CHAPTER 2

Getting Started

This chapter describes information on system requirements, setting up and starting the NCS. The NCS is an application used to configure, manage, and monitor the wired and wireless networks. This chapter contains the following sections:

- NCS Delivery Modes, page 2-1
- Reinstalling NCS on Physical Appliance, page 2-5
- Deploying the NCS Virtual Appliance, page 2-5
- Setting Up NCS, page 2-9
- Starting the NCS Server, page 2-10
- Logging into the NCS User Interface, page 2-11
- Applying the NCS Software License, page 2-12
- Understanding NCS Home Page, page 2-13
- Using the Search Feature, page 2-33

NCS Delivery Modes

Cisco NCS comes preinstalled on a physical appliance with various performance characteristics. The NCS software runs on either a dedicated Cisco Prime Network Control System appliance or on a VMware server. The NCS software image does not support the installation of any other packages or applications on this dedicated platform. The inherent scalability of NCS allows you to add appliances to a deployment and increase performance and resiliency.

NCS is delivered in two modes, the Physical Appliance and Virtual Appliance. This section contains the following topics:

- Physical Appliance, page 2-2
- Virtual Appliance, page 2-2
- Operating Systems Requirements, page 2-3
- Client Requirements, page 2-4
- Prerequisites, page 2-4

Physical Appliance

The Physical Appliance is a dual Intel 2.40GHz Xeon E5620 quad core processor, with 16 GB RAM, and four hard drives running in a RAID level 5 configuration. The appliance will run the latest 64bit Red Hat Linux Operating System.

The Physical Appliance supports up to 15000 Cisco Aironet lightweight access points, 5000 standalone access points, 5000 switches and 1200 Cisco wireless LAN controllers.

Note To receive the expected results with NCS, you should run on High performance Physical appliance with built-in redundancy for hard disks, power supplies and internal cooling fans.

For more information on the Physical Appliance, see *Cisco Prime Network Control System Getting Started Guide, Release 1.0*.

Virtual Appliance

NCS is also offered as a Virtual Appliance, to help support lower level deployments. Cisco NCS can be run on a workstation or a server, and access points can be distributed unevenly across controllers.

The NCS Virtual Appliance software is distributed as an Open Virtualization Archive (OVA) file. There are three recommended levels of NCS distribution with different resources, and numbers of devices supported.

This section contains the following topics:

- Virtual Appliance for Large Deployment, page 2-2
- Virtual Appliance for Medium Deployment, page 2-3
- Virtual Appliance for Small Deployment, page 2-3

Note You can deploy the OVA file directly from the vSphere Client; you do not need to extract the archive before performing the deployment.

You can install NCS Virtual Appliance using any of the method for deploying an OVF supported by the VMware environment. Before starting, make sure that the NCS Virtual Appliance distribution archive is in a location that is accessible to the computer on which you are running the vSphere Client.

Note For more information about setting up your VMware environment, see the VMware vSphere 4.0 documentation.

Virtual Appliance for Large Deployment

- Supports up to 15000 Cisco Aironet lightweight access points, 5000 standalone access points, 5000 switches and 1200 Cisco wireless LAN controllers.
- 8 Processors at 2.93 GHz or better.
- 16-GB RAM.
- 400 GB minimum free disk space is needed on your hard drive.

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

Virtual Appliance for Medium Deployment

- Supports up to 7500 Cisco Aironet lightweight access points, 2500 standalone access points, 2500 Switches and 600 Cisco wireless LAN controllers.
- 4 Processors at 2.93 GHz or better.
- 12-GB RAM.
- 300 GB minimum free disk space is needed on your hard drive.

Virtual Appliance for Small Deployment

- Supports up to 3000 Cisco Aironet lightweight access points, 1000 standalone access points, 1000 Switches and 240 Cisco wireless LAN controllers.
- 2 Processors at 2.93 GHz or better.
- 8-GB RAM.
- 200 GB minimum free disk space is needed on your hard drive.

Note For all server levels, AMD processors equivalent to the listed Intel processors are also supported.

Note The free disk space listed is a minimum requirement, but several variables (such as backups) impact the disk space.

Note If you want to use a Cisco UCS Server to deploy a virtual appliance for Cisco Prime NCS, you can use the UCS C-Series or B-Series. Make sure the server you pick matches to the Processor, RAM and Hard Disk requirements specified in "Virtual Appliance" section on page 2-2 deployment.

Operating Systems Requirements

The following operating systems are supported:

- Red Hat Linux Enterprise Server 5.4 64-bit operating system installations are supported.

  Note You cannot install NCS on a standalone operating system, like Red Hat Linux, as NCS is shipped as a physical or a virtual appliance that comes preinstalled with a secure and hardened Operating System.

- Red Hat Linux version support on VMware ESX version 3.0.1 and later with either local storage or SAN over fiber channel.

- The recommended deployments for virtual appliance are UCS and ESX/ESXi.

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

Client Requirements

The NCS user interface requires Mozilla Firefox 3.6 or later or Microsoft Internet Explorer 8 with the Google Chrome plugin. Microsoft Internet Explorer 6.0 is not supported.

Note We strongly advise that you do not enable third-party browser extensions. In Internet Explorer, you can disable third-party browser extensions by choosing **Tools > Internet Options** and unselecting the **Enable third-party browser extensions** check box from the Advanced tab.

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 minimum screen resolution that is recommended for NCS and use it as 1024 x 768 pixels.

Prerequisites

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

- Meet the necessary hardware and software requirements for Cisco NCS.
- Check the Compatibility Matrix for supported Controller, IOS versions.
- 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 NCS.

- To receive the expected results, you should run no more than 3 concurrent NCS setups for standard server use (4 GB memory and 3 GHz CPU speed) and no more than 5 concurrent NCS 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.

Reinstalling NCS on Physical Appliance

You must have root privileges to install NCS on Physical Appliance.

Step 1 Insert the NCS software Image DVD provided to you. The system boots up and the following console screen appears.

```
ISOLINUX 3.11 2005-09-02  Copyright (C) 1994-2005 H. Peter Anvin

           Welcome to Cisco Prime Network Control System

To boot from hard disk, press <Enter>.

Available boot options:

  [1] Network Control System Installation (Keyboard/Monitor)
  [2] Network Control System Installation (Serial Console)
  [3] Recover administrator password. (Keyboard/Monitor)
  [4] Recover administrator password. (Serial Console)
  <Enter> Boot existing OS from Hard Disk.

Enter boot option and press <return>.

boot:
```

Step 2 Select the option 1 to reinstall the NCS software Image. The system will reboot and take you to configure appliance screen.

Step 3 Enter the initial setup parameters and the system will reboot again. Remove the DVD and follow the steps to start the NCS server.

Deploying the NCS Virtual Appliance

This section describes how to deploy NCS Virtual Appliance both from the vSphere Client using the Deploy OVF Wizard or from the command line.(VMware vSphere Client, a Windows application for managing and configuring the vCenter Server) This section contains the following topics:

- Deploying the NCS Virtual Appliance from the VMware vSphere Client, page 2-6
- Deploying NCS Virtual Appliance using the Command Line Client, page 2-9

Deploying the NCS Virtual Appliance from the VMware vSphere Client

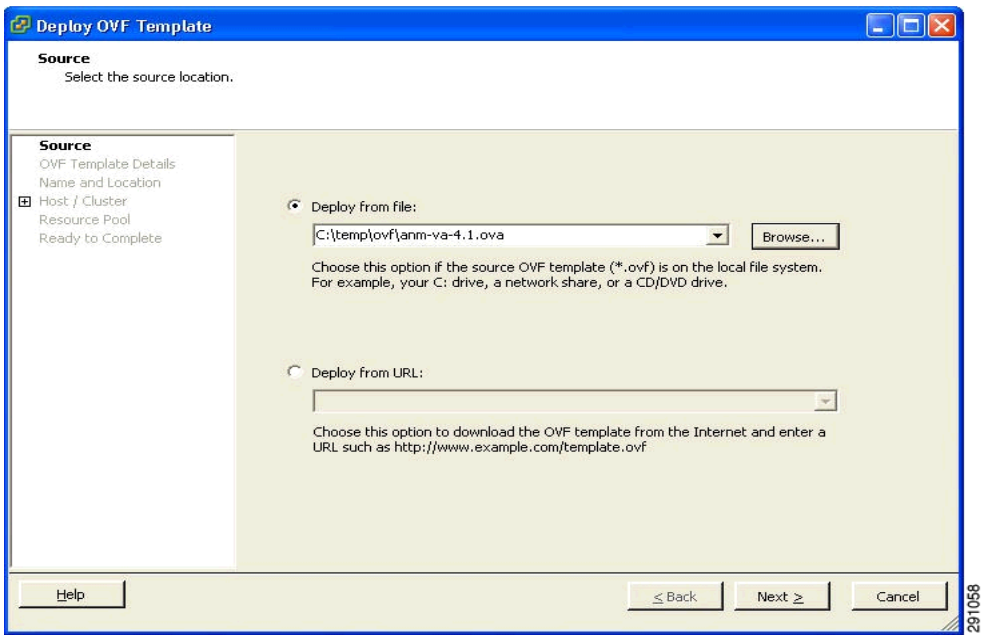
NCS Virtual Image is packaged as an OVA file. An OVF is a collection of items in a single archive. In the vSphere Client, you can use the Deploy OVF Wizard to create a virtual machine, running the NCS Virtual Appliance application, as described in this section.

