Getting Started with Asset Manager - Discovering Assets

CSE Asset Manager and Service Manager have an enormous number of powerful features, and these short introductory guides cannot cover all of them. The purpose of them is to get you started, and lead you to discover more about the features and facilities at your own pace.

If you need help please ask, either by emailing assetmanager@cse-net.co.uk, or telephoning 01993 886688 and asking for Asset Manager support.

To support your exploration of the system further, we have produced a number of application notes that go into greater detail on specific functions. These can be downloaded from our Asset Manager microsite at www.cseassetmanager.co.uk or can be accessed directly within the demo system by going to the Download section.

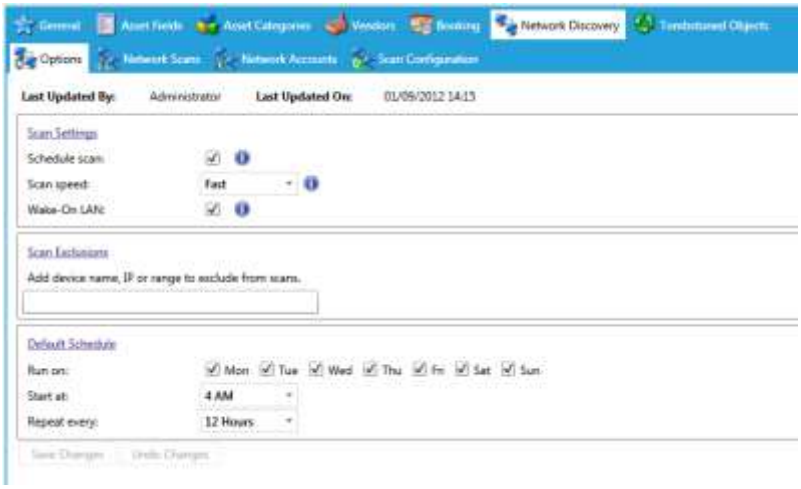
This guide covers using the system to manage your assets.

Network Discovery

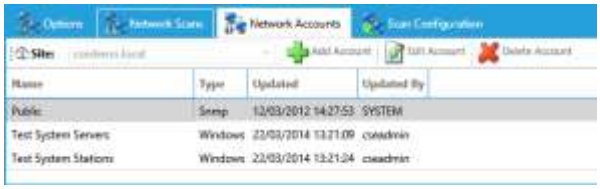
Unfortunately the one thing that the demo system can't really demonstrate is live asset discovery. Whilst the demo system is a 'real' Asset Manager server, for security reasons it is hosted outside any network. However, you can still use the system to explore how network scanning is performed and configured.

This guide therefore covers how to setup scans and run them, and how to monitor their progress.

Navigate to *Preferences*/*Asset Manager Settings* and click on the *Network Discovery* tab.



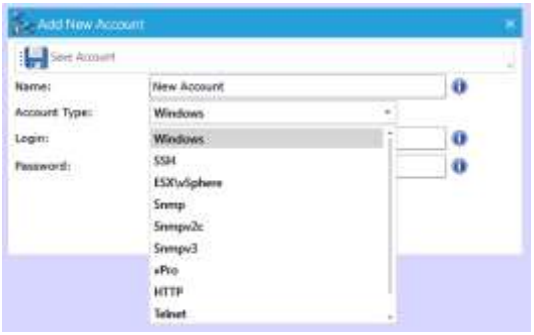
First, click on *Network Accounts* as this needs a little explanation.



As you can see there are a number of separate accounts already configured.

These are the usernames and passwords used to authenticate with devices connected to the network. Most devices being scanned will require some form of authentication in order to gather information from them. It's easy to understand the purpose of this security feature: you don't want just anyone to access your devices and gather information from them.

Click on *Add Account* and expand the account type list box. This gives you an idea of the types of systems asset manager connects to, and ultimately probes and extracts asset information from.



The most important methods (protocols) for querying a remote device to determine its characteristics are SNMP (Simple Network Management Protocol), WMI (Windows Management Instrumentation) and SSH (Secure Shell).

