Cisco FindIT Network Manager Administration Guide, Version 1.1.x

First Published: 2017-08-14

Last Modified: 2018-10-19

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 NONINFRINGEMENT 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.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

CONTENTS

CHAPTER 1

Cisco FindIT Network Management Overview

This chapter contains the following sections:

About Cisco FindIT Network Management

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

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

System Requirements for Cisco FindIT Network Manager

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

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: 2x 64-bit Intel architecture
    - Memory: 4GB
    - Disk space: 20GB

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

- Ubuntu version 16.04.x (Xenial Xerus)
- CPU: 2x 64-bit Intel architecture
- Memory: 4GB
- Disk space: 20GB

To run FindIT Network Manager in AWS, you will need an AWS account.

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 (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

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

Cisco FindIT Network Manager is distributed as a virtual machine image, as an installer for use with the Ubuntu Linux distribution, and is available for Amazon Web Services (AWS) through the AWS Marketplace (*https://aws.amazon.com/marketplace*). 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 virtual machine image also contains the FindIT Network Probe application, allowing a single VM to act as both Manager and Probe for a particular site. Each of these deployment options 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.

Installing using Ubuntu

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

Installing from the AWS Marketplace - 1-click Launch

Note This option is only available for Cisco FindIT Network Manager (BYOL).

1. Log on to your AWS account and navigate to the AWS Marketplace at *https://aws.amazon.com/marketplace*.
2. In the search box, search for Cisco FindIT Network Manager. Choose Cisco FindIT Network Manager (BYOL).

   The BYOL option requires Cisco Smart Licensing to operate, and is functionally identical to the other deployment models for FindIT Network Manager.
3. As 1-click Launch is only available for the BYOL option, click **Subscribe** for Cisco FindIT Network Manager (BYOL). Select **1-click Launch** and fill in the form as required based on your use of AWS. In particular, the VPC and Security Group chosen should allow for access by all the FindIT Network Probes that are deployed.

4. Click **Launch with 1-click**. The instance may take a few moments to initialize. Refer to the AWS EC2 console to see the status of the instance.

Installing from the AWS Marketplace - Manual Launch

You may install the AWS Marketplace using either of the following options:

- Cisco FindIT Network Manager (BYOL)—The BYOL option requires Cisco Smart Licensing to operate, and is functionally identical to the other deployment models for FindIT Network Manager.
- Cisco FindIT Network Manager (Metered)—The Metered option allows you to purchase licenses through Amazon Web Services. License usage is calculated hourly based on the number of devices being managed and charged to your AWS account each month.

Note The Metered option does not support integration with third-party RMM systems.

1. Log on to your AWS account and navigate to the AWS Marketplace at *https://aws.amazon.com/marketplace*.
2. In the search box, search for Cisco FindIT Network Manager. Choose either Cisco FindIT Network Manager (BYOL) or Cisco FindIT Network Manager (Metered).
3. Click **Subscribe** for your preferred deployment model and select **Manual Launch**. Click **Launch with EC2 Console** for your preferred region. Using the wizard, configure the instance as required based on your use of AWS. In particular, the VPC and Security Group chosen should allow for access by all the FindIT Network Probes that is deployed.
4. Click **Review & Launch**. Verify the instance has been configured correctly and then click **Launch**. The instance may take a few moments to initialize. Refer to the AWS EC2 console to see the status of the instance.

Removing FindIT Network Manager from Ubuntu

To remove FindIT Network Manager and all its dependencies from an Ubuntu system but retain the Manager'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-manager` and follow the prompts.

To completely remove FindIT Network Manager, its dependencies and configuration from an Ubuntu 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-manager` and follow the prompts.

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 on the VM Image or AWS instance

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 if using a virtual machine, or by connecting to your AWS instance using SSH
2. If using a virtual machine, log in using the default username and password set to: `cisco`. For an AWS instance, use the key pair you specified when the instance was created, and the username: `cisco`.

