View the Reports on the FindIT Network Manager or Probe

Objective

The Cisco FindIT Network Management application provides tools that help you monitor and manage your Cisco 100 to 500 Series devices on the network conveniently through your web browser. When deployed properly, it automatically discovers your network, and allows you to configure and monitor devices such as Cisco switches, routers, and wireless access points connected to your network. It also prompts you of firmware updates, as well as device warranty, and support contract coverage.

The FindIT Network Manager and Probe generate a series of reports about your network device activity. The manager and probe generate reports such as a Summary report, an End of Life report, and a Maintenance report. The probe has two additional reports that it can generate, the Wireless Network and the Wireless Client.

The objective of this document is to show you how to view the reports generated by the Cisco FindIT Network Probe.

Applicable Devices

- Cisco FindIT Network Probe
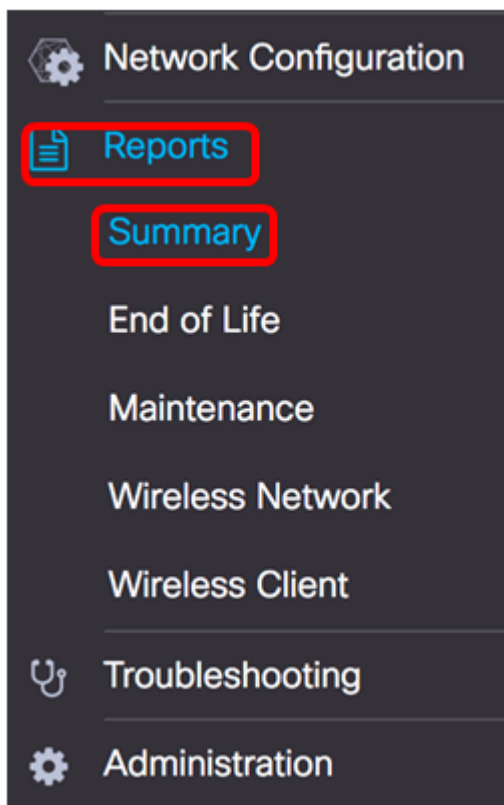- Cisco FindIT Network Manager

Software Version

- 1.1

Reports

Summary Report

The summary report shows a high level view and summary of the network devices.

Step 1. Log in to the web-based utility of the FindIT Network Probe or Network Manager and choose **Reports> Summary**.

The table below describes the high level summary of the network devices. The image below is taken from the Network Probe.

- Hostname — Name assigned to the device.
- Model — Model of the discovered device.
- Device Type — The type of network device discovered on the network. This can be a switch, router, and Wireless Access Point (WAP).
- Firmware Update Available — Displays the latest firmware version available for the network device or states that the device firmware is up to date.
- Current Firmware Version — Displays the current firmware version the device is running.
- End of Life Status — Displays an update of an End of Life status for the network device which includes a bulletin and a next milestone for the End of Life process.
- Maintenance Status — Displays information of the device if it is currently under warranty or covered by a support contract.

The image below is taken from the Network Manager.

| Site Name	Hostname	Device Type	Firmware Update ...	Current Firmware ...	End of Life Status	Maintenance Status
N/A	wampipti	WAP	Up to date	1.1.0.5	N/A	No data available. Contact support for assistance.
Davao	SwitchF4F23D	Switch	Up to date	1.1.2.1	N/A	No data available. Contact support for assistance.
Davao	wap5e0940	WAP	Up to date	1.0.0.3	N/A	No data available. Contact support for assistance.
Davao	switch12ccde	Switch	Up to date	1.4.7.6	N/A	No data available. Contact support for assistance.
Davao	SG350X	Switch	Up to date	2.3.0.130	N/A	No data available. Contact support for assistance.
Davao	WAP150	WAP	Up to date	1.0.1.7	N/A	No data available. Contact support for assistance.
Davao	router447453	Router	Up to date	1.0.01.17	N/A	N/A
Davao	WAP361	WAP	Up to date	1.1.0.5	N/A	No data available. Contact support for assistance.
Davao	RV130W	Router	Up to date	1.0.3.16	N/A	No data available. Contact support for assistance.
Davao	wap0ca750	WAP	Up to date	1.0.1.7	N/A	No data available. Contact support for assistance.

- Site Name — The name of the site in which the device is located.
- Hostname — Name assigned to the device.
- Model — Model of the discovered device.
- Device Type — The type of network device discovered on the network. This can be a switch, router, and Wireless Access Point (WAP).
- Firmware Update Available — Displays the latest firmware version available for the network device or states that the device firmware is up to date.
- Current Firmware Version — Displays the current firmware version the device is running.
- End of Life Status — Displays an update of an End of Life status for the network device which includes a bulletin and a next milestone for the End of Life process.
- Maintenance Status — Displays information of the device if it is currently under warranty or covered by a support contract.

