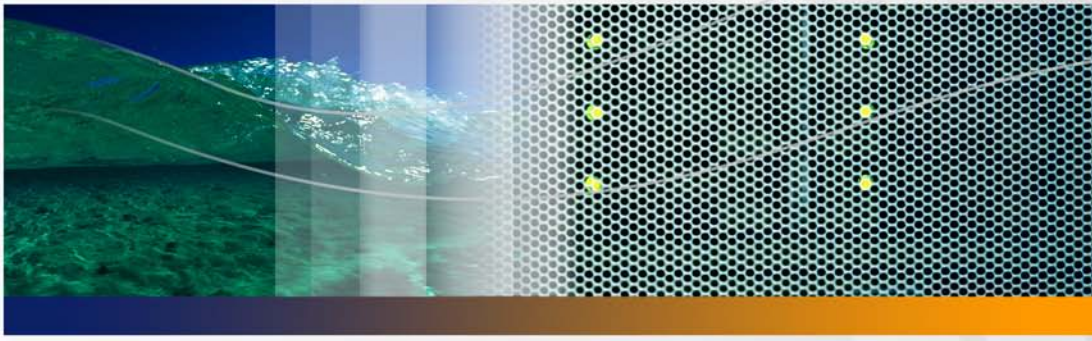
Product Documentation

Peregrine Systems, Inc.

Enterprise Discovery™ 2.0



Installation and Initial Setup

Part No. PED-2-EN03

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, please contact Peregrine Systems, Inc. Technical Publications by email at doc_comments@peregrine.com. This edition applies to version 2.0 of the licensed program.

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

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

PEREGRINE

Contents

CHAPTER 1 Welcome to Enterprise Discovery

Welcome to the *Installation and Initial Setup Guide*.

This guide is intended for the Enterprise Discovery™ Administrator, the person who will have the most control over the setup and operation of Enterprise Discovery.

About Enterprise Discovery Installation

Peregrine Enterprise Discovery enables you to discover and track the hardware, software and network assets that make up your organization's IT infrastructure.

There are two types of installation: server and client. You must install the server components once (on a dedicated server), but you can install the client components on as many computers as you need.

By default, when you install the server software, all the components will be in one of the following locations on your C: drive.

Directory Name	Default Location
Enterprise Discovery Data directory	C:\Documents and Settings\All Users\Application Data\Peregrine\Enterprise Discovery
Enterprise Discovery Program files directory	C:\Program Files\Peregrine\Enterprise Discovery\2.0.0

Peregrine Product Compatibility

Product	Compatible Version
ServiceCenter	6.1 or later
AssetCenter	4.4 or later
Connect-It	3.5 or later

What Next?

To	Go to
Install the server components	Chapter 3, Server Installation
Install the client components	Chapter 4, Client Installation

CHAPTER 2 Upgrade and Migration Scenarios

In this chapter, you will learn the basics of how to approach your installation, whether it be a new installation, an upgrade from Enterprise Discovery 1.0, or a migration from Desktop Inventory.

Introduction

There are many ways you could be approaching your Enterprise Discovery 2.0 installation.

- New Installation on page 14
- Migrating from Desktop Inventory 7.x or later on page 15
- Upgrading from Enterprise Discovery 1.0 on page 21

The following scenarios are best practices for implementing Enterprise Discovery. They are a high-level overview of the installation steps and may need to be customized to your specific situation. Refer to the rest of this Guide for help installing Enterprise Discovery.

New Installation

This *Installation and Initial Setup Guide* will take you through all the steps needed to set up Enterprise Discovery. Depending on what you want to accomplish, you can set up the Enterprise Discovery server to discover devices, automatically deploy agents and scanners, and collect software utilization data.

For a thorough explanation of how to prepare your network, read the *Planning Guide* first.

In general, the following list of tasks will get you through the installation and get your Enterprise Discovery server running.

Task		Instructions	Notes
1	Install the server components.	Server Installation on page 25	
2	Install the client components.	Client Installation on page 41	
3	Configure your server	Configuring your Enterprise Discovery Server on page 61	More details available in the *Customization and Configuration Guide*.
4	Set up IP Ranges	Configuring your Network IP Ranges on page 67	
5	Set up Network and Community Property Groups	Setting up Network Property Groups on page 83 Setting up Community Property Groups on page 89	
6	Activate your changes	Activating Your Configuration Changes on page 111	Wait until Enterprise Discovery has discovered all of those devices before continuing. Check **Status** > **Device status** > **Network model queue**/**Network model processing**.
7	Create Scanners	See the *Customization and Configuration Guide*.	Skip this step if you are only collecting basic hardware information and do not need software data.
8	Set up Agent and Scanner Property Groups for testing	Setting Up Agent Property Groups and Agent Deployment Accounts on page 95 Setting Up Scanner Property Groups and Scheduling Scanners on page 101	Configure Enterprise Discovery to deploy agents to a small portion of your network to ensure your configuration is correct.

Task		Instructions	Notes
9	Activate your changes	Activating Your Configuration Changes on page 111	
10	Manually deploy UNIX agents		This is required to automatically schedule scanning of UNIX/Linux computers.
11	Repeat steps 8, 9, 10 for the remainder of your network.		
12	Set up Accounts	Setting up Accounts on page 117	

Migrating from Desktop Inventory 7.x or later

If you worked with Desktop Inventory, you will need to upgrade to Enterprise Discovery 2.0. All the functionality available in Desktop Inventory has been included in Enterprise Discovery.

You may find yourself in one of the following scenarios. Follow the steps outlined for each scenario, and you will successfully migrate your Desktop Inventory data to Enterprise Discovery.

- I want to use Enterprise Discovery 2.0 as I have been using Desktop Inventory, but I also want to automatically deploy agents and scanners on page 15
- I want to use Enterprise Discovery 2.0 exactly as I used Desktop Inventory on page 19

I want to use Enterprise Discovery 2.0 as I have been using Desktop Inventory, but I also want to automatically deploy agents and scanners

In this scenario, you want to use the additional functionality available in Enterprise Discovery, such as automated agent and scanner deployment.

Follow these tasks to migrate to Enterprise Discovery:

Task		Instructions	Notes
1	Uninstall Desktop Inventory 7.x or later.	See the Desktop Inventory documentation.	This will remove Desktop Inventory from your server, and allow you to install Enterprise Discovery. Any scanners or User SAIs that you have created will remain after the uninstall.
2	Install the Enterprise Discovery server components on the computers where you had a "complete install" of Desktop Inventory.	Server Installation on page 25	If you had Desktop Inventory installed on a workstation, you should install Enterprise Discovery on a new dedicated server. Enterprise Discovery has greater hardware requirements than Desktop Inventory.
3	Install the client components.	Client Installation on page 41	
4	If you were grouping your scan files, you need to reapply the same groupings.	Click **Administration** > **System Preferences** > **Scan File Management**	
5	If you have manually changed the ini file for the Desktop Inventory XML Enricher, you must manually transfer those changes to the new Enterprise Discovery ini file located in the Data directory at \conf\ xmlenricher.ini.		Default location for the data directory: C:\Documents and Settings\All Users\Application Data\Peregrine\Enterprise Discovery
6	Run the Scanner Generator to generate the new scanner configuration for the Enterprise Mode scanners. The scanner configuration file(s) (.cxz) containing the generated configuration will be uploaded to the new server.	See the *Customization and Configuration Guide*.	The Scanner Generator can read the scanner configuration from the Desktop Inventory scanners, and generate new Enterprise Discovery scanners with the same parameters.
7	Migrate the data in your Application Encyclopedia (ApE) database to a user SAI.	Migrate Your ApE Database on page 148	
8	Run the SAI Update Wizard to migrate your Desktop Inventory read-only and user SAIs to the new format used by Enterprise Discovery.	Use the SAI Update Wizard to Upgrade Your Old Read Only SAIs on page 148	
9	Set up IP Ranges	Configuring your Network IP Ranges on page 67	

Task		Instructions	Notes
10	Set up Network and Community Property Groups	Setting up Network Property Groups on page 83 Setting up Community Property Groups on page 89	
11	Activate your changes	Activating Your Configuration Changes on page 111	Wait until Enterprise Discovery has discovered all of those devices before continuing. Check **Status** > **Device status** > **Network model queue**/**Network model processing**.
12	Set up Agent and Scanner Property Groups for testing	Setting Up Agent Property Groups and Agent Deployment Accounts on page 95 Setting Up Scanner Property Groups and Scheduling Scanners on page 101	Configure Enterprise Discovery to deploy agents to a small portion of your network to ensure your configuration is correct.
13	Activate your changes	Activating Your Configuration Changes on page 111	
14	Manually deploy UNIX agents		This is required to automatically schedule scanning of UNIX/Linux computers.
15	Repeat steps 11, 12, 13 for the remainder of your network.		
16	Move all your scan files from the `scans\processed` directory from your Desktop Inventory installation, to the `scans\incoming` directory located under the Enterprise Discovery Data directory.		This step is optional. You can rescan your entire network if you choose. If you used the grouping feature of the Desktop Inventory XML Enricher to sort your processed scan files into subdirectories, make sure to copy the files **without** the same directory structure. Copy all the files into the one main directory.
17	Upgrade to Connect-It 3.5.		Connect-It 3.5 is required to take advantage of the out-of-box scenarios for transferring data from the Enterprise Discovery database to AssetCenter or ServiceCenter.

Task		Instructions	Notes
18	Configure Connect-It to use the Discovery database.		This step is only necessary if you populate AssetCenter with scan file data.
19	Populate AssetCenter.		This step is only necessary if you populate AssetCenter with scan file data.
20	Clean up your old Desktop Inventory data.	**Administration** > **System preferences** > **Scan deployment**. Enable the "Clean PDI data from workstations" option.	
21	Set up Accounts	Setting up Accounts on page 117	

I want to use Enterprise Discovery 2.0 exactly as I used Desktop Inventory

In this scenario, you do not want to use any of the additional functionality available in Enterprise Discovery, such as automated agent deployment.

Follow these tasks to migrate to Enterprise Discovery:

Task		Instructions	Notes
1	Uninstall Desktop Inventory 7.x or later.	See the Desktop Inventory documentation.	This will remove Desktop Inventory from your server, and allow you to install Enterprise Discovery. Any scanners or User SAIs that you have created will remain after the uninstall.
2	Install the Enterprise Discovery server components on the computers where you had a "complete install" of Desktop Inventory.	Server Installation on page 25	If you had Desktop Inventory installed on a workstation, you should install Enterprise Discovery on a new dedicated server. Enterprise Discovery has greater hardware requirements than Desktop Inventory.
3	Install the client components.	Client Installation on page 41	
4	If you were grouping your scan files, you need to reapply the same groupings.	Click **Administration** > **System Preferences** > **Scan File Management**	
5	If you have manually changed the ini file for the Desktop Inventory XML Enricher, you must manually transfer those changes to the new Enterprise Discovery ini file located in the Data directory at \conf\ xmlenricher.ini.		Default location for the data directory: C:\Documents and Settings\All Users\Application Data\Peregrine\Enterprise Discovery
6	Run the Scanner Generator to re-generate new Enterprise Discovery scanners in Manual Deployment mode.	See the *Customization and Configuration Guide*.	The Scanner Generator can read the scanner configuration from the Desktop Inventory scanners, and generate new Enterprise Discovery scanners with the same parameters.
7	Migrate the data in your Application Encyclopedia (ApE) database to a user SAI.	Migrate Your ApE Database on page 148	
8	Migrate your SAIs.	Use the SAI Update Wizard to Upgrade Your Old Read Only SAIs on page 148	

Task		Instructions	Notes
9	Move all your scan files from the `scans\processed` directory from your Desktop Inventory installation, to the `scans\incoming` directory located under the Enterprise Discovery Data directory.		This step is optional. You can rescan your entire network if you choose. If you used the grouping feature of the Desktop Inventory XML Enricher to sort your processed scan files into subdirectories, make sure to copy the files **without** the same directory structure. Copy all the files into the one main directory.
10	Populate AssetCenter.		Use AssetCenter as you did before. You will want to adjust your Connect-It scenario to the new scans/processed directory.
11	Clean up your old Desktop Inventory data.	**Administration** > **System preferences** > **Scan deployment**. Enable the "Clean PDI data from workstations" option.	
12	Set up Accounts	Setting up Accounts on page 117	

Upgrading from Enterprise Discovery 1.0

Enterprise Discovery 1.0 was a marketing bundle containing Network Discovery 5.2 and Desktop Inventory 8.0.

In this scenario, you have been using automatic scanner deployment, and you wish to keep using that feature.

Follow these tasks to upgrade to Enterprise Discovery 2.0:

Task		Instructions	Notes
1	Upgrade to Network Discovery 5.2.4	See the *Network Discovery 5.2.4 Release Notes*.	
2	Install a new Enterprise Discovery server.	Server Installation on page 25	You cannot install Enterprise Discovery and Network Discovery on the same server. Both products must be installed on their own dedicated servers.
3	Install the client components.	Client Installation on page 41	
4	Backup your Network Discovery data using the new **Migrate Data to Enterprise Discovery** feature.	See the *Network Discovery 5.2.4 Release Notes*.	
5	Restore that backup to your Enterprise Discovery server.	See the *Network Discovery 5.2.4 Release Notes*.	
6	Migrate your SAIs.	Use the SAI Update Wizard to Upgrade Your Old Read Only SAIs on page 148	
7	Run the Scanner Generator to generate the new scanner configuration for the Enterprise Mode scanners. The scanner configuration file(s) (.cxz) containing the generated configuration will be uploaded to the new server.	See the *Customization and Configuration Guide*.	The Scanner Generator is able to read the scanner configuration from the Desktop Inventory scanners, so that this configuration can be taken as a base for configuring new Enterprise Mode scanners.

Task		Instructions	Notes
8	Set up Agent and Scanner Property Groups for testing	Setting Up Agent Property Groups and Agent Deployment Accounts on page 95 Setting Up Scanner Property Groups and Scheduling Scanners on page 101	This step is optional. Configure Enterprise Discovery to deploy agents to a small portion of your network to ensure your configuration is correct. This can be done using the old Desktop Inventory Listeners.
9	Activate your changes	Activating Your Configuration Changes on page 111	
10	Manually deploy UNIX agents		This is required to automatically schedule scanning of UNIX/Linux computers.
11	Repeat steps 8, 9, 10 for the remainder of your network.		
12	Copy all your scan files from the `scans\processed` directory from your Network Discovery installation, to the `scans\incoming` directory located under the Enterprise Discovery Data directory.		This step is optional. You can rescan your entire network if you choose. If you used the grouping feature of the Network Discovery XML Enricher to sort your processed scan files into subdirectories, make sure to copy the files **without** the same directory structure. Copy all the files into the one main directory.
13	Upgrade to Connect-It 3.5.		Connect-It 3.5 is required to take advantage of the out-of-box scenarios for transferring data from the Enterprise Discovery database to AssetCenter or ServiceCenter.
14	Configure Connect-It to use the Discovery database.		This step is only necessary if you populate AssetCenter with scan file data.
15	Populate AssetCenter.		This step is only necessary if you populate AssetCenter with scan file data.
16	Uninstall your old Listeners	**Administration** > **Network configuration** > **Agent property groups**. For each of your Agent property groups, select the "Listener Uninstall" option.	Once your system is running well, you can uninstall the old Desktop Inventory Listeners.

Task		Instructions	Notes
17	Clean up your old Desktop Inventory data.	**Administration** > **System preferences** > **Scan deployment**. Enable the "Clean PDI data from workstations" option.	
18	Set up Accounts	Setting up Accounts on page 117	

3 Server Installation

CHAPTER

In this chapter, you will learn how to install the Enterprise Discovery server components. The following topics will be covered:

Introduction

You must install the server components on one dedicated server. The technical specifications are as follows:

Component	Description
Operating System	Windows 2003 Server SP1 (Windows XP SP2 is also compatible, but should only be used for trial or demo installations)
CPU	Pentium 4 2GHz or better with hyper-threading
RAM	1.5 GB
Disk	Need at least 6GB to install Enterprise Discovery **Note:** When calculating the amount of disk space you need, budget at least 1.5MB for each device being scanned. For more information on the disk requirements for an Aggregator server, see Installing the Aggregator Hardware on page 124.
Other Hardware	CD-ROM drive and a 3.5 floppy drive.

Disk Space

Your disk space requirements may differ depending on how you are using Enterprise Discovery.

Scan files, on average, are approximately 270 KB each. By default, Enterprise Discovery stores each scan file in several locations. Because of these duplicates, we recommend that you budget at least 5 times as much disk space for each device being scanned.

Note: If your average scan file size is greater than 270 KB, adjust your disk space requirements accordingly.

Reduce the disk space needed

To save disk space on your server, you can try the following options.

