Configuring Cisco Wireless Controllers and Cisco Catalyst 9800 Series Controllers for Cisco Spaces

This chapter describes the configurations to be done in the CiscoWireless Controller (Cisco AireOS) or Cisco Catalyst 9800 Series Controllers to work with Cisco Spaces. The configurations required differ based on the wireless controller type and connector you use.

Note

- You cannot connect a Cisco Wireless Controller with hyper location with Cisco Spaces and Cisco CMX simultaneously.
- If you want to connect a Cisco Wireless Controller with both Cisco CMX and Cisco Spaces simultaneously, you must use a Cisco Spaces: Connector. Check the limitations for the number of NMSP connections your Cisco Wireless Controller can support, and ensure that your Cisco Wireless Controller can support the addition of a new connection to Cisco Spaces: Connector, especially if there are existing connections to multiple Cisco CMX servers.
- You cannot use a Cisco Wireless Controller simultaneously with Cisco WLC Direct Connect and Cisco Spaces: Connector. Disable the Cisco WLC Direct Connect before using the Cisco Spaces: Connector.
- It is recommended to use Cisco Spaces: Connector rather than Cisco WLC Direct Connect, especially when you are using a lower version of Cisco Wireless Controller.Also, certain apps such as Operation Insights, Detect and Locate, and so on are supported only by Cisco Spaces: Connector.
- It is not recommended to compare the data displayed in your wireless network with the data shown in Cisco Spaces reports as it is expected to defer as per the design.

Note The configurations are done in the external applications that are not a part of Cisco Spaces, and the menu path and names specified for the tabs, windows, options, and so on in this documentation are subject to change.

The features supported by various connector types, and the configurations for various combinations of wireless controllers and connectors are as follows:

- Connecting Cisco Catalyst 9800 Series Wireless Controller or Cisco Wireless Controller to Cisco Spaces Using WLC Direct Connect or Cisco Spaces: Connector, on page 17
- Cisco Spaces Scale Benchmark, on page 46

Features Supported by Various Connectors

The following table lists the features supported by each type of connector. You can opt the connector based on the feature or app that you want to use. Cisco Spaces: Connector is recommended if you want to use the apps such as Operational Insights and Open Roaming.

Table 1: Connectors-Feature Support

Features/Apps	Cisco Spaces Connector	**Cisco WLC Direct Connect (Recommended only for small scale deployments)**[1] Connecting Cisco Spaces to Cisco Wireless Controller Using Cisco WLC Direct Connect Connecting Cisco Spaces to Cisco Catalyst 9800 Series Wireless Controller Using Cisco WLC Direct Connect	Cisco CMX Tethering Connector	**Wired Devices**	Cisco Meraki
Cisco Spaces Dashboard	Supported	Supported	Supported	Not Supported	Supported
Captive Portals	Supported	Supported	Supported	Not Supported	Supported
Engagements	Supported	Supported	Supported	Not Supported	Supported
Location Personas	Supported	Supported	Supported	Not Supported	Supported
Location Analytics	Supported	Supported	Supported	Not Supported	Supported
Impact Analysis	Supported	Supported	Supported	Not Supported	Supported
Camera Metrics	Not Supported	Not Supported	Not Supported	Not Supported	Supported

Features/Apps	Cisco Spaces Connector	Cisco WLC Direct Connect (Recommended only for small scale deployments)[1] Connecting Cisco Spaces to Cisco Wireless Controller Using Cisco WLC Direct Connect Connecting Cisco Spaces to Cisco Catalyst 9800 Series Wireless Controller Using Cisco WLC Direct Connect	Cisco CMX Tethering Connector	Wired Devices	Cisco Meraki
Behaviour Metrics	Supported	Supported	Supported	Not Supported	Supported
RightNow WiFi	Supported	Supported	Supported	Supported	Supported
RightNow Video	Not Supported	Not Supported	Not Supported	Not Supported	Supported
Open Roaming[2]	Supported	Not Supported	Not Supported	Not Supported	Supported
IoT Services	Supported[3]	Not Supported	Not Supported	Supported	—
Detect and Locate	Supported	Limited Support (Associated Clients only)	Supported	Not Supported	—
Hyperlocation	Supported	Not Supported	Supported	Not Supported	Not Supported
Fastlocate	Supported	Not Supported	Supported	Not Supported	Not Supported
Scale Support For more details, see the scale summary in Cisco Spaces Scale Benchmark, on page 46.	Best suited for scaling	Scale supported for AireOS Controller 8.8 MR2 and Cisco Catalyst 9800 Series 16.12.1.	Supports the scale that Cisco CMX can handle.	Not Supported	Best suited for scaling

Features/Apps	Cisco Spaces Connector	Cisco WLC Direct Connect (Recommended only for small scale deployments)[1] Connecting Cisco Spaces to Cisco Wireless Controller Using Cisco WLC Direct Connect Connecting Cisco Spaces to Cisco Catalyst 9800 Series Wireless Controller Using Cisco WLC Direct Connect	Cisco CMX Tethering Connector	Wired Devices	Cisco Meraki
AireOS Controller Platform Support	Supported	Supported	Supported	Not Supported	Not applicable
Cisco Catalyst 9800 Platform Support	Supported	Supported	Supported	Not Supported	Not applicable

[1] Connecting through the Cisco Wireless Controller Direct Connection method is only recommended for small scale deployments. All large scale production deployment require a Cisco Spaces: Connector.

[2] As the **Open Roaming** app is in Beta, currently documentation is not available for this app. For any information related to **Open Roaming**, contact the Cisco Spaces support team.

[3] Currently, support for IoT services is only available for Cisco Catalyst 9800 Controller.

Note

- Connecting through the Cisco Wireless Controller Direct Connection method is only recommended for small-scale deployments. All large-scale production deployments require a Cisco Spaces: Connector.
- For more information about **Cisco Spaces:OpenRoaming**, see Cisco Spaces: OpenRoaming Configuration Guide.

Connecting Cisco Spaces to Cisco Wireless Controller through Cisco CMX

To connect Cisco Spaces with Cisco Wireless Controllers through Cisco CMX, you must have Cisco CMX 10.6 or later.

For Cisco Unified Wireless Network with Cisco CMX, the following configurations are required to work with Cisco Spaces:

Note

- The configuration for internet provisioning and RADIUS authentication is required only if you need RADIUS authentication. This configuration is required only if you need social authentication for your portals.

Configuring Access Point Mode, SSIDs, ACLs, Splash URLs, and Virtual Interface in the WLC

To create a Captive Portal rule, you must initially define the mode for access points, and create the SSIDs and ACLs in the Cisco Wireless Controller. You must also ensure that the splash URL for the SSID is configured in the Cisco Wireless Controller.

Note The SSIDs and ACLs are created in the Cisco Wireless Controller and not in the Cisco CMX.

The Cisco Wireless Controller configurations for the local and flexconnect modes are different.

Note The configurations are done in the Cisco Wireless Controller that is not a part of Cisco Spaces, and the menu path and names specified for the tabs, windows, options, and so on in this documentation are subject to change.

Local Mode Configurations for Using Cisco Spaces

To configure the Cisco Wireless Controller to use with Cisco Spaces in the local mode, perform the following steps:

Configure the Local Mode for an Access Point

To configure a local mode for an access point, perform the following steps:

Step 1 Log in to the Cisco Wireless Controller with your Wireless Controller credentials.

Step 2 In the Cisco Wireless Controller main window, click the **Wireless** tab.

All of the access points are listed.

Step 3 Click the access point for which you want to configure the mode to local.

Step 4 Click the **General** tab.

Step 5 From the **AP Mode** drop-down list, choose **Local**, and click **Apply**.

Create SSIDs in Cisco Wireless Controller

Note The SSIDs are created in the Cisco Wireless Controller, not in the Cisco CMX.

To create the SSIDs in the Cisco Wireless Controller, perform the following steps:

Step 1 In the Cisco Wireless Controller main window, click the **WLANs** tab.

Step 2 To create a WLAN, choose **Create New** from the drop-down list at the right side of the window, and click **Go**.

Step 3 In the **New** window that appears, enter the WLAN details like Type, Profile Name, SSID, and so on.

Step 4 Click **Apply**.

The **Edit <SSID Name>** window appears.

Step 5 Add the SSID to the Cisco Spaces dashboard.

Step 6 In the Cisco Wireless Controller main window, on the **General** tab, uncheck the **Broadcast SSID** check box.

Note The SSID Broadcasting is interrupted to avoid any customer accessing the SSID before completing the configurations.

Step 7 Choose **Security** > **Layer 2**, and check the **MAC Filtering** check box.

Step 8 In the **Layer 3** tab, do the following configurations:

a) From the **Layer 3 security** drop-down list, choose **Web Policy**.

Note **Web Policy** is the Layer 3 security option that enables you to configure captive portal in the Cisco Wireless Controller.

b) Choose the **On Mac Filter Failure** radio button.

c) In the **Preauthentication ACL** area, from the **IPv4** drop-down list, choose the ACL previously defined.

d) Check the **Enable** check box for the Sleeping Client.

Note Enabling sleeping client is not mandatory. But if enabled, the customer who is in sleeping mode after authentication gets connected without authentication if is waken up within the specified time. The clients with guest access that had successful web authentication are allowed to sleep and wake up without having to go through another authentication process through the login page. You can configure the duration for which the sleeping clients are to be remembered for before re-authentication becomes necessary. The valid range is 1 hour to 720 hours (30 days), with the default being 12 hours. Ideally, this should be similar to session timeout.

e) Check the **Enable** check box for the Override Global Config.

Note Enabling **Override global config** allows you to redirect the customer to the Cisco Spaces URL, which is an external URL.

f) From the **Web Auth Type** drop-down list, choose **External (Redirect to External Server)**.

Note The **Web Auth Type** must be **External** as the Cisco Spaces page is hosted in the external server, and not in the controller.

g) In the **URL** field that appears, enter the Cisco Spaces splash URL.

To view the splash URL for your CUWN or AireOS account, in the Cisco Spaces dashboard, the **Configure Manually** link for a AireOS SSID in the **SSIDs** window. The Configure Manually link appears only after adding a Cisco AireOS SSID.

Note You must configure the splash page for the customer to be redirected to the Cisco Spaces web page during on-boarding.

h) Click **Apply**.

Step 9 Click the **Advanced** tab.

Step 10 In the **Enable Session Timeout** field, enter the required session timeout value in seconds. For example, for session timeout of 30 minutes, enter 1800.

Step 11 Click **Apply**.

Step 12 In the **General** tab, check the **Enabled** check box for the **Status** and **Broadcast SSID** options, to enable the SSID.

