Cisco Embedded Wireless Controller on Catalyst Access Points（EWC）

目次

製品概要

Cisco® Embedded Wireless Controller（EWC）on Catalyst® Access Points は、Cisco Catalyst 9100 アクセスポイントに統合されたソフトウェアベースのコントローラです。シンプルで低コストながら機能豊富な Wi-Fi アーキテクチャと、中小規模の環境向けに最適化されたエンタープライズレベルの WLAN 機能を備えています。このソリューションを活用すれば、中小規模ネットワークで大規模企業と同じ品質のユーザエクスペリエンスを実現できます。

Cisco EWC ネットワークでは、ワイヤレスコントローラ機能を実行するアクセスポイント（AP）がアクティブ AP として指定されます。このアクティブ AP によって管理される他のアクセスポイントは従属 AP と呼ばれます。

アクティブ EWC には以下の 2 つの役割があります。

- ワイヤレス LAN コントローラ（WLC）として機能し、従属 AP を管理/制御する。従属 AP は、クライアントにサービスを提供する中央管理型アクセスポイントとして機能します。
- クライアントにサービスを提供するアクセスポイントとして機能する。

サポートされるシスコ アクセスポイント

図 1.
さまざまな導入環境に対応したアクセスポイント

次の表に、EWC 機能をサポートするアクセスポイントを示します。

表 1. EWC をサポートするアクセスポイント

マスターとしてサポートされるアクセスポイント	サポートされる型番	サポートデバイス数
Cisco Catalyst 9115AXI アクセスポイント	C9115AXI-EWC-X	50 アクセスポイント、1000 クライアント
Cisco Catalyst 9115AXE アクセスポイント	C9115AXE-EWC-X	50 アクセスポイント、1000 クライアント
Cisco Catalyst 9117AXI アクセスポイント	C9117AXI-EWC-X	50 アクセスポイント、1000 クライアント
Cisco Catalyst 9120AXI アクセスポイント	C9120AXI-EWC-X	100 アクセスポイント、2000 クライアント
Cisco Catalyst 9120AXE アクセスポイント	C9120AXE-EWC-X	100 アクセスポイント、2000 クライアント
Cisco Catalyst 9120AXP アクセスポイント	C9120AXP-EWC-X	100 アクセスポイント、2000 クライアント
Cisco Catalyst 9130AXI アクセスポイント	C9130AXI-EWC-X	100 アクセスポイント、2000 クライアント
Cisco Catalyst 9130AXE アクセスポイント	C9130AXE-EWC-X	100 アクセスポイント、2000 クライアント

次の表に、従属 AP として機能するアクセスポイントを示します。

表 2. 従属 AP としてサポートされるアクセスポイント

従属 AP としてサポートされるアクセスポイント	サポートされる型番
Cisco Catalyst 9100 シリーズ	C9115AXI C9116AXE C9117AXI C9120AXI C9120AXE C9120AXP C9130AXI C9130AXE
Cisco Aironet 1800 シリーズ	AIR-AP1832I AIR-AP1852I AIR-AP1852E AIR-AP1815I AIR-AP1815W AIR-AP1842I AIR-AP1810W
Cisco Aironet 2800 シリーズ	AIR-CAP2802I AIR-CAP2802E
Cisco Aironet 3800 シリーズ	AIR-CAP3802I

従属 AP としてサポートされるアクセスポイント	サポートされる型番
	AIR-CAP3802E
Cisco Aironet 4800 シリーズ	AIR-CAP4802I
Cisco Aironet 1540 シリーズ	AIR-CAP1540
Cisco Aironet 1560 シリーズ	AIR-CAP1560
Cisco Catalyst IW6300 Heavy Duty シリーズ	IW-6300H

ソフトウェアリリース番号

Cisco EWC on Catalyst Access Points は、リリース 16.12.2s 以降でサポートされます。

相互運用性

Cisco EWC は以下と相互運用可能です。

- Cisco DNA Center 1.3.3 以降
- Cisco Connected Mobile Experiences（CMX）10.6、Cisco DNA Spaces
- Cisco Identity Services Engine（ISE）2.3、2.4、2.5 以降

はじめに

ポート

ポートは、Cisco Catalyst 9100 アクセスポイントをネットワークに接続するために使用される物理エンティティです。9100 アクセスポイントでは以下の 2 つの RJ-45 ポートを使用できます。

- 1 X 100、1000、2500、5000 マルチギガビット イーサネット（RJ-45）– IEEE 802.3bz
- 管理コンソールポート（RJ-45）

インターフェイス

インターフェイスは EWC 上の論理エンティティです。管理インターフェイス（Web UI、Telnet/SSH コマンドライン インターフェイス（CLI）、NETCONF/YANG とのテレメトリ/プログラマブル インターフェイスなど）を必ず設定し、インバンド管理に使用する必要があります。

WLAN

WLAN は、Service Set Identifier（SSID）を VLAN に関連づけるものです。セキュリティタイプ、Quality of Service（QoS）、無線ポリシー、その他のワイヤレス ネットワーク パラメータを設定します。EWC ネットワークでは最大 16 の WLAN を設定できます。WLAN は、スイッチポートでトランキングされた VLAN にマッピングできます。

スイッチの設定

EWC ネットワーク内のアクティブ AP を含むすべてのアクセスポイントは、同じレイヤ 2 ブロードキャストドメインに属している必要があります。

アクセスポイントが接続するスイッチの設定は次のようになります。

```
vlan 10
```

```
name Employee
 vlan 20
  name Guest
 vlan 122
 name Management
 interface Vlan10
 description >> Employee Network <<
 ip address 10.10.10.1 255.255.255.0
 !
 interface Vlan20
  description >> Guest Network <<
  ip address 20.20.20.1 255.255.255.0
  !
  interface Vlan122
   description >> Management and EWC Network <<
   ip address 172.20.229.2 255.255.255.0
  interface GigabitEthernet1/0/37
   description >> Connected to EWC AP<<
   switchport trunk native vlan 122
   switchport trunk allowed vlan 10,20,122
   switchport mode trunk
```

EWC の導入

EWC を導入するための前提条件

EWC ネットワークを導入するための前提条件は次のとおりです。

- Cisco EWC ネットワークのセットアップ中または通常の運用中は、同じネットワーク内に他のシスコワイヤレス コントローラ（アプライアンス/仮想を問わず）を配置できません。
- EWC ネットワークは、同じレイヤ 2 ドメインでサポートされます。
- Cisco Catalyst 9100 アクセスポイントがブートアップ時に IP アドレスを取得できるように、スイッチ上または外部に Dynamic Host Configuration Protocol（DHCP）サーバを構築します。DHCP サーバは、他の AP やワイヤレスクライアントにも IP アドレスを割り当てます。
- DHCP サーバは、デフォルトゲートウェイと DNS サーバの IP アドレスを提供する必要があります。
- ネットワークが複数モデルの AP で構成されている場合、EWC の管理インターフェイスからアクセスできる Trivial FTP（TFTP）サーバを設定する必要があります。C9800-AP-univesalk9<バージョン>.zip ファイル（Zip を解凍して）を TFTP サーバに保存します。
- 最初にセットアップする AP を決定します。この AP は Cisco EWC 機能をサポートしている必要があります。EWC を実行する Cisco Catalyst 9100 アクセスポイントをスイッチに複数接続することもできます。
- EWC をプロビジョニングして設定するために、事前に定義済みの CiscoAirProvision-<AP-MAC の末尾 4 桁> SSID に Wi-Fi 対応のラップトップ（PC）を接続する必要があります。または、Cisco Catalyst

Wireless アプリケーションがインストールされたモバイルデバイス/タブレットを使用して、EWC をプロビジョニング/設定することもできます。

- 802.1X 認証を使用する場合は、認証/認可/アカウンティング（AAA）用に RADIUS サーバが必要です。
- EWC ネットワークに参加するすべての AP で、バージョン 8.10.X または 16.12.X 以上のソフトウェアが実行されている必要があります。

EWC 対応アクセスポイントの接続

EWC 対応アクセスポイントを 9100 アクセスポイントに接続するには、次の手順を実施します。

ステップ 1. EWC 対応アクセスポイントを接続し、電源を入れます。

9100 アクセスポイントが接続するスイッチポートには、アクセスポートまたはトランクポートを利用できます。クライアントトラフィックに複数の VLAN が使用されている場合は、VLAN をトランキングするようにスイッチポートを設定する必要があります。また、管理トラフィックにはタグを付与せず、管理用に VLAN を使用する場合は、スイッチポートでネイティブ VLAN として設定する必要があります。

次に、スイッチポートの例を示します。

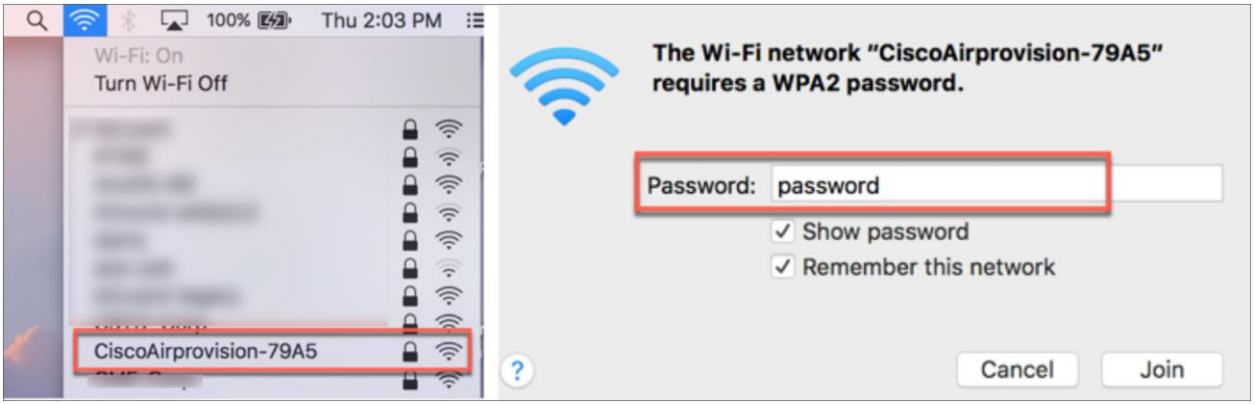
```
interface GigabitEthernet1/0/37
 description » Connected to EWC AP «
 switchport trunk native vlan 122
 switchport trunk allowed vlan 10,20,122
 switchport mode trunk
```

ステップ 2. 約 5 分待ち、アクセスポイントの LED が緑色に点灯して **CiscoAirprovision-<XXXX> SSID** のブロードキャストが開始したことを確認します。

Day-0 – 無線セットアップウィザードを使用したプロビジョニング

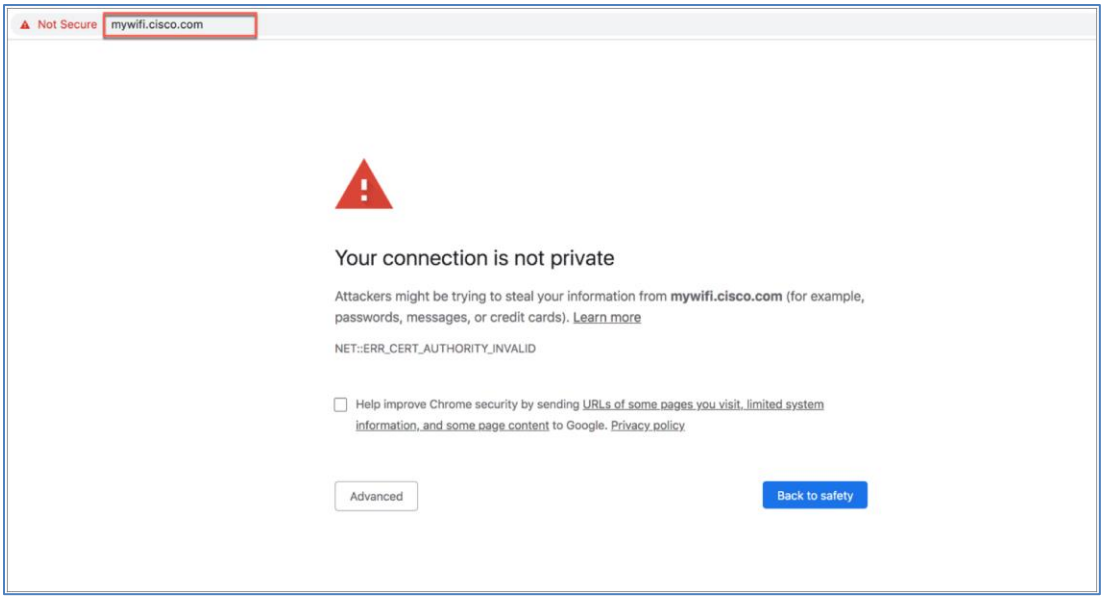
無線セットアップウィザードを使用して EWC を設定するには、次の手順を実施します。

ステップ 1. ワイヤレスクライアントまたはラップトップを **CiscoAirprovision-**<XXXX> SSID（**PSK = password**）に接続します。



注：外部に DHCP サーバが設定されている場合、クライアントは DHCP サーバから IP アドレスを取得します。

ステップ 2. サポートされているブラウザ（Chrome、Firefox、Safari、Edge）を開き、EWC Web UI で https://mywifi.cisco.com にアクセスします。

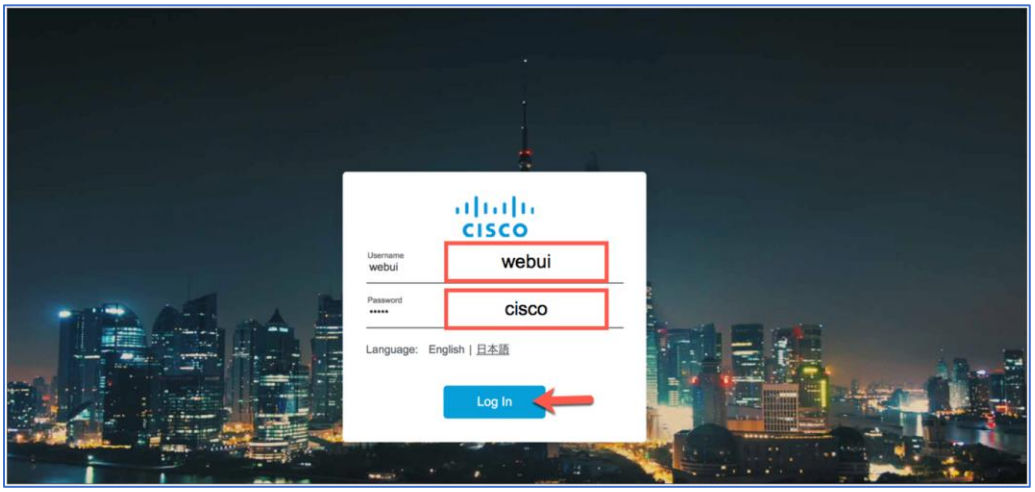


注：EWC は HTTPS に自己署名証明書を使用します。そのため、証明書がブラウザに提示されると警告メッセージが表示され、例外として続行するかどうかが確認されます。リスクを受け入れて先に進み、EWC ログインページにアクセスします。サポートされているブラウザとオペレーティングシステムは次のとおりです。

表 3. サポートされているブラウザとオペレーティングシステム

ブラウザ	バージョン	オペレーティングシステム	ステータス	回避策
Google Chrome	77.0.3865.120	macOS Mojave バージョン 10.14.6	サポート	ブラウザの警告を受け入れて進みます。
Safari	13.0.2（14608.2.40.1.3）	macOS Mojave バージョン 10.14.6	サポート	ブラウザの警告を受け入れて進みます。
Mozilla Firefox	69.0.1	macOS Mojave バージョン 10.14.6	例外が追加された場合のみサポートされます。	例外を設定します。
Mozilla Firefox	69.0.3	macOS Mojave バージョン 10.14.6	例外が追加された場合のみサポートされます。	例外を設定します。
Google Chrome	77.0.3865.90	Windows 10 バージョン 1903（OS ビルド 18362.267）	サポート	ブラウザの警告を受け入れて進みます。
Microsoft Edge	44.18362.267.0	Windows 10 バージョン 1903（OS ビルド 18362.267）	サポート	ブラウザの警告を受け入れて進みます。
Mozilla Firefox	68.02	Windows 10 バージョン 1903（OS ビルド 18362.267）	サポート	ブラウザの警告を受け入れて進みます。
Mozilla Firefox	69.0.3	Windows 10 バージョン 1903（OS ビルド 18362.267）	例外が追加された場合のみサポートされます。	例外を設定します。
Google Chrome	78.0.3904.108	macOS Catalina 10.15.1	サポート対象外	NA

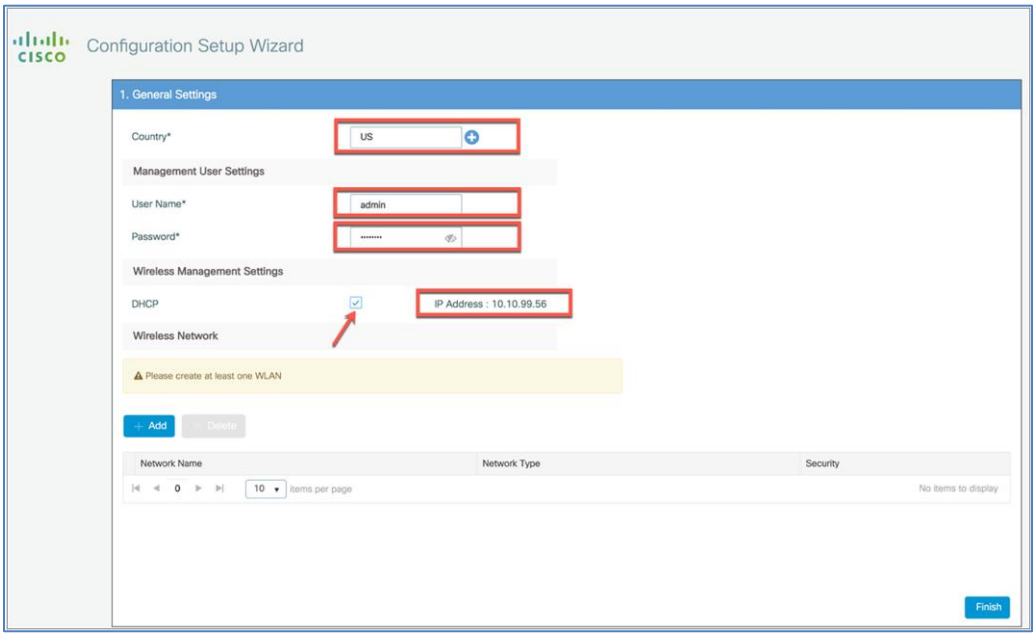
ステップ 3. [ユーザ名（Username）] = webui、[パスワード（Password）] = cisco で EWC ウィザードにログインします（GUI は日本語表示に切り替えられます）。



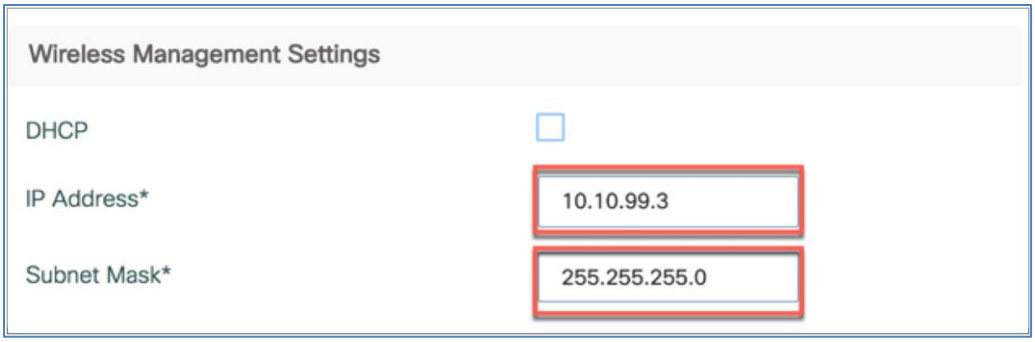
ステップ 4. [ユーザ名（Username）] と [パスワード（Password）] を設定します。[国（Country）] は、AP 規制ドメインに従って選択されます（日本は「J4」を選択してください）。

注：国コードが正しくない場合は、[+] をクリックしてドロップダウンリストから選択できます。

ワイヤレス管理 IP アドレスにはデフォルトで DHCP アドレスが設定されます。必要に応じて [DHCP] チェックボックスをオフにして設定することもできます。



次のように [IPアドレス（IP Address）] と[サブネットマスク（Subnet Mask）] を設定することで、ワイヤレス管理 IP アドレスを手動で割り当てることもできます。



ステップ 5. 最後のステップでは、WLAN を 1 つ以上作成してワイヤレスネットワークを設定します。そのために [+追加（+ Add）] をクリックします。

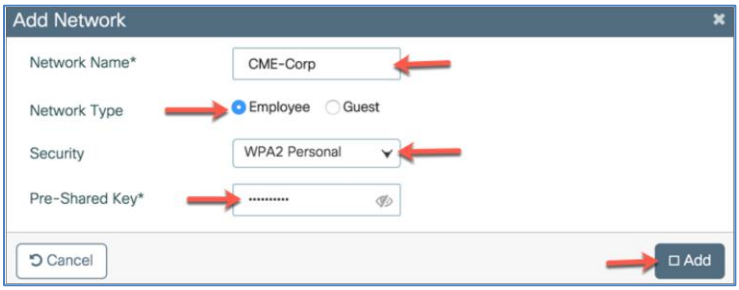
[ネットワークの追加（Add Network）] ダイアログが表示され、WLAN を設定できます。以下のように設定します。

[ネットワーク名（Network Name）] : ネットワーク名または WLAN/SSID 名を定義します。

[ネットワークタイプ（Network Type）] : [従業員（Employee）] または [ゲスト（Guest）] を選択します。[従業員（Employee）] を選択すると、[セキュリティ（Security）] タイプを選択するオプションが表示されます。

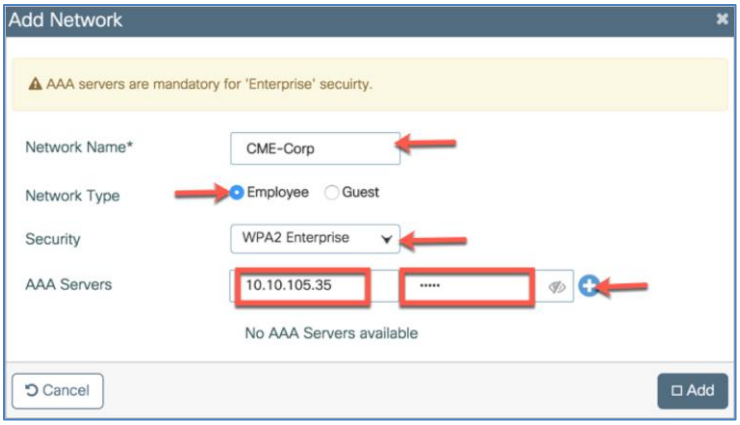
[セキュリティ（Security）] : このオプションでは、WPA2 Personal（PSK/パスワード認証）や WPA2 Enterprise（RADIUS を利用した 802.1X 認証）などの WLAN セキュリティタイプを定義します。

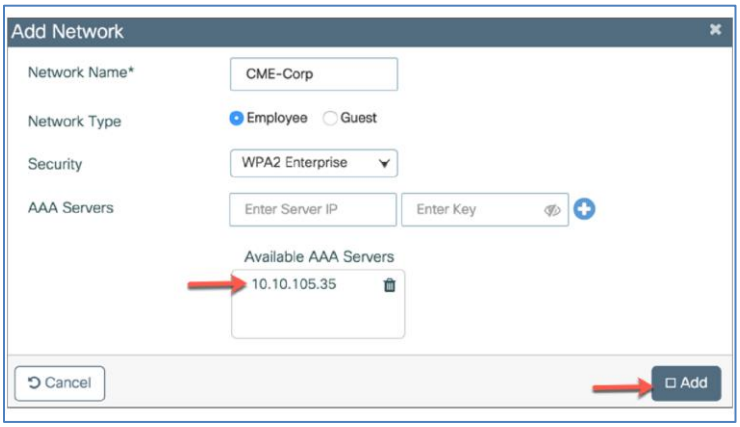
[追加（Add）] をクリックして WLAN を作成します。



[セキュリティ（Security）] タイプに [WPA2 Enterprise] を選択した場合は、AAA サーバを設定する必要があります。

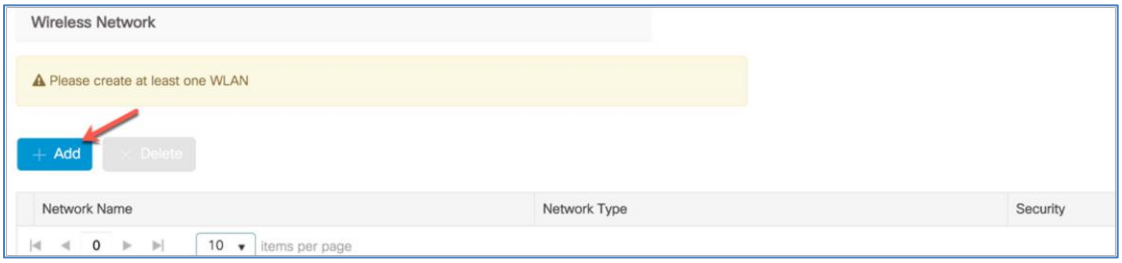
AAA サーバの IP アドレスと共有秘密を設定し、[+] をクリックします。割り当てられた AAA サーバが、[使用可能なAAAサーバ（Available AAA Servers）] のリストに表示されます。[追加（Add）] をクリックして 802.1X 対応 WLAN を設定します。





