HP OpenView Enterprise Discovery

for the Windows operating system

Software Version: 2.1.1

Installation and Initial Setup Guide

hp

invent

Legal Notices

Warranty

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

The information contained herein is subject to change without notice.

Restricted Rights Legend

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

Copyright Notices

Trademark Notices

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

Java™ is a US trademark of Sun Microsystems, Inc.

UNIX® is a registered trademark of The Open Group.

Support

Peregrine Product Support

You can obtain support information for products formerly produced by Peregrine as follows:

- If you work with an HP OpenView Services Integrator (SVI) partner (www.hp.com/managementsoftware/svi_partner_list), contact your SVI agent.

- If you have an active HP OpenView support contract, visit the HP OpenView Support site and use the Self-Solve Knowledge Search to find answers to technical questions.

- For the latest information about support processes and tools available for products formerly produced by Peregrine, we encourage you to visit the HP-Peregrine Software Support web site at: www.hp.com/managementsoftware/peregrine_support where you can download the Customer Support Handbook.

- Contact your HP Sales Representative if you have additional questions.

HP OpenView Support

You can visit the HP OpenView Support web site at:
www.hp.com/managementsoftware/support

HP OpenView online support provides an efficient way to access interactive technical support tools. As a valued support customer, you can benefit by using the support site to:

- Search for knowledge documents of interest

- Submit and track support cases and enhancement requests

- Download software patches

- Manage support contracts

- Look up HP support contacts

- Review information about available services

- Enter into discussions with other software customers

- Research and register for software training

Most of the support areas require that you register as an HP Passport user and sign in. Many also require a support contract. To find more information about access levels, go to:

www.hp.com/managementsoftware/access_level

To register for an HP Passport ID, go to:
www.managementsoftware.hp.com/passport-registration.html

Contents

1 Welcome to Enterprise Discovery

Welcome to the *Installation and Initial Setup Guide*.

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

About Enterprise Discovery Installation

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.

Table 1   Component Locations

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\HP OpenView\Enterprise Discovery\2.1.1

⚠ Perl, MySQL, Tomcat and Apache are standard parts of the Enterprise Discovery, included with each server installation. If you have these components installed already, make sure to remove them before installing Enterprise Discovery. You may NOT substitute any other technologies in place of the standard installation.

License Options

The following packages are available:

Table 2   License Options

Option	Contents
1	Discovery + Inventory
2	Discovery + Inventory + Software Utilization
3	Discovery + Network Topology
4	Discovery + Inventory + Network Topology
5	Discovery + Inventory + Network Topology + Software Utilization

Discovery

With this license, Enterprise Discovery will ping and poll your network IP ranges to find devices. This will give you some basic information on the devices, such as when they are added to or removed from the network.

Inventory

With this license, you can create scanners to scan your network servers and workstations. You can automatically deploy agents to these devices, and then deploy the scanners to determine the hardware and software installed on each device. This data will be combined with the Discovery data in the Enterprise Discovery database.

Software Utilization

With this license, you can expand your inventory data, as the scanners will capture details on what software is used on each Windows® workstation, and report how often it is used and who is using it. You will see this Utilization data appear in the Scan Data Viewer, and in Reports.

Network Topology

With this license, you can expand your discovery data by calculating and displaying connectivity information for your network. Adding a topology license means that you will find additional alarms in the Health Panel/Alarms Viewer. This also adds many new Reports.

What Next?

To	Go to
Install the server components	Chapter 3, Server Installation
Install the client components	Chapter 4, Client Installation
Learn more details about how Enterprise Discovery works	*Reference Guide*

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, 2.0.x, or a migration from Desktop Inventory or Network Discovery.

Introduction

There are many ways you could be approaching your Enterprise Discovery 2.1 installation.

- New Installation on page 16
- Migrating from Desktop Inventory 7.x or later on page 18
- Migrating from Network Discovery 5.2.5 or later on page 26
- Upgrading from Enterprise Discovery 1.0 on page 27
- Upgrading from Enterprise Discovery 2.0 on page 31

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.

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. If you would like more details of how all the components work together, read the "How it Works" section in the *Reference Guide*.

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

Table 1   New Installation

Task		Instructions	Notes
1	Install the server components.	Server Installation on page 33	
2	Install the client components.	Client Installation on page 51	
3	Configure your server	Configuring your Enterprise Discovery Server on page 69	More details available in the *Customization and Configuration Guide*.
4	Set up Network and SNMP Property Groups	Setting up Network Property Groups on page 79 Setting up SNMP Property Groups on page 89	You can create these Property Groups, and add them to a Property Set. Then you can start applying the Sets/Groups to IP ranges in the next step.
5	Set up IP Ranges	Configuring your Network IP Ranges on page 113	

Table 1   New Installation

	Task	Instructions	Notes
6	Activate your changes	Activating Your Configuration Changes on page 125	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 103	Configure Enterprise Discovery to deploy agents to a small portion of your network to ensure your configuration is correct.
9	Activate your changes	Activating Your Configuration Changes on page 125	
10	Manually deploy UNIX® and Mac OS X agents	See the *Customization and Configuration Guide*.	This is required to automatically schedule scanning of UNIX/Linux and Mac OS X machines.
11	Repeat steps 8, 9, 10 for the remainder of your network.		
12	Set up Accounts	Setting up Accounts on page 129	

Migrating from Desktop Inventory 7.x or later

If you worked with Desktop Inventory, you will need to upgrade to Enterprise Discovery 2.1. Most of 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 2.1 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:

Table 2   Migrating from Desktop Inventory

Task		Instructions	Notes
1	Change Desktop Inventory to use XSF file format.	See the XSF white paper available from customer support.	
2	Migrate the data in your Application Encyclopedia (ApE) database to a read only SAI.	Migrate Your ApE Database on page 178	
3	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.
4	Install the Enterprise Discovery server components on the computers where you had a "complete install" of Desktop Inventory.	Server Installation on page 33	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.
5	Install the client components.	Client Installation on page 51	
6	If you were grouping your scan files, you need to reapply the same groupings.	Click **Administration > System Configuration > Scan File Management**	

Table 2   Migrating from Desktop Inventory

Task	Instructions	Notes
7	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
8	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 enriched scan files in xsf format and generate new Enterprise Discovery scanners with the same parameters.
9	Run the SAI Update Wizard to migrate your Desktop Inventory read-only and user SAIs to the new format used by Enterprise Discovery.	Convert Your Old Read Only or User SAIs on page 178	
10	Set up IP Ranges	Configuring your Network IP Ranges on page 113	
11	Set up Network and SNMP Property Groups	Setting up Network Property Groups on page 79 Setting up SNMP Property Groups on page 89	

Table 2   Migrating from Desktop Inventory

Task		Instructions	Notes
12	Activate your changes	Activating Your Configuration Changes on page 125	Wait until Enterprise Discovery has discovered all of those devices before continuing. Check **Status > Device status > Network model queue/Network model processing.**
13	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 103	Configure Enterprise Discovery to deploy agents to a small portion of your network to ensure your configuration is correct.
14	Activate your changes	Activating Your Configuration Changes on page 125	
15	Manually deploy UNIX and Mac OS X agents	See the *Customization and Configuration Guide*.	This is required to automatically schedule scanning of UNIX/Linux and Mac OS X machines.
16	Repeat steps 11, 12, 13, 14 for the remainder of your network.		

Table 2   Migrating from Desktop Inventory

Task		Instructions	Notes
17	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. You should move a maximum of 2500 scan files into the scans\incoming directory per day. This will provide the server with enough time to process all of them. If you add more than 2500 scan files in a day, some of them may be deleted. Also, you can add a new timestamp to each scan file so they do not age out prematurely. For this, you will need to find a utility for changing the timestamp in windows files.	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.
18	Upgrade to Connect-It 3.6.		Connect-It 3.6 is required to take advantage of the out-of-box scenarios for transferring data from the Enterprise Discovery database to AssetCenter.
19	Configure Connect-It to use the Discovery database.		This step is only necessary if you populate AssetCenter with scan file data.
20	Populate AssetCenter.		This step is only necessary if you populate AssetCenter with scan file data.
21	Set up Accounts	Setting up Accounts on page 129	

I want to use Enterprise Discovery 2.1 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:

Table 3   Migrating from Desktop Inventory

Task		Instructions	Notes
1	Change Desktop Inventory to use XSF file format.	See the XSF white paper available from customer support.	
2	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.
3	Install the Enterprise Discovery server components on the computers where you had a "complete install" of Desktop Inventory.	Server Installation on page 33	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.
4	Install the client components.	Client Installation on page 51	

Table 3   Migrating from Desktop Inventory

	Task	Instructions	Notes
5	Configure the Enterprise Discovery server to have a large scan only IP range.	Click **Administration>Network Configuration>Add IPv4 range** Enter the IP ranges and choose **Restrict to scan only** as the **Network Property** group. Activate the changes.	If the Enterprise Discovery server is not configured in this way then the XMLenricher will not process the scan files.
6	If you were grouping your scan files, you need to reapply the same groupings.	Click **Administration > System Configuration > Scan File Management**	
7	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
8	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 enriched scan files in xsf format and generate new Enterprise Discovery scanners with the same parameters.
9	Migrate the data in your Application Encyclopedia (ApE) database to a user SAI.	Migrate Your ApE Database on page 178	

Table 3   Migrating from Desktop Inventory

Task		Instructions	Notes
10	Migrate your SAIs.	Convert Your Old Read Only or User SAIs on page 178	
11	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. You should move a maximum of 2500 scan files into the scans\incoming directory per day. This will provide the server with enough time to process all of them. If you add more than 2500 scan files in a day, some of them may be deleted. Also, you can add a new timestamp to each scan file so they do not age out prematurely. For this, you will need to find a utility for changing the timestamp in windows files.	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.
12	Populate AssetCenter.		Use AssetCenter as you did before. You will want to adjust your Connect-It scenario to the new scans/processed directory.
13	Set up Accounts	Setting up Accounts on page 129	

Migrating from Network Discovery 5.2.5 or later

Network Discovery is the predecessor of Enterprise Discovery.