Reduce the disk space needed by:	Explanation
Changing how long your server keeps the data being sent to the Aggregator.	Click **Administration** > **System preferences** > **Aggregate configuration**. Reduce the amount of time the server keeps its Aggregator data.
Not backing up your scan files	Configure Enterprise Discovery to not backup scan files Click **Administration** > **System preferences** > **Server configuration**. **Note:** If you turn this off, you must backup your scan files on your own.
Turning off Delta scanning	You can turn this off in the Scanner Generator. For more information, see the *Configuration and Customization Guide*.
Deleting orphaned scan files	Click **Administration** > **System preferences** > **Scan file management** > **Delete orphaned scan files**. This option is enabled by default.

Click **Administration** > **System preferences** > **Server configuration**, and turn "Backup scan files" off.

In future, you may need more disk space

In a future release of Enterprise Discovery, there will be a new optional module to collect network topology data for all your devices. This will increase your CPU and disk space requirements.

Once you start collecting topology data, you will only be able to save data for 15,000 devices on one server. If you plan to use this module in the future, you may want to deploy Enterprise Discovery 2.0 differently to avoid reconfiguring your server.

Installing the License on the Server

Peregrine Systems makes increased functionality available through license files.

Important: The license determines how many devices you can discover in your network.

If you do not install a license on your server, Enterprise Discovery will only be able to discover 5 devices.

Enterprise Discovery has the following licence options:

- Number of devices (increments of 100)
- Application Utilization (on/off)
- Aggregation (on/off)

Installing your License on the Server:

When you purchase Enterprise Discovery, you will receive (via e-mail) a .zip file containing a .reg file.

1 Unzip the file.

2 Place the .reg file on the server desktop.

3 Double-click the file to run it.

The license file automatically updates your server registry to give Enterprise Discovery the appropriate capabilities. It will take Enterprise Discovery up to five minutes to react to licensing changes.

You can purchase more licenses at any time, to increase your device capacity, or to add more functionality (to add utilization or aggregation features).

You can see your license information at **Status** > **Current Settings** > **License Status**.

Installing Enterprise Discovery on the Server

This section describes how to install the Enterprise Discovery on your dedicated server.

Before running the Setup program, ensure that:

- The server has Windows 2003 Server (or Windows XP, if this is a trial or demo installation) installed.
- There is not an installed version of ActivePerl.
- No other Windows applications are running.

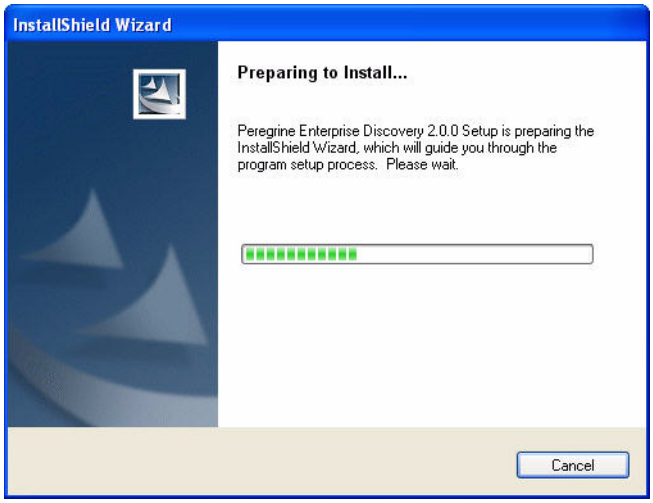
Important: If you have other programs installed on this server, they may interfere with the ports used by Enterprise Discovery. Ensure that you have no other programs installed on this server. For a list of ports used by Enterprise Discovery, see the *Planning Guide*.

To install Enterprise Discovery:

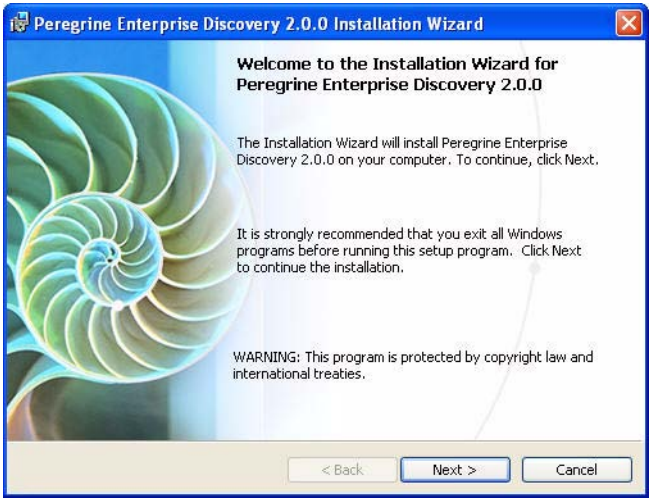
1 While Windows is running, insert the Installation CD into the CD ROM drive of the server.

The CD is configured to auto-run, however if you need to start the Setup program manually, you can do this by navigating to the drive containing the CD and double clicking on the setup.exe file.

First, a Preparing to Install window appears.

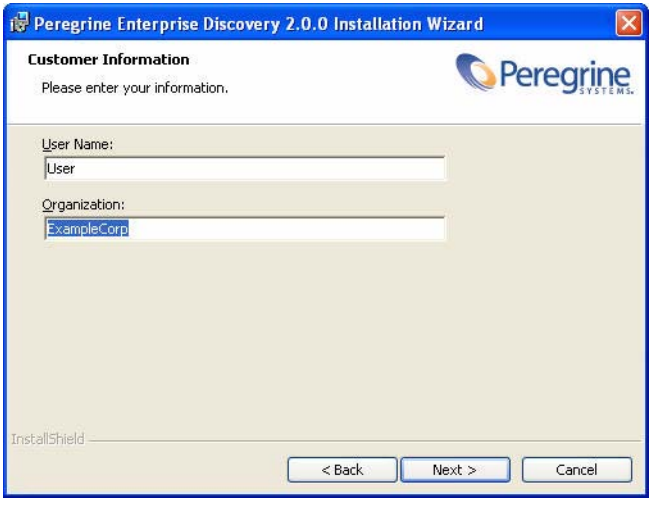


Next, the Installation Wizard appears.



2 Click **Next**.

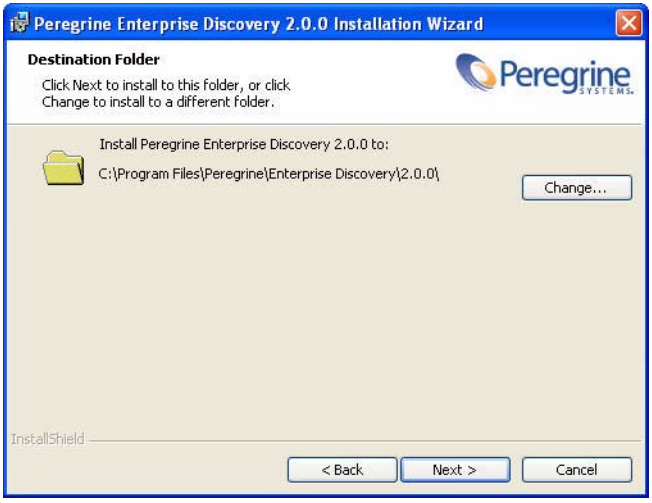
The Customer Information screen appears.



3 Enter your name and organization name.

4 Click **Next**.

The Destination Folder screen appears.



The default installation directory is:

C:\Program Files\Peregrine\Enterprise Discovery\2.0.0

5 Click **Change** to change the destination folder, and follow the instructions.

Note: All components will be installed to this default location. Click **Next**.

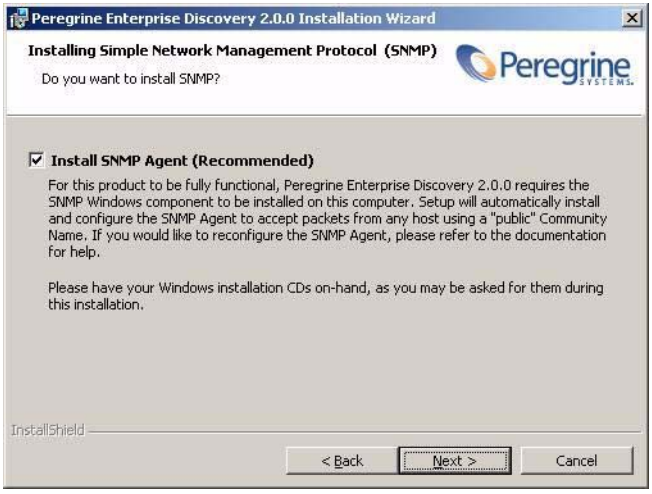
The Setup Type screen appears.

6 Select the "Server" Setup Type.

7 Click **Next**.

If your server does not have SNMP installed, you will see the "Installing Simple Network Management Protocol screen. You have the option of installing SNMP during the installation process.

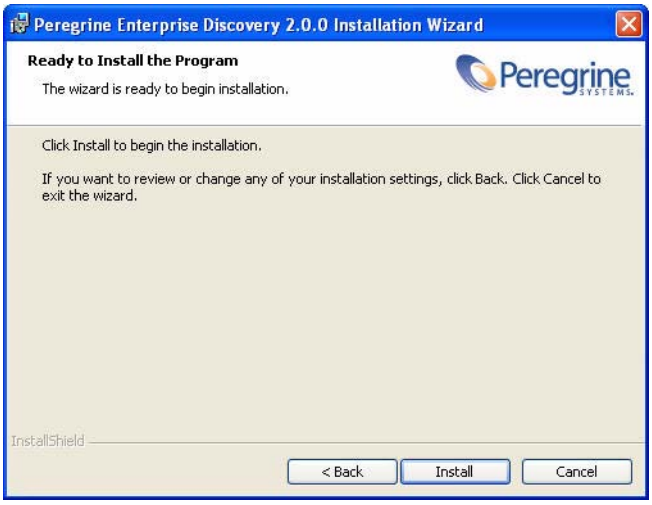
See the Microsoft Help for more information on how to configure SNMP and the related community names.



8 To install SNMP now, select the Install SNMP checkbox, then click **Next**. To wait and install it at another time, deselect the Install SNMP checkbox, then click **Next**.

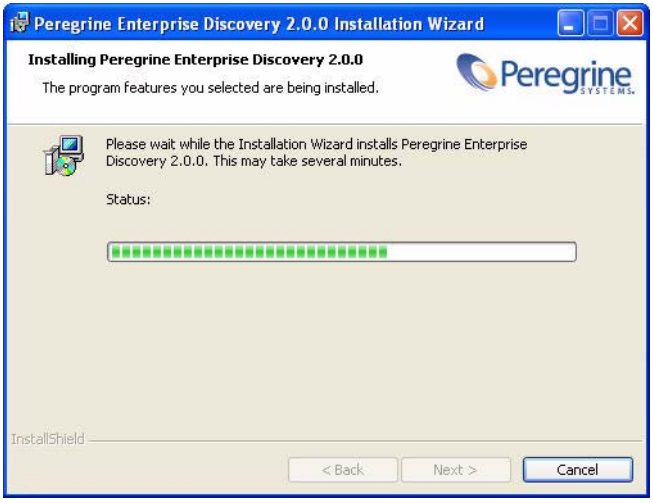
9

The Ready to Install the Program screen appears.



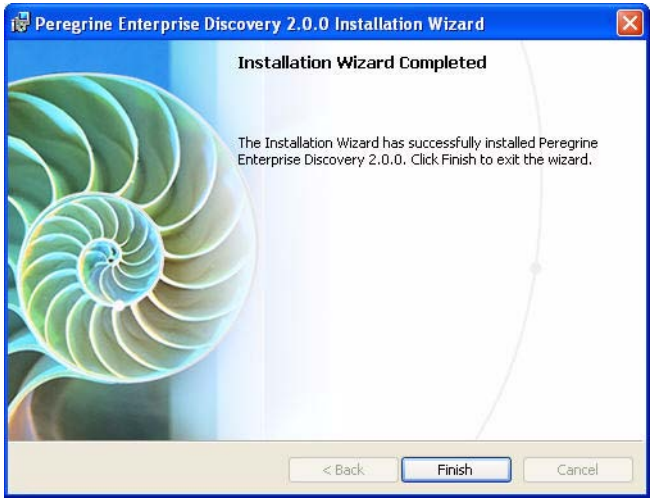
10 Click **Install** to begin the installation.

A progress indicator appears:



This process can take up to 10 minutes. The longest period will be when Enterprise Discovery is installing the "Perl Packages."

Once the installation is complete, the following screen appears.

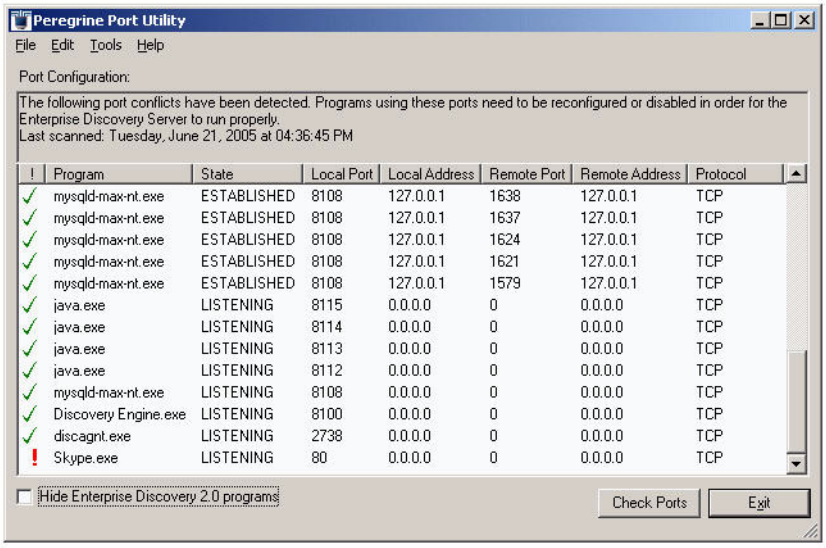


11 Click **Finish**.

The installation of Enterprise Discovery is complete.

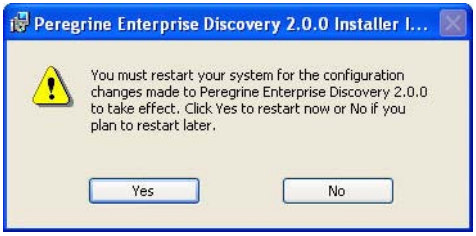
Conflicting Ports

If you have any software installed on this server that is conflicting with the ports needed for Enterprise Discovery, you will see a warning box indicating the conflicts.



Restarting your Server

After the installation is complete, this window appears, asking you to restart your server.



- Click **Yes** to restart now, or **No** if you want to wait and restart later.

Warning: Installation is not complete until the server has been restarted.

Save your Certificates to a Safe Location

Enterprise Discovery uses certificates to communicate with the Agents it distributes to your computer population. Every Enterprise Discovery installation has unique certificates.

If, for any reason, your Enterprise Discovery server is damaged, and its data is lost, you will need to reinstall the software, and you will need you original certificates in order to communicate with the Agents distributed to your computers.

We recommend that you copy your Enterprise Discovery certificates to a floppy disk, USB key, or burn them onto a CD and put it in a safe location.

Important: For security reasons, do not transfer the files over the network.

By default, the certificates are located in this directory:

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

Warning: If you do not save your certificates to a secure location, and your server loses its data for any reason, you will have to redeploy Agents throughout your network.

Create a Shared Directory on the Server

In order for the client workstations to access the scan files on the Enterprise Discovery server, you need to share their directories (all in the Enterprise Discovery Data Directory).

- Scans\
- Scans\Incoming
- Scans\Original

Refer to your Microsoft documentation for information on how to share folders.

Check that all Services are Running

All of these services need to be running once Enterprise Discovery has been installed. Once you've completed your installation, check the list of services on your server (**Control Panel** > **Administrative Tools** > **Services**) to be sure they are all running.

If these services are not running, make sure that you have restarted your server as described in Restarting your Server on page 37.

Warning: The Apache Web Server takes several minutes to start.

Service	Description
Peregrine Agent Communicator	Provides communication services with Peregrine Agents to Peregrine's Discovery products.
Peregrine Apache Web Server	Apache Web Server installed with Peregrine's Discovery products.
Peregrine Authenticator	Provides authentication services for Peregrine's Discovery products.
Peregrine Discovery Engine	Provides network discovery services to Peregrine's Discovery products.
Peregrine Discovery Scheduler	Provides scheduling services for Peregrine's Discovery products.

Service	Description
Peregrine Discovery Tools Database	Provides database services for Peregrine's Discovery products.
Peregrine Logger	Provides logging services to Peregrine's Discovery products.
Peregrine System Monitor	Ensures all Peregrine system processes are running properly.
Peregrine Tomcat Servlet Container	Tomcat Servlet Container bundled with Peregrine's Discovery products.
Peregrine Watchdog	This service ensures the System Monitor process is running.
Peregrine XML Enricher	The XML Enricher is a process that runs in the background and automatically adds application data to scan files. This process is called scan file enrichment.