ゲスト WLAN の追加

同様に [+追加（+ Add）] をクリックしてゲスト WLAN を追加できます。



以下のように設定します。

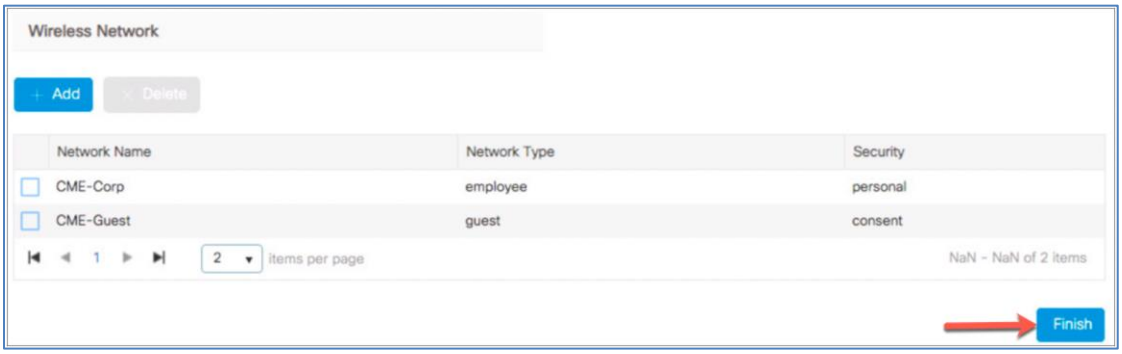
[ネットワーク名（Network Name）]：ネットワーク名または WLAN/SSID 名を定義します。

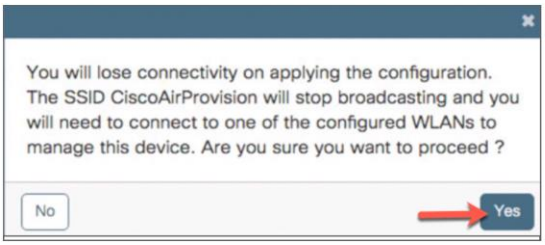
[ネットワークタイプ（Network type）]：[ゲスト（Guest）] オプションを選択します。

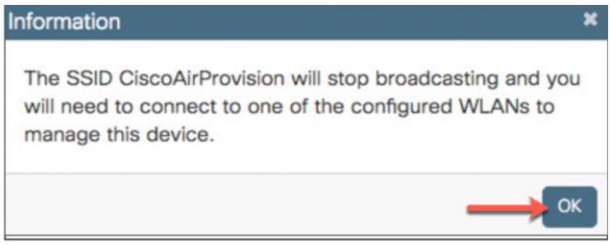
[セキュリティ（Security）]：Day-0 に [同意（Consent）] オプションがデフォルトで選択されています。

[追加（Add）] をクリックして WLAN を作成します。

ステップ 6. 設定を確認後 [完了（Finish）] をクリックして、この設定を EWC にプッシュします。ダイアログがポップアップし、CiscoAirprovision-<XXXX> SSID が無効になることを示すメッセージが表示されます。設定済みの従業員 SSID に接続してデバイスを管理する必要があります。設定が正しい場合は [はい（Yes）] をクリックし、その他の情報ダイアログで [OK] をクリックします。







アクセスポイントは**再起動されず、即設定した SSID が利用可能になります。**

必要に応じて、SSH/CLI ベースの Day-0 プロビジョニングも実施できます。

ワイヤレスクライアントから SSH ベースの Day-0 プロビジョニングを実施するには、次の手順に従います。

1. ワイヤレスクライアントを CiscoAirProvision-<XXXX> SSID に接続します。
2. **ssh -l webui mywifi.cisco.com**（パスワード = **cisco**）を実行してコントローラに SSH で接続します。
3. 接続すると Day-0 バナーが表示され、デバイスの Day-0 プロビジョニングガイドとデバイスにアクセスするためのコマンドが示されます。基本的に Day-0 デバイス プロビジョニング ガイドには、Day-0 デバイスプロビジョニングを完了するための一連の手順が記載されています（以下を参照）。

```
XYZ-MCA:~ tme$ ssh -l webui mywifi.cisco.com
The authenticity of host 'mywifi.cisco.com (10.10.10.196)' can't be established.
RSA key fingerprint is SHA256:0LASolvHdT/+FrmY6DvY+C7Bz/QSAYTr+N48QiHYaEg.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'mywifi.cisco.com,10.10.10.196' (RSA) to the list of known hosts.
Password: cisco


##############################################################################################
#                                                                                            #
#      Welcome to the Cisco Catalyst 9800-AP Embedded Wireless Controller command line interface       #
#                                                                                            #
#                     !!! Please complete the DAY0 Device Provisioning !!!                   #
#                  !!! NOTE: COMPLETE ALL THE STEPS IN PROVISIONING GUIDE !!!                #
#                                                                                            #
#                    To access the provisioning guide type the below command:                #
#                        more bootflash:ewc_day0_device_provisioning_guide                   #
#                                                                                            #
##############################################################################################

WLCC4F7.D54D.5F9C#more bootflash:ewc_day0_device_provisioning_guide

#########################################################################
# Welcome to the Cisco Catalyst 9800-AP Embedded Wireless Controller         #
# command line interface guide for DAY0 device provisioning                 #
# Copyright (c) 2019 by Cisco Systems, Inc.                                  #
#                                                                            #
# Please read carefully and execute all the steps highlighted below to       #
# complete the DAY0 device provisioning.                                     #
#                                                                            #
# 1. The SSH session will timeout if there is 5 minutes of inactivity.       #
#    In that case, please SSH back and continue the provisioning from where  #
#    it was left earlier.                                                    #
#                                                                            #
# 2. Please DO NOT save the configuration unless all the steps are           #
#    completed successfully.                                                 #
#########################################################################

Note: After completing all the steps highlighted below, the device
will be provisioned. In case if the interface GigabitEthernet0 IP address
or the Country Code needs to be changed, please do so using the WEBUI
after connecting the client to SSID Network created in Step 3A

Step 1 - Configure the Host Name (Optional)
===========================================
WLC7069.5A74.7C78#conf t
WLC7069.5A74.7C78 (config)#hostname <#host-name>
<#host-name>(config)#end

For example:
WLC7069.5A74.7C78#conf t
WLC7069.5A74.7C78(config)#hostname C9800-AP
C9800-AP(config)#end

Step 2A - Set the administrative username/password
==================================================
C9800-AP#conf t
C9800-AP(config)# username <#username> privilege 15 password <#password>
C9800-AP(config)#end
```

```
Step 2B - Configure the AP Profile
==================================
To configure the AP management username/password for AP profile,
Please use the SAME username/password configured in step 2A.

C9800-AP#conf t
C9800-AP(config)#ap profile default-ap-profile
C9800-AP(config-ap-profile)#mgmtuser username <#username> password 0 <#password> secret 0 <#password>
C9800-AP(config-ap-profile)#end

For example, to configure the AP management username and password
C9800-AP#conf t
C9800-AP(config)#ap profile default-ap-profile
C9800-AP(config-ap-profile)#mgmtuser username admin password 0 Network123 secret 0 Network123
C9800-AP(config-ap-profile)#end

Step 3A - Configure the Wireless Local Area Network
===================================================
C9800-AP#conf t
C9800-AP(config)#wlan <#wlan-profile-name> <#wlan-id> <#ssid-network-name>
C9800-AP(config-wlan)# no security wpa akm dot1x
C9800-AP(config-wlan)# security wpa psk set-key ascii 0 <#pre-shared-key>
C9800-AP(config-wlan)# security wpa akm psk
C9800-AP(config-wlan)# no shutdown
C9800-AP(config-wlan)#end

For example to configure a PSK WLAN named "employee" with pre-shared key "Cisco123"
C9800-AP#conf t
C9800-AP(config)# wlan employee 1 employee
C9800-AP(config-wlan)# no security wpa akm dot1x
C9800-AP(config-wlan)# security wpa psk set-key ascii 0 Cisco123
C9800-AP(config-wlan)# security wpa akm psk
C9800-AP(config-wlan)# no shutdown
C9800-AP(config-wlan)#end

Step 3B - Configure the Wireless Profile Policy
===============================================
The wireless profile policy name must be SAME as the <#wlan-profile-name>
configured in step 3A.

C9800-AP#conf t
C9800-AP(config)#wireless profile policy <#wlan-profile-name>
C9800-AP(config-wireless-policy)#no central association
C9800-AP(config-wireless-policy)#no central dhcp
C9800-AP(config-wireless-policy)#no central switching
C9800-AP(config-wireless-policy)#http-tlv-caching
C9800-AP(config-wireless-policy)#session-timeout 86400
C9800-AP(config-wireless-policy)#no shutdown
C9800-AP(config-wireless-policy)#end

For example to configure the profile policy for WLAN profile name "employee"
C9800-AP#conf t
C9800-AP(config)#wireless profile policy employee
C9800-AP(config-wireless-policy)#no central association
C9800-AP(config-wireless-policy)#no central dhcp
C9800-AP(config-wireless-policy)#no central switching
C9800-AP(config-wireless-policy)#http-tlv-caching
C9800-AP(config-wireless-policy)#session-timeout 86400
C9800-AP(config-wireless-policy)#no shutdown
C9800-AP(config-wireless-policy)#end
```

```
Step 3C - Configure the Default Policy Tag
==========================================
To map the WLAN to the Profile Policy, use the SAME <#wlan-profile-name>
configured in step 3A.

C9800-AP#conf t
C9800-AP(config)#wireless tag policy default-policy-tag
C9800-AP(config-policy-tag)#wlan <#wlan-profile-name> policy <#wlan-profile-name>
C9800-AP(config-policy-tag)#end

For example to map the WLAN profile name "employee" to the policy profile
name "employee" in the default policy tag
C9800-AP#conf t
C9800-AP(config)#wireless tag policy default-policy-tag
C9800-AP(config-policy-tag)#wlan employee policy employee
C9800-AP(config-policy-tag)#end
```

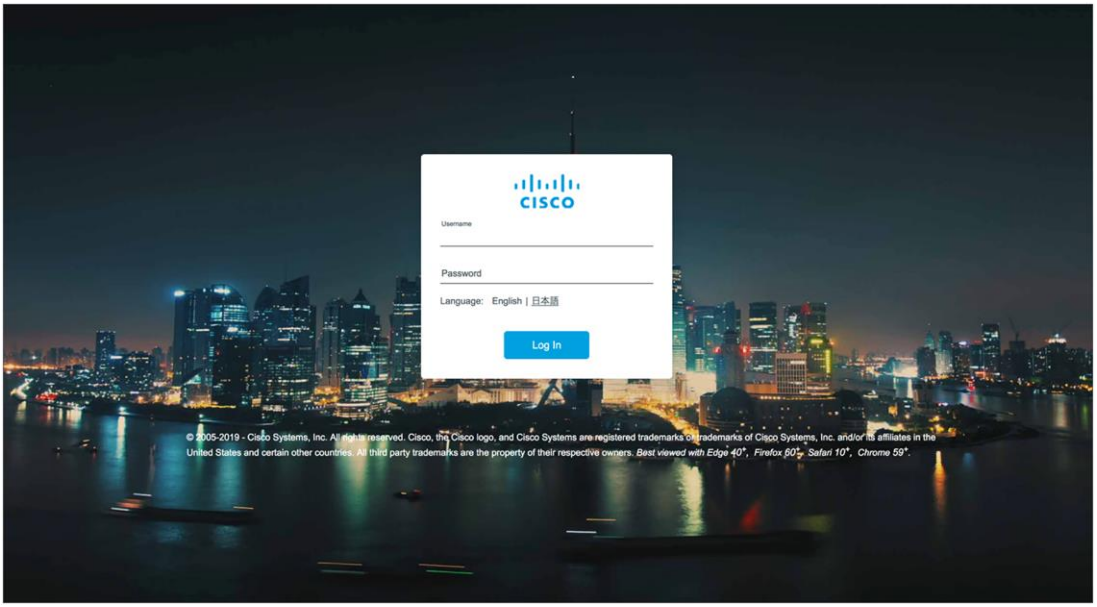
```
Step 4 - Turn on the global encryption
======================================
This config is highly recommended for the security.

Without this config, all the credentials are saved as plain text.
With this configuration, all the credentials are saved as encrypted strings.

User needs to input a "key" for password here, It's recommended to use the SAME
administrative password configured in step 2A as the key for password encryption.

C9800-AP#conf t
C9800-AP(config)#service password-encryption
C9800-AP(config)#password encryption aes
C9800-AP(config)#key config-key newpass <#password>
C9800-AP(config)#end

For example, the global encryption can be configured as below
C9800-AP#conf t
C9800-AP(config)#service password-encryption
C9800-AP(config)#password encryption aes
C9800-AP(config)#key config-key newpass Network123
C9800-AP(config)#end

Step 5 - Save the Configuration
===============================

STOP: IMPORTANT NOTE 1: YOU WILL LOSE CONNECTIVITY NOW
======================================================
When the configuration is saved, the connectivity to the SSH session
will be lost.

STOP: IMPORTANT NOTE 2: THIS IS HOW YOU CONNECT BACK
====================================================

WEBUI:
To make any further configurations to the device, please use the WEBUI.
In order to access the WEBUI, please connect the wireless client to the
Network configured in step 3A and type the URL "https://mywifi.cisco.com"
in the browser. Please use the credentials (username/password) configured
in step 2A to login to the WEBUI.

SSH:
To SSH to the device going forward, connect to the
Network created in step 3A and please use the admin username/password
configured in step 2A

NOW execute the below command to complete the device provisioning:

C9800-AP# write memory


#############################################################################
```

EWC へのログイン

EWC にログインするには、次の手順を実施します。

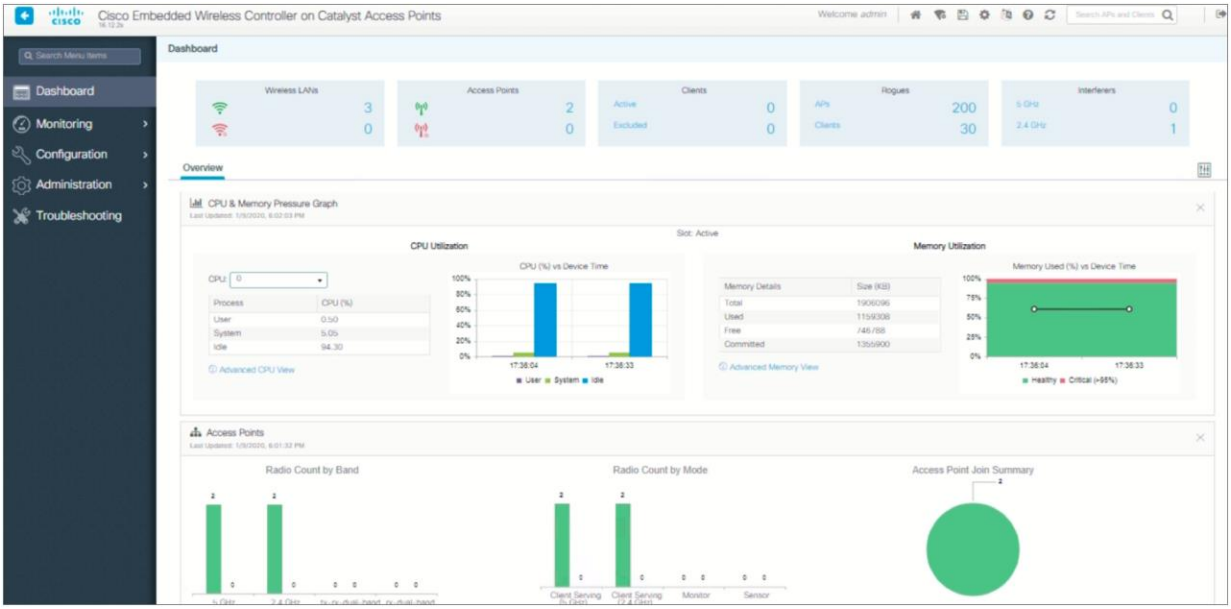
手順

ステップ 1 設定ウィザードで作成した従業員 SSID に接続します。Web ブラウザに URL（https://mywifi.cisco.com）を入力します。Cisco Catalyst EWC のログインページが表示されます。



ステップ 2 管理者のユーザ名とパスワードを入力します。

ネットワークのサマリーページがメインダッシュボードに表示されます。



注：詳細設定またはエキスパートビューを表示するには、ページの右上にある [設定（Preferences）] に移動し、[現在の設定モード（Current Configuration Mode）] を [エキスパート（Expert）] に設定して [保存（Save）] をクリックします。

EWC ネットワークのモニタリング

ネットワークサマリーの表示

モニタリングサービスにより、管理者は Cisco EWC ネットワークをモニタできます。

モニタリングダッシュボード

ネットワークサマリーページのモニタリングダッシュボードには、次の情報が表示されます。

ワイヤレスネットワーク数

アクセスポイント数

2.4 GHz および 5 GHz のアクティブクライアント数

不正な AP およびクライアント数

干渉源数

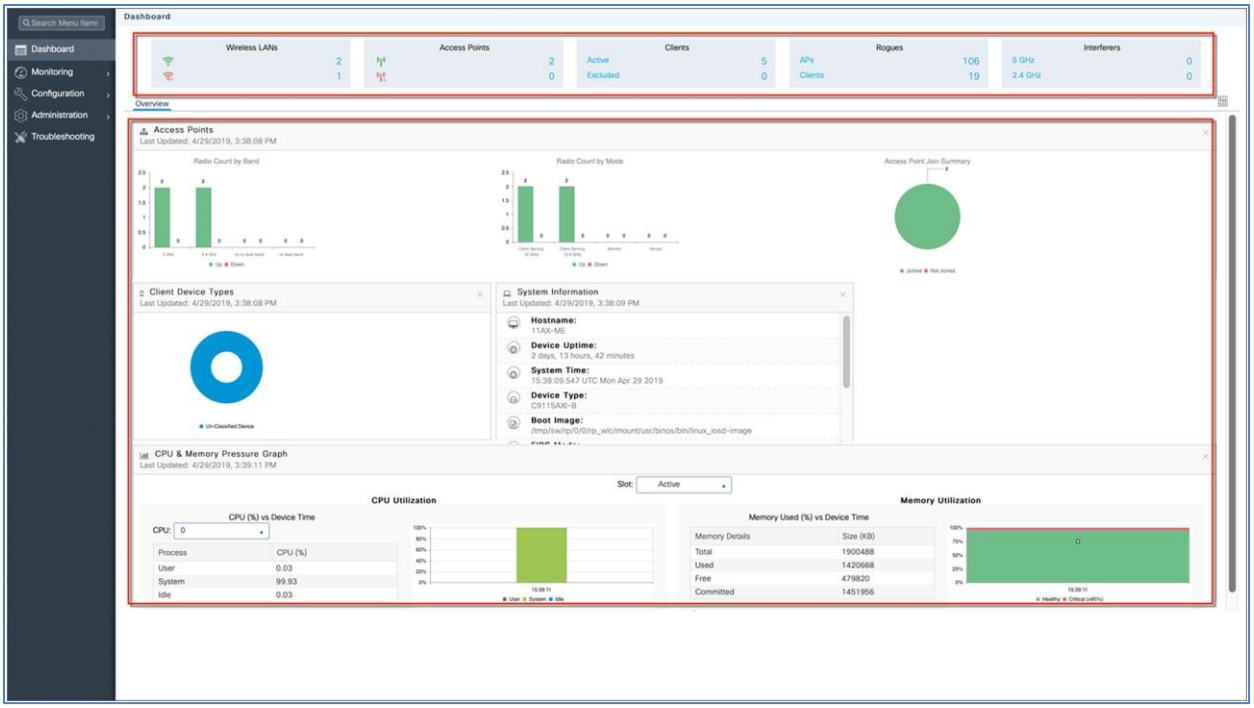
ネットワークサマリーページにはカスタマイズ可能なウィジェットが 5 つあり、次の項目について表形式とグラフ形式の両方でデータが表示されます。

アクセスポイント数（帯域別およびモード別）

クライアントデバイスタイプ

システム情報

CPU/メモリ負荷グラフ



GUI を使用したアクセスポイントのサマリー表示

GUI を使用してアクセスポイントを表示するには、次の手順を実施します。

ステップ1 ダッシュボードでアクセスポイント数をクリックするか、[モニタリング（Monitoring）] > [ワイヤレス（Wireless）] > [AP統計情報（AP Statistics）] に移動します。表にアクセスポイントのリストが表示され、次の情報が示されます。

[AP名（AP Name）]

[AP MAC] アドレス

[管理ステータス（Admin Status）]

[運用ステータス（Operational Status）]

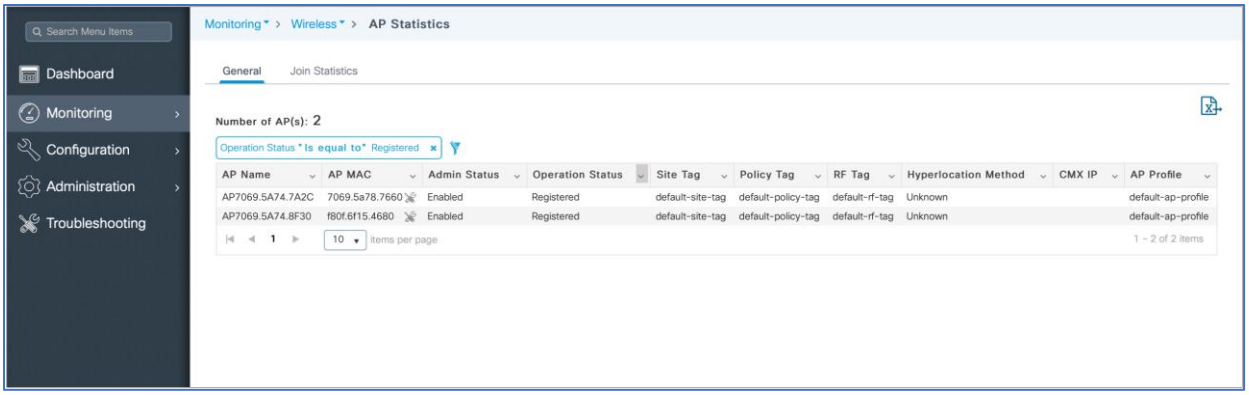
[サイトタグ（Site Tag）]

[ポリシータグ（Policy Tag）]

[RFタグ（RF Tag）]

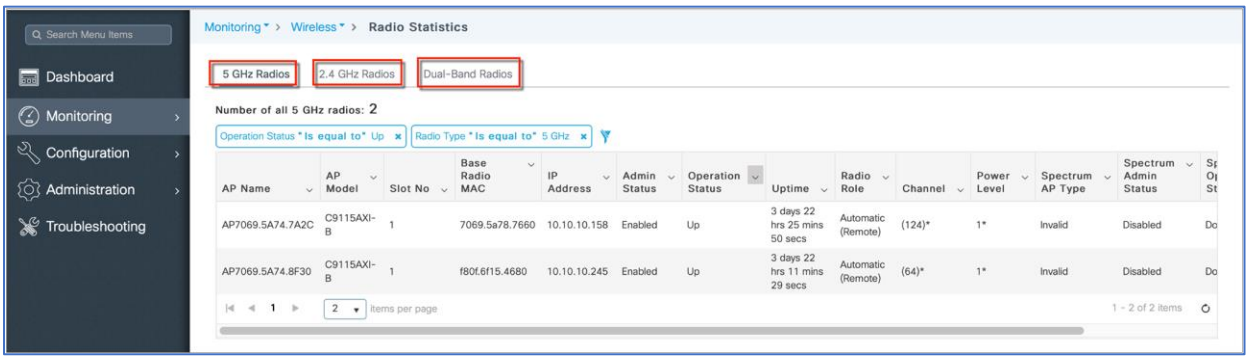
[CMX IP] アドレス

[APプロファイル（AP Profile）]