Note While the following procedure provides a general guideline for how to deploy NCS Virtual Appliance, the exact steps that you need to perform may vary depending on the characteristics of your VMware environment and setup.

To deploy the NCS Virtual Appliance, follow these steps:

Step 1 From the VMware vSphere Client main menu, choose **File > Deploy OVF Template**. The Deploy OVF Template Source window appears: (See Figure 2-1)

Figure 2-1 Deploy OVF Template window

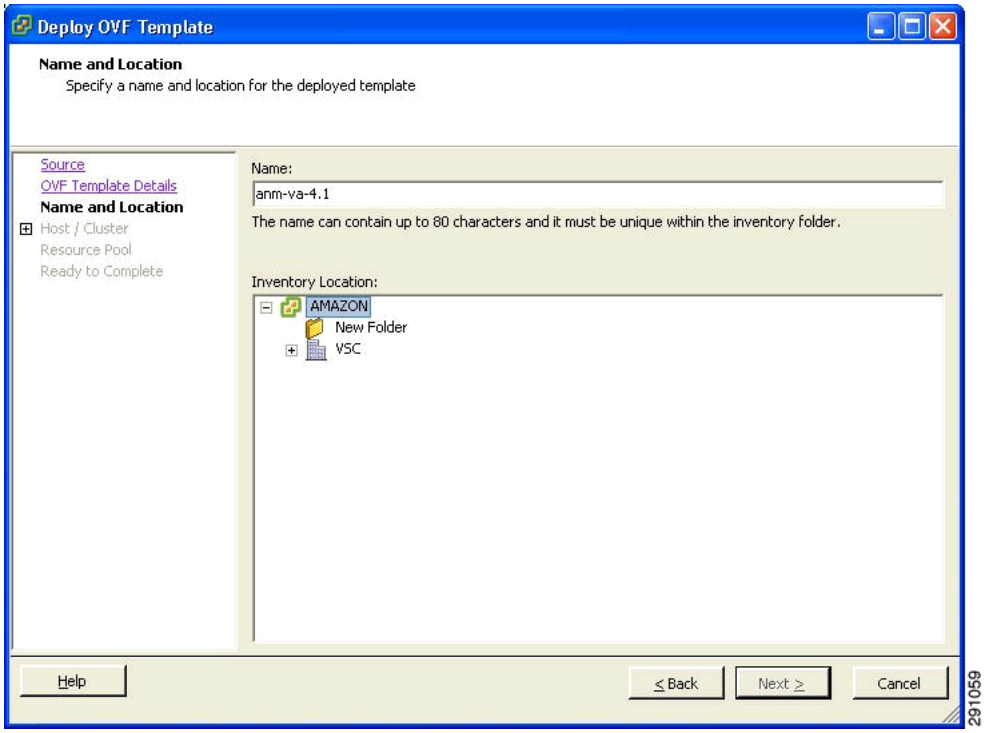


Step 2 Choose **Deploy from file** and choose the OVA file that contains the NCS Virtual Appliance distribution.

Step 3 Click **Next**. The OVF Template Details window appears. VMware ESX/ESXi reads the OVA attributes. The details include the product you are installing, the size of the OVA file (download size), and the amount of disk space that needs to be available for the virtual machine (size on disk).

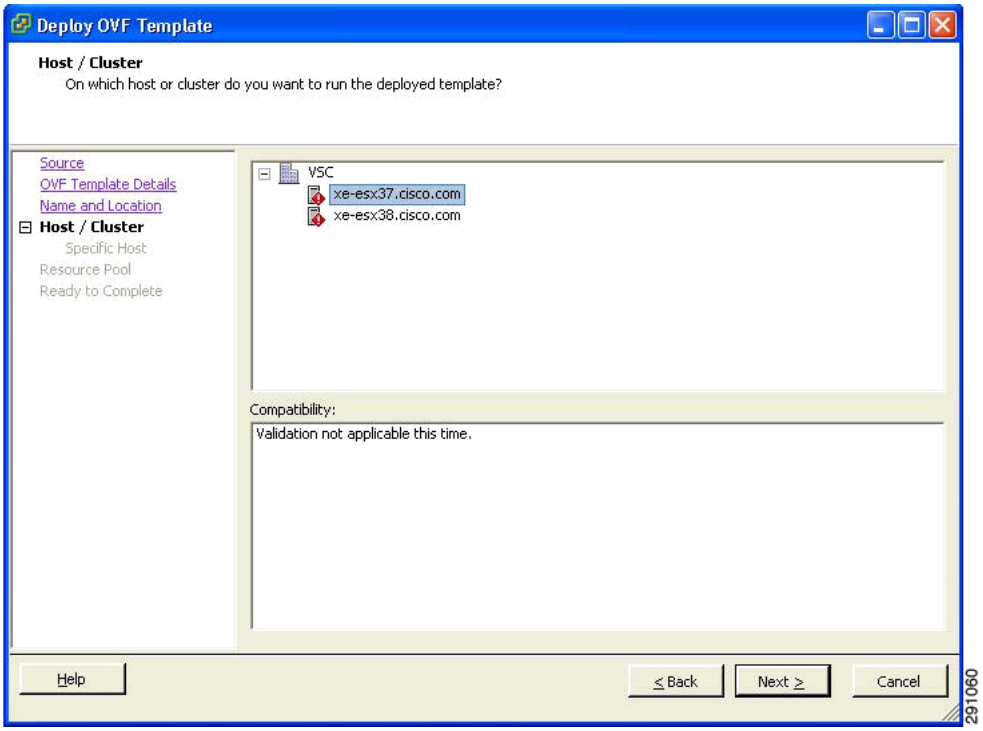
Step 4 Verify the OVF Template details and click **Next**. The Name and Location window appears (See Figure 2-2).

Figure 2-2 Name and Location window



Step 5 Either keep the default name for the VM to be deployed in the Name text box or provide a new one and click **Next**. This name value is used to identify the new virtual machine in the VMware infrastructure so you should use any name that distinguishes this particular VM in your environment.The Host / Cluster window appears (see Figure 2-3).

Figure 2-3 Host/Cluster Window



Step 6 Choose the destination host or HA cluster on which you want to deploy the NCS VM and click **Next**. The Resource Pool window appears.

Step 7 If you have more than one resource pool in your target host environment, choose the resource pool to use for the deployment and click **Next**. The Ready to Complete window appears.

Step 8 Review the settings shown for your deployment and, if needed, click the **Back** button to modify any of the settings shown.

Step 9 Click **Finish** to complete the deployment. A message notifies you when the installation completes and you can see the NCS Appliance in your inventory.

Step 10 Click **Close** to dismiss the Deployment Completed Successfully dialog box.

Configuring the Basic Settings for NCS Virtual Appliance

You have completed deploying (installing) NCS Virtual Appliance on a new virtual machine. A node for the virtual machine now appears in the resource tree in the VMware vSphere Client window. Deploying the OVF template creates a new virtual machine in vCenter with the NCS Virtual Appliance application and related resources already installed on it. After deployment, you need to configure basic settings for NCS Virtual Appliance. To start the NCS setup, follow these steps:

Step 1 In the vSphere Client, click the NCS Virtual Appliance node in the resource tree. The virtual machine node should appear in the Hosts and Clusters tree below the host, cluster, or resource pool to which you deployed NCS Virtual Appliance.

