

# HP OpenView Enterprise Discovery

Software Version: 2.1

---

## Configuration and Customization Guide

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



## Legal Notices

### Warranty

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

The information contained herein is subject to change without notice.

### Restricted Rights Legend

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

### Copyright Notices

© Copyright 1993-2006 Hewlett-Packard Development Company, L.P.

### Trademark Notices

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

# Contents

1	Introduction	9
2	Setting up Accounts	11
	About accounts	11
	Demo accounts	14
	IT Employee accounts	14
	IT Manager accounts	14
	Administrator accounts	15
	Scanner accounts	15
	Aggregator accounts	15
	Setting up Accounts	16
	Generating a list of accounts	16
	Adding an account	16
	Customizing an account's properties	17
	Modifying account contact information	20
	Modifying an account password	20
	Deleting an account	21
	Maintaining Your Account	23
	Testing your e-mail address	23
	Testing your pager address	23
3	Working with SNMP Traps	25
	Installing SNMP Package on your Enterprise Discovery server	25
	Enterprise Discovery Notifications	25
	deviceEvent Notification	25
	portEvent Notification	27
4	Setting up Event Filters	31
	Interactions that affect Event Filters	32
	What is an Event Filter?	33
	Preparing Enterprise Discovery for Event Filters	34
	Event Filter Properties	35
	Examples of common Event Filters	37
	Example 1: Notification when a core device breaks	37
	Example 2: Notification when a router is dropping a lot of traffic	40
	Example 3: Notify me when a line to an important device has long delays	42
	Modifying a filter	45
	Deleting a filter	46
	Listing Event Filters	46

Resetting to Defaults . . . . .	46
<b>5 Adding, Removing, and Replacing Devices . . . . .</b>	<b>47</b>
The importance of unique IP addresses . . . . .	48
Adding a device . . . . .	48
With a new IP address . . . . .	48
With the same IP Address as an active device . . . . .	49
With the same IP Address as a deactivated device. . . . .	49
Replacing a device . . . . .	49
With an identical device . . . . .	49
With a different device . . . . .	49
Changing the IP address of a device . . . . .	50
Changing the cards or ports in a device . . . . .	50
Removing Devices . . . . .	51
Removing devices automatically . . . . .	51
Removing devices manually . . . . .	53
Removing Stale Connections . . . . .	55
Activating devices . . . . .	56
<b>6 Exporting Data into Data Access Applications . . . . .</b>	<b>57</b>
Step 1: Set up your MySQL Account. . . . .	58
Step 2: Install the MySQL ODBC driver . . . . .	58
Step 3: Select MYSQL as the data source (create an ODBC alias). . . . .	58
Step 4: Create a new database in Microsoft Access 2000 . . . . .	60
Step 5: Link in the Enterprise Discovery tables . . . . .	60
Step 6: Create a basic assets and recognition query . . . . .	63
Step 7: Create a basic license query . . . . .	65
<b>7 Deleting Data and Connections . . . . .</b>	<b>67</b>
Deleting data . . . . .	67
Deleting connections . . . . .	69
<b>8 Changing Alarm Thresholds . . . . .</b>	<b>71</b>
Device Types. . . . .	71
Line Alarm Types. . . . .	72
Copying alarm thresholds . . . . .	73
<b>9 Changing Device and Port Properties . . . . .</b>	<b>75</b>
Customizing for IT Manager and Administrator accounts. . . . .	75
Changing Device Properties . . . . .	76
Changing Port Properties . . . . .	78
<b>10 Configuring your Scanner Settings . . . . .</b>	<b>79</b>
AutoSequence Number . . . . .	80
Minimum scanner execution retry frequency. . . . .	81
Maximum scanner upgrade attempts. . . . .	81
Initial time to wait between scanner upgrade attempts (in case of failure). . . . .	81
Initial time to wait between retrieve scan files attempts (in case of failure). . . . .	81

Maximum scanfile download attempts . . . . .	82
Scanner Versions . . . . .	82
Scanner File Names . . . . .	83
<b>11 Agent Communication Configuration . . . . .</b>	<b>85</b>
Supported platforms for discovery agents . . . . .	85
Agent security . . . . .	86
Agent Media files . . . . .	86
Agent Directories . . . . .	87
Initial Agent Deployment . . . . .	87
Deployment via old listener . . . . .	87
Deployment via Win32 RPC . . . . .	88
Custom Deployment . . . . .	89
Step-by-step automatic deployment instructions . . . . .	90
Deployment via login scripts . . . . .	90
Manual Deployment . . . . .	90
Upgrading the Agent . . . . .	91
Upgrading a Win32 Agent . . . . .	91
Upgrading a UNIX Agent . . . . .	91
Step-by-step agent upgrade instructions . . . . .	92
Uninstalling the agent . . . . .	92
Step-by-step agent uninstall instructions . . . . .	92
Uninstalling the old listener . . . . .	93
Step-by-step old listener uninstall instructions . . . . .	93
Software Utilization . . . . .	94
Agent Communication Configuration . . . . .	95
<b>12 Scanner Generator . . . . .</b>	<b>99</b>
The Scan File Formats . . . . .	99
The Components of a Scanner . . . . .	100
Information the Scanners Can Collect . . . . .	101
Hardware and Configuration Information . . . . .	101
Software Information . . . . .	101
User or Asset information . . . . .	102
Supported Platforms . . . . .	102
Starting the Scanner Generator . . . . .	103
Exiting the Scanner Generator . . . . .	103
The Scanner Generator User Interface . . . . .	104
Navigation Between the Pages . . . . .	104
The Scanner Generator Pages . . . . .	104
The Scenario Page . . . . .	105
The Standard Configuration Page . . . . .	106
Enterprise Mode . . . . .	106
Manual Deployment Mode . . . . .	107
The Collection Page . . . . .	109
Selecting the Type of Data to Be Collected . . . . .	109

The Hardware Data Page . . . . .	110
Disabling Specific Hardware Detection Routines . . . . .	111
The Software Data Page . . . . .	114
Selecting a Preset Software Scanning Mode . . . . .	114
Enabling the Command Line Override Option . . . . .	116
The Drives Tab . . . . .	117
Selecting a Predefined Type of Drive to Scan . . . . .	117
The Drive Selection Tab . . . . .	119
Creating a Customized Drive Selection . . . . .	119
Overriding Scanner Generator Settings with Override Files . . . . .	121
File Systems . . . . .	121
Directories and Files . . . . .	122
The Directories Tab . . . . .	123
Selecting the Directories to Scan . . . . .	123
The File Scanning Tab . . . . .	125
Files to Scan Sub Tab . . . . .	125
File Identification Sub Tab . . . . .	128
File Information to Store Sub Tab . . . . .	130
The Stored Files Tab . . . . .	134
File Name to Store Column . . . . .	135
Found Where Column . . . . .	136
The Asset Data Page . . . . .	138
The Asset Data Tab . . . . .	138
The Asset Data Form Layout . . . . .	138
The Asset Field Configuration Dialog Box . . . . .	140
Setting Up a New Asset Field . . . . .	140
The Asset Number Tab . . . . .	156
Asset Number Definition . . . . .	156
The Source for the Asset Number . . . . .	156
The Scanner Options Page . . . . .	157
The Saving Tab . . . . .	158
Saving Local and Offsite Scan Files . . . . .	158
Saving Results Locally . . . . .	158
Saving Results to Network (Offsite) . . . . .	159
Setting Up the Creation of a Log File . . . . .	162
The Settings Tab . . . . .	163
Defining how fast the Scanner should run . . . . .	164
Setting Time-Out Options . . . . .	164
The Miscellaneous Tab . . . . .	165
The Troubleshooting Tab . . . . .	167
Additional command line parameters to supply to the scanner . . . . .	167
Additional content for .override.ini file . . . . .	167
The Scanners to Generate Page . . . . .	168
The Output Options Tab . . . . .	169
Setting Up a Scanner Description . . . . .	169
Saving Scanner Options to a Text File . . . . .	169

Naming the Configuration (.cxz) File .....	170
The Scanners Tab. ....	171
Selecting which Scanners to Generate .....	171
Specifying the Base Scanner File Name and Output Directory .....	171
Setting Naming Conventions for the Scanners.....	172
The Generating Scanners Page.....	173
<b>13 XML Enricher .....</b>	<b>175</b>
The XML Enricher Directory Structure .....	177
Processing Normal Scan Files .....	179
Processing Delta Scan Files .....	180
Delta Calculation Command Line Utility .....	180
Application Utilization Data .....	181
Log Files .....	182
Application Recognition in XML Enricher .....	182
Configuring the XML Enricher using the Web UI .....	184
Process utilization data .....	184
Application Recognition .....	184
Generate MIF Files.....	185
Automatically Defer All New Scans.....	185
Merge Priority .....	185
Managing Scan Files .....	186
Updating the application library used by the Enricher .....	187
Configuring the XML Enricher Using XML Enricher.ini .....	187
The XML Enricher ini File Sections .....	187
RecognitionConfig Section .....	187
RecognitionConfig.RecognitionConfig_cfgJunk Filters Section .....	189
RecognitionConfig.RecognitionConfig_cfgSAIFiles Section .....	190
AssetFieldConfig Section .....	190
Starting and stopping the XML Enricher service in the web UI .....	191
Structure of the Enriched XSF File .....	191
An Example of How the data is stored .....	192
<b>14 Getting Your Data into AssetCenter.....</b>	<b>195</b>
Assumptions.....	195
Where to find the Connect-It scenario .....	195
Prerequisites .....	196
Compatibility .....	196
Prepare AssetCenter .....	196
Prepare Connect-It.....	196
Step 1: Open the scenario.....	197
Step 2: Configure the Source Connector - Enterprise Discovery .....	197
Step 3: Configure the Destination Connector - AssetCenter .....	199
Check your mappings.....	201
Check the reconciliation keys .....	202
Mandatory fields in an Asset Management database.....	202
Test your Enterprise Discovery-AssetCenter Scenario .....	202

Starting the scenario test . . . . .	203
Get the data into AssetCenter . . . . .	203
Starting the scheduler . . . . .	203
Stopping the scenario . . . . .	203
Analyze what happened during the process . . . . .	204
See the results in AssetCenter . . . . .	204
Customize your scenario . . . . .	205
Importing and processing Enterprise Discovery 2.1 Utilization Data in AssetCenter . . . . .	205
<a href="#">Index</a> . . . . .	207



# 1 Introduction

This guide will help you configure and customize the components of Enterprise Discovery™ to your own specifications.

Topics in this guide include:

- Accounts for access to the web interface (administration, reports device managers, etc.)
- How devices are added to and deleted from the Enterprise Discovery database
- Device and Port Properties
- Agent Communication and Configuration
- Scan File Configuration
- Scanner Generator for creating Scanners
- XML Enricher for adding data to scan files
- How to get your data into AssetCenter



## 2 Setting up Accounts

All Enterprise Discovery 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, Enterprise Discovery 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 Enterprise Discovery, 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, Peregrine recommends that there be only one Enterprise Discovery Administrator.

**Table 1    Default Accounts**

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

**Table 2 Account Access to Enterprise Discovery**

	Demo	IT Employee	IT Manager	Administrator
<b>Network Map</b>				
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	—	—	✓	✓
Alarm Thresholds	view	view	view + change	view + change
Purge a device	—	—	✓	✓
Disconnect other accounts' map sessions	—	—	—	✓
<b>Managers (for example, Device Manager)</b>				
View read and write community strings for device	—	—	✓	✓
View and use <i>set</i> link to MIB Browser	—	—	✓	✓
SNMP query default string	"public"	"public"	from Enterprise Discovery	from Enterprise Discovery
Update Model	—	—	✓	✓
Configure connections	—	—	✓	✓
Break and force connections	—	—	✓	✓
Agent and Scan logs	—	—	✓	✓

**Table 2 Account Access to Enterprise Discovery**

	Demo	IT Employee	IT Manager	Administrator
<b>MIB Browser</b>				
Set SNMP variables	—	—	✓	✓
Read community string	—	view + edit	view + edit	view + edit
Write community string	—	—	view + edit	view + edit
<b>Status</b>				
View read and write community strings for network	—	—	✓	✓
<b>Administration</b>				
Change own password	—	✓	✓	✓
Configure own account	—	✓	✓	✓
Configure other accounts	—	—	—	✓
Manage own map configurations	—	✓	✓	✓
Copy map configurations from other accounts	—	✓	✓	✓
Select pager service provider	—	✓	✓	✓
Configure pager service provider	—	—	—	✓
Configure event filters	—	—	—	✓
Configure Enterprise Discovery server	—	—	—	✓
Configure network operations	—	—	—	✓

## Demo accounts

Initially, there is one Demo account. The name for this account is “demo” and the password is “demo” (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 Enterprise Discovery. 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 Enterprise Discovery.

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 Enterprise Discovery sees connections between objects, and break existing connections and create custom connections
- Set SNMP variables in the MIB Browser

## Administrator accounts

There should be one Administrator account owner designated as the Enterprise Discovery 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 Enterprise Discovery server.

An Administrator account can:

- do everything that IT Manager accounts can do
- perform initial configuration of the Enterprise Discovery server
- configure the Enterprise Discovery server operations on the network
- administer the IT Manager, IT Employee and Demo accounts

The default Administrator account must set up the initial Enterprise Discovery 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 Peregrine Systems 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.

## 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*.

# Setting up Accounts

This section is for the Enterprise Discovery 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 Successful Login Time	Last Failed Login Time	Login Failure Count	Web and Applet Access
admin	Administrator	Administrator	n/a	2006-04-11 15:26:07	2006-04-11 15:37:08	0	Yes
demo	Demo	Demo Account	n/a	n/a	n/a	0	Yes
itemployee	IT Employee	IT Employee	n/a	n/a	n/a	0	Yes
itmanager	IT Manager	IT Manager	n/a	n/a	n/a	0	Yes

## Adding an account

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



In Enterprise Discovery, 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, Peregrine recommends that there be only one Enterprise Discovery 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 not be able to log in with it.

Account name:

## Customizing an account's 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 Enterprise Discovery.
Web and Applets access	Determines if the user can access the web and applet components of the Enterprise Discovery user interface.
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.
Long date format	Determines how the date appears at the bottom of most panels and pages.

**Table 3 Account Properties**

<b>Property</b>	<b>Explanation</b>
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 Enterprise Discovery: 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 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:	IT Employee ▼		
Web and applets access:	<input checked="" type="radio"/> Yes <input type="radio"/> No		
Password expiry:	Days: <input type="text" value="0"/>		

---

Name:	<input type="text"/>		
Allow others to copy map configurations?:	<input type="radio"/> Yes <input checked="" type="radio"/> No		
Append IP Address to device titles?:	<input type="radio"/> Yes <input checked="" type="radio"/> No		
Make URLs visible?:	<input type="radio"/> Yes <input checked="" type="radio"/> No		
Alternate colors in table rows?:	<input checked="" type="radio"/> Yes <input type="radio"/> No		
Highlight table rows on mouse over?:	<input type="radio"/> Yes <input checked="" type="radio"/> No		

---

Time before marking statistic as stale:	Days: <input type="text" value="0"/>	Hours: <input type="text" value="2"/>	Minutes: <input type="text" value="0"/>	Seconds: <input type="text" value="0"/>
Long date format:	<input type="text" value="%A, %B %e, %Y %T %Z"/> default: %A, %B %e, %Y %T %Z			
Short date format:	<input type="text" value="%Y-%m-%d %R"/> default: %Y-%m-%d %R			

---

Default Home Page:	Default ▼
Device Manager scan file viewer:	Java ▼
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:	<input type="text" value="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 Enterprise Discovery 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.



E-mail address:

Pager e-mail address:

## 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 > Account administration > 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.

Password:  
  
 Password (again):

## 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**.



Account name:  
Select Account ▼  
Delete Account

## 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 an account's properties](#) on page 17)
- Changing your password (see [Modifying an account password](#) on page 20)
- [Testing your e-mail address](#) on page 23
- [Testing your pager address](#) on page 23

## 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 Enterprise Discovery 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 provided
- an incorrect e-mail address is provided
- a mail server has not been specified for use with Enterprise Discovery
- the receiving mail server is not working

## Testing your pager address

Testing your pager address will send a message to your pager, so that you can:

- test that you have entered your pager address correctly
- test that the Enterprise Discovery 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 a message to your pager, click **Confirm**.

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

- incorrect pager data is provided in the pager service provider profile
- no pager data is provided in your account profile
- incorrect pager data is provided in your account profile

- no external modem is connected to the Enterprise Discovery server
- the external modem connected to the Enterprise Discovery server is turned off
- there are modem synchronization problems
- there is no dial tone on the phone line being used
- your service provider is having problems
- your pager is turned off



## 3 Working with SNMP Traps

Peregrine Enterprise Discovery 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](#)). Peregrine Enterprise Discovery 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 Enterprise Discovery server (this is the default install location):

```
C:\Program Files\Peregrine\Enterprise Discovery\2.1.0\events\mibs
```

### Installing SNMP Package on your Enterprise Discovery server

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

To install this software:

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

### Enterprise Discovery Notifications

Peregrine Enterprise Discovery 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: .1.3.6.1.4.1.1467.100.100.2.1) contains the following members:

**Table 1 deviceEvent Notification**

Order	Object	Type	Description
1	serverID .1.3.6.1.4.1.1467.100.100.1.1	Integer	ServerID is an integer that has been configured by the administrator of the Peregrine Enterprise Discovery server; it is 1 by default. The ServerID makes it easier for consumers of the inventory to correlate devices managed by different Peregrine Enterprise Discovery servers.
2	eventID .1.3.6.1.4.1.1467.100.100.1.2.1	Unsigned32	Increasing sequence number associated with this event. This object is present for compatibility only. It is always blank.
3	datetime .1.3.6.1.4.1.1467.100.100.1.2.2	Octet String	Date and time when event occurred (YYYYMMDD HH:MM:SS).
4	category 1.3.6.1.4.1.1467.100.100.1.2.3	Integer	For a complete list of possible events, see <b>Help &gt; Classifications &gt; Supported Device/Port Attributes</b> , and select the appropriate <i>Internal Name</i> . For example, for “Bytes In”, select <b>in_bytes</b>
5	state .1.3.6.1.4.1.1467.100.100.1.2.4	Integer	Alarm state of the event: info (Add, Delete, PropertyChange, ConnectionChange) na-ok, na-info, na-minor, na-major, na-critical, ok-na, ok-info, ok-minor, ok-major, ok-critical, info-na, info-ok, info-minor, info-major, info-critical, minor-na, minor-ok, minor-info, minor-major, minor-critical, major-na, major-ok, major-info, major-minor, major-critical, critical-na, critical-ok, critical-info, critical-minor, critical-major.
6	deviceNMID .1.3.6.1.4.1.1467.100.100.1.2.5.1	Unsigned32	Network Manager Identification
7	deviceType .1.3.6.1.4.1.1467.100.100.1.2.5.2	Unsigned32	The device type (Icon).
8	deviceTag .1.3.6.1.4.1.1467.100.100.1.2.5.3	Octet String	The name of the device.
9	macAddress .1.3.6.1.4.1.1467.100.100.1.2.5.4	Physical Address	The MAC address associated with the device.

**Table 1 deviceEvent Notification**

Order	Object	Type	Description
10	ipv4Address .1.3.6.1.4.1.1467.100.100.1.2.5.5	IP Address	The IPv4 address associated with the device (if any).
11	deviceTitle .1.3.6.1.4.1.1467.100.100.1.2.5.6	Octet String	The (network map) title of the device as defined by the appliance administrator.
12	priority .1.3.6.1.4.1.1467.100.100.1.2.5.7	Integer	The priority of the device as defined by the appliance administrator: 1, 2, 3, 4, 5 or 6.
13	direction .1.3.6.1.4.1.1467.100.100.1.2.7	Integer	Direction of port that triggered event: notAvailable, in, out.
14	value .1.3.6.1.4.1.1467.100.100.1.2.8	Octet String	Value of threshold variable that triggered event. Value is not present where it makes no sense, for e.g. categories break, add, or delete.
15	units .1.3.6.1.4.1.1467.100.100.1.2.9	Integer	The unit of the Value. Units always appear whenever Value does. Can be one of: notAvailable, count, day, persec, percent, hour, unknown.

## 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 device versus those that correspond to a device, see the *Reference Guide*.

The portEvent event (OID: .1.3.6.1.4.1.1467.100.100.2.2) contains the following members:

**Table 2 portEvent Notification**

Order	Object	Type	Description
1	serverID .1.3.6.1.4.1.1467.100.100.1.1	Integer	ServerID is an integer that has been configured by the administrator of the Peregrine Enterprise Discovery server; it is 1 by default. The ServerID makes it easier for consumers of the inventory to correlate devices managed by different Peregrine Enterprise Discovery servers.
2	eventID .1.3.6.1.4.1.1467.100.100.1.2.1	Unsigned32	Increasing sequence number associated with this event. This object is present for compatibility only. It is always blank.

**Table 2 portEvent Notification**

3	datetime .1.3.6.1.4.1.1467.100.100.1.2.2	Octet String	Date and time when event occurred (YYYYMMDD HH:MM:SS).
4	category .1.3.6.1.4.1.1467.100.100.1.2.3	Integer	For a complete list of possible events, see <b>Help &gt; Classifications &gt; Supported Device/Port Attributes</b> , and select the appropriate <i>Internal Name</i> . For example, for “Bytes In”, select <b>in_bytes</b>
5	state .1.3.6.1.4.1.1467.100.100.1.2.4	Integer	Alarm state of the event: info (Add, Delete, PropertyChange, ConnectionChange) na-ok, na-info, na-minor, na-major, na-critical, ok-na, ok-info, ok-minor, ok-major, ok-critical, info-na, info-ok, info-minor, info-major, info-critical, minor-na, minor-ok, minor-info, minor-major, minor-critical, major-na, major-ok, major-info, major-minor, major-critical, critical-na, critical-ok, critical-info, critical-minor, critical-major.
6	deviceNMID .1.3.6.1.4.1.1467.100.100.1.2.5.1	Unsigned32	Network Manager Identification
7	deviceType .1.3.6.1.4.1.1467.100.100.1.2.5.2	Unsigned32	The device type (Icon).
8	deviceTag .1.3.6.1.4.1.1467.100.100.1.2.5.3	Octet String	The name of the device.
9	macAddress .1.3.6.1.4.1.1467.100.100.1.2.5.4	Physical Address	The MAC address associated with the device.
10	ipv4Address .1.3.6.1.4.1.1467.100.100.1.2.5.5	IP Address	The IPv4 address associated with the device (if any).
11	deviceTitle .1.3.6.1.4.1.1467.100.100.1.2.5.6	Octet String	The (network map) title of the device as defined by the appliance administrator.
12	priority .1.3.6.1.4.1.1467.100.100.1.2.5.7	Integer	The priority of the device as defined by the appliance administrator: 1, 2, 3, 4, 5 or 6.
13	portNMID .1.3.6.1.4.1.1467.100.100.1.2.6.1	Unsigned32	Network Manager Identification.

**Table 2 portEvent Notification**

14	portIndex .1.3.6.1.4.1.1467.100.100.1.2.6.2	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.
15	ifSpeed .1.3.6.1.4.1.1467.100.100.1.2.6.3	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.
16	ifType .1.3.6.1.4.1.1467.100.100.1.2.6.4	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.
17	duplex .1.3.6.1.4.1.1467.100.100.1.2.6.5	Integer	The duplex of port within the device: full, half, or non-applicable.
18	connectedToDevice .1.3.6.1.4.1.1467.100.100.1.2.6.6	Unsigned32	The NMID of the remote device this port connects to.
19	connectedToPort .1.3.6.1.4.1.1467.100.100.1.2.6.7	Unsigned32	The NMID of the port on the remote device this port connects to.
20	alarmType .1.3.6.1.4.1.1467.100.100.1.2.6.8	Unsigned32	The alarm type for this port.
21	direction .1.3.6.1.4.1.1467.100.100.1.2.7	Integer	Direction of port that triggered event: notAvailable, in, out.
22	value .1.3.6.1.4.1.1467.100.100.1.2.8	Octet String	Value of threshold variable that triggered event. Value is not present where it makes no sense, for e.g. categories break, add, or delete.
23	units .1.3.6.1.4.1.1467.100.100.1.2.9	Integer	The unit of the Value. Units always appear whenever Value does. Can be one of: notAvailable, count, day, persec, percent, hour, unknown.



## 4 Setting up Event Filters

[Setting up Event Filters](#) is for Administrator accounts only.

You can configure Enterprise Discovery to notify you when events occur. Enterprise Discovery can notify you by e-mail, 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 that affect Event Filters](#) on page 32
- [What is an Event Filter?](#) on page 33
- [Preparing Enterprise Discovery for Event Filters](#) on page 34
- [Examples of common Event Filters](#) on page 37
- [Modifying a filter](#) on page 45
- [Deleting a filter](#) on page 46
- [Listing Event Filters](#) on page 46
- [Resetting to Defaults](#) on page 46

## Interactions that affect 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 1 Prerequisites**

Concept	Commands and where to get more information
<b>E-mail Issues</b>	
Set up your SMTP server	<b>Administration &gt; Appliance Management &gt; SMTP Server.</b> See the <i>Installation and Initial Setup Guide</i> .
<b>Events Issues</b>	
Understand the types of events recorded by Enterprise Discovery	See the <i>Reference Guide</i> .
<b>Hardware Issues</b>	
Set up and test your pager equipment (hardware and software)	
<b>Account Issues</b>	
Set up account contact information	<b>Administration &gt; Account administration &gt; Account properties.</b>
<b>Network Map Issues</b>	
Change device priorities	<a href="#">Changing Device and Port Properties</a> on page 75
Changing alarm thresholds	<a href="#">Changing Alarm Thresholds</a> on page 71

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 Enterprise Discovery can notify you in the following ways:

- send an e-mail
- send an alphanumeric page
- 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

Enterprise Discovery has two default event filters. You can create your own through **Administration > Event Filters**.

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.

You can also add a “notification delay.” This means that when an event occurs, Enterprise Discovery will wait the specified amount of time before notifying the user. Sometimes, events will be rectified on their own. If the problem is automatically rectified within the notification delay period, the user will not be notified.

**Table 2    Default Event Filters**

Default Event Filter	Description
email-admin-device	Send e-mail to the “admin” account <sup>a</sup> when a device of priority 6 breaks.
email-admin-line	Send e-mail to the “admin” account <sup>a</sup> 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 Enterprise Discovery, you should have changed these default event filters.

# Preparing Enterprise Discovery 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 Enterprise Discovery:
  - SMTP server
  - SNMP traps setup (only if you plan to use SNMP traps)
  - Pager setup (hardware installation and pager service provider information)
- 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 numbers.
  - Test their e-mail addresses and pager numbers to make sure they are working.
- Make sure you have set the system-level priority for your important devices.
- Set up the proper alarm thresholds.

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 3    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	<p>You have a choice of several types of events for which you want to receive notification.</p> <ul style="list-style-type: none"><li>• All (all of the categories listed below)</li><li>• Attributes (when an attribute is in an alarmed state, all of which are available in the second list in the Event Filter menu: Load Average, CPU, Memory, etc.)</li><li>• Adds (when a device is added in your specified IP range)</li><li>• Deletes (when a device is deleted in your specified IP range)</li><li>• 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)</li><li>• 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 <i>Port Moves</i> event in the Health Panel)</li></ul> <p>Note: The safest and easiest way to make sure you get your event notification is to select the <i>All</i> 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.</p>
Attribute Group	If you have chosen <i>Attributes</i> as your Event Type, you can choose one of these attribute groups.
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.

**Table 3    Event Filter Properties**

Property	Explanation
State Transition	<p>If you want to be notified about specific state transitions, you can select them here. Click one state in the <i>From</i> category, and one from the <i>To</i> category and click <b>Add</b>.</p> <p>Note: The “Info” transition comprises Adds and Deletes</p>
IPv4 Range	<p>Enter a range of IPv4 addresses in which you want to be notified of this event.</p>
Notification	<p>Notifications must include an action, and can include an account. You can also add a <i>Delay</i>, so if the event corrects itself within the Delay period, no notification will be sent.</p> <ul style="list-style-type: none"><li>• send e-mail</li><li>• send alphanumeric page via e-mail gateway</li><li>• send SNMP trap data</li><li>• create an XML file</li></ul>

## Examples of common Event Filters

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 1: Notification when a core device breaks

A core device can be any important device in your network. For example, you may consider a particular type of ATM Switch to be very important, and you may want to know when that device is broken. For this example, we will set up an event filter that will page an Administrator account when this type of ATM Switch goes down.

Before you start the procedure, make sure the following has all been done properly:

- Your pager equipment has been installed and configured.
- Your pager service provider information is correct and up to date.