What Next?

To	Go to
Install Enterprise Discovery on client workstations	Chapter 4, Client Installation
Learn how to access the different components	Chapter 5, Getting Started
Set up the server	Chapter 6, Configuring your Enterprise Discovery Server

4 Client Installation

CHAPTER

In this chapter, you will learn how to install the Enterprise Discovery client components. The following topics will be covered:

Introduction

You can install the client portion on several workstations.

The server install contains everything available in Enterprise Discovery 2.0. The client install is a subset of the server install, containing only:

- Analysis Workbench
- Viewer
- SAI Editor
- Scanner Generator
- Help and PDFs

Client Specifications

You can use any properly equipped computer as an Admin workstation. The technical specifications are as follows:

Item	Required	Recommended
MB RAM	1-3 GB if you will be analyzing a large number of scan files.	1-3 GB
CPU	Pentium III, 500 MHz	
Disk	100MB	2GB
Operating system	Windows 98 or later	Windows 200x, XP
Microsoft Office		Microsoft Office 2003 (for processing CSV export files)
Web browser	Firefox 1.0	Firefox 1.0.4
	Internet Explorer 5.5 or later	Internet Explorer 5.5 or later
Java Runtime Environment	1.4.2 or 1.5 [a]	1.5
Video —colors	16,000	65,000 or more
—resolution	800×600	1024 ×768 or more

a Must be downloaded from java.sun.com, do not use the version that comes with your browser

Note: Java and JavaScript must be enabled in order for Enterprise Discovery to work properly.

Installing the License on the Client

Peregrine Systems makes increased functionality available through license files. Use the same .reg file for the Client that you used when installing your server (Installing the License on the Server on page 28).

Important: The license determines how many devices you can discover in your network.

If you do not install a license on your client, you will not be able to use the Viewer or Analysis Workbench with more than 5 devices.

Enterprise Discovery has the following licence options:

- Number of devices (increments of 100)
- Application Utilization (on/off)
- Aggregation (on/off)

Installing your License on the Client:

When you purchase Enterprise Discovery, you will receive (via e-mail) a .zip file containing a .reg file.

1. Unzip the file.
2. Place the .reg file on the server desktop.
3. Double-click the file to run it.

   The license file automatically updates your server registry to give Enterprise Discovery the appropriate capabilities.

You can purchase more licenses at any time, to increase your device capacity, or to add more functionality (to add utilization or aggregation features).

You can see your client license information in the Viewer, Scanner Generator, or Analysis Workbench by clicking **Help** > **About**.

Installing Enterprise Discovery

This section describes how to install Enterprise Discovery on your client workstation.

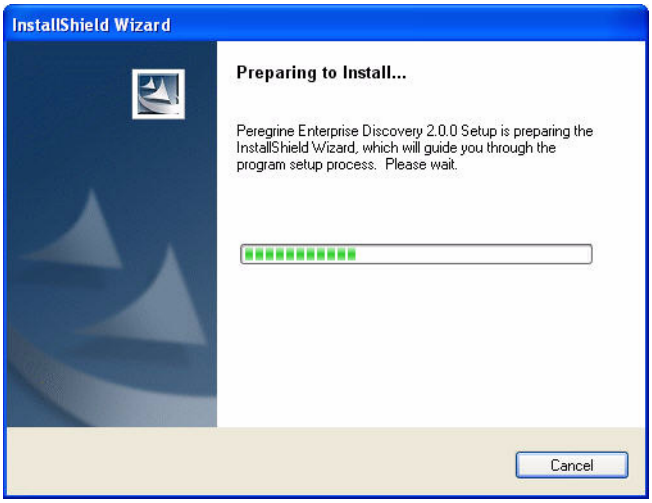
Before running the Setup program, ensure that no other Windows applications are running.

To install Enterprise Discovery on the client workstation:

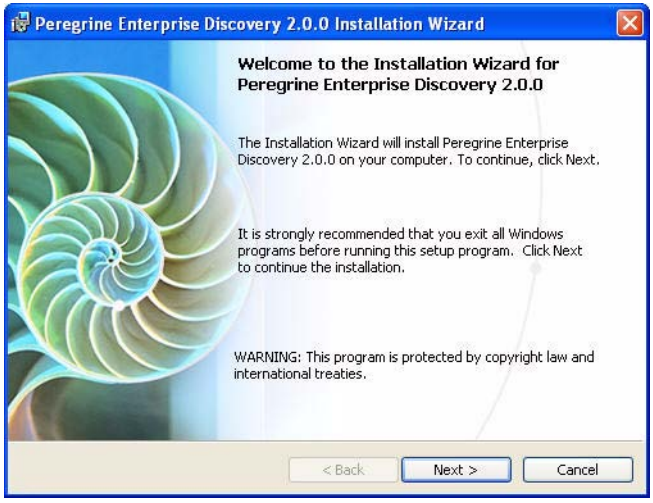
1 While Windows is running, insert the Installation CD into the CD ROM drive of your computer.

The CD is configured to auto-run, however if you need to start the Setup program manually, you can do this by navigating to the drive containing the CD and double clicking on the setup.exe file.

First, a Preparing to Install window appears.

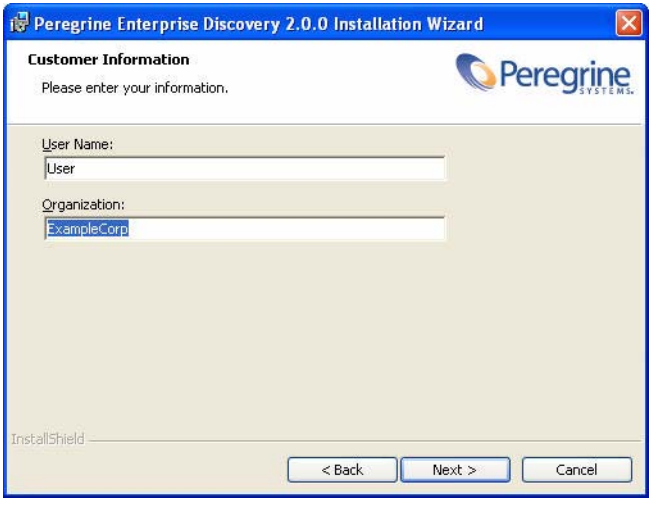


Next, the Installation Wizard appears.



2 Click **Next**.

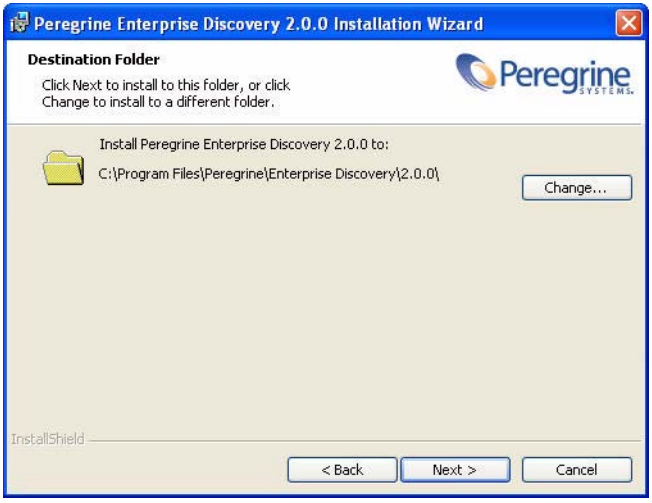
The Customer Information screen appears.



3 Enter your name and organization name.

4 Click **Next**.

The Destination Folder screen appears.



The default installation directory is:

C:\Program Files\Peregrine\Enterprise Discovery\2.0.0

5 Click **Change** to change the destination folder, and follow the instructions.

Note: All components will be installed to this default location.

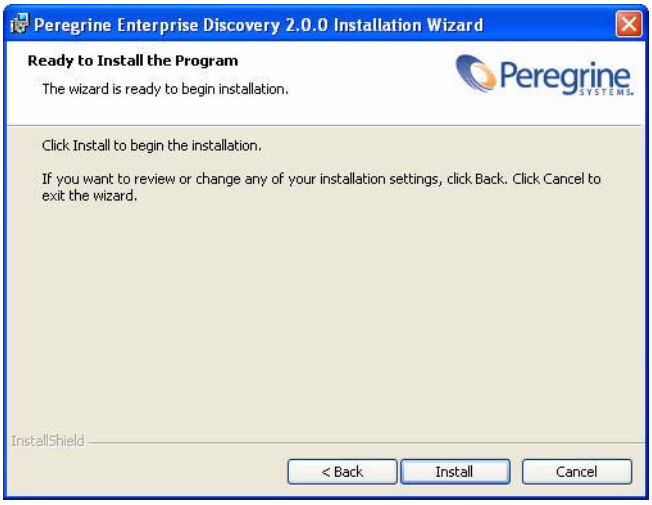
6 Click **Next**.

The Setup Type screen appears.

7 Select the "Client" Setup Type.

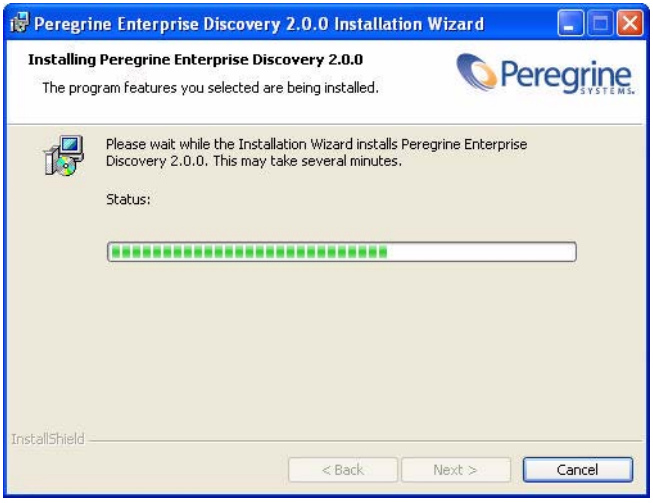
8 Click **Next**.

The Ready to Install the Program screen appears.

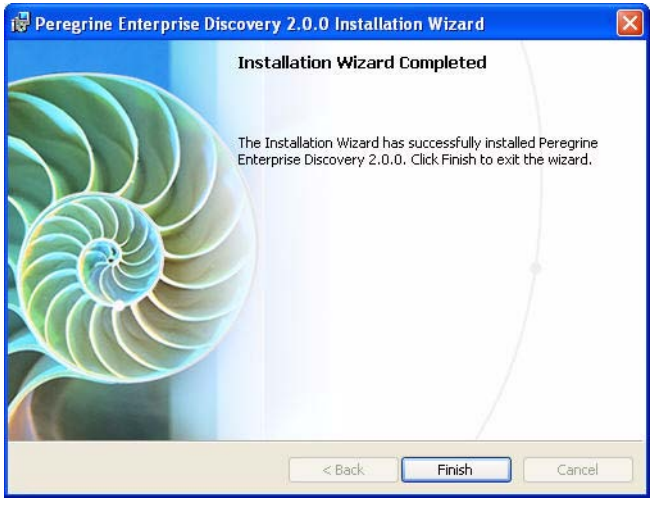


9 Click **Install** to begin the installation.

A progress indicator appears:



Once the installation is complete, the following screen appears.



10 Click **Finish**.

The installation of Enterprise Discovery is complete.

What Next?

To	Go to
Learn how to access the different components	Chapter 5, Getting Started
Set up the server	Chapter 6, Configuring your Enterprise Discovery Server

5 Getting Started

CHAPTER

In this chapter, you will learn how to access the client and server components of Enterprise Discovery. The following topics will be covered:

Introduction

Depending on your installation, there are different ways to access the different Enterprise Discovery components. You can log into the Web Interface with a browser over the intranet. You can access the client (Windows) components only through your client workstation.

The following is a complete list of all the user components, and where they are available:

Windows Components
Documentation
Help
Analysis Workbench
FSF Converter Wizard
SAI Editor
SAI Update Wizard
Scanner Generator
Viewer

Web Interface Components
Find
Health Panel
Alarms Viewer
Events Browser
Reports
Administration
Status

Accessing the Web Interface Components

You can access the web interface through any compatible web browser. In order to use the browser with Enterprise Discovery, your browser must have the following:

- Sun Java 1.4.2 or 1.5 enabled
- Javascript enabled
- pop-up windows enabled

You must also have the following:

- the IP address or domain name of the Enterprise Discovery server (if accessing the server through the intranet)
- a valid Enterprise Discovery account name and password

Enterprise Discovery is shipped with four pre-defined accounts.

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

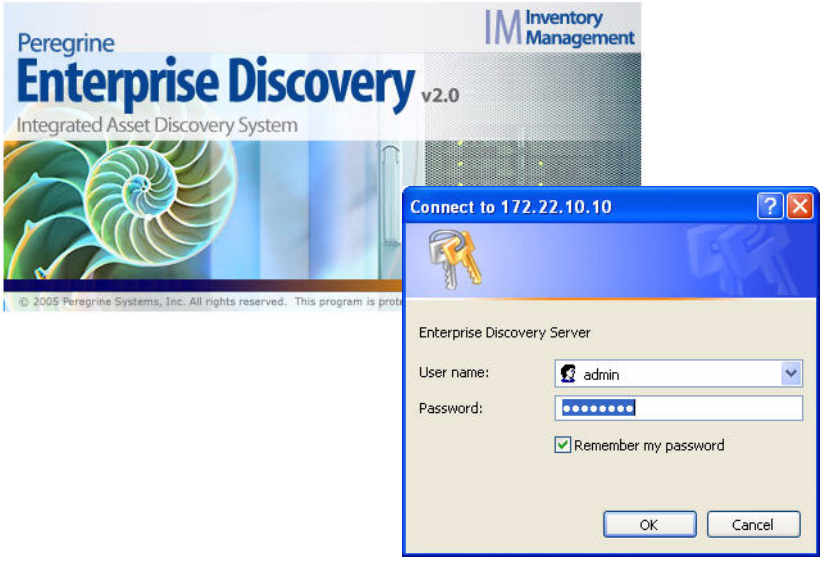
For your first session with Enterprise Discovery, you should use the account named “admin.” Later, you will be instructed to change these default account names and passwords to help secure your Enterprise Discovery server.

To access the Enterprise Discovery web components:

1 Launch your web browser.

2 In the URL area of your browser, enter the IP address or domain name of your Enterprise Discovery server. If you are working on the server itself, enter `localhost` in the URL area.

When the connection is made, the Enterprise Discovery splash screen and Login window appear.



Note: You can bookmark this URL for use with your browser.

3 Enter the default account name (“admin”) and password (“password”).

Note: Account names are all lowercase.

Passwords are case-sensitive. “PASSWORD” and “password” are two different passwords.

- Once the account name and password are accepted, the Enterprise Discovery Home page appears.
- After the Home page appears, your browser may display a security warning. You are asked to grant Enterprise Discovery permission to run.

4 Click the check box next to “Always trust content from Peregrine Systems, Inc.” and click **Yes**.

Note: The security warning will differ depending on the browser you are using.

Note: This should be the only time you use the default password for the “admin” account. Refer to Change the default Admin password on page 143.

Troubleshooting when logging in for the first time

Why can’t I connect to Enterprise Discovery?

If you are unable to access Enterprise Discovery using your web browser, check the following:

- Is the URL correct?
- Is there a firewall in place that is blocking port 80 between your client and server computers?
- Is the server machine visible over the network from the client machine?
- Is the Peregrine Apache Web Server running? This component can take up to 5 minutes to start; if it has not started after 5 minutes, please contact Customer Support.

It’s still not working; what should I do?

- If the Enterprise Discovery server fails to respond, contact your Customer Support representative for further assistance.

The Login did not appear.

- Click the Enterprise Discovery splash screen.

I can ping the server, but there is no web interface appearing.

On the server, check that the "Peregrine Apache Web Server" service is running in the list of Services (Start > Control Panel > Administrative Tools > Services).

