



Device Lifecycle Management using Open-Audit For Cisco Devices

Solutions Guide E-Book by

Rob Pavone

IT Service Management Consultant



Table of Contents

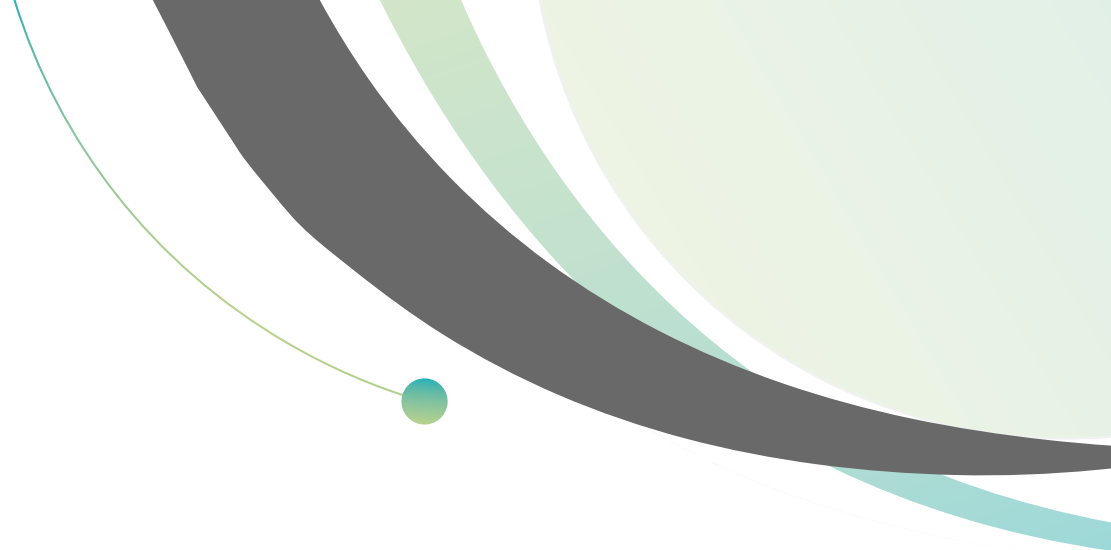
Objective	3
Tasks to Achieve Objective	3
Import the device list	4
Save off your “Cisco Ready xlsb report”	4
Log in to your Open-Audit server	4
Start generating queries and exporting reports	5
Create multiple customized dashboards	7
Supporting Information & References	8
About the Author	9

Objective

The objective of this solution guide is to provide organizations with reporting and dashboarding capabilities, leveraging Open-Audit, for tracking Cisco devices throughout their lifecycle on a network. The information presented in the reports and on the dashboards does rely on the Cisco Ready SMARTNET reports that can be requested from Cisco if you have SMARTNET contracts with them. This solution guide, however, can be applied to other vendors as well if you are able to retrieve detailed inventory information from the vendor similar to that of the Cisco inventory information, especially the EoX dates.

NOTE: In order to perform the dashboard tasks you must have Open-Audit Enterprise to customize and create multiple dashboards





01 Import the device list

If you are already monitoring devices on the network through NMIS, you will need to import the device list along with all credentials to Open-Audit. Open-Audit will do a discovery of the devices to ensure they can be reached. If reachable, the devices will be included in the reports and dashboards. Refer to the [“How to import NMIS Nodes and run discovery upon them”](#) in the Opmantek community for details on how to run the `import_into_open-audit.pl` script.

IMPORTANT: Open-Audit needs to run discovery after the import and

02 Save off your “Cisco Ready xlsb report”

Save off your “Cisco Ready xlsb report” (the Cisco Ready tab sheet) to a CSV format that will be used to import into Open-Audit. Copy that file to your Open-Audit server in to the `/usr/local/omk/bin` directory. Name the file `cisco.csv`.

03 Log in to your Open-Audit server

Next, log in to your Open-Audit server and change directories to `/usr/local/omk/bin`. Copy the script `import_cisco_into_open-audit.pl` into this directory and then run it. For more details on this script and step 2 check out the [Reconciling a spreadsheet from Cisco wiki page](#) in the Opmantek community.

