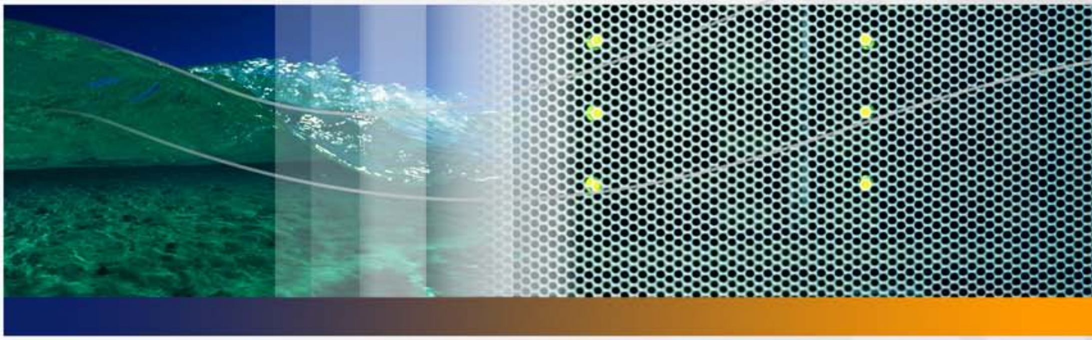
Product Documentation

Peregrine Systems, Inc.

Network Discovery® 5.2.3



Using Network Discovery with Desktop Inventory and Desktop Administration

Part No. DPND-523-EN08

Peregrine SYSTEMS.

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, contact Peregrine Systems, Inc. Technical Publications by email at doc_comments@peregrine.com. This edition of the document applies to version 5.2.3 of the licensed program.

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

PEREGRINE

Contents

1 CHAPTER Introduction

The following three Peregrine products can be configured to work together:

- Network Discovery
- Desktop Inventory
- Desktop Administration

Desktop Inventory collects and maintains an up-to-date view of all computers in your organization. The product is able to support all inventory management projects, from the smallest operational requirement, through to the tactical inventory and the enterprise level strategic solution.

When used with Network Discovery, the process of maintaining an up-to-date IT asset inventory can be automated.

A flexible web-based User Interface is used to configure schedules for distribution and execution of scanners, retrieval of scan files, etc. Once Desktop Inventory has been configured, inventory data is automatically collected, analyzed and published both as internal reports and through a well-structured database accessible via ODBC.

Desktop Administration is a remote administration tool for your company's computers. The Desktop Administration software suite is based on two principle applications:

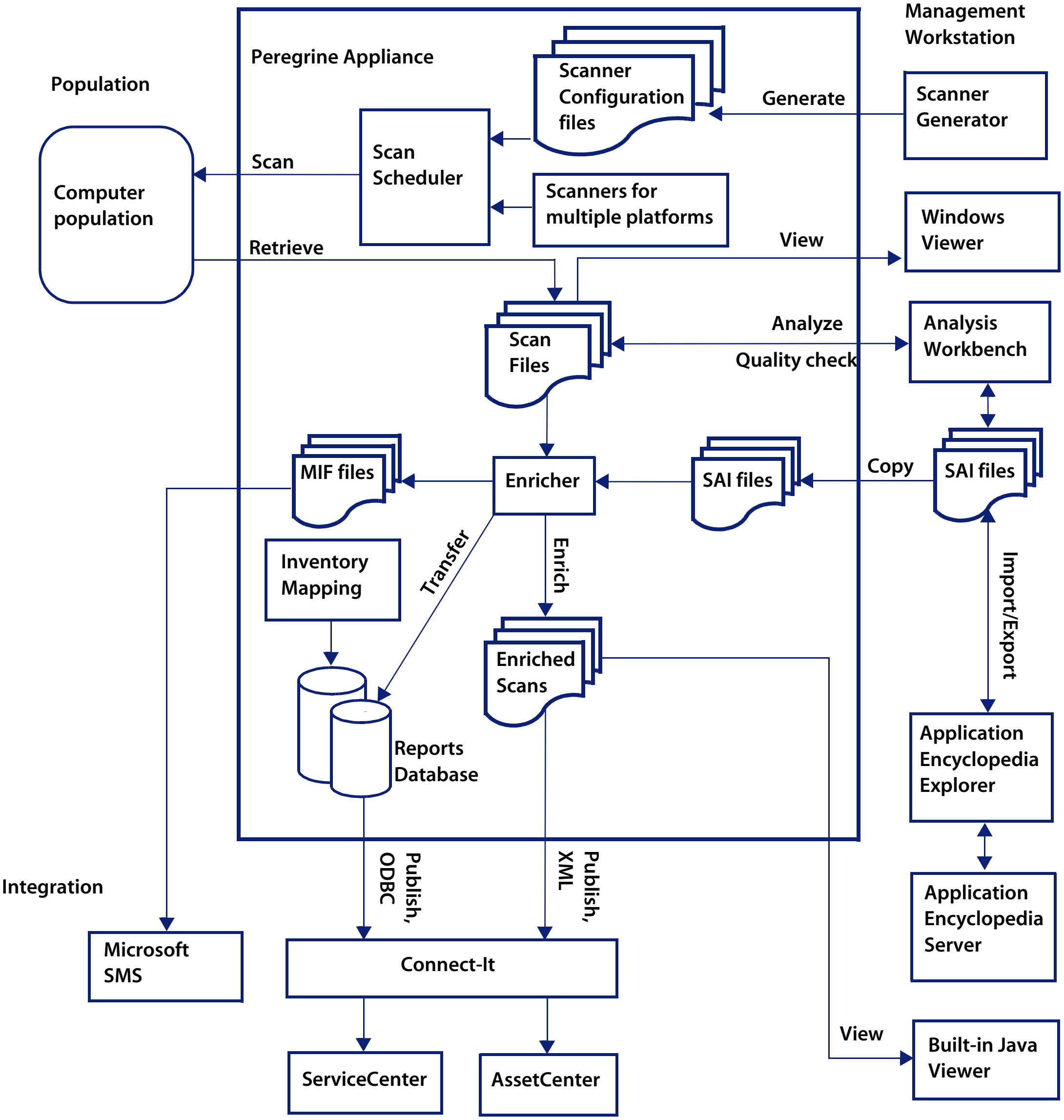
- Automatic Administration
  - Configure remote computers.
  - Propagate and recover data from remote computers.

    - Distribute and deploy software.
    - Verify the implementation of internal security rules on the computers in your IT portfolio.
    - Prevent the propagation of a virus by eradicating it on infected computers and servers.
- Remote Control
    - Perform remote administration duties on your servers.
    - Resolve problems by taking remote control of an employee's computer.
    - Broadcast information rapidly using a message, news, and chat functions.

There are some steps that you must take to ensure the three products work well together in your network. Read this chapter as well as Setting up Network Discovery to work with Desktop Inventory on page 31 to learn the steps involved.

The interaction of the components of Network Discovery and Desktop Inventory

The following diagram shows at a high level the interaction of the main components of Network Discovery and Desktop Inventory. You can see what parts of Desktop Inventory are running inside the Peregrine appliance.


Population
Computer population
Peregrine Appliance
Management Workstation
Scanner Configuration files
Scanner Generator
Generate
Scan
Scan Scheduler
Scanners for multiple platforms
Retrieve
View
Windows Viewer
Scan Files
Analyze
Quality check
Analysis Workbench
MIF files
Enricher
SAI files
Copy
SAI files
Inventory Mapping
Transfer
Enrich
Import/Export
Enriched Scans
Reports Database
Application Encyclopedia Explorer
Application Encyclopedia Server
Integration
Publish, ODBC
Publish, XML
Microsoft SMS
Connect-It
View
Built-in Java Viewer
ServiceCenter
AssetCenter

The Peregrine Appliance

The Peregrine appliance can be made responsible for collecting the scan files generated by the Scanners and storing them centrally.

The Scanners are distributed to individual computers from the appliance using the listener. The appliance maintains a schedule dictating which computers should be scanned and when.

When a particular computer needs to be scanned, the appliance contacts the Listener on the computer, sends a copy of the appropriate Scanner configuration file and a copy of the latest Scanner to the computer, executes it, and retrieves the scan file.

Note: Listener Agents must be deployed to all computers where automatic scan scheduling and scan file retrieval should take place. See Setting up Network Discovery to work with Desktop Inventory on page 31 for information about deploying the Listeners.

Retrieved scan files are stored in a directory on the appliance. A background process, the XML Enricher, polls this directory for new scan files and processes them so they can be added to the appliance's inventory database. It also enriches the scan files with application data and stores these as compressed XML files accessible from a network share.

The automatic deployment of Scanners

In most cases, the Scanners can be automatically deployed to a computer as that computer is discovered with Network Discovery, and executed as needed.

This mechanism makes Scanner deployment an easy task, as opposed to situations where deployment has to rely on network login scripts or manual intervention. Thus, the accuracy and completeness of the collected inventory data can be very high.

Important: Automatic deployment of scanners is supported on all Win32 platforms. Scanners must be deployed by more traditional means for DOS, UNIX/Linux, and OS/2 platforms.

Scheduling of scan execution

It is possible to specify a schedule for computer scanning. The schedule serves at least two purposes.

- First, although the execution of a scan is designed to be as unobtrusive as possible to the user of a computer, some users do notice and find it distracting. So scans can be scheduled to run at a time of day that tends not to conflict with users.
- Second, the accuracy of the inventory depends on the frequency of scan execution. For example, some users want the data refreshed every week, others every month. So the frequency of scans can be specified.

Collection and storage of scan files

A Scanner writes a scan file to the local disk of the scanned computer, and the scan file is transferred to the appliance for storage and processing. There are a few ways in which the scan file can be transferred:

- The appliance contacts the computer and transfers the scan file from the computer. This is the typical case for computers that are permanently connected to the network. The collection of scan files is scheduled and controlled to minimize impact on the network. For example, you can specify what times of day are appropriate for scan file collection, how many files can be transferred in parallel, and how much network bandwidth scan collection is allowed to consume.

Note: Collection of scan files is decoupled from the execution of a scan. You can schedule scans for one time of day, but collect the scan files some time later using a different schedule.

- Some computers, for example laptops, are only occasionally connected to the network. In this case, the scan file can be transferred whenever that computer connects. Since the connection speed may be slow and the connection time short, the transfer mechanism gracefully recovers when the connection is interrupted and can be resumed when the connection is re-established.
- Some computers may never be network accessible to the appliance, for reasons of network topology or security. In this case, it is the responsibility of the administrator to transfer the scan files from such computers to the appliance. The appliance supports an SMB network mountable drive for this

purpose. The administrator can simply mount this network drive and copy as many scan files as required to it.

Once a scan file is transferred to the appliance, it is further processed to recognize software applications (XML enrichment process) and added to the inventory information stored in the Inventory Database. The resulting enriched scan file is stored on the appliance for subsequent access by tools such as Viewer, Analysis Workbench or Connect-It. This enriched scan file is always stored in compressed XML format. At most one scan file for each computer is stored, and the name of the scan file is normally derived from the Asset Tag uniquely identifying the machine. The enriched scan files are optionally backed up along with other appliance data.

The Agent

All Peregrine products use the same agent. In Desktop Inventory documentation, it is called the "Listener Agent." In Desktop Administration documentation, it is called the "Agent."

Each Listener agent originating from a Peregrine appliance will have a security key from that Peregrine appliance. This means that the Listener agent will only be able to communicate with that Peregrine appliance. This is also true of agents originating from the Desktop Administration server, if it is configured to use security keys. Desktop Administration agents with a security key can only communicate with that Desktop Administration server.

To use Network Discovery with Desktop Inventory and Desktop Administration, the security keys must be identical across all products. See Setting up Network Discovery to work with Desktop Inventory on page 31 for more information.

The Listener is installed as a service on a remote computer. This service enables the computer to be securely scanned at any given time. In Windows NT, 2000, 2003, and XP, a manager can instantly deploy this service on computers using the QuickDeploy function.

The Listener is able to perform tasks on a computer on behalf of Peregrine applications.

- The Listener is available on Win32.
- For security reasons, Listener communications are encrypted and authenticated.
- The Listener listens and performs requests for Network Discovery. For example, it can install a Scanner, execute a scan, or transfer a scan file to the appliance.
- If a computer is not connected to the network, the Peregrine appliance is able to detect when a connection is established by making use of the Listener agent (the Listener agent sends broadcast packets to the appliance). Thus the appliance is now able to discover, scan, and collect scan files from, computers that are only temporarily connected to the network.

Note: A newly discovered computer cannot be scanned without first installing the Listener agent.

The Listener component must be installed on every workstation that will be part of the automatic inventory process. This can be done for Windows NT-based computers using the QuickDeploy feature, or it may have to be done manually.

Note: QuickDeploy cannot be used with Windows 95/98/ME.

Note: If you are doing the inventory manually, you do not need the Listener agent.

Once installed, the Listener is capable of communication with the appliance. The communication can only be initiated by the appliance. The Listener is not able to initiate any file transfers, scans, etc.

Further information

For further information about the Listener, refer to Setting up Network Discovery to work with Desktop Inventory on page 31.

Scan file enrichment

The XML Enricher is a process that runs in the background on the appliance. It automatically adds application data to new scan files, and then saves them in the **xsf** format. This process is called scan file enrichment.

Further information

For further information about the XML Enricher, refer to The XML Enricher on page 57.

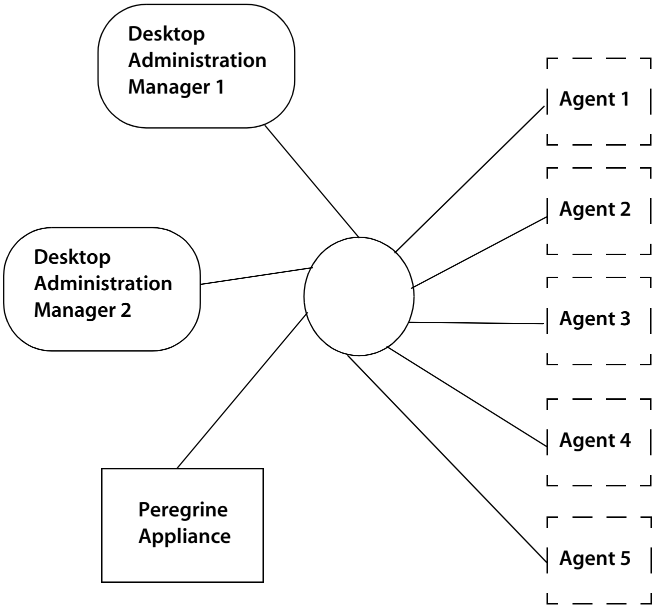
2 CHAPTER Sharing Security Keys

The goal is to make Network Discovery, Desktop Inventory, and Desktop Administration work together.

As discussed in Introduction on page 7, all the Peregrine products use the same agent. By default, the Network Discovery Listener agent uses security keys. The Desktop Administration agent can be configured to use security keys, but the keys are not required for normal operation.

This means that the agents distributed by Desktop Administration may not have any security keys, or will have different security keys than the agent distributed by Network Discovery for use with Desktop Inventory.

Also, each Peregrine appliance has its own security keys. If you have more than one Peregrine appliance in your network, see Sharing Security Keys between your Peregrine Appliances on page 27.


Desktop Administration Manager 1
Desktop Administration Manager 2
Peregrine Appliance
Agent 1
Agent 2
Agent 3
Agent 4
Agent 5

Note: It is ideal for you to make sure Network Discovery and Desktop Administration have the same security keys before you deploy any agents on your network.

Note: If for any reason, you need to have different security keys on your Peregrine appliances or Desktop Administration servers, contact customer support for advice on how to proceed.

The only way to copy the security keys from one product to another (or between Peregrine appliances) is by copying the files (keypriv.key and keypub.key) from one product onto a new DOS/Windows formatted (3.5 inch, 1.44MB) floppy disk and manually loading the files into the other product.

