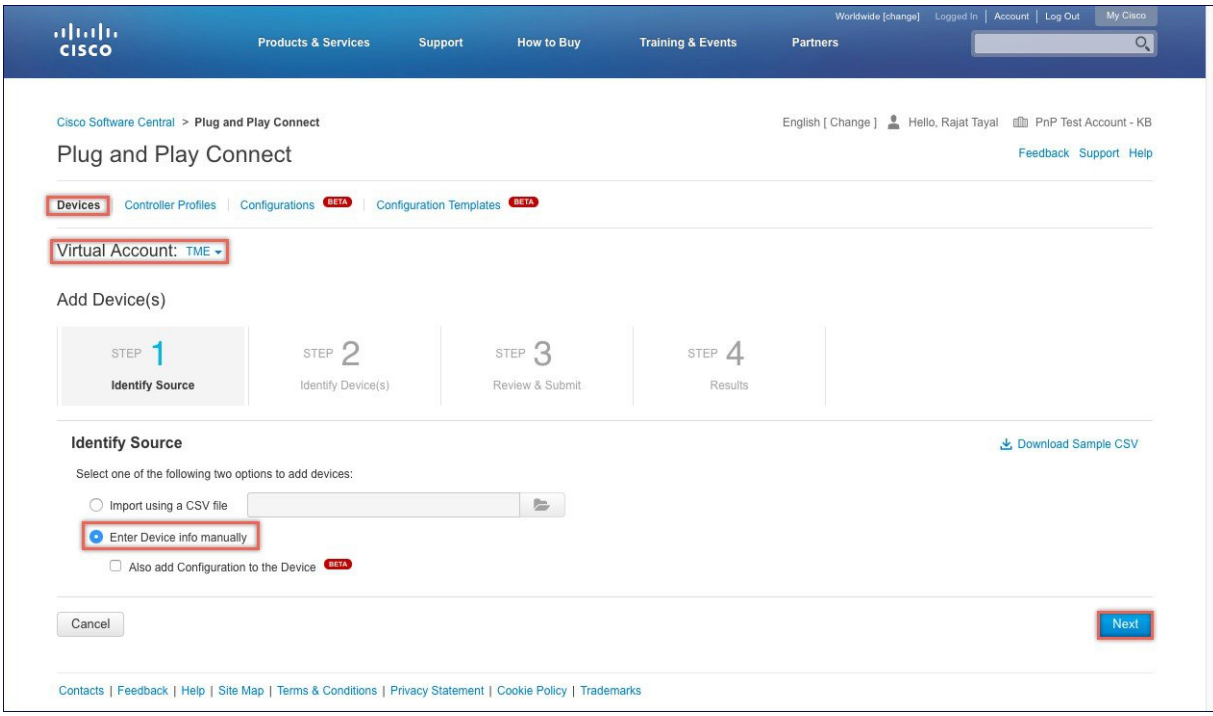
ステップ 1 [Provisioning] > [Plug and Play Connect] に移動します。[Devices] をクリックします。

ステップ 2 [Devices] をクリックします。バーチャル アカウントを選択します。持っていない場合は、まずバーチャル アカウントを作成します。

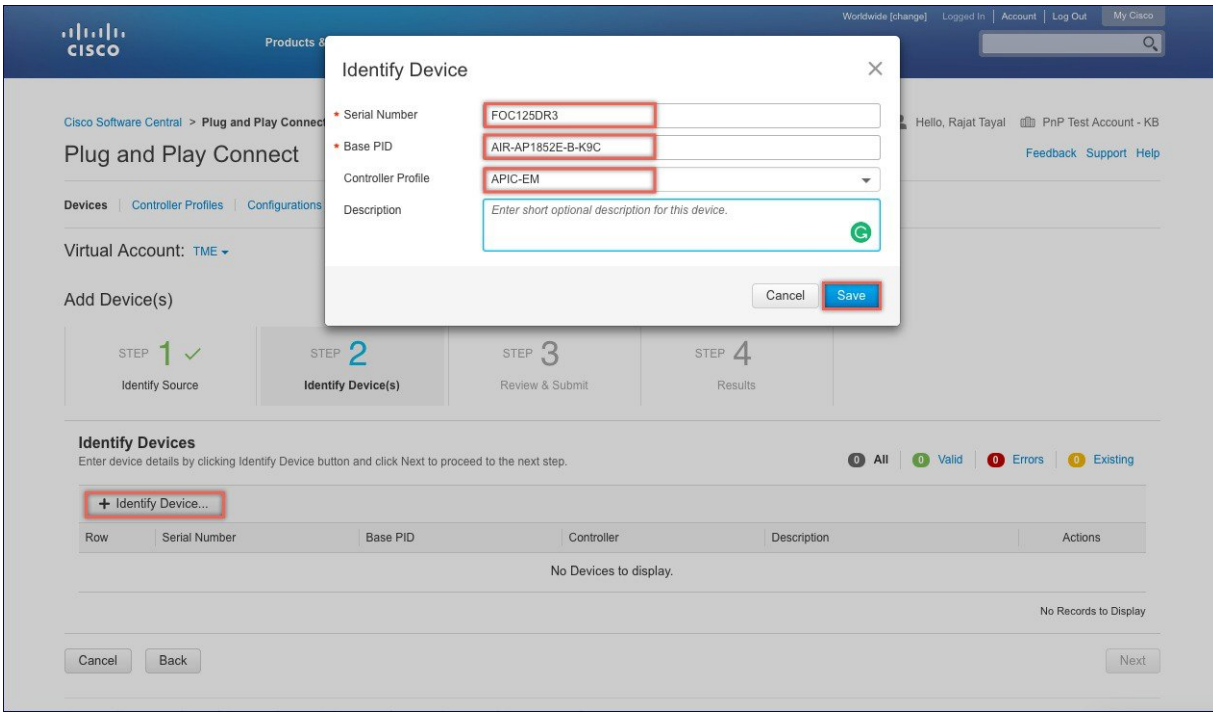
ステップ 3 [Add Devices] ボタンをクリックして、新しいデバイス（Mobility Express アクセス ポイント）を追加します。



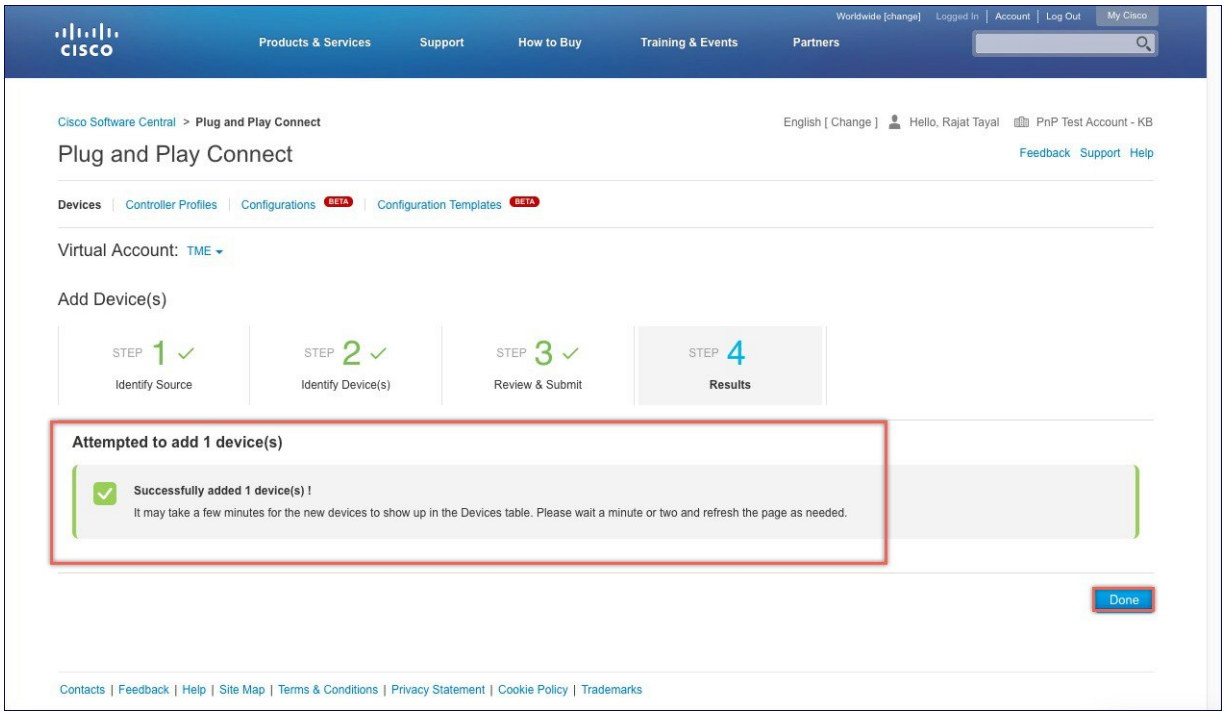
ステップ 4 デバイス情報が記載されている CSV ファイルをインポートするか、[Enter Device info] を手動で選択します。[Next] をクリックします。



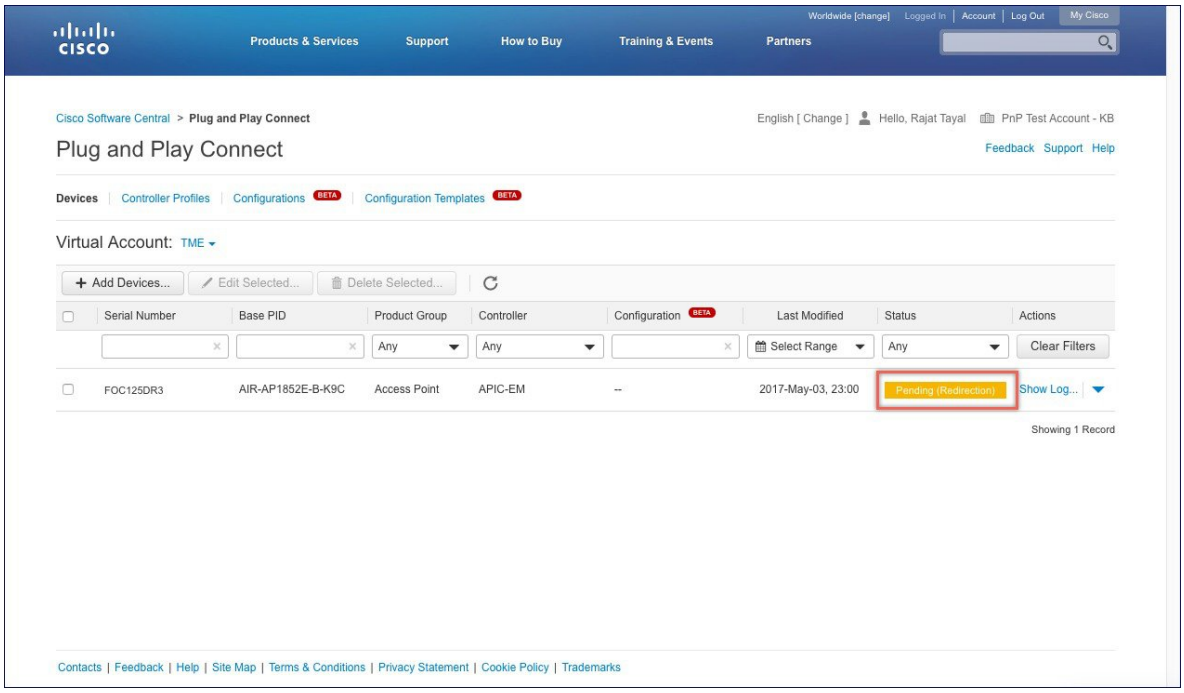
ステップ 5 [Identify Device] ボタンをクリックします。[Identify Device] ウィンドウがポップアップ表示されます。シリアル番号を入力し、[Base PID] および [Controller Profile]（以前に作成）を選択します。[Save] ボタンに続いて [Next] ボタンをクリックします。



ステップ 6 エントリを確認し、[Submit] ボタンをクリックしてデバイスを追加します。最後に、[Done] をクリックします。



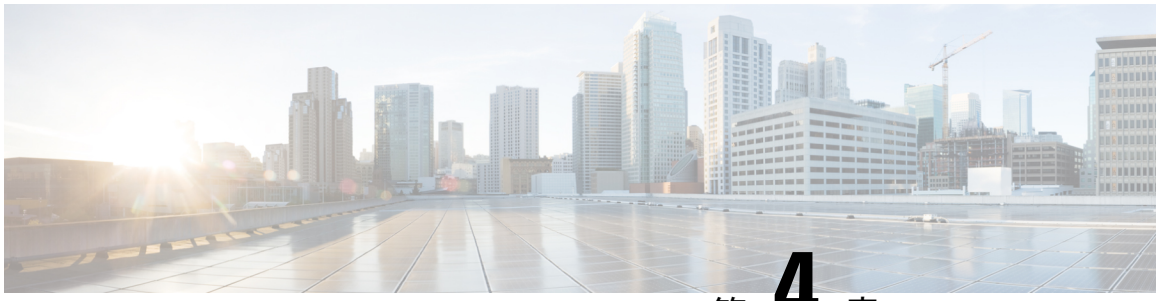
ステップ 7 デバイスが追加され、ステータスが保留状態（リダイレクション）であることを確認します。



Cisco Mobility アクセス ポイントの接続

新しい Mobility Express サイトを起動するには、プラグ アンド プレイ サービスが関連するコントローラ設定を使用した Mobility Express アクセス ポイントで設定されていることを確認します。プライベート クラウド導入オプションの APIC-EM コントローラを使用する場合、DHCP スコープのオプション 43 または DNS ディスカバリを設定する必要があります。APIC-EM コントローラ導入オプションへのクラウド プラグ アンド プレイ接続によるリダイレクトを使用する場合、クラウド プラグ アンド プレイ接続の関連する設定すべてが APIC-EM コントローラに正常にリダイレクトされていることも確認します。

ここで、サイトで Mobility Express アクセス ポイントを接続します。サイトで 1 台以上のアクセス ポイントを接続します。複数の Mobility Express アクセス ポイントがサイトで接続されている場合、マスター選択が最初に発生し、マスターアクセスポイントが選択された後にのみ、ネットワーク プラグ アンド プレイ サービスとの通信を開始し、導入オプションに関係なく、コントローラ設定ファイルをダウンロードすることに注意してください。他のアクセスポイントは、ネットワーク プラグ アンド プレイ サービスとの通信は開始しません。コントローラ設定ファイルがアクセスポイントでダウンロードされた後、再起動してコントローラ機能を実行します。サイトの残りのアクセス ポイントは、従属アクセス ポイントとしてマスター アクセス ポイントに参加します。



第 4 章

Cisco Mobility Express の内部 DHCP サーバの使用

リリース 8.3.102.0 から、内部 DHCP サーバを有効にして、アクセス ポイントおよび WLAN のスコープを作成できます。Cisco Mobility Express では合計 17 個の DHCP スコープがサポートされています。内部 DHCP サーバを使用すると、Cisco Mobility Express は外部 DHCP サーバを使わずにサイト サーベイを実行することもできます。

（注） 1 つの Mobility Express の導入で同時に内部 DHCP サーバと外部 DHCP サーバを使用することは、リリース 8.7 ではサポートされていません。

• DHCP スコープの作成 （33 ページ）

DHCP スコープの作成

内部 DHCP サーバを有効にし、Day 0 のセットアップ ウィザードおよび Day 1 のコントローラ WebUI を使って DHCP スコープを作成できます。通常、WLAN にスコープを関連付ける場合、Day1 のコントローラ WebUI を使って DHCP スコープを作成します。

コントローラ WebUI を使用して、スコープを作成し、WLAN に関連付けるには、以下の手順に従います。

手順

ステップ 1 [Wireless Settings] > [DHCP Server] > [Add new Pool] に移動します。[Add DHCP Pool] ウィンドウがポップアップ表示されます。

ステップ 2 [Add DHCP Pool] ウィンドウで、次のフィールドを入力します。

- WLAN のための **DHCP プール名**を入力します
- **[Pool Status]** を有効にします

- WLAN の **VLAN ID** を入力します
- DHCP クライアントの**リース期間**を入力します。デフォルトは 1 Day です
- **ネットワーク/マスク**を入力します
- DHCP プールの**開始 IP** を入力します
- DHCP プールの終了 IP を入力します

  （注） 集中型 NAT に接続するクライアント デバイス用のスコープの場合は、**デフォルト ゲートウェイ**として **Mobility Express コントローラ**を選択する必要があります

- DHCP プールのデフォルト ゲートウェイを入力します
- DHCP プールの**ゲートウェイ IP** を入力します
- DHCP プールの**ドメイン名**（オプション）を入力します
- **ネーム サーバ**のために、必要に応じて [User Defined] を選択し、ネーム サーバの IP アドレスを入力します。OpenDNS ネーム サーバの IP アドレスが自動的に入力されている場合は OpenDNS を選択します。

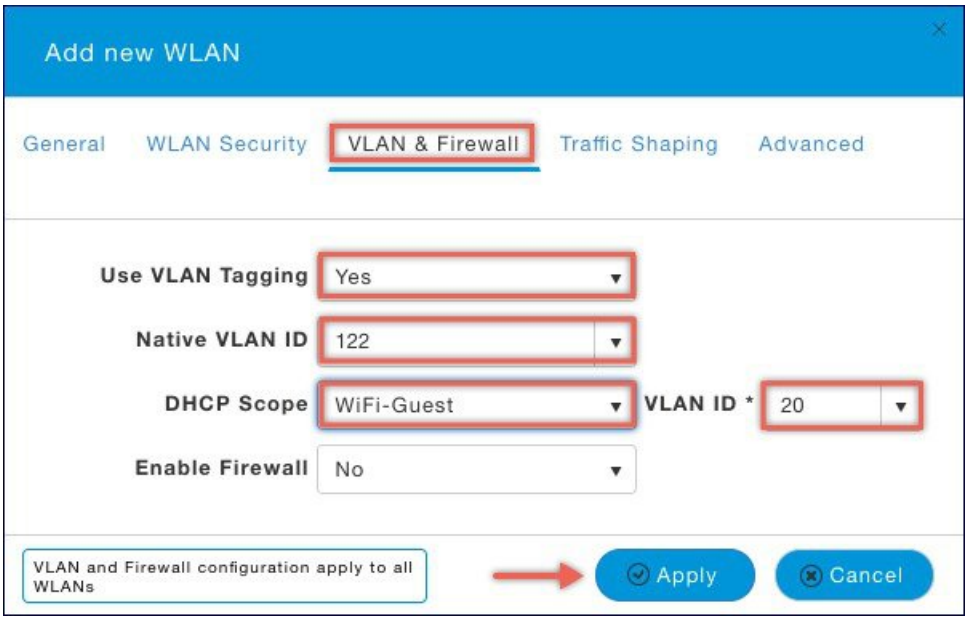
ステップ 3 [Apply] をクリックします。

ステップ 4 スコープを作成した後、DHCP スコープにマップされている VLAN を WLAN に割り当てます。WLAN に VLAN を割り当てるには、[Wireless Settings] > [WLANs] に移動します。

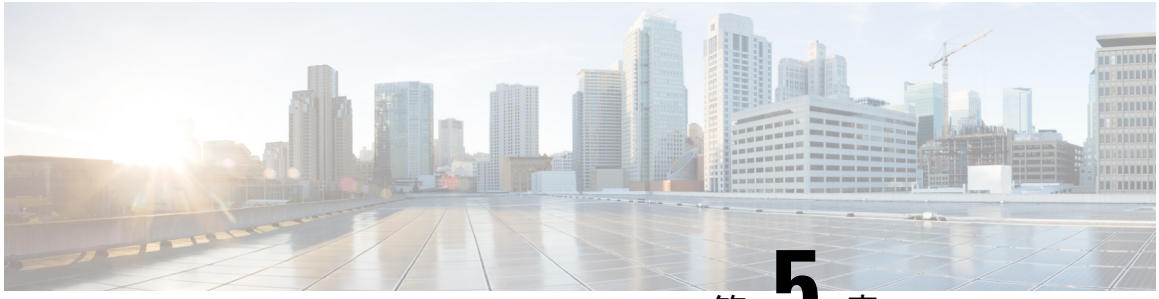
ステップ 5 WLAN が存在しない場合は WLAN を作成し、存在する場合は既存の WLAN を編集して、[VLAN and Firewall] タブをクリックします。

ステップ 6 [VLAN and Firewall] タブで、以下を設定します。

- このスコープが集中型 NAT の WLAN 用の場合、**クライアント IP 管理**または **Mobility Express コントローラ**のために [Network(Default)] を選択します
- [Use VLAN Tagging] で [Yes] を選択します。
- **ネイティブ VLAN ID** を入力します。
- WLAN のために以前に作成した **DHCP スコープ**を選択します。**VLAN ID** は、DHCP スコープを選択した後に自動的に入力されます。



ステップ 7 [Apply] をクリックします。



第 5 章

Mobility Express での TLS サポート

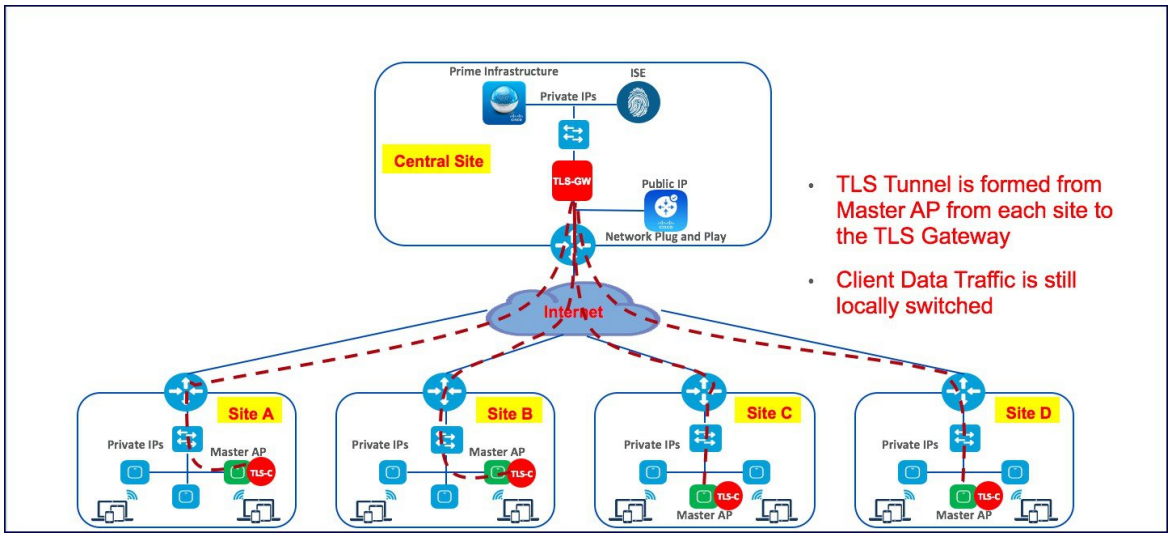
Cisco Mobility Express は、802.11ac Wave 2 アクセス ポイントに組み込まれた仮想ワイヤレス コントローラの機能です。アクセス ポイントでワイヤレス LAN コントローラの機能を実行する柔軟性により、顧客は、各サイトで最大 100 のアクセス ポイントを持つ単一のサイトまたは複数のサイトにエンタープライズ ワイヤレス ソリューションを導入できます。マルチサイト展開では、顧客は、通常は中央サイトに配置される Cisco Prime Infrastructure を使用して、各サイトを管理できます。ただし、個々のサイトが ISP 経由でインターネットに接続されており、専用の WAN 経由で接続されていない場合は、これらのマルチサイト展開を管理することが難しい場合があります。

