HP Discovery and Dependency Mapping Inventory

for the Windows® operating system

Software Version: 7.70

Installation and Initial Setup Guide

Manufacturing Part Number: None
Document Release Date: June 2010
Software Release Date: June 2010

hp invent

Legal Notices

Warranty

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

The information contained herein is subject to change without notice.

Restricted Rights Legend

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

Copyright Notices

Trademark Notices

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

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® and Pentium® are registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

This product includes software developed by the Apache Software Foundation (**http://www.apache.org/**)

Support

You can visit the HP Software Support web site at:

www.hp.com/go/hpsoftwaresupport

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 an active support contract. To find more information about support access levels, go to the following URL:

http://h20230.www2.hp.com/new_access_levels.jsp

To register for an HP Passport ID, go to the following URL:

http://h20229.www2.hp.com/passport-registration.html

Contents

1 Welcome to DDM Inventory

Welcome to the *Installation and Initial Setup Guide*.

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

About DDM Inventory Installation

DDM Inventory enables you to discover, track, and inventory 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.

When you install the server components, the client components are installed as well. There is no need to perform a second client installation.

By default, when you install the DDM Inventory server software, all the components will be in one of the following locations:

Table 1 Component Locations

Folder Name	Default Location
DDM Inventory Program Files folder	`C:\Program Files\Hewlett-Packard\DDMI\7.70`

DDM Inventory Data folder	Windows Server 2003:
	`C:\Documents and Settings\All Users\ Application Data\Hewlett-Packard\DDMI`
	Windows Server 2008
	`C:\ProgramData\Hewlett-Packard\DDMI`

In this document, the following placeholders are used to represent these locations:

- *<InstallDir>* represents the location of the DDM Inventory Program Files folder
- *<DataDir>* represents the location of the DDM Inventory Data folder

You can customize both of these locations when you install the DDM Inventory server.

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

License Options

The following packages are available:

Table 2 License Options

Option	Contents
1	DDM Inventory license
2	DDM Inventory license + Aggregator
3	DDM Inventory license + DDMI Topology[a]
4	DDM Inventory license + Aggregator + DDMI Topology[a]

a. DDMI Topology is no longer available for sale to new customers.

DDM Inventory License

The DDM Inventory license combines the Device Discovery, Device Inventory, and Software Utilization licenses into a single license. When you purchase the DDM Inventory, you automatically own the capabilities of device discovery, device inventory, and software utilization.

Customers who purchased individual components (such as ED Device Discovery, ED Inventory, or ED Automated Inventory), are not automatically entitled to receive the license to use Software Utilization capability during a product upgrade. Please contact your Account Representative to find out how to access the Software Utilization capability of DDM Inventory.

The Device Discovery license specifies the maximum number of devices that can be discovered in the network and provides basic information about the devices, such as when they are added to or removed from the network.

The Device Inventory license defines the maximum number of scanned inventories. With this license, DDM Inventory pings and polls 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.

With the Software Utilization license, you can expand your inventory data, as the scanners will capture details about 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.

A DDM Inventory Agent or the Software Utilization plug-in must be installed on each workstation to collect Utilization data.

Aggregator License

The Aggregator license enables the aggregation feature.

DDMI Topology License

Existing DDMI Topology customers use the DDMI Topology license to expand discovery data by calculating and displaying connectivity information for your network. This license is not available to new customers.

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 DDM Inventory works	*Reference Guide*

2 Upgrade and Migration Scenarios

In this chapter, you will learn the basics of how to approach your installation, whether it is a new installation or an upgrade from a previous release of this product, namely, DDM Inventory version 7.5x and 7.6x.

Versions of DDM Inventory prior to 7.50 were called Enterprise Discovery. You cannot upgrade or migrate Enterprise Discovery to DDM Inventory 7.70.

DDM Inventory 7.70 uses Autopass for license management. To upgrade or migrate to this version, make sure the license file is ready. You will need to import the license file during upgrade/migration procedure. For detailed information, see License Options on page 12 or Installing the License on the Server on page 30.

Introduction

There are two ways you could be approaching your DDM Inventory 7.70 installation.

- New Installations on page 16
- Upgrading from Previous Releases on page 18

The following scenarios are best practices for implementing DDM Inventory. They are a high-level overview of the installation steps and may need to be customized to your specific situation.

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

New Installations

DDM Inventory consists of two types of components:

- **Server** components coordinate the discovery and inventory processes, deploy agents and scanners to devices in your network, collect and organize inventory and software utilization information, and provide a convenient interface from which you can view many different types of information about your network. Depending on what you want to accomplish, you can set up your DDM Inventory server to perform all or a subset of these functions.

  The server components must be installed on a dedicated server. They are required to run DDM Inventory.

- **Client** components are stand-alone tools that enable you to view the contents of individual scan files, consolidate inventory data from multiple devices, and analyze this data by using customizable software application index (SAI) information.

  The client installation is a subset of the server installation. If you already have the server components installed, you do not need to explicitly install the client components to get their functionality. You can install them on additional machines in your network if you like, but this is not required.

This *Installation and Initial Setup Guide* will take you through all the steps needed to install and set up DDM Inventory.

For a thorough explanation of how to prepare your network, read the *Planning Guide* first. If you would like more details about how all the components work together, refer to the "How it Works" chapter in the *Reference Guide*.

The following list of tasks will help you install DDM Inventory and get your DDM Inventory server running.

Table 3 New Installation

Task		Instructions	Notes
1	Install the server components.	Server Installation on page 21	Required.
2	Install the client components.	Client Installation on page 43	Optional. Refer to the *Scan Data Analysis Guide* for more information about the client components. If you install the server components, the client components are installed automatically on that machine. You can also install the client components on other machines if you like.
3	Configure your server	Configuring Your DDM Inventory Server on page 61	More details available in the *Customization and Configuration Guide*.
4	Set up Network and SNMP Configuration Profiles	Setting Up Discovery Configuration Profiles on page 95	After you create these configuration profiles, you can assign them to device groups in the next step.

Table 3 New Installation

Task		Instructions	Notes
5	Set up IP-only device groups	Setting Up Device Groups on page 101	
6	Activate your changes	Activating Your Configuration Changes on page 135	Wait until DDM Inventory has discovered all of those devices before continuing. Check **Status > Device status > Network model queue/Network model processing**.
7	Create Scanners	See the *Customization and Configuration Guide*.	Skip this step if you are only collecting basic hardware information and do not need software data.
8	Set up Agent and Scanner configuration profiles for testing	Setting Up Discovery Configuration Profiles on page 95 Two Types of Scanning: Agent-Based and Agentless on page 119 Setting Up Agents and Scanners on page 119	Configure DDM Inventory to deploy agents to—or perform an agentless scan on— a small portion of your network to ensure your configuration is correct.
9	Activate your changes	Activating Your Configuration Changes on page 135	
10	Manually deploy UNIX and Mac OS X agents	See the *Customization and Configuration Guide*.	Optional. If you are using agentless scanning, this step is not required. If you are using agent-based scanning, this step 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 141	

Upgrading from Previous Releases

In this scenario, you have been using the fully automated discovery features of a previous release of this product, namely, DDM Inventory version 7.5x and 7.6x. Follow these tasks to upgrade to DDM Inventory 7.70:

Task		Instructions
1	Back up your discovery data	See Chapter 15, Backing Up and Restoring Your Data.
2	Copy your Analysis Asset Field configuration (if necessary)	See Copy Analysis Asset Field Configuration below.
3	Uninstall the previous release	See Uninstall Previous Release below.
4	Install DDM Inventory version 7.70	See Chapter 3, Server Installation and Chapter 5, Client Installation.