Step 2 On the Getting Started tab, click the **Power on the virtual machine** link under Basic Tasks. The Recent Tasks pane at the bottom of the vSphere Client pane indicates the status of the task associated with powering on the virtual machine. After the virtual machine successfully starts, the status column for the task displays Completed.

Step 3 Click the **Console** tab, within the console pane to make the console prompt active for keyboard input.

Now you need to set up the virtual appliance, as described in Setting Up NCS, page 2-9 section.

Deploying NCS Virtual Appliance using the Command Line Client

This section describes how to deploy the NCS Virtual Appliance from the command line. As an alternative to using the vSphere Client to deploy the NCS OVA distribution, you can use the VMware OVF Tool, which is a command-line client.

To deploy an OVA with the VMware OVF Tool, use the **ovftool** command, which takes the name of the OVA file to be deployed and the target location as arguments, as in the following example:

```
ovftool NCS-VA-X.X.X-large.ova vi://my.vmware-host.example.com/
```

In this case, the OVA file to be deployed is NCS-VA-X.X.X-large.ova and the target ESX host is my.vmware-host.example.com. For complete documentation on the VMware OVF Tool, see the VMware vSphere 4.0 Documentation.

Setting Up NCS

This section describes how to configure the initial settings of the NCS Virtual Appliance.

Note These steps need to be performed only once, upon first installation of NCS Virtual Appliance.

To configure the basic network and login settings for the NCS Virtual Appliance system, follow the below steps. When the steps are completed, the NCS Virtual Appliance is accessible over the network.

Note Once you put the NCS Image DVD in the physical appliance for reinstallation, you will get the same console prompt. Use the following steps to reinstall NCS for the physical appliance.

Step 1 At the login Prompt, enter **setup**.

```
localhost.localdomain login: setup
```

The NCS configuration script starts. The script takes you through the initial configuration steps for NCS Virtual Appliance. In the first sequence of steps, you configure network settings.

Step 2 As prompted, enter the following settings:

a. Hostname for the virtual appliance.

b. IP address for the virtual appliance.

c. IP default subnet mask for the IP address entered.

d. IP address of the default gateway for the network environment in which you are creating the virtual machine.

e. Default DNS domain for the target environment.

f. IP address or hostname of the primary IP nameserver in the network.

g. At the Add/Edit another nameserver prompt, you can enter y (yes) to add additional nameservers, if desired. Otherwise, press Enter to continue.

h. NTP server location (or accept the default by pressing Enter). At the Add/Edit secondary NTP server prompt, you can enter y (yes) to add another NTP server. Otherwise, enter n (no) to continue.

Step 3 Enter the username for the user account used to access the Cisco NCS system running on the virtual machine. The default username is admin, but you can change this to another username by typing it here.

Step 4 Enter the password for NCS. The password must be at least eight characters and must include both lowercase and uppercase letters and at least one number. It cannot include the username or default Cisco passwords. After you enter the password, the script verifies the network settings you configured. For instance, it attempts to reach the default gateway that you have configured.

After verifying the network settings, the script starts the NCS installation processes. This process can take several minutes, during which there is no screen feedback. When finished, the following banner appears on the screen:

```
=== Initial Setup for Application: NCS ===
```

After this banner, it starts with database scripts and reboots the server as shown in the console:

```
Running database cloning script...
logger: invalid option -- l
usage: logger [-is] [-f file] [-p pri] [-t tag] [-u socket] [ message ... ]
Running database creation script...
logger: invalid option -- l
usage: logger [-is] [-f file] [-p pri] [-t tag] [-u socket] [ message ... ]
Setting Timezone, temporary workaround for DB...
Generating configuration...
Rebooting...
```

Note If you are installaing a physical appliance, remove the ISO DVD from the DVD tray.

Step 5 Log in as admin and enter the admin password.

Step 6 Exit the console using the **exit** command.

Starting the NCS Server

This section provides instructions to start NCS on either a physical appliance or virtual appliance.

Note To check the status of NCS at any time, follow the instructions in the "Verifying the Status of NCS" section on page 4-6.

To start the NCS server, follow these steps:

Step 1 Once you have setup NCS, rebooted the server and login as admin.

Step 2 Enter the following command to start the NCS Server.

```
ncs start
```

Logging into the NCS User Interface

To log into the NCS user interface through a web browser, follow these steps:

Step 1 Launch Internet Explorer 7.0 or later or Mozilla Firefox 3.6 or later on a different computer than the one on which you installed and started NCS.

Note When you use Firefox 3.x to log in and access NCS for the first time, the Firefox web browser displays a warning that the site is untrustable. When Firefox displays this warning, follow the prompts to add a security exception and download the self-signed certificate from the NCS server. After you complete this procedure, Firefox accepts the NCS server as a trusted site both now and during all future login attempts.

Step 2 In the address line of browser, enter *https://ncs-ip-address***,** where *ncs-ip-address* is the IP address of the server on which you installed and started NCS. The NCS user interface displays the Login page.

Step 3 Enter your username. The default username is *root*.

Step 4 Enter the root password you created during setup.

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 5 Click **Login** to log into NCS. The NCS user interface is now active and available for use. The NCS home page appears. The NCS home page enables you to choose the information that you want to see. You can organize the information in user-defined tabs called dashboards. The default view comes with default dashboards and pre-selected dashlets for each, and you can arrange them as you like. You can predefine what appears on the home page by choosing the monitoring dashlets that are critical for your network. For example, you may want different monitoring dashlets for a mesh network so that you can create a customized mesh dashboard.

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

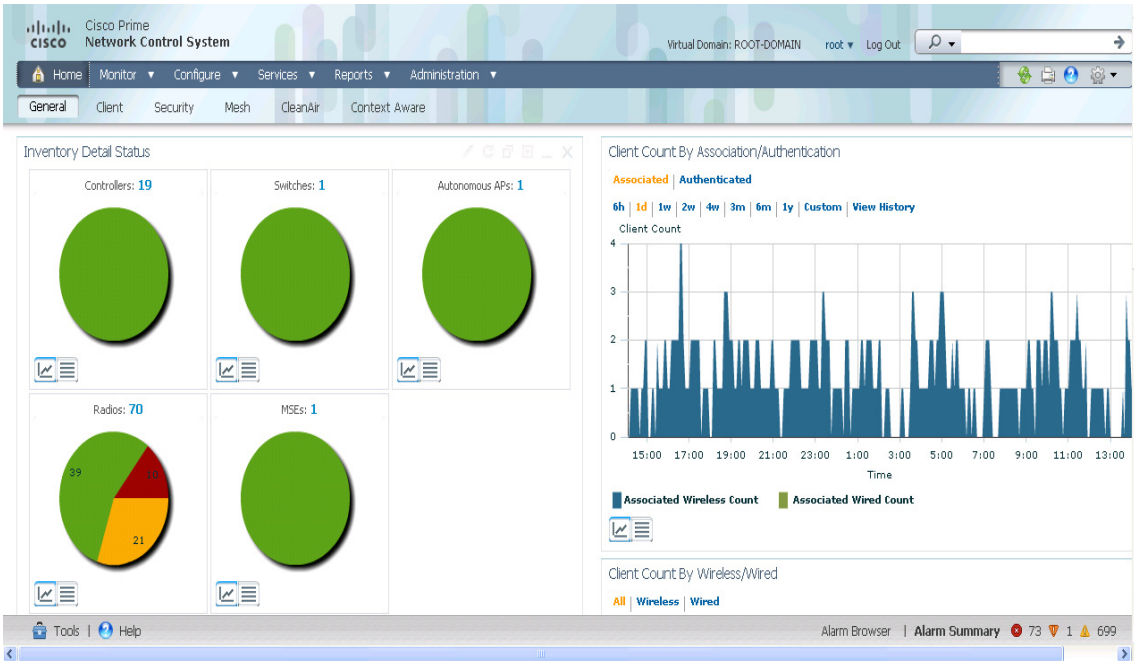
Note When an upgrade occurs, the user-defined tabs arranged by the previous user in the previous version are maintained. Therefore, the latest dashlets may not show. Look at the Edit dashboard link to find what new dashlets are added.

The home page provides a summary of the Cisco Unified 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 2-4 shows a typical NCS home page.

By default, you should see six dashboards on the NCS home page: General, Client, Security, Mesh, CleanAir and ContextAware dashboards.