この課題を解決するために、AireOS リリース 8.6 以降の Cisco Mobility Express では、顧客は TLS トンネルを経由する Cisco Prime Infrastructure を使用してマルチサイト展開を管理できるようになりました。これらのサイトの管理に加えて、DOT1x 認証要求を RADIUS（ISE）に集約して、それを中央サイトでサイト CPI に沿って展開できます。

中央サイトへの TLS トンネルでは SNMP、RADIUS、および SSH トラフィックのみが流れ、データ トラフィックは引き続き個々のサイトでローカルにスイッチングされることに注意してください。

TLS トンネルには 2 つのコンポーネントがあります。

1. TLS クライアント：AireOS リリース 8.6 以降、TLS クライアントは 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。
2. TLS ゲートウェイ：これは、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 ゲートウェイには 2 つのネットワーク インターフェイスがあります。
    1. パブリック ネットワーク：これは、すべてのマスター AP から到達可能なパブリック IP です。TLS クライアントは、このアドレスを使用して、マスター AP と TLS ゲートウェイ間に TLS トンネルを確立します。
    2. プライベート ネットワーク：これは、Cisco Prime Infrastructure、RADIUS およびその他のネットワーク デバイスが展開されている TLS ゲートウェイの背後にあるプライベート ネットワークの IP アドレスです。



• TLS ゲートウェイ （38 ページ）
• TLS クライアント （48 ページ）

TLS ゲートウェイ

TLS ゲートウェイは仮想マシンであり、中央サイトに展開されます。

TLS ゲートウェイのシステム要件

1. ハイパーバイザ：VMware–ESXi 5.5.0/ESXI 6.0
2. VM リソース
   1. 4 vCPU
   2. 8 GB RAM
   3. 100 GB のストレージ
   4. 2 つの NIC（パブリック ネットワーク用とプライベート ネットワーク用）
3. IP ルーティング要件
   1. Prime-infra（SNMP）、ISE（Radius）、DHCP サーバ、SSH、モニタリング システムへの TLS-GW プライベート ネットワークから有効なルーティング（その逆も同様）
4. TLS-GW パブリック IP は ME-AP の管理 IP から到達可能である必要があります。

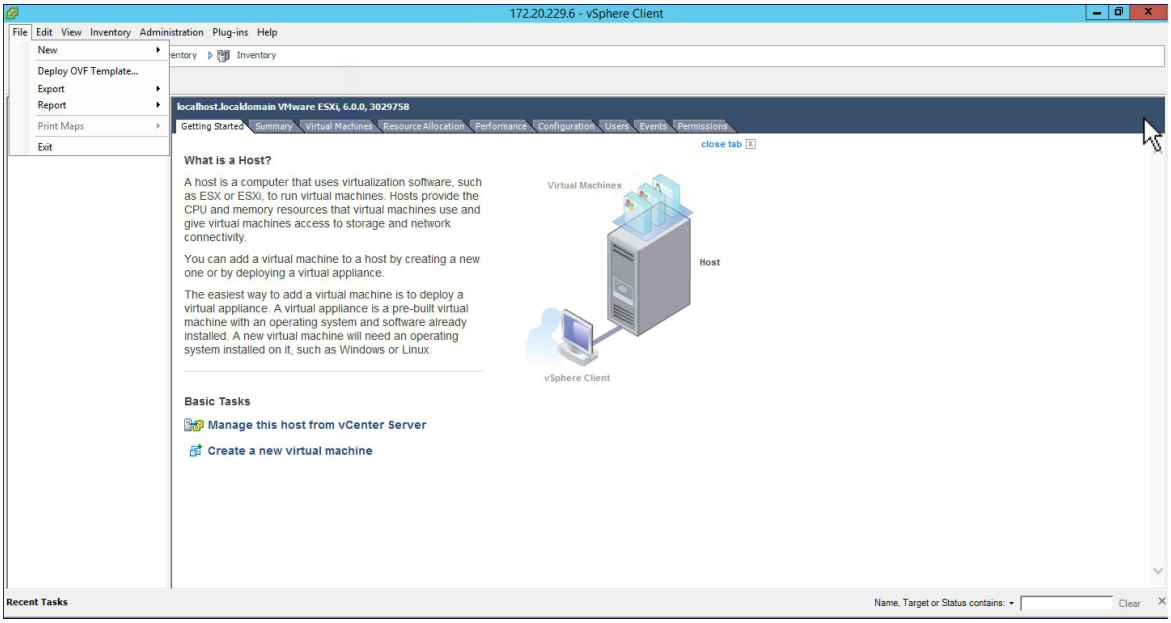
TLS ゲートウェイの展開

以下の手順に従って、中央サイトに TLS ゲートウェイを展開してください。

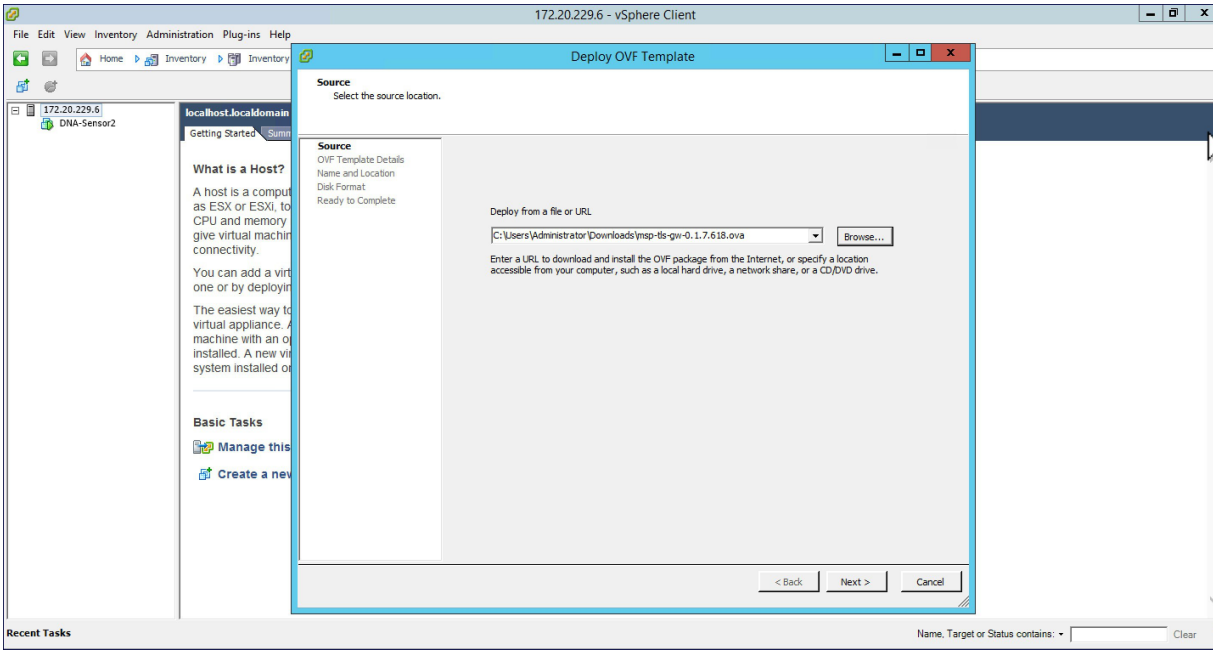
手順

ステップ 1 TLS ゲートウェイの OVA ファイルを入手します。

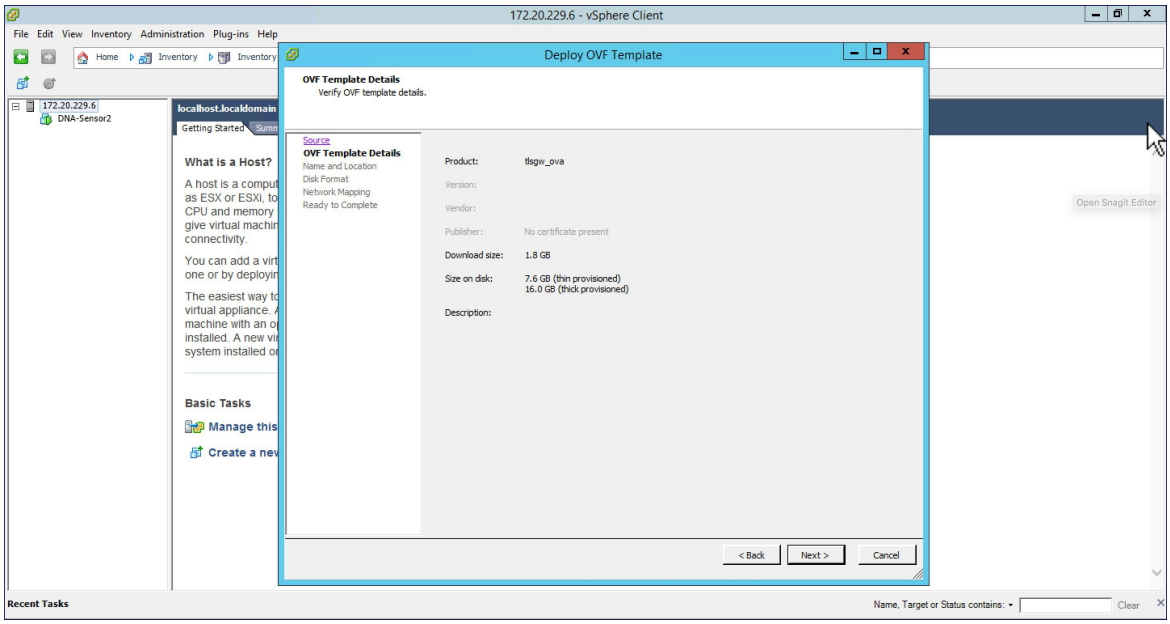
ステップ 2 vSphere クライアント UI で、[File] > [Deploy OVF Template] に移動します。



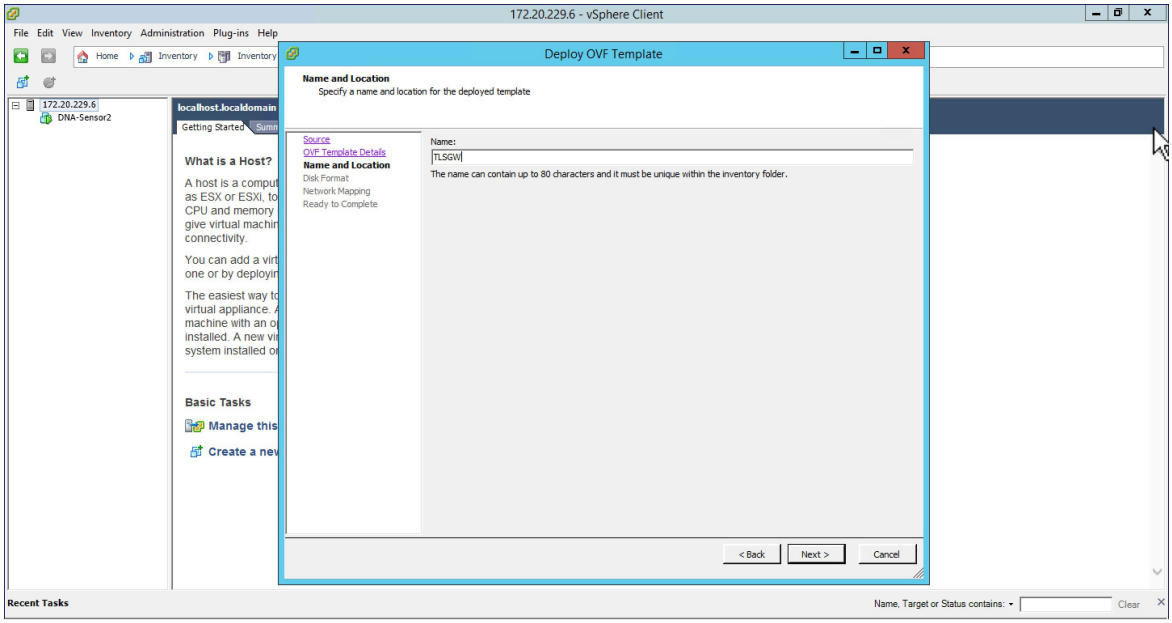
ステップ 3 ローカル マシンの TLS ゲートウェイ OVA ファイルを参照します。[Next] をクリックします。



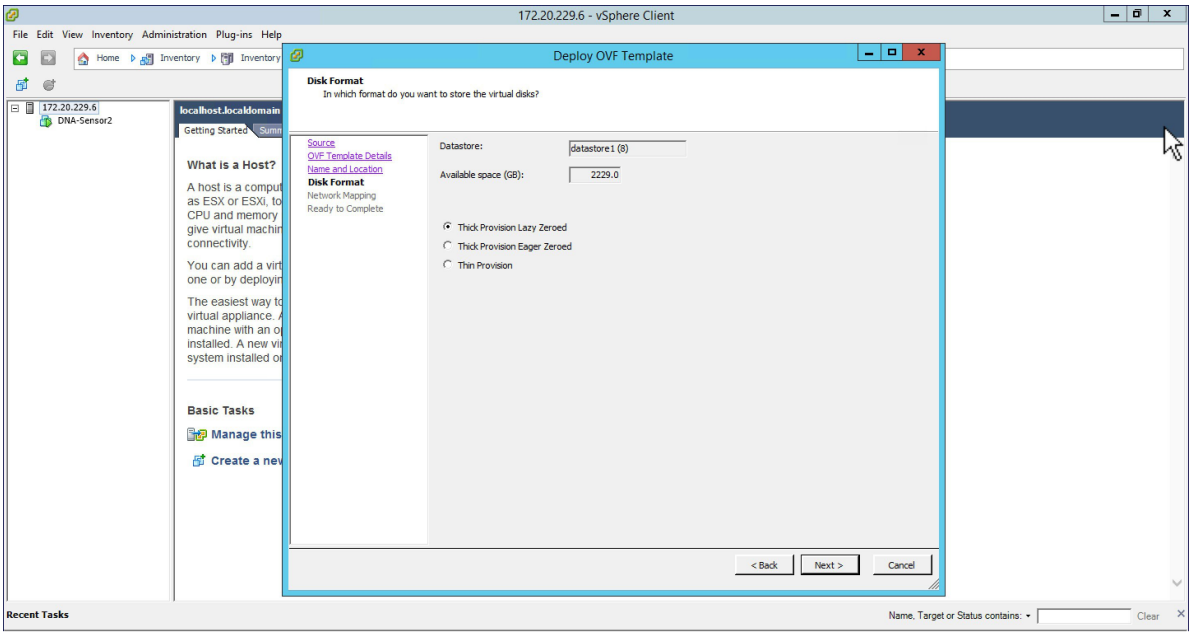
ステップ 4 OVF テンプレートの詳細を確認して、[Next] をクリックします。



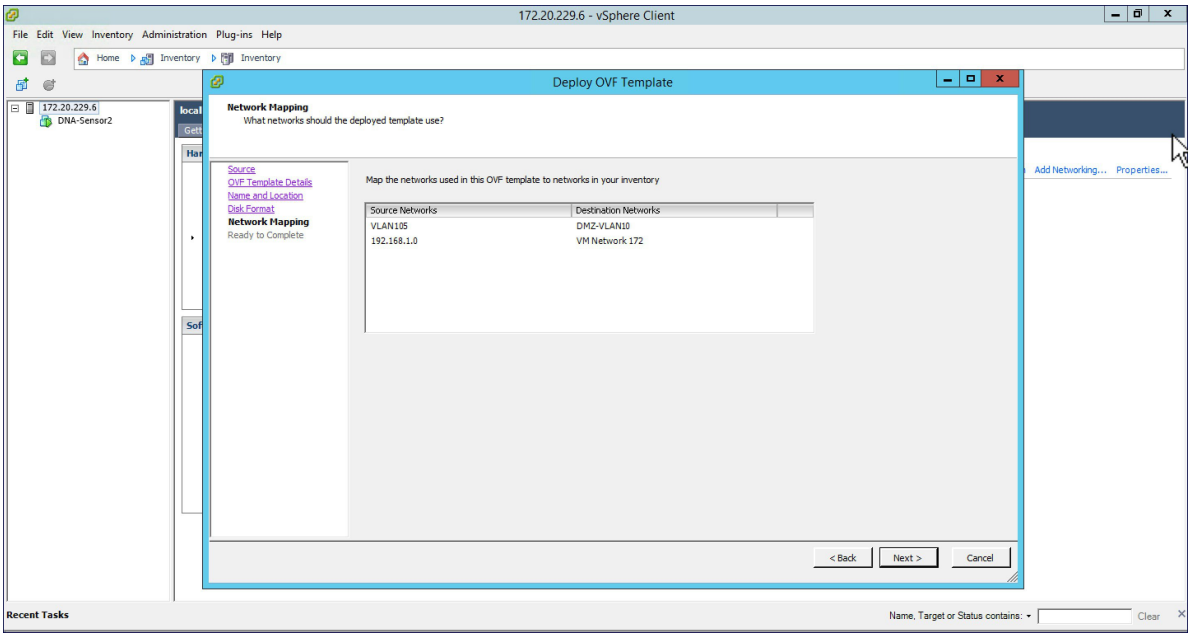
ステップ 5 TLS ゲートウェイの仮想マシンの名前を指定します。



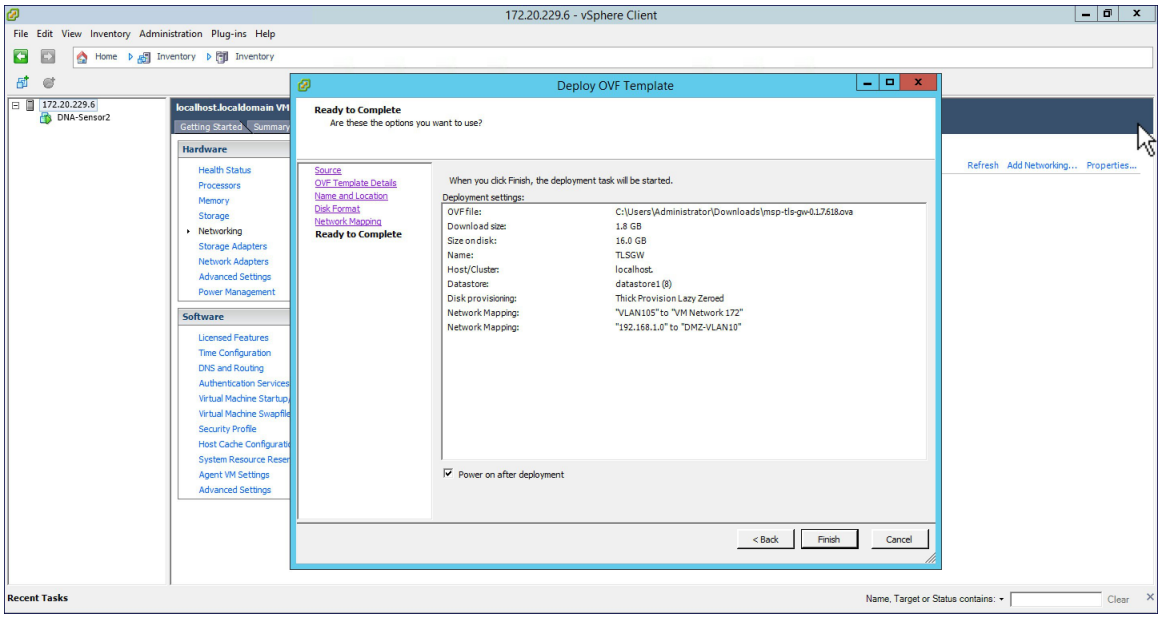
ステップ 6 ディスク形式の場合は、デフォルトのままで [Next] をクリックします。



ステップ 7 ネットワーク マッピングの場合は、パブリック ネットワーク インターフェイスの宛先ネットワークを選択します。[Next] をクリックします。



ステップ 8 展開設定を確認します。[Power On after deployment] チェックボックスを有効にし、[Finish] をクリックします。



TLS ゲートウェイの設定

TLS ゲートウェイの設定は、次の 3 つの手順から成ります。

1. パブリックおよびプライベート ネットワーク インターフェイスの IP アドレスの設定
2. TLS ゲートウェイの構成ファイルの設定およびサービスの開始
3. PSK ID-KEY ペアの設定

TLS ゲートウェイ用の OVA を展開して電源を入れた後、次の手順に従って TLS ゲートウェイを設定します。

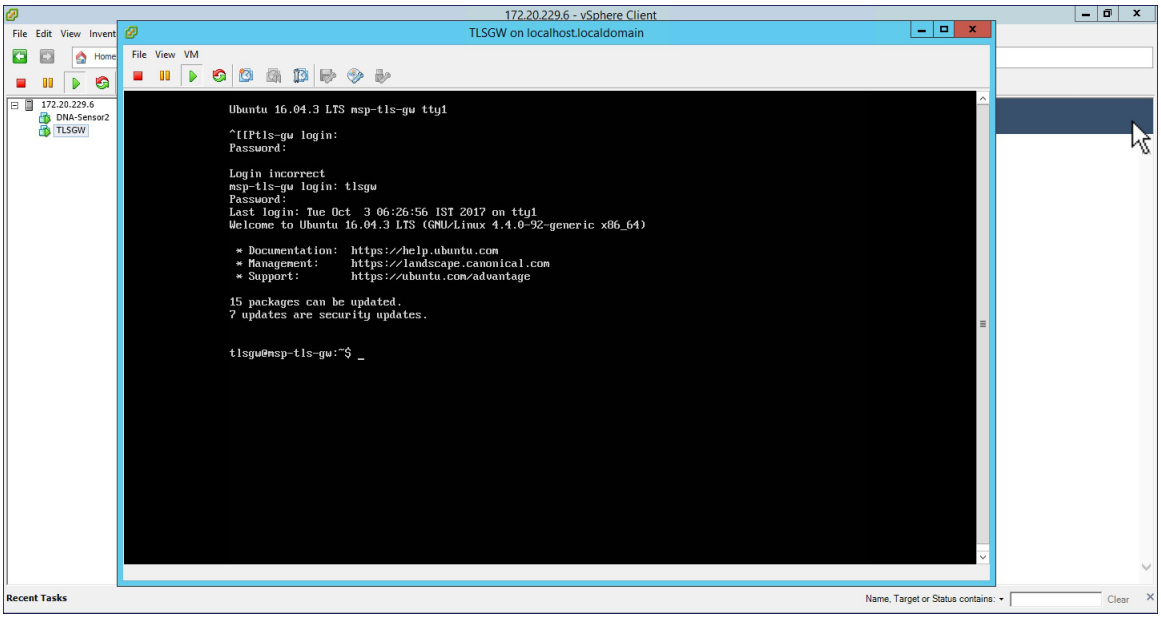
パブリックおよびプライベート ネットワーク インターフェイスの IP アドレスの設定

