

Peregrine

Network Discovery

Using Network Discovery with Desktop Inventory and Desktop Administration

Version 5.1.2

Copyright © 2003 Peregrine Systems, Inc. or its subsidiaries. All rights reserved.

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

Peregrine Systems® and Network Discovery® are registered trademarks of Peregrine Systems, Inc. or its subsidiaries. Microsoft, Windows, Windows NT, Windows 2000, and other names of Microsoft products referenced herein are trademarks or registered trademarks of Microsoft Corporation. DB2 is a registered trademark of International Business Machines Corp.

This document and the related software described in this manual are supplied under license or nondisclosure agreement and may be used or copied only in accordance with the terms of the agreement. The information in this document is subject to change without notice and does not represent a commitment on the part of Peregrine Systems, Inc. Contact Peregrine Systems, Inc., Customer Support to verify the date of the latest version of this document.

The names of companies and individuals used in the sample database and in examples in the manuals are fictitious and are intended to illustrate the use of the software. Any resemblance to actual companies or individuals, whether past or present, is purely coincidental.

If you need technical support for this product, or would like to request documentation for a product for which you are licensed, contact Peregrine Systems, Inc. Customer Support by email at support@peregrine.com.

If you have comments or suggestions about this documentation, contact Peregrine Systems, Inc. Technical Publications by email at doc_comments@peregrine.com.

This edition of the document applies to version 5.1.2 of the licensed program.

Peregrine Systems, Inc.
3611 Valley Centre Drive San Diego, CA 92130
Tel 800.638.5231 or 858.481.5000
Fax 858.481.1751
www.peregrine.com



Contents

Chapter 1	Introduction	7
	The interaction of the components of Network Discovery and Desktop Inventory	9
	The Peregrine Appliance	10
	The automatic deployment of Scanners	10
	Scheduling of scan execution	11
	Collection and storage of scan files	11
	The Agent.	12
	Scan file enrichment	13
Chapter 2	Sharing Security Keys between Network Discovery and Desktop Administration	15
	Putting the Peregrine appliance security keys onto Desktop Administration . .	18
	Putting the Desktop Administration security keys onto the Peregrine appliance	23
Chapter 3	Sharing Security Keys between your Peregrine Appliances	25
Chapter 4	Setting up Network Discovery to work with Desktop Inventory	29
	The automatic deployment of Scanners	30
	Steps	30
	Step 1: Map a drive from Windows workstation to the appliance shared directories	31
	Step 2: Make Network Discovery and Desktop Inventory 'aware' of each other	33
	Step 3: Run Scanner Generator, generate and validate your Scanner configuration files (Windows workstation and appliance)	35
	Step 4: Add or define a Scanner Property Group on the appliance	36
	Step 5: Define a Listener Property Group on the appliance	41

	Step 6: Apply the Scanner and Listener property groups with one or more IPv4 ranges (appliance)	42
	Step 7: Submit and activate your changes	44
	Step 8: Deploy the Listeners to your workstations	45
	Downloading the Listener programs from the appliance	46
	Install the QuickDeploy Manager Console	47
	Saving the response.ans file	48
	Using QuickDeploy from the Manager Console to deploy the Agent module	48
	Manually installing the Agents from a browser on the local Workstation	53
Chapter 5	The XML Enricher	55
	Operating principles	55
	The XML Enricher directory structure.	56
	Checking the status of the Enrichment process	58
	Disk space requirement	58
	Structure of the enriched xml.gz file.	60
	An example of how the data is stored	60
	Launching the XML Enricher from the appliance	63
	Starting and stopping the XML Enricher service	63
	Configuring the XML Enricher on the appliance	64
	Updating the application library used by the Enricher	66
Chapter 6	Scanner Generator	69
	Introduction to the Scanner Generator when being used with Network Discovery	70
	The components of a Scanner	70
	The Scanner Generator pages	72
	Differences in the Scanner Generator pages when in appliance mode	73
	The scenario page	73
	The Appliance Location page	74
	The Standard Configuration page	75
	The Collection page	76
	The Software Data page	77
	The Refilling tab	77
	The Asset Number tab	77
	The Scanner Options page	78

The Scanners To Generate page 80
The Generating Scanners page 80
Index. **83**

1 Introduction

CHAPTER

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:

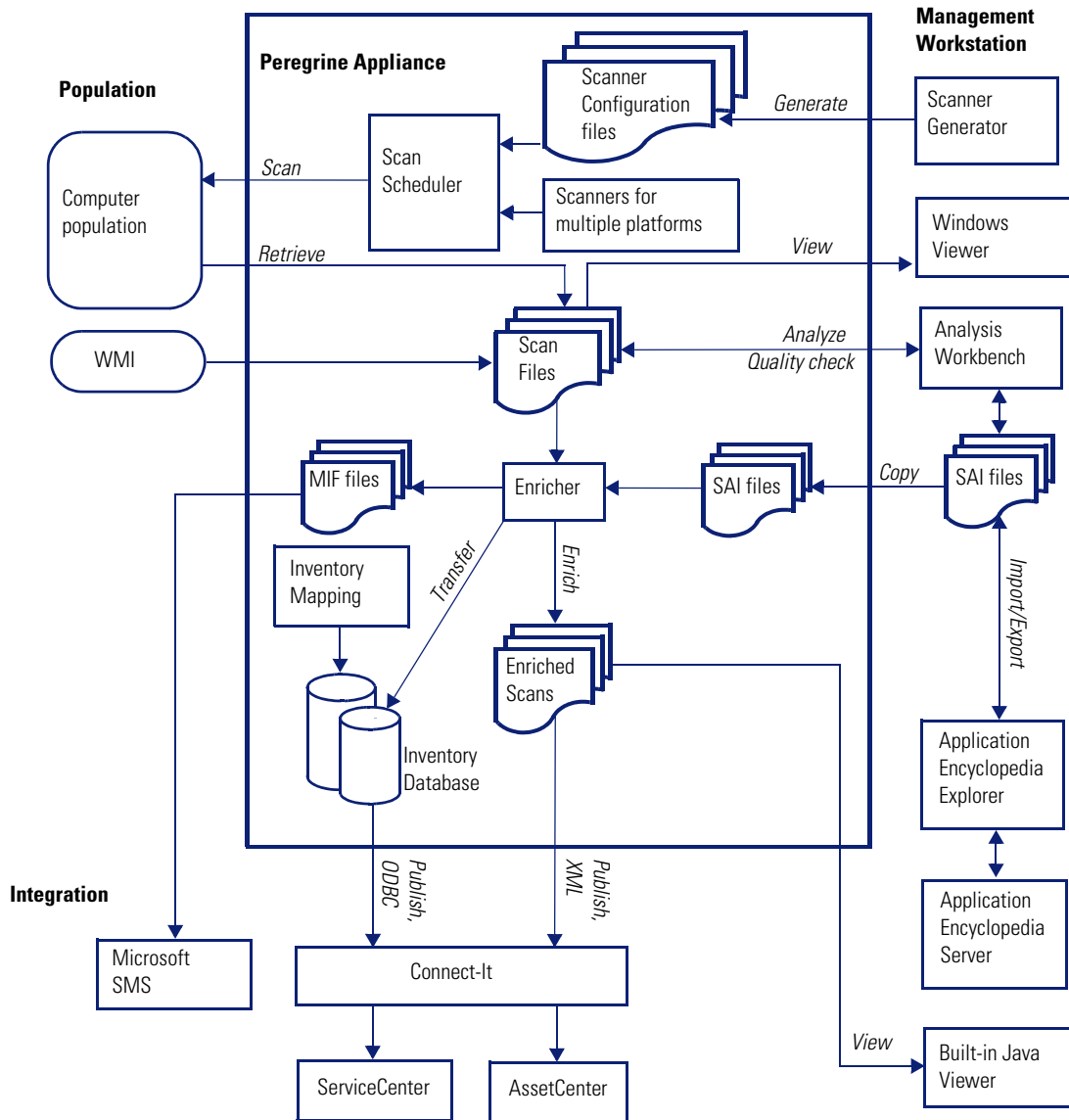
- Automatic Administration
 - Configure remote computers.

- 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 29 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.



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 29 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 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 29 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 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 29.

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 xml.gz format. This process is called scan file enrichment.

Further information

For further information about the XML Enricher, refer to *The XML Enricher* on page 55.

2 Sharing Security Keys between Network Discovery and Desktop Administration

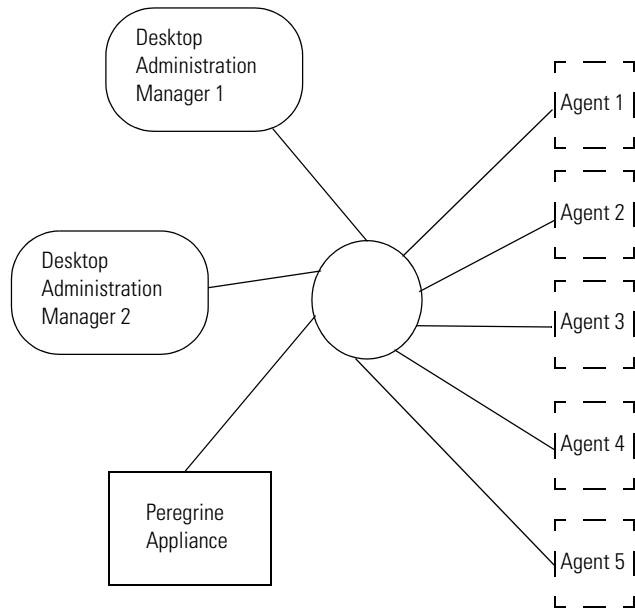
CHAPTER

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 they 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 25.



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 18
- *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: <ul style="list-style-type: none"> ■ 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.” 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=ifltsnr
 - 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

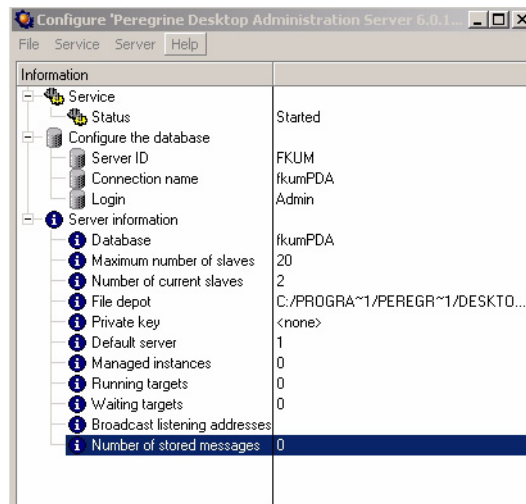
- 4 Exit the program.

Install the security key into the Server Configuration

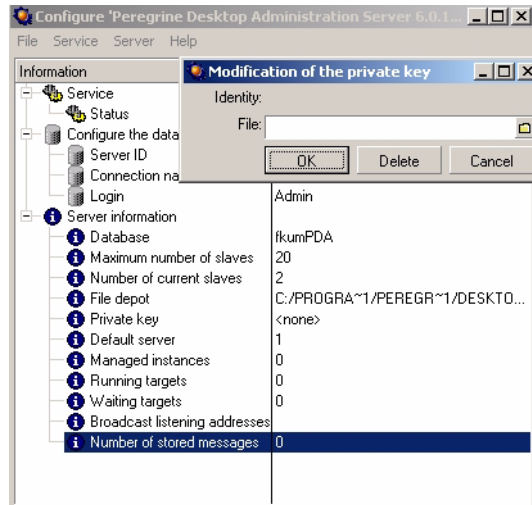
The file you altered in the previous procedure must now be installed in the Desktop Administration Server Configuration program.

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

The Server Configuration Tool appears.