Step 13 Execute the following command in the command prompt to disable captive bypassing. Then, restart the Cisco Wireless Controller.

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

Note If captive bypassing is enabled, the CNA will not pop up for iOS devices.

Step 14 In the **HTTP-HTTPS configuration** window that appears, do the following:

a) From the **HTTP Access** drop-down list, choose **Disabled**.
b) From the **HTTPS Access** drop-down list, choose **Enabled**.
c) From the **WebAuth SecureWeb** drop-down list, choose **Disabled**.
d) Click **Apply**.

Step 15 Choose **Security** > **Web Auth** > **Web Login Page**, and ensure that the Redirect URL after login field is blank.

Note The redirect URL field must be blank so that it won't override the Cisco Spaces splash URL configured in **Layer 3**.

What to do next

Note If you have made any changes to the **Management** tab, then restart your Cisco Wireless Controller for the changes to take effect.

Create Access Control Lists

To restrict the Internet access for customers, and to allow access only to Cisco Spaces splash page URL when connected to the SSID, the Cisco Spaces IPs (wall garden ranges) must be configured in the ACL. Now when a customer connects to the SSID, the splash page appears for the customer.

If ACL is not configured with all the required IPs, the system considers the Cisco Spaces as an external URL, and results into multiple redirection for customer.

To create the access control list, perform the following steps:

Step 1 Log in to the Cisco Wireless Controller with your Wireless Controller credentials.

Step 2 Choose **Security** > **Access Control Lists** > **Access Control Lists**.

Step 3 To add an ACL, click **New**.

Step 4 In the **New** window that appears, enter the following:.

a) In the **Access Control List Name** field, enter a name for the new ACL.

Note You can enter up to 32 alphanumeric characters.

b) Choose the ACL type as **IPv4**.

c) Click **Apply**.

Step 5 When the **Access Control Lists** window reappears, click the name of the new ACL.

Step 6 In the **Edit** window that appears, click **Add New Rule**.

The **Rules** > **New** window appears.

Step 7 Configure a rule for this ACL with the required wall garden ranges.

To view the wall garden ranges, in the **Cisco Spaces** dashboard, click the **Configure Manually** link for a Cisco Unified Wireless Network SSID in the **SSIDs** window. The wall garden ranges are listed under the caption **Creating the Access Control List**. The **Configure Manually** link appears only after adding a Cisco AireOS SSID.

When defining the ACL rule, ensure to configure the values as follows:

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

Step 8 If you want to provide social authentication for your portal, you must also configure the wall garden ranges for social authentication.

Note The wall garden ranges configured for social authentication allows the customers to access all the HTTPS web sites directly after connecting to your SSID, without using the captive portal.

Configure the Virtual Interface

To configure the virtual interface, perform the following steps:

Step 1 Choose **Controller** > **Interfaces**.

Step 2 Click the **Virtual** link.

Step 3 In the **Interfaces** > **Edit** window that appears, enter the following parameters:

a) In the **IP address** field, enter the unassigned and unused gateway IP address, if any.

b) In the **DNS Host Name** field, enter the DNS Host Name, if any.

Note Ideally this field must be blank.

Note To ensure connectivity and web authentication, the DNS server must always point to the virtual interface. If a DNS hostname is configured for the virtual interface, then you must configure the same DNS host name on the DNS servers used by the client.

c) Click **Apply**.

Note If you have made any changes to the virtual interface, restart your Cisco Wireless Controller for the changes to take effect.

FlexConnect Mode Configurations for Using Cisco Spaces

You can configure FlexConnect for central switch or local switch mode.

FlexConnect Central Switch Mode

To configure the Cisco Wireless Controller to use the Cisco Spaces in the FlexConnect central switch mode, perform the following steps:

Configure the FlexConnect Mode for an Access Point

This configuration is applicable for FlexConnect central switch and local switch mode. To configure a FlexConnect Central switch mode for an access point, perform the following steps:

Step 1 In the Cisco Wireless Controller main window, click the **Wireless** tab.

All of the access points are listed.

Note For more details on the access points, see the Cisco Wireless Controller user guide.

Step 2 Click the access point for which you want to configure the mode to FlexConnect.

Step 3 Click the **General** tab.

Step 4 From the **AP Mode** drop-down list, choose **FlexConnect**.

Step 5 Click **Apply** to commit your changes and to cause the access point to reboot.

Create SSIDs in the Cisco Wireless Controller for FlexConnect Central Switch Mode

Create the SSID using the same steps as outlined for the local mode. For more information, see the Create SSIDs in Cisco Wireless Controller , on page 6.

Create Access Control Lists for FlexConnect Central Switch Mode

Create the Access Control List using the same steps as outlined for the local mode. For more information, see the Create Access Control Lists, on page 7.

Configure the Virtual Interface

To configure the virtual interface, perform the following steps:

Step 1 Choose **Controller** > **Interfaces**.

Step 2 Click the **Virtual** link.

Step 3 In the **Interfaces** > **Edit** window that appears, enter the following parameters:

a) In the **IP address** field, enter the unassigned and unused gateway IP address, if any.

b) In the **DNS Host Name** field, enter the DNS Host Name, if any.

Note Ideally this field must be blank.

Note To ensure connectivity and web authentication, the DNS server must always point to the virtual interface. If a DNS hostname is configured for the virtual interface, then you must configure the same DNS host name on the DNS servers used by the client.

c) Click **Apply**.

Note If you have made any changes to the virtual interface, restart your Cisco Wireless Controller for the changes to take effect.

FlexConnect Local Switch Mode

To configure the Cisco Wireless Controller to use the Cisco Spaces in the FlexConnect local switch mode, perform the following steps:

- Configure the FlexConnect Mode for an Access Point, on page 9

Configure the FlexConnect Mode for an Access Point

This configuration is applicable for FlexConnect central switch and local switch mode. To configure a FlexConnect Central switch mode for an access point, perform the following steps:

Step 1 In the Cisco Wireless Controller main window, click the **Wireless** tab.

All of the access points are listed.

Note For more details on the access points, see the Cisco Wireless Controller user guide.

Step 2 Click the access point for which you want to configure the mode to FlexConnect.

Step 3 Click the **General** tab.

Step 4 From the **AP Mode** drop-down list, choose **FlexConnect**.

Step 5 Click **Apply** to commit your changes and to cause the access point to reboot.

Create SSIDs in the Cisco Wireless Controller for the FlexConnect Local Switch Mode

Note The SSIDs are created in the Cisco Wireless Controller, not in the Cisco CMX.

To create the SSIDs in the CUWN for the FlexConnect local switch mode, perform the following steps:

Step 1 In the Cisco Wireless Controller main window, click the **WLANs** tab.

Step 2 To create a WLAN, choose **Create New**from the drop-down list at the right side of the window, and click **Go**.

Step 3 In the **New** window that appears, enter the WLAN details such as, Type, Profile Name, SSID, and so on.

Step 4 Click **Apply**.

The **Edit <SSID Name>** window appears.

Step 5 Add the SSID to the Cisco Spaces dashboard.

Step 6 In the Cisco Wireless Controller main window, on the **General** tab, uncheck the **Broadcast SSID** check box.

Note The SSID Broadcasting is interrupted to avoid any customer accessing the SSID before completing the configurations.

Step 7 Choose **Security** > **Layer 2**, and check the **MAC Filtering** check box.

Step 8 In the **Layer 3** tab, do the following configurations:

a) From the Layer 3 security drop-down list, choose **Web Policy**.

Note **Web Policy** is the **Layer 3** security option that enables you to configure captive portal in the Cisco Wireless Controller.

b) Choose the **On Mac Filter Failure** radio button.

c) In the **Preauthentication AC**L area, from the **WebAuth FlexAC**L drop-down list, choose the ACL previously defined.

d) Check the **Enable** check box for Sleeping Client.

Note Enabling sleeping client is not mandatory. But if enabled, the customer who is in sleeping mode after authentication gets connected without authentication if is waken up within the specified time. The clients with guest access that had successful web authentication are allowed to sleep and wake up without having to go through another authentication process through the login window. You can configure the duration for which the sleeping clients are to be remembered for before re-authentication becomes necessary. The valid range is 1 hour to 720 hours (30 days), with the default being 12 hours. Ideally, this should be similar to session timeout.

e) Check the **Enable** check box for Override Global Config.

Note Enabling **Override Global Config** enables you to redirect the customer to the Cisco Spaces URL, which is an external URL.

f) From the **Web Auth Type** drop-down list, choose **External**.

Note The **Web Auth Type** must be **External** as the Cisco Spaces page is hosted in the external server, and not in the controller.

g) In the URL field that appears, enter the Cisco Spaces Splash URL.

To view the splash URL for your CUWN account, in the Cisco Spaces dashboard, click the **Configure Manually** link for a CUWN SSID in the **SSIDs** window. The **Configure Manually** link appears only after adding a Cisco AireOS SSID.

Note You must configure the splash page for the customer to be redirected to the Cisco Spaces web page during on-boarding.

h) Click **Apply**.

Step 9 Click the **Advanced** tab.

Step 10 In the **Enable Session Timeout** field, enter the required session timeout value in seconds. For example, for session timeout of 30 minutes, enter 1800.

Step 11 In the **FlexConnect** area, check the **Enabled** check box for FlexConnect Local Switching, and click **Apply**.

Step 12 In the **General** tab, select the **Enabled** check box for the Status and Broadcast SSID options, to enable the SSID.

Step 13 Execute the following command in the command prompt to disable captive bypassing. Then, restart the Cisco Wireless Controller.

```
config network web-auth captive-bypass disable
```

Note If captive bypassing is enabled, the CNA will not pop up for iOS devices.

Step 14 Choose **Management** > **HTTP-HTTPS**.

Step 15 In the **HTTP-HTTPS Configuration** window that appears, perform the following:

a) From the **HTTP Access** drop-down list, choose **Disabled**.
b) From the **HTTPS Access** drop-down list, choose **Enabled**.
c) From the **WebAuth SecureWeb** drop-down list, choose **Disabled**.
d) Click **Apply**.

Step 16 Choose **Security** > **Web Auth** > **Web Login Page**, and ensure that the **Redirect URL after login** field is blank.

Note The redirect URL field must be blank so that it will not override the Cisco Spaces splash URL configured in Layer 3.

Create Access Control Lists for FlexConnect Local Switch Mode

To restrict the Internet access for customers, and to allow access only to Cisco Spaces splash page URL when connected to the SSID, the Cisco Spaces IPs (wall garden ranges) must be configured in the ACL. Now when a customer connects to the SSID, the splash page appears for the customer.

