Performing System Tasks

This chapter describes how to use WCS to perform system-level tasks. It contains these sections:

Adding System Components to the WCS Database

This section describes how to add a controller and a location appliance to the WCS database.

Adding a Controller to the WCS Database

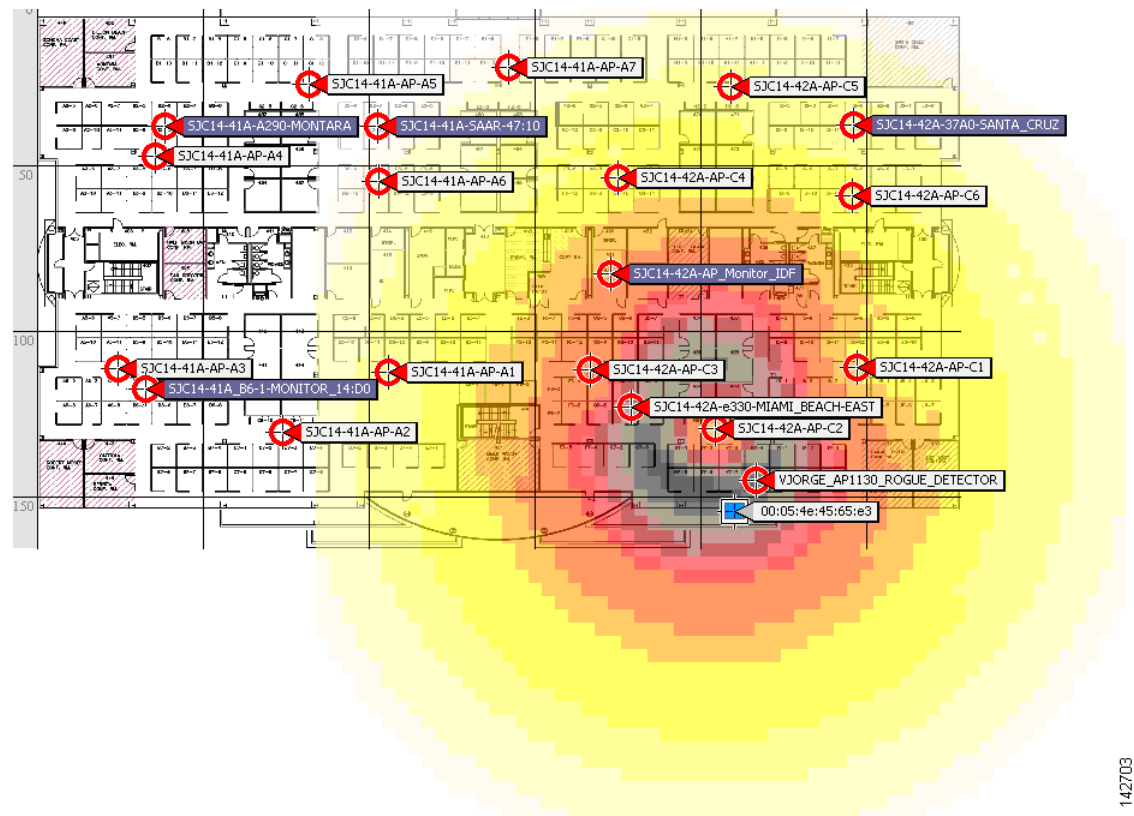Follow these steps to add a controller to the WCS database.

Note   Cisco recommends that you manage controllers through the controller dedicated service port for improved security. However, when you manage controllers that do not have a service port (such as 2000 series controllers) or for which the service port is disabled, you must manage those controllers through the controller management interface.

Step 1   Log into the WCS user interface.

Step 2   Click **Configure > Controllers** to display the All Controllers page.

Step 3   From the Select a command drop-down menu, choose **Add Controller** and click **GO**.

Step 4   On the Add Controller page, enter the controller IP address, network mask, and required SNMP settings.

Step 5   Click **OK**. WCS displays a Please Wait dialog box while it contacts the controller and adds the current controller configuration to the WCS database. It then returns you to the Add Controller page.

Step 6   If WCS does not find a controller at the IP address that you entered for the controller, the Discovery Status dialog displays this message:

```
No response from device, check SNMP.
```

Check these settings to correct the problem:

- The controller service port IP address might be set incorrectly. Check the service port setting on the controller.
- WCS might not have been able to contact the controller. Make sure that you can ping the controller from the WCS server.
- The SNMP settings on the controller might not match the SNMP settings that you entered in WCS. Make sure that the SNMP settings configured on the controller match the settings that you entered in WCS.

Step 7   Add additional controllers if desired.

