MANUAL

VERSION 4.02, 18th September, 2021

Contents

Summary: Legacy Inventory 2013 206

Technical Support and Contact Details

The **Help System** is accessed by clicking on the main Help Icon at the top of the Toolbox screen. The Help is automatically set-up to match the currently selected **Main Tab** and **Panel**. There is also a Search Facility that can search the whole of Toolbox Help and a search limited to a selected feature.

For ordering Toolbox licences and for technical support please contact:

sales@codimatech.com

support@codimatech.com

info@codimatech.com

North America USA
Philadelphia
Tel: +1 215 717 7377
Fax: +1 215 525 9682
e-mail: ussales@codimatech.com

EMEA UK
London
Tel: +44 (0)207 193 8165
e-mail: emeasales@codimatech.com

Latin America
Buenos Aires
Tel: +54-91133345639
e-mail: sasales@codimatech.com

Japan
Tokyo
Tel: +81 073-499-6588
e-mail: supportjp@codimatech.com
salesjp@codimatech.com

INTRODUCTION

System Requirements

Hardware Requirements

Any PC/Server that runs the Toolbox software must meet or surpass the listed specifications below. Every Toolbox version has the same hardware requirements, and these are as follows:

Processor	4 cores
Memory	8GB 64-bit
Hard Drive	Fast hard drive preferably an SSD

Software Requirements

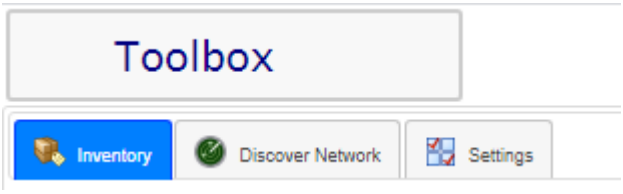
The following table shows compatible operating systems for the three Toolbox versions offered.
If you decide to get a Toolbox license with Visio mapping capability then you have several options as to the version of Visio you can use. The table below shows Visio compatibility in relation to operating systems.

	Windows 7	Windows 10
Toolbox (All Versions)	✓	✓
Visio Professional 2019	✗	✓
Visio Standard 2019	✗	✓
Visio Professional 2016	✓	✓
Visio Standard 2016	✓	✓
Visio Professional 2013	✓	✓
Visio Standard 2013	✓	✓

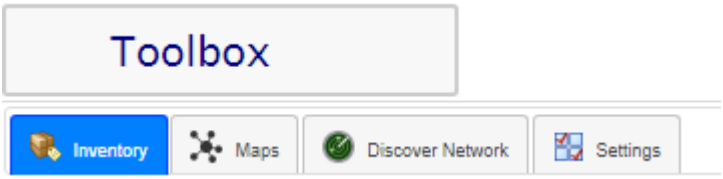
Toolbox Products

Toolbox is a web-based product that is viewed using a web browser and is naturally, a distributed architecture. **This version of the manual covers three Toolbox products, see list of supported products below:**

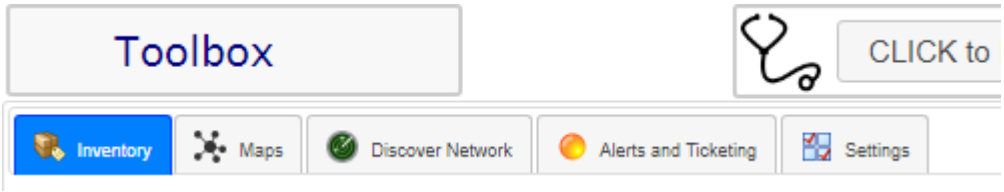
Network Inventory Toolbox
In this product these Tabs are available: Inventory, Discover Network and Settings.



Network Inventory with Maps in Web and Visio Toolbox
In this product these Tabs are available: Inventory, Maps, Discover Network and Settings.



Network Inventory with Maps in Web and Visio and Monitoring + Alert Ticketing Toolbox
In this product these Tabs are available: Inventory, Maps, Discover Network, Alerts & Ticketing, Settings.



Requirements to get a correct Toolbox licence

Useful Terminology

- **Managed Device** – Any device that responds to SNMP, WMI or NetBIOS, such as a PC, Printer, Server, Switch, Router, Firewall, etc.
- **Probe** - Probes are used to extend the geographic reach of the Network Discovery.
- **User** – Individual with access to the Toolbox software
- **PC** – A Personal Computer to install Toolbox onto
- **Server** – A PC that is either partially or fully dedicated to running Toolbox.

Steps to take in order to receive correct Toolbox license

1. There are two types of licenses that can be acquired, these are:
    a. **Free License** – A free license can be acquired here https://codimatech.com/en/free-download/. With this license you are limited up to 25 **Managed Devices** and grant the user full functionality of the software defined as Network Inventory with Maps in Web and Visio and Monitoring + Alert Ticketing Toolbox.
    Note: *With a free license the MAC-address of the PC/Server is not required*

    b. **Paid license** – A paid license can be acquired here https://codimatech.com/en/pricing/. There are several license agreements available in order to accommodate every need, these licenses have the option to decide the level of functionality that is required, the number of Managed devices, number of users, and the number of probes that can be utilized.
    Note: *With a paid license the MAC-address of the PC/Server the software will be downloaded on needs to be provided to Codima for it to work.*

    You only need to continue with these steps if you have or are going to purchase a license.

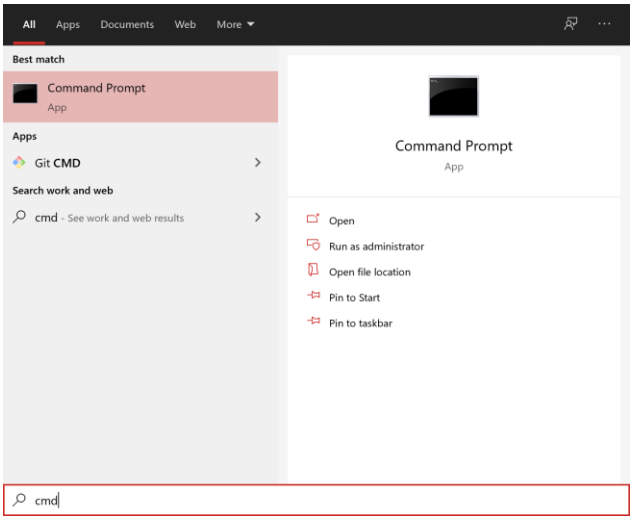
2. Decide the **number of users** that you need for your Toolbox.

3. To ensure you get the correct License for Toolbox estimate **how many Managed Devices** you have on your network.

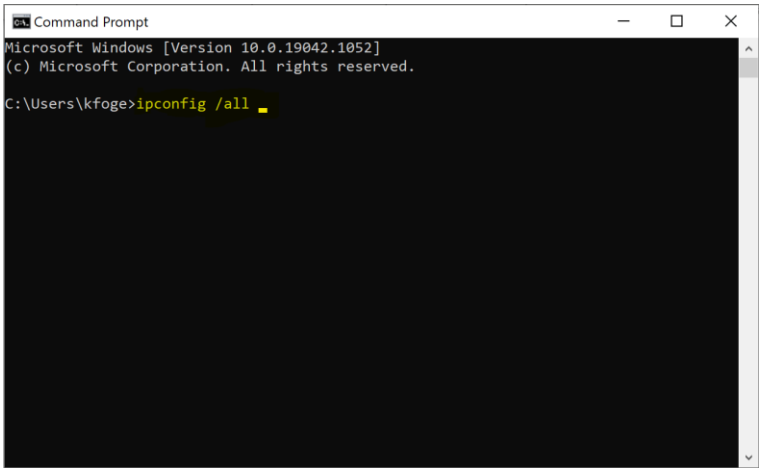
4. Determine the **number of Probes** to install to cover your network.

5. You also need the **Mac address** for the PC/server on which you plan to install the Toolbox on. To get a license please get the 12-digit HEX MAC address of the main network adaptor on the install PC by Following the steps below:

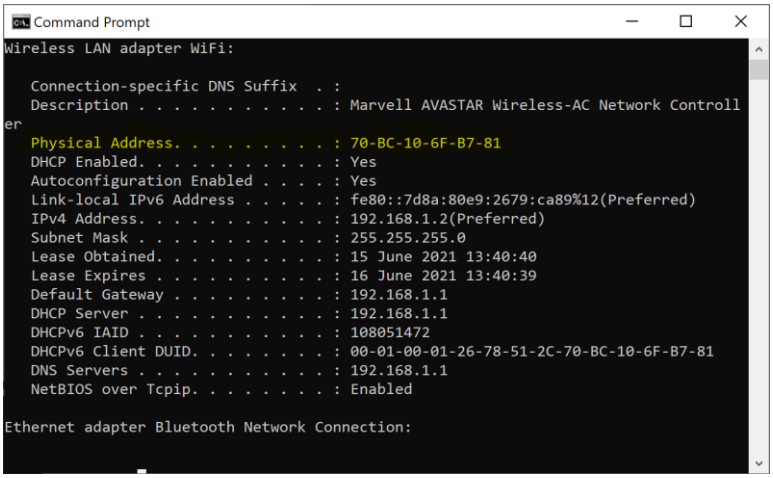
a. Go into Windows Start then type **cmd** and press **Enter**.



b. A DOS window will appear, type **ipconfig /all**



c. Check through the results for **Physical Address** in format AA:BB:CC:DD:EE:FF
See below marked in yellow



Installation

The following section describes installing Toolbox on a machine that has not had Toolbox software installed before. Both a quick guide and a step-by-step guide exists for your convenience.

Many Antivirus programs will interfere with installation, so disable them temporarily during Install. Be aware that key messages can sometimes be hidden by the current installation display window; check the bottom Windows Icon Bar for messages that can block installation.

Depending on your Operating System, either Windows 7 or 10, up to 6 prerequisites are bundled with the main Toolbox installer. These are:

1. Bitnami WAMP Stack New
2. Microsoft Visual C++ 2010 SP1 Redistributable Package (x86)
3. Microsoft Visual C++ 2013 Redistributable Package (x86)
4. Microsoft Visual C++ 2017 Redistributable Package (x86)
5. MySQL Connector ODBC 3.51.30
6. Win10PCap.

The Bitnami **WAMP** Stack Setup Wizard, which runs automatically during the Toolbox installation, will install a **W**indows **A**pache HTTP Server, a **M**ySQL database server and **P**HP.

Toolbox Installation – Quick Start

*This section is a very quick rundown of how to navigate the installation wizard for a more in-depth guide see **Toolbox Installation - Step by Step** just below.*

1. Temporarily disable any antivirus software that may be running on the PC/Server as it could interfere with the installation of Toolbox.
2. Open the Toolbox Setup Wizard that can be found either on the Codima website or through email after securing a license.
3. Simply accept the 'License Agreement' and click the Next button throughout the wizard.
4. Click the 'Finish' button to complete and exit the installer.
5. Once completed you may be asked to restart the PC, make sure to do this before running Toolbox.

Toolbox Installation - Step by Step

This section is a complete sequence of Toolbox product Install Setup Screens with added yellow highlighter mark-up. Folder Paths will vary for installs on 64-bit platforms but makes no difference to the installation process.

Before starting the installation process make sure to disable whatever antivirus software is running on the PC/Server as they can occasionally interfere with the installation of Toolbox.

Figure 1: Toolbox Setup starts with a list of Prerequisites. These are software components required to be installed before the main Toolbox Setup starts. Their installations are bundled with the Toolbox installation Wizard and will start automatically.
To begin click install

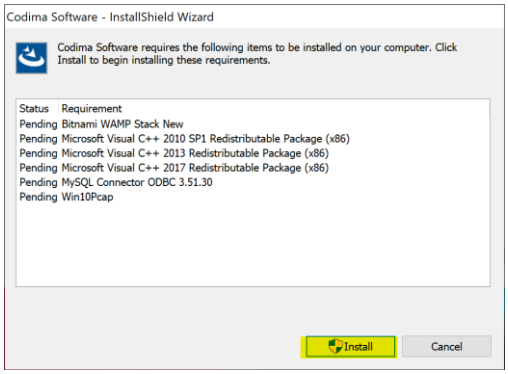


Figure 2: First Prerequisite - the Bitnami Setup Starts

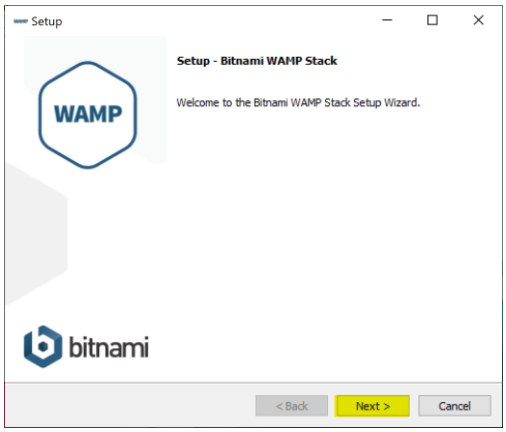


Figure 3: Click Next as the only necessary Bitnami Component is 'PhpMyAdmin'

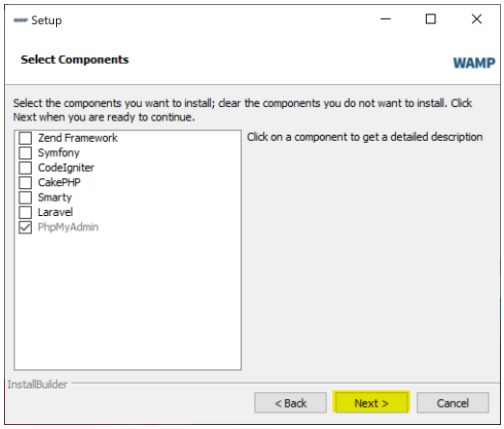


Figure 4: Next input the install path for Bitnami. The Default path is perfectly fine to use

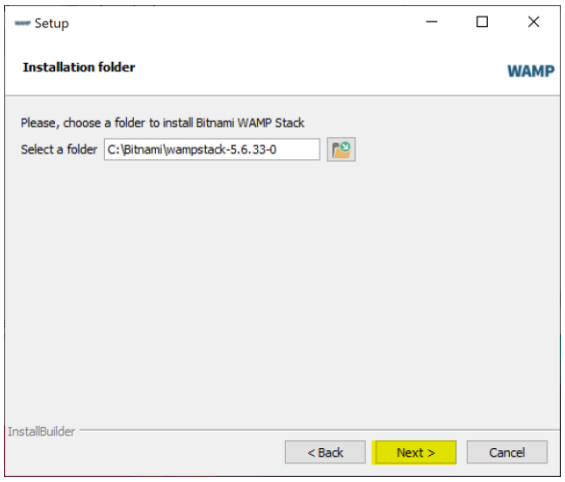


Figure 5: Input a password for MySQL. Make sure to remember this when the installation is complete because you will need to input it when opening Toolbox for the first time
Then click Next

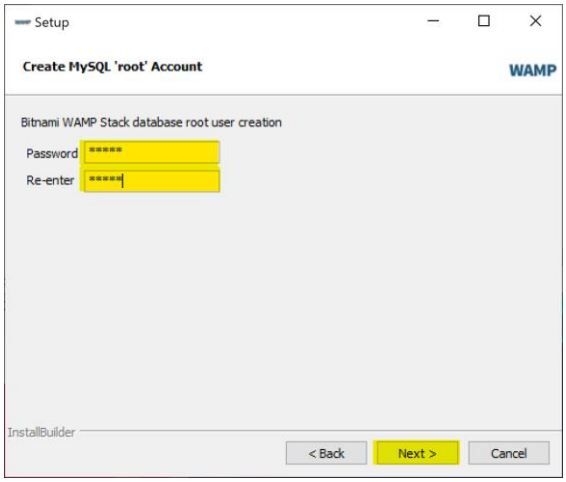


Figure 6: Click Next

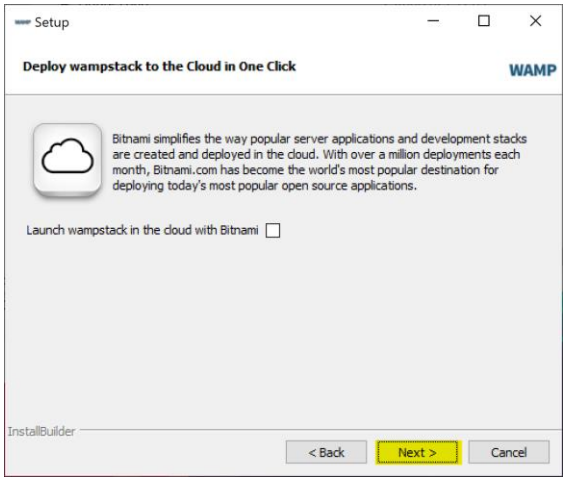


Figure 7: Click Next

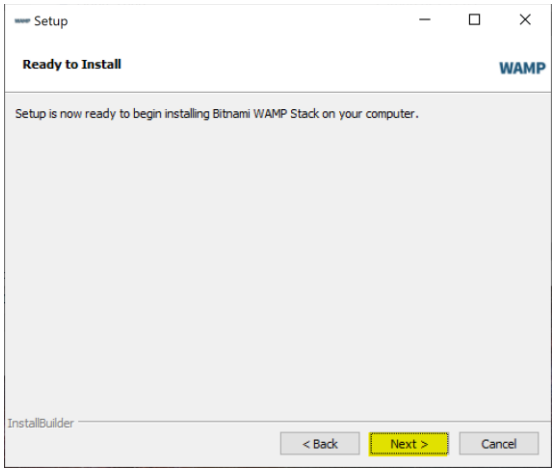


Figure 8: Bitnami Setup now runs...

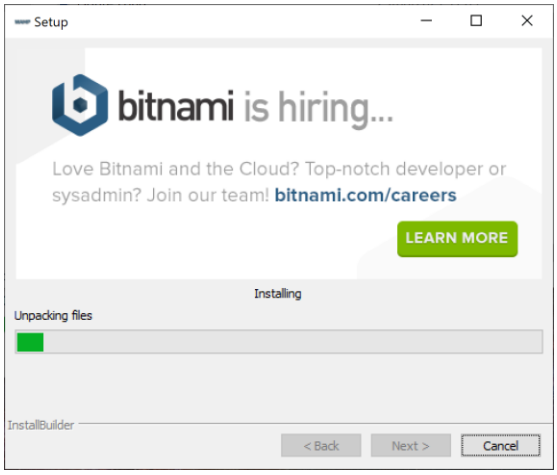


Figure 9: towards the end of Bitnami setup Allow Firewall Access

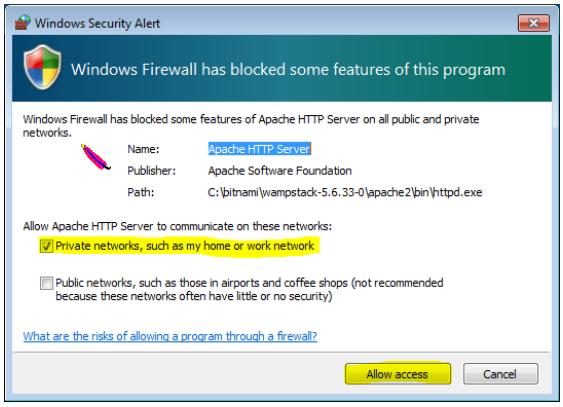


Figure 10: Bitnami successfully installed - Untick Launch then press 'Finish'

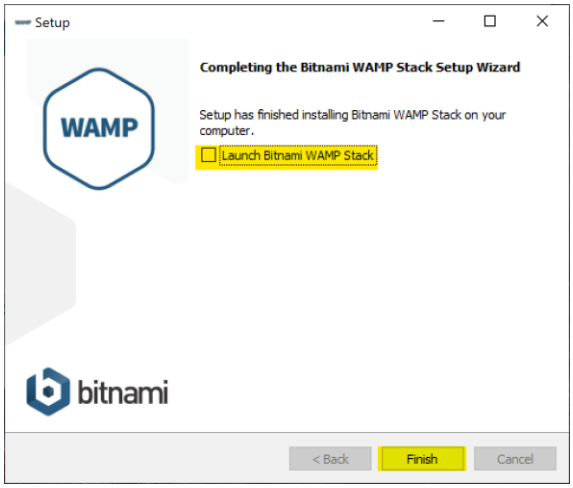


Figure 11: After the 3 C++ Redistributable Packages install silently without any user input, MySQL Connector ODBC setup now starts, click Next.

Figure 12: Accept the license agreement and click Next

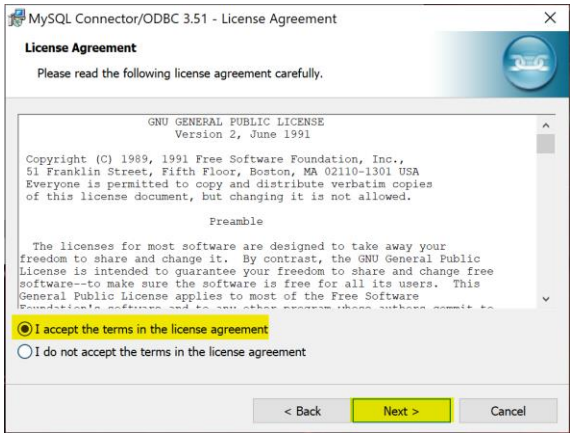


Figure 13: Choose Typical then click Next

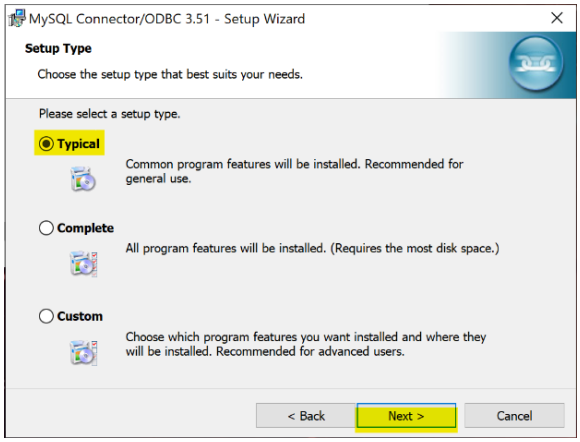


Figure 14: Click Install

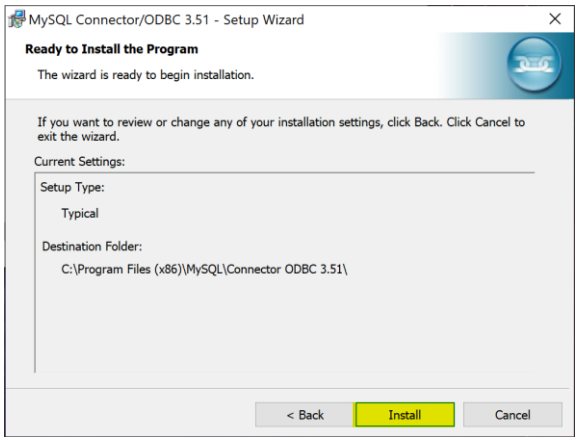


Figure 15: MySQL Connector Installing

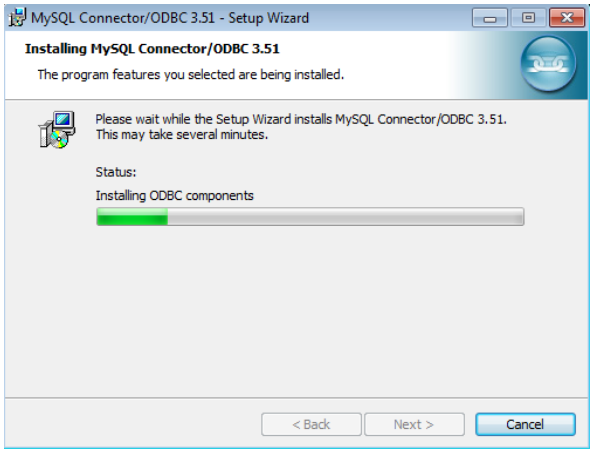


Figure 16: MySQL Connector setup complete, Click Finish

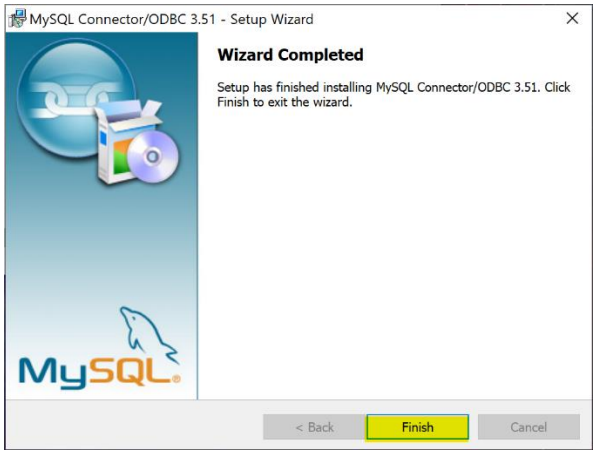


Figure 17: Win10Pcap setup now starts. Click Next

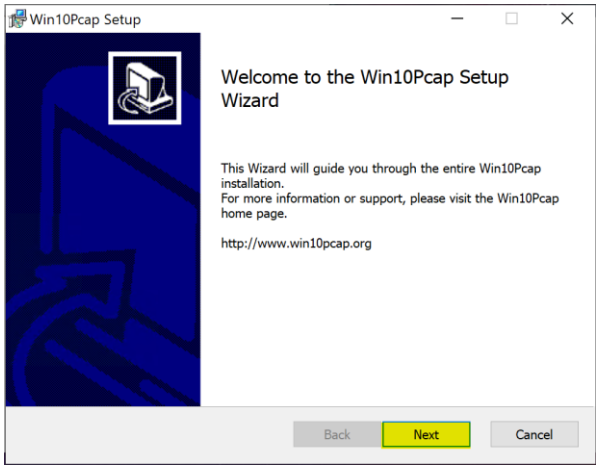


Figure 18: Accept the license agreement and click Next

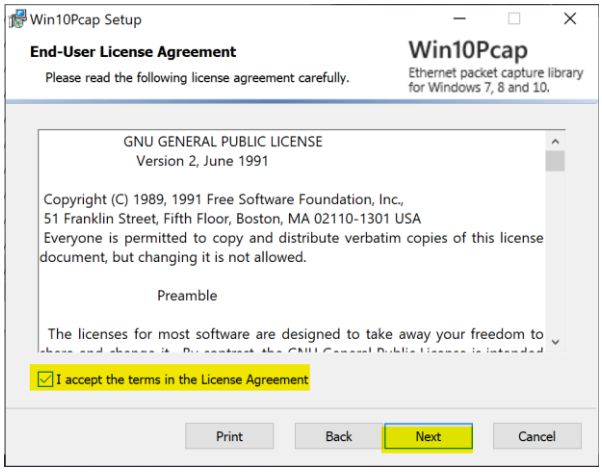


Figure 19: Click Next

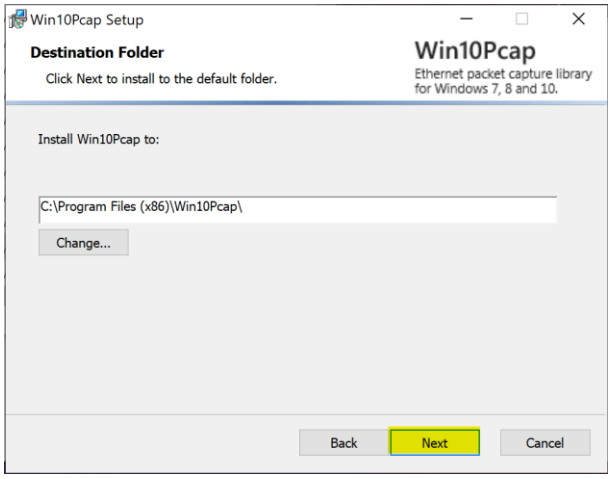


Figure 20: Click Install

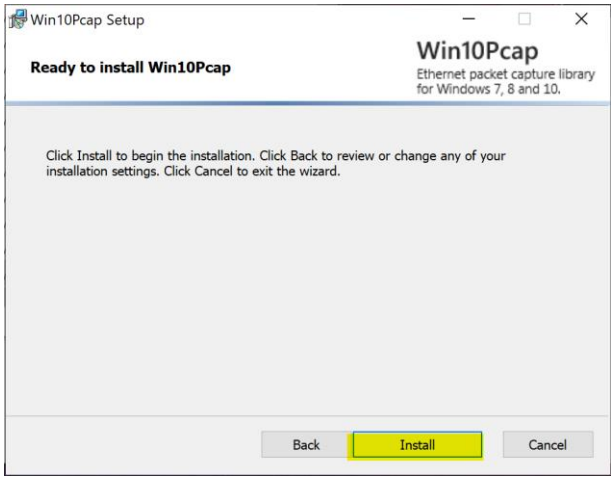


Figure 21: If this window appears tick Always Trust and click Install

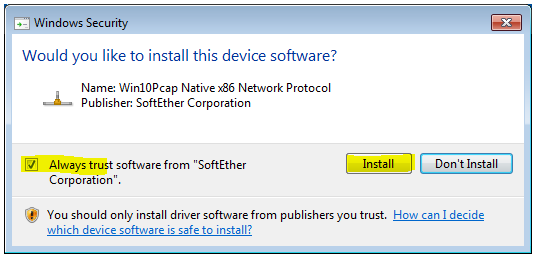


Figure 22: Win10Pcap Installed click Finish.

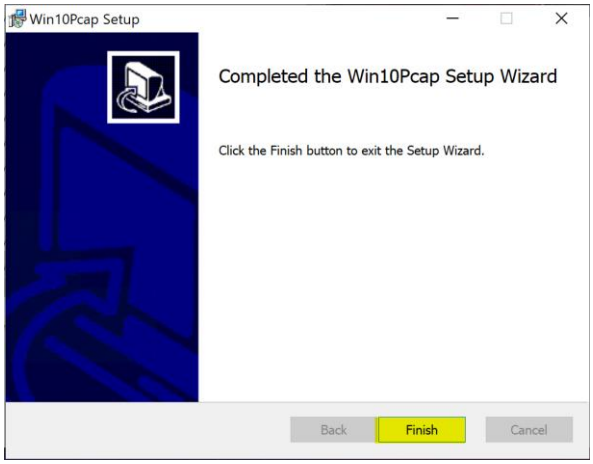


Figure 23: Toolbox Setup starts click Next

Figure 24: Read through the license agreement and if you agree then accept the license agreement and press Next

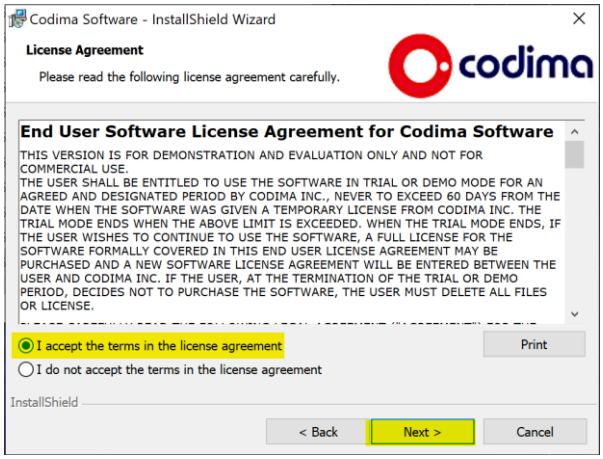


Figure 25: Click Next

Figure 26: Click Install

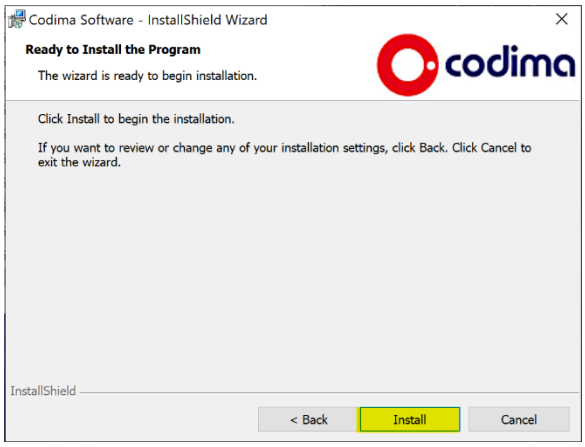


Figure 27: Setup in progress.

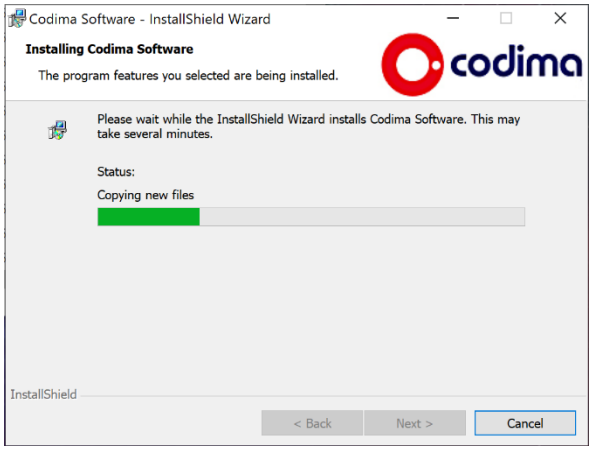


Figure 28: Toolbox Setup completed, click Finish

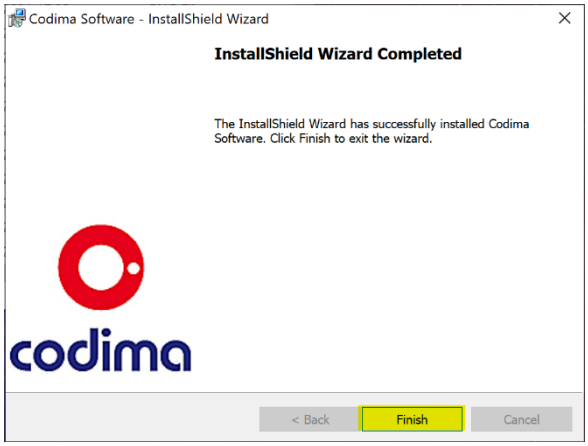


Figure 29: If prompted restart your machine now by clicking Yes

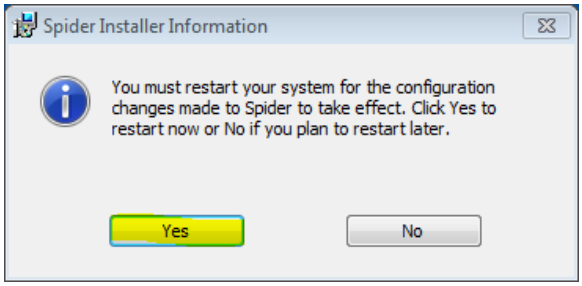


Figure 30: If you have purchased a Codima license place the CodimaLicense.zip in your Document Library, a detailed guide for how to install the license exists in the next section named "License Installation"

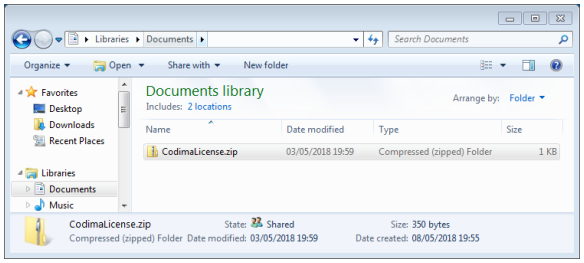


Figure 31: Run Toolbox from the Desktop shortcut icon

First Time Setup

This section details the steps to take the first time you open Toolbox. These steps will not be required every time the program opens, the only time these steps may need to be repeated is upon reinstallation of the software.

*Figure 32: License Changed confirmation, this window will only appear if a license has been installed with Toolbox (An in depth guide for installing a license exists in the next section of this document named "**License Installation**") , click Close*

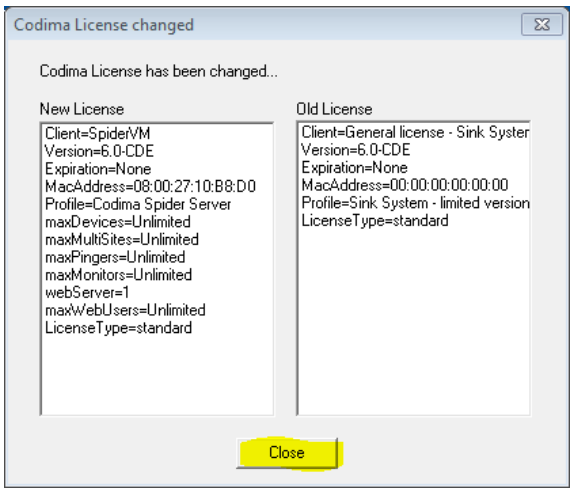


Figure 33: You may be prompted to allow Firewall access, make sure to click Allow access.

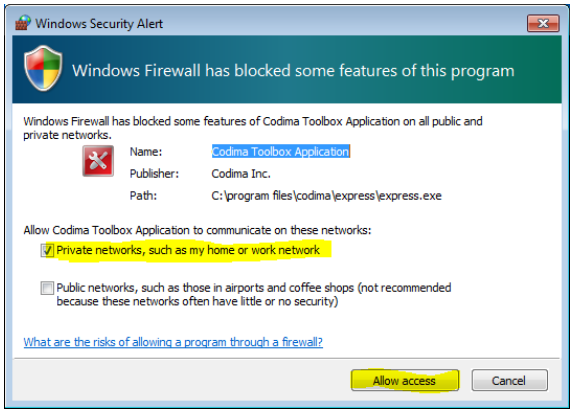


Figure 34: Create the Codima MySQL database entering the password you made a note of earlier during the Bitnami Setup and click OK

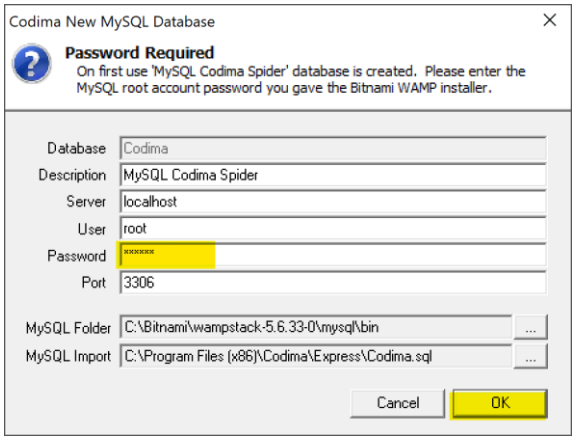


Figure 35: After a minute or two the Toolbox Login Page opens in your browser.

Default User Name = Admin; Password = admin.

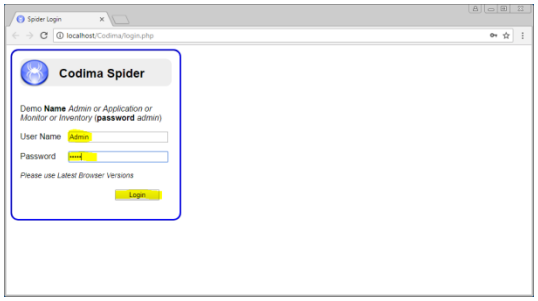


Figure 36: First time running a discovery - Allow the discovery engine firewall access

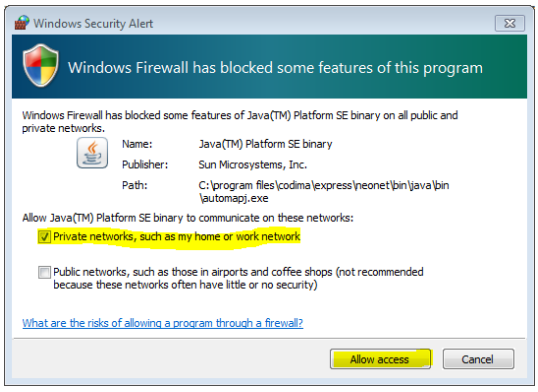


Figure 37: First time running a discovery - Allow the device process firewall access

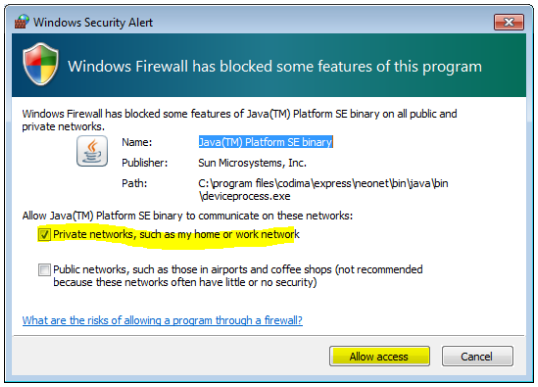


Figure 38: You are entitled to both programmes these icons correspond to if you have either a:
Free license
Network Inventory with Maps in Web and Visio Toolbox license
Network Inventory with Maps in Web and Visio and Monitoring + Alert Ticketing Toolbox license

You are only entitled to use the programme the left icon represents if you have a Network Inventory Toolbox license

The icon on the left is the web-based toolbox, while the icon on the right represents Visio (Network map drawing software)

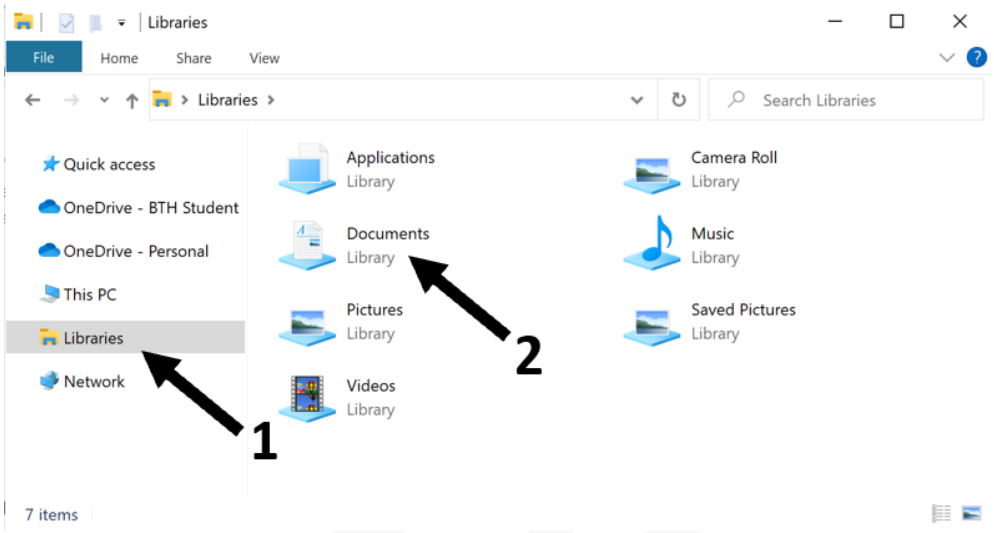
One the installation is complete you have the ability to open toolbox in a number of ways:

1. Clicking on the Toolbox Icon either on your desktop or in the start menu.
2. Typing http://localhost/Codima/login.php into a browser on the installation PC.
3. The Toolbox Web GUI can of course also be launched directly from a remote browser as an IP based URL, as below where 123.123.123.123 is replaced by Toolbox Server (global) IP address: 213.123.123.123/codima/login.php
   Access may be via NAT router using Port Address Translation, in this case a PORT is also specified: 213.249.131.121:49999/codima/login.php – example only

Licence Installation

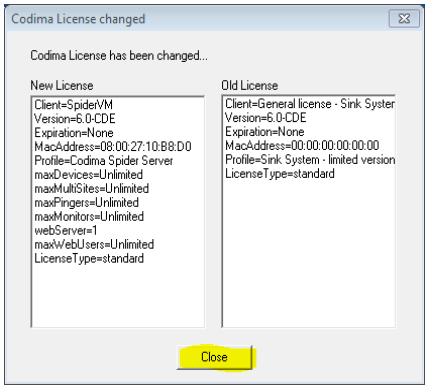
This section details how to install a Toolbox license onto a computer that already has the Toolbox software installed on it.

1. Download the compressed file named **CodimaLicense.zip** from the email that Codima sends to you after the purchase of a license.
   Note: If a zip extractor programme opens then exit out of it
2. Open **File Explorer**, this can be done by pressing **Windows + E**.
3. Navigate to **Libraries** (Marked by the arrow labelled **1**) then open your **Documents** folder (marked by the arrow labelled **2**).



4. Now place the **CodimaLicense.zip** that you just downloaded into you documents folder.
5. To make sure that the license installed correctly open Toolbox the application, the application can be found on the computers desktop and has this Icon:

6. You should now be greeted with a window saying **Codima License Changed** and it should look like the image below. Once you have clicked Close you have successfully installed the license.
   Note: If this window did not appear for you then continue with the steps below



7. If the installation of the license was unsuccessful there are a couple things that can be done.
    i. First make sure that the file you received from Codima called **CodimaLicense.zip** is in your Documents folder and that the file name has not been altered.
    ii. If the first step did not work, try replacing the file **License.txt** at this file destination **C:\Program Files (x86)\Codima\Express\neonet\bin\License** with the **License.txt** file that is found in the **CodimaLicense.zip** file.

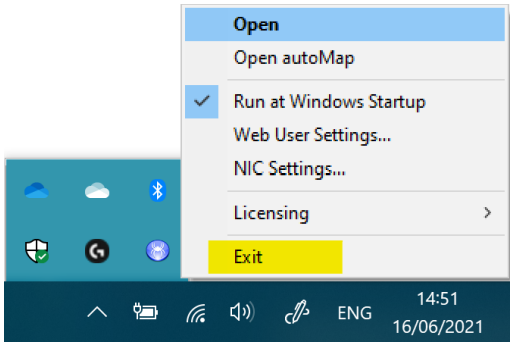
IMPORTANT: Make sure that you make the LATEST licence file, the one called CodimaLicense.zip. That is because if you have multiple downloaded licenses, then later versions will be in the format Codima.License(NN).zip which will NOT be used by the installer. So please rename the latest License file to CodimaLicense.zip.

Update Existing Software with the Latest Version

This section guides the user in how to update the Toolbox software on a PC/Server that is already running Toolbox.

1. First download the newest version of the Toolbox installation wizard. Do this either by downloading the free version here https://codimatech.com/en/free-download/ or by having purchased a Toolbox license here https://codimatech.com/en/pricing/.

2. Make sure to completely exit Toolbox on the Server by using the bottom system tray Blue Icon and select Exit



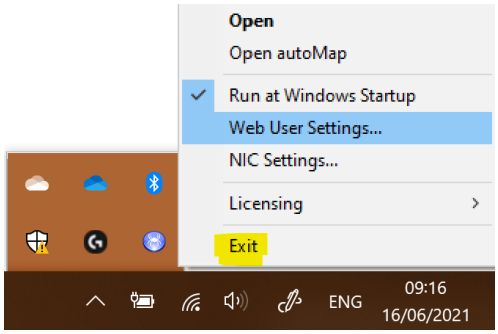
3. Then run the new installer.

Note: *When you first run Toolbox after an update you may need to clear the Web browser cache for the GUI to be displayed correctly. On Chrome press Ctrl + F5 to clear the cache.*

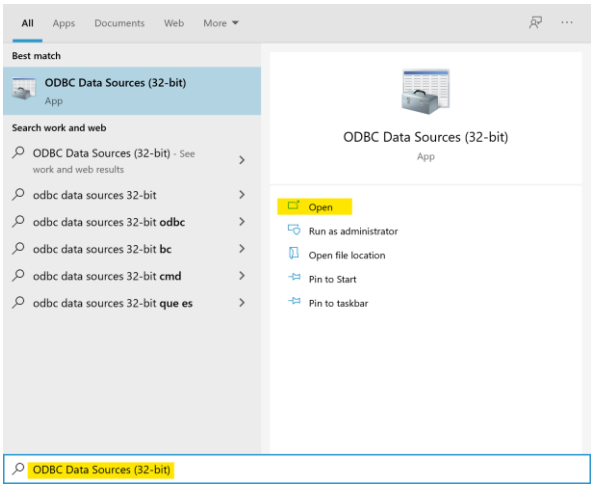
Complete Uninstall – will delete existing discoveries/statistics and all other information for the Toolbox

This will destroy any existing discoveries or other information.

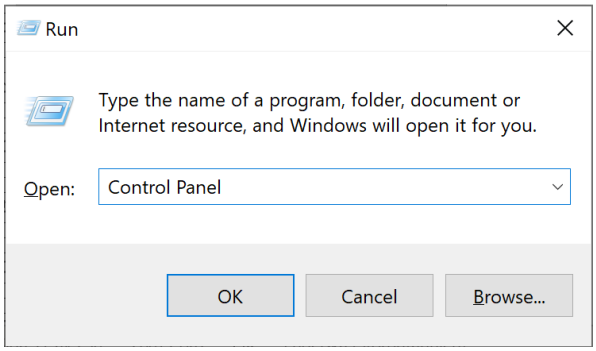
1. Make sure to completely exit Toolbox on the Server by using the bottom system tray Blue Icon and select Exit



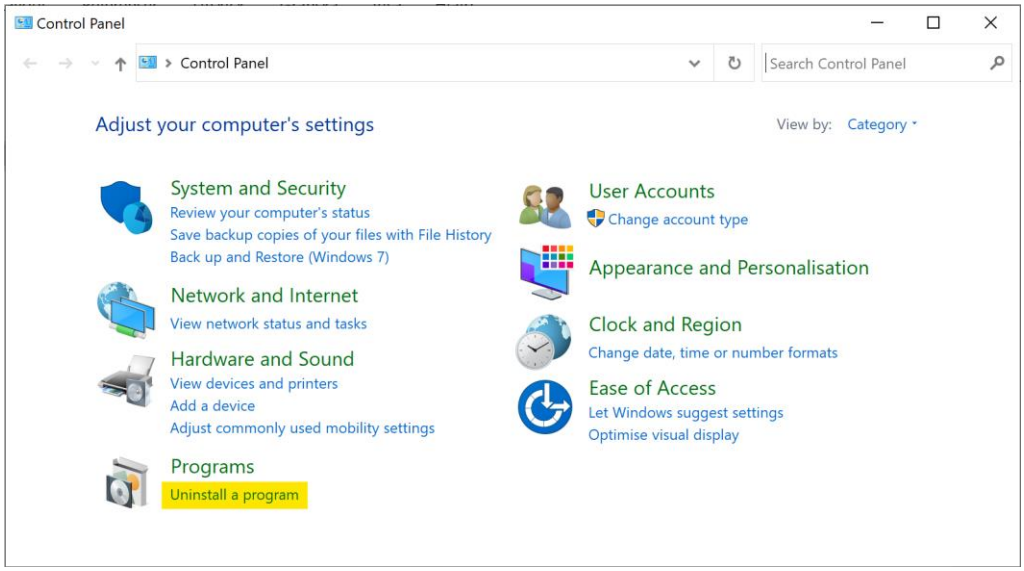
2. Press the **Windows key** then type **ODBC Data Sources (32-bit)** and click **Open** (Marked below in yellow)



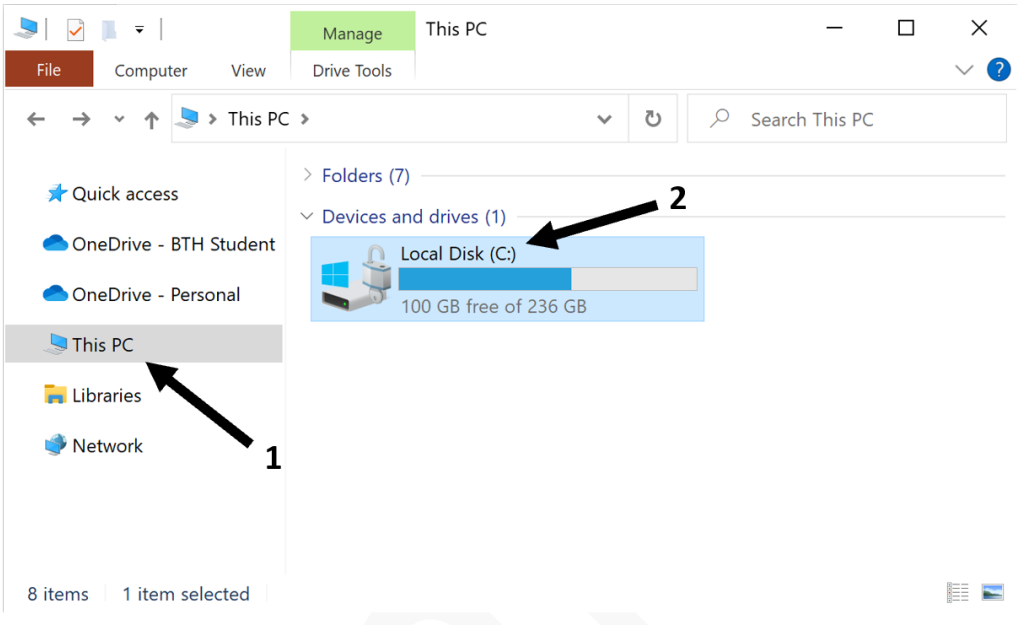
3. Remove all System DSN's associated with Toolbox. This includes Codima and your discovery database names.
4. Now open the Run window again by pressing **Windows + R**, then type Control Panel and press **OK** to open the Control Panel



5. Under the heading Programs is the subheading **Uninstall a program,** click on it



6. Now uninstall the following:
    a. Bitnami WAMP Stack
    b. Codima Software
    c. Win10Pcap
7. The final section is to delete the associated program folders that remain after uninstallation. Find all of these by opening the File Explorer, this can be done by pressing **Windows + E** on your keyboard.
8. Navigate to **This PC** which is found on the left-hand side (as shown by the arrow labelled **1**), then open the Local Drive, which is most commonly the drive named 'C:' (shown in the picture by the arrow labelled **2**)



9. Once the Local Drive has been opened locate and delete the folder named **Bitnami**
10. Then open the folder Named **Program Files (x86)**
11. Once there you will need to locate and delete both the file the named **Codima,** and the file named **Win10Pcap**

12. **Optional:** You may also decide to delete the license for the software, do this by opening the Run window with the key combination **Windows + R**, Search for Documents and the file explorer will open. Now locate and delete the zip file named **CodimaLicense.zip**

TROUBLE SHOOTING INSTALLATION and LOGIN

Antivirus

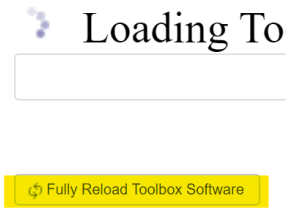
These programs can block installation of Toolbox at many stages. It is highly advisable to turn off during installation. Some less well-known AV can lockup the PC during installs and should be replaced with well-known AV products. Many major AV programs allow the user to specifically White List Codima Software. Remember to turn on AV again after installation.

Windows Firewall

During the initial install Windows will ask the user if they want to allow programs like Apache, MySQL plus Toolbox programs through the Windows firewall, it is important to say yes. If there are later problems with Discovery or Polling the network devices, check in Windows Firewall Advanced Setting that Toolbox programs are not denied access.

Tip: *If loading Toolbox and while logging in nothing is loading, please use Clear Cache and Hard Reset the software. See the steps below if you are unsure on how to do this.*

1. To clear your web browser's cache use the shortcut **Ctrl + Shift + Delete**, this will take you to the settings page where cache can be erased.
2. After opening Toolbox and the software is not loading click on the button that reads **Fully Reload Toolbox Software**, marked in yellow below.



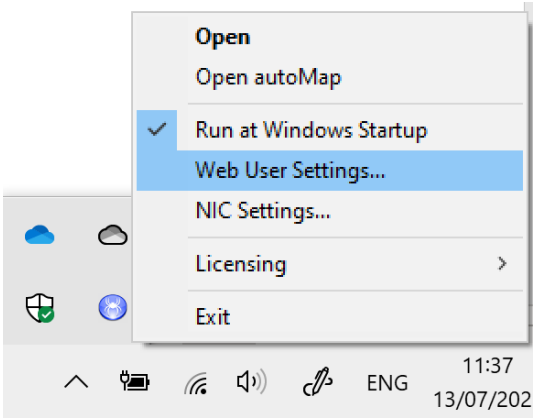
3. Now try reloading the page and logging in again, the software should now load.

Managing User Logins

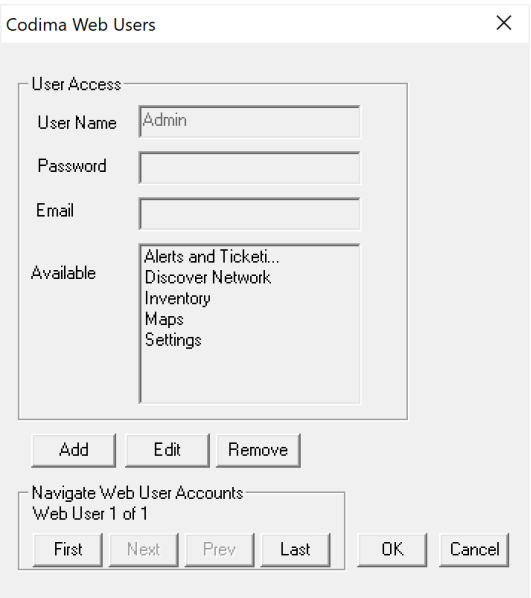
In Toolbox you may create additional users with different levels of access that suits each person's job description. Managing users may only be done on the PC/Server that toolbox is running on

To manage users, you must first click on the **System Tray**, marked in yellow

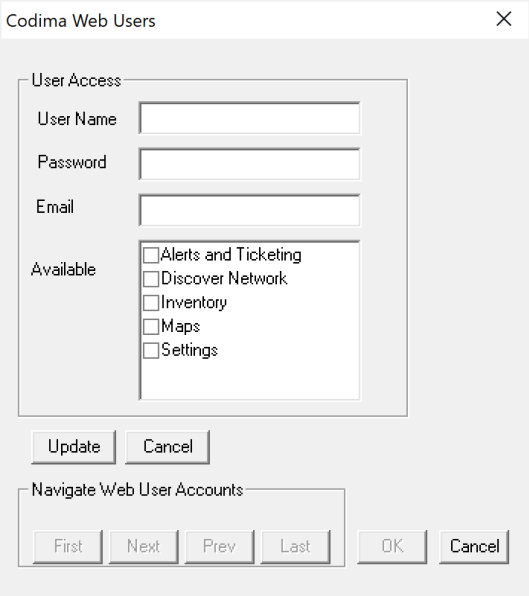
Then **right click** on the Toolbox icon and open the **Web User Settings**



You will now be presented with a window where you can manage all users. Upon installation of Toolbox the default Admin user is provided.



By pressing the **Edit** button, you will be able to change the Username, Password, and available feature for the currently selected user. You may also create an entirely new user by clicking the **Add** button. Remember to click **Update** once you have entered all details to save the User.



By ticking available features you may decide what level of access this user will have to the toolbox system, for example if you only want this person to access the Inventory feature but be unable to run a discovery then only tick **Inventory**.

DISCOVERY Feature

This section details how to use the Network Discovery Tool that is included in all Toolbox products.

What Does Discovery Do?

The Network Discovery Tool automatically creates a detailed Inventory of Software and Hardware without using Agents. Updated and tested over 17 years of development, the field proven discovery engine, discovers large and small networks automatically.

Discovering the Network is fundamental to Mapping and Monitoring the Network as it learns what devices and links are present. That allows the Discovery to be used to automatically poll and monitor the network.

It also means setting up and displaying Netflow and all other features like Alerts know what IP addresses are associated with devices.

Discovery Engine

The Discovery Engine uses a variety of techniques to discover devices, such as inspection of ARP tables and controlled scanning techniques. This overcomes a limitation of many existing approaches, which need to know what to discover in order to draw a network. Once discovered, devices are queried using **SNMP** for **MIB** 2 and current vendor MIBs. The Discovery system has a stored device list database of most current and many old generation equipment types.

Important - Platforms running Discoveries must have hibernation/standby disabled.

Important: Windows has an option to make Devices 'Discoverable', ensure this is enabled. Otherwise, devices will just be discovered as IP addresses - if at all.

Note: If issues arise while attempting to complete a Discovery read the section **Troubleshooting a Discovery**

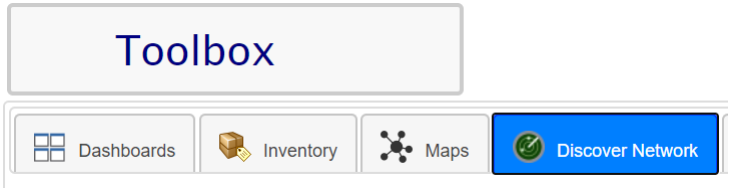
Note: This chapter may gloss over some advanced features, for a full rundown of each section see the next chapter **DISCOVER NETWORK – ADVANCED INFORMATION**.

Creating a Discovery – Step by Step

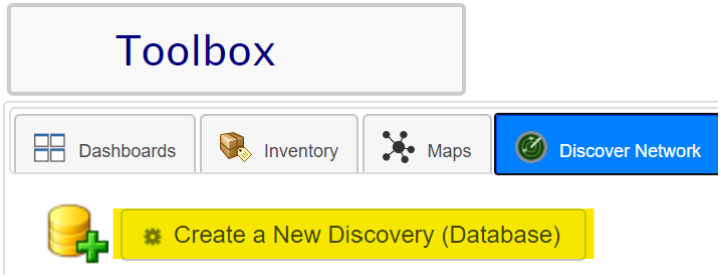
This section details how to create a Discovery in a step-by-step guide that includes images with yellow highlighter markup.

Creating a Database

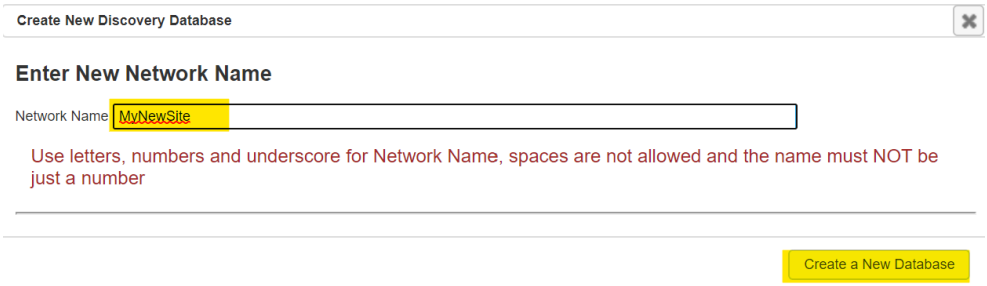
1. First and foremost, you must open the Toolbox software and log in.
2. Next navigate to the **Discover Network** tab found at the top-left corner of the screen.



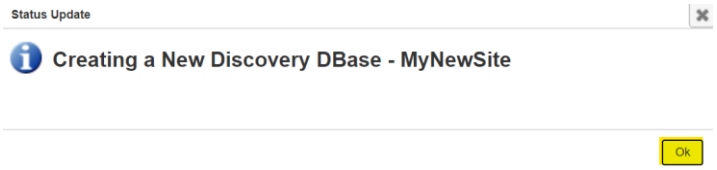
3. Click on the button that says **Create a New Discovery (Database)**



4. A window will appear asking you to name your Discovery, you may name it however you see fit as long as it follows the guidelines found on the window. Once an appropriate name has been entered click the button **Create a New Database**.



5. A new window will appear notifying you that the process of creating the database has begun, press **Ok** and wait a few second for the database to be created.

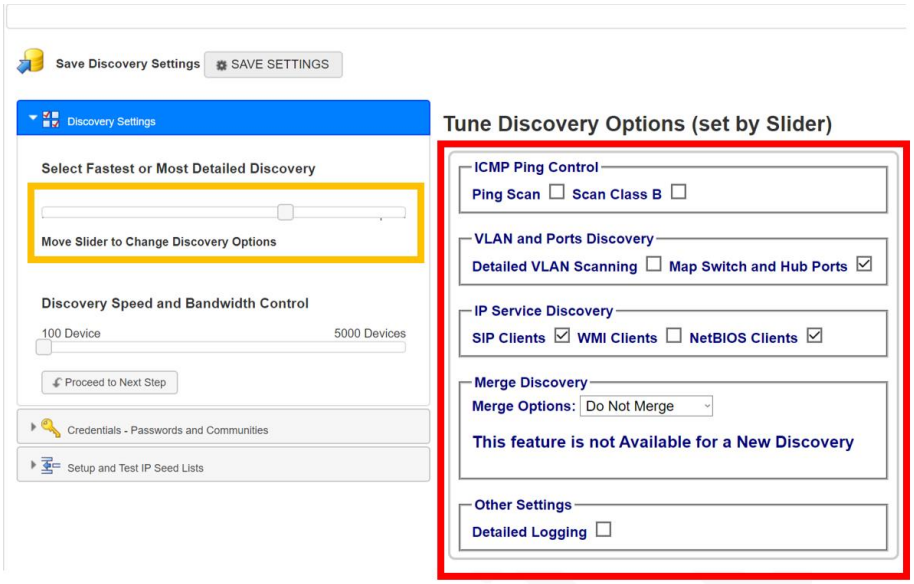


6. Once the database has been created it will be visible in the **Discoveries Status and Control** list at the bottom of the page. Any new discoveries will have a status indicating that it is New, see in the image below.

Configuring Discovery Settings

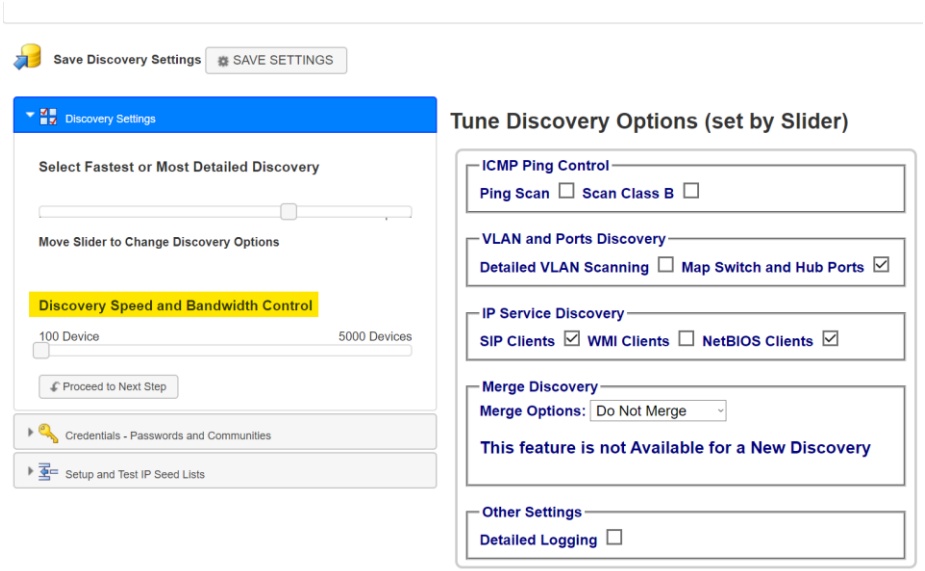
7. Now click on the red text reading **NO Settings>>>** to configure the Discovery settings.

8. A new window will appear where you may decide what you want the Discovery to scan the network for. There are two ways to decide what you want to scan for, the first is to manually tick all the boxes that you want to scan for (these are found on the right side, marked with the red square. Alternatively, you can use the slider on the left-hand side and the software will decide what to scan for based on how detailed of a scan you want to conduct (The slider is marked with the orange square, moving the slider to the left will make the scan more detailed and less detailed if it is moved to the right).

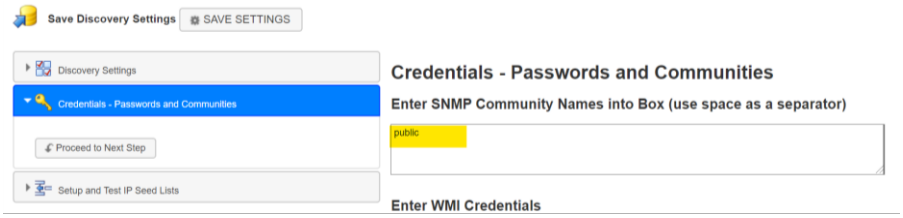


Note: The Merge Discovery feature can be useful if you are conducting several discoveries and don't want to lose any information from previous discoveries.
Note: The Detailed Logging feature collects detailed Logging of the discovery which can be used by Toolbox Support to diagnose issues associated with the discovery

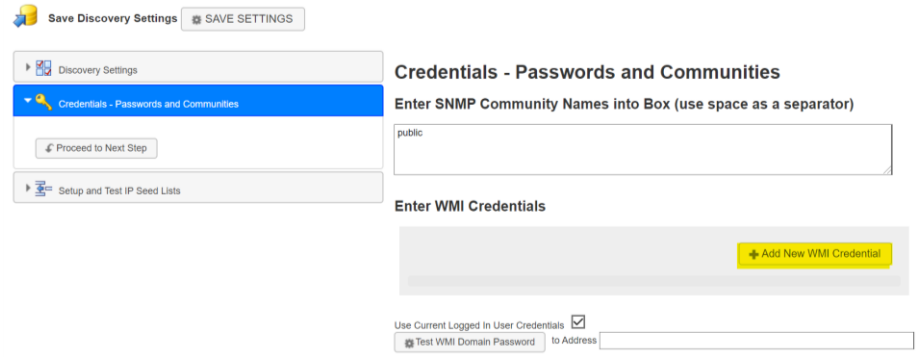
9. In the same step there is a slider titled **Discovery Speed and Bandwidth Control**, this slider will determine how many devices the software will scan simultaneously. If you are scanning a small network, you can leave the slider alone, but for larger networks you may choose to increase the slider to speed up the process (bear in mind this could put a strain on the PC/Server).



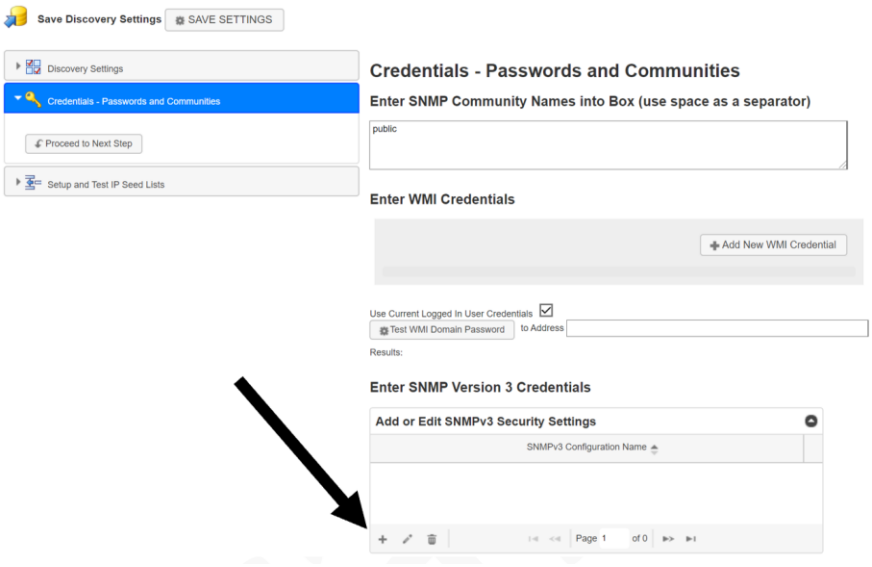
10. Now click on the button beneath the sliders on the left-hand side that reads **Proceed to Next Step**.
11. In this section, the first step is to enter the networks **SNMP Community Names** into the text field. Most PCs will default to public so if you have a simple network this step can often be skipped, however in other networks you may need to add additional SNMP Community Names.



12. Workstations do not usually have SNMP enabled. The key to getting the WMI to work is to make sure the machine the discovery is running on is allowed to ask the workstations for WMI information. Do this by entering WMI Credentials into the into the Discovery setup, *please refer to your network administrator for help on this.*



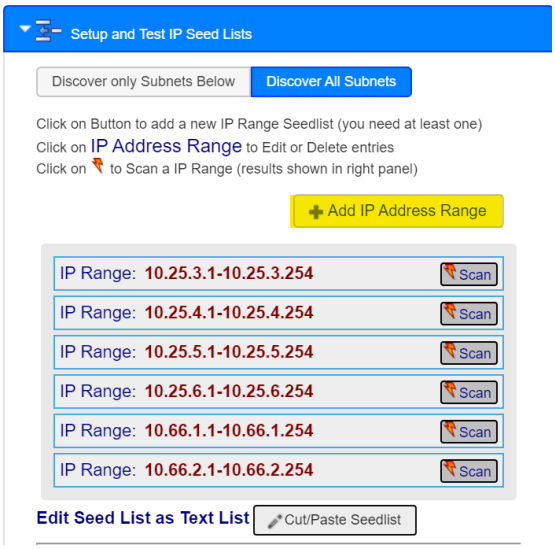
13. You may also enter SNMPv3 Credentials by clicking on the "**+**" icon under the heading **Enter SNMP Version 3 Credentials** (Shown by the arrow in the image below)



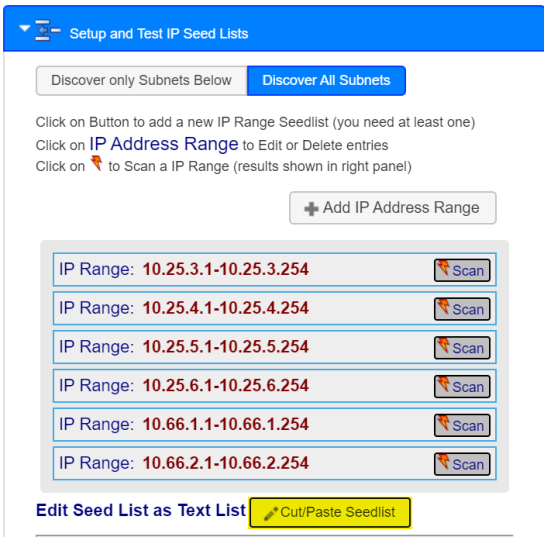
14. Click on the button **Proceed to Next Step** found on left-hand side.

