

Release Notes for Cisco FindIT Network Manager & Probe, Version 2.0.0

First Published: 2019-07-01

Last Modified: 2019-07-18

Introduction

These release notes describe the recommended practices and known issues that apply to software version 2.0.0 of Cisco FindIT Network Manager and Cisco FindIT Network Probe.

What's New in Cisco FindIT Network Manager & Probe, Release 2.0.0

Cisco FindIT Network Manager and Probe release 2.0.0 introduces the following new features and changes:

- The Probe management functionality has been migrated to the Manager. This has the following impact:
 - All network management is performed through the Manager GUI. There is no longer any reason to access the Probe GUI for day to day operations.
 - The device inventory contains all devices from all networks and may be filtered to display devices with common characteristics regardless of which network they are located in.
 - Configuration profiles and device groups may be applied across multiple networks.
 - Reports span all networks.
 - The Network Plug and Play feature is now integrated with the inventory, meaning that a device deployed using PnP will be automatically correlated with the same device discovered by a Probe.
- FindIT Network Manager now supports the concept of Organizations. Organizations allow networks and configuration data to be divided based on administrative characteristics (For example, end customer identity, department or region). Access to network and configuration information may now be restricted to a subset of organizations on a per-user basis.
- The wireless reports have been enhanced to display data visually and be more interactive
- The wireless reports now keep historical data for up to two years
- The dashboard has been reworked to provide simpler and more flexible customization and layout. Dashboard widgets are now more interactive.
- Controls have been added allowing the user to individually enable and disable features that require sharing data with Cisco.
- Software images have been cryptographically signed to prevent tampering.

- Manager scalability is now based on the total number of devices under management, not the number of networks. This allows the Manager to support a larger number of networks with smaller average device counts.
- Numerous small user experience improvements have been made.

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>).

When running FindIT Network Manager in virtual machine, your hypervisor must be one of the following:

- 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

To run FindIT Network Manager under Ubuntu Linux, your environment must be running Ubuntu version 16.04.x (Xenial Xerus) on a 64-bit Intel architecture platform. Cisco recommends using the Ubuntu server distribution and only installing packages required by FindIT Network Manager.

Table 1 lists the compute resources required for FindIT Network Manager based on the number of devices under management.

Table 1: FindIT Network Manager Compute Resource Requirements

#Device Supported	# vCPU	RAM	Disk Space
Up to 300	2	4GB	60GB
Up to 2500	12	24GB	60GB

To run FindIT Network Manager in AWS, you will need an AWS account. The following AWS instances types are supported:

- t2.medium—up to 150 devices under management
- c4.4xlarge/c5.4xlarge—up to 2500 devices under management

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 11 (macOS only) or above
- Google Chrome version 72 (Recommended) or above
- Microsoft Edge version 42 or above

- Mozilla Firefox version 65 or above



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

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*, in the [Cisco FindIT Network Manager and Probe Quick Start Guide](#).

System Requirements for Cisco FindIT Network Probe

Cisco FindIT Network Probe is distributed as a virtual machine image, and as installers for use with the following operating systems:

- Ubuntu Linux distribution running on a PC
- Raspbian Linux distribution running on a Raspberry Pi

FindIT Network Probe is also available as an embedded feature of select Cisco 100 to 500 series products.

To run FindIT Network Probe as a virtual machine, your environment must meet the following requirements:

- Hypervisor:
 - Microsoft Hyper-V version 10.0 or above
 - Oracle VirtualBox version 5.0.2 or above
 - VMWare—It can be one of the following:
 - ESXi version 5.5 or above
 - Fusion version 7 or above
 - Workstation version 12 or above
- Virtual machine resource requirements:
 - CPU: 1x 64-bit Intel architecture
 - Memory: 512MB
 - Disk space: 5GB

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

- Ubuntu version 16.04.x (Xenial Xerus)
- CPU: 1x 64-bit Intel architecture
- Memory: 512MB
- Disk space: 5GB

To run the FindIT Network Probe on a Raspberry Pi operating system, your environment must meet the following requirements:

- Hardware: Raspberry Pi 3 Model B
- Disk space: 5GB
- OS: Raspbian Stretch

To run the FindIT Network Probe as an embedded application on a Cisco 100 to 500 series product, you must have a supported product running a firmware version that supports the FindIT Network Probe feature. Consult the [Cisco FindIT Network Manager – Device Support List](#) for details of hardware and version requirements. Also consult the administration guide for the product to determine any additional platform-specific requirements.

