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.

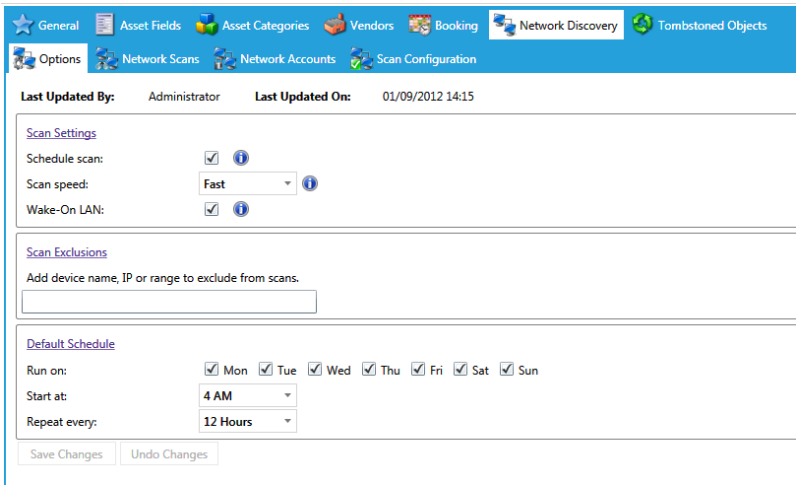
Network Discovery

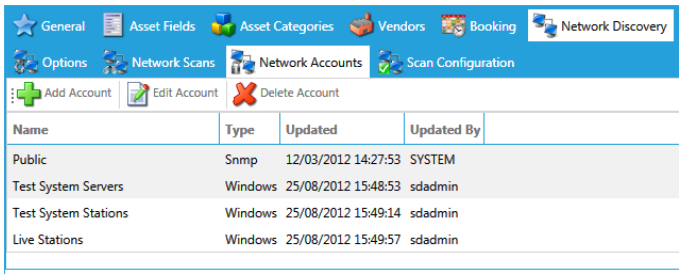
Unfortunately the one thing that the demo system can't really be used for is live asset discovery. Whilst the system is a real asset manager server, for security reasons it is hosted outside of any network. However we can still use the system to look at how network scanning is performed and configured.

We have a separate application note that describes Network Discovery in greater detail. If you want to know how everything behind the scenes works, then we suggest that you obtain a copy and examine it in detail.

This guide only covers how to setup scans, 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 will require any service trying to read information about them to authenticate itself. This is a security feature and one that is very easy to understand: you don't want just anyone being able to access your devices and gather information from them unchallenged.

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 (called protocols) of 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 to-day as it provided the baseline system that many vendors adopted. It is still an important protocol and is probably the most common implementation. SNMP versions 1 differs from subsequent versions in that it required 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.

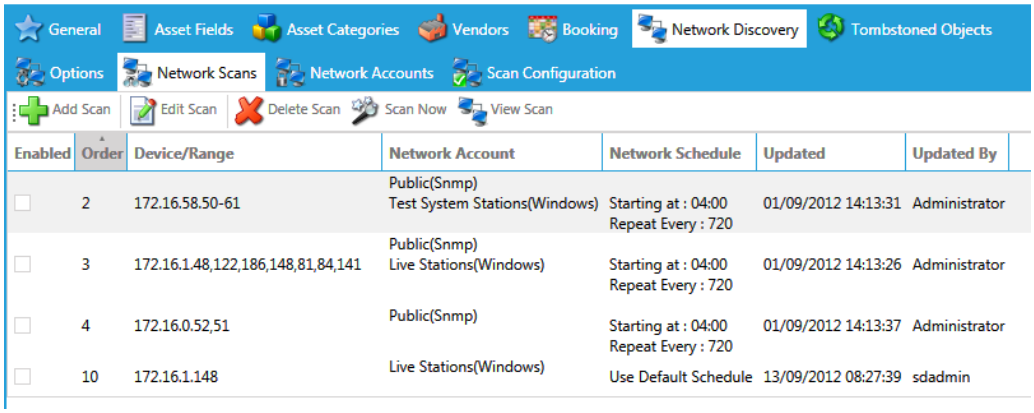
WMI is Microsoft's implementation of Web-Based Enterprise Management (WEBM) and Common Information Models (CIM) standards. It provides a mechanism by which a remote system can run specific queries against a remote Windows based computer with the aim of extracting management information. To query a remote 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 used to remotely access mostly UNIX and Linux-based systems. 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.

