



Cisco FindIT Network Probe Administration Guide, Version 1.1.x

First Published: 2018-03-14

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

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/go/trademarks>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)



The Java logo is a trademark or registered trademark of Sun Microsystems, Inc. in the U.S. or other countries.

© 2018 Cisco Systems, Inc. All rights reserved.



CONTENTS

CHAPTER 1

Cisco FindIT Network Management Overview 1

About Cisco FindIT Network Management 1

Audience 1

Terminology 2

System Requirements for Cisco FindIT Network Probe 3

CHAPTER 2

Getting Started 5

Installing FindIT Network Probe 5

Accessing the Probe User Interface 7

Performing the Initial Setup 8

Configuring the Network 12

CHAPTER 3

Using FindIT Network Probe 17

Using the Cisco FindIT Network Probe GUI 17

Upgrading FindIT Network Probe 21

CHAPTER 4

Discovery 23

About Discovery 23

Overview of the Topology Map and Tools 24

Viewing Basic Device Information 27

Performing Device Actions 29

Accessing the Device Administration Interface 32

Viewing Detailed Device Information 32

Viewing Device Inventory 35

Using Floor Plans 36

CHAPTER 5

Dashboard 39

About Dashboard 39

Adding a Widget	40
Modifying a Widget	40
Deleting a Widget	40
Modifying the Dashboard Layout	41

CHAPTER 6**Port Management 43**

About Port Management	43
-----------------------	----

CHAPTER 7**System Configuration 45**

About System Configuration	45
Using the Wizard	45
Configuring Time Settings	46
Configuring DNS Resolvers	46
Configuring Authentication	47

CHAPTER 8**Network Configuration 49**

About Network Configuration	49
Configuring VLANs	49
Configuring Wireless LANs	50

CHAPTER 9**Reports 53**

About Reports	53
Viewing the Summary Report	54
Viewing the End of Life Report	54
Viewing the Maintenance Report	55
Viewing the Wireless Network Report	56
Viewing the Wireless Client Report	58

CHAPTER 10**Troubleshooting 61**

About Troubleshooting	61
Capturing Network Diagnostic Information	61

CHAPTER 11**Administration 63**

About Administration	63
Managing Device Groups	64

Managing Device Credentials	65
Setting Up CAA Credential	66
Managing Users	66
Managing Site Information	67
Connecting to the Manager	67
Managing Email Settings	67
Managing Log Settings	68
Managing Platform Settings	69
Backing Up and Restoring the Probe Configuration	70

CHAPTER 12**Notifications 73**

About Notifications	73
Supported Notifications	73
Viewing and Filtering Current Device Notifications	74
Viewing and Filtering Historical Device Notifications	76

CHAPTER 13**Frequently Asked Questions 77**

General FAQs	77
Discovery FAQs	77
Configuration FAQs	78
Security Consideration FAQs	79
Remote Access FAQs	81
Software Update FAQs	82



Cisco FindIT Network Management Overview

This chapter contains the following sections:

- [About Cisco FindIT Network Management](#) , page 1
- [Audience](#), page 1
- [Terminology](#), page 2
- [System Requirements for Cisco FindIT Network Probe](#), page 3

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 interfaces: 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, and connect to the Probe installed at a particular site when you wish to view a detailed information for that site.

FindIT Network Manager and FindIT Network Probe are each detailed in their respective administration guides.

For more details on FindIT Network **Probe**, refer to the following sections in this user guide.

Audience

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

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).
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: <ul style="list-style-type: none"> • 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.
<ul style="list-style-type: none"> • 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 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

To run FindIT Network Manager 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 the FindIT Network Manager on a 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

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 9 (macOS only) or above

- Google Chrome version 52 (Recommended) or above
- Microsoft Edge version 38 or above
- Microsoft Internet Explorer version 11 or above
- Mozilla Firefox version 48 or above

**Note**

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

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



Getting Started

This chapter contains the following sections:

- [Installing FindIT Network Probe, page 5](#)
- [Accessing the Probe User Interface, page 7](#)
- [Performing the Initial Setup, page 8](#)
- [Configuring the Network, page 12](#)

Installing FindIT Network Probe

An instance of FindIT Network Probe is required for each site in your network that you want to manage. The Probe discovers the network, and provides you with a single interface that you may use to monitor and manage your Cisco 100 to 500 Series network devices.

FindIT Network Probe is provided 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

The virtual machine image is packaged in both the Distributed Management Task Force's **Open Virtualization Format (OVF)**, and as a zipped **Microsoft Hyper-V** virtual machine. The Probe is also included as part of the FindIT Network Manager virtual machine image, allowing a single VM to act as both Manager and Probe for a particular site. Each of these deployment options is discussed in the following sections:



Note

The network interface card of the FindIT Network Probe virtual machine should be bridged to a VLAN containing the management interfaces for at least one of the network devices. If the Probe is not directly connected to at least one network device, it may be unable to fully discover the network.

Installing using VirtualBox

- 1 Download the FindIT Network Probe ova file by navigating to www.cisco.com/go/findit and selecting the **Download Software for this Product** link in the **Support** pane.
- 2 Open **VirtualBox** and select **File > Import Appliance...**
- 3 Follow the prompts and make sure you have selected the downloaded file for the appliance to import.
- 4 Check that network adapter 1 is enabled and bridged to the correct physical interface on the host machine.
- 5 Start the virtual machine.

Installing using VMWare

- 1 Download the FindIT Network Probe ova file by navigating to www.cisco.com/go/findit and selecting the **Download Software for this Product** link in the **Support** pane.
- 2 Consult the VMWare documentation for your product to determine the procedure for importing a virtual machine. For example, if you are using VMWare Fusion, you would open the VMWare Fusion application and select **File > Import...** and follow the prompts.
- 3 Select the downloaded ova file from your local directory and continue the import process.
- 4 Check that the network interface on the newly created virtual machine is connected and bridged to the correct physical interface on the host machine.
- 5 Start the virtual machine.

Installing using Hyper-V

- 1 Download the FindIT Network Probe Hyper-V virtual machine archive by navigating to www.cisco.com/go/findit and selecting the **Download Software for this Product** link in the **Support** pane.
- 2 Unzip the archive to a convenient location on your PC.
- 3 Open **Hyper-V Manager** and select **Action > Import Virtual Machine ...**
- 4 Follow the prompts and make sure you have selected the directory created when you extracted the archive in step 2. Consider whether you want the VM files to be copied, moved, or left in place when you select the import type.
- 5 Check that the network adapter is connected to a virtual switch that is mapped to the correct external network on the host machine.
- 6 Start the virtual machine.

Installing using Ubuntu

- 1 Download the FindIT Network Probe Ubuntu 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 Ubuntu Linux PC.
- 3 Execute the installer using the command **sh <filename of installer>**. For example **sh finditprobe-1.1.0-ubuntu-xenial-amd64.sh**. If necessary, enter your password at the sudo prompt.

Installing on a Raspberry Pi

- 1 Download the Raspbian Stretch OS image available at <https://www.raspberrypi.org/downloads/raspbian/>. The 'lite' image is recommended to maximize the performance of the Probe.
- 2 Prepare the Raspberry Pi using the installation guide at <https://www.raspberrypi.org/documentation/installation/installing-images/README.md>.
- 3 Navigate to www.cisco.com/go/findit and download the FindIT Network Probe Raspbian Linux installer file.
- 4 Select the **Download Software for this Product** link in the **Support** pane and copy the installer file to the Raspberry Pi.
- 5 Execute the installer using the command `sh <filename of installer>`. For example, `sh finditprobe-1.1.1-raspbian-stretch-armhf.sh`. If necessary, enter your password at the sudo prompt.

