Cisco DNA Space におけるシスコ ワイヤレス コントローラおよび Cisco Catalyst 9800 シリーズ コントローラの設定

この章では、Cisco DNA Spaces で動作するシスコ ワイヤレス コントローラ（Cisco AireOS）または Cisco Catalyst 9800 シリーズ コントローラで行う設定について説明します。必要な設定は、使用するワイヤレスコントローラのタイプとコネクタによって異なります。

（注）

- ハイパーロケーションを備えたシスコ ワイヤレス コントローラを Cisco DNA Spaces と Cisco CMX に同時に接続することはできません。
- シスコ ワイヤレス コントローラを Cisco CMX と Cisco DNA Spaces の両方に同時に接続する場合は、 Cisco DNA Spaces コネクタを使用する必要があります。シスコ ワイヤレス コントローラがサポートできる NMSP 接続数の制限を確認し、シスコ ワイヤレス コントローラが Cisco DNA Spaces コネクタへの新しい接続の追加をサポートできることを確認します（特に、複数の Cisco CMX サーバーへの既存の接続がある場合）。
- シスコ ワイヤレス コントローラを Cisco WLC Direct Connect と Cisco DNA Spaces コネクタの両方に同時に接続することはできません。Cisco DNA Spaces コネクタを使用する前に、Cisco WLC Direct Connect を無効にします。
- 特に古いバージョンのシスコ ワイヤレス コントローラを使用している場合は、Cisco WLC Direct Connect ではなく Cisco DNA Spaces コネクタを使用することをお勧めします。また、Operation Insights、Detect and Locate などの特定のアプリは、Cisco DNA Spaces コネクタによってのみサポートされます。
- ワイヤレスネットワークに表示されるデータを Cisco DNA Spaces レポートに表示されるデータと比較することは推奨されません。これは設計上、遅延することが予想されるためです。

（注） 設定はCisco DNA Spacesの一部ではない外部アプリケーションで行うため、このマニュアル内のメニューパス、タブやウィンドウ、オプションなどに指定する名前が変わる場合があります。

さまざまなコネクタタイプでサポートされる機能、およびワイヤレスコントローラとコネクタのさまざまな組み合わせの設定は次のとおりです。

- 各種コネクタがサポートする機能 （2 ページ）
- Cisco CMX を介して Cisco DNA Spaces をシスコ ワイヤレス コントローラに接続する （5 ページ）
- WLC 直接接続または Cisco DNA Spaces コネクタを使用した、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラまたはシスコ ワイヤレス コントローラの Cisco DNA Spaces への接続 （19 ページ）
- Cisco DNA Spaces 拡張ベンチマーク （53 ページ）

各種コネクタがサポートする機能

次の表に、各タイプのコネクタでサポートされている機能を示します。使用する機能またはアプリに基づいてコネクタを選択できます。Operational Insights や Open Roaming などのアプリを使用する場合は、Cisco DNA Spaces コネクタをお勧めします。

表 *1:* コネクタ：機能サポート

機能/アプリ	Cisco DNA Spaces コネクタ	**Cisco WLC Direct Connect**（小規模な展開でのみ推奨）[1] Cisco WLC Direct Connect を使用した Cisco DNA Spaces のシスコ ワイヤレス コントローラへの接続 Cisco WLC Direct Connect を使用した Cisco DNA Spaces の Cisco Catalyst 9800 シリーズ ワイヤレス コントローラへの接続	Cisco CMX テザリングコネクタ	Cisco Meraki
Cisco DNA Spaces ダッシュボード	サポート対象	サポート対象	サポート対象	サポート対象
キャプティブポータル	サポート対象	サポート対象	サポート対象	サポート対象
エンゲージメント	サポート対象	サポート対象	サポート対象	サポート対象
ロケーションペルソナ	サポートあり	サポートあり	サポートあり	サポートあり
位置分析	サポートあり	サポートあり	サポートあり	サポートあり
影響分析	サポートあり	サポートあり	サポートあり	サポートあり
カメラメトリック	未サポート	未サポート	未サポート	サポートあり
行動メトリクス	サポート対象	サポート対象	サポート対象	サポート対象
RightNow WiFi	サポートあり	サポートあり	サポートあり	サポートあり
RightNow Video	未サポート	未サポート	未サポート	サポートあり
Open Roaming[2]	サポート対象	未サポート	未サポート	サポート対象
IoT サービス	サポート対象[3]	未サポート	未サポート	—

機能/アプリ	Cisco DNA Spaces コネクタ	**Cisco WLC Direct Connect**（小規模な展開でのみ推奨）[1] Cisco WLC Direct Connect を使用した Cisco DNA Spaces のシスコ ワイヤレス コントローラへの接続 Cisco WLC Direct Connect を使用した Cisco DNA Spaces の Cisco Catalyst 9800 シリーズ ワイヤレス コントローラへの接続	Cisco CMX テザリング コネクタ	Cisco Meraki
検出と位置特定	サポートあり	限定サポート（関連クライアントのみ）	サポートあり	—
HyperLocation	サポートあり	未サポート	サポートあり	未サポート
FastLocate	サポートあり	未サポート	サポートあり	未サポート
スケールのサポート 詳細については、Cisco DNA Spaces 拡張ベンチマーク（53 ページ）のスケールの概要を参照してください。	スケーリングに最適	AireOS コントローラ 8.8 MR2 および Cisco Catalyst 9800 シリーズ 16.12.1 ではスケールがサポートされます。最大 50 クライアント。	Cisco CMX が処理できるスケールをサポートします。	スケーリングに最適
AireOS コントローラ プラットフォームのサポート	サポート対象	サポート対象	サポート対象	N/A
Cisco Catalyst 9800 プラットフォームのサポート	サポート対象	サポート対象	サポート対象	N/A

[1] シスコ ワイヤレス コントローラの直接接続方式による接続は、小規模な展開でのみ推奨されます。大規模な実稼働展開には、すべて Cisco DNA Spaces コネクタが必要です。
[2] **Open Roaming** アプリはベータ版であるため、現在、このアプリのドキュメントは利用できません。**Open Roaming** に関連する情報については、Cisco DNA Spaces サポートチームにお問い合わせください。
[3] 現在、IoT サービスのサポートは Cisco Catalyst 9800 コントローラでのみ利用可能です。

（注）
- シスコ ワイヤレス コントローラの直接接続方式による接続は、小規模な展開でのみ推奨されます。大規模な実稼働展開には、すべて Cisco DNA Spaces コネクタが必要です。
- **Open Roaming** アプリはベータ版であるため、現在、このアプリのドキュメントは利用できません。**Open Roaming** に関連する情報については、Cisco DNA Spaces サポートチームにお問い合わせください。

Cisco CMX を介して Cisco DNA Spaces をシスコ ワイヤレス コントローラに接続する

Cisco CMX を介して Cisco DNA Spaces をシスコ ワイヤレス コントローラに接続するには、Cisco CMX 10.6 以降が必要です。

Cisco CMX を使用している Cisco Unified Wireless Network の場合、Cisco DNA Spaces と連携するには、次の構成が必要です。

（注）
- インターネット プロビジョニングと RADIUS 認証の構成は、RADIUS 認証が必要な場合にのみ必要です。この構成は、ポータルにソーシャル認証が必要な場合にのみ必要です。

WLC でのアクセスポイントモード、SSID、ACL、スプラッシュ URL、および仮想インターフェイスの設定

キャプティブポータルルールを作成するには、まずアクセスポイントのモードを定義し、シスコ ワイヤレス コントローラで SSID と ACL を作成します。また、SSID のスプラッシュ URL がシスコ ワイヤレス コントローラで設定されていることを確認する必要があります。

（注） SSID と ACL は、Cisco CMX ではなく、シスコ ワイヤレス コントローラで作成されます。

ローカルモードと flexconnect モードでシスコ ワイヤレス コントローラの設定は異なります。

（注） 設定は Cisco DNA Spaces の一部ではないシスコ ワイヤレス コントローラで行うため、このマニュアル内のメニューパス、タブやウィンドウ、オプションなどに指定する名前が変わる場合があります。

Cisco DNA Spaces を使用したローカルモードの設定

シスコ ワイヤレス コントローラ を、ローカルモードの Cisco DNA Spaces を使用するように設定するには、次の手順を実行します。

アクセス ポイントのローカル モードを設定する

アクセス ポイントのローカル モードを設定するには、次の手順を実行します。

ステップ 1 シスコ ワイヤレス コントローラのログイン情報を使用して、ワイヤレスコントローラにログインします。

ステップ 2 シスコ ワイヤレス コントローラのメインウィンドウで、[Wireless] タブをクリックします。

すべてのアクセス ポイントが一覧表示されます。

ステップ 3 モードをローカルに設定するアクセス ポイントをクリックします。

ステップ 4 [General] タブをクリックします。

ステップ 5 [AP Mode] ドロップダウンリストから、[Local] を選択して、[Apply] をクリックします。

シスコ ワイヤレス コントローラでの SSID の作成

（注） SSID は、Cisco CMX ではなく、シスコ ワイヤレス コントローラで作成されます。

シスコ ワイヤレス コントローラで SSID を作成するには、次の手順を実行します。

ステップ 1 シスコ ワイヤレス コントローラのメインウィンドウで、[WLANs] タブをクリックします。

ステップ 2 WLAN を作成するには、ウィンドウの右側にあるドロップダウンリストで [Create New] を選択し、[Go] をクリックします。

ステップ 3 表示される [New] ウィンドウで、[Type]、[Profile Name]、[SSID] などの WLAN の詳細を入力します。

ステップ 4 [Apply] をクリックします。

[Edit <SSID Name>] ウィンドウが表示されます。

ステップ 5 SSID を Cisco DNA Spaces ダッシュボードに追加します。

ステップ 6 シスコ ワイヤレス コントローラ メインウィンドウの [General] タブで、[Broadcast SSID] チェックボックスをオフにします。

（注） SSID ブロードキャストが中断され、設定を完了する前に顧客が SSID にアクセスすることが回避されます。

ステップ 7 **[Security]** > **[Layer 2]** を選択して、[MAC Filtering] チェックボックスをオンにします。

ステップ 8 [Layer 3] タブで、次を設定します。

a) [Layer 3 security] ドロップダウンリストから、[Web Policy] を選択します。

（注） [Web Policy] は、シスコ ワイヤレス コントローラでキャプティブポータルを設定できるようにする Layer 3 セキュリティのオプションです。

b) [On Mac Filter Failure] ラジオボタンを選択します。

c) [Preauthentication ACL] 領域で、[IPv4] ドロップダウンリストから、先に定義した ACL を選択します。

d) スリープ状態のクライアントの [Enable] チェックボックスをオンにします。

（注） スリープ状態のクライアントを有効にすることは必須ではありません。ただし有効にすると、認証後にスリープモードになっている顧客が指定された時間内にスリープ状態から復帰した場合、認証なしで接続されます。Web 認証に成功したゲストアクセスを持つクライアントは、ログインページから別の認証プロセスを実行せずにスリープおよび復帰することを許可されています。再認証が必要になるまでスリープ状態にあるクライアントが記録される期間を設定できます。有効な範囲は 1 時間から 720 時間（30 日）で、デフォルトは 12 時間です。これがセッション タイムアウトと同じになるのが理想的です。

e) [Over-ride Global Config] の [Enable] チェックボックスをオンにします。

（注） [Override global config] を有効にすると、顧客を外部 URL である Cisco DNA Spaces URL にリダイレクトできます。

f) [Web Auth Type] ドロップダウンリストから [External (Redirect to External Server)] を選択します。

（注） Cisco DNA Spaces ページはコントローラではなく外部サーバーでホストされるため、[Web Auth Type] は [External] である必要があります。

g) 表示される [URL] フィールドに、Cisco DNA Spaces のスプラッシュ URL を入力します。

CUWN または AireOS アカウントのスプラッシュ URL を表示するには、Cisco DNA Spaces ダッシュボードの [SSIDs] ウィンドウで AireOS SSID の [Configure Manually] リンクをクリックします。[Configure Manually] リンクは、Cisco AireOS SSID を追加した後にのみ表示されます。

（注） オンボーディング中に顧客が Cisco DNA Spaces Web ページにリダイレクトされるようにスプラッシュページを設定する必要があります。

h) [Apply] をクリックします。

ステップ 9 [Advanced] タブをクリックします。

ステップ 10 [Enable Session Timeout] フィールドに、必要なセッションタイムアウト値を秒単位で入力します。たとえば、セッションタイムアウトが 30 分の場合は、1800 と入力します。

ステップ 11 [Apply] をクリックします。

ステップ 12 [General] タブで、[Status] および [Broadcast SSID] オプションの [Enabled] チェックボックスをオンにして、SSID を有効にします。

ステップ 13 コマンドプロンプトで次のコマンドを実行して、キャプティブバイパスを無効にします。次に、ワイヤレスコントローラを再起動します。

config network web-auth captive-bypass disable Management > HTTP-HTTPS

（注） キャプティブバイパスが有効になっている場合、CNA は iOS デバイスに対してポップアップしません。

ステップ 14 表示される [HTTP-HTTPS configuration] ウィンドウで、次を実行します。

a) [HTTP Access] ドロップダウンリストから、[Disabled] を選択します。
b) [HTTPS Access] ドロップダウンリストから、[Enabled] を選択します。
c) [WebAuth SecureWeb] ドロップダウンリストから、[Disabled] を選択します。
d) [Apply] をクリックします。

ステップ 15 **[Security]** > **[Web Auth]** > **[Web Login Page]** の順に選択し、[Redirect URL after login] フィールドが空白であることを確認します。

（注） リダイレクト URL フィールドは、[Layer 3] で設定された Cisco DNA Spaces のスプラッシュ URL を上書きしないように空白にする必要があります。

次のタスク

（注） [Management] タブに変更を加えた場合は、変更を反映するためにシスコ ワイヤレス コントローラを再起動します。

アクセス コントロール リストを作成する

顧客のインターネットアクセスを制限し、SSID に接続したときに Cisco DNA Spaces スプラッシュページ URL へのアクセスのみを許可するには、ACL で Cisco DNA Spaces の IP（ウォールガーデン範囲）を設定する必要があります。これで、顧客が SSID に接続すると、スプラッシュページが顧客に表示されます。

