



Cisco FindIT Network Manager Administration Guide

First Published: 2016-09-08

Last Modified: 2016-11-08

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: <http://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. (1110R)



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

© 2016 Cisco Systems, Inc. All rights reserved.



CONTENTS

CHAPTER 1

Cisco FindIT Network Management Overview 1

About Cisco FindIT Network Management 1

Audience 2

Terminology 2

System Requirements for Cisco FindIT Network Manager 3

CHAPTER 2

Getting Started with Cisco FindIT Network Manager 5

Installing Cisco FindIT Network Manager 5

Performing the Initial Setup 6

CHAPTER 3

Using Cisco FindIT Network Manager 9

Using the Cisco FindIT Network Manager GUI 9

CHAPTER 4

Network Map 13

About the Network Map 13

CHAPTER 5

Reports 15

About Reports 15

Viewing the Summary Report 15

Viewing the EoX Report 16

Viewing the Maintenance Report 17

CHAPTER 6

Administration 19

About Administration 19

Managing Users 19

Changing Passwords 20

Backing Up and Restoring the Manager Configuration 20

Managing Platform Settings 21

CHAPTER 7

Frequently Asked Questions 23

General FAQs **23**

Discovery FAQs **24**

Port Management FAQs **24**

Configuration FAQs **24**

Security Consideration FAQs **25**

Remote Access FAQs **27**

Software Update FAQs **28**



Cisco FindIT Network Management Overview

This chapter contains the following sections:

- [About Cisco FindIT Network Management](#) , page 1
- [Audience](#), page 2
- [Terminology](#), page 2
- [System Requirements for Cisco FindIT Network Manager](#), 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. In a single site network, you may choose to run a standalone instance of FindIT Network Probe, but if your network comprises multiple sites, you may install FindIT Network Manager at a convenient location and associate each Probe 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 **Manager**, 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)
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 Manager

Cisco FindIT Network Manager is distributed as a virtual machine image. To run FindIT Network Manager, 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

- CPU: 1x 64-bit Intel architecture
- Memory: 2GB
- Disk space: 20GB

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

- Apple Safari version 9
- Google Chrome version 52
- Microsoft Edge version 38
- Microsoft Internet Explorer version 11
- Mozilla Firefox version 48

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



CHAPTER 2

Getting Started with Cisco FindIT Network Manager

This chapter contains the following sections:

- [Installing Cisco FindIT Network Manager, page 5](#)
- [Performing the Initial Setup, page 6](#)

Installing Cisco FindIT Network Manager

FindIT Network Manager is provided as a virtual machine image, packaged in both the Distributed Management Task Force's **Open Virtualization Format (OVF)**, and as a zipped **Microsoft Hyper-V** virtual machine. Each of these deployment instructions are discussed in the following sections:

Installing using VirtualBox

- 1 Download the FindIT Network Manager 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 Manager 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 Manager 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 directory on your PC when asked for the location of the virtual machine
- 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

Performing the Initial Setup

There are a few configuration tasks that should be performed to ensure that the Manager meets your requirements.

Configuring Basic System Settings

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

- 1 Connect to the console of the Manager using the appropriate tools for your Hypervisor
- 2 Log in 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. When prompted, enter the password for the cisco account. 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 Manager. The hostname is used to identify the Manager 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.
- 6 Finally, you will be prompted to configure the time settings for the Manager. You may opt to configure one or more NTP servers for time synchronization (recommended), and you will be asked to select the timezone.

You may change these settings at any time by re-running the script, or through the web interface at **Administration > Platform Settings**.

Launching the Manager User Interface

- 1 Launch a web browser, such as Microsoft Internet Explorer or Mozilla Firefox.
- 2 In the **Address** field, enter the IP address of the Manager and press **Enter**
- 3 Enter the default user name: `cisco` and password: `cisco`. Click **Login**.
- 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.

The FindIT Network Manager user interface is displayed.

Creating Users and Changing Passwords

The Manager is initially set up with a single, default username and password.

To add new users, do the following:

- 1 Navigate to **Administration > User Management**
- 2 Click on the plus sign at the top of the **Local Users** table
- 3 In the **Add User** window that appears, specify the username and password to use. Also specify whether this user is an Administrator or Operator. Administrators have access to all functionality, while Operators do not have access to the **User Management** functions.
- 4 Click **OK** to create the new user

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

To change your password, do the following:

- 1 Navigate to **Administration > Change Password**
- 2 In the boxes provided, enter your current password, and the new password.
- 3 Click **Save**

Setting Up Licenses

License checking has not been implemented in the current version of FindIT Network Management. However, it is the user's responsibility to ensure that they possess sufficient licenses for the number of network devices being managed. Consult the FindIT Network Manager datasheet at www.cisco.com/go/findit for further details.

