



Configuring WLANs

- [Prerequisites for WLANs, on page 1](#)
- [Restrictions for WLANs, on page 1](#)
- [Information About WLANs, on page 3](#)
- [Creating and Removing WLANs \(GUI\), on page 4](#)
- [Enabling and Disabling WLANs \(GUI\), on page 5](#)
- [Editing WLAN SSID or Profile Name for WLANs \(GUI\), on page 5](#)
- [Creating and Deleting WLANs \(CLI\), on page 5](#)
- [Enabling and Disabling WLANs \(CLI\), on page 6](#)
- [Editing WLAN SSID or Profile Name for WLANs \(CLI\), on page 7](#)
- [Viewing WLANs \(CLI\), on page 7](#)
- [Searching WLANs \(GUI\), on page 7](#)
- [Assigning WLANs to Interfaces, on page 8](#)
- [Configuring Network Access Identifier \(CLI\), on page 8](#)

Prerequisites for WLANs

- You can associate up to 16 WLANs with each access point group and assign specific access points to each group. Each access point advertises only the enabled WLANs that belong to its access point group. The access point (AP) does not advertise disabled WLANs in its access point group or WLANs that belong to another group.
- We recommend that you assign one set of VLANs for WLANs and a different set of VLANs for management interfaces to ensure that controllers properly route VLAN traffic.

Restrictions for WLANs

- Do not configure PSK and CCKM in a WLAN, as this configuration is not supported and impacts client join flow.
- Ensure that TKIP or AES ciphers are enabled with WPA1 configuration, else ISSU may break during upgrade process.

- When you change the WLAN profile name, then FlexConnect APs (using AP-specific VLAN mapping) will become WLAN-specific. If FlexConnect Groups are configured, the VLAN mapping will become Group-specific.
- Do not enable IEEE 802.1X Fast Transition on Flex Local Authentication enabled WLAN, as client association is not supported with Fast Transition 802.1X key management.
- Peer-to-peer blocking does not apply to multicast traffic.
- In FlexConnect, peer-to-peer blocking configuration cannot be applied only to a particular FlexConnect AP or a subset of APs. It is applied to all the FlexConnect APs that broadcast the SSID.
- The WLAN name and SSID can have up to 32 characters.
- WLAN and SSID names support only the following ASCII characters:
 - Numerals: 48 through 57 hex (0 to 9)
 - Alphabets (uppercase): 65 through 90 hex (A to Z)
 - Alphabets (lowercase): 97 through 122 hex (a to z)
 - ASCII space: 20 hex
 - Printable special characters: 21 through 2F, 3A through 40, and 5B through 60 hex, that is: ! " # \$ % & ' () * + , - . / : ; < = > ? @ [\] ^ _ ` { | } ~
- WLAN name cannot be a keyword; for example, if you try to create a WLAN with the name as 's' by entering the **wlan s** command, it results in shutting down all WLANs because 's' is used as a keyword for shutdown.
- You cannot map a WLAN to VLAN 0. Similarly, you cannot map a WLAN to VLANs 1002 to 1006.
- Dual stack clients with a static-IPv4 address is not supported.
- In a dual-stack with IPv4 and IPv6 configured in the Cisco 9800 controller, if an AP tries to join controller with IPv6 tunnel before its IPv4 tunnel gets cleaned, you would see a traceback and AP join will fail.
- When creating a WLAN with the same SSID, you must create a unique profile name for each WLAN.
- All OfficeExtend access points should be in the same access point group, and that group should contain no more than 15 WLANs. A controller with OfficeExtend access points in an access point group publishes only up to 15 WLANs to each connected OfficeExtend access point because it reserves one WLAN for the personal SSID.
- The Cisco Flex 7500 Series Controller does not support the 802.1X security variants on a centrally switched WLAN. For example, the following configurations are not allowed on a centrally switched WLAN:
 - WPA1/WPA2 with 802.1X AKM
 - WPA1/WPA2 with CCKM
 - Conditional webauth
 - Splash WEB page redirect
 - If you want to configure your WLAN in any of the above combinations, the WLAN must be configured to use local switching.

- If you configured your WLAN with EAP Passthrough and if you downgrade to an earlier controller version, you might encounter XML validation errors during the downgrade process. This problem is because EAP Passthrough is not supported in earlier releases. The configuration will default to the default security settings (WPA2/802.1X).



Note The OEAP 600 Series access point supports a maximum of two WLANs and one remote LAN. If you have configured more than two WLANs and one remote LAN, you can assign the 600 Series access point to an AP group. The support for two WLANs and one remote LAN still applies to the AP Group. If the 600 Series OEAP is in the default group, the WLAN or remote LAN IDs must be lower than 8.