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



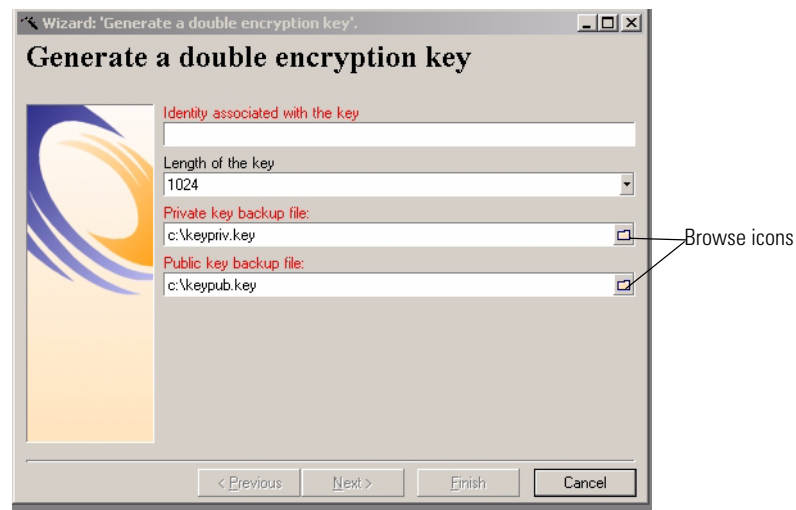
- 3 Click the “browse” icon, and choose the private key file from the floppy disk.
- 4 Click OK.
- 5 Exit the program.

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.



- 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**.

