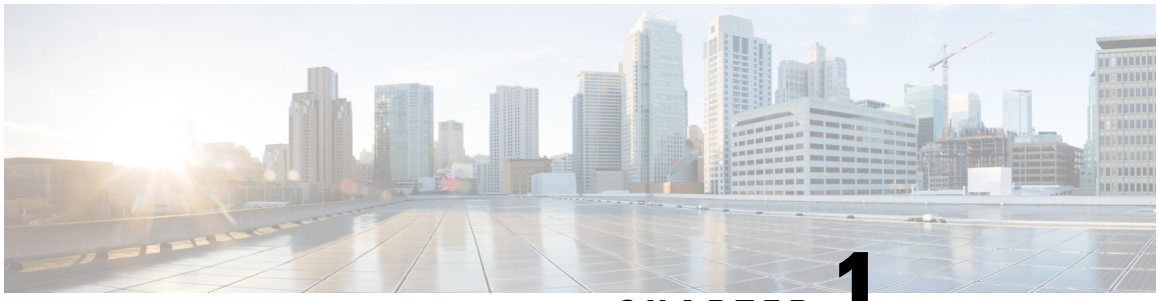
Cisco FindIT Network Manager and Probe Quick Start Guide, Version 2.1

First Published: 2020-03-05

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

CONTENTS



CHAPTER 1

Cisco FindIT Network Management Overview

This chapter contains the following sections:

About Cisco FindIT Network Management

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

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

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

Audience

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

Related Documents

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

- **Quick Start Guide (this document)**—This guide provides details on performing the initial setup for FindIT Network Manager & Probe using the most commonly selected options.
- **Installation Guides**

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

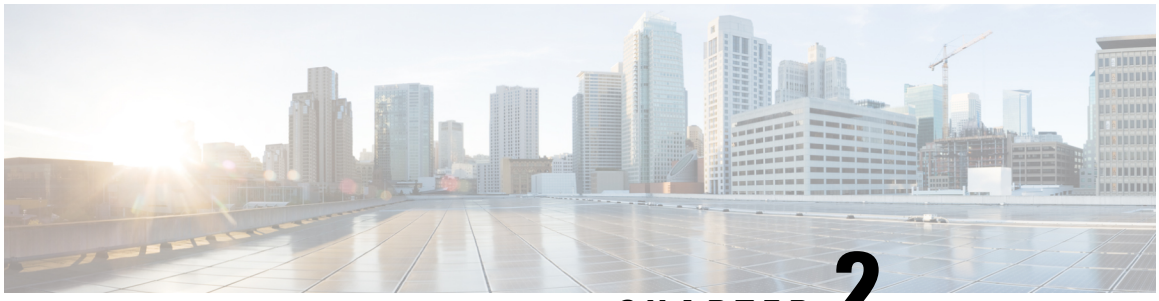
Supported Platforms	Location
Amazon Web Services	Cisco FindIT Network Manager & Probe Installation Guide for Amazon Web Services
Oracle VirtualBox	Cisco FindIT Network Manager & Probe Installation Guide for Oracle VirtualBox
Microsoft Hyper-V	Cisco FindIT Network Manager & Probe Installation Guide for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

- **Administration Guide**—This is a reference guide that provides details about all the features and options provided by the software and how they may be configured and used. Refer to Cisco FindIT Network Manager and Probe Administration Guide.

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/*.

Term	Description
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.



CHAPTER 2

Performing Initial Setup for the Manager

This chapter contains the following sections:

Performing Initial Setup for the Manager

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.
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.

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. Next, 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.

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

8. Finally, you will be asked if you wish to change the bootloader password. The bootloader username and password may be used on the console at system startup to change the system boot process or recover lost operating system passwords. The default bootloader credentials are username: **root** and password: **cisco**.

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 or hostname 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.
5. Click **Next**. You will be presented with information about how FindIT Network Manager uses your data and what information is shared with Cisco. Make any changes necessary and click **Finish**.

