Per-WLAN Wireless Settings

• DTIM Period, on page 1
• Cisco Client Extensions, on page 3
• Client Profiling, on page 4
• Client Count per WLAN, on page 8

DTIM Period

In the 802.11 networks, lightweight access points broadcast a beacon at regular intervals, which coincides with the Delivery Traffic Indication Map (DTIM). After the access point broadcasts the beacon, it transmits any buffered broadcast and multicast frames based on the value set for the DTIM period. This feature allows power-saving clients to wake up at the appropriate time if they are expecting broadcast or multicast data.

Typically, the DTIM value is set to 1 (to transmit broadcast and multicast frames after every beacon) or 2 (to transmit broadcast and multicast frames after every other beacon). For instance, if the beacon period of the 802.11 network is 100 ms and the DTIM value is set to 1, the access point transmits buffered broadcast and multicast frames for 10 times every second. If the beacon period is 100 ms and the DTIM value is set to 2, the access point transmits buffered broadcast and multicast frames for 5 times every second. Either of these settings are suitable for applications, including Voice Over IP (VoIP), that expect frequent broadcast and multicast frames.

However, the DTIM value can be set as high as 255 (to transmit broadcast and multicast frames after every 255th beacon) if all 802.11 clients have power save enabled. Because the clients have to listen only when the DTIM period is reached, they can be set to listen for broadcasts and multicasts less frequently which results in a longer battery life. For example, if the beacon period is 100 ms and you set the DTIM value to 100, the access point transmits buffered broadcast and multicast frames once every 10 seconds. This rate allows the power-saving clients to sleep longer before they have to wake up and listen for broadcasts and multicasts, which results in a longer battery life.

Note

A beacon period, which is specified in milliseconds on the controller, is converted internally by the software to 802.11 Time Units (TUs), where 1 TU = 1.024 milliseconds. On Cisco’s 802.11n access points, this value is rounded to the nearest multiple of 17 TUs. For example, a configured beacon period of 100 ms results in an actual beacon period of 104 ms.
Many applications cannot tolerate huge duration between broadcast and multicast messages, which results in poor protocol and application performance. We recommend that you set a low DTIM value for 802.11 networks that support such clients.

You can configure the DTIM period for the 802.11 radio networks on specific WLANs. For example, you might want to set different DTIM values for voice and data WLANs.

This section contains the following subsections:

### Configuring the DTIM Period (GUI)

#### Procedure

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

**Step 2** Click the ID number of the WLAN for which you want to configure the DTIM period.

**Step 3** Unselect the Status check box to disable the WLAN.

**Step 4** Click Apply.

**Step 5** Choose the Advanced tab to open the WLANs > Edit (Advanced) page.

**Step 6** Under DTIM Period, enter a value between 1 and 255 (inclusive) in the 802.11a/n and 802.11b/g/n text boxes. The default value is 1 (transmit broadcast and multicast frames after every beacon).

**Step 7** Click Apply.

**Step 8** Choose the General tab to open the WLANs > Edit (General) page.

**Step 9** Select the Status check box to reenable the WLAN.

**Step 10** Click Save Configuration.

### Configuring the DTIM Period (CLI)

#### Procedure

**Step 1** Disable the WLAN by entering this command:

```
config wlan disable wlan_id
```

**Step 2** Configure the DTIM period for a 802.11 radio network on a specific WLAN by entering this command:

```
config wlan dtim {802.11a | 802.11b} dtim wlan_id
```

where `dtim` is a value between 1 and 255 (inclusive). The default value is 1 (transmit broadcast and multicast frames after every beacon).

**Step 3** Reenable the WLAN by entering this command:

```
config wlan enable wlan_id
```

**Step 4** Save your changes by entering this command:

```
save config
```
Step 5  Verify the DTIM period by entering this command:

```
show wlan wlan_id
```

---

**Cisco Client Extensions**

The Cisco Client Extensions (CCX) software is licensed to manufacturers and vendors of third-party client devices. The CCX code resident on these clients enables them to communicate wirelessly with Cisco access points and to support Cisco features that other client devices do not, including those features that are related to increased security, enhanced performance, fast roaming, and power management.


