Discovery Scan Options

Introduction

When a discovery is run, the relevant discovery scan option is chosen and those settings are used by Nmap to scan the target devices. The scan options determine which ports nmap scans, how fast they scan and whether or not nmap ping is first used to determine if the IP is live or not.

Starting with Open-AudIT 2.3.2 we have introduced sets of pre-configured options for running the discovery scan, these pre-configured options allow a range of Nmap scan options. More detail is here: New Discovery Options

As at 3.3.0 we have introduced a "filtered|open" option to discovery scan options, this option determines if an open but filtered port is considered as an interesting port on the remote device. It has a default of 'y'. Previously we used the "filtered" column to check for open|filtered. This change aligns the discovery scan options with Nmap return strings.

As at 4.0.3 we allow the user to over-write individual discovery scan options without having to create a 'custom scan'.

How Does it Work?

When a discovery is run, the relevant discovery scan option is chosen and those settings used by Nmap to scan the target devices. If no option set is chosen, the default configuration item (discovery_default_scan_option) is selected and used.

If a device is individually discovered using the "Discover Device" link on the device details page, we first check if this device has been discovered previously (by Discovery) and if so, use the discovery options from that scan. If it has not been previously discovered, we revert to the configuration item discovery_default_scan_option the settings.

Creating a Discovery Scan Options entry

Discovery Scan Options are just another item collection. Enterprise users can create, read, update and delete entries as required. Professional users can read all entries, but not create new entries, update existing entries or delete entries. Community users have no GUI that allows access to this collection.

The attributes for discovery scan options are as below.

Attribute	Description
ping	Must Respond To Ping. If set, Nmap will fist attempt to send and listen for an ICMP response. If the device does not respond, no further scanning will occur. Previously a device did not have to respond to a ping for Open-AudIT to continue scanning.
service_version	Use Service Version Detection. When a detected port is detected as open, if set to 'y', Nmap will query the target device in an attempt to determine the version of the service running on this port. This can be useful when identifying unclassified devices. This was not previously used.

open|filtered	An open|filtered port is considered open (and will trigger device detection). Previously, Open-AudIT considered an Nmap response of "open|filtered" as a device responding on this port. This has caused some customers issues where firewalls respond on behalf of a non-existing device, and hence cause false positive device detection. We now have this attribute available to set per scan.
filtered	A filtered port is considered open (and will trigger device detection).
timing	The standard Nmap timing options. Previously set at T4 (aggressive).
nmap_tcp_ports	Top Nmap TCP Ports. The top 10, 100, 1000 ports to scan as per Nmaps "top ports" options. Previously we scanned the Top 1000 ports (the Nmap standard).
nmap_udp_ports	Top Nmap UDP Ports. The top 10, 100, 1000 ports to scan as per Nmaps "top ports" options. Previously we scanned UDP 161 (snmp) only.
tcp_ports	Custom TCP Ports. Any specific ports we would liuke scanned in addition to the Top TCP Ports. Comma seperated, no spaces.
udp_ports	Custom UDP Ports. Any specific ports we would liuke scanned in addition to the Top UDP Ports. Comma seperated, no spaces.
	The below fields can be overwritten by an individual discovery, while still "using" a discovery_scan_options item for these if they're not set in the discovery (changed as at 4.0.3, see above).
timeout	Timeout per Target. Wait for X seconds for a target response.
exclude_tcp	Exclude any ports listed from being scanned. Comma seperated, no spaces.
exclude_udp	Exclude any ports listed from being scanned. Comma seperated, no spaces.
exclude_ip	Exclude IP Addresses (individual IP - 192.168.1.20, ranges - 192.168.1.30-40 or subnets - 192.168.1.100/30) listed from being scanned. Comma seperated, no spaces.
ssh_ports	Scan for this port(s) and if detected open, use this port for SSH communication. This is added to the list of Custom TCP POrts above, so there is no need to include it in that listr as well. Comma seperated, no spaces.