- 13** 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
```

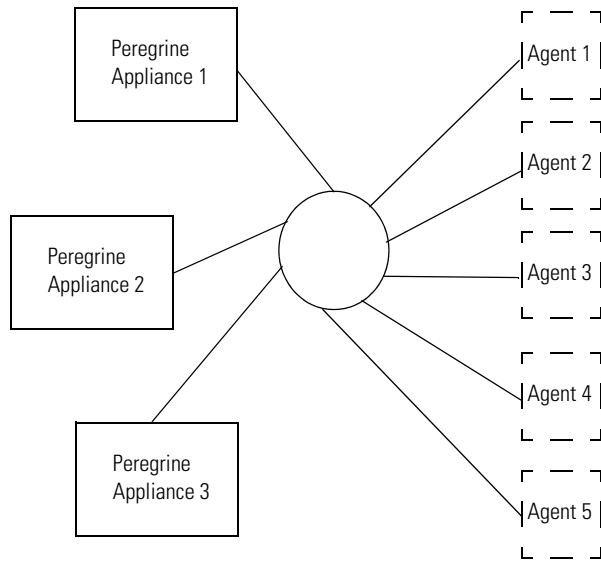
- 14** Press **Enter**.

- 15** Exit the program.

3 Sharing Security Keys between your Peregrine Appliances

CHAPTER

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 Setting up Network Discovery to work with Desktop Inventory

CHAPTER

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 between Network Discovery and Desktop Administration* 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, 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, 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: Map a drive from Windows workstation to the appliance shared directories on page 31.*
- *Step 2: Make Network Discovery and Desktop Inventory 'aware' of each other on page 33.*
- *Step 3: Run Scanner Generator, generate and validate your Scanner configuration files (Windows workstation and appliance) on page 35.*
- *Step 4: Add or define a Scanner Property Group on the appliance on page 36.*
- *Step 5: Define a Listener Property Group on the appliance on page 41.*
- *Step 6: Apply the Scanner and Listener property groups with one or more IPv4 ranges (appliance) on page 42.*

- *Step 7: Submit and activate your changes* on page 44.
- *Step 8: Deploy the Listeners to your workstations* on page 45.

Step 1: 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.
- Scanners 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, XP and any other platform supported by a Samba SMB Client.

For Win98 and WinME there are some other restrictions:

- The Win98/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 2: 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:

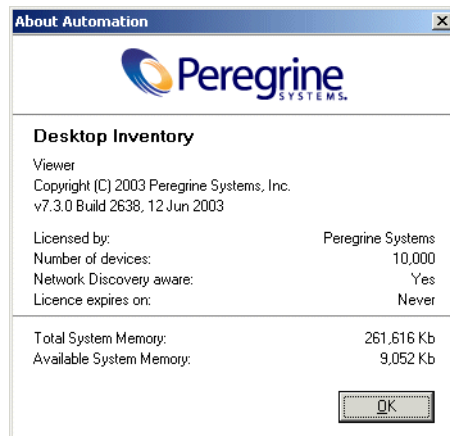
- 1 From your management workstation, login to the Network Discovery.
- 2 Click **Download**.
- 3 On the Download page, click on the **DI-ND.reg** file.
The “File Download” dialog appears.
- 4 Click **Open** to run the file.
The Registry Editor appears.
- 5 Click **Yes** to enter your information into 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:

`\license\incoming`

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.

- 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.



The two applications can now work with each other.

- 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 3: 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 Chapter 4 of this guide.

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 7.3.0 > 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 4: 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 6: Apply the Scanner and Listener property groups with one or more IPv4 ranges (appliance)* on page 42).

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:

Description:

Select for all scanners:

or select individually:

Win32 scanner:

HP/UX scanner:

Linux scanner:

AIX scanner:

Solaris scanner:

Bandwidth Threshold: Set Inherit

Frequency: Set Inherit
 Weeks: Days: Hours:

Scanner upgrade schedule:

Scanner run schedule:

Scan file download schedule:

- 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.
- <hwnonly> - 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 35 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 it's 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.

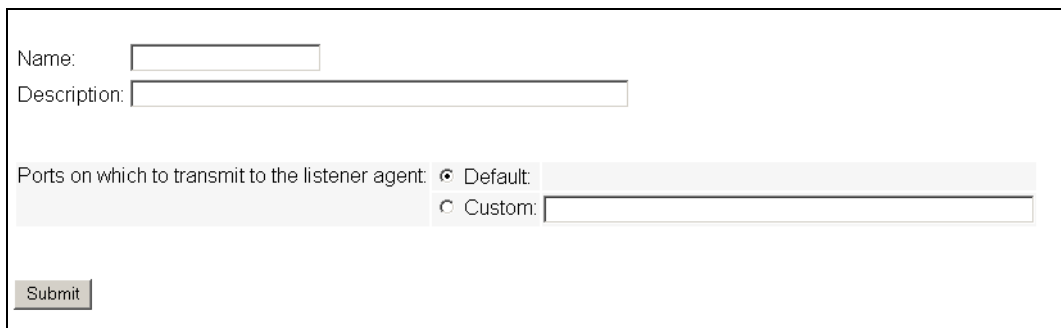
- ▶ Select an option from the **Scan file download schedule** drop down list.

Step 5: 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 6: Apply the Scanner and Listener property groups with one or more IPv4 ranges (appliance)* on page 42).

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 44 for an explanation of the purpose of the **Activate changes** page.

Step 6: 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 address.

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**.

The screenshot shows a web form for configuring an IPv4 range. It includes the following fields and options:

- IPv4 Range:**
 - Add by interval
 - Add by subnet
 - Starting IPv4 Address:
 - Ending IPv4 Address:
 - IPv4 Address:
 - Netmask:
- Location of range in tree:**
 - Default
 - Custom
- Property Set/Group:**
 - Choose existing Property Set/Group:
 - or, if there is not one that matches your requirements...
 - Add new Property Set:
 - Name:
 - Description:
 - Network property groups:
 - Community property groups:
 - Scanner property groups:
 - Listener property groups:

A **Submit** button is located at the bottom left of the form.

- 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 4: Add or define a Scanner Property Group on the appliance* on page 36. (**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 41.
- 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 7: Submit and activate your changes*.

Step 7: 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 8: 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 email 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:

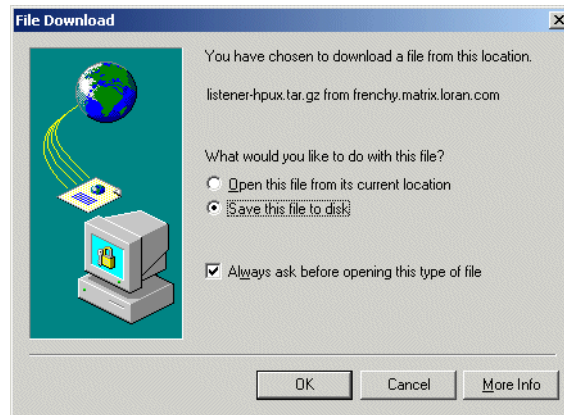
- 1 Login to the appliance.
- 2 On Network Discovery, click the **Download** link. The **Download** download page is displayed.

Filename	Size	Description
agent.exe	972.27 kilobytes	Listener agent for Windows
DI-ND.reg	476 bytes	Registry entry to Enable Network Discovery Awareness features in Desktop Inventory
j2re-1_4_2-windows-1586.exe	13.51 megabytes	Java Runtime Engine for Windows
manager.exe	972.27 kilobytes	Windows console for QuickDeploy
MyODBC-source-2.50.39.tar.gz	221.40 kilobytes	MySQL ODBC driver source code
MyODBC-Windows-2.50.39.tar.gz	1.46 megabytes	MySQL ODBC driver
PeregrineHostMIB3.exe	1.09 megabytes	Host MIB for Windows NT
PeregrineTrapMIB.bt	10.39 kilobytes	Peregrine MIB for SNMP Trap notifications
SumRepExample.doc	67.50 kilobytes	Document to create MS Word based reports
SumRepTemplate.dot	83.50 kilobytes	Template to create MS Word based reports

- 3 There are several 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.



- 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.

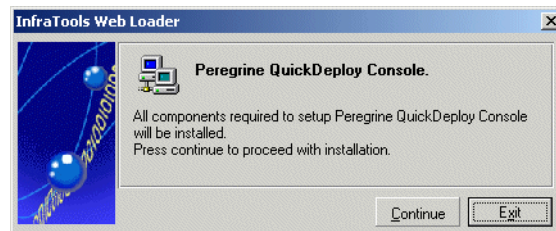
Install the QuickDeploy Manager Console

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

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.



- 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:

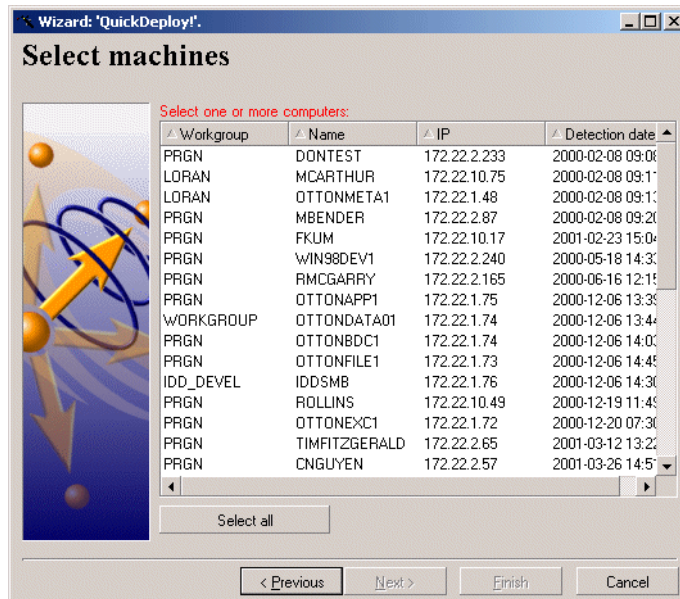
- 1 From the Workstation where the Manager was installed (see previous procedure), click **Start > Programs > Peregrine > Remote Control > Manager**.

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

- 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

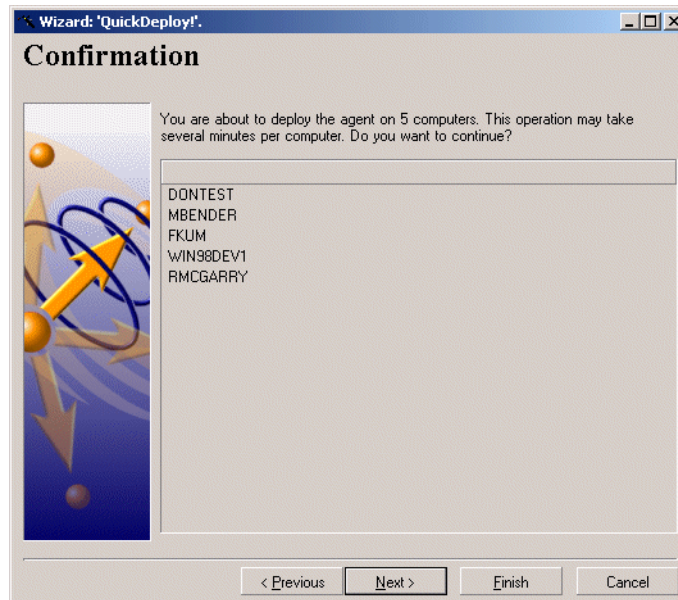
- Click the **Next** button to continue to the **Select machines** page of the Wizard.



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

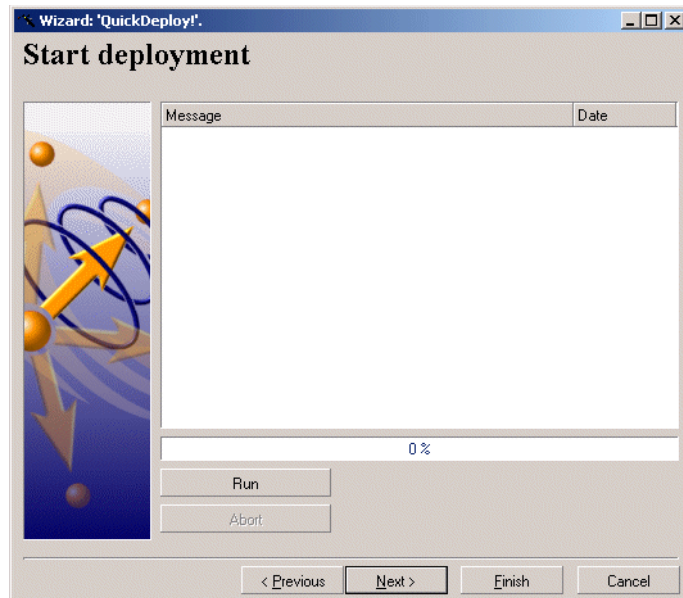
- Select the computers on which you want to remotely install the Agent module.

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



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.



- 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.



- 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.

5 The XML Enricher

CHAPTER

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 (`xml.gz` or `fsf` 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 `.xml.gz` format is created and the original scan file is deleted. If an error occurs, the original scan file is moved to a failure directory and is not deleted.

Important: If an enriched scan file for the same asset already exists, the old file is overwritten. The XML Enricher does not support the storing of historical data.

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.

Viewer and Analysis Workbench can then use this location for analysis or the scan file can be processed by a Connect-It scenario.

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	<p>The scan file is moved to this location if it is a device that the network discovery side does not know about yet.</p> <p>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.</p>
\scans\deferred\firstscan	<p>If the Automatically defer all new scans option was set (see <i>Configuring the XML Enricher on the appliance</i> on page 64.) the scan file is not processed.</p> <p>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</p> <p>This allows the administrator to review the asset and application data.</p> <p>When you are satisfied that the data is ok, you can move it back to the incoming directory.</p> <p>Note, that new scan files from a computer will not be processed while a scan file for it exists in this directory.</p>

Directory	Explanation
<code>\scans\failed</code>	The base failure directory. Failed scans are moved to a sub directory of this.
<code>\scans\failed\corrupt</code>	Scans that cannot be read or may not be scan files are moved here.
<code>\scans\failed\error</code>	When any other error occurs, scan files are moved here.
<code>\scans\failed\filter</code>	The scan ends up here if it has an IP address outside a range that has been configured to allow scanned devices.
<code>\scans\failed\licence</code>	If too many scans are processed, new scans are moved here.
<code>\scans\failed\old</code>	Scan files that are copied to incoming but are older than the one already in the database are moved here.
<code>\scans\incoming</code>	The incoming directory. The enricher looks for new scan files here.
<code>\scans\processed</code>	The processed directory. Enriched scan files are created here.
<code>\scans\processed\mif</code>	The MIF directory. If enabled, MIF files are created here.

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			
	Number of unprocessed scan files:	0			
	Failures due to stale scan files:	0	-		
	Failures due to insufficient scan licences:	0	-	▲	2003-06-14 15:33
	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.

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 click **Find**.
- 4 If a match is found, a hyperlink for the match is listed in the **Find** window and a **Device Manager** session opens automatically for the appliance.

- 5 Scroll down to the **Disk:/** setting and click on the link.

	Virtual Memory: Swap Space	2 GB	0.3035 of 2 GB = 15.18%
▲	IM10294 Disk: /	988.2 MB	476.6 of 988.2 MB = 48.23%
-	Disk: /backup1	12.82 GB	0.6938 of 12.82 GB = 5.41%
-	Disk: /backup2	13.06 GB	6.1e-05 of 13.06 GB = 0.00%
-	Disk: /boot		
*	Disk: /data		

Parameter	Value															
Name:	Disk															
Description:	/															
Volume label:	YYY1															
Serial number:	XXX1															
Units:	MB															
Maximum value:	988.2															
Assigned thresholds:	<table border="1"> <thead> <tr> <th>Low</th> <th>High</th> <th>State</th> </tr> </thead> <tbody> <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> </tbody> </table>	Low	High	State	10 %	30 %	✱	30 %	50 %	▲	50 %	90 %	◆	90 %	+	■
Low	High	State														
10 %	30 %	✱														
30 %	50 %	▲														
50 %	90 %	◆														
90 %	+	■														
State:	▲															
Value:	476.6 of 988.2 MB = 48.23%															
Ticket:	IM10294															

- 6 In the example above, 476.6 of 988.2 MB (48.23%) 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:	51 %	-	2003-06-13 07:11
	Boot Partition:	3 %	-	
	Primary Data Partition:	11 %	-	
	Secondary Data Partition:	13 %	-	
	Primary Data Backup Partition:	6 %	-	
	Primary Data Backup Partition:	6 %	-	

Structure of the enriched xml.gz 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\7.3.0\Common

Note: The file is a text file, but is easiest to read with an XML reader.

An `xml.gz` 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 `xml.gz` 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>
  <application versionid="1111"
    publisher="Microsoft"
    application="Word" apptype="Office App"
    version="2000 sp2" release="2000" os="win" lang="en"
    licencedby="2222"
  />
  <application versionid="2222"
    publisher="Microsoft"
    application="Office" apptype="Office App"
    version="2000 sp2" release="2000" os="win" lang="en"
  />
</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.driv
[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 versionid="1111"
    publisher="Microsoft"
    application="Word" apptype="Office App"
    version="2000 sp2" release="2000" os="win" lang="en"
    licencedby="2222"
  />
  <application versionid="2222"
    publisher="Microsoft"
    application="Office" apptype="Office App"
    version="2000 sp2" release="2000" os="win" lang="en"
  />
/>

