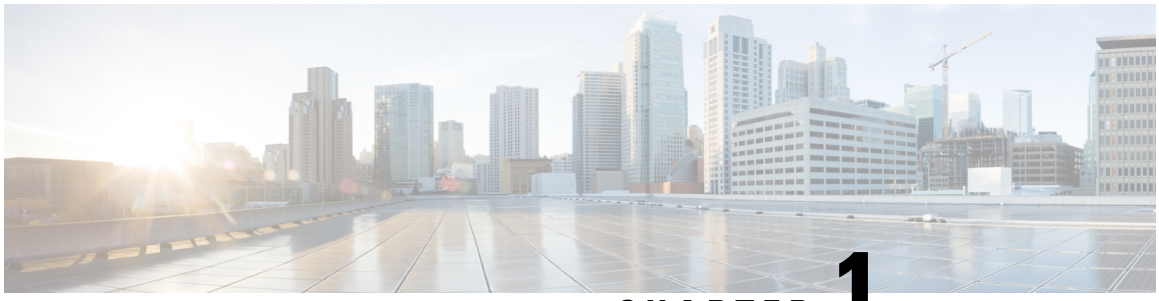
Cisco FindIT Network Manager and Probe Administration Guide, Version 2.0

First Published: 2018-11-14

Last Modified: 2019-07-03

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS



CHAPTER 1

Cisco FindIT Network Management Overview

This chapter contains the following sections:

About Cisco FindIT Network Management

Cisco FindIT Network Management provides tools that help you monitor and manage your Cisco 100 to 500 Series network. FindIT Network Management automatically discovers your network, and allows you to configure and monitor all supported Cisco 100 to 500 Series devices such as Cisco switches, routers, and wireless access points. It also notifies you the availability of firmware updates, and about any devices that are no longer under warranty or covered by a support contract.

FindIT Network Manager is a distributed application which is comprised of two separate components or applications: one or more Probes referred to as FindIT Network Probe and a single Manager called FindIT Network Manager.

An instance of FindIT Network Probe is installed at each site in the network, performs network discovery and communicates directly with each Cisco device. A single instance of FindIT Network Manager is installed at a convenient location in the network and each Probe is associated with the Manager. From the Manager interface, you can get a high-level view of the status of all the sites in your network, or concentrate on a single site or device to see information specific to that site or device.

Audience

This guide is primarily intended for network administrators who are responsible for Cisco FindIT Network Management software installation and management.

Related Documents

The documentation for Cisco FindIT Network Manager & Probe is comprised of a number of separate guides. These include:

- **Administration Guide (this document)**—This is a reference guide that provides details about all the features and options provided by the software and how they may be configured and used.
- **Quick Start Guide**—This guide provides details on performing the initial setup for FindIT Network Manager & Probe using the most commonly selected options. For an overview of the basic tasks required for managing a network, refer the Cisco FindIT Network Manager and Probe Quick Start Guide.
- **Installation Guides**

  The following table lists all the installation guides of FindIT software that can be deployed on different platforms. Refer the path provided in the location column for details:

Supported Platforms	Location
Amazon Web Services	Cisco FindIT Network Manager & Probe Installation Guide for Amazon Web Services
Oracle VirtualBox	Cisco FindIT Network Manager & Probe Installation Guide for Oracle VirtualBox
Microsoft Hyper-V	Cisco FindIT Network Manager & Probe Installation Guide for Microsoft Hyper-V
VMWare vSphere, Workstation and Fusion	Cisco FindIT Network Manager & Probe Installation Guide for VMWare
Ubuntu Linux (Manager and Probe) and Raspbian Linux (Probe only)	Cisco FindIT Network Manager & Probe Installation Guide for Linux

Terminology

Term	Description
Hyper-V	A virtualization platform provided by Microsoft Corporation.
Open Virtualization Format (OVF)	A TAR archive containing one or more virtual machines in OVF format. It is a platform-independent method of packaging and distributing Virtual Machines (VMs).

Term	Description
Open Virtual Appliance or Application (OVA) file	Package that contains the following files used to describe a virtual machine and saved in a single archive using .TAR packaging: • Descriptor file (.OVF) • Manifest (.MF) and certificate files (optional)
Raspberry Pi	A very low cost, single board computer developed by the Raspberry Pi Foundation. For more information, see *https://www.raspberrypi.org/*.
Raspbian	A Debian-based linux distribution optimized for the Raspberry Pi. For more information, see *https://www.raspbian.org/*.
VirtualBox	A virtualization platform provided by Oracle Corporation.
Virtual Hard Disk (VHD)	Virtual hard disk is a disk image file format for storing the complete contents of a hard drive.
Virtual Machine (VM)	A virtual computing environment in which a guest operating system and associated application software can run. Multiple VMs can operate on the same host system concurrently.
• VMWare ESXi • VMWare Fusion • vSphere Server • VMWare Workstation	A virtualization platform provided by VMWare Inc.
vSphere Client	User interface that enables users to connect remotely to vCenter Server or ESXi from any Windows PC. You can use the primary interface for vSphere Client to create, manage, and monitor VMs, their resources, and the hosts. It also provides console access to VMs.

System Requirements for Cisco FindIT Network Manager

Cisco FindIT Network Manager is distributed as a virtual machine image, as an installer for use with the Ubuntu Linux distribution, and is available for Amazon Web Services (AWS) through the AWS Marketplace (*https://aws.amazon.com/marketplace*).

When running FindIT Network Manager in virtual machine, your hypervisor must be one of the following:

- Microsoft Hyper-V version 10.0 or above
- Oracle VirtualBox version 5.0.2 or above
- VMWare—It can be one of the following:
  - ESXi version 5.5 or above

- Fusion version 7 or above
- Workstation version 12 or above

To run FindIT Network Manager under Ubuntu Linux, your environment must be running Ubuntu version 16.04.x (Xenial Xerus) on a 64-bit Intel architecture platform. Cisco recommends using the Ubuntu server distribution and only installing packages required by FindIT Network Manager.

Table 1 lists the compute resources required for FindIT Network Manager based on the number of devices under management.

Table 1: FindIT Network Manager Compute Resource Requirements

#Device Supported	# vCPU	RAM	Disk Space
Up to 300	2	4GB	60GB
Up to 2500	12	24GB	60GB

To run FindIT Network Manager in AWS, you will need an AWS account. The following AWS instances types are supported:

- t2.medium/t3.medium - up to 300 devices under management
- c4.4xlarge/c5.4xlarge - up to 2500 devices under management

FindIT Network Manager is administered through a web user interface. To use this interface, your browser must be one of the following:

- Apple Safari version 11 (macOS only) or above
- Google Chrome version 72 (Recommended) or above
- Microsoft Edge version 42 or above
- Mozilla Firefox version 65 or above

Note When using Safari, check that the certificate from FindIT Network Probe is set to **Always Trust**. Otherwise, certain functions that depend on the use of secure websockets are expected to fail. This is a limitation of the Safari web browser.

Your network must allow all instances of FindIT Network Probe to establish TCP connectivity with FindIT Network Manager. For more details on the ports and protocols used, see Frequently Asked Questions.

System Requirements for Cisco FindIT Network Probe

Cisco FindIT Network Probe is distributed as a virtual machine image, and as installers for use with the following operating systems:

- Ubuntu Linux distribution running on a PC
- Raspbian Linux distribution running on a Raspberry Pi

FindIT Network Probe is also available as an embedded feature of select Cisco 100 to 500 series products.

To run FindIT Network Probe as a virtual machine, your environment must meet the following requirements:

- Hypervisor:
  - Microsoft Hyper-V version 10.0 or above
  - Oracle VirtualBox version 5.0.2 or above
  - VMWare—It can be one of the following:
    - ESXi version 5.5 or above
    - Fusion version 7 or above
    - Workstation version 12 or above
  - Virtual machine resource requirements:
    - CPU: 1x 64-bit Intel architecture
    - Memory: 512MB
    - Disk space: 5GB

To run FindIT Network Manager under Ubuntu Linux operating system, your environment must meet the following requirements:

- Ubuntu version 16.04.x (Xenial Xerus)
- CPU: 1x 64-bit Intel architecture
- Memory: 512MB
- Disk space: 5GB

To run the FindIT Network Probe on a Raspberry Pi operating system, your environment must meet the following requirements:

- Hardware: Raspberry Pi 3 Model B
- Disk space: 5GB
- OS: Raspbian Stretch

To run the FindIT Network Probe as an embedded application on a Cisco 100 to 500 series product, you must have a supported product running a firmware version that supports the FindIT Network Probe feature. Consult the Cisco FindIT Network Manager – Device Support List for details of hardware and version requirements. Also consult the administration guide for the product to determine any additional platform-specific requirements.

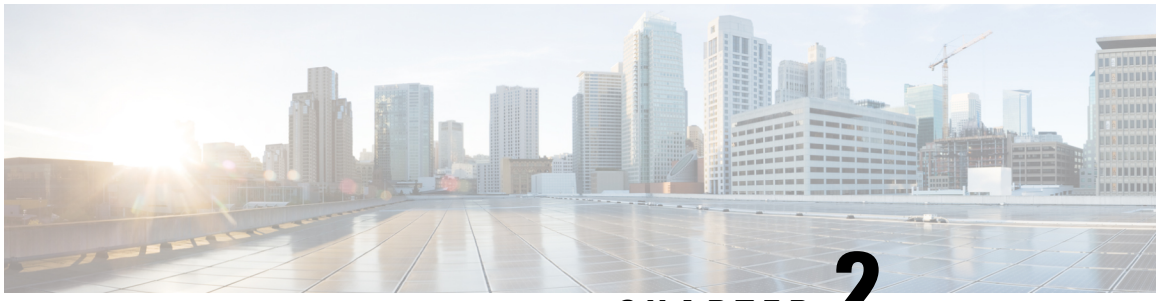
FindIT Network Probe is administered through a web user interface. To use this interface, your browser must be one of the following:

- Apple Safari version 11 (macOS only) or above
- Google Chrome version 72 (Recommended) or above
- Microsoft Edge version 42 or above

- Mozilla Firefox version 65 or above

FindIT Network Probe monitors and accesses the network devices that meet the following requirements:

- Must be in the same subnet as the PC that is running the FindIT Network Probe, or be directly attached to a managed device and reachable via TCP/IP
- Must be a Cisco 100 to 500 Series device with the Bonjour service enabled



CHAPTER 2

Using Cisco FindIT Network Manager and Probe

This chapter contains the following sections:

Using the Cisco FindIT Network Manager GUI

Overview of the Cisco FindIT Network Manager GUI with a description of the navigation pane links

Home window

Figure 1: Cisco FindIT Network Manager Home Page

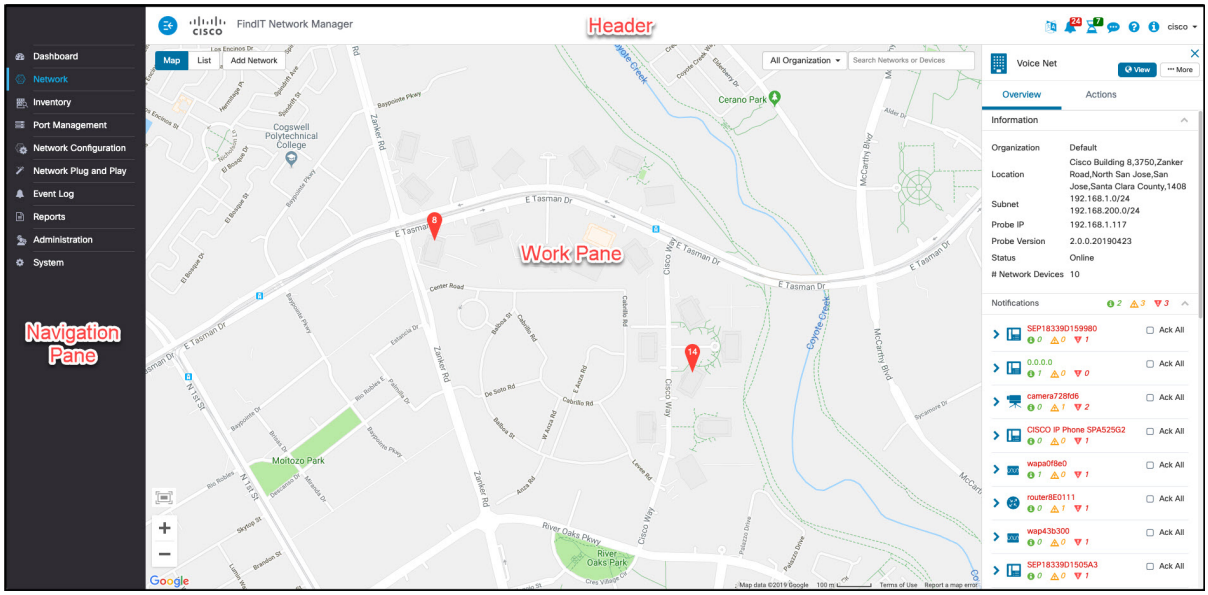


Table 2: Cisco FindIT Network Manager Home Page

Name	Description
Navigation pane	Provides access to the Cisco FindIT Network Manager features.
Work pane	Area where the feature interface is displayed. When you click an option in the **Navigation** pane, its corresponding window opens in this area.
Header toolbar	The header toolbar contains the following options: • A toggle button for expanding and collapsing the navigation pane • Header text • A series of icons for functions such as language selection, notifications, task activity, feedback, context sensitive help, and version information. • The username of the user who has logged into the application

Navigation Pane Options

The **Navigation** pane provides options to access the major Cisco FindIT Network Manager features.

Table 3: Navigation Pane Options

Icon	Name	Description
	**Dashboard**	The **Dashboard** allows you to monitor the performance of your network over time. The dashboard allows you to monitor traffic levels, connected device counts, and other details about the network.
	**Network**	Displays an overview of all of the locations in the network as either a map or a list. Contains different views of each network and the devices discovered. Views include the network topology and a floor-plan view that allows you to track the physical layout of the network.
	**Inventory**	The **Inventory** provides a list of all devices in the network, allows you to view detailed information about the devices, and to perform actions such as update firmware, backup configurations and reboot.
	**Port Management**	**Port Management** provides a front panel view of network devices and allows you to view details about individual ports and make configuration changes.
	**Network Configuration**	The **Network Configuration** page allows you to manage the configuration profiles for in your network.

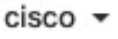
Icon	Name	Description
	**Network Plug and Play**	**Network Plug and Play** enables zero-touch deployment of network devices, allowing them to automatically download firmware and configuration files from FindIT Network Manager at the time of install.
	**Event Log**	The **Event Log** page provides a list of all the events that have occurred in the network, and allows you to use filters to limit the results to only events of interest.
	**Reports**	Under the Reports heading, you will find a number of reports that provide life-cycle information about your network devices, including end of life bulletins, warranty information and service contract details.
	**Administration**	The Administration pages allow you to maintain the FindIT Network Manager.
	**System**	The**System** pages are used to administer the FindIT Network Manager application.

Header Toolbar Options

The **Header** toolbar provides access to other system functions and displays system notifications.

Table 4: Header Toolbar Options

Icon	Option	Description
	**Toggle button**	Located on the top left of the header—This toggle button helps to expand or collapse the navigation pane.
	**Language Selection**	This drop-down list allows you to select the language for the user interface.
	**Notification Center**	This icon displays the number and severity of outstanding notifications in FindIT Network Manager. Click this icon to display the Notification panel. This panel provides capabilities to filter the notification events that are displayed. For more details, see Viewing and Filtering Current Device Notifications, on page 82 in this guide.
	**Task Status**	The Task Status and Task History for actions performed by FindIT Network Manager. Click this icon to display tasks pending, in progress, and completed.

Icon	Option	Description
	**Feedback**	Click to provide feedback about your experience using the Cisco FindIT Network Manager and any suggestions for improvements.
	**Help**	The online-help documentation for FindIT Network Manager.
	**About FindIT**	Click on this icon to see information about FindIT Network Manager, including the current version. If a new version is available, a badge will be displayed on the icon, and a link to apply the update will be available in the popup.
	**User Menu**	This dropdown shows the currently logged in user. Click to see the user role, and to open the user's profile page or to logout.

Using the Cisco FindIT Network Probe GUI

Overview of the Cisco FindIT Network Probe GUI with a description of the navigation pane links.

In version 2.0 and above of FindIT Network Probe, the Probe user interface is limited to a minimal interface sufficient for managing the Probe itself. All network management is performed through the FindIT Network Manager user interface. In the case where the probe application is embedded in a network device such as a switch or router, you should consult the documentation for that device for more information on managing the probe application, and the probe user interface is typically integrated with the device administration interface when the probe version is 2.0 or higher.

Home window

When you log into the Cisco FindIT Network Probe, the **Home** page appears.

Figure 2: Cisco FindIT Network Probe Home Page

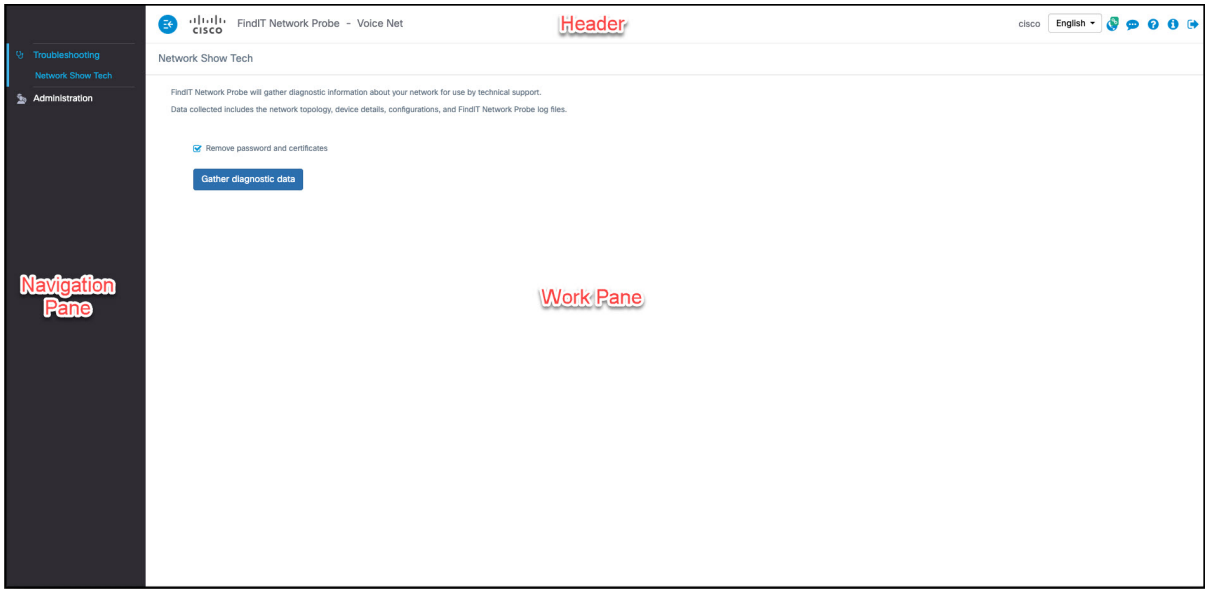


Table 5: Cisco FindIT Network Probe Home Page

Name	Description
Navigation pane	Provides access to the Cisco FindIT Network Probe features.
Work pane	Area where the feature interface is displayed. When you click an option in the **Navigation** pane, its corresponding window opens in this area.
Header bar	The header toolbar contains the following options: • A toggle button for expanding and collapsing the navigation pane • Header text including the site name of the Probe • The username of the user who has logged into the application • Language selection drop-down • A series of icons for functions such as notifications, feedback, context sensitive help, and logging out

Navigation Pane Options

The **Navigation** pane provides options to access the major Cisco FindIT Network Probe features.

