HP Discovery and Dependency Mapping Inventory

for the Windows® operating system

Software Version: 9.30

Configuration and Customization Guide

Manufacturing Part Number: None
Document Release Date: February 2011
Software Release Date: February 2011

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

Windows™ Vista is either a registered trademark or trademark of Microsoft Corporation in the United States and/or other countries.

Java™ is a US trademark of Oracle Corporation.

AMD® is a trademark of Advanced Micro Devices, Inc.

UNIX® is a registered trademark of The Open Group.

Intel® and Intel® Xeon™ are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

This product includes software developed by the Apache Software Foundation (**http://www.apache.org/**).

Support

You can visit the HP software support web site at:

www.hp.com/go/hpsoftwaresupport

HP Software online support provides an efficient way to access interactive technical support tools. As a valued support customer, you can benefit by using the support site to:

- Search for knowledge documents of interest
- Submit and track support cases and enhancement requests
- Download software patches
- Manage support contracts
- Look up HP support contacts
- Review information about available services
- Enter into discussions with other software customers
- Research and register for software training

Most of the support areas require that you register as an HP Passport user and sign in. Many also require an active support contract. To find more information about support access levels, go to the following URL:

http://h20230.www2.hp.com/new_access_levels.jsp

To register for an HP Passport ID, go to the following URL:

http://h20229.www2.hp.com/passport-registration.html

Contents

1 Introduction

This guide will help you configure and customize the components of DDM Inventory^{TM} to your own specifications.

Topics in this guide include:

- Accounts for access to the web interface (administration, reports device managers, etc.) (See Chapter 2, Setting up Accounts for detailed information.).
- How devices are added to and deleted from the DDM Inventory database (See Chapter 5, Adding, Removing, and Replacing Devices for detailed information.).
- Device and port properties (See Chapter 8, Changing Device and Port Properties for detailed information.).
- Pre-scan and post-scan scripts (See Chapter 9, Pre-Scan and Post-Scan Scripts for Collecting Custom Hardware Data for detailed information.).
- Scan file configuration (See Chapter 10, Configuring Scanner Settings for detailed information.).
- Agent communication and configuration (See Chapter 11, Agent Communication Configuration for detailed information.).
- Scanner generator for creating Scanners (See Chapter 12, Scanner Generator for detailed information.).
- XML Enricher for adding data to scan files (See Chapter 13, XML Enricher for detailed information.).
- How to get your data into AssetCenter (See Chapter 14, Getting Data into AssetCenter for detailed information.).

2 Setting up Accounts

All DDM Inventory system configurations can support up to 250 accounts (including at least one Administrator account).

An Administrator can create and maintain all other user accounts. IT Employee and IT Manager accounts can change their own account properties using the **Administration > My Account Administration** menu.

➤ These user accounts are completely distinct from the MySQL Accounts. For more information on those, see the *Installation and Initial Setup Guide*

About Accounts

There are six types of account:

- Demo
- IT Employee
- IT Manager
- Administrator
- Scanner
- Aggregator

By default, DDM Inventory has one of each type of account installed (except for Scanner and Aggregator, which are both used for specific cases). If there are to be any other accounts, the owner of an Administrator account must create them.

‼ In DDM Inventory, all IT Manager and Administrator accounts have access to some powerful features. If you have an IT Manager or Administrator account, be careful not to overwrite the work of other IT Manager or Administrator accounts. In particular, it is recommended that there be only one DDM Inventory Administrator.

Table 1 Default Accounts

Account type	Account name	Password
Demo	demo	password
IT Employee	itemployee	password
IT Manager	itmanager	password
Administrator	admin	password

Table 2 Account Access to DDM Inventory

	Demo	IT Employee	IT Manager	Administrator
Network Map				
Initial map configuration file	Copy of Prime	Copy of Prime	Copy of Prime	Copy of Prime
Default map configuration file	Copy of Prime	last saved or used	last saved or used	last saved or used
Open any saved map configuration	✓	✓	✓	✓
Save any number of map configurations	✓	✓	✓	✓
Save a map configuration as Prime	—	—	✓	✓
Change a device icon	—	—	✓	✓
Change a package icon	✓	✓	✓	✓
Change a device's priority	—	—	✓	✓
Change a device's title or tag	—	—	✓	✓
Purge a device	—	—	✓	✓
Disconnect other accounts' map sessions	—	—	—	✓
Managers (for example, Device Manager)				
View read and write community strings for device	—	—	✓	✓
View and use *set* link to MIB Browser	—	—	✓	✓
SNMP query default string	"public"	"public"	from DDM Inventory	from DDM Inventory
Update Model	—	—	✓	✓
Configure connections	—	—	✓	✓
Break and force connections	—	—	✓	✓
Agent and Scan logs	—	—	✓	✓

Table 2 Account Access to DDM Inventory

	Demo	IT Employee	IT Manager	Administrator
Express Teaching Tool				
Teach unrecognized files	—	—	✓	✓
MIB Browser				
Set SNMP variables	—	—	✓	✓
Read community string	—	view + edit	view + edit	view + edit
Write community string	—	—	view + edit	view + edit
Status				
View read and write community strings for network	—	—	✓	✓
Administration				
Change own password	—	✓	✓	✓
Configure own account	—	✓	✓	✓
Configure other accounts	—	—	—	✓
Manage own map configurations	—	✓	✓	✓
Copy map configurations from other accounts	—	✓	✓	✓
Specify pager e-mail address	—	✓	✓	✓
Configure event filters	—	—	—	✓
Configure DDM Inventory server	—	—	—	✓
Configure network operations	—	—	—	✓

Demo Accounts

Initially, there is one Demo account. The name for this account is "demo" and the password is "password" (account names must be lowercase and passwords are case-sensitive). Demo account owners cannot change this password. An Administrator account owner can create more Demo accounts if needed.

Demo accounts are designed for training and practice. Demo is the least powerful type of account on DDM Inventory. The restrictions on this account make it impossible for the Demo account owner to damage the network.

A Demo account can:

- View the Network Map, with the restriction that each map session will begin with a configuration named "Copy of Prime." The Prime configuration is maintained by an Administrator or IT Manager account.
- Open any saved map configuration
- Save any number of map configurations
- View reports and server status

IT Employee Accounts

An IT Employee account can:

- Do everything a Demo account can do
- View the Network Map; with every map session after the first session automatically loading their default configuration (which is normally the configuration used most recently)
- Manage their own configurations (delete, duplicate, and rename them, and set a default configuration without opening the Network Map)
- Change their own password and account profile

IT Manager Accounts

The owner of an IT Manager account has the power to make changes that affect what other people see in DDM Inventory.

With respect to the Administration menu, an IT Manager account has capabilities similar to an IT Employee account. With respect to the Network Map an IT Manager account is similar to an Administrator account.

An IT Manager account can:

- Do everything an IT Employee account can do
- Set server system variables such as system name, system contact, system location
- Save a copy of the Network Map as Prime
- Change device properties (title, tag, priority, and icon of a device)
- Change port properties
- See a device's read and write community strings (if known) in the Device Manager Configuration panel

- Purge a device or port
- Update the model for a device
- Change how DDM Inventory sees connections between objects, and break existing connections and create custom connections
- Perform express teaching of unrecognized files
- Set SNMP variables in the MIB Browser

Administrator Accounts

There should be one Administrator account owner designated as the DDM Inventory Administrator, whose account cannot be deleted. The default Administrator account name is “admin” and the default password is “password”. This is the most powerful type of account. Administrator accounts can access all components of the DDM Inventory server.

An Administrator account can:

- Do everything that IT Manager accounts can do
- Perform initial configuration of the DDM Inventory server
- Configure the DDM Inventory server operations on the network
- Administer the IT Manager, IT Employee and Demo accounts

The default Administrator account must set up the initial DDM Inventory server parameters and create the other accounts (see the *Installation and Initial Setup Guide*).

If you forget the Administrator password, you will not be able to access the Administrator account without intervention from Customer Support.

Scanner Accounts

The Scanner account is used only for the purpose of allowing scanners to save scan files on to the server. This can be used in cases where automatic scan deployment is not used.

The Scanner account type does not have access privileges to the web and applet components of the DDM Inventory GUI.

Aggregator Accounts

The Aggregator account is used only to send data to an Aggregator server. Typically, an Aggregator server holds the data for multiple “remote” servers that are deployed throughout a large network. In order for an Aggregator server to obtain the data from the remote servers, it must have access to that server through an “Aggregator” user account. For more details, see the *Installation and Initial Setup Guide*.

The Aggregator account type does not have access privileges to the web and applet components of the DDM Inventory GUI.

Setting up Accounts

This section is for the DDM Inventory Administrator only.

All of these commands are available when you click **Administration** > **Account Administration**.

These procedures allow you to create, delete, and configure user accounts.

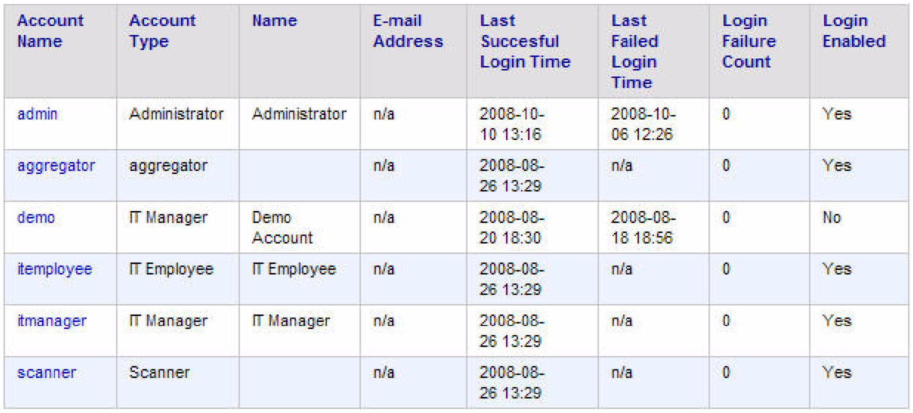
Generating a List of Accounts

This page provides an alphabetical list of currently registered users, complete with their full name and e-mail address. The user names in the list are hyperlinked, so that you can click on the name and see all the options you can perform on that account.

To generate a list of all accounts:

1 Click **Administration** > **Account Administration** > **List accounts**.

A list of all the accounts appears. To modify an account, you can click on the Account name, or go back up a level to the **Account Administration** page and click **Account properties**.



Account Name	Account Type	Name	E-mail Address	Last Succesful Login Time	Last Failed Login Time	Login Failure Count	Login Enabled
admin	Administrator	Administrator	n/a	2008-10-10 13:16	2008-10-06 12:26	0	Yes
aggregator	aggregator		n/a	2008-08-26 13:29	n/a	0	Yes
demo	IT Manager	Demo Account	n/a	2008-08-20 18:30	2008-08-18 18:56	0	No
itemployee	IT Employee	IT Employee	n/a	2008-08-26 13:29	n/a	0	Yes
itmanager	IT Manager	IT Manager	n/a	2008-08-26 13:29	n/a	0	Yes
scanner	Scanner		n/a	2008-08-26 13:29	n/a	0	Yes

Adding an Account

There can be as many as 250 accounts, including yours.

In DDM Inventory, all IT Manager and Administrator accounts have access to some powerful features. If you have an IT Manager or Administrator account, be careful not to overwrite the work of other IT Manager or Administrator accounts. In particular, it is recommended that there be only one DDM Inventory Administrator.

The account name must be 3–16 characters long. Acceptable characters are:

- a through z (must be lower case)
- 0 through 9
- hyphen (-) (the hyphen cannot be the first character in the account name)
- underscore (_) (the underscore cannot be the first character in the account name)

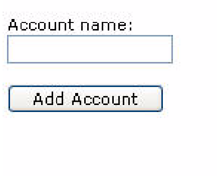
To add an account:

1 Click **Administration** > **Account Administration** > **Add an account**.

2 Enter a login name.

3 Click **Add Account**.

➤ The account is created, but you must still create a password for the account. If you do not create a password, no one will be able to log in with it.



Customizing Account Properties

You can change any of the account properties listed in the following table:

Table 3 Account Properties

Property	Explanation
Account type	Determines the account's level of access to DDM Inventory.
Login enabled	Determines if the account can use DDM Inventory.
Password expiry	The number of days an account can be used before the password expires.
Name	The name of the account owner.
Allow others to copy map configurations	Determines whether or not other users can copy map configuration files from this account.
Append IP Address to device titles?	Determines if device titles are followed by device IP addresses (when available). If chosen, an IP Address column will appear in the Alarm Viewer, Events Browser, and Service Analyzer.
Make URLs visible	Determines if hyperlinks are followed by the associated URL (for easy cut and paste).
Alternate colors in table rows	Tables are easier to read with alternating colors, but they take more space on your screen.
Highlight table rows on mouse over	Lets you highlight a row you want to look at.
Time before marking statistic as stale	Applies to Device Manager, Port Manager, Line Manager, Attribute Manager, Alarms Viewer, Health Panel, and Service Analyzer. When a statistic has not been updated for this set amount of time, the data will appear with a grey background.

Table 3 Account Properties

Property	Explanation
Long date format	Determines how the date appears at the bottom of most panels and pages.
Short date format	Determines how the date appears at the bottom of the Statistics panel's Table view and in Reports, Event Browser and Health Panel.
Default Home Page	Determines the first page you will see when you log in to DDM Inventory: the default home page, or the Asset Questionnaire.
Device Manager scan file viewer	Determines whether you will see a Windows® based Viewer or a Java™ based Scan Data Viewer when you press the View Scan Data button in the Device Manager.
Default Device Manager panel	Determines which panel will appear when you open a Device Manager session.
Default Port Manager panel	Determines which panel will appear when you open a Port Manager session.
Default Attribute panel	Determines which panel will appear when you open an Attribute Manager session.
Default Device Manager Ports panel selection	Determines which configuration will appear when you open a Ports panel in the Device Manager.
Default Device Manager Ports panel increment	Determines how many rows of data the Ports panel displays at a time. Default: 24
Default Device Manager statistic	Statistic selected in the Device Manager Statistics panel.
Default Port Manager statistic	Statistic selected in the Port Manager Statistics panel.
Default Statistic interval	Interval selected for your Statistic panels in the Device Manager and Port Manager.
Default Statistic maximum	Statistic maximum selected for your Statistic panels in the Device Manager and Port Manager.
Default Statistic granularity	Statistic granularity selected for your Statistic panels in the Device Manager and Port Manager

To select an account for customizing:

1 Click **Administration** > **Account Administration** > **Account properties**.

IT Manager and IT Employee accounts can modify their own account properties by clicking **Administration > My Account Administration > Account properties**.

2 Select an account from the list box.

3 Click **Modify Properties**.

To modify an account:

1 Select an account type.

You cannot change the account type, web/applet access, or password expiry period for the account you are currently using.

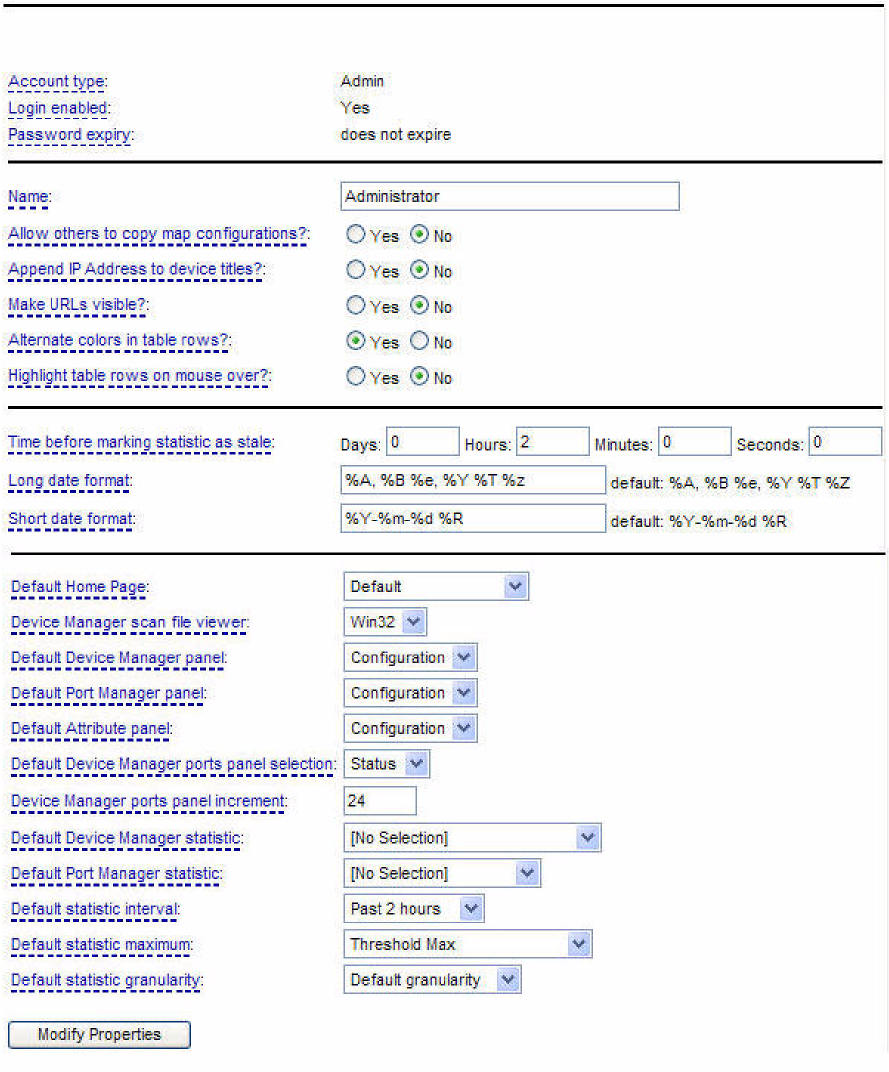
2 Select whether or not this user will have access to the web and applet components of the user interface.

3 Select a time for the user's password to expire.

4 *(optional)* Enter a descriptive name in the Name field.

5 Assign the other appropriate properties.

6 Click **Modify Properties**.



Account type:	Admin
Login enabled:	Yes
Password expiry:	does not expire
Name:	Administrator
Allow others to copy map configurations?:	○ Yes ● No
Append IP Address to device titles?:	○ Yes ● No
Make URLs visible?:	○ Yes ● No
Alternate colors in table rows?:	● Yes ○ No
Highlight table rows on mouse over?:	○ Yes ● No
Time before marking statistic as stale:	Days: 0 Hours: 2 Minutes: 0 Seconds: 0
Long date format:	%A, %B %e, %Y %T %z default: %A, %B %e, %Y %T %Z
Short date format:	%Y-%m-%d %R default: %Y-%m-%d %R
Default Home Page:	Default
Device Manager scan file viewer:	Win32
Default Device Manager panel:	Configuration
Default Port Manager panel:	Configuration
Default Attribute panel:	Configuration
Default Device Manager ports panel selection:	Status
Device Manager ports panel increment:	24
Default Device Manager statistic:	[No Selection]
Default Port Manager statistic:	[No Selection]
Default statistic interval:	Past 2 hours
Default statistic maximum:	Threshold Max
Default statistic granularity:	Default granularity

Modifying Account Contact Information

You can change any of the following properties:

- e-mail address (optional, but required if the user is to receive any e-mail about the DDM Inventory server or the network)
- Pager e-mail address

To modify an account's contact information

1 Click **Administration** > **Account Administration** > **Account contact data.**

IT Manager and IT Employee accounts can modify their own account properties by clicking **Administration > My Account Administration > Account contact data**.

2 Select an account name from the pull-down list.

3 Click **Modify Properties.**

4 You can now modify any of the contact information.

5 Check to make sure the changes are correct.

6 Click **Modify Contact Data**.

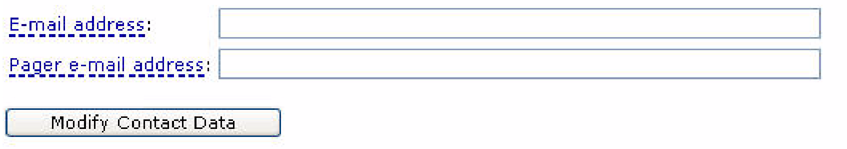
To enable e-mail notification

1 Enter an e-mail address in the E-mail address field.

If the e-mail address is blank, the user will not receive any e-mail.

To enable pager notification through an e-mail gateway

1 Enter a pager address in the Pager e-mail address field.



Modifying an Account Password

An Administrator account must create an account password while creating a new account, or can modify the password at any other time.

Passwords can be up to 20 characters long (the minimum length depends on the setting at **Administration > System Configuration > Server passwords**). Acceptable characters are:

- A through Z
- a through z
- 0 through 9
- underscore (_)
- at (@)

- period (.)
- hyphen (-)

To modify an account password:

1. Click **Administration** > **Account Administration** > **Account password**.

   IT Manager and IT Employee accounts can modify their own account properties by clicking **Administration > My Account Administration > Account password.**

To select an account:

1. Select an account from the list box.
2. Click **Modify Account**.

To modify or create a password:

1. Enter the new password in the first field.

   Do not enter the current password (if any).

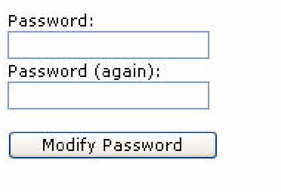
2. Enter the same new password in the second field.

   Entering the same password twice helps guard against typing errors.

3. Click **Modify Password**.

➤ Modifying the password resets the **Password Expiry** and **Failed Login Attempts** features.

➤ If the Administrator has set up the **Password History** feature, you cannot re-use passwords. You must have a new password each time you perform this procedure.



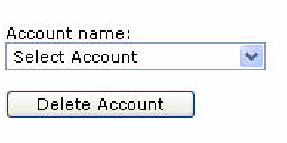
Deleting an Account

This page allows the Administrator account to delete an account from the list of current accounts.

➤ The account you are using to delete accounts, or the “active” account, cannot be deleted.

To select an account:

1. Click **Administration** > **Account Administration** > **Delete an account**.
2. Select an account from the list box.
3. Click **Delete Account**.
4. Click **Confirm**.



Troubleshooting

Why do I see “Account name ‘delme’ does not exist.” when I try to delete an account?

Two possibilities:

- Another Administrator account deleted the account just before you did.
- You deleted the account yourself, but the account login name still appears in the list box because the list has not been updated. To get an updated list of accounts, click your web browser’s Reload or Refresh button.

Maintaining Your Account

This section is intended for Administrator, IT Manager, and IT Employee accounts.

➤ The Demo account cannot perform any administration functions.

You can maintain your own account by setting your own preferences, contact information, and even your password. An Administrator account can also do these tasks as part of setting up accounts.

- Changing your account properties (see Customizing Account Properties on page 19)
- Changing your password (see Modifying an Account Password on page 22)
- Testing Your E-mail Address on page 25
- Testing Your Pager Address on page 25

Testing Your E-mail Address

Testing your e-mail address will send an e-mail message to your account so that you can:

- Test that you have entered your e-mail address correctly.
- Test that the DDM Inventory server has been configured to send e-mail.

To test your e-mail address:

1. Click **Administration** > **My Account Administration** > **Test e-mail address**.
2. To send an e-mail message to your account, click **Confirm**.

If you do not receive the message, it could be because:

- No e-mail address is specified.
- An incorrect e-mail address is specified.
- A mail server has not been specified for use with DDM Inventory
- The receiving mail server is not working.

Testing Your Pager Address

Testing your pager address will send an e-mail message to your pager so that you can:

- Test that you have entered your pager address correctly.
- Test that the DDM Inventory server has been configured to send e-mail.

To test your pager address:

1. Click **Administration** > **My Account Administration** > **Test pager address**.
2. To send an e-mail message to your pager, click **Confirm**.

If you do not receive the page, it could be because:

- No pager e-mail address is specified in your account profile.
- The incorrect pager e-mail address is specified in your account profile.
- Your pager service provider is having problems.
- Your pager is turned off.

3 Working with SNMP Traps

HP DDM Inventory determines network events and places them in an internal events database. Typically an operator can browse these events within the Events Browser, but there are circumstances where the events can be exported to a third party system using Event Filters (see Chapter 4, Setting up Event Filters). DDM Inventory may export SNMP V2C trap event notifications.

To see the full contents of the hpov-ed-trap.my file, go to the following directory on your DDM Inventory server (this is the default install location):

```
C:\Program Files\Hewlett-Packard\DDMI\9.30\events\mibs
```

Installing SNMP Package on DDM Inventory Server

You must install the open source SNMP package on your server in order for DDM Inventory to use SNMP traps. The net-snmp-5.3.0.1-1.win32.exe file is available on the DDM Inventory installation CD.

To install this software:

1. Double-click on the net-snmp-5.3.0.1-1.win32.exe file, available on the DDM Inventory installation CD.
2. Go through the install wizard, selecting all default options.

DDM Inventory Notifications

DDM Inventory issues traps using SNMPv2c messages. SNMPv2c notifications are the successor to SNMPv1 traps. An SNMPv2c notification can contain several objects, which are then parsed by the collector to interpret the event contents. The interpreted contents are then written to a database or forwarded to the notification engine of another NMS system. ‘

There are two notifications, *deviceEvent* and *portEvent*. Each carries a set of SNMP OIDs. These variables cannot be retrieved by an SNMP get request. They are only available as SNMPv2c notification messages.

deviceEvent Notification

The deviceEvent notification is sent for events that correspond to a device, rather than a line. For a detailed description of events that correspond to a device versus those that correspond to a line, see the *Reference Guide*.

The deviceEvent event (OID: .1.3.6.1.4.1.11.2.17.18.0.2.1) contains the following members:

Table 4 deviceEvent Notification

Order	Object	Type	Description
1	serverID .1.3.6.1.4.1.11.2.17.18.0.1.1	Integer	ServerID is an integer that has been configured by the administrator of the DDM Inventory server; it is 1 by default. The ServerID makes it easier for consumers of the inventory to correlate devices managed by different DDM Inventory servers.
2	eventID .1.3.6.1.4.1.11.2.17.18.0.1.2.1	Unsigned32	Increasing sequence number associated with this event. This object is present for compatibility only. It is always blank.
3	datetime .1.3.6.1.4.1.11.2.17.18.0.1.2.2	Octet String	Date and time when event occurred (YYYYMMDD HH:MM:SS).
4	category .1.3.6.1.4.1.11.2.17.18.0.1.2.3	Integer	For a complete list of possible events, see **Help > Classifications > Supported Device/Port Attributes**, and select the appropriate *Internal Name*. For example, for “Bytes In”, select **in_bytes**
5	deviceNMID .1.3.6.1.4.1.11.2.17.18.0.1.2.5.1	Unsigned32	Network Manager Identification
6	deviceType .1.3.6.1.4.1.11.2.17.18.0.1.2.5.2	Unsigned32	The device type (Icon).
7	deviceTag .1.3.6.1.4.1.11.2.17.18.0.1.2.5.3	Octet String	The name of the device.
8	macAddress .1.3.6.1.4.1.11.2.17.18.0.1.2.5.4	Physical Address	The MAC address associated with the device.
9	ipv4Address .1.3.6.1.4.1.11.2.17.18.0.1.2.5.5	IP Address	The IPv4 address associated with the device (if any).
10	deviceTitle .1.3.6.1.4.1.11.2.17.18.0.1.2.5.6	Octet String	The (network map) title of the device as defined by the appliance administrator.
11	priority .1.3.6.1.4.1.11.2.17.18.0.1.2.5.7	Integer	The priority of the device as defined by the appliance administrator: 1, 2, 3, 4, 5 or 6.
12	direction .1.3.6.1.4.1.11.2.17.18.0.1.2.7	Integer	Direction of port that triggered event: notAvailable, in, out.

portEvent Notification

The *portEvent* notification is sent for events that correspond to a port or line, rather than a device. For a detailed description of events that correspond to a port or line versus those that correspond to a device, see the *Reference Guide*.

The portEvent event (OID: .1.3.6.1.4.1.11.2.17.18.0.2.2) contains the following members:

Table 5 portEvent Notification

Order	Object	Type	Description
1	serverID .1.3.6.1.4.1.11.2.17.18.0.1.1	Integer	ServerID is an integer that has been configured by the administrator of the DDM Inventory server; it is 1 by default. The ServerID makes it easier for consumers of the inventory to correlate devices managed by different DDM Inventory servers.
2	eventID .1.3.6.1.4.1.11.2.17.18.0.1.2.1	Unsigned32	Increasing sequence number associated with this event. This object is present for compatibility only. It is always blank.
3	datetime .1.3.6.1.4.1.11.2.17.18.0.1.2.2	Octet String	Date and time when event occurred (YYYYMMDD HH:MM:SS).
4	category .1.3.6.1.4.1.11.2.17.18.0.1.2.3	Integer	For a complete list of possible events, see **Help > Classifications > Supported Device/Port Attributes**, and select the appropriate *Internal Name*. For example, for "Bytes In", select **in_bytes**
5	deviceNMID .1.3.6.1.4.1.11.2.17.18.0.1.2.5.1	Unsigned32	Network Manager Identification
6	deviceType .1.3.6.1.4.1.11.2.17.18.0.1.2.5.2	Unsigned32	The device type (Icon).
7	deviceTag .1.3.6.1.4.1.11.2.17.18.0.1.2.5.3	Octet String	The name of the device.
8	macAddress .1.3.6.1.4.1.11.2.17.18.0.1.2.5.4	Physical Address	The MAC address associated with the device.
9	ipv4Address .1.3.6.1.4.1.11.2.17.18.0.1.2.5.5	IP Address	The IPv4 address associated with the device (if any).
10	deviceTitle .1.3.6.1.4.1.11.2.17.18.0.1.2.5.6	Octet String	The (network map) title of the device as defined by the appliance administrator.

Table 5 portEvent Notification

11	priority .1.3.6.1.4.1.11.2.17.18.0.1.2.5.7	Integer	The priority of the device as defined by the appliance administrator: 1, 2, 3, 4, 5 or 6.
12	portNMID .1.3.6.1.4.1.11.2.17.18.0.1.2.6.1	Unsigned32	Network Manager Identification.
13	portIndex .1.3.6.1.4.1.11.2.17.18.0.1.2.6.2	Octet String	An index value that uniquely identifies this port within a module. The value is determined by the location of the port on the module. Valid entries are 1 to the value of moduleNumPorts for this module.
14	ifSpeed .1.3.6.1.4.1.11.2.17.18.0.1.2.6.3	Integer (Counter64)	An estimate of the interface's current bandwidth in bits per second. For interfaces, which do not vary in bandwidth, or for those where no accurate estimation can be made, this object should contain the nominal bandwidth. If the bandwidth of the interface is greater than the maximum value reportable by this object then this object should report its maximum value (4,294,967,295) and ifHighSpeed must be used to report the interface’s speed. For a sub-layer, which has no concept of bandwidth, this object should be zero.
15	ifType .1.3.6.1.4.1.11.2.17.18.0.1.2.6.4	IANAifType (Integer)	The type of interface. The Internet Assigned Numbers Authority (IANA), through updating the syntax of the IANAifType textual convention, assigns additional values for ifType.
16	duplex .1.3.6.1.4.1.11.2.17.18.0.1.2.6.5	Integer	The duplex of port within the device: full, half, or non-applicable.
17	connectedToDevice .1.3.6.1.4.1.11.2.17.18.0.1.2.6.6	Unsigned32	The NMID of the remote device this port connects to.
18	connectedToPort .1.3.6.1.4.1.11.2.17.18.0.1.2.6.7	Unsigned32	The NMID of the port on the remote device this port connects to.
19	direction .1.3.6.1.4.1.11.2.17.18.0.1.2.7	Integer	Direction of port that triggered event: notAvailable, in, out.

4 Setting up Event Filters

Setting up Event Filters is for Administrator accounts only.

You can configure DDM Inventory to notify you when events occur. DDM Inventory can notify you by email, by pager, or by SNMP trap. For example, you can create an event filter to notify you when a particular device has a Break alarm.

➤ For specific details on SNMP traps, see Chapter 3, Working with SNMP Traps.

Topics in this chapter include:

Interactions Affecting Event Filters

The most important thing to remember about event filters is that they rely on the system-level device priorities which are controlled by Administrator and IT Manager accounts. In order for your event filters to work properly, you must make sure you set the system-level priorities for your devices properly.

Be very careful when setting up your event filters. Many factors contribute to making your event filters work effectively. Make sure you complete all of the tasks in this chapter. If you skip any of these tasks, or if you do any of them incorrectly, your event filters may not work.

If you are not familiar with the following concepts, read the appropriate sections of this *User Guide*.

Table 6 Prerequisites

Concept	Commands and where to get more information
E-mail Issues	
Set up your SMTP server	**Administration > System Configuration > Server configuration > SMTP server.** See the *Installation and Initial Setup Guide*.
Events Issues	
Understand the types of events recorded by DDM Inventory	See the *Reference Guide*.
Account Issues	
Set up account contact information	**Administration > Account Administration > Account properties.**
Network Map Issues	
Change device priorities	Changing Device and Port Properties on page 63

Event filters are an advanced option. You have the power to send pager and e-mail messages whenever a device attribute changes state. This means that the potential exists to send several pager and e-mail messages for the same event on the same device.

You must make sure you are setting up the event filters properly, to avoid excessive notification, or notification on the wrong devices, or no notification at all.

If you have read this section and believe you have set up all the components properly, and your events filters are not working properly, call Customer Support.

What is an Event Filter?

All events in the network are recorded in the event log. You can select events that are important to you, and DDM Inventory can notify you in the following ways:

- Send an e-mail message
- Send an alphanumeric page by means of an e-mail gateway
- Send an SNMP trap to another network management system
- Create an XML file for use with another application

DDM Inventory has two default event filters. You can create your own through **Administration** > **Event Filter Configuration**.

You can enter a range of IP addresses if you want to be alerted about events on a portion of your network. This allows you to create event filters specifically for a network, subnet, or even a single device. If you leave this section blank, the event filter will apply to all devices in your network.

Table 7 Default Event Filters

Default Event Filter	Description
email-admin-device	Send e-mail to the "admin" account[a] when a device of priority 6 breaks.
email-admin-line	Send e-mail to the "admin" account[a]. when a line of priority 6 breaks.

[a] The "admin" account is the default Administrator account. If you have changed the name of this Administrator account when initially setting up DDM Inventory, you should have changed these default event filters.

Preparing DDM Inventory for Event Filters

In order to have event filters work properly, you must have several components set up.

- For a device with multiple IP addresses, be sure to determine its primary IP address when specifying the IP range for your event filters.
- Make sure the following is set up in DDM Inventory:
  - SMTP server
  - SNMP traps setup (only if you plan to use SNMP traps)
- For accounts who are going to receive e-mail or pager messages:
  - Make sure their accounts are set up with proper e-mail addresses and pager e-mail addresses.
  - Test their e-mail addresses and pager e-mail addresses to make sure they are working.
- Make sure you have set the system-level priority for your important devices.

Once you know how to use all of these components together, you are ready to set up your event filters.

Event Filter Properties

The properties of event filters are as follows:

Table 8 Event Filter Properties

Property	Explanation
Name	The name can be 3-20 characters long, can include lower case letters, numbers, underscore (_), and hyphen (-). The underscore and hyphen cannot be the first character.
Description	The description can be 0-60 characters long; used to provide a reminder as to the purpose of the filter.
Event Type	You have a choice of several types of events for which you want to receive notification. • All (all of the categories listed below) • Adds (when a device is added in your specified IP range) • Deletes (when a device is deleted in your specified IP range) • Property (when you change a device property for the type of device specified in your IP range, like an icon, device priority, device tag, or device title) • Moves (when there is a connectivity change within your IP range, i.e., a changed port, or when devices are physically moved and connected differently; indicated by a *Port Moves* event in the Health Panel) Note: The safest and easiest way to make sure you get your event notification is to select the *All* Event Type category. That way, you will be notified if any of these categories has an event occur. However, if you want to receive notification for a very specific event, you should pick an event type.
Priority	The priority of devices about which you want to be notified.
Device Type	The type of device about which you want to be notified.
Line Alarm Type (only for Line Event Filters)	The type of lines about which you want to be notified.
IPv4 Range	Enter a range of IPv4 addresses in which you want to be notified of this event.
Notification	Notifications must include an action, and can include an account. • send e-mail • send alphanumeric page via e-mail gateway • send SNMP trap data • create an XML file

Example of an Event Filter

There are many ways to set up event filters. Sometimes, it is difficult to understand all the possible implications.

It is always best to create simple and specific event filters that are easy to understand.

Read this section to understand how to create a few common, simple, and helpful event filters. If you have more questions, please call Customer Support.

Example: Notification When a Device is Added to or Removed from the Network

You may want to know when a particular type of device is added to or removed from the network. For this example, we will set up an event filter that will page an Administrator account when any Linux workstation is added or removed.

To set up the Administrator account:

1. Click **Administration** > **Account Administration** > **Account contact data**.
2. Select the Administrator account that you want to change.
3. Click **Modify Properties**.
4. Enter your pager e-mail address.
5. Click **Modify Contact Data**.

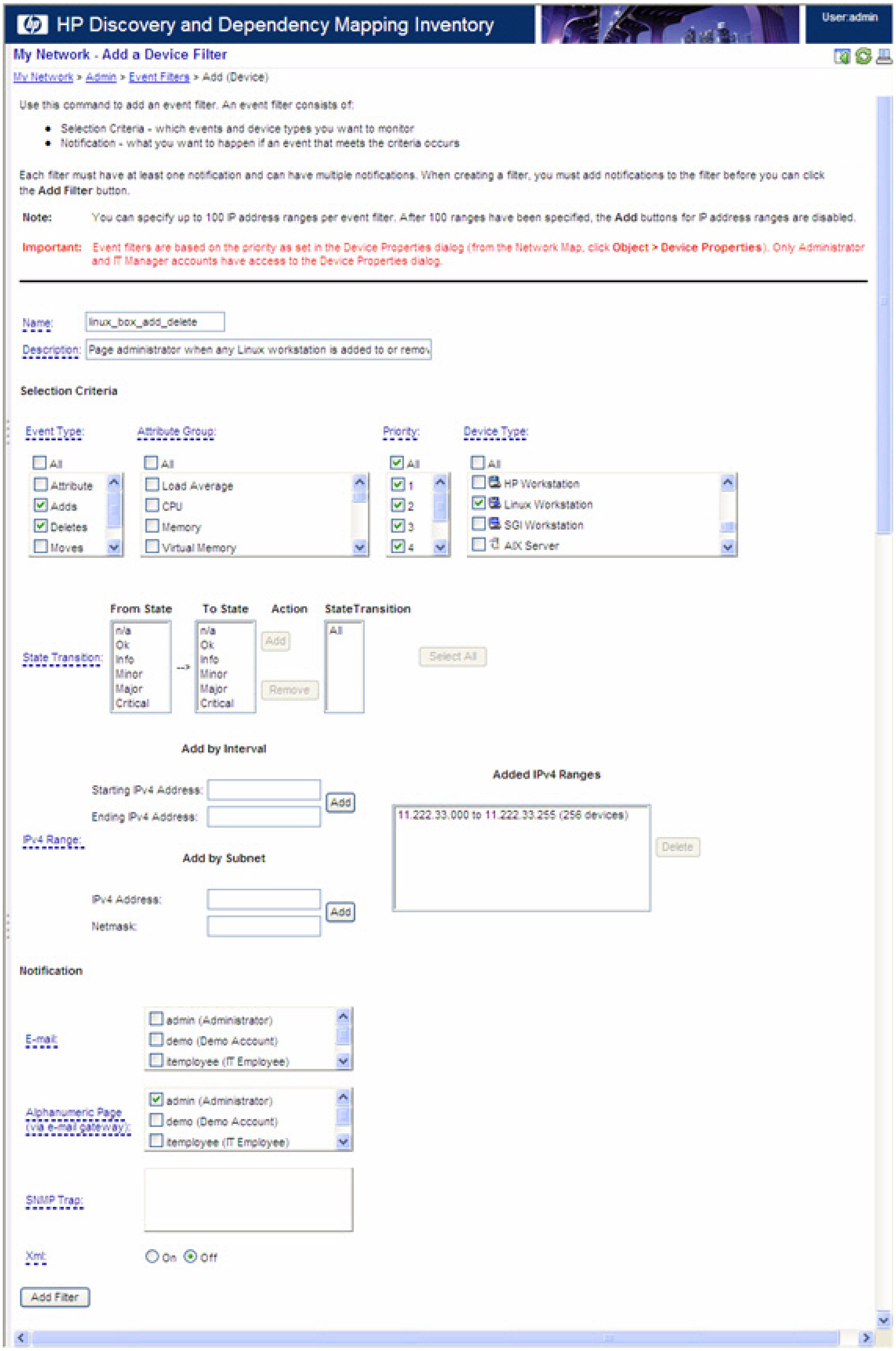
To set up the event filter:

1. Click **Administration** > **Event Filter Configuration** > **Add a device filter**.
2. Enter the event filter information as it appears in this table:

Table 9 Example 1 Input

Field:	Enter:
Name (create a name for the filter)	linux_box_add_delete
Description	Page administrator when any Linux workstation is added/removed
Event Types	Adds and Deletes
Priority	All
Device Type	Linux Workstation
IPv4 Range	Select the devices or IP range you want this event filter to monitor
Alphanumeric Page (via e-mail gateway)	Select the Administrator account

3. Click **Add Filter**.



HP Discovery and Dependency Mapping Inventory

User:admin

My Network - Add a Device Filter

My Network > Admin > Event Filters > Add (Device)

Use this command to add an event filter. An event filter consists of:

- Selection Criteria - which events and device types you want to monitor
- Notification - what you want to happen if an event that meets the criteria occurs

Each filter must have at least one notification and can have multiple notifications. When creating a filter, you must add notifications to the filter before you can click the **Add Filter** button.

Note: You can specify up to 100 IP address ranges per event filter. After 100 ranges have been specified, the **Add** buttons for IP address ranges are disabled.

Important: Event filters are based on the priority as set in the Device Properties dialog (from the Network Map, click **Object > Device Properties**). Only Administrator and IT Manager accounts have access to the Device Properties dialog.

Name: linux_box_add_delete

Description: Page administrator when any Linux workstation is added to or remov

Selection Criteria

Event Type:
- □ All
- □ Attribute
- ☑ Adds
- ☑ Deletes
- □ Moves

Attribute Group:
- □ All
- □ Load Average
- □ CPU
- □ Memory
- □ Virtual Memory

Priority:
- ☑ All
- ☑ 1
- ☑ 2
- ☑ 3
- ☑ 4

Device Type:
- □ All
- □ HP Workstation
- ☑ Linux Workstation
- □ SGI Workstation
- □ AIX Server

State Transition:

From State: n/a, Ok, Info, Minor, Major, Critical

-->

To State: n/a, Ok, Info, Minor, Major, Critical

Action: Add, Remove

StateTransition: All

Select All

IPv4 Range:

Add by Interval

Starting IPv4 Address:

Ending IPv4 Address:

Add

Add by Subnet

IPv4 Address:

Netmask:

Add

Added IPv4 Ranges

11.222.33.000 to 11.222.33.255 (256 devices)

Delete

Notification

E-mail:
- □ admin (Administrator)
- □ demo (Demo Account)
- □ itemployee (IT Employee)

Alphanumeric Page (via e-mail gateway):
- ☑ admin (Administrator)
- □ demo (Demo Account)
- □ itemployee (IT Employee)

SNMP Trap:

Xml: ○ On ● Off

Add Filter

Modifying a Filter

To select a filter to modify:

1. Click **Administration** > **Event Filter Configuration** > **Modify a filter**.
2. Select an event filter from the pull-down list.
3. Click **Modify Filter**.

To edit the description of the filter:

When using Selection Criteria list boxes, you can select multiple options.

Windows users: Use the Shift and Control keys in combination with clicking the mouse.

1. Select one or more options from the Event Type list box.
2. Select one or more options from the Priority list box.
3. Select one or more options from the Device Type list box.
4. Select one or more options from the Line Alarm list box.

➤ These selection criteria apply to all notifications.

To enter the IPv4 range:

1. Click **Add by interval** and enter the starting and ending IPv4 addresses **or** click **Add by subnet** and enter the IPv4 address and netmask.
2. Click **Add IPv4 Range**.

➤ Use primary IPv4 addresses. To find a device's primary IPv4 address, look at the top of the Device Manager.

To select notification:

1. Select the appropriate notification for the event filter:
    - E-mail
    - Alphanumeric Page (via e-mail gateway)
    - SNMP Trap

To modify filter:

1. Click **Modify Filter**.

➤ DDM Inventory does not check to see if the user has provided the appropriate contact data.

Deleting a Filter

To delete an event filter:

1. Click **Administration** > **Event Filter Configuration** > **Delete a filter**.
2. Select a filter name from the list box.

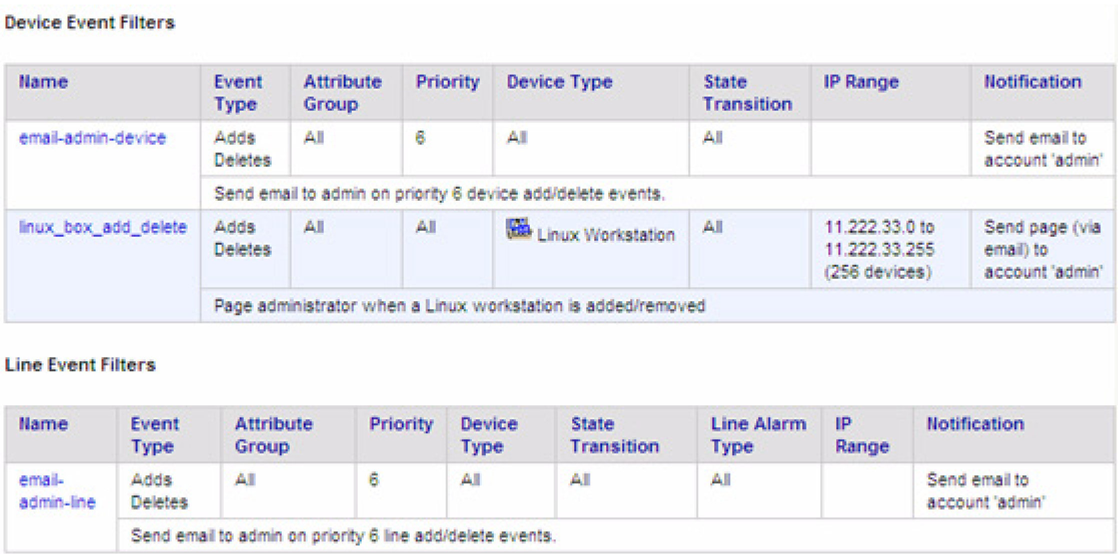
   Profiles are listed by name.
3. Click **Delete Filter**.
4. Click **Confirm**.

Listing Event Filters

The filter names are hyperlinked. Clicking the hyperlinks will take you to the Modifying a Filter page for that filter.

To list filters:

1. Click **Administration** > **Event Filter Configuration** > **List filters**.



Device Event Filters

Name	Event Type	Attribute Group	Priority	Device Type	State Transition	IP Range	Notification
email-admin-device	Adds Deletes	All	6	All	All		Send email to account 'admin'
	Send email to admin on priority 6 device add/delete events.						
linux_box_add_delete	Adds Deletes	All	All	Linux Workstation	All	11.222.33.0 to 11.222.33.255 (256 devices)	Send page (via email) to account 'admin'
	Page administrator when a Linux workstation is added/removed						

Line Event Filters

Name	Event Type	Attribute Group	Priority	Device Type	State Transition	Line Alarm Type	IP Range	Notification
email-admin-line	Adds Deletes	All	6	All	All	All		Send email to account 'admin'
	Send email to admin on priority 6 line add/delete events.							

2. Click a filter name hyperlink for more information about that filter.

Resetting to Defaults

To reset to default filters:

This action cannot be undone.

1. Click **Administration** > **Event Filter Configuration** > **Reset to defaults**.
2. Click **Reset to Defaults**.

5 Adding, Removing, and Replacing Devices

There will be many situations when you are adding or replacing devices in your network. You will have to take precautions when performing these activities, such as making sure all devices have unique IP and MAC addresses.

Topics included in this chapter are:

Importance of Unique IP Addresses

DDM Inventory relies mostly on device IP addresses for gathering statistics and information. It is important to have unique IP addresses for all your devices and their components.

If you have duplicate IP and MAC addresses in your network, you may have difficulty obtaining accurate device and port statistics.

If you do have duplicate IP or MAC addresses, you can purge the devices, then reassign the device addresses as necessary. DDM Inventory will then rediscover the devices and map them properly.

This section features several possible scenarios, for adding, removing, or replacing devices and ports in your network. If you experience problems and cannot find help in the documentation, contact your DDM Inventory Customer Support representative.

➤ When you remove a device from the network, purge the device. This will ensure that it is no longer in the database.

Adding a Device

These procedures will be helpful when you are adding any new device to your network.

➤ If one or more of the ports on the device you add is the end of a Permanent Virtual Circuit (PVC), make sure you add the correct Committed Information Rate (CIR) to the Port Manager.

Once you have added a device to your network, DDM Inventory will discover it automatically. If you want the device to appear in the database and on your map quickly, follow this procedure.

To make a new device appear in DDM Inventory quickly:

1 From the Home page, click the **Find** button.

2 In the Find window, enter the IP address or domain name of the new device.

  A warning appears, saying that DDM Inventory does not have the device in its database. However, a link to the device appears.

3 Double-click the device name to open a Device Manager session.

4 In the Device Manager, click **Update Model**.

5 From the pull-down list, select **Query Device**.

6 Click **Update**. DDM Inventory begins network discovery on the device immediately.

Replacing a Device

There are many reasons for replacing one of your network devices. Perhaps a device has been damaged, or you could be upgrading part of your network. Whenever you are replacing a network device, be sure to use one of the following procedures.

➤ If one or more of the ports on this device is the end of a Permanent Virtual Circuit (PVC), make sure you add the correct Committed Information Rate (CIR) to the Port Manager.

With Identical Device

If you are replacing one device with another of the same model, and the same MAC address, DDM Inventory will see no difference between the two devices. DDM Inventory will register a break alarm when the first device is shut down, but will clear that alarm when the new device is powered on.

If the new device has different MAC and IP addresses, it is best to purge the old device manually. This ensures that the device model for your new device is not merged with the model of the old device.

➤ Properties (such as priority, device type, etc.) from “replaced” devices are not automatically assigned to “new” devices. For example, if the Administrator manually changed the priority of the old device, and you are introducing a new device with the same IP address as the old device, make sure you manually change the priority of the new device. This will ensure correct event notification.

With Different Device

When you replace a device with a different device and a unique IP address, it always best to purge the old device before adding the new device.