Note When you use NCS 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 NCS database with one or more controllers, the NCS home page provides updated information.

Figure 2-4 NCS Home Page



To exit the NCS user interface, close the browser page or click **Log Out** in the upper-right corner of the page. Exiting an NCS user interface session does not shut down NCS on the server.

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

Applying the NCS Software License

This section describes how to apply a license to NCS. Before starting, make sure that you have already acquired the license from the Cisco License Center and put it in a location that is accessible by the network from NCS. To add a new NCS license file, follow these steps:

Step 1 In the Administrator menu, choose **License Center > Files > NCS Files** page, and click Add.

Step 2 In the Add a License File dialog box, enter or browse to the applicable license file.

Step 3 Once displayed in the License File text box, click **Upload**.

To add a new license, see "Managing Licenses" section on page 15-123.

Understanding NCS Home Page

The NCS home page:

- enables the administrator to create and configure Cisco Unified Network Solution coverage area layouts, configure system operating parameters, monitor real-time Cisco Unified Network Solution operations, and perform troubleshooting tasks using an HTTPS web browser page.
- enables the administrator to create, modify, and delete user accounts; change passwords; assign permissions; and schedule periodic maintenance tasks. The administrator creates new usernames and passwords and assigns them to predefined permissions groups.
- allows the administrator to perform all necessary network administration tasks from one page. The NCS home page, is the landing page, displaying real-time monitoring and troubleshooting data. The navigation tabs and menus at the top of the page provide point-and-click access to all other administration features.

The NCS user interface provides an integrated network administration console from which you can manage various devices and services. These include wired and wireless devices and clients. The services may include authentication, authorization, profiler, location and mobility services as well as monitoring, troubleshooting, and reporting. All of these devices and services can be managed from a single console called the Cisco Prime NCS home page.

This section describes the NCS user interface page and contains the following topics:

- Dashboards, page 2-13
- Icons, page 2-22
- Menu Bar, page 2-23
- Global Toolbar, page 2-26
- Alarm Summary, page 2-27
- Main Data Page, page 2-28
- Administrative Elements, page 2-28

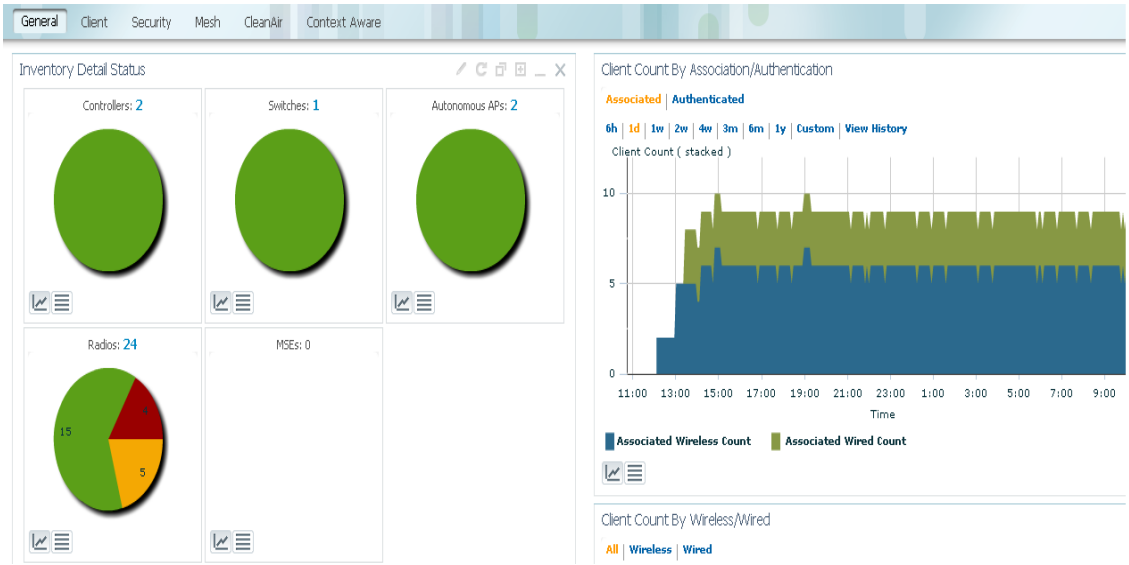
Dashboards

The NCS dashboards consist of dashlets and graphs that provide a visual overview of network health and security. The Dashboard elements visually convey complex information in a simplified format. This display allows you to quickly analyze the data and drill down for in-depth information if needed. Dashlets utilize a variety of elements to display data, including pie-charts, sparklines, stack bars, and metric meters.

The fundamental purpose of a dashboard is to provide an at-a-glance view of the most important parts of NCS. A quick scan of the dashboard should let you know if anything needs attention. Dashboard generally provides the status and alerts, monitoring and reporting information. Dashboards contain several dashlets, which are UI containers that display a variety of widgets, such as text, form elements, tables, charts, tabs, and nested content modules.

The dashboard displays the current status which reflects the status and usage of the network, like client distribution. The dashboard also displays the trend which reflects the usage and status over time which is from data collected over time, like client count.

Figure 2-5 Dashboards



Note You must have Adobe Flash Player installed to view the dashlets on the NCS dashboard.

The six NCS dashboards are described in this section. This section contains the following topics:

- General Dashboard, page 2-15
- Client Dashboard, page 2-16
- Security Dashboard, page 2-17
- Mesh Dashboard, page 2-18
- CleanAir Dashboard, page 2-18
- Context Aware Dashboard, page 2-21

You can customize the predefined set of dashlets depending on your network management needs. You can organize the information in user-defined dashboards. The default view comes with default dashboards and pre-selected dashlets for each.

Note

- The label "**Edited**" next to the dashlet heading indicates that the dashlet has been customized. If you reset to the default settings, the Edited label is cleared. Hover your mouse cursor over the label see the edited information.
- When an upgrade occurs, the arrangement of dashlets in a previous version is maintained. Because of this, dashlets or features added in a new release are not displayed. Click the **Manage Dashboards** link to discover new dashlets.

- The horizontal and vertical scrollbars are visible if you zoom the dashlets. Reset the zoom level back to zero, or no zoom for viewing the dashlets without the scrollbars.

General Dashboard

Table 2-1 lists the factory default dashlets for the General dashboard.

Table 2-1 General Dashboard

Dashlet	Description
Inventory Detail Status	Displays the following: • Controllers—Lists the number of controllers that are managed in NCS. Graphically depicts reachable and unreachable controllers. • Switches—Lists the number of switches managed in NCS. Graphically depicts reachable and unreachable switches. • Radios—Lists the number of radios managed in NCS. Graphically depicts the number of radios in out-of-service (critical), minor, and ok conditions. This dashlet reflects ONLY the greatest radio alarm status, that is, if the radio has a minor alarm, and a critical alarm, then the radio status will show as critical. • Autonomous APs—Lists the number of Autonomous APs managed in NCS. Graphically depicts reachable and unreachable Autonomous APs. • MSEs—Lists the number of MSEs that are managed in NCS. Graphically depicts reachable and unreachable servers. Look at the installation log to verify that nothing went wrong while manually adding the servers to NCS. (The trace for MSEs must be turned on.) **Note** Clicking on the corresponding sections of the chart will take you the item list view of the inventory.
Device Uptime	Displays the devices based upon the device up time.
Coverage Area	Displays access points, radios, and client details for each coverage area.

Table 2-1 General Dashboard (continued)

Dashlet	Description
Client Count by Association/Authentication	Displays the total number of clients by Association and authentication in NCS over the selected period of time. • Associated client—All clients connected regardless of whether it is authenticated or not. • Authenticated client—All clients connected through an RADIUS or TACACS server. **Note** Client count includes autonomous clients.
Client Count by Wireless/Wired	Displays the total number of clients by Wired and Wireless in NCS over the selected period of time. **Note** Client count includes autonomous clients.
Top 5 Devices by Memory Utilization	Displays the Top 5 devices based upon memory utilization.
Recent Coverage Holes	Displays the five most recent coverage alarms.

Client Dashboard

Table 2-2 lists the factory default dashlets for the Client dashboard.