Table 6: Navigation Pane Options

Icon	Name	Description
	**Troubleshooting**	Diagnostic tools that can help you identify problems with your network may be found under the **Troubleshooting** section.
	**Administration**	The **Administration** page allows you to maintain the FindIT Network Probe network application.

Header Bar Options

The **Header** bar provides access to other system functions and displays system notifications.

Table 7: Header Bar Options

Icon	Option	Description
	**Toggle button**	Located on the top left of the header—This toggle button helps to expand or collapse the navigation pane.
	**Language Selection**	This drop-down list allows you to select the language for the user interface.
	**Feedback**	Click to provide feedback about your experience using the Cisco FindIT Network Probe and any suggestions for improvements.
	**Help**	The online-help documentation for the Cisco FindIT Network Probe.
	**About FindIT**	Click on this icon to see information about Cisco FindIT Network Probe, including the current version. If a new version is available, a badge will be displayed on the icon, and a link to apply the update will be available in the popup.
	**Manager Status**	The status of the connection between FindIT Network Manager and the Probe. Click on this icon to open the Manager GUI.
	**Logout**	Click to log out of FindIT Network Probe.

Upgrading FindIT Network Manager and Probe

From time to time, Cisco releases new versions and updates for FindIT Network Manager & Probe and posts them to the Software Center on cisco.com. FindIT Network Manager periodically checks the Software Center for updates and, if one is found, displays a badge on **About FindIT** in the header panel of the UI. You can click to have the Manager download and apply the update, or you can choose to download the update yourself and manually apply it.

To have the Manager download and apply the update, do the following:

1. Click **About FindIT** to open the **About FindIT** popup. If updates are available for the Manager or any associated Probes, they will be listed here.
2. If an update is available for the Manager, select the radio button corresponding to that update and click **Upgrade**.

   The Manager will download and apply the update, and you may view the progress at any time on the **About FindIT** popup. Once the update is complete, the Manager application will restart.

To apply a Manager update manually, do the following:

1. Download the FindIT Network Manager Linux installer file by navigating to *www.cisco.com/go/findit* and selecting the Download Software for this Product link in the Support pane.
2. Copy the installer file to the Manager filesystem.
3. Execute the installer using the command **sh <filename of installer>**. For example **sh finditmanager-1.1.0-ubuntu-xenial-amd64.sh**. If necessary, enter your password at the sudo prompt. The Manager application will restart during this process.

   You may also apply updates to all the Probes in the network from the Manager. You may update all Probes in parallel, or you may update Probes individually.

To update all Probes in parallel from the Manager, do the following:

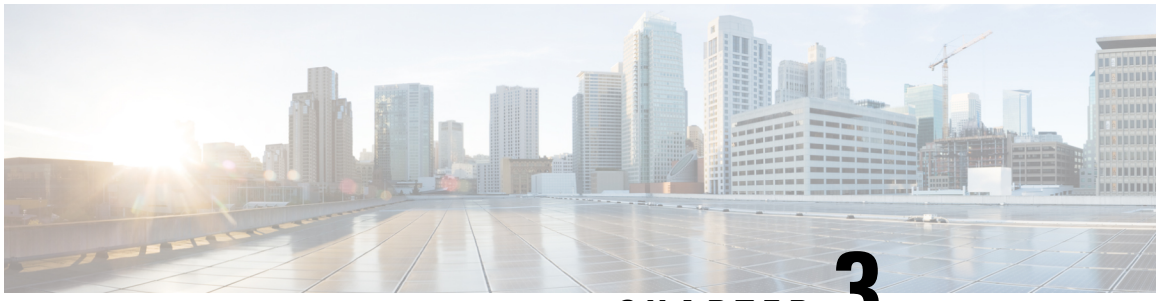
1. Click **About FindIT** to open the **About FindIT** popup. If updates are available for the Manager or any of the associated Probes, they will be listed here.
2. If an update is available for the Manager, perform that update before upgrading the probes. If you try to update the probes first, you will receive an error message.
3. Select the radio button next to the Probe update and click **Upgrade**.
4. You may view the progress of the update in the user interface of the Probe.

To update an individual Probe from the Manager, do the following:

1. If an update is available for the Manager, perform that update before upgrading any probes. If you try to update a probe before updating the Manager, you will receive an error message.
2. Select **Network** in the navigation. Select the site to be updated in either the **Map View** or the **List View**.
3. In the **Basic Info** panel for the site, select the **Actions** tab.
4. Click **Upgrade**.

You may view the progress of the update in the user interface of the Probe.

Note When using an embedded probe running on a network device, you should consult the documentation for that device to perform an update. Some devices do not support the updating of the Probe application independently of the device firmware.



CHAPTER 3

Dashboard

This chapter contains the following sections:

About Dashboard

The **Dashboard** page in the Cisco FindIT Network Manager lets you view the real-time performance of the network and its devices and provides the data in a graphical format. The dashboard is a customizable arrangement of user-selectable widgets. Following are the widgets included by default in the dashboard:

- **Inventory Summary widget**—Displays a breakdown of the devices discovered in the network.
- **Device Health** widget—Displays the overall health of the devices in the network
- **WLAN Client Count** widget—Displays the number of devices associated with the selected wireless network
- **Device Client Count** widget—Displays the number of devices associated with the selected wireless access point
- **Wireless Top Ten** widget – Displays the top ten wireless networks, access points, or clients based on traffic or client count
- **Traffic** widget—Displays a graph of the traffic flowing through the selected interface

Controls on each of the widgets allows the data shown to be customized. The organization dropdown at the top right of the **Dashboard** may be used to restrict the information displayed to a specific organization.

In the graphical widgets, you may click on the labels in the legend on the graph to toggle the display of each set of data. This allows you to further refine the data being shown.

Adding a Widget

This feature allows you to add one or more widgets to the existing default widgets displayed in the dashboard to monitor tasks specific to a device or network you wish to view.

Step 1 Click the gear icon located on the top right of the dashboard window and select **Add Widget**.

Step 2 Select the type of widget to add from the pop-up list. The newly chosen widget appears in the dashboard.

Step 3 Drag the new widget to the desired location in the dashboard and resize if necessary.

Step 4 Click the gear icon again and select **View Mode** to preserve the changes.

Modifying a Widget

Step 1 Use the drop-down lists within the new widget to select the specific data you wish to display.

Step 2 Click the gear icon in the top right of the widget to modify parameters such as sample interval or thresholds. You may also click the edit icon displayed on the widget when the dashboard is in **Edit Mode** to change the title of the widget.

Deleting a Widget

Step 1 Click the gear icon located at the top right of the dashboard window and select **Edit Mode**.

Step 2 Click the **remove widget** icon at the top right of the widget to be removed. Rearrange the remaining widgets as desired.

Step 3 Click the gear icon again and select **View Mode** to preserve the changes.

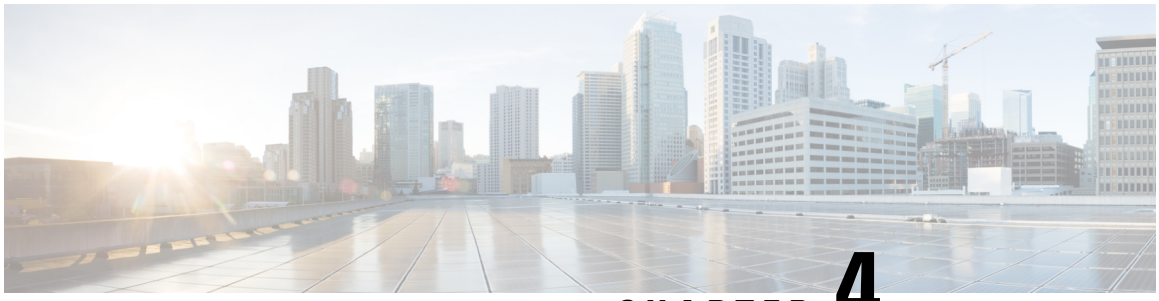
Modifying the Dashboard Layout

The **Dashboard** layout may be easily customized using the following steps:

Step 1 Click the gear icon located at the top right of the dashboard window and select **Edit Mode**.

Step 2 Click in the header of a widget and drag to move the widget in the **Dashboard**. Other widgets will adjust dynamically to make room. Click and drag on the edge or corner of a widget to resize. As you rearrange the layout, the dashboard will dynamically resize to fit in the available width.

Step 3 Click the gear icon again and select **View Mode** to preserve the changes.



CHAPTER 4

Network

This chapter contains the following sections:

About Network

The **Network** page provides an overview of the network as either a geographic map showing the location and status of each site in the network, or as a list of all sites. In the **Map View**, the number displayed on each network icon indicates the number of outstanding notifications that exist for that site, and the color of the icon indicates the highest severity level outstanding. In the **List View**, the same information can be seen in the last column of the table. To see more information about a network, click on the network icon or on the table row for that site.

When two or more network icons are positioned too closely on the map to be easily distinguished, they will be replaced with a single cluster icon. Clicking on the cluster icon will automatically zoom the map to a level where the networks in that cluster can be separated.

The **Network Map** offers the following controls:

- **Map/List** selection—Use this control to chose to view networks on a map or in a table.
- **Add Network** button—Use this button to create a new network record prior to deploying a probe for that network.
- **Organization** drop-down—Select an individual organization from the drop-down to limit the networks displayed.
- **Search** box—Enter all or part of the name, address or IP address of a network to locate that nework on the map. Alternatively, enter all or part of the name, IP address, serial number or MAC address of a device to identify the network where the device is located. As you type, a list of matches is displayed.

Hover over a match and the corresponding network will be highlighted. Select a match and the corresponding network will be selected and centered in the view.

- **Zoom** controls—Use these controls to zoom in and out of the map. Click the (✚) plus sign to zoom in and the (━) minus sign to zoom out.
- **Fit-to-view** button—This button automatically zooms out the map so that all network markers can be displayed.

You may also click and drag anywhere in the map area to move the map in the **Work** pane.

In the **List View**, the following controls are available:

- **Map/List** selection—Use this control to chose to view networks on a map or in a table.
- **Column Select** icon—This icon allows you to select the columns to be displayed. You can click on the column headings to sort the table.
- **Add Network**—Click the (✚) plus sign to add a new network prior to deploying a probe for that network.
- **Refresh**—Click the refresh button to update the table and display the most current information.
- **Organization** drop-down—Select an individual organization from the drop-down to limit the networks displayed.
- **Search** box—Enter all or part of the name, address or IP address of a network to list only matching networks in the table.

Clicking on a network icon or row brings up the **Basic Info** panel for that network. The **Basic Info** panel contains the following information:

- Network name
- The organization the network belongs to.
- The physical address of the network
- The Probe IP address for the network and the IP subnet(s) discovered at the network
- The software version of the Probe
- The connection status
- The number of managed devices in this network
- A list of all current, unacknowledged notifications for this network
- A list of events that occurred for this network in the previous 24 hours

You may also carry out the following actions for a network from the **Basic Info** panel:

- Click **Manage** to view a detailed information about the network including the network topology and floor plans
- Click **Settings** to display the **Network Detail** panel. See About Network Detail, on page 19 for more information on the **Network Detail** panel
- Click on the **Actions** tab to display additional actions available for the network
    - Click **Remove** to delete this network and all associated data from the manager

- Click **Upgrade** to update the Probe software at this network
- Click **Show Tech** to generate a Network Show Tech archive for this network

About Network Detail

The **Network Detail** panel allows you to view and update information specific to that network. This information includes:

- Key network parameters including the network name, description, organization and default device group
- The location of the network
- The credentials to use for the network when uploading inventory information to Cisco Active Advisor
- Logging configuration for the Probe in this network. See Managing Probe Log Settings, on page 86 for more information on configuring Probe logs

About Network View

Click **Manage** in the network's **Basic Info** panel, to display the **Network View** of that network. The **Network View** offers multiple views of the network:

- **Topology** view—Displays a logical topology of all the discovered devices in the network. Information about each device is displayed, and you may perform actions on selected Cisco products
- **Floor Plan** view—Lets you document the physical location of your network devices in your environment

Following are the additional controls provided in common for all the tasks that you perform in the **Network View**:

- **Organization and Network** selection—These dropdowns allow you to switch between networks and organizations without returning to the main network page. To view the topology or floorplan for a different network, simply select that network using the dropdown
- **Network Actions** dropdown—This dropdown allows selected actions to be performed on all devices in the network that support that action. For example, you may backup all network device configurations with a single click. The **Network Actions** dropdown also allows you to restart the discovery process for the network, and upload your inventory to Cisco Active Advisor at *https://www.ciscoactiveadvisor.com*. For more information about Cisco Active Advisor, see *https://help.ciscoactiveadvisor.com*

Overview of the Topology Map and Tools

About the Topology Map

The FindIT Network Manager & Probe query discovered devices for network connectivity details and build a graphical representation or topology from the information gathered. The data collected includes CDP & LLDP neighbor information, MAC Address tables, and Associated Device tables from Cisco 100 to 500 Series

switches, routers and wireless access points. This information is used to determine how the network is constructed. When the network contains network infrastructure devices that are not manageable for any reason, FindIT Network Manager & Probe will attempt to infer the topology based on the information that can be collected.

You may click on devices or links in the topology to display the **Basic Info** panel for that device or link. The **Basic Info** panel provides more detailed information about the device or link, and allows you to carry out different actions on a device.

Clicking on **Overlays** in the **Topology Map** displays the **Overlays & Filters** panel. This panel allows you to limit the devices displayed in the topology by device type or by tag. It also allows you to enhance the topology to show additional information such as the traffic load on links or how a particular VLAN is configured in the network.

Accessing the Topology Map

To access the **Topology Map**, first select **Network** from the **Navigation**, click the icon or table row for the network you are interested in, then click **View**. The **Topology Map** for that network is displayed in the work pane.

Topology Controls

The Topology Controls are located on the top left of the **Topology Map**.

Table 8: Topology Controls

Icon	Icon Name	Description
	**Zoom in**	Adjusts the **Topology** window's view. Click the ✚ (plus) icon on the menu bar to increase the size of the network in the viewing area.
	Zoom out	Adjusts the **Topology** window's view. Click the ━ (minus) icon to reduce the size of the network in the viewing area.
	**Relayout Topology**	Re-enable automatic layout of the topology after it has been disabled by manual changes. Redraw the topology using the automatic layout algorithm.
	**Zoom by selection**	Click and drag to select an area to zoom in on.
	**Fit stage**	Zoom until the entire network fills the viewing area.
	**Enter full screen mode**	Fill the screen with the FindIT Network Manager user interface.
	**Export Topology**	Export the current topology view as an image in PNG format. The image will be saved to the default download location for the browser.

Icon	Icon Name	Description
	**Topology Settings**	Adjust the labels displayed for the topology icons.

Topology Icons

The following icons appear in the **Topology** window:

Table 9: Topology Icons

Icon	Network Element	Description
	**Access Point**	Representation of a Wireless Access Point.
	**Cloud**	Represents a network or part of a network that is not managed by FindIT Network Probe.
	**Links**	Links are connection lines between devices. Click a link to display the target and the source device names and other basic details such as speed and so on. The thickness of the link represents the speed of the link, with a thin line representing 100Mbps or below and a thick line representing 1Gbps or above. A dashed line represents a wireless connection.
	**Router**	Represents a Router.
	**Switch**	Represents a Switch.
	**Host**	Represents a host attached to the network using a wired connection.
	**Wireless Host**	Represents a host attached to the network using a wireless connection.

Overlays & Filters Panel

This panel appears on the right of the **Topology** map when **Overlays** is clicked. **Overlays** may be found at the top-right of the Topology, next to the **search** box.

Table 10: Overlays & Filters Panel

Item	Description
Select Overlay	This feature enhances the **Topology** map with additional information based on the view selection. It can be one of the following: • **Link Utilization View**—Identifies current network performance by monitoring the amount of traffic. This traffic is displayed using the color coded links in the **Topology** map. The color coding changes based on the percentage utilization of the link. Green represents links that are only moderately loaded, while orange and red represent links that are approaching capacity limits. Controls are provided to allow you to adjust the thresholds for different colors. • **VLAN View**—Displays where a VLAN is enabled in the network. This can be used to identify a partitioned VLAN or other misconfiguration. On selecting **VLAN View** in the Overlay drop-down, a second drop-down box appears below this field where you can select the VLAN ID to be displayed. • **POE View**—Highlights links in the topology map which indicates devices that are currently being powered from a POE-enabled switch. • **L2 Path Trace**—Shows the layer 2 path traffic between the two selected devices takes through the network. Devices may be selected by typing the hostname, MAC address or IP address in the fields provided, or by shift-clicking on two devices in the topology map.
Select Tag	Specify a **Device Tag** in the text box below the **Select Tag** label to filter the topology to show devices matching the specified tag. Device tags are assigned in the **Detailed Info** panel.
Show only: • **Routers** • **Switches** • **Wireless** • **Hosts** • **Others**	Check the check box against the devices in the list that you wish to view in the **Topology** map. This feature helps you filter the devices you want to view in the map and removes the ones that are unchecked in the device list.