It may be necessary to clear the browser cache on each computer used to access the DDM Inventory web UI after a DDM Inventory server upgrade.

Copy Analysis Asset Field Configuration

The XML Enricher now reads the analysis asset field configuration from the `viewer.ini` file located in the `<DataDir>\Conf` directory, where `<DataDir>` is the location of the DDM Inventory data folder that you specify at install time.

If your analysis asset field configuration used for the XML Enricher is already in the `viewer.ini` file, it will be used, and no action is required.

If this configuration is no longer available, you must manually copy the analysis field section of the `xmlenricher.ini` file to the `viewer.ini` file before upgrading to DDM Inventory version 7.70.

Uninstall Previous Release

After you have backed up your discovery data, you must uninstall the components from the earlier release of the product before installing DDM Inventory version 7.70.

To remove components from an earlier release:

1. In **Control Panel** > **Add/Remove Programs** (for Windows Server 2003) or **Control Panel** > **Programs and Features** (for Windows Server 2008), select the earlier release of the product that you have currently installed.
2. Click **Remove**. Follow the on-screen instructions.
3. *Optional:* You can also uninstall the discovery Agent if you want to. This is not necessary, however.

When the DDM Inventory server starts up, it installs an Agent if and only if the server machine does not already have an Agent.

4 Remove the following folder: `<OldInstallDir>\Tomcat`

In this case, `<OldInstallDir>` is the installation directory that you specified when you installed DDM Inventory. By default, this was:

Version 7.5x	`C:\Program Files\Hewlett-Packard\DDMI\7.5*`
Version 7.6x	`C:\Program Files\Hewlett-Packard\DDMI\7.6*`

5 *Optional:* View the DDM Inventory uninstall log file, which contains a list of all the files and folders that were removed during the uninstall:

`<OldInstallDir>\uninstall\uninst_ED.log`

6 Restart your server.

You must restart your server before installing DDM Inventory version 7.70.

If you have the client tools installed from the earlier release, you must remove them. DDM Inventory does not support multiple versions of the client tools on the same machine —whether it is the DDM Inventory server machine or any other system where the client tools are already installed.

3 Server Installation

In this chapter, you will learn how to install the DDM Inventory server components. The following topics are covered:

Overview

You must install the DDM Inventory server components on one dedicated server. The server components can be installed on the following platforms:

- Windows Server 2003, SP1, SP2, or R2
- Windows Server 2008

The DDM Inventory server components can also be installed on Windows XP SP2, but this platform should be used for demo or trial installations only. This platform is not supported in a production environment.

If you install the server components on a laptop, be sure to set the power options such that the system never goes into standby or hibernate mode.

Refer to the *DDM Inventory Version 7.70 Release Notes* for detailed information about additional hardware and software requirements.

Installing SNMP on the Server

You should have the Microsoft SNMP Agent installed on your DDM Inventory server. Without it, DDM Inventory 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 (not localhost) of the server itself.

The DDM Inventory installer will prompt you to install the SNMP agent if it is not already installed.

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

Checking for ActivePerl

Many applications including DDM Inventory install ActivePerl, a popular program used for running scripts. Before you install DDM Inventory, 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 DDM Inventory installer.

To see if ActivePerl is installed:

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

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

```
This is perl, v5.8.8 built for MSWin32-x86-multi-thread
(with 33 registered patches, see perl -V for more detail)

Copyright 1987-2006, Larry Wall
```

```
Binary build 819 [267479] provided by ActiveState http://www.Active
State.com
Built Aug 29 2006 12:42:41

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 examines only the system `PATH` environment variable. Most applications that install ActivePerl add it to the `PATH`.

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

The DDM Inventory 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 DDM Inventory on the Server

This section describes how to install the DDM Inventory on your dedicated server.

Before running the Setup program, ensure that:

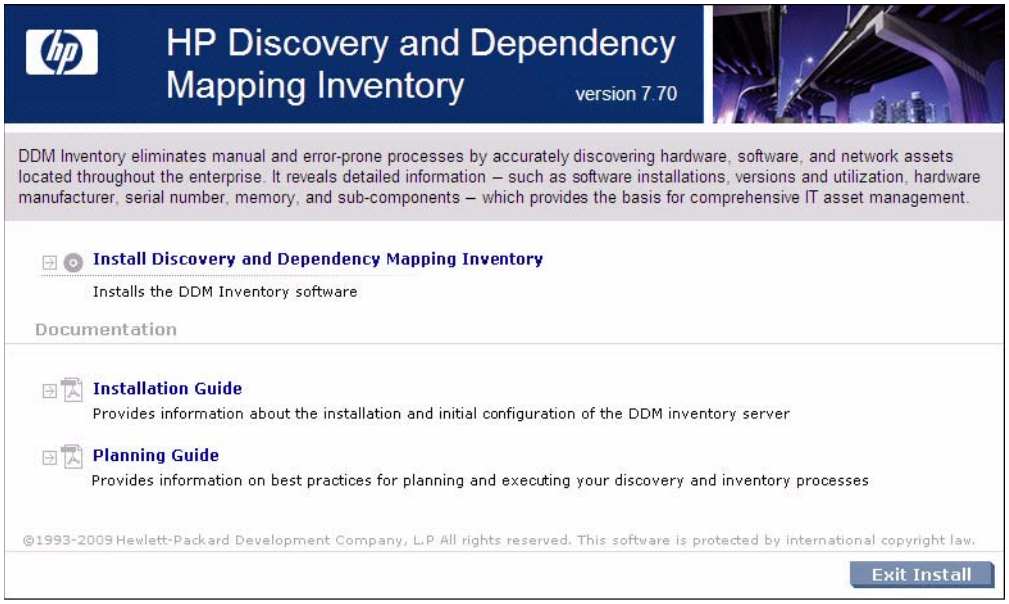
- The server has Windows 2003 Server or Windows 2008 Server installed. (If this is a trial or demo installation, you can have Windows XP installed.)
- ActivePerl is not already installed on the server.
- No other Windows applications are running, with the exception of your standard anti-virus software. The anti-virus agent should be configured to exclude the DDM Inventory <*DataDir*> folder with the exception of the LiveAgents and Scanners folders.

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

To install DDM Inventory:

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

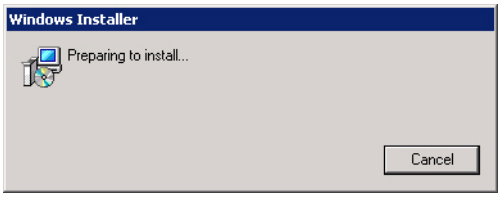
The following screen appears.



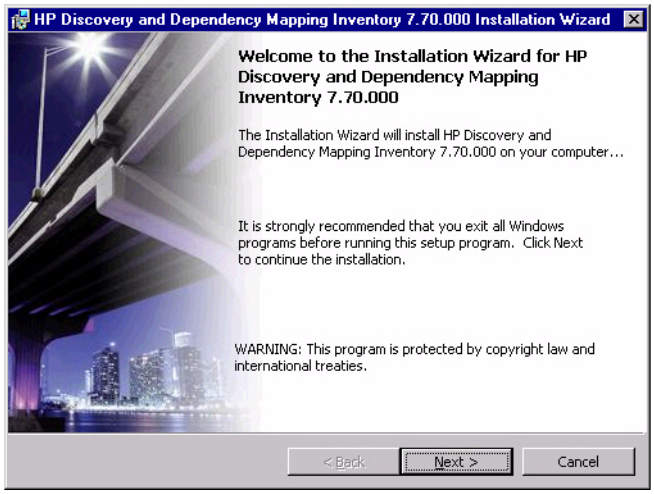
The CD is configured to auto-run, however if you need to start the CD Browser program manually, you can do this by navigating to the drive containing the CD and double clicking on the `Autorun.exe` file.

2 Click **Install Discovery and Dependency Mapping Inventory** to start the install process.

Next, the Preparing to Install window appears.

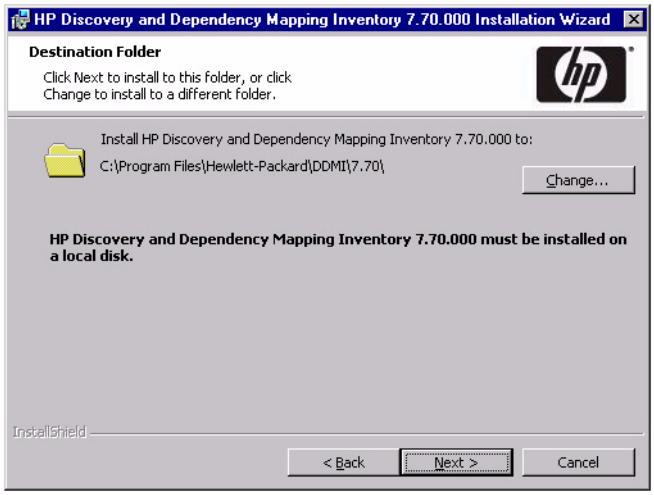


Next, the Installation Wizard appears.



3 Click **Next**.

The Destination Folder screen appears.



The default Destination folder is:

`C:\Program Files\Hewlett-Packard\DDMI\7.70`

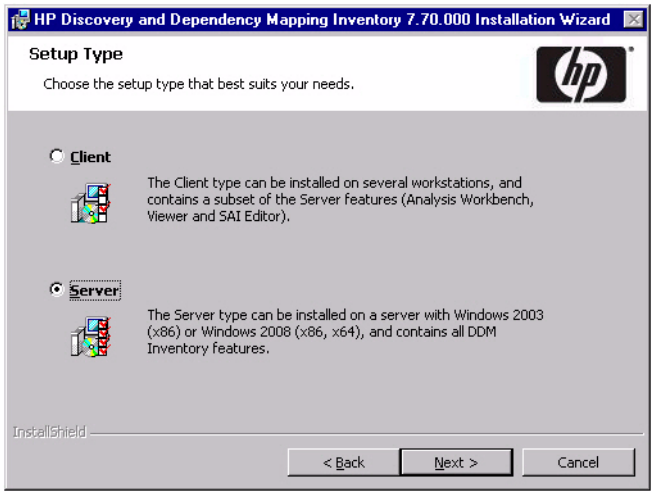
This is also known as the DDM Inventory Program Files folder. The location of this folder is represented by *<InstallDir>* in this document.

➤ DDM Inventory 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. Click **Next**.

The Setup Type screen appears.