Table 2-2 Client Dashboard

Dashlet	Description
Client Troubleshooting	Allows you to troubleshoot a client by entering a client MAC address, then clicking **Troubleshoot**.
Client Distribution	Displays the distribution of clients by protocol, EAP type, and authentication and the total current client count. • 802.3 represents wired clients • 802.11 represents wireless clients **Note** Clicking on the corresponding sections of the chart will take you the item list view of the clients and users.
Client Alarms and Events Summary	Displays a summary of client alarms and events.
Client Traffic	Displays the trend of both upstream and downstream client traffic in a given time period.
Wired Client Speed Distribution	Displays the wired client speeds and the client count for each speed.
Top 5 SSIDs by Client Count	Displays the top 5 SSID client counts.

Table 2-2 Client Dashboard (continued)

Dashlet	Description
Top 5 Switches by Client Count	Displays the 5 switches that have the most clients as well as the number of clients associated to the switch.
Client Posture Status	Displays the client posture status and the number of clients in each of the following status: • Compliant • Non-compliant • Unknown • Pending • Not Applicable • Error

Security Dashboard

Table 2-3 lists the factory default dashlets for the Security dashboard.

Table 2-3 Security Dashboard

Dashlet	Description
Security Index	Indicates the security of the NCS managed network. The security index is calculated by assigning priority to the various security configurations and displaying them in visual form.
Malicious Rogue APs	Displays malicious rogue access points 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.
Adhoc Rogues	Displays ad hoc rogues for the past hour, past 24 hours, and total active.
CleanAir Security	Displays cleanair security events for past hour, 24 hours, and total active.
Attacks Detected	Displays wIPS and signature attacks 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.
AP Threats/Attacks	Displays threats or attacks to access points for the past hour, past 24 hours, and total active.
MFP Attacks	Displays MFP attacks for the past hour, past 24 hours, and total active.
Client Security Events	Displays the client security events for the past hour, past 24 hours and total active.

Note The Rogue alarm which is set as informational, cannot be seen in the security dashboard.

Mesh Dashboard

Table 2-4 lists the factory default dashlets for the Mesh dashboard.

Table 2-4 Mesh Dashboard

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

Table 2-5 lists the factory default dashlets for the Mesh dashboard.

Table 2-5 CleanAir Dashboard

Dashlet	Description
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.

Table 2-5 CleanAir Dashboard (continued)

Dashlet	Description
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 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.

Table 2-5 CleanAir Dashboard (continued)

Dashlet	Description
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 dashlet in different formats.

Context Aware Dashboard

Table 2-6 lists the factory default dashlets for the Context Aware dashboard.

Table 2-6 Context Aware Dashboard

Dashboard	Description
MSE Historical Element Count	Displays the historical trend of tags, clients, rogue APs, rogue clients, interferers, wired clients, and guest client counts in a given period of time. **Note** The MSE Historical Count information is presented in a time-based graph. For graphs that are time-based, there is a link bar at the top of the graph page that displays 6h, 1d, 1w, 2w, 4w, 3m, 6m, 1y, and Custom. When selected, the data for that time frame is retrieved and the corresponding graph is displayed. See the "Time-Based Graphs" section on page 6-71 for more information.
Rogue Elements detected by CAS	Displays the indices of the Rogue APs and Rogue Clients in percentage. It also provides a count of the number of Rogue APs and Rogue Clients detected by each MSE within an hour, 24 hours as well as more than 24 hours. Rogue AP Index is defined as the percentage of total active tracked elements that are detected as Rogue APs across all the MSEs on NCS. Rogue Client Index is defined as the percentage of total active tracked elements that are detected as Rogue Clients across all the MSEs on NCS.
Location Assisted Client Troubleshooting	You can troubleshoot clients using this option with location assistance. You can provide either a MAC Address, Username or IP Address as the criteria for troubleshooting. **Note** Username, IP Address, and partial MAC address-based troubleshooting is supported only on MSEs with version 7.0.200.0 and later. For more information about Location Assisted Client Troubleshooting, see the "Location Assisted Client Troubleshooting from the Context-Aware Dashboard" section on page 12-77.

Table 2-6 Context Aware Dashboard (continued)

Dashboard	Description
MSE Tracking Counts	Represents the tracked and not-tracked count of each of the element types. The element type includes tags, rogue APs, rogue clients, interferers, wired clients, wireless clients, and guest clients.
Top 5 MSEs	Lists the top five MSEs based on the percentage of license utilization. It also provides count for each element type for each MSE. **Note** If you have installed NCS license but you have not added any MSE to NCS then the Context-Aware dashboard will be empty. However a message would be displayed with a link to add an MSE. In the dashlet, click the count link to get a detailed report. Use the icons in a dashlet to switch between chart and grid view. Use the Enlarge Chart icon to view the grid or chart in full screen.

Icons

The icons on the dashlets and within the General, Client, Security, Mesh, CleanAir, and Context Aware dashboards have the following functions listed in Table 2-7.

Table 2-7 Icon Representation

Icon	Description
	The Dashlet Options icon enables you to customize and filter the data by using variables and search options. For example, you can search the client count trends for SSIDs, floor areas, controllers, specific autonomous APs and so on. **Note** Only some of the dashlets have these search by parameters.
	The Refresh Dashlet icon enables you to automatically refresh the dashboard so that it reflects the current network status.
	The Detach Dashlet icon enables you to detach the dashlet.
	The Maximize Dashlet icon enables you to maximize the dashelt so that it is visible in full view.

Table 2-7 Icon Representation

Icon	Description
	The collapse Dashlet icon enables you to minimize the dashlet so that the dashlet is not visible.
	The View in Chart icon enables you to view the dashlet in chart rather than table form.
	The View in Grid icon enables you to view the dashlet in a table rather than chart form.

Menu Bar

The primary navigation is the menu from the top of the Cisco NCS page. Administrators can monitor and perform various tasks from the NCS menus. This menu is an easy-access pop-up menu that provides quick access to the sub menu that are associated with a primary menu. Hover your mouse cursor over the title of a menu to bring up the associated menu. Clicking the name links on the menu takes you directly to the feature page. The following illustration is an example of the NCS menu.

Figure 2-6 NCS Primary Global Menu

This section describes the menus and contains the following topics:

- Monitor Menu, page 2-23
- Configure Menu, page 2-24
- Services Menu, page 2-25
- Reports Menu, page 2-25
- Administration Menu, page 2-25

When you hover your mouse cursor over any of the five menu heading, a drop-down menu appears.

Monitor Menu

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

The following submenu options are available from the Monitor menu:

- Monitoring Devices
  - Monitoring Controllers

  - Monitoring Switches
  - Monitoring Access Points
  - Monitoring RFID Tags
  - Monitoring Chokepoints
  - Monitoring Interferers
  - Monitoring WiFi TDOA Receivers
- Monitoring Radio Resource Management (RRM)
- Monitoring Clients and Users
- Monitoring Alarms and Events
  - Monitoring Alarms
  - Monitoring Events
- Monitoring Maps
  - Monitoring Maps
  - Monitoring Google Earth Maps

Configure Menu

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

The following submenu options are available from the Configure drop-down menu:

- Configuring Devices
  - Configuring Controllers
  - Configuring Switches
  - Configuring Unknown Devices
  - Configuring Access Points
  - Configuring Chokepoints
  - Configuring Spectrum Experts
  - Configuring WiFi TDOA Receivers
- Configuring Scheduled Configuration Tasks
- Configuring Controller Auto Provisioning
- Configuring wIPS Profiles
- Configuring Templates
  - Accessing Controller Template Launch Pad
  - Configuring Lightweight Access Point Templates
  - Configuring Autonomous Access Point Templates
  - Configuring Switch Location Configuration Templates
  - Configuring Autonomous AP Migration Templates
- Configuring Controller Config Groups

- Configuring Servers
  - Configuring ACS View Servers
  - Configuring TFTP Servers

Services Menu

The Services menu enables you to manage mobility services including mobility services engines and Identity Service Engines.

The following submenu options are available from the Services drop-down menu:

- Mobility Services
  - Viewing Current Mobility Services
  - Synchronizing Services
  - Viewing Synchronization History
  - Viewing the Notifications Summary for Mobility Services
- Identity Services

Reports Menu

The Reports menu provides the following submenu options:

- Report Launch Pad
- Managing Scheduled Run Results
- Managing Saved Report Templates

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 NCS).

