HP OpenView Enterprise Discovery

for the Windows® operating system

Software Version: 2.20

Installation and Initial Setup Guide

Manufacturing Part Number: T4180-88007
Document Release Date: April 2007
Software Release Date: April 2007

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.

Windows Vista™ is either a registered trademark or trademark of Microsoft Corporation in the United States and/or other countries.

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

UNIX® is a registered trademark of The Open Group.

Intel® is a registered trademark of Intel Corporation or its subsidiaries in the United States and other countries.

Support

You can visit the HP Software Support web site at:

http://support.openview.hp.com/support.jsp

HP Software 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:

http://support.openview.hp.com/new_access_levels.jsp

Contents

1 Welcome to Enterprise Discovery

Welcome to the *Installation and Initial Setup Guide*.

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

About Enterprise Discovery Installation

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\2.20

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[a]

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

a. The Discovery + Network Topology license combination is also available to customers who upgrade from previous versions of Enterprise Discovery. The Discovery license provides basic information on the devices, such as when they are added to or removed from the network.

Automated Inventory

With this license, Enterprise Discovery will ping and poll your network device groups to find devices. You can also 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 is combined with the Discovery data in the Enterprise Discovery database.

The Automated Inventory license provides the same capability that the Device Discovery and Device Inventory licenses provided in previous versions of Enterprise Discovery. If you have purchased these two licenses for a previous version, you will have access to all features provided with the Automated Inventory license offered with version 2.20.

Software Utilization

With this license, you can expand your inventory data, as the scanners will capture details on what software is used on each 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 2.20 installation.

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 35	
2	Install the client components.	Client Installation on page 57	
3	Configure your server	Configuring your Enterprise Discovery Server on page 75	More details available in the *Customization and Configuration Guide*.
4	Set up Network and SNMP Configuration Profiles	Setting Up Discovery Configuration Profiles on page 110	After you create these configuration profiles, you can assign them to device groups in the next step.
5	Set up IP-only device groups	Setting Up Device Groups on page 120	
6	Activate your changes	Activating Your Configuration Changes on page 147	Wait until Enterprise Discovery has discovered all of those devices before continuing. Check **Status > Device status > Network model queue/Network model processing**.

Table 1 New Installation

Task		Instructions	Notes
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 configuration profiles for testing	Setting Up Discovery Configuration Profiles on page 110 Setting Agent Deployment Accounts on page 139 Setting Up Scanner Schedules on page 145	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 147	
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 155	

Migrating from Desktop Inventory 7.x or later

If you worked with Desktop Inventory, you will need to upgrade to Enterprise Discovery 2.20. 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 2.20 as I have been using Desktop Inventory, but I also want to automatically deploy agents and scanners on page 20
- I want to use Enterprise Discovery 2.20 as I used Desktop Inventory on page 24

I want to use Enterprise Discovery 2.20 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 206	
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.

Table 2 Migrating from Desktop Inventory

Task		Instructions	Notes
4	Install the Enterprise Discovery server components on the computers where you had a “complete install” of Desktop Inventory.	Server Installation on page 35	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 57	
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 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.

Table 2 Migrating from Desktop Inventory

Task		Instructions	Notes
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 206	
4	Set up Network and SNMP Configuration Profiles	Setting Up Discovery Configuration Profiles on page 110	After you create these configuration profiles, you can assign them to device groups in the next step.
5	Set up IP-only device groups	Setting Up Device Groups on page 120	
12	Activate your changes	Activating Your Configuration Changes on page 147	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 configuration profiles for testing	Setting Up Discovery Configuration Profiles on page 110 Setting Agent Deployment Accounts on page 139 Setting Up Scanner Schedules on page 145	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 147	
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.

Table 2 Migrating from Desktop Inventory

Task		Instructions	Notes
16	Repeat steps 11, 12, 13, 14 for the remainder of your network.		
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.

Table 2 Migrating from Desktop Inventory

Task		Instructions	Notes
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 155	

I want to use Enterprise Discovery 2.20 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 35	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 57	
5	Configure the Enterprise Discovery server to have a large scan only IP range.	1 Click **Administration > Discovery Configuration** 2 Create a device group for this IP range. 3 Assign the <Restrict to scanned-only devices> Basic Discovery profile to this device group. 4 Activate these changes.	If the Enterprise Discovery server is not configured in this way then the XMLenricher will not process the scan files.

Table 3 Migrating from Desktop Inventory

Task		Instructions	Notes
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 206	
10	Migrate your SAIs.	Convert Your Old Read Only or User SAIs on page 206	

Table 3 Migrating from Desktop Inventory

Task		Instructions	Notes
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 155	

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 35	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 57	
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 35	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 57	
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 206	

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 configuration profiles for testing	Setting Up Discovery Configuration Profiles on page 110 Setting Agent Deployment Accounts on page 139 Setting Up Scanner Schedules on page 145	This step is optional. 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 147	
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.

Table 5 Upgrading from Enterprise Discovery 1.0

Task		Instructions	Notes
15	Populate AssetCenter.		This step is only necessary if you populate AssetCenter with scan file data.
16	Clean up your old Desktop Inventory data.	**Administration > System Configuration > Scan deployment**. Enable the "Clean PDI data from workstations" option.	
17	Set up Accounts	Setting up Accounts on page 155	

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 2.20:

Table 6 Upgrading from Enterprise Discovery 2.0

Task		Instructions	Notes
1	Back up your Enterprise Discovery data.	See Chapter 15, Backing up and Restoring your data.	
2	Uninstall Enterprise Discovery 2.0	See Chapter 16, Uninstalling Enterprise Discovery	
3	Install Enterprise Discovery 2.20	See Chapter 3, Server Installation and Chapter 4, Client Installation.	

After you upgrade to Enterprise Discovery 2.20, 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 Enterprise Discovery server components on one dedicated server. The server components can be installed on Windows 2003 Server, SP1 or SP2. (Windows XP SP2 is also compatible, but should only be used for trial or demo installation.) If you install the server components on a laptop, be sure to turn hibernation off.

Table 1 details a variety of scenarios that can help you estimate your server hardware requirements. The Disk value is for your data directory. In addition, you will require at least 6GB under Program Files for the Enterprise Discovery installation.

Agg = Aggregator, Auto Inv = Automated Inventory, Top = Topology

Table 1 Suggested Hardware Requirements

Discovered Devices	Inventoried Devices	Ports	Agg	Auto Inv	Top	Memory (GB)	CPU[a]	Disk (GB)
6,000	5,000	36,000		✔		1.5	1 CPU 2.4 GHz	25
6,000	5,000	36,000		✔	✔	3	1 CPU 2.8 GHz	40
18,000	15,000	108,000		✔		2[b]	2 CPUs or cores 3.0 GHz	70
18,000	15,000	108,000		✔	✔	5	2 CPUs or cores 3.0 GHz	105
60,000	50,000	150,000		✔		4	2+ CPUs or cores 3.6 GHz	200

Table 1 Suggested Hardware Requirements

Discovered Devices	Inventoried Devices	Ports	Agg	Auto Inv	Top	Memory (GB)	CPU[a]	Disk (GB)
60,000	50,000	150,000		✔	✔	7	2+ CPUs or cores 3.6 GHz	260
50,000	50,000	n/a	✔	n/a	n/a	2	2 CPUs or cores 3.0 GHz	10
500,000	150,000	n/a	✔	n/a	n/a	3	2 CPUs or cores 3.6 GHz	50

a. CPU processor speeds are approximate guidelines. Newer CPUs may have lower frequencies but higher performance than those shown in the table. Enterprise Discovery is a multi-threaded application, and benefits from Simultaneous Multi-Threading (SMT) technologies such as Intel Hyper-Threading.

b. 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 Automated Inventory license, this includes:

- **Backup Scan Files** in enabled (on average, each scan file is 270KB)
- **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)

The suggested requirements in Table 1 assume 1 XML Enricher. If you choose to run 2 XML Enrichers, additional CPUs and more memory will be required.

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.

Checking for ActivePerl

Many applications including Enterprise Discovery install ActivePerl, a popular program used for running scripts. Before you install Enterprise Discovery, you must verify that there is no other version of ActivePerl installed. If ActivePerl is installed, you will need to remove it before you run the Enterprise Discovery installer.

To see if ActivePerl is installed:

1. On the Server where you intend to install Enterprise Discovery, open a DOS command window or command prompt.
2. Type **`perl -v`**

   If ActivePerl is detected, you will see information like this:

   ```
   This is perl, v5.8.6 built for MSWin32-x86-multi-thread
   (with 3 registered patches, see perl -V for more detail)

   Copyright 1987-2004, Larry Wall

   Binary build 811 provided by ActiveState Corp. http://
   www.ActiveState.com

   ActiveState is a division of Sophos.

   Built Dec 13 2004 09:52:01
   ```

```
Perl may be copied only under the terms of either the
Artistic License or the GNU General Public License, which
may be found in the Perl 5 source kit. Complete
documentation for Perl, including FAQ lists, should be
found on this system using `man perl' or `perldoc perl'.
If you have access to the Internet, point your browser at
http://www.perl.org/, the Perl Home Page.
```

- The **`perl -v`** command only examines the system PATH environment variable. Most applications that install ActivePerl add it to the PATH. To be absolutely sure that no version of ActivePerl is installed on the system, however, you must also examine the system registry.

  If you determine that any version of ActivePerl is installed, you must remove the application that installed ActivePerl before you can install Enterprise Discovery.

- The Enterprise Discovery installer silently runs **`perl -v`** to capture the version information of any existing ActivePerl installation. If it does not find ActivePerl in the system PATH, the installer scans the system registry for installed versions of ActivePerl and stops the installation if one is found.

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 five to twenty minutes to react to licensing changes. Do not restart the server during this time.

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:

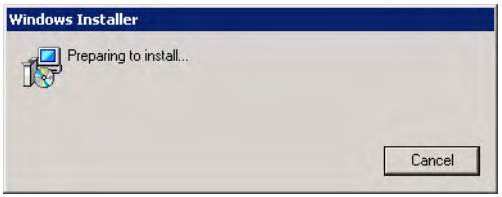
1 While Windows is running, insert the Installation CD into the CD ROM drive of the server.

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.

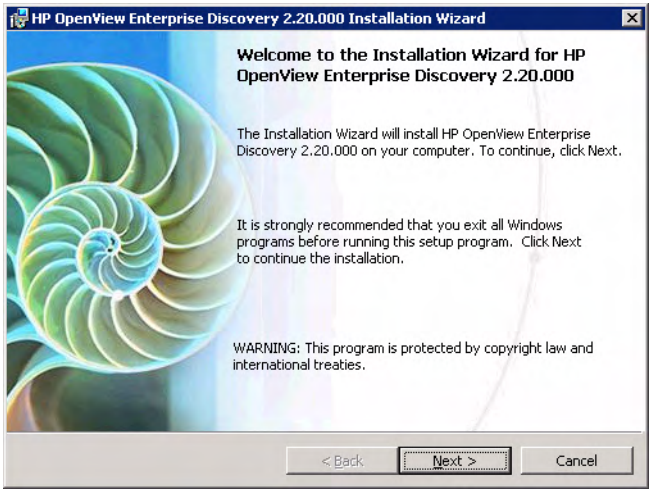
The following screen appears.

2 Click Install Enterprise Discovery to start the install process.

Next, the Preparing to Install window appears.

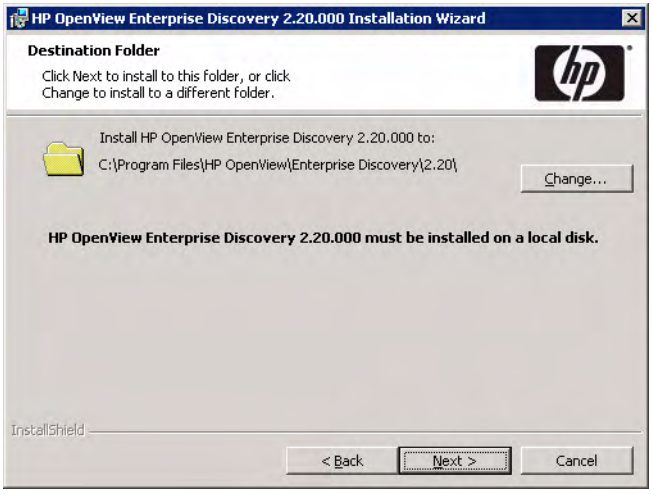


Next, the Installation Wizard appears.



3 Click **Next**.

The Destination Folder screen appears.



The default installation directory is:

C:\Program Files\HP OpenView\Enterprise Discovery\2.20

Enterprise Discovery must be installed on a local disk, and cannot be installed on network drives, SAN drives, or 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.

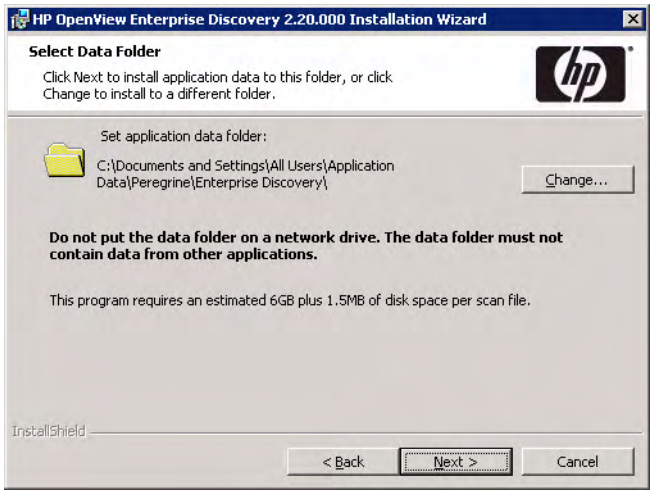
See the Microsoft Help for more information on how to configure SNMP and the related community names.

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.