Table 4   Upgrading from Enterprise Discovery 1.0

	Task	Instructions	Notes
1	Upgrade to Network Discovery 5.2.5	See the *Network Discovery 5.2.5 Release Notes*.	
2	Install a new Enterprise Discovery server.	Server Installation on page 33	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 51	
4	Backup your Network Discovery data using the new **Migrate Data to Enterprise Discovery** feature.	See the *Network Discovery 5.2.5 Release Notes*.	
5	Restore that backup to your Enterprise Discovery server.	See the *Network Discovery 5.2.5 Release Notes*.	

Upgrading from Enterprise Discovery 1.0

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

Table 5   Upgrading from Enterprise Discovery 1.0

Task		Instructions	Notes
1	Upgrade to Network Discovery 5.2.5	See the *Network Discovery 5.2.5 Release Notes*.	
2	Install a new Enterprise Discovery server.	Server Installation on page 33	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 51	
4	Backup your Network Discovery data using the new **Migrate Data to Enterprise Discovery** feature.	See the *Network Discovery 5.2.5 Release Notes*.	
5	Restore that backup to your Enterprise Discovery server.	See the *Network Discovery 5.2.5 Release Notes*.	
6	Migrate your SAIs.	Convert Your Old Read Only or User SAIs on page 178	

Table 5   Upgrading from Enterprise Discovery 1.0

Task		Instructions	Notes
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.
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 103	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 125	
10	Manually deploy UNIX and Mac OS X agents	See the *Customization and Configuration Guide*.	This is required to automatically schedule scanning of UNIX/Linux and Mac OS X machines.
11	Repeat steps 8, 9 for the remainder of your network.		

Table 5   Upgrading from Enterprise Discovery 1.0

Task	Instructions	Notes
12	Move 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. You should move a maximum of 2500 scan files into the scans\incoming directory per day. This will provide the server with enough time to process all of them. If you add more than 2500 scan files in a day, some of them may be deleted. Also, you can add a new timestamp to each scan file so they do not age out prematurely. For this, you will need to find a utility for changing the timestamp in windows files.	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.
13	Upgrade to Connect-It 3.6.		Connect-It 3.6 is required to take advantage of the out-of-box scenarios for transferring data from the Enterprise Discovery database to AssetCenter.
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.

Table 5   Upgrading from Enterprise Discovery 1.0

Task		Instructions	Notes
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.
17	Clean up your old Desktop Inventory data.	**Administration > System Configuration > Scan deployment**. Enable the "Clean PDI data from workstations" option.	
18	Set up Accounts	Setting up Accounts on page 129	

Upgrading from Enterprise Discovery 2.0

In this scenario, you have been using the fully automated discovery features of Enterprise Discovery.

Follow these tasks to upgrade to Enterprise Discovery 2.1:

Table 6   Upgrading from Enterprise Discovery 2.0

Task		Instructions	Notes
1	Back up your Enterprise Discovery data.	See Chapter 16, Backing up and Restoring your data.	
2	Uninstall Enterprise Discovery 2.0	See Chapter 17, Uninstalling Enterprise Discovery	
3	Install Enterprise Discovery 2.1.1	See Chapter 3, Server Installation and Chapter 4, Client Installation.	

> ▶ After you upgrade to Enterprise Discovery 2.1, the icons in the applet windows (Map, Events Browser, etc.) may appear with an "X". The icons will return to normal after the web server has rebooted.

3 Server Installation

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. It can be installed on Windows 2003 Server SP1 (Windows® XP SP2 is also compatible, but should only be used for trial or demo installation).

The following table details a variety of scenarios that can help you estimate your server hardware requirements.

▶ Agg = Aggregator, Inv = Inventory, Top = Topology

Table 1   Suggested Hardware Requirements

Devices	Ports	Agg	Inv	Top	Memory (GB)	CPU	Disk (GB)
5,000	30,000		✔		1.5	1 CPU 2.4 GHz	25
5,000	30,000			✔	1.5*	1 CPU 2.8 GHz hyperthreading	15
5,000	30,000		✔	✔	2*	1 CPU 2.8 GHz hyperthreading	35
15,000	90,000		✔		2	2 CPUs 3.0 GHz hyperthreading	70
15,000	90,000			✔	3.5	2 CPUs 3 GHz hyperthreading	35
15,000	90,000		✔	✔	4	2 CPU 3 GHz hyperthreading	100

Table 1   Suggested Hardware Requirements

Devices	Ports	Agg	Inv	Top	Memory (GB)	CPU	Disk (GB)
50,000	100,000		✔		3	2 CPUs 3.6 GHz hyperthreading	200
50,000	100,000			✔	4	2 CPUs 3.6 GHz hyperthreading	50
50,000	100,000		✔	✔	5	2 CPUs 3.6 GHz hyperthreading	240
50,000	n/a	✔	n/a	n/a	2	2 CPUs 3 GHz hyperthreading	10
500,000	n/a	✔	n/a	n/a	3	2 CPU 3.6 GHz hyperthreading	50

* This is for 5 map sessions. If you want to use more than 5 map sessions, you will require more memory.

These calculations have been tested as scenarios for maximum disk size on the server. For the Inventory license, this includes:

- **Backup Scan Files** in enabled (on average, each scan file is 250KB)
- **Generate MIF Files** is enabled
- **Delta scanning** is enabled
- Space required for two backups (one stored backup, and one "in process" backup)

For the Network Topology license, this includes:

- **Statistic Export** is enabled (CSV files)

- 200 users, with each user account saving 10 map configurations files
- Space required for two backups (one stored backup, and one "in process" backup)

Disk Space

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

For performance reasons, the disk where Enterprise Discovery data is stored should have at least 4K blocks.

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.

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.

Table 2   Reducing disk space

Reduce the disk space needed by:	Explanation
Changing how long your server keeps the data being sent to the Aggregator.	Click **Administration > System Configuration > 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 Configuration > 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 Configuration > Scan file management**. This option is enabled by default.

Installing SNMP on the Server

You should have the Microsoft SNMP Agent installed on your Enterprise Discovery server. Without it, Enterprise Discovery will not be able to build a Network Map.

The SNMP agent should be configured to accept packets from any host. If this presents security issues for your site, you can configure it to allow access from only the IP address.

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

Installing the License on the Server

HP makes increased functionality available through license files.

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 license options:

- Number of devices (increments of 100)
- Network Topology
- Device Inventory
- Software Utilization
- Aggregation

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.

- ActivePerl is not already installed on the server.

- No other Windows applications are running, with the exception of your standard anti-virus software. .

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.

The following screen appears.

2   Click Install Enterprise Discovery to start the install process.

Next, the Preparing to Install window appears.
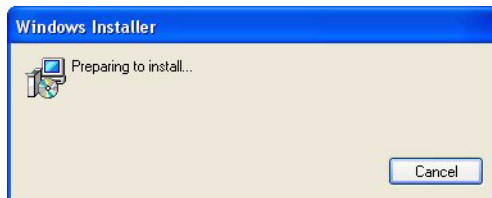
Next, the Installation Wizard appears.
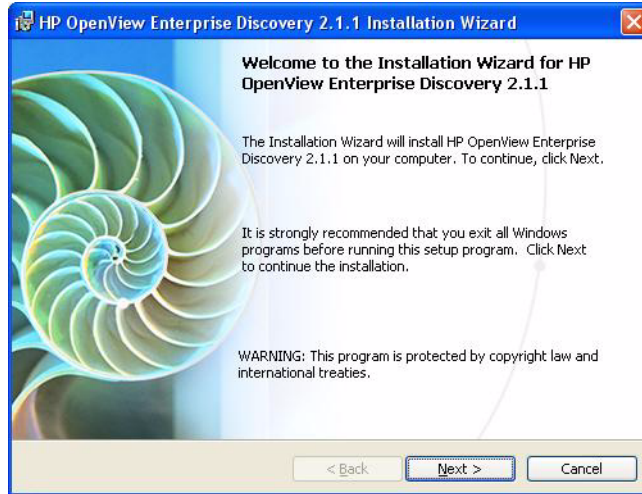
3 Click **Next**.

The Destination Folder screen appears.

The default installation directory is:

C:\Program Files\HP OpenView\Enterprise Discovery\2.1.1

▶ Enterprise Discovery must be installed on a local disk, and cannot be installed on clustered devices.

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

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

The Setup Type screen appears.

5   Select the "Server" Setup Type.

6   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.

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

The Select Data Folder screen appears.

8   To change the location of your Data folder, enter a new location.

If Enterprise Discovery has already been installed on this server, and you want to change the location of the data directory, you must manually move your data directory before continuing with this installation.

> You cannot put the data folder in the root directory (for example, C:).

> The Data folder cannot contain any data from other applications.

9 Click **Next**.

   The SSL Certificate Generation screen appears.

10 Enter the DNS name of the server. This will be used to generate the
    server's SSL certificate.

11 Click **Next**.

The Ready to Install the Program screen appears.
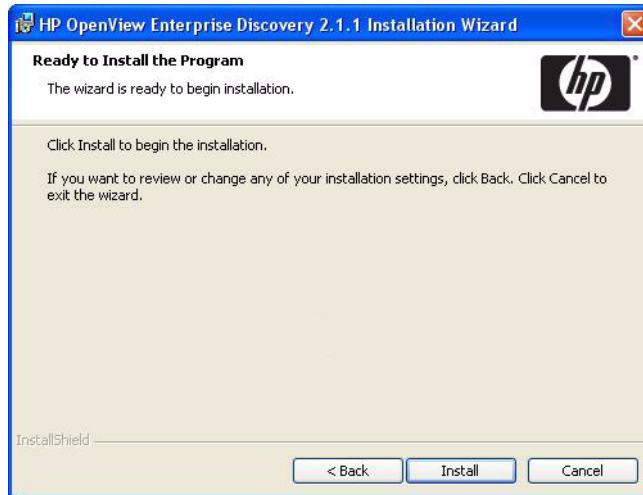
12 Click **Install** to begin the installation.