   You will be required to change the password for the cisco account immediately after logging in. The new password should be a complex, non-dictionary word using a mixture of character types.

   Your password must contain 8 characters that contains, 1 number, 1 upper case or 1 lower case, and 1 special character.
3. Enter the command `sudo finditmgr 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.

Note This step is not available with FindIT Network Manager for AWS

5. Next you will be prompted to change the web server ports. If these ports are changed from the default values, it may also be necessary to change firewall settings in your network, or security group settings in AWS.
6. 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.

Note This step is not available with FindIT Network Manager for AWS. To modify the network configuration, use the EC2 console in AWS.

7. 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 **Google Chrome** or **Microsoft Edge**.
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`. If you are using FindIT Network Manager for AWS, the default password is the instance ID. You can view the instance ID in the AWS EC2 console. .
4. Click **Login**. You will be prompted to change the password for the cisco account. Ensure that the new password is at least 8 characters in length contains 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) icon at the top of the **Local Users** table.
3. In the **Add User** window displayed, specify the username and password to use. Also, specify whether this user is an Administrator, Operator or Readonly.
   Administrators have access to all functionality, while Operators do not have access to the **User Management** functions. Read only users may not make any configuration changes and have only limited access to the Administration menus.
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**.

Disabling the Embedded Probe on the VM Image

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

The virtual machine image for the Manager includes the Probe software for managing devices on the network local to the Manager. If you do not wish to manage the local network, you may disable the embedded Probe using the following steps:

1. Navigate to **Administration** > **Local Probe**.
2. Click the toggle switch to disable the embedded Probe.

3. Click **Save**.

Setting Up Licenses

Note This does not apply to the metered version of FindIT Network Manager for AWS.

FindIT Network Manager is licensed to use Cisco Smart Licensing. When first installed, the Manager is set to Evaluation Mode. Evaluation Mode allows up to ten network devices to be managed without restriction, and allows 90 days to obtain licenses if more than ten devices are being managed. To apply purchased licenses to the system, you must associate the Manager with a Cisco Smart Account containing sufficient FindIT licenses for your network.

To associate the Manager with your Smart Account, perform the following steps:

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

The Manager will register with Cisco Smart Licensing and request sufficient licenses for the number of network devices being managed. If there are insufficient licenses available, a message will be displayed on the user interface, and you will have 90 days to obtain sufficient licenses before system functionality is restricted. For more details on the licensing process, see Managing Licenses, on page 37.

Learn About Your Network

This page shows a high-level view of your network as either a map or a list of sites. To view the network, 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 Overview** in the Manager navigation panel. Click the button to display either the **Map View** or the **List View**.
3. In **Map View**, you may click and drag the map to reposition it, and use the plus and minus buttons to zoom in and out. 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.

   In **List View**, you can click the icon at the top left corner of the table to select the columns to be displayed, and you can click on the column headings to sort the table.

4. Use the Search box to find a specific site or to find the site that contains a particular device. You may enter the name, address or IP address of a site in the Search box, or the name, IP address, MAC address or serial number of a device.

5. When you click on a site, 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 the Security Consideration Security Consideration FAQs for more information on security.

Setting Up Network Plug and Play

FindIT Network Manager provides a Cisco Network Plug and Play server that allows you to centrally manage firmware and configuration files for selected Cisco devices. For more information about Network Plug and Play, see *https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Plug-and-Play/solution/guidexml/b_pnp-solution-guide.html*.

To set up Network Plug and Play, perform the following tasks.

Upload Firmware

1. Navigate to **Network Plug and Play** > **Images**.

2. Click the ✚(plus) icon.

3. Drag a firmware file from your PC and drop it on the target area of the **Upload File** window. Alternatively, click the target area and select a firmware image to upload.

4. Click **Upload**.

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

1. Select the checkbox for the image in the **Images** table and click **edit**.

2. Enter a comma-separated list of product IDs into the **Default Image for Product IDs** field. Product IDs can contain the wildcard characters ‘?’, representing a single character, and ‘*’, representing a string of characters.

