Discovery Scan Options

- Introduction
- How Does it Work?
- Creating a Discovery Scan Options entry
- Database Schema
- API / Web Access
- Default Items
- Introduction
- Feature Availability
- Discovery Scan Types
- Example Scanning Improvement
- Use Cases
 - Handling Duplicate Serials
- Filtered Ports
- Discovery Enterprise Options
- Display Improvements
- Wrap Up

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_ver sion	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	У	у	у
Discovery Scan Options - set default for all discoveries	У	у	у
Discovery Scan Options - read		у	у
Discovery Scan Options - set per discovery		у	у
Discovery Scan Options - create, read, update, delete			у
Discovery Scan Options - Custom per Discovery			у
Discovery Scan Options - Exclude IP, range, subnet per discovery			у
Discovery Scan Options - Exclude ports per discovery			у
Discovery Scan Options - Set device timeout, per discovery			у
Discovery Scan Options - Custom SSH port per discovery			У
Match Rules - set per discovery			У

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	у	у	У	n	у	У	n
Use Service Version Detection	n	n	n	n	n	У	у
Consider Filtered Ports as Open	n	n	n	У	n	У	у
Timing	T4	T4	T4	T4	T4	Т3	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							

¹The 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.

Open-AudIT Enterprise 2.3.2 View	 Discover - Report - Manage - 		Admin - Help - Modules - Licenses - 🚢 User: ad
/ Discoveries			Dashboard
iscoveries			Ξ
Name	My Discovery Name	?	About
Subnet	192.168.1.0/24	?	Discoveries are at the very heart of what Open-AudIT does.
Network Address		- 2	How else would you know "What is on my network?"
Network Address	Submit	✓ F Basic	Discoveries are proprepared 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.
	General Options		For more detailed information, check the Open-Aud/T Knowledge Base.
Organisation	Default Organisation	• ?	Notes
Type	Subpet	• ?	Some examples of valid Subnet attributes are: 192.168.1.1 (a single IP
Devices Assigned to Ora		- 2	aduress, rez. ros. r.u.z4 (a sourier), rez. ros. r-s. r-z0 (a range or in- addresses).
Devices Assigned to Location		• ?	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 desse service that before your un the Discrement your have added a
	Nmap Discovery Options		terings, beade ensure that before you full the Discovery you have access a corresponding network so Open-AudIT will accept audit results from those targets.
Discovery Ontions	LitraEast	-	As at Onen, AuriT 2.3.1, the network address should be set to localized for
Discovery options			Linux and the server's IP for Windows. Only use https://www.endigured and enabled HTTPS on this server and HTTP has been disabled from
Resulting Nmap Command(s)	nmap -n -14 -s5 -p 22,135,62078 (ip)		localhost.
	1111ap 11 - 14 - 50 - p 161 (ip)		Discovery Options
		le.	Discovery Preset details are as follows (including an indicitave time to scan an individual IBY:
Must Respond to Ping	Yes	- ?	UltraFast: 1 second. Scan only the ports that Open-AudiT needs to use to talk
Use Service Version Detection	No	• ?	to the device and detect an IOS device (WIMI, SSH, SNMP, Apple Sync). A "filtered" port is not considered open. Device must respond to an Nmap ping.
Consider Filtered Ports Open	No	• ?	SuperFast: 5 seconds. Scan the top 10 TCP and UDP ports, as well as port
Timing	Aggressive	• ?	62078 (Apple IOS detection). A 'littered' port is not considered open. Device must respond to an Nmap ping. Use aggressive timing.
Top Nmap TCP Ports	None	• ?	Fast: 40 seconds. Scan the top 100 CP and UDP ports, as well as port 62078 (Apple IOS detection). A 'filtered' port is not considered open. Device must
Top Nmap UDP Ports	None		respond to an Nmap ping. Use aggressive timing.
Custom TCP Ports	22,135,62078	?	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 ports is considered open (and will
	The below attributes of timeout, excluding TCP, UDP 4 detection can be set below and will overwrite the given Option.	& IPs and ssh port n Discovery Scan	Negative data databasety to share a submark regaritized of a respective to an Ningpiro, Like agreesses limiting. Medium: 100 seconds. Scan the top 1000 TCP and top 100 UDP ports, as well as port 63707 (Apple ICS detection). A filtered ² port and considered open. Device must respect to an Nina princ, the agreessive timing.
Timeout Per Target (Seconds)		?	Slow: 4 minutes. Scan the top 1000 TCP and top 100 UDP ports, as well as
Exclude TCP Ports		?	port 62078 (Apple IOS detection). Version detection enabled. A 'filtered' port is considered open (and will trigger device detection). Device must respond to an
Exclude UDP Ports		?	Nmap ping. Use normal liming.
Exclude IP Addresses		?	UltraSiow: 20 minutes. Not recommended. Scan the top 1000 TCP and UDP ports, as well as port 62078 (Apple IOS detection). Devices are scanned presented in the scanner is no Mercine a detection excluded a
SSH Running on Ports	22	?	regardises or a response to an Nimap ping. Version detection enabled. A "filtered" port is considered open (and will trigger device detection). Use polite timing.