Removing FindIT Network Probe from Ubuntu or Raspbian

To remove FindIT Network Probe and all its dependencies from an Ubuntu or Raspbian system and retain the Probe's configuration, do the following:

- 1 Log on to the operating system using either the console or SSH.
- 2 Enter the command `sudo apt-get autoremove findit-probe` and follow the prompts

To completely remove FindIT Network Probe, its dependencies and configuration from an Ubuntu or Raspbian system, do the following:

- 1 Log on to the operating system using either the console or SSH.
- 2 Enter the command `sudo apt-get --purge autoremove findit-probe` and follow the prompts.

Accessing the Probe User Interface

The following instructions detail how to get started with FindIT Network Probe:

Configuring the default IP Address using DHCP

The default IP address configuration for the Probe is performed using DHCP. Make sure your DHCP server is running and can be reached.

Locating the IP Address of the Probe

- 1 The Probe can be discovered and accessed using the **Cisco FindIT Network Discovery Utility** that enables you to automatically discover all supported Cisco devices in the same local network segment as your computer. You can get a snapshot view of each device or launch the product configuration utility to view and configure the settings. For more information, see <http://www.cisco.com/go/findit>.
- 2 The Probe is Bonjour-enabled and automatically advertises itself using the Bonjour protocol. If you have a Bonjour-enabled browser, such as **Microsoft Internet Explorer** with a Bonjour plug-in, or the **Apple Mac Safari** browser, you can find the Probe on your local network without knowing its IP address.

You can download the Bonjour for **Microsoft Internet Explorer** browser from Apple's website by visiting: <http://www.apple.com/bonjour/>.

- 3 If you are using the virtual machine image, you can retrieve the IP address of the Probe from the virtual machine console. Use your Hypervisor's management tools to connect to the console of the virtual machine and log on with the default username: `cisco` and password: `cisco`. You will be required to change the password immediately after logging in. The new password should be a complex, non-dictionary word using a mixture of character types. A banner will then be displayed showing the current IP address.

If you have installed the Probe on your own Ubuntu or Raspbian Linux installation, you may use the operating system tools to discover the IP address. For example, you may enter the command `ifconfig` at a shell prompt and see a list of interfaces and their addresses displayed.

- 4 Locate the IP address assigned by your DHCP server by accessing your router or DHCP server. See your DHCP server instructions for more information.

Launching the User Interface on a Standalone Probe

- 1 Launch a web browser, such as **Google Chrome** or **Microsoft Edge**.
- 2 In the **Address** field, enter the default DHCP address and click **Enter**.
- 3 Enter the default user name: `cisco` and password: `cisco`. Click **Login**.
The **FindIT Network Probe** user interface is displayed.
- 4 You will be prompted to change the password for the `cisco` account. Ensure that the new password is at least 8 characters in length using at least 3 different character classes.

Launching the Probe User Interface when the Probe is Co-hosted with a Manager

- 1 Log on to the Manager user interface as described in the Cisco FindIT Network Manager Administration Guide.
- 2 Select the **Network Overview** page in the navigation and identify the site associated with the co-hosted probe. This site will be associated with the Manager automatically when the Manager is installed and will be the only site displayed.
- 3 Click on the site icon on the map in **Map View**, or the row in the table in **List View**, and display the information panel for the site.
- 4 Click on the globe icon to open up the Probe user interface in a new tab.

Performing the Initial Setup

To ensure that the **Probe** meets your requirements, you can perform the following configuration setup.

Configuring Basic System Settings on the VM Image (Optional)

To configure basic system settings such as IP addressing and time settings for the **Probe**, do the following:

- 1 Navigate to **Administration > Platform Settings**.
- 2 Specify a hostname for the **Probe**. The hostname is used to identify the **Probe** in Bonjour advertisements and in the FindIT Network Discovery Utility user interface.

- 3 Optionally, specify static IP parameters in the fields provided. By default, the **Probe** will automatically determine the IP settings using DHCP.
- 4 Optionally, you can set the **Probe** to use its internal clock for keeping time, or you can specify your preferred NTP servers. By default, the **Probe** will synchronize its clock with public NTP servers.

Configuring Basic System Settings on the VM Image through the Command Line (Optional)

As an alternative to configuring basic system settings through the web interface, you may set them using the command line as follows:

- 1 Connect to the virtual machine console.
- 2 Log on using the default username and password set to: `cisco`. You will be required to change the password immediately after logging in. The new password should be a complex, non-dictionary word using a mixture of character types.
- 3 Enter the command `sudo config_vm` to perform the initial configuration. The `config_vm` utility will prompt you with a series of steps to change the platform settings.
- 4 First you will be prompted to change the hostname for the Probe. The hostname is used to identify the Probe in Bonjour advertisements and in the FindIT user interface. Choose a meaningful name here, or you may skip this step to keep the default hostname.
- 5 Next you will be prompted to configure the network interface. The options here are static and dhcp (the default). If you select static, you will be prompted for IP address information, default gateway, and DNS server addresses. The network interface will be reset if you make changes here.

Communicating with FindIT Network Manager (Required)

The Probe must be associated with a Manager, or you will not be able to use the full functionality. You can establish communication between the Probe and an instance of FindIT Network Manager using the following steps:

- 1 Navigate to **Administration > Site Information**.
- 2 Enter a descriptive name for the Probe. This will be displayed in the Manager user interface when viewing this site.
- 3 Specify the location for the site and click **Save**. You may enter the address of the site into the appropriate fields. If you enter a partial address, a list of potential matches will be displayed, and you can select the location from the list. Alternatively, you can click on the location in the map.

If the Probe is co-hosted with the Manager, no further action is required. The connection with the Manager is automatically established. Otherwise, the following additional steps are necessary to establish communication with the Manager:

- 1 Navigate to **Administration > Manager Connection**. Enter the DNS name or IP address of the **Manager** and click **Connect**.
- 2 Your browser will be redirected to the **Manager** login screen. Login using administrator credentials for the **Manager**, and then your browser will be redirected back to the **Probe**.
- 3 Verify that the status of the **Manager** is **Connected**.

Managing User Access



Note User Management on the probe is not required when the Probe is co-hosted with the Manager.

The **Probe** is initially set up with a single, default username and password. These credentials should be used to initially set up the Probe and establish communication with the Manager. Once the Probe is associated with the Manager, you may log on to the Probe using the credentials defined in the Manager, and the initial username and password created at the time of install are only used as a fallback user to log on when the Manager is unable to be reached.

To modify the fallback user, do the following:

- 1 Navigate to **Administration > User Management**.
- 2 Edit the username and password as required.
- 3 Click **Save**

You may also set up password complexity restrictions for the fallback user on the **User Management** page. New passwords will be required to meet these restrictions.

Setting up Licenses

FindIT Network Manager and Probe are licensed using Cisco Smart Licensing. When first installed, the Probe runs in an unlicensed state. Once associated with a Manager, licensing for the Probe is controlled by the Manager. If the Probe is not associated with a Manager, a message will be displayed on the user interface, and you will have 90 days to associate the Probe with a Manager before system functionality is restricted. For more details on the licensing process, see the licensing chapter of the *Cisco FindIT Network Manager Administration Guide*.

Setting up Device Credentials

For FindIT Network Probe to be able to manage the network devices, you must provide suitable credentials to allow access to the device.

