



CHAPTER 2

Getting Started

This chapter describes how to prepare Cisco WCS for operation. It contains these sections:

- [Prerequisites, page 2-1](#)
- [System Requirements, page 2-2](#)
- [Installing WCS for Windows, page 2-6](#)
- [Installing WCS for Linux, page 2-14](#)
- [Starting WCS, page 2-16](#)
- [Logging into the WCS User Interface, page 2-18](#)
- [Customizing Home Page Tabs, page 2-23](#)
- [Using the Cisco WCS User Interface, page 2-28](#)
- [Using the Search Feature, page 2-31](#)

Prerequisites

Before installing the Cisco WCS, ensure that you have completed the following:

- Meet the necessary hardware and software requirements as listed in the “[System Requirements](#)” section on [page 2-2](#) for Cisco WCS.
- Update your system with the necessary critical updates and service packs.



Note See the latest release notes for information on the service packs and patches required for correct operation of Cisco WCS.

- To receive the expected results, you should run no more than 3 concurrent WCS setups for standard server use (4 GB memory and 3 GHz CPU speed) and no more than 5 concurrent WCS setups for high-end server use (8 GB memory and 3 GHz CPU speed).
- Verify that the following ports are open during installation and startup:
 - HTTP: configurable during install (80 by default)
 - HTTPS: configurable during install (443 by default)
 - 1315
 - 1299

- 6789
- 8009
- 8456
- 8005
- 69
- 21
- 162
- 8457

**Note**

Make sure your firewall rules are not restrictive. You can check the current rules on Linux with the built-in *iptables -L* command or on Windows with the Control Panel > Windows Firewall option.

System Requirements

Cisco WCS can be run on a workstation/server class system and access points can be distributed unevenly across controllers. The following requirements must be met for the different components.

High-End Server

- Supports up to 3000 Cisco Aironet lightweight access points, 1250 standalone access points, and 750 Cisco wireless LAN controllers.
- 3.16 GHz Intel Xeon Quad processor X5406 or better.
- 8-GB RAM.
- 200 GB minimum free disk space is needed on your hard drive.

**Note**

If you choose a CPU configuration that is different from what is provided above as a guidance, you may use a website like the following to perform the benchmark tests and assess whether the alternate CPU meets the WCS minimum requirements:

<http://www.cpubenchmark.net>

**Note**

If you use multiple CPU configurations, the benchmarking sites (like the above website) also allow you to make comparisons based on the number of cores that are being selected per CPU.

**Note**

The free disk space listed is a minimum requirement but may be different for your system, depending on the number of backups.

Unified Computing System

The following Cisco Unified Computing System(UCS) C-Series servers provide guidance to plan your system requirements for either UCS or equivalent hardware platform. Any server can be used if it meets the minimum requirements.

Cisco UCS C-Series M1 Server

The following are the recommended specifications for the Cisco UCS C-Series M1 Server, but you can choose higher processing capabilities:

- One Intel Xeon 5500 series processor X5570 (4-core 2.93-GHz).



Note If your processor speed is less than the one mentioned above, we recommend you to use two processors.

- 8-GB RAM.
- 200-GB minimum free disk space on your hard drive.

Cisco UCS C-Series M2 Server

The following are the recommended specifications for the Cisco UCS C-Series M2 Server, but you can choose higher processing capabilities:

- One Intel Xeon 5600 series processor X5680 (6-core 3.33-GHz) or one Intel Xeon 5600 series processor X5670 (6-core 2.93-GHz).
- 8-GB RAM.
- 200-GB minimum free disk space on your hard drive.

Standard Server

- Up to 2000 Cisco Aironet lightweight access points, 1000 standalone access points, and 450 wireless LAN controllers.
- 3.2-GHz Intel Dual Core processor or better.
- 2.13-GHz Intel Quad Core X3210 processor.
- 4 GB of RAM.
- 80-GB minimum free disk space on your hard drive.



Note If you choose a CPU configuration that is different from what is provided above as a guidance, you may use a website like the following to perform the benchmark tests and assess whether the alternate CPU meets the WCS minimum requirements:
<http://www.cpubenchmark.net>

Unified Computing System

The following Cisco Unified Computing System(UCS) C-Series servers provide guidance to plan your system requirements for either UCS or equivalent hardware platform. Any server can be used if it meets the minimum requirements.

Cisco UCS C-Series M1 Server

The following are the recommended specifications for the Cisco UCS C-Series M1 Server, but you can choose higher processing capabilities:

- One Intel Xeon 5500 series processor X5570 (4-core 2.93-GHz) or one Intel Xeon 5500 series processor X5550 (4-core 2.66-GHz) or one Intel Xeon 5500 series processor E5540 (4-core 2.53-GHz).
- 4 GB of RAM.
- 80-GB minimum free disk space on your hard drive.

Cisco UCS C-Series M2 Server

The following are the recommended specifications for the Cisco UCS C-Series M2 Server, but you can choose higher processing capabilities:

- One Intel Xeon 5600 series processor X5650 (6-core 2.66-GHz) or one Intel Xeon 5600 series processor X5670 (6-core 2.93-GHz).
- 4 GB of RAM.
- 80-GB minimum free disk space on your hard drive.

Low-End Server

- Up to 500 Cisco Aironet lightweight access points, 200 standalone access points, and 125 Cisco wireless LAN controllers.
- 3.06-GHz Intel processor or better.
- 1.86-GHz Intel Dual core processor.
- 2 GB of RAM.
- 50-GB minimum free disk space on your hard drive.



Note If you choose a CPU configuration that is different from what is provided above as a guidance, you may use a website like the following to perform the benchmark tests and assess whether the alternate CPU meets the WCS minimum requirements:

<http://www.cpubenchmark.net>

Unified Computing System

The following Cisco Unified Computing System(UCS) C-Series servers provide guidance to plan your system requirements for either UCS or equivalent hardware platform. Any server can be used if it meets the minimum requirements.

Cisco UCS C-Series M1 Server

The following are the recommended specifications for the Cisco UCS C-Series M1 Server, but you can choose higher processing capabilities:

- One Intel Xeon 5500 series processor X5550 (4-core 2.66-GHz).
- 2 GB of RAM.
- 50-GB minimum free disk space on your hard drive.

Cisco UCS C-Series M2 Server

The following are the recommended specifications for the Cisco UCS C-Series M2 Server, but you can choose higher processing capabilities:

- One Intel Xeon 5600 series processor X5650 (6-core 2.66-GHz).
- 2 GB of RAM.
- 50-GB minimum free disk space on your hard drive.

Supported Operating Systems

The following operating systems are supported:

- Windows 2003/SP2 and Windows 2003 R2/SP2 32-bit installations with all critical and security Windows updates installed.

Windows 2003/SP2 64-bit installations are not supported.

Windows 2003 32-bit installations provide support for up to 64 GB of RAM provided Physical Address Extension (PAE) is enabled. See Windows documentation for instructions on enabling this mode.

- Red Hat Linux Enterprise Server 5.X 32-bit operating system installations.

Red Hat Linux Enterprise Server 5.X 64-bit operating system installations are not supported.

- Microsoft Windows Server 2003 and Red Hat Linux version support on VMware ESX version 3.0.1 and above with either local storage or SAN over fiber channel.

**Note**

Individual operating systems running WCS in VMware must follow the specifications for the size of WCS you intend to use.

Client Requirements

The Cisco WCS user interface requires Internet Explorer 7.0 or later with the 9.0.X or later Flash plugin, or Mozilla Firefox 3 or 3.5. Cisco recommends Mozilla Firefox 3.5 for best performance.

Browsing on Windows 2003 Cisco WCS servers is not recommended because recommended Windows 2003 security settings cause browsing problems.

The client running the browser must have a minimum of 1 GB of RAM and a 2-GHz processor. The client device should not be running any CPU or memory-intensive applications.

**Note**

The screen resolution should be set to 1024 x 768 pixels for both WCS and Navigator.

Supported WLC Releases

Cisco WCS 7.0 can manage the following releases of the WLC as found on various controllers (such as 2106, 4400 series, WiSM, and so on):

- 4.2
- 5.2
- 6.0
- 7.0

**Note**

See the release notes

(http://www.cisco.com/en/US/products/ps6305/prod_release_notes_list.html) for the exact version numbers.

WCS on WLSE

- Up to 1500 Cisco Aironet lightweight access points and 100/375 Cisco wireless LAN controllers.
- 3-GHz Intel Pentium4 processor with 3 GB of RAM.
- 38 GB of free space on your hard drive.

WCS Navigator

- Up to 20 WCSs
- Up to 30,000 access points

Installing WCS for Windows

Before installing Cisco WCS, refer to the “Prerequisites” section on page 2-1 and the “System Requirements” section on page 2-2. You must have administrator privileges on Windows. If you receive a message that a previous version of WCS was detected, you must continue with one of two upgrade options. See the “Upgrading WCS” section on page 14-9.

If installing WCS for Linux, see the “Installing WCS for Linux” section on page 2-14.

Before You Begin

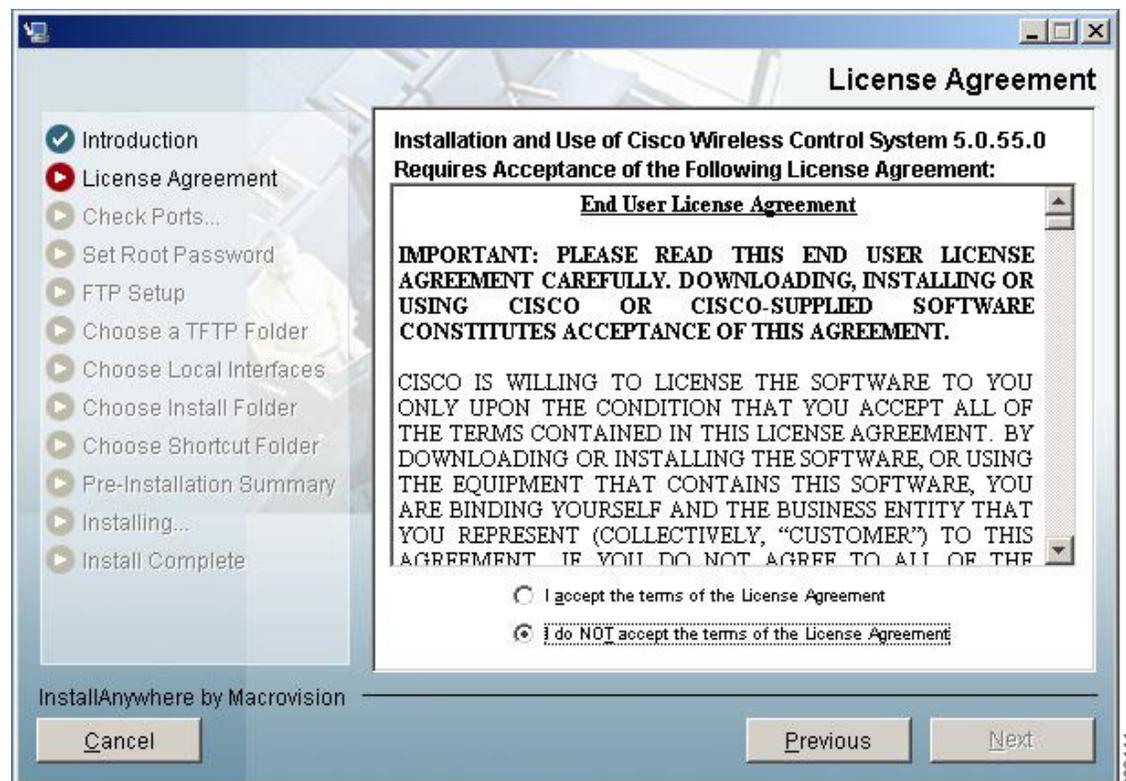
- You cannot install the WCS software if the username used to log into the server contains special characters such as exclamation marks (!). To ensure successful installation, log into the server using a username with no special characters before installing the software.