Viewing Basic Device Information

Click on a network device such as a switch or a router, or a link connecting two devices, to view basic information about the device including outstanding notifications, and actions that may be performed. The **Basic Info** panel also provides access to more detailed information for a device, and allows you to directly access the administration interface of the device.

Note To view detailed information for a device, see Viewing Detailed Device Information, on page 26.

To view more information on accessing the device administration interface, see Accessing the Device Administration Interface, on page 26.

The table in the following section provides the type of device details that are displayed. To view the basic device information do the following:

Step 1 In the **Network** page, select a network and click **Manage** to display the topology.

Step 2 In the Topology map, click on a network device such as a switch or a router for which you want to view the details.

Step 3 In the **Basic Info** panel, the device details are displayed under the **Overview** tab. Each of these items are described in the following table.

Table 11: Basic Device Information

Item Name	Description
Information Panel	
Model	Model name of the device.
Description	Device or product description.
Firmware Version	The firmware version of the device.
PID VID	Product ID and the Version ID.
MAC Address	The *Media Access Control (MAC)* address is a standardized data link layer address that is required for certain network interface types. These addresses are specific and unique to each device and are not used by other devices in the network.
Serial Number	The device serial number.
Status	The online / offline status of the device.
Domain	The domain name of the device.
Vendor	The manufacturer of the device.
Network	The name of the network where the device is located.
Organization	The organization to which the device belongs.
Notification Panel	

Item Name	Description
Notifications Panel Header—The notifications panel header shows summary counts of the outstanding notifications for the device. **Notifications Panel Body**—The body of the notifications panel lists the outstanding notifications for the device. To view and filter a complete list of all device notifications, see Viewing and Filtering Current Device Notifications, on page 82. Check the check box against a notification to acknowledge it and remove it from the list of notifications. You may use notification filtering to display acknowledged notifications if needed..	
Events Panel	
The Events Panel shows a list of all notifications and other events that have occurred over the past 24 hours for this device. To view and filter a complete list of all events for all devices, visit the Event Log on the Manager.	
POE Panel	
The POE Panel is displayed on POE enabled switches and provides a summary of the power usage across each of the ports in the device.	
Stack Information Panel	
The Stack Information panel is displayed for switch stacks, and shows the hardware details for each member of the stack, including model information, serial number and MAC address	
Service	
Lists the network services identified on the device.	
Connected Device	
Host devices include the **Connected Device** panel. This panel shows how the host is attached to the network, listing the upstream network device and, where applicable, port that the host is connected to.	

In addition to the **Overview** tab, the **Basic Info** panel also has an **Actions** tab that allows you to perform various operational tasks on the device. For details, refer to Performing Device Actions, on page 24.

Performing Device Actions

Actions such as firmware update, configuration backup & restore and reboot are easily performed for devices in the network. To perform these actions, do the following:

Step 1 On the **Topology Map** or **Inventory** page, click on a network device such as a switch or a router for which you want to perform the action.

Step 2 In the **Basic Info** panel, select the **Actions** tab. Depending on the device capabilities one or more of the following actions are displayed:

Update firmware to latest	Allows you to apply the latest firmware update to the device. The Probe will download the update from Cisco and then upload it to the device. The device will reboot at the completion of the update.
Upgrade From Local	Allows you to upload a firmware upgrade file from your local drive. The Probe will upload the file to the device, and the device will reboot at the completion of the update.
Backup Configuration	Allows you to save a copy of the current device configuration on the Manager. **1.** Click **Backup Configuration**. **2.** In the **Backup Configuration** window, optionally, you may add a note in the text box for the backup you wish to perform. **Note** This note is displayed whenever the backup is listed in the GUI. **3.** Click **Save Backup** to complete this action or **Cancel** if you no longer wish to proceed. A backup configuration job is created and may be viewed in the **Task Center**.
Restore Configuration	Allows you to restore a previously backed up configuration to the device. Click **Restore Configuration**. The following backup configuration options are provided: • **Backups for *device name***—Lists all available backups to configure for a specific device • **Backup for other device**—Lists all available backups to configure other devices of the same type or same Product ID • **Backup for other compatible device**—Lists all available backups to configure other devices in the series that are compatible with the selected device To perform the backup configuration, do the following: **1.** In the **Restore Configuration** window, select the backup you wish to restore to the device. Use the scroll bar to view all the available backups and click the corresponding radio button. This enables the **Restore Configuration** button. Alternatively, you may choose to upload a configuration file. To do so, drag and drop the configuration file onto the target area, or click on the target area to select a file from the file system. **2.** Click **Restore Configuration** to complete this action. A restore configuration job is created and may be viewed in the **Task Center**.
Reboot	Restarts the device. **Note** When you click this button, you will be prompted to click again to confirm.

Save Running Configuration	For devices that support separate running and startup configurations, this action copies the current running configuration to the startup configuration. This ensures any configuration changes that are retained when the device next reboots.
Delete	Remove an offline device from the Topology and Inventory.

Accessing the Device Administration Interface

In some circumstances, you may need to access the administration interface of a network device directly. To access the administration interface, do the following:

Step 1 On the **Topology** or **Inventory** page, click on a network device such as a switch or a router for which you want to access the administration interface.

Step 2 In the **Basic Info** panel, click **View** at the upper right corner. A new window will open in your browser showing the device administration interface

Note When you access the administration interface by clicking **View**, your browser will connect to the device through the Manager. This means that if you are accessing the network remotely, only the Manager needs to be directly reachable from outside the site.

Because these connections all go through the same host - the Manager - cookies for one device will be presented to other devices, and may be updated by other devices if the name is the same. A common symptom of this is the browser session on the first device will be immediately logged out after connecting to a second device because the session cookie has been updated.

Viewing Detailed Device Information

Step 1 On the **Topology** or **Inventory** page, click on a network device such as a switch or a router for which you want to view detailed information.

Step 2 In the **Basic Info** panel, click **More** at the upper right corner.

Step 3 In the **Detailed Info** panel, you will find a detailed list of device information on the left, and additional functions under the following tabs:

- **Dashboard**—Displays a series of dashboard widgets specific to the device
- **Port Management**—Allows you to manage the configuration of the switch ports

  Note This information is available only for devices with switch ports.

- **Wireless LANs**—Allows you to view the Wireless LANs configured on the device

  Note This information is available only for wireless devices.

- **Event Log**—Provides a list of past actions and notifications for this device
- **Config Backups**—Allows you to view a list of backup configuration of the devices and perform actions such as restore, save or delete configuration

  Note This information is available only for devices that support the Backup Configuration operation

- **Pending Config**—Compares the desired configuration based on the configuration profiles defined with the current configuration on the device and highlights any differences.

  Note This panel is only displayed for devices supported for configuration operations where the current configuration does not match the desired configuration.

Each of these are described in the following steps:

Step 4 A detailed list of information about the device is displayed on the left. This list contains the following information:

Table 12: Detailed Device Information

Item Name	Description
Hostname	Click **Edit** next to the device name to modify the device hostname. Click **Save** to save the changes.
Model	Model name of the device.
MAC Address	The *Media Access Control (MAC)* address is a standardized data link layer address that is required for certain network interface types. These addresses are specific and unique to each device and are not used by other devices in the network.
Status	Displays the current status of the device. For example, online or offline.
Actions	The **Actions** dropdown and **Open Device GUI** icon allow you to act on the device from the **Detailed Info** panel.
IP	The IP Addresses of the device.
Domain	The domain name of the device.
PID VID	Product ID and the Version ID.
Serial Number	The serial number of the device.
Vendor	The manufacturer of the device.
Description	Device or product description.
Device Group	The device group that this device belongs to.
Network	The network that this device belongs to.
Organization	The organization that this device belongs to.
PnP Parameters	The image and config file to be delivered to the device using Network Plug and Play. Click the **Edit** icon to make changes, then click the **Save** icon to apply the changes or **Cancel** to exit without saving.

Item Name	Description
TAGs	In the TAGs field, enter any alphanumeric characters and then press **Enter** to create new tags for this device. To delete an existing tag, click on the ✖ in the tag. Click **Save** to save the changes. Tags may be used to help identify devices with common characteristics. You may use tags elsewhere in FindIT Network Probe to restrict views of the network to displaying a subset of devices.
Firmware Version	The version of the firmware currently running on the device. If a later version is available, then that version is displayed in parentheses beside the current version. Icons are also provided to view the release note for the update, and to apply the same to the device.
Discovery Method	Displays the protocols and devices by which this device was discovered.
Pending Config	Displays the status of the device configuration and whether there are any differences between the current config for the device and the expected config.

Step 5 Click **Dashboard** to display a set of widgets showing the current state of the device. For more details, see About Dashboard.

Step 6 Click **Port Management** to view and manage the configuration of the switch ports on the device. A visual representation of the device is displayed, similar to that shown in the **Port Management** page.

This window specifies the port details of the device in a visual representation. The model and serial number of the device are displayed above the image and a tabular view of the ports is displayed underneath. For more details on the operations, see About Port Management, on page 33.

Step 7 Click **WLAN** to view the radio settings and the Wireless LANs configured on this device.

Step 8 Click **Event Log** to see a list of historical notifications and other events that are recorded for this device. You can use filters to limit the entries that are displayed. For more details, see About the Event Log.

Step 9 Click **Config Backups** to view and manage configuration backups for this device. On this tab, you will see a table listing each backup stored on the Probe, with the following details:

Table 13: Config Backups

Item	Description
Timestamp	The date and time the configuration backup was taken.
Comment	The notes entered by the user at the time the backup was performed.
Backed up by	The user who performed the configuration.
Actions	Choose one of the following backup actions: • **Restore configuration to device**—Restores the selected backup to the device • **Save configuration to PC**—Saves the backup as a zip file to your local drive on your PC • **Delete configuration**—Removes the backup from the Probe • **View configuration**—Helps view the contents of the configuration backup in the browser

You may also trigger a config backup from the tab by clicking **Backup Configuration**.

Step 10 Click **Pending Config** to view a side-by-side comparison between the current device config and the expected configuration based on the configuration profiles applied to the device. Configurations are represented in a device-independent format and any differences are highlighted. You may use the buttons at the top of the page to apply any outstanding changes, accept the current device configuration, or re-read the current device configuration.

Using Floor Plans

The Floor Plan view allows you to keep track of the physical locations of your network equipment. You may upload a plan for each floor in the building(s) and position each of the network devices on the plan. This helps you to easily locate devices if maintenance is required. The Floor Plan is similar in operation to the Topology Map, and devices placed on the Floor Plan may be operated in the same way as devices in the Topology Map.

Creating a New Floor Plan

1. Navigate to **Network View** and click **Floor Plan**. If an existing floor plan is displayed, click the **Home** icon at the top left of the floorplan.
2. If the building you wish to add a floor plan to has already been created, go to the next step. Otherwise, enter a name for the building that houses the floor into the **New Building** field. Click the **save** icon.
3. Drag and drop an image file containing the floor plan onto the target area for the new floor, or click on the target area to specify a file to upload. Supported image formats are `png`, `gif`, and `jpg`. Image files can be a maximum of 500KB in size.
4. Enter a name for the floor into the **New Floor** field. Click the **save** icon.
5. Repeat steps 2 to 4 for each building and floor with network devices.

Placing Network Devices on a Floor Plan

1. Navigate to **Network View** and click **Floor Plan**. If the floor plan you are interested in is not already displayed, then click on the floor plan.
2. Click **Add Devices**, and then use the search box at the bottom left to find the device you wish to place. You may search by hostname, device type, or IP address. As you type, matching devices will be displayed below the search box. Gray icons represent devices that have already been placed on a floor plan.
3. Click and drag a device to add it to the floor plan in the correct location. If you select a device that has already been placed on another floor plan, it will be removed and added to this one.
4. Repeat steps 2 & 3 until all devices have been added to the floor plan.

Removing a Device from the Floor Plan

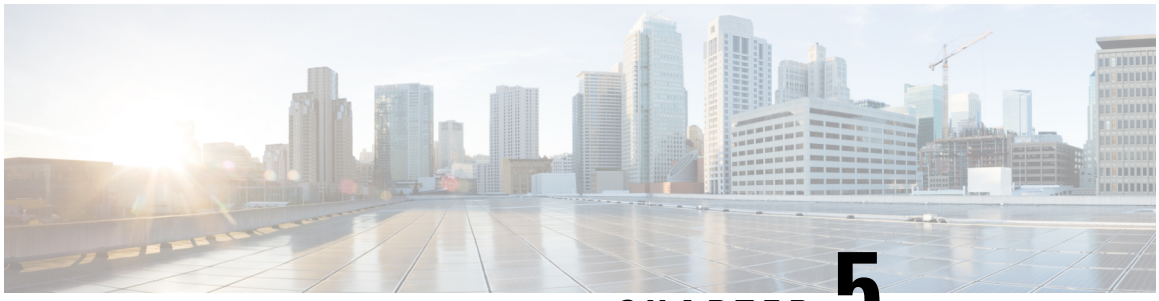
1. Navigate to **Network View** and click **Floor Plan**. If the floor plan you are interested in is not already displayed, then click on the floor plan.
2. Identify the device you wish to remove and click to select it.
3. Click on the red cross that is displayed to remove the device from the floor plan.

Changing the Floor Plan

1. Navigate to **Network View** and click **Floor Plan**. If an existing floor plan is displayed, click the **Home** icon at the top left of the floorplan.
2. To change a building name, click the **edit** icon next to the name. Once the changes are complete, click the **save** icon.
3. To change a floor plan, click the **edit** icon next to the floor plan name. You may change the floor plan by dragging a new image file to the target area, or clicking on the target area to upload a new file from your PC. You may also change the name of the floor plan. Once the changes are complete, click the **save** icon.

Removing a Floor Plan

1. Navigate to **Network View** and click **Floor Plan**. If an existing floor plan is displayed, click the **Home** icon at the top left of the floorplan
2. Identify the floor plan you wish to remove, and click the **delete** icon at the top right corner of the image target area.
3. If you wish to remove an entire building containing all the floor plans, click the **delete** icon next to the building name.



CHAPTER 5

Inventory

This chapter contains the following sections:

Viewing Device Inventory

The **Inventory** page displays a complete list of the devices and their details in a tabular view. Additionally, it also provides action buttons to perform configuration tasks and apply the latest firmware updates for supported devices. The following table provides details of the information displayed:

Table 14: Inventory Details

Item	Description
Hostname	Displays the name of the device.
Type	The type of device such as a switch, router or wireless access point (WAP).
Tags	Lists any tags associated with the device.
IP	The Internet Protocol (IP) addresses of the device.
MAC (hidden by default)	The Media Access Control (MAC) address is a standardized data link layer address that is required for certain network interface types. These addresses are specific and unique to each device and are not used by other devices in the network.
Serial Number	The serial number for the device.
Version	The current firmware version of the device.
Model	Model name of the device.
Organization	The organization to which the device belongs.
Network	The network to which the device belongs
Notification	A count of the outstanding notifications for the device

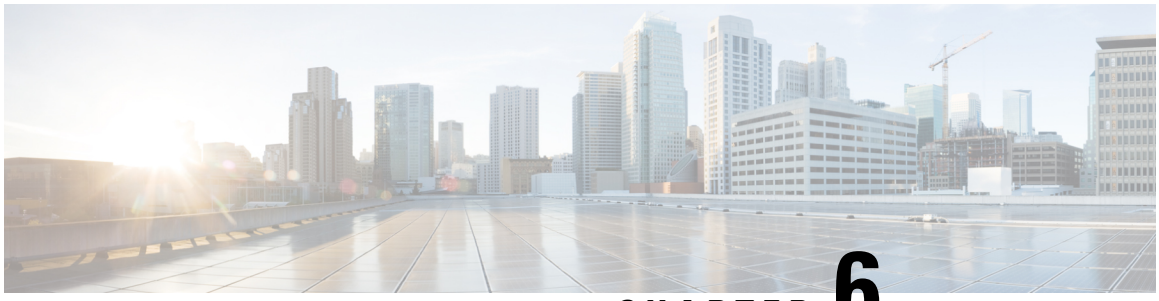
Item	Description
PnP Status (hidden by default)	The current Network Plug and Play status for the device. For more information, see the **Network Plug and Play** pages.

The following additional controls are available on the **Inventory** page:

- **Select columns** button—Use this button located at the top left of the table to choose which columns to display
- **Filter Box**—You may use the **Filter box** to limit the display by typing device names, device types, serial numbers and so on. By default, the inventory is filtered to display only network devices
- **Add** icon—Click the (✚) plus icon to add new devices to the inventory prior to the device being discovered. When manually adding a device to the inventory you can provide basic information about the device including identity information, organization and device group, and PnP settings. Providing this information ahead of time ensures the device will be correctly managed when it is connected to the network
- **Refresh** button—Click this button to update the table to show the latest available information
- **Actions** buttons—The following action buttons allow you to perform actions on one or more selected devices
  - **Download Latest Firmware**
  - **Apply Firmware Upgrade From Local**
  - **Backup Configuration**
  - **Restore Configuration**
  - **Reboot Device**
  - **Save Running Configuration**
  - **Delete**

  Action buttons are only displayed when one or more devices supporting actions are selected.

Note For more details on these actions, see Performing Device Actions



CHAPTER 6

Port Management

This chapter contains the following sections:

About Port Management

Port Management provides a front panel view of each device that includes switch ports that may be configured by FindIT Network Manager. This page allows you to view the status of the ports including traffic counters, and make changes to the port configuration. This page also lets you view and configure the Smartports role for ports on devices that support Smartports. You may use the search box to limit the devices displayed. Type in all or part of a device name, product ID, or serial number to find the desired device.