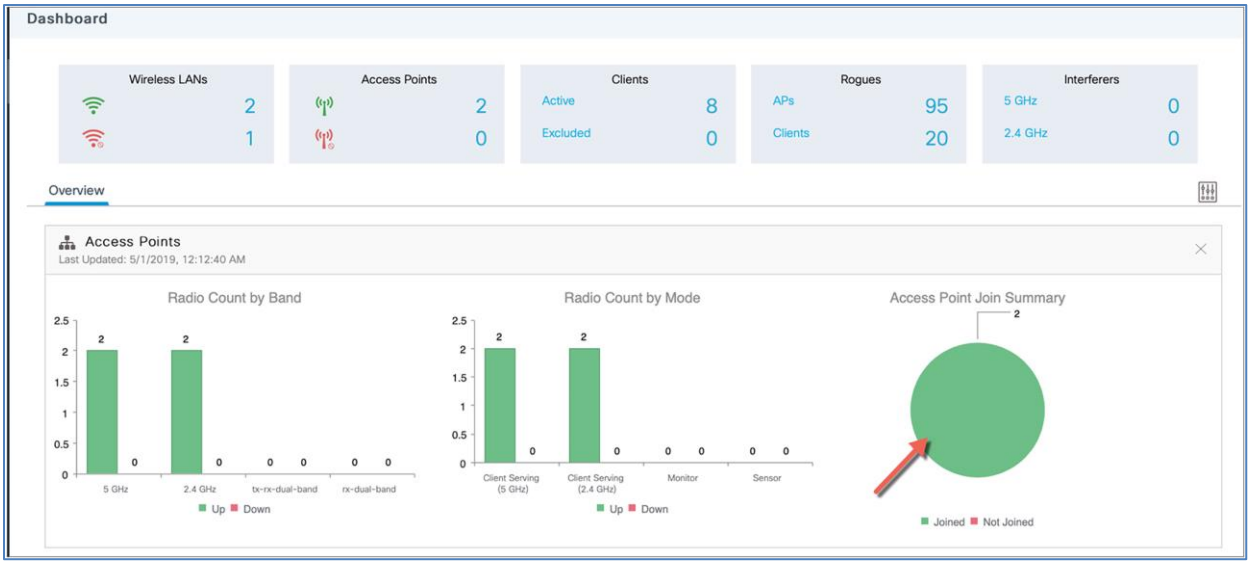


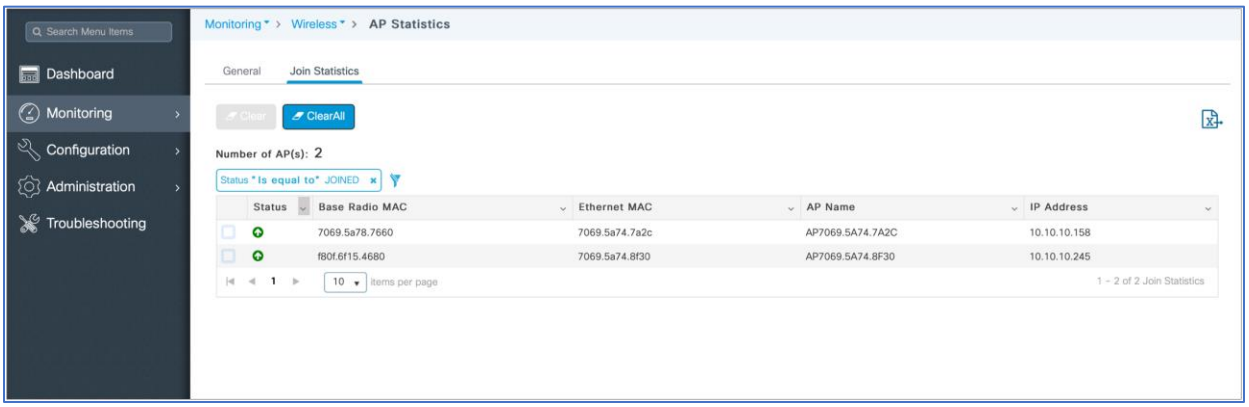
ステップ 2 アクセスポイントの [帯域別無線カウント（Radio Count by Band）] をクリックするか、[モニタリング（Monitoring）] > [ワイヤレス（Wireless）] > [無線統計情報（Radio Stats）] に移動します。表に無線のリストが表示されます。

ステップ 3 [2.4GHz無線（2.4 GHz Radios）]、[5 GHz無線（5 GHz Radios）]、[デュアルバンド無線（Dual-Band Radio）] タブを切り替えて、それぞれの無線周波数で動作しているアクセスポイントのリストを表示します。



ステップ 4 [アクセスポイント参加サマリー（Access Point Join Summary）] をクリックするか、[モニタリング（Monitoring）] > [ワイヤレス（Wireless）] > [AP統計情報（AP Statistics）] > [参加統計情報（Join Statistics）] に移動して、AP 参加統計情報を表示します。





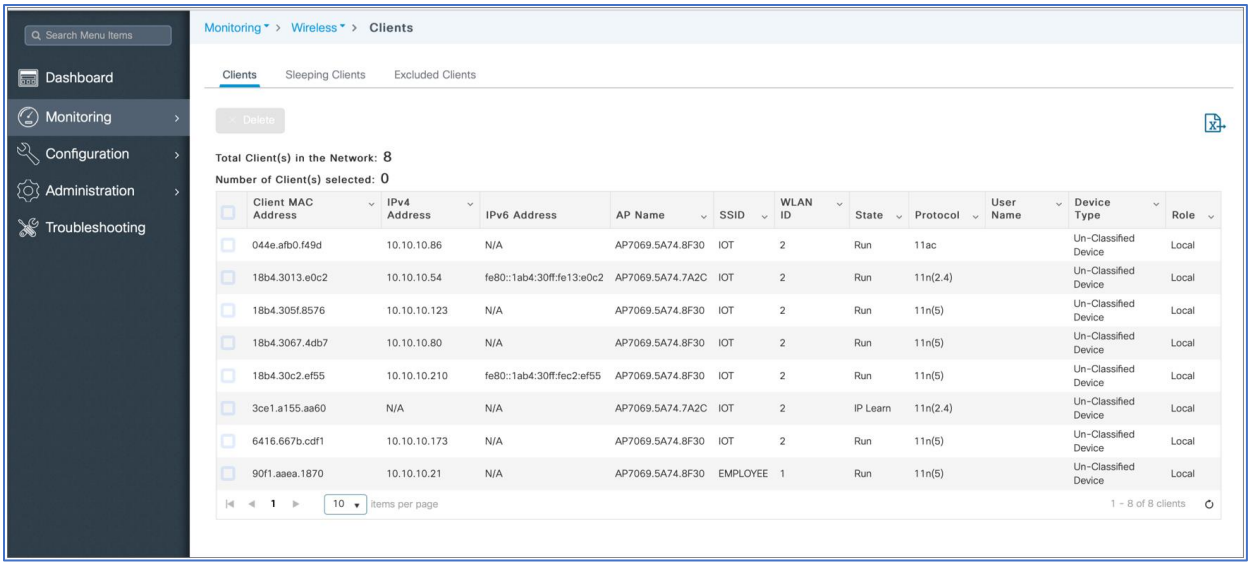
クライアントサマリーの表示

GUI を使用してクライアントサマリーを表示するには、次の手順を実施します。

手順

ステップ 1 モニタリングダッシュボードでクライアント数をクリックするか、[モニタリング（Monitoring）] > [ワイヤレス（Wireless）] > [クライアント（Clients）] に移動します。

ステップ 2 （オプション）各列の下矢印をクリックして、目的のパラメータに基づいて表をフィルタリングします。



ワイヤレス設定の管理

Cisco Catalyst EWC 設定データモデルは、再利用可能性の確保、シンプルなプロビジョニング、柔軟性とモジュール化の向上を設計原則としているため、拡張度合いに応じてネットワークを管理し、変化の激しいビジネスと IT の要件に容易に対応することができます。

このモデルでは、クライアント/AP デバイスはタグ内に含まれるプロファイルから設定を取得できます。AP は静的にタグにマッピングされるか、ルールエンジンによってマッピングされます。ルールエンジンは AP の Join プロセス中に有効になり、コントローラで実行されます。設定はオブジェクトとしてモジュール化されるため再利用できます。さらに、フラットなタグベースの設定モデルにより、継承やコンテナベースのグループ化に伴う複雑さが解消されるため柔軟に設定でき、変更管理も容易になります。

設定モデルの要素：タグとプロファイル

プロファイル

プロファイルは、AP または関連付けられたクライアントの設定および属性を定義するものです。プロファイルは、タグ全体で使用できる再利用可能なエンティティです。デフォルトのポリシープロファイル、AP Join プロファイル、Flex プロファイル、2.4 GHz および 5 GHz RF プロファイルは、ワイヤレスコントローラの起動時にデフォルトで使用できます。

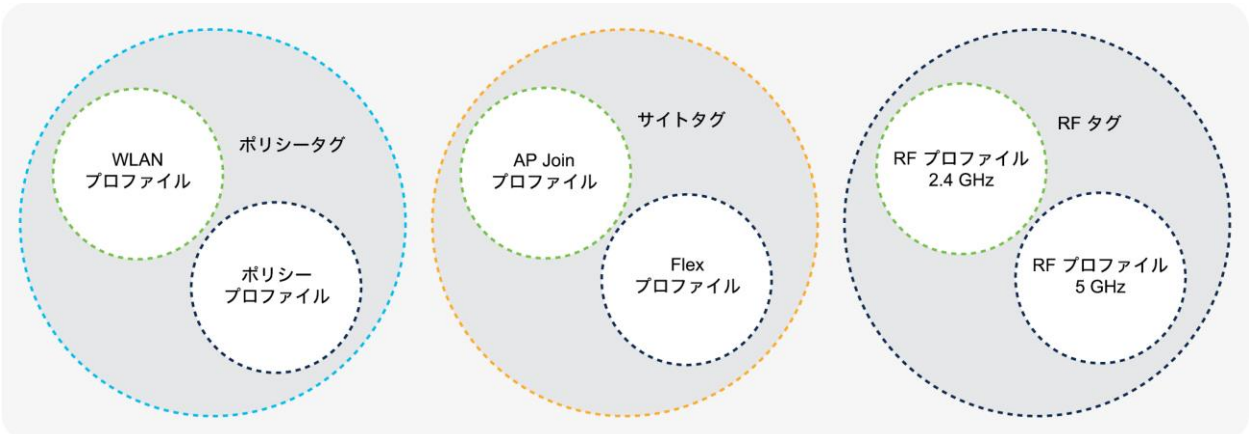


図 2.
プロファイルとタグ

定義するネットワークの特性に応じてさまざまな種類のプロファイルがあります。

WLAN プロファイル

WLAN プロファイルは、プロファイル名、ステータス、WLAN ID、レイヤ 2 およびレイヤ 3 のセキュリティパラメータ、該当の SSID に関連付けられた AAA サーバ、特定の WLAN に固有のその他のパラメータなど、WLAN のプロパティを定義するものです。

ポリシープロファイル

ポリシープロファイルは、クライアントのネットワークポリシーとスイッチングポリシーおよび AP ポリシーを定義するもので、QoS を除くと AP ポリシーと同じです。ポリシープロファイルはタグ全体で再利用できるエンティティです。AP/コントローラに適用されるクライアント向けポリシーはすべて、ポリシープロファイルに移行されます。ポリシーの例として、VLAN、アクセスコントロールリスト（ACL）、QoS、セッションタイムアウト、アイドルタイムアウト、Application Visibility and Control（AVC）プロファイル、Bonjour プロファイル、ローカルプロファイル、デバイス分類などが挙げられます。スイッチングポリシーは、WLAN の中央スイッチングまたはローカルスイッチングの属性を定義するものです。

WLAN プロファイルとポリシープロファイルはどちらもポリシータグに含まれ、WLAN の特性とポリシーを定義します。

AP Join プロファイル

次のパラメータは、AP Join プロファイルを構成するものです。Control And Provisioning of Wireless Access Points（CAPWAP）IPV4/IPV6、User Datagram Protocol（UDP）Lite、高可用性、再送信設定パラメータ、グローバル AP フェールオーバー、ハイパーロケーション設定パラメータ、Telnet/SSH、802.11u パラメータなどです。AP Join プロファイルを変更する場合、これらのパラメータは AP の特性に関連するため、一部のサブセットでは CAPWAP 接続をリセットする必要があります。

Flex プロファイル

Flex プロファイルにはリモートサイト固有のパラメータが含まれています。たとえば、AP リスト、Extensible Authentication Protocol（EAP）プロファイルなどがあり、AP が認証サーバ、ローカル RADIUS サーバの情報提供、VLAN/ACL マッピングなどの機能を担う場合に使用できます。

AP Join プロファイルと Flex プロファイルはどちらもサイトタグに含まれ、リモートサイトの特性を定義します。

RF プロファイル

デフォルトの RF プロファイルは 2 つあります（802.11a 用と 802.11b 用）。RF プロファイルは、データレート、Modulation and Coding Scheme（MCS）設定、電力割り当て、動的チャネル割り当て（DCA）パラメータ、Coverage Hold Detection and Mitigation（CHDM）変数、High Density Experience（HDX）機能などの RF 固有の設定で構成されます。RF タグには 802.11a RF プロファイルを 1 つと 802.11b RF プロファイルを 1 つ追加できます。

タグ

タグのプロパティは、タグに関連付けられたポリシーによって定義されます。このプロパティは、関連するクライアント/AP に継承されます。タグにはさまざまなタイプがあり、それぞれ異なるプロファイルに関連付けられます。共通のプロパティが設定されたプロファイルを含むタグは 1 種類しかありません。そのため設定エン

ティティ間の優先順位に伴う問題を大幅に削減できます。すべてのタグにはシステム起動時に作成されたデフォルトタグがあります。

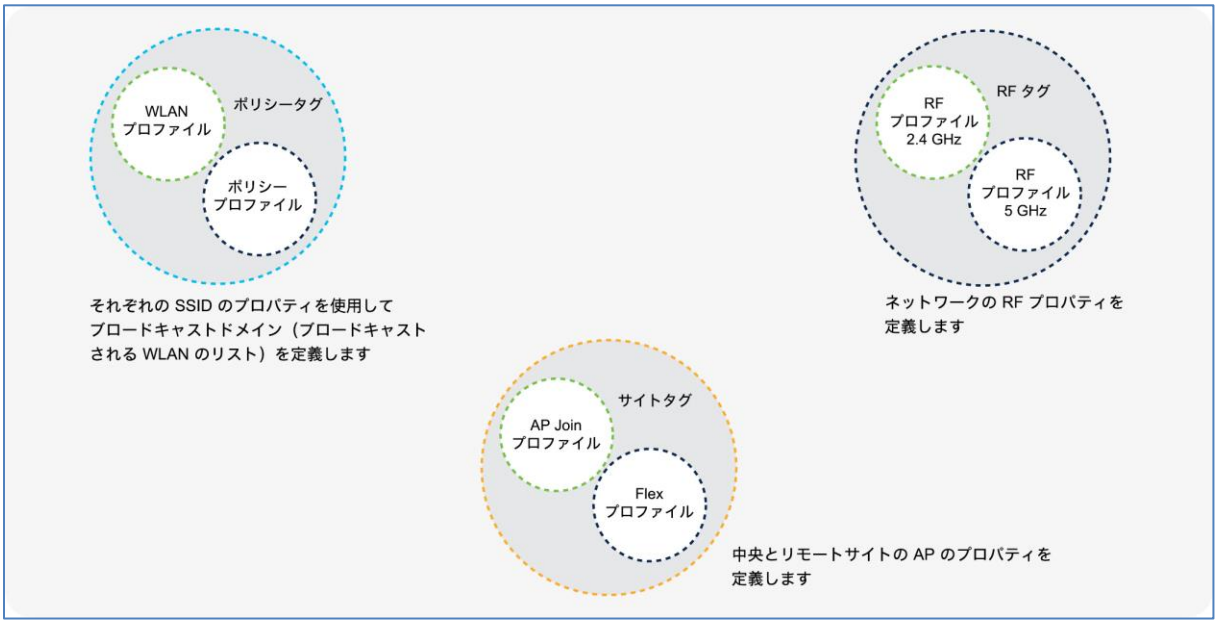


図 3.
3 種類のタグ

ポリシータグ

ポリシータグには、WLAN プロファイルとポリシープロファイルのマッピング情報が含まれています。

WLAN プロファイルを含み、WLAN ID が 16 未満のデフォルトポリシータグは、デフォルトのポリシープロファイルにマッピングされます。

サイトタグ

サイトタグは、Flex プロファイルと AP Join プロファイルの 2 つのプロファイルで構成されます。サイトタグは、中央のサイトとリモート（FlexConnect）サイトの両方に関してプロパティを定義します。中央サイトとリモートサイトに共通するサイト属性は、AP Join プロファイルに含まれています。リモートサイトに固有の属性は Flex プロファイルに含まれています。

デフォルトのサイトタグは、デフォルトの AP Join プロファイルで構成されます。デフォルトの AP Join プロファイルの値は、グローバル AP パラメータの値と同じです。さらに現設定の AP グループからいくつかパラメータが加わります（優先モード、802.11u パラメータ、ロケーションなど）。

注：

EWC ではサイトタグは 1 つだけサポートされており、それが default-site-tag になります。また、EWC は FlexConnect ローカルスイッチング導入であるため、中央サイトの概念はありません。

RF タグ

RF タグには 2.4 GHz および 5 GHz の RF プロファイルが含まれています。

デフォルトの RF タグは、デフォルトの 2.4 GHz RF プロファイルとデフォルトの 5 GHz RF プロファイルで構成されます。これらのデフォルトプロファイルには、各無線のグローバル RF プロファイルのデフォルト値が含まれています。

AP へのタグの関連付け

アクセスポイントには、ブロードキャストドメイン、所属しているサイト、必要な RF 特性に基づいてタグが付与されます。タグが付与されると、AP はブロードキャストされる WLAN のリストの他に、それぞれの SSID のプロパティ、ローカル/リモートサイトの AP のプロパティ、ネットワークの RF プロパティを取得します。明示的に変更しない限り、AP にはデフォルトのポリシータグ、サイトタグ、RF タグが付与されます。AP に関連付けられたタグが変更されると、AP は CAPWAP 接続をリセットします。

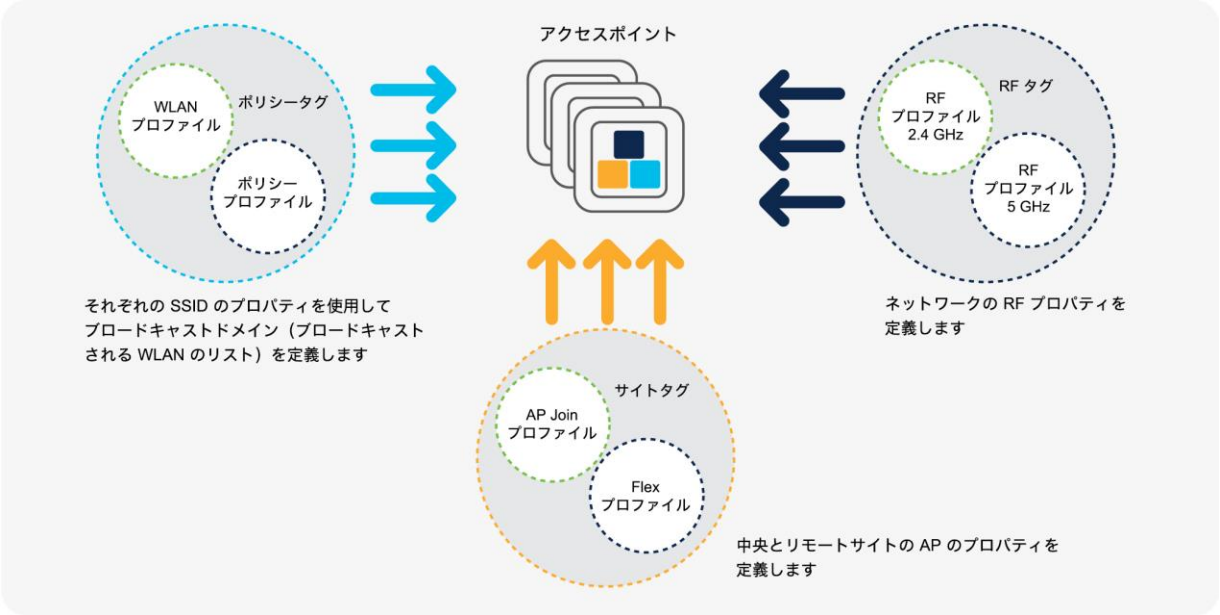


図 4.
アクセスポイントにタグを付与する方法

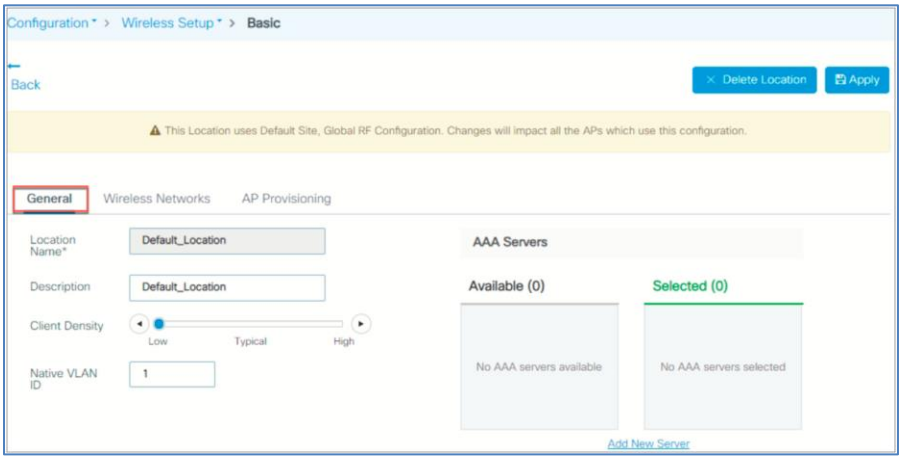
基本的なワイヤレス設定による WLAN の作成

基本的なワイヤレス設定では、インテントベースのワークフローを使用してサイトを定義し、そのサイトのワイヤレスネットワークを作成します。また、VLAN、ACL、QoS などのポリシーを定義し、RF 特性を微調整します。対応するポリシーとタグは新しい設定モデルに従ってバックエンドで作成され、エンドユーザが意識することはありません。アクセスポイントはサイトに割り当てられ、ポリシータグ、RF タグ、サイトタグがアクセスポイントに割り当てられます。

基本のワイヤレス設定にアクセスするには、ダッシュボードページの右上隅にあるワイヤレス設定アイコンをクリックします。

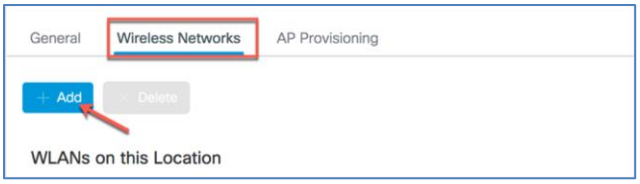
ステップ 1：EWC の右上隅から [ワイヤレス設定（Wireless Setup）] > [タイプの選択（Select Type）] > [基本（Basic）] の順に移動し、[Default_Location] をクリックします。

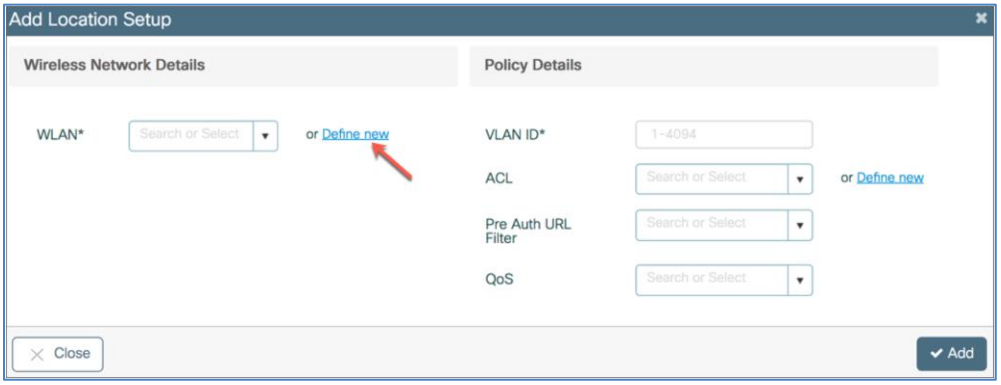
ステップ 2 : [全般（General）] タブでは、導入ごとに [クライアント密度（Client Density）]、[ネイティブ VLAN ID（Native VLAN ID）]、[AAAサーバ（AAA Server）] などのパラメータを定義できます。



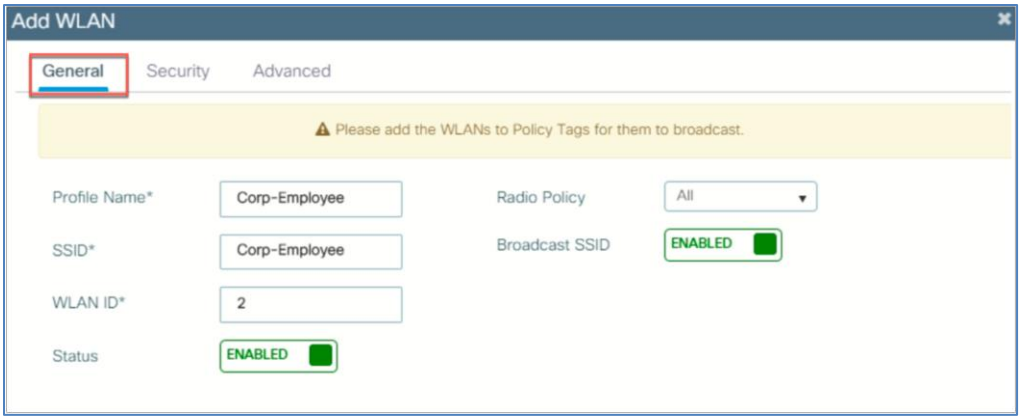
ステップ 3 : Day-0 セットアップの一環で作成された WLAN をこのサイトに追加できます。これらの WLAN はそのまま追加することも、サイト内のネットワークに必要なポリシーに応じて変更することもできます。または、[新規定義（Define new）] ボタンを使用して新しい SSID を作成することもできます。

新しい WLAN を追加するには、[ワイヤレスネットワーク（Wireless Networks）] タブに移動して [+追加（+ Add）] をクリック後、[新規定義（Define new）] をクリックして WLAN を設定します。