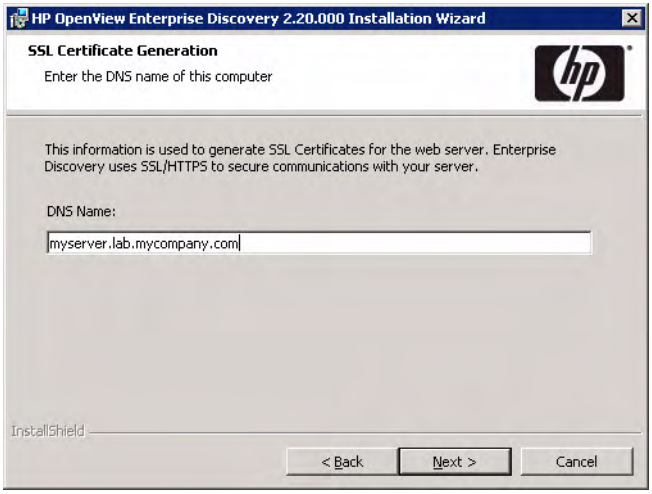
You cannot put the data folder in the root directory (for example, C:).

The Data folder cannot contain any data from other applications.

9 Click **Next**.

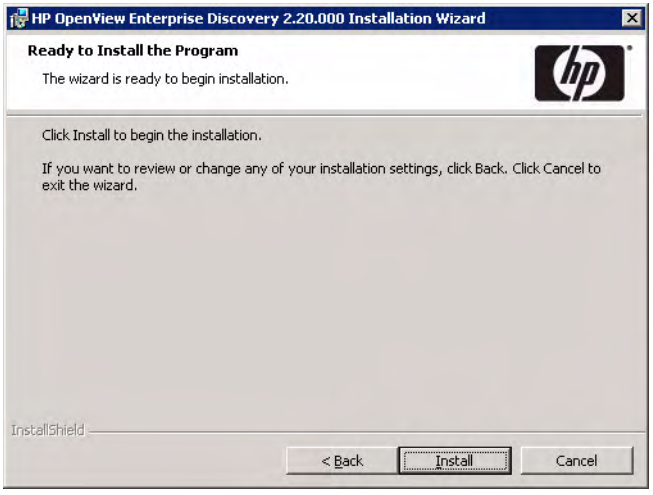
The SSL Certificate Generation screen appears.

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



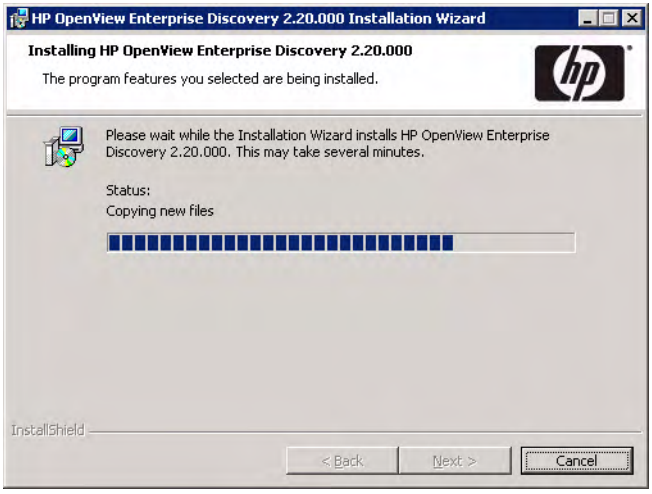
11 Click **Next**.

The Ready to Install the Program screen appears.



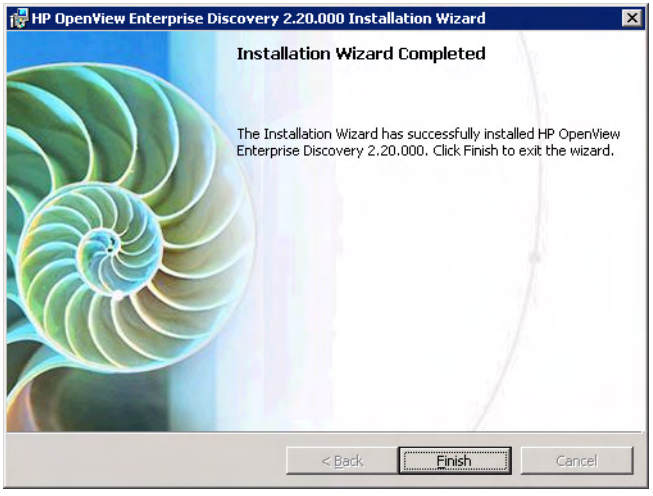
12 Click **Install** to begin the installation.

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.

Running an Unattended Installation of Enterprise Discovery

It is possible to perform an unattended installation of Enterprise Discovery using the MSIEXEC command line with the proper parameters.

To perform an unattended install of Enterprise Discovery

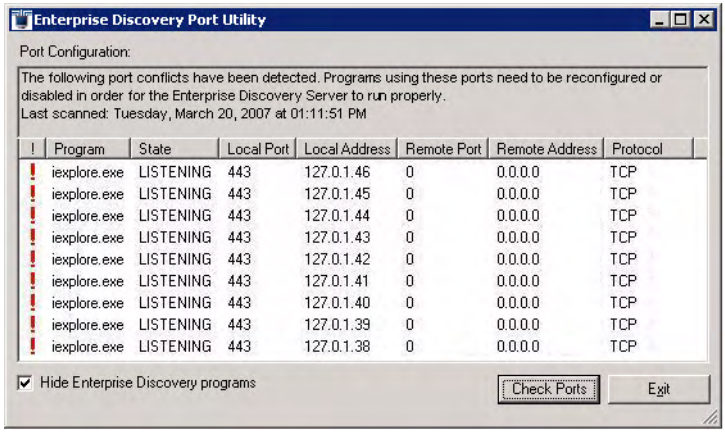
1. Open a command prompt window.
2. Navigate to the directory containing all of the installation files for Enterprise Directory.
3. Type the following command at the prompt:

```
"HP_OpenView_Enterprise_Discovery_2.2x.xxx.msi" ADDLOCAL=ALL
ALLUSERS=1 REBOOT=ReallySuppress SETUPTYPE=TYPICAL /qr
```

4. Manually restart the server after the installation 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.

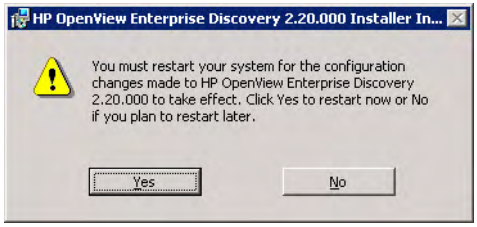


You will need to make these ports available in order to use Enterprise Discovery.

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 Services are Running

The following table contains a comprehensive list of services that run after Enterprise Discovery has been installed. Depending on the type of license that you purchase and how your server is configured, you will see some or all of these services.

After you have completed your installation, check the list of services on your server (**Control Panel > Administrative Tools > Services**) to be sure that all HP OpenView Discovery services (except those marked “optional” in the list) are running.

If these services are not running, make sure that you have restarted your server as described in Restarting your Server on page 50.

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	Enables communication between remote computers and the HP OpenView Discovery Server
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.

Table 3 Services

Service	Description
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.
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 (1)	Additional XML Enricher process that you can enable to enhance the speed of scan file processing. This service is optional; it is not required for Enterprise Discovery to run.
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:

You can install the client portion on several workstations.

The server install contains everything available in Enterprise Discovery 2.20. 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 or 1.5	Firefox 1.5
	Internet Explorer 5.5 or 6.0	Internet Explorer 6.0
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 41).

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.

Installing your License on the Client:

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

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

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

You can 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:

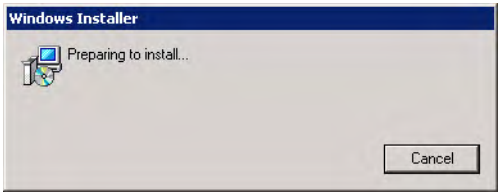
1. While Windows is running, insert the Installation CD into the CD ROM drive of your computer.

   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.

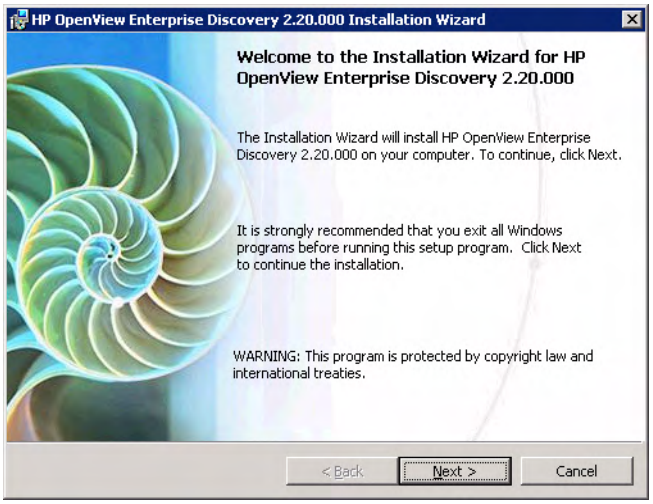
The following screen appears.

2 Click Install Enterprise Discovery to start the install process.

Next, the Preparing to Install window appears.

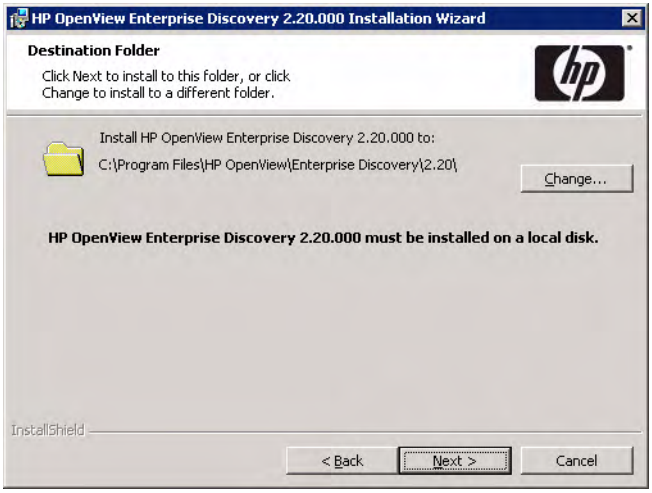


Next, the Installation Wizard appears.



3 Click **Next**.

The Destination Folder screen appears.



The default installation directory is:

C:\Program Files\HP OpenView\Enterprise Discovery\2.20

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.

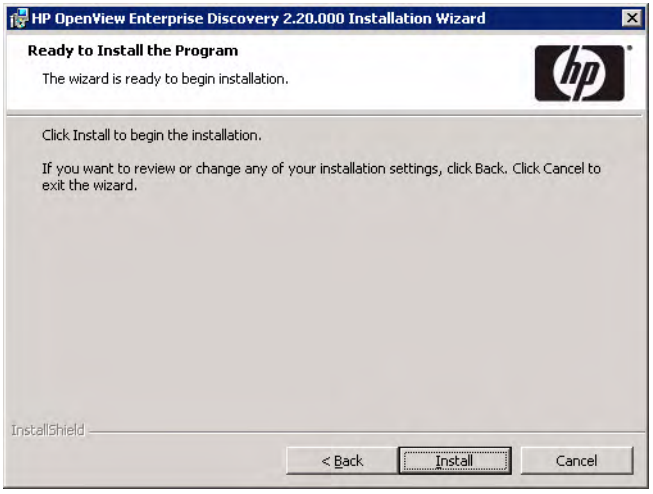
5 Click **Next**.

The Setup Type screen appears.

6 Select the “Client” Setup Type.

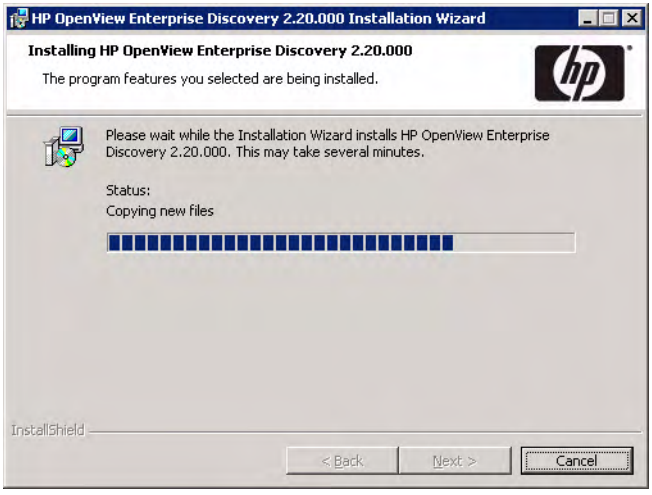
7 Click **Next**.

The Ready to Install the Program screen appears.

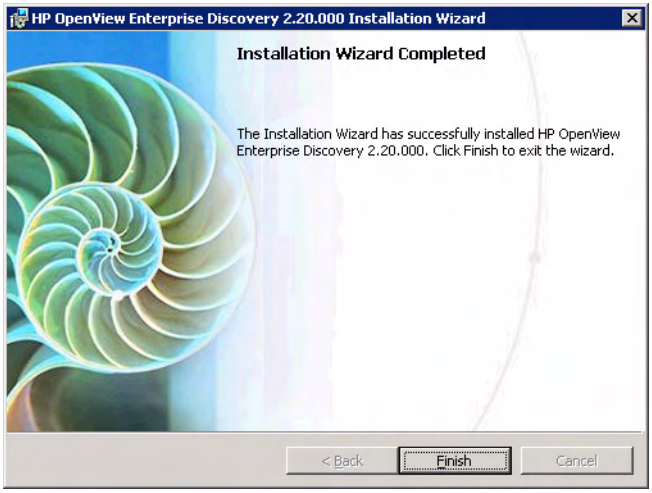


8 Click **Install** to begin the installation.

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:

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

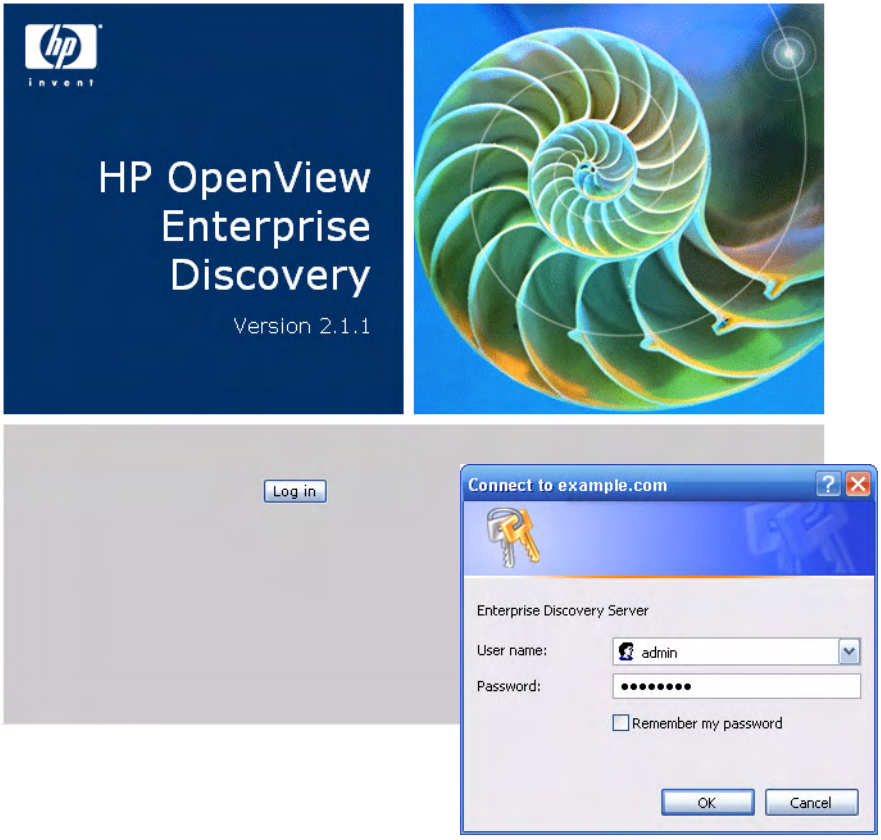
Account type	Account name	Password
Administrator	admin	password
IT Manager	itmanager	password
IT Employee	itemployee	password
Demo	demo	demo

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 189.

