

Peregrine Systems, Inc.

Enterprise Discovery™ 2.0.1



Configuration and Customization



Copyright © 2005 Peregrine Systems, Inc.

PLEASE READ THE FOLLOWING MESSAGE CAREFULLY BEFORE INSTALLING AND USING THIS PRODUCT. THIS PRODUCT IS COPYRIGHTED PROPRIETARY MATERIAL OF PEREGRINE SYSTEMS, INC. ("PEREGRINE"). YOU ACKNOWLEDGE AND AGREE THAT YOUR USE OF THIS PRODUCT IS SUBJECT TO THE SOFTWARE LICENSE AGREEMENT BETWEEN YOU AND PEREGRINE. BY INSTALLING OR USING THIS PRODUCT, YOU INDICATE ACCEPTANCE OF AND AGREE TO BE BOUND BY THE TERMS AND CONDITIONS OF THE SOFTWARE LICENSE AGREEMENT BETWEEN YOU AND PEREGRINE. ANY INSTALLATION, USE, REPRODUCTION OR MODIFICATION OF THIS PRODUCT IN VIOLATION OF THE TERMS OF THE SOFTWARE LICENSE AGREEMENT BETWEEN YOU AND PEREGRINE IS EXPRESSLY PROHIBITED.

Information contained in this document is proprietary to Peregrine Systems, Incorporated, and may be used or disclosed only with written permission from Peregrine Systems, Inc. This book, or any part thereof, may not be reproduced without the prior written permission of Peregrine Systems, Inc. This document refers to numerous products by their trade names. In most, if not all, cases these designations are claimed as Trademarks or Registered Trademarks by their respective companies.

Peregrine Systems, Enterprise Discovery, AssetCenter and ServiceCenter are trademarks or registered trademarks of Peregrine Systems, Inc. or its affiliates.

This document and the related software described in this manual are supplied under license or nondisclosure agreement and may be used or copied only in accordance with the terms of the agreement.

The information in this document is subject to change without notice and does not represent a commitment on the part of Peregrine Systems, Inc. Contact Peregrine Systems, Inc., Customer Support to verify the date of the latest version of this document. The names of companies and individuals used in the sample database and in examples in the manuals are fictitious and are intended to illustrate the use of the software. Any resemblance to actual companies or individuals, whether past or present, is purely coincidental. If you need technical support for this product, or would like to request documentation for a product for which you are licensed, contact Peregrine Systems, Inc. Customer Support by email at support@peregrine.com. If you have comments or suggestions about this documentation, please contact Peregrine Systems, Inc. Technical Publications by email at doc_comments@peregrine.com. This edition applies to version 2.0.1 of the licensed program.

For more copyright information, see the Copyright chapter of the Enterprise Discovery Reference Guide.

Peregrine Systems, Inc.
3611 Valley Centre Drive San Diego, CA 92130
858.481.5000
Fax 858.481.1751
www.peregrine.com



Contents

Chapter 1	Introduction	15
Chapter 2	Setting up Accounts	17
	About accounts	17
	Demo accounts	19
	IT Employee accounts	19
	IT Manager accounts	19
	Administrator accounts.	20
	Scanner accounts	20
	Setting up Accounts	21
	Generating a list of accounts	21
	Adding an account.	21
	Customizing an account’s properties	23
	Customizing an account’s capabilities.	24
	Modifying an account password	26
	Deleting an account	27
	Setting the minimum password length	28

	Setting the number of failed login attempts.	29
	Setting the password history	29
	Maintaining Your Account	30
	Customizing your account	31
	Modifying your password	31
	Testing your e-mail address	32
Chapter 3	Adding, Removing, and Replacing Devices	35
	The importance of unique IP addresses	36
	Adding a device	36
	With a new IP address	36
	With the same IP Address as an active device	37
	With the same IP Address as a deactivated device	37
	Replacing a device.	38
	With an identical device	38
	With a different device	38
	Changing the IP address of a device	39
	Changing the cards or ports in a device.	39
	Removing devices	40
	Removing devices automatically	40
	Removing devices manually	42
	Activating devices	46

Chapter 4	Changing Device and Port Properties	49
	Changing Device Properties	49
	Changing Port Properties.	51
Chapter 5	Agent Communication Configuration	53
	Supported platforms for discovery agents.	54
	Agent security	54
	Agent Media files	55
	Agent Directories	56
	Initial Agent Deployment.	57
	Deployment via old listener	57
	Deployment via Win32 RPC.	58
	Custom Deployment	59
	Step-by-step automatic deployment instructions	60
	Deployment via login scripts	61
	Manual Deployment	61
	Upgrading the Agent	62
	Upgrading a Win32 Agent	62
	Upgrading a UNIX Agent	63
	Step-by-step agent upgrade instructions	63
	Uninstalling the agent	64
	Step-by-step agent uninstall instructions	64
	Uninstalling the old listener	65
	Step-by-step old listener uninstall instructions	65

	The software Utilization Agent Plug-in	66
	Agent Communication Configuration	67
	Agent Deployment Method	69
	Agent Deployment Command for Custom Deployment	69
	Agent Deployment Retry Interval.	70
	Agent Deployment Concurrent Sessions	70
	Agent Deployment Device Types.	70
	Agent Communication Concurrent Sessions	70
	Agent Communication Reserved Sessions	71
	Agent Versions	71
Chapter 6	Configuring your Scanner Settings	73
	Minimum scanner execution retry frequency	74
	Maximum scanner upgrade attempts.	74
	Initial time to wait between scanner upgrade attempts (in case of failure)	75
	Initial time to wait between retrieve scan files attempts (in case of failure)	75
	Maximum scanfile download attempts	75
	Scanner Versions.	76
	Scanner File Names	77
Chapter 7	Scanner Generator	79
	The Scan File Formats	80
	The Components of a Scanner	81

Information the Scanners Can Collect	82
Hardware and Configuration Information	82
Software Information.	83
User or Asset information.	84
Supported Platforms	84
Starting the Scanner Generator.	85
Exiting the Scanner Generator	85
The Scanner Generator User Interface.	86
Navigation Between the Pages	86
The Scanner Generator Pages.	86
The Scenario Page	89
The Standard Configuration Page	90
Enterprise Mode	90
Manual Deployment Mode	92
The Collection Page	95
Selecting the Type of Data to Be Collected	95
The Hardware Data Page	97
Disabling Specific Hardware Detection Routines.	98
The Software Data Page	102
Selecting a Preset Software Scanning Mode	102
Enabling the Command Line Override Option	104
The Drives Tab	105
Selecting a Predefined Type of Drive to Scan	106

The Drive Selection Tab	108
Creating a Customized Drive Selection	108
Overriding Scanner Generator Settings with Override Files	111
File Systems	111
Directories and Files	112
The Directories Tab	114
Selecting the Directories to Scan	115
The File Scanning Tab	117
Files to Scan Sub Tab.	117
File Identification Sub Tab	122
File Information to Store Sub Tab.	124
The Stored Files Tab	130
File Name to Store Column.	131
Found Where Column	133
The Plug-ins Tab.	134
Plug-ins Provided As Part of the Scanner Generator	135
Enabling or Disabling a Plug-In	136
Setting Advanced Options for a Plug-In.	136
Setting the Properties for a Plug-In	137
Removing an Existing Plug-In.	138
Creating Customized Plug-Ins	138
The Asset Data Page	138

The User Entry Tab	139
Asset Questionnaire Definition	139
The User Entry Form Layout	140
The Asset Field Configuration Dialog Box	142
Setting Up a New Asset Field	142
The Refilling Tab	177
How Refilling Works	177
Specifying a Refill Order	179
Specifying Options for Refilling	180
Setting up the Refilling Options to Handle Delta Scan Files Correctly (Manual Deployment mode only)	180
Locating an Offsite Scan File for Refilling	181
The Asset Number Tab	182
Asset Number Definition	182
The Source for the Asset Number	183
Asset Number Batch File Definition	184
Creating an Asset Number Batch File	184
The Scanner Options Page	185
The Saving Tab.	186
Setting the Default Scan File Format	186
Saving Local and Offsite Scan Files	187
Saving Results Locally	187
Enabling Delta Scanning	188

Setting up the Scanner to Handle Delta Scan Files Correctly (Manual Deployment Mode only)	189
Saving Results to Network (Offsite)	189
The User Interaction Tab	194
Setting User Interaction Options for the Scanner	194
Setting Time-Out Options	195
The GUI Options Tab.	197
Setting Scanner GUI Options	197
Setting the Default View When the Scanner Is Run	199
Setting the Mode in Which the Scanner Is Run	200
The Errors Tab	201
Setting Up a Customized Error Message for the Scanner.	201
Setting Up the Creation of a Log File	201
The DOS Options Tab	203
Setting Up the Behavior of the DOS Scanner	203
Setting Up the Behavior When Too Few File Handles Are Available in DOS.	204
The Miscellaneous Tab.	205
The Scanners to Generate Page.	207
The Output Options Tab	209
Setting Up a Scanner Description.	209
Saving Scanner Options to a Text File.	210
Naming the Configuration (.cxz) File	211

	The Scanners Tab	212
	Selecting which Scanners to Generate	212
	Specifying the Base Scanner File Name and Output Directory	213
	Setting Naming Conventions for the Scanners.	214
	The Generating Scanners Page	216
	How Drive Letters and Volumes Are Assigned	217
	Enumerating Physical Hard Disks and Partitions	217
	Processing Drives	218
	Scanning Specific Directories	219
Chapter 8	XML Enricher	221
	The XML Enricher Directory Structure	223
	Processing Normal Scan Files	226
	Processing Delta Scan Files	226
	Delta Calculation Command Line Utility.	227
	Application Utilization Data	229
	Log Files.	229
	Application Recognition in XML Enricher	230
	Configuring the XML Enricher using the Web UI.	232
	Process utilization data	233
	Application Recognition	233
	Generate MIF Files	233
	Automatically Defer All New Scans	234
	Merge Priority	234

	AutoSequence Number	234
	Managing Scan Files	236
	Updating the application library used by the Enricher	237
	Configuring the XML Enricher Using XML Enricher.ini	238
	The XML Enricher ini File Sections	238
	RecognitionConfig Section	238
	RecognitionConfig.RecognitionConfig_cfgJunk Filters Section	240
	RecognitionConfig.RecognitionConfig_cfgSAIFiles Section	241
	AssetFieldConfig Section	242
	Starting and stopping the XML Enricher service in the web UI	243
	Structure of the Enriched XSF File	244
	An Example of How the data is stored	245
Chapter 9	Getting Your Data into AssetCenter	249
	Assumptions	250
	Where to find the Connect-It scenario	250
	Prerequisites	251
	Compatibility	251
	Prepare AssetCenter	252
	Prepare Connect-It.	252
	Step1: Open the scenario.	252
	Step 2: Configure the Source Connector - Enterprise Discovery	253
	Step 3: Configure the Destination Connector - AssetCenter	256
	Check your mappings	259

Check the reconciliation keys	260
Mandatory fields in an Asset Management database.	261
Test your Enterprise Discovery-AssetCenter Scenario	261
Starting the scenario test	262
Get the data into AssetCenter	262
Starting the scheduler	262
Stopping the scenario	263
Analyze what happened during the process.	263
See the results in AssetCenter	263
Customize your scenario	264
Index	265



1 Introduction

CHAPTER

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 ServiceCenter and AssetCenter



2 Setting up Accounts

CHAPTER

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

About accounts

There are five types of account:

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

By default, Enterprise Discovery has one of each type of account installed (except for Scanner). If there are to be any other accounts, the owner of an Administrator account must create them.

Warning: 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.

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

	Demo	IT Employee	IT Manager	Administrator
Managers (for example, Device Manager)				
View read and write community strings for device	—	—	✓	✓
SNMP query default string	“public”	“public”	from Enterprise Discovery	from Enterprise Discovery
Update Model	—	—	✓	✓
Agent and Scan logs	—	—	✓	✓
Status				
View read and write community strings for network	—	—	✓	✓
Administration				
Change own password	—	✓	✓	✓
Configure own account	—	✓	✓	✓
Configure other accounts	—	—	—	✓
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 reports and server status

IT Employee accounts

An IT Employee account can:

- Do everything a Demo account can do
- 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.

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
- 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

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*).

Warning: 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.

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:

- 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
admin	Administrator	Administrator	n/a
demo	Demo	Demo Account	n/a
itemployee	IT Employee	IT Employee	n/a
itmanager	IT Manager	IT Manager	n/a

Adding an account

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

Warning: 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**.

Note: 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:

Property	Explanation
Name	The name of the account owner.
E-mail address	The e-mail address of the account owner.
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.
Long date format	Determines how the date appears at the bottom of most panels and pages.
Short date format	Determines how the date appears at the bottom of the Statistics panel's Table view and in Reports, Event Browser and Health Panel.
Inline help format	Determines if you automatically see short or full help files in HTML menus. If you choose the short help option, you will see a link called "Full Help". Clicking that link opens an Assistant window that displays the Full Help.
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.

To select an account for customizing:

- 1 Click **Administration > Account administration > Account properties**.
- 2 Select an account from the list box.
- 3 Click **Modify Properties**.

To modify an account:

- 1 (optional) Enter a descriptive name in the Name field.
- 2 Assign the appropriate properties.
- 3 Click **Modify Properties**.

Name:	<input type="text" value="Demo Account"/>
E-mail address:	<input type="text"/>
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
<hr/>	
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
<hr/>	
Inline help format:	<input type="text" value="All"/> <input type="button" value="v"/>
<hr/>	
Default Device Manager panel:	<input type="text" value="Configuration"/> <input type="button" value="v"/>
Default Port Manager panel:	<input type="text" value="Configuration"/> <input type="button" value="v"/>
Device Manager ports panel increment:	<input type="text" value="24"/>
<hr/>	
<input type="button" value="Modify Properties"/>	

Customizing an account's capabilities

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

Account type	Determines the account's level of access to Enterprise Discovery.
Web Access	Allows owner to use Enterprise Discovery. You will probably enable this, but conceivably the user only needs MySQL ODBC access
MySQL ODBC Access	Allows owner of the account to export Enterprise Discovery data to third-party data access applications to create custom reports.
Password expiry	The number of days an account can be used before the password expires.

To select an account for customizing:

- 1 Click **Administration > Account administration > Account capabilities**.
- 2 Select an account from the list box.
- 3 Click **Modify Capabilities**.

To modify an account:

- 1 Select an account type from the list box.

Note: You cannot change the account type for the account you are currently using.

- 2 Determine what capabilities the account will have.

Note: You cannot change any capabilities for the account you are currently using.

- 3 Change the appropriate capabilities.
- 4 Click **Modify Capabilities**.

Account type: 

Account capabilities: Web and applets access: Yes No

MySQL ODBC access: Yes No

Password expiry: Days:

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:

- Click **Administration > 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**.

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

Note: 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.

Note: 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:

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.

Setting the minimum password length

Your company may have a standard password length for all accounts in the organization. That standard may be different than the default password length in Enterprise Discovery (which is 4-10 characters).

If your company requires you to have a different minimum password length, you can change Enterprise Discovery so it is compliant with your standards.

To change the minimum password length:

- 1 Click **Administration > System Preferences > Server passwords**.
- 2 Enter a new number in the Custom text box.
- 3 Click **Change**.

<u>Minimum password length:</u>	<input checked="" type="radio"/> Default:	4
	<input type="radio"/> Custom:	<input type="text" value="4"/>

Setting the number of failed login attempts

As a security feature, the Administrator can define how many times an account can try to login to Enterprise Discovery.

If the user cannot login, and this threshold has been passed, the account will be locked out until the Administrator changes the account password (see [Modifying an account password on page 26](#)).

To change the maximum number of failed login attempts:

- 1 Click **Administration > System Preferences > Server passwords**.
- 2 Enter a new number in the Custom text box.
- 3 Click **Change**.

<u>Maximum number failed login attempts:</u>	<input checked="" type="radio"/> Default:	0
	<input type="radio"/> Custom:	<input type="text" value="0"/>

Setting the password history

For security purposes, users should change their passwords often. To increase security, this feature ensures that users use different passwords, rather than re-using the same passwords over and over again. For example, if you set this to "5," a user must use a new, unique password the next 5 times he/she changes his/her password.

The **Delete password history** feature determines how long Enterprise Discovery keeps a record of the passwords used by each account. When this time expires, an user will be able to re-use an old password.

Note: Delete password history always takes precedence. If you surpass the set Password History limit, you cannot reuse a password until the Delete password history time has expired.

To set the password history:

- 1 Click **Administration > System Preferences > Server passwords**.

- 2 Enter a new number in the Custom text box.
- 3 Click **Change**.

<u>Password history:</u>	<input checked="" type="radio"/> Default:	0
	<input type="radio"/> Custom:	<input type="text" value="0"/>

To delete the password history:

- 1 Click **Administration > System Preferences > Server passwords**.
- 2 Set a time for the password history to be deleted.
- 3 Click **Change**.

<u>Delete password history:</u>	<input checked="" type="radio"/> Default:	1 day 0 hours		
	<input type="radio"/> Custom:	Weeks: <input type="text" value="0"/>	Days: <input type="text" value="1"/>	Hours: <input type="text" value="0"/>

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.

Customizing your account

The Enterprise Discovery Administrator (with an Administrator account) sets up your account and determines what levels of access and capabilities you will have, but you (as the user of an IT Employee, IT Manager or Administrator account) can customize your own preferences.

Note: Many of these properties will be of more interest to you when you are more experienced with Enterprise Discovery.

To customize the properties of your account:

- 1 Click **Administration > My account administration > Account properties**.

A screen appears called “Account Properties for [account name]”.

Note: If no password is given, the account cannot be used to log in, even when Web Access is set to “yes”.

- 2 Choose the properties you want.
- 3 Click **Modify Properties**.

Modifying your password

The Enterprise Discovery Administrator may change the passwords occasionally, but this option gives you control over your own password. If you have trouble accessing your account, ask the Enterprise Discovery Administrator to make sure you have the correct password.

Note: Passwords are case-sensitive. “Magic”, “MAGIC”, and “magic” are different passwords

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 change your account password:

- 1 Click **Administration > My account administration > Account password**.
- 2 Enter the new password in the Password field.
- 3 Enter the new password in the Password (again) field.
- 4 Click **Modify Password**.

Note: When you change your password, you will be prompted to log in again using the new password.

Note: 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.

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



3 Adding, Removing, and Replacing Devices

CHAPTER

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 36
- Adding a device on page 36
- Replacing a device on page 38
- Changing the IP address of a device on page 39
- Changing the cards or ports in a device on page 39
- Removing devices on page 40
- Activating devices on page 46

The importance of unique IP addresses

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

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.

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.

Note: 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.

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 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.

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.

Note: 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.

Note: If you change the IP of the device, but the MAC remains the same, the Enterprise Discovery database updates automatically.

Note: If you change the IP of a port, Enterprise Discovery automatically discovers the change. No additional action is required.

Note: 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.

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

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

Action	Hide	Deactivate	Purge	Obliterate ^a
device can be recovered if seen	—	✓	✓ ^b	— ^b
“delete” event generated	✓	✓	✓	—
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.

Note: 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.

Note: 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		
<u>Managed devices deactivation interval:</u>	<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"/>
<u>Unmanaged devices deactivation interval:</u>	<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"/>
<u>Scanner-only devices deactivation interval:</u>	<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		
<u>Managed devices purge interval:</u>	<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"/>
<u>Unmanaged devices purge interval:</u>	<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"/>
<u>Scanner-only devices purge interval:</u>	<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		
<u>Device obliteration interval:</u>	<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 Preferences > 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 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**)

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

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

Note: If a device has not been seen for the period set (in **Administration > System preferences > Expiry** —see [Changing the device expiry intervals on page 41](#)), Enterprise Discovery automatically takes appropriate action.

Note: 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 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 46](#).

Hiding Devices

This command removes the device from all reports, though a complete record of the device and its history is kept. The only way to bring the device back 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.

Important: Hidden devices still count towards your device license limit.

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 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 in Enterprise Discovery reports is to use the Hide command.

Warning: The Purge command cannot be undone.

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. If the device is rediscovered by Enterprise Discovery, it will be reactivated. Otherwise, you can use the Activate command to manually bring this device back. 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 Device Manager:

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

Activating devices

This command will bring a device from the list of hidden or deactivated devices, and Enterprise Discovery will start monitoring this device again.

Note: 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 40](#).

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 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**.

Enterprise Discovery will begin to monitor this device again.



4 Changing Device and Port Properties

CHAPTER

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.

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

Warning: Changing a device icon affects what reports the device appears in.

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**.

Note: 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

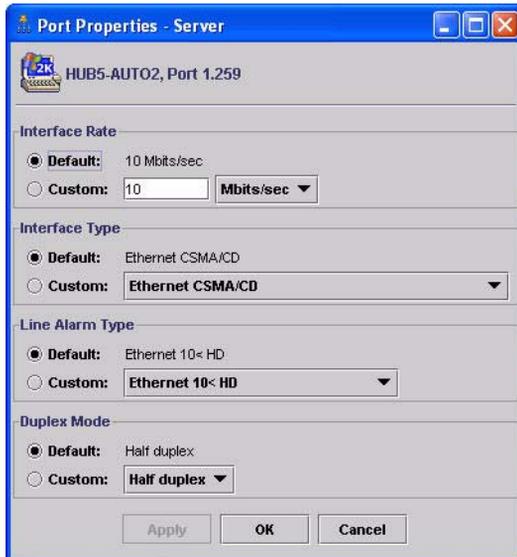
To change these Port Properties:

- 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**.



5 Agent Communication Configuration

CHAPTER

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 listens and performs requests for the Enterprise Discovery Server. For example, it can download a Scanner, 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.

Once installed, the agent is capable of communication with the server. The communication 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 no SP/SP1/SP2
- Windows 2003 Server no SP/SP1

UNIX:

- SUN SunOS 2.5.1 and later, SUN Solaris 8/9 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

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.

Important: 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.

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\Peregrine\Enterprise Discovery\2.0.0\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:

```
peregrine-discovery-agent-aix-2.0.0.2894.tar.Z
peregrine-discovery-agent-hpux-2.0.0.2894.tar.Z
peregrine-discovery-agent-linux-2.0.0.2894.tar.Z
peregrine-discovery-agent-sunos-2.0.0.2894.tar.Z
peregrine-discovery-agent-win32-2.0.0.2894.exe
peregrine-discovery-agent-winnt-2.0.0.2894.exe
Peregrine Discovery Agent 2.0.0.2894.msi
```

- A **.tar.Z** file for each UNIX platform supported by the agent
- An MSI setup file for Win32
- Two versions of executable (.exe) installers for Win32.

The difference between the two versions is the size.

peregrine-discovery-agent-win32-2.0.0.xxxx.exe has an MSI engine for both Windows 9x and Windows NT/200x/XP (about 3.7MB in size).

peregrine-discovery-agent-winnt-2.0.0.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.

Important: 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 Peregrine\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 should be put 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 `prgnagentinstaller.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 methods needs to know the administrator account name and password for the remote computer. This is usually a domain administrator account. As multiple domains can be in use, multiple account names/passwords can be entered. The order in which the accounts are tried is as follows:

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

The deployment code tries to connect to the remote computer's **ADMIN\$** share using the administrator account names and passwords provided in the order described above. Once connection is established, it copies the agent installation to the remote computer and launches the installation. The 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 prnagentinstaller.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 Preferences>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: "2.0.0.2886"). The agent media files need to be taken from the LiveAgents directory.
- Version of the AIX agent media
- Version of the HPUX agent media
- Version of the Linux agent media
- Version of the Solaris 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 Preferences>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.

Note: 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\Peregrine Discovery Agent 2.0.0.2886.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, peregrine-discovery-agent-win32-2.0.0.2886.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.

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 `prgnagentinstaller.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.

Note: 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 **prnagentinstaller.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.

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

Which should help in finding the reason of the failure.

The software Utilization Agent Plug-in

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 preferences > 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**

Note: 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 preferences > 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.

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 Preferences > Agent Communication**.
- 2 Change the settings as necessary.
 - [Agent Deployment Method on page 69](#)
 - [Agent Deployment Command for Custom Deployment on page 69](#)
 - [Agent Deployment Retry Interval on page 70](#)
 - [Agent Deployment Concurrent Sessions on page 70](#)
 - [Agent Deployment Device Types on page 70](#)
 - [Agent Communication Concurrent Sessions on page 70](#)
 - [Agent Communication Reserved Sessions on page 71](#)
 - [Agent Versions on page 71](#)
- 3 Click **Change**.