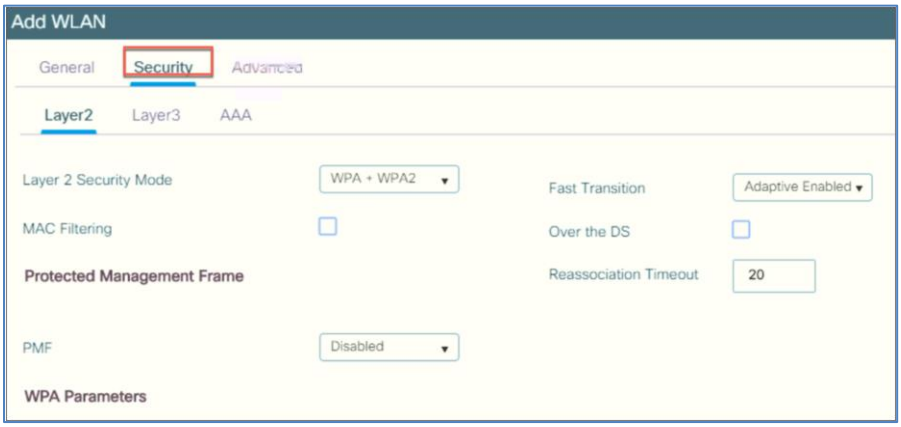




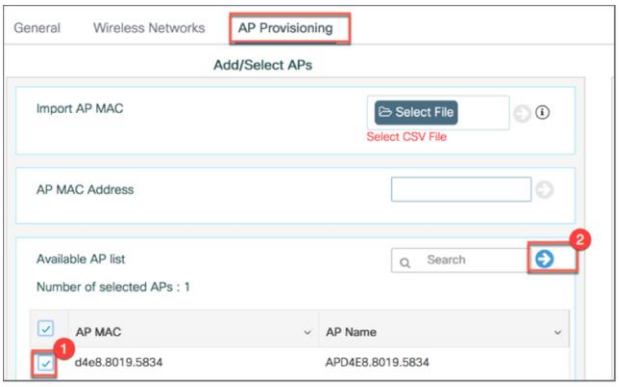
ステップ 4 : WLAN ウィンドウが開きます。[全般（General）] タブで WLAN の [プロファイル名（Profile Name）]、[SSID]、[WLAN ID]、[無線ポリシー（Radio Policy）] を設定します。[ステータス（Status）] を [有効（Enabled）] にして [セキュリティ（Security）] タブに移動します。

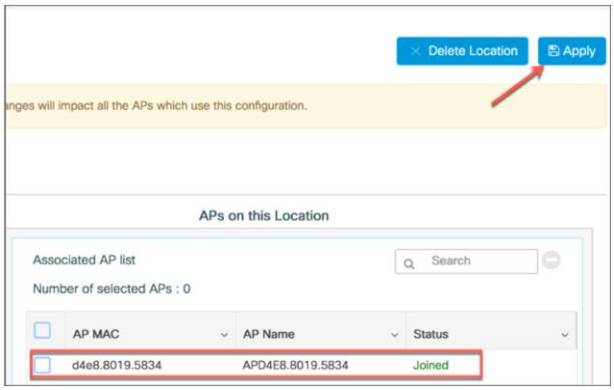


ステップ 5：必要な設定ごとにセキュリティを定義できます。



ステップ 6：ここで AP をプロビジョニングする必要があります。使用可能な AP のリストから AP を選択し、矢印をクリックします。選択した AP が、そのロケーションに関連付けられている AP のリストに移動します。[適用（Apply）] をクリックします。

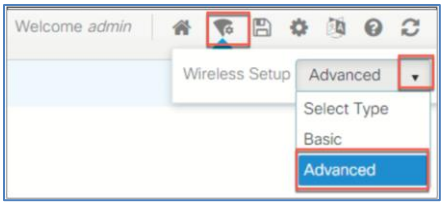


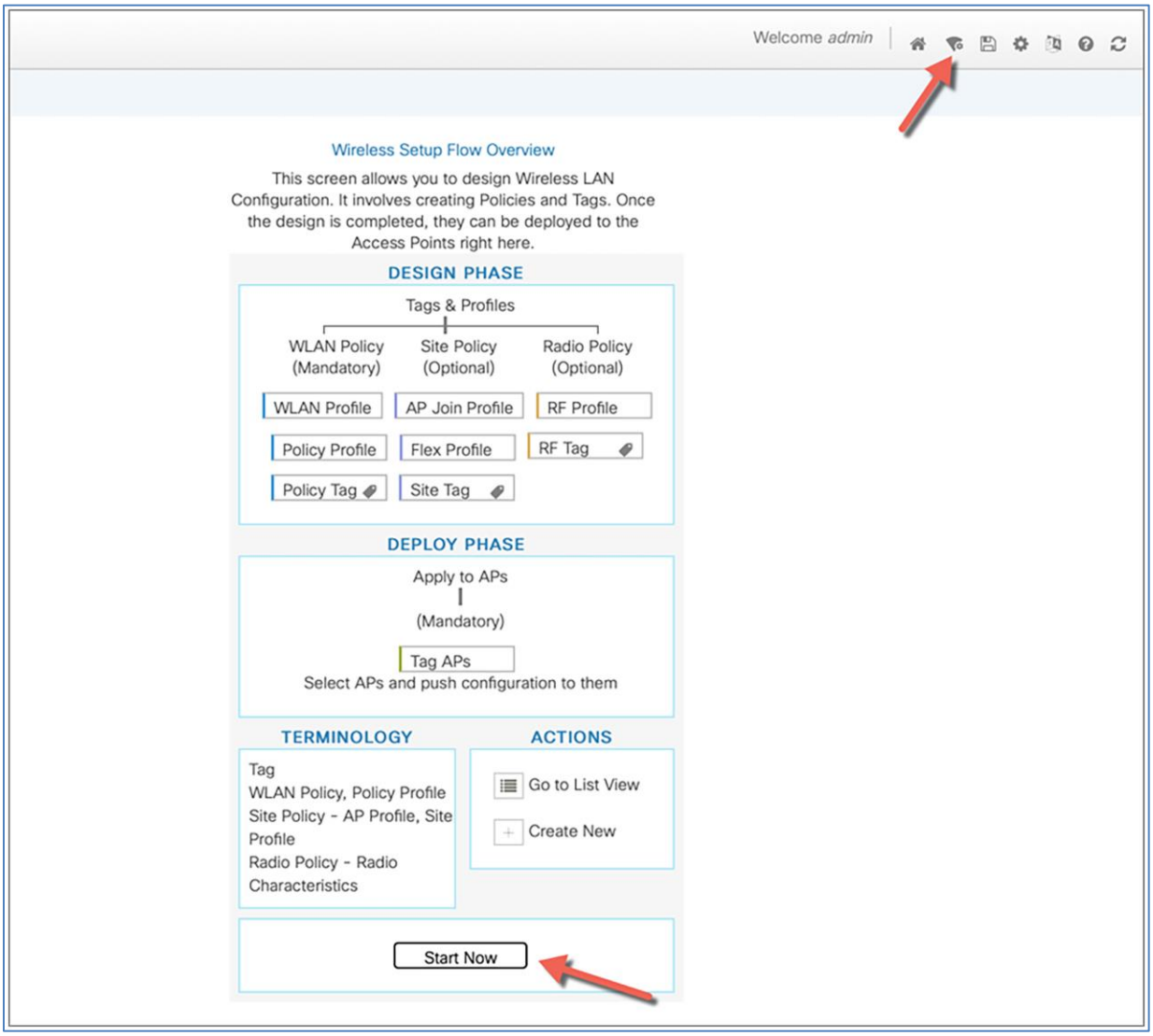


ポリシータグ、サイトタグ、RF タグがプロビジョニング時にアクセスポイントに自動的にプッシュされます。

詳細ワイヤレス設定による WLAN の作成

ダッシュボードページの右上隅にあるワイヤレス設定アイコンをクリックして、ワイヤレス設定にアクセスします。

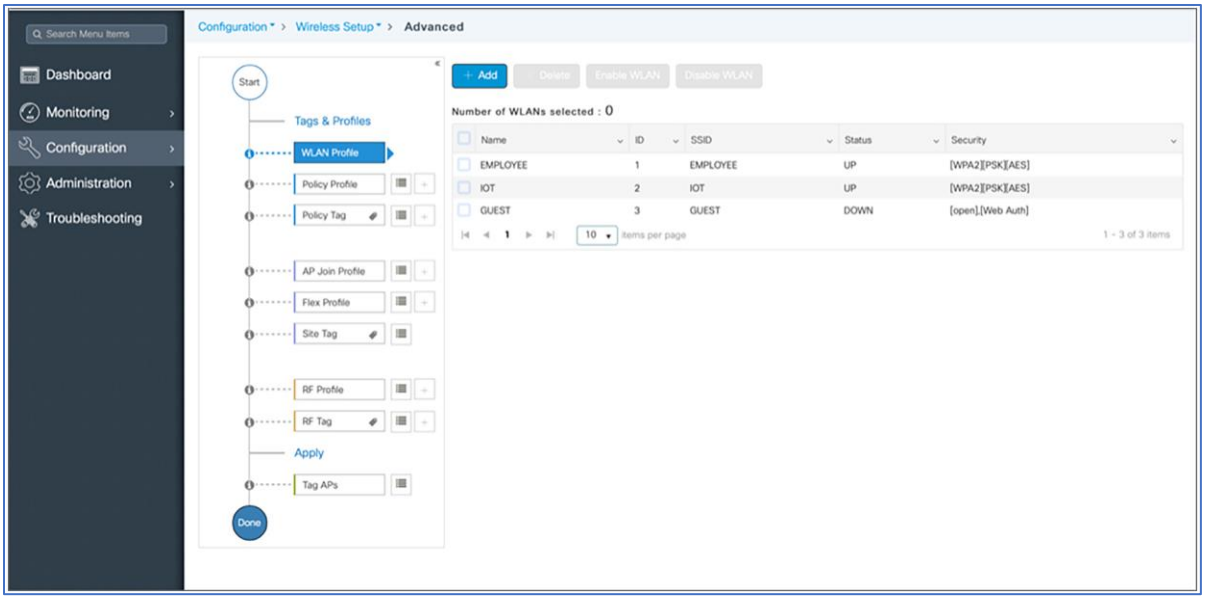




Cisco Catalyst ワイヤレスコントローラでネットワークを設定するために必要な手順を簡単に実施できるように、ガイド付きワークフローが作成されています。

手順

[ワイヤレス設定（Wireless Setup）] > [詳細（Advanced）] を選択し、このページの注意事項を確認したら [今すぐ開始（Start Now）] をクリックしてワイヤレスネットワークの設定を開始します。



注：次の一連の手順では論理的な順序で設定を行います。WLAN プロファイルを除き、すべてのプロファイルとタグにはデフォルトのオブジェクトが関連付けられています。

1. プロファイルを作成する
   - 必要な WLAN プロファイル（SSID）を作成します。
   - ポリシープロファイルを作成します（デフォルト以外が必要な場合）。
   - RF プロファイルを作成します（デフォルト以外が必要な場合）。
   - サイトプロファイルを作成します（デフォルト以外が必要な場合）。
2. タグを作成する
   - ポリシータグを作成し（デフォルト以外が必要な場合）、必要に応じて上記の SSID をポリシープロファイルにマッピングします。
   - RF タグを作成し（デフォルト以外が必要な場合）、802.11a および 802.11b 用の RF プロファイルを追加します。
   - サイトタグを作成し（デフォルト以外が必要な場合）、Flex プロファイル（サイトがリモートの場合）と AP Join プロファイルを追加します（ほとんどの場合デフォルトを使用）。
3. タグを AP に関連付ける

カスタムタグが不要な場合は、デフォルトのタグが AP に関連付けられるためこの手順は不要です。

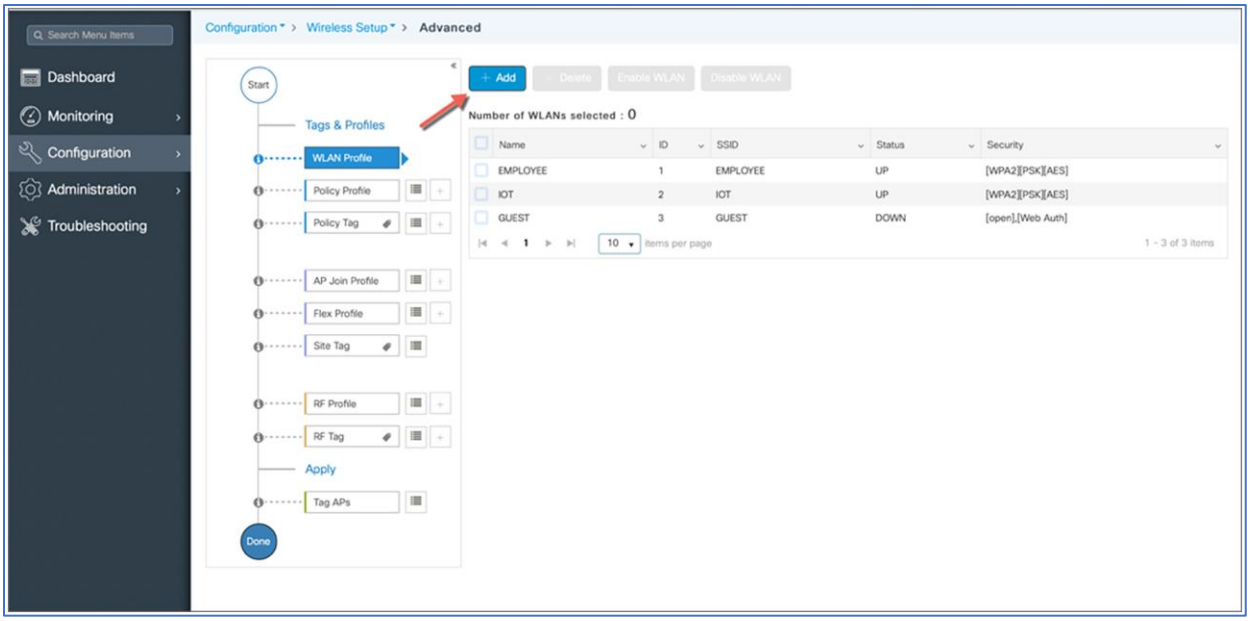
関連付けるタグがデフォルト以外の場合は、AP に関連付けます。

- RF タグを AP または AP のセットに関連付けます。
- ポリシータグを AP または AP のセットに関連付けます。
- サイトタグを AP または AP のセットに関連付けます。

WLAN プロファイルの作成

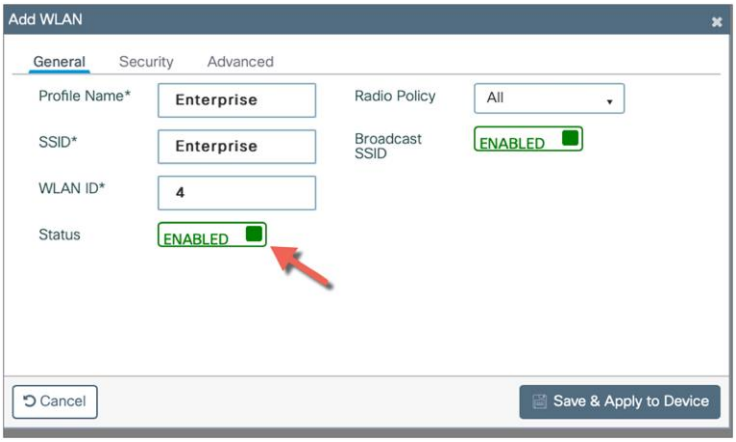
WLAN プロファイルの横にある [+] 記号をクリックして WLAN の設定を開始します。

[追加（Add）] ボタンをクリックします。

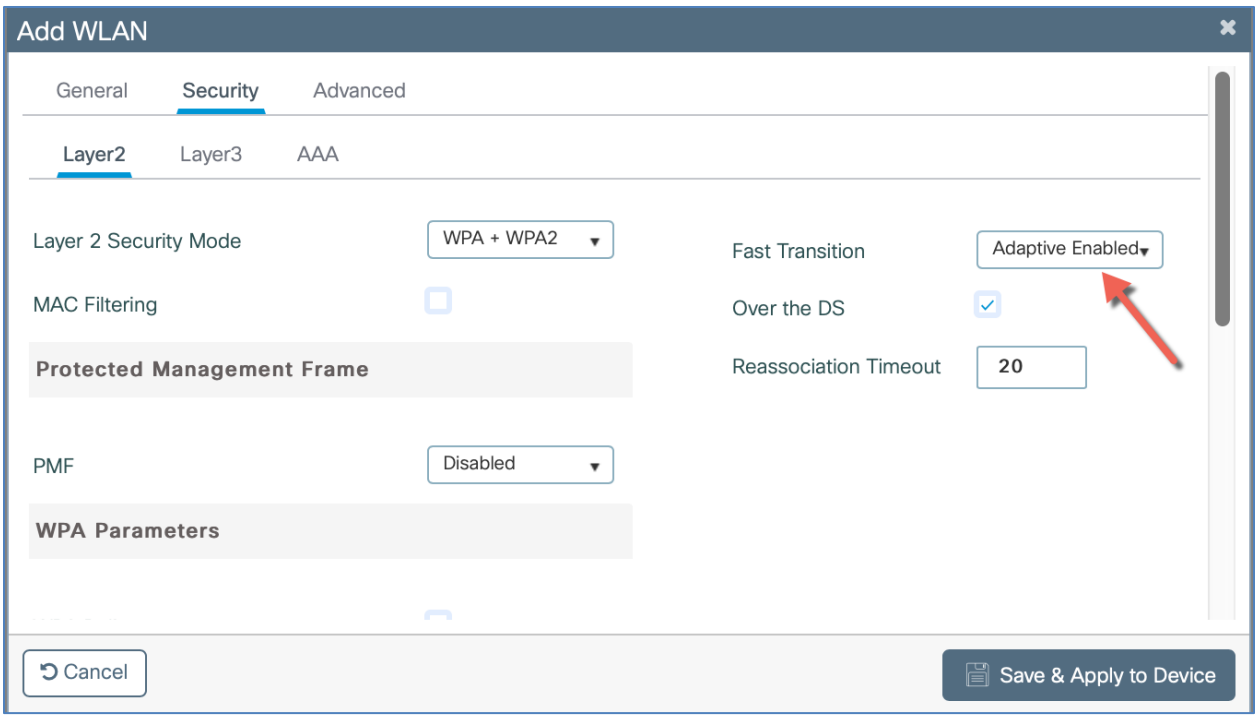


注：Day-0 のフローで作成された SSID は、WLAN プロファイルページに自動的に表示されます。

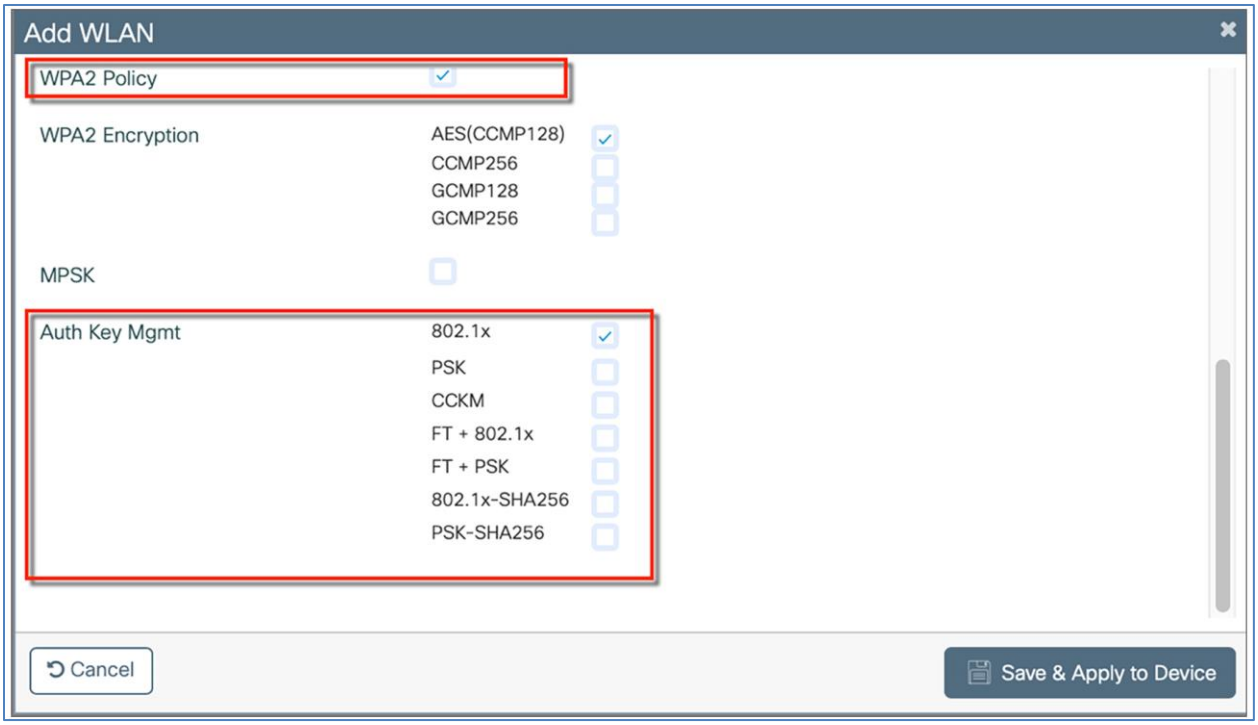
任意のプロファイル名と 1 ー 16 の WLAN ID を指定し、[ステータス（Status）] トグルボタンを [有効（Enabled）] に設定します。



適応型 802.11r およびベストプラクティスに基づくその他の設定はデフォルトでオンになっています。



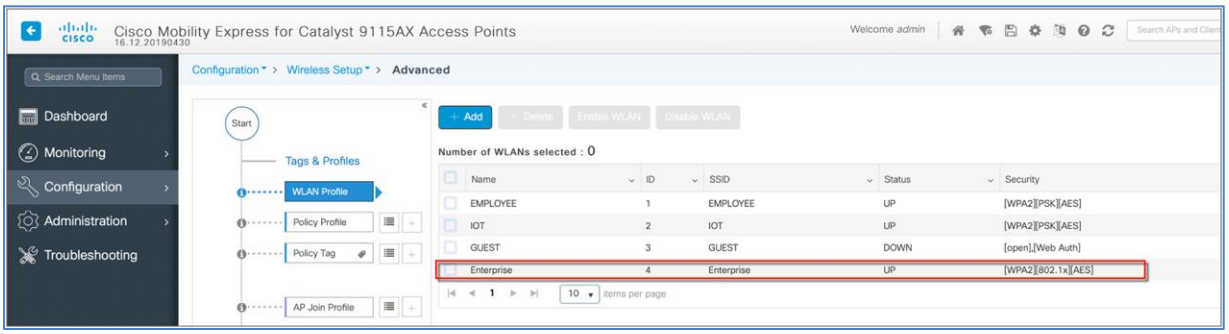
[セキュリティ（Security）] タブで認証キー管理（AKM）として [PSK] または [802.1X] を選択します。[保存してデバイスに適用（Save & Apply to Device）] をクリックします。



[802.1X] を選択した場合は、AAA/RADIUS サーバが追加されていることを確認します。これは、Day-0 の設定セットアップウィザードで追加されているか、Day-1 設定の一環で実施されます。Day-0 で RADIUS サーバを設定した場合、**RADIUS サーバ（RADIUS_SERVER_DAY0_1）**、**RADIUS サーバグループ（RADIUS_SERVER_GROUP_DAY0）**、**AAA 方式リスト名（authentication_dot1x_day0）**が自動的に作成されます。この方式リストは、[WLAN] > [セキュリティ（Security）] > [AAA] > [認証リスト（Authentication List）] に表示されます。

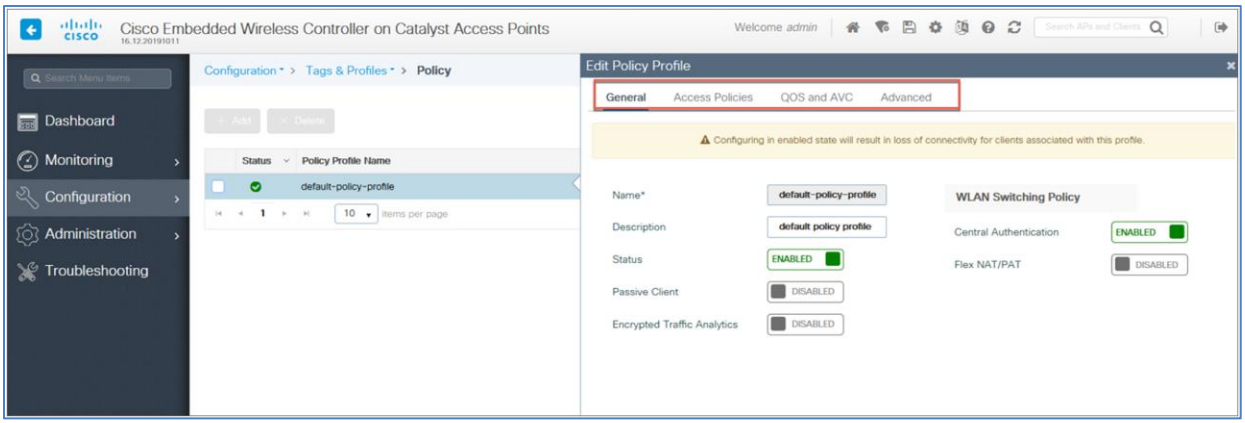
Day-1 での RADIUS 設定については、このガイドの「AAA/RADIUS サーバの設定」の項を参照してください。