When the Probe discovers a device, it will initially attempt to access the device using the default credentials with the username: `cisco`, password: `cisco` and the SNMP community: `public`. However, if the device is not using default credentials, then correct credentials must be supplied as detailed in the following steps:

- 1 Navigate to **Administration > Device Credentials**. You will see a status message showing the total number of devices discovered and the number of discovered devices for which credentials are required. Click on this message to see a list of devices requiring credentials.
- 2 Enter a username and password combination and/or SNMP community in the respective fields. If more sets of credentials are required, then click the **+**(plus) icon. This allows up to three sets of each type of credential to be entered.
- 3 Click **Apply**. The Probe will test each credential against each device for which a credential is required. Working credentials are saved for each device.

Once working credentials are provided, the Probe will discover the network and generate a **Topology** map.

Configuring Email Settings (Optional)

FindIT Network Probe can notify you via email when selected events occur within the network. To control which events will generate an email see [Customizing Notification Display](#), on page 12. To configure email settings, do the following:

- 1 Navigate to **Administration > Email Settings**.
- 2 On this page, you may specify the email server and port to use for outgoing messages, encryption and authentication settings, and the email addresses to be used.
- 3 Once you have completed the configuration, click **Save**.
- 4 Click **Test Connectivity** to test the changes you made.

Customizing the Topology Map (Optional)

Once working credentials are provided, the **Probe** will discover the network and generate a **Topology** map. You may adjust the map as necessary.

- 1 Navigate to **Discovery > Topology**.
- 2 You may drag individual device icons to improve the layout. Any changes you make to the layout are permanent. FindIT Network Probe will not make further changes to the location of the icon.
- 3 Click **Overlays** to open the **Overlays and Filters** panel and use the check boxes to limit the device types that will be displayed in the map.

Uploading Floor Plans (Optional)

You may upload floor plans for site and place your network devices in order to document the location of your equipment. The following steps guide you through this process:

- 1 In the **Discovery** screen, click **Floor Plan**.
- 2 Enter a name for the building and the floor, and then either drag an image file into the drop zone or click inside the widget to select an image file on your PC. Image formats supported include .png, .gif, .jpg
- 3 Click **Save** to save the changes.
- 4 To place a device on the floor plan, type the device name or IP address into the search box at the bottom of the screen. As you type, matching devices will be displayed, where grayed out devices have already been placed on a floor plan.
- 5 Click on a device to add it to the floor plan, and drag the device to the correct location.

Customizing the Dashboard

You may customize the dashboard to suit your requirements using the following steps:

- 1 Select **Dashboard** from the navigation at the left of the screen. The default dashboard will be displayed. To make changes, click **enable edit mode** icon on the top right of the dash board window.
- 2 To change the layout, select the **edit dashboard** settings icon. Select the layout that best suits your screen and the widgets you want to use.

- 3 To relocate individual widgets within the dashboard, click and hold **change widget location** icon. Drag the widget to the desired location in the layout.
- 4 To add a new widget to the dashboard, click **add new widget +** icon at the top right of the dashboard and select the widget from the list. To remove a widget from the dashboard, click **remove widget ✕** icon in the top right corner of the widget.
- 5 To change the behavior of a widget, click **edit widget configuration** icon in the top right of the widget. Use the drop down lists to select the specific device, interface or network the widget should monitor.
- 6 When you have finished making changes, click **save** icon at the top of the dashboard.

Customizing Notification Display

You may customize the behavior of notifications using the following steps:

- 1 Click the **Notification Center** icon to open the **Notifications** panel.
- 2 Click the **Settings** tab. Use the check boxes to control which notifications generate a pop-up alert in the user interface, and those that generate an email notification. If you use email notifications, you must ensure that the email settings are correctly configured. See [Configuring Email Settings \(Optional\)](#), on page 11 for more details.
- 3 Click **Save**.

Configuring the Network

If you are installing a new network, you may want to take this opportunity to perform the initial configuration of the network. Even in an existing network, you may choose to make configuration changes at this time.

Updating Firmware for devices (Optional)

The Probe will notify you if there are firmware updates available for the devices in your network, and an **Update Firmware** icon will be displayed against the device in several areas of the user interface.

To update firmware for a single device, do the following:

- 1 Click on the device in the **Topology Map** to display the **Basic Info** panel.
- 2 Open the **Action** panel and click on the **Upgrade firmware to latest** button. The Probe will download the necessary firmware from Cisco and apply the update to the device. The device will reboot as part of this process.

Alternatively, firmware can be upgraded from your PC by clicking the **Upgrade From Local** option and specifying the firmware image to be uploaded.
- 3 You may view the progress of the upgrade by clicking on the **Task Status** icon in the top right of the Probe user interface.

You may also upgrade individual devices from the **Inventory** view. For details, see [Viewing Device Inventory](#), on page 35.

Updating Firmware for the Network

If you wish to upgrade the entire network to the latest available firmware, do the following:

- 1 Navigate to the **Discovery** page.
- 2 Click **Actions** at the top of the page and select the **Upgrade Firmware** option. The Probe will download the necessary firmware files from Cisco for each device that has an available update, and will apply the update to each device in turn. Each device will reboot as part of this process.
- 3 You may view the progress of the upgrade by clicking on the **Task Status** icon in the top right of the Probe user interface.

Configuring Device Groups

The Probe uses the concept of device groups to allow you to apply configuration to multiple devices at the same time and to ensure that configuration settings match across the network. To allocate devices to a device group, do the following:

- 1 Navigate to **Administration > Device Groups**.
- 2 Click the **+**(plus) icon to add a new group.
- 3 Specify a name and description for the device group.
- 4 Select one or more devices to join the group. Each device can only be a member of one group. If a selected device was previously a member of a different group, it will be removed from that group. If you wish to remove a device from the group, click the **cancel** icon next to the device, and the device will be moved to the **Default** device group. Device groups can contain a mixture of different device types.
- 5 Click the **save** icon to create the group or **cancel** icon to cancel.

System Configuration

The Probe allows you to configure system settings for multiple network devices. You may use the **System Configuration Wizard** to create configuration profiles for each section of the system settings, or you can create profiles individually. To use the **System Configuration Wizard**, do the following:

- 1 Navigate to **System Configuration > Wizard**.
- 2 Enter a description for the configuration profiles to be created, and select one or more device groups to which the configuration will be applied.
- 3 Click **Next**.
- 4 Specify the time settings for this group. A **Time Management** profile contains settings for the timezone, daylight savings, and NTP. If you do not wish to create a **Time Management** profile for this group, click **Skip**, otherwise click **Next**.
- 5 Specify the **DNS settings** for this group. A **DNS Resolvers** profile contains settings for the domain name, and the DNS servers to use. If you do not wish to create a DNS Resolvers profile for this group, click **Skip**, otherwise click **Next**.
- 6 Specify the user authentication settings for this group. An **Authentication profile** contains settings for the local user database for the devices. If you do not wish to create an **Authentication profile** for this group, click **Skip**, otherwise click **Next**.
- 7 Review the configuration settings you have made. If you wish to make changes, use the **Back** button to return to the appropriate screen. Once you are satisfied, click **Finish** to create the profiles and apply to the devices in the selected device groups.

- 8 You may view the progress of the configuration by clicking on the **Task Status** icon in the top right of the Probe user interface.

Wireless Networks and VLANs

The Probe allows you to create a Virtual LAN and apply to multiple groups at the same time.

To create a Virtual LAN, do the following:

- 1 Navigate to **Network > Virtual LAN**.
- 2 Click the **+**(plus) icon to add a new VLAN.
- 3 Specify a VLAN name and VLAN ID.
- 4 Select one or more groups to apply.
- 5 Click the **save** icon to create a VLAN or the **Cancel** button to cancel.