<u>Agent deployment method:</u>	<input type="radio"/> Default:	Using Listener Windows RPC											
	<input checked="" 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>Using Listener Custom</td> <td>Add>></td> <td>Windows RPC</td> <td>Move Up</td> </tr> <tr> <td></td> <td><<Remove</td> <td></td> <td>Move Down</td> </tr> </tbody> </table>	Choose From	Action	Selected	Order	Using Listener Custom	Add>>	Windows RPC	Move Up		<<Remove	
Choose From	Action	Selected	Order										
Using Listener Custom	Add>>	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 type="radio"/> Default:	2 days 0 hours 0 minutes											
	<input checked="" type="radio"/> Custom:	Days: <input type="text" value="1"/> Hours: <input type="text" value="0"/> Minutes: <input type="text" value="0"/>											
<u>Agent deployment concurrent sessions:</u>	<input checked="" type="radio"/> Default:	25											
	<input type="radio"/> Custom:	<input type="text" value="25"/>											
<u>Agent deployment device types:</u>	<input checked="" type="radio"/> Default:	<ul style="list-style-type: none"> <input type="checkbox"/> Workstation <input type="checkbox"/> Server <input type="checkbox"/> Storage Server <input type="checkbox"/> Microsoft Server <input type="checkbox"/> Web Server <input type="checkbox"/> Microsoft Workstation <input type="checkbox"/> Laptop <input type="checkbox"/> Network Computer <input type="checkbox"/> Win98 Workstation <input type="checkbox"/> WinME Workstation <input type="checkbox"/> WinNT Workstation 											
	<input type="radio"/> Custom:	<ul style="list-style-type: none"> <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 											
<u>Agent communication concurrent sessions:</u>	<input checked="" type="radio"/> Default:	80											
	<input type="radio"/> Custom:	<input type="text" value="80"/>											
<u>Agent communication reserved sessions:</u>	<input checked="" type="radio"/> Default:	4											
	<input type="radio"/> Custom:	<input type="text" value="4"/>											
<u>Usage 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)											

Agent Deployment Method

This option determines how you want to deploy Agents to your network devices. You can use any of the following options:

- the old Peregrine Desktop Inventory (PDI) Listener (for customers upgrading PDI and PND running in Aware Mode or from Enterprise Discovery 1.0).
- Windows RPC (works for computers running Windows NT/XP/200x Operating Systems)
- a custom-designed method provided by the user

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.

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.

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 Enterprise Discovery's internal device number)
- Version of the agent Win32 media to be installed (for example: "2.0.0.2518"). The agent media files need to be taken from the **LiveAgents** directory, located under the 'Enterprise Discovery data directory':
C:\Documents and Settings\All Users\Application Data\Peregrine\Enterprise Discovery\
- 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

- 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. Any other code indicates failure, and Enterprise Discovery will try again based on the Agent Deployment Retry Interval.

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. This option only takes effect for those devices that have an SNMP agent enabled.

Note: If a device has not yet been scanned, the device type is likely to be general. For example, attempting to use this feature to deploy only to XP Workstations is likely to fail because the device type is likely "unknown" or a generic "workstation." This feature should primarily be used to avoid deploying Agents to printers, switches, routers, etc.

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. Enterprise Discovery may need these reserved sessions in cases where the administrator wants to schedule this manually.

The Reserved Sessions count towards your Concurrent Sessions count. For example, if the Concurrent Session count is 80, and the Reserved count is 4, the server will use 76 sessions at a time, leaving 4 sessions available for other purposes.

Note: Reserved sessions cannot exceed 5% of the total concurrent sessions.

Agent Versions

Also on this screen, you can manually change the version of the Agent you want to use for running different Operating Systems.

Agent Versions		
Win32 agent version:	<input checked="" type="radio"/> Default:	<latest>
	<input type="radio"/> Custom:	<latest> ▼
HP/UX agent version:	<input checked="" type="radio"/> Default:	<latest>
	<input type="radio"/> Custom:	<latest> ▼
Linux agent version:	<input checked="" type="radio"/> Default:	<latest>
	<input type="radio"/> Custom:	<latest> ▼
AIX agent version:	<input checked="" type="radio"/> Default:	<latest>
	<input type="radio"/> Custom:	<latest> ▼
Solaris agent version:	<input checked="" type="radio"/> Default:	<latest>
	<input type="radio"/> Custom:	<latest> ▼

To change your Agent versions:

- 1 Click **Administration > System Preferences > Agent Communication**.
- 2 Change the Agent versions as necessary.
- 3 Click **Change**.

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.



6 Configuring your Scanner Settings

CHAPTER

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 Preferences** > **Scanner Deployment**.
- 2 Change the settings as necessary.
 - Minimum scanner execution retry frequency on page 74
 - Maximum scanner upgrade attempts on page 74
 - Initial time to wait between scanner upgrade attempts (in case of failure) on page 75
 - Initial time to wait between retrieve scan files attempts (in case of failure) on page 75
 - Maximum scanfile download attempts on page 75
 - Scanner Versions on page 76
 - Scanner File Names on page 77
- 3 Click **Change**.

<u>Minimum scanner execution retry frequency:</u>	<input checked="" type="radio"/> Default:	5 hours 30 minutes
	<input type="radio"/> Custom:	Days: <input type="text" value="0"/> Hours: <input type="text" value="5"/> Minutes: <input type="text" value="30"/>
<u>Maximum scanner upgrade attempts:</u>	<input checked="" type="radio"/> Default:	5
	<input type="radio"/> Custom:	<input type="text" value="5"/>
<u>Initial time to wait between scanner upgrade attempts (in case of failure):</u>	<input checked="" type="radio"/> Default:	5 minutes
	<input type="radio"/> Custom:	Days: <input type="text" value="0"/> Hours: <input type="text" value="0"/> Minutes: <input type="text" value="5"/>
<u>Initial time to wait between retrieve scan files attempts (in case of failure):</u>	<input checked="" type="radio"/> Default:	1 minute 0 seconds
	<input type="radio"/> Custom:	Hours: <input type="text" value="0"/> Minutes: <input type="text" value="1"/> Seconds: <input type="text" value="0"/>
<u>Maximum scanfile download attempts:</u>	<input checked="" type="radio"/> Default:	5
	<input type="radio"/> Custom:	<input type="text" value="5"/>

Minimum scanner execution retry frequency

The minimum amount of time Enterprise Discovery will wait to attempt scanner execution.

Note: 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		
Win32 scanner version:	<input checked="" type="radio"/> Default:	<latest>
	<input type="radio"/> Custom:	<latest> 
HP/UX scanner version:	<input checked="" type="radio"/> Default:	<latest>
	<input type="radio"/> Custom:	<latest> 
Linux scanner version:	<input checked="" type="radio"/> Default:	<latest>
	<input type="radio"/> Custom:	<latest> 
AIX scanner version:	<input checked="" type="radio"/> Default:	<latest>
	<input type="radio"/> Custom:	<latest> 
Solaris scanner version:	<input checked="" type="radio"/> Default:	<latest>
	<input type="radio"/> Custom:	<latest> 

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

Note: 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.

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

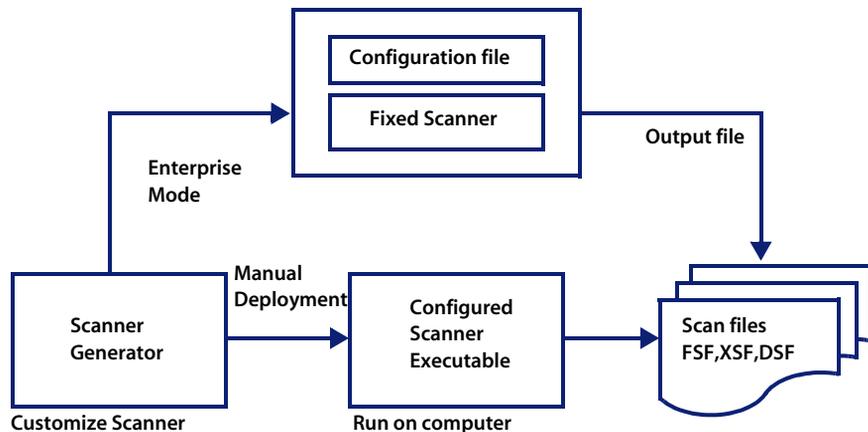
7 Scanner Generator

CHAPTER

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 three formats:

- Fingerprint Save File (FSF) - with the file extension .fsf
- Compressed XML (XSF) - with the file extension .xfs
- Delta Scan File (DSF) - with the extension .dsf

Note: 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.

FSF Scan File

The FingerPrint Save File (.fsf) is a proprietary format created by Enterprise Discovery.

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 221](#).

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
- bitmaps
- database files
- the Scanner executable code
- plug-ins

- **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 two files listed previously.

Scanner Support

FSF files can be created by any Scanner, while XSF files can only be created by the Win32 and UNIX/Linux Scanners. Although the Remote Scanner is a Win32 program, it does not support XSF files. DSF files can be created by all Scanners except the DOS Scanner.

Scan File Compression

All Scanners (except the DOS Scanner) compress the scan file on saving. Even though scan files are compressed, the asset entry information can still be edited in the analysis tools (Viewer and Analysis Workbench).

Information the Scanners Can Collect

The three types of information collected are:

- Hardware and Configuration Information
- Software Information
- User or Asset information

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, which during an initial inventory may have to be entered manually, includes any information which may or may not be available electronically (such as office location, floor). 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. As part of the detailed asset information configuration, an asset questionnaire is defined. This is presented to the user as a list of entry fields which can be filled in and the content recorded in the scan file. Asset data fields can also be automatically populated, and the data extracted from, for example, text files, the Windows registry and environment variables.

Supported Platforms

Scanner Generator runs on the following platforms:

- Windows 95
- Windows 98
- Windows NT 4.0
- Windows ME
- Windows 2000
- Windows XP
- Windows 2003 Server
- Windows Media Server

Scanners can be generated for the following operating systems:

Scanner	Runs on...
DOS Scanner	DOS 3.3 or later
Windows 16-bit Scanner	Windows 3.1x

Scanner	Runs on...
Windows 32-bit Scanner	<ul style="list-style-type: none"> ■ Windows 95
No-UI 32-bit Scanner	<ul style="list-style-type: none"> ■ Windows 98 (includes Windows 98 SE)
Remote Scanner	<ul style="list-style-type: none"> ■ Windows NT 4.0 (includes Windows NT Server) ■ Windows ME ■ Windows 2000 (includes Windows 2000 Server) ■ Windows XP ■ Windows 2003 ■ Windows 2003 Server ■ Windows Media Server
OS/2 Scanner	OS/2 2.1 or later and OS/2 Warp
UNIX Solaris Scanner	Solaris 2.5, 2.6, 7, 8 and 9 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

Starting the Scanner Generator

To start Scanner Generator:

- From the Windows Start menu select **Programs|Peregrine|Enterprise Discovery 2.0.0|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 86](#)
- [The Scanner Generator Pages on page 86](#)

Navigation Between the Pages

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

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.

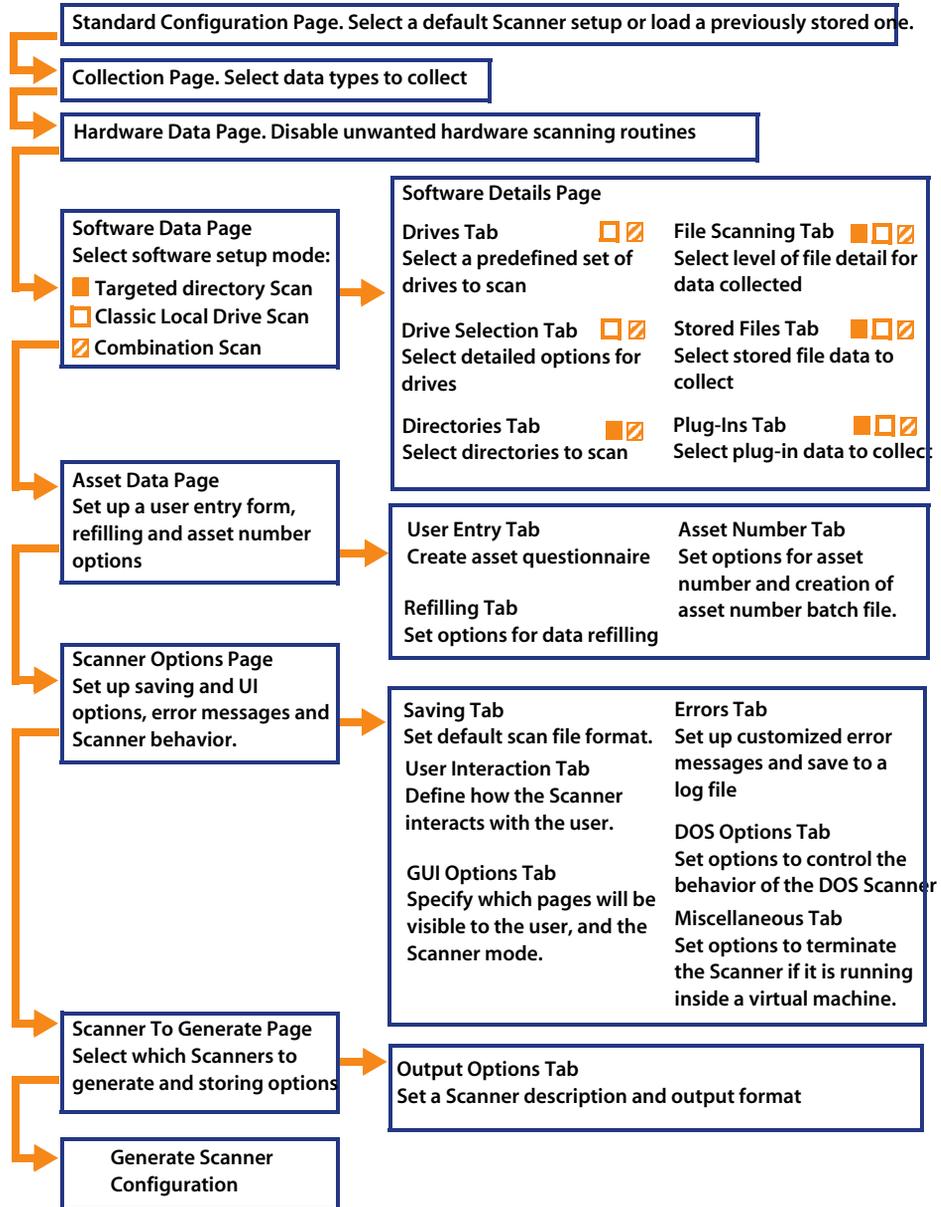
The Scanner Generator Pages

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.

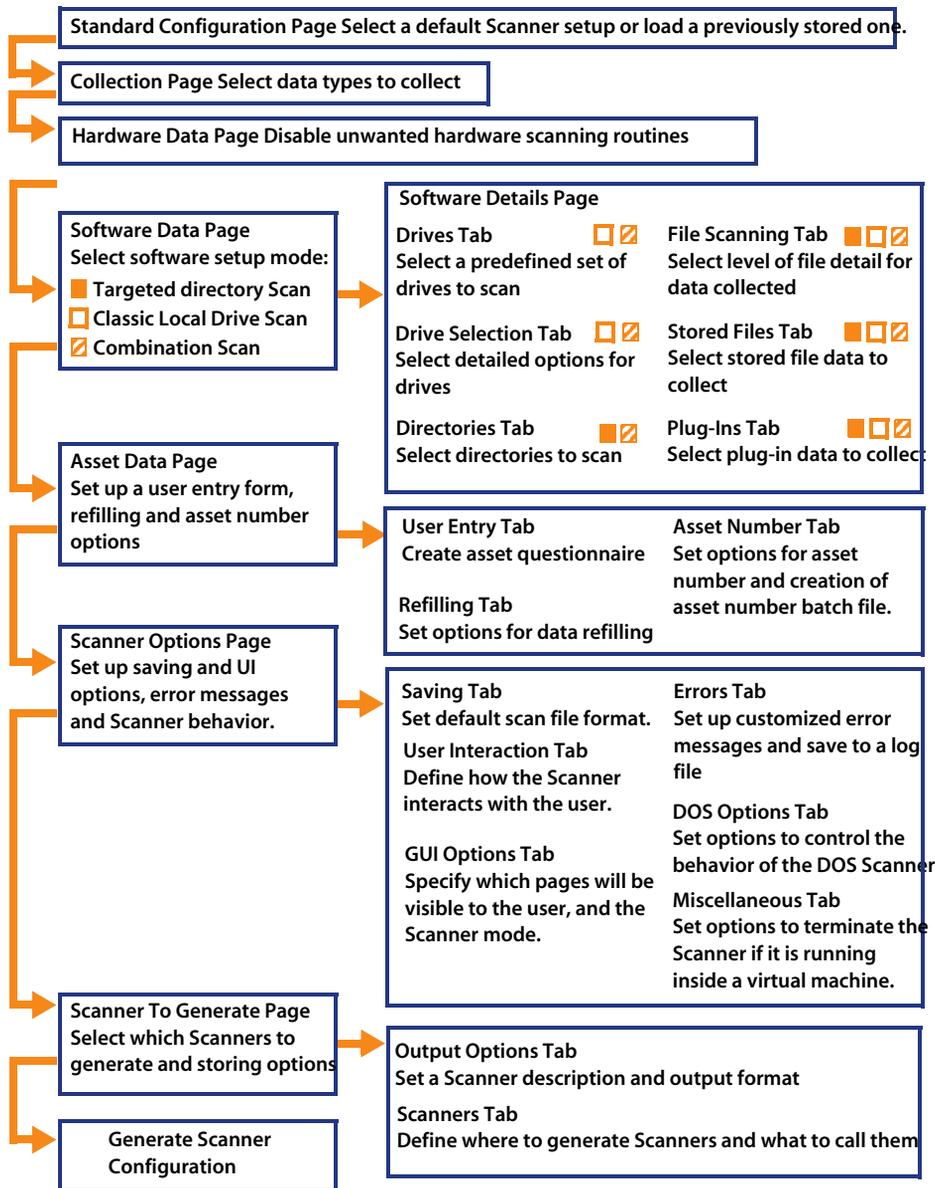
There are two scenarios in which the Scanners can be used. This is determined on the first page of the Scanner Generator. Depending on which of these scenarios you select, different tab pages are displayed.

- [Enterprise Mode](#)
- [Manual Deployment Mode](#)

Enterprise Mode

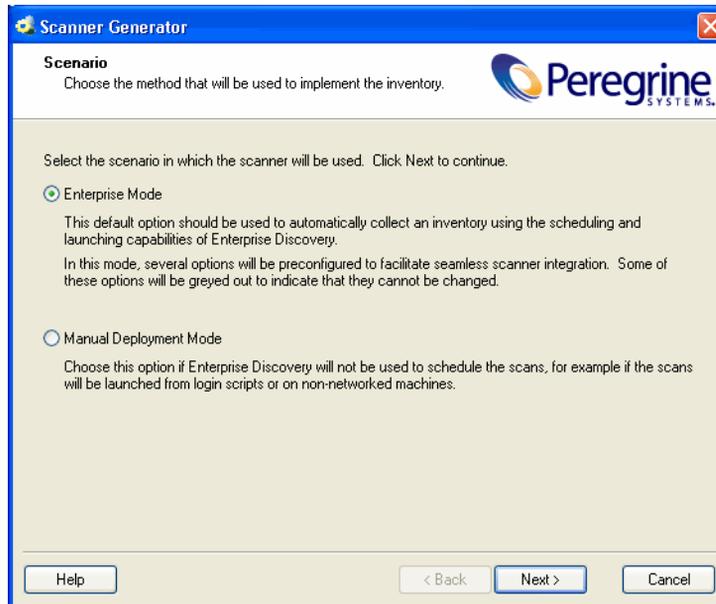


Manual Deployment Mode



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 on the Enterprise Discovery Server 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**

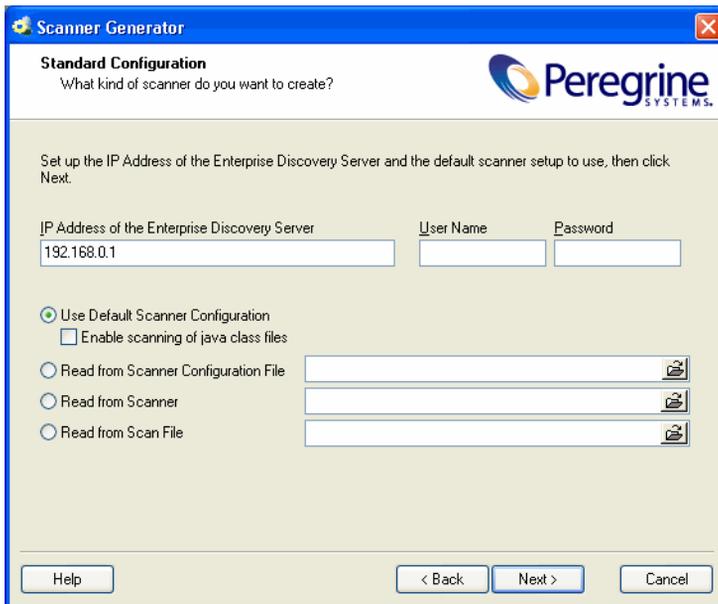
This option should be chosen if the Enterprise Discovery Server will not be used to schedule and launch scans. For example, if the scans will be launched from login scripts or on non-networked machines.

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 dialog box titled "Scanner Generator" with a "Standard Configuration" section. The question "What kind of scanner do you want to create?" is displayed. Below this, instructions state: "Set up the IP Address of the Enterprise Discovery Server and the default scanner setup to use, then click Next." There are three input fields: "IP Address of the Enterprise Discovery Server" (containing "192.168.0.1"), "User Name", and "Password". Below these are radio button options: "Use Default Scanner Configuration" (selected), "Read from Scanner Configuration File", "Read from Scanner", and "Read from Scan File". A checkbox "Enable scanning of java class files" is also present. At the bottom are buttons for "Help", "< Back", "Next >", and "Cancel". The Peregrine Systems logo is in the top right corner.

- 1 Enter the IP address 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 must have an administrator account.

- **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.
 - Win32 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). This file contains the configuration settings only from a previous Scanner. Typically this file is 3 kb in size.

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. For example, if a previous Scanner contains lists of departments, machines make use of this data by taking the configuration options from the old

Scanner and using them in the new one. 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.

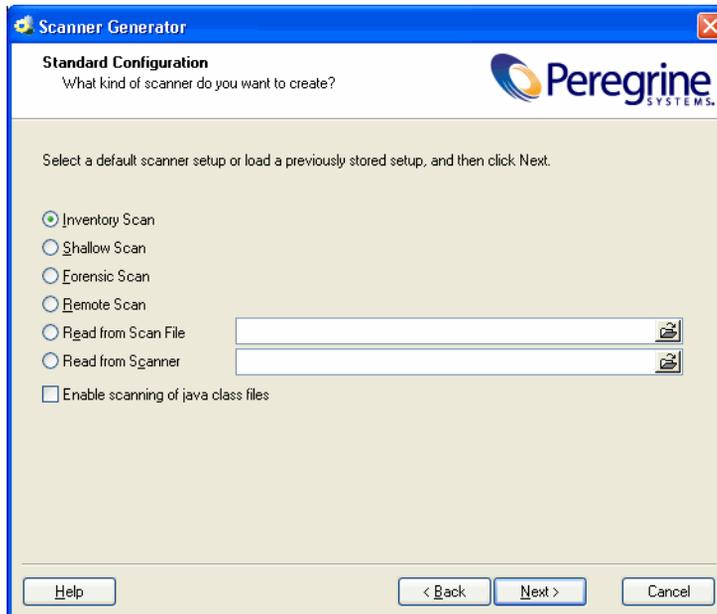
- **Read from Scan File**

Reads the settings from an existing scan file (.fsf or .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 asset questionnaire is 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 licence 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.
- **Remote Scan**

Selects the predefined options for the Remote Scanner. The Remote Scanner is used to perform a software scan of a remote computer. Refer to The Remote Scanner in the Scanners chapter of the *Reference Guide*.
- **Read from Scan file**

Reads the settings from an existing scan file (.fsf or .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. For example, if a previous Scanner contains lists of departments, machines make use of this data by taking the configuration options from the old

Scanner and using them in the new one. 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.

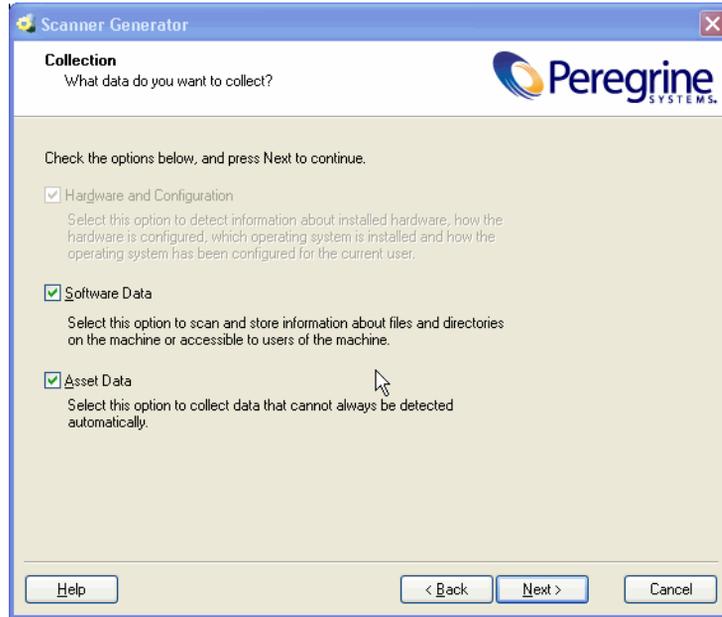
- **Enable scanning of Java class files**

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.
 - Win32 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.



Tip: 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 97](#).

Note: For inventories configured to use the Enterprise Discovery Server, this option is always selected and cannot be disabled as shown in the previous screen shot.

