HP OpenView Enterprise Discovery

Software Version: 2.1

Planning Guide

Document Release Date: July 21 2006
Software Release Date: July 21 2006

Legal Notices

Warranty

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

Restricted Rights Legend

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright Notices

Trademark Notices

Microsoft® and Windows® are U.S. registered trademarks of Microsoft Corporation.

Contents

1 An Overview of Enterprise Discovery

Enterprise Discovery™ collects large amounts of data about your network and devices. It can discover devices on its own by working its way through a list of IP ranges that you provide and can also collect detailed data from devices using configurable Scanners.

From a data-gathering perspective, Enterprise Discovery performs three distinct functions:

- Discovery
- Inventory
- Software Utilization

The following diagram shows the type of data collected by each of these functions.

Device	
Discovery	• Type • IP/MAC • Ports • Name
Inventory	• Disk Configuration • Asset Tag • Monitor Information • Services • Software Licenses
Software Utilization	• Usage information

Further Information

You can find a detailed technical description of how Enterprise Discovery works in the *Reference Guide*.

Discovery

As a starting point, Enterprise Discovery needs to determine what devices are in your network and gather basic information about each of them. This process is referred to as Discovery and allows you to get a good overview of the number and types of devices in your network, as well as a basic set of attributes for each. It also servers as the foundation for the other modules of Enterprise Discovery.

Discovery is based on ranges of IP addresses. For each IP range in your network, Enterprise Discovery can use a variety of methods to discover devices, allowing you to use choose the appropriate settings for different groups of devices. For example, UNIX servers in the data centre may have different requirements for Discovery than laptops in the Finance group.

For an initial discovery setup, it is normally sufficient to define a small set of big IP ranges - and then fine-tune the setup later as you discover ranges of devices that need to be treated differently in some way.

To deal effectively with very large networks, more than one Enterprise Discovery server can be deployed in an organization, typically organized by geographical location. An additional server can then be designated to aggregate the results from all of the other servers through a process called Aggregation. It would then be possible for example, to run the results from each Enterprise Discovery Server to one central repository database (such as AssetCenter).

Inventory

After discovering a device, Enterprise Discovery can run a Scanner on it to gather detailed hardware, configuration and software license information. This process is referred to as Inventory and makes it possible to drive standardization and compliance initiatives, manage risk, implement chargeback policies, etc.

The Scanners can be launched automatically according to a configurable schedule, allowing complete control over network bandwidth usage and any impact on the end-user.

In order to manage the Scanners, the HP OpenView Discovery Agent needs to be in place. This is a small program that runs all the time and deals with security and communications. The Agent can be automatically deployed to Windows machines in your network, and must be manually deployed to UNIX machines. Once this is done, Enterprise Discovery can automatically upgrade the Scanners and agents when necessary.

Enterprise Discovery includes Agents and Scanners for most common desktop and server operating systems.

Software Utilization

On Windows machines, Enterprise Discovery can gather information about what software is used. This is referred to as Software Utilization and the information collected is necessary to optimize software license cost, for example by eliminating unused or under-utilized software installations.

The Software Asset Management module of AssetCenter 4.4 or later is ideal for performing the analysis of the data collected by Enterprise Discovery.

2 Preparing Your Network for Discovery

There are several steps you can take to prepare your network for using Enterprise Discovery.

Turn on SNMP management in all routers and core switches

Depending on the device, this may be a case of enabling an existing SNMP agent or setting up an SNMP agent.

You may also turn on SNMP management in other devices. The more managed devices in your network, the better. However, enable switches and routers first.

If you use HSRP (Hot Standby Routing Protocol) in your network, ensure you turn on SNMP management in all the affected devices.

What if you don't turn on SNMP management in your switches and routers?

- Enterprise Discovery will appear to work, but you'll eventually notice that it is working poorly. Once Enterprise Discovery is up and running, the Exceptions reports can advise you of problems. Much of the information that Enterprise Discovery collects comes from the SNMP MIB of devices in your network, so it is crucial that you enable SNMP management.

How do you turn on SNMP management?

- The exact procedure is different for every device. Consult the documentation that came with your switch or router.

  When you turn on SNMP management in a device, you often assign a community string (for SNMPv1/v2) or a user (for SNMPv3). If you assign a new string later, be sure you give the community string/user information to Enterprise Discovery. For more information, see About SNMP Configuration on page 8.

(Optional) Turn on SNMP management in other devices

Your decision to turn on SNMP management in your remaining switches, hubs, servers and workstations depends on the results you expect from Enterprise Discovery. For example, in many networks, monitoring the performance of workstations is not important.

Set DHCP lease time

If you use DHCP (Dynamic Host Configuration Protocol) in your network, set the IP address lease time to at least 7 days and turn on SNMP management on the DHCP servers.

About SNMP Configuration

A community string (SNMPv1/v2) or a user (SNMPv3) is like a password. A device uses a community string/user to protect its SNMP MIB—and it's the data from the SNMP MIB that Enterprise Discovery relies on. Enterprise Discovery must know at least one of a device's passwords to collect data from that device. If you do not give Enterprise Discovery a device's community string/user, Enterprise Discovery will behave as though the device does not have SNMP management turned on. Enterprise Discovery will appear to work, but you'll eventually notice that it is working poorly. Once Enterprise Discovery is up and running, the Exceptions reports can advise you of problems.