- Cisco WCS does not support the underscore character (_) in the name of the Windows server running the WCS software. If the server name contains an underscore, you can install the WCS software, but WCS fails to start.
- You must install WCS on a dedicated Windows server with no other services running (including those running as primary or secondary domain controllers) to avoid conflict with WCS.
- No hard-coded limits exist regarding the number of users or the type of user activities, but a heavy memory and CPU load on the server may affect functionality.

To install Cisco WCS, follow these steps:

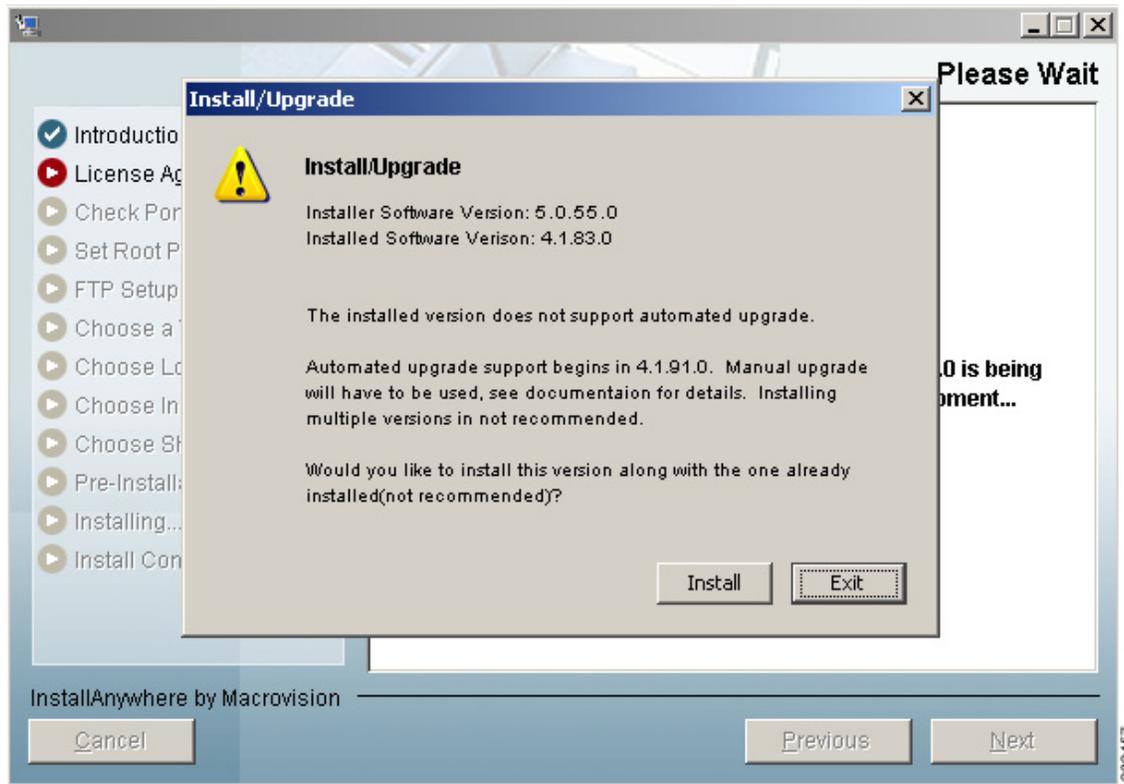
- Step 1** Insert the Windows Cisco WCS CD into the CD-ROM drive and double-click the WCS-STANDARD-K9-7.0.XX.Y.exe file where 7.0.XX.Y is the software build. If you received the installer from Cisco.com, double-click the WCS-STANDARD-K9.7-0.XX.Y.exe file that you downloaded to your local drive.
- Step 2** The Install Anywhere page appears and prepares the system for installation. After a few seconds, the Introduction window appears, followed by the license agreement window (see [Figure 2-1](#)). You must select the “I accept the terms of the License Agreement” radio button to continue.

Figure 2-1 License Agreement Page

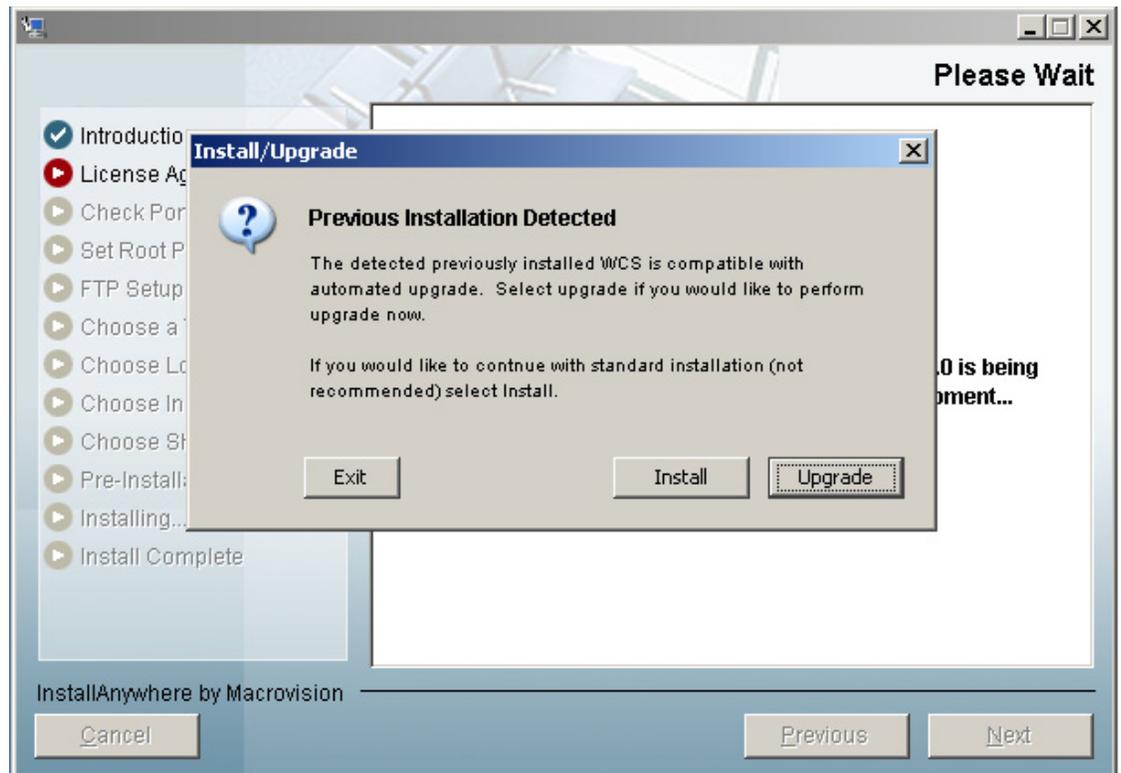


- Step 3** If the install wizard detects a previous version of WCS, you see a window similar to [Figure 2-2](#) or [Figure 2-3](#). If a previous version is detected, you must proceed as an upgrade and refer to the “Upgrading WCS” section on page 14-9. For a first-time installation, continue to Step 4.