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.

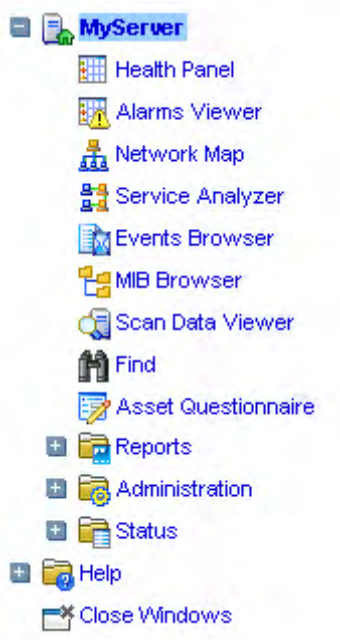
Since this is the first time you are logging into Enterprise Discovery, there will be no useful statistics presented. Once you have configured your server, however, you should see these statistics change.

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

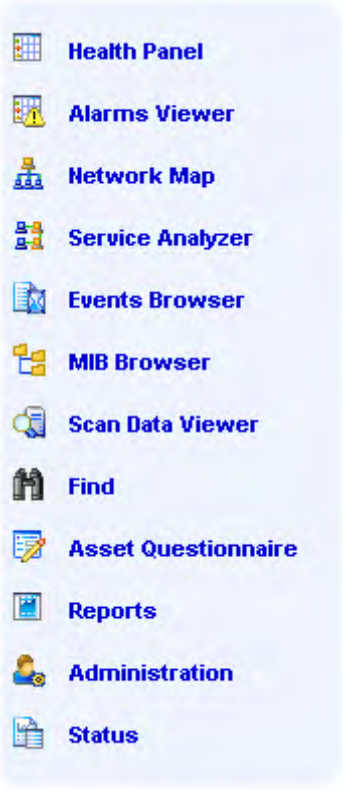
Table	Description
Discovery Status	This table will show you a breakdown of your network devices, so you can see how many devices have been discovered, how many have agents installed, etc.
Discovery Server Configuration	This table will show you how many device groups you have configured, and the status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

You can navigate the menus using the tree on the left side, the short-cut menu on the right side, or the links throughout the interface.

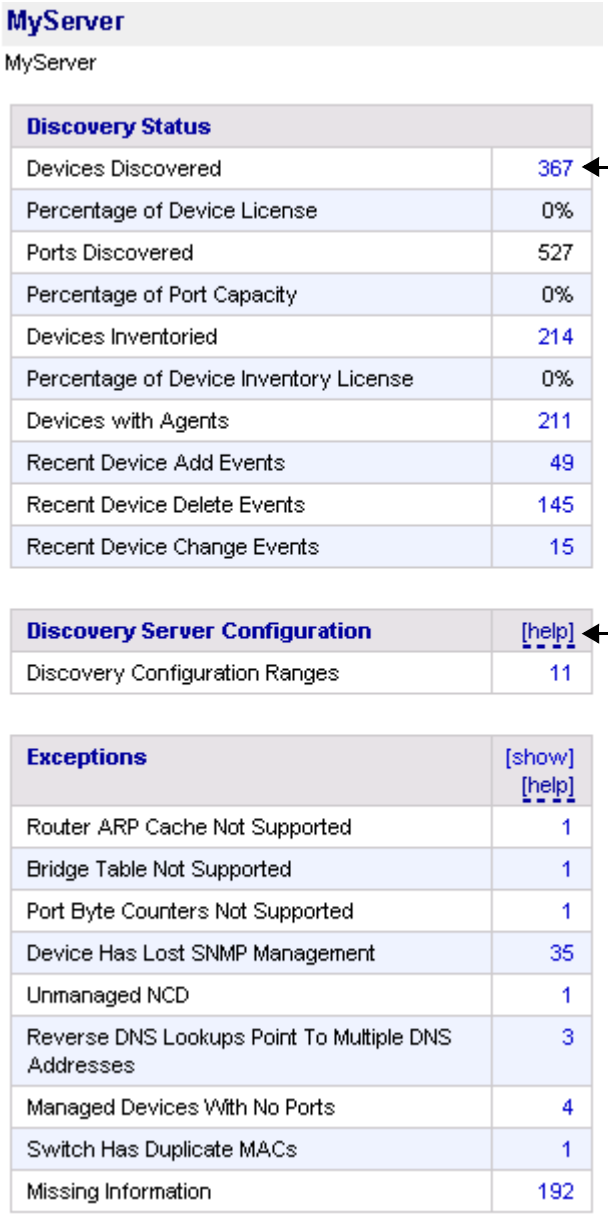
Navigation Tree:



Short-Cut Menu:



Network Status Information:



MyServer

MyServer

Discovery Status	
Devices Discovered	367
Percentage of Device License	0%
Ports Discovered	527
Percentage of Port Capacity	0%
Devices Inventoried	214
Percentage of Device Inventory License	0%
Devices with Agents	211
Recent Device Add Events	49
Recent Device Delete Events	145
Recent Device Change Events	15

Discovery Server Configuration	[help]
Discovery Configuration Ranges	11

Exceptions	[show] [help]
Router ARP Cache Not Supported	1
Bridge Table Not Supported	1
Port Byte Counters Not Supported	1
Device Has Lost SNMP Management	35
Unmanaged NCD	1
Reverse DNS Lookups Point To Multiple DNS Addresses	3
Managed Devices With No Ports	4
Switch Has Duplicate MACs	1
Missing Information	192

Click blue numbers and words for more detailed information

Click words underlined with dashes for online help in a separate window

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 2.20**.
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

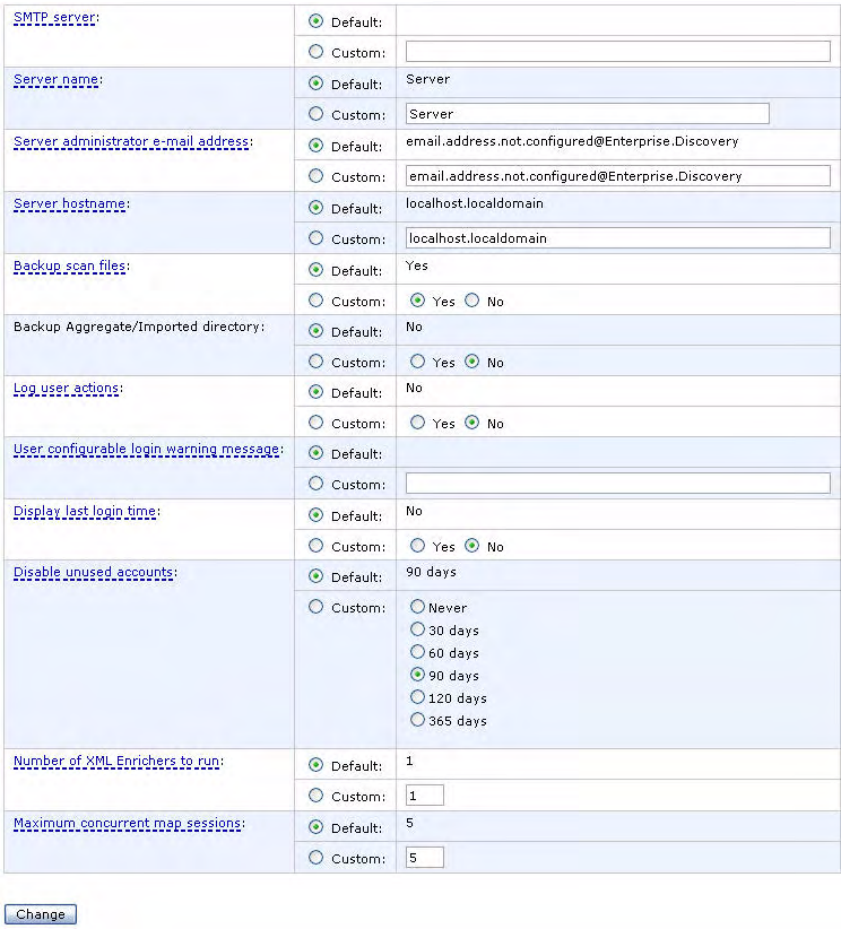
Once you have installed the software, and you have seen where the components are located, you can now configure the Enterprise Discovery server. Once this is completed, you can then configure the server to start discovering your network.

To configure your server, log in to the Web Interface as described in Getting Started on page 65, and then complete the following procedures:

- Enter the SMTP server on page 76
- Enter a server name on page 77
- Enter the Administrator e-mail address on page 77
- Enter the server host name on page 78

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.



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 IP 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 IP 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 profiles	Chapter 8, Configuring the Discovery Process
Create SNMP profiles	Chapter 8, Configuring the Discovery Process
Create Agent profiles and Agent deployment accounts	Chapter 8, Configuring the Discovery Process and Chapter 10, Setting Agent Deployment Accounts
Create Scanner profiles and Scanner schedules	Chapter 8, Configuring the Discovery Process and Chapter 11, Setting Up Scanner Schedules
Set up device groups, and assign your profiles to these groups	Chapter 8, Configuring the Discovery Process
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 Discovery Quick Start Scenario

In this chapter, you will learn how to quickly set up Enterprise Discovery so that it can start discovering your network. The following topics are covered:

The purpose of this chapter is to help you get the discovery process started as simply and quickly as possible. For a more in-depth explanation of discovery configuration, see Chapter 8, Configuring the Discovery Process.

Introduction

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

This chapter will show you how to do three things:

- Set up a small number of device groups based on IP ranges.
- Set up an SNMP configuration profile that contains the correct SNMP credentials for your network, and associate this profile with your device groups.
- Apply the predefined <Active discovery> configuration profile to your device groups.

After you have a better idea of what your network contains, you can fine-tune your discovery configuration by setting up customized device groups and configuration profiles. This is covered in Chapter 8, Configuring the Discovery Process.

Set up an SNMP profile

If you provide the correct SNMP information, Enterprise Discovery can interrogate the MIB of any SNMP-managed device that it discovers and gather detailed information about that device. If you don't provide the SNMP information, it can only discover the IP address of each device.

To create an SNMP profile:

1. Click **Administration > Discovery Configuration > Profiles**.
2. Click the **SNMP** tab.
3. Click **New.**
4. Provide a unique name for your profile.
5. *Optional:* Provide a more detailed description of your profile.
6. With the **SNMP Version 1/2** tab active, click **New**.
7. Provide all community strings used in your network.
8. If you have SNMPv3 devices in your network, click the **SNMP Version 3** tab.
9. Provide all user names used in your network, including authentication and encryption information as appropriate.
10. When you are finished adding SNMP information, click **Save and Close**.

At this point, you have an SNMP profile that you can assign to any device groups that you create. This profile will not be permanently saved until you review and activate your changes.

Set up device groups

Before you can start the discovery process, you must tell Enterprise Discovery where to look for your devices by setting up one or more device groups. In this quick start process, you will use device groups based on IP ranges. There are two ways to start setting up these device groups:

If you know	You can
Little about the contents of your network, and you're not sure where to begin	Run router discovery on page 83.
The IP ranges used in your network, and the types of devices contained in each range	Set up IP range device groups to discover on page 85. You can also Set up an IP range device group to avoid on page 86 and Configure discovery for DHCP servers and unmanaged routers on page 87.

Run 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 that it finds, and you can use that list to define device groups.

Router Discovery only runs when you initiate it. This is not a continuous process. Also, you must specify or create an SNMP profile that contains the correct SNMP access information—either community strings or user names and pass phrases. If you do not provide this information, Router Discovery will not be successful.

If you prefer to set up your device groups manually, go to Set up IP range device groups to discover on page 85.

To set up Router Discovery:

1. Click **Administration > Router discovery > Router discovery limits**.
2. Set the maximum hops, minimum line speed, and maximum line speed.

   Hop 0 (zero) is always the Enterprise Discovery server itself, and hop 1 is always the default gateway.
3. Click **Change**.
4. Click **Administration > Router discovery > SNMP settings.**
5. Enter the SNMP credentials for your routers.
6. Click **Change**.

To run Router Discovery:

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

To activate an IP range device group that Router Discovery has identified:

1. Click **Administration > Router discovery > Router discovery results**.
2. For each discovered IP range device group, select the following configuration profiles:
   a. The <Active Discovery> Basic Discovery profile
   b. The SNMP profile you created earlier
3. If you want to make any changes to the definition of the device group, click its name—in this case, its name is the IP range that it includes. You can change the name, the description, or the IP range.
4. Click **Activate**.

Set up IP range device groups to discover

For each IP range that you want to discover, you must create an IP range device group and assign the appropriate configuration profile to that device group.