Note: 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.

End of Life Report

The End of Life Report lists any device that have an End of Life bulletin published, along with key dates in the End of Life process, and the recommended replacement platform.

Step 1. From the Reports menu, choose **End of Life**.
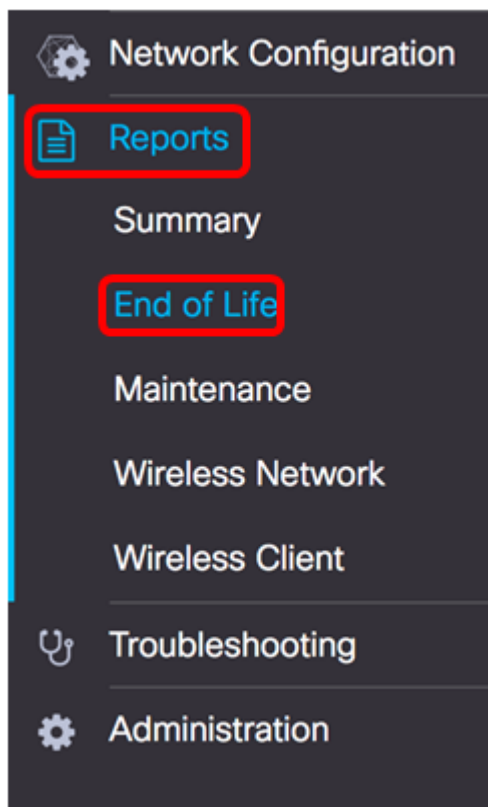
The list below describes the following:

Note: In this example, there are currently no announcements for devices with End of Life status. This image was taken from the Cisco FindIT Network Probe.
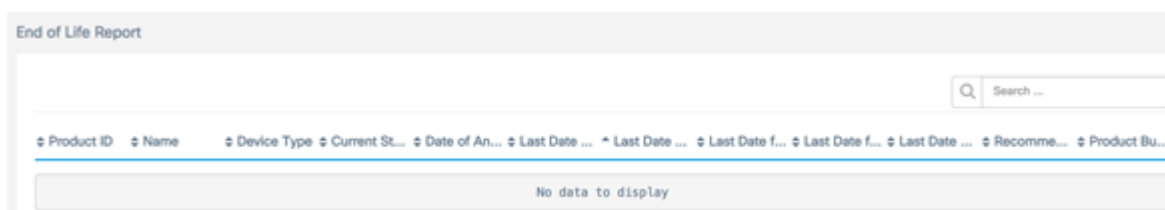
- Product ID — The product ID or part number of the device.
- Name — Assigned name of the device.
- Device Type — The type of network device discovered on the network. This can be a switch, router, and Wireless Access Point (WAP).
- Current Status — Stage or period of the device in the End of Life process.
- Date of Announcement — The date the End of Life announcement was published.
- Last Date of Sale — The date after which the product will no longer be sold by Cisco.
- Last Date of Software Release —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
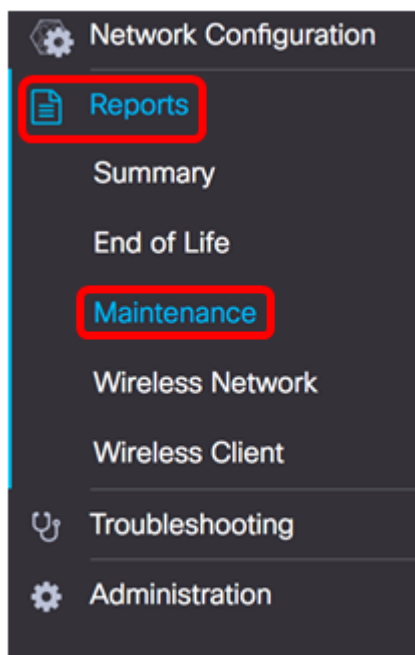
website.

Note: 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.

You should now have successfully views the End of Life Report.

Maintenance Report

The Maintenance Report is a list of the network devices which includes information about the warrant and support contract status for each device.

Step 1. From the Reports menu, choose **Maintenance**.

The list below describes the following:

- Device Type — The type of network device discovered on the network. This can be a switch, router, and Wireless Access Point (WAP).
- Hostname — Name assigned to the device.
- Model — Model of the discovered device.
- Serial Number — The serial number of 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 warrant for the device will expire.

You should now have successfully viewed the Maintenance Report on the Cisco FindIT Network Probe.