ACL で一部の必要な IP が設定されていない場合、Cisco DNA Spaces が外部 URL と見なされ、顧客に対して複数回のリダイレクトが発生します。

アクセス コントロール リストを作成するには、次の手順を行います。

ステップ 1 シスコ ワイヤレス コントローラのログイン情報を使用して、ワイヤレスコントローラにログインします。

ステップ 2 **[Security]** > **[Access Control Lists]** > **[Access Control Lists]** を選択します。

ステップ 3 ACL を追加するには、[New] をクリックします。

ステップ 4 表示される [New] ウィンドウに、次のように入力します。

a) [Access Control List Name] フィールドに新しい ACL の名前を入力します。

（注） 最大 32 文字の英数字を入力できます。

b) ACL タイプとして [IPv4] を選択します。
c) [Apply] をクリックします。

ステップ 5 [Access Control Lists] ウィンドウが再度表示されたら、新しい ACL の名前をクリックします。

ステップ 6 表示される [Edit] ウィンドウで、[Add New Rule] をクリックします。

[Rules] > **[New]** ウィンドウが表示されます。

ステップ 7 必要なウォールガーデンの範囲にこの ACL のルールを設定します。

ウォールガーデンの範囲を表示するには、[Cisco DNA Spaces] ダッシュボードの [SSIDs] ウィンドウで、Cisco Unified Wireless Network SSID の [Configure Manually] リンクをクリックします。ウォールガーデンの範囲は、キャプション [Creating the Access Control List] の下に一覧表示されています。[Configure Manually] リンクは、Cisco AireOS SSID を追加した後にのみ表示されます。

ACL ルールを定義するときには、次のように値を設定します。

- **Direction**：Any
- **Protocol**：Any
- **Source Port Range**：0-65535
- **Destination Port Range**：0-65535
- **DSCP**：Any
- **Action**：Permit

ステップ 8 ポータルにソーシャル認証を装備する場合は、ソーシャル認証用にウォールガーデン範囲も構成する必要があります。

（注） ソーシャル認証用に設定されたこのウォールガーデン範囲により、顧客は SSID に接続した後、キャプティブポータルを使用せずに、すべての HTTPS Web サイトに直接アクセスできます。

仮想インターフェイスの設定

仮想インターフェイスを設定するには、次の手順を実行します。

ステップ 1 **[Controller]** > **[Interfaces]** を選択します。

ステップ 2 [Virtual] リンクをクリックします。

ステップ 3 表示される **[Interfaces]** > **[Edit]** ページで、次のパラメータを入力します。

a) [IP address] フィールドに、未割り当ておよび未使用のゲートウェイ IP アドレス（存在する場合）を入力します。
b) [DNS Host Name] フィールドに、DNS ホスト名（存在する場合）を入力します。

（注） 理想的には、このフィールドは空白になります。

（注） 接続して Web 認証を確立するには、DNS サーバは常に仮想インターフェイスをポイントしている必要があります。仮想インターフェイスに DNS ホスト名が設定されている場合は、クライアントが使用する DNS サーバ上で同じ DNS ホスト名が設定されている必要があります。

c) [Apply] をクリックします。

（注） 仮想インターフェイスに変更を加えた場合は、変更を反映するためにシスコ ワイヤレス コントローラを再起動します。

Cisco DNA Spaces を使用するための FlexConnect モードの設定

中央スイッチまたはローカル スイッチのモードに FlexConnect を設定できます。

FlexConnect 中央スイッチ モード

FlexConnect 中央スイッチモードで Cisco DNA Spaces を使用するようにシスコ ワイヤレス コントローラを設定するには、次の手順を実行します。

アクセス ポイントの *FlexConnect* モードを設定する

この設定は、FlexConnect の中央スイッチおよびローカルスイッチモードに適用されます。アクセスポイントに FlexConnect 中央スイッチモードを設定するには、次の手順を実行します。

ステップ 1 シスコ ワイヤレス コントローラのメインウィンドウで、[Wireless] タブをクリックします。

すべてのアクセス ポイントが一覧表示されます。

（注） アクセスポイントの詳細については、シスコ ワイヤレス コントローラのユーザーガイドを参照してください。

ステップ 2 モードを FlexConnect に設定するアクセス ポイントをクリックします。

ステップ 3 [General] タブをクリックします。

ステップ 4 [AP Mode] ドロップダウンリストから [FlexConnect] を選択します。

ステップ 5 [Apply] をクリックして変更を適用し、アクセス ポイントをリブートします。

シスコ ワイヤレス コントローラでの *FlexConnect* 中央スイッチモード用の *SSID* の作成

ローカルモードの場合と同じ手順で SSID を作成します。詳細については、シスコ ワイヤレス コントローラでの SSID の作成 （6 ページ）を参照してください。

FlexConnect 中央スイッチ モードのアクセス制御リストの作成

ローカル モードの場合と同じ手順を使用して、アクセス コントロール リストを作成します。詳細については、アクセス コントロール リストを作成する （8 ページ）を参照してください。

仮想インターフェイスの設定

仮想インターフェイスを設定するには、次の手順を実行します。

ステップ 1 **[Controller]** > **[Interfaces]** を選択します。

ステップ 2 [Virtual] リンクをクリックします。

ステップ 3 表示される **[Interfaces]** > **[Edit]** ページで、次のパラメータを入力します。

a) [IP address] フィールドに、未割り当ておよび未使用のゲートウェイ IP アドレス（存在する場合）を入力します。

b) [DNS Host Name] フィールドに、DNS ホスト名（存在する場合）を入力します。

（注） 理想的には、このフィールドは空白になります。

（注） 接続して Web 認証を確立するには、DNS サーバは常に仮想インターフェイスをポイントしている必要があります。仮想インターフェイスに DNS ホスト名が設定されている場合は、クライアントが使用する DNS サーバ上で同じ DNS ホスト名が設定されている必要があります。

c) [Apply] をクリックします。

（注） 仮想インターフェイスに変更を加えた場合は、変更を反映するためにシスコ ワイヤレス コントローラを再起動します。

FlexConnect ローカル スイッチ モード

FlexConnect ローカルスイッチモードで Cisco DNA Spaces を使用するようにシスコ ワイヤレス コントローラ を設定するには、次の手順を実行します。

• アクセス ポイントの FlexConnect モードを設定する （10 ページ）

アクセス ポイントの *FlexConnect* モードを設定する

この設定は、FlexConnect の中央スイッチおよびローカルスイッチモードに適用されます。アクセスポイントに FlexConnect 中央スイッチモードを設定するには、次の手順を実行します。

ステップ 1 シスコ ワイヤレス コントローラのメインウィンドウで、[Wireless] タブをクリックします。

すべてのアクセス ポイントが一覧表示されます。

（注） アクセスポイントの詳細については、シスコ ワイヤレス コントローラのユーザーガイドを参照してください。

ステップ 2 モードを FlexConnect に設定するアクセス ポイントをクリックします。

ステップ 3 [General] タブをクリックします。

ステップ 4 [AP Mode] ドロップダウンリストから [FlexConnect] を選択します。

ステップ 5 [Apply] をクリックして変更を適用し、アクセス ポイントをリブートします。

シスコ ワイヤレス コントローラでの *FlexConnect* ローカルスイッチモード用 *SSID* の作成

（注） SSID は、Cisco CMX ではなく、シスコ ワイヤレス コントローラで作成されます。

FlexConnect のローカル スイッチ モードの CUWN で SSID を作成するには、次の手順を実行します。

ステップ 1 シスコ ワイヤレス コントローラのメインウィンドウで、[WLANs] タブをクリックします。

ステップ 2 WLAN を作成するには、ウィンドウの右側にあるドロップダウンリストで [Create New] を選択し、[Go] をクリックします。

ステップ 3 表示される [New] ウィンドウで、[Type]、[Profile Name]、[SSID] などの WLAN の詳細を入力します。

ステップ 4 [Apply] をクリックします。

[Edit <SSID Name>] ウィンドウが表示されます。

ステップ 5 SSID を Cisco DNA Spaces ダッシュボードに追加します。

ステップ 6 シスコ ワイヤレス コントローラ メインウィンドウの [General] タブで、[Broadcast SSID] チェックボックスをオフにします。

（注） SSID ブロードキャストが中断され、設定を完了する前に顧客が SSID にアクセスすることが回避されます。

ステップ 7 **[Security]** > **[Layer 2]** を選択して、[MAC Filtering] チェックボックスをオンにします。

ステップ 8 [Layer 3] タブで、次を設定します。

a) [Layer 3 security] ドロップダウン リストから、[Web Policy] を選択します。

（注） [Web Policy] は、シスコ ワイヤレス コントローラでキャプティブポータルを設定できるようにする [Layer 3] のセキュリティオプションです。

b) [On Mac Filter Failure] ラジオボタンを選択します。

c) [Preauthentication ACL] 領域で、[WebAuth FlexACL] ドロップダウンリストから、事前に定義されている ACL を選択します。

d) スリープ状態のクライアントの [Enable] チェックボックスをオンにします。

（注） スリープ状態のクライアントを有効にすることは必須ではありません。ただし有効にすると、認証後にスリープモードになっている顧客が指定された時間内にスリープ状態から復帰した場合、認証なしで接続されます。Web 認証に成功したゲストアクセスを持つクライアントは、ログインウィンドウから別の認証プロセスを実行せずにスリープおよび復帰することを許可されています。再認証が必要になるまでスリープ状態にあるクライアントが記録される期間を設定できます。有効な範囲は 1 時間から 720 時間（30 日）で、デフォルトは 12 時間です。これがセッション タイムアウトと同じになるのが理想的です。

e) [Over-ride Global Config] の [Enable] チェックボックスをオンにします。

（注） [Override Global Config] を有効にすると、顧客を外部 URL である Cisco DNA Spaces URL にリダイレクトできます。

f) [Web Auth Type] ドロップダウンリストから、[External] を選択します。

（注） Cisco DNA Spaces ページはコントローラではなく外部サーバーでホストされるため、[Web Auth Type] は [External] である必要があります。

g) 表示される [URL] フィールドに、Cisco DNA Spaces のスプラッシュ URL を入力します。

CUWN アカウントのスプラッシュ URL を表示するには、Cisco DNA Spaces ダッシュボードの [SSIDs] ウィンドウで CUWN SSID の [Configure Manually] リンクをクリックします。[Configure Manually] リンクは、Cisco AireOS SSID を追加した後にのみ表示されます。

（注） オンボーディング中に顧客が Cisco DNA Spaces Web ページにリダイレクトされるようにスプラッシュページを設定する必要があります。

h) [Apply] をクリックします。

ステップ 9 [Advanced] タブをクリックします。

ステップ 10 [Enable Session Timeout] フィールドに、必要なセッションタイムアウト値を秒単位で入力します。たとえば、セッションタイムアウトが 30 分の場合は、1800 と入力します。

ステップ 11 [FlexConnect] 領域で、FlexConnect ローカルスイッチングの [Enabled] チェックボックスをオンにして、[Apply] をクリックします。

ステップ 12 [General] タブで、[Status] および [Broadcast SSID] オプションの [Enabled] チェックボックスをオンにして、SSID を有効にします。

ステップ 13 コマンドプロンプトで次のコマンドを実行して、キャプティブバイパスを無効にします。次に、ワイヤレスコントローラを再起動します。

config network web-auth captive-bypass disable

（注） キャプティブバイパスが有効になっている場合、CNA は iOS デバイスに対してポップアップしません。

ステップ 14 **[Management]** > **[HTTP-HTTPS]** を選択します。

ステップ 15 表示される [HTTP-HTTPS Configuration] ウィンドウで、次を実行します。

a) [HTTP Access] ドロップダウンリストから、[Disabled] を選択します。
b) [HTTPS Access] ドロップダウンリストから、[Enabled] を選択します。
c) [WebAuth SecureWeb] ドロップダウンリストから、[Disabled] を選択します。
d) [Apply] をクリックします。

ステップ 16 **[Security]** > **[Web Auth]** > **[Web Login Page]** の順に選択し、[Redirect URL after login] フィールドが空白であることを確認します。

（注） リダイレクト URL フィールドは、[Layer 3] で設定された Cisco DNA Spaces のスプラッシュ URL を上書きしないように空白にする必要があります。

FlexConnect ローカルスイッチモードのアクセス制御リストの作成

顧客のインターネットアクセスを制限し、SSID に接続したときに Cisco DNA Spaces スプラッシュページ URL へのアクセスのみを許可するには、ACL で Cisco DNA Spaces の IP（ウォールガーデン範囲）を設定する必要があります。これで、顧客が SSID に接続すると、スプラッシュページが顧客に表示されます。

ACL で一部の必要な IP が設定されていない場合、Cisco DNA Spaces が外部 URL と見なされ、顧客に対して複数回のリダイレクトが発生します。

FlexConnect のローカル スイッチ モードでのアクセス コントロール リストを作成するには、次の手順を実行します。

ステップ 1 シスコ ワイヤレス コントローラのログイン情報を使用して、ワイヤレスコントローラにログインします。

ステップ 2 **[Security]** > **[Access Control Lists]** > **[FlexConnect ACLs]** の順に選択します。

ステップ 3 ACL を追加するには、[New] をクリックします。

ステップ 4 表示された [New] ウィンドウに、次のように入力します。

a) [Access Control List Name] フィールドに新しい ACL の名前を入力します。

（注） 最大 32 文字の英数字を入力できます。

b) [Apply] をクリックします。

ステップ 5 [Access Control Lists] ウィンドウが再度表示されたら、新しい ACL の名前をクリックします。

ステップ 6 表示される [Edit] ウィンドウで、[Add New Rule] をクリックします。

[Rules] > **[New]** ウィンドウが表示されます。

ステップ 7 必要なウォールガーデンの範囲にこの ACL のルールを設定します。

ウォールガーデンの範囲を表示するには、Cisco DNA Spaces ダッシュボードの [SSIDs] ウィンドウで CUWN SSID の [Configure Manually] リンクをクリックします。