Reviewing Network Map

The Network Map provides you with a high-level view of your network. To access the network map, perform the following steps:

- 1 Make sure you have associated your FindIT Network Probes with the Manager as described in the *FindIT Network Probe Administration Guide*.
- 2 Click **Network Map** in the Manager navigation panel

- 3 You may click and drag the map to reposition it, and use the plus and minus buttons to zoom in and out
- 4 Each site with a FindIT Network Probe installed will be displayed as an icon on the map. Each icon contains a number showing the number of outstanding notifications for that site, and the color of the icon shows the highest severity level outstanding. Click on an icon to see more details about that site.
- 5 When you click on a site icon, the **Basic Info** panel appears showing you more information about that site. This information includes the site name and address, and a list of outstanding notifications for the site.
- 6 You may click on the globe icon in the **Basic Info** panel to open the user interface for the FindIT Network Probe at that site in a new window. Your connection to the Probe passes through a secure tunnel between the Probe and the Manager. See [Security Consideration FAQs](#) for more information on security.



CHAPTER

3

Using Cisco FindIT Network Manager

This chapter contains the following sections:

- [Using the Cisco FindIT Network Manager GUI, page 9](#)

Using the Cisco FindIT Network Manager GUI

Home window

Figure 1: Cisco FindIT Network Manager Home Page

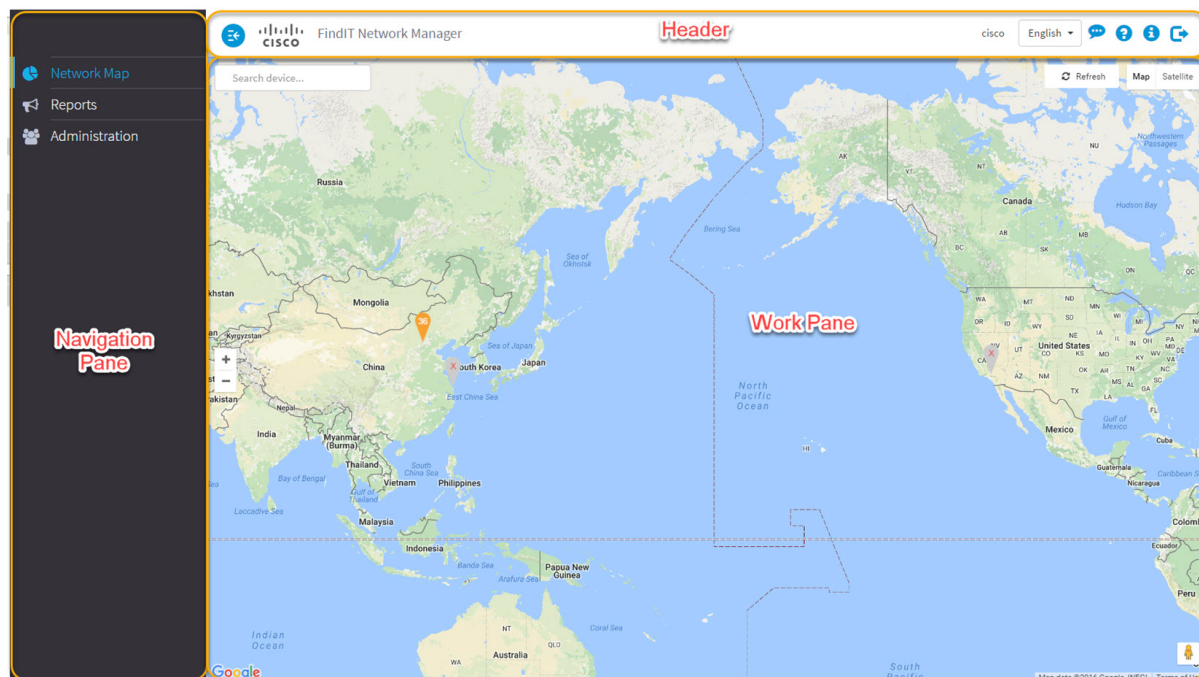





Table 1: Cisco FindIT Network Manager Home Page

Name	Description
Navigation pane	Provides access to the Cisco FindIT Network Manager features.
Work pane	Area where the feature interface is displayed. When you click an option in the Navigation pane, its corresponding window opens in this area.
Header toolbar	The header toolbar contains the following options: <ul style="list-style-type: none"> • A toggle button for expanding and collapsing the navigation pane • Header text including the site name of the Manager • 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 Manager features.