When you entered the IP address of your Enterprise Discovery server, the subnet in which that server resides was automatically determined, as was the address of the default gateway. A device group was automatically created for each of these items.

View existing IP range device groups

If you have run Router Discovery, the IP range device groups that you activated in the previous section should appear in this list.

To view your IP range device groups:

1 Click **Administration > Discovery Configuration > Device Groups**.

Create an IP range device group

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

To create an IP range device group:

1 Click **Administration > Discovery Configuration > Device Groups**.

2 Click **New**.

3 Specify a unique **Device group name**.

4 *Optional:* Specify a **Description** for the device group.

5 From the **Condition Type** list, select **IP Address**.

6 From the **IP Type** list, select **IP Range**.

7 In the **IP Address** boxes, enter the starting and ending IP addresses of your whole network—or a range within your network.

If you prefer, you can specify the IP range using one of the alternate IP types. See Create a Device Group on page 120 for more information.

8 Click **Continue**.

9 Click the **Configuration Profiles** tab.

10 From the **Basic Discovery** profiles list, select <Active Discovery>.

11 Click **Save and Close**.

Repeat this procedure for each IP range device group that you want Enterprise Discovery to discover.

At this point, you have added at least one IP range device group to your proposed new configuration, but your changes will not take effect until you review and activate your changes.

Set up an IP range device group to avoid

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

To avoid a range of IP addresses:

1 Create a new IP range device group for the IP range that you want to avoid. Follow steps 1–9 under Create an IP range device group on page 85.

2 From the **Basic Discovery** profiles list, select <All Off>.

3 Click **Save and Close**.

Repeat this procedure for each IP range device group that you want Enterprise Discovery to avoid.

At this point, you have added at least one IP range device group to your proposed new configuration that you want Enterprise Discovery to avoid, but your changes will not take effect until you review and activate your changes.

Configure discovery for DHCP servers and unmanaged routers

If you have one or more SNMP-managed DHCP servers or unmanaged routers, you can create a device group with their IP addresses and apply the appropriate configuration profile so that Enterprise Discovery will monitor these IP addresses differently.

To configure discovery for SNMP-managed DHCP servers:

1. Click **Administration > Discovery Configuration > Device Groups**.
2. Create a new device group to represent your DHCP servers. See Setting Up Device Groups on page 120 for more information.
3. For each DHCP server, add an IP Range condition specifying the starting and ending IP addresses for this server. (If this is a range consisting of only one device, add a Single IP condition instead.)
4. Assign the following configuration profiles to this device group:
   a. The system-defined <Active discovery> Basic Discovery profile.
   b. An SNMP profile specifying the correct SNMP credentials for your DHCP servers.
   c. The system-defined <DHCP Server> Network configuration profile.

   See Setting Up Discovery Configuration Profiles on page 110 for more information.
5. Click **Save and Close**.

To configure discovery for unmanaged routers:

1. Click **Administration > Discovery Configuration > Device Groups**.
2. Create a new device group to represent your unmanaged routers.
3. For each unmanaged router, add an IP range condition specifying the starting and ending IP addresses for this router. (If this is a range consisting of only one device, add a Single IP condition instead.)
4. Assign the following configuration profiles to this device group:
   a. The system-defined <Active discovery> Basic Discovery profile

b The system-defined <Unmanaged router> Network configuration profile.

5 Click **Save and Close**.

You have now specified the IP ranges to be treated as DHCP servers and unmanaged routers in your proposed new configuration, but your changes will not take effect until after you have reviewed and activated your changes.

Activate your pending changes

The **Activate** page enables you to review all the discovery configuration changes you have proposed before actually making those changes take effect.

When you have completed all the changes you wanted to make, you can activate those changes and start the discovery process.

To activate configuration changes:

1 Click **Administration > Discovery Configuration > Activate**.

2 Review the information on each of the tabs on the Activate page.

3 To apply your changes, click **Activate Changes**. To discard you changes, click **Revert Changes**.

For more information, see Activating Your Changes on page 125.

Making Future Configuration Changes

This chapter provided instructions to enable you to set up discovery quickly and simply just to get started. The instructions were to apply the <Active discovery> configuration profile to all of your IP range device groups and give them all the same set of SNMP credentials.

You can leave discovery set up this way if that is satisfactory to you. In fact, if there is a great deal 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 have Enterprise Discovery treat certain device groups—or individual devices, for that matter—differently than others.

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 IP range in a particular building one way and single out all the routers or servers across your network another way.

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 device groups can be deleted or that they need less than full active discovery.

On the other hand, you may decide you want even more information for certain device groups.

What Next?

So far, you have set Enterprise Discovery up to examine every device the same way. If you want to look at certain parts of the network or individual devices differently—or not at all—you can create device groups representing those devices. You can then apply configuration profiles to those groups to specify precisely how you want Enterprise Discovery to treat them.

To	Go to
Learn more about discovery configuration	Chapter 8, Configuring the Discovery Process
Learn about user accounts and access	Chapter 13, Setting up Accounts
Learn about setting up an Aggregator server	Chapter 14, Setting up Enterprise Discovery Aggregation

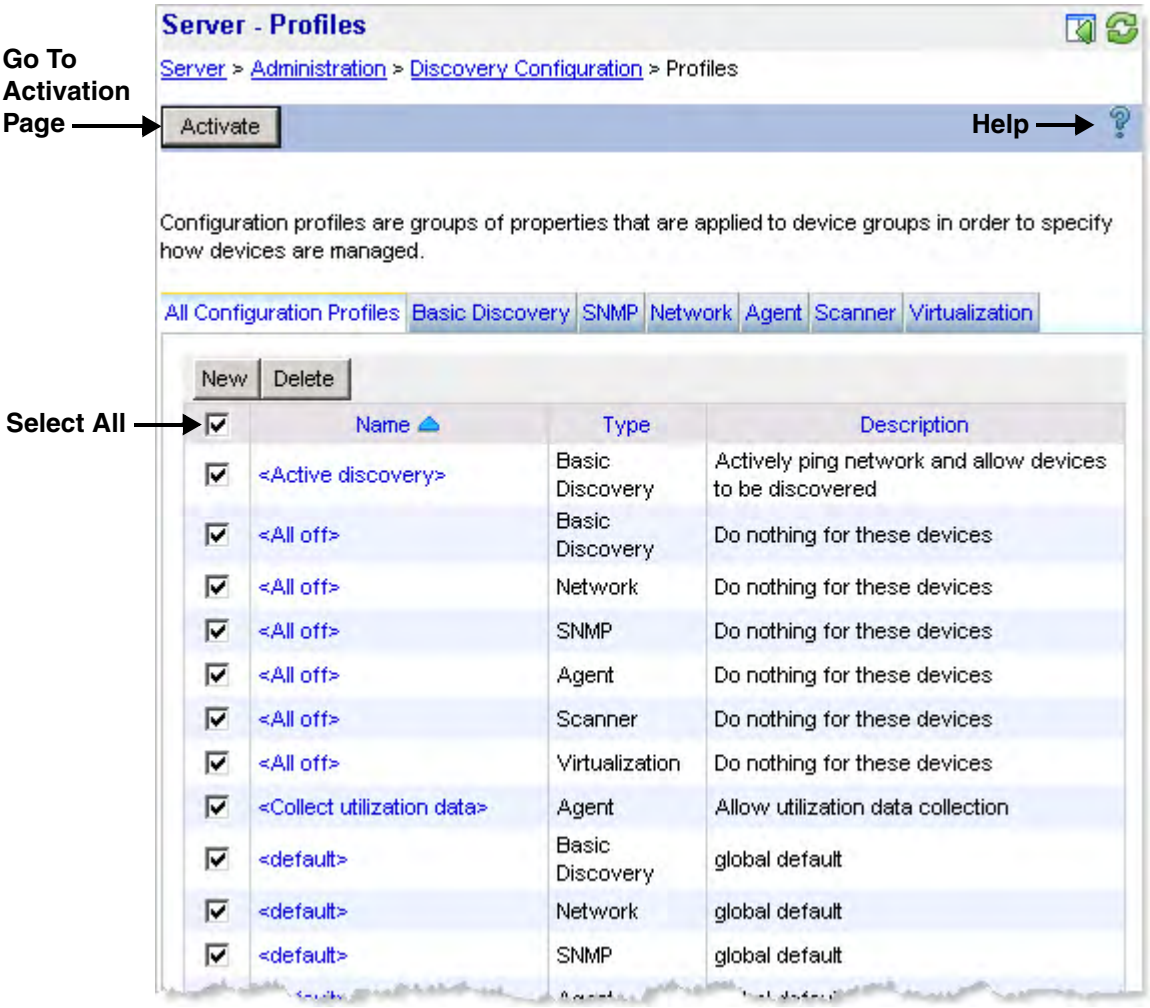
8 Configuring the Discovery Process

In this chapter, you will learn how to set up configuration profiles and device groups so that Enterprise Discovery can start discovering your network. The following topics are covered:

Enterprise Discovery uses the IPv4 network layer protocol. All IP address, range, and subnet fields referenced in this chapter are in IPv4 format.reprint.

Notation and Navigation

In the Enterprise Discovery user interface, the <item name> notation is used to indicate a system defined item. All the configuration profiles listed on the page shown here are system defined items. You cannot modify or delete system defined items, but you can view their properties.



The single check box located in the header row of certain data tables has the Select All function. When you select this box, all items in the table are then selected.

The Help icon located on the blue button bar at the top of each page provides context-sensitive help in a separate window.

The Activate button, as shown here, does not actually activate your changes. It simply opens the Activation page, where you can then preview and either activate or revert your changes.

Discovery Configuration Overview

Enterprise Discovery enables you to precisely define what devices in your network it will discover and how these devices will be managed. To do this, you must set up two things:

- **Configuration profiles** specify *how* network devices are discovered and managed by Enterprise Discovery.
- **Device groups** specify *what* devices are discovered and managed.

You establish device groups by creating one or more **conditions** that specify a collection of IP addresses, a particular type of device, or both. You then assign configuration profiles to a device group to specify how the devices in that device group should be treated.

Configuration Profiles

Configuration profiles are sets of attributes that define how a device is managed. Profiles are associated with device groups. There are six types of configuration profiles.

- Basic Discovery profiles specify how Enterprise Discovery finds devices to manage.
- SNMP profiles specify how Enterprise Discovery should access an SNMP-managed device in order to gather additional information, such as the type of device or its location. SNMP profiles also contain SNMP credentials.
- Network profiles specify additional information that can be gathered from devices as well instructions as to how to use this information.
- Agent profiles specify high-level agent deployment and communication preferences.
- Scanner profiles specify when devices should be scanned, how they should be scanned, and how the data should be returned to Enterprise Discovery.
- Virtualization profiles specify how often and when to discover virtual devices such as VMware virtual machines. VMware credentials are also specified in Virtualization profiles.

When you create a device group, you select one profile of each pertinent type to associate with that device group. The default selection for each type is the system defined <default> profile for that type. If you want to use customized profiles, you must first create those profiles before you can assign them to device groups.

Every configuration profile has a unique name. It can also have a more detailed description. The name and description are listed in the tables on each tab on the Discovery Configuration > Profiles page. Both system defined and customized profiles are included in the tables.

The Enterprise Discovery licensing model controls which configuration profiles are available. For example, you can only create, modify, or delete Agent and Scanner profiles when the Inventory license is present.

Purpose of Configuration Profiles

Configuration profiles control the kind of information that Enterprise Discover can obtain from your network devices. You can use profiles to determine where Enterprise Discovery will distribute Agents, run Scanners, and precisely how it will access your network devices. By setting up different configuration profiles, you can instruct Enterprise Discovery to treat device groups differently. For example, you may want <Active discovery> for one IP range, and <All off> for another.

System Defined Profiles

System defined profiles are identified by the <profileName> notation in the Enterprise Discovery UI. These profiles support common discovery behaviors. You can view the settings specified by any system defined profile, but you cannot modify or delete a system defined profile. You can, however, duplicate a system defined profile—or any existing profile—and use it as a starting point to create a new profile.

See System Defined Configuration Profiles on page 115 for descriptions of all system defined profiles.

Default Configuration Profiles

Default configuration profiles are provided with your Enterprise Discovery software. All default profiles have the same name: <default>. When you create a new device group, the default profile for each profile type applies unless you explicitly assign a different profile to the group.

Many of the values in the default profiles are either “Off” or “None.” If you do not assign more powerful profiles to a device group, it is likely that devices in that group will not be discovered.

Types of Configuration Profiles

Each of the six types of configuration profiles specifies a unique set of attributes, as described in the following tables. The tables show two types of default values for each attribute.

The Default Value for New Profiles column shows the initial setting for each attribute. You will see these values when you create a new configuration profile. You can modify these settings as you create the profile.

The <default> Profile Value column shows the setting for the system defined <default> profile. When you create a new device group, the <default> profile for each available profile type is selected. You can either accept the <default> profile or assign a different profile for each profile type.

Basic Discovery Profiles

Basic Discovery profiles specify how devices within a particular device group are discovered.

Basic Discovery Option	**Default Value for New Profiles**	**<default> Profile Value**	**Description**
Allow the group to manage devices	On	Off	Determines whether Enterprise Discovery adds devices that it discovers within this device group to the database.

Basic Discovery Option	Default Value for New Profiles	<default> Profile Value	Description
Actively ping devices	On	Off	Determines whether devices in this device group are periodically pinged for discovery.
Allow ICMP and SNMP	On	Off	If **Off**, the network model is filtered. If the device is already in the database, Enterprise Discovery will still poll and ping the device. Devices can still be scanned and included in the database.
Allow IP addresses	On	On	Set to **Off** when multiple servers have the same IP address, and you do not want to see this address. This is useful, for example, when you are using Network Address Translation (NAT). Set to **On** when you want to allow the duplicate IP addresses to be included. If all the IP addresses of a device have this property enabled, the network model will be filtered.

SNMP Profiles

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 profiles, including both community strings (for SNMPv1 and SNMPv2) and users (for SNMPv3).