Adding a Location Appliance to the WCS Database

To add a location appliance to the WCS database, follow the instructions in the *Cisco Location Appliance Configuration Guide*. It provides documentation on the Location > Location Server option within WCS and all of its capabilities (such as editing general properties, tracking, filtering, history, advanced, and NMSP parameters). WCS without the use of the location appliance supports on-demand or query-based location. This version visually displays a single device's location at a time, placing each single device on the floor map associated with the floor it is on. Location determination using this version of WCS with location is captured in Figure 4-1 where the blue icon is the only visual presented of a Wi-Fi client device.

Figure 4-1   Location Determination

Additional Functionality with Location Appliance

Cisco 2700 series location appliances operate within the Cisco Wireless LAN Solution infrastructure. Location appliances compute, collect, and store historical location data using Cisco wireless LAN controllers and access points to track the physical location of wireless devices.

The location appliance can track up to 2,500 elements. You can track the following elements: client stations, active asset tags, rogue clients and access points. Updates on the locations of elements being tracked are provided to the location server from the Cisco wireless LAN controller.

Only those elements designated for tracking by the controller are viewable in Cisco WCS maps, queries, and reports. No events and alarms are collected for non-tracked elements, and they are not used in calculating the 2,500 element limit.

You can modify the following tracking parameters using Cisco WCS:

- Enable and disable which element locations (client stations, active asset tags, and rogue clients and access points) you actively track
- Set limits on how many of a specific element you want to track

  You can set limits on how many of a specific element you wish to track. For example, given a limit of 2,500 trackable units, you could set a limit to track only 1,500 client stations. Once the tracking limit is met, the number of elements not being tracked is summarized on the Tracking Parameters page.

- Disable tracking and reporting of ad hoc rogue clients and access points

> **Note** Even though all clients are loaded in the map, the display has a limit of 250 clients per floor to prevent overcrowding. You can do an advanced search of the map to see the items of interest.

Selectable filters enable you to search collected data and display specific elements on a map. For example, a biomedical user may want to display only active RFID tags that are tracking key medical equipment rather than access points or clients for a given floor.

Using WCS to Update System Software

Follow these steps to update controller (and access point) software using WCS.

Step 1   Enter **ping** *ip-address* to be sure that the WCS server can contact the controller. If you use an external TFTP server, enter **ping** *ip-address* to be sure that the WCS server can contact the TFTP server.

> **Note** When you are downloading through a controller distribution system (DS) network port, the TFTP server can be on the same or a different subnet because the DS port is routable.

Step 2   Click the **Configure > Controllers** to navigate to the All Controllers page.

Step 3   Check the check box of the desired controller, choose **Download Software** from the Select a Command drop-down menu, and click **GO**. WCS displays the Download Software to Controller page.

Step 4   If you use the built-in WCS TFTP server, check the **TFTP Server on WCS System** check box. If you use an external TFTP server, uncheck this check box and add the external TFTP server IP address.

Step 5   Click **Browse** and navigate to the software update file (for example, AS_2000_*release*.aes for 2000 series controllers). The files are uploaded to the root directory which was configured for use by the TFTP server. You can change to a different directory.

> **Note** Be sure that you have the correct software file for your controller.

Step 6   Click **Download**. WCS downloads the software to the controller, and the controller writes the code to flash RAM. As WCS performs this function, it displays its progress in the Status field.

Downloading Vendor Device Certificates

Each wireless device (controller, access point, and client) has its own device certificates. For example, the controller is shipped with a Cisco-installed device certificate. This certificate is used by EAP-TLS and EAP-FAST (when not using PACs) to authenticate wireless clients during local EAP authentication. However, if you wish to use your own vendor-specific device certificate, it must be downloaded to the controller.

Follow the instructions below to download a vendor-specific device certificate to the controller.

Step 1   Choose **Configure > Controller**.

Step 2   You can download the certificates in one of two ways:

  a. Click the check box of the controller you choose.

  b. Choose **Download Vendor Device Certificate** from the Select a command drop-down menu and click **GO**.

  or

  a. Click the URL of the desired controller in the IP Address column.

  b. Choose **System > Commands** from the left sidebar menu.

  c. Choose **Download Vendor Device Certificate** from the Upload/Download Commands drop-down menu and click **GO**.

Step 3   In the Certificate Password field, enter the password which was used to protect the certificate.

Step 4   Specify if the certificate to download is on the TFTP server or on the local machine. If it is on the TFTP server, the name must be supplied in the Server File Name parameter in Step 10. If the certificate is on the local machine, you must specify the file path in the Local File Name parameter in Step 9 using the Browse button.