SNMP is the oldest and the most common protocol used to query and manage peripheral devices such as switches, printers, and wireless access points. Being one of the older systems, it has evolved over time to take into account the evolution of devices. SNMP v1 is still in common use, as it provided the baseline system that many vendors adopted. It is still an important protocol and is probably the most common implementation. SNMP v1 differs from subsequent versions in that it requires no authentication in order to be able to access a device. Subsequent versions, v2, v2c and v3 introduced better security features, including the need for authentication.

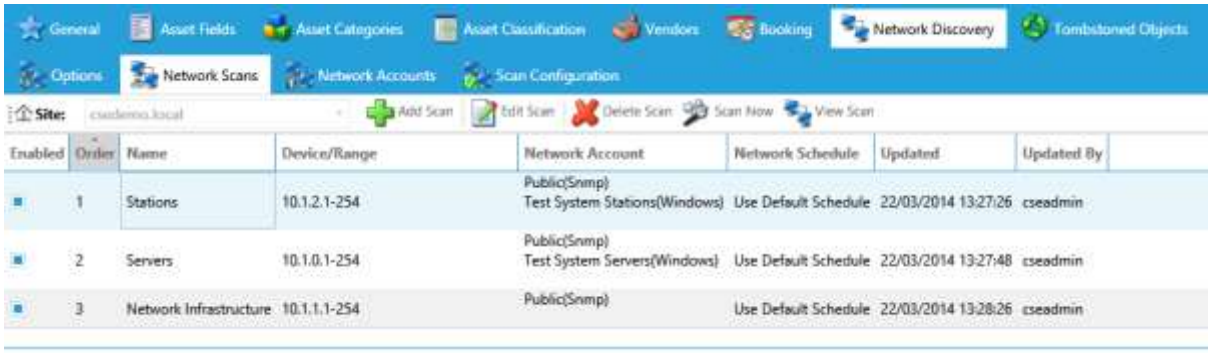
WMI is Microsoft's implementation of Web-Based Enterprise Management (WEBM) and Common Information Models (CIM) standards. It provides a mechanism by which a remote system can run specific queries against a remote Windows based computer to extract management information. To query a remote computer, you are required to authenticate yourself before being given access to the management database every Windows based computer maintains.

SSH is a secure mechanism mostly used to access UNIX and Linux-based systems remotely. The system is akin to providing a remote console from which you can run commands and thus gather information about the remote system. Most notably, Apple iOS supports SSH.

The remaining protocols are simply additional ways of connecting to and querying remote systems. For the time being, these are outside of the scope of this document.

This information about protocols, remote systems and running queries to gather information from devices may seem complicated, and in fact it is. However one of Asset Manager's great strengths in asset discovery is that most, if not all, of the hard work has been done for you. The system is supplied preconfigured and will run straight out of the box. The most complicated thing that you will have to do is to specify the correct user names and passwords.

Click on the *Network Scans* tab.



Displayed within the table are our predefined network scans. You can see the IP addresses configured, which network accounts are assigned to each one, and what the schedule is.

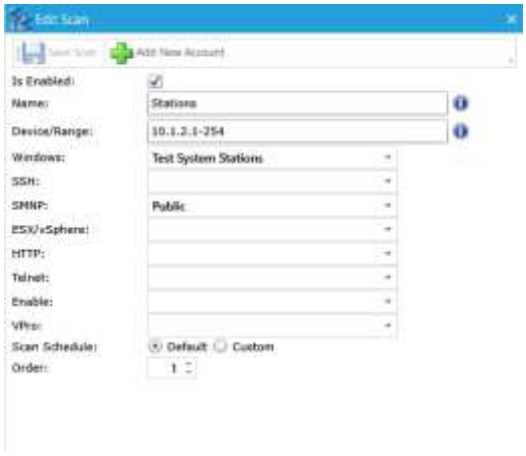
You may wonder why there is not a configured scan that covers the entire internal IP address range of the network. There are several reasons why it is best to avoid doing that.