The following submenu options are available from the Administration drop-down menu:

- Performing Background Tasks
- Configuring Virtual Domains
- Configuring Administrative Settings
- Setting User Preferences
- Viewing Appliance Details
- Configuring AAA
- Establishing Logging Options
- Configuring High Availability
- Managing Licenses

Global Toolbar

The Global Toolbar is always available at the bottom of the NCS page, providing instantaneous access to the Tools, NCS online Help system and a summary of alarm notifications. Hover your mouse cursor over the Help icon to access the available online Help.

Hover your mouse cursor over the Alarms Browser to display the summarized Alarms page, with a list of recent system alarms and the ability to filter for alarms of a specific nature. You can also drill down for detailed information on individual alarms. For more information on Alarms, see Alarm Summary, page 2-27.

Figure 2-7 Global Toolbar

This section contains the following topics:

- Tools, page 2-26
- Help, page 2-26

Tools

The Tools menu provides access to the Voice Audit, Configuration Audit, and Migration Analysis features of NCS.

The following submenu options are available from the Tools drop-down menu:

- Configuring Voice Audit
- Configuring Location Accuracy Tool
- Configuring Audit Summary
- Configuring Migration Analysis
- Configuring TAC Case Attachments

Help

The Help menu allows you to access online help, learning modules, submit feedback, and to verify the current version of NCS. The Help icon is located in the bottom left corner of the Global Toolbar in the NCS page. The Help provides quick access to the comprehensive online help for NCS.

The following submenu options are available from the Help drop-down menu:

- Online Help—enables you to view online help. The online help is context sensitive and will open to documentation for the NCS window that you currently have open.
- Learning Modules—allows you to access short video clips of certain NCS features. To learn more about Cisco NCS features and functionality, go to Cisco.com to watch multimedia presentations about NCS configuration workflow, monitoring, troubleshooting, and more. Over future releases, more overview and technical presentations will be added to enhance your learning.
- MSE Installation Guide—provides links to the MSE installation section.
- Submit Feedback—allows you to access a page where you can enter feedback on the NCS.

- Help Us Improve Cisco Products—allows you to enable and provide permission to automatic collect data about how you and your organization use your Cisco wireless products, this data will be useful to improve product performance and usability. The data will be automatically collected and sent to Cisco in encrypted form. The data may contain information about your organization and it will not be shared or used outside of Cisco.

Note To get the automated feedback enabled, you have to configure your Mail Server Configuration by choosing **Administration > Settings > Mail Server Configuration**.

- About Cisco NCS—allows you to verify the version of NCS that you are running. It provides the version, host name, feature, AP limit, and type.

To verify the version of NCS, choose **About Cisco NCS**. The following information is displayed:

- Product Name
- Version Number
- Host Name
- Feature
- AP Limit
- License Type
- Copyright statement

Alarm Summary

When NCS receives an alarm message from a controller, it displays an alarm indicator at the bottom of the NCS page (see Figure 2-8). 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. The Critical (red), Major (orange) and Minor (yellow) alarms appear in the alarm dashboard, left to right.

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 NCS and alarms lists page. By default, acknowledged alarms are not shown.

Figure 2-8 NCS Alarm Summary

Note Alarm counts are refreshed every 15 seconds.

Command Buttons

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

- Apply: Applies the selected information

- 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 NCS database device configurations

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
- Drop-down lists 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 NCS 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 Elements

The following provides information regarding the current NCS user:

- User—Indicates the username for the current NCS user. Click the User link to change the user password. See the "Changing Password" section on page 15-128 for more information.
- Virtual Domain—Indicates the current virtual domain for this NCS user. See the "Configuring Virtual Domains" section on page 18-1 for more information.

Note To switch domain names, click the blue inverted triangle to the right of the virtual domain name to open the Switch to another Virtual Domain page. Select the new virtual domain radio button and click **Save**. Your privileges are changed accordingly.

Icon	Description
	Click to access the NCS online help. **Note** The online help provides information applicable to your current NCS version.
	Click to update the data in the current NCS version.

Icon	Description
	Click to access a print-friendly version of the current NCS. **Note** Click **Print** to print the current NCS version or **Exit Print View** to return to the previous page.
	Click to edit the dashboard or to add a new dashboard in NCS.

Customizing NCS Home Page

NCS home page dashlets, contains default predefined list of dashlets which you can customize. The following customization are possible in the NCS home page:

- drag-and-drop dashlets
- add or delete dashboards
- reordering dashboards
- renaming dashlets and dashboards
- customize layout

Note You can add or delete dashlets by selecting from the predefined list.

You can customize the home page with time-based or non-time-based interactive graphs which you can display in grid or chart format (by clicking the appropriate icon). These graphs refresh automatically within a predetermined time based on the default polling cycles of dependent tasks, or you can click the Refresh dashlet icon to get the most current status. You can click the Enlarge Chart icon to enlarge the graph in a separate page.

This section contains the following topics:

- Editing NCS Home Page, page 2-29
- Adding Dashlets, page 2-30
- Adding a New Dashboard, page 2-32

Editing NCS Home Page

To customize the NCS home page dashlets, follow these steps:

Step 1 On the NCS home page, click the Edit Dashboard icon. The drop-down list appears.

Step 2 Click the Add dashlets link, which lists the available dashlets drop-down list. Add the desired dashlet by clicking the **Add** link in the right column. The dashlet is added to the appropriate dashboard.

Step 3 Click **Apply**.

Adding Dashlets

Table 2-7 lists the default dashlet options you can add in your NCS home page.

Table 2-8 Default Dashlets

Dashlet	Description
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.
Cisco Wired IPS Events	Displays wired IPS events for the previous hour, previous 24 hours, and total active.
Client	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	Displays count based upon the EAP type.
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.

Table 2-8 Default Dashlets (continued)

Dashlet	Description
Coverage Areas	Displays the list coverage areas and details about each coverage area.
Friendly Rogue APs	Displays friendly rogue access points for the previous hour, previous 24 hours, and total active.
Guest Users Count	Displays Guest client count over a specified time.
Inventory Detail Status	Displays the Chart summarizing the status for the following device types. - Controllers - Switches - Autonomous APs - Radios - MSEs
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	Displays the most recent guest users to login.
Mesh AP by Hop Count	Displays the APs based upon hop count.
Mesh AP Queue Based on QoS	Displays the APs based upon QOS.
Mesh Parent Changing AP	Displays the worst Mesh APs based upon changing parents.
Mesh Top Over Subscribed AP	Displays the considered over subscribed APs.
Mesh Worst Node Hop Count2-28	Displays the Worst AP node hop counts from the root AP.
Mesh Worst Packet Error Rate	Displays the worst Mesh AP links based upon the packet error rates of the links.
Mesh Worst SNR Link	Displays the worst Mesh AP links based upon the SNR values of the links.
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	Displays the most recent client alarms.
Most Recent Mesh Alarms	Displays the 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	Displays the most recent guest user accounts created or modified.

Table 2-8 Default Dashlets (continued)

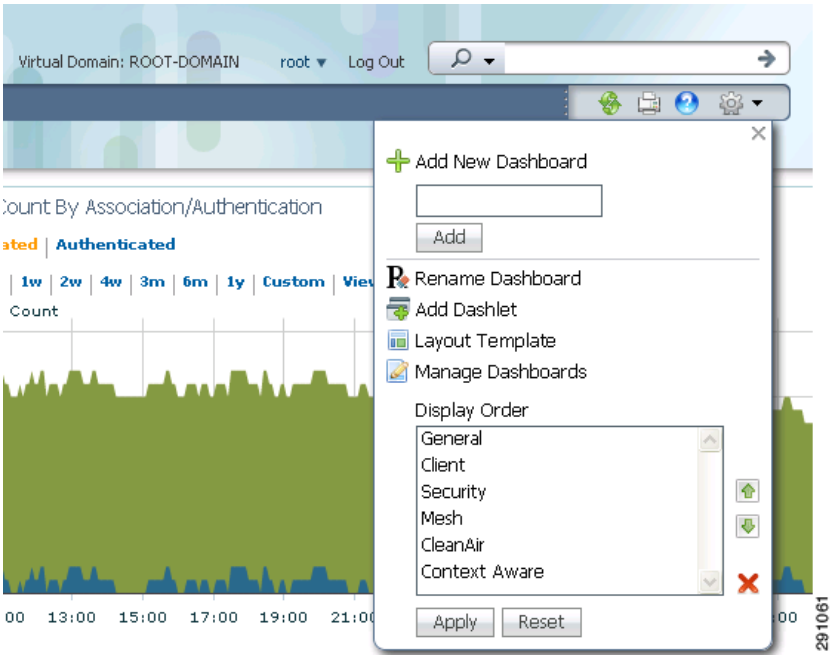
Dashlet	Description
Recent Alarms	Displays the five most recent alarms by default. Click the number in parentheses to open the Alarms page.
Recent Coverage Holes	Displays the recent coverage hole alarms listed by access point.
Recent Malicious Rogue AP Alarms	Displays the recent malicious rogue AP alarms.
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	Displays the security index score for the wireless network.Security index is calculated as part of 'Configuration Sync' background task.
Top APs by Client Count	Displays the Top APs by client count are displayed.
Unclassified Rogue APs	Displays unclassified rogue access points for the previous hour, previous 24 hours, and total active.