ACL ルールを定義するときには、次のように値を設定します。

- **Direction**：Any
- **Protocol**：Any
- **Source Port Range**：0-65535
- **Destination Port Range**：0-65535
- **DSCP**：Any
- **Action**：Permit

ステップ 8 ポータルにソーシャル認証を装備する場合は、ソーシャル認証用にウォールガーデン範囲も構成する必要があります。ソーシャル認証用に設定する必要があるウォールガーデンの範囲については、「ソーシャル認証に向けたワイヤレスネットワークの設定」のセクションを参照してください。

（注） ソーシャル認証用に設定されたこのウォールガーデン範囲により、顧客は SSID に接続した後、キャプティブポータルを使用せずに、すべての HTTPS Web サイトに直接アクセスできます。

仮想インターフェイスの設定

仮想インターフェイスを設定するには、次の手順を実行します。

ステップ 1 **[Controller]** > **[Interfaces]** を選択します。

ステップ 2 [Virtual] リンクをクリックします。

ステップ 3 表示される **[Interfaces]** > **[Edit]** ページで、次のパラメータを入力します。

a) [IP address] フィールドに、未割り当ておよび未使用のゲートウェイ IP アドレス（存在する場合）を入力します。

b) [DNS Host Name] フィールドに、DNS ホスト名（存在する場合）を入力します。

（注） 理想的には、このフィールドは空白になります。

（注） 接続して Web 認証を確立するには、DNS サーバは常に仮想インターフェイスをポイントしている必要があります。仮想インターフェイスに DNS ホスト名が設定されている場合は、クライアントが使用する DNS サーバ上で同じ DNS ホスト名が設定されている必要があります。

c) [Apply] をクリックします。

（注） 仮想インターフェイスに変更を加えた場合は、変更を反映するためにシスコ ワイヤレス コントローラを再起動します。

インターネット プロビジョニングおよび RADIUS 認証のためのシスコ ワイヤレス コントローラの設定

キャプティブポータルには RADIUS 認証を使用することを強くお勧めします。

（注） Cisco DNA Spaces クラウド RADIUS サーバーは、Web RADIUS 認証用の PAP のみをサポートします。CHAP はサポートされていません。クライアント認証の失敗を回避するには、シスコ ワイヤレス コントローラで Web RADIUS 認証方式として PAP を設定する必要があります。

次の機能は、RADIUS 認証を設定した場合にのみ機能します。

- シームレスなインターネット プロビジョニング。
- 拡張されたセッション期間とインターネット帯域幅。
- インターネットの拒否

また、キャプティブポータルによる顧客オンボーディングには、インターネットプロビジョニング設定が必要です。

RADIUS認証とシームレスなインターネットプロビジョニングを設定するには、次の手順に従います。

ステップ 1 シスコ ワイヤレス コントローラのログイン情報を使用して、シスコ ワイヤレス コントローラにログインします。

ステップ 2 [Cisco Wireless Controller] のメインウィンドウで、 **Security** タブをクリックします。

ステップ 3 **[Radius]** > **[Authentication]** の順に選択します。

[Radius Authentication Servers] ウィンドウが表示されます。

ステップ 4 [Auth Called Station ID Type] ドロップダウンリストから、[AP MAC Address:SSID] を選択します。

ステップ 5 [MAC-Delimiter] ドロップダウンリストから、[Hyphen] を選択します。

ステップ 6 [New] をクリックします。

ステップ 7 表示された [New]] ウィンドウで、サーバーの IP アドレス、ポート番号、秘密鍵など、認証用の RADIUS サーバーの詳細を入力し、[Server Status] で [Enabled] を選択し、[Apply] をクリックします。

ポート番号：1812

（注） Cisco DNA Spaces RADIUS サーバーのみを設定できます。RADIUS サーバーの IP アドレスと秘密鍵を表示するには、Cisco DNA Spaces ダッシュボードで、[SSIDs] ウィンドウの CUWN SSID の [Configure Manually] リンクをクリックします。 [Configure Manually] リンクは、Cisco AireOS SSID を追加した後にのみ表示されます。プライマリとセカンダリの両方の Radius サーバー IP を設定します。Cisco DNA Spaces サポートチームに連絡することもできます。

ステップ 8 **[Radius]** > **[Accounting]** の順に選択します。

[Radius Accounting Servers] ウィンドウが表示されます。

ステップ 9 [Acct Called Station ID] タイプから、[AP MAC Address:SSID] を選択します。

ステップ 10 [MAC-Delimiter] ドロップダウンリストから、[Hyphen] を選択します。

ステップ 11 [New] をクリックします。

ステップ 12 表示された [New] ウィンドウで、サーバーの IP アドレス、ポート番号、秘密鍵など、アカウンティング用の RADIUS サーバーの詳細を入力し、[Server Status] で [Enabled] を選択し、[Apply] をクリックします。

Port Number: 1813

（注） Cisco DNA Spaces の Radius サーバーのみを設定できます。Cisco DNA Spaces の Radius サーバーのみを設定できます。RADIUS サーバーの IP アドレスと秘密鍵を表示するには、Cisco DNA Spaces ダッシュボードで、[SSIDs] ウィンドウの CUWN SSID の [Configure Manually] リンクをクリックします。

ステップ 13 シスコ ワイヤレス コントローラのメインウィンドウで、[WLANs] タブをクリックします。

ステップ 14 キャプティブポータルルールの SSID の [WLAN] をクリックします。

ステップ 15 [Security] を選択します。

ステップ 16 [Layer 2] タブで、[MAC Filtering] チェックボックスをオンにします。

ステップ 17 [Layer 3] タブで、次が設定されていることを確認します。

[Layer 3 security] ドロップダウンリストで、[Web Policy] が選択されていること、また [Mac Filter Failure] ラジオボタンが選択されていること。

（注） SSID を作成するときに、[Layer 3] でこれらの設定が実行されます。

ステップ 18 [AAA Servers] タブの、[Radius Servers] 領域で、次の手順を実行します。

a) [Authentication Servers] の [Enabled] チェックボックスをオンにします。

a) [Server 1] ドロップダウンリストで、先に定義した RADIUS サーバーを選択します。

ステップ 19 [web-auth user] 領域の認証の優先順位に、[Order Used for Authentication] ボックスで、[Radius] を順序の先頭に設定します。

（注） [Up] および [Down] ボタンを使用し、順序を並び替えます。

ステップ 20 [Advanced] タブをクリックし、[Allow AAA Override] の [Enabled] チェックボックスをオンにします。

ステップ 21 [Apply] をクリックします。

ステップ 22 [Cisco Wireless Controller] のメインウィンドウで、[Security] タブをクリックします。

ステップ 23 **[AAA]** > **[MAC Filtering]** の順に選択します。

ステップ 24 表示される [MAC Filtering] ウィンドウで、次の手順を実行します。

a) [RADIUS Compatibility Mode] ドロップダウンリストから、[Cisco ACS] を選択します。

b) [MAC-Delimiter] ドロップダウンリストから、[Hyphen] を選択します。

c) [Apply] をクリックします。

ステップ 25 ウォールガーデンが ACL に応じて設定されていることを確認します。ウォールガーデンの範囲を表示するには、Cisco DNA Spaces ダッシュボードで、[SSID] ウィンドウの CUWN SSID の [Configure Manually] リンクをクリックします。[Configure Manually] リンクは、Cisco AireOS SSID を追加した後にのみ表示されます。

ソーシャル認証のためのシスコ ワイヤレス コントローラの設定

Cisco Unified Wireless Network へのソーシャル認証のためには、シスコ ワイヤレス コントローラに設定を行う必要があります。

ソーシャル認証のために Cisco Unified Wireless Network を設定するには、次の手順を実行します。

ステップ 1 ログイン情報を使用して、シスコ ワイヤレス コントローラにログインします。

ステップ 2 **[Security]** > **[Access Control Lists]** > **[Access Control Lists]** を選択します。

ステップ 3 表示される [Access Control List] ウィンドウで、Cisco DNA Spaces のために設定されたアクセス制御リストをクリックします。

[Add New Rule] をクリックし、次の情報を持つ 2 つの追加ルールを追加します。.

いいえ	アクション	送信元IPアドレス/ネットマスク	宛先 IP アドレス/ネットマスク	プロトコル	送信元ポート範囲	宛先ポート範囲	DSCP	方向
1	Permit	0.0.0.0/0.0.0.0	0.0.0.0/0.0.0.0	TCP	HTTPS	いずれか（Any）	いずれか（Any）	いずれか（Any）
2	Permit	0.0.0.0/0.0.0.0	0.0.0.0/0.0.0.0	TCP	いずれか（Any）	HTTPS	いずれか（Any）	いずれか（Any）

（注） ソーシャル認証用に設定構成されたこのウォールガーデン範囲により、顧客は SSID に接続した後、キャプティブポータルを使用せずに、すべての HTTPS Web サイトに直接アクセスできます。

ステップ 4 認証に使用するソーシャルネットワークに基づき、ソーシャルプラットフォーム固有のドメインを ACL として追加します。ソーシャルドメインを ACL として追加するには、次の手順を実行します。

a) シスコ ワイヤレス コントローラ ダッシュボードで、**[Security]** > **[Access Control Lists]** を選択します。
b) Cisco DNA Spaces 用に設定されたアクセス制御リストの [More Actions] をクリックします。
c) [Add Remove URL] をクリックします。
d) ソーシャル URL 名を入力し、[Add] をクリックします。
e) ドメインごとに、手順 **c** と **d** を繰り返します。

（注） これらのドメイン名はソーシャルネットワークによって管理され、いつでも変更できます。また、これらのドメイン名は、国/地域によって変更される可能性があります。問題が発生した場合は、Cisco DNA Spaces サポートチームにお問い合わせください。

さまざまなソーシャルプラットフォームで一般的に使用されるドメイン名は次のとおりです。

表 2:

ソーシャルドメイン
Facebook
facebook.com
static.xx.fbcdn.net
www.gstatic.com
m.facebook.com
fbcdn.net
fbsbx.com
LinkedIn
www.linkedin.com
static-exp1.licdn.com
Twitter

ソーシャルドメイン
abs.twimg.com
syndication.twitter.com
twitter.com
analytics.twitter.com
Instagram
instagram.com
*.instagram.com
api.instagram.com
d36xtkk24g8jdx.cloudfront.net
www.facebook.com
connect.facebook.net
*.akamaihd.net

WLC 直接接続または Cisco DNA Spaces コネクタを使用した、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラまたはシスコ ワイヤレス コントローラの Cisco DNA Spaces への接続

Cisco 9800 シリーズ ワイヤレス コントローラまたはシスコ ワイヤレス コントローラ（CMX なし）から Cisco DNA スペースにロケーションをインポートするには、最初にいずれかのコネクタを介してコントローラを Cisco DNA Spaces に接続する必要があります。

[Cisco WLC Direct Connect] と [Cisco DNA Spaces Connector] の両コネクタは、シスコ ワイヤレス コントローラと Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの両方に使用できます。

（注）

- シスコ ワイヤレス コントローラを Cisco CMX と Cisco DNA Spaces の両方に同時に接続する場合は、Cisco DNA Spaces コネクタを使用する必要があります。ただし、1 つのコントローラを Cisco DNA Spaces と Cisco CMX の両方に同時に接続することは推奨しません。
- 行動メトリクスなどの Cisco DNA Spaces レポートに表示されるデータを、シスコ ワイヤレス コントローラまたは Cisco CMX に表示されるデータと比較しないようにお勧めします。設計によって表示されるデータが異なることが予想されるためです。
- コントローラを Cisco DNA Spaces にインポートするには、少なくとも 1 つの AP がその特定のコントローラに接続されていることを確認してください。
- コントローラで、新しい AP がコントローラに追加されると、追加された AP は次のコントローラ同期の際に自動的にインポートされます。インポートされた AP がコントローラから削除された場合、この変更は 48 時間経過しないと Cisco DNA Spaces に反映されません。ただし、更新されない AP は、更新が他の AP から送信されている場合にのみ 48 時間後に削除されます。たとえば、10 の AP が設定されていて、2 つの AP がコントローラから削除された場合、削除された 2 つの AP は、他の 8 つの AP から更新が受信された場合にのみ Cisco DNA Spaces から削除されます。
- AP がコントローラとの関連付けを解除された場合、Cisco DNA Spaces からすぐに削除されて AP 数に反映されることありません。その AP は、48 時間経過しないと Cisco DNA Spaces から削除されません。

ワイヤレスコントローラとコネクタのさまざまな組み合わせに必要な設定は次のとおりです。

Cisco WLC Direct Connect を使用した Cisco DNA Spaces のシスコ ワイヤレス コントローラへの接続

シスコ ワイヤレス コントローラ バージョン 8.3 以降（Cisco CMX のインストールなし）を Cisco DNA Spaces に接続し、シスコ ワイヤレス コントローラとそのアクセスポイントを Cisco DNA Spaces にインポートするには、次の手順を実行します。

始める前に

- シスコ ワイヤレス コントローラ バージョン 8.3 以降が必要です。
- シスコ ワイヤレス コントローラを Cisco DNA Spaces にインポートするには、少なくとも 1 つの AP がその特定のシスコ ワイヤレス コントローラに接続されていることを確認してください。
- シスコ ワイヤレス コントローラは、HTTPS 経由で Cisco DNA Spaces クラウドに到達できる必要があります。
- シスコ ワイヤレス コントローラはインターネットに接続できる必要があります。