Warning: The security key files are transferred on a floppy disk for security reasons. Do not ever transfer the private key over the network in a non-encrypted format.

There are two procedures described in this section:

- Putting the Peregrine appliance security keys onto Desktop Administration on page 17
- Putting the Desktop Administration security keys onto the Peregrine appliance on page 23

If you have deployed agents from Desktop Administration first, then copy the keys from Desktop Administration onto the Peregrine appliance. If you have deployed agents from the Peregrine appliance first, then copy the keys from the appliance onto your Desktop Administration server.

If you have deployed Listener agents from Network Discovery first, and you want to copy security keys to your Desktop Administration server, you will need to reinstall the agents already deployed from Desktop Administration.

The Network Discovery Listener agent is a smaller version of the agent from Desktop Administration. They do not have the same functionality. For example, you cannot remotely control computers using the Network Discovery Listener.

For more information on how to set up and use Desktop Administration, refer to the *Desktop Administration Installation Guide* and *Desktop Administration User Guide*.

Putting the Peregrine appliance security keys onto Desktop Administration

Copying the Security Key files to a floppy disk

1. Select one Peregrine appliance in your network as the “master” appliance. You will use the security keys from this appliance to copy to the other Peregrine appliances in your network.

2. Insert a floppy disk into the disk drive on the “master” appliance.

3. On the “master” Peregrine appliance, access the configuration interface by connecting a keyboard and monitor directly to the appliance.

4 Login with your configuration password (the default is “Appliance”).

The screen shows the Appliance Management menu:
1) Settings
2) Actions
3) Appliance hardware information
4) Exit and log off

5 Type **2** (or use the arrow keys to move the cursor to 2) and press **Enter.**

The screen shows the Appliance Actions menu:
1) Return to main menu
2) Appliance shutdown
3) Appliance restart
4) Set time
5) Synchronize time
6) Add licenses from floppy
7) Copy listener security keys to floppy
8) Copy listener security keys from floppy
9) Check CD

6 Type **7** (or use the arrow keys to move the cursor to 7) and press **Enter.**

The screen shows the following text:
Mounting floppy disk...
Copying files...
Copied file “keypriv.key”.
Copied file “keypub.key”.
Copied file “response.ans”.
Unmounting floppy disk...
Press Enter to continue.

7 Press **Enter**.

8 Exit the program.

9 Remove the floppy disk from the drive.

Create a new Remote Control Certificate in Desktop Administration using the Security Keys

1 Insert the floppy disk into your Desktop Administration server.

2 Login to Desktop Administration (**Start** > **Programs** > **Peregrine** > **Desktop Administration Console**).

3 Click **Open**, then click **OK** on the splash screen.

4 Click **Tools** > **Actions** > **Create a Remote Control Certificate**.

The Manager Authentication window appears, and you will now go through a setup wizard. The following table shows the basic setup. If you have already configured Desktop Administration, you may need to have different settings in some of the wizard screens. Refer to your Desktop Administration documentation for more information.

Wizard Page	Action
Manager Authentication	Click **Next**.
NT Security	Click **Next**.
InfraTools Servers	Click **Next**.
Broadcast Detectors	Select all three options: ■ Use the broadcast detector ■ View the properties of the broadcast detector ■ Edit broadcast detector Click **Next**.
Direct Accesses	Click **Next**.
Default Logon Parameters	Select “Ask for this password” if you want to be asked for a password every time you log on to a remote workstation through Remote Control. Click **Next**.
Default Control Options	Click **Next**.
Default Control Rights	Click **Next**.
Permission to modify default parameters	Click **Next**.

Wizard Page	Action
Validity	Change the date if you want a longer license period. Click **Next**.
Add Security Keys	Select the keypriv.key file on your floppy disk. Click **Next**.
Generate Certificate	Save the new Certificate as **certificate.cfg** Click **Finish**.

Set up the Certificate using the Private Key in Peregrine Remote Control

1 Login to the Peregrine Remote Control Manager.

2 Click **File** > **Start the Configuration Wizard**.

The Configure InfraTools Manager wizard appears, and you will now go through a setup wizard.

Wizard Page	Action
Configure InfraTools Manager	Select "Use another certificate" and choose the "certificate.cfg" file that you have already created. Click **Next**.
InfraTools agent version	Select "All versions." Click **Next**.
End of Configuration	Click **Finish**.

Configure the response.ans file for QuickDeploy of the Agents

The response.ans file is used by QuickDeploy to deploy listeners to remote workstations with the appropriate configuration settings. Response.ans contains the public key (in an encrypted format).

1 Insert the floppy disk into your Desktop Administration server.

2 In order to have the complete agent required with Desktop Administration, you must alter the text of the response.ans file.

   a Open response.ans in a text editor such as Notepad.

   b Find the line with this information:

      Packages=iftlsnr

   c Change the line to read as follows:

      Packages=iftlsnr,iftmsg,iftrc,iftsys

   d Save the file onto the disk with the same filename.

3 In Windows Explorer, copy the file and also save it to the following two locations:

   \Program Files\Peregrine\Remote Control\deploy\generic

   \Program Files\Peregrine\Desktop Administration Server\depot\deploy\generic

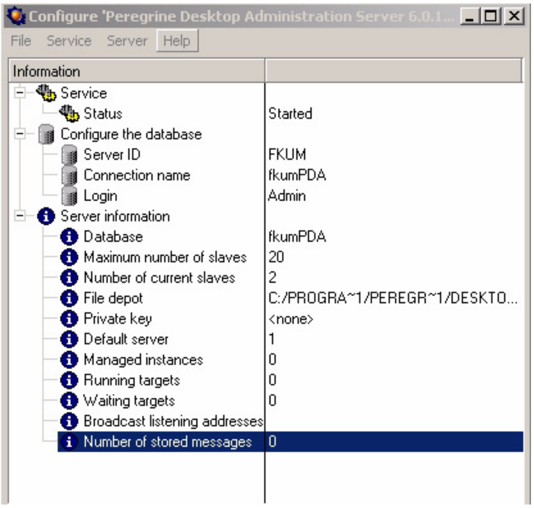
4 Exit the program.

Install the security key into the Server Configuration

The file you altered in the previous procedure must now be installed in the Desktop Administration Server Configuration program.

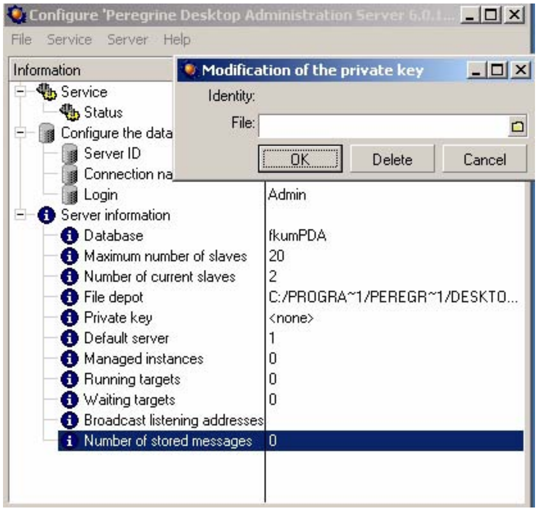
1 In Windows, click **Start** > **Programs** > **Peregrine** > **Desktop Administration Server** > **Server Configuration Tool**.

The Server Configuration Tool appears.



Information	
Service	
Status	Started
Configure the database	
Server ID	FKUM
Connection name	fkumPDA
Login	Admin
Server information	
Database	fkumPDA
Maximum number of slaves	20
Number of current slaves	2
File depot	C:/PROGRA~1/PEREGR~1/DESKTO...
Private key	<none>
Default server	1
Managed instances	0
Running targets	0
Waiting targets	0
Broadcast listening addresses	
Number of stored messages	0

2 Click **Server** > **Modify the private key**.


Configure 'Peregrine Desktop Administration Server 6.0.1...
File
Service
Server
Help
Modification of the private key
OK
Delete
Cancel

Identity:

File:

Information	
Service	
Status	
Configure the data	
Server ID	
Connection na	
Login	Admin
Server information	
Database	fkumPDA
Maximum number of slaves	20
Number of current slaves	2
File depot	C:/PROGRA~1/PEREGR~1/DESKTO...
Private key	<none>
Default server	1
Managed instances	0
Running targets	0
Waiting targets	0
Broadcast listening addresses	
Number of stored messages	0

3 Click the “browse” icon, and choose the private key file from the floppy disk.

4 Click **OK**.

5 Exit the program.

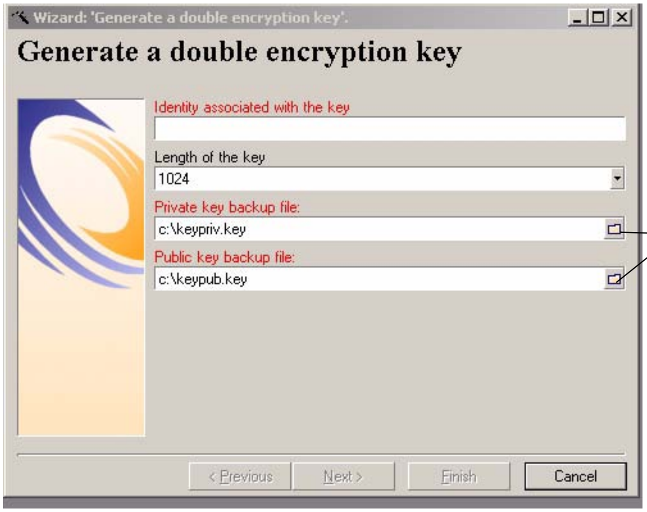
Putting the Desktop Administration security keys onto the Peregrine appliance

Putting the Desktop Administration keys onto the Peregrine appliance

1 Insert a floppy disk into your Desktop Administration server.

2 In Desktop Administration, go to **Tools** > **Actions** > **Generate a double encryption key**.

A wizard appears. From here, you can save the public and private security key files.



Wizard: 'Generate a double encryption key'.

Generate a double encryption key

Identity associated with the key

Length of the key: 1024

Private key backup file: c:\keypriv.key

Public key backup file: c:\keypub.key

Browse icons

3 Enter an identity (name) for the keys.

4 Click the “browse” icon for each file, and choose the floppy drive as the place to save the public and private security keys.

5 Click **Finish**.

This process may take a few seconds.

6 Wait for the system to confirm that the files have been saved to the floppy.

7 Remove the floppy disk from the Desktop Administration server.

8 Put the floppy disk in the Peregrine appliance drive.

9 On the Peregrine appliance, access the configuration interface by connecting a keyboard and monitor directly to the appliance.

10 Login with your configuration password (the default is “Appliance”).

The screen shows the Appliance Management menu:
1) Settings
2) Actions
3) Appliance hardware information
4) Exit and log off

11 Type **2** (or use the arrow keys to move the cursor to 2) and press **Enter.**

The screen shows the Appliance Actions menu:
1) Return to main menu
2) Appliance shutdown
3) Appliance restart
4) Set time
5) Synchronize time
6) Add licenses from floppy
7) Copy listener security keys to floppy
8) Copy listener security keys from floppy
9) Check CD

12 Type **8** (or use the arrow keys to move the cursor to 8) and press **Enter.**

The screen shows the following text:
Mounting floppy disk...
Copying files...
Copied file “keypriv.key”.
Copied file “keypub.key”.
Unmounting floppy disk...
Press Enter to continue

13 Press **Enter**.

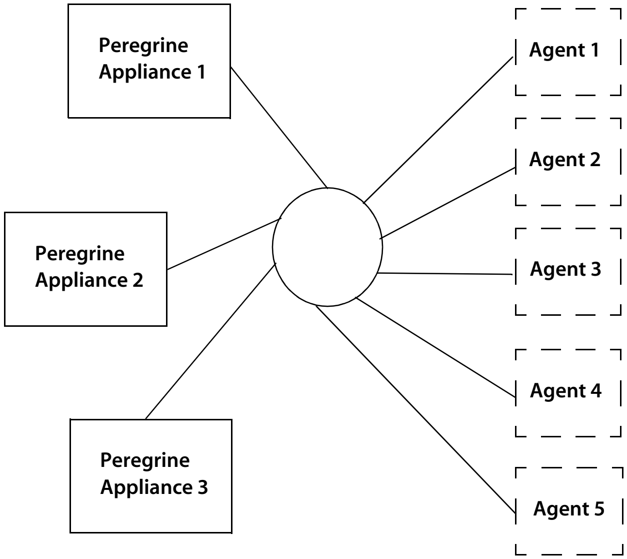
14 Exit the program.

3

CHAPTER

Sharing Security Keys between your Peregrine Appliances

Each Peregrine appliance is shipped with a unique Listener agent security key. If you are aggregating multiple appliances, and using Desktop Inventory, you should make sure all your Peregrine appliances have the same security keys.



This can be accomplished in a few simple steps:

- Copy the security keys from one appliance onto a floppy disk.
- Copy those security keys from the floppy to the other appliances

Copying the Security Key files to a floppy disk

1 Select one Peregrine appliance in your network as the “master” appliance. You will use the security keys from this appliance to copy to the other Peregrine appliances in your network.

2 Insert a floppy disk into the disk drive on the “master” appliance.

3 On the “master” Peregrine appliance, access the configuration interface by connecting a keyboard and monitor directly to the appliance.

4 Login with your configuration password (the default is “Appliance”).

The screen shows the Appliance Management menu:
1) Settings
2) Actions
3) Appliance hardware information
4) Exit and log off

5 Type **2** (or use the arrow keys to move the cursor to 2) and press **Enter.**

The screen shows the Appliance Actions menu:
1) Return to main menu
2) Appliance shutdown
3) Appliance restart
4) Set time
5) Synchronize time
6) Add licenses from floppy
7) Copy listener security keys to floppy
8) Copy listener security keys from floppy
9) Check CD

6 Type **7** (or use the arrow keys to move the cursor to 7) and press **Enter.**

The screen shows the following text:
Mounting floppy disk...
Copying files...
Copied file “keypriv.key”.
Copied file “keypub.key”.
Copied file “response.ans”.

Unmounting floppy disk...
Press Enter to continue.

7 Press **Enter**.

8 Exit the program.

9 Remove the floppy disk from the drive.

Copying the Security Key files onto the other appliances

Note: Repeat the following steps on all other Peregrine appliances on your network.

Warning: Copying a security key overwrites the one existing on the appliance. If any agents have been deployed using this security key, you will no longer be able to communicate with them.

1 Insert the floppy disk into the disk drive on the Peregrine appliance.

2 On the Peregrine appliance, access the configuration interface by connecting a keyboard and monitor directly to the appliance.

3 Login with your configuration password (the default is “Appliance”).

The screen shows the Appliance Management menu:
1) Settings
2) Actions
3) Appliance hardware information
4) Exit and log off

4 Type **2** (or use the arrow keys to move the cursor to 2) and press **Enter.**

The screen shows the Appliance Actions menu:
1) Return to main menu
2) Appliance shutdown
3) Appliance restart
4) Set time
5) Synchronize time
6) Add licenses from floppy
7) Copy listener security keys to floppy

8) Copy listener security keys from floppy
9) Check CD

5. Type **8** (or use the arrow keys to move the cursor to 8) and press **Enter.**

   The screen shows the following text:
   Mounting floppy disk...
   Copying files...
   Copied file “keypriv.key”.
   Copied file “keypub.key”.
   Unmounting floppy disk...
   Press Enter to continue

Note: The “response.ans” file is not copied. The Peregrine appliance will automatically regenerate this file.

6. Press **Enter**.

7. Exit the program.

8. Remove the floppy disk from the drive.

4 CHAPTER Setting up Network Discovery to work with Desktop Inventory

This chapter provides a step-by-step approach to getting started when using Network Discovery with Desktop Inventory and Desktop Administration.

Some of the steps are carried out on the Windows workstation running Desktop Inventory and some on the Peregrine appliance running Network Discovery. We have indicated this where applicable.