Adding a New Dashboard

To create a new dashboard, follow these steps:

Step 1 Click the **Edit Dashboard** icon on NCS home page. The Edit Dashboard menu appears (see Figure 2-9).

Figure 2-9 Edit Dashboard



Step 2 Enter the name of the new dashboard you are creating, and click **Add**. The dashboard name you just added appears in the Display Order list.

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

Step 3 You can add dashlets to the new dashboard. For more information see the "Adding Dashlets" section on page 2-30.

Note If you want to return to the restored factory defaults as shown in Figure 2-8, click **Reset** to reset to factory defaults.

Using the Search Feature

The enhanced NCS Search feature (see Figure 2-10) provides easy access to advanced search options and saved searches. You can access the search options from any page within NCS making it easy to search for a device or SSID (Service Set IDentifier).

Figure 2-10 NCS Search Feature

The following searches are possible using NCS:

- Quick Search, page 2-33
- Advanced Search, page 2-34
- Saved Searches, page 2-46

Quick Search

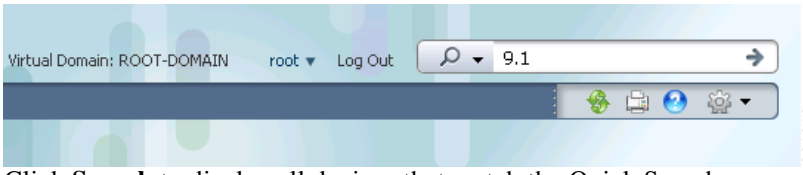
For a quick search, you can enter a partial or complete IP address, MAC address, name, or SSID for clients, alarms, access points, controllers, maps, tags, or rogue clients (see Figure 2-10).

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 Search text box (see Figure 2-11).

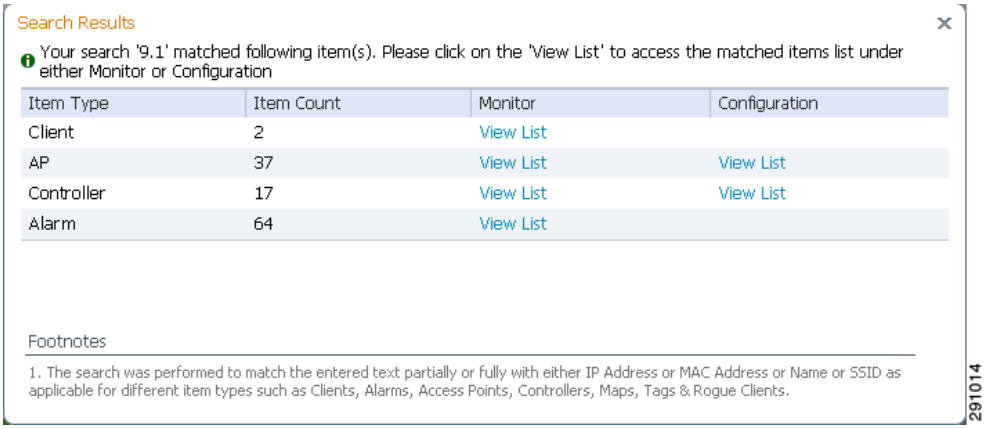
Figure 2-11 Quick Search with Partial IP Address



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 2-12). Click **View List** to view the matching devices from the Monitor or Configuration pages.

Figure 2-12 Quick Search Results Advanced Search



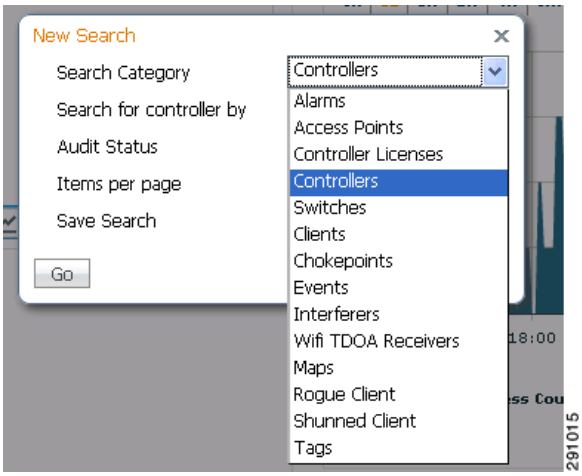
Advanced Search

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

Step 1 Click **Advanced Search** located in the top right corner of NCS (see Figure 2-10).

Step 2 In the New Search dialog, select a category from the Search Category drop-down list (see Figure 2-13).

Figure 2-13 Search Category Drop-Down List



Note Click each of the following categories for more information.

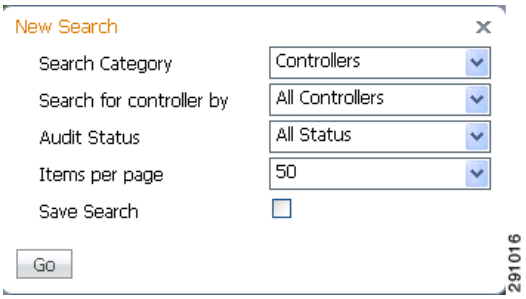
Search categories include the following:

- Searching Alarms
- Searching Access Points
- Searching Controller Licenses
- Searching Controllers
- Searching Switches
- Searching Clients
- Searching Chokepoints
- Searching Events
- Searching Interferers
- Searching Wi-Fi TDOA Receivers
- Searching Maps
- Searching Rogue Clients
- Searching Shunned Clients
- Searching Tags

Step 3 Select all applicable filters or parameters for your search (see Figure 2-14).

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 2-14 New Search Parameters



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**.

Searching Alarms

You can configure the following parameters when performing an advanced search for alarms (see Table 2-9).

Table 2-9 Search Alarms Parameters

Parameter	Options
Severity	Choose All Severities, Critical, Major, Minor, Warning, or Clear.
Alarm Category	Choose All Types, Access Points, Controller, Switches, Coverage Hole, Config Audit, Mobility Service, Context Aware Notifications, Interference, Mesh Links, Rogue AP, Adhoc Rogue, Security, NCS or Performance.
Condition	Use the drop-down list to select a condition. Also, you can enter a condition by typing it in this drop-down list. **Note** If you have selected an alarm category, this drop-down list would contain the conditions available in that category.
Time Period	Choose a time increment from Any Time to Last 7 days. The default is Any Time.

Table 2-9 Search Alarms Parameters (continued) (continued)

Parameter	Options
Acknowledged State	Select this check box 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	Select this check box 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 appears on the alarm search results page. See the "Configuring the Search Results Display (Edit View)" section on page 2-46 for more information.

Searching Access Points

You can configure the following parameters when performing an advanced search for access points (see Table 2-10).

Table 2-10 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 2-10 Search Access Points Parameters (continued) (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.
CleanAir Support	Check to search for access points which support CleanAir.
CleanAir Enabled	Check to search for access points which support CleanAir and which are enabled.
Items per page	Configure the number of records to be displayed in the search results page.

Note You can decide what information displays on the access points search results page. See the "Configuring the Search Results Display (Edit View)" section on page 2-46 for more information.

Searching Controller Licenses

You can configure the following parameters when performing an advanced search for controller licenses (see Table 2-11).

Table 2-11 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.
Items per page	Configure the number of records to be displayed in the search results page.

See the "Managing Licenses" section on page 15-123 for more information on licenses and the License Center.

Searching Controllers

You can configure the following parameters when performing an advanced search for controllers (see Table 2-12).