First: system performance. Scanning an entire IP subnet takes time, and if run during working hours it could affect the performance of your system. This in itself is good enough reason to avoid doing it.

Second, it is very likely that your system has a segmented IP address range. What we mean by this is that your system has distinct IP address ranges in which certain categories of devices are located. For instance all servers are within the range 10.1.0.1 – 254, switches between 10.1.1.1.1 – 254 and so on. It makes some sense to create scans that broadly follow your IP addressing conventions.

Third, some devices don't change very often and don't need to be scanned on a regular basis. Other devices, such as printers, might benefit from being scanned several times a day in order to detect problems (such as running out of toner, or even running out of paper!)

Double click on one of the predefined scans to open its details page.



Is Enabled effectively switches on the scheduled scanning option. Scheduled scans can either use default settings or can be customised.

The IP address range can be entered in a number of different ways. Click the information icon and see the different formats available.

The remaining protocol settings allow you to specify the various network accounts to be used within this scan. You can use the appropriate list boxes to select from your preconfigured network accounts.

Whilst opportunities to perform network discovery scans using the demo system are limited, we can set up a scan of the demo server itself.

Navigate to *Preferences/Asset Manager Settings/Network Discovery* and click on the *Network Scans* tab.

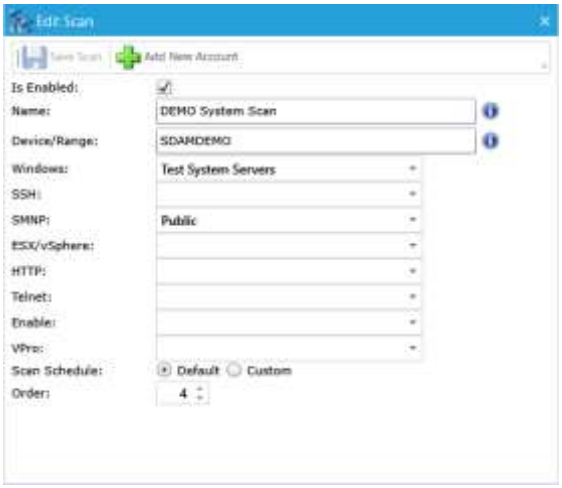
Click on the *Add Scan* button.

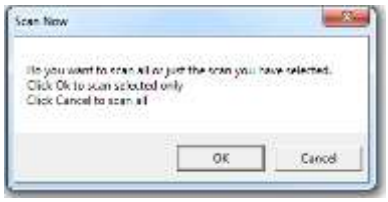
Rather than enter an IP address, we will use the server's name – enter *AMDEMO* in the Device/Range box.

In the Windows account selection box, select *Test System Servers*.

Then click *Save Scan.*

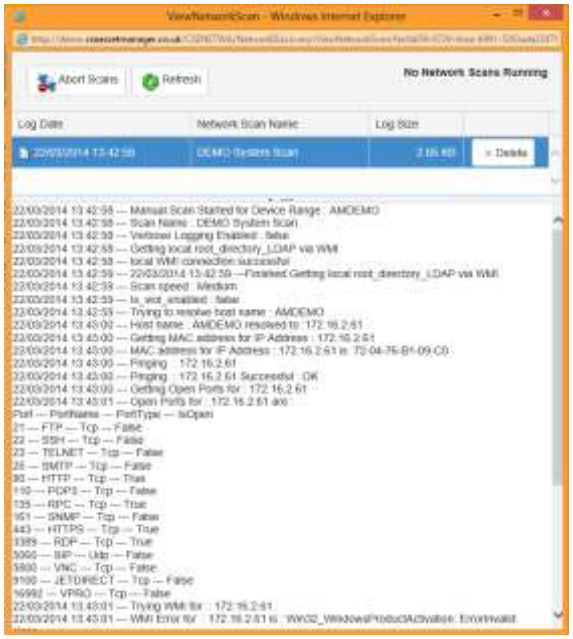
Click on the *SDAMDEMO* table entry and highlight it and then click *Scan Now*.





We only want to run this single job, so click on OK.