15. The following step is optional but is highly recommended as it decreases the Discovery length drastically.
    You can import a range of known IP addresses into the Discovery facility, effectively creating a list of seed addresses that then provide a means of speeding up the discovery process, as the Discovery Engine will bypass the early discovery stages and immediately activate SNMP operations for the listed addresses.
    There are two ways to create a seed list and they work in conjunction with one another:

    a. Manually Add ranges one at a time using the **Add IP Address Range** button, this method works well for a couple of ranges.



    b. The second method is to paste a saved text file seed list into the prompt that appears once the **Cut/Paste Seedlist** button is pressed, this method works great if you have many seed list ranges.

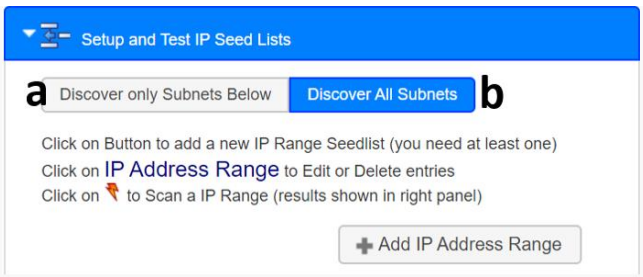


Note: You can check that the start parameters are ok, prior to starting the discovery. Do this by clicking on the **Scan** button to initiate a test to an IP Range, this can take several minutes.

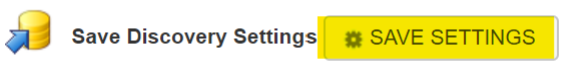
16. There is an additional option under the **Setup and Test IP Seed Lists** tab, and these are to either **Discover only Subnets Below,** or to **Discover all Subnets**. An explanation of what these do, are as follows:

    a. Selecting **Discover only Subnets Below** option will ensure that once all the addresses in the Seed List are processed the discovery will stop, this method allows you to restrict your discovery to a defined range of addresses.

    b. Selecting **Discover All Subnets** option will ensure that all the addresses in the Seed List are processed first, then the system will continue to operate to find more devices.



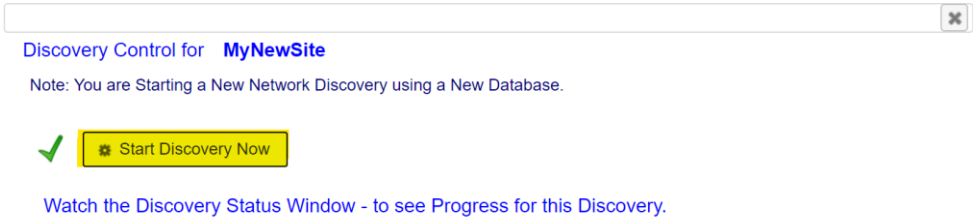
17. Make sure to **SAVE SETTINGS**, otherwise none of the changes you made will be saved. This button is found in the top left corner of the Discovery Settings window.



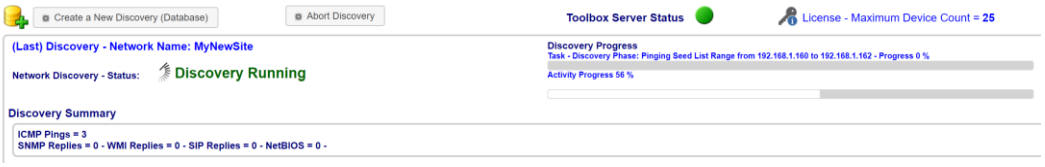
Running the Discovery

18. To start the Discovery process, click on the start button, marked in the image below with yellow.

19. A new window will appear click **Start Discovery Now**.



20. Now you must wait for the Discovery to complete. You can monitor the progress of the Discovery in the Discovery Status Window. You may also at any time cancel the Discovery by clicking the **Abort Discovery** button at the top of the GUI, but keep in mind that this process can take a long time complete.



21. Once the Discovery is completed you will be greeted with this message

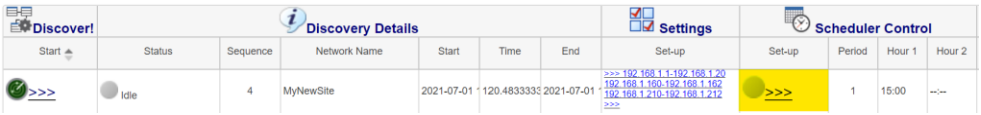
22. You now will also see that a Summary Report has been produced in the righthand panel of the GUI and will in essence look something like the image below. It contains counts of discovered devices organised by device category.

Only devices that respond to SNMP will be identified and classified. Unknown devices can be mailed to your reseller and included in a release.

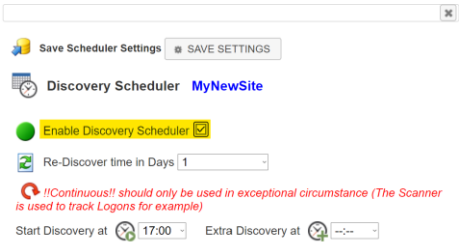
Discovery Scheduler

This feature has the capability to automatically schedule and execute Network Discoveries using the Toolbox's web GUI. The following guide shows how to setup the Discovery Scheduler in a step-by-step manner.

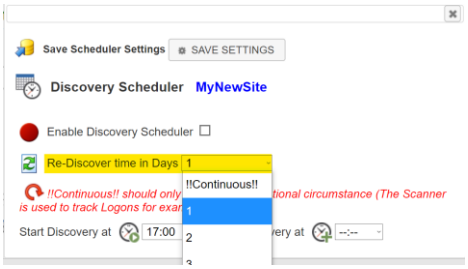
1. First you must have completed a Discovery in order to setup the Discovery Scheduler.
2. Next find the column named **Scheduler Controller** in the Discovery grid, and click on the three arrows "**>>>**" under **Set-up**.



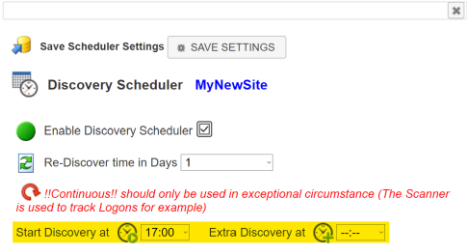
3. A new window will appear, click on the tick box to enable the Discovery Scheduler. If at any point in the future you wish to disable this feature just uncheck this box and **SAVE SETTINGS**.



4. Next decide how often you wish to run the Discovery. Note that the **!!Continuous!!** option starts a new discovery as soon as the Discovery Engine is free, this option is seldom recommended.



5. Now you can decide at what time the discovery will start. You may also decide whether you want to run an Extra Discovery on the same day.



6. Lastly click **SAVE SETTINGS** otherwise none of the changes will be saved.

How long should discovery take?

A typical inventory/discovery run can take between five minutes and many hours. The rules set out below will assist in determining the time an inventory/discovery will take.

General Rule

Each IP address is tested individually for Ping, SNMP v1, SNMP v2c or SNMPv3, and optionally WMI, NetBIOS and SIP Queries for a total of 15 seconds.

If that IP address is an SNMP device then it is fully processed. The processing of a simple device such as a printer takes 15 seconds. The processing of a high-end router or switch with hundreds of interfaces and VLANs takes several minutes.

You also need to be careful in a situation where the Ping Scan is applied to Class B networks, that process will slow the discovery and if it is not required should be disabled.

The average time to process one IP address is 30 seconds.

This average, combined with the number of IP addresses, and the number of parallel processing threads, can be used in the formula below to calculate an approximate maximum time for the inventory duration.

*Maximum Duration (Mins) = (Total IP Addresses)/(2 * (number of parallel processes))* A network can include many subnets of different sizes:

Number of IP Addresses

Subnet Class - Number of IP Addresses
A - 16,000,000
B - 65,000
C - 254

The total number of IP addresses in this context is the sum of the number of IP addresses in all subnets. Not all IP addresses are used, however, hence our calculation is an upper limit on inventory/discovery duration.

If the total number of devices is actually known, then it should be used instead. This would give a much more accurate view of the duration of the inventory/discovery.

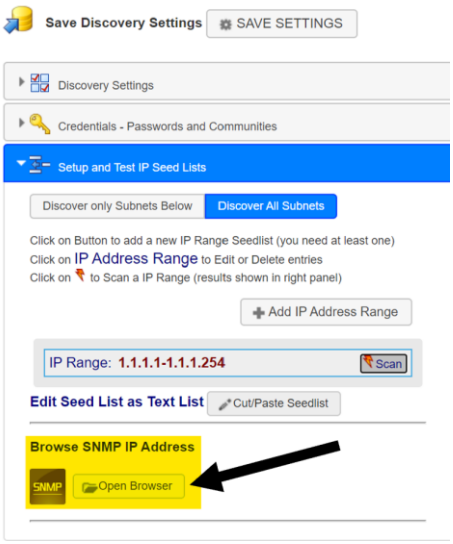
Number of Parallell Processes

The **Discovery Engine** can process multiple IP addresses in parallel as a means of speeding up the inventory. The user can adjust the bandwidth using the Discovery Speed slide bar provided in the Discovery Setup.

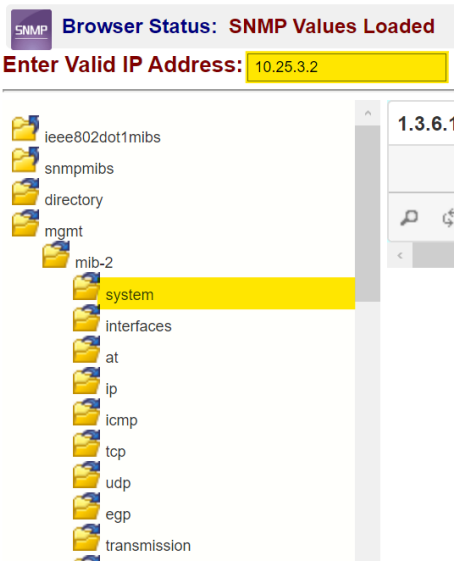
Any IP Address SNMP Browser

A facility has been added to the Toolbox to allow any IP Address to be investigated with a SNMP Browser, this is especially useful when debugging Discovery Issues.

The Browser is launched from the **Discovery Settings** in the tab called **Setup and Test IP Seed Lists**- as can be seen in the picture below. Clicking the **Open Browser** button opens the SNMP Browser window.



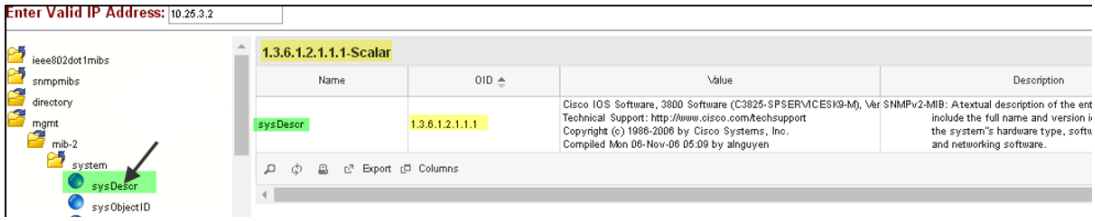
The Browser opens in a new dialog box as below, this is called the **MIB Tree**:



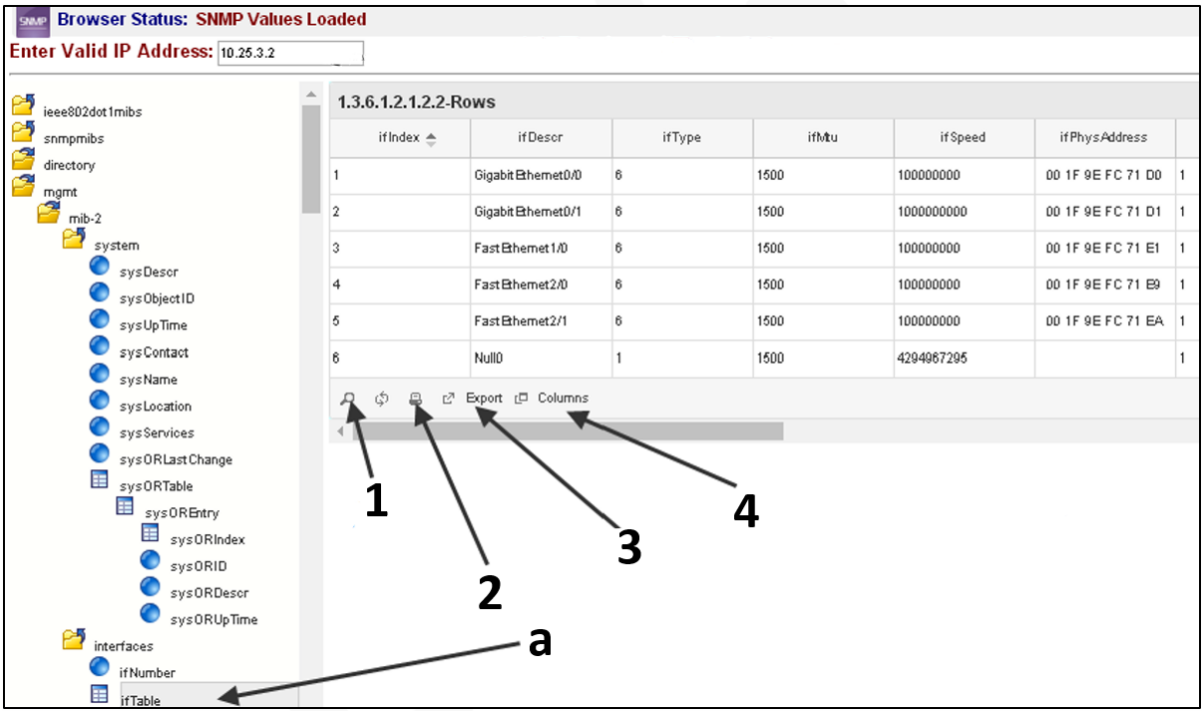
To Browse a Device such as a Server or Switch one enters the IP address of the target device as in the picture above.

Next open a MIB Tree leaf like **system** above then click on **sysDescr** to show the MIB System Description. After a few seconds an analysis appears for, in this case for **sysDescr**.

The Toolbox Web GUI sends a SNMP request to the Toolbox server which then polls the requested MIB information and returns it to the Toolbox Browser.



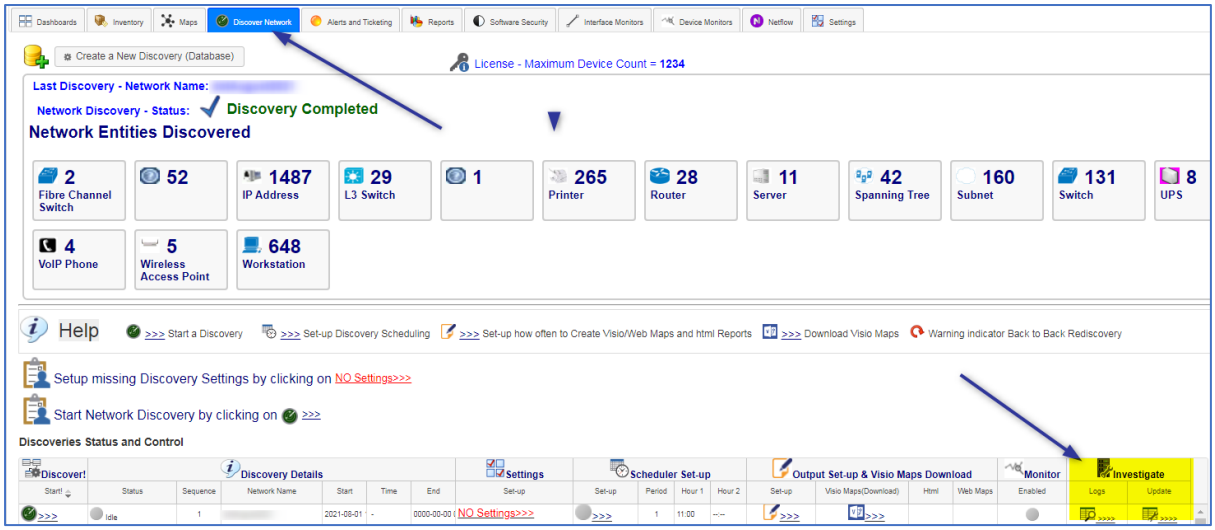
The sysDesr example above is a simple SCALAR value, however by clicking on an MIB Table like **ifTable**(a), then a full list of rows like Interfaces, can be examined too.



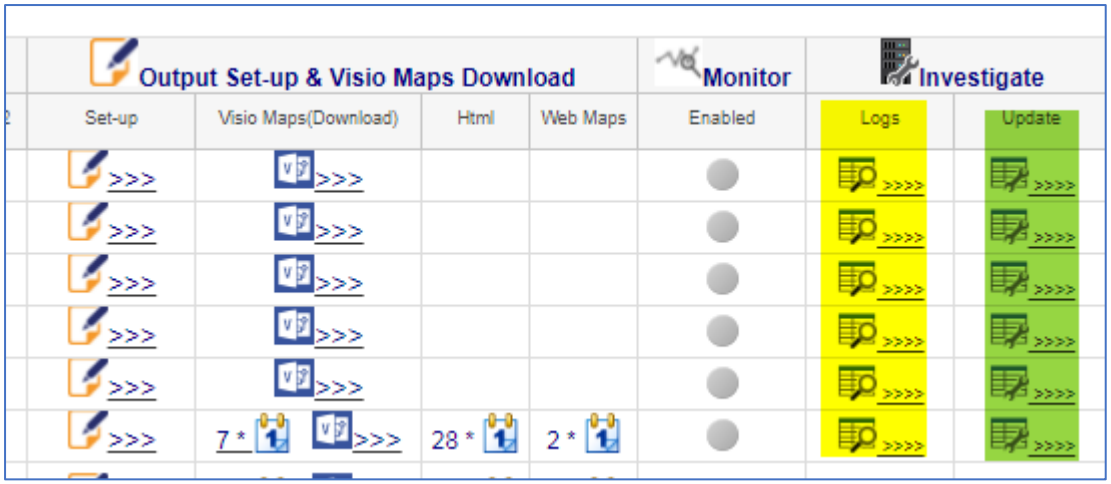
Note. the Grid can be searched(1), sorted, filtered(4), and exported to a CSV file(3) or alternatively printed(2).

Investigate Feature

The **Investigate** Column is found in the Discoveries Grid. The column is split into two sections, one section where you can view the logs created by the discovery, and the other where you can update unknown device details using their MAC addresses.

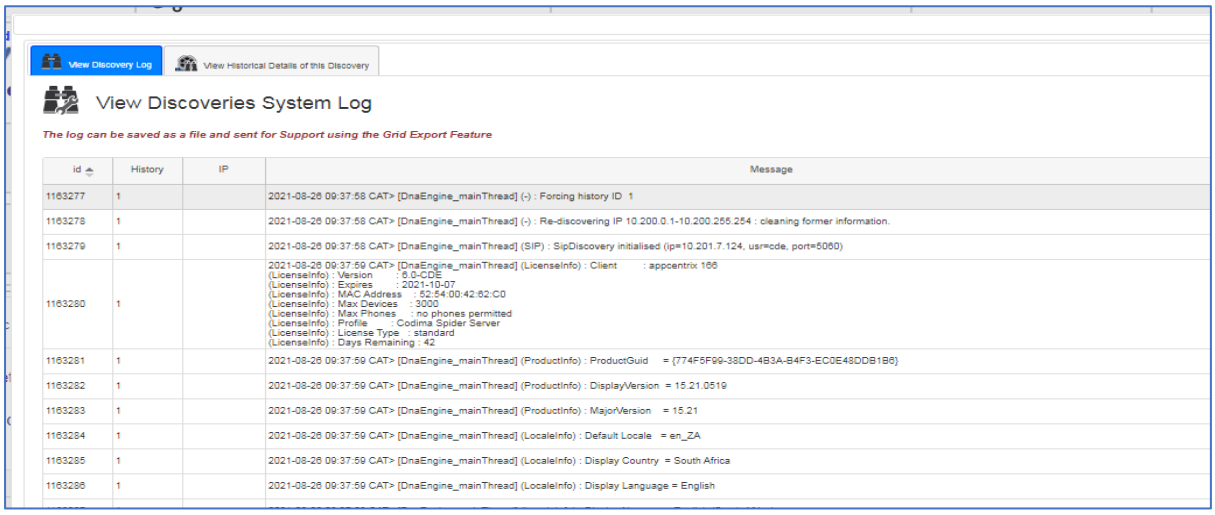


The new **Logs** column links to Discovery Reports and the Update Column links to the optional MAC to Vendor (post discovery) facility.

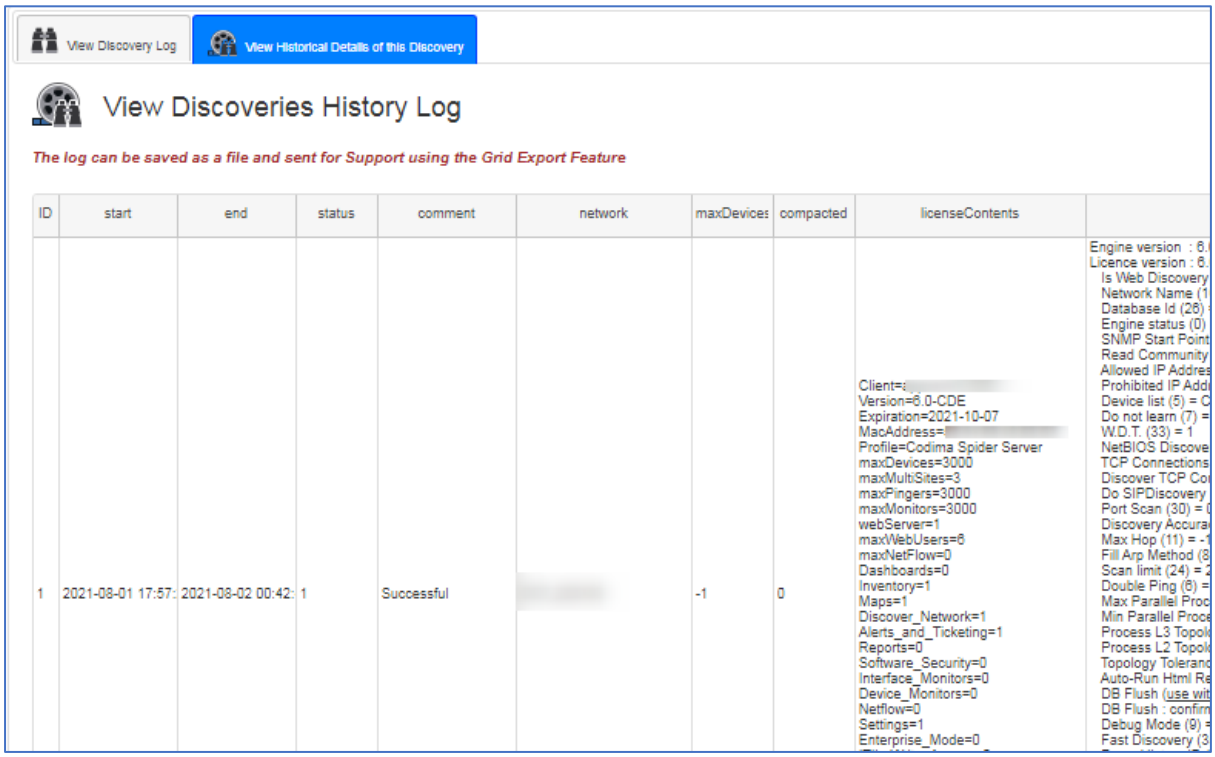


The Logs Column

Once you clicked on the **Logs** icon for a certain discovery the window shown below will be displayed.



Above, the **View Discovery log** is selected to show the discovery details for the selected discovery from the Discoveries Status and Control grid.

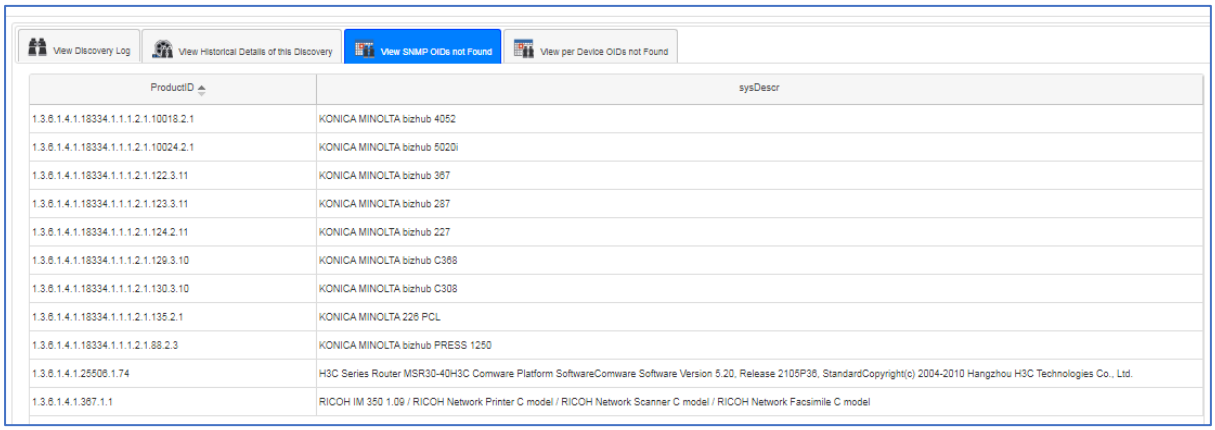


To view historical logs (from previous discoveries) click on the **View Historical Detail of this Discovery** tab.

Tracking Device Types reported as Unknown to the System SNMP Object Identifiers (OIDs)

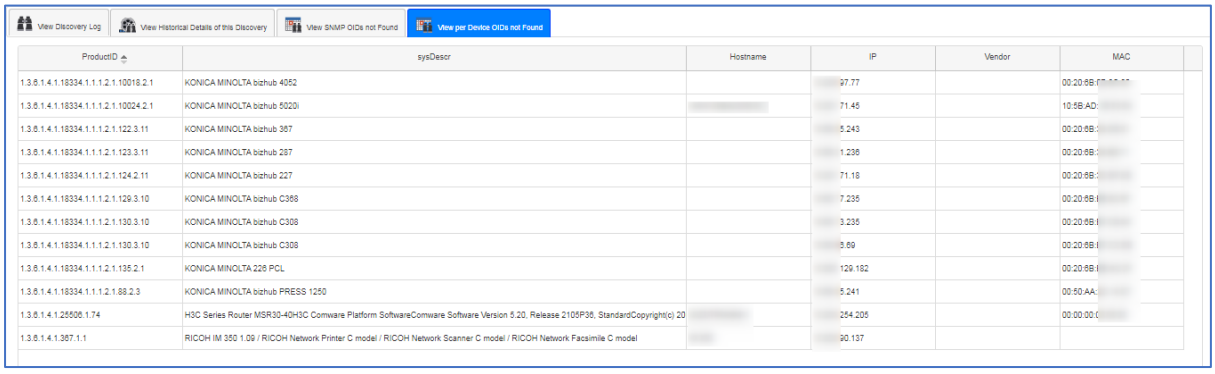
The last two tabs in the **Logs** window are for support purposes, allowing an inspection of unknown devices found in a discovery

The third tab is labelled **View SNMP OIDs Not Found**, as shown below:



ProductID	sysDescr
1.3.6.1.4.1.18334.1.1.1.2.1.10018.2.1	KONICA MINOLTA bizhub 4052
1.3.6.1.4.1.18334.1.1.1.2.1.10024.2.1	KONICA MINOLTA bizhub 5020i
1.3.6.1.4.1.18334.1.1.1.2.1.122.3.11	KONICA MINOLTA bizhub 367
1.3.6.1.4.1.18334.1.1.1.2.1.123.3.11	KONICA MINOLTA bizhub 287
1.3.6.1.4.1.18334.1.1.1.2.1.124.2.11	KONICA MINOLTA bizhub 227
1.3.6.1.4.1.18334.1.1.1.2.1.129.3.10	KONICA MINOLTA bizhub C368
1.3.6.1.4.1.18334.1.1.1.2.1.130.3.10	KONICA MINOLTA bizhub C308
1.3.6.1.4.1.18334.1.1.1.2.1.135.2.1	KONICA MINOLTA 226 PCL
1.3.6.1.4.1.18334.1.1.1.2.1.88.2.3	KONICA MINOLTA bizhub PRESS 1250
1.3.6.1.4.1.25506.1.74	H3C Series Router MSR30-40H3C Comware Platform SoftwareComware Software Version 5.20, Release 2105P36, StandardCopyright(c) 2004-2010 Hangzhou H3C Technologies Co., Ltd.
1.3.6.1.4.1.367.1.1	RICOH IM 350 1.09 / RICOH Network Printer C model / RICOH Network Scanner C model / RICOH Network Facsimile C model

This grid shows Object Identifiers that system could not identify. The grid list can be saved as a CSV file using the Grid Export Feature, this file should then be emailed to - support@codimatech.com in order for the unknown devices to be added into the Codima database.

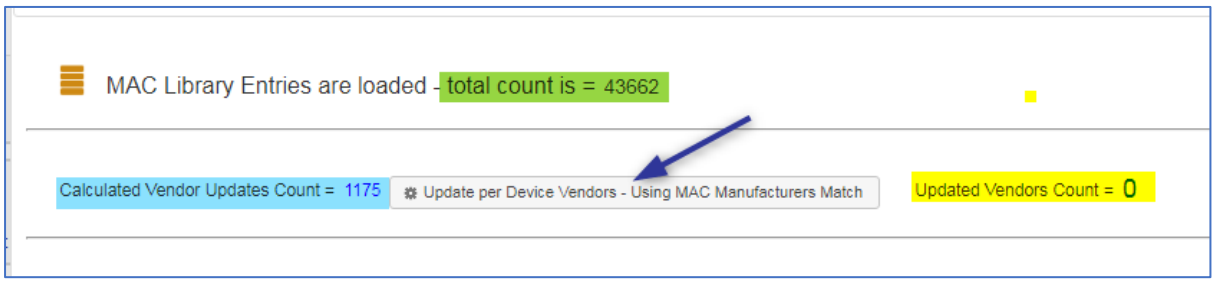


ProductID	sysDescr	Hostname	IP	Vendor	MAC
1.3.6.1.4.1.18334.1.1.1.2.1.10018.2.1	KONICA MINOLTA bizhub 4052		[redacted]7.77		00:20:6B:[redacted]
1.3.6.1.4.1.18334.1.1.1.2.1.10024.2.1	KONICA MINOLTA bizhub 5020i	[redacted]	[redacted]71.45		10:5B:AD:[redacted]
1.3.6.1.4.1.18334.1.1.1.2.1.122.3.11	KONICA MINOLTA bizhub 367		[redacted]5.243		00:20:6B:[redacted]
1.3.6.1.4.1.18334.1.1.1.2.1.123.3.11	KONICA MINOLTA bizhub 287		[redacted]1.236		00:20:6B:[redacted]
1.3.6.1.4.1.18334.1.1.1.2.1.124.2.11	KONICA MINOLTA bizhub 227		[redacted]71.18		00:20:6B:[redacted]
1.3.6.1.4.1.18334.1.1.1.2.1.129.3.10	KONICA MINOLTA bizhub C368		[redacted]7.235		00:20:6B:[redacted]
1.3.6.1.4.1.18334.1.1.1.2.1.130.3.10	KONICA MINOLTA bizhub C308		[redacted]3.235		00:20:6B:[redacted]
1.3.6.1.4.1.18334.1.1.1.2.1.130.3.10	KONICA MINOLTA bizhub C308		[redacted]5.69		00:20:6B:[redacted]
1.3.6.1.4.1.18334.1.1.1.2.1.135.2.1	KONICA MINOLTA 226 PCL		[redacted]129.182		00:20:6B:[redacted]
1.3.6.1.4.1.18334.1.1.1.2.1.88.2.3	KONICA MINOLTA bizhub PRESS 1250		[redacted]5.241		00:50:AA:[redacted]
1.3.6.1.4.1.25506.1.74	H3C Series Router MSR30-40H3C Comware Platform SoftwareComware Software Version 5.20, Release 2105P36, StandardCopyright(c) 20	[redacted]	[redacted]254.205		00:00:00:[redacted]
1.3.6.1.4.1.367.1.1	RICOH IM 350 1.09 / RICOH Network Printer C model / RICOH Network Scanner C model / RICOH Network Facsimile C model	[redacted]	[redacted]90.137		

The Tab **View SNMP OIDs per Device** grid above, shows which devices do not have a known OID and is provided just for reference.

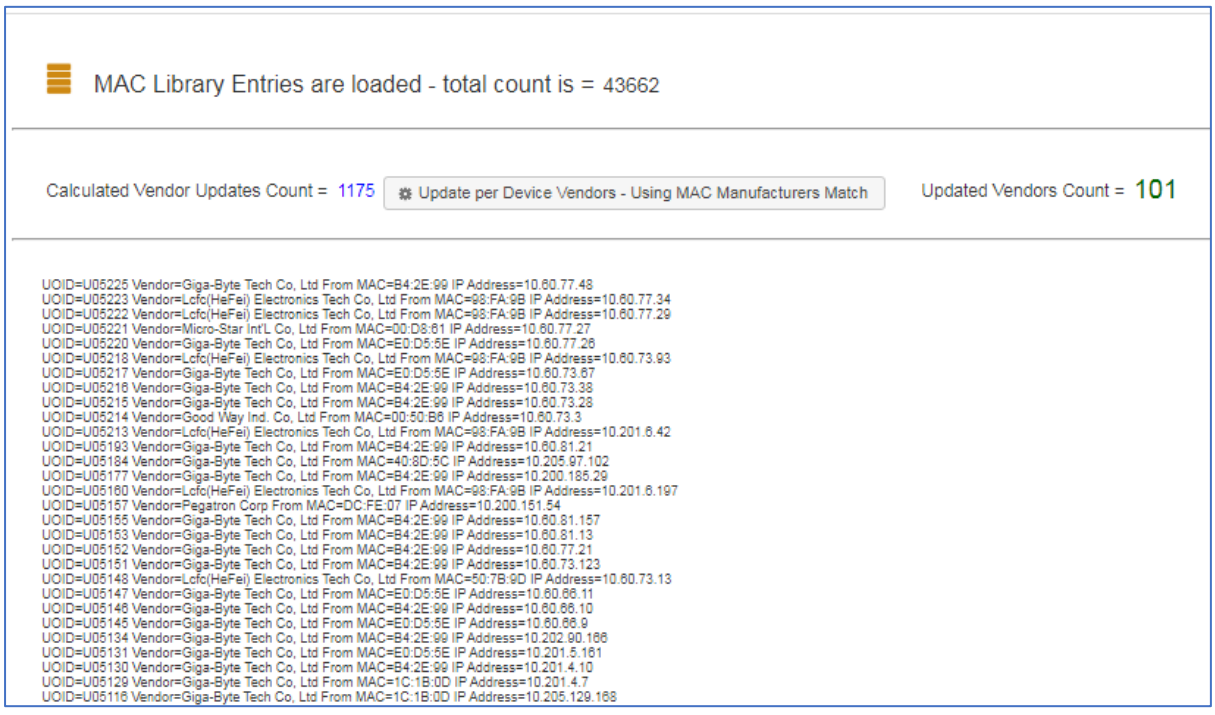
The Update Column

This links to the post discovery facility to match MAC vendor 3-byte codes to Vendor names. The system loads a list of MAC vendors and shows the count in the green highlight below.



The system also checks the discovery database checking for devices that have a MAC Address but do not have a Vendor set. That number is shown in blue.

To update Device Vendors from the MAC Vendor lookup, simply click on the Update per Device Vendors button and a running count of updates is seen as per in the yellow highlight. A list of updates is also shown in the window as below, so the user can see which devices have been updated with which vendors together with the IP address.



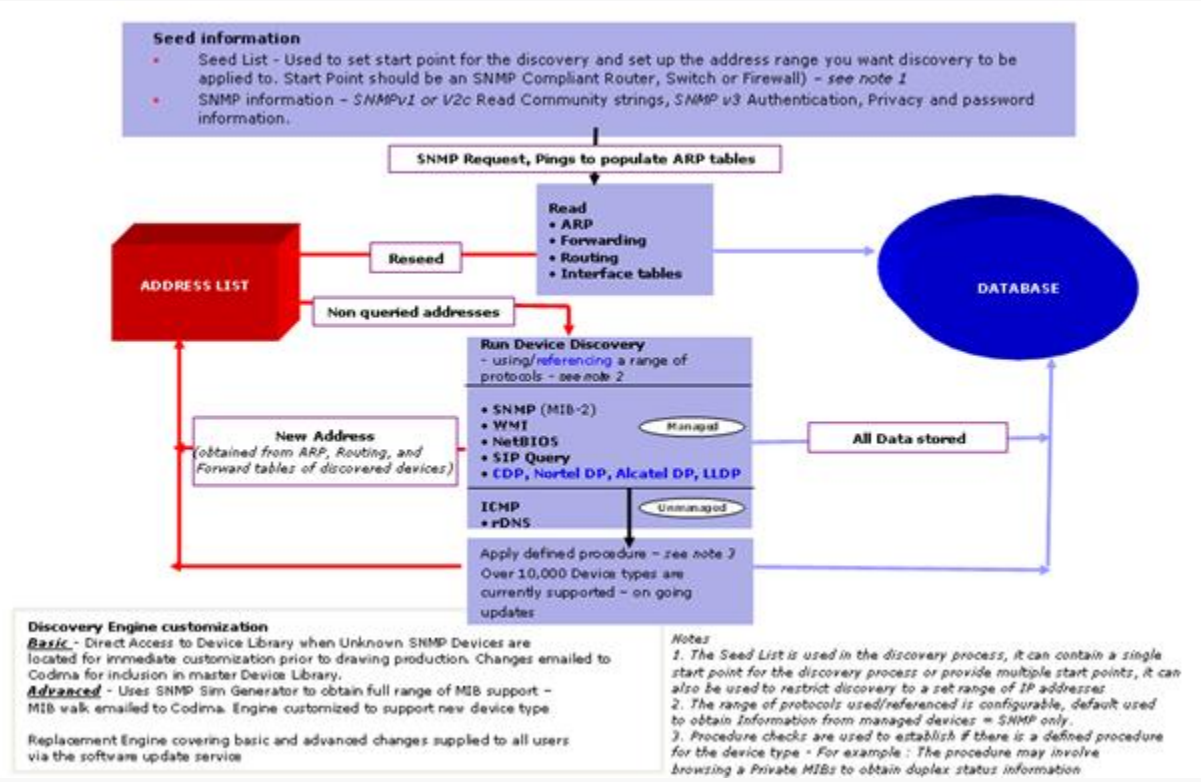
NETWORK DISCOVERY – ADVANCED INFORMATION

Discovery Engine

The Discovery Engine uses a variety of techniques to discover devices, such as inspection of ARP tables and controlled scanning techniques. This overcomes a limitation of many existing approaches, which need to know what to discover in order to draw a network. Once discovered, devices are queried using **SNMP** for **MIB** 2 and current vendor MIBs. The discovery system has a stored device list database of most current and many old generation equipment types.

The protocols used/referenced in the discovery process include SNMP, WMI, NetBIOS, SIP Query, Cisco DP, Alcatel DP, Cabletron DP, Extreme Discovery Protocol, LLDP, ICMP and rDNS.

WMI is used to obtain information on Microsoft® devices. The **Start Discovery Box** controls the protocols used in the discovery. The default settings switch off WMI, NetBIOS and SIP.



Note: *SNMPv1 and SNMPv2c and SNMPv3 protocols are supported. The system can also read SMIv1 and SMIv2 MIBs.*

How to prepare for a Discovery - Site Planning

To make best use of the Toolbox Discovery Engine you need to consider the methods used by the discovery process, and how well your site is prepared to enable it to run efficiently.

- The Toolbox Discovery Engine uses a number of protocols in the discovery and inventory process, including SNMP, WMI, NetBIOS, SIP Queries and rDNS. For the most complete inventory, you need to ensure that your devices are correctly enabled to use these technologies, this is especially important for the SNMP and WMI. See SNMP and WMI Planning entries below.

SNMP Planning

It is important that all devices that are going to rely on SNMP as the main discovery protocol are configured correctly for IP and have SNMP Agents installed. SNMP v1, v2c and v3 are supported.

User needs to provide:

- The IP address that is to be used as a start point for the discovery - ideally an SNMP compliant Router or switch.
- A suitable IP address for Toolbox Host PC
- SNMP information needed to start the discovery, i.e., Read Community strings or, authentication and privacy information – range subject to SNMP version.
- A physical connection to the network, e.g., free switch port
- The range of IP addresses to be included in the discovery process. *Note: This IP Address range applies to an optional facility that can be used to restrict the scope of the discovery*

Check list:

- **SNMP support** – Key devices need to have an SNMP Agent installed.
- **SNMP access -** You must be able to browse the discovery start point
- **SNMP community** - The correct range of SNMP Read Communities must be included in the startup parameters
- **VLAN** - The Host Workstation must be on the management VLAN.
- **Access restrictions** - Devices should be checked to ensure they are not configured with filters or “Access Lists” restricting which administration addresses are allowed.
- **Firewalls** - For discovery to work, the Host PCs IP address needs to be configured to transmit and receive as a trusted ICMP and SNMP source and destination through the Firewall.

WMI Planning

Microsoft WMI is implemented and enabled, by default, on all recent Windows systems.

Check list:

- Does the discovery engine have the correct WMI Credentials?
- Do the devices support WMI? - Discovery Engine will identify all WMI supported machines logged on the Domain it has the credentials for.

Microsoft recommends the latest service pack when using WMI.
Wrong permission means that the workstation you are running the discovery from does not have the correct WMI Credentials.

To obtain WMI information the discovery must be provided with the relevant Domain Name/User Name and Password.

Discovery Check List before Starting a Discovery

WARNING - Platforms running Discoveries must have hibernation/standby disabled.

The following check list covers some situations that can impact on the effectiveness of the Discovery Engine. Prior to running the Discovery Engine, you should be aware of these potential danger areas:

1. Switches may not respond to SNMP: The user needs to check SNMP access, SNMP community and VLAN – the **autoMap Host Workstation** must be on the management VLAN. Devices should be checked to ensure they are not configured with filters or “Access Lists” restricting which administration addresses are allowed.
2. Forwarding tables may not be accurate (e.g., Switches broadcasting instead of keeping clean forwarding tables, creating virtual broadcast domains).
3. Devices may not respond to Ping Scan - the discovery operation is blocked by a **Firewall**. Unless the Firewall is configured to allow the Host PCs IP address through as a trusted device, the **Discovery Engine** will not discover beyond the Firewall. For autoMap discovery to work, it needs to be configured to transmit and receive as a trusted ICMP and SNMP source and destination through the Firewall.
4. There may be unknown switches with a proprietary interface index: a MIB Walk and information on device type and characteristics will be required to customize/update the discovery engine.
5. Any address restrictions applied to the discovery, will limit the scope of the discovery. For example, if you have used a seed list and set the Start Discovery Settings to not do a discovery beyond the seed list.
6. Any other restrictions applied to the discovery, for example if you do not include settings in the Start Discovery - Advanced settings box to gather information on VLANs or Switch/Hub port information.
7. WMI information may not be provided - To obtain this information the discovery engine must have this option selected in the Start Discovery - Advanced settings box and be in the same Domain as the devices it is requesting information from. To address this, you can for example login on the Host PC as the Domain Administrator or you can run multiple

discoveries using different WMI credentials each time. It will identify all the Windows machines logged on that **Domain**.

For example if the **Discovery Summary Report** shows that the Host PC did not have the correct permission, it means that the workstation you are running the product from does not have the correct WMI Credentials, and Windows has subsequently not given permission for you to access the WMI RPC services on the remote workstation.

Troubleshooting a Discovery

Discovery does not start

Check that Toolbox Server is running - see Windows Task Manager Express.exe is running, if click on product Icon to Launch the Toolbox Server.

Devices Support

If a discovery does not correctly classify known Switches or Routers under a type category of Switch or Router, this is usually an indication that the devices type has not been included in the device list. It is recommended that you check the device list used by product prior to running a discovery, as it will help you establish if the key device types on your network have already been incorporated into the **Discovery Engine**.

Many thousands of device types are supported by the **Discovery Engine**. The supported device list is constantly being updated.

Missing devices, ports, or links - checklist

There are several reasons why a discovery may not cover the complete enterprise network. The following check list covers some areas that should be investigated:

1. Switches may be not responding to SNMP

User needs to check

- **SNMP access -** Can you browse the start point? Can you browse the Switches?
- **SNMP community** - Have you included all the required SNMP **Read Communities** in the startup parameters?
- **VLAN** - The Toolbox Host Workstation must be on the management VLAN.
- **Access Restrictions** - Devices should be checked to ensure they are not configured with filters or “Access Lists” restricting which administration addresses are allowed.

2. Forwarding tables may not be accurate (e.g., Switches broadcasting instead of keeping clean forwarding tables, creating virtual broadcast domains).
3. Devices may not respond to Ping Scan or other protocols - the discovery operation is blocked by a Firewall.

User needs to check

- **Firewalls** - For discovery to work, the Host PCs IP address needs to be configured to transmit and receive as a trusted ICMP and SNMP source and destination through the Firewall.

There are switches with an unknown proprietary interface index.

User needs to provide

- A MIB walk
- Information on device type and characteristics

This information is then used to customize/update the discovery engine.

5. The *Discover Devices outside the scope of the Seed list* setting may have been switched off, limiting the scope of the discovery.

Missing asset Information – checklist

There are several reasons why a discovery may not show all the expected asset information. The following check list covers some areas that should be investigated:

1. Devices may be not responding to SNMP

User needs to check

- **SNMP Support** – does the device have an SNMP Agent, is it operational
- **SNMP access -** can you browse the device
- **SNMP community** - have you included all the required SNMP Read Communities in the startup parameters
- **VLAN** - the Host Workstation must be on the management VLAN.
- **Access Restrictions** - devices should be checked to ensure they are not configured with filters or "Access Lists" restricting which administration addresses are allowed.

2. Devices may not be responding to NetBIOS

User needs to check

- If the Start Discovery - Advanced settings box settings for the discovery run included tracking NetBIOS

3. WMI information may not be provided

User needs to check

- If the Start Discovery - Advanced settings box settings for the discovery run included tracking WMI
- If the discovery engine has the correct WMI Credentials
- If the devices support WMI - the discovery will identify all the Windows machines logged on that Domain.

If the Asset report states that WMI did not have the correct permission, it means that the Host PC does not have the correct WMI Credentials, and Windows subsequently has not given permission to access the WMI RPC services on the remote workstation.

4. The Asset report may not show all the port status information

User needs to check

- If the Start Discovery - Advanced settings box settings for the discovery run included the Map Switch/Hub Port setting.

5. Asset report may not show VLAN information

User needs to check

- If the Start Discovery - Advanced settings box settings for the discovery run included the Detailed VLAN Scanning setting.

Map Switch/Hub Ports Option

Background Information – Map Switch/Hub Ports Control

The discovery can be set to:

- Just find out about Infrastructure devices such as Router/Switch connections and not gather information for example on the Workstations or Servers connected to the Routers/Switches. Typically, this setting applies when scanning a network where CDP or NDP are implemented and you are only interested in switch and router links - see example 1.
- Find all the connection information for the Routers/Switches - including non-infrastructure devices, such as Workstations - see example 2.

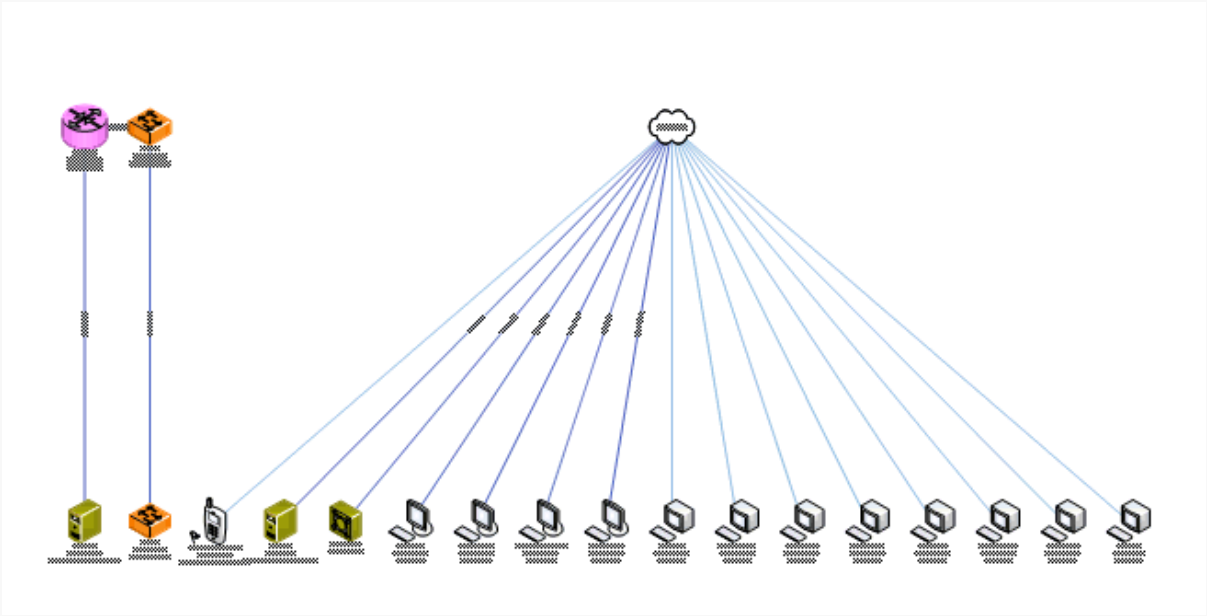
HOW TO CONTROL DISCOVERY OF INFRASTRUCTURE AND NON -INFRASTRUCTURE CONNECTIVITY INFORMATION

Tick or untick the Map Switch/Hub Ports option, as required:

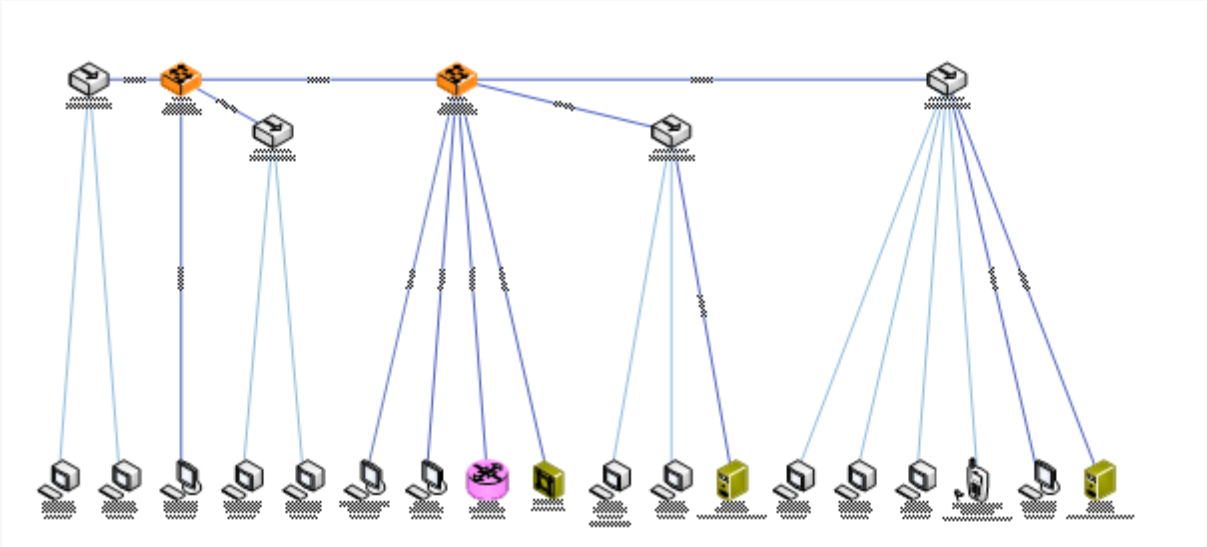
- When unticked this restricts the discovery to just finding out about Infrastructure devices such as Router/Switch connections, it will not show for example the Workstations or Servers connected to the Routers/Switches. Typically, this setting applies when scanning a Network where CDP or NDP are implemented and you are only interested in switch and router links - see - example 1 on next page.
- If you wish the discovery to include connection information for non-infrastructure devices then this box needs to be ticked - see example 2 on next page.

The two examples below are for illustration purposes only.

Example 1: Topology drawing when Map Switch/Hubs Ports option IS NOT selected.



Example 2: Topology drawing when Map Switch/Hubs Ports option IS selected.



Note: Discovery is faster if the Map Switch/Hubs Ports box is unticked, but the discovery will not obtain as much connectivity information.

Detailed VLAN Scanning

Tick '**Detailed VLAN Scanning**' to add per VLAN interface SNMP scanning using Community Name Indexing.

Note when option is ticked, the time taken to discover complex SNMP enabled devices can increase dramatically, potentially adding several hours to the overall discovery.

Background – VLAN

Virtual LAN
A group of Nodes on different physical LAN segments that can communicate with each other as if they were all on the same physical LAN segment. A Broadcast Domain within a defined set of switches.

IEEE 802.1Q
IEEE 802.1Q standard, Tag-based Virtual LAN uses an extra tag in the MAC header to identify the VLAN membership of a frame across bridges. This tag is used for VLAN and QoS (Quality of Service) priority identification. The VLAN's can be created statically by hand or dynamically through GVRP. The VLAN ID associates a frame with a specific VLAN and provides the information that switches need to process the frame across the network. Usually, a tagged frame is four bytes longer than an untagged frame and contains two bytes of TPID (Tag Protocol Identifier = 0x8100) and two bytes of TCI (Tag Control Information).

An optional two-byte Route Control Field followed by 0-15 two-byte Route Descriptor fields may also be included. If these fields are included (indicated by the **CFI** Flag) they immediately follow the EtherType field.

Tag Control Information (TCI) Format

Byte 1					Byte 2				
User Priority			CFI	VLAN identifier					
8		6	5	4	1	8			1

Embedded-RIF Route Control Field Format

Byte 1				Byte 2			
Routing Type		RD Length		D	Largest Frame		NCFI
8	6	5	1	8	7	2	1

IEEE 802.1Q header specifies the virtual LAN number, Ethernet switches use this information to decide which port(s) the frame can go to.

Protocols available for routing between VLANs include:

- Inter-Switch Link (ISL)
- IEEE 802.10
- ATM LAN Emulation

Discovery Speed and Bandwidth Control

Number of Parallel Processes

The Discovery Engine can process multiple IP addresses in parallel as a means of speeding up the inventory.

The user can adjust the bandwidth used by the Discovery Engine during a discovery.

This process uses the Discovery Speed slide bar.

Since processing one address requires up to 64kbits, this parameter effectively allows from 1 to 50 parallel operations to occur.

Whilst increasing the amount of bandwidth used can considerably reduce the inventory time it can also impact the network performance for other users. Care should be taken when performing an inventory/discovery on slow links with critical business traffic.

IP Service Discovery (SIP, WMI, NetBIOS)

SIP - VoIP Session Initiation Protocol

SIP Queries are used to obtain information on VoIP phones that support SIP.

Tick the option '**SIP Clients**' to turn on the SIP Discovery process, which can discover SIP Servers and Phones.

Background - SIP

The Session Initiation Protocol (SIP) is a communications protocol for signalling, for the purpose of controlling multimedia communication sessions. The most common applications of SIP are in Internet telephony for voice and video calls, private IP telephone systems, as well as instant messaging over Internet Protocol (IP) networks.
The protocol defines the messages that are sent between endpoints, which govern establishment, termination and other essential elements of a call. SIP can be used for creating, modifying and terminating sessions consisting of one or several media streams. SIP is designed to be independent (although not agnostic) of the underlying transport layer, and can be used with UDP, TCP, and SCTP; it can also be secured using TLS over the latter two. It is a text-based protocol, incorporating many elements of the Hypertext Transfer Protocol (HTTP) and the Simple Mail Transfer Protocol (SMTP). By itself, SIP only provides signalling; it is used in conjunction with other protocols that specify the media format and protocol to be used to subsequently communicate the media. Although SIP can carry arbitrary data, SIP is typically used to carry a Session Description Protocol (SDP) message specifying the codec and the use of either the Real-time Transport Protocol (RTP) or Secure Real-time Transport Protocol (SRTP) for (media) communication.

Windows Management Instrumentation (WMI)

1. Check **WMI Clients** box - to include WMI discovery.
2. Ensure you have set up the correct WMI Credentials in the Next Discovery Setup Panel.

Background - WMI

Windows Management Instrumentation (WMI) is a set of specifications from Microsoft for consolidating the management of devices and applications in a network from Windows computing systems. WMI is installed on all computers with Windows Millennium Edition (Me), Windows 2000, Windows XP, or Windows Server 2003. It can be downloaded for computers using Windows 98 or Windows NT 4.0. WMI is the Microsoft implementation of Web Based Enterprise Management (WBEM), which is built on the Common Information Model (CIM), a computer industry standard for defining device and application characteristics so that system administrators and management programs can control devices and applications from multiple manufacturers or sources in the same way.

NetBIOS

Tick the **NetBIOS Clients** option, NetBIOS is used to obtain information from Microsoft™ devices.

Background - NetBIOS

NetBIOS (Network Basic Input/Output System) is a program that allows applications on different computers to communicate within a local area network (LAN). It was created by IBM for its early PC Network, was adopted by Microsoft, and has since become a de facto industry standard.

SNMP Communities

Enter a list of SNMP (read) Communities separated by space characters.

This is a basic security check to prevent unauthorised access to SNMP MIBs, however the Communities can be easily 'Sniffed' using a protocol analyser such as Wireshark.

Background Information – SNMP Communities

SNMPv1 and v2c

SNMPv1 and SNMPv2c are very similar SNMP Agent protocols that are used by most currently deployed network devices. Any device that supports v2c will generally also support v1. The product uses automatic intelligence to switch from one version to the other as needed.

SNMP v3

SNMP v3 is a secure SNMP Agent protocol. Most currently deployed network devices *do not* support SNMPv3. You should never use SNMPv3 device discovery unless you are sure that the network being discovered does have devices that support v3 and is properly configured. To use v3 you need to select an Authentication and Privacy (encryption) mode, as well as passwords for each mode.

WMI Credentials

WMI credentials are supplied when the Network Discovery is set up using the **Discover** main tab. They are entered in the Credentials Passwords and Communities Panel.

The WMI credentials are entered in the **Enter WMI Credentials** section on the right-hand page. The Credentials may be tested to be correct, by clicking on the **Test WMI Domain Password** button, which is recommended.

SNMP Version 3 Credentials

Provide the following SNMP v3 Configuration parameters

- **Configuration Name:** The name of the group of SNMPv3 Settings.
- **User Name:** The name of a user.
- **Context Name:** The optional context name for an access group which defines what parts of the agents MIB can be accessed by the username.
- **Authentication Level:** The authentication level used to authenticate the query.
- **Authentication Type:** The authentication protocol used to authenticate the query.
- **Authentication Password:** The password used for authentication.
- **Privacy Type:** The protocol used to encrypt the query. Only DES is supported (not AES).
- **Privacy Password:** The password used for encryption.
- **Treat Password As Key:** When ticked the password used for authentication or privacy is treated as the key.

Background Information – SNMP versions

SNMPv1 and v2c

SNMPv1 and SNMPv2c are very similar SNMP Agent protocols that are used by most currently deployed network devices. Any device that supports v2c will generally also support v1. The product uses automatic intelligence to switch from one version to the other as needed.

SNMP v3

SNMP v3 is a secure SNMP Agent protocol. Most currently deployed network devices ***do not*** support SNMPv3. You should never use SNMPv3 device discovery unless you are sure that the network being discovered does have devices that support v3 and is properly configured. To use v3 you need to select an Authentication and Privacy (encryption) mode, as well as passwords for each mode.

Background Information - How is the Discovery Information stored?

Discovery Engine databases (SQL Database)

SQL Database - contains information obtained by running the Discovery Engine

Structured Query Language (SQL) forms the backbone of most modern database systems - the Discovery Engine uses an SQL database to store discovery results. SQL databases are 100\% open, so SQL queries can be run on them. The installation program installs and configures the SQL database connector to the discovery database.

SQL Database range

The following SQL Databases are used:

- MySQL Database – Codima Software Version 8.00 or later
- MySQL Database or Microsoft Access Database - Codima Software Version 7.60 or earlier

Storage

MySQL - .sql stored in ..*autoMap**data*\

Database structure

The Discovery Engine normally relies on a single database for static and network specific data, the database contains data gathered from the network or processed from it along with all the static tables such as the vendors' identifiers.

The database schema is designed to store a detailed representation of a network device across multiple tables. Such a network device is made of many subcomponents, and the subcomponents themselves are also stored in many tables. For example, a router is potentially made of a chassis and some modules, and therefore that router is represented in the database with those subcomponents.

The physical interfaces found on the modules are also subcomponents. The subcomponents of a device are stored as rows in the database. Within most tables, the Unique Object Identifier (UOID) uniquely identifies each subcomponent. The UOID is the primary key for most tables. Therefore, retrieving all the properties for a particular network device requires a Structured Query Language (SQL) JOIN operation on two or more tables using the UOID.

The UOID for a new row in the database is automatically generated by the application and is guaranteed to be unique.

Relationships between network subcomponents are achieved using the identifier of one subcomponent within a row of data corresponding to another subcomponent. This second key relationship enables an association of one network component with others. In many cases, there are one-to-many relationships. For example, network interfaces are represented in the ntxcmib2interface table. The interface index intIndex is the link to the interface-specific data tables.

Each device is described into multiple tables, linked by a unique object ID.

Table Naming convention

ntx (c) (mib2) - c = client
ntx (c) (priv) - c = client , priv = private mib

ntx (c) (proc) - c = client , proc = processed
ntx (c) (set) - c = client , set = setup
ntx (c) (dna) - c = client , dna = dna internal
ntx (a) (ref) - a = admin , ref = reference
ntx (a) (exp) - a = admin , exp = expert interface

There are four table categories:

1. Debug - stored Debug traces: Internal use only.
2. MIB2 - stores raw data collected from mib2 OIDs 1.3.6.1.2.1
3. Vendor - stores vendor data from private enterprise mib OIDs 1.3.6.1.4.1
4. Generic - produced based on mib2 and vendor tables to provide a coherent representation of each device, including its content, configuration and connectivity.

Tables include:

- ntxccprivcardInfo - This table describes the hardware configuration of the modules of a chassis:
  - UOID
  - Module Slot
  - Module Type
  - Number of Ports
  - Software, Hardware and Firmware versions
  - Module Serial number
  - Part number
- ntxccprivchassis
  - UOID
  - Serial number
  - Type
  - Number of slots
  - Software, Hardware and Firmware versions
  - Dimensions
  - Rack (manual input)
- ntxcprivciscocdp - Describes the connectivity between Cisco devices, as given by CDP (Cisco Discovery Protocol).
- ntxcprivciscohsrp - Describes the **HSRP** configuration for a Router.

- ntxcdnadiscovery - the list of all the IP addresses found and their process status.

- ntxcprocdialup - some routes are not stable in the routing tables. Usually, those routes are Remote Access lines that are up when a distant user dials into the network.
- ntxcprocl2topology - The physical connectivity access Layer 2 Switches.
    - This table is computed based on the hardware configuration and the Forwarding table 1.3.6.1.2.1.17.4.3 of each switch and the vendor-specific topology protocols.
    - This table gives the Layer 2 physical topology. Each port of each device is connected to another port, it covers speed, duplex status, port type, VLAN, Spanning Tree group etc.

- ntxcmib2stg - All the Spanning Tree configuration across all the switch ports.
- ntxcprocsubnet -
    - For every IP addresses of every object, dnaSubnets indicates its *interface index* and its *subnet*.
    - For each *subnet*, dnaSubnets indicates the *broadcast address*, *max* and *min IP* addresses and theoretical *number of addresses*.
    - The *name* and *description* fields are for the user.
    - *InRouterIp* is the address of the last router to cross to reach *subnet* when coming from the Toolbox server.
    - *DateFound* indicates the first time an address IP on this *subnet* was identified.
    - *ArpDate* indicates if/when the *subnet 's* ARP table was queried.

- ntxcprivvlan - table of all the VLANs

- ntxcmib2arp -This table contains all the devices, both IP and MAC address, that have been heard within the last 5 minutes by that interface.

- ntxcmib2fdbinterface - Forwarding Interface Table: each IP address where any data can be sent to, through this Interface.

- ntxamib2InterfaceTypes - Used with the mib2interfacetypes to identify the type of the interface: Ethernet, ISDN, etc

- ntxcmib2Interface - A description of the interface, sometimes giving the slot and port.

- ntxcmib2IpInterface - The IP address and mask of the interfaces with an IP address.

- ntxcmib2mactofdbint - Matches each MAC address with an interface index.

- ntxcmib2Routing - This table is a copy of the Routing Table 1.3.6.1.2.1.4.21 of the object identified by the UOID.
    - To reach *Subnet* with *Mask*, the next router's address is *Nexthop*
    - *Metric* is the distance in hops (routers) to the destination *Subnet*. >
    - Metric2, Metric3 and Metric4 are not used by RIP, only OSPF.
    - Protocol is the source of the route (RIP, OSPF…)
    - Type indicates if the route is static or dynamically learnt.
    - Age indicates how long that route has been learnt or configured by the router.
- ntxcmib2sys - This table stores all the mib2 System 1.3.6.1.2.1.1 data: location, type, name etc.
- ntxcprocnetworkobject - The NetworkObject table is the reference table as it includes all the devices discovered and created. A Unique Object IDentifier identifies each device (object) by combining hostname, sysObjectId and IP address, and is used in all object-related tables.

The PrimaryIPAddress is the original address found for this object.
The ObjectType value corresponds to the ntxarefobjectType table and identify router, switch, workstation, etc
The PublicCommunity and PrivateCommunity are the SNMP ReadOnly and ReadWrite communities.
Hostname is the sysName 1.3.6.1.2.1.1.5
VendorID is an index into the ntxarefianavendor table to identify the vendor of the device.
ProductID is an index into the ntxarefsysObjectVendor table to identify the type/model, based on the sysObjectID 1.3.6.1.2.1.1.2.
CreationDate is the first time this object was discovered.
LastUpdated is the last time this object was seen.
ProblemFlag and DeleteFlag are for future use.

- ntxprivsynoptics topology - The Layer 2 topology given by the SynOptics devices.
- ntxarefianaVendor - The IANA is an official IEEE body in charge, among other things, to assign a Mib OID to each vendor where to put their private Mib. In the Mib tree, private/enterprise mibs are positioned in 1.3.6.1.4.1. The following number is vendor specific and corresponds to the VendorID index. For example, 9 for Cisco and the Cisco private mib will be found at 1.3.6.1.4.1.9.
- ntxarefmib2interfacetypes - When querying the type of each interface via the Mib2 mib2iftyp OID, a value is returned. The mib2interfacetypes translates that value into its real meaning: Ethernet, ISDN etc.
- ntxarefs5ChassisType - This table includes all the Chassis types found in the s5Top topology derived from the SynOptics / Bay Networks topology protocol. S5Top encompasses the devices from those vendors since 1994.

- ntxarefsysObject - In the Mib2/system table, the sysObjectID describes the type of the device. The value is 1.3.6.1.4.1.X.Y.Z where X is the vendor and Y and possibly Z the model of the device.

Polling

The Discovery Engine polls the SQL databases every second.

INVENTORY Feature

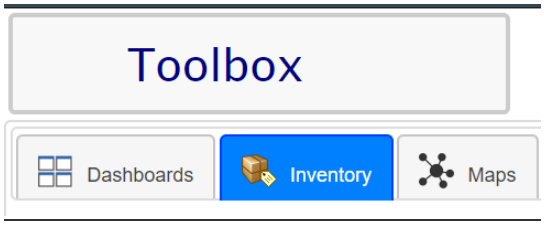
Introduction to Inventory

The **Inventory** feature provided in all Toolbox products, enables deep exploration of the MySQL asset Database using a consistent and compact interface. It primarily uses the Database created by a network discovery but the easy-to-use ITIL function allows additional details to be added including adding extra devices. It is cross integrated with the Toolbox web map. The **Inventory GUI** is very compact with no complex menu drill downs. A layered tabbed structure automatically organises Asset views.

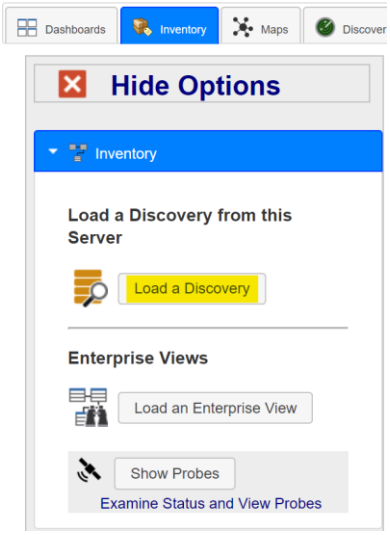
Loading an Inventory

The information that can be found in the **Inventory** is received from a **Network Discovery**, so in order to use this feature you must first complete a Discovery of the Network. For help on this see a previous chapter titled **DISCOVERY Feature**.
Once a Discovery has been performed no additional configuration is required to use the Inventory feature

The first step is to navigate to the Inventory panel found in the top left corner of the Toobox GUI

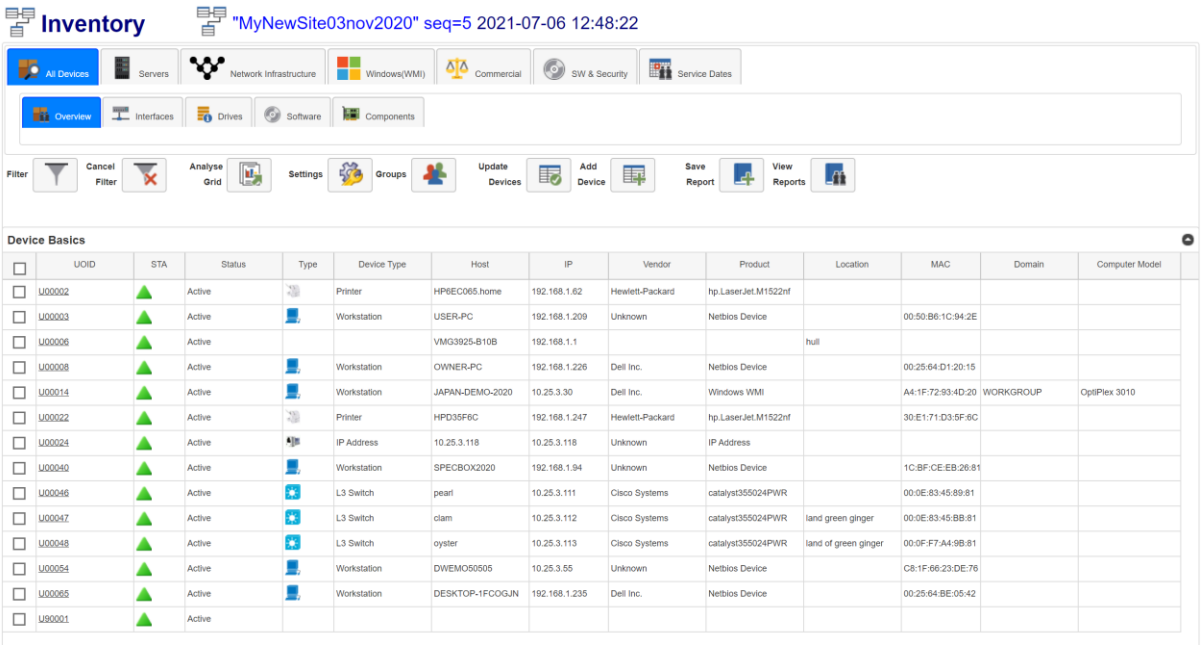


In order to view the information the Discovery uncovered you must load a discovery from the side panel, marked below in yellow (The side panel may be hidden requiring you to click the **Select Discovery and more** tab on the far left side of the screen to view it).



A window will now appear where you may choose which Discovery you would like to view, do this by clicking on it.

After selecting a previously saved Discovery, you will be greeted with an Inventory Explorer Report as seen below. This report is titled **Device Basics** and lists all discovered devices along with details of each device.