If ACL is not configured with all the required IPs, the system considers the Cisco Spaces as an external URL, and results into multiple redirection for customer.

To create the access control list for the FlexConnect local switch mode, perform the following steps:

Step 1 Log in to the Cisco Wireless Controller with your Wireless Controller credentials.

Step 2 Choose **Security** > **Access Control Lists** > **FlexConnect ACLs**.

Step 3 To add an ACL, click **New**.

Step 4 In the **New** window that appears, enter the following:

a) In the **Access Control List Name** field, enter a name for the new ACL.

Note You can enter up to 32 alphanumeric characters.

b) Click **Apply**.

Step 5 When the **Access Control Lists** window reappears, click the name of the new ACL.

Step 6 In the **Edit** window that appears, click **Add New Rule**.

The **Rules** > **New** window appears.

Step 7 Configure a rule for this ACL with the required wall garden ranges.

To view the wall garden ranges, in the Cisco Spaces dashboard, click the **Configure Manually** link for a CUWN SSID in the **SSIDs** window.”.

When defining the ACL rule, ensure to configure the values as follows:

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

Step 8 If you want to provide social authentication for your portal, you must also configure the wall garden ranges for social authentication. To know the wall garden ranges that you must configure for social authentication, see the “Configuring the Wireless Network for Social Authentication” section.

Note The wall garden ranges configured for social authentication allows the customers to access all the HTTPS web sites directly after connecting to your SSID, without using the captive portal.

Configure the Virtual Interface

To configure the virtual interface, perform the following steps:

Step 1 Choose **Controller** > **Interfaces**.

Step 2 Click the **Virtual** link.

Step 3 In the **Interfaces** > **Edit** window that appears, enter the following parameters:

a) In the **IP address** field, enter the unassigned and unused gateway IP address, if any.

b) In the **DNS Host Name** field, enter the DNS Host Name, if any.

Note Ideally this field must be blank.

Note To ensure connectivity and web authentication, the DNS server must always point to the virtual interface. If a DNS hostname is configured for the virtual interface, then you must configure the same DNS host name on the DNS servers used by the client.

c) Click **Apply**.

Note If you have made any changes to the virtual interface, restart your Cisco Wireless Controller for the changes to take effect.

Configuring Cisco Wireless Controller for Internet Provisioning and RADIUS Authentication

We highly recommend the use of RADIUS authentication for captive portals.

Note The Cisco Spaces cloud RADIUS server only supports PAP for web RADIUS authentication. CHAP is not supported. To avoid client authentication failure, you will need to configure PAP as the web RADIUS authentication method on the Cisco wireless controller.

The following features work only if you configure RADIUS authentication.

- Seamless Internet Provisioning.
- Extended session duration and Internet bandwidth.
- Deny Internet.

Also, for Customer onboarding by captive portal, internet provisioning configuration is required.

To configure radius authentication and seamless internet provisioning, perform the following steps:

Step 1 Log in to Cisco Wireless Controller with your Cisco Wireless Controller credentials.

Step 2 In the **Cisco Wireless Controller** main window, click the **Security** tab.

Step 3 Choose **Radius** > **Authentication**.

The **RADIUS Authentication Servers** window is displayed.

Step 4 From the **Auth Called Station ID Type**e drop-down list, choose **AP MAC Address:SSID**.

Step 5 From the **MAC Delimiter** drop-down list, choose **Hyphen**.

Step 6 Click **New**.

Step 7 In the **New** window that appears, enter the details of the radius server for authentication, such as server IP address, port number, and secret key, select the **Server Status** as **Enabled**, and click **Apply**.

Port Number: 1812

Note You can configure only the Cisco Spaces RADIUS servers.To view the radius server IP address and secret key, in the Cisco Spaces dashboard, click the **Configure Manually** link for a CUWN SSID in the **SSIDs** window. The **Configure Manually** link appears only after adding a Cisco AireOS SSID. Configure both the primary and secondary radius server IPs. You can also contact the Cisco Spaces support team.

Step 8 Choose **Radius** > **Accounting**.

The Radius Accounting Servers window appears.

Note Enabling RADIUS Accounting is not mandatory for Captive Portals. The applicable use cases for Accounting are OpenRoaming and Change of Authorisation (CoA).

Step 9 From **Acct Called Station ID** Type, choose **AP MAC Address:SSID**.

Step 10 From the **MAC Delimiter** drop-down list, choose **Hyphen**.

Step 11 Click **New**.

Step 12 In the New window that appears, enter the details of the radius server for accounting, such as server IP address, port number, and secret key, select the Server Status as **Enabled**, and click **Apply**.

Port Number: 1813

Note You can configure only the Cisco Spaces RADIUS servers. You can configure only the Cisco Spaces RADIUS servers. To view the RADIUS server IP address and secret key, in the Cisco Spaces dashboard, click the "Configure Manually" link for a CUWN SSID in the **SSIDs** window.

Step 13 In the Cisco Wireless Controller main window, click the **WLANs** tab.

Step 14 Click the **WLAN** of the SSID for the Captive Portal rule.

Step 15 Choose **Security**.

Step 16 In the **Layer 2** tab, select the **MAC Filtering** check box.

Step 17 In the **Layer 3** tab, ensure that the following is configured.

In the Layer 3 security drop-down list, Web Policy is selected, and the On Mac Filter Failure radio button is selected.

Note These configurations in the Layer 3 are done when creating the SSIDs.

Step 18 In the AAA Servers tab, in the Radius Servers area, do the following:

a) Select the **Enabled** check box for the Authentication Servers.

a) From the **Server 1** drop-down list, choose the radius server you have previously defined.

Step 19 In the Authentication priority order for the web-auth user area, in the Order Used for Authentication box, set **Radius** as first in the order.

Note Use the Up and Down buttons to rearrange the order.

Step 20 Click the **Advanced** tab, and select the **Enabled** check box for Allow AAA Override.

Step 21 Click **Apply**.

Step 22 In the Cisco Wireless Controller main window, click the **Security** tab.

Step 23 Choose **AAA** > **MAC Filtering**.

Step 24 In the **MAC Filtering** window that appears, do the following:

a) From the **RADIUS Compatibility Mode** drop-down list, choose **Cisco ACS**.

b) From the **MAC Delimiter** drop-down list, choose **Hyphen**.

c) Click **Apply**.

Step 25 Ensure that the wall gardens are configured for the ACLs. To view the wall garden ranges, in the Cisco Spaces dashboard, click the **Configure Manually** link for a CUWN SSID in the **SSIDs** window.The **Configure Manually** link appears only after adding a Cisco AireOS SSID.

Configuring Cisco Wireless Controller for Social Authentication

For social authentication with Cisco Unified Wireless Network, you must do some configurations in the Cisco Wireless Controller.

To configure the Cisco Unified Wireless Network for social authentication, perform the following steps:

Step 1 Log in to Cisco Wireless Controller using your credentials.

Step 2 Choose **Security** > **Access Control Lists** > **Access Control Lists**.

Step 3 In the **Access Control List** window that appears, click the Access Control List configured for Cisco Spaces.

Click **Add New Rule** and add additional two rules with following information. .

No	Action	Source IP Address/Netmask	Destination IP Address/Netmask	Protocol	Source Port Range	Destination Port Range	DSCP	Direction
1	Permit	0.0.0.0/0.0.0.0	0.0.0.0/0.0.0.0	TCP	HTTPS	Any	Any	Any
2	Permit	0.0.0.0/0.0.0.0	0.0.0.0/0.0.0.0	TCP	Any	HTTPS	Any	Any

Note This wall garden ranges configured for social authentication will allow the customers to access all the HTTPS web sites directly after connecting to your SSID, without using the captive portal.

Step 4 Add social platform specific domains as ACLs based on the social networks that you want to use for authentication. To add social domains as ACLs, perform the following steps:

a) In the Cisco Wireless Controller dashboard, choose **Security** > **Access Control Lists**.
b) Click **More Actions** for the Access Control List configured for Cisco Spaces.
c) Click **Add Remove URL**.
d) Enter a social URL name, and click **Add**.
e) Repeat steps **c** and **d** for each domain.

Note These domain names are managed by the social networks and can change at any time. Also, these domain names are subjected to change based on country/region. If you are facing any issue, contact the Cisco Spaces support team.

The commonly used domain names for various social platforms are as follows:

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

- abs.twimg.com
- syndication.twitter.com

- twitter.com
- analytics.twitter.com

Connecting Cisco Catalyst 9800 Series Wireless Controller or Cisco Wireless Controller to Cisco Spaces Using WLC Direct Connect or Cisco Spaces: Connector

To import the locations from Cisco 9800 Series Wireless Controller or Cisco Wireless Controller (without CMX) to Cisco Spaces, you must first connect the Controller to Cisco Spaces through one of the connectors.

The connectors, **Cisco WLC Direct Connect** and **Cisco Spaces Connector** can be used for both Cisco Wireless Controller and Cisco Catalyst 9800 Series Wireless Controller.

Note

- If you want to connect a Cisco Wireless Controller with both Cisco CMX and Cisco Spaces simultaneously, you must use a Cisco Spaces: Connector. However, it is not recommended to connect a single Controller to both Cisco Spaces and Cisco CMX simultaneously.
- It is recommended not to compare the data displayed in Cisco Spaces reports such as Behavior Metrics with the data displayed in Cisco Wireless Controller or Cisco CMX, as it is expected to differ as per design.
- For importing a Controller to Cisco Spaces, ensure that at least one AP is connected to that particular Controller.
- In the Controller, if new APs are added to the Controller, those APs get automatically imported during the next Controller synchronization. If an imported AP is deleted from the Controller, the changes will be reflected in Cisco Spaces only after 48 hours. However, an AP without updates will be deleted after 48 hours only if updates are coming from other APs. For example, if there are 10 APs that are configured, and if 2 APs are removed from Controller, these 2 APs will be removed from Cisco Spaces only when updates are received from other 8 APs.
- If an AP is disassociated from the Controller, it is not immediately removed from Cisco Spaces to release the AP count. The APs will be removed from Cisco Spaces only after 48 hours.