Database Schema

The database schema can be found in the application is the user has database::read permission by going to menu: Admin -> Database -> List Tables, then clicking on the details button for the table.

API / Web Access

You can access the collection using the normal Open-AudIT JSON based API. Just like any other collection. Please see The Open-AudIT API documentation for further details.

Default Items

Shipped are a set of default items. These can be found by going to menu: Help Defaults Discovery Scan Options.

Introduction

As at Open-AudIT 2.3.2 and later, we have introduced some easy to use and extremely powerful options for discovering devices. These options centre around directing Nmap on *how* to discover devices.

We have grouped these options into what we're calling Discovery Scan Options. We ship seven different groups of options (items) by default that cover the common use-cases.

This benefits Community, Professional and Enterprise customers.

Feature Availability

Feature availability is dependent on license type as per the table below.

Feature	Community	Professional	Enterprise
Match Rules - set default for all discoveries	y	y	y
Discovery Scan Options - set default for all discoveries	y	y	y
Discovery Scan Options - read		y	y
Discovery Scan Options - set per discovery		y	y
Discovery Scan Options - create, read, update, delete			y
Discovery Scan Options - Custom per Discovery			y
Discovery Scan Options - Exclude IP, range, subnet per discovery			y
Discovery Scan Options - Exclude ports per discovery			y
Discovery Scan Options - Set device timeout, per discovery			y
Discovery Scan Options - Custom SSH port per discovery			y
Match Rules - set per discovery			y

Discovery Scan Types

The Discovery Scan Options we ship are detailed in the table below. As above, Enterprise users can create more of these or edit the shipped items.

Attribute	UltraFast	SuperFast	Fast	Medium (Classic)[1]	Medium	Slow	UltraSlow
Approximate time in seconds for remote IP scan	1	5	40	90	100	240	1200
Must Respond to Ping	y	y	y	n	y	y	n
Use Service Version Detection	n	n	n	n	n	y	y
Consider Filtered Ports as Open	n	n	n	y	n	y	y
Timing	T4	T4	T4	T4	T4	T3	T2
Top Nmap TCP Ports		10	100	1000	1000	1000	1000
Top Nmap UDP Ports		10	100		100	100	1000
Custom TCP Ports	22,135,62078	62078	62078	62078	62078	62078	62078
Custom UDP Ports	161			161			
Exclude TCP Ports							
Exclude UDP Ports							
Timeout per Host							
Exclude IP (address, range, subnet)							
Custom SSH Port							

[1] The item for Medium (Classic) is similar to the Nmap for Discovery setting available in Open-AudIT 2.3.2.

Check the wiki here for a deeper look at Discovery Scan Options.

Example Scanning Improvement

We have a customer who is running discovery on a /22. The scan time to complete when using the original (hard set) options, prior to 2.3.2 was 29 hours. Using 2.3.2's UltraFast option, that scan now takes less than 10 minutes. To say they are impressed would be an understatement! They are now left with a smaller set of unknown devices that they can run a more detailed audit against. And remember, if the audited device is a computer, you will have a list of open ports derived from Netstat, anyway - possibly saving another audit cycle.

Use Cases

Handling Duplicate Serials

Recently we had cause to scan a subnet that was made up of virtual Cisco networking devices. These devices all happened to have identical serial numbers. Using the Match Rules per Discovery (available to Enterprise users) we were able to tweak the ruleset for this discovery only, without affecting other discoveries that rely upon matching a serial number. This ability solved a long-standing issue of working around a less than ideal setup on a network. A serial number, by definition, should be unique.