The Virtual LAN page displays a table which lists any VLANs in the network that were not configured by FindIT Network Management. You can view the details of the VLAN that are displayed, and remove the VLAN if desired. If the Probe is unable to edit the VLAN for any reason, a message will be displayed, and you may edit the VLAN in the device **Administration** interface.

The Probe also allows you to create Wireless LANs. To create a Wireless LAN, do the following:

- 1 Navigate to **Network > Wireless LAN**.
- 2 Click the **+**(plus) icon to add a new Wireless LAN.
- 3 Specify a SSID name, VLAN ID and the authentication method.
- 4 Select one or more groups to apply.
- 5 Click the **save** icon to create a WLAN or **Cancel** button to cancel.

The Wireless LAN page displays a table which lists any SSIDs in the network that were not configured by FindIT Network Management. You can view the details of the SSID that are displayed, and remove the SSID if desired. If the Probe is unable to edit the SSID for any reason, a message will be displayed, and you may edit the SSID in the device **Administration** interface.

Backingup Device Configurations

The Probe allows you to back up the configurations of your network devices. To back up the configuration for a single device, do the following:

- 1 Click on the device in the **Topology Map** to display the **Basic Info** panel.
- 2 Open the **Action** panel and click **Backup Configuration** button. Optionally, you may add a note describing this backup in the window that appears. The **Probe** will copy the configuration of the device and store it locally on the Probe.
- 3 You may view the progress of the backup by clicking on the **Task Status** icon in the top right of the Probe user interface.

You may also backup individual devices by clicking **Backup Configuration** in the **Inventory** view.

If you wish to back up the configurations for the entire network, do the following:

- 1 Navigate to the **Discovery** page.

- 2 Click **Actions** button at the top of the page and select the **Backup Configurations** option. Optionally, add a note describing this backup in the window that appears. The Probe will copy the configuration of each device and store them locally on the Probe.
- 3 You may view the progress of the backup by clicking on the **Task Status** icon in the top right of the Probe user interface.



Using FindIT Network Probe

This chapter contains the following sections:

- [Using the Cisco FindIT Network Probe GUI, page 17](#)
- [Upgrading FindIT Network Probe, page 21](#)

Using the Cisco FindIT Network Probe GUI

Home window

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

Figure 1: Cisco FindIT Network Probe Home Page

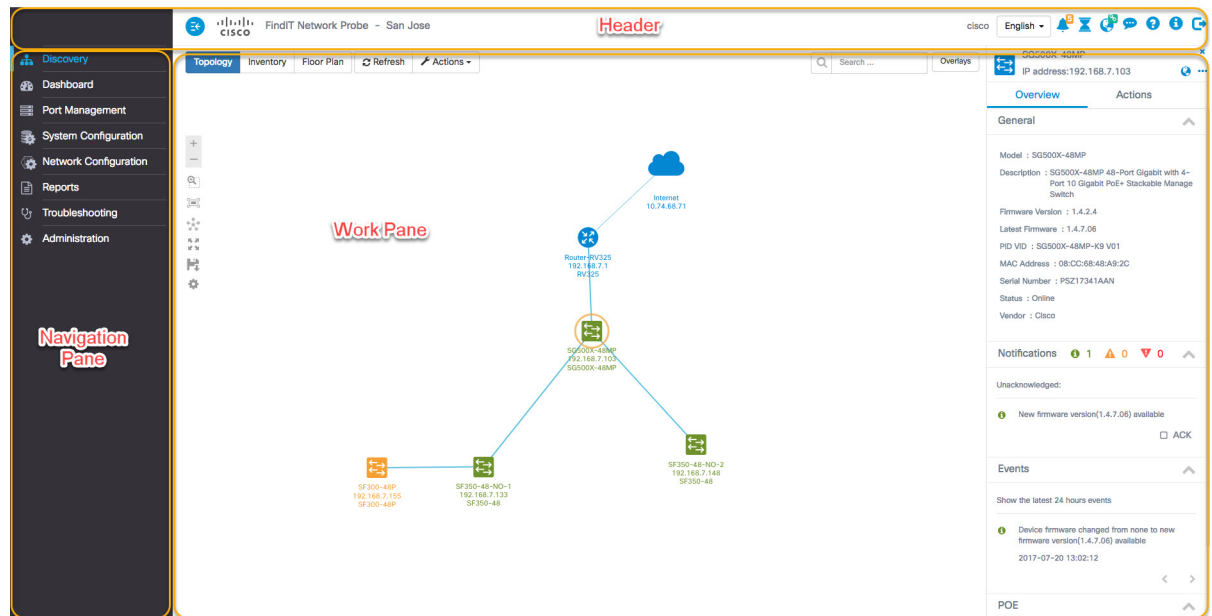





Table 1: Cisco FindIT Network Probe Home Page






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: <ul style="list-style-type: none"> • 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 2: Navigation Pane Options



Icon	Name	Description
	Discovery	Contains different views of the network devices discovered by FindIT Network Probe. Views include the network topology, an inventory view, and a floor-plan view that allows you to track the physical layout of the network.
	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.
	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.








Icon	Name	Description
	System Configuration	The System Configuration page allow you to modify system settings for your network devices.
	Network Configuration	The Network Configuration page allow you to manage the VLANs and WLANs in your network.
	Reports	Under the Reports heading, you will find a number of reports that provide life-cycle and performance information about your network devices.
	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 3: 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.

Icon	Option	Description
	Notification Center	This icon displays the number and severity of outstanding notifications in FindIT Network Probe. 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 74 in this guide.
	Task Status	The Task Status and Task History for actions performed by FindIT Network Probe. Click this icon to display tasks in progress, and completed.
	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 Probe

From time to time, Cisco releases new versions and updates for FindIT Network Probe and posts them to the Software Center on cisco.com. FindIT Network Probe 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 Probe download and apply the update, or you can choose to download the update yourself and manually apply it.

**Note**

Prior to updating the Probe software, you should ensure that the Manager software is first updated. Otherwise the Probe may not be able to connect to the Manager until after the Manager has been updated.

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

- 1 Click **About FindIT** icon to open the **About FindIT** popup. If an update is available for the Probe, it will be shown here.
- 2 Click the message about the update to have the Probe download the update and apply it.

The Probe will download and apply the update. During the download process, you may view the progress of the download by clicking on the Task Status icon in the top right of the Probe user interface. Once the download is complete, the Probe will begin applying the update, and the Probe UI will display the update progress. Once the update has been applied, the Probe application will restart.

To apply a Probe update manually, do the following:

- 1 Download the FindIT Network Probe 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 Probe filesystem.
- 3 Execute the installer using the command **sh <filename of installer>**. For example **sh finditprobe-1.1.0-ubuntu-xenial-amd64.sh**. If necessary, enter your password at the sudo prompt. The Probe application will restart during this process.

An update for a probe may also be initiated from the associated Manager. For more details, see the *Cisco FindIT Network Manager Administration Guide*.