Prerequisites

What you should have completed by now:
Setup the Peregrine appliance successfully for Network Discovery and have a populated Network Map.
Installed Desktop Inventory on a workstation (see the *Desktop Inventory User's Guide* for more information on how to do this).
Installed a valid Desktop Inventory license (see the *Desktop Inventory Installation and Upgrade Guide* for more information on how to do this).
Shared the security keys between the Peregrine Appliance and Desktop Administration (see Sharing Security Keys on page 15).

There are many default configurations already set up for you, and it would be wise to choose some of these to get started.

The automatic deployment of Scanners

First, you must make sure the Listeners have been deployed to the computers in your network.

Then, the Scanners can often be automatically deployed as computers are discovered on the network, and executed as needed.

This greatly reduces the effort involved in maintaining an inventory. Since the process is automated and does not rely on network login scripts or manual intervention, accuracy and coverage is increased.

Automatic deployment of scanners is supported on all Win32 platforms. Scanners must be deployed by other means for DOS, UNIX/Linux, Win16 and OS/2 platforms, if applicable.

You will need to know what devices are in your network to follow this procedure. You will be giving Network Discovery a list of IP addresses for it to find and from which to collect scan data.

Important: You cannot automate the deployment of DOS, UNIX/Linux, Win16 and OS/2 Scanners. You will need to deploy these manually.

Steps

Use the following checklist to track your progress setting up Network Discovery, Desktop Inventory, and Desktop Administration.

- Step 1: Tell Network Discovery which version of Desktop Inventory scanners you are using on page 33
- Step 2: Map a drive from Windows workstation to the appliance shared directories on page 35
- Step 3: Make Network Discovery and Desktop Inventory ‘aware’ of each other on page 36.
- Step 4: Add a Scanner Account on the appliance (optional) on page 38

- Step 5: Run Scanner Generator, generate and validate your Scanner configuration files (Windows workstation and appliance) on page 39
- Step 6: Add or define a Scanner Property Group on the appliance on page 40
- Step 7: Define a Listener Property Group on the appliance on page 45
- Step 8: Apply the Scanner and Listener property groups with one or more IPv4 ranges (appliance) on page 46
- Step 9: Submit and activate your changes on page 48
- Step 10: Deploy the Listeners to your workstations on page 48

Step 1: Tell Network Discovery which version of Desktop Inventory scanners you are using

This feature allows you to tell Network Discovery which version of Desktop Inventory you are using (either 7.3.1 or 8.0, earlier versions of Desktop Inventory are not supported).

There are two possible scenarios in which you would use this feature:

- Upgrading to Network Discovery 5.2 on page 33
- New Network Discovery 5.2 Installation on page 34

Note: Regardless of your installation scenario, Network Discovery 5.2 requires a Desktop Inventory 8.0 .SAI file. If you are upgrading to Network Discovery 5.2, this means that the XML Enricher will be disabled until you manually re-enable it, presumably after upgrading your SAI and re-installing it on the appliance.

Note: In previous versions of Network Discovery (for example, 5.1.2), if you were adding a User.SAI file built in 7.3.1 you needed to add in the Master, French and German SAI with the User.SAI. This was because the User.SAI made links to the Masters. In Network Discovery 5.2.x, this is not longer the case. The SAI files work independently, so you only need to add our User.SAI(s).

Upgrading to Network Discovery 5.2

If you upgrade to Network Discovery 5.2, the default setting will be to work with scanners from Desktop Inventory 7.3.1. If you are also upgrading to Desktop Inventory 8.0, you should change this default setting.

New Network Discovery 5.2 Installation

If you have a new Network Discovery 5.2 installation, the default setting will be to work with scanners from Desktop Inventory 8.0.

Warning: When you decide to change this setting to be 7.3.1, you must do so before you set your network configuration. You will lose all of your scanner configurations (all will be reset to the default settings, see Step 6: Add or define a Scanner Property Group on the appliance on page 40) if you change this setting when Network Discovery is already running in your network.

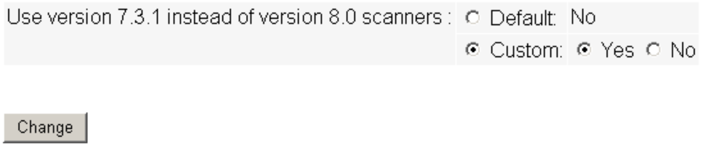
Note: If you have already deployed 8.0 scanners on machines in your network, and decide to change this setting to work with 7.3.1 scanners, your 8.0 scanners will not revert.

To tell Network Discovery which version of Desktop Inventory scanners you are using:

1 Click **Administration** > **System preferences** > **Scanner Version**.

2 If you want to change the default setting, make your selection.

3 Click **Change**.



Use version 7.3.1 instead of version 8.0 scanners : ○ Default: No
● Custom: ● Yes ○ No

Step 2: Map a drive from Windows workstation to the appliance shared directories

Before implementation, you will need to make the Shared directories share on the appliance accessible to Windows.

To map a drive letter to the shared directories share on the appliance:

1 Open Windows Explorer on your workstation. Click **Start** > **Programs** > **Accessories** > **Windows Explorer**.

2 Click **Tools** > **Map Network Drive**.

3 In **Drive**, select the drive letter to map to the shared directories.

4 In **Folder**, type the server and share name of the appliance, in the form of `x:\\<appliance_IP_Address>\share`. For example enter:

```
x:\\172.22.5.2\share
```

Note: You can use the domain name or the IP address of the appliance.

To reconnect to the mapped drive every time you log on, check the **Reconnect at logon** check box.

Support of Network Share

This share is used for several purposes:

- Scan files for unconnected desktops are deposited to the share for subsequent processing.
- Enriched scan files are accessed from the share by other applications such Viewer, Analysis Workbench and Connect-It.
- Scanner configuration files produced by Scanner Generator are deposited here.

The valid login name and password of a user account on the appliance is required to access the share. Connecting to a share is supported on the following platforms: Windows 98, ME, NT4 SP3+, 2000, 2003, XP and any other platform supported by a Samba SMB Client.

For Windows 98 and Windows ME there are some other restrictions:

- The Windows 98/ME login name must be the same as the account name used to access the appliance.
- When accessing the shared directory, you need to use the DNS name of the Peregrine appliance (i.e. you cannot use the IP address).

Step 3: Make Network Discovery and Desktop Inventory ‘aware’ of each other

The activation of the interoperability between Network Discovery and Desktop Inventory requires several steps.

To make Network Discovery and Desktop Inventory ‘aware’ of each other:

1 From your management workstation, login to the Network Discovery.

2 Click **Download**.

3 On the Download page, click on the **DI-ND.reg** file.

The “File Download” dialog appears.

4 Click **Open** to run the file.

The Registry Editor prompt appears.

5 Click **Yes** to enter your information into the registry.

6 Click **OK** to confirm the action.

7 Copy the **license.reg** file sent to you by Peregrine to the following directory on the appliance:

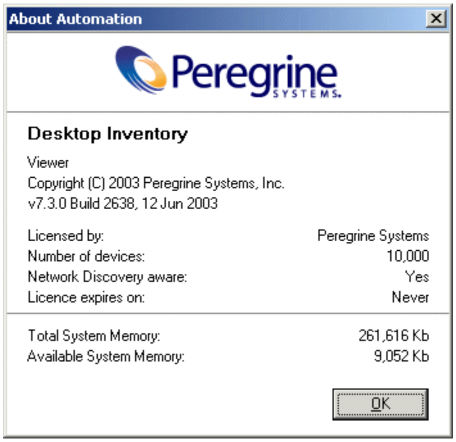
share\license\incoming

Note: The license.reg is the license file that you received with the Desktop Inventory software.

This enables the Desktop Inventory license and options in Network Discovery.

You will now have access to Desktop Inventory related options in the Network Discovery user interface.

8 Now launch the Desktop Inventory Viewer and check the **About** box. You will see that the Network Discovery **aware** entry indicates that interoperability has been enabled.



About Automation

Peregrine SYSTEMS

Desktop Inventory

Viewer
Copyright (C) 2003 Peregrine Systems, Inc.
v7.3.0 Build 2638, 12 Jun 2003

Licensed by:	Peregrine Systems
Number of devices:	10,000
Network Discovery aware:	Yes
Licence expires on:	Never
Total System Memory:	261,616 Kb
Available System Memory:	9,052 Kb

The two applications can now work with each other.

9 On the appliance, go to **Status** > **Current Settings** > **Installed Licenses** to verify that the Desktop Inventory licenses are in place.

Note: The licenses for using Desktop Inventory with Network Discovery will be maximized at the number of devices Network Discovery is licensed for. For example, if you have a 10,000 user license for Desktop Inventory and a 5000 device license for Network Discovery, then only 5000 licenses will be valid here.

Step 4: Add a Scanner Account on the appliance (optional)

If you will be using delta scanning, and transmitting your scan files over HTTP, you will need to setup a Scanner account on the Peregrine appliance.

The Scanner account is only used to establish a connection to the appliance when there are no Listeners (for example, when scanning UNIX machines). You will set up the account in Network Discovery, and then you will enter the same user name and password in the Scanner Generator (see The Scanner Options page on page 86).

To set up the Scanner account:

1. Click **Administration** > **Account administration** > **Add an account**.
2. Enter an account name, and click **Add Account**.
3. Click **Modify account capabilities**.
4. Select the “Scanner” account type.
5. Enable Web access.
6. Click **Modify Capabilities**.
7. Click **Modify account password**.
8. Enter the password (twice) and click **Modify Password**.
9. You are finished. There is no need to configure any account properties for this account.

Step 5: Run Scanner Generator, generate and validate your Scanner configuration files (Windows workstation and appliance)

Two screens are different when you use the Scanner Generator in the appliance mode. These are the first screen and the last screen and are described in Scanner Generator on page 77

For the purpose of this procedure, so you can become familiar with the process, you can also use the sample Scanner configuration files supplied on the appliance. These configuration files have already been validated.

Alternatively, follow the steps below to create a new Scanner configuration.

To start the Scanner Generator on the Windows Workstation:

- Click **Start** > **Programs** > **Peregrine** > **Desktop Inventory 8.0** > **Scanner Generator**.

The Scanner Generator appears.

Create a scanner configuration file called **Test** and validate it.

Further information

See the *Scanner Generator* chapter in the *Desktop Inventory User's Guide* for instructions on how to generate and validate Scanner configuration files.

Step 6: Add or define a Scanner Property Group on the appliance

A Scanner Property Group is a named group of Scanner-related settings. These settings can later be applied to one or more IP ranges of devices to scan (see Step 8: Apply the Scanner and Listener property groups with one or more IPv4 ranges (appliance) on page 46).

These settings allow you to define the following:

- Assign a name and description to the property group.
- Choose which Scanners should be run on which devices in your network.

  For example, if you only want to scan Windows devices in your network, you can choose to only deploy the Win32 Scanner. This setting will allow you to deploy the correct Scanner to any particular IP range in your network. Here are the possible options:

  Scanner Configuration File for:

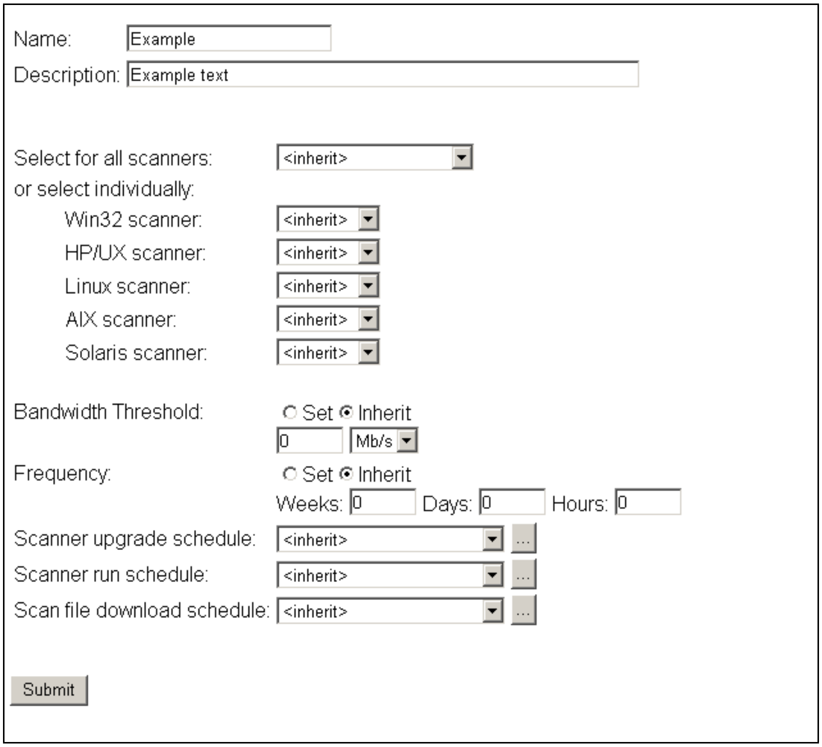
  - Win32
  - HP/UX
  - Linux
  - AIX
  - Solaris

- Choose the maximum bandwidth allowed for scanner deployment.
- Choose when:
  - Scanners are deployed or upgraded
  - Scanners are run
  - Scan files are retrieved

To define a Scanner property group:

1 Click **Administration** > **Network Configuration** > **Scanner Property Groups** > **Add a scanner property group**.

The **Add a Scanner Property Group** page appears:



Name: Example

Description: Example text

Select for all scanners: <inherit>

or select individually:

Win32 scanner: <inherit>

HP/UX scanner: <inherit>

Linux scanner: <inherit>

AIX scanner: <inherit>

Solaris scanner: <inherit>

Bandwidth Threshold: ○ Set ● Inherit
0 Mb/s

Frequency: ○ Set ● Inherit
Weeks: 0 Days: 0 Hours: 0

Scanner upgrade schedule: <inherit>

Scanner run schedule: <inherit>

Scan file download schedule: <inherit>

2 Give the property group a name. For example, ‘Example Scan’

3 Add a description if you want to.

Choosing which Scanners are applied to the devices in your network

You can select Scanner configuration files:

- For all Scanners in one go (Win32, HP/UX, Linux, AIX, Solaris).
- For the different platforms individually. To do this, select individual Scanner Configuration files for each of the platforms. For example, you may want to select the following:

Scanner type	Scanner configuration
Win32 Scanner	Test
HP/UX Scanner	Hardware only
Linux Scanner	Hardware only
AIX Scanner	Default
Solaris Scanner	Hardware only

We have supplied some predefined scanner configuration files. These are accessible from the drop down Select from the Scanners list:

- <**None**> - No Scanner configuration file will be associated with the Scanner Property Group.
- <**inherit**> - You can inherit Scanner configuration settings from the parent IP range.
- <**default**> - This configuration uses the default inventory settings of the Scanner Generator.
- <**fastsw**> - This configuration does a fast software scan of your machines - no signaturing, file identification, etc.
- <**hwonly**> - This configuration does a hardware scan only of your machines

In addition, the drop down lists also show any configuration files that you have validated. Your **Test** configuration file will also appear in the list if you carried out the Scanner configuration file validation step on page 39 correctly.

To choose which Scanners are applied to the devices in your network:

- Select it from the drop down list, either for all Scanners or for Scanners individually.

Setting the bandwidth threshold

In order to avoid congestion of low-bandwidth links, it is possible to set a bandwidth threshold here. The bandwidth threshold specifies the maximum bandwidth that will be used when communicating with a single device for sending the Scanner or retrieving the scan file. There are two options - you can Set a threshold or Inherit one.

To set the bandwidth threshold:

- Select one of the two options:

  a **Set** - You can enter the bandwidth threshold in Kb/s Mb/s, Gb/s

  b **Inherit** - The bandwidth threshold will be inherited from its parent IP range. This is primarily of interest in networks where a large number of IP ranges need to be configured. In this case the setting for many IP ranges can be changed by changing the parent setting if all of the child IP ranges have used inherit.