5 Select the “Server” setup type. When you select Server, both the server components and client components are installed.

6 Click **Next**.

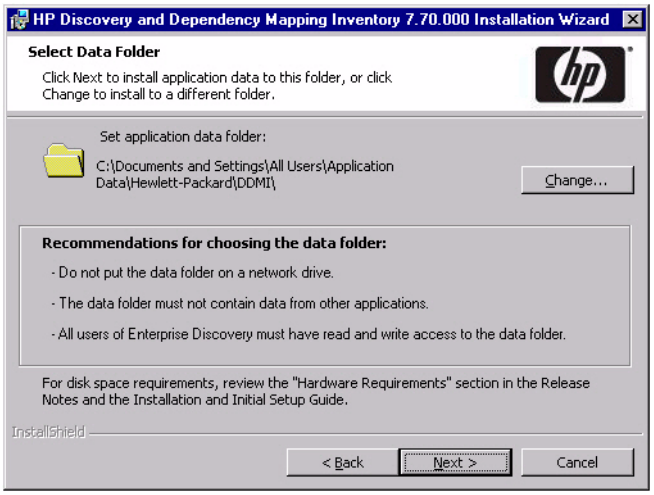
If your server does not have SNMP installed, you will see the “Installing Simple Network Management Protocol” screen. You have the option of installing SNMP during the installation process.

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 DDM Inventory has already been installed on this server, and you want to retain your existing configuration and data but change the location of the Data folder, you must manually move your Data folder to the new location before continuing with this installation.

The default Data folder for Windows Server 2003 installations is as follows:

`C:\Documents and Settings\All Users\Application Data\Hewlett-Packard\DDMI`

For Windows Server 2008 installations, the default Data folder is:

`C:\ProgramData\Hewlett-Packard\DDMI`

The location of the Data folder is represented by *<DataDir>* in this document.

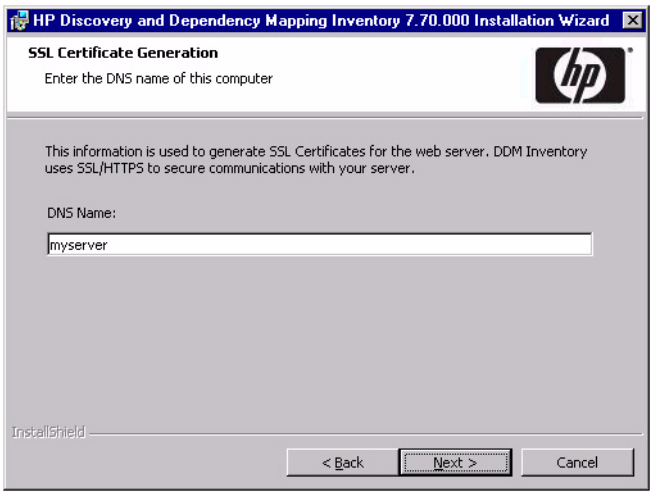
You cannot put the Data folder in the root directory (for example, `C:\`).

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.



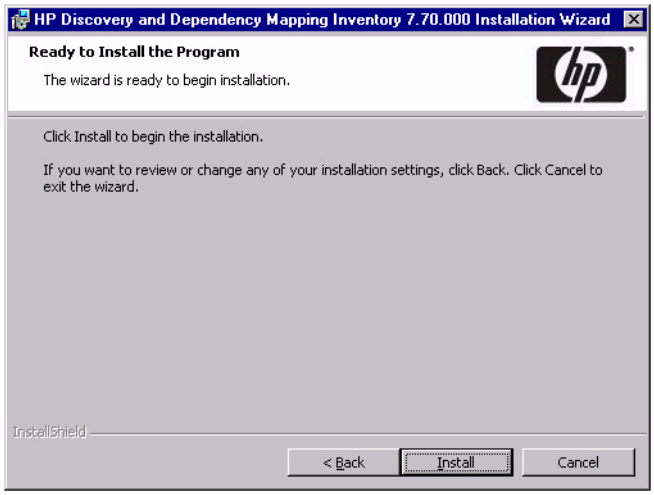
You can specify the simple host name (for example, `myserver`), the fully qualified host name (`myserver.mycompany.us.com`), or the IP address. The DNS name that you specify here will be the same name that you use each time you start the DDM Inventory web user interface.

If you are upgrading from an earlier version of DDM Inventory, and you specify a different DNS name for this server, you will need to manually remove your existing SSL certificates. You will receive a warning similar to this one:

The SSL certificates are stored in the `Certs` subdirectory of the Data folder that you specified in Step 8 on page 26.

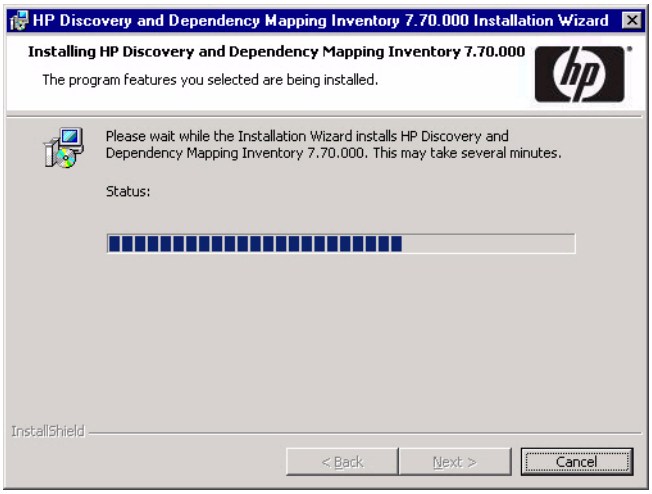
11 Click **Next**.

The Ready to Install the Program screen appears.



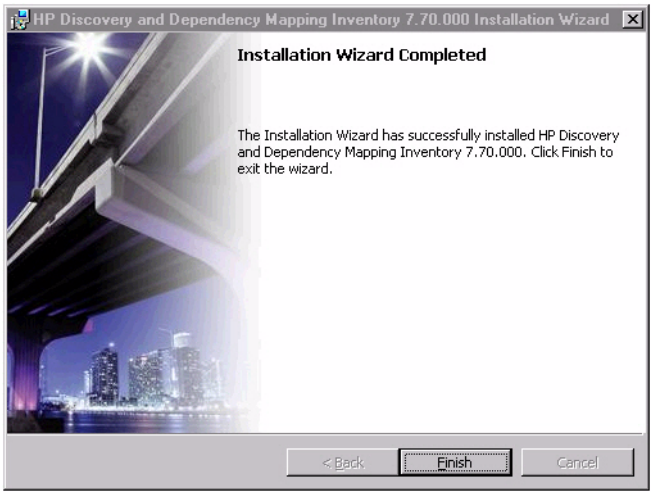
12 Click **Install** to begin the installation.

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 DDM Inventory is complete.

Running an Unattended Installation of DDM Inventory

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

To perform an unattended install of DDM Inventory:

1 Open a command prompt window.

2 Navigate to the directory containing all of the installation files for DDM Inventory.

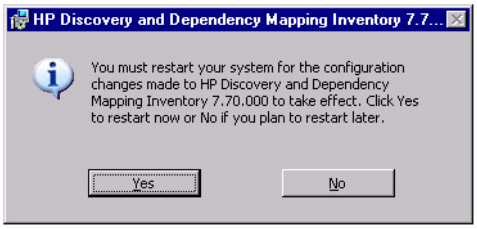
3 Type the following command at the prompt:

```
"HP_DDM_Inventory_7.70.000.msi"  ADDLOCAL=ALL ALLUSERS=1
REBOOT=ReallySuppress SETUPTYPE=TYPICAL /qr
```

4 Manually restart the server after the installation is complete.

Restarting Your Server

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



Click **Yes** to restart the server 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.

Installing the License on the Server

The HP License Key Delivery Service web site (**www.webware.hp.com**) manages HP software licensing for DDM Inventory. You can view or download the latest version of the *ESD and Webware License Management Guide* from this site. The guide describes the current process to obtain your *entitlement certificate*, which contains the HP order number that you need to generate your permanent license keys.

Follow the steps in the *ESD and Webware License Management Guide* to present your HP order number, select the products that need licenses, and provide other required information. If you are a first time visitor to the web site, you will be asked to create an account with an email address and password. Most requests to generate permanent license keys require the following:

- DDM Inventory product names and numbers shown on the product receipt or in the email sent by HP to acknowledge the order.
- The order number from the entitlement certificate.
- The host name of each DDM Inventory server.
- Contact information, such as company name, your name, fax and phone numbers, and license ownership details.

The DDM Inventory license determines how many devices you can discover in your network.

Before you visit the HP License Key Delivery Service web site to generate a license, determine how many installations you need for each purchased product, identify the server for each product, and decide how many installations of each product will go on each DDM Inventory server.

Manage the Permanent License Keys

After you create your user account on the HP License Key Delivery Service web site, generate the entitlement certificate, and generate the license keys, the License Key Delivery Service sends permanent keys to you in an email text file attachment. When you receive the permanent license key files, stage them in a convenient directory on the DDM Inventory server.

If necessary, you can return to the HP License Key Delivery Service web site and retrieve the permanent license keys again by selecting **Manage Licenses** on the web site home page and logging into your account.

Port the Permanent License Key Files

From the stored location of the license files, you must copy the appropriate license to a similar directory on each server where you plan to install one of these DDM Inventory components:

- Inventory Devices
- Discovery Devices
- Topology
- Software Utilization
- Aggregation

The DDM Inventory license combines the Device Discovery, Device Inventory, and Software Utilization licenses into a single license. For detailed information about DDM Inventory license options, see License Options on page 12.

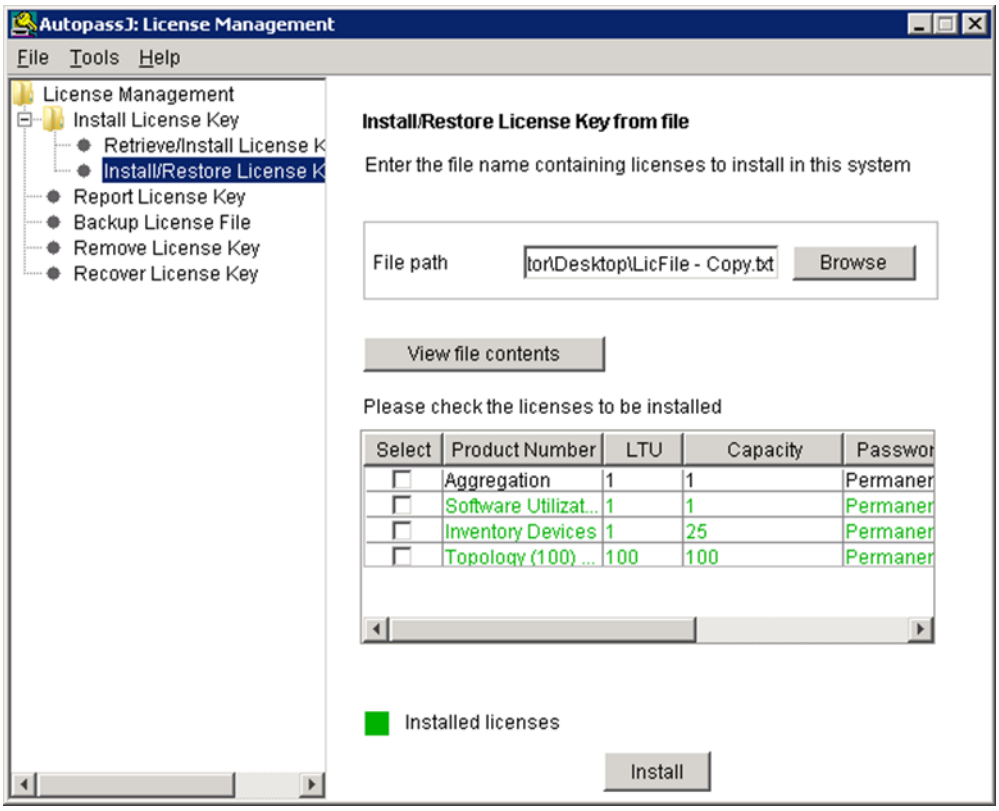
To port the license files, copy them to an external USB storage device or use a File Transfer Protocol (FTP) tool and transfer the appropriate license file to each affected server.

Install the Permanent License Key Files

On each DDM Inventory server, follow these directions to install the license file that you saved in Port the Permanent License Key Files on page 30.

1. From the server where you want to install the license file, click the Windows **Start** menu and select **Programs** > **Hewlett-Packard** > **DDM Inventory 7.70** > **Autopass**.
2. From the left pane of the AutopassJ License Management window, expand the Install License Key folder and select **Install/Restore License Key from file**.