Understanding the Home page

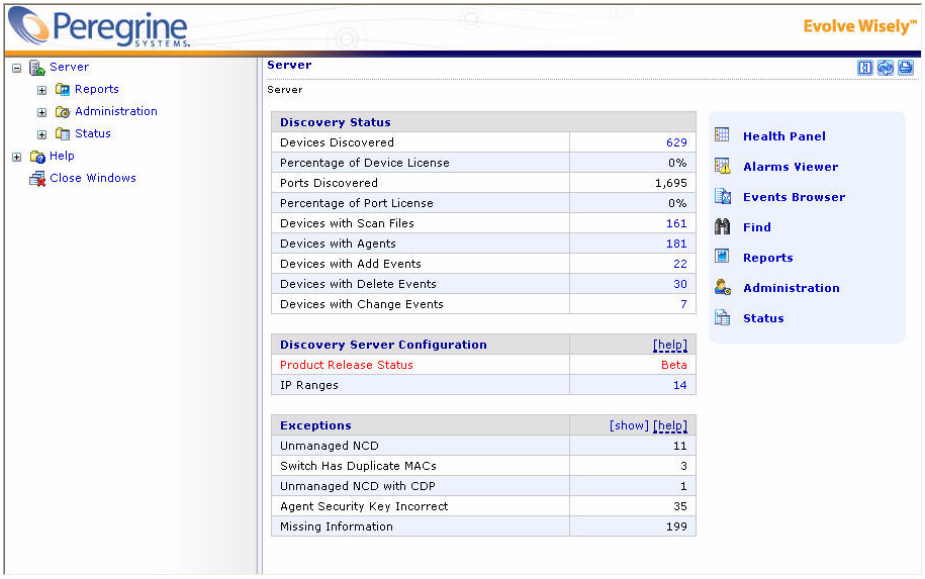
The Home page welcomes you to Enterprise Discovery. On the Home page, you will see links to the web-based features of Enterprise Discovery, and a summary of your current network status.

Note: Since this is the first time you are logging into Enterprise Discovery, there will be no useful statistics presented. Once you have configured your server, you should see these statistics change.

The following is a list of the data you can see on the Home page:

Table	Description
Discovery Status	This table will show you a breakdown of your network devices, so you can see how many devices have been discovered, how many have agents installed, etc.
Discovery Server Configuration	This table will show you how many IP ranges you have configured, and the status of your Enterprise Discovery software.
Exceptions	This table displays the most important Exceptions seen in your network. For a complete list of Exceptions, check the Alarms Viewer.

You can navigate the menus using the tree on the left side, or the links throughout the interface.



Accessing the Windows Components

If you have done a server or client install, you will have access to the Windows components of Enterprise Discovery. These components are all available through the Windows Start menu.

To access the Enterprise Discovery Windows components:

1 Click **Start** > **All Programs** > **Peregrine** > **Enterprise Discovery 2.0**.

2 Select an option to start up any of the following components:

- Documentation
- Help
- Analysis Workbench
- FSF Converter Wizard
- SAI Editor
- SAI Update Wizard

- Scanner Generator
- Viewer

What Next?

To	Go to
Configure the server	Chapter 6, Configuring your Enterprise Discovery Server

CHAPTER 6 Configuring your Enterprise Discovery Server

In this chapter, you will learn how to configure your Enterprise Discovery server.

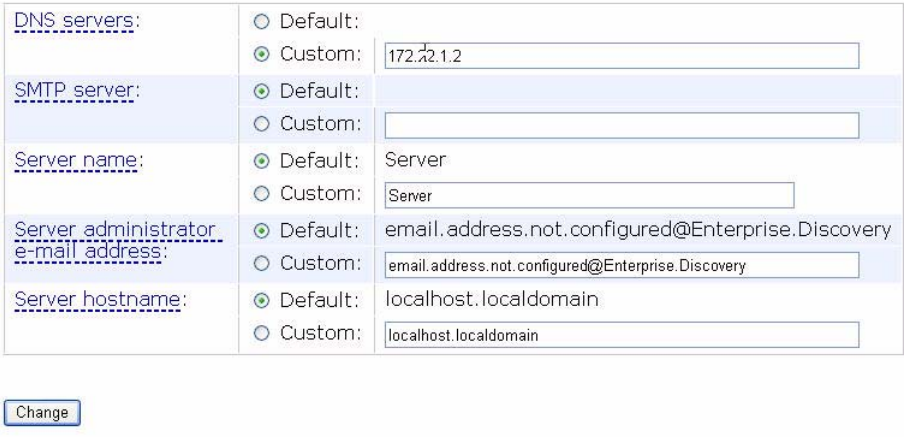
Introduction

Once you have installed the software, and you have seen where the components are located, you can now configure the Enterprise Discovery server. Once this is completed, you can then configure the server to start discovering your network.

Log in to the Web Interface as described in Getting Started on page 53, and then complete the following procedures:

- Enter the DNS server(s) on page 62
- Enter the SMTP server on page 63
- Enter a server name on page 63
- Enter the Administrator e-mail address on page 64
- Enter the server host name on page 65

All of these options are available on the same page in the Web Interface. To get there, click **Administration** > **System Preferences** > **Server Configuration**.



Enter the DNS server(s)

A domain name server translates between alphabetic domain names—also known as DNS names—(for example, "website.example.com") and numeric IP addresses (for example, "192.168.133.1"). Enterprise Discovery needs to know where your domain name servers are so that it can take advantage of this "translation service."

Unless you set the domain name server, domain names will not appear in reports, and so on.

To enter the domain name server(s):

- In the **DNS servers** field, type the IP address (IPv4) of the new domain name server in the top field. To enter more than one, separate each IP address with a comma.

Enter the SMTP server

An SMTP server handles standard Internet e-mail. Enterprise Discovery can use this server when it generates e-mail messages to tell you what is going on in your network or with other processes.

If you do not enter an SMTP server, e-mail from Enterprise Discovery will not be sent.

Note: You may wish to use the IPv4 address rather than the domain name of the SMTP server so that Enterprise Discovery can still contact you even if the domain name server is unavailable.

To enter the SMTP server:

- Enter the Host name or IPv4 address of the SMTP server.

Enter a server name

"Server name" is the name of the network or part of the network that Enterprise Discovery is currently managing. The server name appears in the web interface navigation tree and menu path.

To assign a server name:

- Enter the server name.

  The server name can be a maximum of 250 characters long (including spaces).

Note: After five minutes, refresh the browser window to see the new server name web browser banner.

Enter the Administrator e-mail address

Enter the e-mail address of the Enterprise Discovery Administrator, and that address will receive information on mail delivery problems.

If you enter an e-mail address that is not valid, you will cause "message undeliverable" e-mails to be sent to the account of the administrator for the mail server. This account is normally called "postmaster". Consult your mail server's documentation for details.

If you do not enter an Administrator e-mail address, e-mails generated by the server will have the following "sender" information:

```
From: Enterprise Discovery at Server
[mailto:email.address.not.configured@Enterprise.Discovery]
```

To enter the Enterprise Discovery Administrator e-mail address:

- Enter the e-mail address of the Enterprise Discovery Administrator.

Enter the server host name

A host name allows you to refer to a device by a name rather than an IP address. Enterprise Discovery uses the host name to refer to itself in the e-mails it sends.

Note: Define a domain name server before changing the host name.

To change the host name:

- Enter the new host name.

Initiate the Changes

In order to initiate these Server Configuration options, you must click **Change**.

What Next?

To	Go to
Optionally create custom Scanners	the Scanner Generator chapter in the *Configuration and Customization Guide*
Set your IP ranges	Chapter 7, Configuring your Network IP Ranges

CHAPTER 7 Configuring your Network IP Ranges

In this chapter, you will learn how to configure your IP ranges so Enterprise Discovery can start discovering your network. The following topics will be covered:

Introduction

Enterprise Discovery allows you to precisely define what devices in your network it will discover and how. For now, it is recommended to keep things simple and set up Enterprise Discovery to perform active discovery on all of the network that you know has devices.

After you have a better idea of your network contents, you can change your IP ranges, and create your own Property Groups and Property Sets.

How it works

First you must set up your IPv4 ranges. To the various ranges you can apply groups of properties (for example, “Active Discovery,” “Do not allow discovery,” or “DHCP server”).

You can apply default groups of properties or customize your own. Enterprise Discovery guides you with graphic views of the ranges you set up. The setup can be quite sophisticated. There is more information on how to take advantage of this flexibility in the next chapter, Setting up Property Groups and Property Sets on page 79.

There are several ways to start configuring your IP ranges.

If you know	you can
Little about the contents of your network, and you’re not sure where to begin	Running router discovery on page 69.
The IP ranges used in your network, and the types of devices contained in each range	Setting up the IPv4 range(s) to discover on page 70. You can also Setting up the IPv4 range(s) to avoid on page 72, or Adding ranges for DHCP servers and unmanaged routers on page 72.
That some of your adjacent IP ranges are configured the same way	Merging IP Ranges on page 73
All the details of your network, IP ranges, and the Property Groups/Sets that you would like to use	Importing your IPv4 Ranges from a CSV File on page 74. You can also Exporting your IPv4 ranges to a CSV file on page 75.

Running router discovery

Router Discovery is a tool you can use to automatically locate the SNMP-managed routers and subnets in your network. Enterprise Discovery will give you a list of routers, and you can use that list to populate your IPv4 ranges while setting up Enterprise Discovery.

Router Discovery only runs when you initiate it. This is not a continuous process.

If you would rather enter your IPv4 ranges manually, go to Setting up the IPv4 range(s) to discover on page 70.

Set up Router Discovery:

1 Click **Administration** > **Router discovery** > **Router discovery settings**.

2 Set the community strings, maximum hops, minimum and maximum line speeds.

Note: The list of community strings must be separated by commas (for example, "public,private,string1,string2").

3 Click **Change**.

Note: Hop 0 (zero) is always the Enterprise Discovery server itself, and hop 1 is always the default gateway.

Run Router Discovery:

1 Click **Administration** > **Router discovery** > **Run router discovery**.

2 Click **Confirm**.

Apply the Router Discovery results to your IPv4 Range:

1 Click **Administration** > **Router discovery** > **Router discovery results**.

2 Choose a property set for each discovered router (typically, you should choose the "Active Discovery" option).

3 Click **Add to IPv4 Ranges**.

Setting up the IPv4 range(s) to discover

As soon as you entered the IPv4 address of the Enterprise Discovery server, Enterprise Discovery automatically determines the subnet in which the Enterprise Discovery server resides. It may have suggested a range that is either too big or too small. Take a look at the suggested IPv4 range.

View an IPv4 range

Note: If you have run Router Discovery, the IPv4 ranges you added in the previous procedure should also appear in this list.

To view IPv4 ranges:

- Click **Administration** > **Network configuration** > **List IPv4 ranges**.

If the IPv4 range suggested by Enterprise Discovery is too big or too small, delete it and add the correct range or ranges.

Add an IPv4 range

For each subnet in your network that you want Enterprise Discovery to discover, add a new IPv4 range.

Note: If you add an IPv4 range that is 65536 or more devices, you will see a warning message. The warning is only there to guard against possible errors when you are configuring your IPv4 ranges. Enterprise Discovery will still operate normally if you choose to use IPv4 ranges of that size.

To add a range of IPv4 addresses:

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

2 Enter the starting and ending IPv4 addresses of your whole network or of a range in your network.

Note: If you prefer, you can also enter a single octet netmask (for example, enter an IPv4 address of 172.22.1.1, and a Netmask of 24). To enter a range for one address, you can enter the IPv4 address, and a netmask of 32.

3 For **Property Set/Group**, select one of the default options, or one that you create yourself (see Setting up Network Property Groups on page 83, Setting up Community Property Groups on page 89, Setting Up Agent Property Groups and Agent Deployment Accounts on page 95, or Setting Up Scanner Property Groups and Scheduling Scanners on page 101).

Enterprise Discovery will perform network discovery (ping, poll, and table read) on the range you have entered.

4 Click **Submit**.

Repeat step 1 to step 4, if necessary, for all your subnets.

You have added the range(s) to discover to your proposed new configuration, but your changes will not take effect until after you have reviewed and activated your changes.

Delete an IPv4 range

To delete an IPv4 range:

1 From **Administration** > **Network configuration** > **List IPv4 ranges**.

2 Select the IPv4 range.

If the range has subranges, Enterprise Discovery gives you a choice of deleting only the range or of deleting the range plus all of its subranges.

3 Click **Delete this IPv4 range**.

4 Click **Delete**.

You have deleted the range in your proposed new configuration, but your change will not take effect until after you have reviewed and activated your changes.

Setting up the IPv4 range(s) to avoid

Within an IP range that you have added, there may be an IPv4 range that your network does not use. For each subnet in your network that you want Enterprise Discovery to avoid, add a new IPv4 range.

To add a range of IPv4 addresses:

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

2 Enter the starting and ending IPv4 addresses for your network.

3 For **Property Set/Group**, select **Network: Do not allow discovery**.

Enterprise Discovery will not perform network discovery on this IPv4 range.

4 Click **Submit**.

Repeat steps 1 to 4, if necessary, for all the subnets you want Enterprise Discovery to avoid.

You have added the range(s) to avoid to your proposed new configuration, but your changes will not take effect until after you have reviewed and activated your changes.

Adding ranges for DHCP servers and unmanaged routers

If you have one or more SNMP-managed DHCP servers or you have unmanaged routers, add their IPv4 addresses and apply the appropriate Property Group so that Enterprise Discovery will monitor the ranges differently.

To add IPv4 addresses to be treated as DHCP servers or unmanaged routers:

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

2 Enter the starting and ending IPv4 addresses for the DHCP server or unmanaged router. (If it's a range consisting of one device, the starting and ending IPv4 addresses are the same.)

3 For **Property Set/Group**, select one of the default Network Property Groups, **DHCP server** or **Unmanaged router**.

Enterprise Discovery gives the device the properties it should have.

4 Click **Submit**.

Repeat steps 1 to 4, if necessary, for all the devices you want Enterprise Discovery to treat as DHCP servers or unmanaged routers.

You have added the range(s) to be treated as DHCP servers and unmanaged routers to your proposed new configuration, but your changes will not take effect until after you have reviewed and activated your changes.

Merging IP Ranges

Note: A range can consist of one device. The starting and ending IPv4 addresses are the same.

Note: If you decide that two adjacent IPv4 ranges really should not be separate, you can merge them. The ranges must have identical properties or you cannot merge them.

To merge IPv4 ranges:

1 **Administration > Network configuration > Merge IPv4 ranges.**

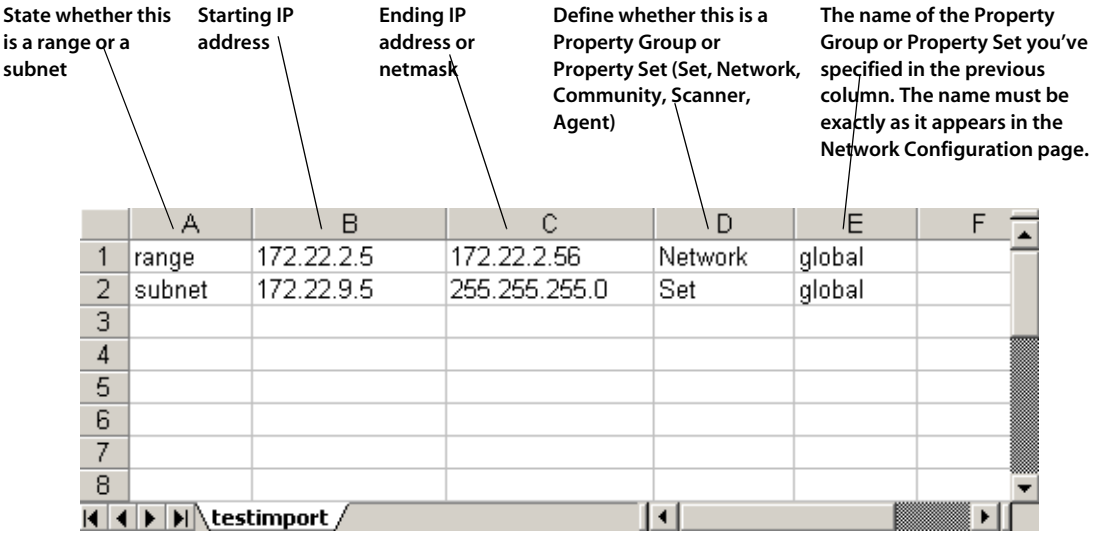
Enterprise Discovery displays all adjacent ranges sharing identical properties along with what the results of merge will be.

2 Click **Merge**.

You have merged any adjacent identical IPv4 ranges in your proposed new configuration, but your changes will not take effect until after you have reviewed and activated your changes.

Importing your IPv4 Ranges from a CSV File

Instead of entering all your IP ranges manually, you can import them from a CSV file. The file must be set up properly, as in the example below.



Note: This feature imports the IP ranges and the names of the Property Groups/Sets. The individual property settings must be configured if you want to change the defaults.

To import IPv4 ranges from a CSV file:

1. Click **Administration** > **Network configuration** > **Import IPv4 Range Definitions**.
2. Click the **Browse** button to select your CSV file.
3. If you wish to delete your existing IPv4 ranges before you import the CSV file, click **Yes**.
4. Select a default Property Group/Set.

Note: If you have not specified Property Groups/Sets in your CSV file, you can choose one to apply to all of your IPv4 ranges. If you have specified Property Groups/Sets for some of the IP ranges in the CSV files, the ones in the CSV file will take precedence. If you do not specify Property Groups/Sets in the CSV file, and you do not select a default, the IP range will not be imported.

5 Click **Import**.

Once you import the CSV file, you will see a report explaining whether or not the import was successful. Read the report carefully to ensure that all your IPv4 ranges have been imported properly.