3. Click **save**.

Upload Configurations

1. Navigate to **Network Plug and Play** > **Configurations**.

2. Click the ✚(plus) icon.

3. Drag a configuration file from your PC and drop it on the target area of the **Upload File** window. Alternatively, you can click on the target area and select a configuration file to upload.

4. Click **Upload**.

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

Setting up Discovery

In order for network devices to use **Network Plug and Play**, they first need to discover the **Network Plug and Play** server. There are three mechanisms that may be used to provide this information to the devices:

1. **DHCP**: The network device can learn the address of the Network Plug and Play server using DHCP option 43. For more detail on the option format, see About Network Plug and Play, on page 19.
2. **DNS**: If the network device does not learn the server address through DHCP, it will attempt to lookup up a well-known hostname, pnpserver, in the local domain – e.g *pnpserver.example.com*. You may configure your DNS infrastructure to ensure that this name resolves to the address of the FindIT Network Manager.
3. **Plug and Play Connect**: Cisco provides a redirection service, **Plug and Play Connect**, that the device will query if it is not able to find the address of the server any other way. To set up the redirection service for your network, please refer to *https://www.cisco.com/c/en/us/buy/smart-accounts/plug-play-connect.html*

Registering Devices

To register devices in preparation for installation, do the following:

1. Navigate to **Network Plug and Play** > **Projects**.
2. Enter the name of an existing project in the search box, or type the name of a new project and click **Create Project** .
3. Enter the name, product ID (PID) and serial number of the device to be registered and click **Add New**.
4. Select the checkbox for the newly created device and click **edit**.
5. You may select either or both of a firmware image and configuration file to use for this device. If you choose Default image as the image, the device will use the image designated as the default for that device type at the time the device connects to the server.
6. Click **save**.

Auto Claiming Devices

A device that connects to the server when that device has not been registered with the server is considered to be an unclaimed device. Unclaimed devices may be automatically claimed and provisioned by the server by creating an Auto Claim rule for that product ID. To create an Auto-Claim rule, do the following:

1. Navigate to **Network Plug and Play** > **Auto Claim Devices**.
2. Enter the product ID (PID) to automatically claim and click **Add New**.
3. Select the checkbox for the newly created rule and click **edit**.
4. You may select either or both of a firmware image and configuration file to use for this product ID. If you choose Default image as the image, auto claimed devices will use the image designated as the default for that device type at the time the device connects to the server.
5. Click **save**.