A list view of the same information is also provided to show all the switch ports in a tabular format. The front panel view in **Port Management** presents two different views of the device:

- **Physical**—This view allows you to see the status and change the configuration of the port at the physical layer. You may view or change settings for speed, duplex, flow control, Energy Efficient Ethernet (EEE), Power over Ethernet (PoE), and VLANs. Each port is shown with a green LED indicating link and a yellow LED indicating that power is being supplied to the attached device
- **Smartports**—This view allows you to see the current Smartports role for each port, and to change the role. Each port is overlaid with an icon indicating the current role

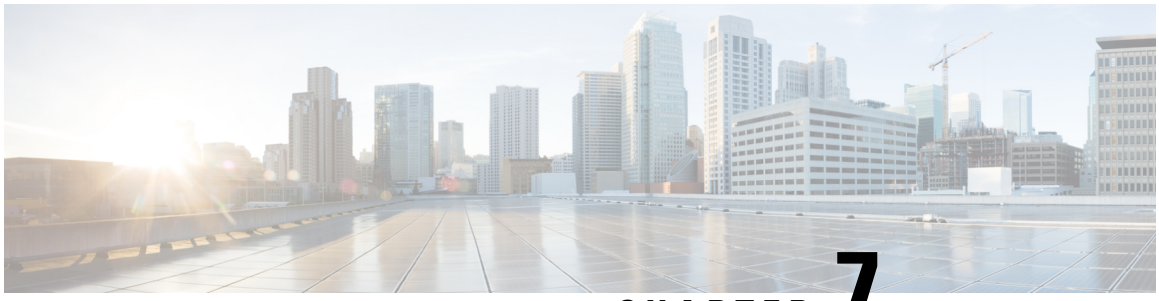
Note A Smartport is an interface to which a built-in (or user-defined) template may be applied. These templates are designed to provide a means of quickly configuring the device to support the communication requirements and utilize the features of various types of network devices.

To view the status of a port, click on the port in either the front panel view or list view. The **Basic Info** panel for the port appears, showing a series of panels as follows:

- **General**— The **General** panel shows the physical layer status of the port
- **Ethernet**— Allows you to control speed and duplex settings
- **VLAN** — The **VLAN** panel shows the VLANs currently configured on the port. Click the **Select VLAN** or **Create VLAN** buttons to modify this configuration

- **POE**—The **POE** panel is only displayed for POE-enabled ports, and allows you to configure the POE settings for the port. You may also power-cycle an attached POE device by clicking the Toggle Power button
- **Green Ethernet**—The **Green Ethernet** panel allows you to manage the Energy Efficient Ethernet (EEE) configuration for the port
- **Smartports**—The **Smartports** panel shows the Smartports roles available for this port. Click on a role to apply that configuration to the port. The currently configured role is highlighted.

To make changes to the port settings, click the **edit** icon in the top right of the pane containing that setting. Once the changes have been made, click the **Save** icon.



CHAPTER 7

Network Configuration

This chapter contains the following sections:

About Network Configuration

The **Network Configuration** pages allow you to define various configuration parameters that typically apply to some or all devices in the network. These parameters include configuration such as time settings, domain name services, administrator authentication, and Virtual LANs and Wireless LANs. You may create configuration profiles for each of these areas separately, or you may use the wizard to create profiles for each area in a single workflow. The configuration profiles are applied to one or more device groups, and then pushed out to the devices.

Using the Wizard

The wizard allows you to create configuration profiles for each of the Network Configuration elements and assign those profiles to one or more device groups in a single workflow.

Using the Wizard

1. Navigate to **Network Configuration** > **Wizard**.
2. In the **Device Group Selection** screen, enter a profile name for this configuration, choose an organization and select one or more device groups to be configured. Click **Next**.
3. In each of the screens that follow, select the configuration as required. For more details on these parameters, see the following sections.

4. Complete the configuration settings on each screen and click **Next**. If you do not wish to configure settings on a particular screen for this profile, click **Skip**. Click **Back** to visit the previous screens or you may click the headings on the left.
5. Complete the configuration and review the settings on the final screen. Click **Finish** to apply the configuration to the selected devices.

Configuring Time Management

The **Time Management** page allows you to configure timezones, daylight saving, and NTP servers for the network. The following sections provide you instructions on creating, modifying and deleting the Time Settings configuration profile.

Creating a Time Management Configuration Profile

1. Navigate to **Network Configuration** > **Time Management**.
2. Click the ✚(plus) icon to add a new profile.
3. On the **Device Group Selection** section, enter a profile name for this configuration, choose an organization and select one or more device groups to be configured.
4. In the **Time Setting** section, select an appropriate timezone from the drop-down list.
5. Optionally enable **Daylight Saving** by checking the check box, and then specify the parameters for daylight saving in the fields provided. You may choose to specify fixed dates or a recurring pattern. You may also specify the offset to be used.
6. Optionally enable the Network Time Protocol (NTP) in the **Use NTP** section for clock synchronization by checking the check box. In the boxes provided specify at least one NTP server address.
7. Click **Save**.

Modifying a Time Management Configuration Profile

1. Select the radio button next to the profile to be changed, and click the **edit** icon.
2. Make the required changes to the profile settings and click **Update**.

Removing a Time Management Configuration Profile

1. Select the radio button next to the profile which needs to be removed.
2. Click the **delete** icon.

Configuring DNS Resolvers

The **DNS Resolvers** page allows you to configure the domain name and domain name servers for the network. The following sections provide you instructions on creating, modifying and deleting the DNS resolvers configuration profile.

Creating a DNS Resolver Configuration Profile

1. Navigate to **Network Configuration** > **DNS Resolvers**.
2. Click the ✚(plus) icon to add a new profile.
3. On the **Device Group Selection** section, enter a profile name for this configuration, choose an organization and select one or more device groups to be configured.
4. Specify the domain name for the network.
5. Specify at least one DNS server address.
6. Click **Save**.

Modifying a DNS Resolver Configuration Profile

1. Select the radio button next to the profile to be changed, and click the **edit** icon.
2. Make the required changes to the profile settings and click **Update**.

Removing a DNS Resolver Configuration Profile

1. Select the radio button next to the profile to be removed.
2. Click the **delete** icon.

Configuring Authentication

The **Authentication** page allows you to configure administrative user access to network devices. The following sections provide you instructions on creating, modifying and deleting the authentication configuration profile.

Creating an Authentication Configuration Profile

1. Navigate to **Network Configuration** > **Authentication**.
2. Click the ✚(plus) icon to add a new profile.
3. On the **Device Group Selection** section, enter a profile name for this configuration, choose an organization and select one or more device groups to be configured.
4. Specify at least one username and password combination for local user authentication. Additional users may be added by clicking the ✚ (plus) icon.
5. You may also choose to require the use of complex passwords.
6. Click **Save**.

Modifying an Authentication Configuration Profile

1. Select the radio button next to the profile to be changed, and click the **edit** icon.
2. Make the required changes to the profile settings and click **Update**.

Removing an Authentication Configuration Profile

1. Select the radio button next to the profile which needs to be removed.
2. Click the **delete** icon.

Configuring Virtual LANs

The **Virtual LANs** page allows you to split your switch network into multiple virtual networks or VLANs. You can find the existing VLANs in the network that were not configured by the Manager also displayed on this page in a separate table. The following sections provide you instructions on creating, modifying and deleting Virtual LAN configuration profiles.

Creating a Virtual LAN

1. Navigate to **Network Configuration** > **Virtual LANs**.
2. Click the ✚(plus) icon to add a new VLAN.
3. On the **Device Group Selection** section, enter a profile name for this configuration, choose an organization and select one or more device groups to be configured.
4. Specify a descriptive name for the VLAN, and the VLAN ID to be used. The VLAN ID should be a number in the range 1-4094.
5. You may create multiple VLANs using a single profile. If you want to create additional VLANs in this profile, click **Add Another** and go back to step 4.
6. Click **Save**. The new VLAN will be created on all VLAN-capable devices in the selected groups.

If the VLAN ID of the newly created VLAN matches an existing VLAN already present on devices in the device group, that VLAN will be adopted by the Manager and removed from the discovered Virtual LANs table.

Modifying a VLAN

1. Check the radio button next to the VLAN to be changed, and click the **edit** icon.
2. Make the required changes to the VLAN settings and click **Update**.

Removing a VLAN

Check the radio button next to the VLAN to be removed, and click the **delete** icon.

Removing a VLAN not created by the Probe

In the table of discovered VLANs, click the **delete** icon next to the VLAN or VLANs to be removed.

Note VLAN 1 may not be deleted.

Configuring Wireless LANs

The **Wireless LANs** page allows you to manage the wireless networks in your environment. You can find the existing Wireless LANs in the network that were not configured by the Manager also displayed in a separate table. The following sections provide you instructions on creating, modifying and deleting Wireless LAN configuration profiles.

Creating a Wireless LAN

1. Navigate to **Network Configuration** > **Wireless LANs**.
2. Click the **+**(plus) icon to add a new Wireless LAN.
3. On the **Device Group Selection** section, enter a profile name for this configuration, choose an organization and select one or more device groups to be configured.
4. Specify an SSID name for the Wireless LAN, and the VLAN ID that it should be associated with. The VLAN ID should be a number in the range 1-4095, and if it does not already exist in the network, a new VLAN will be created automatically.
5. Optionally change the **Enable**, **Broadcast**, **Security** and **Radio** settings to match your requirements.
6. You may create multiple Wireless LANs using a single profile. If you want to create additional Wireless LANs in this profile, click **Add Another** and go back to step 3.
7. Depending on the security mode selected – **Enterprise** or **Personal** – specify either the RADIUS server to be authenticated against, or a pre-shared key.
8. Click **Save**. The new WLAN will be created on all devices with wireless access point capabilities in the selected groups.

If the Wireless LAN configuration of the newly created profile matches an existing Wireless LAN already present on devices in the device group, that Wireless LAN will be adopted by the Manager and removed from the discovered Wireless LANs table.

Modifying a Wireless LAN

1. Check the radio button next to the Wireless LAN to be changed, and click the **edit** icon.
2. Make the required changes to the Wireless LAN settings and click **Update**.

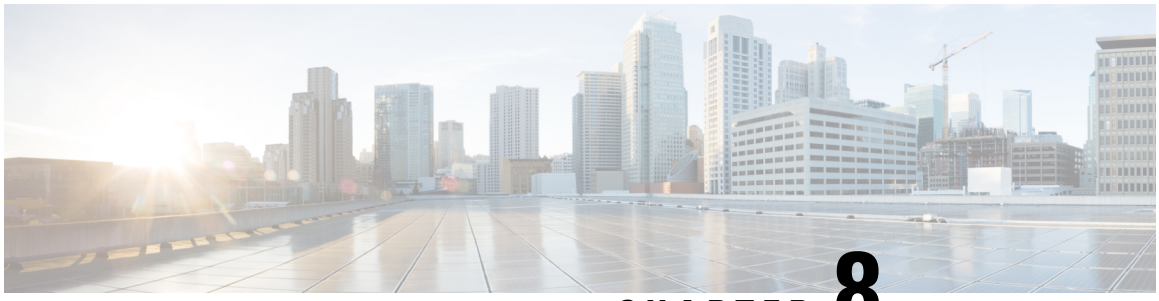
Removing a Wireless LAN

Select the radio button next to the Wireless LANs to be removed, and then click the **delete** icon.

Note If a Virtual LAN was created automatically when creating the Wireless LAN, the Virtual LAN will not be deleted when the Wireless LAN is deleted. The Virtual LAN may be deleted on the **Virtual LANs** page.

Removing a Wireless LAN Not Created By the Manager

In the table of discovered Wireless LANs, click the radio button for the Wireless LAN to be removed and then click the **delete** icon. In some cases, a WLAN may not be able to be deleted from certain devices. In these cases, it will be necessary to make changes to the device configuration directly.



CHAPTER 8

Network Plug and Play

This chapter contains the following sections:

About Network Plug and Play

Network Plug and Play is a service that works in conjunction with Network Plug and Play enabled devices to allow firmware and configuration to be managed centrally, and to allow zero-touch deployment of new network devices. When installed, a Network Plug and Play enabled device will identify the Network Plug and Play server through one of manual configuration, DHCP, DNS, or the Plug and Play Connect service. The following sections provide more detail on the configuration of the Network Plug and Play service in Cisco FindIT Network Manager.

Network Requirements

A Network Plug and Play device will automatically find the address of the Network Plug and Play server using one of the following methods. Each method will be attempted in turn until an address is found or all methods have failed. The methods used are, in order:

- **Manual configuration**—A Network Plug and Play enabled device may be manually configured with the address of the server through the administration interface
- **DHCP**—The address of the server may be supplied to the device in the Vendor-specific Information option
- **DNS**—If the DHCP Vendor-specific Information option has not been provided, then the device will perform a DNS lookup for the server using a well-known hostname
- **Plug and Play Connect Service**—Finally, if no other method has been successful, the device will attempt to contact the Plug and Play Connect service. This service will then redirect the device to your server

Once the device has identified the server, it will contact the server and update firmware and configuration as specified by the server.

Setting up Discovery using DHCP

To discover the server address using DHCP, the device will send a DHCP discover message with option 60 that contains the string “ciscopnp”. The DHCP server must send a response containing the Vendor-specific Information option (option 43). The device extracts the server address from this option and uses this address to contact the server. An example of an option 43 string containing the address of a Network Plug and Play server is “5A1N;B2;K4;I172.19.45.222;J80”.

The option 43 string has the following components, delimited by semicolons:

- 5A1N—Specifies the DHCP sub-option for Plug and Play, active operation, version 1, no debug information. It is not necessary to change this part of the string.
- B2—IP address type:
  - B1 = hostname
  - B2 = IPv4
- Ixxx.xxx.xxx.xxx—IP address or hostname of the server (following a capital letter i). In this example, the IP address is 172.19.45.222.
- Jxxxx—Port number to use to connect to the server. In this example, the port number is 80. The default is port 80 for HTTP and port 443 for HTTPS.
- K4—Transport protocol to be used between the Cisco Plug and Play IOS Agent and the server:
  - K4 = HTTP (default)
  - K5 = HTTPS
- T*trustpoolBundleURL*—Optional parameter that specifies the external URL of the trustpool bundle if it is to be retrieved from a different location than the server. For example, to download the bundle from a TFTP server at 10.30.30.10, you would specify the parameter like this: Ttftp://10.30.30.10/ca.p7b
- If you are using trustpool security and you do not specify the T parameter, the device retrieves the trustpool bundle from the server.
- Zxxx.xxx.xxx.xxx;—IP address of the NTP server. This parameter is mandatory when using trustpool security to ensure that all devices are synchronized.

Consult the documentation for your DHCP server for details on how to configure DHCP options.

Setting up Discovery using DNS

If DHCP discovery fails to get the IP address of the server, the device falls back to a DNS lookup method. Based on the network domain name returned by the DHCP server, the device constructs a fully qualified domain name (FQDN) for the server, using the preset hostname “pnpserver”.

For example, if the DHCP server returns the domain name “example.com”, the device constructs the FQDN “pnpserver.example.com”. It then uses the local name server to resolve the IP address for this FQDN.

Certificate Requirements

When establishing a connection to a Network Plug and Play server, the client checks to ensure the certificate presented by the server is valid and can be trusted. For the certificate to be acceptable and the connection to proceed, the certificate must meet the following conditions:

- The certificate must be signed by a trusted Certificate Authority (CA), or the certificate itself must be trusted by the client. A certificate downloaded from the TrustpoolBundleURL learned from DHCP, or from the Plug and Play Connect service is trusted by the client
- If the server identity is discovered using manual configuration, DHCP or Plug and Play Connect, and is an IP address, then either the **Common Name** field or the **Subject-Alt-Name** field must contain that IP address
- If the server identity is discovered using manual configuration, DHCP or Plug and Play Connect, and is a hostname, then either the **Common Name** field or the **Subject-Alt-Name** field must contain that hostname
- If the server identity is discovered using DNS discovery, then either the **Common Name** field or the **Subject-Alt-Name** field must contain the IP address corresponding to the well-known hostname pnpserver.<*local domain*>

Note Some of the older Network Plug and Play client implementations do not verify the presence of the server identity in the certificate.

Setting up Discovery using Plug and Play Connect

Plug and Play Connect is a Cisco-provided service that is the last resort used by a Network Plug and Play-enabled device to discover the server. To use Plug and Play Connect for server discovery, you must first create a Controller Profile representing the Manager, and then register each of your devices with the Plug and Play Connect Service.

Accessing the Plug and Play Connect Service

To access the Plug and Play Connect Service, do the following:

1. In your web browser, navigate to *https://software.cisco.com*
2. Click the **Log In** button at the top right of the screen. Log in with a cisco.com ID associated with your Cisco Smart Account.
3. Select the **Plug and Play Connect** link under the **Network Plug and Play** heading. The main page for the **Plug and Play Connect** service is displayed.

Creating a Controller Profile

To create a Controller Profile for the Manager, do the following:

1. Open the Plug and Play Connect web page in your browser. If necessary, select the correct Virtual Account to use.

2. Select the Controller Profiles link, and then click the Add Profile button.
3. Select a Controller Type of PNP SERVER from the dropdown list. Then click Next.
4. Specify a name, and optionally a description for the profile.
5. Under the heading for Primary Controller, use the dropdown provided to select whether to specify the server by name or IP address. Fill in the name or addresses of the server in the fields provided.
6. Select the protocol to use when communicating with the server. It is strongly recommended that HTTPS be used to ensure the integrity of the provisioning process.
7. If the protocol selected is HTTPS, the certificate used by the server should be uploaded using the controls provided. See Managing Certificates, on page 72 for details on downloading the certificate from the Manager.
8. Optionally specify a Secondary Controller.
9. Click **Next**, and review the settings before clicking **Submit**.

Registering Devices

Certain products purchased directly from Cisco may be associated with your Cisco Smart Account at the time of order, and these will automatically be added to Plug and Play Connect. However, the majority of Cisco 100 to 500 series Plug and Play-enabled products will need to be registered manually. To register devices with Plug and Play Connect, do the following:

1. Open the Plug and Play Connect web page in your browser. If necessary, select the correct Virtual Account to use.
2. Select the **Devices** link, and then click **Add Devices**. You may need to be approved to manually add devices to your account. This is a one-time process, and, if it is required, you will be notified by email once approval has been granted.
3. Choose whether to add devices manually, or to add multiple devices by uploading details in CSV format. Click the link provided to download a sample CSV file. If you choose to upload a CSV file, click the **Browse** button to select the file. Then click **Next**.
4. If you selected to add devices manually, click **Identify Device**. Specify the Serial Number and Product ID for the device to be added. Select a Controller Profile from the dropdown. Optionally enter a description for this device.
5. Repeat step 4 until you have added all your devices, then click **Next**.
6. Review the devices you have added, and then click **Submit**.

Configuring the Network Plug and Play Service

There are several tasks that you may need to perform when setting up the Network Plug and Play service for your environment. These include uploading configurations and images, adding and configuring devices to use Network Plug and Play, and managing devices that connect to the service when they have not previously been registered with the service. The following sections describe these tasks in detail.