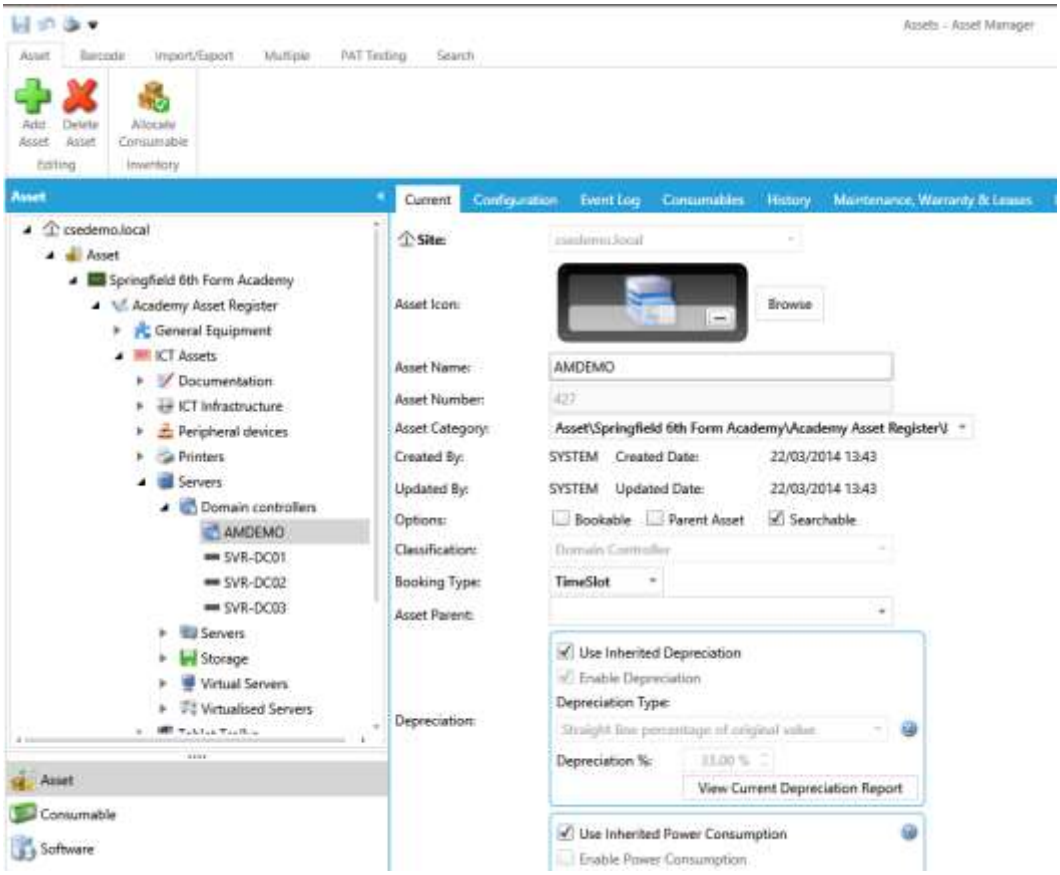
Please Note: you will need to make sure that you browser has been configured to allow pop-up windows from demo.cseassetmanager.co.uk.



Wait half a minute to let the scan get going and then click on the *View Scan* tab. This opens up what is essentially a diagnostic aid that allows the results of your discovery scans to be checked minutely, step by step. Usually this information would only be used to help debug issues, but we are using it here to demonstrate the actual scan process.

Click the small plus sign against the last entry in the table. You can now see the exact scan process, line by line.

Let the scan finish, then look at the *Domain Controller* category under *Asset Manager*.



Here are the results of the discovery scan, imported into the database as *AMDEMO*.

Check the various tabs like *History* – notice that the time and date stamp corresponds approximately to the time you ran the scan.

Check the *Notifications* tab. See that several emails have been generated. In particular, notice the last one indicating that the system thinks that Microsoft Server 2008 R2 is not compliant.

Check the *Software & Services* tab. Notice that Microsoft Windows Server 2008 R2 has picked up a license key, but it has not been verified.