Cisco FindIT Network Management Frequently Asked Questions

Objective

The Cisco FindIT Network Management is a software that allows you to easily manage your whole network including your Cisco devices through your web browser. It automatically discovers, monitors, and configures all supported Cisco devices in your network. This software also sends you notification about firmware updates and information about the devices in your network that are no longer supported by warranty.

The Cisco FindIT Network Management has two separate components: a single Manager known as the FindIT Network Manager and one or more Probes known as the FindIT Network Probe.

This article contains the frequently asked questions in setting up, configuring, and troubleshooting the Cisco FindIT Network Management and their answers.

Frequently Asked Questions

Table of Contents

General

Discovery

Port Management

Configuration

Security Consideration

Remote Access

Software Update

General

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

FindIT Network Management is translated into the following languages:

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

Discovery

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

FindIT uses a variety of protocols to discover and manage the network. The exact protocol being used for a particular device varies depending on the device type. These protocols include:

- Multicast Domain Name System (mDNS) and DNS Service Discovery — This protocol is also known as Bonjour. It locates devices such as printers, other computers, and the services that those devices offer on a local network. To learn more about mDNS, click here. For more information on DNS Service Discovery, click here.

- Cisco Discovery Protocol (CDP) — A Cisco proprietary protocol used to share information about other directly connected Cisco equipment, such as the operating system version and IP address.
- Link Layer Discovery Protocol (LLDP) — A vendor neutral protocol used to share information about other directly connected equipment, such as the operating system version and IP address.
- Simple Network Management Protocol (SNMP) — A network management protocol used for collecting information and configuring network devices such as servers, printers, hubs, switches, and routers on an Internet Protocol (IP) network.
- RESTCONF — An Internet Engineering Task Force (IETF) draft that describes how to map a Yet Another Next Generation (YANG) data modeling language specification to a RESTful interface. To know more, click here.

3. How does FindIT discover my network?

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 and LLDP adjacency tables, Media Access Control (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.

4. Does FindIT do network scans?

FindIT does not actively scan the network address ranges. It uses a combination of passive monitoring of certain network protocols and actively querying network devices for information.

Port Management

5. Why doesn't Port Management show stack ports?

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

Configuration

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

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 also be applied to newly discovered devices.

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

Any Virtual Local Area Network (VLAN) or Wireless Local Area Network (WLAN) configuration associated with profiles that are currently applied to the original device group and are not applied to the new device group will be removed, and VLAN or WLAN configuration associated with profiles that are applied to the new group and 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

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

The following table contains the protocols and ports used by FindIT Network Manager:

Port	Direction	Protocol	Usage
TCP 22	Inbound	SSH	Command-line access to Manager
TCP 80	Inbound	HTTP	Web access to Manager. Redirects to secure web server (port 443)
TCP 443	Inbound	HTTPS	Secure web access to Manager
TCP 1069	Inbound	NETCONF/TLS	Communication between Probe and Manager
TCP 9443	Inbound	HTTPS	Remote access to Probe GUI
TCP 50000-51000	Inbound	Device dependent	Remote access to devices
UDP 53	Outbound	DNS	Domain name resolution
UDP 123	Outbound	NTP	Time synchronization
UDP 5353	Outbound	mDNS	Multicast DNS service advertisements to local network advertising the Manager

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

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

Port	Direction	Protocol	Usage
TCP 22	Inbound	SSH	Command-line access to Probe
TCP 80	Inbound	HTTP	Web access to Manager. Redirects to secure web server (port 443)
TCP 443	Inbound	HTTPS	Secure web access to Manager
UDP 5353	Inbound	mDNS	Multicast DNS service advertisements from the local network. Used for device discovery.
TCP 10000-10100	Inbound	Device dependent	Remote access to devices
UDP 53	Outbound	DNS	Domain name resolution
UDP 123	Outbound	NTP	Time synchronization
TCP 80	Outbound	HTTP	Management of devices without secure web services enabled
UDP 161	Outbound	SNMP	Management of network devices
TCP 443	Outbound	HTTPS	Management of devices with secure web services enabled. Access Cisco web services for information such as software updates, support, status,

			and end of life notices
TCP 1069	Outbound	NETCONF/TLS	Communication between Probe and Manager
UDP 5353	Outbound	mDNS	Multicast DNS service advertisements to the local network advertising the Probe

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

All communication between the Manager and the Probe is encrypted using a Transport Layer Security (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.

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

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 default username and password: cisco, or the default 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.

12. How secure are the credentials stored in FindIT?

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.

13. How do I recover a lost password for the Administration GUI?

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

```
cisco@FindITProbe:~# recoverpassword

Are you sure? (y/n) y

Reset the cisco account to default password

cisco@FindITProbe:~#
```

Remote Access

14. When I connect to the Administration GUI of a device from FindIT Network Management, is the session secure?

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.

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

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 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.

16. 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?

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

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

The Manager uses the CentOS Linux distribution for an operating system. The packages and kernel may be updated using the standard CentOS processes. For example, to perform a manual update, log on to the console as the cisco user and enter the command *sudo yum -y* update. The system should not be upgraded to a new CentOS release, and no additional packages should be installed beyond those included in the virtual machine image supplied by Cisco.

18. How do I update Java on the Manager?

Updates to Java should be downloaded from Oracle and manually installed using the following commands:

To download a new Java package directly to the Manager:

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

Below is an example:

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

To install the updated Java version:

Step 1. Remove the old version with the command *sudo yum -y remove jre1.8.0_102*

Step 2. Install the new version with the command *sudo yum -y localinstall jre-<version>-*

linux-x64.rpm

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

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

20. What is the Cisco FindIT Kaseya Plugin?

The Cisco FindIT Kaseya Plugin is designed to increase operational efficiency by tightly integrating Cisco FindIT Network Manager with the Kaseya Virtual System Administrator (VSA). The Cisco FindIT Kaseya Plugin offers powerful features including action management, dashboards, device discovery, network topology, remote device management, actionable alerts and event history.

The Plugin is designed to be extremely easy to install, requiring only a few clicks. It complies with all third-party integration requirements for Kaseya on-premise VSA versions 9.3 and 9.4. To learn more, click here.