This section contains the following subsections:

### Prerequisites for Configuring Cisco Client Extensions

- The software supports CCX versions 1 through 5, which enables controllers and their access points to communicate wirelessly with third-party client devices that support CCX. CCX support is enabled automatically for every WLAN on the controller and cannot be disabled. However, you can configure Aironet information elements (IEs).

- If Aironet IE support is enabled, the access point sends an Aironet IE 0x85 (which contains the access point name, load, number of associated clients, and so on) in the beacon and probe responses of this WLAN, and the controller sends Aironet IEs 0x85 and 0x95 (which contains the management IP address of the controller and the IP address of the access point) in the reassociation response if it receives Aironet IE 0x85 in the reassociation request.

### Configuring CCX Aironet IEs (GUI)

**Procedure**

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

**Step 2**  Click the ID number of the desired WLAN to open the WLANs > Edit page.

**Step 3**  Choose the Advanced tab to open the WLANs > Edit (Advanced tab) page.

**Step 4**  Select the Aironet IE check box if you want to enable support for Aironet IEs for this WLAN. Otherwise, unselect this check box. The default value is enabled (or selected).

**Step 5**  Click Apply to commit your changes.

**Step 6**  Click Save Configuration to save your changes.
Viewing a Client’s CCX Version (GUI)

A client device sends its CCX version in association request packets to the access point. The controller then stores the client’s CCX version in its database and uses it to limit the features for this client. For example, if a client supports CCX version 2, the controller does not allow the client to use CCX version 4 features.

Procedure

Step 1: Choose Monitor > Clients to open the Clients page.
Step 2: Click the MAC address of the desired client device to open the Clients > Detail page.

The CCX Version text box shows the CCX version supported by this client device. Not Supported appears if the client does not support CCX.

Step 3: Click Back to return to the previous screen.
Step 4: Repeat this procedure to view the CCX version supported by any other client devices.

Configuring CCX Aironet IEs (CLI)

Use this command to configure CCX Aironet IEs:

```
config wlan ccx aironet-ie {enable | disable} wlan_id
```

The default value is enabled.

Viewing a Client’s CCX Version (CLI)

See the CCX version supported by a particular client device using the controller CLI by entering this command:

```
show client detail client_mac
```

Client Profiling

When a client tries to associate with a WLAN, it is possible to determine the client type from the information received in the process. The controller acts as the collector of the information and sends the ISE with the required data in an optimal form. Local Client profiling (DHCP and HTTP) is enabled at WLAN level. Clients on the WLANS will be profiled as soon as profiling is enabled.

Controller has been enhanced with some of these following capabilities:

- Controller does profiling of devices based on protocols like HTTP, DHCP, etc. to identify the end devices on the network.

- You can configure device-based policies and enforce per user or per device end points, and policies applicable per device.

- Controller displays statistics based on per user or per device end points, and policies applicable per device.
Profiling can be based on:

- Role, defining the user type or the user group to which the user belongs.
- Device type, such as Windows machine, Smart Phone, iPad, iPhone, Android, etc.
- Username/password pair.
- Location, based on the AP group to which the endpoint is connected
- Time of the day, based on what time of the day the endpoint is allowed on the network.
- EAP type, to check what EAP method the client uses to get connected.

Policing is decided based on a profile which are:

- VLAN
- QoS Level
- ACL
- Session timeout value

Information about Custom HTTP Port Profiling

This feature is designed to enable the controller to identify and profile clients connecting from ports apart from HTTP port 80.

The custom http port profiling feature including High Availability (HA) will be supported on all controller and AP platforms in 8.2 release. The profiling port configuration will be configurable and maintained in the controller, and the value will be included in the configuration update when the AP joins this controller.