Figure 2-2 Ineligible for Automated Upgrade

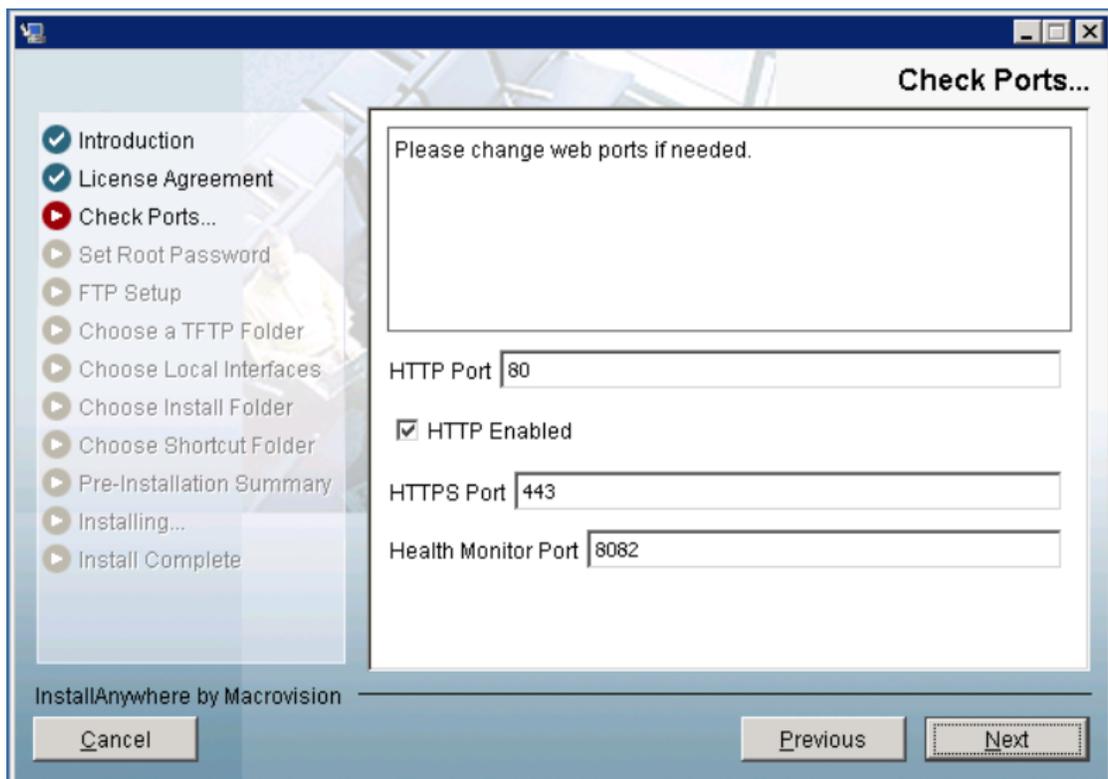


232457

Figure 2-3 Previous Installation Detected

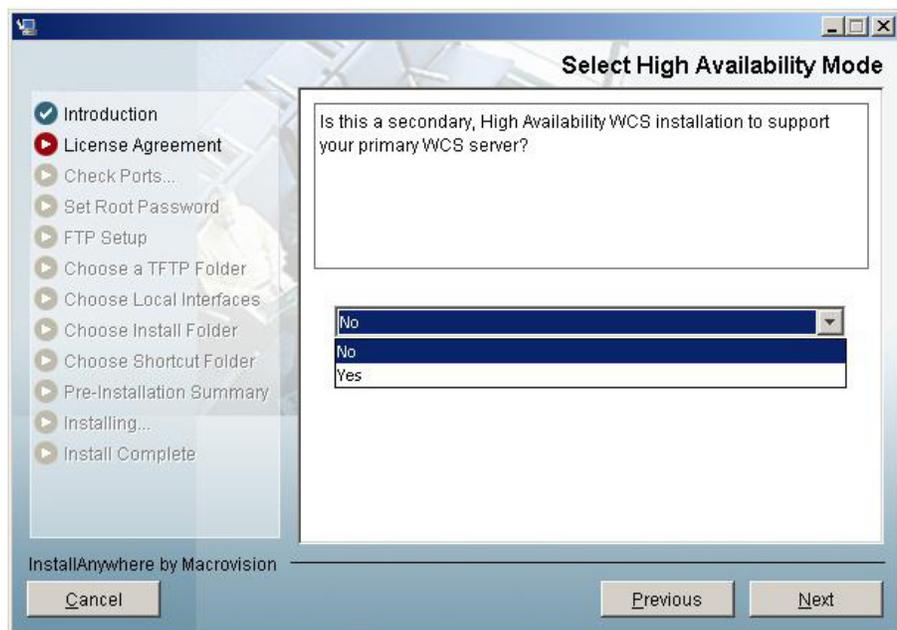
- Step 4** The Check Ports window appears (see [Figure 2-4](#)). In the Check Ports window, change the default HTTP and HTTPS ports if necessary. The default ports for HTTP and HTTPS are 80 and 443, respectively. HTTP Enabled is selected by default.

Figure 2-4 Check Ports Window



Step 5 Enter a Health Monitor Port. Click Next. The Select High Availability Mode window appears (see Figure 2-5).

Figure 2-5 Select HA Mode Window



- Step 6** Determine if this is a secondary, high availability WCS installation to support your primary WCS controller. The secondary WCS installation question refers to high availability only. You cannot install two different versions of WCS on the same server. If you are not enabling high availability, choose No (the default) and continue with Step 7. If this is a secondary installation for high availability purposes, choose **Yes** and follow Steps a through c.
- Enter an authentication key for the primary WCS device and click **Next**.
 - Choose a folder in which to install the secondary WCS in the Choose Install Folder window. Click **Next** to continue.
 - Choose a shortcut location for the secondary WCS.
- Step 7** Enter and then re-enter the root password. The rules for a strong password are as follows:
- The minimum password length is 8 characters.
 - No character can be used more than three times consecutively in the password.
 - The password must contain three of the four following character classes: uppercase, lowercase, numbers, and special characters.
- Step 8** Enter the root FTP password.
- Step 9** In the FTP Server File page, choose a folder in which to store the FTP server files and click **Next** to open the TFTP File Server window.



Note Store the FTP server files in a folder outside the main installation folder. This ensures that the FTP server files are not deleted if WCS is uninstalled.

- Step 10** In the TFTP Server File window, choose a folder in which to store the TFTP server files and click **Next**.

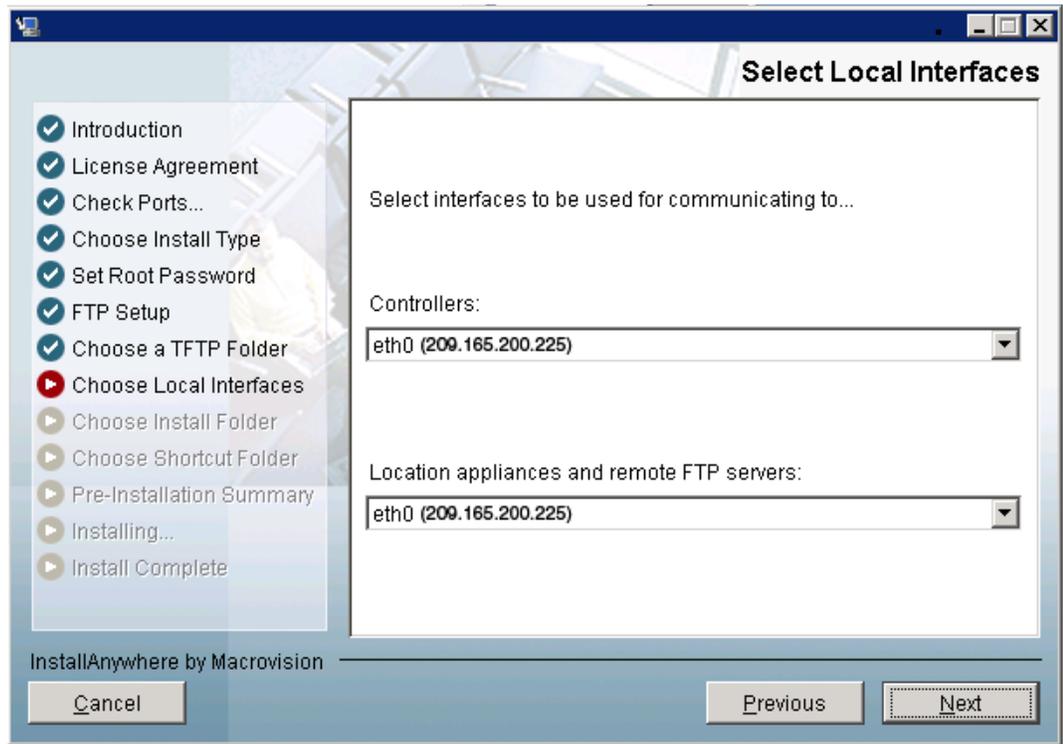


Note If you want to use a network-mounted drive for the TFTP root, you must configure WCS to run as a domain user (see the “[Installing WCS for Windows](#)” section on page 2-6) and then configure the TFTP root (see the “[Configuring TFTP as a Network Drive](#)” section on page 2-16).



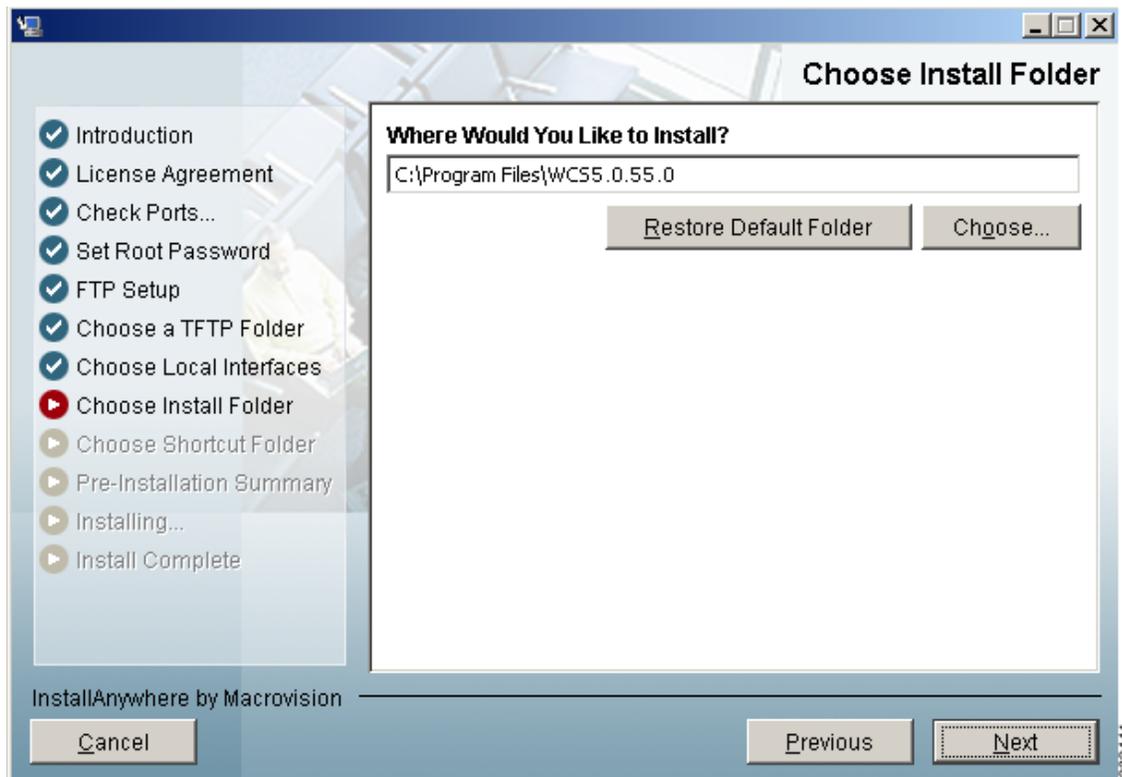
Note Store the TFTP server files in a folder outside the main installation folder. This ensures that the TFTP server files are not deleted if WCS is uninstalled.

- Step 11** If you are installing Cisco WCS on a multi-homed server (a server having multiple interfaces), the installer automatically detects the presence of multiple interfaces. The Select Local Interfaces window appears (see [Figure 2-6](#)). Choose the interfaces to be used by the server for communicating with controllers, MSEs and remote FTP servers, and clients. Click **Next**.

Figure 2-6 *Select Local Interfaces Window*

- Step 12** Choose a folder in which to install the Cisco WCS at the Choose Install Folder window (see [Figure 2-7](#)). Click **Next** to continue.

Figure 2-7 Choose Install Folder



- Step 13** Follow the prompts that appear in the window to complete the installation. After the installation is complete, the Install Complete window appears. Click **Done** to complete the installation.