- Cisco DNA Spaces をアンカーモードで使用するには、アンカーコントローラモードと外部コントローラモードの両方でシスコ ワイヤレス コントローラをネットワーク展開する必要があります。ネットワーク展開にアンカーコントローラモードと外部コントローラモードのシスコ ワイヤレス コントローラが含まれている場合、このセクションで説明するコマンドを使用して、両方のコントローラで Cisco WLC Direct Connect を有効にする必要があります。さらに、どちらのモードのシスコ ワイヤレス コントローラも、HTTPS 経由で Cisco DNA Spaces クラウドに到達できる必要があります。ただし、Cisco DNA Spaces は、アンカーモードのシスコ ワイヤレス コントローラ バージョン 8.3.102 をサポートしていません。
- Cisco WLC Direct Connect を使用して Cisco AirOS ワイヤレス コントローラ バージョン 8.3 以降を Cisco DNA Spaces に正常に接続するには、DigiCert CA が発行するルート証明書が必要です。ネットワーク展開にアンカーコントローラモードと外部コントローラモードのシスコ ワイヤレス コントローラが含まれている場合、両方のモードのシスコ ワイヤレス コントローラに証明書をインポートする必要があります。

ステップ 1 DigiCert CA ルート証明書をインポートします。

a) 次のリンクからルート証明書をダウンロードします。
'

https://global-root-ca.chain-demos.digicert.com/info/index.html

b) ルート証明書の内容を .cer 拡張子のファイルにコピーし、ファイルを {your_filename}.cer として保存します。

c) **{your_filename}.cer** ファイルを TFTP サーバー上のデフォルトディレクトリにコピーします。

d) シスコ ワイヤレス コントローラの CLI にログインし、次のコマンドを実行します。

```
transfer download datatype cmx-serv-ca-cert
transfer download mode tftp
transfer download filename {your_filename}.cer
transfer download serverip {your_tftp_server_ip}
transfer download start
```

e) **Y** を入力してアップロードを開始します。

f) 新しいルート証明書が正常にアップロードされたら、次のコマンドを実行して Cisco CMX クラウドサービスを無効にし、その後で有効にします。

```
config cloud-services cmx disable
config cloud-services cmx enable
```

（注） ルート証明書をアップロードした後、シスコ ワイヤレス コントローラの再起動が求められます。再起動をお勧めしますが、必須ではありません。いずれの場合も証明書がインストールされます。

DigiCert CA が発行したものではないルート証明書を使用してワイヤレスコントローラを Cisco DNA Spaces に接続しようとすると、次のエラーが発生します。

```
https:SSL certificate problem: unable to get local issuer certificate
```

ステップ 2 シスコ ワイヤレス コントローラの CLI モードで、次のコマンドを実行します。

```
config cloud-services cmx disable
 config cloud-services server url https://{Customer Path Key}.{LB Domain} {LB IP Address}
config cloud-services server id-token <Customer JWT Token>
 config network dns serverip <dns server ip>
 config cloud-services cmx enable
```

（注） {Customer Path Key}、{LB Domain}、{LB IP Address}、および {Customer JWT Token} を表示するには、Cisco DNA Spaces ダッシュボードにログインし、ダッシュボードの左上に表示される 3 本線のメニューアイコンをクリックします。[Setup] > [Wireless Networks] の順に選択します。次に、[Connect WLC / Catalyst 9800 Directly] を展開し、[View Token] をクリックします。[WLC] タブをクリックすると、ステップ 1b で {Customer Path Key}、{LB Domain}、および {LB IP Address} を、ステップ 1c で {Customer JWT Token} を表示できます。

ステップ 3 次のコマンドを使用して、概要を確認します。

```
show cloud-services cmx summary
```

結果が表示されます。

Cisco DNA Spaces ダッシュボードで、[Add a Wireless Network] ウィンドウの [CUWN-WLC] を選択すると、WLC が一覧表示されます。これにより、その WLC の AP を Cisco DNA Spaces にインポートできます。

例：

結果サンプル

(Cisco Controller) >show cloud-services cmx summary

CMX Service

Server ..... https://$customerpathkey.dnaspaces.io

IP Address..... <Local System IP Address>

Connectivity..... https: UP

Service Status ..... アクティブ

Last Request Status..... HTTP/1.1 200 OK

Heartbeat Status ..... OK

これで、シスコ ワイヤレス コントローラを Cisco DNA Spaces ロケーション階層にインポートできるようになりました。マップサービスまたはアクセス ポイント プレフィックスを使用してロケーションをインポートできます。

- アクセスポイントのプレフィックスに基づいてロケーションをインポートするには、アクセス ポイント プレフィックスを使用したロケーションのインポートを参照してください。
- マップサービスを使用してロケーションをインポートするには、マップサービスを使用したロケーションのロケーション階層へのインポートを参照してください。

次のタスク

ソーシャル認証、RADIUS認証、およびインターネットプロビジョニングについては、次のセクションを参照してください。

- インターネットプロビジョニングおよびRADIUS認証のためのシスコ ワイヤレス コントローラの設定
- インターネットプロビジョニングおよびRADIUS認証のためのシスコ ワイヤレス コントローラの設定

通知およびレポート用のシスコ ワイヤレス コントローラ（Cisco CMX なし）の設定

Cisco CMX を使用しない場合、WLC Direct Connectおよび Cisco DNA Spaces コネクタといったコネクタを使用して、シスコ ワイヤレス コントローラを Cisco DNA Spaces に接続できます。このような場合、通知とレポートに必要な設定は、シスコ ワイヤレス コントローラをインポートするときに自動的に行われます。

（注） Cisco DNA Spaces で WLC Direct Connect または Cisco DNA Spaces コネクタを使用している場合、コントローラは「フォーリンコントローラ」モードである必要があります。

Cisco WLC Direct Connect を使用した Cisco DNA Spaces の Cisco Catalyst 9800 シリーズ ワイヤレス コントローラへの接続

始める前に

- Cisco Catalyst 9800 シリーズ ワイヤレス コントローラを Cisco DNA Spaces にインポートする場合、少なくとも 1 つの AP がその特定の Cisco Catalyst 9800 シリーズ ワイヤレス コントローラに接続されていることを確認してください。
- Cisco Catalyst 9800 シリーズ ワイヤレス コントローラは、HTTPS 経由で Cisco DNA Spaces クラウドに到達できる必要があります。
- Cisco Catalyst 9800 シリーズ ワイヤレス コントローラは、インターネットに接続できる必要があります。
- Cisco WLC Direct Connect を使用して Cisco Catalyst 9800 シリーズ ワイヤレス コントローラを Cisco DNA Spaces に正常に接続するには、シスコが信頼するルート証明書が必要です。

Cisco Catalyst 9800 シリーズ コントローラを Cisco DNA Spaces に接続し、そのコントローラとそのアクセスポイントを Cisco DNA Spaces にインポートするには、次の手順を実行します。

ステップ 1 シスコ社外の信頼できるルートストアをインポートして、コントローラに DigiCert グローバルルート CA をインストールします。

a) 次のコマンドを使用してルート証明書をダウンロードします。

```
(config)#crypto pki trustpool import url http://www.cisco.com/security/pki/trs/ios.p7b
```

b) 次のコマンドを使用して証明書のインストールを検証します。

```
#show crypto pki trustpool | section DigiCert Global Root CA
cn=DigiCert Global Root CA
cn=DigiCert Global Root CA
```

（注） 出力をチェックして、トラストプールが正しくインストールされていることを確認する必要があります。

ステップ 2 Cisco Catalyst 9800 シリーズ コントローラで、次のコマンドを使用して、DNS が Cisco DNA Spaces URL を解決できるようにします。

```
a. (config)#ip name-server <Primary IP> <Secondary IP>
b. (config)#ip domain lookup
c. (config)#ip route 0.0.0.0 0.0.0.0 <default_gw_ip_addr>
```

ステップ 3 HTTPS 経由で Cisco DNA Spaces Cloud と通信するため、Cisco Catalyst 9800 シリーズ コントローラで nmsp cloud-services を有効にします。

```
a. (config)#nmsp cloud-services server url <URL>
b. (config)#nmsp cloud-services server token <Customer JWT TOKEN>
c. (config)#nmsp cloud-services http-proxy <proxy ip_addr> <proxy port> -This command is optional,
 and must be used only if the proxy server needs to reach the internet.
d. (config)#nmsp cloud-services enable
```

（注） サーバーの URL とトークンを表示するには、Cisco DNA Spaces ダッシュボードにログインし、ダッシュボードの左上に表示される 3 本線のメニューアイコンをクリックします。[Setup] > [Wireless Networks] の順に選択します。次に、[Connect WLC / Catalyst 9800 Directly] を展開し、[View Token] をクリックします。[Cisco Catalyst 9800] タブをクリックすると、ステップ 2b で URL が表示され、ステップ 2c でトークンが表示されます。

ステップ 4 次のコマンドを実行して、Cisco Catalyst 9800 シリーズ コントローラと Cisco DNA Spaces Cloud 間の接続を確認します。

```
#show nmsp cloud-services summary
```

結果は次のようになります。

例：

結果サンプル

サーバー：https://abc.dnaspaces.io

CMX サービス：Enabled

接続：https: UP

サービスステータス：Active

最後の IP アドレス：<ローカルシステム IP アドレス>

最後のリクエストステータス：HTTP/1.1 200 OK

ハートビートステータス：OK

これで、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラを Cisco DNA Spaces のロケーション階層にインポートできるようになります。

ステップ 5 アクティブ/非アクティブな Cisco CMX クラウド接続の概要を表示するには、次のコマンドを実行します。

```
#show nmsp status
```

（注） Cisco DNA Spaces Cloud 接続への接続状態を確認できます。

ステップ 6 すべてのアクティブな Cisco DNA Spaces クラウド接続の集約されたサブスクリプションの概要を表示するには、次のコマンドを実行します。

```
# show nmsp subscription summary
```

（注） 接続が確立されると、Cisco DNA Spaces Cloud が登録しているサービスを表示できます。

ステップ 7 ロケーションを Cisco DNA Spaces ダッシュボードにインポートします。ロケーションのインポートの詳細については、「Cisco Catalyst 9800 シリーズ ワイヤレス コントローラまたはシスコ ワイヤレス コントローラ（Cisco CMX なし）のロケーション階層の定義」を参照してください。

ステップ 8 **キャプティブポータル**および **Engagements** アプリを使用する場合は、以下のうち必要な設定を実行します。

CLI を使用したキャプティブポータルおよびエンゲージメントアプリ用の Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ（ローカルモード）の設定

（注） サポートされる Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの最小バージョンは、16.10.20181030 です。

キャプティブポータルおよびエンゲージメントアプリ用に Cisco Catalyst 9800 シリーズ ワイヤレス コントローラを設定するには、次の手順を実行します。

ステップ 1 Cisco DNA Spaces ダッシュボードで、Cisco Catalyst SSID を設定します。SSID の設定の詳細については、「Cisco Unified Wireless Network 用の SSID のインポート」セクションを参照してください。

（注） SSID には任意の名前を定義できます。Cisco Catalyst 9800 シリーズ ワイヤレス コントローラを設定したときと同じ SSID 名を使用する必要があります。

ステップ 2 Cisco Catalyst 9800 シリーズ ワイヤレス コントローラで、次のように HTTP と HTTPS を有効にします。

ip http server

ip http secure-server

ステップ 3 クライアントのリダイレクト用のパラメータマップを設定します。

parameter-map type webauth <map name>

type consent

timeout init-state sec 600

redirect for-login <splash page URL>

redirect append ap-mac tag ap_mac

redirect append wlan-ssid tag wlan

redirect append client-mac tag client_mac

redirect portal ipv4 <IP Address>

logout-window-disabled

success-window-disable

（注） スプラッシュ URL と IP アドレスについては、Cisco DNA Spaces ダッシュボードで、Captive Portal アプリをクリックします。[SSIDs] をクリックし、ステップ 1 で作成した Cisco Catalyst SSID の [Configure Manually] リンクをクリックします。CUWN アカウントのスプラッシュ URL は、[Creating the SSIDs in CUWN-WLC] セクションにリストされます。IP アドレスは、[Creating the Access Control List] セクションに一覧表示されます。リストにある IP アドレスのいずれか 1 つのみを使用する必要があります。Cisco DNA Spaces サポートチームに連絡することもできます。

ステップ 4 クライアントリダイレクト用の仮想 IP アドレスを設定します。

parameter-map type webauth global

virtual-ip ipv4 192.0.2.0

intercept-https-enable

（注）
- **ipV4** *192.0.2.0* の代わりに、任意の仮想 IP を構成できます。virtual-ip は、ルーティング不可能な未使用の IP アドレスである必要があります。
- Cisco Catalyst 9800 シリーズ ワイヤレス コントローラに仮想 IP/ドメインの有効な SSL 証明書をインストールする必要があります。

ステップ 5 FQDN URL フィルタリングを設定します。

中央スイッチの WLAN の場合、URL フィルタリストはポリシープロファイルに添付されます。

urlfilter list social_login_fqdn_central

action permit

url <splash page domain>

（注） 手順 3 で設定したドメインを「redirect for-login」用に設定します。

url *.fbcdn.net

url *.licdn.com

url *.licdn.net
url *.twimg.com
url *.gstatic.com
url *.twitter.com
url *.akamaihd.net
url *.facebook.com
url *.facebook.net
url *.linkedin.com
url ssl.gstatic.com
url *.googleapis.com
url static.licdn.com
url *.accounts.google.com
url *.connect.facebook.net
url oauth.googleusercontent.com
wireless profile policy default-policy-profile
urlfilter list pre-auth-filter social_login_fqdn_central

フレックス WLAN の場合、URL フィルタリストはフレックスプロファイルに添付されます。

urlfilter list social_login_fqdn_flex
action permit
url <splash page domain>

（注） 手順 3 で設定したドメインを「redirect for-login」用に設定します。

url *.fbcdn.net
url *.licdn.com
url *.licdn.net
url *.twimg.com
url *.gstatic.com
url *.twitter.com
url *.akamaihd.net
url *.facebook.com
url *.facebook.net
url *.linkedin.com
url ssl.gstatic.com
url *.googleapis.com
url static.licdn.com

url *.accounts.google.com

url *.connect.facebook.net

url oauth.googleusercontent.com

urlfilter list social_login_fqdn_central

wireless profile flex default-flex-profile

acl-policy <WA-sec-<ip>>

urlfilter list social_login_fqdn_flex

description "default flex profile"