The FindIT Network Manager user interface is displayed.

Create Organizations (Optional)

Organizations are used in FindIT Network Manager to split networks, users, and devices into groups that are typically administered separately. Each network or device belongs to an organization, and each user can manage one or more organizations. An organization might represent a customer or a department or a region, but the use of organizations allows more granular control over who can manage the different parts of the network. A single organization is created by default when the Manager is installed.

To create a new organization, do the following:

1. Navigate to **Administration** > **Organizations**.
2. Click the ✚(plus) icon at the top of the table.

3. Specify a name for the organization and enter the required details.
4. Enter a name for a new device group that should be used as the default group for newly discovered devices. The new device group will be created along with the organization.
5. Click **Save**
6. Repeat steps 1 to 5 for each organization you wish to create.

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** > **Users**.
2. Click on the ✚(plus) icon at the top of the **Users** table.
3. In the **Add User** window displayed, enter the details of the user to be created. Specify whether this user is an Administrator, Org Administrator, Operator or Readonly. Following are the privileges provided depending on the type of user
   - Administrators have access to all functionality including system management
   - Org Administrators have access to all functionality across one or more organizations but do not have access to the System menus
   - Operators have access to all functions within their assigned organizations, but do not have the ability to manage users. They do not have access to System menus
   - Read only users may not make any configuration changes and have only limited access to the Administration menus and no access to the System menus.
4. Click **Save** to create the new user.

You may also set up password complexity restrictions on the **Users** page by selecting the **User Settings** tab. New passwords will be required to meet these restrictions.

To change your password, do the following:

1. At the top-right of the user interface, click on your user name to display the drop down menu an select **My Profile**. A page is displayed.
2. Click the Reset password link.
3. In the boxes provided, enter your current password, and the new password.
4. 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* in the *Cisco FindIT Network Manager and Probe Administration Guide*.

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 **System** > **Local Probe**.
2. Click the toggle switch to disable the embedded Probe.
3. Click **Save**.

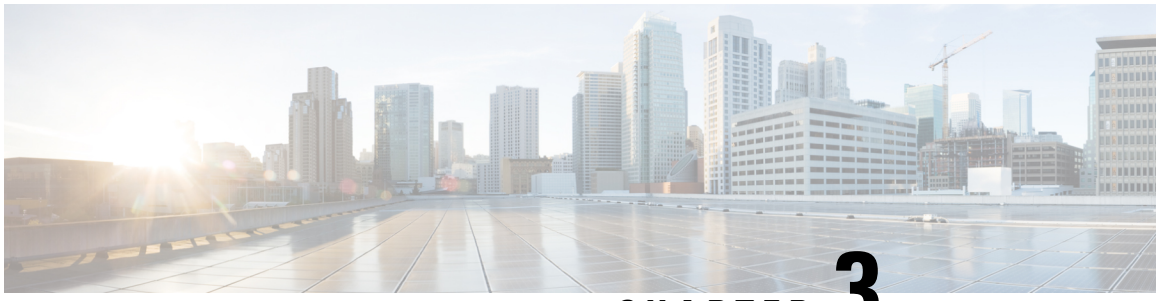
Create Networks (Optional)

You may pre-define network records in the Manager for Probes that you will associate later. Typically, each network represents a separate site, but you can have multiple networks in the same location. To create a new network, do the following:

1. Navigate to **Network**.
2. Click **Add Network** in the **Map View** or +(plus) icon in the **List View**.

3. Specific a name, organization and default device group for the network.
4. Enter the address of the network into the appropriate fields. If you enter a partial address, a list of potential matches will be displayed, and you can select the location from the list. Alternatively, you can click on the location in the map.
5. Click **Save**.
6. Repeat steps 1 to 5 for each network you wish to create.