Note: By default, Enterprise Discovery will insert the "global" IPv4 range of 0.0.0.0 - 255.255.255.255, even if you have not listed it in your CSV file.

You have imported your IPv4 ranges, but your changes will not take effect until after you have reviewed and activated your changes.

Exporting your IPv4 ranges to a CSV file

You can export a CSV file as a way of keeping an external record of your IPv4 ranges. Also, you can modify the configuration in the CSV file and then "import" them.

Note: This feature exports the IP ranges and the names of the Property Groups/Sets. The individual property settings are not included in the CSV file.

To export the IPv4 ranges:

1 Click **Administration** > **Network configuration**.

2 On the **List IPv4 Ranges** line, click **CSV Export**.

3 Save the file.

Activating your proposed changes

The **Activate Changes** page allows you to review all the changes you have proposed for Enterprise Discovery network configuration before actually making those changes take effect.

If you have completed all the changes you wanted to make, Activate the changes. For more information, see Activating Your Configuration Changes on page 111.

Making Future Changes to Your Configuration

In this chapter, there were instructions to set up discovery quickly and simply just to get started. The instructions are to apply the Network Property Group, "Active discovery", to all of your IPv4 range or ranges and give them all the same set of community strings.

You can leave discovery set up that way, if it is satisfactory to you. In fact, if there is a lot of change in your network, leaving it alone may be the best thing to do. However, you *can* set discovery up more precisely. For instance, you may want to reduce overhead on the network, or you may have a lot of community strings for security reasons and want to set up separate ranges for them. You can pick out IPv4 ranges or individual devices for Enterprise Discovery to handle differently.

Enterprise Discovery allows you to set up a matrix of network discovery, analyzing your network both geographically and functionally. For example, you might arrange discovery for an IPv4 range in a particular building one way and single out all the routers or servers across your network another way.

A tree of IPv4 ranges

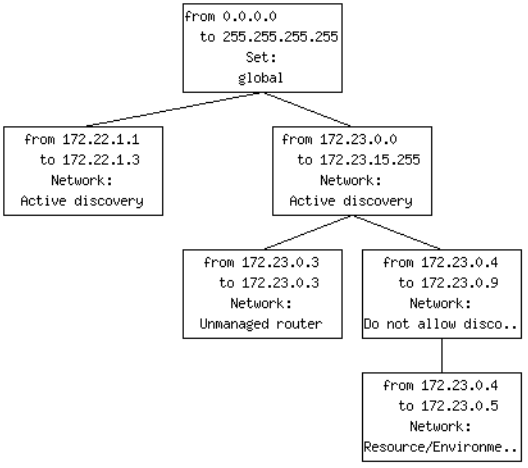
Enterprise Discovery actually works harder when it doesn't find devices than when it does, because it keeps trying. Once Enterprise Discovery has been running for a while, you may know that some ranges can be deleted or that they need less than full active discovery.

On the other hand, you may decide you want even more information from certain ranges.

So far, you have Enterprise Discovery set up to examine every device the same way. If you want to look at some parts of the network or some individual devices differently or not at all, add ranges that you want to have treated differently. You can then apply Property Groups to the ranges.

You will be creating a tree of ranges and the tree can be as complicated as necessary to have Enterprise Discovery monitor your network the way you want.

IPv4 Range	Property Set/Group Name
|--[0.0.0.0 to 255.255.255.255]	Set: global
| |--[172.22.1.1 to 172.22.1.3]	Network: Active discovery
| |--[172.23.0.0 to 172.23.15.255]	Network: Active discovery
| | |--[172.23.0.3 to 172.23.0.3]	Network: Unmanaged router
| | |--[172.23.0.4 to 172.23.0.9]	Network: Do not allow discovery
| | | |--[172.23.0.4 to 172.23.0.5]	Network: Resource/Environment manage



What Next?

To	Go to
Learn about Property Groups and Sets	Chapter 8, Setting up Property Groups and Property Sets
To create Network Property Groups	Chapter 9, Setting up Network Property Groups
To create Community Property Groups	Chapter 10, Setting up Community Property Groups
To create Agent Property Groups	Chapter 11, Setting Up Agent Property Groups and Agent Deployment Accounts
To create Scanner Property Groups	Chapter 12, Setting Up Scanner Property Groups and Scheduling Scanners
To Activate your configuration changes	Chapter 13, Activating Your Configuration Changes

CHAPTER 8 Setting up Property Groups and Property Sets

In this chapter, you will learn the difference between Property Groups and Property Sets. The following topics will be covered:

Introduction

Property Groups and Property Sets allow you to control the kind of data Enterprise Discovery can obtain from your network devices.

You can use these Groups and Sets to determine where Enterprise Discovery will distribute Agents, run Scanners, and how Enterprise Discovery will access your network devices.

Property Groups

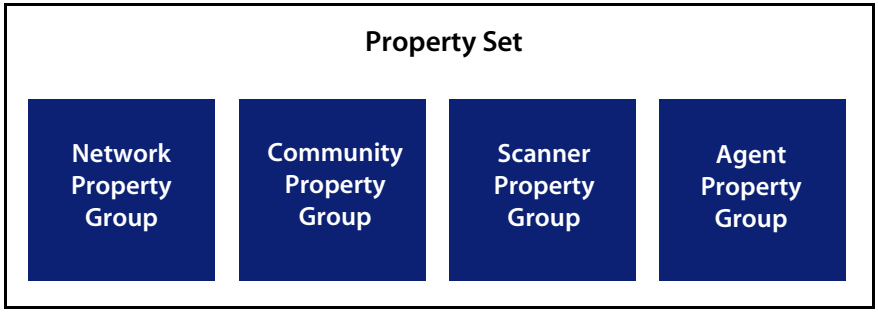
Enterprise Discovery comes with default property groups you can apply to the IPv4 ranges you set up. A property group contains characteristics or properties that distinguish a range from other ranges, especially from its parent range. You can also modify the default Property Groups and create new ones.

There are four kinds of property groups:

- Network—for properties that govern network discovery
- Community—for community strings
- Scanner—for Scanner deployment
- Agent—for Agent deployment

Property Sets

The use of Property Sets is optional. A Property Set is a collection of Property Groups. Applying a Property Set to a range is a convenient way of applying more than one Property Group at a time.



For example: If you find you are setting up several ranges and applying the Network Property Group, "Active discovery", and then setting up the same ranges with a Community Property Group you have defined, you might find it easier to create a Property Set. Property Set "X" can contain the Network Property Group, "Active discovery" and your Community Property Group with the strings you added. It's a shortcut to save you from entering IPv4 ranges more than once.

You should always give your Property Sets meaningful names, for example "servers" or "routers" so you can apply it to specific portions of your network.

You can list, add, modify and delete Property Sets, the same way you do with Property Groups.

What Next?

To	Go to
Create Network Property Groups	Chapter 9, Setting up Network Property Groups
Create Community Property Groups	Chapter 10, Setting up Community Property Groups
Create Agent Property Groups	Chapter 11, Setting Up Agent Property Groups and Agent Deployment Accounts
Create Scanner Property Groups	Chapter 12, Setting Up Scanner Property Groups and Scheduling Scanners
Apply your Property Groups to an IP range	Chapter 7, Configuring your Network IP Ranges
Activate your configuration changes	Chapter 13, Activating Your Configuration Changes

9 Setting up Network Property Groups

CHAPTER

In this chapter, you will learn how to set up Network Property Groups. The following topics will be covered:

Introduction

Network Property Groups are groups of settings that can be applied to IP ranges (see Configuring your Network IP Ranges on page 67). Depending on the devices located in different ranges, you may want Enterprise Discovery to treat each range differently. For example, you may want "Active Discovery" for one IP range, and "Do not allow Discovery" for another.

Enterprise Discovery comes with many default Network Property Groups. You can add, change, or delete them if you want. However, in most cases, the default settings will be sufficient for your needs.

To see a list of all Network Property Groups:

- **Click Administration > Network configuration > Network Property Groups > List Network Property Groups**

The list is a table with the names of the groups on the left and the names of the properties across the top.

The Properties

Each Network Property Group contains the same properties, but the value of each property is different—"on," "off," or "inherit"—depending on the group. If a group "inherits" a value, it takes whatever value belongs to the parent range of any range the group is applied to.

You can change any of the Network Property Groups, or add your own as you become better acquainted with Enterprise Discovery. It is important to understand that Enterprise Discovery has a series of hardcoded default settings for these properties, and the user cannot change them. This means that even the "global" property group can "inherit" settings from this hardcoded list.

The following properties are in every Network Property Group:

Property	Purpose	Hardcoded Default Setting
Allow devices	Allow devices to be added	Off
Actively ping	Actively ping devices for discovery	Off
NetBIOS query	Query devices for their NetBIOS names (the computer user names)	Off
Resource/Environment manage	Query devices for resource management	Off
Force ARP table read	Force ARP table to be read	Off
Accumulate IP Addresses	Accumulate IP addresses instead of replacing them	Off
Allow IP addresses	Set to **Off** when multiple servers have the same IPv4 address that you don't want to see, for instance, when you are using Network Address Translation (NAT). Set to **On** when you want to allow the repeated IPv4 addresses to be included.	On

Property	Purpose	Hardcoded Default Setting
Allow ICMP and SNMP	Pinging and polling is turned off, so devices will not be modelled. If the device is already in the database, Enterprise Discovery will still poll and ping the device for other reasons. Although pinging and polling is turned off, devices can still be scanned and included in the database.	Off
Device modeler interval	Determines how frequently Enterprise Discovery updates your view of the network. The device modeler interval is not "on," "off," or "inherit", but rather "set" or "inherit". If the value is set, it is set to a specific time.	172800 seconds (48 hours)

How to use Network Property Groups

Some of the property groups cause Enterprise Discovery to give you more data than others, but in doing so they also generate more traffic on the network and cause more load on the device being monitored. It can be a trade-off, a balance between efficiency and performance. You might choose to do less discovery on some parts of the network and more on others.

To Perform More Discovery

These groups offer more discovery power, but take more network bandwidth to run.

Property Group	Purpose
global	The starting point, assigned to the 0–255 range. Almost completely set to off, but does allow IP addresses.
Active discovery	Ping, poll, table read. Find devices and information about them to add to database.

Property Group	Purpose
Resource manage	The most active of the Network Property Groups. Provides disk, CPU, and memory information from servers, printers or UPSs.
Unmanaged router	In this Property Group, **Accumulate IP addresses** is set to "on". For routers that do not have SNMP management enabled.
DHCP Server	This Property Group has **Force ARP table read** set to "on". For servers providing Dynamic Host Configuration Protocol (DHCP) services, or for any other device (except routers) with a large ARP cache.

To Perform Less Discovery

These groups take less network bandwidth to run, but will not find as much data about your devices.

Property Group	Purpose
Do not allow discovery	For ranges that you do not want Enterprise Discovery to ping and poll.
Do not resource manage	Use it as a "child" range of a **Resource Manage** range.
Passive Discovery	Enterprise Discovery does not actively look for devices, but will include them if it happens to find them. (For example, Enterprise Discovery may be able to gather the information from the ARP cache of a device.)
Restrict to scanned-only	For IPv4 ranges where there is only information from scan files.
Remove Address	Used for removing IP addresses from the device model.
All off	The least active of the default Property Groups. For use when it's easier to turn a range off than to delete it.

Making changes to Network Property Groups

The default Network Property Groups will almost certainly meet your needs, but if they do not, you can create your own.

Important: Once you create new Property Groups, make sure to **Activate** your changes.

Note: If a Property Group has been altered, the shortcut menu of "add", "modify", and "delete" has an additional entry, "Reset to default".

Modify a Network Property Group

Modify a Network Property Group:

1. Click **Administration** > **Network configuration** > **Network Property Groups** > **Modify a Network Property Group**.
2. Select the Network Property Group you want to modify.
3. For each parameter, click **On** or **Off** or **Inherit**.
4. Click **Submit**.

Create a Network Property Group

Add a Network Property Group:

1. **Click Administration** > **Network configuration** > **Network Property Groups** > **Add a Network Property Group.**
2. Give your new Property Group a name.
3. Give your new Property Group a description.
4. For each parameter, click **On** or **Off** or leave it at the default value, **Inherit**.
5. Click **Submit**.

Delete a Network Property Group

You can delete a Network Property Group that no longer meets your needs and is just cluttering up the list.

Note: Before you can delete a Property Group, you must remove it from any IPv4 ranges to which it has been applied. If the Property Group belongs to a Property Set that has been applied to a range, you can delete the Property Group. The Property Set will then set the deleted values to "inherit".

Delete a Network Property Group:

1. **Click Administration > Network configuration > Network Property Groups > Delete a Network Property Group.**
2. Select the Network Property Group you want to delete.
3. Click **Select**.
4. Click **Delete.**

Note: You cannot erase default Property Groups.

What Next?

To	Go to
To create Community Property Groups	Chapter 10, Setting up Community Property Groups
To create Agent Property Groups	Chapter 11, Setting Up Agent Property Groups and Agent Deployment Accounts
To create Scanner Property Groups	Chapter 12, Setting Up Scanner Property Groups and Scheduling Scanners
Apply your Property Groups to an IP range	Chapter 7, Configuring your Network IP Ranges
To Activate your configuration changes	Chapter 13, Activating Your Configuration Changes

10 CHAPTER Setting up Community Property Groups

In this chapter, you will learn how to set up Community Property Groups. The following topics will be covered:

Introduction

Community Property Groups are groups of community strings that can be applied to IP ranges (see Configuring your Network IP Ranges on page 67). Depending on the devices located in different ranges, you may want Enterprise Discovery to use different community strings. For example, you may have a series of read/write community strings for your network workstations, and a different set of read/write community strings for servers.

Note: Community strings are the only property associated with an IP range that does not allow inheritance.

The one default Community Property Group is "global." If you are not sure what strings apply to your devices or subnets, you can add all of your community strings to this global list.

If you do not add any community strings, but keep "public" (the default) in the list, Enterprise Discovery will attempt to read the MIB of all devices in the defined IP range or set of ranges using only "public."

Note: If you do not add any community strings and delete "public" from the global Community Property Group (that is, if no community strings are defined) Enterprise Discovery will not interrogate any devices in your network. As a result, Enterprise Discovery will discover devices but may not be able to identify them.

Warning: Do not delete "public" from the global Community Property Group unless you are absolutely sure you do not need it.

Adding community strings—the quick way

If all of your devices have the community string, "public", you don't need to read this section or add any community strings.

As a quick method of adding your community strings, just add all your strings to the "global" Community Property Group.

Note: Community strings are case-sensitive. "PUBLIC" and "public" are two different strings.

To add community strings to the global Community Property Group:

1. Click **Administration** > **Network configuration** > **Community Property Groups**.
2. Click **Modify a community property group**.
3. Select **Community: global** from the pull-down list.
4. Click **Select**.
5. Under the heading **Add a Community String** enter a string name, and select the appropriate **Type** (**read** or **write**, or both).
6. Click **Add**.
7. Repeat steps 5 and 6 for each of your community strings.

8 When you add community strings, the order is important. Are your most frequently used community strings at the top of the list? If necessary, select a community string and click the **Move Up** or **Move Down** button to move it to the right place.

9 Click **Submit**.

Note: To assign different community strings to different IPv4 ranges, refer to the next chapter, Setting up Property Groups and Property Sets on page 79.

Creating new Community Property Groups

If you are more concerned with security, and you have community strings for particular devices or subnets, you can create a Community Property Group with a "list" of strings. You then apply the Community Property Group to the IPv4 range or ranges. Remember that you must activate any changes to Network configuration in order to have the changes take effect.

To create a Community Property Group:

1 **Click Administration > Network configuration > Community Property Group > Add a community property group.**

2 Give a name to the Community Property Group. Use a name that is meaningful to you.

3 Add a description.

4 Under the heading **Add a Community String** enter a string name, and select the appropriate **Type** (**read** or **write**, or both).

5 Click **Add**.

6 Repeat steps 4 and 5 for each community string that can be applied to the same set of devices or subnets.

7 If necessary, select a community string and click the **Move Up** or **Move Down** buttons to move it to the right place.

When you add community strings, the order is important, make sure the most frequently used strings are at the top of the list.

8 Click **Submit**.

To apply the Community Property Group to the IPv4 range:

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

2 Click **Add by interval** and enter the starting and ending IPv4 addresses for the range you want.

3 In the **Choose existing Property Set/Group** drop-down list, select the name of your newly created Community Property Group.

4 Click **Submit**.

Deleting a community string

You can delete a single community string, or you can delete an entire Community Property Group of community strings. Be sure you know which procedure you want to perform.

You cannot delete an entire Community Property Group if an IPv4 range is using it.

To delete a single community string:

1 Click **Administration** > **Network Configuration** > **Community Property Groups** > **Modify a community property group**.