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 the correct pager information:
  - Pager number or Pager e-mail address
  - Pager service provider
- 5 Click **Modify Contact Data**.

To set the device priority:

- 1 Open a Network Map session.
- 2 Find your core device and select it.
- 3 Click **Object > Device Properties**.
- 4 In the Device Properties window, make this device priority 6.
- 5 Click **Apply**.
- 6 Click **OK**.

You have now changed the priority of your core device to 6.

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 4 Example 1 Input**

<b>Field</b>	<b>Enter:</b>
Name (create a name for the filter)	core_device_broken
Description	Page administrator when core device breaks
Event Type	Attribute
Attribute Group	Breaks
Priority	6
Device Type	ATM Switch
Transitions	OK to Minor, OK to Major, OK to Critical, Minor to Major, Minor to Critical, Major to Critical
IPv4 Range	Select the devices or IP range you want this event filter to monitor
Alphanumeric Page	Select the Administrator account

- 3 You can have Enterprise Discovery delay the notification by entering a time in the Delay section of the notification table.
- 4 Click **Add Filter**.

Name: core\_device\_broken  
Description: Page the administrator when a core device breaks

#### Selection Criteria

Event Type:	Attribute Group:	Priority:	Device Type:
<input type="checkbox"/> All <input checked="" type="checkbox"/> Attribute <input type="checkbox"/> Adds <input type="checkbox"/> Deletes <input type="checkbox"/> Moves	<input type="checkbox"/> All <input type="checkbox"/> Disk <input type="checkbox"/> Packet Loss <input checked="" type="checkbox"/> Breaks <input type="checkbox"/> Backplane Utilization	<input type="checkbox"/> All <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input checked="" type="checkbox"/> 6	<input type="checkbox"/> All <input type="checkbox"/> Enterprise Switch Layer 2 or below <input checked="" type="checkbox"/> ATM Switch <input type="checkbox"/> Ethernet/100 Hub <input type="checkbox"/> FDDI

State Transition:	From State	To State	Action	StateTransition	
	n/a Ok Info Minor Major Critical	--> n/a Ok Info Minor Major Critical	<input type="button" value="Add"/> <input type="button" value="Remove"/>	OK to Minor OK to Major OK to Critical Minor to Major Minor to Critical Major to Critical	<input type="button" value="Select All"/>

#### Add by Interval

Starting IPv4 Address:   
Ending IPv4 Address:

IPv4 Range:

#### Add by Subnet

IPv4 Address:   
Netmask:

#### Added IPv4 Ranges

172.22.1.253 to 172.22.1.253 (1 devices)

#### Notification

E-mail:	<input type="checkbox"/> admin (Administrator) <input type="checkbox"/> aggregator <input type="checkbox"/> demo (Demo Account)	Delay: Hours: <input type="text"/> Minutes: <input type="text"/> Seconds: <input type="text"/>
Alphanumeric Page (via e-mail gateway):	<input checked="" type="checkbox"/> admin (Administrator) <input type="checkbox"/> aggregator <input type="checkbox"/> demo (Demo Account)	Delay: Hours: <input type="text"/> Minutes: <input type="text"/> Seconds: <input type="text"/>
SNMP Trap:	<input type="text"/>	Delay: Hours: <input type="text"/> Minutes: <input type="text"/> Seconds: <input type="text"/>
Xml:	<input type="radio"/> On <input checked="" type="radio"/> Off	Delay: Hours: <input type="text"/> Minutes: <input type="text"/> Seconds: <input type="text"/>
<input type="button" value="Add Filter"/>		

## Example 2: Notification when a router is dropping a lot of traffic

This example shows how to create an event filter that will notify you (or someone else with an Administrator account) by e-mail message when your priority 6 routers have packet loss alarms.

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 the correct e-mail address.
- 5 Click **Modify Contact Data**.

To set the device priority:

- 1 Open a Network Map session.
- 2 Find your Router and select it.
- 3 Click **Object > Device Properties**.
- 4 In the Device Properties window, make this device priority 6.
- 5 Click **Apply**.
- 6 Click **OK**.

If you want to set this up for several routers, then repeat these steps for each router. Note their IPv4 addresses if you want to specify the IPv4 range.

- 7 Set the Packet Loss thresholds by clicking **Edit > Alarm Thresholds**.
- 8 Click **Apply**.
- 9 Click **OK**.

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 5 Example 2 Input**

Field	Enter:
Name (create a name for the filter)	routers_dropping_traffic
Description	E-mail me when routers are dropping a lot of traffic
Event Type	Attribute
Attribute Group	Packet Loss
Priority	6
Transitions	OK > Minor, OK > Major, OK > Critical, Minor > Major, Minor > Critical, Major > Critical



**Table 5 Example 2 Input**

Field	Enter:
Device Type	Router
E-mail	select the Administrator account
IPv4 Range	Select the devices or IP range you want this event filter to monitor

**3 Click Add Filter.**

Name:

Description:

**Selection Criteria**

Event Type: ☐ All ☒ Attribute ☐ Adds ☐ Deletes ☐ Moves

Attribute Group: ☐ All ☐ DISK ☒ Packet Loss ☐ Breaks ☐ Backplane Utilization

Priority: ☐ All ☐ 3 ☐ 4 ☐ 5 ☒ 6

Device Type: ☐ All ☐ Discovery Server ☐ Cloud ☒ Router ☐ Workstation

**State Transition:**

From State	To State	Action	StateTransition
n/a	n/a	Add	OK to Minor
Ok	Ok		OK to Major
Info	Info		OK to Critical
Minor	Minor		Minor to Major
Major	Major		Minor to Critical
Critical	Critical	Remove	Major to Critical

Select All

**Add by Interval**

Starting IPv4 Address:

Ending IPv4 Address:  Add

**Add by Subnet**

IPv4 Address:

Netmask:  Add

**Added IPv4 Ranges**

172.22.1.79 to 172.22.1.251 (173 devices)  
172.22.2.2 to 172.22.5.56 (823 devices)

Delete

**Notification**

E-mail: ☒ admin (Administrator) ☐ aggregator ☐ demo (Demo Account)

Delay: Hours:  Minutes:  Seconds:

Alphanumeric Page (via e-mail gateway): ☐ admin (Administrator) ☐ aggregator ☐ demo (Demo Account)

Delay: Hours:  Minutes:  Seconds:

SNMP Trap:

Delay: Hours:  Minutes:  Seconds:

Xml: ☐ On ☒ Off

Delay: Hours:  Minutes:  Seconds:

Add Filter

## Example 3: Notify me when a line to an important device has long delays

This example demonstrates how to set up an event filter that will e-mail you when a line has delay alarms. Line event filters are a little more complex than device event filters, because you must select both a device, and the type of line connected to that device. For this example, we will use a server connected to a half duplex Ethernet line of 10Mbps or less (Ethernet 10< HD).

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 the correct e-mail address.
- 5 Click **Modify Contact Data**.

To set the device priority:

- 1 Open a Network Map session.
- 2 Find your server and select it.
- 3 Click **Object > Device Properties**.
- 4 In the Device Properties window, make this Server priority 6.  
Lines get their priority from the highest priority devices they connect. By making this device a priority 6, the lines attached to it are automatically a priority 6.
- 5 Click **Apply**.
- 6 Click **OK**.  
If you want to be paged for several servers, repeat steps 2-6 for each server.
- 7 Set the Line Alarm thresholds by clicking **Edit > Alarm Thresholds**.
- 8 Click **Apply**.
- 9 Click **OK**.

To set up the Event Filter:

- 1 Click **Administration > Event filter configuration > Add a line filter**.
- 2 Enter the event filter information as it appears in this table:

**Table 6 Example 3 Input**

Field	Enter:
Name (create a name for the filter)	server_delays
Description	E-mail me when server lines have Delay alarms
Event Type	Attribute
Attribute Group	Delays

**Table 6    Example 3 Input**

<b>Field</b>	<b>Enter:</b>
Priority	6
Device Type	Server
Line Alarm Type	Ethernet 10< HD
Transitions	OK > Minor, OK > Major, OK > Critical, Minor > Major, Minor > Critical, Major > Critical
E-mail	select the Administrator account
IPv4 Range	Select the devices or IP range you want this event filter to monitor

3    Click **Add Filter**.

Name: server\_delays

Description: e-mail me when server lines have delay alarms

#### Selection Criteria

Event Type:	Attribute Group:	Priority:	Device Type:	Line Alarm Type:
<input type="checkbox"/> All <input checked="" type="checkbox"/> Attribute <input type="checkbox"/> Adds <input type="checkbox"/> Deletes <input type="checkbox"/> Moves	<input type="checkbox"/> All <input type="checkbox"/> Data Delivery Ratio <input type="checkbox"/> Frame Delivery Ratio <input checked="" type="checkbox"/> Delay <input type="checkbox"/> Line Utilization	<input type="checkbox"/> All <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input checked="" type="checkbox"/> 6	<input type="checkbox"/> All <input type="checkbox"/> unmapped IP <input type="checkbox"/> Unknown NCD <input checked="" type="checkbox"/> Server <input type="checkbox"/> Printer	<input type="checkbox"/> All <input type="checkbox"/> Generic HD <input type="checkbox"/> Generic FD <input checked="" type="checkbox"/> Ethernet 10< HD <input checked="" type="checkbox"/> Ethernet 10< FD

State Transition:	From State	To State	Action	StateTransition	Select All
	n/a Ok Info Minor Major Critical	--> n/a Ok Info Minor Major Critical	Add Remove	OK to Minor OK to Major OK to Critical Minor to Major Minor to Critical Major to Critical	

#### Add by Interval

Starting IPv4 Address:

Ending IPv4 Address:

Add

#### Added IPv4 Ranges

172.22.1.79 to 172.22.1.251 (173 devices)  
172.22.2.2 to 172.22.2.56 (55 devices)

Delete

IPv4 Range:

#### Add by Subnet

IPv4 Address:

Netmask:

Add

#### Notification

E-mail:	<input checked="" type="checkbox"/> admin (Administrator) <input type="checkbox"/> aggregator <input type="checkbox"/> demo (Demo Account)	Delay: Hours: <input type="text"/> Minutes: <input type="text"/> Seconds: <input type="text"/>
Alphanumeric Page (via e-mail gateway):	<input type="checkbox"/> admin (Administrator) <input type="checkbox"/> aggregator <input type="checkbox"/> demo (Demo Account)	Delay: Hours: <input type="text"/> Minutes: <input type="text"/> Seconds: <input type="text"/>
SNMP Trap:	<input type="text"/>	Delay: Hours: <input type="text"/> Minutes: <input type="text"/> Seconds: <input type="text"/>
Xmi:	<input type="radio"/> On <input checked="" type="radio"/> Off	Delay: Hours: <input type="text"/> Minutes: <input type="text"/> Seconds: <input type="text"/>
<input type="button" value="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 Attribute Group list box.
- 3 Select one or more options from the Priority list box.
- 4 Select one or more options from the Device Type list box.
- 5 Select one or more options from the Line Alarm list box.
- 6 Select one or more options from the State Transitions 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
  - Alphanumeric Page (through e-mail gateway)
  - SNMP Trap

To modify filter:

- 1 Click **Modify Filter**.



Enterprise Discovery 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.**
- 2 Click a filter name hyperlink.

Device Event Filters

Name	Event Type	Attribute Group	Priority	Device Type	State Transition	IP Range	Notification	Notification Delay
email-admin-device	Attribute	Breaks	6	All	All		Send email to account 'admin'	Email: 0 seconds
Send email to admin on priority 6 device break events.								

Line Event Filters

Name	Event Type	Attribute Group	Priority	Device Type	State Transition	Line Alarm Type	IP Range	Notification	Notification Delay
email-admin-line	Attribute	Breaks	6	All	All	All		Send email to account 'admin'	Email: 0 seconds
Send email to admin on priority 6 line break events.									

## 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:

- [The importance of unique IP addresses](#) on page 48
- [Adding a device](#) on page 48
- [Replacing a device](#) on page 49
- [Changing the IP address of a device](#) on page 50
- [Changing the cards or ports in a device](#) on page 50
- [Removing Devices](#) on page 51
- [Activating devices](#) on page 56

## The importance of unique IP addresses

Enterprise Discovery 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. Enterprise Discovery 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 Enterprise Discovery 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.

## With a new IP address

Once you have added a device to your network, Enterprise Discovery 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 Enterprise Discovery 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 Enterprise Discovery 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 Network**.
- 6 Click **Update**.

Enterprise Discovery begins network discovery on the device immediately.



## With the same IP Address as an active device

If 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.”

## With the same IP Address as a deactivated device

If a device has been deactivated (either manually by the user, or automatically by Enterprise Discovery), 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 Enterprise Discovery), there will be a “duplicate IP address” exception. At that point, the newly reactivated device will remain active, and the other device will be deactivated.

## 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 an identical device

If you are replacing one device with another of the same model, and the same MAC address, Enterprise Discovery will see no difference between the two devices. Enterprise Discovery 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 a 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 the 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 Enterprise Discovery sees the network. Read the following notes to make sure you understand how Enterprise Discovery reacts.

- If you change the IP of the device, but the MAC remains the same, the Enterprise Discovery database updates automatically.
- If you change the IP of a port, Enterprise Discovery 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 the cards or ports in a device

If you change all the cards in a device (and they have all new MAC addresses), Enterprise Discovery 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, Enterprise Discovery rediscovers the device as if it were new.

## Removing Devices

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

**Table 1 Automatic and Manual Device Removal**

Method	Performed by	How it works
automatic	Enterprise Discovery	3 stages <ul style="list-style-type: none"><li>• deactivate</li><li>• purge</li><li>• obliterate</li></ul>
manual	an IT Manager or Administrator user	3 methods <ul style="list-style-type: none"><li>• hide</li><li>• deactivate</li><li>• purge</li></ul>

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

**Table 2 Hide, Deactivate, and Purge**

Action	Hide	Deactivate	Purge	Obliterate <sup>a</sup>
device removed from Network Map	✓	✓	✓	✓
device can be recovered if seen	—	✓	✓ <sup>b</sup>	— <sup>b</sup>
“delete” event generated	✓	✓	✓	—
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 Enterprise Discovery 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 Enterprise Discovery 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 Enterprise Discovery keeps depends on your license. For example, if you have a 10,000 device license, with 8,000 active devices in your network, Enterprise Discovery 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, Enterprise Discovery will not save any purged devices in its database.

## Changing the device expiry intervals

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

### Changing the expiry intervals

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.

Device Deactivation Intervals		
Managed devices deactivation interval:	<input checked="" type="radio"/> Default:	8 weeks 0 days 0 hours
	<input type="radio"/> Custom:	Weeks: <input type="text" value="8"/> Days: <input type="text" value="0"/> Hours: <input type="text" value="0"/>
Unmanaged devices deactivation interval:	<input checked="" type="radio"/> Default:	1 week 0 days 0 hours
	<input type="radio"/> Custom:	Weeks: <input type="text" value="1"/> Days: <input type="text" value="0"/> Hours: <input type="text" value="0"/>
Scanner-only devices deactivation interval:	<input checked="" type="radio"/> Default:	12 weeks 0 days 0 hours
	<input type="radio"/> Custom:	Weeks: <input type="text" value="12"/> Days: <input type="text" value="0"/> Hours: <input type="text" value="0"/>
Device Purge Intervals		
Managed devices purge interval:	<input checked="" type="radio"/> Default:	4 weeks 0 days 0 hours
	<input type="radio"/> Custom:	Weeks: <input type="text" value="4"/> Days: <input type="text" value="0"/> Hours: <input type="text" value="0"/>
Unmanaged devices purge interval:	<input checked="" type="radio"/> Default:	4 weeks 0 days 0 hours
	<input type="radio"/> Custom:	Weeks: <input type="text" value="4"/> Days: <input type="text" value="0"/> Hours: <input type="text" value="0"/>
Scanner-only devices purge interval:	<input checked="" type="radio"/> Default:	4 weeks 0 days 0 hours
	<input type="radio"/> Custom:	Weeks: <input type="text" value="4"/> Days: <input type="text" value="0"/> Hours: <input type="text" value="0"/>
Device Obliteration Interval		
Device obliteration interval:	<input checked="" type="radio"/> Default:	52 weeks 0 days 0 hours
	<input type="radio"/> Custom:	Weeks: <input type="text" value="52"/> Days: <input type="text" value="0"/> Hours: <input type="text" value="0"/>

To change the expiry intervals:

- 1 Click **Administration > System Configuration > Expiry**.
- 2 Enter the time values deactivation, purge, and obliteration.
- 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
- apply to the device a Network Property Group or Set with the property, “Allow devices” set to “Off” (**Administration > Network Configuration > Network Property Groups**)



If a device has multiple IP addresses, all of them must be entered.

- 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 the device expiry intervals](#) on page 52), Enterprise Discovery automatically takes appropriate action.



If you change the address ranges in **Network 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 56.

### 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 in the Enterprise Discovery IP range. 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 Enterprise Discovery 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. Enterprise Discovery will stop monitoring the device's statistics. If the device is rediscovered by Enterprise Discovery, 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. Enterprise Discovery will start monitoring this device again.



You can re-activate devices if they have been deactivated or hidden by Enterprise Discovery, or by an Administrator.

For information on how to Hide, Purge, or Deactivate devices, see [Removing Devices](#) on page 51.

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 Enterprise Discovery 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 Enterprise Discovery 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](http://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 Enterprise Discovery 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](#) on page 58
- [Step 2: Install the MySQL ODBC driver](#) on page 58
- [Step 3: Select MYSQL as the data source \(create an ODBC alias\)](#) on page 58
- [Step 4: Create a new database in Microsoft Access 2000](#) on page 60
- [Step 5: Link in the Enterprise Discovery tables](#) on page 60
- [Step 6: Create a basic assets and recognition query](#) on page 63
- [Step 7: Create a basic license query](#) on page 65

## 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 Enterprise Discovery 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 the 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://www.mysql.com/products/connector/odbc/>

In this example we have downloaded version 3.51 of the MYSQL Connector/ODBC driver.

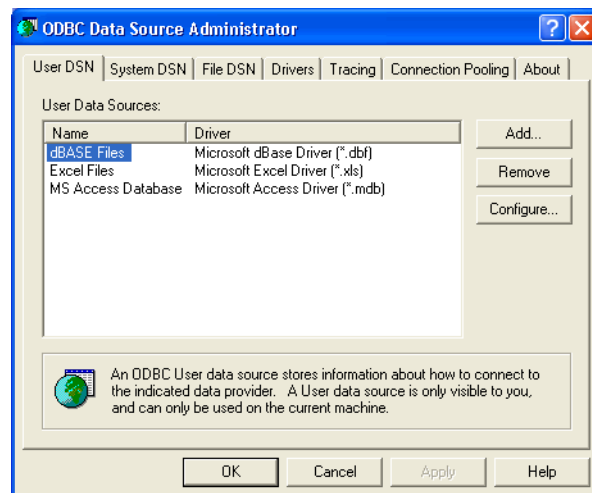
## Step 3: Select MYSQL as the data source (create an ODBC alias)

Before you can use the Enterprise Discovery data with Microsoft Access you need to create an ODBC alias for the database.

To set up MySQL as the data source

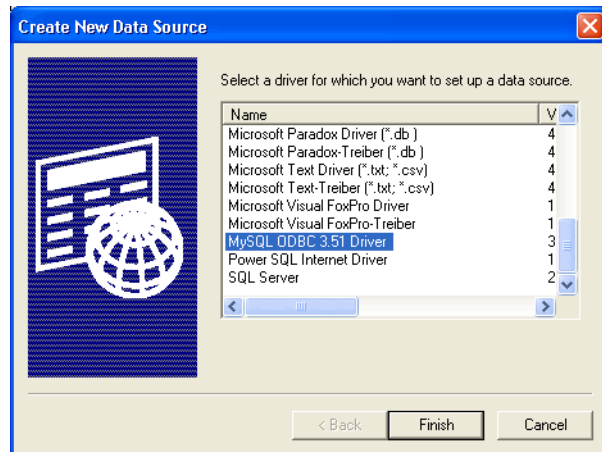
- 1 From the Windows **Control Panel**, select **Administrative Tools|Data Sources (ODBC)**.

The **ODBC Data Source Administrator** appears.



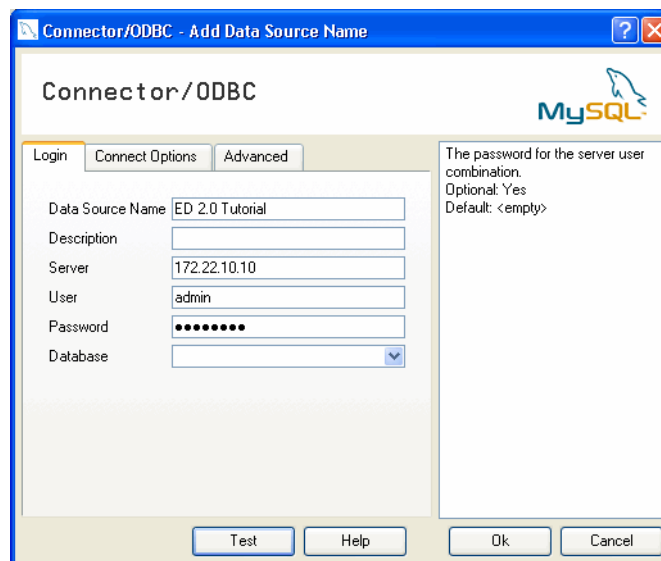
- 2 In the **User DSN** tab, click **Add**.

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



- 3 In the list box select **MySQL ODBC**.
- 4 Click **Finish**.

The **Connector/ODBC - Add Data Source Name** dialog appears.



- 5 Enter the following information:
  - The Windows Data Source Name (DSN). In the following example we have called it **ED Tutorial**.
  - The name or IP address of the Enterprise Discovery server.
  - 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 Click on the **Connect Options** tab. For the number of the port, always enter **8108**.
- 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 Enterprise Discovery database with applications such as MS Access by means of ODBC.

## Step 4: Create a new database in Microsoft Access 2000

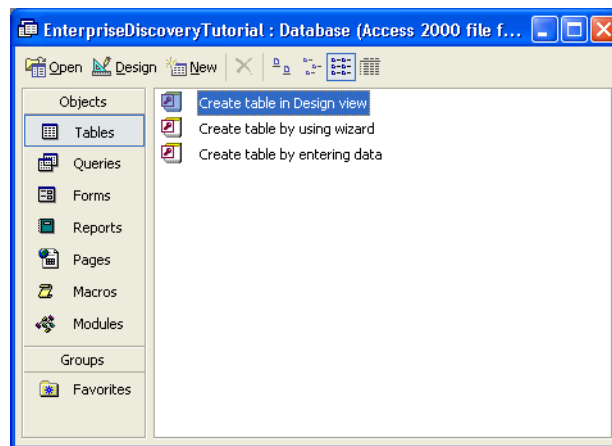
To create a new database

- 1 Start Microsoft Access.
- 2 Create a new blank database. Give it a name and save it.

The following screen is displayed. In this example, the database has been named **EnterpriseDiscoveryTutorial.mdb** and saved in the following directory

C:\Program Files\HP OpenView\Enterprise Discovery\2.1.0\Common

The following dialog is displayed.



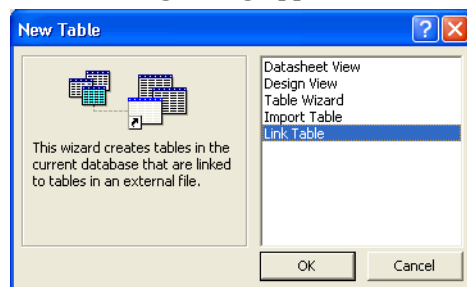
## Step 5: Link in the Enterprise Discovery tables

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

To link in the Enterprise Discovery tables

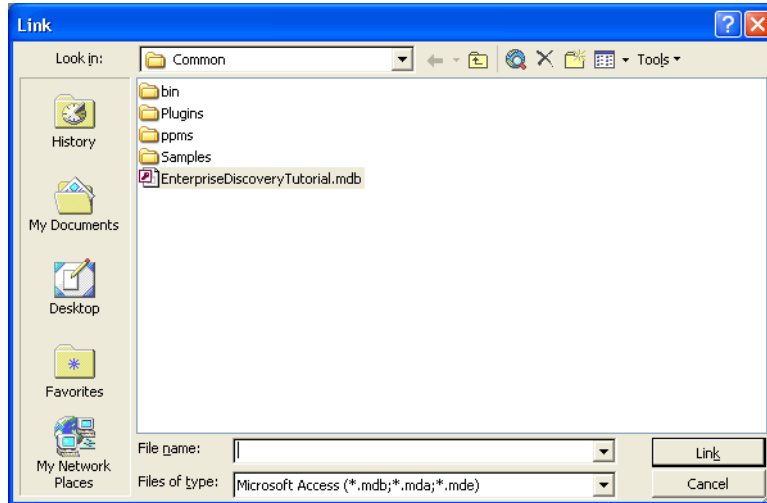
- 1 In the Objects menu, select **Tables** and click **New**.

The following dialog appears.



- 2 Select **Link Table** and click **OK**.

The following screen appears.

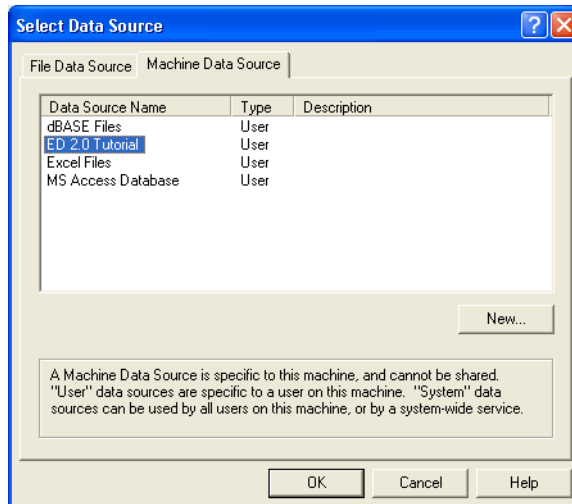


- 3 In the **Files of type** pull-down list, select **ODBC Databases**.

The following dialog appears.

➤ The **EnterpriseDiscoveryTutorial.mdb** file is not supplied with Enterprise Discovery, but is the file that you created in [step 2](#) on page 60.

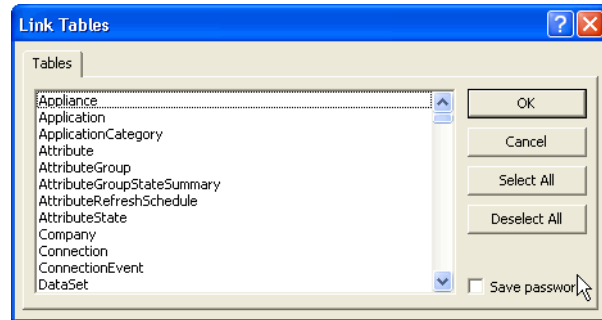
- 4 Click the **Machine Data Source** tab.



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

➤ This is the Tutorial data source name that you created in [step 5](#) on page 59.

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

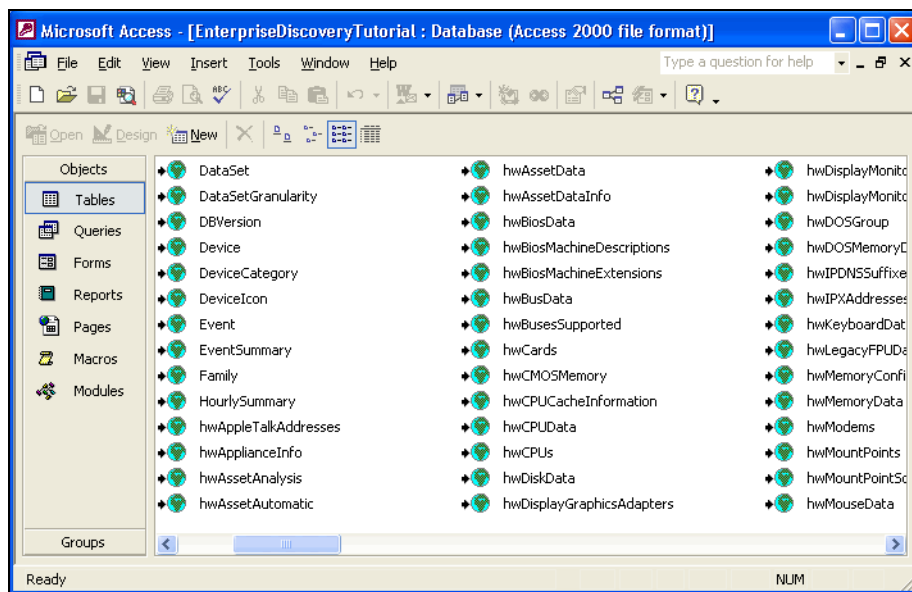


- 6 Click **Select All**.