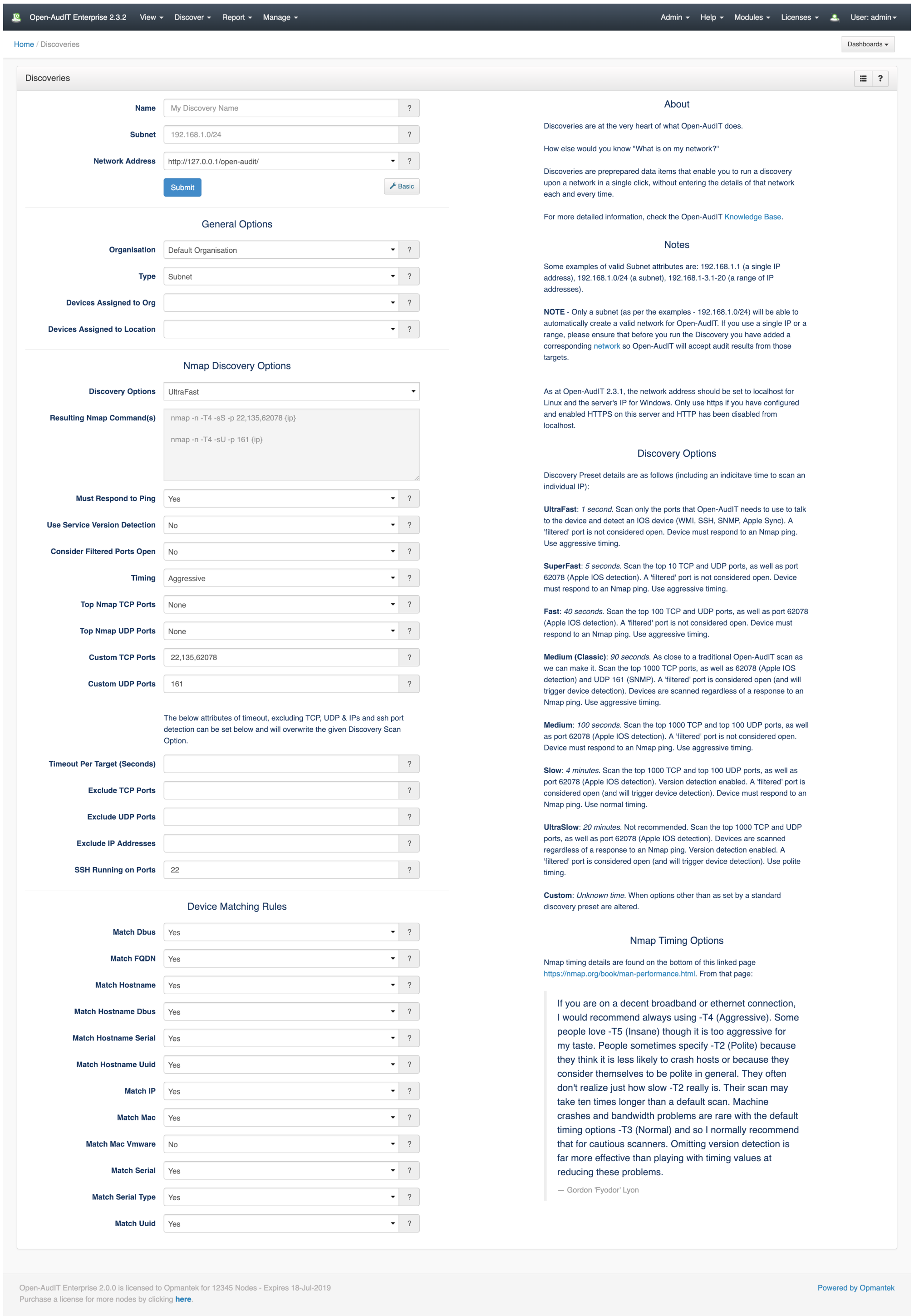
Filtered Ports

Networks respond differently depending on how they're configured. Some routers and/or firewalls can respond "on behalf" of IPs on the other side of their interfaces to the Open-AudIT Server. It is quite common to see Nmap report a probe for SNMP (UDP port 161) to respond as open|filtered for devices that do and do not exist. This is misleading as there is no device at that IP, yet it ends up with a device entry in the database. 99.9% of the time, it is not Open-AudIT, nor even Nmap, but the network causing this issue. Now that we have the options to treat open|filtered ports as either open or closed, we can eliminate a lot of this confusion. Enterprise users even have the option to change this on a per discovery basis (more than just using the Medium (Classic) item, as above).