All this talk about protocols, remote systems and running queries to gather information from devices sounds pretty complicated, and truth be told, it is. However, and this is where Asset Manager's strengths in terms of scanning devices comes into play; most, if not all of the hard work has been done for you. The system comes preconfigured and will run straight out of the box. The most complicated thing that you will have to do is specify the correct user names and passwords.

Click on the *Network Scans* tab.



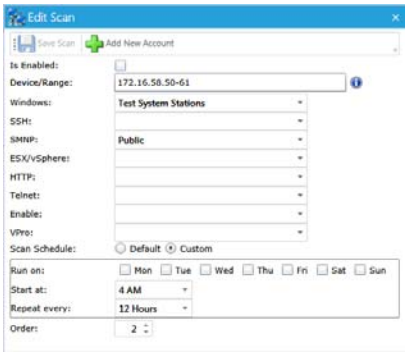
Displayed within the table are our predefined network scans. You can see the IP addresses configured, which network accounts are assigned to each one, and what the schedule is.

You might be wondering why we just don't configure a scan that covers the entire internal IP address range of our network. There are a couple of reasons why it is best to avoid doing that.

First is simply a consideration in terms of system performance. Scanning an entire IP subnet takes time, and if run during working hours 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 where certain categories of devices are located. For instance all servers are within the range 169.122.200.1 – 128, switches between 169.122.201.1-128, WAP 169-122.201.129-254, 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 pick up on situations like running out of toner or even running out of paper!



Segmented scanning therefore has a lot of merit.

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

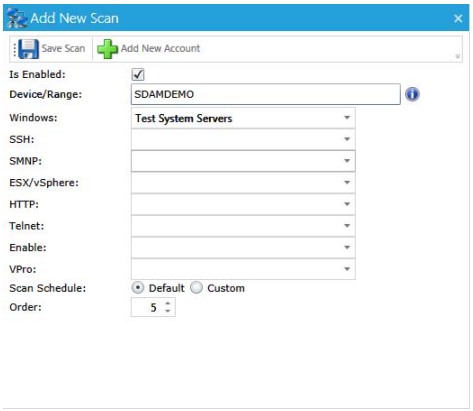
Is Enabled effectively switches on the scheduled scanning option. Scheduled scans can either use default settings or can be custom.

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 that are going 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.



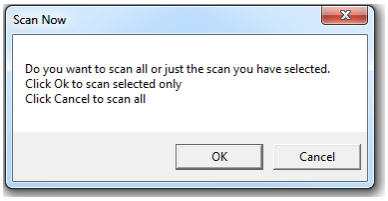
Click on the *Add Scan* button.