2 Select a Community Property Group from the pull-down list.

3 Click **Select**.

4 Under the "Delete a Community String" heading, select the community string you want to delete and click **Submit**.

You have deleted a single community string from a Community Property Group in your proposed configuration, but your change will not take place until you activate changes.

To delete a Community Property Group:

1 Click **Administration** > **Network configuration** > **Community Property Groups** > **Delete a community property group**.

2 Select a Community Property Group from the pull-down list and click **Select**.

3 Click **Delete**.

You have deleted a Community Property Group from your proposed configuration, but your change will not take place until you activate changes.

What Next?

To	Go to
To create Network Property Groups	Chapter 9, Setting up Network Property Groups
To create Agent Property Groups	Chapter 11, Setting Up Agent Property Groups and Agent Deployment Accounts
To create Scanner Property Groups	Chapter 12, Setting Up Scanner Property Groups and Scheduling Scanners
To Activate your configuration changes	Chapter 13, Activating Your Configuration Changes
Apply your Property Groups to an IP range	Chapter 7, Configuring your Network IP Ranges

CHAPTER 11 Setting Up Agent Property Groups and Agent Deployment Accounts

In this chapter, you will learn how to set up Agent Property Groups and Agent Deployment Accounts. The following topics will be covered:

Introduction

Agent Property Groups are groups of settings that can be applied to IP ranges (see Configuring your Network IP Ranges on page 67). Depending on the devices located in different ranges, you may want Enterprise Discovery to treat each range differently.

Enterprise Discovery comes with many default Agent Property Groups. You can add, change, or delete them if you want. However, in most cases, the default settings will be sufficient for your needs.

Before you can deploy agents to the computers in your network, you must first configure the Agent Deployment Accounts. By entering the correct Admin account name and password, Enterprise Discovery will be able to install the Agents automatically.

Note: To ensure the Agent deployment works properly, you can also configure some Agent Communication Settings. For more information, see the *Configuration and Customization Guide*.

What is an Agent?

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

Important: For those users who are upgrading from Network Discovery and Desktop Inventory (Enterprise Discovery 1.0), you will have to replace the old Listener with the new Enterprise Discovery Agent. You can do this as you set up your new ED property groups. See Upgrading your Custom Application Library on page 147 for more information.

For new users of Enterprise Discovery, you can start with setting up Agent Property Groups. These groups will ensure that agents are distributed to workstations as they are discovered by Enterprise Discovery.

Configure Agent Deployment Accounts to give Enterprise Discovery access to the workstations

When you set up an Agent Deployment Account, it is equivalent to having Enterprise Discovery log in to your network computers as an administrator. Once Enterprise Discovery has access to the computer, it can then deploy the agent to that computer.

This usually is an administrator account. As multiple accounts can be used in the network, you can enter multiple account names/passwords. The order in which the accounts are tried are as follows:

- The account names that match the network's model workgroup name. The network's model workgroup is normally available when NetBIOS over

TCP/IP is enabled on the remote computer. This allows the appropriate administrator account to be used first.

- The account names where the domain name is not specified (local administrator accounts).
- Any other remaining accounts.

Enterprise Discovery tries to connect to the remote computer's ADMIN$ share using the administrator account names and passwords provided. Once a connection is established, Enterprise Discovery installs the Agent on the remote computer.

Note: This feature uses remote execution capabilities found in Windows NT/200x/XP operating systems.

For it to work properly on Windows XP with Service Pack 2, one of the following should apply:

- The firewall is off
- The firewall is on, but the "File and Printer sharing" is enabled in its exception list
- Remote Administration is enabled and the “do not allow exceptions” setting is turned off

Important: This method of Agent deployment uses Windows RPC, and does not work on computers with Windows 9x/ME.

Configuring the Agent Deployment Accounts:

1. Click **Administration** > **Agent deployment accounts** > **Add an agent deployment account**.
2. Enter the account name.
3. Enter the Login.
4. Enter the password (twice).
5. Click **Submit**.

List deployment accounts	View existing deployment accounts.
Change sort order of deployment accounts	Change the order in which deployment accounts are tried.

Add a deployment account	Add a new deployment account.
Deployment account properties	Modify an existing deployment account.
Delete a deployment account	Delete an existing deployment account.

Distributing Agents with Agent Property Groups

An Agent Property Group is a named group of agent-related settings. These settings can later be applied to one or more IP Ranges of devices to scan (see Configuring your Network IP Ranges on page 67).

Important: The Listener Uninstall option is only needed by users who are upgrading from Network Discovery and Desktop Inventory. Do not change this default unless you are upgrading.

To define an agent property group:

1. Click **Administration** > **Network Configuration** > **Agent Property Groups** > **Add an Agent Property Group**.
2. Give the property group a name. For example, '**Windows Workstations**'
3. Add a description.
4. Enter the following information for your Agent Property Group:

Option	Explanation
Agent Upgrade	Select **On** if you want to upgrade your Agents automatically. Select **Off** if you do not want the Agent upgraded automatically. Select **Inherit** if you want the parent IP range to dictate Agent upgrades.
Agent Upgrade Schedule	These are the same schedules used for Scanner distribution. You can create your own at **Administration** > **Schedule Management**.

Option	Explanation
Agent Action	Select **No Action** if you want no action at all. Select **Deploy** if you want to automatically deploy Agents to the computers in this IP range. Select **Uninstall** if you want to automatically uninstall the Agents from the computers in this IP range. Select **Inherit** if you want the parent IP range to dictate the Agent Action.
Listener Uninstall	Select **On** if you want to uninstall the old Desktop Inventory Listeners automatically. Select **Off** if you do not want the old Desktop Inventory Listeners uninstalled automatically. Select **Inherit** if you want the parent IP range to dictate Listener Uninstall.
Collect Utilization Data	Select **On** if you want to collect utilization data. Select **Off** if you do not want to collect utilization data. Select **Inherit** if you want the parent IP range to dictate utilization data collection.

5 Once you have done this, click the **Submit** button. A summary appears.

6 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.

What Next?

To	Go to
Create Network Property Groups	Chapter 9, Setting up Network Property Groups
Create Community Property Groups	Chapter 10, Setting up Community Property Groups
Create Scanner Property Groups	Chapter 12, Setting Up Scanner Property Groups and Scheduling Scanners
Activate your configuration changes	Chapter 13, Activating Your Configuration Changes

To	Go to
Apply your Property Groups to an IP range	Chapter 7, Configuring your Network IP Ranges
Manually deploy agents (UNIX and Windows)	the *Configuration and Customization Guide*

12 CHAPTER Setting Up Scanner Property Groups and Scheduling Scanners

In this chapter, you will learn how to set up Scanner Property Groups and Schedules. The following topics will be covered:

Introduction

Scanner Property Groups are groups of settings that can be applied to IP ranges (see Configuring your Network IP Ranges on page 67).

Once you have installed Agents on to your network devices, you can start deploying Scanners. The Scanners will run on the devices, and send back scan files to the Enterprise Discovery server for processing and storage.

After the scan file is delivered to the server, the XML Enricher process the scan file, adding application data.

Scheduling Scanners

Before you set up your property groups, you should think about when you want the scanners to run on your network. Enterprise Discovery gives you complete control over the scanning schedules. You can configure when you want Enterprise Discovery to perform the following actions:

- Scanner Upgrade Schedule
- Scanner Run Schedule
- Scan File Download Schedule

For example, you could set it up so the scanners are upgraded on a Monday, the scanners run on Tuesday, and the scan files downloaded to the server on Wednesday.

To set up a Schedule:

1. Click **Administration** > **Schedule management** > **Add a schedule**.
2. Give the schedule a name.
3. Use the pull down menus to select the days and times to add to your schedule.

   You can add multiple day, hour, and minute ranges, and delete them as required.
4. Click **Submit**.

Defining Scanner Property Groups

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 Configuring your Network IP Ranges on page 67).

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:

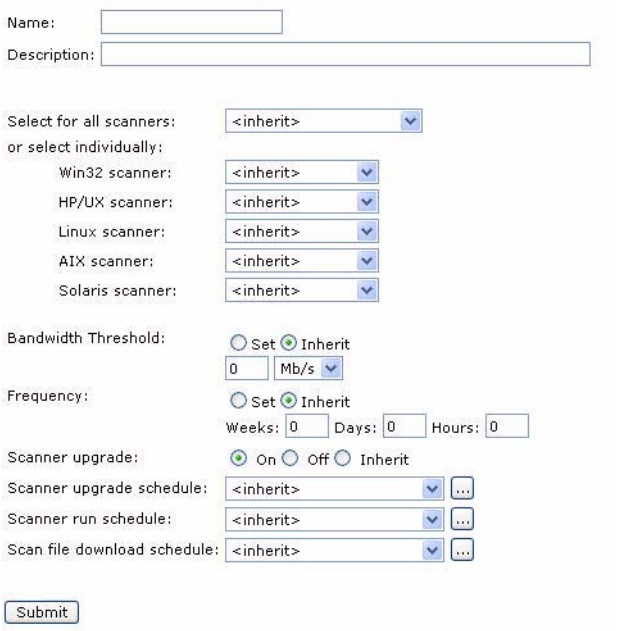
  - Win32
  - HP/UX
  - Linux
  - AIX
  - Solaris

- Choose the maximum bandwidth allowed for scanner deployment/scan file download.
- 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:



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

3 Add a description if you need to.

4 Continue to configure your Scanner Property Group by making the following changes:

- Choosing which Scanners are applied to the devices in your network on page 105
- Setting the bandwidth threshold on page 106
- Setting the frequencies of scans on page 107
- Setting scan schedule properties on page 107

Choosing which Scanners are applied to the devices in your network

You can select Scanner configuration files:

- For all Scanners at once (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:

Scanner	Description
<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
<defaultdelta>	The same as <default> but with delta scanning turned on.
<fastsw>	This configuration does a fast software scan of your machines - no signaturing, file identification, etc.
<fastswdelta>	The same as <fastsw> but with delta scanning turned on.
<hwonly>	This configuration does a hardware scan only of your machines.
<hwonlydelta>	The same as <hwonly> but with delta scanning turned on.

Note: You can also create your own Scanner configuration files using Scanner Generator. Refer to the *Configuration and Customization Guide* for more information on how to do this.

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 its parent IP range.

Setting scan schedule properties

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

- <**None**> - No scan schedule will be set for the property, meaning that scanners can be run all the time.
- <**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** pull-down list. If you created a schedule in Scheduling Scanners on page 102, it appears in this pull-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** pull-down list. If you created a schedule in Scheduling Scanners on page 102, it appears in this pull-down list.

To set the Scan file download schedule:

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

- Select an option from the **Scan file download schedule** pull-down list. If you created a schedule in Scheduling Scanners on page 102, it appears in this pull-down list.

What Next?

To	Go to
To create Network Property Groups	Chapter 9, Setting up Network Property Groups
To create Community Property Groups	Chapter 10, Setting up Community Property Groups
To create Agent Property Groups	Chapter 11, Setting Up Agent Property Groups and Agent Deployment Accounts
To Activate your configuration changes	Chapter 13, Activating Your Configuration Changes
Apply your Property Groups to an IP range	Chapter 7, Configuring your Network IP Ranges

To	Go to
Configure more Scanner settings	the *Configuration and Customization Guide*
Learn more about Scanners	the *Reference Guide*

13 CHAPTER Activating Your Configuration Changes

In this chapter, you will learn how to activate your configuration changes. The following topics will be covered:

Introduction

You must activate any changes to the system in order to have the changes take effect. If you have made a lot of changes, you should first review the setup and the changes.

Reviewing Your Changes

Before activating your changes, it is advised that you review the changes you want to make.

To review proposed changes:

1 Click **Administration** > **Network configuration** > **Review changes.**

A tree diagram of your proposed IPv4 ranges appears, along with a table detailing all the changes made in this section.

Enterprise Discovery tells you how many potential devices it will have to explore, and how long it will take to ping each address scheduled for active discovery (for example, “at least 33 minutes”).

Enterprise Discovery also shows you any configuration problems it detects. You can ignore the warnings, but do so at your own risk.

2 If you wish to see details on the proposed changes to the IPv4 ranges, you can click on the tree diagram to expand it.

New ranges appear in green. Changes to existing ranges are in yellow. Removed ranges are in grey.

3 Review the changes to make sure the new configuration is correct.

If you decide to implement the changes you have made, applying the changes will update your network configuration. You can also discard all changes.

Discarding the Changes

To discard current changes:

1 Click **Administration** > **Network configuration** > **Reset to previous configuration**.

2 Click **Undo**.

Activating the Changes

To activate your current changes:

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

Warning: If you configuring the network for the first time, but you already have scan files in the Enterprise Discovery database, you will see a warning on the Activation page. Before activating your changes, make sure to add IP ranges for these devices, or you will lose the scan data.

2 Click **Activate Changes**.

Checking that Enterprise Discovery is working as expected

There are a couple of things you can do to make sure Enterprise Discovery is up and running properly. If you are unsure of why some devices are appearing, and other devices are not appearing, here are some suggestions to help you investigate.

Peregrine Systems recommends waiting at least 48 hours while Enterprise Discovery is first discovering your network. If you have concerns after that, call customer support.

Check the Server License Limit

On the server web UI, check the Home Page. There you will see the number of **Devices Discovered**, and the **Percentage of Device License**. You should see these numbers change within minutes of activating your configuration.

Check the Device Filters report

There may be devices on your network that do not appear because the devices are being filtered. To check if any devices are being filtered out, check the Device Filters report.

To check the Device Filters Report:

- Click **Status** > **Device Status** > **Filtered devices**

To see a full list of possible filters, click **Help** > **Classifications** > **Device Filters**.

Check the Device Modeling Queue

During the initial discovery of your network, the modeling queue may show devices, depending on the size of your network and how quickly Enterprise Discovery is discovering and modelling devices. At most other times, the queue will be empty.

To check the Device Status Reports:

1. Click **Status** > **Device Status** > **Network model queue** to view the devices that are waiting to be network modeled.

2. Click **Status** > **Device Status** > **Network model processing** to view the devices that are in the process of being network modeled.

3. Click **Status** > **Device Status** > **Agent Deployment Queue** to view the devices that are waiting to have Agents deployed.

4. Click **Status** > **Device Status** > **Scanner model processing** to view the devices that are currently being scanned.

What Next?

To	Go to
Add user accounts	Chapter 14, Setting up Accounts
Configure your data backups	Chapter 16, Backing up and Restoring your data

14 Setting up Accounts

CHAPTER

In this chapter, you will learn how to set up accounts so your staff can access Enterprise Discovery. The following topics will be covered:

Introduction

Once you have set up the Enterprise Discovery server and configured Enterprise Discovery, you should set up accounts. For each account, you can configure the name, password, and other important information. Make sure anyone who needs to work with Enterprise Discovery has an account, and knows the limits of their account level.

There are four pre-installed accounts

Enterprise Discovery comes with four accounts pre-installed, one of each of the following types:

- Demo
- IT Employee
- IT Manager
- Administrator

The Enterprise Discovery Administrator must create all other accounts.

Account Name	Account Type	Name	E-mail Address
admin	Administrator	Administrator	n/a
demo	Demo	Demo Account	n/a
itemployee	IT Employee	IT Employee	n/a
itmanager	IT Manager	IT Manager	n/a

How many people can use Enterprise Discovery at once?

Enterprise Discovery supports a maximum of 250 accounts.

More than one account can be used at a time. Up to 20 accounts can use any part of Enterprise Discovery simultaneously.

How the types of accounts differ

Each type of account has different permissions. The principal difference between the types of account is the amount of administration permitted.

- Demo—limited control, “safe” for demonstration and training
- IT Employee—can make some changes that affect what their own account sees
- IT Manager—can make changes that affect what other accounts see

- Administrator—the most powerful, sets up Enterprise Discovery, sets up more accounts
- Scanner—exclusively used to upload scan files.

For a full list of account properties and capabilities, refer to the *Configuration and Customization Guide*.

Warning: While it is possible to create more than one Administrator account, we recommend you have only one Administrator account. That account should be reserved for use by the Enterprise Discovery Administrator. If you have more than one Administrator account, there is a danger that each Administrator account will overwrite the work of all others.

Creating accounts

To create a usable account, you must add an account, then assign a password.

You should also modify the capabilities of the account and the contact data for the person who owns the account.

You can also modify the properties of the account, but this is optional; the account owner can perform these actions on his or her own account.

Whether you just create an account or whether you customize each account for each owner is your decision. You may consider such factors as the number of accounts to be created, how knowledgeable each account owner is, and the restrictions of your work environment.

To create an account:

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

2 Enter an account name.

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

- a through z
- 0 through 9

- hyphen (-) (the hyphen cannot be the first character in the account name)
- underscore (_) (the underscore cannot be the first character in the account name)

3 Click **Add Account**.

You have created an IT Employee account.