Discovery Enterprise Options

The screenshot below is the Open-AudIT discovery page where all the audit configuration is set. I've added ample notes in the page explaining all the options making the tool easy to use for less technical staff.

Click to enlarge.



Name	My Discovery Name
Subnet	192.168.1.0/24
Network Address	http://127.0.0.1/open-audit/

General Options

Organisation	Default Organisation
Type	Subnet
Devices Assigned to Org	
Devices Assigned to Location	

Nmap Discovery Options

Discovery Options	UltraFast

Resulting Nmap Command(s)	nmap -n -T4 -sS -p 22,135,62078 {ip}
	nmap -n -T4 -sU -p 161 {ip}

Must Respond to Ping	Yes
Use Service Version Detection	No
Consider Filtered Ports Open	No
Timing	Aggressive
Top Nmap TCP Ports	None
Top Nmap UDP Ports	None
Custom TCP Ports	22,135,62078
Custom UDP Ports	161

The below attributes of timeout, excluding TCP, UDP & IPs and ssh port detection can be set below and will overwrite the given Discovery Scan Option.

Timeout Per Target (Seconds)	
Exclude TCP Ports	
Exclude UDP Ports	
Exclude IP Addresses	
SSH Running on Ports	22

Device Matching Rules

Match Dbus	Yes
Match FQDN	Yes
Match Hostname	Yes
Match Hostname Dbus	Yes
Match Hostname Serial	Yes
Match Hostname Uuid	Yes
Match IP	Yes
Match Mac	Yes
Match Mac Vmware	No
Match Serial	Yes
Match Serial Type	Yes
Match Uuid	Yes

About

Discoveries are at the very heart of what Open-AudIT does.

How else would you know "What is on my network?"

Discoveries are preprepared data items that enable you to run a discovery upon a network in a single click, without entering the details of that network each and every time.

For more detailed information, check the Open-AudIT Knowledge Base.

Notes

Some examples of valid Subnet attributes are: 192.168.1.1 (a single IP address), 192.168.1.0/24 (a subnet), 192.168.1-3.1-20 (a range of IP addresses).

NOTE - Only a subnet (as per the examples - 192.168.1.0/24) will be able to automatically create a valid network for Open-AudIT. If you use a single IP or a range, please ensure that before you run the Discovery you have added a corresponding network so Open-AudIT will accept audit results from those targets.

As at Open-AudIT 2.3.1, the network address should be set to localhost for Linux and the server's IP for Windows. Only use https if you have configured and enabled HTTPS on this server and HTTP has been disabled from localhost.

Discovery Options

Discovery Preset details are as follows (including an indicitave time to scan an individual IP):

UltraFast: *1 second*. Scan only the ports that Open-AudIT needs to use to talk to the device and detect an IOS device (WMI, SSH, SNMP, Apple Sync). A 'filtered' port is not considered open. Device must respond to an Nmap ping. Use aggressive timing.

SuperFast: *5 seconds*. Scan the top 10 TCP and UDP ports, as well as port 62078 (Apple IOS detection). A 'filtered' port is not considered open. Device must respond to an Nmap ping. Use aggressive timing.

Fast: *40 seconds*. Scan the top 100 TCP and UDP ports, as well as port 62078 (Apple IOS detection). A 'filtered' port is not considered open. Device must respond to an Nmap ping. Use aggressive timing.

Medium (Classic): *90 seconds*. As close to a traditional Open-AudIT scan as we can make it. Scan the top 1000 TCP ports, as well as 62078 (Apple IOS detection) and UDP 161 (SNMP). A 'filtered' port is considered open (and will trigger device detection). Devices are scanned regardless of a response to an Nmap ping. Use aggressive timing.

Medium: *100 seconds*. Scan the top 1000 TCP and top 100 UDP ports, as well as port 62078 (Apple IOS detection). A 'filtered' port is not considered open. Device must respond to an Nmap ping. Use aggressive timing.