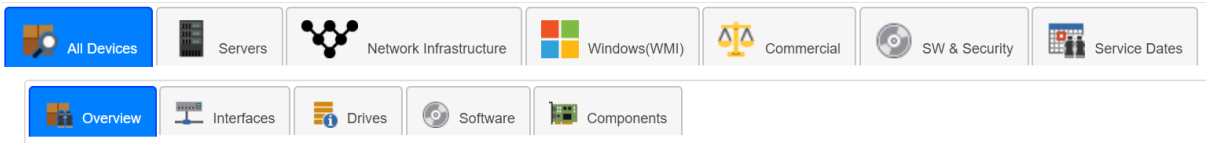


UOID	STA	Status	Type	Device Type	Host	IP	Vendor	Product	Location	MAC	Domain	Computer Model
U00002		Active		Printer	HP6EC065.home	192.168.1.62	Hewlett-Packard	hp.LaserJet.M1522nf				
U00003		Active		Workstation	USER-PC	192.168.1.209	Unknown	Netbios Device		00:50:B6:1C:94:2E		
U00006		Active			VMG3925-B10B	192.168.1.1			hull			
U00008		Active		Workstation	OWNER-PC	192.168.1.226	Dell Inc.	Netbios Device		00:25:64:D1:20:15		
U00014		Active		Workstation	JAPAN-DEMO-2020	10.25.3.30	Dell Inc.	Windows WMI		A4:1F:72:93:4D:20	WORKGROUP	OptiPlex 3010
U00022		Active		Printer	HPD35F6C	192.168.1.247	Hewlett-Packard	hp.LaserJet.M1522nf		30:E1:71:D3:5F:6C		
U00024		Active		IP Address	10.25.3.118	10.25.3.118	Unknown	IP Address				
U00040		Active		Workstation	SPECBOX2020	192.168.1.94	Unknown	Netbios Device		1C:BF:CE:EB:26:81		
U00046		Active		L3 Switch	pearl	10.25.3.111	Cisco Systems	catalyst355024PWR		00:0E:83:45:89:81		
U00047		Active		L3 Switch	clam	10.25.3.112	Cisco Systems	catalyst355024PWR	land green ginger	00:0E:83:45:BB:81		
U00048		Active		L3 Switch	oyster	10.25.3.113	Cisco Systems	catalyst355024PWR	land of green ginger	00:0F:F7:A4:9B:81		
U00054		Active		Workstation	DWEMO50505	10.25.3.55	Unknown	Netbios Device		C8:1F:66:23:DE:76		
U00065		Active		Workstation	DESKTOP-1FCOGJN	192.168.1.235	Dell Inc.	Netbios Device		00:25:64:BE:05:42		
U90001		Active										

Navigating Inventory Tabs

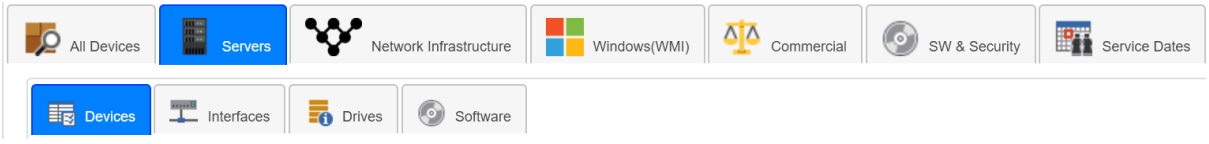
There are two sets of Tabs in Inventory (Major and Minor tabs). These are used to select the type of report you are looking for; examples can be found below.

All Devices Tab



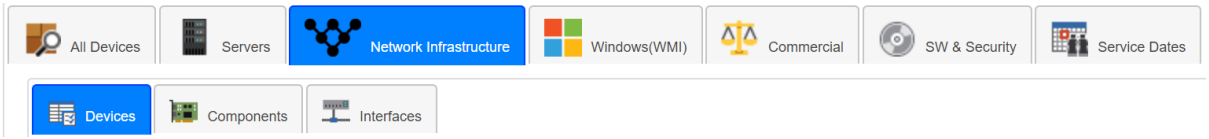
This is a general overview of all devices in the Inventory Database.

Servers Tab



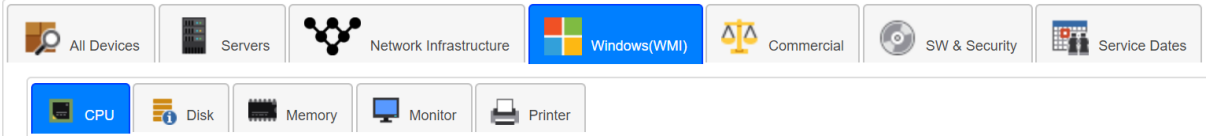
This tab filters devices that identified as Device Type equals Server.

Network Infrastructure Tab



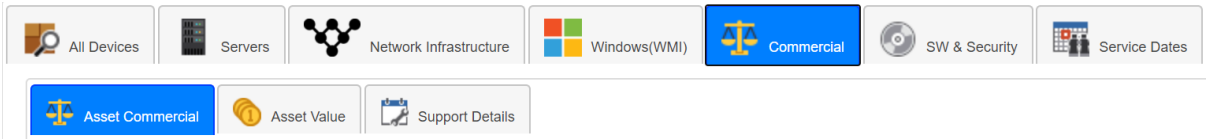
This tab lists devices identified as routers or switches.

Windows Tab



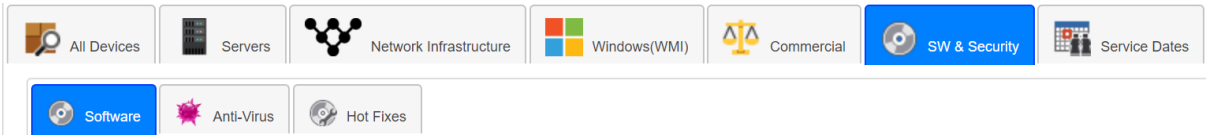
This shows a list of devices that are Windows based and support WMI (windows management instrumentation). WMI supports a large range of device metrics that can be seen in the Drill Down Reports.

Commercial Tab



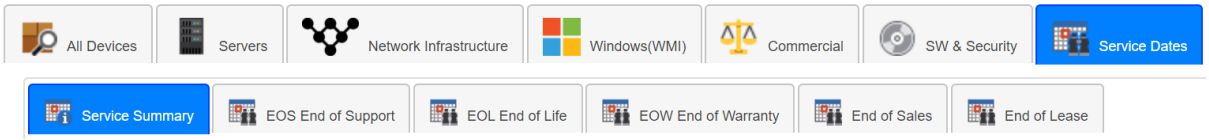
This tab focuses on Product Value, Depreciation and Support information and contact addresses.

Software and Security Tab



The tab analyses installed software, anti-virus and its state plus Hot Fixes installed (patches).

Service Dates



This tab summarises EOS, EOL, Warranty details, End of Sale, and Lease Details.
The Minor tabs under Service Dates filter devices that are for example outside their warranty or End of Life. The Update Devices feature can be used to set each metric such as warranty or end of life in conjunction with the Filters feature. For example, filter all devices of type Cisco Model 4508, and then set EOS, EOL etc in one simple Update operation. For a more in depth guide on this, see the next section.

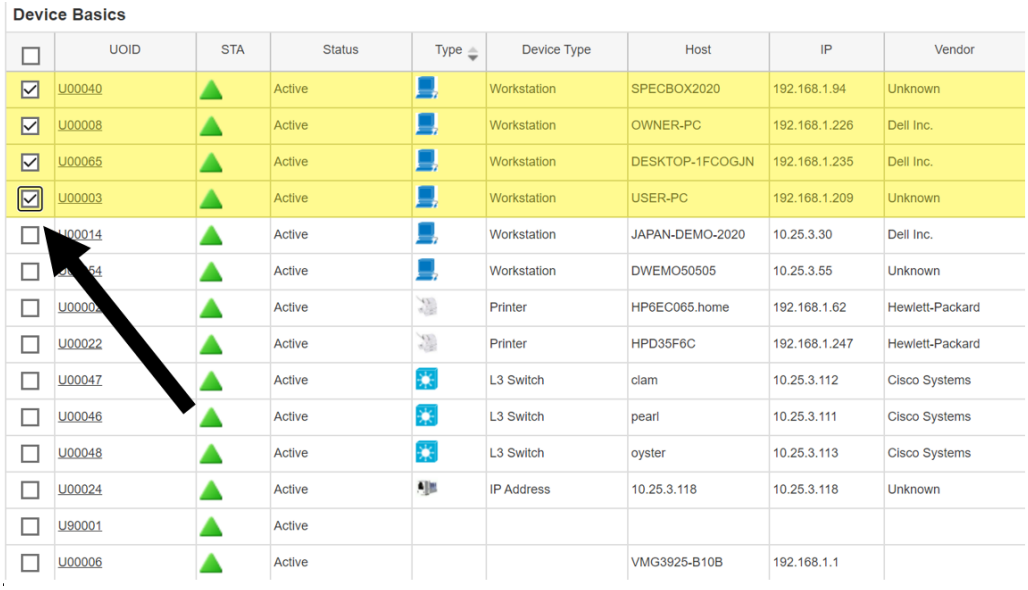
Using Toolbox as an ITIL Product

Toolbox shows an extensive list of device details harvested from the Discovery Engine using SNMP and from Windows products using WMI. The ITIL aspect of the product enables the user to add some extra details, such as detailed Location, Commercial details or modify the details from the Discovery Engine.

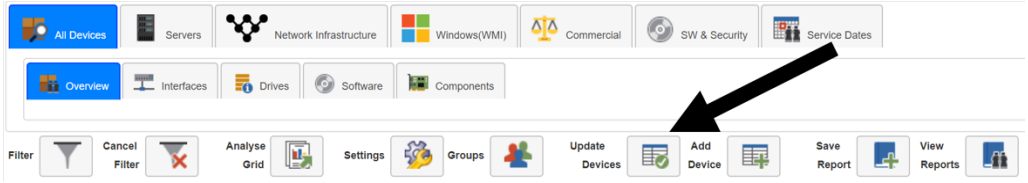
The Inventory system uses the Discovery Engine to populate the device database. Very many fields are setup automatically by the Discovery Engine, but fields such as detailed Location, Suppliers, Monetary Values, Warranties, and device state like Scrapped or In Storage cannot be set automatically. They need to be setup by the user, to do this see the guide below:

Updating Device Information

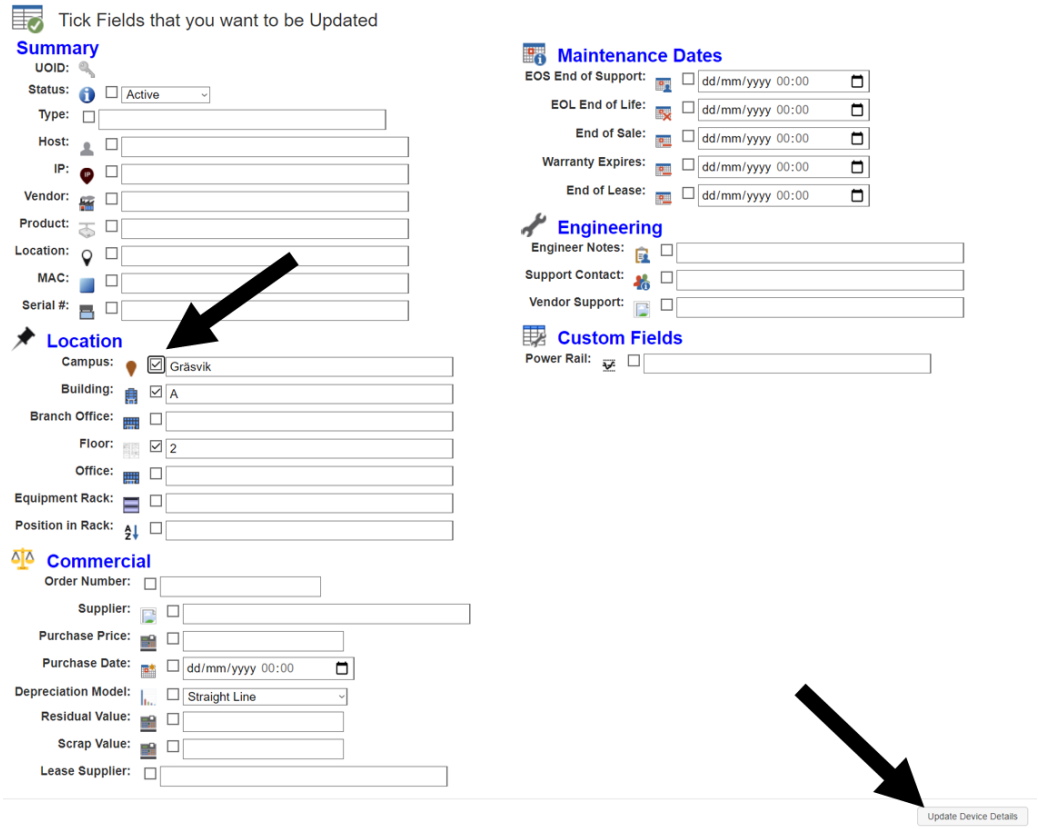
1. Firstly, you must navigate to the inventory tab and load a Discovery to see a list of discovered devices. You may also choose to use the filter option to narrow down the list to specific devices.
2. Next tick all the devices you wish to update. You may only want to update one device, but you have the option to update as many devices as you want all at once.



3. Click on the **Update Devices** option to edit their information



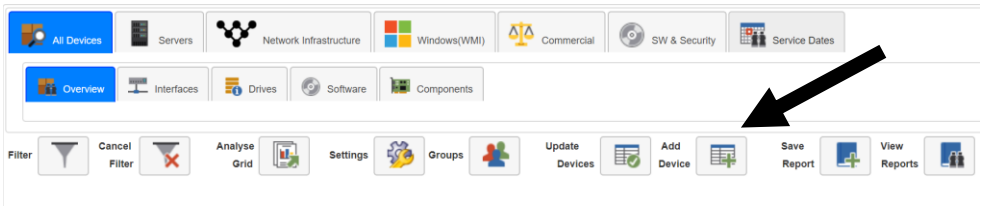
4. A new window will appear, with fields that you can update manually. Remember that updates will only be registered if the Check box next to the field is ticked and **Update Device Details** button is clicked at the bottom of the window.



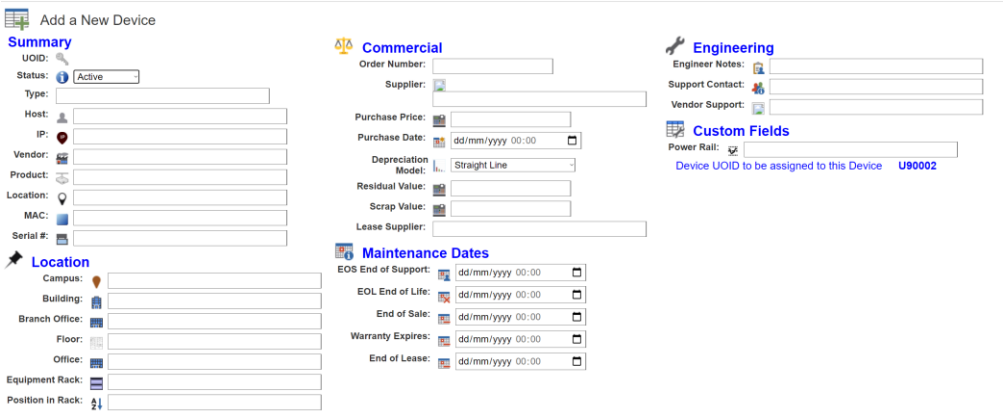
Adding New Devices

You may wish to add a new device to your Inventory since it was not discovered automatically, this could be because the device was in storage or offline during the discovery. To do this complete the following steps:

1. Click on the **Add Device** option



2. A new window will appear where you can input all the relevant information for the device in question.



3. Once done adding the relevant information make sure to click the **Add New Device** button at the bottom of the window to save the device.

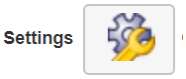
Tip: For multiple devices with most details the same for example Product Type, Supplier, Commercial Values, then its quicker to only add UNIQUE information during the Add Device stage. When all devices have been added, select them all in the Main Grid (or use a Filter to find them) then click Update Devices to set all the Common Details in one operation.

Adding Custom Fields (*User Updateable Fields*)

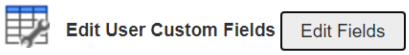
Toolbox supplies a large range of predefined fields such as Location, Commercial and Maintenance. In addition to these, there are up to 30 Custom Fields allowed. These Custom Fields can be updated by the user (*User Updateable Fields*). These extra fields behave in the same way as other built in standard fields with no restrictions meaning they are used in **Filters,** in Analytics, and Summary features. New fields are added in one click, then the attributes of the user field can be set up.

To access the setting for Custom Fields:

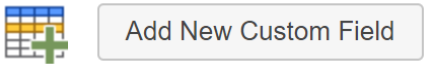
1. Click the **Settings** option in the **Inventory** GUI



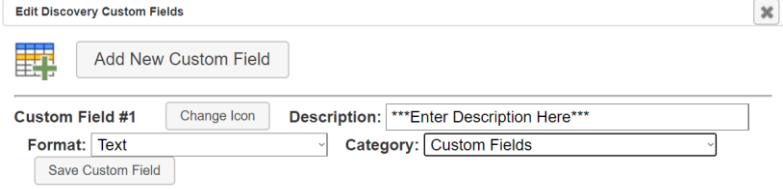
2. Click **Edit Fields**



3. Then click **Add New Custom Field**



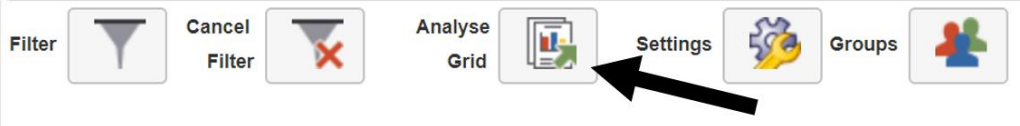
4. Now you may change the icon, description, format, and category of the Custom Field to suit your needs.



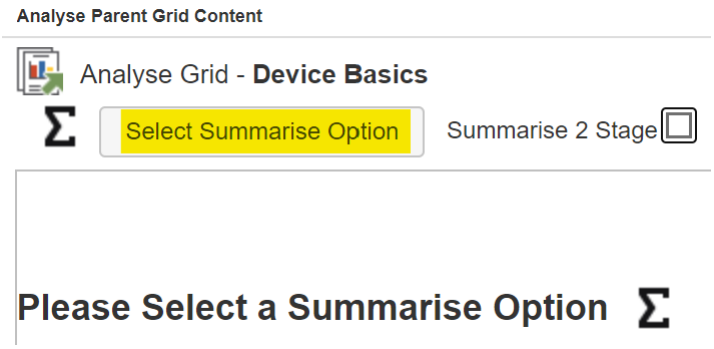
Note: As with other products, changing the details for a slot, need to be done with care, so as not invalidate existing usage of that slot. Minor changes are not typically a problem, such as changing the spelling or the Icon.

Analysing and summarising the information database

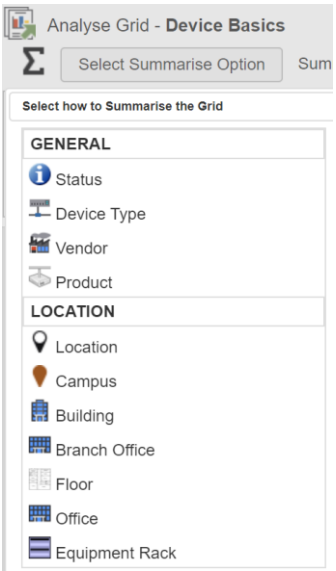
This feature is launched by clicking on main GUI interface **Analyse Grid** as below:



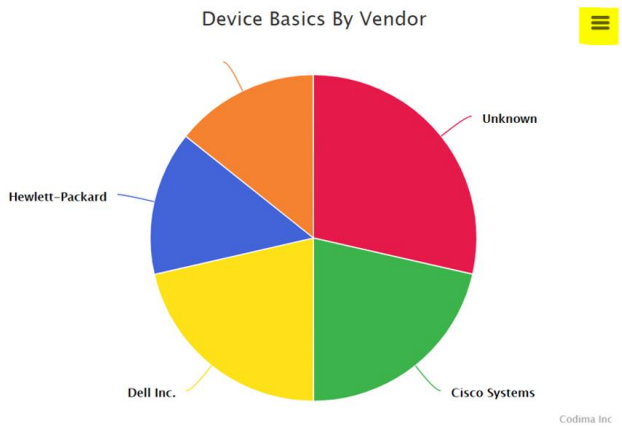
The following interface appears in a Popup window. Click on **Select Summarize Option** to configure what information to display.



The next action is to select a Summarise type from the Menu. Note the contents of the Menu follow the field columns in the Parent Grid. In the case below, the Field list follows the **Device Basics** grid contents.

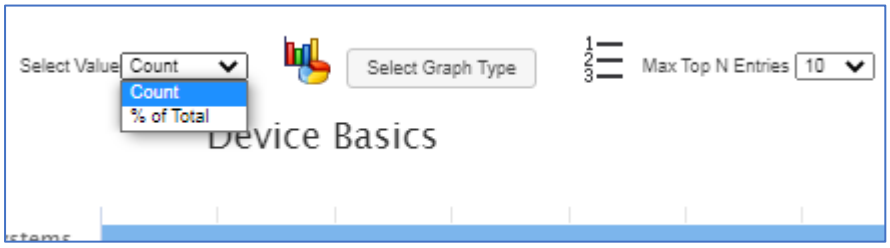


Note Fields are separated into functional groups **General** and **Location** in this case.
To create an analysis simply click on one of the options, such as vendor then you will be presented with a graph, like this:

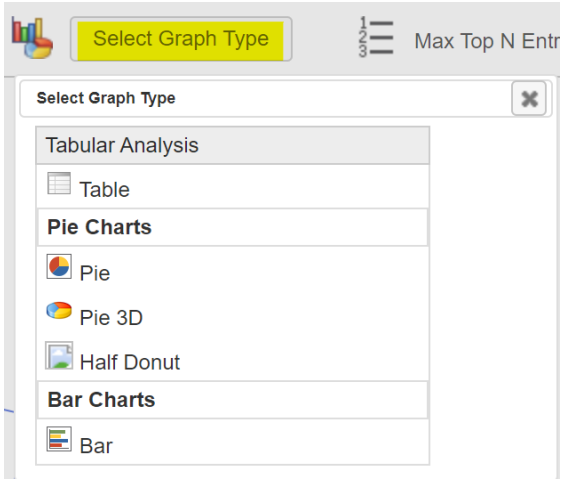


By hovering over one of the sections you will be presented with the value that section represents. You may also export the graph into several different formats including PDF by clicking on the menu icon marked above in yellow.

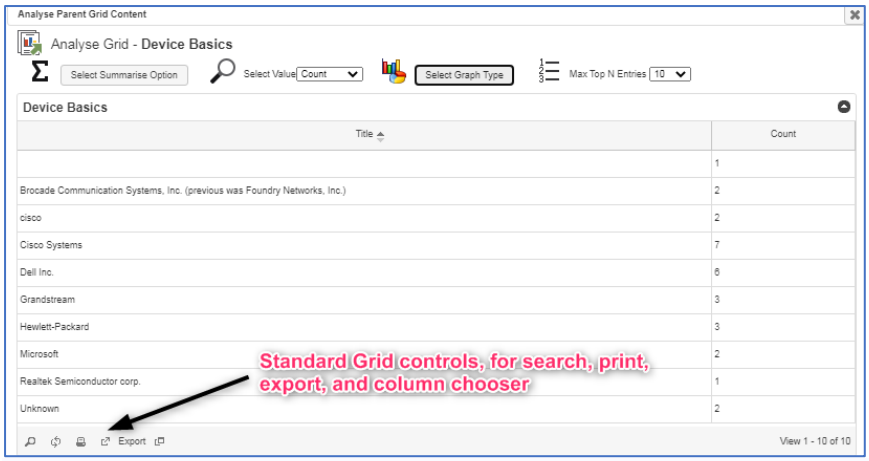
The values selector allows a choice between counts and % values for this Parent Grid Analysis type (other options are available for Sales type grids).



You are not limited to using Pie Charts, by clicking **Select Graph Type** you will be presented will several alternatives.



Tabular Analyses using Grids can also be created to show results in columns with multiple values for some Fields like Sales Values. Grids also allow numeric CSV (Excel) output plus all Grid Export formats. The Grids allow Sort, Search and Column Entries selection. The grids can also be resized per column and the whole grid in the dynamic Toolbox GUI. See below:



The grid output format allows further analysis plus the ability to Export the results to Excel for example, or other user defined processing.

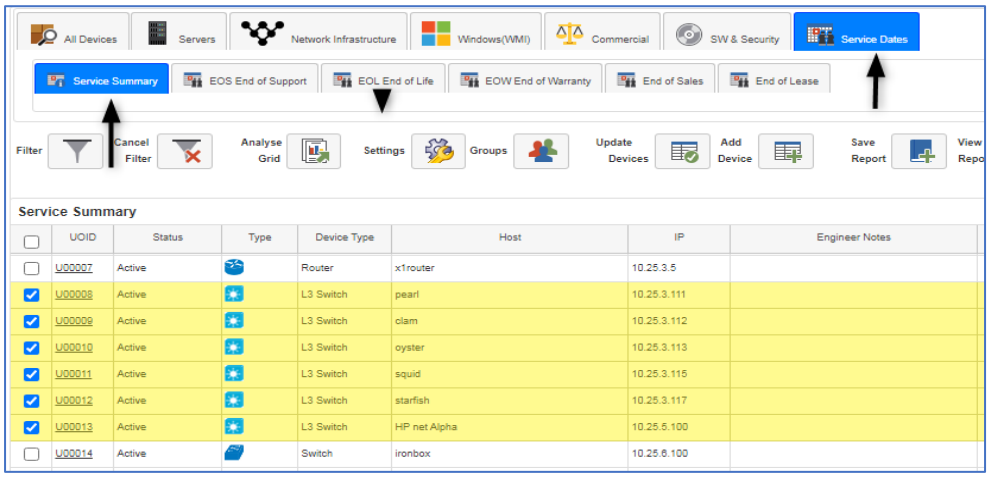
Scenarios

Toolbox presents several standard situations with tips to simplify updating the Database.

Service Dates for a particular Device Type

First click the **Filter Icon** to setup a match for the target Device Type if there are many devices, alternatively, if there are just a few devices that can be located in the Main Grid easily, one can just tick those devices without filtering first.

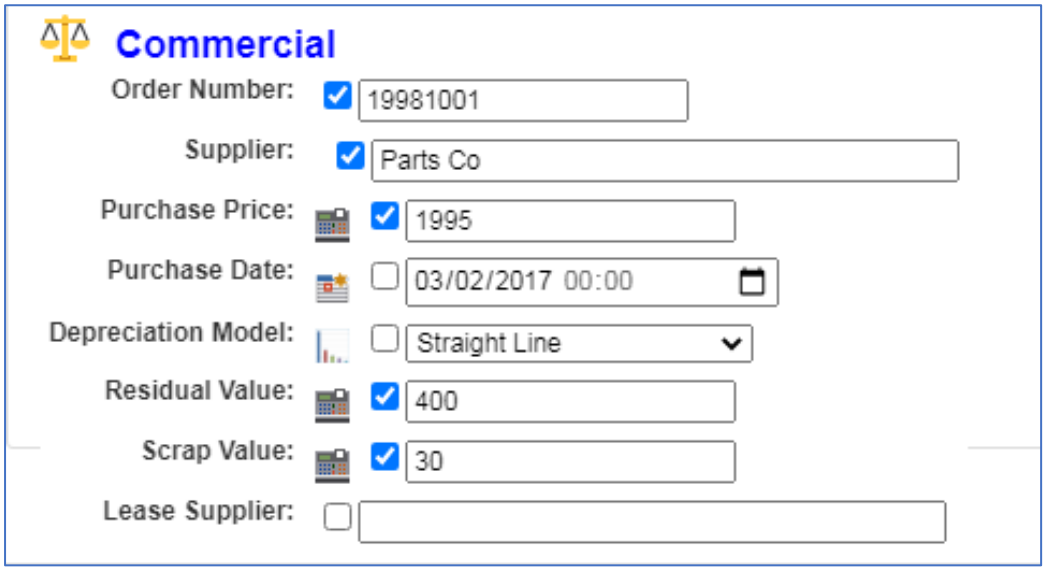
Note the **Service Dates** tab main tab and **Service Summary** minor tab have been selected to review existing details, as a convenience.



The Popup appears as below. Here we have chosen to update the devices with EOS, EOL and End of Sale, as they are all the same device model.

Set Commercial Details for One or more Devices.

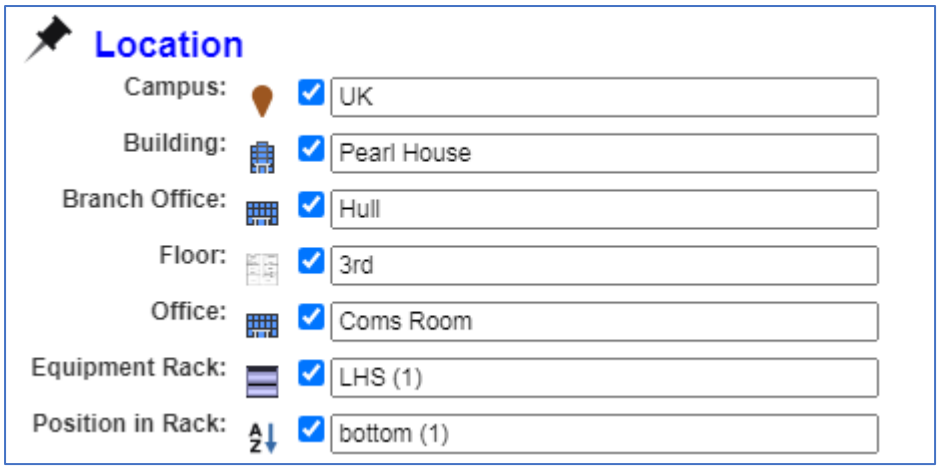
Decide how to select the devices that are to have Commercial details updated. Selecting the **Commercial Tab** is useful to update existing commercial details. Manually, select one or more devices, or setup a **Filter** to show the devices to update in the Main Grid. For a single update simply click on the UOID _____ link and edit under **User Updates** tab.



In this example we are updating commercial values and the supplier and order number.

Set Location Information for One or more Devices.

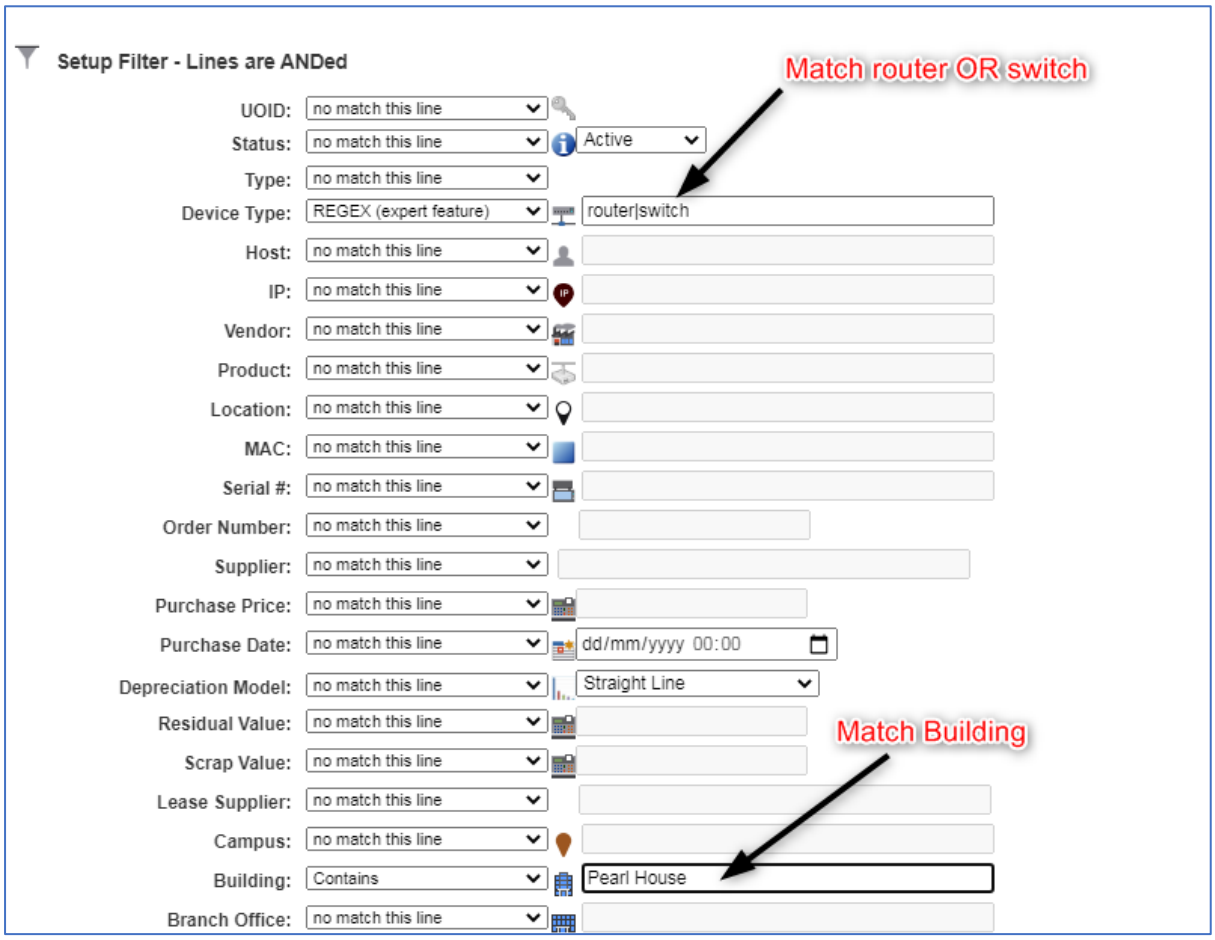
Decide how to select the devices that are to have location details updated. Either manually select one or more devices, or setup a Filter to show the devices to update in the Main Grid. For a single update simply click on the UOID _____ link and edit under **User Updates** tab.



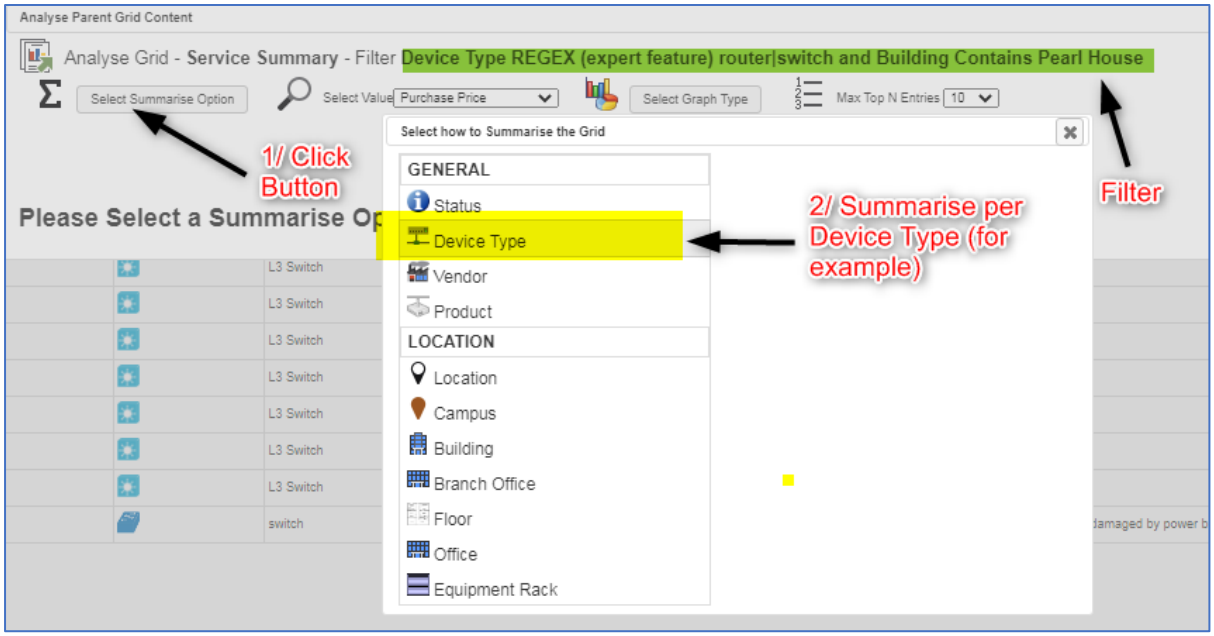
In this example we are updating all **Location Details**, probably for a single device as the Equipment Rack and position are specified.

Calculate the Router and Switch Commercial Values in a particular Building

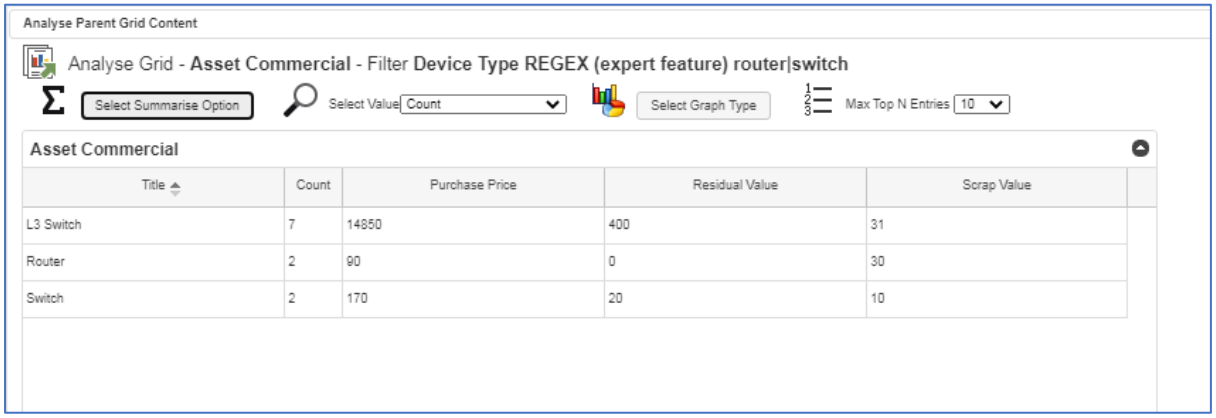
First set up a **Filter** to match the Device Types and the Building name match.



Next click on the **Analyse Grid** main icon, to launch the **Analyse Grid Popup** as below, note Filter settings are carried through and used in the Summarise operation.



Next click on the **Select Summarise** button, here we have chosen Device Type to summarise. A pie chart appears, to see the values directly, swap to Table display format by clicking on the **Select Graph** button.

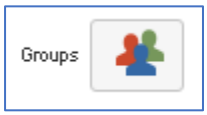


This Grid may be exported, columns removed, printed, sorted and filtered as it is a normal Toolbox Grid.

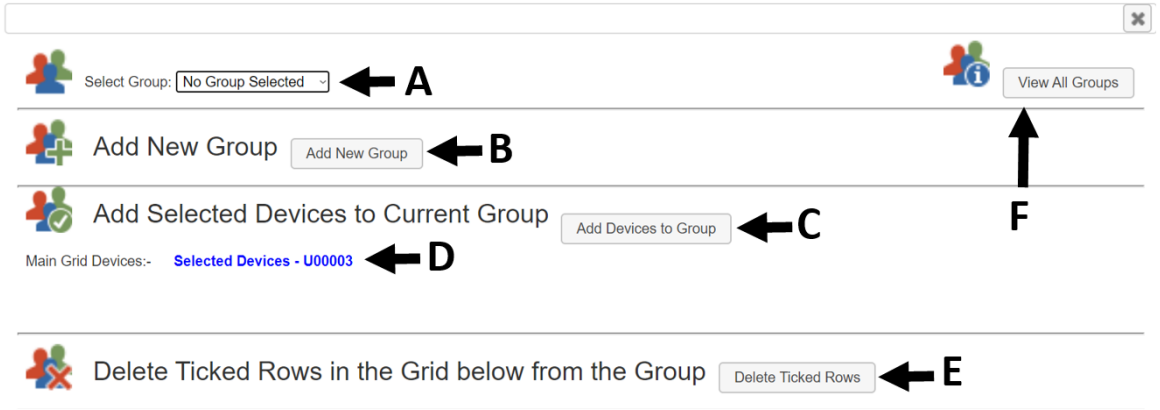
Using Inventory Groups

The system supports an unlimited number of Groups, and a device can be in multiple Groups (100s). Groups are created by the user. These groups are specific to Inventory and are separate from the product Groups used in Netflow etc.

The Groups feature is accessed by clicking on the icon below:



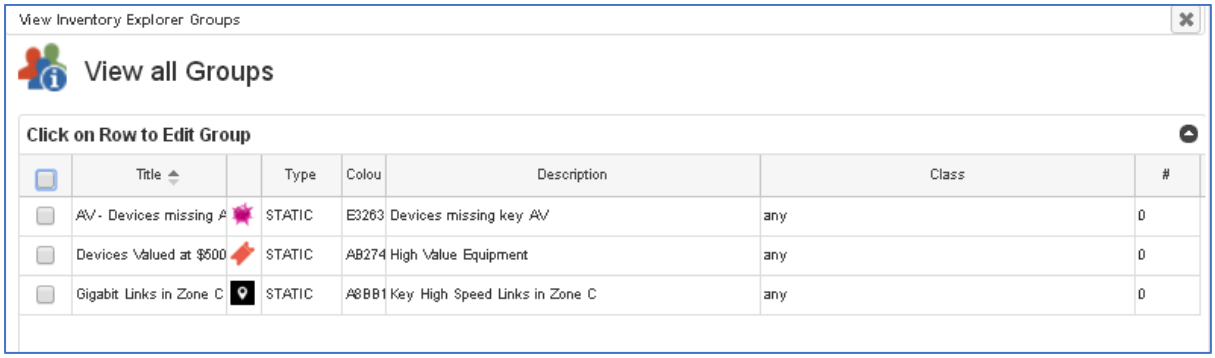
The main Groups Control dialog appears as below:



A. Select a Group.
B. Create a New Group
C. Add devices to the selected group.
D. Devices that have been ticked in the Main Grid.
E. Open a Grid and select devices to remove from the selected Group.
F. View all the Groups that have been setup.

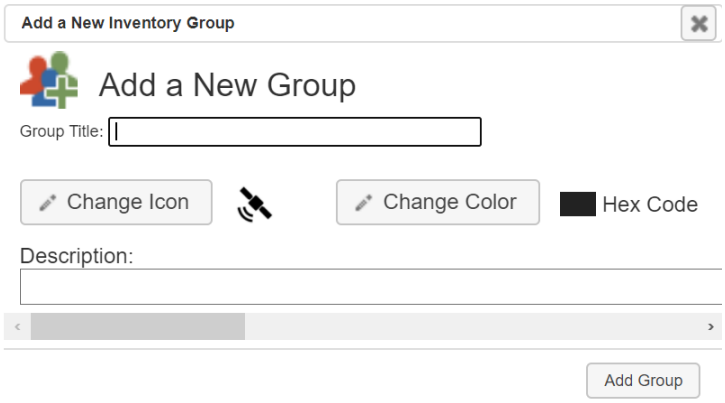
Viewing the Groups

Click on the **View All Groups** button to see the currently setup Groups as below:



Adding a New Group

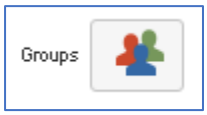
Click on the **Add New Group button** to add a new Group where you have to input a Group Title, optionally you may also change the Group Icon, change the Group's colour, as well as adding a description.



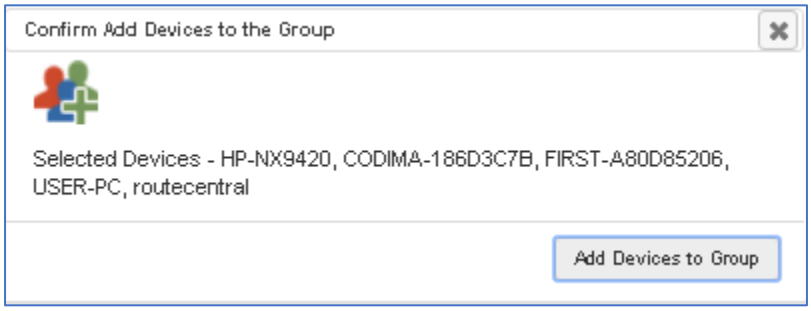
Adding Devices to a Group

In the main report grid tick the devices that are to be added to the Group. Use Filters to automatically select devices to be added.

Now click on the Group Icon.



First select a Group in the main Group dialog. Next click on the **Add Devices** button.



The dialog lists the devices to be added. Click on the Add Devices to Group button to complete the operation.

Removing Devices from a Group

To remove devices from a Group first select a Group using the Select Group drop down menu at the top of the Groups dialog so that grid appears showing current Group members.

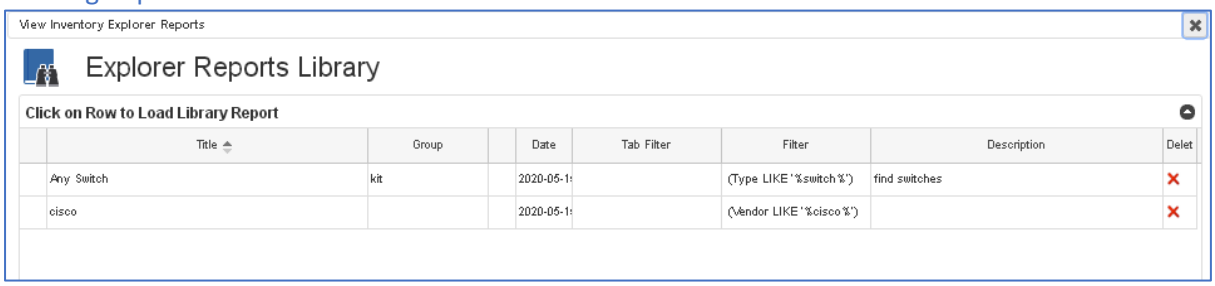
Tick Device rows that are to be removed from the Group. Click on the Delete Ticked Rows to confirm deletion of the devices from the Group.

Inventory Explorer Reports

Inventory Explorer Reports are accessed by clicking on one of the icons below.

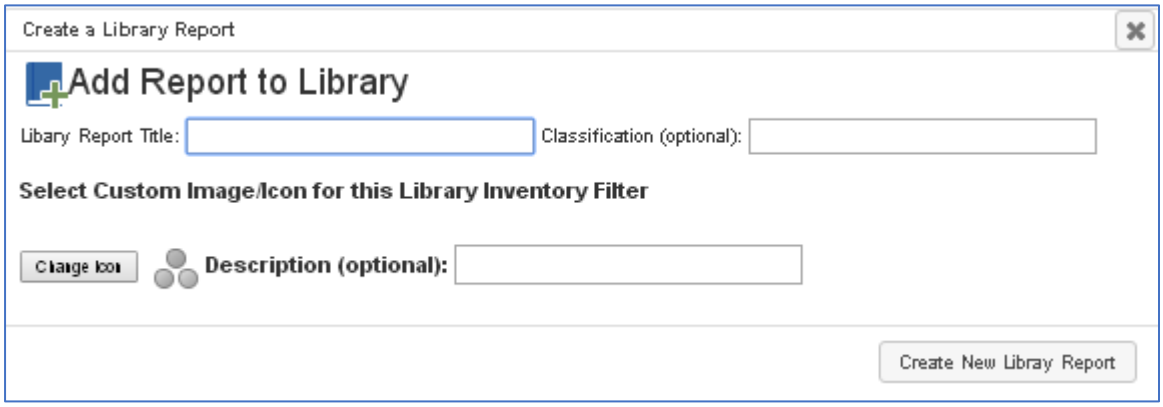
Click **Reports** to **see** the inventory explorer report list and click **Save Report** to **add** a new inventory explorer report to the library.

Viewing Reports



To view a Report simply click on a Report Row in the Grid.

Adding Reports

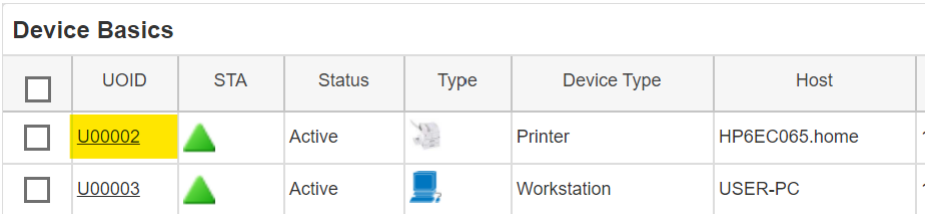


New Reports can be created by clicking on the Save Report icon. Details can be filled in as above. The Report Title is required; the other options to associate an Icon, a Classification and Description are optional but recommended.

A new Report would typically be created after Filtering an existing main grid report, for example to Filter on location, Asset Value etc.

Drill Down Inventory Explorer Reports

From the Main Grid the Device Identifier (U00099 format) can be seen underlined. Click on the link to see the Device Drill Down Inventory Explorer Report (Marked below in yellow):



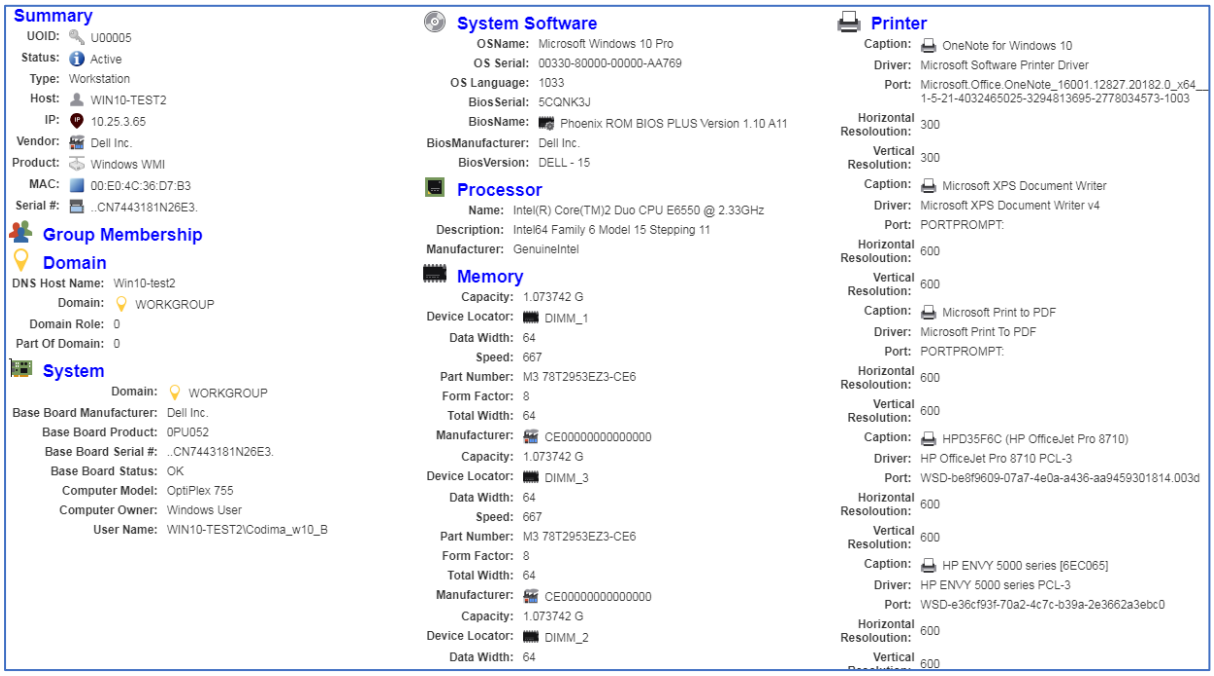
Device Basics

	UOID	STA	Status	Type	Device Type	Host
☐	U00002	▲	Active		Printer	HP6EC065.home
☐	U00003	▲	Active		Workstation	USER-PC

The report is controlled by a set of Tabs: *Per Device Discovery Overview, User Update, Interfaces, Hot Fixes, Drill Down Processes, Drill Down Services*.

See details on each Tab below.

Per Device Discovery Overview Tab



Summary
UOID: U00005
Status: Active
Type: Workstation
Host: WIN10-TEST2
IP: 10.25.3.65
Vendor: Dell Inc.
Product: Windows WMI
MAC: 00:E0:4C:36:D7:B3
Serial #: ..CN7443181N26E3.

Group Membership

Domain
DNS Host Name: Win10-test2
Domain: WORKGROUP
Domain Role: 0
Part Of Domain: 0

System
Domain: WORKGROUP
Base Board Manufacturer: Dell Inc.
Base Board Product: 0PU052
Base Board Serial #: ..CN7443181N26E3.
Base Board Status: OK
Computer Model: OptiPlex 755
Computer Owner: Windows User
User Name: WIN10-TEST2\Codima_w10_B

System Software
OSName: Microsoft Windows 10 Pro
OS Serial: 00330-80000-00000-AA769
OS Language: 1033
BiosSerial: 5CQNK3J
BiosName: Phoenix ROM BIOS PLUS Version 1.10 A11
BiosManufacturer: Dell Inc.
BiosVersion: DELL - 15

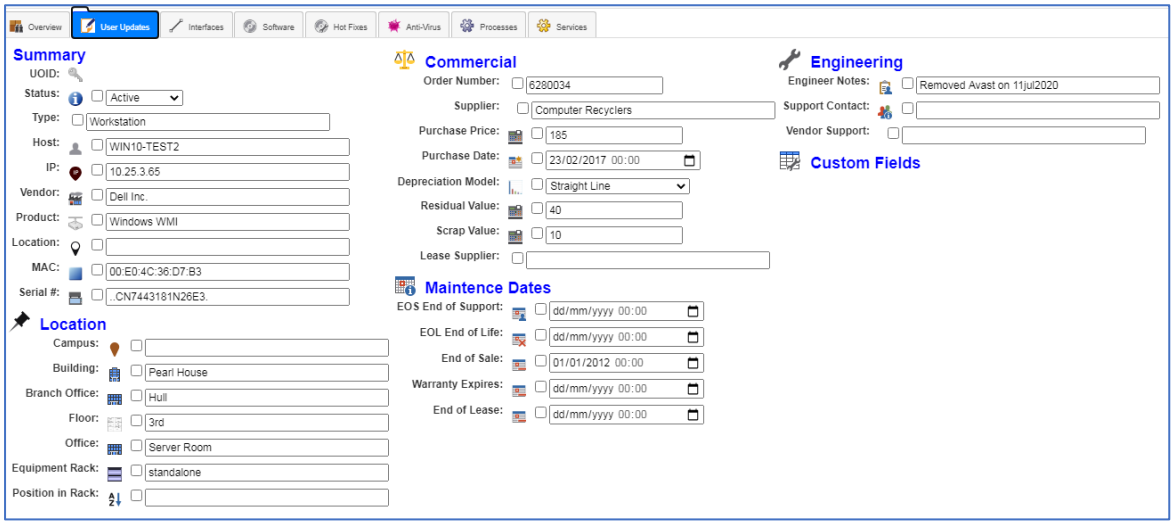
Processor
Name: Intel(R) Core(TM)2 Duo CPU E6550 @ 2.33GHz
Description: Intel64 Family 6 Model 15 Stepping 11
Manufacturer: GenuineIntel

Memory
Capacity: 1.073742 G
Device Locator: DIMM_1
Data Width: 64
Speed: 667
Part Number: M3 78T2953EZ3-CE6
Form Factor: 8
Total Width: 64
Manufacturer: CE00000000000000
Capacity: 1.073742 G
Device Locator: DIMM_3
Data Width: 64
Speed: 667
Part Number: M3 78T2953EZ3-CE6
Form Factor: 8
Total Width: 64
Manufacturer: CE00000000000000
Capacity: 1.073742 G
Device Locator: DIMM_2
Data Width: 64

Printer
Caption: OneNote for Windows 10
Driver: Microsoft Software Printer Driver
Port: Microsoft.Office.OneNote_16001.12827.20182.0_x64__1-5-21-4032465025-3294813695-2778034573-1003
Horizontal Resolution: 300
Vertical Resolution: 300
Caption: Microsoft XPS Document Writer
Driver: Microsoft XPS Document Writer v4
Port: PORTPROMPT:
Horizontal Resolution: 600
Vertical Resolution: 600
Caption: Microsoft Print to PDF
Driver: Microsoft Print To PDF
Port: PORTPROMPT:
Horizontal Resolution: 600
Vertical Resolution: 600
Caption: HPD35F6C (HP OfficeJet Pro 8710)
Driver: HP OfficeJet Pro 8710 PCL-3
Port: WSD-be8f9609-07a7-4e0a-a436-aa9459301814.003d
Horizontal Resolution: 600
Vertical Resolution: 600
Caption: HP ENVY 5000 series [6EC065]
Driver: HP ENVY 5000 series PCL-3
Port: WSD-e36cf93f-70a2-4c7c-b39a-2e3662a3ebc0
Horizontal Resolution: 600
Vertical 600

This report provides a detailed analysis of the selected device found during the Discovery process. A device that supports WMI provides a more extensive report.

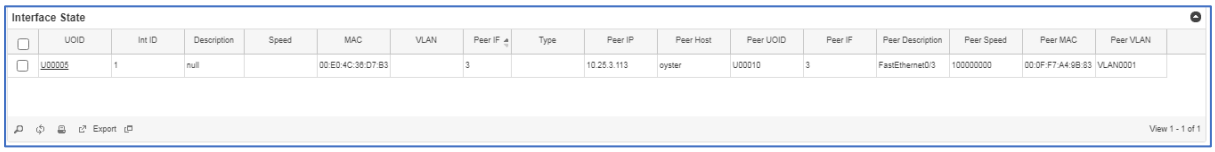
User Updates Tab Analysis



This tab shows User Updates that have been added using the Update features.

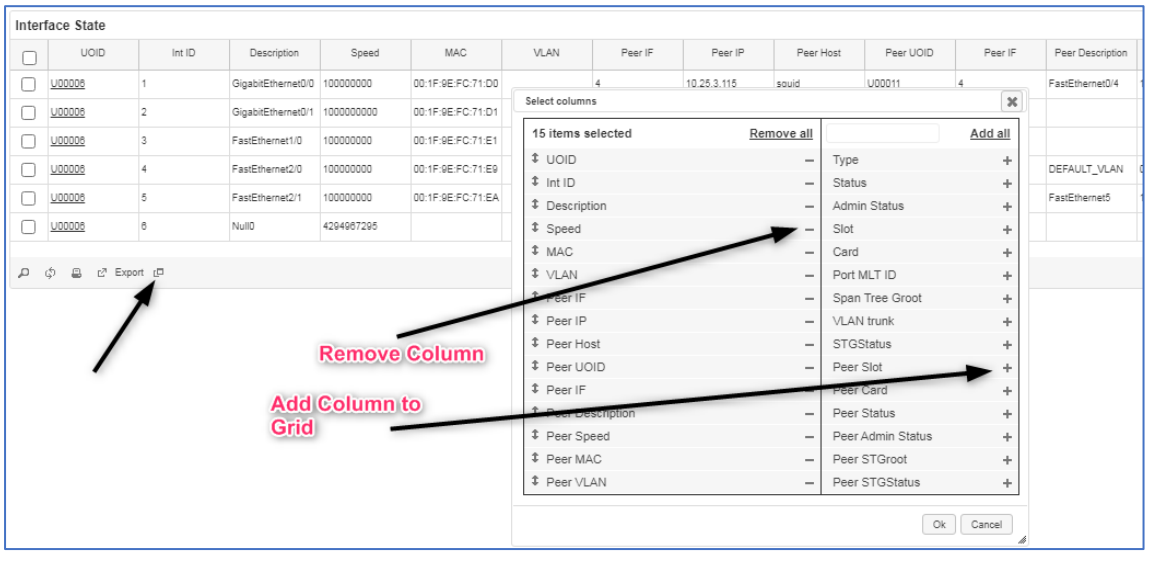
Details can also be amended from this screen by ticking the fields tick box(s), then clicking on the **Save Ticked Details** button for one or more updates to this device's database record.

Interfaces Tab

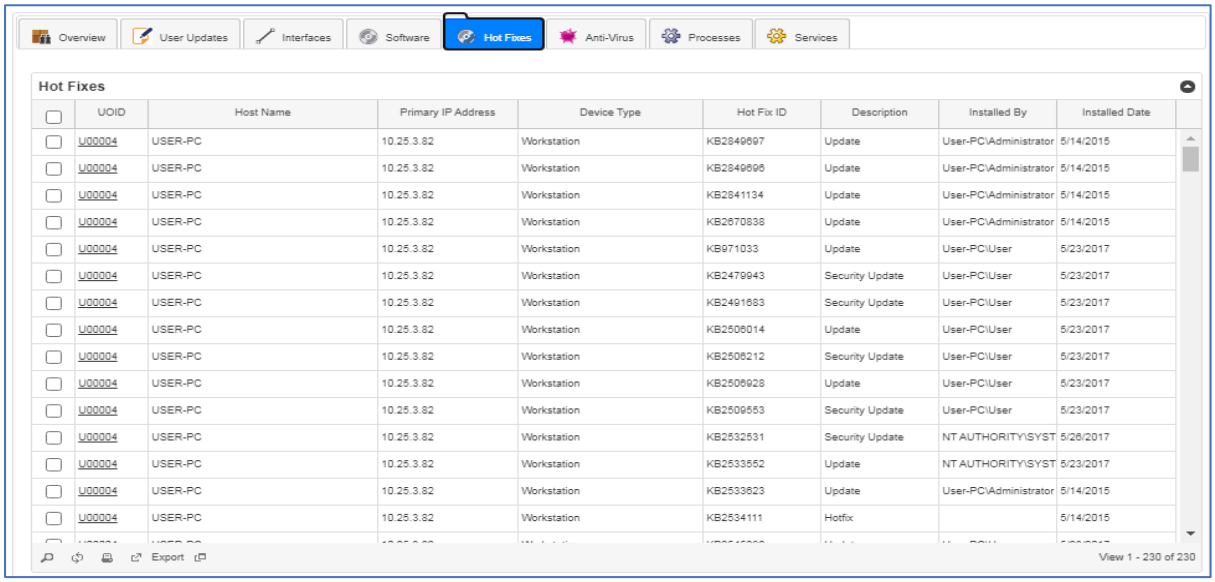


This tab gives details of the Interfaces present on the drill down device. Both ends of the link are shown in the grid including, IP, MAC, speed, device details. The Grid can be Filtered and Sorted as with other Grids, the columns and the grid itself are fully dynamic, and can be dragged bigger or smaller.

There are a large number of possible fields available for this grid, these can be added or removed by clicking on the column picker icon as below.

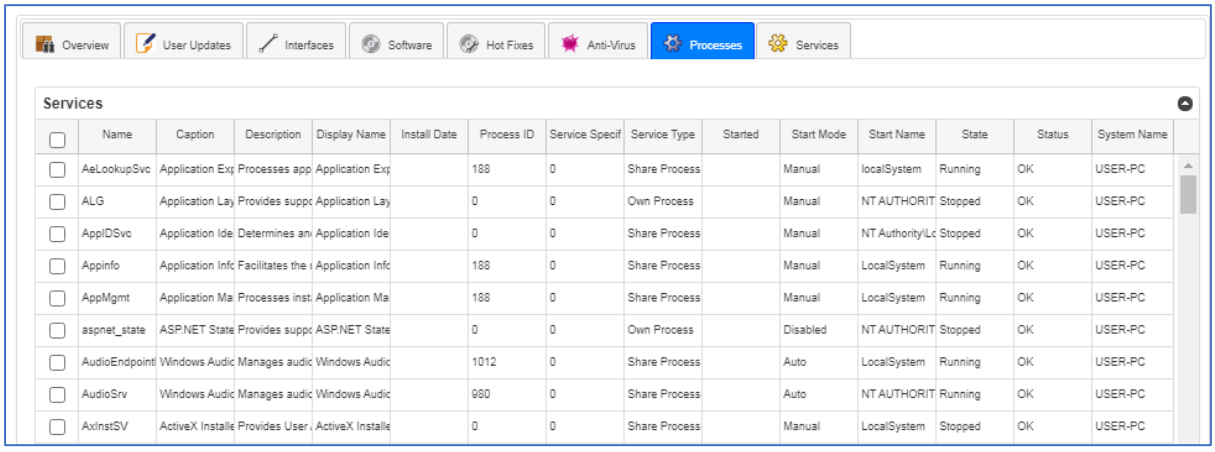


Hot Fixes Tab



This provides an analysis of Hot Fix/ Security Patches installed on the selected device - at Discovery time.

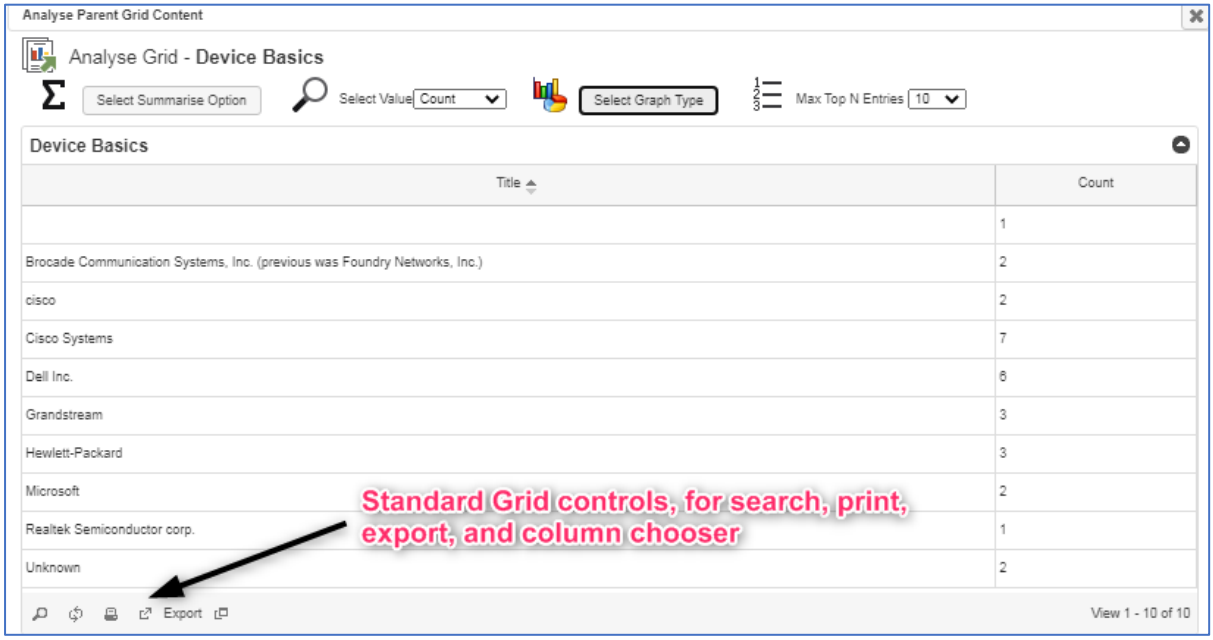
Drill Down Processes Tab



This is a list of Processes that were running on the device at Discovery Time (note. Toolbox Monitoring does this in real time).

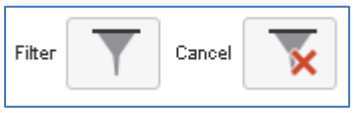
Drill Down Services Tab

Tabular Analyses using Grids can also be created to show results in columns with multiple values for some Fields like Sales Values. Grids also allow numeric CSV (Excel) output plus all Grid Export formats. The Grids allow Sort, Search and Column Entries selection. The grids can also be resized per column and the whole grid in the dynamic Toolbox GUI. See below:

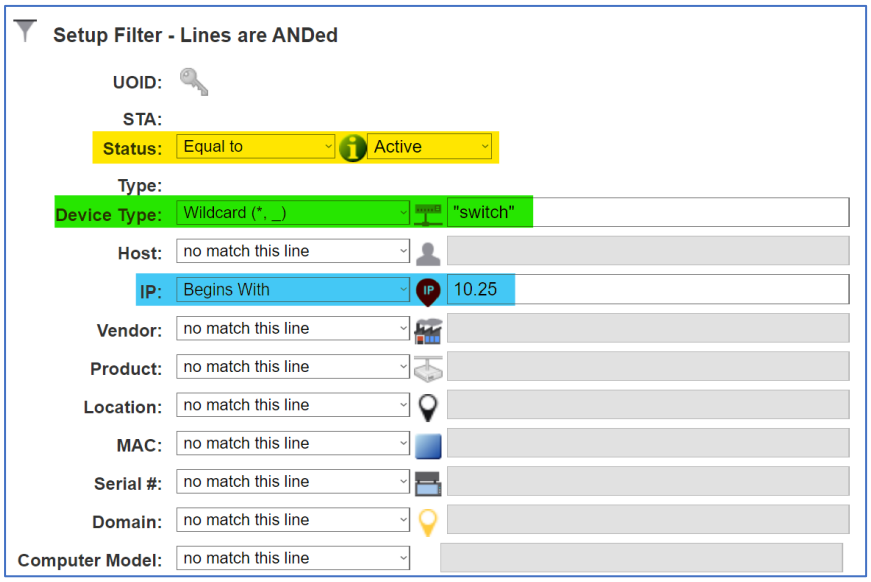


Filters

A comprehensive Filter can be selected by clicking on the **Filter** Icon. An active Filter can be cancelled by clicking on the **Cancel** Filter Icon.



A typical Filter is shown below:



The Matching operators include true Wild Card matching such **'*cisco*3805*PWR*'** for flexible multi-term-matches in a simple format.

REGEX is supported for flexible matches for example 'router|switch|phone' to match a **router** OR **switch** OR **phone'.** Much more complex matches can also be made.

ENTERPRISE VIEW Feature

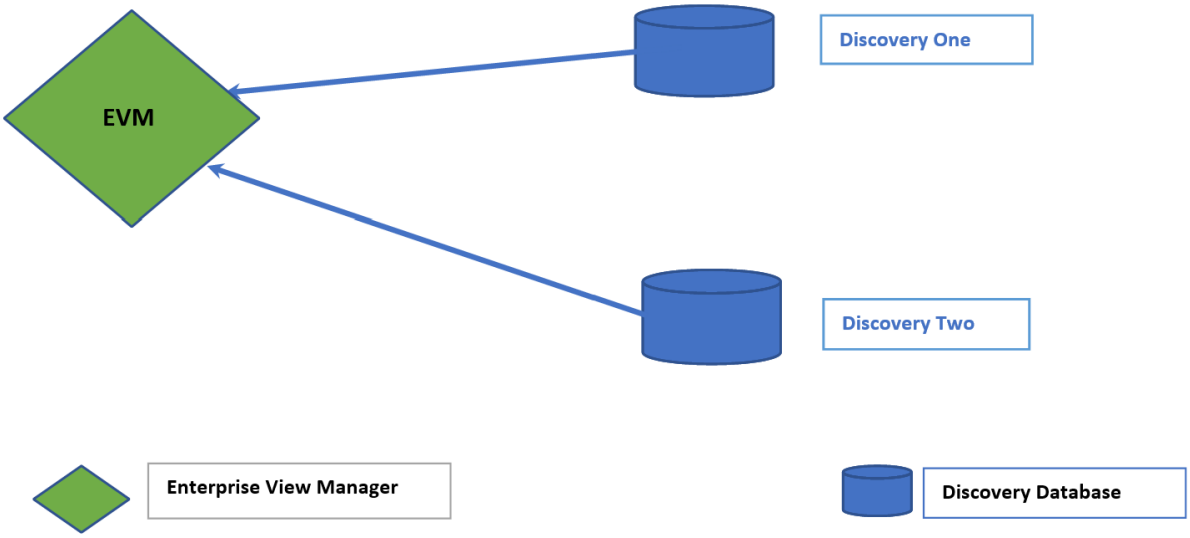
Introduction

In essence Enterprise View is an extension of the Inventory feature, it is Codima Toolbox's way of managing probes that are used to extend the geographic reach of this network management tool. Enterprise view offers the ability to combine several discoveries in one manageable view, these discoveries can either be viewed individually or as a summation. This allows you to either see location specific information such as a probe located in the UK or view how large your collection of inventory assets is on a worldwide scale.

Enterprise View has the same functionality that the original Inventory feature has, except any number of probes can be accessed from one GUI all running in parallel to ensure quick response times.