Performing Initial Setup for the Manager



CHAPTER 3

Performing Initial Setup for the Probe

This chapter contains the following sections:

Performing Initial Setup for the Probe

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

Locating the IP Address of the Probe

To find the IP address being used by the probe, use one of the following methods:

1. The default IP address configuration for the Probe is performed using DHCP. Make sure your DHCP server is running and can be reached. If no DHCP server is available, the IP address will default to 192.168.1.10.
2. The Probe can be discovered and accessed using the **Cisco FindIT Network Discovery Utility** that enables you to automatically discover all supported Cisco devices in the same local network segment as your computer. You can get a snapshot view of each device or launch the product configuration utility to view and configure the settings. For more information, see http://www.cisco.com/go/findit.
3. The Probe is Bonjour-enabled and automatically advertises itself using the Bonjour protocol. If you have a Bonjour-enabled browser, you can find the Probe on your local network without knowing its IP address.
4. If you are using the virtual machine image, you can retrieve the IP address of the Probe from the virtual machine console. Use your Hypervisor's management tools to connect to the console of the virtual machine and log on with the default username: `cisco` and password: `cisco`. You will be required to change the password immediately after logging in. The new password should be a complex, non-dictionary word using a mixture of character types. A banner will then be displayed showing the current IP address.

   If you have installed the Probe on your own Ubuntu or Raspbian Linux installation, you may use the operating system tools to discover the IP address. For example, you may enter the command `ifconfig` at a shell prompt and see a list of interfaces and their addresses displayed.
5. Locate the IP address assigned by your DHCP server by accessing your router or DHCP server. See your DHCP server instructions for more information.

Setting Up a Software Probe

A software probe is a probe running in a virtual machine or on a Linux host when there is no manager application running on the same VM or host.

To set up a software probe, do the following:

1. Launch a web browser, such as **Google Chrome** or **Microsoft Edge**.
2. In the **Address** field, enter the DHCP-assigned IP address and click **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. Click **Save**.
5. Specify the address or hostname of a Manager to connect to and click **Next**.
6. Your browser will be redirected to the Manager login screen. Login using administrator credentials for the Manager, and then your browser will be redirected back to the Probe.
7. Choose to either create a new network or to select an existing network from the drop-down provided. If you choose to create a new network, then specify a name and location for the network in the boxes provided.

   You may enter the address of the network into the appropriate fields. If you enter a partial address, a list of potential matches will be displayed, and you can select the location from the list. Alternatively, you can click on the location in the map.
8. Click **Finish**.

Setting up an Embedded Probe on a Cisco 100 to 500 Series Product

The process for associating an embedded probe with a manager changed in version 2.1 from requiring user interaction to a process that requires explicit configuration on both the Manager and Probe prior to connecting. This process enables the device hosting the embedded probe to be pre-configured prior to installation, or to be automatically configured using a zero-touch deployment mechanism such as Network Plug and Play.

Note If your device is running a version 1.x embedded probe, then use the process described in Settings Up a Software Probe above

To set up a version 2.1 embedded probe, do the following:

1. Create a new network record for the embedded probe using the steps described in Performing Initial Setup for the Manager. Take note of the organization name and network name.
2. On the Manager UI, go to the **My Profile** page using the dropdown at the top right of the screen. Use this page to create a new **Access Key** using the **Generate Access Key** button. You may also use an existing access key if you prefer.

Note The access key used for associating an embedded probe with the manager does not need to be a long lived key. This key only needs to be valid at the time the initial association takes place. Once the probe and manager are associated, the connection is authenticated using limited access, short-lived credentials that are unique to the network and regenerated periodically.

3. Using the device UI, navigate to the FindIT Probe configuration page and fill out the fields provided. At the minimum, you will need to supply configuration for the manager address and port, organization name, network name, and access key ID and secret. It may also be necessary to configure the manager certificate. See below for more details. Optionally you may make other changes.
4. Submit the changes. The probe will connect to the manager and be associated with the network created in step 1.