3. In the right pane, click **Browse** and navigate to the location of the license file. Select the license file and click **Open**.
4. Click **View file contents**.
5. Select the products you want to install on this server, then click **Install**.

The text in the table becomes green for the products with installed permanent license keys.



Save Your Certificates to a Safe Location

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

If, for any reason, your DDM Inventory server is damaged and its data is lost, you will need to reinstall the DDM Inventory software. You will need your original certificates in order to communicate with the Agents distributed to your network devices.

We recommend that you copy your DDM Inventory 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.

The certificates are located in the `<DataDir>\Cert` folder.

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 DDM Inventory server, you need to share the folders where these files reside. The scan files are located in the following subfolders of the *<DataDir>* folder that you specified on page 26:

- `Scans\`
- `Scans\Processed`
- `Scans\Original`

These folders should be accessible only to the Administrator user. If you plan only to view scan files from the client machines, read-only permissions are sufficient. If you plan to save scan files using the Manual scanner mode, you will also need write access to the `Scans\Incoming` folder for the user account under which the manual scanners are executed.

For more information about scanners, refer to the *Planning Guide* and the *Reference Guide*. Refer to your Windows documentation for information on how to share folders.

DDM Inventory Services

The following table contains a comprehensive list of services that run after DDM Inventory 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.

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 4 Services

Service	Description
HP DDMI Agent	Enables communication between remote computers and the HP DDM Inventory Server
HP DDMI Agent Communicator	Provides communication services with HP Agents to HP's Discovery products.
HP DDMI Apache SSL Web Server	Secure Apache Web Server installed with HP's Discovery products.
HP DDMI Apache Web Server	Apache Web Server installed with HP's Discovery products.
HP DDMI Authenticator	Provides authentication services for HP's Discovery products.
HP DDMI Database	Provides database services for HP DDM Inventory products

Table 4 Services

Service	Description
HP DDMI Discovery Engine	Provides network discovery services to HP's Discovery products.
HP DDMI Discovery Scheduler	Provides scheduling services for HP's Discovery products.
HP DDMI Event Manager	Provides event processing services to HP DDM Inventory products.
HP DDMI Logger	Provides logging services to HP's Discovery products.
HP DDMI Software Utilization Agent	Collects software utilization data for DDM Inventory. This service is only available if the Agent is installed in the software utilization only mode (scanners are manually deployed). Refer to "Manual Deployment" in the *Configuration and Customization Guide* for more information.
HP DDMI System Monitor	Ensures all HP system processes are running properly.
HP DDMI System Status	Provides system information for the System Panel.
HP DDMI Tomcat Servlet Container	Tomcat Servlet Container bundled with HP's Discovery products.
HP DDMI Topology Converter	Provides connectivity data processing services to HP DDM Inventory products.
HP DDMI Topology Engine	Identifies the network topology, applies the break fault detection logic and calculates some statistics.
HP DDMI Watchdog	This service ensures the System Monitor process is running.