All the entries are now highlighted.

- 7 Click **OK**.

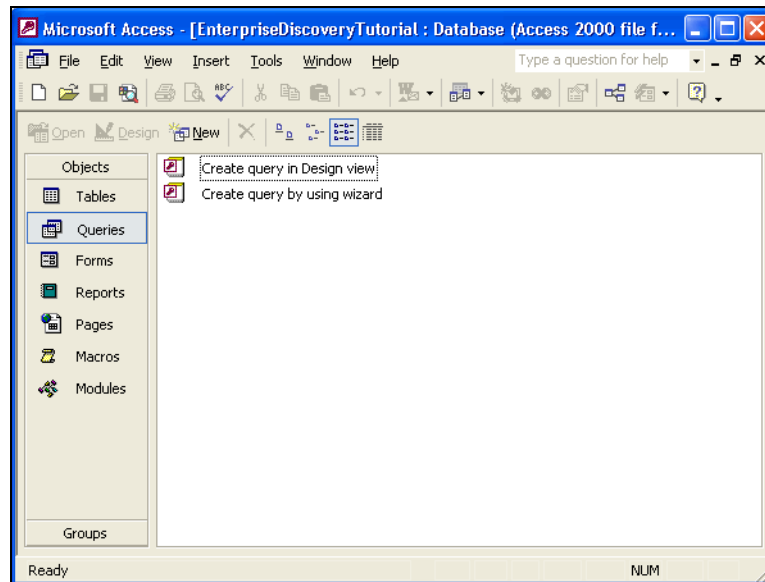
You are returned to the **Tables** Tab which shows the newly linked Enterprise Discovery tables.



## Step 6: Create a basic assets and recognition query

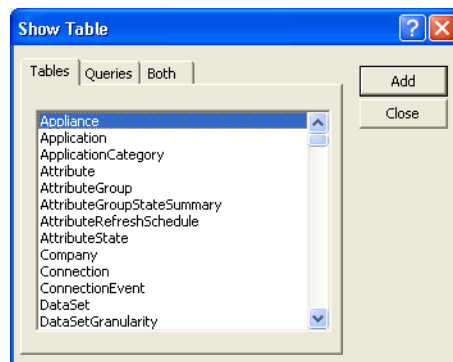
To create a basic assets and recognition query

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



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

The **Show Table** dialog appears.



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

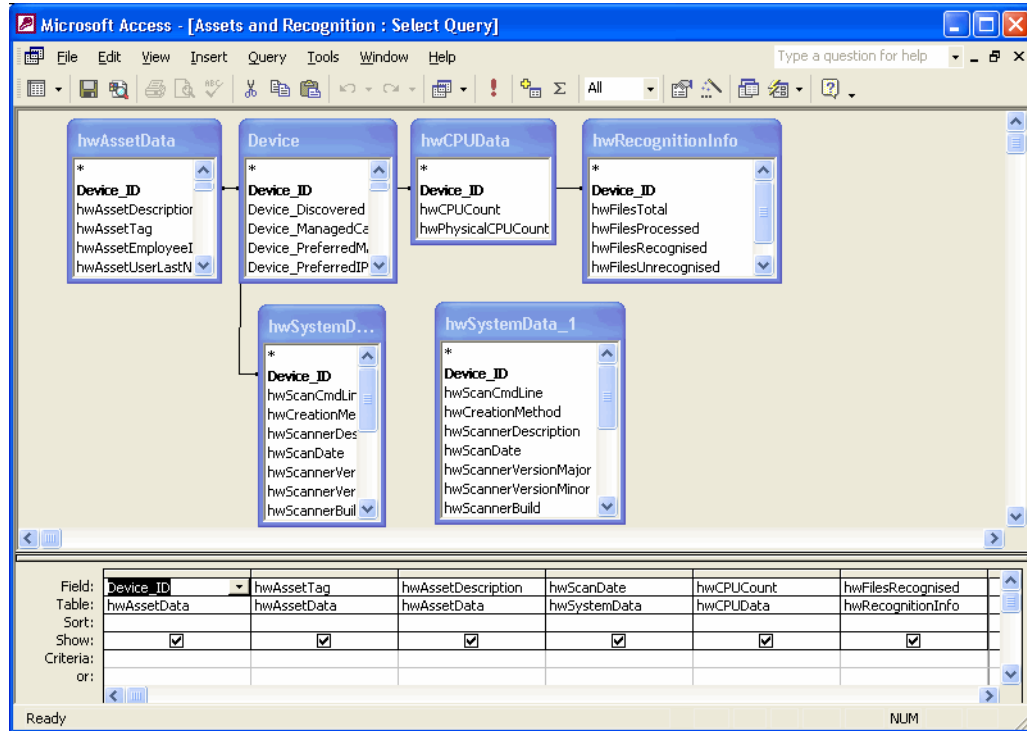
- hwAssetData
- Device
- hwCPUData
- hwRecognitionInfo
- hwSystemData

- 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:



- 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.

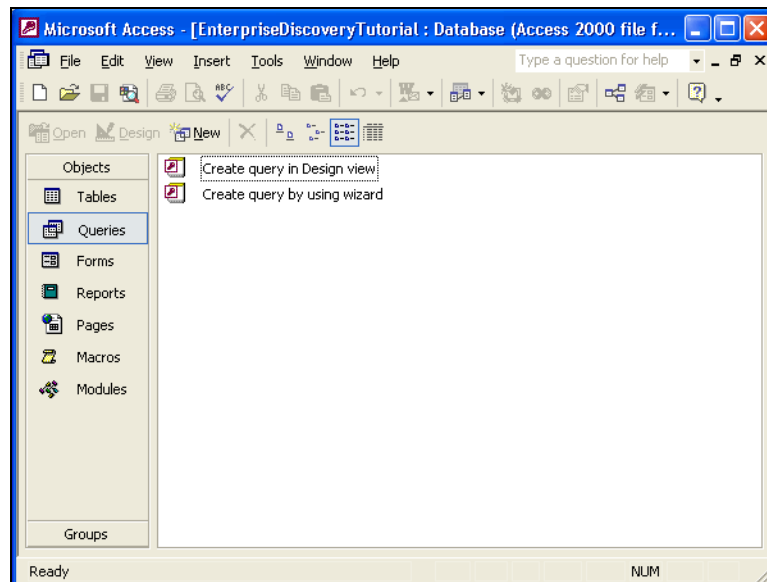
Device_ID	hwAssetTag	hwAssetDescription	hwScanDate	hwCPUCount	hwFilesRecognised
56	0010F3043879	0010F3043879 - Pentium III, 700MHz, 128Mb	i/2005 23:40:28	1	0
58	Windows_2000_Professiona	Windows_2000_Professional 7895 - Pentium III, 700MHz, 128Mb	i/2005 23:39:48	1	0
59	0010F30437F6	0010F30437F6 - Pentium III, 700MHz, 128Mb	i/2005 22:02:20	1	0
60	78Y0099	78Y0099 - Pentium III, 1133MHz, 1280Mb	i/2005 00:29:51	1	0
61	0010F30437CE_Nex01-16	0010F30437CE_Nex01-16 - Pentium III, 700MHz, 128Mb	i/2005 22:38:10	1	0
62	0010F304372D	0010F304372D - Pentium III, 700MHz, 128Mb	i/2005 23:38:56	1	0
66	6118FCM4A100	() - Pentium III, 866MHz, 512Mb	i/2005 14:57:20	1	2105
67	0010F3043874	0010F3043874 - Pentium III, 700MHz, 128Mb	i/2005 23:40:58	1	0
68	0010F304385C	0010F304385C - Pentium III, 700MHz, 128Mb	i/2005 23:42:23	1	0
69	0010F304389D	0010F304389D - Pentium III, 700MHz, 128Mb	i/2005 23:37:08	1	0
70	0010F304B044	0010F304B044 - Pentium III, 1200MHz, 128Mb	i/2005 04:58:01	1	0
72	0010F304388C	0010F304388C - Pentium III, 700MHz, 128Mb	i/2005 02:00:46	1	0
73	0010F3043757	0010F3043757 - Pentium III, 700MHz, 128Mb	i/2005 23:10:56	1	0
74	0010F3043780_Nex10-04	0010F3043780_Nex10-04 - Pentium III, 700MHz, 128Mb	i/2005 17:41:36	1	0
75	0010F304B030	0010F304B030 - Pentium III, 1200MHz, 128Mb	i/2005 23:18:18	1	0
76	KCMC1FW	KCMC1FW - Pentium 4, 3000MHz, 1536Mb	i/2005 08:51:03	2	0
77	6107FCM4A173	6107FCM4A173 - Pentium III, 866MHz, 256Mb	i/2005 17:13:55	1	0
165	0010F30437E1	0010F30437E1 - Pentium III, 700MHz, 128Mb	i/2005 04:27:33	1	0
172	0010F30437ED	0010F30437ED - Pentium III, 700MHz, 128Mb	i/2005 23:32:37	1	0
176	0010F30438C8	0010F30438C8 - Pentium III, 700MHz, 128Mb	i/2005 02:04:33	1	0
179	NEX03-01	NEX03-01 - Pentium III, 700MHz, 128Mb	i/2005 10:19:04	1	0
182	0010F3043778	0010F3043778 - Pentium III, 700MHz, 128Mb	i/2005 23:38:44	1	0



## Step 7: Create a basic license query

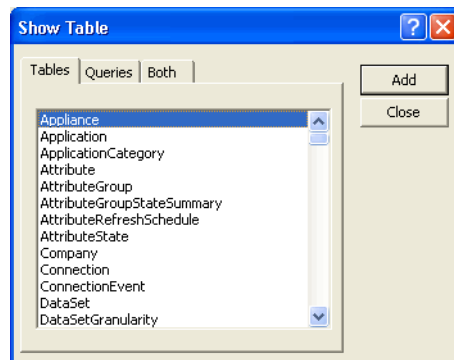
To create a basic license query

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



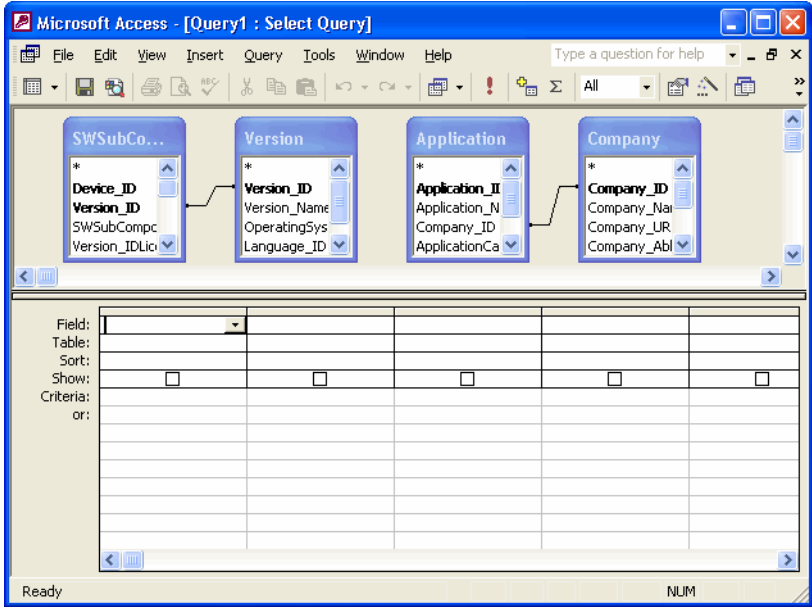
- 2 Double click **Create query in Design view**.

The **Show Table** dialog appears.

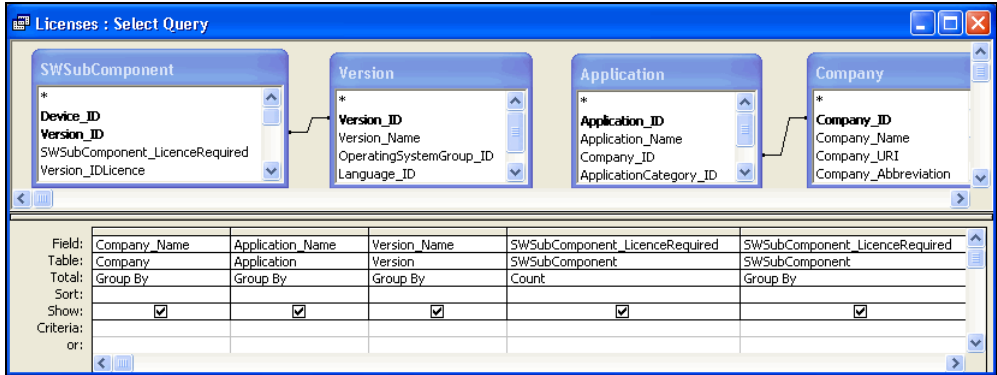


- 3 In the **Tables** tab page, select:
  - Company.Company\_Name
  - Release.Release\_Name
  - SWSubComponent.SWSubComponent\_LicenceRequired
  - Version.Version\_Name
  - Application.Application\_Name
- 4 With the table selected, click **Add**, then **Close**.

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:



- 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.

## 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, Enterprise Discovery 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 Enterprise Discovery.



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 1 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 1 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	—	—	✓
Network Configuration (IP ranges, Property Groups, 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 <sup>a</sup>	—	—	✓

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

To delete Enterprise Discovery 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**.

## 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 Enterprise Discovery and those defined by the user
- just the connections defined by the user

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



You can potentially lose all the connectivity data Enterprise Discovery 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, Enterprise Discovery 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**.

☐ All  
☒ User-defined only  
**Delete Connections**



## 8 Changing Alarm Thresholds

This section is for IT Manager and Administrator accounts.

Enterprise Discovery generates alarms of different severity depending on where you set the thresholds.

The Alarm Thresholds feature lets you set alarm levels for all the functions that Enterprise Discovery monitors. Any changes to the Alarm Thresholds apply globally to all accounts.

You can access the Alarm Thresholds menu from any map window. Click **Edit > Alarm Thresholds**. You can check all your alarm thresholds at **Status > Current Settings > Device alarm thresholds/Line alarm thresholds**.

There are a few important notes you should know before you start changing alarm thresholds:

- One alarm value can be associated with multiple ranges. For example, you can apply a Critical alarm range if your line utilization is too high or too low.
- You do not need to cover the entire range of possible values. you can only create thresholds for the levels you care about
- You can clean alarms with the “Alarm State Timeout” in **Administration > System Preferences > Network Devices**.

### Device Types

Enterprise Discovery initially sets all thresholds to default values. If a value of a threshold has not been set for a device type, the default will be used.

**Alarm Thresholds - Server**

**Threshold Selection**

Attribute: Breaks

Line alarm type:

Device type: ATM Switch

**Threshold Values**

☒ Default ☐ Custom

Low	High	State
1	1	▲
2	2	◆

Units: none

Copy Paste

Add Remove

Apply OK Cancel

### To change the Device Alarm Thresholds

- 1 Select a device attribute from the pull-down list.  
The **Device type** list is enabled.
- 2 Select a device type by clicking an icon from the pull-down list.
- 3 To change an alarm threshold, click a text box and enter a new number for the low or high value.
- 4 To create a new alarm threshold, click the **Add** button and a new row will appear.
- 5 To change the State of any alarm, click the box in the State column, and select the new state from the list that appears.
- 6 Click **Apply** or **OK**.

If the values for different states overlap, a warning message will appear, and the affected values will be highlighted in red.

## Line Alarm Types

Enterprise Discovery initially sets all threshold values to default values. If a value of a threshold has not been set for a line type, the default will be used.

**Alarm Thresholds - Server**

Threshold Selection

Attribute:

Line alarm type:

Device type:

Threshold Values

☒ Default ☐ Custom

Low	High	State
45	65	▲
65	+	◆

Units: %

### To change the Line Alarm Thresholds

- 1 Select a line attribute from the pull-down list.  
The **Line alarm type** list is enabled.
- 2 Select a line alarm type from the pull-down list.
- 3 To change an alarm threshold, click a text box and enter a new number for the low or high value.
- 4 To create a new alarm threshold, click the **Add** button and a new row will appear.



- 5 To change the State of any alarm, click the box in the State column, and select the new state from the list that appears.
- 6 Click **Apply** or **OK**.

If the values for different states overlap, a warning message will appear, and the affected values will be highlighted in red.

## Copying alarm thresholds

If you wish to use the same alarm threshold values for different device or line types, you can use the **Copy** and **Paste** buttons.

### To copy alarm thresholds

- 1 Select the custom alarm threshold setting you want to duplicate.
- 2 Click **Copy**.
- 3 Select an attribute from the pull-down list.
- 4 Select a line or device type from the pull-down list.
- 5 Click **Paste**.

The alarm thresholds you selected in step 1 will now appear in the custom area of the Alarm Thresholds dialog for the newly selected attribute and device/line alarm type.

- 6 Click **Apply** to apply the changes.
- 7 Click **OK** to close the dialog.



## 9 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 1 Properties**

To change	Do this	Affects other accounts and maps	Also affects
icon—devices	see <a href="#">Changing Device Properties</a> on page 76	✓	<ul style="list-style-type: none"><li>• thresholds (all accounts)</li><li>• whether event filters are applied (all accounts)</li><li>• reports</li></ul>
icon—packages	see the <i>Network Data Analysis Guide</i>	—	—
tag	<a href="#">Changing Device Properties</a> on page 76	—	—
derived title (devices)	see <b>Administration &gt; System Configuration &gt; Display preferences</b>	✓	—
title	see <a href="#">Changing Device Properties</a> on page 76	✓	—
priority (devices)	see <a href="#">Changing Device Properties</a> on page 76	✓	whether event filters are applied (all accounts)
to top object	see the <i>Network Data Analysis Guide</i>	—	—

# 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**.

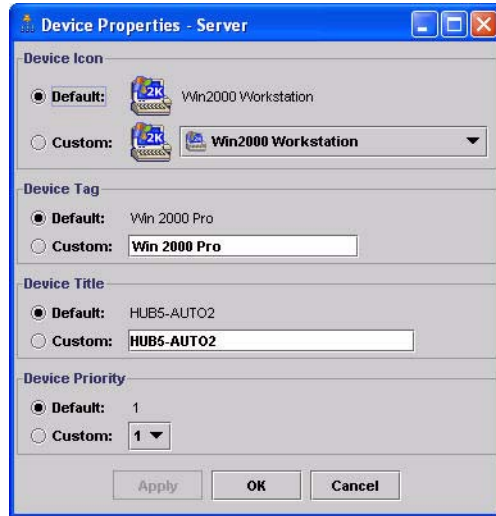
You might increase the priority of a device that is important to you or a device that you will want to monitor more closely. Devices with priority 6 are the most important. The higher the number, the higher the priority and the greater the importance.

To change these 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, Enterprise Discovery will register a change event in the Events Browser.



To reset the 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**.

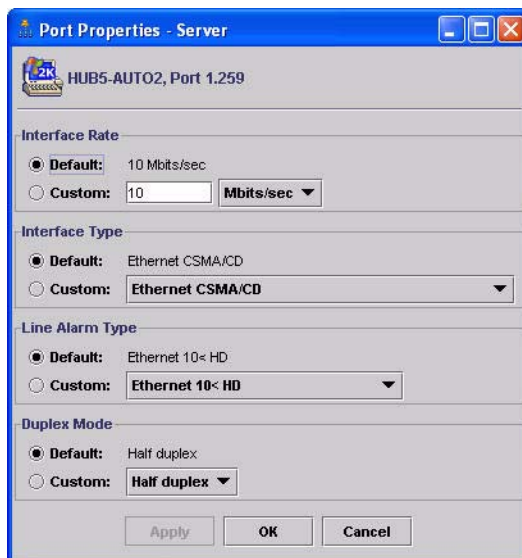
# Changing Port Properties

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 these 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**.



To reset the 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**.

# 10 Configuring your Scanner Settings

When you installed Enterprise Discovery, you set up some Scanner Property Groups 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 80
  - [Minimum scanner execution retry frequency](#) on page 81
  - [Maximum scanner upgrade attempts](#) on page 81
  - [Initial time to wait between scanner upgrade attempts \(in case of failure\)](#) on page 81
  - [Initial time to wait between retrieve scan files attempts \(in case of failure\)](#) on page 81
  - [Maximum scanfile download attempts](#) on page 82
  - [Scanner Versions](#) on page 82
  - [Scanner File Names](#) on page 83
- 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 Enterprise Discovery Server in your network. If one asset is being monitored by two Enterprise Discovery Servers, the sequence number from one Enterprise Discovery 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:	<input checked="" type="radio"/> Default:	
	<input type="radio"/> Custom:	<input type="text"/>
AutoSequence_character_count:	<input checked="" type="radio"/> Default:	5
	<input type="radio"/> Custom:	<input type="text" value="5"/>
AutoSequence_next_number:	<input checked="" type="radio"/> Default:	0
	<input type="radio"/> Custom:	<input type="text" value="0"/>



## Minimum scanner execution retry frequency



The minimum amount of time Enterprise Discovery 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, Enterprise Discovery 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 Enterprise Discovery 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 (in case of failure)

Initial time to wait between scanner upgrade attempts controls how long after a failed attempt will Enterprise Discovery 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 files attempts (in case of failure)

Initial time to wait between retrieve scan files attempts (in case of failure) controls how long after a failed attempt will Enterprise Discovery 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 Enterprise Discovery 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 <hwnonly>, 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 scanfile download attempts

Maximum scanfile download attempts controls the maximum number of attempts made by Enterprise Discovery to transfer the resulting scan file back to the server.

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

## Scanner Versions

You can manually change the version of Scanner you want to use for running different Operating Systems.

Scanner Versions		
<u>Win32 scanner version:</u>	<input checked="" type="radio"/> Default:	<latest>
	<input type="radio"/> Custom:	<latest> ▼
<u>HP-UX scanner version:</u>	<input checked="" type="radio"/> Default:	<latest>
	<input type="radio"/> Custom:	<latest> ▼
<u>Linux scanner version:</u>	<input checked="" type="radio"/> Default:	<latest>
	<input type="radio"/> Custom:	<latest> ▼
<u>AIX scanner version:</u>	<input checked="" type="radio"/> Default:	<latest>
	<input type="radio"/> Custom:	<latest> ▼
<u>Solaris scanner version:</u>	<input checked="" type="radio"/> Default:	<latest>
	<input type="radio"/> Custom:	<latest> ▼
<u>Mac OSX scanner version:</u>	<input checked="" type="radio"/> Default:	<latest>
	<input type="radio"/> Custom:	<latest> ▼

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



For the Win32 scanner, “.exe” is automatically appended to the name.

If this is your first installation of Enterprise Discovery, then there are only two options in the list: <latest> and the version shipped with the version of Enterprise Discovery 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.

Scanner File Name		
<u>Win32 scanner executable name:</u>	<input checked="" type="radio"/> Default:	scan
	<input type="radio"/> Custom:	<input type="text" value="scan"/>
<u>HP-UX scanner executable name:</u>	<input checked="" type="radio"/> Default:	scan
	<input type="radio"/> Custom:	<input type="text" value="scan"/>
<u>Linux scanner executable name:</u>	<input checked="" type="radio"/> Default:	scan
	<input type="radio"/> Custom:	<input type="text" value="scan"/>
<u>AIX scanner executable name:</u>	<input checked="" type="radio"/> Default:	scan
	<input type="radio"/> Custom:	<input type="text" value="scan"/>
<u>Solaris scanner executable name:</u>	<input checked="" type="radio"/> Default:	scan
	<input type="radio"/> Custom:	<input type="text" value="scan"/>
<u>Mac OSX scanner executable name:</u>	<input checked="" type="radio"/> Default:	scan
	<input type="radio"/> Custom:	<input type="text" value="scan"/>

Some antivirus programs may take note when Enterprise Discovery 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.



# 11 Agent Communication Configuration

In order to distribute and run Scanners on your workstations, you must first install an agent on each workstation. The Agent is the component that communicates with your Enterprise Discovery server, allowing the server to run the Scanner, and send data back to the server.

The agent is installed as a permanently running program on a remote computer. On Windows NT/200x/XP 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 Enterprise Discovery 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

The following platforms are supported for the agents:

Windows:

- Windows 98 Second Edition.
- Windows NT 40 SP6a, Windows 2000 SP4, Windows XP SP/SP1/SP2
- Windows 2003 Server SP1

UNIX:

- Sun OS 2.5.1 and later, SUN Solaris 8/9/10 SPARC.
- IBM AIX 4.3.x, AIX 5.x
- Linux i386 distribution with a 2.2, 2.4 or 2.6 kernel
- HP-UX 10.20+, HP-UX 11.x

Mac:

- Mac OS X 10.3. Mac OS X 10.4

## Agent security

During the initial setup and installation Enterprise Discovery 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 Enterprise Discovery data directory (usually C:\Documents and Settings\All Users\Application Data\Peregrine\Enterprise Discovery\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, Enterprise Discovery 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 Enterprise Discovery servers are used to communicate with the same agents, the certificates generated on one server need to be copied onto all the other servers.

## Agent Media files

After the security keys and certificates become available, Enterprise Discovery 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 Enterprise Discovery program directory (usually C:\Program Files\HP OpenView\Enterprise Discovery\2.1.0\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 Enterprise Inventory data directory (usually C:\Documents and Settings\All Users\Application Data\Peregrine\Enterprise Discovery\LiveAgents).