Changing IP address of a Device

There are several reasons why you may be changing the IP address for a device. Some common reasons are:

- You have been changing your subnets.
- You assigned an IP to a device, but discovered that the IP is not allowed because it falls within a reserved IP range.
- You have accidentally created a duplicate IP in your network, and need to change one of the addresses.

Changing the IP address of the device does not affect how DDM Inventory sees the network. Read the following notes to make sure you understand how DDM Inventory reacts.

➤ If you change the IP of the device, but the MAC remains the same, the DDM Inventory database updates automatically.

➤ If you change the IP of a port, DDM Inventory automatically discovers the change. No additional action is required.

➤ If you change the IP of the device, and the MAC is not known, the update is slightly delayed.

Changing Cards or Ports in a Device

If you change all the cards in a device (and they have all new MAC addresses), DDM Inventory reads the device as a completely new device.

If you change all but one card in a device, the new information is temporarily merged with the old information. The new ports are discovered automatically, but the old ports remain in the database until they are aged out. This means there may be some duplicate ports listed in the Device Manager.

The best procedure is to purge the device before you change its ports or purge the old ports. Then, DDM Inventory rediscovers the device as if it were new.

Removing Devices

Devices can be removed from the DDM Inventory database in one of two ways: automatic or manual. This table shows the methods of removing devices.

Table 10 Automatic and Manual Device Removal

Method	Performed by	How it works
automatic	DDM Inventory	3 stages • deactivate • purge • obliterate
manual	an IT Manager or Administrator user	3 methods • hide • deactivate • purge

This table compares the Hide, Deactivate, Purge, and Obliterate features.

Table 11 Hide, Deactivate, and Purge

Action	Hide	Deactivate	Purge	Obliterate[a]
device removed from Network Map	✓	✓	✓	✓
device can be recovered if seen	—	✓	✓[b]	—[b]
“delete” event generated	✓	✓	✓	—

Table 11 Hide, Deactivate, and Purge

Action	Hide	Deactivate	Purge	Obliterate[a]
device statistics deleted	—	—	✓	✓
device events deleted from Events Browser	—	—	✓	✓
device events deleted from Reports Database	—	—	—	✓

a. Devices cannot be manually obliterated.

b. Once removed from the Discovery Database, a device can still be rediscovered, but it will be considered a new device.

Removing Devices Automatically

The deactivation interval begins as soon as a device is discovered, and restarts after every model update. When the deactivation interval ends, the device is made inactive.

A deactivation interval refers to the length of time DDM Inventory will wait before it makes a device inactive. The deactivation interval should be long enough that devices are allowed to be turned off for long periods, but short enough that devices removed from the network are not needlessly kept in the database.

There is limited space for deactivated devices. Once this capacity is exceeded, devices are purged, regardless of the deactivation interval. The number of devices that can be deactivated at one time is 10% of the device license for the DDM Inventory server.

When the device is inactive, it is considered “deactivated” and appears in the list of devices at **Status > Deactivated Devices**. Once the device is inactive, the purge interval begins. When the device is set to be purged, one of two things can happen:

- If your device license capacity is full in the Discovery database, the purged device will be obliterated, meaning that the device and all its associated data will be removed from the database.
- If there is space in the Discovery database, the purged device will remain in the database until the obliteration interval passes.

The number of purged devices that DDM Inventory keeps depends on your license. For example, if you have a 10,000 device license, with 8,000 active devices in your network, DDM Inventory will be able to keep records for 2,000 purged devices. However, active devices always take precedence over purged devices. If you have 10,000 active devices, DDM Inventory will not save any purged devices in its database.

Changing Device Expiry Intervals

Device expiry has three steps: deactivation, purge, and obliteration.

For deactivation and purge, there are three intervals, one each for devices with:

- SNMP management
- no SNMP management
- Scanner-only devices (if available in your network)

Whether or not the deactivation interval is accepted depends on your Device Modeler Interval.

The obliteration interval is the same for all devices.

To change the expiry intervals:

1 Click **Administration** > **System Configuration** > **Expiry.**

2 Enter the time values deactivation, purge, and obliteration.

3 Click **Change**.

Managing Devices with Dynamically Assigned IP Addresses

Reusing IP addresses is a common occurrence for users who connect their laptops over VPN, where a new temporary IP address is assigned to the device each time the user connects to the network. IP addresses can also be reassigned to devices if your office network has a short DHCP address lease time-out. In this case, devices may get disconnected from the network for longer periods of time causing their IP addresses to be reused.

By default, DDM Inventory will not deactivate devices with duplicate IP addresses in its database. However, it will remove the main IP address from the older device record and unschedule all modeling and scanning requests to run on the older device until the device's new IP address is discovered. The default setting ensures that DDM Inventory will not deactivate devices in its database that have had their IP addresses reassigned to a different device. The devices will continue to be active and searchable in the database. When there is a duplicate IP address for a device in the database, DDM Inventory will create an exception, and the device is marked with an asterisk (*) in the Configuration Panel of the Device Manager.

You can configure DDM Inventory to deactivate a device in its database if it discovers another device with the same IP address. If you decide to deactivate devices with duplicate IP addresses and you add a new device to the network that has the same IP address as an active device, the old device will automatically be moved to the list of Deactivated Devices (**Status** > **Deactivated Devices**). You will also see an exception for the old device, stating that the device has been deactivated because of a "duplicate IP address."

Also, if you decide to use this option and a device has been deactivated (either manually by the user, or automatically by DDM Inventory), and you add a new device with the same IP address, there will not be a "duplicate IP address" exception.

However, if the deactivated device becomes reactivated (either manually by the user or it is rediscovered by DDM Inventory), there will be a "duplicate IP address" exception. Reactivation works similarly for deactivated devices and for devices with cleaned IP addresses.

If you turn on this option, it will also be enabled if you upgrade to a later release of DDM Inventory in order to preserve the current behavior of your system.

To deactivate devices with duplicate IP addresses

1 Click **Administration** > **System Configuration** > **Network Devices**.

2 For the **Deactivate older devices with duplicate IP addresses** option, select **Custom** and select **Yes**.

3 Click **Change**.

Removing Devices Manually

The manual removal process can occur in three ways. An Administrator can Deactivate, Hide, or Purge a device.

By using these commands, you are *not* making a physical change to the device or network. The manual removal of a device from the database and Network Map should be accompanied by its physical removal from the network, otherwise the device may reappear.

To prevent the device from reappearing, you must do one of three things:

- Actually disconnect the device from your network
- Assign a Basic Discovery configuration profile with the "Allow group to manage devices" property turned off to the device group that manages this device (**Administration > Discovery Configuration > Configuration Profiles)**

  ➤ Devices can belong to multiple device groups. Be sure to apply this profile to the device group that actually manages this device. To determine which device group this is, open the Device Manager, click the Diagnosis button, and see the Configuration Profiles table.

- Use the Hide command to stop a device from being rediscovered

➤ If a device has not been seen for the period set (in **Administration > System Configuration > Expiry** —see Changing Device Expiry Intervals on page 43), DDM Inventory automatically takes appropriate action.

➤ If you change the address ranges in **Discovery Configuration**, devices that are no longer included in the ranges are automatically deactivated.

The Deactivate, Hide, and Purge commands are available on the Network Map, through the Object menu. The commands are also available through the Device Manager Device Visibility panel, or by right-clicking on the device in any applet window (for example, the Alarms Viewer).

If you want to Activate a device that you have hidden or deactivated, see Activating Devices on page 48.

Hiding Devices

This command removes the device from the Network Map and all reports, though a complete record of the device and its history is kept. The only way to bring the device back to the Network Map is to use the Activate command. Once hidden, this device will appear on the list at **Status > Device Status > Hidden Devices**.

The device remains hidden until reverted manually by an administrative command.

For example, if you have a MAC-only device that appears on the map, and you don't want to see it, "Hiding" it is the best way to get rid of it. Hidden devices still count towards your device license limit.

To hide a device—starting from the Network Map

1. Select a device on the Network Map.
2. Click **Object > Visibility > Hide**.

   A confirmation message appears.
3. Click **OK**.

To hide a device from the network—starting from the Device Manager:

1. Click the **Device Visibility** button.
2. Select **Hide** from the pull-down list.
3. Click **Hide**.

Purging Devices

If you use Purge, the device will vanish from the Network Map and database, but will reappear if the device is still included in an actively discovered device group. Purging removes all traces of the device from the system, including all identification and history. If the device is still on the network, it may be rediscovered at some future time.

The only way to make sure a device never reappears on the Network Map or in DDM Inventory reports is to use the Hide command.

‼ The Purge command cannot be undone.

To purge a device from the network—starting from the Network Map

1. Physically remove the device from your network following your company's standard procedures.
2. Locate the device on the Network Map using the **Find** tool.
3. With the device icon selected, **Object > Visibility > Purge**.

   A confirmation message appears.
4. Click **OK**.

To purge a device from the network—starting from the Device Manager:

1. Click the **Device Visibility** button.
2. Select **Purge** from the pull-down list.
3. Click **Purge**.

To purge a port from a device:

1. In the Port Manager, click the **Purge port** button.

   A confirmation message appears.
2. Click **Purge**.

Deactivating Devices

This command makes a device inactive. DDM Inventory will stop monitoring the device's statistics. If the device is rediscovered by DDM Inventory, it will be reactivated, and will return to the Network Map. Otherwise, you can use the Activate command to manually bring this device back to the Network Map. When deactivated, this device will appear on the list at **Status > Device Status > Deactivated Devices**.

To deactivate a device from the network—starting from the Network Map

1. Select a device on the Network Map.
2. Click **Object > Visibility > Deactivate**.

   A confirmation message appears.

3 Click **OK**.

To deactivate a device from the network—starting from the Device Manager:

1 Click the **Device Visibility** button.

2 Select **Deactivate** from the pull-down list.

3 Click **Deactivate**.

Removing Stale Connections

Related to removing devices (deactivate, purge, obliterate), you can also automatically remove stale connections from your database.

Once a connection has a line break, you can change the length of time that will pass until the connection is automatically deleted.

Activating Devices

This command will bring a device from the list of hidden or deactivated devices, and back onto the Network Map. DDM Inventory will start monitoring this device again.

➤ You can re-activate devices if they have been deactivated or hidden by DDM Inventory, or by an Administrator.

For information on how to Hide, Purge, or Deactivate devices, see Removing Devices on page 42.

To reactivate a device from the hidden list:

1. Click **Status > Device Status > Hidden Devices**.
2. Click on the device title.

   A Device Manager will open for that hidden device.
3. Click the Device Visibility button.
4. Select "Activate" from the pull-down list.
5. Click **Activate**.

The device should return to the database and the Network Map, and DDM Inventory will begin to monitor this device again.

To reactivate a device from the deactivated list:

1. Click **Status > Device Status > Deactivated Devices**.
2. Click on the device title.

   A Device Manager will open for that deactivated device.
3. Click the Device Visibility button.
4. Select "Activate" from the pull-down list.
5. Click **Activate**.

The device should return to the Network Map, and DDM Inventory will begin to monitor this device again.

6 Exporting Data into Data Access Applications

There are many tools that you can use to gain access to the MySQL database. You can use any tools from MySQL (www.mysql.com), or others that you already use in your organization.

In order to gain access to the MySQL database, you must first create a MySQL account under **Administration > MySQL accounts**. Once that is complete, you can export the data into your other applications.

This chapter contains a sample tutorial, taking you through a simple example of how to connect to the DDM Inventory database from Microsoft Access by means of ODBC; how to link in the tables and perform two basic queries.

Topics in this chapter include:

Step 1: Set up Your MySQL Account

In order to access the MySQL database through ODBC, you must create a MySQL account in **Administration > MySQL accounts**.

These accounts are completely distinct from regular DDM Inventory accounts. They will only give the user access to MySQL, not to any UI features.

1 Click **Administration > MySQL accounts > Add an account**.

2 Enter the account name and password (twice).

3 Click **Add User**.

Step 2: Install MySQL ODBC Driver

If your computer does not already have a MySQL driver, download the latest MySQL Connector/ODBC driver MSI or executable from the following URL and run the program:

http://dev.mysql.com/downloads/connector/odbc/

In this example we have downloaded version 5.1.8 of the MySQL Connector/ODBC driver.

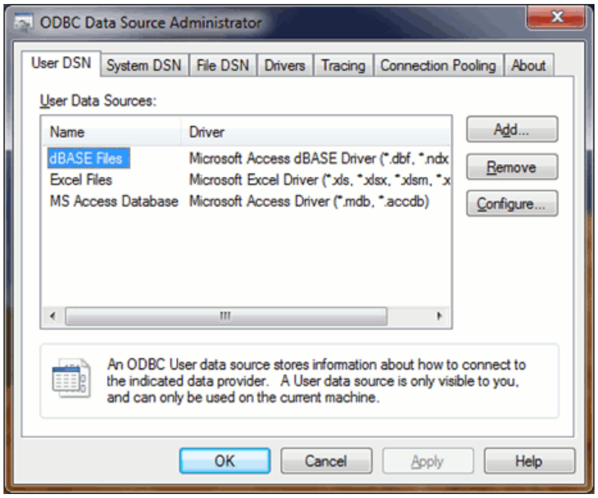
Step 3: Select MySQL as Data Source (Create ODBC Alias)

Before you can use the DDM Inventory data with Microsoft Access, you need to create an ODBC alias for the database.

To set up MySQL as the data source, perform the following steps:

1 In the Windows **Control Panel**, select **Administrative Tools > Data Sources (ODBC)**.

The **ODBC Data Source Administrator** dialog box appears.



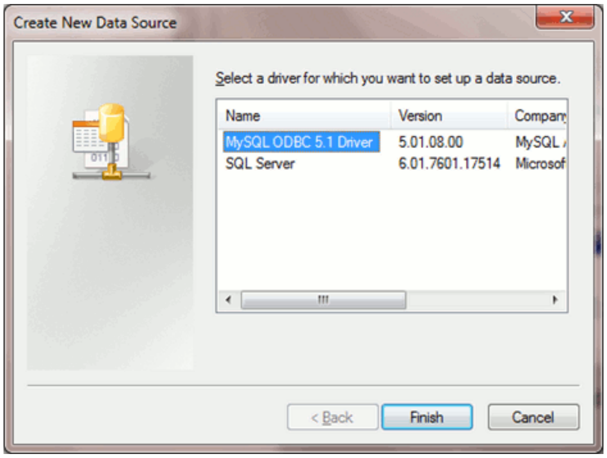
User Data Sources:

Name	Driver
dBASE Files	Microsoft Access dBASE Driver (*.dbf, *.ndx
Excel Files	Microsoft Excel Driver (*.xls, *.xlsx, *.xlsm, *.x
MS Access Database	Microsoft Access Driver (*.mdb, *.accdb)

An ODBC User data source stores information about how to connect to the indicated data provider. A User data source is only visible to you, and can only be used on the current machine.

2 On the **User DSN** tab, click **Add**.

The **Create New Data Source** dialog box appears.



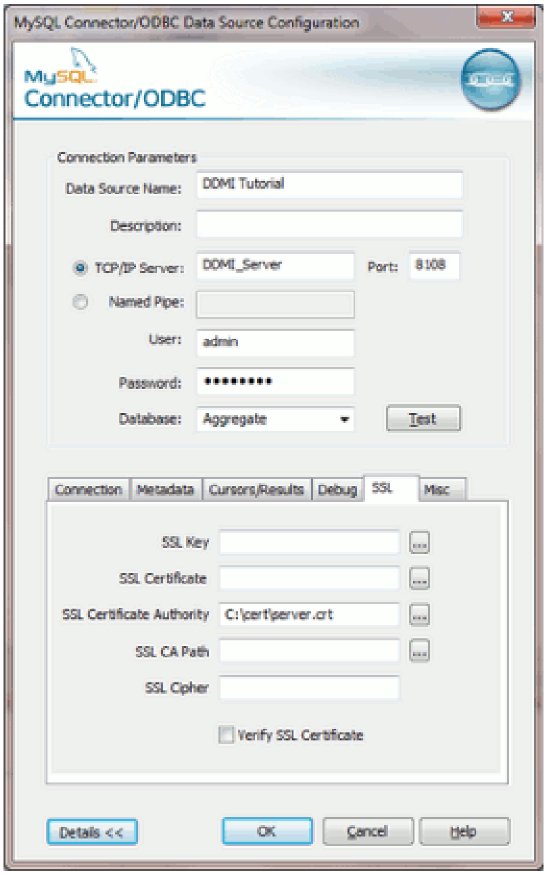
Select a driver for which you want to set up a data source.

Name	Version	Compan
MySQL ODBC 5.1 Driver	5.01.08.00	MySQL /
SQL Server	6.01.7601.17514	Microsof

3 In the list box, select **MySQL ODBC**.

4 Click **Finish**.

The **My SQL Connector/ODBC Data Source Configuration** dialog box appears.



Connection Parameters

Data Source Name: DDMI Tutorial

Description:

● TCP/IP Server: DDMI_Server Port: 8108

○ Named Pipe:

User: admin

Password: ••••••••

Database: Aggregate

SSL Key

SSL Certificate

SSL Certificate Authority C:\cert\server.crt

SSL CA Path

SSL Cipher

□ Verify SSL Certificate

5 Enter the following information:

- The Windows Data Source Name (DSN). In the following example, we have called it **DDMI Tutorial**.
- The name or IP address of the DDM Inventory server.
- For the port number, always enter **8108**.

- For the name of the user, enter the account name of anyone who has been set up with a user account.
- Enter the password for the above user.
- In the **Database** name field, select the name of the database from the drop-down list.

6 Although optional, we recommend that you protect MySQL connections via SSL to avoid any potential security problems. To establish a secure connection, you will need to navigate to the **SSL** tab. For the **SSL Certificate Authority** field, enter the name of the SSL certificate file (server.crt) that is copied from the DDM Inventory server. You can find the server.crt file in the `<DataDir>\cert\ssl.crt` folder.

7 Once you have entered these fields, click **OK**.

Now you are returned to the **UserDSN** tab in the **ODBC Data Source Administrator** dialog box.

8 Click **OK** to exit.

You are now ready to connect to the DDM Inventory database with applications such as MS Access by means of ODBC.

Step 4: Create New Database in Microsoft Access 2000

To create a new database

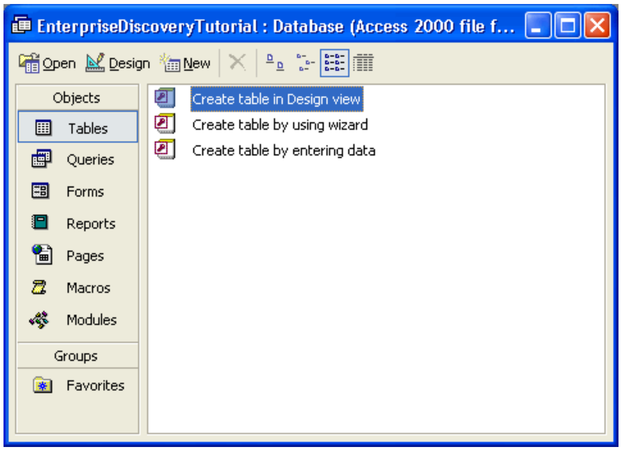
1 Start Microsoft Access.

2 Create a new blank database. Give it a name and save it.

In this example, the database has been named **DDMITutorial.mdb** and saved in the following directory

```
C:\Program Files\Hewlett-Packard\DDMI\9.30\Common
```

The following dialog is displayed.


EnterpriseDiscoveryTutorial : Database (Access 2000 file f...
Open
Design
New
Objects
Tables
Queries
Forms
Reports
Pages
Macros
Modules
Groups
Favorites
Create table in Design view
Create table by using wizard
Create table by entering data

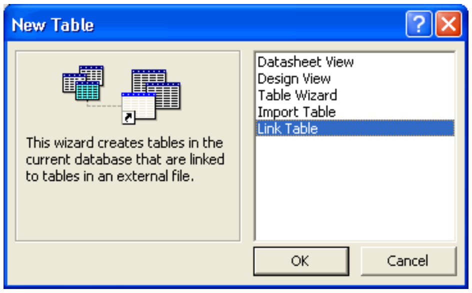
Step 5: Link in DDM Inventory Tables

To fully understand the DDM Inventory database, you can read full documentation in the web UI by clicking **Help > Database Schema**.

To link in the DDM Inventory tables

1 In the Objects menu, select **Tables** and click **New**.

The New Table dialog appears.


New Table
This wizard creates tables in the current database that are linked to tables in an external file.
Datasheet View
Design View
Table Wizard
Import Table
Link Table
OK
Cancel

2 Select **Link Table** and click **OK**. The Link screen opens.

3 On the Link screen from the **Files of type** pull-down list, select **ODBC Databases**.

The following dialog appears.

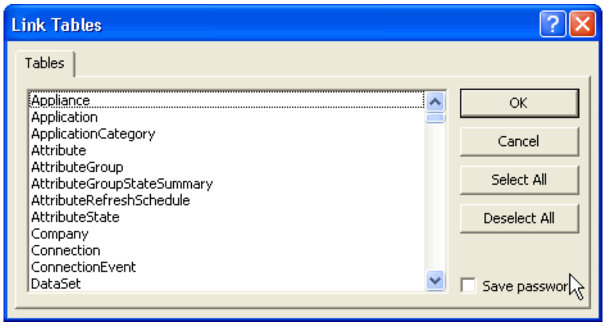
The **DDMITutorial.mdb** file is not supplied with DDM Inventory but is the file that you created in step 2 on page 52.

4 Click the **Machine Data Source** tab.

5 Select your entry (in this case **DDMITutorial**) and click **OK**.

This is the Tutorial data source name that you created in step 5 on page 51.

The following **Link Tables** dialog is displayed.

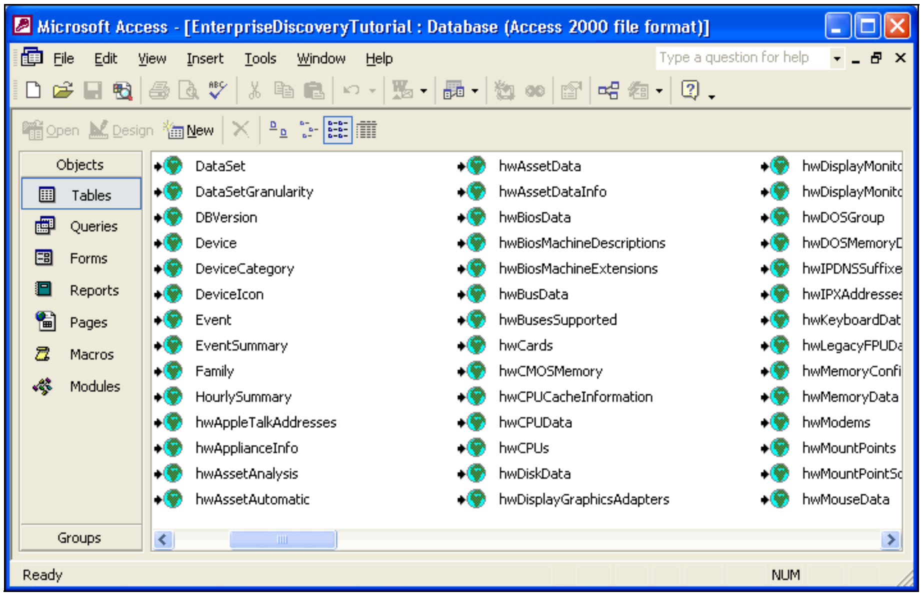


6 Click **Select All**.

All the entries are now highlighted.

7 Click **OK**.

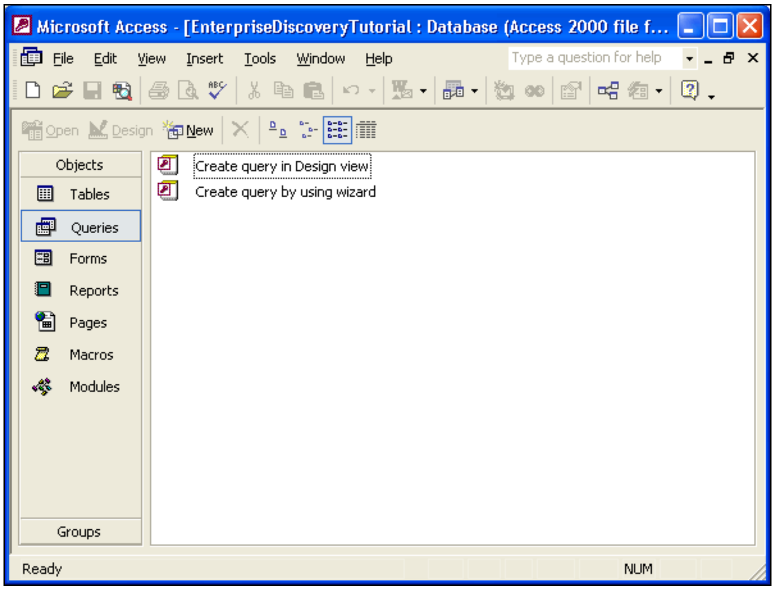
You are returned to the **Tables** Tab which shows the newly linked DDM Inventory tables.



Step 6: Create Basic Assets and Recognition Query

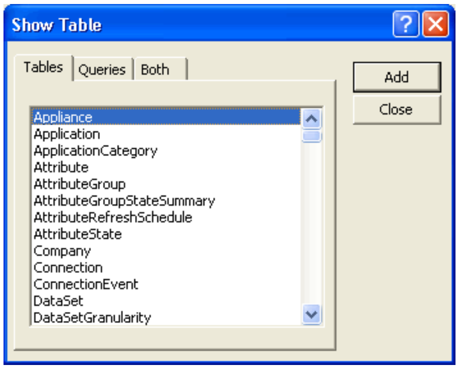
To create a basic assets and recognition query

1 From the **Objects** list, select **Queries**.


Microsoft Access - [EnterpriseDiscoveryTutorial : Database (Access 2000 file f...
File Edit View Insert Tools Window Help
Type a question for help
Open Design New
Objects
Tables
Queries
Forms
Reports
Pages
Macros
Modules
Groups
Create query in Design view
Create query by using wizard
Ready
NUM

2 Double click **Create query in Design view.**

The **Show Table** dialog appears.



Appliance
Application
ApplicationCategory
Attribute
AttributeGroup
AttributeGroupStateSummary
AttributeRefreshSchedule
AttributeState
Company
Connection
ConnectionEvent
DataSet
DataSetGranularity

3 In the **Tables** tab page, from the list, select:

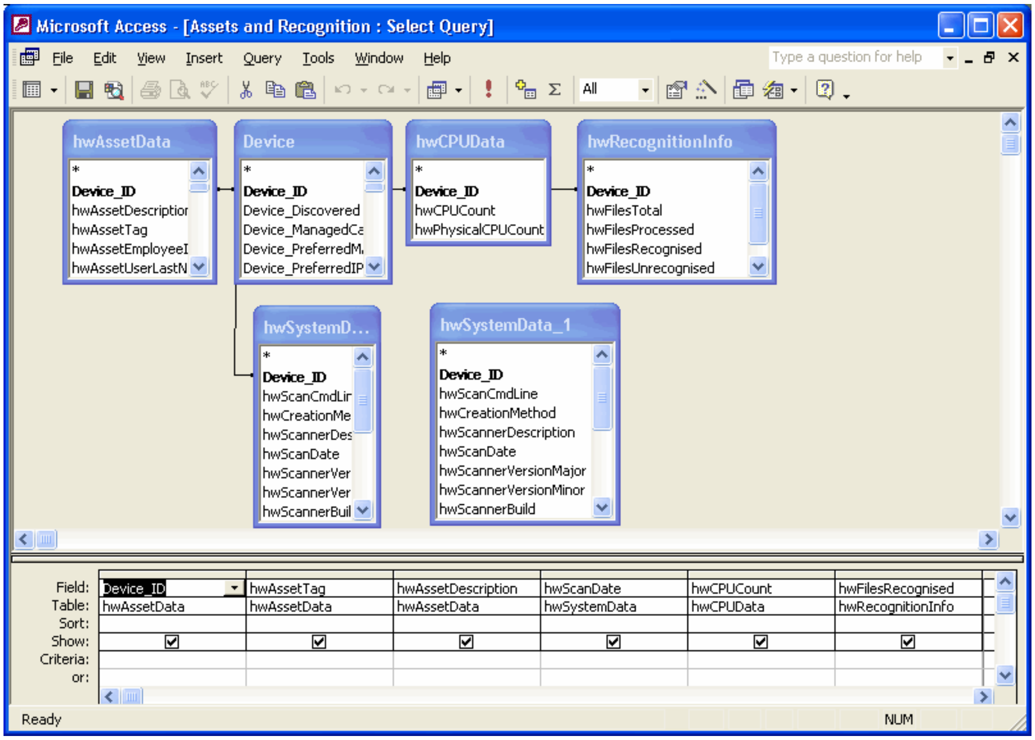
- hwAssetData
- Device
- hwCPUData
- hwRecognitionInfo
- hwSystemData

4 With the table selected, click Close.

The table appears.

5 Save the query. (In this example we have called it **Assets and Recognition**.)

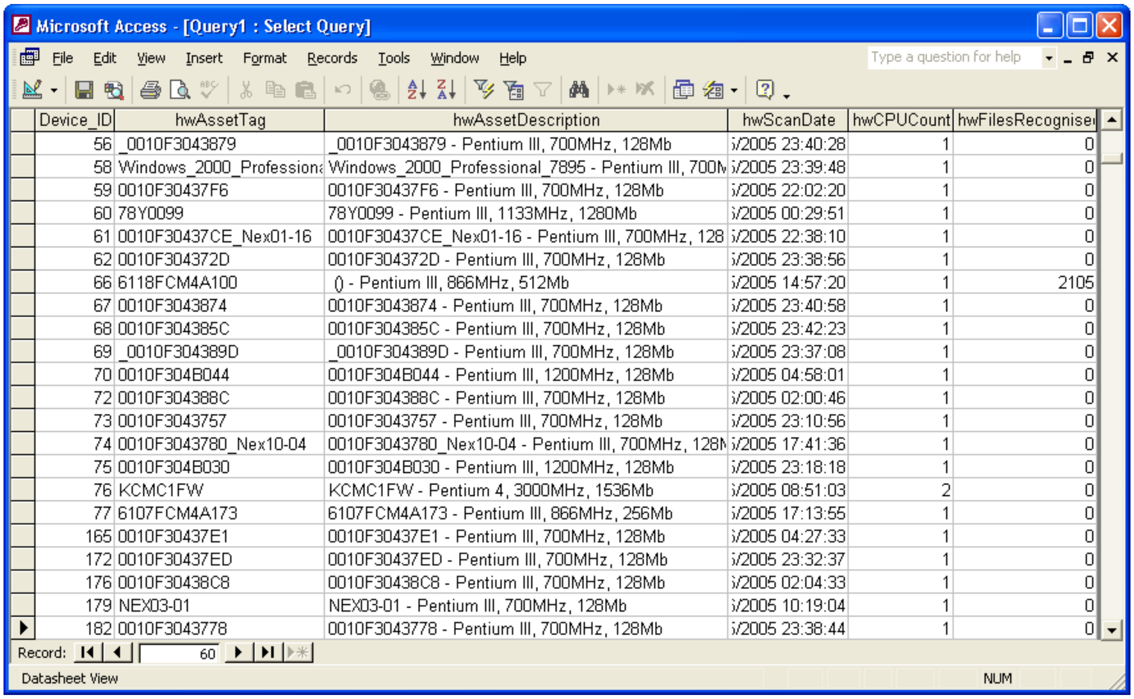
6 Enter the query field parameters as shown below:



Field:	Device_ID	hwAssetTag	hwAssetDescription	hwScanDate	hwCPUCount	hwFilesRecognised
Table:	hwAssetData	hwAssetData	hwAssetData	hwSystemData	hwCPUData	hwRecognitionInfo
Sort:						
Show:	☑	☑	☑	☑	☑	☑
Criteria:						
or:						

7 Run the Query. From the **Query** pull-down menu, select **Run**.

A query is generated, showing asset and recognition data from the inventory scans in the Inventory Database.


Microsoft Access - [Query1 : Select Query]
File Edit View Insert Format Records Tools Window Help
Type a question for help

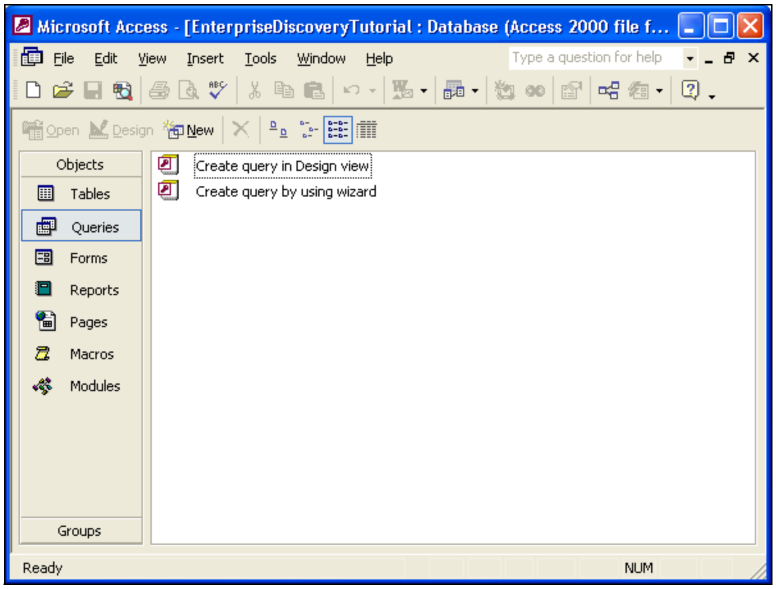
Device_ID	hwAssetTag	hwAssetDescription	hwScanDate	hwCPUCount	hwFilesRecognise
56	_0010F3043879	_0010F3043879 - Pentium III, 700MHz, 128Mb	/2005 23:40:28	1	0
58	Windows_2000_Professiona	Windows_2000_Professional_7895 - Pentium III, 700M	/2005 23:39:48	1	0
59	0010F30437F6	0010F30437F6 - Pentium III, 700MHz, 128Mb	/2005 22:02:20	1	0
60	78Y0099	78Y0099 - Pentium III, 1133MHz, 1280Mb	/2005 00:29:51	1	0
61	0010F30437CE_Nex01-16	0010F30437CE_Nex01-16 - Pentium III, 700MHz, 128	/2005 22:38:10	1	0
62	0010F304372D	0010F304372D - Pentium III, 700MHz, 128Mb	/2005 23:38:56	1	0
66	6118FCM4A100	() - Pentium III, 866MHz, 512Mb	/2005 14:57:20	1	2105
67	0010F3043874	0010F3043874 - Pentium III, 700MHz, 128Mb	/2005 23:40:58	1	0
68	0010F304385C	0010F304385C - Pentium III, 700MHz, 128Mb	/2005 23:42:23	1	0
69	_0010F304389D	_0010F304389D - Pentium III, 700MHz, 128Mb	/2005 23:37:08	1	0
70	0010F304B044	0010F304B044 - Pentium III, 1200MHz, 128Mb	/2005 04:58:01	1	0
72	0010F304388C	0010F304388C - Pentium III, 700MHz, 128Mb	/2005 02:00:46	1	0
73	0010F3043757	0010F3043757 - Pentium III, 700MHz, 128Mb	/2005 23:10:56	1	0
74	0010F3043780_Nex10-04	0010F3043780_Nex10-04 - Pentium III, 700MHz, 128M	/2005 17:41:36	1	0
75	0010F304B030	0010F304B030 - Pentium III, 1200MHz, 128Mb	/2005 23:18:18	1	0
76	KCMC1FW	KCMC1FW - Pentium 4, 3000MHz, 1536Mb	/2005 08:51:03	2	0
77	6107FCM4A173	6107FCM4A173 - Pentium III, 866MHz, 256Mb	/2005 17:13:55	1	0
165	0010F30437E1	0010F30437E1 - Pentium III, 700MHz, 128Mb	/2005 04:27:33	1	0
172	0010F30437ED	0010F30437ED - Pentium III, 700MHz, 128Mb	/2005 23:32:37	1	0
176	0010F30438C8	0010F30438C8 - Pentium III, 700MHz, 128Mb	/2005 02:04:33	1	0
179	NEX03-01	NEX03-01 - Pentium III, 700MHz, 128Mb	/2005 10:19:04	1	0
182	0010F3043778	0010F3043778 - Pentium III, 700MHz, 128Mb	/2005 23:38:44	1	0

Record: 60

Step 7: Create Basic License Query

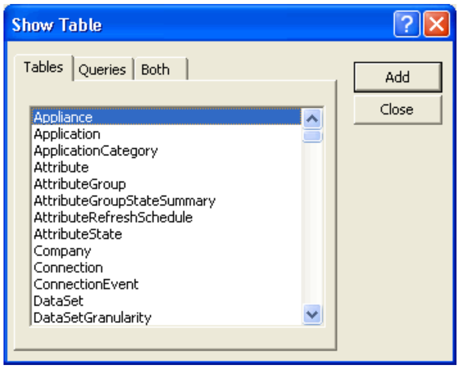
To create a basic license query

1 From the **Objects** list, select **Queries**.


Microsoft Access - [EnterpriseDiscoveryTutorial : Database (Access 2000 file f...
File Edit View Insert Tools Window Help
Type a question for help
Open
Design
New
Objects
Tables
Queries
Forms
Reports
Pages
Macros
Modules
Groups
Create query in Design view
Create query by using wizard
Ready
NUM

2 Double click **Create query in Design view.**

The **Show Table** dialog appears.



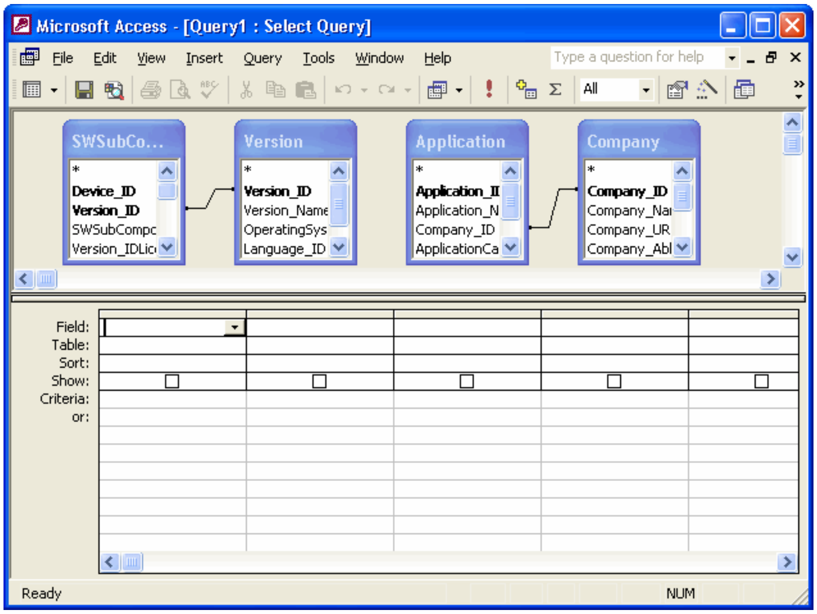
Appliance
Application
ApplicationCategory
Attribute
AttributeGroup
AttributeGroupStateSummary
AttributeRefreshSchedule
AttributeState
Company
Connection
ConnectionEvent
DataSet
DataSetGranularity

3 In the **Tables** tab page, select:

- Company.Company_Name
- Release.Release_Name
- SWSubComponent.SWSubComponent_LicenceRequired
- Version.Version_Name
- Application.Application_Name

4 With the table selected, click **Add**, then **Close**.

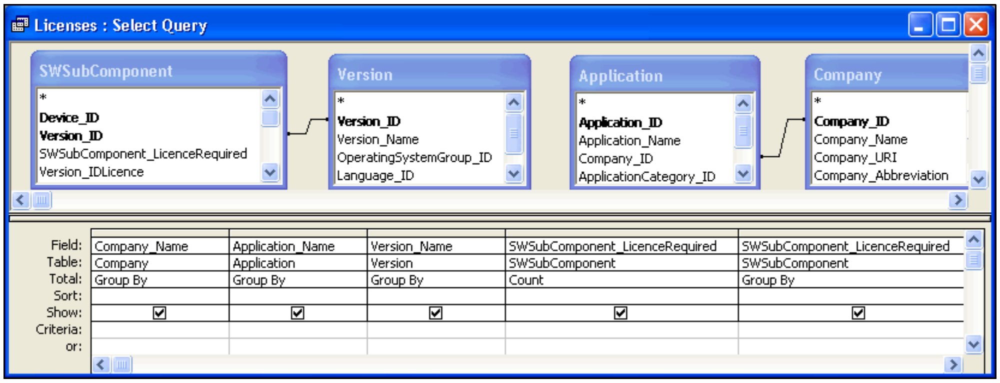
The table displayed is similar to this:



5 Click **File > Save As** and save the query

In this example, we have called it **Licenses**.

6 Enter the query field parameters as shown below:



Field:	Company_Name	Application_Name	Version_Name	SWSubComponent_LicenceRequired	SWSubComponent_LicenceRequired
Table:	Company	Application	Version	SWSubComponent	SWSubComponent
Total:	Group By	Group By	Group By	Count	Group By
Sort:					
Show:	☑	☑	☑	☑	☑
Criteria:					
or:					

7 Run the Query. From the **Query** pull down menu, select the **Run** option.

A query is generated, showing license data from the inventory scans in the Inventory Database.

Establishing a Secure Connection to MySQL

As mentioned in Step 3, although optional, we recommend that you protect MySQL connections via SSL to avoid any potential security problems. In Step 3, we demonstrated how to enable SSL connections on ODBC connections. However, if you prefer to use the MySQL command line tools to access the database, you may proceed with the instructions outlined in this step. To establish a secure connection, you will need to perform the following actions:

1 Copy the server.crt file from the DDM Inventory server to the client machine. The server.crt file is located in the `<DataDir>\cert\ssl.crt` folder.

2 Connect securely by using the **--ssl-ca** option, as follows:

```
shell> mysql --user==user_name --password=your_password --host=host_name
--port=8108 --ssl-ca=c:\cert\server.crt
```

Here, the account has no special SSL requirements, or was created using a GRANT statement that includes the **REQUIRE SSL** option.

A client can determine whether the current connection with the server uses SSL by checking the value of the **Ssl_cipher** status variable. To check whether the current connection is secure, you will need to manually issue the SQL command (SHOW STATUS LIKE 'Ssl_cipher'). The value of **Ssl_cipher** is not empty if SSL is used, and empty otherwise. For example, when you check the value of the **Ssl_cipher** status variable, you will see code that resembles the following:

```
mysql> SHOW STATUS LIKE 'Ssl_cipher';

+------------+----------------+

| Variable_name | Value |

+------------+----------------+

| Ssl_cipher | DHE-RSA-AES256-SHA |

+------------+----------------+
```

Here, the value is not empty; therefore, the connection is secure.

7 Deleting Data and Connections

This section is for Administrator accounts only.

Do not perform these procedures unless you completely understand the consequences.

After you delete connections, DDM Inventory will start building connections again. This could take a long time, especially in large networks.

By changing the deactivation and purge intervals, you risk removing devices from your network that would not be removed with the default settings.

Deleting Data

This procedure will delete all of your network and configuration data. Once you complete this operation, your server will appear as it did when you first installed DDM Inventory.

Deleting network data and statistics stored on your server is an extremely drastic action that cannot be undone. Your backup data will not be deleted, however you should consider making an external backup of your data first. See the *Installation and Initial Setup Guide*.

There are three options of increasing severity, and the options are outlined in the following table:

Table 12 Delete Data

What gets deleted	Network data	Above plus accounts	Above plus configuration data
Device models	✓	✓	✓
Connection data	✓	✓	✓
Device and Port Statistics	✓	✓	✓
Forecast views	✓	✓	✓
Scan Files	✓	✓	✓
Prime Map Configuration	✓	✓	✓
Map Configuration Files for all accounts	✓	✓	✓

Table 12 Delete Data

What gets deleted	Network data	Above plus accounts	Above plus configuration data
Device and Line fault events	✓	✓	✓
Reports	✓	✓	✓
Account names and passwords	—	✓	✓
Account Properties and Contact Data	—	✓	✓
Account Map Preferences	—	✓	✓
Server Configuration	—	—	✓
Discovery Configuration (Device groups, configuration profiles, etc.)	—	—	✓
System Configuration settings	—	—	✓
SNMP Trap Recipients	—	—	✓
Event Filters	—	—	✓
Router Discovery Settings/Results	—	—	✓
MySQL Accounts	—	—	✓
Agent Deployment Accounts	—	—	✓
Asset Questionnaire configuration	—	—	✓
All Remote Server data[a]	—	—	✓

[a] This applies only when an Aggregator license is present.

To delete DDM Inventory data:

1 Click **Administration** > **Data management** > **Delete data**.

2 Select one of the following:

- Network data
- Above plus accounts

- Above plus configuration data

3 Click **Delete Data**.

4 Click **Confirm** to delete the data.

Deleting Connections

This procedure will delete connections between objects on the Network Map. It will take a few minutes for changes to be reflected in the map.

You can choose to delete:

- all the connections that have been made, both those established by DDM Inventory and those defined by the user
- just the connections defined by the user

If you delete all connections, DDM Inventory will start over in its attempts to establish connections between objects. User-defined connections will not be re-established by DDM Inventory, no matter which of the two options you select.

You can potentially lose all the connectivity data DDM Inventory has gathered.

This action cannot be undone.

To delete all connections:

1 Click **Administration** > **Data management** > **Delete connections**.

2 Select **All**.

3 Click **Delete Connections**.

4 Click **Confirm**.

Both automatic and user-defined connections are deleted.

After connections are deleted, DDM Inventory will restart its attempts to establish automatic connections between objects. It will not reconstruct user-defined connections.

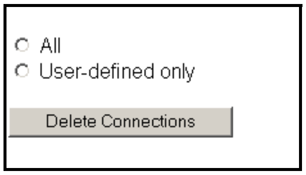
To delete user-defined connections:

1 Click **Administration** > **Data management** > **Delete connections**.

2 Select **User-defined only**.

3 Click **Delete Connections**.

4 Click **Confirm**.



8 Changing Device and Port Properties

If you have an Administrator or IT Manager account, you can change various Device and Port Properties. This chapter shows you how to do this.

Customizing for IT Manager and Administrator Accounts

This section is for IT Manager and Administrator accounts.

IT Manager and Administrator accounts can make changes to the Network Map that affect what all accounts see.

When you make changes to a map configuration, the changes have the potential to affect all accounts and all configurations.

Table 13 Properties

To change	Do this	Affects other accounts and maps	Also affects
icon—devices	see Changing Device Properties on page 64	✓	• whether event filters are applied (all accounts) • reports
icon—packages	see the *Network Data Analysis Guide*	—	—
tag	Changing Device Properties on page 64	—	—
derived title (devices)	see **Administration > System Configuration > Display preferences**	✓	—
title	see Changing Device Properties on page 64	✓	—
priority (devices)	see Changing Device Properties on page 64	✓	whether event filters are applied (all accounts)
to top object	see the *Network Data Analysis Guide*	—	—

Changing Device Properties

If you have an Administrator or IT Manager account, you can change the following in the Device Properties dialog (click the Properties button on the Device Manager):

- Device Icon
- Device Tag
- Device Title
- Device Priority

‼ Changing a device icon affects what reports the device appears in.

Changing a device icon can change how it is packaged. Certain icons are packaged automatically. For example, when you change an end node icon to an icon that is not an end node, the device may be automatically unpacked. If you change a device icon to an end node icon, that device can be automatically packaged with the end nodes. See **Administration > System Configuration > Automatic packaging**.

You might increase the priority of a device that is important to you or a device that you will want to monitor more closely. Devices with priority 6 are the most important. The higher the number, the higher the priority and the greater the importance.

To change Device Properties:

1 In the Device Manager, click the **Properties** button.

The Device Properties dialog appears.

2 To change the device icon, select a new icon from the pull-down list.

3 To change the device tag, enter your own custom text.

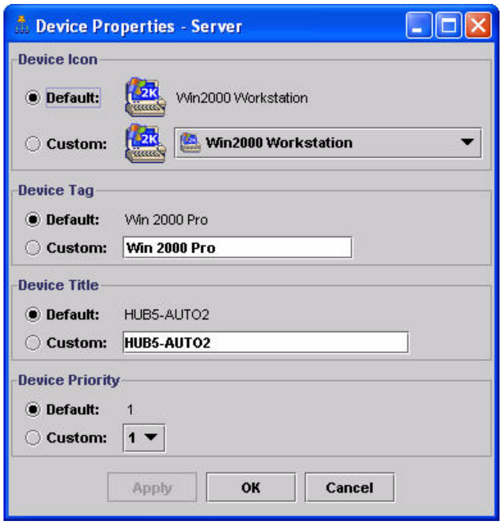
4 To change the device title, enter your own custom text.

5 To change the device priority, select a new priority from the pull-down list.

6 Click **Apply**.

7 Click **OK**.

➤ As soon as you change a property, DDM Inventory will register a change event in the Events Browser.



Device Properties - Server

Device Icon

● Default: Win2000 Workstation

○ Custom: Win2000 Workstation ▼

Device Tag

● Default: Win 2000 Pro

○ Custom: Win 2000 Pro

Device Title

● Default: HUB5-AUTO2

○ Custom: HUB5-AUTO2

Device Priority

● Default: 1

○ Custom: 1 ▼

To reset Device Properties to the default settings:

1 In the Device Manager, click the **Properties** button.

The Device Properties dialog appears.

2 For the properties you wish to reset, select “Default.”

3 Click **Apply**.

4 Click **OK**.

Changing Port Properties

If you have an Administrator or IT Manager account, you can change the following in the Port Properties dialog (click the Properties button on the Port Manager):

- Interface Rate
- Interface Type
- Line Alarm Type
- Duplex Mode

To change Port Properties:

1 In the Port Manager, click the **Properties** button.

The Port Properties dialog appears.

2 To change the Interface Rate, add a new rate in the custom text box.

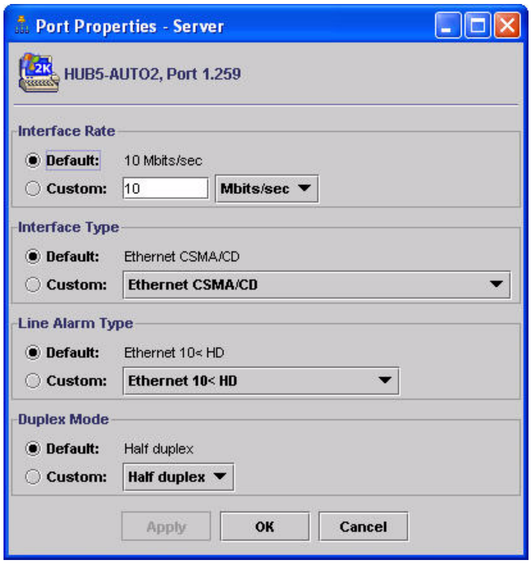
3 To change the Interface Type, select a new type from the pull-down list.