04 Start generating queries and exporting reports

Once the inventory is imported from NMIS, discovered, and the filtered Cisco Ready csv file is imported into Open-Audit, you can start generating queries and exporting Reports. All of these reports can be exported to csv format and manipulated in Excel for further analysis. The [Reconciling a spreadsheet from Cisco wiki page](#) in the Opmantek community has a couple examples of some queries specific for this use case. Once the queries are created and ran, you can export the table to csv for further analysis and reporting. Refer to the [Open-Audit documentation to guide you through creating queries and exporting the reports](#) or [contact Opmantek support](#) for assistance.

A Full Inventory Report

The full inventory report from Open-Audit reports the entire devices list of active devices found on the network and contains serial numbers and EoX date information (End of Life, End of Service Contract, End of Sales, End of Warranty, etc). This report is a good up to date reference report for you and/or your customer to track timelines and serial numbers of devices that reside on the network.

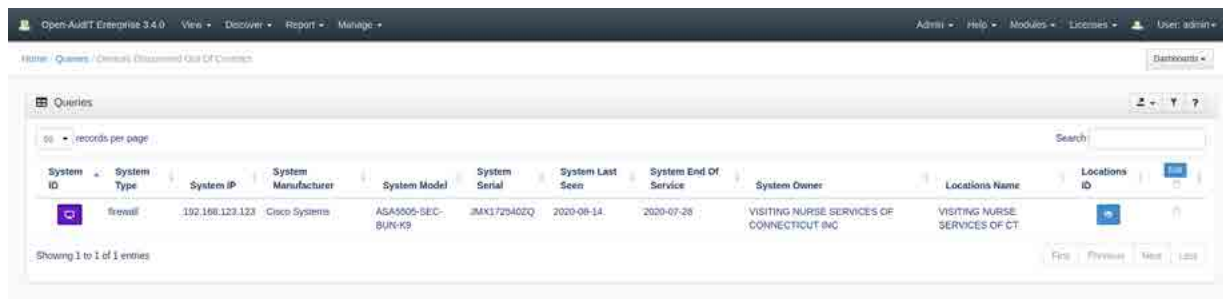


The screenshot shows the Open-Audit Enterprise 3.4.0 interface. The top navigation bar includes 'Admin', 'Help', 'Modules', 'Licenses', and 'User: admin'. The main content area displays a table of system information. The table has columns for System ID, System Type, System IP, System Manufacturer, System Model, System Serial, System Last Seen, System End Of Service, System End Of Life, System End Of Production, System Maintenance Expires, System Warranty Expires, System Owner, Location Name, and Location ID. A single entry is visible for a firewall system with IP 192.168.123.123, manufactured by Cisco Systems, model ASA5505-SEC-BUN-K9, and serial JMX172540ZQ. The system was last seen on 2020-08-14 and has an end of service date of 2020-07-28. The system owner is VISITING NURSE SERVICES OF CONNECTICUT INC, located at VISITING NURSE SERVICES OF CT.

System ID	System Type	System IP	System Manufacturer	System Model	System Serial	System Last Seen	System End Of Service	System End Of Life	System End Of Production	System Maintenance Expires	System Warranty Expires	System Owner	Location Name	Location ID
1	firewall	192.168.123.123	Cisco Systems	ASA5505-SEC-BUN-K9	JMX172540ZQ	2020-08-14	2020-07-28	2022-08-31	2017-08-28	2018-08-25	2014-01-03	VISITING NURSE SERVICES OF CONNECTICUT INC	VISITING NURSE SERVICES OF CT	

B Expired Contract Inventory

This report highlights devices that are no longer covered under the Cisco SNT contract and are active on the network.