ステップ 6 RADIUS サーバーを設定します。

aaa new-model

aaa group server radius <group name>

server name <radius server name>

subscriber mac-filtering security-mode mac

mac-delimiter hyphen

aaa accounting login <authentication> group <group name>

aaa authorization network <Authorization> group <Group Name>

aaa accounting identity <Accounting> start-stop group <Group Name>

aaa server radius dynamic-author

client <Radius Server IP> server-key <Radius Secret>

aaa session-id common

radius-server attribute wireless accounting call-station-id ap-macaddress-ssid

radius server <Radius Name>

address ipv4 <Radius Server IP> auth-port 1812 acct-port 1813

key <Radius Secret>

（注） Cisco DNA Spaces の Radius サーバーのみを設定できます。Radius サーバー設定用の ipV4 IP アドレス、秘密鍵およびポートを表示するには、Cisco DNA Spaces ダッシュボードで、[Captive Portal] アプリをクリックします。[SSIDs] をクリックし、ステップ 1 で作成した Cisco Catalyst SSID の [Configure Manually] リンクをクリックします。Radius サーバーの詳細は、[Radius Server Configuration] セクションのリストに表示されます。プライマリとセカンダリの両方の Radius サーバー IP を設定します。Cisco DNA Spaces サポートチームに連絡することもできます。

ステップ 7 ポリシープロファイルを設定します。

wireless profile policy default-policy-profile

aaa-override

accounting-list <Accounting Server>

autoqos mode voice

description "default policy profile"

service-policy input platinum-up

service-policy output platinum

urlfilter list pre-auth-filter <url filter>

vlan <id>

no shutdown

ステップ 8 WLAN を設定します。

wlan <WLAN name >

ip access-group web <ACL Name>

no security wpa

no security wpa akm dot1x

no security wpa wpa2 ciphers aes

security web-auth

security web-auth authentication-list default

security web-auth parameter-map <map name>

no shutdown

（注） ここで指定する WLAN 名が、ステップ 1 で Cisco DNA Spaces で設定した SSID 名と一致することを確認してください。

ステップ 9 DNS 解決を有効にして、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラにデフォルトゲートウェイが設定されていることを確認します。

ip name-server <dns_ip_address>

ip domain-lookup

ip route 0.0.0.0 0.0.0.0 <default_gw_ip_addr>

その後、SSID を Cisco DNA Spaces にインポートし、キャプティブポータルルールを使用して SSID のキャプティブポータルを設定します。

キャプティブポータルおよびエンゲージメントアプリ用の Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ GUI（ローカルモード）

（注） サポートされる Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの最小バージョンは、16.10.1E および 16.10.11 です。

キャプティブポータルおよびエンゲージメントアプリ用に Cisco Catalyst 9800 シリーズ ワイヤレス コントローラを設定するには、次の手順を実行します。

ステップ 1 Cisco DNA Spaces ダッシュボードで、Cisco Catalyst SSID を設定します。SSID の設定の詳細については、「Cisco Unified Wireless Network 用の SSID のインポート」セクションを参照してください。

ステップ 2 パラメータマップを作成します。

a) Cisco Catalyst 9800 シリーズ ワイヤレス コントローラにログインします。
b) **[Configuration]** > **[Security]** > **[Web Auth]** の順に選択します。
c) [Web Auth Parameter Map] タブで、[Add] をクリックします。
d) [Parameter-map name] フィールドに、パラメータマップ名を入力します。
e) [Type] ドロップダウンリストから [Consent] を選択し、[Apply to Device] をクリックします。
新しく作成されたパラメータマップが [Web Auth Parameter Map] タブのリストに表示されます。
f) 新しく作成された [Parameter Map] をクリックします。
g) [General] タブで、[Disable Success Window] チェックボックスと [Disable Logout Window] チェックボックスをオンにします。
h) [Advanced] タブで、次の操作を実行します。

- [Redirect for log-in] フィールドに、スプラッシュページの URL（https://<domain>/p2/<customerPathKey>）を入力します。
- [Redirect Append for AP MAC Address] フィールドに、「ap_mac」を入力します。
- [Redirect Append for Client MAC Address] フィールドに、「client_mac」を入力します。
- [Redirect Append for WLAN SSID] フィールドに、wlan を入力します。
- [Portal IPV4 Address] フィールドに、許可される Cisco DNA Spaces IP を入力します。

（注） 許可される IP アドレスを表示するには、Cisco DNA Spaces ダッシュボードで、[Captive Portals] アプリをクリックします。[SSIDs] をクリックしてから、Cisco Catalyst SSID の [Configure Manually] リンクをクリックします。IP アドレスは、[Creating the Access Control List] セクションに一覧表示されます。リストにある IP アドレスのいずれか 1 つのみを使用する必要があります。残りの IP は、ACL の作成時に指定されます。[Configure Manually] リンクは、Cisco Catalyst SSID を追加するまで表示されません。

i) [Update and Apply] をクリックします。

ステップ 3 Web 認証証明書をインストールし、グローバルパラメータマップを設定します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラに仮想 IP/ドメインの有効な SSL 証明書をインストールする必要があります。任意のワイルドカード証明書を購入できます。

a) Cisco Catalyst 9800 シリーズ ワイヤレス コントローラにログインします。
b) Cisco Catalyst 9800 Series Wireless Controller ダッシュボードで、**[Configuration]** > **[Security]** > **[Web Auth]** を選択します。
c) パラメータマップ名 [global] をクリックします。
d) [Maximum Http connections] を [100] に設定します。
e) [Init-State Timeout(Secs)] を [120] に設定します。
f) [General] タブの [Type] ドロップダウンリストから、[Webauth] を選択します。

g) それぞれのフィールドで仮想IPv4アドレス（仮想IP）または仮想IPv4ホスト名（ドメイン）を指定します。

h) [Watch List Expiry Timeout(Secs)] を [600] に設定します。

i) [Web Auth intercept HTTPS] チェックボックスをオンにします。

j) [Update & Apply] をクリックします。

k) 証明書を pkcs12 に変換します。

ファイル形式は .p12 になります。

l) ファイルを TFTP サーバーにコピーします。

m) 次の手順を使用して、TFTP サーバーにコピーされた証明書をダウンロードします。

- Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの CLI で、次のコマンドを入力します。

```
crypto pki import <name> pkcs12 tftp://<tftp server ip>:/ password <certificate password>
```

- **tftp** サーバーの IP を確認するには、「**yes**」と入力します。
- 証明書ファイル名を入力します。たとえば「wildcard.wifi-mx.com.p12」のように入力します。

  証明書がダウンロードされます。

n) インストールされている証明書を確認するには、Cisco Catalyst 9800 Series Wireless Controller ダッシュボードで、**[Configuration]** > **[Web Auth]** > **[Certificate]** を選択します。

ダウンロードされた証明書は、リスト末尾の証明書として表示されます。

o) インストールされた証明書をウェブ認証パラメータマップにマッピングするには、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの CLI で、次のコマンドを実行します。

- `Conf t`
- `parameter-map type webauth global`
- `trustpoint <installed trustpool name > ex: trustpool name`
- `end`
- `wr (to save the configuration)`

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラをリロードします。

ステップ 4 URL フィルタを追加して ACL を作成します。

a) **[Configuration]** > **[Security]** > **[URL Filter]** を選択します。

b) [URL Filters] ウィンドウで、[Add] をクリックします。

c) [List Name] フィールドに、リストの名前を入力します。

d) [Action] のステータスを [Permit] に変更します。

e) [URLs] フィールドに、ステップ 2h（パラメータマップ）で設定したスプラッシュページドメインを入力します。

ソーシャル認証を有効にする場合は、次のドメインを追加します。

- *.fbcdn.net
- *.licdn.com

- *.licdn.net
- *.twimg.com
- *.gstatic.com
- *.twitter.com
- *.akamaihd.net
- *.facebook.com
- *.facebook.net
- *.linkedin.com
- ssl.gstatic.com
- *.googleapis.com
- static.licdn.com
- *.accounts.google.com
- *.connect.facebook.net
- oauth.googleusercontent.com

f) **[Configuration]** > **[Tags and Profiles]** > **[Policy]** を選択します。
g) [Policy Profile] ウィンドウで、[default-policy-profile] をクリックします。
h) [Edit Policy Profile] ウィンドウで、[Access Policies] タブをクリックします。
i) [URL Filters] エリアの [Pre Auth] ドロップダウンリストから、以前に作成した ACL を選択します。
j) [Update & Apply to Device] をクリックします。

ステップ 5 SSID を作成します。

a) **[Configuration]** > **[Tags and Profiles]** > **[WLANs]** を選択します。
b) [Add] をクリックします。
a) [General] タブで、[Profile Name] フィールドにプロファイル名を入力します。
b) [SSID] フィールドに、ステップ 1 で定義した SSID 名を入力します。
c) ステータスを [Enabled] に設定します。
d) [Security] タブをクリックしてから、[Layer2] タブをクリックします。
e) [Layer 2 Security Mode] ドロップダウンリストから、[None] を選択します。
f) [Layer3] タブをクリックします。
g) [Web Policy] チェックボックスをオンにします。
h) [Web Auth Parameter Map] ドロップダウンリストから、ステップ 2 で作成した Web 認証パラメータマップを選択します。
i) [Save & Apply to Device] をクリックします。

ステップ 6 RADIUS サーバを設定します。

（注） キャプティブポータルにはRADIUS認証を使用することを強く推奨します。次の機能は、RADIUS認証を設定した場合にのみ使用できます。

- シームレスなインターネット プロビジョニング
- セッション持続時間の延長
- インターネットの拒否

a) **[Configuration]** > **[Security]** > **[AAA]** の順に選択します。
b) [Authentication Authorization and Accounting] ウィンドウで、[Servers/Groups] タブをクリックします。
c) **[Radius]** > **[Servers]** を選択して、[Add] をクリックします。
d) [Name] フィールドに、Radius サーバーの名前を入力します。
e) [IPv4/IPv6 Server Address] フィールドに、Radius サーバーのアドレスを入力します。

（注） Cisco DNA Spaces の Radius サーバーのみを設定できます。Radius サーバーの IP アドレスと秘密鍵を表示するには、Cisco DNA Spaces ダッシュボードで、[Captive Portal] アプリをクリックします。[SSIDs] をクリックしてから、ステップ 1 で作成した Cisco Catalyst SSID の [Configure Manually] リンクをクリックします。表示されるウィンドウで、Radius サーバーの詳細が [Radius Server Configuration] セクションのリストに表示されます。プライマリおよびセカンダリ Radius サーバの両方の IP を設定します。Cisco DNA Spaces サポート チームに連絡することもできます。

f) [Key] フィールドにキーを入力し、[Confirm Key] フィールドでキーを確認します。
g) [Auth Port] フィールドに「1812」と入力します。
h) [Acct Port] フィールドに「1813」と入力します。
i) [Save & Apply to Device] をクリックします。
追加されたサーバーは、[Servers] リストに表示されます。
j) **[Radius]** > **[Server Groups]** を選択して、[Add] をクリックします。
k) [Name] フィールドに、名前を入力します。
l) [MAC-Delimiter] ドロップダウンリストから、[hyphen] を選択します。
m) [MAC-Filtering] ドロップダウンリストから、[mac] を選択します。
n) 矢印ボタンを使用して、以前に作成した Radius サーバーを [Available Servers] から [Assigned Servers] に移動します。
o) [Save & Apply to Device] をクリックします。
p) [Authentication Authorization and Accounting] ウィンドウで、[AAA Method List] タブをクリックします。
q) [Authentication] をクリックし、[Add] をクリックして、次の詳細を指定します。

1. [Method List Name] フィールドに、メソッドリストの名前を入力します。
2. [Type] ドロップダウンリストから、[Login] を選択します。
3. [Group Type] ドロップダウンリストから、[Group] を選択します。
4. 以前に作成したサーバーグループ（ステップ j からステップ o）を [Available Server Groups] から [Assigned Servers Groups] に移動し、[Save & Apply to Device] をクリックします。

r) [AAA Method List] タブで、[Authorization] をクリックし、[Add] をクリックして、次の詳細を指定します。

1. [Method List Name] フィールドに、メソッドリストの名前を入力します。
2. [Type] ドロップダウンリストから、[Network] を選択します。
3. [Group Type] ドロップダウンリストから、[Group] を選択します。
4. 矢印ボタンを使用して、以前に作成したサーバーグループ（ステップ j からステップ o）を [Available Servers] から [Assigned Servers] に移動し、[Save & Apply to Device] をクリックします。

s) [AAA Method List] タブで、[Accounting] をクリックし、[Add] をクリックして、次の詳細を指定します。

1. [Method List Name] フィールドに、メソッドリストの名前を入力します。
2. [Type] ドロップダウンリストから、[Identity] を選択します。
3. [Group Type] ドロップダウンリストから、[Group] を選択します。
4. 矢印ボタンを使用して、以前に作成したサーバーグループ（ステップ j からステップ o）を [Available Servers] から [Assigned Servers] に移動し、[Save & Apply to Device] をクリックします。

ステップ 7 L3 および L2 認証（MAC フィルタリング）を有効にします。

Radius 認証のパラメータマップで、[Type] として [webauth] が選択されていることを確認します。

（注） L3 および L2 認証を設定するには、SSID を作成し、ステップ 5 のすべての設定を完了していることを確認してください。その後、SSID を Cisco DNA Spaces にインポートし、キャプティブポータルルールを使用して SSID のキャプティブポータルを設定します。

a) **[Configuration]** > **[Tags and Profiles]** > **[WLANs]** を選択します。
b) L2 および L3 認証を設定する SSID をクリックします。
c) [Edit WLAN] ウィンドウで [Security] タブをクリックします。
d) [Layer3] タブで、[Authentication] ドロップダウンリストから、以前に（ステップ 6q で）設定した Radius 認証を選択します。
e) [Layer2] タブで、[MAC Filtering] チェックボックスをオンにして、MAC フィルタリングを有効にします。
f) 表示される [Authorization List] ドロップダウンリストから、以前に（ステップ 6r で）作成した許可サーバーを選択します。
g) [Show Advanced Settings] をクリックします。
h) [On Mac Filter Failure] チェックボックスをオンにします。
i) [Update & Apply to Device] をクリックします。
j) **[Configuration]** > **[Tags and Profiles]** > **[Policy]** を選択します。
k) [default-policy-profile] をクリックします。
l) [Advanced] タブの [AAA Policy] エリアで、[Allow AAA Override] チェックボックスをオンにします。
m) [Policy Name] ドロップダウンリストから、デフォルトの [aaa] ポリシーが選択されていることを確認します。

n) [Update & Apply to Device] をクリックします。

キャプティブポータルおよびエンゲージメントアプリ用の Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ GUI（フレックスモードまたは Mobility Express）