A progress indicator appears:

This process can take up to 10 minutes.

After the installation is complete, the following screen appears.
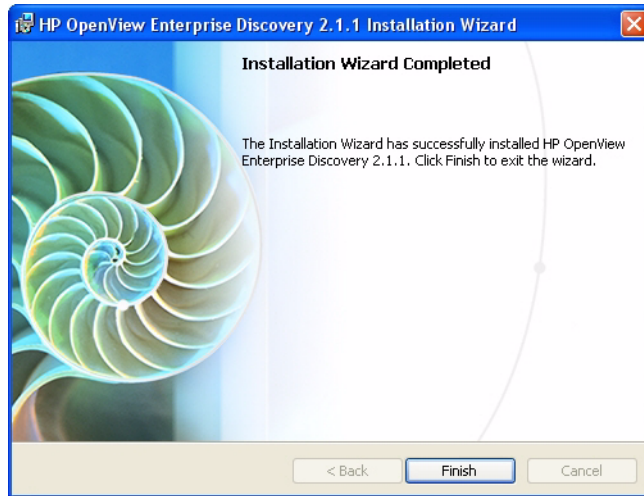
13   Click **Finish**.

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.
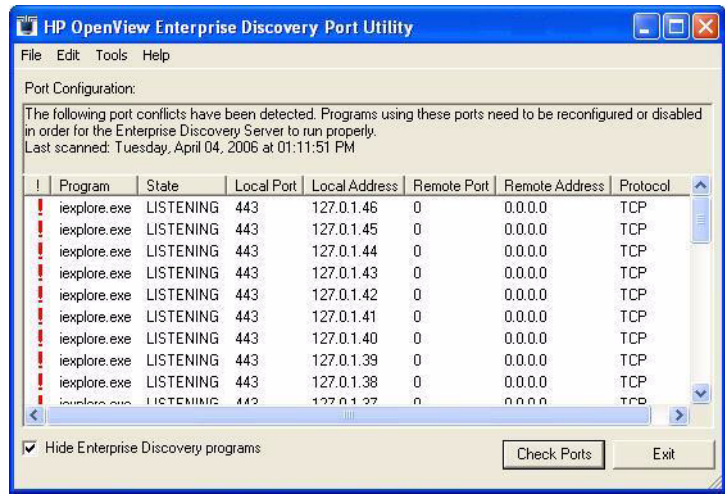
You will need to make these ports available in order to use Enterprise Discovery.

For a complete list of ports used by Enterprise Discovery, see the *Planning Guide*.

Restarting your Server

After the installation is complete, this window appears, asking you to restart your server.
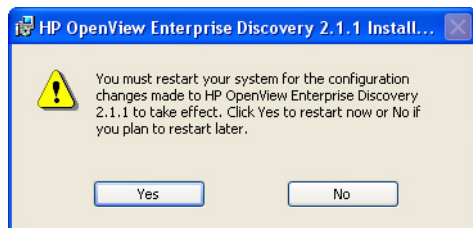
- Click **Yes** to restart now, or **No** if you want to wait and restart later.

Installation is not complete until the server has been restarted.

You should also restart your server after an upgrade, or if you change the DNS server, or the time zone.

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.