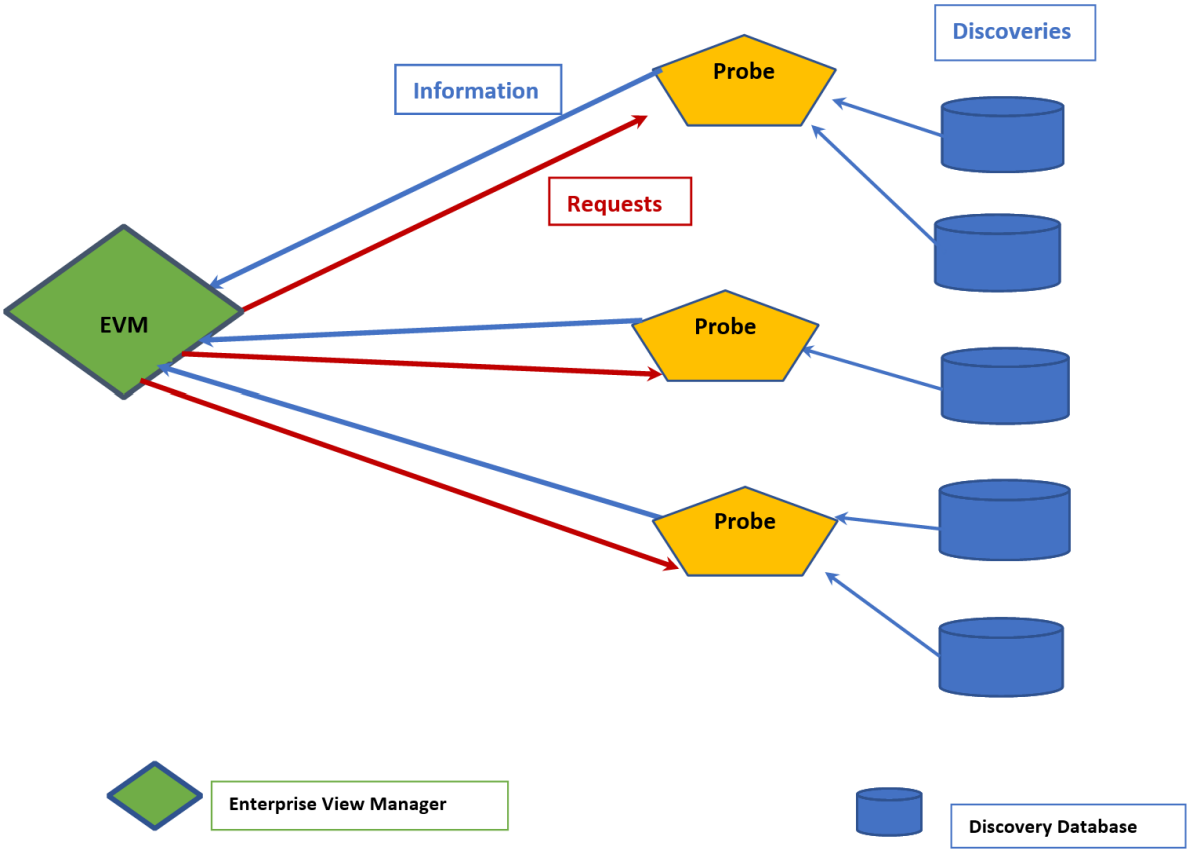
Deployment Scenarios

1. Combining Discoveries on a Single Installation



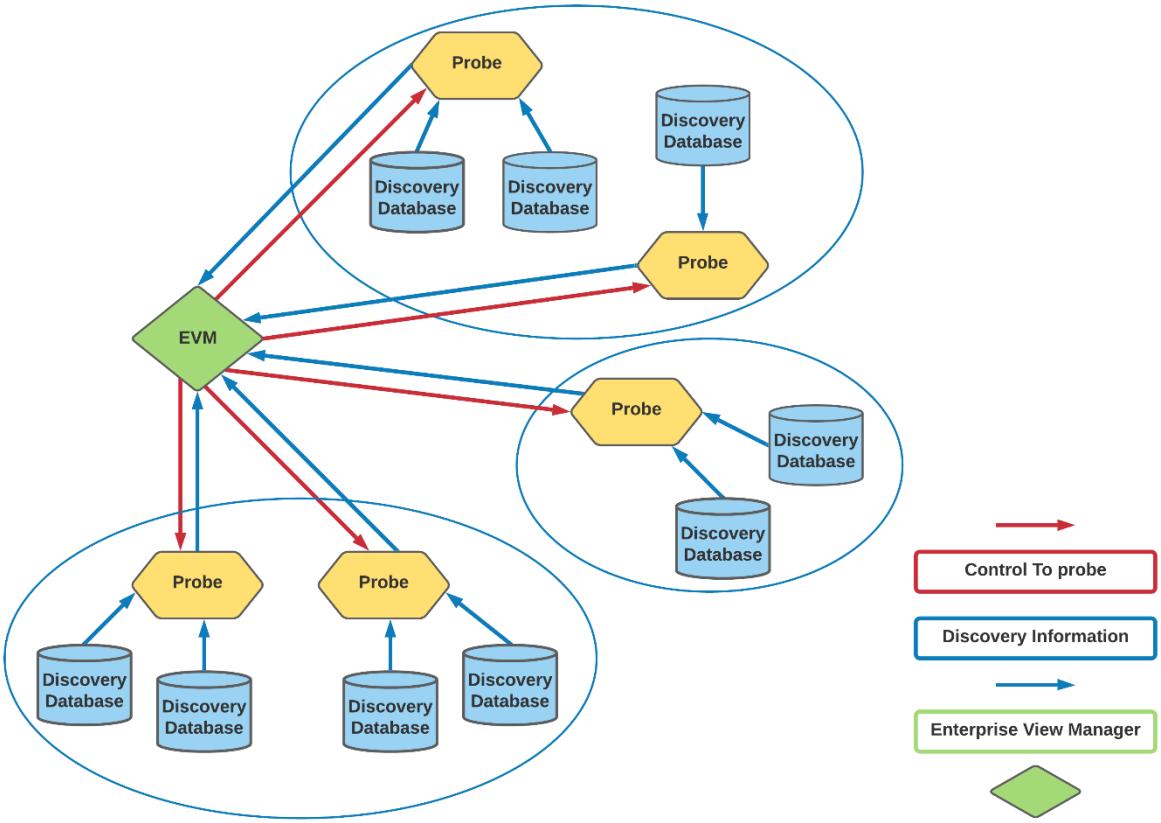
This is a scenario where a single Enterprise View Manager splits up one or more Networks into multiple Discoveries (Databases), possibly to reduce per Discovery time or to limit Database sizes. Alternatively, separate Discoveries are required because the Discoveries use individual IP Ranges, which could be overlapping in which case separate Discoveries are a necessity.

2. Using Multiple Probes



There are several advantages to using multiple probes. Full parallel processing both during the Network Discovery Process plus equally importantly, the ability to Process Inventory Display Requests, such as a simple or very sophisticated Inventory Explorer Filter to be executed on all Discoveries in the View. There can be any number of Views, with combined or separate reports.

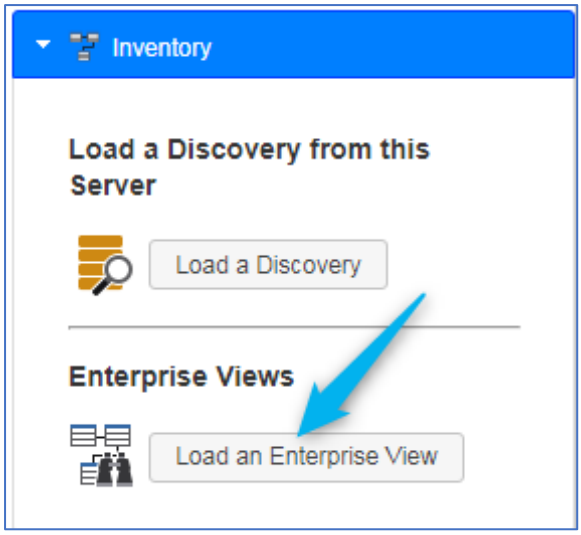
3. Geographically Distributed Probes and Discoveries



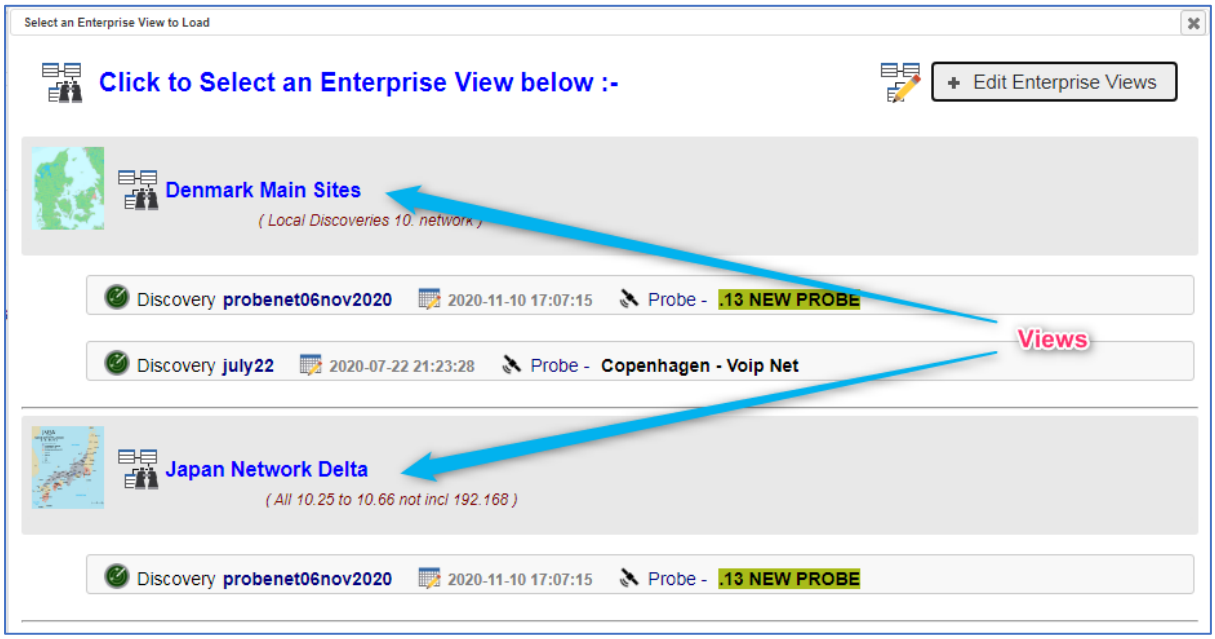
Above is a typical Geographically distributed system. The *blue circles* represent Views that have been set up in the Enterprise View Manager. The views can focus on a Region, Building or Campus. There can be a highly localised View say of one Building for one User, and perhaps another View for all the Discoveries.

Basic GUI Operation

The original Inventory view is retained as can be seen in the picture below by clicking on the **Load a Discovery** button, this option only allows you to see individual local discoveries.



The button **Load an Enterprise View** gives you access to the Enterprise View. Clicking on this button opens the Select Enterprise View user interface as below (If no views are present read the **Add New Views** section to create them):

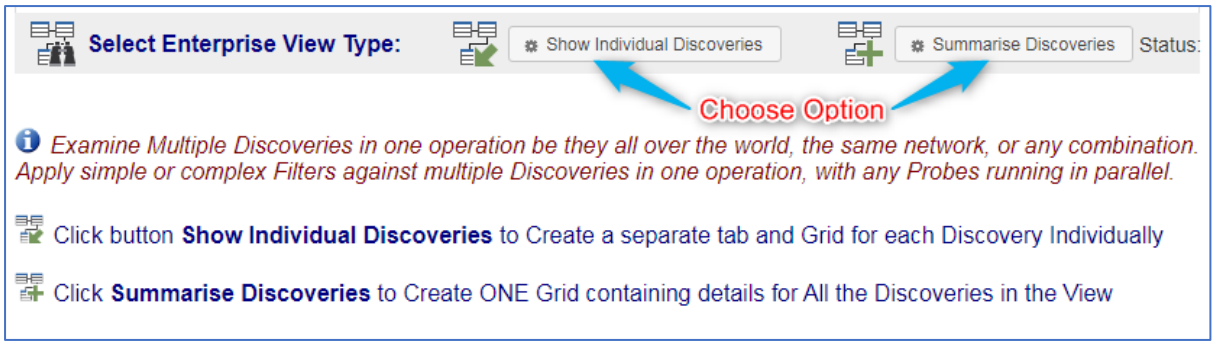


Two Enterprise Views are defined above, 'Denmark Main Sites' and 'Japan Network Delta' with a geographical Map of the two regions. Following the Enterprise View entry are individual Discovery entries. The Discoveries can be on any Remote Probe and/or the local Enterprise View Manager. There is no limit to the number of Views and no limit to the number of Discoveries per View. The Views and Discoveries can be used in any combination.

The selected View controls the user interface Inventory content by displaying the Discoveries attached to each View. This means the Probes can work in parallel to deliver multiprobe and multi-Discovery content fully automatically.

Simply click on the desired View, to start examining the Discovered Inventories of the selected View.

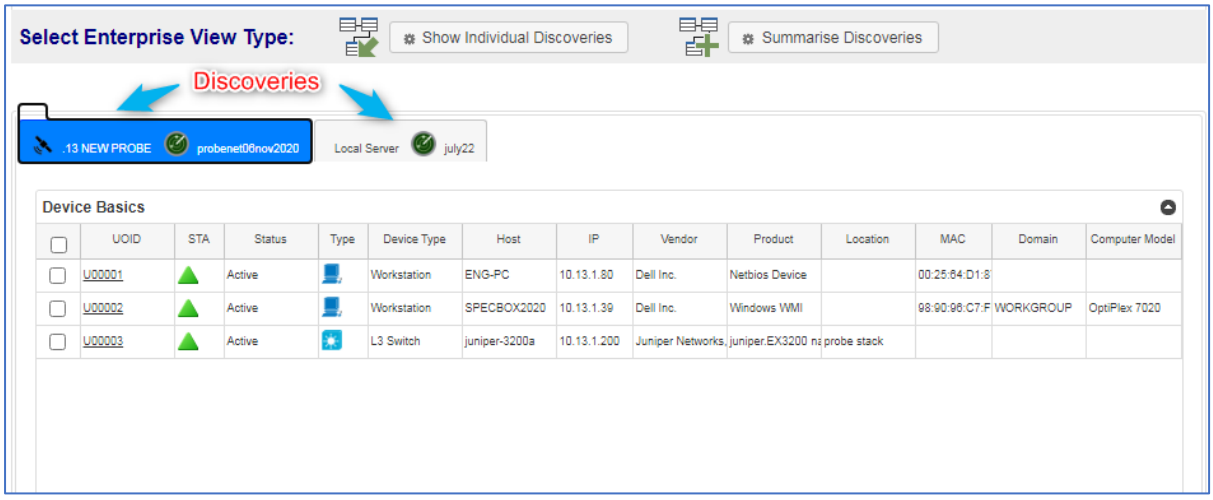
Below is the initial screen after clicking on a View.



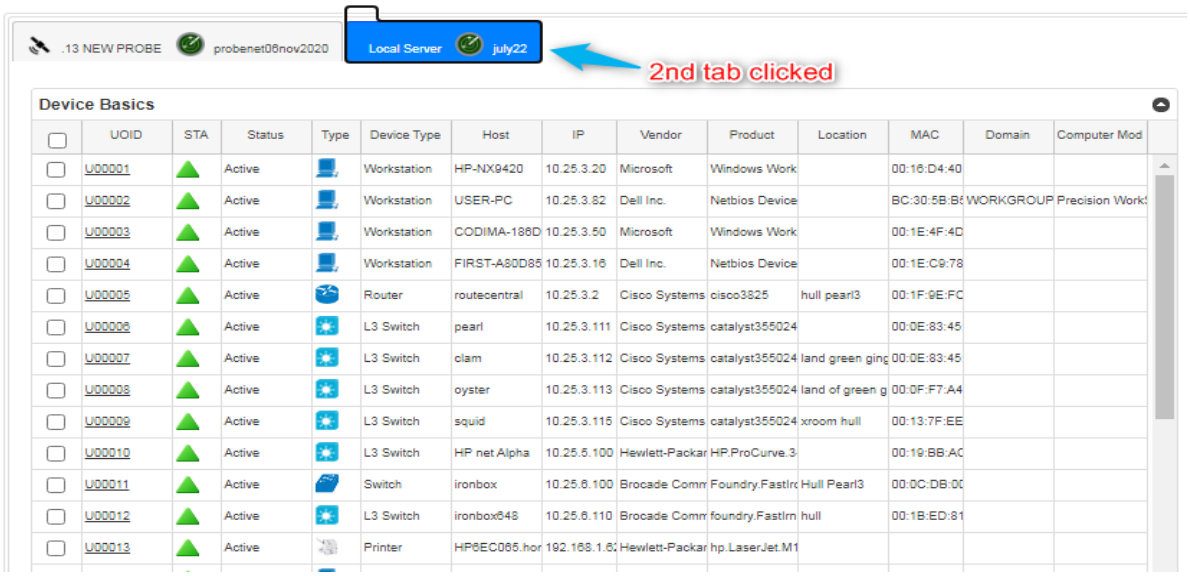
As per instructions, simply click one of the two buttons to kick off the Analysis type, at any time, swap between the modes to suit your needs. Continue reading to learn more about these modes.

Individual Discoveries Mode

Clicking on the **Show Individual Discoveries** button, kicks off loading a Grid/Tab per Discovery in the selected View as below. The first tab is a Discovery on a remote Probe, as indicated by the Probe icon.



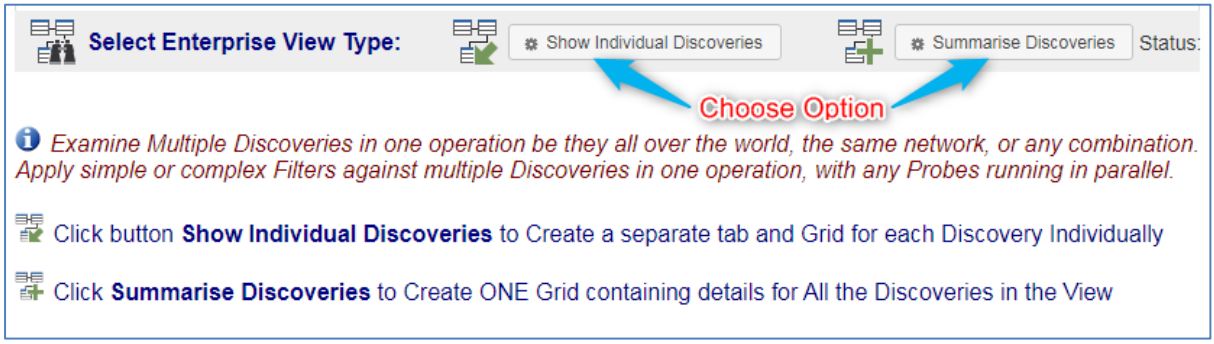
By clicking on the second tab a Discovery from a local Probe is shown, as indicated by the text “Local Server”.



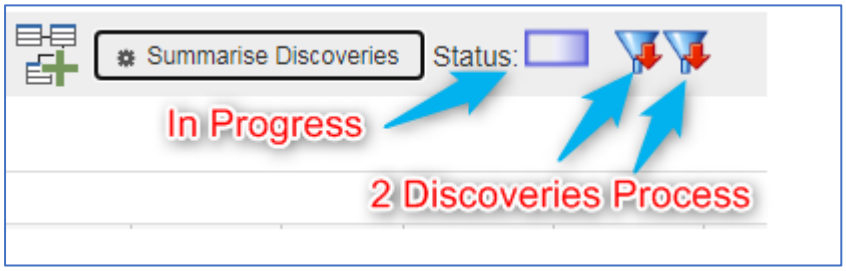
The user created View defines what Discoveries are shown in this feature, there is no upper limit to the number of Views or the number of Discoveries in a View. Discoveries on Probes are processed in parallel by the Probe, making the system totally scalable. Full Analytics are available per individual Tab, which is one Discovery.

Discoveries Summary Mode

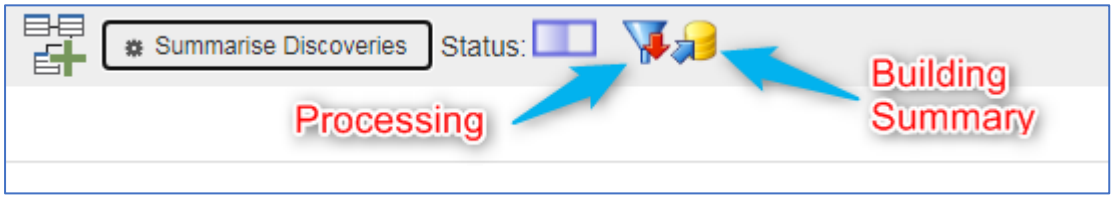
Clicking on the **Summarise Discoveries** button, kicks off creating a combined analysis of all the Discoveries in the View.



Since this is a complex process involving Discoveries from Distributed Probes and Local Systems, status indicators show progress per Discovery.



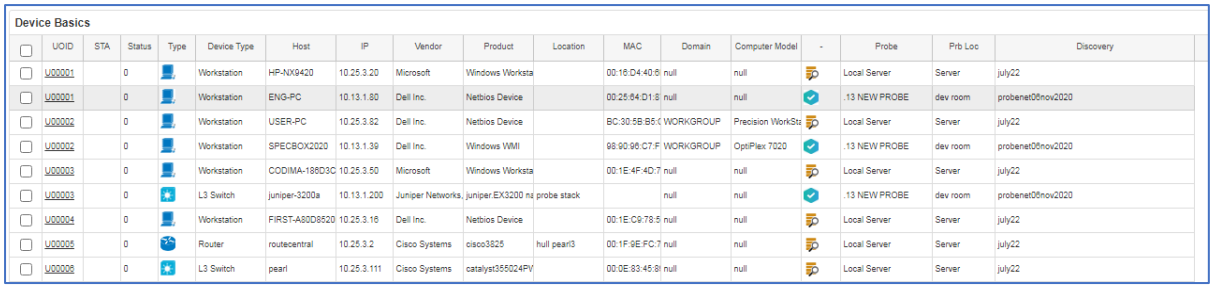
Above two Discoveries are Processing extracting the requested details and apply potentially complex filters.



Above the 2nd Discovery is now building the Combined Database of all the Discoveries. The first Discovery is still processing.

The job is done successfully, both discoveries are processed and combined.

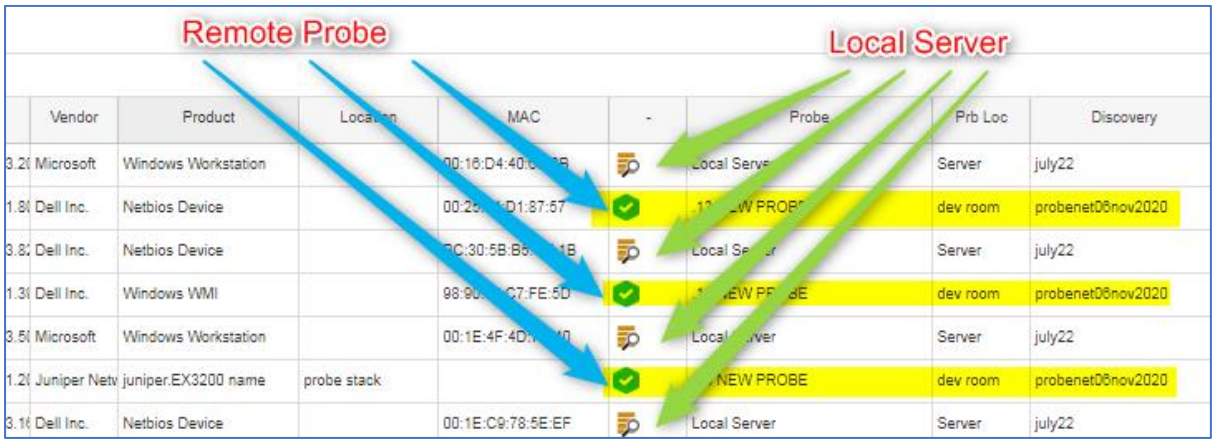
There is now a single Grid which shows the results of the two discoveries in this example.



Device Basics

	UOID	STA	Status	Type	Device Type	Host	IP	Vendor	Product	Location	MAC	Domain	Computer Model	-	Probe	Prb Loc	Discovery
	U00001		0		Workstation	HP-NX9420	10.25.3.20	Microsoft	Windows Worksta		00:16:D4:40:6	null	null		Local Server	Server	july22
	U00001		0		Workstation	ENG-PC	10.13.1.80	Dell Inc.	Netbios Device		00:25:64:D1:8	null	null		.13 NEW PROBE	dev room	probenet06nov2020
	U00002		0		Workstation	USER-PC	10.25.3.82	Dell Inc.	Netbios Device		BC:30:5B:B5:(	WORKGROUP	Precision WorkSt		Local Server	Server	july22
	U00002		0		Workstation	SPECBOX2020	10.13.1.39	Dell Inc.	Windows WMI		98:90:96:C7:F	WORKGROUP	OptiPlex 7020		.13 NEW PROBE	dev room	probenet06nov2020
	U00003		0		Workstation	CODIMA-186D3C	10.25.3.50	Microsoft	Windows Worksta		00:1E:4F:4D:7	null	null		Local Server	Server	july22
	U00003		0		L3 Switch	juniper-3200a	10.13.1.200	Juniper Networks,	juniper.EX3200 na	probe stack		null	null		.13 NEW PROBE	dev room	probenet06nov2020
	U00004		0		Workstation	FIRST-A80D8520	10.25.3.16	Dell Inc.	Netbios Device		00:1E:C9:78:5	null	null		Local Server	Server	july22
	U00005		0		Router	routecentral	10.25.3.2	Cisco Systems	cisco3825	hull pearl3	00:1F:9E:FC:7	null	null		Local Server	Server	july22
	U00006		0		L3 Switch	pearl	10.25.3.111	Cisco Systems	catalyst355024PV		00:0E:83:45:8	null	null		Local Server	Server	july22

The combined results of the two discoveries are now in one grid. Below there is a zoom in to the Discoveries and Probe columns.

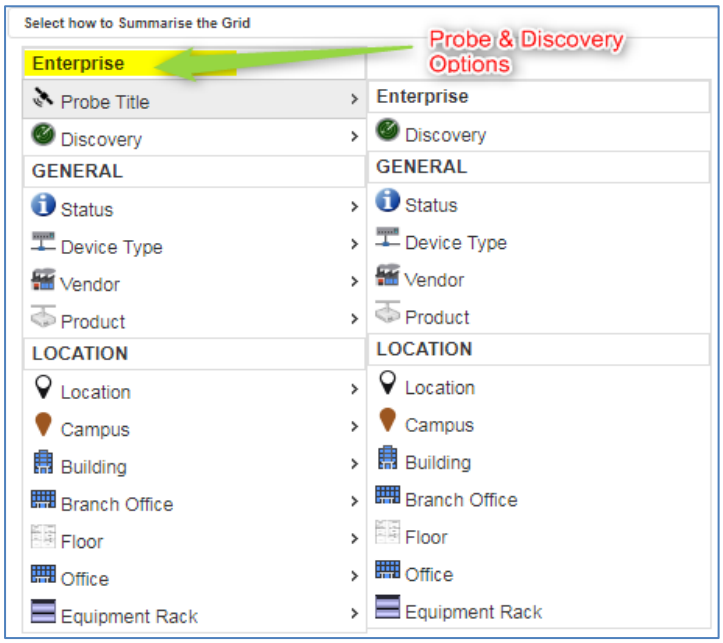


	Vendor	Product	Location	MAC	-	Probe	Prb Loc	Discovery
3.2(	Microsoft	Windows Workstation		00:16:D4:40:6		Local Serve	Server	july22
1.8(	Dell Inc.	Netbios Device		00:25:64:D1:87:67		.13 NEW PROBE	dev room	probenet06nov2020
3.8(	Dell Inc.	Netbios Device		BC:30:5B:B5:(		Local Server	Server	july22
1.3(	Dell Inc.	Windows WMI		98:90:96:C7:FE:5D		.13 NEW PROBE	dev room	probenet06nov2020
3.5(	Microsoft	Windows Workstation		00:1E:4F:4D:7		Local Server	Server	july22
1.2(	Juniper Netv	juniper.EX3200 name	probe stack			.13 NEW PROBE	dev room	probenet06nov2020
3.1(	Dell Inc.	Netbios Device		00:1E:C9:78:5E:EF		Local Server	Server	july22

This combined Discoveries grid can now be Sorted, Searched and Exported as normal, showing results from any number of Discoveries, anywhere in the world in one report.

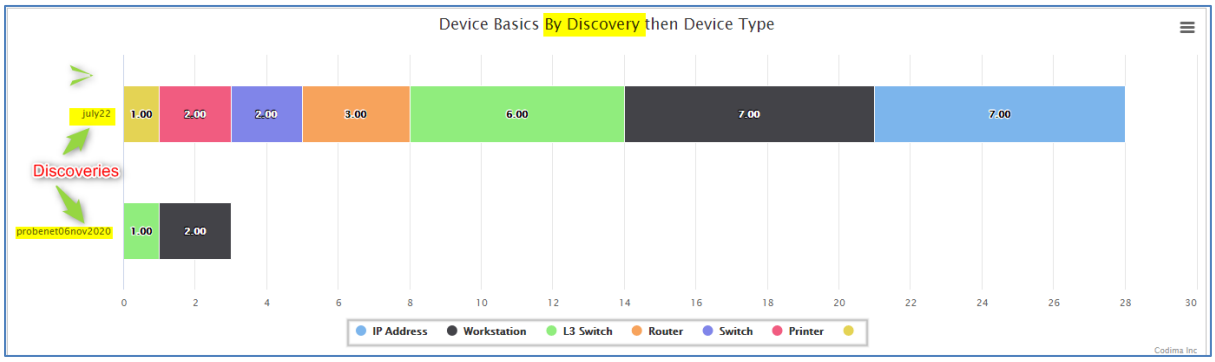
Analytics

For the Summary Mode where discoveries are combined, then new Graphing Options are available.

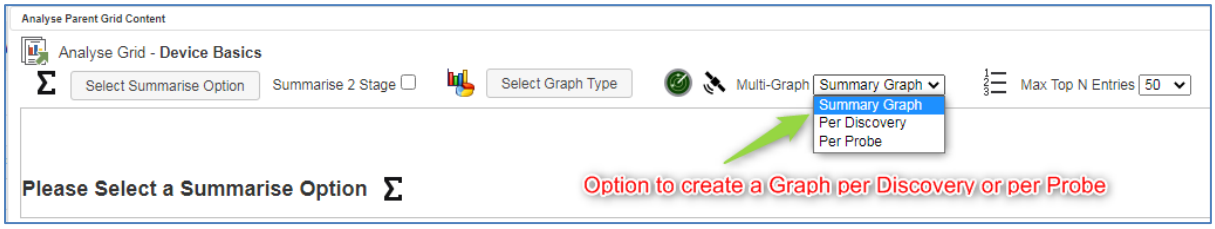


New options are available to compare Discoveries and Probe-Discoveries in one Graph or multiple Graphs.

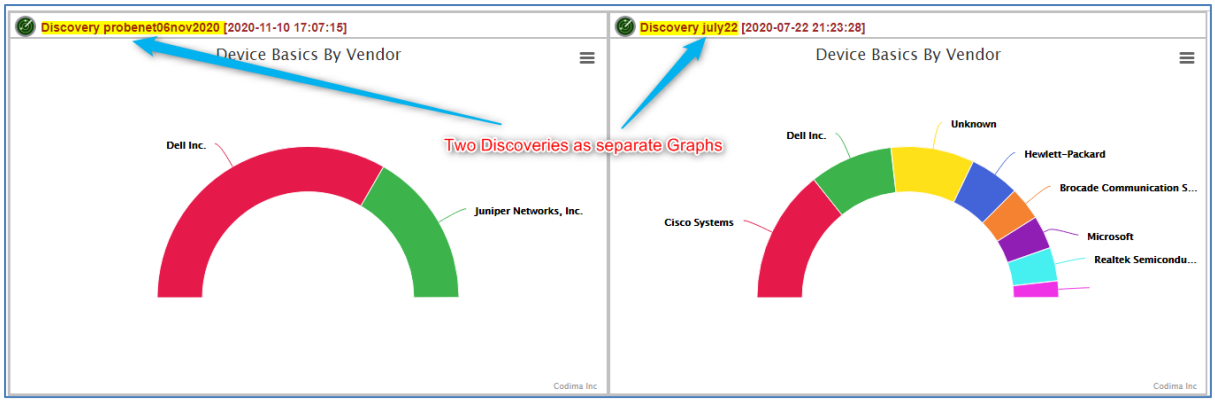
Below is a single graph showing two Discoveries with counts of Devices Types in each Discovery.

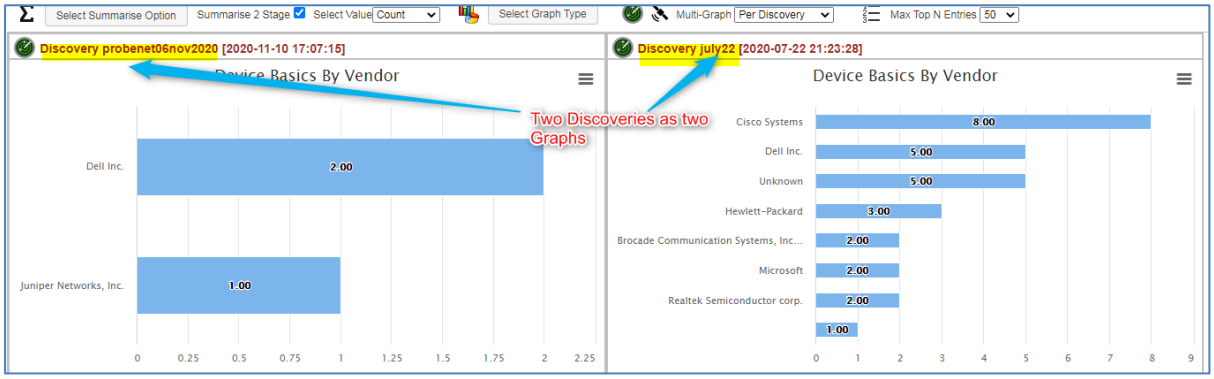


There is an option to create a graph per Discovery, per Probe, or combined in one Summary:

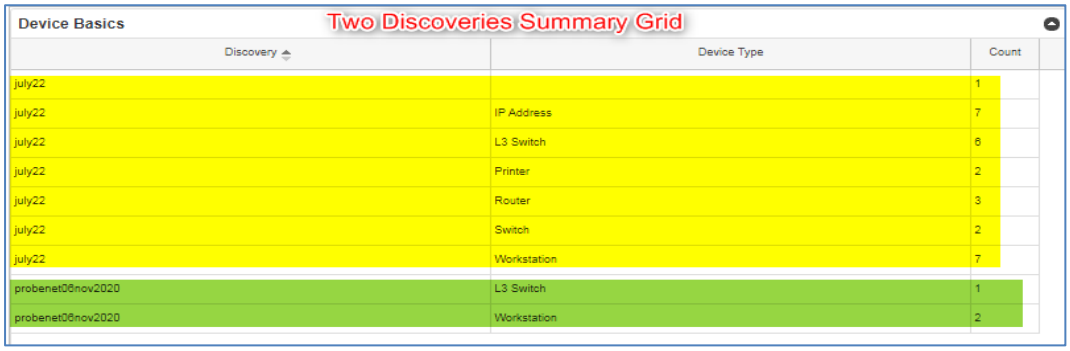


A multiple Graph option is selected to produce these graphs.





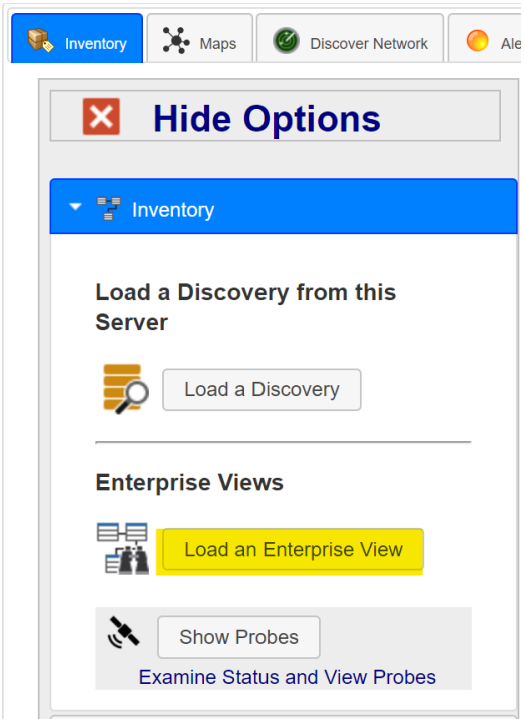
Grid Format can be selected to produce Grids of Multiple Probes and Discoveries (with CSV Export of course). The grid section in yellow is from one Discovery and in green for the other Discovery.



Discovery	Device Type	Count
july22		1
july22	IP Address	7
july22	L3 Switch	6
july22	Printer	2
july22	Router	3
july22	Switch	2
july22	Workstation	7
probenet06nov2020	L3 Switch	1
probenet06nov2020	Workstation	2

Adding New Views

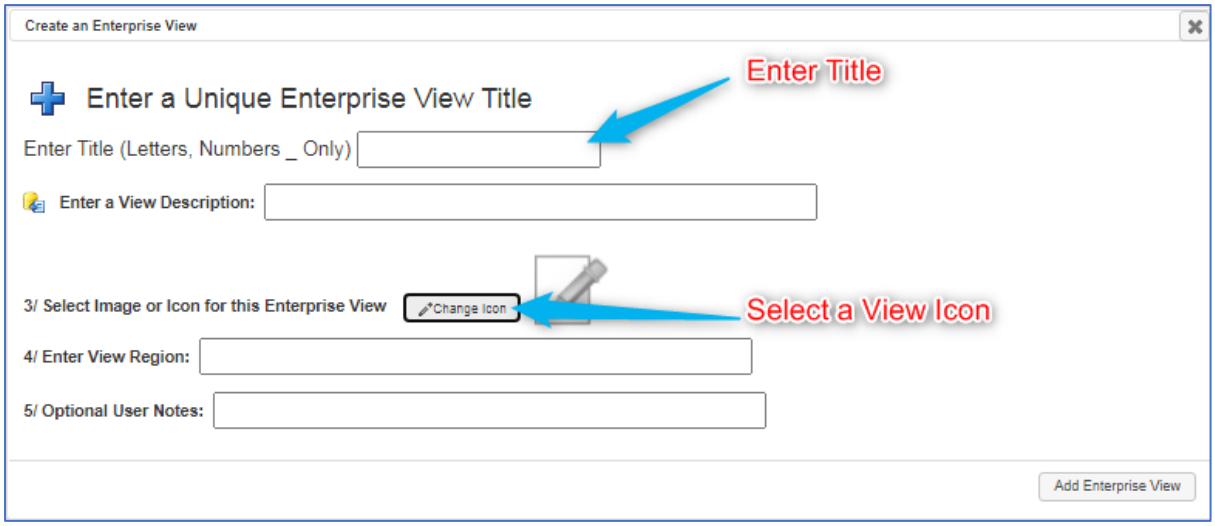
Navigate to the main **Inventory** tab, then click **Load an Enterprise View** in the sidebar.



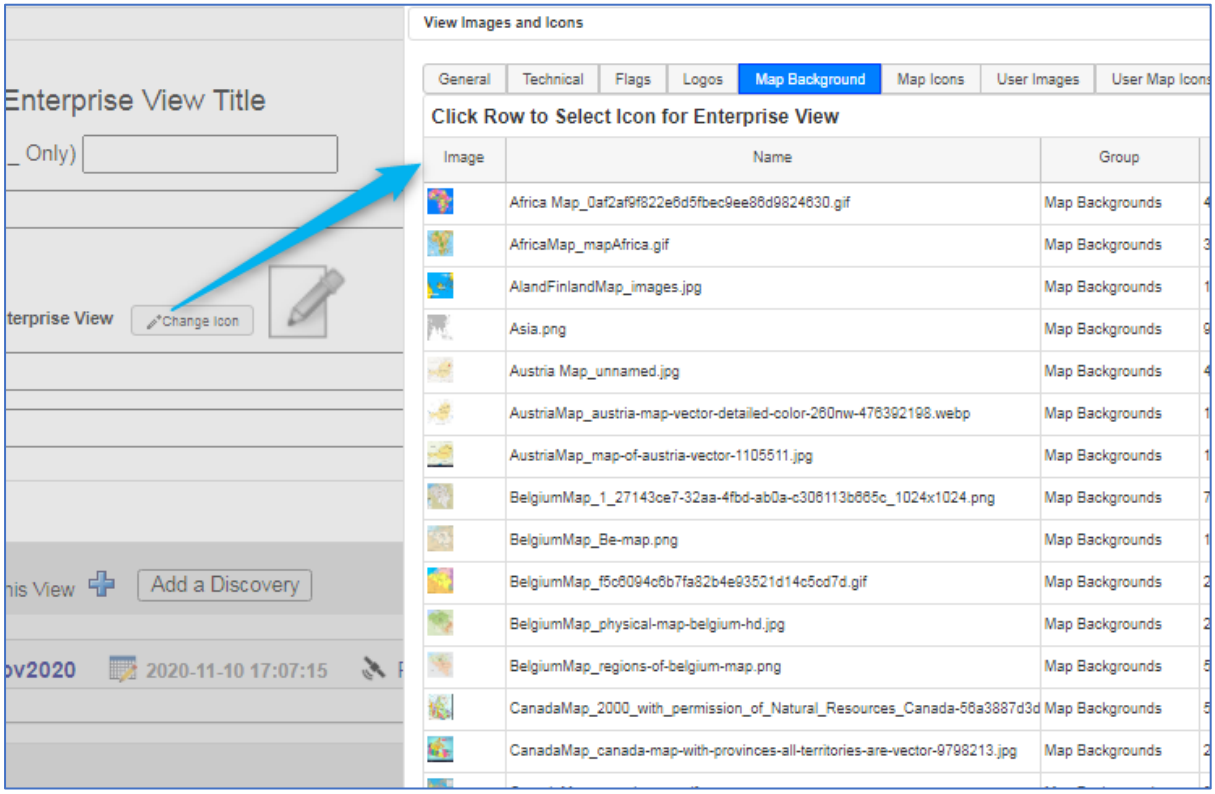
To add a new View, click the **Edit Enterprise Views** button:

Now a new View can be added by clicking **Add a New Enterprise View**:

After clicking **Add a New Enterprise View** a dialog appears to enter the View details.



It is mandatory to **enter a unique Enterprise View Title**, and highly recommended to add other details especially an Image for the view as below:



There is a list of maps supplied by Codima, but the user can use their own map images too.

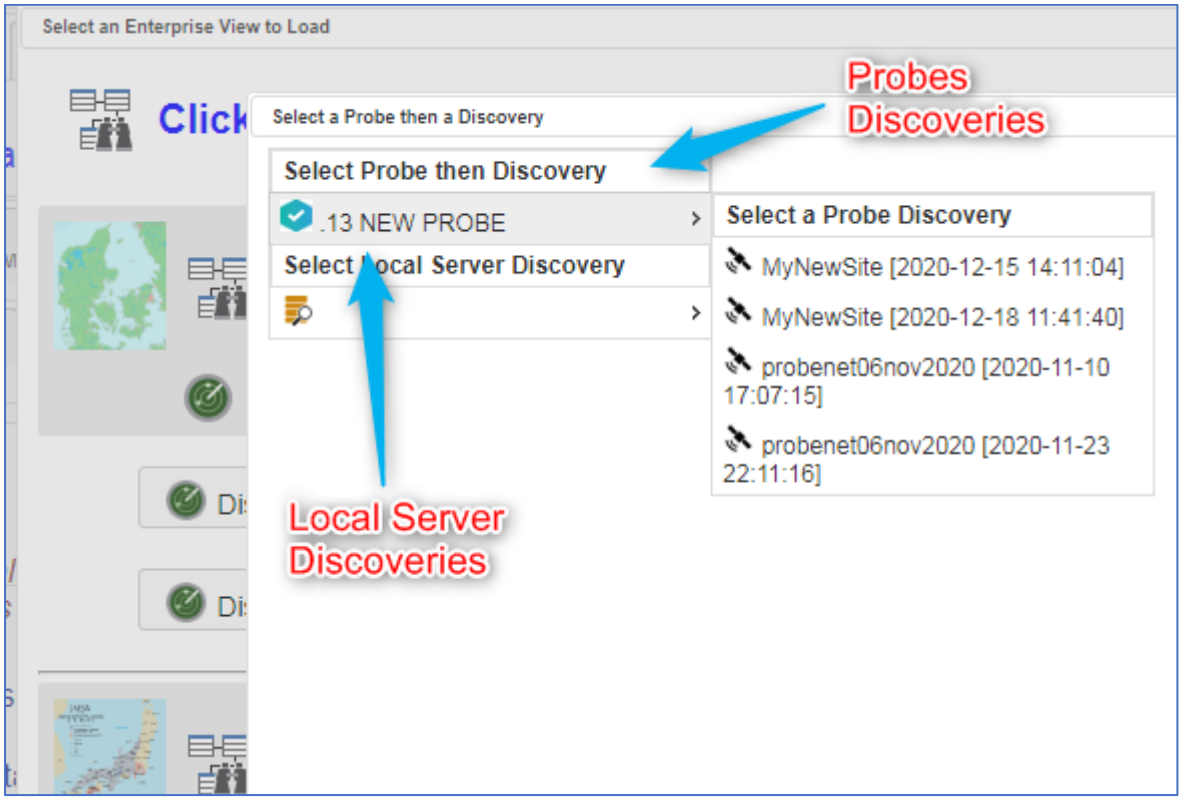
The next job is to enter Discoveries to each View.

A single view is shown below: -

This Enterprise View has two Discoveries attached which are from two different Probes. Discoveries can be all on the local Manager, all on Probes, or any combination of the two.

For example, a view could be used to combine two or more Discoveries on the local Manager, or two or more Discoveries on a Remote Probe, or any combination thereof. This is useful to combine multiple Discoveries from different Subnets on the same network.

Any number of Discoveries can be added to a View by clicking on the Add a Discovery button to launch the GUI below:

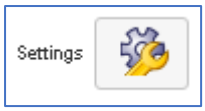


Discoveries can be added from the Local Server Menu list or the Remote Probe Discoveries list – automatically set up by the Manager when it talks to Probes.

Note: Discoveries are retrieved from Connected Remote Probes when the Browser is Refreshed, they are stored and can then be accessed even when a Probe is no longer connected.

Settings

This is accessed by clicking on the icon as below:



Maximum Grid Rows

Currently the settings allow the creation of User Customisable fields in the database and also control the maximum rows in the main report grid.

The maximum number of rows in the Main Grid can be set. Note, a very high value will slow the time it takes for the system to populate the grid. The maximum rows selection also sets the maximum number of rows that can be Exported or Printed from the Grid.

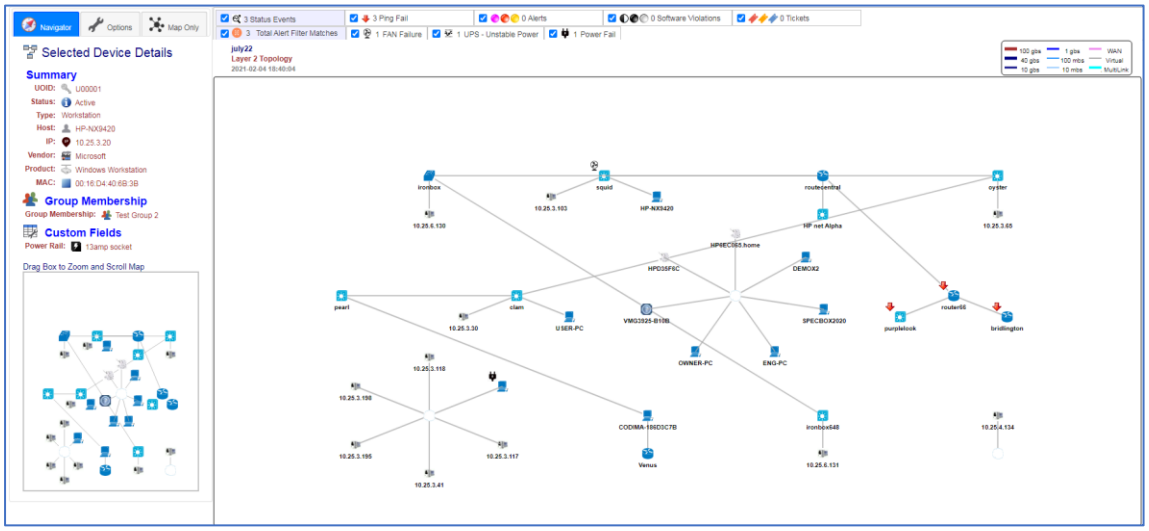
WEB MAPS Feature

The Maps feature is only available with the following licenses:
- Free License
- Network Inventory with Maps in Web and Visio Toolbox
- Network Inventory with Maps in Web and Visio and Monitoring + Alert Ticketing Toolbox

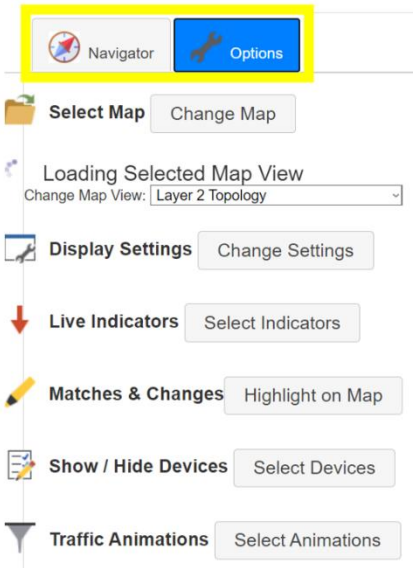
Toolbox Web Map

A straightforward Interface that allows all functions from one GUI, this allows direct mixing of all edit, display, and animation features. **Maps are created automatically by doing a Network Discovery.**

Shown below is a Map with the Navigator tab selected.

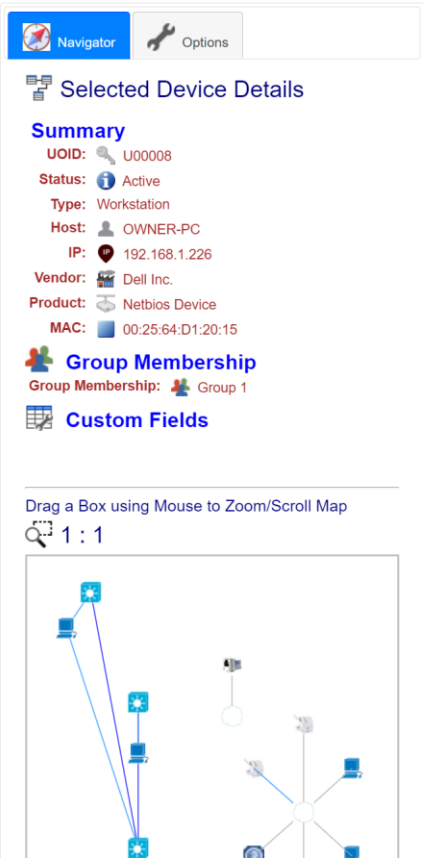


Note that there are two tabs, **Navigator** and **Options**, shown when viewing a web map using the Maps Tab.



Above the Map **Options** tab has been selected and is showing the Options panel, which allows maps to be selected using the **Change Map** button. A range of facilities to control how the Map is displayed can also be selected here.

The **Navigator** Tab shows two things – Firstly details on a user selected device on the Map, A device is selected by holding **Shift** and double clicking a device on the map. Secondly a Mini-Map to scroll and zoom the main map, to do this click and drag a box on the Mini-Map.

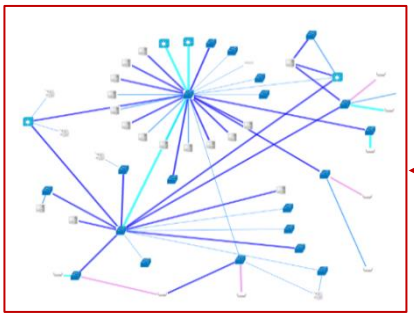


Map Creation

Maps are created automatically by doing a Network Discovery. Maps are produced in both a **Topology** format, and a **Tree** format as shown below. These maps are restricted to showing Layer 3 devices. Layer 2 Maps typically show many more devices. The **Mapping** feature is integrated with, and boosted by Live Animation, Distributed Live Maps and Drill Downs to Monitoring and Netflow.

With these maps you are able to view Live or Historic Replay of monitored traffic patterns and events. Device loading like CPU, Interface Loading and Errors, Alerts of All Kinds and can be all Animated at the same time.

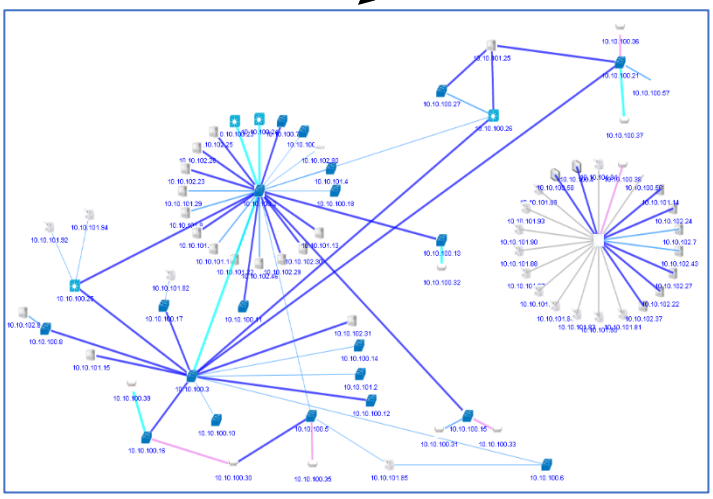
A Microsoft Visio Map can also be created if that suits your needs better than the Web Maps.



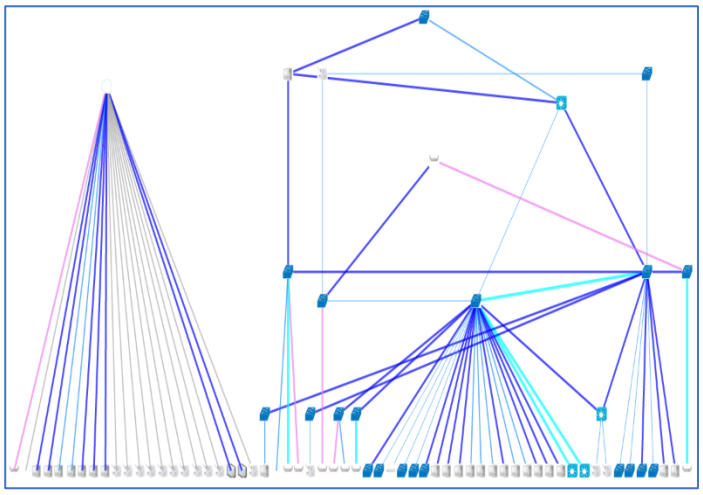
Network to Discover

Discovery Engine Analyses the Target Network and Creates Several Map Formats

Optional Visio Map depending on the Toolbox Licence



Topology Format Layer 3 Map

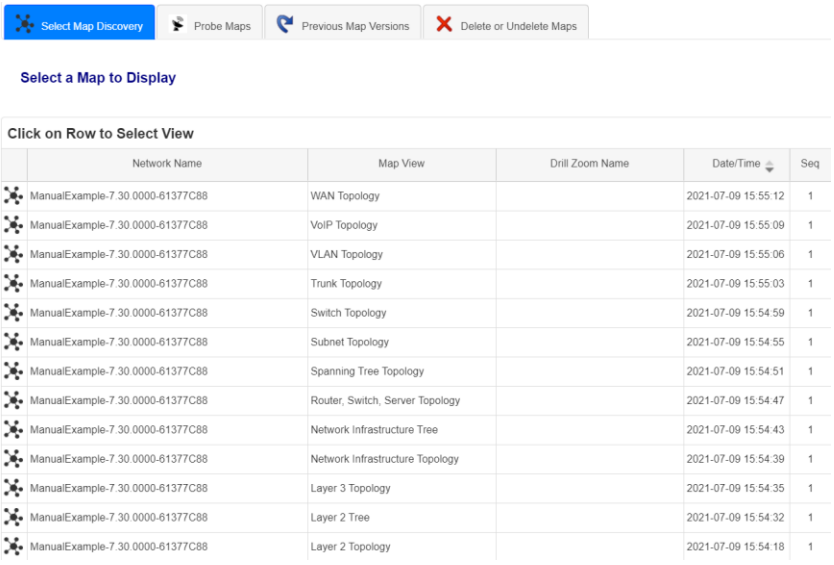


Tree Format Layer 3 Map

Managing Web Maps

Selecting a Map to View

After Network Discovery click on the Maps Tab and a Pop-Up will be automatically launched. A list of map views will be visible, these have all been created automatically in conjunction with the discovery.



Network Name	Map View	Drill Zoom Name	Date/Time	Seq
ManualExample-7.30.0000-61377C88	WAN Topology		2021-07-09 15:55:12	1
ManualExample-7.30.0000-61377C88	VoIP Topology		2021-07-09 15:55:09	1
ManualExample-7.30.0000-61377C88	VLAN Topology		2021-07-09 15:55:06	1
ManualExample-7.30.0000-61377C88	Trunk Topology		2021-07-09 15:55:03	1
ManualExample-7.30.0000-61377C88	Switch Topology		2021-07-09 15:54:59	1
ManualExample-7.30.0000-61377C88	Subnet Topology		2021-07-09 15:54:55	1
ManualExample-7.30.0000-61377C88	Spanning Tree Topology		2021-07-09 15:54:51	1
ManualExample-7.30.0000-61377C88	Router, Switch, Server Topology		2021-07-09 15:54:47	1
ManualExample-7.30.0000-61377C88	Network Infrastructure Tree		2021-07-09 15:54:43	1
ManualExample-7.30.0000-61377C88	Network Infrastructure Topology		2021-07-09 15:54:39	1
ManualExample-7.30.0000-61377C88	Layer 3 Topology		2021-07-09 15:54:35	1
ManualExample-7.30.0000-61377C88	Layer 2 Tree		2021-07-09 15:54:32	1
ManualExample-7.30.0000-61377C88	Layer 2 Topology		2021-07-09 15:54:18	1

To view a map, just click on the desired **Map View**

Selecting Other Versions of the Map View

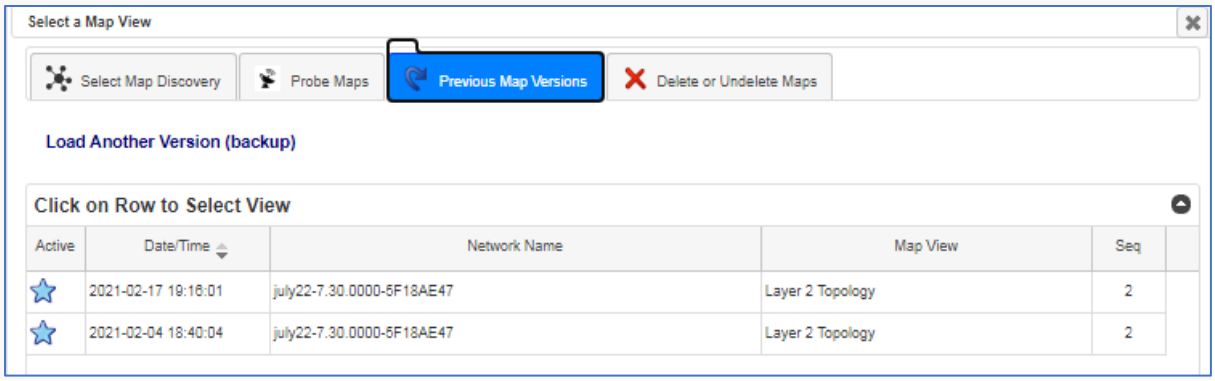
Toolbox automatically catalogues previous versions of Map Views when a Map View is Saved.

Select the **Previous Map Versions** tab to quickly select another version of the currently loaded map.

A blue star indicates which Map View version is current.

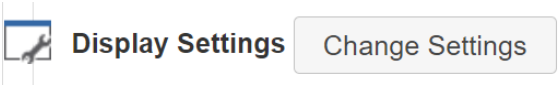
Click on a row to make that Map View the **Current Version** - this will also make this version current in Dashboard maps.

Note: You must select a Map under **Select Map Discovery** first to use this feature.

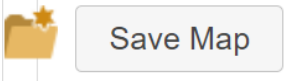


Simple Editing and Controlling Presentation

Devices may be freely dragged around the display, so that you can customize the map to your liking. To change device sizes, backgrounds etc, click on the **Displays Setting** button under the **Options** tab.



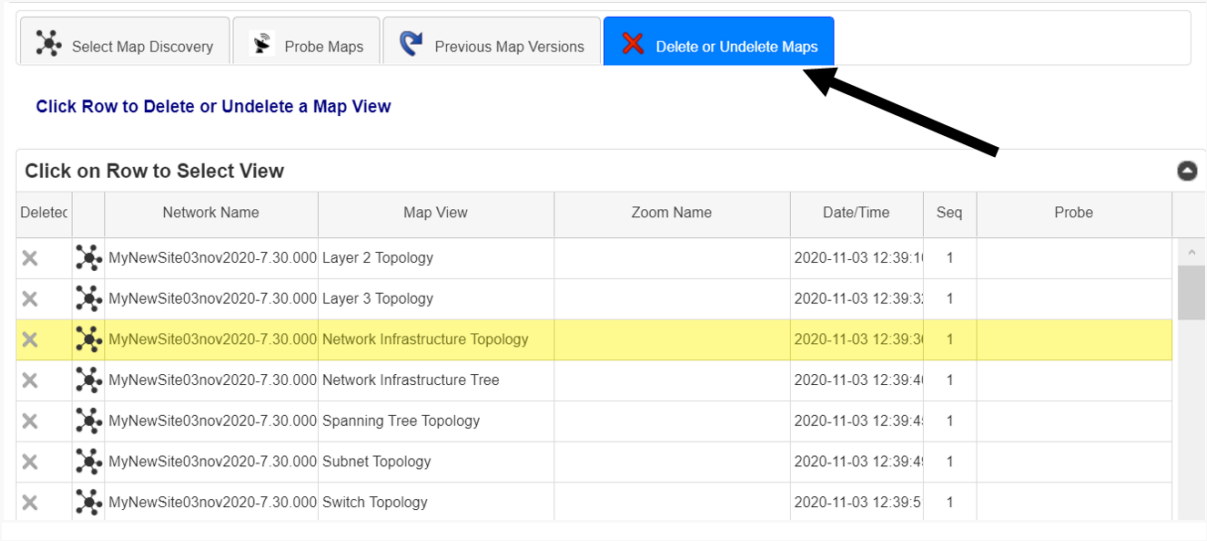
To save any changes that have been made to the Map, click the **Save Map** button that is found under the **Options** tab (a backup is automatically created).



Deleting and Un-Deleting Maps

Maps can be Deleted and Hidden from the Toolbox GUI, however they are kept permanently on the Toolbox Map Views DBase and can be un-deleted at any time.

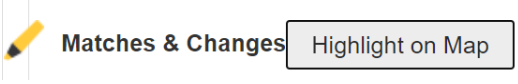
Select the **Delete or Undelete Maps** tab, then click on a Map View row to swap between Deleted <-> Undeleted status.



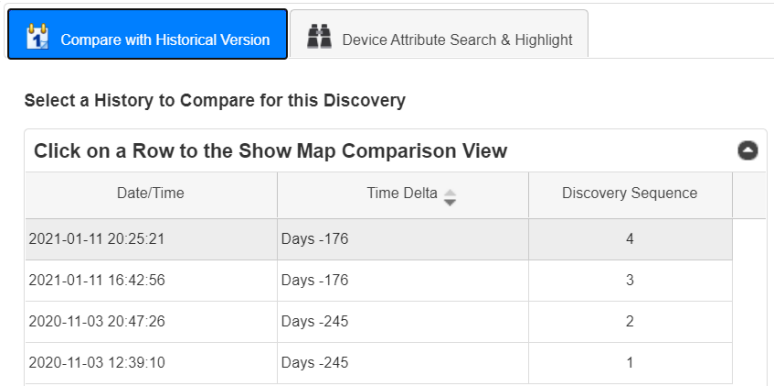
Compare Historical Maps

It is a frequent requirement to want to see changes in a map between Historical Discoveries. **Compare Historical Maps** shows extra, and missing devices between Discovery Histories graphically on the maps.

To view changes from Discovery Histories, firstly click the **Highlight on Map** button found under the **Options** tab:

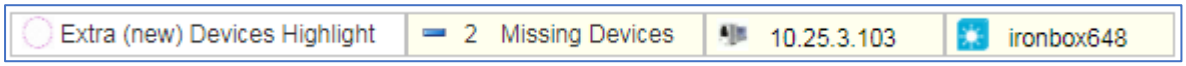


A window will appear asking you to select a previous version of the Discovery to compare with, click on the desired one:

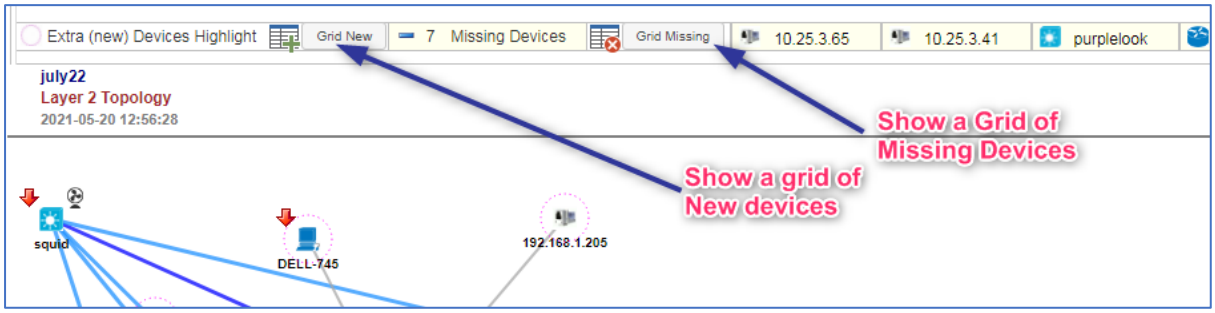


New devices will now be highlighted with a dotted ring like this:

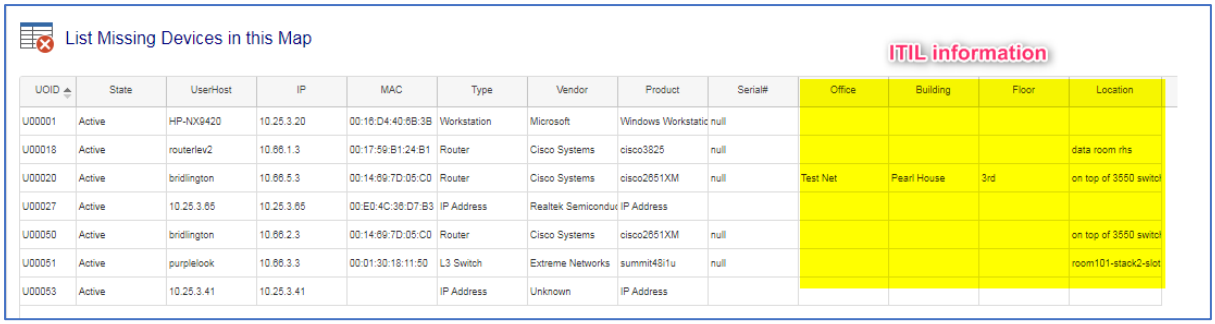
Devices that have been removed since the selected Discovery are listed above the Map view, like this:



The Map also has two buttons **Grid New**, and **Grid Missing**, which can be clicked on to show the corresponding Grid views.

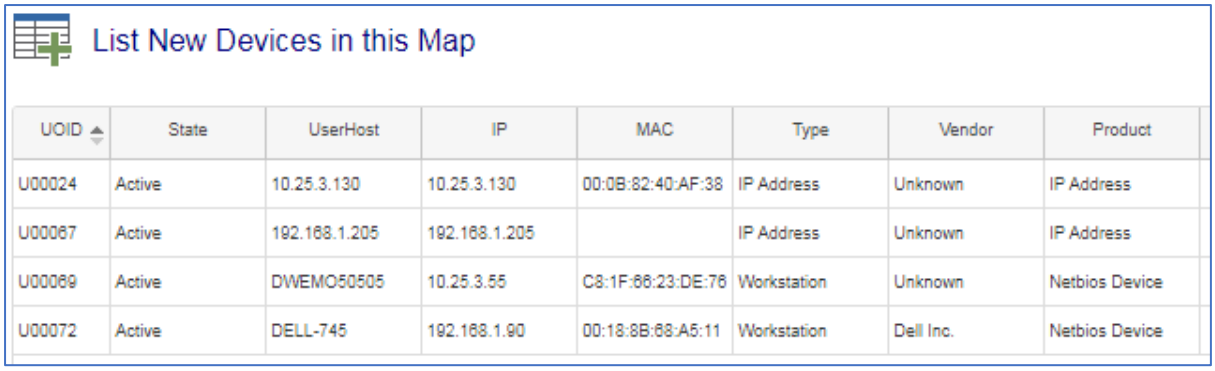


The Grids are shown below, note ITIL information is integrated into these Grids, as setup.



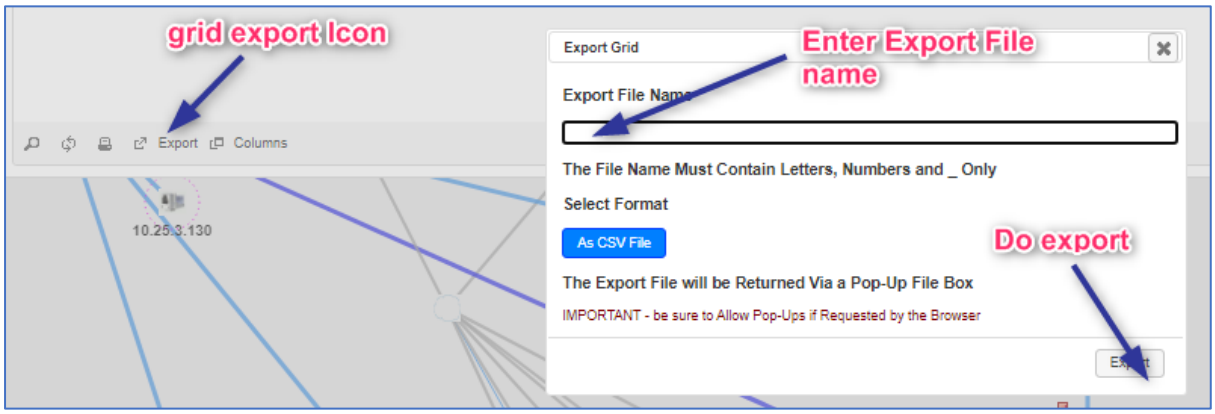
UOID	State	UserHost	IP	MAC	Type	Vendor	Product	Serial#	Office	Building	Floor	Location
U00001	Active	HP-NX9420	10.25.3.20	00:16:D4:40:6B:3B	Workstation	Microsoft	Windows Workstatic	null				
U00018	Active	routerlev2	10.66.1.3	00:17:59:B1:24:B1	Router	Cisco Systems	cisco3825	null				data room rhs
U00020	Active	bridlington	10.66.5.3	00:14:69:7D:05:C0	Router	Cisco Systems	cisco2651XM	null	Test Net	Pearl House	3rd	on top of 3550 switcl
U00027	Active	10.25.3.65	10.25.3.65	00:E0:4C:36:D7:B3	IP Address	Realtek Semiconduc	IP Address					
U00050	Active	bridlington	10.66.2.3	00:14:69:7D:05:C0	Router	Cisco Systems	cisco2651XM	null				on top of 3550 switcl
U00051	Active	purplelook	10.66.3.3	00:01:30:18:11:50	L3 Switch	Extreme Networks	summit48i1u	null				room101-stack2-slot
U00053	Active	10.25.3.41	10.25.3.41		IP Address	Unknown	IP Address					

Above is a summary of Missing Devices between the comparison discoveries as selected by the user, below is a Grid showing devices that are new in this historical version.



UOID	State	UserHost	IP	MAC	Type	Vendor	Product
U00024	Active	10.25.3.130	10.25.3.130	00:0B:82:40:AF:38	IP Address	Unknown	IP Address
U00067	Active	192.168.1.205	192.168.1.205		IP Address	Unknown	IP Address
U00069	Active	DWEMO50505	10.25.3.55	C8:1F:66:23:DE:76	Workstation	Unknown	Netbios Device
U00072	Active	DELL-745	192.168.1.90	00:18:8B:68:A5:11	Workstation	Dell Inc.	Netbios Device

To export the Grid, click on the standard Grid Export icon as displayed below:

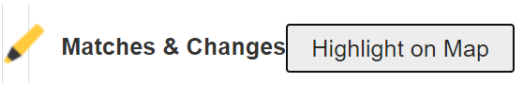


Device Attribute Search & Highlight

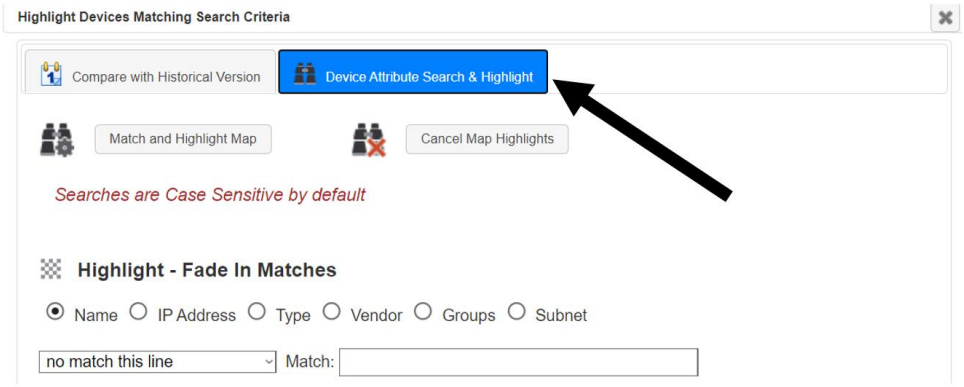
The **Device Attribute Search and highlight** function has advanced search options like true wild cards and REGEX. There are three independent highlights offered to show different match classes on the same map.