（注） サポートされる Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの最小バージョンは、16.10.1E および 16.10.11 です。

キャプティブポータルおよびエンゲージメントアプリ用に「フレックスモードの Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ」または「Mobility Express を備えた Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ」を設定するには、次の手順を実行します。

ステップ 1 フレックスモードの Cisco Catalyst 9800 シリーズ ワイヤレス コントローラを設定するには、次の設定が完了していることを確認します。

この設定は、Mobility Express には必要ありません。

a) Cisco Catalyst 9800 シリーズ ワイヤレス コントローラにログインします。
b) **[Configuration]** > **[Tags]** > **[Site]** を選択します。
c) 必要なサイト名を選択します。
d) [Enabled Local Site] チェックボックスをオフにします。
e) [Update & Apply to Device] をクリックします。
f) **[Configuration]** > **[Policy]** を選択します。
g) 必要なポリシー名を選択します。
h) [Central Switching] を無効にします。
i) [Update & Apply to Device] をクリックします。

（注） [Local Mode] から [Flex Mode] に変更すると、AP が再起動してワイヤレスコントローラに再参加する場合があります。

ステップ 2 Cisco DNA Spaces ダッシュボードで、Cisco Catalyst SSID を設定します。SSID の設定の詳細については、「Cisco Unified Wireless Network 用の SSID のインポート」セクションを参照してください。

ステップ 3 パラメータマップを作成します。

a) Cisco Catalyst 9800 シリーズ ワイヤレス コントローラにログインします。
b) **[Configuration]** > **[Security]** > **[Web Auth]** の順に選択します。
c) [Web Auth Parameter Map] タブで、[Add] をクリックします。
d) [Parameter-map name] フィールドに、パラメータマップ名を入力します。
e) [Type] ドロップダウンリストから [Consent] を選択し、[Apply to Device] をクリックします。
新しく作成されたパラメータマップが [Web Auth Parameter Map] タブのリストに表示されます。
f) 新しく作成された [Parameter Map] をクリックします。

g) [General] タブで、[Disable Success Window] チェックボックスと [Disable Logout Window] チェックボックスをオンにします。

h) [Advanced] タブで、次の操作を実行します。

- [Redirect for log-in] フィールドに、スプラッシュページの URL（https://<domain>/p2/<customerPathKey>）を入力します。
- [Redirect Append for AP MAC Address] フィールドに、ap_mac を入力します。
- [Redirect Append for Client MAC Address] フィールドに、client_mac を入力します。
- [Redirect Append for WLAN SSID] フィールドに、wlan を入力します。
- [Portal IPV4 Address] フィールドに、許可される Cisco DNA Spaces IP を入力します。

（注） 許可される IP アドレスを表示するには、Cisco DNA Spaces ダッシュボードで、[Captive Portals] アプリをクリックします。[SSIDs] をクリックしてから、CUWN/Catalyst SSID の [Configure Manually] リンクをクリックします。IP アドレスは、[Creating the Access Control List] セクションに一覧表示されます。リストにある IP アドレスのいずれか 1 つのみを使用する必要があります。残りの IP は、ACL の作成時に指定されます。[Configure Manually] リンクは、Cisco Catalyst SSID を追加するまで表示されません。

i) [Update and Apply] をクリックします。

ステップ 4 Web 認証証明書をインストールし、グローバルパラメータマップを設定します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラに仮想 IP/ドメインの有効な SSL 証明書をインストールする必要があります。任意のワイルドカード証明書を購入できます。

a) Cisco Catalyst 9800 シリーズ ワイヤレス コントローラにログインします。

b) Cisco Catalyst 9800 Series Wireless Controller ダッシュボードで、**[Configuration]** > **[Security]** > **[Web Auth]** を選択します。

c) パラメータマップ名 [global] をクリックします。

d) [Maximum Http connections] を [100] に設定します。

e) [Init-State Timeout(Secs)] を [120] に設定します。

f) [General] タブの [Type] ドロップダウンリストから、[Webauth] を選択します。

g) それぞれのフィールドで仮想 IPv4 アドレス（仮想 IP）または仮想 IPv4 ホスト名（ドメイン）を指定します。

h) [Watch List Expiry Timeout(Secs)] を [600] に設定します。

i) [Web Auth intercept HTTPS] チェックボックスをオンにします。

j) [Update & Apply] をクリックします。

k) 証明書を pkcs12 に変換します。

ファイル形式は .p12 になります。

l) ファイルを TFTP サーバーにコピーします。

m) 次の手順を使用して、TFTP サーバーから証明書をダウンロードします。

- Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの CLI で、次のコマンドを入力します。

```
crypto pki import <name> pkcs12 tftp://<tftp server ip>:/ password <certificate password>
```

- **tftp** サーバーの IP を確認するには、「**yes**」と入力します。
- 証明書ファイル名を入力します。たとえば「wildcard.wifi-mx.com.p12」のように入力します。

  証明書がダウンロードされます。

n) インストールされている証明書を確認するには、Cisco Catalyst 9800 Series Wireless Controller ダッシュボードで、**[Configuration]** > **[Web Auth]** > **[Certificate]** を選択します。

ダウンロードされた証明書は、リスト末尾の証明書として表示されます。

o) インストールされた証明書をウェブ認証パラメータマップにマッピングするには、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの CLI で、次のコマンドを実行します。

- `Conf t`
- `parameter-map type webauth global`
- `trustpoint <installed trustpool name > ex: trustpool name`
- `end`
- `wr (to save the configuration)`

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラをリロードします。

ステップ 5 URL フィルタを追加して ACL を作成します。

a) **[Configuration]** > **[Security]** > **[URL Filter]** を選択します。
b) [URL Filters] ウィンドウで、[Add] をクリックします。
c) [List Name] フィールドに、リストの名前を入力します。
d) [Action] のステータスを [Permit] に変更します。
e) [URLs] フィールドに、ステップ 3h（パラメータマップ）で設定したスプラッシュページドメインを入力します。

ソーシャル認証を有効にする場合は、次のドメインを追加します。

- *.fbcdn.net
- *.licdn.com
- *.licdn.net
- *.twimg.com
- *.gstatic.com
- *.twitter.com
- *.akamaihd.net
- *.facebook.com
- *.facebook.net
- *.linkedin.com
- ssl.gstatic.com

- *.googleapis.com
- static.licdn.com
- *.accounts.google.com
- *.connect.facebook.net
- oauth.googleusercontent.com

f) **[Configuration]** > **[Tags and Profiles]** > **[Policy]** を選択します。
g) [Policy Profile] ウィンドウで、[default-policy-profile] をクリックします。
h) [Edit Policy Profile] ウィンドウで、[Access Policies] タブをクリックします。
i) [URL Filters] エリアの [Pre Auth] ドロップダウンリストから、以前に作成した ACL を選択します。
j) [Update & Apply to Device] をクリックします。
k) **[Configuration]** > **[Tags and Profiles]** > **[Flex]** を選択します。
l) 使用中のプロファイルをクリックします。
m) 表示される [Edit Flex Profile] ウィンドウで、[Policy ACL] タブをクリックします。
n) [Add] をクリックします。
o) [ACL Name] ドロップダウンリストから、[WA-sec-<ip>] を選択します。
p) [Pre Auth URL Filter] ドロップダウンリストから、以前に作成した URL フィルタ ACL を選択します（ステップ 5a から 5e）。
q) [Save] をクリックします。
r) [Update & Apply to Device] をクリックします。

ステップ 6 SSID を作成します。

a) **[Configuration]** > **[Tags and Profiles]** > **[WLANs]** を選択します。
b) [Add] をクリックします。
a) [General] タブで、[Profile Name] フィールドにプロファイル名を入力します。
b) [SSID] フィールドに、ステップ 2 で定義した SSID 名を入力します。
c) ステータスを [Enabled] に設定します。
d) [Security] タブをクリックしてから、[Layer2] タブをクリックします。
e) [Layer 2 Security Mode] ドロップダウンリストから、[None] を選択します。
f) [Layer3] タブをクリックします。
g) [Web Policy] チェックボックスをオンにします。
h) [Web Auth Parameter Map] ドロップダウンリストから、ステップ 3 で作成した Web 認証パラメータマップを選択します。
i) [Save & Apply to Device] をクリックします。

ステップ 7 RADIUS サーバを設定します。

（注） キャプティブポータルには Radius 認証を使用することを強く推奨します。次の機能は、Radius 認証を設定した場合にのみ使用できます。

- シームレスなインターネット プロビジョニング
- セッション持続時間の延長
- インターネットの拒否

a) **[Configuration]** > **[Security]** > **[AAA]** の順に選択します。
b) [Authentication Authorization and Accounting] ウィンドウで、[Servers/Groups] タブをクリックします。
c) **[Radius]** > **[Servers]** を選択して、[Add] をクリックします。
d) [Name] フィールドに、Radius サーバーの名前を入力します。
e) [IPv4/IPv6 Server Address] フィールドに、Radius サーバーのアドレスを入力します。

（注） Cisco DNA Spaces の Radius サーバーのみを設定できます。Radius サーバーの IP アドレスと秘密鍵を表示するには、Cisco DNA Spaces ダッシュボードで、[Captive Portal] アプリをクリックします。[SSIDs] をクリックし、ステップ 2 で作成した Cisco Catalyst SSID の [Configure Manually] リンクをクリックします。表示されるウィンドウで、Radius サーバーの詳細が [Radius Server Configuration] セクションのリストに表示されます。プライマリおよびセカンダリ Radius サーバの両方の IP を設定します。Cisco DNA Spaces サポート チームに連絡することもできます。

f) [Key] フィールドにキーを入力し、[Confirm Key] フィールドでキーを確認します。
g) [Auth Port] フィールドに「1812」と入力します。
h) [Acct Port] フィールドに「1813」と入力します。
i) [Save & Apply to Device] をクリックします。
追加されたサーバーは、[Servers] リストに表示されます。
j) **[Radius]** > **[Server Groups]** を選択して、[Add] をクリックします。
k) [Name] フィールドに、名前を入力します。
l) [MAC-Delimiter] ドロップダウンリストから、[hyphen] を選択します。
m) [MAC-Filtering] ドロップダウンリストから、[mac] を選択します。
n) 矢印ボタンを使用して、以前に作成した Radius サーバーを [Available Servers] から [Assigned Servers] に移動します。
o) [Save & Apply to Device] をクリックします。
p) [Authentication Authorization and Accounting] ウィンドウで、[AAA Method List] タブをクリックします。
q) [Authentication] をクリックし、[Add] をクリックして、次の詳細を指定します。

1. [Method List Name] フィールドに、メソッドリストの名前を入力します。
2. [Type] ドロップダウンリストから、[Login] を選択します。
3. [Group Type] ドロップダウンリストから、[Group] を選択します。
4. 以前に作成したサーバーグループ（ステップ j からステップ o）を [Available Server Groups] から [Assigned Servers Groups] に移動し、[Save & Apply to Device] をクリックします。

r) [AAA Method List] タブで、[Authorization] をクリックし、[Add] をクリックして、次の詳細を指定します。

1. [Method List Name] フィールドに、メソッドリストの名前を入力します。
2. [Type] ドロップダウンリストから、[Network] を選択します。
3. [Group Type] ドロップダウンリストから、[Group] を選択します。
4. 矢印ボタンを使用して、以前に作成したサーバーグループ（ステップ j からステップ o）を [Available Servers] から [Assigned Servers] に移動し、[Save & Apply to Device] をクリックします。

s) [AAA Method List] タブで、[Accounting] をクリックし、[Add] をクリックして、次の詳細を指定します。

1. [Method List Name] フィールドに、メソッドリストの名前を入力します。
2. [Type] ドロップダウンリストから、[Identity] を選択します。
3. [Group Type] ドロップダウンリストから、[Group] を選択します。
4. 矢印ボタンを使用して、以前に作成したサーバーグループ（ステップ j からステップ o）を [Available Servers] から [Assigned Servers] に移動し、[Save & Apply to Device] をクリックします。

ステップ 8 L3 および L2 認証（MAC フィルタリング）を有効にします。

Radius 認証のパラメータマップで、[Type] として [webauth] が選択されていることを確認します。

（注） L3 および L2 認証を設定するには、SSID を作成し、ステップ 6 のすべての設定を完了していることを確認してください。その後、SSID を Cisco DNA Spaces にインポートし、キャプティブポータルルールを使用して SSID のキャプティブポータルを設定します。

a) **[Configuration]** > **[Tags and Profiles]** > **[WLANs]** を選択します。
b) L2 および L3 認証を設定する SSID をクリックします。
c) [Edit WLAN] ウィンドウで [Security] タブをクリックします。
d) [Layer3] タブで、[Authentication] ドロップダウンリストから、以前に（ステップ 7q で）設定した Radius 認証を選択します。
e) [Layer2] タブで、[MAC Filtering] チェックボックスをオンにして、MAC フィルタリングを有効にします。
f) 表示される [Authorization List] ドロップダウンリストから、以前に（ステップ 7r で）作成した許可サーバーを選択します。
g) [Show Advanced Settings] をクリックします。
h) [On Mac Filter Failure] チェックボックスをオンにします。
i) [Update & Apply to Device] をクリックします。
j) **[Configuration]** > **[Tags and Profiles]** > **[Policy]** を選択します。
k) [default-policy-profile] をクリックします。
l) [Advanced] タブの [AAA Policy] エリアで、[Allow AAA Override] チェックボックスをオンにします。
m) [Policy Name] ドロップダウンリストから、デフォルトの [aaa] ポリシーが選択されていることを確認します。

n) [Update & Apply to Device] をクリックします。

Cisco DNA Spaces コネクタを使用した、Cisco DNA Spaces の Cisco AireOS ワイヤレスコントローラまたは Cisco Catalyst 9800 シリーズ ワイヤレス コントローラへの接続