- **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 102](#).

- **Asset Data**

During an initial inventory this may have to be entered manually. It includes any information which may or may not be available electronically (such as office location, floor). 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.

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

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

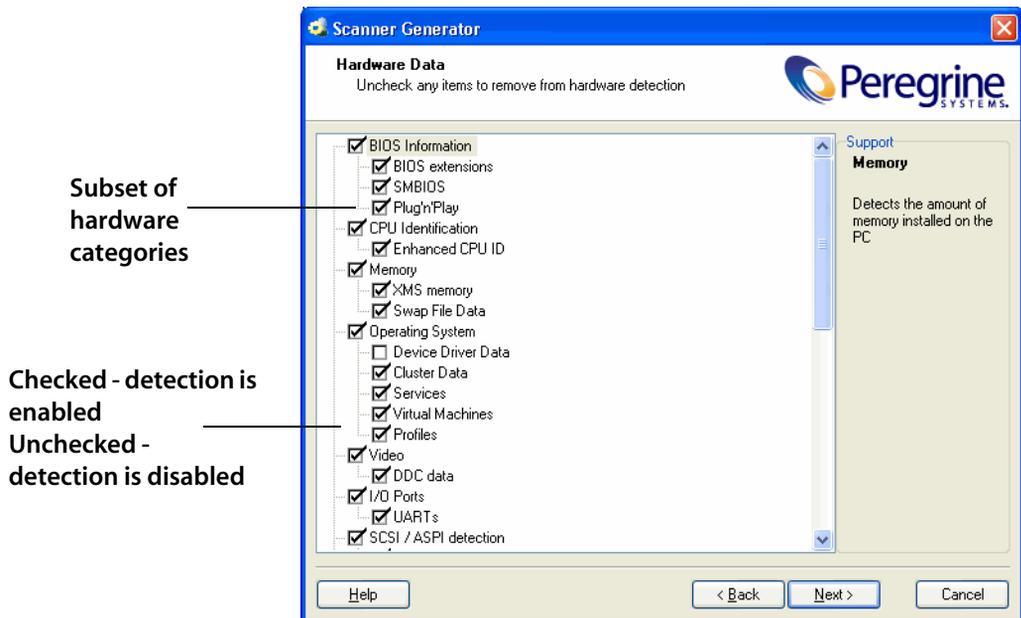
The Hardware Data Page

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:

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).

Important: By default most of the categories are shown selected. This indicates that the hardware detection routine for that particular category is enabled.

The only two hardware options which are unchecked by default are:

- DMI 1.x version**
 This is because most early implementations of DMI 1.x are unstable. Enabling this setting when scanning a population of machines is not recommended.
- 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

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.
Compaq Asset Tag	Determines asset tags on Compaq computers that support Intelligent Manageability.
Plug'n'Play	Provides details of whether the BIOS installed on the computer is Plug and Play compatible. If the BIOS supports Plug and Play specification, the version of the specification is collected.
CPU Identification	Identifies the CPU (model), establishes if it has got FPU (numeric coprocessor), MMX (MultiMedia eXtensions) and ISSE/SSIMD capability and reports the speed of the CPU, cache characteristics. For newer Intel and compatible processors, the manufacturer, model, family and stepping ID are reported.
Enhanced CPU ID	This applies to DOS Scanners only. Attempts to correctly identify 32-bit processors (386s, 486s and Pentiums) using a method not compatible with Windows. If unchecked, some CPUs will not identify correctly.
Memory	Detects the total amount of memory installed on the computer, including the amount of conventional and extended memory. The amounts of memory available with the XMS, EMM and DPMI specifications are also collected together with the version of the driver and the specification, where possible. XMS, EMM and DPMI are applicable to DOS and Win16 Scanners only.
XMS Memory	Determines the amount of XMS memory. Applicable to DOS and Win16 Scanners only.
Swap File data	Collects data about swap files used for virtual memory.
Operating System	Collects information about the operating system and its configuration. Information about DOS or the DOS subsystem is also provided where applicable.
Device Driver Data	When this option is enabled, the Windows 32-bit 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.

Options	Description
Virtual Machines	<p>Detects whether the Scanner is running in VMWare, Virtual PC or Terminal Services.</p> <p>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).</p>
Profiles	Collects data about user profiles.
Video	<p>Records details of the Video Display Adapter, which include the adapter type (EGA, XGA, VGA and so on) and model/manufacturer, where possible.</p> <p>In Windows and OS/2, the current desktop resolution and number of colors are also picked up.</p>
DCC 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.
UARTs	Detects the UARTs associated with each serial port.
SCSI/ASPI Detection	Checks for the presence of an ASPI (Advanced SCSI Programming Interface) driver for a SCSI adapter. If the driver is available, the host SCSI adapter name is reported.
SCSI/IDE/ATAPI devices	Detects installed devices, such as hard drives, CD-ROMs, tape drives and other such devices. Also detects Serial ATA disks.
SCSI/IDE/ATAPI serial numbers	Detects serial numbers of the installed devices (where available). Also detects the serial number of Serial ATA disks.
Network Information	<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.

Options	Description
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).
Detect mouse without the driver	Attempts to detect information about the mouse if a driver is not loaded. Applicable only to Win16 Scanners when no DOS mouse driver is installed.
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.
Partition Table Scan	Identifies location of hard drive partitions on physical hard disk(s) and matches them with logical drive letters.
Bus Detection	Detects the architecture of the bus used in the PC – ISA, EISA, PCI, MCA or PCMCIA.
EISA	Detects and reports details of EISA cards.
MCA	Detects and reports details of MCA cards.
PCI	Detects and reports details of PCI cards.
PCMCIA	Detects and reports details of PCMCIA cards.
ISA PnP Cards	Detects and reports details of ISA Plug and Play cards.
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.
DMI Information	Collects information about the Desktop Management Interface.
DMI 1.x Version	Detects the version of the Desktop Management Interface and the description of the DMI layer. Note: The DMI version 1.x layer is a potential problem and enabling this setting is not recommended.
DMI 2.x Version	Detects the version of the Desktop Management Interface and the description of the DMI layer.
UNIX system configuration	Collects the UNIX/Linux configuration information.

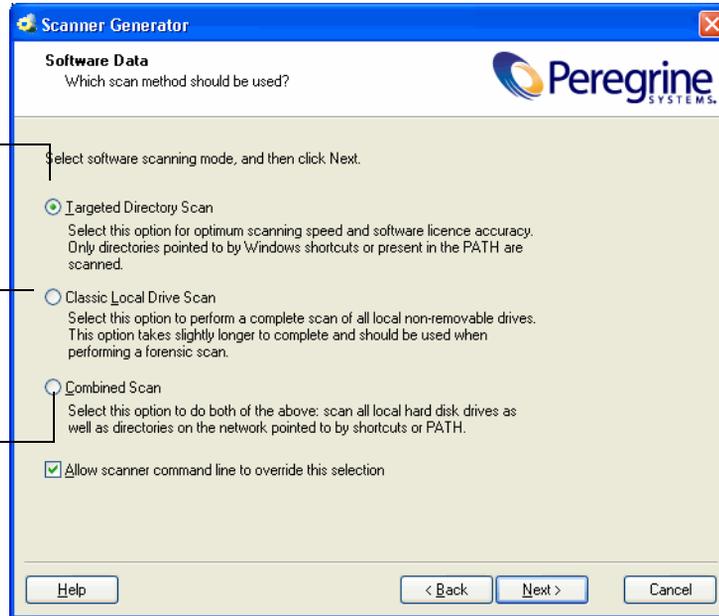
The Software Data Page

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, Stored Files and Plug-ins tabs

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

Displays the Drives, Drive Selection, Directories, File Scanning, Stored Files and Plug-ins 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.

Scanning Mode	Tab Pages Displayed...
Targeted Directory Scan	Directories File Scanning Stored Files Plug-ins
Classic Local Drive Scan	Drives Drive Selection File Scanning Stored Files Plug-ins
Combined Scan	Drives Drive Selection Directories File Scanning Stored Files Plug-ins

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.

Note: This page is not shown if Remote Scanner was selected on the Standard Configuration page in Manual Deployment Mode.

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

- **Targeted Directory Scan**

Select this option for optimum scanning speed and software licence 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
- Plug-ins

- **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
 - Plug-ins

- **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
 - Plug-ins

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 C:\Windows D:\Test
```

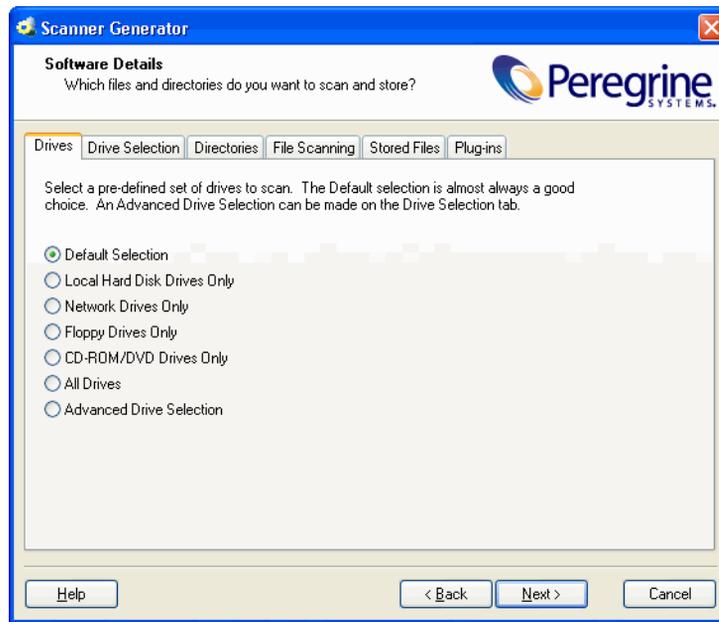
If you clear this check box, you cannot change the scan selection by specifying drive letters and/or paths on the command line.

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**.



Further Information

You can find information about how Scanners assign and use drive letters, what the volume list means in the section entitled [How Drive Letters and Volumes Are Assigned on page 217](#).

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 and OS/2).

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).

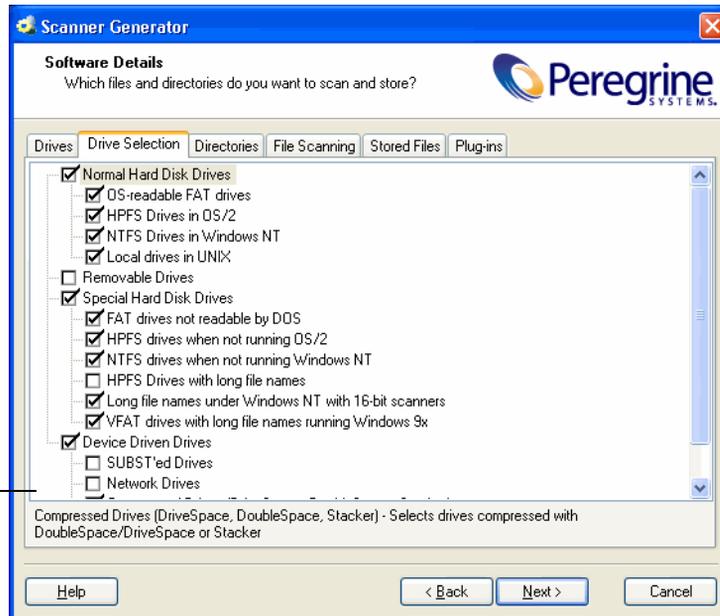
Scanner Configuration	Description
Default Selection	This setting selects sensible defaults for a standard inventory scan. Only fixed local drives are scanned. It also includes other non-network and non-SUBST'ed device driven drives.
Local Hard Disk Drives Only	This setting instructs the Scanner to scan 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 any other drive letter).
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 DOS, Windows and OS/2, normal hard disk drives are assigned

drive letters by the operating system and are usually included in the scanning process.

Drive Selection	Description
OS-readable FAT drives	Scans normal FAT drives accessible to the Operating System.
HPFS Drives in OS/2	Scans HPFS drives that OS/2 can access.
NTFS Drives in Windows NT	Scans NTFS drives that Windows NT/2000/XP/2003 can access.
Local drives in UNIX	Selects all normal partitions used in UNIX (ufs, ext2, ext3, tmps, etc.)

- **Removable Drives**

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

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.

- **Special Hard Disk Drives**

This group covers hard disk partitions not included in the Normal Hard Disk Drives category. Drives in this group are either not supported by the current operating system (such as FAT32 drives in Windows NT Version 4 or below or NTFS drives in DOS), or access to the drives may be restricted.

For these drives, the DOS, Win16, Win32 and OS/2 Scanners can employ sophisticated scanning algorithms that bypass the operating system and avoid the restrictions it imposes. Drives that are not assigned a drive letter

by the operating system are assigned a lower case drive letter for analysis purposes.

Drive Selection	Description
FAT drives not readable by DOS	Scans drives with FAT partitions (not readable by DOS). Normally all FAT drives are accessible by DOS. The exception is multiple primary FAT partitions on the same physical hard disk or FAT drives that are not mounted in Windows NT/2000/XP/2003.
HPFS drives when not running OS/2	Scans HPFS Drives when not running OS/2.
NTFS drives when not running Windows NT	Scans NTFS drives when not running Windows NT/2000/XP/2003.
HPFS drives with long file names	Enables long file name processing when running DOS Scanners under OS/2.
Long file names under Windows NT with 16-bit scanners	Enables long file name processing when running 16-bit Scanners under Windows NT/2000/XP/2003.
VFAT drives with long file names running Windows 9x	Enables 16-bit Scanners to scan FAT drives with long file name under Windows 95/98/ME.

- **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. In DOS, and OS/2 these drives always have drive letters associated with them and include networked drives and compressed 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.

Drive Selection	Description
Compressed Drives (DoubleSpace, DriveSpace, Stacker)	Scans compressed drives (DoubleSpace, DriveSpace and Stacker drives).
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

You can override the settings of:

- File Systems
- Directories and Files

File Systems

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

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

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

Because it is always possible, particularly on UNIX 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** for UNIX file systems.
- **override.ini** for Windows, DOS and OS/2 file systems.

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
```

Note: The name of the file, the sections and the files systems are case-sensitive.

Important: For the feature to work correctly, the .override.ini or 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.

Note: 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
```

Note: 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. This is useful when testing asset entries without having run software scan.

```
[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.

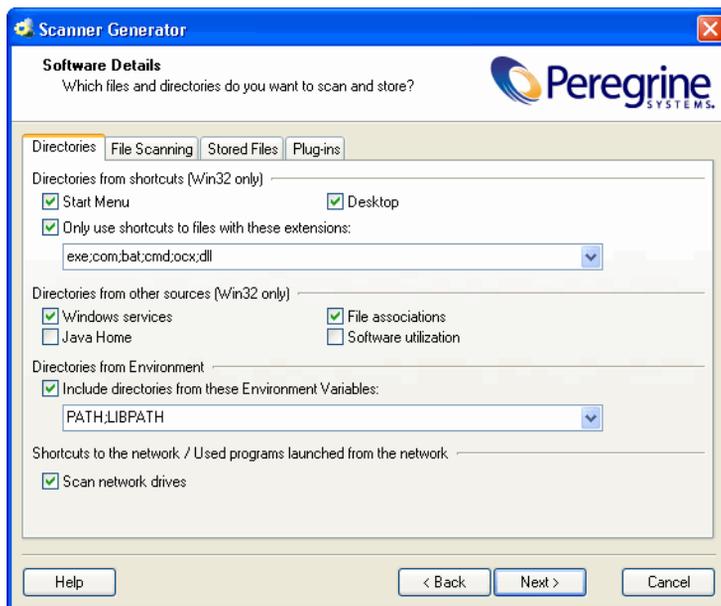
To prevent this happening, use the override.ini file with *.vir specified for exclusion (where .vir is a typical quarantine file extension). Check the specific virus product to find the extension for this type of file.

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 32-bit 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 (Win32 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 (Win32 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.
- Note:** 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

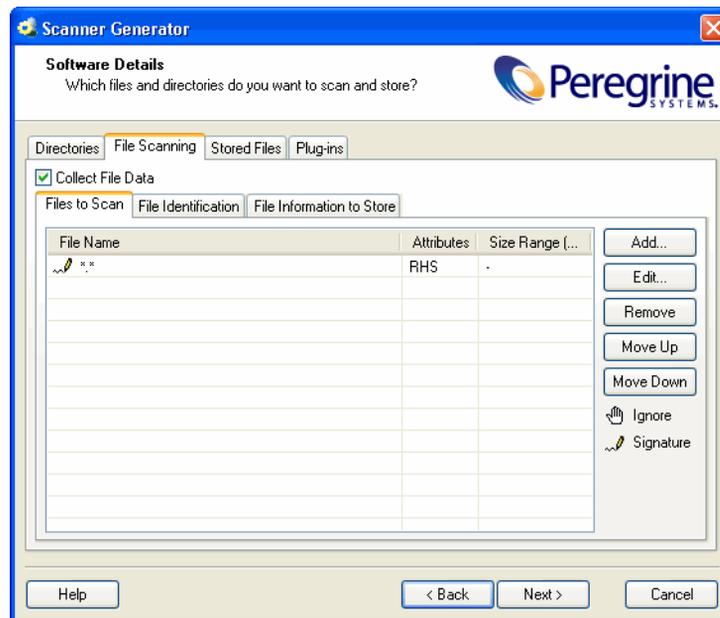
The **File Scanning** tab is used to specify the level of detail for the information collected about files and directories and the methods used to check and identify files.

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:

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 122](#)).

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).

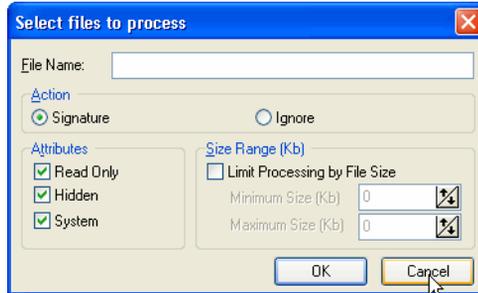
Important: When conducting a remote scan of Novell Netware compressed volumes, use the setting to Ignore all files. This is because the collection of signatures for compressed files results in NetWare decompressing the files, which uses a lot of server resources and reduces the available disk space.

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	-
 Dblspace.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.

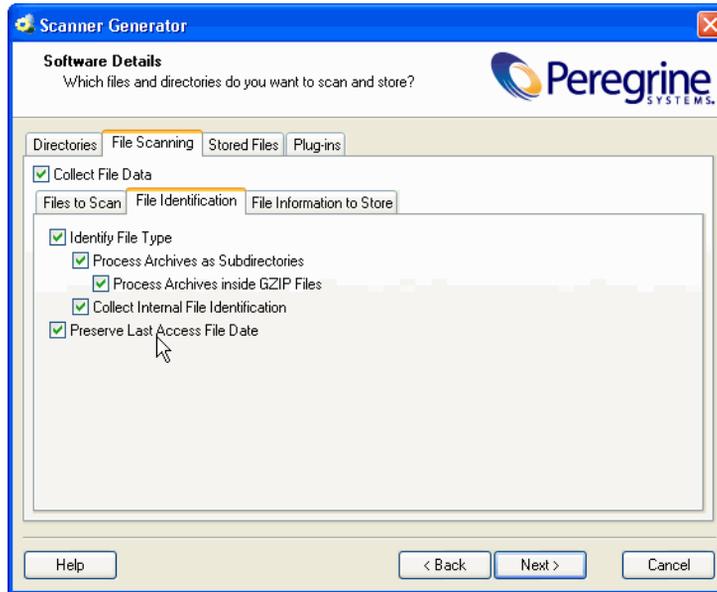
2-3: Ignore the following files, including files with read-only, hidden and system attributes:

- 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.
 - Dblspace.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, (CAB with plug-in), 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**

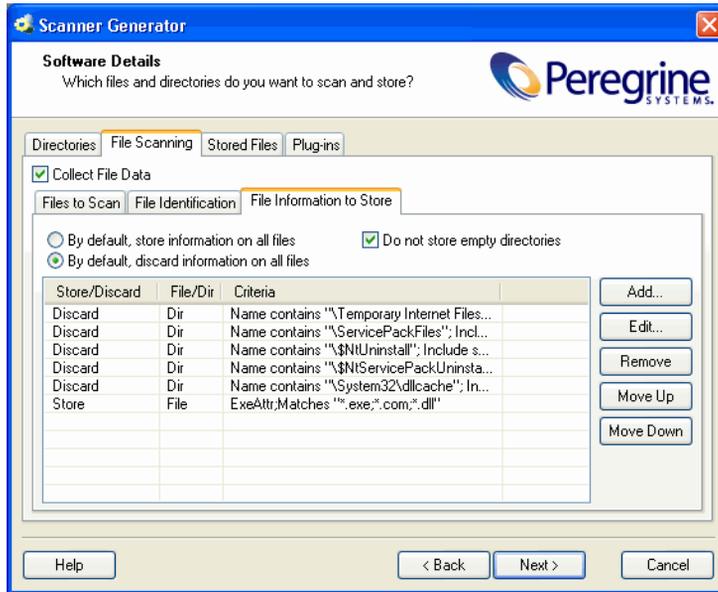
Collects the Last Accessed time stamp for files (where available). The support for the Last Accessed time stamp varies depending on the Operating System and file system used.

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 or Unix computers.

Important: 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.

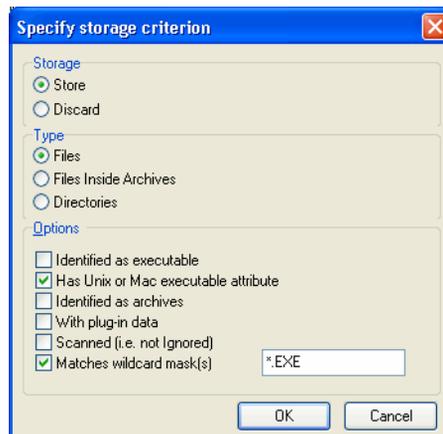
- Multiple filter criteria can be specified on each line if they are separated by a semicolon.
- Entries can be edited by double-clicking on them.
- The sequence and priority of an entry can be reordered by clicking on the row and dragging it up or down to its new location. This can also be achieved 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**.

Important: 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.

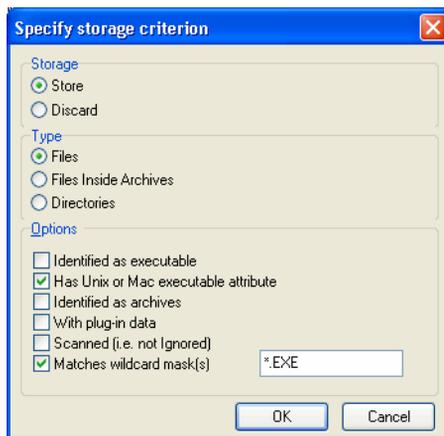


This dialog box has three types (shown in the Type group box):

- 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 90](#)), 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.

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, or are identified as such by an archive scanning plug-in. If Identify file type is not checked this has no effect.

- **With plug-in data**

Files that have plug-in data associated with them.

- **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

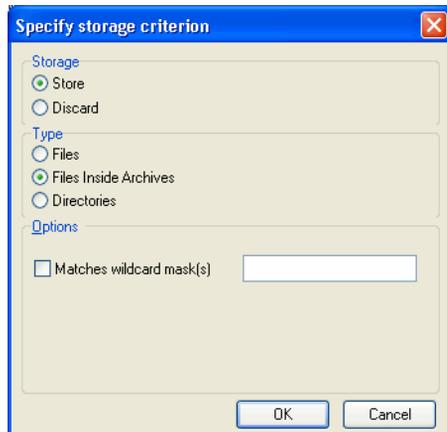
All file check box options specified are OR-ed together, that is, the entry is considered a match if any of the selected entries match.

For example, if Executable and With plug-in data are specified, this includes all executables, as well as all files with plug-in data. There is no way to select just executables with plug-in data.

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.

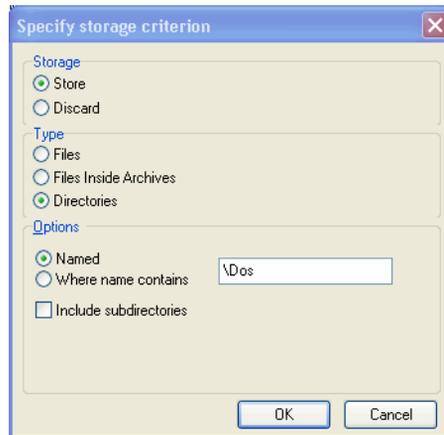


To include or exclude files based on the files inside archives:

- 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 124) 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 .