	Device Matching Rules		Custom: Unknown time. When options other than as set by a standard discovery preset are altered.
Match Dbus	Yes	• ?	Nmap Timing Options
Match FQDN	Yes	• ?	Nmap timing details are found on the bottom of this linked page
Match Hostname	Yes	• ?	https://nmap.org/book/man-performance.html. From that page:
Match Hostname Dbus	Yes	• ?	If you are on a decent broadband or ethernet connection,
Match Hostname Serial	Yes	- ?	people love -T5 (Insane) though it is too aggressive for
	Yes	• ?	my taste. People sometimes specify -T2 (Polite) because they think it is less likely to crash hosts or because they
Match Hostname Uuid			consider themselves to be polite in general. They often don't realize just how slow -T2 really is. Their scan may
Match Hostname Uuid	Man	- 2	tale ta time lange the set of the set Markins
Match Hostname Uuid Match IP	Yes	• ?	areabaa and bandwidth arabiama are rare with the d-f
Match Hostname Uuid Match IP Match Mac	Yes Yes	- ?	crashes and bandwith problems are rare with the default timing options -T3 (Normal) and so I normally recommend
Match Hostname Uuid Match IP Match Mac Match Mac Vmware	Yes Yes No	• ? • ? • ?	case et intres outpart uter a detaut scart, wachine crashes and banger turn a detaut scart, wachine timing options -13 (Normal) and so 1 normally recommend that for cautious scanners. Omitting version detection is far more effective than playing with timing values at
Match Hostname Uuid Match IP Match Mac Match Mac Vmware Match Serial	Yes No Yes	• ? • ? • ? • ?	crashes and hardwidth problems are rare with the default crashes and hardwidth problems are rare with the default timing options -T3 (Normai) and so I normally recommend that for caulious scanners. Omitting version detection is far more effective than playing with timing values at reducing these problems.
Match Hostname Uuid Match IP Match Mac Match Mac Vriware Match Serial Match Serial Type	Yes	 ? ? ? ? ? ? ? 	crashes and barger turar a deviatil scale. Machine crashes and barger turar a deviatil scale. Machine timing options -T3 (Normai) and so 1 normally recommend that for calutous scanners. Once thing version detection is far more effective than playing with timing values at reducing these problems. — Genton Pyotor Lyon
Match Hostname Uuid Match IP Match Mac Match Mac Vmware Match Serial Match Serial Type Match Uuid	Yes No Yes Yes Yes Yes Yes	 ? 	crashes and bandwich problems are rare with the default crashes and bandwich problems are rare with the default timing options -T3 (Normai) and so I normally recommend that for cautious scanners. Ownitting version detaction is far more effective than playing with timing values at reducing these problems. — Gorden Fyeder Lyon

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.

Casooveries / 122 108 88 0		Image: Condition per page to 27 of 27 entrines 192.168.88.1 computer 192.168.88.1 computer 192.168.88.1 computer 192.168.88.4 computer 192.168.88.4 192.168.88.4 192.168.88.10 computer 192.168.88.20 192.168.88.20 192.168.88.31 192.168.88.51 192.168.88.52 undroputer 192.168.88.52 undroputer		Name 0 Wind 0 Gymanitek.com 0 Gymanitek.com 0 Hornamitek.com 0 Gymanitek.com 0	Identification Identification Corported running Linux from TP-Link Identification Server from TP-Linux Identification Corported running Linux from TP-Link Identification Server from TP-Linux Identification Server from TP-Link Identification Server from Gigatry to Technology Con-Link Identification Server from Gigatry to Technology Con-Link Identification Server from Gigatry to Technology Con-Link Identification Virtual server from VMware, Inc. Identification	SMAP detected, but no valid SNAP credentials found for 152, 168,88,1.	2019-02-08 2019-02-08 15:43-05 2019-02-08 15:43-05 2019-02-08 15:43-05 2019-02-08 15:43-05 2019-02-08 15:43-05 2019-02-08 15:44-02 15:44-02 2019-02-08 15:44-02 15:44-02 2019-02-08 15:44-02 15:44-02 2019-02-08 15:44-02 2019-02-08 15:44-02 2019-02-08 15:44-02 2019-02-08 15:44-02 2019-02-08 15:44-02 2019-02-08 15:44-02 2019-02-08 15:44-02 2019-02-08 15:44-02 2019-02-08 15:44-02 2019-02-08 15:44-02 2019-02-08 15:44-02 2019-02-08 15:44-02 2