Community strings are case-sensitive. "Public" and "public" are two different strings.

Directed community strings

Directed community strings give devices another layer of protection: a list of IP addresses of approved devices. When Enterprise Discovery tries to get information from a device with a directed community string, the device asks not only "What's the password?" but also "Are you on the list?"

Give the Enterprise Discovery server's IP address to all devices using directed community strings

When directed community strings are used, it is not enough to give Enterprise Discovery access to the device. You must also configure the device to recognize the Enterprise Discovery server. You must put it on the list of approved devices.

What happens if a device with directed community strings is not configured with the IP address of the Enterprise Discovery server?

1. Enterprise Discovery will behave as though the device does not have SNMP management turned on. Enterprise Discovery will appear to work, but you'll eventually notice that it is working poorly. Once Enterprise Discovery is up and running, the Exceptions reports can advise you of problems.

(Optional) Adjust bridge aging

To improve the reliability and speed of Enterprise Discovery, adjust bridge aging on your bridges, routers, switches, and concentrators. Turn bridge aging on, and set the bridge aging interval to 2-6 hours. Smaller networks can use shorter intervals; larger networks will need longer intervals. Enterprise Discovery's Exceptions reports can tell you which devices should have their bridge aging adjusted.

Plan the device and port to which the Enterprise Discovery server will be attached

Plan to attach the server:

- behind your corporate firewall
- to an Ethernet port on a device close to the top of your network. Enterprise Discovery works best if the port is SNMP managed.

Server Ports

Firewall Ports

Enabling these firewall ports will allow Enterprise Discovery system to perform through a corporate firewall.

If you have a corporate firewall that could impede Enterprise Discovery, configure the corporate firewall to allow ICMP (ping) to pass through, and enable the following ports:

Table 1 Firewall Ports

Used for	Port	Note	From	To
Echo Reply	0/icmp		device	Enterprise Discovery server
Error Messages	3/icmp		device	Enterprise Discovery server
Echo Request	8/icmp		Enterprise Discovery server	device
TTL Timeout	11/icmp	5	Enterprise Discovery server	device
			device	Enterprise Discovery server
Netmask Request	17/icmp		Enterprise Discovery server	device

Table 1 Firewall Ports

Netmask Reply	18/icmp		device	Enterprise Discovery server
SMTP	25/tcp		Enterprise Discovery server	SMTP server
DNS	53/udp		Enterprise Discovery server	DNS server
NetBIOS-n (name server)	137/udp		Enterprise Discovery server	device
NetBIOS-dgm (datagram)	138/udp		management workstation	Enterprise Discovery server
NetBIOS-ssn (session—file and printer sharing)	139/tcp		management workstation	Enterprise Discovery server
SNMP	161/udp		Enterprise Discovery server	device
SNMP traps	162/udp	3	Enterprise Discovery server	external network management server
HTTPS	443/tcp		management workstation	Enterprise Discovery server
		1	management workstation	device
		1	Enterprise Discovery server	device
		2	Enterprise Discovery server	aggregated Enterprise Discovery server
Windows communication (Windows 200x and XP)	445/tcp		Enterprise Discovery server	device with Enterprise Discovery Agent
Peregrine Listener	1738/tcp	4	Enterprise Discovery server	device with Listener (from Desktop Inventory)
HP OpenView Agent	2738/tcp		Enterprise Discovery server	device with Enterprise Discovery Agent
Remote Desktop	3389/udp		HP OpenView Customer Support	Enterprise Discovery server

Table 1 Firewall Ports

MySQL ODBC	8108/tcp	1	management workstation	Enterprise Discovery server
Traceroute	33263/ udp 33436/ udp		Enterprise Discovery server	device

1. Depending on your settings for Server proxy services
2. If you have an Aggregator license
3. If you are using SNMP trap notification
4. This listener port is the default.
5. TTL Timeout can go in either direction, from the Enterprise Discovery server or to the Enterprise Discovery server.

Other Ports used by the Server

These are additional ports used on the Enterprise Discovery server that do not need to be enabled in the firewall.

Table 2 Other Ports

Service	Port
MIB Browser	8100
Network Map	8101
authd	8109
acs	8110
old listener SDK	8111
Java loggers	8112
C++/delphi loggers	8113
scheduler	8114
Perl/text based loggers	8115
Tomcat	8116
Apache	8117
Event Manager	8118
Topology Converter	8119
DiscoveryEngine.jay_polls0	8200
DiscoveryEngine.jay_polls1	8201
DiscoveryEngine.jay_polls2	8202
DiscoveryEngine.jay_polls3	8203

Table 2 Other Ports

Service	Port
DiscoveryEngine.jay_polls4	8204
DiscoveryEngine.jay_idd	8196
DiscoveryEngine.jay_tables	8197
DiscoveryEngine.jay_jaywalks	8198
DiscoveryEngine.jay_debug	8199

Check Cisco devices

It is strongly recommended that firmware/software in your Cisco devices be IOS version 12 or higher. If you want ATM or Frame Relay support, IOS 12 is mandatory in your Cisco devices.