CHAPTER 3

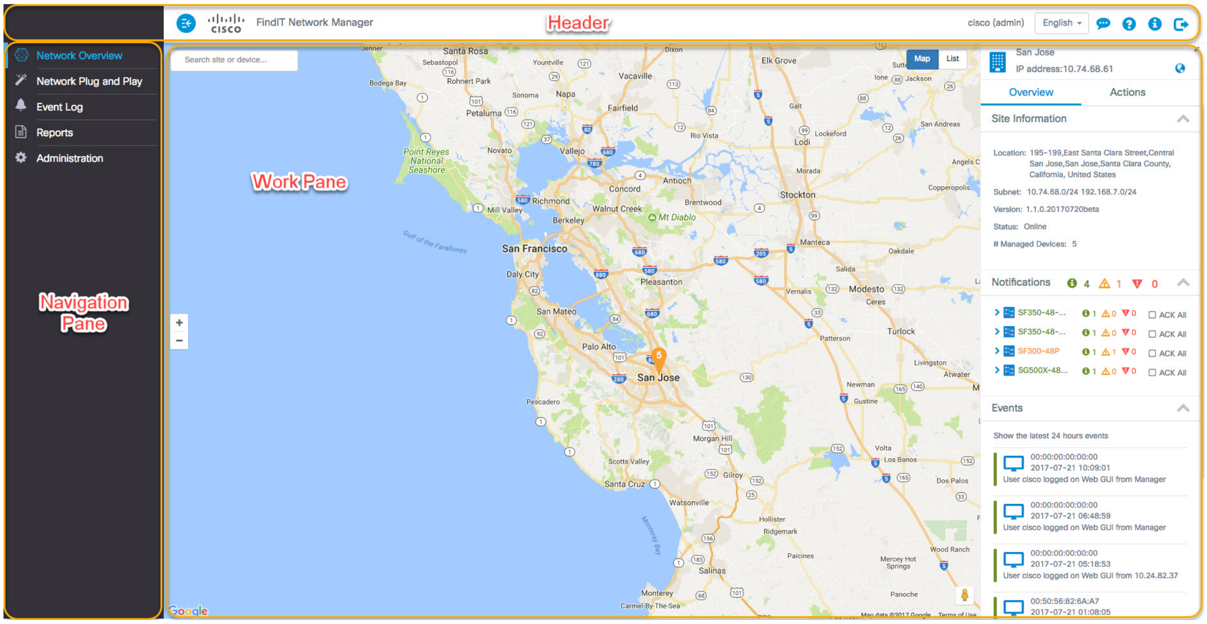
Using Cisco FindIT Network Manager

This chapter contains the following sections:

Using the Cisco FindIT Network Manager GUI

Home window

Figure 1: Cisco FindIT Network Manager Home Page



San Jose
IP address:10.74.68.61

Site Information

Location: 195-199,East Santa Clara Street,Central San Jose,San Jose,Santa Clara County, California, United States
Subnet: 10.74.68.0/24 192.168.7.0/24
Version: 1.1.0.20170720beta
Status: Online
Managed Devices: 5

Notifications 4 1 0

SF350-48-...	1	0	0	□ ACK All
SF350-48-...	1	0	0	□ ACK All
SF300-48P	1	1	0	□ ACK All
SG500X-48...	1	0	0	□ ACK All

Events

Show the latest 24 hours events

00:00:00:00:00:00
2017-07-21 10:09:01
User cisco logged on Web GUI from Manager

00:00:00:00:00:00
2017-07-21 06:48:59
User cisco logged on Web GUI from Manager

00:00:00:00:00:00
2017-07-21 05:18:53
User cisco logged on Web GUI from 10.24.82.37

00:50:56:82:6A:A7
2017-07-21 01:08:05

Table 1: Cisco FindIT Network Manager Home Page

Name	Description
Navigation pane	Provides access to the Cisco FindIT Network Manager features.

Name	Description
Work pane	Area where the feature interface is displayed. When you click an option in the **Navigation** pane, its corresponding window opens in this area.
Header toolbar	The header toolbar contains the following options: • A toggle button for expanding and collapsing the navigation pane • Header text 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 Overview**	Displays an overview of the network as either a map or a list.
🪄	**Network Plug and Play**	Network Plug and Play enables zero-touch deployment of network devices, allowing them to automatically download firmware and configuration files from FindIT Network Manager at the time of install.
🔔	**Events**	The Events page provides a list of all the events that have occurred in the network, and allows you to use filters to limit the results to only events of interest.
📄	**Reports**	Under the Reports heading, you will find a number of reports that provide life-cycle information about your network devices, including end of life bulletins, warranty information and service contract details.
⚙	**Administration**	The Administration pages allow you to maintain the FindIT Network Manager.

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.
English ▾	**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.
ℹ	**About FindIT**	Click on this icon to see information about FindIT Network Manager, including the current version. If a new version is available, a badge will be displayed on the icon, and a link to apply the update will be available in the popup.
⇨	**Logout**	Click to log out of FindIT Network Manager.

Upgrading FindIT Network Manager

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

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

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

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

To apply a Manager update manually, do the following:

1. Download the FindIT Network Manager Linux installer file by navigating to *www.cisco.com/go/findit* and selecting the Download Software for this Product link in the Support pane.