Note Look at the installation log to verify that nothing went wrong during the installation. The install log resides in the installation root directory if the installation completes. If the installation did not complete, the install log resides in the directory from which the installer was run or the install root directory.

Configuring WCS to Run as a Domain User

To configure WCS to run as a domain user, follow these steps:

- Step 1** Stop WCS.
- Step 2** Add the domain user that will be used to run the service to the Administrators group of the local machine.
- Choose **Administrative Tools > Computer Management > Users and Groups > Groups**.
 - Double-click the Administrators group.

- c. Add the domain user.
- Step 3** Install WCS as instructed in the [“Installing WCS for Windows”](#) section on page 2-6.
- WCS consists of two services: Cisco Wireless Control System (A.B.C.D) and Nms_Apache_A_B_C_D, where A.B.C.D represents the current release number.
- Step 4** Set the WCS service to run as the domain user:
- a. Choose Administrative Tools > Services.
 - b. Right-click **Cisco Wireless Control System (A.B.C.D)** and choose **Properties**.
 - c. Click the **Log On** tab.
 - d. Click **This Account**.
 - e. Enter the domain user with “domain” before the name (such as DOMAIN\username), and the domain user password.
 - f. Click **OK**.
- Step 5** Set the Apache service to run as the domain user:
- a. Choose Administrative Tools > Services.
 - b. Right click **Nms_Apache_A_B_C_D** and choose **Properties**.
 - c. Click the **Log On** tab.
 - d. Click **This Account**.
 - e. Enter the domain user with “domain” before the name (such as DOMAIN\username), and the domain user password.
 - f. Click **OK**.
- Step 6** Start WCS.
-

Installing WCS for Linux

You must have root privileges on Linux to install WCS.

- Step 1** If not already done, log in as root. If you are using the GUI, open a terminal window.
- Step 2** Using the command line, perform one of the following:
- a. If you are installing from a CD, switch to the /media/cdrom directory. Skip to Step 4.
 - b. If you are installing from Cisco.com, switch to the directory that the install file was downloaded to. For example, if the install file was placed in /root/Desktop, enter **cd /root/Desktop**. Continue to Step 3.
- Step 3** If you downloaded the file from Cisco.com, you need to make it executable using the following command:
- chmod +x WCS-STANDARD-K9-7.0.XX.Y.bin** where xx.y represents the current release number.
- Step 4** Enter **./WCS-STANDARD-K9-7.0.XX.Y.bin** to start the install script.
- The install script prepares the install environment and displays the license agreement. You are asked to accept the terms of the license agreement.

- Step 5** If the install wizard detects a previous version of WCS, you see a message that states whether the detected version is eligible for an automated upgrade or not. If a previous version is detected, you must proceed as an upgrade and refer to the “[Upgrading WCS](#)” section on page 14-9. For a first-time installation, continue to Step 6.
- Step 6** Determine if this is a secondary, high availability WCS installation to support your primary WCS controller. Choose 1 for No (the default) or 2 for Yes. You cannot install two different versions of WCS on the same server. If you are not enabling high availability, choose 1 (No). If you are installing a secondary WCS for high availability mode and choose 2 (Yes), you will be prompted for an authentication key and a location for installing the secondary WCS.
- Step 7** The Check HTTP Port prompt appears. In the Check HTTP Port window, change the default HTTP and HTTPS ports if necessary. The default ports for HTTP and HTTPS are 80 and 443, respectively.
- Step 8** Specify whether you want to enable HTTP redirect. If HTTP redirect is enabled, any requests received on the HTTP port are redirected to the HTTPS port. If it is not enabled, the HTTP port is disabled.
- Step 9** Determine whether you want the default Health Monitor port of 8082 or you need to change the port.
- Step 10** Enter and then re-enter the root password. The rules for a strong password are as follows:
- The minimum password length is 8 characters.
 - The password cannot contain the username or the reverse of the username.
 - The password cannot be *Cisco* or *ocsic* (Cisco reversed).
 - The root password cannot be *public*.
 - No character can be used more than three times consecutively in the password.
 - The password must contain three of the four character classes: uppercase, lowercase, numbers, and special characters.
- Step 11** Enter the root FTP password.
-
-  **Note** WCS has a built-in ftp server. The functionality of this ftp server is used to perform routine management tasks, such as backing-up of data, or to send upgrade media to a local directory. You must not use this ftp server for tasks outside the scope of WCS and you must not install any other instances of an ftp server on your WCS server to avoid any port utilization conflicts.
-
- Step 12** Choose a folder in which to store the FTP server files.
-
-  **Note** If the folder does not already exist, you must enter **mkdir** and create it.
-
- Step 13** Choose a folder in which to store the TFTP server files.
-
-  **Note** Store the TFTP server files in a folder outside the main installation folder. This ensures that the TFTP server files are not deleted if Cisco WCS is uninstalled.
-
- Step 14** If you are installing Cisco WCS on a multi-homed server (a server having multiple interfaces), the installer automatically detects the presence of multiple interfaces. Choose the interfaces to be used by the server for communicating with controllers, MSEs and remote FTP servers, and clients.
- Step 15** Choose a folder in which to install the Cisco WCS.
- Step 16** Choose to create links from the default location (`/opt/WCS5.2.98.0`), from your home folder, or another location.

- Step 17** Follow the prompts that appear to complete the installation. After the installation is complete, the Install Complete statement appears.



Note Look at the installation log to verify that nothing went wrong during the installation. The install log is located in the installation root directory if the installation completes. If the installation did not complete, the install log resides in the directory from which the installer was run or the install root directory.

Configuring TFTP as a Network Drive

To configure TFTP as a network drive, you must have completed the steps in the [“Installing WCS for Linux”](#) section on page 2-14. The desired drive must also be accessible from that domain.

- Step 1** Make a backup of `installDir/webnms/classes/com/cisco/packaging/PackagingResources.properties`.

- Step 2** Edit the following line:

```
TftpRoot=\\\\servername\\resourcename
```

where your particular *servername* and *resourcename* are entered.

Choose Administration > ServerSettings.

At the TFTP Root setting, enter the desired network resource using the appropriate UNC format (such as `\\servername\\resourcename`) where your particular *servername* and *resourcename* are entered with only one set of backslashes.

- Step 3** Restart WCS.

Starting WCS

This section provides instructions for starting WCS on either a Windows or Linux server.

In Windows and Linux, Cisco WCS is installed as a service. The service runs continuously and resumes after a reboot.



Note You can check the status of WCS at any time. To do so, follow the instructions in the [“Verifying the Status of WCS”](#) section on page 14-1.

This section includes the following topics:

- [Starting WCS on Windows, page 2-17](#)
- [Starting WCS on Linux, page 2-17](#)

Starting WCS on Windows

Follow these steps to start WCS when it is installed on Windows.



Note When WCS is installed as a Windows service, WCS runs automatically upon system bootup.

Step 1 Log into the system as administrator.

Step 2 Perform one of the following:

- From the shortcut location (defaulted to Windows Start menu > **Programs > Wireless Control System A.B.C.D**) > **StartWCS**.
- From the command prompt, navigate to the WCS installation bin directory (the default is C:\Program Files\WCSA.B.C.D\bin) and enter **StartWCS**.

The WCS Admin window appears and displays messages indicating that WCS is starting.



Note If WCS is installed as a service, messages also appear to indicate that the Nms_Server service is starting.

Step 3 Close the WCSAdmin window when the Close button becomes active.

Step 4 WCS is ready to host WCS user interfaces (clients). Go to the [“Logging into the WCS User Interface” section on page 2-18](#) to use a web browser to connect to the WCS user interface.

Starting WCS on Linux

Follow these steps to start WCS when it is installed on Linux.



Note To see the version of WCS you currently have installed, enter **nmsadmin.sh version**.



Note When WCS is installed as a Linux service, WCS runs automatically upon system bootup.

Step 1 Log into the system as root.

Step 2 Using the Linux command-line interface (CLI), perform one of the following:

- Navigate to the shortcut location (defaulted to /opt/WCSA.B.C.D directory) and enter **./StartWCS**.
- Navigate to the installation bin directory (the default is opt/WCSA.B.C.D/bin) and enter **./StartWCS**.

The CLI displays messages indicating that WCS is starting.

Step 3 WCS is ready to host WCS user interfaces (clients). Go to the [“Logging into the WCS User Interface” section on page 2-18](#) to use a web browser to connect to the WCS user interface.

Logging into the WCS User Interface

Follow these steps to log into the WCS user interface through a web browser.

- Step 1** Launch Internet Explorer 7.0 or later or Mozilla Firefox 3.5 or later on a different computer than the one on which you installed and started WCS.



Note Some WCS features may not function properly if a browser and WCS are running on the same Windows workstation.

- Step 2** In the browser's address line, enter **https://wcs-ip-address**, where *wcs-ip-address* is the IP address of the computer on which you installed and started WCS.

- Step 3** When the WCS user interface displays the Login page, enter the root password you created during installation.



Note If any licensing problems occur, a message appears in an alert box. If you have an evaluation license, the number of days until the license expires is shown. You are also alerted to any expired licenses. You have the option to go directly to the licensing page to address these problems.

- Step 4** Click **Submit** to log into WCS. The WCS user interface is now active and available for use. The WCS home page appears. You can predefine what appears on the home page by choosing the monitoring components that are critical for your network. For example, you may want different monitoring components for a mesh network so that you can create a customized tab for a mesh dashboard.



Note If the database or Apache web server does not start, check the launchout.txt file in Linux or the wrapper.log file in Windows. You will see a generic “failed to start database” or “failed to start the Apache web server” message.



Note When the WCS database is restarted after a crash or any other severe condition, the full roll-forward recovery process is initiated automatically. You must either wait for the WCS database to finish the recovery process or delete the transaction logs to terminate the recovery process, and then restart the database.

This page enables you to choose the information that you want to see. You can organize the information in user-defined tabs. The default view comes with default tabs and pre-selected components for each, and you can arrange them as you like.