Table 2-12 Search Controllers Parameters

Parameter	Options
Search for controller by	Choose All Controllers, IP Address, Controller 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.
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.
Audit Status	Choose one of the following from the drop-down list: • All Status • Mismatch—Config differences were found between NCS and controller during the last audit. • Identical—No config differences were found during the last audit. • Not Available—Audit status is unavailable.
Items per page	Configure the number of records to be displayed in the search results page.

Note You can decide what information displays on the controllers search results page. See the "Configuring the Search Results Display (Edit View)" section on page 2-46 for more information.

Searching Switches

You can configure the following parameters when performing an advanced search for switches (see Table 2-13).

Table 2-13 Search Switches Parameters

Parameter	Options
Search for Switches by	Choose All Switches, IP Address, or Switch Name. You can use wildcards (*). For example, if you select IP Address and enter `172*`, NCS returns all switches that begin with IP address 172.
Items per page	Configure the number of records to be displayed in the search results page.

You can decide what information displays on the client search results page. See the "Configuring the Search Results Display (Edit View)" section on page 2-46 for more information.

Searching Clients

You can configure the following parameters when performing an advanced search for clients (see Table 2-14).s

Table 2-14 Search Clients Parameters

Parameter	Options
Media Type	Choose All, Wireless Clients, Wired Clients.
Wireless Type	Choose All, Lightweight or Autonomous Clients. If you have selected Wireless Clients in Media Type.
Search By	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, Switch Name, Switch Type. **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.
Clients Detected By	Choose NCS or MSEs. Clients detected by NCS—Clients stored in NCS databases. Clients detected by MSE—Clients located by Context Aware service in the MSE directly communicating with the controllers.
Client States	Choose All States, Idle, Authenticated, Associated, Probing, or Excluded.
Posture Status	Choose All, Unknown, Passed, Failed if you want to know if the devices are clean or not.
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.
SSID	Select the check box and choose the applicable SSID from the drop-down list.

Table 2-14 Search Clients Parameters (continued)

Parameter	Options
Profile	Select the check box to list all of the clients associated to the selected profile. **Note** Once the check box is selected, choose the applicable profile from the drop-down list.
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 NCS has historical records.
Items per page	Configure the number of records to be displayed in the search results page.

Note You can decide what information displays on the client search results page. See the "Configuring the Search Results Display (Edit View)" section on page 2-46 for more information.

Searching Chokepoints

You can configure the following parameters when performing an advanced search for chokepoints (see Table 2-15).

Table 2-15 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.

Searching Events

You can configure the following parameters when performing an advanced search for events (see Table 2-16).

Table 2-16 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 NCS.
Condition	Use the drop-down list to select a condition. Also, you can enter a condition by typing it in this drop-down list. **Note** If you have selected an event category, this drop-down list would contain the conditions available in that category.
Search All Events	Configure the number of records to be displayed in the search results page.

See the "Monitoring Rogue Alarm Events" section on page 5-108 for more information on events.

Searching Interferers

You can configure the following parameters when performing an advanced search for interferers detected by access points (see Table 2-17).

Table 2-17 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.
Interferer Status	
Restrict by Radio Bands/Channels	Configure the search by radio bands or channels.
Items per page	Configure the number of records to be displayed in the search results page.

You can decide what information displays on the SE-detected interferers search results page. See the "Configuring the Search Results Display (Edit View)" section on page 2-46 for more information.

Searching AP-Detected Interferers

You can configure the following parameters when performing an advanced search for interferers detected by access points (see Table 2-18).

Table 2-18 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 (Edit View)" section on page 2-46 for more information.

Searching Wi-Fi TDOA Receivers

You can configure the following parameters when performing an advanced search for Wi-Fi TDOA receivers (see Table 2-19).

Table 2-19 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.

Searching Maps

You can configure the following parameters when performing an advanced search for maps (see Table 2-20).

Table 2-20 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.
Items per page	Configure the number of records to be displayed in the search results page.

Note You can decide what information displays on the maps search results page. See the "Configuring the Search Results Display (Edit View)" section on page 2-46 for more information.

See the "Information About Maps" section on page 6-2 for more information on maps.

Searching Rogue Clients

You can configure the following parameters when performing an advanced search for rogue clients (see Table 2-21).

Table 2-21 Search Rogue Client Parameters

Parameter	Options
Search for clients by	Choose All Rogue Clients, MAC Address, Controller, MSE, Floor Area, or Outdoor Area.
Search In	Choose MSEs or NCS 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 "Rogue Access Points, Ad hoc Events, and Clients" section on page 3-9 for more information on rogue clients.

Searching 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 2-22).

Table 2-22 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.

Searching Tags

You can configure the following parameters when performing an advanced search for tags (see Table 2-23).

Table 2-23 Search Tags Parameters

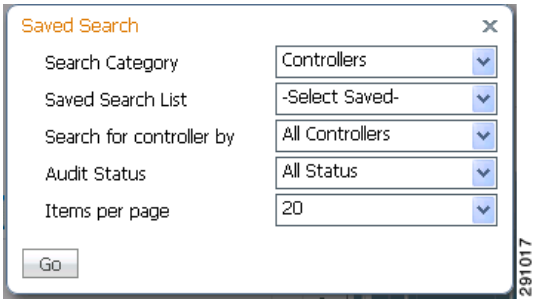
Parameter	Options
Search for tags by	Choose All Tags, Asset Name, Asset Category, Asset Group, MAC Address, Controller, MSE, Floor Area, or Outdoor Area. **Note** Search parameters may change depending on the selected category. When applicable, enter the additional parameter or filter information to help identify the Search By category.
Search In	Choose MSEs or NCS Controllers.
Last detected within	Choose a time increment from 5 minutes to 24 hours. The 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.
Items per page	Configure the number of records to be displayed in the search results page.

Saved Searches

The Saved Search feature enables you to access and run any previously saved search (see Figure 2-15).

Note When saving a search, you must assign a unique name to the search. Saved searches apply only to the current partition.

Figure 2-15 Saved Search Page



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

Step 1 Click **Saved Search**.

Step 2 Choose a category from the Search Category drop-down list.

Step 3 Choose a saved search from the Saved Search List drop-down list.

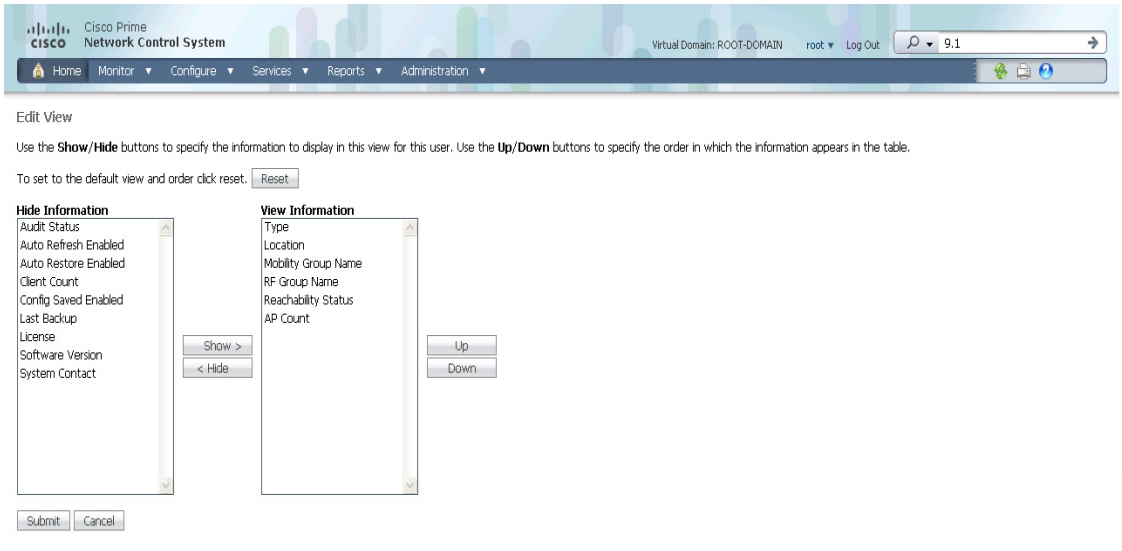
Step 4 If necessary, change the current parameters for the saved search.

Step 5 Click **Go**.

Configuring the Search Results Display (Edit View)

The Edit View page (see Figure 2-16) enables you to choose which columns appear on the Search Results page.

Figure 2-16 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.