手順

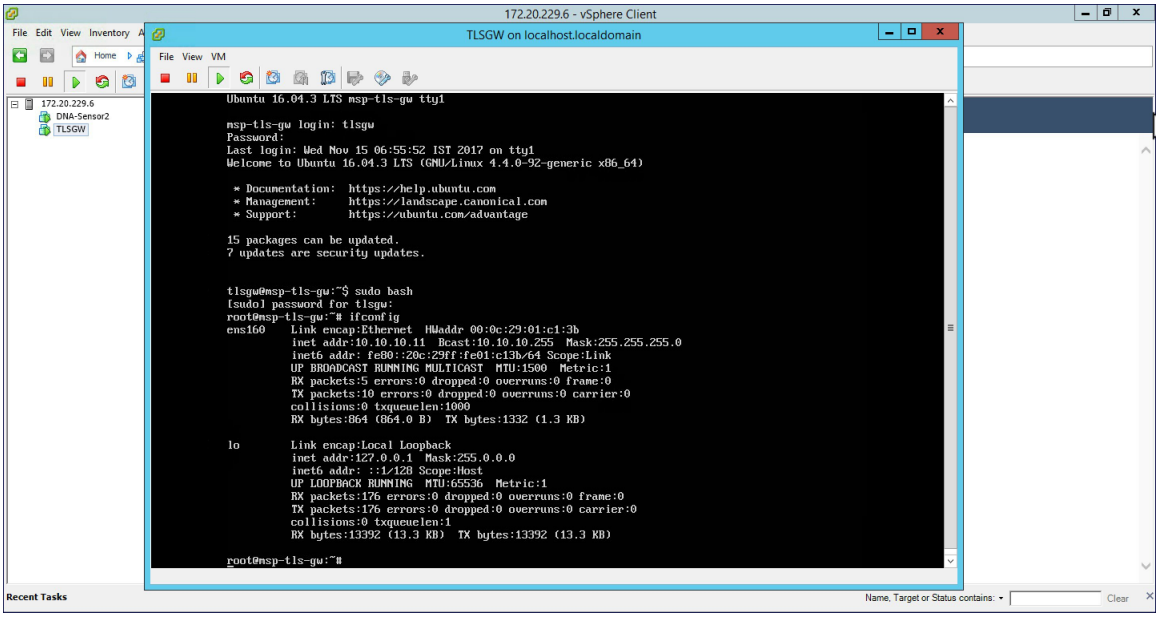
ステップ 1 TLS ゲートウェイ VM へのコンソール セッションを開き、次のクレデンシャルを使用してログインします。

ユーザ名：tlsgw

パスワード：tlsgw



ステップ 2 以下に示すように、***ifconfig*** と入力してパブリック インターフェイスとプライベート インターフェイスの IP アドレスを確認します。

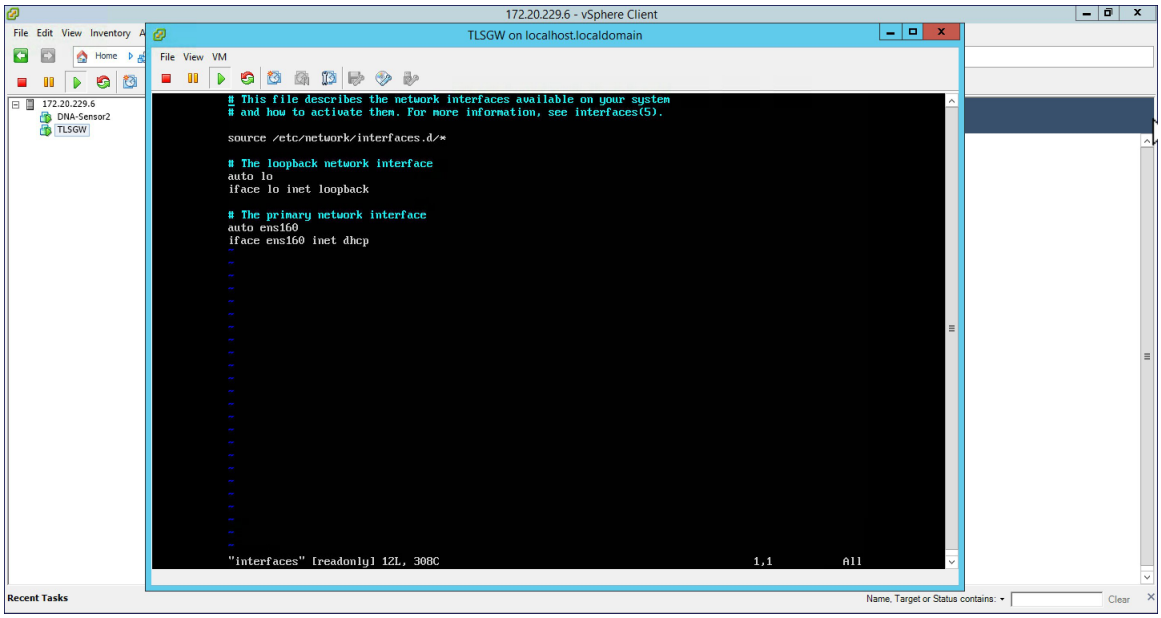


（注） ***ens160*** はパブリック ネットワーク インターフェイスに対応し、上記の例では DHCP サーバから ***10.10.10.11*** の IP を取得しています。また、IP アドレスを静的に割り当てることもでき、以降の手順で説明しています。また、上記の ***ifconfig*** 出力にはプライベート ネットワークのインターフェイスはありません。これは手動で設定することもでき、以降の手順で説明しています。

ステップ 3 **tlsgw@msp-tls-gw:** プロンプトで ***sudo bash*** と入力し、tlsgw の [sudo] パスワードとして ***tlsgw*** と入力します。

ステップ 4 パブリックおよびプライベート ネットワーク インターフェイスの IP アドレスを設定するには、シェルで ***cd /etc/interfaces*** と入力して ***/etc/network*** ディレクトリに移動します。

ステップ 5 シェルで ***vi interfaces*** と入力し、vi エディタを使用して ***interfaces*** ファイルを開きます。

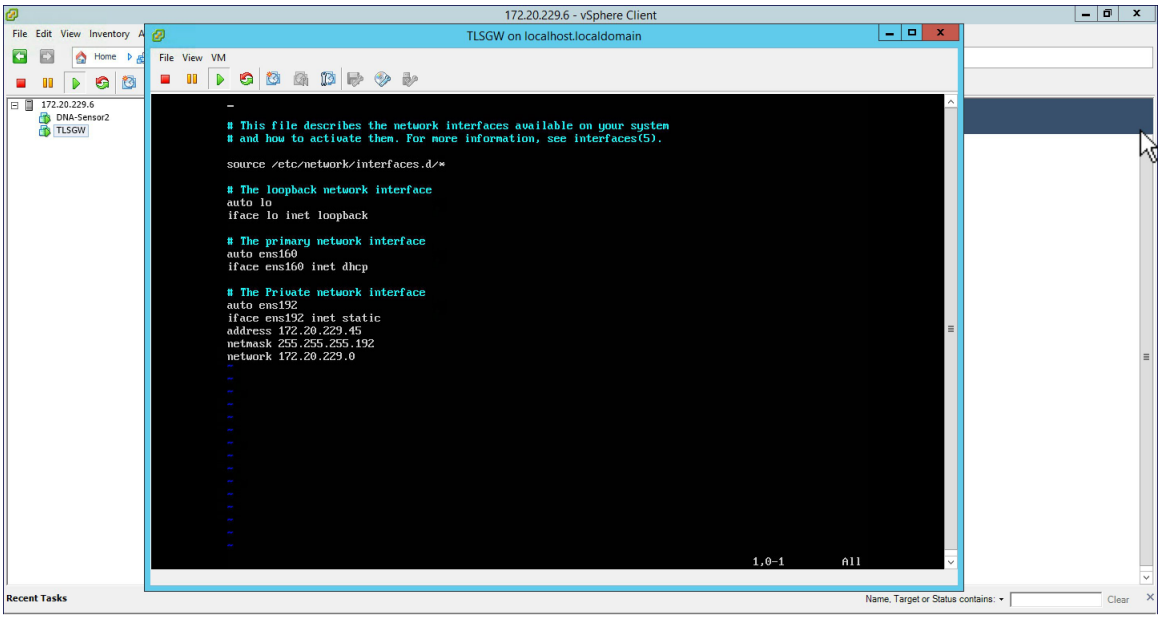


（注） ：***ens160*** はパブリック ネットワーク インターフェイスであり、デフォルトで DHCP 用に設定されています。パブリック ネットワーク インターフェイスの IP アドレスを静的に設定する場合は、以下の例のように ***ens160*** の設定を次のように置き換えます。

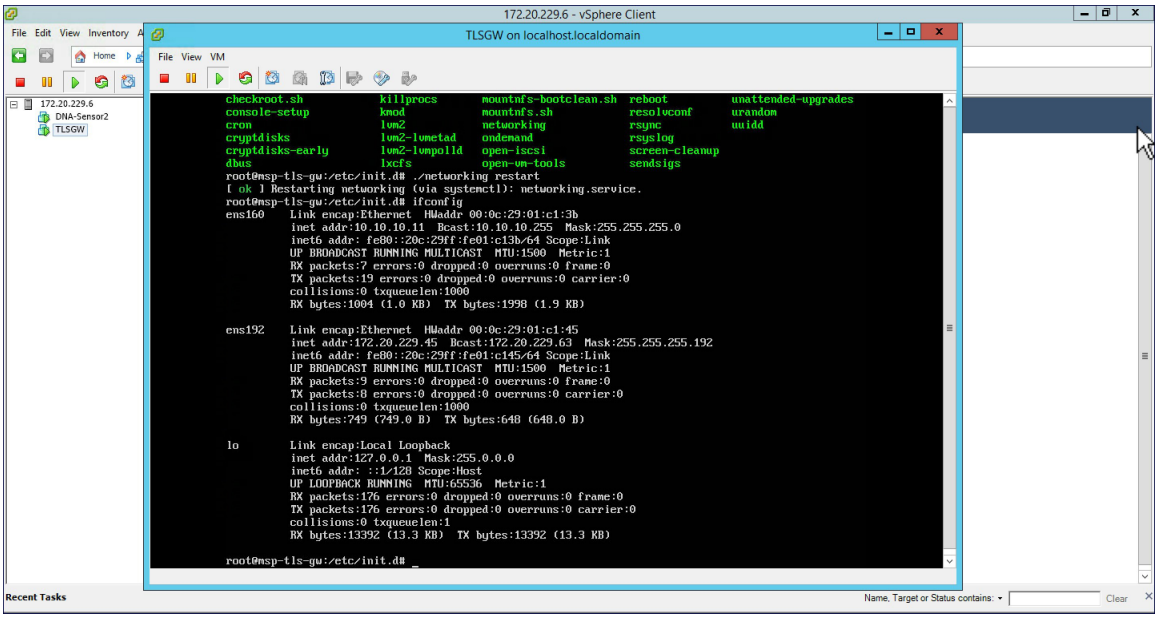
```
auto ens160
iface ens160 inet static
address 10.10.10.11
netmask 255.255.255.0
network 10.10.10.0
```

ステップ 6 プライベート ネットワーク インターフェイスの IP アドレスを設定するには、次のように ***interfaces*** ファイルに以下を追加し、ファイルを保存します。

```
auto ens192
iface ens192 inet static
address 172.20.229.60
netmask 255.255.255.192
network 172.20.229.0
```



ステップ 7 ネットワーク サービスを再起動するには、***/etc/init.d*** に移動し、***/networking restart*** と入力します。これで、ifconfig を実行すると、パブリック インターフェイスの IP アドレスとプライベート インターフェイスの IP アドレスの両方が表示されます。パブリックとプライベートの両方の IP アドレスに ping を実行して接続を確認します。



TLS ゲートウェイの構成ファイルの設定およびサービスの開始

手順

ステップ 1 ***/opt/cisco/msp-tls-gw/bin/*** に移動し、以下のように ***tlsgw_config.txt*** を編集します。

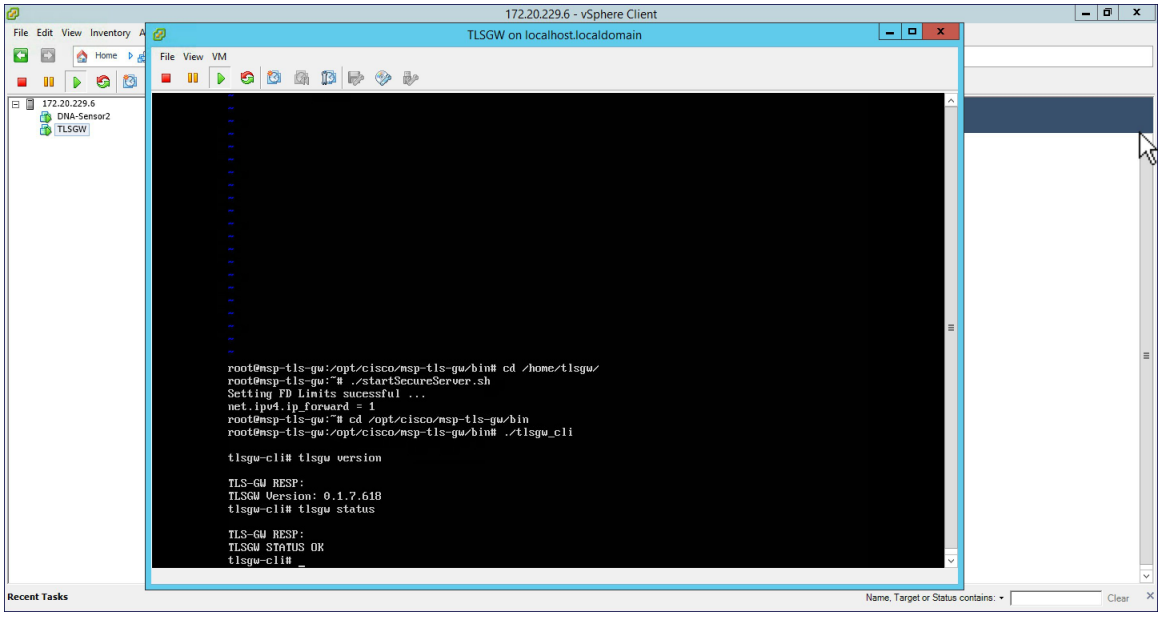
```
server_listening_ipv4_address=10.10.10.11 // Public IP of TLS Gateway
server_listening_port=443 // Port
server_private_ipv4_address=172.20.229.45 // Private IP of TLS Gateway
prefix_subnet=172.20.229.0 // Private IP network of TLS Gateway
prefix_length=26
debug_level=4 // Loglevel for TLS Gateway
dhcp_static_pool_ipv4=20.1.0.0:255.255.0.0 // Local IP pool configured for TLS Client
IP allocation
dpd_interval=60 // Dead Pear Detection timer value for client
rekey_interval=3600 // Rekey timer value  for client
retry_interval=20 // Retry timer value for client
```

（注） TLS ゲートウェイの背後で DHCP サーバを使用している場合は、tlsgw_config.txt ファイルに dhcp_static_pool_ipv4 を構成しないでください。これは、ブロードキャストが tls-gw のプライベート IP 経由で送信され、DHCP サーバが TLS ゲートウェイの背後に存在する場合、TLS クライアントに IP アドレスを割り当てる必要があるためです。

ステップ 2 ファイルを保存します。

ステップ 3 ***/home/tlsgw*** に移動し、スクリプト ***./startSecureServer.sh*** を使用して TLS ゲートウェイ サービスを開始します。

ステップ 4 TLS ゲートウェイ サービスが正常に実行されていることを確認するには、次に示すように ***/opt/cisco/msp-tls-gw/bin/*** に移動して、***./tlsgw_cli*** を実行します。



PSK ID-KEY ペアの設定

TLS ゲートウェイで事前共有キー（PSK）を設定します。これは、マスター AP 上の TLS クライアントが TLS ゲートウェイで認証するために使用されます。

（注） TLSGW には最大 3 つの PSK ID-KEY ペアを設定できます。PSK-ID には 3 ～ 50 文字の長さの文字列を使用でき、PSK パスワード（またはキー）には 5 ～ 256 の長さの文字列を使用できます。文字「:」、スペースまたはタブは psk-id と psk-key の両方で許可されていません。

設定するには、次の手順を実行します。

手順

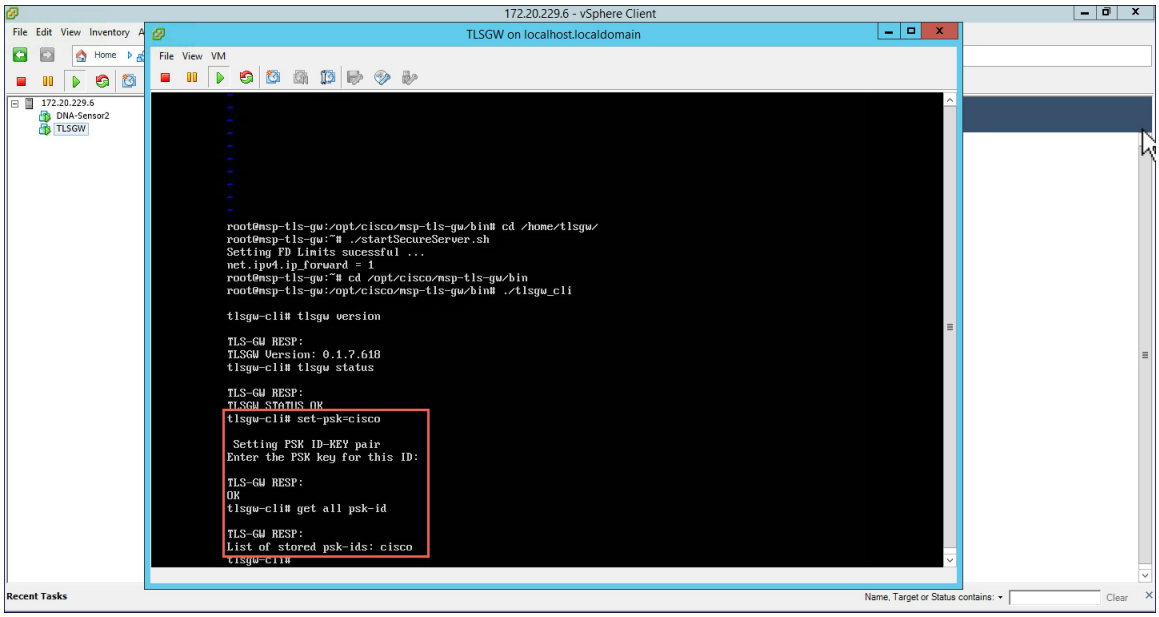
ステップ 1 */opt/cisco/msp-tls-gw/bin/* に移動して、*/tlsgw_cli* を実行します。

ステップ 2 次の CLI を使用して PSK を設定します。

```
tlsgw-cli# set-psk=cisco
 Setting PSK ID-KEY pair
Enter the PSK key for this ID:
TLS-GW RESP:
OK
```

ステップ 3 次の CLI を使用して PSK ID が設定されていることを確認します。

```
tlsgw-cli# get all psk-id
TLS-GW RESP:
List of stored psk-ids: cisco
```



TLS クライアント

TLS クライアントは、AireOS リリース 8.6 に統合されており、コード内にネイティブに存在します。TLS クライアントで TLS ゲートウェイとの TLS トンネルを確立するには、マスター AP が TLS ゲートウェイのパブリック IP と通信できる必要があります。

TLS クライアントの前提条件

1. Cisco Mobility Express AireOS リリース 8.6 以上
2. TLS ゲートウェイのパブリック IP アドレスは、マスター AP から到達可能である必要があります。TLS ゲートウェイの FQDN を使用する場合は、TLS_GW FQDN をローカル DNS サーバに設定し、同じ DNS サーバの IP を ME コントローラに設定して TLS ゲートウェイの FQDN を解決する必要があります。

TLS トンネルの設定

TLS クライアントと TLS ゲートウェイの間に TLS トンネルを設定するには、2 つの方法があります。設定方法は次のとおりです。

オプション 1：ネットワーク PnP を使用したゼロ タッチ プロビジョニング

Day 0 で、ネットワーク PnP からコントローラ設定をダウンロードできます。マスター AP が設定ファイルをダウンロードして再起動し復帰した後に、自動的に TLS ゲートウェイとの TLS

トンネルを確立するように、TLS トンネル設定をコントローラの設定ファイルに組み込むこともできます。

オプション 2：WebUI から TLS トンネルを手動で設定する

ME WebUI から TLS トンネルを設定するには、次の手順に従います。

手順

ステップ 1 コントローラ WebUI で [Expert View] に切り替えます。

ステップ 2 左側のメニューから [Services] > [TLS] に移動します。

ステップ 3 [TLS Tunnel] ページで、次のパラメータを設定します。

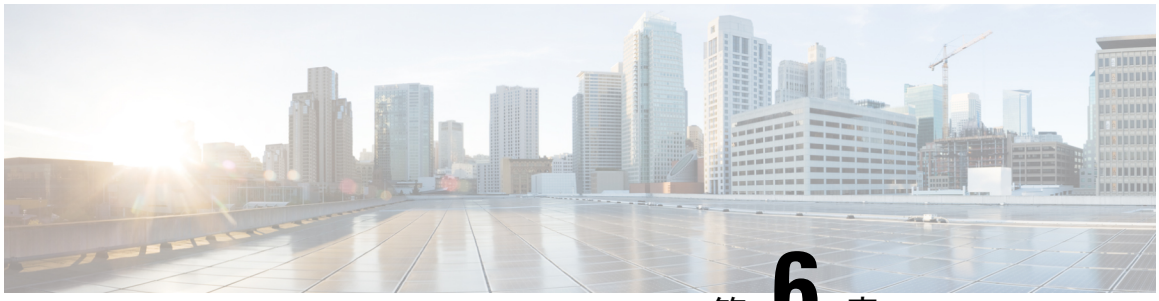
1. TLS ゲートウェイのパブリック IP アドレスまたは FQDN を入力します。
2. ポート番号を入力します。デフォルト値は 443 です。
3. PSK ID を入力します。
4. PSK キーを入力します。
5. RADIUS と SNMP を有効にします。