2:168.86.0	All Professional Constraints of the second s	conds per page to 27 of 27 entries 192.168.88.1 computer 192.168.88.6 computer 192.168.88.7 computer 192.168.88.7 computer 192.168.88.7 computer 192.168.88.7 computer 192.168.88.10 computer 192.168.88.10 computer 192.168.88.10 computer 192.168.88.10 computer 192.168.88.10 computer 192.168.88.11 192.168.88.12 192.168.88.14 computer 192.168.88.51 192.168.88.51 192.168.88.52 uhrome		Name Pame Will opmantek.com Commutek.com Odr opmantek.com Commutek.com opmantek.com		SNAP detected, but no valid SNAP credentials for for 182, 168,88,7 SNAP detected, but no valid SNAP credentials for for 182, 168,88,7 SNAP detected, but no valid SNAP credentials for for 182, 168,88,7 SNAP detected, but no valid SNAP credentials for for 182, 168,88,6 SNAP detected, but no valid SNAP credentials for for 182, 168,88,14	Next Last Next Last 2019-02-08 15:43-29 15:43-29 2019-02-08 15:43-29 2019-02-08 15:43-29 2019-02-08 15:43-29 2019-02-08 15:43-29 2019-02-08 15:54-41 2019-02-08 15:54-10 2019-02-08 15:54-11 2019-02-08 15:54-12 2019-02-08 15:54-12 2019-02-08 15:54-12 2019-02-08 15:54-12 2019-02-08 15:54-12 2019-02-08 15:54-12 2019-02-08 15:54-12 2019-02-08 15:54-12 2019-02-08 15:54-12 2019-02-08 15:54-12 2019-02-08 15:54-12 2019-02-08 15:54-12 2019-02-08
mmay mais ge de la serie de la	All v recent of the second sec	to Z7 of Z7 of Z7 of thirding 192 168.08.1 192.168.08.7 computer 192.168.08.10 computer 192.168.08.11 computer 192.168.08.14 computer 192.168.08.45 computer 192.168.08.52 computer		Name Opfinatelic Cond Opfinatelic Cond <td>Devices identification Concluder running Linux from TP-Linux Server from TP Concluder running Linux from HP Starter from UMaren, Inc. Starter from UMaren, Inc. Virtual server from UMaren, Inc. Dividual server from UMaren, Inc. Virtual server from UMaren, Inc. Vi</td> <td>Search: First Previous SSH detected, but no valid SSH oredentials for 122.168.88.1 SSH detected, but no valid SNMP credentials found for 122.168.88.7 SSMP detected, but no valid SNMP credentials found for 122.168.88.8 SSH detected, but no valid SNMP credentials for 122.168.88.20 SSMP detected, but no valid SSH credentials for 122.168.88.20 SSMP detected, but no valid SSH credentials for 122.168.88.20 SSMP detected, but no valid SSH credentials for 122.168.88.20 SSMP detected, but no valid SSH credentials for 122.168.88.20 SSMP detected, but no valid SSH credentials for 122.168.88.20 SSMP detected, but no valid SSH credentials for 122.168.88.20 SSMP detected, but no valid SSH credentials for 123.168.88.20 SSMP detected, but no valid SSH credentials for 123.168.88.20 SSMP detected, but no valid SSH credentials for 123.168.84.20 SSMP detected, but no valid SSH credentials for 123.168.84.20 SSMP detected, but no valid SSH credentials for 123.168.84.20 SSMP detected, but no valid SSH credentials for 123.168.84.20 SSMP detected, but no valid SSH credentials for 123.168.84.20 SSMP detected, but no valid SSH credentials for 123.168.84.20 SSMP detected, but no valid SSH credentials for 123.168.84.20 SSMP detected, but no valid SSH credentials for 123.168.84.20 SSMP detected, but no valid SSH credentials for 123.168.84.20 SSMP detected, but no valid SSH credentials for 123.168.84.20 SSMP detected, but no valid SSH credentials for 123.168.85.20 SSMP detected, but no valid SSH credentials for 123.168.85.20 SSMP detected, but no valid SSH credentials for 123.168.85.20 SSMP detected, but no valid SSH credentials for 123.168.85.20 SSMP detected, but no valid SSH credentials for 123.168.85.20 SSMP detected, but no valid SSH credentials for 123.168.85.20 SSMP detected, but no valid SSH credentials for 123.168.85.20 SSMP detected, but no valid SSH credentials for 123.168.85.20 SSMP detected, but no valid SSH credentials for 123.168.85.20 SSMP detected, but no valid SSH credentials for 123.168.85.20 SSMP detected, but no valid S</td> <td>Next Last 2019-02-08 15:43:40 2019-02-08 15:43:40 2019-02-08 15:43:50 2019-02-08 15:43:50 2019-02-08 15:44:50 2019-02-08 15:44:00 2019-02-08 15:44:00 2019-02-08 15:44:10 2019-02-08 15:44:10 2019-02-08 15:44:12 2019-02-08 15:44:12 2019-02-08 15:44:12 2019-02-08 15:44:12 2019-02-08 15:44:12 2019-02-08 15:44:12 2019-02-08 15:44:12 2019-02-08 15:44:12 2019-02-08 15:44:12</td>	Devices identification Concluder running Linux from TP-Linux Server from TP Concluder running Linux from HP Starter from UMaren, Inc. Starter from UMaren, Inc. Virtual server from UMaren, Inc. Dividual server from