The configurations required for various combinations of Wireless Controllers and Connectors are as follows:

Connecting Cisco Spaces to Cisco Wireless Controller Using Cisco WLC Direct Connect

To connect the Cisco Wireless Controller Version 8.3 or later (without Cisco CMX installation) to the Cisco Spaces, and to import the Cisco Wireless Controller and its access points to the Cisco Spaces, perform the following steps:

Before you begin

- You need Cisco Wireless Controller Version 8.3 or later.
- For importing a Cisco Wireless Controller to Cisco Spaces, ensure that at least one AP is connected to that particular Cisco Wireless Controller.
- The Cisco Wireless Controller must be able to reach Cisco Spaces cloud over HTTPS.
- Cisco Wireless Controller must be able to reach out to the internet.
- To use Cisco Spaces with anchor mode, you must have a network deployment with Cisco Wireless Controllers in both anchor controller mode and foreign controller mode. If the network deployment contains Cisco Wireless Controller in Anchor Controller mode and Foreign Controller mode, Cisco WLC Direct Connect must be enabled in both controllers using the commands described in this section. In addition, the Cisco Wireless Controllers in both modes must be able to reach the Cisco Spaces cloud over HTTPS. However, Cisco Spaces does not support Cisco Wireless Controller Version 8.3.102 in anchor mode.
- To connect the Cisco AireOS Wireless Controller Version 8.3 or later successfully to the Cisco Spaces using Cisco WLC Direct Connect, you must have a root certificate issued by DigiCert CA. If the network deployment contains Cisco Wireless Controller in Anchor Controller mode and Foreign Controller mode, you must import the certificate to the Cisco Wireless Controllers in both modes".

Step 1 Import the DigiCert CA root certificate.

a) Download your root certificate from the following link:

   https://cacerts.digicert.com/DigiCertGlobalRootCA.crt.pem

b) Copy the root certificate content to a file with .cer extension, and save the file as {your_filename}.cer.

c) Copy the **{your_filename}.cer** file to the default directory on your TFTP.

d) Log in to the Cisco Wireless Controller CLI, and execute the following commands:

```
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) Type **Y** to start the upload

f) After the new root certificate has been uploaded successfully, execute the following commands to disable, and then enable your Cisco CMX Cloud Services:

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

Note After uploading the root certificate, Cisco Wireless Controller will prompt for reboot. Rebooting is recommended, but not mandatory. The certificate will be installed in either case.

If you try to connect the Wireless Controller to Cisco Spaces using a root certificate not issued by DigiCert CA, you will get the following error:

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

Step 2 In the Cisco Wireless Controller CLI mode, execute the following commands:

```
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
```

Note To view the {Customer Path Key}, {LB Domain}, {LB IP Address}, and {Customer JWT Token}, log in to Cisco Spaces dashboard, and click the three-line menu icon that is displayed at the top-left of the dashboard. Choose **Setup** > **Wireless Networks**. Then expand **Connect WLC / Catalyst 9800 Directly**, and click **View Token**. Click the **WLC** tab, and you can view the {Customer Path Key}, {LB Domain}, and {LB IP Address} at Step 1b and {Customer JWT Token} at Step 1c.

Step 3 Check the summary using the following command:

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

The result appears.

Now in the Cisco Spaces dashboard, when you choose **CUWN-WLC** in the **Add a Wireless Network** window, the WLC will be listed. So, you can import the APs of that WLC to the Cisco Spaces.

Example:

Sample Result

(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 .... Active

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

Heartbeat Status .... OK

Now the Cisco Wireless Controller will be available for import in the Cisco Spaces location hierarchy. You can import the locations using Map services or Access Point Prefix.

- To import the locations based on Access Point prefix, see Importing the Locations using Access Point Prefix
- To import the locations using Map Services, see Importing Locations to the Location Hierarchy Using Map Services

What to do next

For social authentication, radius authentication, and internet provisioning, refer to the following sections:

- Configuring Cisco Wireless Controller for Internet Provisioning and RADIUS Authentication
- Configuring Cisco Wireless Controller for Internet Provisioning and RADIUS Authentication

Configuring Cisco Wireless Controller (without Cisco CMX) for Notification and Reports

Without Cisco CMX, you can connect Cisco Wireless Controller to Cisco Spaces using the connectors **WLC Direct Connect** and **Cisco Spaces Connector**. In these cases, the configurations required for notifications and reports aredone automatically when you import the Cisco Wireless Controller.

Note If you are using Cisco Spaces with **WLC Direct Connect** or **Cisco Spaces Connector**, the controller must be in **Foreign controller** mode.

Connecting Cisco Spaces to Cisco Catalyst 9800 Series Wireless Controller Using Cisco WLC Direct Connect

Before you begin

- For importing a Cisco Catalyst 9800 Series Wireless Controller to Cisco Spaces, ensure that atleast one AP is connected to that particular Cisco Catalyst 9800 Series Wireless Controller.
- Cisco Catalyst 9800 Series Wireless Controller must be able to reach Cisco Spaces cloud over HTTPS.
- Cisco Catalyst 9800 Series Wireless Controller must be able to reach out to the internet.
- To connect the Cisco Catalyst 9800 Series Wireless Controller successfully to the Cisco Spaces using Cisco WLC Direct Connect, you must have a root certificate trusted by Cisco.

To connect the Cisco Catalyst 9800 Series Controller to Cisco Spaces, and to import that controller and its access points to the Cisco Spaces, perform the following steps:

Step 1 Import the Cisco External Trusted Root Store to install the DigiCert Global Root CA on the Controller.

a) Download the root certificate using the following command:

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

b) verify the certificate installation using the following command:

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

Note You must check the output to verify correct trustpool installation.

Step 2 (Optional) On Cisco Catalyst 9800 Series Controller, enable DNS to resolve the Cisco Spaces URL using the following commands:

```
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>
```

Step 3 Enable nmsp cloud-services on Cisco Catalyst 9800 Series Controller to communicate with Cisco Spaces Cloud over HTTPS.

```
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
```

Note To view the server URL and token, log in to Cisco Spaces dashboard, and click the three-line menu icon that is displayed at the top-left of the dashboard. Choose **Setup > Wireless Networks**. Then expand **Connect WLC / Catalyst 9800 Directly**, and click **View Token**. Click the **Cisco Catalyst 9800** tab, and you can see the URL at Step 2b and token at Step 2c.

Step 4 Confirm the connection between Cisco Catalyst 9800 Series Controller and Cisco Spaces Cloud by executing the following command:

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

The result must be as follows.

Example:

Sample Result

Server : https://abc.dnaspaces.io

CMX Service : Enabled

Connectivity : https: UP

Service Status : Active

Last IP Address : <Local System IP Address>

Last Request Status : HTTP/1.1 200 OK

Heartbeat Status : OK

Now the Cisco Catalyst 9800 Series Wireless Controller will be available for import in the Cisco Spaces location hierarchy.

Note The controller connects to the data.dnaspaces.io URL and not the abc.dnaspaces.io URL.

Step 5 To view the breif summary of active/inactive Cisco CMX cloud connections, execute the following command:

```
#show nmsp status
```

Note You can see the state of the connection to Cisco Spaces Cloud connection.

Step 6 To view aggregated subscriptions summary for all active Cisco Spaces cloud connections, execute the following command:

```
# show nmsp subscription summary
```

Note You can view the services that Cisco Spaces Cloud is subscribed to, after the connection is established.

Step 7 Import the locations to the Cisco Spaces dashboard. For more information on importing the location, see Defining the Location Hierarchy for Cisco Catalyst 9800 Series Wireless Controllers or Cisco Wireless Controller (without Cisco CMX).

Step 8 If you want to use the **Captive Portals** and **Engagements** apps, do the required configuration from the following:

Configuring Cisco Catalyst 9800 Series Wireless Controller (Local Mode) for Captive Portals and Engagements Apps Using CLI

Note The minimum supported Cisco Catalyst 9800 Series Wireless Controller Version is **16.10.20181030**.

To configure Cisco Catalyst 9800 Series Wireless Controller for Captive Portals and Engagements app , perform the following steps:

Step 1 In the Cisco Spaces dashboard, configure a Cisco Catalyst SSID. For more information on configuring the SSIDs, see the "Importing the SSIDs for Cisco Unified Wireless Network" section.

Note You can define any name for the SSID. You must use the same SSID name when configuring the Cisco Catalyst 9800 Series Wireless Controller .

Step 2 On Cisco Catalyst 9800 Series Wireless Controller , enable HTTP and HTTPS as follows:

```
ip http server

ip http secure-server
```

Step 3 Configure parameter maps for client redirection.

```
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
```

Note For Splash URL and IP address, in the Cisco Spaces dashboard, click the **Captive Portal** app. Click **SSIDs**, and then click the **Configure Manually** link for the Cisco Catalyst SSID created in Step 1. The splash URL for your CUWN account will be listed in the **Creating the SSIDs in CUWN-WLC** section. The IP address will be listed in the **Creating the Access Control List** section. You must use only any one IP address from the list. You can also contact the Cisco Spaces support team.

Step 4 Configure virtual IP address for client redirection.

```
parameter-map type webauth global

virtual-ip ipv4 192.0.2.0

intercept-https-enable
```

Note

- Instead of **ipV4** *192.0.2.0*, you can configure any virtual IP. The virtual-ip should be a non-routable and a not used IP address.
- You must have a valid SSL certificate for the virtual IP/Domain installed in Cisco Catalyst 9800 Series Wireless Controller controller.

Step 5 Configure FQDN URL filtering.

For central switch wlans, the URL filter list is attached to the policy-profile:

```
urlfilter list social_login_fqdn_central
action permit
url <splash page domain>
```

Note Configure the domain configured at Step 3 for "redirect for-login".

```
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
```

For flex WLANs the URL filter list is attached to the flex-profile

```
urlfilter list social_login_fqdn_flex
action permit
url <splash page domain>
```

Note Configure the domain configured at Step 3 for "redirect for-login".

```
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"
```

Step 6 Configure Radius server.

```
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>
```

Note You can configure only the Cisco Spaces RADIUS servers. To view the IPv4 IP address, secret key, and port for RADIUS server configuration, in the Cisco Spaces dashboard, click the **Captive Portal** app. Click **SSIDs**, and then click the **Configure Manually** link for the Cisco Catalyst SSID created in Step 1. The radius server details will be listed in the **Radius Server Configuration** section. Configure both the primary and secondary RADIUS server IPs. You can also contact the Cisco Spaces support team.

Step 7 Configure Policy Profile.

```
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
```

Step 8 Configure WLAN.

```
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
```

Note Ensure that the WLAN name you mention here matches with the SSID name you configured in Cisco Spaces at step 1.

Step 9 Enable DNS resolution and make sure you have a default gateway configured on the Cisco Catalyst 9800 Series Wireless Controller .