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

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

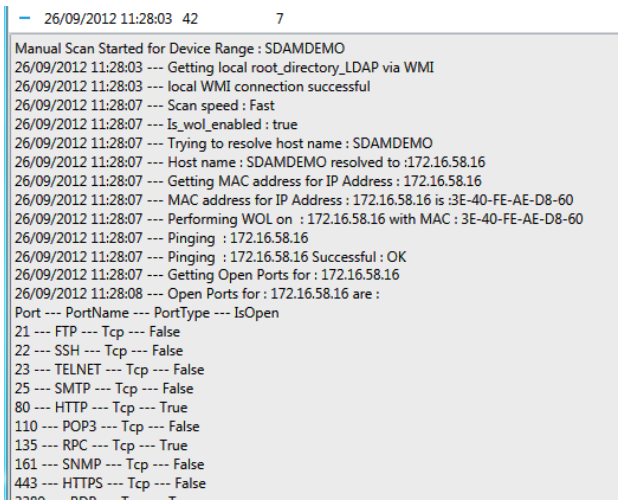
Then click on *Save Scan.*

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



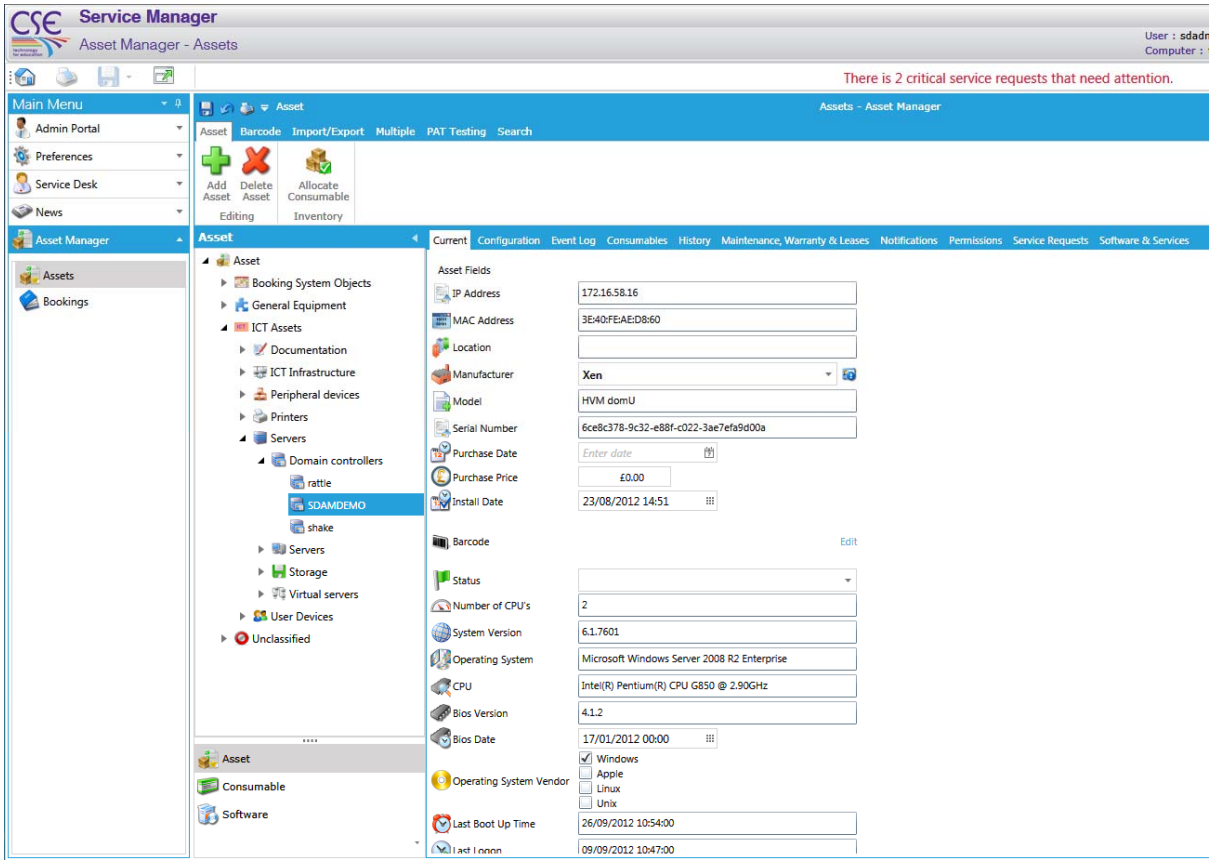
We only want to run this single job, so click on OK.

Wait half a minute to let the scan get going and then click on the *View Scan* tab. This opens up what is in essence a diagnostic aide that allows the results of your discovery scans to be minutely checked over 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 on 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 and then go and look at the *Domain Controller* category under *Asset Manager*.



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

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