（注） RADIUS は ISE に使用され、SNMP は Prime Infrastructure に使用されます。

ステップ 4 [Apply] をクリックします。

ステップ 5 最後に、ページ上部で TLS トンネルを有効にします。すべての前提条件が満たされている場合、TLS ゲートウェイの場合はマスター AP からパブリック インターフェイスにトンネルが作成されます。


Monitoring
Wireless Settings
Management
Services
TLS
TLS Tunnel
Disabled
TLS Tunnel
TLS Tunnel Uptime Stamp
Not Available
TLS Tunnel Uptime
Not Available
Failure Reason
Feature disabled
Refresh



第 6 章

サイト サーベイ用 Cisco Mobility Express の設定

サイト サーベイ用 Cisco Mobility Express の設定

Cisco 802.11ac Wave 2 アクセス ポイントは、仮想ワイヤレス コントローラの機能をアクセス ポイントに組み込んだ Cisco Mobility Express に対応しています。

ワイヤレス コントローラの機能を実行する Cisco Mobility Express のアクセス ポイントは、クライアントのワイヤレス接続も提供します。アクセス ポイントがサイト サーベイに使用できる内部 DHCP サーバもサポートします。

前提条件

1. アクセス ポイント：Cisco Mobility Express ソフトウェアを実行する Cisco 802.11ac Wave 2 アクセス ポイント。以下の AP は Cisco Mobility Express をサポートします。

アクセス ポイント	サイトサーベイの機能をサポートするリリース
1540 シリーズ	AireOS® リリース 8.5 以降
1560 シリーズ	AireOS リリース 8.3.111.0 以降
1815I シリーズ	AireOS リリース 8.4 以降
1815M シリーズ	AireOS® リリース 8.5 以降
1815W シリーズ	AireOS リリース 8.4 以降
1830 シリーズ	AireOS リリース 8.3.111.0 以降
1850 シリーズ	AireOS リリース 8.3.111.0 以降
2800 シリーズ	AireOS リリース 8.3.111.0 以降

アクセス ポイント	サイトサーベイの機能をサポートするリリース
3800 シリーズ	AireOS リリース 8.3.111.0 以降

2. 電源：サイト サーベイに使用されるアクセス ポイントによりますが、アクセス ポイントに十分な電力を提供できる電源アダプタまたはバッテリ パックを使用してください。
3. コンソール ケーブル（オプション）：Cisco Mobility Express は、CLI または Over-the-Air を使用して設定できます。CLI によって Cisco Mobility Express を設定する場合、アクセス ポイントへのコンソール接続が必要です。

CLI を使用したサイト サーベイのための Mobility Express の設定

手順

ステップ 1 アクセス ポイントのコンソールに接続します。

ステップ 2 電源アダプタまたはバッテリ パックを使用してアクセス ポイントの電源を入れます。

ステップ 3 アクセス ポイントが完全に起動する（ワイヤレス コントローラが実行され設定待ち状態になる）まで待ちます。

ステップ 4 CLI セットアップ ウィザードを使用してワイヤレス コントローラを設定します。

（注） サイト サーベイでは、DHCP サーバは必須で、Cisco Mobility Express でサポートされます。以下に強調表示されている DHCP サーバの設定は、Cisco Mobility Express の DHCP サーバを有効にするために必須です。

```
Would you like to terminate autoinstall? [yes]:yes
Enter Administrative User Name (24 characters max):admin
Enter Administrative Password (3 to 24 characters max):Cisco123
Re-enter Administrative Password: Cisco123
System Name:[Cisco_3a:d2:b4] (31 characters max):me-wlc
Enter Country Code list(enter 'help' for a list of countries)[US]:US
Configure a NTP server now?[YES][no]:no
Configure the system time now?[YES][no]:yes
Enter the date in MM/DD/YY format:02/28/17
Enter the time in HH:MM:SS format:11:30:00
Enter timezone location index(enter 'help' for a list of timezones):5
Management Interface IP Address: 10.10.10.2
Management Interface Netmask: 255.255.255.0
Management Interface Default Router: 10.10.10.1
Create Management DHCP Scope?[yes][NO]:yes
DHCP Network: 10.10.10.0
DHCP Netmask: 255.255.255.0
Router IP: 10.10.10.1
Start DHCP IP address: 10.10.10.10
Stop DHCP IP address: 10.10.10.250
DomainName: mewlc.local
DNS Server:[OPENDNS][user DNS]OPENDNS
Create Employee Network?[YES][no]:yes
Employee Network Name(SSID)?:site_survey
Employee VLAN Identifier?[MGMT][1-4095]:MGMT
Employee Network Security?[PSK][enterprise]:PSK
Employee PSK Passphrase (8-38 characters)?: Cisco123
```

```
Re-enter Employee PSK Passphrase: Cisco123
Re-enter Employee PSK Passphrase: Cisco123
Create Guest Network? [yes][NO]:NO
Enable RF Parameter Optimization?[YES][no]:no
Configuration correct? If yes, system will save it and reset.[yes][NO]:yes
```

ステップ 5 アクセス ポイントが完全に起動するまで待ちます。ワイヤレス コントローラ機能が実行された後で、初期セットアップ ウィザード中に設定した管理ユーザ名またはパスワードを使用してコントローラに再度ログインします。

ステップ 6 （オプション）：CLI のセットアップ ウィザード中に、従業員ネットワーク セキュリティは、PSK に設定されています。これにより、クライアントの簡単な接続を無効にできます。不必要なクライアントが SSID に接続しないように SSID ブロードキャストを無効にすることもできます。PSK と SSID ブロードキャストを無効にするには、コントローラ CLI で次のコマンドを入力します。

```
(Cisco Controller)>config wlan disable 1
(Cisco Controller)>config wlan security wpa disable 1
(Cisco Controller)>config wlan broadcast-ssid disable wlan 1
(Cisco Controller)>config wlan enable 1
(Cisco Controller)>save config
```

ステップ 7 チャネル、送信出力、および Radio のチャネル幅を設定するには、最初に Radio を無効にして、変更を行ってから再度有効にします。

2.4GHz の Radio をチャネル 6 に変更するには、次の手順を実行します。

```
(Cisco Controller)>config 802.11b disable <ap name>
(Cisco Controller)>config 802.11b channel <ap name> <ap name> 6
(Cisco Controller)>config 802.11b enable <ap name>
```

2.4 GHz の Radio 送信出力をレベル 3 に変更するには、次の手順を実行します。

```
(Cisco Controller)>config 802.11b disable <ap name>
(Cisco Controller)>config 802.11b txPower <ap name> <ap name> 3
(Cisco Controller)>config 802.11b enable <ap name>
```

5 GHz の Radio をチャネル 44 に変更するには、次の手順を実行します。

```
(Cisco Controller)>config 802.11a disable <ap name>
(Cisco Controller)>config 802.11a channel <ap name> <ap name> 44
(Cisco Controller)>config 802.11a enable <ap name>
```

5 GHz の Radio 送信出力をレベル 5 に変更するには、次の手順を実行します。

```
(Cisco Controller)>config 802.11a disable <ap name>
(Cisco Controller)>config 802.11a txPower <ap name> <ap name> 5
(Cisco Controller)>config 802.11a enable <ap name>
```

5 GHz の Radio チャンネル幅を 40 MHz に変更するには、次の手順を実行します。

```
(Cisco Controller)>config 802.11a disable <ap name>
(Cisco Controller)>config 802.11a chan_width <ap name> 40
(Cisco Controller)>config 802.11a enable <ap name>
```

2800 および 3800 シリーズのアクセス ポイントをサイト サーベイに使用する場合、XOR Radio についての次の内容に注意してください。

1. XOR Radio のデフォルト動作ステータスは 2.4GHz です。

2. 2.4 GHz から 5 GHz へアンテナ内蔵アクセス ポイントの XOR Radio の設定を変更できます。また、その逆も可能です。アンテナ外付けアクセス ポイントでは、XOR Radio で設定を変更する前に外部アンテナが DART コネクタに接続されていることが必要です。
3. XOR（2.4 GHz）Radio が 5 GHz で動作するように設定されると、5 GHz 専用 Radio から 100 MHz 以上チャネルを離す必要があります。
4. XOR Radio がアンテナ内蔵アクセス ポイントで 5 GHz モードで動作するように設定されると、送信出力（tx）の出力は固定され、変更はできません。

XOR（2.4 GHz）Radio を 2800 および 3800 シリーズのアクセス ポイントで、5 GHz で動作するように設定するには、次の手順を実行します。

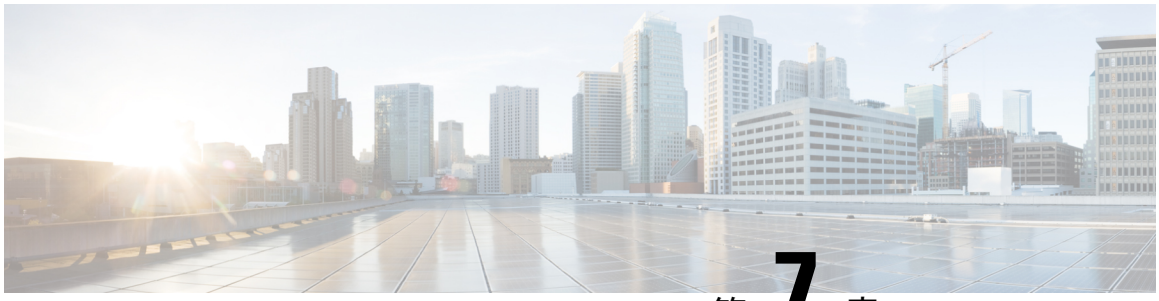
```
(Cisco Controller) >config 802.11-abgn disable ap
(Cisco Controller) >config 802.11-abgn role ap manual client-serving
(Cisco Controller) >config 802.11-abgn band ap ap 5GHz
(Cisco Controller) >config 802.11-abgn enable ap
```

5 GHz で動作する XOR Radio をチャネル 40 に設定するには、次の手順を実行します。

```
(Cisco Controller) >config 802.11-abgn disable ap
(Cisco Controller) >config 802.11-abgn channel ap ap 40
(Cisco Controller) >config 802.11-abgn enable ap
```

5 GHz で動作する XOR Radio のチャネル幅を 40 MHz に設定するには、次の手順を実行します。

```
(Cisco Controller) >config 802.11-abgn disable ap
(Cisco Controller) >config 802.11-abgn chan_width ap 40
(Cisco Controller) >config 802.11-abgn enable ap
```



第 7 章

ワイヤレス ネットワークの作成

WLAN

Cisco Mobility Express ソリューションは最大 16 個の WLAN をサポートします。各 WLAN には、一意の WLAN ID（1 ～ 16）、一意のプロファイル名、SSID が割り当てられます。また、異なるセキュリティ ポリシーを割り当てることもできます。

アクセス ポイントは、すべてのアクティブな WLAN SSID をブロードキャストし、WLAN ごとに定義するポリシーを適用します。

Cisco Mobility Express ソリューションでは、いくつかの WLAN セキュリティ オプションがサポートされます。主なオプションは次のとおりです。

1. Open
2. WPA2 パーソナル

3. WPA2 エンタープライズ（外部 RADIUS、AP）

ゲスト WLAN については、いくつかの機能がサポートされます。

1. CMX ゲスト接続
2. WPA2 パーソナル
3. キャプティブ ポータル（AP）
4. キャプティブ ポータル（外部 Web サーバ）

従業員 WLAN の作成

WPA2 パーソナルを使用した従業員 WLAN の作成

手順

ステップ 1 [Wireless Settings] > [WLANs] に移動してから、[Add new WLAN] ボタンをクリックします。[Add new WLAN] ウィンドウがポップアップ表示されます。

ステップ 2 [Add new WLAN] ウィンドウの [General] ページで、以下を設定します。

a) **プロファイル名**を入力します。
b) **SSID** を入力します。

ステップ 3 [WLAN Security] をクリックし、以下を設定します。

a) [Security] で *WPA2* パーソナルを選択します。
b) **パスフレーズ**を入力し、**パスフレーズ** を確認します。

ステップ 4 [Apply] をクリックします。

WPA2 エンタープライズおよび外部 RADIUS サーバを使用した従業員 WLAN の作成

手順

ステップ 1 [Wireless Settings] > [WLANs] に移動して、[Add new WLAN] ボタンをクリックします。[Add new WLAN] ウィンドウがポップアップ表示されます。

ステップ 2 [Add new WLAN] ウィンドウの [General] ページで、以下を設定します。

a) **プロファイル名**を入力します。

b) **SSID** を入力します。

ステップ 3 [WLAN Security] をクリックし、以下を設定します。

a) [Security Type] で **WPA2 エンタープライズ**を選択します。

b) [Authentication Server] で**[External Radius]** を選択します。

ステップ 4 RADIUS サーバを追加し、以下を設定します。

- RADIUS IP を入力します
- RADIUS ポートを入力します
- Shared Secret を入力します
- [tick] アイコンをクリックします

ステップ 5 [Apply] をクリックします。

WPA2エンタープライズおよび認証サーバとしてAPを使用した従業員WLANの作成

手順

ステップ 1 [Wireless Settings] > [WLANs] に移動して、[Add new WLAN] ボタンをクリックします。[Add new WLAN] ウィンドウがポップアップ表示されます。

ステップ 2 [Add new WLAN] ウィンドウの [General] ページで、以下を設定します。

a) **プロファイル名**を入力します。

b) **SSID** を入力します。

ステップ 3 [WLAN Security] をクリックし、以下を設定します。

a) [Security] で **WPA2 エンタープライズ**を選択します。

b) [Authentication Server] で **AP** を選択します。

（注） APは、コントローラ機能を実行しているマスターAPです。この使用例では、コントローラは認証サーバであるため、ローカル WLAN ユーザ アカウントは、クライアントの接続するコントローラに存在する必要があります。

ステップ 4 [Apply] をクリックします。

WPA2 エンタープライズ/外部 RADIUS および MAC フィルタリングを使用した従業員 WLAN の作成

手順

ステップ 1 [Wireless Settings] > [WLANs] に移動して、[Add new WLAN] ボタンをクリックします。[Add new WLAN] ウィンドウがポップアップ表示されます。

ステップ 2 [Add new WLAN] ウィンドウの [General] タブで、以下を設定します。

- **プロファイル名**を入力します。
- **SSID** を入力します。

ステップ 3 [WLAN Security] タブをクリックし、以下を設定します。

- [MAC Filtering] を有効にします
- [Security Type] で [WPA2 Enterprise] を選択します。
- [Authentication Server] で [External RADIUS] を選択します。
- ドロップダウン リストから [RADIUS Compatibility] を選択します
- ドロップダウン リストから [MAC Delimiter] を選択します

ステップ 4 RADIUS サーバを追加し、以下を設定します。

- **RADIUS IP** を入力します
- **RADIUS ポート**を入力します
- **Shared Secret** を入力します
- [tick] アイコンをクリックします。

ステップ 5 [Apply] をクリックします。

WLAN でのセントラル Web 認証サポート

ユーザは Web 認証 SSID に接続します。実際にはオープンな MAC フィルタリングであり、レイヤ 3 セキュリティではありません。

1. ユーザがブラウザを開きます。
2. WLC がゲスト ポータルにリダイレクトします。
3. ユーザがポータルで認証されます。

4. ISEが、ユーザが有効であることをコントローラに示すためのRADIUS認可変更（CoA-UDP ポート 1700）を送信し、最終的にアクセス コントロール リスト（ACL）などの RADIUS 属性をプッシュします。

WLAN でのセントラル Web 認証サポート

セントラル Web 認証を使用すると、ゲスト ユーザは、ポータルにリダイレクトされてからデバイス登録やセルフプロビジョニングを実施することで、ネットワークにアクセスできるようになります。CWA のフローには、次の処理が含まれます。

1. ユーザはWeb認証SSIDに接続します。実際にはオープンなMACフィルタリングであり、レイヤ 3 セキュリティではありません。
2. ユーザがブラウザを開きます。
3. WLC がゲスト ポータルにリダイレクトします。
4. ユーザがポータルで認証されます。
5. ISEが、ユーザが有効であることをコントローラに示すためのRADIUS認可変更（CoA-UDP ポート 1700）を送信し、最終的にアクセス コントロール リスト（ACL）などの RADIUS 属性をプッシュします。

セントラル Web 認証方式の WLAN を作成するには、次の手順に従います。

手順

ステップ 1 [Wireless Settings] > [WLANs] に移動し、[Add new WLAN/RLAN] をクリックします。

ステップ 2 [Security Type] で [Central Web Auth] を選択します。

ステップ 3 [Add the RADIUS Authentication Server] をクリックし、デバイス登録用のポータルをホストしているサーバを追加します。

ステップ 4 [Apply] をクリックします。

（注） CWA WLAN 作成の一環として、事前認証 ACL が自動的に作成され、AAA オーバーライド、CoA、ISE NAC が WLAN で有効になります。

（注） CWA を機能させるには、さらに ISE を設定する必要があります。

ゲスト WLAN の作成

Cisco Mobility Express 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。WLANをゲストユーザアクセス専用に設定するために、[WLAN Security] タブの下の [Guest Network] を有効にします。

CMX Connect のキャプティブ ポータルを使用したゲスト WLAN の作成

手順

ステップ 1 [Wireless Settings] > [WLANs] に移動して、[Add new WLAN] ボタンをクリックします。[Add new WLAN] ウィンドウがポップアップ表示されます。

ステップ 2 [Add new WLAN] ウィンドウの [General] タブで、以下を設定します。

- **プロファイル名**を入力します。
- **SSID** を入力します。

ステップ 3 [WLAN Security] タブの下の [Guest Network] を有効にします。

ステップ 4 [Captive Portal] で **CMX Connect** を選択します。

ステップ 5 **キャプティブ ポータルの URL** を入力します。

（注） キャプティブ ポータルの URL は、https://yya7lc.cmxcisco.com/visitor/login 形式にする必要があります。**yya7lc** は CMX Cloud のアカウント ID です。

ステップ 6 [Apply] をクリックします。

（注） 追加の手順が、キャプティブ ポータル、アクセス ポイントがあるサイトおよびサイトに関連付けられているキャプティブ ポータルを作成するために CMX Cloud 側で必要です。

内部スプラッシュ ページを使用したゲスト WLAN の作成

ゲスト WLAN に接続しているクライアントのオンボードに使用できる Mobility Express コントローラにビルトインされた内部スプラッシュ ページがあります。この内部スプラッシュ ページでは、カスタマイズされたバンドルをアップロードしてページをカスタマイズすることもできます。カスタマイズされた内部スプラッシュ ページをアップロードするには、[Wireless Settings] > [Guest WLANs] に移動します。[Page Type] で **[Customized]** を選択し、[Upload] ボタンをクリックして、カスタマイズされたページのバンドルをアップロードします。

内部スプラッシュ ページのために、Cisco Mobility Express は**アクセス タイプ**の複数のオプションをサポートします。サポートしているアクセス タイプは次のとおりです。

1. ローカル ユーザ アカウント
2. Web 許諾
3. 電子メール アドレス
4. RADIUS
5. WPA2 パーソナル

手順

ステップ 1 [Wireless Settings] > [WLANs] に移動して、[Add new WLAN] ボタンをクリックします。[Add new WLAN] ウィンドウがポップアップ表示されます。

ステップ 2 [Add new WLAN] ウィンドウの [General] タブで、以下を設定します。

- プロファイル名を入力します。
- SSID を入力します。

ステップ 3 [WLAN Security] タブの下の [Guest Network] を有効にします。

ステップ 4 [Captive Portal] で**内部スプラッシュ ページ**を選択します。

ステップ 5 必要に応じて、次の**アクセス タイプ**のうちの 1 つを選択します。

1. **ローカル ユーザ アカウント**：スプラッシュ ページは、ネットワーク アクセスを許可する前に、コントローラによって認証する必要があるユーザ名とパスワードの入力をユーザに表示します。ローカル WLAN ユーザは、ゲスト クライアントが接続するコントローラで作成する必要があります。
2. **Web 許諾**：スプラッシュ ページは、ネットワーク アクセスが許可される前に許諾をユーザに表示します。
3. **電子メール アドレス**：スプラッシュ ページは、ネットワーク アクセスが許可される前に電子メール アドレスの入力をユーザに表示します。
4. **RADIUS**：スプラッシュ ページは、ネットワーク アクセスが許可される前に RADIUS サーバで認証する必要があるユーザ名とパスワードの入力をユーザに表示します。[Access Type] で **RADIUS** を選択し、RADIUS サーバの設定を入力します。
5. **WPA2 パーソナル**：これは、L2 + L3 の例（Web 許諾）です。レイヤ 2 PSK セキュリティ認証が最初に行われ、次に、ネットワーク アクセスが許可される前にスプラッシュ ページが許諾をユーザに表示します。[Access Type] で **WPA2 パーソナル**を選択し、**パスフレーズ**を入力します。

ステップ 6 [Apply] をクリックします。

外部スプラッシュ ページを使用したゲスト WLAN の作成

外部スプラッシュ ページは、外部 Web サーバに存在します。内部スプラッシュ ページと同様に、Cisco Mobility Express は、外部スプラッシュ ページを使用して**アクセス タイプ**の複数のオプションをサポートします。サポートしているアクセス タイプは次のとおりです。

1. ローカル ユーザ アカウント
2. Web 許諾

3. 電子メール アドレス
4. RADIUS
5. WPA2 パーソナル

手順

ステップ 1 [Wireless Settings] > [WLANs] に移動して、[Add new WLAN] ボタンをクリックします。[Add new WLAN] ウィンドウがポップアップ表示されます。