Step 5   Enter the TFTP server name in the Server Name parameter. The default is for the WCS server to act as the TFTP server.

Step 6   Enter the server IP address.

Step 7   In the Maximum Retries field, enter the maximum number of times that the TFTP server attempts to download the certificate.

Step 8   In the Timeout field, enter the amount of time (in seconds) that the TFTP server attempts to download the certificate.

Step 9   In the Local File Name field, enter the directory path of the certificate.

Step 10   In the Server File Name field, enter the name of the certificate.

Step 11   Click **OK.**

Downloading Vendor CA Certificates

Controllers and access points have a Certificate Authority (CA) certificate that is used to sign and validate device certificates. The controller is shipped with a Cisco-installed CA certificate. This certificate may be used by EAP-TLS and EAP-FAST (when not using PACs) to authenticate wireless clients during local EAP authentication. However, if you wish to use your own vendor-specific CA certificate, it must be downloaded to the controller. Follow the instructions in this section to download vendor CA certificate to the controller.

Step 1   Click **Configure > Controllers**.

Step 2   You can download the certificates in one of two ways:

  a. Click the check box of the controller you choose.

  b. Choose **Download Vendor CA Certificate** from the Select a command drop-down menu and click **GO**.

or

    a. Click the URL of the desired controller in the IP Address column.

    b. Choose **System > Commands** from the left sidebar menu.

    c. Choose **Download Vendor CA Certificate** from the Upload/Download Commands drop-down menu and click **GO**.

Step 3 Specify if the certificate to download is on the TFTP server or on the local machine. If it is on the TFTP server, the name must be supplied in the Server File Name parameter in Step 9. If the certificate is on the local machine, you must specify the file path in the Local File Name parameter in Step 8 using the Browse button.

Step 4 Enter the TFTP server name in the Server Name parameter. The default is for the WCS server to act as the TFTP server.

Step 5 Enter the server IP address.

Step 6 In the Maximum Retries field, enter the maximum number of times that the TFTP server attempts to download the certificate.

Step 7 In the Timeout field, enter the amount of time (in seconds) that the TFTP server attempts to download the certificate.

Step 8 In the Local File Name field, enter the directory path of the certificate.

Step 9 In the Server File Name field, enter the name of the certificate.

Step 10 Click **OK.**

Using WCS to Enable Long Preambles for SpectraLink NetLink Phones

A radio preamble (sometimes called a *header*) is a section of data at the head of a packet. It contains information that wireless devices need when sending and receiving packets. Short preambles improve throughput performance, so they are enabled by default. However, some wireless devices, such as SpectraLink NetLink phones, require long preambles.

To optimize the operation of SpectraLink NetLink phones on your wireless LAN, follow these steps to use WCS to enable long preambles.

Step 1 Log into the WCS user interface.

Step 2 Click **Configure > Controllers** to navigate to the All Controllers page.

Step 3 Click the IP address of the desired controller.

Step 4 In the sidebar, click **802.11b/g/n > Parameters**.

Step 5 If the *IP Address* > 802.11b/g/n Parameters page shows that short preambles are enabled, continue to the next step. However, if short preambles are disabled, which means that long preambles are enabled, the controller is already optimized for SpectraLink NetLink phones, and you do not need to continue this procedure.

Step 6 Enable long preambles by unchecking the **Short Preamble** check box.

Step 7 Click **Save** to update the controller configuration.

Step 8   To save the controller configuration, click **System > Commands** in the sidebar, **Save Config To Flash** from the Administrative Commands drop-down menu, and **GO**.

Step 9   To reboot the controller, click **Reboot** from the Administrative Commands drop-down menu and **GO**.

Step 10   Click **OK** when the following message appears:

```
Please save configuration by clicking "Save Config to flash". Do you want to continue
rebooting anyways?
```

The controller reboots. This process may take some time, during which WCS loses its connection to the controller.

> **Note**   You can view the controller reboot process with a CLI session.

Creating an RF Calibration Model

If you would like to further refine WCS Location tracking of client and rogue access points across one or more floors of a building, you have the option of creating an RF calibration model that uses physically collected RF measurements to fine-tune the location algorithm. When you have multiple floors in a building with the same physical layout as the calibrated floor, you can save time calibrating the remaining floors by using the same RF calibration model for the remaining floors.

The calibration models are used as RF overlays with measured RF signal characteristics that can be applied to different floor areas. This allows the Cisco Unified Wireless Network Solution installation team to lay out one floor in a multi-floor area, use the RF calibration tool to measure and save the RF characteristics of that floor as a new calibration model, and apply that calibration model to all the other floors with the same physical layout. See Chapter 5 for calibration instructions.