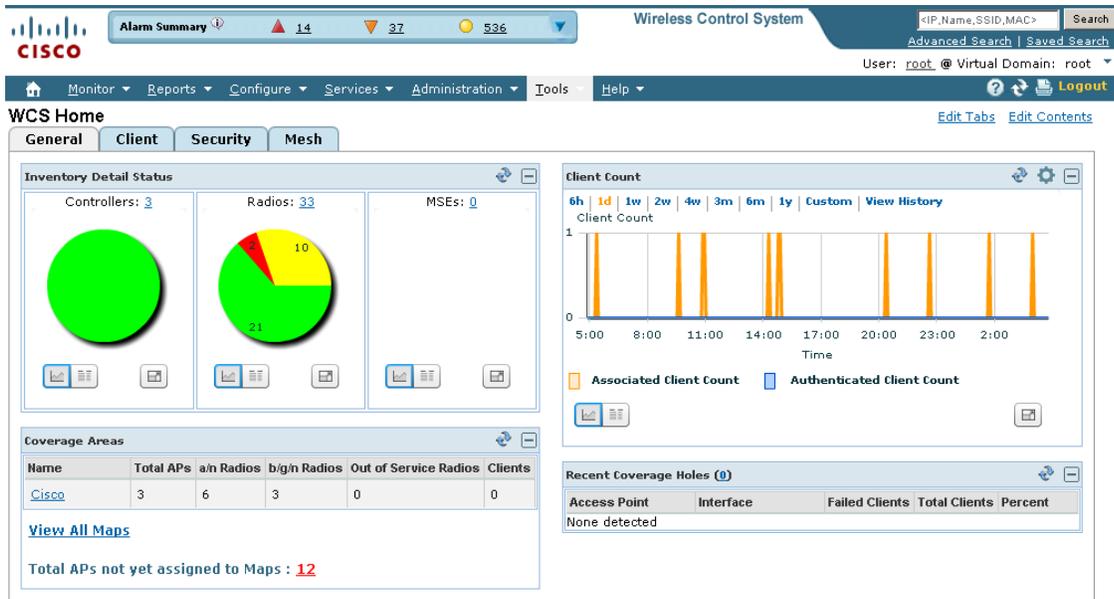
Note When an upgrade occurs, the user-defined tabs arranged by the previous user in the previous version are maintained. Therefore, the latest components may not show. Look at the Edit Components link to find what new components are added.

This page provides a summary of the Cisco Unified Wireless Network Solution, including coverage areas, the most recently detected rogue access points, access point operational data, reported coverage holes, and client distribution over time. [Figure 2-8](#) shows a typical WCS home page.

You should see four tabs on the WCS home page: General, Client, Security, and Mesh.

**Note**

When you use WCS for the first time, the network summary pages show that the Controllers, Coverage Areas, Most Recent Rogue APs, Top 5 APs, and Most Recent Coverage Holes databases are empty. It also shows that no client devices are connected to the system. After you configure the WCS database with one or more controllers, the WCS home page provides updated information.

Figure 2-8 WCS Home

251634

To exit the WCS user interface, close the browser page or click **Logout** in the upper right corner of the page. Exiting a WCS user interface session does not shut down WCS on the server.

When a system administrator stops the WCS server during your WCS session, your session ends, and the web browser displays this message: “The page cannot be displayed.” Your session does not reassociate to WCS when the server restarts. You must restart the WCS session.

General Tab

The following are factory default components for the General tab.

Table 2-1 General Tab Components

Component	Description
Inventory Detail Status	Displays the following: <ul style="list-style-type: none"> • Controllers—Lists the number of controllers that are managed in WCS. Graphically depicts reachable and unreachable controllers. • Radios—Lists the number of radios managed in WCS. Graphically depicts the number of radios in out-of-service (critical), minor, and ok conditions. • MSEs—Lists the number of MSEs that are managed in WCS. Graphically depicts reachable and unreachable servers. Look at the installation log to verify that nothing went wrong while manually adding the servers to WCS. (The trace for MSEs must be turned on.)
Coverage Areas	Displays access points, radios, and client details for each coverage area.
Client Count	Displays the total number of clients in WCS over the selected period of time. Note Client count includes autonomous clients.
Recent Coverage Holes	Displays the five most recent coverage alarms.
Total APs not yet assigned to Maps	Indicates the number of unassigned access points. Click the number link to view the list of these access points.

Client Tab

When you click the Client tab from the WCS home page, you see the following factory default components (see [Table 2-2](#)).

Table 2-2 Client Tab Components

Component	Description
Client Count	Displays the trend of associated and authenticated client counts in a given period of time.
Client Traffic	Displays the trend of both upstream and downstream client traffic in a given time period.
Client Alarm Summary	Displays the failures and errors of the five most recent client alarms.
Client Protocol Distribution	Displays the distribution of each radio band and the total current client count.
Client Distribution	Displays the distribution of clients by protocol, EAP type, and authentication and the total current client count.

Additionally, refer to “[Troubleshooting from the Client Tab Dashboard](#)” section on page 11-10 which describes the Client Troubleshooting portion of the Client tab.

Security Tab

When you click the Security tab from the WCS home page, you see the following factory default components:

Table 2-3 Security Tab Components

Component	Description
AP Threats/Attacks	Displays threats or attacks to access points for the past hour, past 24 hours, and total active.
Attacks Detected	Displays wIPS and signature attacks for the past hour, past 24 hours, and total active.
Recent Rogue AP Alarms	Displays the five most recent rogue alarms. Click the number in parentheses to access the Alarms page. Click an item under MAC Address to view alarm details.
Recent Ad hoc Rogue Alarm	Displays the five most recent ad hoc rogue alarms. Click the number in parentheses to access the Alarms page. Click an item under MAC address to view ad hoc details.
Most Recent Security Alarms	Displays the five most recent security alarms. Click the number in parentheses to access the Alarms page.
MFP Attacks	Displays MFP attacks for the past hour, past 24 hours, and total active.
Malicious Rogue APs	Displays malicious rogue access points for the past hour, past 24 hours, and total active.
Cisco Wired IPS Events	Displays Wired IPS events for the past hour, past 24 hours, and total active.
Unclassified Rogue APs	Displays unclassified rogue access points for the past hour, past 24 hours, and total active.
Friendly Rogue APs	Displays friendly rogue access points for the past hour, past 24 hours, and total active.
Ad hoc Rogues	Displays ad hoc rogues for the past hour, past 24 hours, and total active.
Security Index	Indicates the security of the WCS managed network. The security index is calculated by assigning priority to the various security configurations and displaying them in visual form.

Mesh Tab

If you click the Mesh tab from the WCS home page, you see the following factory default components:

Table 2-4 Mesh Tab Components

Component	Description
Most Recent Mesh Alarms	Displays the five most recent mesh alarms. Click the number in parentheses to access the Alarms page.
Worst SNR Link	Displays the worst signal-to-noise ratio (SNR) links. Data includes the Parent AP Name, the Child AP Name, and the Link SNR.
Worst Node Hop Count	Displays the worst node hop counts. Data includes the AP Name, the Hop Count, and the Parent AP Name.
Worst Packet Error Rate	Displays the worst packet error rates. Data includes the Parent AP Name, the Child AP Name, and the Packet Error Rate.

CleanAir Tab



Note To enable CleanAir on WCS, you need to have WCS Plus License installed.

The following factory default components appear on the CleanAir tab:

- 802.11a/n Avg Air Quality—Provides a line chart representing the average air quality for the entire network over a set period of time. Displays the average air quality on the 802.11 a/n band. Data includes time and the average air quality.
- 802.11b/g/n Avg Air Quality—Provides a line chart representing the average air quality for the entire network over a set period of time. Displays the average air quality on the 802.11 b/g/n band. Data includes time and the average air quality.
- 802.11a/n Min Air Quality—Provides a line chart representing the minimum air quality for the entire network over a set period of time. Displays the minimum air quality on the 802.11 a/n band. Data includes time and the minimum air quality.
- 802.11b/g/n Min Air Quality—Provides a line chart representing the minimum air quality for the entire network over a set period of time. Displays the minimum air quality on the 802.11 b/g/n band. Data includes time and minimum air quality.
- Worst 802.11a/n Interferers—Provides a list of active interferers with the worst severity level for the 802.11 a/n band. The graph displays the the top ten worst interferers that are currently active. Data includes InterfererID, Type, Status, Severity, Affected Channels, Duty Cycle(%), Discovered, Last Updated, and Floor.
- Worst 802.11b/g/n Interferers—Provides a list of active interferers with the worst severity level for 802.11 b/g/n band. The graph displays the top ten worst interferers that are currently active. Data includes InterfererID, Type, Status, Severity, Affected Channels, Duty Cycle(%), Discovered, Last Updated, and Floor.
- 802.11a/n Interferer Count—Provides a line chart representing the total number of interferers on all channels over the selected period of time. Displays the number of devices interfering in the 802.11 a/n band. Data includes time and interferer count.



Note The air quality is calculated for all controllers in your network that have CleanAir-enabled access points. The report includes aggregated air quality data across your network.

- 802.11b/g/n Interferer Count—Provides a line chart representing the total number of interferers on all channels over the selected period of time. Displays the number of devices interfering in the 802.11 b/g/n band. Data includes time and interferer count.



Note The information in the worst interferer and interferer count charts is collected from Mobility Services Engines (MSE). If MSEs are not available, this chart will not show any results.

- Recent Security-risk Interferers—Provides a list of active interferers with the worst severity level for each band. Displays the recent security risk interferers on your wireless network. Data includes Type, Severity, Affected Channels, Last Detected, Detected AP.



Note This chart includes information for the interferers for which security alarms are enabled.

You can also view the data presented on this tab in different formats.

Customizing Home Page Tabs

You can customize the predefined set of components depending on your network management needs. This page enables you to choose the displayed information. You can organize the information in user-defined tabs. The default view comes with default tabs and pre-selected components for each. When you click the Edit Tabs link in the WCS home page, the Edit Tabs page appears in which customization can begin (see [Figure 2-9](#)).



Note When an upgrade occurs, the arrangement of components in a previous version is maintained. Because of this, components or features added in a new release are not displayed. Click the Edit Contents link to discover new components. See the “[Customizing Home Page Tabs](#)” section on [page 2-23](#) for more information.

Creating a New Tab

Follow these steps to create a new tab.

-
- Step 1** Click **Edit Tabs** from the WCS home page. The Edit Tabs page appears (see [Figure 2-9](#)).

Figure 2-9 WCS Home > Edit Tabs



251636

- Step 2** Enter the name of the new tab you are creating and click **Add**. The tab name you add appears in the Tab Order page.



Note Add is the only function that does not require a Save after its operation. If you click **Delete**, **Rename**, **Move Up**, or **Move Down**, you must click **Save** for the changes to be applied.

- Step 3** Click the tab names in the Tab Order page and assign placement by clicking **Move Up** or **Move Down**.



Note If you want to return to the restored factory defaults as shown in [Figure 2-8](#), click **Reset to Factory Default**.

Customizing Home Page Content

Follow these steps to customize WCS home page components. You can add or delete components by selecting from the predefined list.