Check Committed Information Rate values

If your network uses Frame Relay, check your Committed Information Rate (CIR) values for your connectivity devices. Make sure you set the CIR on these connections, so the correct statistics will be calculated.

In Frame Relay networks, a CIR is a bandwidth (expressed in bits per second) associated with a logical connection in a permanent virtual circuit (PVC).

The CIR values for these devices are available from your service provider. Check the appropriate documentation to obtain these values.

If the network activity on any particular PVC goes over normal operating thresholds, you should be aware that the Frame Relay controller may mark some packets to be deleted.

3 Planning Form

This chapter contains a preformatted example Enterprise Discovery planning form. Use this form as a starting point and customize to suit your organization's discovery, inventory and software utilization needs. You will find information on the following topics:

The Planning Form Overview

To ensure that Enterprise Discovery knows where to collect data from and how to collect that data, you must do a little preliminary work. You only have to do this once.

By using the planning form in this chapter before implementing Enterprise Discovery you will:

- Ensure the network is ready and prepared for Discovery.
- Determine what Inventory data is to be collected and how it will be used.
- Determine the user asset information that will be recorded.
- Extract the information necessary to plan the logistics of an inventory.

Instructions for completing the Planning Form

This planning form is the first step in defining the requirements for a Discovery and Asset Inventory project. Depending on how the project is to be implemented, further requirements will need to be defined to deal with detailed logistics. For example, site access for engineers, security clearance etc.

If you wish, you can fill in the questionnaire and send it to HP OpenView customer support. They can review your information and provide feedback on how you set up Enterprise Discovery.

If you need help filling out the questionnaire, please contact your HP OpenView or OEM/VAR (Original Equipment Manufacturer or Value Added Reseller) sales representative.

Discovery Questions

Table 1 Questions

Question	General instructions
Describe the network node and subnet setup	Enter information to help determine the scale of your network. Enterprise Discovery defines a node as any network device with at least one MAC address. A managed device is a network device that has an SNMP agent and MIB so it can respond to SNMP requests.
Enter Enterprise Discovery Server network information	Enter the information that you will assign to the Enterprise Discovery Server at startup. If your network uses DHCP, ensure that the IP address for the Enterprise Discovery Server is static.
List IPv4 ranges for Enterprise Discovery to discover	Enterprise Discovery uses IPv4 ranges to discover the devices in your network. It works best when you give it a broad idea of where the devices in your network are—but exclude ranges where you know there are no devices. While you are making a list of devices in your networks, indicate bridges, routers, switches, and concentrators, so that you can identify them easily. Please add the IPv4 ranges you want Enterprise Discovery to discover in your network. For example, to discover an entire class C subnet with subnet mask 255.255.255.0 enter an IP range from xxx.xxx.xxx.0 to xxx.xxx.xxx.255 such as 172.17.1.0. to 172.17.1.255. If you require more space, please attach additional sheets as needed.
List IPv4 ranges for Enterprise Discovery to avoid	If there are subsets of the above IPv4 ranges that you do not want Enterprise Discovery to discover, enter them here.
List the network device community strings (SNMP v1/v2) and users (SNMPv3)	For an explanation of community strings/users, see the *Installation and Initial Setup Guide*. This is a list of non-directed community strings. Directed Community strings are covered later. Does Enterprise Discovery need to know the Write Community String/User? No. Enterprise Discovery will operate without write strings/users. However, if you do give Enterprise Discovery the write strings/users, the owner of an Administrator account will be able to manage the device from the Enterprise Discovery interface.
Enter TCP/IP configuration	The Enterprise Discovery server must have its own static IP address, but it can manage devices with either static or dynamic IP addresses. Please enter the following information to show how the devices on your network receive IP addresses.

Inventory and Software Utilization Questions

Table 2 Questions

Question	General instructions
Project staff details	On projects such as these, there is often a project co-ordinator who is separate from the technical resource. The technical resource needs to be someone who has the necessary skill and access rights to set up directories and files at the correct level.
Reasons for data collection	Pinpoint the business drivers for conducting the Inventory. Include as little or as much information as you want. This can be used to list the information you seek to gain from the project
Project Timing	An inventory project is not an instantaneous event. Sufficient time needs to be given to the development of a deployment plan as well as testing. If the data is required for other parts of a larger project, the sooner the work is started the better. Inventory should progress in parallel with the rest of the project, rather than being left as an afterthought. The business driver should be specified so that interfacing to other parts of a project can be evaluated to see if the time-scale is realistic.
Current Environment	What is currently available for asset identification and for deploying software such as Scanners? It is important to identify if any existing facilities are available that can be used in the new project. Unique asset identification is crucial to differentiate machines. If nothing exists, then time and effort needs to be given to considering how this identification is achieved.
Site information	Knowing the split of locations and the estimate of machines at each site is necessary to establish how much work is required at each site and the amount of space required for storage of the data. This leads to discussion of whether all the data is stored locally at each site and uploaded in bulk or push all the data back to one central repository.
If the data is to be uploaded, how fast are the network connections?	Knowing how often the scan is run will identify traffic flow and when the transfer activities will take place. If there are any current network performance issues, these need to be understood before additional activity is added to the current load.