Examples of bandwidth thresholds have been given below:

- Over a dial up line - 5Kb/s
- Over a LAN - 1 Mb/s
- Over a WAN - 10 Kb/s

Note: The default is 0/sec which means there is no limit.

Setting the frequencies of scans

It is the job of scheduling to ensure that the population is re-scanned at regular intervals to ensure the inventory is reasonably up to date at all times.

These settings allow you to choose when scanners are run, collected, or upgraded in your network.

To set the Frequency of the scan:

- The frequency setting determines how often the scan will take place. You can select from two options:

  a If you select the **Set** button, you can enter the frequency parameters in Weeks, Days and Hours.

  b If you select the **Inherit** button, the frequency setting will be inherited from it's parent IP range.

Setting scan schedule properties

Some predefined scanner schedules have been supplied. These are accessible from the drop down lists:

- <**None**> - No scan schedule will be set for the property.
- <**Inherit**> - You can inherit Scanner configuration settings from the parent IP range.
- <**All the time**> - The scan schedule property will be in effect all the time.
- <**Weekends**> - The scan schedule property will only be in effect on weekends.
- <**Not during working hours**> - The scan schedule property will only be in effect outside working hours.
- <**working hours**> - The scan schedule property will only be in effect during working hours (i.e. between 9 am and 5 pm).

To set the Scanner upgrade schedule:

This setting determines how often the Scanners will be upgraded.

- Select an option from the **Scanner upgrade schedule** drop down list.

To set the Scanner run schedule:

This setting determines when the Scanner can be run.

- Select an option from the **Scanner run schedule** drop down list.

To set the Scan file download schedule:

This setting determines when the Scan file will be retrieved from the workstation to the appliance.

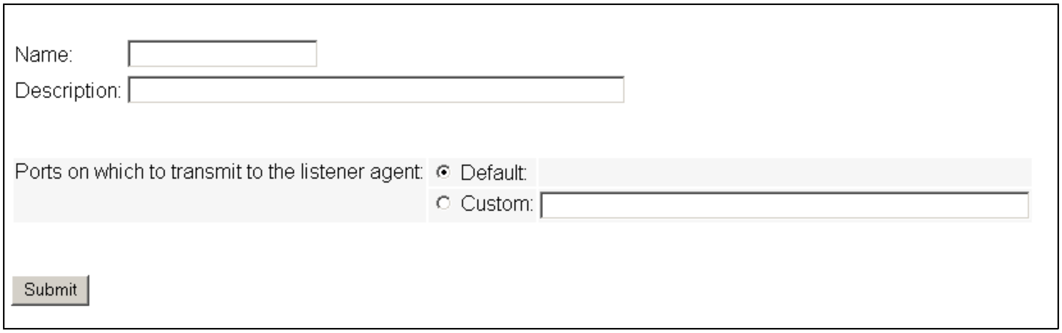
- Select an option from the **Scan file download schedule** drop down list.

Step 7: Define a Listener Property Group on the appliance

A Listener Property Group is a named group of Listener-related settings. These settings can later be applied to one or more IP Ranges of devices to scan (see Step 8: Apply the Scanner and Listener property groups with one or more IPv4 ranges (appliance) on page 46).

To define a Listener property group:

1. Login to Network Discovery.
2. Click **Administration** > **Network Configuration** > **Listener Property Groups** > **Add a Listener Property Group**.



Name:

Description:

Ports on which to transmit to the listener agent: ● Default: ○ Custom:

3. Give the property group a name. For example, '**Windows Workstations**'
4. Add a description if you want to.
5. In the **Ports on which to transmit to the listener agent** field, select **Default** to use the default port (1738) or **Custom** to enter the port on the workstation that the Listener will be transmitted manually.
6. Once you have done this, click the **Submit** button. A summary is displayed.
7. Review the changes and summary and scroll to the bottom of the page. If you are happy with the settings, click the **Activate changes** button. See page 48 for an explanation of the purpose of the **Activate changes** page.

Step 8: Apply the Scanner and Listener property groups with one or more IPv4 ranges (appliance)

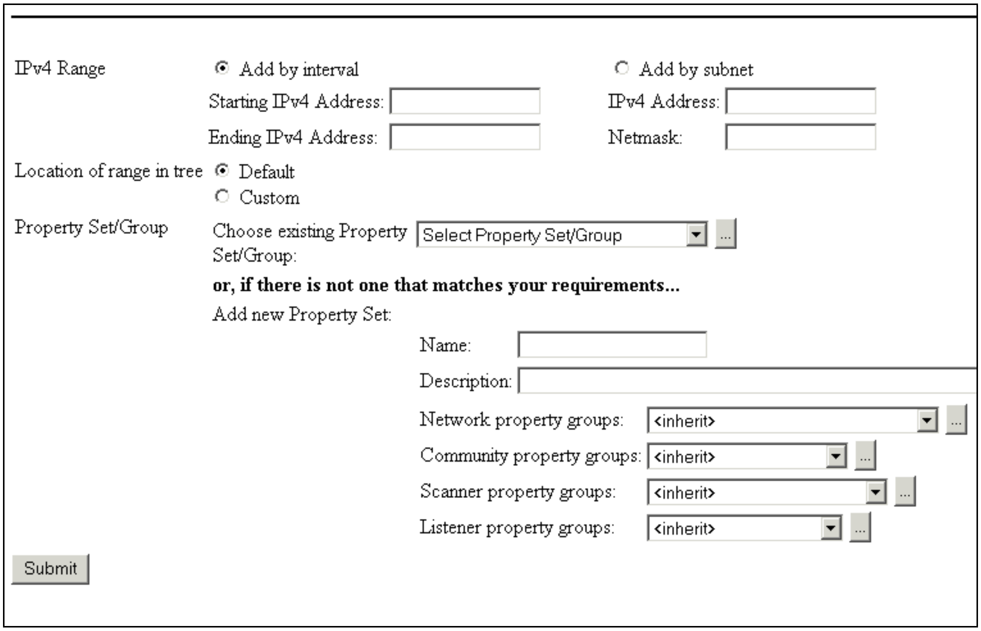
In this step we are specifying what to scan and where, by applying the previously defined Property Groups to a set of IP addresses.

In this step, we use Property Sets, which are named sets of Property Groups. You can either use an existing Property Set or define a new one consisting of different Property Groups.

You should have a good idea of what devices are in your network.

Apply the Scanner and Listener property groups.

1 Click **Administration** > **Network Configuration** > **Add IPv4 range**.



IPv4 Range
● Add by interval
Starting IPv4 Address:
Ending IPv4 Address:
○ Add by subnet
IPv4 Address:
Netmask:

Location of range in tree
● Default
○ Custom

Property Set/Group
Choose existing Property Set/Group: Select Property Set/Group
or, if there is not one that matches your requirements...
Add new Property Set:
Name:
Description:
Network property groups: <inherit>
Community property groups: <inherit>
Scanner property groups: <inherit>
Listener property groups: <inherit>

2 Select the **Add by interval** option.

3 Enter the **Start IP** and **End IP** addresses for the range of computers you want to scan.

4 In the **Property Set/Group** drop down list scroll down to the **Scanner Group** in the list.

5 Now do one of the following:

a Select the new **Scanner Property Group** you created in Step 6: Add or define a Scanner Property Group on the appliance on page 40 (**Example Scan**) and click ... to inspect a summary of the property group. To return to the Add an IPv4 range page click the **Go back to Add an IPv4 Range** link.

Note: You can select one of the many default selections provided. If none of them suits your needs, you can select “global” for now, and then create your own configuration that would be best suited to your IP range.

b Give the IPv4 range a name and description (optional) and specify the settings for the various property groups. You can select one of the many default selections provided.

- Network property groups
- Community property groups
- Scanner property groups - select **Example Scan** from the drop down list.
- Listener property groups - select **Deploy Listener to Windows Workstations** from the drop down list. This is the Listener property group you created on page 45.

6 Click the **Submit** button when you are finished. A screen appears, showing you the options of where your range can fit into the entire network. Typically, the first option (selected by default) is the best, but choose another option if you feel it is necessary.

Important: The **Submit** button adds this change to a list of changes, but does not activate the changes. You can make more changes if so desired and activate them all using **Activate Changes** as described in Step 9: Submit and activate your changes.

Step 9: Submit and activate your changes

Activate your changes

1 Click **Administration** > **Network Configuration** > **Activate changes**.

2 The activate changes page is displayed showing a summary of the changes you have made.

3 Review the changes and summary and scroll to the bottom of the page. If you are happy with the settings, click the **Activate changes** button.

The Activate changes page

The **Activate Changes** page allows the administrator to review all the changes that have been made before actually having the changes take effect.

You must activate the changes to the system in order to have the changes take effect.

You will be told how many potential devices will have to be explored, and given a minimum exploration time (for example, "at least 33 minutes").

Also, you will be told of any configuration problems detected. You can ignore the warnings, but do so at your own risk.

If you decide to implement the changes you have made, activating the changes will update your network configuration.

Step 10: Deploy the Listeners to your workstations

The previously discussed settings allow you to choose a listener port on your desktops, through which the Listener will communicate with the appliance.

The Listener is installed onto the desktops in your network, and can upload Scanners to desktops, execute them to collect software and hardware information and download back the scan data to the appliance for detail inventory of desktops.

For each of the Scanner types you will need a corresponding Listener on the computers where it will be run in order for Scanners to be scheduled.

Note: There is no Listener for DOS, OS/2, Unix, or Linux - therefore these Scanners cannot be automated.

Ways of deploying the Listener

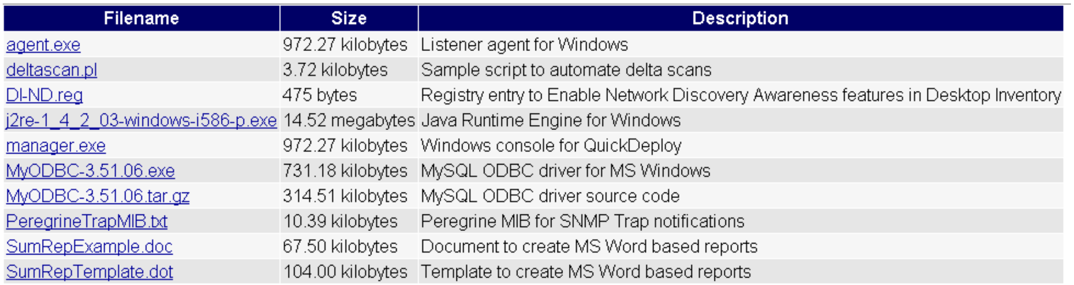
- Download the Listener agent from the appliance and manually install it onto the computer.
- Download the Manager Console and use QuickDeploy to install the Listener to many computers at the same time.
- You could use login scripts.
- You could also send out a company wide e-mail instruction employees to visit the download page on the appliance via their web browser and download and install the listener on their own machine. For this method to be successful, users should reach it from /**download** which is not password protected (/**nm/download** is password protected).

Downloading the Listener programs from the appliance

To download the Listener programs from the appliance:

1 Login to the appliance.

2 On Network Discovery, click the **Download** link. The **Download** page is displayed.

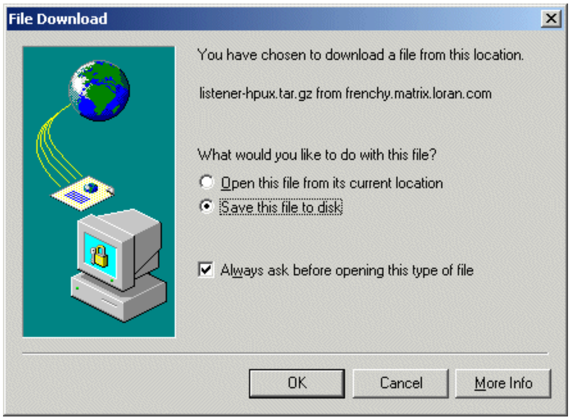


Filename	Size	Description
agent.exe	972.27 kilobytes	Listener agent for Windows
deltascan.pl	3.72 kilobytes	Sample script to automate delta scans
DI-ND.reg	475 bytes	Registry entry to Enable Network Discovery Awareness features in Desktop Inventory
j2re-1_4_2_03-windows-i586-p.exe	14.52 megabytes	Java Runtime Engine for Windows
manager.exe	972.27 kilobytes	Windows console for QuickDeploy
MyODBC-3.51.06.exe	731.18 kilobytes	MySQL ODBC driver for MS Windows
MyODBC-3.51.06.tar.gz	314.51 kilobytes	MySQL ODBC driver source code
PeregrineTrapMIB.txt	10.39 kilobytes	Peregrine MIB for SNMP Trap notifications
SumRepExample.doc	67.50 kilobytes	Document to create MS Word based reports
SumRepTemplate.dot	104.00 kilobytes	Template to create MS Word based reports

3 There are two Listener related files on this page:

File	Description
manager.exe	The QuickDeploy Console Manager for Windows
agent.exe	The Listener Agent for Windows

4 To download a file, click on the file link. A dialog similar to the following is displayed.


File Download

You have chosen to download a file from this location.

listener-hpux.tar.gz from frenchy.matrix.loran.com

What would you like to do with this file?

○ Open this file from its current location

● Save this file to disk

☑ Always ask before opening this type of file

5 Select the **Save this program to disk** option.

6 Navigate to the location where you want to save the file and click **Save**. The installation program is saved to the specified location.

Install the QuickDeploy Manager Console

Important: You must have **Administrator** privileges to be able to install the Manager Console.

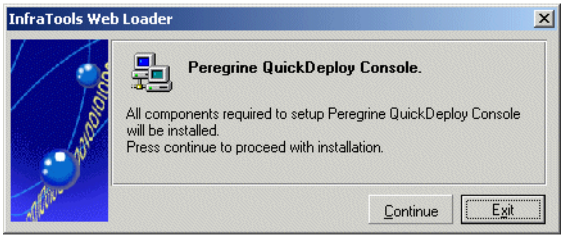
Important: In order to use QuickDeploy on your Windows workstations, the workstations must have their “Server Properties” enabled. This setting is enabled by default, but may have been turned off by an Administrator. Check the status by clicking **Start** > **Settings** > **Control Panel** > **Administrative Tools** > **Services** > **Server**.

Note: If a warning message appears saying that your evaluation period has expired, you can still use QuickDeploy.

The Manager Console enables you to remotely install the Listener Agent module on one or more Windows computers.

To install the Manager Console on your workstation:

1 Double click on the **manager.exe** file you downloaded in the previous procedure. The following dialog is displayed.



InfraTools Web Loader

Peregrine QuickDeploy Console.

All components required to setup Peregrine QuickDeploy Console will be installed.
Press continue to proceed with installation.

2 Click **Continue**. The console is installed.

Saving the response.ans file

To function properly, you must copy the response.ans file from the Peregrine appliance to your newly installed version of QuickDeploy.

To copy the response.ans file to QuickDeploy:

1 Open Windows Explorer.

2 Access the following folder on your Peregrine appliance:

http://<*appliance_IP_address*>/download/agent/

3 Right-click on response.ans.

4 Click **Save Target As**.

5 Save the file to the following location (replacing the file that already exists in that folder).

Program Files\Peregrine\Remote Control\deploy\generic

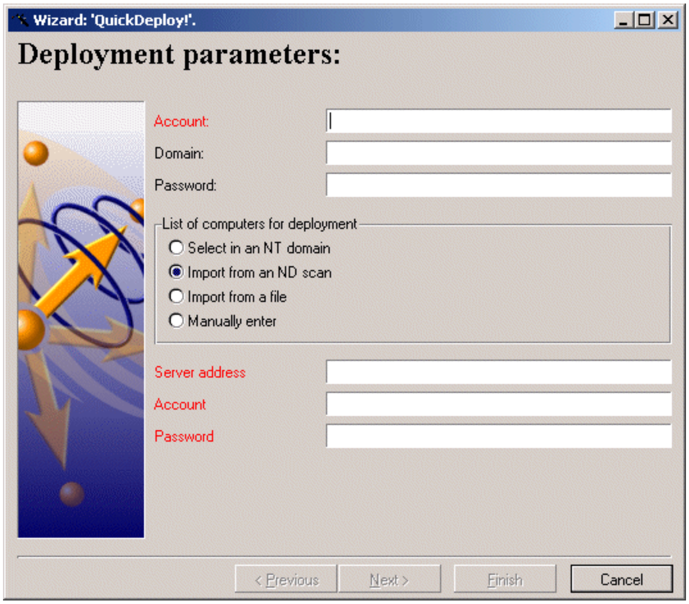
6 Exit the program.