When establishing a connection to the manager, the probe checks to ensure the certificate presented by the manager 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 added to the device configuration as a trusted certificate. Refer the device administration guide for details on adding a trusted certificate.
- If the manager is configured as an IP address, then either the Common Name field or the Subject-Alt-Name field of the certificate must contain that IP address
- If the manager is configured as a hostname, then either the Common Name field or the Subject-Alt-Name field of the certificate must contain that hostname

Configuring Basic System Settings on the VM image using Web User Interface (Optional)

To configure basic system settings such as IP addressing and time settings for the Probe using the web user interface, do the following:

1. Navigate to **Administration** > **Platform Settings**.
2. Specify a hostname for the Probe. The hostname is used to identify the Probe in Bonjour advertisements and in the FindIT Network Discovery Utility user interface.
3. Optionally, specify static IP parameters in the fields provided. By default, the Probe will automatically determine the IP settings using DHCP.
4. Alternatively, you can set the Probe to use its internal clock for keeping time, or you can specify your preferred NTP servers. By default, the Probe will synchronize its clock with public NTP servers.

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

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

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

1. Connect to the virtual machine console.
2. Log on using the default username and password set to: `cisco`. You will be required to change the password immediately after logging in. The new password should be a complex, non-dictionary word using a mixture of character types.

3. Enter the command `sudo config_vm` to perform the initial configuration. The `config_vm` utility will prompt you with a series of steps to change the platform settings.
4. First you will be prompted to change the hostname for the Probe. The hostname is used to identify the Probe in Bonjour advertisements and in the FindIT user interface. Choose a meaningful name here, or you may skip this step to keep the default hostname.
5. Next you will be prompted to 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.
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.
7. Next you will be prompted to configure the time settings for the Probe. You may opt to configure one or more NTP servers for time synchronization (recommended), and you will be asked to select the timezone.

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

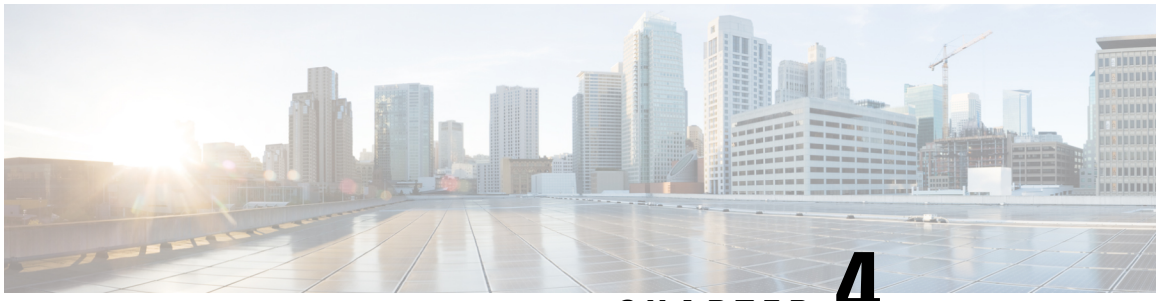
8. Finally, you will be asked if you wish to change the bootloader password. The bootloader username and password may be used on the console at system startup to change the system boot process or recover lost operating system passwords. The default bootloader credentials are username: **root** and password: **cisco**.

Configuring Basic System Settings when the Probe is Embedded on a Cisco 100 to 500 Series Product

If you are using a Probe embedded in a Cisco 100 to 500 series product, then the Probe user interface is accessed through the device administration interface. Consult the device administration guide for more information on associating the Probe with the Manager and making changes to system settings.

Configuring Basic System Settings when the Probe is Co-hosted with a Manager

A Probe that is co-hosted with a version 2.0 or higher Manager does not have any user interface. The Probe is managed entirely through the Manager user interface.



