

How to discover a single Device

Discover a single device.

With this feature that was implemented in the Open-Audit 2.0.6 release, you can audit a single machine to get an idea of how OpenAudit works. Furthermore, you can use this feature to add a single device without performing a full discovery on a subnet.

Watch support engineer Paul McClendon quickly show you how to discover a single device.

Discover a single device Walk-Through



If you use a single IP or a range, please ensure that before you run a Discovery that you have added a corresponding [Network](#) so Open-Audit will accept audit results from those target IP's.

Navigate to the menu and go to Discover -> Discoveries -> Discover a single device

The screenshot shows the Open-Audit Enterprise 3.3.0 web interface. The top navigation bar includes 'Open-Audit Enterprise 3.3.0', 'View', 'Discover', 'Report', and 'Manage'. The 'Discover' menu is open, showing options like 'Clouds', 'Credentials', 'Discoveries', 'Files', 'Audit Scripts', 'List Discoveries', 'Create Discoveries', 'Import Multiple Discoveries', 'Discover a single device', 'Global Discovery Options', 'Discovery Match Options', 'Discovery Change Logs', 'Discovery Data Retention', 'Discovery Scan Options', and 'Schedule Discoveries'. The 'Discover a single device' option is highlighted in green. Below the menu, the 'Discoveries' form is visible, with fields for 'Device IP Address' (192.168.1.1), 'Network Address' (http://127.0.0.1/open-audit/), 'Devices Assigned to Org', 'Devices Assigned to Location', 'Windows Username' (user@domain.org), 'Windows Password', 'SSH Username' (username), 'SSH Password', 'SNMP Community (v1)' (public), and 'SNMP Community (v2)' (public). An 'Execute' button is at the bottom of the form. To the right, an 'About' section provides information on Discoveries and Notes.

Next, enter the Network Address of the machine you wish to audit and ensure you have added the credentials for this device. As displayed below there are places to enter credentials using a Windows username, SSH, or SNMP Community. Choose the option that best suites your situation. After all the required information is entered press the **Execute** button for the results.

The screenshot shows the Open-Audit Enterprise 3.3.0 web interface with the 'Discoveries' form filled out. The 'Device IP Address' field contains '192.168.1.1'. The 'Network Address' field contains 'http://127.0.0.1/open-audit/'. The 'Devices Assigned to Org' field is empty. The 'Devices Assigned to Location' field is empty. The 'Windows Username' field contains 'user@domain.org'. The 'Windows Password' field is empty. The 'SSH Username' field contains 'username'. The 'SSH Password' field is empty. The 'SNMP Community (v1)' field contains 'public'. The 'SNMP Community (v2)' field contains 'public'. An 'Execute' button is at the bottom of the form. To the right, an 'About' section provides information on Discoveries and Notes.

You will see a blue bar at the top of the window that indicates that the discovery of that device is running.

Discovery started.

Device Discovery for 192.168.88.0

- Summary
- Details
- Logs
- All IP Addresses
- Responding IPs
- Devices Discovered
- Devices Unknown or Unclassified

Logs

25 records per page

Showing 1 to 6 of 6 entries

Timestamp	ID	IP	Status	Message
2020-03-11 08:22:53	8503	127.0.0.1	start	Starting discovery for Device Discovery for 192.168.88.0
2020-03-11 08:22:53	8504	127.0.0.1	notice	Scanning 1 IP addresses using Nmap to test for response.
2020-03-11 08:22:54	8505	127.0.0.1	notice	Nmap response scanning completed. Time to execute: 0.4 seconds.
2020-03-11 08:22:54	8506	127.0.0.1	notice	Updating discovery log with non-responding IPs Time to execute: 0.0 seconds.
2020-03-11 08:22:54	8508	127.0.0.1	notice	No IPs are responding. You may wish to check your discovery configuration.
2020-03-11 08:22:54	8509	127.0.0.1	finished	Discovery has finished.

Showing 1 to 6 of 6 entries

Once the discovery has finished, navigate back to the Open-Audit home page to see the discovered device. You should see some of the charts on the dashboard screen start to populate with information.

To view more information on the device just audited: From the dashboard you will see a menu on the left of the screen. From there click on "My Devices" and select the device that was just audited by clicking the blue box details icon to the left.

Resources (All Devices)

Devices

50 records per page

System ID	System Icon	System Type	System Name	System IP	System One FQDN	System Identification	System Description	System Manufacturer	System OS Family	System Status	Bulk Action
		router	asgard	192.168.88.254	asgard.opmarketk.com	Router from Cisco Systems	Cisco IOS Software, 1841 Software (C1841-ADVENTERPRISEK9-M, Version 12.4(25), RELEASE SOFTWARE (fc2)) Technical Support: http://www.cisco.com/techsupport Copyright (c) 1986-2011 by Cisco Systems, Inc. Compiled Tue 16-Aug-11 06:21 by prod_nli_team	Cisco Systems	Cisco IOS	production	

After clicking the details button, a summary page is displayed containing information on the device selected. Using the menu on the left of the summary page you can view even more information such as the hardware, software, logs, as well as many other useful pieces of information. This information is displayed in a window below that opens after selecting a menu option. Navigate around to the different menu options to see all of the great features OpenAudit provides.

Summary - asgard

Name	asgard	Status	Production
IP	192.168.88.254	Environment	Production
Type	Router	Manufacturer	Cisco Systems
Description	Cisco IOS Software, 1841 Software (C1841-ADVENTERPRISEK9-M, Version 12.4(25), RELEASE SOFTWARE (fc2)) Technical Support: http://www.cisco.com/techsupport Copyright (c) 1986-2011 by Cisco Systems, Inc. Compiled Tue 16-Aug-11 06:21 by prod_nli_team	Model	Cisco 1841
OS Family	Cisco IOS	Serial	FHK11472788

- Actions
- Summary
- Summary
- Details
- Attachments
- Call Details
- Change Log
- Clusters
- Credentials
- Discovery Log
- Edit Log
- Fields
- Images
- IP Addresses
- Location
- Modules
- Opmarketk Details
- Owned By
- Purchase
- SNAP Details
- Hardware
- Settings
- Applications

Running into problems? Visit our [Troubleshooting](#) page.