```
ip name-server <dns_ip_address>
ip domain-lookup
ip route 0.0.0.0 0.0.0.0 <default_gw_ip_addr>
```

You can then import the SSIDs to Cisco Spaces, and configure captive portals for SSIDs using the Captive Portal Rule.

Configuring Cisco Catalyst 9800 Series Wireless Controller GUI (Local Mode) for Captive Portals and Engagements Apps

Note The minimum supported Cisco Catalyst 9800 Series Wireless Controller Versions are 16.10.1E and 16.10.11.

To configure Cisco Catalyst 9800 Series Wireless Controller for Captive Portals and Engagements apps, perform the following steps:

Step 1 In the Cisco Spaces dashboard, configure a Cisco Catalyst SSID. For more information on configuring the SSIDs, see the Importing the SSIDs for Cisco Unified Wireless Network section.

Step 2 Create the Parameter Map:

a) Log into Cisco Catalyst 9800 Series Wireless Controller .
b) Choose **Configuration** > **Security** > **Web Auth**.
c) On the **Web Auth Parameter Map** tab, click **Add**.
d) In the **Parameter-map name** field, enter parameter-map name.
e) From the **Type** drop-down list, choose **consent**, and click **Apply to Device**.

The newly created Parameter Map gets listed on the Web Auth Parameter Map tab.

f) Click the newly created **Parameter Map**.
g) On the **General** tab, check the **Disable Success Window** check box, and the **Disable Logout Window** check box.
h) On the **Advanced** tab, do the following:

- In the **Redirect for log-in** field, enter the splash page URL https://<domain>/p2/<customerPathKey>.
- In the **Redirect Append for AP MAC Address** field, enter ap_mac.
- In the **Redirect Append for Client MAC Address** field, enter client_mac.
- In the **Redirect Append for WLAN SSID** field, enter wlan.
- In the **Portal IPV4 Address** field, enter the Cisco Spaces IP to be allowed.

Note To view the IP address to be allowed, in the Cisco Spaces dashboard, click the **Captive Portals** app. Click **SSIDs**, and then click the **Configure Manually** link for the Cisco Catalyst SSID. The IP addresses will be listed in the Creating the Access Control List section. You must use only any one IP address from the list. The remaining IPs are specified when creating the ACL. The **Configure Manually** link appears only after adding a Cisco Catalyst SSID.

i) Click **Update and Apply**.

Step 3 Install the web-auth certificate and configure the global parameter map.

You must have a valid SSL certificate for the virtual IP/Domain installed in Cisco Catalyst 9800 Series Wireless Controller. You can purchase any wild card certificate.

a) Log into Cisco Catalyst 9800 Series Wireless Controller.
b) In the Cisco Catalyst 9800 Series Wireless Controller dashboard, choose **Configuration** > **Security** > **Web Auth**.

c) Click the Parameter map name, **global**.
d) Configure **Maximum Http connections** as **100**
e) Configure **Init-State Timeout(Secs)** as **120**
f) On the **General** tab, from the **Type** drop-down list, choose **Webauth**.
g) Specify virtual IPv4 address (virtual IP) or virtual IPv4 Host name (domain) in the respective field.
h) Configure **Watch List Expiry Timeout(Secs)** as **600**.
i) Check the **Web Auth intercept HTTPS** check box.
j) Click **Update & Apply**.
k) Convert the certificate into pkcs12.

   The file format will be .p12.

l) Copy the file into the tftp server.
m) Download the certificate copied to the tftp server using the following steps:

   - In the Cisco Catalyst 9800 Series Wireless Controller CLI, enter the following command:

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

   - To confirm the **tftp** server IP, enter **yes**.
   - Enter the certificate file name. For example, wildcard.wifi-mx.com.p12.

     The certificate gets downloaded.

n) To verify the installed certificate, in the Cisco Catalyst 9800 Series Wireless Controller dashboard, choose **Configuration** > **Web Auth** > **Certificate**.

   The downloaded certificate appears as the last certificate in the list.

o) To map the installed certificate with webauth parameter map, in the Cisco Catalyst 9800 Series Wireless Controller CLI, execute the following commands:

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

   Reload Cisco Catalyst 9800 Series Wireless Controller .

Step 4 Create the ACL by adding URL filters.

a) Choose **Configuration** > **Security** > **URL Filter**.
b) In the **URL Filters** window, click **Add**.
c) In the **List Name** field, enter the list name.
d) Change the status of **Action** to **Permit**
e) In the **URLs** field, enter the splash page domain configured at Step 2h (Parameter Map).

   Add the following domains, if you want to enable social authentication:

   - *.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) Choose **Configuration** > **Tags and Profiles** > **Policy**.
g) In the **Policy Profile** window, click **default-policy-profile.**
h) In the **Edit Policy Profile** window, click the **Access Policies** tab.
i) In the **URL Filters** area, from the **Pre Auth** drop-down list, choose the previously created ACL.
j) Click **Update & Apply to Device** .

Step 5 Create the SSID.

a) Choose **Configuration** > **Tags and Profiles** > **WLANs**.
b) Click **Add**.
a) On the **General** tab, in the **Profile Name** field, enter the profile name.
b) In the **SSID** field, enter the SSID name defined at Step 1.
c) Set the status as **Enabled**.
d) Click the **Security** tab, and then click the **Layer2** tab.
e) From the **Layer 2 Security Mode** drop-down list, choose **None**.
f) Click the **Layer3** tab.
g) Check the **Web Policy** check box.
h) From the **WebAuth Parameter Map** drop-down list, choose the Web Auth Parameter Map created at step 2.
i) Click **Save & Apply to Device**.

Step 6 Configure the RADIUS server.

Note We highly recommend to use RADIUS authentication for captive portals. The following features work only if you configure RADIUS authentication.

- Seamless Internet Provisioning.
- Extended session duration.
- Deny Internet.

a) Choose **Configuration** > **Security** > **AAA**.

b) In the **Authentication Authorization and Accounting** window, click the **Servers/Groups** tab.

c) Choose **Radius** > **Servers**, and click **Add**.

d) In the **Name** field, enter a name for the radius server.

e) In the **IPv4 / IPv6 Server Address** field, enter the radius server address.

Note You can configure only the Cisco Spaces RADIUS servers. To view the radius server IP address and secret key, in the Cisco Spaces dashboard, click the **Captive Portal** app. Click **SSIDs**, and then click the **Configure Manually** link for the Cisco Catalyst SSID created at Step 1.In the window that appears, the radius server details will be listed in the **Radius Server Configuration** section. Configure both the primary and secondary RADIUS server IPs.You can also contact the Cisco Spaces support team.

f) In the **Key** field, enter the key, and confirm it in the **Confirm Key** field.

g) In the **Auth Port** field, enter 1812.

h) In the **Acct Port** field, enter 1813.

i) Click **Save & Apply to Device**.

The server added will be available in **Servers** list.

j) Choose **Radius** > **Server Groups**, and click **Add**.

k) In the **Name** field, enter a name.

l) From the **MAC-Delimiter** drop-down list, choose **hyphen**.

m) From the **MAC-Filtering** drop-down list, choose **mac**.

n) Move the radius server previously created from “Available Servers” to “Assigned Servers” using the arrow button.

o) Click **Save & Apply to Device**.

p) In the **Authentication Authorization and Accounting** window, click the **AAA Method List** tab.

q) Click **Authentication**, and click **Add** and specify the following details:

1. In the **Method List Name** field, enter the method list name.
2. From the **Type** drop-down list, choose **Login**
3. From the **Group Type** drop-down list, choose **Group**.
4. Move the server group created earlier (step j to Step o) from **Available Server Groups** to **Assigned Servers Groups**, and click **Save & Apply to Device**.

r) On the **AAA Method List** tab, click **Authorization**, and click **Add**, and specify the following details:

1. In the **Method List Name** field, enter the method list name.
2. From the **Type** drop-down list, choose **Network**.
3. From the **Group Type** drop-down list, choose **group**.
4. Move the server group previously created (step j to Step o) from **Available Servers** to **Assigned Servers** using the arrow button, and click **Save & Apply to Device**.

s) On the **AAA Method List** tab, click **Accounting**, and click **Add**, and specify the following details:

1. In the **Method List Name** field, enter the method list name.
2. From the **Type** drop-down list, choose **Identity**.
3. From the **Group Type** drop-down list, choose **group**.

4. Move the server group previously created (step j to Step o) from **Available Servers** to **Assigned Servers** using the arrow button, and click **Save & Apply to Device**.

Step 7 Enable L3 and L2 authentication (Mac Filtering).

Make sure **Type** is selected as **webauth** in parameter-map for RADIUS Authentication.

Note To configure L3 and L2 authentication, ensure that you have created the SSIDs and have done all the configurations at step 5. You can then import the SSIDs to Cisco Spaces, and configure captive portals for SSIDs using the Captive Portal Rule.

a) Choose **Configuration** > **Tags and Profiles** > **WLANs**.
b) Click the SSID for which you want to configure L2 and L3 Authentication.
c) In the **Edit WLAN** window, click the **Security** tab.
d) On the **Layer3** tab, from the **Authentication** drop-down list, choose the radius authentication configured previously(step 6q).
e) On the **Layer2** tab, to enable Mac Filtering, check the **MAC Filtering** check box.
f) From the **Authorization List** drop-down list that appears, choose the authorization server created previously(step 6r).
g) Click **Show Advanced Settings**.
h) Check the **On Mac Filter Failure** check box.
i) Click **Update & Apply to Device**.
j) Choose **Configuration** > **Tags and Profiles** > **Policy**.
k) Click **default-policy-profile**.
l) On the **Advanced** tab, in the **AAA Policy** area, check the **Allow AAA Override** check box.
m) Ensure that default **aaa** policy is selected from the **Policy Name** drop-down list.
n) Click **Update & Apply to Device**.

Configuring Cisco Catalyst 9800 Series Wireless Controller GUI (Flex Mode or Mobility Express) for Captive Portals and Engagements Apps

Note The minimum supported Cisco Catalyst 9800 Series Wireless Controller Versions are 16.10.1E and 16.10.11.

To configure "Cisco Catalyst 9800 Series Wireless Controller in Flex mode" or "Cisco Catalyst 9800 Series Wireless Controller with Mobility Express" for Captive Portals and Engagements apps, perform the following steps:

Step 1 To configure the Cisco Catalyst 9800 Series Wireless Controller in Flex mode, ensure that the following configurations are done:

This configuration is not required for Mobility Express.