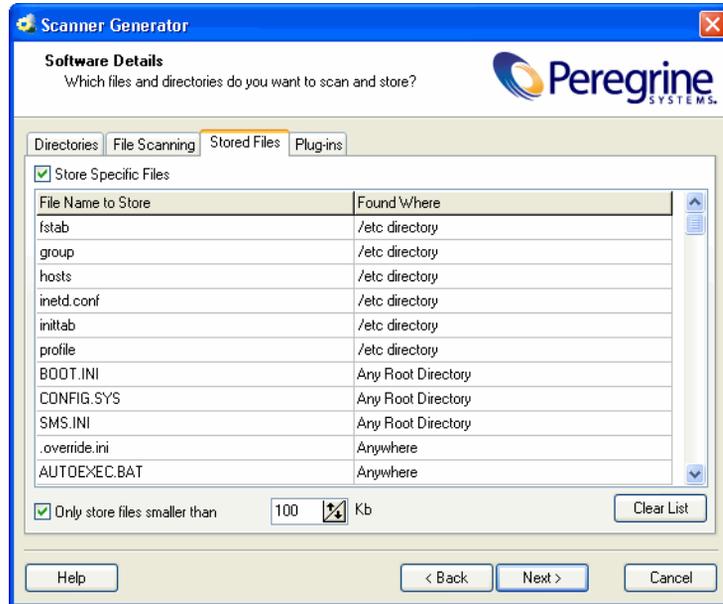
Directories are filtered prior to scanning (that is, directories that will not be stored are not scanned at all). Consequently, directory filters may speed up scanning.

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 (non UNIX) and .override.ini (UNIX)**

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 111.

Enabling the Controls on the Stored Files Page

To enable the controls on the Stored Files page:

- Select the **Store Specific Files** check box to enable the controls on this page.

Adding Another File to the List of Files Stored

To add another file to the list of files stored:

- 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.

Note: 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.

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.

Setting	Description
/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.</p> <p>For example, the list of specific stored files could be configured to be:</p> <p>C:\Documents\config.txt Z:\net.ini /etc/fstab</p> <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>

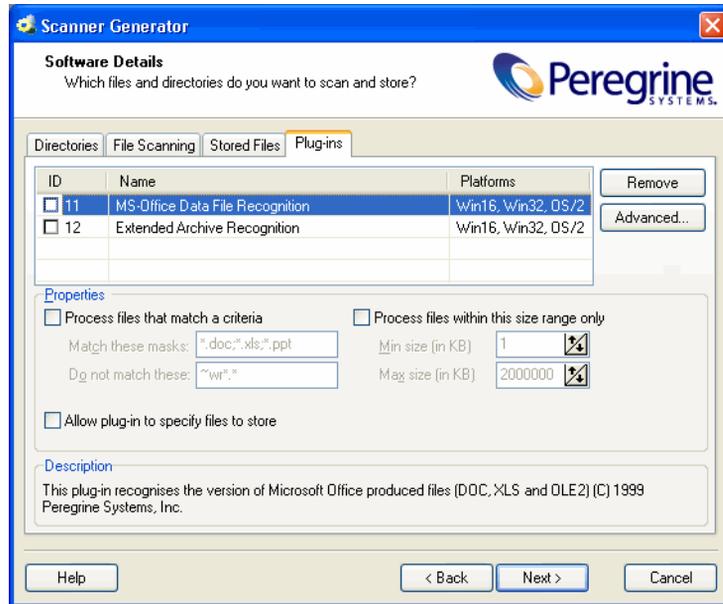
Note: Files will only be stored if the directory where the file is located is included in the software scan, unless the specific directory is specified.

The Plug-ins Tab

The **Plug-ins** tab is used to enable, disable and configure plug-ins for the Scanner.

Plug-ins extend the functionality of the base Scanner. This is achieved by using extra library functions to provide additional data.

Important: Plug-ins are currently supported by the Win16, Win32 and OS/2 Scanners only.



Plug-ins Provided As Part of the Scanner Generator

Two plug-ins are provided as part of the Scanner Generator.

- **Extended Archive recognition**

This plug-in extends the functionality of the Scanner by adding CAB archive processing to the Scanner. This displays the file list contained in Microsoft Cabinet (CAB) compressed files.

- **MS Office Data File recognition**

This plug-in determines the version used to create Word, Excel and other OLE2 document files. For these documents, the Title, Subject, Author, Comment and Keyboard fields can be extracted.

Note: The OLE Scanner plug-in may not always handle Office 2000 and Office XP files correctly. When doing enterprise-wide scans, it is recommended that this plug-in is not used.

Enabling or Disabling a Plug-In

The **Plug-ins** page shows a list of existing plug-ins that are currently installed, along with check boxes used to enable/disable a given plug-in.

To enable or disable a plug-in:

- Select the check box next to the entry to include/exclude it from the Scanner.

Check Box	Status
Checked	Plug-in enabled
Unchecked	Plug-in disabled

Setting Advanced Options for a Plug-In

Depending on the specific plug-in advanced options may be available.

To set advanced options for a plug-in:

- Select the plug-in that you want to set advanced properties for. If advanced properties are available for that plug-in, the **Advanced...** button will become enabled.
- Click the **Advanced...** button. The **Advanced Plug-in Configuration** dialog box appears.

Currently, only the MS-Office Data File Recognition (plug-in ID 11) plug-in has advanced configurable options. This plug-in has options to identify the specific file types to be read.

- From these files the specific columns to be displayed can be selected. Select the options as required.



Future plug-ins, or third party plug-ins may define their own advanced plug-in property dialog boxes.

Setting the Properties for a Plug-In

To set the properties for a plug-in:

- Click on a plug-in in the list.
- Set the options in the **Properties** group box.

This group box is used to specify various filters based on file size, location or file name. Only files matching the filter are sent to the plug-in to be processed.
- **To filter by the type of file:**

Enable the Process files that match a criteria box and specify the parameters to match.

This box accepts DOS wildcard characters, using * and ? as well as normal alphanumeric characters. Multiple file types must be separated by a semicolon. For example, *.doc ; *.xls
- **To filter by size:**

Enable the Process files within this size range only box and specifying the maximum and minimum size of the range in which the file size must lie. This allows you to specify only files of a size reasonable for the plug-in in question. For example, files with a size less than 100 bytes are unlikely to be valid OLE2 documents.
- **Allow plug-in to specify files to store**

When enabled, this option allows the plug-in to specify that files will be stored in the scan file. None of the default plug-ins use this option. Plug-ins may use this option to provide a way of dynamically adding specific files to the list of files to store in the scan file, after having inspected the contents of the file.

Removing an Existing Plug-In

To remove an existing plug-in:

- From the list, click on the plug-in to remove.
- Click the **Remove** button. A confirmation message appears.
- Click the **Yes** button. The files associated with a particular plug-in are deleted from the Program Files\Peregrine\Enterprise Discovery\2.0.0\Common\Pugins directory.

Note: Because removing the plug-in deletes files associated with it, ensure that copies of the plug-in files exist in another directory.

Creating Customized Plug-Ins

Enterprise Discovery includes an SDK (Software Development Kit) for writing custom plug-ins.

Please refer to the Scanner Plug-in SDK chapter in the *Reference Guide*.

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 three tabs:

- **The User Entry Tab** - Used to create an asset questionnaire
- **The Refilling Tab** - Used to set options that are used to prepare for re-scans
- **The Asset Number Tab** - Used to create an asset number batch file

After the asset data settings have been configured, click the **Next** button to continue.

The User Entry Tab

The **User Entry** tab is used to create an asset questionnaire which collects customized asset information as each computer is scanned.

Indicates that this field is the Asset Tag Field

Indicates that this is an Asset Data field

Indicates that this field is the Description Field



A default list of entries is displayed initially. These can be modified to create a custom list of entries.

Asset Questionnaire Definition

Information that is not automatically collected by the Scanner can be entered manually as each computer is scanned. The information collected is usually referred to as asset data, and includes details about users, departments, physical assets, equipment, and any other information that is useful to record.

Asset information that is manually entered, is defined using the User Entry form. This form allows:

- Fields for the information recorded to be defined.
- The page display for the user prompted information to be fully customized.

The effect is to present the user with a dynamic asset questionnaire, which prompts for and records specific information, as each computer is scanned.

The following figure shows a user entry form in the Scanner Generator and the resulting asset questionnaire page that is presented to a user when the Scanner is run.

These fields have been set up as **Required Fields** - they are shown in **Bold** in the Scanner Asset Questionnaire

The image displays two windows from the Peregrine Systems software. The top window, 'Scanner Generator', is titled 'Asset Data' and contains a table with three columns: 'User Prompt', 'Field', and 'Field Type'. The table lists several fields, with 'Asset Tag', 'Last Name', and 'First Name' highlighted in bold. The bottom window, 'Scanner - Win32 version', is titled 'User Asset Entry' and shows a form with the same fields. The 'Asset Tag', 'Last Name', and 'First Name' fields are bolded and have a grey background, indicating they are read-only. The 'Asset Tag' field contains the value 'FRB34401W0'. The 'Description' field contains 'Pentium 4, 2800MHz, 1024Mb'. The bottom window also shows a navigation bar with 'User Assets', 'Software', and 'Log' buttons, and a page number '116'.

User Prompt	Field	Field Type
Asset Tag	Asset Tag	Sequence
Last Name	Last Name	Formatted string
First Name	First Name	Formatted string
Department	Department	Type or Pick List
Office Location	Office Location	Type or Pick List
Telephone Extension	Telephone Extension	Field with minimum value

Read-Only fields cannot be modified by the user

The User Entry Form Layout

The **User Entry** form is made up of a number of rows and three columns. Each row in the form is used to define an entry for the asset questionnaire and results in one item being collected during the inventory.

The asset questionnaire is built up by using the combination of up to 23 predefined standard fields, 30 user fields and 28 automatic fields to create a fully customized data entry form.

The User Entry Form Toolbar

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

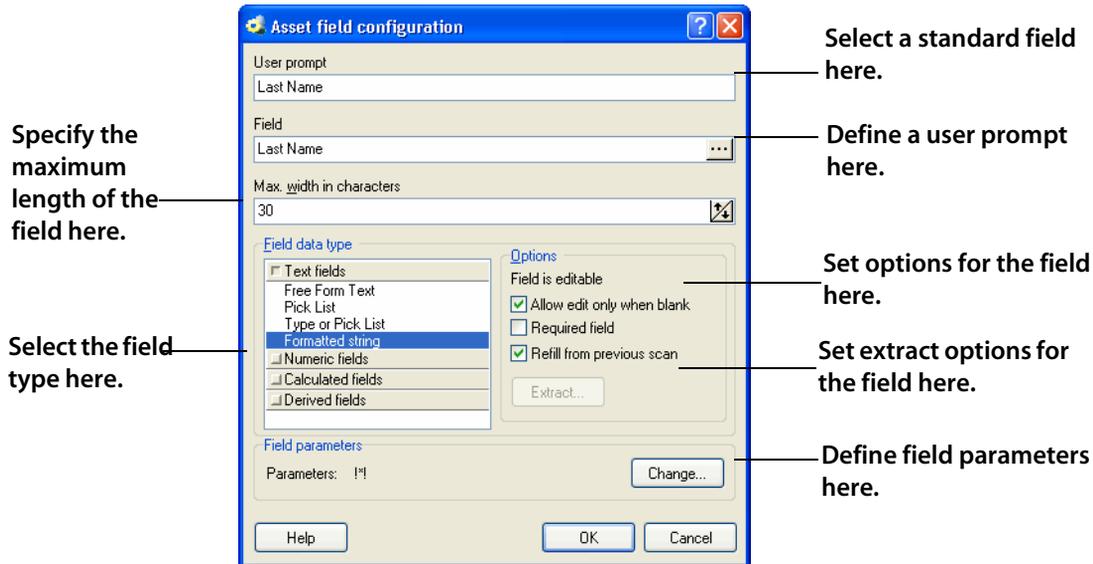
Button	Function	Shortcut
	Create a new field The Choose Field dialog box appears.	Ctrl+N
	Create a new label field A dialog box is displayed allowing you to enter the text to show in the label. This field type is used only to provide information to a user during the scan. The limit on the length of labels is 255 characters.	Ctrl+L
	Delete field	None
	Delete all fields Clear all the entries in the User Entry 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 asset entry 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:

Step	Title	See...
1	Choose a standard field	page 143
2	Set up a user prompt	page 146
3	Specify the maximum number of characters the user can enter in the field	page 146
4	Choose the field data type	page 146
5	Set up field options	page 150
6	Set up field parameters	page 151
7	Set up extract options for calculated fields	page 174
8	Correct the order of the fields in the form	page 176

Step 1: 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.

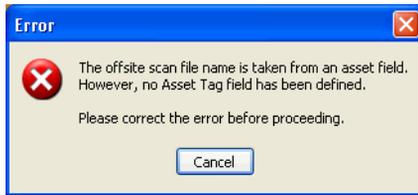
When loading data from scans into the analysis tools (Analysis Workbench and Viewer), the contents of the description field are displayed for each scan file to help identify them.

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, Dell or Compaq 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 in the questionnaire 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.

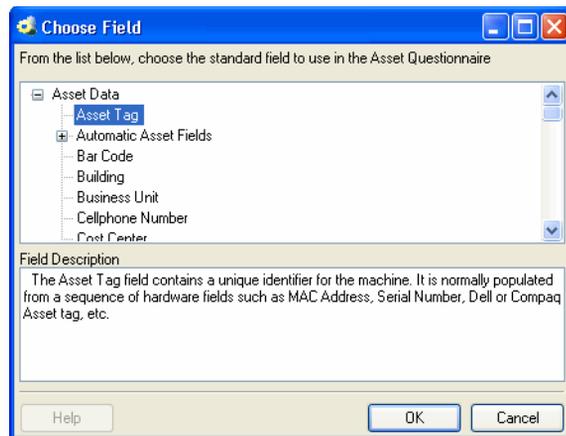


Refer to [The Asset Number Tab on page 182](#) for more information about setting the Asset Tag options.

Important: It is strongly recommended that **Description** and **Asset Tag** fields are included in your asset questionnaire.

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.

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
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

Field	Description	Field mapped to in the hwAssetData table
Telephone Number	Full direct telephone number of user	hwAssetTelephoneNumber
User Field	These are user-defined fields that are displayed in the asset questionnaire. You can configure up to 30 User fields.	hwAssetUserField1..30

- Click **OK** to return to the user entry form.

Step 2: Setting Up a User Prompt

This text prompt is used to identify each data input item on the asset questionnaire and to inform the user what information to enter (Scanner Generator truncates the prompt at 22 characters).

To set up a user prompt:

- Double-click on the row to bring up the **Asset field configuration** dialog box.
- To change the user prompt, change the entry in the **User prompt** field.
The text entered here will be displayed as an on-screen text prompt when the user sees the asset questionnaire.

Step 3: Specifying the Maximum Number of Characters the User Can Enter in the Field

To specify the maximum number of characters the user can enter in the field:

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

Step 4: Choosing the Field Data Type

There are two classes of fields:

- **User entered (numeric or text)**
These asset data fields require manual input or selection from the user.

- **Calculated (automatic or derived)**

These asset data fields can be automatically populated, and the data extracted from text files, the Windows registry and environment variables. All automatic 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 used to input user asset data and whether they are user entered or calculated.

Text Fields

These fields allow the user to enter text or select entries from a predefined list (pick list).

Field	Description
Free Form Text (user entered)	Allows the user to enter free text that is not formatted or restricted in any way (except length). A Free Form Text field allows the user to enter text from the keyboard without any restrictions on the characters entered.
Pick List (user entered)	Displays a predefined drop-down list of options for the user to select an entry.
Type or Pick List (user entered)	Displays a predefined drop-down list, from which an entry can be selected. If the required option is not in the list, the required data can be typed in by the user.
Formatted String (user entered)	Accepts data entered in a predefined format according to a specified mask, that is, restricting input to numeric, letters and so on. This is useful for ensuring data consistency and can be used to force letters to upper case or to conform to a certain standard. For example, A preformatted telephone number: 0208 563 2359 could be set up as the following formatted string: 0208 563 [#####]

Numeric Fields

These fields accept numerical values only. This forces entries to be:

- Above or equal to a defined minimum value.
- Below or equal to a defined maximum value
- Between an upper and lower limit

Field	Description
Field with minimum value (user entered)	Accepts a numeric value that is greater than or equal to a specified number.
Field with maximum value (user entered)	Accepts a numeric value that is less than or equal to a specified number.
Field with a valid range of values (user entered)	Accepts a numeric range that is between two specified numbers (which form the inclusive upper and lower limits of the range).

Calculated Fields

These asset data fields can be automatically populated from data extracted from text files, the Windows registry, environment variables and so on.

Note: Calculated asset fields do not work with the Remote Scanner as it does not run on the computer being scanned.

Field	Description
Environment Variable Extract (calculated)	Accepts data from a specified environment variable set in the operating system.
Text File Extract (calculated)	<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>

Field	Description
Registry Extract (calculated)	This field type extracts its value from the Windows registry. The Data field must contain a valid registry key name to extract from, for example: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\TimeZoneInformation\StandardName
DMI Extract (calculated)	The DMI field allows you to select the search criteria for the DMI attribute, the value of which you wish to have in this field. DMI extract fields are supported by the Win32 and OS/2 Scanners only.
WMI Extract (calculated)	This field type allows you to extract and store pieces of data on Windows 32-bit systems available through the WMI interface. The Win32 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.

Field	Description
Sequence (derived)	The Sequence field allows you to define a sequence of up to ten asset or hardware fields. Each of these fields returns a value depending on the machine or environment running. The value returned as the result of the sequence field will be the first of these fields which contains a non-blank value.

Field	Description
OS/Scan (derived)	<p>Allows a single field to collect different information for different operating systems. For example, you may want to extract information from a file only on machines running Windows 95.</p> <p>For each valid combination of Scanner and operating system, a separate asset field must be defined. When the Scanner is executed the appropriate asset entry is selected.</p>
Combination (derived)	<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 questionnaire.</p> <p>Up to five fields can be combined into one.</p>

Step 5: Setting Up Field Options

You will notice that depending upon the field data type you selected in the previous step, the options available for that field data type change accordingly.

In summary the options are grouped as follows:

- **For a text or numeric field**

The field is editable by default. This means that unless you change the settings here, the user will always be able to change the information in this field. The options are:
- **Allow edit only when blank**

Only allow the user to enter or change data in this field if the field is empty. The only way a field of this type can be non-blank is if it is refilled.
- **Required Field**

Designate this field as 'required'. The field is displayed in bold text in the Asset data page and the Scanner and must be filled in. The Scanners will not save a scan file until a non-blank value is entered.
- **Refill from previous scan**

The field will be refilled with data from a previous scan. You can set up various refilling parameters from the Refilling tab of the Asset Data page. See [page 177](#) for more information.

- **For a calculated or derived field**

The field is not editable by default. This means that unless you change the settings here, the user will not be able to enter or change the information in this field. Generally, for automatic and derived fields you do not want users to be able to change or enter data into these types of fields because the information is obtained from elsewhere. The options are:

- **Allow edit if blank**

This option can be set so that if the data for an automatic or derived field cannot be successfully obtained, the user will be able to enter some data manually into the field. When you select this option, a further option to make the field a 'Required' field is made available.

- **Refill from previous scan**

The field will be refilled with data from a previous scan. You can set up various refilling parameters from the Refilling tab of the Asset Data page. See [page 177](#) for more information.

Step 6: Setting Field Parameters

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

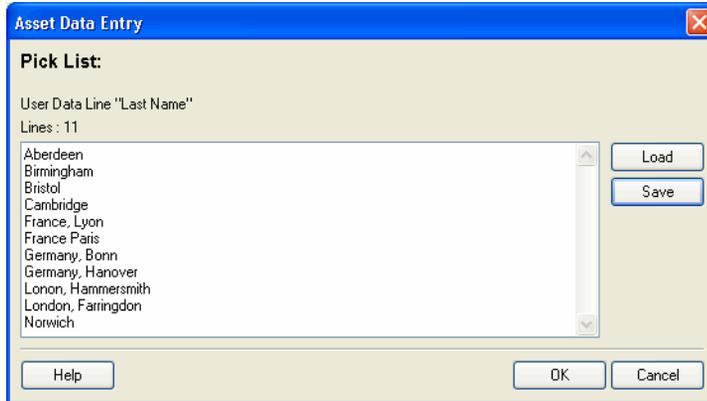
Field	See...
Pick List	page 152
Type or Pick List	page 153
Formatted String	page 153
Numeric	page 155
Environment Variable Extract	page 156
Text File Extract	page 156
Registry Extract	page 159
DMI Extract	page 160
WMI Extract	page 164
Sequence	page 167
OS/Scan	page 168
Combination	page 173

Setting Pick List Field Parameters

A pick list consists of a fixed list of entries that provide the entry options. The only entry choices available to the user are from this list.

To set pick list field parameters:

- After you have selected Pick List as the data field type, click the **Change...** button next to the **Field Parameters** box.



- Click in the list box and type the text into the scrolling list area. Enter a list of predefined entries that you want to provide, or add, modify or delete existing entries.

Important: The limit on the size of pick lists in the DOS Scanner is 8k. The size of the lists in any other Scanners is restricted to 4000 entries. Scanner Generator displays a warning if the size is greater 8K indicating that the pick lists will be truncated for DOS Scanners. Although the size is not limited for non-DOS Scanners, it is not advisable to create too large lists as they increase the size of the Scanner configuration that will be stored in the Scanner itself.

- You can also generate a list in a text editor (for example, in Notepad) and load in this dialog box. A sample of the entries in such a file could be as follows entries in a **Department** pick list.

Accounts
 Corporate Finance
 Development
 Facilities Management

Legal Management

To load a list of text entries from a text file, click the Load button to browse the directories and select a file. A file loaded using this option must be an ASCII text file.

- This list can also be used in the Analysis Workbench to provide query selection criteria for machines. To save a list so that it can be re-used, click the Save button to select a destination and file name for the file. A file saved using this option is an ASCII text file.
- Click **OK** to return to the **Asset Field configuration** dialog box.

Setting Up Pick List or Type/Pick List Parameters

This uses a list in the same way as in the pick list but with the additional option of allowing data entry of an item that does not appear in the list.

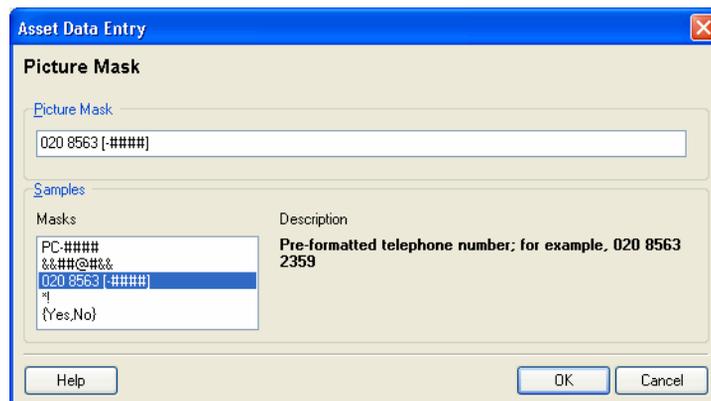
Use this option when generating an initial walkaround Scanner, to allow for unexpected additions.

Setting Up Formatted String Parameters

This field is set up to force data entry to conform to a particular mask of characters.

To set up formatted string parameters:

- After you have selected **Formatted string** as the data field type, click the **Change...** button next to the **Field Parameters** box.



- Create a picture mask for the formatted string field using character combinations from the picture characters provided.

The following characters can be used to create a picture mask:

Character	Stands for
#	Numeric digit.
?	Any letter (uppercase or lowercase).
&	Any letter (convert to uppercase).
@	Any character.
!	Any character (convert to uppercase, if alphabetical).
*	The next character following the * in the mask can be repeated zero or more times.
[abc]	Optional characters a, b, or c.
{a,b,c}	Grouping operators a, b, or c can supply a set of alternatives separated by commas. So {a,b,c} means accept either character 'a', 'b' or 'c'. Any other character will be erroneous.

Note: Semicolon (;) interprets the next character as a literal, not as a special picture string character.

If any other character is used in a picture mask, it is treated as a constant. When a value with a picture validity check is entered into a field, at the point where a constant is specified, it is automatically inserted.

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

Example of Formatted String Parameters

Character string	Stands for
PC-####	Asset number; for example, PC-2085
&###	Room number; for example, D502
020 8563 [#####]	Preformatted telephone number; for example, 020 8563 2359
*!	Creates a mask that accepts any number of characters and converts them to upper case.
{Yes, No}	Either Yes or No

Setting Up Numeric Field Parameters

These fields accept numerical values only. This forces entries to be:

- Above or equal to a defined minimum value
- Below or equal to a defined maximum value
- Between an upper and lower limit (inclusive)

The screenshot shows a dialog box titled "Asset Data Entry" with a close button in the top right corner. The main heading is "Specify range restriction". Under the "Minimum" section, there is a label "Minimum Value:" followed by a text input field containing the number "0" and a small icon with a slash and a square. Under the "Maximum" section, there is a label "Maximum Value:" followed by a text input field containing the number "10" and the same icon. At the bottom of the dialog, there are three buttons: "Help", "OK", and "Cancel".

To set up numeric field parameters:

- After you have selected a **Numeric field** as the data field type, click the **Change...** button next to enter the parameters as follows:
- If you selected **Field with minimum** value, then enter the lower limit for the value into the **Field parameters** box.
- If you selected **Field with maximum** value, then enter the upper limit for the value into the **Field parameters** box.

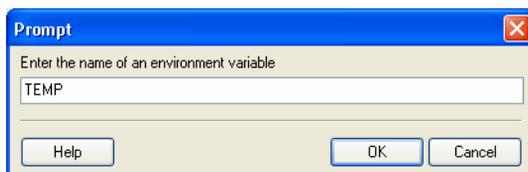
- If you selected **Field with a valid range of values**, then enter the upper and lower limits. For example, 0-10 indicates that values between 0 and 10 will be accepted, including the values 0 and 10.
- Click **OK** to return to the **Asset field configuration** dialog box.