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
```

⚠️ 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 Windows 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

⚠️ The Apache Web Server takes several minutes to start.

⚠️ DO NOT MANUALLY START OR STOP ANY OF THESE SERVICES. When you restart the server, the services will start on their own, in the correct order. Do not alter the services in any way, unless instructed to do so by customer support.

Table 3   Services

Service	Description
HP OpenView Discovery Agent Communicator	Provides communication services with HP Agents to HP's Discovery products.
HP OpenView Discovery Apache SSL Web Server	Secure Apache Web Server installed with HP's Discovery products.
HP OpenView Discovery Apache Web Server	Apache Web Server installed with HP's Discovery products.
HP OpenView Discovery Authenticator	Provides authentication services for HP's Discovery products.
HP OpenView Discovery Engine	Provides network discovery services to HP's Discovery products.
HP OpenView Discovery Event Manager	Provides event processing services to HP OpenView's Discovery products.
HP OpenView Discovery Scheduler	Provides scheduling services for HP's Discovery products.
HP OpenView Discovery Tools Database	Provides database services for HP's Discovery products.
HP OpenView Discovery Logger	Provides logging services to HP's Discovery products.
HP OpenView Discovery System Monitor	Ensures all HP system processes are running properly.
HP OpenView Discovery Tomcat Servlet Container	Tomcat Servlet Container bundled with HP's Discovery products.
HP OpenView Discovery Topology Converter	Provides connectivity data processing services to HP OpenView's Discovery products.

Table 3   Services

Service	Description
HP OpenView Discovery Topology Engine	Identifies the network topology, applies the break fault detection logic and calculates some statistics.
HP OpenView Discovery Watchdog	This service ensures the System Monitor process is running.
HP OpenView Discovery XML Enricher (Main)	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.
	If you configure your Enterprise Discovery server to run two XML Enricher instances, the following service is also started: HP OpenView Discovery XML Enricher (1). For additional information, see "Running Multiple XML Enrichers" in the *HP OpenView Enterprise Discovery Configuration & Customization Guide*.

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

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

- Client Specifications on page 51
- Installing the License on the Client on page 52
- Installing Enterprise Discovery on page 53

You can install the client portion on several workstations.

The server install contains everything available in Enterprise Discovery 2.1. The client install is a subset of the server install.

Client Specifications

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

Table 1   Client Specifications

Item	Required	Recommended
RAM	500 MB	1-3 GB if you will be analyzing a large number of scan files.
CPU	Pentium III, 500 MHz	
Disk	100MB	2GB
Operating system	Windows 2000, XP, or 2003	Windows 2000, XP, or 2003

Table 1   Client Specifications

Item	Required	Recommended
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

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

🚩   Ensure that you have a Java plug-in installed with your browser.

Installing the License on the Client

HP 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 38).

🚩   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.

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 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.

The following screen appears.

2　Click Install Enterprise Discovery to start the install process.

Next, the Preparing to Install window appears.
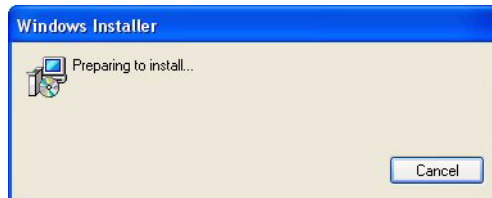
Next, the Installation Wizard appears.
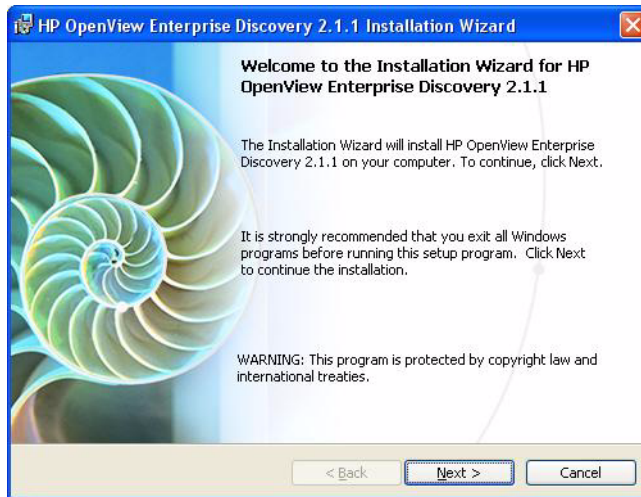
3   Click **Next**.

The Destination Folder screen appears.

The default installation directory is:

C:\Program Files\HP OpenView\Enterprise Discovery\2.1.1

> Enterprise Discovery must be installed on a local disk.

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

> All components will be installed to this default location.

5   Click **Next**.

The Setup Type screen appears.

6   Select the "Client" Setup Type.

7   Click **Next**.

The Ready to Install the Program screen appears.
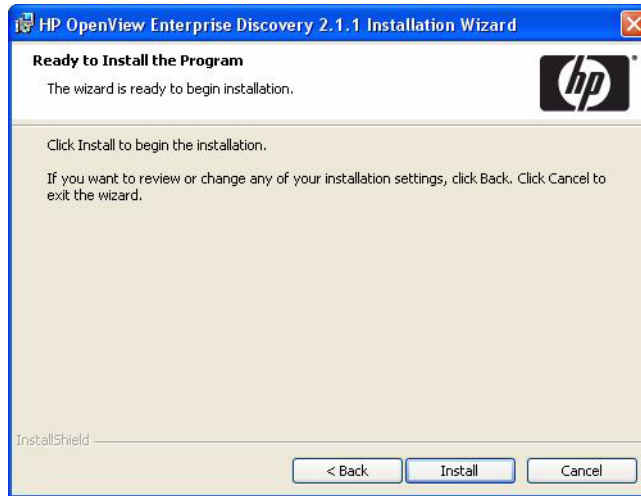
8   Click **Install** to begin the installation.

A progress indicator appears:

After the installation is complete, the following screen appears.
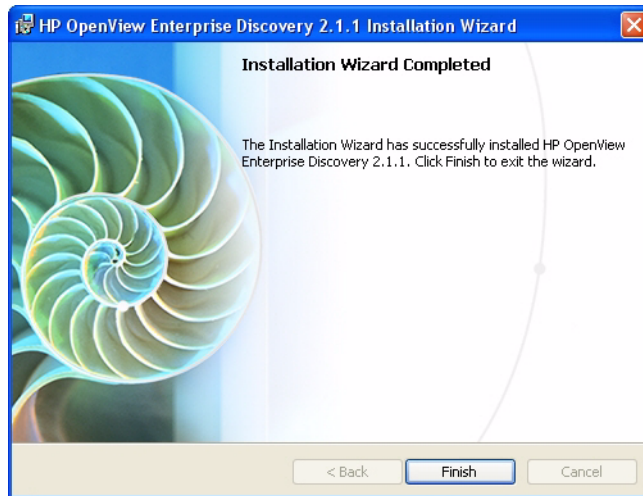
9   Click **Finish**.

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

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

- Accessing the Web Interface Components on page 60

- Accessing the Windows Components on page 66

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 (available through the Windows Start menu):
    — Documentation
    — Help
    — Analysis Workbench
    — SAI Editor
    — SAI Update Wizard
    — Scanner Generator
    — Viewer
- Web Interface Components (available through your web browser)
    — Health Panel

- — Alarms Viewer
- — Network Map
- — Service Analyzer
- — Events Browser
- — MIB Browser
- — Scan Data Viewer
- — Find
- — Asset Questionnaire
- — Reports
- — Administration
- — Status
- — Help

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.

Table 1   Default 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.

▶ You can bookmark this URL for use with your browser.

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

▶ 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**.

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

▶ This should be the only time you use the default password for the "admin" account. Refer to Change the default Admin password on page 162.

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 HP 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 "HP OpenView Apache Web Server" service is running in the list of Services (Start > Control Panel > Administrative Tools > Services).

I can connect to the Enterprise Discovery server, but I cannot open a component I would expect to see with my license, such as the Health Panel. The two most common reasons for this problem are:

- Your management workstation and the Enterprise Discovery server are on opposite sides of your corporate firewall. You should see a dialog box that explains that Enterprise Discovery is trying to connect and shows an error message.

  To resolve the problem, do one of the following:

  — Ensure that your management workstation and the Enterprise Discovery server are on the same side of the firewall.

  — Configure the firewall to allow connections from the subnet with your management workstation to the subnet with the Enterprise Discovery server for the ports: 80, 443, 8100, 8101 to 8105, and 8108.

- Your web browser may be configured to use a proxy server.

  To resolve the problem:

  — If you have a manual proxy connection, you may be able to add your own exception or bypass.

  — If you have an automatic proxy connection, it may be necessary to consult the administrator for your network.

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.

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.
Network Availability Graphs	These graphs display the average network availability for the last 7, 30, and 90 days.

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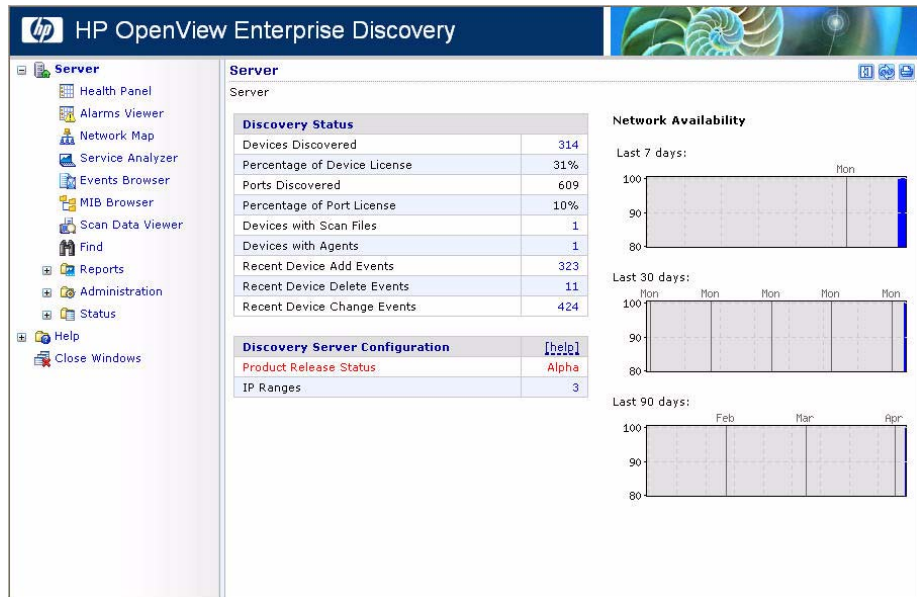
Accessing the Windows Components

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 > HP OpenView > Enterprise Discovery 2.1**.

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

   • Documentation

   • Help

   • Analysis Workbench

   • SAI Editor

- SAI Update Wizard

- Scanner Generator

- Viewer

What Next?

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

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.

To configure your server, log in to the Web Interface as described in Getting Started on page 59, and then complete the following procedures:

- Enter the SMTP server on page 70

- Enter a server name on page 71

- Enter the Administrator e-mail address on page 71

- Enter the server host name on page 72

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

There are other options available on this page, but they are not necessary for configuring the server. Read the related help files to determine if you would like to change any of the default settings.

SMTP server:	⦿ Default:	
	○ Custom:	[ ]
Server name:	⦿ Default:	Server
	○ Custom:	[Server]
Server administrator e-mail address:	⦿ Default:	email.address.not.configured@Enterprise.Discovery
	○ Custom:	[email.address.not.configured@Enterprise.Discovery]
Server hostname:	⦿ Default:	localhost.localdomain
	○ Custom:	[localhost.localdomain]
Backup scan files:	⦿ Default:	Yes
	○ Custom:	⦿ Yes ○ No
Backup Aggregate/Imported directory:	⦿ Default:	No
	○ Custom:	○ Yes ⦿ No
Log user actions:	⦿ Default:	No
	○ Custom:	○ Yes ⦿ No
User configurable login warning message:	⦿ Default:	
	○ Custom:	[ ]
Display last login time:	⦿ Default:	No
	○ Custom:	○ Yes ⦿ No
Disable unused accounts:	⦿ Default:	90 days
	○ Custom:	○ Never ○ 30 days ○ 60 days ⦿ 90 days ○ 120 days ○ 365 days
Number of XML Enrichers to run:	⦿ Default:	1
	○ Custom:	[1]
Maximum concurrent map sessions:	⦿ Default:	5
	○ Custom:	[5]

[Change]

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.

HP recommends that you use a local SMTP server. If your mail server is off-site, you may not be able to rely on it to send you a message that a network device is down.

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).

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.

▶ 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
Create Network Property Groups	Chapter 8, Setting up Network Property Groups
Create SNMP Property Groups	Chapter 9, Setting up SNMP Property Groups
Create Agent Property Groups	Chapter 10, Setting Up Agent Property Groups and Agent Deployment Accounts
Create Scanner Property Groups	Chapter 11, Setting Up Scanner Property Groups and Scheduling Scanners
Apply your Property Groups to an IP range	Chapter 12, Configuring your Network IP Ranges
Optional: Create custom scanners	Chapter 11, Scanner Generator in the *Configuration and Customization Guide*
Optional: Enable multiple XML Enricher services	Chapter 12, XML Enricher in the *Configuration and Customization Guide*

7 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:

- Property Groups on page 75

- Property Sets on page 76

Once you create Property Groups and Sets, you can then apply them to IP Ranges (see Configuring your Network IP Ranges on page 113).

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

- SNMP—for SNMP access through community strings (v1/v2) or users (v3)
- 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.
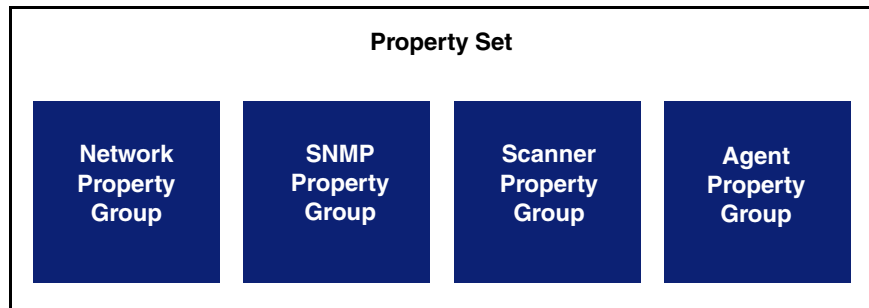
For example: If you find you are setting up several ranges and applying the Network Property Group, "Active discovery", and then setting up the same ranges with an SNMP Property Group you have defined, you might find it easier to create a Property Set. Property Set "X" can contain the Network Property Group, "Active discovery" and your SNMP 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.

Agent Property Groups and Scanner Property Groups are only available if the Inventory license is present.

What Next?

To	Go to
Create Network Property Groups	Chapter 8, Setting up Network Property Groups
Create SNMP Property Groups	Chapter 9, Setting up SNMP Property Groups
Create Agent Property Groups	Chapter 10, Setting Up Agent Property Groups and Agent Deployment Accounts
Create Scanner Property Groups	Chapter 11, Setting Up Scanner Property Groups and Scheduling Scanners
Apply your Property Groups to an IP range	Chapter 12, Configuring your Network IP Ranges
Activate your configuration changes	Chapter 13, Activating Your Configuration Changes

8 Setting up Network Property Groups

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

- The Properties on page 80
- How to use Network Property Groups on page 82
- Making changes to Network Property Groups on page 85

Introduction

Network Property Groups are groups of settings that can be applied to IP ranges (see Configuring your Network IP Ranges on page 113). 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:

1   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:

Table 1   Network Properties

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

Table 1   Network Properties

Property	Purpose	Hardcoded Default Setting
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
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.

Table 2   More Discovery

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.

Table 2   More Discovery