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

- Apple Safari version 11 (macOS only) or above
- Google Chrome version 72 (Recommended) or above
- Microsoft Edge version 42 or above
- Mozilla Firefox version 65 or above

FindIT Network Probe monitors and accesses the network devices that meet the following requirements:

- Must be in the same subnet as the PC that is running the FindIT Network Probe, or be directly attached to a managed device and reachable via TCP/IP
- Must be a Cisco 100 to 500 Series device with the Bonjour service enabled

Cisco Supported Devices

FindIT Network Manager supports the Cisco 100 to 500 series products. For a detailed list of devices and features supported, please refer to the [Cisco FindIT Network Manager - Device Support List](#).

License Requirements

FindIT Network Manager is a licensed application. Device licenses are required for each Cisco 100 to 500 series product being managed. A count of up to ten Cisco 100 to 500 series devices may be managed in **Evaluation Mode** without a license. For more information, please refer to the [FindIT Network Manager Datasheet](#) page.

Upgrading to Cisco FindIT 2.0.0 from 1.1.x

To upgrade from FindIT Network Manager or Probe version 1.1.x to version 2.0.0, do the following:

1. On the Manager, click **About FindIT**
2. Select the radio button next to the Manager update and click **Upgrade**. The Manager will download and apply the update and then restart
3. Log back on to the Manager, click **About FindIT** again
4. Select the radio button next to the Probe update and click **Upgrade**. Each Probe will download and apply the update and then restart

When upgrading from 1.1.x to 2.0.0, the following changes will be made during the upgrade process:

- Each **Network Plug and Play** Project will be converted to a network and a device group with names corresponding to the project name prefixed with PnP
- Device Groups defined on each probe are moved to the manager and the group name is prefixed with the name of the network
- Network and System configuration profiles will be moved to the manager

In addition, certain information previously stored on the Probe will not be migrated to the Manager:

- Device credentials defined in the **Add New Credentials** section of the **Device Credentials** page will not be migrated to the Manager. However, any device that has working credentials assigned will continue to have those credentials assigned after the upgrade.
- Device configuration backups will not be retained through the upgrade. Backups should be downloaded to the local PC prior to performing the upgrade.
- Floorplans will be lost during the upgrade.
- Any dashboard customization will be lost during the upgrade.



Note

Probe configuration will only be migrated to the manager if the probe upgrade is triggered through the manager user interface. If the probe upgrade is triggered from the probe user interface, or the probe is manually upgraded by running the linux installer on the probe platform, the configuration migration process will not take place.

Support for 1.1.x Probes with a 2.0.0 Manager

FindIT Network Manager 2.0.0 provides limited support for FindIT Network Probe version 1.1.x to allow upgrades to be gradually deployed across the network. Selecting the network and clicking Manage opens the Probe GUI in a new window giving the same experience as with a version 1.1.x manager. The network may then be managed through the probe user interface as normal. Please note that any changes to the network name or location in the Probe user interface will not be reflected in the Manager user interface.

In addition to the ability to access the probe user interface directly, the following functionality is available from the Manager user interface:

- Viewing device information through the inventory is supported for networks with probe version 1.1.x
- The **Lifecycle**, **End of Life** and **Maintenance** reports include devices from networks with probe version 1.1.x
- The **Event Log** displays events for networks with probe version 1.1.x
- The probe may be upgraded to version 2.0.0 from the manager user interface

Limitations and Restrictions

The Cisco FindIT Network limitations and restrictions are described in the following sections:

- [General Limitations](#)
- [System Backup and Restore](#)

General Limitations

- The web interface on FindIT Network Manager takes a few minutes to become operational after the application is started
- Depending on the size of the network, it may take the Probe several minutes to discover all devices and calculate the network topology
- Up to 50 network devices can be managed by single Probe instance
- Up to 2500 devices can be managed by a single Manager instance
- SNMPv3 authentication keys and privacy keys must be at least 8 characters in length
- When using Safari, ensure that the certificate presented by the FindIT Network Probe is set to **Always Trust**