Using the Network Plug and Play Dashboard

The **Network Plug and Play** Dashboard provides an overview of the devices currently being provisioned using Network Plug and Play. Three charts are displayed, showing device status broken down by device group, by PnP enabled device, and by devices that are not already known by the Manager (unclaimed devices). Each chart shows the number of devices or groups in each of the states listed. You may click on the state heading on any of the charts to see a detailed list of devices or groups that fall into that category.

You may restrict the data displayed to a specific organization using the organization dropdown at the top right of the page. When viewing device groups, type all or part of a group name in the search box to limit the groups displayed in the table. Similarly, you may enter a device name, product ID or serial number in the search box when viewing provisioning rules to display the current status of an individual device.

Note The chart for unclaimed devices is only displayed to **Administrators** who are viewing data for **All Organizations**.

Managing PnP Enabled Devices

PnP Enabled Devices are devices in the inventory that have been configured to use Network Plug and Play or were previously discovered by FindIT Network Manager and have attempted to connect using Network Plug and Play. To create a new PnP Enabled Device, do the following:

1. Navigate to **Network Plug and Play** > **Enabled Devices**.
2. Click the **+**(plus) icon to add a new PnP enabled device to the inventory
3. Fill out the form with the requested parameters, including identifying details for the device, the organization, network and device group it should belong to, and select either or both of the desired firmware image and configuration file to be used. If you choose **Default** for the firmware image, the device will use the image designated as the default for that product ID at the time the device connects to the server.
4. Click **save**.

To edit an existing device, do the following:

1. Navigate to Network Plug and **Play** > **Enabled Devices**.
2. Select the radio button for the device to be modified and click **Edit**.
3. Change the image and/or configuration file as required and click **Save**.

Note If the PnP settings are changed for a device that has already been provisioned, that device's state will reset to pending, and the device will be re-provisioned the next time it checks in with the PnP server.

To remove a PnP Enabled Device, do the following:

1. Navigate to **Network Plug and Play** > **Enabled Devices**.
2. Select the radio button for the device to be deleted and click **delete**.

Note If a PnP Enabled Device is deleted when that device is otherwise known to FindIT and the device is online, only the PnP settings for that device will be removed. The device will remain in the inventory similar to any other managed device. If a device subsequently connects to the Manager using PnP, a new entry will be added to the PnP Enabled Devices table.

Unclaimed Devices

Note The **Unclaimed Devices** page is only available to Administrators.

An unclaimed device is one that has connected to the service, but there is no device record in the inventory that matches the device. To see a list of unclaimed devices, and to claim an unclaimed device so it can be managed using Network Plug and Play, do the following:

1. Navigate to **Network Plug and Play** > **Unclaimed Devices** and select the **Unclaimed** tab.
2. Click the claim button for the device to be managed.
3. Fill out the form with the organization, network and device group the device should belong to, and select either or both of the desired firmware image and configuration file to be used. If you choose **Default** for the firmware image, the device will use the image designated as the default for that product ID at the time the device connects to the server.
4. Click **Save**. A PnP Enabled Device entry will be created for the device and may be viewed on the **Enabled Devices** page.

To remove a device from the Unclaimed list without provisioning it, do the following:

1. Navigate to **Network Plug and Play** > **Unclaimed Devices** and select the **Unclaimed** tab.
2. Click **Ignore** for the device you wish to remove from the list.

The devices will be moved to the **Ignored** list and no further action will be taken. To reclaim an ignored device, do the following:

1. Navigate to **Network Plug and Play** > **Unclaimed Devices** and select the **Ignored** tab.
2. Click the **Unignore** button for the device to be reclaimed.

The devices will be moved to the **Unclaimed** list, and you may claim the devices as described above.

Auto Claiming Devices

Note The **Auto Claim** page is only available to Administrators

Unclaimed devices may be automatically claimed and provisioned by the server by creating an Auto Claim rule for that product ID. To create an Auto-Claim rule, do the following:

1. Navigate to **Network Plug and Play** > **Auto Claim Devices**.

2. Click the ✚(plus) icon to create a new **Auto Claim** rule.
3. Select the checkbox for the newly created rule and click **edit**.
4. Fill out the form with the requested parameters, including the product ID (PID) to automatically claim, the organization network and device group matching devices should belong to, and select either or both of the desired firmware image and configuration file to be used. If you choose **Default** for the firmware image, the device will use the image designated as the default for that product ID at the time the device connects to the server.
5. Click **save**.

New devices that are not present in the inventory will be compared against the list of Auto Claim rules. If there is a match, a new device record will be created in the inventory with the image and configuration file defined by the **Auto Claim** rule. The device will then be provisioned accordingly. If the device does not match an **Auto Claim** rule, it will be added to the Unclaimed list and no further action will be taken.

Device Firmware Images

The **Images** page allows you to upload firmware images that may then be deployed to the devices. Firmware images may be designated as the default image for different platforms, allowing you to update the firmware across an entire family of devices very easily. Firmware images are specific to an organization and may only be used for PnP Enabled Devices associated with the same organization.

To upload a firmware image, do the following:

1. Navigate to **Network Plug and Play** > **Images**.
2. Click the ✚(plus) icon.
3. Select the organization for the image from the dropdown.
4. Drag a firmware image from your PC and drop it on the target area of the **Upload File** window. Alternatively, click the target area and select a firmware image to upload.
5. Click **Upload**.

You may designate an image as the default image for one or more device types. To designate an image as a default image, do the following:

1. Navigate to **Network Plug and Play** > **Images**.
2. Select the radio button for the image in the **Images** table and click **edit**.
3. Enter a comma-separated list of product IDs into the **Default Image for Product IDs** field. Product IDs can contain the wildcard characters '?', representing a single character, and '*', representing a string of characters.
4. Click **Save**.

To remove an image, do the following:

1. Navigate to **Network Plug and Play** > **Images**.
2. Select the radio button for the image to be deleted and click **delete**.

Device Configuration Files

The Configurations page allows you to upload configuration files that may then be deployed to the devices. Configuration files are specific to an organization and may only be used for PnP Enabled Devices associated with the same organization. To upload a configuration file, do the following:

1. Navigate to **Network Plug and Play** > **Configurations**.
2. Click the ✚(plus) icon.
3. Select the organization for the configuration from the dropdown.
4. Drag a configuration file from your PC and drop it on the target area of the **Upload File** window. Alternatively, click the target area and select a configuration file to upload.
5. Click **Upload**.

   You can click on the filename of the uploaded configuration file to view the contents if you wish.

To remove a configuration, do the following:

1. Navigate to **Network Plug and Play** > **Configurations**.
2. Select the radio button for the configuration to be deleted and click **delete**.

Managing Settings

The Network Plug and Play Settings page allows you to control the operation of the Network Plug and Play Protocol. The **Check In Time Interval** controls how frequently a device will connect to the Network Plug and Play service after initial provisioning. To modify this parameter, do the following:

1. Navigate to **Network Plug and Play** > **Settings**.
2. Enter the desired interval between connections in the field provided. The time is in minutes, and the default is 2880 minutes, or two days.
3. Click **Save**.

The **Check In Time Interval** is set for the system as a whole, but can be overridden at the organization level. If no interval is set for the organization, then the system value is used.

Configuring the Certificate

The certificate automatically generated by FindIT Network Manager during first startup is a self-signed certificate. In most cases, this will not be sufficient for the certificate to be accepted by the Network Plug and Play client, and it will be necessary to generate a new certificate. When generating a new self-signed certificate or certificate signing request (CSR), the Manager will include the contents of the **Common Name** field in the **Subject Alternative Name** field in addition to any values specified in the **Subject Alternative Name** field on the GUI.

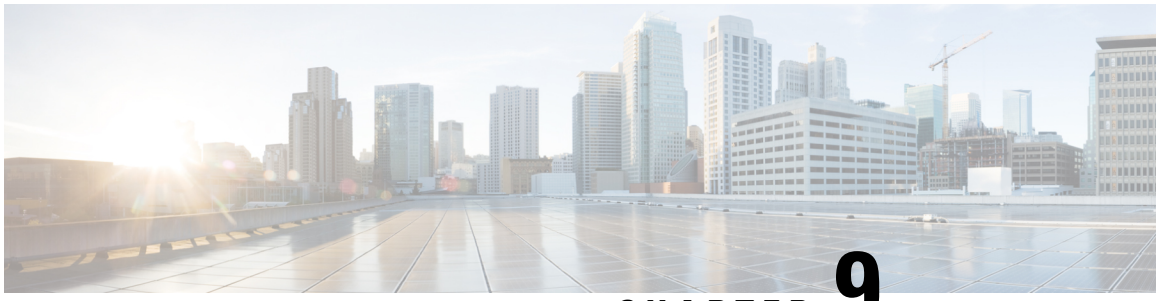
For more information on configuring the Manager's certificate, see Managing Certificates, on page 72.

Monitoring Network Plug and Play

Each device known to the Network Plug and Play service is shown on either the **Enabled Devices** page or the **Unclaimed Devices** page with a status displayed. This status may also be viewed on the **Inventory** page by enabling the display of the **PnP Status** column. The status field shows the current state of the device, and will contain one of the values as listed in the following table. By clicking on the status field, you can see more detail, including a history of the state changes for this device over time.

Table 15: Network Plug and Play - Device Status

Status	Description
PENDING	Device is defined but has not made contact with the service.
PROVISIONING	The device has made the initial connection to the service.
PROVISIONING_IMAGE	A firmware image is being applied by the device.
PROVISIONED_IMAGE_REBOOTING	The device is rebooting to run the new firmware.
PROVISIONED_IMAGE	New firmware has been applied successfully.
PROVISIONING_CONFIG	A configuration file is being applied to the device.
PROVISIONED_CONFIG	The configuration file has been successfully applied to the device. Depending on the type of device, it may reboot to apply the configuration.
ERROR	An error has occurred. Check log files for more details.
PROVISIONED	The provisioning process for the device is complete.



CHAPTER 9

Event Log

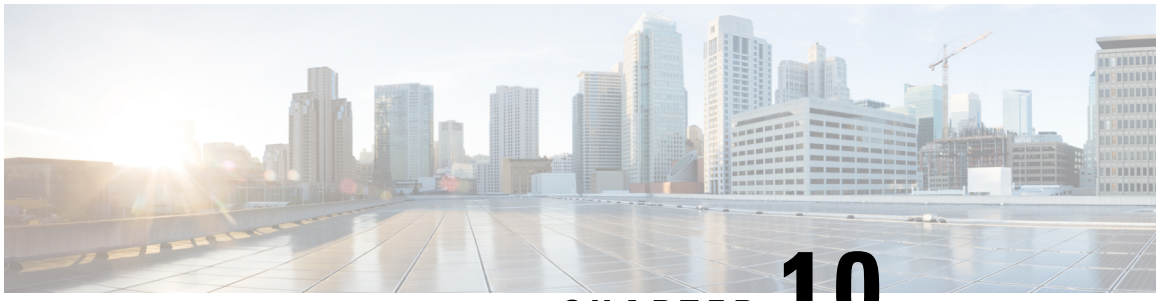
This chapter contains the following sections:

About the Event Log

The Event Log provides an interface for searching and sorting through the events generated across the network. You may use the filter controls provided to limit the events displayed based on any combination of the following parameters:

- **Time**—Specify the start and end times for the period of interest. Only events occurring in this period will be displayed.
- **Severity**—Select the severity level of events to display. You may also check the *Higher* checkbox to include events with a higher severity level.
- **Type**—Select one or more event types to display. The types are arranged in a tree structure, and selecting a type will automatically include all event types underneath the selected type in the tree.
- **Network**—Select one or more networks to display events for. As you type, matching sites will be displayed.
- **Device** —Select one or more devices to display events for. As you type, matching devices will be displayed. You may specify devices by name, IP address, or MAC address.

Events that match the filter conditions will be displayed in the table below. The table may be sorted by clicking on the column headings.



CHAPTER 10

Reports

This chapter contains the following sections:

About Reports

The **Reports** option in the Cisco FindIT Network Manager provides a series of reports about your network. The reports provided include:

- **Lifecycle Report**—Provides a summary of the lifecycle status of the devices in the network.
- **End of Life Report**—Shows any devices that have an End of Life bulletin published.
- **Maintenance Report**—Lists all devices and their warranty state and whether the device has an active support contract.
- **Wireless Network**— Shows information about the wireless environment, including SSIDs, access points, and spectrum usage.
- **Wireless Client**—Displays details about wireless clients seen on the network.

Viewing the Lifecycle Report

The **Lifecycle Report** provides a high level view of the status of the network devices, taking into account both software and hardware lifecycle status. The following table describes the information provided:

Table 16: Lifecycle Report

Field	Description
Network Name	The name of the network in which the device is located.

Field	Description
Organization	The organization the device belongs to.
Hostname	The hostname of the device.
Device Type	The type of device.
Model	The model number of the device.
Week of Manufacture	The date of manufacture for the device, displayed as week number and year.
Firmware Update Available	Displays the latest firmware version available for the device, or states that the device firmware is currently up to date.
Firmware Version	Displays the current firmware version running on the device.
End of Life Status	Specifies if an End of Life bulletin has been published for the device and the date of the next key milestone in the End of Life process.
Maintenance Status	Specifies if the device is currently under warranty or covered by a support contract.

The row in the table for a device that may require attention is color-coded to indicate the urgency. For example, a device with a published End of Life bulletin will be colored orange if the End of Support milestone has not been reached, and red if the device is no longer supported by Cisco.

The Search box located at the top of the report can be used to filter the results. Enter text in the Search box to limit the number of entries that are displayed with the matching text. Results may be limited to a specific organization using the Organization dropdown.

The column selection icon at the top left of the report can be used to customize the information displayed. Click on the icon and then use the checkboxes that appear to select the columns you wish to include in the report.

Viewing the End of Life Report

The **End of Life Report** lists any devices that have an **End of Life** bulletin published, along with key dates in the End of Life process, and the recommended replacement platform. The following table describes the information provided:

Table 17: End of Life Report

Field	Description
Network Name	The name of the network in which the device is located.
Organization	The organization the device belongs to.

Field	Description
Product ID	The product ID or part number of the device.
Hostname	The hostname of the device.
Device Type	The type of device.
Current Status	The stage at which the End of Life process of the product is at.
Date of Announcement	The date the End of Life bulletin was published.
Last Date of Sale	The date after which the product will no longer be sold by Cisco.
Last Date of Software Releases	The date after which no more software versions will be released for the product.
Last Date for New Service Contract	The last date for taking out a new support contract on the device.
Last Date for Service Renewal	The last date for renewing an existing support contract on the device.
Last Date of Support	The date after which Cisco will no longer provide support for the product.
Recommended Replacement	The recommended replacement product.
Product Bulletin	The product bulletin number and a link to the bulletin on the Cisco website.

Each row of the table is color-coded to indicate the stage of the End of Life process the device is at. For example, a device that has past the Last Date of Sale but not yet reached the Last Date of Support will be colored orange, and a device that is past the Last Date of Support is colored red.

The Search box located at the top of the report can be used to filter the results. Enter text in the Search box to limit the number of entries that are displayed with the matching text. Results may be limited to a specific organization using the Organization dropdown.

The column selection icon at the top left of the report can be used to customize the information displayed. Click on the icon and then use the checkboxes that appear to select the columns you wish to include in the report.

Viewing the Maintenance Report

The **Maintenance Report** lists all network devices which includes the warranty and support contract status information for each of them. The following table describes the information provided:

Table 18: Maintenance Report

Field	Description
Network Name	The name of the network in which the device is located.
Organization	The organization the device belongs to.
Hostname	The hostname of the device.
Device Type	The type of device.
Model	Model number of the device.
Serial Number	The serial number for the device.
Status	The current support status of the device.
Coverage End Date	The date at which the current support contract will expire.
Warranty End Date	The date at which the warranty for the device will expire.

Each row of the table is color-coded to indicate the support status for the device. For example, a device that is approaching the expiry date of the warranty or support contract will be colored orange, while a device that is out of warranty and does not have a current support contract will be colored red.

The Search box located at the top of the report can be used to filter the results. Enter text in the Search box to limit the number of entries that are displayed with the matching text. Results may be limited to a specific organization using the Organization dropdown.

The column selection icon at the top left of the report can be used to customize the information displayed. Click on the icon and then use the checkboxes that appear to select the columns you wish to include in the report.

Viewing the Wireless Network Report

The **Wireless Network Report** shows details about the wireless network broken down by SSID, wireless spectrum usage, and access point, and includes a list of rogue access points that have been detected. Reports may be generated for time ranges from daily to yearly using the controls at the top of the page.

Several of the data sets include a graph that shows a breakdown over time for the selected row. You may click on the labels in the legend on the graph to toggle the display of each set of data.

The following table describes the information provided in the different sections of the report:

Table 19: Wireless Network Report

Field	Description
Wireless Networks Table	

Field	Description
SSID	The wireless network name.
Network (hidden by default)	The network where the SSID is located.
Organization (hidden by default)	The organization the SSID belongs to.
Guest	Whether the SSID is configured for guest access.
Security	The security method configured for the SSID.
Client Count (Peak)	The maximum number of clients associated with the SSID during the period covered by the report.
Client Count (Average)	The average number of clients associated with the SSID during the period covered by the report.
Traffic (Peak)	The maximum aggregate traffic rate through the SSID during the period covered by the report.
Traffic (Average)	The average aggregate traffic rate through the SSID during the period covered by the report.
Spectrum Usage Table	
Radio Freq	The radio frequency band in use – either 2.4GHz or 5GHz.
Network	The network the spectrum usage data displayed applies to.
Organization	The organization the spectrum usage data applies to.
Client Count (Peak)	The maximum number of clients using the frequency band during the period covered by the report.
Client Count (Average)	The average number of clients using the frequency band during the period covered by the report.
Traffic (Peak)	The maximum aggregate traffic rate through the frequency band during the period covered by the report.
Traffic (Average)	The average aggregate traffic rate through the frequency band during the period covered by the report.
Wireless Access Point Table	
Access Point	The name of the access point.
Network (hidden by default)	The network where the access point is located.
Organization (hidden by default)	The organization the access point belongs to.
Model	The model of the access point.
Version	The firmware version running on the access point.