The content of this directory looks similar to this:

```
HP OpenView-discovery-agent-aix-2.1.0.3989.tar.Z
HP OpenView-discovery-agent-hpux-2.1.0.3989.tar.Z
HP OpenView-discovery-agent-linux-2.1.0.3989.tar.Z
HP OpenView-discovery-agent-macosx-2.1.0.3989.tar.Z
HP OpenView-discovery-agent-sunos-2.1.0.3989.tar.Z
HP OpenView-discovery-agent-win32-2.1.0.3989.exe
HP OpenView-discovery-agent-winnt-2.1.0.3989.exe
HP OpenView Discovery Agent 2.1.0.3989.msi
HP OpenView Discovery Agent 2.1.0.3989.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.

- Two versions of executable (.exe) installers for Win32.

The difference between the two versions is the size. HP

OpenView-discovery-agent-win32-2.1.0.xxxx.exe has an MSI engine for both Windows 9x and Windows NT/200x/XP (about 3.7MB in size). HP

OpenView-discovery-agent-winnt-2.1.0.xxxx.exe has the MSI engine for Windows NT/200x/XP only (about 2.0MB in size).

If the Microsoft Installer (MSI) is installed on Windows, the agent's MSI file can be used to directly install the agent. If the MSI is not installed, the .exe installer program can be used which will install the appropriate MSI and install the agent itself. The agent MSI file must be available in the same directory as the executable installer.

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 **RawAgents** 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.

## 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 HP OpenView\Discovery Agent directory under standard Windows Program Files directory. For UNIX agents, the installation directory is chosen manually during its deployment.
- **Agent data directory.** This directory is used by the agent to store various files, such as logs, utilization data, etc. Under Windows it is normally located under the profile for the local service in Application Data\Peregrine\Enterprise Discovery\Data. On UNIX the data directory is located in **\$HOME/.discagnt** directory.

## Initial Agent Deployment

### Deployment via old listener

This deployment method can only be used when the Enterprise Discovery server was migrated from a previous Peregrine Network Discovery installation. When the migration is completed, the following happens:

- The migrated database contains the information on all discovered devices and whether the old listener is installed on a particular device or not, including the port number that the installed listener is using.
- The private security key of the Peregrine Network Discovery appliance is made available to the Enterprise Discovery server. The private security key file is named keypriv.key and will be automatically placed in the **Cert** directory located under the Enterprise Discovery data directory. This key is used by the Enterprise Discovery to communicate with the old listeners.

Provided that the old listener information is available for the device, the private security key of the appliance is available and the deployment via the old listener is enabled, the deployment logic tries to install the new agent via the old listener. It contacts the old listener, copies the new installation files on to the remote computer and launches the new agent installation.

The minimum requirements for this deployment method are as follows:

- As the old listeners were only available for Win32 platforms (Windows 9x/XP/200x), only these platforms are supported.
- The agent installation relies on the Microsoft Installer (MSI) being installed on the target computer. The MSI comes preinstalled with the following operating systems: Windows 2000, Windows ME, Windows XP, Windows 2003 Server. It is included in the latest services packs for Windows 98 and Windows NT 4. It also comes included with many installation programs that contain the MSI redistributable installation, such as Microsoft Office (starting from Microsoft Office 2000) as well as many other 3rd party products. Microsoft Windows update program usually installs the most up to date version of the Microsoft Installer.
- Windows Installer must be enabled in the Group Policy.

The Enterprise Discovery 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 installation directory used by the old listener. It can be used for troubleshooting agent installation problems.

## Deployment via Win32 RPC

This deployment method uses remote execution capabilities found in the Windows NT/200x/XP 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 not allow exceptions** check box should not be checked in the firewall configuration.

In order to access remote computers, this deployment method 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 Enterprise Discovery 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.

## 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. Enterprise Discovery 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 Enterprise Discovery Database
- Version of the agent Win32 media to be installed (for example: "2.1.0.3989"). The agent media files need to be taken from the LiveAgents directory.
- Version of the AIX agent media
- Version of the HP-UX agent media
- Version of the Linux agent media
- Version of the Solaris agent media
- Version of the Mac 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.

## Step-by-step automatic deployment instructions

- 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 **Network Configuration** section and check the value for the **Agent action** property. The value should be **no action** 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 range of devices:
  - Configure the agent property group to include agent deployment.  
**Network configuration>Agent Property Groups>Add/Modify - set Agent Action to Deploy**
  - Configure the required IP range to include this agent property group.
  - Activate the network changes.



There is a predefined Agent group called **Deploy agent** which has the **Agent Action** property set to **deploy**. Apply this to your IP range

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 via 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 OpenView Discovery Agent  
2.1.0.3989.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.

## Manual Deployment

If Microsoft Installer is not available on the client computer, automatic agent deployment will fail. The agents can still be installed manually using the supplied executable installer files (for example, HP OpenView-discovery-agent-win32-2.1.0.3989.exe in the example given above). This executable file has to be available in the same directory as the agent MSI file. Then the installation can be performed by running this executable. It first installs the MSI engine and then launches the agent installation using MSI.

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:

- 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.



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.

## Upgrading the Agent

### Upgrading a Win32 Agent

When a Win32 agent is upgraded, a copy of the new MSI agent media file is uploaded to the remote computer, the old agent gets uninstalled and the new agent is getting installed instead. 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 Enterprise Discovery 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.

## Step-by-step agent upgrade instructions

- 1 To upgrade 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 the **Update Model** icon at the top.
  - Select **Upgrade Agent** from the drop-down box and click the **Update** button.
- 2 To upgrade the agent on a range of devices:
  - Configure the agent property group to include agent upgrade:  
**Network configuration>Agent Property Groups>Add/Modify**  
 Set **Agent Upgrade** to **On** and select the desired agent upgrade schedule.  
  
 The default value for the **Agent Upgrade** property is **On** for all groups except **All of**
  - Configure the required IP range to include this agent property group.
  - Activate the network 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.

## Step-by-step agent uninstall instructions

- 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 **Network Configuration** section and check the value for the **Agent action** property. The value should be **no action** 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 a range of devices:
- Configure the agent property group to include agent uninstall:  
**Network configuration>Agent Property Groups>Add/Modify**
  - Set **Agent Action** to **Uninstall**
  - Configure the required IP range to include this agent property group.
  - Activate the network changes.



There is a predefined Agent group called **Uninstall agent** which has the **Agent Action** property set to **uninstall**. Just apply this to your IP range

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 the old listener

When Enterprise Discovery was migrated from a previous installation of Peregrine Network Discovery (PND) and the new agent was deployed to all computers, it is possible to uninstall no longer needed old listeners used by PND automatically.

A predefined Agent Property Group called **Uninstall Listener** is also available in the following place:

Administration > Network configuration > Agent property groups

For each of your Agent property groups, you can select the “Uninstall Listener” option.

### Step-by-step old listener uninstall instructions

To uninstall the agent on a range of devices:

- 1 Configure the agent property group to include agent uninstall:  
**Network Configuration>Agent Property Groups>Add/Modify**
- 2 Set **Listener Uninstall** to **On**.
- 3 Configure the required IP range to include this agent property group.
- 4 Activate the network changes.

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

**Device Manager> Diagnosis> Agent Log**

# Software Utilization

Windows agents include a plug-in that allows collection of the software utilization data. If software utilization capability was purchased and enabled in the Enterprise Discovery license, it can be enabled both globally and on per-IP range basis. The IP range 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 per-IP range setting is available in the agent property group settings under **Administration > Network configuration > Agent Property Groups > Add/Modify an Agent Property Group**



There is a predefined Agent group called **Collect utilization data** which has the **Collect Utilization Data** property set to **on**. Just apply this to your IP range

- 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.

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 Enterprise Discovery, you set up some Agent Property Groups 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 Enterprise Discovery 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 1 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 Enterprise Discovery will attempt to send the Agent to a network device.
Agent Deployment Concurrent Sessions	Agent Deployment Concurrent Sessions determines how many Agents Enterprise Discovery 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 Enterprise Discovery will try to send Agents.
Agent Communication Concurrent Sessions	Agent Communication Concurrent Sessions determines how many Agents Enterprise Discovery 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 Enterprise Discovery will keep utilization data.

**Table 1 Description of the Settings**

Setting	Description
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.
Agent Port	This option determines which port Enterprise Discovery will use to communicate with the Agent. You can select 2738 or 7738 (the later of which is registered with IANA).
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**.



<u>Agent deployment method:</u>	<input checked="" type="radio"/> Default:	Using Listener Windows RPC											
	<input type="radio"/> Custom:	<table border="1"> <thead> <tr> <th>Choose From</th> <th>Action</th> <th>Selected</th> <th>Order</th> </tr> </thead> <tbody> <tr> <td>Custom</td> <td>Add &gt;&gt;</td> <td>Using Listener Windows RPC</td> <td>Move Up</td> </tr> <tr> <td></td> <td>&lt;&lt; Remove</td> <td></td> <td>Move Down</td> </tr> </tbody> </table>	Choose From	Action	Selected	Order	Custom	Add >>	Using Listener Windows RPC	Move Up		<< Remove	
Choose From	Action	Selected	Order										
Custom	Add >>	Using Listener Windows RPC	Move Up										
	<< Remove		Move Down										
<u>Agent deployment command for custom:</u>	<input checked="" type="radio"/> Default:												
	<input type="radio"/> Custom:	<input type="text"/>											
<u>Agent deployment retry interval:</u>	<input checked="" type="radio"/> Default:	2 days 0 hours 0 minutes											
	<input type="radio"/> Custom:	Days: <input type="text"/> Hours: <input type="text"/> Minutes: <input type="text"/>											
<u>Agent deployment concurrent sessions:</u>	<input checked="" type="radio"/> Default:	25											
	<input type="radio"/> Custom:	<input type="text"/>											
<u>Agent deployment device types:</u>	<input checked="" type="radio"/> Default:	<div>  Workstation   Server   Storage Server   Microsoft Server   Web Server   Microsoft Workstation   Laptop   Unknown   Network Computer   Win98 Workstation   WinNT Workstation </div>											
	<input type="radio"/> Custom:	<div> <input type="checkbox"/> Enterprise Router  <input type="checkbox"/> Enterprise ATM Switch  <input type="checkbox"/> Enterprise Switch Layer 3 or above  <input type="checkbox"/> Enterprise Switch Layer 2 or below  <input type="checkbox"/> Access Switch  <input type="checkbox"/> Router  <input type="checkbox"/> Routing Server  <input type="checkbox"/> ATM Switch  <input type="checkbox"/> Switch Layer 3 or above  <input type="checkbox"/> Switch Layer 2 or below </div>											
<u>Agent communication concurrent sessions:</u>	<input checked="" type="radio"/> Default:	80											
	<input type="radio"/> Custom:	<input type="text"/>											
<u>Agent communication reserved sessions:</u>	<input checked="" type="radio"/> Default:	4											
	<input type="radio"/> Custom:	<input type="text"/>											
<u>Utilization period:</u>	<input checked="" type="radio"/> Default:	Year (365 days)											
	<input type="radio"/> Custom:	<input type="radio"/> Month (31 days) <input type="radio"/> Quarter (90 days) <input checked="" type="radio"/> Year (365 days)											
<u>Allow downgrade agent version:</u>	<input checked="" type="radio"/> Default:	No											
	<input type="radio"/> Custom:	<input type="radio"/> Yes <input checked="" type="radio"/> No											
<u>Agent port:</u>	<input checked="" type="radio"/> Default:	2738 (legacy)											
	<input type="radio"/> Custom:	<input checked="" type="radio"/> 2738 (legacy) <input type="radio"/> 7738 (assigned by IANA)											

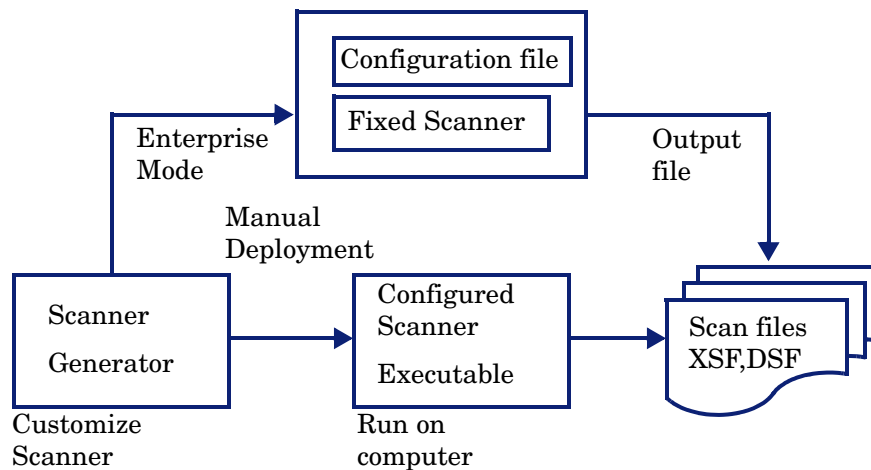


## 12 Scanner Generator

After defining requirements, the next step in an IT asset inventory is to collect data. This is accomplished using the Enterprise Discovery Scanner Generator and then running the generated Scanners.

The Scanner is configured and generated in 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 or manually.

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 three different types of information and can be configured to collect any or all of them. 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).

### The Scan File Formats

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

- Compressed XML (XSF) - with the file extension .xfs

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



In Peregrine Desktop Inventory 7.x the .xfs extension was known as .xml.gz. The file format is the same.

It is from these files that the information collected 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 175.

#### 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 Enterprise Discovery. Delta Scan files cannot be viewed in the analysis tools (Analysis Workbench and Viewer).

## The 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 binary 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 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.

### The 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 the Scanners Can Collect

The four types of information collected are:

- [Hardware and Configuration Information](#) on page 101
- [Software Information](#)
- [User or Asset information](#)
- [Software Utilization](#)

## 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). Disabling network detection in Enterprise Mode will cause the Scanner Generator to show you an error - it has to be enabled.
- 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, refer to the document entitled *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 which drives 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, and the data extracted from, for example, text files, the Windows registry and environment variables.

## Software Utilization

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

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)

## Supported Platforms

Scanner Generator runs on the following platforms:

- Windows 98
- Windows NT 4.0
- Windows ME
- Windows 2000
- Windows XP
- Windows 2003 Server

Scanners can be generated for the following operating systems:

**Table 1 Supported platforms**

Scanner	Runs on...
Windows Scanner	<ul style="list-style-type: none"><li>• Windows 98 (includes Windows 98 SE)</li><li>• Windows NT 4.0 (includes Windows NT Server)</li><li>• Windows ME</li><li>• Windows 2000 (includes Windows 2000 Server)</li><li>• Windows XP</li><li>• Windows 2003 Server</li><li>• Windows Media Server</li></ul>
UNIX Solaris Scanner	Solaris 2.5, 2.6, 7, 8, 9 and 10 on SPARC
UNIX HP-UX Scanner	HP-UX 10.2 and 11.0, 11i on HPPA
AIX Scanner	AIX 4.3, 5.0, 5.1, 5.2, 5.3 on IBM R6000
Linux Scanner	Any distribution with a 2.2x, 2.4x or 2.6x kernel on i386
Mac OS X Scanner	Mac OS X 10.3, 10.4

## Starting the Scanner Generator

To start Scanner Generator:

- 1 From the Windows Start menu select **Programs\HP OpenView\Enterprise Discovery 2.1.0\Scanner Generator**.

The Scanner Generator appears.

## Exiting the Scanner Generator

To exit the Scanner Generator, either:

- Click the **Cancel** button, or
- Click the Windows close icon in the top right of the page.

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

# The Scanner Generator User Interface

## In This Section...

- [Navigation Between the Pages](#) on page 104
- [The Scanner Generator Pages](#) on page 104

## Navigation Between the Pages

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

**Table 2** 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. That is, generate self-contained Scanner executables.
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.

## The 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.

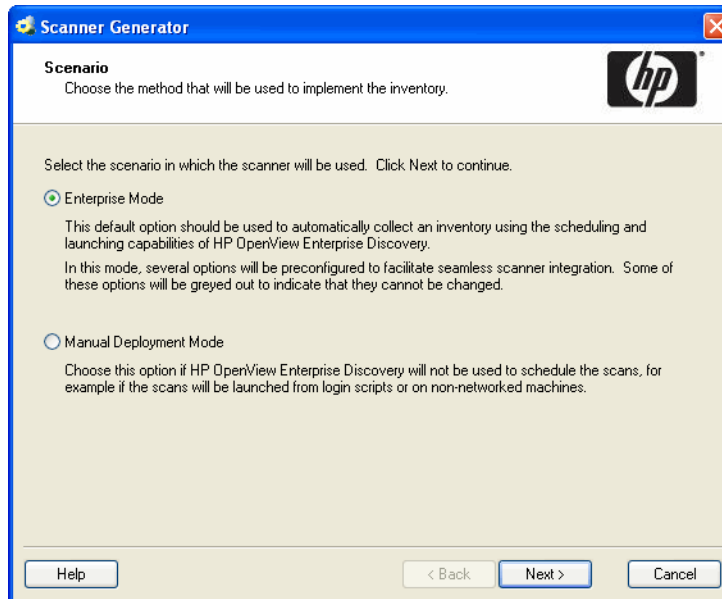
There are two scenarios in which the Scanners can be used. This is determined on the first page of the Scanner Generator. Depending on which of these scenarios you select, different tab pages are displayed.

- Enterprise Mode
- Manual Deployment Mode



# The Scenario Page

On starting the Scanner Generator, the **Scenario** page appears. You will need to determine whether you want to carry out an automatic inventory using the Enterprise Discovery agents or manually deploy the Scanners.



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

- **Enterprise Mode**

This is the default option and should be used to automatically collect an inventory using scheduling and launching on the Enterprise Discovery Server.

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

- **Manual Deployment Mode**

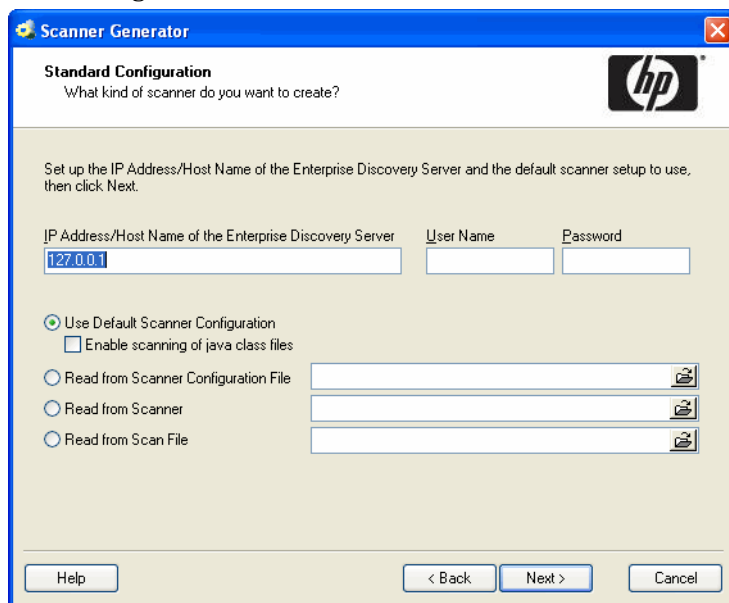
This option should be chosen if the Enterprise Discovery Server will not be used to schedule and launch scans. For example, if the scans will be launched from login scripts or on non-networked machines.

# The 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.

## Enterprise Mode

If **Enterprise** mode was selected on the Scenario page, the following page will be displayed. Use this page to set up the Enterprise Discovery Server location and the configuration to be used for creating the Scanner file.

The screenshot shows a Windows-style dialog box titled "Scanner Generator" with a blue title bar and an HP logo in the top right corner. Below the title bar, the text "Standard Configuration" is followed by the question "What kind of scanner do you want to create?". The main area of the dialog has a light beige background and contains the instruction: "Set up the IP Address/Host Name of the Enterprise Discovery Server and the default scanner setup to use, then click Next." Below this instruction are three input fields: "IP Address/Host Name of the Enterprise Discovery Server" (containing "127.0.0.1"), "User Name", and "Password". Under these fields are four radio button options: "Use Default Scanner Configuration" (which is selected), "Enable scanning of java class files" (with an unchecked checkbox), "Read from Scanner Configuration File", "Read from Scanner", and "Read from Scan File". Each of the last three radio button options has a corresponding text input field and a file selection icon (a folder with a magnifying glass) to its right. At the bottom of the dialog are four buttons: "Help", "< Back", "Next >", and "Cancel".

- 1 Enter the IP address or Host name of the Enterprise Discovery Server.
- 2 Enter the **User Name** and **Password** to access the Server. The User Names and Passwords are defined when the administrator sets up the accounts on the Server.

You should enter the administrator account details here.

- **Use Default Scanner Configuration**

Uses default configuration setting for the Scanner.


- **Enable scanning of java class files**

This setting deals with Java scanning. Enabling this setting will do 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.

- **Read from Scanner Configuration File**


Reads the settings from a previously saved external configuration file (.cxz).

Click the  button and navigate to the configuration file stored on a local disk drive or network drive.

You can drag and drop a configuration file onto this page of the Scanner Generator to automatically load the settings from that file. The path to the file will be shown in the field here.


- **Read from Scanner**

Reads the settings selected for a previously configured Scanner executable. You can make any amendments to the configuration as necessary.

Click the  button and navigate to the Scanner executable stored on a local disk drive or network drive. You can also drop a Scanner directly from Windows Explorer.

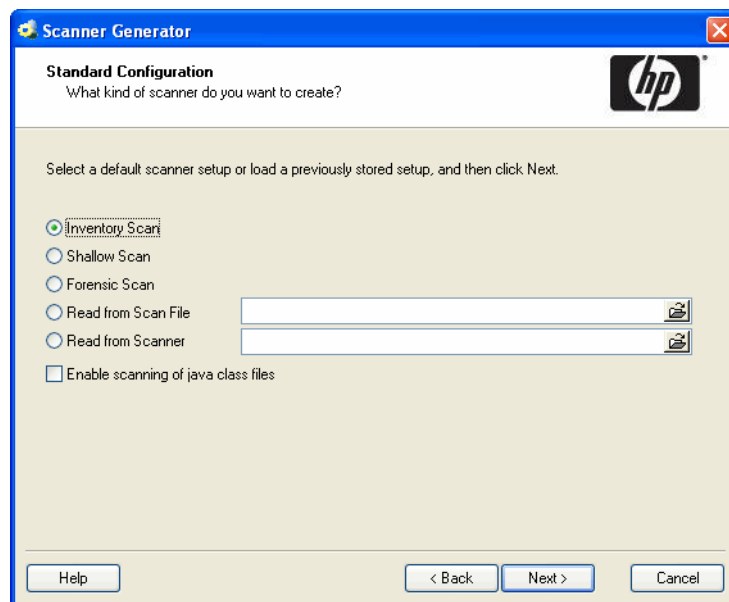
- **Read from Scan File**

Reads the settings from an existing scan file (.xsf) file.

Click the  button and navigate to the scan file stored on a local disk drive or network drive. You can also drop a scan file directly from Windows Explorer.

## Manual Deployment Mode

If **Manual Deployment** mode was selected on the Scenario page, the following page will be displayed.



To select the type of Scanner to create:

Start by selecting one of the Scanner default settings:

- **Inventory Scan (default)**

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, all hardware items are collected, but limited software scanning takes place and the data collected is not sufficient to perform reliable software license recognition.

- **Forensic Scan**

If scanning time is not a critical factor, the Forensic 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.


- **Read from Scan file**

Reads the settings from an existing scan file (.xsf) file.

Click the  button and navigate to the scan file stored on a local disk drive or network drive. You can also drop a scan file directly from Windows Explorer.

- **Read from Scanner**

Reads the settings selected for a previously configured Scanner executable.

Click the  button and navigate to the Scanner executable stored on a local disk drive or network drive. You can also drop a Scanner directly from Windows Explorer.

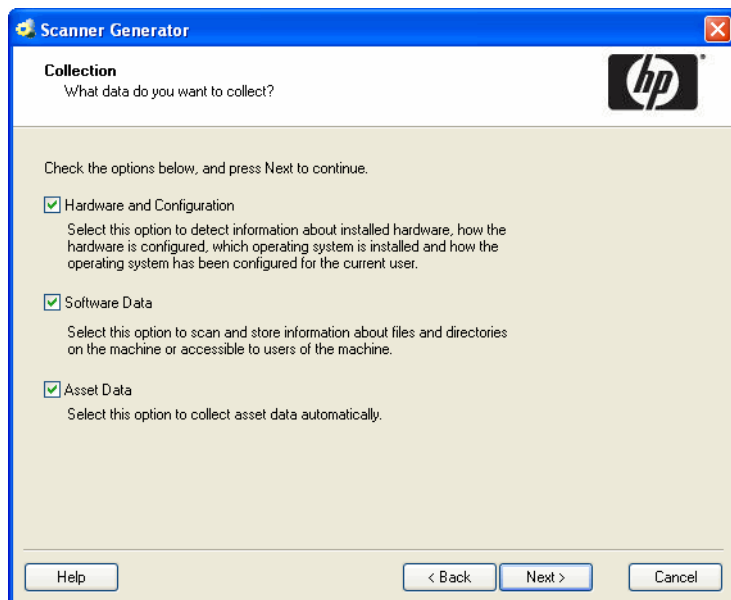
- **Enable scanning of Java class files**

This setting deals with Java scanning. Enabling this setting will do 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.
- Click the **Next** button to continue to the **Collection** page.

# The Collection Page

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



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 the 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:

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 [The Hardware Data Page](#) on page 110.



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 registered in the scan file and which are ignored.

See [The Software Data Page](#) on page 114.

- **Asset Data**

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

See [The Asset Data Page](#) on page 138

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

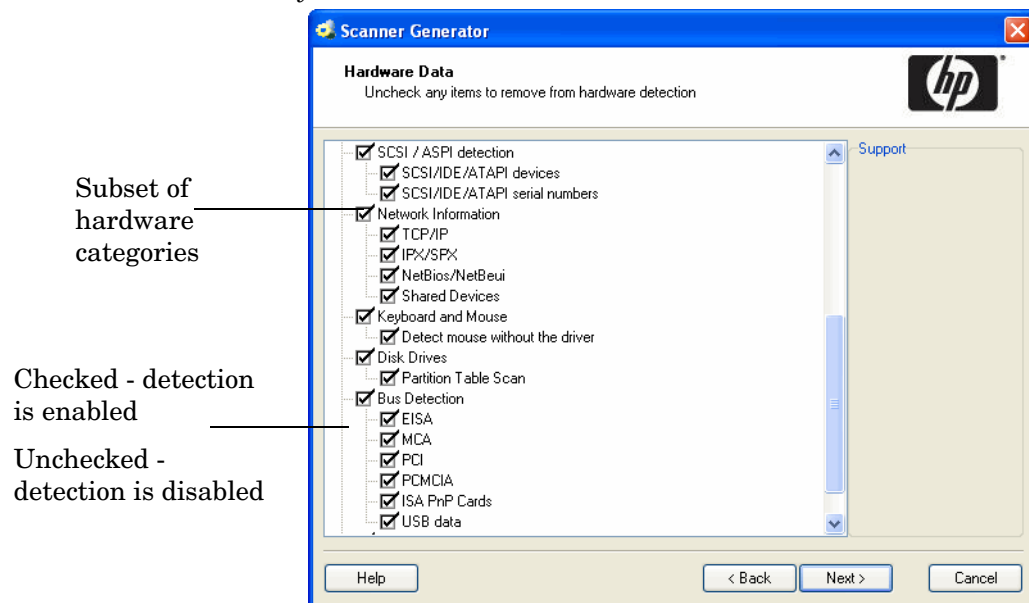
## The Hardware Data Page

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, refer to the document entitled *Data collected by the Scanners*.



The left side of this page shows a subset of the hardware categories detected by the Scanner.

To expand a category, select the check box:

**Table 3 Hardware Data page check boxes**

Check box	Indicates that the routine is...
Checked	Enabled
Unchecked	Disabled

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 of the categories are shown selected. This indicates that the hardware detection routine for that particular category is enabled.

The only hardware option which are unchecked by default is **Device Driver Data**

This is because it usually takes a long time to perform this detection. You can enable the detection of this hardware category to take advantage of the automatic device driver recognition.

## 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:

- Clear the check box next to that particular category to remove it from hardware detection.
- Click the **Next** button to continue.

## Hardware Categories

**Table 4 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.

**Table 4 Hardware categories**

Options	Description
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.
Virtual Machines	Detects whether the Scanner is running in VMWare, Virtual PC or Terminal Services.  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.
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.



**Table 4 Hardware categories**

<b>Options</b>	<b>Description</b>
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	<p>Detects the network configuration, including Logon Name, Workgroup Name, Machine ID and Domain Name.</p> <p>Detects information such as multiple network adapters, gateways, DNS servers, subnet masks, DHCP status.</p> <p>Information about installed network protocols (TCP/IP, NetBIOS/NetBEUI, IPX/SPX) and network addresses is also provided.</p> <p>Note: In Enterprise mode, it is possible to disable subsets of network information. However, you should not disable ALL network information.</p>
TCP/IP	<p>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.</p> <p>Network adapter information (including description, IP address, IP routing status, subnet mask, default gateways, DHCP status, DNS suffix, autoconfiguration status) is also provided.</p>
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.
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.

**Table 4 Hardware categories**

Options	Description
ISA PnP Cards	Detects and reports details of ISA Plug and Play cards.
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/Mac OS X configuration information.

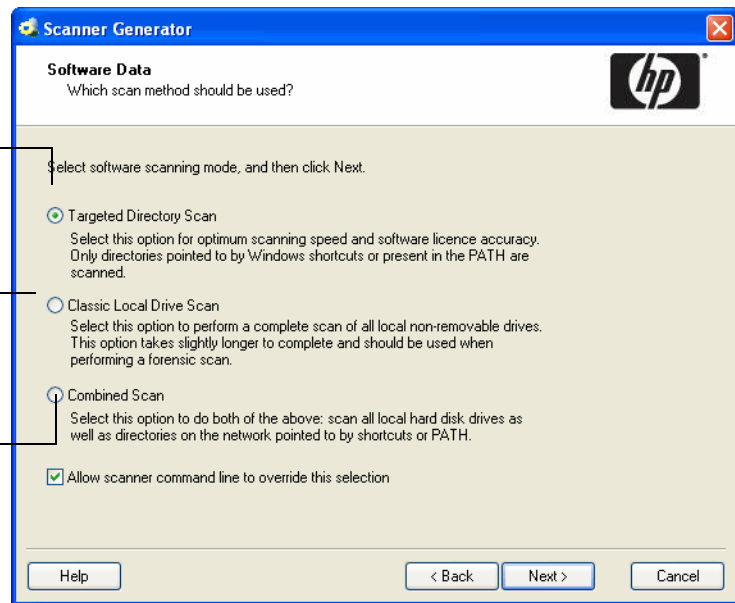
## The Software Data Page

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.

Displays the Directories, File Scanning and Stored Files tabs.

Displays the Drives, Drive Selection, File Scanning and Stored Files tabs

Displays the Drives, Drive Selection, Directories, File Scanning and Stored Files 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 the **Next** button.

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 5    Preset software scanning modes**

Scanning Mode	Tab Pages Displayed...
Targeted Directory Scan	Directories File Scanning Stored Files
Classic Local Drive Scan	Drives Drive Selection File Scanning Stored Files
Combined Scan	Drives Drive Selection 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 and environment variables. 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 forensic scan. The tab pages shown when you click **Next** are:

- Drives
- Drive Selection
- 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
- Drive Selection
- 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.

An example of a command line override is:

```
ScanW32 C: N: Z:
```

or

```
ScanW32 -paths:C:\Windows
```

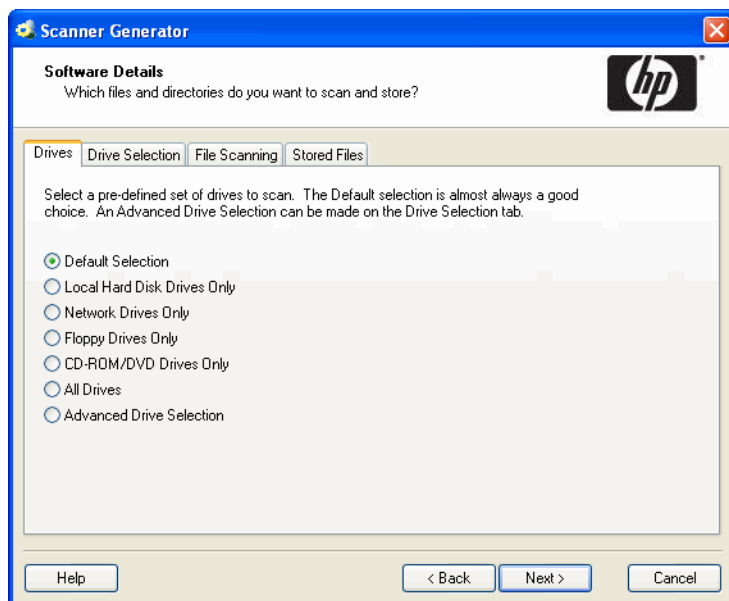
If you clear this check box, you cannot change the scan selection by specifying drive letters and/or paths on the command line.

### 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*.

## The 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**.



### Selecting a Predefined Type of Drive to Scan

Options are provided for scanning all drives or just a particular type of drive, for example, local, network and floppy drives, as well as drives not usually accessible to DOS (to cater for computers running under different operating environments, for example, Windows NT 4.0).

The default drive selection provides an option for scanning a standard set of drives, and facilities for defining a custom set of drives and alternative options for defining a custom set of drives.

When selected, you can review and modify the detailed options by clicking the **Drive Selection** tab.

To select a predefined type of drive to scan:

- Select the Scanner configuration that has the closest settings to the Scanner you want (usually the Default Selection).

**Table 6    Predefined types of drive to scan**

<b>Scanner Configuration</b>	<b>Description</b>
Default Selection	This setting selects sensible defaults for a standard inventory scan. Only fixed local drives are scanned.  It also includes other non-network and non-SUBST'ed device driven drives.
Local Hard Disk Drives Only	This setting instructs the Scanner to scan only hard disk drives.
Network Drives Only	This setting instructs the Scanner to scan only drives attached to the network.
Floppy Drives Only	This setting instructs the Scanner to scan floppy disk drives only (in NT/2000/XP/2003 you can remap a floppy to a drive letter other than A: or B:).
CD-ROM/DVD Drives Only	This setting enables the scan of CD-ROM and DVD drives only.
All Drives	This setting instructs the Scanner to scan all available drives.
Advanced Drive Selection	This setting allows the selection of any other configuration.

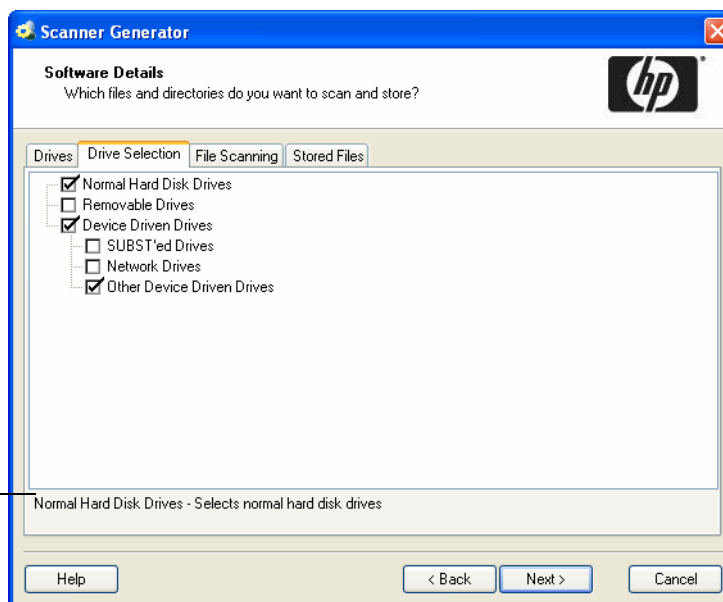
- Click the **Drive Selection** tab.
- Modify the settings to achieve the configuration you need.

When you return to the **Drives** tab after modifying the advanced configuration the **Advanced Drive Selection** option will be automatically selected.

## The Drive Selection Tab

The **Drive Selection** tab page is used to create a customized drive selection.

The status bar shows a description of each item in the list (displayed as the mouse pointer passes over each item in the list box)



## Creating a Customized Drive Selection

You can create a customized drive in the following ways:

- Define the specific types of drives scanned from this tab page.
- Take the settings for the drive type already selected in the **Drives** tab page and modify them.

The drives listed on this tab page apply to non standard disk selections.

To create a customized drive selection select the appropriate check boxes as required:

- **Normal Hard Disk 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 7    Removable drives**

Drive Selection	Description
CD-ROM/DVD Drives	Scans the contents of CD-ROM and DVD drives.
Floppy Drives	Scans floppy 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.

- **Device Driven 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 8    Device driven drives**

Drive Selection	Description
SUBST'ed 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.
Network Drives	Scans network drives. Note that network drives can be scanned by multiple computers. Use this option with caution.
Other Device Driven 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.



# Overriding Scanner Generator Settings with Override Files

The **Software Data page - Drive Selection** tab, allows you to specify the files systems and Directories (known to the Scanner Generator) that you want to include or exclude during scanning.



This tab page is only displayed if you selected the **Classic Local Drive Scan** or **Combined Scan** option on the **Software data** page.

You can override the settings of the file systems and specific Directories and Files during the software scanning.

Additional content for the override files can be specified on the **Scanner Options|Troubleshooting** tab page.

## File Systems

You can override the settings of the file systems during the software scanning.

Because it is always possible, particularly on UNIX/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.

Name the file name **.override.ini**

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 .override.ini 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.ini 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 wildcards.

### Example

```
[exclude]
fs=autofs
dir=/temp
dir=/etc
file=*.exe
```



When excluding files using .override.ini 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, the 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.

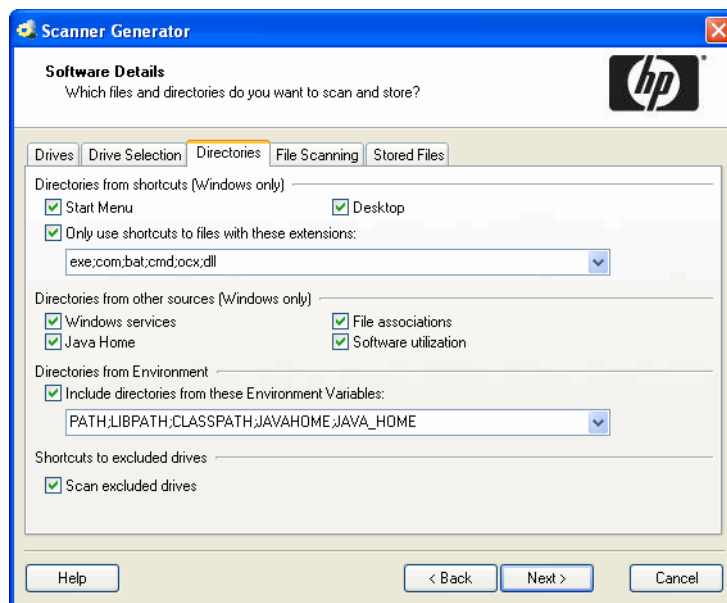
To prevent this happening, use the .override.ini file with \*.vir specified for exclusion (where .vir is a typical quarantine file extension). Check the specific virus product to find the extension for this type of file.

## The 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.



## Selecting the 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 (Windows only) group**

- **Windows services**

Check this box to include directories containing Windows Services for targeted scanning.

- **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 targeted directories to scan.

- **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.



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 to scan. This ensures that the Scanner collects the file data required for recognition of used applications.

- **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 checkbox. 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.

## The File Scanning Tab

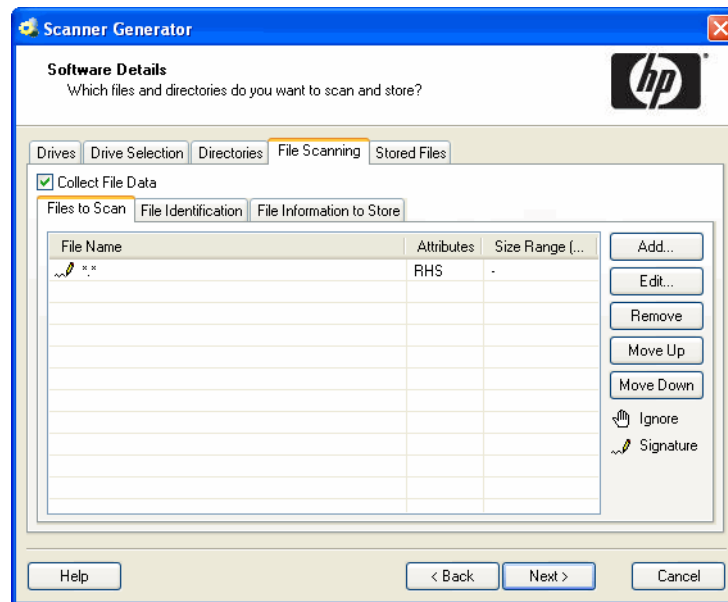
The **File Scanning** tab is used to specify the level of detail for the information collected about files and directories and the methods used to check and identify files.

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.





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

### The 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 9 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.

- The sequence and priority of a file processing 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.
- Multiple file name entries can be made on each line if they are separated by a semicolon.
- Entries can be edited by double-clicking on them.

## 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 8K of the file. To calculate the signature, the Scanner opens the file and reads the first 8K 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).

## The 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.

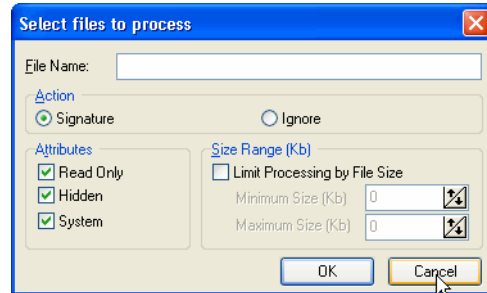
For example, files that are normally used as swap files (386part.par, pagefile.sys, swapper.dat, win386.swp) or files that contain volumes of compressed drives, such as, DriveSpace, DoubleSpace or Stacker (Dblspace.0??, Drvspace.0??, Stackvol?.sys).

## Specifying the Information Collected About Files and the 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:

- In the **Files to Scan** sub tab, select the **Collect File Data** check box. This option activates the controls on this tab page.
- Click the **Add...** button. The following dialog box appears.



- 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.
- 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.
- 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.  
If a given attribute is not selected, the entry will not match, even if the file name does.
- 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.
- Click **OK**.

## File Action Options - Example

File Name	Attributes	Size Range [...]
*.tmp	RHS	-
386part.par;pagefile.sys;swapper.dat;win386.swp	RHS	-
D:\space.0??;Drvspace.0??;Stackvol?.sys	RHS	-
**	RHS	-

These entries in this list box mean:

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

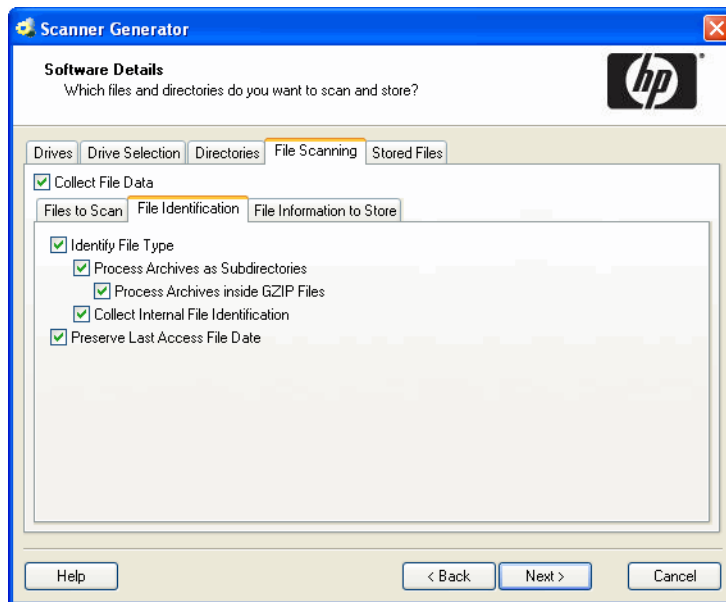
**2-3:** Ignore the following files, including files with read-only, hidden and system attributes:

- Files that are normally used as swap files:
- 386part.par
- pagefile.sys
- swapper.dat
- win386.swp
- Files that contain volumes of compressed drives, such as DriveSpace, DoubleSpace or Stacker.
- Dbldspace.0??
- Drvspace.0??
- Stackvol?.sys

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

## File Identification Sub Tab

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



## Specifying Whether the Scanner Will Identify Files Based on Their Content

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

- Ensure that the **Collect File Data** check box is selected. This option activates the controls on this tab page.
- 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.

- **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.

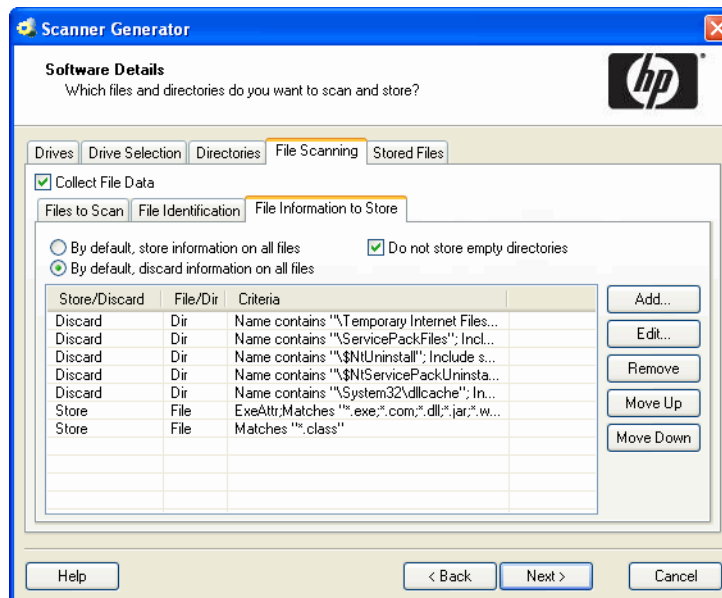
When this setting is used on Unix computers, although the last access time will be preserved, the ctime of the file gets changed. For this reason we recommend that you do not use this setting on Linux, Mac OS X or Unix computers.



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.

## 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.



### Adding, Editing or Removing File Filter Storage Criteria

The three options at the top of the page sets 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:

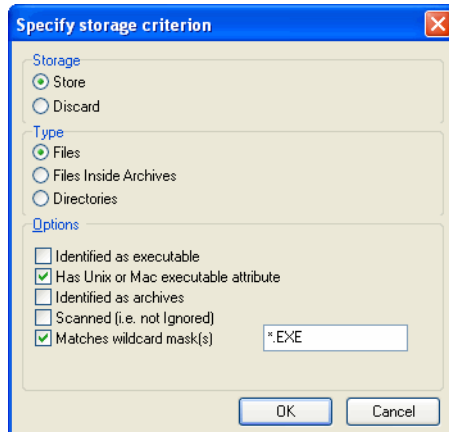
- To add another filter criteria, click **Add...**
- To edit an existing filter criteria, click **Edit...** or double-click on the entry.

- 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**, then the **Specify storage criterion** dialog box appears.

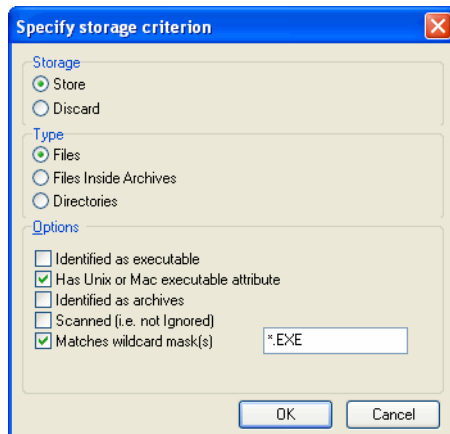


This dialog box has three types (shown in the Type group box):

- Files
- Files Inside Archives
- Directories

## Including or Excluding Files Based on the File Name or Scanned Attributes

Follow this procedure if you selected the **Files** Type in the **Specify storage criterion** dialog box.



To include or exclude files based on the file name or scanned attributes:

- 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.
- Select the **Files** option in the **Type** group box.
- Check the **Matches wildcard mask(s)** option.

- Specify a list of wildcards separated by a semicolon (;). For example, when scanning of Java class files is enabled (see [The Standard Configuration Page](#) on page 106), 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.
- 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 people: owner, group and other.

**Table 10 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 directory.

Checking this option would cause the Scanner to store or discard files that have the executable file access.

- **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.

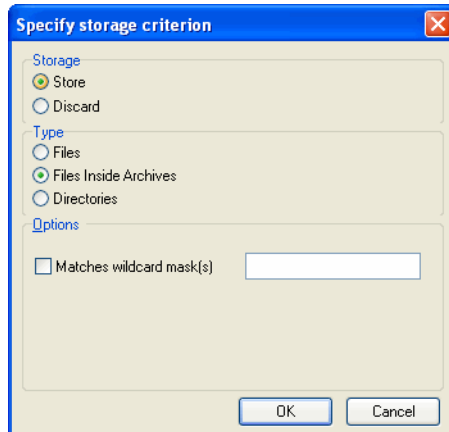
### Explanation of the Operation

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 the Files Inside Archives

Follow this procedure if you selected the **Files Inside Archives** Type in the **Specify storage criterion** dialog box.

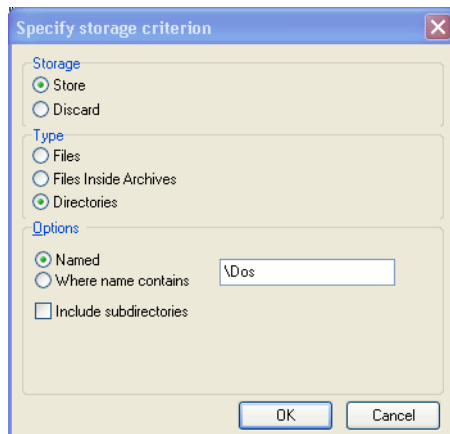


To include or exclude files based on the files inside archives:

- 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.
- Select the **Files Inside Archives** option in the **Type** group box.
- Check the **Matches wildcard mask(s)** option.
- 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 the Directory

Follow this procedure if you selected the **Directories** type in the **Specify storage criterion** dialog box.




To include or exclude files based on the directory:

- 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.
- Select the **Directories** option in the **Type** group box.

- 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

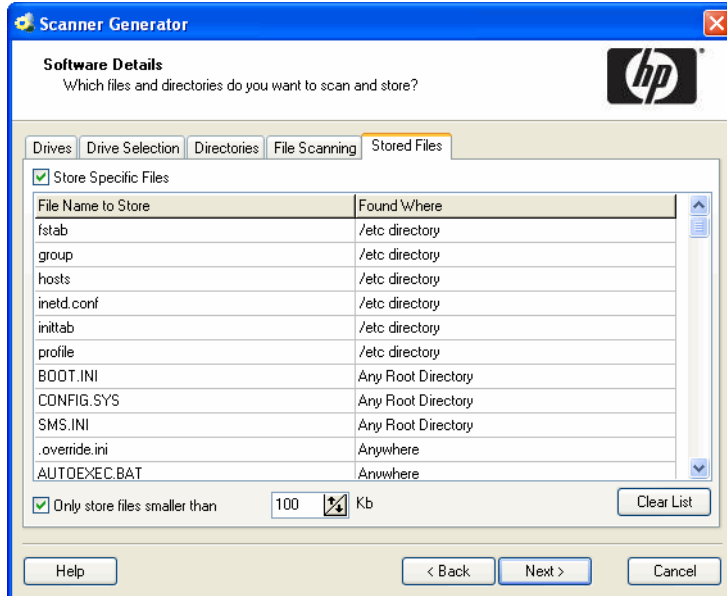
The contents of filtered directories are not stored in the scan file. If the Do not store empty directories ([page 130](#)) option is checked, filtered directories are considered to be empty and are not stored in the scan file either. If this option is unchecked, the filtered directories are represented 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.

## The 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.



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`.

There is one Enterprise Discovery specific file included in the list:

- **.override.ini**

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 [Overriding Scanner Generator Settings with Override Files](#) on page 121.

## Enabling the Controls on the Stored Files Page

To enable the controls on the Stored Files page:

- 1 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:

- Enter a file name at the bottom of the **File Name to Store** column (or overwrite an existing entry).
- 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:

- Highlight the file name.
- Press the **Delete** key or right-click on the entry and select the **Delete** option from the shortcut menu.

## Clearing the Entire List of Files to Be Stored

To clear the entire list of files to be stored:

- Select the **Clear List** button. A confirmation message is displayed.
- Select the **Yes** button to clear the list.

## Limiting the Size of Files to Be Stored

To limit the size of files to be stored:

- Select the **Only store files smaller than** option.
- 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 the Files

To change the directories that are scanned to locate the files

- Click on an entry in the **Found Where** column.



- Change the setting by selecting an option from the drop-down list.

**Table 11 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	<p>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:</p> <pre>C:\Documents\config.txt Z:\net.ini /etc/fstab</pre> <p>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).</p>



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.

## The 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:

- [The Asset Data Tab](#) - Used to define which asset data is to be collected automatically.
- [The 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 the **Next** button to continue.

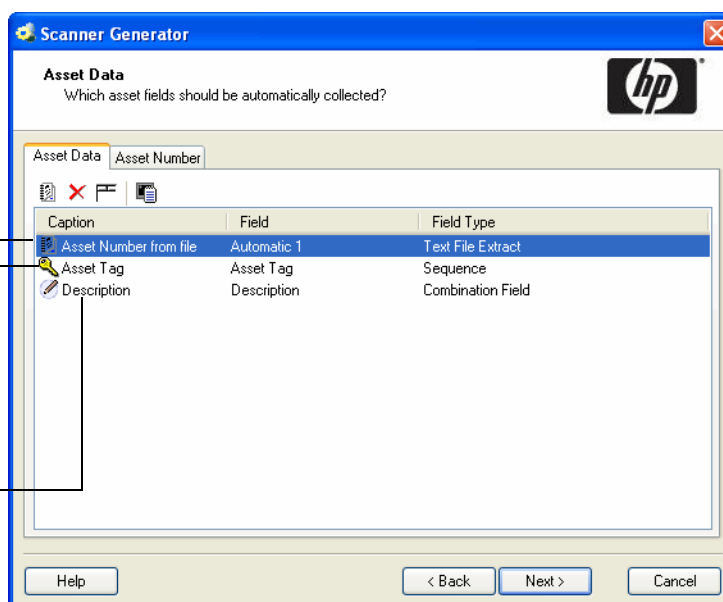
## The Asset Data Tab

The **Asset Data** tab is used to configure customized asset information as each computer is scanned.

Indicates that this is an **Asset Data** field

Indicates that this field is the **Asset Tag** Field

Indicates that this field is the **Description** Field



The screenshot shows the 'Scanner Generator' window with the 'Asset Data' tab selected. The window title is 'Scanner Generator' and the subtitle is 'Asset Data'. Below the subtitle is the question 'Which asset fields should be automatically collected?'. There are two tabs: 'Asset Data' and 'Asset Number'. The 'Asset Data' tab is active, showing a table with three columns: 'Caption', 'Field', and 'Field Type'. The table contains three rows: 'Asset Number from file' (Automatic 1, Text File Extract), 'Asset Tag' (Asset Tag, Sequence), and 'Description' (Description, Combination Field). There are icons for adding, deleting, and saving fields. At the bottom are buttons for 'Help', '< Back', 'Next >', and '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 Enterprise Discovery 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.

## The 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 28 automatic fields.


## The Asset Data Form Toolbar

A toolbar is displayed at the top of the Asset Data form. The buttons have the following functions:

**Table 12 Asset data form toolbar**

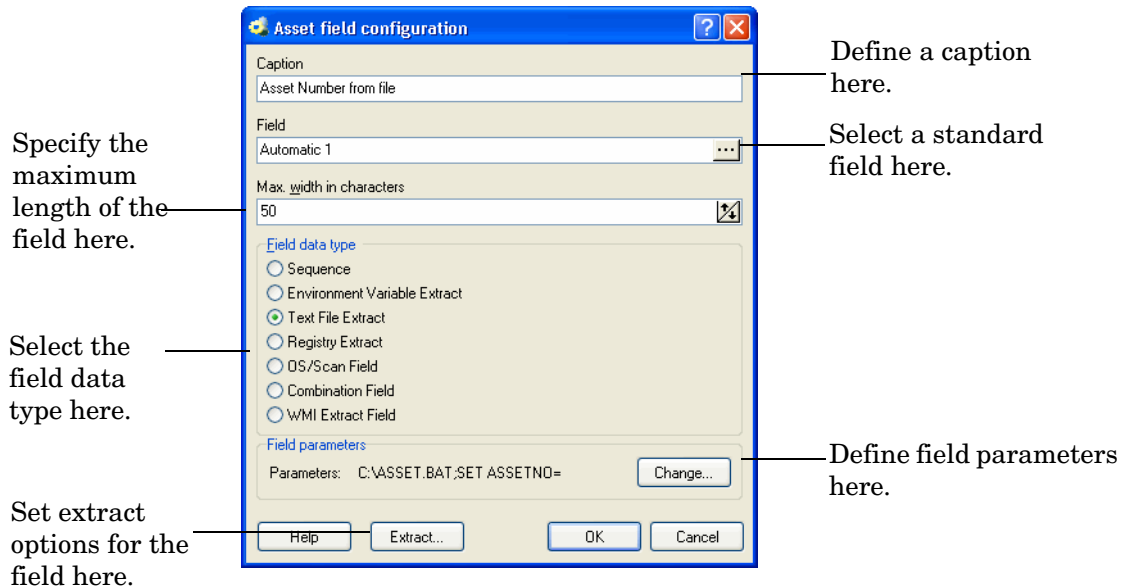
Button	Function	Shortcut
	Create a new field The Choose Field dialog box appears.	Ctrl+N
	Delete field	None
	Delete all fields Clear all the entries in the Asset Data form. A confirmation message is displayed before the entries are cleared.	None
	Edit the type and settings for field The Asset field configuration dialog box appears, which allows you to edit the information for the field.	Ctrl+T

Each of the toolbar functionality is also available 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.

## The Asset Field Configuration Dialog Box

This dialog box is where the major part of the asset field configuration takes place.



## 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 13 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
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.

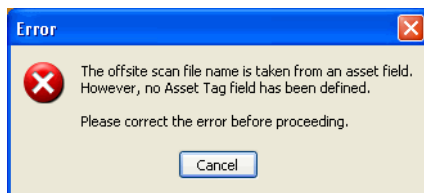
When loading data from scans into the analysis tools (Analysis Workbench and Viewer), the contents of the description field are displayed for each scan file to help identify them.

### 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.

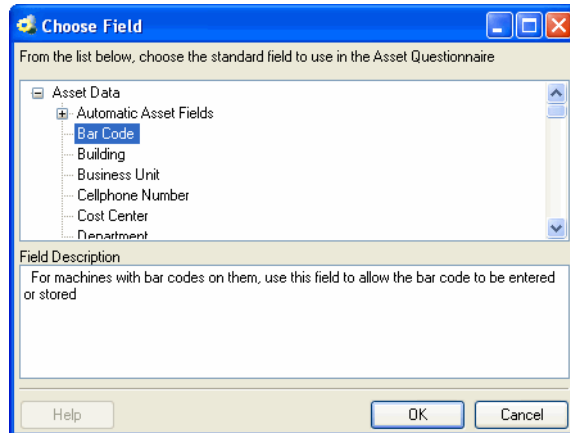


It is strongly recommended that **Description** and **Asset Tag** fields are included in your list of asset fields.

To choose a standard field:

- Click the  icon.

- The **Choose Field** dialog box is displayed, showing all standard fields not currently in use.



- Choose a new standard field from the list.

These fields are legacy fields left from previous releases of Enterprise Discovery 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 14 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. These fields are automatic and are not displayed when the Scanner runs. You can configure up to 28 automatic fields, which can then be used in the calculation of derived or calculated fields.	hwAssetAutomatic1..28
Bar Code	For machines with bar codes on them, use this field to allow the bar code to be entered or stored	hwAssetBarCode
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

**Table 14 Standard fields**

Field	Description	Field mapped to in the hwAssetData table
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

- Click **OK** to return to the Asset Data form.

### Step 3: Specifying the Maximum Number of Characters for the Field

To specify the maximum number of characters for the field:

- 1 Enter a numeric value in the **Max. width in characters** field.

### Step 4: Choosing the 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 15** Calculated fields

Field	Description
Environment Variable Extract	Accepts data from a specified environment variable set in the operating system.
Text File Extract	<p>Extracts information from a single line in a named text file.</p> <p>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:</p> <pre>SET ASSETNO=</pre> <p>Other useful file extracts include the predefined SMS, which extracts the SMS Unique Machine ID.</p>
Registry Extract	<p>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:</p> <pre>HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\TimeZoneInformation\StandardName</pre>
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 16 Derived fields**

Field	Description
Sequence	<p>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.</p> <p>The value returned as the result of the sequence field will be the first of these fields which contains a non-blank value.</p>
OS/Scan	<p>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.</p> <p>For each Scanner platform a separate asset field could be defined.</p>
Combination	<p>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.</p> <p>Up to five fields can be combined into one.</p>

## Step 5: Setting Field Parameters

Field parameters need to be set for the following types of fields:

**Table 17 Field types**

Field	See...
Sequence	<a href="#">page 146</a>
Environment Variable Extract	<a href="#">page 147</a>
Text File Extract	<a href="#">page 147</a>
Registry Extract	<a href="#">page 149</a>
OS/Scan	<a href="#">page 150</a>
Combination	<a href="#">page 150</a>
WMI Extract	<a href="#">page 152</a>

## Setting Up a Sequence Field

The sequence field is used to test multiple entries from hardware and asset fields. The entries are tested until a non-empty value is found, This can be modified so that certain values can be ignored so that the test fails.

The sequence field can be used to select the desired element of a hardware field that can have multiple values. For example, when trying to identify the MAC address on a machine, fake MAC addresses of PPP adapters etc. can be filtered out by specifying them in the Ignore Strings option.

The sequence asset field allows up to ten asset or hardware fields to be specified. Each of these fields return a value depending on the machine or environment running.

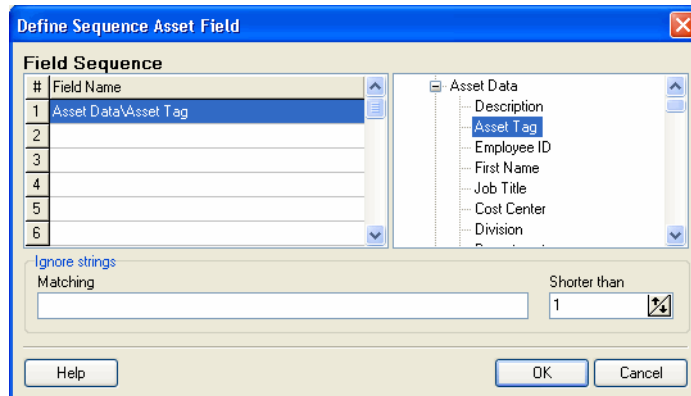
The value returned as the result of the sequence field, will be the first of these fields which contains a non-blank value. If all values are blank, then the user can be allowed to type a manual entry instead.

A blank field can be defined based on either of the two following criteria:

- The string matches one of a set of 'ignore' strings.
- A field is considered blank if the length of the field is shorter than the number specified.

To set up a sequence field:

- After you have selected a **Sequence** field as the data field type, click the **Change...** button.



- In the **Define Sequence Asset Field** dialog box, select the field type by expanding the tree on the right side and clicking on the required field.

The entry will now be displayed in the **Field Name** list on the left side.

- In the Ignore strings group box, specify the criteria for a blank field using one or all of the following methods:
- In the **Matching** box, enter a sequence of strings (case-sensitive) separated by semicolons.

If the content of the field matches (is equal to) any of the strings specified here, the field is considered to be blank. For example, if the text string Not Found is entered here, then a field that has the value 'Not Found' is considered to be blank.

Multiple entries must be separated by semicolons ( ;), for example:

'Unknown;Not Tested'

- You can type a string in the form: \*STRING\*

Here the asterisks (\*) are ignored and any string that contains the text between the two asterisks will be ignored too.

- **Specify ignore strings that are less than 'n' characters.**

In the **Shorter than** box, use the arrow keys or type in a number to specify the maximum length of text strings that are to be used to define a blank field (between 1 and 255). If the string is shorter than the specified number, then the field will be considered blank.

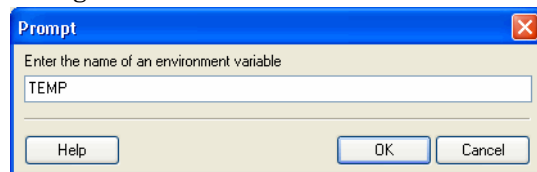
- Click **OK** to return to the **Asset Field configuration** dialog box.

## 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:

- After you have selected an Environment Variable Extract as the data field type, click the Change... button.



- Enter the name of the environment variable in the Prompt dialog box. Examples of environment variables are TEMP or PATH.
- Click OK to return to the Asset Field configuration dialog box.

## Setting Up Text File Extract Field Parameters

If using environment variables in the file path, they must be in uppercase. For example:

```
%WINDIR%\SMSCFG.INI
```

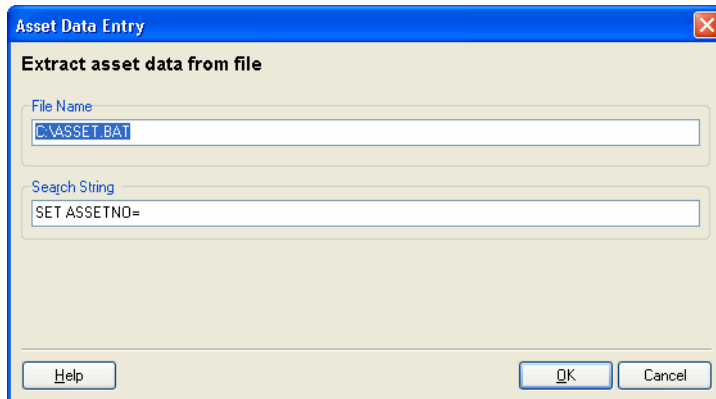
This field searches a named text file for a defined character string and makes an automatic entry of the characters between the search string and the end of the line.

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:

- After you have selected a **Text File Extract** field as the data field type, click the **Change...** button.



- 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:

`\\EnterpriseDiscoveryServer\Enterprise Discovery\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 environment variable HOME



This is applicable to all platforms and UNIX notation of the form \$NAME is not supported.

- 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).



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.

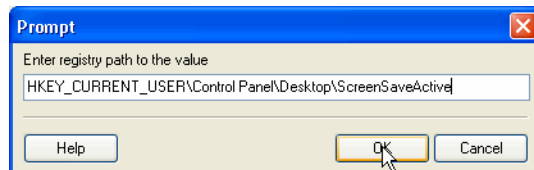
- Click OK to return to the Asset Field configuration dialog box.

## 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:

- After you have selected a **Registry Extract** field as the data field type, click the **Change...** button.



- 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
```

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.

- Click **OK** to return to the **Asset Field configuration** dialog box.

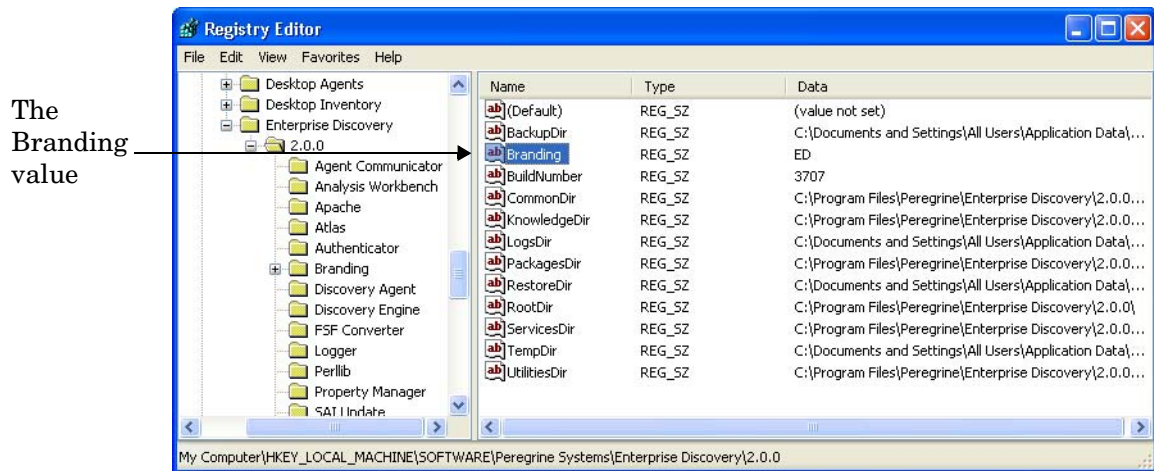


Do not change any of the settings in the Registry Editor. Doing this could result in lost registry settings and may cause some of your applications to fail.

## Extracting the Registry (Default) Value

Sometimes, you may want to extract the (default) value for a registry entry.

The following screenshot shows the regedit screen with a Branding value.



To extract the Branding value from the registry:

- 1 End the registry extract value command in a backslash.

For example, to extract the value of "ED", the following key will be used:

```
"HKEY_LOCAL_MACHINE\SOFTWARE\HP OpenView\Enterprise  
Discovery\2.0.0\Branding"
```

## 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/ Mac OS X.

To set up OS/Scan fields:

- After you have selected an OS/Scan field as the data field type, click the **Change** button. The **Define Multi-OS Asset Entry Field** dialog box appears.
- In the **Operating System** list select the operating system that will be affected by this definition.
- 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).
- Click the **Add** button. 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.

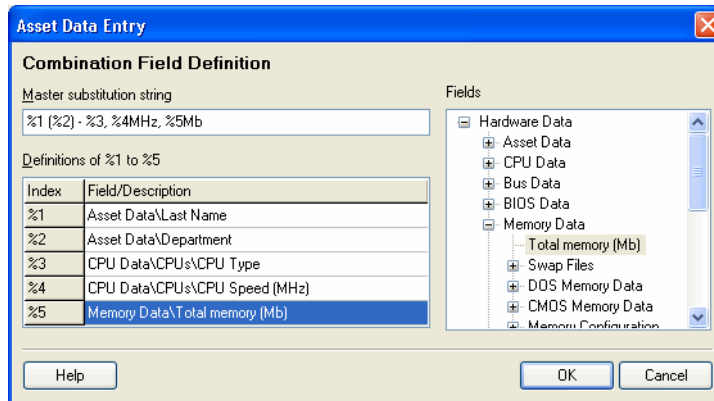
## Setting Up a Combination Field

**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:

- After you have selected a **Combination** field as the data field type, click the **Change...** button.



- 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)'
- The **Definitions** box lists the fields that have been defined for use in the substitution string.
- 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.
- To clear an entry select the **Delete** command from the right-click menu or press the **Delete** key.
- 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).
- 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.
- Continue this for up to five index entries.
- 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.
- You can also specify some text before or after the percent notation which will be a constant part of the value of the field.
- Click **OK** to return to the **Asset Field configuration** dialog box.
- 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 18 Example of a Master Substitution String**

Index	Field/Description	Displayed as...
%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

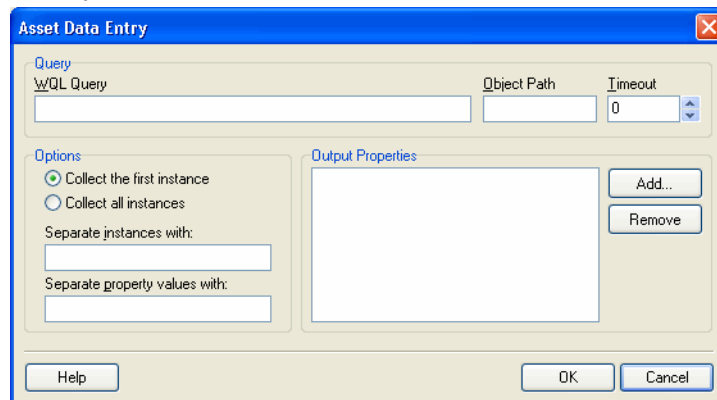
Windows Management Instrumentation Query Language (WQL) is a subset of SQL that is used to make data queries inside WMI.

#### Further Information

For further information about WMI and WQL refer to the Microsoft MSDN website.

To set up a WMI extract field:

- After you have selected a **WMI Extract field** as the data field type, click the **Change...** button.



- 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.

- Enter the **Object Path**

The Object Path should usually be:

```
root\cimv2
```

This is the default path for CIM v2 data provided by WMI.

- 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 until the query returns data. However, since this may cause the query to hang, therefore it is not recommended.

- 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.

- 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.

- Click **OK** to return to the **Asset Field configuration** dialog box.

## An Example WQL Extract Field Setup

**Table 19 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

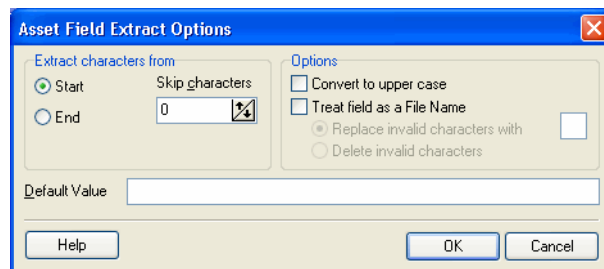
All calculated asset fields defined can be set up so that only part of the string is selected instead of the entire string. They can also be set up, for example, to use the last part rather than the first part of the string. This can be useful for obtaining the last part of an calculated field that is too long.

Various other settings for manipulating the field contents are also available.

To set extract options:

- After you have selected the field data type, click the **Extract...** button. 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.



- 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:
- 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.

- **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.
- In the **Options** group box, select the options as follows:
- **Convert to upper case** Select this option to convert the alphabetic characters to upper case, if required.
- **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.
- 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.

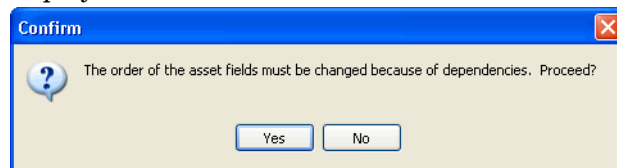
## Step 8: Correcting the Order of the Fields in the Form

You will need to consider the order of the fields in the form and move them round accordingly. The rule is:

- 1 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:

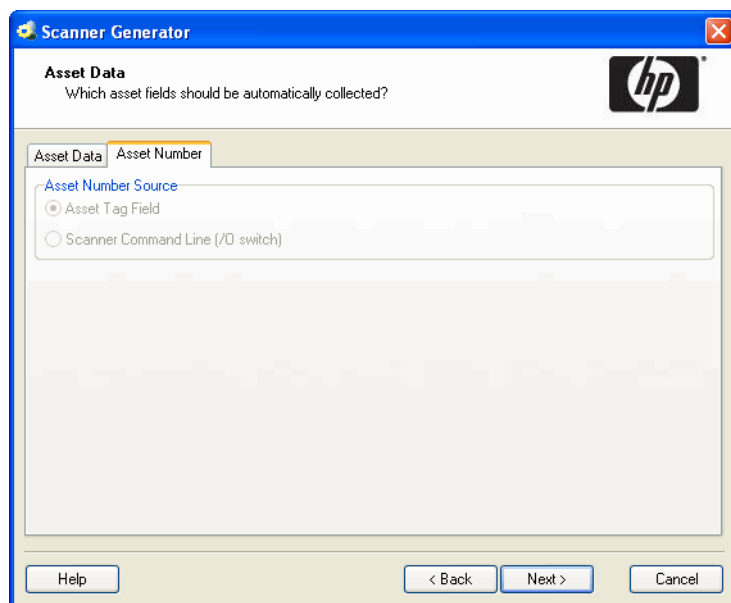
- Re-order the fields by clicking on a row and dragging the selected line to its new location in the form.
- When you click the **Next** button in the **Asset Data** page, a confirmation message may be displayed.



- Click **Yes** to have the Scanner Generator automatically do this for you.
- Click **No** to do this manually.

## The Asset Number Tab

The **Asset Number** tab is used to set options for managing the asset number used to uniquely identify a machine.



### 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 Enterprise Discovery 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.

### The Source for the 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,

```
ScanW32 -O:FP00017
```

## The 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.

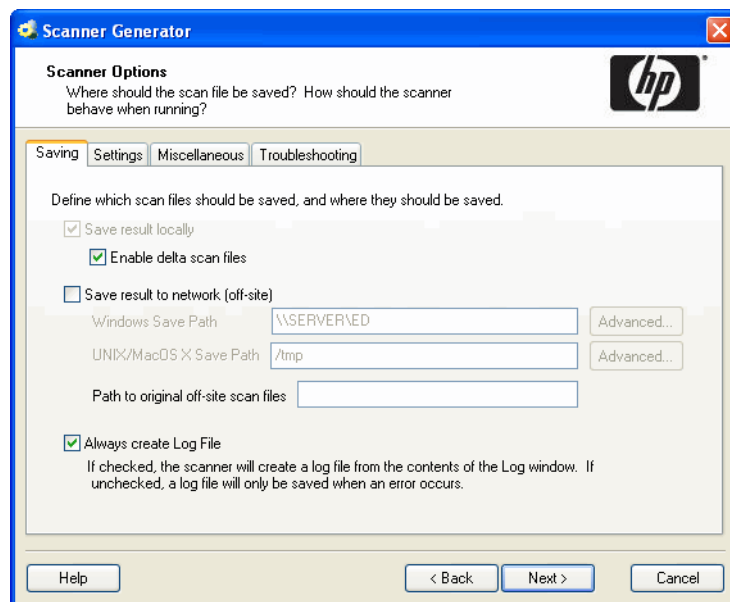
The **Scanner Options** page has four tabs:

- [The Saving Tab](#)
- [The Settings Tab](#)
- [The Miscellaneous Tab](#)
- [The Troubleshooting Tab](#)

After the options have been selected as required, click the **Next** button to continue.

# The Saving Tab

The **Saving** tab page is used to set options for saving the inventory results.



► 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 Enterprise Discovery. 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 Enterprise Discovery 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:

- Configure the Scanner to save results to the XML enricher Incoming directory. This directory can be found in the following location on the Enterprise Discovery Server by default:

```
C:\Documents and Settings\All Users\Application Data\Peregrine\Enterprise  
Discovery\Scans\incoming
```

Create a share on the Enterprise Discovery 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.

- 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\Peregrine\Enterprise  
Discovery\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:

```
\\EnterpriseDiscoveryServer\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:

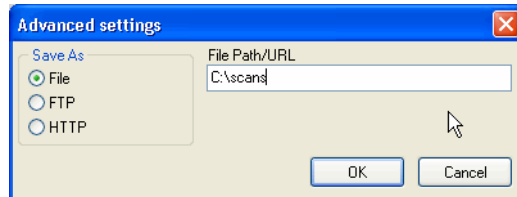
- [Normal File Path](#)
- [UNC Path](#)
- [FTP URL](#)

- HTTP URL

## Normal File Path

To save to a normal file path:

- Click the **Advanced...** button.



- 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:

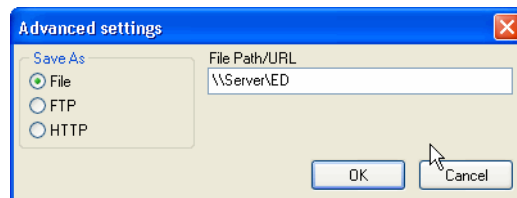
A: \Inventory\Scans

## UNC Path

A UNC path can be entered as the offsite save path.

To save to a UNC path:

- Click the **Advanced...** button.



- 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:

\\EnterpriseDiscoveryServer\Enterprise Discovery\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:

ScanW32 -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:

ScanW32 -p:\\EnterpriseDiscoveryServer\Enterprise Discovery\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.

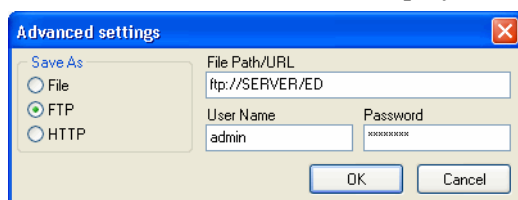
- Click the **OK** button to return to the **Savings** tab page.

## FTP URL

The Scanners can save to any FTP server.

To save to an FTP server:

- Click the **Advanced** button to display the **Advanced Settings** dialog.

A screenshot of the 'Advanced settings' dialog box. On the left, under 'Save As', the 'FTP' radio button is selected. On the right, the 'File Path/URL' field contains 'ftp://SERVER/ED'. Below it, the 'User Name' field contains 'admin' and the 'Password' field contains a series of dots. At the bottom right are 'OK' and 'Cancel' buttons.

- Select the **FTP** option.  
Extra fields are displayed.
- Enter the FTP path and enter a User Name and Password if one is to be supplied.
- Click the **OK** button 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:

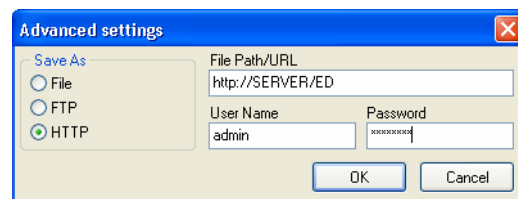
**ftp://user:password@host:port/dir**

## 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:

- Click the **Advanced** button to display the **Advanced Settings** dialog.

A screenshot of the 'Advanced settings' dialog box. On the left, under 'Save As', the 'HTTP' radio button is selected. On the right, the 'File Path/URL' field contains 'http://SERVER/ED'. Below it, the 'User Name' field contains 'admin' and the 'Password' field contains a series of dots. At the bottom right are 'OK' and 'Cancel' buttons.

- Select the **HTTP** option.  
Extra fields are displayed.
- Enter the HTTP path and enter a User Name and Password if one is to be supplied.

- Click the **OK** button 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.

## 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>\httpass" 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>\httpass"
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:

XSFO14.xsf

Then the log file generated will be called:

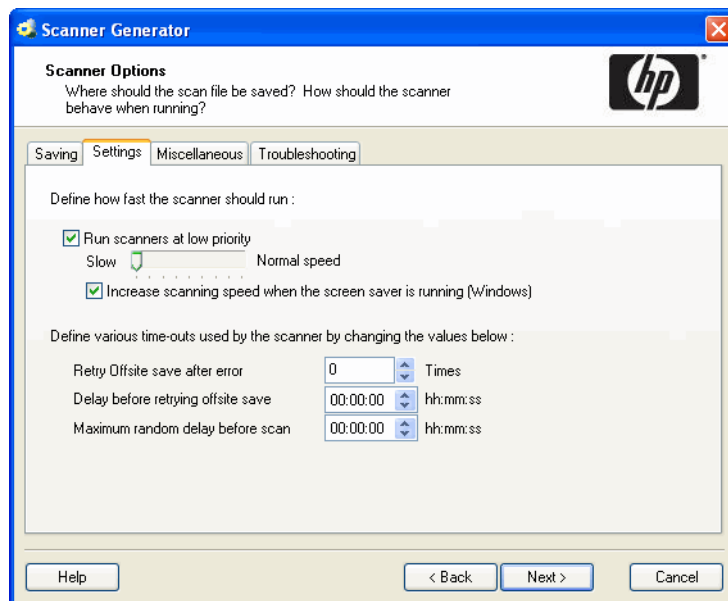
XSFO14.log



The log file is not stored with the offsite scan file if the offsite scan is saved to an FTP or an HTTP location.

## The Settings Tab

The options on this page are used to control the behavior of the Scanner as it scans each computer.



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/ Mac OS X, the Scanner performs a renice 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.

# The Miscellaneous Tab

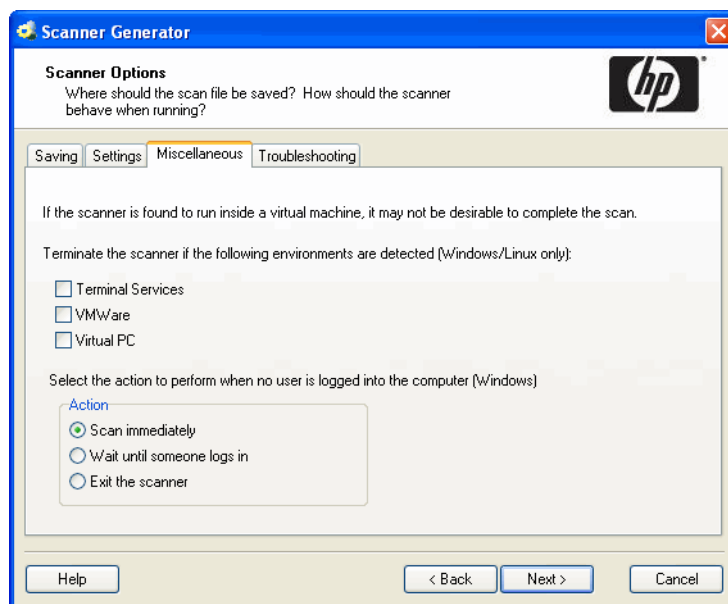
The **Miscellaneous** tab allows you to:

- 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 this page 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.



The settings for Virtual Machines are applicable to Linux and Windows Scanners only.

For Windows all three options are valid, for Linux only VMWare and Virtual PC are valid.

Select the virtual environment(s) you want the Scanner to terminate for, if detected:

- Terminal Services
- VMWare
- Virtual PC

## 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 Enterprise Discovery 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:

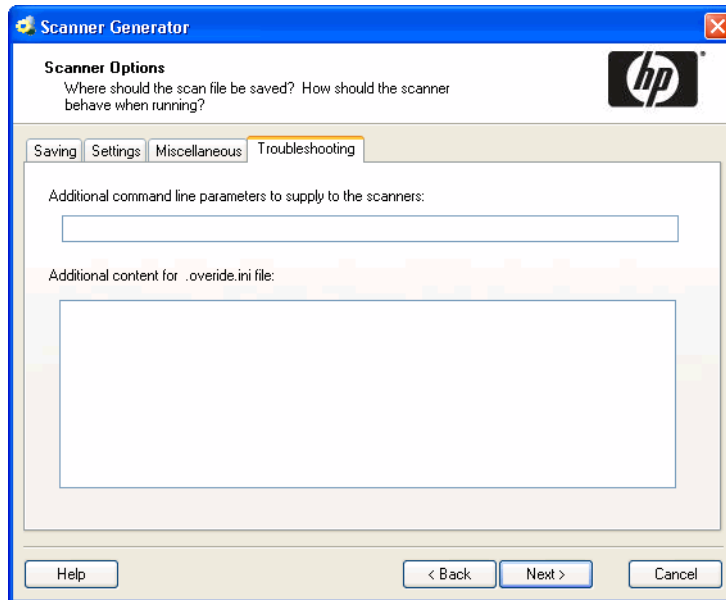
- **Scan Immediately:** Forces the Scanner to run under the local system account. However, it will not be able to collect the environment information for a particular user. The environment settings for the local system account will be detected. Also any program running under the local system account 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 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 such a case the above logic for Enterprise mode applies.

# The Troubleshooting Tab

This page is used to set up additional troubleshooting options for the Scanners.



## Additional command line parameters to supply to the scanner

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.

Further information on command line parameters and how to use them can be found in the Scanners chapter of the Reference Guide.

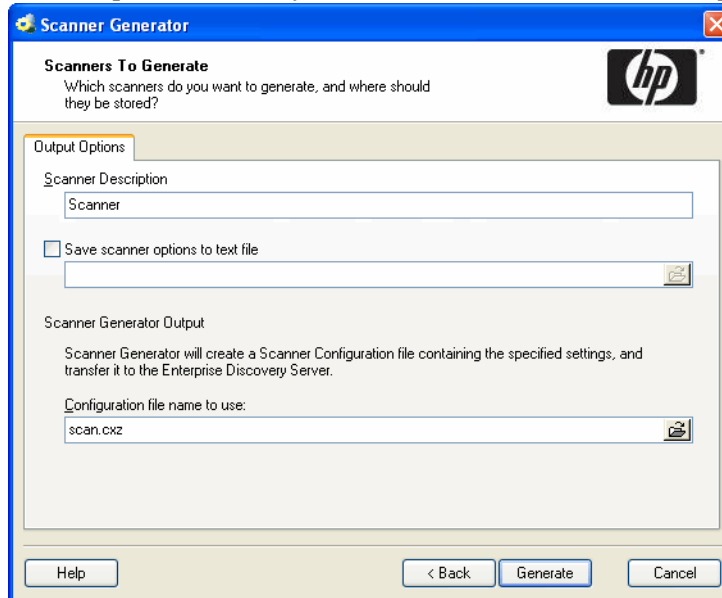
## Additional content for .override.ini file

You can specify additional content for the override files here. Information about the override files and how they are used can be found on [page 121](#).

## The Scanners to Generate Page

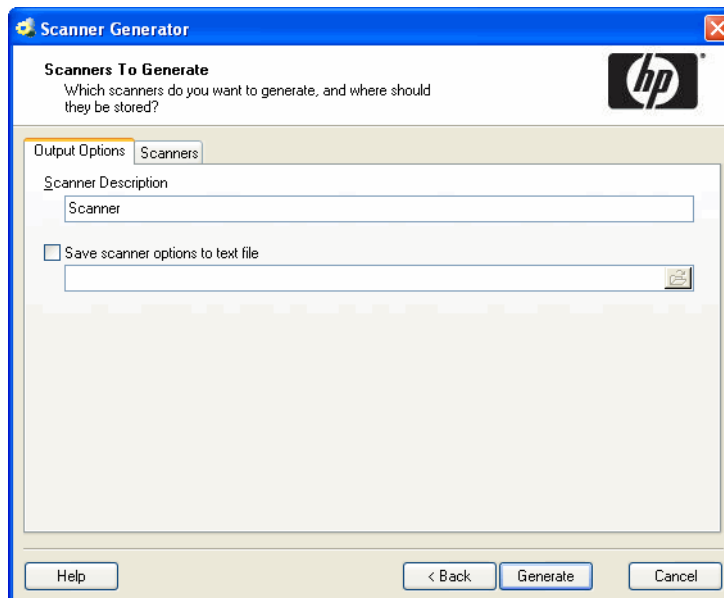
The **Scanners to Generate** page is used to specify which Scanners to generate and where they will be stored.

In Enterprise mode only the **Output Options** tab will be displayed.



The screenshot shows the "Scanner Generator" dialog box with the "Output Options" tab selected. The dialog has a blue title bar and an HP logo. The main content area is divided into sections. The "Scanner Description" section has a text box containing "Scanner". Below it is a checkbox labeled "Save scanner options to text file" which is unchecked, followed by an empty text box. The "Scanner Generator Output" section contains explanatory text and a "Configuration file name to use:" label with a text box containing "scan.cxz". At the bottom are buttons for "Help", "< Back", "Generate", and "Cancel".

In Manual Deployment mode, both the **Output Options** and **Scanners** tab will be displayed.



The screenshot shows the "Scanner Generator" dialog box in Manual Deployment mode. Both the "Output Options" and "Scanners" tabs are visible at the top. The "Output Options" tab is currently active, showing the same fields as the previous screenshot: "Scanner Description" (Scanner), "Save scanner options to text file" (unchecked), and "Configuration file name to use:" (scan.cxz). The "Scanners" tab is also visible but empty. The bottom buttons are "Help", "< Back", "Generate", and "Cancel".



# The Output Options Tab

The **Output Options** page is used to set up Scanner descriptions, save the configuration to a text file if required and for Enterprise mode only, the option to name the configuration (.cxz) file.

## Setting Up a Scanner Description

These options allow you to specify the Scanner description. You can also optionally produce a text 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 a text file:

- In the **Scanner Description** box, enter a description to identify the Scanner.

For example:

Standard PC Inventory - July 18, 2006

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 a Text File

The **Save scanner options to text file** box is used to instruct the Scanner Generator to output a text file containing a complete textual listing of all settings defined elsewhere in the program. Select the check box and specify the path and text file name to which the Scanner options will be saved to. The text file cannot be used by the Scanner Generator, but is intended for user/internal documentation purposes.

## Example Section of the Settings.txt File

You can look at a Settings.txt file using a text editor (such as Notepad). The following listing shows a sample section of such a file:

```
Enterprise Discovery 2.1.0 - 18 August 2006
General Options:
- Description : Scanner
- User can abort Scan
- INI file is used
- XSF is saved offsite
> Save path is \\SERVER\Enterprise Discovery
> XSF Name specified on command line using /O<name>
- Log file .LOG is always created
- Fatal Error Message Line 1: Please write down the above
information, and
- Fatal Error Message Line 2: contact technical support
GUI Scanner Options:
- Scanner runs at normal priority
- Software page is enabled
- User is allowed to expand the view
- Default page: Asset Data
Software scanning is enabled:
- Scanning Default Drives
- Drive selection can be overridden by the command line
- Collection of File Data is enabled
```

## Naming the Configuration (.cxz) File

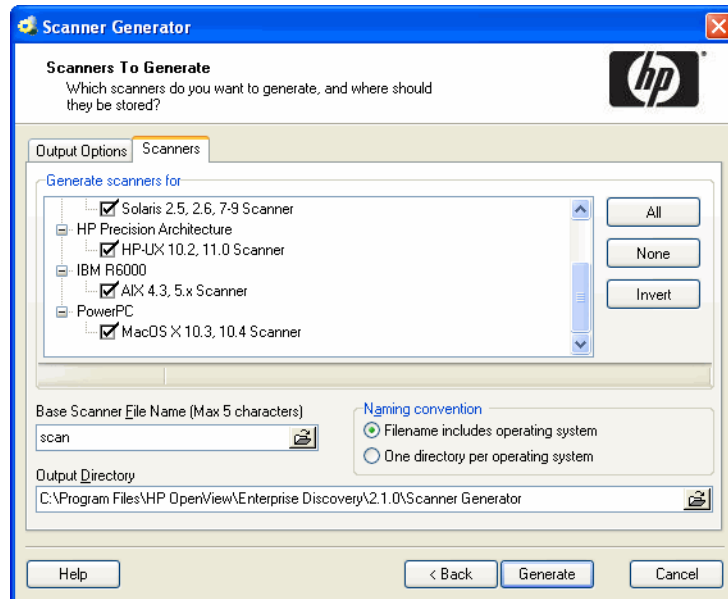
In Enterprise mode the configuration file is saved on the Enterprise Discovery Server as well, using the same file name as the copy specified in the Configuration file name to use field.

The configuration file is a binary 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 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.

## The Scanners Tab

The **Scanners** tab is only available in Manual Deployment mode. It is used to select which of the Scanners to generate.



## 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.

- Whether 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 the 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:

- For all selected Scanners, specify a fully qualified file name. The initial part of this file name (up to five characters) can be entered in the **Base Scanner File Name (Max 5 characters)** 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 can be selected in the **Generate scanners for** list box):

**Table 20 Base Scanner file names and output directories**

Scanner File Name	Scanner Type
scanW32.exe	Windows
scansp2	Solaris 2.5/2.6/7/8/9
scanhpx	HP-UX 10.2, 11.0
scanaix	AIX 4.3, 5.0, 5.1, 5.2, 5.3
scanlnx	Kernel v2.2x, 2.4x, 2.6x
scanmac	Mac OS X 10.3, 10.4

- 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 the Scanners

The **Naming conventions** options determine the manner in which Scanner files are named:

To set naming conventions for the Scanners:

Select one of the following:

- Filename includes operating system**

This option incorporates the Scanner name with the operating system, for example:

ScanW32.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 would appear in directories for all operating system options selected:

C:\ Program files\HP OpenView\Enterprise Discovery\2.1.0\W32\Scan.exe

C:\ Program files\HP OpenView\Enterprise Discovery\2.1.0\Sp2\Scan

C:\ Program files\HP OpenView\Enterprise Discovery\2.1.0\hpx\Scan

C:\ Program files\HP OpenView\Enterprise Discovery\2.1.0\aix\Scan

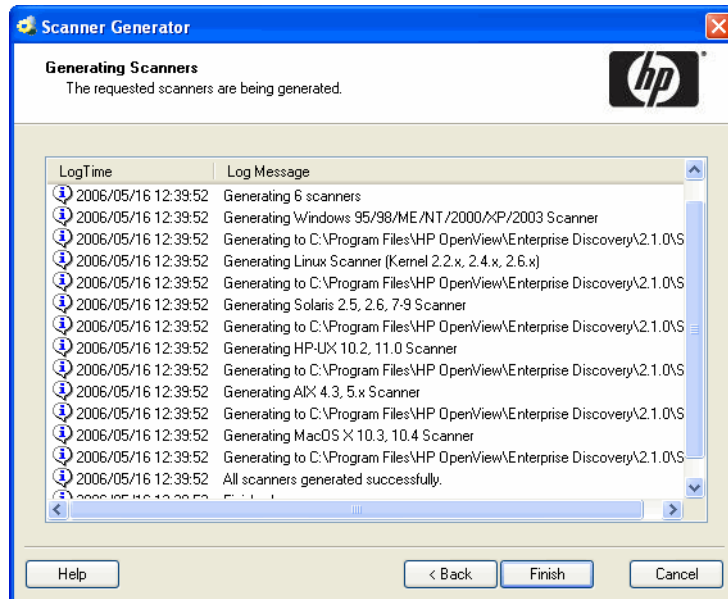
C:\ Program files\HP OpenView\Enterprise Discovery\2.1.0\lnx\Scan

C:\ Program files\HP OpenView\Enterprise Discovery\2.1.0\mac\Scan

- Click the **Generate** button to create the Scanner executable files.

## The Generating Scanners Page

After you have selected the Scanners to be generated and have clicked the **Generate** button, the last page of the Scanner Generator is displayed.



This shows the progress during the generation of the actual Scanner executable. Errors and progress information are shown in the log window.

In Enterprise Mode the Scanner configuration is generated instead of stand-alone Scanners and the configuration is uploaded to the Enterprise Discovery Server.

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, then a confirmation message is displayed. This allows you to choose whether to overwrite the existing Scanner.

After the Scanners have been generated, click the Finish button 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.

XML Enricher looks for new scan files (xsf or dsf format) in the Incoming directory.

If a file is found, it processes the file using SAI (Software Application Index) application recognition.

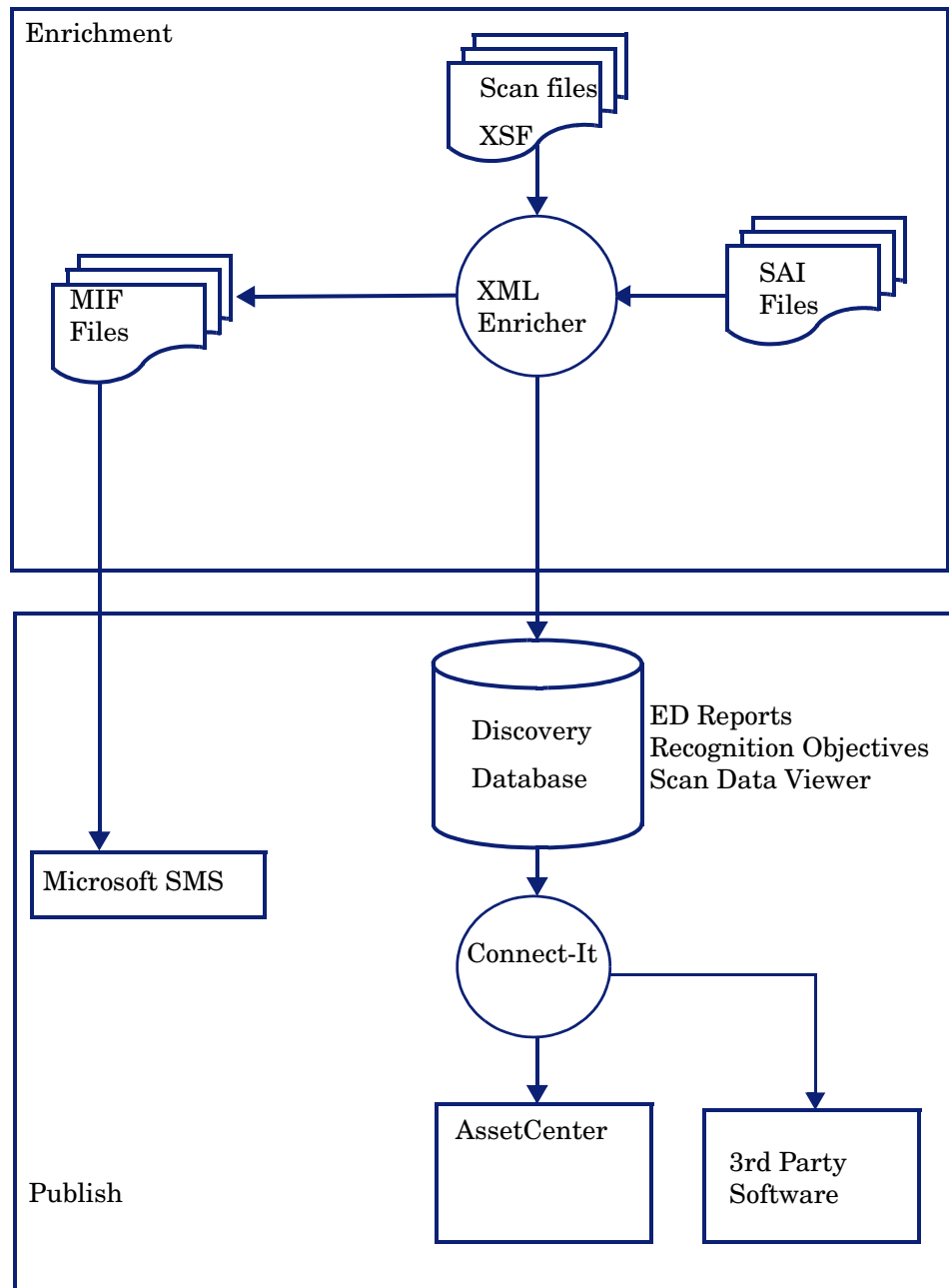
Information about recognized applications is added to the file data and a separate **<applicationdata>** section is added to the XML file.

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.





# The XML Enricher Directory Structure

The XML Enricher uses a directory structure under the **Enterprise Discovery Data** directory.

By default, the Enterprise Discovery Data directory is:

C:\Documents and Settings\All Users\Application Data\Peregrine\Enterprise  
Discovery



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 Enterprise Discovery.

The following table shows the various directories that are used by the XML Enricher.

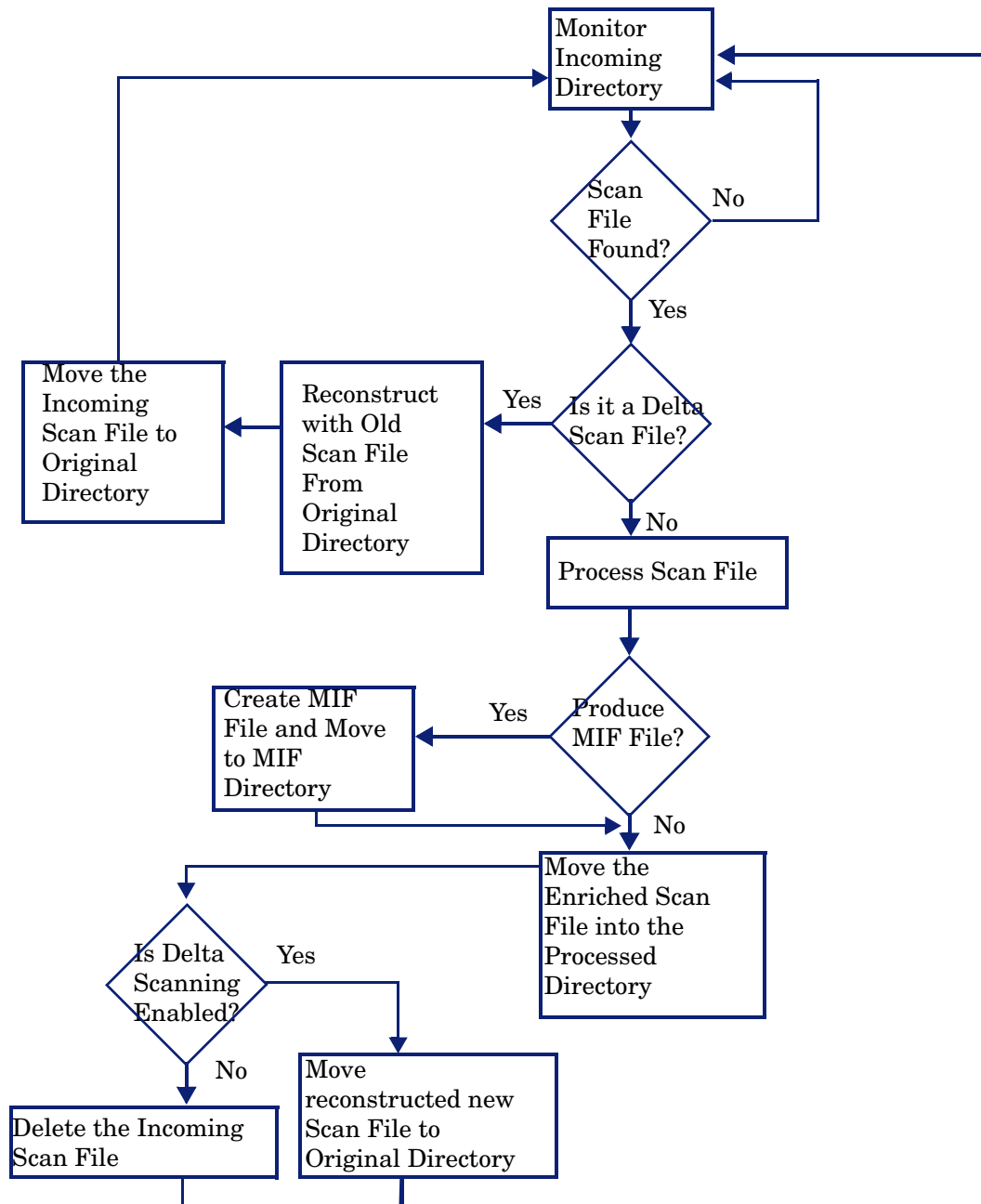
**Table 1 Directories used by the XML Enricher**

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 licences, 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	<p>If the <b>Automatically defer all new scans</b> option was set, the scan file is not processed. See <a href="#">Configuring the XML Enricher Using XML Enricher.ini</a> on page 187.</p> <p>Instead, it is moved to this directory.</p> <p>Any scan files in this directory are from the first time a scan file was seen for a particular computer.</p> <p>This allows the administrator to review the asset and application data.</p> <p>When you are satisfied that the data is OK, you can move it back to the incoming directory.</p> <p>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.</p>

**Table 1     Directories used by the XML Enricher**

<b>Directory</b>	<b>Explanation</b>
\Scans\Incoming	The incoming directory. The enricher looks for new scan files here.
\Scans\Mif	The MIF directory. If enabled, MIF files are created here.
\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: <b>Administration &gt; System Configuration &gt; Scan file management.</b> See <a href="#">Group Processed Scan Files</a> on page 186.
\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.



## 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 Enterprise Discovery Data Directory in the following folders:

```
[Enterprise Discovery 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:

```
[Enterprise Discovery 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 Enterprise Discovery 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\HP OpenView\Enterprise Discovery\2.1.0\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 12345. 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
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 licence for Microsoft Internet Explorer - with this licence, no separate Outlook Express licence is required.

# Configuring the XML Enricher using the Web UI

You can configure the following options to control the XML Enrichment process:

- Application Recognition
- Generate MIF Files
- Automatically Defer All New Scans
- Merge Priority

To configure the XML Enricher:

- 1 Click **Administration > System Configuration > Scan Processing**.
- 2 Set the options as required.

Process utilization data:	<input checked="" type="radio"/> Default: Yes								
	<input type="radio"/> Custom: <input checked="" type="radio"/> Yes <input type="radio"/> No								
Application Recognition:	<input type="radio"/> Default: Yes								
	<input checked="" type="radio"/> Custom: <input checked="" type="radio"/> Yes <input type="radio"/> No								
Generate MIF files:	<input type="radio"/> Default: Never								
	<input checked="" type="radio"/> Custom: <input checked="" type="radio"/> Always <input type="radio"/> Never <input type="radio"/> When SMS is detected								
Automatically defer all new scans:	<input checked="" type="radio"/> Default: No								
	<input type="radio"/> Custom: <input type="radio"/> Yes <input checked="" type="radio"/> No								
Merge priority:	<input checked="" type="radio"/> Default: BIOS asset tag BIOS serial number NetBIOS name and Windows domain MAC Address Asset tag Scan filename								
	<input type="radio"/> Custom: <table><thead><tr><th>Choose From</th><th>Action</th><th>Selected</th><th>Order</th></tr></thead><tbody><tr><td><div></div></td><td><div>Add&gt;&gt;</div></td><td>BIOS asset tag BIOS serial number NetBIOS name and Windows domain MAC Address Asset tag Scan filename</td><td><div>Move Up</div><div>Move Down</div></td></tr></tbody></table>	Choose From	Action	Selected	Order	<div></div>	<div>Add&gt;&gt;</div>	BIOS asset tag BIOS serial number NetBIOS name and Windows domain MAC Address Asset tag Scan filename	<div>Move Up</div> <div>Move Down</div>
Choose From	Action	Selected	Order						
<div></div>	<div>Add&gt;&gt;</div>	BIOS asset tag BIOS serial number NetBIOS name and Windows domain MAC Address Asset tag Scan filename	<div>Move Up</div> <div>Move Down</div>						

## Process utilization data

If you want to stop collecting utilization data, turn this option off. The default option is **Yes**.



Enterprise Discovery can only collect Utilization data if you have a license for it.

## Application Recognition

There are two options for Application Recognition:

- **Yes**

This is the default setting. 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 `cfgFilterFlag` setting in the XML Enricher.ini file.

- **No**



No files are sent to the recognition engine for processing. In this state, no <applicationdata> section will be added to the scan files.

## Generate MIF Files

There are three options for Generating MIF Files.

- **Always**

The XML enricher will always produce MIF files from scan files.

- **Never**

The XML enricher will never produce MIF files from scan files. This is the default option.

- **When SMS is Detected**

Only scan files with a value in the hwOSMIFPath field will cause a MIF file to be produced (i.e. computers where the SMS client is installed).

## 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. It is only used when scan files are placed in the Incoming directory. If the Scanners are automatically launched by Enterprise Discovery, then this option is not 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 Enterprise Discovery.

# 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:	<input checked="" type="radio"/> Default: Always
	<input type="radio"/> Custom: <input checked="" type="radio"/> Always <input type="radio"/> On purge <input type="radio"/> Never
<b>Group Processed Scan Files</b>	
Group processed scan files by primary:	<input checked="" type="radio"/> Default: <input type="text"/>
	<input type="radio"/> Custom: <input type="text"/>
Group processed scan files primary blank:	<input checked="" type="radio"/> Default: unknown
	<input type="radio"/> Custom: <input type="text"/>
Group processed scan files by secondary:	<input checked="" type="radio"/> Default: <input type="text"/>
	<input type="radio"/> Custom: <input type="text"/>
Group processed scan files secondary blank:	<input checked="" type="radio"/> Default: unknown
	<input type="radio"/> Custom: <input type="text"/>
Group processed scan files by tertiary:	<input checked="" type="radio"/> Default: <input type="text"/>
	<input type="radio"/> Custom: <input type="text"/>
Group processed scan files tertiary blank:	<input checked="" type="radio"/> Default: unknown
	<input type="radio"/> Custom: <input type="text"/>

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 Enterprise Discovery 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 the application library used by the 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\HP OpenView\Enterprise Discovery\2.1.0\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.

## Configuring the XML Enricher Using XML Enricher.ini

The ini file is called XML Enricher.ini and by default can be found in:

[Enterprise Discovery Data Directory]\Conf

By default, the Enterprise Discovery Data directory is:

C:\Documents and Settings\All Users\Application Data\HP OpenView\Enterprise Discovery

The Data Directory is customizable during the installation process.

## The XML Enricher ini File Sections

The XML Enricher ini file can contain three main configurable sections:

- [RecognitionConfig Section](#)
- [RecognitionConfig.RecognitionConfig\\_cfgJunk Filters Section](#)
- [RecognitionConfig.RecognitionConfig\\_cfgSAIFiles Section](#)
- [AssetFieldConfig Section](#)

The options available in each are described in the following sections.

## RecognitionConfig Section

The RecognitionConfig section is where the application recognition setup is defined. It corresponds to the controls available on the Recognition tab of the Options dialog box in Viewer and Analysis Workbench.

The easiest way to edit the recognition settings is to start Viewer, change the settings and copy the [RecognitionConfig] section from Viewer's ini file (Viewer.ini) to the XML Enricher.ini file.

```
cfgAutoIdentifyDeviceDriverFiles=True  
cfgExtensions=EXE;COM;DLL
```

```

cfgFilterFlags=[ffeAll,ffeExeOnly]
cfgForceLanguage=False
cfgJunkBeforeFiltered=True
cfgPreferredLanguageCode=
cfgRecognition=rtSai
cfgReprocess=True
cfgUseEnriched=True
cfgUseJunkFilter=False
cfgAutoSai=-1

```

**Table 2 RecognitionConfig Section options**

Option	Explanation
cfgAutoIdentifyDeviceDriver Files True/False	When enabled (the default), files that cannot be identified by the standard SAI recognition and have the Device Driver attribute will be marked as recognized in the enriched scan file.
cfgAutoSai	Any items encountered that were created by rules will be added to a file called <b>Auto.zsai</b> and put this in the same location as the first Master SAI.  These rules are present within the SAI files themselves and additional rules can be added using SAI Editor.
cfgExtensions	This is a recognition filter that determines which of the files are sent to the recognition engine for processing (ignored if ffeInclExt is not specified).
cfgFilterFlags	Decides what files to process for recognition ffeAll (all files) ffeExeOnly (only executable files) ffeNoArc (don't load files in archives) ffeInclExt (include the files with extensions listed in cfgExtensions) Items must be separated by comma and enclosed in square brackets.
cfgForceLanguage True/False	Check the Override OS Language box if you want the recognition engine to overlook the operating system locale setting and take the setting you specified in the Preferred language box.

**Table 2 RecognitionConfig Section options**

Option	Explanation
cfgPreferredLanguageCode	Preferred language is used for cases when the recognition engine encounters more than one language version of the same file– for example, Microsoft Word in English and in French. Because these versions are equally recognized, this setting instructs the recognition server on which of the versions to select.
cfgRecognition	Chooses the recognition method that will be used (one of rtSAI, rtNone, rtInstalled).
cfgReprocess True/False	If this option is enabled, the recognition engine defers its final recognition decision until all the files in all the directories on the machine have been read. If disabled, 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.
cfgUseEnriched True/False	If SAI recognition is not used and the Installed Applications option is used for recognition, then the application data from the enriched scan file is used instead of running ‘real’ recognition.
cfgUseJunkFilter True/False	<p>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, TMP000001.\$\$\$.</p> <p>This option is a way for the recognition engine to ignore such files, by allowing one or more file name masks to be specified as ‘junk’.</p> <p>These files are not passed to the recognition engine and will be marked as junk</p>

## RecognitionConfig.RecognitionConfig\_cfgJunk Filters Section

This section corresponds to the junk filter options in the Filtering tab of the configuration dialog in Viewer and Analysis Workbench.

Some files may be executable but are of no interest for licensing or other purposes. The Treat Files matching the following regular expressions as junk option is a way for the recognition engine to ignore such files, by allowing one or more file name masks to be specified as 'junk'.