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.

Table 3   Less Discovery

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.

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

If a default 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.

▶ 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.**

   ▶ You cannot erase default Property Groups.

What Next?

To	Go to
To create SNMP Property Groups	Chapter 9, Setting up SNMP Property Groups
To create Agent Property Groups	Chapter 10, Setting Up Agent Property Groups and Agent Deployment Accounts

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

9 Setting up SNMP Property Groups

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

Introduction

Enterprise Discovery supports SNMPv1, SNMPv2, and SNMPv3. Depending on your network, you may have devices using any of these versions. You can set up many SNMP Property Groups including both community strings (for SNMPv1 and SNMPv2) and users (for SNMPv3).

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 community strings or users for your network workstations, and a different set of community strings or users for servers.

Once you configure your SNMP Property Groups, you can then apply them to IP ranges (see Configuring your Network IP Ranges on page 113).

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

By default, the global SNMP Property Group has one read community string (public), and no SNMPv3 users. If you do not add any data to your SNMP Property Groups, but keep *public* 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*.

If you do not add any community strings or users, and delete *public* from the global SNMP 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.

Do not delete *public* from the global SNMP Property Group unless you are absolutely sure you do not need it.

Adding community strings and users—the quick way

The one default SNMP Property Group is "global." If you are not sure what strings (SNMPv1/v2) and users (SNMPv3) apply to your devices or subnets, you can add all of your community strings and users to this global list.

If your network uses SNMPv1/v2 exclusively, and 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 and users to the "global" SNMP Property Group.

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

To add community strings/users to the global SNMP Property Group:

1   Click **Administration** > **Network configuration** > **SNMP Property Groups**.

2   Click **Modify an SNMP Property Group**.

3   Select **SNMP: 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   Under the heading **Add a User** enter a user name, and select the
    appropriate **Type** (**read** or **write**, or both).

9   For each user, add any necessary algorithms and pass phrases.

10 Click **Add**.

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

12 Click **Submit**.

▶   To assign different community strings to different IPv4 ranges, refer to
    Setting up Property Groups and Property Sets on page 75.

Creating new SNMP Property Groups

If you are more concerned with security, and you have community strings for
particular devices or subnets, you can create an SNMP Property Group with a
"list" of strings. You then apply the SNMP 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 an SNMP Property Group:

1   Click **Administration > Network configuration > SNMP Property Group > Add an
    SNMP Property Group.**

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

3   Add a description.

4   Add community strings for SNMPv1/v2 devices:

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

    b   Click **Add**.

    c   Repeat steps a and b for each community string that can be applied to
        the same set of devices or subnets.

d   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.

5   Add users for SNMPv3 devices:

a   Under the heading **Add SNMPv3 Users** enter a user name. The user name cannot be an empty string.

b   Optionally, you can select an Authentication Algorithm. **None** indicates that you do not want to use an Authentication Algorithm. **SHA** or **MD5** indicates the specific Authentication Algorithm you want to use.

c   If you have selected a specific Authentication Algorithm, you must enter an Authentication pass phrase. This pass phrase must be at least 8 characters long.

d   If you have selected an Authentication Algorithm, you can optionally select an Encryption Algorithm. **None** indicates that you do not want to use an Encryption Algorithm. **DES** or **AES** indicates the specific Encryption Algorithm you want to use. You can have authentication with or without encryption, but in order to specify encryption, you must have authentication.

e   If you selected a specific Encryption Algorithm, you must enter an Encryption pass phrase. This pass phrase must be at least 8 characters long.

f   Select the appropriate **Type** (**read** or **write**, or both).

g   Click **Add**.

h   Repeat these steps for each user that can be applied to the same set of devices or subnets.

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

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

6   Click **Submit**.

To apply the SNMP 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 SNMP Property Group.

4   Click **Submit**.

Deleting a community string or user

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

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

To delete a single community string or user:

1   Click **Administration** > **Network Configuration > SNMP Property Groups** > **Modify an SNMP Property Group**.

2   Select an SNMP Property Group from the pull-down list.

3   Click **Select**.

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

5   Under the "Change Order/Delete a User" heading, select the community string you want to delete and click **Delete**.

6   Click **Submit**.

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

To delete an SNMP Property Group:

1   Click **Administration > Network configuration > SNMP Property Groups > Delete an SNMP Property Group**.

2   Select an SNMP Property Group from the pull-down list and click **Select**.

3   Click **Delete**.

You have deleted an SNMP 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 8, Setting up Network Property Groups
To create Agent Property Groups	Chapter 10, Setting Up Agent Property Groups and Agent Deployment Accounts
To create Scanner Property Groups	Chapter 11, 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 12, Configuring your Network IP Ranges

10 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:

- What is an Agent? on page 96

- Setting the Agent Port on page 96

- Configure Agent Deployment Accounts to give Enterprise Discovery access to the workstations on page 97

- Distributing Agents with Agent Property Groups on page 99

If you need to deploy agents manually, find more information in the *Configuration and Customization Guide*.

▶ Agent Property Groups are only available if the Inventory license is present.

Introduction

Agent Property Groups are groups of settings that can be applied to IP ranges (see Configuring your Network IP Ranges on page 113). 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 (onto Windows workstations).

▶ 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.

▶ 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 Enterprise Discovery property groups. See Upgrading your Custom Application Library on page 177 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.

Setting the Agent Port

There are two ports your Enterprise Discovery server can use to communicate with the Agent on a network device:

- 2738 (default)
- 7738 (IANA registered)

The default setting should be sufficient for most users, unless you use port 2738 for another service.

Port 7738 is exclusively used by HP, and is registered with IANA. If you need to use a standard port for Agent communication, complete the following procedure.

⚠️ **WARNING**:

This procedure is intended for when you are first installing Enterprise Discovery in your network. If you are upgrading, or you decide to change this port number after Enterprise Discovery has been running, you must first uninstall the Agents from your network devices. For full details, read the online help file available at **Administration > System Configuration > Agent Communication > Agent Port**.

Changing the Default Agent Port:

1   Click **Administration > System Configuration > Agent Communication.**

2   Next to Agent Port, select 7738.

3   Click **Change**.

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.

The default ADMIN$ is configurable. Change the **Share** name in the following procedure.

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

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 domain.

3   Enter the Login.

4   Enter the password (twice).

5   Enter the Share (if you want to change it from the default ADMIN$)

6   Enter the Path (if you want to change it from the default %SystemRoot%)

7   Enter a description.

8   Click **Submit**.

Domain:

Login:

Password:

Password:

Share: ADMIN$

Path: %SystemRoot%

Description:

Submit

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 113).

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:

9   Click **Administration > Network Configuration > Agent Property Groups > Add an Agent Property Group**.

10   Give the property group a name. For example, '**Windows Workstations**'.

11   Add a description.

12 Enter the following information for your Agent Property Group:

Table 1   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**.
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.

13 Click **Submit**. A summary appears.

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

What Next?

To	Go to
Create Network Property Groups	Chapter 8, Setting up Network Property Groups
Create SNMP Property Groups	Chapter 9, Setting up SNMP Property Groups
Create Scanner Property Groups	Chapter 11, Setting Up Scanner Property Groups and Scheduling Scanners
Activate your configuration changes	Chapter 13, Activating Your Configuration Changes
Apply your Property Groups to an IP range	Chapter 12, Configuring your Network IP Ranges
Manually deploy agents (UNIX, Mac OS X, and Windows)	*Configuration and Customization Guide*

11 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:

- Scheduling Scanners on page 103
- Defining Scanner Property Groups on page 104

> Scanner Property Groups are only available if the Inventory license is present.

Introduction

Scanner Property Groups are groups of settings that can be applied to IP ranges (see Configuring your Network IP Ranges on page 113).

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 processes 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 113).

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
- Mac OSX
- 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:

Name: [   ]
Description: [   ]

Select for all scanners: [<inherit>   ▼]
or select individually:
    Win32 scanner: [<inherit>   ▼]
    HP-UX scanner: [<inherit>   ▼]
    Linux scanner: [<inherit>   ▼]
    AIX scanner: [<inherit>   ▼]
    Solaris scanner: [<inherit>   ▼]
    Mac OSX scanner: [<inherit>   ▼]

Bandwidth Threshold: ○ Set ⊙ Inherit
    [0   ] [Mb/s ▼]
Frequency: ○ Set ⊙ Inherit
    Weeks: [0   ] Days: [0   ] Hours: [0   ]
Scanner upgrade: ⊙ On ○ Off ○ Inherit
Scanner upgrade schedule: [<inherit>   ▼] [...]
Scanner run schedule: [<inherit>   ▼] [...]
Scan file download schedule: [<inherit>   ▼] [...]

[Submit]

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 106

- Setting the bandwidth threshold on page 108

- Setting the frequencies of scans on page 109

- Setting scan schedule properties on page 109

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, Mac, 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
Mac OSX Scanner	Hardware only

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

Table 1   Default Scanner Configuration Files

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.

Table 1   Default Scanner Configuration Files

Scanner	Description
<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.

➤   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

▶ 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.

▶ If you **set** the frequency to **0** (zero), this will produce a one-time scan.

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:

- **<all the time>** - 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.
- **Working hours** - The scan schedule property will only be in effect during working hours (i.e. between 9 am and 5 pm).
- **Not during working hours** - The scan schedule property will only be in effect outside working hours.

- **Weekends** - The scan schedule property will only be in effect on weekends.

- **All the time** - The scan schedule property will be in effect all the time.