Table 2 Questions

Scanner Configuration	The Scanner can be configured to select various combinations of Hardware, Software and Assets. For example, the first scan of an asset may only be concerned with Asset Information and Hardware details. Whereas, some machines may only require a Software scan on subsequent rescans. • Hardware Normally, the default selection of all hardware tests data is sufficient. The tests take very little time to run and unless there is a known problem it is best to leave the settings as they are. • Software The software choices determine how many and what types of files to both scan and store in the resulting scan file. Exclusions may be because of known scanning problems with a particular file. To assist with software recognition, it is useful to have at least one sample set with signatures. The file signature is a calculation on the first 8K bytes of a file. This requires the file to be opened. If the file is opened, then it is also possible to extract the version information (same as properties under Windows). This header information can provide vendor and application details. The Scanner has the ability to store the contents of ZIP files as directories. This allows the display of the file names that have been compressed, but it cannot extract version information or open the individual compressed files. • Asset Information Asset information is data that has been extracted from files and/or Windows registry. The asset data can be read from a previous scan file and loaded into the fields.
	• Stored Files These files can be embedded in the scan file. They are usually configuration or other data files.
Scan Admin	Checking whether there is any anti-virus or other security software running is important because it can have a profound impact on the speed of the scan. If a file has to be opened for signature, a real-time virus scanner would intercept the request and check the file before releasing it for scanning. To avoid opening a file it may be necessary to configure the scanner to ignore file information. In this instance directory information about the file would still be captured – file name, size, attributes etc. but version information would not be captured.

Computer Population Details

Table 3 Questions

Question	General instructions
Total population	Enter the total number of workstations and servers that are to be included in the inventory project. Also include whether this number is believed to be accurate to within 5%, 10%, or greater.
Percentage Networked	Indicate the percentage of machines that are, or are likely to be network connected during the inventory.
Number of Laptops	Indicate the approximate number of laptop within the overall population. Often special arrangements need to be made to ensure that these are on site during the period of the data collection.
Operating Systems (% of populations)	The scanning software can be configured for the following operating systems: 32 Bit Window, 64 bit Windows , Linux, Unix and Mac OS. Indicate the percentage of differing operating systems, i.e., Win 98, NT x.x, OS 2, AIX, HP-UX, Solaris. From this you can determine the number of different Scanners likely to be needed.
Network Types	Include the network operating software and speed of network if available.
Policy on passwords	Indicate whether power on (boot-up) and/or screensaver passwords are used. If possible, consider not only company policy but the likelihood of individual departments/persons making use of them.

Manual Inventories

Table 4 Questions

Question	General instructions
Special conditions?	Special users, remote or standalone need to be considered along with any non-working equipment. You may decide to leave these out or perform the work manually.
Are there any issues concerning site access?	Consider whether there might be physical constraints when gaining access to the sites. Are parking facilities available?
Are passes required for access?	Are passes needed for access to locations within the sites. Are swipe cards used? Will they be made available to your project team members?
Security Software Installed?	Indicate whether security software is installed which would prevent an executable file from being run from the floppy drive. If such software is installed, identify.

Table 4 Questions

Floppy disk locks in place?	Indicate whether floppy disk drive locks are fitted. Also consider whether any of the floppy drives might be either disabled or not-connected.
Asset Labels	Each scan file needs to be uniquely identified during the data collection. The easiest and most efficient way of doing this is to use an asset number assigned to that equipment. If you do not have a system of asset labelling in place you might like to consider introducing one during the data capture, as the labels can be fitted as each PC is visited.
Scan schedule times	Check access times for your team. You can often expect that access can only be granted to certain locations/departments outside of these times. This can assist with estimating the time taken to complete each site and hence the overall project.
If needed will 'audit' logins be provided?	In order to fully scan some machines, local administrator access rights to the machine are required.

The Enterprise Discovery Planning Form

Client Details and Contacts

Table 5 Client Details and Contacts

Client name	
Address	
Phone	
Project Contact	Name: Phone: Email:
Technical Contact	Name: Phone: Email:

Network node and subnet setup

Table 6 Network node and subnet setup

How many nodes do you believe are active on your network?	
Are there any remote sites to be managed?	Yes ☐ No ☐
If yes, approximately how many managed nodes are at remote sites?	
Is your network divided into subnets?	Yes ☐ No ☐
If yes, how many subnets does your network contain?	

Enterprise Discovery Server network information

You will give this IPv4 address to new Enterprise Discovery users so they can log in easily.

Table 7 Enterprise Discovery Server network information

Planned IPv4 address for your Enterprise Discovery server	
Subnet mask address	
Default gateway IP address	

List IPv4 ranges for Enterprise Discovery to discover

When you assign IPv4 ranges, be aware of the size of the ranges you are requesting. If you request a large range of IPv4 addresses to sweep, it can take several hours or days.