Using QuickDeploy from the Manager Console to deploy the Agent module

To use QuickDeploy from the Manager Console to deploy the Agent module:

1 From the Workstation where the Manager was installed (see previous procedure), click **Start** > **Programs** > **Peregrine** > **Remote Control** > **Manager**.

The **Manager Console** appears, and then the **QuickDeploy** wizard is launched. (If the wizard does not appear, you can click **File** > **Start Deployment Wizard**.)



Wizard: 'QuickDeploy!'.

Deployment parameters:

Account:

Domain:

Password:

List of computers for deployment

○ Select in an NT domain

● Import from an ND scan

○ Import from a file

○ Manually enter

Server address

Account

Password

2 The **List of computers for deployment** setting should be defaulted to **Import from an ND scan**. If this is not the case click on this option.

3 Populate the **Account, Domain** and **Password** fields. That is, the NT User having administrative rights on the target computers.

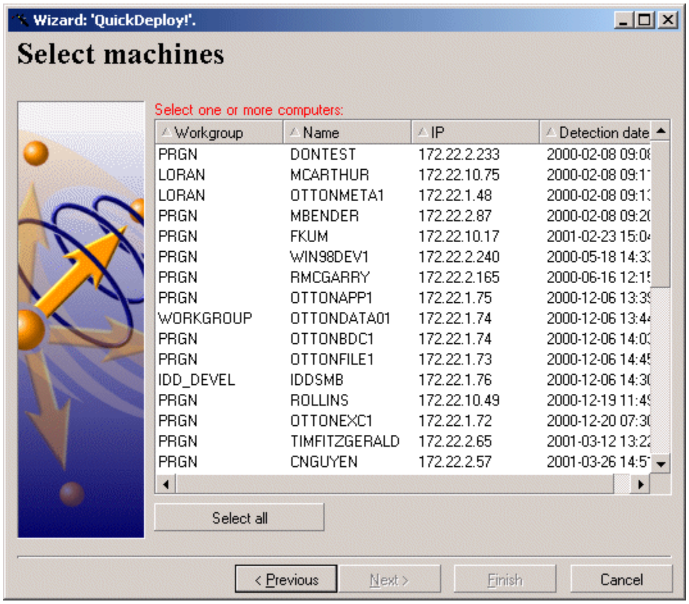
Note: This user should have enough privilege to access the c$ share and run services on remote computers.

4 Enter the Server address (appliance name or IP address for appliance).

5 Enter the Account login and password for the appliance. For example:

- Account: admin
- Password: password

6 Click the **Next** button to continue to the **Select machines** page of the Wizard.



Select machines

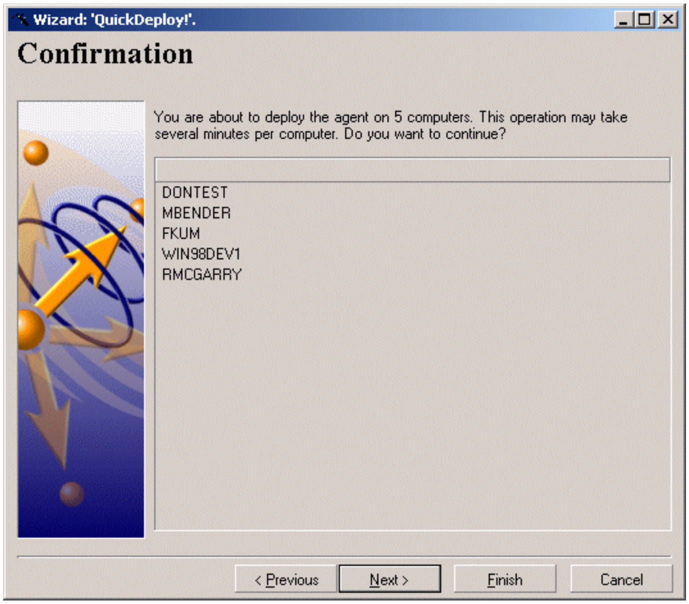
Select one or more computers:

Workgroup	Name	IP	Detection date
PRGN	DONTEST	172.22.2.233	2000-02-08 09:0
LORAN	MCARTHUR	172.22.10.75	2000-02-08 09:1
LORAN	OTTONMETA1	172.22.1.48	2000-02-08 09:1
PRGN	MBENDER	172.22.2.87	2000-02-08 09:2
PRGN	FKUM	172.22.10.17	2001-02-23 15:0
PRGN	WIN98DEV1	172.22.2.240	2000-05-18 14:3
PRGN	RMCGARRY	172.22.2.165	2000-06-16 12:1
PRGN	OTTONAPP1	172.22.1.75	2000-12-06 13:3
WORKGROUP	OTTONDATA01	172.22.1.74	2000-12-06 13:4
PRGN	OTTONBDC1	172.22.1.74	2000-12-06 14:0
PRGN	OTTONFILE1	172.22.1.73	2000-12-06 14:4
IDD_DEVEL	IDDSMB	172.22.1.76	2000-12-06 14:3
PRGN	ROLLINS	172.22.10.49	2000-12-19 11:4
PRGN	OTTONEXC1	172.22.1.72	2000-12-20 07:3
PRGN	TIMFITZGERALD	172.22.2.65	2001-03-12 13:2
PRGN	CNGUYEN	172.22.2.57	2001-03-26 14:5

This page presents a list of computers detected on the network and having no agents.

7 Select the computers on which you want to remotely install the Agent module.

8 Click the **Next** button to continue to the **Confirmation** page.

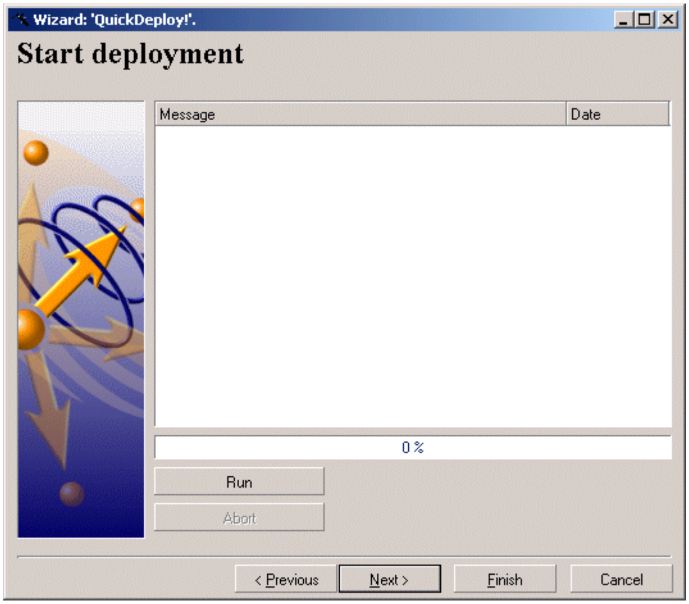


You are about to deploy the agent on 5 computers. This operation may take several minutes per computer. Do you want to continue?

DONTEST
MBENDER
FKUM
WIN98DEV1
RMCGARRY

This page lists the names of the computers on which you want to install the Agent module. Look at the confirmation page to check the list of selected computers.

9 Click the **Next** button to continue to the **Start Deployment** page.



Wizard: 'QuickDeploy!'.

Start deployment

Message	Date

0 %

10 Click **Run** to launch the remote installation of an Agent module. The length of time it takes to deploy the Agent module depends on the number of computers selected. You can stop the deployment process at any time by clicking **Abort**.

Note: We advise you to select a small set of computers to avoid large processing times and massive error reporting in case invalid information was provided.

11 Click **Finish** after the deployment process has terminated. The status bar will indicate that it is 100% complete.

Manually installing the Agents from a browser on the local Workstation

Instead of using QuickDeploy, you can manually install the Agent from a remote computer.

To manually install the Agents from a browser on the local Workstation:

1 Login to Network Discovery on your local workstation.

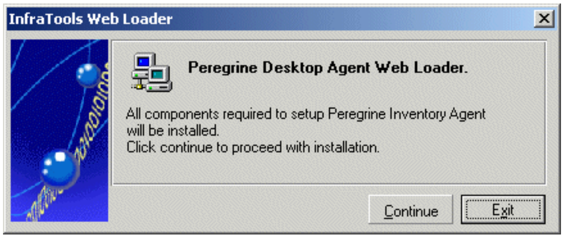
2 Click **Download**.

3 On the Download page, click on the **agent.exe** file.

The "File Download" dialog appears.

4 Click **Open** to run the program.

The **Web Loader** is displayed.



InfraTools Web Loader

Peregrine Desktop Agent Web Loader.

All components required to setup Peregrine Inventory Agent will be installed.
Click continue to proceed with installation.

5 Click **Continue**.

Important: The Agent is installed on the machine and will have a key corresponding to the appliance it comes from. Other appliances will not be able to talk to it. For more information, see Sharing Security Keys between your Peregrine Appliances on page 27.

5 CHAPTER The XML Enricher

The XML Enricher is a process that runs on the Peregrine appliance and automatically adds application data to scan files. This process is called scan file enrichment.

When using the XML Enricher on the appliance, it is no longer necessary to use the Windows-based XML Enricher that is installed with PDI.

Operating principles

When the XML Enricher is running, it looks for new scan files (**xsf**, **fsf,** or **dsf** format) in a directory on the appliance every 20 seconds.

When 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 scan file.

At the end of the process, a new enriched scan file in **xsf** format is created and the original scan file is deleted (unless you have enabled delta scanning, in which case the original scan file is moved to the “original” directory). 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. The XML Enricher does not support the storing of historical data.

Note: Using the Desktop Inventory Scanner Generator, you can configure the “delta scanning” feature. Enabled by default, the delta scanning feature allows you to merge new data in your existing scan files. To disable or enable this feature, see The Scanner Options page on page 86. For more information on the feature, see your *Desktop Inventory User's Guide*.

During the Enrichment process, the Enricher also prepares the data for the Inventory Database on the appliance. Within an hour of enrichment, data for a computer will be available for Reports, Aggregation, etc.

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 application library.

The XML Enricher directory structure

The enricher uses a directory structure like the following, which resides on the appliance.

Directory	Explanation
`\scans`	The base directory
`\scans\deferred`	The scan file is moved to this location if it is a device that the Network Discovery side does not know about yet. This only happens when a manual scan was done and copied to the **scans\incoming** directory. It eventually gets moved from this directory back to the **scans\incoming** directory.

Directory	Explanation
`\scans\deferred\first scan`	If the **Automatically defer all new scans** option was set (see Configuring the XML Enricher on the appliance on page 67) the scan file is not processed. Instead, it is moved to this directory. Any scan files in this directory are for the first time a scan file was seen for a particular computer. This allows the administrator to review the asset and application data. When you are satisfied that the data is ok, you can move it back to the incoming directory. Note: New scan files from a computer will not be processed while a scan file for it exists in this directory. The existing scan file in this directory will be overwritten by a new scan file.
`\scans\failed`	The base failure directory. Failed scans are moved to a sub directory of this.
`\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 if there is an error applying the delta scan file to the original one, the delta scan file will be moved here.
`\scans\failed\error`	When any other error occurs, scan files are moved here.
`\scans\failed\filter`	The scan ends up here if it has an IP address outside a range that has been configured to allow scanned devices.
`\scans\failed\licence`	If too many scans are processed, new scans are moved here.
`\scans\failed\old`	Scan files that are copied to incoming but are older than the one already in the database are moved here.
`\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 versions of the scan files. Do not change or move the contents.

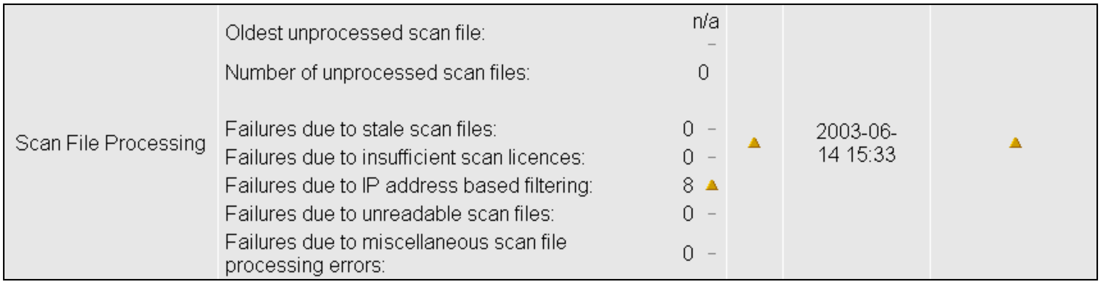
Directory	Explanation
`\scans\processed`	The processed directory. Enriched scan files are created here.
`\scans\processed\[user defined]`	You can group the scan files based on Hardware Fields. This is user-defined. Define the settings at **Administration** > **System preferences** > **Scan file management**. See Managing Scan Files on page 71.

Checking the status of the Enrichment process

To check the status of the Enrichment process:

1. Click **Status** > **Appliance Health** > **Software Environment**. The **Appliance Software Environment** status page is displayed.

2. Scroll down to the **Scan File Processing** section.



Scan File Processing	Oldest unprocessed scan file:	n/a	–	▲	2003-06-14 15:33	▲
	Number of unprocessed scan files:	0				
	Failures due to stale scan files:	0	–			
	Failures due to insufficient scan licences:	0	–			
	Failures due to IP address based filtering:	8	▲			
	Failures due to unreadable scan files:	0	–			
	Failures due to miscellaneous scan file processing errors:	0	–			

This section shows the number of scans waiting to be processed, as well as the number of scans that failed, grouped by failure reason.

If the number of failed scans is too high, this is indicated by an appliance Health indicator of **Warning** or **Alarm**.

Disk space requirement

You will need to have enough free disk space on the appliance to hold all of the scan files for your organization. As an estimate, each scan file is 200kB in size (assuming default Scanner options were used). For example, if you are licensed for 5000 devices, a minimum of 1GB disk will be used.

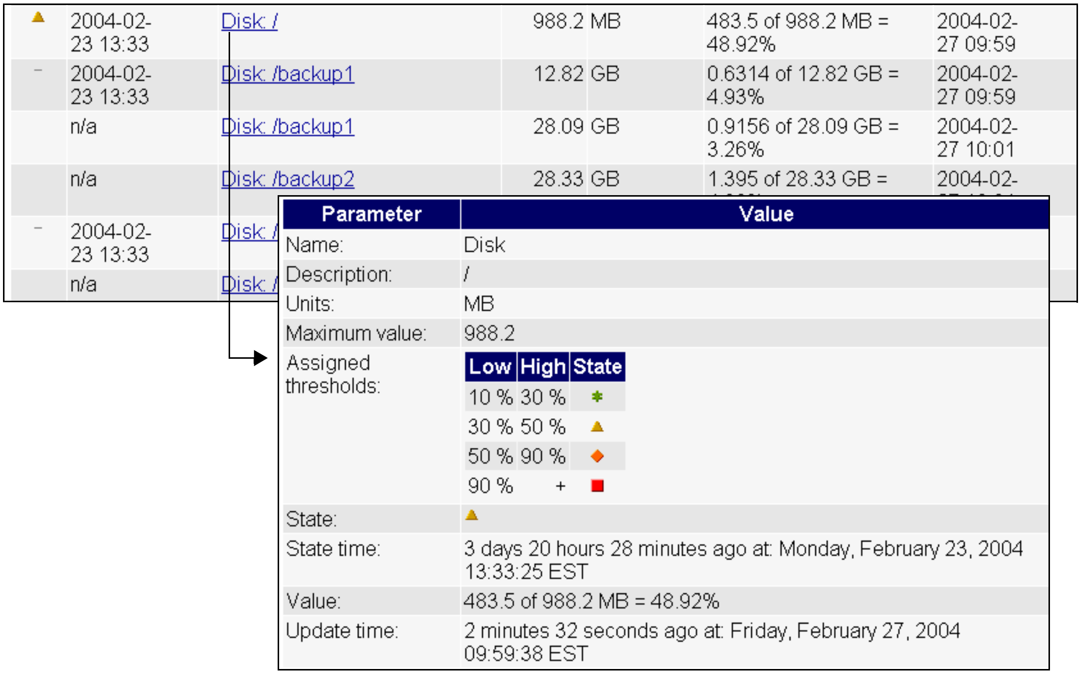
Important: If you enable the delta scanning feature (see The Scanner Options page on page 86), you will need to have twice the disk space available.