Discovery

This chapter contains the following sections:

- [About Discovery, page 23](#)
- [Overview of the Topology Map and Tools, page 24](#)
- [Viewing Basic Device Information, page 27](#)
- [Performing Device Actions, page 29](#)
- [Accessing the Device Administration Interface, page 32](#)
- [Viewing Detailed Device Information, page 32](#)
- [Viewing Device Inventory, page 35](#)
- [Using Floor Plans, page 36](#)

About Discovery

The **Discovery** page in the FindIT Network Probe 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
 - **Inventory** view—Displays a table listing all devices in the network with information such as Model ID, Firmware Version, Serial Number, IP address and MAC Address. This view also allows the same actions to be performed that are provided in the **Topology** view
 - **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 **Discovery** page
- **Refresh** button—Rediscovered the network and updates the topology
 - **Actions** button—This button allows selected actions to be performed on all devices in the network that support that task. For example, you may backup all network device configurations with a single click. The **Actions** button also allows you to 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 Probe queries discovered devices for network connectivity details and builds a graphical representation or topology from the information it has gathered. The data collected by the Probe includes CDP & LLDP neighbor information, MAC Address tables, and Associated Device tables from Cisco 100 to 500 Series switches, routers and wireless access points. The Probe uses this information to determine how the network is constructed. When the network contains network infrastructure devices that are not manageable for any reason, FindIT Network 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**, from the **Navigation** pane, click **Discovery**. The **Discovery** window appears and, by default, displays the **Topology** map of your network.

Topology Controls

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

Table 4: 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.






Icon	Icon Name	Description
	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.
	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.
	Enter full screen mode	Fill the screen with the FindIT Network Probe 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.
	Topology Settings	Adjust the labels displayed for the topology icons.

Topology Icons

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

Table 5: 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.

Icon	Network Element	Description
	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 6: Overlays & Filters Panel

Item	Description
Select Overlay	<p>This feature enhances the Topology map with additional information based on the view selection. It can be one of the following:</p> <ul style="list-style-type: none"> • 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 code changes based on the percentage utilization of the link. It displays green to represent a moderate traffic and may change to red or orange to indicate a heavy traffic. Fields 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 the Device Tag in the text box below the Select Tag label to view the presence of a specific device you wish. This device tag can be assigned in the Detailed Info panel for the chosen device. When a tag is specified, only devices that match that tag will be displayed in the topology.
Show only: <ul style="list-style-type: none"> • 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 32.

To view more information on accessing the device administration interface, see [Accessing the Device Administration Interface](#), on page 32.

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 **Discovery** page, click **Topology** on the tool bar.
- 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 7: Basic Device Information

Item Name	Description
General 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 <i>Media Access Control (MAC)</i> 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.
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 74 . 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

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 29](#).

Performing Device Actions

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

- Step 1** On the **Discovery** page, click on a network device such as a switch or a router for which you want to perform the configuration tasks.
- 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:
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	<p>Allows you to save a copy of the current device configuration on the Probe.</p> <ol style="list-style-type: none">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. Note This button changes to Saving... when the backup is in progress. <p>On completion of this action, a notification is displayed.</p>

Restore Configuration	<p>Allows you to restore a previously backed up configuration to the device.</p> <p>Click Restore Configuration. The Select configuration backup to apply to device name window is displayed.</p> <p>The following backup configuration options are provided in this window:</p> <ul style="list-style-type: none"> • 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 <p>Note Different options are only displayed when relevant backups are available for a device.</p> <p>To perform the backup configuration, do the following:</p> <ol style="list-style-type: none"> 1 In the Select configuration backup to apply to device name 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. 2 Click Restore Configuration to complete this action. This button changes to Restoring... which indicates that the configuration is in progress. <p>On completion, a notification will be displayed showing the success or failure of the operation.</p> <p>Alternatively, you may choose to upload a configuration file. Drag and drop the configuration file onto the target area, or click on the target area to select a file from the file system. Click Restore Configuration to complete the process.</p>
Reboot	<p>Restarts the device.</p> <p>Note When you click this button, you will be prompted to click again to confirm.</p>
Save Running Configuration	<p>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.</p>
Delete	<p>Remove an offline device from the Topology and Inventory.</p>

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 **Discovery** 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 the **Open Device GUI** icon 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 the **Open Device GUI**, your browser will connect to the device through the Probe. This means that if you are accessing the network remotely, only the Probe needs to be directly reachable from outside the site.
- Because these connections all go through the same host - the Probe - 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 **Discovery** 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 the **three dot** icon at the upper right corner.
- Step 3** In the **Detailed Info** attribute panel, you will find a complete list of device information under the following categories:
- **Overview**—Allows you to view the complete device details
 - **Port Management**—Allows you to manage the configuration of the switch ports
 - Note** This information is available only for devices with switch ports.
 - **WLAN**—Allows you to view the Wireless LANs configured on the device
 - Note** This information is available only for wireless devices.
 - **Events**—Provides a list of past actions and notifications for this device
 - **Configuration**—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

Each of these are described in the following steps:

- Step 4** Click **Overview** to view the following details:
You can click the arrow in the upper right corner of these panels to expand or collapse the display.

Table 8: Overview

Item Name	Description
Overview > GENERAL —Displays a detailed list of information for a particular device	
Hostname	Click Edit next to the device name to modify the device hostname in the text box. Click Save to save the changes.
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.
Model	Model name of the device.
Description	Device or product description.
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.
PID VID	Product ID and the Version ID.
MAC Address	The <i>Media Access Control (MAC)</i> 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 of the device.
IP	The IP Addresses of the device.
Domain	The domain name of the device.
Vendor	The manufacturer of the device.
Discovery Method	Shows the protocols and devices by which this device was discovered.
Overview > DASHBOARD —Displays a single dashboard widget for this device.	
Type	You can click the drop-down and choose the widget you wish to display. This option lists only those widgets supported by the device. For more details on Dashboard widgets, see About Dashboard , on page 39.

Item Name	Description
Overview > NOTIFICATION	Displays all notifications pertaining to a device
	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 74 . 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.

Step 5 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 serial number and the PID VID information of the device is displayed in the upper right corner of the image.

Note For more details on the operations, see [About Port Management, on page 43](#).

Step 6 Click **WLAN** to view the radio settings and the Wireless LANs configured on this device.

Step 7 Click **Events** to see a list of historical notifications and other events that are retained on the Probe for this device. You can use filters to limit the entries that are displayed. For more details, see [Viewing and Filtering Historical Device Notifications, on page 76](#). To see events over a longer history, visit the *Event Log* on the Manager.

Step 8 Click **Configuration** 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 9: Configuration Details

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: <ul style="list-style-type: none"> • 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

Viewing Device Inventory

The **Inventory** window 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. To access the **Inventory**, click the **Inventory** button on the **Discovery** page. The following table provides details of the information displayed:

Table 10: Inventory Details

Item	Description
Hostname	Displays the device hostname.
Type:	The type of device such as a switch, router or wireless access point (WAP).
Model	Model name of the device.
Version	The current firmware version of the device.
SN	The serial number for the device.
MAC	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.
IP	The Internet Protocol (IP) addresses of the device.
Actions	<p>Lets you perform one or more of the following actions on a device:</p> <ul style="list-style-type: none"> • Download Latest Firmware • Apply Firmware Upgrade From Local • Backup Configuration • Restore Configuration • Reboot Device • Save Running Configuration • Delete <p>Note For more details on these actions, see Performing Device Actions, on page 29</p>

Use the radio buttons at the top of the table to select between viewing devices and hosts. You may use the **Search** box to limit the display by typing hostnames, device types, serial numbers and so on.

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 **Discovery** and click **Floor Plan**. If an existing floor plan is displayed, click the **Floor Plan** link immediately above the floor plan controls.
- 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 floor with network devices.