4 To change the Line Alarm Type, select a new type from the pull-down list.

5 To change the Duplex Mode, select a mode from the pull-down list.

6 Click **Apply**.

7 Click **OK**.



Port Properties - Server

HUB5-AUTO2, Port 1.259

Interface Rate

● Default: 10 Mbits/sec

○ Custom: 10 Mbits/sec

Interface Type

● Default: Ethernet CSMA/CD

○ Custom: Ethernet CSMA/CD

Line Alarm Type

● Default: Ethernet 10< HD

○ Custom: Ethernet 10< HD

Duplex Mode

● Default: Half duplex

○ Custom: Half duplex

To reset Port Properties to the default settings:

1 In the Port Manager, click the **Properties** button.

The Port Properties dialog appears.

2 For the properties you wish to reset, select "Default."

3 Click **Apply**.

4 Click **OK**.

9 Pre-Scan and Post-Scan Scripts for Collecting Custom Hardware Data

The pre-scan and post-scan scripts feature enables you to customize and execute scripts on scanned devices as part of the DDM Inventory scanning process. It expands the capabilities of standard scanner detection by capturing custom data on specific hardware, settings, or applications that the scanner does not currently collect in its inventory data. External scripts can be run as part of the scanner operation to capture this additional inventory information.

The pre-scan scripts run at scanner start-up, before the hardware and software scanning. The post-scan scripts run after the hardware and software scanning is complete.

➤ By default, the Scanners will not run the pre-scan and post-scan scripts until you enable this option in the scanner profile. For detailed information, refer to “Configuration Profiles” in the “Discovery Configuration Overview” section in the *Installation and Initial Setup Guide*.

➤ The pre-scan and post-scan scripts feature only works if the DDM Inventory agent 7.70 or later is installed. This feature will not work with older agents.

Pre-Scan and Post-Scan Script File Names

You can create the pre-scan and post-scan script files based on your own requirements. But you must save them with the file names shown below:

- For UNIX:
  - `prescan.sh`
  - `postscan.sh`
- For Windows:
  - `prescan.cmd`
  - `postscan.cmd`

Pre-Scan and Post-Scan Script File Path

The DDM Inventory server creates sub-directories under the `<DataDir>\PrePostScripting` directory to store the pre-scan and post-scan script files as well as other related files and folders. Each of these sub-directories corresponds to a different operating system (See the table below).

➤ It is important to save all pre-scan and post-scan files in the correct sub-directory. For more information about the data directories, refer to the *Server Installation* chapter in the *Installation and Initial Setup Guide*.

Table 14 Sub-directories and descriptions

Sub-directory	Description
`all-unix`	This directory applies to all supported UNIX-based platforms, such as UNIX and Mac OS X. Because the scripting logic is common for all UNIX-based platforms, it can be included only once in this directory. You can put the pre-scan and post-scan script files in either the `\all-unix` directory or the UNIX directory that corresponds to the device's UNIX platform (for example, AIX (POWER)). The DDM Inventory server will search for the pre-scan and post-scan script files in the directory corresponding to the device's specific UNIX platform (for example, `\aix-ppc`) first. If it cannot find any scripts, the server will search in the `\all-unix` directory.
`aix-ppc`	This directory applies to AIX (POWER) only.
`hpux-hppa`	This directory applies to HP-UX (HPPA) only.
`hpux-ia64`	This directory applies to HP-UX (ia64) only.
`macosx-ppc`	This directory applies to Mac OS X (PPC) only.
`macosx-x86`	This directory applies to Mac OS X (x86) only.
`linux-x86`	This directory applies to Linux (x86) only.
`solaris-sparc`	This directory applies to Solaris (SPARC) only.
`solaris-x86`	This directory applies to Solaris (x86) only.
`win32-x86`	This directory applies to Windows (32-bit and 64-bit) operating systems.

You must copy the script files to the corresponding directory of the device's OS system. For example, copy the script files to `\Linux-x86` if the device's OS system is Linux. When pre-scan and post-scan scripts are detected, the Scanner will include an additional option *`-scripts:<folder>`* where *`<folder>`* is the directory to which you upload the scripts. Then the Scanner will execute the pre-scan and post-scan script files, such as `prescan.sh` and `postscan.sh`.

On the target computer, the script files are copied to the PrePost subdirectory of the agent's data directory, depending on the operating system that you are running.

- UNIX/Mac OS X: $HOME/.discagnt/prepost
- Windows: <*AppData*>\Peregrine\Enterprise Discovery\Data\prepost, where <*AppData*> is the Application Data directory for the profile that is used by the agent Windows service, which by default is usually one of the following locations:
    - Windows XP/Windows Server 2003: C:\Documents and Settings\LocalService\Application Data
    - Windows Vista and above: C:\Windows\system32\config\systemprofile\AppData\Roaming

Pre-scan and Post-scan Script Process

You need to create the pre-scan and post-scan script files and copy them to the appropriate folder.

To use pre-scan and post-scan scripts:

1 Create the pre-scan and post-scan script files.

Be sure to name the script files as described in Pre-Scan and Post-Scan Script File Names on page 67.

2 Copy the script files along with any related files and folders to the corresponding folder on the DDM Inventory server. For detailed information, see Pre-Scan and Post-Scan Script File Path on page 67.

After you complete these steps, the following steps are performed automatically:

1 The server uploads the script files and related files or folders to the corresponding device.

2 The DDM Inventory Scanner runs the pre-scan scripts.

3 The Scanner performs the normal inventory scan process.

4 The Scanner runs the post-scan scripts.

5 The Scanner reads the output of the post-scan script and captures all lines with the following structure:

```
<attribute>=<value>
```

- The length of `<attribute>` can be up to 256 characters, and the length of `<value>` can be up to 1024 characters.
- The Scanner captures any script output line that has an **=** in it, except if **=** is the first character on the line.
- Spaces are valid characters and will be included in the `<attribute>` or `<value>`. For example:
  `<attribute> = <value>` will be collected as `<attribute>`<space> and <space>`<value>`.
- If multiple `<attribute>=<value>` entries exist, the Scanner will capture and store them all in the scan file.
- Empty value is permitted and will be collected as the name-only captures, such as: `<attribute>=`.

The Scanner will parse these lines and extract a list of key-value pairs. Only this list will be saved in the scan file and all the other lines will be ignored.

6 The Scanner collects and saves the scanned data in the scan file.

When the scan file is processed on the server, the keys and values captured by the post-scan script will be saved in the `Aggregate` database's `hwAssetCustomData` table.

You can process this data later to complement the information captured by the Scanner.

The Scanner has a hard-coded timeout of 5 minutes for the pre-scan and post-scan scripts. If the scripts run longer than 5 minutes, not all of its output may be captured.

User Scripts

You can execute other scripts and executables, or access datafiles by referencing them in the pre-scan and post-scan script files. To confirm that the scripts are running properly, you should test them on local machines using the same login credentials that the agent or agentless scanning process uses.

- UNIX scripts run using the default `sh` shell. If you want to use `bash` or other shells, you need to call another script from the pre-scan and post-scan script.

  For example:

  ```
  /bin/bash myBashScript.sh
  ```

- Windows scripts always run using the `cmd.exe`.
- UNIX scripts should be written with UNIX text editors. Using a Windows editor to create a UNIX script may result in the script not running correctly on UNIX.

Example of a Post-Scan Script File

The following example shows you how to create, test, and save a post-scan script file.

Example:

A DDM Inventory user wants to create a post-scan script file to obtain the following information:

- The installed date of the operating system on the Solaris 10 server.
- The version of Bash running on the Solaris machine.
- The version of Perl running on the Solaris machine.

➤ The installed data is stored in the EEPROM of the Solaris server. The scanner cannot obtain this value without the help of the Sun Microsystems "`sneep`" utility. The user needs to create a script to execute the `sneep` utility so that the custom field `OriginalInstallDate` can be stored in an asset field in the scan file.

Create the postscan.sh file

To create the `postscan.sh` file, save the following scripts into the `postscan.sh` file:

```
echo OriginalInstallDate=’sneep -t OriginalInstallDate’

echo BASH_VERSION=$BASH_VERSION

echo PerlVersion=’perl -v |  cut -d\  -f4 | grep v’
```

Test the postscan.sh file

To confirm if the post-scan file correctly displays the data in the format `<attribute>=<value>`, run the following command:

```
bash-3.00# ./postscan.sh
```

After running the `postscan.sh` file, you get the following information:

```
OriginalInstallDate=Oct-13-2007

BASHVERSION=3.00.16(1)-release
```

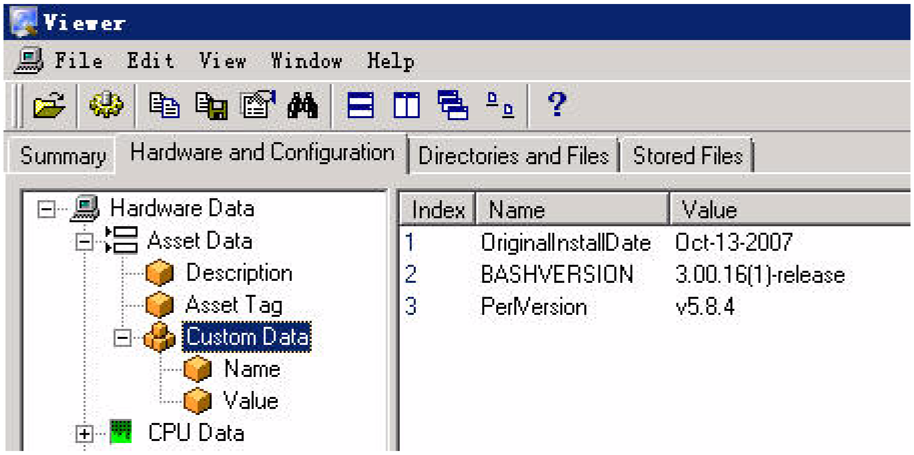
```
PerlVersion=v5.8.4
```

Save the postscan.sh file

You need to copy the `postscan.sh` file into the `<Datadir>\PrePostScripting\solaris-sparc` directory on the DDM Inventory Server.

When the Solaris scanner runs this `postscan.sh` script file, it will add the `OriginalInstallDate`, `BASHVERSION`, and `PerlVersion` fields into the Custom Data section of the asset data in the scan file.

You can view the data using the Viewer as shown below:



Index	Name	Value
1	OriginalInstallDate	Oct-13-2007
2	BASHVERSION	3.00.16(1)-release
3	PerlVersion	v5.8.4

Deleting Script Files after Execution

DDM Inventory always uploads pre-scan and post-scan script files, as well as any auxiliary files, but does not delete them from the managed computer. Therefore, if the scripts are renamed, they have to be cleaned up manually in the scripts themselves. You can easily clean all pre-scan and post-install script and other files after each execution, by performing the following steps:

Windows: add the following lines at the very end of the `postscan.cmd` file:

```
del <ScriptFile1>

del <ScriptFile2>

...

del postscan.cmd
```

UNIX/Mac OS X: add the following lines at the very end of the `postscan.sh` file:

```
rm -f <ScriptFile1>

rm -f <ScriptFile2>

...

rm -f postscan.sh
```

Where `<ScriptFileX>` is the name of extra script files that are used in addition to `postscan.sh`. If none are used, then only the last line is required to delete the `postscan.cmd/postscan.sh` file itself.

However, please note that it only makes sense to do this if the script files are small, as during each scanning workflow execution, the scripts have to be uploaded by the server again, thus using higher network bandwidth in comparison with cases in which the scripts are left in place after the scanner execution.

10 Configuring Scanner Settings

When you installed DDM Inventory, you set up some Scanner configuration profiles as part of your initial configuration (see the *Installation and Initial Setup Guide* for more details). If you choose to, you can change various Scanner deployment options.

To start configuring your Scan File settings:

1. Click **Administration** > **System Configuration** > **Scanner deployment**.
2. Change the settings as necessary.
   - AutoSequence Number on page 74
   - Minimum Scanner Execution Retry Frequency on page 75
   - Maximum Scanner Upgrade Attempts on page 75
   - Initial Time to Wait between Scanner Upgrade Attempts on page 75
   - Initial Time to Wait between Retrieve Scan File Attempts on page 75
   - Maximum Scan File Download Attempts on page 76
   - Download Current Scan File before Running Scanner on page 76
   - Scanner Versions on page 76
   - Scanner File Names on page 76
   - Scanner Locations on page 77
3. Click **Change**.

AutoSequence Number

The **AutoSequence Number** commands will help you assign an automatically generated number to your scan files. This feature is optional, but it will be helpful if you want to assign numbers to your scanned workstations. If you enable this function, each new scan file will be given a “hwAutoSequenceNumber” field that will contain this automatically generated number. You can use these options to determine the format of the number.

If you are using aggregation, you should assign unique sequences to every DDM Inventory Server in your network. If one asset is being monitored by two DDM Inventory Servers, the sequence number from one DDM Inventory server will be visible on the other.

The **Prefix** can be an alphanumeric string (valid characters are A-Z, a-z, 0-9, dash, and underscore).

There must be a prefix configured.

The **Character Count** determines how many digits will be in the **AutoNumber**.

The Next Number will be the number at which the Auto-generator will start. For example, if you enter “1”, the first asset number will be 0001.

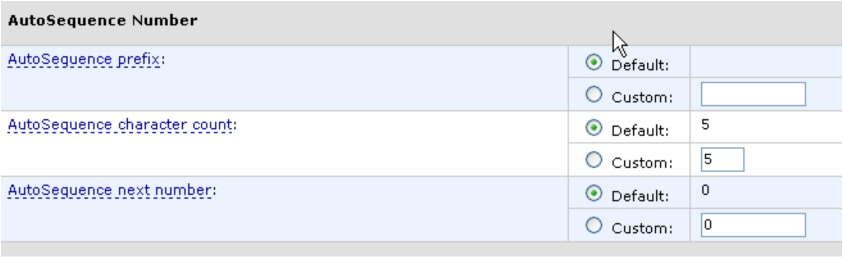
If you enter a **Next Number** that is more digits than configured in the character count, the character count will automatically change to accommodate.

To configure AutoSequence numbers:

1 Click **Administration** > **System Configuration** > **Scanner deployment**.

2 Enter a **Prefix**, **Character Count**, and **Next Number**.

3 Click **Change**.



AutoSequence Number		
AutoSequence prefix:	● Default:	
	○ Custom:	
AutoSequence character count:	● Default:	5
	○ Custom:	5
AutoSequence next number:	● Default:	0
	○ Custom:	0

Minimum Scanner Execution Retry Frequency

The minimum amount of time DDM Inventory will wait to attempt scanner execution.

➤ This setting should not occur every 24 hours. Try to avoid executing scanners at the same time every day. If you have many users on VPNs, set this to a shorter frequency.

If for some reason communication with a device is down, DDM Inventory will wait this length of time before trying to run the scanner again.

Maximum Scanner Upgrade Attempts

Maximum scanner upgrade attempts controls the maximum number of attempts made by DDM Inventory to transfer the relevant scanner executable and configuration files to a machine.

If the maximum is reached, processing begins from the Agent Upgrade step.

Initial Time to Wait between Scanner Upgrade Attempts

Initial time to wait between scanner upgrade attempts controls how long after a failed attempt will DDM Inventory wait before retrying to transfer the relevant scanner executable and configuration files to a machine. The time between the unsuccessful attempts becomes longer and longer (based on an exponential formula) and the value defined here represents the initial delay, after the first attempt.

Initial Time to Wait between Retrieve Scan File Attempts

Initial time to wait between retrieve scan files attempts (in case of failure) controls how long after a failed attempt will DDM Inventory wait before retrying to transfer the resulting scan file back to the server. The time between the unsuccessful attempts becomes longer and longer (based on an exponential formula) and the value defined here represents the initial delay, after the first attempt.

This option also controls how long DDM Inventory will wait after sending the Run Scanner request, before transferring the resulting scan file back to the server.

For example, the <fastsw> scanner takes a different amount of time than <hwonly>, so you may want to adjust this setting so that it is long enough for more than 80% of your network computers to complete scanning.

Maximum Scan File Download Attempts

Maximum scan file download attempts controls the maximum number of attempts made by DDM Inventory to transfer the resulting scan file back to the server.

If the maximum is reached, the process begins from the Agent Deployment step.

Download Current Scan File before Running Scanner

This option determines if the DDM Inventory Server will check how current the scan file is on the remote device before running the scanner. If the scan file on the remote device is newer than the one on the server, DDM Inventory will download the device's scan file before running the scheduled scan. When enabled, this option allows DDM Inventory to always have the most recent device information in its database before initiating a new scan.

You should enable this option if you have several users who connect to your network infrequently for short periods of time, such as VPN clients. When there are short connections, a scan may start but not complete during the connection interval. In this case, DDM Inventory will not have had the opportunity to download the latest scan file to its database since the scan completed after the user disconnected the device.

➤ If the connect time for a particular device is always short (and this option is not set), this process can repeat forever. As a result, even though the device is regularly scanned, the associated scan files are never downloaded and the related device information is never refreshed on the server database.

Scanner Versions

You can manually change the version of scanners you want to use for running on different operating systems. See **Help** > **Compatibility Matrix** in the DDM Inventory GUI for a complete list of supported operating system platforms.

This allows Scanner patches or upgrades to be applied for selected platforms only.

➤ For the Windows (x86) scanner, ".exe" is automatically appended to the name.

If this is your first installation of DDM Inventory, then there are only two options in the list: <latest> and the version shipped with the version of DDM Inventory you are using. As you upgrade to newer versions of the product, new versions will appear in this list.

Scanner File Names

You can manually change the name of the Scanner that will be sent to a particular type of computer.

Some antivirus programs may take note when DDM Inventory uploads a Scanner executable onto the remote computer. Using these setting to give the Scanner a unique name can exclude this name from being monitored by the antivirus program.

The default setting is appropriate in most cases.

Scanner Locations

If you use a tool other than DDM Inventory to deploy Scanners, you must specify the path name for the scanner executable on the network devices. Refer to "Using A Different Tool to Deploy Scanners" in the *Installation and Initial Deployment Guide* for more information.

The default setting is appropriate in most cases.

11 Agent Communication Configuration

In order to distribute and run Scanners on your workstations, you must first install an agent on each workstation.

The DDM Inventory server communicates with the Agent, allowing the server to run the Scanner and retrieve data from the devices and export it back to the server.

The agent is installed as a permanently running program on a remote computer. On Windows NT/200x/XP/Vista agent is installed as a Windows service. The agent enables the computer to be securely scanned at any given time.

- For security reasons, agent communication is encrypted and authenticated.
- The agent performs requests for the DDM Inventory server. For example, it can access a new scanner and execute it, or transfer a scan file to the server.

The agent must be installed on every computer that will be part of the automatic inventory process. If you are doing the inventory manually using manual deployment mode, you do not need the agent.

Communication with the agent can only be initiated by the server. The agent is not able to initiate any file transfers, scans, etc.

➤ Each agent originating from a server will have a security key from that server. This means that the agent will only be able to communicate with that server.

Supported Platforms for Discovery Agents

For a list of supported platforms for the discovery agents, see **Help** > **Compatibility Matrix** in the DDM Inventory GUI.

Disk Space Requirements on the Managed Device

Running scanners on your workstations requires a certain amount of available disk space on the workstation. Refer to the “Disk Space on Managed Devices” chapter in the *Installation and Initial Setup Guide*.

Agent Security

During the initial setup and installation DDM Inventory generates a new set of security certificates and keys to be used for secure communication between the agent and the server. These certificates and keys are stored in the `Cert` directory located under the `DDMI` data directory (usually `C:\Documents and Settings\All Users\Application Data\Hewlett-Packard\DDMI\Cert`). The generated files are as follows:

- `ACSKeyStore.bin` - contains private security key of the server, server and agent certificates.
- `acstrust.cert` - contains the exported server certificate to be used by the agent
- `agentca.pem` - contains the agent's private key and certificate.

‼ These are crucial files. Keeping a reliable backup of them is extremely important. `ACSKeyStore.bin` contains the private server key, so it must also be kept secret. If these files get overwritten or a new set is generated, DDM Inventory will not be able to talk to the installed agents any longer.

Once the set of certificates and keys has been generated, any successive installation on the same computer will not generate new certificates/keys, but will use the old ones instead.

If multiple DDM Inventory servers are used to communicate with the same agents, the certificates generated on one server need to be copied onto all the other servers.

‼ If you manually overwrite the security keys on the DDM Inventory server, you must restart the DDM Inventory server by restarting the System Monitor service. When the server is restarted, a new client set of security keys becomes embedded into the agent media files that correspond to the current keys that were used to overwrite the original ones on the DDM Inventory server.

Agent Media Files

After the security keys and certificates become available, DDM Inventory generates the agent media containing the corresponding agent security keys and certificates. In order to do this, the agent media files are taken from the `Agents\RawMedia` directory located under the DDM Inventory program directory (usually `C:\Program Files\Hewlett-Packard\DDMI\9.30\Agents\RawMedia`), the two agent specific security keys/certificate files `acstrust.cert` and `agentca.pem` are added to the agent media files and the resulting files are placed into the `LiveAgents` directory located under the `DDMI` data directory (usually `C:\Documents and Settings\All Users\Application Data\Hewlett-Packard\DDMI\LiveAgents).`

The content of this directory looks similar to this:

```
hp-ddm-inventory-agent-aix-ppc-9.30.000.1300.tar.Z
hp-ddm-inventory-agent-hpux-hppa-9.30.000.1300.tar.Z
hp-ddm-inventory-agent-linux-x86-9.30.000.1300.tar.Z
hp-ddm-inventory-agent-macosx-x86-9.30.000.1300.tar.Z
hp-ddm-inventory-agent-solaris-sparc-9.30.000.1300.tar.Z
hp-ddm-inventory-agent-solaris-x86-9.30.000.1300.tar.Z
HP DDM Inventory Agent (x86) 9.30.000.1300.msi
HP DDM Inventory Agent (PPC) 9.30.000.1300.dmg
```

- A `.tar.Z` file for each UNIX platform supported by the agent.
- A MAC disk image file (.dmg).
- An MSI setup file for Win32.

The agent version and the build number are included as part of the file name for each agent media file. Files from the `LiveAgent` directory are then used either for automatic or manual agent deployment.

Under no circumstances the agent media files from the `RawMedia` directory could be used to install agents. The files in this directory do not contain the agent keys/certificate required for secure communication. Only agent media files from the LiveAgent directory must be used.

Only the agent media files for the current version of the product are updated with the latest keys. Other agent media files that happen to be in the `LiveAgents` directory (for example, those belonging to older versions of DDM Inventory/Enterprise Discovery) are *not* updated.

Agent Directories

When the agent is installed on the computer it uses two directories for its operation:

- **Agent program directory.** This is the directory where the agent is installed to. The MSI installer uses the `Hewlett-Packard\Discovery Agent` directory under standard Windows `Program Files` directory. For UNIX agents, the installation directory is chosen manually during its deployment. For Mac OS X agents, the installation directory is the `/Library/StartupItems/DiscoveryAgent` directory.
- **Agent data directory.** This directory is used by the agent to store various files, such as logs, utilization data, etc.

  On Windows, it is normally located under the profile for the local service in `Application Data\Peregrine\Enterprise Discovery\Data`. The `discagnt.log` file is found in this directory. It is the log file that is written to by the agent on the local workstations and servers on which the agent runs.

  On UNIX, the data directory containing log files is the **$HOME/.discagnt** directory. On Mac OS X, it is the `/var/root/.discagnt` directory.

Initial Agent Deployment

Deployment through Windows RPC

This deployment method uses remote execution capabilities found in the Windows NT/200x/XP/Vista operating systems. For this reason it does not work on Windows 98SE based computers. In order for this method to work, the computer on which the agent is to be installed needs to meet these minimum requirements:

- Windows Installer must be installed and enabled in the Group Policy (see above for more details).
- On Windows XP, Simple File sharing mode should be turned off. This is controlled from the following Windows Explorer menu:

  `Tools->Folder Options->View -> Advanced Settings->Use simple file sharing`
- On Windows XP with Service Pack 2 installed or Windows 2003 Server with Service Pack 1, the firewall either should be switched off or when left on, the remote administration should be enabled. The officially recommended (by Microsoft) way of enabling remote administration on a population of computers is to enable it in the Group Policy. The remote administration can also be enabled manually by using this simple script (save as **enableremoteadmin.vbs** and run):

```
Set objFirewall = CreateObject("HNetCfg.FwMgr")
Set objPolicy = objFirewall.LocalPolicy.CurrentProfile
Set objAdminSettings = objPolicy.RemoteAdminSettings
objAdminSettings.Enabled = TRUE
```

However, this script requires administrator rights to work properly and must be run locally on the target computer.

Also if the firewall is enabled, **Do now allow exceptions** check box should not be checked in the firewall configuration.

In order to access remote computers, this deployment methods needs to know the administrator account name and password for the remote computer. This is usually a domain administrator account. As multiple domains can be in use, multiple account names/passwords can be entered. The order in which the accounts are tried is as follows:

- The account names where the domain matches the network model workgroup name. The network model workgroup is normally available when NetBIOS over TCP/IP is enabled on the remote computer. This allows the appropriate domain administrator account to be used first.
- The account names where the domain name is not specified (local administrator accounts).
- Any other remaining accounts.

The deployment code tries to connect to the remote computer's **ADMIN$** share using the administrator account names and passwords provided in the order described above. Once connection is established, it copies the agent installation to the remote computer and launches the installation. The DDM Inventory server only registers successful attempts to launch the installation. Once successfully launched, the agent installation can still fail because of external factors, such as lack of available disk space, etc. When this happens, detailed information is available in the log file `ovedagentinstaller.log` located in the Windows directory on the remote computer. This log file can help in troubleshooting agent installation problems.

Automatic Agent Deployment to Computers Running Windows Vista and Server 2008

In Windows Vista and Server 2008, a new feature called User Account Control (UAC) has been introduced to reduce the privileges of running programs. By default, a program launched by a local administrator is not given full administrator privileges. To run a program with full administrator rights, a local administrator can launch the program through a special Windows Explorer command, namely, "Run as administrator." Alternatively, a program can request to be run with full administrator rights, in which case the UAC dialog is shown so that the user can confirm that the program should be run with full local administrator rights.

UAC has an unfortunate side effect with regard to remote administration. When a local administrator account is connected to a computer remotely (either through Remote Desktop, "net use", etc.), the account is not given full administrator rights. Since accessing system shares requires full administrator privileges, it is not possible to connect to the default remote administration shares, such as `ADMIN$` using a local administrator account. For this reason, automatic agent deployment does not work properly using local administrator accounts.

There are two ways of resolving this issue:

- If a computer is in a domain, use a domain administrator account. When a domain administrator is logged in remotely, it is given full administrator privileges.
- Otherwise, if a local administrator account must be used, the policy on the Windows Vista computer needs to be modified to enable a local administrator to connect remotely with full administrator rights.

  To do this, run `regedit` on the Windows Vista or Server 2008 computer in question and look for the following registry key:

  ```
  HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\sys
  tem
  ```

  The registry value that gives full administrator rights is located under this registry key. The value is called `LocalAccountTokenFilterPolicy`. Create this registry value if it does not already exist. It is not there by default. To create this value, create a new `DWORD` value, name it `LocalAccountTokenFilterPolicy`, and set the value to 1. If the value is already there, make sure it is of type `DWORD` and has the value of 1. After this modification, agent deployment should work properly when using local administrator accounts.

➤ After this change has been made, local administrators connecting to the computer remotely will have full administrator privileges.

Custom Deployment

This deployment method allows the end user to create custom deployment process using a Windows batch script and/or other programs. For example, it is possible to implement a custom UNIX agent deployment, using SSH. DDM Inventory runs the currently configured shell (usually cmd.exe) with the /C parameter and passes the name of the program/batch file configured in the web UI (**Administration > System Configuration > Agent communication > Agent deployment command for custom**) to it. This custom program receives the following command line parameters:

- IP address of the box where the agent needs to be installed
- NMID of the device. This is the internal ID of the device in the DDM Inventory Database
- Version of the Windows (x86) agent media to be installed (for example: "`9.30.1300`"). The agent media files need to be taken from the LiveAgents directory.
- Version of the AIX (POWER) agent media
- Version of the HP-UX (HPPA) agent media
- Version of the HP-UX (ia64) agent media
- Version of the Linux (x86) agent media
- Version of the Solaris (SPARC) agent media
- Version of the Mac OS X (PPC) agent media
- Version of the Mac OS X (x86) agent media
- Version of the Solaris (x86) agent media
- Max bandwidth to use for the operation (in K/sec) or 0 if no limit was configured.
- Workgroup - network workgroup from the network model. This is detected from the NetBIOS workgroup name, which usually corresponds to the destination computer's domain name.

The deployment is considered to be successful if the program returns an exit code of 0.

To automatically deploy an agent

1. Configure the deployment methods to be used in the web UI.

   Administration > System Configuration > Agent communication > Agent deployment method

2. To deploy to a single device:

   - Open the device manager for the required device (for example by using the **Find** command on the front page of the web UI)
   - Click on the **Diagnosis** panel, go to the **Discovery Configuration** section and check the value for the **Agent deployment** property. The value should be **None** or **Deploy** in order to be able to execute the next step.
   - Click the **Update Model** icon at the top.
   - Select **Deploy Agent** from the drop-down box and click the **Update** button.

3. To deploy to a device group, configure the Agent configuration profile assigned to this device group to include agent deployment:

   a. Click **Administration > Discovery Configuration > Configuration Profiles.**

   b. Click the **Agent** tab.

   c. Click the name of the profile assigned to this device group.

   d. Make sure that **Allow Agent Communication** is selected.

   e. Select **Allow Agent Upgrade**, and specify the <All the time> schedule.

   f. From the **Agent deployment** list, select **Deploy.**

   g. Click **Save and Close**.

4 Activate the configuration changes.

➤ There is a system defined Agent configuration profile called <Deploy agent> which has the **Agent deployment** property set to **Deploy**. You can assign this profile to this device group if you prefer.

If the deployment attempt failed to start the agent installation, detailed progress log is available in the following place:

Device Manager> Diagnosis> Agent Log

Deployment through Login Scripts

Agents can also be installed via login scripts or a software distribution mechanism. In order to execute a silent installation that does not require any user interaction, the MSI installer can be executed with the following command line:

```
msiexec -qn -i "D:\PathToLiveAgents\HP DDM Inventory Agent (x86)
9.30.000.1300.msi"  -lv* D:\PathToLog\agentinstall.log
```

Where `D:\PATHToLiveAgents` specifies the path of where the live agents are located (for example, the LiveAgents directory could be shared and the UNC path of that share can be specified). The **-lv*** logfile parameter is optional – `D:\PathToLog\agentinstall.log` is the full name of the log file where the MSI will output the detailed progress/error information, which could be useful to diagnose installation problems.

To install the agent in “Manual Deployment” mode, which installs only the software utilization plug-in, add the property `SETUPTYPE=Manual`. For example:

```
msiexec /i "HP DDM Inventory Agent (x86) 9.30.000.1300.msi" /qn /Lv*
c:\agentinstalllog.txt SETUPTYPE=Manual
```

If this option is not set, the agent is installed in Enterprise mode. Refer to Manual Deployment on page 85 for additional details on agent setup types.

Manual Deployment

The agent installation requires Microsoft Installer version 2.0 or above, which is part of the Windows operating system (earlier service packs of Windows 2000 may have an older version installed). When an older version is installed, the MSI installation must be upgraded to version 2.0 or above. This can be done using Windows Update or by downloading the Windows Installer 2.0 for Windows 2000 and Windows NT redistributable from the Microsoft web site.

The agent installation can be performed by running the install program located in the following directory on the DDM Inventory server by default:

C:\Documents and Settings\All Users\Application Data\Hewlett-Packard\DDMI\LiveAgents

The agent installer will prompt for setup type:

- **Enterprise Mode (recommended)**

  Selecting this mode will cause the scanners to be deployed by the DDMI server via the agent. This mode will install both the agent and the software utilization plug-in. Enterprise Mode is appropriate in most instances

- **Manual Deployment**

This mode installs only the software utilization plug-in and is useful if you will be using agentless scanning, but would still like to collect utilization data. Scanners must be deployed manually, using either a third-party software distribution tool or a login script, etc.

➤ The Software Utilization license module must be enabled in order to collect usage information. If this module is not enabled, utilization data is discarded when the scan file is processed. See Chapter 1 of the *Installation and Initial Setup Guide* for additional information.

Deploying a UNIX Agent

Because of high sensitivity of many UNIX environments, UNIX agents should be installed either via custom deployment or manually. The following is the recommended way of installing the UNIX agents:

- They should be installed into a directory which is only accessible by root.
- The content of the live agent media **.tar.Z** file should be extracted into the agent installation directory.
- The agent should be run as root.

The agent could be launched as part of the UNIX startup scripts as follows:

```
cd /agentdir

nohup ./bin/discagnt&
```

Where **agentdir** should be replaced with the actual agent installation directory.

- The agent data directory is stored under **$HOME/.discagnt**. Special care needs to be taken if **$HOME** refers to a common directory mounted via NFS to avoid agents from different computers sharing the same data directory. In such cases, the HOME environment variable needs to be redefined to point to a local directory prior to launching the agent.

To install the agent for UNIX in Manual Deployment mode (see Manual Deployment on page 85), you would use the following command:

```
cd /agentdir

nohup ./Plugins/usage/discusge -d $HOME/.discagnt&
```

Where **agentdir** should be replaced with the actual agent installation directory.

The following option can be passed to `discusge`:

`-d <usage-dir>` : To specify a directory for usage data

The utilization period is automatically set based on the PERIOD= value in the `discusge.ini` file. This value can be either 365, 90, or 31 If the number of days must be changed after the agent is deployed, modify the value in the discusge.ini file.

If the scanner has to later collect usage information it is recommended to run the scanner under the same account as the usage agent which is in most cases, root.

Also, to avoid ambiguities with the position of scanner data, it is recommended that you set explicitly the usage data path to $HOME/.discagnt/ using option -d. The `.discagnt` folder under the home directory may need to be created if it does not exist.

This will allow the scanner to take usage information from the same location it usually uses when run via the normal agent.

➤ During normal operation on UNIX, the agent (discagnt) will generate 2 log files:

- `discagnt.log`: General information about agent status, this file is located in `$HOME/.discagnt`.
- `nohup.out`: This file contains all outputs from agent and other programs executed by the agent. This file is located in `/opt/Discovery`.

These log files may be added to the system list of "rotated" log files (files that will split when they grow to a certain size). Normally, they will not grow to more than 1MB of data for a year of operation.

Deploying a Mac OS X Agent

The following is the recommended way of installing the Mac OS X agents:

- Copy the `HP DDM Inventory Agent 9.30.xxx.xxxx.dmg` file from the `DATA\LiveAgents` directory to a folder on your Mac OS X machine. For example, you can copy it to your Mac Desktop.

  ➤ The `DATA` directory refers to the `C:\Documents and settings\All Users\Application Data\Hewlett-Packard\DDMI` on the DDM Inventory server.

- Double-click the `.dmg` file to mount it. A drive icon named **HP DDM Inventory Agent** appears.
- Double-click the newly mounted icon. A window opens showing the Agent package, `DiscoveryAgent.pkg`.
- Double-click `DiscoveryAgent.pkg` to start the installation process.

  ➤ You may be asked for a system password to complete installation. This can occur if you do not have the appropriate privileges on the system you are accessing to perform the install.

  ➤ The `DiscoveryAgent.pkg` tree in the agent `.dmg` file can be used directly for installation. For example, you can copy it to a Mac Xserve share.

The installation process installs the agent in the `/Library/StartupItems/DiscoveryAgent` directory and starts the agent.

The following files are installed in the `/Library/StartupItems/DiscoveryAgent` directory:

— `acstrust.cert` - agent certificate

— `agentca.pem` - agent private key

— `bin/discagnt` - agent executable

— `postinstall`

— `postupgrade`

— `StartupParameters.plist`

— `Plugin/usage/discusge`

— `Plugin/usage/discusge.ini`

— `Plugin/usage/plugin.ini`

➤ Do not change the location or edit any of the agent files.

During normal operation, the agent (`discagnt`) generates the `/var/root/.discagnt/discagnt.log` log file.

The startup logs for the Mac OS X agent are located in `/var/log/discagnt.log`.

To start and stop the service from the terminal using the root account, run the following commands:

```
SystemStarter start “DDM Inventory Agent”

SystemStarter stop “DDM Inventory Agent”
```

To install the agent for Mac OS X in Manual Deployment mode use the following commands (note that Manual Deployment mode installs only the usage plugin--scanners must be managed separately. For additional information, see Manual Deployment on page 85):

1 As a root user in a terminal window, stop the DDMI agent using the command:

```
SystemStarter stop "DDM Inventory Agent"
```

2 Edit the service script () StartService function and replace the following lines:

```
cd $AGENTPATH

$AGENTPATH/bin/discagnt >> $AGENTLOG 2>&1 &
```

With:

```
cd $AGENTPATH

$AGENTPATH/Plugins/usage/discusge >> $AGENTLOG 2>&1 &
```

3 Restart the service with the following command:

```
SystemStarter start "DDM Inventory Agent"
```

The following option can be passed to `discusge`:

`-d <usage-dir>` : To specify a directory for usage data

The utilization period is automatically set based on the PERIOD= value in the `discusge.ini` file. This value can be either 365, 90, or 31 If the number of days must be changed after the agent is deployed, modify the value in the `discusge.ini` file.

If the scanner has to later collect usage information it is recommended to run the scanner under the same account as the usage agent which is in most cases, root.

Also, to avoid ambiguities with the position of scanner data, it is recommended that you set explicitly the usage data path to `$HOME/.discagnt/` using option `-d`. The `.discagnt` folder under the home directory may need to be created if it does not exist.

This will allow the scanner to take usage information from the same location it usually uses when run via the normal agent.

Upgrading the Agent

Upgrading a Windows Agent

When a Windows (x86) agent is upgraded the following occurs:

- a copy of the new MSI agent media file is uploaded to the remote computer
- the old agent is uninstalled
- the new agent is installed

Any problems with initiating the upgrade sequence can be seen from the log available in:

Device Manager > **Diagnosis** > **Scan Log**

Once the upgrade has been successfully started, it can still fail on the remote computer. If anything goes wrong during this uninstall/install process, the detailed error information is saved into the log file ovedagentinstaller.log located in the agent's program directory. This file can be used to diagnose problems with the upgrade.

Upgrading a UNIX Agent

When a UNIX agent is upgraded the following happens:

- The file `Agents\bin\agentupgrade.sh` located under the DDM Inventory program directory is getting uploaded to the remote computer to the agent's program directory together the appropriate agent's live media `.tar.Z` file.
- `agentupgrade.sh` is started on the remote computer, giving the name of the new `.tar.Z` media file.
- The agent upgrade script makes an assumption that a few standard UNIX commands are available in PATH: uname, which, uncompress/gzip, nohup, etc. The script should be reviewed and amended as necessary to accommodate the actual UNIX environment.

Upgrade Procedure

1. To upgrade the agent on a single device:
   a. Open the **Device Manager** for the required device (for example by using the **Find** command on the front page of the web UI)
   b. Click the **Update Model** icon at the top.
   c. Select **Upgrade Agent** from the drop-down box and click the **Update** button.
2. To upgrade the agent on all devices in a device group, configure the Agent configuration profile to include agent upgrade:
   a. Click **Administration > Discovery Configuration > Configuration Profiles**.
   b. Click the **Agent** tab.
   c. Click the name of the profile assigned to this device group.
   d. Make sure that **Allow Agent Communication** is selected.
   e. Select **Allow Agent Upgrade**, and specify the schedule that you want.
   f. Click **Save and Close**.

3 Activate the configuration changes.

If the agent upgrade attempt failed to start the agent installation, a detailed progress log is available in the following place:

Device Manager> Diagnosis> Scan Log

Uninstalling the Agent

As automatic deployment is only supported on Windows, automatic agent uninstall is only available on Windows too.

➤ UNIX scanners must be uninstalled manually or via a scripted uninstall applicable to the environment.

To uninstall an agent on a Windows system

1 To uninstall the agent on a single device:

- Open the **Device Manager** for the required device (for example by using the **Find** command on the front page of the web UI).
- Click on the **Diagnosis** panel, go to the **Discovery Configuration** section and check the value for the **Agent deployment** property. The value should be **None** or **Uninstall** in order to be able to execute the next step.
- Click the **Update Model** icon at the top.
- Select **Uninstall Agent** from the drop-down box and click the **Update** button.

2 To uninstall the agent on all devices in a device group, configure the Agent configuration profile assigned to this device group to include agent uninstall:

a Click **Administration > Discovery Configuration > Configuration Profiles**.

b Click the **Agent** tab.

c Click the name of the profile assigned to this device group.

d Make sure that **Allow Agent Communication** is selected.

e From the **Agent deployment** list, select **Uninstall**.

f Click **Save and Close**.

- Activate the configuration changes.

If the agent uninstall attempt failed to start the agent installation, a detailed progress log is available in the following place:

Device Manager> Diagnosis> Agent Log

Even when the agent uninstall was launched successfully on the remote computer, it can still fail because of external factors, such as files being locked on the computer, etc. To troubleshoot agent uninstall problems the log file **ovedagentinstaller.log** located in the agent's program directory can be used.

Uninstalling a Mac OS X Agent

Mac OS X agents must be uninstalled manually.

To uninstall a Mac OS X agent

To uninstall the agent on a single device by using the GUI:

1. Use the Finder to select the correct **System Disc**.
2. Navigate to **Library** > **StartupItems**.
3. Select the **DiscoveryAgent** folder and move it to the Trash.

   ➤ Users need local system rights (computer password) to be able to delete the **DiscoveryAgent** folder.

4. Reboot the system.

Software Utilization

DDM Inventory agents include a plug-in that allows collection of the software utilization data. If software utilization capability was purchased and enabled in the DDM Inventory license, it can be enabled both globally and on a per device group basis. The device group property applies to data collection, and the global one applies to the data processing.

- The global setting is available in **Administration > System Configuration > Scan processing > Process utilization data**.
- The device group setting is available in the Agent configuration profile under **Administration > Discovery Configuration > Configuration Profiles.** Select the **Collect utilization data** option.

  ➤ There is a predefined Agent profile called <Collect utilization data> which has the **Collect utilization data** property selected. Just apply this to your device group.

- The time period for which the software utilization is collected (31, 90 or 365 days) is configured in the **Administration > System Configuration > Agent communication > Utilization period** setting.

  In Enterprise Mode, the utilization period is automatically transferred to the managed device by the DDM Inventory agent.

  In Manual Mode (only the software utilization portion of the agent is installed), the agent media is generated automatically with the correct software utilization period embedded. Only the agent media files for the current version of the product are updated with the correct utilization period. Any other files in the `LiveAgents` directory (for example, from previous releases) are *not* updated.

Once utilization data is enabled in both places, the agent is instructed to collect utilization data. It launches its software utilization plug-in that constantly monitors the processes that are running on the computer and collects software utilization information. The plug-in stores its data in the `Perf` subdirectory of the agent data directory. There is a separate file for each day as well as the summarized version named **discusg.cxu** which contains the aggregated utilization information.

When the inventory of a computer is performed, the scanner collects a copy of the discusg.cxu file and stores its content in the scan file in a special stored file called Software Utilization Data. While processing the scan file, the XML Enricher, the Viewer and the Analysis Workbench make use of this special stored file to extract and process software utilization data.

You can import this data into AssetCenter to assist in tracking license compliance.

Agent Communication Configuration

When you installed DDM Inventory, you set up some Agent configuration profiles as part of your initial configuration (see the *Installation and Initial Setup Guide* for more details). If you choose to, you can change how the DDM Inventory server communicates with the Agents on your network computers.

To start configuring your Agent Communication settings:

1. Click **Administration > System Configuration > Agent communication**.
2. Change the settings as necessary.

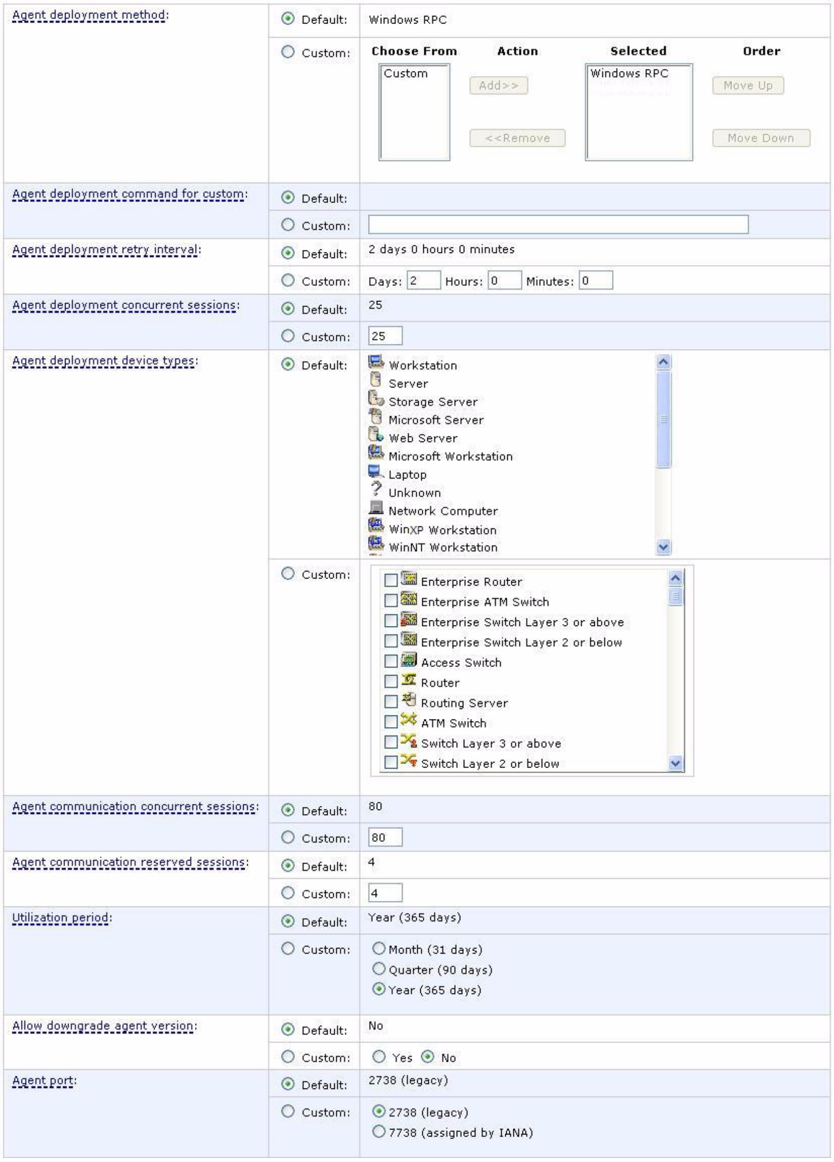
Table 15 Description of the Settings

Setting	**Description**
Agent Deployment Method	This option determines how you want to deploy Agents to your network devices.
Agent Deployment Command for Custom Deployment	Agent Deployment Command For Custom deployment allows you to specify the full filename of your own custom Agent deployment process.
Agent Deployment Retry Interval	Agent Deployment Retry Interval determines how often DDM Inventory will attempt to send the Agent to a network device.
Agent Deployment Concurrent Sessions	Agent Deployment Concurrent Sessions determines how many Agents DDM Inventory can deploy at any one time. This controls how fast you want Agent rollout to occur.
Agent Deployment Device Types	Agent Deployment Device Types determines the types of devices to which DDM Inventory will try to send Agents.
Agent Communication Concurrent Sessions	Agent Communication Concurrent Sessions determines how many Agents DDM Inventory Server can communicate with at any one time.
Agent Communication Reserved Sessions	Agent Communication Reserved Sessions determines how many Agent sessions will be reserved for manual operations, such as debugging or testing.
Utilization Period	This option determines how long DDM Inventory will keep utilization data.
Allow Downgrade Agent Version	This option allows you to downgrade your Agent version. You can downgrade your Agent version in situations where you have distributed new Agents that cannot work in your network.

Table 15 Description of the Settings

Setting	Description
Agent Port	This option determines which port DDM Inventory will use to communicate with the Agent. You can select 2738 or 7738 (the later of which is registered with IANA).
Agent Call Home	If you have enabled the Agent Call Home option, these options specify the DDM Inventory server names or IP addresses to be used by the Agent to call the DDM Inventory server.
Agent Versions	Also on this screen, you can manually change the version of the Agent you want to use for running different Operating Systems.

3 Click **Change**.



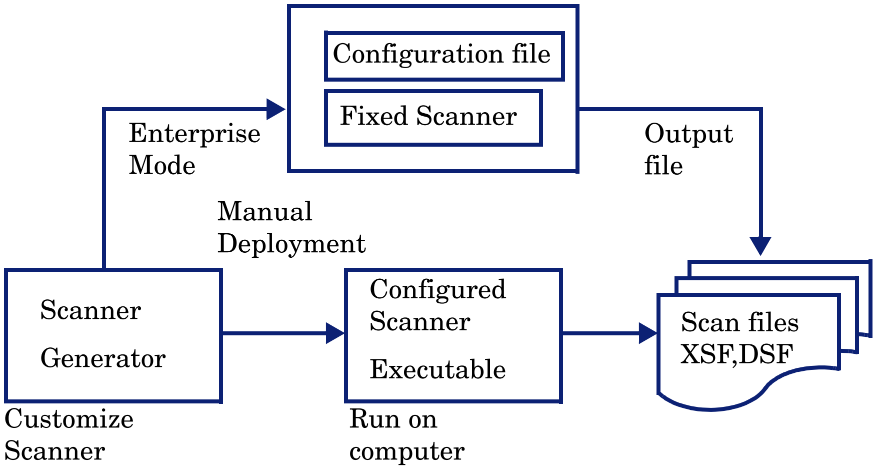
Agent deployment method:	● Default:	Windows RPC
	○ Custom:	**Choose From** **Action** **Selected** **Order** Custom Add>> Windows RPC Move Up <<Remove Move Down
Agent deployment command for custom:	● Default:	
	○ Custom:	
Agent deployment retry interval:	● Default:	2 days 0 hours 0 minutes
	○ Custom:	Days: 2 Hours: 0 Minutes: 0
Agent deployment concurrent sessions:	● Default:	25
	○ Custom:	25
Agent deployment device types:	● Default:	Workstation Server Storage Server Microsoft Server Web Server Microsoft Workstation Laptop Unknown Network Computer WinXP Workstation WinNT Workstation
	○ Custom:	□ Enterprise Router □ Enterprise ATM Switch □ Enterprise Switch Layer 3 or above □ Enterprise Switch Layer 2 or below □ Access Switch □ Router □ Routing Server □ ATM Switch □ Switch Layer 3 or above □ Switch Layer 2 or below
Agent communication concurrent sessions:	● Default:	80
	○ Custom:	80
Agent communication reserved sessions:	● Default:	4
	○ Custom:	4
Utilization period:	● Default:	Year (365 days)
	○ Custom:	○ Month (31 days) ○ Quarter (90 days) ● Year (365 days)
Allow downgrade agent version:	● Default:	No
	○ Custom:	○ Yes ● No
Agent port:	● Default:	2738 (legacy)
	○ Custom:	● 2738 (legacy) ○ 7738 (assigned by IANA)

12 Scanner Generator

After defining requirements, the next step in an IT asset inventory is to collect data. This is accomplished by using the DDM Inventory Scanner Generator to generate scanners and then by running the generated scanners.