2. Copy the installer file to the Manager filesystem.

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

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

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

1. Click **About FindIT** to open the **About FindIT** popup. If updates are available for the Manager or any of the associated Probes, they will be listed here.

2. If an update is available for the Manager, perform that update before upgrading the probes. If you try to update the probes first, you will receive an error message.

3. Select the radio button next to the Probe update and click **Upgrade**.

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

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

1. If an update is available for the Manager, perform that update before upgrading any probes. If you try to update a probe before updating the Manager, you will receive an error message.

2. Select **Network Overview** in the navigation. Select the site to be updated in either the **Map View** or the **List View**.

3. In the **Basic Info** panel for the site, select the **Actions** tab.

4. Click **Upgrade**.

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

CHAPTER 4

Network Overview

This chapter contains the following sections:

- About the Network Overview, on page 17

About the Network Overview

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

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

- **Search** box—Enter all or part of the name, address or IP address of a site to locate that site in the network. Alternatively, enter all or part of the name, IP address, serial number or MAC address of a device to identify the site where the device is located. As you type, a list of matches is displayed. Hover over a match and the corresponding site will be highlighted. Select a match and the corresponding site will be selected and centered in the view.

- **Zoom** controls—Usethese controls to zoom in and out of the map. Click the ✚(plus)s sign to zoom in and the ━ (minus) sign to zoom out.

- **Map/Satellite** controls—Usethese 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.

In the List View, you can click the icon at the top left corner of the table to select the columns to be displayed, and you can click on the column headings to sort the table.

Clicking on a site icon or row 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 and the IP subnet(s) discovered at the site

- The physical address of the site

- The software version of the Probe

- The connection status
- The number of managed devices in this site
- A list of all current, unacknowledged notifications for this site
- A list of notifications that occurred for this site in the previous 24 hours

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.
  - Click **Remove** to delete this site and all associated data from the manager
  - Click **Upgrade** to update the Probe software at this site

CHAPTER 5

Network Plug and Play

This chapter contains the following sections:

About Network Plug and Play

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

Network Requirements

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

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

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

Setting up Discovery using DHCP

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

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

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

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

Setting up Discovery using DNS

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

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

Certificate Requirements

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

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

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

Setting up Discovery using Plug and Play Connect

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

Accessing the Plug and Play Connect Service

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

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

Creating a Controller Profile

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

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

2. Select the Controller Profiles link, and then click the Add Profile button.
3. Select a Controller Type of PNP SERVER from the dropdown list. Then click Next.
4. Specify a name, and optionally a description for the profile.
5. Under the heading for Primary Controller, use the dropdown provided to select whether to specify the server by name or IP address. Fill in the name or addresses of the server in the fields provided.
6. Select the protocol to use when communicating with the server. It is strongly recommended that HTTPS be used to ensure the integrity of the provisioning process.
7. If the protocol selected is HTTPS and the server is configured with a self-signed certificate (default) or one that is not signed by a well-known certificate authority, then the certificate used by the server should be uploaded using the controls provided. See Managing Certificates, on page 39 for details on downloading the certificate from the Manager.
8. Optionally specify a Secondary Controller.
9. Click **Next**, and review the settings before clicking **Submit**.

Registering Devices

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

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

Configuring the Network Plug and Play Service

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

Using the Dashboard

The **Network Plug and Play** Dashboard provides an overview of the devices currently being provisioned using Network Plug and Play. Three charts are displayed, showing device status broken down by project, by pre-configured devices assigned to any project, and by devices that are not assigned to a project. Each chart shows the number of devices or projects in each of the states listed. You may click on the state heading on any of the charts to see a detailed list of devices or projects that fall into that category.

Two search boxes are also provided at the top of the dashboard – one for projects, and one for devices. Type all or part of a project name in the projects search box and select the project of interest to display detailed information for that project. Similarly, you may enter a device name, product ID or serial number in the device search box to display the current status of an individual device.