▶ The first two options are system defaults (<**all the time**> and <**inherit**>). The others can be edited or deleted in **Administration > Schedule Management**.

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 103, 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 103, 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 103, it appears in this pull-down list.

What Next?

To	Go to
To create Network Property Groups	Chapter 8, Setting up Network Property Groups
To create SNMP Property Groups	Chapter 9, Setting up SNMP Property Groups
To create Agent Property Groups	Chapter 10, 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 12, Configuring your Network IP Ranges
Configure more Scanner settings	the *Configuration and Customization Guide*
Learn more about Scanners	the *Reference Guide*

12 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 configure up to 2000 IP ranges.

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 75.

There are several ways to start configuring your IP ranges.

Table 1   Configuring 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 115.
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 116. You can also Setting up the IPv4 range(s) to avoid on page 118, or Adding ranges for DHCP servers and unmanaged routers on page 118.
That some of your adjacent IP ranges are configured the same way	Merging IP Ranges on page 119
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 120. You can also Exporting your IPv4 ranges to a CSV file on page 121.

Running router discovery

You can use Router Discovery 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. Also, you must have the correct SNMP access information (community strings or users). If not, router discovery will not be successful.

If you would rather enter your IPv4 ranges manually, go to Setting up the IPv4 range(s) to discover on page 116.

Set up Router Discovery:

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

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

3   Click **Change**.

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

4   Click **Administration > Router discovery > SNMP settings.**

5   Add your SNMPv1/v2 community strings, and/or your SNMPv3 user information.

   a   For SNMPv1/v2, enter a community string and click **Add**. Repeat this for each community string.

   b   For SNMPv3, enter the user name, authentication algorithm and pass phrase, and the encryption algorithm and pass phrase, and click **Add**. Repeat this for each user.

   c   Click **Change**.

Run Router Discovery:

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

2   Click **Confirm**.

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

➤   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:

1   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.

➤   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.

▶ 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 79, Setting up SNMP 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 103).

   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

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

➤   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.

State whether this is a range or a subnet

Starting IP address

Ending IP address or netmask

Define whether this is a Property Group or Property Set (Set, Network, SNMP, Scanner, Agent)

The name of the Property Group or Property Set you've specified in the previous column. The name must be exactly as it appears in the Network Configuration page.

	A	B	C	D	E	F
1	range	172.22.2.5	172.22.2.56	Network	global	
2	subnet	172.22.9.5	255.255.255.0	Set	global	
3						
4						
5						
6						
7						
8						

testimport

▶ 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.

▶   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.

▶   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.

▶   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 125.

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
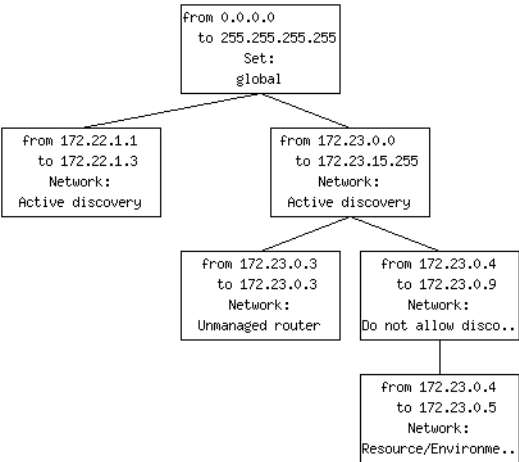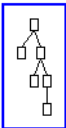
What Next?

To	Go to
Learn about Property Groups and Sets	Chapter 7, Setting up Property Groups and Property Sets
To create Network Property Groups	Chapter 8, Setting up Network Property Groups
To create SNMP Property Groups	Chapter 9, Setting up SNMP Property Groups
To create Agent Property Groups	Chapter 10, Setting Up Agent Property Groups and Agent Deployment Accounts
To create Scanner Property Groups	Chapter 11, Setting Up Scanner Property Groups and Scheduling Scanners
To Activate your configuration changes	Chapter 13, Activating Your Configuration Changes

13 Activating Your Configuration Changes

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

- Reviewing Your Changes on page 125

- Discarding the Changes on page 126

- Activating the Changes on page 126

- Checking that Enterprise Discovery is working as expected on page 127

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**.

If you are 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.

HP 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.

Low to medium.

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

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.

Depending on your license, as many as 10 accounts can use a Network Map session at the same time.

To check how many people are using a map:

- Click **Status** > **Network Map Sessions**. You will see how many of the map sessions are currently available.

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.

- Aggregator—exclusively used to configure the Enterprise Discovery Aggregator.

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

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.

Administrative Password Options

There are several restrictions on account passwords that allow for greater security of your Enterprise Discovery server. Some are included by default, but some can be changed by an Administrator at **Administration > System Configuration > Server passwords**.

Password Restrictions

There are some default restrictions for all account passwords:

- No more than 2 consecutive identical characters
- A user password cannot be the same as the user name, a portion of the user name, or the inverse of the user name.

There are also several restrictions an Administrator can control:

- Minimum password length
- Minimum number of lower case letters
- Minimum number of upper case letters
- Minimum number of digits
- Minimum number of symbols
- Minimum number of digits or symbols

Other Account Preferences

There are some default restrictions for all accounts:

- If an account is inactive for 90 days, it will be disabled.
- When changing your account password, you must enter your old password as well as your new password.
- On the Home Page, you will always see the times of your most recent successful login, and your most recent failed login attempt.

There are also several restrictions an Administrator can control:

- Maximum number of failed login attempts

- Keeping track of an account's old passwords (Password history)
- Force user to change password at first login

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.

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.

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

▶ A user password cannot be the same as the user name, a portion of the user name, or the inverse of the user name.

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.

Password:

Password (again):

Modify Password

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 properties**.

2 Select the account from the list box.

3 Click **Modify properties**.

4   Select the account type from the list box.

> 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 properties, as appropriate.

6   Click **Modify Properties**.

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:

- Installing the Aggregator Hardware on page 138
- Installing the Aggregator license on page 138
- Installing the Remote Enterprise Discovery Servers on page 139
- Sharing Security Keys between all your Servers on page 139
- Configuring the Aggregator on page 141
- Setting up the Remote Servers on page 143
- Navigating through multiple servers on page 144
- Deleting Remote servers on page 145

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 version 2.1 (Enterprise Discovery 2.0 does not support SSL, which is necessary for the servers to communicate).

Installing the Aggregator Hardware

The Aggregator is the backbone of your Enterprise Discovery system, collecting device data from up to 50 remote servers, and up to a total of 500,000 devices.

▶ An individual Enterprise Discovery server can collect data from up to 50,000 devices. An Aggregator can collect data from a maximum of 500,000 devices. This means that you cannot maximize 50 remote servers and have all their data recorded on the Aggregator. The Aggregator will collect data from the first 500,000 devices in the database. If you have more than 500,000 device being monitored by your remote servers, you will not be able to see all that data in the Aggregator.

Install your Aggregator as you would any Enterprise Discovery server, as described in Server Installation on page 33.

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.

⛔ Do not configure your IP ranges, Agents, or Scanners until you have completed Sharing Security Keys between all your Servers on page 139.

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 HP Customer Support.

For details on installing the license, see Installing the License on the Server on page 38.

⚑ The Aggregator server will require more hardware resources (larger disk, more RAM) than a regular Enterprise Discovery server. See Server Installation on page 33 for details.

Installing the Remote Enterprise Discovery Servers

Follow the instructions in Server Installation on page 33 to install each remote server.

⛔ Do not configure your IP ranges, Agents, or Scanners until you have completed Sharing Security Keys between all your Servers on page 139.

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.

⛔ 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.
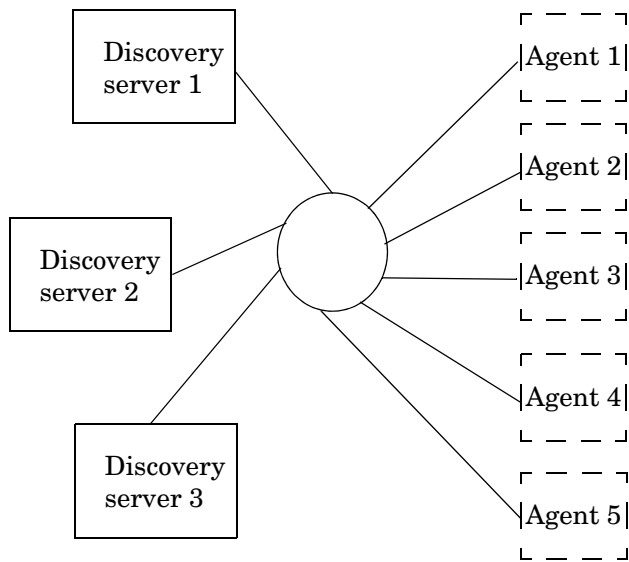
This can be accomplished in a few simple steps:

• 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).

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.

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

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 Aggregator account

•   the Aggregate health update interval

- the Aggregate events update interval

➤ You can install your Aggregator and remote servers, and test that the communication works between them by adding small IP ranges on each remote server. Once you are satisfied with your setup, you can fully configure each remote server. Ideally, you should configure one remote server at a time, and allow it begin discovering its portion of the network before configuring another remote server. If you add the remote servers too quickly, you will overload the Aggregator with data. If you notice performance problems, you may have overloaded the Aggregator. See Troubleshooting the Aggregator on page 146 for suggestions.

➤ You must also do network configuration for your Aggregator. For example, add IP ranges for your remote server and router, and then be sure to **Activate** the changes. See Configuring your Network IP Ranges on page 113 for details.

On each individual Enterprise Discovery server that you will be aggregating, set up an Aggregator account that will allow the Aggregator to access the remote server's database.

⛔ The Aggregator will communicate with the remote server(s) on port 443. Make sure you enable this port in your firewall.

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 Aggregator account and password that will be used to collect data for the Aggregate Health Panel.

➤ This account must be an Aggregator account. Normal user accounts cannot be used to access the server's database. On your remote server, click **Administration > Account administration** to configure it properly. (For more information, see Setting up the Remote Servers on page 143.)

6 Select data transfer intervals:

- Aggregate network inventory

- Aggregate events
- Aggregate workstation inventory

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 On the remote servers, click **Administration > Account administration > Add an account**.

2 Follow the instructions to create an Aggregator account that matches the account name you configured on the Aggregator (Configuring the Aggregator on page 141).

   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 Configuration > 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.

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**.

Troubleshooting the Aggregator