SNMP Option	Default Value for New Profiles	<default> Profile Value	Description
Community String			For SNMPv1/2
Authorization Type	Read		For SNMPv1/2/3: Read, Write, or both
User Name			For SNMPv3
Authentication Algorithm	None		For SNMPv3: None, SHA, or MD5
Authentication Password			For SNMPv3: Only available if an Authentication Algorithm is selected; must be at least 8 characters.
Encryption Algorithm	None		For SNMPv3: None, DES, or AES
Encryption Password			For SNMPv3: Only available if an Encryption Algorithm is selected; must be at least 8 characters.

You can use the **Move Up** and **Move Down** arrows on the SNMPv1/2 or SNMPv3 tabs to specify the order (priority) of the SNMP credentials. For more efficient discovery, the most frequently used strings or user names should appear at the top of the list.

For SNMPv3, you can have authentication with or without encryption, but in order to specify encryption, you must enable authentication.

The <global> system defined SNMP profile has one Read community string (*public*) and no SNMPv3 users. If you use this profile, Enterprise Discovery will attempt to read the MIB of all devices in the device group using only *public*.

Network Profiles

Network profiles specify what sources of information in addition to the MIB are queried during discovery.

Network Option	New Profile Default Value	<default> Profile Value	Description
Query devices for their NetBIOS name	On	Off	The NetBIOS names are the computer user names.
Query devices for resource/ environment management	On	Off	Get disk, CPU, and memory information from servers, printers or UPSs.
Force ARP table to be read	Off	Off	Enables Enterprise Discovery to look for information about unmanaged devices in the ARP caches of other devices. This is useful for servers providing Dynamic Host Configuration Protocol (DHCP) services, or for any other device (except routers) with a large ARP cache.
Accumulate IP Addresses	Off	Off	Accumulate IP addresses instead of replacing them. This is for routers that do not have SNMP management enabled.

Network Option	New Profile Default Value	<default> Profile Value	Description
Device modeler interval	2 days	2 days	Determines how frequently Enterprise Discovery updates the devices in the network.

Agent Profiles

Agent profiles tell Enterprise Discovery how to deploy Agents to devices in the network and how to collect information from the Agents.

Agent Option	New Profile Default Value	<default> Profile Value	Description
Allow agent communication	On	Off	This option must be turned on in order for any of the other options to work.
Limit bandwidth for data transfers	Off	Off	The maximum bandwidth that will be used when communicating with a single device for sending the Scanner or retrieving the scan file. If you do not select this option—or if you select it and specify zero KB—this means that bandwidth is unlimited.

Agent Option	New Profile Default Value	<default> Profile Value	Description
Collect Utilization Data	Off	Off	Determines whether Enterprise Discovery collects software utilization data from the Agent. A software utilization plug-in license is required to collect this data.
Allow agent upgrade	On	On	Select **On** if you want to upgrade your Agents automatically. Select **Off** if you do not want the Agent upgraded automatically.
Agent automatic upgrade schedule	<All the time>	<All the time>	These are the same schedules used for Scanner distribution. You can create your own at **Administration > Schedule Management**. This option is only meaningful if **Allow agent upgrade** is on.
Agent deployment	No action	No action	Select **No action** if you want no action at all. Select **Deploy** if you want to automatically deploy Agents to the devices in this device group. Select **Uninstall** if you want to automatically uninstall the Agents from the devices in this device group.

Scanner Profiles

Scanner profiles determine if and how often scanners run on devices in the network, how often the scanners are upgraded, and how often the scanner data is sent back to the server to be processed.

Scanner Option	New Profile Default Value	<default> Profile Value	Description
Deploy/upgrade scanners using this schedule	<All the time>	<default>	Determines when scanners are deployed to devices that do not yet have them or upgraded on devices that do. The choices are defined on the Administration > Schedule Management page.
Run the scanner using this schedule	<All the time>	<default>	When scanners should be run on devices within this device group.
Download the scan file using this schedule	<All the time>	<default>	When the scan file results should be sent back to the server.
Automatic workflow interval	4 weeks	None	How often scanners are automatically deployed.
Allow scanners to be upgraded	On	On	This must be set to On for the scanners to be automatically upgraded from the server.
Scan method	Use one method: <default>	Use one method: <default>	You can specify a specific scanning method for each supported operating system, or you can use one method for all operating systems.

Virtualization Profiles

A virtualization profile enables you to specify two things: (1) VMware credentials, and (2) how often and when the discovery process for virtual devices is initiated.

Virtualization Options	**New Profile Default Value**	**<default> Profile Value**	**Description**
VMware discovery interval	None	None	How often devices that support VMware technology are polled.
Discover VMware using this schedule	<All the time>	<default>	When the discovery process for virtual devices is initiated.
VMware credentials			User name, password, and password hint for VMware virtual machines.

Device Groups

Device groups determine what devices are discovered by Enterprise Discovery. Device groups are defined by IP addresses, device types, or both. Configuration profiles are assigned to device groups. These profiles specify how the devices in the group are managed by Enterprise Discovery.

You can create up to 2000[1] device groups, although it is unlikely that you will need that many.

Conditions

Conditions are parameters, such as an IP address range or device type, that define a potential set of devices. For example, if a condition specifies a range of 20 IP addresses, Enterprise Discovery will attempt to find any devices that exist within that range. When a device is found, it is added to the device group so that it can be managed.

You can define multiple conditions to increase or decrease the number of devices managed by a device group. When a device group specifies multiple conditions, the resulting set of managed devices includes only those devices that match all of the conditions for that device group. Conditions are evaluated in the following way:

- Within a specific condition type (IP address or device type), a logical OR is used.
- Between condition types, a logical AND is used.

For example, say a device group is defined by the following conditions:

– IP addresses in 100.100.100.* or 200.*.*.*

– Windows XP servers, Windows 2003 servers, or Windows Vista servers

The following devices *would* be included in this device group:

Windows XP server with IP address 200.12.45.21
Windows 2003 server with IP address 100.100.100.243

The following devices *would not* be included in this device group:

Windows XP server with IP address 201.156.121.14.
Linux server with any IP address.

1.This upper bound means 2000 single condition device groups. The maximum number of device groups decreases as the number of conditions per device group increases.

Note that if you specify an IP address condition and a device type condition that are mutually exclusive, that device group will contain no devices.

How Device Groups are Defined

IP-Only

IP-only device groups are tied to specific address locations in a network and contain at least one condition that specifies a single IP address, a set of IP addresses that match a wildcard string, an IP address range, or a subnet. IP-only device groups do not have any device type conditions. Because devices within an IP-only device group can be found by accessing an IP address directly, all configuration profile types can be assigned to IP-only device groups.

Device Type

Device type groups contain device type conditions, such as Windows workstations or enterprise routers. They can also contain IP address conditions. Because a device must already be discovered before Enterprise Discovery can identify its device type, however, you cannot use device type groups to discover devices. For this reason, Basic Discovery and SNMP configuration profiles cannot be assigned to device type groups.

If you add a device type condition to an IP-only device group, that device group can no longer be used to discover devices.

Using Device Groups

A convenient way to use Enterprise Discovery is to first use IP-only device groups to discover all the devices on your network. Then, after the devices have been discovered, use device type groups to manage your Agents and Scanners.

Assigning Configuration Profiles to Device Groups

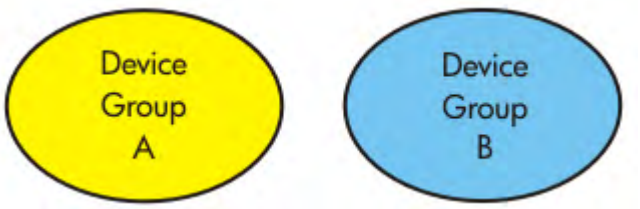
There are multiple ways to assign configuration profiles to device groups. When you initially create a device group, the system defined <default> profile is selected for each applicable configuration profile type.

You can change the configuration profile assignments for a single device group, or you can change the assignments for multiple device groups by using a “batch” assignment process.

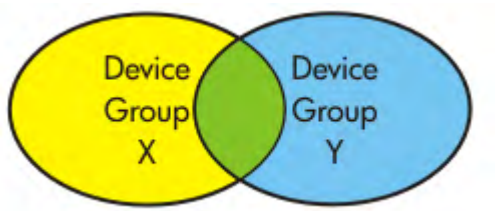
You can only assign Basic Discovery and SNMP configuration profiles to IP-only device groups. Device type device groups do not have Basic Discovery and SNMP profiles. A device within a device type group can only acquire these properties if this device also belongs to an IP-only group. Devices that do not belong to at lease one IP-only group cannot be discovered.

Potential Conflicts and Priorities

A single device group that does not intersect with any other groups is easy to understand. Any device that Enterprise Discovery finds within that device group is managed using the configuration profiles associated with that device group.



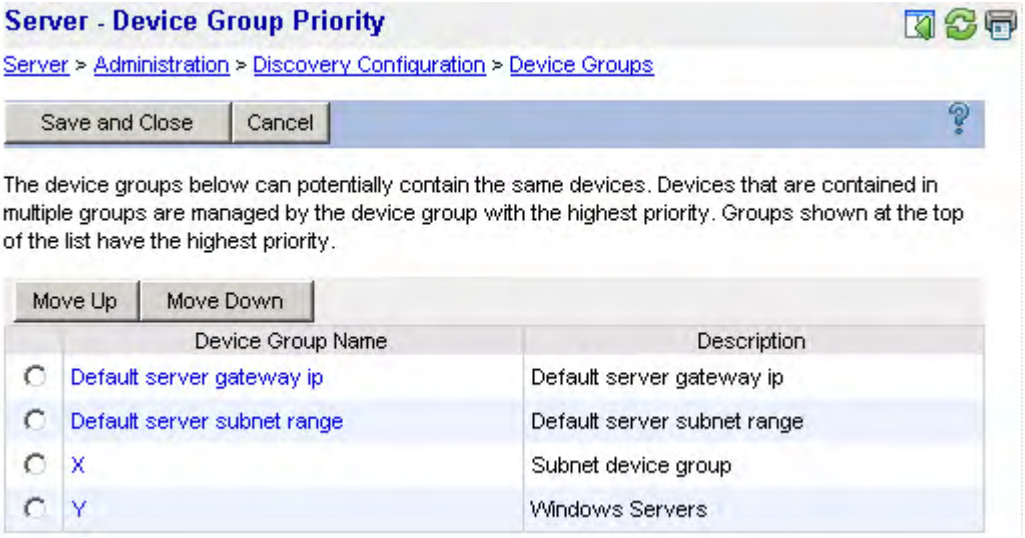
When two or more device groups intersect (contain a common device), the priority of the device groups determines which configuration profiles are applied. In the following example, device group X (yellow) and device group Y (blue) each have conditions that result in at least one device being part of both groups (green).



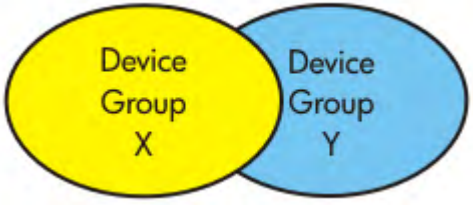
Say that device group X contains devices in a certain subnet, and device group Y contains devices of a particular type—say, Windows servers. In this case, any Windows servers whose IP addresses are in this subnet belong to both group X and group Y.

The problem with this is that Enterprise Discovery must be told whether to use the configuration profiles associated with group X or the configuration profiles with group Y to manage the behavior of any shared devices.

You can provide this information to Enterprise Discovery by prioritizing your device groups. Here, group X has a higher priority than group Y:



Because the priority of device group X is higher than that of device group Y, Enterprise Discovery manages all shared devices using configuration profiles defined in Device Group X.



In this example, the following statements are true:

- Any device in X that is not also in Y is managed by X.
- Any device in Y that is not also in X is managed by Y.
- Any device that is common to both X and Y is managed by X.

Configuration Import and Export

You can export your discovery configuration data to a tab-separated value file (TSV) file as a way of keeping an external record of your configuration information. There are certain circumstances in which you might want to import a complete set of discovery configuration data from a file. If you decide to install Enterprise Discovery on a new server, for example, you can import your configuration data from an existing server.

For security reasons, passwords are not exported.

It is possible to export your discovery configuration data to a TSV file, modify the TSV file in a text editor, and import the modified data back into Enterprise Discovery. This is a potentially dangerous process, however. When you import discovery configuration data from a file and then activate your changes, any existing configuration data is over-written. There is no “undo” option available after the activation process is completed. A mistake could result in a loss of data.

Do not attempt to modify and then import configuration data from a file unless you are an experienced Enterprise Discovery administrator and you fully understand the implications of this operation.

Activation

When you click **Save and Close** after you create or modify a device group or configuration profile, you are actually saving your changes in a working copy of the configuration database. To commit your changes to their permanent location in the Enterprise Discovery database and have them take effect, you must activate them.

Pending Changes

Enterprise Discovery does not immediately commit your configuration changes to the database, because there may be conflicts or other consequences that you did not anticipate. The impact of your pending changes is summarized on the tabs of the Activation page.

The Summary tab contains the total number of device groups and configuration profiles that will be affected as well as the total number of devices that will be managed differently as a result of your changes. It flags

any areas of conflict, which are described in greater detail on the IP Range Conflicts and Device Type Conflicts tabs. The Summary tab also shows you the estimated time it will take to ping all the IP addresses within your device groups that are configured to allow ICMP ping.

The Devices Removed tab shows you a list of devices that will no longer belong to a device group after your changes are activated. These devices cannot be discovered or managed after they are removed.

The Activation page tabs provide detailed information about the nature and scope of your pending changes. If you have made a large number of changes, be sure to examine each tab carefully before you activate your changes.

Result of Activation

After you click the Activate Changes button, your configuration changes are stored in the Enterprise Discovery database, and they take effect. The Activation page now shows no pending changes.

If you decide that you do not want to make your changes permanent, you can click the Revert Changes button. All pending configuration changes will be erased. The working copy of your discovery configuration then matches the currently active configuration.

How Activation Works

Activation is an “all or nothing” operation. You must either activate or revert all pending changes. You cannot choose to activate or revert specific pending changes.

When you review your pending changes using the tabs on the Activation page, you may discover that you have inadvertently created a consequence that you do not want. For example, you may have deleted a configuration profile or device group that you want to keep. If this happens, you must revert all the pending changes.