System Backup and Restore

- When performing a system backup or restore, FindIT will prevent you from doing any further configuration actions
- Prior to beginning a system backup or restore, the idle timeout value in **Administration > User Management > User Session Settings** should be set to at least 30 minutes (default is 60 minutes)

Caveats

The following table lists the open caveats for version 2.0.0

Table 2: Open Caveats

Caveat ID Number	Headline
CSCvc02341	Roaming devices connect to multiple APs on topology Workaround There is no workaround at this time.
CSCvc03176	System configurations and network settings don't apply on devices when restoring configurations Workaround Apply configuration to device using Apply Pending Config button in the Device Detail page.
CSCvc04204	Getting the duplicated entry in the credentials table for switch stack after power off the master Workaround When the stack is stable, reboot Probe.

Caveat ID Number	Headline
CSCvc04252	<p>Sometimes it report error when online upgrade device firmware</p> <p>Workaround</p> <p>Make sure Probe can connect to cisco.com and then reboot Probe, or upgrade firmware from local.</p>
CSCvf49309	<p>FindIT displays outside WAN IP instead of device IP on Network Plug and Play - Unclaimed Devices page</p> <p>Workaround</p> <p>None</p>
CSCvf49332	<p>FindIT responses are slow when display is over 300 hosts on topology page</p> <p>Workaround</p> <p>Don't try displaying hosts when there are many.</p>
CSCvf58349	<p>Sometimes the data related to time in wireless report is not correct on modifying time setting</p> <p>Workaround</p> <p>None</p>
CSCvq25755	<p>Probe does NOT update ca-bundle periodically</p> <p>Workaround</p> <p>Reboot probe</p>
CSCvq25771	<p>System does not sync time from the host on VirtualBox</p> <p>Workaround</p> <p>Install VirtualBox Guest additions in the virtual machine with the command 'sudo apt-get install -y virtualbox-guest-utils' and reboot the virtual machine.</p> <p>Note The presence of VirtualBox Guest Additions in the virtual machine will prevent timesyncd from running and NTP will not function.</p>
CSCvq25794	<p>Profile with duplicated name is allowed to create in Network Configuration</p> <p>Workaround</p> <p>Select unique names when creating configuration profiles</p>
CSCvq25807	<p>Stack switch unit configuration is missing after master recovery from offline</p> <p>Workaround</p> <p>Manually read and accept current config or wait for the daily schedule job.</p>
CSCvq25817	<p>It doesn't show real VLAN setting info on a LAG port</p> <p>Workaround</p> <p>Review the VLAN configuration for the LAG on the device administration GUI</p>

Caveat ID Number	Headline
CSCvq34602	VLAN list in Topology Overlays does not refresh when switching networks Workaround Refreshing the browser will cause the VLAN list to display correctly.

The following table lists the resolved caveats for version 2.0.0

Table 3: Resolved Caveats

Caveat ID Number	Headline
CSCvc02354	Topology: Sometimes device names are covered by device icons when navigating back to the topology page
CSCvc02371	The same device event will pop up more than 2 times at the same time
CSCvc02381	There won't be a task record in task center when applying configuration to a new added group member
CSCvc04230	Can't add created VLAN to switch's trunk ports on new group member
CSCvn19635	It can't pass authentication when SNMP community length is over 15
CSCvo93538	Cisco FindIT Network Management Software Static Credentials Vulnerability
CSCvq35115	VM operating system subject to TCP DoS issues

Where to Find Support

For current support information, visit the following URLs:

Table 4: Where to Find Support

Support	
Cisco FindIT Network Support Forums	http://www.cisco.com/go/findit-support
Phone Support Contacts	http://www.cisco.com/go/sbse
Product Documentation	
Cisco FindIT Network Management Support and Documentation Resources	http://www.cisco.com/go/findit-docs
Cisco Small Business	
Cisco Small Business Home	http://www.cisco.com/go/smb
Cisco Small Business Support Community	http://www.cisco.com/go/smallbizsupport