Managing Projects

Projects allow you to group related devices for easier management. To create a new project, do the following:

1. Navigate to **Network Plug and Play** > **Projects**
2. Type the name of a new project in the **Project** field and click **Create Project**.

To add devices to a project in preparation for installation, do the following:

1. Navigate to **Network Plug and Play** > **Projects**.
2. Start typing the name of the project in the search box, and then select the project from the search results.
3. Enter the name, product ID (PID) and serial number of the device to be registered and click **Add New**.
4. Select the checkbox for the newly created device and click **edit**.
5. You may select either or both of a firmware image and configuration file to use for this device. If you choose **Default Image** as the image, the device will use the image designated as the default for that device type at the time the device connects to the server.
6. Click **save**.

To remove a device from a project, do the following:

1. Navigate to **Network Plug and Play** > **Projects**.
2. Start typing the name of the project in the search box, and then select the project from the search results.
3. Select the checkboxes for one or more devices and click **delete**.

To remove an entire project and all the device associated with that project, do the following:

1. Navigate to **Network Plug and Play** > **Projects**.
2. Start typing the name of the project in the search box, and then select the project from the search results.
3. Click **Delete Project**.

Device Firmware Images

The **Images** page allows you to upload firmware images that may then be deployed to the devices. Firmware images may be designated as the default image for different platforms, allowing you to update the firmware across an entire family of devices very easily.

To upload a firmware image, do the following:

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

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

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

To remove an image, do the following:

1. Navigate to **Network Plug and Play** > **Images**.
2. Select the checkboxes for one or more images in the **Images** table and click **delete**.

Device Configuration Files

The Configurations page allows you to upload configuration files that may then be deployed to the devices. To upload a configuration file, do the following:

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

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

To remove a configuration, do the following:

1. Navigate to **Network Plug and Play** > **Configurations**.
2. Select the checkboxes for one or more configuration files in the **Configurations** table and click **delete**.

Unclaimed Devices

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

1. Navigate to **Network Plug and Play** > **Unclaimed Devices** and select the **Unclaimed** tab.
2. Click the checkboxes for one or more devices.
3. Select either a configuration file or a firmware image, or both for each device.
4. Click **Claim**.

The devices will be moved to the **Claimed** list and provisioned with the configuration and image that you have specified.

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

1. Navigate to **Network Plug and Play** > **Unclaimed Devices** and select the **Unclaimed** tab.
2. Click the checkboxes for one or more devices.
3. Click **Ignore**.

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

1. Navigate to **Network Plug and Play** > **Unclaimed Devices** and select the **Ignored** tab.
2. Click the checkboxes for one or more devices
3. Click **Unignore**

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

Auto Claiming Devices

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

1. Navigate to **Network Plug and Play** > **Auto Claim Devices**.
2. Enter the product ID (PID) to automatically claim and click **Add New**.
3. Select the checkbox for the newly created rule and click **edit**.
4. You may select either or both of a firmware image and configuration file to use for this product ID. If you choose Default image as the image, auto claimed devices will use the image designated as the default for that device type at the time the device connects to the server.
5. Click **save**.

New devices that do not match an existing rule in a Project will be compared against the list of Auto Claim rules. If there is a match, the device will be added to the Claimed list with the image and configuration file defined by the Auto Claim rule. The device will then be provisioned according to those rules. If the device does not match an Auto Claim rule, it will be added to the Unclaimed list and no further action will be taken.

Managing Settings

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

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

Configuring the Certificate

The certificate automatically generated by FindIT Network Manager during first startup is a self-signed certificate with the IP address(es) of the Manager listed in the **Subject-Alt-Name** field. In most cases, this will not be sufficient for the certificate to be accepted by the Network Plug and Play client, and it will be necessary to generate a new certificate. When generating a new self-signed certificate or certificate signing request (CSR), the Manager will include the following identities in the **Subject-Alt-Name** field:

- The current IP address(es)
- The contents of the Common Name field
- The hostname that was used in the web browser to connect to the administration GUI

For more information on configuring the Manager’s certificate, see Managing Certificates, on page 39.