As mentioned in Configuring the Aggregator on page 141, you should fully configure one remote server at a time when setting up your Aggregator. This will avoid overloading the Aggregator with too much data at once.

If you have remote servers monitoring small portions of your network, it will take less time for those to aggregate. If you have remote servers monitoring large networks (thousands of devices), it would be best to add one remote server per day.

If you have overloaded the Aggregator, you can resolve the situation by:

- adding more CPU and RAM to your Aggregator server

- deleting some remote servers (starting with the ones added most recently) until the server stabilizes

What Next?

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

16 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:

- Setting up your backups on page 149
- Backing up Aggregator files on page 149
- Backing up your data immediately on page 151
- Restoring your data on page 151

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:

Table 1   **Backup 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.

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 47.

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**.

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.

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.

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 Configuration > Server configuration**.

2   Set the **Backup Scan Files** option to "No."

3   Click **Change**.

Backing up Aggregator files

You also have control over whether Enterprise Discovery backs up the contents of the following directory:

<DataDir>/Aggregate/Imported

This directory contains files that are used to synchronize an individual remote server with an Aggregator server. To save disk space and reduce the time required to perform the daily backup, the files in this directory are not saved by default. You can choose to save the contents of this directory if you prefer.

If either of the following two conditions is true, you do not need to backup the Aggregator synchronization files:

- This Enterprise Discovery server is not aggregated.

- It is acceptable to lose a small amount of historical data on the Aggregator in the event that the local server needs to be restored from the content of the archive file.

  For the following reasons, the consequences of losing this historical data are not severe:

  — Under normal circumstances, an Aggregator keeps itself synchronized with remote servers on a timely basis. Even if some data is lost following a restore, it is likely to be minimal.

  — Some data will be lost anyway, because the period between the time of the archive and the current time will not be in the archive.

  — This missing period may not be completely lost, because the Aggregator has likely had time to synchronize itself during that time. In this case, the recovered data (files) would not be used anyway, because they would already have been processed.

  — By its very nature, this data is refreshed periodically. There may be a temporary gap, but eventually the data will resynchronize itself with what is discovered on the network. Again, the only long term exposure resides in the loss of historical data that cannot be rediscovered.

To instruct Enterprise Discovery to backup your Aggregator synchronization files:

1 Click **Administration > System Configuration > Server configuration**.

2 Set the **Backup Aggregate/Imported directory** option to **Yes**.

3 Click **Change**.

There is also another way to minimize space and time requirements for the daily backup while still preserving some recovery capabilities for files that are aggregated. By default, these files are kept for 15 days. This is done so that if the network link to the Aggregator, or the Aggregator itself, is down for an extensive period of time (up to 15 days by default), the Aggregator can still re-synch itself without loss of any data.

Depending on your network and Aggregator reliability track record, you may choose to reduce the time that the Aggregator files are kept. By doing this, you will considerably reduce the time and space requirements to save the aggregator synchronization files.

1   Click **Administration > System Configuration > Aggregate configuration**.

2   For the **Number of days to keep imported Discovery Database files** option, click **Custom**.

3   In the **days** box, type the number of days that you want to keep these files on this server.

4   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

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

Windows security permissions are not retained after a restore. Once you perform a restore, you will have to reapply the HP Security Template. See Enterprise Discovery Security Template on page 159.

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 (within your data directory), and copy your latest backup files into that location, Enterprise Discovery will automatically do a restore when you next restart your 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 Uninstalling Enterprise Discovery

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

➤ 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 HP Enterprise Discovery entry.

2   Click **Add/Remove**. Follow the on screen instructions.

3   Restart your server.

🛑 You need to restart your server before installing a new version of Enterprise Discovery.

18 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.

Using HTTPS and SSL

To increase security on your Enterprise Discovery server, all web UI pages are served via a secure HTTPS/SSL connection. When you install Enterprise Discovery, it generates default SSL keys and a certificate which are used to ensure secure communication with the server.

► The Scanners and Scanner Generator use HTTP, not HTTPS.

The server installation wizard prompts you for the full qualified domain name of the server (for example, edserver.yourcompany.com) that will be included in the default security certificate. Once installed, the following URL will access your server: https://edserver.yourcompany.com.

► All HTTPS communication between the server and client (and for multiple aggregated servers) take place over port 443.

The disadvantage of the default SSL certificate is that it is not issued by a recognized certificate authority, which browsers trust by default. Therefore, when you access the web UI, a security alert message will appear stating that the certificate is valid, but not trusted.

To avoid these security alert messages every time you access the web UI, you must do one of two things:

- Install the default server certificate onto each Enterprise Discovery client workstation.

- Purchase a commercial certificate from a recognized certificate authority (such as Versign), and install it on the Enterprise Discovery server, replacing the default certificate.

Putting the Certificate on your Enterprise Discovery client

If you use the default certificate, or a new signed certificate, you must copy it to the Enterprise Discovery client workstations as well.

There are two ways to make sure your client has the security certificate:

- Copy the files from the server to the client (most secure)

- Install the certificate through the web browser

Copy the files from the server to the client

These instructions are for Windows XP. Other versions of Windows may have different instructions.

1 Copy the server.crt file onto a secure media (such as a floppy disk of USB drive). Do not send this file via email.

2 Copy the server.crt file onto the client machine.

3 Right-click the file, and select **Local > Install Certificate**.

   The certificate import dialog appears.

4 Click **Next**.

5 Select "Automatically select the certificate store based on the type of certificate".

6 Click **Next**.

7 Click **Finish**.

8 Then, with Microsoft Internet Explorer, navigate to your Enterprise Discovery server using the host name that you used when generating the certificate. Do not use the plain IP address.

   Internet Explorer should access the server without any warnings about SSL security certificates.

Install the certificate through the web browser

The first time you access the Enterprise Discovery web UI through your browser, you will see a security alert. Follow these steps to give the client secure access to the server.

1 In the Security Alert dialog, click **View Certificate**.

2 Review the certificate, click the **General** tab, and then click **Install Certificate**.

3 Click **Next**.

4 Select "Automatically select the certificate store based on the type of certificate".

5 Click **Next**.

6 Click **Finish**.

Creating your own SSL Certificate

To create your own SSL certificate for the Enterprise Discovery server, you must:

1   Create the following directory:

    C:/install/apache/bin/

2   Place the "openssl" file in this new directory.

    This "openssl" file is found in C:\Program Files\HP OpenView\Enterprise Discovery\2.1.x\apache\bin

    > If there are two "openssl" files in the above directory, choose the one with Type SpeedDial and Size 10K.

3   Follow the instructions available at this site:

    http://httpd.apache.org/docs/2.0/ssl/ssl_faq.html#realcert

Once you have the server.crt and server.key files, you can place them in the following locations (these are defaults, and may have changed if you have moved your Data directory):

Table 1   Default Locations

File	Location
server.crt	C:\Documents and Settings\All Users\Application Data\Peregrine\Enterprise Discovery\Cert\ssl.crt
server.key	C:\Documents and Settings\All Users\Application Data\Peregrine\Enterprise Discovery\Cert\ssl.key

Finally, restart the Apache SSL service (**Start > Control Panel > Administrative Tools > Services**).

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. You can modify this template, if necessary, to suit the needs of your company.

Click **Start > All Programs > HP > Enterprise Discovery 2.1 > Install Security Template**. Once you make that selection, the following security settings will be automatically applied to your system.

Folder security for user accounts:

Table 2   Folder Security

Folder	Security Measure
C:\Perl	Read-only access
..\HP	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:

Table 3   Registry Security

Registry	Security Measure
HKLM\ SYSTEM \CurrentControlSet\Services\hpovXmlEnricher	Read-only access
HKLM \SYSTEM\CurrentControlSet\Services\hpovWatchdog	Read-only access
HKLM \SYSTEM\CurrentControlSet\Services\hpovTomcat	Read-only access
HKLM \SYSTEM\CurrentControlSet\Services\hpovSysmon	Read-only access
HKLM \SYSTEM\CurrentControlSet\Services\hpovSched	Read-only access
HKLM \SYSTEM\CurrentControlSet\Services\hpovLogger	Read-only access
HKLM \SYSTEM\CurrentControlSet\Services\hpovDiscEng	Read-only access
HKLM \SYSTEM\CurrentControlSet\Services\hpovDiscDB	Read-only access
HKLM \SYSTEM\CurrentControlSet\Services\hpovAuth	Read-only access
HKLM \SYSTEM\CurrentControlSet\Services\hpovApache	Read-only access
HKLM \SYSTEM\CurrentControlSet\Services\hpovAgentCom m	Read-only access
HKLM \SOFTWARE\HP	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 read 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 read community string ("public") will be able to access the SNMP MIB of your Enterprise Discovery server.

Eliminate Default User Account Names

The account names "admin", "itmanager", "itemployee", and "demo" 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 (see Change the default Admin password on page 162).

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 129.

Change the default Admin password

▶ 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**.

Password:

Password (again):

Modify Password

Eliminate Default MySQL Account Names

By default, there are two MySQL accounts available with Enterprise Discovery (admin and itmanager). As with the user accounts, it is recommended that you delete these accounts or at least change the default passwords.

To change the admin account password:

1 Click **Administration > MySQL accounts > Modify password**.

2 Select an account name and click **Modify Account**.

3 Enter the new password in the Password field.

4 Enter the new password in the Password (again) field.

5 Click **Modify Password**.

Password:

Password (again):

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 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.

▶ 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

⚑ 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 From the HP support web site, download the latest Discovery Knowledge package.

▶ If you use Internet Explorer to download the file, rename the file to match the name listed on the support web site. For example DiscoveryKnowledge-2.0.xxxx.cab.

2 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\HP OpenView\Enterprise
Discovery\2.1.1\Install
```