For this reason, it is recommended that you make small configuration changes so that you never have an extensive list of pending changes. This way, if you must revert a change, you will not sacrifice a large amount of work. This approach also minimizes the likelihood that unintended consequences will occur as a result of your changes.

Setting Up Discovery Configuration Profiles

This section provides detailed instructions for creating, modifying, viewing, and deleting configuration profiles.For an overview of configuration profiles, see Configuration Profiles on page 94.

View a List of Existing Profiles

There are two methods that you can use to view discovery configuration data. If you want to view configuration data that has already been activated, you can use the Current Settings page. See Viewing Your Current Discovery Configuration Settings on page 129 for more information.

If you want to view both activated and pending configuration information, you must use the Administration > Discovery Configuration page, which shows the working copy of the configuration data. This method will be detailed here.

When you view the list of configuration profiles using the Discovery Configuration page, there is no indication of what has been activated and what is pending activation.

To view your configuration profiles:

1. Click **Administration > Discovery Configuration.**
2. Click **Configuration Profiles**.

The All Configuration Profiles tab shows a comprehensive list of all your configuration profiles, including system defined profiles and customized profiles that you have created. This list is initially sorted by profile name. Click any column header to change the sort parameter or toggle the sort order. The blue triangle ( ) indicates the sort order.

The subsequent tabs show the profiles of each type. Each tab lists all the profiles that have been defined and saved for that profile type, including those profiles that have not yet been activated.

Create a Profile

You can create a customized configuration profile that you can then assign to one or more device groups.

To create a configuration profile:

1. Click **Administration > Discovery Configuration.**
2. Click **Configuration Profiles**.
3. Click the tab for the type of profile that you want to create.
4. Click **New**.
5. Enter a unique **Name** for your new profile.
6. *Optional:* Enter a more detailed **Description** of the profile.
7. Specify the settings for your profile. These settings will vary depending on the type of profile. For detailed information about each setting, see the online help for that profile type or Types of Configuration Profiles on page 96.
8. After you finish customizing the settings, click **Save and Close**.

Remember to activate your changes to have them take effect.

Modify a Profile

You can modify any configuration profile that is not a system defined profile. You cannot modify the name of a profile, but you can modify any other setting.

To modify a configuration profile:

1. Click **Administration > Discovery Configuration.**
2. Click **Configuration Profiles**.
3. In the list of profiles, click the name of the profile that you want to modify.

   The settings that you can modify will vary depending on the type of profile. For detailed information about each setting, see the online help for that profile type or Types of Configuration Profiles on page 96.
4. After you finish modifying the profile, click **Save and Close**.

Remember to activate your changes to have them take effect.

Duplicate a Profile

You can make a copy of any configuration profile. This is particularly useful if you want to copy the settings in a system defined profile and then modify the duplicate.

To duplicate a configuration profile:

1. Click **Administration > Discovery Configuration.**
2. Click **Configuration Profiles**.
3. Click the tab for the type of profile that you want to duplicate.
4. Select the check box for the specific profile that you want to duplicate. Note that only one profile can be duplicated at a time.
5. Click **Duplicate**.
6. Modify any settings that you want to change.

   The settings will vary depending on the type of profile. For detailed information about each setting, see the online help for that profile type or Types of Configuration Profiles on page 96.
7. After you finish modifying the profile, click **Save and Close**.

Remember to activate your changes to have them take effect.

Determine Device Groups Associated with Each Profile

After you create device groups and associate profiles with them, you can view a list of profiles that are associated with each profile.

To view a list of device groups associated with each profile:

1. Click **Administration > Discovery Configuration.**
2. Click **Configuration Profiles**.
3. Click the name of the profile you want to work with.
4. Click the **Associated Groups** tab.

Any device group that is assigned the <default> profile for a particular profile type will appear in the Associated Groups list for that <default> profile.

Delete a Profile

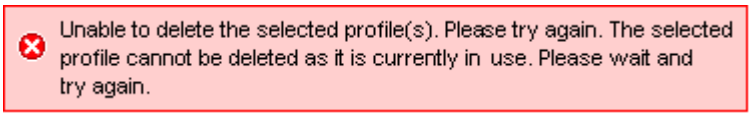
You can delete any configuration profile that is not a system defined profile. Use caution when deleting profiles, however. Be sure to carefully review the implications of your pending changes on the Activation page before permanently deleting a profile.

If a profile is assigned to a device group, you cannot delete that profile. You must first break the association by selecting a different profile of this type for that device group. You will then be able to delete the original profile.

To delete a configuration profile:

1. Click **Administration > Discovery Configuration.**
2. Click **Configuration Profiles**.
3. In the list of profiles, select the check box for the profile (or profiles) that you want to delete.
4. Click **Delete**.
5. Review the list of proposed deletions. If you selected any system defined profiles in step 3, these profiles will not appear in the list.
6. If the list of profiles to be deleted matches what you want to delete, click **Continue**. One of the following two things happens next:

- If none of the profiles in the list are assigned to device groups, you return to the main Configuration Profiles page.
- If one or more of the profiles is assigned to a device group, the following error message appears:



In this case, you must determine which profile (or profiles) in your list is attached to a device group and assign a different profile to that device group. Then, you can attempt the delete operation again.

Remember to activate your changes to have them take effect.

System Defined Configuration Profiles

Some of the system defined configuration profiles 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.

The profiles in the following tables are listed in order from least expensive to most expensive in terms of network traffic. In some cases, multiple profiles have the same properties.

Basic Discovery Profiles

See Basic Discovery Profiles on page 115 for information about Basic Discovery profile options.

Profile	Purpose
<All off>	The least active of the Basic Discovery profiles. For use when it's easier to turn a device group off than to delete it.
<default>, <global>	Almost completely set to off, but do allow IP addresses.
<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.)

Profile	Purpose
< Restrict to scanned-only devices>	For device groups where there is only information from scan files.
<Active discovery>	The most active of the Basic Discovery profiles. Ping, poll, table read. Find devices and information about them to add to database.

SNMP Profiles

See SNMP Profiles on page 116 for information about SNMP profile options.

Profile	Purpose
<All off>, <default>, <No SNMP>	No SNMP credentials are provided.
<Global>	Only the “public” community string SNMPv1/2 is provided. Enterprise Discovery will attempt to read the MIB of all devices in the device group using only “public.”

Network Profiles

See Network Profiles on page 117 for information about Network profile options.

Profile	Purpose
<default>, <All off>, <Global>	The least active of the Network profiles. No options are selected.
<Resource/environment manage>	The most active of the Network profiles. Provides disk, CPU, and memory information from servers, printers or UPSs.
<Unmanaged router>	In this profile, **Accumulate IP addresses** is set to “on”. For routers that do not have SNMP management enabled.
<DHCP Server>	This profile 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.

Agent Profiles

See Agent Profiles on page 118 for information about Agent profile options.

Profile	Purpose
<All off>	No Agent communication is allowed.
<default>	Allows the Agent to be upgraded using the <All the time> system defined schedule.
<Deploy agent>, <Global>	Allows Agent communication, and allows the Agent to be upgraded using the <All the time> system defined schedule.
<Collect utilization data>	Allows the Agent to be upgraded using the <All the time> system defined schedule, and allows software utilization data to be collected from servers and workstations in this device group.

Scanner Profiles

See Scanner Profiles on page 118 for information about Scanner profile options.

Profile	Purpose
<All off>, <default>	Do nothing: Do not deploy, upgrade, download, or run scanners, and do not upgrade the Agent.
<Global>	Upgrade or deploy the scanners (and the Agent, if necessary) every 4 weeks.

Profile	Purpose
<Hardware only>	Use the system defined <hwonly> scan method for all operating systems. Upgrade or deploy the scanners (and the Agent, if necessary) every 4 weeks.
<Fast software>	Use the system defined <fastsw> scan method for all operating systems. Upgrade or deploy the scanners (and the Agent, if necessary) every 4 weeks.

Virtualization Profiles

See Virtualization Profiles on page 119 for information about Virtualization profile options.

Profile	Purpose
<All off>, <default>, <Global>	Do not discover virtual devices.

Setting Up Device Groups

This section provides detailed instructions for creating, modifying, viewing, and deleting device groups. For an overview of device groups, see Device Groups on page 104.

View a List of Existing Device Groups

To view your device groups:

1. Click **Administration > Discovery Configuration.**
2. Click **Device Groups**.

The Device Groups page shows a comprehensive list of all your device groups. This list is initially sorted by device group name. Click any column header to change the sort parameter or toggle the sort order. The blue triangle ( ) indicates the sort order.

The list contains all the device groups that have been defined and saved, including those groups that have not yet been activated.

If you want to see the groups listed in priority order, click the **Assign Priority** tab.

Create a Device Group

The particular settings that you specify when you create a device group depend on whether the device group is an IP address group or a device type group. The following procedure provides instructions for either type of device group.

To create a device group:

1. Click **Administration > Discovery Configuration.**
2. Click **Device Groups**.
3. Click **New.**
4. Provide a unique **Device group name**.
5. *Optional:* Provide a more detailed **Description** of the device group.

6 From the **Condition Type** list, select either **IP Address** or **Device Type**.

7 If you selected **IP Address** in step 6, follow these steps:

   a From the **IP Type** list, select the IP format that you want to use: Single IP, Wildcard IP, IP Range, or Subnet.

   b In the **IP Address** box (or boxes), specify the IP information. Click the **Valid IP formats** link for additional tips about how to specify this.

   If you selected **Device Type** in step 6, select one or more device types from the **Device Types** list. You can select more than one by using **CTRL+Click** or **SHIFT+Click**.

8 Click **Continue**.

9 To include additional conditions, follow these steps:

   a Click **New**.

   b Repeat steps 6 and 7.

   c Click **Add**.

   d When you are finished adding conditions, click **OK**.

10 When you have finished creating the device group, click **Save and Close**.

Remember to activate your changes to have them take effect.

Modify a Device Group

You can modify any device group. You cannot modify the name of the device group, but you can modify any other setting.

To modify a device group:

1 Click **Administration > Discovery Configuration.**

2 Click **Device Groups**.

3 In the list of device groups, click the name of the device group that you want to modify.

4 After you finish modifying the device group, click **Save and Close**.

Remember to activate your changes to have them take effect.

Assign Configuration Profiles to a Single Device Group

You can either assign configuration profiles to one device group at a time, or you can assign profiles to multiple device groups all at once. This procedure shows you how to work with a single device group.

To assign configuration profiles to a single device group:

1. Click **Administration > Discovery Configuration > Device Groups**.
2. Click the name of an individual device group.
3. Click the **Assign Profiles** tab.
4. For each profile type that you want to assign, select the check box to the left of that profile type, and choose a profile from the list.
5. When you are finished selecting profiles, click **Save and Close**.

Remember to activate your changes to have them take effect.

Assign Configuration Profiles to Multiple Device Groups at One Time

You can assign configuration profiles to multiple device groups at one time by using a “batch” process. The following procedure assigns the same configuration profiles to all selected device groups.

To assign configuration profiles to multiple device groups:

1. Click **Administration > Discovery Configuration > Device Groups**.
2. Select the check box to the left of each device group that you want to work with.
3. Click the **Assign Profiles** tab.
4. For each profile type that you want to assign, select the check box to the left of that profile type, and choose a profile from the list.
5. When you are finished selecting profiles, click **Save and Close**.

Remember to activate your changes to have them take effect.

Change the Priority of a Device Group

You can change the priority of any device group relative to the other device groups.

To change the relative priority of a device group:

1. Click **Administration > Discovery Configuration.**
2. Click **Device Groups**.
3. Click the **Assign Priority** tab.
4. Select the check box for the device group whose priority you want to change.
5. Click **Move Up** to increase its relative priority; click **Move Down** to decrease it.
6. Repeat steps 4 and 5 until the device groups are listed in the order that you want.
7. Click **Save and Close**.

Remember to activate your changes to have them take effect.

Duplicate a Device Group

You can make a copy of any device group. This is particularly useful if you want to make a small refinement in the settings without starting from scratch.

To duplicate a device group:

1. Click **Administration > Discovery Configuration.**
2. Click **Device Groups**.
3. Select the check box for the specific device group that you want to duplicate.
4. Click **Duplicate**.

5 Modify any settings that you want to change. To modify the properties of a specific condition, click the name of that condition. To delete a condition, select the check box for that condition, and click **Delete**.

6 After you finish modifying the device group, click **Save and Close**.

Remember to activate your changes to have them take effect.

Delete a Device Group

You can delete any device group. Before activating your changes, be sure to review the information on the Activation page to be sure that the consequences of the deletion match your expectations.

To delete a device group:

1 Click **Administration > Discovery Configuration.**

2 Click **Device Groups**.

3 In the list of device groups, select the check box to the left of each device group that you want to delete.

4 Click **Delete**.

5 Review the list of proposed deletions.

6 If the list of device groups to be deleted matches what you want to delete, click **Continue**. Otherwise, click **Cancel**. In either case, you return to the main Device Groups page.

Remember to activate your changes to have them take effect.

Activating Your Changes

For an overview of the activation process, see Activation on page 108.

Preview the Effect of Pending Changes

The Activation page enables you to review all the network configuration changes you have proposed before actually making those changes take effect.

To preview pending discovery configuration changes:

Click **Discovery Configuration > Activate**.

Activate All Pending Changes

When you have completed all the changes you wanted to make, you can activate those changes, and they will take effect.

To activate configuration changes:

1. Click **Discovery Configuration > Activate**.
2. Review the information on each of the tabs on the Activation page.
3. To apply your changes, click **Activate Changes**.

This is an “all or nothing” operation. You cannot choose which changes to activate; all pending changes in the list will be activated.

Revert All Pending Changes

If you decide that you do not want to activate the list of pending changes, you can do one or two things. You can go back to the Configuration Profiles or Device Groups pages and make changes there, or you can revert all the pending changes at once.

To revert pending configuration changes:

1. Click **Discovery Configuration > Activate**.

2 To discard you changes, click **Revert Changes**.

This is an “all or nothing” operation. You cannot choose which changes to revert; all pending changes in the list will be reverted.

Importing and Exporting Discovery Configuration Information

You can export your discovery configuration information to a tab-separated value (TSV) file. You can also import discovery configuration from a TSV file. This is useful, for example, if you are setting up a new Enterprise Discovery server and you want to use existing discovery configuration information from another server.