To access the Device Attribute Search & Highlight follow the steps below:

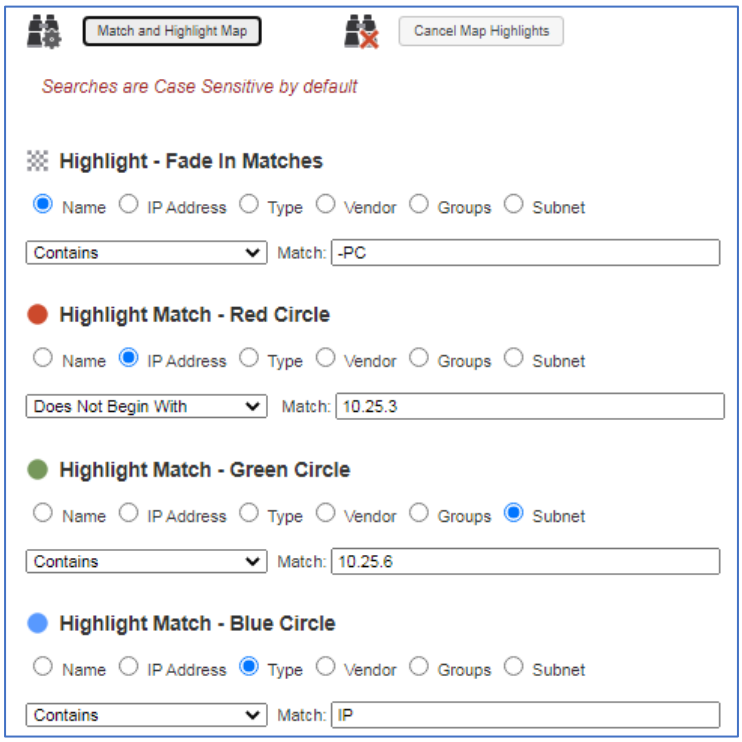
First, click the **Matches & Changes** button found in the **Maps** panel under the **Options** tab:



Next switch over to the **Device Attribute Search & Highlight** tab



As seen below multiple searches can be set up at the same time:

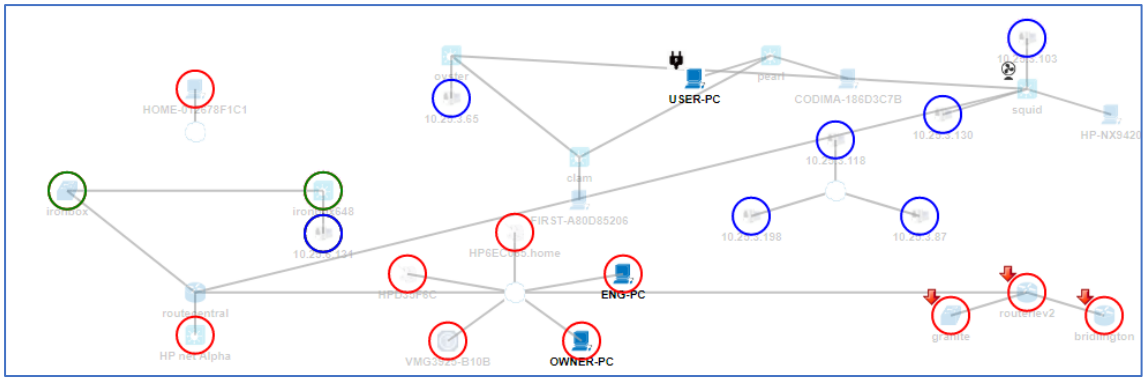


In the example map below, only devices Containing '-PC' are **not faded out**.

Devices not in IP prefix `**10.25.3**' are circled red.

Devices in Subnet '**10.25.6'** are circled green.

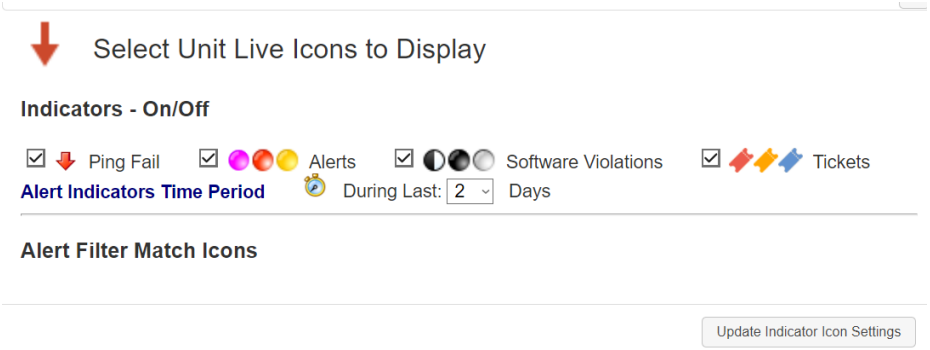
Devices Type '**IP**' are circled blue.



Live Indicators

Click on the **Live Indicators** button, found under the **Options** tab, to view a popup that allows live monitoring of Down Devices, Alerts, Software Violations, and Job Tickets.

Indicators can be turned on and off and the settings will be saved with **Map Save**. So, specialist Maps can be created just showing Job Tickets for example.



Drill Downs – Network Device

Double clicking on a Network Device links to a comprehensive analysis of the device on Traffic, Alerts, Tickets, and an SNMP browser.

Instant Drill to the Navigator panel is selected if SHIFT Double click is done over a device in the map.

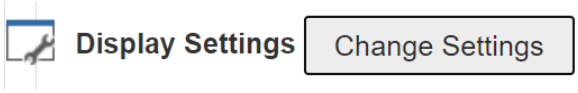
Drill Down – Inter-Device Link

Double clicking on a Link in the Network Map gives a traffic analysis and the ability to switch Monitoring On/Off.

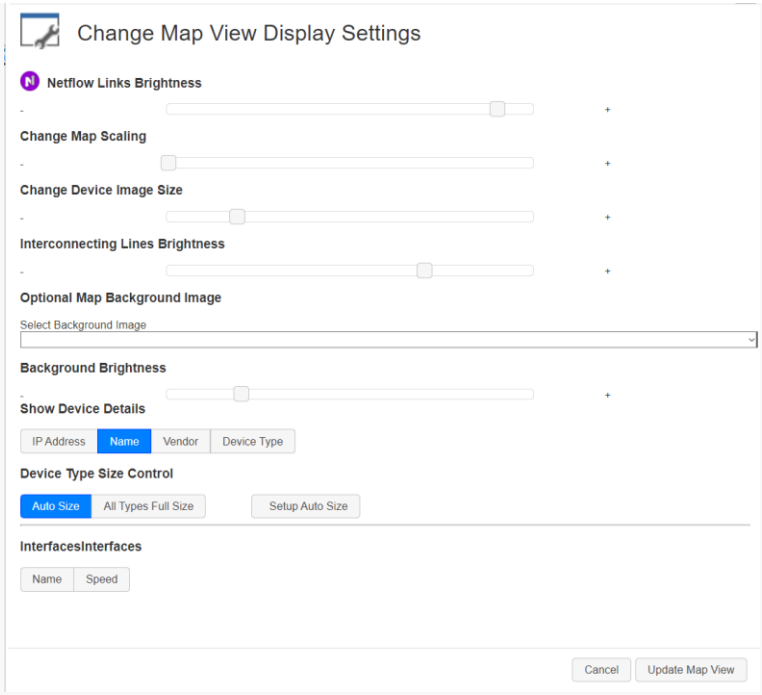
Web Map Display Settings

The Map Display Settings allow you to customize the appearance of the network map to your liking.

To access the Map Display Settings, click the **Display Settings** button found under the **Options** tab.



A window will now appear with several setting that alter the maps appearance, an explanation of each setting can be found below:



Change Map Scaling - Use this slider to change total size of the Map View. The map will attach scroll bars if the map no longer fits in the display area.

Change Device Image Size - The Map Devices will shrink or expand and the associated Indicators like Ping Down will also try to follow the Device scaling (within practical limits).

Interconnecting Lines Brightness - use this slider to fade out or intensify the Lines between Devices.

Optional Map Background Image - The user has an option to select an image as a map background, see **How to Add my own Map Background** if you would like to add your own images.

Background Brightness - The slider allows the user to fade or brighten the selected map background.

Show Device Details – Select what information to show under each device.

Device Type Size Control – Adjust the size of the images for a specific device type.

Interfaces – gives you the options to see the name and speed of connections between network devices.

Using Alert Filters to show Filter Matched Alerts in the Map

The system accepts Alerts from many internal sources such as Ping Fails, CPU overloads, Link Errors created by the Toolbox monitoring engine.

NetFlow violations such as Security breaches detected by NetFlow Analytics module such as DDoS attacks or Blacklisted IPs such as Botnet controller IP matches, or DNS or other server types, Spoofing attacks.

Additionally, external Alerts can be directed to Toolbox via Syslog or SNMP TRAPs from network devices which give device status changes like a Fan Failure, plus security information from Firewalls.

Windows logs can be tracked in Toolbox, which provide information on configuration and Security events that are converted by Toolbox into Alerts that can also be matched and displayed on the Web Maps.

These incoming Alerts are processed by the Toolbox Alerts and Ticketing System and matches are tracked per network device. This tracking information is presented in the Toolbox Map. There can be any number of Alert Filters, so the Toolbox Map interface has been heavily revised to display and control the new Alert Matcher information.

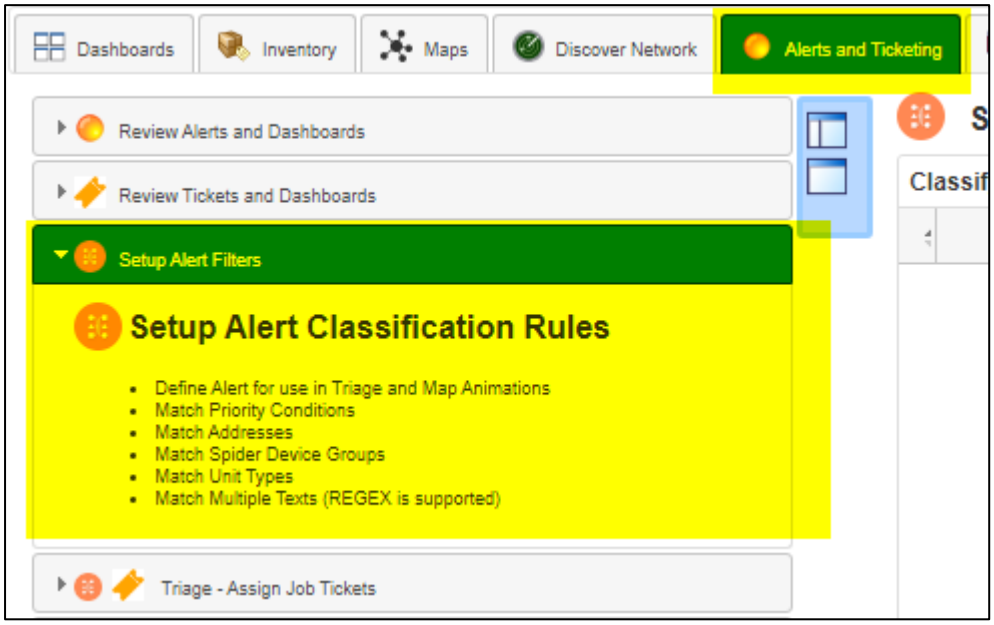
The Alert Matchers are also used to create Job Tickets which is still fully functional.

The Filter Alerts can be a very extensive list as an unlimited list of filters can be created.

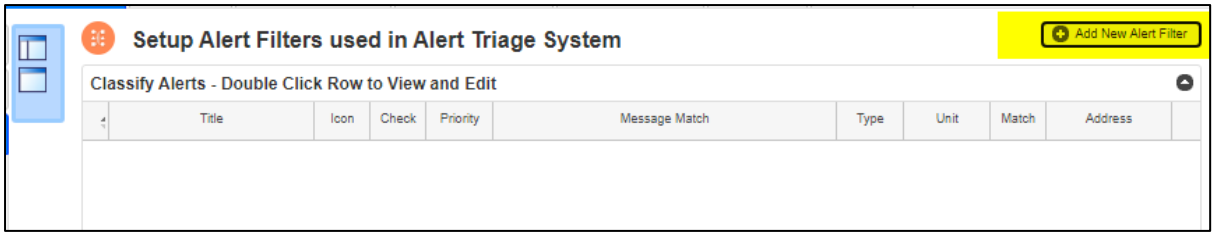
The filters are created under the Alerts and Ticketing Tab as below: -

Setting Up Alert Filters

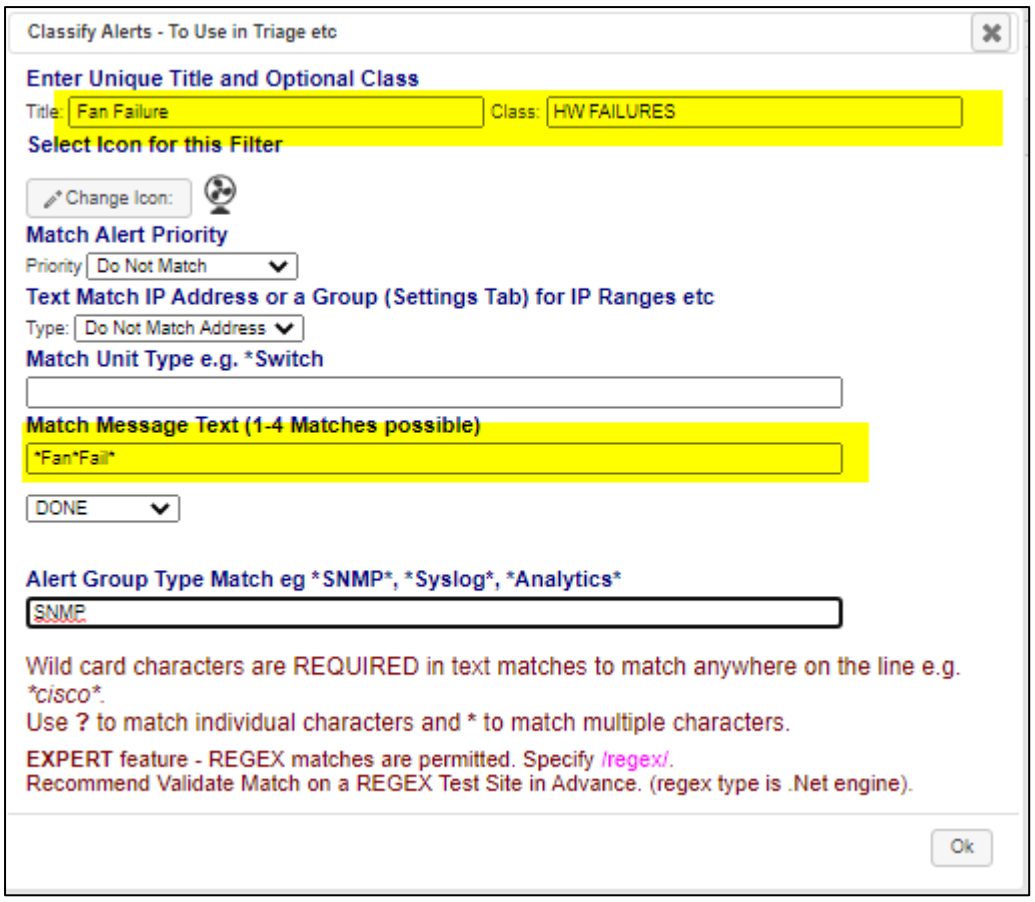
Click on the Setup Filters panel as below:



Click on the **Add New Filter** button to add a new Alert Filter.



A dialog box appears allowing very detailed Alert Matching options: -



Any number of matchers may be added. For Map usage it is important to select an Icon using **the Change Icon** button.

After an Alert Filter is setup, the system will track each alert match per network device.

Showing Filtered Alerts on the Map

Matched filters will appear on the Network map as below represented by the Alert Filter ICON

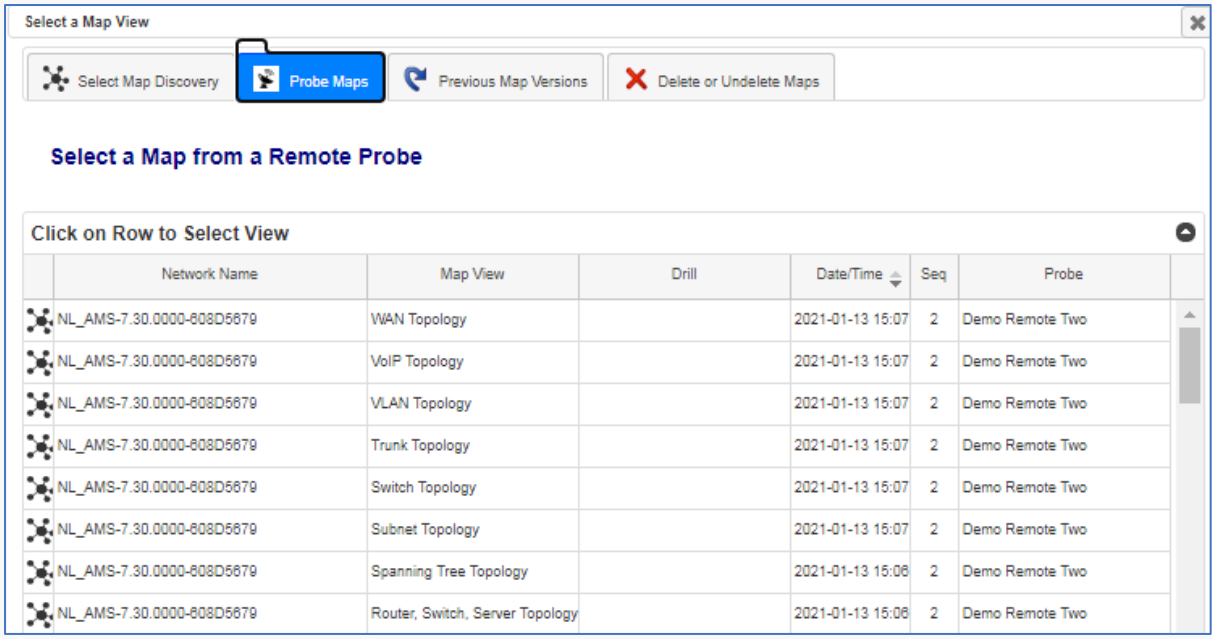
Two devices are shown above, device **ironbox** shows a link down and a fan failure. The device named **Codima**-186D3C7B, shows a Windows Event match plus a Netflow detected Worm. Toolbox supports Windows Event Log Retrieval and also NetFlow Analytics to detect blacklisted sites etc.

The Map GUI gives direct control over which Icons are displayed. Below is the standard Icons that show Toolbox monitoring status. Clicking the Status Events tick box turns all status events on or off. Clicking on individual tick boxes, such as Ping Fail, switches only that Status on or off.

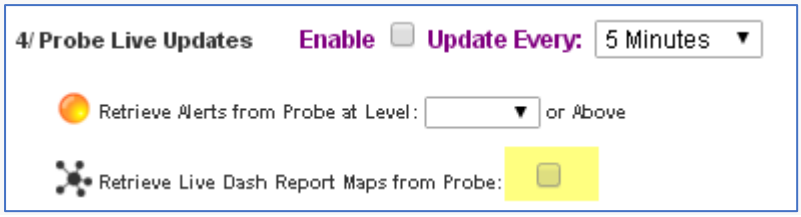
Alert Filter matches can also be selectively shown on the Map.

Viewing Probe Maps

Under the Main GUI Settings tab Probe Maps tab, Map Views can be viewed from Remote Probes.



Note: Probe maps are automatically retrieved from the Probes if requested under the Probe settings setup popup. To change auto-Map retrieval, under **Settings** tab, panel **Probes** are selected and a Probe Grid row is clicked. The popup below will appear, tick box highlighted in yellow in the screen shot below.



What do Animations Do?

A probably unique feature of Toolbox is to be able to show both Live and Replayed Animations of Network Events on the Topology maps.

This gives the capability to see for example a DDoS Attack detected by Toolbox Netflow Analytics against Link Loadings from SNMP and CPU Utilization on the Servers - also with Filtered Alert Animations. (For NetFlow contact product support for further details)

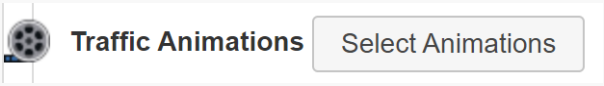
For example, one can see running Software with Black/White Rules against Highly Filtered Netflow Traffic matching Known Virus Attacks detected by Netflow on any number of Probes in a single Dashboard Report. For Netflow support please contact local support.

Animation Control

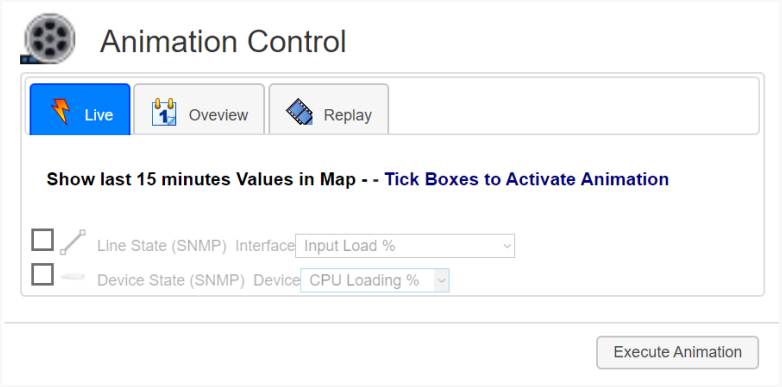
Traffic and System metrics can be replayed to check network conditions historically. The monitored devices CPU loading can also be replayed. Link colouring for monitored inter-device links shows traffic levels or error levels like dropped packets.

Overview and Replay Animations

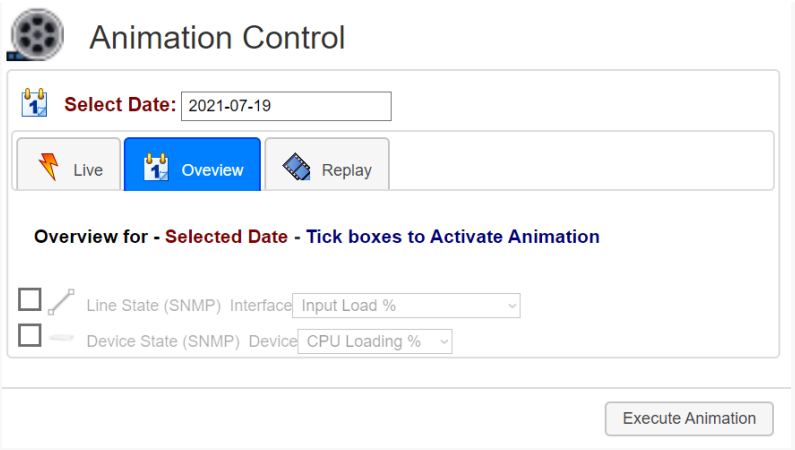
There are 3 different Animation Modes, **Live,** which shows the current measured values, **Overview,** which shows a Day Summary - good for quickly assessing where to look and **Replay** historical patterns with full video recorder type controls. These can all be accessed from the **Traffic Animations** button found in the **Maps** GUI under the **Options** tab.



Live mode is shown below:

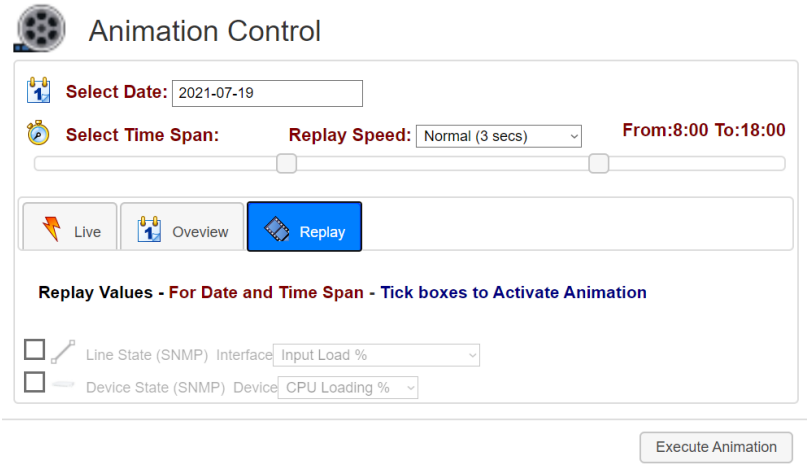


Overview mode is shown below:



To activate this mode simply set the **Select Date:** calendar control and click on the **Execute Animation** button.

Replay Mode is shown below:



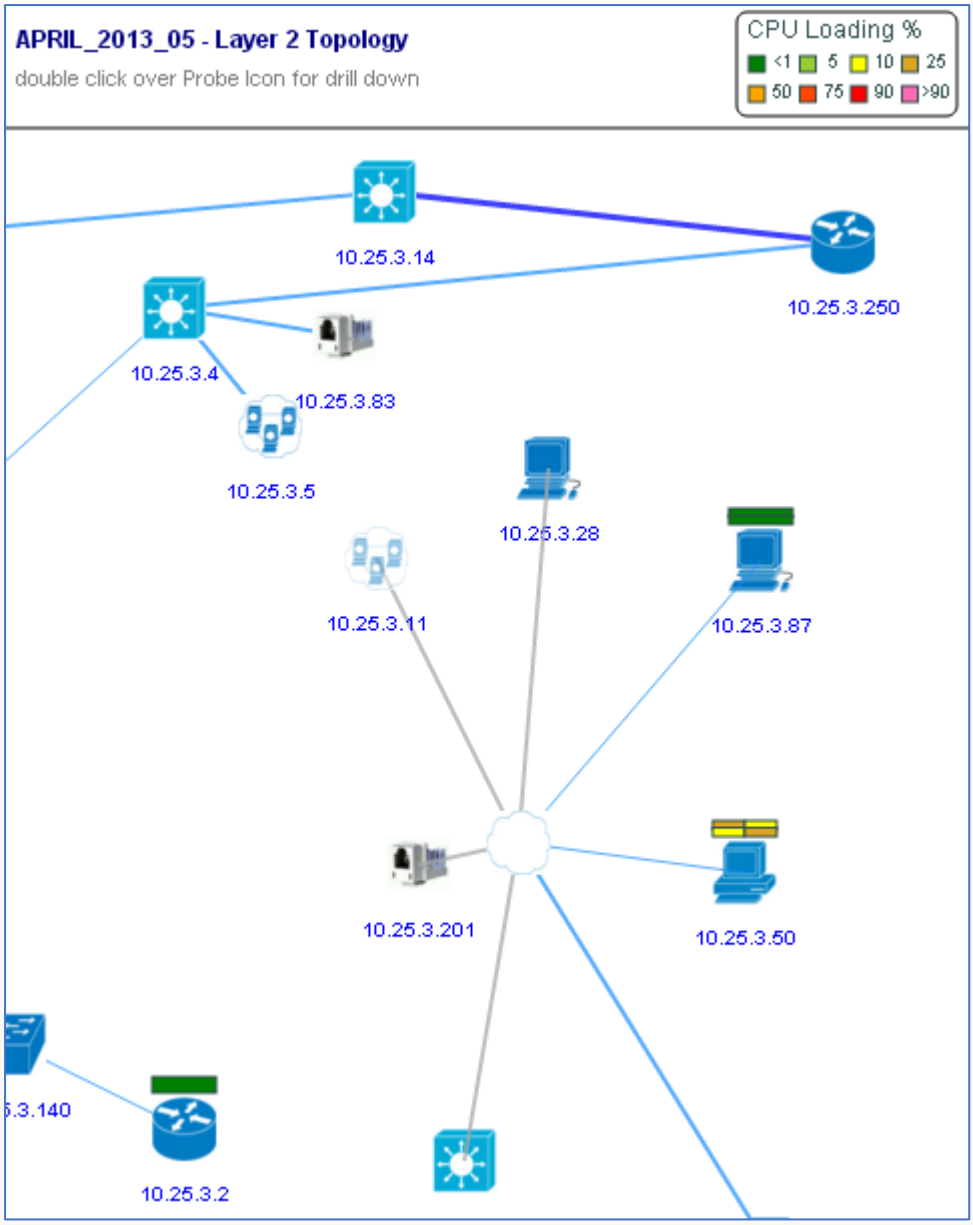
First select the date from the Calendar control **Select Date:**

Next use the slider control **Select Time Span** to drag the two handles to the required time span, for instance around the time an incident was known to occur.

Then choose a **Replay Speed** using the dropdown control. This can be used to quickly run through an animation, or it can be done in slow motion instead.

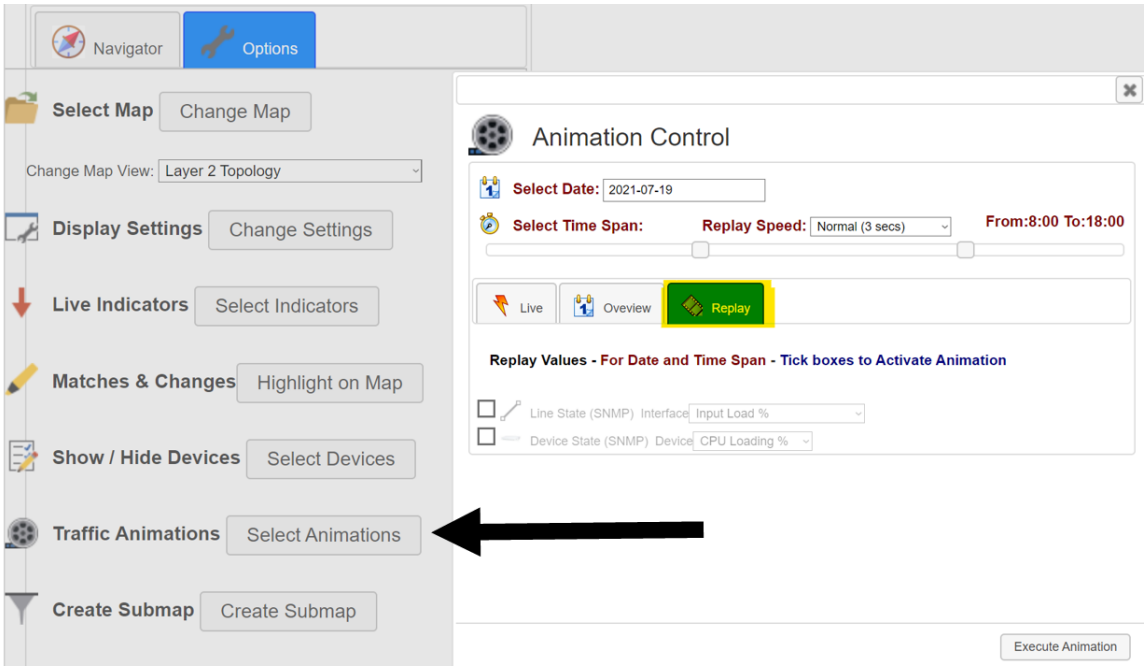
Click on the **Execute Animation** button to start the animation processing.

Below is an example of Animations on a Web Map.



A single bar denotes a single CPU for **10.25.3.2**, double bar shows there are 2 CPUs for **10.25.3.87** and 4 CPUs for **10.25.3.50**. Note the Color Key box in the top right, this decodes the bar colours into \% Loadings. In the case of 10.25.3.2 loading is less than 1\%, in the case 10.25.3.50 loadings 10-25\% for the 4 CPUs.

Below we have selected Replay Animation mode, this allows the user to replay on a chosen date:



When Animation is selected in the dialog above then a bar appears across the top of the map:

The controls to play forward in time, pause the animations and go backwards in time, are highlighted in yellow.

The green highlight is the time progress bar, it shows the current animation time and can also be used to drag the animation time to a new time by dragging the handle using a mouse. The arrow points to the mouse drag handle.

The current animation time is shown in the blue highlighted section below. The icon shows the selected mode; going forward, paused or going backwards in time.

Device Front Panel View

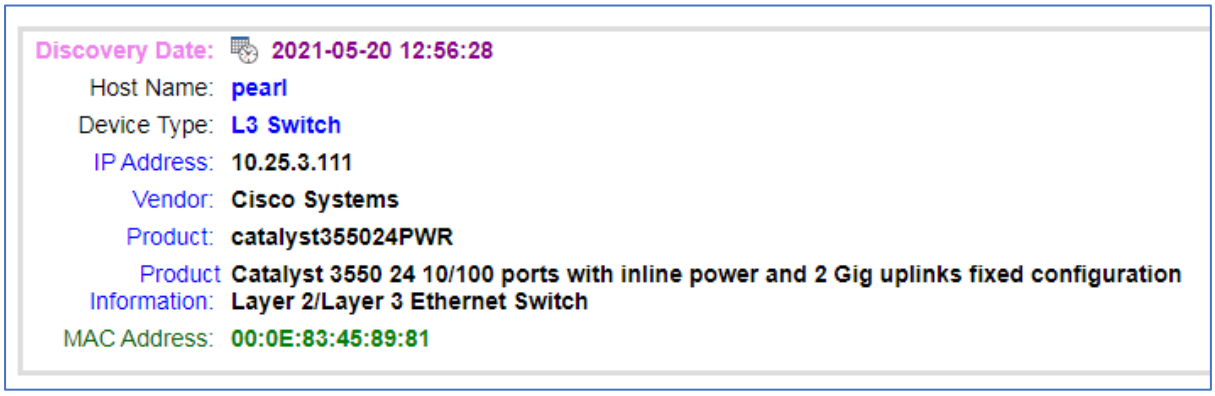
The Port View is a feature that is accessed by double clicking on a device in the web map and then clicking **View Ports**. A simulated device front panel is then shown with information on VLAN membership and also Link States, full breakdown of Device Details including ITIL.

To use this feature, click on **the View Ports** menu option which displays the Device Ports View as below:

This panel shows a large amount of information that is great for getting an instant handle on the switch configuration without having to browse complex configuration files.

Device Details

Extensive device details learned during the Discovery process, are shown to the left of the device summary box as below:



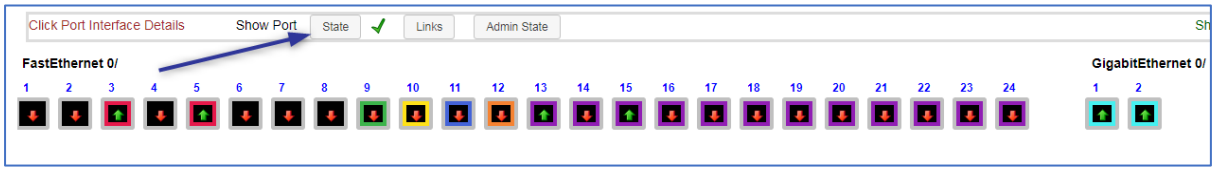
For each device that is selected by the map, comprehensive device details are revealed, including the date the information was updated in Discovery Date above.

ITIL Details

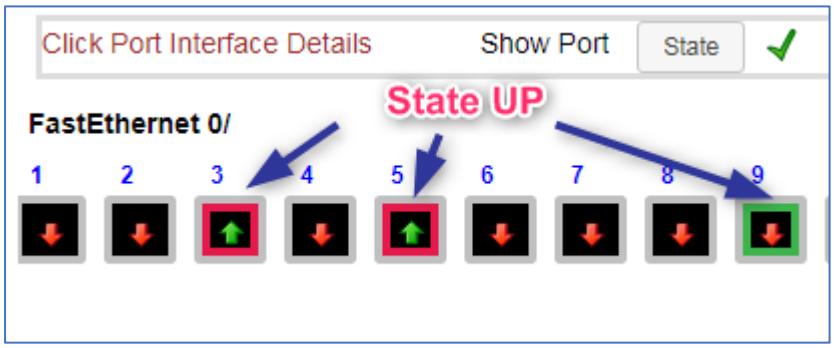
Direct access to an ITIL summary is shown to the right of the device summary box shown below:

Port Status Options

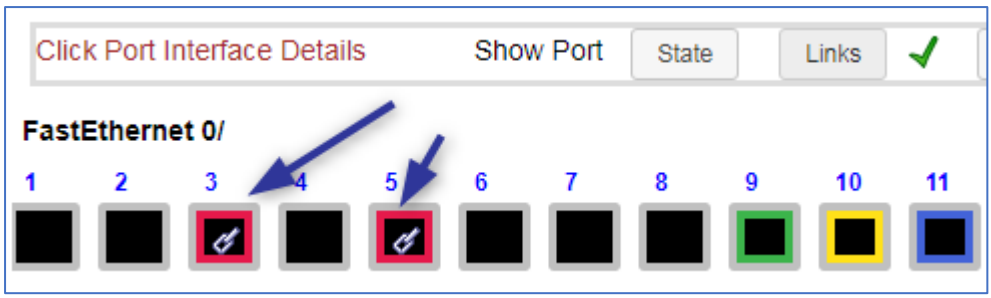
There are three options to show all ports status by clicking on **Status**, **Links** or **Admin Status** buttons as below: -



The **State** button is clicked (green tick), and it can be seen that ports 3, 5 and 9 were up at Network Discovery time.

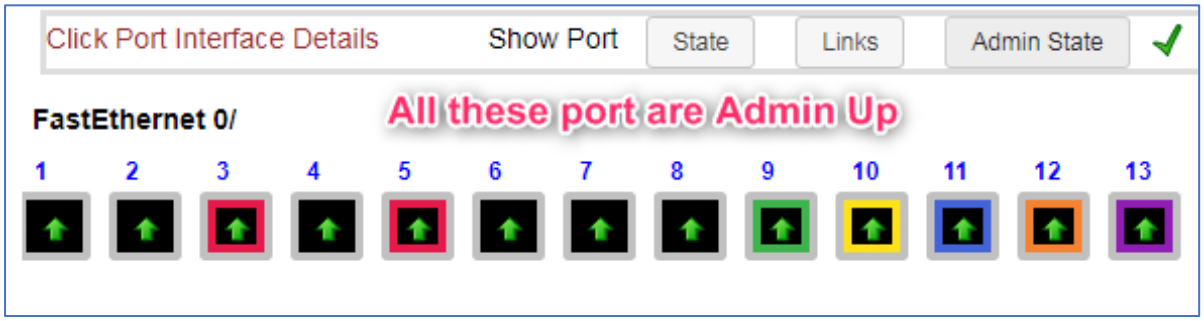


In this screenshot the **Links** button has been clicked (green tick).



The ports containing the Link icon, as pointed to by the arrows in the diagram, show ports where Discovery has identified a linked device.

It is useful to see which ports have been Administratively Configured to be in state up or down. This can pinpoint configuration errors at a glance, click **Admin State** button (green tick), to select this view.

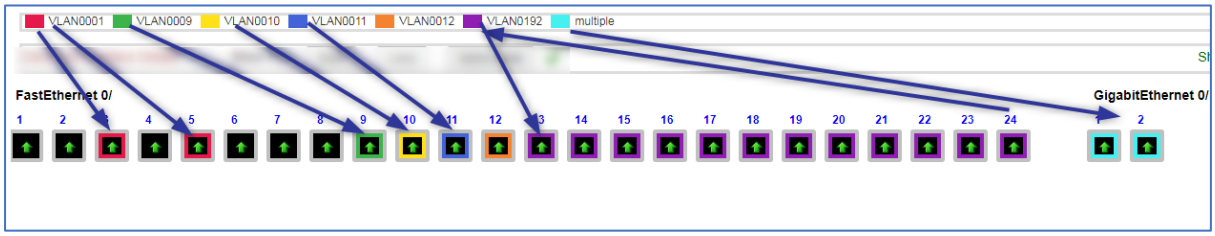


All ports in the picture are configured to be Up.

VLAN Information

The Device Port View always shows which ports are in which VLANs.

The VLAN colour swatches (top) identify VLAN numbers (which are often given names by the network administration, like 'Building 25, 2nd floor').

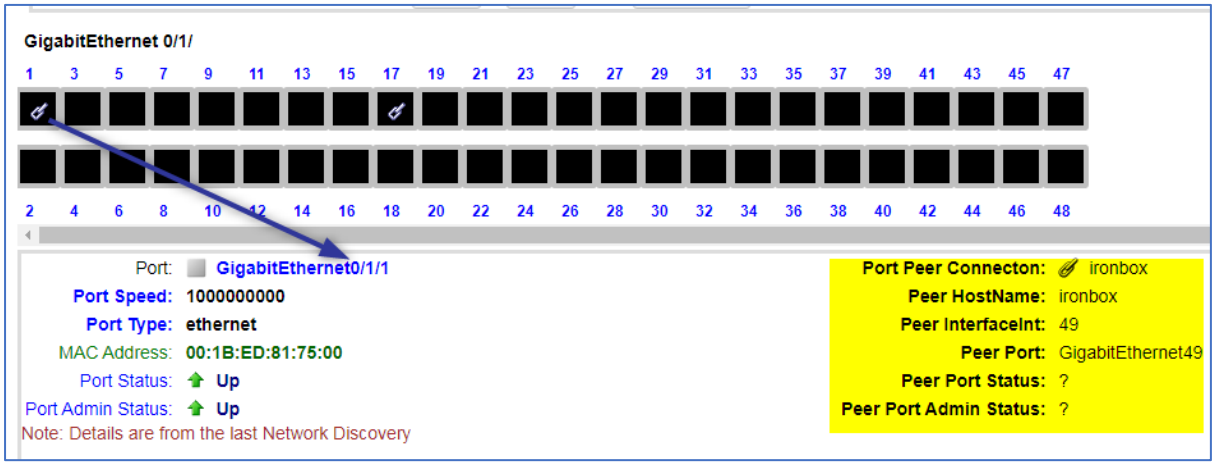


Port Drill Down

The Device Ports view gives detailed information per port - that is derived during the Network Discovery. It is accessed simply by clicking on any port.

In this case by clicking on **GigabitEthernet** port number **1**, a breakout is given for this port in the window underneath the ports Block.

Selecting Links mode shows which ports are linked to other devices found during the discovery.

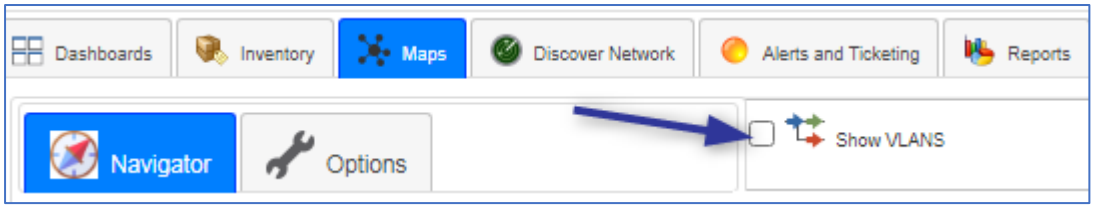


Clicking on a linked port such as port 1 above, shows the peer details highlighted in yellow. Extremely helpful information on the ground next to the box or somewhere remote.

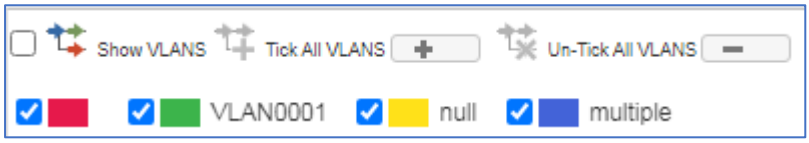
VLAN Display for Web Maps

VLANs are used extensively to segment network user groups using the Layer 2 port based VLAN concept built into virtually all switches. The map aims to show which links are in which VLANS, thereby showing at a glance on the Web maps, what VLAN groups are active and where in the Topology.

This option is selected when viewing a Web Map by clicking the tick box as per the diagram below: -

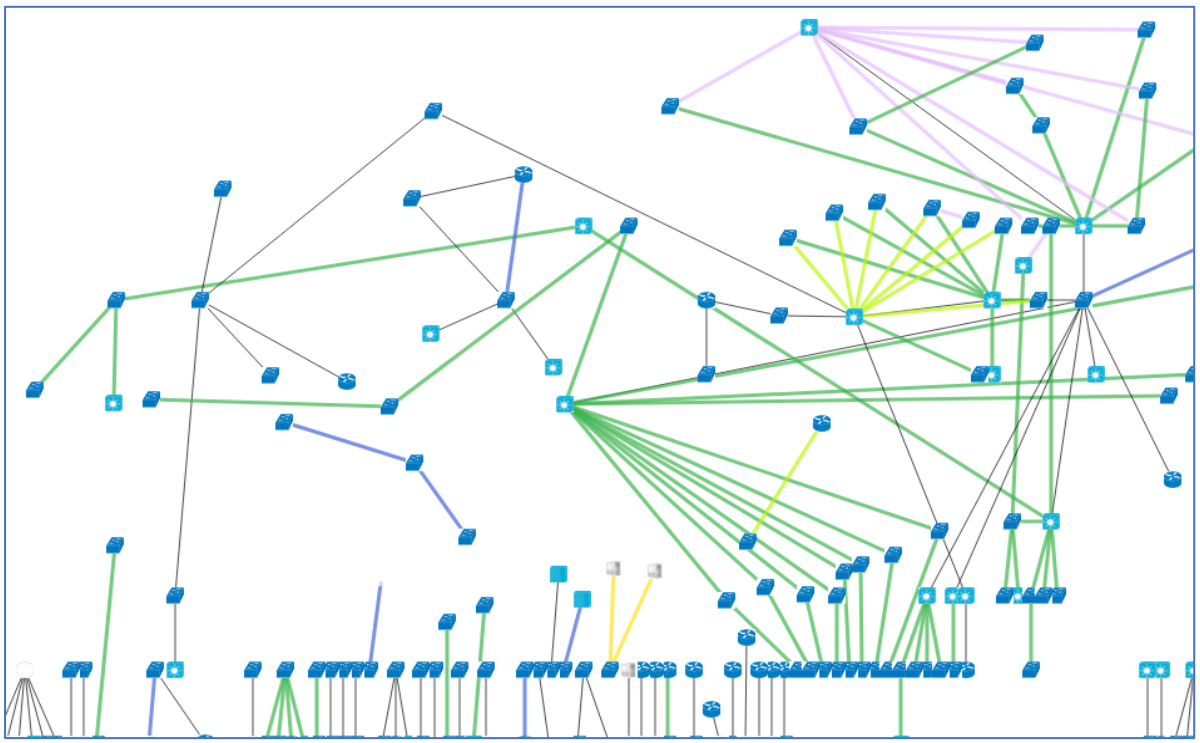


After ticking the **Show VLANS** checkbox the following display appears: -



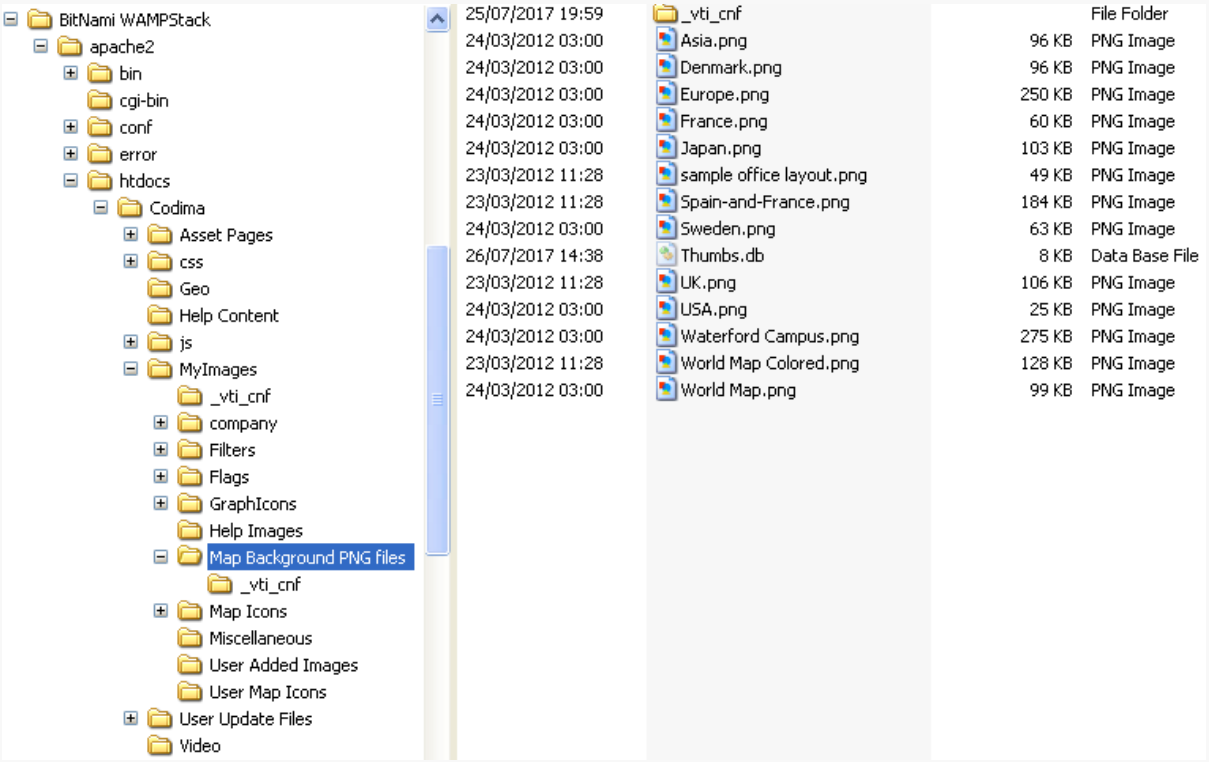
This gives control over which VLANs are to be displayed on the Web Map by ticking or un-ticking specific VLANs.

The **Tick All VLANS** and **Un-Tick All VLANS** buttons quickly show all or no VLANS, useful when there are very many VLANs, as is often the case with large networks.



How to Add my own Map Background

The Map Backgrounds are stored in a special folder in the Web Server Directory under **Program Files** see below:



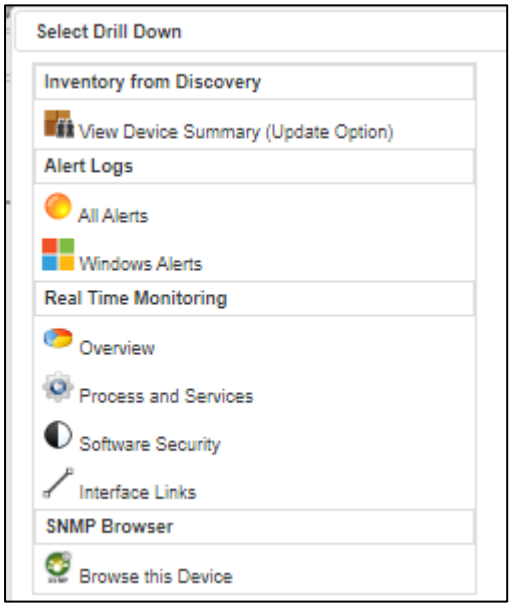
After adding new Map Backgrounds, refresh the Toolbox Web Page to load the new Map Background images.

Around 80 Background Web Maps are available for use in Inventory Explorer Views and as backgrounds for the Web Maps.

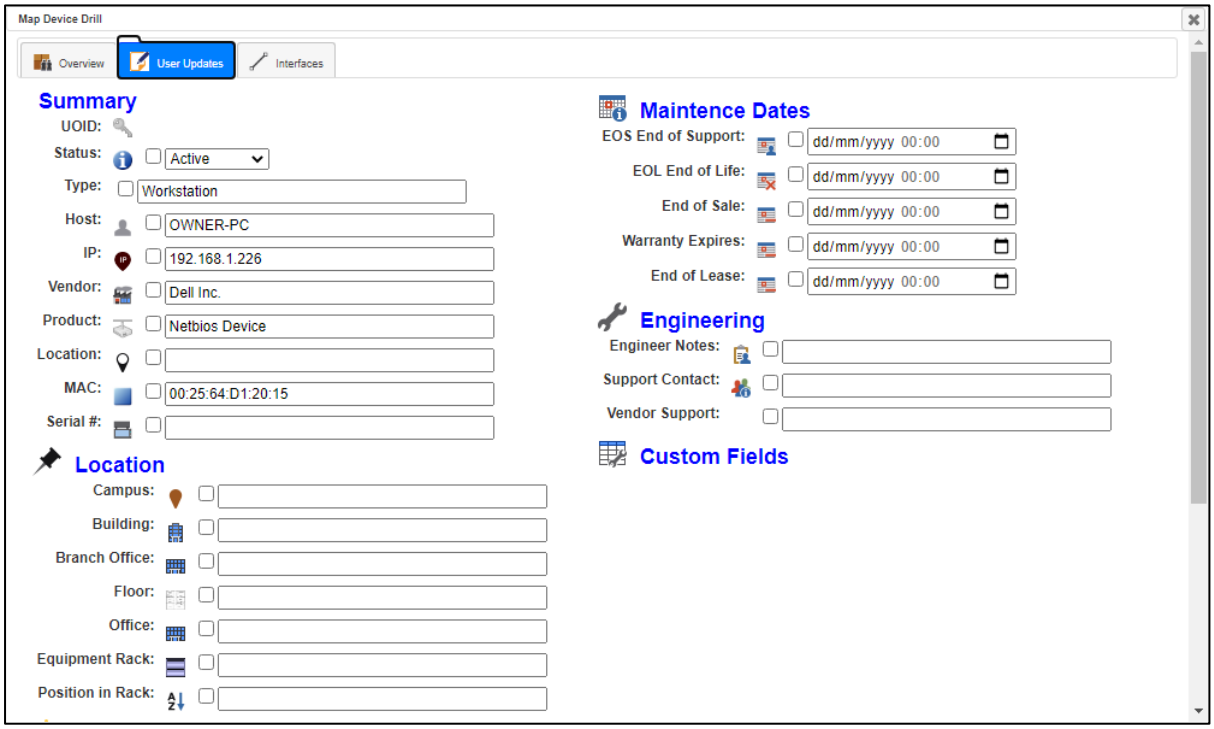
They will then appear in the Select Map Background dropdown list in the **Change Map View Display** dialog box (after clicking display options icon on LHS icon list in the map view).

Inventory/ITIL drill down from the Web Map

The Map System matches Map details including the Discovery Name and History Sequence to link Discoveries to Maps. The map can then support drill down from a map device to an inventory device details. The Map Drill allows direct selection of other existing features such as a SNMP Browser.



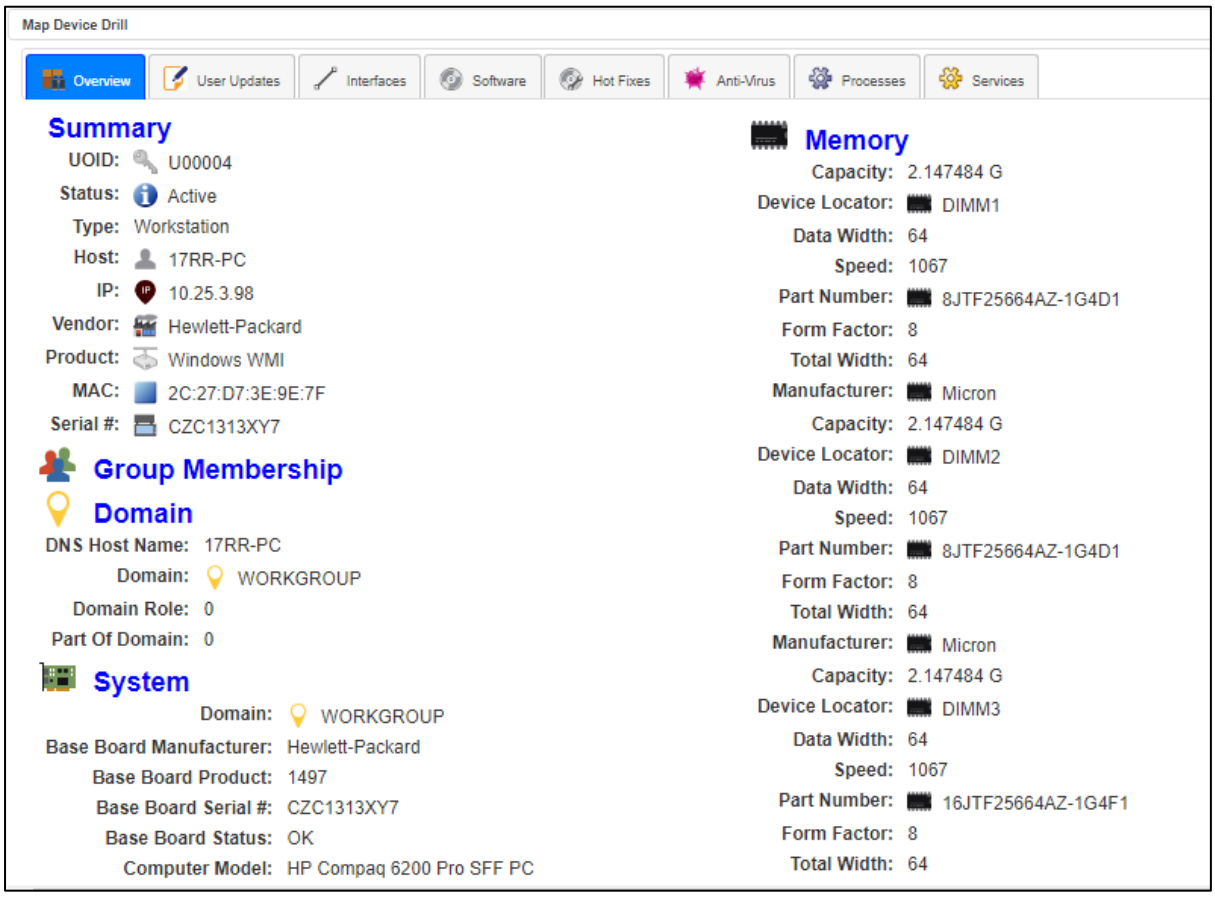
Clicking on the View Device Summary option brings up the new ITIL drill down dialog box for a non-WMI device.



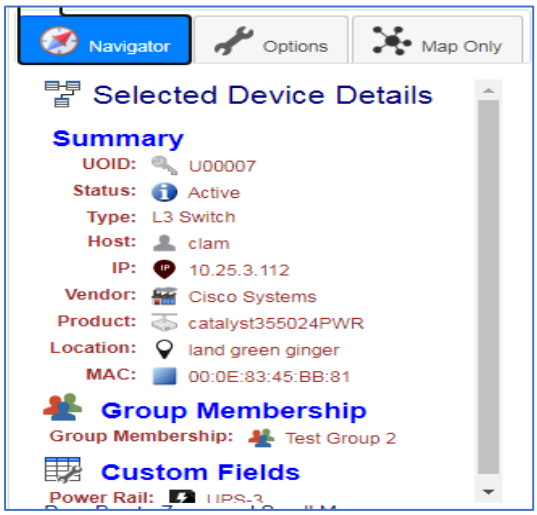
All update features and views are supported such as setting the Device Building.

Below is a Map Device drill down for a device that supports WMI.

The analysis has now got additional detailed information and other options such as Hot Fixes, Anti-Virus and installed software plus running software (processes and services) are available.



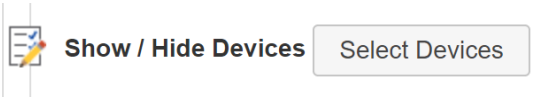
Note there is also a SHIFT Double click function to see a detailed breakdown in the Navigator Panel as below, ***in addition to the Inventory NO SHIFT Double click on a device.***



Filtering Web Map Content

Sometimes Maps can be extraordinarily complex when large networks have been discovered by Toolbox. That is why we have the option to filter maps in several different ways, in order to help you narrow down a map immensely.

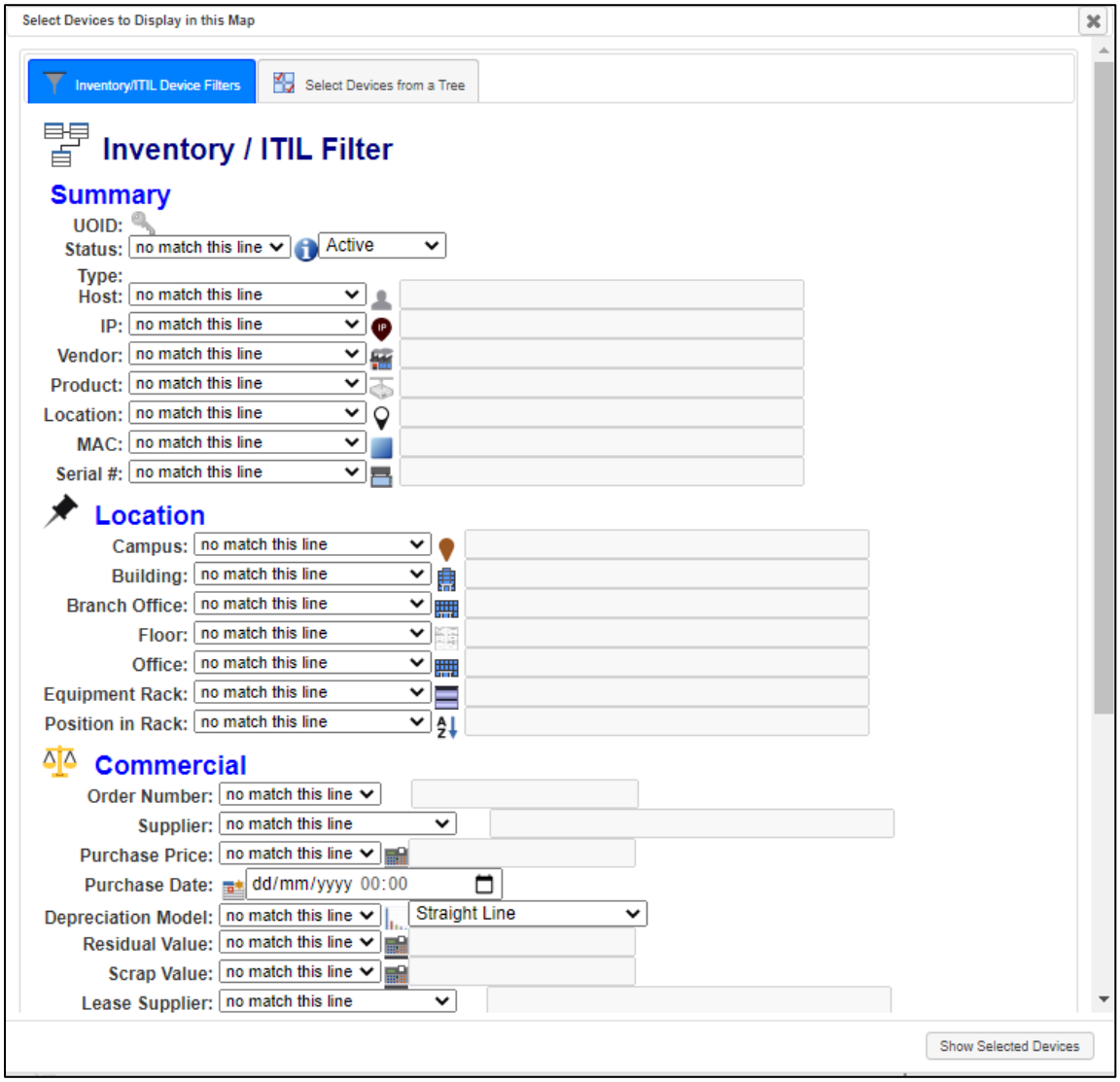
To access the Map filter click on the **Show/Hide Devices** button



Inventory/ITIL Device Filters

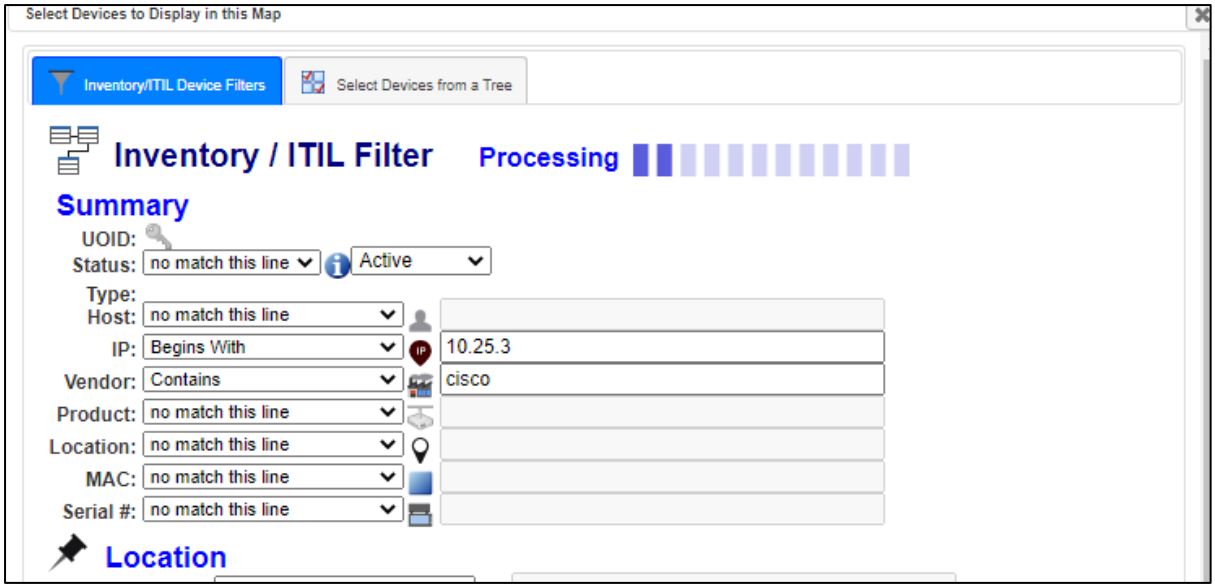
The first method of filtering your map is through using the Inventory/ITIL filter.

For example, you may restrict Map to Devices on a Campus and that are also over a certain value. The filter options are very extensive.

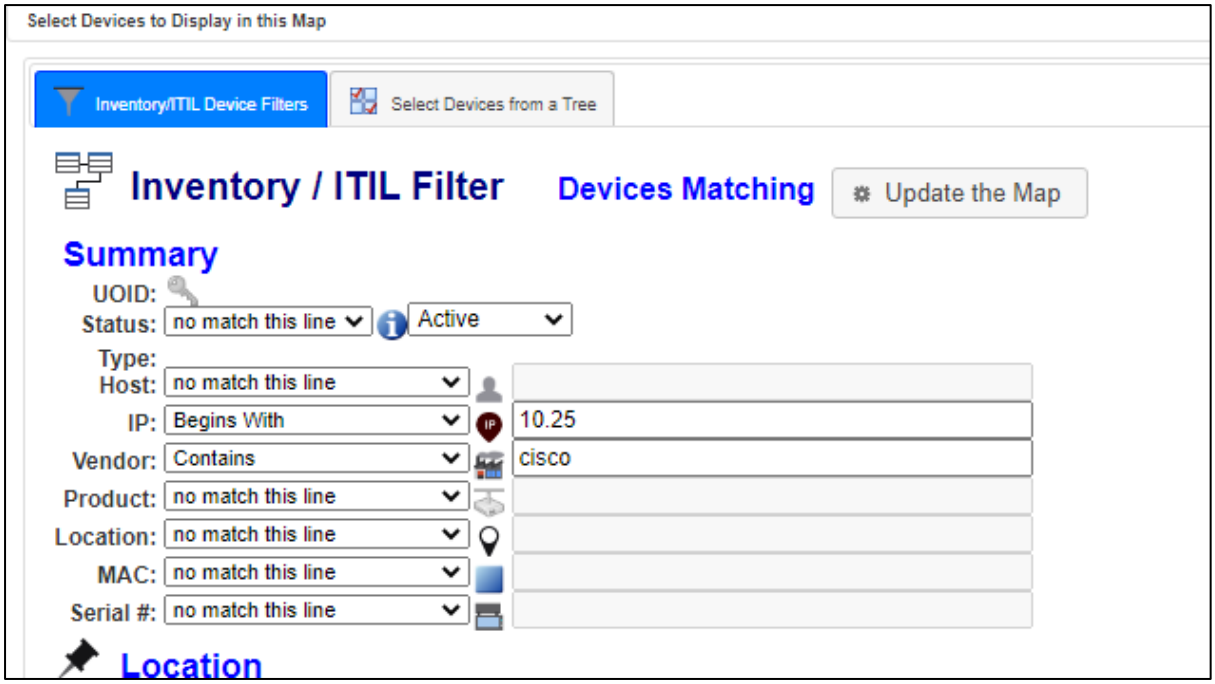


Filter Options are selected in the dialog box shown above.

Clicking on the **Show Selected Devices** starts the Filter Process and the processing indicator appears



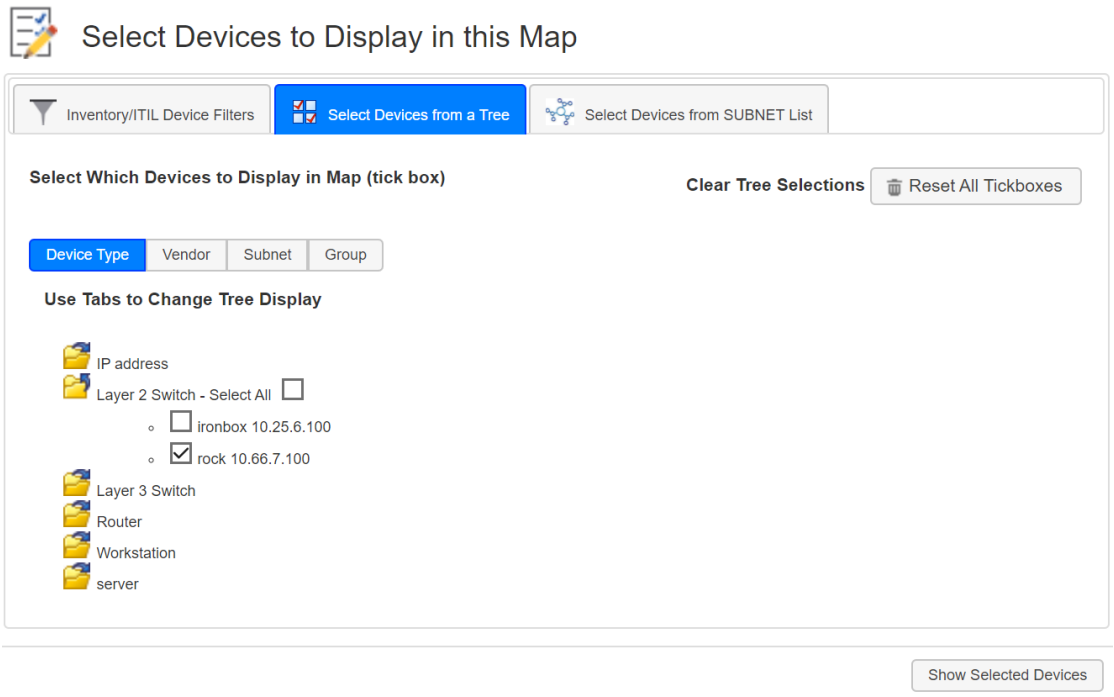
When processing is complete a button appears to update the currently loaded map.



Clicking on **Update the Map** will show only the devices matching the Inventory/ITIL filters in the updated Web Map. To cancel the Filtering simply reload the map.

Select Devices from a Tree

The second method of filtering the map view is to select devices from a file tree.

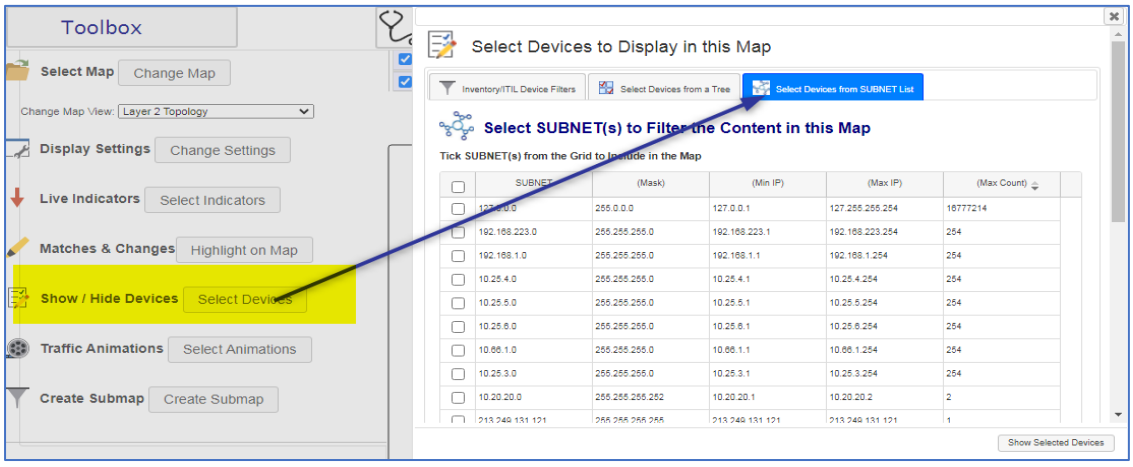


Deciding which devices to be displayed on the map is as simple as ticking devices that you wish to view on the map and unticking devices that you want to be hidden.