WLAN プロファイルが次のように作成されていることを確認します。

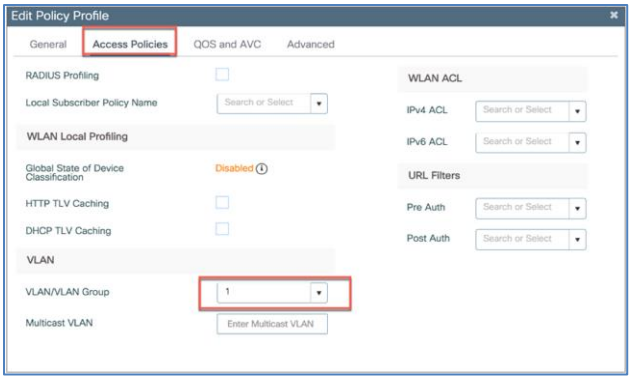


ポリシープロファイル

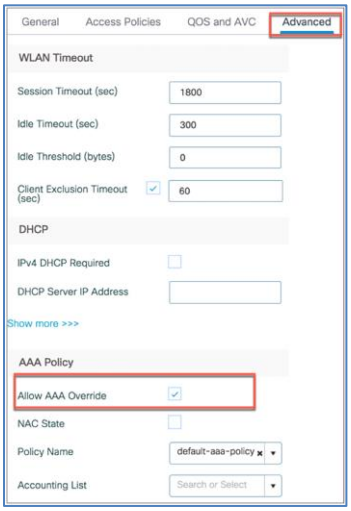
デフォルトのポリシープロファイルとデフォルトのポリシータグは事前に設定されているため、カスタマイズする必要がない場合は特別なポリシー設定は不要です（アクセスポリシー、ローカルスイッチ VLAN、QoS、AVC、AAA オーバーライドなど）。



[アクセスポリシー（Access Policies）] > [VLAN] > [VLAN/VLANグループ（VLAN/VLAN Group）] オプションでローカルスイッチ VLAN を設定できます。

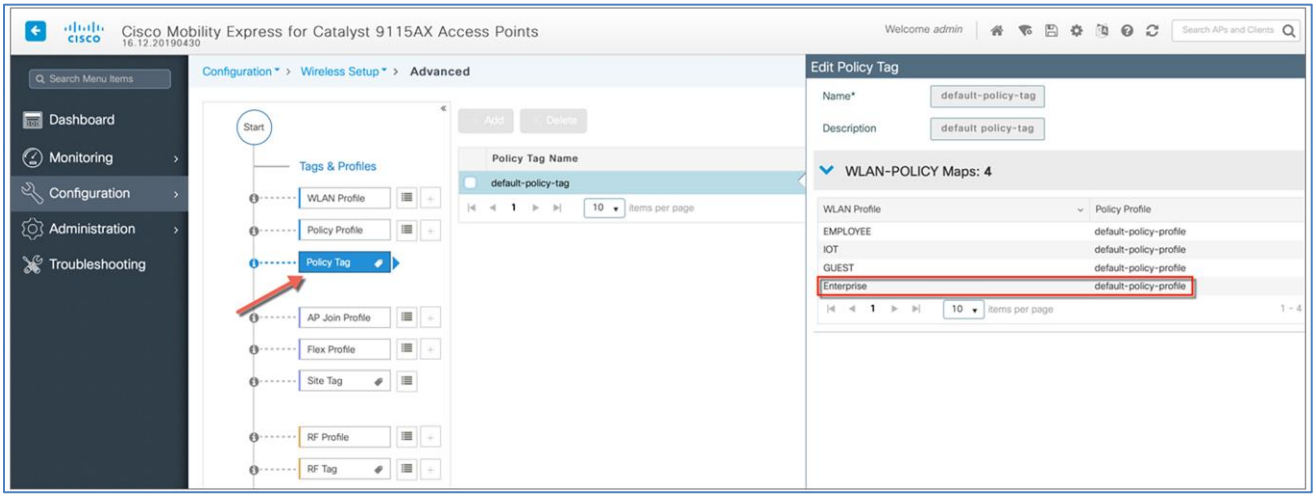


[詳細（Advanced）] > [AAAポリシー（AAA Policy）] で [AAAオーバーライドを許可（Allow AAA Override）] オプションを選択して、特定のポリシープロファイルに関連付けられた WLAN に AAA 属性の一部を適用または渡すこともできます。

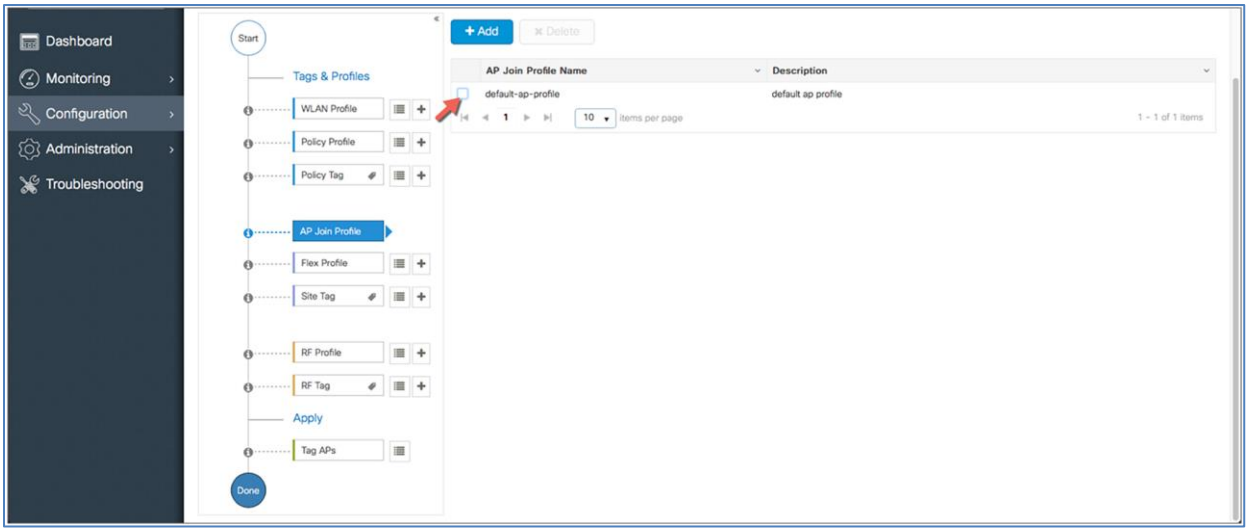


ポリシータグ

デフォルトでは WLAN ID 1 ー 16 がデフォルトのポリシータグに関連付けられます。最初の手順で作成された SSID は、次に示すように、このデフォルトのポリシータグに自動的に追加されます。



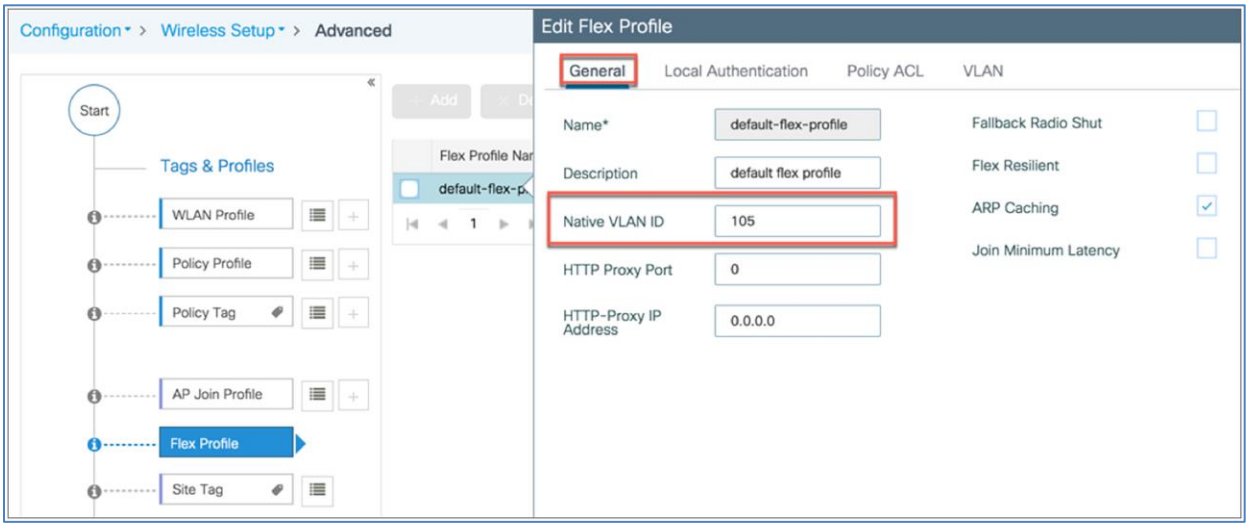
デフォルトの AP Join プロファイルとサイトタグは自動的に使用されるため、特別なサイト設定は不要です。EWC は、デフォルトのサイトタグであるグローバルサイトを 1 つだけサポートします。



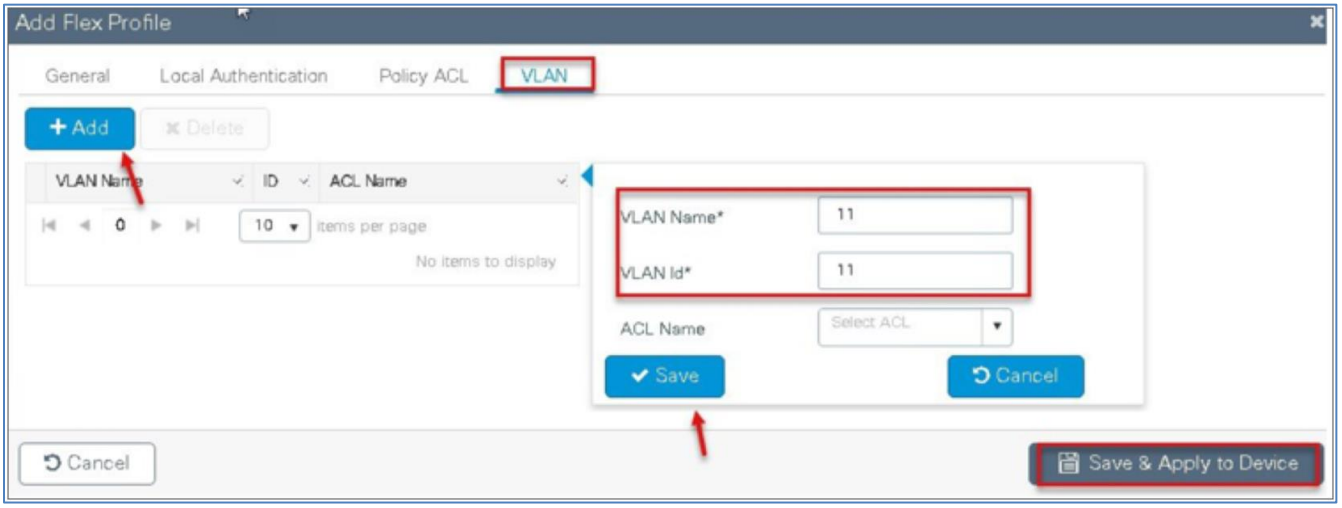
Flex プロファイル

Flex プロファイルは、ローカルにスイッチされた SSID に使用される VLAN が AAA によってオーバーライドされた際に、AP で VLAN を設定するために使用されます。

Flex プロファイルのネイティブ VLAN を定義できます。

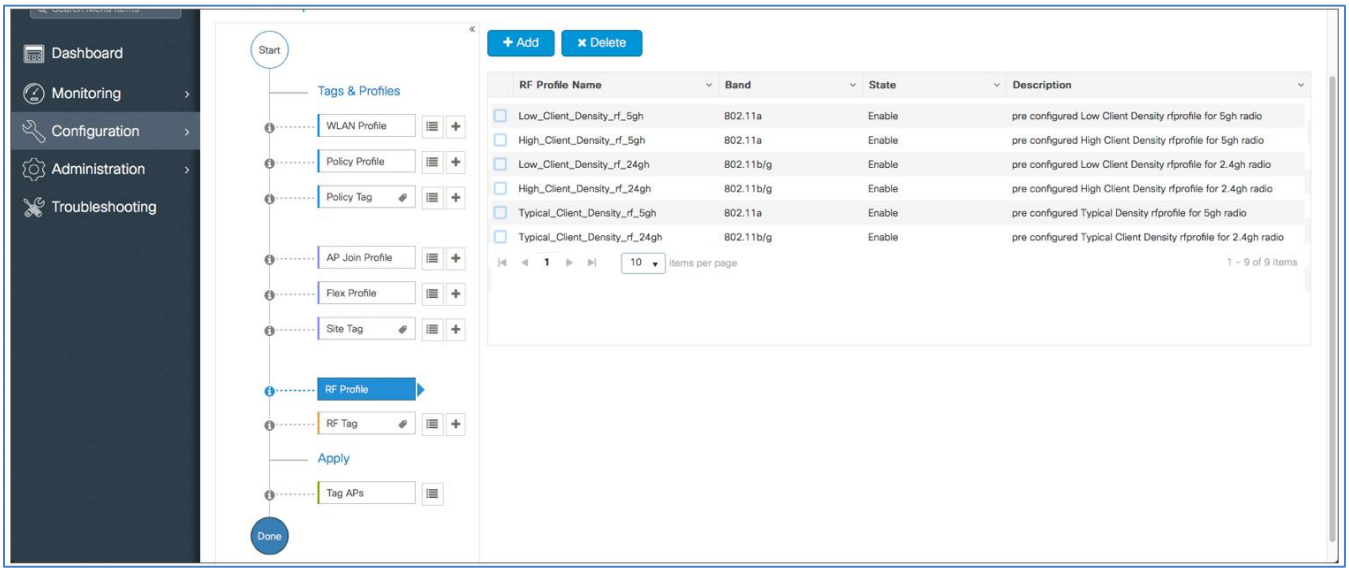


ローカルにスイッチされた SSID に使用される VLAN を定義することもできます。この例では、VLAN 11 を使用します。VLAN 11 は、AAA VLAN オーバーライドオプションを使用した場合に AP からローカルにスイッチされる VLAN です。

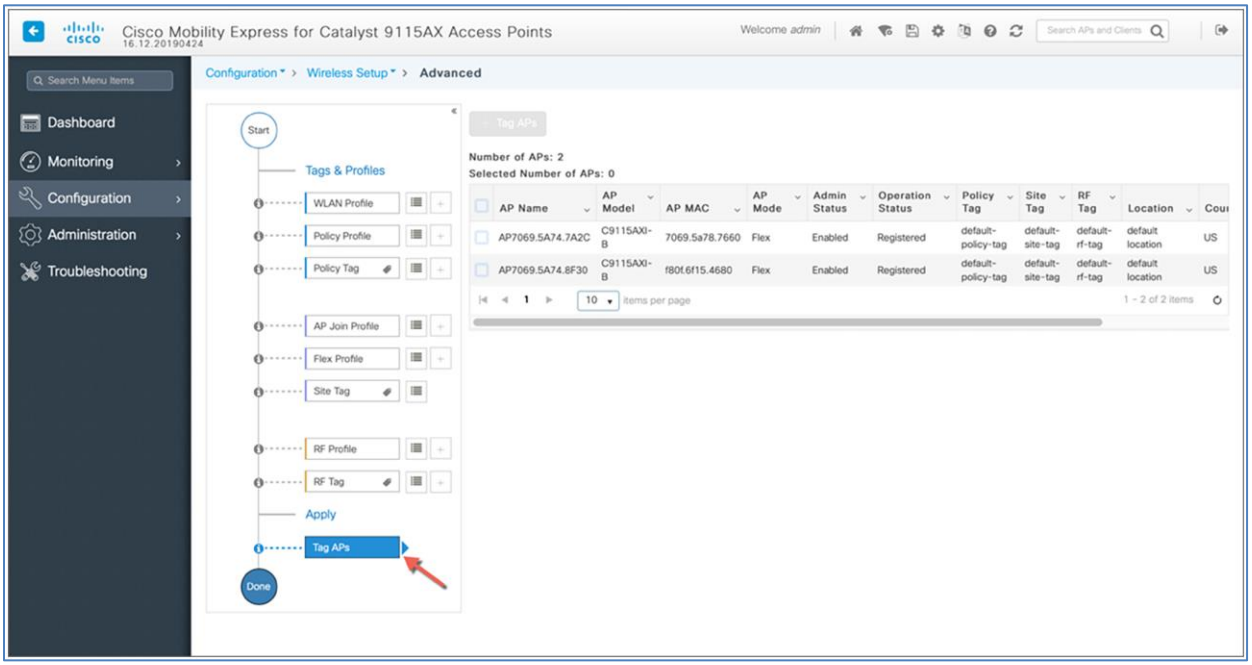


RF プロファイル

デフォルトの RF プロファイルと RF タグは事前に設定されているため、RF 設定は不要です。



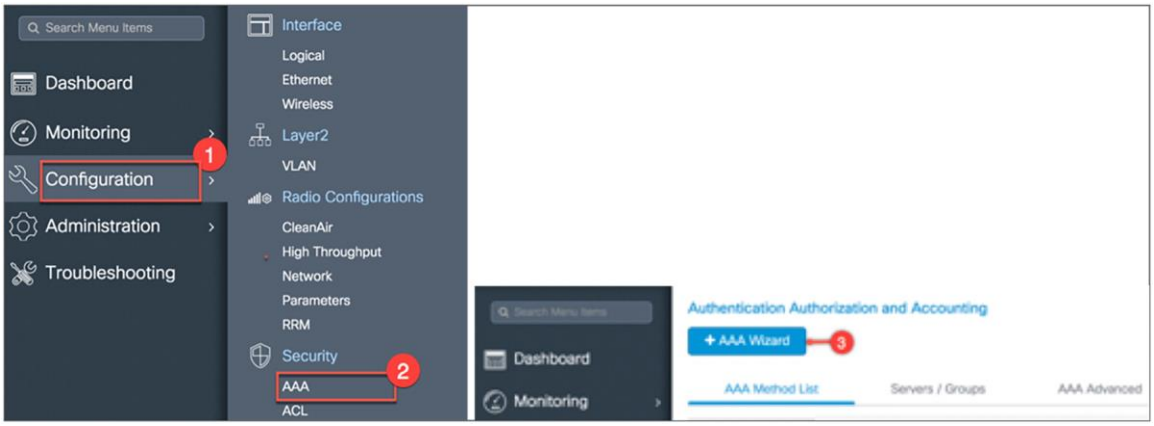
AP にはデフォルトのポリシータグ、サイトタグ、RF タグが自動的に付与されるため明示的なタグ付けは不要で、SSID（1 ー 16）がネットワーク全体にブロードキャストされます。



AAA/RADIUS サーバの設定

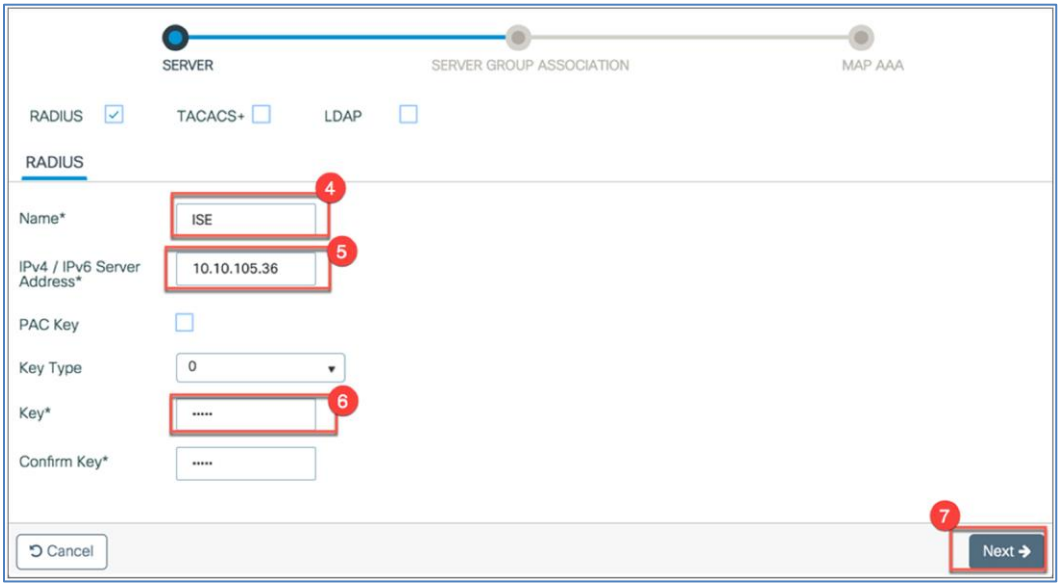
AAA サーバを Day-0 で設定していない場合は、次の手順に従って AAA/RADIUS サーバを追加できます。

EWC のメインメニューから、[設定（Configuration）] > [セキュリティ（Security）] > [AAA] の順に移動し、[AAA追加ウィザード（+ AAA Wizard）] をクリックします。

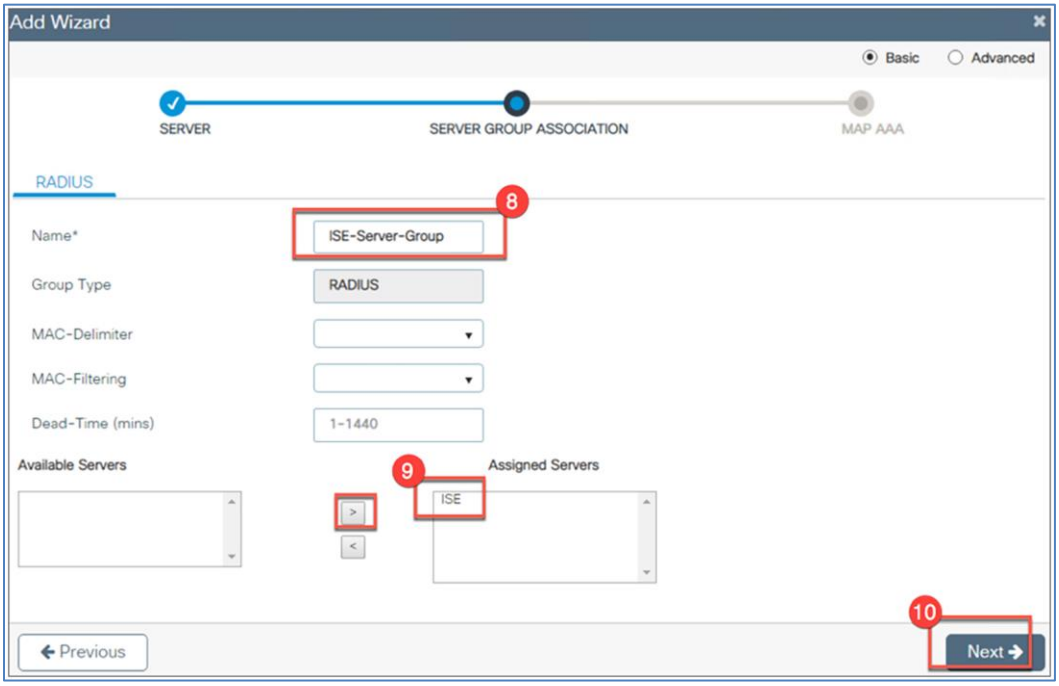


次のように設定します。

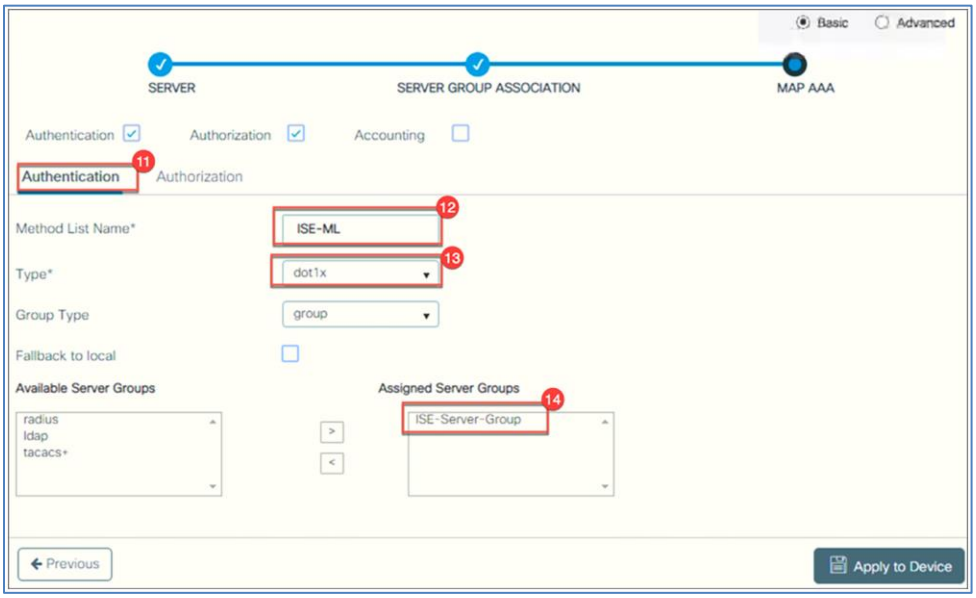
1. **RADIUS**：名前、サーバの IP アドレス、キー（共有秘密）。[次へ（Next）] をクリックします。この例では「ISE」という名前にしています。