Table 8 List of IPv4 ranges for Enterprise Discovery to discover

Range	**From**	**To**
IPv4 range 1		
IPv4 range 2		
IPv4 range 3		

Table 8 List of IPv4 ranges for Enterprise Discovery to discover

Range	From	To
IPv4 range 4		
IPv4 range 5		
IPv4 range 6		

List of IPv4 ranges for Enterprise Discovery to avoid

You do not need to enter ranges outside the ranges you have specified. Enterprise Discovery does not discover ranges unless you specify them.

Table 9 List of IPv4 ranges for Enterprise Discovery to avoid

Range	From	To
IPv4 range 1		
IPv4 range 2		
IPv4 range 3		
IPv4 range 4		
IPv4 range 5		
IPv4 range 6		

List the SNMPv1/v2 Community Strings for your network devices

Table 10 List the Community Strings of your network devices

		Rights granted	
Community string	**Associated device/IPv4 range**	**Read**	**Write**
		☐	☐
		☐	☐
		☐	☐
		☐	☐
		☐	☐
		☐	☐

These should be made available at installation time.

List the SNMPv3 Users for your network devices

Table 11 List the Community Strings of your network devices

User Name	Associated device/IPv4 range	Authentication Algorithm and Passphrase	Encryption Algorithm and Passphrase	Rights granted	
				Read	Write
				☐	☐
				☐	☐
				☐	☐
				☐	☐
				☐	☐
				☐	☐

These should be made available at installation time.

TCP/IP configuration

Table 12 TCP/IP configuration

Are TCP/IP addresses static or dynamic?	Static ☐ Dynamic ☐
If dynamic, enter the following:	
— The IPv4 address(es) of Dynamic Host Configuration Protocol (DHCP) server(s)	
— The DHCP IPv4 address lease time (recommended lease time of at least 7 days.)	

Table 12 TCP/IP configuration

Is SNMP management enabled on the DHCP server?	Yes ☐ No ☐
Enable SNMP management on the DHCP server so that Enterprise Discovery can poll the DHCP server ARP cache for the current IP and MAC address pair information of the devices on your network.	

Please list the IP addresses of any routers you want Enterprise Discovery to monitor, that do not have SNMP management enabled now and will not have management enabled in the future (for example, a router controlled by an Internet Service Provider).

Table 13 Unmanaged Routers

Unmanaged router number 1	
Unmanaged router number 2	
Unmanaged router number 3	

Reasons for Data Collection

Table 14 Reasons for Data Collection

1	
2	
3	
4	
5	

Project Timing

Table 15 Project Timing

Desired start date for project	
Target implementation date (move to Production) Business driver for target date	

The Current Environment

Table 16 The current environment

Is there an existing asset control system in place with unique identifiers?	Yes ☐ No ☐
If yes, is this information stored electronically?	
If no, what identifier is to be used?	

Table 17 Existing software deployment

Is there an existing software deployment system in place?	Yes ☐ No ☐
If yes, what system?	
If no, how are applications distributed currently?	

Site Information

Table 18 Site information

Locations	
1	
2	
3	
4	
5	

Table 19 Equipment

Locations	**1**	**2**	**3**	**4**	**5**	**Total**
Workstations						
PCs Win 95/98/NT/2000 (Win32)						
Solaris workstations 2.5, 2.6, 7, 8						
HP/UX workstations 10.2, 11.0						
Linux Kernel v2.2, 2.4						
AIX 4.3, 5.x						
Mac OS 10.3, 10.4						

Table 19 Equipment

Servers						
NT Servers						
Netware Servers						
Site totals						

Novell Netware servers need to be scanned in two phases.

1 Assets and Hardware only after downing the server and restarting under DOS.

2 Software only scan – if volumes compressed, run scan without signatures

Data Storage Estimates

If sample files are available from previous scans, use their average size as an indicator.

Table 20 Data storage estimates

Locations	**1**	**2**	**3**	**4**	**5**	**Total**
Workstations						
Mbytes/ Workstation						
Servers						
Mbytes/Server						
Site totals Mbytes						

Table 21 Anti Virus software and high speed network connections

Any Anti Virus/ Security products which may impact audit?	Yes ☐ No ☐
Are there high speed network connections between sites?	Yes ☐ No ☐

Scanner Configuration

For Automated scanning the Hardware detection is always included in the Scanner.