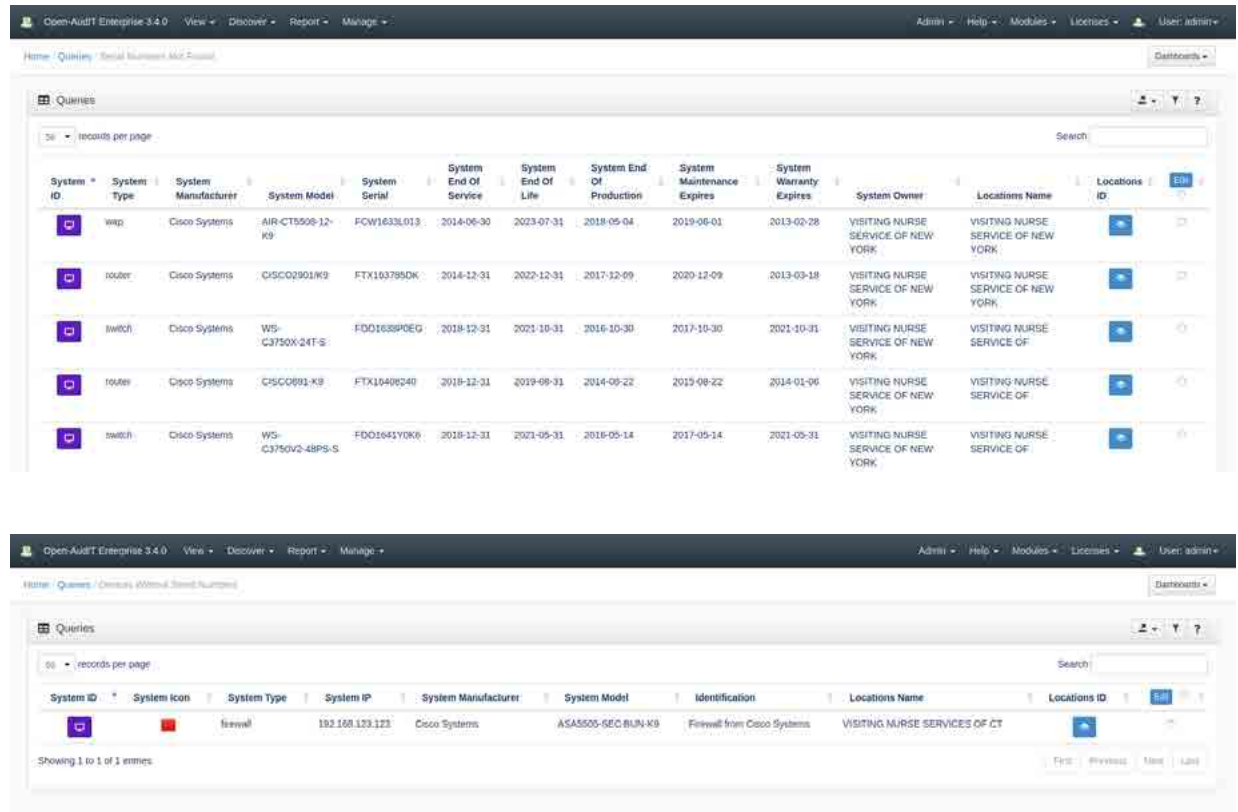
The screenshot shows the Open-Audit Enterprise 3.4.0 interface with the 'Expired Contract Inventory' query results. The table displays a single entry for a firewall system with IP 192.168.123.123, manufactured by Cisco Systems, model ASA5505-SEC-BUN-K9, and serial JMX172540ZQ. The system was last seen on 2020-08-14 and has an end of service date of 2020-07-28. The system owner is VISITING NURSE SERVICES OF CONNECTICUT INC, located at VISITING NURSE SERVICES OF CT.

System ID	System Type	System IP	System Manufacturer	System Model	System Serial	System Last Seen	System End Of Service	System Owner	Location Name	Location ID
1	firewall	192.168.123.123	Cisco Systems	ASA5505-SEC-BUN-K9	JMX172540ZQ	2020-08-14	2020-07-28	VISITING NURSE SERVICES OF CONNECTICUT INC	VISITING NURSE SERVICES OF CT	

C

Serial numbers not found

This report identifies devices covered in Cisco SNT contract but are not managed or seen as active on the network anywhere. The second report also highlights devices that are active on the network with no corresponding Cisco SNT coverage based on serial numbers.