Also part of the customizable home page are time-based or non-time-based interactive graphs which you can display in graphical or chart form (by clicking the appropriate icon). (Interactive graphs also appear in Monitor > Clients.) These graphs refresh automatically within a predetermined time based on the default polling cycles of dependent tasks, or you can click the Refresh Component icon to get the most current status. When a graph is time based, an additional link bar at the top of the graph page displays the options as follows:

- 6h—the last six hours of data from the current time and current database table

- 1d—the last day of data from the current time and current database table
- 1w—the last week of data from the current time and the hourly aggregated table
- 2w—the last two weeks of data from the current time and hourly aggregated table
- 4w—the last four weeks of data from the current time and hourly aggregated table
- 3m—the last three months of data from the current time and daily aggregated table
- 6m—the last six months of data from the current time and the weekly aggregated table
- 1y—the last year of data from the current time and weekly aggregated table
- custom—the user can set both the days and hours for the start and end date. The appropriate aggregated source (either current, hourly, or daily) is chosen based on the starting date.

After you specify the timeframe, the data for that timeframe is retrieved and the corresponding graph is displayed. The link for which the graph is drawn is shown in a different color (orange) than the other links. The interactive graphs that are available within WCS include line graphs, area graphs, pie graphs, and stacked bar graphs.

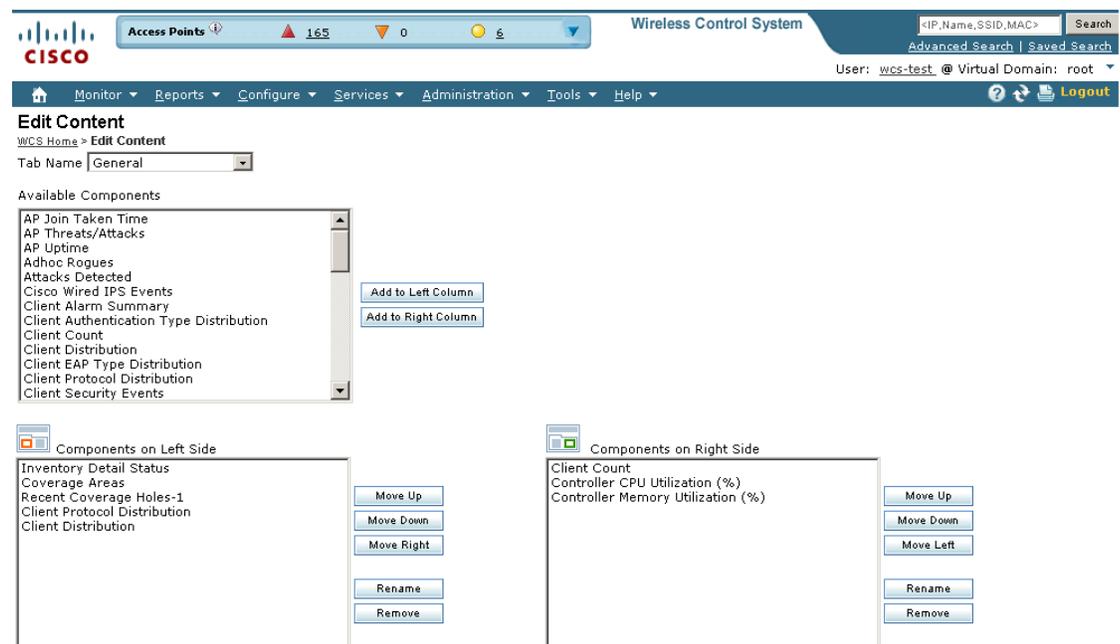
You can click **Enlarge Chart** icon to enlarge the graph in a separate page.

Editing Content

Follow these steps to customize WCS home page components:

- Step 1** On the WCS home page, click **Edit Contents**. The Edit Content page appears (see [Figure 2-10](#)).

Figure 2-10 Edit Content Page



- Step 2** In the Available Components drop-down list, highlight the desired component and choose to add it to the left column or add it to the right column. The component moves to the appropriate column.
- Step 3** Click the component in the Left Side or Right Side Column page and move it up, down, or to the right or left.

1637



Note To remove a component, choose it from the Left or Right Column list and click **Remove**.

Step 4 Click **Save**.

Additional Edit Content Page Components

The WCS > Edit Content page lists the following available components:

- AP Join Taken Time—Displays the access point name and the amount of time (in days, minutes, and seconds) that it took for the access point to join.
- AP Threats/Attacks—Displays various types of access point threats and attacks and indicates how many of each type have occurred.
- AP Uptime—Displays each access point name and amount of time it has been associated.
- Ad hoc Rogues—Displays ad hoc rogues for the previous hour, previous 24 hours, and total active.
- Attacks Detected
- Cisco Wired IPS Events—Displays wired IPS events for the previous hour, previous 24 hours, and total active.
- Client Alarm Summary—Displays the five most recent client alarms with client association failures, client authentication failures, client WEP key decryption errors, client WPA MIC errors, and client exclusions.
- Client Authentication Type—Displays the number of clients for each authentication type.
- Client Count—Displays the trend of associated and authenticated client counts in a given period of time.
- Client Distribution—Displays how clients are distributed by protocol, EAP type, and authentication type.
- Client EAP Type Distribution
- Client Protocol Distribution—Displays the current client count distribution by protocols.
- Client Security Events—Displays client security events within the previous 24 hours including excluded client events, WEP decrypt errors, WPA MIC errors, shunned clients, and IPSEC failures.
- Client Traffic—Displays the trend of client traffic in a given time period.
- Client Troubleshooting—Allows you to enter a MAC address of a client and retrieve information for diagnosing the client in the network.
- Clients Detected by Context Aware Service—Displays the client count detected by the context aware service within the previous 15 minutes.
- Controller CPU Utilization (%)— Displays the average, maximum, and minimum CPU usage.
- Controller Memory Utilization—Displays the average, maximum, and minimum memory usage as a percentage for the controllers.
- Coverage Areas
- Friendly Rogue APs—Displays friendly rogue access points for the previous hour, previous 24 hours, and total active.
- Guest Users Count

- Inventory Detail Status
 - Inventory Status—Displays the total number of client controllers and the number of unreachable controllers.
 - LWAPP Uptime—Displays the access point name and the amount of its uptime in days, minutes, and seconds.
 - Latest 5 Logged in Guest Users
 - MFP Attacks
 - Malicious Rogue APs
 - Mesh AP by Hop Count
 - Mesh AP Queue Based on QoS
 - Mesh Parent Changing AP—Displays the access point name, the parent name, and the number of changes made per minute.
 - Mesh Top Over Subscribed AP
 - Mesh Worst Node Hop Count
 - Mesh Worst Packet Error Rate
 - Mesh Worst SNR Link
 - Most Recent AP Alarms—Displays the five most recent access point alarms. Click the number in parentheses to open the Alarms page which shows all alarms.
 - Most Recent Client Alarms
 - Most Recent Mesh Alarms
 - Most Recent Security Alarms—Displays the five most recent security alarms. Click the number in parentheses to open the Alarms page.
 - Recent 5 Guest User Accounts
 - Recent Alarms—Displays the five most recent alarms by default. Click the number in parentheses to open the Alarms page.
 - Recent Coverage Holes
 - Recent Malicious Rogue AP Alarms
 - Recent Rogue Alarms—Displays the five most recent rogue alarms. Click the number in parentheses to open the Alarms page which shows alarms.
 - Security Index
 - Top APs by Client Count
 - Unclassified Rogue APs—Displays unclassified rogue access points for the previous hour, previous 24 hours, and total active.
-

Guest Components for WCS Home Page

The following guest user components are also available for the WCS home page General tab using the Edit Contents feature:

Table 2-5 *Guest User Components*

Component	Description
Guest User Accounts	Status of the last five WCS guest accounts configured on the network. Account information includes the guest username, the time and date the account was created, who created or modified the account, the lifetime of the account (days, minutes, and seconds), and the account status (active, scheduled, not active, expired).
Currently Logged Guest Users	List of guest users that are currently logged into the network. Guest user information includes guest username, profile name, date and time the guest user associated with WCS, and the amount of time remaining before the account expires.
Guest Count	Interactive graph showing the number of guest users in the network.

Using the Cisco WCS User Interface

A typical Cisco WCS user interface page consists of these elements:

- [Icons, page 2-28](#)
- [Menu Bar, page 2-29](#)
- [Sidebar Area, page 2-30](#)
- [Command Buttons, page 2-30](#)
- [Main Data Page, page 2-31](#)
- [Alarm Summary, page 2-30](#)
- [Administrative Tools, page 2-31](#)
- [Using the Search Feature, page 2-31](#)

Icons

The icons on the WCS home page and within the General, Client, Security, and Mesh tabs have the following functions.

Client Tab Icon	Description
	The Component Options icon enables you to filter the data by variables. For example, you can compare client count trends for SSIDs, floor areas, controllers, and so on.
	The Refresh Component icon enables you to automatically adjust the dashboard so that it reflects the current network status.
	The View in Chart icon enables you to view the component in chart rather than table form.
	The View in Grid icon enables you to view the component in a table rather than chart form.

Menu Bar

There are seven menus on each page: **Monitor**, **Reports**, **Configure**, **Services**, **Administration**, **Tools**, and **Help**. When you move the mouse over any of the heading, a drop-down list appears.

Monitor Menu

The Monitor menu provides you with a top-level description of the devices on your network. You can monitor your network, maps, Google Earth maps, various devices (controllers, access points, clients, tags, chokepoints, Wi-Fi TDOA receivers), RRM, alarms, and events.

Configure Menu

The Configure menu enables you to configure templates, controllers, access points, Ethernet switches, chokepoints, Wi-Fi TDOA receivers, config groups, auto provisioning, scheduled configuration tasks, profiles, ACS view servers, and TFTP servers on your network.

Administration Menu

The Administration menu enables you to schedule tasks like making a backup, checking a device status, auditing your network, synchronizing the MSE, and so on. It also contains Logging to enable various logging modules and specify restart requirements. For user administration such as changing passwords, establishing groups, setting application security settings, and so on, choose AAA. From the Administration Menu, you can also access the licensing information, set user preferences, and establish high availability (a secondary backup device running WCS).

Tools Menu

The Tools Menu covers voice audit, location accuracy, config audit, and migration analysis.

Help Menu

Clicking **Help > Online Help** enables you to view online help. The online help is context sensitive and will open to documentation for the WCS window that you currently have open.

Clicking **Help > Learning Modules** allows you to access short video clips of certain WCS features.

Clicking **Help > Submit Feedback** allows you to access a page where you can enter feedback on the WCS product.

Clicking **Help > About WCS** allows you to verify the version of WCS that you are running. It provides the version, host name, feature, AP limit, and type.

Sidebar Area

The sidebar area enables you to choose a new configuration page under the currently selected menu area. You may choose to display or configure any of the available data. The selector area options vary based on which menu you have chosen.