Wireless Network Report

Wireless Networks

The Wireless Network Report shows details about the wireless network broken down by SSID, wireless spectrum usage, and access point, and includes a list of rogue access points that have been detected. Daily or weekly reports may be generated using the controls at the top of the page. Up to seven days of data is retained on the Probe.

Note: This report is not available on the Network Manager.

Step 1. From the Reports menu, choose **Wireless Network**.
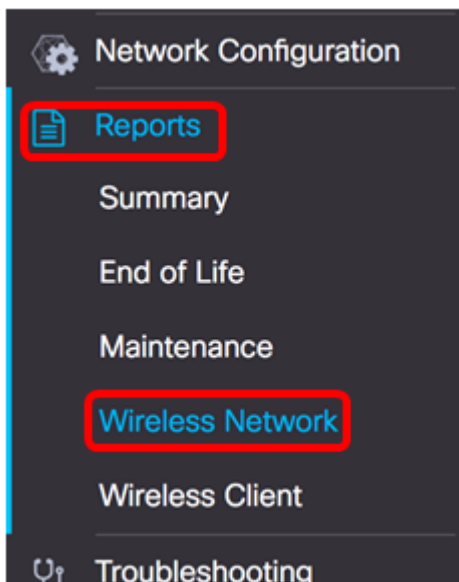
The list below describes the following:

Network	Security	Guest	Client Count (Peak)	Client Count (Ave...	Traffic (Peak)	Traffic (Average)
Ang Bandang Shirley	WPA/PSK	false	0	0	0Mbps	0Mbps
HelloEuphoria	WPA/PSK	false	0	0	0Mbps	0Mbps
Humming	WPA/PSK	false	0	0	0Mbps	0Mbps
Rick	WPA/PSK	false	0	0	0Mbps	0Mbps

- Network — Service Set Identifier (SSID) of the Wireless Network.
- Security — The password security applied to the network.
- Guest — Determines if the network is configured for guest access. Possible outcomes are either true or false.
- Client Count (Peak) — The maximum number of clients connected to the network during

the period covered by the report.

- Client Count (Average) — The average number of clients connected to the network during the period covered by the report.
- Traffic (Peak) — The maximum aggregate traffic rate through the network during the period covered by the report. This is measured in Mbps.
- Traffic (Average) — The average aggregate traffic rate through the network during the period covered by the report. This is measured in Mbps.

Spectrum Usage

The Spectrum Usage shows details about the average consumption of clients on a specific radio frequency or spectrum. Daily or weekly reports may be generated using the controls at the top of the page. Up to seven days of data is retained on the Probe.

Radio Freq	Client Count (Peak)	Client Count (Average)	Traffic (Peak)	Traffic (Average)
2.4GHz	0	0	0Mbps	0Mbps
5GHz	0	0	0Mbps	0Mbps

- Radio Freq — The radio frequency band in use. This can either be 2.4 GHz or 5 GHz.
- Client Count (Peak) — The maximum number of clients connected to the network during the period covered by the report.
- Client Count (Average) — The average number of clients connected to the network during the period covered by the report.
- Traffic (Peak) — The maximum aggregate traffic rate through the network during the period covered by the report. This is measured in Mbps.
- Traffic (Average) — The average aggregate traffic rate through the network during the period covered by the report. This is measured in Mbps.

Wireless Access Points

The Wireless Access Points report shows details about the number of clients and their average consumption. Daily or weekly reports may be generated using the controls at the top of the page. Up to seven days of data is retained on the Probe.

| Access Point	Model	Version	Client Count (P...	Client Count (A...	Traffic (Peak)	Traffic (Average)
wap5e0940	WAP125	1.0.0.3	0	0	11.713Mbps	0.019Mbps
wampipti	WAP150	1.1.0.5	0	0	0.319Mbps	0.017Mbps
WAP150	WAP150	1.0.1.7	0	0	0Mbps	0Mbps
WAP361	WAP361	1.1.0.5	0	0	0Mbps	0Mbps
wap0ca750	WAP361	1.0.1.7	0	0	0Mbps	0Mbps

- Access Point — Name of Access Point.

- Model — Model of the discovered device.
- Version — The current firmware running on the access point.
- Client Count (Peak) — The maximum number of clients connected to the network during the period covered by the report.
- Client Count (Average) — The average number of clients connected to the network during the period covered by the report.
- Traffic (Peak) — The maximum aggregate traffic rate through the network during the period covered by the report. This is measured in Mbps.
- Traffic (Average) — The average aggregate traffic rate through the network during the period covered by the report. This is measured in Mbps.