UMaren, Inc. Virtual server from UMaren, Inc. Vi	Search: First Previous SSH detected, but no valid SSH oredentials for 122.168.88.1 SSH detected, but no valid SNMP credentials found for 122.168.88.7 SSMP detected, but no valid SNMP credentials found for 122.168.88.8 SSH detected, but no valid SNMP credentials for 122.168.88.20 SSMP detected, but no valid SSH credentials for 122.168.88.20 SSMP detected, but no valid SSH credentials for 122.168.88.20 SSMP detected, but no valid SSH credentials for 122.168.88.20 SSMP detected, but no valid SSH credentials for 122.168.88.20 SSMP detected, but no valid SSH credentials for 122.168.88.20 SSMP detected, but no valid SSH credentials for 122.168.88.20 SSMP detected, but no valid SSH credentials for 123.168.88.20 SSMP detected, but no valid SSH credentials for 123.168.88.20 SSMP detected, but no valid SSH credentials for 123.168.84.20 SSMP detected, but no valid SSH credentials for 123.168.84.20 SSMP detected, but no valid SSH credentials for 123.168.84.20 SSMP detected, but no valid SSH credentials for 123.168.84.20 SSMP detected, but no valid SSH credentials for 123.168.84.20 SSMP detected, but no valid SSH credentials for 123.168.84.20 SSMP detected, but no valid SSH credentials for 123.168.84.20 SSMP detected, but no valid SSH credentials for 123.168.84.20 SSMP detected, but no valid SSH credentials for 123.168.84.20 SSMP detected, but no valid SSH credentials for 123.168.84.20 SSMP detected, but no valid SSH credentials for 123.168.85.20 SSMP detected, but no valid SSH credentials for 123.168.85.20 SSMP detected, but no valid SSH credentials for 123.168.85.20 SSMP detected, but no valid SSH credentials for 123.168.85.20 SSMP detected, but no valid SSH credentials for 123.168.85.20 SSMP detected, but no valid SSH credentials for 123.168.85.20 SSMP detected, but no valid SSH credentials for 123.168.85.20 SSMP detected, but no valid SSH credentials for 123.168.85.20 SSMP detected, but no valid SSH credentials for 123.168.85.20 SSMP detected, but no valid SSH credentials for 123.168.85.20 SSMP detected, but no valid S	Next Last 2019-02-08 15:43:40 2019-02-08 15:43:40 2019-02-08 15:43:50 2019-02-08 15:43:50 2019-02-08 15:44:50 2019-02-08 15:44:00 2019-02-08 15:44:00 2019-02-08 15:44:10 2019-02-08 15:44:10 2019-02-08 15:44:12 2019-02-08 15:44:12 2019-02-08 15:44:12 2019-02-08 15:44:12 2019-02-08 15:44:12 2019-02-08 15:44:12 2019-02-08 15:44:12 2019-02-08 15:44:12 2019-02-08 15:44:12
tatas ps Moos Addresses	All	Ipp: 4 Ipp: 4 IP Ipp: 168.38.1 Ipp: 168.38.7 192.168.38.7 Ipp: 168.38.7 Ipp: 168.38.7 192.168.38.7 Ipp: 168.38.7 Ipp: 168.38.7 192.168.38.1 Ipp: 168.38.1 Ipp: 168.38.1 192.168.38.45 Ipp: 168.38.2 Ipp: 168.38.2		Name Image: Constraint of the constr	Identification Image: Computer running Linux from TP-Link Computer running Linux from TP-Link Image: Computer running Linux from HP Computer running Linux from HP Image: Computer running Linux from HP Stream from Gigabyte Tachnology Cox. Image: Computer running Linux from HP Stream from Gigabyte Tachnology Cox. Image: Computer running Linux from HP Virtual server from VMware, Inc. Image: Computer running SSH Virtual server from VMware, Inc. Image: Computer running SSH Virtual server from VMware, Inc. Image: Computer running SSH Virtual server from VMware, Inc. Image: Computer running SSH Virtual server from VMware, Inc. Image: Computer running SSH Virtual server from VMware, Inc. Image: Computer running SSH Virtual server from VMware, Inc. Image: Computer running SSH Virtual server from VMware, Inc. Image: Computer running SSH Virtual server from VMware, Inc. Image: Computer running SSH Virtual server from VMware, Inc. Image: Computer running SSH Virtual server from VMware, Inc. Image: Computer running SSH Virtual server from VMware, Inc. Image: Computer running SSH Virtual server from VMware, Inc. Image: Computer running SSH	SNAP detected, but no valid SNAP codentials form for 182, 168,88,14 SNAP detected, but no valid SNAP codentials form for 182, 168,88,14 SNAP detected, but no valid SNAP codentials form for 182, 168,88,14 SNAP detected, but no valid SNAP codentials form for 182, 168,88,14 SNAP detected, but no valid SNAP codentials form for 182, 168,88,14 SNAP detected, but no valid SNAP codentials form for 182, 168,88,14 SNAP detected, but no valid