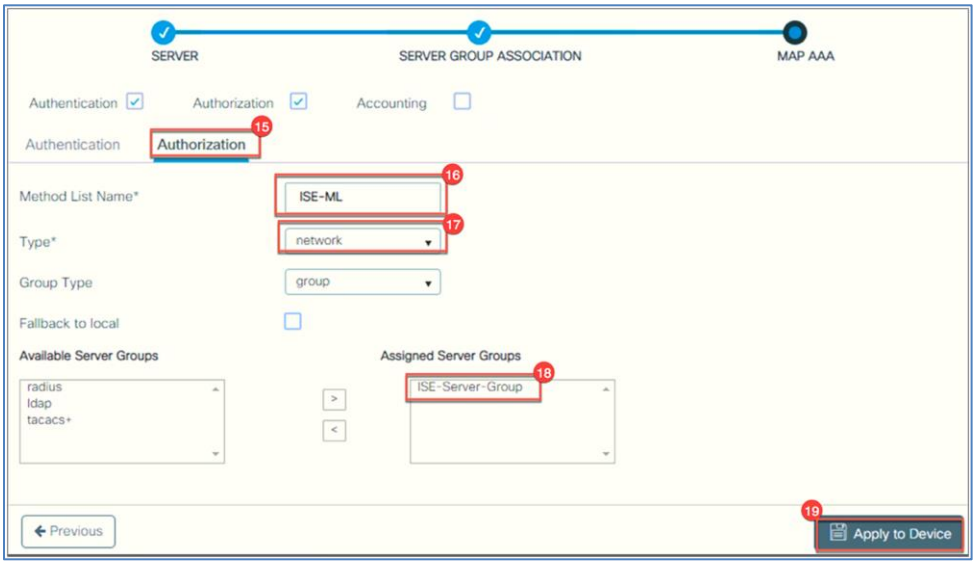
2. **サーバグループ関連付け**：サーバグループの名前を設定し、[利用可能なサーバ（Available Servers）] リストから、上記で作成したサーバ（この例では「ISE」）を選択します。[>] 記号をクリックして選択したサーバを [割り当て済みサーバ（Assigned Servers）] リストに移し、[次へ（Next）] をクリックします。



3. **AAA のマッピング**：[認証（Authentication）] を選択後 [方式リスト名（Method List Name）] を設定し（デフォルトを使用しない場合）、[タイプ（Type）] に [dot1x] を設定します。[利用可能なサーバグループ（Available Server Groups）] で、作成したグループを選択します。この例では、ISE-Server-Group を作成しています。認可機能を使用しない場合は、[認可（Authorization）] チェックボックスをオフにします。[デバイスに適用（Apply to Device）] をクリックします。



4. 認可機能を設定する場合は、[認可（Authorization）] に移動し、[タイプ（Type）] で [ネットワーク（network）] を選択します。[使用可能なサーバグループ（Available Server Groups）] で [ISE-Server-Group] を選択し、[デバイスに適用（Apply to Device）] をクリックします。



EWC ネットワークの管理

GUI を使用した管理アクセスの設定

EWC コントローラの管理アクセスインターフェイスは、コントローラのインバンド管理やエンタープライズサービスへの接続に使用されるデフォルトインターフェイスです。また、コントローラとアクセスポイント間の通信にも使用されます。[運用（Administration）] > [管理（Management）] > [HTTP/HTTPS/Netconf] に移動します。

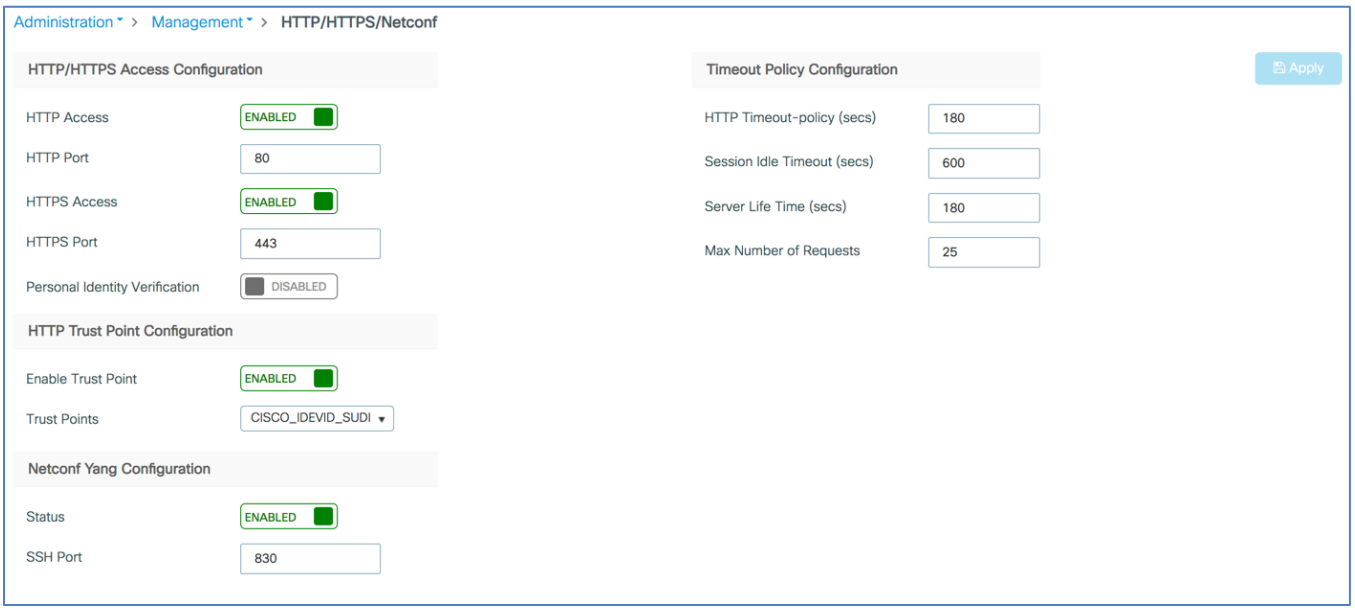
[HTTPアクセス（HTTP Access）] : HTTP アクセスモードを有効にするには、[HTTPアクセス（HTTP Access）] ドロップダウンリストで [有効（Enabled）] を選択します。有効にすることで、Web ブラウザから https://<ip アドレス> の形式でコントローラ GUI にアクセスできます。有効にしない場合は、[無効（Disabled）] を選択します。

デフォルトは [無効（Disabled）] です。HTTP アクセスモードでの接続は安全ではありません。

[HTTPSアクセス（HTTPS Access）] : HTTPS アクセスモードを有効にするには、[HTTPSアクセス（HTTPS Access）] ドロップダウンリストで [有効（Enabled）] を選択します。有効にすることで、Web ブラウザから https://<ip アドレス> の形式でコントローラ GUI にアクセスできます。有効にしない場合は、[無効（Disabled）] を選択します。

デフォルトは [有効（Enabled）] です。HTTPS アクセスモードでの接続は安全です。

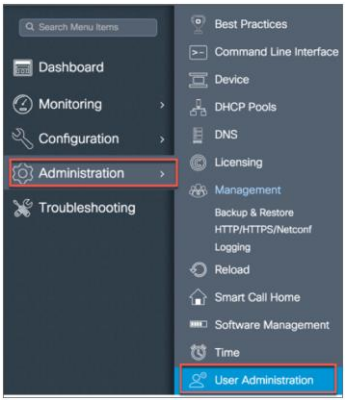
同様に、HTTP トラストポイントはデフォルトで有効になっています。また、Netconf もデフォルトで有効になっており、デフォルトのポート番号は 830 です。

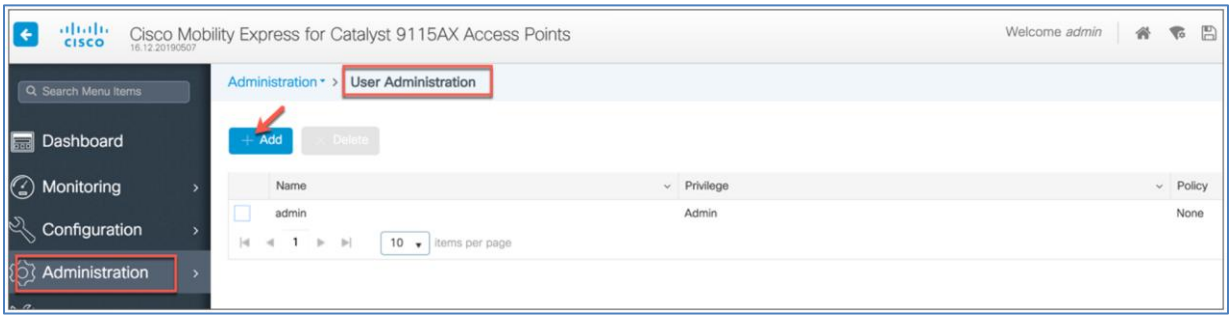


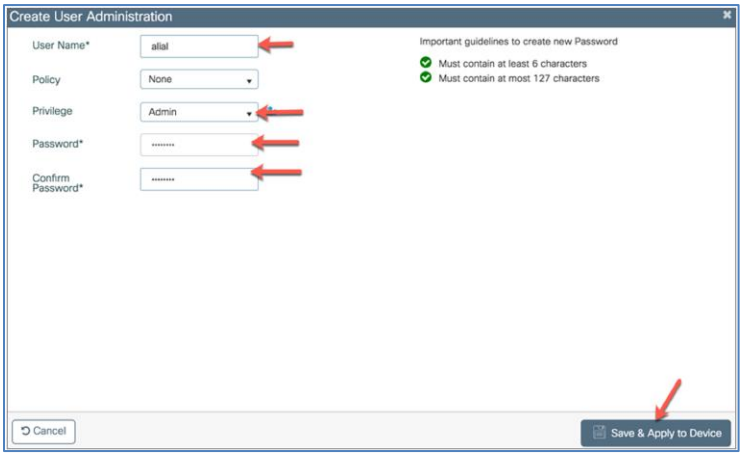
管理者アカウントの管理

管理者のユーザ名とパスワードを設定しておくと、権限のないユーザがコントローラの設定を変更したり設定情報を表示したりするのを防げます。

EWC コントローラにログインしてワイヤレスネットワークを設定/モニタリングするには、管理者ユーザアカウントが必要です。読み取り/書き込み権限または読み取り専用権限を設定するには、WLC のメインメニューに移動し、[運用（Administration）] > [ユーザ管理（User Administration）] > [追加（Add）] の順に選択します。

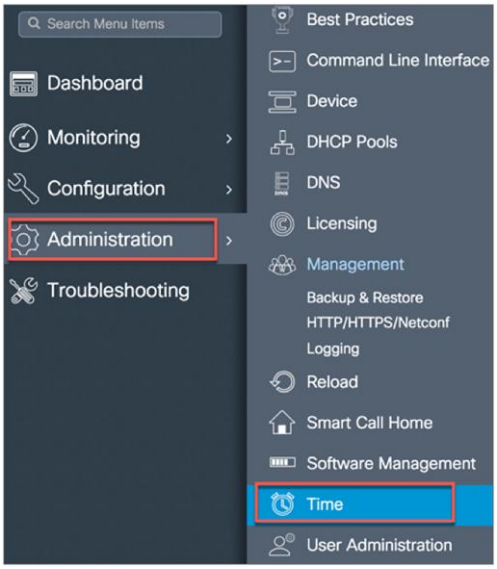




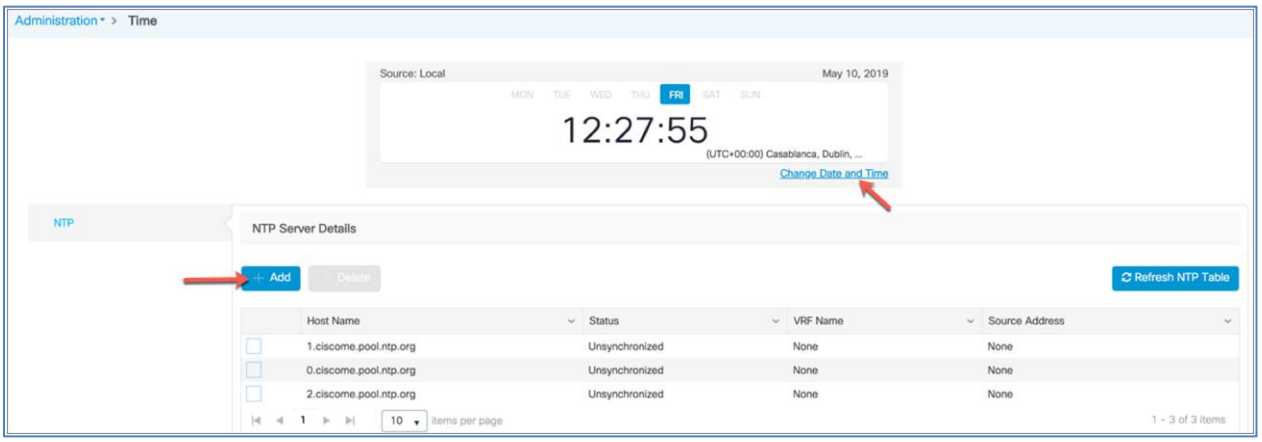


EWC での時刻の管理

最初の Wireless Express セットアップウィザードでは、まず Cisco EWC のシステム日時を設定します。[運用（Administration）] > [時刻（Time）] を選択すれば WLC メニューから時刻を設定/変更できます。



Network Time Protocol（NTP）サーバは、Wireless Express セットアップ中に日付と時刻が設定されていない場合に同期するように設定できます。コントローラ上のタイムゾーンは、Greenwich Mean Time（GMT; グリニッジ標準時）を基準として設定します。特定の NTP サーバを EWC に追加/更新することもできます。



Cisco EWC ソフトウェアのアップデート

Cisco Catalyst EWC ソフトウェアは、コントローラの Web インターフェイスを使用してアップデートできます。ソフトウェアをアップデートすると、コントローラソフトウェアと関連のすべての AP がアップデートされます。古いソフトウェアがインストールされている AP は、マスター AP に参加すると自動的に EWC ソフトウェアにアップグレードされます。コントローラに新たに参加する AP は、そのソフトウェアのバージョンとマスター AP のバージョンを比較し、一致しない場合は、ソフトウェアのアップグレードを要求します。マスター AP は、新たに参加する AP に新しいソフトウェアを転送するよう TFTP サーバに要求します。

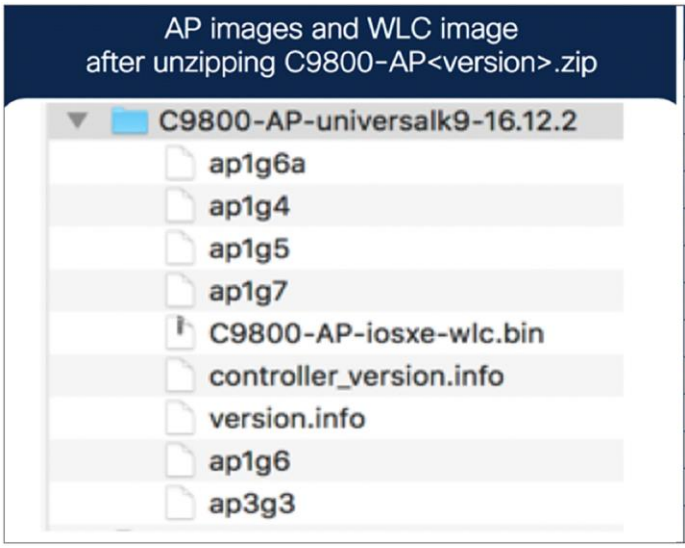
Cisco Catalyst 9115AX および 9120AX シリーズのアクセスポイントは、同じ AP イメージファイル（ap1g7）を共有します。一方、9117AX シリーズのイメージは ap1g6、C9130 シリーズ AP のイメージは ap1g6a（**C9800-AP-universalk9 <バージョン>.zip** ファイルに含まれる）です。HTTP 転送モードの場合は、ローカルマシン上のアクセスポイント イメージ ファイルへのパスを指定します。

アクティブ AP は、従属 AP にイメージを転送するよう TFTP サーバに要求します。AP イメージは TFTP サーバに格納されており、要求に応じて TFTP サーバから提供されます。

EWC ネットワークをアップグレードする前に、次の前提条件が満たされていることを確認します。

HTTP ソフトウェアアップデートの前提条件

- ネットワークは同じタイプ、つまり、すべての AP が同じ AP イメージタイプを使用している必要があります。そうでない場合は、TFTP/SFTP でのダウンロードが必要です。
- Cisco.com からダウンロードした各 AP イメージ（ap1g6、ap1g6a、ap1g7、ap3g3 など）と WLC イメージ（C9800-AP-iosxe-wlc.bin）を含む AP バンドルが解凍され、ローカルマシンにコピーされます。
- 解凍された EWC イメージフォルダおよび AP モデルと AP イメージの対応を以下に示します。

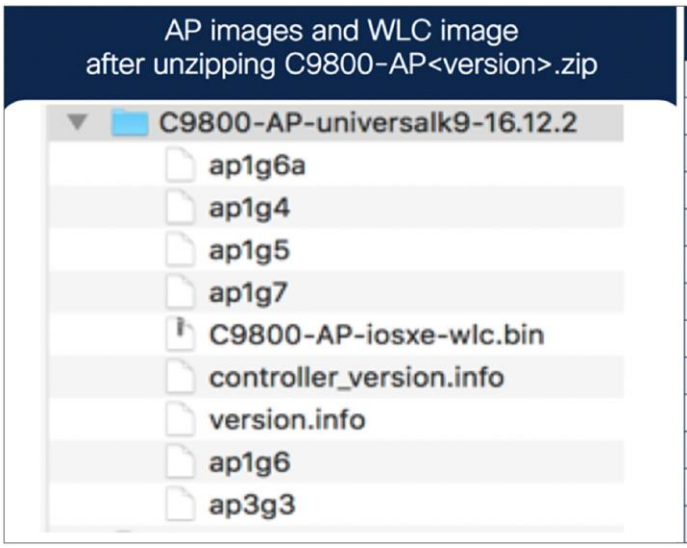


AP Model	AP Image
C9115AX	ap1g7
C9117AX	ap1g6
C9120AX	ap1g7
C9130AX	ap1g6a
AIR-AP1815	ap1g5
AIR-AP1832	ap1g4
AIR-AP1840	ap1g5
AIR-AP1852	ap1g4
AIR-AP2802	ap3g3
AIR-AP3802	ap3g3
AIR-AP4802	ap3g3
AIR-AP1542	ap1g5
AIR-AP1562	ap3g3

図 5.
AP モデルと AP イメージの対応

TFTP ソフトウェアアップデートの前提条件

- TFTP サーバが WLC の管理 IP アドレスから到達できる必要があります。
- Cisco.com からダウンロードした AP イメージ（ap1g6、ap1g6a、ap1g7、ap3g3 など）と WLC イメージ（C9800-AP-iosxe-wlc.bin）を含むアップグレードバンドルが解凍され、TFTP サーバにコピーされている必要があります。解凍された EWC イメージフォルダおよび AP モデルと AP イメージの対応を以下に示します。



AP Model	AP Image
C9115AX	ap1g7
C9117AX	ap1g6
C9120AX	ap1g7
C9130AX	ap1g6a
AIR-AP1815	ap1g5
AIR-AP1832	ap1g4
AIR-AP1840	ap1g5
AIR-AP1852	ap1g4
AIR-AP2802	ap3g3
AIR-AP3802	ap3g3
AIR-AP4802	ap3g3
AIR-AP1542	ap1g5
AIR-AP1562	ap3g3

図 6.
AP モデルと AP イメージの対応

ソフトウェアアップデートの手順

Cisco.com から **C9800-AP-universalk9<バージョン>.zip** ファイルをダウンロードします。HTTP 転送モードの場合は、EWC Web UI へのアクセスに使用しているローカルマシンにファイルがダウンロードされます。TFTP 転送モードの場合は、TFTP サーバを実行しているデバイスに zip ファイルがダウンロードされます。

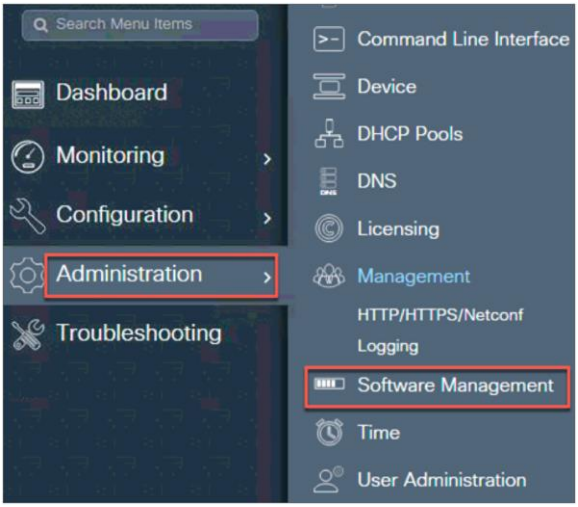
- ファイルを解凍して AP イメージを抽出します。
- 転送モードとして [HTTP]、[TFTP]、[SFTP] のいずれかを選択し、ソフトウェア アップグレード ページで対応するパラメータを設定します。
- EWC ネットワークでイメージのプレダウンロードを開始します。
- EWC および関連するアクセスポイントを再起動してアクティブにします。

ソフトウェアアップデートを開始するには、次の手順を実施します。

HTTP でのダウンロード手順

ステップ 1 ベータサイトからローカルマシンに **C9800-AP-universalk9<バージョン>.zip** ファイルをダウンロードします（解凍済みファイル）。

ステップ 2 WLC のメインメニューから [運用（Administration）] > [ソフトウェア管理（Software Management）] > [ソフトウェアアップグレード（Software Upgrade）] の順に移動します。

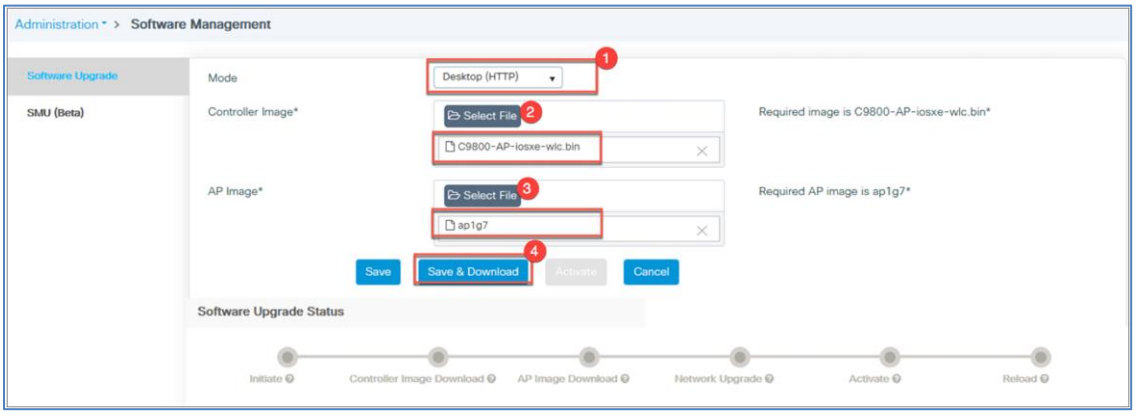


ステップ 3 [モード（Mode）] ドロップダウンメニューから [デスクトップ（HTTP）（Desktop (HTTP)）] を選択します。

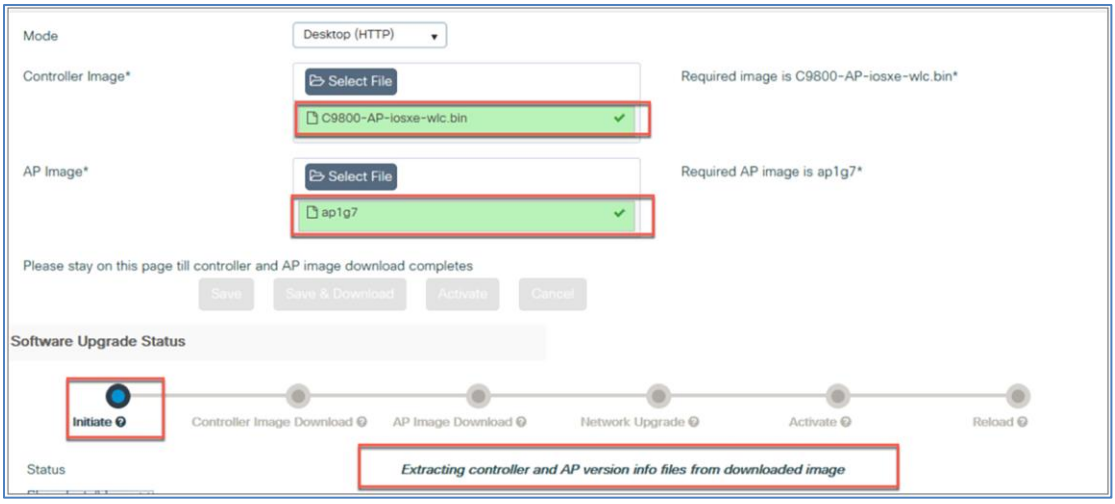
[コントローライメージ（Controller Image）] オプションで [ファイルの選択（Select File）] をクリックすると、ローカルマシンのドライブが開きます。**C9800-AP-iosxe-wlc.bin** ファイルを選択します。