Note: Even though the account has been created, it cannot be used until you assign it a password. An account without a password is considered disabled. The account owner will not be able to use it to log in to Enterprise Discovery.

After you create an account, a shortcut menu appears.

You can use the shortcut menus to continue working with the account.

To create a password for an account:

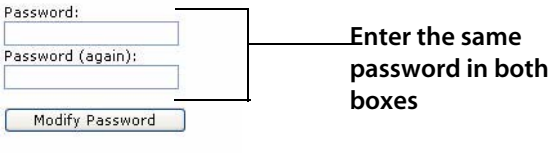
Note: Alternative: If you see a brief menu on the screen, click **Modify account password**, then skip to Step 4.

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

2 Select the account from the list box.

3 Click **Modify Account**.

4 Enter an account password in both boxes.



5 Click **Modify Password**.

The account may now be used.

You can change the account type or customize any of its other properties or capabilities in **Administration** > **Account administration** > **Account properties/Account capabilities**. For more detail, refer to the *Configuration and Customization Guide*.

To change an account type:

1 Click **Administration** > **Account administration** > **Account capabilities**.

2 Select the account from the list box.

3 Click **Modify Capabilities**.

4 Select the account type from the list box.

Note: You should have a single Administrator account. That account should be reserved for use by the Enterprise Discovery Administrator. If you have more than one Administrator account, there is a danger that each Administrator account will overwrite the work of all the others.

5 (optional) Change any other account capabilities, as appropriate.

6 Click **Modify Capabilities**.

(Optional) More Account Administration

There are other account settings you may want to set. For more information on these topics, refer to the *Configuration and Customization Guide*, or read the help information associated with each feature in **Administration** > **Account administration**.

Feature	Description
Server passwords	These are global settings for all account passwords. Change the length of passwords, password history, and the number of allowed login attempts.
Account capabilities	These settings control the account type, the access to Enterprise Discovery components, and password expiry. Only Administrator users can access this menu.
Account properties	These settings control how the user will view data in Enterprise Discovery.

Note: You can make changes to your own account at **Administration** > **My account administration**.

CHAPTER 15 Setting up Enterprise Discovery Aggregation

In this chapter, you will learn how to set up an Aggregator server to collect data from multiple remote Enterprise Discovery servers. The following topics will be covered:

Introduction

If you have purchased an Aggregator license, this chapter will show you how to set up and use the Enterprise Discovery Aggregator. To use the Aggregator, all of your Enterprise Discovery servers must be at least Enterprise Discovery version 2.0.

Installing the Aggregator Hardware

The Aggregator is the backbone of your Enterprise Discovery system, collecting device data from up to 10 remote servers.

Install your Aggregator as you would any Enterprise Discovery server, as described in Server Installation on page 25.

Your Aggregator server must have considerably more disk space than a regular Enterprise Discovery server. You will require 6GB for the operating system and Enterprise Discovery software. For every 10,000 devices, you should have an additional 1GB of disk space. For example, if you want to monitor 500,000 devices with your Aggregator, you will need 56GB of disk space.

Warning: Do not configure your IP ranges, Agents, or Scanners until you have completed Sharing Security Keys between all your Servers on page 125.

Installing the Aggregator license

Only one Enterprise Discovery server on your network needs to have the Aggregator license. So, you must decide which server that will be. If you are not sure how to decide, contact Peregrine Systems Customer Support.

For details on installing the license, see Installing the License on the Server on page 28.

Important: The Aggregator server will require more hardware resources (larger disk, more RAM) than a regular Enterprise Discovery server. See Server Installation on page 25 for details.

Installing the Remote Enterprise Discovery Servers

Follow the instructions in Server Installation on page 25 to install each remote server.

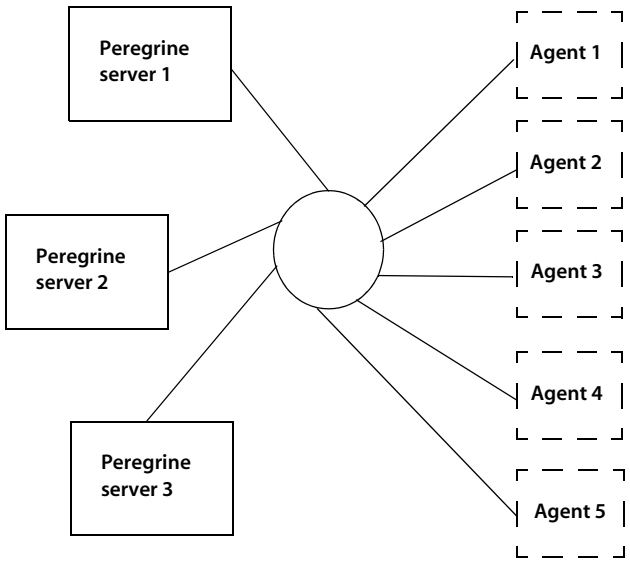
Warning: Do not configure your IP ranges, Agents, or Scanners until you have completed Sharing Security Keys between all your Servers on page 125.

Sharing Security Keys between all your Servers

When you install Enterprise Discovery, it automatically generates a unique security key. When you are aggregating multiple servers, you should make sure all the servers have the same security keys.

Warning: If you fail to share the security keys across all Enterprise Discovery servers, you will encounter major communication problems in your network, as the servers communicate with network devices and each other.

The following conceptual diagram shows a network where all Enterprise Discovery servers have the same security keys.



This can be accomplished in a few simple steps:

- Copy the security keys from one server to a floppy disk or USB key.
- Copy those security keys from the floppy to the other server(s).

Important: For security reasons, do not copy the security keys over the network.

Copying the Security Key files to a floppy disk:

1 Select one Enterprise Discovery server in your network as the "master" server. This will most often be the Aggregator server, but it can be any Enterprise Discovery server in your network. You will use the security keys from this server to copy to the other Enterprise Discovery servers in your network.

2 Log in to the server as an Administrator.

3 On the "master" server, either insert a floppy disk into the disk drive, or plug in a USB key.

4 Copy the files from the Cert directory (..\Application Data\Peregrine\Enterprise Discovery\Cert) onto the floppy disk/USB key.

5 Remove the floppy disk from the drive, or remove the USB key from the server.

Copying the Security Key files onto the other servers:

Note: Repeat the following steps on all other Enterprise Discovery servers on your network.

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

1 Either insert the floppy disk into the disk drive, or attach the USB key to the Enterprise Discovery server.

2 Copy the files from the floppy disk to the Cert directory (..\Application Data\Peregrine\Enterprise Discovery\Cert).

3 Either remove the floppy disk from the drive, or remove the USB key.

4 Restart your Enterprise Discovery server.

Configuring the Aggregator

For the Aggregator to work, you must prepare the Aggregator and you must prepare each individual server. You give the Aggregator:

- the IP address or DNS name of the remote server
- the remote account
- the Aggregate health update interval
- the Aggregate events update interval

On each individual Enterprise Discovery server you set up an account that allows access to the Aggregator.

To set up the Aggregator to access a remote server:

1 On the Aggregator, click **Aggregate Administration** > **Remote server administration** > **Add a remote server**.

2 Enter the IP address or DNS name, and the name of the remote server.

3 Click **Add**.

4 Click **Modify Properties**.

5 Enter a remote account (example, "admin") to collect data for the Aggregate Health Panel.

Note: This can be any account on the remote server, as long as the account has its web access enabled, and is of the same type (Demo, IT Employee, IT Manager, or Admin), and has the same password as an account on the Aggregator.

6 Select data transfer intervals:

- Aggregate network inventory
- Aggregate events
- Aggregate workstation inventory

Note: More frequent updates use more bandwidth.

7 Click **Change**.

Setting up the Remote Servers

You must also set up each remote server separately. Perform this procedure on each remote server that you wish to be aggregated.

To set up the remote servers:

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

2 Follow the on screen instructions to create an account that matches the account name you configured on the Aggregator (Configuring the Aggregator on page 127).

You have now added the appropriate account. Next, you must configure the remote server so it can send data to the Aggregator.

3 Click **Administration** > **System preferences** > **Aggregate configuration.**

4 Give the remote server a unique ID.

5 Enter how long you would like the Aggregator to keep the database files from this server.

6 Click **Change**.

Navigating through multiple servers

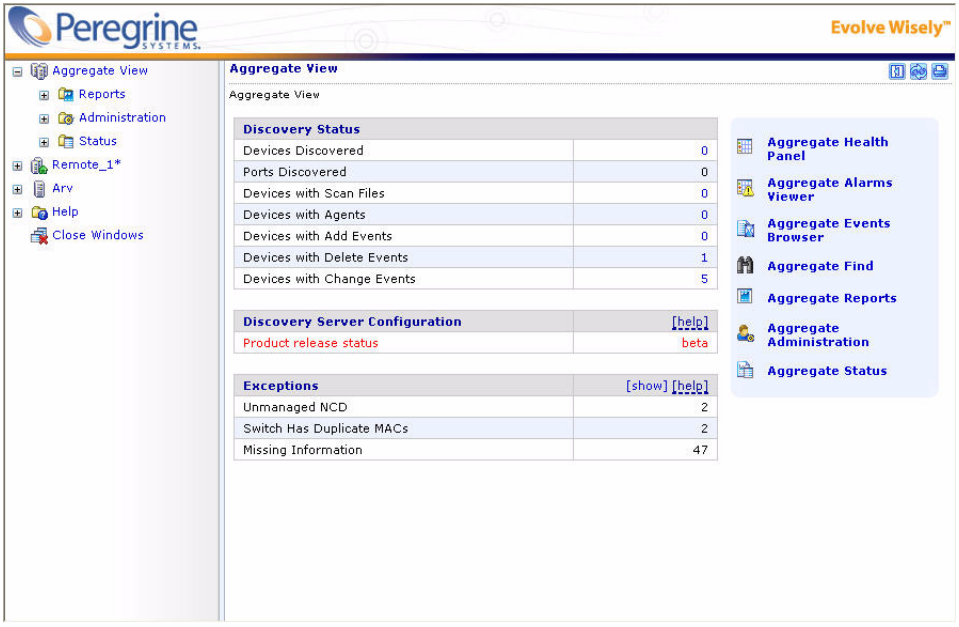
You can use the navigation frame on the left side of your window to look at the Aggregator, or any of your remote servers.

You must be careful, because this flexibility allows you to open windows for any number of remote servers at the same time. The window you are looking at may be showing you:

- aggregated data
- unaggregated data from the Aggregator itself
- data from any of your remote servers.

To be sure what you are looking at, check the name in the banner at the top of the window.

Important: There can be duplicate devices. The Aggregator does not eliminate duplicates. If a device has been included in discovery ranges for more than one remote server, you will see that device appear multiple times in an Aggregate Health Panel report.



Deleting Remote servers

By deleting a server from the list of "remote servers," the Aggregator will no longer communicate with that server. The remote server itself will still function and collect data from its portion of the network, but that data will not be passed along to the Aggregator.

To delete a remote server from the Aggregator:

1. On the Aggregator, click **Administration** > **Remote server administration** > **Delete a remote server**.
2. Select a remote server and click **Delete**.
3. A confirmation message appears.
4. Click **Delete**.

What Next?

To	Go to
Configure your individual servers	Chapter 3, Server Installation

16 CHAPTER Backing up and Restoring your data

In this chapter, you will learn how to back up your Enterprise Discovery data, and how to restore it if necessary. The following topics will be covered:

Introduction

In order to backup your data, Enterprise Discovery automatically creates a series of backup files every 24 hours (shortly after midnight). Depending on your configuration, Enterprise Discovery will save the following files:

File	Description
certs.zip	Contains all certificates.
MySQL.zip	Contains a series of SQL scripts to compose your MySQL tables.
data.zip	Contains all the files from your data directory, except for files that are already in their own backup zip file.
scans.zip	Contains all of your scan files.

Important: The Certificates are saved with every backup. However, it is highly recommended that you also save these to an alternate location (burn them onto a CD, and store it safely). For more information, see Save your Certificates to a Safe Location on page 38.

These files will be split up if any zip file is over 1GB. For example, if you have 3GB of scan files, you will get three files named **scans.001.zip**, **scans.002.zip**, and **scans.003.zip**.

Note: Each backup zip contains a file called version.properties, which contains the backup time stamp, IP address of your Enterprise Discovery server, and the current version of your Enterprise Discovery software.

You can find the backup files in a "Backup" subdirectory of the Data directory.

The following data is not backed up by Enterprise Discovery:

- License information in the registry.
- Log files.
- The absolute path of your directory hierarchy. Instead, the backup file contains the path to the files relative to the `Data` directory.

Warning: The backup performed by Enterprise Discovery saves the data onto the server's Data Directory. It is up to you to move those files to another location, such as another server or a tape drive.

Setting up your backups

You have control over whether Enterprise Discovery backs up your scan files. Not saving scan files will save you a lot of disk space, especially if you have a large number of scanned devices.

Important: If you choose to not include the scan files in your backup, you must back up the scan files yourself. You can copy the files to another location if you wish. If you do not back up the scan files anywhere, you risk losing all of your scan data in the event of server failure.

To stop Enterprise Discovery from backing up your scan files:

1. Click **Administration** > **System Preferences** > **Server configuration**.
2. Set the **Backup Scan Files** option to "No."
3. Click **Change**.

Backing up your data immediately

If you have made substantial changes to your network or network configuration, you may want to backup your data immediately rather than waiting for the daily automatic backup.

To back up your data immediately:

1 Click **Administration** > **Data management** > **Run backup now**.

2 Click **Confirm**.

Restoring your data

Important: Restoring overwrites the active data. This action cannot be undone.

Warning: Windows security permissions are not retained after a restore. Once you perform a restore, you will have to reapply the Peregrine Security Template. See Enterprise Discovery Security Template on page 140.

Enterprise Discovery creates an internal backup every night. You can restore your data from this backup if you need to do so.

There is no user interface involved in restoring your data from the backup.

You must create a `restore` directory, and copy your latest backup files into that location, Enterprise Discovery will automatically do a restore when you next restart your server.

To restore your backup data to the server:

1 Create an empty directory called “Restore” in the Data directory.

2 Add your latest backup files to the restore directory. You must include at least the following files:

- certs.zip

- MySQL.zip
- data.zip

And may include the “scans.zip” file as well.

3 Restart your Enterprise Discovery server.

When the server has restarted, you will see that the current network data reflects what was in the backup files. You will also see that the “Restore” directory you created has disappeared, and that your original backup files are in the “backup” directory.

17 CHAPTER Uninstalling Enterprise Discovery

In this chapter, you will learn how to uninstall Enterprise Discovery.

Note: A complete uninstall may take 10-20 minutes.

Removing Enterprise Discovery Components

To remove Enterprise Discovery components installed on your system:

1. In Control Panel|Add/Remove Programs, select the Peregrine Enterprise Discovery entry.
2. Click **Add/Remove**. Follow the on screen instructions.

18 CHAPTER Security Checklist

In this chapter, you will learn how to ensure that your Enterprise Discovery server is secure. The following topics will be covered:

Introduction

Although your Enterprise Discovery server will operate even if you do not follow these procedures, we strongly recommend that you take the following steps to reduce risk.

Accessing Enterprise Discovery

Peregrine recommends doing two separate installations of Enterprise Discovery: server and client.

Peregrine recommends that you only access the web user interface through the server on which the software is installed. By accessing the server through the intranet, it is possible that a person with a network sniffer would be able to decipher your administrative passwords, or your local admin and domain passwords that need to be entered for deployment.

Enterprise Discovery Security Template

The Enterprise Discovery security template protects your software by preventing unauthorized users from gaining access to critical data files and registry settings.

Click **Start** > **All Programs** > **Peregrine** > **Enterprise Discovery 2.0** > **Install Security Template**. Once you make that selection, the following security settings will be automatically applied to your system.

Folder security for user accounts:

Folder	Security Measure
C:\Perl	Read-only access
..\Peregrine	Read-only access
..\Application Data\Peregrine\Enterprise Discovery\LiveAgents	No visibility
..\Application Data\Peregrine\Enterprise Discovery\Scans	Read-only access
..\Application Data\Peregrine\Enterprise Discovery\Database\mysql	No visibility
..\Application Data\Peregrine\Enterprise Discovery\Cert	No visibility

Registry security for user accounts:

Registry	Security Measure
HKLM\ SYSTEM \CurrentControlSet\Services\prgnXmlEnricher	Read-only access
HKLM \SYSTEM\CurrentControlSet\Services\prgnWatchdog	Read-only access
HKLM \SYSTEM\CurrentControlSet\Services\prgnTomcat	Read-only access
HKLM \SYSTEM\CurrentControlSet\Services\prgnSysmon	Read-only access
HKLM \SYSTEM\CurrentControlSet\Services\prgnSched	Read-only access
HKLM \SYSTEM\CurrentControlSet\Services\prgnLogger	Read-only access
HKLM \SYSTEM\CurrentControlSet\Services\prgnDiscEng	Read-only access
HKLM \SYSTEM\CurrentControlSet\Services\prgnDiscDB	Read-only access
HKLM \SYSTEM\CurrentControlSet\Services\prgnAuth	Read-only access
HKLM \SYSTEM\CurrentControlSet\Services\prgnApache	Read-only access
HKLM \SYSTEM\CurrentControlSet\Services\prgnAgentComm	Read-only access
HKLM \SOFTWARE\Peregrine Systems	Read-only access

Place your Enterprise Discovery server behind your institution/corporation's firewall

The Enterprise Discovery server stores a lot of information about your network. You do not want this information to be publicly available.