SNAP codentials form for 182, 168,88,14 SNAP detected, but no valid SNAP codentials form for 182, 168,88,14 SNAP detected, but no valid SNAP codentials form for 182, 168,88,14 SNAP detected, but no valid SNAP codentials form for 182, 168,88,14 SNAP detected, but no valid SNAP codentials form for 182, 168,88,14	Next Last 2019-02-08 15:543-08 15:543-08 2019-02-08 15:43-52 2019-02-08 15:43-52 2019-02-08 15:54-08 2019-02-08 15:54-08 2019-02-08 15:54-08 2019-02-08 15:54-12 2019-02-08 15:54-12 2019-02-08 15:54-12 2019-02-08 15:54-12 2019-02-08 15:54-12 2019-02-08 15:54-12 2019-02-08 15:54-12 2019-02-08 15:54-12 2019-02-08 15:54-12 2019-02-08 15:54-12 2019-02-08 15:54-12 2019-02-08 15:54-12 2019-02-08 15:54-12 2019-02-08 15:54-12 2019-02-08 15:54-12 2019-02-08 15:54-12 2019-02-08 15:54-12 2019-02-08
gs (2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2	All e View 0 O 0	Ip Im IP <		Name I Odr I Odr I Odr I Odramatek.com I	Identification I Conputer running Linux from TP-Link Sarver from HP Conguter running Linux from HP I Virtual server from YMware, Inc. I Sarver from Gigabyte Technology Co., I Virtual server from YMware, Inc. I	SNMP detected, but no valid SNMP credentials form for 182, 168,88,14 SSH detected, but no valid SNMP credentials form for 182, 168,88,7 SNMP detected, but no valid SNMP credentials form for 182, 168,88,7 SNMP detected, but no valid SNMP credentials form for 182, 168,88,14 SSH detected, but no valid SNMP credentials form for 182, 168,88,14 SSH detected, but no valid SSH credentials form for 182, 168,88,14 SSH detected, but no valid SSH credentials form for 182, 168,88,14 SSH detected, but no valid SSH credentials form for 182, 168,88,14 SSH detected, but no valid SSH credentials form for 182, 168,88,14 SSH detected, but no valid SSH credentials form for 182, 168,88,14 SSH detected, but no valid SSH credentials form for 182, 168,88,14 SSH detected, but no valid SSH credentials form for 182, 168,88,14 SSH detected, but no valid SSH credentials form for 182, 168,88,14 SSH detected, but no valid SSH credentials form for 182, 168,88,14 SSH detected, but no valid SSH credentials form for 182, 168,88,14 SSH detected, but no valid SSH credentials form for 182, 168,88,14 SSH detected, but no valid SSH credentials form for 182, 168,88,14 SSH detected, but no valid SSH credentials form for 182, 168,88,14 SSH detected, but no valid SSH credentials form for 182, 168,88,14 SSH detected, but no valid SSH credentials form for 182, 168,88,14 SSH detected, but no valid SSH credentials form form form form form form form form form	Next Last Last 2019-02:08 15:43:49 2019-02:08 15:43:52 2019-02:08 15:43:52 2019-02:08 15:54:05 2019-02:08 15:54:05 2019-02:08 15:54:40 2019-02:08 15:54:41 2019-02:08 15:54:41 2019-02:08 15:54:41 2019-02:08 15:54:42 2019-02:08 15:54:42 2019-02:08 15:54:42 2019-02:08 15:54:42 2019-02:08 15:54:42 2019-02:08 15:54:22 2019-02:08 15:54:22 2019-02:08
Addresses		IP 192.168.88.1 computer 192.168.88.1 computer 192.168.88.1 192.168.88.1 computer 192.168.88.1 computer 192.168.88.10 computer 192.168.88.10 computer 192.168.88.10 computer 192.168.88.10 192.168.88.10 192.168.88.10 192.168.88.10 192.168.88.10 192.168.88.10 192.168.88.10 192.168.88.10 192.168.88.10 192.168.88.10 192.168.88.10 192.168.88.10 192.168.88.10 192.168.88.10 192.168.88.52 Unorder 192.168.88.52		Ame Image: Comparison of Com	Autolitation Computer running Linux from TP-Link Sarver from HP Computer running Linux from HP Vitual server from VMware, Inc. Sarver from Gigabyte Technology Co., Sarver from Gigabyte Technology Co., Vitual server from VMware, Inc.	SNMP detected, but no valid SNMP credentials form for 182, 168,88,1 (2014) SNMP detected, but no valid SNMP credentials form for 182, 168,88,7 (2014) SNMP detected, but no valid SNMP credentials found for 182, 168,88,8 (2014) SNMP detected, but no valid SNMP credentials form for 182, 168,88,1 (2014) SSM detected but no valid SSM credentials form for 182, 168,88,1 (2014) SSM detected but no valid SSM credentials form for 182, 168,88,1 (2014) SSM detected but no valid SSM credentials form for 182, 168,88,1 (2014) SSM detected but no valid SSM credentials form for 182, 168,88,1 (2014) SSM detected, but no valid SSM credentials form for 182, 168,88,1 (2014) SSM detected, but no valid SSM credentials form for 182, 