ステップ 2 [Add new WLAN] ウィンドウの [General] タブで、以下を設定します。

- **プロファイル名**を入力します。
- **SSID** を入力します。

ステップ 3 [WLAN Security] タブの下の [Guest Network] を有効にします。

ステップ 4 [Captive Portal] で**外部スプラッシュ ページ**を選択します。

ステップ 5 必要に応じて、次の**アクセス タイプ**のうちの 1 つを選択します。

1. **ローカル ユーザ アカウント**：スプラッシュ ページは、ネットワーク アクセスを許可する前に、コントローラによって認証する必要があるユーザ名とパスワードの入力をユーザに表示します。ローカル WLAN ユーザは、ゲスト クライアントが接続するコントローラで作成する必要があります。
2. **Web 許諾**：スプラッシュ ページは、ネットワーク アクセスが許可される前に許諾をユーザに表示します。
3. **電子メール アドレス**：スプラッシュ ページは、ネットワーク アクセスが許可される前に電子メール アドレスの入力をユーザに表示します。
4. **RADIUS**：スプラッシュ ページは、ネットワーク アクセスが許可される前に RADIUS サーバで認証する必要があるユーザ名とパスワードの入力をユーザに表示します。[Access Type] で **RADIUS** を選択し、RADIUS サーバの設定を入力します。
5. **WPA2 パーソナル**：これは、L2 + L3 の例（Web 許諾）です。レイヤ 2 PSK セキュリティ認証が最初に行われ、次に、ネットワーク アクセスが許可される前にスプラッシュ ページが許諾をユーザに表示します。[Access Type] で **WPA2 パーソナル**を選択し、**パスフレーズ**を入力します。

ステップ 6 [Apply] をクリックします。

ウォールド ガーデン（DNS 事前認証 ACL）

クライアントがゲスト WLAN に接続した際、通常、スプラッシュ ページまたはゲスト ポータルは、認証が成功するまでインターネットアクセスをブロックするように設定されています。認証を完了させるためには、アクセスを許可する Web サイトの特定のドメインと IP アドレスを追加する必要があります。

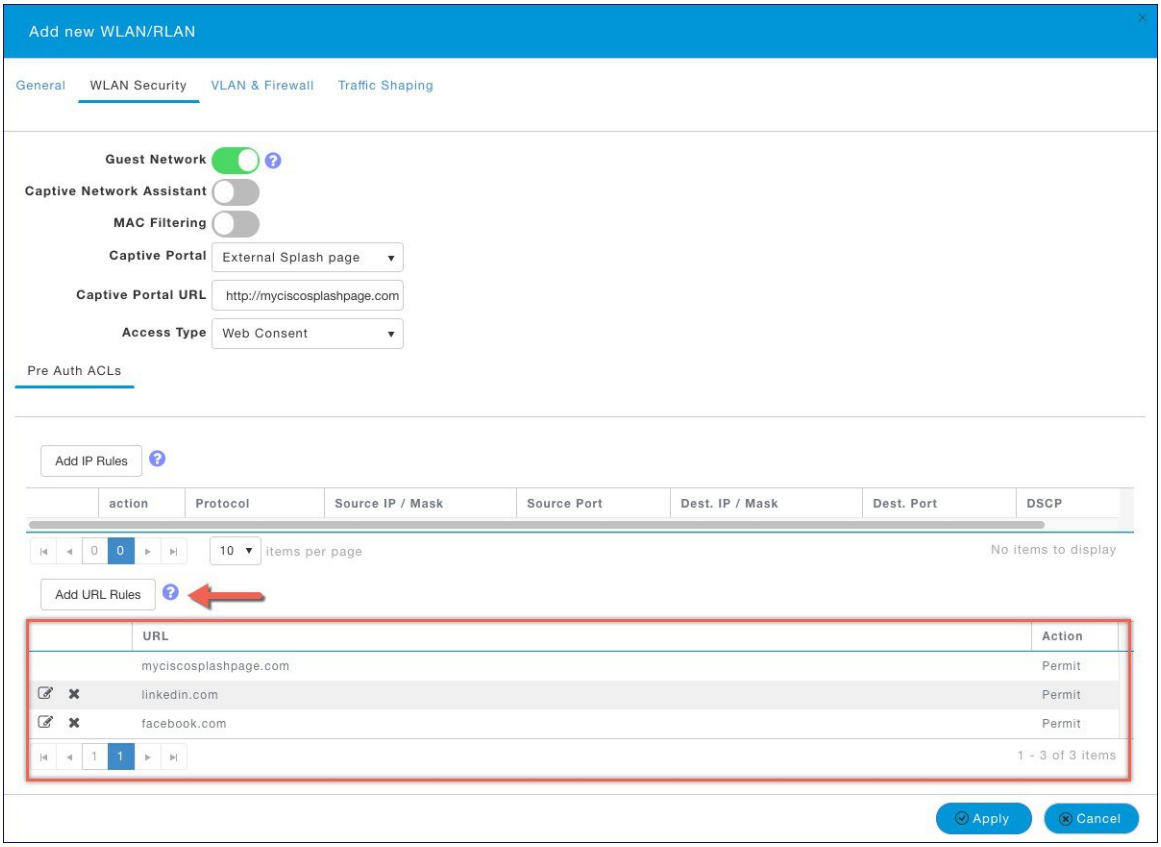
リリース 8.7 以降では、WLAN 上に DNS 事前認証 ACL と IPv4 ベースの事前認証 ACL を設定できます。1 つの ACL につき最大 20 の URL ルールがサポートされます。各 URL の長さは最大 255 文字です。URL ではワイルドカードもサポートされています。

手順

ステップ 1 [Wireless Settings] > [WLANs] > [Add new WLAN/RLAN] に移動します。

ステップ 2 [General] タブで、必要に応じて WLAN の値を入力します。

ステップ 3 [WLAN Security] タブで、[Guest Network] を有効にします。[External Splash Page] として [Captive Portal] を選択し、[Captive Portal URL] を入力します。[Access Type] として [Web Consent] を選択します。[DNS Pre-Auth ACLs] を追加するには、[Add URL Rules] ボタンをクリックし、許可または拒否する URL を追加します。



ステップ 4 [Apply] をクリックします。

Web 認証の内部スプラッシュ ページ

Cisco Mobility Express は、デフォルトの内部ゲスト ポータルをサポートします。ユーザがインポートできるカスタマイズされた内部ゲストポータルもサポートします。

デフォルトの内部ゲスト ポータルの使用

デフォルトのゲスト ポータル ページを使用したり、カスタマイズされたゲスト ポータル ページをインポートするには、以下の手順に従います。

手順

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

ステップ 2 ゲスト WLAN ページで以下を設定します。

- **Page Type**：[Internal]（デフォルト）を選択します
- **Preview**：[Preview] ボタンをクリックして、ページをプレビューできます。
- **Display Cisco Logo**：デフォルト ページの右上隅に表示されるシスコ 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。
- **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には、このテキスト ボックスに必要な 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**：ログイン ページに独自のヘッドラインを表示するには、このテキスト ボックスに必要なテキストを入力します。最大 127 文字を入力することができます。デフォルトのヘッドラインは、「Welcome to the Cisco Wireless Network」です。
- **Page Message**：ログイン ページで独自のメッセージを表示するには、このテキスト ボックスに必要なテキストを入力します。最大 2047 文字を入力することができます。デフォルトのメッセージは、「Cisco is pleased to provide the Wireless LAN infrastructure for your network.Please login and put your air space to work.」です。

ステップ 3 [Apply] をクリックします。

カスタマイズされた内部ゲスト ポールの使用

カスタマイズされたゲスト ポータルをゲスト ユーザに表示する必要がある場合、編集した後に Cisco Mobility Express コントローラにインポートできるサンプルページを Cisco.com からダウンロードできます。ページを編集し、Cisco Mobility Express コントローラへのアップロードの準備ができた後、次の手順に従います。

手順

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

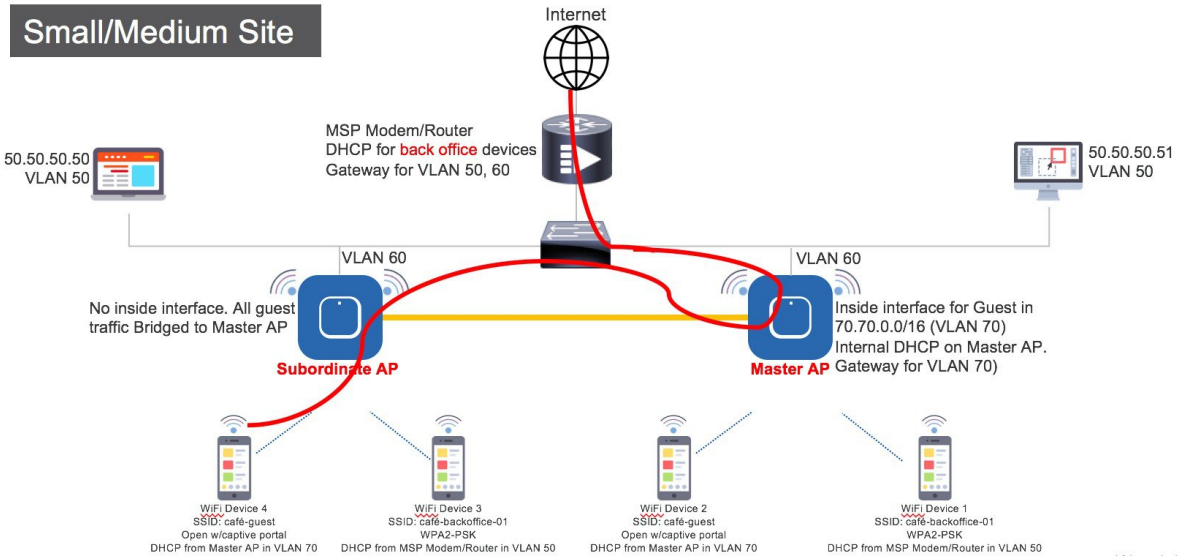
ステップ 2 ゲスト WLAN ページで以下を設定します。

- **Page Type**：**[Customized]** を選択します。
- **Customized page Bundle**：[Upload] ボタンをクリックして、カスタマイズされたページのバンドルを Mobility Express コントローラにアップロードします。
- **Preview**：[Preview] ボタンをクリックして、ゲスト ポータルをプレビューできます。
- **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には、このテキスト ボックスに必要な 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 3 [Apply] をクリックします。

ゲスト WLAN での集中型 NAT

マネージド サービス プロバイダは、1 つのサイトで 1 ～ 70 台の AP があり、同時に 300 以上のワイヤレス クライアントが接続するようなホテルや小売店に対してマネージド Wi-Fi サービスを提供します。このような場所では WAN 接続が制限されるため総スループットが通常、250 Mbps を下回ります。クライアントに対して外部 DHCP サーバを使用することは、規模の制限があるため、業務用のデバイスおよびクライアントに限定されます。ゲスト デバイスの場合、ゲストのすべてのトラフィックをマスター アクセス ポイント経由でルーティングできるように、マスター AP の内部 DHCP サーバの使用が期待されます。



ゲスト WLAN で集中型 NAT を設定するには、以下の手順に従います。

手順

ステップ 1 NAT 処理される WLAN のための DHCP プールを追加します。スコープを作成するには、[Wireless Settings] > [DHCP Server] > [Add new Pool] に移動します。[Add DHCP Pool] ウィンドウがポップアップ表示されます。[Add DHCP Pool] ウィンドウで、以下を設定します。

- WLAN のための **DHCP プール名**を入力します
- **[Pool Status]** を有効にします
- WLAN の **VLAN ID** を入力します
- DHCP クライアントの**リース期間**を入力します。デフォルトは 1 Day です
- [Network/Mask] を入力します
- DHCP プールの**開始 IP** を入力します
- DHCP プールの**終了 IP** を入力します
- DHCP プールの**デフォルト ゲートウェイ**を入力します

  （注） 集中型 NAT に接続するクライアント デバイス用のスコープの場合は、**デフォルト ゲートウェイ**として **Mobility Express コントローラ**を選択する必要があります。

- DHCP プールの**ドメイン名**（オプション）を入力します
- **ネーム サーバ**のために、必要に応じて [User Defined] を選択し、ネーム サーバの IP アドレスを入力します。OpenDNS ネーム サーバの IP アドレスが自動的に入力されている場合は OpenDNS を選択します。

- [Apply] をクリックします。

ステップ 2 WLAN を作成するには、[Wireless Settings] > [WLANs] に移動します。[Add new WLAN] または [Edit WLAN] ウィンドウで、[VLAN and Firewall] タブをクリックし、以下を設定します。

- [Client IP Management] で [Mobility Express Controller] を選択します
- [Peer to Peer Block] をチェックして、その WLAN に接続している 2 つのクライアント間の通信を無効にします
- **ネイティブ VLAN ID** を入力します。
- Mobility Express コントローラでゲスト クライアント用に作成された **DHCP スコープ**を選択します

（注） ：この WLAN のための VLAN は、AP が接続しているすべてのスイッチ ポートで設定する必要があります。

ステップ 3 [Apply] をクリックします。

WLAN ユーザの管理

Cisco Mobility Express はローカル ユーザ アカウントの作成をサポートします。このユーザは、AP を認証サーバとして設定しセキュリティとして WPA2 エンタープライズを使用するように設定されている WLAN、または**ローカル ユーザ アカウント**としての**アクセス タイプ**と内部または外部スプラッシュ ページを使用するように設定されているゲスト WLAN のために認証されます。

ローカル ユーザ アカウントを作成するには、以下の手順に従います。

手順

ステップ 1 [Wireless Settings] > [WLAN Users] に移動して、[Add WLAN User] ボタンをクリックします。

ステップ 2 WLAN ユーザとして以下を設定します。

- **User Name**：ユーザ名を入力します。
- **Guest User**：ゲスト ユーザの場合、[Guest User] チェックボックスを有効にします。
- **Lifetime**：ゲスト ユーザの場合、ユーザ アカウントの有効性を定義します。デフォルトは、作成時から 86400 秒（または 24 時間）です。
- **WLAN Profile**：ユーザが接続する WLAN を選択します。
- **Password**：ユーザ アカウントのパスワードを入力します。
- **Description**：ユーザ アカウントに関する詳細またはコメント。

• [tick] アイコンをクリックします。

WLAN での最大クライアント数の設定

Mobility Express は、最大 100 AP と 2000 クライアントをサポートします。1 つの WLAN に接続できるクライアントの最大数を制限するには、次の手順に従います。

手順

ステップ 1 [Expert View] を有効にします。

ステップ 2 [Wireless Settings] > [WLANs] > [Add new WLAN/RLAN] に移動します。

ステップ 3 [Advanced] タブで、[Maximum Allowed Clients] の値を入力するか、またはドロップダウン リストから数を選択します。

ステップ 4 [Apply] をクリックします。

AP Radio ごとの最大クライアント数の設定

Mobility Express は、radio ごとに最大 200 クライアントまでサポートします。radio に接続できるクライアントの最大数を制限するには、次の手順に従います。

手順

ステップ 1 [Expert View] を有効にします。

ステップ 2 [Wireless Settings] > [WLANs] > [Add new WLAN/RLAN] に移動します。

ステップ 3 [Advanced] タブで、[Maximum Allowed Clients per AP Radio] の値を入力します。

ステップ 4 [Apply] をクリックします。

WLAN での AAA オーバーライド

WLAN の AAA オーバーライド オプションを使用すると、WLAN で ID ネットワーキングを設定できます。ID ネットワーキングでは、AAA サーバから返された RADIUS 属性に基づいて、各 WLAN に、VLAN、アクセス コントロール リスト（ACL）、および Quality of Service（QoS）を適用できます。

手順

ステップ 1 [Expert View] を有効にします。

ステップ 2 [Wireless Settings] > [WLANs] > [Add new WLAN/RLAN] に移動します。

ステップ 3 [Advanced] タブで、[Allow AAA Override] を有効にします。

ステップ 4 [Apply] をクリックします。

双方向レート制限

AireOS 8.7 から、双方向レート制限が次の単位でサポートされます。

- クライアント単位
- BSSID 単位
- WLAN 単位

手順

ステップ 1 [Expert View] を有効にします。

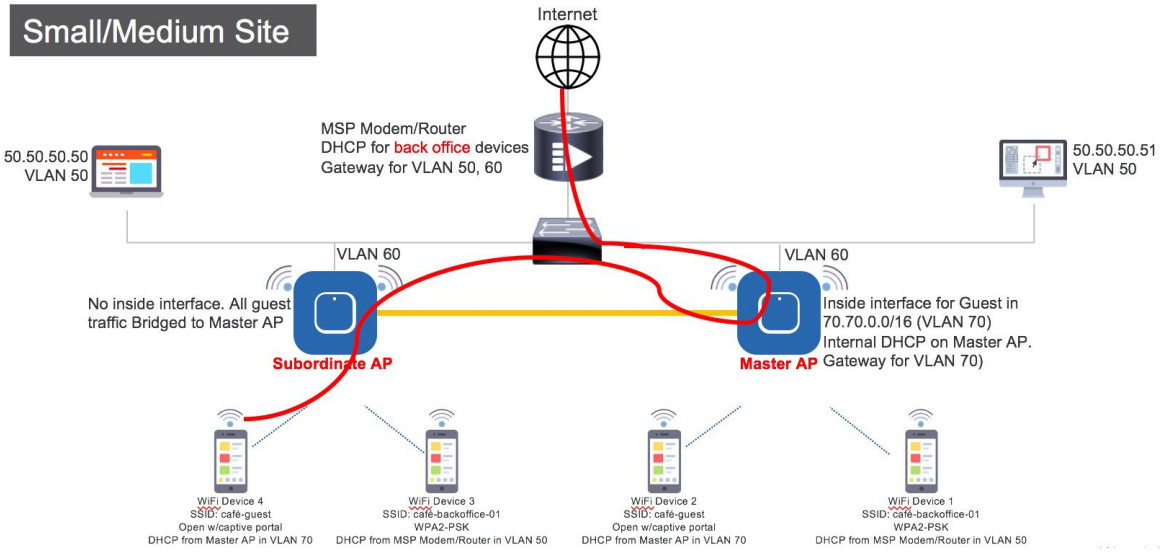
ステップ 2 [Wireless Settings] > [WLANs] > [Add new WLAN/RLAN] に移動します。

ステップ 3 [Traffic Shaping] タブで、必要に応じてレート制限を設定します。

ステップ 4 [Apply] をクリックします。

WLAN での集中型 NAT

マネージド サービス プロバイダは、1 つのサイトで 1 ～ 70 台の AP があり、同時に 300 以上のワイヤレス クライアントが接続するようなホテルや小売店に対してマネージド Wi-Fi サービスを提供します。このような場所では WAN 接続が制限されるため総スループットが通常、250 Mbps を下回ります。クライアントに対して外部 DHCP サーバを使用することは、規模の制限があるため、業務用のデバイスおよびクライアントに限定されます。ゲストデバイスの場合、ゲストのすべてのトラフィックをマスター アクセス ポイント経由でルーティングできるように、マスター AP の内部 DHCP サーバの使用が期待されます。



WLAN で集中型 NAT を設定するには、以下の手順に従います。

手順

ステップ 1 NAT 処理される WLAN のための DHCP プールを追加します。スコープを作成するには、[Wireless Settings] > [DHCP Server] > [Add new Pool] に移動します。[Add DHCP Pool] ウィンドウがポップアップ表示されます。[Add DHCP Pool] ウィンドウで、以下を設定します。

- WLAN のための **DHCP プール名**を入力します
- **[Pool Status]** を有効にします
- WLAN の **VLAN ID** を入力します
- DHCP クライアントの**リース期間**を入力します。デフォルトは 1 Day です
- [Network/Mask] を入力します
- DHCP プールの**開始 IP** を入力します
- DHCP プールの**終了 IP** を入力します
- DHCP プールの**デフォルト ゲートウェイ**を入力します

  （注） 集中型 NAT に接続するクライアント デバイス用のスコープの場合は、**デフォルト ゲートウェイ**として **Mobility Express コントローラ**を選択する必要があります。

- DHCP プールの**ドメイン名**（オプション）を入力します。
- **ネーム サーバ**のために、必要に応じて [User Defined] を選択し、ネーム サーバの IP アドレスを入力します。OpenDNS ネーム サーバの IP アドレスが自動的に入力されている場合は OpenDNS を選択します。

- [Apply] をクリックします。

（注） DHCP プールを作成する際に、集中型 NAT 用に設定された WLAN にこのスコープを使用する必要がある場合は、**デフォルト ゲートウェイ**として **Mobility Express コントローラ**を選択する**必要があります**。

ステップ 2 WLAN を作成するには、[Wireless Settings] > [WLANs] に移動します。[Add new WLAN] または [Edit WLAN] ウィンドウで、[VLAN and Firewall] タブをクリックし、以下を設定します。

- [Client IP Management] で [Mobility Express Controller] を選択します
- [Peer to Peer Block] をチェックして、その WLAN に接続している 2 つのクライアント間の通信を無効にします
- **ネイティブ VLAN ID** を入力します。
- ゲスト クライアント用に作成した **DHCP スコープ**を選択します。

（注） この WLAN のための VLAN は、AP が接続しているすべてのスイッチ ポートで設定する必要があります。

ステップ 3 [Apply] をクリックします。

WLAN でのローカル MAC フィルタリングのための MAC の追加

Cisco Mobility Express は、コントローラの WLAN での設定、および外部 RADIUS を使用して、MAC フィルタリングをサポートします。コントローラに MAC アドレスを追加して、ホワイトリストまたはブラックリストのいずれかに記載できます。コントローラへ MAC アドレスを追加するには、以下の手順に従います。

手順

ステップ 1 [Wireless Settings] > [WLAN Users] に移動して、[Local MAC Addresses] をクリックします。

ステップ 2 [Add MAC Address] をクリックします。

ステップ 3 [Add MAC Address] ウィンドウで、以下を設定します。

- **MAC Address**：デバイスの MAC アドレスを入力します
- **Description**：説明を入力します
- **Type**：この MAC がホワイトリストまたはブラックリストのいずれになるかを選択します
- **Profile Name**：ユーザが接続する WLAN を選択します

ステップ 4 [Apply] をクリックします。

WLAN Passpoint のサポート

リリース 8.5 から、Cisco Mobility Express では WLAN での Passpoint サポートが追加されています。IEEE 802.11u ベースのネットワーク情報をサポートするアクセス ポイントと、WiFi Alliance で認定された電話クライアント デバイスは連携して動作し、Passpoint 機能をサポートします。

802.11u 対応電話クライアント デバイスは、802.11u 対応 AP/Cisco Mobility Express コントローラから pre-association の際に収集された情報に基づき、ターゲット AP を検出し、選択します。電話クライアント デバイスは、デバイス内の設定ファイルに含まれるホーム OI 情報、レルム名やドメイン名などのプロビジョニング前のネットワーク情報を持ちます。さらに、電話クライアント デバイスは、挿入された SIM/USIM カードから得た IMSI データを使用してホーム ネットワーク情報を取得することもできます。

802.11u 対応 AP は、ホット スポットの所有者の詳細、ローミング パートナー、レルム リスト、3GPP セルラー情報、ドメイン名を含むさまざまな情報のリストを提供します。レルム リストは、レルム名と、関連する EAP 認証タイプ マッピングのリストも提供します。この情報を知ることは、正しい EAP 資格情報の交換を行うために、電話クライアント デバイスにとって必要不可欠です。