The scanner is configured and generated in the Scanner Generator according to the specifications determined in the planning stage of the inventory. Then the scanner is run across the computer population to collect inventory data, either automatically using the scheduling mechanism (Enterprise Mode) or manually (Manual Deployment Mode).

The Scanner Generator is used to both configure and define the level of information to be collected. One or more scanner executable programs with the desired configuration are then generated and subsequently run across a computer population.



Scanners can collect four different types of information and can be configured to collect any or all of them. See Information Scanners Can Collect. The details recorded for each computer within each main category depend on the options and settings selected when the scanner is generated and the configuration of the computer.

The Scanner Generator also provides a set of options for controlling the behavior of the scanner as it scans each computer, under both normal and exceptional conditions (such as when an error occurs).

Scan File Formats

The information collected from each computer can be stored in two formats:

- Compressed XML (XSF) - with the file extension `.xsf`

- Delta Scan File (DSF) - with the extension `.dsf`

➤ In Desktop Inventory 7.x, the `.xsf` extension was known as `.xml.gz`. The file format is the same.

The information collected in these scan files can be viewed and analyzed.

XSF Scan File

The compressed XML scan file format (.xsf) allows the scan data to be augmented with application recognition information. The uncompressed XML data inside these scan files is compressed using gzip compression. The files can be uncompressed using gzip, WinZip, or any other program that supports gzip decompression.

Further information about the XSF format can be found in XML Enricher on page 179.

DSF Scan File

Instead of sending a full scan file to a server after every scan, the scanners can calculate the difference (the 'delta') between the last full scan and the current one and transfer just this in Delta Scan File format (DSF). This can dramatically reduce the network bandwidth used when using DDM Inventory. Delta Scan files cannot be viewed in the analysis tools (Analysis Workbench and Viewer).

Components of a Scanner

A scanner consists of two files:

- **The scanner executable file**

  This file is an executable file. It contains the constant parts of the scanner:

  - strings
  - data files
  - the scanner executable code

- **The scanner configuration file**

  The configuration file is a compressed XML file containing the settings for the scanner you are currently configuring.

  When the scanners are used in Enterprise Mode, they read the configuration from a separate configuration file. This is a binary file with a `.cxz` extension. The typical size of the configuration file is about 3K. As the size of the configuration file is significantly smaller than the size of the complete scanner, a separate scanner configuration is useful for repetitive inventory collection when the configuration of the scanner has been altered. In this case, only a small configuration file is delivered to the user's computer to run with the original scanner instead of delivering the entire new scanner.

Self-Contained Scanner Executable

When used in Manual Deployment Mode, the Scanner Generator generates self-contained scanner executables that consist of a combination of the scanner executable and configuration file.

Information Scanners Can Collect

The four types of information collected are:

- Hardware and Configuration Information on page 99
- Software Information on page 99
- User or Asset Information on page 100
- Software Utilization on page 100

Hardware and Configuration Information

Hardware information is detected automatically. The scanners collect and store from 100 to 1500 hardware items for a computer depending on the type and manageability options available on the computer.

The Scanner Generator allows a subset of the hardware collection to be disabled. Normally this is not required but may be desirable to decrease scan file size or scan time.

The hardware details that can be defined and recorded by the scanner include the following:

- The processor type and BIOS details.
- The memory size and configuration details.
- The computer bus type and details of the attached cards.
- The hard disk drive specifications (including the total size and free space).
- The network type and ID (if applicable). This hardware item cannot be disabled in Enterprise Mode.
- Comprehensive detection of network settings, including detection of multiple network adapters, TCP/IP settings, gateways, DNS servers, subnet masks, DHCP status.
- The monitor and video display adapter details.
- The type of keyboard and mouse driver installed and details of the I/O ports.
- The version and other details of the Operating System the computer is running under.
- The expansion (or adapter) cards detected.
- The hardware data information from System Management BIOS (SMBIOS).

Further Information

For a comprehensive list of hardware data the scanners can collect, see **Help** > **Data Collected by the Scanners**.

Software Information

Software information is scanned automatically, and consists of detailed information about the files and directories on the drives scanned. The information collected about files can be defined (including the file types and the level of information collected). It is possible to define the drives that are to be scanned based on either the media or format of the drive, or to use the targeted scanning option to scan just a set of directories. Specific files can be collected (that is, stored in the scan file) for further analysis or for error recovery purposes. It is also possible to configure the level of file detail stored in the scan file and filters can be set up that specify directories or files to be included or excluded from being stored.

User or Asset Information

User or asset information consists of configurable fields that can be collected automatically. It usually includes the asset number which is used to uniquely identify each computer. On subsequent inventories, the asset information entered during the initial inventory can optionally be re-used. Asset data fields are automatically populated from the data extracted from text files, the Windows registry and environment variables.

Software Utilization

If you have a Utilization license, DDM Inventory can gather information about the software that is being used on the machines in your network. This is referred to as Software Utilization and the information collected can be used to optimize software license cost, for example by eliminating unused or under-utilized software installations.

From a software recognition perspective, any files that are Unknown and are shown to have a high Utilization should be marked for teaching.

Software utilization data shows the number of days that an application was used (as a percentage) over a period of time. This period of time is known as the 'Utilization Period'

As a guideline the Utilization Periods are as follows:

- Month (31 days)
- Quarter (90 days)
- Year (365 days)

Starting Scanner Generator

To start the Scanner Generator

Log into the DDM Inventory Web UI and select **Server > Scanner Generator**.

The Scanner Generator opens.

Exiting Scanner Generator

To exit the Scanner Generator

- Either click **Cancel**
- Or click the close icon in the top right of the window.

  A message appears, informing you that you are now exiting the Scanner Generator.

Scanner Generator User Interface

Navigation between Pages

You can navigate between the different pages of the Scanner Generator using the following buttons:

Table 16 Buttons in the Scanner Generator pages

Button	Function
Next	Move to the following page after the settings on the page reflect your requirements.
Back	Return to a previous page to edit your previous settings.
Generate	Execute the final action of the Scanner Generator. For Manual Deployment Mode, self-contained scanner executables are generated. For Enterprise Mode, a scanner configuration file is sent to the DDM Inventory server.
Finish	The Generate button changes to a Finish button after the scanners have been successfully generated. Click this button to exit from the Scanner Generator when you have finished.
Cancel	Cancel the execution of the Scanner Generator completely.
Help	Obtain help for the tab pages you are currently on.

Scanner Generator Pages

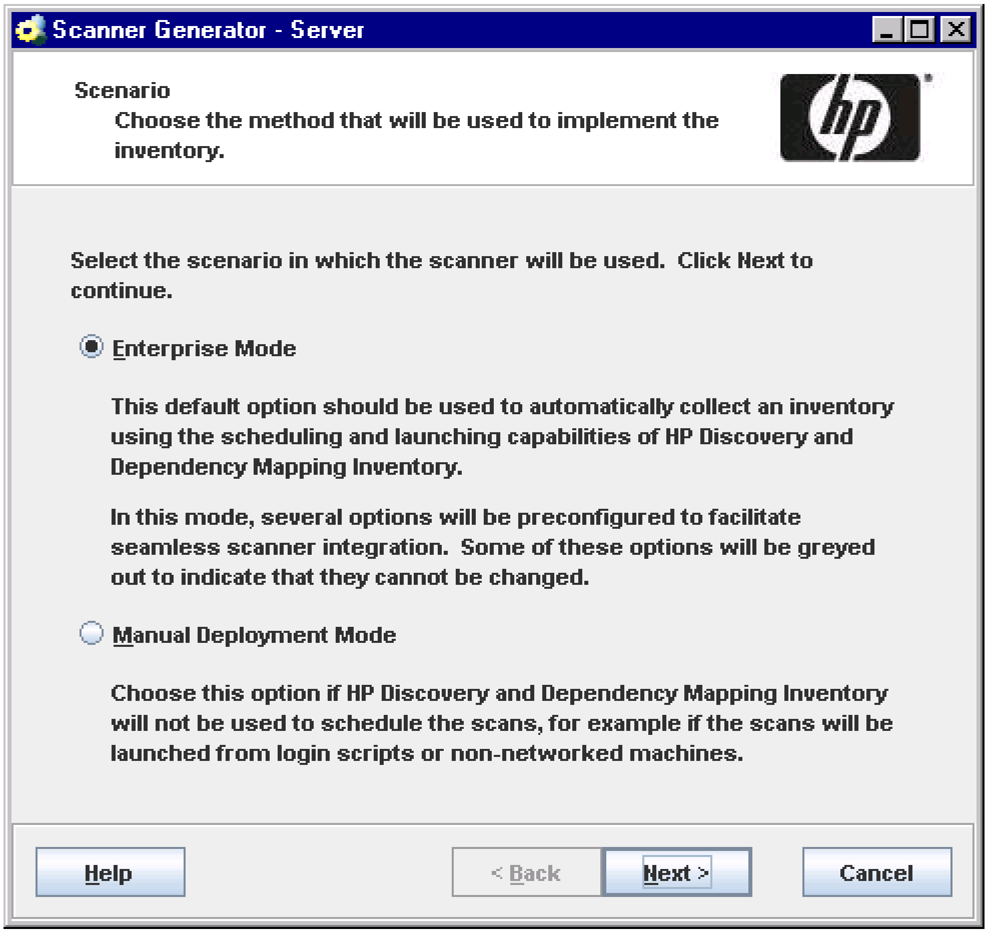
The Scanner Generator is composed of a succession of pages. Each of these pages displays information or requires user input, such as selection of options or entry of data items.

There are two scenarios in which the scanners can be used. This is determined on the first page of the Scanner Generator. Depending on which of these scenarios you select, different tab pages are displayed.

- Enterprise Mode
- Manual Deployment Mode

Scenario Page

On starting the Scanner Generator, the **Scenario** page appears. You will need to determine if you want to carry out an automatic inventory using the DDM Inventory agents or manually deploy the scanners.



Scenario

Choose the method that will be used to implement the inventory.

Select the scenario in which the scanner will be used. Click Next to continue.

● Enterprise Mode

This default option should be used to automatically collect an inventory using the scheduling and launching capabilities of HP Discovery and Dependency Mapping Inventory.

In this mode, several options will be preconfigured to facilitate seamless scanner integration. Some of these options will be greyed out to indicate that they cannot be changed.

○ Manual Deployment Mode

Choose this option if HP Discovery and Dependency Mapping Inventory will not be used to schedule the scans, for example if the scans will be launched from login scripts or non-networked machines.

To select the method used to implement the inventory select one of the following options:

- **Enterprise Mode**

  This is the default option. Use this option to automatically collect an inventory using scheduling and launching on the DDM Inventory Server.

  In this mode, several options in the Scanner Generator have been preconfigured to facilitate the integration between the scanners and the DDM Inventory Server. Some of these options will be greyed out to indicate they cannot be changed.

- **Manual Deployment Mode**

  Use this option if the DDM Inventory Server will not be used to schedule and launch scans. For example, choose this option if the scans will be launched from login scripts or on non-networked machines.

  In this mode, you must configure the scanners to save the off-site scan files into the `<DataDir>\Scans\Incoming` directory of the XML Enricher for the data to be processed by the DDM Inventory server. You can save the off-site scan files into the Incoming directory directly, or you can copy the scan files from where they are saved into the

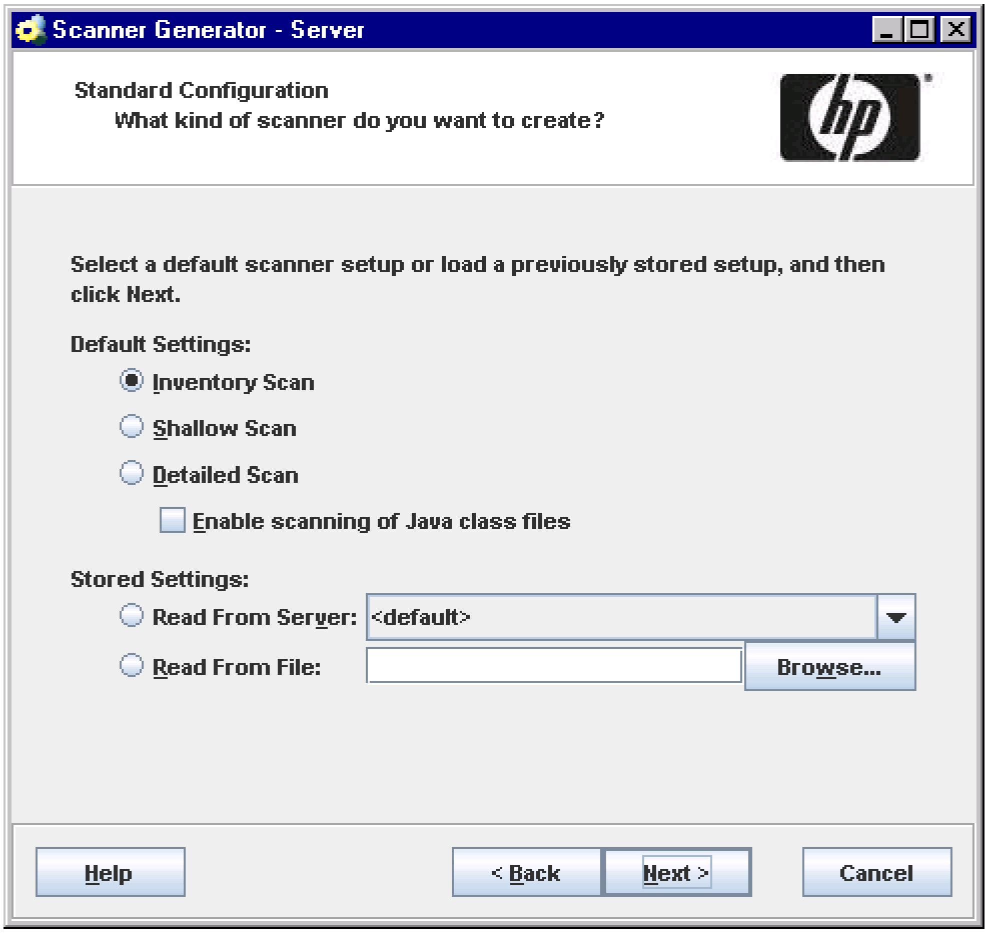
Incoming directory. To save the off-site scan file into the Incoming directory, you can either share the `<DataDir>\Scans\Incoming` directory through file sharing, or save the off-site scan files through FTP, or HTTP.

For how to save the off-site scan files into the Incoming diretory in the Scanner Generator, see Saving Results to Network (Offsite) on page 159, or refer to the Scanners section in the *Reference Guide*.

Standard Configuration Page

This page is used to select a preset configuration for the scanners. It is a starting point only and the settings can be amended as required.

Use this page to select a default scanner setup or to select a previously stored setup.



Standard Configuration

What kind of scanner do you want to create?

Select a default scanner setup or load a previously stored setup, and then click Next.

Default Settings:

● Inventory Scan

○ Shallow Scan

○ Detailed Scan

□ Enable scanning of Java class files

Stored Settings:

○ Read From Server: <default>

○ Read From File:

To select the type of scanner to create

1 You can do one of the following:

Under **Default Settings**, select a default scanner setup.

- **Inventory Scan**

Uses default configuration setting for the scanner. Defines a set of options suitable for a general inventory. Enough software information is collected to allow comprehensive inventory analysis. All hardware information is collected and a standard series of asset data fields are defined

- **Shallow Scan**

Defines a set of options to allow very quick scans. Because hardware scanning is very fast, most hardware items (as some are disabled by default) are collected, but limited software scanning takes place and the data collected is not sufficient to perform reliable software license recognition.

- **Detailed Scan**

If scanning time is not a critical factor, the Detailed Scan option can be used to collect the maximum amount of information. This, however, extends the scanning time significantly. Use this option in special cases only.

If you select **Inventory Scan** or **Detailed Scan**, you can choose to **Enable scanning of Java class files**. This setting deals with Java scanning. Enabling this setting does the following:

- Java `.class` files will be stored in the scan file
- Java specific environment variables for targeted scanning will be enabled.
- Windows scanner will add the location of the Java Home directory to the list of directories for a targeted scan.

Or alternatively, under **Stored Settings**, select a previously stored setup.

- **Read From Server**

Reads the settings from a previous Enterprise Mode configuration stored on the server. The drop down combo box shows the list of previously configured scanner configurations. The names displayed with angle brackets around them (for example, <default>) are predefined configurations. It is possible to read predefined configuration settings, but it is not possible to overwrite them when generating the new configuration. If you have chosen a predefined configuration, you will have to rename it when you come to the last page of the Scanner Generator in order to save it to the server. If you save this configuration, it will be available from the server with the other previous configurations.

Refer to the "Scanner Profiles"section under the "System Defined Configuration Profiles" section in the "Configuring the Discovery Process" chapter in the *Installation and Initial Setup Guide* to see how you can create and edit existing scanner configurations on the DDM Inventory Server.

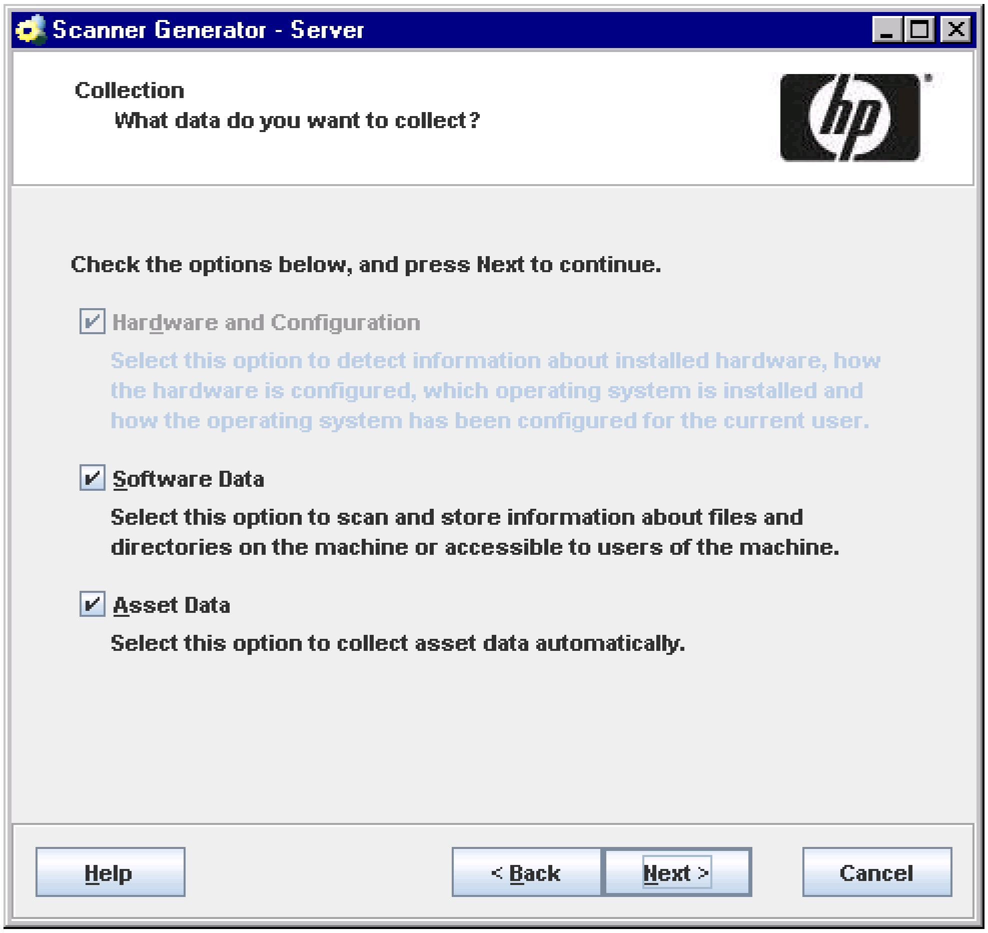
- **Read From File**

Replaces various configuration settings by reading information from files on the local machine. It can read parameters from previously generated scanners, scanner configuration files (`.cxz`), and scan files (`.xsf`). When the file name is provided, the scanner generator determines the type of the file based on the file extension, which eliminates the need to have a separate entry for each.

2 Click **Next** to continue to the **Collection** page.

Collection Page

The **Collection** page is used to select the type of computer data to collect.



Collection

What data do you want to collect?

Check the options below, and press Next to continue.

☑ Hardware and Configuration

Select this option to detect information about installed hardware, how the hardware is configured, which operating system is installed and how the operating system has been configured for the current user.

☑ Software Data

Select this option to scan and store information about files and directories on the machine or accessible to users of the machine.

☑ Asset Data

Select this option to collect asset data automatically.

When carrying out initial scanner deployments you might want to use hardware and asset data collection to establish basic information for the target machine. This can be followed up later by a more comprehensive scan that includes software data.

Selecting Type of Data to Be Collected

The selections you make on this page determine which of the data detail pages will be displayed.

To select the type of data to be collected:

1 Select from the following options as required:

- **Hardware**

  Includes details of the processor, memory configuration, computer bus, attached cards, hard disks, attached drives, monitor, video adapter, keyboard, mouse, OS version, network protocols and addresses.

See Hardware Data Page on page 107.

➤ For Enterprise Mode, this option is always selected and cannot be disabled.

- **Software Data**

  Consists of detailed information about files and directories on all scanned drives. The information collected about files can be defined (including the file types inventoried and the level of information collected). It is possible to define which drives are to be scanned, based on either the media or format of the drive, as well as determine which files are included in the scan file and which are ignored.

  See Software Data Page on page 114.

- **Asset Data**

  Asset data consists of asset fields that can be collected automatically.

  See Asset Data Page on page 137

2 Click **Next** to view specific data settings for each of the options.

Hardware Data Page

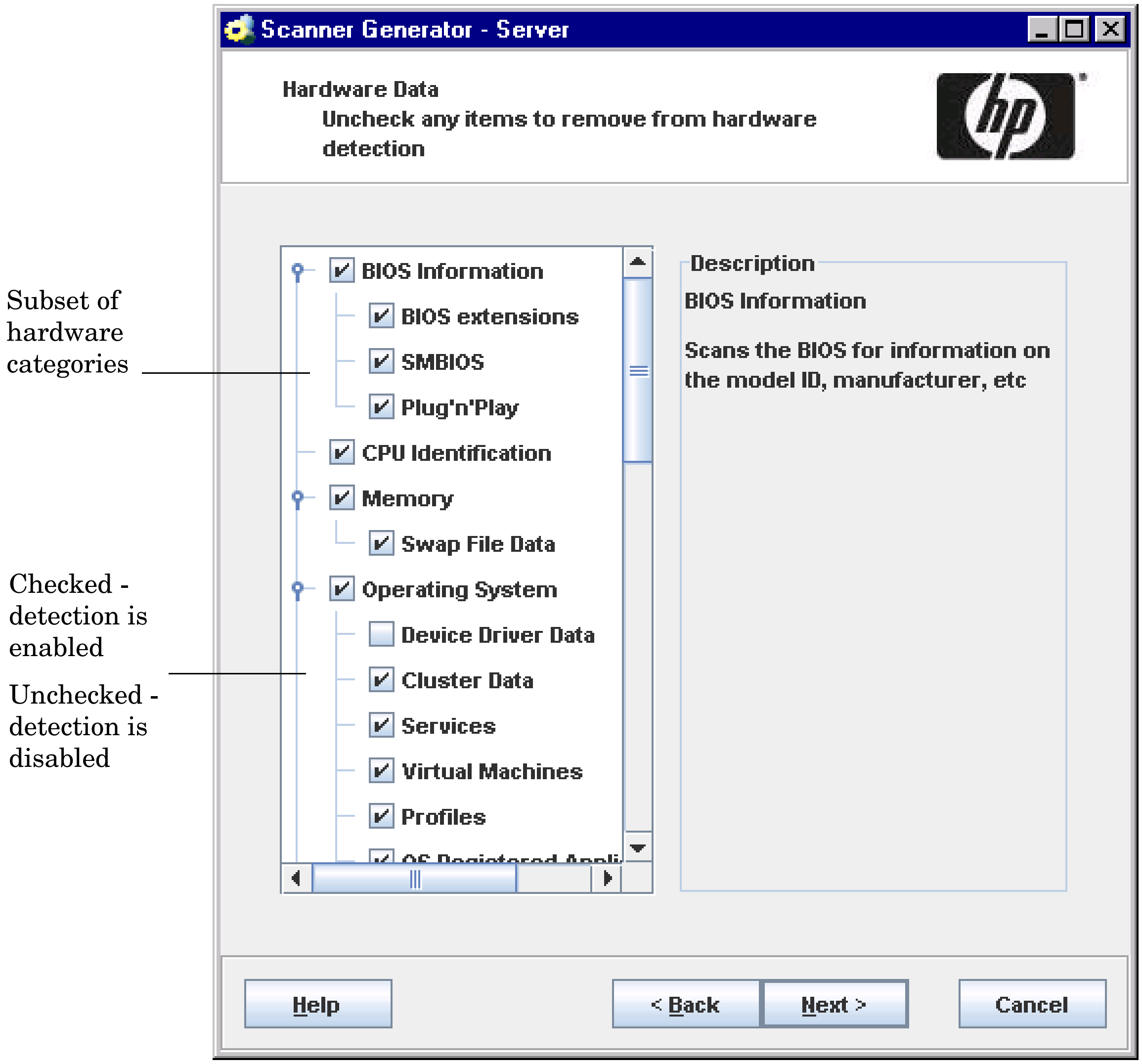
The **Hardware Data** page displays a subset of the hardware categories the scanner can collect. It is used to disable specific hardware detection routines.

Normally all hardware options are selected. Routines only need to be removed if there is a known problem scanning these hardware items. The hardware options have equivalent command line options that can be used at run-time.

Further Information

- You can find more information about scanner command line options in the section entitled “Command Line Options and Switches” in the *Scanners* chapter of the *Reference Guide*.

- For a comprehensive list of hardware data the scanners can collect, see **Help** > **Data Collected by the Scanners**.


Scanner Generator - Server
Subset of hardware categories
Checked - detection is enabled
Unchecked - detection is disabled
Help
< Back
Next >
Cancel

Hardware Data
Uncheck any items to remove from hardware detection

- ☑ BIOS Information
  - ☑ BIOS extensions
  - ☑ SMBIOS
  - ☑ Plug'n'Play
- ☑ CPU Identification
- ☑ Memory
  - ☑ Swap File Data
- ☑ Operating System
  - ☐ Device Driver Data
  - ☑ Cluster Data
  - ☑ Services
  - ☑ Virtual Machines
  - ☑ Profiles
  - ☑ OS Registered Appli

Description
BIOS Information

Scans the BIOS for information on the model ID, manufacturer, etc

The left side of the **Hardware Data** page shows a subset of the hardware categories detected by the scanner. The right side of this page is a Support panel which shows a description of each hardware item (displayed as the mouse pointer passes over each item in the list box). By default, most categories are selected. This indicates that the hardware detection routine for that particular category is enabled.

➤ The only hardware options which are unchecked by default are **Device Driver Data** and **WMI Software Features**. This is the default because both detections take a long time to perform. You can enable the detection of these hardware categories by selecting them to take advantage of the automatic device driver detection and collection of software features from WMI.

Disabling Specific Hardware Detection Routines

You can disable the hardware detection routines for specific categories. All other hardware detection will take place as usual.

To disable specific hardware detection routines:

1 Clear the check box next to that particular category to remove it from hardware detection.

2 Click **Next** to continue.

Hardware Categories

Table 17 Hardware categories

Options	Description
BIOS information	Collects information about the computer BIOS, including the computers asset tag, the BIOS date, ID, manufacturer and revision (where applicable).
BIOS extensions	Detects installed BIOS extensions, such as video or SCSI BIOS.
SMBIOS	Collects hardware data from System Management BIOS.
Plug'n'Play	Provides details of whether the BIOS installed on the computer is Plug and Play compatible. If the BIOS supports Plug and Play specification, the version of the specification is collected.
CPU Identification	Identifies the CPU (model), establishes if it has got FPU (numeric coprocessor), MMX (MultiMedia eXtensions) and ISSE/SSIMD capability and reports the speed of the CPU, cache characteristics. For newer Intel and compatible processors, the manufacturer, model, family and stepping ID are reported.
Memory	Detects the total amount of memory installed on the computer, including the amount of conventional and extended memory.
Swap File data	Collects data about swap files used for virtual memory.
Operating System	Collects information about the operating system and its configuration.
Device Driver Data	When this option is enabled, the Windows scanner enumerates all devices to determine which files are used as device drivers. Each file in this list is given the 'Device Driver' attribute when stored in the scan file. The device driver option is now disabled by default to increase speed of the hardware scanning.
Cluster Data	Collects information about Windows Server Cluster membership. It detects that the machine is part of a cluster, the name and description of the cluster and the list of nodes connected to the cluster.
Services	Collects information about installed operating system services.

Table 17 Hardware categories

Options	Description
Virtual Machines	Detects whether the scanner is running in VMware, Virtual PC, Terminal Services, Hyper-V, LPAR, vPar, or nPartition. From an asset management point of view, it is important to be able to determine which scanned machines are virtual (for example, so you don't pay too much maintenance for too many machines).
Profiles	Collects data about user profiles.
OS Registered Applications	Collects data about installed applications that are registered with the operating system. On Windows (pre-Vista), it collects data as displayed by the Add/Remove programs item in the Control Panel. On Windows Vista, it collects data as displayed by the Programs and Features item in the Control Panel. On UNIX, it collects data from the system's software package manager.
Packaged File Data	Collects information about the relationship between the installed applications (packages) and the files that belong to them. When this option is set, it causes the scanner to interrogate the native operating system package manager to retrieve the relationship information. This ensures that the installed package rule-based recognition can correctly recognize the files as belonging to the installed package/ application.
WMI Software Features	Collects the information about installed applications from WMI as stored in the `Win32_SoftwareFeature` class. The `Win32_SoftwareFeature` WMI class is not available on the Windows 2003 Server by default. The WMI provider that supports this class is an optional component on Windows 2003 Server, and it is not installed by default. To enable this WMI provider, you must go to **Control Panel** > **Add Remote Programs** > **Add/Remove Windows Components** > **Management and Monitoring Tools** > **WMI Windows Installer Provider** and install the WMI Windows Installer Provider component. Once this component is installed, the data collected by WMI Software Features hardware detection becomes available.
Containers	Collects data about containers available in the operating system. Currently, this is only supported by the Solaris scanner, which can collect information about Solaris zones.

Table 17 Hardware categories

Options	Description
Software Identification Tags	Collects the information in software identification tag files, which are XML files that consist of identification and management information about a software product. These tag files uniquely identify the software product, providing data for software inventory and asset management. During the hardware detection phase, the Scanner collects the information from software tag files from the common system location, as well as from the top level directory of the application in the event that both the **OS Registered Applications** and **Packaged File Data** checkboxes are selected and the application is packaged in the standard package format. If you do not select the **Software Identification Tags** checkbox, the Scanner will not collect any information from tag files during the hardware detection phase. For detailed information, refer to the "Software Identification Tags" chapter in the *Scan Data Analysis Guide*.
Video	Records details of the Video Display Adapter, which include the adapter type (EGA, XGA, VGA and so on) and model/ manufacturer, where possible. In Windows the current desktop resolution and number of colors are also picked up.
DDC Data	When connected to a VESA DDC compliant monitor, collects full monitor information.
I/O Ports	Detects and reports on the number of serial and parallel ports, the I/O address for each, and for serial ports, the UARTs attached.
SCSI/ASPI Detection	Checks for the presence of an ASPI (Advanced SCSI Programming Interface) driver for a SCSI adapter. If the driver is available, the host SCSI adapter name is reported.
SCSI/IDE/ATAPI devices	Detects installed devices, such as hard drives, CD-ROMs, tape drives and other such devices. Also detects Serial ATA disks.
SCSI/IDE/ATAPI serial numbers	Detects serial numbers of the installed devices (where available). Also detects the serial number of Serial ATA disks.
Network Information	Detects the network configuration, including Logon Name, Workgroup Name, Machine ID, and Domain Name. Detects information such as multiple network adapters, gateways, DNS servers, subnet masks, DHCP status. Information about installed network protocols (TCP/IP, NetBIOS/NetBEUI, IPX/SPX) and network addresses is also provided. Note: In Enterprise Mode, it is possible to disable subsets of network information. However, you should not disable ALL network information.

Table 17 Hardware categories

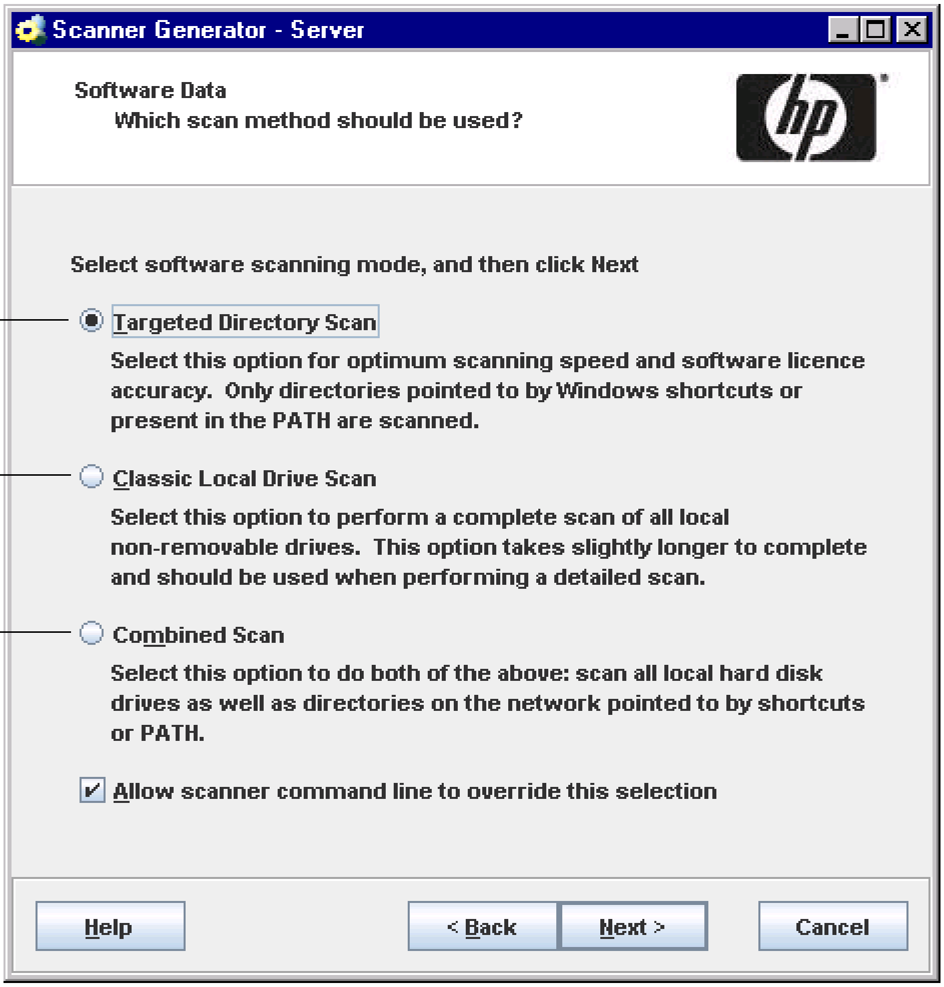
Options	Description
TCP/IP	Collects information about an installed TCP/IP protocol. This information includes domain, DNS Servers, Node type, NetBIOS Scope ID, WINS proxy status, NetBIOS resolution status. Network adapter information (including description, IP address, IP routing status, subnet mask, default gateways, DHCP status, DNS suffix, autoconfiguration status) is also provided.
IPX/SPX	Collects information about the IPX/SPX protocol.
NetBIOS/NetBeui	Collects information about the NetBIOS or NetBEUI protocol.
Shared Devices	Collects information about shared devices, such as disks and printers.
Keyboard & Mouse	Reports on the type of keyboard attached (extended or normal); whether a mouse is connected and mouse driver is loaded; the mouse brand and version of the driver, number of buttons and type of connection (serial, PS/2, bus).
Disk Drives	Collects advanced information about all attached disk drives. This information includes the type of the drive (floppy disk, hard disk, CD-ROM, network), the type of the file system (FAT, NTFS, HPFS), amount of total and free space, location of the hard drive partitions on the physical hard disk and so on.
Local USB Hard Drives	Controls the way USB hard drives are treated. If checked (default setting), the USB hard drives are treated as local hard drives, and their size is counted towards the total and free space on the local hard drives, which is recorded in the `hwDiskTotalFreeMB` and `hwDiskTotalSizeMB` hardware fields. If the option is unchecked, the USB hard drives are treated as removable drives, and their size will not be counted towards the total size. Also, by default, the USB hard drives will not be scanned during a "classic" local hard drive scan. However, you can enable scanning by checking the **Software Details** > **Drives** > **Removable Drives** > **Other removable drives** check box. This option is currently only applicable to the Windows scanner.
Bus Detection	Detects the architecture of the bus used in the PC – ISA, EISA, PCI, MCA, or PCMCIA.
EISA	Detects and reports details of EISA cards.
MCA	Detects and reports details of MCA cards.
PCI	Detects and reports details of PCI cards.
PCMCIA	Detects and reports details of PCMCIA cards.
ISA PnP Cards	Detects and reports details of ISA Plug and Play cards.

Table 17 **Hardware categories**

Options	Description
USB Data	Detects and reports details of the USB host adapters, hubs and devices attached to them.
If the bus types checked for by the scanner are not available, the tests for checking the cards will not be performed.	
Peripherals	Checks for installed peripherals, such as printers, modems and sound cards.
UNIX system configuration	Collects UNIX, Linux, and Mac OS X configuration information.

Software Data Page

The **Software Data** page is used to select the software scanning method. The choice of scan method determines how extensive the software scan will be.



Software Data

Which scan method should be used?

Select software scanning mode, and then click Next

● Targeted Directory Scan

Select this option for optimum scanning speed and software licence accuracy. Only directories pointed to by Windows shortcuts or present in the PATH are scanned.

○ Classic Local Drive Scan

Select this option to perform a complete scan of all local non-removable drives. This option takes slightly longer to complete and should be used when performing a detailed scan.

○ Combined Scan

Select this option to do both of the above: scan all local hard disk drives as well as directories on the network pointed to by shortcuts or PATH.

☑ Allow scanner command line to override this selection

Displays the Directories, File Scanning, and Stored Files tabs

Displays the Drives. File Scanning, and Stored Files tabs

Displays all of the above tabs

Selecting a Preset Software Scanning Mode

Three preset modes are available in this page of the Scanner Generator. Depending on which of these modes you select, different sets of tab pages will be displayed when you click **Next**.

Each of the tab pages are described in the next section, even though you might not see all of them depending on the choice you make on this tab page.

Table 18 Preset software scanning modes

Scanning Mode	Tab Pages Displayed
Targeted Directory Scan	Directories File Scanning Stored Files
Classic Local Drive Scan	Drives File Scanning Stored Files
Combined Scan	Drives Directories File Scanning Stored Files

Under most circumstances, the default settings (which are determined by the presets chosen on the Standard Configuration page) are satisfactory for defining the software information collected, but the Scanner Generator allows the default options to be modified to create custom settings.

To select a preset software scanning mode, select one of the following:

- **Targeted Directory Scan**

  Select this option for optimum scanning speed and software license accuracy. Only selected locations are scanned, which are identified by the scanner from various sources, such as Windows shortcuts, Services, file associations, environment variables, and so on. The tab pages shown when you click **Next** are:

  - Directories
  - File Scanning
  - Stored Files

- **Classic Local Drive Scan**

  Select this option to perform a complete scan of all local non-removable drives. This option takes longer to complete and is used when performing a detailed scan. The tab pages shown when you click **Next** are:

  - Drives
  - File Scanning
  - Stored Files

- **Combined Scan**

  Select this option to do both of the previous options: scan all local hard drives as well as directories on the network pointed to by shortcuts, file associations and environment variables, such as PATH. The tab pages shown when you click **Next** are:

  - Drives
  - Directories

- File Scanning
- Stored Files

Enabling the Command Line Override Option

The **Allow Command Line Override** option is available for overriding the drive selection configured in the Scanner Generator.

If you select this check box, the default drive selection specified can be overridden by specifying a list of drive letters or directories to scan on the command line using the `-paths` command line option.

An example of a command line override is:

```
Scanwin32-x86 -paths:C:\Windows -paths:D:
```

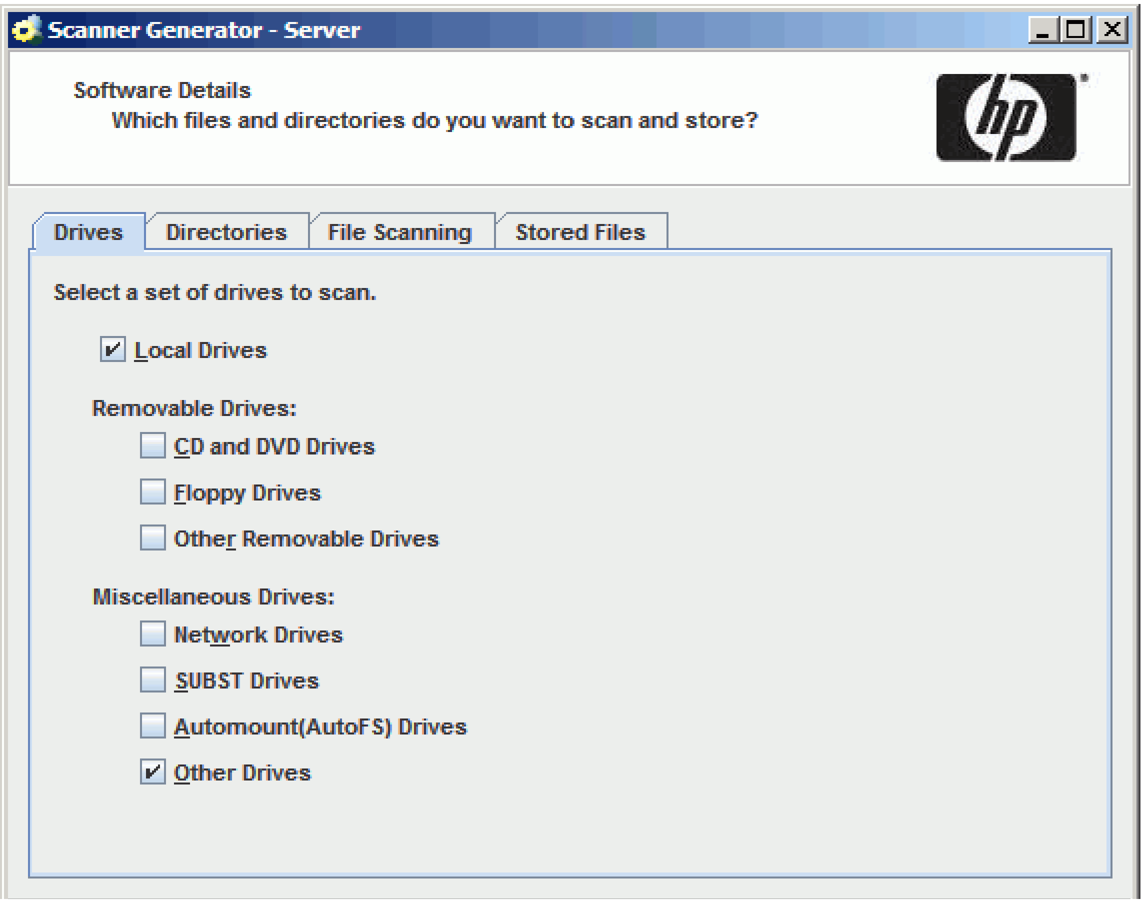
If you clear this check box, you cannot change the scan selection by specifying drive letters and/or paths on the command line.

Further Information

You can find more information about scanner command line options in the section entitled “Command Line Options and Switches” in the *Scanners* chapter of the *Reference Guide*.

Drives Tab

The **Drives** tab page is used to define which of the drives are to be scanned when using either **Classic Local Drive Scan** or **Combined Scan**.



Software Details

Which files and directories do you want to scan and store?

Select a set of drives to scan.

☑ Local Drives

Removable Drives:

☐ CD and DVD Drives

☐ Floppy Drives

☐ Other Removable Drives

Miscellaneous Drives:

☐ Network Drives

☐ SUBST Drives

☐ Automount(AutoFS) Drives

☑ Other Drives

Selecting Type of Drive to Scan

Options are provided for scanning all drives or just a particular type of drive.

To select the type of drive to scan, check the appropriate check boxes as required:

- **Local Drives**

  These are hard disk drives visible and mounted by the current operating system. In Windows, normal hard disk drives are assigned drive letters by the operating system and are usually included in the scanning process.

- **Removable Drives**

  Removable drives are drives with non fixed media that can be removed or exchanged. Removable drives are normally not included for scanning.

Table 19 Removable drives

Drive Selection	Description
CD and DVD Drives	Scans the contents of CD and DVD drives. See Automount (AutoFS) Drives for detailed information about scanning automatically mounted drives.
Floppy Drives	Scans the contents of floppy drives. See Automount (AutoFS) Drives for detailed information about scanning automatically mounted drives.
Other Removable Drives	Scans other removable drives (for example, SyQuest drives). Scanning removable media is not usually recommended, as the content of these drives vary depending on the media currently in the drive.

- **Miscellaneous Drives**

  These drives are any drives that do not fall into any of the previous categories, and may or may not have local physical media associated with them.

Table 20 Miscellaneous drives

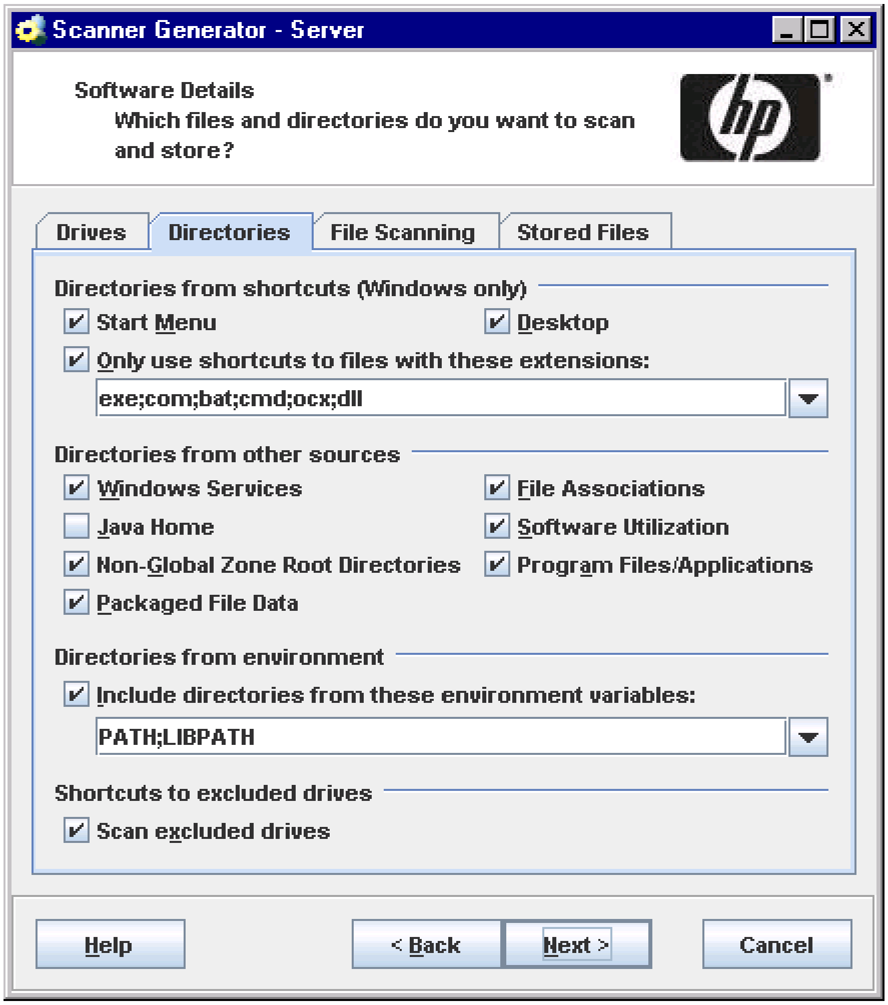
Drive Selection	Description
Network Drives	Scans the contents of network drives. Note that network drives can be scanned by multiple computers. Use this option with caution. See Automount (AutoFS) Drives for detailed information about scanning automatically mounted drives.
SUBST Drives	Scans 'virtual' drives created using the operating system substitute command - SUBST. This is not normally desirable as a substituted drive can be scanned using both its true drive letter and substituted letter. Use this option with caution.
Automount (AutoFS) Drives	When unchecked (the default setting), the scanner will not scan any auto-mounted drives. The scanner will not attempt to mount any indirect automount drives. It may mount a direct automount drive if it comes across its mount point during the software scanning process, but the direct automount drive itself will not be scanned. When checked, the automount drives are scanned only if all of the following conditions are met: • The directory where the drive's mount point is located is itself getting scanned. For example, it is located on a drive for which the corresponding drive-type checkbox is checked. • The drive-type checkbox for the real drive type of the automount drive is also checked. For example, an auto-mounted NFS drive will only be scanned when the **Network Drives** checkbox is also checked. • The drive is a direct automount drive or if the drive is an indirect automount drive, it has to be either already mounted or during the scanning process the scanner has to encounter a symbolic link pointing to a location within the indirect automount drive's directory structure. The following example shows how these three conditions are met: A direct automount DVD drive mounted under `/usr/local/cd` (where `/usr/local` is located on a local hard drive) is scanned only when both **Local Drives** and **CD and DVD Drives** checkboxes are checked.
Other Drives	Scans drives created using other devices drives (for example, RAM drives). Note that scanning drives created using device drivers can lead to false reporting of files on a computer. Use this option with caution.