Some pages contain a group of menus in this area. Click the menu item to reveal a submenu and then click the item to choose it.

Command Buttons

The Cisco WCS user interface uses a number of command buttons throughout its pages. The most common of these are as follows:

- **Apply to Controllers:** Applies the selected information to the controllers
- **Delete:** Deletes the selected information
- **Cancel:** Cancels new information entered on the current page and returns to the previous page
- **Save:** Saves the current settings
- **Audit:** Discovers the present status of this access point
- **Place AP:** Audits the configuration of the selected entity by flagging the differences between WCS database device configurations

Alarm Summary

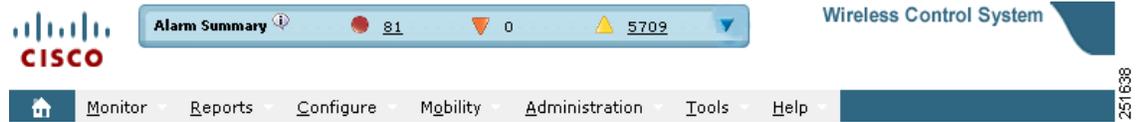
When WCS receives an alarm message from a controller, it displays an alarm indicator at the top of the WCS window (see [Figure 2-11](#)).

**Note**

The Administration > Settings > Alarms page has a Hide Acknowledged Alarms check box. You must unselect it if you want acknowledged alarms to appear in the WCS Alarm Summary and alarms lists page. By default, acknowledged alarms are not shown.

Critical (red), Major (orange) and Minor (yellow) alarms appear in the alarm dashboard, left to right.

Figure 2-11 WCS Alarm Summary



Alarms indicate the current fault or state of an element that needs attention, and they are usually generated by one or more events. The alarm can be cleared but the event remains.

**Note**

Alarm counts are refreshed every 15 seconds.

Main Data Page

The main data page is determined by the required parameter information. Active areas on the data pages include the following:

- Text boxes into which data may be entered using the keyboard
- Pull-downs from which one of several options may be chosen
- Check boxes in lists allow you to choose one or more items from the displayed list
- Radio buttons allow you to turn a parameter on or off
- Hyperlinks take you to other pages in the Cisco WCS user interface

Input text boxes are black text on a white background. When data is entered or selected, it is not sent to the controller, but it is saved in the text box until you click Go.

Administrative Tools

This area provides shortcuts to administration functions (such as logged in as, logout, refresh, and help) that you use regularly when configuring a controller through the web user interface.

Using the Search Feature

The enhanced WCS Search feature (see [Figure 2-12](#)) provides easy access to advanced search options and saved searches. You can access the search options from any page within WCS making it easy to search for a device or SSID (Service Set Identifier).

Figure 2-12 WCS Search Feature



Quick Search

For a quick search, you can enter a partial or complete IP address, MAC address, name, or SSID for clients, alarms, access points, controllers, maps, tags, or rogue clients (see [Figure 2-12](#)).



Note

You can also enter a username if you are searching for a client.

To quickly search for a device, follow these steps:

- Step 1** Enter the complete or partial IP address, device name, SSID, or MAC address of the device in the quick Search text box (see [Figure 2-13](#)).

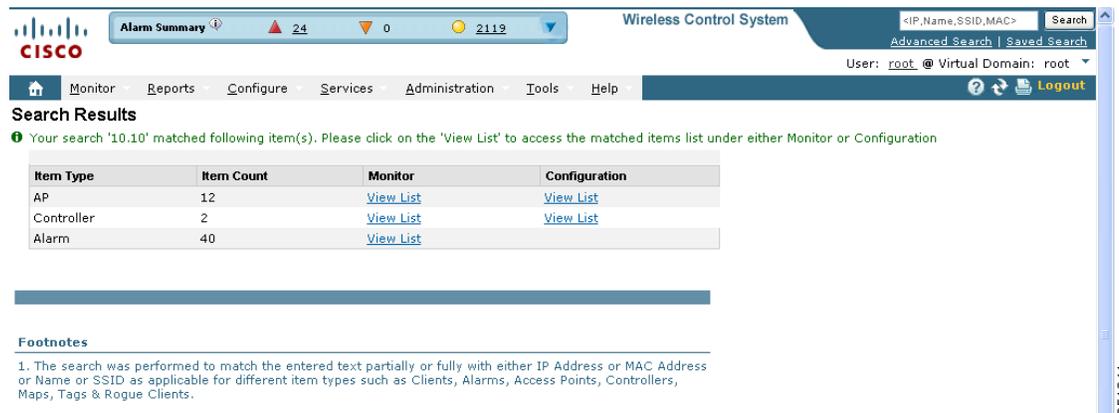
Figure 2-13 Quick Search with Partial IP Address



- Step 2** Click **Search** to display all devices that match the Quick Search parameter.

The search results display the matching item type, the number of items that match your search parameter, and links to the list of matching results (see [Figure 2-14](#)). Click **View List** to view the matching devices from the Monitor or Configuration pages.

Figure 2-14 Quick Search Results Advanced Search



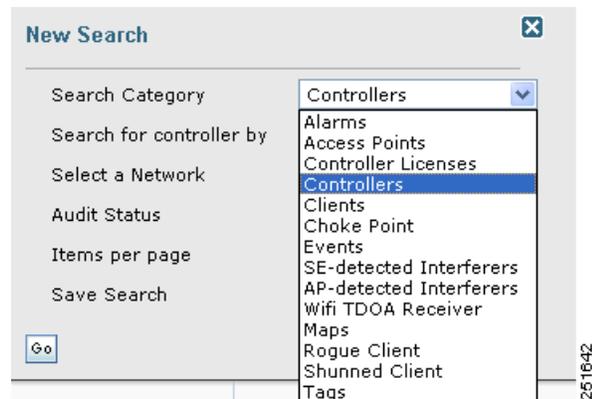
Advanced Search

To perform a more specific search for a device in WCS, follow these steps:

- Step 1** Click **Advanced Search** located in the top right corner of WCS (see [Figure 2-12](#)).

Step 2 In the New Search page, select a category from the Search Category drop-down list (see [Figure 2-15](#)).

Figure 2-15 Search Category Drop-Down List



Note Click each of the following category for more information.

Search categories include:

- [Alarms](#)
- [Access Points](#)
- [Controllers](#)
- [Clients](#)
- [Chokepoints](#)
- [Events](#)
- [SE-Detected Interferers](#)
- [Wi-Fi TDOA Receivers](#)
- [Maps](#)
- [Rogue Clients](#)
- [Shunned Clients](#)
- [Tags](#)
- [Controller Licenses](#)

Step 3 Select all applicable filters or parameters for your search (see [Figure 2-16](#)).



Note Search parameters change depending on the selected category. The following pre-defined search filters have been added in release 6.0: Associated Clients, Authenticated Clients, Excluded Clients, Probing Clients, All Clients, New Clients detected in last 24 hours, unauthenticated clients, 2.4 GHz clients, and 5 GHz clients.

Figure 2-16 *New Search Parameters*

The screenshot shows a 'New Search' dialog box with the following fields and values:

- Search Category: Controllers
- Search for controller by: Networks
- Select a Network: All Networks
- Audit Status: All Status
- Items per page: 50
- Save Search: (with an empty text box next to it)

A 'Go' button is located at the bottom left of the dialog box. A vertical ID number '251643' is visible on the right side of the dialog box.

- Step 4** Choose the number of items to display on the results page.
- Step 5** To save this search, select the **Save Search** check box and enter a name for the search in the text box.
- Step 6** When all filters and parameters are set, click **Go**.

Alarms

You can configure the following parameters when performing an advanced search for alarms (see [Table 2-6](#)):

Table 2-6 *Search Alarms Parameters*

Parameter	Options
Severity	Choose All Severities, Critical, Major, Minor, Warning, or Clear.
Alarm Category	Choose All Types, Access Points, Controller, Coverage Hole, Config Audit, Mobility Service, Context Aware Notifications, Interference, Mesh Links, Rogue AP, Adhoc Rogue, Security, WCSm or Performance.
Time Period	Choose a time increment from Any Time to Last 7 days. Default is Any Time.

Table 2-6 Search Alarms Parameters (continued)

Parameter	Options
Acknowledged State	Check to search for alarms with an Acknowledged or Unacknowledged state. If this check box is not selected, the acknowledged state is not taken into search criteria consideration.
Assigned State	Check to search for alarms with an Assigned or Unassigned state or by Owner Name. If this check box is not selected, the assigned state is not part of the search criteria. Note If you choose Assigned State > Owner Name, type the owner name in the available text box.

**Note**

You can decide what information displays on the alarm search results page. See the “[Configuring the Search Results Display](#)” section on page 2-44 for more information.

See the “[Monitoring Alarms](#)” section on page 16-5 for more information on alarms.

Access Points

You can configure the following parameters when performing an advanced search for access points (see [Table 2-7](#)):

Table 2-7 Search Access Points Parameters

Parameter	Options
Search By	Choose All APs, Base Radio MAC, Ethernet MAC, AP Name, IP Address, Controller Name, Controller IP, All Unassociated APs, Floor Area, Outdoor Area, Unassigned APs, or Alarms. Note Search parameters may change depending on the selected category. When applicable, enter the additional parameter or filter information to help identify the Search By category. For example, when you select Floor Area, you also must identify its campus and building. Or, if you select Alarms, you can search for access points based on the severity of the alarm.
AP Type	Choose All Types, LWAPP, or Autonomous.
AP Mode	Choose All Modes, Local, Monitor, H-REAP, Rogue Detector, Sniffer, Bridge, or SE-Connect.
Radio Type	Choose All Radios, 802.11a, or 802.11b/g.

Table 2-7 Search Access Points Parameters (continued)

Parameter	Options
802.11n Support	Check to search for access points with 802.11n support.
OfficeExtend AP Enabled	Check to search for OfficeExtend access points.

**Note**

You can decide what information displays on the access points search results page. See the [“Configuring the Search Results Display”](#) section on page 2-44 for more information.

Controllers

You can configure the following parameters when performing an advanced search for controllers (see [Table 2-8](#)):

Table 2-8 Search Controllers Parameters

Parameter	Options
Search for controller by	Choose All Controllers, IP Address, Controller Name, or Network. Note Search parameters may change depending on the selected category. When applicable, enter the additional parameter or filter information to help identify the Search By category.
Enter Controller IP Address	This text box appears only if you select IP Address from the Search for controller by text box.
Enter Controller Name	This text box appears only if you select Controller Name from the Search for controller by text box.
Select a Network	Choose All Networks or an individual network.
Audit Status	Choose one of the following from the drop-down list: <ul style="list-style-type: none"> All Status Mismatch—Config differences were found between WCS and controller during the last audit. Identical—No config differences were found during the last audit. Not Available—Audit status is unavailable.