Field	Description
Client Count (Peak)	The maximum number of clients associated with the access point during the period covered by the report.
Client Count (Average)	The average number of clients associated with the access point during the period covered by the report.
Traffic (Peak)	The maximum aggregate traffic rate through the access point during the period covered by the report.
Traffic (Average)	The average aggregate traffic rate through the access point during the period covered by the report.
Rogue Access Points Table	
SSID	The SSID detected.
Network (hidden by default)	The network where the detecting access point is located.
Organization (hidden by default)	The organization the detecting access point belongs to.
MAC	The MAC address of the rogue access point.
First Seen	The time at which the rogue access point was first detected.
Last Seen	The time at which the rogue access point was last seen.
Total Time Visible	The total time that the rogue access point was online.
Channel	The wireless channel used by the rogue access point.
Average Signal Strength	The average signal strength of the rogue access point as seen by the detecting access point.
Seen By	The access point(s) that detected the rogue access point.

Viewing the Wireless Client Report

The **Wireless Client Report** shows details about the wireless clients on the network. Reports may be generated for time ranges from daily to yearly using the controls at the top of the page.

Each data sets includes graphs that shows a breakdown over time for the selected row. You may click on the labels in the legend on the graph to toggle the display of each set of data.

The following table describes the information provided:

Table 20: Wireless Client Table

Wireless Clients Table	
MAC	The MAC address of the client
Hostname	The hostname of the client, where available.

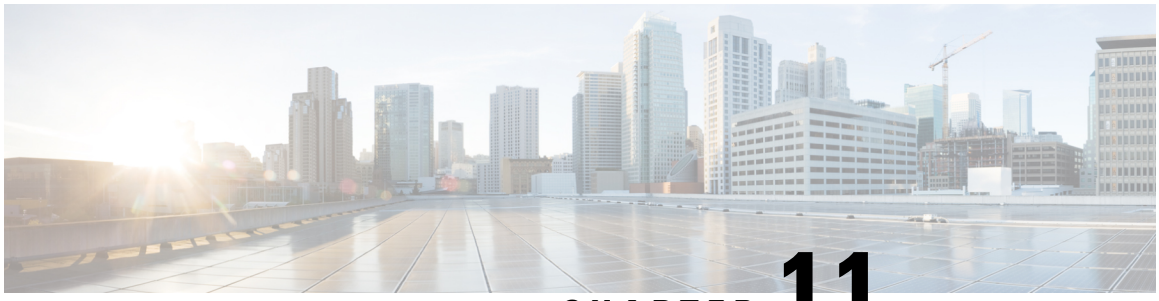
Wireless Clients Table	
Organization	The organization in which the client was last seen.
Network	The network where the client was last seen.
SSID	The SSID the client was last associated with.
802.11 Type	The 802.11 variant used by the client.
Frequency	The frequency band used by the client.
Max Data Rate	The maximum data rate used by the client.
Upload	The volume of data uploaded by the client.
Download	The volume of data downloaded by the client.
Total	The total volume of data sent and received by the client.
First Seen	The time at which the client was first detected.
Last Seen	The time at which the client was last seen.
Time Online	The total time that the client was online.
% Online Time	The percentage of time the client was online in the total time the client was known to the network.

Table 21: Wireless Guests Table

Wireless Guests Table	
MAC	The MAC address of the client.
Hostname	The hostname of the client, where available.
Username	The username entered by the client in the guest portal.
Organization	The organization in which the client was last seen.
Network	The network where the client was last seen.
SSID	The SSID the client was last associated with.
802.11 Type	The 802.11 variant used by the client.
Frequency	The frequency band used by the client.
Max Data Rate	The maximum data rate used by the client.
Upload	The volume of data uploaded by the client.
Download	The volume of data downloaded by the client.
Total	The total volume of data sent and received by the client.

Wireless Guests Table	
First Seen	The time at which the client was first detected.
Last Seen	The time at which the client was last seen.
Time Online	The total time that the client was online.
% Online Time	The percentage of time the client was online in the total time the client was known to the network.

Note **First Seen** and **Last Seen** timestamps are the time reported by the access point. It is recommended that all network devices implement clock synchronization using a mechanism such as the Network Time Protocol (NTP).



CHAPTER 11

Administration

This chapter contains the following sections:

About Administration

The **Administration** option in FindIT Network Manager allows you to control the operation of the application at the organizational level. This option is divided into the following pages:

- **Organizations**—Create and maintain organizations in FindIT Network Manager.
- **Device Groups**—Allocate network devices into groups for easy management.
- **Device Credentials**—Enter credentials to be used when accessing network devices.
- **Users**— Define user access to FindIT Network Manager.
- **Notification Defaults**—Change the default notification behavior for FindIT Network Manager.
- **Login Attempts**—Provides a log of all user access to FindIT Network Manager.
- **Report Settings**—Change settings controlling how reports are generated.

Not all pages are visible to all roles. Operators cannot manage user settings. **Notification Defaults** and **Report Settings** are only visible to Administrators.

Managing Organizations

Organizations are used in FindIT Network Manager to split networks, users, and devices into groups that are typically administered separately. Each network or device belongs to an organization, and each user can

manage one or more organizations. An organization might represent a customer or a department or a region – whatever is most suitable for your company – but in all cases, the use of organizations allows more granular control over who can view and manage the different parts of the network. A single organization is created by default when the Manager is installed.

Creating a New Organization

To create a new organization, do the following:

1. Navigate to **Administration** > **Organizations**.
2. Click the ✚(plus) icon at the top of the table.
3. Specify a name for the organization and enter the required details.
4. Enter a name for a new device group that should be used as the default group for newly discovered devices. The new device group will be created along with the organization.
5. Click **Save**.
6. Repeat the steps above for each organization you wish to create.

Modifying an Existing Organization

To modify an existing organization, do the following:

1. Navigate to **Administration** > **Organizations**.
2. Select the radio button for the organization to be modified and click the **Edit** icon
3. Make changes as required and click **Save**.

Deleting an Organization

To delete an organization, do the following:

1. Navigate to **Administration** > **Organizations**.
2. Select the radio button for the organization to be modified and click the **Delete** icon.

Managing Notification Settings for an Organization

Notification Settings allow you to control how the different types notifications are delivered. The settings applied at the organization level will be applied across all networks in the organization.

To change the Notification Settings for an organization, do the following:

1. Navigate to **Administration** > **Organizations**.
2. Click the name of the organization to be modified and select the **Notification Settings** tab.
3. Set the checkboxes for the different types of notification to reflect how you want them to be handled. Options are for notifications to be delivered as any combination of pop-ups in the GUI or as emails to the specified email address.

   You may also choose to follow the behavior defined at system level by checking the Inherit from **Notification Defaults** checkbox.

4. Click **Save**.

Note See Notifications for more information about the types of notifications available and how to manage them. See Changing Notification Defaults for details on changing notification settings at the system level.

Managing Users Associated with an Organization

Users with a role of **Organization Administrator** or lower must be explicitly associated with an organization to be able to view or manage devices in that organization.

To associate a user with the organization, do the following:

1. Navigate to **Administration** > **Organizations**.
2. Click the name of the organization to be modified and select the **Users** tab.
3. Click the ✚(plus) icon. Select the user from the dropdown list.

Note **Administrator** level users are implicitly associated with all organizations and will not appear in the dropdown list.

To remove a user from the organization, do the following:

1. Navigate to **Administration** > **Organizations**.
2. Click the name of the organization to be modified and select the **Users** tab.
3. Click the **Delete** icon next to the user in the table.

Managing Networks Associated with an Organization

Every network in FindIT Network Manager belongs to a single organization. You can view a list of networks associated with an organization by selecting the **Networks** tab on the **Organization Detail** page.

Associating a network with an organization is done when the network is first created. To change the organization a network is associated with, do the following:

1. Navigate to **Network** and select the network that you wish to change. Click **More** to display the **Network Detail** panel.
2. Click the **Edit** icon next to the network name.
3. Select the new organization from the dropdown list.
4. Click **OK**.

You may create new networks for an organization from this view. Click the ✚(plus) icon to create a new network and fill in appropriate values in the form that is displayed.

Managing Device Groups

FindIT Network Manager uses device groups for performing most configuration tasks. Multiple network devices are grouped together so that they may be configured in a single action.

Each device group can contain devices of multiple types, and when configuration is applied to a device group, that configuration is only applied to devices in the group that support that feature. For example, if a device group contains wireless access points, switches and routers, then configuration for a new wireless SSID will be applied to the wireless access points, will not be applied to the switches, and will be applied to the routers only if they are wireless routers.

Device groups may include devices from multiple networks, but all devices must belong to a single organization. A device group may be designated as the default group for an organization or network, and any newly discovered devices for that network or organization will be placed in the default device group.

Creating a New Device Group

To create a new Device Group, do the following:

1. Navigate to **Administration** > **Device Groups**.
2. Click on the ✚(plus) sign to create a new group.
3. Enter an organization, a name and a description for the group. Click **Save**.
4. Optionally, add devices to the device group by clicking the ✚(plus) icon and using the search box to select devices to be added to the group. You may add devices individually or by network. If the selected device is already a member of a different group, it will be removed from that group. Each device may only be a member of a single group.

Modifying the Device Group

To change an existing Device Group, do the following:

1. Navigate to **Administration** > **Device Groups**.
2. Select the radio button next to the group to be changed and click the **edit** icon.
3. Change the name and description if necessary. Click **Save**.
4. Add and remove devices from the group as required. To remove a device that was previously added to the group, click the **trashcan** icon next to the device. The device will be moved to the **Default** group for the network or organization.

Note You cannot delete a device from the **Default** group. To remove a device from the **Default** group you must add it to a new group.

Deleting a Device Group

To delete a Device Group, do the following:

1. Navigate to **Administration** > **Device Groups**.

2. Click the radio button for the device group to be removed, and then click the **delete** icon.

Note You cannot delete a **Default** group.

Managing Device Credentials

For FindIT Network Manager to fully discover and manage the network, it needs credentials to authenticate with the network devices. When a device is first discovered, the Probe will attempt to authenticate with the device using the default username: `cisco`, password: `cisco`, and SNMP community: `public`. If this attempt fails, a notification will be generated and valid credentials must be supplied by the user. To supply valid credentials, do the following:

1. Navigate to **Administration** > **Device Credentials**. The first table on this page lists all the devices that have been discovered that require credentials.
2. Enter valid credentials into any or all of the **Username/Password** fields, **SNMP Community** field, and **SNMPv3** credential fields. You may click the ✚(plus) icon next to the corresponding field to enter up to three of each type of credential. Ensure that passwords are entered using plaintext.

Note For **SNMPv3** credentials, the supported authentication protocols are None, MD5, and SHA, and the supported encryption protocols are None, DES, and AES

3. Click **Apply**. The Probes will test each credential against each device that requires that type of credential. If the credential is valid, it will be stored for later use with that device.
4. Repeat steps 2 to 3 as necessary until every device has valid credentials stored.

To enter a single credential for a specific device, do the following:

1. Click the **Edit** icon shown against the device in the discovered devices table. A popup will appear prompting you to enter a credential that corresponds to the Credential Type selected.
2. Enter a username and password or an SNMP credential in the fields provided.
3. Click **Apply**. To close the window without applying, click the ✖ on the top right corner of the popup.

Underneath the **Add New Credential** section is a table showing the identity for each device for which the Probe has a valid credential stored and the time that credential was last used. To display the stored credential for a device, you may click the **Show Password** icon next to the device. To hide the credentials again, click the **Hide Password** icon. You may also show and hide credentials for all devices using the button at the top of the table. You may also delete credentials that are no longer required. To delete stored credentials, do the following:

1. Navigate to **Administration** > **Device Credentials**.
2. In the **Saved Credentials** table, select the check box against one or more sets of credentials to be deleted. You may also select the checkbox at the top of the table to select all credentials.
3. Click **Delete Selected Credentials**.

To delete a credential for a single device, you may also click the **Delete** icon next to the device.

Managing Users

The **User Management** page allows you to define users that can access FindIT Network Manager, and also allows you to change settings that affect how those users interact with the Manager.

FindIT Network supports four types of users:

- **Administrator**—An Administrator has full access to the FindIT Network features including the ability to maintain the system
- **Organization Administrator**—An Organization Administrator is limited to managing one or more organizations, but cannot make changes to the system
- **Operator**—An Operator has similar power to an Organization Administrator, but cannot manage users
- **Readonly**—A Readonly user can only view network information, they cannot make any changes

When the FindIT Network Manager is first installed, a default **Administrator** is created with the username and password both set to `cisco`.

Note User settings can be managed by **Administrators** and **Organization Administrators** only.

Adding a New User

To add a new user, do the following:

1. Navigate to **Administration** > **Users** and select the **Users** tab.
2. Click the ✚ (plus) icon to create a new user.
3. In the fields provided, enter a username, display name, email address and password, and specify the user type. You may also provide contact details for the user.
4. Click **Save**.

If the user is not an **Administrator**, then you must add the user to one or more organizations. To do so, select the **Organizations** tab and click the ✚(plus) icon. Select the desired organization from the dropdown list.

Modifying a User

To modify an existing user, do the following:

1. Navigate to **Administration** > **Users** and select the **Users** tab.
2. Select the radio button next to the user that needs to be changed and click the **Edit** icon.
3. Make the modifications as required.
4. Click **Save**.

To add the user to a new organization, select the **Organizations** tab and click the ✚(plus) icon. Select the desired organization from the dropdown list. To remove them from an organization, click the **Delete** icon next to the organization in the table.

Deleting a User

To delete an existing user, do the following:

1. Navigate to **Administration** > **Users** and select the **Users** tab.
2. Select the radio button next to the user that needs to be deleted and click **delete** at the top of the table.

Changing password complexity

To enable or change password complexity requirements, do the following:

1. Navigate to **Administration** > **Users** and select the **User Settings** tab.
2. Modify the **User Password Complexity** settings as required and click **Save**.

Changing session timeouts

To change idle and absolute timeouts for user sessions, do the following:

1. Navigate to **Administration** > **Users** and select the **User Settings** tab .
2. Modify the **User Session** parameters as required and click **Save**. Hover over the help icons to see allowable ranges for these parameters.

Changing Notification Defaults

Notification Settings allow you to control the different types of notifications that are delivered. Settings may be applied at the organization level or at the system level. Organizations that choose to inherit system level notification settings will have the behavior controlled by the **Notification Defaults** page.

To change the **Notification Settings** for the system, do the following:

1. Navigate to **Administration** > **Notification Defaults**.
2. Set the checkboxes for different types of notification to reflect how you want them to be handled. Options are for notifications to be delivered as any combination of pop-ups in the GUI or as emails to the specified email address.
3. Click **Save**.

If you use email notifications, you must ensure that the email settings are correctly configured. See Managing Email Settings for more details. See About Notifications more information about the types of notifications available and how to manage them. See Managing Organizations for details on changing notification settings at the organization level.

Viewing Login Attempts

FindIT Network Manager keeps a log of every attempt made to log in and out of the system, both successful and unsuccessful. To view the log, navigate to **Administration** > **Login Attempts**. The table displays the following information:

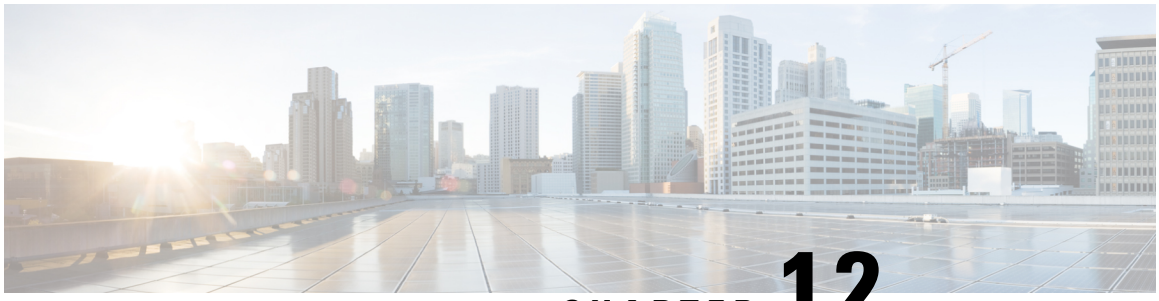
Table 22: Login Attempts Table

Field	Description
Username	The username associated with the event.
Display Name	The display name for the user.
IP	The IP address of the device from which the user logged in.
Type	The type of event. Valid values include, LOGIN and LOGOUT.
Status	Indicates if the attempt succeeded or failed.
Timestamp	The date and time the event took place.

You may use the search box above the table to show only entries that match a particular user or IP address.

Managing Report Settings

The **Report Settings** page allows you to set the timezone that reports will be generated for. The start and end times for the report period will be in the local time of the selected timezone.



CHAPTER 12

System

This chapter contains the following sections:

About System

The System option in FindIT Network Manager allows you to manage the operation of the platform.

This option is divided into the following pages:

- **License**—Manage software licensing for the Manager
- **Certificate**—Manage security certificates on the Manager
- **Email Settings**—Set up email
- **API Usage**—Monitor the use of the FindIT Network Manager API
- **Backup**— Backup the configuration and other data for the Manager
- **Restore**—Restore the configuration and other data for the Manager
- **Platform Settings**—Manage network configuration for the Manager
- **Privacy Settings**—Control the data that can be shared with Cisco
- **Log Settings**—Change log settings for the Manager
- **Local Probe**—Manage a Probe hosted on the Manager

These pages are only available to **Administrators**.

Managing Licenses

Note This page is not present on the metered version of FindIT Network Manager for AWS.

The **License** page allows you to see the number and type of licenses required for your network, and allows you to connect the **Manager** to the Cisco Smart Licensing system. On this page are two information panels:

- **Smart Software Licensing Status**— This panel shows the registration state of the Smart License client and information about the Smart Account in use.
- **Smart License Usage**— This panel lists the quantities and types of license required based on the current state of the network. This information will automatically update as the network changes, and the Manager will update the number of licenses requested from the Smart Account. The Status field shows whether the required number of licenses have been successfully obtained.

This page also contains controls allowing you to register and deregister the Manager from your Smart account.

If the Manager is running in Evaluation Mode, or is not able to obtain sufficient licenses to manage the network, a message will be displayed in the header of the Manager's user interface. If more than ten devices are in use in Evaluation Mode, or the Manager cannot obtain sufficient licenses to operate, then you have 90 days to correct the situation. If the problem is not addressed within 90 days, some functionality of the Manager will be restricted until the problem is addressed, either by obtaining more licenses, or reducing the number of devices being managed.