Rogue Access Points

A Rogue Access Point (AP) is an access point that is installed on a secure network without the consent of the network administrator. Rogue APs can pose a security threat because anyone who installs a wireless router within the range of your network can potentially gain access to your network.
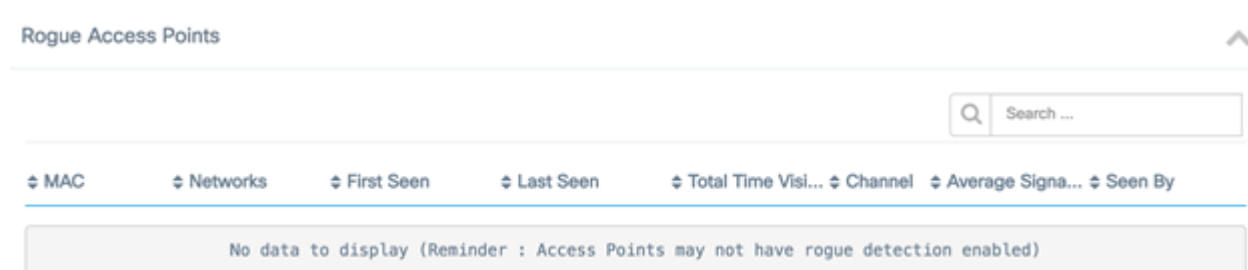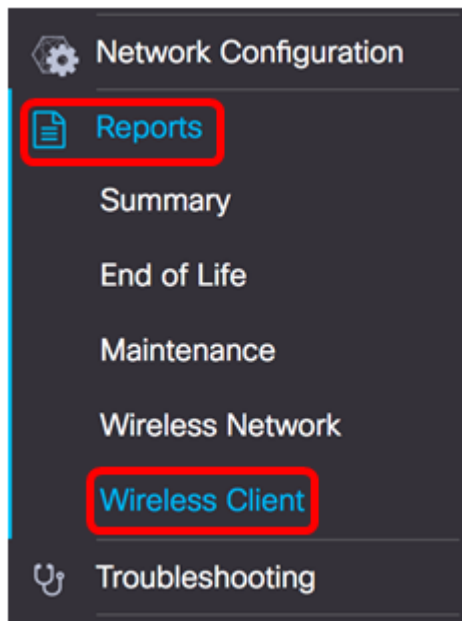

- MAC — The MAC address of the rogue AP.
- Networks — Shows the SSID detected.
- First Seen — The time at which the rogue AP was first detected.
- Last Seen — The time at which the rogue AP was last detected.
- Total Time Visible — The total amount of time that the rogue AP was online.
- Channel — The wireless channel used by the rogue AP.
- Average Signal Strength — The average signal strength of the rogue AP as seen by the detecting AP.
- Seen by — The AP that detected the rogue AP.

Wireless Client Report

The Wireless Client Report shows details about the wireless clients on the network. Daily or weekly reports may be generated using the controls at the top of the page. Up to seven days of data is retained on the Probe. This feature is not present on the Network Manager.

Step 1. From the Reports menu, choose **Wireless Client**.

The list below describes the following:

- MAC — The MAC address of the client.
- Networks — The SSID where the client was detected.
- 802.11 Type Frequency — The 802.11 variant and frequency band used by the client.
- Data Rate — The data rate last used by the client.
- Upload — The volume of data uploaded by the client.
- Download — The volume of data downloaded by the client.
- Total — The total volume of data transmitted and received by the client.
- First Seen — The time at which the client is first detected.
- Last Seen — The time at which the client is last detected.
- Time Online — The total amount of time at which a client is connected.
- % Online Time — The percentage of time the client was online and the total time the client was known on the network.

Wireless Guests

The Wireless Guests is used to monitor, maintain, and optimize the wireless connectivity between guests authenticated through a Captive Portal and the Wireless Access Point. Up to seven days of data is retained on the Probe.

Q Search ...

⇕ MAC	⇕ User...	⇕ Netw...	⇕ 802....	⇕ Data ...	⇕ Upload	⇕ Dow...	⇕ Total	⇕ First ...	⇕ Last ...	⇕ Time...	⇕ % On...

No data to display

- MAC — The MAC address of the guest.
- User — The user logged in and associated to the guest network.
- Network — The SSID where the guest was detected.
- 802.11 Type Frequency — The 802.11 variant and frequency band used by the guest.
- Data Rate — The data rate last used by the guest.
- Upload — The volume of data uploaded by the guest.
- Download — The volume of data downloaded by the guest.
- Total — The total volume of data transmitted and received by the guest.
- First Seen — The time at which the guest was first detected.
- Last Seen — The time at which the guest was last detected.
- Time Online — The total amount of time at which a guest is connected.
- % Online Time — The percentage of time the guest was online and the total time the client was known on the network.

You should now have successfully viewed the reports on the Cisco FindIT Network Probe and Manager.