[APイメージ（AP Image）] オプションで [ファイルの選択（Select File）] をクリックするとローカルマシンのドライブが開きますので、AP イメージファイルを選択します。

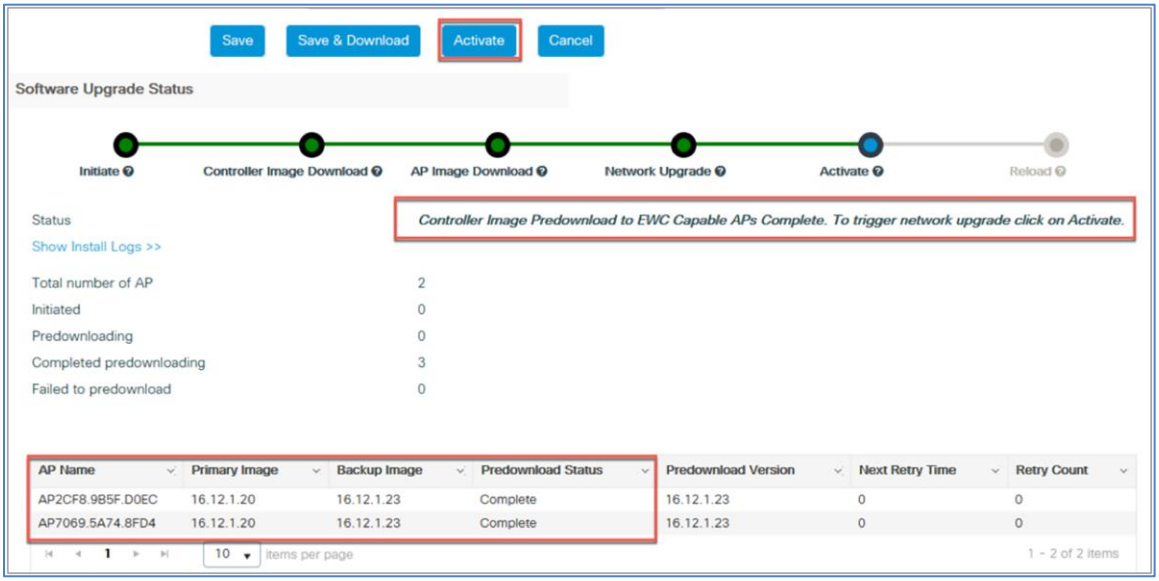
[保存してダウンロード（Save and Download）] をクリックします。コントローラと AP イメージの進捗バーがすべて緑になって完了したことを示すまでそのまま待機します。



ステップ 4 ソフトウェアアップグレードのステータスを確認します。ステータスには、AP およびコントローライメージのアップデートに関するメッセージが表示されます。オプションのボタン（[保存（Save）]、[保存してダウンロード（Save and Download）]、[有効化（Activate）]）はグレー表示になります。

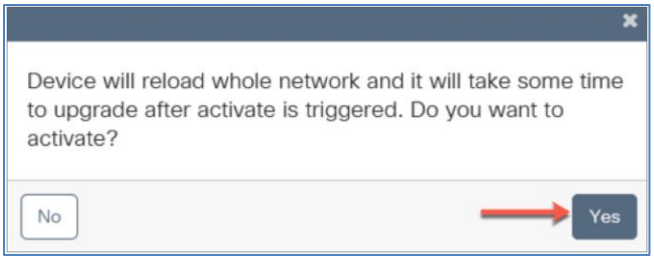


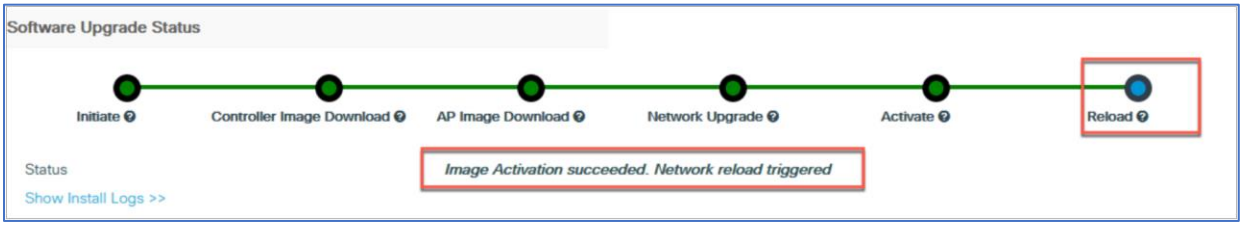
ステップ 5 ソフトウェアアップグレードのステータスに「**Controller Image Predownload to EWC Capable APs Complete（EWC 対応 AP へのコントローライメージのプレダウンロードが完了しました）**」というメッセージが表示されたら、[有効化（Activate）] ボタンをクリックしてソフトウェアを起動します。



警告ウィンドウがポップアップし、デバイスが再起動されることを示すメッセージが表示されます。

[はい（Yes）] をクリックすると EWC がリロードされ、アップデートされたソフトウェアが再起動されます。

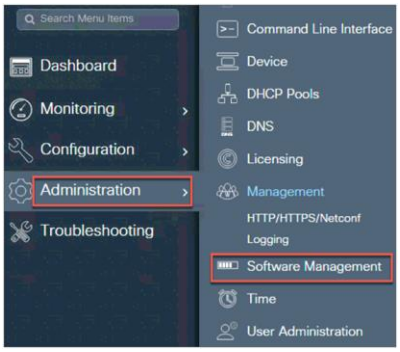




TFTP でのダウンロード手順

ステップ 1 **C9800-AP-universalk9<バージョン>.zip** ファイルをベータサイトから TFTP サーバにダウンロードします（解凍済みファイル）。

ステップ 2 WLC のメインメニューから [運用（Administration）] > [ソフトウェア管理（Software Management）] > [ソフトウェアアップグレード（Software Upgrade）] の順に移動します。

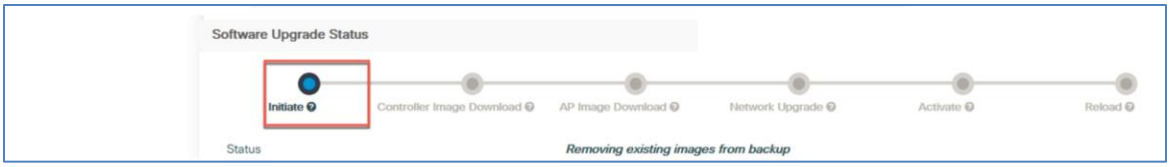


ステップ 3 [モード（Mode）] ドロップダウンメニューから [TFTP] を選択します。

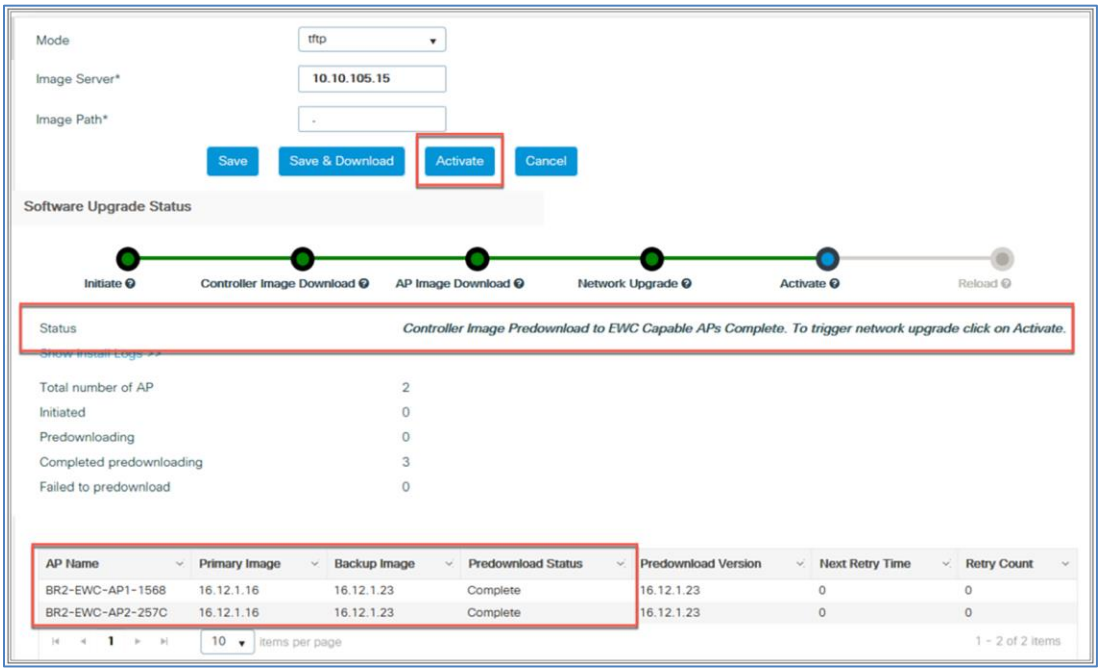
イメージサーバの IP アドレス（TFTP サーバの IP アドレス）を選択します。

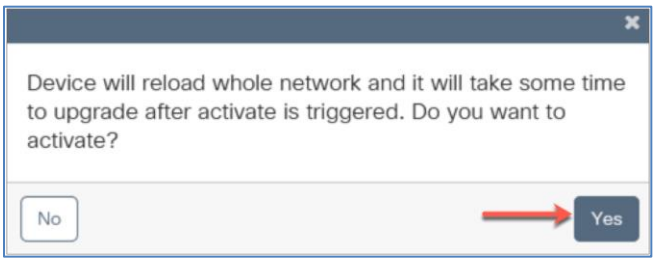
パスを定義します。TFTP サーバに TFTP ディレクトリがすでに存在する場合は、ピリオド（.）を使用します。

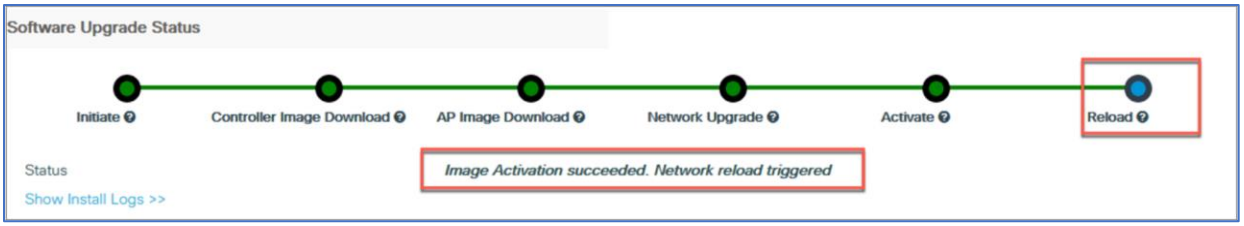
[保存してダウンロード（Save and Download）] をクリックして、ソフトウェアアップグレードを開始します。



ステップ 4 ソフトウェアアップグレードのステータスに「**Controller Image Predownload to EWC Capable APs Complete（EWC 対応 AP へのコントローライメージのプレダウンロードが完了しました）**」というメッセージが表示されたら、[有効化（Activate）] ボタンをクリックしてソフトウェアを起動します。





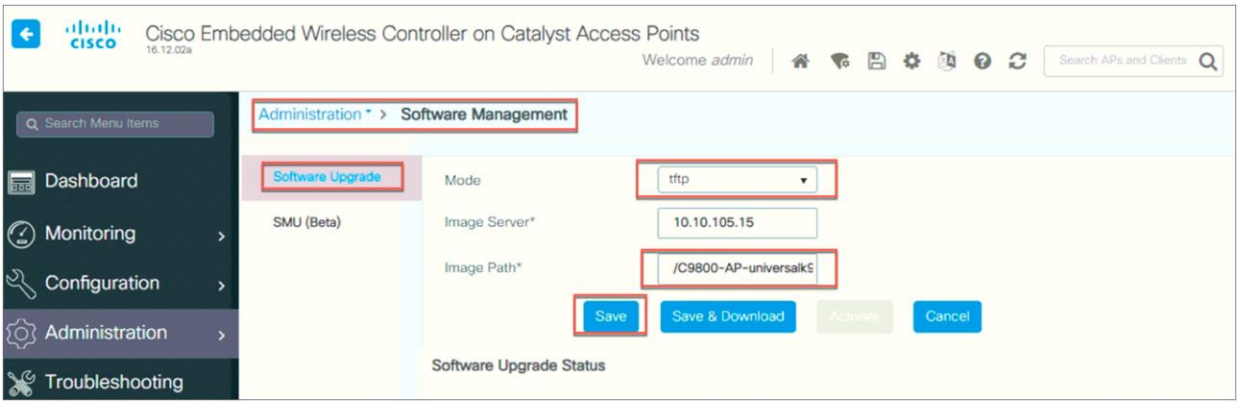


異種ネットワーク用の AP イメージ ダウンロード プロファイル

EWC ネットワークに追加される AP がアクティブ EWC と同じモデル、同じイメージである場合、ソフトウェアをホストする外部サーバは必要ありません。AP のモデルとイメージがアクティブ AP と異なる場合は、AP が参加する際にソフトウェアをダウンロードできるように、ソフトウェアをホストする外部サーバが必要です。

たとえば EWC ネットワークのアクティブ EWC が 9120AX で、従属 AP が 9115AX、9117AX、9130AX モデルである場合、9117AX および 9130AX AP がソフトウェアをダウンロードできるように、ソフトウェアをホストする外部サーバをセットアップする必要があります。

WLC のメインメニューから、[運用（Administration）] > [ソフトウェア管理（Software Management）] > [ソフトウェアアップグレード（Software Upgrade）] に移動します。転送モードとして TFTP または SFTP を選択します。TFTP または SFTP のパラメータを設定して [保存（Save）] をクリックし、プロファイルを保存します。



詳細設定の活用

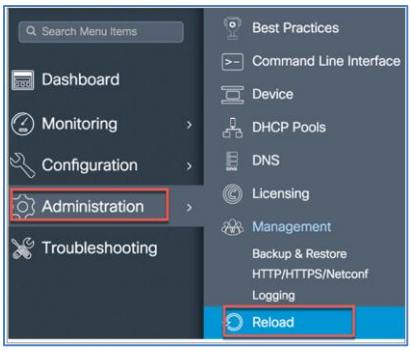
ロギング

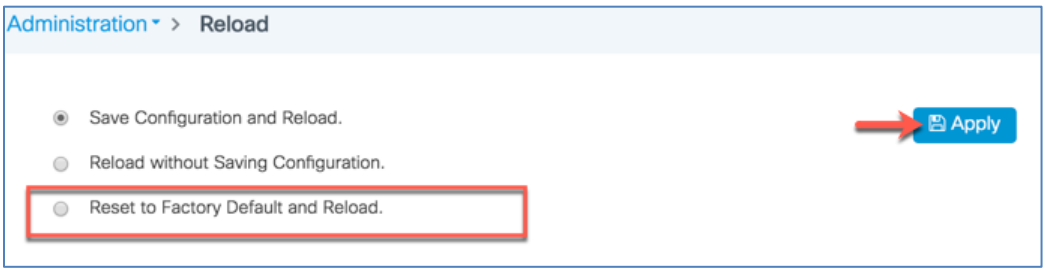
システムメッセージロギングは、システムイベントを syslog サーバと呼ばれるリモートサーバに記録する機能です。各システムイベントは、イベントの詳細を含む syslog メッセージをトリガーします。

システムメッセージロギング機能が有効になっている場合、コントローラは、コントローラに設定されている syslog サーバに syslog メッセージを送信します。

工場出荷時のデフォルトにリセット

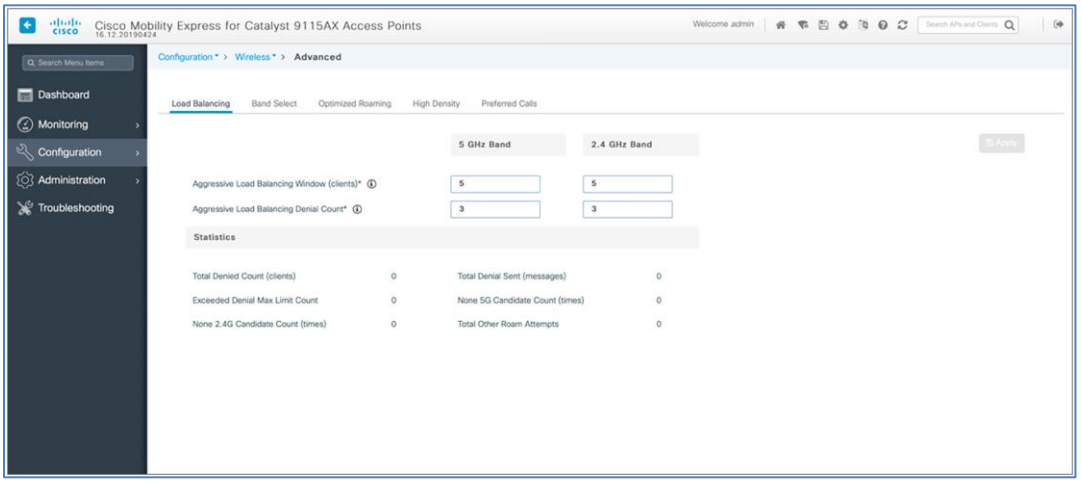
EWC ネットワークを工場出荷時のデフォルトにリセットすることで、初期状態に戻すことができます。





ワイヤレス詳細設定

WLC のメインメニューから [設定（Configuration）] > [ワイヤレス（Wireless）] > [詳細（Advanced）] に移動し、[ロードバランシング（Load Balancing）]、[帯域幅選択（Band Select）]、[最適化ローミング（Optimized Roaming）] などの高度なパラメータを設定することもできます。



EWC HA アクティブおよびスタンバイ

Cisco Catalyst EWC は Cisco Catalyst 9100 アクセスポイントでサポートされており、アクティブ AP が選択される際にどの 9100 AP が EWC 機能を実行するかが決まります。アクティブ AP が選択された後に EWC 対応の他の従属 9100 AP がアクティブ AP に参加するとスタンバイ AP が選択され、冗長構成が形成されます。

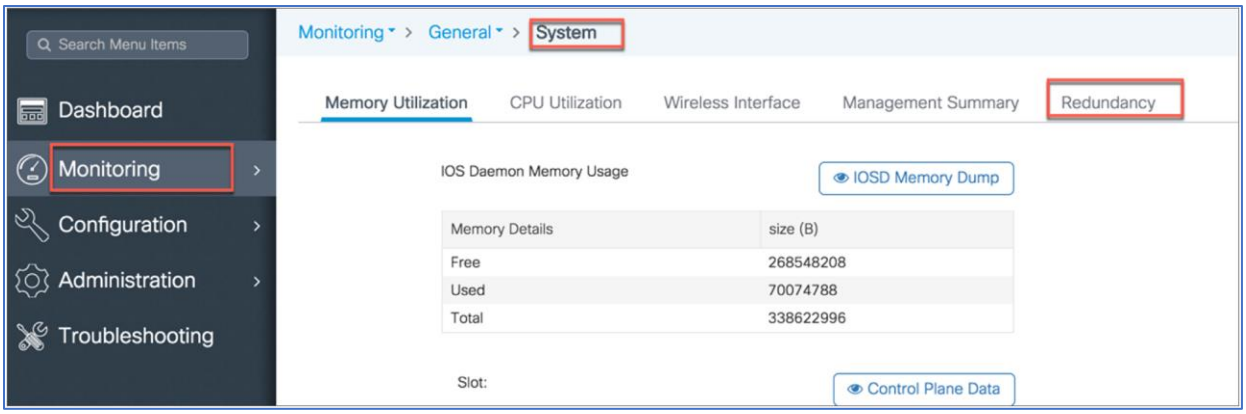
この高可用性（HA）アーキテクチャは、Cisco Catalyst 9800 HA アーキテクチャをベースにしながら、さらに次の特徴があります。

HA ペアリングの仕組みが異なります。最初の起動では、アクティブ EWC はすべての AP が参加するまで待機します。次に、（自動選択または設定によって）指定されたスタンバイ AP を選択し、そのロールと HA パラメータ（ローカル/ピア IP、キープアライブ間隔、優先順位など）を CAPWAP 制御メッセージを介して選択した AP に送信します。

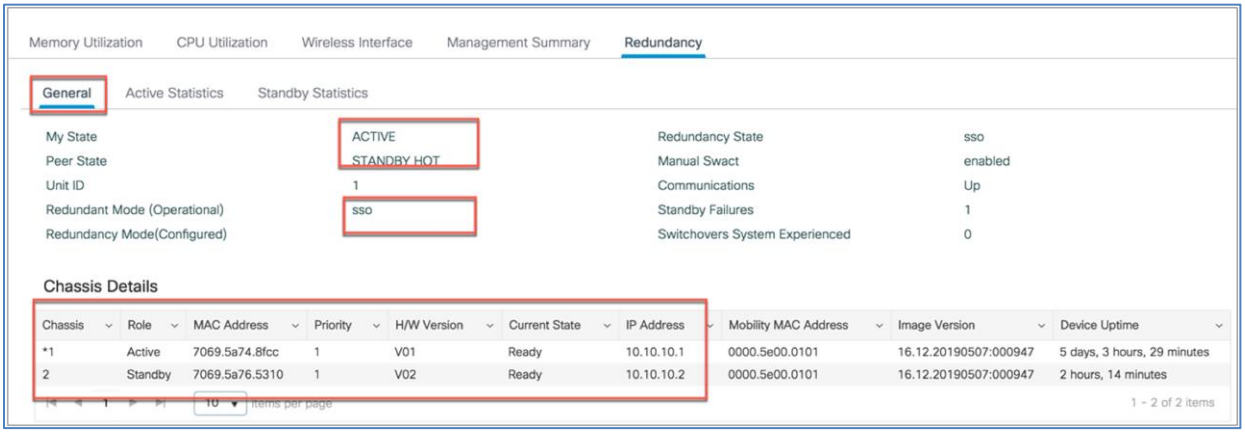
選択したスタンバイ AP が起動し、手動操作なしで HA パラメータが動的に設定されます。

アクティブ AP とスタンバイ AP 間の冗長性を確認するには、EWC GUI にアクセスします。

[モニタリング（Monitoring）] > [システム（System）] > [冗長性（Redundancy）] に移動します。



[全般（General）] タブでアクティブモードとスタンバイモードの詳細を確認できます。



アクティブ EWC の選択プロセス

EWC 選択プロセスは、コントローラを起動する AP を選択するためのプロセスです。Virtual Router Redundancy Protocol（VRRP）を使用してアクティブ AP を選択します。アクティブ/スタンバイ EWC の選択ロジックを以下に示します。

アクティブ EWC の選択

次のアルゴリズムで 2 つの AP を比較します。

- 優先コントローラとして設定されている AP が最も優先されます。
- 次に AP のタイプが比較されます。モデル番号が大きい AP ほど値が高くなり、最も高い値の AP がアクティブになります。

- AP のタイプが同じ場合は、クライアントの負荷（アソシエートしているクライアントの数）が比較され、負荷が一番小さい AP が選択されます。
- 上記で決まらない場合（AP 間ですべて同じ場合）、MAC アドレスが最も小さい AP がアクティブになります。

スタンバイ EWC の選択（Day-1 時のみ）

スタンバイ EWC は VRRP では選択されません。次のように選択されます。

- アクティブ EWC が決まり、外部 AP が参加してからスタンバイの選択が始まります。
- 外部 AP が参加すると、アクティブ EWC によって参加したすべての AP に優先順位が割り当てられます。優先順位が最も高い AP がスタンバイとして選択されます。複数の AP で優先順位が同じ場合、MAC アドレスが最も小さい AP が選択されます。EWC イメージがインストールされている EWC 対応 AP のみが選択の対象になります。
- 優先順位は、次のパラメータに基づいて計算されます。
  - ユーザによる明示的な設定：次の優先コントローラとして優先順位が最も高い AP を選択します。
  - AP タイプ
  - AP 参加時刻

Day-0 と Day-1 の違い

Day-0 にはスタンバイの概念はありません。Day-0 では、アクティブ EWC が 1 つだけ存在します。何らかの理由でアクティブ EWC がダウンすると、新しい EWC を選択するために VRRP による選択が再度行われます。

注：1 台の AP でコントローラが実行されると、コントローラとして機能していない他の AP よりも常に優先順位が高くなります。たとえば、9115AX シリーズ AP が 1 台起動すると、選択できる他の AP がないため、その AP がアクティブになってコントローラを起動します。このネットワークで 9117AX シリーズ AP を起動しても、9115AX よりモデル番号は大きいですが、コントローラがすでにネットワークで稼働しているため、コントローラにはなりません。選択プロセスは、2 つの AP を同時に起動した場合にのみ開始されます。