Monitoring Network Plug and Play

Each device known to the Network Plug and Play service is shown on either the **Project** page or the **Unclaimed Devices** page with a status displayed. The status field shows the current state of the device, and will contain one of the values as listed in the following table. By clicking on the status field, you can see more detail, including a history of the state changes for this device over time.

Table 4: Network Plug and Play - Device Status

Status	Description
PENDING	Device is defined but has not made contact with the service.
PROVISIONING	The device has made the initial connection to the service.
PROVISIONING_IMAGE	A firmware image is being applied by the device.
PROVISIONED_IMAGE_REBOOTING	The device is rebooting to run the new firmware.
PROVISIONED_IMAGE	New firmware has been applied successfully.
PROVISIONING_CONFIG	A configuration file is being applied to the device.
PROVISIONED_CONFIG	The configuration file has been successfully applied to the device. Depending on the type of device, it may reboot to apply the configuration.

Status	Description
ERROR	An error has occurred. Check log files for more details.
PROVISIONED	The provisioning process for the device is complete.

CHAPTER 6

Event Log

This chapter contains the following sections:

About the Event Log

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

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

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

CHAPTER 7

Reports

This chapter contains the following sections:

About Reports

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

- **Summary Report**—Provides a summary of the status of the devices in the network
- **End of Life Report**—Shows any devices that have an End of Life bulletin published
- **Maintenance Report**—Lists all devices and their warranty state and whether the device has an active support contract
- **API Usage Report** —Displays usage information for the integration interface with third-party RMM tools

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 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 5: Summary Report

Field	Description
Site Name	The name of the site in which the device is located.
Hostname	The hostname of the device.
Model	The model number 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 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 6: End of Life Report

Field	Description
Site Name	The name of the site in which the device is located.
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 7: Maintenance Report

Field	Description
Site Name	The name of the site in which the device is located.
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.
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 API Usage Report

The API Usage Report displays information about any external applications that have been integrated with the FindIT Network Manager. This report is broken up into the following four sections:

- The 15-minute Request Monitor—Displays the average and peak request rate over the last 15 minutes
- The Request History graph—Displays a graph of request activity over time. You may select time periods of the last four hours, the last seven days, or all available information. You may then use the sliders underneath the graph to narrow the focus of the graph to a particular period of interest.
- The Endpoints table—Lists all the endpoints that have requested event notifications for at least one network. The following table describes the information provided in the Endpoints table:

Table 8: The Endpoints Table

Field	Description
Endpoint	The callback URL to which the Manager should post event notifications
Username	The username presented by the application when authenticating to the Manager
Type	The type of application associated with this endpoint
Version	The version of the application associated with this endpoint
# Networks	The number of networks where the application has requested event notifications
# Managed Devices	The number of managed devices for which event notifications will be sent to this endpoint

- The Networks table—Lists the networks currently being monitored by an external application. The following table describes the information provided in the Networks table:

Table 9: The Networks Table

Field	Description
Network	The name of the network being monitored by an external application
# Managed Devices	The number of managed devices in this network for which event notifications will be sent

CHAPTER 8

Administration

This chapter contains the following sections:

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
- **License**—Manage software licensing for the Manager
- **Certificate**— Manage security certificates on the Manager
- **Backup & Restore**—Backup and restore the configuration and other data for the **Manager**
- **Platform Settings**—Manage network configuration for the Manager
- **Logging Settings**— Change log settings for the Manager
- **Local Probe**—Manage a Probe hosted on the Manager

The pages available are different for different user roles. Operators cannot manage user settings, and Readonly users will only see the **Change Password** page.

Managing Users

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

FindIT Network supports three types of users: **admin**, **operator** and **readonly**. An admin has full access to the FindIT Network features, while an operator can do everything except managing users. A readonly user can only view network information, they cannot make any changes.

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

Note User settings can be managed by admin users only.