Slow: *4 minutes*. Scan the top 1000 TCP and top 100 UDP ports, as well as port 62078 (Apple IOS detection). Version detection enabled. A 'filtered' port is considered open (and will trigger device detection). Device must respond to an Nmap ping. Use normal timing.

UltraSlow: *20 minutes*. Not recommended. Scan the top 1000 TCP and UDP ports, as well as port 62078 (Apple IOS detection). Devices are scanned regardless of a response to an Nmap ping. Version detection enabled. A 'filtered' port is considered open (and will trigger device detection). Use polite timing.

Custom: *Unknown time*. When options other than as set by a standard discovery preset are altered.

Nmap Timing Options

Nmap timing details are found on the bottom of this linked page https://nmap.org/book/man-performance.html. From that page:

> If you are on a decent broadband or ethernet connection, I would recommend always using -T4 (Aggressive). Some people love -T5 (Insane) though it is too aggressive for my taste. People sometimes specify -T2 (Polite) because they think it is less likely to crash hosts or because they consider themselves to be polite in general. They often don't realize just how slow -T2 really is. Their scan may take ten times longer than a default scan. Machine crashes and bandwidth problems are rare with the default timing options -T3 (Normal) and so I normally recommend that for cautious scanners. Omitting version detection is far more effective than playing with timing values at reducing these problems.
>
> — Gordon 'Fyodor' Lyon

Open-AudIT Enterprise 2.0.0 is licensed to Opmantek for 12345 Nodes - Expires 18-Jul-2019
Purchase a license for more nodes by clicking **here**.

Powered by Opmantek

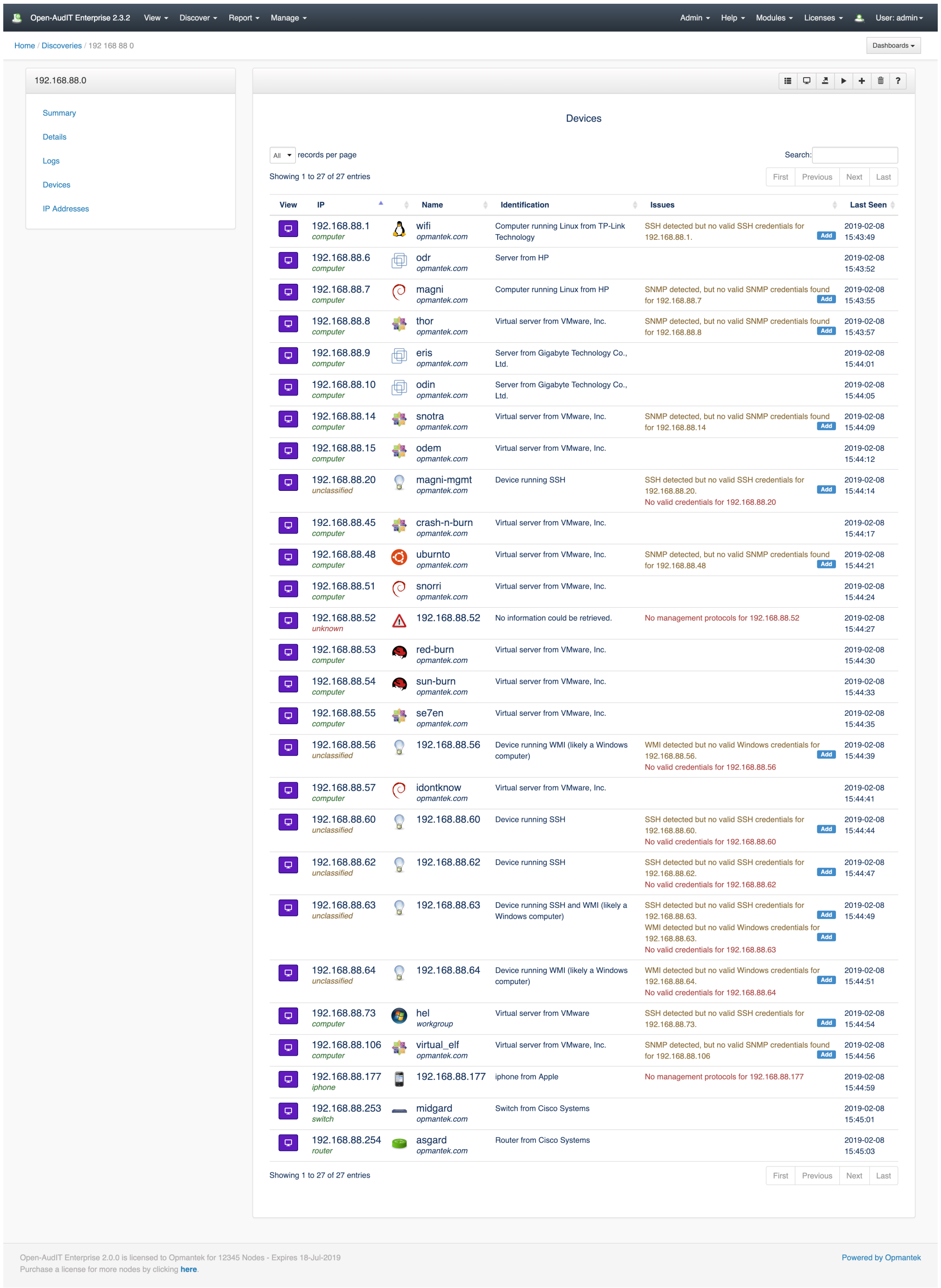
Check the wiki for a more detailed explanation about Discoveries