a) Log into Cisco Catalyst 9800 Series Wireless Controller .
b) Choose **Configuration** > **Tags** > **Site.**
c) Select the required site name.
d) Uncheck the **Enable Local Site** check box.

e) Click **Update & Apply to Device.**
f) Choose **Configuration** > **Policy**.
g) Select the required policy name.
h) Disable **Central Switching**.
i) Click **Update & Apply to Device.**.

Note AP might reboot and rejoin the wireless controller on changing from **Local Mode** to **Flex mode**.

Step 2 In the Cisco Spaces dashboard, configure a Cisco Catalyst SSID. For more information on configuring the SSIDs, see the Importing the SSIDs for Cisco Unified Wireless Network section.

Step 3 Create the Parameter Map:

a) Log into Cisco Catalyst 9800 Series Wireless Controller .
b) Choose **Configuration** > **Security** > **Web Auth**.
c) On the **Web Auth Parameter Map** tab, click **Add**.
d) In the **Parameter-map name** field, enter parameter-map name.
e) From the **Type** drop-down list, choose **consent**, and click **Apply to Device**.

The newly created Parameter Map gets listed on the **Web Auth Parameter Map** tab.

f) Click the newly created **Parameter Map**.
g) On the **General** tab, check the **Disable Success Window** check box, and the **Disable Logout Window** check box.
h) On the **Advanced** tab, do the following:

- In the **Redirect for log-in** field, enter the splash page URL https://<domain>/p2/<customerPathKey>.
- In the **Redirect Append for AP MAC Address** field, enter ap_mac.
- In the **Redirect Append for Client MAC Address** field, enter client_mac.
- In the **Redirect Append for WLAN SSID** field, enter wlan.
- In the **Portal IPV4 Address** field, enter the Cisco Spaces IP to be allowed.

Note To view the IP address to be allowed, in the Cisco Spaces dashboard, click the **Captive Portals** app. Click **SSIDs**, and then click the **Configure Manually** link for the CUWN/Catalyst SSID. The IP addresses will be listed in the **Creating the Access Control List** section. You must use only any one IP address from the list. The remaining IPs are specified when creating the ACL. The **Configure Manually** link appears only after adding a Cisco Catalyst SSID.

i) Click **Update and Apply**.

Step 4 Install the web-auth certificate and configure the global parameter map.

You must have a valid SSL certificate for the virtual IP/Domain installed in Cisco Catalyst 9800 Series Wireless Controller. You can purchase any wild card certificate.

a) Log into Cisco Catalyst 9800 Series Wireless Controller.
b) In the Cisco Catalyst 9800 Series Wireless Controller dashboard, choose **Configuration** > **Security** > **Web Auth**.
c) Click the Parameter map name, **global**.
d) Configure **Maximum Http connections** as **100**
e) Configure **Init-State Timeout(Secs)** as **120**
f) On the **General** tab, from the **Type** drop-down list, choose **Webauth**.
g) Specify virtual IPv4 address (virtual IP) or virtual IPv4 Host name (domain) in the respective field.
h) Configure **Watch List Expiry Timeout(Secs)** as **600**.

i) Check the **Web Auth intercept HTTPS** check box.

j) Click **Update & Apply**.

k) Convert the certificate into pkcs12.

The file format will be .p12.

l) Copy the file into the tftp server.

m) Download the certificate from the tftp server using the following steps:

- In the Cisco Catalyst 9800 Series Wireless Controller CLI, enter the following command:

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

- To confirm the **tftp** server IP, enter **yes**.
- Enter the certificate file name. For example, wildcard.wifi-mx.com.p12.

  The certificate gets downloaded.

n) To verify the installed certificate, in the Cisco Catalyst 9800 Series Wireless Controller dashboard, choose **Configuration** > **Web Auth** > **Certificate**.

The downloaded certificate appears as the last certificate in the list.

o) To map the installed certificate with webauth parameter map, in the Cisco Catalyst 9800 Series Wireless Controller CLI, execute the following commands:

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

Reload Cisco Catalyst 9800 Series Wireless Controller .

Step 5 Create the ACL by adding URL filters.

a) Choose **Configuration** > **Security** > **URL Filter**.

b) In the **URL Filters** window, click **Add**.

c) In the **List Name** field, enter the list name.

d) Change the status of **Action** to **Permit**

e) In the **URLs** field, enter the splash page domain configured at Step 3h (Parameter Map).

Add the following domains, if you want to enable social authentication:

- *.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) Choose **Configuration** > **Tags and Profiles** > **Policy**.
g) In the **Policy Profile** window, click **default-policy-profile.**
h) In the **Edit Policy Profile** window, click the **Access Policies** tab.
i) In the **URL Filters** area, from the **Pre Auth** drop-down list, choose the previously created ACL.
j) Click **Update & Apply to Device** .
k) Choose **Configuration** > **Tags and Profiles** > **Flex**.
l) Click the Profile in use.
m) In the **Edit Flex Profile** window that appears, click **Policy ACL** tab.
n) Click **Add**.
o) From the **ACL Name** drop-down list, choose **WA-sec-<ip>**.
p) From the **Pre Auth URL Filter** drop-down list, choose URL filter ACL created previously(Step 5a to 5e).
q) Click **Save**.
r) Click **Update & Apply to Device**.

Step 6 Create the SSID.

a) Choose **Configuration** > **Tags and Profiles** > **WLANs**.
b) Click **Add**.

a) On the **General** tab, in the **Profile Name** field, enter the profile name.
b) In the **SSID** field, enter the SSID name defined at Step 2.
c) Set the status as **Enabled**.
d) Click the **Security** tab, and then click the **Layer2** tab.
e) From the **Layer 2 Security Mode** drop-down list, choose **None**.
f) Click the **Layer3** tab.
g) Check the **Web Policy** check box.
h) From the **WebAuth Parameter Map** drop-down list, choose the Web Auth Parameter Map created at step 3.
i) Click **Save & Apply to Device**.

Step 7 Configure the RADIUS server.

Note We highly recommend to use RADIUS authentication for captive portals. The following features work only if you configure RADIUS authentication.

- Seamless Internet Provisioning.
- Extended session duration.
- Deny Internet.

a) Choose **Configuration** > **Security** > **AAA**.
b) In the **Authentication Authorization and Accounting** window, click the **Servers/Groups** tab.
c) Choose **Radius** > **Servers**, and click **Add**.
d) In the **Name** field, enter a name for the radius server.
e) In the **IPv4 / IPv6 Server Address** field, enter the radius server address.

Note You can configure only the Cisco Spaces RADIUS servers. To view the RADIUS server IP address and secret key, in the Cisco Spaces dashboard, click the **Captive Portal** app. Click **SSIDs**, and then click the **Configure Manually** link for the Cisco Catalyst SSID created at Step 2. In the window that appears, the RADIUS server details will be listed in the **Radius Server Configuration** section. Configure both the primary and secondary RADIUS server IPs.You can also contact the Cisco Spaces support team.

f) In the **Key** field, enter the key, and confirm it in the **Confirm Key** field.
g) In the **Auth Port** field, enter 1812.
h) In the **Acct Port** field, enter 1813.
i) Click **Save & Apply to Device**.

The server added will be available in **Servers** list.

j) Choose **Radius** > **Server Groups**, and click **Add**.
k) In the **Name** field, enter a name.
l) From the **MAC-Delimiter** drop-down list, choose **hyphen**.
m) From the **MAC-Filtering** drop-down list, choose **mac**.
n) Move the radius server previously created from “Available Servers” to “Assigned Servers” using the arrow button.
o) Click **Save & Apply to Device**.
p) In the **Authentication Authorization and Accounting** window, click the **AAA Method List** tab.
q) Click **Authentication**, and click **Add** and specify the following details:

1. In the **Method List Name** field, enter the method list name.
2. From the **Type** drop-down list, choose **Login**
3. From the **Group Type** drop-down list, choose **Group**.
4. Move the server group created earlier (step j to Step o) from **Available Server Groups** to **Assigned Servers Groups**, and click **Save & Apply to Device**.

r) On the **AAA Method List** tab, click **Authorization**, and click **Add**, and specify the following details:

1. In the **Method List Name** field, enter the method list name.
2. From the **Type** drop-down list, choose **Network**.
3. From the **Group Type** drop-down list, choose **group**.
4. Move the server group previously created (step j to Step o) from **Available Servers** to **Assigned Servers** using the arrow button, and click **Save & Apply to Device**.

s) On the **AAA Method List** tab, click **Accounting**, and click **Add**, and specify the following details:

1. In the **Method List Name** field, enter the method list name.
2. From the **Type** drop-down list, choose **Identity**.
3. From the **Group Type** drop-down list, choose **group**.
4. Move the server group previously created (step j to Step o) from **Available Servers** to **Assigned Servers** using the arrow button, and click **Save & Apply to Device**.

Step 8 Enable L3 and L2 authentication (Mac Filtering).

Make sure **Type** is selected as **webauth** in parameter-map for RADIUS Authentication.

Note To configure L3 and L2 authentication, ensure that you have created the SSIDs and have done all the configurations at step 6. You can then import the SSIDs to Cisco Spaces

Step 9 , and configure captive portals for SSIDs using the Captive Portal Rule.

a) Choose **Configuration** > **Tags and Profiles** > **WLANs**.
b) Click the SSID for which you want to configure L2 and L3 Authentication.
c) In the **Edit WLAN** window, click the **Security** tab.
d) On the **Layer3** tab, from the **Authentication** drop-down list, choose the radius authentication configured previously(step 7q).
e) On the **Layer2** tab, to enable Mac Filtering, check the **MAC Filtering** check box.
f) From the **Authorization List** drop-down list that appears, choose the authorization server created previously(step 7r).
g) Click **Show Advanced Settings**.
h) Check the **On Mac Filter Failure** check box.
i) Click **Update & Apply to Device**.
j) Choose **Configuration** > **Tags and Profiles** > **Policy**.
k) Click **default-policy-profile**.
l) On the **Advanced** tab, in the **AAA Policy** area, check the **Allow AAA Override** check box.
m) Ensure that default **aaa** policy is selected from the **Policy Name** drop-down list.
n) Click **Update & Apply to Device**.

Connecting Cisco Spaces to Cisco AireOS Wireless Controller or Cisco Catalyst 9800 Series Wireless Controller using Cisco Spaces: Connector

Cisco Wireless Controller with Cisco DNA Spaces Connector

To connect Cisco AireOS Wireless Controller to Cisco Spaces using a Cisco Spaces: Connector, and to configure captive portal authentication or notifications, do the following:

- Connect Cisco AireOS Wireless Controller to Cisco Spaces using a Cisco Spaces: Connector refering the procedure mentioned in Cisco DNA Spaces: Connector Configuration Guide
- After connecting Cisco AireOS Controller to Cisco Spaces, configure RADIUS authentication and internet provisioning as described in Configuring Cisco Wireless Controller for Internet Provisioning and RADIUS Authentication.

- If Captive Portal Authentication is required, import SSIDs, create captive portal with the required authentication type, and configure Captive Portal rule based on the procedure mentioned in chapter Cisco Spaces: Captive Portal App
- If social authentication is required for captive portal, configure social authentication as described in Configuring Cisco Wireless Controller for Social Authentication, on page 15
- If you want to send notifications using Cisco Spaces, configure the engagement rules based on the procedure mentioned in chapter Cisco Spaces: Engagements App

Cisco Catalyst 9800 Series Wireless Controller with Cisco DNA Spaces Connector

To connect Cisco Catalyst 9800 Series Wireless Controller to Cisco Spaces using a Cisco Spaces: Connector, and to configure captive portal authentication or notifications, do the following:

- To connect Cisco Catalyst 9800 Series Wireless Controller to Cisco Spaces using a Cisco Spaces: Connector, see Cisco DNA Spaces: Connector Configuration Guide"
- After connecting Cisco Catalyst 9800 Series Wireless Controller to Cisco Spaces, for social authentication, RADIUS authentication, and internet provisioning (for using the **Captive Portals** app and **Engagements** app), see the following:
  - Configuring Cisco Catalyst 9800 Series Wireless Controller (Local Mode) for Captive Portals and Engagements Apps Using CLI , on page 22
  - Configuring Cisco Catalyst 9800 Series Wireless Controller GUI (Local Mode) for Captive Portals and Engagements Apps, on page 26
  - Configuring Cisco Catalyst 9800 Series Wireless Controller GUI (Flex Mode or Mobility Express) for Captive Portals and Engagements Apps, on page 30.
- To configure Captive Portal Authentication, import SSIDs, create captive portal with the required authentication type, and configure Captive Portal rule based on the procedure mentioned in chapter Cisco Spaces: Captive Portal App
- If you want to send notifications using Cisco Spaces, configure the engagement rules based on the procedure mentioned in chapter Cisco Spaces: Engagements App

Configuring Mobility Express to work with Cisco Spaces

This section describes the configurations to be done in the Mobility Express Controller for using Cisco Spaces.

The configurations required for various Mobility Express versions are different. The configurations for various Mobility Express versions are as follows:

Configuring Mobility Express 8.7 or Later for Cisco Spaces

To configure the Mobility Express 8.7 or later for Cisco Spaces, perform the following steps:

Creating SSIDs in the Mobility Express

To create SSIDs in the Mobility Express, perform the following steps:

Step 1 Log in to **Mobility Express** with your credentials.

Step 2 In the main window, click **Wireless Settings** in the left pane.

Step 3 Click **WLANs**.

Step 4 To create a WLAN, click **Add new WLAN/RLAN**.

Step 5 In the window that appears, in the **General** tab, enter the WLAN details like Type, Profile Name, SSID, and so on.

Step 6 Click **Apply**.

The **Add new WLAN/RLAN** window appears.

Step 7 Click **WLAN Security**.

Step 8 Enable the **Guest Network** toggle switch.

Step 9 Enable the **Captive Network Assistant** toggle switch.

Step 10 From the Captive Portal drop-down list, choose **External Splash Page**.

Step 11 From the Access Type drop-down list, choose **Web Consent**.

Step 12 In the Captive Portal URL field that appears, enter the Cisco Spaces splash URL.

To view the splash URL for your ME account, in the Cisco Spaces dashboard, click the **Configure Manually** link for a CUWN SSID in the **SSIDs** window.

Step 13 Click **Apply**.

Step 14 To enable and broadcast the SSID, in the **General** tab, from the Admin drop-down list, choose “Enabled”, and enable the “Broadcast SSID” toggle switch.

Step 15 Execute the following command in the command prompt to disable the secure webauth mode. Then, restart the ME.

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

Step 16 Execute the following command in the command prompt to change the webauth login success page from **Default** to **None**.

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

Configuring RADIUS Authentication in Mobility Express 8.7 or Later

To configure radius authentication in the Mobility Express 8.7 or later, perform the following steps:

Step 1 Log in to **Mobility Express** with your credentials.

Step 2 In the ME main window, click **Switch to Expert View** in the top right of the window.

Step 3 In the pop up window that appears, select **OK**.

Step 4 In the left pane, click **Management > Admin Accounts**.

Step 5 In the window that appears, click the **Radius** tab.

Step 6 Click **Add RADIUS Authentication Server**.

In the **Add/ Edit Radius Authentication Server** window appears, enter the following radius server details:

a) In the **Server IP Address** field, enter the IP address of the radius server.
b) In the **Shared Secret** field, enter your radius secret key.
c) In the **Confirm Shared Secret** field, re-enter the radius secret key.

Note You can configure only the Cisco Spaces RADIUS servers. To view the IP address and secret key for radius server configuration, in the Cisco Spaces dashboard, click the **Captive Portal** app. Click **SSIDs**, and then click the **Configure Manually** link for a Cisco Unified Wireless Network (Cisco AireOS) SSID. Click the **Configure SSID in CUWN-WLC** tab. The RADIUS server details will be listed in the **Radius Server Configuration** section. Configure both the primary and secondary RADIUS server IPs.You can also contact the Cisco Spaces support team.

Step 7 Click **Apply**.

Step 8 In the **Mobility Express** main window, click **Wireless Settings** in the left pane.

Step 9 Click **WLANs** .

The **WLAN/RLAN Configuration** window appears with the SSIDs list.

Step 10 Click the **Edit** icon for the SSID created previously.

Step 11 In the **Edit WLAN** window that appears, click the **WLAN Security** tab.

Step 12 From the **Access Type** drop-down list, choose **Radius**.

Step 13 Click the Radius Server tab, and click **Add RADIUS Authentication Server**.

Step 14 From the **Server IP Address** drop-down list, select your Radius Server, and click **Apply**.

Step 15 In the **Edit WLAN** window, click **Apply**.

Now the Mobility Express 8.7 or later is configured for radius server authentication.

Creating Access Control Lists in Mobility Express 8.7 or Later

To create Access Control Lists in the Mobility Express 8.7 or later, perform the following steps:

Step 1 Log in to **Mobility Express** with your credentials.

Step 2 In the **Mobility Express** main window, click the Wireless Settings in the left pane.

Step 3 Click **WLANs**.

The WLAN/RLAN Configuration window appears with the SSIDs list.

Step 4 Click the **Edit** icon for the SSID created previously.

In the **Edit WLAN** window that appears, click the **WLAN Security** tab.

Step 5 Click the **Pre Auth ACLs** tab.

Step 6 Click **Add IP Rules**.

Step 7 In the Add/Edit IP ACLs, create rules with the following configuration:

Action	Source IP Address/Netmask	Destination IP Address/Netmask	Protocol	Source Port Range	Dest Port Range	DSCP
Permit	34.235.248.212/255.255.255.255	0.0.0.0/0.0.0.0	Any	Any	Any	Any
Permit	0.0.0.0/0.0.0.0	34.235.248.212/255.255.255.255	Any	Any	Any	Any
Permit	52.55.235.39/255.255.255.255	0.0.0.0/0.0.0.0	Any	Any	Any	Any
Permit	0.0.0.0/0.0.0.0	52.55.235.39/255.255.255.255	Any	Any	Any	Any

Note For EU region, `34.235.248.212, 52.55.235.39` must be replaced with `54.77.207.183,34.252.175.120`.

When defining the ACL rule, ensure to configure the values as follows:

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

Step 8 Click **Apply**.

Configuring Mobility Express 8.7 or Later for Social Authentication

To configure the Mobility Express for Social Sign authentication for captive portals, perform the following steps:

Step 1 Log in to Mobility Express with your credentials.

Step 2 In the **Mobility Express** main window, click the **Wireless Settings** in the left pane.

Step 3 Click **WLANs**.

The **WLAN/RLAN Configuration** window appears with the SSIDs list.

Step 4 Click the **Edit** icon for the SSID created previously.

In the **Edit WLAN** window that appears, click the **WLAN Security** tab.

Step 5 Click the **Pre Auth ACLs** tab.

Step 6 Click **Add IP Rules**.

Step 7 In the Add/Edit IP ACLs, configure the following two rules in addition to the existing ACL rules:

Action	Source IP Address/Netmask	Destination IP Address/Netmask	Protocol	Source Port Range	Dest Port Range	DSCP
Permit	0.0.0.0/0.0.0.0	0.0.0.0/0.0.0.0	TCP	HTTPs	Any	Any
Permit	0.0.0.0/0.0.0.0	0.0.0.0/0.0.0.0	TCP	Any	HTTPS	Any

Allowing the URLs in the Mobility Express 8.7 or Later

To allow a URL in the Mobility Express 8.7 or later, perform the following steps:

Step 1 Log in to **ME** with your credentials.

Step 2 In the **ME** main window, click the **Wireless Settings** in the left pane.

Step 3 Click **WLANs**.

The **WLAN/RLAN Configuration** window appears with the SSIDs list.

Step 4 Click the **Edit** icon for the SSID created previously.

Step 5 In the **Edit WLAN** window that appears, click the **WLAN Security** tab.

Step 6 Click the **Pre Auth ACLs** tab.

Step 7 Click **Add URL Rules**.

Step 8 In the **Add/Edit URL ACLs** window that appears, configure the URL that you want to include in the allowed list.

When defining the URL rule, ensure to configure the values as follows:

- **URL**: domain
- **Action**: Permit

Step 9 Click **Update**.

Configuring Mobility Express for Notifications and Reports

If you are using Mobility Express with WLC connect, to configure for location updates, perform the following steps:

Step 1 In the **Cisco Wireless Controller CLI**, execute the following commands:

a. config cloud-services cmx disable

b. config cloud-services server url https://{Customer Path Key}.{LB Domain} {LB IP Address}

c. config cloud-services server id-token {Customer JWT Token}

d. config network dns serverip <dns server ip>

e. config cloud-services cmx enable

Note To view the {Customer Path Key}, {LB Domain}, {LB IP Address}, and {Customer JWT Token}, in the Cisco Spaces dashboard, click the **Configure Manually** link for a CUWN SSID in SSIDs window. You can also contact the Cisco Spaces support team. Ensure that there are no trailing or leading spaces.

Step 2 Check the summary using the following command:

show cloud-services cmx summary

The result appears.

Now in the Cisco Spaces dashboard, when you choose **CUWN-WLC** in the **Add a Wireless Network** window, the WLC will be listed. So, you can import the APs of that WLC to the Cisco Spaces.

Sample Result