```

The section of code above could be found for a computer with just two applications on it: Microsoft Office 2000 and Word 2000 (with Service Pack 2 installed). The “licensedby” attribute indicates that MS Word is licensed by MS Office. In other words, while both are licensable applications, this computer requires 1 licence for Microsoft Office - with this licence, no separate Word 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:	<input checked="" type="radio"/> Default: Yes <input type="radio"/> Custom: <input checked="" type="radio"/> Yes <input type="radio"/> 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

To configure the XML Enricher on the appliance:

- 1 Click **Administration > System Preferences > Scanned Devices**. The **XML Enricher Configuration** page is displayed.

The screenshot shows the XML Enricher Configuration page with the following settings:

- 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
 - MAC Address
 - Asset tag
 - Scan filename
 - NetBIOS name and Windows domain
 - Custom:

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

A **Change** button is located at the bottom left of the configuration area.

- 2 Set the options as required.

Option	Description
Application Recognition	
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.

Option	Description
No Application Recognition	<p>No files are sent to the recognition engine for processing.</p> <p>In this state, no <applicationdata> section will be added to the scan files.</p>
Generate MIF Files	
Always	The XML enricher will always produce MIF files from scan files.
Never	The XML enricher will never produce MIF files from scan files. This is the default option.
When SMS is detected	Only scan files with a value in the hwOSMIFPath field will cause a MIF file to be produced (i.e. computers where the SMS client is installed).
Automatically defer all new scans	
Yes	<p>If enabled, the following happens when a scan file is found in incoming:</p> <ul style="list-style-type: none"> ■ 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. <p>This means that it is possible to control the process if this option is enabled.</p> <p>When a new computer is scanned for the first time, the data is not added to the database until it has been reviewed and the scan file has been moved back to the incoming directory.</p>
No	This is the default option.
Merge Priority	See description below

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.

Updating the application library used by the Enricher

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

- 1 Copy the complete set of SAI files to the `/sai` directory on the network share.
- 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.

Error message	Meaning
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.
Only a User.Sai file found; a Master SAI must also exist	Only a User SAI was found. No Master SAI file was found. For a User SAI file to be used, a Master SAI file must also exist.
Only one User.Sai file is allowed	Multiple User SAI files were found in the directory.
Too many SAI sets to add a new one. Delete some SAI sets.	<p>There is a limit to the number of SAI sets that can reside in the \sai directory. This limit is 10 sets.</p> <p>Note: A set of SAIs consists of a group of SAI files you want to use together.</p> <p>If this limit is exceeded then this error message is displayed. You will have to delete a set of SAIs on the Manage SAI page: (Administration>Data Management>Manage SAI).</p>
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.
Cannot create directory <dir name>	The directory name cannot be created.
"Cannot copy file <file name>	The file could not be copied.

6 Scanner Generator

CHAPTER

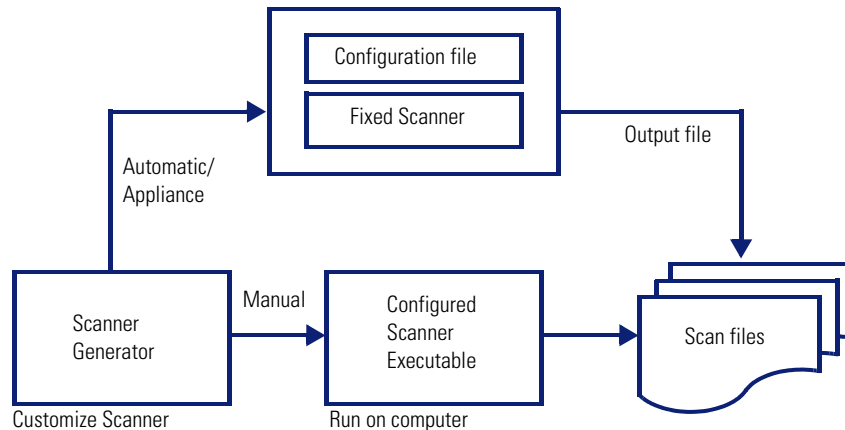
In this chapter you will find information on the following topics:

- *Introduction to the Scanner Generator when being used with Network Discovery* on page 70
- *The Scanner Generator pages* on page 72
- *Differences in the Scanner Generator pages when in appliance mode* on page 73