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 select the name of the file that the information is to be extracted from. There are three predefined file names and search strings:

- Asset.bat**

Extracts the asset number on the line starting SET ASSETNO= in the Asset.bat file. This file may have been created by an earlier scan.

- Sms.ini**

Extracts the SMS ID on the line starting SMS Unique ID= in the SMS.ini file.

- InfrTool.ini**

Extracts the asset number on the line starting ASSETNUMBER= in the InfrTool.ini file. This file may have been created by an earlier scan.

- Select the **Other** option to specify another file to extract 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
```

Note: Entries in this field are case-sensitive. This is applicable to UNIX only because in Windows and DOS the case does not matter.

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

Note: 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).

Note: 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.

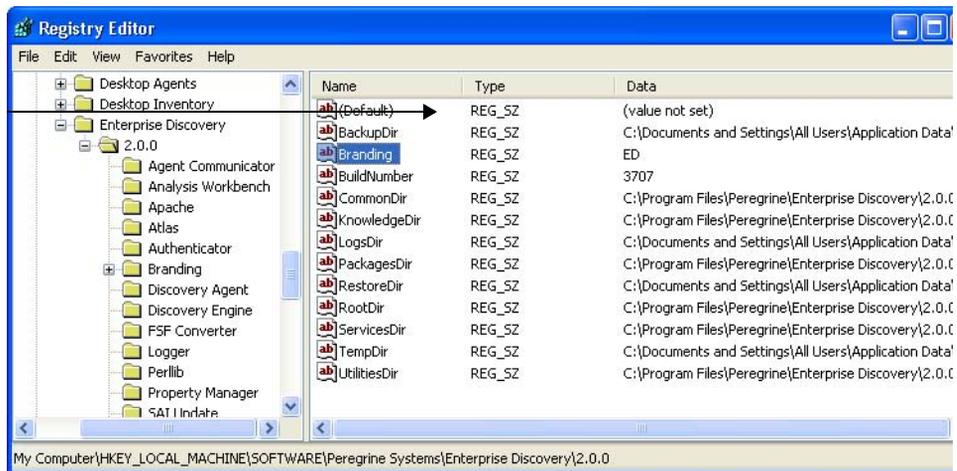
Warning: Do not change any of the settings in the Registry Editor. Doing this could result in lost registry settings and may cause some of your applications to fail.

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.

The Branding value



To extract the Branding value from the registry:

- 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\Peregrine Systems\Enterprise Discovery\2.0.0\Branding"
```

Setting Up a DMI Extract Field

Desktop Management Interface (DMI) data is organized as a collection of Components. Components are physical or logical entities on a system, such as hardware, software or firmware.

Important: DMI extract fields are supported by the Win32 and OS/2 Scanners only.

Components have one or more named Attributes that collectively define the information available to a management application. Attributes are collected into named Groups for ease of reference. Groups may be scalar or may be replicated, such as the set of attributes for each instance of a network interface table. Replicated groups are called Tables, and a row (instance) of a table is referred to by a set of attributed that form a Key.

Definitions

- **Component** - Any hardware, Software or Firmware element contained in (or primarily attached to) a computer system.
- **Attribute** - A piece of information about a component.
- **Group** - A collection of attributes. A group with multiple instances is called a table.
- **Class string** - A text string that identifies a group outside the context of a particular component declaration. Identical group definitions will have identical class strings.

To set up a DMI extract field:

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

Define DMI Extract Asset Field

DMI Attribute Name: DMI Component Name: Description: Type the name of the DMI attribute you want to be collected in this DMI extract field.

DMI Class Name: For example, to extract the asset tag from the standard DMTF system MIF, use the following attribute name:

Collect Values: All values First Matching All Matching Attribute: Asset Tag Class: DMTFSystem Enclosure

Separate values with:

#	Name	Value
1		
2		
3		
4		
5		

Buttons: Help, OK, Cancel

- Define the search criteria for the DMI attribute
Type the name of the **DMI attribute** that you want to be collected in the **DMI Attribute Name** box. For example, to extract the asset tag from the standard DMTF (Desktop Management Task Force), use the following attribute name:

Asset Tag

- Define the search criteria for the DMI class name

In the **DMI Class Name** box, type the name of the class that identifies the DMI group in which the attribute is located. DMTF defines a number of standard groups, which have the form:

DMTF|Group|Version

For example:

DMTF|System Enclosure|002

Partial names are allowed. A group is considered to be match if the beginning of the string entered here is identical to the beginning of the class name.

In the example, if all System Enclosure groups are of interest, a version does not need to be specified, for example:

DMTF|System Enclosure|

- Define the search criteria for the DMI component name

In the **DMI Component Name** box, type the name of the DMI component that contains the field of interest. Multiple names must be separated by semicolons.

The **Component Name** is usually specified only for standard groups, such as ComponentID, for which the attribute and class names are not enough to identify the attribute or when the standard groups occur more than once. If this field is empty, any component is considered to be a match.

For example, to extract the Manufacturer attribute of a network card, use the following:

DMI Attribute Name: Manufacturer
DMI Class Name: DMTF|ComponentID|
DMI Component Name: LAN Adapter

- Specify DMI value options

To collect values for a particular attribute, in the **Collect Values** group, select one of the following:

- **All values**

Select this option to collect all values for an attribute. If the group is a table, all values in the table for the attribute specified are collected and separated with a string defined in the Separate values with box.

Specify the string of characters that are used to separate multiple values of a table attribute. For example, a comma or a semicolon can be used, provided they are unlikely to be part of the value itself.

- **First matching**

Select this option to collect a specific value for an attribute to match, in the grid on the right. If the attributes to match are not key attributes, there may be more than one value that matches the criteria. This option forces only the first matching value to be collected.

- **All matching**

Select this option to collect a specific value for an attribute in a table group. Specify the attributes to be matched in the grid on the right. If the attributes to be matched are not key attributes, there may be more than one value that matches the criteria. This option forces all matching attributes to be collected and separated with a string specified in the Separate values with box:

Specify the string of characters that are used to separate multiple values. For example a comma or a semicolon can be used, provided they are unlikely to be part of the value itself.

- Specify a set of attribute names and attribute value pairs to match.

The values of an attribute will only be collected if all attributes to match have got the values specified in the Attributes to match grid. This option is normally used for attributes inside table groups. For example, to collect a description of the device that occupies IRQ3, the following can be used:

```
DMI Attribute Name: IRQ Description
DMI Class Name: DMTF|IRQ|
Attributes to match: Name=IRQ Number
Value=3
```

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

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 Win32 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

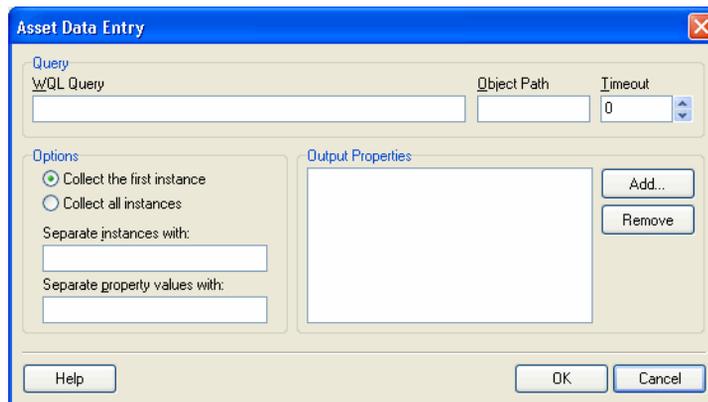
Windows Management Instrumentation Query Language (WQL) is a subset of SQL that is used to make data queries inside WMI.

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 WML Extract Field Setup

Options	Entry
WML 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
```

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.

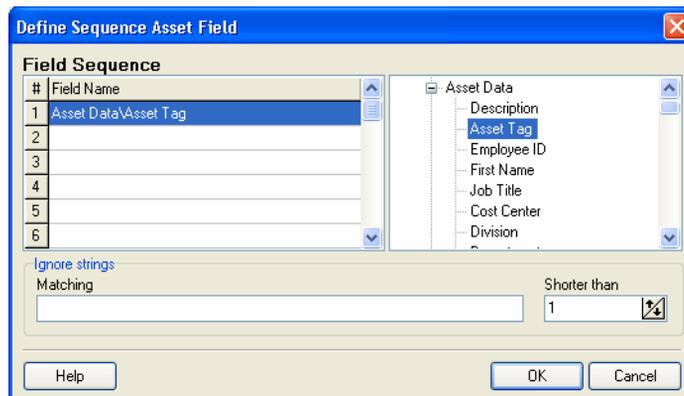
The value returned as the result of the sequence field, will be the first of these fields which contains a non-blank value. If all values are blank, then the user can be allowed to type a manual entry instead.

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 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, a registry key, where source for registry keys is held in different locations for different operating systems. In this case, you can set up an OS/Scan field, which alleviates the need to set up multiple registry key field extract fields.

In addition, it allows you to set up a method to obtain the value when scanning operating systems that have no registry. An example of this is in DOS, where an environment variable or file extract field could be used.

The Multi-OS asset entry field dialog box has two tabs:

- **Other** - Used to set up OS/Scan fields for DOS, Windows 3.x, Windows 95, Windows NT/2000/XP/2003 and OS/2 operating systems.
- **Unix** - Used to set up OS/Scan fields for UNIX Operating systems.

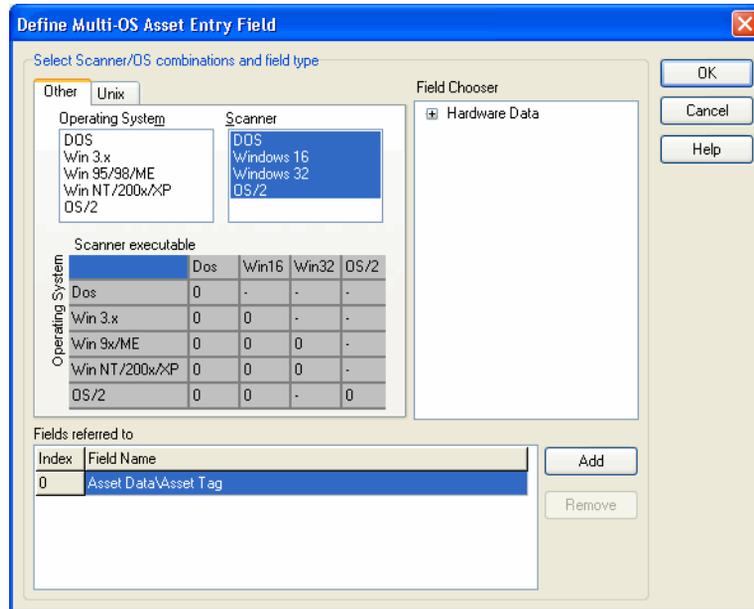
Setting Up OS/Scan Fields for DOS, Windows 3.x, Windows 95, Windows NT/2000/XP/2003 and OS/2

For these operating systems, multiple Scanners are compatible and the OS/Scan field allows the following combinations of Scanners and operating systems to be defined.

Operating System	Scanner
DOS	DOS
Windows 3.x	DOS
Windows 3.x	Windows 16-bit
Windows 95/98/ME	DOS
Windows 95/98/ME	Windows 16-bit
Windows 95/98/ME	Windows 32-bit
Windows NT/200x/XP	DOS
Windows NT/200x/XP	Windows 16-bit
Windows NT/200x/XP	Windows 32-bit
OS/2	DOS
OS/2	Windows 16-bit (in Win-OS/2)
OS/2	OS/2

To set up OS/Scan fields for DOS, Windows 3.x, Windows 9x/ME, Windows NT/200x/XP and OS/2:

- 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.
- Click the **Other** tab.



- In the **Operating System** list select the operating system(s) that will be affected by this definition. To select multiple operating systems, hold down the Ctrl key and click on each one in turn.
- In the Scanner list select the Scanner types that will be affected by this definition. To select multiple Scanner types hold down the Ctrl key and click on each one in turn.
- 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.
- Click **OK** to return to the Asset Field configuration dialog box.

Interpreting The Matrix

The selection matrix is the grid that is displayed in the middle of this dialog box. It shows the current assignments of each of the list items. For each combination of Scanner and Operating System, the number in the matrix refers to a line number in the Fields referred to list (a hyphen '-' in the grid indicates that the combination is invalid).

The matrix sorts through the list (the bottom-most entry has the highest priority). The priority can be changed by dragging the a row up or down in the list. If a matching combination is not found it defaults to index 0 (the top most entry in the list).

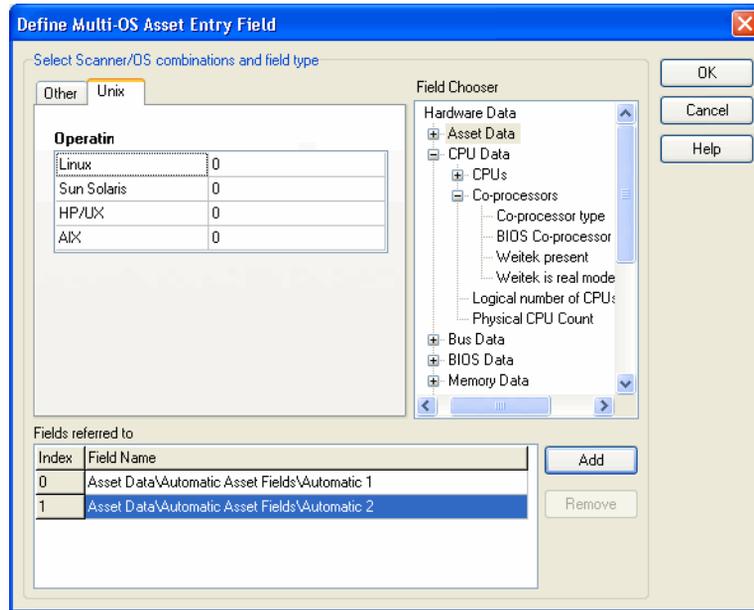
Setting Up Multi OS-Scanner Fields for UNIX Environments

The UNIX environments currently supported are:

- Sun Solaris 2.5, 2.6, 7, 8 and 9
- HP-UX 10.2 and 11.0
- Linux Kernel v2.2, 2.4, 2.6
- AIX 4.3, 5.0, 5.1, 5.2, 5.3

To set up multi OS-Scanner fields for UNIX environments:

- After you have selected an OS/Scan field as the data field type, click the Change button.
- Click the **UNIX** tab.



- Select a row in the UNIX Operating System list.
- If the field to refer to is not already in the list, select the field that is to be included in this definition from the Field Chooser tree. Otherwise, just set the field index in the grid.
- Click the **Add** button. It is added to the **Fields referred to** list.
- Click **OK** to return to the **Asset Field configuration** dialog box.

Interpreting the Grid

The **Field Index** column has a drop-down list which refers to the line numbers in the Fields referred to list.

Because multiple OS-Scanner combinations for the UNIX Scanners do not exist, (that is, an HP-UX Scanner cannot be used on a Solaris machine and so on) the selection matrix logic does not apply here.

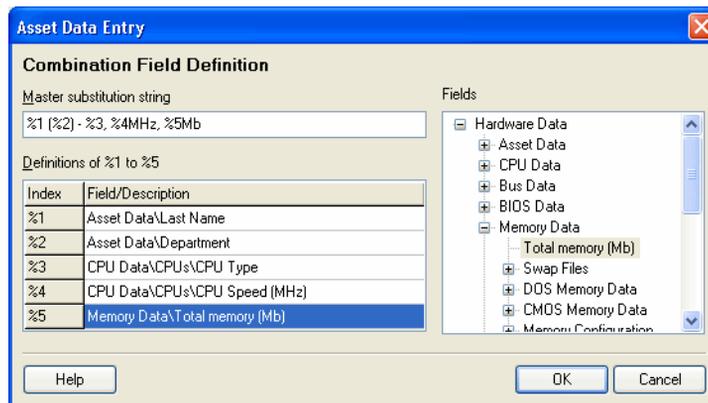
Setting Up a Combination Field

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 (%2) - %3, %4MHz, %5Mb is defined for the Description field in the asset entry form, where the following index definitions apply:

Index	Field/Description	Displayed in asset questionnaire as...
%1	Asset Data\Last Name	Last Name
%2	Asset Data\Department	(Department)
%3	CPU Data\CPUs\CPU Type	-CPU Type
%4	CPU\CPUs\CPU Speed (MHz)	CPU SpeedMHz
%5	Memory Data\Total memory (Mb)	Total MemoryMb

The **Description** field in the Asset Questionnaire may look as follows:

SMITH (Accounts) - Pentium II, 333MHz, 128Mb

Step 7: Setting Extract Options

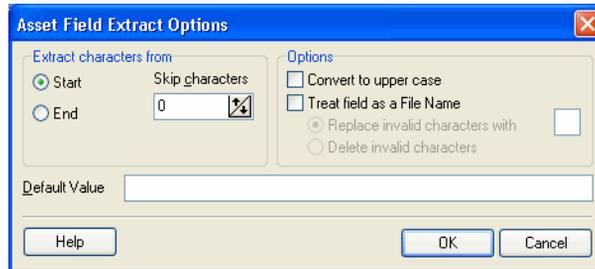
All calculated asset fields defined can be set up so that only part of the string is selected instead of the entire string. They can also be set up, for example, to use the last part rather than the first part of the string. This can be useful for obtaining the last part of an calculated field that is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

- 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.

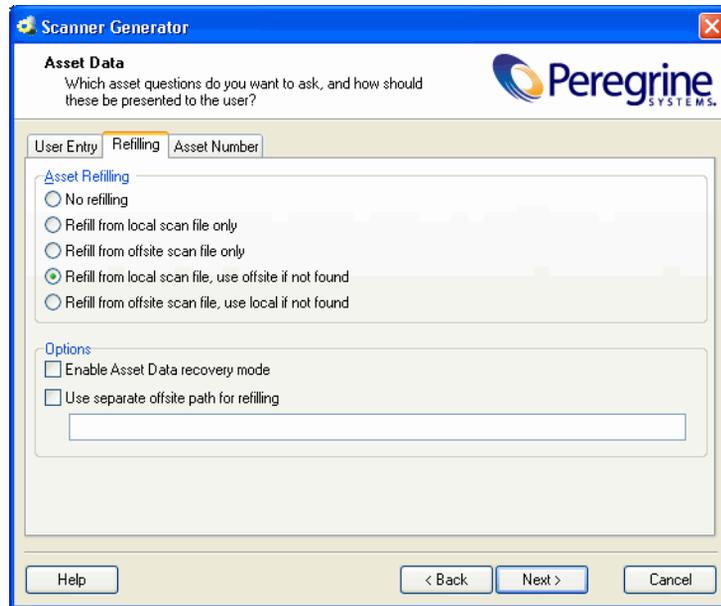


- Click **Yes** to have the Scanner Generator automatically do this for you.
- Click **No** to do this manually.

The Refilling Tab

The **Refilling** tab sets options used to prepare for re-scans.

Note: Extract fields are filled in after the refill has completed. This ensures the current state of the machine is recorded.



The tab page is divided into two sections:

- **Asset Refilling** - These options determine where refilled data will be taken from on subsequent scans.
- **Options** - These options are used to refine the asset refilling process.

How Refilling Works

Refilling is used to help reduce the amount of data entry required on re-scans by filling the asset entry fields with data from previous scans.

When a scan starts, the Scanner will attempt to locate an old scan file for the machine to read the asset data from, so that the user need not retype all of the data.

When refilling asset data, the Scanner searches for the scan file to be used for refilling. The following message is output to the log window:

```
Refilling asset data from <filename>
```

Where <filename> is the fully qualified scan file name that will be used to refill the asset questionnaire.

If the asset questionnaire of the Scanner has changed since the last scan, the old and new asset information is matched up based on the field names. The old data is then validated using the constraint of the current Scanner asset field configuration, if any, and if valid, the refill of that field is permitted.

Asset refilling can take place from either of two files:

The Local Scan File

The location of the local scan file varies depending on the platform.

- If the Scanner can write there, for Win32 the location is:
C:\Documents and Settings\All Users\Application Data\Peregrine\Enterprise Discovery

For restricted users in Manual Deployment mode the location is:

```
User profile\Application Data\Peregrine\Enterprise Discovery
```

- For DOS, OS/2 the location is in the directory of the first logical drive, usually
C:\infrtool
- For UNIX the location is in the agent's data directory, which is
\$home/discagent

The name of the local scan file is always **local\$.fsf** or **local\$.xsf**. In Enterprise mode, the Scanners always save a local scan file.

Offsite Scan File

This is a copy of the scan result that has been saved to remote disk (such as floppy disk or network disk).

The offsite scan file name is generated from the asset field that has been designated as a field that will identify this computer across the population.

Note: Off-site refilling is only available from a UNC path.

Specifying a Refill Order

To specify a refill order:

- In the **Asset Data** page, click the **Refilling** tab.
- The refill order is set in the **Asset Refilling** group box. It can be one of the following:
 - **No refilling** The refilling options are disabled. No data is refilled.
 - **Refill from local scan file only** The refilled data is taken from scan file saved on the local machine. This is the default in Enterprise mode, since only a local scan file is saved in this mode.
 - **Refill from offsite scan file only** The refilled data is taken from a scan file saved on a remote disk (such as floppy disk or network disk). The local scan file, even if present, is not used.
 - **Refill from local scan file, use offsite if not found** The refilled data is taken from a scan file saved on the local machine. If no local scan file is found, the refilled data is taken from a scan file saved on a remote disk, if present.
 - **Refill from offsite scan file, use local if not found** The refilled data is taken from a scan file saved on a remote disk. If no remote scan file is found, the refilled data is taken from a scan file saved on the local machine, if present.

By taking the offsite scan file first, it is possible for an administrator to perform a quality check on the asset data (using the asset data editing functionality of Analysis Workbench and Viewer). The updated data is then automatically used on re-scan.

Note: The refill path can be overridden by using the `-r:` command line option. 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*.

Specifying Options for Refilling

To specify options for refilling:

- Select the **Enable Asset Data recovery mode** check box to ensure that data is not lost if, for some reason, the Scanner does not complete.

When selected, the Scanner saves a backup of the asset questionnaire as soon as it is complete. When the scan file is saved, it deletes this file. If the Scanner is started and it finds this file, it assumes a problem occurred and refills from it.

- Select the **Use separate offsite path for refilling** check box to specify a separate path to be used for locating the scan files for refilling, which is separate from the path used to store the new scan file.

If the **Use separate offsite path for refilling** check box is not checked, the refilling data is taken from the default save path for the correct platform specified in the **Saving** tab of the **Scanner Options** page (displayed by clicking the **Next** button).

If the **Use separate offsite path for refilling** check box is checked the refilling data is taken from the path specified here.

A UNC path can also be entered as the refill path. The format for the UNC path is:

```
\\Servername\ShareName\path\
```

For example:

```
\\EnterpriseDiscoveryServer\Inventory\Scans\
```

Setting up the Refilling Options 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 in this tab page:

Set the separate refilling path 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
```

You can also use the Scanner -r:<path> command line option to specify the location of this directory.

Important: Delta scanning will only work if the Scanner has been configured to collect Asset Data.

Locating an Offsite Scan File for Refilling

When the Scanner has determined that an offsite scan file is to be used for refilling, it needs to identify the file name of the scan file from which to refill. Because the offsite save path (or separate refill path) is likely to contain many scan files for different machines, the scan file is assumed to be named **AssetTag.fsf** or **AssetTag.xsf**.

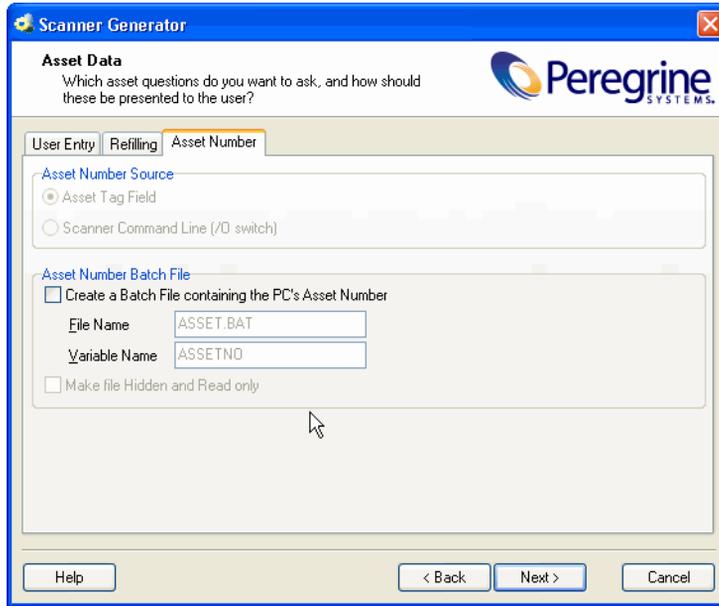
To determine the asset tag (and from that, the file names, the Scanner reads the scanner.ini file from the local save directory and extracts the value of the [AssetTag]= entry in the [options] section.