Registering the Manager to your Smart Account

To register the Manager with your Smart Account, do the following:

1. Log on to your Smart Account at *https://software.cisco.com*. Select the **Smart Software Licensing** link located under the License section.
2. Select the **Inventory** page, and if necessary, change the selected virtual account from the default. Then click on the **General** tab.
3. Create a new **Product Instance Registration Token** by clicking on the **New Token…** button. Optionally add a description and change the **Expire After** time. Then click **Create Token**.
4. Copy the newly created token to the clipboard by selecting **Copy** from the **Actions** drop-down located at the right of the token.
5. Navigate to the FindIT Network Manager user interface and select **System** > **License**.
6. Click the **Register** button and paste the token into the field provided. Click **OK**.

The Manager will register with Cisco Smart Licensing and request sufficient licenses for the number of network devices being managed. If there are insufficient licenses available, a message will be displayed on the user interface, and you will have 90 days to obtain sufficient licenses before system functionality is restricted.

Removing the Manager from your Smart Account

To remove the Manager from your Smart Account and return any licenses allocated back to the pool, do the following:

1. Navigate to the FindIT Network Manager user interface and select **System** > **License**.
2. Select **Deregister…** from the dropdown list located at the top right. Click **Deregister** in the popup to confirm.

Immediately Check for Licenses

FindIT Network Manager checks daily to ensure there are still sufficient licenses available for the network, and will update immediately if the number of licenses required decreases. However, if the number of licenses required increases, or if licenses are added or removed from the pool, it may take up to a day before the Manager will be updated. To force the Manager to update its license allocation immediately, do the following:

1. Navigate to the FindIT Network Manager user interface and select **System** > **License**.
2. Select **ReCheck License Now…** from the dropdown list located at the top right. The Manager will query Cisco Smart Licensing immediately to ensure that there are sufficient licenses available for the FindIT Network Manager to operate.

Renew Authorization Now

The Renew Registration Now action cause the Manager to refresh the certificates used to authenticate communication with Cisco Smart Licensing. Typically, this will only be required at the request of Cisco Support when rectifying an extended communications outage. To renew the registration, do the following:

1. Navigate to the FindIT Network Manager user interface and select **System** > **License**.
2. Select **Renew Authorization Now…** from the dropdown list located at the top right.

Renew Registration Now

The Renew Registration Now action causes the Manager to refresh the certificates used to authenticate communication with Cisco Smart Licensing. Typically, this will only be required at the request of Cisco Support when rectifying an extended communications outage. To renew the registration, do the following:

1. Navigate to the FindIT Network Manager user interface and select **System** > **License**.
2. Select **Renew Registration Now…** from the dropdown list located at the top right.

Transfer the Manager to a Different Account

Re-registering a Manager allows it to be moved from one Virtual Account to another. To move a Manager between accounts, do the following:

1. Navigate to the FindIT Network Manager user interface and select **System** > **License**.
2. Select **Reregister...** from the dropdown list located at the top right.
3. Enter the new registration token in the box provided. If the Manager is currently registered to another account, ensure the **Reregister this product instance if it is already registered** checkbox is selected, then click **OK**.

Managing Certificates

At the time of installation, FindIT Network Manager will generate a self-signed certificate to secure web and other communication with the server. You may choose to replace this certificate with one signed by a trusted certificate authority (CA). To do this, you will need to generate a certificate signing request (CSR) for signing by the CA.

You may also choose to generate a certificate and the corresponding private key completely independent of the Manager. If so, you can combine the certificate and private key into a PKCS#12 format file prior to upload.

Generating a Certificate Signing Request (CSR)

To generate a CSR, do the following:

1. Navigate to **System** > **Certificate** and select the **CSR** tab.
2. Enter appropriate values into the fields provided in the form that is displayed. These values will be used to construct the CSR, and will be contained in the signed certificate you receive from the CA.
3. Click **Create** and the CSR will be automatically downloaded to your PC. Alternatively, you can download the CSR at a later date by clicking **Download** next to the CSR label.
4. If necessary, you can modify the CSR by returning to step 2.

Uploading a New Certificate

To upload a new certificate, do the following:

1. Navigate to **System** > **Certificate** and select the **Update Certificate** tab.
2. Select **Upload Cert** radio button. The file containing the certificate can be dropped on the target area, or you may click the target area to browse the file system. The file should be in PEM format.

   You may also upload a certificate with the associated private key in PKCS#12 format by selecting the **Upload PKCS12** option instead. The password to unlock the file should be specified in the field provided.
3. Click **Upload** to upload the file and replace the current certificate.

Note Some browsers may generate certificate warnings for certificates that have been signed by a well-known certificate authority, while other browsers accept the certificate without any warning. Network Plug and Play clients may also fail to accept the certificate. This is because the certificate authority has signed the certificate with an intermediate certificate that is not included in the browser or PnP client's trusted authorities store. In these circumstances, the certificate authority provides a bundle of certificates that must be concatenated with the server certificate before uploading to the Manager. The server certificate must appear first in the concatenated bundle.

Regenerating the Self-Signed Certificate

To regenerate the self-signed certificate, do the following:

1. Navigate to **System** > **Certificate** and select the **Update Certificate** tab.

2. Click **Renew Self-Signed Cert**. Enter appropriate values into the fields provided in the form that is displayed. These values will be used to construct the certificate.
3. Click **Save**.

Viewing the Current Certificate

To view the current certificate, do the following:

1. Navigate to **System** > **Certificate** and select the **Current Certificate** tab.
2. The certificate is displayed in plain text format in your browser.

Downloading the Current Certificate

To download a copy of the current certificate, do the following:

1. Navigate to **System** > **Certificate** and select the **Current Certificate** tab.
2. Click **Download** at the bottom of the page. The certificate will be downloaded in PEM format by your browser.

Managing Email Settings

The **Email Settings** page allows you to control how emails will be sent by FindIT Network Manager. This page allows you to set the following parameters:

Table 23: Email Setting

Field	Description
SMTP Server	The domain name or IP address of the SMTP server that will be used.
SMTP Port	The TCP port to use for sending mail.
Email Encryption	The encryption method to use. Options include the following: • None • TLS • SSL
Authentication	Enable or disable email authentication.
Username	The username to present if authentication is enabled.
Password	The password to present if authentication is enabled.
From Email Address	The email address to originate messages from.

To test the configuration, click **Test Connectivity**. This will prompt for a target email address and generate a test email to the specified address.

Viewing API Usage

The API Usage page displays information about any external applications that have been integrated with the FindIT Network Manager. This report is divided into the following three sections:

- The **15-minute Request Monitor**—Displays the average and peak request rate over the last 15 minutes
- The **Request History** graph—Displays a graph of request activity over time. You may select time periods of the last four hours, the last seven days, or all available information. You may then use the sliders underneath the graph to narrow the focus of the graph to a particular period of interest.
- The **API Client Information** table—Lists all the clients that have used the API at least once. The following table describes the information provided in the **API Client Information** table:

Table 24: The API Client Information Table

Field	Description
API Version	The version used by the client when accessing the API.
Client ID	The identifier for a particular instance of the client application.
Client IP	The IP address associated with this client. Also displays the callback URL to which the Manager should post event notifications when the API version is v1 and notifications have been requested.
Client Module	The type of application associated with this client.
Client Version	The version of the application associated with this client.
Username	For clients using the v1 API, this field shows the username presented by the application when authenticating to the Manager. For clients using the v2 API, this field shows the **Access Key ID** used by the client and the username that key is associated with.
Time Since Last Access	The time since the last activity from this client.
# Subscribed Networks	The number of networks where the application has requested event notifications. This number is a link that, when clicked, displays the Subscribed Networks table for this client. The Subscribed Networks table is described below.
# Subscribed Licensed Devices	The number of managed devices for which event notifications will be sent to this client.

To view information about the networks for which a client has requested notifications, click on the **# Subscribed Networks** link for the client in the **API Client Information** table. The**Subscribed Networks** table will be displayed for the client containing a list of the networks the client has requested notification for. The following table describes the information provided in the **Subscribed Networks** table:

Table 25: The Subscribed Networks Table

Field	Description
Network	The name of the network being monitored by the client.
# Subscribed Licensed Devices	The number of managed devices in this network for which event notifications will be sent

Backing Up and Restoring the Manager Configuration

The configuration and other data used by FindIT Network Manager can be backed up for disaster recovery purposes, or to allow the Manager to be easily migrated to a new host. Backups are encrypted with a password in order to protect sensitive data.

To perform a backup, do the following:

1. Navigate to **System** > **Backup**.
2. Enter a password to encrypt the backup in the **Password** and **Confirm Password** fields.
3. Click **Backup & Download**. A popup window will appear showing the progress of the backup. Larger systems may require some time to complete the backup, so you may dismiss the progress meter and display it again later with the **View Status** button.

When complete, the backup file will be downloaded to your PC.

To restore a configuration backup to the Manager, do the following:

1. Navigate to **System** > **Restore**.
2. Enter the password that was used to encrypt the backup in the **Password** field.
3. Click **Upload & Restore** to proceed. A popup will appear allowing you to upload a backup file from your PC. You can drag and drop the backup file onto the target area provided, or click the target area to specify a file in your PC's file system. Click **Restore** to proceed.

Managing Platform Settings

The **Platform Settings** page is only available when using the Cisco-provided virtual machine images. This page allows you to modify key system settings without needing to directly access the operating system.

Changing the Hostname

Note This does not apply to FindIT Network Manager for AWS.

The hostname is the name used by the operating system to identify the system, and is used by FindIT Network Manager to identify the Manager when generating Bonjour advertisements. To change the hostname for the Manager, do the following:

1. Navigate to **System** > **Platform Settings**.
2. Specify a hostname for the Manager in the field provided.
3. Click **Save**.

Changing Port Settings

The **Port Settings** control the TCP ports the Manager's user interface is hosted on. To change the default web server ports, do the following:

1. Navigate to **System** > **Platform Settings**.
2. Change the ports used by the web server for the HTTP and HTTPS protocols.
3. Click **Save**.

Changing Network Settings

Note This does not apply to FindIT Network Manager for AWS. To modify the network configuration, use the EC2 console in AWS.

To change the network configuration for the Manager, do the following:

1. Navigate to **System** > **Platform Settings**.
2. Select the method for IP address assignment. The available options are DHCP (default) and Static IP. If you choose the Static IP option, then specify the address, subnet mask, default gateways and DNS servers in the appropriate fields.
3. Click **Save**

Changing Time Settings

The **Time Settings** manage the system clock for the Manager. To adjust the system clock, do the following:

1. Navigate to **System** > **Platform Settings**.
2. Select the appropriate timezone for the Manager.
3. Select the method for time synchronization. The available options are **NTP (default)** and **Local Clock**. If the NTP option is chosen, then optionally modify the NTP servers to use for synchronization.

   If **Local Clock** is selected, the you may manually adjust the date and time using the controls provided. Alternatively, click **clock** to synchronize the time with your PC.
4. Click **Save**.

Note If the virtual machine is configured to synchronize the local clock with the host machine, any changes to the local clock done through the **Platform Settings** page will be overwritten by the hypervisor.

If the hypervisor in use is VirtualBox and the VirtualBox Guest Additions are installed in the VM, the NTP service - timesyncd - will not operate.

Managing Privacy

Some of the features of FindIT Network Manager require the use of online services hosted by Cisco and result in the sharing of certain information with Cisco. These services include:

- **Cisco Active Advisor**—FindIT Network Manager can upload network inventory information to the Cisco Active Advisor service, *https://www.ciscoactiveadvisor.com*. This feature is disabled by default.
- **Lifecycle Reporting**—This feature includes the generation of the **Lifecycle Report**, **End of Life Report and Maintenance Report** in FindIT Network Manager. Lifecycle Reporting is enabled by default.
- **Software Updates**— Notification of the availability of software updates for network devices, and the ability to have those updates automatically applied. Software Updates are enabled by default.
- **Product Improvement**—This feature allows the Manager to send information about hardware and software usage in the network for the purpose of further developing the Cisco product portfolio. Product Improvement is enabled by default.

All of these features are subject to the Cisco Privacy Policy and you may enable or disable them at any time. The **Privacy Settings** page is displayed during the initial setup of the Manager, allowing you to disable any of the default enabled features prior to any network data being collected. More detail for each of these features and the information shared may be found below.

Cisco Active Advisor

Cisco Active Advisor (CAA) is a cloud-based service that provides essential lifecycle information about your network inventory. By enabling this feature, the Manager sends network inventory information to CAA and you can view the lifecycle information in the CAA portal. Sensitive information such as usernames and passwords is not sent.

Uploads may be performed automatically or on demand. To perform an on-demand upload, do the following:

1. Navigate to the **Network** page and select to view a network.
2. Select **Upload to CAA** from the **Network Actions** dropdown.
3. If prompted, provide your cisco.com credentials.
4. Optionally, select a label to be applied to the upload.
5. Click **Upload**. You may also click **View inventory data before sending** in order to inspect the data prior to uploading.

Note The cisco.com credentials provided must be used to log on to the Cisco Active Advisor portal (*https://www.ciscoactiveadvisor.com*) at least once prior to being used for upload.

To enable automatic uploads, do the following:

1. Navigate to the **Network** page, select a network and click **More**. Then select the CAA tab.
2. Enter your cisco.com credentials in the fields provided. Optionally, select a label to be applied to the upload.
3. Ensure the **Automatically upload newly discovered devices** checkbox is checked.
4. Click **Save**. You may also view an example of the data to be uploaded by clicking the link on this page.

To disable automatic uploads, do the following:

1. Navigate to the **Network** page, select a network and click **More**. Then select the CAA tab.
2. Uncheck the **Automatically upload newly discovered devices** checkbox.
3. Click **Save**.

Lifecycle Reporting

FindIT Network Manager provides information on the lifecycle state of each of the Cisco devices in the network. In order to do this, the Manager must provide Cisco with the product ID, serial number and hardware and software versions for each Cisco device. The IP address of the Manager may also be recorded. No personal or sensitive information will be intentionally collected during this process.

To disable the generation of lifecycle reports, do the following:

1. Navigate to **System** > **Privacy Settings**.
2. Uncheck the checkboxes for the reports you wish to disable.
3. Click **Save**.

Product Improvement

By enabling this feature, FindIT Network Manager periodically sends hardware and software product usage information to Cisco. The IP address of the Manager may also be recorded. No personal or sensitive information will be intentionally collected during this process.

To see an example of what information is sent, do the following:

1. Navigate to **System** > **Privacy Settings**.
2. Click the **View a Sample** link next to the **Send product improvement data to Cisco** checkbox. An example of an upload with sample data will be displayed.

To disable the generation of product improvement data, do the following:

1. Navigate to **System** > **Privacy Settings**.
2. Uncheck the **Send product improvement data to Cisco** checkbox.

3. Click **Save**.

Software Updates

Use of this feature requires FindIT to send the product ID and hardware and software version information for each device to Cisco. Your local IP address may also be recorded. No personal or sensitive information will be intentionally collected during this process.

To disable the use of automatic software updates, do the following:

1. Navigate to **System** > **Privacy Settings**.
2. Uncheck the checkboxes for both device firmware checks and FindIT application checks.
3. Click **Save**.

Managing Logging Settings

The **Log Settings** page allows you to control the amount of detail included in log files by the different software modules. The default logging level is **Info**, but you can reduce the number of messages logged by selecting **Warn** or **Error**, or view more detail by selecting **Debug**.

To change the log levels for the Manager, do the following:

1. Navigate to **System** > **Log Settings**.
2. Use the radio buttons to select the desired logging level for each software module
3. Click **Save**

The log files for the Manager may be found in the directory `/var/log/findit/manager/` on the local file-system. You may click **Download Log File** to download an archive of the contents of this directory. It may take several minutes to collect all the data.

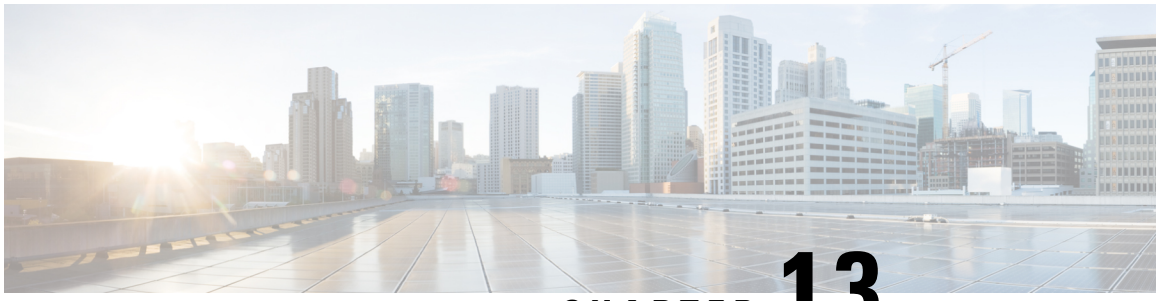
Managing the Local Probe

Note This page is not present on FindIT Network Manager for AWS.

Cisco FindIT Network Probe may be installed on the same host as the Manager in order to manage devices on the network local to the Manager, and the Cisco virtual machine image for the Manager does include the Probe. If you do not wish to manage the network local to the Manager, you may disable the co-located Probe using the following steps:

1. Navigate to **System** > **Local Probe**.
2. Click the toggle switch to disable the local Probe.
3. Click **Save**.

To remove the Probe software entirely from the Manager, log on to the operating system and use the command `sudo apt-get --purge autoremove findit-probe`. This removes the Probe software, configuration and dependencies that are not required by any other application.



CHAPTER 13

Notifications

This chapter contains the following sections:

About Notifications

The FindIT Network Manager generates notifications when different events occur in the network. A notification may generate an email or a pop-up alert that appears in the lower right corner of the browser, and all notifications are logged for later review. Notifications may also be acknowledged when they are no longer of interest and those notifications will be hidden from the **Notification Center** by default.

Supported Notifications

The following table lists the notifications supported by the FindIT Network Manager:

Table 26: Supported Notifications

Event	Level	Description	Clears Automatically?
Device Notifications			
Reachability/Device Discovered	Information	A new device is detected on the network.	Yes, 5 minutes after the device is discovered.
Reachability/Device Unreachable	Warning	A device is known through a discovery protocol, but is not reachable using IP.	Yes, when the device is reachable through IP again.
Reachability/Device Offline	Alert	A device is no longer detectable on the network	Yes, when the device is rediscovered.