When you import discovery configuration from a file, the imported data overwrites any existing discovery configuration data.

For security reasons, passwords are not exported.

Export Your Configuration Information to a TSV File

You can export your discovery configuration data to a (TSV) file as a way of keeping an external record of your configuration information.

To export your configuration data:

1. Click **Administration > Discovery configuration**.
2. Click **Import/Export**.
3. Click the **Export** button.
4. Specify the location and name for the TSV file.

   Depending on how you browser is configured, you may not have the opportunity to specify the name and location for this file. If your browser is set up to store all downloaded files in a single folder, for example, the `ConfigImportExport.tsv` file will be stored there.
5. Save the file.

Import Configuration Information from a TSV File

There are certain circumstances in which you might want to import a complete set of discovery configuration data from a file.

To import your configuration data:

1. Click **Administration > Discovery configuration**.
2. Click **Import/Export**.
3. Click **Browse**, and specify the file to import.
4. Click **Import**.

It is possible to export your discovery configuration data to a TSV file, modify the TSV file in a text editor, and import the modified data back into Enterprise Discovery. This is a potentially dangerous process, however. When you import discovery configuration data from a file and then activate your changes, any existing configuration data is over-written. There is no "undo" option available after the activation process is completed. A mistake could result in a loss of data.

Do not attempt to modify and then import configuration data from a file unless you are an experienced Enterprise Discovery administrator and you fully understand the implications of this operation.

Viewing Your Current Discovery Configuration Settings

You can view all discovery configuration settings that have been activated in table format by selecting the following item in the left navigation tree:

Status > Current Settings > Discovery configuration

This page contains a series of tables that reflect the settings that were most recently configured on the Administration > Discovery Configuration page. Only changes that have been activated are reflected in these tables. Refer to Activating Your Changes on page 125 for more information.

Discovery Configuration Table

The information in the table is organized by device group. The groups are listed in priority order. For each device group, the following items are displayed:

Column	Information Displayed
Name	The name associated with this device group. This is specified when the device group is created.
Description	A description that is specified when the device group is created. You can modify the description at any time.
Profiles	A link to detailed information about each configuration profile associated with this device group. This link leads to a specific profile table displayed further down on the same UI page. There are six profile columns: Basic Discovery, SNMP, Network, Agent, Scanner, and Virtualization. If a particular profile type does not apply to this device group, the column is blank.
Conditions	A list of the device types, IP ranges, or both that define this device group.

Profile Tables

The next six tables on this page show you the detailed settings for each configuration profile that has been established. Some of these profiles are provided with Enterprise Discovery, and others have been created by your administrator.

Basic Discovery Profiles

This table corresponds to the Basic Discovery column in the Discovery Configuration table above. It shows you the values of the following settings for each profile listed:

- Allow the group to manage devices
- Actively ping devices
- Allow ICMP and SNMP
- Allow IP addresses

SNMP Profiles

This table corresponds to the SNMP column in the Discovery Configuration table above. It shows you the values of the following SNMP credentials for each profile listed:

- Authorization type
- Version
- Community string / User name
- Authentication Algorithm
- Authentication Password
- Encryption Algorithm
- Encryption Password

This information is only visible if your account type is `admin` or `itmanager`.

Network Profiles

This table corresponds to the Network column in the Discovery Configuration table above. It shows you the values of the following settings for each profile listed:

- Query devices for their NetBIOS name
- Query devices for resource/environment management
- Force ARP table to be read
- Accumulate IP addresses
- Device modeler interval

Agent Profiles

This table corresponds to the Agent column in the Discovery Configuration table above. It shows you the values of the following settings for each profile listed:

- Allow agent communication
- Limit bandwidth for data transfers
- Collect utilization data
- Allow agent upgrade
- Agent automatic upgrade schedule
- Agent deployment

Scanner Profiles

This table corresponds to the Scanner column in the Discovery Configuration table above. It shows you the values of the following settings for each profile listed:

- Deploy/upgrade scanners using this schedule
- Run the scanner using this schedule
- Download the scan file using this schedule
- Automatic workflow interval
- Allow scanners to be upgraded

- Win32 scanner
- HP-UX scanner
- Linux scanner
- AIX scanner
- Solaris scanner
- MAC OS X scanner

Virtualization Profiles

This table corresponds to the Virtualization column in the Discovery Configuration table above. It shows you the values of the following settings for each profile listed:

- VMware discovery interval
- Discover VMware using this schedule
- VMware credentials

9 Migrating Configuration Information

Enterprise Discovery version 2.20 uses a new and more convenient method of configuring the discovery of network devices. If you are upgrading a version 2.1.x installation, this chapter pertains to you.

The following topics are covered:

Background and Purpose

In earlier versions of Enterprise Discovery, the only way to group network devices was by using IP ranges. Devices in the same IP range shared the same set of properties. This was inconvenient, because an IP range could encompass devices with completely different functionality. A network switch and a printer, for example, would be grouped together. In this chapter, we refer to this method of grouping as “old” network configuration format.

Beginning with Enterprise Discovery version 2.20, you can group devices based on either of the following criteria:

- Device type (for example, switches, routers, workstations, or printers)
- IP addresses (single addresses, ranges, subnets, or wildcard strings)

You must still set up device groups based on IP addresses to start the discovery process. New rules based on these new grouping choices apply, however, as soon as a device is discovered and categorized.

When you upgrade from Enterprise Discovery version 2.1.x to version 2.20 (or later), your network configuration information is automatically migrated from the old format to the new format. This is done automatically by the Configuration Migration utility. This utility converts each IP range configured in the old format into a device group with IP Range conditions in the new format.

How it Works

When you upgrade an installation from version 2.1.x to version 2.20 (or later), the old network configuration information is seamlessly migrated into the new format.

Enterprise Discovery version 2.20 includes a new network configuration user interface. In the future, only this new user interface will be available. For a short period of time, however, the old network configuration user interface will also be available.

While both the old and new configuration user interfaces are available, there are two ways that you can control how your data is migrated.

Preferred Method

The best way to work with your configuration data is to browse it using the new configuration user interface: **Administration > Discovery Configuration**.

You can view your configuration information without saving it. As soon as you save any configuration settings using the new user interface, however, the old IP range-based configuration disappears, and the old configuration user interface becomes unavailable.

Alternate Method

For the time being, you can still configure IP ranges by using the old network configuration user interface. If you save network configuration settings using the new user interface, however, the old interface becomes unavailable.

If you use the old network configuration user interface, each time that you click **Activate Changes**, the Configuration Migration utility runs in the background and migrates your changes to the new format. The utility preserves the data and IP range hierarchy. All properties that you set to "inherit" values are resolved from parent ranges in the IP range tree.

You can see the results of the configuration migration process in the following file:

`<DataDir>/log/migrateConfig.log`

where *<DataDir>* is the location of your Enterprise Discovery data files. This log file lists all property values for all IP ranges defined in the old format.

The old network configuration format and user interface is a transitional feature, and it will eventually be phased out. You are strongly encouraged to use the new network configuration user interface to configure device groups.

What Exactly Gets Migrated?

The Configuration Migration Utility converts each IP range configured in the old format into an IP-only type device group in the new format. Each new device group gets a name and description. In most cases, the name is based on the IP range and complies with the following format:

```
IP range 172.22.5.0 - 172.22.5.255 : device group 1
```

The description of the device group consists of the description of the property set associated with the old IP range followed by the range specification:

```
Discover network and apply resource management. IP range
172.22.5.0 - 172.22.5.255
```

There is a special case where multiple child IP ranges under the same parent range have exactly the same properties, and these properties originated from the same property set. In this case the Migration Utility consolidates the ranges into a single device group, and the name has this format:

```
Consolidated IP ranges : device group 7
```

The description is derived from the property set description followed by a list of all the IP ranges. It looks like this:

```
Actively ping network and allow devices to be discovered.
Consolidated IP ranges: 15.2.32.0 - 15.2.32.255, 15.2.112.0 -
15.2.112.255, 15.2.121.0 - 15.2.123.255, 15.2.128.0 -
15.2.135.255, 15.2.144.0 - 15.2.144.255, 15.2.149.0 -
15.2.150.255, 15.6.96.0 - 15.6.97.255
```

Each device group that the Migration Utility creates is linked to one or more of the following profiles:

Old Format Property Group	**New Format Configuration Profile**
Network property group	Basic Discovery and Network profiles
SNMP property group	SNMP profile
Scanner property group	Scanner profile
Agent property group	Agent profile

In each case, the profile name is derived from the old property group or set name followed by a sequence number. The profile description is the same as the old property group or set description (if available).

Configured property sets and groups that are not used in IP ranges do NOT get migrated.

Configuration Migration FAQ

- Does migration take place for new ED 2.20 or later installations?

  No.

- Can I use the old IP range based network configuration method after I install Enterprise Discovery version 2.20 (or later) on a particular machine for the first time (not an upgrade)?

  No.

- When does the migration occur?

  When you upgrade from Enterprise Discovery version 2.1.x to version 2.20 (or later) and each time you activate changes from the old network configuration after the upgrade.

- What does this migration accomplish—in other words, what exactly is migrated?

  IP-range properties configured in older versions of Enterprise Discovery are migrated to device groups with IP Range conditions.

- Is this migration mandatory or optional?

  It is necessary for Enterprise Discovery 2.20 (or later) to start the discovery process. It is accomplished automatically when you upgrade or when you make changes using the old network configuration user interface.

- When do I need to perform this migration—only on an upgrade, or also on a new installation?

  You do not need to do anything. Migration is performed automatically when you upgrade to Enterprise Discovery 2.20 or later or when you activate changes from the old network configuration user interface.

- What do I need to do, if anything, to initiate this migration?

  Nothing. The process is automatic.

- What do I need to know before initiating this migration—for example, should I backup any files?

  You do not need to know or do anything.

- How do I know that the migration was successful?

  You can verify changes in the new network configuration user interface (preferred method), or you can check the `migrateConfig.log` file located in the `<DataDir>/logs` directory.

- Can anything go wrong with the migration? If so, how do I troubleshoot the process and fix whatever is wrong?

  The process occurs seamlessly, and no verification is needed.

10 Setting Agent Deployment Accounts

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

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

Agent configuration profiles are only available if the Inventory license is present.

Introduction

Agent configuration profiles are groups of settings that can be applied to device groups (see Setting Up Device Groups on page 120). Depending on the devices included in different device groups, you may want Enterprise Discovery to treat each group differently.

Enterprise Discovery comes with many system defined Agent configuration profiles. You can add your own profiles if you want. However, in most cases, the system defined 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.

For new users of Enterprise Discovery, you can start with setting up Agent configuration profiles. These profiles 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 and Windows™ Vista operating systems.

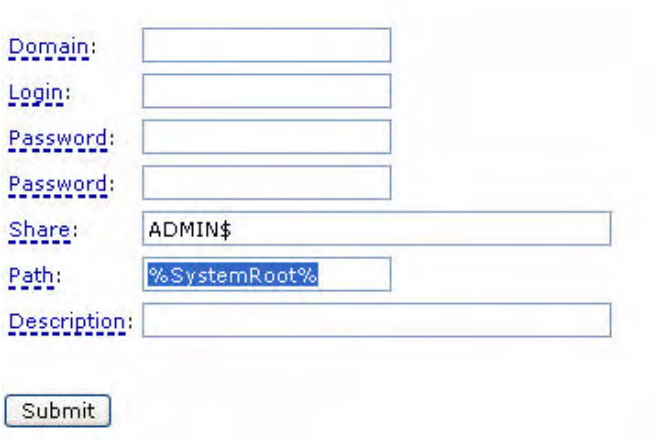
For it to work properly on Windows XP with Service Pack 2, one of the following should apply:

- 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**.



What Next?

To	Go to
Create Network, SNMP, and Scanner configuration profiles	Chapter 8, Configuring the Discovery Process
Create Scanner schedules	Chapter 11, Setting Up Scanner Schedules

To	Go to
Activate your configuration changes	Activating Your Changes on page 125
Apply configuration profiles to device groups	Chapter 8, Configuring the Discovery Process
Manually deploy agents (UNIX, Mac OS X, and Windows)	*Configuration and Customization Guide*

11 Setting Up Scanner Schedules

In this chapter, you will learn how to set up Scanner Schedules.

Introduction

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 configuration profiles, 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**.

- Choose when:
  - Scanners are deployed or upgraded
  - Scanners are run
  - Scan files are retrieved

What Next?

To	Go to
To create Network, SNMP, and Agent configuration profiles	Chapter 8, Configuring the Discovery Process
Apply configuration profiles to device groups	Chapter 8, Configuring the Discovery Process
To Activate your configuration changes	Chapter 12, Activating Your Configuration Changes
Configure more Scanner settings	*Configuration and Customization Guide*
Learn more about Scanners	*Reference Guide*

12 Activating Your Configuration Changes

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

Introduction

When you click **Save and Close** after you create or modify a device group or configuration profile, you are actually saving your changes in a working copy of the configuration database. To commit your changes to their permanent location in the Enterprise Discovery database and have them take effect, you must activate them. If you have made numerous changes, you should review the pending changes before you activate them.

For additional information about activation, see Activation on page 108.

Reviewing Your Changes

Enterprise Discovery does not immediately commit your discovery configuration changes to the database, because there may be conflicts or other consequences that you did not anticipate. The impact of your pending changes is summarized on the tabs of the Activation page. These tabs provide detailed information about the nature and scope of your pending changes.

To review pending changes:

Click **Administration** > **Discovery Configuration** > **Activate**

The following sections describe the information available for you to review on each of the seven tabs on the Activation page. If you decide to activate the pending changes, your configuration information will be updated in the Enterprise Discovery database. You can also revert the pending changes.

Summary Tab

The Summary tab contains the total number of device groups and configuration profiles that will be affected as well as the total number of devices that will be managed differently as a result of your changes. It flags any areas of conflict, which are described in greater detail on the IP Range Conflicts and Device Type Conflicts tabs. The Summary tab also shows you the estimated time it will take to ping all the IP addresses within your device groups that are configured to allow ICMP ping.

Device Group Changes

The Device Groups tab lists all device groups that will be affected if the pending changes are activated. There are three possible impacts: Add, Modify, or Delete.