168,88,1 (2014) SSM detected, but no valid SSM credentials form for 182, 168,88,1 (2014) SSM detected, but no valid SSM credentials form for 182, 168,88,1 (2014) SSM detected, but no valid SSM credentials form for 182, 168,88,1 (2014) SSM detected, but no valid SSM credentials form for 182, 168,88,1 (2014) SSM detected, but no valid SSM credentials form for 182, 168,88,1 (2014) SSM detected, but no valid SSM credentials form for 182, 168,88,1 (2014) SSM detected, but no valid SSM credentials form for 182, 168,88,1 (2014) SSM detected, but no valid SSM credentials form for 182, 168,88,1 (2014) SSM detected, but no valid SSM credentials form for 182, 168,88,1 (2014) SSM detected, but no valid SSM credentials for 182, 168,88,1 (2014) SSM detected, but no valid SSM credentials for 182, 168,88,1 (2014) SSM detected, but no valid SSM credentials for 182, 168,88,1 (2014) SSM detected, but no valid SSM credentials for 182, 168,88,1 (2014) SSM detected, but no valid SSM credentials for 182, 168,88,1 (2014) SSM detected, but no valid SSM credentials for 182, 168,88,1 (2014) SSM detected, but no valid SSM credentials for 182, 168,88,1 (2014) SSM detected, but no valid SSM credentials for 182, 168,88,1 (2014) SSM detected, but no valid SSM credentials for 182, 168,88,1 (2014) SSM detected, but no valid SSM credentials	Last Seen 2019-02-08 15:43-94 2019-02-08 15:43-52 2019-02-08 15:43-52 2019-02-08 15:43-52 2019-02-08 15:44-05 2019-02-08 15:44-10 2019-02-08 15:44-12 2019-02-08 15:44-12 2019-02-08 15:44-12 2019-02-08 15:44-23 2019-02-08
		192.168.88.1 computer 192.168.88.6 computer 192.168.88.7 computer 192.168.88.9 computer 192.168.88.9 computer 192.168.88.10 computer 192.168.88.14 computer 192.168.88.15 computer 192.168.88.20 unclassified 192.168.88.51 computer 192.168.88.48 computer 192.168.88.48 computer 192.168.88.51 computer 192.168.88.51 computer 192.168.88.51 computer 192.168.88.51 computer		wfl qpmatele.com dqmatele.com magnitematele.com thormantele.com qpmate	Computer running Linux from TP-Link Technology Server from HP Computer running Linux from HP Virtual server from VMware, Inc. Server from Gigateyte Technology Co., Ltd. Virtual server from VMware, Inc. Utual server from VMware, Inc. Utual server from VMware, Inc. Virtual server from VMware, Inc. Virtual server from VMware, Inc. Virtual server from VMware, Inc. Virtual server from VMware, Inc.	SSH detected, but no valid SSH oredentials for 192, 168,88,1.	2019-02-08 15:543-52 2019-02-08 15:543-52 2019-02-08 15:543-52 2019-02-08 15:54-00 15:544-00 2019-02-08 15:544-10 2019-02-08 15:544-10 2019-02-08 15:544-20 2019-02-08 15:544-20 2019-02-08 15:544-20 2019-02-08
		192.168.88.6 computer 192.168.88.7 computer 192.168.88.9 computer 192.168.88.9 computer 192.168.88.10 computer 192.168.88.14 192.168.88.15 computer 192.168.88.50 unclassified 192.168.88.48 computer 192.168.88.48		ord operated com operated com o	Server from HP Computer running Linux from HP Virtual server from VMware, Inc. Server from Gigabyte Technology Co., Lid. Virtual server from VMware, Inc. Device running SSH Virtual server from VMware, Inc. Lid. Virtual server from VMware, Inc. Lid. Virtual server from VMware, Inc. Lid. No information could be retrieved.	SNUP-detected, but no valid SNMP credentials found for 192.168.88.7 SNMP-detected, but no valid SNMP credentials found for 192.168.88.14 SSM detected, but no valid SNMP credentials found for 192.168.88.14 SSM detected, but no valid SSM prodentials for 192.168.88.00 No valid credentials for 192.168.88.20 SNMP-detected, but no valid SNMP credentials found for 192.168.84.4	2019-02-08 15:43-55 2019-02-08 15:43-55 2019-02-08 15:43-55 2019-02-08 2019-02-08 2019-02-08 15:44:10 2019-02-08 15:44:12 2019-02-08 2019-02-08 2019-02-08