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, display name, 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. Click **edit** next to the user to be changed.
3. Change the user type, display name and password as required.
4. Click **OK**.

Deleting a User

To delete an existing user, do the following:

1. Navigate to **Administration** > **User Management**
2. Click **delete** next to the user to be deleted, or select the checkboxes for multiple users and click **delete** at the top of the table. 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 session timeouts

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

1. Navigate to **Administration** > **User Management**.
2. Modify the **User Session Setting** parameters as required. Hover over the help icons to see allowable ranges for these parameters.

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**.

Managing Licenses

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

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

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

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

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

Registering the Manager to your Smart Account

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

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

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

Removing the Manager from your Smart Account

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

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

Immediately Check for Licenses

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

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

Renew Authorization Now

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

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

Renew Registration Now

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

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

Transfer the Manager to a Different Account

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

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

Managing Certificates

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

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

Generating a Certificate Signing Request (CSR)

To generate a CSR, do the following:

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

Uploading a New Certificate

To upload a new certificate, do the following:

1. Navigate to **Administration** > **Certificate**. Click **Update** next to the HTTPS Certificate label.

2. Select **Upload Cert** radio button. The file containing the certificate can be dropped on the target area, or you may click the target area to browse the file system. The file should be in PEM format.

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

3. Click **Upload** to upload the file and replace the current certificate.

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

Viewing the Current Certificate

To view the current certificate, do the following:

1. Navigate to **Administration** > **Certificate**. Click **View** next to the HTTPS Certificate label.
2. The certificate will be displayed in plain text format in your browser.

Downloading the Current Certificate

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

1. Navigate to **Administration** > **Certificate**. Click **Download** next to the HTTPS Certificate label.
2. The certificate will be downloaded in PEM format by your browser.

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

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

Changing the Hostname

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

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

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

Changing Port Settings

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

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

Changing Network Settings

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

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

1. Navigate to **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 Manager. To adjust the system clock, do the following:

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

2. Select the appropriate timezone for the Manager.

3. Select the method for time synchronization. The available options are **NTP (default)** and **Local Clock**. If the NTP option is chosen, then optionally modify the NTP servers to use for synchronization.

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

4. Click **Save**.

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

Managing Logging Settings

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

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

1. Navigate to **Administration** > **Logging Settings**.

2. Use the radio buttons to select the desired logging level for each software module

3. Click **Save**

The log files for the Manager may be found in the directory `/var/log/findit/manager/` on the local file-system.

Managing the Local Probe

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

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

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

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

CHAPTER 9

Frequently Asked Questions

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

General FAQs

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

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

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

Discovery FAQs

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

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

The protocols used include:

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

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

Q. How does FindIT discover my network?

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

Q. Does FindIT do network scans?

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

Configuration FAQs

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

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

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

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

Security Consideration FAQs

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

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

Table 10: FindIT Network Manager - Protocols and Ports

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

Port	Direction	Protocol	Usage
TCP 80	Inbound	HTTP	Web access to Manager. Redirects to secure web server (port 443)
TCP 443	Inbound	HTTPS	Secure web access to Manager
TCP 1069	Inbound	NETCONF/TLS	Communication between Probe and Manager
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 11: FindIT Network Probe - Protocols and Ports

Port	Direction	Protocol	Usage
TCP 22	Inbound	SSH	Command-line access to Probe. SSH is disabled by default on the Cisco virtual machine image.
TCP 80	Inbound	HTTP	Web access to Probe. Redirects to secure web server (port 443).
TCP 443	Inbound	HTTPS	Secure web access to Probe.
UDP 5353	Inbound	mDNS	Multicast DNS service advertisements from the local network. Used for device discovery.
TCP 10000 - 10100	Inbound	Device dependent	Remote access to devices.
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.

Port	Direction	Protocol	Usage
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 logout the session.

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

A. After doing many remote access sessions with different devices, the browser will have a large number of cookies stored for the 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 updated 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.