Table 22 Scanner configuration

Hardware only	Yes ☐ No ☐
Hardware, Assets	Yes ☐ No ☐
Hardware, Assets, S/W	Yes ☐ No ☐
Software only	Yes ☐ No ☐

Table 23 Hardware Scanner configuration

Hardware	
Use default setting of all tests? If No, which tests to remove?	Yes ☐ No ☐

Table 24 Software Scanner configuration

Software	
All file data to be stored, only Executable files, Selected files If Selected, which file types? Any specific exclusions? If yes, detail files and/or directories	All ☐ Executables ☐ Selected ☐ _____; _____; _____; _____; Yes ☐ No ☐
Will file scan include signatures?	Yes ☐ No ☐
If Yes, will version information be extracted?	Yes ☐ No ☐
Will ZIP files be stored as directories?	Yes ☐ No ☐

Files to be Collected by the Scanner

Default files collected

Config.sys, Sms.ini, Drvspace.ini, Autoexec.bat, System.ini, Win.ini, Boot.ini, Infrtool.ini, Exclude.fp, Net.cfg, Protocol.ini

For UNIX

fstab, group, hosts, inetd.conf, inittab, profile

Table 25 Files to be collected by the Scanner

File	Location	String for file extract

Software Recognition

Table 26 Software recogntion

Bespoke software to be recognized?	Yes ☐ No ☐
Number of applications	
Note: Each application may have many releases. Ensure that you note these.	

Scan Administration

Table 27 Scan administration

What systems will be fed with scan data e.g. AssetCenter, ServiceCenter using [Connect-It]?	

Special Considerations

Table 28 Any other special considerations

Contractors/Special Users	
Are they to be scanned?	Yes ☐ No ☐
If yes, will a restricted Scanner be used?	Yes ☐ No ☐
Any other considerations?	

Table 29 Remote access users

Remote Access Users	
Are they to be scanned?	Yes ☐ No ☐
If yes, will a restricted scanner be used?	Yes ☐ No ☐
Any other considerations?	

Table 30 Standalone users

Standalone Users	
Are they to be scanned?	Yes ☐ No ☐
If yes, will a restricted scanner be used?	Yes ☐ No ☐
Any other considerations?	

Table 31 Non-operational equipment

Non-operational equipment	
Are they to be scanned?	Yes ☐ No ☐
If no, will data be captured manually?	Yes ☐ No ☐
If yes, who will make them operational?	
Any other considerations?	

4 Planning an Enterprise Discovery Deployment

This section provides information on how Enterprise Discovery can be deployed to discover, collect and maintain current inventory data.

You will find information on the following topics:

- What are IT assets
- What is Discovery Data
- Purpose of an Enterprise Discovery Deployment
- Planning the Enterprise Discovery Deployment
- Steps for Planning an Enterprise Discovery Deployment

These are key concepts that are important to understand before proceeding with an inventory.

What are IT Assets?

An IT asset is any piece of IT equipment or software that your company owns or leases. The information about these assets should be stored and kept up to date in your IT asset database.

Hardware IT Assets

Examples of your hardware IT assets are:

- Desktops
- Workstations
- Servers
- Portable devices (for example, laptops)
- Printers
- Modems
- Monitors
- Keyboards
- IP Telephones
- Scanners
- Routers
- Bridges
- Switches

Software IT Assets

Your software IT assets are the software and applications that are being run on computers in your organization. Examples of software IT assets are:

- Commercially available software applications
- Proprietary software your company has produced
- Information stored in files

What is Discovery Data?

Discovery Data is information about all IT Assets in your organization. Enterprise Discovery is used to automatically detect and collect network, hardware and software data for these devices.

The data discovered by Enterprise Discovery can be used in a number of ways, even without integrating it with an asset repository:

- To get an accurate list of devices in your network, including core network devices, IP telephones, computers, and intermittently connected devices such as laptops.
- To get a complete view of software applications deployed,
- To identify top software license requirements by publisher or application,
- To identify devices in your network that do not work as well as they should.

To get the full value of the data discovered by Enterprise Discovery, it should be reconciled with the financial data held in a central asset repository such as AssetCenter. This makes the data valuable in a much wider range of business processes:

- As a valuable company resource for other departments.
- For data management. Keeping track of versions of electronic price lists for consistency, keeping track of databases for business continuity etc.
- To perform spot checks to ensure all changes within an IT asset's life cycle are recorded.
- To manage hardware and software resources efficiently. This results in more effective user support, software purchasing, licensing and better hardware utilization.
- To detect and solve problems such as software piracy, computer pornography and other abuses.
- As a mechanism to ensure compliance with internal standards for software application licensing.
- To drive a range of standardization initiatives, whether hardware- or software-related.

Purpose of Conducting an Enterprise Discovery Deployment

An Enterprise Discovery deployment can be conducted for a number of reasons, including software license compliance, but is also an opportunity to gain beneficial information and effective control of costly IT assets.

It is important to consider various business drivers in order to maximize the benefit. Once Discovery data is available within an organization, interested parties begin to request information for their particular needs. Consider the needs of the following functions:

- Technical Support (Helpdesk)
- Asset management
- Software licensing
- Business continuity
- Disk grooming
- Platform upgrading
- Software Licensing
- Virus Impact Assessment

Technical Support (Helpdesk)

Helpdesk inventory data usage can include:

- User and machine information
- Software versions
- Configuration files

Inventory data facilitates Helpdesk by:

- Reducing time spent managing users
- Detecting problems earlier
- Verifying implementation of changes
- Giving users better service

Asset Management

Asset management data usage can include:

- User and machine information
- Software versions
- Software utilization information

This data can be used to:

- Analyze the computer estate
- Reduce software license infringement and down-time
- Optimize software license costs
- Improve asset management and utilization
- Improve supplier leverage

Asset management products often manage only a minimum set of data fields and traditionally have focused on hardware information. To make best use of the data, you should use AssetCenter, which now includes a Software Asset Management module dedicated to managing and optimizing software licenses.