The Win32 Scanners in Enterprise mode store the asset tag in the agent options which is located in the registry. The Unix Scanners store the asset tag in the agent options file located in the agent directory (\$home/discagent).

- If neither of these are present, refilling from an offsite scan file fails.
- If multiple scan files are present
If both **Asset.fsf** and **Asset.xsf** exist, the newest one is used for refilling. However, if the time difference is less than a full day, the fsf is used.

The Asset Number Tab

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



The tab is divided into two groups:

- Asset Number Source
- Asset Number Batch File

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.

After a computer has been scanned, it is important to store the asset number in electronic form on the computer for future identification. This enables the asset number to be picked up automatically (without manual input) when follow-up scans are performed over the network, which crucially allows accurate asset tracking over a long period of time.

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 User Entry 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 questionnaire.

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 User Entry 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 questionnaire.
- **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 on the **Asset Number** tab page. 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
```

Asset Number Batch File Definition

The facilities provided by the Scanner Generator for defining the asset information collected, allow an asset number batch file to be automatically created. This batch file stores the asset number automatically in the root directory of drive C.

To ensure that the file is not accidentally removed from the system, the file can be set to be a hidden, read-only file.

The default name of this file is Asset.bat. It contains a single meaningful line:

```
SET ASSETNO=<Asset Number of PC>
```

Where ASSETNO is the environment variable.

The file created can be called from a script. When this is done, the ASSETNO environment variable contains as its value, the asset tag of the machine. This can be useful when performing asset management or support tasks on the machine, such as when opening a help desk ticket with Peregrine Get-Service.

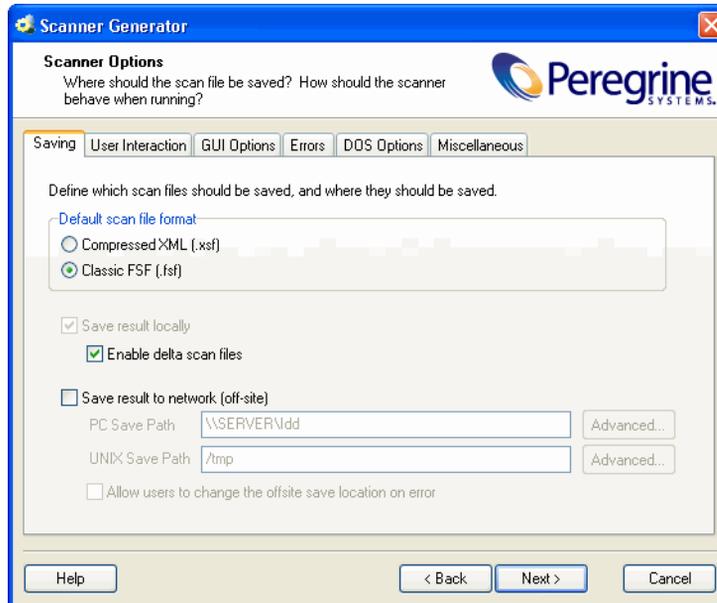
Creating an Asset Number Batch File

To create an asset number batch file:

- Select the **Create a Batch File containing the PC's Asset Number** option. Two further options are now enabled:
- **File Name:** To select a different name for the asset number batch file, enter a name in the File Name box (otherwise the default name Asset.bat is used). This file will run the SET ASSETNO command and will add the variable to the environment.
- **Variable Name:** The name of the environment variable used in the asset.bat file.
- Select the **Make file Hidden and Read only** option, to assign read-only and hidden file attributes to protect the asset number batch file.

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.



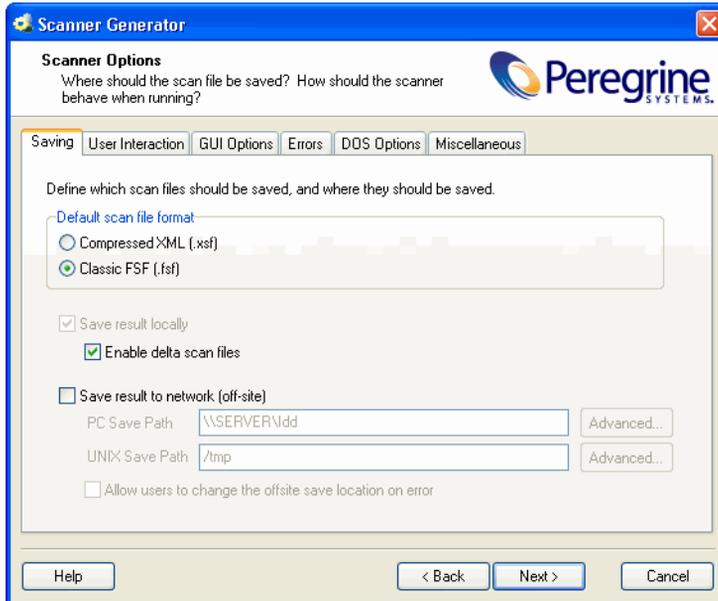
The **Scanner Options** page has six tabs:

- The Saving Tab
- The User Interaction Tab
- The GUI Options Tab
- The Errors Tab
- The DOS Options Tab
- The Miscellaneous 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.



Note: For Enterprise mode some of the options are pre-set to optimal values and cannot be changed.

Setting the Default Scan File Format

This setting determines the type of scan file produced.

- The compressed XML scan file format (.xsf) allows the scan data to be augmented with application recognition information. The uncompressed XML data can be read with XML tools.
- The FSF scan file format (.fsf) is a proprietary format that can be produced by all scanners. FSF scan files are more efficient than XSF files. Analysis tools can process them faster, resulting in shorter loading times.

Both scan file formats can be read by Viewer and Analysis Workbench. FSF scan files can be converted to XML using the FSF Converter or the XML Enricher (the XSF files will also be enriched with application data).

To set the default scan file format:

Select one of the following:

- Compressed XML (.xsf)
- Classic FSF (.fsf)

The default FSF file format is used unless the scan file must be readable before enrichment.

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\$.fsf** or **local\$.xsf**.

- **For 32-bit Windows Scanners**

The Win32 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
```

The local scan file can be used for refilling asset fields when the machine is next scanned.

- For DOS, Win16 and OS/2 Scanners
All partitions are searched and one is selected by the following process:
- The minimum space requirement starts off at 10Mb.
- The first acceptable FAT drive is selected.
- If one is not found, then the first acceptable HPFS or NTFS drive is selected.
- If one is not found, the selection will be repeated, after halving the minimum space requirement.
- If after this, there is still nothing suitable, the save drive is arbitrarily set to C:. After the save drive has been selected, the scan file is saved in the Infrtool directory.

For restricted users in Manual Deployment mode the location is:

User profile\Application Data\Peregrine\Enterprise Discovery

For UNIX the location is in the agent's data directory, which is

`$home/discagent`

Scan files saved using this option are saved with **Read Only** and **Hidden** file attributes.

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. By default Delta Scanning is enabled.

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.

Note: This feature is not supported by the DOS Scanner.

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.

Important: Delta scanning will only work if the Scanner has been configured to collect Asset Data.

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 separate refilling path 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 Use separate path for refilling setting on the **Asset Data|Refill tab** page to do this.

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.

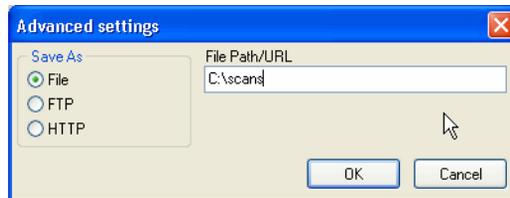
- Normal File Path
- UNC Path

- 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:

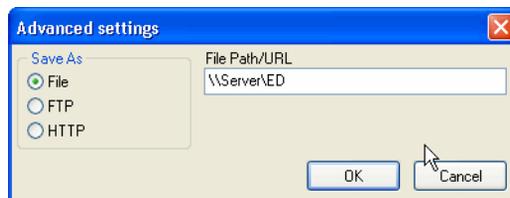
A:\Inventory\Scans

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:

```
ScanWin32 -p:C:\Scanners\
```

A UNC path can also be entered as the argument to this option. The format for the UNC path is:

```
\\servername\sharename\path\
```

For example:

```
ScanWin32 -p:\\EnterpriseDiscoveryServer\Enterprise  
Discovery\Scans\
```

If the save location specifies a UNC name (for example, `\\Accounts\Inventory`), the DOS and Win16 Scanners will try to map this to a mounted drive.

If there is no drive mapped to the specified UNC location, the scan file will not be saved. Again, the Win32 is the exception. In Win32, 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 machines, the UNIX save path is used instead, allowing UNIX-style syntax for specifying directories to be used. On UNIX, do not use drive letters, and the UNIX 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 Win32 and Unix Scanners can save to any FTP server.

To save to an FTP server:

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

- 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.

Important: When an FTP location is specified with the `-p` Scanner command line option (Win32 and Unix scanners only), the User Name and Password can be encoded into the URL as follows:

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

HTTP URL

The Win32 and Unix 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.

- 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.

Important: 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 webservers are set to enable Post and Get commands. You will need to ensure that if you are using http saving that the Put command is enabled in the directory.

The following is a quick description of what you would have to enable for http saving on both IIS and Apache.

Setup of Apache 2.0

If you are using basic authentication:

In the bin directory run:

```
htpasswd -c "<path>\htpass" Username
```

You will need to put the following in the .htaccess file of the directory that you intend to save in:

```
PUT_EnablePut On
PUT_EnableDelete Off
AuthType Basic
AuthName "Write" AuthUserFile "<path>\htpass"
Require user Username
```

Download the `mod_put.so` file and put it into the modules directory.

Enter the following into the httpd.conf file:

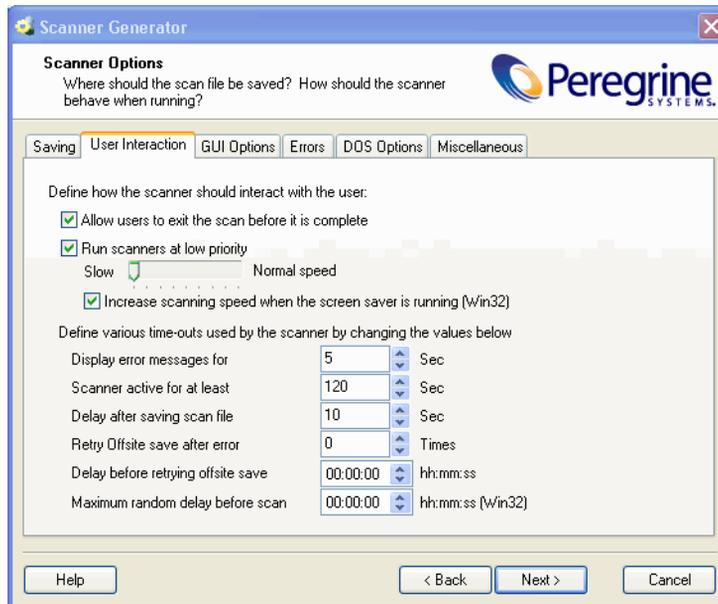
```
LoadModule put_module modules/mod_put.so
```

Setup for IIS

Check the option that allows writing to the desired save directory. Ensure that you have given write access to the Username and Password that you plan on adding to the Scanners http save path.

The User Interaction Tab

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



Setting User Interaction Options for the Scanner

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.

To set user interaction options for the Scanner, select from the following:

- **Allow users to exit the scan before it is complete**
Allows users to abort the scanning process (for any reason) by:
 - Pressing the Alt and X keys (DOS, Windows and OS/2 Scanners).
 - Selecting File -> Exit (DOS, Windows and OS/2 Scanners).
Select this check box for walkaround inventories, and clear it for a network inventory. If this option is cleared, the Scanner cannot be terminated prior to completing the scan.

- **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 (Win32)**
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, 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:

- **Display error messages for**
If an error occurs during the scan, the Scanner is delayed for the period specified. An error message is displayed. When the time specified has elapsed, the error message is cleared and the scan continues.

- **Scanner active for at least**

The Scanner is active for at least the number of seconds specified, to allow the entry of the asset details to be completed. Each time a key is pressed during entry of the asset data, the timer is reset to its original value.

This value is used as the starting value for a countdown timer, which is initialized at the start of the software scan. When this time elapses, the Scanner verifies that all required asset fields are filled in.

If the required asset fields are not completed, the user will be prompted for input and the timer is reset to its original value.

If completed, providing the software scan has finished, the Scanner will automatically save the result and exit.

- **Delay after saving scan file**

Causes the Scanner to delay for the number of seconds specified before exiting, after the scan is completed and the scan file has been saved.

- **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.

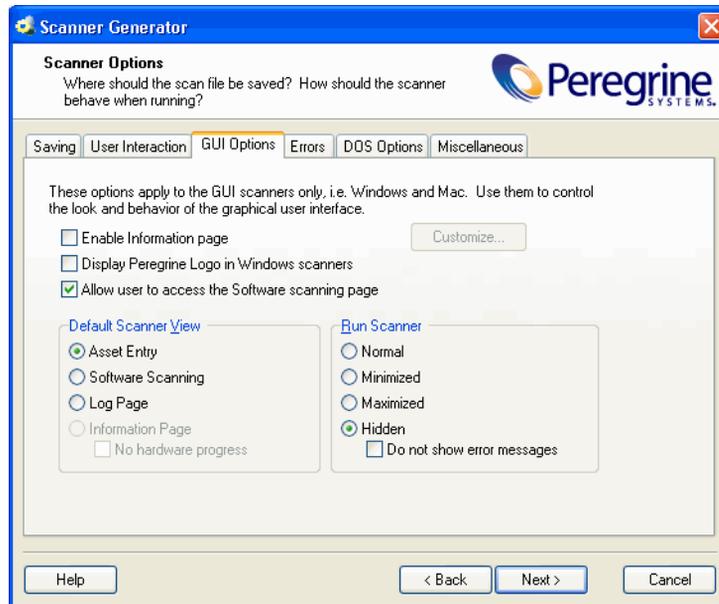
- **Maximum random delay before scan**

This setting is applicable to the Win32 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 GUI Options Tab

The **GUI Options** tab page is used to determine which pages (Software Scanning, Asset Entry, Information and Log) are visible to the user, the default page displayed when the Scanner is started and in which mode to run the Scanner (Normal, Minimized, Maximized or Hidden).



The page is divided into three sections:

- GUI Scanners
- Default Scanner View
- Run Scanner

Setting Scanner GUI Options

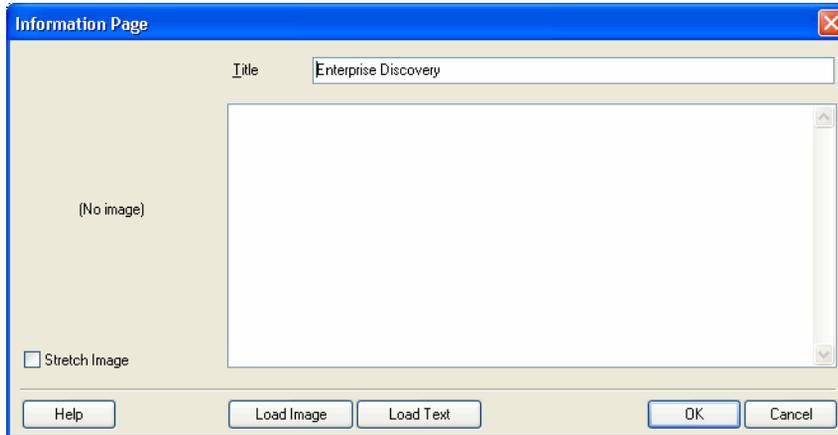
For those Scanners with a graphical user interface (Win16, Win32), various options can be set here.

To set Scanner GUI options, select from the following:

- **Enable Information Page**

Allows Windows-based Scanners to display an Information page. To do this:

After you have selected this option, click the **Customize...** button. The **Information Page** dialog box appears.



The **Information** page allows a user-defined bitmap and text to be displayed while the Scanners runs.

- In the **Title** box, type in the text that you want to appear as the heading of the **Information** page.
- Click the **Load Image** button to load a prepared bitmap file that you want to be displayed on the Information page. The largest allowed size of the bitmap file is 64 KB. The bitmap can be stretched by selecting the Stretch Image check box and sizing it using the splitter between the bitmap and text.
- Click the **Load Text** button to load a previously prepared text file or type in the text to be displayed directly into the memo box.
- Click the **OK** button to return to the **User Interface** tab page.
- **Display Peregrine Logo in Windows Scanners**
This option allows you to remove the Peregrine logo shown at the top of the Scanner page when it is running.

By default, the option is checked and the Peregrine logo is shown.

- **Allow user to access the Software Scanning page**

This controls viewing access to the Software pages. When this option is unchecked, the Software tab is not displayed and the Software page cannot be chosen from the Window menu.

Setting the Default View When the Scanner Is Run

This controls which page is displayed when the Scanner starts.

To set the default view when the Scanner is run:

- Select from the following options:

- **Asset Entry**

This can not be chosen if asset data is not collected.

- **Software Scanning**

This can not be chosen if the option to allow access to the Software Scanning page is unchecked.

- Log Page**

This option is always available.

- **Information Page**

This can only be selected if the Enable information page option was checked. You can also specify whether you want the hardware scanning progress to be displayed or not.

If the **No hardware progress** option is checked, the information page is shown even during hardware scanning. If **No hardware progress** is unchecked, the scanning progress window is shown during the hardware scanning stage. After the hardware scanning is finished, the Information page is shown.

Setting the Mode in Which the Scanner Is Run

To set the mode in which the Scanner is run:

- Select from the following options:
 - **Normal**

The Scanner runs like a normal application. The user can of course minimize the application if desired.
 - **Minimized**

The Scanner runs minimized and the user can restore the window if desired. If a required asset entry field is blank, the Scanner is restored and the user is prompted for an answer.
 - **Maximized**

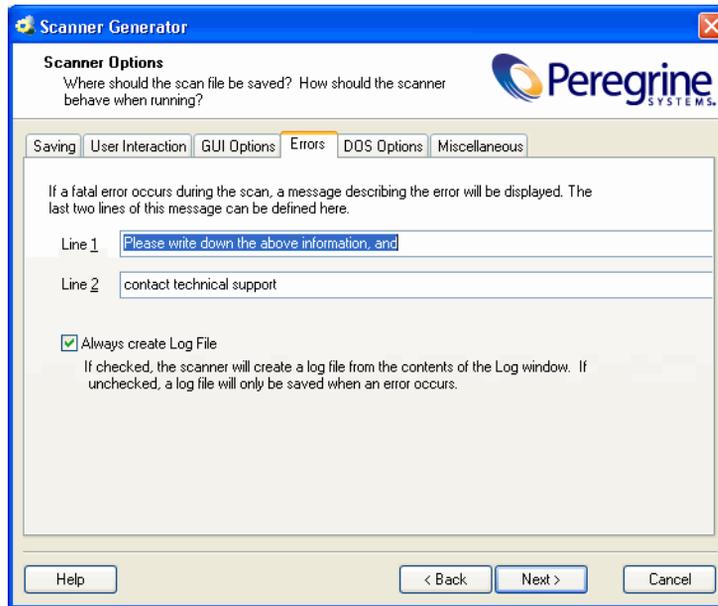
The Scanner runs maximized and the user can restore or resize the window if desired.
 - **Hidden**

Prevents the Scanner from showing up in the Task bar but otherwise works as **Minimized** mode. In Enterprise Mode the Scanner is Hidden but allows errors such as an unfilled asset questionnaire to be reported to the user.

You can also specify whether error messages are displayed to the user or not. If the **Do not show error messages** option is checked and the Scanner encounters an error, it will exit quietly. If this option is not checked, the Scanner will display the error to the user and if appropriate, ask the user to correct the error. For example, if a required asset field is empty, the Scanner will prompt the user to enter a value.

The Errors Tab

The **Errors** page is used to set up customized error messages in the event that an error causes the Scanner to stop running (sometimes called a fatal error).



Setting Up a Customized Error Message for the Scanner

Two additional error message lines can be set up and displayed.

To set up a customized error message for the Scanner:

- Type the two lines of text in boxes Line 1 and Line 2. Usually, Line 1 states what to do and Line 2 states who to contact.

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:

FSF014.fsf

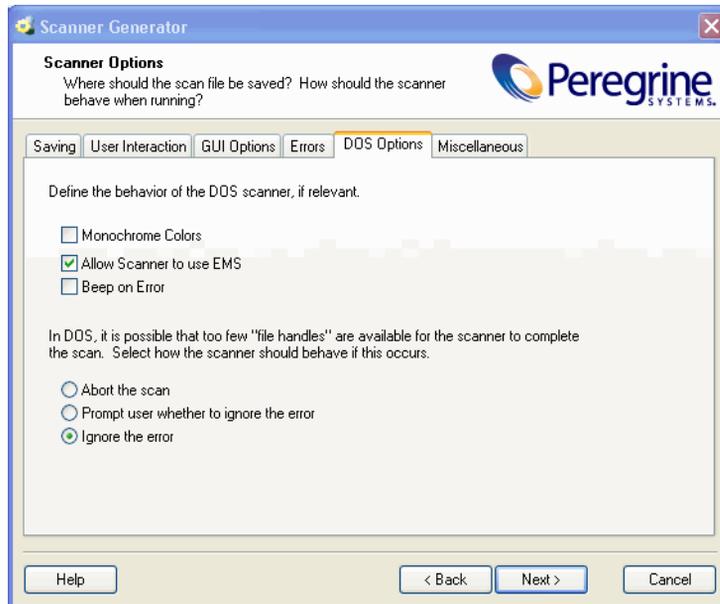
Then the log file generated will be called:

FSF014.log

Note: 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 DOS Options Tab

The **DOS Options** page is used to select options that control the behavior of the DOS Scanner as it scans each computer. If the DOS Scanner is not used, these options have no effect.



This tab page is divided into two sections:

- Behavior of DOS Scanner
- Behavior when too few File Handles available

Setting Up the Behavior of the DOS Scanner

These options are used to control the behavior of the DOS Scanner as it scans each computer. They include options for the screen display and how the program allocates extra memory (if required).

To set up the behavior of the DOS Scanner, select the options as required:

- **Monochrome Colors**
(DOS and OS/2 Scanners only) Specifies that the Scanner will run with monochrome (black and white only) screen display, instead of the default color display.
- **Allow Scanner to use EMS**
(DOS Scanners only) Allows the Scanner to use EMS memory for swap space. If this option is cleared, the Scanner uses hard disk space instead.

Note: Enabling this option will speed up the scanning process.

- **Beep on Error**
Causes the Scanner to beep when an error occurs

Setting Up the Behavior When Too Few File Handles Are Available in DOS

If too few file handles are available when the DOS Scanner is scanning a computer, an error results and the scan is stopped. When too few file handles are available, the Scanner is unable to open files when scanning and cannot complete. In this case the behavior of the Scanner can be controlled, so that the Config.sys file is modified to provide a suitable number of file handles when the computer is re-scanned.

To set up the behavior when too few File Handles are available in DOS, select one of the following options:

- **Abort audit**
This is the default option. The scan is stopped with an error message.
- **Prompt user whether to ignore error**
Displays an error message, and allows the scan to continue. In many cases, choosing to ignore will cause the Scanner to abort with a fatal error message as it tries to open files and is unable to do so.

- **Ignore the error**

The error is ignored and the scan is continued. However, the Scanner may abort with a fatal error message.

It is strongly recommended that the first option (Abort Audit) is used. Unpredictable results may occur when using either of the other two options.

The Miscellaneous Tab

The **Miscellaneous** tab allows you to:

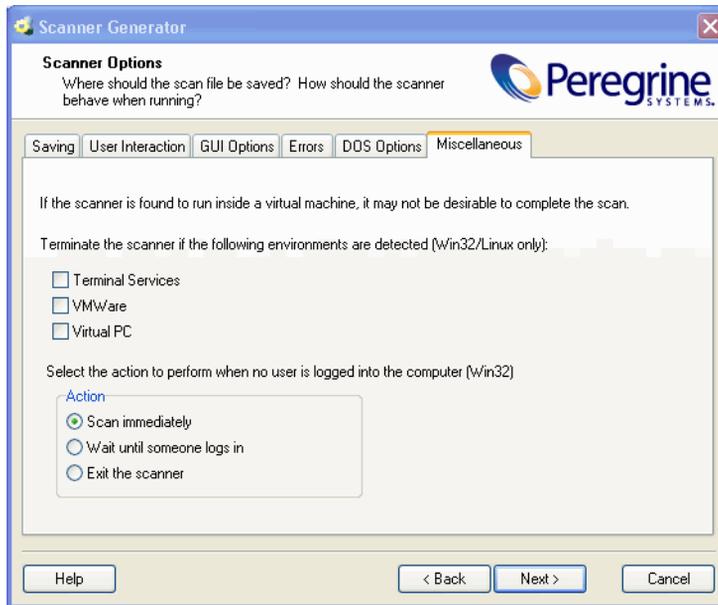
- Terminate the Scanners if running in a virtual machine
- Set the behavior when a user is not logged into a computer.

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.



Note: The settings for Virtual Machines are applicable to Linux and Win32 Scanners only.