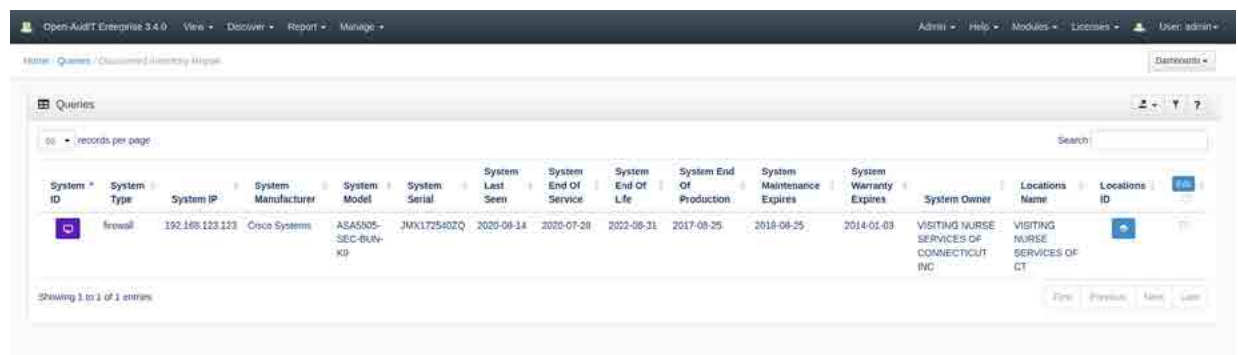
The screenshot shows the Open-Audit Enterprise 3.4.0 interface. The top navigation bar includes 'View', 'Discover', 'Report', and 'Manage'. The user is logged in as 'admin'. The main content area displays a table titled 'Queries' with the following columns: System ID, System Type, System Manufacturer, System Model, System Serial, System End Of Service, System End Of Life, System End Of Production, System Maintenance Expires, System Warranty Expires, System Owner, Locations Name, and Locations ID. The table contains five rows of data, all of which are Cisco Systems devices. The 'System Serial' column is empty for all entries, indicating that serial numbers are not found for these devices.

System ID	System Type	System Manufacturer	System Model	System Serial	System End Of Service	System End Of Life	System End Of Production	System Maintenance Expires	System Warranty Expires	System Owner	Locations Name	Locations ID
1	wap	Cisco Systems	AIR-CT5508-12-K9		2014-06-30	2023-07-31	2018-05-04	2019-06-01	2013-02-28	VISITING NURSE SERVICE OF NEW YORK	VISITING NURSE SERVICE OF NEW YORK	
2	router	Cisco Systems	CISCO2901/K9		2014-12-31	2022-12-31	2017-12-09	2020-12-09	2013-03-18	VISITING NURSE SERVICE OF NEW YORK	VISITING NURSE SERVICE OF NEW YORK	
3	lswitch	Cisco Systems	WS-C3750X-24TS		2018-12-31	2021-10-31	2016-10-30	2017-10-30	2021-10-31	VISITING NURSE SERVICE OF NEW YORK	VISITING NURSE SERVICE OF	
4	router	Cisco Systems	CISCO893-K9		2018-12-31	2019-08-31	2014-09-23	2015-08-22	2014-01-06	VISITING NURSE SERVICE OF NEW YORK	VISITING NURSE SERVICE OF	
5	switch	Cisco Systems	WS-C3750V2-48PS-S		2018-12-31	2021-05-31	2016-05-14	2017-05-14	2021-05-31	VISITING NURSE SERVICE OF NEW YORK	VISITING NURSE SERVICE OF	

D

EoX reports

There are multiple EoX reports that can be generated and useful for planning and budget forecasting. These reports include End of Service Contract, End of Warranty, End of Sales, End of Life (aka Last Day of Support (LDOS)), and Last day of Software Maintenance. The full inventory report can be used, downloaded and filtered to determine all the EoX devices for the respective fields.



The screenshot shows the Open-Audit Enterprise 3.4.0 interface. The top navigation bar includes 'View', 'Discover', 'Report', and 'Manage'. The user is logged in as 'admin'. The main content area displays a table titled 'Queries' with the following columns: System ID, System Type, System IP, System Manufacturer, System Model, System Serial, System Last Seen, System End Of Service, System End Of Life, System End Of Production, System Maintenance Expires, System Warranty Expires, System Owner, Locations Name, and Locations ID. The table contains one row of data, which is a Cisco Systems firewall device. The 'System Serial' column is empty, indicating that the serial number is not found for this device.