Placing Network Devices on a Floor Plan

- 1 Navigate to **Discovery** and click **Floor Plan**. If the floor plan you are interested in is not already displayed, then click on the floor plan.
- 2 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 on a device to add it to the floor plan. If you select a device that has already been placed on another floor plan, it will be removed and added to this one. Once the device has been added to the floor plan, you may drag it to the correct location.
- 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 **Discovery** 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 **Discovery** and click **Floor Plan**. If an existing floor plan is displayed, click the **Floor Plan** link immediately above the floor plan controls.
- 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 **Discovery** and click **Floor Plan**. If an existing floor plan is displayed, click the **Floor Plan** link immediately above the floor plan controls.
- 2 Identify the floor plan you wish to remove, and click the **delete** icon next to the floor plan name.
- 3 If you wish to remove an entire building containing all the floor plans, click the **delete** icon next to the building name.



Dashboard

This chapter contains the following sections:

- [About Dashboard, page 39](#)
- [Adding a Widget, page 40](#)
- [Modifying a Widget, page 40](#)
- [Deleting a Widget, page 40](#)
- [Modifying the Dashboard Layout, page 41](#)

About Dashboard

The **Dashboard** page in the Cisco FindIT Network Probe 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:

- **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
- **Traffic** widget—Displays a graph of the traffic flowing through the selected interface
- **Wireless Top Ten** widget – Displays the top ten wireless networks, access points, or clients based on traffic or client count

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 **enable edit mode** icon provided on the top right of the dashboard window.
 - Step 2** Click **add new widget** icon. Select the type of widget to add from the pop-up list. The new chosen widget appears in the dashboard.
 - Step 3** Click and hold the **change widget location** icon to drag the new widget to the desired location in the dashboard.
 - Step 4** Click the **save changes** icon at the top right of the dashboard window to preserve the changes.
-

Modifying a Widget

-
- Step 1** Click the **enable edit mode** icon provided on the top right of the dashboard window.
 - Step 2** Use the drop-down lists within the new widget to select a specific device, interface or network to be monitored.
Note For the **Device Health** widget, the devices are listed in the widget display.
 - Step 3** Click the **edit widget configuration** icon in the top right of the widget to modify the behavior of the widget.
 - Step 4** Click the **save changes** icon at the top right of the dashboard window to preserve the changes.
-

Deleting a Widget

-
- Step 1** Click the **enable edit mode** icon provided on the top right of the dashboard window.
 - Step 2** Click the **remove widget** icon at the top right of the widget to be removed.
 - Step 3** Click the **save changes** icon at the top right of the dashboard window to preserve the changes.
-

Modifying the Dashboard Layout

You can customize the dashboard layout and assign a name for the newly customized dashboard.

-
- Step 1** Click the **enable edit mode** icon provided on the top right of the dashboard window.
 - Step 2** Click the **edit dashboard** icon and select your preferred layout from the pop-up. Each option in the pop-up includes a diagram showing the layout of the widget containers for that option.
 - Step 3** Click the **change widget location** icon in the top right of each widget to move the widget into a different widget container. Click and hold to drag the widget into the new container. Each container can hold multiple widgets.
 - Step 4** Click the **save changes** icon at the top right of the dashboard window to preserve the changes.
-



Port Management

This chapter contains the following sections:

- [About Port Management, page 43](#)

About Port Management

Port Management provides a front panel view of each device that includes switch ports that may be configured by the FindIT Network Probe. 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 port 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.

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) macro may be applied. These macros 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 that port in the **Physical** view of **Port Management**. 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, and 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
- **EEE**—The EEE panel allows you to manage the Energy Efficient Ethernet (EEE) configuration for the port

To view the Smartport information for a port, click on that port in the **Smartports** view of **Port Management**. The **Basic Info** panel for the port appears, showing the following panels:

- **General** —The General panel shows the current Smartport configuration and status
- **Smartports**—The Smartports panel shows the Smartports roles available for this port. Click on a role to apply that configuration to the port



System Configuration

This chapter contains the following sections:

- [About System Configuration, page 45](#)
- [Using the Wizard, page 45](#)
- [Configuring Time Settings, page 46](#)
- [Configuring DNS Resolvers, page 46](#)
- [Configuring Authentication, page 47](#)

About System Configuration

The **System Configuration** page allow you to define various system level parameters that typically apply to all devices in the network. These parameters include configuration such as time settings, domain name services, and administrator authentication. 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 then 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 **Time Management**, **DNS Resolvers**, and **Authentication** and assign those profiles to one or more device groups in a single workflow.

Using the Wizard

- 1 Navigate to **System Configuration > Wizard**.
- 2 In the **Group Selection** screen, enter a description for this configuration, 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 Settings

The **Time Settings** 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 Settings Configuration Profile

- 1 Navigate to **System Configuration > Time Settings**.
- 2 Click the **+**(plus) icon to add a new profile.
- 3 On the **Device Group Selection** section, enter a description for this configuration, 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 Settings 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 Settings 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 **System Configuration > DNS Resolvers**.
- 2 Click the **+**(plus) icon to add a new profile.
- 3 On the **Device Group Selection** section, enter a description for this configuration, 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 **System Configuration > Authentication**.
- 2 Click the **+** (plus) icon to add a new profile.
- 3 On the **Device Group Selection** section, enter a description for this configuration, 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.



Network Configuration

This chapter contains the following sections:

- [About Network Configuration, page 49](#)
- [Configuring VLANs, page 49](#)
- [Configuring Wireless LANs, page 50](#)

About Network Configuration

The **Network Configuration** page allows you to define Virtual LANs (VLANs) and Wireless LANs (WLANs) for your network. Having multiple VLANs and WLANs in your network allows you to divide the network into multiple logical networks based on business needs rather than physical topology. This can help enhance both the performance and security of your network. Each WLAN must be associated with a VLAN, but a single VLAN can have any number of WLANs associated with it.

Configuring VLANs

The **Virtual LAN** 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 Probe also displayed in a separate table

Creating a Virtual LAN

- 1 Navigate to **Network > Virtual LAN**.
- 2 Click the **+**(plus) icon to add a new VLAN.
- 3 Specify a descriptive name for the VLAN, and the VLAN ID to be used. The VLAN ID should be a number in the range 1-4095, and should not already be in use in the network.
- 4 Select one or more device groups from the drop-down list. The new VLAN will be created on all VLAN-capable devices in the selected groups.
- 5 Click the **save** icon.

Modifying a VLAN

- 1 Check the check box next to the VLAN to be changed, and click the **edit** icon.
- 2 Make the required changes to the VLAN settings and click the **save** icon.

Removing a VLAN

Check the check box next to a VLAN or multiple VLANs 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 LAN** 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 Probe also displayed in a separate table.

Creating a Wireless LAN

- 1 Navigate to **Network > Wireless LANs**.
- 2 Click the **+**(plus) icon to add a new WLAN.
- 3 Specify a descriptive name for the WLAN, 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.
- 4 Optionally change the **Enable**, **Broadcast**, **Security** and **Radio** settings to match your requirements.
- 5 Depending on the security mode selected – **Enterprise** or **Personal** – specify either the RADIUS server to be authenticated against, or a pre-shared key.
- 6 Select one or more device groups from the drop-down list. The new WLAN will be created on all devices with wireless access point capabilities in the selected groups.
- 7 Click the **save** icon.

Modifying a Wireless LAN

- 1 Check the check box next to the WLAN to be changed, and click the **edit** icon.
- 2 Make the required changes to the WLAN settings and click the **save** icon.

Removing a Wireless LAN

You can select a single check box or choose multiple check boxes to select multiple WLANs to be removed, and then click the **delete** icon.

**Note**

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

Removing a Wireless LAN Not Created By the Probe

In the table of discovered Wireless LANs, click the **delete** icon next to the WLAN or choose multiple check boxes to select multiple WLANs to be removed. 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.