		192.168.88.7 computer 192.168.88.7 computer 192.168.88.9 computer 192.168.88.10 computer 192.168.88.10 computer 192.168.88.10 computer 192.168.88.10 computer 192.168.88.11 computer 192.168.88.15 computer 192.168.88.45 computer 192.168.88.45 computer 192.168.88.48 computer 192.168.88.51 192.168.88.51 192.168.88.52 unknown	 ? ?<	epinetmeter approximately.com et/s ef/s approximately.com et/s approximately.com app	Computer running Linux from HP Chitual server from VMware, Inc. Server from Gigabyte Technology Co., Lid. Server from Gigabyte Technology Co., Virtual server from VMware, Inc. Device running SSH Virtual server from VMware, Inc. Virtual server from VMware, Inc. Nitual server from VMware	SNMP detected, but no valid SNMP credentials found for 1192, 168,88,7 SNMP detected, but no valid SNMP credentials found for 1192, 168,88,8 SNMP detected, but no valid SNMP credentials for 192, 168,88,14 SSH detected but no valid SSH credentials for 192, 168,88,20 No valid credentials for 192, 168,88,20 SNMP detected, but no valid SNMP credentials found for 192, 168,88,48	2019-02-08 15-43-55 2019-02-08 15-43-57 2019-02-08 15-44-08 2019-02-08 15-44-08 2019-02-08 15-44-10 2019-02-08 2019-02-08 2019-02-08 2019-02-08
		Computer 192.168.88.9 computer 192.168.88.9 computer 192.168.88.10 computer 192.168.88.10 computer 192.168.88.15 computer 192.168.88.15 computer 192.168.88.45 computer 192.168.88.45 computer 192.168.88.45 computer 192.168.88.45 computer 192.168.88.45 computer 192.168.88.45 computer 192.168.88.51 computer 192.168.88.51 computer 192.168.88.51 computer		epiniamento deprination entry	Virtual server from VMware, Inc. Server from Gigsbyte Technology Co., List. Server from Gigsbyte Technology Co., Virtual server from VMware, Inc. Device running SSH Virtual server from VMware, Inc. Virtual server from VMware, Inc. Virtual server from VMware, Inc. Ninter Server from VMware, Inc. Server from VMware, Inc. Ninter Server from VMware, In	No Ind. Cesso J Cost of Cost o	13.3433 2019.02.08 2019.02.08 15.343.57 2019.02.08 15.34.05 2019.02.08 15.34.05 2019.02.08 15.34.12 2019.02.08 2019.02.08 15.34.21 2019.02.08 2019.02.08
		Computer 192.168.88.9 computer 192.168.88.10 computer 192.168.88.10 computer 192.168.88.14 computer 192.168.88.15 computer 192.168.88.45 computer 192.168.88.45 computer 192.168.88.45 computer 192.168.88.51 computer 192.168.88.51 computer 192.168.88.52		epinamek.com eris opmantek.com odin snotra opmantek.com opmantek.com opmantek.com magni-mgmt opmantek.com crash-n-burn opmantek.com comantek.com snorri opmantek.com	Server from Gigabyte Technology Co., Ltd. Server from Gigabyte Technology Co., Ltd. Virtual server from VMware, Inc. Device running SSH Virtual server from VMware, Inc. Virtual server from VMware, Inc. Virtual server from VMware, Inc. Nitial server from VMware, Inc.	Nor TH2, Tes.38.4 State of the second	15/435/ 2019-02/08 15/44/01 2019-02/08 15/44/05 2019-02/08 15/44/08 2019-02/08 15/44/12 2019-02/08 15/44/17 2019-02/08 15/44/21 2019-02/08 15/44/21 2019-02/08 15/44/24
		computer 192.168.88.10 computer 192.168.88.14 computer 192.168.88.15 computer 192.168.88.45 computer 192.168.88.45 computer 192.168.88.45 computer 192.168.88.51 192.168.88.51 192.168.88.52 unknown		ogmantek.com odin gemantek.com snotra opmantek.com offen gemantek.com offen gemantek.com organitek.com crash-n-burn opmantek.com uburnto opmantek.com snorri opmantek.com	Lid. Server from Gigabyte Technology Co., Lid. Virtual server from VMware, Inc. Davice running SSH Virtual server from VMware, Inc. Virtual server from VMware, Inc. Virtual server from VMware, Inc. No information could be retrieved.	SNMP detected, but no valid SNMP credentials found for 182, 168,88,14	15.44.01 2019-02.08 15.44.05 2019-02.08 15.44.09 2019-02.08 15.44.10 2019-02.08 15.44.12 2019-02.08 15.44.21 2019-02.08 15.44.21 2019-02.08
		computer 192.168.88.14 computer 192.168.88.15 computer 192.168.88.20 unclassified 192.168.88.45 computer 192.168.88.48 computer 192.168.88.51 192.168.88.52 unknown		opmantek.com snotra.com opmantek.com magni-ringmt opmantek.com cpmantek.com cpmantek.com uburnto opmantek.com snorri opmantek.com	Lid. Unit of the second	SNMP detected, but no valid SNMP credentials found for 192.168.88.14	15:44:05 2019-02:08 15:44:09 2019-02:08 2019-02:08 15:44:14 2019-02:08 2019-02:08 15:44:24 2019-02:08
		192.168.88.15 computer 192.168.88.15 computer 192.168.88.20 Linclassification 192.168.88.45 computer 192.168.88.45 computer 192.168.88.45 computer 192.168.88.45 computer 192.168.88.51 computer 192.168.88.51 192.168.88.52 unchnolm 192.168.88.52	** ** * * * * * * * * * * *	opmantek.com opmantek.com magni-mgmt opmantek.com crash-n-burn opmantek.com uburnto opmantek.com snorri opmantek.com	Virtual server from VMware, Inc. Nitual server from VMware, Inc. No information could be retrieved,	SNMP detected, but no valid SNMP credentials for SNMP detected, but no valid SNH predentials for SNMP detected, but no valid SNMP credentials found for 152, 168,88,48	2019-02-08 15:44:09 2019-02-08 15:44:12 2019-02-08 15:44:14 2019-02-08 15:44:21 2019-02-08 15:44:24 2019-02-08 15:44:24