Method 1: To check how much disk space is left on the appliance using the Device Manager:

1. On the main Toolbar, click **Find**. The **Find** panel is displayed.
2. Click the **Device** icon.
3. Enter the IP address for the appliance (you can also type in **nmc**) and press **Enter**.
4. Double-click on the device listed in the Find panel.

   A **Device Manager** session opens for the appliance.

5 On the State panel, scroll down to the **Disk:/** setting and click on the link.



▲	2004-02-23 13:33	Disk: /	988.2 MB	483.5 of 988.2 MB = 48.92%	2004-02-27 09:59
–	2004-02-23 13:33	Disk: /backup1	12.82 GB	0.6314 of 12.82 GB = 4.93%	2004-02-27 09:59
	n/a	Disk: /backup1	28.09 GB	0.9156 of 28.09 GB = 3.26%	2004-02-27 10:01
	n/a	Disk: /backup2	28.33 GB	1.395 of 28.33 GB =	2004-02-
–	2004-02-23 13:33	Disk: /			
	n/a	Disk: /			

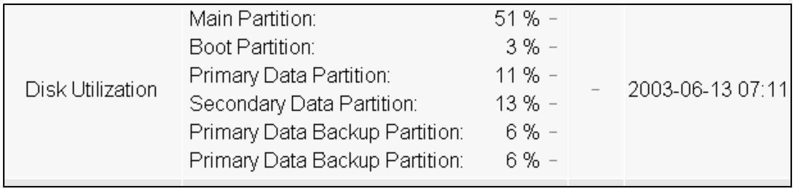
<table>
<tr><th>Parameter</th><th>Value</th></tr>
<tr><td>Name:</td><td>Disk</td></tr>
<tr><td>Description:</td><td>/</td></tr>
<tr><td>Units:</td><td>MB</td></tr>
<tr><td>Maximum value:</td><td>988.2</td></tr>
<tr><td>Assigned thresholds:</td><td><table>
<tr><th>Low</th><th>High</th><th>State</th></tr>
<tr><td>10 %</td><td>30 %</td><td>✱</td></tr>
<tr><td>30 %</td><td>50 %</td><td>▲</td></tr>
<tr><td>50 %</td><td>90 %</td><td>◆</td></tr>
<tr><td>90 %</td><td>+</td><td>🟥</td></tr>
</table></td></tr>
<tr><td>State:</td><td>▲</td></tr>
<tr><td>State time:</td><td>3 days 20 hours 28 minutes ago at: Monday, February 23, 2004 13:33:25 EST</td></tr>
<tr><td>Value:</td><td>483.5 of 988.2 MB = 48.92%</td></tr>
<tr><td>Update time:</td><td>2 minutes 32 seconds ago at: Friday, February 27, 2004 09:59:38 EST</td></tr>
</table>

6 In the example above, 483.5 of 988.2 MB (48.92%) disk space is being used.

Method 2: To check how much disk space is left on the appliance using the Hardware Environment status page:

1 Click **Status** > **Appliance Health** > **Hardware Environment**. The **Appliance Hardware Environment** status page is displayed.

2 Scroll down to the **Disk Utilization** section.



Disk Utilization	Main Partition: Boot Partition: Primary Data Partition: Secondary Data Partition: Primary Data Backup Partition: Primary Data Backup Partition:	51 % 3 % 11 % 13 % 6 % 6 %	– – – – – –	–	2003-06-13 07:11

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:

```
Program Files\Peregrine\Desktop Inventory\8.0.0\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>

Note to Connect-It users

If using Connect-It 3.0.1 or later, use the DTD to describe the format of the scan file to Connect-It.

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="1252" locale="English (United States)"
fsfmajorver="7" fsfminorver="10">

<hardwaredata>
    <hwAssetData type="shell">
      <hwAssetDescription type="attrib">Dallas (15950 North Dallas
Parkway) -  - (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"/>
   </recogconfig>
   <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="2048-00-00 00:00:00" contains="-1">
      <file name="AUTOEXEC.BAT" size="0" modified="2000-04-03
13:51:04" attr="a"/>
      <file name="BOOT.INI" size="288" modified="2000-04-03
15:14:38" attr="rsa"/>
      <file name="sd_settings.ini" size="462" msdos="SD_SET~1.INI"
modified="2001-06-14 09:08:44" attr="a">
        <verinfo name="DOS 8.3 Name" value="SD_SET~1.INI"/>
      </file>
    </dir>
</filedata>
<storedfiles>
<storedfile type="storedfile" name="SYSTEM.INI" size="217"
istext="1" istruncated="0" dir="C:\WINNT\SYSTEM.INI">
      <contents encoding="text">; for 16-bit app support
[386Enh]
woafont=dosapp.fon
EGA80WOA.FON=EGA80WOA.FON
EGA40WOA.FON=EGA40WOA.FON
CGA80WOA.FON=CGA80WOA.FON
CGA40WOA.FON=CGA40WOA.FON
[drivers]
wave=mmdrv.dll
timer=timer.drv
[mci]
</contents>
    </storedfile>
</storedfiles>
</inventory>
```