CHAPTER 4

Setting Up the Network

This chapter contains the following sections:

Setting Up the Network for Manager

Setting Up Device Credentials

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

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

1. Navigate to **Administration** > **Device Credentials**. The first table on this page lists all the devices that have been discovered that require credentials, while the second table lists all the discovered devices for which working credentials are known.
2. Enter a username and password combination and/or SNMP credentials in the respective fields at the top of the page. If more sets of credentials are required, then click the +(plus) icon. This allows up to three sets of each type of credential to be entered.
3. Click **Apply**. The Probes will test each credential against each device for which a credential is required. Working credentials are saved for each device.

   The Probes will discover each network and generate a topology map and inventory for the network after being provided with the working credentials.

Learn About Your Network

FindIT Network Manager provides a high-level view of your network as either a map or a list of networks. To see the high-level view of all networks, perform the following steps:

1. Make sure you have associated your FindIT Network Probes with the Manager as described in the earlier section.

2. Click **Network** 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 network 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 network, and the color of the icon shows the highest severity level outstanding. Click on an icon to see more details about that site. If multiple icons are too close to be easily distinguished, they will be replaced with a cluster marker showing the number of Network icons in that cluster. Click on the cluster marker to zoom in on the sites in that cluster.

   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 network or to find the network that contains a particular device. You may enter the name, address or IP address of a network in the Search box, or the name, IP address, MAC address or serial number of a device.
5. When you click on a network, the **Basic Info** panel appears showing you more information about that network. This information includes the network name and address, and a list of outstanding notifications for the network.
6. You may click **View** in the **Basic Info** panel to view a detailed information about that network, including the network topology diagram and floor-plans. Clicking **More** opens up the **Network Detail** view that allows you to modify settings for this network and view all the devices discovered in this network.

You may also use the **Inventory** to see detailed information about all the devices in your network. The **Inventory** page provides a list of all discovered devices in a tabular view. You can filter the list to restrict the devices displayed, and click on individual devices to see more information about that device.

Customizing the Topology Map (Optional)

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

1. Navigate to **Network** and select the network of interest. Click **View** to display the topology.
2. You may drag individual device icons to improve the layout. Any changes you make to the layout are permanent. FindIT Network Manager will not make further changes to the location of the icons. If you wish to re-enable automatic placement of icons, then click **Relayout Topology**.
3. Click **Overlays** to open the **Overlays and Filters** panel and use the check boxes to limit the device types that are displayed in the topology diagram.

Uploading Floor Plans (Optional)

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

1. When viewing the topology diagram for a network, click **Floor Plan**.
2. Enter a name for the building and the floor, and then either drag an image file into the drop zone or click inside the widget to select an image file on your PC. Image formats supported include `.png, .gif, .jpg`
3. Click **Save** to save the changes.

4. To place a device on the floor plan, click **Add Devices** and type the device name or IP address into the search box at the bottom of the screen. Matching devices will be displayed, where grayed out devices have already been placed on a floor plan.
5. Click and drag a device to add it to the floor plan in the correct location.

Customizing the Dashboard

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

1. Select **Dashboard** from the navigation at the left of the screen. The default dashboard will be displayed.
2. To relocate individual widgets within the dashboard, click on the gear icon at the top right of the dashboard and select the **Edit Mode** option. Click and hold to drag each widget to the desired location. To resize a widget, click and hold on the edge or corner of the widget to resize.
3. To add a new widget to the dashboard, click the gear icon at the top right of the dashboard and select to add a widget. Select the desired widget from the list. To remove a widget from the dashboard, click **remove widget ✖** icon in the top right corner of the widget when in edit mode.
4. Once the dashboard is laid out correctly, click the gear icon at the top right of the dashboard and select **View Mode** to lock the changes in place.
5. To change the behavior of a widget, click **edit widget configuration** icon in the top right of the widget. Use the drop down lists to select the specific device, interface or network the widget should monitor.

