WLANs

Information About WLANs

This feature enables you to control WLANs for lightweight access points. Each WLAN has a separate WLAN ID, a separate profile name, and a WLAN SSID. All access points can advertise up to 16 WLANs. However, you can create up to 4096 WLANs and then selectively advertise these WLANs (using profiles and tags) to different APs for better manageability.

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.

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.

  For more information about access point groups, see the *AP Groups* chapter.

- Controllers use different attributes to differentiate between WLANs with the same Service Set Identifier (SSID):

- WLANs with the same SSID and same Layer 2 policy cannot be created if the WLAN ID is lower than 17.
- Two WLANs with IDs that are greater than 17 and that have the same SSID and same Layer 2 policy are allowed if WLANs are added in different AP groups.

- We recommend that you assign one set of VLANs for WLANs and a different set of VLANs for management interfaces to ensure that client traffic is kept separate from management traffic.

Restrictions for WLANs

- 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. For central switched WLAN, the profile name can be of 32 characters.
- Peer-to-peer blocking does not apply to multicast traffic.
- 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 VLAN0, and you cannot map VLANs 1002 to 1006.
- When creating a WLAN with the same SSID, you must create a unique profile name for each WLAN.
- 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.
- 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.

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

- All leading spaces in the profile and SSID names get truncated to one leading space. The truncation of leading spaces is an XML format limitation. Hence the truncation occurs during the controller's XML configuration file upload or download procedure on all AireOS controller releases.

Creating and Removing WLANs (GUI)

Procedure

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)

Procedure

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)

Procedure

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)

Procedure

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.