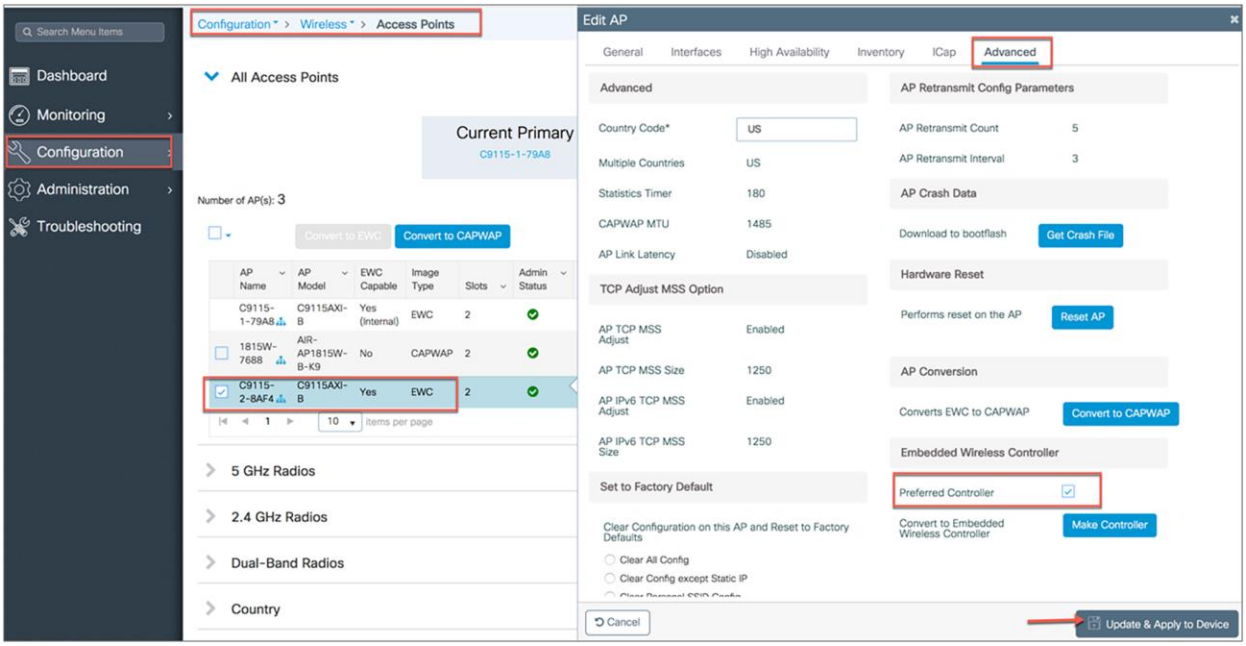
優先コントローラの選択（新しいスタンバイ EWC）

アクティブ EWC とスタンバイ EWC は、上記のプロセスで選択されます。ただし、何らかの理由でスタンバイとして別の AP を選択する場合は、任意の EWC 対応 AP を優先コントローラとして選択できます。

注：現在スタンバイではない別の AP を優先コントローラとして選択すると、現在のスタンバイ EWC がダウンし、選択した新しい EWC がスタンバイ EWC になります。

ステップ 1：優先コントローラにする EWC AP を選択します。

ステップ 2：AP の [詳細（Advanced）] タブに移動して [組み込みワイヤレスコントローラ（Embedded Wireless Controller）] の下の [優先コントローラ（Preferred Controller）] を選択し、[更新してデバイスに適用（Update & Apply to Device）] をクリックします。



[コントローラに指定（Make Controller）] オプション（新しいアクティブ EWC の選択）

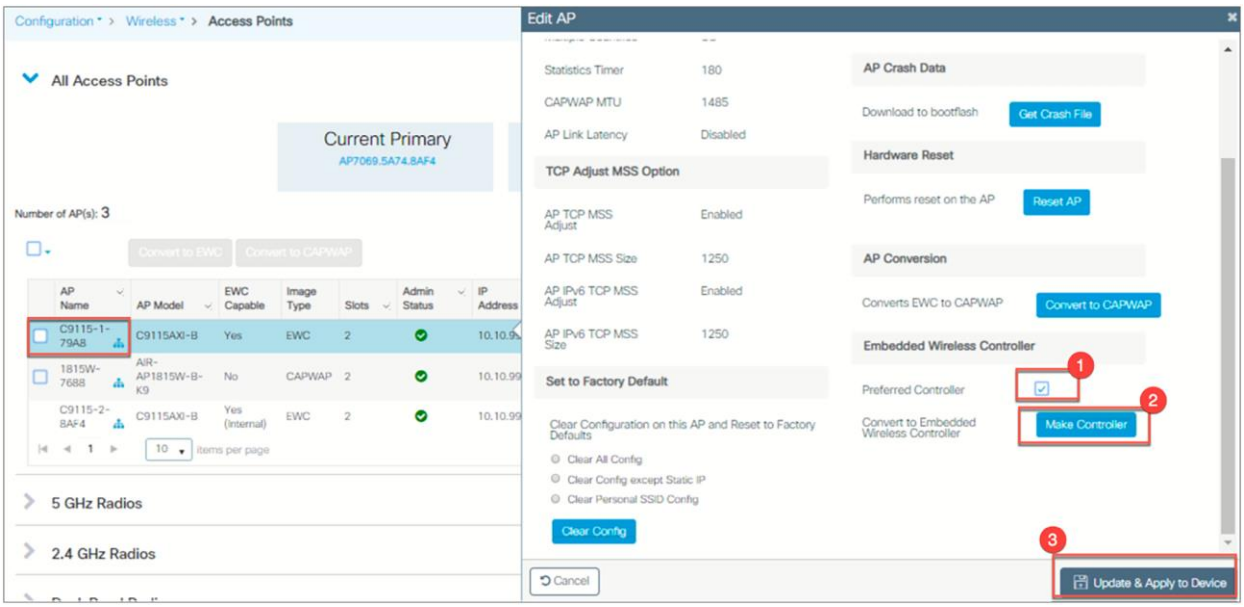
アクティブ EWC とスタンバイ EWC は、上記のプロセスで選択されます。ただし、何らかの理由で別の AP をアクティブ EWC として選択する場合は、[コントローラに指定（Make Controller）] オプションを使用します。このオプションを使用する前に、対象の AP を優先コントローラとして設定する必要があります。現在アクティブではない EWC AP をコントローラとして選択すると、リロード後に新しい AP がアクティブ EWC になり、現在の EWC が新たにスタンバイになります。

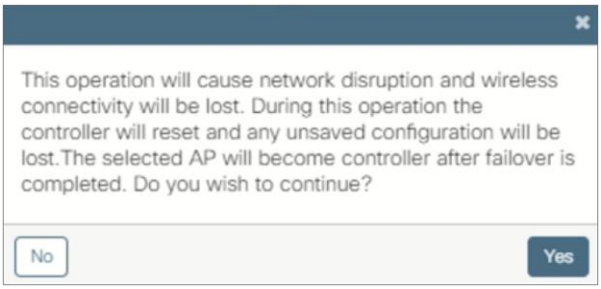
ステップ 1：優先コントローラにする EWC AP を選択します。

ステップ 2：AP の [詳細（Advanced）] タブに移動して [組み込みワイヤレスコントローラ（Embedded Wireless Controller）] の下の [優先コントローラ（Preferred Controller）] を選択し、[更新してデバイスに適用（Update & Apply to Device）] をクリックします。

ステップ 3：EWC AP の [詳細（Advanced）] タブに戻って [コントローラに指定（Make Controller）] をクリックし、[更新してデバイスに適用（Update & Apply to Device）] をクリックします。

注：この操作によってコントローラがリセットされるため、ネットワークが中断されることを警告するメッセージが表示されます。





OS 変換

注：CAPWAP から EWC への変換は、AireOS 8.10.105.0 または Cisco IOS®XE 16.12.2s 以降でサポートされています。CAPWAP を EWC に変換するには、9100 アクセスポイントの CAPWAP イメージが 8.10.105.0 または 16.12.2 以降でなければなりません。

Cisco Catalyst 9100 アクセスポイントは、CAPWAP AP または EWC 対応 AP（EWC ネットワークでコントローラ機能を実行）として動作して他のアクセスポイントを管理し、クライアントにサービスを提供します。

次の変換がサポートされています。

CAPWAP AP から EWC 対応 AP への変換：この変換は、8.10.X または 16.12.X CAPWAP イメージを実行する 9100 アクセスポイントがあり、それを使用して EWC ネットワークを展開する場合に必要です。そのために、CAPWAP AP をアクティブ EWC AP（EWC ネットワークでコントローラ機能を実行する AP）に変換します。

Cisco Catalyst 9100 アクセスポイントは、次の 2 種類のイメージをサポートしています。

CAPWAP イメージ：アクセスポイントにインストールされた CAPWAP イメージは CAPWAP アクセスポイントとしてのみ動作し、コントローラ機能はサポートしません。

EWC イメージ：アクセスポイントにインストールされた EWC イメージは、コントローラとアクセスポイントの両方として動作することも、アクセスポイント単独として動作することも可能です。

アクセスポイントのイメージと機能を確認するには、AP の CLI で show version コマンドを実行します。結果から AP イメージタイプを判断して AP 設定を確認できます。

show version コマンドで AP イメージタイプと AP 設定パラメータが表示されない場合は、AP が CAPWAP イメージを実行しているということです。

show version コマンドで AP イメージタイプが EWC IMAGE と表示され、AP 設定が EWC CAPABLE と表示される場合、コントローラとアクセスポイントの両方として動作します。フェールオーバーした場合は、アクティブ AP 選択プロセスの対象となります。

show version コマンドで AP イメージタイプが EWC IMAGE と表示され、AP 設定が NOT EWC CAPABLE と表示される場合は、アクセスポイントとしてのみ動作し、フェールオーバー時にアクティブ AP 選択プロセスの対象にはなりません。

show version コマンドの結果サンプルを次に示します。

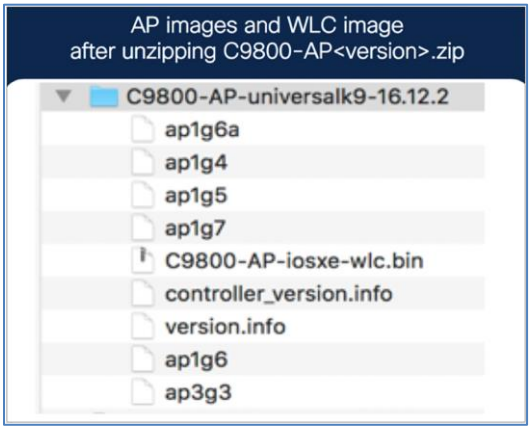
```
Cisco C9117AXI-B  with 1927052/380724K bytes of memory.
Processor board ID KWC224709BU
AP Running Image      : 16.12.2
Primary Boot Image    : 16.12.2
Backup Boot Image     : 8.10.105.5
Primary Boot Image Hash:
Backup  Boot Image Hash:
AP Image type     : EWC IMAGE
AP Configuration : EWC CAPABLE
1 Gigabit Ethernet interfaces
2 802.11 Radios
Radio FW version : QC_IMAGE_VERSION_STRING=WLAN.HK.1.0-03095-QCAHKSWPL_SILICONZ-
1.198262.4.200256.9


NSS FW version : NSS.HK.H.CS.q_len512-E_custC
cisco C9117AXI-B  with 1927052/1296108K bytes of memory of memory.
Processor board ID RFDP2BCR021
AP Running Image : 16.12.2
Primary Boot Image : 16.12.2
Backup Boot Image : 8.10.105.5
AP Image type : EWC IMAGE
AP Configuration : NOT EWC CAPABLE
2 Gigabit Ethernet interfaces
2 802.11 Radios
Radio FW version : 1401b63d121b073a3008aa67f0c039d0
NSS FW version : NSS.AK.1.0.c4-00O26-E_cust C-1. 24160.1
```

CAPWAP AP から EWC AP への変換

CAPWAP イメージを実行しているアクセスポイントを EWC 対応アクセスポイントに変換するには、EWC イメージを TFTP サーバからダウンロードしてインストールする必要があります。TFTP サーバから EWC イメージをダウンロードし、AP 設定を EWC CAPABLE に変換する単一のコマンドが用意されています。

CAPWAP AP を EWC AP に変換するための前提条件

- 解凍された EWC イメージファイルが TFTP サーバに保管されている必要があります。解凍されたファイルには、EWC イメージ C9800-AP-iosxe-wlc.bin と、それぞれの AP イメージ（ap1g6、ap1g6a、ap1g7）が含まれています。



AP Model	AP Image
C9115AX	ap1g7
C9117AX	ap1g6
C9120AX	ap1g7
C9130AX	ap1g6a

- Cisco Catalyst 9100 アクセスポイントに IP アドレスを割り当てる DHCP サーバが必要です。
- EWC イメージをロードする際、9100 アクセスポイントをネットワーク内の既存のコントローラに参加させないでください。AP が参加できる既存のコントローラがネットワーク上にある場合、変換できません。

CAPWAP イメージを実行している AP を EWC に変換するには、次の手順を実施します。

手順

ステップ 1 Cisco Catalyst 9100 アクセスポイントの CLI またはコンソールに接続してログインします。

ステップ 2 **enable** と入力して、特権実行モードに移行します。

ステップ 3 アクセスポイントの CLI で **show version** と入力します。show version の出力結果から AP イメージタイプと AP 設定を確認し、変換プロセスを進めます。

ステップ 4 show version の出力結果に AP イメージタイプと AP 設定が表示されない場合は、AP で CAPWAP イメージが実行されていることを示します。変換するには次のコマンドを実行します。

AP#ap-type EWC tftp://<TFTP サーバ IP>/< ap イメージ> tftp://<TFTP サーバ IP>/< WLC イメージ>

例：AP#ap-type EWC tftp://10.10.10.15/ap1g7 tftp://10.10.10.15/C9800-AP-iosxe-wlc.bin

ステップ 5 AP の再起動後、Day-0 で EWC が開始し、CiscoAirProvision-<MAC> SSID がブロードキャストされます。その後、ワイヤレス設定ウィザードから設定できます。

Web UI を利用して EWC AP から CAPWAP AP に変換

EWC 対応 AP を CAPWAP AP に変換する理由は 2 つあります。

- 9100 アクセスポイントを EWC ネットワークから別のコントローラ（EWC 対応ではない）ネットワークに移行するため。
- 9100 アクセスポイントを EWC ネットワークでのアクティブ AP 選択プロセスの対象にしないため。

AP タイプが CAPWAP の場合 AP にはコントローラ機能がなく、アクティブ AP 選択プロセスの対象になりません。

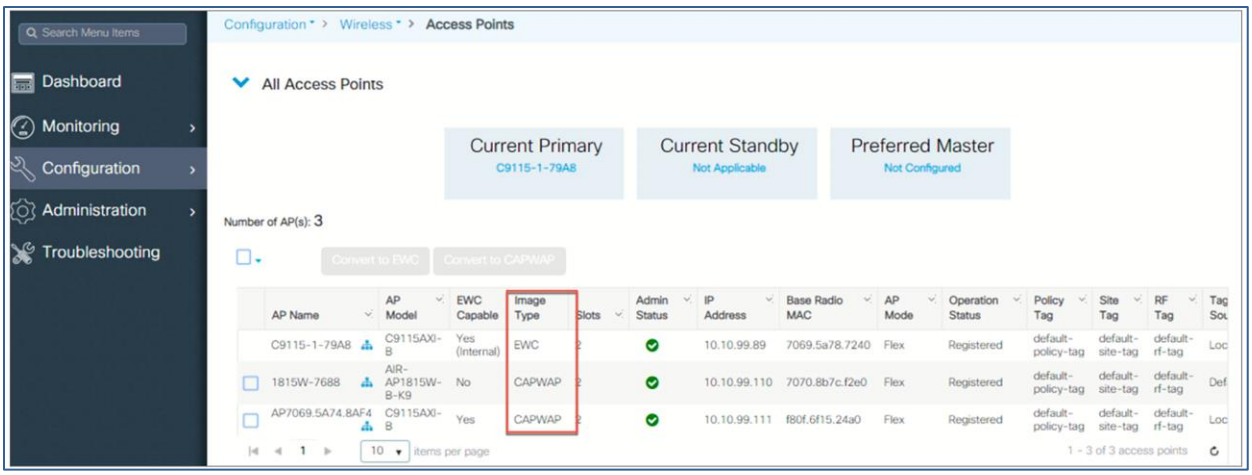
AP タイプを変更した後、その AP を非 EWC ネットワークに移行すると、そのネットワーク内のコントローラに参加します。そのコントローラのイメージが AP のイメージと異なる場合は、新しい CAPWAP イメージがコントローラから要求されます。

AP タイプが CAPWAP の場合（この変換の結果）、AP はコントローラ機能を開始しません。また AP が外部コントローラに参加すると、コントローラから新しいイメージが要求され、AP が CAPWAP イメージを取得します。

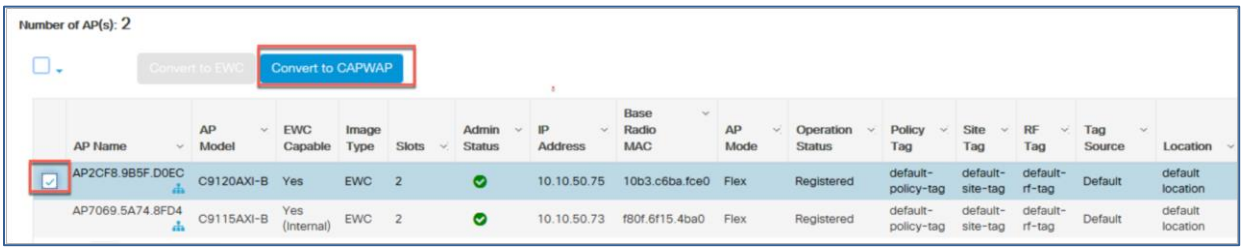
EWC AP を CAPWAP AP に変換するには、次の手順を実施します。

手順

ステップ 1：[設定（Configuration）] > [ワイヤレス（Wireless）] > [アクセスポイント（Access Points）] の順に移動し、AP を表示します。[イメージタイプ（Image Type）] には、AP が CAPWAP か EWC のどちらかが示されます。



ステップ 2：1 つまたは複数の AP を選択して CAPWAP に変換します。



オプション 43 を使用した EWC から CAPWAP への変換

DHCP オプション 43 はベンダー固有のオプションで、アクセスポイントに WLC IP アドレスを付与するために使用されます。オプション 43 を特定のサブタイプオプションと合わせて使用すると、EWC を CAPWAP に変

換して WLC アプライアンスまたは仮想コントローラに参加させられます。ブートアップ時に AP が DHCP オプション 43 とサブタイプ 0xF2 を受信すると、AP タイプは CAPWAP に変換され、通常の参加プロセスに従います。

スイッチの DHCP 設定を次に示します。

```
Switch(dhcp-config)#option 43 hex F2056464645801
```

AP CLI を使用した EWC から CAPWAP AP への変換

アクセスポイントの CLI から 1 つのコマンドを実行することで、EWC から CAPWAP に変換できます。

```
AP#ap-type capwap
```

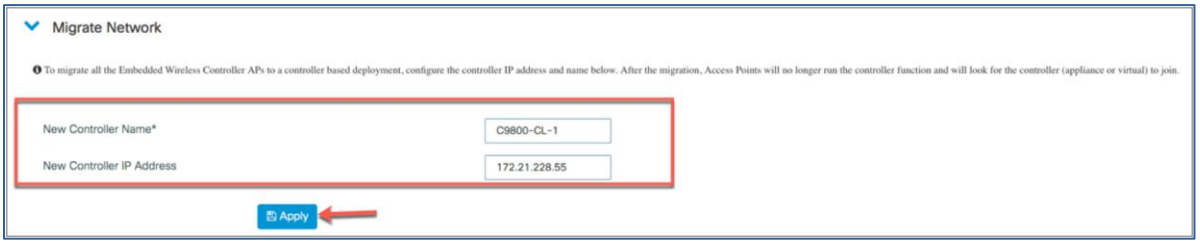
注：アクセスポイントが再起動して、AP タイプが NOT EWC CAPABLE に変わります。また、AP が CAPWAP に変換されると、アクティブ AP 選択プロセスの対象から外れます。

EWC ネットワークからコントローラベースのネットワークへの移行

ネットワークに 100 台を超える AP が必要な場合は、既存の EWC ネットワークをコントローラベースのネットワーク（Cisco Catalyst 9800 シリーズ（アプライアンス/仮想）または AireOS（3504、5520、8540 ワイヤレスコントローラまたは 8.10.X ソフトウェアが稼働する仮想コントローラ））に簡単に移行できます。

ステップ 1：EWC Web UI から、[設定（Configuration）] > [ワイヤレス（Wireless）] > [アクセスポイント（Access Points）] の順に移動し、[ネットワークの移行（Migrate Network）] オプションまで下にスクロールします。

ステップ 2：AP の移行先コントローラの名前と IP アドレスを設定し、[適用（Apply）] をクリックします。移行すると AP はコントローラ機能を実行せず、設定済みのコントローラに参加します。



サイトサーベイオプション

Cisco EWC on Catalyst APs は次世代の自律型 EWC で、Cisco IOS XE リリース 16.12.2s のサイトサーベイ機能をサポートしています。EWC イメージが搭載された次のアクセスポイントは、サイトサーベイ機能をサポートしています。

Cisco Catalyst 9120AX シリーズ（C9120AX-x）

Cisco Catalyst 9117AX シリーズ（C9117AX-x）

Cisco Catalyst 9115AX シリーズ（C9115AX-x）

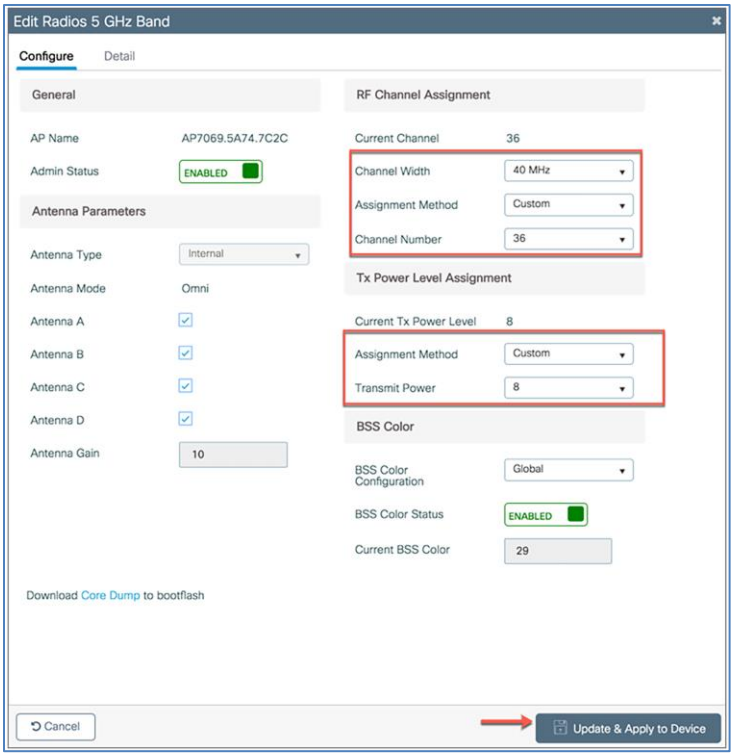
Cisco Catalyst 9130AX シリーズ（C91130AX-x）

Cisco EWC は内部の DHCP サーバをサポートし、ping 可能ゲートウェイなしで動作します。そのためユーザは、バッテリパックを搭載したアクセスポイントとクライアントデバイスでアクティブ調査を実施できます。電源アダプタは外部の電源に接続する必要があります。

サイトサーベイ AP として EWC を稼働させるには、このドキュメントの「Day-0 プロビジョニング」の項で説明している Day-0 設定から始める必要があります。

プロビジョニングが完了し、設定した SSID が開始されたら定義済みの PSK を使用して参加し、Web ブラウザを開いて https://192.168.1.1 または https://mywifi.cisco.com にアクセスします。

無線の伝送パワーとチャネルを設定するには、[設定（Configuration）] > [アクセスポイント（Access Points）] > [5 GHz無線（5 GHz radio）] または[2.4 GHz無線（2.4 GHz radio）] に移動し、AP を選択します。そこで [割り当て方式（Assignment Method）] を [グローバル（Global）] から [カスタム（Custom）] に変更し、必要な値を設定して [更新してデバイスに適用（Update & Apply to Device）] をクリックすると、AP 無線のチャネルと伝送パワーを変更できます。



参照資料

- クイックスタートガイド：
  https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/mobility-express/guide-c07-741338.pdf
- EWC-AP 導入デモ：
  https://xd.adobe.com/view/76b25e06-d905-487c-4de1-3d19719a5ac5-0083/
- CAPWAP AP から EWC-AP への変換デモ：
  https://xd.adobe.com/view/8fd6c90c-2543-4ded-772c-12be163103f7-f9e7/
- Cisco DNA Spaces によるゲストアクセスのデモ：
  https://xd.adobe.com/view/e7af8c14-b2ea-426c-5bf4-0ca6efa022f5-919e/
- リリースノート：
  https://www.cisco.com/c/en/us/td/docs/wireless/controller/ewc/16-12/rel-notes/ewc-rn-16-12-2.html
- 設定ガイド：
  https://www.cisco.com/c/en/us/td/docs/wireless/controller/ewc/16-12/config-guide/ewc_cg_16_12.html
- コマンドリファレンス：
  https://www.cisco.com/c/en/us/td/docs/wireless/controller/ewc/16-12/cmd-ref/ewc_cr_16_12.html
- オンラインヘルプ：
  https://www.cisco.com/c/dam/en/us/td/docs/wireless/controller/ewc/16-12/olh/Default.htm
- モバイルアプリ：
  https://www.cisco.com/c/en/us/td/docs/wireless/controller/ewc/mob-app/user-guide/cisco_catalyst_wifi_app_user_guide.html

お問い合せ先

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

C11-743398-01JA 20.08