```
RecognitionConfig.RecognitionConfig_cfgJunk Filters
Count = 2
Item0 = *.dat
Item1 = *.tmp
```

**Table 3 RecognitionConfig.RecognitionConfig\_cfgJunk Filters options**

Option	Explanation
Count	Number of file name masks to be matched and treated as junk.
Item [0 to n]	The file name mask (regular expression) to be matched and treated as junk.

## RecognitionConfig.RecognitionConfig\_cfgSAIFiles Section

This section defines the Software Application Index (ZSAI) files to use when SAI recognition is used. Again, copying this information from Viewer.ini is the easiest way of editing it.

If this section is not present in the ini file, the enricher automatically searches the HP OpenView\Enterprise Discovery\2.1.0\Common directory for SAI files and uses the appropriate SAI files in this directory for recognition.

It 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-substet locations.

Here is an example of this section:

```
[RecognitionConfig.RecognitionConfig_cfgSAIFiles]
Count=2
Item0=C:\Program Files\HP OpenView\Enterprise
Discovery\2.1.0\Common\User.zsai
Item1=C:\Program Files\HP OpenView\Enterprise
Discovery\2.1.0\Common\Master.zsai
```

## AssetFieldConfig Section

Each of the Analysis Asset fields is defined in its own section. The first field has a section name [Field\_AssetFieldConfig\_0], with Line\_N fields containing the actual setup.

The easiest way to edit the settings is to start Viewer, change the settings for Analysis Asset fields and copy the [AssetFieldConfig] section from Viewer's ini file (Viewer.ini) to the XML Enricher.ini file.

## Starting and stopping the XML Enricher service in the web UI

If you make changes to the XML Enricher.ini file to configure the XML Enricher you will need to stop and start the XML Enricher service manually.



Stopping the service in Windows Control Panel will not work. The System Monitor will notice it is not running and re-start it unless this option is set to 'No'.



You must make sure that the XML Enricher is started and configured if you want application data to be added to your scan files.

To manually start or stop the xml enricher service:

- 1 Click Administration > System Configuration > Discovery Services.
- 2 Scroll down to the **XML Enricher Active** entry.

### Discovery services

Server > Admin > System Preferences > Discovery Services

Configures the server, services.

Explorer ping active:	<input checked="" type="radio"/> Default:	Yes
	<input type="radio"/> Custom:	<input checked="" type="radio"/> Yes <input type="radio"/> No
Table reader active:	<input checked="" type="radio"/> Default:	Yes
	<input type="radio"/> Custom:	<input checked="" type="radio"/> Yes <input type="radio"/> No
Automatic agent deployment active:	<input checked="" type="radio"/> Default:	Yes
	<input type="radio"/> Custom:	<input checked="" type="radio"/> Yes <input type="radio"/> No
Automatic scanner deployment active:	<input checked="" type="radio"/> Default:	Yes
	<input type="radio"/> Custom:	<input checked="" type="radio"/> Yes <input type="radio"/> No
Device modeler active:	<input checked="" type="radio"/> Default:	Yes
	<input type="radio"/> Custom:	<input checked="" type="radio"/> Yes <input type="radio"/> No
XML Enricher active:	<input checked="" type="radio"/> Default:	Yes
	<input type="radio"/> Custom:	<input checked="" type="radio"/> Yes <input type="radio"/> No

Change

- 3 Click **Yes** to start the service, or click **No** to stop the service.
- 4 Click **Change** to activate the desired state.

## Structure of the 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\HP OpenView\Enterprise Discovery\2.1.0\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>

## An Example of How the 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)" xsfmajorver="7"
xsfminorver="5" enricherver="8.0.0.3125">
<hardwaredata>
  <hwAssetData type="shell">
    <hwAssetDescription type="attrib">Dallas (125 North Drive) - - (Pentium
    III, 448MHz, 256Mb)</hwAssetDescription>
    <hwAssetTag type="attrib">000590 </hwAssetTag>
    <hwAssetUserLastName type="attrib">tod.brown@.com</hwAssetUserLastName>
    <hwAssetUserJobTitle type="attrib">Dallas (15950 North Dallas Parkway)</
    hwAssetUserJobTitle>
  </hwAssetData>
  <hwMemoryData type="shell">
    <hwMemTotalMB type="attrib">256</hwMemTotalMB>
    <hwSwapFiles type="shell">
      <hwSwapFiles_value type="shell_value">
        <hwMemSwapFileName type="attrib">C:\pagefile.sys</hwMemSwapFileName>
        <hwMemSwapFileSize type="attrib">203</hwMemSwapFileSize>
      </hwSwapFiles_value>
    </hwSwapFiles>
    <hwDOSMemoryData type="shell">
      <hwMemConventional type="attrib">640</hwMemConventional>
    </hwDOSMemoryData>
    <hwCMOSMemory type="shell">
      <hwMemExtended type="attrib">260724</hwMemExtended>
      <hwMemCMOSTotal type="attrib">261364</hwMemCMOSTotal>
      <hwMemCMOSConventional type="attrib">640</hwMemCMOSConventional>
    </hwCMOSMemory>
  </hwMemoryData>
</hardwaredata>
<applicationdata>
<recogconfig>
<sai name="C:\Program Files\HP OpenView\Desktop
Inventory\2.1.0\Common\User.zsai" desc="User SAI File" date="14/04/2004"
type="Editable"/>
```



```

        <sai name="C:\Program Files\HP OpenView\Desktop
Inventory\8.0.0\Common\Master.zsai" desc="" date="07/05/2004"
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="2003-09-26 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="2004-05-05 00:00:00"
versionid="12790" releaseid="131"
/>
</applicationdata>
<filedata>
    <dir name="C:\" date="2005-07-03 03:23:04" contains="-1">
        <file name="AUTOEXEC.BAT" size="0" modified="2000-04-03 13:51:04"
attr="a"/>
        <file name="BOOT.INI" size="288" modified="2000-04-03 15:14:38"
attr="rsa"/>
        <file name="sd_settings.ini" size="462" msdos="SD_SET~1.INI"
modified="2001-06-14 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>
```

# 14 Getting Your Data into AssetCenter

This chapter explains how you can get your data from Enterprise Discovery into AssetCenter using the out-of-the-box Enterprise Discovery 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, Enterprise Discovery, AssetCenter and Connect-It.
- You have already installed AssetCenter and Connect-It on a machine.
- You are using the following software versions:
  - Enterprise Discovery version 2.1
  - Connect-It version 3.6
  - AssetCenter 4.4
- 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 Enterprise Discovery to AssetCenter Connect-It scenario is supplied with Connect-It not Enterprise Discovery. You can find the scenario files (.scn) in the following default location:

C:\Program Files\HP OpenView\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 Enterprise Discovery Server.

## Compatibility

The Enterprise Discovery 2.0 connector is fully compatible with AssetCenter 4.4.  
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 Enterprise Discovery 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 - Enterprise Discovery
- Task 3: Configure the Destination Connector - AssetCenter

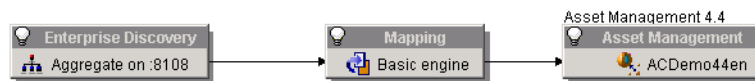
## Step 1: Open the scenario


- 1 Select **Open** from the **File** menu and navigate to the Enterprise Discovery to Asset Management out-of-the-box scenario edac.scn file.

By default this file is located in:

C:\Program Files\HP OpenView\ConnectIt\scenario\ed\ed2ac44

A three box scenario diagram is now shown.



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 Enterprise Discovery-AssetCenter out-of-the-box scenario.

## Step 2: Configure the Source Connector - Enterprise Discovery

Click on the title bar of the Enterprise Discovery connector box to highlight it.

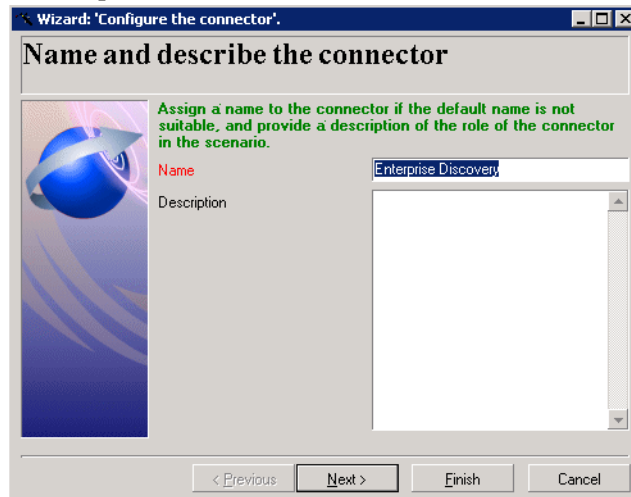
To configure the connector you can either:

- Right-click on the Enterprise Discovery 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 Enterprise Discovery connector is displayed.

## Page 1: Name and describe the connector

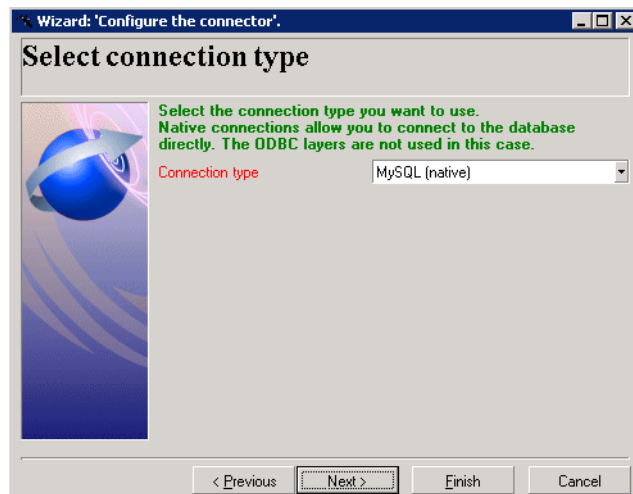
The first page of the wizard enables you to name the Enterprise Discovery connector and add a description for it.



- 1 **Name:** By default, the value of this field is Enterprise Discovery.
- 2 **Description:** Enter text to describe the connector. This field is not mandatory.
- 3 Click the **Next** button to continue.

## Page 2: Select a connection type

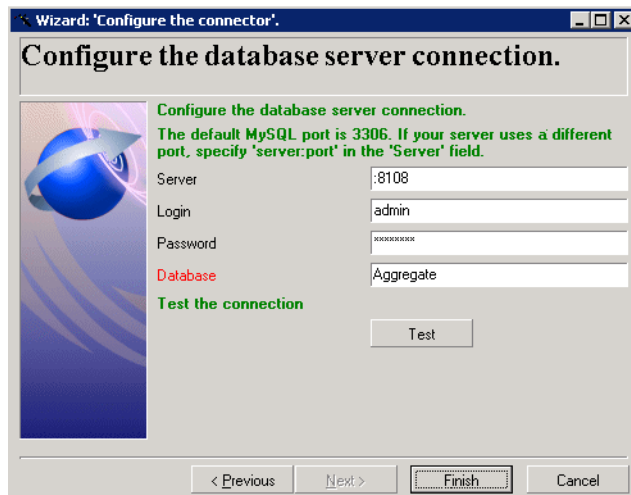
This page allows you to specify the connection protocol.



For the purpose of Enterprise Discovery this should always be MySQL (native). Click **Next** to continue.

## Page 3: Define the database server connection

This page allows you to set up the connection to the Enterprise Discovery database.



### 1 Server

Enter the port used for the database server connection.

If the Connect-It installation is on a different computer from the Enterprise Discovery Server, enter the DNS name or IP address of the Enterprise Discovery 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 Enterprise Discovery 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

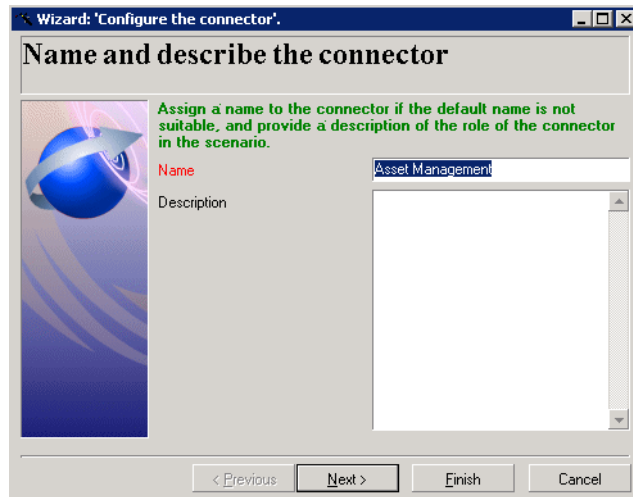
Click on the title bar of the Asset Management connector to highlight it. To configure the connector you can either:

- 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

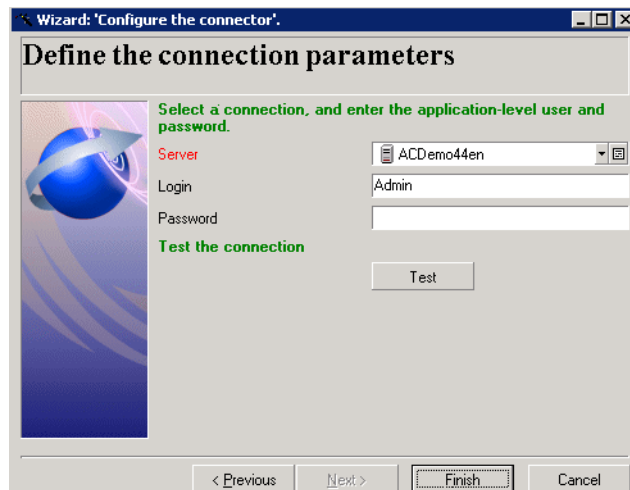
The first page of the wizard enables you to name the Asset Management connector and provide a description for it.

The screenshot shows a Windows-style wizard window titled 'Wizard: 'Configure the connector''. The main heading is 'Name and describe the connector'. On the left is a blue sphere icon with a white arrow. To the right of the icon, green text reads: 'Assign a name to the connector if the default name is not suitable, and provide a description of the role of the connector in the scenario.' Below this, there are two fields: 'Name' with the text 'Asset Management' and 'Description' with an empty text area. At the bottom are four buttons: '< Previous', 'Next >', 'Finish', and 'Cancel'.

- 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.

## Page 2: Define the connection parameters

This page allows you to set up the connection to your AssetCenter database.

The screenshot shows the second page of the wizard, titled 'Define the connection parameters'. It features the same blue sphere icon on the left. Green text instructs: 'Select a connection, and enter the application-level user and password.' Below this, there are three input fields: 'Server' (a drop-down menu showing 'ACDemo44en'), 'Login' (a text box with 'Admin'), and 'Password' (an empty text box). A 'Test the connection' button is located below the password field. At the bottom are four buttons: '< Previous', 'Next >', 'Finish', and 'Cancel'.

- 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**



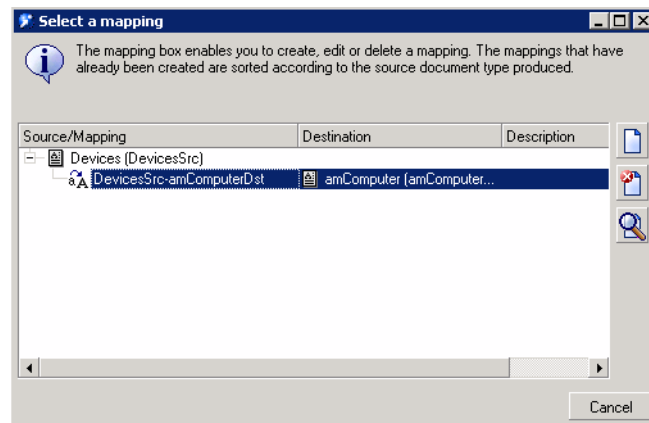
In this case (demo database) you do not need to enter a password.

- 4 Now test the connection to the database.
- 5 Click **Finish** to finalize the basic configuration of the connector.

## Check your 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** - Enterprise Discovery - shows the Inventory document that is produced by Connect-It which contains the Enterprise Discovery structures, collections and fields as represented by Connect-It
  - **Mapping** - shows the actual mappings between Enterprise Discovery 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 Enterprise Discovery 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 the reconciliation keys

Reconciliation is the integration of input data coming from Enterprise Discovery 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 your Enterprise Discovery-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 Enterprise Discovery connector. Refer to the *Connect-It Users Guide* for more information about logs.

## Get the 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 Enterprise Discovery.

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 Enterprise Discovery 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 Enterprise Discovery 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.

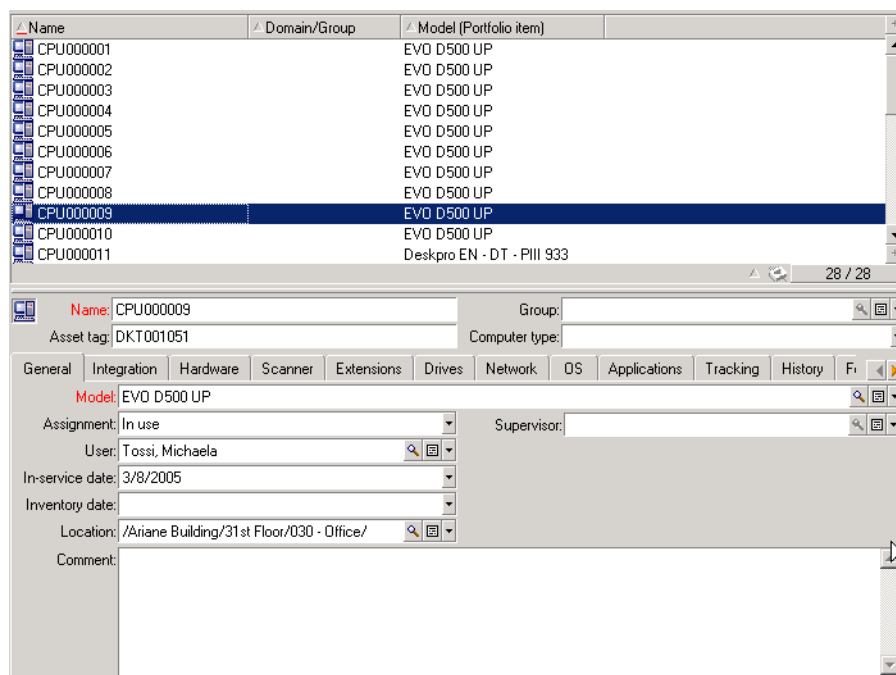
You can unfold or collapse messages by right-clicking and then selecting the appropriate command from the shortcut menu.

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 the 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 Enterprise Discovery scans has been populated into fields in the **Computers** tab in the AssetCenter database.



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 about these customization options and tasks.

## Importing and processing Enterprise Discovery 2.1 Utilization Data in AssetCenter



This section only applies if you have purchased the Enterprise Discovery Software Utilization license.

In Enterprise Discovery 2.1, 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

## A

Access Query, Creating, 63, 65

### account

- adding an account, 16
- changing name, 17
- changing the type, 17
- customizing a profile, 17
- deleting, 21
- listing user accounts, 16
- modifying contact information, 20
- modifying password, 20
- setting type, 17
- types
  - admin, 15
  - demo, 14
  - IT employee, 14
  - IT manager, 14
  - Scanner, 15

### account properties

- account type, 17
- allow to copy map configurations, 17
- append IP address, 17
- default device panel, 18
- default port panel, 18
- long date format, 17
- make URLs visible, 17
- name, 17
- short date format, 18

ACSKeyStore.bin, 86

acstrust.cert, 86

activating devices, 56

### Adding

- directories and files to the override file, 122
- file filter storage criteria in SG, 130

adding a new device, 48

### admin account

- customizing the Network Map, 75
- description, 15

## Administration

- account contact information, 20
- account password, modifying, 20
- adding an account, 16
- customizing a user profile, 17
- deleting an account, 21
- deleting connections, 69
- device deactivation intervals, 52
- event filters, 31
  - delete, 46
  - list, 46
  - modify, 45
  - reset to defaults, 46
- expiry controls, 52
- listing user accounts, 16
- test e-mail address, 23
- test pager address, 23

## Agent

### deployment

- automatic, 90
- custom, 89
- manual, 90
- via listener, 87
- via login scripts, 90
- via Win32 RPC, 88

directories, 87

media files, 86

security, 86

uninstalling

- agent, 92

upgrade

- unix agent, 91
- win 32 agent, 91

agentca.pem, 86

## AIX Scanner

### setting up

- file name and output directory, 171
- supported platforms, 102

## alarm thresholds

- changing, 71
- copy and paste values, 73
- device types, 71
- line alarm types, 72

Allow command line override option, 116

- Apache
  - setup for saving to, 162
- application library, 187
- Asset fields
  - configuring in SG, 140
- Asset number
  - choosing a source for, 156
- Asset tag field, 141
- ATAPI
  - disabling hardware detection routine, 111
- automatically defer all new scans, 185

## B

- BIOS
  - disabling hardware detection routine, 111
- Bus Detection
  - disabling hardware detection routine, 111

## C

- Calculated fields
  - in SG, 144
- Cascade Database
  - Using With Microsoft Access, 60
- CD-ROM drives
  - creating a customized drive selection, 119
- Changing
  - directories scanned to locate files, 136
- Classic local drive scan, 114
- Combination fields
  - setting up in SG, 150
- Combined scan, 114
- Command line
  - offsite scan file name, 156
  - offsite scan file save location, 159
  - override option in scanner generator, 116
- Compaq Asset Tag
  - disabling hardware detection routine, 111
- Compressed Drives
  - creating a customized drive selection, 120
- Configuring
  - agent communication, 95
- connections
  - deleting, 69
- copy
  - alarm thresholds command, 73
- copying map configurations, 13

- CPU identification
  - disabling hardware detection routine, 111
- Creating An Access query, 63, 65

## D

- data access applications
  - ODBC, 57
- date format, change, 17
- DCC data
  - disabling hardware detection routine, 111
- d command line switch, 180
- deactivate, 51
- deactivate device, 55
- deactivation intervals, 52
- default map configuration, 12
- deferred directory
  - firstscan, 185
- deleting connections, 69
- deleting data, 67
- Delta calculation utility, 180
- Delta scanning
  - command line utility, 180
  - delta scan files, 180
  - enabling delta scanning, 159
  - setting up the scanners to handle them, 180
- demo account, description, 14
- Derived fields
  - in SG, 145
- Description field, 141
- device
  - activating, 56
  - adding, 48
  - changing IP address, 50
  - changing ports, 50
  - deactivate, 55
  - deactivating, 53
  - hide, 54
  - purge, 54
  - purging, 53
  - remove automatically, 51
  - removing, 53
  - replacing, 49
- device, disconnecting, 12
- Device driven drives
  - creating a customized drive selection, 120
  - selecting a pre-defined type of drive to scan, 117
- Device Manager
  - changing default panel, 17, 18



- device priority
  - changing, 76
- device tag
  - changing, 76
- device title
  - changing, 76
- device types, 71
- disconnecting
  - map session, 12
- discusg.cxu, 94
- Disk space
  - xml enricher, 177
- Drives
  - creating a customized drives selection, 119
  - disabling hardware detection routine, 111
  - selecting a pre-defined type of drive to scan, 117
- DSF file
  - definition, 100

**E**

- ED Server
  - connecting to in SG, 106
- EISA
  - disabling hardware detection routine, 111
- e-mail
  - change account e-mail address, 20
  - test your e-mail address, 23
- Enhanced CPU ID
  - disabling hardware detection routine, 111
- Enterprise mode, 105
- Environment fields
  - setting up in SG, 147
- event filters, 31
  - definition, 33
  - delete, 46
  - examples, 37
  - list, 46
  - modify, 45
  - preparation, 34
  - reset to defaults, 46
- Exiting
  - scanner generator, 103
- expiry, 51, 52
- Extract field options
  - setting in SG, 154

**F**

- FAT
  - creating a customized drive, 119
- Field data type
  - selecting, 143
- Field parameters
  - setting in SG, 145
- File associations
  - including in targeted scan, 124
- firstscan directory, 185
- Floppy drives
  - creating a customized drive selection, 119
  - selecting a pre-defined type of drive to scan, 117
- Forensic scan, 108
  - selecting as preset scanner configuration, 106
- French SAI
  - application recognition in the xml enricher, 189, 190
- FTP URL
  - for offsite save path, 161

**G**

- Generating scanners, 171
- German SAI
  - application recognition in the xml enricher, 189, 190

**H**

- Hardware data
  - disabling hardware detection routine, 110
  - selecting as data to be collected by scanner, 109
  - structure in an xsf file, 191
- Hardware detection
  - disabling, 111
- help format
  - change, 17
- hiding devices, 54
- HPFS
  - creating a customized drive selection, 119
- HP-UX Scanner
  - setting up file name and output directory, 171
  - supported platforms, 102
- HTTP URL
  - for offsite save path, 161
  - saving on Apache and IIS Web Servers, 162

- I**
- I/O ports
  - disabling hardware detection routine, 111
- Icons
  - files to scan list box in scanner generator, 125
- icons
  - changing, 76
- IDE
  - disabling hardware detection routine, 111
- IIS
  - setup for saving to, 162
- Inventory scan, 107
  - selecting as preset scanner configuration, 106
- IP address
  - append to device labels, 17
  - changing in a device, 50
- IPX/SPX
  - disabling hardware detection routine, 111
- ISA PnP cards
  - disabling hardware detection routine, 111
- IT employee account, description, 14
- IT manager account, description, 14
- J**
- Java class files
  - enabling in SG, 106, 108
- Java Home directory
  - including in targeted scan, 124
- K**
- Keyboard
  - disabling hardware detection routine, 111
- keyboard shortcuts
  - scanner generator user entry form, 138
- L**
- Language options
  - setting in xmilenricher, 187
- Licence
  - default directory used in xml enricher, 177
  - using targeted directory scan for software licence accuracy, 115
- line alarm types, 72
- Line Manager
  - default panel
  - changing, 17
- Linking Cascade Tables, 60
- Linux Scanner
  - setting up file name and output directory, 171
  - supported platforms, 102
- Listener
  - agent deployment, 87
  - uninstalling, 93
- LiveAgent, 87
- local\$ file, 158
- Local scan file
  - saving, 158
- login
  - enabling, 17
- Login scripts
  - agent deployment, 90
- Logs
  - creating in scanner generator, 162
  - log window in scanner generator, 173
  - xml enricher, 182
- long date format, 17
- M**
- Manual deployment
  - agent, 90
- Manual deployment mode, 105
- map configuration
  - allowing others to copy, 17
  - copy permissions, 17
- Master SAI
  - application recognition in the xml enricher, 189, 190
- MCA
  - disabling hardware detection routine, 111
- media files, 86
- Memory
  - disabling hardware detection routine, 111
- MIF files, 178
- modem
  - external (for paging), 24
- Mouse
  - disabling hardware detection routine, 111
- N**
- name of account, 17
- NetBIOS/NETBEUI
  - disabling hardware detection routine, 111
- Network
  - saving scan results to, 159

- Network drives
  - creating a customized drive selection, 120
  - selecting a pre-defined type of drive to scan, 117

- Network information
  - disabling hardware detection routine, 111

- Network Map
  - change icon, 76

- NMID, 89

- No UI Scanner
  - setting up file name and output directory, 171

- NTFS
  - creating a customized drive selection, 119

## O

- Offsite scan file
  - saving, 158

- OS/scan fields
  - setting up in SG, 150

- Override option, 116

## P

- pager
  - change account information, 20

- pager address
  - testing, 23

- password
  - account, modifying, 20

- paste
  - alarm thresholds command, 73

- Peripherals
  - disabling hardware detection routine, 111

- Plug'n'Play
  - disabling hardware detection routine, 111

- Port Manager
  - changing default panel, 18
  - default panel
    - changing, 17

- priority
  - device, 76

- purge, 51

## R

- Rawmedia, 86

- Registry extract fields
  - setting up in SG, 149

- removing a device
  - automatically, 51
  - manually, 53

- replacing a device, 49

## S

- Saving

- scanner options to text file, 169

- scan results
    - locally, 158
    - to network, 159

- Scanner

- components, 100
  - disabling hardware detection routines, 111
  - enabling scanning of java class files, 108
  - saving options to text files, 169
  - selecting directories to scan, 123
  - selecting hardware data to collect, 109
  - selecting type of scanner to create, 107
  - selecting which to generate, 171
  - setting naming conventions, 172
  - setting up descriptions, 169
  - software scanning modes, 114
  - supported platforms, 102
  - time-out options, 164

- Scanner account, description, 15

- Scanner configuration file
  - reading setting from, 106

- Scanner generator
  - enterprise mode, 105
  - manual deployment mode, 105
  - starting, 103

- SCSI

- disabling hardware detection routine, 111

- Security

- agent
    - Certificates
      - agent, 86

- selection, 119

- Sequence fields
  - setting up in SG, 146

- Settings.txt, 170

- Shallow scan, 107
  - selecting as preset scanner configuration, 106

- short date format, 18

- SMBIOS

- disabling hardware detection routine, 111

- Software scanning modes, 114

- Software utilization plug-in, 94

- Solaris Scanner

- setting up file name and output directory, 171
  - supported platforms, 102

Standard fields, 141

Starting  
    scanner generator, 103

status  
    receive reports by e-mail, 17

Stored files  
    setting up in SG, 134

SUBST'ed drives  
    creating a customized drive selection, 120

## T

Targeted directory scan, 114

Text fields  
    in SG, 144

Text file  
    saving scanner options to, 169

Text file extract  
    setting up field in SG, 147

thresholds  
    alarm  
        changing, 71  
    device, 71  
    line alarms, 72

type of account  
    setting, 17

## U

UNC path  
    for offsite save path, 160

Uninstalling  
    agent, 92

Unix Scanners  
    supported platforms, 102

Upgrading  
    unix agent, 91  
    win 32 agent, 91

URL  
    make visible, 17

user accounts, listing, 16

User prompt  
    setting up in SG, 140

utilization plug-in, 94

## V

VFAT  
    creating a customized drive selection, 120

Virtual machines, 165

## W

Welcome page, 105

Win 32 RPC  
    agent deployment, 88

Windows 16-bit Scanner  
    setting up  
        file name and output directory, 171

Windows 32-bit Scanner  
    setting up file name and output directory, 171

Windows Scanner, 102

Windows services  
    including in targeted scan, 124

WMI extract fields  
    setting up in SG, 152

## X

XML Enricher  
    application library, 187

XML enricher  
    directory structure used, 177  
    disk space requirement, 177  
    log files, 182  
    structure of the xml file, 191

XSF  
    contents of, 192  
    creating, 179  
    definition, 100  
    enriching with xml enricher, 175

XSFDelta.exe, 180