Display Improvements

As well as the functional improvements to discovery, we have also revised the Discovery Details page. We have sections for Summary, Details, Devices, Logs and IP Addresses. The Devices section, in particular, is now much more useful. We have added a new type of Unclassified to the list and we use this when we have more than just an IP and/or name for the device. For instance, we may know it's IP, name and the fact that it has port 135 open. This at least is a good indication that the device is likely a Windows machine. So we know "something". More than just "there is something at this IP". That is now an Unclassified device. We still support Unknown devices as always - for those devices we really know nothing about. An example of this screen is below. We also provide a quick link to creating credentials when a service (SSH, WMI, SNMP) has been identified, but we were not able to authenticate to it.

We think these display improvements will go a long way to assisting you to remove any Unknown or Unclassified devices that are on your network.

Click to enlarge.



Home / Discoveries / 192 168 88 0

192.168.88.0

Devices

All records per page

Search:

Showing 1 to 27 of 27 entries

View	IP	Name	Identification	Issues	Last Seen
	192.168.88.1 *computer*	wifi *opmantek.com*	Computer running Linux from TP-Link Technology	SSH detected but no valid SSH credentials for 192.168.88.1. Add	2019-02-08 15:43:49
	192.168.88.6 *computer*	odr *opmantek.com*	Server from HP		2019-02-08 15:43:52
	192.168.88.7 *computer*	magni *opmantek.com*	Computer running Linux from HP	SNMP detected, but no valid SNMP credentials found for 192.168.88.7 Add	2019-02-08 15:43:55
	192.168.88.8 *computer*	thor *opmantek.com*	Virtual server from VMware, Inc.	SNMP detected, but no valid SNMP credentials found for 192.168.88.8 Add	2019-02-08 15:43:57
	192.168.88.9 *computer*	eris *opmantek.com*	Server from Gigabyte Technology Co., Ltd.		2019-02-08 15:44:01
	192.168.88.10 *computer*	odin *opmantek.com*	Server from Gigabyte Technology Co., Ltd.		2019-02-08 15:44:05
	192.168.88.14 *computer*	snotra *opmantek.com*	Virtual server from VMware, Inc.	SNMP detected, but no valid SNMP credentials found for 192.168.88.14 Add	2019-02-08 15:44:09
	192.168.88.15 *computer*	odem *opmantek.com*	Virtual server from VMware, Inc.		2019-02-08 15:44:12
	192.168.88.20 *unclassified*	magni-mgmt *opmantek.com*	Device running SSH	SSH detected but no valid SSH credentials for 192.168.88.20. Add No valid credentials for 192.168.88.20	2019-02-08 15:44:14
	192.168.88.45 *computer*	crash-n-burn *opmantek.com*	Virtual server from VMware, Inc.		2019-02-08 15:44:17
	192.168.88.48 *computer*	uburnto *opmantek.com*	Virtual server from VMware, Inc.	SNMP detected, but no valid SNMP credentials found for 192.168.88.48 Add	2019-02-08 15:44:21