HP DDMI 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 DDM Inventory to run.
HP DDMI 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 DDM Inventory server to run two XML Enricher instances, the following service is also started: HP DDM Inventory XML Enricher (1). For additional information, see "Running Multiple XML Enrichers" in the *Configuration & Customization Guide*.

Some of these services stop or restart automatically. For example, the Topology Engine stops after each run. The Apache Web Server restarts every morning at 2:00 AM. These are normal events.

What Next?

To	Go to
Learn how to use the SystemPanel	Chapter 4, Using the System Panel
Install DDM Inventory on client workstations	Chapter 5, Client Installation
Learn how to access the different components	Chapter 7, Getting Started with DDM Inventory
Set up the server	Chapter 8, Configuring Your DDM Inventory Server

4 Using the System Panel

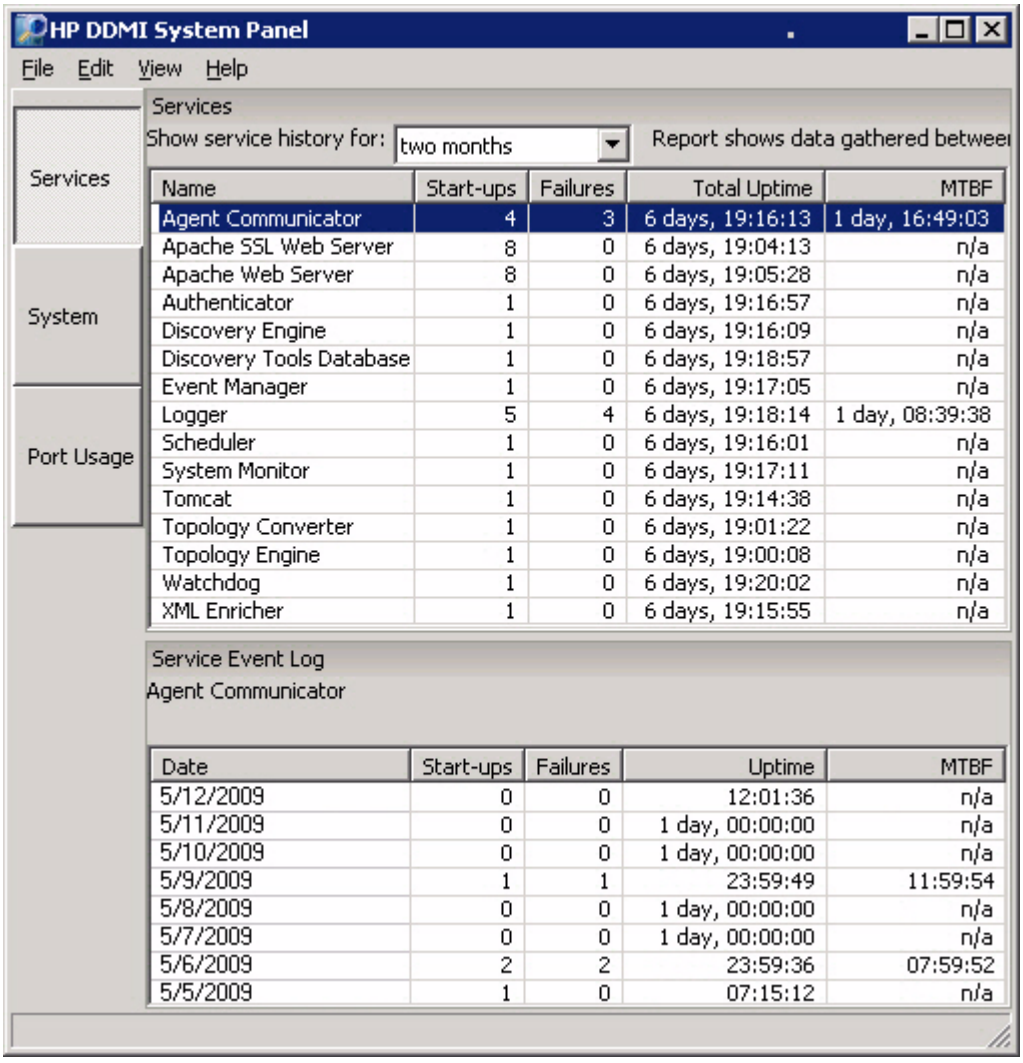
You can use the System Panel to view status information about DDM Inventory. Specifically, the panel displays information about the following items in one of its three views:

- Services View: Lists the current status of each service and indicates whether an abnormal termination or unplanned restart has occurred.
- System View: Shows the status of the hardware components of your DDM Inventory server.
- Port Usage View: Lists the current status of the ports that DDM Inventory uses and indicates whether any software installed on the server is using one of these ports and causing a conflict.

To access the System Panel, double-click the  icon in the system tray of the machine on which you have DDM Inventory installed. When you click the icon in your system tray, the System Panel opens to the Services view.

Services View

The Services view contains two boxes:



The upper box in this view lists all the DDM Inventory services and reports cumulative statistics for each service during the time period specified in the drop-down list. The information shown depends on the time period specified, as shown here:

Show service history for	**Statistics reflect**
one day	The current day's data (cumulative data minus the cumulative data the previous day at midnight)
one week	Data for the last seven days
one month	Data for the last 30 days
two months	Data for the last 60 days

The lower box shows the daily statistics for a particular service. DDM Inventory assumes that the date changes at midnight local time.

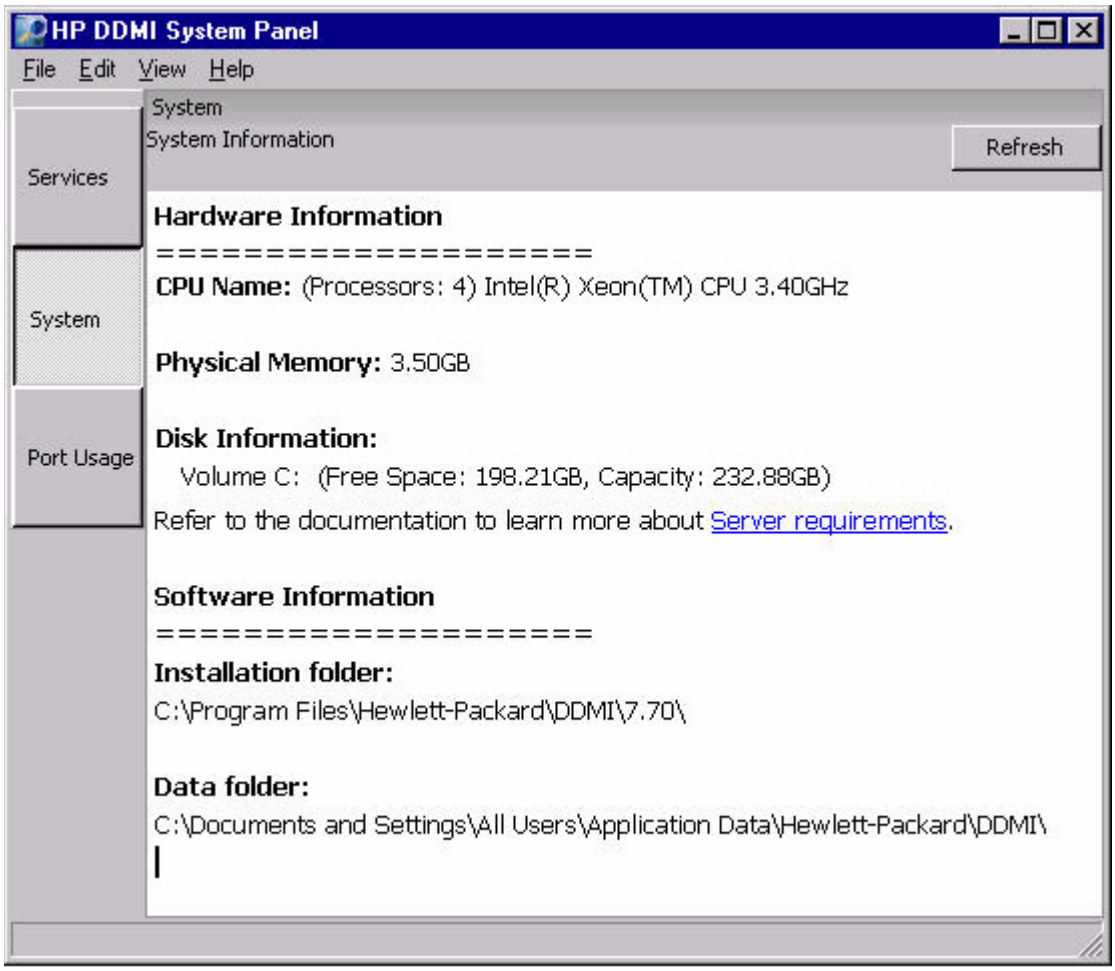
To show the Services Event Log for a particular service, select that service in the upper box. The following information then appears in the lower box:

- Date—Each row in the table corresponds to a single day.
- Start-ups—How many times the service was started on each day listed.
- Failures—How many times the service failed on each day listed. The failure count is incremented when a service transitions to an unexpected state. Valid transitions states are as follows:

  Stopped > Starting > Started > Stopping > Stopped
- Uptime—The total elapsed uptime for the service on each day listed.
- MTBF—Mean time between failures for the service on each day listed.

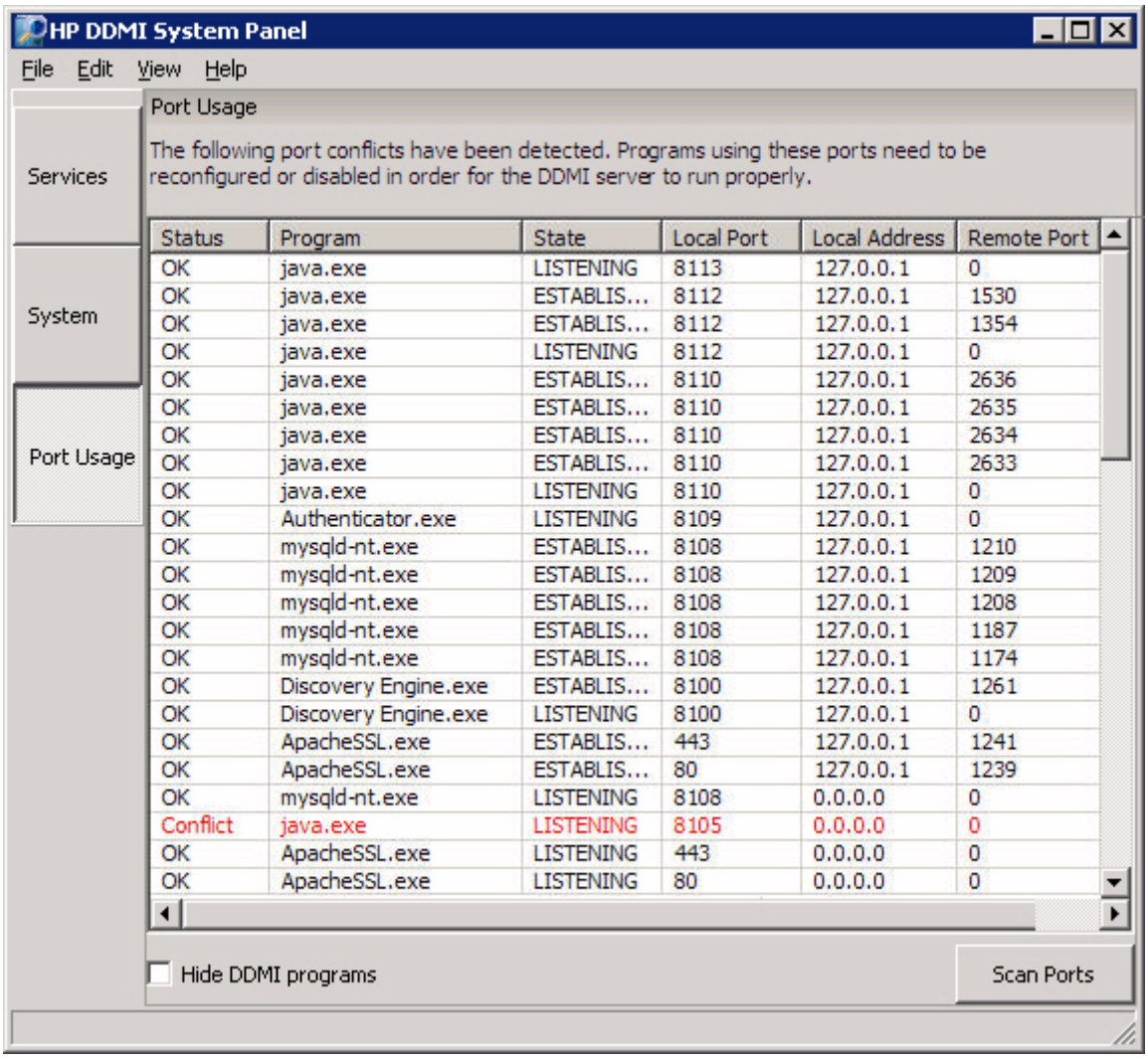
System View

To see the status of the hardware components of your DDM Inventory server, click the **System** button on the left side of the System Panel.



Port Usage View

To see the status of the ports that DDM Inventory uses, click the **Port Usage** button on the left side of the System Panel.



The Port Usage view enables you to detect possible conflicts with other applications using the same ports that DDM Inventory uses (ports 80, 443, 2738 or 7738, 8005, and 8100-8119).