When you review this tab, make sure that you do not inadvertently delete a device group that you want to keep.

Configuration Profile Changes

The Configuration Profiles tab lists all configuration profiles that will be affected if the pending changes are activated. There are three possible impacts: New, Modify, or Delete.

When you review this tab, make sure that you do not inadvertently delete a profile that you want to keep.

IP Range Conflicts

The IP Range Conflicts tab lists the IP ranges that will not be properly configured if the pending changes are activated. The Issue column describes the nature of the problem. The Resolution tells you how to address the problem. In some cases, Enterprise Discovery resolves the problem for you. In other cases, you must manually modify your configuration settings.

The IP Range column lists the number of ranges to which this issue applies. Click this number to see a list of the specific IP ranges that are affected.

The following issues are detected:

Issue	**Resolution**
"Allow Devices" property is off, but "Actively Ping" property is on.	"Actively Ping" property will be changed to off.
No read SNMP configuration defined.	Review SNMP configuration.
SNMP configuration contains "public" community string(s) which do not consist entirely of lowercase letters.	Review SNMP configuration.
SNMP configuration contains "private" string(s) which do not consist entirely of lowercase letters.	Review SNMP configuration.

Device Conflicts

The Device Conflicts tab lists the devices whose configuration will not work. In some cases, this is because certain settings are incompatible with each other. In other cases, the current license settings do not support certain settings - this can happen if you first establish your configuration settings and later change your Enterprise Discovery license type.

The following issues are detected:

Issue	Resolution
No license available for software utilization.	"Collect Utilization Data" property will be changed to off.
No license available for scanned devices.	"Scanner Frequency" property will be changed to 0.
"Allow Devices" property is off, but "NetBIOS Query" property is on.	"NetBIOS Query" property will be changed to off.
"Allow Devices" property is off, but "Resource/Environment Manage" property is on.	"Resource/Environment Manage" property will be changed to off.
"Allow Devices" property is off, but "Force ARP Table Read" property is on.	"Force ARP Table Read" property will be changed to off.
"Allow Devices" property is off, but "Accumulate IP Addresses" property is on.	"Accumulate IP Addresses" property will be changed to off.

Issue	Resolution
"Allow Devices" property is off, but "Allow Agent" property is on.	"Allow Agent" property will be changed to off.
"Allow Devices" property is off, but "Collect Utilization Data" property is on.	"Collect Utilization Data" property will be changed to off.
"Allow Agent" property is off, but "Scanner Frequency" property is set.	"Scanner Frequency" property will be changed to 0.

Devices Removed

The Devices Removed tab on the Activation page shows you a list of devices that will no longer belong to any device group after your changes are activated. As a consequence, all devices listed on this tab will no longer be managed by Enterprise Discovery. The automatic aging process will therefore take place and eventually discard all information that it has collected regarding these devices over time. It is very important to review the information on this tab before activating your changes. If you inadvertently remove devices, information about them will no longer be available in Enterprise Discovery.

Devices Managed Differently.

The Devices Managed Differently tab shows you a list of all devices whose configuration has been altered in any way. If a different configuration profile has been assigned to the device group that manages this device, the device appears in the list. If one of the settings in a configuration profile assigned to the device groups that manages this device changes, the device appears in the list. If the priority of the device groups changes and a device is now managed by a different device group, the device appears in the list.

A Device will appear on that list in any of the following scenarios:

- A different configuration profile has been assigned to the device group that manages this device.
- One of the settings in a configuration profile assigned to the device group that manages this device changes.
- The priority of the device groups changes and a device is now managed by a different device group.
- The device will be removed. In that case, this device is also listed under the Device Removed tab.

For more detailed information on a device in the list, click its name. This opens the Device Manager for that device.

Reverting the Changes

To revert the pending changes:

1 Click **Administration** > **Discovery Configuration > Activate.**

2 Click **Revert Changes**.

Activating the Changes

To activate the pending changes:

1 Click **Administration** > **Discovery Configuration** > **Activate**.

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.

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 13, Setting up Accounts
Configure your data backups	Chapter 15, Backing up and Restoring your data

13 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.

To create a password for an 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.

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**.

14 Setting up Enterprise Discovery Aggregation

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

Introduction

If you have purchased an Aggregator license, this chapter will show you how to set up and use the Enterprise Discovery Aggregator. To use the Aggregator, all of your Enterprise Discovery servers must be at least 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 35.

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 device groups, Agents, or Scanners until you have completed Sharing Security Keys between all your Servers on page 165.

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 41.

The Aggregator server will require more hardware resources (larger disk, more RAM) than a regular Enterprise Discovery server. See Server Installation on page 35 for details.

Installing the Remote Enterprise Discovery Servers

Follow the instructions in Server Installation on page 35 to install each remote server.

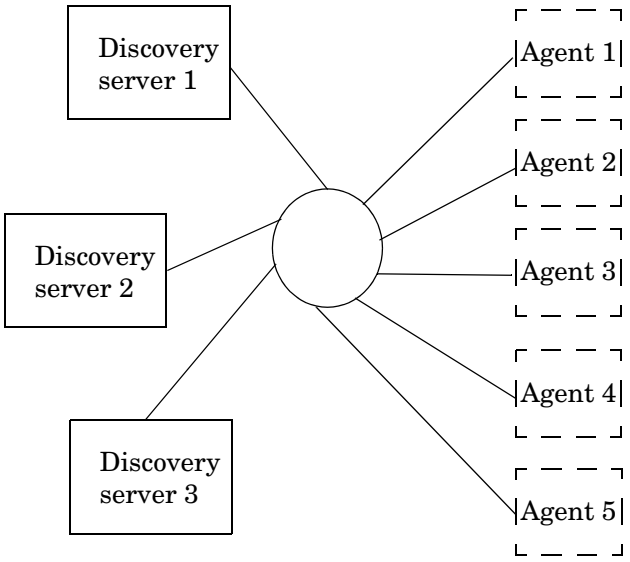
Do not configure your device groups, Agents, or Scanners until you have completed Sharing Security Keys between all your Servers on page 165.

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 or the USB key. Copy only the `ACSkeyStore.bin`, `acstrucst.cert`, and `agentca.pem` files.

Do not copy the `ssl.*` directories located in the `Cert` directory. You do not want to copy the SSL security keys onto the other ED servers. This causes a Hostname mismatch error when accessing the other ED servers.

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

Copying the Security Key files onto the other servers:

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 range device groups 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 172 for suggestions.

You must also perform discovery configuration for your Aggregator. For example, add device groups for your remote server and router, and then be sure to **Activate** the changes. See Chapter 8, Configuring the Discovery Process 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 169.)

6. Select data transfer intervals:
   - Aggregate network inventory

- Aggregate events
- Aggregate workstation inventory

More frequent updates use more bandwidth.

If you change a data transfer interval from a larger to a smaller interval, the smaller interval does not take affect until you have completed the original larger interval setting.

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 167).

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

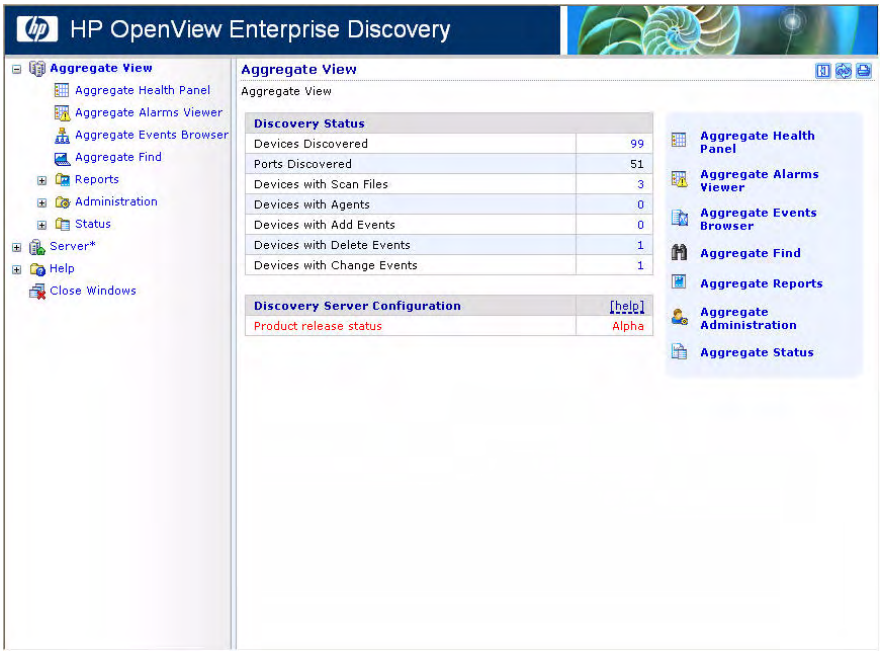
You can use the navigation frame on the left side of your window to look at the Aggregator, or any of your remote servers.

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 167, 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

15 Backing up and Restoring your data

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

Introduction

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

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 50.

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.

To set the number of days that Aggregator files are kept:

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 185.

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.

To restore your backup data to the server:

1. Create an empty directory called “Restore” in the Data directory.
2. Add your latest backup files to the restore directory. You must include at least the following files:
   - certs.zip
   - MySQL.zip
   - data.zip

   And may include the “scans.zip” file as well.
3. Restart your Enterprise Discovery server.

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

16 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.

17 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 Verisign), 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\2.20\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 2.20 > 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\ovedAgentComm	Read-only access
HKLM \SYSTEM\CurrentControlSet\Services\ovedApache	Read-only access
HKLM \SYSTEM\CurrentControlSet\Services\ovedApacheSSL	Read-only access
HKLM \SYSTEM\CurrentControlSet\Services\ovedAuth	Read-only access
HKLM \SYSTEM\CurrentControlSet\Services\ovedADiscDB	Read-only access
HKLM \SYSTEM\CurrentControlSet\Services\ovedDiscEng	Read-only access
HKLM \SYSTEM\CurrentControlSet\Services\ovedEventMgr	Read-only access
HKLM \SYSTEM\CurrentControlSet\Services\ovedLogger	Read-only access
HKLM \SYSTEM\CurrentControlSet\Services\ovedSched	Read-only access
HKLM \SYSTEM\CurrentControlSet\Services\ovedSysmon	Read-only access

Table 3 Registry Security

Registry	Security Measure
HKLM \SYSTEM\CurrentControlSet\Services\ovedTomcat	Read-only access
HKLM \SYSTEM\CurrentControlSet\Services\ovedTplgConv	Read-only access
HKLM \SYSTEM\CurrentControlSet\Services\ovedTplgEng	Read-only access
HKLM \SYSTEM\CurrentControlSet\Services\ovedWatchdog	Read-only access
HKLM \SYSTEM\CurrentControlSet\Services\ovedXmlEnricher	Read-only access
HKLM \SYSTEM\CurrentControlSet\Services\ovedXmlEnricher1	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 189).

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 155.

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**.

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**.

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.

18 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-2.2.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\2.20\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.

19 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.

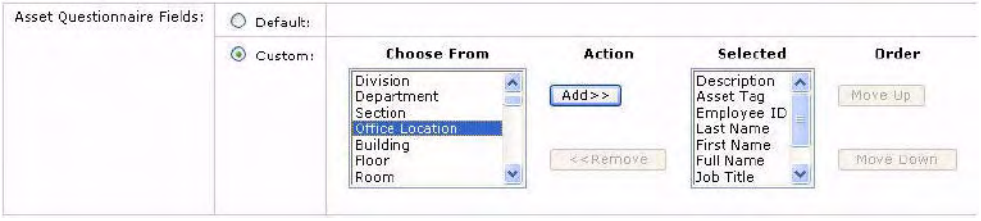
There are several other default options to add to your questionnaire, including items like Telephone Number, Floor, Room, Barcode, etc. If you require more question fields on your questionnaire, you can also add up to 30 of your own.

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.

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.**

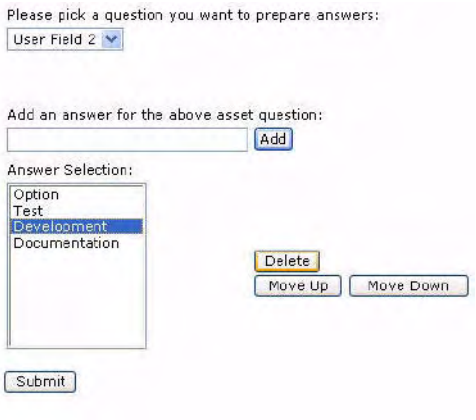
17 Configure a series of answers for the Lists on your Asset Questionnaire.

If you would prefer to compose your answers separately, and import them into the UI, see Importing Your Answer Selections on page 201.

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 included in an IP-only device group

If the device is included in an IP-only device group, and you want to add asset information from the Questionnaire, just enter the information as needed, and click **Submit**.

The Workstation is NOT in included in an IP-only device groups

If the device you are connecting from has not been included in an IP-only device group, 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**.

20 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 2.20.

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 2.20.

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 2.20 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.

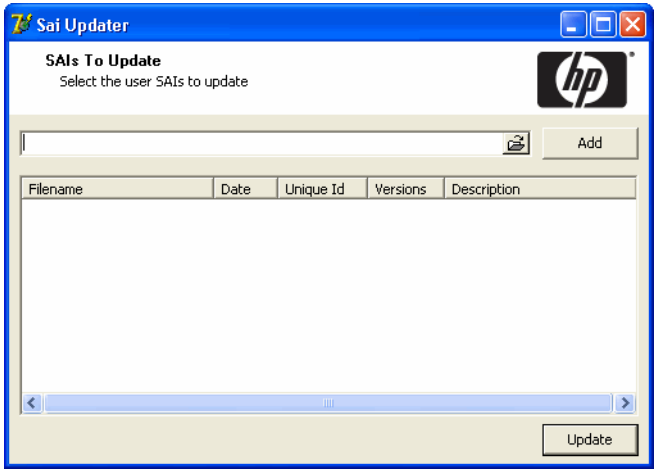
When a read-only SAI is updated, applications taught by the customers are extracted into a new User SAI.

Starting the SAI Update Wizard

To start the SAI Update Wizard:

- From the Windows **Start** menu select **Programs > HP > Enterprise Discovery 2.20 > 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\2.20\Common

21 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/2.20/logs`.

Index

D