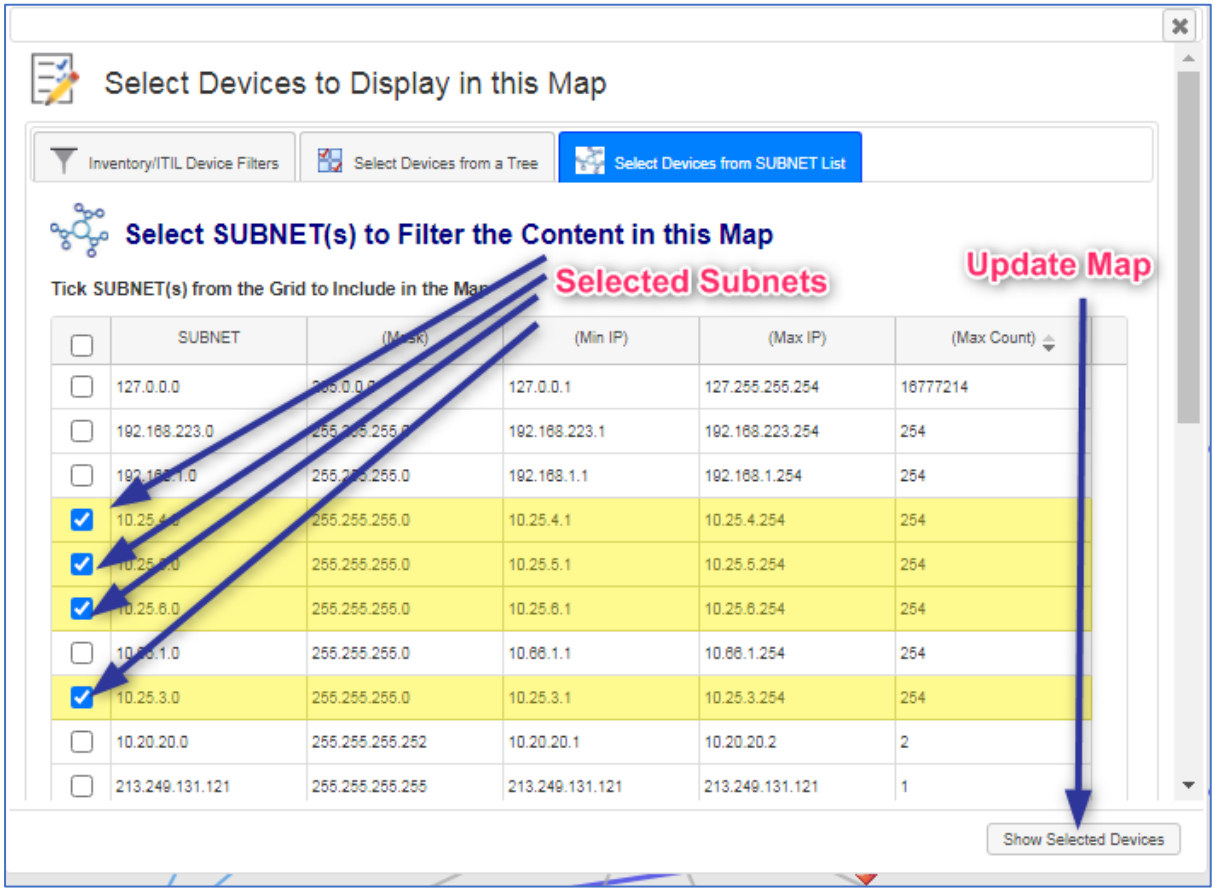
You may sort the file tree in a few different ways, in order to more easily find the devices, you are searching for. The options available for sorting the directories are **Device Type**, **Vendor**, **Subnet**, and **Group**.

Select Devices from a Subnet Group

The last method is **Select Devices from Subnets** as below:



The user can choose subnets, that are to be included in the map to reduce complexity as required, by using the row tick boxes.



Downloading Visio Maps

Being able to professionally document and display network maps is important for any organisation with an IT infrastructure. Codima Toolbox comes equipped with an integrated Visio diagram download feature that doesn't require any plugins and supports a wide range of map layouts. There are only two requirements to be able to use this feature, the first is that a copy of Microsoft Visio is installed on the same machine that runs your networks discoveries, the second is that you must have one of the following licenses:

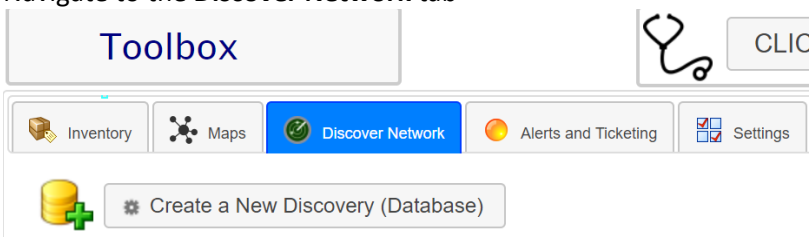
- Free License
- Network Inventory with Maps in Web and Visio Toolbox
- Network Inventory with Maps in Web and Visio and Monitoring + Alert Ticketing Toolbox

Setting up Visio Export

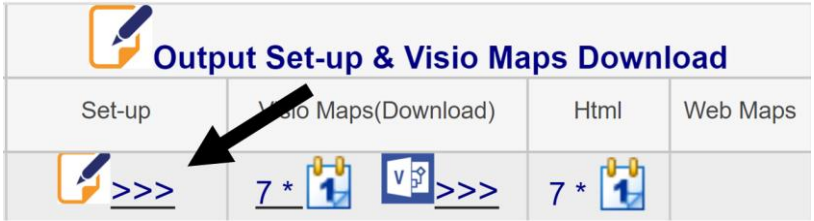
To set up Visio downloads make sure that a copy of Visio is installed on the device that your network discoveries are performed. This is crucial as Codima Toolbox uses the Microsoft Visio application to produce your maps.

Note: You do not have to setup Visio export settings for maps to be exportable, Layer 2 Topology/Tree diagrams are created by default and stored in Toolbox. By changing the export settings, you can choose the map layouts that suit your needs best.

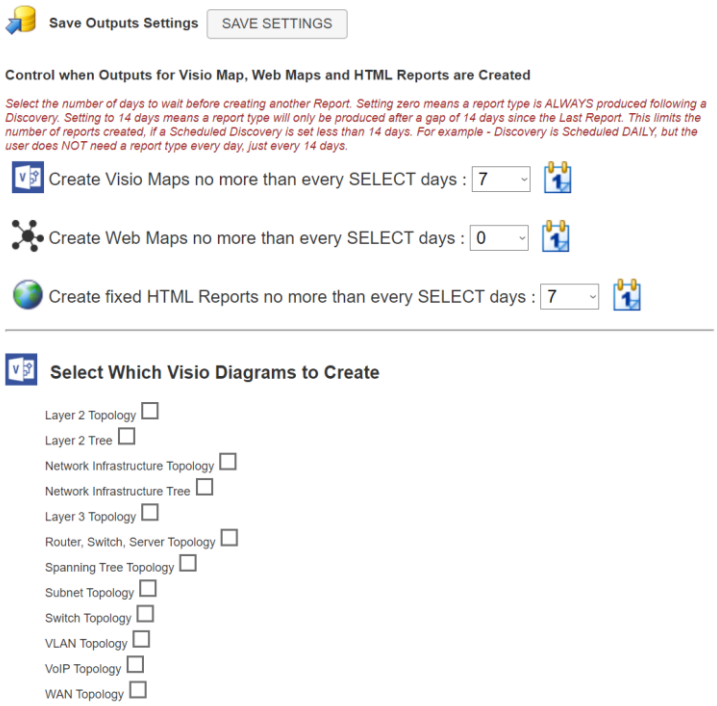
1. Navigate to the **Discover Network** tab



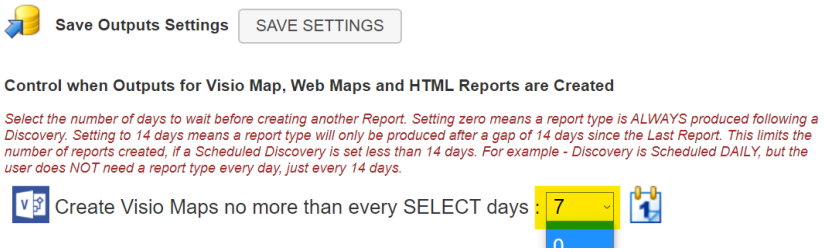
2. Click on the link in the **Set-up** column under the heading **Output Set-up & Visio Maps Download**.



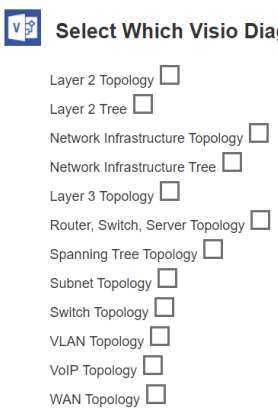
3. A window will appear with options relating to the Visio export feature.



4. The option marked below in yellow allows you to select a number of days that toolbox will wait before allowing you to download a Visio Map. This is used to limit the output frequency of Visio maps, as creating large Visio maps can take a long time, and doing so for each discovery is not always necessary.

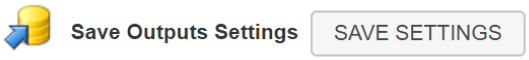


5. Under the Heading **Select Which Visio Diagrams to Create** you may choose what Network Map views you would like Visio to display, by ticking the box next to them. Below you will find an explanation of what each map layout displays.



a. **Layer 2 Topology** – Shows all devices the Network Discovery found in a topology format.
b. **Layer 2 Tree** – Shows all devices the Network Discovery found in a tree format.
c. **Network Infrastructure Topology** - includes all devices that provide services to customers on the network.
d. **Network Infrastructure Tree** - includes all devices that provide services to customers on the network.
e. **Layer 3 Topology** - includes all devices that have a routing table. i.e., they have an entry in the databases layer 3 topology table populated by the Codima Discovery Engine.
f. **Router, Switch, Server Topology –** Displays all routers, switches, and servers on your network.
g. **Spanning Tree Topology –** Displays you Network as a spanning tree.
h. **Subnet Topology** - shows all Subnet edge devices (i.e., route between Subnets) and Subnet Clouds.
i. **Switch Topology** – Shows all switches on your network.
j. **VLAN Topology** – Displays the Virtual Local Area Network Topology.
k. **VoIP Topology** - Shows all SIP Devices and important Network Infrastructure devices like Routers, Switches and Wireless access points.
l. **WAN Topology –** Shows the Wide Area Network Topology

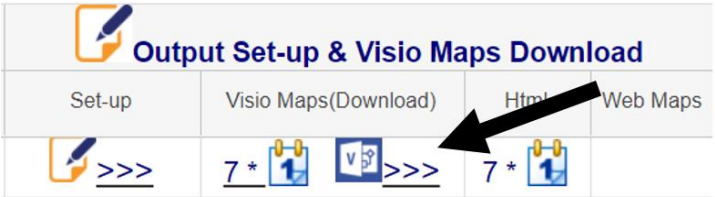
6. Make sure to click **Save Settings** in order to keep all the changes made.



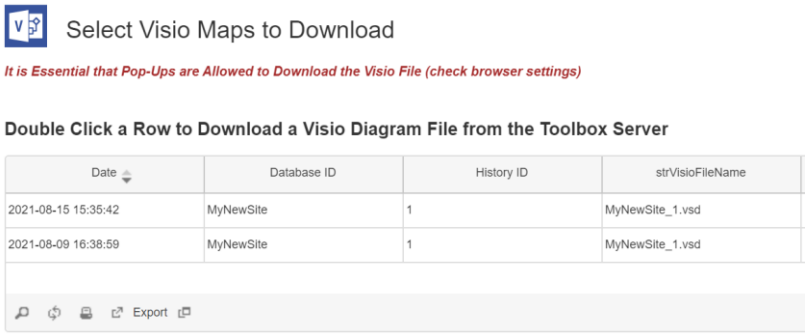
Viewing Visio Diagrams

Viewing Visio Diagrams can be done by anyone with access to your Codima Toolbox web interface. Keep in mind that in order to edit Visio diagrams you must have a copy of Microsoft Visio installed on your computer. If you do not have a copy of Microsoft Visio then you may use the free Visio Viewer that Microsoft offers, you can download the latest version here: https://www.microsoft.com/en-us/download/details.aspx?id=51188

1. To get access to a Visio map you must first have completed a Network Discovery. Then open the **Discover Network** tab, In the Main Grid at the bottom of the GUI, click on the **Visio Maps(Download)** link (Marked below with the arrow)



2. A grid will appear, double click the Discovery view you want to see as a Visio Diagram.



3. A download will start via the standard Download Pop-up for your browser. Visio will open if it is installed showing the Map. Typically, if there is no Visio installed then you will be prompted to install/launch the Visio Web Viewer. The Visio Web Viewer will open the map in Internet Explorer with ActiveX enabled.

ALERTS & TICKETING Feature

Alerts and Ticketing is a from the ground up, Integrated system (not a bolted-on package with a different GUI). It pulls together Alerts from Toolbox Monitoring and External Alerts such as Syslog, and then Classifies and Presents them throughout the system including in Toolbox Live Maps (including Probes).

Tickets can be generated Automatically or added Manually and sent to general or specialised Teams. The system automatically Tracks and chases up Tickets by talking to engineer and supervisor pools, using an elegant but world class setup. A diagram illustrates Polling operation, see next page.

What Alert System does

The system is designed to Analyse and Classify Alerts and work with other (SIEM) Alert Management Systems to Display Alerts in the Distributed Toolbox GUI especially in the Live Maps.

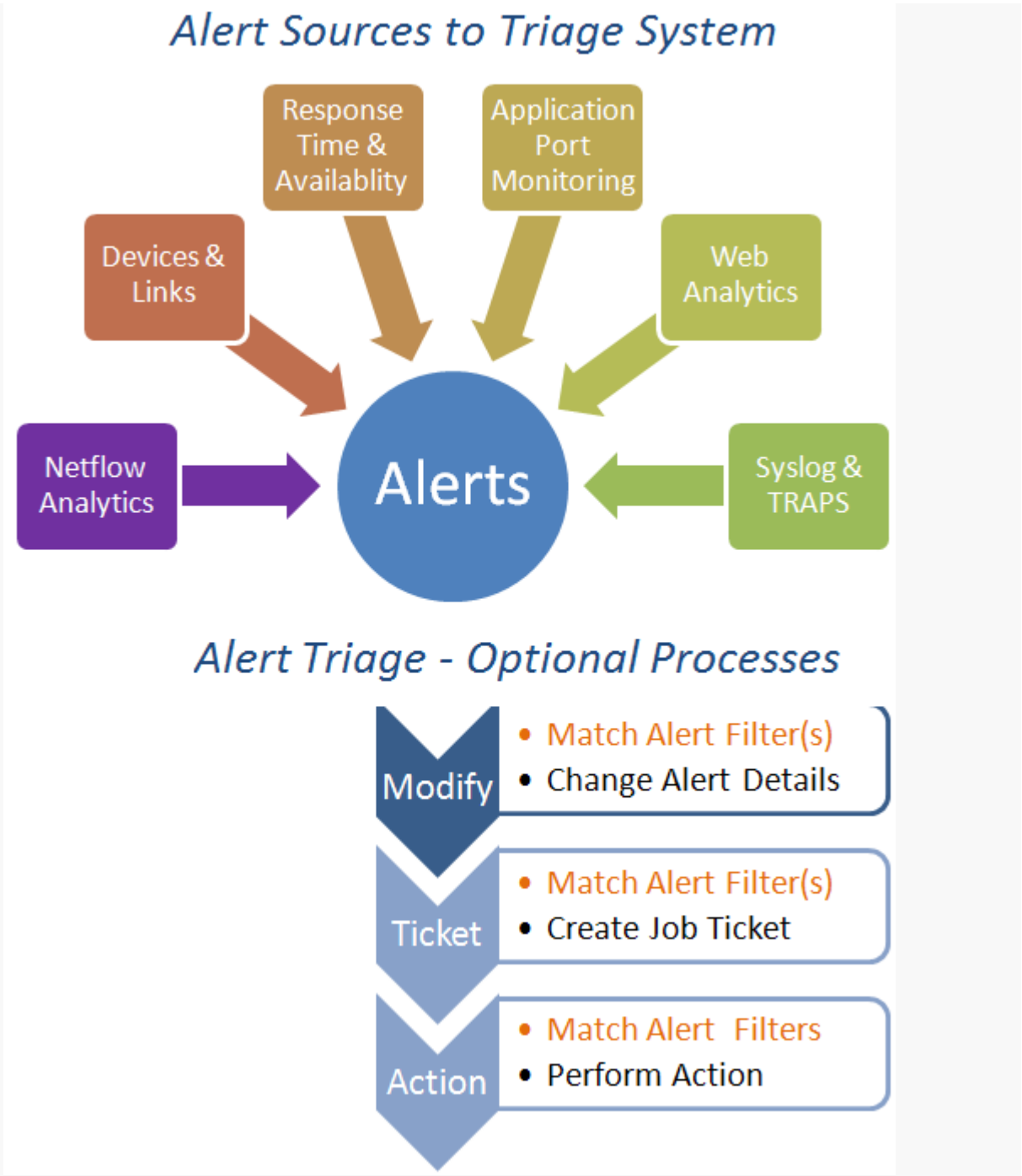
Alerts are created by Monitors within Toolbox and Externally by network devices as SNMP TRAPs and Syslog messages. These sources are combined in Alerts processing and viewed in the raw Alert form in the Review Alerts top panel. The Alerts are broken down into many categories (user programmable) and displayed in Standard and (optionally) in User Created Dashboards.

Alerts can be modified, collected together using Triage (kills alert floods) and can be used to create Job Tickets. First Alerts must be Classified with a Filter Matcher using the Alert Filter system, this saves time later as Alert Classifications (filters) can be applied in Map Animations too.

Incoming Alerts may be modified say to change priority or change the message to something easy to understand. They can then be re-transmitted as TRAPS or Syslog or just processed internally.

The Job Ticketing system works with Triage and is a powerful but simple Job Ticket Allocation system with 3 Ticket Priorities. A Pool of Engineers is created by the user to address specific functions such as Server maintenance or geographical areas. A single interface specifies actions per Ticket Priority including a full set of Reports to Track Engineers and Ticket Progress.

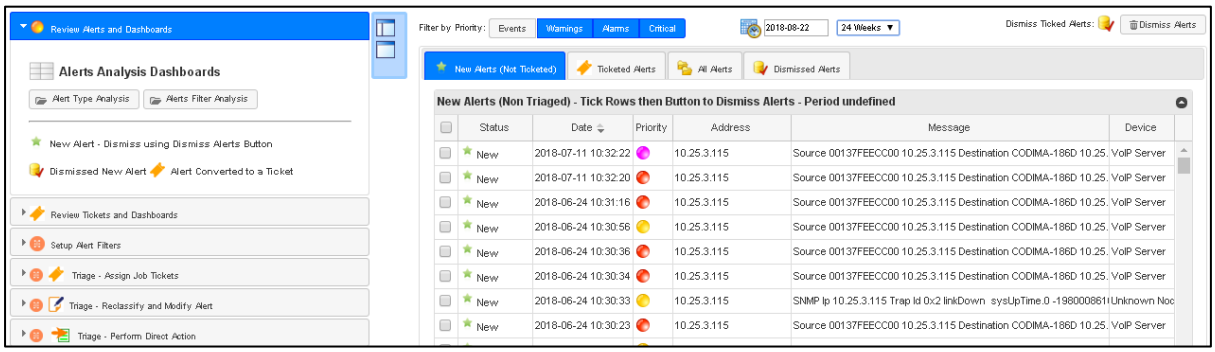
Alert Sources Diagram



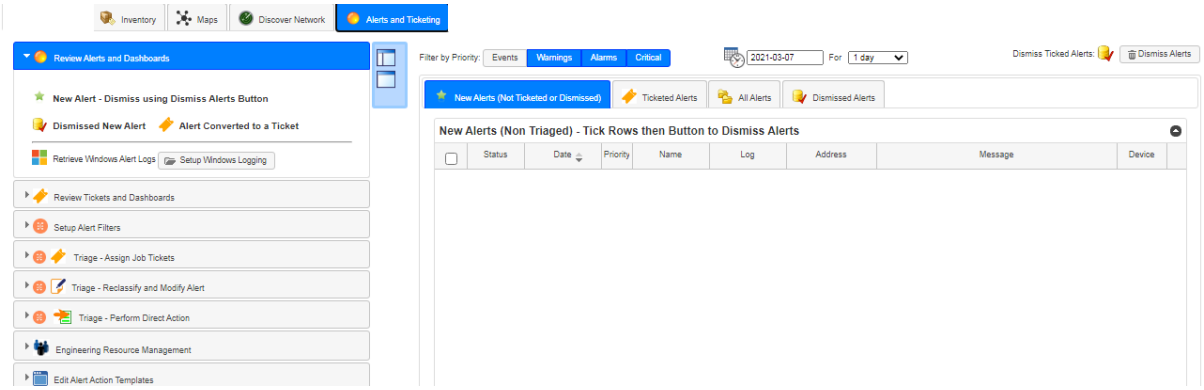
Alert and Ticketing Overview Display

A quick dismiss Alerts mechanism can be used if the full Alerts Triage and Ticketing system is not required.

An example of the Alerts GUI with a list of alerts below:



New Alerts (Non Triaged) - Tick Rows then Button to Dismiss Alerts, see below:



Simple Alerts Dismiss or the Full Triage System?

Alert Operation

Processing Incoming New Alerts can be

1) ticked in the New Alerts display to Dismiss them

or 2) be intelligently processed by the Alert Triage System.

1) Simple New Alerts Dismissal Process

- **+ It is simple to use.**
- + No setup required.
- - All Alerts have to be manually dismissed.
- - Cannot create tickets automatically.
- - Cannot automatically suppress alert floods.

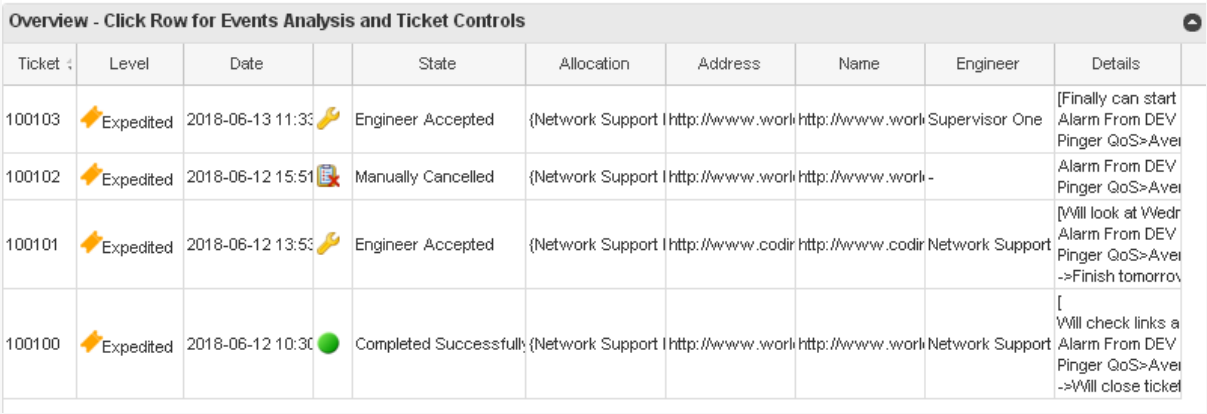
2) Triage New Alerts Process

- + Automatically suppresses alert floods by converting them to a ticket (the Alerts are linked to the Ticket for later drill down).
- + Creates Tickets to allocate engineer resources and track fix processing.
- + Extensive reports to analyse alerts based on Triage Classification.
- - Requires setup of engineer's pool, email, Alert Tickets and Triage Rules.

Ticketing Full Status Tracking

This is a very major upgrade that allows full tracking and also interaction with both Engineers and tickets – see except from Help System below: -

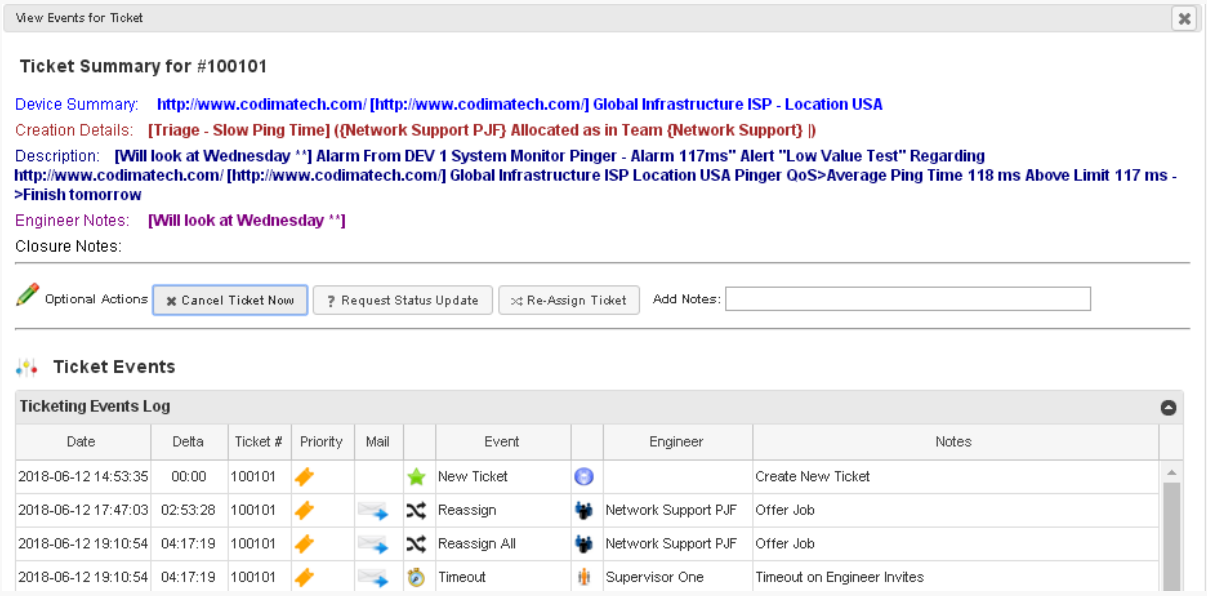
The right-side Window contains the Ticket Summary Grid which gives a live update of Ticket Status: -



Overview - Click Row for Events Analysis and Ticket Controls

Ticket	Level	Date		State	Allocation	Address	Name	Engineer	Details
100103	Expedited	2018-06-13 11:33		Engineer Accepted	{Network Support I	http://www.worl	http://www.worl	Supervisor One	[Finally can start Alarm From DEV Pinger QoS>Aver
100102	Expedited	2018-06-12 15:51		Manually Cancelled	{Network Support I	http://www.worl	http://www.worl	-	Alarm From DEV Pinger QoS>Aver
100101	Expedited	2018-06-12 13:53		Engineer Accepted	{Network Support I	http://www.codir	http://www.codir	Network Support	[Will look at Wedr Alarm From DEV Pinger QoS>Aver ->Finish tomorrov
100100	Expedited	2018-06-12 10:30		Completed Successfull	{Network Support I	http://www.worl	http://www.worl	Network Support	[Will check links a Alarm From DEV Pinger QoS>Aver ->Will close ticket

On clicking on a Ticket Row the Ticket Summary appears as below: -



View Events for Ticket

Ticket Summary for #100101

Device Summary: http://www.codimatech.com/ [http://www.codimatech.com/] Global Infrastructure ISP - Location USA

Creation Details: [Triage - Slow Ping Time] ({Network Support PJF} Allocated as in Team {Network Support})

Description: [Will look at Wednesday **] Alarm From DEV 1 System Monitor Pinger - Alarm 117ms" Alert "Low Value Test" Regarding http://www.codimatech.com/ [http://www.codimatech.com/] Global Infrastructure ISP Location USA Pinger QoS>Average Ping Time 118 ms Above Limit 117 ms ->Finish tomorrow

Engineer Notes: [Will look at Wednesday **]

Closure Notes:

Optional Actions | Cancel Ticket Now | ? Request Status Update | Re-Assign Ticket | Add Notes:

Ticket Events

Ticketing Events Log

Date	Delta	Ticket #	Priority	Mail		Event		Engineer	Notes
2018-06-12 14:53:35	00:00	100101				New Ticket			Create New Ticket
2018-06-12 17:47:03	02:53:28	100101				Reassign		Network Support PJF	Offer Job
2018-06-12 19:10:54	04:17:19	100101				Reassign All		Network Support PJF	Offer Job
2018-06-12 19:10:54	04:17:19	100101				Timeout		Supervisor One	Timeout on Engineer Invites

Here it is possible to Cancel the Ticket immediately, Request an Update from the assigned engineer, or Re-Assign the Ticket to another Engineer.

How to Use Alerts and Ticketing

Alerts of all kinds are initially displayed in the Alerts Tab top panel grid.

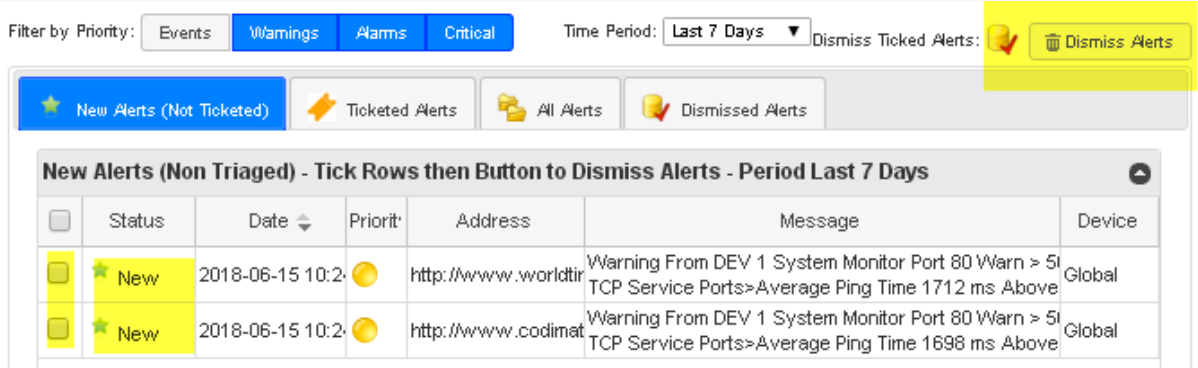
They can be simply Dismissed or use the automated dismissal using the Triage System by creating a Job Ticket.

However, if there is a **Triage Rule** that matches any incoming Alert then it will be automatically acknowledged and be removed from the top panel grid. The matching Alerts are retained in the system and attached to the matching Triage Rule which are viewable in Triage Analysis Grid Reports.

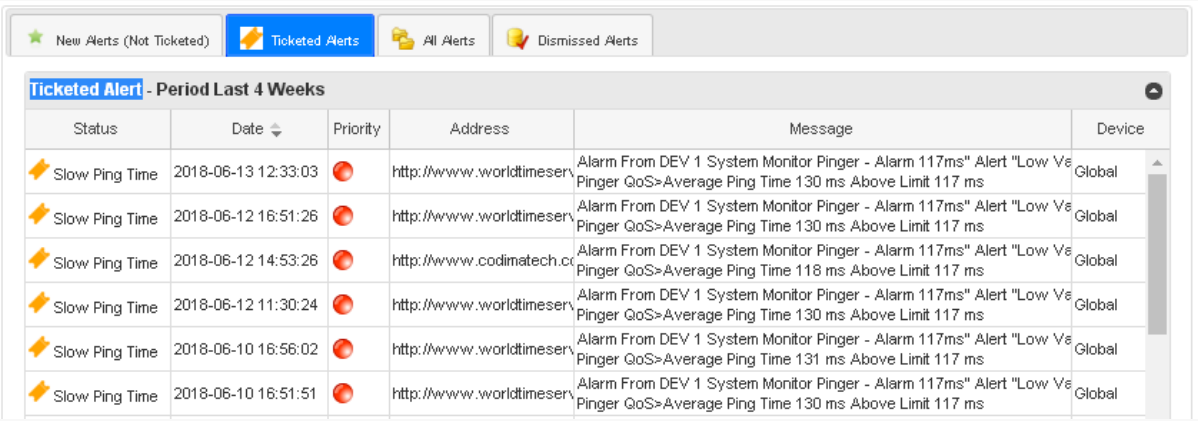
Key to using the Triage System is to setup **Alert Filter** matcher(s) as these are used to Trigger Triage Rule Matches.

Using the Alert Tabbed Grid

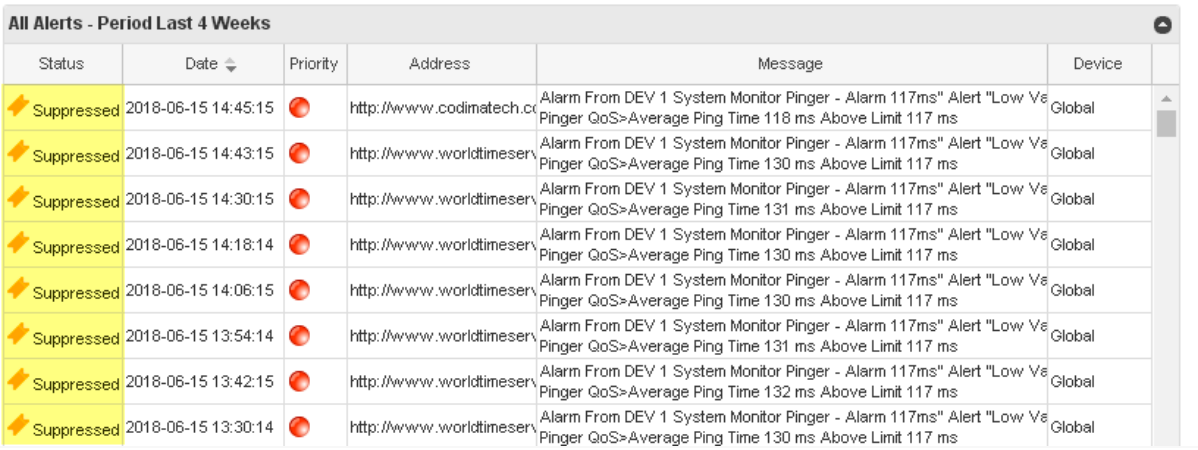
The Grid shows New Alerts: that can be Dismissed as explained under **Using Alerts and Simple Alert Dismissal**.



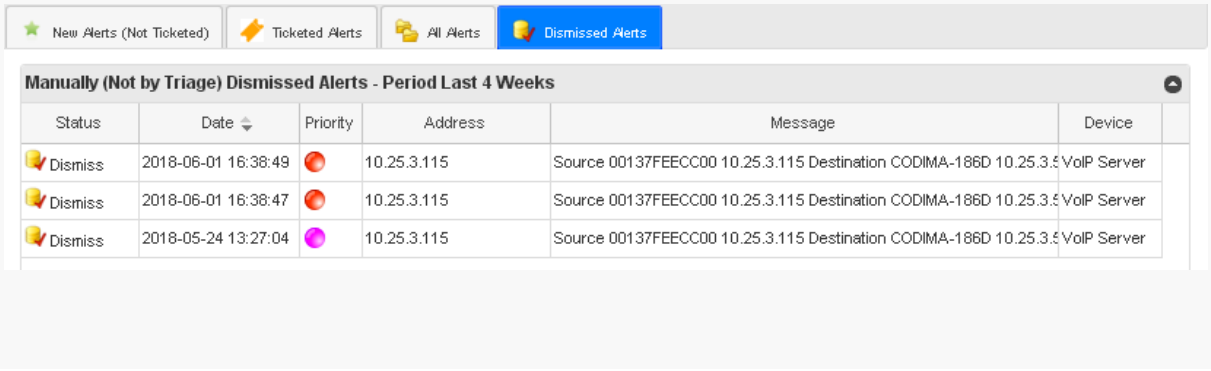
Ticketed Alerts are Alerts that have been Successfully Triaged under the Triage Rule listed in the Status Column - in this case Alerts have been Ticketed using the **Slow Ping Time** Triage rule.



The **All Alerts** tab shows all Alerts including Manually Dismissed and Triage Dismissed Alerts. The list can be searched/filtered and sorted using the standard Grid features. The Suppressed Alerts refer to Alerts being auto suppressed by the Triage System.



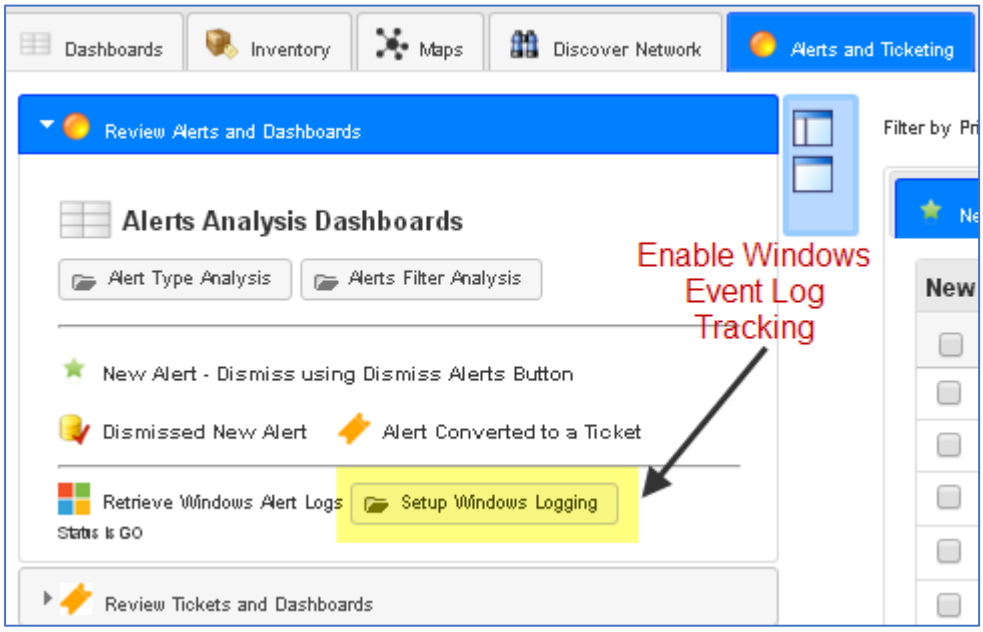
The **Dismissed Alerts** tab can be used to view Alerts that have been Manually Dismissed.



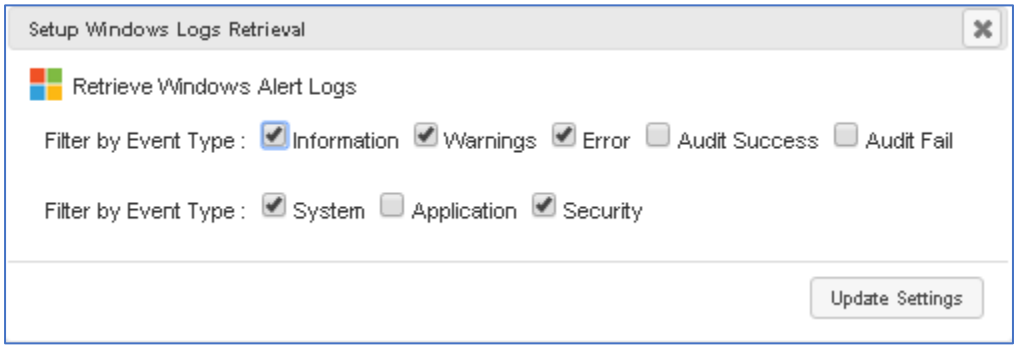
Retrieving Windows Alerts

Toolbox can talk to Windows boxes using WMI to collect Events from their Windows NT Logs and then convert them to Toolbox Alert Format. They are then processed as normal in Toolbox that means they can use **Alert Filters** to modify the alerts, create Tickets or send out as SYSLOG or SNMP Traps for example.

The Windows Alert processing is setup by clicking on the Setup Windows Logging button as in the picture below:

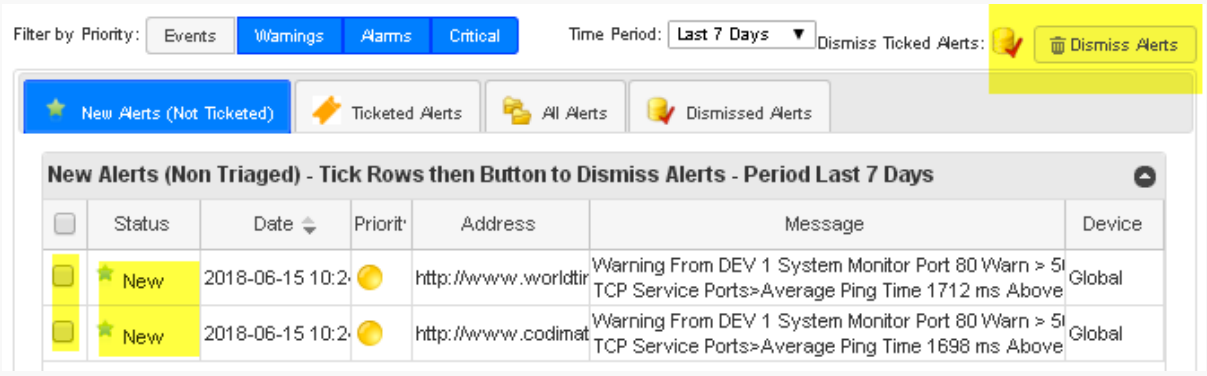


The following Dialog appears. Select which Windows Logs and what Priorities of Alerts you want to retrieve from the Windows System.

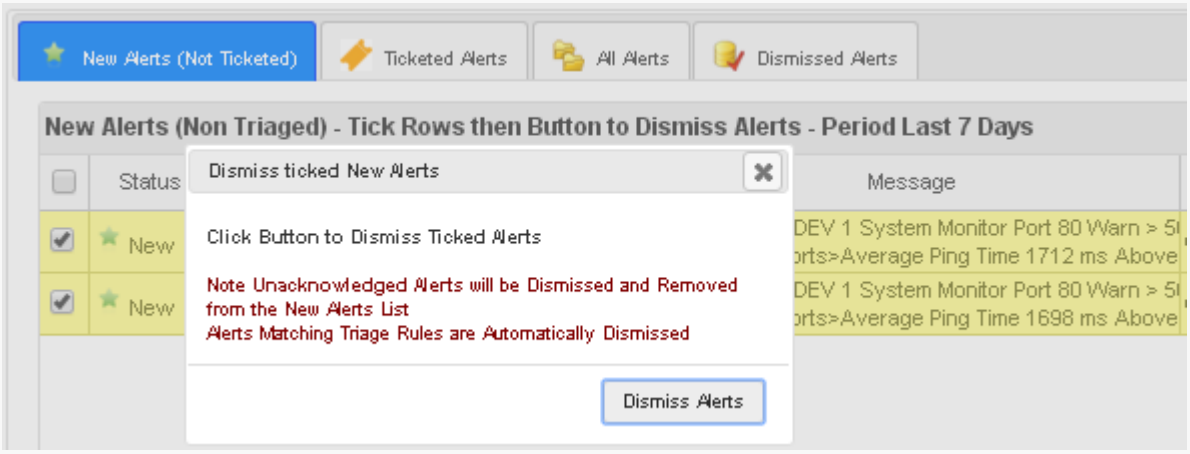


Using Alerts and Simple Alert Dismissal

This Panel shows the Alerts under several classifications that show what is happening both for the Simple Dismiss Alerts system or the Triage System Results.



Using the Simple Manual Alerts Dismiss system click on the tick boxes on the Grid Rows to select the Alerts, then click on the **Dismiss Alerts** button. A popup will appear, as below:-



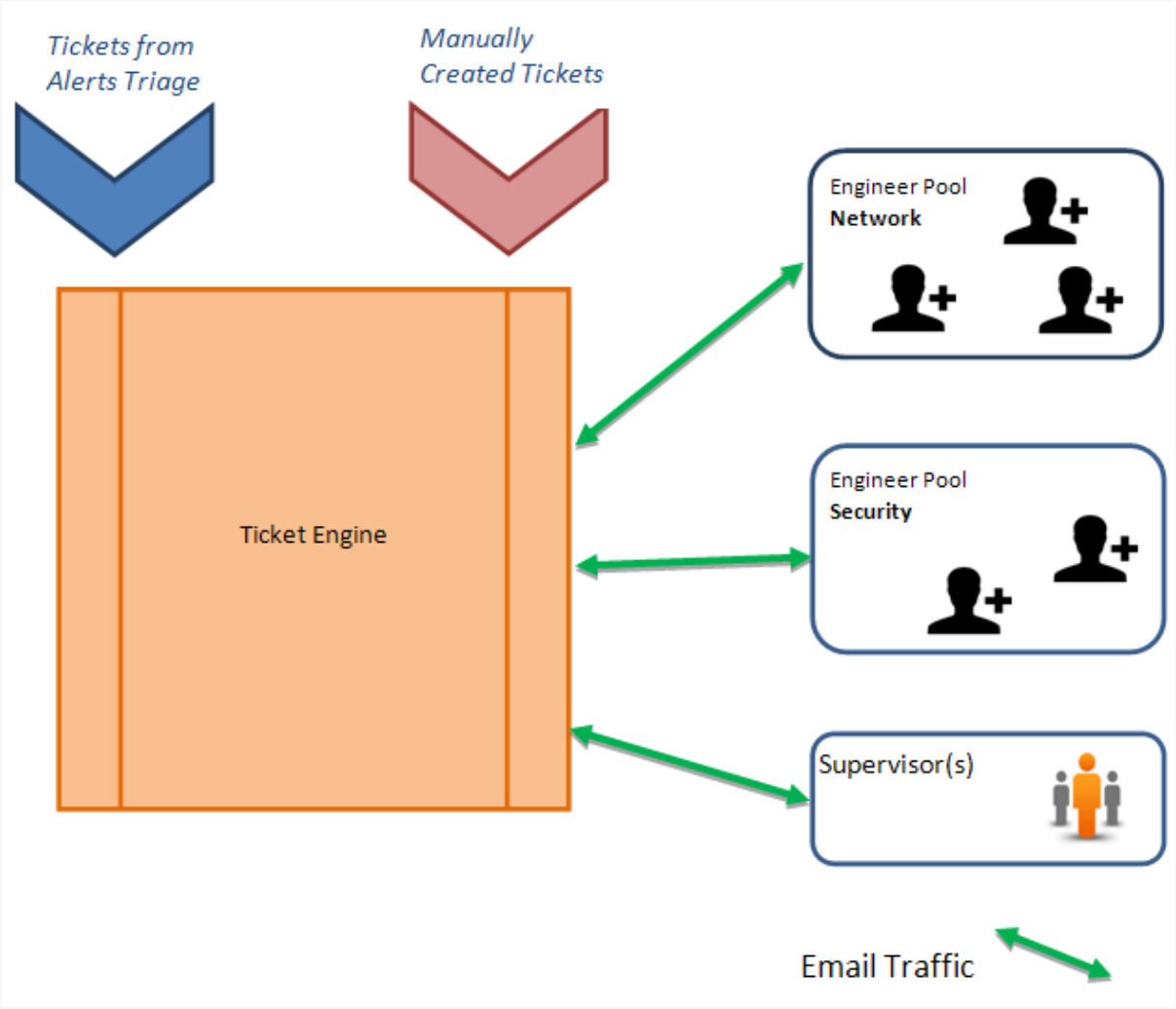
Clicking on the **Dismiss Alerts** button in the dialog will move the Alert to the Dismissed Alerts tab and they will no longer be Active in Toolbox e.g. in the Maps or Diagnose.

A Diagram of the Ticketing Process

Tickets can be Created Automatically by the Triage Engine or Added Manually in the Toolbox Web GUI.

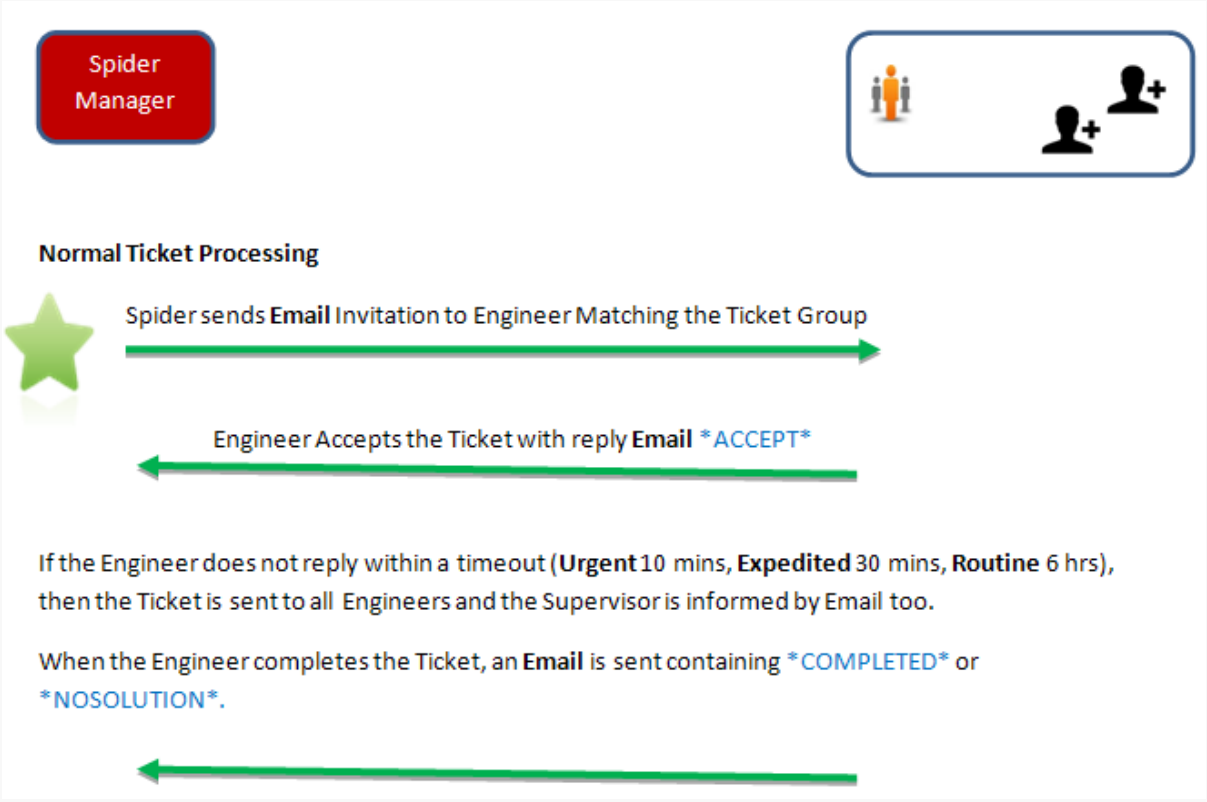
Depending on the Group Assigned by the Triage Rule or the Manual Ticket Dialogue box, then the Ticket is assigned to a particular Group of Engineers. New Tickets are assigned to Engineers by Email.

The Supervisor, if Setup, is kept informed of Ticket Assignments and Failure to Respond by Email.



Communicating with Engineers by Email

Below is the Action of the Toolbox Ticketing System on Creation of a New Ticket. First the System looks for an Engineer that is Free and in the same Engineer Group as specified in the Ticket.



The eMail *COMMAND*s between Toolbox <-> Engineer

A Ticket is assigned to an Engineer in a format as below:

<<<You have been assigned this Ticket - Reply *ACCEPT* or *DECLINE*

? for command help>>>

Add Comments after the REPLY CODE (*....*) terminated by **

Priority Expedited - Ticket Reference #100103,

Created 2018-06-13 11:33:16, As Slow Ping Time

Device - http://www.worldtimeserver.com/ [http://www.worldtimeserver.com/] Global web site no vendor - Location USA

Site - Local

(Ticket Assignment Summary - Alarm From DEV 1 System Monitor Pinger - Alarm 117ms" Alert "Low Value Test" Regarding http://www.worldtimeserver.com/ [http://www.worldtimeserver.com/] Global web site no vendor Location USA

Pinger QoS>Average Ping Time 130 ms Above Limit 117 ms)

The Engineer is invited to Accept the ticket by replying with *ACCEPT* usually followed by a Comment such as "will investigate now**". The ** is used to terminate the Engineer comment (if it is omitted the rest of the email will be logged by the system). On the Toolbox System reading the reply, it will send out a confirmation to the Engineer and the system will update status on the Ticket and the Engineer.

"*ACCEPT*" I will accept responsibility for this ticket. Ticket now registered to this Engineer.

"*DECLINE*" I cannot accept this ticket.
"*REASSIGN*" Although I accepted this Ticket I now need someone else to deal with it. The Ticket is advertised to all Engineers in Group

"*UPDATE*" Here is a Status Update, Status Updates may be Requested by the Supervisor too.

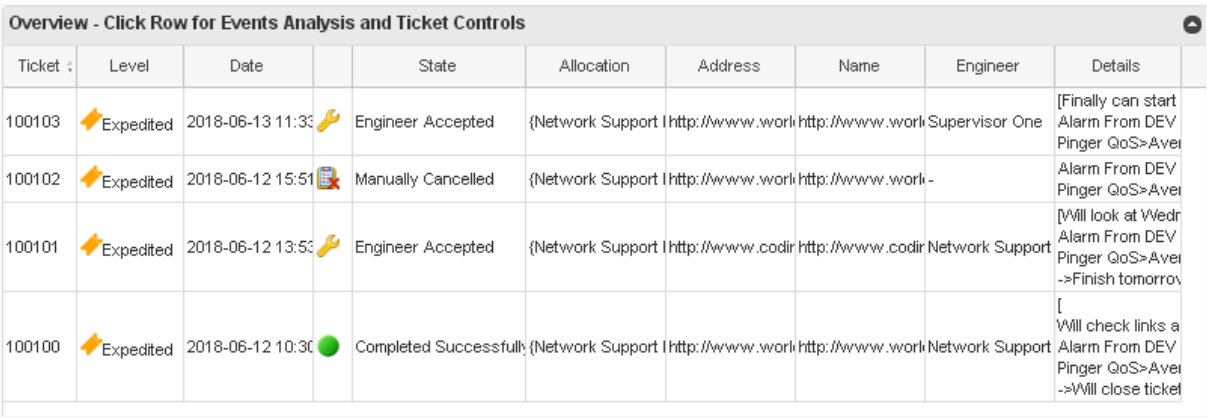
"*COMPLETED*" I have successfully completed the Ticket. The Ticket is now marked as Closed Successfully.
"*NOSOLUTION*" I have not been able to fix the problem and have marked as closed Unsuccessfully.

These are Status Message sent by the Engineer to Update the Supervisor - they do not impact existing Ticket Assignments.
"*BUSY*" I cannot Accept more Tickets, until updated by an AVAILABLE message to the Toolbox System.
"*AVAILABLE*" I can now accept new Tickets
"*SICK*" - reporting in Ill
"*HOLIDAY*", - reporting in On Holiday

"*HELP*" or "*?*" - Request for a full list of Commands and their meaning.

Using the Ticket Summary Dialog

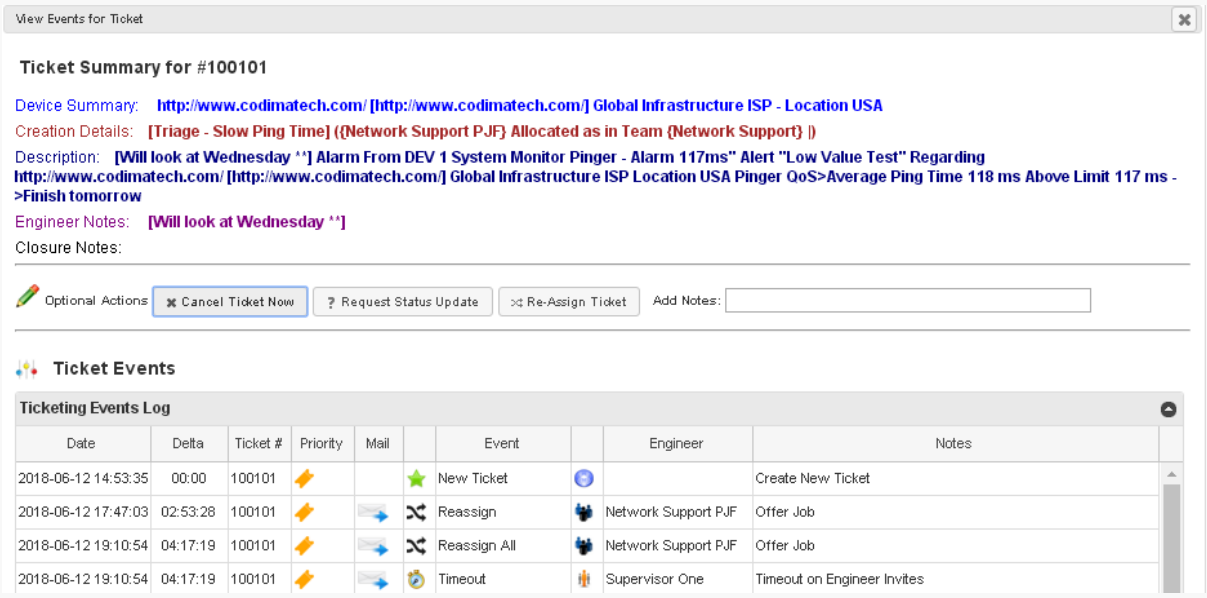
The righthand side Window contains the Ticket Summary Grid which give a live update of Ticket Status:



Overview - Click Row for Events Analysis and Ticket Controls

Ticket	Level	Date		State	Allocation	Address	Name	Engineer	Details
100103	Expedited	2018-06-13 11:33		Engineer Accepted	{Network Support I	http://www.work	http://www.work	Supervisor One	[Finally can start Alarm From DEV Pinger QoS>Aver
100102	Expedited	2018-06-12 15:51		Manually Cancelled	{Network Support I	http://www.work	http://www.work	-	Alarm From DEV Pinger QoS>Aver
100101	Expedited	2018-06-12 13:53		Engineer Accepted	{Network Support I	http://www.codir	http://www.codir	Network Support	[Will look at Wedr Alarm From DEV Pinger QoS>Aver ->Finish tomorrov
100100	Expedited	2018-06-12 10:30		Completed Successfull	{Network Support I	http://www.work	http://www.work	Network Support	[Will check links a Alarm From DEV Pinger QoS>Aver ->Will close ticket

On clicking on a Ticket Row the Ticket Summary appears as below:



View Events for Ticket

Ticket Summary for #100101

Device Summary: http://www.codimatech.com/ [http://www.codimatech.com/] Global Infrastructure ISP - Location USA

Creation Details: [Triage - Slow Ping Time] ({Network Support PJF} Allocated as in Team {Network Support})

Description: [Will look at Wednesday **] Alarm From DEV 1 System Monitor Pinger - Alarm 117ms" Alert "Low Value Test" Regarding http://www.codimatech.com/ [http://www.codimatech.com/] Global Infrastructure ISP Location USA Pinger QoS>Average Ping Time 118 ms Above Limit 117 ms ->Finish tomorrow

Engineer Notes: [Will look at Wednesday **]

Closure Notes:

Optional Actions | Cancel Ticket Now | ? Request Status Update | Re-Assign Ticket | Add Notes:

Ticket Events

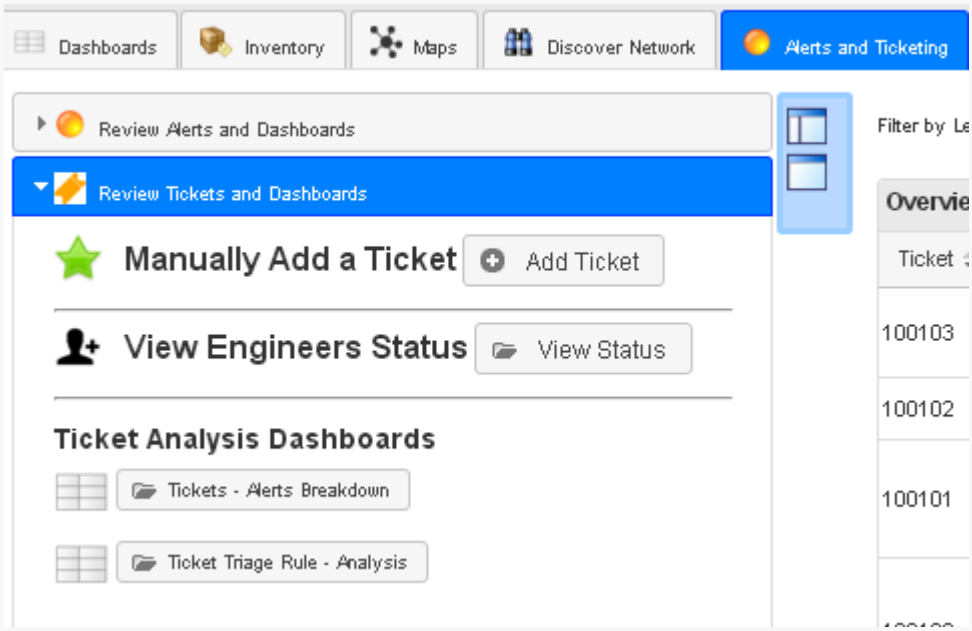
Ticketing Events Log

Date	Delta	Ticket #	Priority	Mail		Event		Engineer	Notes
2018-06-12 14:53:35	00:00	100101				New Ticket			Create New Ticket
2018-06-12 17:47:03	02:53:28	100101				Reassign		Network Support PJF	Offer Job
2018-06-12 19:10:54	04:17:19	100101				Reassign All		Network Support PJF	Offer Job
2018-06-12 19:10:54	04:17:19	100101				Timeout		Supervisor One	Timeout on Engineer Invites

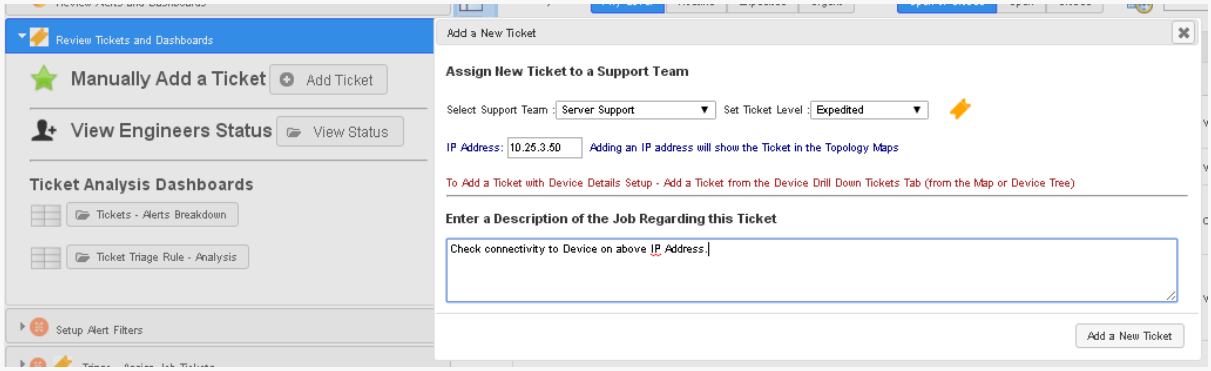
Here it is possible to Cancel the Ticket immediately, Request an Update from the assigned engineer, or Re-Assign the Ticket to another Engineer.

The Ticketing Panel Description

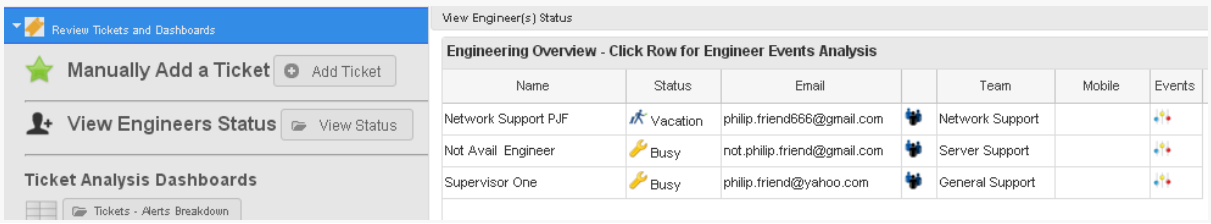
This Panel gives access to several Ticketing features:



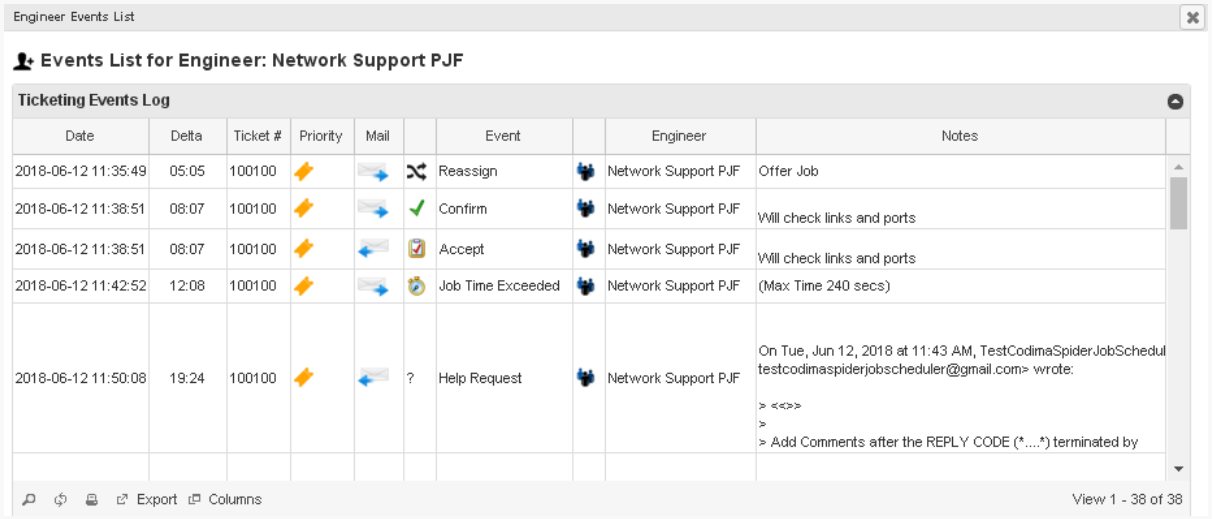
A New Ticket can be added directly to the Ticketing System by the Operator without going through the Alerts Triage System by clicking on the **Add Ticket** Button, as below:



The Status of all Engineers regarding Ticket Progress and a further drill down to individual Ticket Events is available, as below:



Clicking on a Grid Row will bring up an analysis of events for that Engineer as below:



Engineer Events List

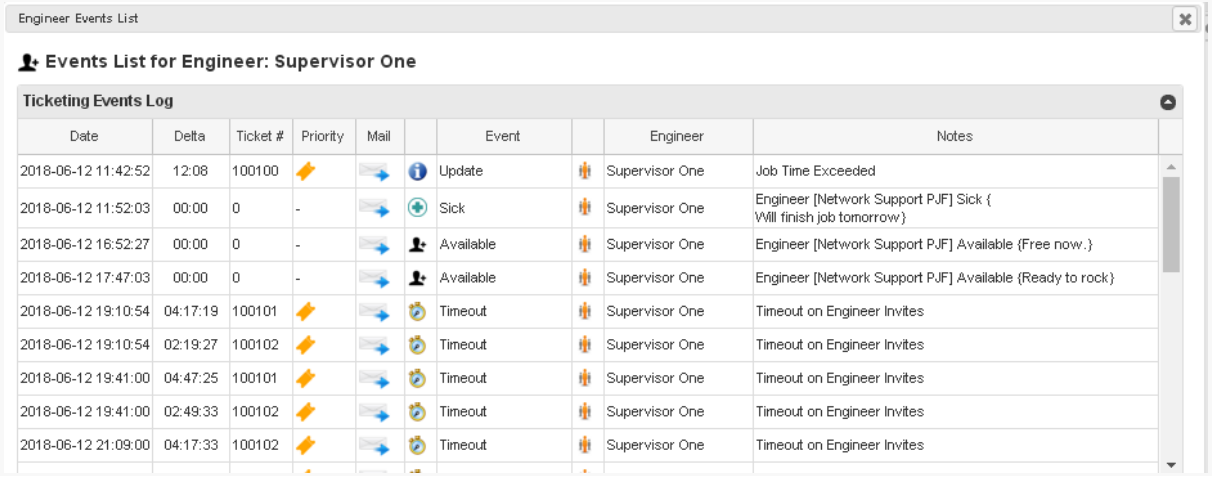
Events List for Engineer: Network Support PJF

Ticketing Events Log

Date	Delta	Ticket #	Priority	Mail		Event		Engineer	Notes
2018-06-12 11:35:49	05:05	100100				Reassign		Network Support PJF	Offer Job
2018-06-12 11:38:51	08:07	100100				Confirm		Network Support PJF	Will check links and ports
2018-06-12 11:38:51	08:07	100100				Accept		Network Support PJF	Will check links and ports
2018-06-12 11:42:52	12:08	100100				Job Time Exceeded		Network Support PJF	(Max Time 240 secs)
2018-06-12 11:50:08	19:24	100100			?	Help Request		Network Support PJF	On Tue, Jun 12, 2018 at 11:43 AM, TestCodimaSpiderJobSchedul testcodimaspiderjobscheduler@gmail.com> wrote: > <<>> > > Add Comments after the REPLY CODE (*....*) terminated by

Export Columns View 1 - 38 of 38

Clicking on a Grid Row for a Supervisor, also brings up an Event List for the Supervisor:



Engineer Events List

Events List for Engineer: Supervisor One

Ticketing Events Log

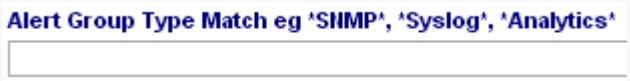
Date	Delta	Ticket #	Priority	Mail		Event		Engineer	Notes
2018-06-12 11:42:52	12:08	100100				Update		Supervisor One	Job Time Exceeded
2018-06-12 11:52:03	00:00	0	-			Sick		Supervisor One	Engineer [Network Support PJF] Sick { Will finish job tomorrow }
2018-06-12 16:52:27	00:00	0	-			Available		Supervisor One	Engineer [Network Support PJF] Available {Free now.}
2018-06-12 17:47:03	00:00	0	-			Available		Supervisor One	Engineer [Network Support PJF] Available {Ready to rock}
2018-06-12 19:10:54	04:17:19	100101				Timeout		Supervisor One	Timeout on Engineer Invites
2018-06-12 19:10:54	02:19:27	100102				Timeout		Supervisor One	Timeout on Engineer Invites
2018-06-12 19:41:00	04:47:25	100101				Timeout		Supervisor One	Timeout on Engineer Invites
2018-06-12 19:41:00	02:49:33	100102				Timeout		Supervisor One	Timeout on Engineer Invites
2018-06-12 21:09:00	04:17:33	100102				Timeout		Supervisor One	Timeout on Engineer Invites

Using Alert Filters

This panel allows the user to define very broadly based Alert Filters like simple Alert Priority or very detailed such as a complex Alert Text match with multiple match components.

They are used primarily in Triage of Alerts but can also be used to Filter Alert Animations in the Topology Maps of the Toolbox product.

Toolbox Alert Groups

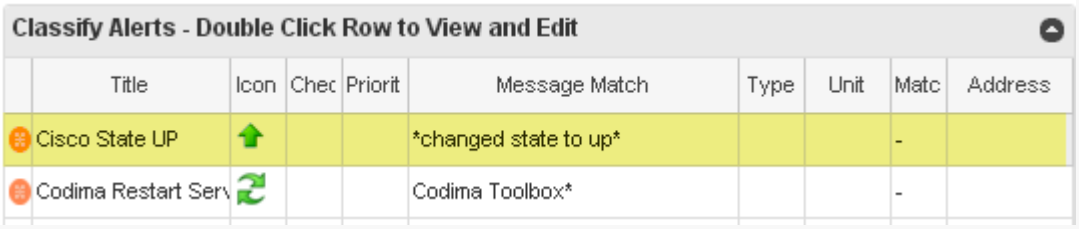


This matcher matches Toolbox internal alert type Groups, it is added for completeness rather than a frontline feature. Groups can be seen in raw Alerts by switching on the Groups Grid Column to learn the Toolbox internal group names.