- Profile name of WLAN can be of max 31 characters for a locally switched WLAN. For central switched WLAN, the profile name can be of 32 characters.
- When multiple WLANs with the same SSID get assigned to the same AP radio, you must have a unique Layer 2 security policy so that clients can safely select between them.
- When WLAN is local switching, associate the client to local-switching WLAN where AVC is enabled. Send some traffic from client, when you check the AVC stats after 90 sec. Cisco WLC shows stats under top-apps but does not show under client. There is timer issue so for the first slot Cisco WLC might not show stats for the clients. Earlier, only 1 sec stats for a client is seen if the timers at AP and at WLC are off by 89 seconds. Now, clearing of the stats is after 180 seconds so stats from 91 seconds to 179 seconds for a client is seen. This is done because two copies of the stats per client cannot be kept due to memory constraint in Cisco 5508 WLC.
- RADIUS server overwrite is not configured on a per WLAN basis, but rather on a per AAA server group basis.
- Downloadable ACL (DACL) is not supported in the FlexConnect mode or the local mode.



Caution Some clients might not be able to connect to WLANs properly if they detect the same SSID with multiple security policies. Use this WLAN feature with care.

Information About WLANs

You can control up to WLANs for lightweight access points. Each WLAN has a separate WLAN ID, a separate profile name, and a WLAN SSID. All controllers publish up to 16 WLANs to each connected access point. However, you can create till the maximum number of supported WLANs and then selectively publish these WLANs (using profiles and tags) to different access points for managing your wireless network in a better way.

You can configure WLANs with different SSIDs or with the same SSID. An SSID identifies the specific wireless network that you want the controller to access.

Creating and Removing WLANs (GUI)

Step 1 Choose **WLANs** to open the WLANs page.

This page lists all of the WLANs currently configured on the controller. For each WLAN, you can see its WLAN ID, profile name, type, SSID, status, and security policies.

The total number of WLANs appears in the upper right-hand corner of the page. If the list of WLANs spans multiple pages, you can access these pages by clicking the page number links.

Note If you want to delete a WLAN, hover your cursor over the blue drop-down arrow for that WLAN and choose **Remove**, or select the check box to the left of the WLAN, choose **Remove Selected** from the drop-down list, and click **Go**. A message appears asking you to confirm your decision. If you proceed, the WLAN is removed from any access point group to which it is assigned and from the access point's radio.

Step 2 Create a new WLAN by choosing **Create New** from the drop-down list and clicking **Go**. The **WLANs > New** page appears.

Note The controller creates the default-group access point group and automatically populates it with the first 16 WLANs (WLANs with IDs 1 through 16, or fewer if 16 WLANs are not configured). This default group cannot be modified (you cannot add WLANs to it nor delete WLANs from it). It is dynamically updated whenever the first 16 WLANs are added or deleted. If an access point does not belong to an access point group, it is assigned to the default group and uses the WLANs in that group. If an access point joins the controller with an undefined access point group name, the access point keeps its group name but uses the WLANs in the default-group access point group.

Step 3 From the **Type** drop-down list, choose **WLAN** to create a WLAN.

Note If you want to create a guest LAN for wired guest users, choose **Guest LAN**.

Step 4 In the **Profile Name** field, enter up to 32 characters for the profile name to be assigned to this WLAN. The profile name must be unique.

Step 5 In the **WLAN SSID** field, enter up to 32 characters for the SSID to be assigned to this WLAN.

Note The WLAN name and SSID can have up to 32 characters. If the WLAN is locally switched, the limit on the WLAN name is 31 characters.

Step 6 From the **WLAN ID** drop-down list, choose the ID number for this WLAN.

Note If the Cisco OEAP 600 is in the default group, the WLAN/Remote LAN IDs need to be set as lower than ID 8.

Step 7 Click **Apply** to commit your changes. The **WLANs > Edit** page appears.

Note You can also open the **WLANs > Edit** page from the **WLANs** page by clicking the ID number of the WLAN that you want to edit.

Step 8 Use the parameters on the **General**, **Security**, **QoS**, and **Advanced** tabs to configure this WLAN. See the sections in the rest of this chapter for instructions on configuring specific features for WLANs.

Step 9 On the **General** tab, check the **Status** check box to enable this WLAN. Be sure to leave it unselected until you have finished making configuration changes to the WLAN.

Step 10 Click **Apply** to commit your changes.

Step 11 Click **Save Configuration** to save your changes.

Enabling and Disabling WLANs (GUI)

Step 1 Choose **WLANs** to open the WLANs page.

This page lists all of the WLANs currently configured on the controller.

Step 2 Enable or disable WLANs from the WLANs page by selecting the check boxes to the left of the WLANs that you want to enable or disable, choosing **Enable Selected** or **Disable Selected** from the drop-down list, and clicking **Go**.

Step 3 Click **Apply**.

Editing WLAN SSID or Profile Name for WLANs (GUI)

Step 1 Choose **WLANs** to open the WLANs page.

This page lists all of the WLANs currently configured on the controller. For each WLAN, you can see its WLAN ID, profile name, type, SSID, status, and security policies.

The total number of WLANs appears in the upper right-hand corner of the page. If the list of WLANs spans multiple pages, you can access these pages by clicking the page number links.

Step 2 To edit the a WLAN profile or SSID, click the WLAN ID link in the **WLANs > Edit** page.