Directories Tab

The **Directories** tab is used to specify which directories you want to scan when using **Targeted Scan** or **Combined Scan**.

The settings allow you to specify the directories you want to add to the list of directories to scan. For Windows Operating Systems, you also have the ability to scan desktop and Start menu shortcuts.

By scanning only selected directories rather than complete drives, software scanning is made faster.



Software Details
Which files and directories do you want to scan and store?

Directories from shortcuts (Windows only)

☑ Start Menu ☑ Desktop

☑ Only use shortcuts to files with these extensions:

exe;com;bat;cmd;ocx;dll

Directories from other sources

☑ Windows Services ☑ File Associations

□ Java Home ☑ Software Utilization

☑ Non-Global Zone Root Directories ☑ Program Files/Applications

☑ Packaged File Data

Directories from environment

☑ Include directories from these environment variables:

PATH;LIBPATH

Shortcuts to excluded drives

☑ Scan excluded drives

Selecting Directories to Scan

To select the directories to scan, select the options as required:

- **Directories from Windows shortcuts (Windows only) group**
  - **Start menu**

    This option will scan the directories that are pointed to by shortcuts on the Start menu.
  - **Desktop**

    This option will scan the directories that are pointed to by shortcuts on the desktop.

    - **Only use shortcuts to files with these extensions**

      When checked, only shortcuts that point to files with one of the extensions specified will be scanned.

- **Directories from other sources group**

  - **Windows services**

    Check this box to include directories containing Windows Services for targeted scanning. As the name implies, this option applies to Windows scanners only.

  - **File associations**

    Check this box if you want the scanners to add directories containing applications that are associated with various file types (for example NotePad for `.txt` files) to the list of directories for a targeted scan. This option applies to Windows scanners only.

  - **Java Home**

    Check this box if you want the scanners to add the Java Home directory to the list of directories for a targeted scan. This option applies to Windows scanners only.

If you checked the Enable scanning of Java class files on the Standard Configuration page, this option is selected by default.

  - **Software utilization**

    This setting instructs the scanner to include any directories from where used programs are executed. These directories will be included in the list of directories for a targeted scan. This ensures that the scanner collects the file data required for recognition of used applications. This option applies to all scanners.

  - **Non-global zone root directories**

    Check this box if you want the scanners to add the Solaris non-global (local) zone root directories to the list of directories for a targeted scan. This ensures that all directories used by non-global zones are scanned during the software scanning process. This option applies to Solaris scanners only.

  - **Program Files/Applications**

    Check this box if you want the scanners to add the standard location for program files to the list of directories for a targeted scan. On Windows, it is the `Program Files` directory, which is normally located in the root of the Windows system drive (such as `C:\Program Files`). On Mac OS X, it is the `/Applications` directory where the applications are installed by default.

  - **Packaged File Data**

    Check this box if you want to make sure that the directories where the files belonging to installed packages are located are added to the list of directories to be scanned. For this option to work, the **Packaged File Data** option must be enabled on the Hardware Data Page.

- **Directories from environment group**

  The paths included in the environment variables specified here will also be added to list to scan if you enable this check box. If multiple environment variables are supplied, their names must be separated by a semicolon (;).

- **Shortcuts to the network/Used programs launched from the network**

  This option is available for Targeted Directory Scans only

    - **Scan network drives**

      When checked, this option forces all directories pointed to by shortcuts to be scanned. The scanners may scan directories on network volumes. This is particularly useful when scanning for software licenses as the scanner will detect files that are part of a network install that is accessible from the machine.

      If unchecked, the directories that are located on the drives that are excluded by the drive selection on the Drives and Drive Selection tabs will not be scanned. Usually shortcuts to network drives or network directories from which used programs were executed will not be scanned.

- **Shortcuts to excluded drives**

  This option is available for Combined scans only.

    - **Scan excluded drives**

      When checked, this option forces all directories pointed to by shortcuts to be scanned. If unchecked, the directories that are located on the drives that are excluded by the drive selection on the Drives and Drive Selection tabs will not be scanned.

      When this option is checked, the scanners may scan directories on network volumes. This is particularly useful when scanning for software licenses as the scanner will detect files that are part of a network install that is accessible from the machine.

Although the **Directories** tab page allows you to specify the file systems and directories (known to the Scanner Generator) that you want to include or exclude during scanning, you can override the settings of the file systems and specific directories and files during software scanning by using the content in the override files. How to add content to the override files is explained in the section on Troubleshooting Tab on page 168.

File Scanning Tab

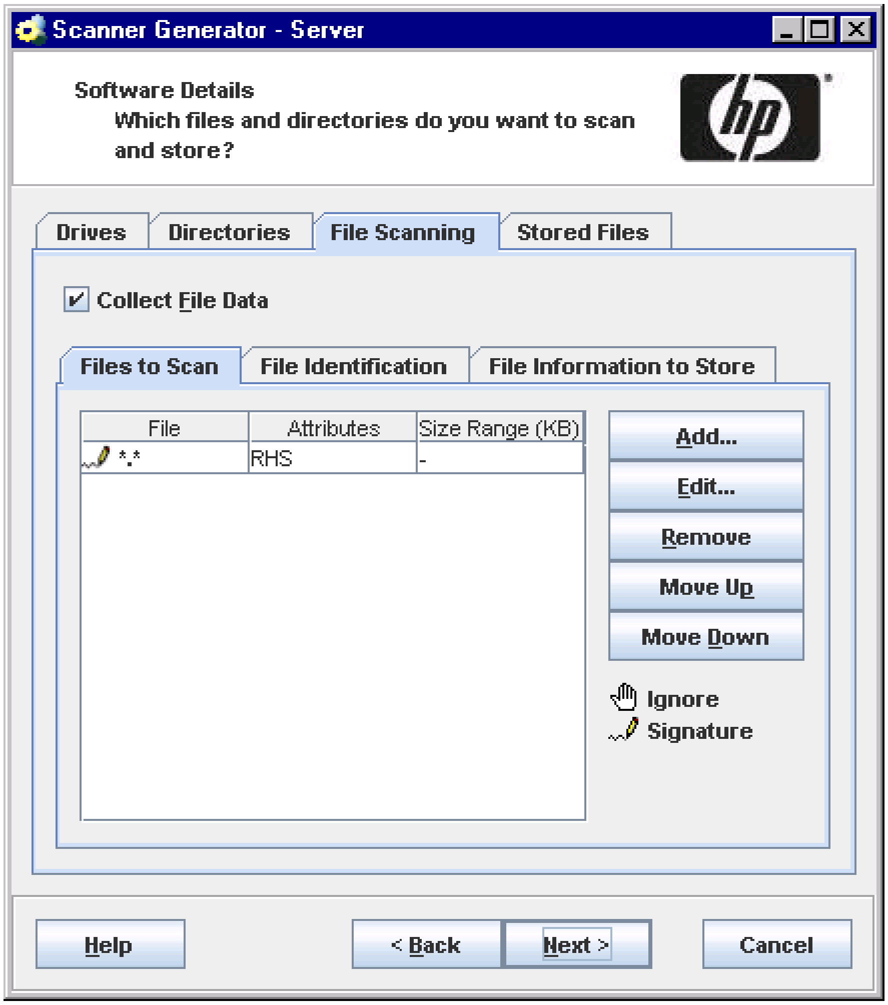
The **File Scanning** tab is used to specify the level of detail for the information collected about files and directories and the methods used to check and identify files.

This tab page contains three sub tabs:

- Files to Scan Sub Tab
- File Identification Sub Tab
- File Information to Store Sub Tab

Files to Scan Sub Tab

The **Files to Scan** sub tab is used to specify how much information is collected about files and the checking processes used.



Scanner Generator - Server

Software Details
Which files and directories do you want to scan and store?

☑ Collect File Data

File	Attributes	Size Range (KB)
.	RHS	-

Using the options on this page, it is possible to define which files get signatured based on criteria such as file extension, attributes or size.

Files to Scan List Box

The **File to Scan** list box displays the checking methods used for processing files. You can build up a prioritized list of filters which specify a sequence of checking processes to be used.

The checking processes are denoted by the following icons:

Table 21 Icons in the Files to Scan List Box

Icon	Meaning
✋	Ignore the specified type of file. In this case, Ignore means do not open the file. Its name, size and attributes may be still picked up in the scan file.
✎	Collect file signatures for the specified type of file. A signature is a checksum of the first 8 KB of the file.

- New filters can be added by clicking **Add**. See Specifying Information Collected about Files and Checking Methods Used on page 125.
- Filters can be edited by double-clicking on them or by selecting them and clicking **Edit**.
- Filters can be reordered by clicking on the row and dragging it up or down to its new location or by clicking **Move Up** and **Move Down**.

Timing Considerations

Only files that have signatures enabled are opened and are available for further processing. If a copy of the file name is all that is required, use the following command.

```
Ignore *.*
```

The file name, size and attributes may still be picked up in the scan file but no signatures will be calculated. Scanning time will be greatly reduced but because less data is collected, application recognition accuracy may be adversely affected.

File Signatures

The signature is an ISO checksum (CRC) of the first 8KB of the file. To calculate the signature, the scanner opens the file and reads the first 8KB from it. Collecting signatures helps to establish the file's identity. Two different files rarely have the same signature. Signatures are used by the software recognition in analysis tools to improve software application recognition. Also, only those fields for which signatures were collected can optionally be identified by the scanner (see File Identification Sub Tab on page 128).

Importance of the Order of Process Selections

The order in which process selections occur is important. For example, use Ignore first before making Signature process selections.

This ensures that the Ignore items are processed first before a file needs to be opened. It may be necessary to ignore certain files, the content of which is constantly changing.

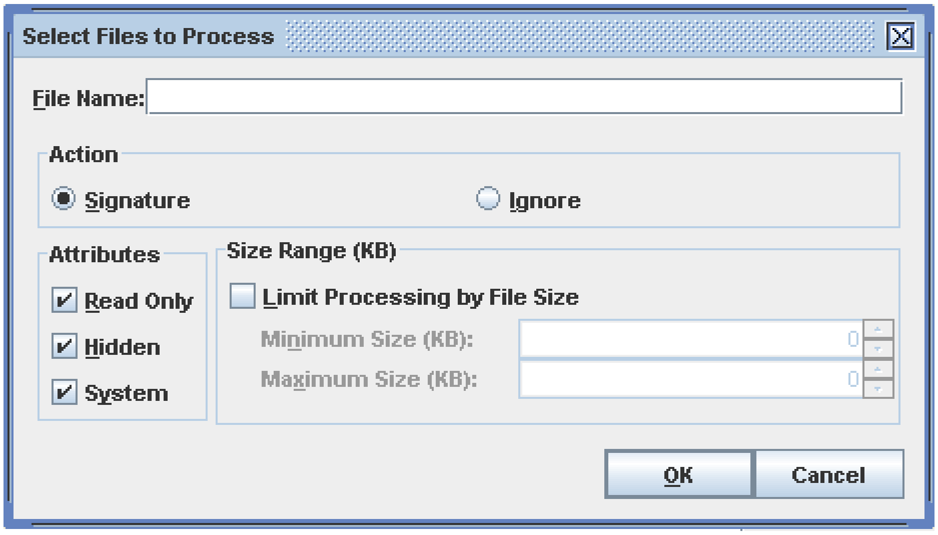
Examples of files to ignore because of changing content are files that are normally used as swap files (386part.par, pagefile.sys, swapper.dat, win386.swp) or files that contain volumes of compressed drives, such as, DriveSpace, DoubleSpace or Stacker (Dblspace.0??, Drvspace.0??, Stackvol?.sys).

Specifying Information Collected about Files and Checking Methods Used

A scanner configured using the Scanner Generator scans selected files on the drives or in the directories selected.

To specify the information collected about files and the checking methods used:

1. In the **Files to Scan** sub tab, select the **Collect File Data** check box. This option activates the controls on this tab page.
2. Click **Add**. The Select files to process dialog box opens.



Select Files to Process

File Name:

Action

● Signature ○ Ignore

Attributes

☑ Read Only

☑ Hidden

☑ System

Size Range (KB)

□ Limit Processing by File Size

Minimum Size (KB): 0

Maximum Size (KB): 0

3. In the **File Name** box, specify the relevant wildcard file type to process.

   For example, *.tmp means all files with tmp extension. Multiple specifications, separated with semicolons, are also accepted.

4. In the Action group box select one of the following options:

   - **Signature**

     Collect file signatures for the specified type of file.

   - **Ignore**

     Ignore the type of file specified in the File Name box.

5. In the Attributes group box, select from the following options as required:

   - **Read Only**

     Files with the read-only attribute are capable of being displayed, but not modified or deleted.

   - **Hidden**

     Files with the hidden attribute are not normally visible to users. For example, hidden files are not listed when you execute the `DOS DIR` command. However, most file management utilities allow you to view hidden files.

   - **System**

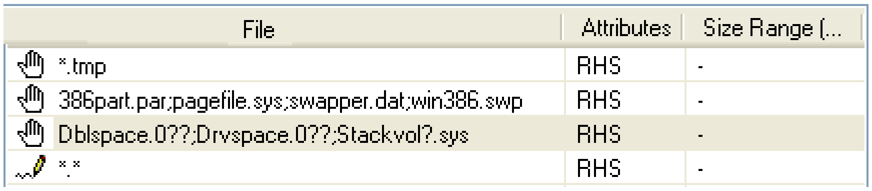
     Files with the System attribute.

   In general, if a given attribute is not selected, the entry having the attribute will not match, even if the file name does.

6 In the **Size Range (Kb)** group, if required, select the **Limit Processing by File Size** check box and specify the maximum and minimum file sizes. Only files within this size range will be processed.

7 Click **OK**.

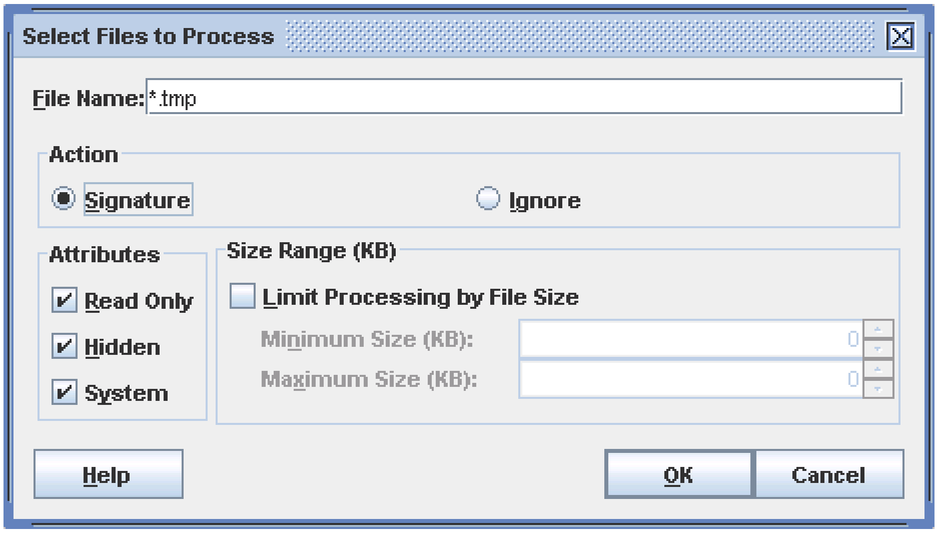
File Action Options - Example



File	Attributes	Size Range (...
*.tmp	RHS	-
386part.par;pagefile.sys;swapper.dat;win386.swp	RHS	-
Dblspace.0??;Drvspace.0??;Stackvol?.sys	RHS	-
.	RHS	-

The entries in the file list box mean:

1 Ignore (do not open) any files (including read-only, hidden or system) with a `.tmp` extension.



Select Files to Process

File Name: *.tmp

Action

● Signature ○ Ignore

Attributes

☑ Read Only

☑ Hidden

☑ System

Size Range (KB)

□ Limit Processing by File Size

Minimum Size (KB): 0

Maximum Size (KB): 0

2 Ignore the following files, including files with read-only, hidden and system attributes:

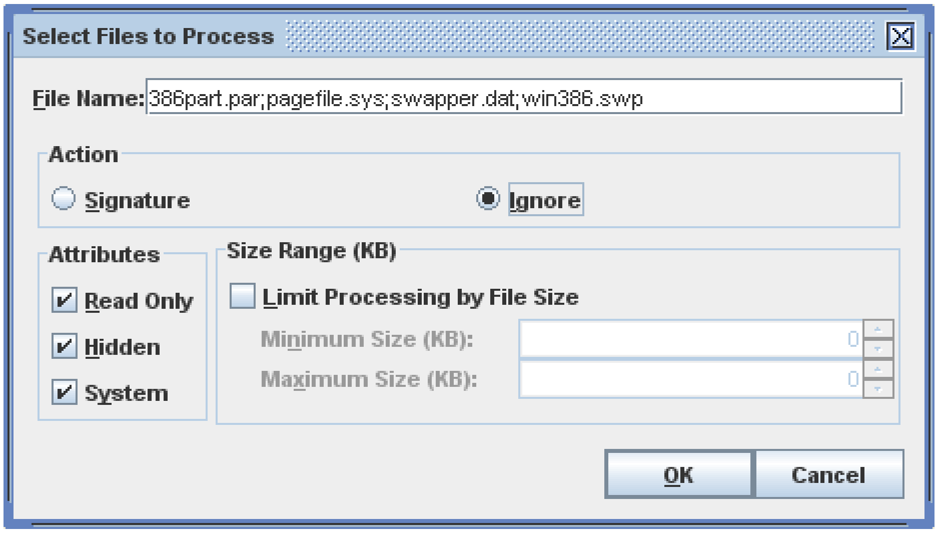
— Files that are normally used as swap files:

— `386part.par`

— `pagefile.sys`

— `swapper.dat`

— `win386.swp`



Select Files to Process

File Name: 386part.par;pagefile.sys;swapper.dat;win386.swp

Action

○ Signature ● Ignore

Attributes

☑ Read Only

☑ Hidden

☑ System

Size Range (KB)

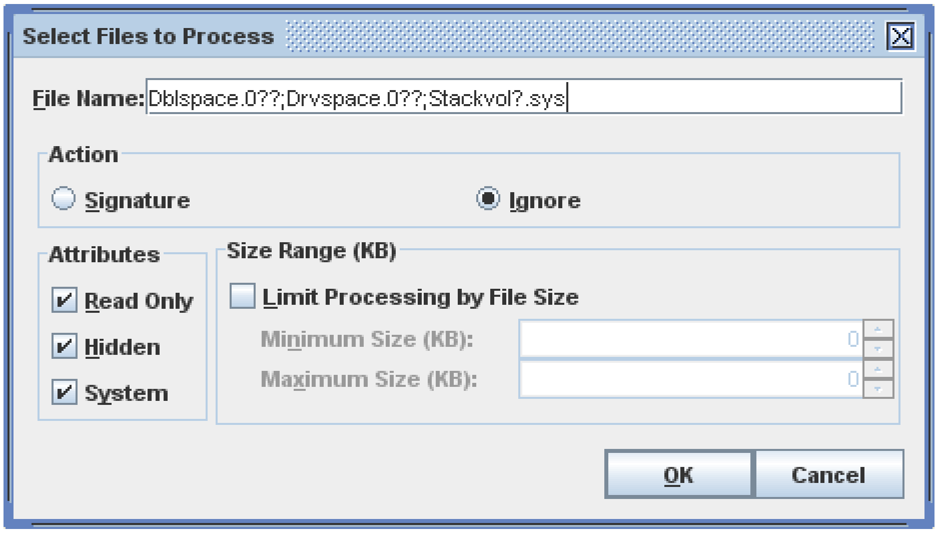
☐ Limit Processing by File Size

Minimum Size (KB): 0

Maximum Size (KB): 0

3 Ignore the following files, including files with read-only, hidden and system attributes:

- Files that contain volumes of compressed drives, such as DriveSpace, DoubleSpace or Stacker.
- `Dblspace.0??`
- `Drvspace.0??`
- `Stackvol?.sys`



Select Files to Process

File Name: Dblspace.0??;Drvspace.0??;Stackvol?.sys

Action

○ Signature ● Ignore

Attributes

☑ Read Only

☑ Hidden

☑ System

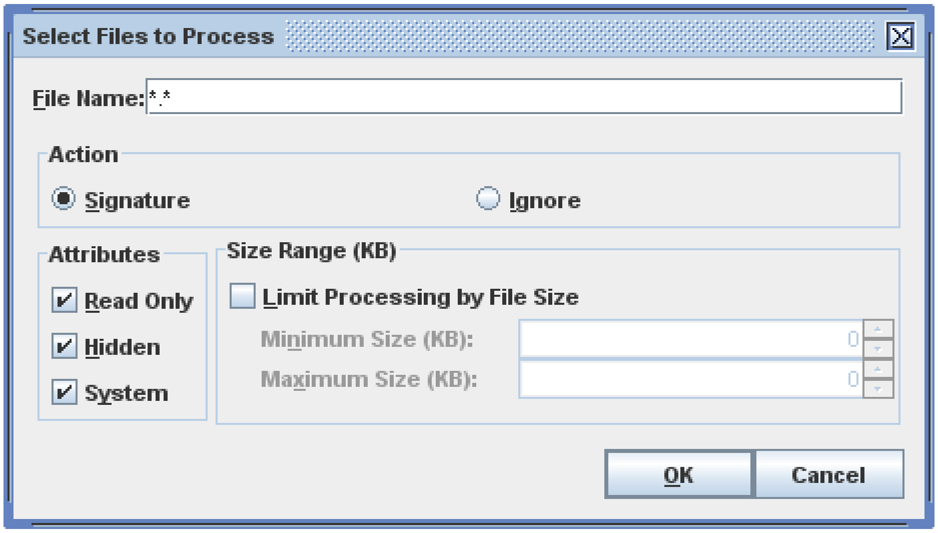
Size Range (KB)

☐ Limit Processing by File Size

Minimum Size (KB): 0

Maximum Size (KB): 0

4 Calculate file signatures for all files, including files with read-only, hidden and system attributes.


Select Files to Process

File Name: *.*

Action

● Signature ○ Ignore

Attributes

☑ Read Only

☑ Hidden

☑ System

Size Range (KB)

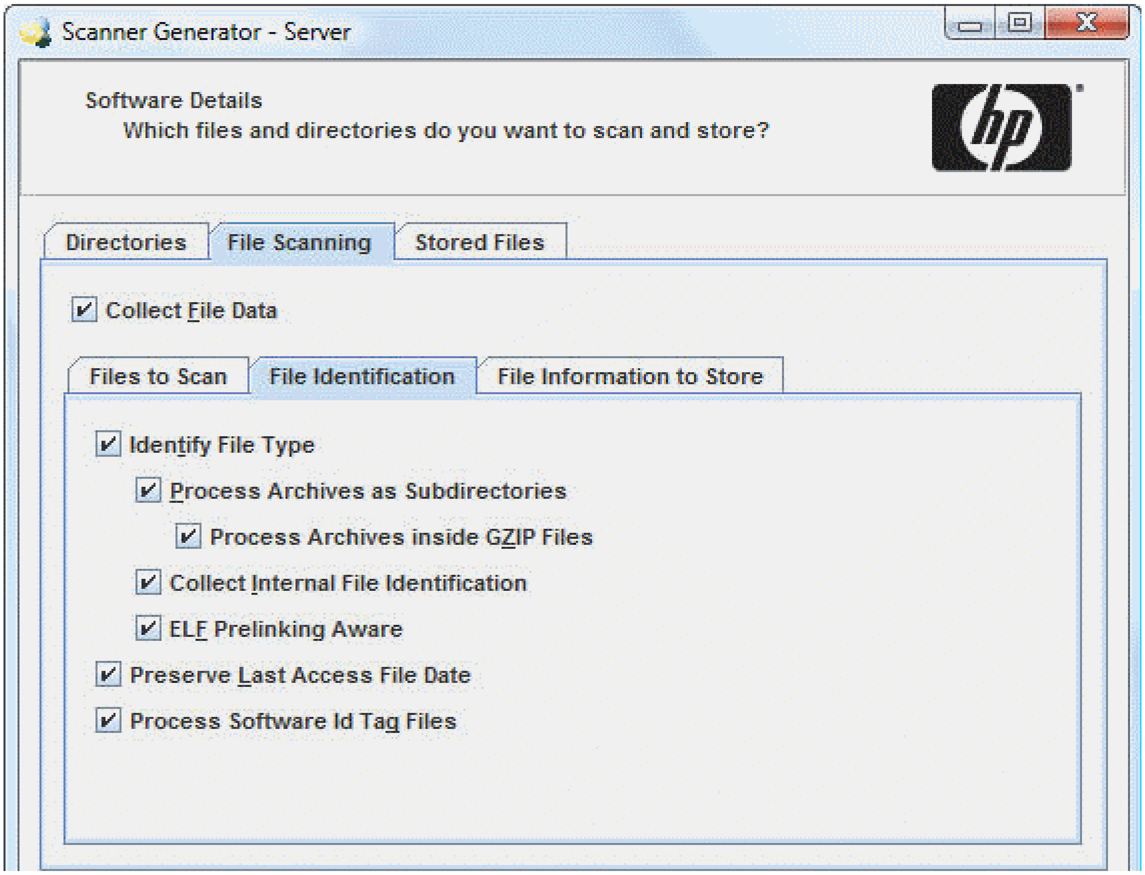
□ Limit Processing by File Size

Minimum Size (KB): 0

Maximum Size (KB): 0

File Identification Sub Tab

The **File Identification** sub tab page is used to determine whether the scanner will identify files based on their content.


Scanner Generator - Server

Software Details

Which files and directories do you want to scan and store?

☑ Collect File Data

☑ Identify File Type

☑ Process Archives as Subdirectories

☑ Process Archives inside GZIP Files

☑ Collect Internal File Identification

☑ ELF Prelinking Aware

☑ Preserve Last Access File Date

☑ Process Software Id Tag Files

Specifying Whether the Scanner Will Identify Files Based on their Content

To specify whether the scanner will identify files based on their contents:

1. Ensure that the **Collect File Data** check box is selected. This option activates the controls on this tab page.
2. Select the options as required:
   - **Identify File Type**

     Instructs the scanner to check every file that was selected for signatures to identify all executable and archive files. The scanner can identify LZH, LHA, ZIP, ARJ, ARC and PAK archives. Selecting this check box will enable two further options:

   — **Process Archives as Subdirectories**

     Treats archive files as subdirectories and lists the files included in each archive (it does not extract information from within these files). If this check box is not selected, archive files are not scanned for embedded files and directories.

     A further option is made available:

     – **Process Archives inside GZIP files**

     This option enables the handling of archives located in gzip files (such as `.tar.gz` files). These are tar archives that were compressed using gzip. Checking this option will instruct the scanner to process such archives.

   — **Collect Internal File Identification**

     Collects internal file information included in the executable file, for example, version data and legal copyright.

   — **Elf Prelinking**

     During software scanning, this option instructs the scanner to check if an executable file has been pre-linked by the ELF Prelinking Utility (prelink). The ELF Prelink Utility is used to speed uploading times of ELF shared libraries and executables by modifying them to reduce the number of the reallocations the dynamic linker needs to do to load them in memory. If this option is enabled, the scanner will calculate the size and signature of the file before it was pre-linked. This is useful for accurate application recognition since the file size and signature are used to perform application matching. However, enabling this option does produce extra overhead during the scan as the scanner needs to run the prelink utility to obtain the original executable file. The prelinked file is not modified by the scanning process; the original file is only reconstructed temporarily in order to collect the size and signature. This is for Linux platforms only.

   - **Preserve Last Access File Date**

     Collects the Last Accessed time stamp for files (where available). The support for the Last Accessed time stamp varies depending on the Operating System and file system used.

     When this setting is used on Unix computers, although the last access time will be preserved, the `ctime` of the file gets changed. For this reason we recommend that you do not use this setting on Linux, Mac OS X or Unix computers.

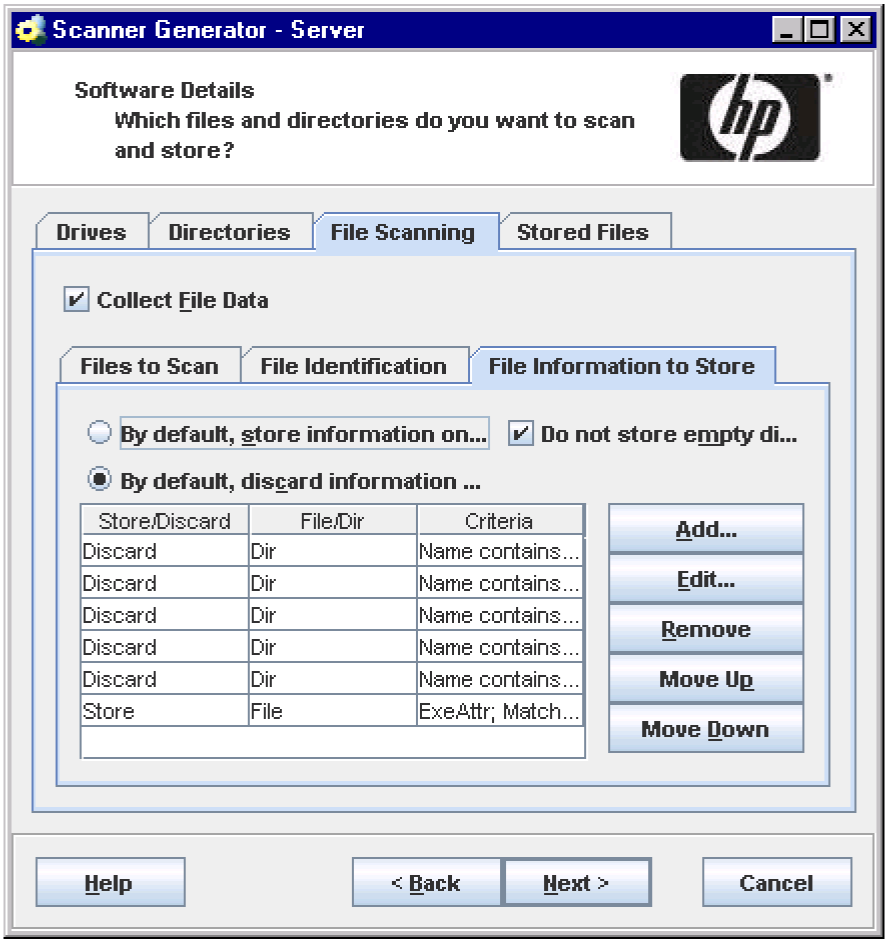
➤ When this option is enabled, the XML Enricher can make use of this feature to accurately estimate the time when recognized applications were last executed.

- **Process Software Id Tag Files**

  This setting is used to enable or disable the collection of information from software tag files during the software scanning phase. During the hardware detection phase, the information from tag files that are located in the common system location and in the root of the application's installation directory is picked up. However, it is not possible to locate a tag file stored in the root of the application's installation directory if the application is not packaged in a standard package format. In such cases, the Scanner will collect the tag file information from such applications during the software scanning phase.

File Information to Store Sub Tab

The **File Information to Store** sub tab is used to define what file details to store in the scan file.



☑ Collect File Data

○ By default, store information on... ☑ Do not store empty di...

● By default, discard information ...

Store/Discard	File/Dir	Criteria
Discard	Dir	Name contains...
Discard	Dir	Name contains...
Discard	Dir	Name contains...
Discard	Dir	Name contains...
Discard	Dir	Name contains...
Store	File	ExeAttr; Match...

Adding, Editing or Removing File Filter Storage Criteria

The three options at the top of the page set the default to either:

- **By default, store information on all files** - If selected, and no other options are specified, then information about all files is stored in the scan file.
- **By default, discard information on all files** - If selected, and no other options are specified, then no file data at all is stored in the scan file.

- **Do not store empty directories** - This option is selected by default. When checked, the scanner discards information about directories that have no files in them. This can include directories that may have files in them, but you have set up the scanner not to scan for these particular types of file.

In addition to the default settings, you can define a prioritized list of filters, in a manner similar to that of the **File to Scan** page.

Each filter can specify directories or files to be included or excluded from being stored. Each file and directory entry found during scanning is looked up in the list, and the first matching entry determines whether the entry is stored or not.

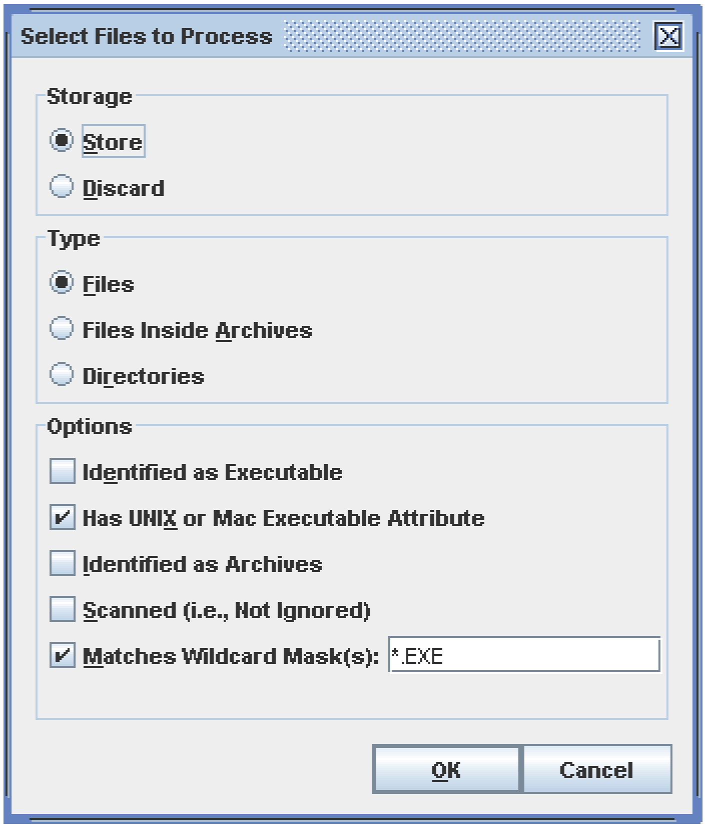
- Multiple filter criteria can be specified on each line if they are separated by a semicolon.
- Entries can be edited by double-clicking on them.
- The sequence and priority of an entry can be reordered by clicking on the row and dragging it up or down to its new location. This can also be achieved by using the **Move Up** and **Move Down** buttons.

To add, edit or remove file filter storage criteria:

- To add another filter criteria, click **Add...**
- To edit an existing filter criteria, click **Edit...** or double-click on the entry.
- To remove an existing filter criteria, click **Remove**.

The options chosen here can dramatically affect both scanning speed and scan file size. Under normal circumstances, the default options are adequate.

If you clicked **Add** or **Edit**, the **Select Files to Process** dialog box appears.



Select Files to Process

Storage

● Store

○ Discard

Type

● Files

○ Files Inside Archives

○ Directories

Options

□ Identified as Executable

☑ Has UNIX or Mac Executable Attribute

□ Identified as Archives

□ Scanned (i.e., Not Ignored)

☑ Matches Wildcard Mask(s): *.EXE

This dialog box has three types (shown in the Type group box):

- Files
- Files Inside Archives
- Directories

Including or Excluding Files Based on File Name or Scanned Attributes

Follow this procedure if you selected the **Files** Type in the **Select Files to Process** dialog box.

To include or exclude files based on the file name or scanned attributes:

1. Choose one of the options **Store** or **Discard** from the **Storage** group box. This determines whether a matching file is stored in the scan file, or discarded. Discarded entries are not available for analysis.
2. Select the **Files** option in the **Type** group box.
3. Check the **Matches wildcard mask(s)** option.
4. Specify a list of wild cards separated by a semicolon (;). For example, when scanning of Java class files is enabled (see Standard Configuration Page on page 104), the entry to include *.class files inside archives is added to the default configuration. This causes the scanner to only store the information about files with the `.class` extension found inside of archives.
5. Files can also be stored or discarded based on attributes not known until the file has been scanned. Select from the following in the **Options** group box:

- **Identified as executable**

  Files that are identified as any kind of executable (that is, not just `.exe` and `.com` files). If Identify file type is not checked this has no effect.

- **Has Unix or Mac executable attribute**

  UNIX allows three different levels of access to a file for three different categories of users: owner, group and other.

Table 22 UNIX levels of access

Level	Description
Read	View the file or directory without making changes.
Write	Make changes to the file or directory
Execute	Execute the file or list files in a directory.

  Checking this option causes the scanner to store or discard files that have executable file access in any of the user categories (namely, owner, group or other.)

- **Identified as archives**

  Files that are identified as compressed, such as .ZIP, .LZH. If Identify file type is not checked this has no effect.

  - **Scanned (i.e. not Ignored)**

    Includes all files that are not ignored on the File Scanning page.

  - **Matches wildcard mask(s)**

    Includes files that match the wildcards specified here.

Explanation of the Operation

All file check box options specified are OR-ed together, that is, the entry is considered a match if any of the selected entries match.

The order and content of these options can affect scanning speed and function significantly. If the default is Discard, and a Store - Identified as executable entry is included, all files have to be scanned before the scanner can determine if they are to be discarded.

Including or Excluding Files Based on Files Inside Archives

Follow this procedure if you selected the **Files Inside Archives** Type in the **Select Files to Process** dialog box.

To include or exclude files based on the files inside archives:

1. Choose one of the options **Store** or **Discard** from the **Storage** group box. This determines whether a matching file inside an archive is stored in the scan file, or discarded. Discarded entries are not available for analysis.
2. Select the **Files Inside Archives** option in the **Type** group box.
3. Check the **Matches wildcard mask(s)** option.
4. Specify a list of wildcards separated by a semicolon (;). Files discarded in this way are not scanned either, and a wildcard filter can speed up the scanning process.

Including or Excluding Files Based on Directory

Follow this procedure if you selected the **Directories** type in the **Select Files to Process** dialog box.

To include or exclude files based on the directory:

1. Choose one of the options **Store** or **Discard**. This determines whether a matching directory is stored in the scan file, or discarded. Discarded entries are not available for analysis.
2. Select the **Directories** option in the **Type** group box.
3. Select from the following in the **Options** group box:
   - **Named**

     If this option is selected, the directory name specified in the entry field must match 100% (however, it is not case-sensitive) in order for a match to be established. The directory name must begin with a path separator to match any entries, but must not include a drive letter. The root directory \ or / cannot be excluded in this way.
   - **Where name contains**

     If this option is selected, the name specified in the entry field is a partial string; any directory containing this string in its name is considered a match. Typical examples of entries would be:

     \Private would match any directory where a directory starts with Private.

     Temporary which would match any directory with Temporary anywhere in the name.
   - **Include subdirectories**

     For either of the directory options, there is an option to include subdirectories of matching entries as well. This is particularly useful for discarding entire directory trees, such as recycle folders, temporary Internet files and private directories.

Explanation of the Operation

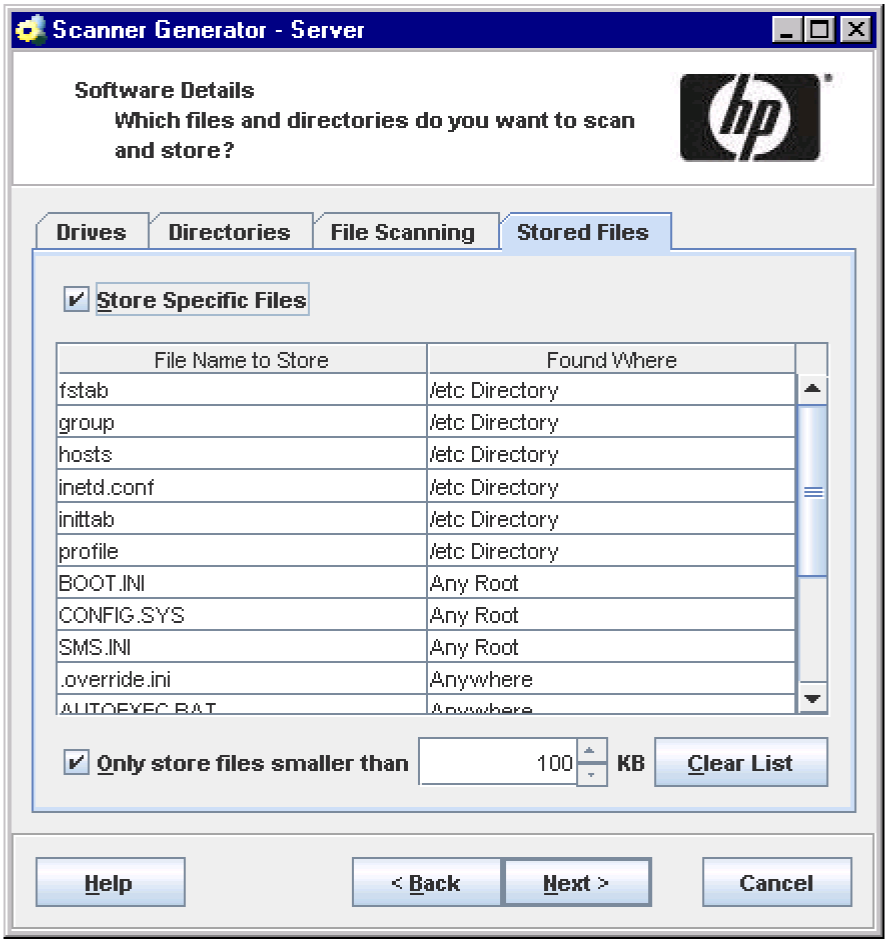
The contents of filtered directories are not stored in the scan file. If the Do not store empty directories (page 130) option is checked, filtered directories are considered to be empty and are not stored in the scan file either. If this option is unchecked, the filtered directories are represented in the Directories and Files tab of the Viewer application by a no entry icon ⛔.

Directories are filtered prior to scanning (that is, directories that will not be stored are not scanned at all). Consequently, directory filters may speed up scanning.

Stored Files Tab

The **Stored Files** tab is used to allow specific files to be collected and stored (embedded) in the scan file created for each computer scanned. The types of files usually collected are system configuration files. These files can be viewed in Viewer or exported from Analysis Workbench.

If a targeted directory scan selection was made earlier and does not include a specific directory in which a stored file may be found (including the root directory), then any required stored file must be specifically defined here with the full path.



Software Details

Which files and directories do you want to scan and store?

☑ Store Specific Files

File Name to Store	Found Where
fstab	/etc Directory
group	/etc Directory
hosts	/etc Directory
inetd.conf	/etc Directory
inittab	/etc Directory
profile	/etc Directory
BOOT.INI	Any Root
CONFIG.SYS	Any Root
SMS.INI	Any Root
.override.ini	Anywhere
AUTOEXEC.BAT	Anywhere

☑ Only store files smaller than 100 KB

The dialog box shows a list with two columns:

- File Name to Store Column
- Found Where Column

File Name to Store Column

This column displays a default list of system files. The name of the files can include wildcard characters unless a specific directory is used.

For example, collecting the `Config.sys` file for each computer scanned across a population provides a snapshot of the system configuration for each computer. This enables the analysis and consolidation of system configuration across the computer population.

Other commonly collected files are `Net.cfg`, `Profile.ini`, `AutoExec.Bat`, `Win.ini`, `System.ini` and `Boot.ini`.

The one DDM Inventory specific file included in the list is the override file, which is named `override.ini` on Windows systems and `.override.ini` on UNIX/Mac OS X systems. This is an ASCII file used by the scanner at run-time to store a list of files to be ignored (that is not opened at run-time). See Directories Tab on page 120.

Enabling the Controls on the Stored Files Page

To enable the controls on the Stored Files page:

Select the **Store Specific Files** check box to enable the controls on this page.

Adding another File to the List of Files Stored

To add another file to the list of files stored:

1 Enter a file name at the bottom of the **File Name to Store** column (or overwrite an existing entry).

2 Select an option from the drop-down list in the **Found Where** column.

Deleting a File From the File Name to Store Column

To delete a file from the File Name to Store column:

1 Highlight the file name.

2 Press the **Delete** key or right-click on the entry and select the **Delete** option from the shortcut menu.

Clearing Entire List of Files to Be Stored

To clear the entire list of files to be stored:

1 Click **Clear List**. A confirmation message is displayed.

2 Click **Yes** to clear the list.

Limiting Size of Files to Be Stored

To limit the size of files to be stored:

1 Select the **Only store files smaller than** option.

2 In the **Kb** box, use the arrows to select a value for the upper size limit or type the value directly into the edit box.

➤ Not restricting the size of files collected could result in very large scan files when large files are collected and stored.

Found Where Column

This column shows the location where the files to be stored can be found.

Changing the Directories that Are Scanned to Locate Files

To change the directories that are scanned to locate the files

1 Click on an entry in the **Found Where** column.

2 Change the setting by selecting an option from the drop-down list.

Table 23 Options for changing directories that are scanned to locate files

Setting	Description
Any Root Directory	Only stores the file if it is found in a root directory.
Root of Boot Drive	Only stores the file if it is found in the root of the boot drive.
Anywhere	Store the file wherever it is located.
/etc directory	Only stores the file if it is found in the Unix /etc directory.
/var directory	Only stores the file if it is found in the Unix /var directory.

Specific directory	A specific copy of the file is collected irrespective of whether it is included in the software scan or not.
	For example, the list of specific stored files could be configured to be:
	`C:\Documents\config.txt`
	`Z:\net.ini`
	`/etc/fstab`
	In this case, the scanner will store the config.txt file from the C: drive (when scanning PCs), the net.ini on the Z: drive (if it is available, and only on PCs) and a file named fstab in the /etc directory (when scanning UNIX machines).

➤ Files will only be stored if the directory where the file is located is included in the software scan, unless the specific directory is specified.

Asset Data Page

The **Asset Data** page is used to define and set up the asset data collected by the scanners.

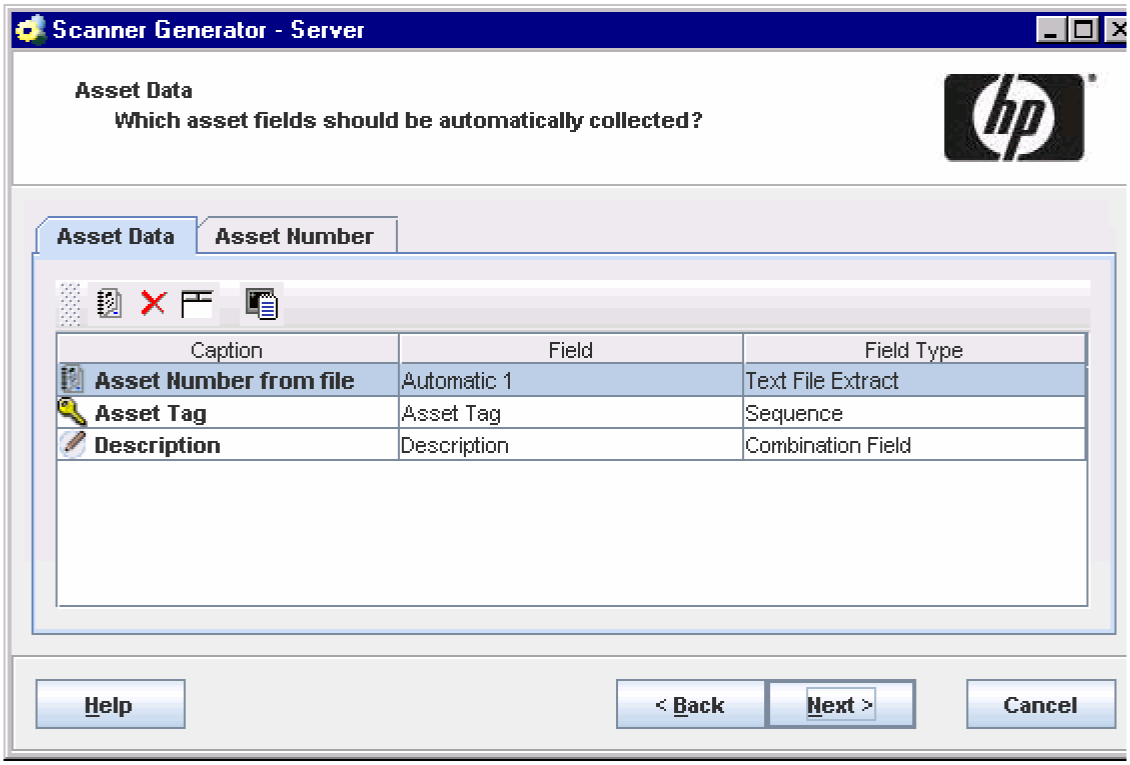
The Asset Data page has two tabs:

- Asset Data Tab - Used to define which asset data is to be collected automatically.
- Asset Number Tab - Used to specify the source for the Asset Number (Manual Deployment Mode only)

After the asset data settings have been configured, click **Next** to continue.

Asset Data Tab

The **Asset Data** tab is used to configure customized asset information as each computer is scanned.



Scanner Generator - Server
Asset Data
Which asset fields should be automatically collected?
Asset Data
Asset Number
Help
< Back
Next >
Cancel

Caption	Field	Field Type
Asset Number from file	Automatic 1	Text File Extract
Asset Tag	Asset Tag	Sequence
Description	Description	Combination Field

A default list of entries is displayed initially. These can be modified to create a custom list of entries.

The Asset Data tab will help the scanner find specific asset information that is available on the scanned device. To include other information about the user, you can use the Asset Questionnaire through the web user interface. Log into your DDM Inventory server, and click **Administration** > **Asset Questionnaire** to configure the fields you want in your questionnaire. See the *Installation and Initial Setup Guide* for more information.

Asset Data Form Layout

The **Asset Data** form is made up of a number of rows and three columns. Each row in the form is used to define a piece of asset data and results in one item being collected during the inventory.

The form is built up by using the combination of up to 23 predefined standard fields, 30 user-defined fields and 56 automatic fields.