Business Continuity

Data necessary for business continuity is:

- User and machine information
- Software versions

This information is used to:

- Use stored files to aid computer configuration
- Check restored data for versioning

Business continuity is an important aspect of asset management. One concern is recovering machines critical to the organization, after a failure. Another issue, is change. As users are re-deployed within an organization, knowing their previous equipment capability makes it easier to assign a machine with the same or better specification. If new equipment is needed, the previous specifications are available.

By comparing the inventory of a rebuilt machine with its baseline, differences in software versions and additional data files can be highlighted. When an inventory is complete, an accurate status of changes in assets, hardware, software or deployment can be maintained. Key files can be embedded into the inventory data so that they are available from an alternative resource to the specific machine.

Disk Grooming

Enterprise Discovery can be configured to collect information that can be used for disk grooming, such as:

- Duplicate file and application installations
- Multiple versions
- Small and empty files
- Unbalanced directory structures
- Mixed data and program directories
- Space available on accessible drives

Disk drives tend to accumulate superfluous files, such as, old versions of programs, more than one copy of a local file and old installations that were incompletely removed. Empty and small files consume at least a few KB of disk space per file, and even the contents of Temp directory of the recycle bins can impact disk space.

Duplicate applications can have licensing implications. Some vendors do not permit more than one version of their software on a computer without an additional license. This can happen when upgrades are installed and a previous version remains on the machine during the migration period.

Applications, particularly graphical and multi-media applications, consume a significant amount of disk space. If applications are to be migrated to a server, then it is vital that odd data files are not mixed with the executable files as they might be given access rights preventing user updates.

By making periodic inventories, disk usage can be tracked and remedial action taken. This will help users organize data more effectively and increase their productivity.

Platform Upgrading

Inventory data facilitates platform upgrading in:

- Determining current configurations
- Comparing current configurations with target requirements
- Controlling rollout programs

When upgrading software or migrating data, it is necessary to know the current and the target configurations. By comparing current and inventory data with target requirements, it can be determined which machines meet specifications, which need to be upgraded and which need to be replaced. Re-inventory of machines after they are upgraded can identify what 'standard builds' are compromised and provide a check on the progress of a rollout program.

Software Licensing

Inventory data can be used to:

- Identify applications and versions
- Produce summary counts
- Update software indices for local applications
- Identify redundant software installations that are not used or under-utilized.
- Check license breaches

Due to the number of phases involved in the process, software licensing needs to be handled as a specific project. Since many applications occur as software suites, inventory data is useful for matching software licenses to application counts and can help companies avoid the over-purchasing of licenses.

Establishing ownership of software may require input from sources such as suppliers. Even if unlicensed software is detected, the user should not hesitate to consult suppliers. Software publishers are generally pleased to know that users are taking steps to mitigate the problem.

Virus Impact Assessment

Inventory software is not a replacement for virus detection; however, an important use of inventory data is to check the current version of the anti-virus software deployed. Sometimes the most current version is not fully deployed leaving the computer unprotected against new viruses.

Inventory data provides support information for virus detection. For example:

- If a boot sector virus has been detected and cleaned, it may leave that boot sector inoperable. A standard inventory embeds a copy of the boot sector in the data it collects, and this information can be used to rebuild the damaged sector.
- Some viruses create a time stamp of 62 seconds. The file list can be searched for such an occurrence.
- Some viruses create or rename files. By knowing the file names, a search can be undertaken.
- If a file has been infected, it's size could have changed. Re-running the scan may result in different data being produced.

Reusing Inventory Data

Once inventory data is collected, it is necessary to keep the data current. Managing upgrades is one re-use of inventory data, others are:

- Producing management reports of product usage
- Cutting out non-essential product evaluations
- Supplier leverage

Planning the Inventory

For an inventory to be successful, front-end analysis should be done to fine-tune the objectives, determine the ultimate use of the data and specify exactly what data is needed. Well conducted front-end analysis coupled with effective project management practices ensures the successful implementation of the IT asset inventory with minimum disruption to your business.

Overcoming the Data Mountain

At the start of the inventory, the exact data requirement may be unknown. Once the user begins looking at the inventory data, there is a temptation to start investigating all sorts of ancillary issues. For example, what about those stored outdated computers? As a result, the people performing the inventory may mistakenly employ the 'if in doubt, inventory it' approach.

While there may be a short-term tactical need for specific information, or the inventory might be an opportunity to gather information that is difficult to capture, redundancies can be eliminated by ascertaining exactly what information needs to be extracted.

For example, machines awaiting disposal may not need to be inventoried, but may simply need manual asset recording. Also, consider whether mice and keyboards need to be recorded.

As a general guideline, focus on achieving specific objectives before investigating special interests. If the data collected is not going to be maintained, then its inventory capture should be questioned.