```
(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 .............................. Active
```

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

Heartbeat Status ............................. OK
```

What to do next

Now the Cisco Wireless Controller will be available for importing to the CiscoCisco Spaces location hierarchy. For more information on importing the Cisco Wireless Controller and its access points, follow from Step 4 of the procedure mentioned in Connecting Cisco Spaces to Cisco Wireless Controller Using Cisco WLC Direct Connect , on page 17.

Configuring Mobility Express 8.6 or Earlier for Cisco Spaces

To configure Mobility Express 8.6 or earlier for Cisco Spaces:

Creating SSIDs in Mobility Express 8.6 or Earlier

The steps to create SSIDs in Mobility Express 8.6 or earlier are same as that for Mobility Express 8.7 or later. To know the configuration steps, see the Creating SSIDs in the Mobility Express, on page 36.

Configuring RADIUS Authentication for Mobility Express 8.6 or Earlier

In Mobility Express 8.6 or earlier, you cannot configure RADIUS servers individually.

To configure Mobility Express 8.6 or earlier for RADIUS authentication, perform the following steps:

Step 1 Log in to **Mobility Express** with your credentials.

Step 2 In the **Mobility Express** main window, click **Wireless Settings** in the left pane.

Step 3 Click **WLANs**.

The **WLAN/RLAN Configuration** window appears with the SSIDs list.

Step 4 Click the **Edit** icon for the SSID created previously.

Step 5 In the **Edit WLAN** window that appears, click the WLAN Security tab.

Step 6 From the **Access Type** drop-down list, choose **Radius**.

Step 7 To add the radius server, click **Add**.

Step 8 In the window that appears, enter the following radius server details:

a. In the **Server IP Address** field, enter the IP address of the radius server.

b. In the **Shared Secret** field, enter your radius secret key.

c. In the **Confirm Shared Secret** field, re-enter the radius secret key.

d. Click **Apply**.

Note You can configure only the Cisco Spaces RADIUS servers. To view the IP address and secret key for radius server configuration, in the Cisco Spaces dashboard, click the **Captive Portal** app. Click **SSIDs**, and then click the **Configure Manually** link for a Cisco Unified Wireless Network (Cisco AireOS) SSID. Click the **Configure SSID in CUWN-WLC** tab. The RADIUS server details will be listed in the **Radius Server Configuration** section. Configure both the primary and secondary RADIUS server IPs.You can also contact the Cisco Spaces support team.

Step 9 In the **Edit WLAN** window, click **Apply**.

Now, the Mobility Express is configured for radius server authentication of Cisco Spaces captive portals.

Creating ACLs for Mobility Express 8.6 or Earlier

Mobility Express 8.6 or earlier does not provide user interface to configure Access Control Lists. So for creating ACLs, and configuring social authentication, you must use the command prompt. For the commands to use for these ACL configurations, see the “ Mobility Express Command Reference Guide”.

Now the Cisco Wireless Controller will be available for import in Cisco Spaces location hierarchy. For more information on importing the Cisco Wireless Controller and access points to the Cisco Wireless Controller, follow from Step 3 of the procedure mentioned in Connecting Cisco Spaces to Cisco Wireless Controller Using Cisco WLC Direct Connect , on page 17.

Configuring Mobility Express for Notifications and Reports

If you are using Mobility Express with WLC connect, to configure for location updates, perform the following steps:

Step 1 In the **Cisco Wireless Controller CLI**, execute the following commands:

a. config cloud-services cmx disable

b. config cloud-services server url https://{Customer Path Key}.{LB Domain} {LB IP Address}

c. config cloud-services server id-token {Customer JWT Token}

d. config network dns serverip <dns server ip>

e. config cloud-services cmx enable

Note To view the {Customer Path Key}, {LB Domain}, {LB IP Address}, and {Customer JWT Token}, in the Cisco Spaces dashboard, click the **Configure Manually** link for a CUWN SSID in SSIDs window. You can also contact the Cisco Spaces support team. Ensure that there are no trailing or leading spaces.

Step 2 Check the summary using the following command:

show cloud-services cmx summary

The result appears.

Now in the Cisco Spaces dashboard, when you choose **CUWN-WLC** in the **Add a Wireless Network** window, the WLC will be listed. So, you can import the APs of that WLC to the Cisco Spaces.

Sample Result

(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 .... Active

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

Heartbeat Status .... OK

What to do next

Now the Cisco Wireless Controller will be available for importing to the CiscoCisco Spaces location hierarchy. For more information on importing the Cisco Wireless Controller and its access points, follow from Step 4 of the procedure mentioned in Connecting Cisco Spaces to Cisco Wireless Controller Using Cisco WLC Direct Connect , on page 17.

Configuring Aironet 4800 Series Mobility Express Controller 8.10.150.0 for Cisco Spaces

To configure AireOS 4800 Series Mobility Express Controller 8.10.150.0 for Cisco Spaces:

Configuring Mobility Express 8.10.150.0

To configure Mobility Express 8.10.105.0 for Cisco Spaces, perform the following steps:

Step 1 Log in to **Mobility Express** with your credentials.

Step 2 Go to **Advanced** > **Security Settings**.

Step 3 Click **Add New ACL**.

Step 4 In the **Add ACL Rule** window, enter the ACL details:

a) From the **ACL Type** drop-down list, choose **IPv4**.

b) In the **ACL** name field, enter a name for the ACL.

c) Click **Add URL Rules**.

The **Add /Edit URL ACLs** window appears.

d) In the **URL** field, enter splash page URL domain.

e) From the **Action** drop-down list, choose **Permit**.

f) To enable social authentication, add the following domains in the ACL:

- *.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

This step is required only of you want to enable social authentication.

g) Click **Update**.

Step 5 To add radius server configuration, perform the following steps:

a) Create an ACL.
b) Enable **Expert** view.
c) Go to **Managenent** > **Admin Accounts** > **Radius**
d) From the **Authentication Call Station ID Type** drop-down list, choose **AP MAC Address:SSID**.
e) From the **Authentication MAC Delimiter** drop-down list, choose **Hyphen**.
f) From the **Accounting Call Station ID Type** drop-down list, choose **AP MAC Address:SSID**.
g) From the **Accounting MAC Delimiter** drop-down list, choose **Hyphen**.
h) From the **Fallback Mode** drop-down list, choose **Off**.
i) Click **Apply**.

Step 6 Click **Add Radius Authentication Server**, and in the **Add/Edit Radius Authentication Server** that appears, enter the following details:

a) Disable **CoA**.
b) In the **Server Ip Address** field, enter the radius server IP address.
c) In the **Shared Secret** field, enter the secret key.
d) In the **Confirm Shared Secret** field, enter the secret key to confirm
e) Click **Apply**.

Added radius server will be listed under the Radius Servers list.

Note You can configure only the Cisco Spaces RADIUS servers. To view the IP address and secret key for the radius server configuration, in the Cisco Spaces dashboard, click the **Captive Portals**app. Click **SSIDs**, and then click the **Configure Manually** link for a Cisco Unified Wireless Network (Cisco AireOS) SSID. The RADIUS server details will be listed in the RADIUS Server Configuration section. Configure both the primary and secondary RADIUS server IPs. You can also contact the Cisco Spaces support team.

Step 7 To configure **WLAN** for radius server, perform the following steps:

a) In the Cisco Aironet ME dashboard, choose **Wireless Settings** > **WLAN**.
b) Click the **General** tab.
c) In the **Profile Name** field, enter the SSID name.
d) From the **Admin State** drop-down list, choose **Enabled**.
e) From the **Radio Policy** drop-down list, choose **ALL**.
f) Click the **WLAN Security** tab.
g) Enable **Guest Network**.
h) Enable **Captive Network Assistant**.

i) In the **Captive Portal URL** field, enter the captive portal URL.

Note To view the Captive Portal URL, in the Cisco Spaces dashboard, click the **Captive Portals**app. Click **SSIDs**, and then click the **Configure Manually** link for a Cisco Unified Wireless Network (Cisco AireOS) SSID. Go to the **Creating the SSIDs in WLC Direct Connect** section. The URL is displayed at Step 7g.

j) From the **Access Type**, choose **RADIUS**.
k) In the **ACL Name (IPV4)**, choose the ACL name configured at Step 4b.
l) For radius server, click **Add Radius Authentication Server**
m) Select Radius server IP added at Step 6b from the list.

Step 8 For Radius L2 Authentication, enable **MAC Filtering** and **ON MAC Filter failure**.

Step 9 Click **Apply**.

Configuring Mobility Express for Notifications and Reports

If you are using Mobility Express with WLC connect, to configure for location updates, perform the following steps:

Step 1 In the **Cisco Wireless Controller CLI**, execute the following commands:

a. config cloud-services cmx disable

b. config cloud-services server url https://{Customer Path Key}.{LB Domain} {LB IP Address}

c. config cloud-services server id-token {Customer JWT Token}

d. config network dns serverip <dns server ip>

e. config cloud-services cmx enable

Note To view the {Customer Path Key}, {LB Domain}, {LB IP Address}, and {Customer JWT Token}, in the Cisco Spaces dashboard, click the **Configure Manually** link for a CUWN SSID in SSIDs window. You can also contact the Cisco Spaces support team. Ensure that there are no trailing or leading spaces.

Step 2 Check the summary using the following command:

show cloud-services cmx summary

The result appears.

Now in the Cisco Spaces dashboard, when you choose **CUWN-WLC** in the **Add a Wireless Network** window, the WLC will be listed. So, you can import the APs of that WLC to the Cisco Spaces.

Sample Result

```
(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 .... Active

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

Heartbeat Status .... OK

What to do next

Now the Cisco Wireless Controller will be available for importing to the CiscoCisco Spaces location hierarchy. For more information on importing the Cisco Wireless Controller and its access points, follow from Step 4 of the procedure mentioned in Connecting Cisco Spaces to Cisco Wireless Controller Using Cisco WLC Direct Connect , on page 17.

Cisco Spaces Scale Benchmark

Table 2: Scale Summary

SNO	Cisco Spaces: Connector	Cisco WLC Direct Connect		CMX Tethering Connector
Platforms	Cisco AireOS	Cisco AireOS	Cisco Catalyst 9800 Series	Cisco AireOS
Max Scale on supported appliance.	12.5K APs, 250K clients Incoming NMSP should not be more than 10.5K messages/sec.	50 APs and 50 Clients	50 APs and 50 Clients	60K clients, 5K APs, and 50k RFID tags Maps with 1BLDG-100 Floors and each floor with 50 APs
Scale supported releases	Connector version 2.1.1 with docker v2.0.204	8.8MR2	16.12, 17.1	8.8MR2 with CMX 10.6 (high end)

Note Currently, scaling is not available for Mobility Express.