Reports

This chapter contains the following sections:

- [About Reports, page 53](#)
- [Viewing the Summary Report, page 54](#)
- [Viewing the End of Life Report, page 54](#)
- [Viewing the Maintenance Report, page 55](#)
- [Viewing the Wireless Network Report, page 56](#)
- [Viewing the Wireless Client Report, page 58](#)

About Reports

Cisco FindIT Network Probe generates a series of reports about your network devices. These reports include the following:

- **Summary Report**—Provides a high level view of the summary of the network devices
- **End of Life**—Shows any devices that have an End of Life bulletin published
- **Maintenance Report**—Lists all devices, the warranty status, and specifies if 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

The **Search** box located at the top of each 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. The results displayed in the table are updated automatically as you type.

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

Viewing the Summary Report

The **Summary 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 11: Summary Report

Field	Description
Hostname	The hostname of the device.
Model	The model number of the device.
Device Type	The type of device.
Firmware Update Available	Displays the latest firmware version available for the device, or states that the device firmware is currently up to date.
Current 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.

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 12: End of Life Report

Field	Description
Product ID	The product ID or part number of the device.
Name	The hostname of the device.

Field	Description
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.

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 13: Maintenance Report

Field	Description
Device Type	The type of device.
Host Name	The hostname of the device.
Model	Model number of the device.

Field	Description
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.

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. Daily or weekly reports may be generated using the controls at the top of the page. Up to seven days of data is retained on the Probe.

The following table describes the information provided:

Table 14: Wireless Network Report

Field	Description
Wireless Networks Table	
Network	The SSID or name of the network
Security	The type of security applied to the network
Guest	Whether the network is configured for guest access
Client Count (Peak)	The maximum number of clients attached to the network during the period covered by the report
Client Count (Average)	The average number of clients attached to the network during the period covered by the report
Traffic (Peak)	The maximum aggregate traffic rate through the network during the period covered by the report
Traffic (Average)	The average aggregate traffic rate through the network during the period covered by the report

Field	Description
Spectrum Usage Table	
Radio Freq	The radio frequency band in use – either 2.4GHz or 5GHz
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
Model	The model of the access point
Version	The firmware version running on the access point
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	
MAC	The MAC address of the rogue access point
Networks	The SSID detected
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

Field	Description
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 that detected the rogue access point

Viewing the Wireless Client Report

The **Wireless Client Report** shows details about the wireless clients on the network. Daily or weekly reports may be generated using the controls at the top of the page. Up to seven days of data is retained on the Probe.

The following table describes the information provided:

Table 15: Wireless Client Report

Wireless Clients Table	
MAC	The MAC address of the client
Network	The SSID with which the client is associated
802.11 Type Frequency	The 802.11 variant and frequency band used by the client
Data Rate [Byte/S]	The data rate last used by the client
Upload [Mb]	The volume of data uploaded by the client
Download [Mb]	The volume of data downloaded by the client
Total [Mb]	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
Wireless Guests Table	
MAC	The MAC address of the client

Wireless Clients Table	
Username	The username entered by the client in the guest portal
Network	The SSID the client is associated with
802.11 Type Frequency	The 802.11 variant and frequency band used by the client
Data Rate [Byte/S]	The data rate last used by the client
Upload [Mb]	The volume of data uploaded by the client
Download [Mb]	The volume of data downloaded by the client
Total [Mb]	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



Troubleshooting

This chapter contains the following sections:

- [About Troubleshooting, page 61](#)
- [Capturing Network Diagnostic Information, page 61](#)

About Troubleshooting

The **Troubleshooting** page in the FindIT Network Probe provides tools to help diagnose problems in the network.

Network Show Tech is one such tool which allows you to easily capture diagnostic information for your network and send it to a support engineer for analysis. For more details, see [Capturing Network Diagnostic Information, on page 61](#).

Capturing Network Diagnostic Information

The **Network Show Tech** page allows you to easily capture diagnostic information for your network in a form which you can analyze later or send to a support engineer. To capture diagnostic information, do the following:

- 1 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
- 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.



Administration

This chapter contains the following sections:

- [About Administration, page 63](#)
- [Managing Device Groups, page 64](#)
- [Managing Device Credentials, page 65](#)
- [Setting Up CAA Credential, page 66](#)
- [Managing Users, page 66](#)
- [Managing Site Information, page 67](#)
- [Connecting to the Manager, page 67](#)
- [Managing Email Settings, page 67](#)
- [Managing Log Settings, page 68](#)
- [Managing Platform Settings, page 69](#)
- [Backing Up and Restoring the Probe Configuration, page 70](#)

About Administration

The **Administration** page in the FindIT Network Probe allows you to manage the Probe software. The following pages consists of options to perform various administration tasks:

- **Device Groups**—Allocate network devices into groups for easy management
- **Device Credentials**—Enter credentials to be used when accessing network devices
- **CAA Credentials**—Specify the credentials to use for Cisco Active Advisor
- **User Management**—Manage the fallback user
- **Site Information**—Specify the location and other details about the site
- **Manager Connection**—Associate the Probe with a FindIT Network Manager
- **Email Settings**—Setup email for the Probe

- **Log Settings**—Manage system logging for the Probe
- **Platform Settings**—Manage network configuration for the Probe
- **Backup & Restore**—Backup and restore the Probe configuration

Managing Device Groups

FindIT Network Probe 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.

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 a name and a description for the group.
- 4 Use the drop-down list to select devices to be added to the group. 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.
- 5 Click the **save** icon.

Modifying the Device Group

To change an existing Device Group, do the following:

- 1 Navigate to **Administration > Device Groups > .**
- 2 Check the check box next to the group to be changed and click the **edit** icon
- 3 Change the name and description as required.
- 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.



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.

- 5 Click the **save** icon.

Deleting a Device Group

To delete a Device Group, do the following:

- 1 Navigate to **Administration > Device Groups**.
- 2 You can select a single check box or choose multiple check boxes to select multiple groups to be removed, and then click the **delete** icon.



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

Managing Device Credentials

For FindIT Network to fully discover and manage the network, the Probe must have 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**.
- 2 Under the **Add New Credential** heading, you will see a status message telling you the total number of devices discovered and how many require credentials. You may click on this message to display a table listing the discovered devices and whether each device has a valid credential.
- 3 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

- 4 Click **Apply**. The Probe 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.
- 5 Repeat steps 2 to 4 as necessary until every device has valid credentials stored.

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

- 1 Click the red **✘** 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 credentials, you may click the **Show Password** button. To hide the credentials again, click the **Hide Password** button. 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**.

Setting Up CAA Credential

Cisco Active Advisor (CAA) is a free online service that automates network discovery and analysis of your network inventory. Cisco Active Advisor reduces the overall risk of your network administration by keeping you up-to-date on the following:

- Warranty and service contract status
- Product advisories, including Product Security Incident Response Team notices (PSIRTs) and field notices
- End-of-Life milestones for hardware and software

You can view the reports in a web based interface and setup alerts.

FindIT Network Management allows you to easily upload your discovered devices to CAA by selecting the **Upload to CAA** action in the **Discovery** page. You may store your CAA credentials to simplify this process by removing the need to enter the credentials each time you upload data. To setup your CAA credentials, do the following:

- 1 Navigate to **Administration > CAA Credential**.
- 2 Enter your user name, password and confirm password in the appropriate fields provided. Your CAA credential is normally the same as your *Cisco.com* credential.
- 3 Click **Save** to save the credentials or **Reset** to enter a different set of credentials.

Managing Users

The **User Management** page allows you to manage the fallback user that can access the Probe when the Manager is unreachable, and also allows you to implement password complexity requirements for that user.