The goals of an IT Asset Inventory

The major goals of an inventory might be:

- Listing all known applications – indicating how many licenses are needed.
- Listing all unknown software – highlights any threats.
- Reporting asset deployment – assists with asset management.
- Listing all computer and server hardware – aids in future upgrade plans.
- Maintaining the Discovery database

Steps for Planning an IT Asset Inventory

The steps outlined here will help bring into focus some of the issues you may face when planning your IT asset inventory.

Step 1: Identifying Your Existing Data Collection Process and Current Environment

Throughout your organization you will find that different departments will be using different methods for the collection of their data.

For example:

- Your HR department may be using a spreadsheet that contains all the data for employees (Employee names, functions, departments, software contracts etc.).
- Your IT department may use an in-house database that contains data on the machines the company owns.

Identifying existing data collection methods is also an important first step in identifying the data needs of your various departments.

The Current Environment

- Have previous scans been undertaken?
- Are there any existing electronic identifiers?
- Are there any facilities for application deployment?
- What percentage of machines are networked?
- How many servers?
- What operating environment do they use?

Step 2: Planning the Collection of This Data

The data collection processes identified in Step 1 will become a source of one-time input into your repository.

Step 3: Designating and Training Members of Staff for the Maintenance of the Data

You must designate tasks to employees who can ensure that the data accuracy and consistency is maintained regularly.

In order to ensure data accuracy and consistency, both across the organization and over time, it is important that ownership of these issues is assigned early in the process.

These tasks must be considered a vital part of the overall asset management effort, as accuracy of the data is an absolute requirement if later analysis is to be of significant value.

It is vital that there are staff nominated as contact points to answer both project and technical questions. There may be more than one person in each category depending on the size of the project.

Step 4: Deciding What Data is Needed and Determining How to Source that Information

You will need to take a detailed look at the data that is required. Bear in mind that the data needs will be different from department to department. Step 1 will have already provided some indication as to what these departmental data needs are.

This can have a significant bearing on how a project is undertaken and the amount of data to be collected. Also consider whether the data will be forwarded to other applications, if so, how is this envisaged.

Further Information

For information on what data the Scanners collect refer to the document entitled 'Data collected by the Scanners'.

Step 5: Configuring the Scanners

Configure a Scanner that collects this data for the various platforms used by the computers in your company using Scanner Generator.

Hardware detection is fast - typically 10-30 seconds. The main areas that need configuring in Scanner Generator are Software and Asset data collection. For almost all purposes, you can use the default Hardware detection settings.

If possible, avoid configuring more than one Scanner for each platform. Running different Scanners for different departments can become a labour intensive exercise and should be avoided if possible.

Further Information

For more information on creating customized Scanners, refer to the Enterprise Discovery *Configuration and Customization Guide*.

Step 6: Deciding How You Will Gather the Data

The Scan Repository

Regardless of whether you carry out a manual or automated scan, the scan files will end up in your repository. The repository should be designed to hold all your scan files and should be cleaned up periodically.

Automatic Inventory

This type of inventory will allow you to collect information about hardware and software assets and pinpoint basic information about where those assets are located, who is logged into them, and what operating systems they are running on etc.

This information can serve as the basis for the initial walk around inventory as it helps define and establish "what is there".

The Scanners are distributed to individual machines. You can set up a schedule using Enterprise Discovery dictating which machines should be scanned and at what frequency. The retrieved scan files are placed in a central repository.

You can then use the data for use in asset management systems, such as AssetCenter using Connect-It.

Manual Inventory

A walk-round (or manual) inventory captures data about assets that are not connected to your network (i.e. stand-alone).

In these cases a memory stick or floppy disk with the Scanner executable will ensure that all important configuration items about that PC (such as installed software, and hardware), monitors and Asset Tags, etc. are known.

During the course of the inventory you may come across unused and surplus assets. These surplus assets can be re-deployed to other employees or should be properly removed from the inventory.

A walk-round inventory also allows each asset to be physically inspected. The state of the machine can then be stored in an asset field.

The results of the Scan should then be saved to the central repository.

Step 8: Creating and Maintaining a Set of Methodologies

Inventory capture is not a one time event.

Once the initial asset inventory and asset reconciliation is complete, you should create and maintain a set of processes that are designed to keep your inventory up-to-date.

- Any time a machine has had changes made to it, for example, software and hardware upgrades, it has been allocated to another member of staff etc., a scan should be initiated.

  The fields about the user and asset can then be updated and automatically reconciled again against the data in your asset management system for example.
- Spot-check practices should be established that verify automatically-collected data samples for accuracy.
- Non-networked assets must have a process for the manual entry of new data initially and then follow-up inventories must also ensure that these assets are included and the data is kept up-to-date.
- Scans should be run on networked systems at least once monthly to keep the data about these systems up-to-date.

Re-inventory

The regularity of re-inventory depends on a number of factors, including:

- How often assets change condition - moves, upgrades, additions etc.
- How often information needs to be reported. For example, is it necessary to perform a daily inventory check if the results are only reported quarterly?
- How often the people in charge are likely to have the time to look at it.
- What it is used for.
  - If for asset management - then rarely
  - If for services/support - then more often.

Index