		192.168.88.15 computer 192.168.88.20 unclassified 192.168.88.45 computer 192.168.88.45 computer 192.168.88.51 computer 192.168.88.51 computer 192.168.88.52 unknown	** ** (*) (*) (*) (*) (*) (*) (*	odem opmantek.com magni-mgmt opmantek.com uburnto opmantek.com uburnto opmantek.com snorri opmantek.com	Virtual server from VMware, Inc. Device running SSH Virtual server from VMware, Inc. Virtual server from VMware, Inc. Virtual server from VMware, Inc. No information could be retrieved.	SSH detected but no valid SSH credentials for 122:168.88.20. No valid credentials for 152:168.88.20 SNMP detected, but no valid SNMP credentials found for 152:168.88.48 No management protocols for 192:168.88.52	2019-02-08 15:44:12 2019-02-08 15:44:14 2019-02-08 15:44:17 2019-02-08 15:44:21 2019-02-08 15:44:24 2019-02-08
		192.168.88.20 unclassified 192.168.88.45 computer 192.168.88.48 192.168.88.51 computer 192.168.88.52 unknown	♀ ◆ ● ○ ▲	magni-mgmt opmantek.com crash-n-burn opmantek.com uburnto opmantek.com snorri opmantek.com	Device running SSH Virtual server from VMware, Inc. Virtual server from VMware, Inc. Virtual server from VMware, Inc. No information could be retrieved.	SSH detected but no valid SSH coedentials for 1922-168.88.20 No valid createntials for 1922-168.88.20 SNMP detected, but no valid SNMP credentials found for 1922-168.88.48 No management protocols for 1922-168.88.52	2019-02-08 15:44:14 2019-02-08 15:44:17 2019-02-08 15:44:21 2019-02-08 15:44:24 2019-02-08
		192,168.88.45 computer 192,168.88.48 computer 192,168.88.51 computer 192,168.88.52 unknown 192,168.88.52	* (© ()	crash-n-burn opmantek.com uburnto opmantek.com snorri opmantek.com 192.168.88.52	Virtual server from VMwaro, Inc. Virtual server from VMwaro, Inc. Virtual server from VMwaro, Inc. No information could be retrieved.	SNMP detected, but no valid SNMP credentials found for 192.168.88.48	2019-02-08 15:44:17 2019-02-08 15:44:21 2019-02-08 15:44:24 2019-02-08
	0	192.168.88.48 computer 192.168.88.51 computer 192.168.88.52 unknown 192.168.88.52	⊙▲	uburnto opmantek.com snorri opmantek.com 192.168.88.52	Virtual server from VMware, Inc. Virtual server from VMware, Inc. No information could be retrieved.	SNMP detected, but no valid SNMP credentilats found for 192.168.88.49	2019-02-08 15:44:21 2019-02-08 15:44:24 2019-02-08
		192.168.88.51 computer 192.168.88.52 unknown	© ▲	snorri opmantek.com 192.168.88.52	Virtual server from VMware, Inc.	No management protocols for 192.168.88.52	2019-02-08 15:44:24 2019-02-08
	•	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
	Φ	102 168 88 52					15:44:27
		computer	4	red-burn opmantek.com	Virtual server from VMware, Inc.		2019-02-08 15:44:30
	Φ	192.168.88.54 computer	4	sun-burn opmantek.com	Virtual server from VMware, Inc.		2019-02-08 15:44:33
	Φ	192.168.88.55 computer	-	se7en opmantek.com	Virtual server from VMware, Inc.		2019-02-08 15:44:35
	Q	192.168.88.56 unclassified	Q	192.168.88.56	Device running WMI (likely a Windows computer)	WMI detected but no valid Windows credentials for 192.168.88.56. No valid credentials for 192.168.88.56	2019-02-08 15:44:39
	Q.	192.168.88.57 computer	0	idontknow opmantek.com	Virtual server from VMware, Inc.		2019-02-08 15:44:41
	P	192.168.88.60 unclassified		192.168.88.60	Device running SSH	SSH detected but no valid SSH credentials for 192.168.88.60. No valid credentials for 192.168.88.60	2019-02-08 15:44:44
	Q	192.168.88.62 unclassified	P	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	Q	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
	D	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
	P	192.168.88.73 computer	0	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
	Q	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	2019-02-08 15:44:56
	Φ	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
	Q	192.168.88.253 switch	-	midgard opmantek.com	Switch from Cisco Systems		2019-02-08 15:45:01
	Q	192.168.88.254	9	asgard opmantek.com	Router from Cisco Systems		2019-02-08
SI	Showing 1	to 27 of 27 entries				First Previous	Next Last

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.