Configuring Email Settings (Optional)

FindIT Network Probe can notify you via email when selected events occur within the network. To control which events will generate an email see Customizing Notification Display, on page 17. To configure email settings, do the following:

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

Customizing Notification Display

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

1. Navigate to **Administration** > **Organizations** and select the organization where you want to customize notification behavior.
2. Click **Notification**
3. Unchecked the **Inherit from Notification Defaults** checkbox. Use the check boxes to control which notifications generate a pop-up alert in the user interface, and those that generate an email notification. If you use email notifications, you must ensure that the email settings are correctly configured. See Configuring Email Settings (Optional), on page 17 for more details.
4. Click **Save**.

You may also customize the **Notification Defaults** by navigating to **Administration** > **Notification Defaults**.

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, refer to the PnP Solution Guide.

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. Choose an organization and then 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. Choose an organization and then 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, refer to section, *About Network Plug and Play*, in the FindIT Network Manager & Probe Administration Guide, Version 2.0.

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—For example, *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 Plug & Play Connect

Registering Devices

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

1. Navigate to **Network Plug and Play** > **Enabled Devices**.
2. Click the ✚(plus) icon.
3. Enter the name, product ID (PID) and serial number of the device to be registered and select an organization, network, device group and device type from the dropdown lists.
4. 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.
5. Click **Save**.

Auto Claiming Devices

A device that connects to the server and is not present in the inventory 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. Click the ✚(plus) icon.
3. Enter the product ID (PID) to automatically claim and select an organization, network, device group and device type from the dropdown lists.
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**.

Configuring the Network

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

Updating Firmware for devices (Optional)

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

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

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

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

You may also upgrade individual devices from the **Inventory** view. For details, refer to section, *Viewing Device Inventory*, in the FindIT Network Manager & Probe Administration Guide, Version 2.0.

Updating Firmware for a Network

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

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

Configuring Device Groups

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

1. Navigate to **Administration** > **Device Groups**.
2. Click the ✚(plus) icon to add a new group.
3. Specify an organization, a name and description for the device group. Click **Save**.
4. To add devices to the device group, click the ✚(plus) icon in the **Devices** table. Use the search box to find devices to add to the group. Select one or more devices to join the group. Each device can only be a member of one group. If a selected device was previously a member of a different group, it will be removed from that group. If you wish to remove a device from the group, click the **Delete** icon next to the device, and the device will be moved to the **Default** device group. Device groups can contain a mixture of different device types.

Creating Configuration Profiles

The Manager allows you to easily apply common configuration to multiple network devices. You may use the **Network Configuration Wizard** to create configuration profiles for each section of the configuration, or you can create profiles individually. To use the **Network Configuration Wizard**, do the following:

1. Navigate to **Network Configuration** > **Wizard**.
2. Enter a profile name for the configuration profiles to be created, choose an organization and select one or more device groups to which the configuration will be applied.
3. Click **Next**.
4. Specify the time settings for this group. A **Time Management** profile contains settings for the timezone, daylight savings, and NTP. If you do not wish to create a **Time Management** profile for this group, click **Skip**, otherwise click **Next**.
5. Specify the **DNS settings** for this group. A **DNS Resolvers** profile contains settings for the domain name, and the DNS servers to use. If you do not wish to create a DNS Resolvers profile for this group, click **Skip**, otherwise click **Next**.
6. Specify the user authentication settings for this group. An **Authentication profile** contains settings for the local user database for the devices. If you do not wish to create an **Authentication profile** for this group, click **Skip**, otherwise click **Next**.
7. Specify the Virtual LANs to be created for this group. A VLAN profile contains the details for one or more VLANs. If you do not wish to create a VLAN profile, click **Skip**. To add multiple VLANs, click **Add Another** after completing each VLAN. Click **Next**.
8. Specify the Wireless LANs to be created for this group. A Wireless LAN profile contains the details for one or more SSIDs. If you do not wish to create a Wireless LAN profile, click **Skip**. To add multiple SSIDs, click **Add Another** after completing each SSID. Click **Next**.
9. Review the configuration settings you have made. If you wish to make changes, use **Edit** or **Back** to return to the appropriate screen. Once you are satisfied, click **Finish** to create the profiles and apply to the devices in the selected device groups.
10. You may view the progress of the configuration by clicking on the **Task Status** icon in the top right of the user interface.