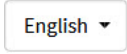




Table 2: Navigation Pane Options

Icon	Name	Description
	Network Map	Displays a geographic map showing the location and status of each site in the network
	Reports	Under the Reports heading, you will find a number of reports that provide life-cycle information about your network devices, including end of life bulletins, warranty information and service contract details.
	Administration	The Administration pages allow you to maintain the FindIT Network Manager.

Header Toolbar Options

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

Table 3: Header Toolbar Options

Icon	Option	Description
	Toggle button	Located on the top left of the header—This toggle button helps to expand or collapse the navigation pane.
	Language Selection	This drop-down list allows you to select the language for the user interface.
	Feedback	Click to provide feedback about your experience using the Cisco FindIT Network Manager and any suggestions for improvements.
	Help	The online-help documentation for FindIT Network Manager.
	About FindIT	The version information for FindIT Network Manager.
	Logout	Click to log out of FindIT Network Manager.



Network Map

This chapter contains the following sections:

- [About the Network Map, page 13](#)

About the Network Map

The **Network Map** provides a geographic map showing the location and status of each site in the network. The number displayed on each site icon indicates the number of outstanding notifications that exist for that site, and the color of the icon indicates the highest severity level outstanding. To see more information about a site, click on the site icon.

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

- **Search** box—Enter all or part of a device name, IP address, serial number or MAC address to locate that device in the network. As you type, a list of matching devices is displayed. Hover over a device and the corresponding site will be highlighted. Select a device and the corresponding site will be selected and centered in the view.
- **Zoom** controls—Use these controls to zoom in and out of the map. Click the (+) plus sign to zoom in and the minus sign to zoom out.
- **Map/Satellite** controls—Use these controls to select your preferred view - a map, or aerial imagery

You may also click and drag anywhere in the map area to move the map in the **Work** pane. Clicking on a site icon brings up the **Basic Info** panel for that site. The **Basic Info** panel contains the following information:

- Site name as defined in the Probe located at that site
- The Probe IP address for the site
- The physical address of the site
- The connection status
- A count of the outstanding notifications for the site and a list of the ten most recent notifications

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

- Click the globe icon to open the Probe user interface which displays the **Probe** installed at the site in a new window. The connection to the **Probe** is tunneled through the Manager, so no additional firewall rules are required at the site to allow access.
- Click on the **Actions** button to display additional actions available for the site, and then click **Remove** to delete this site and all associated data from the manager.



Reports

This chapter contains the following sections:

- [About Reports, page 15](#)
- [Viewing the Summary Report, page 15](#)
- [Viewing the EoX Report, page 16](#)
- [Viewing the Maintenance Report, page 17](#)

About Reports

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

- **Summary Report**—Provides a summary of the status of the devices in the network
- **EoX Report**—Shows any devices that have an End of Life bulletin published
- **Maintenance Report**—Lists all devices and their warranty state and whether the device has an active support contract

The **Search** box located at the top of each report can be used to filter the results. Enter a text in the **Search** box and click the **search** icon 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 then use the checkboxes 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 4: Summary Report

Field	Description
Site Name	The name of the site in which the device is located.
Hostname	The hostname of the device.
Device Type	The type of device.
Firmware Version	Displays the current firmware version running on the device.
Firmware Update Available	Displays the latest firmware version available for the device, or states that the device firmware is currently up to date.
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 EoX Report

The **EoX 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 5: EoX Report

Field	Description
Product ID	The product ID or part number of the device.
Name	The hostname of the device.
Device Type	The type of device.
Current Status	The stage at which the End of Life process of the product is at.
Date of Announcement	The date the End of Life bulletin was published.

Field	Description
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 6: Maintenance Report

Field	Description
Name	The hostname of the device.
Device Type	The type of device.
Model	Model number of the device.
Serial Number	The serial number for the device.
Status	The current support status of the device.
Coverage End Date	The date at which the current support contract will expire.

Field	Description
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.



Administration

This chapter contains the following sections:

- [About Administration, page 19](#)
- [Managing Users, page 19](#)
- [Changing Passwords, page 20](#)
- [Backing Up and Restoring the Manager Configuration, page 20](#)
- [Managing Platform Settings, page 21](#)

About Administration

The **Administration** option in the FindIT Network Manager allows you to manage the **Manager** software. This option is broken up into a number of pages:

- **User Management**—Define user access to FindIT Network Manager
- **Change Password**—Change the password for the currently logged in user
- **Backup & Restore**—Backup and restore the configuration and other data for the **Manager**
- **Platform Settings**—Manage network configuration for the Manager

Managing Users

The **User Management** page allows you to define users that can access FindIT Network, and also allows you to implement password complexity requirements for those users.