- In the **Profile Name** field, edit the WLAN profile name.
- In the **WLAN SSID** field, edit the WLAN SSID.

Step 3 Click **Apply** to commit your changes.

Step 4 Click **Save Configuration** to save your changes.

Creating and Deleting WLANs (CLI)

- Create a new WLAN by entering this command:

```
config wlan create wlan-id profile-name ssid
```

**Note**

- If you do not specify an *ssid*, the *profile-name* parameter is used for both the profile name and the SSID.
- When you create a new WLAN using the **config wlan create** command, it is created in disabled mode. Leave it disabled until you have finished configuring it.

- Delete a WLAN by entering this command:

```
config wlan delete wlan-id
```

**Note**

If you try to delete a WLAN that is assigned to an access point group, you are prompted with message asking you to continue or not. If you proceed, the WLAN is removed from the access point group and from the access point's radio.

- View the WLANs configured on the controller by entering this command:

```
show wlan summary
```

Enabling and Disabling WLANs (CLI)

Procedure

- Enable a WLAN (for example, after you have finished making configuration changes to the WLAN) by entering this command:

```
config wlan enable {wlan_id | all}
```

**Note**

If the command fails, an error message appears (for example, "Request failed for wlan 10 - Static WEP key size does not match 802.1X WEP key size").

- Disable a WLAN (for example, before making any modifications to a WLAN) by entering this command:

```
config wlan disable {wlan_id | all}
```

where

wlan_id is a WLAN ID between 1 and 512.

all is all WLANs.

**Note**

If the management and AP-manager interfaces are mapped to the same port and are members of the same VLAN, you must disable the WLAN before making a port-mapping change to either interface. If the management and AP-manager interfaces are assigned to different VLANs, you do not need to disable the WLAN.

Editing WLAN SSID or Profile Name for WLANs (CLI)

- Edit a profile name or SSID associated to a WLAN:
 - Disable the WLAN first before changing the profile name or SSID by entering this command:
config wlan disable *wlan_id*
 - Rename the WLAN profile name or SSID by entering this command:
config wlan ssid *wlan_id ssid*
config wlan profile *wlan_id profile-name*
- View the WLANs configured on the controller by entering this command:
show wlan summary

Viewing WLANs (CLI)

- View the list of existing WLANs and to see whether they are enabled or disabled by entering this command:
show wlan summary

Searching WLANs (GUI)

Step 1 On the WLANs page, click **Change Filter**. The Search WLANs dialog box appears.

Step 2 Perform one of the following:

- To search for WLANs based on profile name, check the **Profile Name** check box and enter the desired profile name in the edit box.
- To search for WLANs based on SSID, check the **SSID** check box and enter the desired SSID in the edit box.
- To search for WLANs based on their status, check the **Status** check box and choose **Enabled** or **Disabled** from the drop-down list.

Step 3 Click **Find**. Only the WLANs that match your search criteria appear on the WLANs page, and the Current Filter field at the top of the page specifies the search criteria used to generate the list (for example, None, Profile Name:user1, SSID:test1, Status: disabled).

Note To clear any configured search criteria and display the entire list of WLANs, click **Clear Filter**.

Assigning WLANs to Interfaces

Use these commands to assign a WLAN to an interface:

- Assign a WLAN to an interface by entering this command:

```
config wlan interface {wlan_id | foreignAp} interface_id
```

- Use the *interface_id* option to assign the WLAN to a specific interface.
- Use the *foreignAp* option to use a third-party access point.
- Verify the interface assignment status by entering the **show wlan summary** command.

For the client with an IPv6 address, controller supports only one untagged interface for a controller. However, in an ideal scenario of IPv4 address, the controller supports one untagged interface per port.

Configuring Network Access Identifier (CLI)

You can configure a network access server identifier (NAS-ID) on each WLAN profile, VLAN interface, or AP group. The NAS-ID is sent to the RADIUS server by the controller through an authentication request to classify users to different groups so that the RADIUS server can send a customized authentication response.

If you configure a NAS-ID for an AP group, this NAS-ID overrides the NAS-ID that is configured for a WLAN profile or the VLAN interface. If you configure a NAS-ID for a WLAN profile, this NAS-ID overrides the NAS-ID that is configured for the VLAN interface.

- Configure a NAS-ID for a WLAN profile by entering this command:

```
config wlan nasid {nas-id-string | none} wlan-id
```

- Configure a NAS-ID for a VLAN interface by entering this command:

```
config interface nasid {nas-id-string | none} interface-name
```

- Configure a NAS-ID for an AP group by entering this command:

```
config wlan apgroup nasid {nas-id-string | none} apgroup-name
```

When the controller communicates with the RADIUS server, the NAS-ID attribute is replaced with the configured NAS-ID in an AP group, a WLAN, or a VLAN interface.

The NAS-ID that is configured on the controller for an AP group, a WLAN, or a VLAN interface is used for authentication. The configuration of NAS-ID is not propagated across controllers.



Note

If WLAN interface is overridden at AP group then overridden interface NAS ID will be used. Since Interface NASID is given priority over WLAN NAS ID.