Event	Level	Description	Clears Automatically?
Credential Required/SNMP	Warning	The Probe is unable to access the device due to an authentication error.	Yes, when the Probe authenticates.
Credential Required/User ID	Warning	The Probe is unable to access the device due to an authentication error.	Yes, when the Probe authenticates.
Device Service/SNMP	Warning	SNMP is disabled on the device.	Yes, when SNMP is enabled.
Device Service/Web service	Warning	The web service is disabled on the device.	Yes, when web service API is enabled
Health	Warning/Alert	The device health level changes to warning or alert.	Yes, when the device health returns to normal.
Cisco Support Notifications			
Firmware	Information	A later version of firmware is available on cisco.com	Yes, when the device is updated to the latest version.
End of Life	Warning/Alert	An End of Life bulletin is found for the device or an End of Life milestone has been reached.	No
Maintenance Expiry	Warning/Alert	The device is out of warranty and/or does not have a currently active maintenance contract.	Yes, if a new maintenance contract is taken out.
Device Health Notifications			
CPU	Warning/Alert	Device CPU usage exceeds maximum thresholds.	Yes, when the CPU usage returns to a normal level.
Uptime	Warning/Alert	Device uptime is below minimum thresholds.	Yes, when the device uptime exceeds minimum levels.
Connected Clients	Warning/Alert	The number of connected clients exceeds maximum thresholds.	Yes, when the number of connected clients returns to an acceptable level.

Viewing and Filtering Current Device Notifications

To view currently active notifications for a single device or all devices, do the following:

1. In the **Home** window, click **Notification Center** icon on the top right corner of the global tool bar. The number badge on the icon specifies the total number of unacknowledged notifications outstanding, and the color of the badge indicates the highest severity level currently outstanding.

Any notifications currently outstanding are listed below the icons in the **Notification Center**. The number on the severity icon provides a total of the number of notifications in each of the following categories:

- Information (green circle icon)
- Warning (orange triangle icon)
- Alert (red inverted triangle icon)

2. In the **Notification Center**, you can perform the following actions:
   - Acknowledge a notification—Check the check box against the notification to acknowledge it. You may acknowledge all notifications in the display by checking the **ACK All** checkbox
   - Filter the displayed notifications—Instructions for this action is provided in the following step
3. The Filter box limits the notifications displayed in the table. By default, notifications of all types and all severity levels will be displayed. To change an existing filter, double click on that filter to change the setting. To add a new filter, click on the Add Filter label and select a filter from the dropdown list. The following filters are available:

Table 27: Available Filters

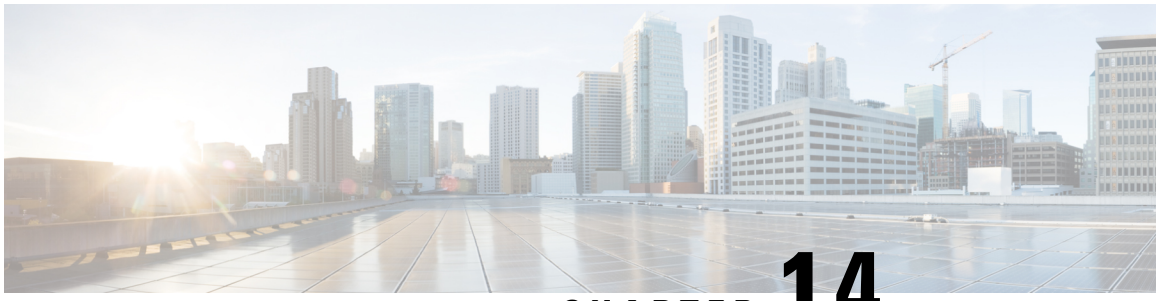
Filter	Description
Notification Type	The type of notification to be displayed. For example, to display notifications for devices that are offline, choose **Device Offline** from the drop-down list.
Severity	The severity level of the notifications to be displayed. It can be one of the following: • Info • Warning • Alert You may include higher severity levels by selecting the **Higher** checkbox.
Include Ack	Include notifications that have been acknowledged.
Network	Displays notifications for the specified network(s). Start typing in the filter and matching networks will be listed in a dropdown. Click to select the desired network. You may include multiple networks in the filter.
Device	Displays notifications for the specified device(s). Start typing in the filter and matching devices will be listed in a dropdown. Click to select the desired device. You may include multiple devices in the filter.

Note Notifications for individual devices may be seen in the **Basic Info** and the **Detailed Info** panels for the device.

To control how you receive notifications, change the notification settings at the organization or system level. For more information, see Managing Organizations or Changing Notification Defaults.

Viewing and Filtering Historical Device Notifications

The occurrence or change in state of any notification is recorded as an event on the Manager, and may be viewed through the Event Log. A subset of the event log may be viewed through the **Basic Info** panel or the **Device Detail** panel for individual devices. The **Basic Info** Panel shows only the last 24 hours' worth of events, while the **Device Detail** panel shows all historical data for the device that is available on the Probe. Events on the **Device Detail** panel may be filtered to help isolate those events you are interested in. See About the Event Log for more information on viewing and filtering historical events.



CHAPTER 14

Troubleshooting

This chapter contains the following sections:

Capturing Network Diagnostic Information

The **Network Show Tech** feature allows you to easily capture diagnostic information for your network in a form which you can analyze later or send to a support engineer. A **Network Show Tech** can be generated from the Manager UI or directly from the Probe UI in the event you are troubleshooting problems with the Manager-Probe connection. To capture a **Network Show Tech**, do the following:

1. Navigate to **Network** and select the Network for which you want to collect diagnostic information. Select the **Actions** tab and click **Show Tech**.

   Alternatively, log on to the Probe UI and navigate to **Troubleshooting** > **Network Show Tech**.

2. Use the check boxes to control whether or not to exclude passwords and certificates from device configurations, and where the diagnostic information should be sent. The following options are available:

   - Attach the diagnostic information to an existing Cisco support case. To do this, enter the case number in the field provided
   - Send the diagnostic information using email. Enter a comma-separated list of email addresses in the field provided
   - Download the diagnostic information to your PC

   If you are generating the **Network Show Tech** from the Probe, you do not have the options to email or attach to a support case. You must download the diagnostic information to your PC.

3. Click **Gather diagnostic data**.

The diagnostic information is delivered as a zip file, and includes a basic webpage to help navigate the data collected. To access the data, do the following:

1. Unzip the diagnostic information file to a convenient location on your PC.
2. Use a web browser to open the index.html file located in the directory created.

Managing Probe Log Settings

Log Settings for a Probe can be managed from the Manager UI or directly from the Probe UI in the event you are troubleshooting problems with the Manager-Probe connection. Log settings control what information the Probe will retain in its log files. This information is of primary interest to support engineers diagnosing problems with FindIT Network Management.

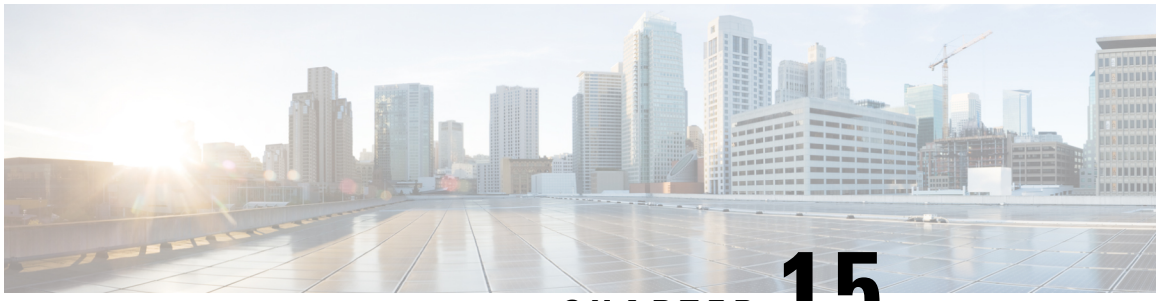
To change the log settings for a given network, navigate to **Network** and select the network for which you want to change the settings. Click **More** to display the **Network Detail** panel and then select the **Log Settings** tab. Alternatively, log on to the Probe UI and navigate to **Administration** > **Log Settings**.

The settings available include the following parameters:

Table 28: Log Settings

Field	Description
Log Level	The level of detail that should be logged. The following options are available: • **Error**—Error level messages only • **Warning**—Warnings and errors • **Info**(default)—Informational messages and above • **Debug**—all messages including low level debugging messages
Log Module	The module(s) for which messages should be logged. The following options are available: • **All (default)**—All modules • **Call-home Agent**—Communication between the Probe and Manager • **Discovery**—Device discovery events and topology discovery • **Northbound** —Communication between the Manager and the Probe • **Services**—Message translation between northbound and southbound • **Southbound**—Low level communication between the Probe and devices • **System**—Core system process not covered by any other module You may select multiple modules as needed.

The Probe log files are included in the **Network Show Tech** content. For more details on **Network Show Tech** option, see Capturing Network Diagnostic Information, on page 85 section.



CHAPTER 15

Frequently Asked Questions

This chapter answers frequently asked questions about the Cisco FindIT Network Management features and issues that may occur. The topics are organized into the following categories:

General FAQs

Q. What languages are supported by the FindIT Network Management?

A. FindIT Network Management is translated into the following languages:

- Chinese
- English
- French
- German
- Japanese
- Spanish

Discovery FAQs

Q. What protocols does FindIT use to manage my devices?

A. FindIT uses a variety of protocols to discover and manage the network. Exactly which protocols are using for a particular device will vary between device types.

The protocols used include:

- Multicast DNS and DNS Service Discovery (aka *Bonjour*, see *RFCs 6762 & 6763*)

- Cisco Discovery Protocol (CDP)
- Link Layer Discovery Protocol (see *IEEE specification 802.1AB*)
- Simple Network Management Protocol (SNMP)
- RESTCONF (See *https://datatracker.ietf.org/doc/draft-ietf-netconf-restconf/)*
- Private XML API for switch platforms

Q. How does FindIT discover my network?

A. The FindIT Network Probe builds an initial list of devices in the network from listening to CDP, LLDP, and mDNS advertisements. The Probe then connects to each device using a supported protocol and gathers additional information such as CDP & LLDP adjacency tables, MAC address tables, and associated device lists. This information is used to identify additional devices in the network, and the process repeats until all devices have been discovered.

Q. Does FindIT do network scans?

A. FindIT does not actively scan the network. The Probe will use the ARP protocol to scan the IP subnet it is directly attached to, but will not attempt to scan any other address ranges. The Probe will also test each discovered device for the presence of a webserver and SNMP server on the standard ports.

Configuration FAQs

Q. What happens when a new device is discovered? Will its configuration be changed?

A. New devices will be added to the default device group. If configuration profiles have been assigned to the default device group, then that configuration will be applied to newly discovered devices.

Q. What happens when I move a device from one device group to another?

A. Any VLAN or WLAN configuration associated with profiles that are currently applied to the original device group that are not also applied to the new device group will be removed, and VLAN or WLAN configuration associated with profiles that are applied to the new group that are not applied to the original group will be added to the device. System configuration settings will be overwritten by profiles applied to the new group. If no system configuration profiles are defined for the new group, then the system configuration for the device will not change.

Security Consideration FAQs

Q. What port ranges and protocols are required by FindIT Network Manager?

A. The following table lists the protocols and ports used by FindIT Network Manager:

Table 29: FindIT Network Manager - Protocols and Ports

Port	Direction	Protocol	Usage
TCP 22	Inbound	SSH	Command-line access to Manager. SSH is disabled by default on the Cisco virtual machine image

Port	Direction	Protocol	Usage
TCP 80	Inbound	HTTP	Web access to Manager. Redirects to secure web server (port 443)
TCP 443	Inbound	HTTPS	Secure web access to Manager
TCP 1069	Inbound	NETCONF/TLS	Communication between Probe and Manager with release 1.x. Used only in release 2.0 when release 1.x Probes are present.
TCP 50000 - 51000	Inbound	Device dependent	Remote access to devices
UDP 53	Outbound	DNS	Domain name resolution
UDP 123	Outbound	NTP	Time synchronization
UDP 5353	Outbound	mDNS	Multicast DNS service advertisements to the local network advertising the Manager

Q. What port ranges and protocols are required by FindIT Network Probe?

A. The following table lists the protocols and ports used by FindIT Network Probe:

Table 30: FindIT Network Probe - Protocols and Ports

Port	Direction	Protocol	Usage
TCP 22	Inbound	SSH	Command-line access to Probe. SSH is disabled by default on the Cisco virtual machine image.
TCP 80	Inbound	HTTP	Web access to Probe. Redirects to secure web server (port 443).
TCP 443	Inbound	HTTPS	Secure web access to Probe.
UDP 5353	Inbound	mDNS	Multicast DNS service advertisements from the local network. Used for device discovery.
TCP 10000 - 10100	Inbound	Device dependent	Remote access to devices. This range is only used by FindIT Network Probe version 1.x.
UDP 53	Outbound	DNS	Domain name resolution.
UDP 123	Outbound	NTP	Time synchronization
TCP 80	Outbound	HTTP	Management of devices without secure web services enabled.

Port	Direction	Protocol	Usage
UDP 161	Outbound	SNMP	Management of network devices.
TCP 443	Outbound	HTTPS	Management of devices with secure web services enabled. Access Cisco web services for information such as software updates, support status, and end of life notices.
TCP 1069	Outbound	NETCONF/TLS	Communication between Probe and Manager.
UDP 5353	Outbound	mDNS	Multicast DNS service advertisements to the local network advertising the Probe.

Q. How secure is the communication between FindIT Network Manager and FindIT Network Probe?

A. All communication between the Manager and the Probe is encrypted using a TLS 1.2 session authenticated with client and server certificates. The session is initiated from the Probe to the Manager. At the time the association between the Manager and Probe is first established, the user must log on to the Manager from the Probe, at which point the Manager and Probe exchange certificates to authenticate future communications.

Q. Does FindIT have 'backdoor' access to my devices?

A. No. When FindIT discovers a supported Cisco device, it will attempt to access the device using the factory default credentials for that device with the username and password: `cisco`, or the SNMP community:`public`. If the device configuration has been changed from the default, then it will be necessary for the user to supply correct credentials to FindIT.

Q. How secure are the credentials stored in FindIT?

A. Credentials for accessing FindIT are irreversibly hashed using the SHA512 algorithm. Credentials for devices and other services, such as the **Cisco Active Advisor**, are reversibly encrypted using the AES-128 algorithm.

Q. How do I recover a lost password for the web UI?

A. If you have lost the password for all the admin accounts in the web UI, you can recover the password by logging on the console of the Probe and running the **finditprb recoverpassword** tool, or logging on the console of the Manager and running the **finditmgr recoverpassword** tool. This tool resets the password for the cisco account to the default of cisco, or, if the cisco account has been removed, it will recreate the account with the default password. Following is an example of the commands to be provided in order to recover the password using this tool.

```
cisco@finditmanager:~$ finditmgr recoverpassword
Are you sure? (y/n) y
Recovered the cisco account to default password
recoverpassword FindIT Manager successful!
cisco@finditmanager:~$
```

Note When using FindIT Network Manager for AWS, the password will be set to the AWS instance ID.

Remote Access FAQs

Q. When I connect to a device's administration interface from FindIT Network Management, is the session secure?

A. FindIT Network Management tunnels the remote access session between the device and the user. The protocol used between the Probe and the device will depend on the end device configuration, but FindIT will always establish the session using a secure protocol if one is enabled (e.g. HTTPS will be preferred over HTTP). If the user is connecting to the device via the Manager, the session will pass through an encrypted tunnel as it passes between the Manager and the Probe, regardless of the protocols enabled on the device. The connection between the user's web browser and the Manager will always be HTTPS.

Q. Why does my remote access session with a device immediately log out when I open a remote access session to another device?

A. When you access a device via FindIT Network Manager, the browser sees each connection as being with the same web server (FindIT) and so will present cookies from each device to every other device. If multiple devices use the same cookie name, then there is the potential for one device's cookie to be overwritten by another device. This is most often seen with session cookies, and the result is that the cookie is only valid for the most recently visited device. All other devices that use the same cookie name will see the cookie as being invalid and will logout the session.

Q. Why does my remote access session fail with an error like the following? **Access Error: Request Entity Too Large HTTP Header Field exceeds Supported Size**

A. After doing many remote access sessions with different devices, the browser will have a large number of cookies stored for the Manager domain. To work around this problem, use the browser controls to clear cookies for the domain and then reload the page.

Software Update FAQs

Q. How do I keep the Manager operating system up to date?

A. From version 1.1.0, the Manager uses the Ubuntu Linux distribution for an operating system. The packages and kernel may be updated using the standard Ubuntu processes. For example, to perform a manual update, log on to the console as the cisco user and enter the commands `sudo apt-get update` and `sudo apt-get upgrade`. The system should not be upgraded to a new Ubuntu release, and it is recommended that no additional packages should be installed beyond those included in the virtual machine image supplied by Cisco, or those installed as part of a minimal Ubuntu install.

Q. How do I update Java on the Manager?

A. From version 1.1.0, FindIT Network Manager uses the OpenJDK packages from the Ubuntu repositories. OpenJDK will automatically be updated as part of the updating the core operating system.

Q. How do I keep the Probe operating system up to date?

A. From version 1.1.0, the Probe uses the Ubuntu Linux distribution for an operating system. The packages and kernel may be updated using the standard Ubuntu processes. For example, to perform a manual update, log on to the console as the cisco user and enter the commands `sudo apt-get update` and `sudo apt-get upgrade`. The system should not be upgraded to a new Ubuntu release, and it is

recommended that no additional packages should be installed beyond those included in the virtual machine image supplied by Cisco, or those installed as part of a minimal Ubuntu install.

Q. How do I keep the Probe operating system up to date when using a Raspberry Pi?

A. The Raspbian packages and kernel may be updated using the standard processes used for Debian-based Linux distributions. For example, to perform a manual update, log on to the console as the cisco user and enter the commands `sudo apt-get update` and `sudo apt-get upgrade`. The system should not be upgraded to a new Raspbian major release. It is recommended that no additional packages are installed beyond those installed as part of the 'Lite' version of the Raspbian distribution and those that are added by the Probe installer.