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

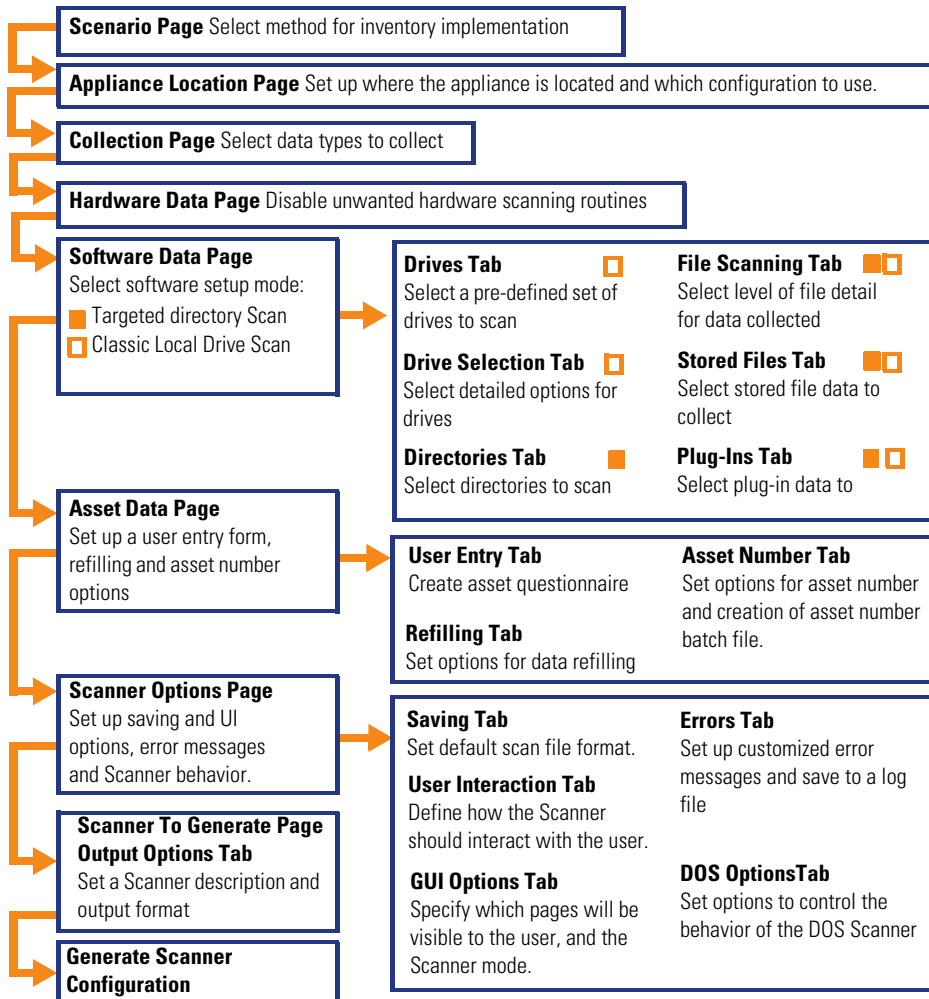
When used in stand-alone mode, the Scanner Generator generates self-contained Scanner executables that consist of a combination of the two files listed above.

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



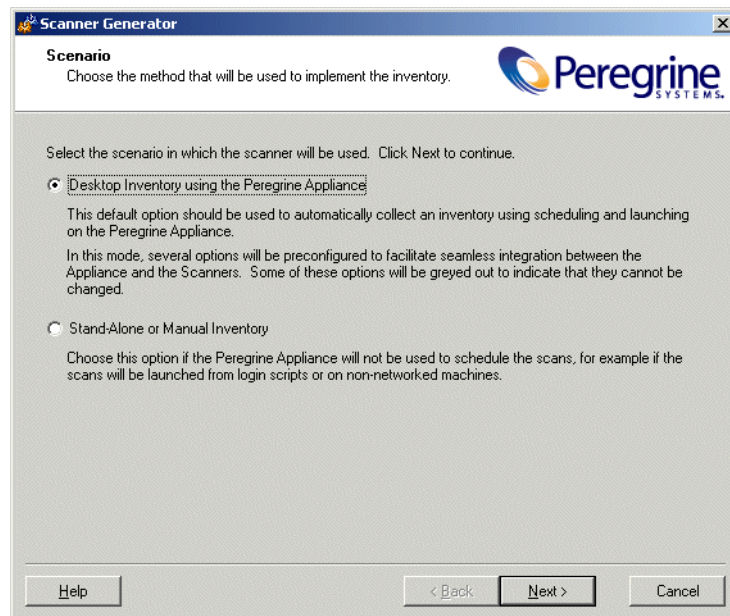
Differences in the Scanner Generator pages when in appliance mode

When you select the option to 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.



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.

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

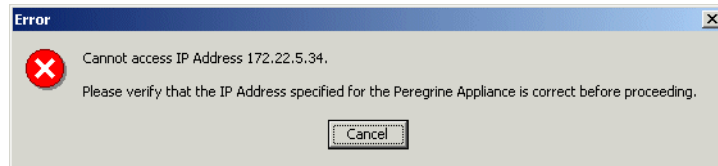
Reads the settings from a previously saved external configuration file (.cxz). This file contains the configuration settings only from a previous Scanner. Typically this file is 3 KB in size.

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.