Cisco DNA Spaces コネクタを備えた シスコ ワイヤレス コントローラ

Cisco DNA Spaces コネクタを使用して Cisco AireOS ワイヤレスコントローラを Cisco DNA Spaces に接続し、キャプティブポータルの認証または通知を設定するには、次の手順を実行します。

- 『Cisco DNA Spaces：コネクタ コンフィギュレーション ガイド』に記載されている手順を参照しながら、Cisco DNA Spaces コネクタを使用して Cisco AireOS ワイヤレスコントローラを Cisco DNA Spaces に接続します。
- Cisco AireOS コントローラを Cisco DNA Spaces に接続した後、インターネット プロビジョニングおよびRADIUS認証のためのシスコ ワイヤレス コントローラの設定の説明に従い、RADIUS 認証とインターネット プロビジョニングを設定します。
- キャプティブポータル認証が必要な場合は、SSID をインポートし、必要な認証タイプでキャプティブポータルを作成し、「キャプティブポータルアプリの使用」の章で説明されている手順に基づき、キャプティブポータルルールを設定します。
- キャプティブポータルにソーシャル認証が必要な場合は、「ソーシャル認証のためのシスコ ワイヤレス コントローラの設定 （17 ページ）」の説明に従って、ソーシャル認証を設定します。
- Cisco DNA Spaces を使用して通知を送信する場合は、「 Engagements アプリによる通知の送信」の章で説明されている手順に基づき、エンゲージメントルールを設定します。

Cisco DNA Spaces コネクタを備えた Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ

Cisco DNA Spaces コネクタを使用して Cisco Catalyst 9800 シリーズ ワイヤレス コントローラを Cisco DNA Spaces に接続し、キャプティブポータルの認証または通知を設定するには、次の手順を実行します。

- Cisco DNA Spaces コネクタを使用して Cisco Catalyst 9800 シリーズ ワイヤレス コントローラを Cisco DNA Spaces に接続するには、『Cisco DNA Spaces：コネクタ コンフィギュレーション ガイド』に記載されている手順を参照してください。
- Cisco Catalyst 9800 シリーズ ワイヤレス コントローラを Cisco DNA Spaces に接続した後、ソーシャル認証、RADIUS 認証、および（**キャプティブポータル**アプリと**エンゲージメント**アプリ使用のための）インターネットプロビジョニングについては、次の該当するセクションを参照してください。
  - CLI を使用したキャプティブポータルおよびエンゲージメントアプリ用の Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ（ローカルモード）の設定 （25 ページ）

- キャプティブポータルおよびエンゲージメントアプリ用の Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ GUI（ローカルモード） （29 ページ）
- キャプティブポータルおよびエンゲージメントアプリ用の Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ GUI（フレックスモードまたは Mobility Express） （35 ページ）。

- キャプティブポータル認証を設定するには、SSID をインポートし、必要な認証タイプでキャプティブポータルを作成し、「キャプティブポータルアプリの使用」の章で説明されている手順に基づき、キャプティブポータルルールを設定します。
- Cisco DNA Spaces を使用して通知を送信する場合は、「Engagements アプリによる通知の送信」の章で説明されている手順に基づき、エンゲージメントルールを設定します。

Cisco DNA Spaces と連携するための Mobility Express の設定

この項では、Cisco DNA Spaces を使用するために Mobility Express コントローラで行う設定について説明します。

必要な設定は、Mobility Express のバージョンによって異なります。Mobility Express バージョン別の設定方法を次に示します。

Cisco DNA Spaces 用の Mobility Express 8.7 以降の設定

Cisco DNA スペース用に Mobility Express 8.7 以降を設定するには、次の手順を実行します。

Mobility Express での SSID の作成

Mobility Express で SSID を作成するには、次の手順を実行します。

ステップ 1 ログイン情報を使用して [Mobility Express] にログインします。

ステップ 2 メインウィンドウで、左ペインの [Wireless Settings] をクリックします。

ステップ 3 [WLAN（WLANs）] をクリックします。

ステップ 4 WLAN を作成するには、[Add New WLAN] をクリックします。

ステップ 5 表示されるウィンドウの [General] タブで、[Type]、[Profile Name]、[SSID] などの WLAN の詳細を入力します。

ステップ 6 [Apply] をクリックします。

[Add New WLAN/RLAN] ウィンドウが表示されます。

ステップ 7 [WLAN Security] をクリックします。

ステップ 8 [Guest Network] トグルスイッチを有効にします。

ステップ 9 [Captive Network Assistant] トグルスイッチを有効にします。

ステップ 10 [Captive Portal] ドロップダウンリストから、[External Splash Page] を選択します。

ステップ 11 [Access Type] ドロップダウンリストから、[Web Consent] を選択します。

ステップ 12 表示される [Captive Portal URL] フィールドに、Cisco DNA Spaces のスプラッシュ URL を入力します。

ME アカウントのスプラッシュ URL を表示するには、Cisco DNA Spaces ダッシュボードの [SSIDs] ウィンドウで CUWN SSID の [Configure Manually] リンクをクリックします。

ステップ 13 [Apply] をクリックします。

ステップ 14 SSID を有効にしてブロードキャストするには、[General] タブの [Admin] ドロップダウンリストから [Enabled] を選択し、[Broadcast SSID] トグルスイッチを有効にします。

ステップ 15 コマンドプロンプトで次のコマンドを実行して、secure webauth モードを無効にします。その後、ME を再起動します。

```
config network web-auth secureweb disable
```

ステップ 16 コマンド プロンプトで次のコマンドを実行して、webauth login success page を [Default] から [None] に変更します。

config custom-web webauth-login-success-page none

Mobility Express 8.7 以後での Radius 認証の設定

Mobility Express 8.7 以後で Radius 認証を設定するには、次の手順を実行します。

ステップ 1 ログイン情報を使用して [Mobility Express] にログインします。

ステップ 2 ME のメインウィンドウで、ウィンドウ右上の [Switch to Expert View] をクリックします。

ステップ 3 表示されるポップアップウィンドウで、[OK] を選択します。

ステップ 4 左ペインで、[Management] > [Admin Accounts] をクリックします。

ステップ 5 表示されるウィンドウで、[Radius] タブをクリックします。

ステップ 6 [Add RADIUS Authentication Server] をクリックします。

[Add/ Edit Radius Authentication Server] ウィンドウが表示されたら、Radius サーバーに関する次の詳細を入力します。

a) [Server IP Address] フィールドに、Radius サーバーの IP アドレスを入力します。
b) [Shared Secret] フィールドに、Radius 秘密鍵を入力します。
c) [Confirm Shared Secret] フィールドに、Radius 秘密鍵を再入力します。

（注） Cisco DNA Spaces の Radius サーバーのみを設定できます。Radius サーバー設定用の IP アドレスと秘密鍵を表示するには、Cisco DNA Spaces ダッシュボードで、[Captive Portal] アプリをクリックします。[SSIDs] をクリックし、次に Cisco Unified Wireless Network（Cisco AireOS）SSID の [Configure Manually] リンクをクリックします。[Configure SSID in CUWN-WLC] タブをクリックします。Radius サーバーの詳細は、[Radius Server Configuration] セクションのリストに表示されます。プライマリおよびセカンダリ Radius サーバーの両方の IP を設定します。Cisco DNA Spaces サポートチームに連絡することもできます。

ステップ 7 [Apply] をクリックします。

ステップ 8 [Mobility Express] メインウィンドウで、左側のペインの [Wireless Settings] をクリックします。

ステップ 9 [WLANs] をクリックします。

[WLAN/RLAN Configuration] ウィンドウに SSID リストが表示されます。

ステップ 10 以前に作成した SSID の [Edit] アイコンをクリックします。

ステップ 11 表示される [Edit WLAN] ウィンドウで [WLAN Security] タブをクリックします。

ステップ 12 [Access Type] ドロップダウンリストから、[Radius] を選択します。

ステップ 13 [Radius Server] タブをクリックし、[Add Radius Authentication Server] をクリックします。

ステップ 14 [Server IP Address] ドロップダウンリストから Radius サーバーを選択し、[Apply] をクリックします。

ステップ 15 [Edit WLAN] ウィンドウで、[Apply] をクリックします。

これで、Mobility Express 8.7 以降が Radius サーバー認証用に設定されました。

Mobility Express 8.7 以降でのアクセス制御リストの作成

Mobility Express 8.7 以降でアクセス制御リストを作成するには、次の手順を行います。

ステップ 1 ログイン情報を使用して Mobility Express にログインします。

ステップ 2 Mobility Express のメインウィンドウで、左側のペインの [Wireless Settings] をクリックします。

ステップ 3 [WLAN（WLANs）] をクリックします。

[WLAN/RLAN Configuration] ウィンドウに SSID リストが表示されます。

ステップ 4 以前に作成した SSID の [Edit] アイコンをクリックします。

表示される [Edit WLAN] ウィンドウで [WLAN Security] タブをクリックします。

ステップ 5 [Pre Auth ACLs] タブをクリックします。

ステップ 6 [Add IP Rules] をクリックします。

ステップ 7 [Add/Edit IP ACLs] で、次の構成のルールを作成します。

アクション	送信元 IP アドレス/ネットマスク	宛先 IP アドレス/ネットマスク	プロトコル	送信元ポート範囲	宛先ポート範囲	DSCP
許可	3425248125252525	0.0.0.0/0.0.0.0	いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）
許可	0.0.0.0/0.0.0.0	3425248125252525	いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）
許可	5252539252525525	0.0.0.0/0.0.0.0	いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）
許可	0.0.0.0/0.0.0.0	5252539252525525	いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）

（注） EU リージョンの場合、34.235.248.212、52.55.235.39を 54.77.207.183、34.252.175.120 に置き換える必要があります。

ACL ルールを定義するときには、次のように値を設定します。

- **Protocol**：Any
- **DSCP**：Any
- **Action**：Permit

ステップ 8 [Apply] をクリックします。

ソーシャル認証のための Mobility Express 8.7 以降の設定

キャプティブポータルのソーシャルサイン認証用に Mobility Express を設定するには、次の手順を実行します。

ステップ 1 ログイン情報を使用して Mobility Express にログインします。

ステップ 2 Mobility Express のメインウィンドウで、左側のペインの [Wireless Settings] をクリックします。

ステップ 3 [WLAN（WLANs）] をクリックします。

[WLAN/RLAN Configuration] ウィンドウに SSID リストが表示されます。

ステップ 4 以前に作成した SSID の [Edit] アイコンをクリックします。

表示される [Edit WLAN] ウィンドウで [WLAN Security] タブをクリックします。

ステップ 5 [Pre Auth ACLs] タブをクリックします。

ステップ 6 [Add IP Rules] をクリックします。

ステップ 7 [Add/Edit IP ACLs] で、既存の ACL ルールに加えて、次の 2 つのルールを設定します。

アクション	送信元 IP アドレス/ネットマスク	宛先 IP アドレス/ネットマスク	プロトコル	送信元ポート範囲	宛先ポート範囲	DSCP
許可	0.0.0.0/0.0.0.0	0.0.0.0/0.0.0.0	TCP	HTTPS	いずれか（Any）	いずれか（Any）
許可	0.0.0.0/0.0.0.0	0.0.0.0/0.0.0.0	TCP	いずれか（Any）	HTTPS	いずれか（Any）

Mobility Express 8.7 以降での URL の許可

Mobility Express 8.7 以降で URL を許可するには、次の手順を行います。

ステップ 1 ログイン情報を使用して Mobility Express にログインします。

ステップ 2 Mobility Express のメインウィンドウで、左ペインの [Wireless Settings] をクリックします。

ステップ 3 [WLAN（WLANs）] をクリックします。

[WLAN/RLAN Configuration] ウィンドウに SSID リストが表示されます。

ステップ 4 以前に作成した SSID の [Edit] アイコンをクリックします。

ステップ 5 表示される [Edit WLAN] ウィンドウで [WLAN Security] タブをクリックします。

ステップ 6 [Pre Auth ACLs] タブをクリックします。

ステップ 7 [Add URL Rules] をクリックします。

ステップ 8 表示される [Add/Edit URL ACLs] ウィンドウで、許可リストに含める URL を設定します。

URL ルールを定義するときには、次のように値を設定します。

- [URL]：domain
- **Action**：Permit

ステップ 9 [更新（Update）] をクリックします。

通知およびレポート用 Mobility Express の設定

WLC 接続で Mobility Express を使用している場合、ロケーションの更新を設定するには、次の手順を実行します。

ステップ 1 シスコ ワイヤレス コントローラの **CLI** で、次のコマンドを実行します。

1. config cloud-services cmx disable
2. config cloud-services server url https://{Customer Path Key}.{LB Domain} {LB IP Address}
3. config cloud-services server id-token {Customer JWT Token}
4. config network dns serverip <dns server ip>
5. config cloud-services cmx enable

（注） Customer Path Key}、{LB Domain}、{LB IP Address}、{Customer JWT Token} を表示するには、Cisco DNA Spaces ダッシュボードの [SSID] ウィンドウで、CUWN SSID の [Configure Manually] リンクをクリックします。Cisco DNA Spaces サポートチームに連絡することもできます。末尾または先頭にスペースがないことを確認します。

ステップ 2 次のコマンドを使用して、概要を確認します。

show cloud-services cmx summary

結果が表示されます。

Cisco DNA Spaces ダッシュボードで、[Add a Wireless Network] ウィンドウの [CUWN-WLC] を選択すると、WLC が一覧表示されます。これにより、その WLC の AP を Cisco DNA Spaces にインポートできます。