	192.168.88.51 *computer*	snorri *opmantek.com*	Virtual server from VMware, Inc.		2019-02-08 15:44:24
	192.168.88.52 *unknown*	192.168.88.52	No information could be retrieved.	No management protocols for 192.168.88.52	2019-02-08 15:44:27
	192.168.88.53 *computer*	red-burn *opmantek.com*	Virtual server from VMware, Inc.		2019-02-08 15:44:30
	192.168.88.54 *computer*	sun-burn *opmantek.com*	Virtual server from VMware, Inc.		2019-02-08 15:44:33
	192.168.88.55 *computer*	se7en *opmantek.com*	Virtual server from VMware, Inc.		2019-02-08 15:44:35
	192.168.88.56 *unclassified*	192.168.88.56	Device running WMI (likely a Windows computer)	WMI detected but no valid Windows credentials for 192.168.88.56. Add No valid credentials for 192.168.88.56	2019-02-08 15:44:39
	192.168.88.57 *computer*	idontknow *opmantek.com*	Virtual server from VMware, Inc.		2019-02-08 15:44:41
	192.168.88.60 *unclassified*	192.168.88.60	Device running SSH	SSH detected but no valid SSH credentials for 192.168.88.60. Add No valid credentials for 192.168.88.60	2019-02-08 15:44:44
	192.168.88.62 *unclassified*	192.168.88.62	Device running SSH	SSH detected but no valid SSH credentials for 192.168.88.62. Add No valid credentials for 192.168.88.62	2019-02-08 15:44:47
	192.168.88.63 *unclassified*	192.168.88.63	Device running SSH and WMI (likely a Windows computer)	SSH detected but no valid SSH credentials for 192.168.88.63. Add WMI detected but no valid Windows credentials for 192.168.88.63. Add No valid credentials for 192.168.88.63	2019-02-08 15:44:49
	192.168.88.64 *unclassified*	192.168.88.64	Device running WMI (likely a Windows computer)	WMI detected but no valid Windows credentials for 192.168.88.64. Add No valid credentials for 192.168.88.64	2019-02-08 15:44:51
	192.168.88.73 *computer*	hel *workgroup*	Virtual server from VMware	SSH detected but no valid SSH credentials for 192.168.88.73. Add	2019-02-08 15:44:54
	192.168.88.106 *computer*	virtual_elf *opmantek.com*	Virtual server from VMware, Inc.	SNMP detected, but no valid SNMP credentials found for 192.168.88.106 Add	2019-02-08 15:44:56
	192.168.88.177 *iphone*	192.168.88.177	iphone from Apple	No management protocols for 192.168.88.177	2019-02-08 15:44:59
	192.168.88.253 *switch*	midgard *opmantek.com*	Switch from Cisco Systems		2019-02-08 15:45:01
	192.168.88.254 *router*	asgard *opmantek.com*	Router from Cisco Systems		2019-02-08 15:45:03

Showing 1 to 27 of 27 entries

Open-AudIT Enterprise 2.0.0 is licensed to Opmantek for 12345 Nodes - Expires 18-Jul-2019
Purchase a license for more nodes by clicking **here**.

Powered by Opmantek

Wrap Up

This new functionality makes Open-AudIT a powerful and easy to use discovery solution while providing great flexibility for advanced users.

I hope you enjoy the new features as much as our test customers and I do.

Mark Unwin.