**Note**

You can decide what information displays on the controllers search results page. See the [“Configuring the Search Results Display”](#) section on page 2-44 for more information.

Clients

You can configure the following parameters when performing an advanced search for clients (see [Table 2-9](#)):

Table 2-9 Search Clients Parameters

Parameter	Options
Search By	<p>Choose All Clients, All Excluded Clients, All Wired Clients, All Logged in Guests, IP Address, User Name, MAC Address, Asset Name, Asset Category, Asset Group, AP Name, Controller Name, Controller IP, MSE IP, Floor Area, or Outdoor Area.</p> <p>Note Search parameters may change depending on the selected category. When applicable, enter the additional parameter or filter information to help identify the Search By category. For example, when you select IP address, you must enter the specific IP address for this search.</p>
Clients Detected By	<p>Choose WCS or MSEs.</p> <p>Clients detected by WCS—Clients stored in WCS databases.</p> <p>Clients detected by MSE—Clients stored on the mobility services engine that were detected by the MSE through controller polling.</p>
Client States	Choose All States, Idle, Authenticated, Associated, Probing, or Excluded.
Restrict By Radio Band	Select the check box to indicate a specific radio band. Choose 5 GHz or 2.4 GHz from the drop-down list.
Restrict By Protocol	Select the check box to indicate a specific protocol. Choose 802.11a, 802.11b, 802.11g, 802.11n, or Mobile from the drop-down list.
Search on Controllers Now	<p>Select the check box to indicate a search for clients on current controllers.</p> <p>Note When selected, the CCX and E2E Compatible check boxes become unavailable.</p>
SSID	Select the check box and choose the applicable SSID from the drop-down list.
Profile	<p>Select the check box to list all of the clients associated to the selected profile.</p> <p>Note Once the check box is selected, choose the applicable profile from the drop-down list.</p>

Parameter	Options
CCX Compatible	Select the check box to search for clients that are compatible with Cisco Client Extensions. Note Once the check box is selected, choose the applicable version, All Versions, or Not Supported from the drop-down list.
E2E Compatible	Select the check box to search for clients that are End to End compatible. Note Once the check box is selected, choose the applicable version, All Versions, or Not Supported from the drop-down list.
NAC State	Select the check box to search for clients identified by a certain Network Admission Control (NAC) state. Note Once the check box is selected, choose the applicable state from the drop-down list. Select from Quarantine, Access, Invalid, and Not Applicable.
Include Disassociated	Select to include clients that are no longer on the network but for which WCS has historical records.

**Note**

You can decide what information displays on the client search results page. See the [“Configuring the Search Results Display”](#) section on page 2-44 for more information.

Chokepoints

You can configure the following parameters when performing an advanced search for chokepoints (see [Table 2-10](#)):

Table 2-10 Search Chokepoint Parameters

Parameter	Options
Search By	Choose MAC Address or Chokepoint Name. Note Search parameters may change depending on the selected category. When applicable, enter the additional parameter or filter information to help identify the Search By category. For example, when you select MAC address, you must enter the specific MAC address for this search.

Events

You can configure the following parameters when performing an advanced search for events (see [Table 2-11](#)):

Table 2-11 Search Events Parameters

Parameter	Options
Severity	Choose All Severities, Critical, Major, Minor, Warning, Clear, or Info. Color coded.
Event Category	Choose All Types, Access Points, Controller, Security, Coverage Hole, Rogue AP, Adhoc Rogue, Interference, Mesh Links, Client, Mobility Service, Location Notifications, Pre Coverage Hole, or WCS.

See the “[Monitoring Rogue Alarm Events](#)” section on page 16-22 for more information on events.

SE-Detected Interferers

You can configure the following parameters when performing an advanced search for interferers detected by access points (see [Table 2-12](#)):

Table 2-12 Search SE-Detected Interferers Parameters

Parameter	Options
Search By	Choose All Interferers, Interferer ID, Interferer Category, Interferer Type, Affected Channel, Affected AP, Severity, Power, or Duty Cycle. Note Search parameters may change depending on the selected category. When applicable, enter the additional parameter or filter information to help identify the Search By category.
Detected By	Choose All Spectrum Experts or a specific spectrum expert from the drop-down list.
Detected within the last	Choose the time range for the interferer detections. The times range from 5 minutes to 24 hours to All History.
Active Interferers Only	Select the check box to only include active interferers in your search.

You can decide what information displays on the SE-detected interferers search results page. See the “[Configuring the Search Results Display](#)” section on page 2-44 for more information.

AP-Detected Interferers

You can configure the following parameters when performing an advanced search for interferers detected by access points (see [Table 2-13](#)):

Table 2-13 Search AP-Detected Interferers Parameters

Parameter	Options
Search By	Choose All Interferers, Interferer ID, Interferer Type, Affected Channel, Severity, Duty Cycle, or Location. Note Search parameters may change depending on the selected category. When applicable, enter the additional parameter or filter information to help identify the Search By category.
Detected within the last	Choose the time range for the interferer detections. The times range from 5 minutes to 24 hours to All History.
Active Interferers Only	Select the check box to only include active interferers in your search.

**Note**

You can decide what information displays on the AP-detected interferers search results page. See the [“Configuring the Search Results Display”](#) section on page 2-44 for more information.

Wi-Fi TDOA Receivers

You can configure the following parameters when performing an advanced search for Wi-Fi TDOA receivers (see [Table 2-14](#)):

Table 2-14 Search Wi-Fi TDOA Receivers Parameters

Parameter	Options
Search By	Choose MAC Address or Wi-Fi TDOA Receivers Name. Note Search parameters may change depending on the selected category. When applicable, enter the additional parameter or filter information to help identify the Search By category.

Maps

You can configure the following parameters when performing an advanced search for maps (see [Table 2-15](#)):

Table 2-15 Search Map Parameters

Parameter	Options
Search for	Choose All Maps, Campuses, Buildings, Floor Areas, or Outdoor Areas.
Map Name	Search by Map Name. Enter map name in the text box.



Note

You can decide what information displays on the maps search results page. See the [“Configuring the Search Results Display”](#) section on page 2-44 for more information.

See the [“Monitoring Maps Overview”](#) section on page 5-2 for more information on maps.

Rogue Clients

You can configure the following parameters when performing an advanced search for rogue clients (see [Table 2-16](#)):

Table 2-16 Search Rogue Client Parameters

Parameter	Options
Search By	Choose All Rogue Clients, MAC Address, Controller, MSE, Floor Area, or Outdoor Area.
Search In	Choose MSEs or WCS Controllers.
Status	Select the check box and choose Alert, Contained, or Threat from the drop-down list to include status in the search criteria.

See the [“Monitoring Rogue Access Points, Ad hoc Events, and Clients”](#) section on page 3-9 for more information on rogue clients.

Shunned Clients



Note

When a Cisco IPS sensor on the wired network detects a suspicious or threatening client, it alerts the controller to shun this client.

You can configure the following parameters when performing an advanced search for shunned clients (see [Table 2-17](#)):

Table 2-17 Search Shunned Client Parameters

Parameter	Options
Search By	Choose All Shunned Clients, Controller, or IP Address. Note Search parameters may change depending on the selected category. When applicable, enter the additional parameter or filter information to help identify the Search By category.

Tags

You can configure the following parameters when performing an advanced search for tags (see [Table 2-18](#)):

Table 2-18 Search Tags Parameters

Parameter	Options
Search By	Choose All Tags, Asset Name, Asset Category, Asset Group, MAC Address, Controller, MSE, Floor Area, or Outdoor Area. Note Search parameters may change depending on the selected category. When applicable, enter the additional parameter or filter information to help identify the Search By category.
Search In	Choose MSEs or WCS Controllers.
Last detected within	Choose a time increment from 5 minutes to 24 hours. Default is 15 minutes.
Tag Vendor	Select the check box and choose Aeroscout, G2, PanGo, or WhereNet.
Telemetry Tags only	Check the Telemetry Tags only to search tags accordingly.

Controller Licenses

You can configure the following parameters when performing an advanced search for controller licenses (see [Table 2-19](#)):

Table 2-19 Search Controller Licenses Parameters

Parameter	Options
Controller Name	Type the controller name associated with the license search.
Feature Name	Choose All, Plus, or Base depending on the license tier.
Type	Choose All, Demo, Extension, Grace Period, or Permanent.
% Used or Greater	Select the percentage of the license use. The percentages range from 0 to 100.

See the “[Accessing the License Center](#)” section on page 18-67 for more information on licenses and the License Center.

Saved Searches

The Saved Search feature enables you to access and run any previously saved search (see [Figure 2-17](#)).



Note

When saving a search, you must assign a unique name to the search.



Note

Saved searches apply only to the current partition.

Figure 2-17 Saved Search Page

The screenshot shows a 'Saved Search' dialog box with the following fields and values:

- Search Category: Controllers
- Saved Search List: -Select Saved-
- Search for controller by: Networks
- Select a Network: All Networks
- Audit Status: All Status
- Items per page: 20

A 'Go' button is located at the bottom left of the dialog box. A vertical ID number '275975' is visible on the right side of the dialog box.

To access and run a saved search, follow these steps:

Step 1 Click **Saved Search**.

- Step 2** Select a category from the Search Category drop-down list.
- Step 3** Select a saved search from the Saved Search List drop-down list.
- Step 4** If necessary, change the current parameters for the saved search.
- Step 5** Click **Go**.

Configuring the Search Results Display

The Edit View page (see [Figure 2-18](#)) enables you to choose which columns appear in the Search Results page.

Figure 2-18 Edit View Page



Column names appear in one of the following lists:

- Hide Information—Lists columns that do not appear in the table. The **Hide** button points to this list.
- View Information—Lists columns that do appear in the table. The **Show** button points to this list.

To display a column in a table, click it in the Hide Information list, then click **Show**. To remove a column from a table, click it in the View Information list, then click **Hide**. You can select more than one column by holding down the shift or control key.

To change the position of a column in the View Information list, click it, then click **Up** or **Down**. The higher a column is in the list, the farther left it appears in the table.

Command Buttons

The following command buttons appear in the Edit View page:

- Reset—Sets the table to the default display.
- Show—Moves the highlighted columns from the Hide Information list to the View Information list.

- Hide—Moves the highlighted columns from the View Information list to the Hide Information list.
- Up—Moves the highlighted columns upward in the list (further to the left in the table).
- Down—Moves the highlighted columns downward in the list (further to the right in the table).
- Submit—Saves the changes to the table columns and returns to the previous page.
- Cancel—Undoes the changes to the table columns and returns to the previous page.

