New Discovery 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.

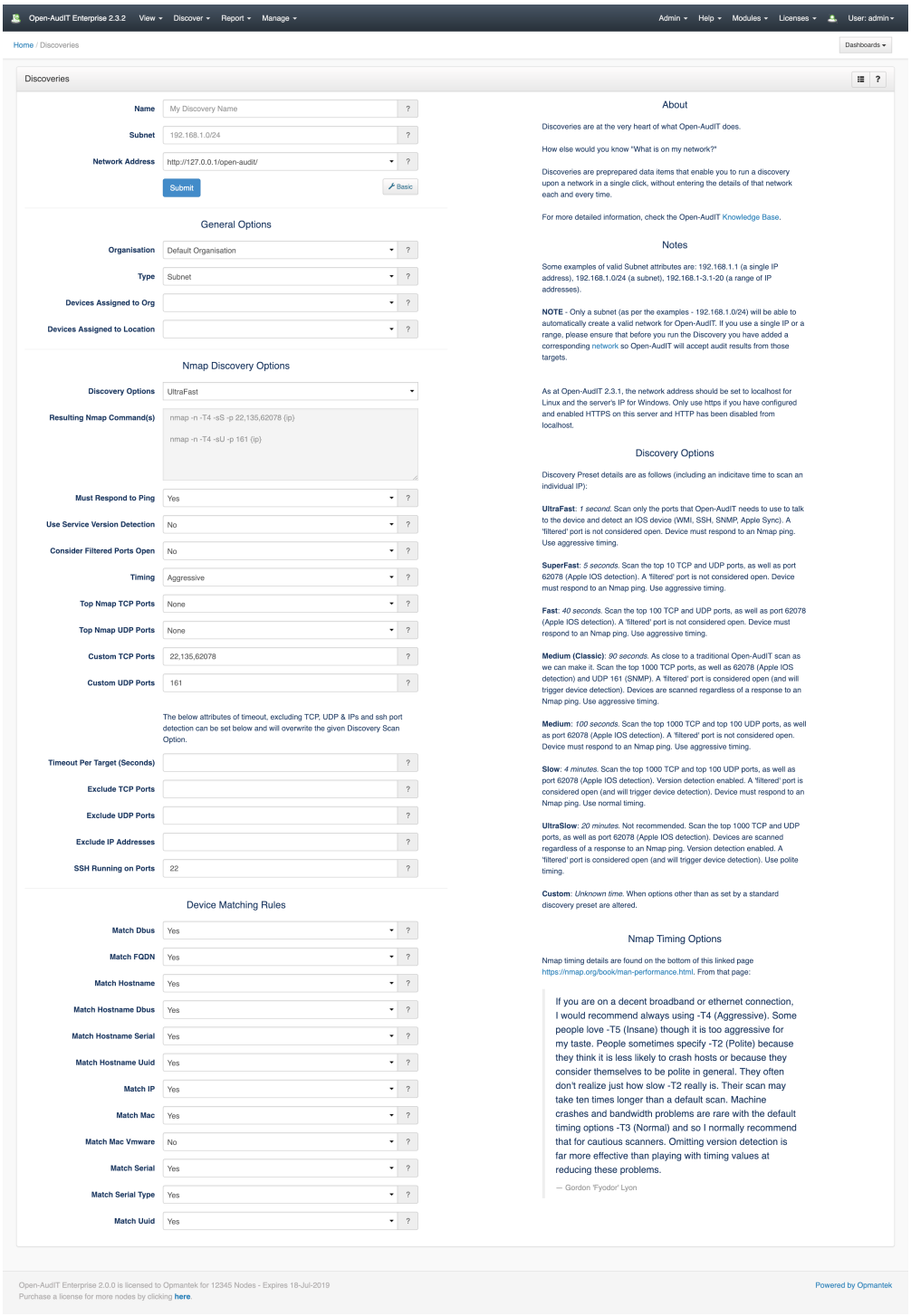
Filtered Ports

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.