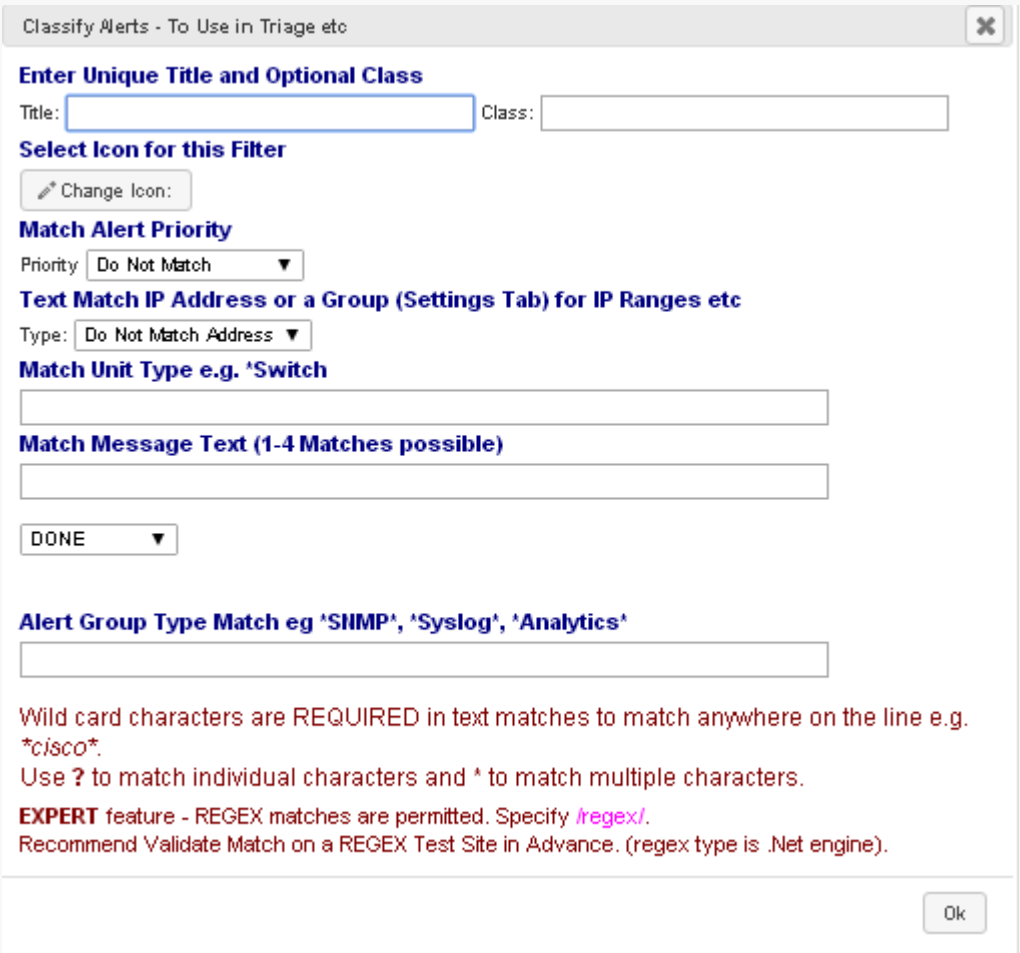
Setting up Alert Filters in Detail

To **Add a new Alert Filter,** simply click on the button highlighted in yellow below:

To **Edit an existing Alert Filter** double click on a Grid Row, as below:



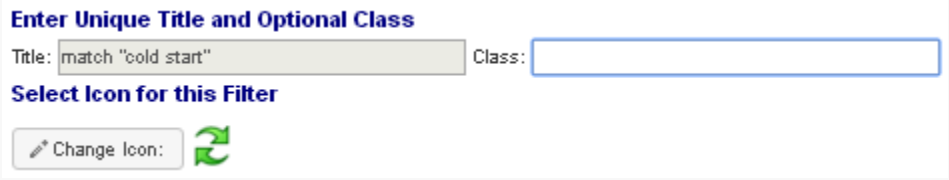
To add or modify an Alert Filter the Alert Filter Dialog pop-up is used, as below:



Although this pop-up has very many options, typically, only one or a few are actually required.

The various options are now described one by one.

Filter Title, Class and Icon

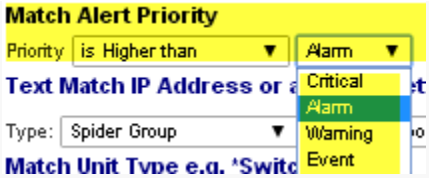


Key for the filter is to enter a **UNIQUE** title. It is important that the Name needs to say what the filter Matches.

An optional **Class** may also be added that is useful to categorise Filters like for example Security alert matching. Note: **Class** can be shown in the Alerts Grid by adding the Class Column by clicking on the Columns Icon at the bottom of the Grid.

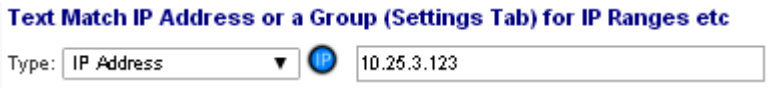
Additionally, an optional **Icon** may be added to the Filter Match. This is highly recommended to make Filters more graphical throughout the Toolbox System.

Match Alert Priority



The incoming Alert Priority can be matched by first selecting the Condition and then the Priority Level in two dropdown menus. Useful for matching high priority alerts probably combined with some Alert filter match property.

Match IP Address or a Toolbox Group



This can be used to match a whole IP Address or a fragment of an IP address like "10.26.", by selecting the IP Address **Type:** option.

By selecting a Group **Type:** option the filter will look for IP Addresses in the Specified Group IP Range(s). Note: Groups are setup under the Setting Tab->Groups Panel.

Match Unit/Device Type

This is used to match Device (Unit) types like **Switch**, **Router**, **Server** or other types. To match, say Layer 3 and also Layer 2 switches, match ***Switch** so the match begins with a wildcard * character (i.e. match **L3 Switch** and also **Switch**).

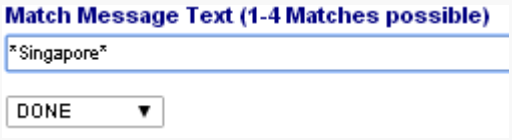
Match Message Text

This is probably the most important matcher as it matches the content of the message, like a **Syslog Message** content or an **SNMP Trap** content or **Toolbox Generated Alert**s like Threshold Breaches etc.

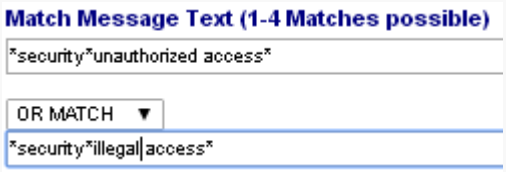
The matcher makes full use of Wildcards like * and _ - to wildcard multiple or single characters respectively.

The matcher can have from 1 up to 4 individual matcher terms that can be ANDed or ORed together.

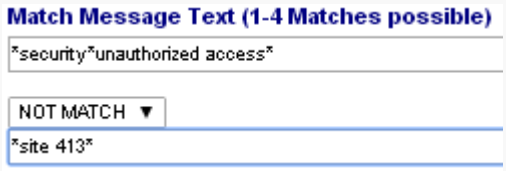
One Term



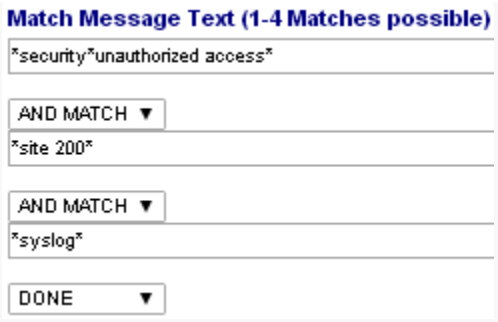
Two ORed Terms



Two Terms with a Not Match exclusion Term

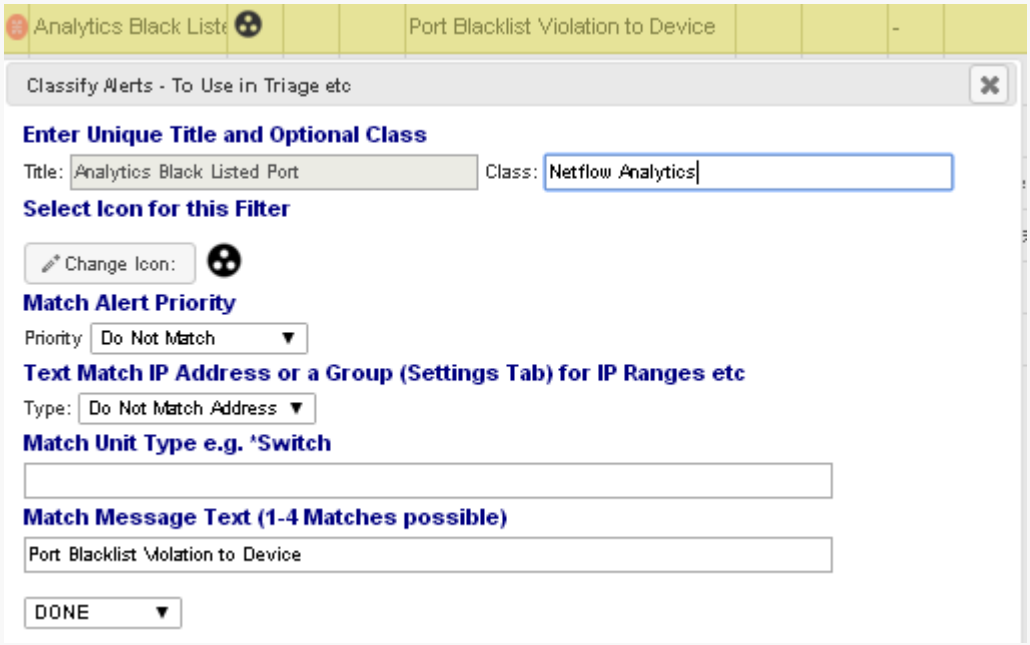


Three Terms ANDed match.



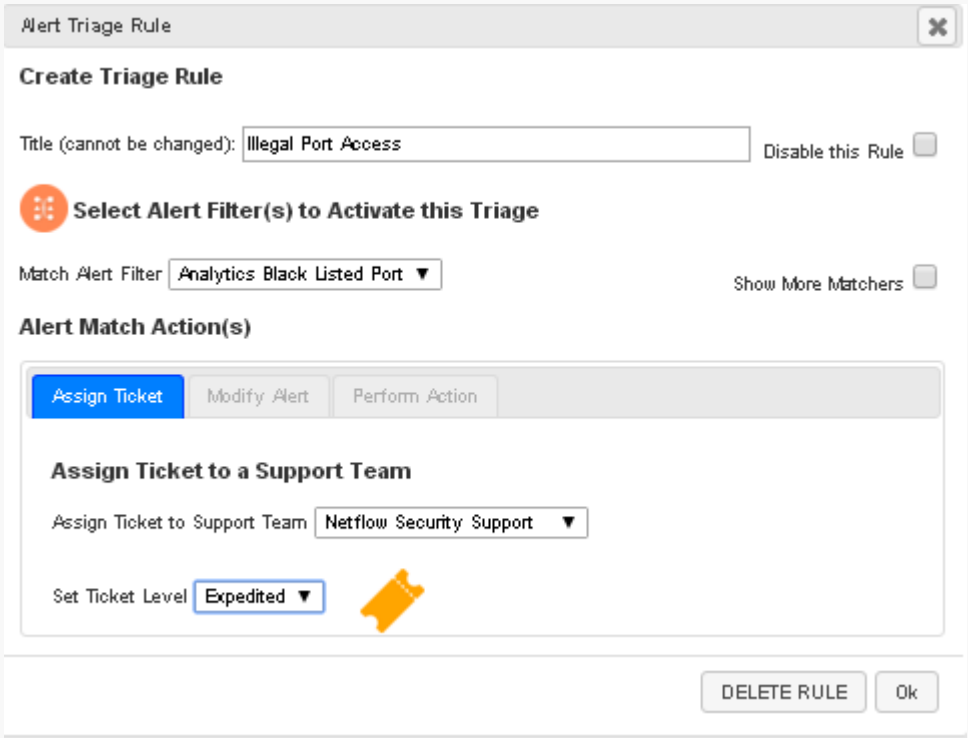
Using Triage to Job Ticket System

The triage system depends on Alert Filters, see below:



An Alert Filter has been created to Match Alerts coming from Toolbox Netflow Analytics, for example.

The Triage references the Filter as below to start a Triage Action - in this case to create a Job Ticket.



The **Title** is the Name of the Triage Rule which is set by the user and should describe the Triage Rule.

Absolutely key is the **Match Alert Filter**, which is a dropdown list of all the **Alert Filters** that are in the System, setup under the **Alert Filters** panel.

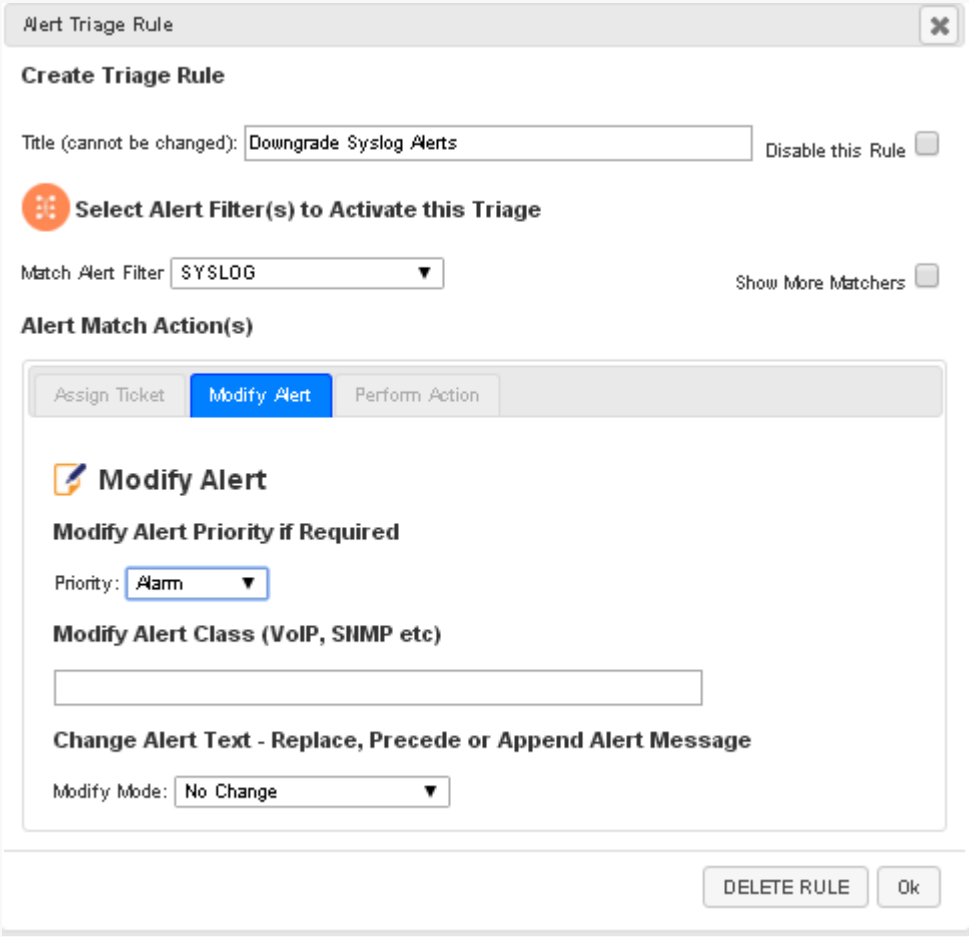
There can be several Alert filters which all can be associated with a Triage Rule and are processed by the Toolbox to create many Reports showing the drill downs of why the Triage was triggered. For instance, Alert Filters can be setup to Track Alerts for Pinger, TCP Port and Web Page Access which will all be associated with the Rule Trigger. Other Points of Failure such as intermediate Links and Devices can be Tracked with Alert Filters (e.g. based on SNMP or Pingers) such as dropped packets, slow response to add more information and analysis in the Triage Rule drill reports.

The **Match Actions** for this Job Ticket Triage Rule specify which **Support Team** will be Assigned the Ticket. There are several standard Teams setup by Toolbox, but the user can add as many Support Teams as required. The **Priority** drop down selects **Urgent**, **Expedited** or **Routine** which influences directly how the Tickets are processed when assigning and progressing Tickets. **Urgent** Tickets will be chased more aggressively than **Routine** Tickets by the Toolbox Job Tracking system

The Job Tickets are also shown in the Live Network Maps including from Remote Probes.

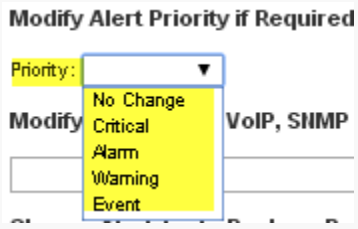
Using Triage to Modify Alerts

The Modify Alerts system works on individual Alerts that **Match** one or more **Alert Filters.**



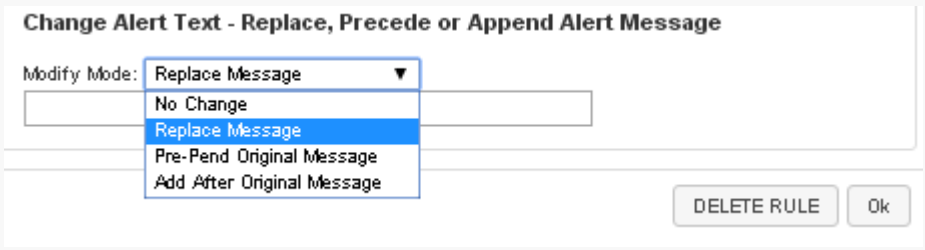
The Modify Alert rule should be given a Unique descriptive **Title**.

One or more **Alerts Filters** are selected to trigger this Modify type Triage Rule.



To optionally modify the Alert Priority, select a priority using the **Priority**: drop down control. This can be used to downgrade Alert priorities to reduce importance of matching Alerts, or alternatively, upgrade priorities on the specified Alert Filter matching Alerts.

The Alert Group (**Class**) can be changed if a better or alternative grouping is known, based on Alert Filter matching.

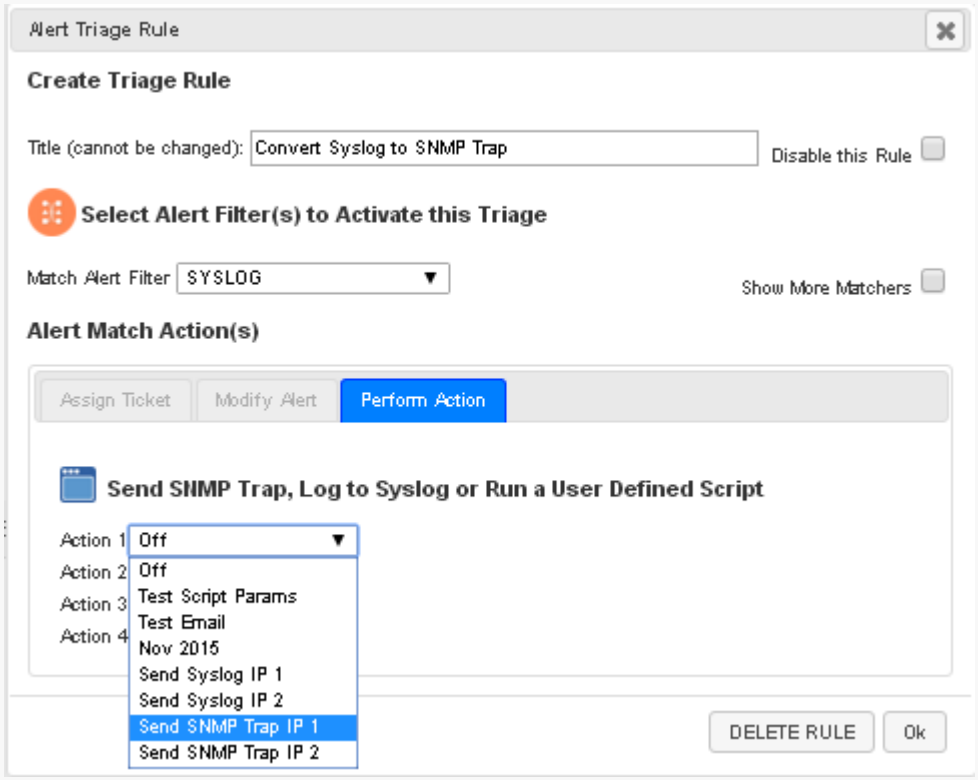


The Alert Text can be modified for matching Alerts to either Prepend Text, Replace Text or Append text to the Alert. Useful to explain cryptic Alerts or translate foreign language content to match the local site language.

Note: Alert Modification is done before any other Alert Processing is done.

Using Triage to Perform Direct Action

This Triage type allows a range of actions to be performed such as converting Alerts into different Alert types like SNMP, Email or Syslog. Additionally, it can Trigger Execution of predefined Server Scripts. It can also be used to **Copy** Traps and Syslog for example to forward to another destination like a special management station.



As with other Triage types the mechanism is driven by Matching a predefined Alert Filter.

Ticket Creation and Processing

Tickets are created by the Alerts and Triage system and optionally manually by the Toolbox User.

To process Tickets needs a list of Engineers and optionally Supervisor(s). When a new ticket is created, the system scans the list of Engineers looking for a free Engineer that Matches the Support Group of the Ticket. Support groups are predefined in Toolbox, but the user can add other groups, for instance for Geographical Regions.

When a matching FREE engineer is found then system will email a Job Ticket to that Engineer. The Engineer can choose to *ACCEPT* or *DECLINE* that ticket in a reply email. The system depends on the Ticket Reference #999999 in the email Subject line (do not edit) to track responses from Engineers.

Engineers can asynchronously report unforeseen circumstances like illness at any time to the system and likewise availability. Holidays and availability are tracked by the system based on submitted plans to Toolbox. See The eMail *COMMAND*s between Toolbox <-> Engineer.

Tickets are processed following the rules set-up by the Edit Rules and Time-outs button. This specifies Time-outs (per Ticket Priority) and Procedures like when the Supervisor is updated by email on Assignments and procedure failures.

Full List of Engineer Requests

These messages are automatically sent to the Engineer by the System.

"You have been assigned this Ticket - Reply *ACCEPT* or *DECLINE*"

"Job Ticket Offer to Any Engineer - Reply *ACCEPT* to take this Ticket"

"The system has Acknowledged you have ACCEPTED this Ticket.\n You can supply progress details using further *UPDATE* replies and *COMPLETED* when Ticket is completed successfully.\n Reply *REASSIGN* to relinquish this Ticket.\n Reply *NOSOLUTION* to indicate not fixable"

"There was no Response from you to Ticket Assignment - Reply *ACCEPT* or *DECLINE*"

"Can you update the system on Progress - Type *UPDATE* then details or *CLOSED* or *REASSIGN* or *NOSOLUTION*"

"The system did not recognise your response - please respond with the Correct Reply Text "

"The system did not recognise your last response - the Ticket details will be re-sent now (do not modify the Header Line)"

"The system has Acknowledged you have DECLINED this Ticket."

"Supervisor - Ticket has been assigned to "

"Supervisor - Ticket Assignment Timeout - Re-Assigning Ticket"

"Ticket Completed Confirm",

"Ticket No Solution Confirm",

"UPDATE receipt confirm",

"The system has Acknowledged you have RE-ASSIGNED this Ticket.",

"The System Operator has Cancelled this Ticket.",

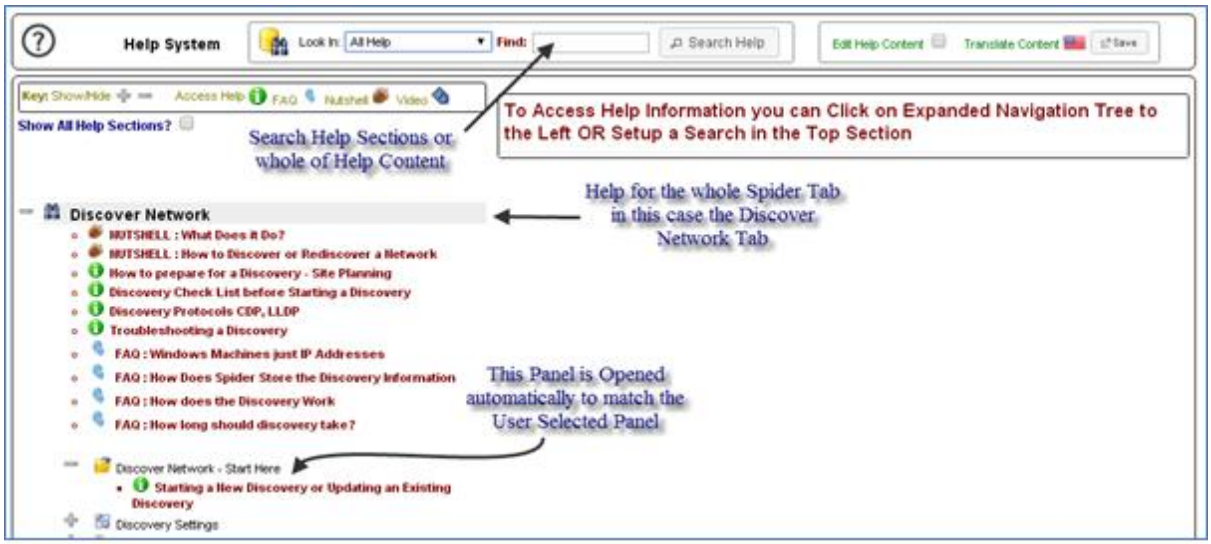
"The System Operator has Re-Assigned this Ticket.",

"Maximum Job Time Exceeded for this Ticket.",

"Help - *ACCEPT* offered ticket\n*COMPLETED* ticket completed ok\n*UPDATE* add details to ticket\n*REASSIGN* re-allocate ticket to engineers\n*NOSOLUTION* close not fixed\n\nTo Supervisor Status Update - *BUSY*, *AVAILABLE*, *SICK*, *HOLIDAY*"

HELP SYSTEM

To Access Help information, you can Click on the Expanded Navigation Tree to the Left OR Setup a Search in the Top Section



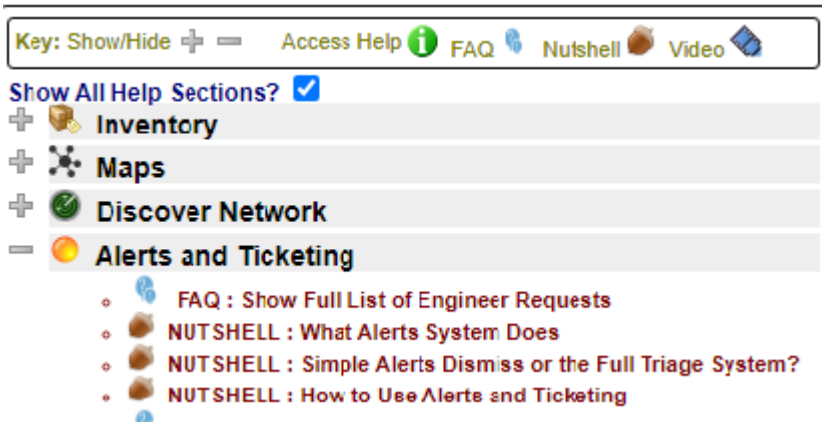
The Help System is accessed by clicking on the main Help Icon at the top of the Toolbox screen. The Help is automatically set-up to match the currently selected **Main Tab** and **Panel**. There is also a Search Facility that can search the whole of Toolbox Help or limited to a selected feature.

Help Items are defined as Nutshell (brief summary), Information and FAQs. The Nutshell items are designed to give a quick summary of a feature.

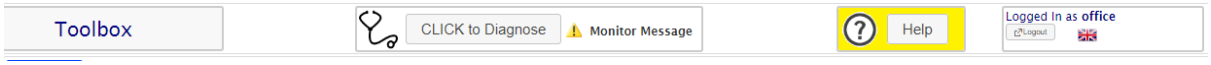
The Help System is a major component of Toolbox and should be used extensively by the Toolbox operator.

Toolbox built-in Help System

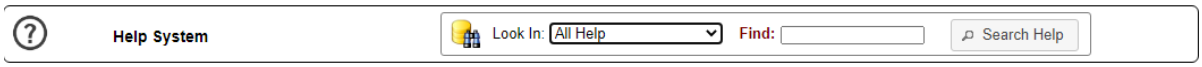
Help Navigator System



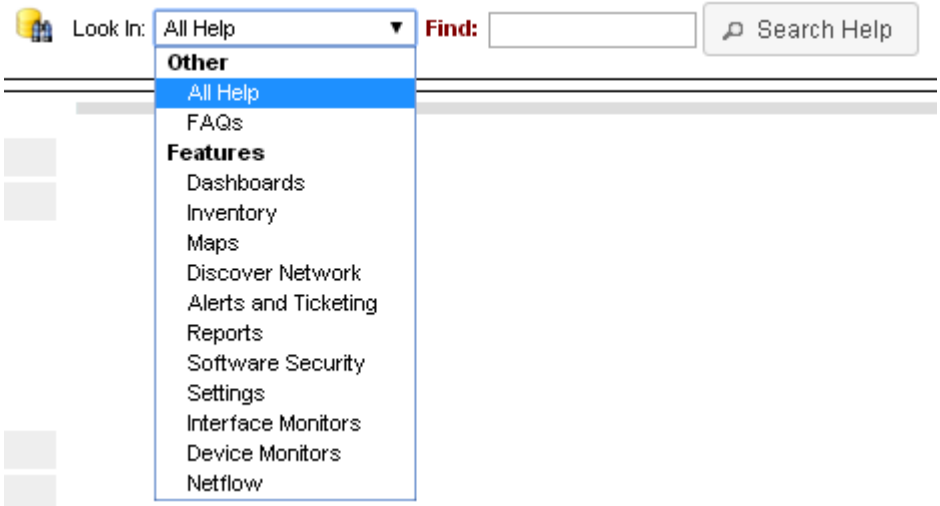
The Help Navigator system is designed to mirror the structure of the Toolbox Tabs and Accordions structure, so that Help is presented in a logical manner, so the user does not get lost.



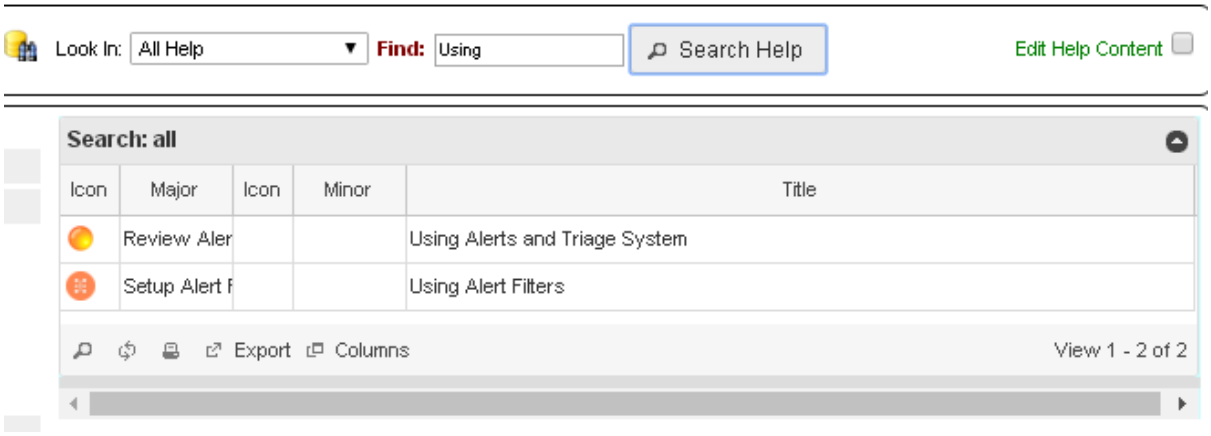
Help is always available from the GUI (yellow highlight) and is fully context sensitive to provide relevant Help to the Toolbox Feature that is active.



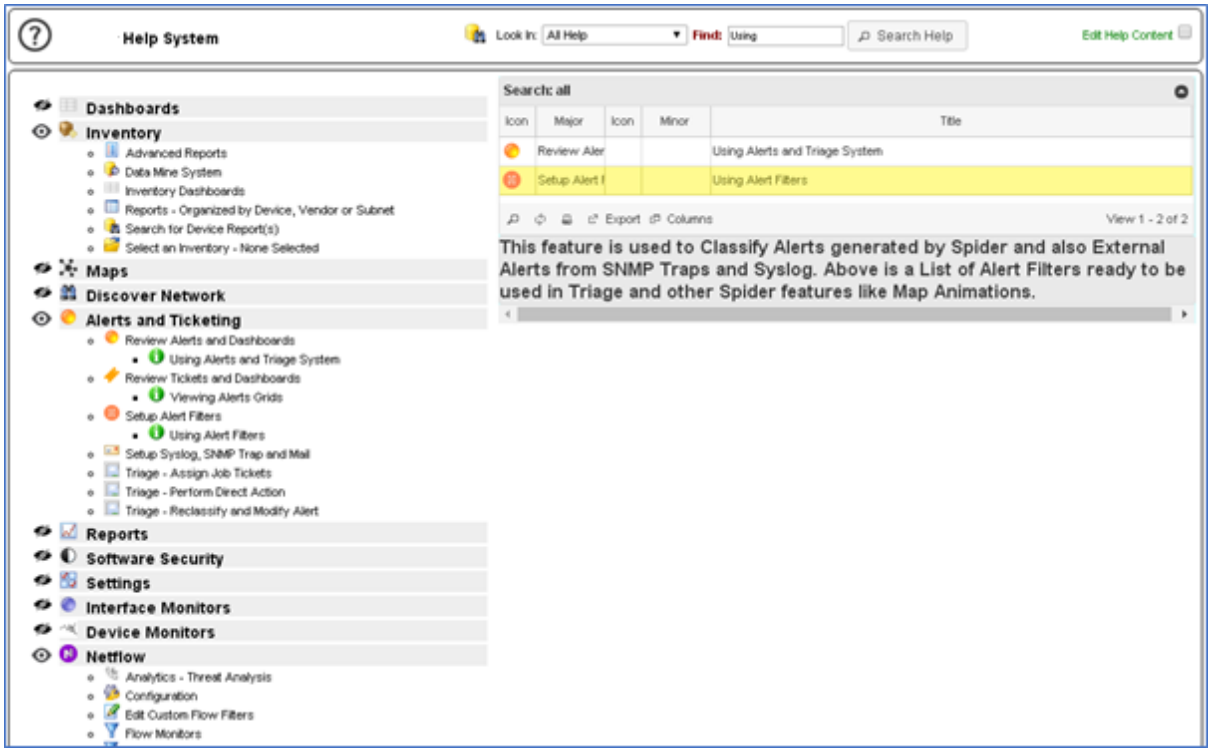
In addition to the Help Navigator there is a parallel Help Search System which is a way to locate Help based on complex matches including wild cards.



The search can be qualified to restrict the search by feature or to limit the search to FAQs.

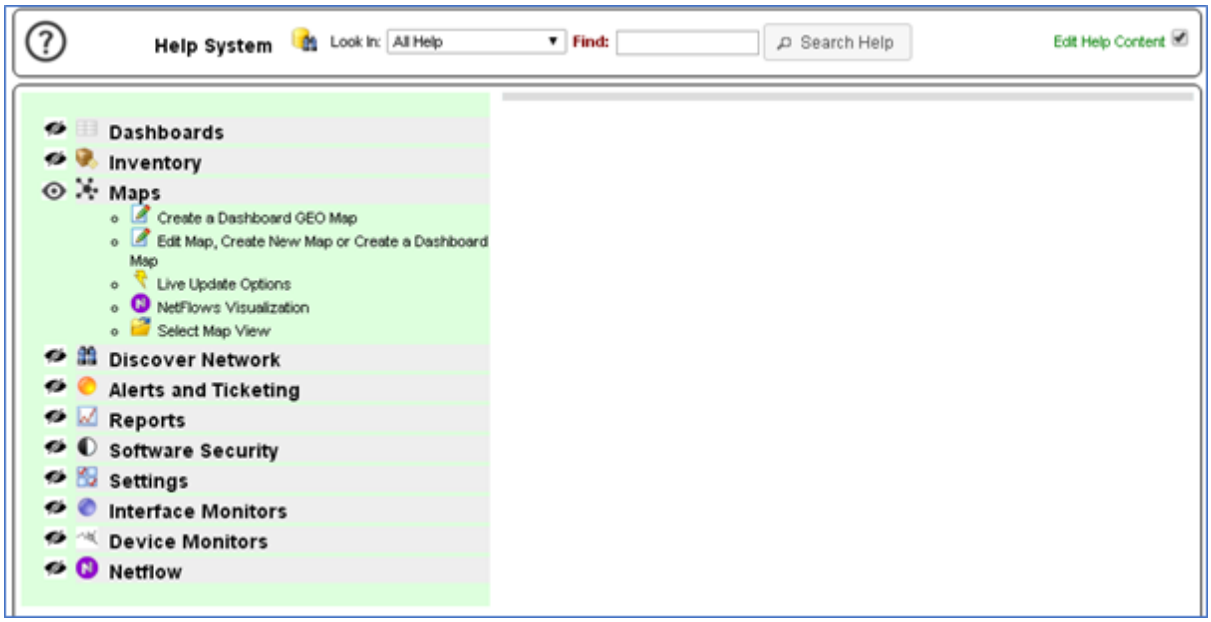


After clicking the Search Help button, a grid showing a list of matching entries is presented. The user simply clicks on a row to be presented with Help Content. The list can be sorted and further filtered using the Grid search and sort, if required.



The Help system is flexible in that both the Navigator and the Search are available at the same time.

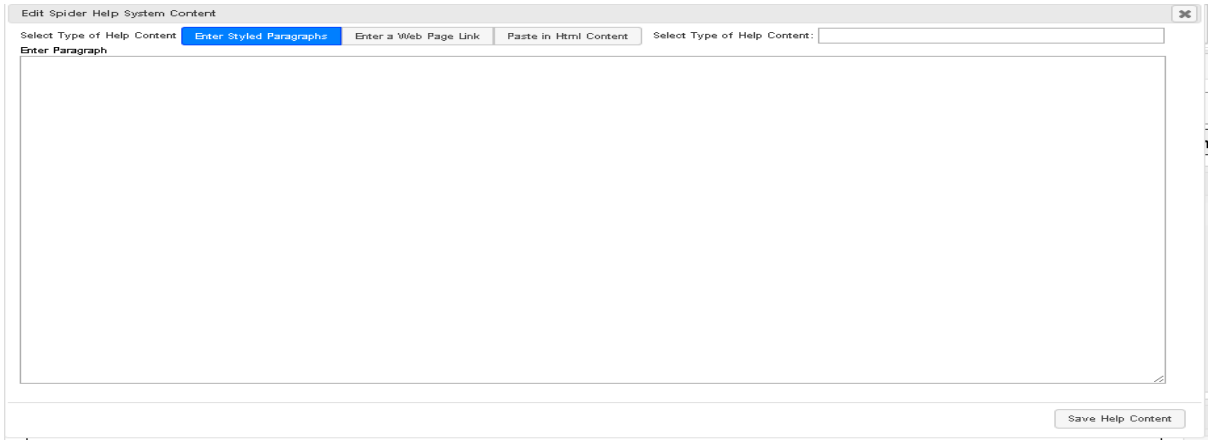
Edit Help Content



When the user clicks the Edit Help Content tick box then the GUI is modified to allow content to be directly entered into the Help Database. The Navigator is highlighted in green to prompt that Edit Mode is in force. Please remember to save any user edits to Help.

When a Section Header like 'Maps' is clicked, a Dialogue box appears to accept Help Content. Help can also be attached to second level items such as 'Live Update Options'.

The *Edit Help feature* is only accessible using a *special Login*, please contact your local support for further details. There is also a facility to Translate the Help Content, please contact your local support for further details.



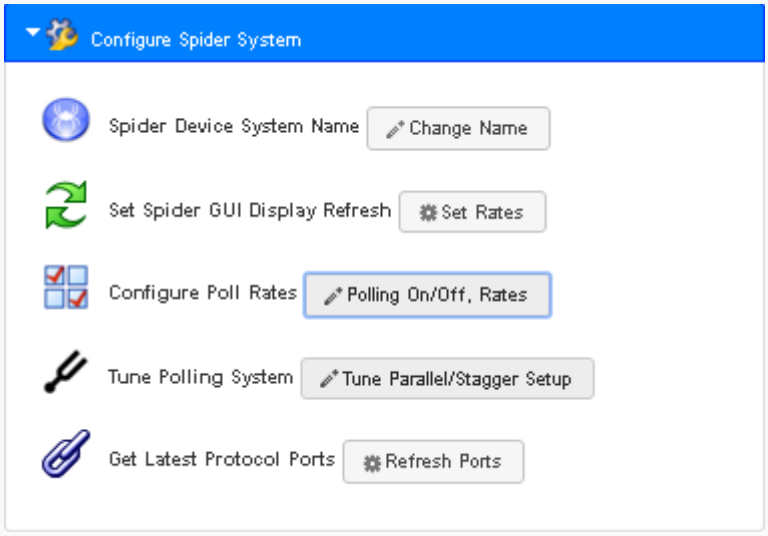
The Help Content can be entered in three formats: -

- One or More Paragraphs as Text with Paragraph Styles.
- A Web Page Link to content on the Toolbox Server or other sites (run in an IFrame).
- Direct HTML possibly exported from a Document such as MS Word that has been exported as HTML.

SETTINGS

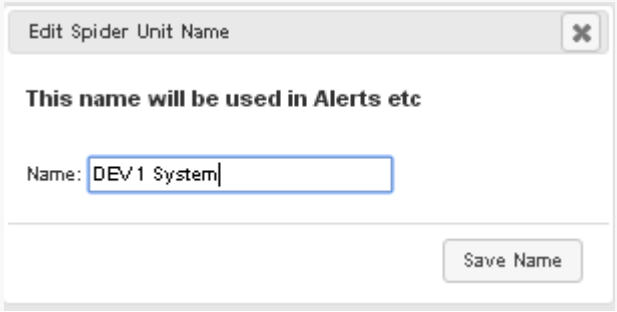
Configure Toolbox System

Below is the Configure Toolbox panel under the Settings tab.



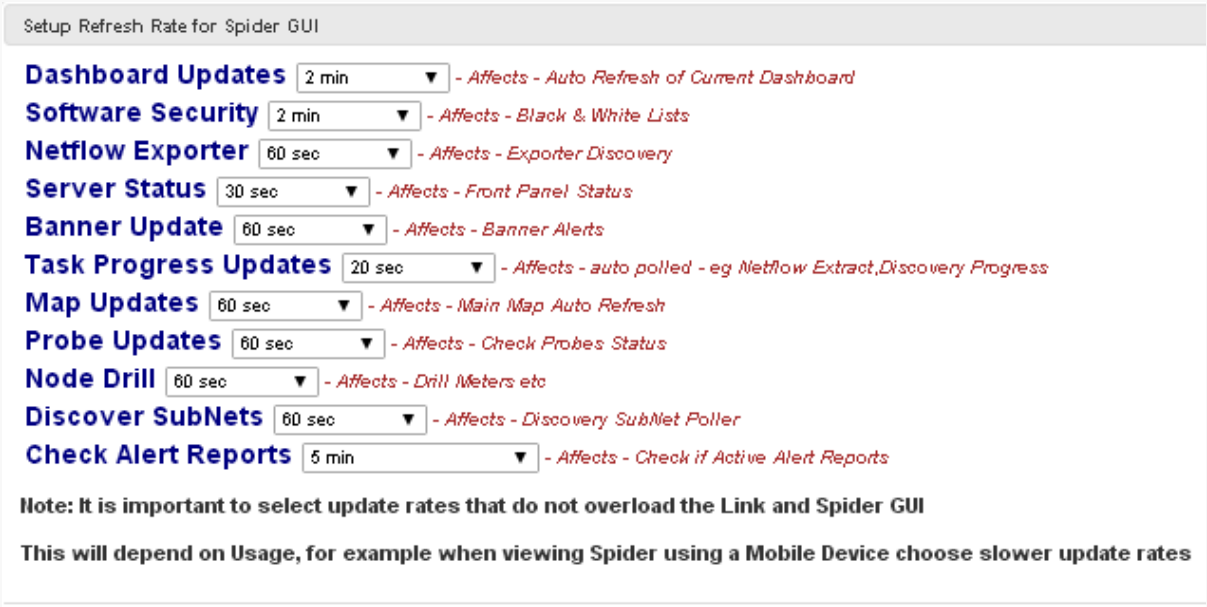
Toolbox Device System Name

This is used to change the internal name Toolbox uses (independent from any Probe name).



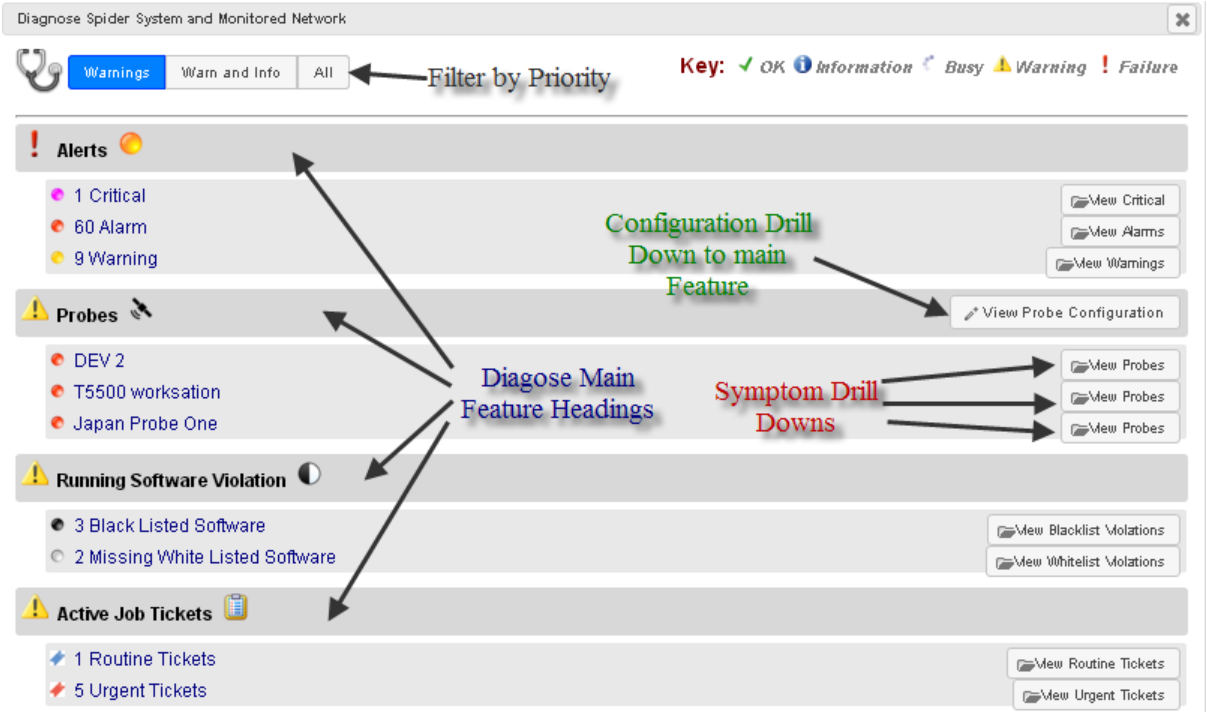
Set Toolbox GUI Display Refresh

This is used to control the traffic from Toolbox Server to the Browser. It controls the trade-off between how current the display is, versus the traffic loading. These values are held local to the BROWSER not the Server, so multiple device types can have their own refresh rates.



Note, some of the settings above do not apply to products 1-4. Settings like the Netflow Exporter apply to other Toolbox products. Please contact your local support for more detailed information.

Diagnose



Diagnose gives an extensive summary of error conditions both locally and as a summary for remote **probes**, see section **PROBES**.

The Diagnosis can be examined further by clicking on a Diagnose Feature or Symptom Entry. The priority level of the Diagnosis display is determined by the Diagnose Tabs, showing only important conditions or general information.

How to Add a Probe

Click on Add Probe, as a minimum just enter the IP Address of the Probe and a Unique Title.

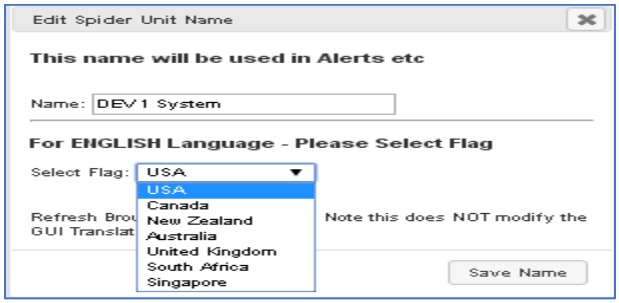
To show Probe Maps in the Dashboards tick retrieve Maps.

Adding other details like Icon enhances the Toolbox web reports and Maps.

Note: The Probe IP address **must be IP routable** from the Master Server to the Remote Probe using Html XHR traffic in both directions.

Toolbox Main Screen User Selection Flag Icon

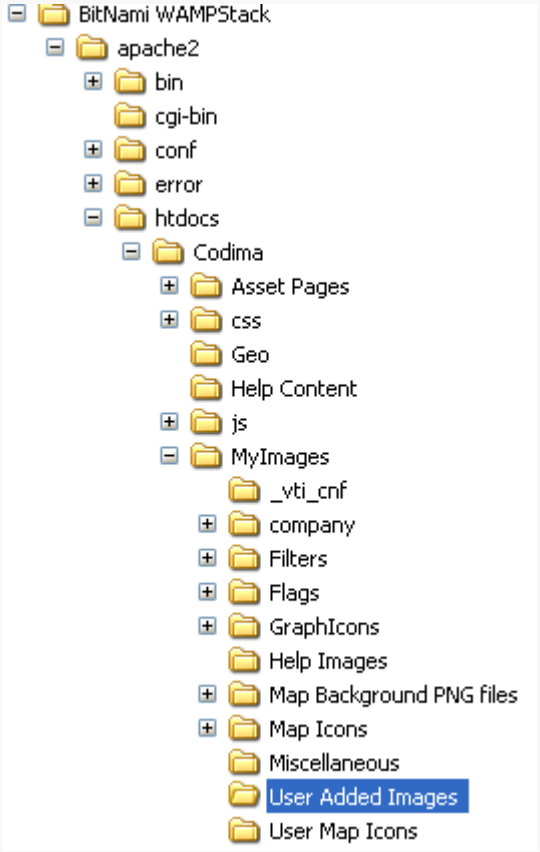
This allows the user to select English Language for the Toolbox GUI language, but choose other Flags in the GUI (other than the USA) as below:



Viewing Toolbox Icon Set – Add Own Icons

Click on the View Images and Icons to View the Icons set that can be used throughout the system for instance to add an Icon to a Probe or a Global Polling Address.

The Update button will rescan the Images file set on the Server and Update Toolbox with the directory contents, as below: -



The directory **User Added Images** is where the User should put their Images.

The other directories will be replaced by the Toolbox Installation program Updates when Toolbox is Updated - so do not update those directories.

Toolbox Integration to Existing Management Systems

The Toolbox system can work as a Standalone or Distributed System and handle itself all monitoring, mapping finally to Job Ticket creation.

However, Toolbox can also augment existing management systems in the following ways.

The Live Web Maps can be used to add a Live and Replay Visual overview of the network status, taking in Alerts from the existing management system thru Traps or Syslog to Update the Web maps. Job Ticketing, similarly, can take in Alerts to drive a Toolbox Alert Triage and add full specification Job Ticketing system.

The various Toolbox Security features can be added to an existing system, for instance processing Security Alerts from an existing IPS system to display events and status on the Live Maps or maybe drive Job Ticketing.

For some large, centralized management systems, it may not be economic to monitor certain network locations due to poor or expensive upload speeds to the central server. Toolbox offers a very low-cost monitoring solution using tiny network bandwidth and a free Server as it uses free MySQL server.

Toolbox Alerts system supports Event Translation and Forwarding. This can be used as a utility to an existing management system to send Syslog or Traps to other management platforms. That is following Language or Obscure Jargon Translation. It can also convert from for example Syslog messages to SNMP Traps.

Contact your local support for details on the product.

PROBES

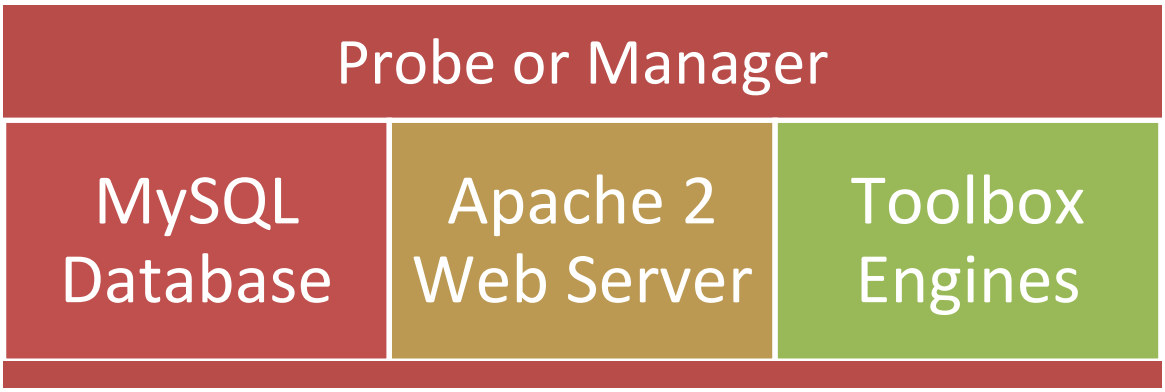
Toolbox Deployment of Probes

All Toolbox installations install exactly the same software, so a Probe install is exactly the same as a Manager install. Functional variations are controlled entirely by the Toolbox license.

The Toolbox Probes, and Managers, can be viewed thru one or more, local, or remote probes, Web Browser. Critical is the ability of any Manager to view any combination of Probes.

Toolbox Probe and Manager System Software Architecture

All Toolbox installations install the same software, so a Probe install is the same software installation as a Manager installation, structure as illustrated below.



How Probes Work

Probes are a full installation of Toolbox Software including Web and MySQL Servers. They are fully standalone systems that can be viewed as a standalone system directly in a web browser.

However, they can also be attached to another Toolbox System and viewed as part of a distributed monitoring system. The distributed system supports remote maps with animation and drilldown.

Probes communicate with other Toolbox Systems using an IP Address and HTML GET and PUT Web requests - which simplifies firewall setup.

Installation of Probes

To do this go to Settings Tab and select the Probes Panel then follow the Help Instructions.

NOTE: The Probes are created under the Settings Tab -> Probes.

Setting-Up a Probe

This is a simple process. Select the Settings main tab and click on the Probes panel. New probes can be added by clicking on the Add Probe button. The critical setup parameters being the Probe Title and its IP Address, it a good idea to add the other fields such as Icon too.

Probe Usage

Probes can automatically send their Discoveries to the Probe Master system; they can then be viewed Live in the Master System. A Master system is a system that monitors one or more Probes, otherwise it is the same as a Probe.

Multiple Probes Monitoring a Single Large Network

Multiple probes are typically used with large or multiple networks to scale monitoring (worldwide).

Probe Licensing

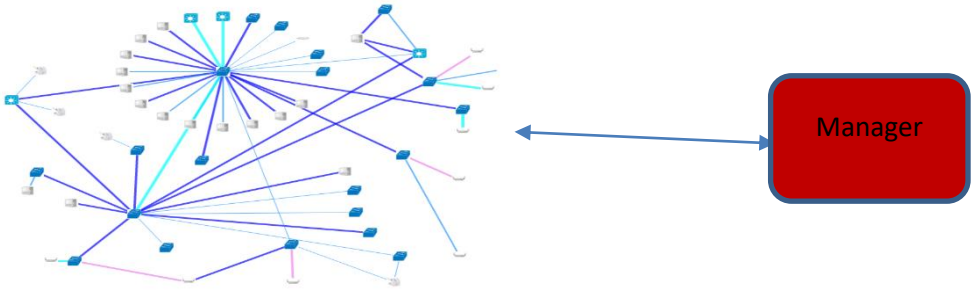
Probe Licensing has a facility to warn when the maximum Web Users (set in the product license) is exceeded to avoid confusion in the field.

The number of Probes a manager can control is now set in the license. A new license type has been administered to limit a product to Probe Only Tabs Discovery and Settings, with Inventory Explorer and Maps tabs removed. See section **Probes Licencing and Administration Details.**

Single Manager

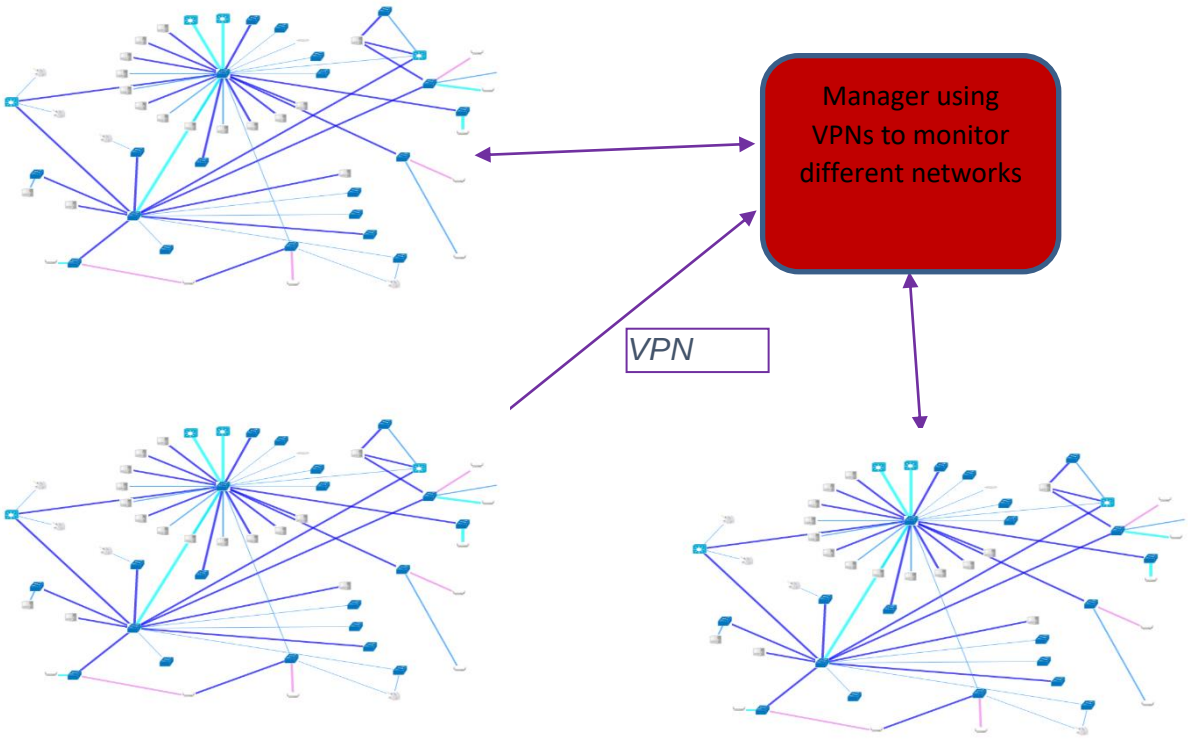
Single System Deployment Connected to One Network

This would apply to a small or medium sized network in terms of Monitored Devices so could be a very large network - however with only key devices and links monitored.



Single System Deployment Connected to Several Networks using a VPN

This configuration is suited to a discovery and monitoring of multiple remote networks accessible via VPN links. The Manager sees the individual networks as one network, however individual Drill Down Maps can be created per VPN linked Network to view the networks individually with the multiple Drill Down Maps.



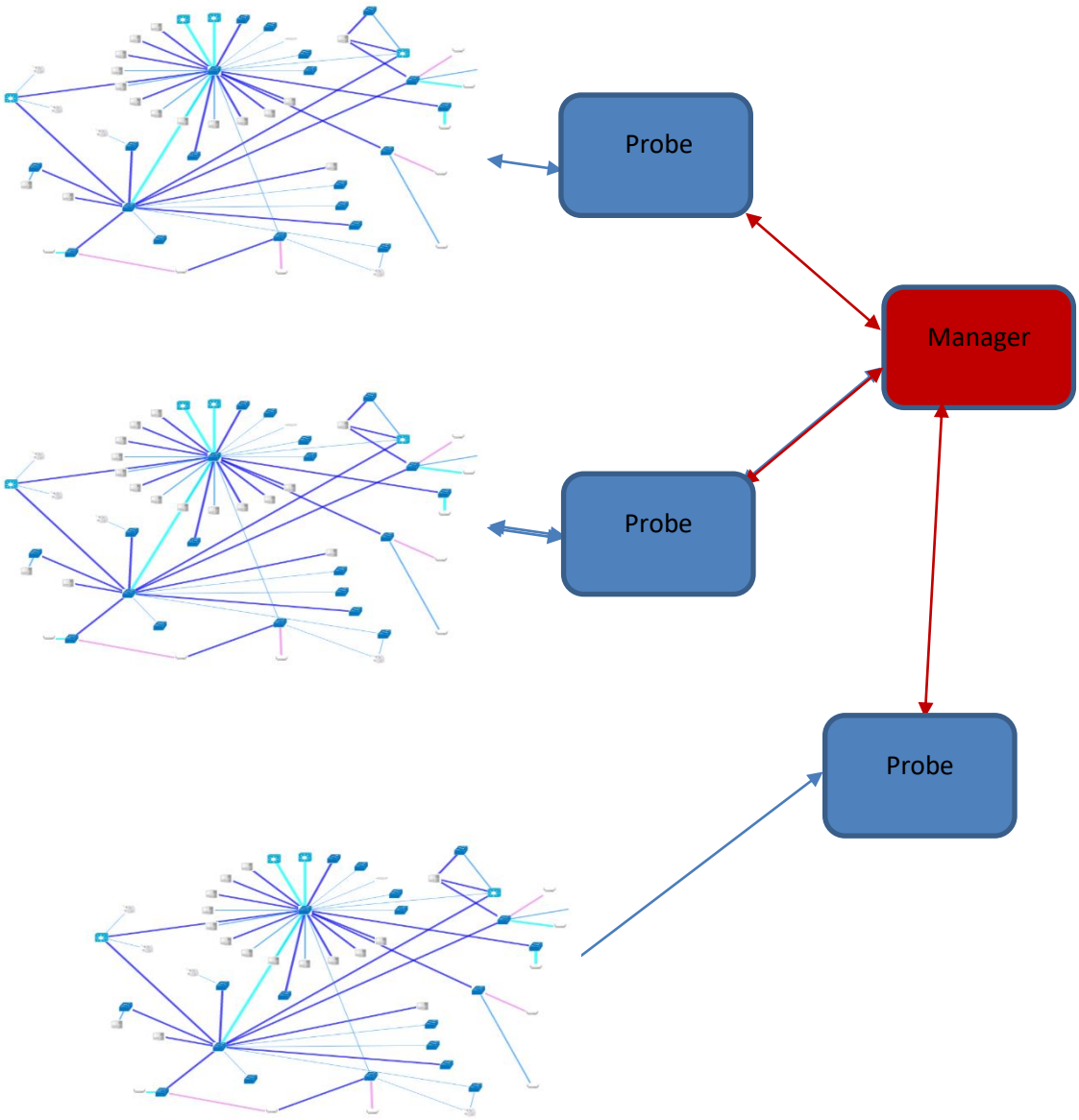
Multiple Probes with a Manager

A Manager and Probes configuration is used for the following reasons-

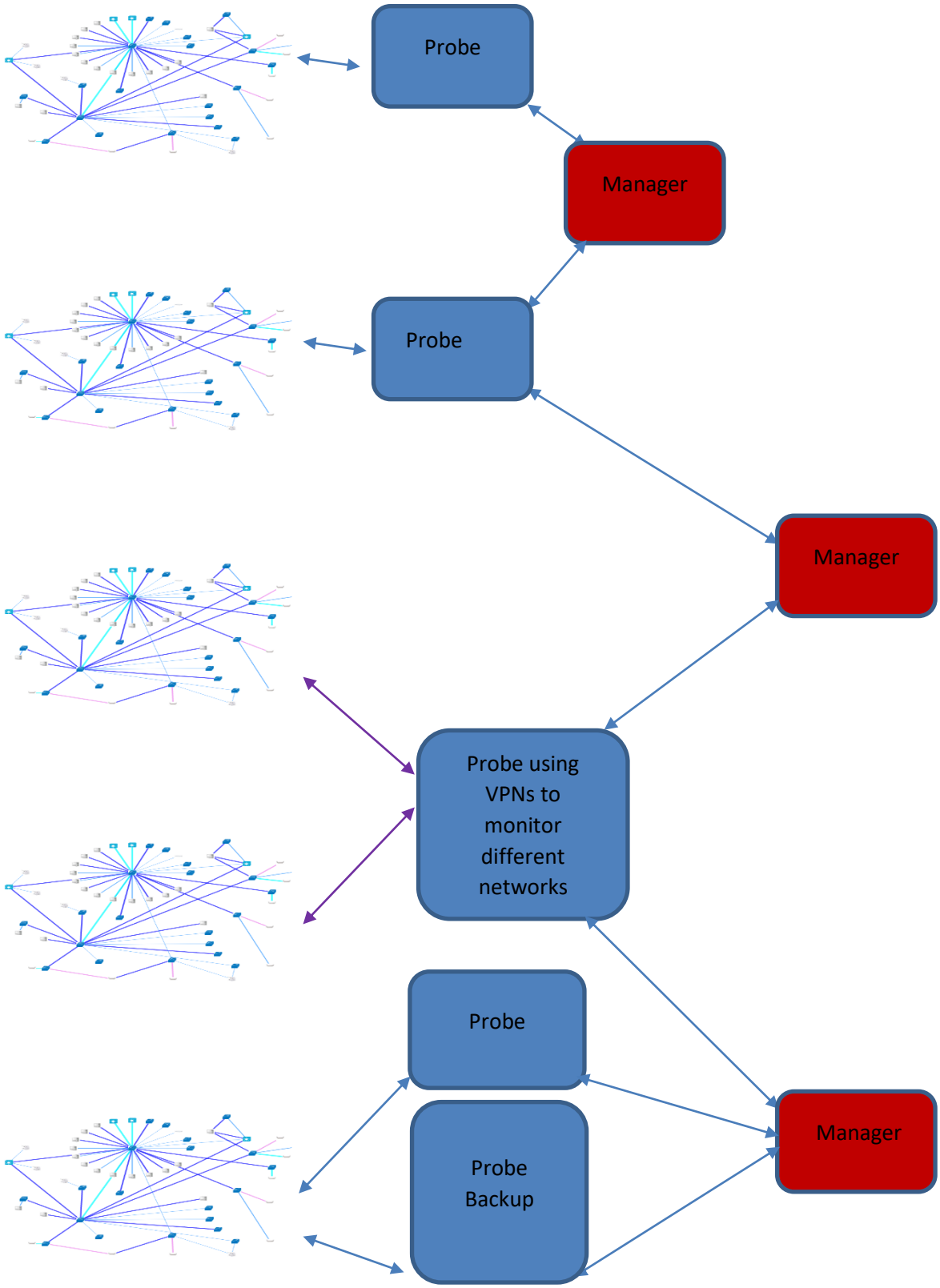
- To reduce remote polling traffic by polling locally
- To reduce the Polling and storage requirements per System. Unrelated Networks need Polling separately.

Typical Scenarios: -

- Multiple Network Locations – keep Probes Local
- Split up the Polling Loading per System – reduce loading per System
- Poll individual functions of a Network Separately – unrelated networks



Mixed Manager and Probes Hierarchy (Including Possible VPN Links)



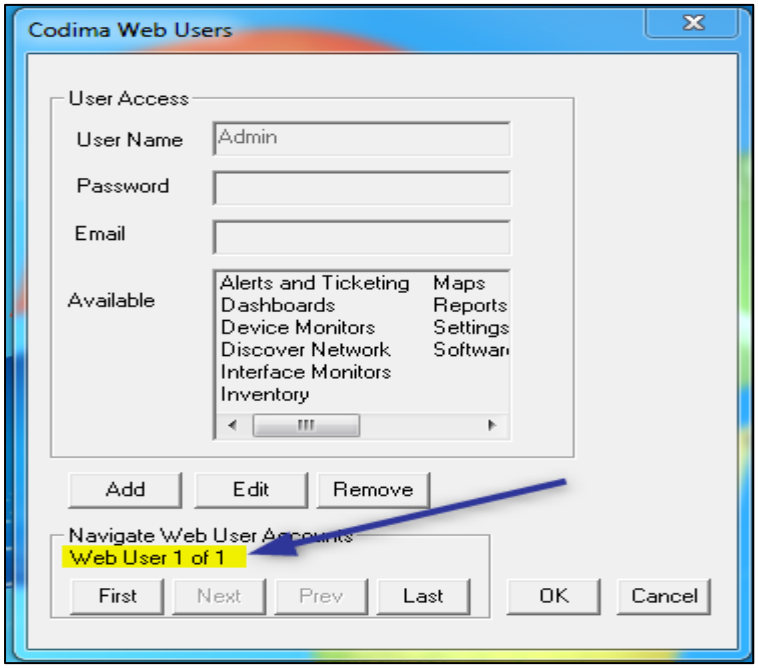
Probes Licencing and Administration

To support Probes administration in **Enterprise Inventory Explorer** a Probes Admin GUI shows status, discovery license and probe performance in one click.

Probes Licensing

Show Maximum Web Users

By clicking on the product icon in the Windows System Tray the Web Users option is shown.

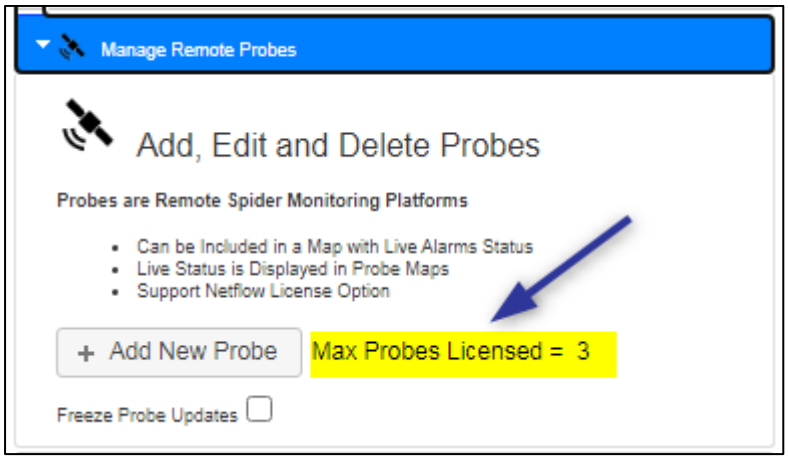


The user can see how many Web Users are allowed in the supplied product license. In this case one user is permitted under the license running on the product install server.

Maximum Probes that can be Managed

Probes are added under the product Setting tab on the main GUI.

A panel under the Settings Tab is used to add Probes that are managed by the product GUI as below:

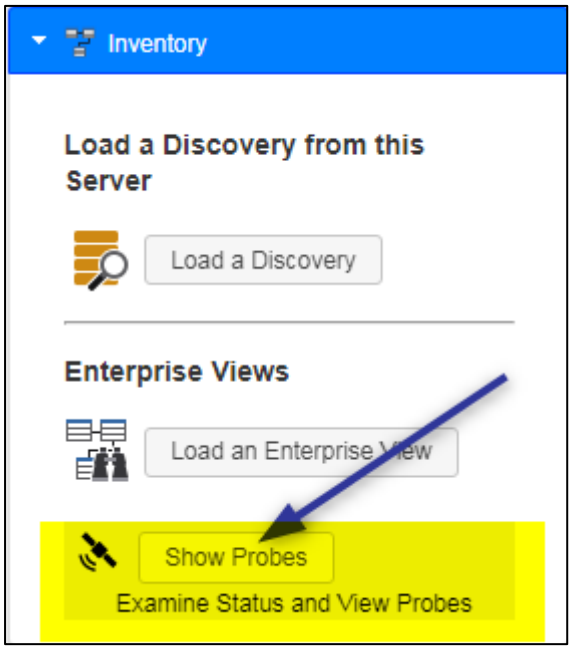


In this case 3 probes may be added as per the supplied product license.

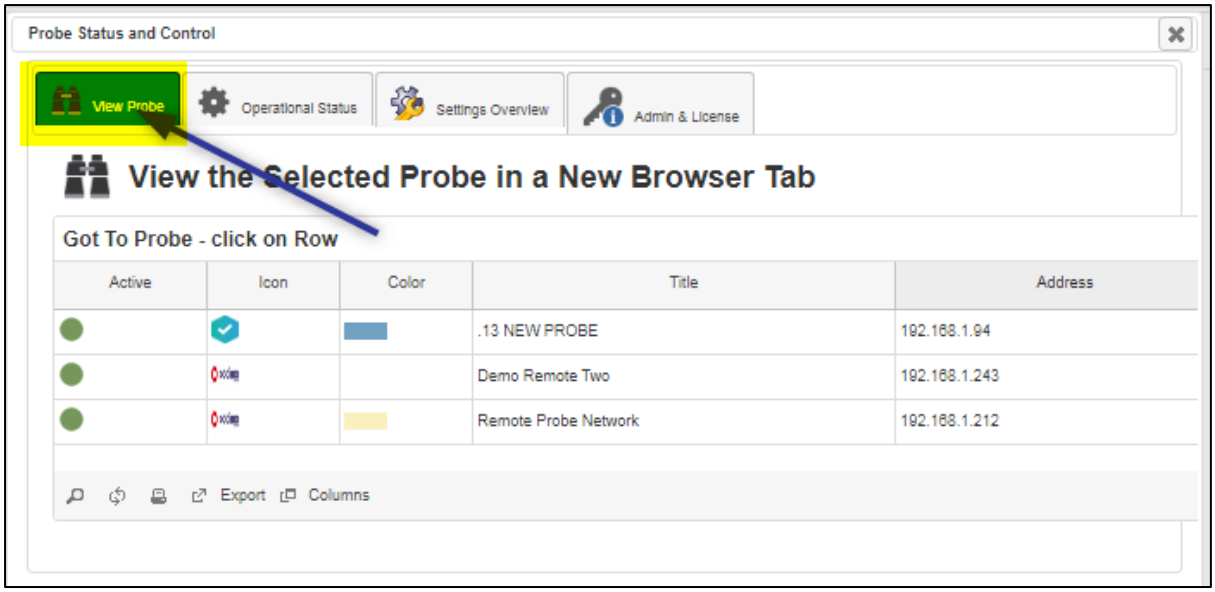
Probes Administration

Probes are added and setup under the Settings Tab.