WLAN 設定で、単一 SSID と複数 SSID は必要な Passpoint 情報と共に設定されます。この追加の Passpoint 情報は、ビーコンまたはプローブ応答情報に追加され、Passpoint 対応の電話クライアント デバイスが AP を検出し、クエリを実行してさらなる情報を取得できるようにします。クエリ処理中に ANQP-Access Network Query プロトコルと呼ばれる標準プロトコル形式が使用されます。ここでは、プロトコルは、標準的な 2 ウェイまたは 4 ウェイ ハンドシェイク プロセスを記述し、AP と ANQP サーバから十分な情報を取得して、電話クライアント デバイスが認証され接続される最適な AP を決定します。このハンドシェイク プロセスは、GAS-Generic Advertisement Service プロトコルと呼ばれ、IEEE 802.11u 標準で定義されています。

Passpoint を設定するには、以下の手順に従います。

手順

ステップ 1 Cisco Mobility Express で [Expert View] を有効にします。 [Expert View] は次に示すように、Cisco Mobility Express WebUI のトップ バナーで使用可能です。これにより、WLAN の [802.11u] と [Hotspot 2.0] タブが有効になります。

ステップ 2 WLAN の 802.11u および Hotspot 2.0 を設定するには、[Wireless Setting] > [WLANs] に移動します。[Add new WLAN] または [Edit WLAN] ウィンドウで、[802.11u] タブおよび [Hotspot 2.0] タブをクリックし、関連する設定を入力します。

ステップ 3 [Apply] をクリックします。

Mobility Express での RLAN サポート

リリース 8.7 以降では、Cisco Mobility Express で RLAN を作成し、1810W および 1815W の有線ポートを管理できます。

Mobility Express はデータ トラフィックのローカル スイッチングをサポートしているため、RLAN データ トラフィックもローカルでスイッチされます。次の例では、802.1x 認証を使用してローカル スイッチング用の RLAN を設定し、有線アクセス用の AIR-AP1815W 上のイーサネット LAN ポートに関連付けます。設定タスクは次のとおりです。

1. 802.1x 認証を使用して RLAN を作成します。
2. AP グループを作成し、RLAN を AP グループに関連付けてから AP を AP グループに追加し、最後に有線ポートを RLAN に関連付けます。

802.1x 認証を使用して RLAN を作成するには、次の手順に従います。

手順

ステップ 1 [Wireless Settings] > [WLANs] に移動し、[Add new WLAN/RLAN] ボタンをクリックします。

ステップ 2 [General] タブで、[Type] ドロップダウンリストから [RLAN] を選択します。

ステップ 3 [Profile Name] を入力します。

ステップ 4 [RLAN Security] で、[Security Type] に [802.1x] を選択します。

ステップ 5 有線クライアントに 802.1x 認証を使用するので、[Add RADIUS Authentication Server] をクリックして RADIUS サーバを入力します。

ステップ 6 [VLAN & Firewall] タブで、[Use VLAN Tagging] を有効にし、データ トラフィックに使用する ID を [Native VLAN ID] と [VLAN ID] に入力します。

ステップ 7 [Apply] をクリックします。

AP グループの作成および AP グループへの 1815W の追加

AP グループを作成し、AP グループに 1815W を追加するには、次の手順に従います。

手順

ステップ 1 [Wireless Settings] > [Access Point Groups] に移動して、[Add new group] ボタンをクリックします。

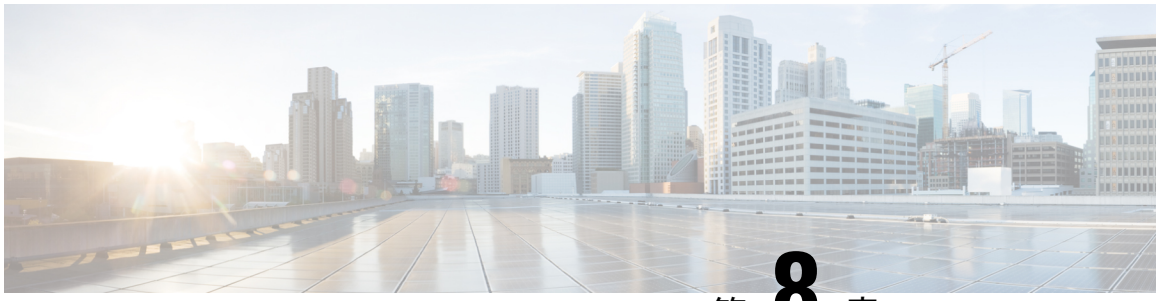
ステップ 2 [General] タブで、[AP Group Name] と [AP Group Description] を入力します。

ステップ 3 [WLANs] タブで、[Add new WLAN/RLAN] ボタンをクリックし、AP グループに追加する RLAN を選択します。

ステップ 4 [Access Points] タブで、この AP グループに追加するウォール プレート AP を選択します。

ステップ 5 [Ports] タブで、必要な LAN ポートを有効にし、そのポート用の RLAN を選択します。

ステップ 6 [Apply] をクリックします。



第 8 章

Cisco Mobility Express を使用したサービスの管理

Cisco Mobility Express 導入でサポートされるいくつかのサービスがあります。このセクションでは、次のサービスを説明します。

Application Visibility and Control（アプリケーションの可視化と制御）

Network Based Application Recognition（NBAR）は、ワイヤレス ネットワークでのアプリケーション制御を可能にし、管理性と生産性を向上させます。また、エンドツーエンドのソリューションとして Cisco の Application Visibility and Control（AVC）を拡張します。これにより、ネットワーク内のアプリケーションの完全な可視化が提供され、管理者は同時にアプリケーションの制御もできます。

NBAR は、ステートフル L4 ～ L7 分類をサポートするディープ パケット インスペクション テクノロジーです。NBAR の主な使用例として、キャパシティ プランニング、ネットワーク使用量のベースライン化、および帯域幅を消費するアプリケーションのより的確な把握があります。アプリケーションの使用状況の傾向を把握できるため、ネットワーク管理者は、ネットワーク上で輻輳が生じた場合に帯域幅消費の激しいアプリケーションから重要なアプリケーションを保護することでユーザエクスペリエンスの質を改善できます。さらに、特定のアプリケーション トラフィックの優先順位を変更したり、ドロップしたりすることもできます。AVC/NBAR2 エンジンは、特定の WLAN の QoS 設定と相互運用します。

WLAN でのアプリケーションの可視化の有効化

WLAN でのアプリケーションの可視化を設定するには、以下の手順に従います。

手順

WLAN でのアプリケーションの可視化を有効にするには、[Wireless Settings] > [WLANs] に移動します。[Add new WLAN] または [Edit WLAN] ウィンドウで、[Traffic Shaping] タブをクリックします。この WLAN でのアプリケーションの可視化を有効にするには、[Application Visibility Control] で [Enabled] を選択します。

WLAN でのアプリケーションの制御の有効化

アプリケーションの可視化が WLAN で有効になった後、さまざまなアプリケーションのための制御を追加できます。アプリケーションの制御を追加するには、2 つの方法があります。[Network Summary] ページの [Applications] ウィジェットからアプリケーションの制御を直接追加するか、[Monitoring] > [Applications] に移動し、必要に応じてアプリケーションの制御を追加できます。

[Network Summary] ページからアプリケーション制御の追加

手順

ステップ 1 [Network Summary] ページで [Applications] ウィジェットを追加します。[Applications] ウィジェットを追加するには、[Network Summary] バナーの右側にある [+] アイコンをクリックします。[Applications] ウィジェットを選択します。[Applications] ウィジェットは、Mobility Express ネットワークのクライアントが参照する上位 10 個のアプリケーションを表示します。

ステップ 2 制御を追加するアプリケーションをクリックします。[Add AVC Rule] ウィンドウがポップアップ表示されます。[Action] を選択します。[Action] は、**マーク**、**ドロップ**または**レート制限**です。**マーク**の場合は、DSCP として [Platinum]、[Gold]、[Silver]、[Bronze]または [Custom] を選択できます。カスタムを選択した場合は、DSCP 値を指定する必要があります。レート制限の場合、アプリケーションの平均レートとバースト レートを指定できます。

ステップ 3 1 つ以上の **AVC プロファイルと SSID** の組み合わせを選択します。

ステップ 4 [Apply] をクリックします。

[Applications] ページからアプリケーション制御の追加

手順

ステップ 1 [Monitoring] > [Applications] ページに移動します。

ステップ 2 制御を追加するアプリケーションをクリックします。[Add AVC Rule] ウィンドウがポップアップ表示されます。[Action] を選択します。[Action] は、**マーク**、**ドロップ**または**レート制限**で

す。**マーク**の場合は、DSCP として [Platinum]、[Gold]、[Silver]、[Bronze]または [Custom] を選択できます。カスタムを選択した場合は、DSCP 値を指定する必要があります。レート制限の場合、アプリケーションの平均レートとバースト レートを指定できます。

ステップ 3 1 つ以上の **AVC プロファイルと SSID** の組み合わせを選択します。

ステップ 4 [Apply] をクリックします。

iOS によって最適化された Wi-Fi 接続と Fast Lane

最適化された Wi-Fi 接続の設定

802.11r 対応 WLAN は、ワイヤレス クライアント デバイスのローミングを高速化します。ローミング エクスペリエンスを向上させるためには、iOS 10 を実行する iOS デバイスを 11r 対応 WLAN に接続することをお勧めします。ただし、WLAN で 11r を有効にすると、FT AKM のビーコンおよびプローブ応答を認識しないレガシー デバイスを WLAN に接続できなくなります。何らかの方法で、クライアント デバイスの機能を識別して 11r 対応デバイスを FT 対応デバイスとして WLAN に接続可能にし、同時に、レガシー デバイスを 11i/WPA2 デバイスとして接続できるようにする必要があります。

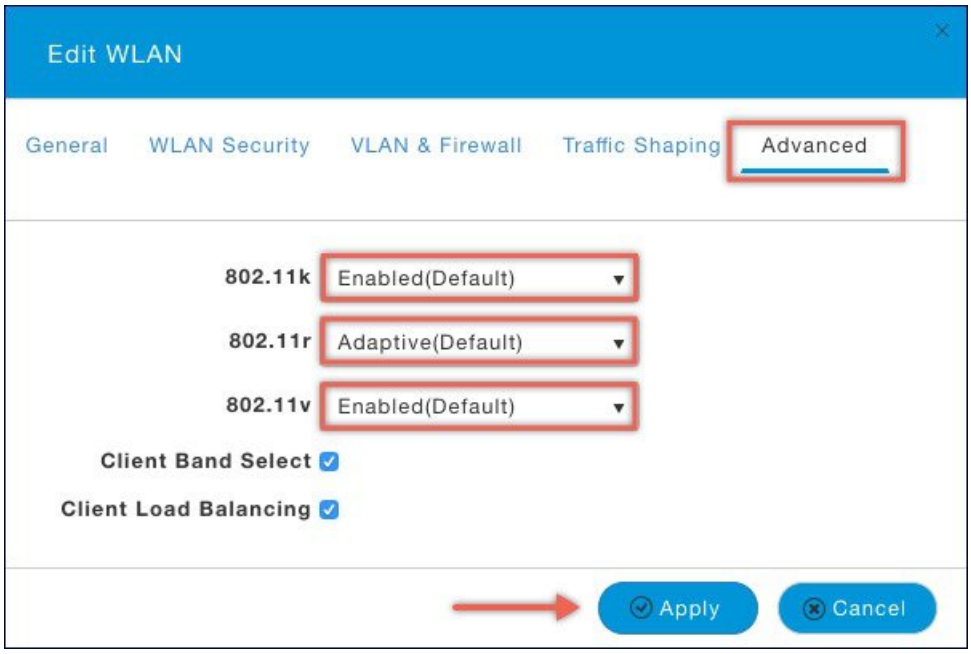
Cisco Mobility Express リリース 8.4 は、802.11i が有効な WLAN で、iOS デバイスに対してのみ 802.11r を有効にできます。対応する iOS デバイスはこの機能を識別し、その WLAN に対して FT アソシエーションを行います。シスコ ワイヤレス インフラストラクチャは、非 FT WLAN で FT アソシエーションをネゴシエートできるデバイスに対して、WLAN 上で FT アソシエーションを行うことを許可します。加えて AireOS 8.4 が動作している Mobility Express では、SSID で 802.11k と 802.11v がデフォルトで有効になっています。これらの機能により、ローミングすべきタイミングとネイバー AP に関する情報がクライアントに通知され、ローミングが必要なときに無駄にスキャニングすることがなくなるので、クライアント ローミングの改善に役立ちます。iOS デバイスはデュアルバンドをサポートするため、802.11k ネイバー リストは、iOS デバイスに対応してデュアル バンドで更新されます。

WLAN で、11k、r、v を設定するには、以下の手順に従います。

手順

ステップ 1 Cisco Mobility Express で [Expert View] を有効にします。**Expert View** は Cisco Mobility Express WebUI のトップ バナーで利用でき、標準ビューで利用できないさまざまな設定可能パラメータを有効にできます。

ステップ 2 [Wireless Settings] > [WLANs] に移動します。[Add new WLAN] または [Edit WLAN] ウィンドウで、[Advanced] タブをクリックします。このページで、必要に応じて、802.11k、r、v を設定します。



ステップ 3 [Apply] をクリックします。

Fast Lane の設定

Apple iOS デバイスは、IETF の推奨に従って QoS マーキングを行います。AireOS 8.5 が動作している Mobility Express では、CLI から Fastlane 機能を有効にすることにより、次のような便利な機能を活用できます。

- WLC QoS 設定がグローバルに最適化され、リアルタイム アプリケーションのサポートが向上します。
- iOS 10 デバイスでは、WMM TSPEC/TCLAS ネゴシエーションを実行することなくアップストリーム音声トラフィックを送信できます。インフラストラクチャがこれらの端末の音声マーキングに対応します。
- QoS プロファイルを iOS 10 デバイスに適用することで、アップストリームで QoS マーキングが適用されるアプリケーションと、ベストエフォートまたはバックグラウンドで送信されるアプリケーションを決定できます。

UI から WLAN に Fast Lane を設定するには、以下の手順に従います。

手順

ステップ 1 WLAN でアプリケーションの可視化を有効にするには、[Wireless Settings] > [WLANs] に移動します。[Add new WLAN] または [Edit WLAN] ウィンドウで、[Traffic Shaping] タブをクリックします。この WLAN で **Fastlane** を有効にするには、[Fastlane] に対して [Enabled] を選択します。

ステップ 2 [Apply] をクリックします。

Cisco Mobility Express と CMX Cloud

Cisco CMX Cloud

Cisco Connected Mobile Experiences Cloud (Cisco CMX Cloud)は、簡単でスケーラブルです。シスコの Radio インフラストラクチャとシームレスに統合することで、ワイヤレス ゲスト アクセスの提供と施設内での使用状況の分析に大きな変化をもたらします。

このクラウドが提供する Software-as-a-Service（SaaS）は、導入が容易で直感的に使用できます。これは、CMX 10.x コードに基づき、Cisco Mobility Express リリース 8.3 と互換性があります。次のサービスが提供されます。

- ゲスト アクセスのための接続：ソーシャル、セルフ登録、ショート メッセージ サービス（SMS）などのさまざまな認証方法を使用するカスタム ポータルによって、使いやすいゲストアクセス ソリューションを訪問者に提供します。
- プレゼンス分析：施設内のすべての Wi-Fi デバイス（以下「デバイス」）を検出し、滞在時間、新規訪問者対リピータ、およびピーク時間などのプレゼンスを分析します。

Cisco CMX Cloud ソリューションの互換性マトリックス

- AireOS リリース 8.3 以降を実行する Cisco Mobility Express
- Cisco Mobility Express に対応しているすべてのアクセス ポイント

Cisco CMX Cloud 導入の最小要件

CMX Cloud 導入の最小要件は次のとおりです。

1. 上記の Cisco CMX Cloud ソリューションの互換性マトリックスを確認します。
2. 推奨するブラウザは Chrome 45 以降です。
3. 60 日間のトライアルのために https://cmxcisco.com でサインアップするか、Cisco Commerce Workspace（CCW）から選択した CMX Cloud のサービス ライセンスを購入します。

プレゼンス分析のために Mobility Express で CMX Cloud サービスを有効にする

CMX Cloud アカウントを作成したら、次の手順は、マスター アクセス ポイントで CMX Cloud サービスを設定して有効化し、CMX Cloud にデータを送信できるようにすることです。設定するには、以下の手順に従います。

手順

ステップ 1 Cisco Mobility Express WebUI で、[Advanced] > [CMX] に移動します。

ステップ 2 **CMX サーバの URL**（サイト URL）を入力します。

ステップ 3 **CMX サーバ トークン**（アカウント トークン）を入力します。

ステップ 4 [Apply] をクリックします。

ヒント　設定した情報を使用してマスター AP から CMX Cloud サイトへの接続性を確認するために、[Test Link] ボタンをクリックします。

プレゼンス分析のための CMX Cloud 上のサイトの設定

CMX Cloud 上にサイトを作成して、プレゼンス分析のためにサイトにアクセス ポイントを追加するには、以下の手順に従います。

手順

ステップ 1 https://cmscisco.com/ で CMX Cloud アカウントにログインします。

ステップ 2 [Manage] > [Cloud Enabled WLC] に移動して、WLC の IP アドレスがリストに表示されることを確認します。

ステップ 3 [PRESENCE ANALYTICS] > [Manage] に移動します。[Sites] ペインが開きます。[Add Site] ボタンをクリックして、サイトを作成します。

ステップ 4 [NEW SITE] ウィンドウで、次の詳細を設定します。

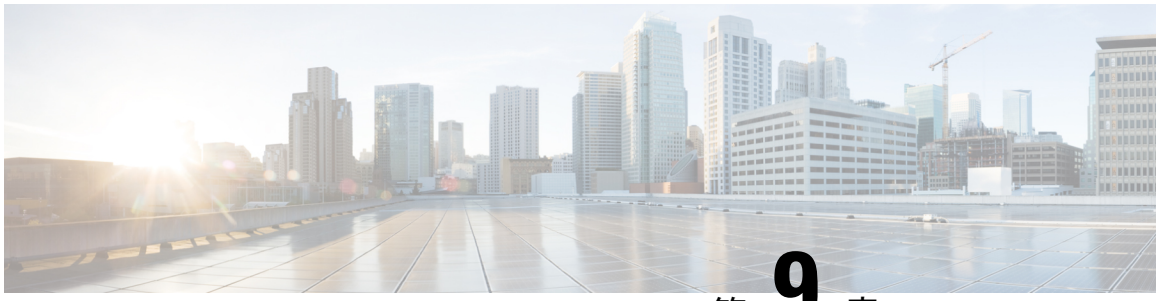
- サイトの**名前**を入力します。
- サイトの**アドレス**を入力します。
- ドロップダウン リストから**タイムゾーン**を選択します。
- **信号強度のしきい値**（Ignore、Passerby、Visitors）を選択します。
- **訪問者の最小滞在時間**（分）を入力します。

ステップ 5 [Save] をクリックしてサイトを作成します。

ステップ 6 サイトを作成したら、[PRESENCE ANALYTICS] > [Manage] の下の [Access Points] をクリックします。

ステップ 7 アクセス ポイントを選択し、[Add to Site] ボタンをクリックし、ドロップダウン リストからサイトを選択して追加します。

ステップ 8 最後に、[Presence Analytics] ダッシュボードに移動します。作成した**サイト**を選択します。数分以内に、**プレゼンス** データが読み込まれているのを確認します。



第 9 章

Cisco Mobility Express 導入の管理

アクセス ポイントの管理

リリース 8.4 から、Cisco Mobility Express は最大 100 台のアクセス ポイントまでサポートします。アクセス ポイントのリストを表示したり、パラメータを変更するには、以下の手順に従います。

手順

ステップ 1 [Wireless Settings] > [Access Points] に移動します。

（注） [P] アイコンで表示されている最初のアクセス ポイントがマスター AP であり、残りは従属アクセス ポイントです。

ステップ 2 アクセス ポイントのパラメータを変更するには、[Edit] ボタンをクリックします。[Access Point] ウィンドウは、アクセス ポイントに関する一般的なパラメータを表示します。

- Operating Mode（読み取り専用フィールド）：マスター AP の場合、このフィールドには [AP & Controller] と表示されます。他の従属 AP の場合、このフィールドには AP のみが表示されます。
- AP Mac（読み取り専用フィールド）：アクセス ポイントの MAC アドレスが表示されます。
- AP Model（読み取り専用フィールド）：アクセス ポイントのモデルの詳細が表示されます。
- 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。または、[Static IP] を選択します。[Static IP] アドレスを選択した場合は、[IP Address]、[Subnet Mask]、および [Gateway] の各フィールドを編集できます。
- AP Name：アクセス ポイント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：アクセス ポイント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。

ステップ 3 [Controller] タブ（マスター AP でのみ使用可能）で、次のパラメータを変更できます。

- System Name：Mobility Express のシステム名を入力します。
- IP Address：IP アドレスによって、コントローラの Web インターフェイスへのログイン URL が決定されます。この URL は、https://<ip address> という形式です。この IP アドレスを変更すると、ログイン URL も変更されます。
- Subnet Mask：サブネット マスクを入力します。
- Country Code：国番号を入力します。

ステップ 4 Radio 1（2.4 GHz）と Radio 2（5 GHz）で、次のパラメータを編集できます。

- Admin Mode：有効/無効にします。これは、AP で対応する Radio を有効または無効にします（802.11 b/g/n 用に 2.4 GHz または 802.11 a/n/ac 用に 5 GHz）。
- Channel：デフォルトは Automatic です。[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、Cisco Mobility Express コントローラの制御下にある各 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 が同じチャネルでブロードキャストできないようになるため、干渉やその他の通信上の問題が回避されます。2.4 GHz Radio の場合、米国では 11 のチャネル、世界の他の地域では最大で 14 のチャネルが提供されますが、これらのチャネルが隣接する AP で使用される場合、重複しないと見なせるのは 1-6-11 だけです。5GHz の Radio 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、AP にそのチャネルが静的に割り当てられます。
  - 802.11 b/g/n：1 ～ 11。

- 802.11 a/n/ac：40、44、48、52、56、60、64、100、104、108、112、116、132、136、140、149、153、157、161、165。

- Channel Width：2.4 GHz の場合は 20 MHz、5 GHz の場合は 20、40、および 80 MHz で設定されます。
- Transmit Power：[1] ～ [8]。デフォルト値は Automatic です。