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

4 To view the knowledge package you have installed, click **Status > Current Settings > Installed Components**.

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.

Using SAI files

The Discovery Knowledge Package contains the following SAI files:

- Master.zsai
- French.zsai
- German.zsai
- Unix.zsai

By default Enterprise Discovery is configured to use only the Master SAI.

To ensure that any other SAI files are included in the enrichment process you will need to configure the **xmlenricher.ini** file and restart the XML Enricher Service.

See the section entitled *Configuring the XML Enricher Using xmlenricher.ini* in the *Configuration and Customization Guide* for information on how to do this.

To extract the SAIs to a standalone client, you need to unzip the CAB file and move the files as needed.

20 Asset Questionnaire

Once you have installed your Enterprise Discovery server, you may want to set up an Asset Questionnaire that will help you track your devices with details that would normally be unavailable to the product database.

This Questionnaire will allow you to associate a person's name, department, phone number, or other personal information that you want to associate with this device in the Enterprise Discovery database. This data will be saved with the other data for a specific device (obtained by discovery or scanning), and will appear in the Device Manager.

You can configure one global Asset Questionnaire. Configure that first, and then you can access the Asset Questionnaire from any workstation with a web browser.

▶ This Asset Questionnaire data will be saved in the Enterprise Discovery server database, and will also be saved in the Aggregator (if you have one configured.

Configuring your Asset Questionnaire

By default, the Asset Questionnaire contains only the following fields:

- Description
- Asset Tag
- Employee ID
- Last Name
- First Name
- Full Name

- Job Title
- Cost Center
- Business Unit
- Division

➤ If you configure a First Name or Last Name with the questionnaire, this data will override what was found by the Enterprise Discovery scanner.

There are several other default options to add to your questionnaire, including items like Telephone Number, Floor, Room, Barcode, etc. If you require more question fields on your questionnaire, you can also add up to 30 of your own.

This procedure will take you through the basic steps of setting up your complete Asset Questionnaire. You can make changes to the Questionnaire at any time, but we recommend creating it once.

Configuring your Asset Questionnaire

1 Click **Administration > System Configuration > Asset Questionnaire.**

2 To create your own question fields, click **User-defined questions**.

3 Configure your questions by entering field names into the "custom" area of each entry. You can enter up to 30 different fields.

4 Click **Change** to submit your entries.

   As you configure the rest of your Questionnaire, you will see your own fields as well as the default fields.

5 To select which question fields will appear in your Asset Questionnaire, click **Administration > System Configuration > Asset Questionnaire > Question Selection.**

6   Under custom, configure the question fields you would like to see in your Questionnaire.

⮞   Be sure to enter any of the fields you entered in Step 3.

7   Click **Change** to submit your entries.

8   To configure the type of responses allowed for each question, click **Administration > System Configuration > Asset Questionnaire > Question type.**

9   Configure the type of answer that can be entered in the Asset Questionnaire.

For example, if you want to be able only a text string (for example, department name), or only a number (for example, employee number), you can make sure that only appropriate answers are collected.

You have the following options:

* Text
* Yes or No
* Number
* List (select from a series of selectable answers)

- Text + List

10 Click **Change** to submit your entries.

11 To configure which questions are required in the Asset Questionnaire, click **Administration > System Configuration > Asset Questionnaire > Required fields.**

12 For each entry, select Yes if you want it to be a required field.

Required Fields		
Description:	⦿ Default:	No
	○ Custom:	○ Yes ⦿ No
Asset Tag:	⦿ Default:	No
	○ Custom:	○ Yes ⦿ No
Employee ID:	⦿ Default:	No
	○ Custom:	○ Yes ⦿ No
Last Name:	⦿ Default:	No
	○ Custom:	○ Yes ⦿ No
First Name:	○ Default:	No
	⦿ Custom:	⦿ Yes ○ No
Full Name:	○ Default:	No
	⦿ Custom:	⦿ Yes ○ No
Job Title:	⦿ Default:	No
	○ Custom:	○ Yes ⦿ No
User Field 2:	⦿ Default:	No
	○ Custom:	○ Yes ⦿ No
User Field 1:	⦿ Default:	No
	○ Custom:	○ Yes ⦿ No

13 Click **Change** to submit your entries.

14 To set rules for each question, click **Administration > System Configuration > Asset Questionnaire Configuration > Answer rules.**

If you wish, you can set up some validation rules for your text strings. You can set minimum and maximum length, and any regular expression that should be included in the answers.

Answer Rules						
Description:	⦿ Default:					
	○ Custom:	Min: 0	Max:	Regex:		Case-sensitive: ⦿ Yes ○ No
Asset Tag:	⦿ Default:					
	○ Custom:	Min: 0	Max:	Regex:		Case-sensitive: ⦿ Yes ○ No
Employee ID:	⦿ Default:					
	○ Custom:	Min: 0	Max:	Regex:		Case-sensitive: ⦿ Yes ○ No
Last Name:	⦿ Default:					
	○ Custom:	Min: 0	Max:	Regex:		Case-sensitive: ⦿ Yes ○ No
First Name:	⦿ Default:					
	○ Custom:	Min: 0	Max:	Regex:		Case-sensitive: ⦿ Yes ○ No
Full Name:	⦿ Default:					
	○ Custom:	Min: 0	Max:	Regex:		Case-sensitive: ⦿ Yes ○ No
Job Title:	⦿ Default:					
	○ Custom:	Min: 0	Max:	Regex:		Case-sensitive: ⦿ Yes ○ No
User Field 1:	○ Default:					
	⦿ Custom:	Min: 0	Max:	Regex: PAT		Case-sensitive: ○ Yes ⦿ No

15 Click **Change** to submit your entries.

16 If you have configured any of your questions to have a List of possible answers, you should now configure the List. Click **Administration > System Configuration > Asset Questionnaire > Answer selection.**

17 Configure a series of answers for the Lists on your Asset Questionnaire.

➤ If you would prefer to compose your answers separately, and import them into the UI, see Importing Your Answer Selections on page 173.

In order for a question to appear on this page, you must first configure it as a list in step Step 9.

• Select a question from the first pull-down list.

- Type in an answer in the text field (maximum of 255 characters) and click **Add**.

18 When you have added your answers, click **Submit**.

You have completed your Asset Questionnaire configuration.

Importing Your Answer Selections

If you would prefer to compose your answers separately, you can import them into the UI as a CSV file.

1 Click **Administration > System Configuration > Asset Questionnaire Configuration > Import answer selection.**

2 Click **Browse** to locate the file on your computer.

3 Click **Import**.

Exporting Your Answer Selections

If you would like to save your answer selections to an external location, you can export them as a CSV file.

1 Click **Administration > System Configuration > Asset Questionnaire Configuration > Export answer selection.**

A **File Download** dialog appears.

2   Click **Save**.

3   Save the file to your computer.

Using the Asset Questionnaire

Setting Your Default Home Page

You can set the Questionnaire as your default home page, so when you are working on a user's workstation, you can log in to Enterprise Discovery and see the Questionnaire first.

To set the Asset Questionnaire as your home page:

1   Click **Administration > My Account Administration > Account Properties**.

2   For **Default Home Page**, select **Asset Questionnaire**.

3   Click **Modify Properties**.

Logging in from a User Workstation

1   From the user's workstation, access their web browser and log in to Enterprise Discovery.

2   Click **Asset Questionnaire**.

show the screen displaying your current IP etc.

Logging in from the Device Manager

There is an Asset Questionnaire button in the Device Manager.

Enter the Asset Information

When you access the Asset Questionnaire from a workstation, what you see will depend on how Enterprise Discovery is configured.

The Workstation is in your IPv4 Ranges

If the device is in your IPv4 ranges, and you want to add asset information from the Questionnaire, just enter the information as needed, and click **Submit**.

The Workstation is NOT in your IPv4 Ranges

If the device you are connecting from has not been included in Enterprise Discovery's IPv4 ranges, you will be asked to add the address to the ranges being polled.

You cannot enter an Asset Questionnaire for a device until it has been discovered by Enterprise Discovery.

This is NOT the workstation you want to configure

If you want to do the Asset Questionnaire for another device, you need to enter its IP address and click **Change**. Then, you can enter the Questionnaire info and click **Submit**.

21 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, 8.x and Enterprise Discovery 2.0.x will need to follow these procedures to upgrade their application libraries so they can work with Enterprise Discovery 2.1.

Table 1   Upgrade Steps

If you have...	You will need to...
Desktop Inventory 7.x	• Contact HP Support
Desktop Inventory 8.x	• Migrate Your ApE Database or Convert Your Old Read Only or User SAIs
Enterprise Discovery 2.0.x	• Convert Your Old Read Only or User SAIs

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 2.1.1.

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 2.1.1 software.

Convert Your Old Read Only or User SAIs

SAI Update Wizard is used to:

- Convert read-only SAIs to an Enterprise Discovery User SAI.
- Convert old 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.

Starting the SAI Update Wizard

To start the SAI Update Wizard:

- From the Windows **Start** menu select **Programs > HP > Enterprise Discovery 2.1.1 > SAI Update Wizard**.

On starting the SAI Update Wizard, the following page appears.
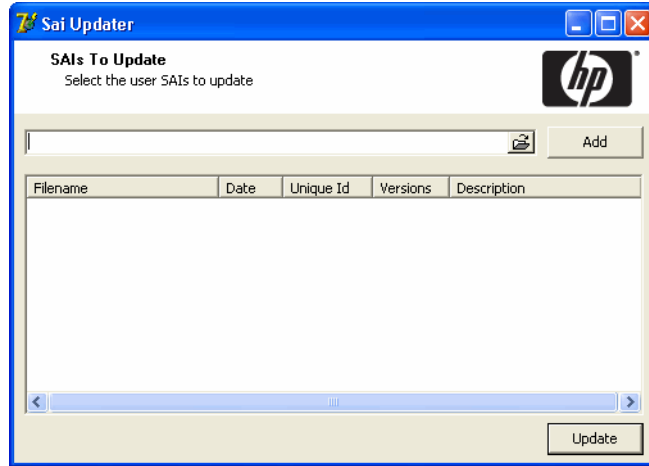
This page allows you to update your User SAI to work with the latest version if Enterprise Discovery.

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.

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

The SAI update procedure is completed and has been saved in the following directory.

HP OpenView\Enterprise Discovery\2.1.1\Common

22 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.

▶ 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/Peregrine/Enterprise Discovery/2.1.1/logs`.

Index

troubleshooting, 146
    activating changes, 127
    when logging in, 63

U

uninstalling Enterprise Discovery, 153

unmanaged routers, 118

upgrade
    restart, 47

upgrade scenarios, 15

upgrading your Custom Application Library,
    177

users
    Global SNMP Property Group, 90

Utilization, 100

V

Virtual Network Computing (VNC), 182

W

web interface, 59

Windows components, 59

Windows Remote Desktop, 181