Asset Data Form Toolbar

A toolbar is displayed at the top of the Asset Data form. The buttons have the following functions:

Table 24 Asset data form toolbar

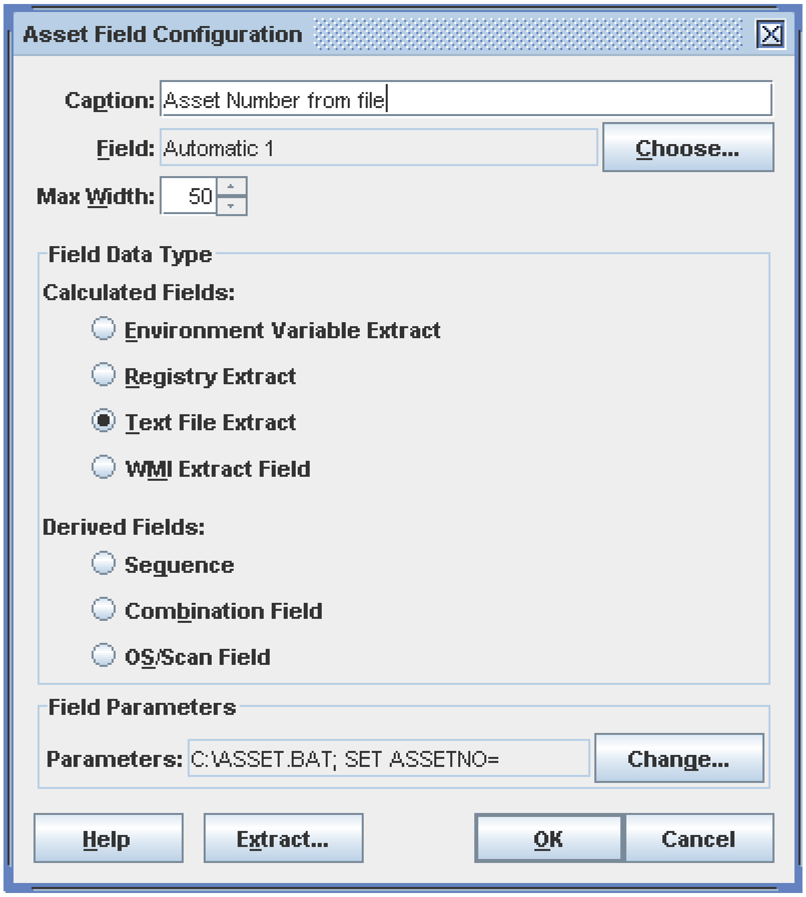
Button	Function	Shortcut
	Create a new field The Choose Field dialog box appears.	Ctrl+N
✕	Delete field	None
	Delete all fields Clear all the entries in the Asset Data form. A confirmation message is displayed before the entries are cleared.	None
	Edit the type and settings for field The Asset field configuration dialog box appears, which allows you to edit the information for the field.	Ctrl+T

These functions are also available by using a right-click menu.

To further configure the field, double-click on the row or click the **Edit** button to bring up the **Asset Field Configuration** dialog box.

Asset Field Configuration Dialog Box

This dialog box is where the major part of the asset field configuration takes place.



Asset Field Configuration

Caption: Asset Number from file

Field: Automatic 1

Max Width: 50

Field Data Type

Calculated Fields:

- ○ Environment Variable Extract
- ○ Registry Extract
- ● Text File Extract
- ○ WMI Extract Field

Derived Fields:

- ○ Sequence
- ○ Combination Field
- ○ OS/Scan Field

Field Parameters

Parameters: C:\ASSET.BAT; SET ASSETNO=

Setting up a New Asset Field

Each row in the form has three columns. Each of these columns must be configured for a new asset field.

The following table shows the steps that are required in setting up a new asset field and the pages they are described on:

Table 25 Steps for setting up a new asset field

Step	Title
1	Set up a caption
2	Choose a standard field
3	Specify the maximum width in characters for the fields
4	Choose the field data type

Table 25 Steps for setting up a new asset field

Step	Title
6	Set up field parameters
7	Set up extract options for calculated fields
8	Correct the order of the fields in the form

Step 1: Setting up a Caption

This text caption is used to identify each data input item (Scanner Generator truncates the prompt at 22 characters).

To change the caption, change the entry in the **Caption** field.

The text entered here will be displayed in the analysis tools (Analysis Workbench and Viewer).

Step 2: Choosing a Standard Field

To make the task of entering data as simple as possible, and to avoid discrepancies due to typing and naming conventions, the Scanner Generator provides several predefined standard field types with automatic validation controls.

The standard asset fields indicate to which hardware field the asset field will be mapped. For example, if you choose Employee ID as the standard field, the data contained in this field will be mapped to the Employee ID field, while allowing you to customize the prompt displayed on-screen (for example, by translating it to French).

There are two special standard fields that you need to understand before proceeding with this step.

Description Field

The **Description** field is represented by the ✎ icon and can be configured to contain a brief description of the computer. This field is normally read-only and by default is configured to be of type Combination. It combines information from several hardware and asset fields.

When loading data from scans into the analysis tools (Analysis Workbench and Viewer), the contents of the description field are displayed for each scan file to help identify them.

Asset Tag Field

The **Asset Tag** field is represented by the 🔑 icon. It contains a unique identifier for the machine. It is normally populated from a sequence of hardware fields such as MAC Address, Serial Number or Asset tag.

The asset number entered in this field is usually used to name the scan file the scan results are recorded to.

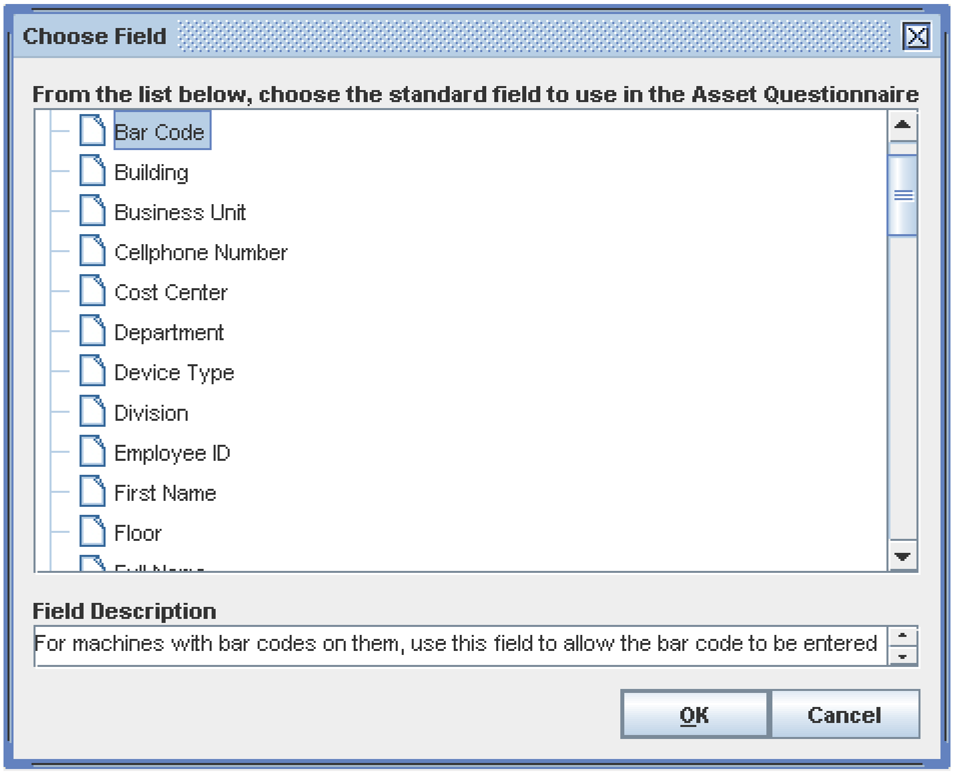
If you have not configured an asset tag field and the **Asset Number Source** is set to **Asset Field**, you will not be allowed to proceed to the next page and a warning will appear.

➤ It is strongly recommended that **Description** and **Asset Tag** fields are included in your list of asset fields.

To choose a standard field:

1 Click the icon.

2 The **Choose Field** dialog box is displayed, showing all standard fields not currently in use.



Choose Field

From the list below, choose the standard field to use in the Asset Questionnaire

- Bar Code
- Building
- Business Unit
- Cellphone Number
- Cost Center
- Department
- Device Type
- Division
- Employee ID
- First Name
- Floor
- Full Name

Field Description

For machines with bar codes on them, use this field to allow the bar code to be entered

3 Choose a new standard field from the list.

These fields are legacy fields left from previous releases of DDM Inventory when it was possible to enter the asset data manually in the scanners. In this version of the software, the scanners do not have such ability. Instead this kind of manual data entry can be done using the new web-based asset questionnaire.

Table 26 Standard fields

Field	Description	Field mapped to in the hwAssetData table
Asset Tag	The Asset Tag field contains a unique identifier for the machine.	`hwAssetTag`
Automatic Asset Fields	These asset data fields can be automatically populated from data extracted from text files, the Windows registry or environment variables. You can configure up to 56 automatic fields, which can then be used in the calculation of derived or calculated fields.	`hwAssetAutomatic1..56`
Bar Code	For machines with bar codes on them, use this field to allow the bar code to be entered or stored	`hwAssetBarCode`

Table 26 Standard fields

Field	Description	Field mapped to in the hwAssetData table
Building	Identified the building containing the machine	`hwAssetBuilding`
Business Unit	Name of business unit	`hwAssetBusinessUnit`
Cellphone Number	Cell/Mobile phone number of user.	`hwAssetCellphoneNumber`
Cost Center	Cost center description or code	`hwAssetCostCenter`
Device Type	Device type of the machine (Server, Notebook, Tower and so on)	`hwAssetDeviceType`
Division	Division description or code	`hwAssetDivision`
Employee ID	Employee ID as used in the organization.	`hwAssetEmployeeID`
Floor	The floor on which the machine is located	`hwAssetFloor`
Full Name	Full name of user	`hwAssetFullName`
Job Title	Job title of user	`hwAssetUserJobTitle`
Machine Model	Model of the machine. This data can be populated from SMBIOS using a Sequence Field on machines supporting SMBIOS.	`hwAssetMachineModel`
Printer Asset Tag	Asset tag of a local printer attached to the machine, if any	`hwAssetPrinterAssetTag`
Printer Description	Contains a description of a local printer attached to the machine, if any	`hwAssetPrinterDescription`
Room	Description, name or number of the room containing the machine	`hwAssetRoom`
Section	Section description or code	`hwAssetSection`
Telephone Number	Full direct telephone number of user	`hwAssetTelephoneNumber`
User Field	These are user-defined fields. You can configure up to 30 User fields.	`hwAssetUserField1..30`

4 Click **OK** to return to the Asset Data form.

Step 3: Specifying Maximum Number of Characters for Field

To specify the maximum number of characters for the field:

Enter a numeric value in the **Max. width in characters** field.

Step 4: Choosing Field Data Type

The asset data fields are automatically populated. The data is either **calculated** or **derived**. The data can be extracted from text files, the Windows registry, environment variables and WMI fields. All data entry fields can be given a default value.

To chose the field data type:

In the **Asset field configuration** dialog box, choose a standard field type from the **Field data type** list.

The following table describes the types of fields and whether they are derived or calculated.

Calculated Fields

These asset data fields can be automatically populated from data extracted from text files, the Windows registry, environment variables and so on.

Table 27 Calculated fields

Field	Description
Environment Variable Extract	Accepts data from a specified environment variable set in the operating system.
Text File Extract	Extracts information from a single line in a named text file. This field type is normally used for the Asset Number field. This is used to extract the asset number from the file Asset.bat on the line containing the text: `SET ASSETNO=` Other useful file extracts include the predefined SMS, which extracts the SMS Unique Machine ID.
Registry Extract	This field type extracts its value from the Windows registry. The Data field must contain a valid registry key name to extract from, for example: `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\TimeZoneInformation\StandardName`
WMI Extract	This field type allows you to extract and store pieces of data on Windows available through the WMI interface. The Windows scanner will populate this field (if set up) on systems where WMI is enabled.

Derived Fields

Derived fields are those that have dependencies on the data of other types of fields. In other words, the data they contain is derived from other fields.

Table 28 Derived fields

Field	Description
Sequence	The Sequence field allows you to define a sequence of up to ten asset or hardware fields. Each of these fields returns a value depending on the machine or environment running. The value returned as the result of the sequence field will be the first of these fields which contains a non-blank value.
OS/Scan	Allows a single field to collect different information for different operating systems. For example, you may want to extract information from a registry on Windows and from a file on UNIX. For each scanner platform a separate asset field could be defined.
Combination	The Combination field uses a substitution string to replace occurrences of %1, %2 and so on. placeholders with the actual values of hardware or asset fields. An example of a Combination field can be found in the Description field of the default Asset Data tab. Up to five fields can be combined into one.

Step 5: Setting Field Parameters

Field parameters need to be set for the following types of fields:

Table 29 Field types

Field	Reference
Sequence	page 144
Environment Variable Extract	page 146
Text File Extract	page 146
Registry Extract	page 148
OS/Scan	page 150
Combination	page 150
WMI Extract	page 152

Setting up a Sequence Field

The Sequence field enables you to define a sequence of up to ten asset or hardware fields. Each of these fields returns a value depending on the machine or environment running. The value returned as the result of the sequence field is the first of these fields containing a non-blank value.

Ignore Strings

Ignore strings are used to specify a set of values that are known to be incorrect, fake, or unwanted. These values should be ignored. For example, when specifying a MAC address as one of the hardware fields in a sequence, you can designate the known fake MAC addresses in the **Ignore Strings** so that they can be filtered out.

A blank field can be defined based on either of the following two criteria:

- The string matches an ignore string.
- The length of the field is shorter than the number specified in the **Shorter Than** field.

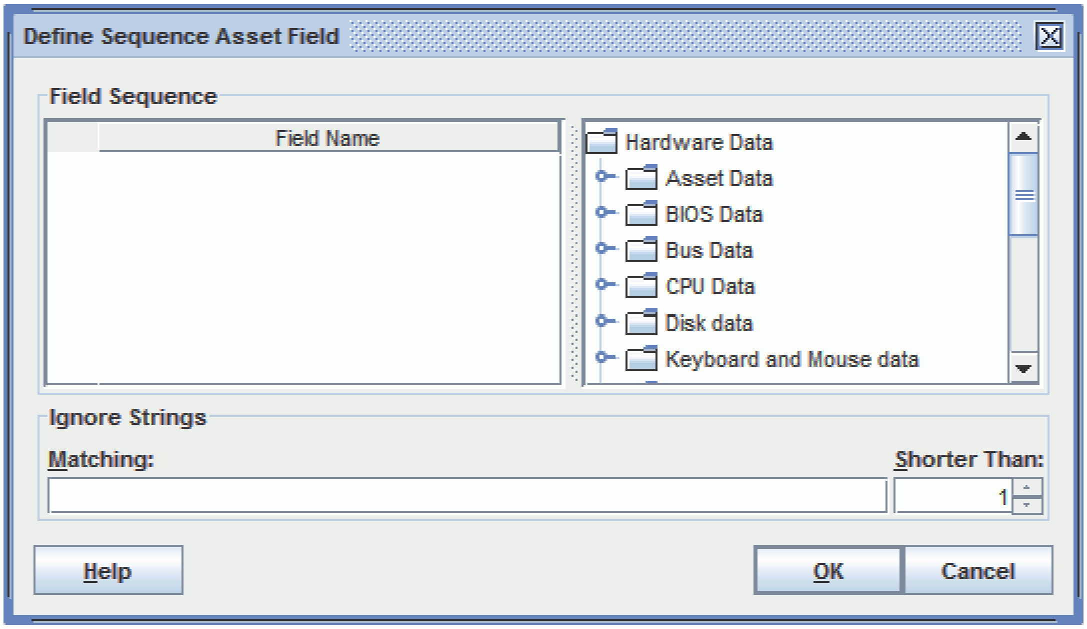
> For how to define the ignore strings, see step 4 on page 145.

To set up a sequence field, perform the following steps:

1 Select **Sequence** from the **Field Data Type**.

2 Click **Change**.

The **Define Sequence Asset Field** dialog box opens.



Shorter Than: 1

3 Select the desired field by expanding the tree on the right side and double-clicking it.

The selected field appears in the **Field Name** list on the left side.

You can also select the field with the drag-and-drop operation.

4 Use one or both of the following methods to specify the ignore strings:

— In the **Matching** box, type a string or a set of strings.

> The string is case-sensitive and the strings are separated by semicolons (;). For example, you can define a set of ignore strings as `Unknown;unknown;Not Tested`.

If the content of the sequence field matches (is equal to) any of the strings specified here, the field is considered to be blank. For example, if the string **`Not Found`** is defined here, then a field that has the value ‘Not Found’ is considered to be blank.

You can type a string in the form: *STRING*. Here the asterisks (*) are ignored and any string that contains the texts between the two asterisks will also be ignored.

- In the **Shorter than** box, use the arrows or type a number to specify the minimum length of the string to be considered as non-blank.

  The default value is 1 and the maximum value is 255. If a field value's length is shorter than the specified number, then the field is ignored and considered blank.

➤ As an empty value's length is 0, an empty field is always ignored.

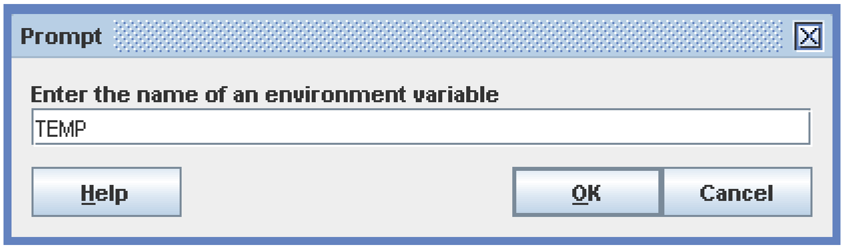
5 Click **OK**.

Setting up Environment Field Parameters

This field is set up to read the value contained in an operating system's environment string. For example, you may have the Host Name or SMS ID stored in an environment variable and want this to be automatically picked up by the scanner.

To set up environment field parameters:

1 After you have selected an Environment Variable Extract as the data field type, click **Change**.



Prompt

Enter the name of an environment variable

TEMP

2 Enter the name of the environment variable in the Prompt dialog box. Examples of environment variables are TEMP or PATH.

3 Click OK to return to the Asset Field configuration dialog box.

Setting up Text File Extract Field Parameters

If you are using environment variables in the file path, they must be in uppercase. For example:

```
%WINDIR%\SMSCFG.INI
```

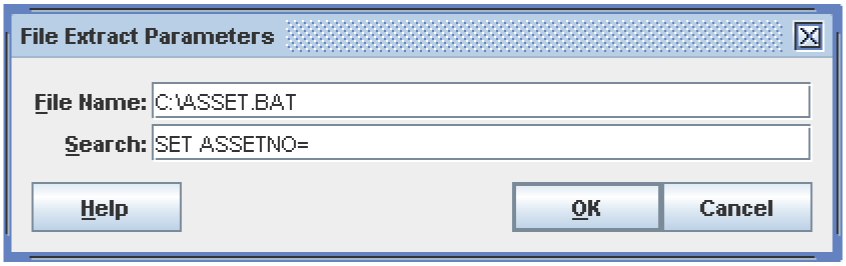
This field searches a named text file for a defined character string and makes an automatic entry of the characters between the search string and the end of the line.

This field type is normally used for the **Asset Number** field. This is used to extract the asset number from the file **Asset.bat** on the line containing the text:

```
SET ASSETNO=
```

To set up the Text File Extract field parameters:

1 After you have selected a **Text File Extract field** as the data field type, click **Change**.



File Extract Parameters

File Name: C:\ASSET.BAT

Search: SET ASSETNO=

2 In the **File Name** group enter the name of the file that the information is to be extracted from. Type the name and path to the file in the box.

A UNC path can also be entered as the path. The format for the UNC path is:

```
\\servername\sharename\path\
```

For example:

```
\\DDMIServer\DDM Inventory\Asset.bat
```

Entries in this field are case-sensitive. This is applicable to UNIX and Mac OS X only.

Using environment variables

You can use an environment variable in the file extract asset **Other** field. The environment variable name must be in upper case for this to happen. If it is not, the string is interpreted as a literal.

For example, if the path is

```
%WINDIR%\SMS.INI
```

Then the final path (assuming WinDir=C:\WINNT) will be

```
C:\WINNT\SMS.INI
```

But if the path is

```
%WinDir%\SMS.INI
```

Then no substitution will take place and the file extract will fail. This is done to ensure that it's possible to extract files from a directory or a file that has one or more `%` signs in the name.

Another example of using an environment variable is as follows:

You can type:

```
%HOME%/.bashrc
```

or

```
%SYSTEMDIR%\win.ini
```

Then the `%HOME%` will be replaced with the value of the `HOME` environment variable.

This is applicable to all platforms and UNIX notation of the form `$NAME` is not supported.

3 Enter the **Search String**. This determines what information is to be extracted. Any text that appears on the line after the search string is extracted (up to the total number of characters set by the field width). The search string is case *insensitive*.

➤ In the file being extracted from, if a comment is on the same line as the search string, then the comment will also be returned. In other words, white space is counted in the search string. Ensure that any comments in the file are placed on separate lines from the search string. This is particularly relevant to UNIX users.

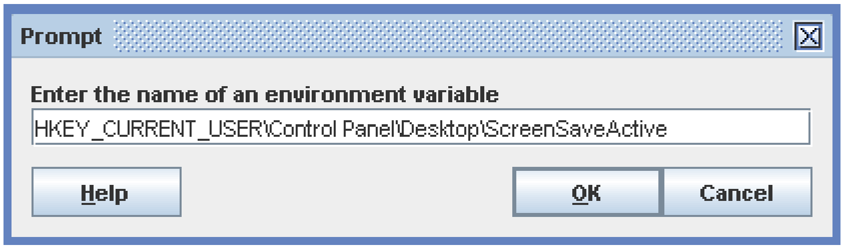
4 Click OK to return to the Asset Field configuration dialog box.

Setting up Registry Extract Field Parameters

This type of field searches the Windows registry for the defined key and makes an automatic entry of the key value. This extract field is applicable to Windows only.

To set up registry extract field parameters:

1 After you have selected a **Registry Extract** field as the data field type, click **Change**.



Prompt

Enter the name of an environment variable

HKEY_CURRENT_USER\Control Panel\Desktop\ScreenSaveActive

2 Type the full path to the registry value you want to have in this field in the form RegistryKey\Value.

For example, to find out whether the Screen Saver is active on the system, you can use the following registry extract field:

```
HKEY_CURRENT_USER\Control Panel\Desktop\ScreenSaveActive
```

➤ The registry does not allow the backslash ("\") character in the RegistryKey. However, it can be used in Value. If the backslash character is contained in the Value name, it must be escaped. For example, if Value is "a\b", it must be specified as follows:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Hewlett-Packard\ED\9.30\\a\b
```

In Windows, the paths to various registry values can be found by viewing the content in the Registry Editor. For more information about the Registry Editor refer to the documentation supplied with Windows.

In 64-bit versions of Windows, portions of the registry entries are stored separately for 32-bit applications and 64-bit applications and mapped into separate logical registry views using the registry redirector and registry reflection. This is because the 64-bit version of an application may use different registry keys and values than the 32-bit version. There are also shared registry keys that are not redirected or reflected.

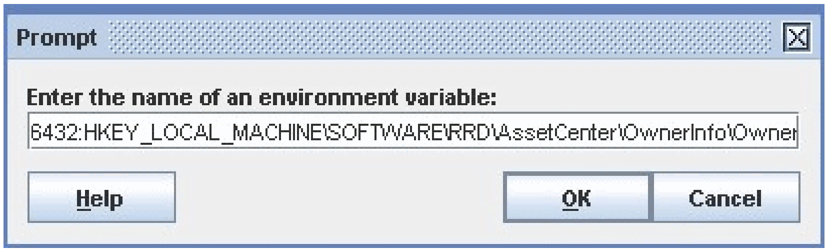
As the DDM Inventory Windows scanner is a 32-bit application, by default, the scanner only reads the 32-bit portion of the registry. In order to access the 64-bit registry portion in 64-bit versions of Windows, the scanner supports the following prefixes:

- “32:” - forces only the 32-bit registry value to be read.

- “64:” - forces only the 64-bit registry value to be read. In 32-bit versions of Windows, the registry extract field with this prefix will always be empty.
- “3264:” - reads the 32-bit registry value, and, if it is empty, reads the 64-bit registry value.
- “6432:” - reads the 64-bit registry value, and, if it is empty, reads the 32-bit registry value.

If no prefix is given, the scanner will only read the 32-bit registry value.

The actual registry value path should follow the prefix, as shown in the following example:



Enter the name of an environment variable:

6432:HKEY_LOCAL_MACHINE\SOFTWARE\RRD\AssetCenter\OwnerInfo\Owner

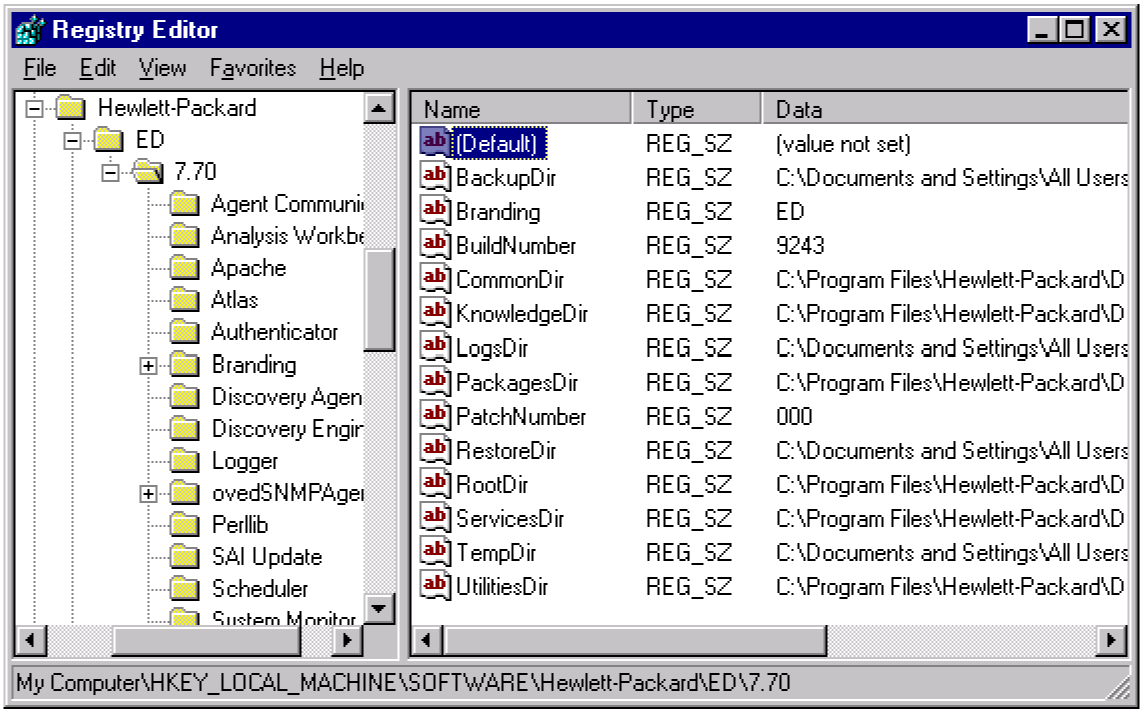
3 Click **OK** to return to the **Asset Field configuration** dialog box.

Do not change any of the settings in the Registry Editor. Doing this could result in lost registry settings and may cause some of your applications to fail.

Extracting the Registry (Default) Value

Sometimes, you may want to extract the (Default) value for a registry entry.

The following screen image shows the regedit screen with the (Default) value:



Name	Type	Data
(Default)	REG_SZ	(value not set)
BackupDir	REG_SZ	C:\Documents and Settings\All Users
Branding	REG_SZ	ED
BuildNumber	REG_SZ	9243
CommonDir	REG_SZ	C:\Program Files\Hewlett-Packard\D
KnowledgeDir	REG_SZ	C:\Program Files\Hewlett-Packard\D
LogsDir	REG_SZ	C:\Documents and Settings\All Users
PackagesDir	REG_SZ	C:\Program Files\Hewlett-Packard\D
PatchNumber	REG_SZ	000
RestoreDir	REG_SZ	C:\Documents and Settings\All Users
RootDir	REG_SZ	C:\Program Files\Hewlett-Packard\D
ServicesDir	REG_SZ	C:\Program Files\Hewlett-Packard\D
TempDir	REG_SZ	C:\Documents and Settings\All Users
UtilitiesDir	REG_SZ	C:\Program Files\Hewlett-Packard\D

My Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Hewlett-Packard\ED\7.70

To extract the (Default) value from the registry:

End the registry extract value command in a backslash.

For example, to extract the (Default) value of "9.30," the following key will be used:

```
"HKEY_LOCAL_MACHINE\SOFTWARE\Hewlett-Packard\ED\9.30\"
```

Setting Up OS/Scan Field Parameters

The **OS/Scan** fields allow the definition of multiple types of data sources to provide an automatic entry depending on the scanner used and the operating system being scanned.

This type of asset field is very useful in situations when you want to scan multiple operating systems but want to collect the same piece of information for each from different sources.

For example, the data can be extracted from the registry on Windows or from a file on UNIX and Mac OS X.

To set up OS/Scan fields:

1. After you have selected an OS/Scan field as the data field type, click **Change**. The **Define Multi-OS Asset Entry Field** dialog box appears.
2. In the **Operating System** list select the operating system that will be affected by this definition.
3. Select the field that is to be included in this definition from the Field Chooser tree. This can be any existing asset field or any hardware/configuration field (except hardware fields where multiple values may be collected, such as CPU type or IP address).
4. Click **Add**. The new definition will be included in the **Fields referred to** list.

The **Field Index** column has a drop-down list which refers to the line numbers in the **Fields referred to** list.

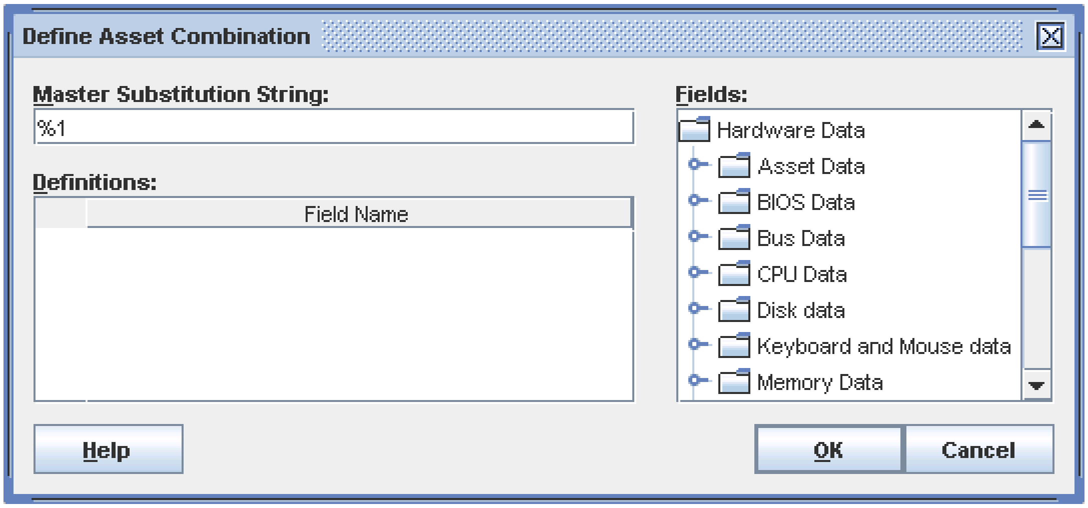
Setting up a Combination Field

Combination fields can combine up to five asset or hardware fields into a single field. This is particularly useful for the description field.

The combination field is made up by string substitution.

To set up a combination field:

1 After you have selected a **Combination** field as the data field type, click **Change**.



Define Asset Combination

Master Substitution String: %1

2 Assign a **Master substitution string** by typing the template string in the box. The convention is to use percentage signs followed by a number. For example, '%1 (%2)'

3 The **Definitions** box lists the fields that have been defined for use in the substitution string.

4 To add a field to the **Combination** field, select either the **Asset** or **Hardware** field option and the available fields will be listed in the **Definitions** box.

5 To clear an entry select the **Delete** command from the right-click menu or press the **Delete** key.

6 In the **Definitions of %1 to %5** grid, build up a list of up to five index entries (represented as %1, %2, %3, %4 and %5).

7 Click in a row in the grid and from the Fields tree select the asset or hardware item that is to be associated with the index. The asset or hardware field will now appear in the **Field/ Description** column.

8 Continue this for up to five index entries.

9 Define a master substitution string which replaces the percent values (for example, %1) with the appropriate hardware or asset item. An example of a master substitution string is shown in the next section.

10 You can also specify some text before or after the percent notation which will be a constant part of the value of the field.

11 Click **OK** to return to the **Asset Field configuration** dialog box.

12 Click **OK** to return to the asset entry form.

Example of a Master Substitution String

If the master substitution string %1 %2MHz %3Mb is defined for the Description field in the asset entry form, where the following index definitions apply:

Table 30 Example of a Master Substitution String

Index	Field/Description	Display
%1	CPU Data\CPUs\CPU Type	CPU Type
%2	CPU\CPUs\CPU Speed (MHz)	CPU SpeedMHz
%3	Memory Data\Total memory (Mb)	Total MemoryMb

The **Description** field may look as follows:

```
Pentium II, 333MHz, 128Mb
```

Setting up a WMI Extract Field

Some data on Windows operating systems is only available via the WMI interface. This type of field allows the scanner to be configured to extract and store specific pieces of WMI data. The Windows scanner will populate this field on computers where WMI is enabled.

Windows Management Instrumentation (WMI)

Windows Management Instrumentation (WMI) is a component of the Microsoft Windows operating system that provides management information.

WQL

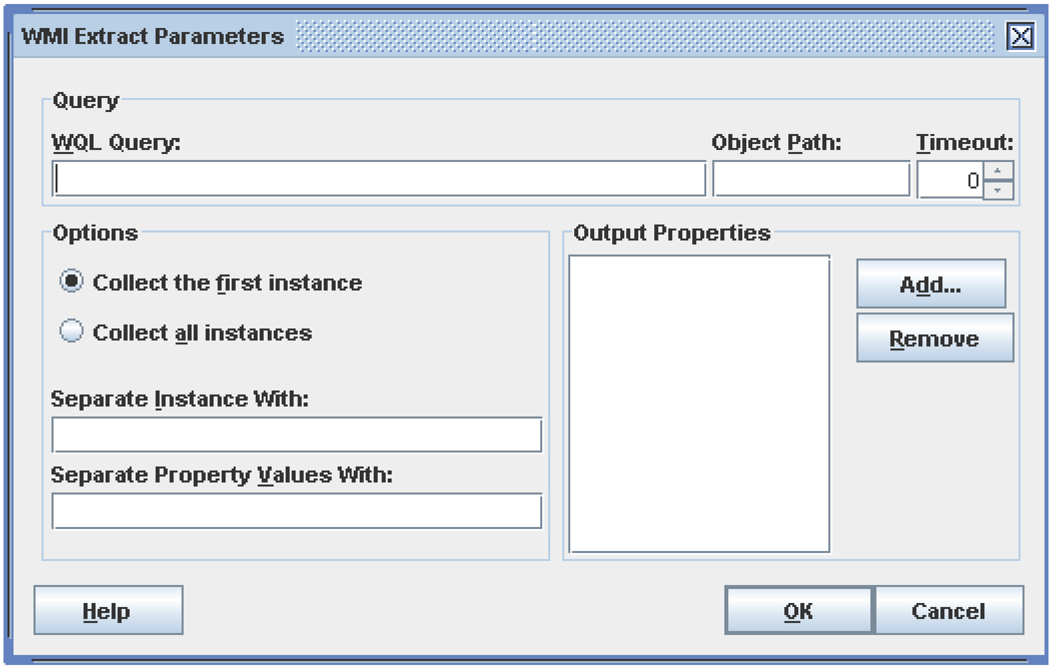
Windows Management Instrumentation Query Language (WQL) is a subset of SQL that is used to make data queries inside WMI.

Further Information

For further information about WMI and WQL refer to the Microsoft MSDN web site.

To set up a WMI extract field:

1 After you have selected a **WMI Extract field** as the data field type, click **Change**.



2 Enter the WQL query. For example:

```
select Name,CurrentClockSpeed from Win32_Processor
```

The above query collects the name and the frequency properties of the installed processor.

3 Enter the **Object Path**

The Object Path should usually be:

```
root\cimv2
```

This is the default path for CIM v2 data provided by WMI.

4 Enter the **Timeout** - This specifies the number of seconds to wait until the query returns a single instance of the queried data. If no data is returned within this period, the query will return nothing and the value of the field will be blank.

You can use **-1** to wait indefinitely for the query to return data. However, this is not recommended since it may cause the query to hang.

5 Enter the **Output Properties**

These are properties whose value is required in the asset field. The WQL query returns an instance of the WMI class which can have many properties. The required ones need to be specified manually.

For example:

```
select * from Win32_Processor
```

This will return all properties for processor, but if Name is required, it should be specified in the **Output Properties** list box.

6 Specify any Options

Collect First Instance and **Collect all Instances**

These options specify whether the first returned instance or all returned instances should be used.

For example, if there are several processors in a computer you can choose to have the information about the very first processor or have the information about all processors.

If all instances are requested, their values will be separated with the string specified in the Separate instances with field.

When multiple properties are specified, the values returned by the query will be separated with the string specified in the Separate property values with field.

7 Click **OK** to return to the **Asset Field configuration** dialog box.

An Example WQL Extract Field Setup

Table 31 An Example WQL Extract Field Setup

Options	Entry
WQL Query	select Name,CurrentClockSpeed from Win32_Processor Object Path: root\cimv2
Timeout	10
Properties	Name, CurrentClockSpeed
Options	Collect all instances Separate Instances with ; Separate property values with ,

When executed on a computer with 4 CPUs it produces the following output in the WMI Extract asset field:

```
Intel(R) Xeon(TM) CPU 2.80GHz,2790; Intel(R) Xeon(TM) CPU 2.80GHz,2791;
Intel(R) Xeon(TM) CPU 2.80GHz,2791; Intel(R) Xeon(TM) CPU 2.80GHz,2791
```

If only the first instance is requested, this will be the value:

```
Intel(R) Xeon(TM) CPU 2.80GHz,2790
```

Step 7: Setting Extract Options

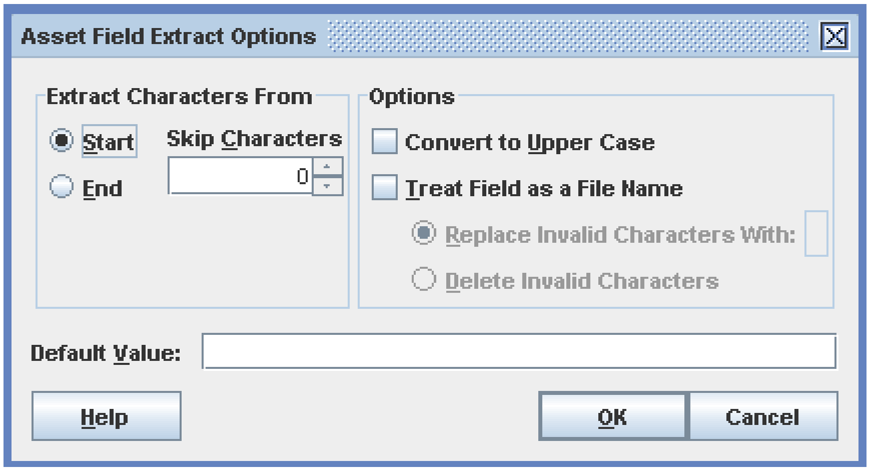
All calculated asset fields defined can be set up so that only part of the string is selected instead of the entire string. They can also be set up, for example, to use the last part rather than the first part of the string. This can be useful for obtaining the last part of an calculated field that is too long.

Various other settings for manipulating the field contents are also available.

To set extract options:

1 After you have selected the field data type, click **Extract**. The button is only enabled for those field that are calculated. This option is not available for user-entered fields.

The **Asset Field Extract Options** dialog box is displayed.



Asset Field Extract Options

Extract Characters From

● Start

○ End

Skip Characters: 0

Options

□ Convert to Upper Case

□ Treat Field as a File Name

● Replace Invalid Characters With:

○ Delete Invalid Characters

Default Value:

2. In the **Extract characters from** group box, specify whether you want to use the last part or the first part of the string. Select one of the following options:
3. **Start** Uses the first part of the string. Use the arrows next to the **Skip characters** box to specify how many characters are to be skipped from the beginning of the string.
4. **End** Uses the last part of the string. Use the arrows next to the **Skip characters** box to specify how many characters are to be skipped from the end of the string.

   For example, 'ABCDEF123' If you select End and skip 4 characters, then the result will be ABCDE.
5. In the **Options** group box, select the options as follows:
6. **Convert to upper case** Select this option to convert the alphabetic characters to upper case, if required.
7. **Treat field as File Name** Select this option to treat the string in the asset field as a file name.

   Some characters are invalid in file names, so any invalid characters can be replaced with the character specified in the Replace invalid characters with box. For example, underscore '_' is a valid file name character and can be used to replace invalid characters.

   If you select the **Delete invalid characters** option then any invalid characters will be deleted.
8. If the extracted field is empty or is not found, then a default value for the string can be specified in the **Default Value** box. For example, if the text string **Not Found** is entered in this box, then an empty field or a field that has not been found will be assigned this default value.

Step 8: Correcting the Order of the Fields in the Form

You will need to consider the order of the fields in the form and move them round accordingly. The rule is:

A field cannot depend on a field that is placed below it in the form.

That is, if you have set up any derived or automatic fields that require data from fields below them in the form, you will have to move them to a position in the form that is above these fields.

To correct the order of the field in the form:

1 Re-order the fields by clicking on a row and dragging the selected line to its new location in the form.

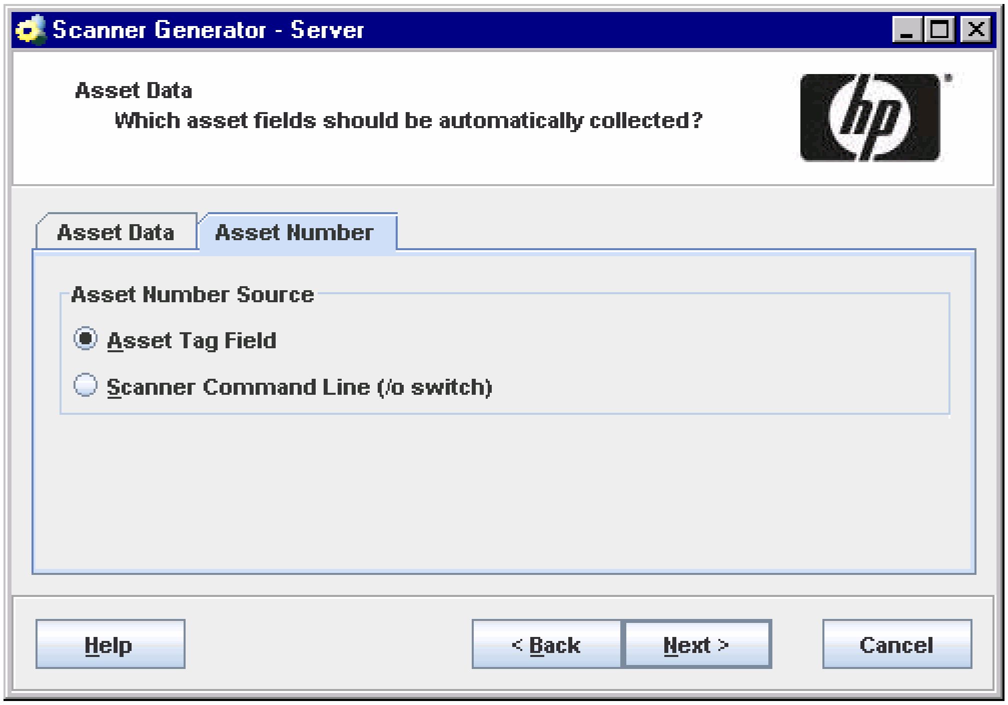
2 When you click **Next** in the **Asset Data** page, a confirmation message may be displayed.

3 Click **Yes** to have the Scanner Generator automatically do this for you.

4 Click **No** to do this manually.

Asset Number Tab

The **Asset Number** tab is used to set options for managing the asset number used to uniquely identify a machine.



Scanner Generator - Server

Asset Data

Which asset fields should be automatically collected?

Asset Number Source

● Asset Tag Field

○ Scanner Command Line (/o switch)

Asset Number Definition

Each computer that is scanned needs to be identified by a unique tag known as the **Asset Tag**.

Asset tags are generally assigned to allow each hardware item to be recorded and identified in an asset management tool, such as AssetCenter. The conventions used depend on the numbering system and asset registering policies adopted by your organization. Ensure that your asset numbers can be reconciled between DDM Inventory and AssetCenter.

In Enterprise Mode, the Asset Tag is also available for display in the Device Manager, just as it can be used for performing a “Find”. The Asset Tag is used to identify each asset. In all reports, the Asset Tag is used to identify each asset.

Source for Asset Number

In Enterprise Mode the options for selecting the source for asset number source are disabled. The source is always from the **Asset tag** field. This option will use the value in the Asset Tag field that was created in the Asset Data tab page. This is usually used as the unique key to identify each computer. When this (the default) is selected and an offsite scan file will be saved, an Asset Tag field must be defined in the Asset Data tab.

If you chose to deploy the scanner manually in Manual Deployment Mode you will need to configure this yourself as follows:

To specify how the Asset Tag identifying the machine is chosen:

Select one of the following to use as the source for the asset number:

- **Asset Tag Field:**

  This option will use the value in the Asset Tag field that was created in the Asset Data tab page. This is usually used as the unique key to identify each computer. When this (the default) is selected and an offsite scan file will be saved, an Asset Tag field must be defined in the Asset Data tab.

- **Scanner Command Line (/o switch):**

  An offsite scan file name can also be specified by the -o: command line option. This overrides the scan file name (as well as the path, if specified).

  To configure this:

  Select the **Scanner Command Line (/o)** option. The scan file name is taken from the command line. This is entered using the /o: command line option when the scanner is started, using the name specified. For example,

  ```
  Scanwin32-x86 -o:FP00017
  ```

Scanner Options Page

The **Scanner Options** page is used to set options for controlling the behavior of the scanner during the usual scanning process and under exception conditions, as well as options for saving the inventory results.

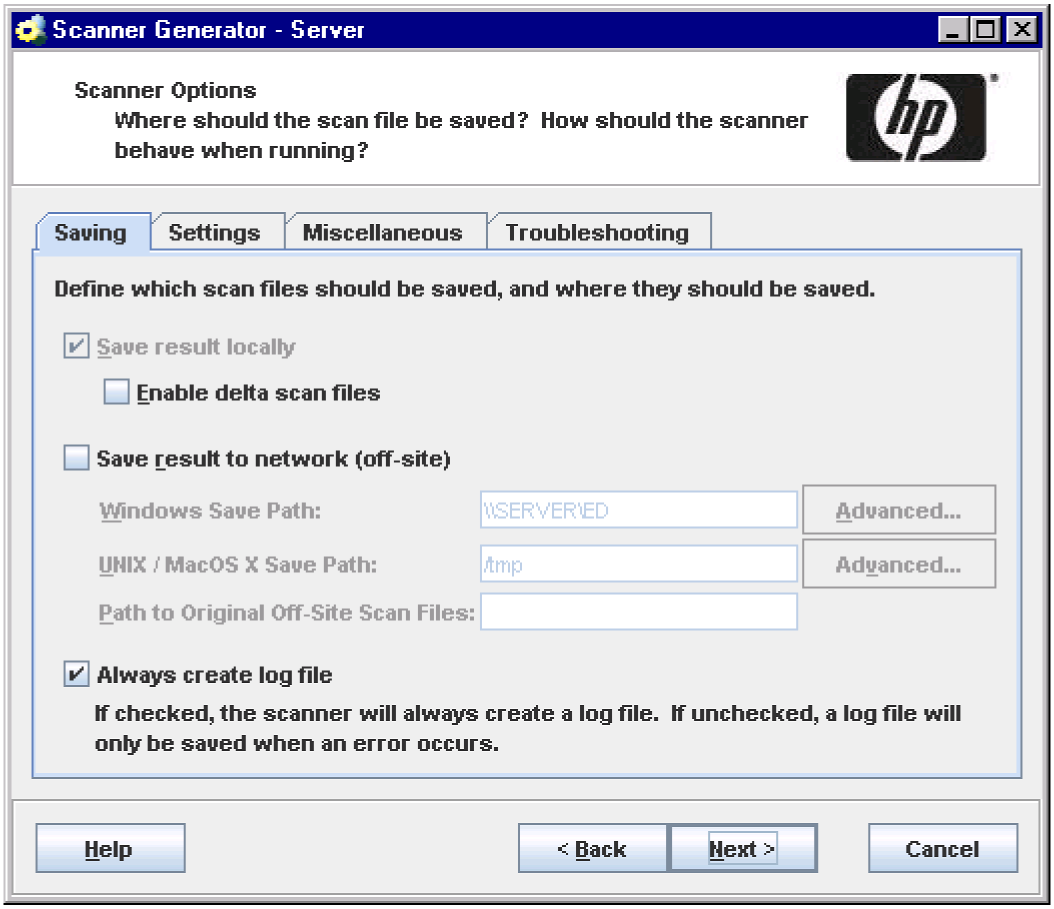
The **Scanner Options** page has four tabs:

- Saving Tab
- Settings Tab
- Miscellaneous Tab
- Troubleshooting Tab

After the options have been selected as required, click **Next** to continue.

Saving Tab

The **Saving** tab page is used to set options for saving the inventory results.



Scanner Options

Where should the scan file be saved? How should the scanner behave when running?

Define which scan files should be saved, and where they should be saved.

☑ Save result locally

□ Enable delta scan files

□ Save result to network (off-site)

Windows Save Path: \\SERVER\ED

UNIX / MacOS X Save Path: /tmp

Path to Original Off-Site Scan Files:

☑ Always create log file

If checked, the scanner will always create a log file. If unchecked, a log file will only be saved when an error occurs.

➤ For **Enterprise Mode** some of the options are pre-set to optimal values and cannot be changed.

Saving Local and Offsite Scan Files

The scanners can save two scan files per scan:

- Local scan file - Saved to a local directory.
- Offsite scan file - Saved to a specified output directory, with its name being derived from the value in the Asset Tag field specified as the asset number.

The saving of local scan files cannot be disabled in Enterprise Mode (the option is on and is greyed out).

In Manual Deployment Mode both of these scan files (local and offsite) are saved by default, however, one or the other can be disabled.

Saving Results Locally

The **Save results locally** option determines whether the scan file is saved to the local machine.

The local scan file is always called **local$.xsf**.

The Windows scanner uses the `Peregrine\Discovery` subdirectory of the application data directory of all users. The location of this directory varies. For example, on Windows XP installed on `C:\`, it could be:

```
C:\Documents and Settings\All Users\Application Data\Peregrine\Discovery
```

Enabling Delta Scanning

The **Enable delta scan files** option enables/disables this feature. It can only be enabled if a local scan file is saved. When delta file scanning is enabled, the scanner first saves the complete scan file copy offsite by copying the local scan file.

Instead of sending a full scan file to a server after every scan, the scanners calculate the difference (the delta) between the last full scan and the current one - and transfer just this data. This can dramatically reduce the amount of network bandwidth used when using DDM Inventory. By default delta scanning is enabled.

The XML Enricher re-assembles the full scan files based on the previous scan and the delta scan. No other DDM Inventory component uses the delta scan file. The re-assembled scan can however, be used in Viewer and Analysis Workbench. See the section about the "Delta Command Line Utility" in the *XML Enricher* chapter of the *Configuration and Customization Guide* for a description of a standalone utility that can be used to manipulate delta scan files.

Setting up the Scanner to Handle Delta Scan Files Correctly (Manual Deployment Mode Only)

In Manual Deployment Mode for the delta scan file processing in the XML Enricher to work correctly, ensure that you do the following:

1. Configure the scanner to save results to the XML Enricher incoming directory. This directory can be found in the following location on the DDM Inventory Server by default:

   ```
   C:\Documents and Settings\All Users\Application
   Data\Hewlett-Packard\DDMI\Scans\incoming
   ```

   Create a share on the DDM Inventory Server to share this disk and specify its UNC path in the Save result to network (off-site) field on this page. See the next section for more information about off-site saving.

2. Set the **Path to original off-site scan files** to the **Original** directory. This directory can be found in the following place by default:

   ```
   C:\Documents and Settings\All Users\Application
   Data\Hewlett-Packard\DDMI\Scans\original
   ```

   Create a share for this directory and specify its UNC location in the **Path to original off-site scan files:** field to do this. The format for the UNC path is:

   ```
   \\Servername\ShareName\path\
   ```

   For example:

   ```
   \\DDMIServer\Inventory\Scans\
   ```

Saving Results to Network (Offsite)

The **Save result to network (off-site)** option saves the scan file to remote (offsite) disk (such as floppy disk or network drive).

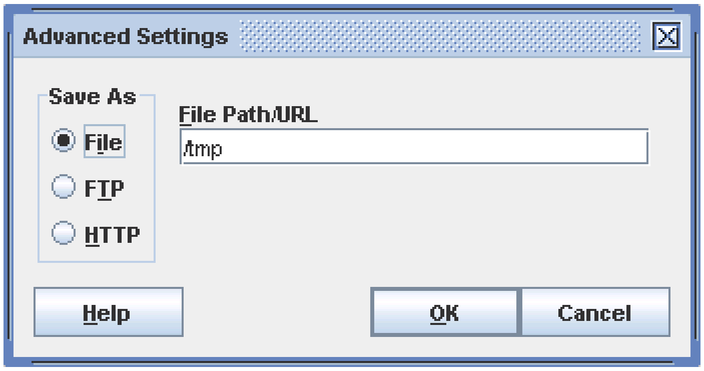
The **Offsite Save Path** can take the following four types of values:

- Normal File Path
- UNC Path
- FTP URL
- HTTP URL

Normal File Path

To save to a normal file path:

1 Click **Advanced**.



Save As: ● File ○ FTP ○ HTTP

File Path/URL: /tmp

2 Select the **File** option and enter the path in the **File Path/URL** field.

The full path name (beginning with the drive letter) must be specified in the PC Save Path or Unix Save Path box. For example:

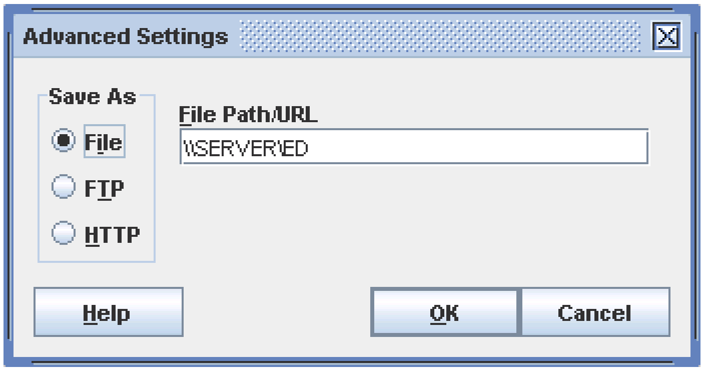
```
c:\Inventory\Scans
```

UNC Path

A UNC path can be entered as the offsite save path.

To save to a UNC path:

1 Click **Advanced**.



Save As: ● File ○ FTP ○ HTTP

File Path/URL: \\SERVER\ED

2 Select the **File** option and enter the **UNC path** In the **File Path/URL** field.

The format for the UNC path is:

```
\\servername\sharename\path\
```

For example:

```
\\DDMIServer\DDM Inventory\Scans\
```

The specified UNC path must have write access. Do not specify a file name here.

The offsite save location can be overridden by using the -p: or /p: command line option. For example:

```
Scanwin32-x86 -p:C:\Scanners\
```

A UNC path can also be entered as the argument to this option. The format for the UNC path is:

```
\\servername\sharename\path\
```

For example:

```
Scanwin32-x86 -p:\\DDMIServer\DDM Inventory\Scans\
```

In Windows, if the UNC name specified is visible to the machine, the scan file will be saved to the specified location, even if it is not mapped to a drive letter.

On UNIX and Mac OS X machines, the UNIX/Mac OS X save path is used instead, allowing UNIX-style syntax for specifying directories to be used. On UNIX/Mac OS X, do not use drive letters, and the save path must instead start with '/' (root) and point to a directory writable by the scanner.

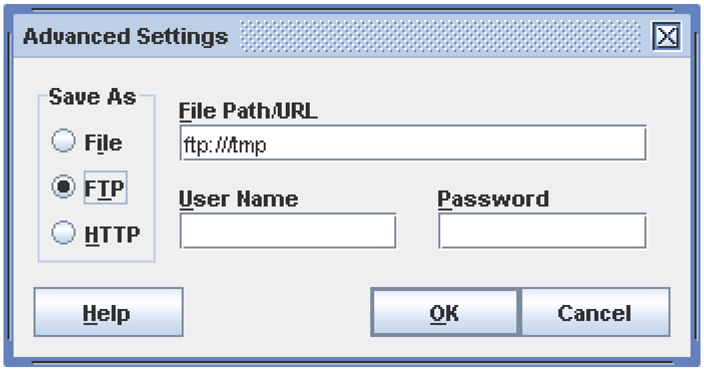
3 Click **OK** to return to the **Savings** tab page.

FTP URL

The scanners can save to any FTP server.

To save to an FTP server:

1 Click **Advanced** to display the **Advanced Settings** dialog.



Advanced Settings

Save As

○ File

● FTP

○ HTTP

File Path/URL: ftp://tmp

User Name:

Password:

2 Select the **FTP** option.

Extra fields are displayed.

3 Enter the FTP path and enter a User Name and Password if one is to be supplied.

4 Click **OK** to return to the **Savings** tab page.

When an FTP location is specified with the `-p` scanner command line option, the User Name and Password can be encoded into the URL as follows:

ftp://user:password@host:port/dir

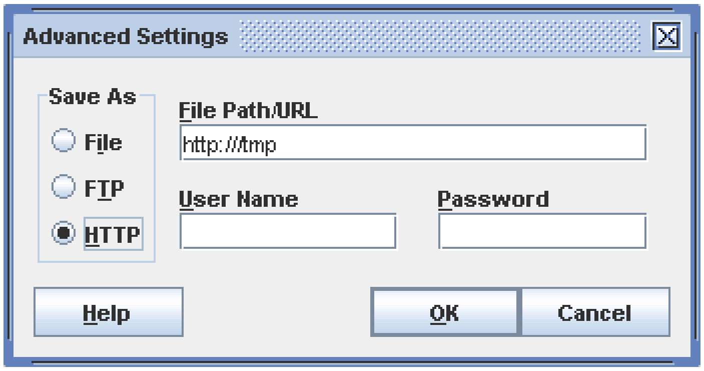
For detailed information, refer to the description of `-p:<path>` in the Scanners section in the *Reference Guide*.

HTTP URL

The scanners can save to an HTTP server if one has been configured to allow writing to a particular directory.

To save to an HTTP server:

1 Click **Advanced** to display the **Advanced Settings** dialog.



Save As: ○ File ○ FTP ● HTTP

File Path/URL: http://tmp

2 Select the **HTTP** option.

Extra fields are displayed.

3 Enter the HTTP path and enter a User Name and Password if one is to be supplied.

4 Click **OK** to return to the **Savings** tab page.

If the `-p` scanner command line option is used with an HTTP location, ensure that the location is not password protected. If the User Name and Password is required with HTTP saving, specify it using the setting in the Advanced Settings dialog. The `-p` switch should not be used in this case.

For detailed information, refer to the description of `-p:<path>` in the Scanners section in the *Reference Guide*.

HTTP Saving for Apache and IIS Web Servers

The Web Server needs to be configured to allow execution of the Put command. Usually, by default web servers are set to enable Post and Get commands. You will need to ensure that if you are using HTTP saving that the Put command is enabled in the directory.

The following is a quick description of what you would have to enable for HTTP saving on both IIS and Apache.

Setup of Apache 2.0

If you are using basic authentication:

In the bin directory run:

```
htpasswd -c "<path>\htpass" Username
```

You will need to put the following in the .htaccess file of the directory that you intend to save in:

```
PUT_EnablePut On

PUT_EnableDelete Off

AuthType Basic

AuthName "Write" AuthUserFile "<path>\htpass"

Require user Username
```

Download the mod_put.so file and put it into the modules directory.

Enter the following into the httpd.conf file:

```
LoadModule put_module modules/mod_put.so
```

Setup for IIS

Check the option that allows writing to the desired save directory. Ensure that you have given write access to the Username and Password that you plan on adding to the scanners http save path.

Setting up the Creation of a Log File

The log file stores progress messages for scanner hardware detection, indicates what directory data is scanned, how long the software scanning took, and contains the status of the scan file saving.

To set up the creation of a log file:

Check the **Always Create Log File** option.

A log file is always created if this option is selected (which indicates the successful completion of the scan if no errors are encountered).

Otherwise, a log file is only created if an error is encountered.

Depending on the saving options chosen, the log file is saved to the following locations:

- The same location as the local scan file.
- The same location as the offsite scan file (if an offsite location has been specified).
- In the scan file itself (as a stored file).

The name given to the log file is the same as the name of the scan file. For example, if the scan file is called:

```
XSF014.xsf
```

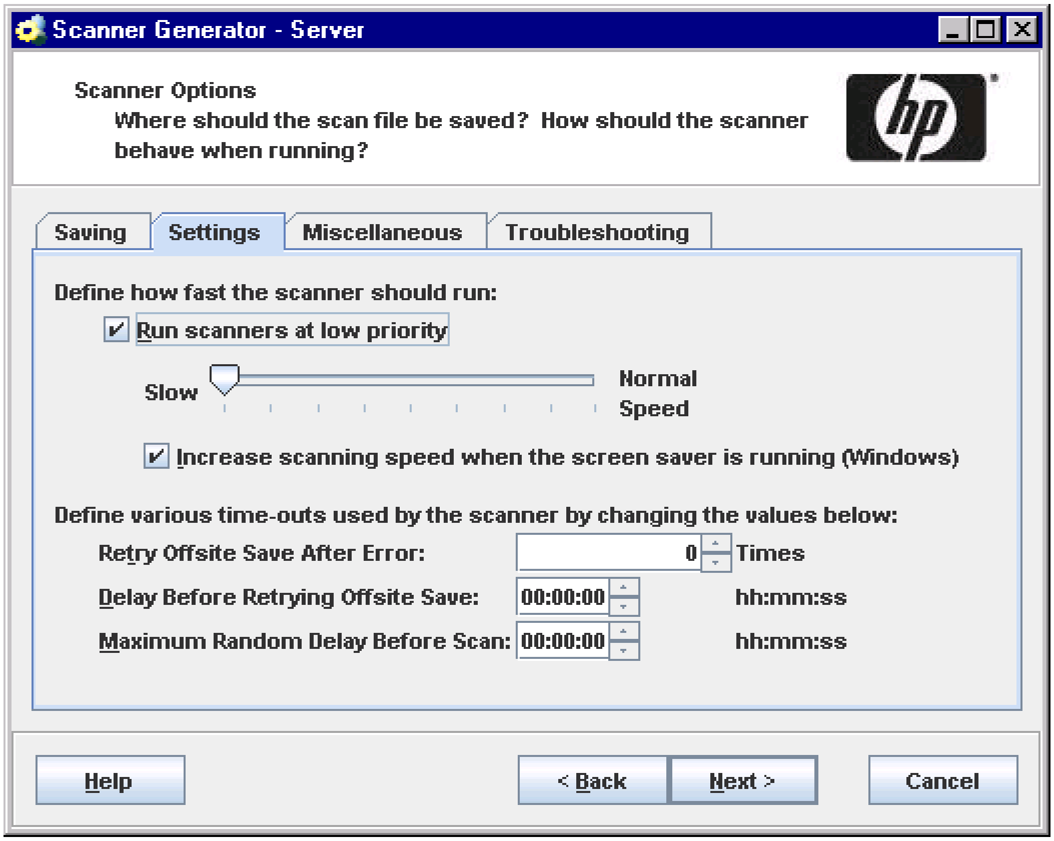
Then the log file generated will be called:

```
XSF014.log
```

➤ The log file is not stored with the offsite scan file if the offsite scan is saved to an FTP or an HTTP location.

Settings Tab

The options on **Settings** tab of the Scanner Options page are used to control the behavior of the scanner as it scans each computer.



Scanner Options

Where should the scan file be saved? How should the scanner behave when running?

Define how fast the scanner should run:

☑ Run scanners at low priority

☑ Increase scanning speed when the screen saver is running (Windows)

Define various time-outs used by the scanner by changing the values below:

Retry Offsite Save After Error: 0 Times

Delay Before Retrying Offsite Save: 00:00:00 hh:mm:ss

Maximum Random Delay Before Scan: 00:00:00 hh:mm:ss

These options are used for controlling the behavior of the scanner as it scans each computer and how it interacts with users.

By default the scanner is made to run with the lowest priority but will go to full speed when the screen saver is active.

Defining How Fast the Scanner Should Run

To set user interaction options for the scanner, select from the following:

- **Run scanners at low priority**

  The scanners can be set to run at slower than normal speed, so that they do not impact on the users work.

  Use the slider control to specify how slow or how fast the scanner will run. A further option is enabled.

- **Increase scanning speed when the screen saver is running (Windows)**

  This option will allow the scanner to run at an increased speed when a screen saver is enabled. When this setting is checked, the scanner runs slower. It increases its speed to normal when it detects that the screen saver is running. As soon as the screen saver disappears, the scanner runs slower again.

When the option to run at low priority is checked, the PC-based scanners allocate CPU resources less aggressively and wait much longer between each file scanned. In UNIX and Mac OS X, the scanner performs a re-`nice` of itself to run at a lower priority.

Setting Time-Out Options

These options set scanner time-out settings.

To set up the timer options, select the options as required:

- **Retry Offsite save after error**

  The scanner will attempt to retry the offsite scan file saving if an error occurs the number of times specified here.

- **Delay before retrying offsite save**

  The scanners will wait for the time specified here before retrying the offsite scan file saving if an error previously occurred in this process.

- **Maximum random delay before scan**

  This setting is applicable to the Windows scanner only. The scanner can wait for the amount of time specified here before doing anything on the machine. The default setting for this is 00:00:00 with a maximum allowed value of 23:59:59

If the scanner is launched via a login script, using this option allows the saving of scan files to be spread over a longer period to avoid overloading the network at busy periods. For example, in the morning when all users come to work, power up their computers and start the scanners at approximately the same time.

Miscellaneous Tab

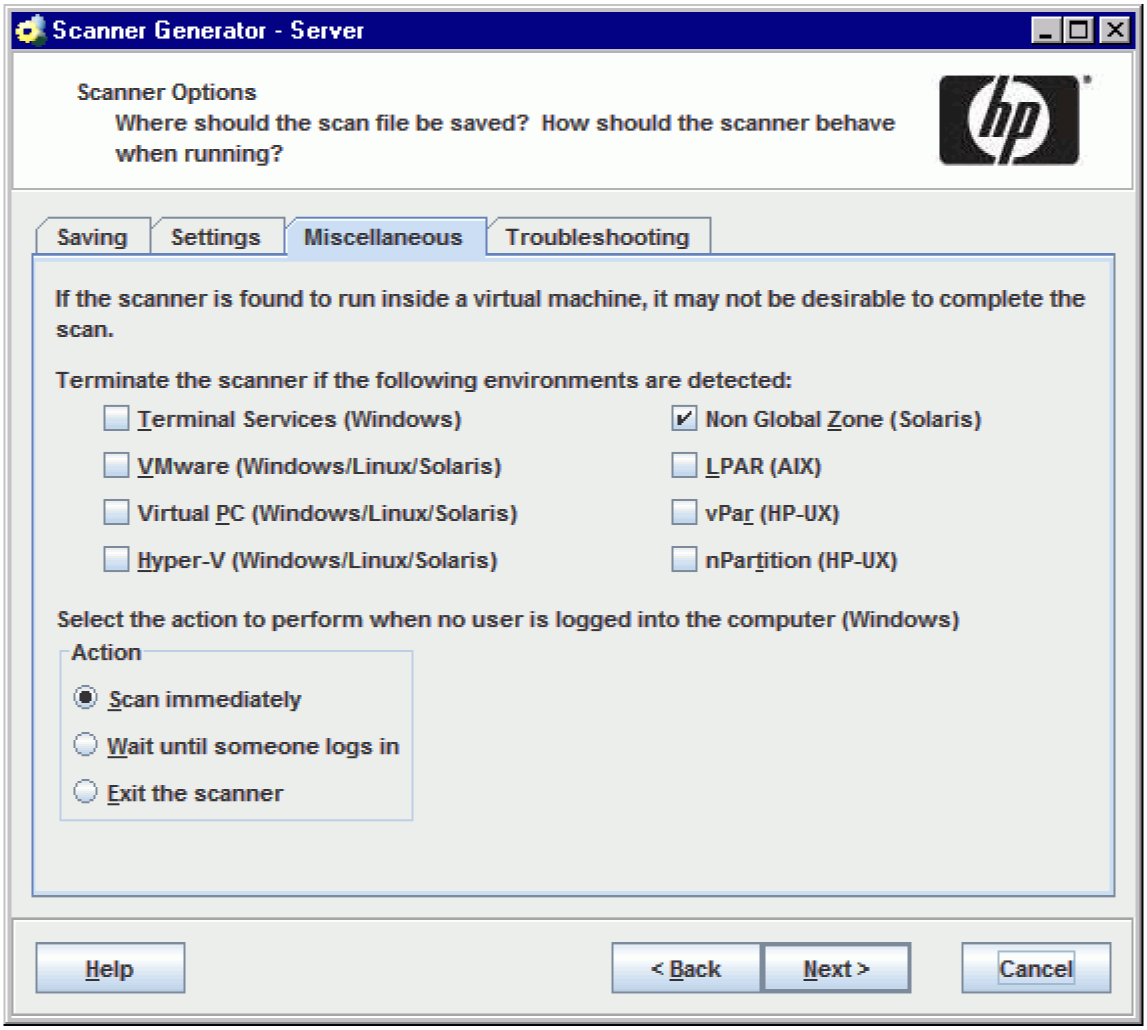
The **Miscellaneous** tab allows you to:

- Terminate the scanners if running in a virtual machine
- Set the behavior when a user is not logged into a computer.

Virtual Machines

When the scanner is run inside a virtual environment, you may not want a full software scan to take place, because this would scan the server for every client.

Settings on the **Miscellaneous** tab can instruct the scanner to exit without doing any processing with a special error level 20, allowing a script that launched the scanner to handle this situation and launch another scanner tailored for the virtual environment if required.



Scanner Generator - Server

Scanner Options

Where should the scan file be saved? How should the scanner behave when running?

If the scanner is found to run inside a virtual machine, it may not be desirable to complete the scan.

Terminate the scanner if the following environments are detected:

□ Terminal Services (Windows)	☑ Non Global Zone (Solaris)
□ VMware (Windows/Linux/Solaris)	□ LPAR (AIX)
□ Virtual PC (Windows/Linux/Solaris)	□ vPar (HP-UX)
□ Hyper-V (Windows/Linux/Solaris)	□ nPartition (HP-UX)

Select the action to perform when no user is logged into the computer (Windows)

Action

● Scan immediately

○ Wait until someone logs in

○ Exit the scanner

Select the virtual environment(s) for which you want the scanner to terminate. If detected:

- Terminal Services (Windows scanner only): The scanner is going to exit without doing a scan if launched within a Windows terminal services session.
- VMware (Windows, Linux, and Solaris x86 scanners): The scanner terminates if launched within a VMware virtual machine.

- Virtual PC (Windows, Linux, and Solaris x86 scanners): The scanner terminates if launched within a Virtual PC's virtual machine.
- Non Global Zone (Solaris scanner only): The scanner terminates without doing a scan if launched in a non global zone on the Solaris operating systems supporting zones.
- Hyper-V (Windows, Linux, and Solaris x86 scanners): The scanner terminates without doing a scan if launched within a Microsoft Hyper-V's virtual machine.
- LPAR (AIX scanner only): The scanner terminates without doing a scan if launched in an LPAR partition on the AIX operation systems.
- vPar (HPUX scanner only): The scanner terminates without doing a scan if launched in a vPar partition on the HP-UX operation systems.
- nPartition (HPUX scanner only): The scanner terminates without doing a scan if launched in an nPartition partition on the HP-UX operation systems.

Setting Actions when a User is Not Logged into the Computer

This option is for the Windows scanner only.

Enterprise Mode

The scanner is launched via the DDM Inventory agent. The agent itself runs as a Windows service under the LocalSystem account. However, the scanner always tries to impersonate the account of the currently logged in user in order to collect the required network, environment, and other configuration information for the user. This setting specifies the scanner behavior when no user is logged in at the time the scan is scheduled:

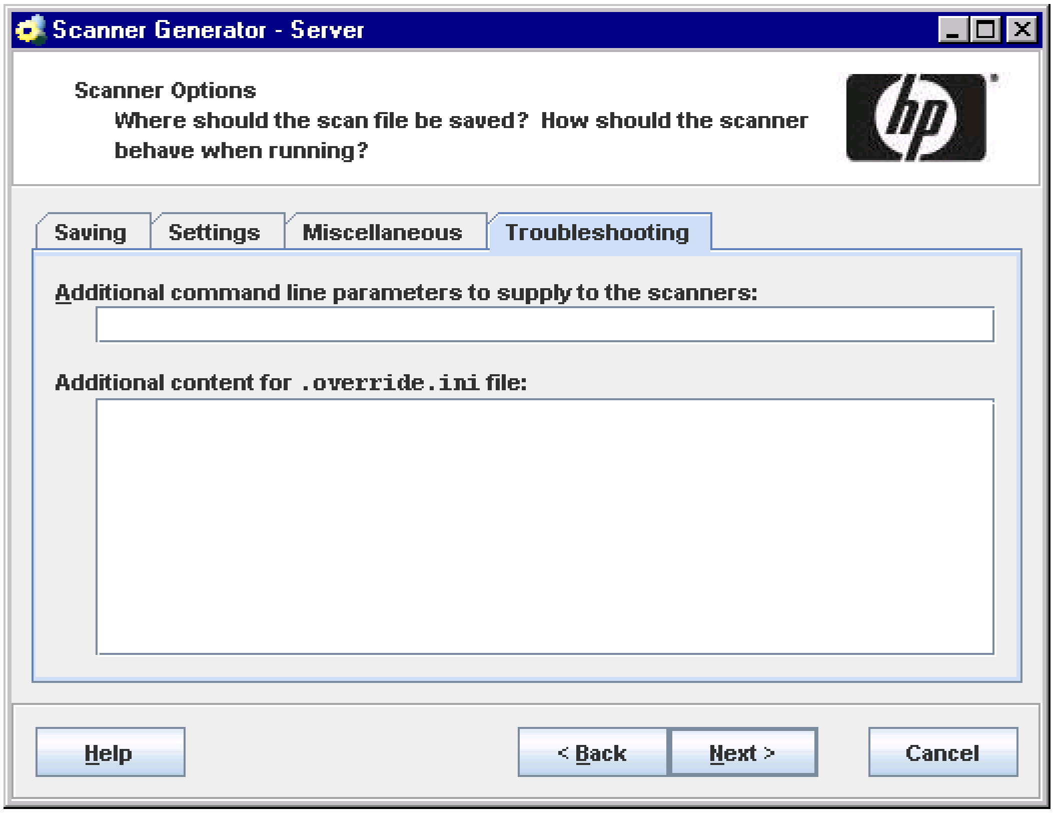
- **Scan Immediately:** Forces the scanner to run under the local system account. However, it will not be able to collect the environment information for a particular user. The environment settings for the local system account will be detected. Also any program running under the local system account does not have access to network resources, so the scanner will not be able to access any files or directories on the network.
- **Wait until someone logs in:** This instructs the scanner to wait until an interactive user logs into the system. When this is detected, the scanner impersonates this user and executes using this user's account. This allows the scanner to collect environment information for the user. However, this setting is not suitable for standalone servers where interactive users rarely log in.
- **Exit the scanner:** The scanner simply exits without scanning the computer.

Manual Deployment Mode

The scanner runs under the account of the currently logged in user, so normally these settings do not apply. They may only take effect when the scanner is launched by a software distribution tool that can run it under the LocalSystem account. In this case, the above logic for Enterprise Mode applies.

Troubleshooting Tab

The **Troubleshooting** tab is used to set up additional troubleshooting options for the scanners.



Scanner Generator - Server

Scanner Options

Where should the scan file be saved? How should the scanner behave when running?

Additional command line parameters to supply to the scanners:

Additional content for .override.ini file:

Additional Command Line Parameters to Supply to the Scanner

You can specify additional content for the override files here. Although the options for the scanner are normally set using the Scanner Generator, it may be necessary to change some settings to allow better operation on some machines. The operation of a scanner can be modified with the use of the various command line parameters.

Additional file scanning configuration specified in the `override.ini` (Windows) file and the `.override.ini` file (UNIX/Mac OS X) can be entered in this field. The content specified here is processed by the scanner before processing the content of the override file (if available on the system where the scanner runs).

Override Files

You can override the settings of the file systems, directories and files during the software scanning process by specifying additional settings in the override file. As indicated, on Windows systems, the name of this file is `override.ini`. On UNIX and Mac OS X systems, the name of this file is `.override.ini`. The override file must be located in the same directory as the scanner executable.

File Systems

Because it is always possible, particularly on UNIX and Mac OS X systems, that some file systems are not in the list, you can create a file where you can specify any additional names of file systems that you want to include or exclude during scanning.

You can also specify names of existing file systems in case you want to change the inclusion/ exclusion of such file systems after the scanner has been generated.

The format of the file is as follows:

```
[include]

fs=<name of a file system>

[exclude]

fs=<name of a file system>
```

There can be several “fs” entries in each section.

For example, to ensure that all `afs` mount points are scanned, and that `nfs` and `swap` volumes are not, create the override file with the following contents and place it in the same directory as the scanner prior to running:

```
[include]

fs=afs

[exclude]

fs=nfs

fs=swapfs
```

➤ The name of the file, the sections and the files systems are case-sensitive.

➤ For the feature to work correctly, the override file must be present in the directory in which the scanner resides.

Directories and Files

The override file can also be used to exclude specific directories or files from being scanned without regenerating the scanner.

➤ Files can only be excluded; they cannot be included.

To make use of this file, add one or more

```
dir = <name>
```

or

```
file = <name>
```

entries to the `[exclude]` section of the override file. Excluded directory names must be fully qualified. Excluded file names can contain wild cards.

Example

```
[exclude]

fs=autofs

dir=/temp
```

```
dir=/etc

file=*.exe
```

When excluding files using the override file, the scanner may still store information about the excluded files in the scan file. Adding file entries to the override file ensures that the file will not be opened for any reason, so no file identification, signatures, or archive processing will happen for excluded files.

Example 1

Exclude a specific file system, two directories and all files with exe extension.

```
[exclude]

fs=autofs

dir=/temp

dir=/etc

file=*.exe
```

Example 2

This runs a scan without software on a Windows machine.

```
[exclude]

fs=FAT

fs=NTFS
```

Example 3 Virus Warning

Since the scanner opens files on the computer, if real-time antivirus software is in operation, it may detect a virus being present in a file.

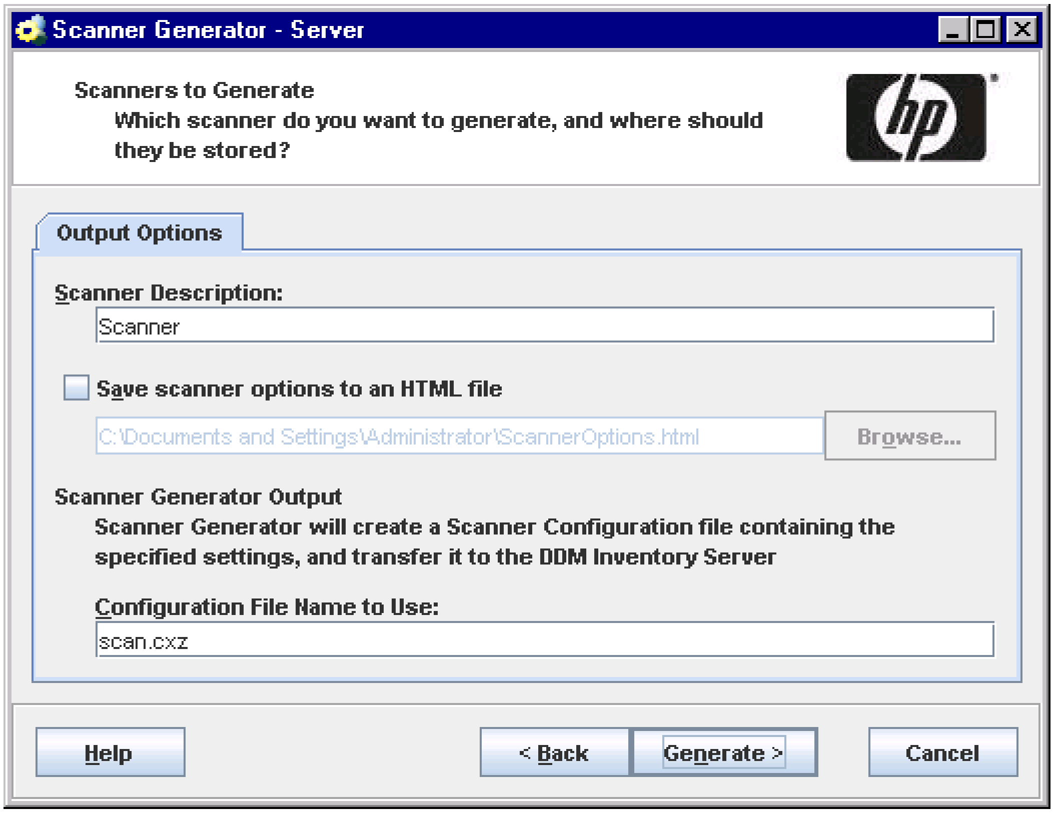
Depending on the virus product being used, actions will have been defined to deal with an encountered virus. Some will try to deal with the problem and immediately disinfect the file. Others will try to move the infected file to a quarantine directory and rename its file extension. In this case, the quarantine directory may be scanned by the scanner later during its scan.

To prevent this from happening, use the override file with *.vir specified for exclusion (where .vir is a typical quarantine file extension). Check the specific virus product to find the extension for this type of file.

Scanners to Generate Page

The **Scanners to Generate** page is used to specify which scanners to generate and where they will be stored.

In Enterprise Mode only the **Output Options** tab will be displayed.



Scanner Generator - Server

Scanners to Generate

Which scanner do you want to generate, and where should they be stored?

Scanner Description: Scanner

□ Save scanner options to an HTML file

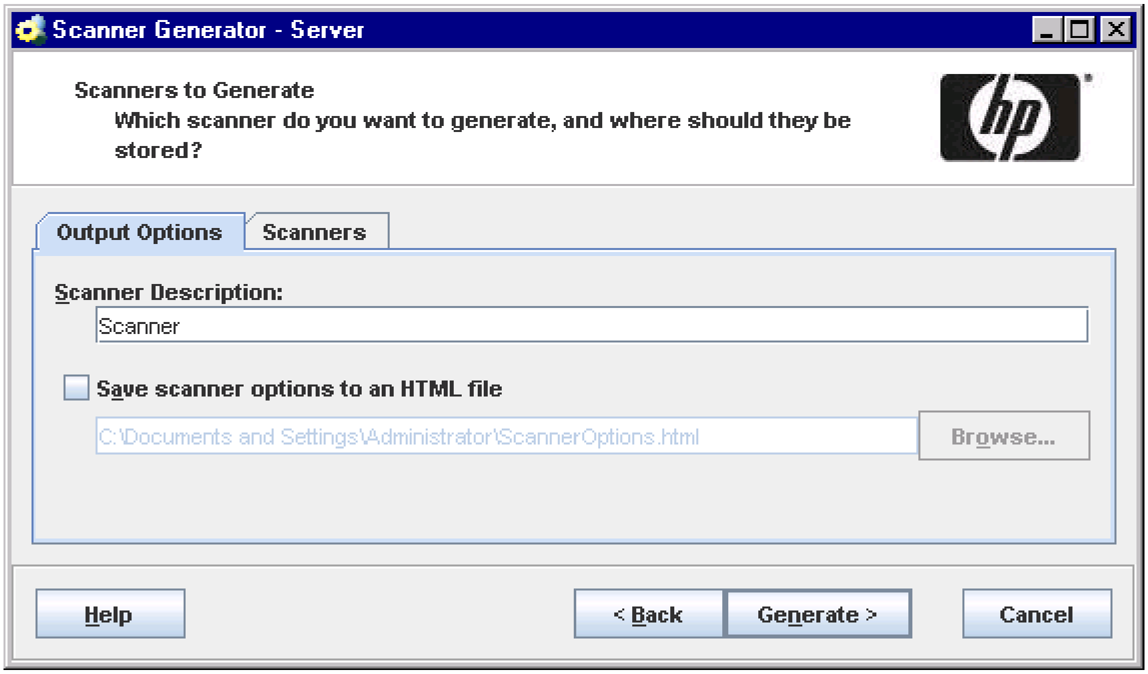
C:\Documents and Settings\Administrator\ScannerOptions.html

Scanner Generator Output

Scanner Generator will create a Scanner Configuration file containing the specified settings, and transfer it to the DDM Inventory Server

Configuration File Name to Use: scan.cxz

In Manual Deployment Mode, both the **Output Options** and **Scanners** tab will be displayed.



Scanner Generator - Server

Scanners to Generate

Which scanner do you want to generate, and where should they be stored?

Scanner Description: Scanner

□ Save scanner options to an HTML file

C:\Documents and Settings\Administrator\ScannerOptions.html

Output Options Tab

The **Output Options** page is used to set up scanner descriptions, save the configuration to an HTML file if required, and, for Enterprise Mode only, name the configuration (`.cxz`) file.

Setting up a Scanner Description

These options allow you to specify the scanner description. You can also optionally produce an HTML file of the scanner selections that you have made.

Having a scanner description is very useful for change control if different scanners are being developed for different circumstances.

It is useful for documentation purposes, to have a file with the scanner's configuration stored in a file. If this step is missed, then load the scanner or a scan file derived from it into Scanner Generator and produce the documentation from this.

To set up a scanner description and save the options to an HTML file:

- In the **Scanner Description** box, enter a description to identify the scanner.

  For example:

  ```
  Standard PC Inventory - July 18, 2007
  ```

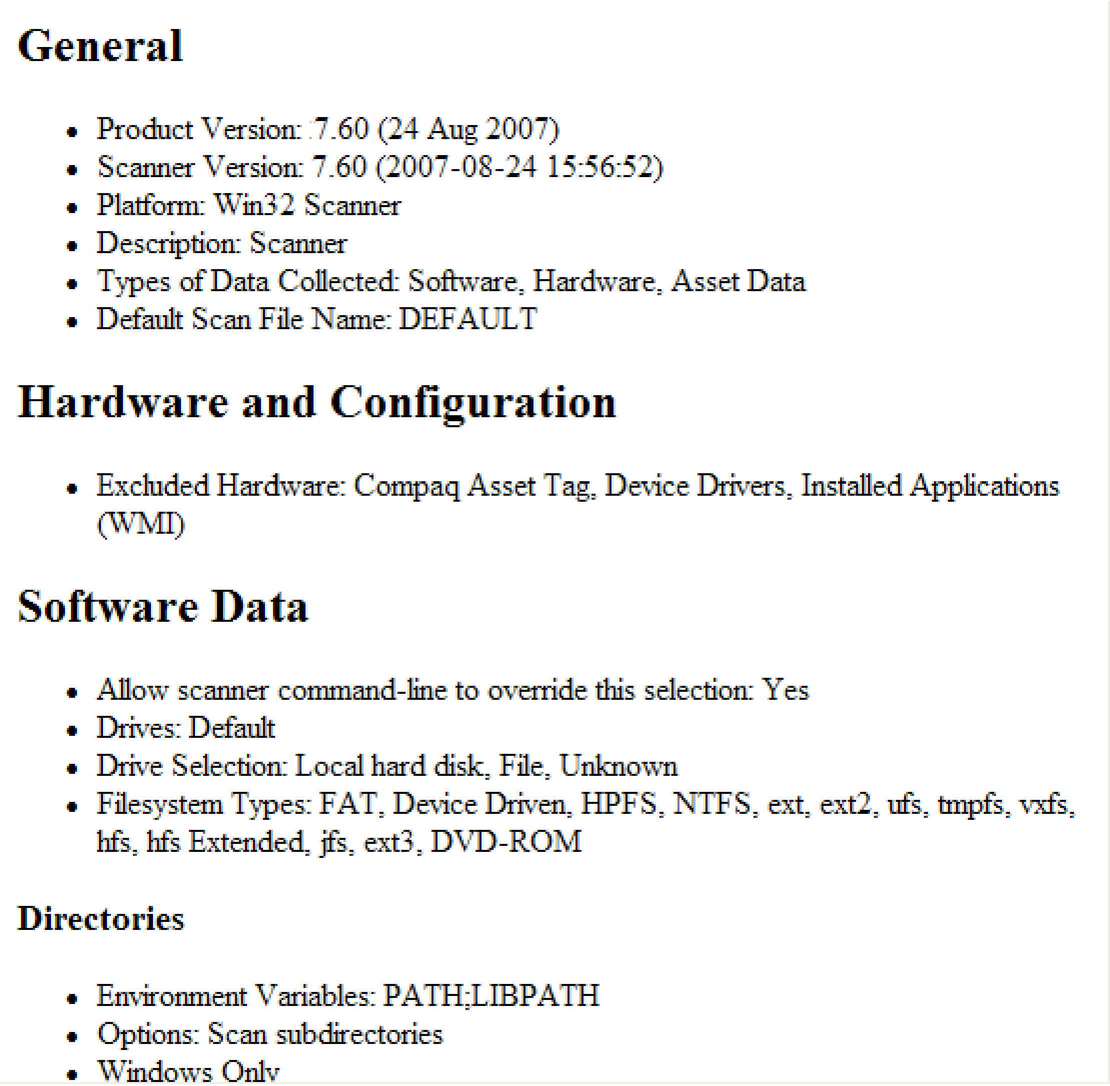
  The scanner description is saved in the scan file as the **hwScannerDescription** hardware field and subsequently in the Discovery Database in the **hwSystemData** table.

Saving Scanner Options to an HTML File

The **Save scanner options to HTML file** box is used to instruct the Scanner Generator to output an HTML file containing a complete listing of all settings defined elsewhere in the program. Select the check box and specify the path and file name to which the scanner options will be saved to. The HTML file cannot be used by the Scanner Generator, but is intended for user/internal documentation purposes.

Example of the ScannerOptions.html File

You can look at a `ScannerOptions.html` file using an Internet browser such as the Microsoft Internet Explorer. The following shows the first few sections that you will find in the file:



General

- Product Version: 7.60 (24 Aug 2007)
- Scanner Version: 7.60 (2007-08-24 15:56:52)
- Platform: Win32 Scanner
- Description: Scanner
- Types of Data Collected: Software, Hardware, Asset Data
- Default Scan File Name: DEFAULT

Hardware and Configuration

- Excluded Hardware: Compaq Asset Tag, Device Drivers, Installed Applications (WMI)

Software Data

- Allow scanner command-line to override this selection: Yes
- Drives: Default
- Drive Selection: Local hard disk, File, Unknown
- Filesystem Types: FAT, Device Driven, HPFS, NTFS, ext, ext2, ufs, tmpfs, vxfs, hfs, hfs Extended, jfs, ext3, DVD-ROM

Directories

- Environment Variables: PATH;LIBPATH
- Options: Scan subdirectories
- Windows Only

Naming the Configuration (.cxz) File

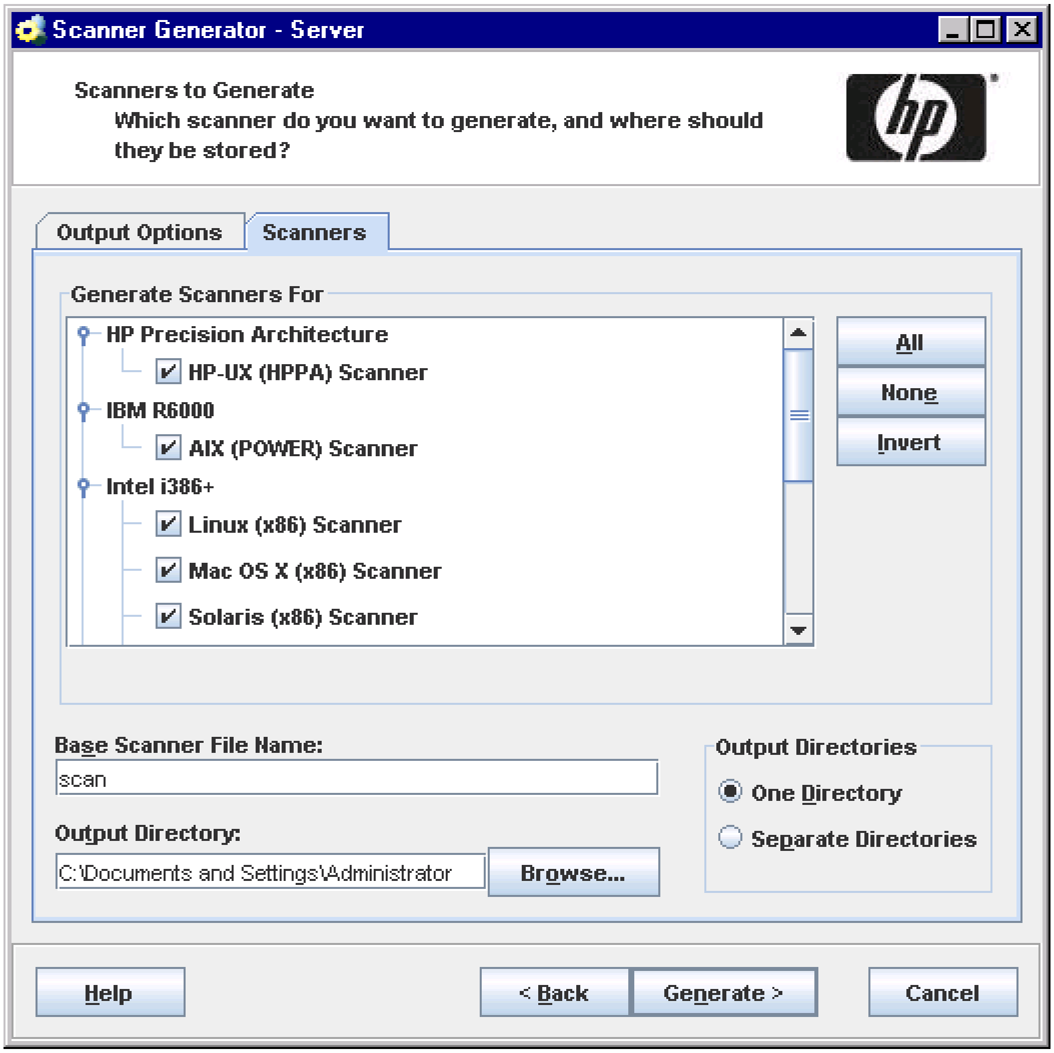
In Enterprise Mode the configuration file is saved on the DDM Inventory Server as well, using the same file name as the copy specified in the Configuration file name to use field.

The configuration file is a compressed XML file containing the settings for the scanner you are currently configuring.

When the scanners are used in the Enterprise Mode, they read the configuration from a separate configuration file. This is a binary file with a `.cxz` extension. The typical size of the configuration file is about 3KB. As the size of the configuration file is significantly smaller than the size of the complete scanner, a separate scanner configuration is useful for repetitive inventory collection when the configuration of the scanner has been altered. In this case only a small configuration file is delivered to the user’s computer to run with the original scanner instead of delivering the entire new scanner.

Scanners Tab

The **Scanners** tab is only available in Manual Deployment Mode. It is used to select which of the scanners to generate.



Scanners to Generate

Which scanner do you want to generate, and where should they be stored?

Generate Scanners For

- HP Precision Architecture
  - ☑ HP-UX (HPPA) Scanner
- IBM R6000
  - ☑ AIX (POWER) Scanner
- Intel i386+
  - ☑ Linux (x86) Scanner
  - ☑ Mac OS X (x86) Scanner
  - ☑ Solaris (x86) Scanner

Base Scanner File Name: scan

Output Directory: C:\Documents and Settings\Administrator

Output Directories

● One Directory

○ Separate Directories

Selecting which Scanners to Generate

The scanners are presented in a tree view in the Generate scanners for list box.

As the mouse pointer passes over a scanner in the list, the status bar (just below the list box) displays the following information for that particular scanner:

- If the scanner is enabled (meaning it is valid with the current set of options).
- The directory that the scanner will be generated in. If the scanner was invalid, then a description of why this is the case is displayed instead.

To select which scanners to generate:

Select the check boxes next to the scanner.

Buttons

- **All** - Selects all scanners
- **None** - Deselects all scanners
- **Invert** - The Invert button allows the selections to be reversed. This saves having to deselect all the scanners one by one, when only a single scanner is required. If all the scanners are selected, just deselect the one you want and choose Invert.

Specifying Base Scanner File Name and Output Directory

You can define the base name of the scanner (up to 5 characters). Alternatively for each scanner, you can either have a file name to identify the operating system or you can use a separate directory for each operating system.

To specify the base scanner file name and output directory:

1. For all selected scanners, specify a fully qualified file name. The initial part of this file name can be entered in the **Base Scanner File Name** box. The remaining three characters of the file name are used to describe the scanner executable.

   For example, by entering **Scan** (the default setting) in the **Base Scanner File Name (Max 5 characters)** box, the following scanners can be generated (if they have been selected in the **Generate scanners for** list box):

Table 32 Base scanner file names and output directories

Scanner File Name	Scanner Type
scanwin32-x86.exe	Windows (x86)
scanwin32h-x86.exe	Windows (86, hidden)
scansolaris-sparc	Solaris (SPARC)
scansolaris-x86	Solaris (x86)
scanhpux-hppa	HP-UX (HPPA)
scanhpux-ia64	HP-UX (ia64)
scanaix-ppc	AIX (POWER)
scanlinux-x86	Linux (x86)
scanmacosx-ppc	Mac OS X (PPC)
scanmacosx-x86	Mac OS X (x86)

2. In the **Output Directory** box, type in or click the 📂 button to specify the directory that the generated scanners will be saved to.

Setting Naming Conventions for Scanners

The **Naming conventions** options determine the manner in which scanner files are named:

To set naming conventions for the scanners:

1 Select one of the following:

- **Filename includes operating system**

  This option incorporates the scanner name with the operating system, for example:

  `scanwin32h-x86.exe`

- **One directory per operating system**

  This option dictates that the names of each scanner generated are the same, but are copied into individual subdirectories which are named as per the operating system.

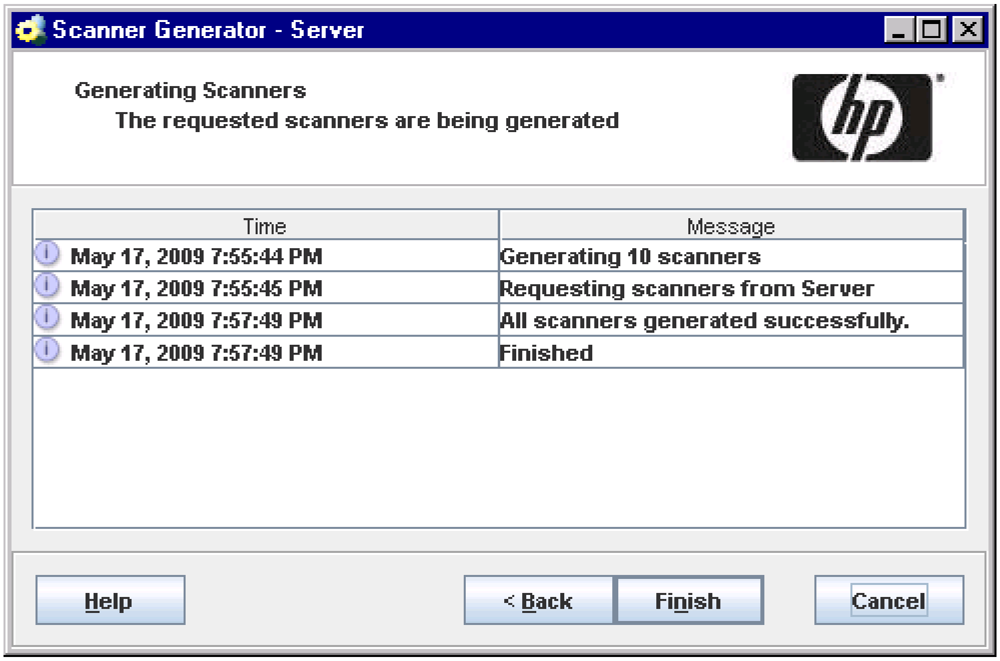
  For example, a scanner named `scan.exe` (Windows)/`scan` (other platforms) would appear in directories for all operating system options selected:

  ```
  C:\Program Files\Hewlett-Packard\DDMI\9.30\win32-x86

  C:\Program files\Hewlett-Packard\DDMI\9.30\solaris-sparc

  C:\Program files\Hewlett-Packard\DDMI\9.30\hpux-hppa

  C:\Program files\Hewlett-Packard\DDMI\9.30\hpux-ia64

  C:\Program files\Hewlett-Packard\DDMI\9.30\aix-ppc

  C:\Program files\Hewlett-Packard\DDMI\9.30\linux-x86

  C:\Program files\Hewlett-Packard\DDMI\9.30\macosx-ppc

  C:\Program files\Hewlett-Packard\DDMI\9.30\macosx-x86
  ```

2 Click **Generate** to create the scanner executable files.

Generating Scanners Page

After you have selected the scanners to be generated and have clicked **Generate**, the last page of the Scanner Generator is displayed.



Generating Scanners

The requested scanners are being generated

Time	Message
May 17, 2009 7:55:44 PM	Generating 10 scanners
May 17, 2009 7:55:45 PM	Requesting scanners from Server
May 17, 2009 7:57:49 PM	All scanners generated successfully.
May 17, 2009 7:57:49 PM	Finished

This page shows the progress information during the generation of the actual scanner executable.

In Enterprise Mode, the scanner configuration is generated instead of stand-alone scanners and the configuration is uploaded to the DDM Inventory Server. If you chose to generate your scanner from a stored default predefined configuration on the server when you were on the Standard Configuration page, you will be told to rename it since default predefined configurations cannot be overwritten.

Right-clicking anywhere in the log window displays a shortcut menu which allows you to:

- Save the contents of the window to a log file.
- Copy the contents of the log window to the clipboard.
- Clear the log window.

If a scanner already exists with the same name in the chosen directory, a confirmation message is displayed. This allows you to choose whether to overwrite the existing scanner.

After the scanners have been generated, click **Finish** to exit the Scanner Generator.

The generated scanners can be found in the directory specified in the Scanners tab of the Scanners to Generate page.

13 XML Enricher

The XML Enricher is a process that runs in the background and automatically adds application data to scan files. This process is called scan file enrichment. It works as follows:

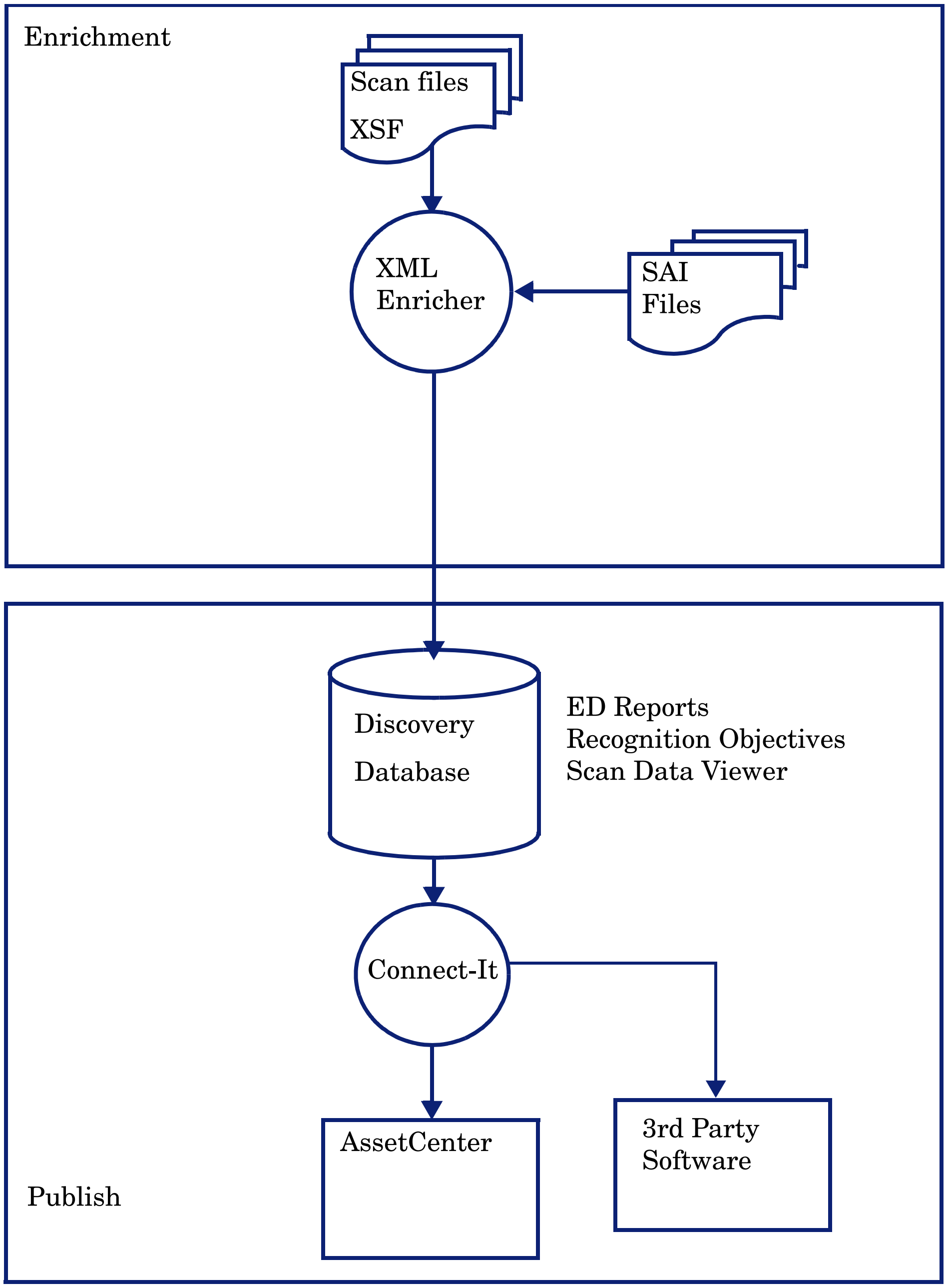
1. The XML Enricher looks for new scan files (xsf or dsf format) in the Incoming directory.
2. If a file is found, it processes the file using SAI (Software Application Index) application recognition.
3. Information about recognized applications is added to the file data and a separate **<applicationdata>** section is added to the XML file.

The XML Enricher provides data that is automatically imported into the aggregate database.

You can set up Viewer and Analysis Workbench to use the processed scan files in the Processed directory for analysis, or the processed scan file can be consumed by a Connect-It script.

The XML Enricher can also be used to re-enrich scan files that were enriched previously. This can be useful after applying a significant update to the SAIs.

As a guideline, on a fast machine an average sized scan file (200-300Kb) will take 3 to 8 seconds to process.



XML Enricher Directory Structure

The XML Enricher uses a directory structure under the DDM Inventory `Data` directory.

By default, the DDM Inventory `Data` directory is:

`C:\Documents and Settings\All Users\Application Data\Hewlett-Packard\DDMI.`

‼ The Data Directory is customizable during the installation process. Ensure that you have no other data in this directory. The data directory must be dedicated to DDM Inventory.

The following table shows the various directories that are used by the XML Enricher.

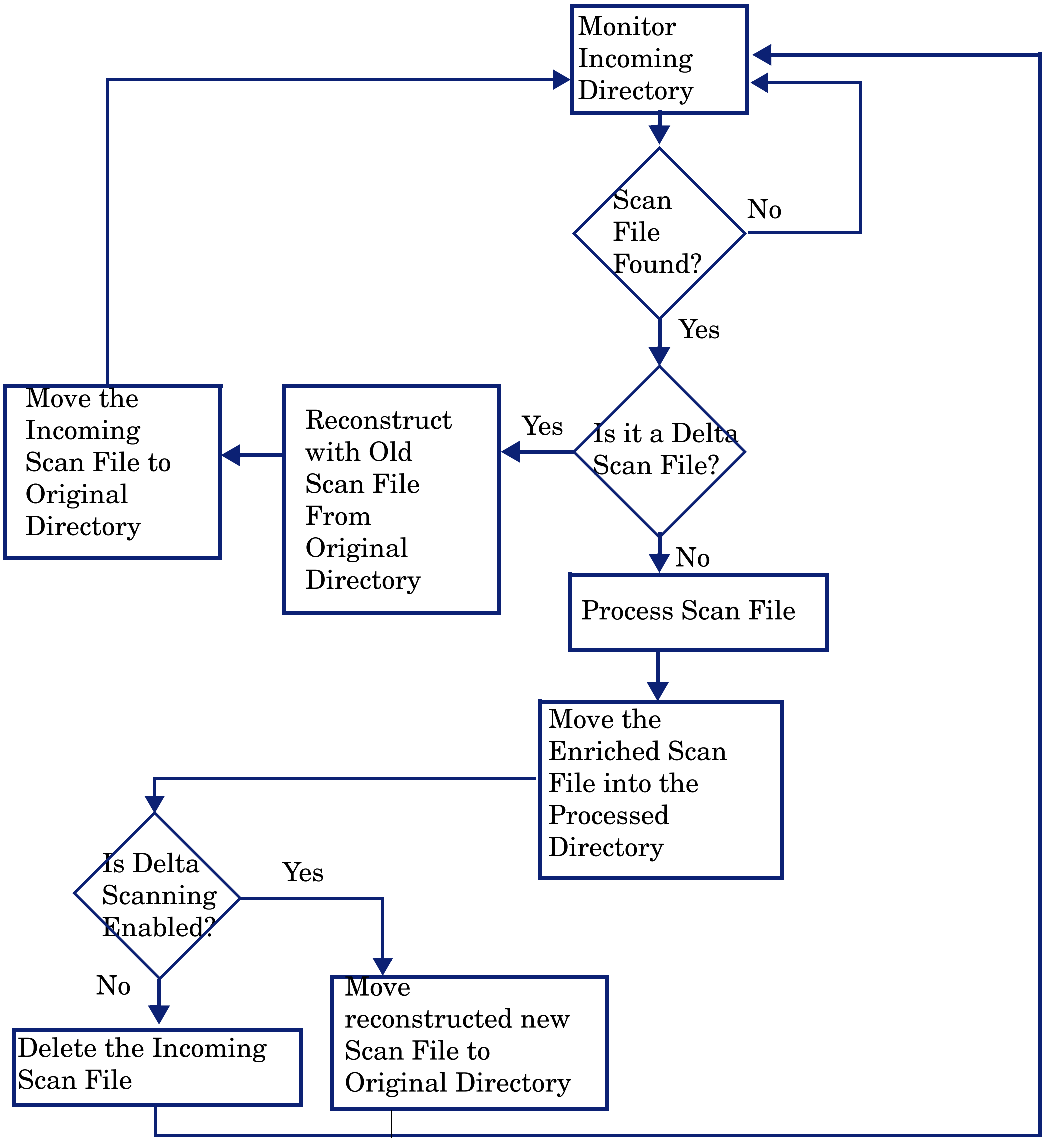
Table 33 Directories used by the XML Enricher

Directory	Explanation
`\Scans`	The base directory
`\Scans\Failed`	The base failure directory. Failed scans are moved to a subdirectory of this one.
`\Scans\Failed\Corrupt`	Scans that cannot be read or may not be scan files are moved here.
`\Scans\Failed\Delta`	If the original scan file is missing or there is an error applying the delta scan file to the original one, then those delta scan files will be moved here.
`\Scans\Failed\Error`	When any other error occurs, scan files are moved here.
`\Scans\Failed\Filter`	The scan file ends up here if it has an IP address outside a range that has been configured to allow scanned devices.
`\Scans\Failed\Licence`	If the number of processed scan files exceed the maximum number of licenses, new scans are moved here.
`\Scans\Failed\Old`	Scan files that are copied to the incoming directory but are older than the one already in the database are moved here.
`\Scans\Deferred\Firstscan`	If the **Automatically defer all new scans** option was set, the scan file is not processed. See Automatically Defer all New Scans on page 189. Instead, it is moved to this directory. Any scan files in this directory are from the first time a scan file was seen for a particular computer. This allows the administrator to review the asset and application data. When you are satisfied that the data is OK, you can move it back to the incoming directory. Note: New scan files from a computer will not be processed while a scan file for it exists in this directory. The existing scan file in this directory will be overwritten by the new scan file.
`\Scans\Incoming`	The incoming directory. The enricher looks for new scan files here.

Table 33 Directories used by the XML Enricher

Directory	Explanation
`\Scans\Original`	This folder is used for delta scanning. It stores copies of original scan files, which are then used in conjunction with delta scan files to recreate the new version of the scan file.
`\Scans\Processed`	The processed directory. Enriched scan files are created here.
`\Scans\Processed\[user defined]`	You can group the scan files based on Hardware fields. This is user-defined. Define the setting on the following web UI page: **Administration > System Configuration > Scan file management**. See Group Processed Scan Files on page 193.
`\Scans\Temp`	This is where the XML Enricher stores its temporary files.

The following flowchart shows how the enrichment process works for XSF and delta (DSF) scan files.


Monitor Incoming Directory
Scan File Found?
No
Yes
Is it a Delta Scan File?
Yes
No
Reconstruct with Old Scan File From Original Directory
Move the Incoming Scan File to Original Directory
Process Scan File
Move the Enriched Scan File into the Processed Directory
Is Delta Scanning Enabled?
Yes
No
Delete the Incoming Scan File
Move reconstructed new Scan File to Original Directory

Processing Normal Scan Files

At the end of the process, a new enriched scan file is created. If delta scanning was enabled in the parameters for the Scanner used to produce the scan file, the incoming scan file gets stored in the **Original** directory for future use by the delta scan processing. If delta scanning was disabled, the incoming scan file is deleted.

If an error occurs, the original scan file is moved to a failure directory and is not deleted.

If an enriched scan file for the same asset/device already exists, the old file is overwritten.

Processing Delta Scan Files

The delta scan file is used in conjunction with the previous version of the scan file located in the **Original** directory to reconstruct the new full version of the scan file. This full version is then moved into the **Incoming** directory, where it gets processed in the same way as other normal scan files.

At the end of the process, the reconstructed scan file is moved to the **Original** directory, ready for the next time a delta scan is found for this particular scan file instance.

Setting up the Scanner to Handle Delta Scan Files Correctly in Manual Deployment Mode

When conducting an inventory in Manual Deployment mode, for the delta scan file processing in the XML Enricher to work correctly, ensure that you do the following:

- Configure the Scanner to save results to the XML Enricher Incoming directory. This is done in the Save result to network (off-site) field on the Scanner Generator Scanner **Options** > **Saving** tab page.

  This directory can be found in the DDM Inventory Data Directory in the following folders:

  ```
  [DDM Inventory Data Directory]\Scans\Incoming
  ```

  This directory should be accessible to all users as the Scanner should be configured to save to the incoming directory used by the XML Enricher.

  You can also use the command line option `-p:<path>` with the Scanner to override the selection made in the Scanner Generator.

- Set the separate refilling path to the Original directory. This directory can be found in the following place:

  ```
  [DDM Inventory Data Directory]\Scans\Original
  ```

  This directory should be accessible to all users. This will ensure that the Original directory will contain the original scan file to be used in reconstruction.

  You can also use the Scanner `-r:<path>` command line option to specify the location of this directory.

Delta Calculation Command Line Utility

A command line utility can be used for calculating the delta between two scan files and applying a delta scan file to a full scan file. This utility is not used by any of the DDM Inventory components; delta scan file processing is built into them. It is only provided for technical support purposes and can also be used to create custom delta scan processing, which is different from the built-in delta scan support.

This utility is called **FSFDelta.exe** and can be found in the following location:

```
C:\Program Files\Hewlett-Packard\DDMI\9.30\Scanner Generator
```

The convention for using this command line utility is as follows:

```
XSFDelta OldFile NewFile DeltaFile
```

Where:

- **[XSFDelta]** is the command
- **[OldFile]** is the name and path to the old scan file - Enter the full scan file name (for example, `Test.xsf`)
- **[NewFile]** is the name and path to the latest scan file - Enter the full scan file name (for example, `Latest.xsf`)
- **[DeltaFile]** is the name and path to the delta scan file produced. If no extension is specified for this file, the default `.dsf` is assumed.

➤ If you have all three of these files contained in the same directory as the XSFDelta utility, then you do not have to specify the full path to these files.

To create a delta scan file, run XSFDelta specifying the two input scan file names and the name of the output delta scan file. XSFDelta compares the two full scan files specified and creates a delta scan file containing the differences between them.

To perform the reverse process of reconstructing the new version of the full scan file using the previous scan file and a delta scan file, run XSFDelta with the –d command line switch, specifying the input OldFile name and DeltaFile names and the output NewFile name.

XSFDelta will apply the differences in DeltaFile to OldFile to reconstruct the new version of the scan file in NewFile.

Application Utilization Data

Agent software utilization generates individual utilization files, one per day when it runs up to the maximum period for which utilization data is collected.

In addition, it also produces a summary file for the entire utilization period. This file is an XML data file compressed using gzip (Compressed XML utilization). The XML is encoded using the UTF-8 encoding.

The XML Enricher does the following during its processing:

- Extracts and parses the XML data out of the stored file.
- Calculates the software utilization for each recognized application and adds this information to the enriched scan file.
- Adds a 'Utilized' flag to the file attributes, calculates and adds utilization figures for executables that were executed.

Log Files

Whenever enrichment of a scan file fails, an entry describing the occurrence is added to a file named log.txt in the relevant failed subdirectory.

For example, the following is an excerpt from log.txt from the Licence directory:

```
2005-August-28 13:21:08.000 - Asset19 (Licence limit reached)

2005-August-28 13:21:29.125 - Asset292 (Licence limit reached)
```

The format of a line in the log file is

```
<date> <time> - <AssetTag> (<Failure reason>).
```

The XML Enricher also adds entries to the Discovery Log in the following circumstances:

- When it starts up and shuts down.
- When it starts enrichment of a new scan file.
- If an error occurs.

Application Recognition in XML Enricher

The XML Enricher reads scan files and outputs ‘enriched’ XML scan files containing all of the original data as well as data identified in the application recognition step.

Each file is stored as a <file> element. When a file is identified as belonging to an application, two attributes are added to the element: `versionid` and `flag`.

For example,

```
<file name=”winword.exe” size=”12345” versionid=”1111” type=”M”/>
```

would represent a file named winword.exe identified as belonging to the application with a version ID of 1111. The type of the file is “M”, which means Main file. The possible values for the type field are:

Type	“type” tag in enriched XML file
Main	M
Associated	Y
3rd Party	3
Device Driver	A
Unknown	N

The `versionid` attribute refers to the unique ID associated with every version in the library. In an enriched XML scan file, the <applicationdata> section contains a list of applications identified on the machine along with the version IDs.

For example,

```
<applicationdata>
<application version="6.0 sp1"
    release="6.0"
     name="Internet Explorer"
     desc="Microsoft Internet Explorer"
     publisher="Microsoft"
     language="English"
     os="Windows 98/NT/2K/ME/XP"
     type="Web Browsers"
     maindir="C:\Program Files\Internet Explorer"
     lastUsed="2004-05-05 00:00:00"
     versionid="12790"
     releaseid="131"
 />
<application version="6.0 sp1"
    release="6.0" name="Outlook Express"
    publisher="Microsoft"
    language="English"
    os="Windows 98/NT/2K/ME/XP"
    type="Communications"
   maindir="C:\Program Files\Outlook Express"
    lastUsed="2004-05-05 00:00:00"
    versionid="12792"
    releaseid="372"
    licencedby="12790"
    licencedbyrelease="131"
/>
</applicationdata>
```

The example above could be found for a machine with just two applications on it: Microsoft Internet Explorer and Microsoft Outlook Express. The “licencedby” attribute indicates that Microsoft Outlook Express is licensed by Microsoft Internet Explorer. In other words, while both are licensable applications, this machine requires 1 license for Microsoft Internet Explorer - with this license, no separate Outlook Express license is required.

Configuring the XML Enricher

You can configure the following options to control the XML Enrichment process:

- Process Utilization Data
- Application Recognition
- Automatically Defer all New Scans
- Merge Priority
- Generate Solaris Local Zone Inventory from Global Zone
- Advanced SAI Recognition Options
- SAIs
- Filtering

To configure the XML Enricher:

1 Click **Administration > System Configuration > Scan processing.**

2 Set the options as required.

Process Utilization Data

If you want to stop collecting utilization data, turn this option off. The default option is **Yes**.

DDM Inventory can only collect Utilization data if you have a license for it.

Application Recognition

There are three options for Application Recognition:

- **Software application index (SAI)**

  This is the default setting. If you select this application recognition option, the XML Enricher uses the Software Application Index files (`.zsai`) to perform application recognition. The SAI files contain a database of software applications. By default, only executable files are sent to the recognition engine for processing. You can set this so that all files are sent to the recognition engine by modifying the filter settings. See Filtering on page 191.

- **No recognition**

  This option is used to disable any application recognition. When recognition is disabled, scan file processing is slightly faster as no file information is sent to the recognition engine for processing. However, the processed scan files are not enriched with application data and no application data is added to the database.

- **Installed applications**

  If you select this application recognition option, the XML Enricher uses the operating system's internal list of installed applications to report the application data. As this list is incomplete and not normalized, it is not recommended as the preferred recognition method, except for quick initial assessment.

Refer to the “Application Recognition and Teaching” chapter in the *Scan Data Analysis Guide* for more details.

Automatically Defer all New Scans

If enabled, the following happens when a scan file is found in the Incoming directory:

- The scan file is looked up in the internal database (Not the Discovery Database).
- If the machine has never before been scanned, the scan file is not processed or enriched. Instead, it is moved to the firstscan directory.
- If the machine has been scanned before, the enricher checks if there is a scan file with the same name in the firstscan directory. If there is, the old scan in the firstscan directory is deleted and is replaced with the new one.

When a new computer is scanned for the first time, the data is not added to the Discovery database until it has been manually reviewed and the scan file has been moved back to the Incoming directory.

Merge Priority

This allows you to define what to use as the primary data merge keys. In the case of the automatic deployment of the scanner in Enterprise Mode, the scanner has extra information (for example, the NMID), but if this information cannot be used, the other fields will be used.

For example, if NetBIOS Name and Windows Domain are chosen, then it will use this information in the scan file to find the matching device in DDM Inventory.

Generate Solaris Local Zone Inventory from Global Zone

For Solaris zones, this option allows you to specify to the XML Enricher how you want it to process the global zone scan file. If this option is enabled, the XML Enricher generates individual scan files for each local zone from the global zone scan file on the Solaris server. You want to enable this option if you are running the scanner in the recommended global zone scan mode. This option is enabled by default. Disable this option if you are running the scanner in the non-recommended local zone mode.

➤ If you are running the scanner in the non-recommended local zone mode and enable this option, the XML Enricher will discard the local scan files produced for each local zone by the individual scanners and replace them with the scan files that are generated from the global scan file.

Advanced SAI Recognition Options

These three sets of options determine how the XML Enricher performs the SAI application recognition. They correspond to the controls available on the Recognition tab of the Options dialog box in Viewer and Analysis Workbench.

Advanced Recognition Methods

There are two advanced recognition options. They are independent of each other. By default, both are selected.

- The **Level 3 recognition heuristics** option determines when the XML Enricher processes scan files for a particular machine. If this option is selected, the XML Enricher waits until all the files in all the directories on that machine have been read before issuing its final recognition information.

  If this option is selected, more accurate recognition is achieved. If this option is not selected, machine-based recognition does not take place, and recognition data is returned after each directory is loaded. A time overhead of about 10% is normal when Level 3 Recognition is enabled.

- The **Auto-identify unrecognized device driver files** option instructs the XML Enricher to mark files that meet the following criteria as recognized in the enriched scan file:

  — They cannot be identified by standard SAI recognition.

  — They have the Device Driver attribute.

  Files used as Device Drivers represent a large portion of the files that are not identified by the Application Library. Being able to identify these automatically can significantly reduce the effort required to achieve good recognition rates.

Preferred Language

This option enables you to specify the language that the XML Enricher uses when it encounters more than one language version of the same file - for example, Microsoft Word in both English and French. Because these versions are equally recognized, this setting tells the XML Enricher which version to select.

This option works in concert with the Override OS Language option. By default, no preferred language is set.

Override OS Language

This option works in concert with the Preferred Language option. If you specify a Preferred Language, and you select the Override OS Language option, the recognition engine will overlook the OS locale setting and use the Preferred Language that you specify.

By default, this option is set to **No**.

For more information about the process of application recognition, refer to the *Scan Data Analysis Guide*.

SAIs

There are two XML Enricher options that pertain to Software Application Index (SAI) files:

SAI files

This option enables you to specify the SAI files that the XML Enricher uses to recognize applications.

The list of available SAI files matches the contents of the SAI folder in your DDM Inventory data directory. By default, this is:

```
C:\Documents and Settings\All Users\Application Data\Hewlett-Packard\
DDMI\SAI
```

For each SAI file that appears in the list, the following information is displayed:

- A description
- The size (in kilobytes)
- The number of unique application versions the SAI file contains
- The type: Master (read-only) or User (editable)
- The creation date for a Master SAI file. For a User SAI, the date the file was last saved.

The XML Enricher searches for `master.zsai` and `user.zsai`. If the locale is France, it adds `french.zsai`. If the locale is Germany, it adds `german.zsai`.

The XML Enricher can only load SAIs from non-substed locations. This is because Windows drives created by the SUBST command are not accessible to Windows services.

SAI File Used to Store Rule-created Items

This option specifies the SAI file to which items encountered that were created by rules will be added. These rules are present within the SAI files themselves. You can specify additional rules by using the SAI Editor.

If this field is left blank, DDM Inventory will create a file called Auto.zsai and put this in the same location as the first Master SAI.

For more information about SAI files and the process of application recognition, refer to the *Scan Data Analysis Guide*.

Filtering

There are four filtering options that determine what types of files the XML Enricher processes:

Use Only Files with the Following Extensions

This option specifies the extensions of the particular file types that will be processed by the XML Enricher. Type the extension(s) that you want to use directly into the box. Separate extensions with commas or semicolons. Only these file types will be processed.

Use Only Executable Files

This option specifies that only executable files should be processed by the recognition engine. This includes `*.exe, *.com, *.dll` and other files containing executable code.

Look also for Files within Archives

Use this option to specify that files within archive files should be processed. The following archive file types are supported: `ARJ, ZIP v1, ZIP v2, LHA, LZH, ARC, CAB, TAR, GZIP, TAR/GZIP` and `PAK`.

Comma Separated List of Regular Expressions used to Filter Junk Files

Some files may be executable but are of no interest for licensing or other purposes. These files are often identifiable via the file name. For example: `TMP[0-9]*\.\$\$\$`. This option enables you to specify file names that should be ignored by the XML Enricher. Do this by entering comma-separated regular expressions in the text box. Any files whose names match the regular expressions will be ignored.

When the XML Enricher matches a file name against a junk filter regular expression, the file name is first converted to lower-case. For this reason, all letters entered as part of the regular expression must be in lower-case for a match to successfully occur.

For more information about the process of application recognition, refer to the *Scan Data Analysis Guide*.

Analysis Asset Field Configuration

The Analysis Asset Field configuration settings that affect the XML Enricher cannot be modified in the Web UI. You can change these settings by using the Viewer. To do this, follow these steps.

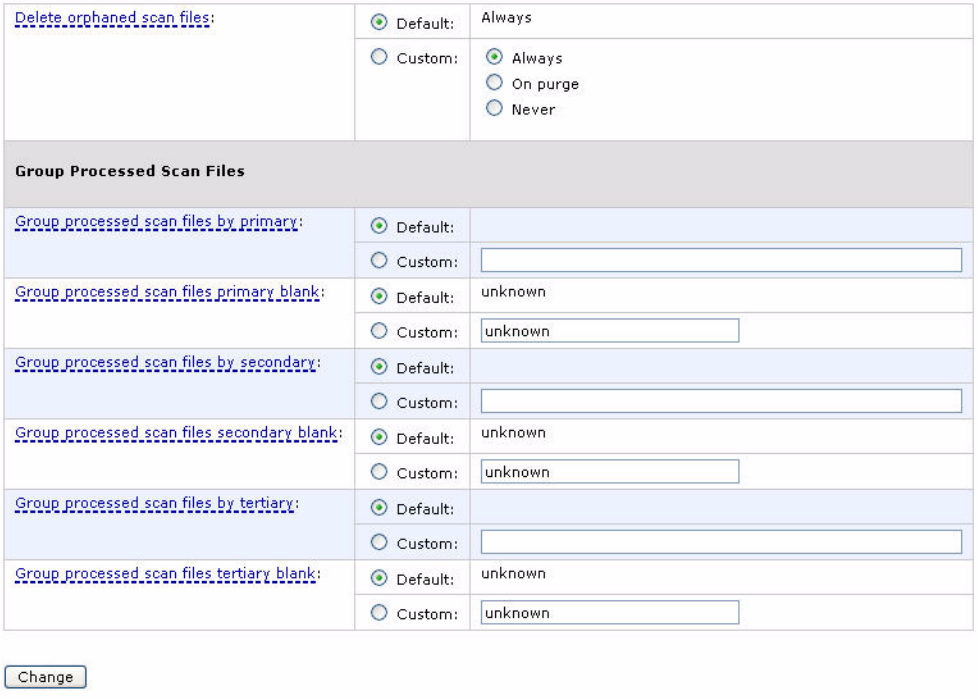
1. Select **Start** > **All Programs** > **Hewlett-Packard** > **DDM Inventory 9.30**> **Viewer**.
2. Use **File** > **Options** > **Asset Fields** to configure the Analysis Asset Fields.

For more information, see the “Viewer” chapter of the *Scan Data Analysis Guide*.

Managing Scan Files

You can configure the following options to control scan file management:

- Delete Orphaned Scan Files
- Group Processed Scan Files



Delete orphaned scan files:	● Default:	Always
	○ Custom:	● Always ○ On purge ○ Never
Group Processed Scan Files		
Group processed scan files by primary:	● Default:	
	○ Custom:	
Group processed scan files primary blank:	● Default:	unknown
	○ Custom:	unknown
Group processed scan files by secondary:	● Default:	
	○ Custom:	
Group processed scan files secondary blank:	● Default:	unknown
	○ Custom:	unknown
Group processed scan files by tertiary:	● Default:	
	○ Custom:	
Group processed scan files tertiary blank:	● Default:	unknown
	○ Custom:	unknown

To configure scan file management:

1 Click **Administration > System Configuration > Scan file management**.

2 Set the options as required. They are described below.

Delete Orphaned Scan Files

Orphaned scan files are scan files that are no longer associated with a network device.

There are two scenarios that create orphaned scan files:

- The network device has been purged from the database.
- An admin user has changed the scan file groupings, so the original scan file is orphaned, while the new scan file for that device is located in another folder.

You can use this feature to have DDM Inventory automatically delete these orphan scan files.

Group Processed Scan Files

The grouping commands will help you organize your scan files in the processed directory. You can group your scan files based on Hardware Fields (for a complete list, see **Help > Classifications > Hardware Fields**).

The value of the selected hardware field will be used as the name of a subdirectory under the “processed” directory.

If the Hardware field you have chosen is blank in a scan file, that file will be moved to a “Blank” directory.

Updating Application Library used by Enricher

This is done via an update package that contains Rulebase, JAY Scripts and the latest SAI files. This gets dropped into the `C:\Program Files\Hewlett-Packard\DDMI\9.30\Install` directory and the system monitor service automatically detects this, unpacks it and installs it.

Refer to the chapter entitled *Installing Knowledge Updates* in the *Installation and Upgrade Guide* for further information on how to do this.

Structure of Enriched XSF File

`Scanfile.dtd` describes the structure of the scan file in standard DTD format. By default this file can be found in the following location:

```
C:\Program Files\Hewlett-Packard\DDMI\9.30\Common
```

The file is a text file, but is easiest to read with an XML reader.

An XSF scan file contains a sequence of elements, each of which have various attributes. Root elements are:

- <hardwaredata>
- <applicationdata>
- <filedata>
- <storedfiles>
- <configurationdata>

Example of How Data is Stored

The following is an example of several sections in an xsf file.

```
<?xml version="1.0" encoding = "UTF-8" ?>
<inventory codepage="1251" locale="English (United States)" fsfmajorver="7"
fsfminorver="6" enricherver="9.30.000.1300">
<hardwaredata>
    <hwAssetData type="shell">
      <hwAssetDescription type="attrib">tbrown - Xeon, 2800MHz, 3712Mb</
hwAssetDescription>
      <hwAssetTag type="attrib">000590 </hwAssetTag>
    </hwAssetData>
    <hwMemoryData type="shell">
      <hwMemTotalMB type="attrib">3712</hwMemTotalMB>
      <hwSwapFiles type="shell">
        <hwSwapFiles_value type="shell_value">
         <hwMemSwapFileName type="attrib">C:\pagefile.sys</hwMemSwapFileName>
          <hwMemSwapFileSize type="attrib">1534</hwMemSwapFileSize>
        </hwSwapFiles_value>
      </hwSwapFiles>
      <hwDOSMemoryData type="shell">
        <hwMemConventional type="attrib">640</hwMemConventional>
      </hwDOSMemoryData>
      <hwCMOSMemory type="shell">
        <hwMemExtended type="attrib">3799944</hwMemExtended>
        <hwMemCMOSTotal type="attrib">3800584</hwMemCMOSTotal>
        <hwMemCMOSConventional type="attrib">640</hwMemCMOSConventional>
      </hwCMOSMemory>
    </hwMemoryData>
</hardwaredata>
<applicationdata>
<recogconfig>
<sai name="C:\Documents and Settings\All Users\Application
Data\Hewlett-Packard\DDMI\SAI\user.zsai" desc="User SAI File" date="04/06/
2007"
type="User"/>
      <sai name="C:\Documents and Settings\All Users\Application
Data\Hewlett-Packard\DDMI\SAI\master.zsai" desc="" date="07/05/2007"
type="Master"/>
<application version="6.4.09"
release="6.4"
name="Windows Media Player"
publisher="Microsoft"
language="English"
os="Windows 2000"
type="Interactive Media Tools"
maindir="C:\Program Files\Windows Media Player"
lastUsed="2007-08-26 00:00:00"
versionid="9978"
releaseid="582"
licencedby="11907"
licencedbyrelease="84"
/>
<application version="6.0 sp1"
release="6.0"
name="Internet Explorer"
desc="Microsoft Internet Explorer"
publisher="Microsoft"
language="English"
os="Windows 98/NT/2K/ME/XP"
type="Web Browsers"
maindir="C:\Program Files\Internet Explorer"
lastUsed="2007-05-07 00:00:00"
versionid="12790" releaseid="131"
/>
</applicationdata>
<filedata>
    <dir name="C:\" date="2007-07-03 03:23:04" contains="-1">
      <file name="AUTOEXEC.BAT" size="0" modified="2007-04-03 13:51:04"
attr="a"/>
      <file name="BOOT.INI" size="288" modified="2007-04-03 15:14:38"
attr="rsa"/>
```

```
      <file name="sd_settings.ini" size="462" msdos="SD_SET~1.INI"
modified="2007-06-14 09:08:44" attr="a">
        <verinfo name="DOS 8.3 Name" value="SD_SET~1.INI"/>
      </file>
    </dir>
</filedata>
<storedfiles>
<storedfile type="storedfile" name="SYSTEM.INI" size="217" istext="1"
istruncated="0" dir="C:\WINNT\SYSTEM.INI">
      <contents encoding="text">; for 16-bit app support
[386Enh]
woafont=dosapp.fon
EGA80WOA.FON=EGA80WOA.FON
EGA40WOA.FON=EGA40WOA.FON
CGA80WOA.FON=CGA80WOA.FON
CGA40WOA.FON=CGA40WOA.FON
[drivers]
wave=mmdrv.dll
timer=timer.drv
[mci]
</contents>
    </storedfile>
</storedfiles>
</inventory>
```

Running Multiple XML Enricher Services

By default, DDM Inventory is configured to use one XML Enricher service. This is adaquate for most situations. However, in exceptional circumstances when the scan files flow into the incoming directory faster than the XML Enricher is able to process them, a build-up of scan files can appear in the incoming directory. To allocate more processing power to enriching scan files, DDM Inventory can be configured to use 2 XML Enricher services. You can specify this in **Administration** > **System Configuration** > **Server configuration** > **Number of XML Enrichers to run**.

➤ Running two XML Enricher services makes sense only if the computer on which DDM Inventory is running has multiple physical CPUs or a single CPU with multiple cores. Although some benefit can be gained if a single processor system has hyper-threading supported and enabled, the real benefit can be seen on multi-core or multi-processor systems.

14 Getting Data into AssetCenter

This chapter explains how you can get your data from DDM Inventory into AssetCenter using the out-of-the-box DDM Inventory to Asset Management scenario supplied.

The scenario is an example only and as such does not necessarily reflect your data needs. For further information on customizing the scenario, refer to the *Connect-It Users Guide*.

Assumptions

The following assumptions have been made throughout this chapter:

- You are familiar with one or more of the components of this process. That is, DDM Inventory, AssetCenter and Connect-It.
- You have already installed AssetCenter and Connect-It on a machine.
- You will be using a new empty AssetCenter database.
- You have a valid account for accessing the AssetCenter database.

Where to Find the Connect-It Scenario

The DDM Inventory to AssetCenter Connect-It scenario is supplied with Connect-It not DDM Inventory. You can find the scenario files (`.scn`) in the following default location:

```
C:\Program Files\Hewlett-Packard\ConnectIt\scenario\ed\ed2ac44
```

Prerequisites

We strongly recommend that you follow the procedures in this chapter using test data before you actually use them on a production AssetCenter database containing live data. This will ensure that:

- You have good working knowledge and confidence in carrying out the processes
- You will not damage the data that it already in your AssetCenter database
- You will be able to experiment with the scenario and the data associated with it.

Installation

The Asset Management application client (AssetCenter) must be installed on the same computer as Connect-It. We also recommend that you do not install Connect-It on the same machine as the DDM Inventory Server.

Compatibility

Refer to the Compatibility Matrix in the DDM Inventory GUI under **Help** > **Compatibility Matrix** for the correct versions of Connect-It and Asset Center to be running with DDM Inventory 9.30.

For AssetCenter 4.x (where x is less than 4) some of the fields may not exist.

You will need to do the following:

1. Load the scenario and open the connectors.

   Error messages will be displayed for any field that does not exist.

2. Unmap those fields.

Prepare AssetCenter

Once you are familiar with the processes, you can export the DDM Inventory data directly into your normal AssetCenter database.

Refer to your AssetCenter documentation for instructions on how to do this.

Prepare Connect-It

There are three steps to setting up Connect-It for the scenario:

Task 1: Open the Scenario

Task 2: Configure the Source Connector - DDM Inventory

Task 3: Configure the Destination Connector - AssetCenter

Step 1: Open the Scenario

1 Select **Open** from the **File** menu and navigate to the DDM Inventory to Asset Management out-of-the-box scenario edac.scn file.

By default this file is located in:

```
C:\Program Files\Hewlett-Packard\ConnectIt\scenario\ed\ed2ac44
```

A three box scenario diagram is now displayed showing the mapping between DDM Inventory and Asset Management.

You may have to use the Zoom bar in the top right of the Connect-It window to position the boxes so they become visible.

2 Select the **Save as** option from the **File** menu and give the scenario another file name so you will not be overwriting the original DDM Inventory-AssetCenter out-of-the-box scenario.

Step 2: Configure the Source Connector - DDM Inventory

Click on the title bar of the DDM Inventory connector box to highlight it.

To configure the connector you can either:

- Right-click on the DDM Inventory connector title bar and select the Configure Connector... option.
- Select the **Configure** option from the **Tools** menu.
- Press the **F2** key on your keyboard.

  A wizard for the configuration of the DDM Inventory connector is displayed.

Page 1: Name and describe the connector

The first page of the wizard enables you to name the DDM Inventory connector and provide a description for it.

1 **Name:** By default, the value of this field is DDM Inventory.

2 **Description:** Enter text to describe the connector. This field is not mandatory.

3 Click the **Next** button to continue. The Select connection type page opens.

Page 2: Select a connection type

This page allows you to specify the connection protocol.

1 For the purpose of DDM Inventory, always select MySQL (native).

2 Click **Next** to continue. The Configure the database server connection page opens.

Page 3: Define the database server connection

This page allows you to set up the connection to the DDM Inventory database.

1 **Server**

Enter the port used for the database server connection.

If the Connect-It installation is on a different computer from the DDM Inventory Server, enter the DNS name or IP address of the DDM Inventory server before the colon. For example:

```
myserver.mycompany.com:8108
```

or

```
127.0.0.1:8108
```

2 **Login**

Enter the login required to interact with the Discovery database. In this case, enter admin.

The profile of this login must allow you to execute the actions performed by your scenario (reading data). You can enable this in the DDM Inventory Web UI (Click **Administration > MySQL accounts > Add an account**).

3 **Password**

Enter the password associated with the user login.

4 Click the **Test** button to test the connection to the Discovery database.

5 Click **Finish**.

Step 3: Configure the Destination Connector - AssetCenter

Click on the title bar of the Asset Management connector to highlight it. To configure the connector you can either:

- Right-click on the connector title bar and select the **Configure Connector...** option.
- Select the **Configure** option from the **Tools** menu.
- Press the **F2** key on your keyboard.

A wizard for the configuration of the Asset Management connector is displayed.

Page 1: Name and describe the connector

The first page of the wizard enables you to name the Asset Management connector and provide a description for it.

1 **Name:** By default, the value of this field is 'Asset Management'.

2 **Description**: Enter text to describe the connector. This field is not mandatory.

3 Click the **Next** button. The Define the connection parameters page opens.

Page 2: Define the connection parameters

This page allows you to set up the connection to your AssetCenter database.

1 **Server**

In the drop-down list, select the AssetCenter connection that you can access from your computer.

2 **Login**

Enter the login required to interact with AssetCenter.

The profile of this login must allow you to execute the actions performed by your scenario (reading and writing data).

3 **Password**

In this case (demo database) you do not need to enter a password.

4 Now test the connection to the database.

5 Click **Finish** to finalize the basic configuration of the connector.

Check Mappings

It is advised that you always check your field mappings before publishing the data to the AssetCenter database.

1 In the scenario diagram, double click on the **Mapping** box title bar. You will see a **Select a mapping** dialog box.

2 Double click on the **DevicesSrc-amComputerDst** entry. After a short time an **Edit mapping** window is displayed. This is where you can view and check your mappings.

➤ You may be asked whether you want to save the scenario. Click **Yes** to save.

3 Maximize this window to make it easier to see what is happening. There are three main panes in this window.

- **Source** - DDM Inventory - shows the Inventory document that is produced by Connect-It which contains the DDM Inventory structures, collections and fields as represented by Connect-It
- **Mapping** - shows the actual mappings between DDM Inventory and AssetCenter fields
- **Destination** - Asset Management - shows the AssetCenter documents, tables, structures, collections and fields that can be updated by the scenario.

4 In the Source pane expand the tree so that you can see the branches of the tree. You will notice that some of the entries are blue. This indicates that the field has been mapped to a field in the AssetCenter database.

Black entries have no mapping for them. However, you can choose to include a black field (i.e. one that doesn't have a mapping already) by manually creating the mapping yourself. This is covered in detail in the *Connect-It Users Guide*.

5 You can check what the mapping for a blue DDM Inventory field is by double clicking on it.

Now in the central Mapping pane an entry would have turned to green. Initially this may not be obvious, but scroll down the Mapping pane list to find it.

6 Double click on this mapping entry and the appropriate mapped AssetCenter field in the Destination - Asset Management pane will be automatically highlighted.

7 Do not close the mapping window yet.

Check Reconciliation Keys

Reconciliation is the integration of input data coming from DDM Inventory that is considered more up-to-date than the already existing data in AssetCenter.

This mechanism is based on the following question:

‘Does the information that I would like to reconcile already exist in AssetCenter?’

- If the answer is ‘no’, the input data is inserted. A new record is created because the field that was the reconciliation key was not found in AssetCenter.
- If the answer is “yes”, the existing data is updated with the information contained in the scan. The record is updated because Connect-It finds a match based on the fields that were used as the reconciliation keys.

Generally, reconciliation keys should be placed on unique fields in AssetCenter.

To view the fields that have reconciliation keys attached to them:

1 Look down the list of entries in the Mappings pane

2 Any entries that have a key icon next to them have reconciliation keys attached to them.

Mandatory Fields in an Asset Management Database

In an Asset Management application, a given field or link may be mandatory by default or have been customized this way by the administrator of the Asset Management application.

In the case of reconciliation, each structure published by the Asset Management application corresponds to a record. If an element in this structure is a mandatory field and is not populated, the structure is rejected.

Test DDM Inventory-AssetCenter Scenario

Before you actually produce documents and publish the data into the AssetCenter database you will want to test the scenario. By testing a scenario first you can ascertain that both the reading and mapping components are configured properly, before attempting to write to AssetCenter.

To enable this mode, select the **Scenario/Test mode** menu. You can choose between enabled (checked) and disabled (unchecked) values.

Starting the Scenario Test

To start the scenario test, do one of the following:

- Click the ▶ icon
- Select the **Produce Now** option from the **Tools** menu
- Press **F5** on your keyboard

You may be asked if you want to save the changes you have made. Click **Yes** to save the changes.

Consult the Document log to see if any problems were encountered while processing the documents produced by the DDM Inventory connector. Refer to the *Connect-It Users Guide* for more information about logs.

Getting Data into AssetCenter

Once you have made the initial check of the reading and mapping components, you can start checking the writing components. To do this, reset your selection in the **Scenario/Test mode** menu.

This step is where you actually populate your AssetCenter database with the data from DDM Inventory.

You can run the scenario in two ways: manually, or through the scheduler. For testing purposes, it is best to run it manually. To run it manually, press F5 or select **Produce Now** from the **Tools** menu.

Starting the Scheduler

Creating a schedule determines when your scenario's source connectors will process data.

The DDM Inventory connector produces Machine document-types every day from 9 A.M. to 10 P.M. at intervals of five minutes (this is the default schedule). Outside of this period, the DDM Inventory connector produces documents every hour.

You can add a rule to change these parameters for the days of your choice by using the Connect-It scheduler which is covered in the *Connect-It User's Guide*.

To start the scenario, do one of the following:

- Select Start all Schedulers from the Scenario menu.
- Click the ▶ button

Stopping the Scenario

To stop the scenario, do one of the following:

- Select **Stop** from the **Scenario** menu.
- Click the ■ button.

Analyze What Happened During the Process

You can see the processes that Connect-It goes through by clicking on the Connect-It log tab in the Scenario builder.

In the log, each action is represented by an icon. An action's message can be composed of several sub-messages that detail the action. These sub-messages can, themselves, be composed of other sub-messages. Each message is dated according to when the action was launched.

You can unfold or collapse messages by right-clicking and then selecting the appropriate command from the shortcut menu.

Right click anywhere in this log pane and select Collapse all levels. Now you are left with the basic actions that were carried out. Expand an action to see what happened in further detail.

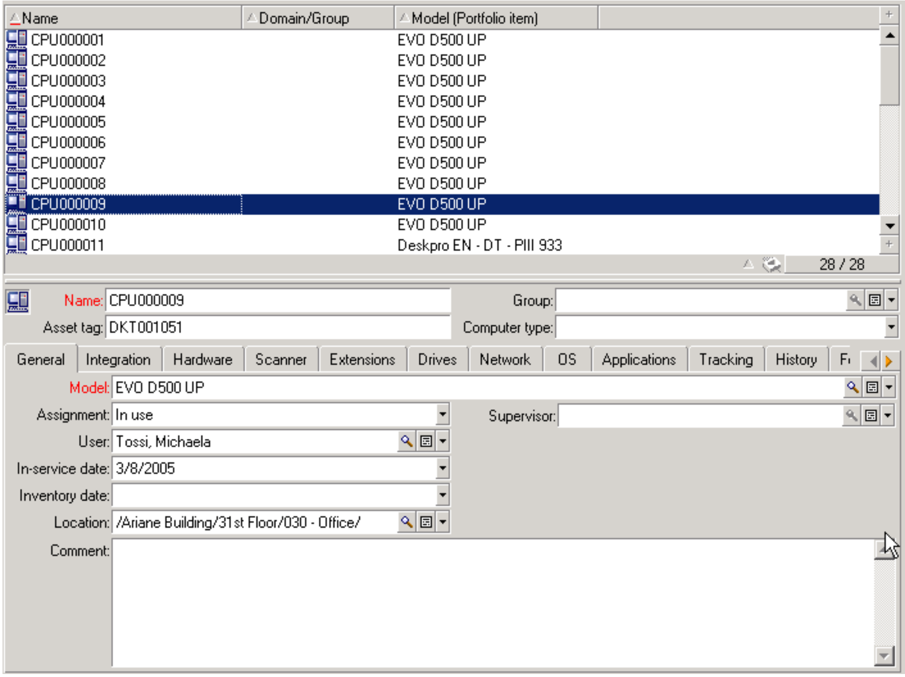
See Results in AssetCenter

1 Start AssetCenter

2 Log into the database

3 Click on the **Computers** toolbar button

You will see that your data from the DDM Inventory scans has been populated into fields in the **Computers** tab in the AssetCenter database.



Name	Domain/Group	Model (Portfolio item)
CPU000001		EVO D500 UP
CPU000002		EVO D500 UP
CPU000003		EVO D500 UP
CPU000004		EVO D500 UP
CPU000005		EVO D500 UP
CPU000006		EVO D500 UP
CPU000007		EVO D500 UP
CPU000008		EVO D500 UP
CPU000009		EVO D500 UP
CPU000010		EVO D500 UP
CPU000011		Deskpro EN - DT - PIII 933

28 / 28

Name: CPU000009
Asset tag: DKT001051
Group:
Computer type:

Model: EVO D500 UP
Assignment: In use
Supervisor:
User: Tossi, Michaela
In-service date: 3/8/2005
Inventory date:
Location: /Ariane Building/31st Floor/030 - Office/
Comment:

For further information on what you can do with this data, refer to the AssetCenter documentation.

Customize Your Scenario

You can configure a connector of your own or you can modify the existing scenarios to better match your data needs.

Refer to the Connect-It documentation for information about these customization options and tasks.

Importing and Processing DDM Inventory Utilization Data in AssetCenter

➤ This section only applies if you have purchased the DDM Inventory Software Utilization license.

In Enterprise Discovery 2.1 and later, Utilization data has been expanded to specify “per computer” data and “per user” data. This means that the data is broken down based on each user on each device, so you can see who uses specific applications.

Besides regular users, you can also see “All Users” and “System” user data, that collect total utilization for the device, and also utilization for all system process that can not be associated with a specific user.

Index