System ID	System Type	System IP	System Manufacturer	System Model	System Serial	System Last Seen	System End Of Service	System End Of Life	System End Of Production	System Maintenance Expires	System Warranty Expires	System Owner	Locations Name	Locations ID
1	firewall	192.168.123.123	Cisco Systems	ASA5505-SEC-BUN-K9		JMK172540ZQ	2020-08-14	2020-07-28	2022-08-31	2017-08-25	2018-08-25	2014-01-03	VISITING NURSE SERVICES OF CONNECTICUT INC	VISITING NURSE SERVICES OF CT

In order to create multiple customized dashboards within Open-Audit, you will need Open-Audit Enterprise. The following two dashboard recommendations are examples of Lifecycle Management dashboards for asset tracking that complement the reports. Refer to the Open-Audit documentation to guide you through **installing the “widgets” that create the dashboards** or contact **Opmantek support** for assistance.

A

DASHBOARD 1: Device Status Information Dashboard

- I. Organization (menu item filter)
- II. Device Type inventory
- III. Device Model inventory
- IV. Devices per location
- V. Active vs Expired devices in contract
- VI. Serial Numbers Found vs Not Found on the network (*Note: Cisco Ready data is considered the trusted source for serial numbers*)

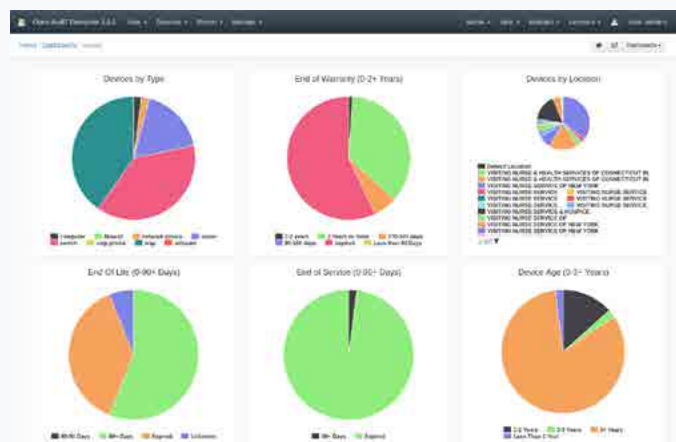


EXAMPLE SCREENSHOT OF DEVICE STATUS DASHBOARD

A

DASHBOARD 2: Device Lifecycle Timeline Dashboard

- I. Organization (menu item filter)
- II. Device Model inventory
- III. End of Warranty – expired, within 2 years, and longer
- IV. End of Service Contract – expired, within 90 days, and longer
- V. End of Product sale date – expired, within 2 years, and longer
- VI. End of Software Maintenance date – expired, within 2 years, and longer
- VII. End of Life (aka LDoS) – expired, within 1 year, 3 years, and longer



EXAMPLE SCREENSHOT OF DEVICE LIFECYCLE TIMELINE DASHBOARD

Supporting Information & References

Script: [How to import NMIS inventory and credentials into Open-Audit](#)

Script: [Importing Cisco Ready data into Open-Audit](#)

Documentation: [Open-Audit documentation in the Opmantek Community](#)

General [Cisco Partner Tools](#) link to get to Cisco Ready reports (you must have a Cisco account to access the tool)

About the Author



Rob Pavone

IT Service Management Consultant

Rob is an experienced technology Consultant spending most of his time helping organizations improve network availability, resiliency, and operational efficiency, as well as reducing Operational (OpEx) and Capital expenses (CapEx). He has been helping some of the largest enterprise organizations align business requirements with the level of service availability needed to support their business requirements.

He has accomplished this through establishing operational baselines, comparing existing practices with industry identified leading practices, and providing actionable recommendations, improving the clients' processes, tools, and staffing resources. Rob has been in the IT network industry for 30 years, having spent the last 26 years at Cisco Systems in the support organizations of the Technical Assistance Center (TAC) and Advanced Services based in Research Triangle Park, NC. Rob has achieved the following notable accomplishments throughout his career: ITILv3 Expert, ITIL4 Managing Professional, CCIE, SCRUM Master.



Thank You

Need a Hand?

If you'd like some guidance around setup and configuration, or If there's a specific issue you're trying to solve in your network environment - click below to request a demo from an Opmantek engineer.