An explanation of the <applicationdata> element

In an enriched XML scan file, the <**applicationdata**> section contains a list of applications identified on the computer along with the version IDs.

```
<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.

Launching the XML Enricher from the appliance

The XML Enricher is a pre-installed service. The service is enabled by default on the appliance and will start processing scan files as soon as the Network Configuration has been configured and activated.

Starting and stopping the XML Enricher service

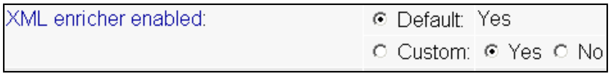
Important: You must make sure that the XML Enricher is started and configured if you want application data to be added to your scan files.

You may sometimes want to stop and start the XML Enricher service manually.

To manually start or stop the xml enricher service:

1. Click **Administration** > **System Preferences** > **Appliance Services**.

2. Scroll down to the **XML enricher** entry.



XML enricher enabled: ● Default: Yes
○ Custom: ● Yes ○ No

3. Click **Yes** to start the service, or click **No** to stop the service.

4. Click **Change** to activate the desired state.

Configuring the XML Enricher on the appliance

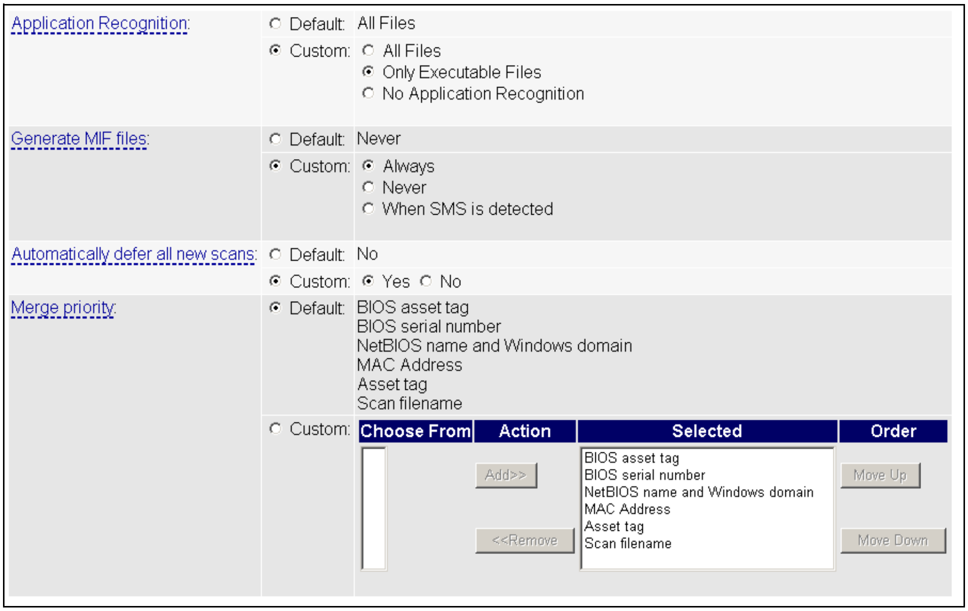
You can configure the following options to control the XML Enrichment process:

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

To configure the XML Enricher on the appliance:

1 Click **Administration > System Preferences > Scanned Devices**.

2 Set the options as required. They are described below.



Application Recognition:
○ Default: All Files
● Custom: ○ All Files
● Only Executable Files
○ No Application Recognition

Generate MIF files:
○ Default: Never
● Custom: ● Always
○ Never
○ When SMS is detected

Automatically defer all new scans:
○ Default: No
● Custom: ● Yes ○ No

Merge priority:
● Default: BIOS asset tag
BIOS serial number
NetBIOS name and Windows domain
MAC Address
Asset tag
Scan filename

○ Custom:

Choose From	Action	Selected	Order
	Add>> <<Remove	BIOS asset tag BIOS serial number NetBIOS name and Windows domain MAC Address Asset tag Scan filename	Move Up Move Down

Application Recognition

There are three options for Application Recognition:

Option	Description
All Files	All files are sent to the recognition engine for processing. This is the default option.
Only Executable Files	Only executable files are sent to the recognition engine for processing.
No Application Recognition	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:

Option	Description
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 incoming:

- The scan file is looked up in the internal database (Not the Inventory Database).
- If the machine has never before been scanned, the scan file is not processed or enriched. Instead, it is moved to the **deferred/firstscan** directory.
- If the machine has been scanned before, the enricher checks if there is a scan file with the same name in the **deferred/firstscan** directory. If there is, the old scan in the **deferred/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 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 then this is not necessary.

For example, if NetBIOS Name and Windows Domain are chosen (both Desktop Inventory and Network Discovery can detect these), then it will use this information in the scan file to find the matching device in Network Discovery.

If this was not done, then the Desktop Inventory scans would create new devices or be merged with the wrong data.

AutoSequence Number

The AutoSequence Number commands will help you assign an automatically generated number to your scan files. This feature is optional, but 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 Peregrine appliance in your network. If one asset is being monitored by two appliances, the sequence number from one appliance 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.

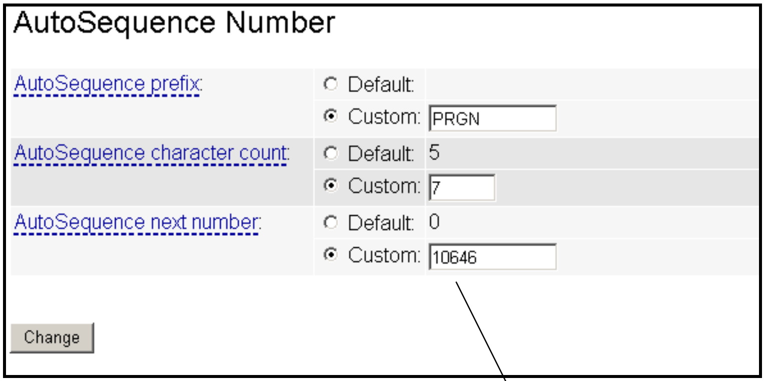
Note: If you enter a Next Number that is more digits than configured in the character count, the character count will automatically change to accommodate.

To configure AutoSequence numbers

1. Click **Administration** > **System Preferences** > **Scanned devices**.

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

3 Click **Change**.



AutoSequence Number

AutoSequence prefix:	○ Default:	
	● Custom:	PRGN
AutoSequence character count:	○ Default:	5
	● Custom:	7
AutoSequence next number:	○ Default:	0
	● Custom:	10646

The example above would produce the following number: PRGN0010646

Managing Scan Files

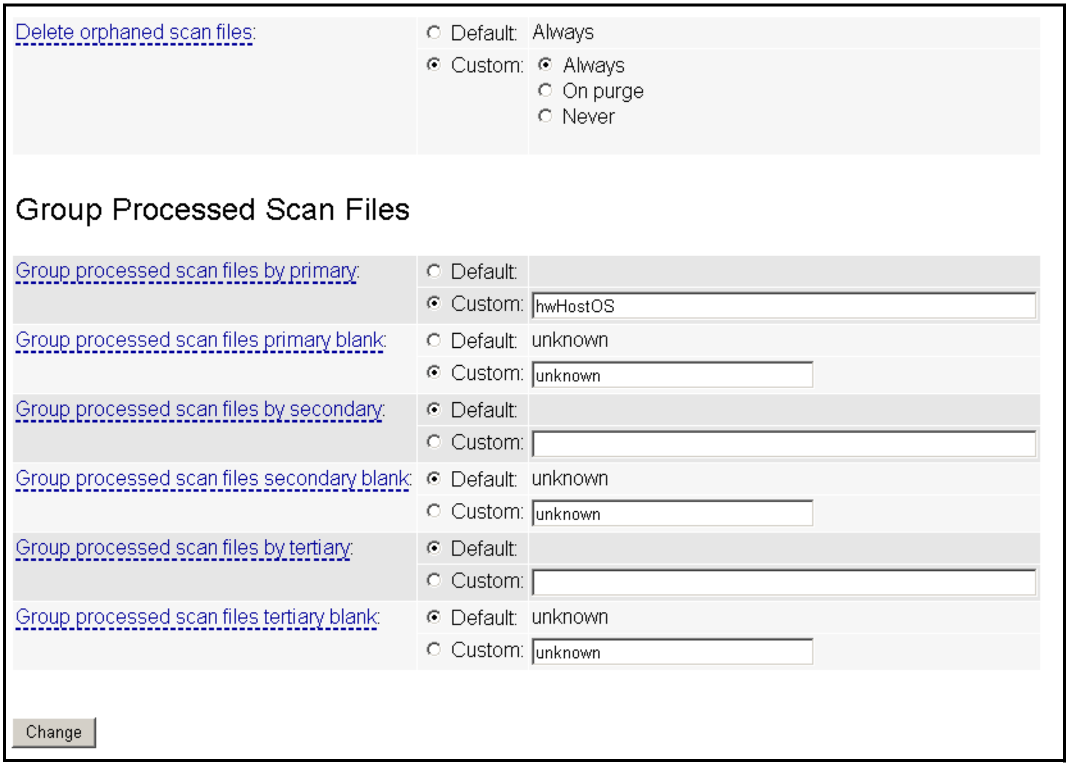
You can configure the following options to control scan file management:

- Delete Orphaned Scan Files
- Group Processed Scan Files

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:	○ Default:	Always
	● Custom:	● Always ○ On purge ○ Never

Group Processed Scan Files

Group processed scan files by primary:	○ Default:	
	● Custom:	hwHostOS
Group processed scan files primary blank:	○ Default:	unknown
	● Custom:	unknown
Group processed scan files by secondary:	● Default:	
	○ Custom:	
Group processed scan files secondary blank:	● Default:	unknown
	○ Custom:	unknown
Group processed scan files by tertiary:	● Default:	
	○ Custom:	
Group processed scan files tertiary blank:	● Default:	unknown
	○ Custom:	unknown

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 new scan file for that device is located in another folder.

You can use this feature to have Network 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

When you want to update the application library, do the following:

1 Copy the user SAI files to the /**sai** directory on the network share.

Note: The master.sai is automatically used from the sai8.apm package

2 In Network Discovery, click **Administration** > **Data Management** > **Validate SAI.**

3 Click **Validate**.

The enricher automatically finds and loads all SAI files located in the /**sai** directory when restarted.

Error messages

The following table shows the possible error messages you may come across and what they mean.

Error message	Meaning
A ReadOnly SAI is not allowed together with master and national SAIs	This happens if both a Read Only SAI and a Master SAI and/or National SAI is found
This file does not match the time stamp of the other master or national SAI files	This happens if Master/National SAIs with different timestamps are found.
This SAI type is not allowed here	The type of SAI file is not allowed. Not relevant for this release.
The <filename> is not a valid SAI	If a file is not a valid SAI file.
No SAI files found	No SAI files were found in the /**sai** share.
Too many SAI sets to add a new one. Delete some SAI sets.	There is a limit to the number of SAI sets that can reside in the \sai directory. This limit is 10 sets. Note: A set of SAIs consists of a group of SAI files you want to use together. If this limit is exceeded them this error message is displayed. You will have to delete a set of SAIs on the **Manage SAI** page: (**Administration > Data Management > Manage SAI**).
No new SAI to validate. Use ApE to create new SAI files and upload to the \sai directory.	A new SAI has not been found in the \sai directory.
Cannot copy file	The file could not be copied.
Invalid name. Valid characters are a-z, A-Z, 0-9 and underscore.	The file name uses invalid characters.
Invalid name. Maximum length is 20 characters.	The file name is too long.
SAI set named <sai name> is already in use.	The file name is already in use.

Error message	Meaning
Cannot create directory <dir name>	The directory name cannot be created.
“Cannot copy file <file name>	The file could not be copied.

6 CHAPTER Scanner Generator

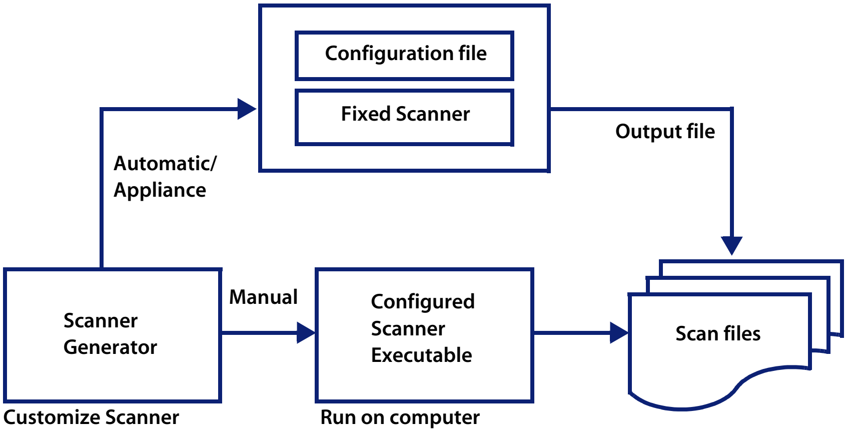
In this chapter you will find information on the following topics:

Introduction to the Scanner Generator when being used with Network Discovery

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, automatically using the scheduling mechanism on the appliance.

Figure 6-1: Summary of Scanner life cycle



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 appliance 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

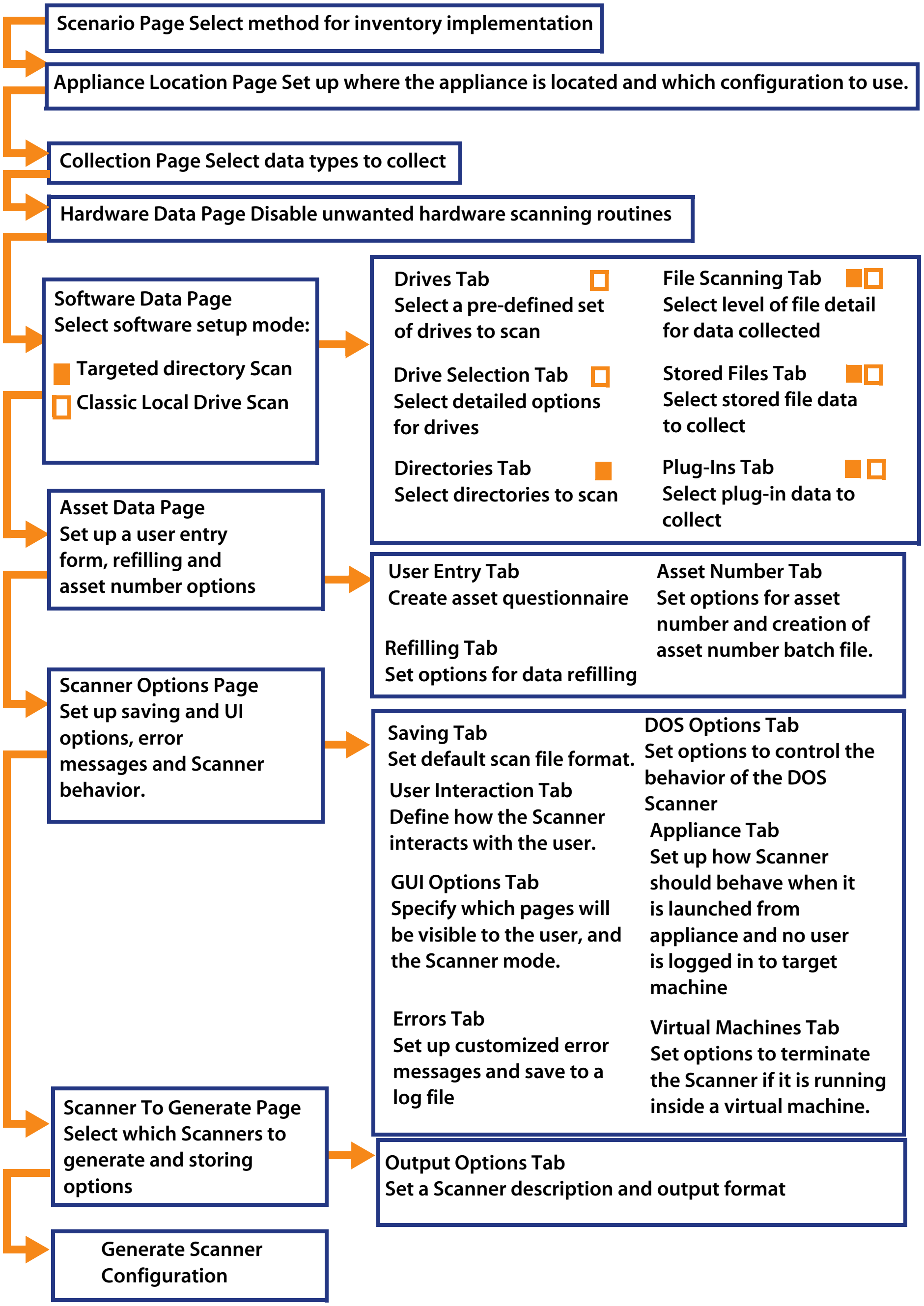
When used in stand-alone mode, the Scanner Generator generates self-contained Scanner executables that consist of a combination of the two files listed above.

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.

Appliance-based inventory



Scenario Page Select method for inventory implementation

Appliance Location Page Set up where the appliance is located and which configuration to use.

Collection Page Select data types to collect

Hardware Data Page Disable unwanted hardware scanning routines

Software Data Page
Select software setup mode:

■ Targeted directory Scan

□ Classic Local Drive Scan

Drives Tab □
Select a pre-defined set of drives to scan

Drive Selection Tab □
Select detailed options for drives

Directories Tab ■
Select directories to scan

File Scanning Tab ■□
Select level of file detail for data collected

Stored Files Tab ■□
Select stored file data to collect

Plug-Ins Tab ■□
Select plug-in data to collect

Asset Data Page
Set up a user entry form, refilling and asset number options

User Entry Tab
Create asset questionnaire

Refilling Tab
Set options for data refilling

Asset Number Tab
Set options for asset number and creation of asset number batch file.

Scanner Options Page
Set up saving and UI options, error messages and Scanner behavior.

Saving Tab
Set default scan file format.

User Interaction Tab
Define how the Scanner interacts with the user.

GUI Options Tab
Specify which pages will be visible to the user, and the Scanner mode.

Errors Tab
Set up customized error messages and save to a log file

DOS Options Tab
Set options to control the behavior of the DOS Scanner

Appliance Tab
Set up how Scanner should behave when it is launched from appliance and no user is logged in to target machine

Virtual Machines Tab
Set options to terminate the Scanner if it is running inside a virtual machine.

Scanner To Generate Page
Select which Scanners to generate and storing options

Output Options Tab
Set a Scanner description and output format

Generate Scanner Configuration

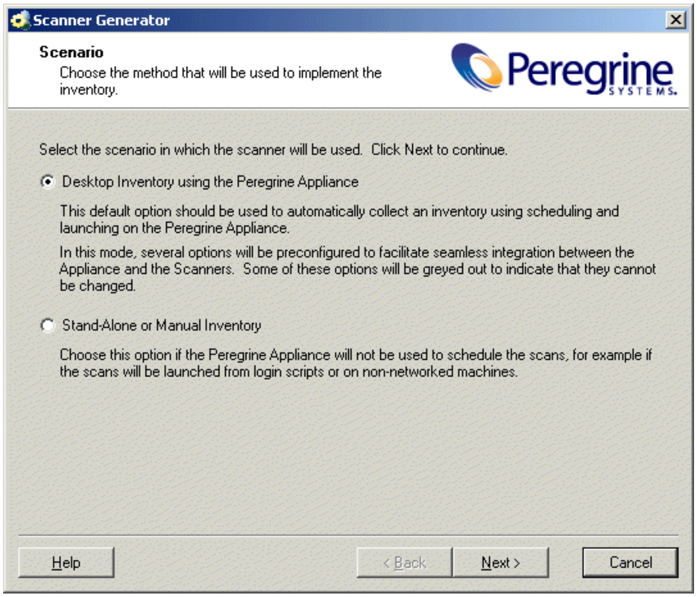
Differences in the Scanner Generator pages when in appliance mode

When you select the option the work in appliance mode, some parts of the Scanner Generator User Interface change. This section highlights those changes. For comprehensive information on the whole of the Scanner Generator User Interface refer to the *Desktop Inventory Users Guide*. Only changes from Stand-alone Desktop Inventory have been shown here.

The scenario page

On starting the Scanner Generator, the **Scenario** page appears.

- Select the Desktop Inventory using Peregrine appliance option.



Scenario

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

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

● Desktop Inventory using the Peregrine Appliance

This default option should be used to automatically collect an inventory using scheduling and launching on the Peregrine Appliance.

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

○ Stand-Alone or Manual Inventory

Choose this option if the Peregrine Appliance will not be used to schedule the scans, for example if the scans will be launched from login scripts or on non-networked machines.

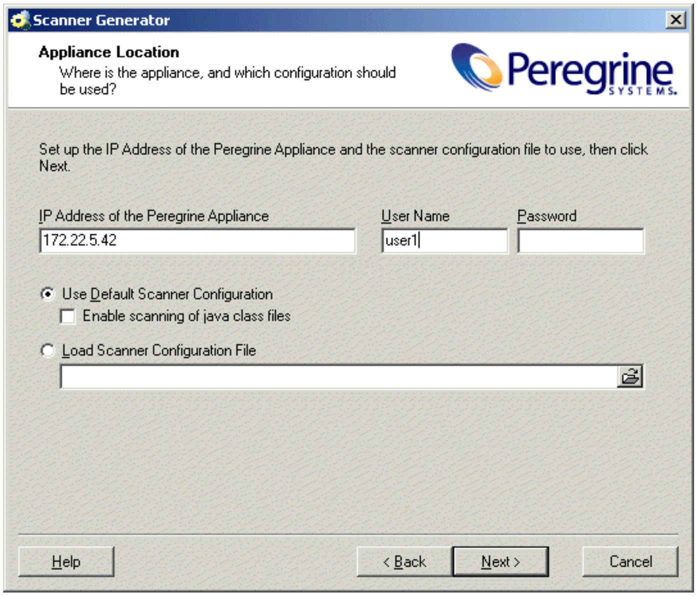
This option should be used to automatically collect an inventory using scheduling and launching on the appliance.

In this mode several options in the Scanner Generator have been preconfigured to facilitate the interoperability with between the Scanners and the Peregrine appliance. Some options will be greyed out to indicate they cannot be changed.

The Appliance Location page

This page will appear if you selected the **Desktop Inventory using the Peregrine Appliance** option on the **Scenario** page.

This page is used to set-up the appliance location and the configuration to be used for creating the Scanner file.



Appliance Location

Where is the appliance, and which configuration should be used?

Set up the IP Address of the Peregrine Appliance and the scanner configuration file to use, then click Next.

IP Address of the Peregrine Appliance: 172.22.5.42

User Name: user1

Password:

● Use Default Scanner Configuration

□ Enable scanning of java class files

○ Load Scanner Configuration File

To set up the appliance location:

1 Enter the IP address of the appliance.

2 Enter the **User Name** and **Password** to access the appliance. The User Names and Passwords are defined when the administrator sets up the accounts on the appliance.

Note: The Scanner Generator automatically maps the share “\\<*Appliance_IP_Address*>\share”. No drive letter is used for this mapping. The mapping will remain active even when the Scanner Generator is exited. If this is not desirable you can use the Windows Explorer’s **Tools** > **Disconnect Network Drive** menu command to disconnect from the appliance after terminating the Scanner Generator.

3 Select one of the following configuration sources:

a **Use default Scanner configuration**

Uses default configuration settings for the Scanner.

b **Load Scanner configuration File**

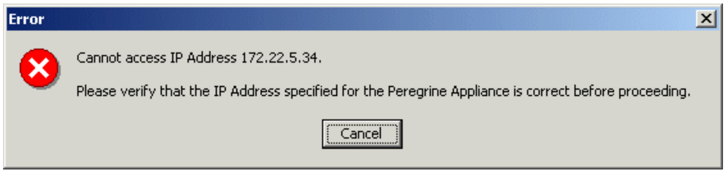
Reads the settings from a previously saved external configuration file (.cxz). This file contains the configuration settings only from a previous Scanner. Typically this file is 3 KB in size.

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.

4 Click the **Next** button to continue to the **Collection** page.

When the **Next** button is clicked, the Scanner Generator verifies that an appliance is available at the specified IP address. If not, an error message is displayed.



Error

Cannot access IP Address 172.22.5.34.

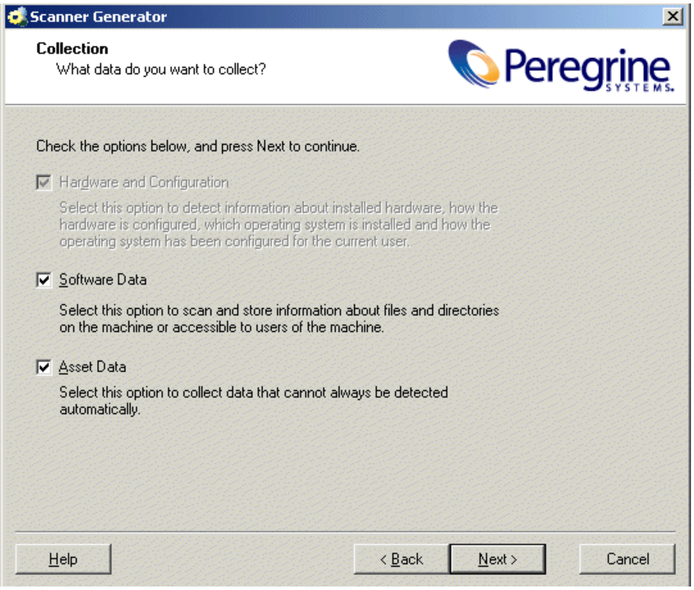
Please verify that the IP Address specified for the Peregrine Appliance is correct before proceeding.

The Standard Configuration page

This page is displayed if you selected the **Stand-Alone or Manual Inventory** option on the **Scenario** page.

The Collection page

The **Collection** page is used to select the computer data to be collected.



Scanner Generator

Collection

What data do you want to collect?

Check the options below, and press Next to continue.

☑ Hardware and Configuration

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

☑ Software Data

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

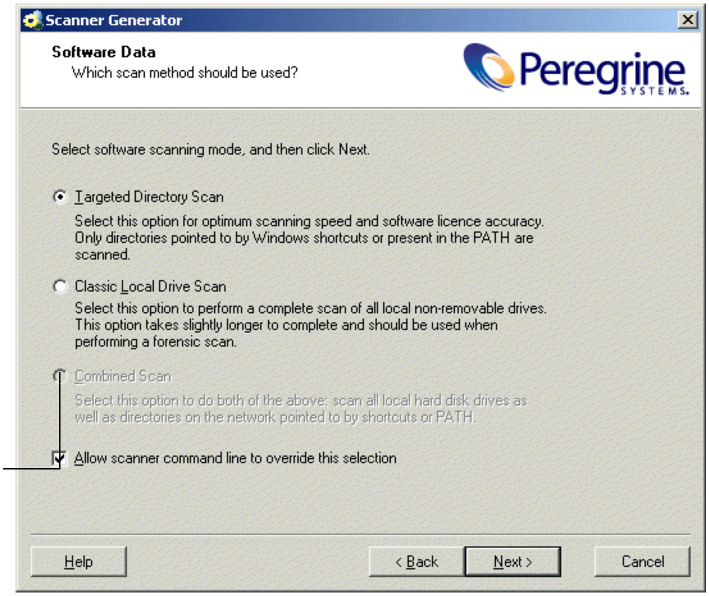
☑ Asset Data

Select this option to collect data that cannot always be detected automatically.

For inventories configured to use the appliance, the hardware option is always selected and cannot be disabled as shown in the screen shot above.

The Software Data page

The **Software Data** page is used to select the software scanning method.



Scanner Generator

Software Data

Which scan method should be used?

Select software scanning mode, and then click Next.

● Targeted Directory Scan

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

○ Classic Local Drive Scan

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

○ Combined Scan

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

☑ Allow scanner command line to override this selection

This option is disabled for appliance inventories

Combined Scan

Note: This option is disabled for appliance inventories.

The Refilling tab

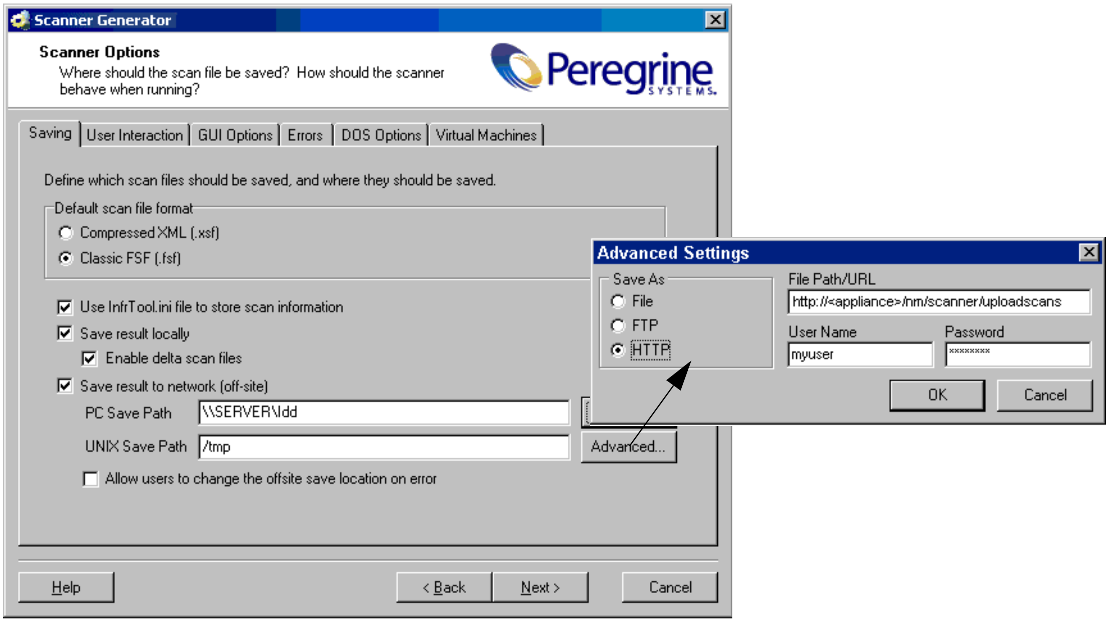
In **Desktop Inventory using the Peregrine Appliance** mode, the Scanners only save a local scan file, and this file is always used for refilling.

The Asset Number tab

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

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 exceptional conditions, as well as options for saving the inventory results.



Scanner Options

Where should the scan file be saved? How should the scanner behave when running?

Define which scan files should be saved, and where they should be saved.

Default scan file format

○ Compressed XML (.xsf)

● Classic FSF (.fsf)

☑ Use InfrTool.ini file to store scan information

☑ Save result locally

☑ Enable delta scan files

☑ Save result to network (off-site)

PC Save Path: \\SERVER\ldd

UNIX Save Path: /tmp

□ Allow users to change the offsite save location on error

Save As

○ File

○ FTP

● HTTP

File Path/URL: http://<appliance>/nm/scanner/uploadscans

User Name: myuser

Password: ********

The Saving tab

The **Saving** tab page is used to set options for saving the inventory results. This is the location where you can enable/disable the delta scanning feature (by default, it is disabled).

Special Case: Using Delta Scanning with UNIX Scanners

There are no Listeners available for UNIX. Therefore, if you want to use delta scanning with your UNIX devices, you must configure access to the Peregrine appliance over HTTP, and use a script to check and transmit scan file data.

In order to work properly, the scanner must be able to compare the scanfile ID on the Peregrine appliance with its own scanfile ID. If both scan files have the same ID, the scanner can then send the delta data to the Peregrine appliance.

First you must set up the Scanner Options page with the correct data. Then, you must use a script to run when doing your delta scanning.

Set up Scanner Options

1 Select **Enable delta scan files**.

2 Select **Save result to network (off site)**.

3 Click the **Advanced** button next to **UNIX Save Path**.

   The **Advanced Settings** dialog appears.

4 Under **Save As**, select **HTTP**.

5 Under **File Path/URL**, enter **http://<*appliance*>/nm/scanner/uploadscans**

   <*appliance*> is the IP address of your Peregrine appliance.

6 Enter the user name and password that you created in Step 4: Add a Scanner Account on the appliance (optional) on page 38).

7 Click **OK**.

8 To continue with the Scanner Generator, click **Next**.

To set up a script

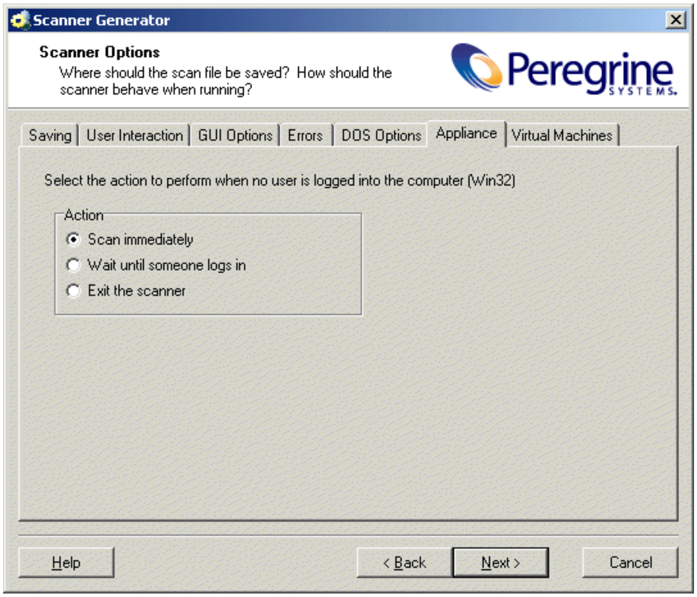
1 You must use a script that calls for the scan file ID at the following URL:

   http://<appliance>/nm/scanner/getscanid.pcgi?AssetTag=<asset_tag>

2 You can download a script from the Download directory on the Peregrine appliance. Click **Download > deltascan.pl**.

The Appliance tab

The **Appliance** tab is used to choose how the scanner should behave when it is launched from the appliance and no user is logged in to the target machine.



Scanner Generator

Scanner Options

Where should the scan file be saved? How should the scanner behave when running?

Select the action to perform when no user is logged into the computer (Win32)

Action

● Scan immediately

○ Wait until someone logs in

○ Exit the scanner

To define the behavior of the Win32 scanner when no user is logged in, select one of the available options:

1 Scan Immediately

   No special action is taken by the scanner. Note that the information collected will be limited by the fact that no user is logged in.

2 Wait until someone logs in

   The scanner sleeps until a user logs in to the machine, at which point the scanner scans the machine. Full information can be collected by the scanner.

3 Exit the scanner

The scanner terminates and does not collect a scan file.

The Scanners To Generate page

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

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 appliance based inventories only, the option to name the configuration (.cxz) file.

Note: The configuration file is saved on the appliance as well, using the same file name as the copy specified here.

The Generating Scanners page

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

Now that you have generated Scanner configuration files for the Scanners you want. These will now have to be validated for use on the appliance.

This is necessary to ensure that the configuration options chosen are compatible with scanners being deployed automatically.

To validate a scan configuration:

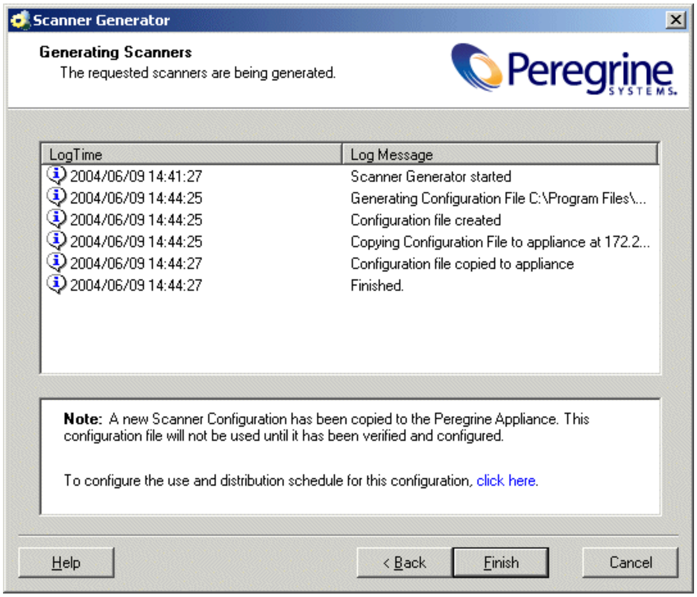
1 Choose the name of the configuration file from the drop-down list.

2 Click **Validate**.

If the configuration is valid, a message **The configuration is now in use** is shown.

If you selected the Desktop Inventory using the Peregrine Appliance option on the first page of the Scanner Generator, then the following screen will be displayed when the Scanner configuration file has been created and copied to the appliance.

Note: Only a configuration file is created for an appliance mode inventory.



Generating Scanners

The requested scanners are being generated.