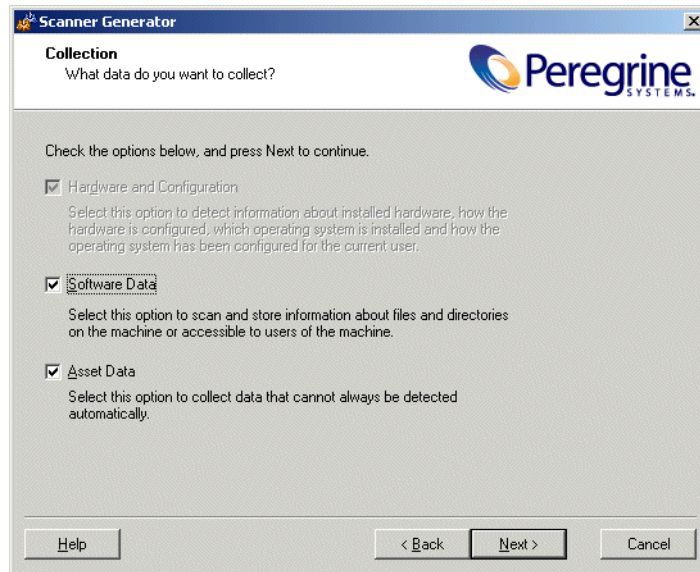


The Standard Configuration page

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

The Collection page

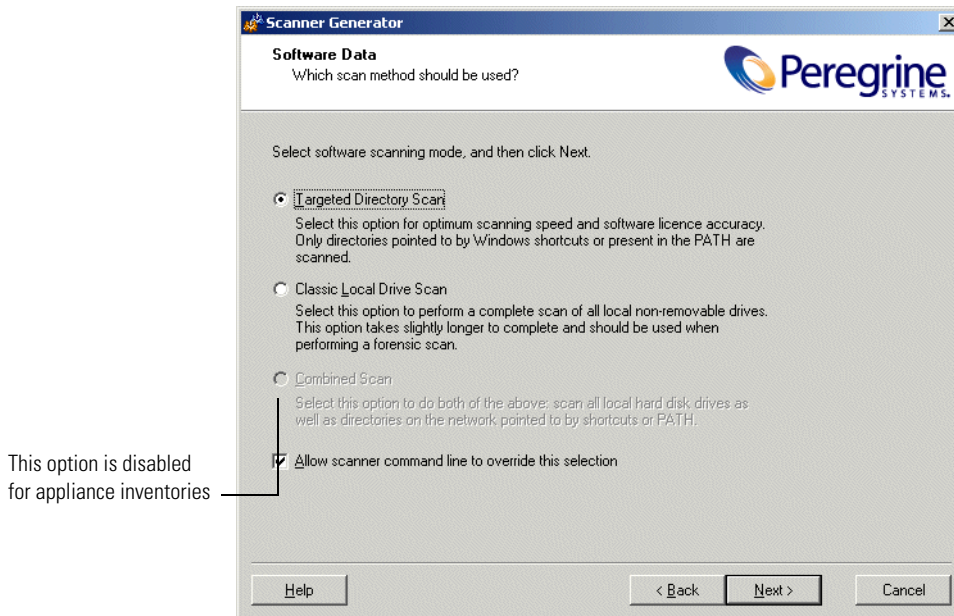
The Collection page is used to select the computer data to be collected.



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.



Combined Scan

Note: This option is disabled for appliance inventories.

The Refilling tab

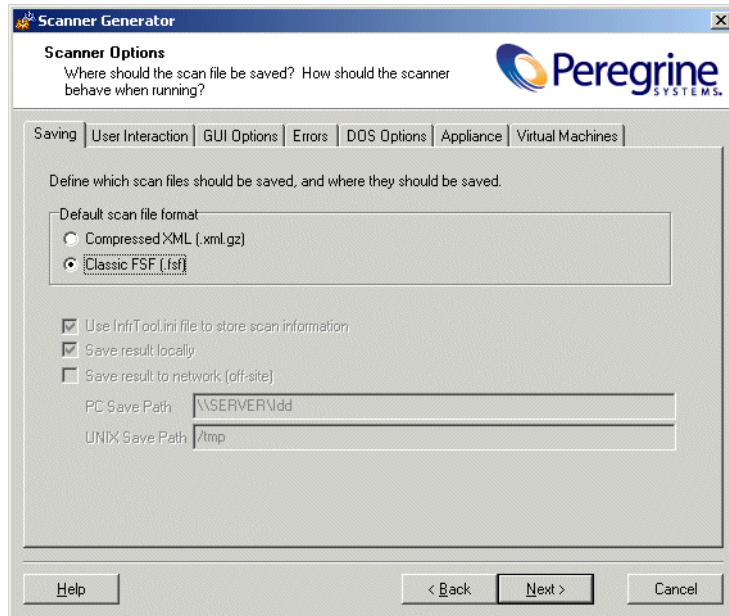
In **Desktop Inventory using the Peregrine Appliance** mode, the Scanners only save a local scan file, and this file is always used for refilling.

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.

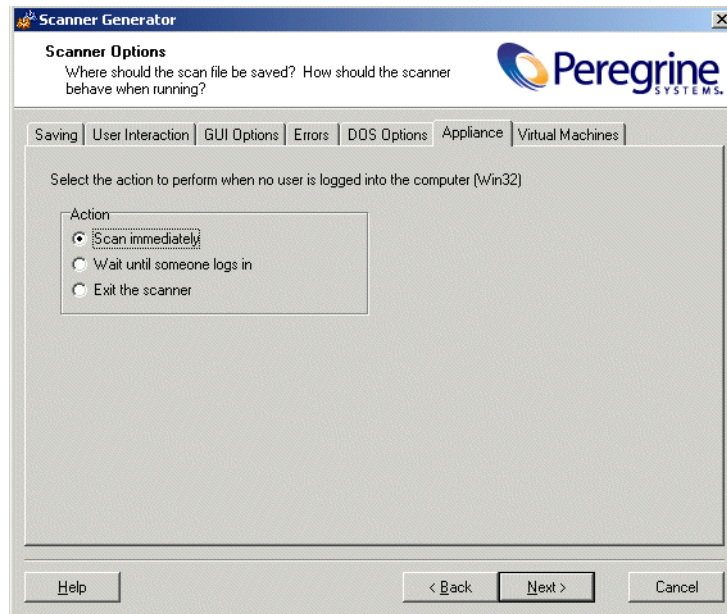


The Saving tab

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

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.



To define the behaviour 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.

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

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

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.
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.
Offsite FSF save is enabled	The Scanner configuration file has been created with the FSF save setting enabled. For a Scanner configuration file to be valid, this setting must be disabled.

Index

A

Activate Changes 44
Agent 12
Agent module 48
Appliance Location 74
application library 66
Asset Number tab 77
awareness 33

B

bandwidth threshold 39
BUS detection 76

C

Collection 76

D

Desktop Administration
 server configuration 21
disk space requirements 58

F

floppy disk 16, 26

G

General tab 77
Generating Scanners 80

L

Listener
 deploy to workstations 45
 download from appliance 46
Listener agent 12
Listener Property Groups 41
 apply to IP range 42

O

Options 78

P

Peregrine appliance 10

Q

QuickDeploy Manager Console 47

R

Refilling tab 77
Remote Control
 certificate 19
Remote Scanner 73
response.ans 20, 48

S

scan deployment
 automatic 30
scan execution 11
scan files
 collect and store 11
 enrichment 13

- scan frequency 39
- scan schedule properties 40
- scanfile.dtd 60
- scanner components 70
- scanner deployment
 - automatic 10
- Scanner Generator 35, 69
 - from the appliance 73
 - pages 72
- Scanner Options 78
- Scanner Property Groups 36
 - apply to IP range 42
- Scanners to Generate 80
- security keys
 - sharing between Network Discovery and Desktop Administration 15
 - sharing between Peregrine appliances 25
- setting up Network Discovery and Desktop Inventory 29
- Software Data 77
- Standard Configuration 75

W

- Welcome page 73

X

- XML Enricher 55
 - application library 66
 - configuring 64
 - directory structure 56
 - enrichment process status 58
 - launching from the appliance 63
- xml.gz file 60



December 8, 2003