When the FindIT Network Probe is first installed, a default fallback user is created with the username and password both set to cisco.

**Note**

This menu option is not present when the Probe is collocated on the same host as the Manager

Modifying the Fallback User

To modify the fallback user, do the following:

- 1 Navigate to **Administration > User Management**
- 2 Change the user name and the password as required
- 3 Click **OK**

Changing password complexity

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

- 1 Navigate to **Administration > User Management**
- 2 Modify the **Local User Password Complexity** settings as required.

Managing Site Information

The Site Information page allows you to identify the site this Probe is located at and to specify the geographic location of the site. This information is used by FindIT Network Manager when displaying information from this Probe. To set the identity and location, do the following:

- 1 Navigate to **Administration > Site Information**.
- 2 Enter an identifying name for the site in the **Name** field.
- 3 Enter the address of the site in the fields provided. You can enter a partial address in the first **Location** field and hit enter, and the map will update to show the location specified. You can then click on the map to specify the desired location.
- 4 Click **Save**.

Connecting to the Manager

To establish an association between the **Probe** and a **Manager**, do the following:

- 1 Navigate to **Administration > Manager Connection**.
- 2 Enter the DNS name or the IP address of the manager into the field provided.
- 3 Click **Connect**. The login screen for the Manager is displayed.
- 4 Log in using valid credentials for the Manager. This authenticates the Probe to the Manager and establishes the association.

**Note**

This menu option is not present when the Probe is collocated on the same host as the Manager.

Managing Email Settings

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

Table 16: 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: <ul style="list-style-type: none"> • None • TLS • SSL
Authentication	The authentication method to use. Options include the following: <ul style="list-style-type: none"> • None • Clear text • MD5
Username	The username to present if authentication is enabled.
Password	The password to present if authentication is enabled.
Send Email to 1	The first email address to send notifications to.
Send Email to 2	The second email address to send notifications to.
From Email Address	The email address to originate messages from.

To test the configuration, click the **Test Connectivity** button. This will generate a test email to the recipients specified.

Managing Log Settings

The **Log Settings** page controls 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 which helps the support engineer to provide the desired settings. The settings available include the following parameters:

Table 17: Log Settings

Field	Description
Log Level	<p>The level of detail that should be logged. The following options are available:</p> <ul style="list-style-type: none"> • 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	<p>The module(s) for which messages should be logged. The following options are available:</p> <ul style="list-style-type: none"> • All (default)—All modules • System—Core system process not covered by any other module • Discovery—Device discovery events and topology discovery • Monitor—Dashboard activity • NETCONF—NETCONF and RESTCONF processes • Device configuration—All device configuration activity • Report—Data retrieval and correlation for report generation • Show tech—Data collection and processing for Network Show Tech • Administration—Probe configuration and management operations • Call-home Agent—Communication between the Probe and Manager <p>You may select multiple modules as needed.</p>

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 61 section.

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

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

- 1 Navigate to **Administration > Platform Settings**.

- 2 Specify a hostname for the Probe in the field provided.
- 3 Click **Save**.

Changing Network Settings

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

- 1 Navigate to **Administration > 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 Probe. To adjust the system clock, do the following

- 1 Navigate to **Administration > Platform Settings**.
- 2 Select the appropriate timezone for the Probe.
- 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 the **Clock** icon to synchronise 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.

Backing Up and Restoring the Probe Configuration

The configuration and other data used by the Probe can be backed up for disaster recovery purposes, or to allow the Probe 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 **Administration > Backup & Restore**.
- 2 Enter a password to encrypt the backup in the **Password** and **Confirm Password** fields in the **Backup** box.
- 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 Probe, do the following:

- 1 Enter the password that was used to encrypt the backup in the **Password** field of the **Restore** box.
- 2 Click **Upload & Restore** to upload the backup file from your PC and restore the settings to the Probe.



CHAPTER 12

Notifications

This chapter contains the following sections:

- [About Notifications, page 73](#)
- [Supported Notifications, page 73](#)
- [Viewing and Filtering Current Device Notifications, page 74](#)
- [Viewing and Filtering Historical Device Notifications, page 76](#)

About Notifications

The FindIT Network Probe 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 home page, 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 log by default.

Supported Notifications

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

Table 18: 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

Event	Level	Description	Clears Automatically?
Reachability/Device Offline	Alert	A device is no longer detectable on the network	Yes, when the device is rediscovered
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	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	An End of Life bulletin is found for the device.	No
Maintenance Expiry	Warning	The device is out of warranty and does not have a currently active maintenance contract.	Yes, if a new maintenance contract is taken out

Viewing and Filtering Current Device Notifications

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

Step 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.

If notifications have occurred, they are listed below the icons in the **Notification Center** dialog box. 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)

Step 2 In the **Notification Center** dialog box, 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

Step 3 Click **Filter** icon to open the **Filter** panel. Specify the details as described in the following table:

Table 19: Filter Panel

Field	Description
Severity Level	<p>The severity level of the notifications to be displayed. It can be one of the following:</p> <ul style="list-style-type: none"> • --All Levels-- • Information • Warning • Alert <p>You may include higher severity levels by selecting the Higher checkbox</p>
Notification Type	<p>The event type of the notifications to be displayed. For example, to display notifications for devices that are offline, choose Device Offline from the drop-down list.</p>
Device	<p>The device for which the notifications are displayed.</p>
<p>Check the check box against Include Acknowledged Events in the window to display all notifications that have been acknowledged.</p>	

Step 4 Select the **Settings** tab to control how you receive notifications. You can check the check box against the appropriate option such as **Popup Notification** or **Email** for an event type. Based on these settings, the system will generate a pop-up and/or send an email when a notification occurs. Click **Save** to save the settings or click **Restore Defaults** to restore the default settings.

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

Viewing and Filtering Historical Device Notifications

A log of historical notifications is stored on the Manager, and may be viewed through the Event Log. See the *Cisco FindIT Network Manager Administration Guide* for more information. A subset of historical event information is retained on the Probe and 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.

To filter the events shown on the **Device Detail** panel, do the following:

- 1 In the **Topology** map, click on a network device such as a switch or a router for which you want to view a detailed information.
- 2 In the **Basic Info** panel, click the **three dot** icon at the upper right corner, then select the **Events** tab.
- 3 Click **Filter** icon to open the **Filter** panel. Specify the details as described in the following table:

Table 20: Device Detail – Events Filter Panel

Field	Description
Display Events From: To:	The time and date range for which the events are to be displayed.
Severity Level	<p>The severity level of the events to be displayed. It can be one of the following:</p> <ul style="list-style-type: none"> • --All Levels-- • Information • Warning • Alert <p>You may include higher severity levels by selecting the Higher checkbox</p>
Event Type	The type of the events to be displayed. Available events include both device notifications and actions, arranged in a tree structure. Selecting a higher-level branch of the tree automatically includes all the lower level branches. Multiple events may be selected by holding down the shift key. For example, to display offline events, select the Notifications/Reachability/Offline branch.

- 4 Click **Filter**.



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, page 77](#)
- [Discovery FAQs, page 77](#)
- [Configuration FAQs, page 78](#)
- [Security Consideration FAQs, page 79](#)
- [Remote Access FAQs, page 81](#)
- [Software Update FAQs, page 82](#)

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 21: 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
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
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 22: 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.

Port	Direction	Protocol	Usage
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.
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.
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@findit-manager:~$ finditmgr recoverpassword
Are you sure? (y/n) y
Recovered the cisco account to default password
recoverpassword FindIT Manager successful!
cisco@findit-manager:~$
```



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 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.

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 Management, 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 log out 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 Probe 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.