- 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

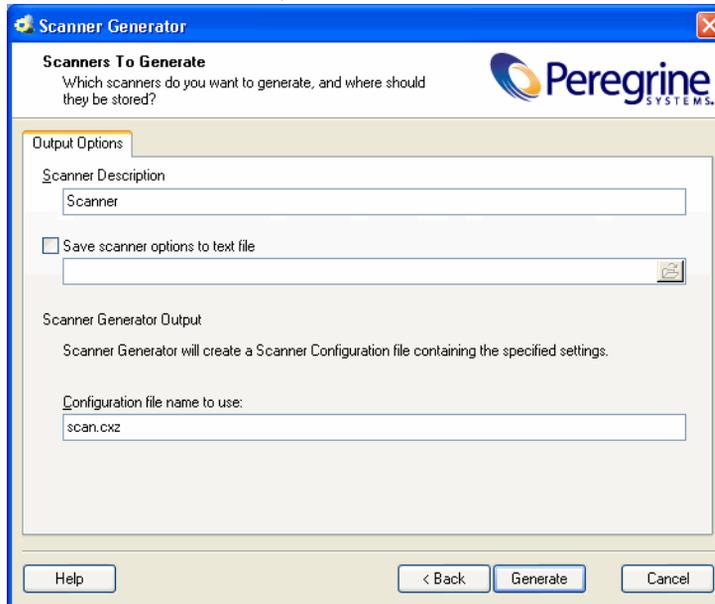
- Scan immediately
- Wait until some logs in
- Exit the Scanner

Note: In Manual Mode you may wish to set these actions to accommodate cases when the Scanner is launched by software distribution tools that can run it under the LocalSystem account.

The Scanners to Generate Page

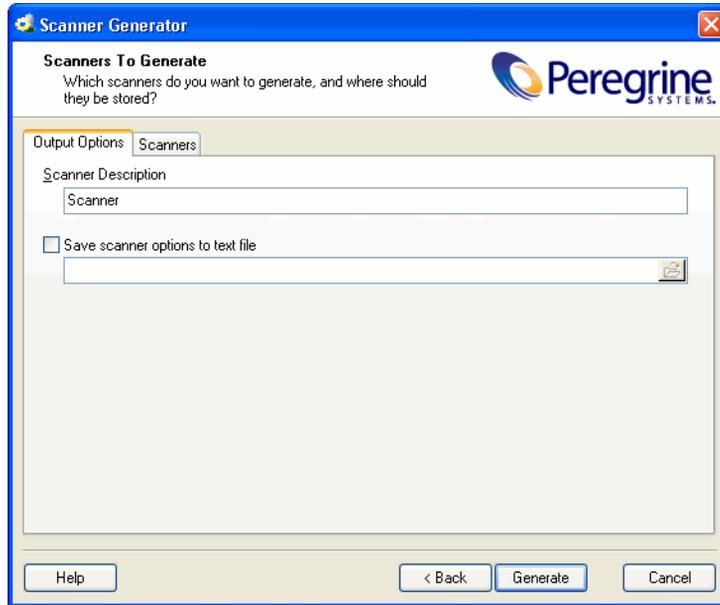
The **Scanners to Generate** page is used to specify which Scanners to generate and where they will be stored.

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



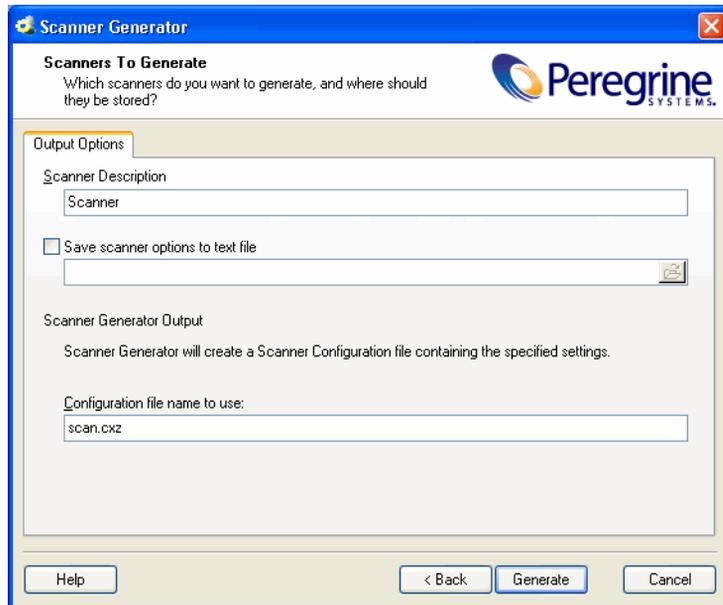
The screenshot shows a dialog box titled "Scanner Generator" with the Peregrine Systems logo. The main heading is "Scanners To Generate" with the subtext "Which scanners do you want to generate, and where should they be stored?". The "Output Options" tab is active, showing a "Scanner Description" field with the text "Scanner". There is an unchecked checkbox for "Save scanner options to text file" and a file selection button. Below this, it states "Scanner Generator Output" and "Scanner Generator will create a Scanner Configuration file containing the specified settings." A "Configuration file name to use:" field contains the text "scan.cxz". At the bottom, there are buttons for "Help", "< Back", "Generate", and "Cancel".

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



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 – August 18, 2005

The Scanner description is saved in the scan file 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 2.0 - 18 August 2005
General Options:
- Description : Scanner
- User can abort Scan
- INI file is used
- FSF is saved offsite
  > Save path is \\SERVER\Enterprise Discovery
  > FSF 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

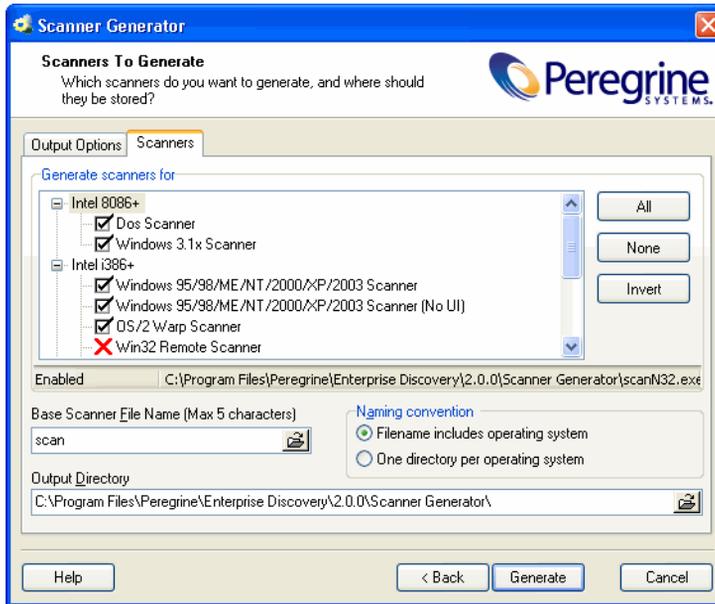
In Enterprise mode the configuration file is saved on the Enterprise Discovery Server as well, using the same file name as the copy specified in the Configuration file name to use field.

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. Scanners shown with a red cross X are invalid with the current set of options.

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.

Important: The Remote (Win32) option will generate the Win32 Remote Scanner. The Remote Scanner cannot be generated if any of the calculated fields are being used: Registry Extract, DMI Extract, WMI Extract, Environment Extract, File Extract.

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 (DOS, W16, OS/2 and so on).

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):

Scanner File Name	Scanner Type
scanDos.exe	DOS 16-bit
scanW16.exe	Windows 16-bit
scanW32.exe	Windows 32-bit
scanN32.exe	Windows 32-bit (no UI)
scanOs2.exe	OS/2 32-bit
scanR32.exe	Remote (Windows 32-bit)
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

- 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:

Scandos.exe

Scanw16.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\Peregrine\Enterprise  
Discovery\2.0.0\Dos\Scan.exe
```

```
C:\ Program files\Peregrine\Enterprise  
Discovery\2.0.0\W16\Scan.exe
```

```
C:\ Program files\Peregrine\Enterprise  
Discovery\2.0.0\W32\Scan.exe
```

```
C:\ Program files\Peregrine\Enterprise  
Discovery\2.0.0\N32\Scan.exe
```

```
C:\ Program files\Peregrine\Enterprise Discovery\2.0.0\Sp2\Scan
```

```
C:\ Program files\Peregrine\Enterprise Discovery\2.0.0\hpx\Scan
```

```
C:\ Program files\Peregrine\Enterprise Discovery\2.0.0\xaix\Scan
```

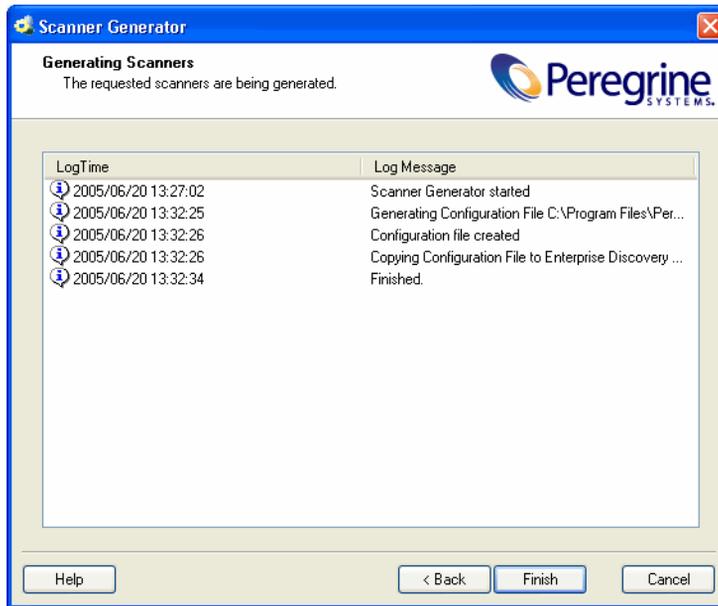
```
C:\ Program files\Peregrine\Enterprise Discovery\2.0.0\Irx\Scan
```

```
C:\ Program files\Peregrine\Enterprise  
Discovery\2.0.0\OS2\Scan.exe
```

- 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.

How Drive Letters and Volumes Are Assigned

This section outlines how Enterprise Discovery assigns and uses drive letters, what the volume list means and related topics.

In This Section....

- [Enumerating Physical Hard Disks and Partitions on page 217](#)
- [Processing Drives on page 218](#)
- [Scanning Specific Directories on page 219](#)

Enumerating Physical Hard Disks and Partitions

When performing the hardware scan, the Scanners attempt to enumerate physical hard disks in the machine and also enumerates partitions (or ‘volumes’) on those disks.

This enumeration may not succeed, or may only succeed partially, for several reasons. To access parts of this information, Administrator rights must be available for the Scanner - if it runs with normal user privilege, the hard disk cannot be accessed in low level (‘raw’) mode, which is what is used for low level scans and partition scans. However, even when in user mode, much information can be extracted from Windows and the Scanner relies on this information if the low level information is not available.

Additionally, when running in operating systems that support the notion of drive letters, the Scanner enumerates all drive letters available to determine which type they are, and attempts to match drive letters with actual partitions enumerated previously.

Finally, on operating systems supporting this, the Scanner enumerates all mount points (which is roughly equivalent to symbolic links for directories), which provides a list of virtual directories that are links to other directories or to partitions/volumes.

The result of the enumeration can consist of the following data, with some parts potentially missing due to access restrictions or operating system restrictions:

- List of valid drive letters
- List of physical disks
- List of partitions from low level scanning of partition tables
- List of volumes retrieved from operating system
- List of mount points

Processing Drives

The mechanism for assigning drive letters to hard disk partitions differs from operating system to operating system. For example, some operating systems support multiple primary FAT partitions simultaneously, whereas others only can 'see' one at a time. Some operating systems allow drive letters to be assigned dynamically according to the users' wishes, and others assign static drive letters that cannot be changed. Finally, some operating systems do not use drive letters at all.

With the data from the enumeration processes available, the Scanner attempts to determine the type of each drive letter. Drives that are SUBST'ed, point to network shares, RAM disks and so on are easily handled.

Drive letters that refer to hard disk partitions are then processed. The Scanner now attempts to match the three lists of partitions available (drive letters referring to disk drives, the low level scan partition list and the operating system partition list) to create a list of partitions containing the following key fields:

- Drive letter (if applicable)
- Partition type (for example FAT, NTFS)
- Read type (how the Scanner intends to read the partition)
- Physical hard disk reference (on which disk does the partition reside)
- Cylinder/Head/Sector offsets (indicating where on the disk the partition is)
- Total Size/Freespace

At the end of this process, it is possible that some hard disk partitions are still available, detected during the low level or operating systems enumeration but not assigned a drive letter by the operating systems. This can happen in several cases:

- The operating system does not support multiple primary partitions simultaneously. If multiple primary partitions are available on a single disk, the operating system will assign a drive letter to just one of them and cannot access any other ones.
- One or more partitions of an unsupported type exists. For example, FAT32, HPFS or NTFS partitions when in DOS, NTFS partitions in OS/2, Linux partitions outside Linux and so on.
- One or more partitions are not of a type that contains files, such as a Boot manager partition not known by the operating system but used solely for multi-boot systems.
- One or more partitions has not been assigned a drive letter by the user. This can happen in Windows NT/2000/XP/2003, which allow drive letters to be assigned and removed at will.

For any such partitions, the Scanner will assign a lower case drive letter in the range from a: to z:, unless the partition is accessible through one or more mount points or symbolic links. In this case, no lower case drive letter will be assigned to the partition.

Note: The lower case drive letters are different from the upper case variant (C: to Z:), which are used to signify a ‘real’ drive letter available to the operating system.

Scanning Specific Directories

When the Scanner is launched, it may be desirable to scan only a subset of the partitions/directories selected based on the Scanner Generator configuration. Provided this has not been allowed in the Scanner configuration, it can be done by simply specifying the directory paths or drive letters to scan on the command line, such as this:

```
ScanW32 C:\Windows D:
```

The drive letters specified are case-sensitive. As explained previously, the upper case drive letters match the corresponding operating system assigned drive

letters, while lower case drive letters are assigned by the Scanner to those partitions which the operating system cannot access.

To specify lower case drives for scanning, use a lower case letters followed by a colon (:) to specify these drives, for example:

ScanW32 c: a:



8 XML Enricher

CHAPTER

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, fsf or dsf format) in the Incoming directory.

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

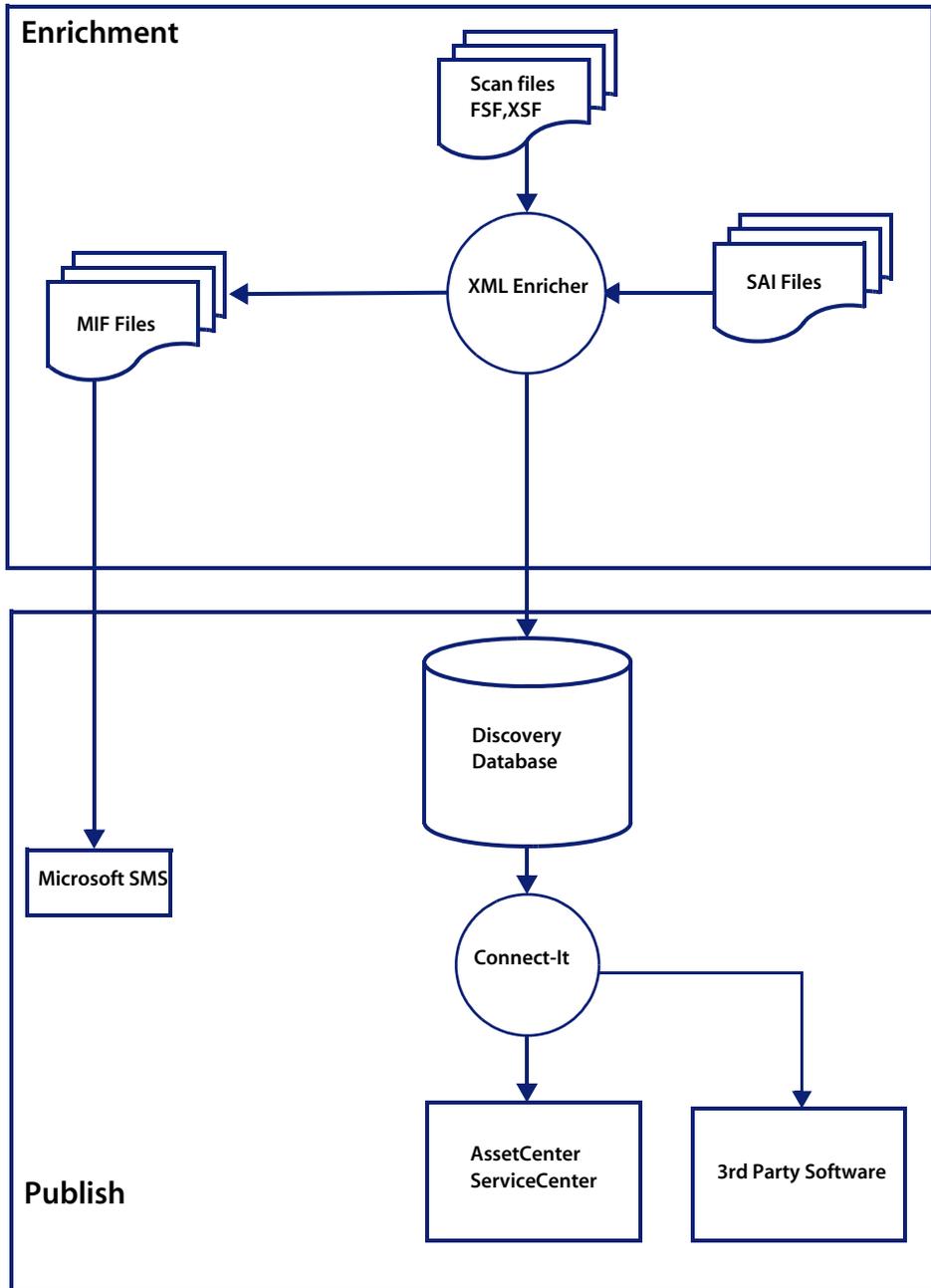
Information about recognized applications is added to the file data and a separate **<applicationdata>** section is added to the XML file.

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

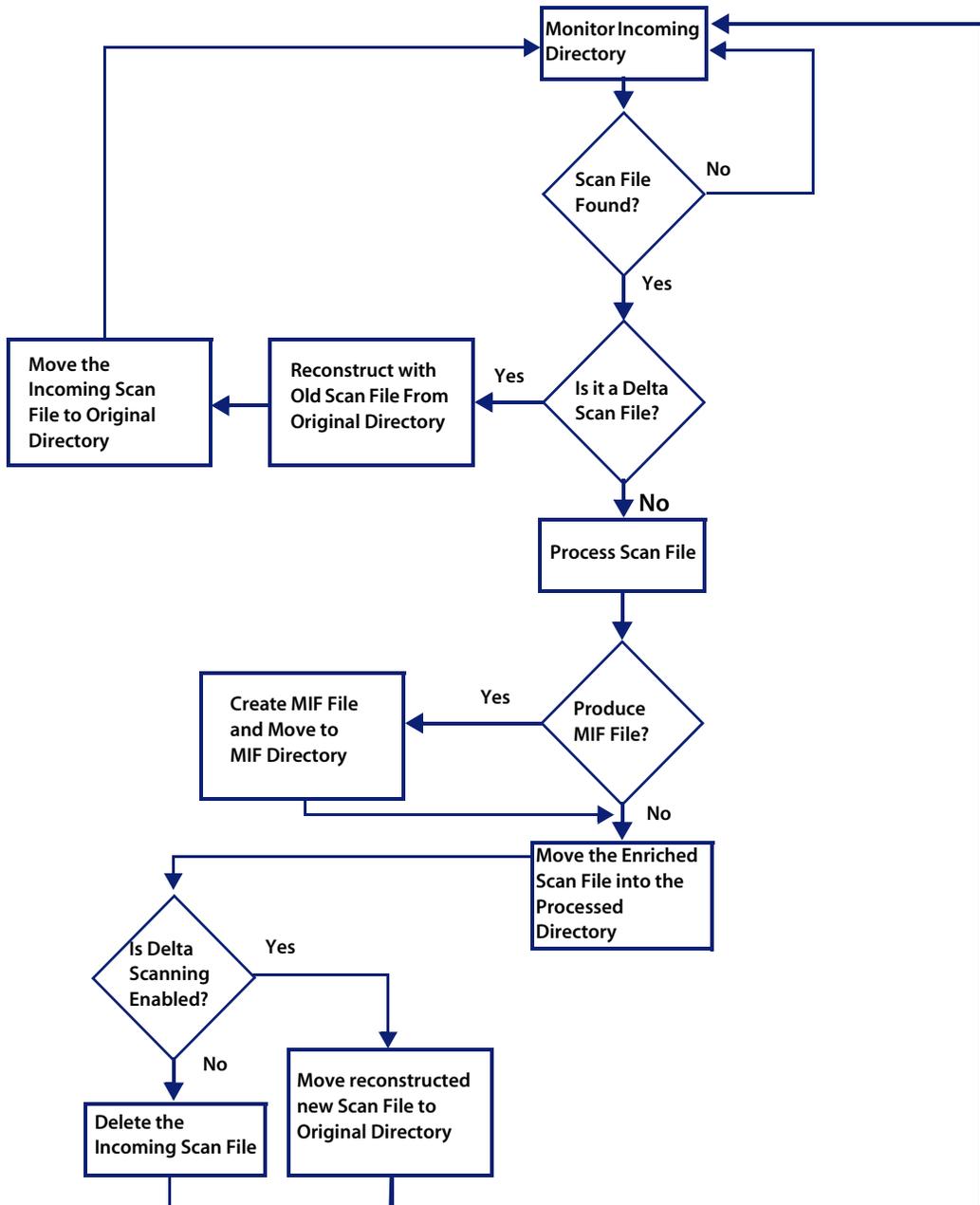
The Data Directory is customizable during the installation process.

The following table shows the various directories that are 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.

Directory	Explanation
\Scans\Deferred\Firstscan	<p>If the Automatically defer all new scans option was set, the scan file is not processed. See Configuring the XML Enricher Using XML Enricher.ini on page 238.</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>
\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]	<p>You can group the scan files based on Hardware fields. This is user-defined. Define the setting on the following web UI page: Administration>System Preferences>Scan file management. See Group Processed Scan Files on page 237.</p>
\Scans\Temp	This is where the XML Enricher stores its temporary files.

The following flowchart shows how the enrichment process works for normal (FSF and XSF) and delta (DSF) scan files.



Processing Normal Scan Files

At the end of the process, a new enriched scan file in **.xsf** format 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.

Important: If an enriched scan file for the same asset 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 in **.xsf** format 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.

Important: Delta scanning in Manual Deployment mode will only work if the Scanner has been configured to collect Asset Data.

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\Peregrine\Enterprise Discovery\2.0.0\Scanner  
Generator
```

The convention for using this command line utility is as follows:

```
FSFDelta OldFile NewFile DeltaFile
```

Where:

- **[FSFDelta]** is the command
- **[OldFile]** is the name and path to the old scan file - Enter the full scan file name (for example Test.fsf or Test.xsf)
- **[NewFile]** is the name and path to the latest scan file - Enter the full scan file name (for example Latest.fsf or 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.

Note: If you have all three of these files contained in the same directory as the FSFDelta utility, then you do not have to specify the full path to these files.

To create a delta scan file, run FSFDelta specifying the two input scan file names and the name of the output delta scan file. FSFDelta 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 FSFDelta with the `-d` command line switch, specifying the input OldFile name and DeltaFile names and the output NewFile name.

FSFDelta will apply the differences in DeltaFile to OldFile to reconstruct the new version of the scan file in NewFile.

Application Utilization Data

An agent software utilization plug-in 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
- AutoSequence Number

To configure the XML Enricher:

- 1 Click **Administration > System Preferences > 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 border="1"> <thead> <tr> <th>Choose From</th> <th>Action</th> <th>Selected</th> </tr> </thead> <tbody> <tr> <td><input type="text"/></td> <td><input type="button" value="Add>>"/></td> <td> BIOS asset tag BIOS serial number NetBIOS name and Windows domain MAC Address Asset tag Scan filename </td> </tr> <tr> <td></td> <td><input type="button" value="<<Remove"/></td> <td></td> </tr> </tbody> </table>	Choose From	Action	Selected	<input type="text"/>	<input type="button" value="Add>>"/>	BIOS asset tag BIOS serial number NetBIOS name and Windows domain MAC Address Asset tag Scan filename		<input type="button" value="<<Remove"/>
Choose From	Action	Selected								
<input type="text"/>	<input type="button" value="Add>>"/>	BIOS asset tag BIOS serial number NetBIOS name and Windows domain MAC Address Asset tag Scan filename								
	<input type="button" value="<<Remove"/>									

Process utilization data

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

Note: 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.

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.

Note: 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).

Note: 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.