Use the built-in Windows firewall

You should enable the built-in Windows firewall that comes available with Windows 2003 SP1 (or Windows XP SP2, if this is a demo or trial installation).

There are several ports that you should enable in the firewall to allow Enterprise Discovery to work properly. Information about the firewall ports to enable is in the *Planning Guide*.

Change the write community string of the Enterprise Discovery server

This is a documented community string, known to:

- Admin accounts at your site
- existing and prospective Enterprise Discovery customers

Anyone who knows the default write community string will be able to change the SNMP MIB of your Enterprise Discovery server.

Eliminate known account names “admin” “itmanager”, “itemployee”, and “demo”

These are documented account names, known to:

- users at your site
- existing and prospective Enterprise Discovery customers

  Anyone who knows the default account names may be able to gain access to your Enterprise Discovery server more easily, even if you have changed the passwords for the accounts.

If you don’t want to delete the accounts, at least change the password for the “admin” account.

Anyone who knows the default password for the “admin” account may be able to gain top-level access to your Enterprise Discovery server.

There is information about accounts in Setting up Accounts on page 117.

Change the default Admin password

Note: When you change the password for the admin account, you will have to log in again. (It is always necessary to log in again when you change the password for the account you are using.)

Passwords can be 4–20 characters long by default. The minimum password length can be specified in **Administration** > **Account administration** > **Server passwords**.

The password may contain upper and lower case letters (A–Z and a–z), numerals (0–9), underscores (_), hyphens (-), at signs (@), and periods (.).

To change the admin account password:

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

Apply all Microsoft OS patches

When Microsoft introduces new security patches for your Windows OS, make sure to install it. Use the Windows Update feature to keep Windows updated with the latest security features.

19 CHAPTER Installing Knowledge Updates

In this chapter, you will learn how to keep your Enterprise Discovery software up-to-date with the latest Discovery Knowledge. You should install these product updates on a regular basis.

It is important to keep your Enterprise Discovery software up-to-date, to ensure the continued accuracy of the collected data.

Note: An updated Discovery Knowledge Package will normally be available monthly, whereas new Agent and Scanner packages will be available as necessary.

There are four kinds of updates that can be contained in a Discovery Knowledge Package:

- Scripts
- SAIs
- MIB
- Rulebase

Important: When a new version of Enterprise Discovery is made available, you will need to upgrade your software before applying new packages. See the *Release Notes* for upgrade instructions.

To Install the Discovery Knowledge Package:

1 Copy the 'cab' file into the following directory (this is the default setting; if you have installed the product in a different location, make sure to place the file in the correct location):

```
C:\Program Files\Peregrine\Enterprise Discovery\2.0.0\Install
```

2 Restart your Enterprise Discovery server so it can recognize the update.

Enterprise Discovery then validates the package signature and applies it to the system. If the package is invalid, it is discarded and the system is unchanged. If there are any problems with installation, check the `package-verify.log` file in the `Logs` directory. It contains the details of the package verification process.

20 CHAPTER Upgrading your Custom Application Library

In this chapter, you will learn how to upgrade your Custom Application Library.

Introduction

Customers who have used Desktop Inventory 7.x and 8.x will need to follow these procedures to upgrade their application libraries so they can work with Enterprise Discovery 2.0.

If you have...	You will need to...
Desktop Inventory 7.x	■ Migrate Your ApE Database ■ Use the SAI Update Wizard to Upgrade Your Old Read Only SAIs
Desktop Inventory 8.x	■ Migrate Your ApE Database

Important: You must complete these procedures before uninstalling the old software.

Migrate Your ApE Database

Carry out this procedure if you want to migrate the data in your Application Encyclopedia (ApE) database to a user SAI for use in Enterprise Discovery 2.0.0.

Important: Before carrying out this procedure, ensure that you have not removed the old software from your machine.

To migrate your old ApE database:

- From your old software, export the contents of the database to a read-only SAI file.

Information on how to do this can be found in the *Application Encyclopedia Users Guide* supplied with your Desktop Inventory software.

This exported file will be a read-only SAI that you will update for use in Enterprise Discovery 2.0.0 software.

Use the SAI Update Wizard to Upgrade Your Old Read Only SAIs

SAI Update Wizard is used to:

- Convert read-only SAIs to an Enterprise Discovery User SAI.
- Convert old Peregrine Desktop Inventory User SAI to the User SAI format used by Enterprise Discovery.

When a read-only SAI is updated, applications taught by the customers are extracted into a new User SAI.

When a User SAI is updated, a standalone User SAI is created. If an application is linked to a publisher in the Master SAI, the publisher information is written to the User SAI so that it no longer relies on the Master SAI.

Starting the SAI Update Wizard

To start the SAI Update Wizard:

- From the Windows **Start** menu select **Programs|Peregrine|Enterprise Discovery 2.0.0|SAI Update Wizard**.

Exiting the SAI Update Wizard

To exit the SAI Update Wizard:

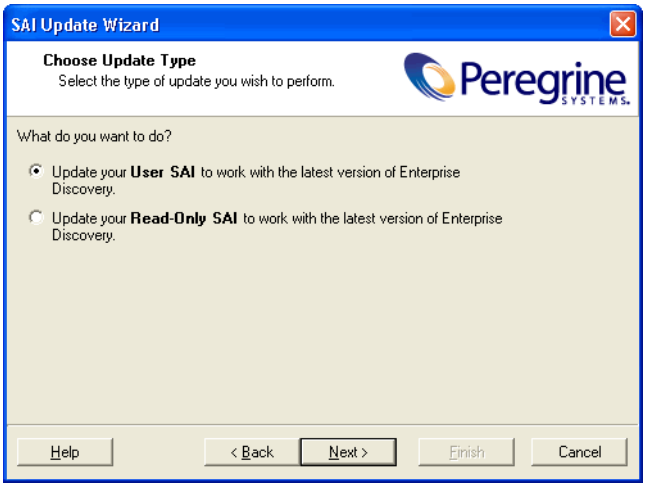
- Click the Windows close icon or click the **Cancel** button.

Welcome Page

On starting the SAI Update Wizard, the following page appears.

Click the **Next** button to continue.

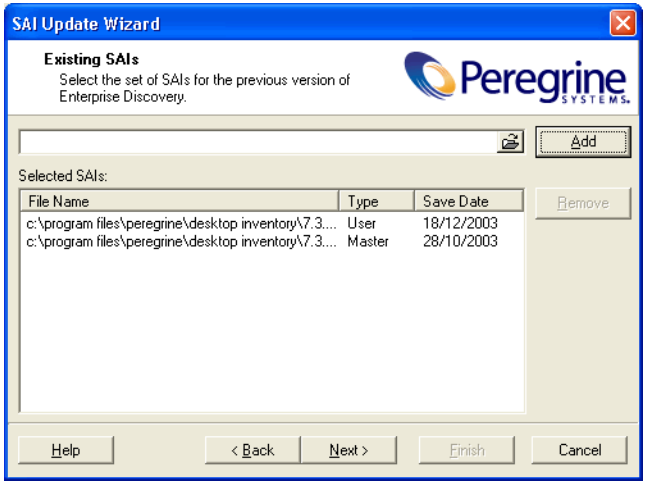
Choose Update Type Page



This page has two options:

- Update your User SAI to work with the latest version if Enterprise Discovery
- Update your Read-Only SAI to work with the latest version of Enterprise Discovery

If you chose the **Update your User SAI to work with the latest version if Enterprise Discovery** option, the following dialog is displayed.



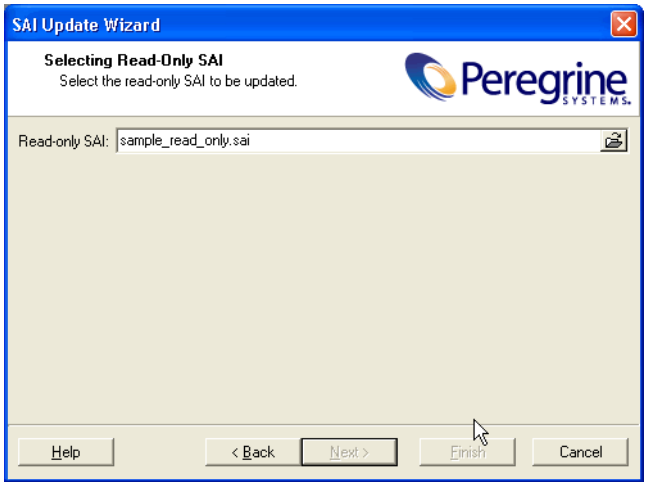
1 Select your existing (old) Master SAI files and the (old) User SAI file. Navigate to the files and add them individually by clicking the **Add** button.

   The SAI files you have selected will be shown in the bottom pane.

   You need to load all the Master files that you had loaded when you created the User SAI file. An error message appears if the incorrect files are selected.

2 Click the **Next** button to continue.

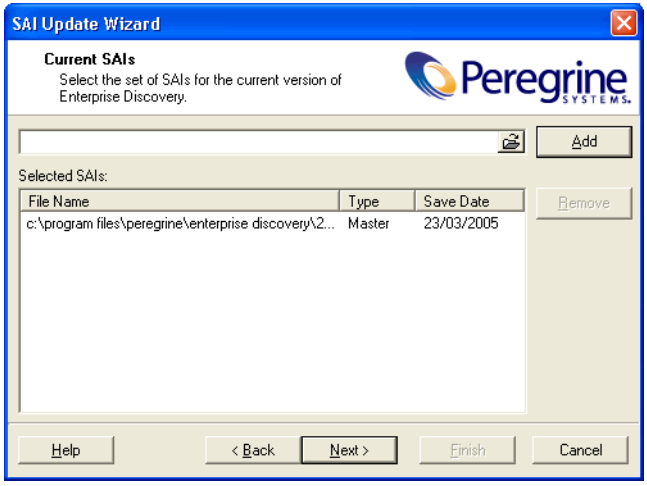
If you chose the **Update your Read-Only SAI to work with the latest version of Enterprise Discovery** option, the following dialog is displayed.



1 Select your existing (old) Read Only SAI file to be updated.

2 Click the **Next** button to continue.

Current SAIs Page

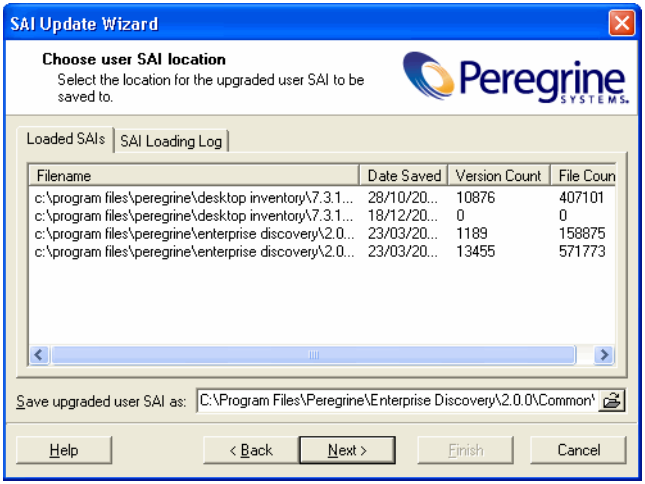


1 Select the new Master SAI file(s). Navigate to the files and add them individually by clicking the **Add** button.

2 Any SAI files you have selected are shown in the bottom pane.

3 Click the **Next** button to continue.

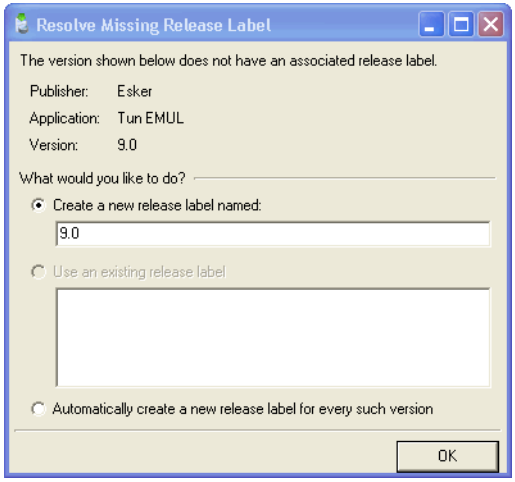
Choose User SAI Location Page



1 Enter a location to save the new upgraded User SAI file to.

2 Click the **Next** button to continue.

You may see the **Resolve Missing Release Label** dialog if the SAI file contains a version with no associated release label.



3 Create a new release label name for the specific application version.

4 You can use an existing release label if the application already had release labels. These are shown in the Use an existing release label pane if they exist.

5 Automatically create a new release label for every such version - Checking this option has the same effect as selecting the first option every time this dialog appears.

6 Click the **Next** button to continue.

Summary Page

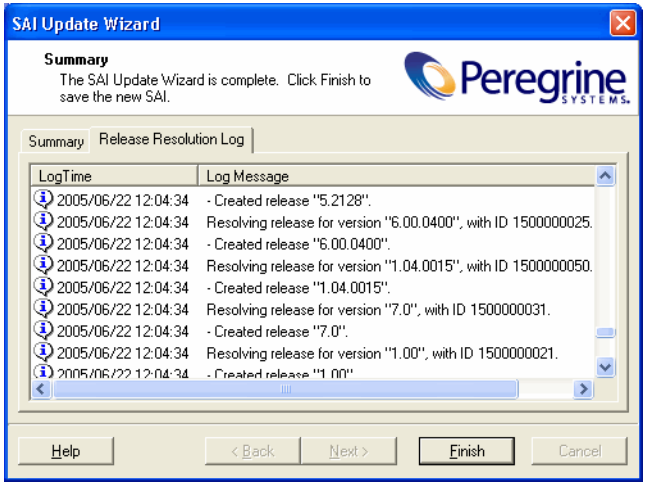
Summary Tab Page

This screen shows a summary of the following for the newly updated User SAI:

- Number of publishers
- Number of Application
- Number of Releases
- Number of Versions
- Number of Files
- How many pre-upgrade Version Relations were translated to Release Relations in the new file.

Release Resolution Log

This screen shows the results of any action that were carried in the **Resolve Missing Release Label** dialog if missing release labels were encountered.



Click the **Finish** button. The SAI update procedure is completed.

21 CHAPTER Contacting Customer Support

In this chapter, you will learn how to contact support, and allow the support team access to your data (if necessary). The following topics will be covered:

Introduction

There may be times when customer support will need access to your server to help diagnose an issue. In order to help accelerate the process, we recommend that you prepare for support to gain access.

Using Windows Remote Desktop

On your Enterprise Discovery server, enable access for an outside user with the native Remote Desktop feature.

1. From the Control Panel, select **System**.
2. Click the **Remote** tab.
3. Click the **Select Remote Users** button and configure an administrative account for Customer Support.

Note: It can be a local account, but must have administrative privileges.

For more details, check your Microsoft documentation.

Using Virtual Network Computing (VNC)

If Windows Remote Desktop is not appropriate for you, we recommend using VNC via VPN instead. WinVNC is freeware that comes highly recommended.

What Support Needs to Know

When you call Customer Support, please have the following information available:

- Customer number.
- The operating System installed on your server.
- The version of Enterprise Discovery, including the build number (click Status > Current settings > License status).
- The latest knowledge package that you have installed on the server.
- Any other software that you have installed on the server.
- Where to find log files that may be requested by support. (the specific log file will depend on the problem). The logs are available at `C:/Documents and Settings/All Users/Application Data/ED/2.0.0/logs`.

Contacting Support

For further information and assistance with this release or Enterprise Discovery in general, contact Peregrine's Customer Support.

Peregrine's CenterPoint Web site

Contact information for local support offices is available through the main contacts shown below or through Peregrine's CenterPoint Web site: http://support.peregrine.com

After logging in with your login and password:

- Select **General Information**, on the left.

Under **Customer Support References**, select **Support Contacts Worldwide**.

Corporate Headquarters

Contact Customer Support at Peregrine headquarters using one of the following:

Address:	Peregrine Systems, Inc.
Attn:	Customer Support
	3611 Valley Centre Drive
	San Diego, CA 92130 USA
Telephone:	(1) (800) 960-9998 (US and Canada only, toll free)
	+ (1) (858) 794-7428
Fax:	+ (1) (858) 480-3928
Email:	support@peregrine.com

PEREGRINE

Index