FindIT Network supports two types of users: **admin** and **operator**. An admin has full access to the FindIT Network features, while an operator can do everything except managing users. When the FindIT Network Manager is first installed, a default admin user is created with the username and password both set to `cisco`.

Adding a New User

To add a new user, do the following:

- 1 Navigate to **Administration > User Management**.
- 2 Click the **+**(plus) icon to create a new user.
- 3 In the fields provided, enter a username, password, and specify the user type.
- 4 Click **OK**.

Modifying a User

To modify an existing user, do the following:

- 1 Navigate to **Administration > User Management**.
- 2 Select the radio button for the user to be changed, and then click the **edit** icon.
- 3 Change the user type and the password as required.
- 4 Click **OK**.

Deleting a User

To delete an existing user, do the following:

- 1 Navigate to **Administration > User Management**
- 2 Select the radio button for the user to be deleted, and click the **delete** icon. You will see a notification confirming your action.

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.

Changing Passwords

To change the password for the currently logged in user, do the following:

- 1 Navigate to **Administration > Change Password**.
- 2 Specify the current password, new password, and confirm your new password in the appropriate fields.
- 3 Click **Save**.

Backing Up and Restoring the Manager Configuration

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

To perform a backup, do the following:

- 1 Navigate to **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**. A popup window will appear showing the progress of the backup. Larger systems may require some time to complete the backup, so you may dismiss the progress meter and display it again later with the **View Status** button.

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

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

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

Managing Platform Settings

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

- 1 Navigate to **Administration > Platform Settings**.
- 2 Specify a hostname for the Manager in the field provided.
This hostname is used to identify the Manager when generating Bonjour advertisements
- 3 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.
- 4 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
- 5 Click **Save**



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 23](#)
- [Discovery FAQs, page 24](#)
- [Port Management FAQs, page 24](#)
- [Configuration FAQs, page 24](#)
- [Security Consideration FAQs, page 25](#)
- [Remote Access FAQs, page 27](#)
- [Software Update FAQs, page 28](#)

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/>)

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 address range(s). It uses a combination of passive monitoring of certain network protocols and actively querying network devices for information.

Port Management FAQs

Q. Why doesn't **Port Management** show stack ports?

A. The **Port Management** illustrations are drawn based on the list of ports provided by the device via the management protocols. When in stacking mode, the stack ports are considered to be an internal connection within the stack, so are not included by the device in the lists provided via the management protocols.

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 7: FindIT Network Manager - Protocols and Ports

Port	Direction	Protocol	Usage
TCP 22	Inbound	SSH	Command-line access to Manager
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 9443	Inbound	HTTPS	Remote access to Probe GUI
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 8: FindIT Network Manager - Protocols and Ports

Port	Direction	Protocol	Usage
TCP 22	Inbound	SSH	Command-line access to Probe
TCP 80	Inbound	HTTP	Web access to Manager. Redirects to secure web server (port 443)
TCP 443	Inbound	HTTPS	Secure web access to Manager
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 or Manager and running the **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@FindITProbe:~# recoverpassword
Are you sure? (y/n) y
Reset the cisco account to default password
cisco@FindITProbe:~#
```

## 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 logout the session.
- Q.** Why does my remote access session fail with an error like the following?
- A. 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. The Manager uses the CentOS Linux distribution for an operating system. The packages and kernel may be updated using the standard CentOS processes. For example, to perform a manual update, log on to the console as the cisco user and enter the command `sudo yum -y update`. The system should not be upgraded to a new CentOS release, and no additional packages should be installed beyond those included in the virtual machine image supplied by Cisco.

### Q. How do I update Java on the Manager?

- A. Updates to Java should be download from Oracle and manually installed using the following commands:

To download a new Java package directly to the Manager:

```
curl -L -O -H "Cookie: oraclelicense=accept-securebackup-cookie"
-k http://download.oracle.com/otn-pub/java/jdk/<version>-<build>/jre-<version>-linux-x64.rpm
```

For example:

```
curl -L -O -H "Cookie: oraclelicense=accept-securebackup-cookie"
-k "http://download.oracle.com/otn-pub/java/jdk/8u102-b14/jre-8u102-linux-x64.rpm"
```

To install the updated Java version:

- 1 Remove the old version with the command `sudo yum -y remove jre1.8.0_102`
- 2 Install the new version with the command `sudo yum -y localinstall jre-<version>-linux-x64.rpm`

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

- A. The Probe uses OpenWRT for an operating system. Included packages may be updated using the `opkg` tool. For example, to update all packages on the system, log on to the console as the cisco user and enter the command `update-packages`. When necessary, kernel updates will be provided by Cisco as part of a new version of the Probe. No additional packages should be installed beyond those included in the virtual machine image supplied by Cisco.