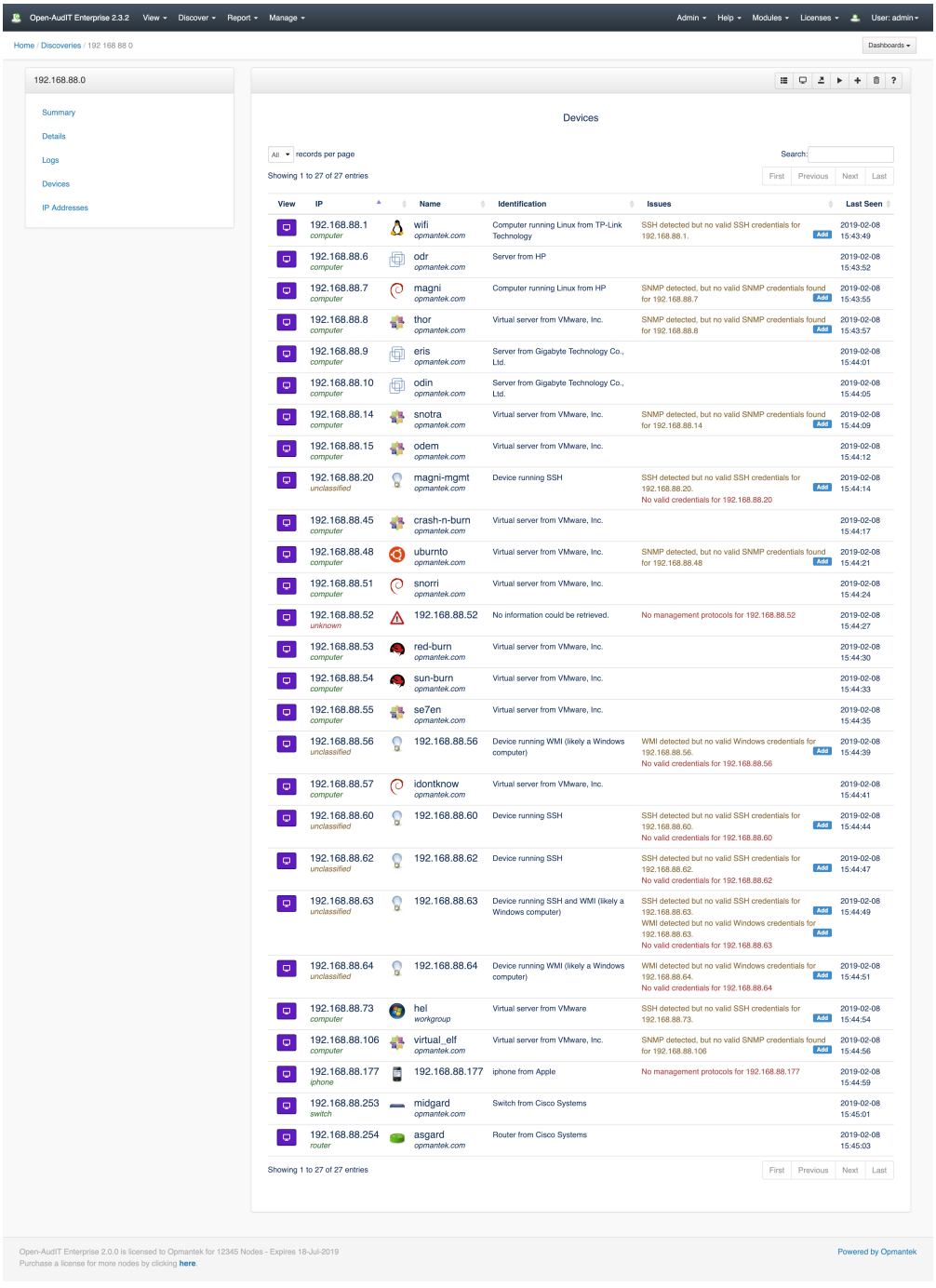
Check the wiki for a more detailed explanation about Discoveries

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.



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.