結果サンプル

(Cisco Controller) >show cloud-services cmx summary

CMX Service

Server ..... https://$customerpathkey.dnaspaces.io

IP Address..... 50.16.12.224

Connectivity..... https: UP

Service Status ..... アクティブ

Last Request Status..... HTTP/1.1 200 OK

Heartbeat Status ..... OK

次のタスク

これで、シスコ ワイヤレス コントローラを Cisco DNA Spaces のロケーション階層にインポートできるようになります。シスコ ワイヤレス コントローラとそのアクセスポイントのインポートの詳細については、「Cisco WLC Direct Connect を使用した Cisco DNA Spaces のシスコ ワイヤレス コントローラへの接続 （20 ページ）」で説明されている手順のステップ 4 から実行してください。

Cisco DNA Spaces 用の Mobility Express 8.6 以前の設定

Cisco DNA Spaces 用に Mobility Express 8.6 以前を設定するには、次の手順を実行します。

Mobility Express 8.6 以前での SSID の作成

Mobility Express 8.6 以前で SSID を作成する手順は、Mobility Express 8.7 以降の場合と同じです。設定手順については、Mobility Express での SSID の作成 （42 ページ）を参照してください。

Mobility Express 8.6 以前での Radius 認証の設定

Mobility Express 8.6 以前の場合、Radius サーバーを個別に設定することはできません。

Mobility Express 8.6 以前で Radius 認証を設定するには、次の手順を実行します。

ステップ 1 ログイン情報を使用して [Mobility Express] にログインします。

ステップ 2 [Mobility Express] メインウィンドウで、左側のペインの [Wireless Settings] をクリックします。

ステップ 3 [WLAN（WLANs）] をクリックします。
[WLAN/RLAN Configuration] ウィンドウに SSID リストが表示されます。

ステップ 4 以前に作成した SSID の [Edit] アイコンをクリックします。

ステップ 5 表示される [Edit WLAN] ウィンドウで [WLAN Security] タブをクリックします。

ステップ 6 [Access Type] ドロップダウンリストから、[Radius] を選択します。

ステップ 7 Radius サーバーを追加するには、[Add] をクリックします。

ステップ 8 表示されるウィンドウで、次の Radius サーバーの詳細を入力します。

1. [Server IP Address] フィールドに、Radius サーバーの IP アドレスを入力します。
2. [Shared Secret] フィールドに、Radius 秘密鍵を入力します。
3. [Confirm Shared Secret] フィールドに、Radius 秘密鍵を再入力します。
4. [Apply] をクリックします。

（注） Cisco DNA Spaces の Radius サーバーのみを設定できます。Radius サーバー設定用の IP アドレスと秘密鍵を表示するには、Cisco DNA Spaces ダッシュボードで、[Captive Portal] アプリをクリックします。[SSIDs] をクリックし、次に Cisco Unified Wireless Network（Cisco AireOS）SSID の [Configure Manually] リンクをクリックします。[Configure SSID in CUWN-WLC] タブをクリックします。Radius サーバーの詳細は、[Radius Server Configuration] セクションのリストに表示されます。プライマリおよびセカンダリ Radius サーバーの両方の IP を設定します。Cisco DNA Spaces サポートチームに連絡することもできます。

ステップ 9 [Edit WLAN] ウィンドウで、[Apply] をクリックします。

これで、Cisco DNA Spaces キャプティブポータルの Radius サーバー認証が Mobility Express に設定されました。

Mobility Express 8.6 以前での ACL の作成

Mobility Express 8.6 以前には、アクセス制御リストを設定するためのユーザーインターフェイスがありません。そのため、ACL を作成し、ソーシャル認証を設定するには、コマンドプロンプトを使用する必要があります。これらの ACL の設定に使用するコマンドについては、『Mobility Express コマンドリファレンスガイド』を参照してください。

これで、シスコ ワイヤレス コントローラを Cisco DNA Spaces のロケーション階層にインポートできるようになります。シスコ ワイヤレス コントローラと、シスコ ワイヤレス コントローラへのアクセスポイントのインポートの詳細については、「Cisco WLC Direct Connect を使用した Cisco DNA Spaces のシスコ ワイヤレス コントローラへの接続 （20 ページ）」で説明されている手順のステップ 3 から実行してください。

通知およびレポート用 Mobility Express の設定

WLC 接続で Mobility Express を使用している場合、ロケーションの更新を設定するには、次の手順を実行します。

ステップ 1 シスコ ワイヤレス コントローラの CLI で、次のコマンドを実行します。

1. config cloud-services cmx disable

2. config cloud-services server url https://{Customer Path Key}.{LB Domain} {LB IP Address}
3. config cloud-services server id-token {Customer JWT Token}
4. config network dns serverip <dns server ip>
5. config cloud-services cmx enable

（注） Customer Path Key}、{LB Domain}、{LB IP Address}、{Customer JWT Token} を表示するには、Cisco DNA Spaces ダッシュボードの [SSID] ウィンドウで、CUWN SSID の [Configure Manually] リンクをクリックします。Cisco DNA Spaces サポートチームに連絡することもできます。末尾または先頭にスペースがないことを確認します。

ステップ 2 次のコマンドを使用して、概要を確認します。

show cloud-services cmx summary

結果が表示されます。

Cisco DNA Spaces ダッシュボードで、[Add a Wireless Network] ウィンドウの [CUWN-WLC] を選択すると、WLC が一覧表示されます。これにより、その WLC の AP を Cisco DNA Spaces にインポートできます。

結果サンプル

(Cisco Controller) >show cloud-services cmx summary

CMX Service

Server ..... https://$customerpathkey.dnaspaces.io

IP Address..... 50.16.12.224

Connectivity..... https: UP

Service Status ..... アクティブ

Last Request Status..... HTTP/1.1 200 OK

Heartbeat Status ..... OK

次のタスク

これで、シスコ ワイヤレス コントローラを Cisco DNA Spaces のロケーション階層にインポートできるようになります。シスコ ワイヤレス コントローラとそのアクセスポイントのインポートの詳細については、「Cisco WLC Direct Connect を使用した Cisco DNA Spaces のシスコ ワイヤレス コントローラへの接続 （20 ページ）」で説明されている手順のステップ 4 から実行してください。

Cisco DNA Spaces 用 Aironet 4800 シリーズ Mobility Express コントローラ 8.10.150.0 の設定

Cisco DNA Spaces 用 AireOS 4800 シリーズ Mobility Express コントローラ 8.10.150.0 を設定するには、次の手順を実行します。

Mobility Express 8.10.150.0 の設定

Cisco DNA Spaces 用に Mobility Express 8.10.105.0 を設定するには、次の手順を実行します。

ステップ 1 ログイン情報を使用して Mobility Express にログインします。

ステップ 2 **[Advanced]** > **[Security Settings]** に移動します。

ステップ 3 [Add New ACL] をクリックします。

ステップ 4 [Add ACL Rule] ウィンドウで、ACL の詳細を入力します。

a) [ACL Type] ドロップダウンリストから、[IPv4] を選択します。

b) [ACL Name] フィールドに、新しい ACL の名前を入力します。

c) [Add URL Rules] をクリックします。

[Add /Edit URL ACLs] ウィンドウが表示されます。

d) [URL] フィールドに、スプラッシュページの URL ドメインを入力します。

e) [Action] ドロップダウンリストで、[Permit] を選択します。

f) ソーシャル認証を有効にするには、ACL に次のドメインを追加します。

- *.facebook.com
- *.facebook.com
- ssl.gstatic.com
- static.licdn.com
- *.fbcdn.net
- *.akamaihd.net
- *.twitter.com
- *.twimg.com
- oauth.googleusercontent.com
- *.googleapis.com
- *.accounts.google.com
- *.gstatic.com
- *.linkedin.com
- *.licdn.net
- *.licdn.com

この手順は、ソーシャル認証を有効にする場合にのみ必要です。

g) [更新（Update）] をクリックします。

ステップ 5 RADIUS サーバーを設定する手順は、次のとおりです。

a) ACL を作成します。

b) [Expert View] を有効にします。
c) **[Managenent]** > **[Admin Accounts]** > **[Radius]** に移動します。
d) [Authentication Call Station ID Type] ドロップダウンリストから、[AP MAC Address:SSID] を選択します。
e) [Authentication MAC Delimiter] ドロップダウンリストから、[Hyphen] を選択します。
f) [Accounting Call Station ID Type] ドロップダウンリストから、[AP MAC Address:SSID] を選択します。
g) [Accounting MAC Delimiter] ドロップダウンリストから、[Hyphen] を選択します。
h) [Fallback Mode] ドロップダウンリストから、[Off] を選択します。
i) [Apply] をクリックします。

ステップ 6 [Add Radius Authentication Server] をクリックし、表示される [Add/Edit Radius Authentication Server] で、次の詳細を入力します。

a) [CoA] を無効にします。
b) [Server Ip Address] フィールドに RADIUS サーバーの IP アドレスを入力します。
c) [Shared Secret] フィールドに、秘密鍵を入力します。
d) [Confirm Shared Secret] フィールドに、確認のための秘密鍵を入力します。
e) [Apply] をクリックします。

追加された Radius サーバーは、Radius サーバーリストの下に表示されます。

（注） Cisco DNA Spaces の Radius サーバーのみを設定できます。Radius サーバー設定の IP アドレスと秘密鍵を表示するには、Cisco DNA Spaces ダッシュボードで、[Captive Portals] アプリをクリックします。[SSIDs] をクリックし、次に Cisco Unified Wireless Network（Cisco AireOS）SSID の [Configure Manually] リンクをクリックします。Radius サーバーの詳細は、[Radius Server Configuration] セクションに表示されます。プライマリとセカンダリの両方の Radius サーバー IP を設定します。Cisco DNA Spaces サポートチームに連絡することもできます。

ステップ 7 Radius サーバーの [WLAN] を設定するには、次の手順を実行します。

a) [Cisco Aironet ME] ダッシュボードで、**[Wireless Settings]** > **[WLAN]** を選択します。
b) [General] タブをクリックします。
c) [Profile Name] フィールドに、SSID の名前を入力します。
d) [Admin State] ドロップダウンリストから、[Enabled] を選択します。
e) [Radio Policy] ドロップダウンリストから、[ALL] を選択します。
f) [WLAN Security] タブをクリックします。
g) [Guest Network] を有効にします。
h) [Captive Network Assistant] を有効にします。
i) [Captive Portal URL] フィールドに、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 を表示するには、Cisco DNA Spaces ダッシュボードで、[Captive Portals] アプリをクリックします。[SSIDs] をクリックし、次に Cisco Unified Wireless Network（Cisco AireOS）SSID の [Configure Manually] リンクをクリックします。**WLC Direct Connect の SSID の作成**セクションに移動します。手順 7g で URL が表示されます。

j) [Access Type] から、[RADIUS] を選択します。
k) [ACL Name (IPV4)] で、手順 4b で設定した ACL の名前を選択します。

l) Radius サーバーの場合、[Add Radius Authentication Server] をクリックします。
m) リストから、手順 6b で追加した Radius サーバーの IP を選択します。

ステップ 8 Radius L2 認証の場合、[MAC Filtering] と [ON MAC Filter failure] を有効にします。

ステップ 9 [Apply] をクリックします。

通知およびレポート用 Mobility Express の設定

WLC 接続で Mobility Express を使用している場合、ロケーションの更新を設定するには、次の手順を実行します。

ステップ 1 シスコ ワイヤレス コントローラの **CLI** で、次のコマンドを実行します。

1. config cloud-services cmx disable
2. config cloud-services server url https://{Customer Path Key}.{LB Domain} {LB IP Address}
3. config cloud-services server id-token {Customer JWT Token}
4. config network dns serverip <dns server ip>
5. config cloud-services cmx enable

（注） Customer Path Key}、{LB Domain}、{LB IP Address}、{Customer JWT Token} を表示するには、Cisco DNA Spaces ダッシュボードの [SSID] ウィンドウで、CUWN SSID の [Configure Manually] リンクをクリックします。Cisco DNA Spaces サポートチームに連絡することもできます。末尾または先頭にスペースがないことを確認します。

ステップ 2 次のコマンドを使用して、概要を確認します。

show cloud-services cmx summary

結果が表示されます。

Cisco DNA Spaces ダッシュボードで、[Add a Wireless Network] ウィンドウの [CUWN-WLC] を選択すると、WLC が一覧表示されます。これにより、その WLC の AP を Cisco DNA Spaces にインポートできます。

結果サンプル

(Cisco Controller) >show cloud-services cmx summary

CMX Service

Server ..... https://$customerpathkey.dnaspaces.io

IP Address..... 50.16.12.224

Connectivity..... https: UP

Service Status ..... アクティブ

Last Request Status..... HTTP/1.1 200 OK

Heartbeat Status ..... OK

次のタスク

これで、シスコ ワイヤレス コントローラを Cisco DNA Spaces のロケーション階層にインポートできるようになります。シスコ ワイヤレス コントローラとそのアクセスポイントのインポートの詳細については、「Cisco WLC Direct Connect を使用した Cisco DNA Spaces のシスコ ワイヤレス コントローラへの接続 （20 ページ）」で説明されている手順のステップ 4 から実行してください。

Cisco DNA Spaces 拡張ベンチマーク

表 *3 :* 拡張の概要

SNO	Cisco DNA Spaces コネクタ	Cisco WLC Direct Connect		CMX テザリング コネクタ
プラットフォーム	Cisco AireOS	Cisco AireOS	Cisco Catalyst 9800 シリーズ	Cisco AireOS
サポートされているアプライアンスでの最大拡張	12500 台の AP、250000 台のクライアント 着信 NMSP は、10500 メッセージ/秒を超えることはできません。	50 台の AP と 50 台のクライアント	50 台の AP と 50 台のクライアント	60000 台のクライアント、5000 台の AP、50000 個の RFID タグ 1 ビルディング - 100 フロアと各フロアに 50 台の AP のマップ
拡張がサポートされているリリース	コネクタバージョン 2.1.1 と docker v2.0.204	8.8MR2	16.12、17.1	8.8MR2 と CMX 10.6（ハイエンド）

（注） 現在、Mobility Express は拡張に対応していません。