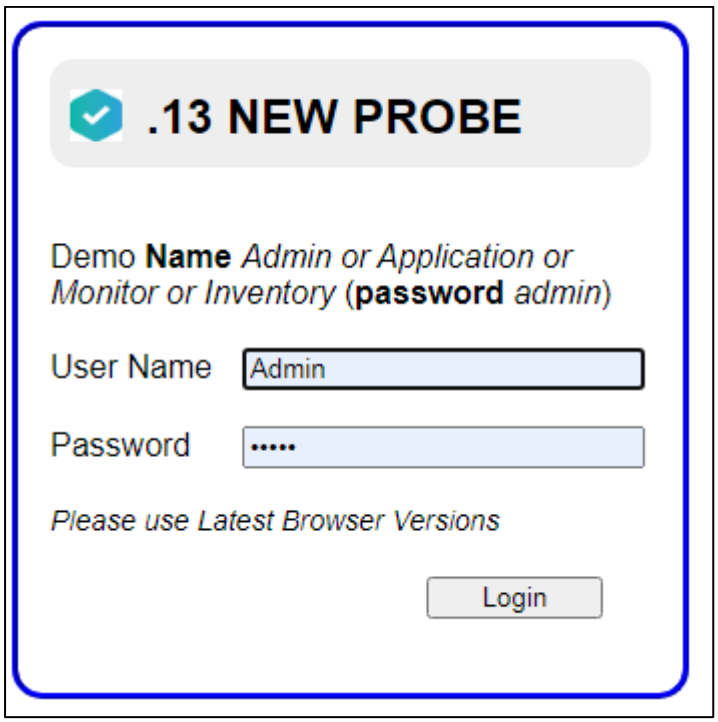
A new Probes Information and Go-View GUI has been added under the main **Inventory Tab**, **Inventory panel** as below: -



Clicking on the **Show Probes** button shows the Probes as below:

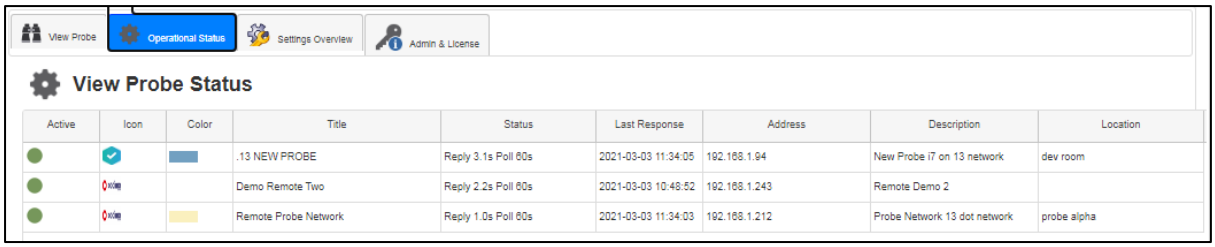


The View Probe tab is selected. Clicking on a row in the Grid opens a new Browser Tab and the selected Probe may be accessed from the new Browser Tab as below:

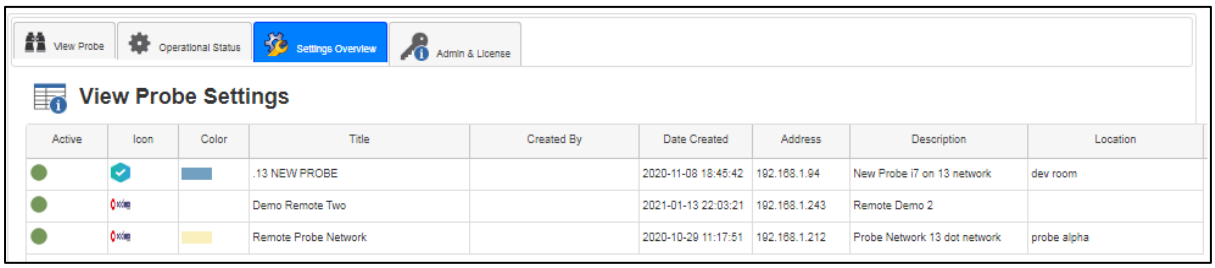


Note the Login details matches the selected row in the grid row that was clicked to access the remote probe. This feature is useful to setup or change Discovery Parameters on a remote probe system.

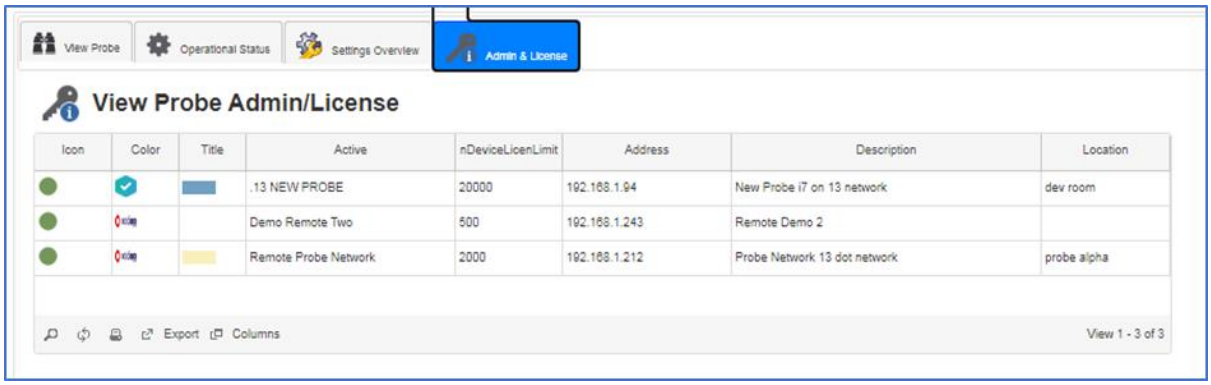
Selecting the **Operation Status** shows the Response Time of the Probe and other details.



The **Settings Overview** tab shows further details about the Probe such as when it was created, and by whom.



The final tab **Admin and License** shows the Licence Device Counts to track total device discovery limits in one view. The Grids can be manipulated and Exported or Printed.



APPENDICES

LEGACY INVENTORY - 2013

NOTE. This section LEGACY INVENTORY – 2013 refers to the product introduced in 2013 and has been retained in this manual as some customers are actively using this feature.

For new customers it is strongly recommended to use the Inventory Explorer product introduced in 2020.

Explanation of what the Legacy Inventory 2013 feature does

There are three outputs from this feature after running a Network Discovery.

1. A set of Web Page based reports that give an in-depth breakdown of Devices, Connections and Installed Software.
2. A set of Grids that can be Used to dynamically search for items such as Device Serial Numbers, Link Types, Device Components and Installed Software. The contents of the Grids can be Exported.
3. A Set of Dashboard Reports that breakdown the items in the Current Discovery into Multilevel Donut Charts with matching Multilevel Grid Analyses.

Legacy Inventory builds on the Inventory and Mapping product to copy all the Inventory and Mapping web report output, then adding a whole range of new functionality in its dynamic search capabilities and fully customisable extra sets of Dashboard Reports.

Selecting a Discovery in Legacy Inventory 2013

If this table is empty, then that is because a Discovery has not been run yet. Go to the Discovery Tab in Toolbox and start a Network Discovery. Otherwise click on a grid row to select a discovery and its associated Web Reports.

Note: only the currently loaded Discovery is used to display the Toolbox Dashboard Reports which is unaffected by the Discovery chosen in this tab Panel.

What can I do with Legacy Inventory 2013?

Post Discovery a system of HTML linked Reports is created of Devices, Interfaces, Installed Software etc as Linked Pages HTML system.

There is a search capability for finding details for a particular device.

Advanced reports that Analyse the raw data to produce intelligence like free port counts and much more.

Data Mine give a detailed search capability to find anything from Software Patches to Device Serial Numbers.

There is a direct Link to Dashboards to give Comprehensive Breakdowns and Highly graphical matching Donut Charts.

How do I use Legacy Inventory 2013?

The Legacy Inventory content come from Network Discovery, so a Discovery needs to be performed first.

Then, the following is available: -

- Select Inventory - Displays structured HTML reports with drill links similar to the Toolbox product.
- Reports - These are a means to locate individual reports per Device using a Selection Tree and also a Search which process a list of matching reports.
- Advanced Reports - A collection of processed reports giving deeper analysis of the Inventory.
- Search - A means to match Individual Device Reports based on search criteria.
- Data Mine - This is based on multiple Grids and their in-built Search and Sort capabilities for a variety of different discovered objects.
- various report categories.

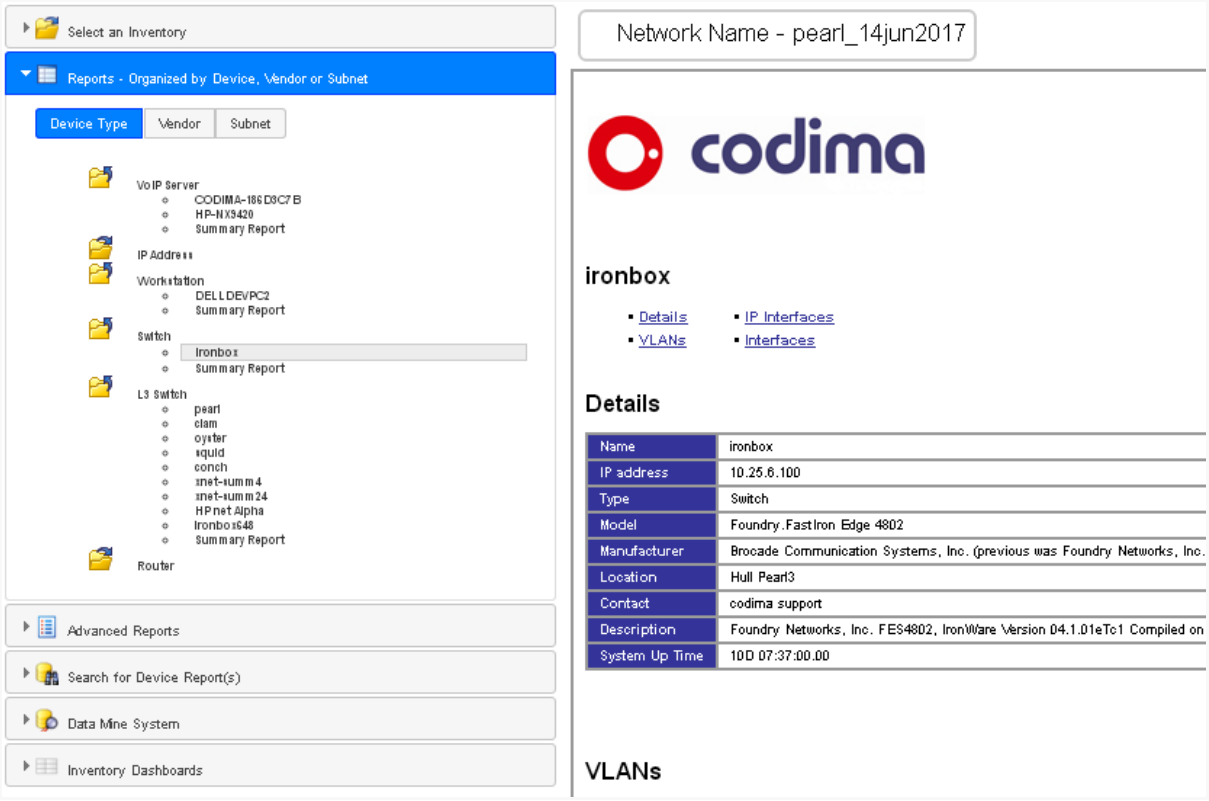
The Legacy Inventory 2013 is also supported by the Dashboard system, there is a quick link directly into Custom Fields and they are treated exactly the same as regular fields and are used in Filters and also in Analytics and Summary features.

A typical installation of the product involves Discovering the attached Network in detail, which is stored in MySQL database tables, ready for sophisticated data-mining analysis. As an example, knowledge of discovered devices, gives knowledge of Wi-Fi access points that may have been illicitly added.

Legacy Inventory 2013 - Report Pages Organised as a Tree

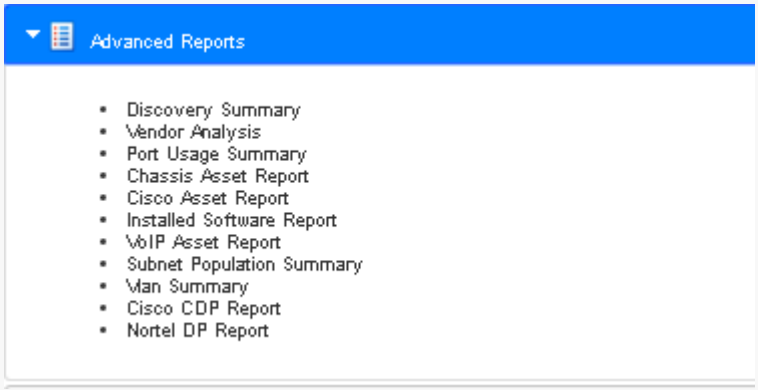
This facility allows the user to quickly find Report Pages organised by Device Type, Vendor or Subnet selected by clicking on a button list above the Tree Control.

The items are revealed by clicking on a tree Heading and a Report Selected by clicking on a tree leaf such as a Switch Item.

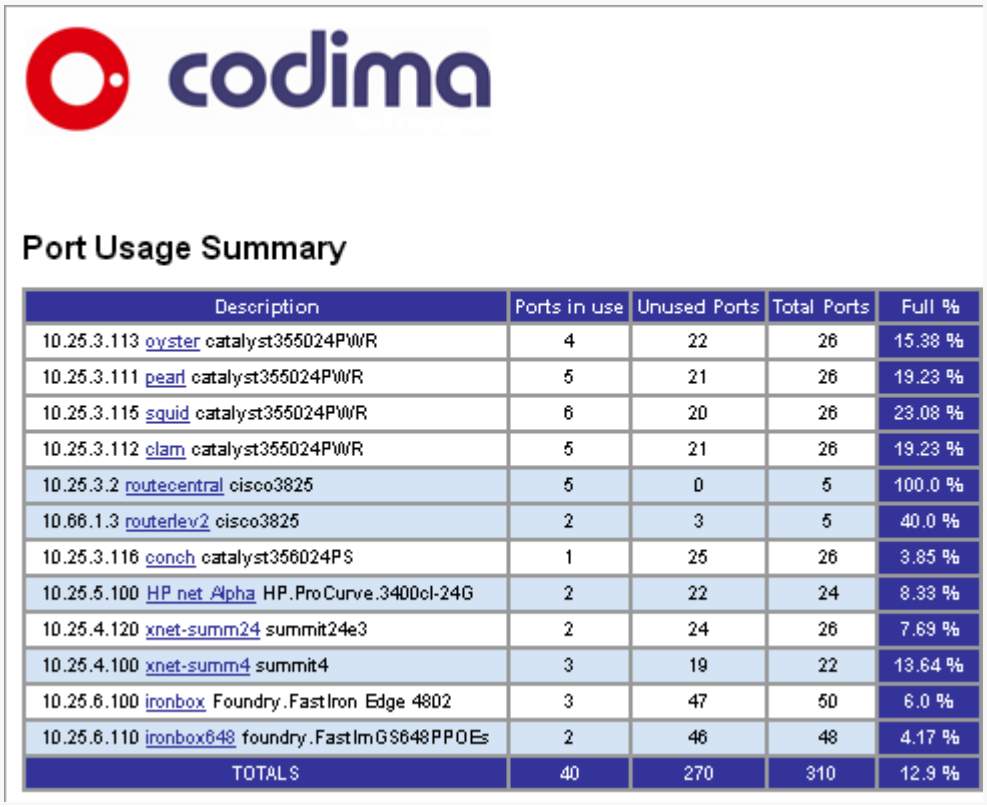


Legacy Inventory 2013 - Using Advanced Reports

This panel links to Advanced Reports created by the Discovery Engine. The titles below are self-explanatory.



Clicking on an item such as Port Usage Summary for example will show a custom HTML Report as below in the right display panel.



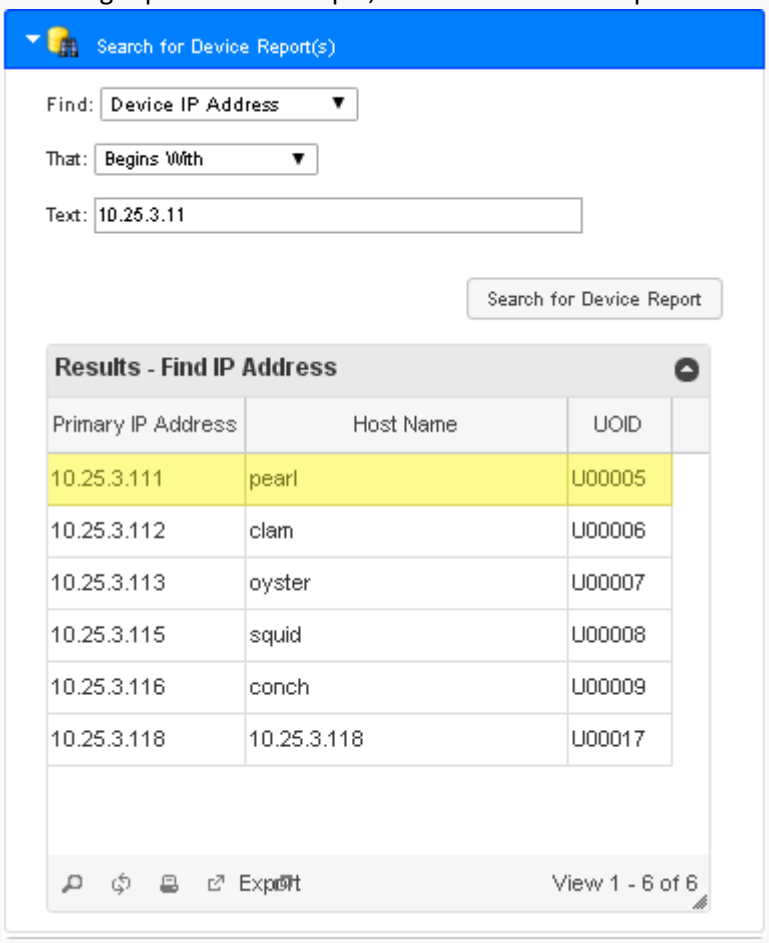
codima

Port Usage Summary

Description	Ports in use	Unused Ports	Total Ports	Full %
10.25.3.113 oyster catalyst355024PWR	4	22	26	15.38 %
10.25.3.111 pearl catalyst355024PWR	5	21	26	19.23 %
10.25.3.115 squid catalyst355024PWR	6	20	26	23.08 %
10.25.3.112 clam catalyst355024PWR	5	21	26	19.23 %
10.25.3.2 routecentral cisco3825	5	0	5	100.0 %
10.66.1.3 routerlev2 cisco3825	2	3	5	40.0 %
10.25.3.116 conch catalyst356024PS	1	25	26	3.85 %
10.25.5.100 HP net Alpha HP.ProCurve.3400cl-24G	2	22	24	8.33 %
10.25.4.120 xnet-summ24 summit24e3	2	24	26	7.69 %
10.25.4.100 xnet-summ4 summit4	3	19	22	13.64 %
10.25.6.100 ironbox Foundry.FastIron Edge 4802	3	47	50	6.0 %
10.25.6.110 ironbox648 foundry.FastIronGS648PPOEs	2	46	48	4.17 %
TOTALS	40	270	310	12.9 %

Legacy Inventory 2013 - Creating a List of Matching Device Reports

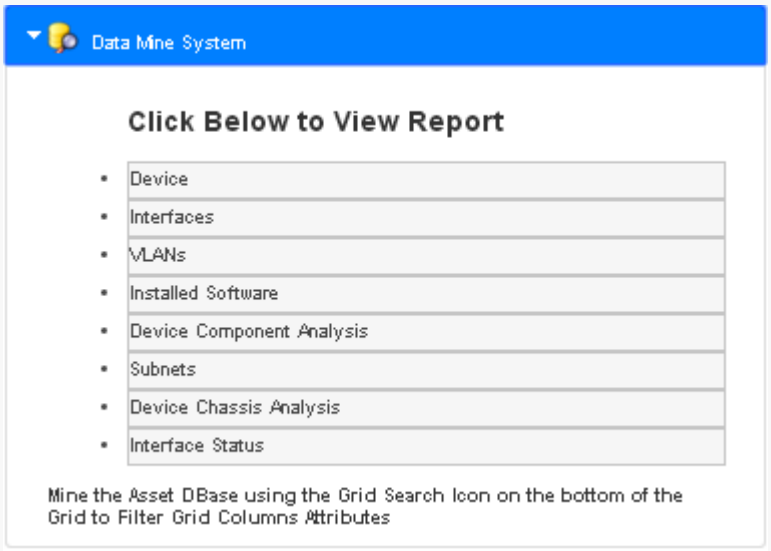
This panel is used to search through Device Reports matching some user search and produce a list of matching reports. For example, below a search for reports with IP beginning with '10.25.3.11'



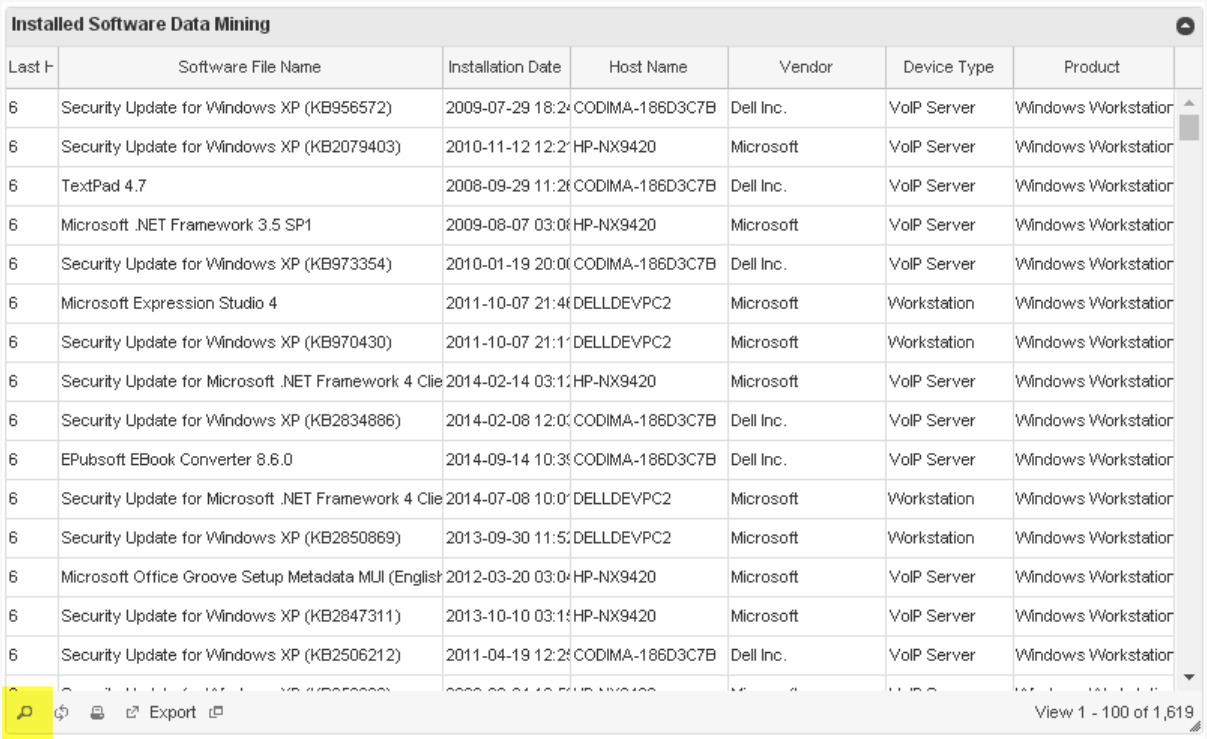
The device report is displayed by clicking on a row in the Match Results Grid.

Legacy Inventory 2013 - Using the Data Mine System

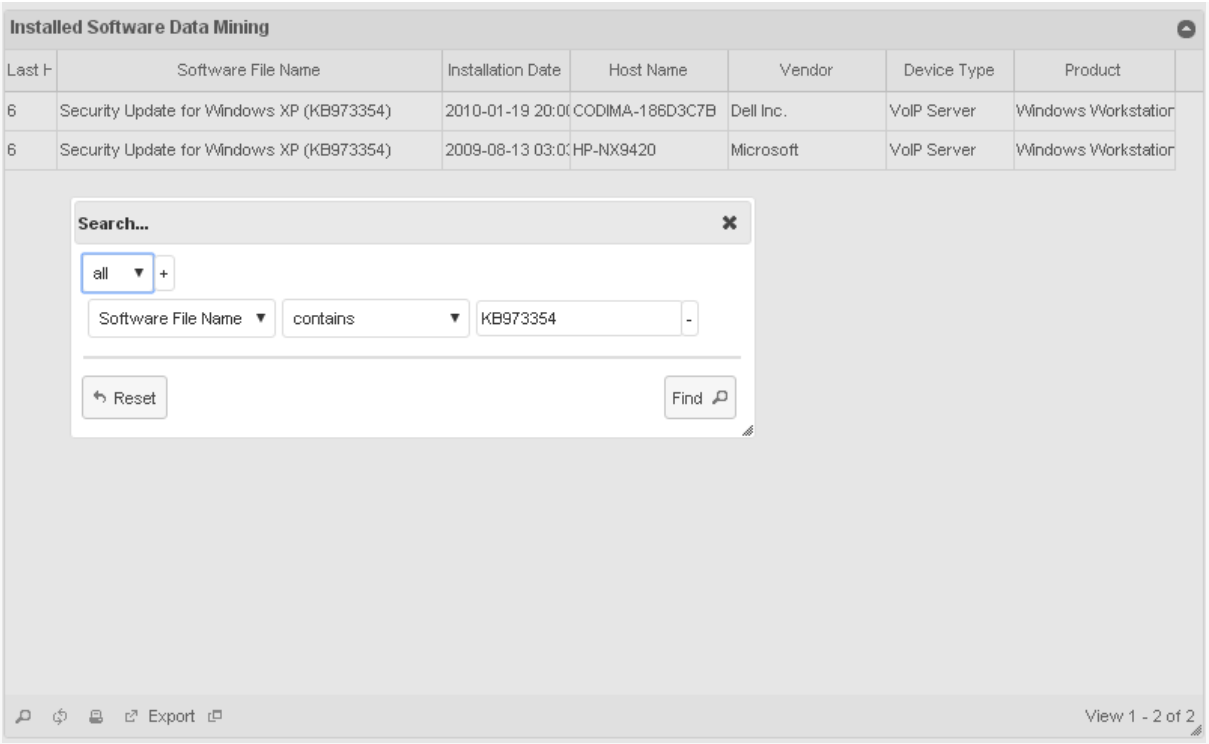
This panel is based around Grids (not Html Reports) and uses the Grid built in search to Mine the Discovery for user defined criteria.



On clicking an item such as Installed Software above a Grid will appear in the right-hand display panel as below.



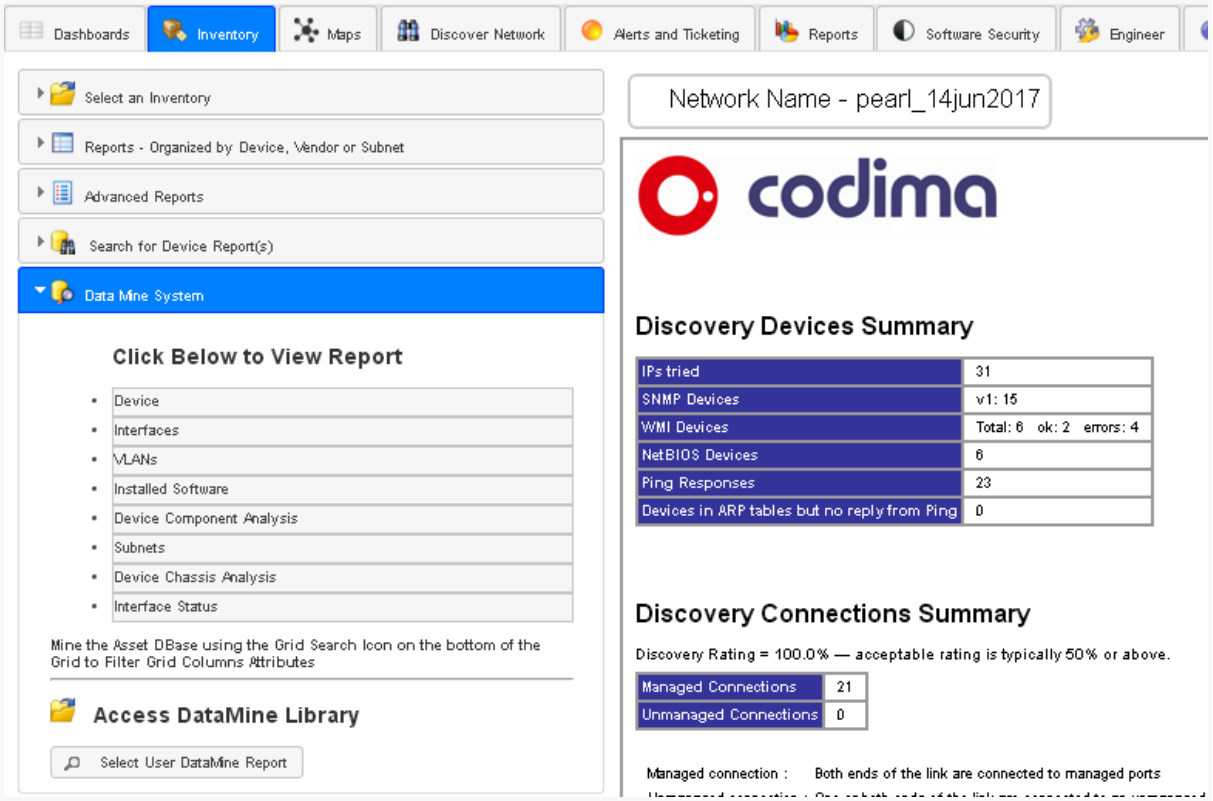
To search the Grid, click on the search icon highlighted in yellow in the picture above.



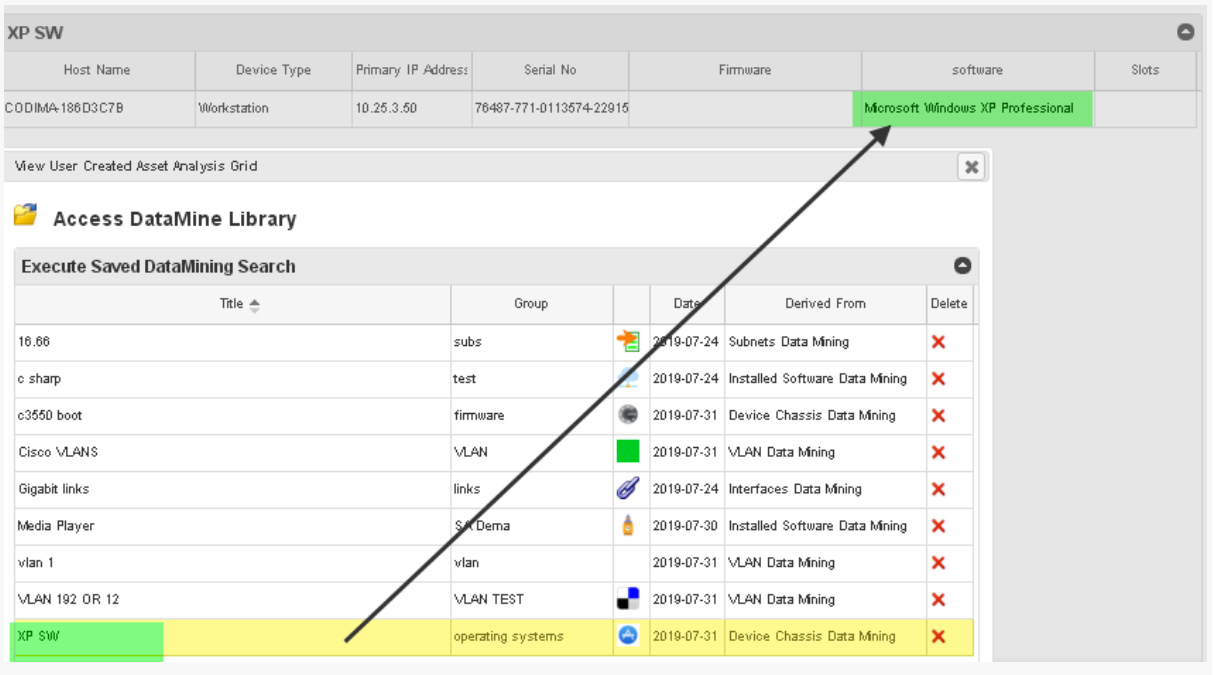
Above the Search pop-up is set to find software patch **KB973354** giving a list of all devices where this patch is installed at Discovery time.

Legacy Inventory 2013 - Using the Data Mine Library

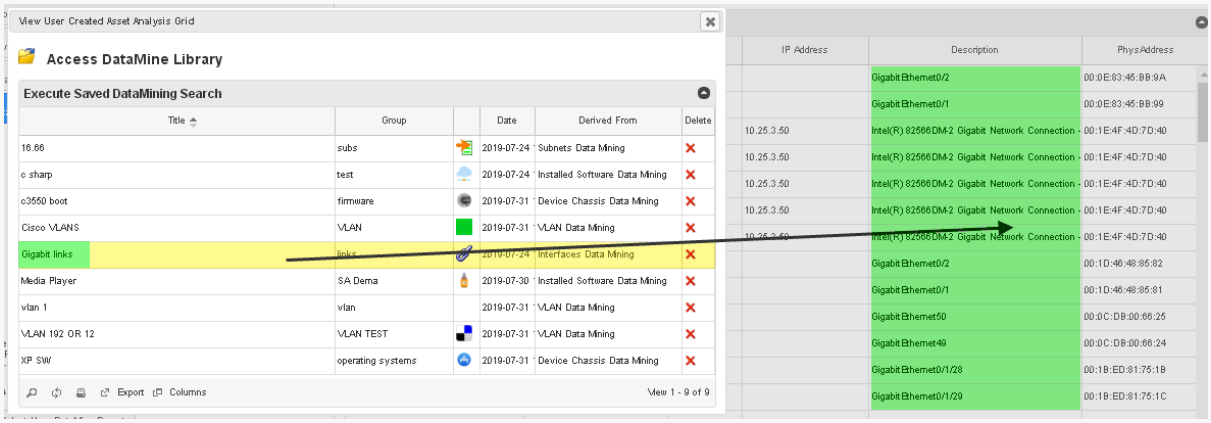
This feature allows the user to search the asset Library under the Data mine Panel and then save a search into a new Library feature.



Above a Discovery Inventory has been selected ***pearl_14jun2017*** under the Inventory Tab. The user clicks on the **Select User Datamine Report** button.



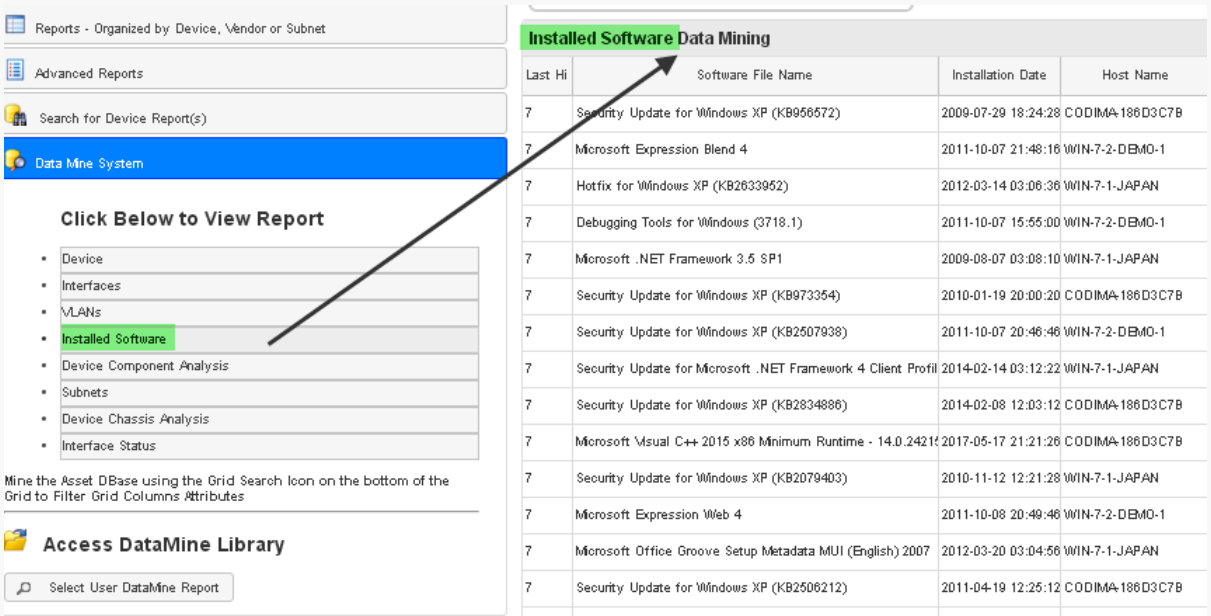
Above we see the Datamine Library Feature. In the picture above the user has clicked on 'XP SW' row in the Library Grid. The Grid **XP SW** is now shown listing the PCs running XP Software, see green highlights.



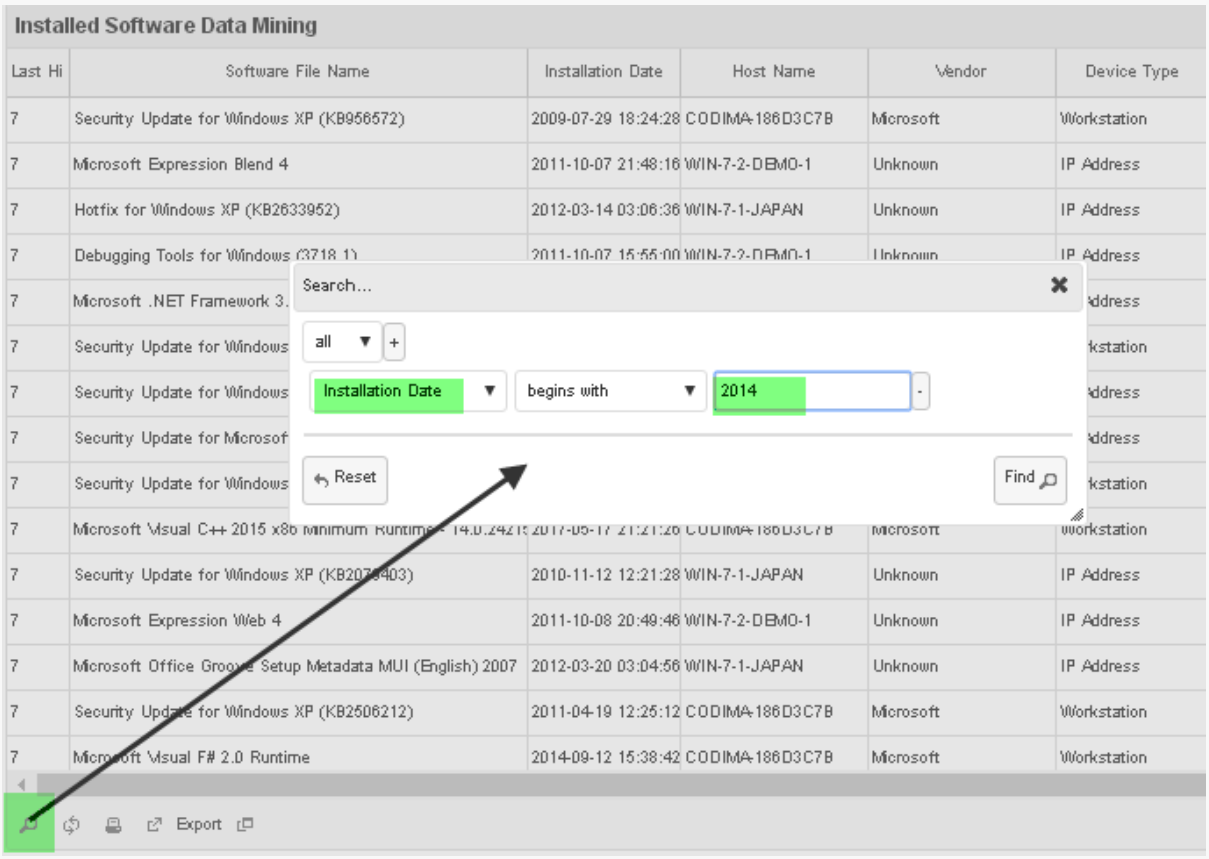
In the example above Gigabit Links have been selected from the Library and listed in the Datamining Grid.

To setup a New Search in the Library the steps below are followed:-

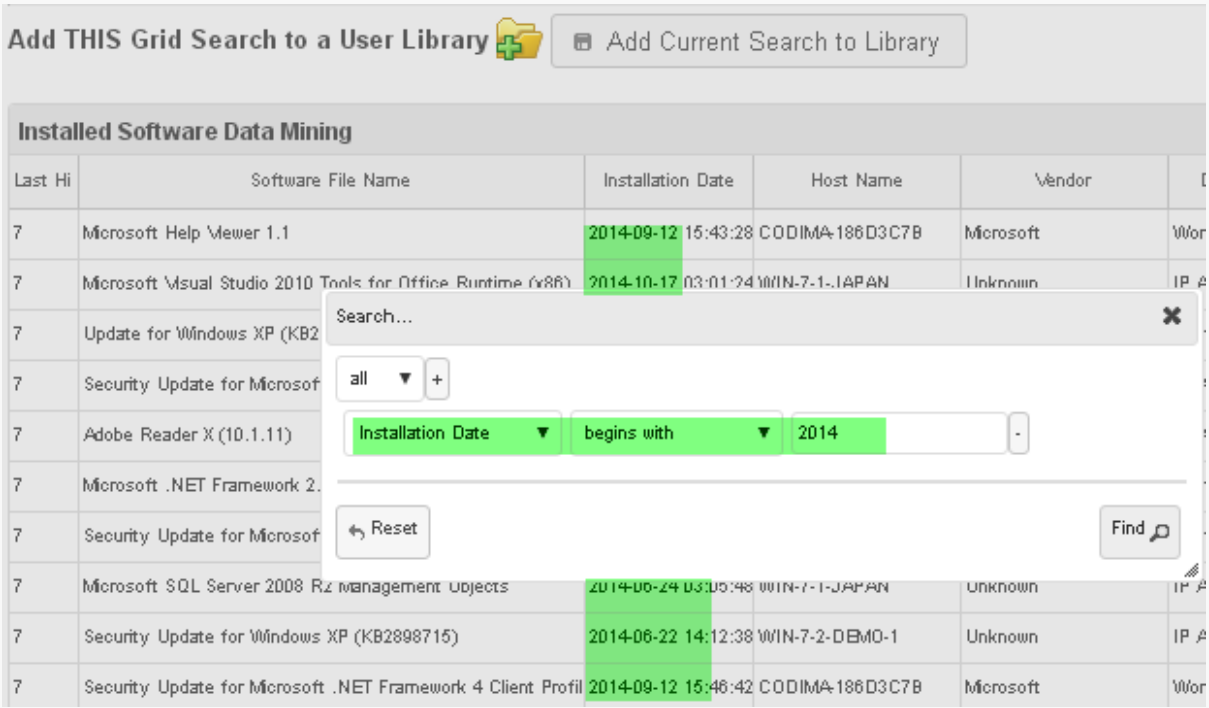
First do a Datamining search as normal e.g. 'Installed Software'



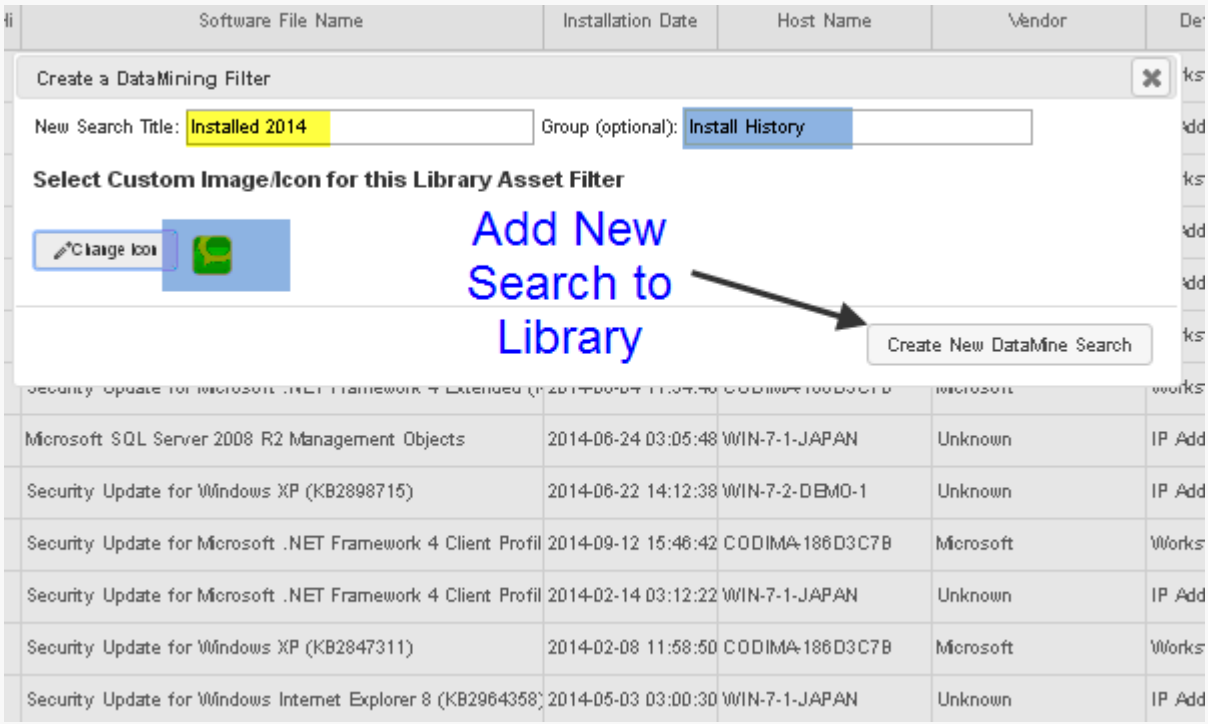
Next search this Grid as below, in this case for software installed in 2014: -



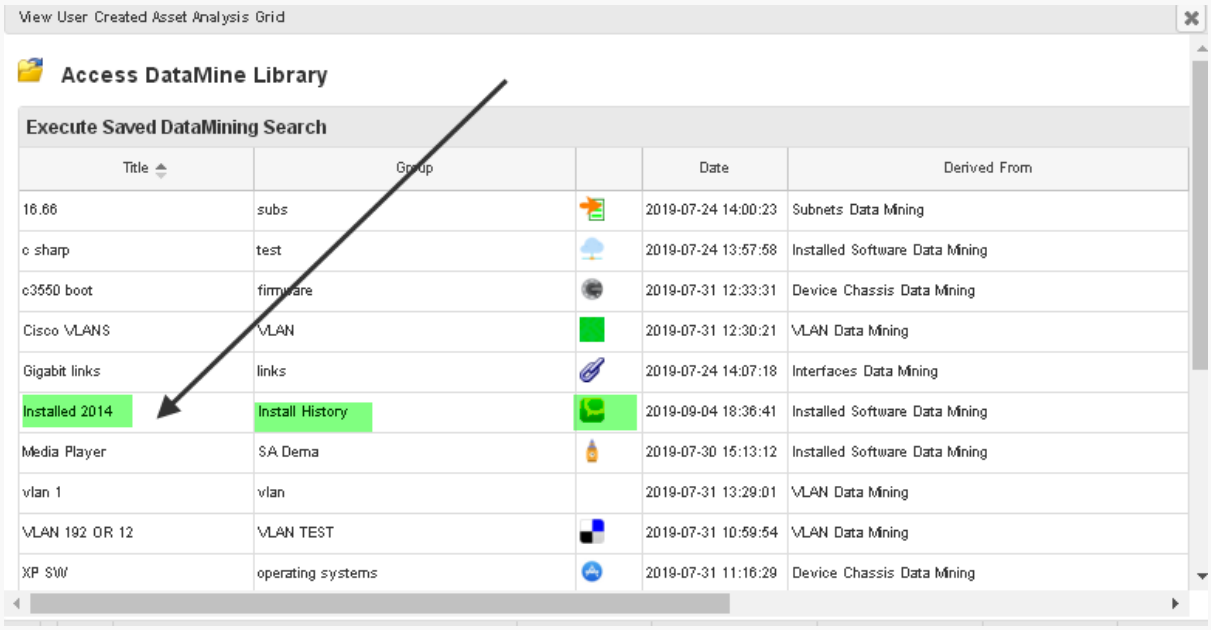
Clicking on the **Find** button creates a new grid below with install date 2014: -



Exit the Search dialog box:-



The new Library entry is filled in Installed 2014 and optional Group and Icon can be added if desired. Click on Create New Datamine Search to add to the library as below: -



The new Library entry is highlighted in green. Note a group and an Icon was added to this new entry.

Legacy Inventory 2013

Following a Network Discovery, then a MySQL Database is created containing a detailed list of Devices, Links and Software Installed. The differences between **Legacy Inventory and Mapping product (Windows GUI product), also called old inventory (pre-2013) and Legacy Inventory from 2013 (Web GUI)** are fully described below.

The two products share a Network Discovery Engine that is used to create an extensive database of Network Devices, Links, Installed Software and VLAN configurations.

The **Legacy Inventory and Mapping (old inventory pre-2013)** product is a windows-based GUI product and **Legacy Inventory 2013** is a pure Web GUI, that can be accessed remotely.

Legacy Inventory 2013 - Server Reports

There is an extensive range of Server Reports produced by both **Legacy Inventory and Mapping (old inventory pre-2013)** product and the **Legacy Inventory 2013**. The screenshots typically just show the first page of a report in the examples from the **Legacy Inventory and Mapping (old inventory pre-2013**) product below.

Summary

CODIMA-186D3C7B

- Details
- VoIP Details
- IP Interfaces
- Interfaces
- Devices Installed
- Disk Drives
- Software Installed
- Storage
- Tasks Running
- WMI CPU
- WMI Monitor
- WMI Disk
- WMI Printer
- WMI Service
- WMI Process
- WMI Hot Fixes

Details

Name	CODIMA-186D3C7B
IP address	10.25.3.50
Type	\oIP Server
Model	Windows Workstation
Manufacturer	Dell Inc.
Description	Hardware: x86 Family 6 Model 15 Stepping 11 AT/AT COMPATIBLE - Software: Windows 2000 Version 5.1 (Build 2600 Multiprocessor Free)
System Up Time	00:51:25.32
Serial Number	76487-771-0113574-22915
Physical Memory	3.25 GB
Tasks Running	89
Users	2
Bios Manufacturer	Dell Inc.
Bios Name	Phoenix ROM BIOS PLUS Version 1.10 A01
Bios Serial Number	
Bios Version	DELL - d
Computer Manufacturer	Dell Inc.
Computer Model	OptiPlex 755
Computer Owner	Codima
Computer User Name	CODIMA-186D3C7B\Phil
Organization	Codima
OS Language	1033

Installed Devices

Devices Installed

Type	Description	Status	Errors	Load (%)
Disk Storage	E:\	unknown	0	
Disk Storage	F:\	unknown	0	
Disk Storage	Fixed Disk	unknown	0	
Disk Storage	Fixed Disk	running	0	
Disk Storage	G:\Format is unknown	running	0	
Disk Storage	Unknown Media	running	0	
Keyboard	IBM enhanced (101- or 102-key) keyboard, Subtype=(0)	running	0	
Network	High Speed USB Ethernet Adapter - Packet Scheduler Miniport	unknown	0	
Network	Intel(R) 82566DM-2 Gigabit Network Connection - Packet Scheduler	unknown	0	
Network	MS TCP Loopback interface	unknown	0	
Parallel Port	LPT1:	unknown	0	
Pointing	3-Buttons (with wheel)	running	0	
Printer	HP Photosmart C4400 series	running	0	
Printer	Microsoft XPS Document Writer	running	0	
Printer	Send To Microsoft OneNote Driver	running	0	
Printer	SnagIt 8 Printer	running	0	
Printer	Snagit 9 Printer	running	0	
Processor	Intel	running	0	1
Processor	Intel	running	0	1
Processor	Intel	running	0	2
Processor	Intel	running	0	3
Serial Port	COM1:	unknown	0	
Serial Port	COM2:	unknown	0	
Serial Port	COM3:	unknown	0	

Disk Drives

Disk Drives

Type	Description	Capacity (GB)	Mode	Status	Removable	Errors
floppy Disk	F:\	0.0	read\Write	unknown	true	0
floppy Disk	G:\Format is unknown	1.9	read\Write	running	true	0
hard Disk	Fixed Disk	0.8	read\Write	running	false	0
hard Disk	Fixed Disk	0.0	read\Write	unknown	false	0
hard Disk	Unknown Media	1.9	read\Write	running	false	0
optical Disk ROM	E:\	0.0	read Only	unknown	true	0

Installed Software

Software Installed

Filename	Installed Date
32 Bit HP CIO Components Installer	2009-07-22 13:22:14
Acrobat.com	2008-11-14 09:14:34
Active@ ISO Burner	2009-12-23 17:59:20
ActivePerl 5.10.1 Build 1007	2010-06-01 14:32:18
Adobe AIR	2008-11-14 09:14:26
Adobe Flash Player 10 ActiveX	2011-02-18 10:37:30
Adobe Flash Player 10 Plugin	2011-03-03 08:29:58
Adobe Reader X (10.1.3)	2012-04-13 19:22:28
Adobe SVG Viewer 3.0	2009-11-24 17:50:14
Apple Application Support	2012-03-30 10:29:16
Apple Mobile Device Support	2012-03-30 10:30:34
Apple Software Update	2011-07-11 16:19:52
ATI - Software Uninstall Utility	2008-09-26 17:54:26
ATI Display Driver	2008-09-29 13:19:26
avast! Internet Security	2012-03-28 18:17:04
BitNami WAMPStack	2012-06-25 21:14:52
Bonjour	2011-10-12 17:21:58
BufferChm	2009-07-14 10:53:02
C4400_Help	2009-07-14 11:05:14
Cards_Calendar_OrderGift_DoMorePlugout	2009-07-14 10:55:36
CmdHere Powertoy For Windows XP	2008-09-29 11:09:00
Codima Spider	2012-06-25 21:19:36
Common Setup Files (3718.1)	2008-09-29 11:06:08
Copy	2009-07-14 10:54:12
Core SDK (Windows .NET Server RC2) (3718.1)	2008-09-29 11:06:02
Critical Update for Windows Media Player 11 (KB959772)	2009-07-29 16:23:48
CustomerResearchQFolder	2009-07-14 10:54:18
CVSNT	2008-09-29 11:27:22

Running Tasks

These are the tasks that were running at Discovery Time. The examples below are from the **Legacy Inventory and Mapping (old inventory, pre-2013)** product**.** The **Legacy Inventory 2013** product also has a Live list of running Services and Processes.

Tasks Running

Name	Path	Parameter	Type
afwServ.exe	C\Program Files\Alwil Software\Avast5\		application
alg.exe	C\WINDOWS\System32\		application
AppleMobileDeviceService.exe	C\Program Files\Common Files\Apple\Mobile Device Support\		application
ati2evxx.exe	C\WINDOWS\system32\		application
ati2evxx.exe		-Client	application
autoMapJ.exe		-Xmx384m DnaEngine autoCleanLog nolog	application
AvastSvc.exe	C\Program Files\Alwil Software\Avast5\		application
AvastUI.exe	C\Program Files\Alwil Software\Avast5\	/nogui	application
c2c_service.exe	C\Documents and Settings\All Users\Application Data\Skype\Toolbars\Skype C2C Service\		application
chrome.exe	C\Program Files\Google\Chrome\Application\	--type=gpu-process --channel="4504.1.252849704\1174402135" --use-gl=swiftshader --swiftshader-path="C\Documents and Settings\P	application
chrome.exe	C\Program Files\Google\Chrome\Application\		application
chrome.exe			application
cidaemon.exe		DownLevelDaemon "c\inetpub\catalog.wci" 196672l 1040l	application
cidaemon.exe		DownLevelDaemon "c\documents and settings\all users\application data\microsoft\visio\catalog.wci" 196672l 1040l	application
cisvc.exe	C\WINDOWS\system32\		application
cmd.exe			application
csrss.exe	C\WINDOWS\system32\	ObjectDirectory=\Windows SharedSection=1024,3072,512 Windows=On SubSystemType=Windows ServerDll=basesrv,1 ServerDll=winsrv:UserS	application

WMI – Windows Management Interface

WMI Monitor

Description	DeviceId	Manufacturer	ScreenHeight	ScreenWidth	Type
Plug and Play Monitor	DesktopMonitor1	(Standard monitor types)	1080	1920	Plug and Play Monitor
Default Monitor	DesktopMonitor2				Default Monitor

Top of table • Top of page

WMI Disk

Capacity (GB)	Description	Drive	FileSystem	FreeSpace (GB)
68.4	Local Fixed Disk	C:	NTFS	10.2
164.5	Local Fixed Disk	D:	NTFS	7.5
	CD-ROM Disc	E:		
	Removable Disk	F:		
1.9	Removable Disk	G:	FAT	0.0

Top of table • Top of page

WMI Printer

Caption	Driver	Hres	Port	Share	VRes
Snagit 9	Snagit 9 Printer	200	C:\Documents and Settings\All Users\Application Data\TechSmith\Snagit 9\PrinterPortFile		200
SnagIt 8	SnagIt 8 Printer	200	C:\Documents and Settings\All Users\Application Data\TechSmith\SnagIt 8\PrinterPortFile		200
Send To OneNote 2007	Send To Microsoft OneNote Driver	300	Send To Microsoft OneNote Port:		300
Microsoft XPS Document Writer	Microsoft XPS Document Writer	600	XPSPort:		600
HP Photosmart C4400 series	HP Photosmart C4400 series	600	USB001		600

Services Running

WMI Service

Caption	Description	DisplayName	Install Date	Name	PathName
Alerter	Notifies selected users and computers of administrative alerts. If the service is stopped, programs that use administrative alerts will not receive them. If this service is disabled, any services that explicitly depend on it will fail to start.	Alerter		Alerter	C:\WINDOWS\system32\svchost.exe -k LocalService
Application Layer Gateway Service	Provides support for 3rd party protocol plug-ins for Internet Connection Sharing and the Windows Firewall.	Application Layer Gateway Service		ALG	C:\WINDOWS\System32\alg.exe
Apple Mobile Device	Provides the interface to Apple mobile devices.	Apple Mobile Device		Apple Mobile Device	"C:\Program Files\Common Files\Apple\Mobile Device Support\AppleMobileDeviceService.exe"
Application Management	Provides software installation services such as Assign, Publish, and Remove.	Application Management		AppMgmt	C:\WINDOWS\system32\svchost.exe -k netsvcs

Processes Running

WMI Process

Caption	CommandLine
System Idle Process	
System	
smss.exe	\SystemRoot\System32\smss.exe
csrss.exe	C:\WINDOWS\system32\csrss.exe ObjectDirectory=\Windows SharedSection=1024,3072,512 Windows=On SubSystemType=Windows ServerDll=bas ServerDll=winsrv:UserServerDllInitialization,3 ServerDll=winsrv:ConServerDllInitialization,2 ProfileControl=Off ...
winlogon.exe	winlogon.exe
services.exe	C:\WINDOWS\system32\services.exe
lsass.exe	C:\WINDOWS\system32\lsass.exe
ati2evxx.exe	C:\WINDOWS\system32\Ati2evxx.exe
svchost.exe	C:\WINDOWS\system32\svchost -k DcomLaunch

Security Updates

Update	Security Update for Windows Internet Explorer 8 (KB2183461)	KB2183461-IE8	SP0
Update	Security Update for Windows Internet Explorer 8 (KB2360131)	KB2360131-IE8	SP0
Update	Security Update for Windows Internet Explorer 8 (KB2497640)	KB2497640-IE8	SP0
Update	Security Update for Windows Internet Explorer 8 (KB2510531)	KB2510531-IE8	SP0
Update	Security Update for Windows Internet Explorer 8 (KB2544521)	KB2544521-IE8	SP0
Update	Security Update for Windows Internet Explorer 8 (KB2586448)	KB2586448-IE8	SP0
Update	Security Update for Windows Internet Explorer 8 (KB2699988)	KB2699988-IE8	SP0
Update	Security Update for Windows Internet Explorer 7 (KB938127-v2)	KB938127-v2-IE7	SP0
Update	Security Update for Windows Internet Explorer 7 (KB953838)	KB953838-IE7	SP0
Update	Security Update for Windows Internet Explorer 7 (KB969897)	KB969897-IE7	SP0
Update	Security Update for Windows Internet Explorer 8 (KB971961)	KB971961-IE8	SP0
Update	Security Update for Windows Internet Explorer 8 (KB972260)	KB972260-IE8	SP0
Update	Update for Windows Internet Explorer 8 (KB972636)	KB972636-IE8	SP0
Update	Security Update for Windows Internet Explorer 8 (KB976325)	KB976325-IE8	SP0
Update	Update for Windows Internet Explorer 8 (KB976662)	KB976662-IE8	SP0
Update	Security Update for Windows Internet Explorer 8 (KB978207)	KB978207-IE8	SP0
Update	Security Update for Windows Internet Explorer 8 (KB981332)	KB981332-IE8	SP0
Update	Security Update for Windows Internet Explorer 8 (KB982381)	KB982381-IE8	SP0
Update	Security Update for Microsoft Windows (KB2564958)	KB2564958	SP10
Update	Microsoft Compression Client Pack 1.0 for Windows XP	MSCompPackVI	SP10
Service Pack	Windows XP Service Pack 3	KB936929	SP3
Update	Security Update for Windows XP (KB2079403)	KB2079403	SP4
Update	Security Update for Windows XP (KB2115168)	KB2115168	SP4
Update	Security Update for Windows XP (KB2121546)	KB2121546	SP4
Update	Security Update for Windows XP (KB2124261)	KB2124261	SP4
Update	Update for Windows XP (KB2141007)	KB2141007	SP4
Update	Hotfix for Windows XP (KB2158563)	KB2158563	SP4
Update	Security Update for Windows XP (KB2160329)	KB2160329	SP4
Update	Security Update for Windows XP (KB2229593)	KB2229593	SP4
Update	Security Update for Windows XP (KB2259922)	KB2259922	SP4

Differences: Legacy Inventory 2013 and old inventory (pre-2013) - information from 2013

Legacy Inventory 2013 produces a large HTML Web report divided into sections for Devices, Installed software, etc as its output. The web reports contain a fully linked drill down as below, with summaries.

codima

CODIMA-186D3C7B

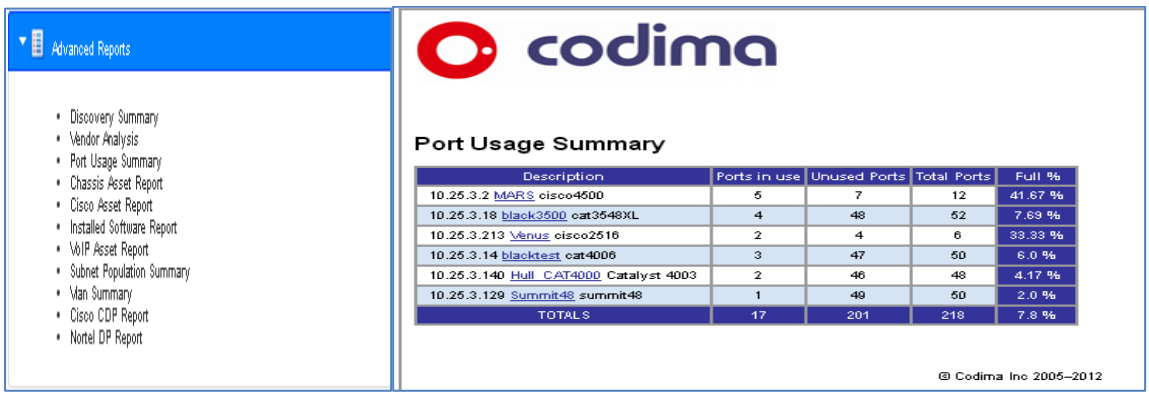
- Details
- VoIP Details
- IP Interfaces
- Interfaces
- Devices Installed
- Disk Drives
- Software Installed
- Storage
- Tasks Running
- WMI CPU
- WMI Monitor
- WMI Disk
- WMI Printer
- WMI Service
- WMI Process
- WMI Hot Fixes

Details

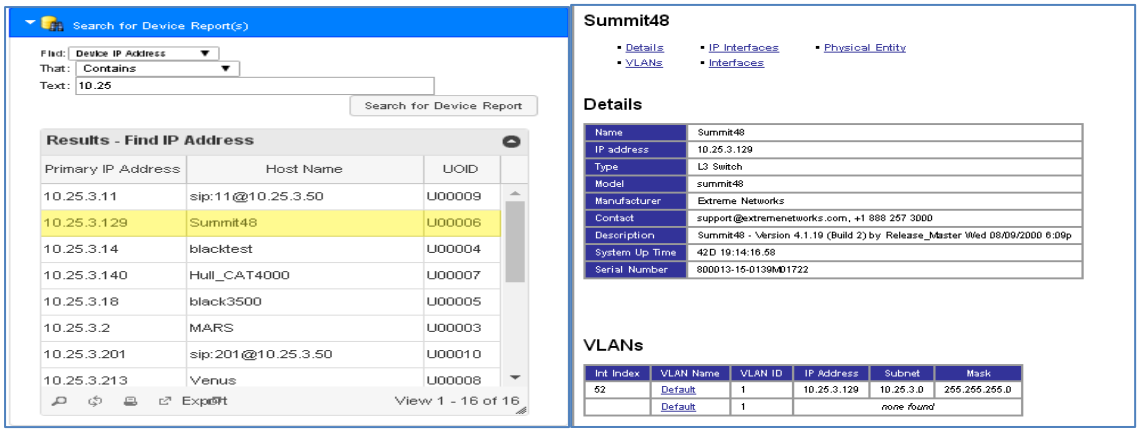
Name	CODIMA-186D3C7B
IP address	10.25.3.50
Type	\VoIP Server
Model	Windows Workstation
Manufacturer	Dell Inc.
Description	Hardware: x86 Family 6 Model 15 Stepping 11 AT/AT COMPATIBLE - Software: Windows 2000 Version 5.1 (Build 2600 Multiprocessor Free)
System Up Time	00:51:25.32
Serial Number	76487-771-0113574-22915
Physical Memory	3.25 GB
Tasks Running	89
Users	2
Bios Manufacturer	Dell Inc.
Bios Name	Phoenix ROM BIOS PLUS Version 1.10 A01
Bios Serial Number	
Bios Version	DELL - d

Legacy Inventory 2013 builds on old Inventory (pre-2013) product in that it retains access to the Web Report, but it adds a whole array of extra features as below:

In Legacy Inventory 2013 there is direct access to Advanced Reports.

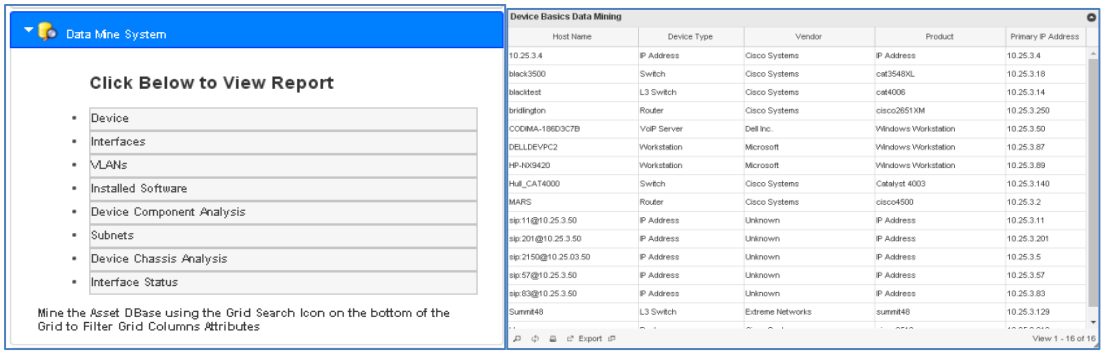


Legacy Inventory 2013 has a search facility unlike the old Inventory.



In **Legacy Inventory 2013** a device can be tracked down using multiple search criteria then produce a summary.

Legacy Inventory 2013

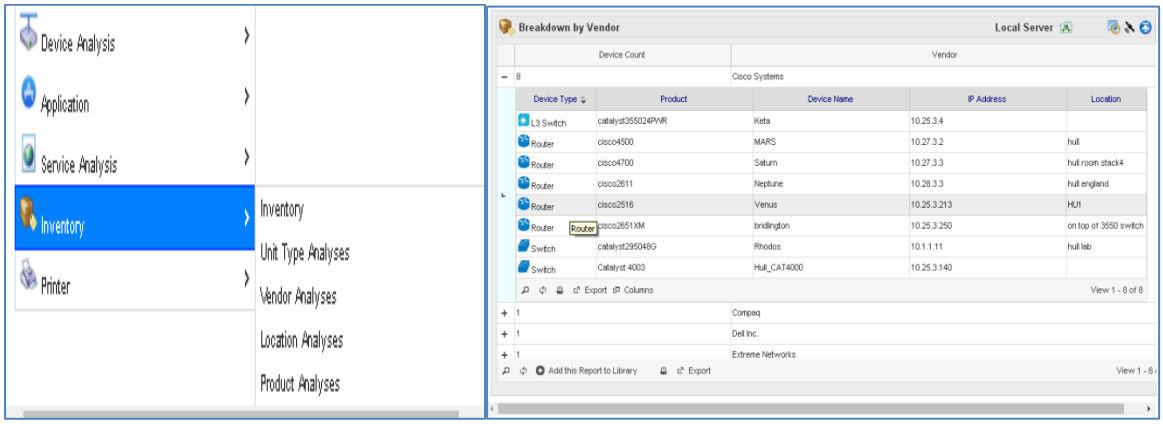


Unlike the old Inventory (pre-2013), the **Legacy Inventory 2013** can search the Discovery Database Directly. This is extremely useful to search for Chassis Numbers or produce summaries of Installed Software and Patches for example. The Toolbox Grids are extra powerful with Search, Sort and Filter based on complex criteria.

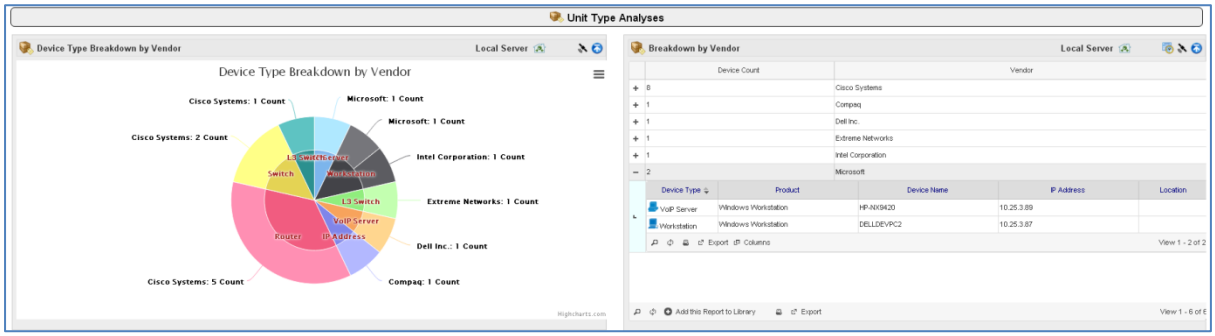
The old inventory (pre-2013) product, in contrast, only processes static HTML reports.

Legacy Inventory 2013 Dynamic Inventory

Unlike old inventory (pre-2013) product, the **Legacy Inventory 2013** boasts fully **dynamic** reports as below:



The reports can be filtered by the **Legacy Inventory 2013** GUI to create new specialised reports, perhaps, based on device location or manufacturer etc. Search, Filter, Sort and direct export to file or printer are supported – unlike Legacy Inventory and Mapping Toolbox (pre-2013) product.



The **Legacy Inventory 2013** inventory creates a large set of Dash Reports with both Donut charts and matching Multi-level Grids reports as above.

Summary: Legacy Inventory 2013

The **Legacy Inventory 2013** product builds on the old inventory (pre-2013) but adds a whole range of new functionality in its dynamic search capabilities and fully customisable extra sets of Reports. **Legacy Inventory 2013** is, of course, a pure web product so, is naturally remotely accessible from a range of devices like tablets.