これは対数目盛の送信出力、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、Radio の送信出力が調整されます。これによりトランスミッタは、フェーディング状態が発生した場合に、ほとんどの時間、最大出力未満で動作できます。これが最大値に到達するまで、送信出力が必要に応じて増加します。

ステップ 5 [Apply] をクリックします。

Mobility Express ネットワークへのアクセス ポイントの追加

アクセス ポイントを Cisco Mobility Express ネットワークに追加する際には、以下を考慮する必要があります。

アクセス ポイントのソフトウェア バージョン：追加するアクセス ポイントのソフトウェア コードがマスター AP のものと異なる場合は、マスター AP で実行しているコードのソフトウェアを、追加するアクセス ポイントにダウンロードする必要があります。マスター AP で実行しているコードをダウンロードするために、新しいアクセス ポイントに次のいずれかを設定する必要があります。

- Optimal Join：Optimal Join は、追加する AP がマスター AP と同じ AP モデルである場合に、マスター AP からコードをダウンロードできる機能です。この機能では、マスター AP 上で実行しているコードをホストする外部サーバは必要ありません。

（注） この機能は、2800、3800、1560 シリーズのアクセス ポイントでサポートされています。

- SFTP または TFTP サーバの詳細とアクセス ポイントのイメージ パス情報を、ソフトウェア アップデートのページで設定する必要があります。
- マスター AP に 8.3.102.0 以降のコードがあれば、ソフトウェア アップデートのページで Cisco.com ログイン クレデンシャルを設定し、新しいアクセス ポイントが参加するときに新しいコードが Cisco.com から自動的にダウンロードされます。

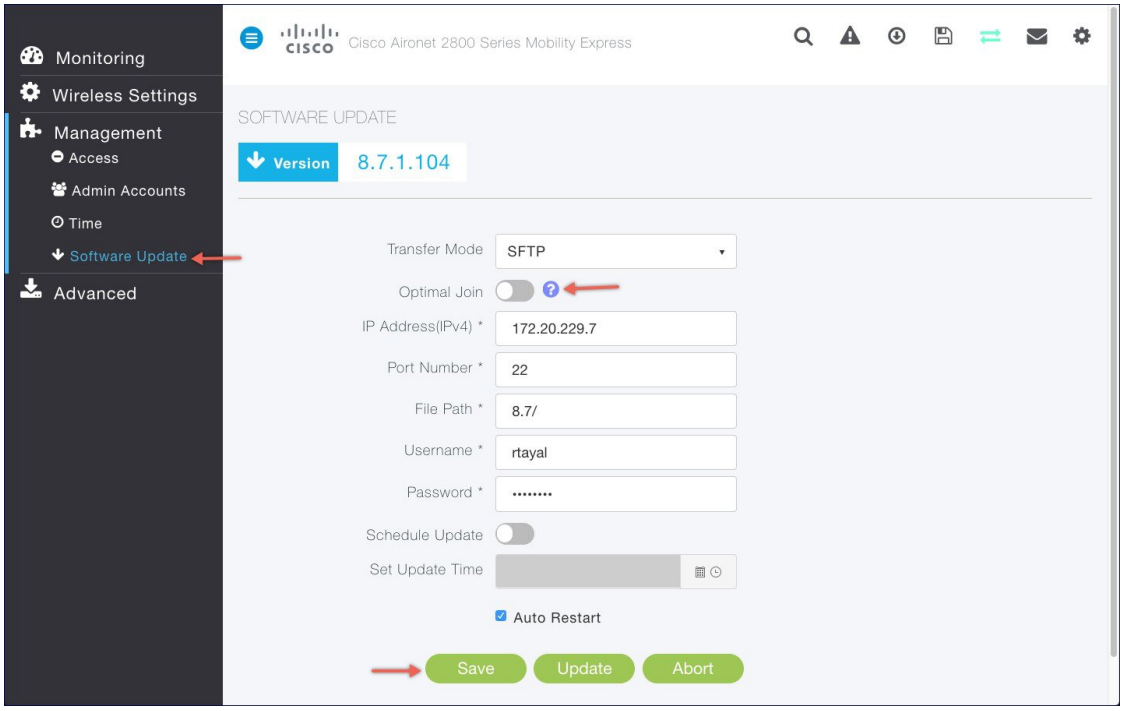
（注） Cisco.com から直接ソフトウェアをダウンロードするには、マスター AP が SMARTNet 契約の対象である必要があります。

Optimal Join：Optimal Join を有効にするには、次の手順に従います。

手順

ステップ 1 [Management] > [Software Update] に移動します。[Transfer Mode] で [TFTP] または [SFTP] を選択し、SFTP または TFTP パラメータを設定します。

ステップ 2 次に示すように [Optimal Join] を有効にします。



ステップ 3 **[Save]** をクリックします。

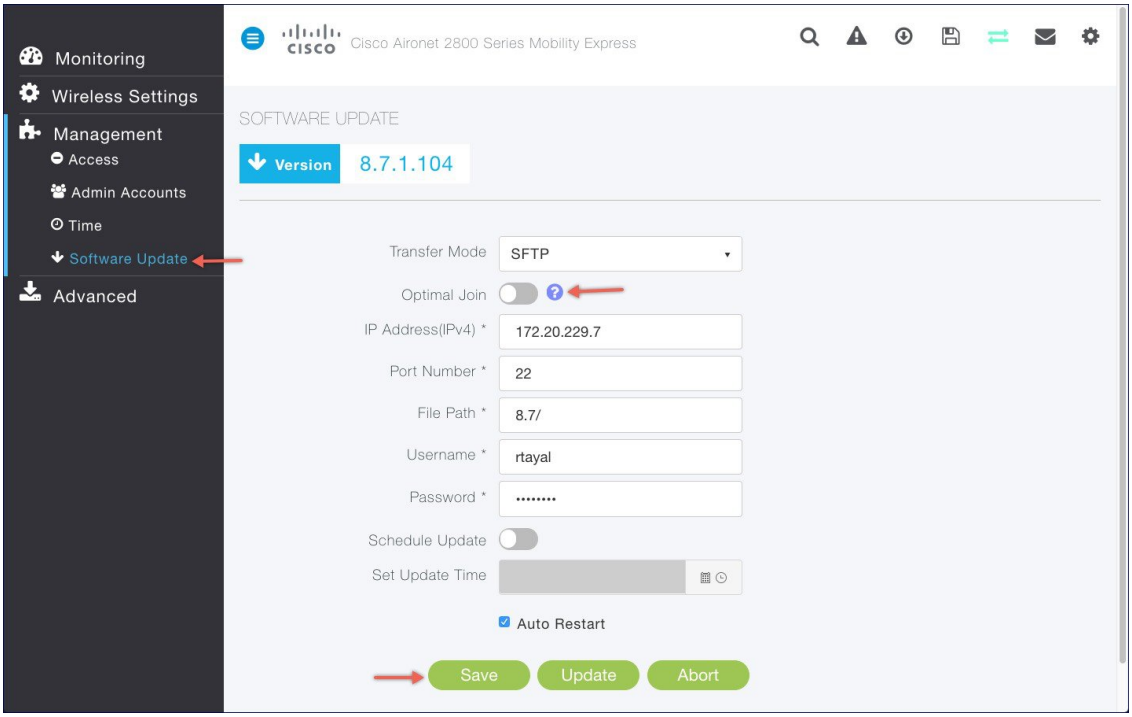
Optimal Join

Optimal Join を有効にするには、次の手順に従います。

手順

ステップ 1 [Management] > [Software Update] に移動します。[Transfer Mode] で [TFTP] または [SFTP] を選択し、SFTP または TFTP パラメータを設定します。

ステップ 2 次に示すように [Optimal Join] を有効にします。



ステップ 3 **[Save]** をクリックします。

AP Join のための SFTP または TFTP の設定

手順

ステップ 1 TFTP サーバに Cisco.com からアクセス ポイント イメージの zip ファイルをダウンロードします。バンドルのバージョンは、マスター AP 上で実行されているバンドルと同じバージョンである必要があります。個々のアクセス ポイント イメージを抽出するファイルを解凍します。

ステップ 2 [Management] > [Software Update] に移動します。[Transfer Mode] で [SFTP] または [TFTP] を選択し、SFTP または TFTP パラメータを設定します。

AP Join のための Cisco.com の設定

手順

[Management] > [Software Update] に移動します。**転送モード**で [Cisco.com] を選択し、Cisco.com のユーザ アカウントに関連するパラメータを設定します。

（注） イメージのダウンロード中にサービスの中断は発生しません。イメージのダウンロードが完了したら、AP は自動的に再起動してから、マスター AP に参加します。

802.1x サプリカントとしてのアクセス ポイントの設定

AireOS リリース 8.7 以降、Cisco Mobility Express を実行するアクセス ポイントを 802.1x サプリカントとして設定できます。Mobility Express AP は 802.1x サプリカントとして機能し、EAP-FAST、および EAP-TLS と PEAP を使用する ISE に対してスイッチによって認証されます。802.1x認証用のポートが設定されると、スイッチは、ポートに接続されたデバイスが正しく認証されるまでは、802.1x トラフィック以外のトラフィックがポートを通過することを許可しません。AP は、ME-WLC に参加する前、または参加した後のいずれかで認証されます。いずれの場合でも、アクセス ポイントが WLC に参加した後に 802.1x をスイッチに設定します。

手順

ステップ 1 [Wireless Settings] > [Access Points] に移動します。

ステップ 2 [Global AP Configuration] ボタンをクリックして、[Credentials(802.1x)] タブで次の項目を設定します。

- **[Username]**
- **[Password]**
- **[Enable Password]**

ステップ 3 [EAP Method and LSC AP Auth State] を選択します。

ステップ 4 [Apply] をクリックします。

RF プロファイルの設定

AireOS リリース 8.6 以降、Cisco Mobility Express は事前に構築された 6 つの RF プロファイルと RF プロファイルの作成をサポートしています。

RF プロファイルを使用すると、共通のカバレッジ ゾーンを共有する AP グループを調整し、そのカバレッジ ゾーン内の AP に対する RRM の動作を選択的に変更できます。たとえば、多くのユーザが集まる、または会合するエリアに、大学が高密度の AP を展開する場合があります。この場合は、同一チャネル干渉を管理しながら、セル密度に対処するために、データ レートと電力の両方を操作する必要があります。隣接エリアでは、通常のカバレッジが提供されますが、そのような操作によって高密度エリアのカバレッジが失われることがあります。RF プロファイルと AP グループを使用すると、異なる環境やカバレッジ ゾーンで動作する AP グループに対する RF 設定を最適化できます。RF プロファイルは、802.11 radio 用に作成されます。RF プロファイルは、AP グループに属するすべての AP に適用され、そのグループ内のすべての AP に同じプロファイルが設定されます。RF プロファイルを使用して、データ レートおよび電力（TPC）値を制御できます。RF プロファイル内のビルドを AP グループに関連付けたり、新しい RF プロファイルを作成してから AP グループに関連付けることができます。

RF プロファイルの設定

RF プロファイルを設定するために、Cisco Mobility Express で *Expert View* を有効にします。***Expert View*** は次に示すように Cisco Mobility Express WebUI のトップ バナーで利用でき、標準ビューで利用できないさまざまな設定可能パラメータを有効にできます。

手順

ステップ 1 [Advanced] > [RF Profiles] に移動します。

ステップ 2 [Add new RF Profile] ボタンをクリックします。

ステップ 3 [General] タブで、次の項目を設定します。

- [RF Profile Name]
- [RF Profile Description]
- [Band]
- [Maximum clients per radio]
- [RxSOP Threshold]
- [Multicast datarates]

ステップ 4 [802.11] タブで、次の項目を設定します。

- [Data rates]
- [MCS Settings]

ステップ 5 [RRM] タブで、次の項目を設定します。

- Channel Width
- [Select DCS Channels]

ステップ 6 [Client Distribution] タブで、次の項目を設定します。

- [Window]（0 ～ 20 クライアント）
- [Denial]（1 ～ 10）

アクセス ポイント グループの設定

AP グループを設定するために、Cisco Mobility Express で **Expert View** を有効にします。**Expert View** は Cisco Mobility Express WebUI のトップ バナーで利用でき、標準ビューで利用できないさまざまな設定可能パラメータを有効にできます。

手順

ステップ 1 [Wireless Settings] > [Access Point Groups] に移動します。

ステップ 2 [Add new group button] をクリックします。

ステップ 3 [General] タブで、次の項目を設定します。

- **[AP Group Name]**
- **[AP Group Description]**
- **[NAS-ID]（オプション）**
- **[Venue Group]（オプション）**
- **[Venue Type]（オプション）**

ステップ 4 [WLANs] タブで、[Add WLAN] ボタンをクリックして、WLAN を AP グループに追加します。

ステップ 5 [Access Points] タブで、AP グループに追加する必要があるアクセス ポイントを選択します。

ステップ 6 [RF Profiles] タブで、2.4 および 5.0 GHz 帯の RF プロファイルを選択します。RF プロファイルがこの AP グループに適用されます。

ステップ 7 [Apply] をクリックします。

アクセス ポイント グループの設定

AireOS リリース 8.6 以降、Cisco Mobility Express は、ワイヤレス コントローラ機能を実行している AP のモデルに応じて、最大 100 の AP グループをサポートします。

AP グループは、ワイヤレス ネットワーク内のアクセス ポイントを論理的にグループ化したものです。AP グループではロケーションベースのサービスが可能です。つまり、ある一連のアクセス ポイントの SSID と異なる一連のアクセス ポイントの別の SSID をブロードキャストする場合は、AP グループを作成し、適宜アクセス ポイントを追加することで実行できます。

（注） Mobility Express では最大 50 個の AP グループがサポートされ、1 つの AP グループには最大 100 個の AP を追加できます。

管理アクセスの設定

Mobility Express コントローラの [Management Access] 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のインターフェイスです。また、コントローラとアクセス ポイント間の通信にも使用されます。

Mobility Express コントローラでサポートされる管理アクセスには次の 4 つのタイプがあります。

1. **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。HTTP アクセス モードは、セキュアな接続ではありません。
2. **HTTPS Access**：HTTPS アクセス モードを有効にして、Web ブラウザで https://ip-address を使用してコントローラの GUI にアクセス可能にするには、[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。HTTPS アクセス モードは、セキュアな接続です。
3. **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。Telnet アクセス モードは、セキュアな接続ではありません。
4. **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、データを暗号化しセキュア 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。SSHv2 アクセス モードは、セキュアな接続です。

コントローラの異なるタイプの管理アクセスを有効または無効にするには、次の手順を実行します。

手順

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

ステップ 2 各アクセス タイプについて、[Enabled] または [Disabled] を選択します。

（注） 少なくとも 1 つのアクセス タイプを有効にする必要があります。いずれも有効にしない場合、管理ユーザが Mobility Express コントローラからロックアウトされるため、アクセスを再度提供するためには、コンソールを使用して変更する必要があります。

ステップ 3 変更を送信するには、[Apply] をクリックします。

Admin アカウントの管理

Cisco Mobility Express は、Admin アカウントの作成をサポートしており、認証されていないユーザがコントローラを再設定したり設定を表示するのを防止します。Admin ユーザ アカウントは次の 3 つのアクセス レベルでサポートされます。

1. 読み取り/書き込み：読み取りと書き込みの権限を持つアカウントには完全なプロビジョニングとモニタリング機能があります。
2. 読み取り専用：読み取り専用の権限を持つアカウントは、モニタリング機能のみですべての画面を参照できます。
3. ロビー アンバサダー：ロビー アンバサダーは、Cisco Mobility Express でゲスト ユーザ アカウントを作成して管理できます。ロビーアンバサダーは、限定的な設定権限を持ち、ゲスト アカウントを管理するために使用する Web ページのみにアクセスできます。

（注） ローカル ユーザ データベースは、最大エントリ数が 2048（デフォルト値）に制限されています。データベースは、ローカル管理ユーザ（ロビー アンバサダーを含む）、ローカル ネットワーク ユーザ（ゲスト ユーザを含む）、MAC フィルタ エントリ、除外リスト エントリで共有されます。これらを合わせて、最大値を超えることはできません。

Admin ユーザを作成するには、次の手順に従います。

手順

ステップ 1 [Management] > [Admin Accounts] に移動し、[Add New User] ボタンをクリックします。

ステップ 2 Admin ユーザ アカウントを設定するには、以下を入力します。

- **Account Name**：Admin ユーザ名を入力します。ユーザ名では大文字と小文字が区別され、最大で 24 文字の ASCII 文字を使用できます。ユーザ名に、スペースを含めることはできません。また、一意にする必要があります。
- **Access**：Admin アカウントのために、[Read/Write]、[Read Only] または [Lobby Ambassador] アクセスを選択します。
- **New Password & Confirm Password**：次のルールに従って、Admin ユーザ アカウントにパスワードを入力します。
  - パスワードでは大文字と小文字が区別されます。スペースは使用できません。
  - パスワードは、次のすべてのクラスの文字を 8 文字以上含む必要があります。
    - 小文字の英字
    - 大文字の英字
    - 数字
    - 特殊文字
    - パスワード内で同じ文字を連続して 4 回以上繰り返すことはできません。
    - パスワードに、Cisco という語または Admin ユーザ名は使用できません。さらに、これらの語の文字を逆順にしたもの、大文字を小文字に変更したもの、i を 1、|、または ! に置き換えたもの、o を 0 に置き換えたもの、s を $ に置き換えたものを使用することもできません。

ステップ 3 [tick] アイコンをクリックします。

TACACS+ および RADIUS サーバの管理

リリース 8.5 から、Cisco Mobility Express は最大で 6 つの RADIUS および 3 つの TACACS サーバをサポートします。RADIUS と TACACS+ サーバを設定するために、Cisco Mobility Express で **Expert View** を有効にします。 **Expert View** は Cisco Mobility Express WebUI のトップ バナーで利用でき、標準ビューで利用できないさまざまな設定可能パラメータを有効にできます。

TACACS+ サーバの追加

手順

ステップ 1 [Management] > [Admin Accounts] に移動します。

ステップ 2 TACACS+ サーバを追加するには、[TACACS+] タブをクリックします。[Add TACACS+ Authentication Server] ボタンをクリックし、次を入力します。

- Server Index：1 から 3 を選択します
- State：[state] を有効化します
- Server IP Address：TACACS+ サーバの IPv4 アドレスを入力します
- Shared Secret：shared secret を入力します
- Port Number：TACACS+ サーバとの通信に使用されているポート番号を入力します
- Server Timeout：サーバ タイムアウトを入力します

ステップ 3 同じことを RADIUS 承認サーバで行います。

RADIUS サーバの追加

手順

ステップ 1 [Management] > [Admin Accounts] に移動します。

ステップ 2 RADIUS サーバを追加するには、[RADIUS] タブをクリックします。[Add RADIUS Authentication Server] ボタンをクリックし、次を入力します。

- Server Index：1 から 6 を選択します
- State：[state] を有効化します
- Server IP Address：RADIUS サーバの IPv4 アドレスを入力します
- Shared Secret：shared secret を入力します
- Port Number：RADIUS サーバとの通信に使用されているポート番号を入力します
- Server Timeout：サーバ タイムアウトを入力します

ステップ 3 同じことを RADIUS 承認サーバで行います。

AP SSH クレデンシャルの設定

Cisco Mobility Express では、AP SSH クレデンシャルはデフォルトでコントローラのクレデンシャルとして設定されています。すべての AP で AP SSH クレデンシャルを変更するには、次の手順に従います。

手順

ステップ 1 [Wireless Settings] > [Access Points] に移動します。

ステップ 2 [Global AP Configuration] ボタンをクリックして、[Credentials(SSH)] タブで次の項目を設定します。

- **[Username]**
- **[Password]**
- **[Enable Password]**

ステップ 3 [Apply] をクリックします。

Admin ユーザ優先順位の管理

リリース 8.5 より前では、Cisco Mobility Express の Admin アカウントは、コントローラでローカルに作成されました。リリース 8.5 TACACS+ および RADIUS サーバは、Admin ユーザの認証にも使用できます。

複数のデータベースが設定されている場合、Admin アカウントのユーザ優先順位を設定することが重要です。優先順位を設定するには、以下の手順に従います。

手順

ステップ 1 Cisco Mobility Express で [Expert View] を有効にします。**Expert View** は Cisco Mobility Express WebUI のトップ バナーで利用でき、標準ビューで利用できないさまざまな設定可能パラメータを有効にできます。

ステップ 2 [Management] > [Admin Accounts] に移動し、[Management User Priority Order] をクリックします。

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

ステップ 3 TACACS+ と RADIUS 間の優先順位を変更するには、いずれかをクリックし、上下に移動します。ローカルの Admin アカウントは、優先順位 3 に移動できませんのでご注意ください。1 または 2 のいずれかのみです。

Cisco Mobility Express の時間の管理

最初の Wireless Express セットアップ ウィザードを実行する際に、Cisco Mobility Express コントローラのシステムの日付と時刻が通常設定されます。

NTP サーバの設定

Wireless Express のセットアップ時に日付と時刻を設定しなかった場合、日付と時刻を同期化するために Network Time Protocol（NTP）サーバを 3 つまで設定できます。タイム ゾーンはクロックを補正するために設定できます。

タイム ゾーンと NTP サーバを設定するには、以下の手順に従います。

手順

ステップ 1 [Management] > [Time] に移動します。

ステップ 2 適切な**時間帯**を選択します。

ステップ 3 **NTP のポーリング間隔**を入力します。ポーリング間隔の範囲は 3600 ～ 604800 秒です。

ステップ 4 NTP サーバを追加するには、[Add NTP Server] ボタンをクリックして、以下を設定します。

- **NTP Index**：1、2、または 3 のいずれかです。
- **NTP Server**：これは、NTP サーバの IP アドレス、NTP サーバ名またはプールです。最大 3 つの NTP サーバがサポートされます。
- [tick] アイコンをクリックします。

（注） コントローラが再起動されるたび、およびユーザ定義のポーリング間隔ごとに、日時が NTP サーバと同期されます。

Cisco Mobility Express ソフトウェアのアップデート

Cisco Mobility Express コントローラのソフトウェア アップデートは、コントローラの Web インターフェイスを使用して実行できます。ソフトウェア アップデートによって、コントローラと、すべての従属しているアクセスポイントの両方の更新が保証されます。

コントローラに参加する AP は、自分のソフトウェアのバージョンをマスター AP のバージョンと比較し、不一致の場合はソフトウェア アップデートを要求します。ソフトウェア アップデートでは、[Software Update] ページで**転送モード**と対応する詳細を設定する必要があります。

（注） マスターAPはAPイメージを持っていません。これは、設定された**転送モード**からソフトウェア アップデートを要求しているアクセス ポイントへの新しいソフトウェアの転送を容易にします。