Note: 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 Preferences > 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"/>

Managing Scan Files

You can configure the following options to control scan file management:

- Delete Orphaned Scan Files
- Group Processed Scan Files

<u>Delete orphaned scan files:</u>	<input checked="" type="radio"/> Default: Always <input type="radio"/> Custom: <ul style="list-style-type: none"> <input checked="" type="radio"/> Always <input type="radio"/> On purge <input type="radio"/> Never
Group Processed Scan Files	
<u>Group processed scan files by primary:</u>	<input checked="" type="radio"/> Default: <input type="text"/> <input type="radio"/> Custom: <input type="text"/>
<u>Group processed scan files primary blank:</u>	<input checked="" type="radio"/> Default: unknown <input type="radio"/> Custom: <input type="text"/>
<u>Group processed scan files by secondary:</u>	<input checked="" type="radio"/> Default: <input type="text"/> <input type="radio"/> Custom: <input type="text"/>
<u>Group processed scan files secondary blank:</u>	<input checked="" type="radio"/> Default: unknown <input type="radio"/> Custom: <input type="text"/>
<u>Group processed scan files by tertiary:</u>	<input checked="" type="radio"/> Default: <input type="text"/> <input type="radio"/> Custom: <input type="text"/>
<u>Group processed scan files tertiary blank:</u>	<input checked="" type="radio"/> Default: unknown <input type="radio"/> Custom: <input type="text"/>

To configure scan file management:

- 1 Click **Administration > System Preferences > 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. It is a zip file. This gets dropped into the C:\Program Files\Peregrine\Enterprise Discovery\2.0.0\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\Peregrine\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

```

Option	Explanation
cfgAutoidentifyDeviceDriverFiles 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.
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.
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).

Option	Explanation
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	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.\$\$\$. 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'. These files are not passed to the recognition engine and will be marked as junk

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
```

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 (SAI) 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 Peregrine\Enterprise Discovery\2.0.0\Common directory for SAI files and uses the appropriate SAI files in this directory for recognition.

It searches for Master.SAI and User.SAI:

- If the locale is France, it adds French.SAI.
- If the locale is Germany, it adds German.SAI.

Note: The XML enricher can only load SAIs from non-network locations.

Here is an example of this section:

```
[RecognitionConfig.RecognitionConfig_cfgSAIFiles]
Count=2

Item0=C:\Program Files\Peregrine\Enterprise
Discovery\2.0.0\Common\User.sai

Item1=C:\Program Files\Peregrine\Enterprise
Discovery\2.0.0\Common\Master.sai
```

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.

Note: 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'.

Important: 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 Preferences > 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\Peregrine\Enterprise Discovery\2.0.0\Common

Note: 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)"
fsfmajorver="7" fsfminorver="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@peregrine.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\Peregrine\Desktop
      Inventory\8.0.0\Common\User.sai" desc="User SAI File"
date="14/04/2004"
  type="Editable"/>
    <sai name="C:\Program Files\Peregrine\Desktop
      Inventory\8.0.0\Common\Master.sai" 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.driv
[mci]
</contents>
  </storedfile>
</storedfiles>
</inventory>

```




9 Getting Your Data into AssetCenter

CHAPTER

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.

Important: 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 2.0.1
 - Connect-It version 3.5
 - 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\Peregrine\ConnectIt\scenario\ed\ed2ac44

Note: An Enterprise Discovery to ServiceCenter scenario is also provided in the C:\Program Files\Peregrine\ConnectIt\scenario\ed\ed2sc60 directory

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:

Step 1 Open the scenario

Step 2 Configure the Source Connector - Enterprise Discovery

Step 3 Configure the Destination Connector - AssetCenter

Step1: 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\Peregrine\ConnectIt\scenario\ed\ed2ac44

A three box scenario diagram is now shown.



Note: 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.

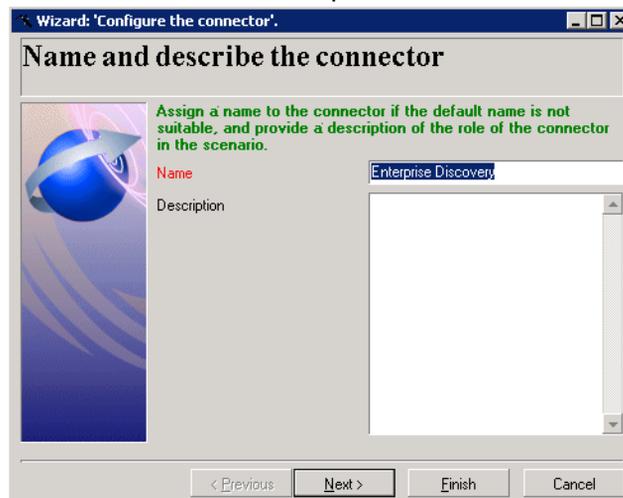
To configure the connector you can either:

- 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.

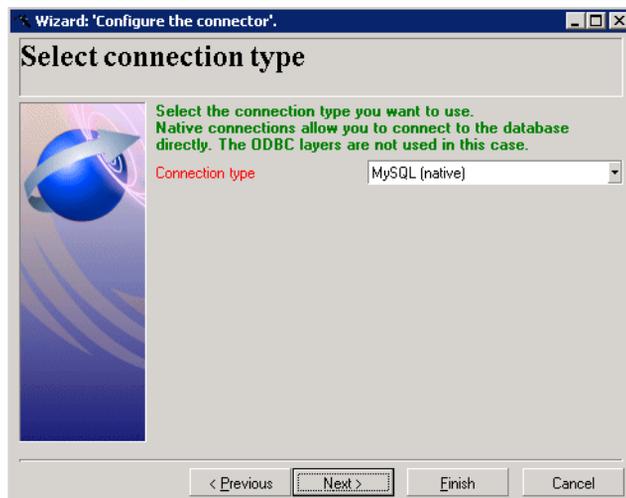


- 1 **Name:** By default, the value of this field is Enterprise Discovery.

- Description:** Enter text to describe the connector. This field is not mandatory.
- 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.

Wizard: "Configure the connector".

Configure the database server connection.

Configure the database server connection.
The default MySQL port is 3306. If your server uses a different port, specify 'server.port' in the 'Server' field.

Server: :8108
Login: admin
Password: *****
Database: Aggregate

Test the connection

Test

< Previous Next > Finish Cancel

1 Server

Enter the port used for the database server connection.

If the ConnectIt installation is on a different computer to the Enterprise Discovery Server, enter the DNS name or IP address of the ED 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 or writing data). You can enable this in the Enterprise Discovery Web UI.

Administration>Account Administration

3 Password

Enter the password associated with the user login.

4 Click the **Test** button to test the connection to the Discovery database.

5 Click **Finish**

Step 3: Configure the Destination Connector - AssetCenter

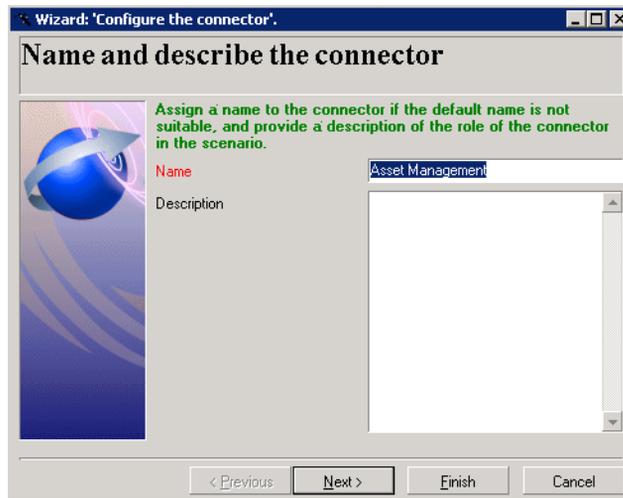
Click on the title bar of the Asset Management connector to highlight it. To configure the connector you can either:

- Right-click on the connector title bar and select the **Configure Connector...** option.
- Select the **Configure** option from the **Tools** menu.
- Press the **F2** key on your keyboard.

A wizard for the configuration of the Asset Management connector is displayed.

Page 1: Name and describe the connector

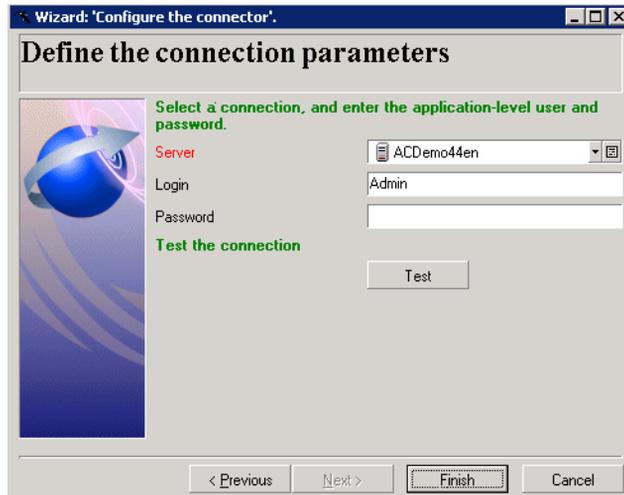
The first page of the wizard enables you to name the Asset Management connector and provide a description for it.



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

Page 2: Define the connection parameters

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



1 Server

In the drop-down list, select the AssetCenter connection that you can access from your computer.

2 Login

Enter the login required to interact with AssetCenter.

The profile of this login must allow you to execute the actions performed by your scenario (reading or writing data).

3 Password

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

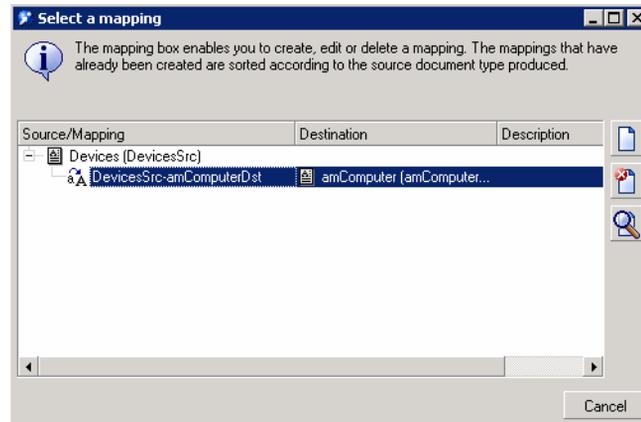
4 Now test the connection to the database.

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.

Note: 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.

- 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 whether:

- 1 The Enterprise Discovery connector correctly produced the documents.
- 2 The mapping box correctly transformed these documents.
- 3 The Asset Management connector correctly consumed these documents after the mapping box transformed them.

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

This step is where you actually populate your AssetCenter database with the data from Enterprise Discovery.

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.

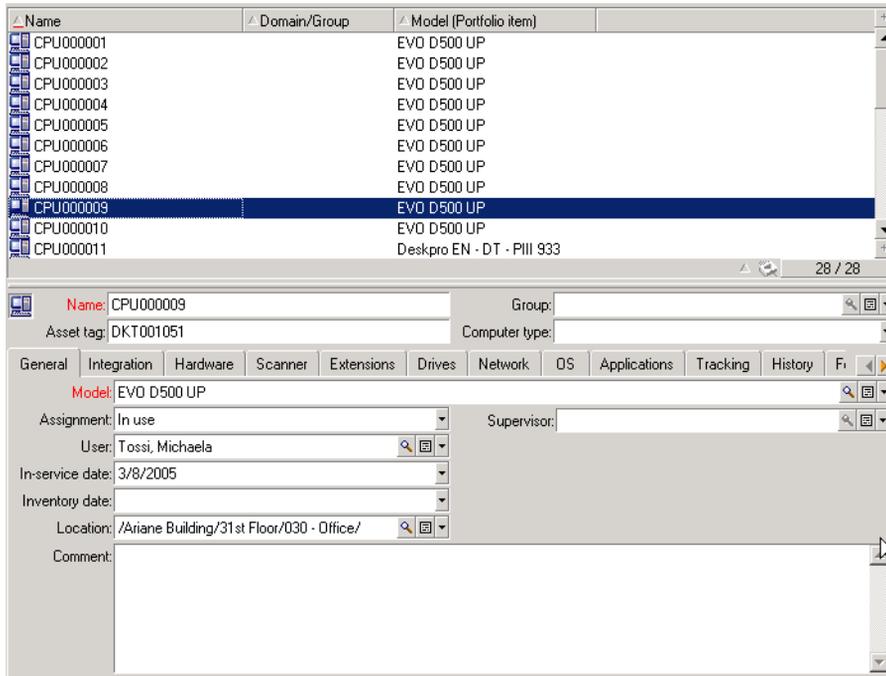
Right click anywhere in this log pane and select Collapse all levels. Now you are left with the basic actions that were carried out. Expand an action to see what happened in further detail.

See the results in AssetCenter

Note: If you have configured the Enterprise Discovery connector to use learning mode, then no data would have been populated.

- 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.



Index

A

account

- adding an account 21
- changing name 23
- changing the type 23
- customizing a profile 23
- deleting 27
- listing user accounts 21
- modifying password 26
- modifying properties 31
- password
 - minimum length 28
- setting type 24
- types
 - admin 20
 - demo 19
 - IT employee 19
 - IT manager 19
 - Scanner 20

account properties

- account type 24
- append IP address 23
- default device panel 23
- default port panel 23
- help format 23
- long date format 23
- make URLs visible 23
- name 23
- short date format 23

ACSKeyStore.bin 54

acstrust.cert 55

activating devices 46

Adding

- directories and files to the override file 112
- file filter storage criteria in SG 124

adding a new device 36

admin account

- description 20

Administration

- account password, modifying 26
- account properties 31
- adding an account 21
- customizing a user profile 23
- deleting an account 27
- device deactivation intervals 41
- expiry controls 41
- listing user accounts 21
- modify password 31
- test e-mail address 32

Agent

deployment

- automatic 60
- configuring 69
- custom 59
- manual 61
- via listener 57
- via login scripts 61
- via Win32 RPC 58

directories 56

media files 55

security 54

- uninstalling
 - agent 64
- upgrade
 - unix agent 63
 - win 32 agent 62
- versions 71
- agentca.pem 55
- AIX Scanner
 - setting up
 - file name and output directory 213
 - os-scanner fields for unix 171
 - supported platforms 84
- Allow command line override option 104
- Apache
 - setup for saving to 193
- application library 237
- Asset data recovery mode 180
- Asset fields
 - configuring in SG 142
- Asset number
 - choosing a source for 183
- Asset number batch file 184
 - creating 184
- Asset questionnaire 139
 - layout for user entry 140
- Asset tag field 143
- Assistant window 23
- ATAPI
 - disabling hardware detection routine 99
- automatically defer all new scans 234
- B**
- BIOS
 - disabling hardware detection routine 99
- Bus Detection
 - disabling hardware detection routine 99
- C**
- Calculated fields
 - in SG 148
- CD-ROM drives
 - creating a customized drive selection 109
- Changing
 - directories scanned to locate files 133
- Classic local drive scan 102
- Combination fields
 - setting up in SG 173
- Combined scan 102
- Command line
 - offsite scan file name 183
 - offsite scan file save location 189
 - override option in scanner generator 104
 - scanning specific directories 219
 - specifying refill order in scanner generator 179
- Compaq Asset Tag
 - disabling hardware detection routine 99
- Compressed Drives
 - creating a customized drive selection 110
- Concurrent session
 - Configuring
 - agent deployment
 - concurrent sessions 70
- Configuring
 - agent communication 67
 - agent deployment
 - command for custom deployment 69
 - device types 70
 - method 69
 - reserved sessions 71
 - retry interval 70
 - agent versions 71
- CPU identification
 - disabling hardware detection routine 99
- Custom deployment of agent 69
- customizing your account 31
- D**
- d command line switch 227
- date format, change 23
- DCC data
 - disabling hardware detection routine 99
- deactivate 40
- deactivate device 44
- deactivation intervals 41
- Default view
 - for scanners 199
- deferred directory
 - firstscan 234
- Delta calculation utility 227

- Delta scanning
 - command line utility 227
 - delta scan files 226
 - enabling delta scanning 188
 - setting up the scanners to handle them 227
 - specifying refill options 180
- demo account, description 19
- Deployment method 69
- Derived fields
 - in SG 149
- Description field 143
- device
 - activating 46
 - adding 36
 - changing IP address 39
 - changing ports 39
 - deactivate 44
 - deactivating 42
 - hide 43
 - purge 44
 - purging 42
 - remove automatically 40
 - removing 42
 - replacing 38
- Device driven drives
 - creating a customized drive selection 110
 - selecting a pre-defined type of drive to scan 106
- Device Manager
 - changing default panel 23
- device priority
 - changing 49
- device tag
 - changing 49
- device title
 - changing 49
- Device types 70
- discusg.cxu 66
- Disk space
 - compression on netware servers 119
 - xml enricher 223
- DMI
 - disabling hardware detection routine 99
 - setting up extract fields in SG 160
- DOS Scanner
 - allocating memory to 203
 - supported platforms 84
 - too few file handles 204
- Drives
 - creating a customized drives selection 108
 - disabling hardware detection routine 99
 - how the scanners process drives 218
 - selecting a pre-defined type of drive to scan 106
- DSF file
 - definition 81
- E**
- ED Server
 - connecting to in SG 90
- EISA
 - disabling hardware detection routine 99
- e-mail
 - test your e-mail address 32
- Enhanced CPU ID
 - disabling hardware detection routine 99
- Enterprise mode 89
- Environment fields
 - setting up in SG 156
- Errors
 - customizing messages for Scanners 201
- Exiting
 - scanner generator 85
- expiry 40, 41
- Extract field options
 - setting in SG 174
- F**
- FAT
 - creating a customized drive 108
 - creating a customized drive selection 109
- Field data type
 - selecting 146
- Field parameters
 - setting in SG 151
- File associations
 - including in targeted scan 115
- firstscan directory 234

- Floppy drives
 - creating a customized drive selection 109
 - selecting a pre-defined type of drive to scan 106
- Forensic scan 93
 - selecting as preset scanner configuration 90
- Formatted strings
 - setting up in SG 153
- French SAI
 - application recognition in the xml enricher 240, 241
- FSF
 - definition 80
 - setting as default scan file format 186
- FSFDelta.exe 227
- FTP URL
 - for offsite save path 192
- G**
- Generating scanners 212
- German SAI
 - application recognition in the xml enricher 240, 241
- H**
- Hardware data
 - disabling hardware detection routine 97
 - selecting as data to be collected by scanner 95
 - structure in an xsf file 244
- Hardware detection
 - disabling 98
- help format 23
 - change 23
- help, Assistant window 23
- hiding devices 43
- HPFS
 - creating a customized drive selection 108, 109
- HP-UX Scanner
 - setting up file name and output directory 213
 - supported platforms 84
- HTTP URL
 - for offsite save path 192
 - saving on Apache and IIS Web Servers 193
- I**
- I/O ports
 - disabling hardware detection routine 99
- Icons
 - files to scan list box in scanner generator 118
- icons
 - changing 49
- IDE
 - disabling hardware detection routine 99
- IIS
 - setup for saving to 193
- Information page 197
- Inventory scan 93
 - selecting as preset scanner configuration 90
- IP address
 - append to device labels 23
 - changing in a device 39
- IPX/SPX
 - disabling hardware detection routine 99
- ISA PnP cards
 - disabling hardware detection routine 99
- IT employee account, description 19
- IT manager account, description 19
- J**
- Java class files
 - enabling in SG 91, 94
- Java Home directory
 - including in targeted scan 115
- K**
- Keyboard
 - disabling hardware detection routine 99
- keyboard shortcuts
 - scanner generator user entry form 140
- L**
- Language options
 - setting in xmlenricher 238

- Licence
 - default directory used in xml enricher 223
 - using targeted directory scan for software licence accuracy 103
- Line Manager
 - default panel
 - changing 23
- Linux Scanner
 - setting up file name and output directory 213
 - supported platforms 84
- Listener
 - agent deployment 57
 - uninstalling 65
- LiveAgent 56
- Local scan file
 - refilling from 178
 - saving 187
- local\$ file 187
- Locating
 - offsite scan file for refilling 181
- login
 - enabling 23
- Login scripts
 - agent deployment 61
- Logs
 - creating in scanner generator 201
 - log window in scanner generator 216
 - xml enricher 229
- long date format 23
- M**
- Manual deployment
 - agent 61
- Manual deployment mode 90
 - setting up to handle delta scan files 180
- map configuration
 - copy permissions 23
- Master SAI
 - application recognition in the xml enricher 240, 241
- MCA
 - disabling hardware detection routine 99
- media files 55
- Memory
 - disabling hardware detection routine 99
- MIF files 224
- Mouse
 - disabling hardware detection routine 99
- N**
- name of account 23
- NetBIOS/NETBEUI
 - disabling hardware detection routine 99
- Netware servers
 - disk space compression 119
- Network
 - saving scan results to 189
- Network drives
 - creating a customized drive selection 110
 - selecting a pre-defined type of drive to scan 106
- Network information
 - disabling hardware detection routine 99
- Network inventory
 - disabling the ability for users to abort scan 194
- Network Map
 - change icon 49
- NMID 59
- No UI Scanner
 - setting up file name and output directory 213
- NTFS
 - creating a customized drive selection 108, 109
 - how the scanners process drives 218
- Numeric field
 - definition 148
 - setting up in SG 155
- O**
- Office plug-in 135
- Offsite scan file
 - locating 181
 - refilling from 178
 - saving 187

- OS/2 Scanner
 - setting up file name and output directory 213
 - supported platforms 84
- OS/scan fields
 - setting up in SG 168
- Override option 104

P

- password
 - account, modifying 26
 - minimum length 28
 - modify 31
- PC Scanners
 - supported platforms 84
- Peripherals
 - disabling hardware detection routine 99
- Pick list fields
 - setting up in SG 152
- platforms 84
- Plug'n'Play
 - disabling hardware detection routine 99
- Plug-ins
 - creating customized 138
 - enabling or disabling in scanner generator 136
 - plug-ins provided 135
 - removing plug-in in scanner generator 138
 - setting advanced options in scanner generator 136
 - setting properties in scanner generator 137
 - setting up in SG 134
- Port Manager
 - changing default panel 23
 - default panel
 - changing 23
- priority
 - device 49
- Processing drives 218
- purge 40

R

- Rawmedia 55
- Refilling
 - how it works 177
 - local scan file 178
 - offsite scan file 178
 - specifying options for 180
 - specifying options for delta scans 180
 - specifying the order 179
- Registry extract fields
 - setting up in SG 159
- Remote scan 93
 - selecting as preset scanner configuration 90
- Remote Scanner 89
 - setting up file name and output directory 213
 - supported platforms 84
- removing a device
 - automatically 40
 - manually 42
- replacing a device 38
- Required fields 150
- Reserved sessions 71
- Retry interval 70

S

- Saving
 - scan results
 - locally 187
 - to network 189
 - scanner options to text file 210
- Scan file
 - setting default scan file format for saving 186
- Scanner
 - components 81
 - compression 82
 - customizing error messages 201
 - disabling hardware detection routines 98
 - enabling scanning of java class files 94
 - exit options 194
 - GUI options 197
 - saving options to text files 210
 - selecting directories to scan 114
 - selecting hardware data to collect 95
 - selecting type of scanner to create 92

- selecting which to generate 212
 - setting default view when scanner is run 199
 - setting naming conventions 214
 - setting up descriptions 209
 - setting up information page 197
 - software scanning modes 102
 - time-out options 195
 - Scanner account, description 20
 - Scanner configuration file
 - reading setting from 91
 - Scanner generator
 - enterprise mode 89
 - manual deployment mode 90
 - starting 85
 - SCSI
 - disabling hardware detection routine 99
 - Security
 - agent
 - Certificates
 - agent 54
 - selection 108
 - Sequence fields
 - setting up in SG 167
 - Settings.txt 210
 - Shallow scan 93
 - selecting as preset scanner configuration 90
 - short date format 23
 - SMBIOS
 - disabling hardware detection routine 99
 - Software scanning modes 102
 - Software utilization plug-in 66
 - Solaris Scanner
 - setting up file name and output directory 213
 - supported platforms 84
 - Standard fields 143
 - Starting
 - scanner generator 85
 - status
 - receive reports by e-mail 23
 - Stored files
 - setting up in SG 130
 - SUBST'ed drives
 - creating a customized drive selection 110
- T**
- Targeted directory scan 102
 - Text fields
 - in SG 147
 - Text file
 - saving scanner options to 210
 - Text file extract
 - setting up field in SG 156
 - type of account
 - setting 24
 - Type/pick list fields
 - setting up in SG 153
- U**
- UNC path
 - for offsite save path 190
 - Uninstalling
 - agent 64
 - Unix Scanners
 - supported platforms 84
 - Upgrading
 - unix agent 63
 - win 32 agent 62
 - URL
 - make visible 23
 - user accounts, listing 21
 - User prompt
 - setting up in SG 146
 - utilization plug-in 66
- V**
- Version
 - agent 71
 - Version data plug-in 135
 - VFAT
 - creating a customized drive selection 109, 110
 - Virtual machines 205
- W**
- Welcome page 89
 - Win 32 RPC
 - agent deployment 58

- Windows 16-bit Scanner
 - setting up
 - file name and output directory 213
 - OS-Scan fields for 169
 - supported 84
- Windows 32-bit Scanner
 - setting up file name and output directory 213
 - supported platforms 84
- Windows services
 - including in targeted scan 115
- WMI extract fields
 - setting up in SG 164

X

- XML Enricher
 - application library 237
- XML enricher
 - directory structure used 223
 - disk space requirement 223
 - log files 229
 - structure of the xml file 244
- XSF
 - contents of 245
 - creating 226
 - definition 80
 - enriching with xml enricher 221
 - setting as default scan file format 186