This section contains the following subsections:

Prerequisites for Configuring Client Profiling

- By default, client profiling will be disabled on all WLANs.
- Client profiling is supported on access points that are in Local mode and FlexConnect mode.
- Both DHCP Proxy and DHCP Bridging mode on the controller are supported.
- Accounting Server configuration on the WLAN must be pointing at an ISE running 1.1 MnR or later releases. Cisco ACS does not support client profiling.
- The type of DHCP server used does not affect client profiling.
- If the DHCP_REQUEST packet contains a string that is found in the Profiled Devices list of the ISE, then the client will be profiled automatically.
- The client is identified based on the MAC address sent in the Accounting request packet.
- Only a MAC address should be sent as calling station ID in accounting packets when profiling is enabled.
- To enable client profiling, you must enable the DHCP required flag and disable the local authentication flag.
• Client profiling uses pre-existing profiles in the controller.
• Profiling for Wireless clients are done based on MAC OUI, DHCP, HTTP User agent.

---

Note

DHCP is required for DHCP profiling and Webauth for HTTP user agent.

Restrictions for Configuring Client Profiling

• Profiling is not supported for clients in the following scenarios:
  • Clients associating with FlexConnect mode APs in Standalone mode.
  • Clients associating with FlexConnect mode APs when local authentication is done with local switching is enabled.
  • Wired clients behind the WGB will not be profiled and policy action will not be done.

• With profiling enabled for local switching FlexConnect mode APs, only VLAN override is supported as an AAA override attribute.

• While the controller parses the DHCP profiling information every time the client sends a request, the profiling information is sent to ISE only once.

• Custom profiles cannot be created for this release.

• This release contains 88 pre-existing policies where CLI is check only except if you create a policy.

• When local profiling is enabled radius profiling is not allowed on a particular WLAN.

• Only the first policy rule that matches is applied.

• Only 16 policies per WLAN can be configured and globally 16 policies can be allowed.

• Policy action is done only after L2/L3 authentication is complete or when the device sends http traffic and gets the device profiled. Profiling and policing actions will happen more than once per client.

• If AAA override is enabled and if you get any AAA attributes from the AAA server other than role type, configured policy does not apply since the AAA override attributes have a higher precedence.

• For Apple devices, the version and operating system information is displayed only for iPhones 7 and later versions and iPads 6,11 and later generations, provided the WLAN is not open. The version and operating system information is not displayed for older devices.

Restrictions for Configuring Custom HTTP Port Profiling

• This feature supports HTTP profiling based on custom HTTP port and only one custom HTTP port can be configured.

• For a Cisco Aironet 1850 Series AP, DHCP profiling is applied, and HTTP port profiling is not applied.

• HTTP profiling will not work for Apple devices.
Configuring Client Profiling (GUI)

**Procedure**

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

**Step 2** Click the WLAN ID. The WLANs > Edit page appears.

**Step 3** Click the **Advanced** tab.

**Step 4** In the RADIUS and Local Client Profiling area, do the following:
   a) To profile clients based on DHCP, select the **DHCP Profiling** check box.
   b) To profile clients based on HTTP, select the **HTTP Profiling** check box.

You can configure client profiling in both RADIUS mode and Local mode on the WLAN.

**Step 5** Click **Apply**.

**Step 6** Click **Save Configuration**.

---

Configuring Client Profiling (CLI)

- Enable or disable client profiling for a WLAN based on DHCP by entering this command:

  ```
  config wlan profiling radius dhcp {enable | disable} wlan-id
  ```

- Enable or disable client profiling in RADIUS mode for a WLAN based on HTTP, DHCP, or both by entering this command:

  ```
  config wlan profiling radius {dhcp | http | all} {enable | disable} wlan-id
  ```

  **Note** Use the **all** parameter to configure client profiling based on both DHCP and HTTP.

- Enable or disable client profiling in Local mode for a WLAN based on HTTP, DHCP, or both by entering this command:

  ```
  config wlan profiling local {dhcp | http | all} {enable | disable} wlan-id
  ```

- To see the status of client profiling on a WLAN, enter the following command:

  ```
  show wlan wlan-id
  ```

- To enable or disable debugging of client profiling, enter the following command:

  ```
  debug profiling {enable | disable}
  ```
Configuring Custom HTTP Port for Profiling (GUI)

Note
The HTTP port 80 is always open for gathering HTTP profiling data, irrespective of the custom HTTP port configuration.

Procedure

Step 1
Choose Controller > General to open the general page.