```
LogTime               Log Message
2004/06/09 14:41:27   Scanner Generator started
2004/06/09 14:44:25   Generating Configuration File C:\Program Files\...
2004/06/09 14:44:25   Configuration file created
2004/06/09 14:44:25   Copying Configuration File to appliance at 172.2...
2004/06/09 14:44:27   Configuration file copied to appliance
2004/06/09 14:44:27   Finished.
```

Note: A new Scanner Configuration has been copied to the Peregrine Appliance. This configuration file will not be used until it has been verified and configured.

To configure the use and distribution schedule for this configuration, click here.

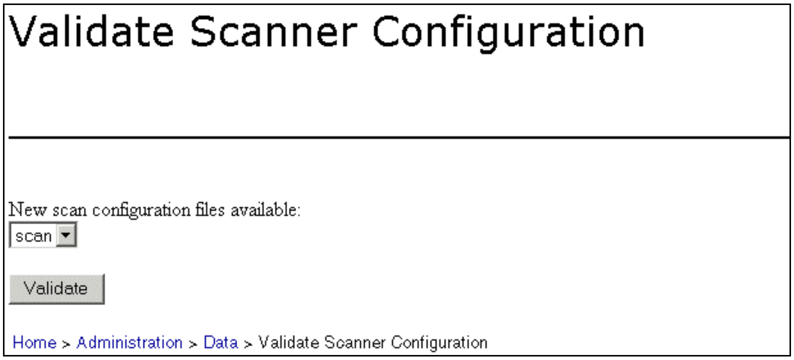
If the Scanner configuration cannot be copied to the appliance for some reason, an error message is displayed in the log and the bottom panel does not appear.

In this case, check that you have write access to the share directory on the target appliance. It may also occur if another scan configuration with the same name already exists on the appliance.

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.

1 Click on the hyperlink to access the appliance web pages to configure the use and distribution schedule for this configuration. The following web page is displayed.



Validate Scanner Configuration

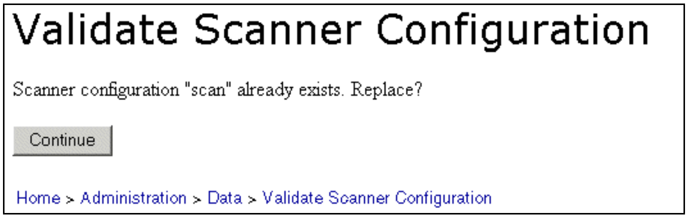
New scan configuration files available:

Home > Administration > Data > Validate Scanner Configuration

2 Select the Scanner configuration file that you have just generated from the pull-down list. In this example the configuration file was called scan.

3 Click the Validate button.

If the scanner configuration already exists, you will be presented with the following screen.



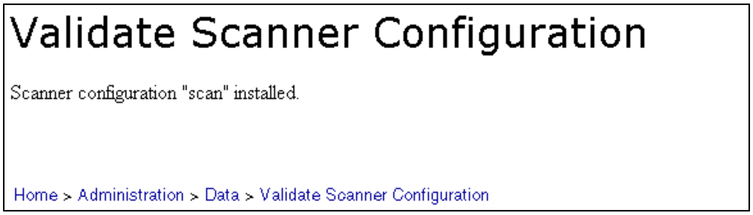
Validate Scanner Configuration

Scanner configuration "scan" already exists. Replace?

Home > Administration > Data > Validate Scanner Configuration

4 Click the **Continue** button if you want to replace the Scanner configuration.

A confirmation message will be displayed informing you that the Scanner has been successfully installed.



Validate Scanner Configuration

Scanner configuration "scan" installed.

Home > Administration > Data > Validate Scanner Configuration

If the Scanner configuration is not valid for an automated appliance-based inventory, a list of error messages is displayed instead. To proceed, correct the problems in Scanner Generator and generate a new Scanner configuration to proceed.

What happens if the file is not valid

The following table lists the possible error messages you may encounter when validating a Scanner configuration file:

Error message	Explanation
File is not a scanner configuration file; cannot read	The file type is not a Scanner configuration file (.cxz).
Hardware detection is disabled	The Scanner configuration file has been created with hardware detection disabled. For a Scanner configuration file to be valid, hardware detection must be enabled.
Network detection is disabled	The Scanner configuration file has been created with network detection disabled. For a Scanner configuration file to be valid, network detection must be enabled.

Error message	Explanation
Local FSF save is disabled	The Scanner configuration file has been created with the Local FSF save setting disabled. For a Scanner configuration file to be valid, this setting must be enabled.
Use of **InfrTool.ini** is disabled	The Scanner configuration file has been created with the **InfrTool.ini** setting disabled. For a Scanner configuration file to be valid, this setting must be enabled.

PEREGRINE

Index

Peregrine SYSTEMS

11/23/04