Backing Up Device Configurations

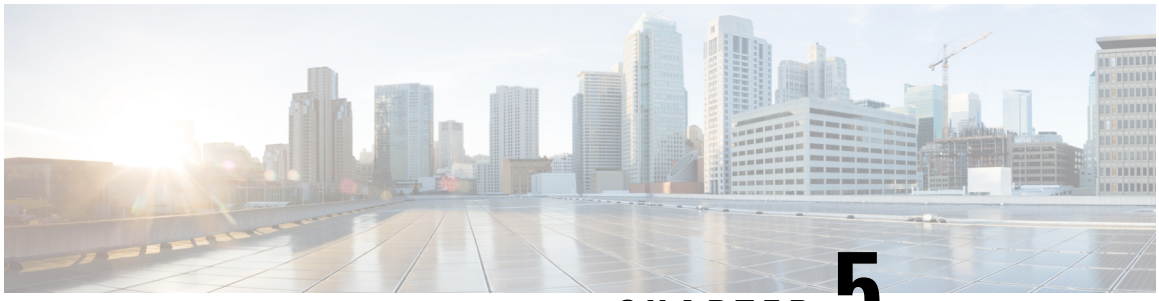
The Manager allows you to back up the configurations of your network devices. To back up the configuration for a single device, do the following:

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

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

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

1. Open the **Topology Map** for the network you wish to back up.
2. Click **Actions** button at the top of the page and select the **Backup Configurations** option. Optionally, add a note describing this backup in the window that appears. The Probe will copy the configuration of each device and store them on the Manager.
3. You may view the progress of the backup by clicking on the **Task Status** icon in the top right of the user interface.



CHAPTER 5

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 1: 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 Multiplexed TCP	Secure web access to Manager Communication between Probe and Manager with release 2.x
TCP 1069	Inbound	Multiplexed TCP	Communication between Probe and Manager with release 1.x. Used only in release 2.0 when release 1.x Probes are present.
TCP 50000 - 51000	Inbound	HTTPS	Remote access to devices
UDP 53	Outbound	DNS	Domain name resolution
UDP 123	Outbound	NTP	Time synchronization
TCP 443	Outbound	HTTPS Multiplexed TCP	Access Cisco web services for information such as software updates, support status, and end of life notices. Access OS and application update services.
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 2: 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.

Port	Direction	Protocol	Usage
TCP 10000 - 10100	Inbound	Device dependent	Remote access to devices. This range is only used by FindIT Network Probe version 1.x.
UDP 53	Outbound	DNS	Domain name resolution.
UDP 123	Outbound	NTP	Time synchronization
TCP 80	Outbound	HTTP	Management of devices without secure web services enabled.
UDP 161	Outbound	SNMP	Management of network devices.
TCP 443	Outbound	HTTPS Multiplexed TCP	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. Access OS and application update services. Communication between Probe and Manager with release 2.x
TCP 1069	Outbound	Multiplexed TCP	Communication between Probe and Manager. This range is only used by FindIT Network Probe version 1.x.
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.

Q. What is the default username and password for the Virtual Machine bootloader?

A. The default credentials for the Virtual Machine bootloader are username: **root** and password: **cisco**. These may be changed by running the config_vm tool and answering yes when asked if you want to change the bootloader password.

Remote Access FAQs

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

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

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

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

cookie is only valid for the most recently visited device. All other devices that use the same cookie name will see the cookie as being invalid and will logout the session.

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

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

Software Update FAQs

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

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

Q. How do I update Java on the Manager?

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

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

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

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

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