Step 2
Enter the port value under HTTP Profiling Port field.

Configuring Custom HTTP Port for Profiling (CLI)

Procedure

Step 1
Configure custom HTTP port by entering this command:
`config network profiling http-port port number`
The default port value is 80.

Step 2
View the configured HTTP profiling port and other inband connectivity settings by entering this command:
`show network summary`
The network configuration is displayed.

Client Count per WLAN

You can set a limit to the number of clients that can connect to a WLAN, which is useful in scenarios where you have a limited number of clients that can connect to a controller. For example, consider a scenario where the controller can serve up to 256 clients on a WLAN and these clients can be shared between enterprise users (employees) and guest users. You can set a limit on the number of guest clients that can access a given WLAN. The number of clients that you can configure for each WLAN depends on the platform that you are using.

This section contains the following subsections:

Restrictions for Setting Client Count for WLANs

- The maximum number of clients for each WLAN feature is not supported when you use FlexConnect local authentication.
• The maximum number of clients for each WLAN feature is supported only for access points that are in connected mode.

• When a WLAN has reached the limit on the maximum number of clients connected to it or an AP radio and a new client tries to join the WLAN, the client cannot connect to the WLAN until an existing client gets disconnected.

• Roaming clients are considered as new clients. The new client can connect to a WLAN, which has reached the maximum limit on the number of connected clients, only when an existing client gets disconnected.

Note
For more information about the number of clients that are supported, see the product data sheet of your controller.

Configuring the Client Count per WLAN (GUI)

Procedure

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Choose WLANs to open the WLANs page.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Click the ID number of the WLAN for which you want to limit the number of clients. The WLANs &gt; Edit page appears.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Click the Advanced tab.</td>
</tr>
<tr>
<td>Step 4</td>
<td>In the Maximum Allowed Clients text box, enter the maximum number of clients that are to be allowed.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Click Apply.</td>
</tr>
<tr>
<td>Step 6</td>
<td>Click Save Configuration.</td>
</tr>
</tbody>
</table>

Configuring the Maximum Number of Clients per WLAN (CLI)

Procedure

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Determine the WLAN ID for which you want to configure the maximum clients by entering this command: show wlan summary</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Get the WLAN ID from the list.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Configure the maximum number of clients for each WLAN by entering this command: config wlan max-associated-clients max-clients wlan-id</td>
</tr>
</tbody>
</table>
Configuring the Maximum Number of Clients for each AP Radio per WLAN (GUI)

**Procedure**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Choose <strong>WLANs</strong> to open the WLANs page.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Click the ID number of the <strong>WLAN</strong> for which you want to limit the number of clients. The WLANs &gt; Edit page appears.</td>
</tr>
<tr>
<td>Step 3</td>
<td>In the <strong>Advanced</strong> tab, enter the maximum allowed clients for each access point radio in the Maximum Allowed Clients Per AP Radio text box. You can configure up to 200 clients.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Click <strong>Apply</strong>.</td>
</tr>
</tbody>
</table>

Configuring the Maximum Number of Clients for each AP Radio per WLAN (CLI)

**Procedure**

| Step 1 | Determine the WLAN ID for which you want to configure the maximum clients for each radio by entering this command:  
`show wlan summary`  
Obtain the WLAN ID from the list. |
|--------|-------------------------------------------------------------|
| Step 2 | Configure the maximum number of clients for each WLAN by entering this command:  
`config wlan max-radio-clients client_count`  
You can configure up to 200 clients. |
| Step 3 | See the configured maximum associated clients by entering the **show 802.11a** command. |

Deauthenticating Clients (CLI)

Using the controller, you can deauthenticate clients based on their user name, IP address, or MAC address. If there are multiple client sessions with the same user name, you can deauthenticate all the client sessions based on the user name. If there are overlapped IP addresses across different interfaces, you can use the MAC address to deauthenticate the clients.

**Note**

It is not possible to deauthenticate clients using the controller GUI.
Procedure

- **config client deauthenticate** \{mac-addr | ipv4-addr | ipv6-addr | user-name\}
Deauthenticating Clients (CLI)