アクセス ポイントでのソフトウェア ダウンロードは、ソフトウェアを同時にダウンロードしている AP が 5 台以下になるように自動的に順序付けられ、アップグレードが必要な AP すべてが新しいイメージのダウンロードを完了するまで、そのキューの更新を続けます。

Cisco Mobility Express のソフトウェア アップデートでは、次の**転送モード**がサポートされます。

1. Cisco.com
2. HTTP
3. SFTP
4. TFTP

（注） イメージの事前ダウンロード中にサービスが中断されることはありません。イメージの事前ダウンロードがすべての AP で完了した後に、Mobility Express ネットワークを手動で再起動するか、または再起動をスケジュール設定して実行します。

Cisco.com 転送モードを使用したソフトウェア アップデート

Cisco.com 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 ポイントで動作します。以下の要件は、Cisco.com からソフトウェア アップデートする際に満たしている必要があります。

- インターネット アクセスは、Cisco.com から AP へのソフトウェア ダウンロードに必要です。ただし、プロキシは不要です。
- ユーザ名とパスワードがそろった、有効な Cisco.com（CCO）アカウント。
- ユーザごとの EULA 承認。マスター AP にのみ（ネットワークのすべての AP ではありません）SMARTNet 契約が必要です。契約がないとソフトウェア アップデートは開始しません。

（注） Cisco.com からのソフトウェア アップデートは、GUI によってのみサポートされます。

Cisco.com 転送モードを使用するソフトウェア アップデートを実行するには、以下の手順に従います。

手順

ステップ 1 Cisco.com によるソフトウェア アップデートを行うには、[Management] > [Software Update] に移動して以下を設定します。

- [Transfer Mode] で [Cisco.com] を選択します。
- **Cisco.com のユーザ名**を入力します。
- **Cisco.com のパスワード**を入力します。
- [Automatically Check for Updates] を有効にします。確認は 30 日に一度行われます。
- [Check Now] をクリックして、最新のソフトウェア リリースと Cisco.com 推奨のソフトウェア リリースを取得します。

ステップ 2 [Apply] をクリックします。

ステップ 3 [Update] をクリックしてソフトウェア アップデート ウィザードを開始します。

ステップ 4 ソフトウェア アップデート ウィザードで、推奨されるソフトウェア リリースまたは最新のソフトウェア リリースを選択します。[Next] をクリックします。

ステップ 5 ソフトウェア アップデートをすぐに開始するためには、 [Update Now]、または [Schedule the Update for Later] を選択します。

（注） [Schedule the Update for Later] を選択した場合は、[Set Update Time] フィールドを設定します。

ステップ 6 ソフトウェア アップデートが完了した後に、ネットワーク内のすべてのアクセス ポイントの自動再起動が必要な場合は、[Auto Restart] チェックボックスをクリックします。[Next] をクリックします。

ステップ 7 [Confirm] をクリックしてソフトウェア アップデートを開始します。

個々のアクセス ポイントのダウンロード進捗をモニタするには、[Predownload image status] を展開します。

HTTP 転送モードを使用したソフトウェア アップデート

Mobility Express 導入でアクセス ポイントのモデルが同じ場合、ソフトウェア アップデートを実行するために HTTP 転送モードを使用できます。HTTP 転送モードでは、ローカル マシンからアクセス ポイントのアップグレード イメージを簡単にアップロードできます。HTTP 転送モードを使用してソフトウェア アップデートを実行するには、以下の手順に従います。

手順

ステップ 1 Cisco.com からローカル マシンに AP のイメージ バンドルをダウンロードします。次の表は、リリース 8.7.102.0 のイメージを示しています。

アクセス ポイント	アクセス ポイントのイメージ バンドル。ソフトウェア アップデートに使用する個々の AP イメージが含まれます。
Cisco Aironet® 1540 シリーズ	AIR-AP1540-K9-ME-8-7-102-0.zip
Cisco Aironet® 1560 シリーズ	AIR-AP1560-K9-ME-8-7-102-0.zip
Cisco Aironet® 1815I シリーズ	AIR-AP1815-K9-ME-8-7-102-0.zip
Cisco Aironet® 1815M シリーズ	AIR-AP1815-K9-ME-8-7-102-0.zip
Cisco Aironet® 1815W シリーズ	AIR-AP1815-K9-ME-8-7-102-0.zip
Cisco Aironet® 1830 シリーズ	AIR-AP1830-K9-ME-8-7-102-0.zip
Cisco Aironet® 1850 シリーズ	AIR-AP1850-K9-ME-8-7-102-0.zip
Cisco Aironet® 2800 シリーズ	AIR-AP2800-K9-ME-8-7-102-0.zip
Cisco Aironet® 3800 シリーズ	AIR-AP3800-K9-ME-8-7-102-0.zip

ステップ 2

（注） 上記のイメージは AireOS リリース 8.4.100.0 用です。イメージ バンドルは、リリースごとに異なります。

ステップ 3 AP イメージ バンドルを解凍して、個々の AP イメージを抽出します。対応するイメージへのアクセス ポイントのマッピングは次のとおりです。

アクセス ポイント	アクセス ポイント イメージ
Cisco Aironet® 1540 シリーズ	ap1g5
Cisco Aironet® 1560 シリーズ	ap3g3
Cisco Aironet® 1815I シリーズ	ap1g5
Cisco Aironet® 1815M シリーズ	ap1g5
Cisco Aironet® 1815W シリーズ	ap1g5
Cisco Aironet® 1830 シリーズ	ap1g4
Cisco Aironet® 1850 シリーズ	ap1g4
Cisco Aironet® 2800 シリーズ	ap3g3
Cisco Aironet® 3800 シリーズ	ap3g3

ステップ 4 **HTTP** 転送モードによるソフトウェア アップデートを行うには、[Management] > [Software Update] に移動して、以下を設定します。

- [Transfer Mode] で [HTTP] を選択します。
- 自分のネットワークのアクセス ポイントに対応するローカル AP イメージを参照します。
- ソフトウェア アップデートが完了した後ネットワーク内のすべてのアクセス ポイントの自動再起動が必要な場合、[Auto Restart] チェックボックスをクリックします。

ステップ 5 [Apply] をクリックします。

ステップ 6 [Update] をクリックして、ソフトウェア アップデートを開始します。

SFTP 転送モード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。

WebUI からのアップグレード

WebUI から SFTP 転送モードを使用してソフトウェア アップデートを実行するには、次の手順に従います。

手順

ステップ 1 AP イメージ バンドルを Cisco.com から SFTP サーバにダウンロードします。

ステップ 2 AP イメージ バンドルを解凍して、個々の AP イメージを抽出します。

ステップ 3 **SFTP** 転送モードによるソフトウェア アップデートを行うには、[Management] > [Software Update] に移動して、以下を設定します。

- [Transfer Mode] で [SFTP] を選択します。
- [SFTP] サーバの [IP Address] と [Port Number] を入力します。
- SFTP サーバ上に解凍された AP イメージへの [File Path] を入力します。
- SFTP サーバの [Username] と [Password] を入力します。

（注） よくある間違いは、このパスの入力です。次の手順に進む前にこのパスを正しく入力することが重要です。個々の AP イメージをポイントしないでください。AP イメージを含むディレクトリをポイントする必要があります。

ステップ 4 ソフトウェアのダウンロードが完了した後に、ネットワーク内のすべてのアクセスポイントの自動再起動が必要な場合は、[Auto Restart] チェックボックスをオンにします。

ステップ 5 [Apply] をクリックします。

ステップ 6 [Update Now] ボタンをクリックして、ソフトウェア アップデートを開始します。

（注） 後での更新をスケジュールするには、[Set Update Time] フィールドの日時を選択し、[Schedule Later] ボタンをクリックする必要があります。再起動時間の設定は、イメージの事前ダウンロードが開始された時間から少なくとも 2 時間空けることを推奨します。これにより、Mobility Express ネットワーク上ですべてのアクセス ポイントのイメージの事前ダウンロードが完了していることが保証されます。

TFTP 転送モードを使用したソフトウェア アップデート

TFTP 転送モードによるソフトウェア アップデートは、Cisco Mobility Express 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 TFTP 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。

WebUI からのアップグレード

WebUI から TFTP 転送モードを使用するソフトウェア アップデートを実行するには、次の手順に従います。

手順

ステップ 1 AP イメージ バンドルを Cisco.com から TFTP サーバにダウンロードします。

ステップ 2 AP イメージ バンドルを解凍して、個々の AP イメージを抽出します。

ステップ 3 **TFTP** 転送モードによってソフトウェア アップデートを実行するには、[Management] > [Software Update] に移動し、以下を設定します。

- [Transfer Mode] で [TFTP] を選択します。
- [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。
- TFTP サーバの解凍された AP イメージへの**ファイル パス**を入力します。

（注） よくある間違いは、このパスの入力です。次の手順に進む前にこのパスを正しく入力することが重要です。個々の AP イメージをポイントしないでください。AP イメージを含むディレクトリをポイントする必要があります。

ステップ 4 [Apply] をクリックします。

ステップ 5 [Update Now] をクリックして、ソフトウェア アップデートを開始します。

（注） 後での更新をスケジュールするには、[Set Update Time] フィールドの日時を選択し、[Schedule Later] ボタンをクリックする必要があります。再起動時間の設定は、イメージの事前ダウンロードが開始された時間から少なくとも 2 時間空けることを推奨します。これにより、Mobility Express ネットワーク上ですべてのアクセス ポイントのイメージの事前ダウンロードが完了していることが保証されます。

CLI からのアップグレード

手順

ステップ 1 SSH または Telnet（有効な場合）によって Mobility Express コントローラを実行している AP にログインします。

ステップ 2 データ タイプを指定します。

```
(Cisco Controller) >transfer download datatype ap-image
```

ステップ 3 転送モードを指定します。

```
(Cisco Controller) >transfer download ap-images mode tftp
```

ステップ 4 TFTP サーバの IP アドレスを指定します。

```
(Cisco Controller) >transfer download ap-images serverIp <IP addr>
```

ステップ 5 TFTP サーバの AP イメージのパスを指定します。

```
(Cisco Controller) >transfer download ap-images imagePath <path to AP images>
```

（注） よくある間違いは、このパスの入力です。次の手順に進む前にこのパスを正しく入力することが重要です。個々の AP イメージをポイントしないでください。AP イメージを含むディレクトリをポイントする必要があります。

ステップ 6 AP のイメージの事前ダウンロードを開始します。

```
(Cisco Controller) >transfer download start
Mode..................................... TFTP
Data Type................................ ap-image
TFTP Server IP........................... 10.1.1.77
TFTP Packet Timeout...................... 10
TFTP Max Retries......................... 10
TFTP Path................................ ap_bundle_8.1.112.30/
This may take some time.
Are you sure you want to start? (y/N) y
TFTP Code transfer starting.
Triggered APs to pre-download the image.
Reboot the controller once AP Image pre-download is complete
```

ステップ 7 次の CLI を実行して、事前ダウンロードのステータスを確認します。

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

Total number of APs.............. 3
Number of APs
```

```
       Initiated.....................1
       Predownloading................2
       Completed predownloading......0
       Not Supported.................0
       Failed/BackedOff to Predownload...0

                    Primary    Backup  Predownload Predownload Next Retry  Retry Failure
AP Name               Image     Image     Status      Version    Time       Count Reason
---------------   ----------  ---------  --------    ---------   -------   ----  -----
AP6412.256e.0e78 8.1.112.21  8.1.112.21 Predownloading   --         NA     NA
APAOEC.F96C.D640 8.1.112.21  8.1.112.21 Predownloading   --         NA     NA
3600-gemini   8.1.112.21  8.1.112.21 Predownloading   --            NA
```

ステップ 8 アクセス ポイントのイメージの事前ダウンロードが完了するのを待ちます。

```
(Cisco Controller) >show ap image all
Total number of APs.............. 3
Number of APs
       Initiated.....................1
       Predownloading................2
       Completed predownloading......0
       Not Supported.................0
       Failed/BackedOff to Predownload...0

                    Primary    Backup  Predownload Predownload Next Retry Retry Failure
AP Name               Image     Image     Status      Version    Time      Count Reason
 ---------------   ----------  ---------  --------    ---------   -------   ----  -----
AP6412.256e.0e78 8.1.112.21  8.1.112.21 Complete     --          NA          NA
APAOEC.F96C.D640 8.1.112.21  8.1.112.21 Complete     --          NA          NA
3600-gemini   8.1.112.21  8.1.112.21 Complete   --              NA
```

ステップ 9 事前ダウンロードが完了したら、次に示すように、reset system を実行します。

```
(Cisco Controller) >reset system
The system has unsaved changes.
Would you like to save them now? (y/N) y
Configuration Saved!
System will now restart!
```

Mobility Express でのパッシブ クライアント サポート

パッシブ クライアントとは、固定 IP アドレスが設定されている、スケールやプリンタなどのワイヤレス デバイスです。これらのクライアントは、アクセス ポイントにアソシエートするとき、IP アドレス、サブネット マスク、およびゲートウェイ情報などの IP 情報を送信しません。

ローカルにスイッチされる WLAN を持つ FlexConnect AP の場合、パッシブ クライアント機能によって、ARP 要求のブロードキャストが有効になり、AP はクライアントの代わりに応答します。

（注） パッシブ クライアント サポートは、ゲストと CWA WLAN では利用できません。

AP でパッシブ クライアントを有効にするには、次の手順に従います。

手順

ステップ 1 [Expert View] を有効にします。

ステップ 2 [Wireless Settings] > [WLANs] に移動し、[Add new WLAN/RLAN] ボタンをクリックします。

ステップ 3 [Advanced] タブで、WLAN に [Passive Client] を有効にします。

ステップ 4 [Multicast IP] に値を入力します。

ステップ 5 [Apply] をクリックします。

アドバンスド RF パラメータの管理

Cisco Mobility は、管理者が設定できるいくつかの RF パラメータをサポートして、ネットワークの導入を最適化します。アドバンスド RF パラメータを管理するには、以下の手順に従います。

手順

ステップ 1 Cisco Mobility Express の [Expert View] を有効にします。**Expert View** は Cisco Mobility Express WebUI のトップ バナーで利用でき、標準ビューで利用できないさまざまな設定可能パラメータを有効にできます。

ステップ 2 [Advanced RF Parameters] の下にある、次のパラメータを使用できます。

- **2.4 GHz Band**：これはグローバル設定で、有効または無効にできます。
- **5.0 GHz Band**：これはグローバル設定で、有効または無効にできます。
- **Automatic Flexible Radio Assignment**：Cisco Mobility Express の環境にフレキシブル ラジオ アサインメントをサポートする 2800 と 3800 シリーズのアクセス ポイントがある場合、有効または無効を選択できます。
- **Optimized Roaming**：これはグローバル設定で、有効または無効にできます。
- **Event Driven RRM**：これはグローバル設定で、有効または無効にできます。
- **CleanAir Detection**：CleanAir は 2800 および 3800 シリーズのアクセス ポイントでサポートされ、有効または無効を選択できます。
- **5.0 GHz Channel Width**：グローバル設定が best に設定され、チャネル幅に 20、40、80 または 160 MHz を選択できます。
- **2.4 GHz Data Rates**：スライダを移動させて、2.4 GHz バンドでデータ レートを有効/無効にします。
- **5.0 GHz Data Rates**：スライダを移動させて、5.0 GHz バンドでデータ レートを有効/無効にします。
- **Select DCA Channels**：チャネルを選択（個々のチャネルをクリック）して、2.4 GHz、5.0 GHz バンド両方の DCA に含めることができます。

（注） チャネルに引かれている緑色の下線は、選択されていることを示します。

ステップ 3 [Apply] をクリックします。

UIを使用した、OUI、EAPデバイス証明書、EAPCA証明書のアップロード

8.7 より前では、OUI ファイル、EAP デバイス証明書、および EAP CA 証明書のアップロードは CLI からしかできませんでした。8.7 以降では、ローカル ファイル アップロード（HTP）、FTP、または TFTP を使用して WebUI からアップロードできます。

アップロードするには、次の手順に従います。

手順

ステップ 1 [Advanced] > [Controller Tools] > [Upload File] に移動します。

ステップ 2 アップロードする [File Type] を選択します。タイプは、OUI ファイル、EAP デバイス証明書、および EAP CA 証明書から選択できます。

ステップ 3 [Transfer Mode] に HTTP、FTP または TFTP を選択し、適切な詳細情報を入力します。

ステップ 4 [Transfer Mode] が [HTTP(Local Machine)] の場合は、[Browse] ボタンをクリックしてファイルをアップロードします。

ステップ 5 [Apply settings] および [Import] をクリックします。

CALEA サポート

Communications Assistance for Law Enforcement Act（CALEA）が Cisco Mobility Express リリース 8.5 からサポートされています。CALEA サーバを設定するには、以下の手順に従います。

手順

ステップ 1 Cisco Mobility Express で [Expert View] を有効にします。[Expert View] は次に示すように、Cisco Mobility Express WebUI のトップ バナーで使用可能です。

ステップ 2 [Advanced] > [Controller Tools] に移動します。[CALEA] タブをクリックし、以下を設定します。

- [CALEA status] を有効にします
- [CALEA server IP address] と [Port] を入力します
- [Sync] の間隔を分単位で入力します
- [Venue] 情報を入力します

ステップ 3 [Apply] をクリックします。

第 10 章

マスター AP のフェールオーバーおよび新しいマスターの選定

Cisco Mobility Express は、Cisco 1560、1815I、1815M、1815W、1830、1850、2800、および 3800 シリーズのアクセス ポイントでサポートされます。Cisco Mobility Express 環境でこれらのアクセス ポイントが混在している場合、マスター AP の選択プロセスは、アクティブ マスター AP のフェールオーバー時にどのアクセスポイントが（Mobility Express コントローラ機能を実行するために）選択されるかを決定します。VRRP は、新しいマスターの選択のため、マスター AP の障害を検出するために使用されます。

（注） Mobility Express は、VRID が 1 である MAC 00-00-5E-00-01-VRID を使用します。その環境内に実行している VRRP の他のインスタンスがある場合は、それらのインスタンスには 1 以外 の VRID を使用します。

マスター AP のフェールオーバー

Mobility Express ネットワークに冗長性を持たせるには、2 台以上の Mobility Express 対応のアクセス ポイントが必要です。これらのアクセス ポイントは、AP Image type を MOBILITY EXPRESS IMAGE、AP Configuration を MOBILITY EXPRESS CAPABLE にする必要があります。マスター AP の障害が発生した場合、別の Mobility Express 対応 AP がマスターとして自動的に選定されます。新しく選定されたマスター AP には、元のマスター AP と同じ IP と設定が保持されます。

（注） サポートされるアクセス ポイント数に関して、アクセス ポイント モデルごとにサポートする規模の制限が異なることを考慮すると、同じ規模制限をサポートする2台以上のアクセス ポイントを設定することを強く推奨します。たとえば、100台のアクセス ポイントをサポートする必要がある場合、少なくとも 2 台以上の 3800、2800、または両方の組み合わせが必要です。

（注） Mobility Express Image を持っているが、**AP Configuration** が **NOT MOBILITY EXPRESS CAPABLE** であるアクセスポイントは、マスター AP の選定プロセスには参加しません。

新しいマスター アクセス ポイントの選択

マスター選択プロセスは、一連の優先度に基づいています。アクティブなマスター アクセス ポイントで障害が発生すると、選択プロセスが開始され、優先度が一番高いアクセス ポイントがマスター AP として選択されます。

（注） マスター選択プロセス中に、コントローラの機能を実行しているマスター AP がダウンしていても、残りのアクセス ポイントは、スタンドアロン モードになり、接続しているクライアントとデータ トラフィックをローカルに処理し続けます。新しいマスターが選択された後で、スタンドアロン アクセス ポイントはコネクテッド モードに移行します。

前述のように、マスター アクセス ポイントの選択は、一連の優先度に基づいています。優先順位は次のとおりです。

手順

ステップ 1 **User Defined Master**：ユーザはマスター アクセス ポイントにするアクセス ポイントを選択できます。このような選択をした場合、新しいマスターは、アクティブなマスターに障害が発生してすぐに選択されることはありません。5分後も現在のマスターがアクティブでない場合は、故障していると想定され、新しいマスターの選択を開始します。手動でマスターを定義するには、以下の手順に従います。

a) [Wireless Settings] > [Access Points] に移動します。
b) アクセス ポイントのリストから、マスター AP として選択するアクセス ポイントの [Edit] アイコンをクリックします。
c) [General] タブで、[Make me Controller] ボタンをクリックします。
d) [Confirmation] ウィンドウで、[Yes] をクリックします。

（注） 以前のマスターが再起動し、選択されたアクセスポイントがすぐにコントローラ機能を起動してアクティブなマスターになります。

ステップ 2 **Next Preferred Master**：管理者は、**Next Preferred Master** UI および CLI を設定できます。これが設定されてアクティブなマスター AP に障害が発生すると、[Next Preferred Master] として設定されているものがマスターとして選択されます。[Next Preferred Master] を設定するには、以下の手順に従います。

（注） Cisco Mobility Express では、**Next Preferred Master** を 1 つだけ設定できます。

a) [Wireless Settings] > [Access Points] に移動します。
b) **Next Preferred Master** として作成する AP を編集します。
c) [Edit AP] ウィンドウで、[Set as Preferred Master] トグルを有効にします。
d) [Apply] をクリックします。

コントローラ CLI から **Next Preferred Master** を設定するには、次の手順に従ってください。

[Next Preferred Master] を設定するには、次の CLI を実行します。

```
(Cisco Controller) >config ap next-preferred-master <Cisco AP>
       <Cisco AP> Enter the name of the Cisco AP
```

[Next Preferred Master] を表示するには、次の CLI を実行します。

```
(Cisco Controller) >show ap next-preferred-master
```

[Next Preferred Master] をクリアするには、次の CLI を実行します。

```
Cisco Controller) >clear ap next-preferred-master
```

ステップ 3 **Most Capable Access Point**：最初の 2 つの優先順位が設定されていない場合、マスター AP の選択アルゴリズムはアクセス ポイントの機能に基づいて新しいマスターを選択します。たとえば、3800 が最も優先度が高く、2800、1850、1830、および最後に 1815 シリーズと続きます。

（注） 1815 シリーズのアクセス ポイントの優先度はすべて同等です。

ステップ 4 **Least Client Load**：同じ機種の複数のアクセス ポイント（たとえば複数の 3800 アクセス ポイント）の場合、最小のクライアント接続数のアクセス ポイントがマスター アクセス ポイントとして選択されます。

ステップ 5 **Lowest MAC Address**：すべてのアクセス ポイントが同じである場合、最も小さい MAC を持つアクセス ポイントがマスターとして選択されます。