If you have any software installed on the DDM Inventory server that conflicts with one of the ports that DDM Inventory uses, it will be flagged in this view and highlighted in red. You will need to make these ports available in order to use DDM Inventory. You may need to reconfigure or remove other applications.

After you take the necessary steps to resolve any port conflicts that appear in the list, click the **Scan Ports** button to refresh the view.

If you select the **Hide DDMI programs** check box, you will filter the programs listed to those software applications that are not part of DDM Inventory but are using one or more of the ports that DDM Inventory uses.

What Next?

To	Go to
Install DDM Inventory on client workstations	Chapter 5, Client Installation
Learn how to access the different components	Chapter 7, Getting Started with DDM Inventory
Set up the server	Chapter 8, Configuring Your DDM Inventory Server

5 Client Installation

In this chapter, you will learn how to install the DDM Inventory client components. The following topics are covered:

You can install the client components on multiple workstations.

The client installation is optional. When you installed the server components, the client components were automatically installed on that system. The instructions in this chapter are required only if you want to install the client components on systems other than the DDM Inventory server system.

The server installation contains everything available in DDM Inventory version 7.70. The client installation is a subset of the server installation.

For more information about the relationship between the server components and the client components, refer to New Installations on page 16.

Client Specifications

You can use any properly equipped computer as an Admin workstation. For specific technical requirements, refer to the *DDM Inventory Version 7.70 Release Notes*.

Client systems also require an Internet browser and the Java Runtime Environment (JRE). You can download the JRE from the **java.sun.com** web site. For a list of currently supported browser and JRE versions, refer to the *DDM Inventory Compatibility Matrix*.

For DDM Inventory to work properly, both Java and JavaScript must be enabled in your browser. Be sure that you have a Java plug-in installed with your browser.

Installing DDM Inventory

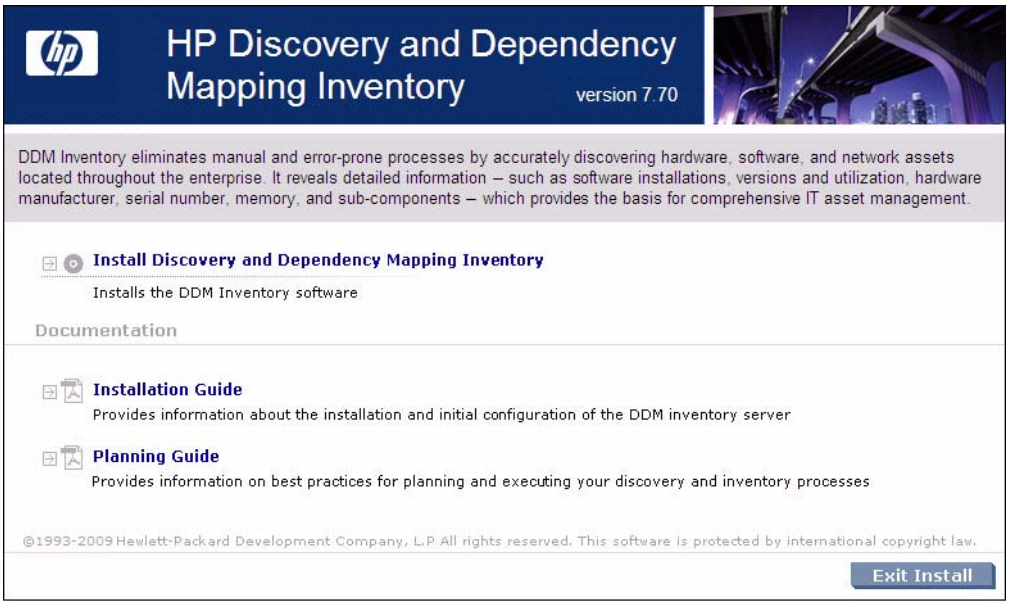
This section describes how to install DDM Inventory on your client workstation.

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

To install DDM Inventory on the client workstation:

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

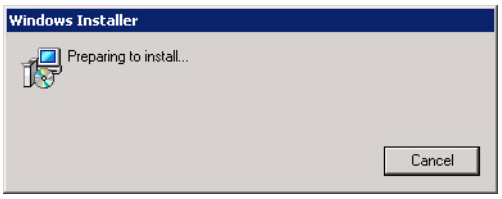
The following screen appears.



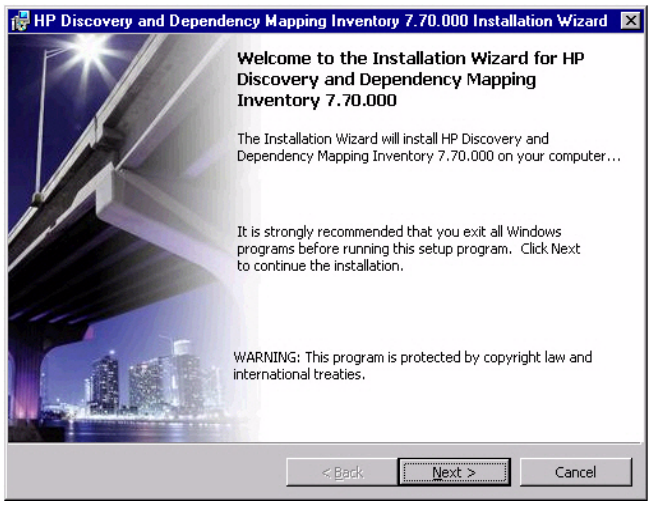
The CD is configured to auto-run, however if you need to start the CD Browser program manually, you can do this by navigating to the drive containing the CD and double clicking the `Autorun.exe` file.

2 Click **Install Discovery and Dependency Mapping Inventory** to start the install process.

Next, the Preparing to Install window appears.

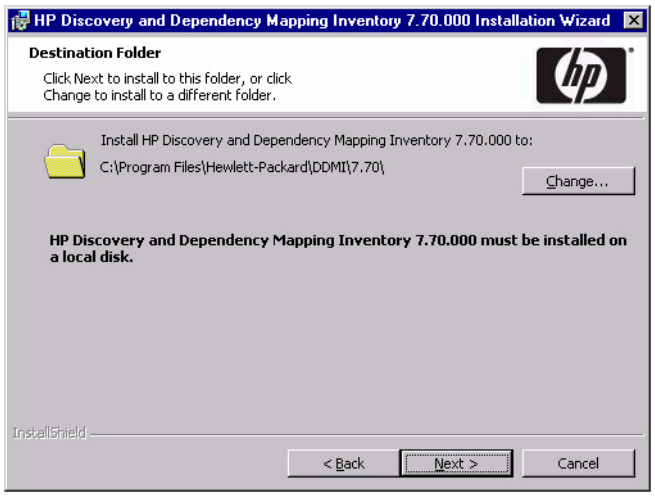


Next, the Installation Wizard appears.



3 Click **Next**.

The Destination Folder screen appears.



The default Destination folder is:

`C:\Program Files\Hewlett-Packard\DDMI\7.70`

This is also known as the DDM Inventory Program Files folder. The location of this folder is represented by *<InstallDir>* in this document.

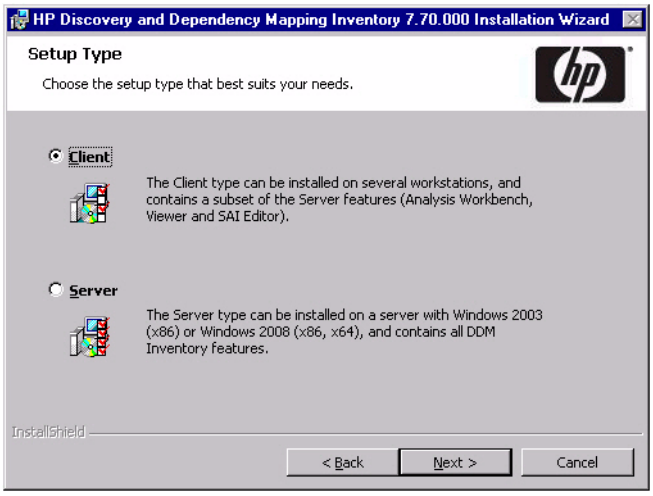
➤ DDM Inventory must be installed on a local disk.

4 If you do not want to use the default installation folder, click **Change** and follow the on-screen instructions to specify a different folder.

➤ All components will be installed to this default location.

5 Click **Next**.

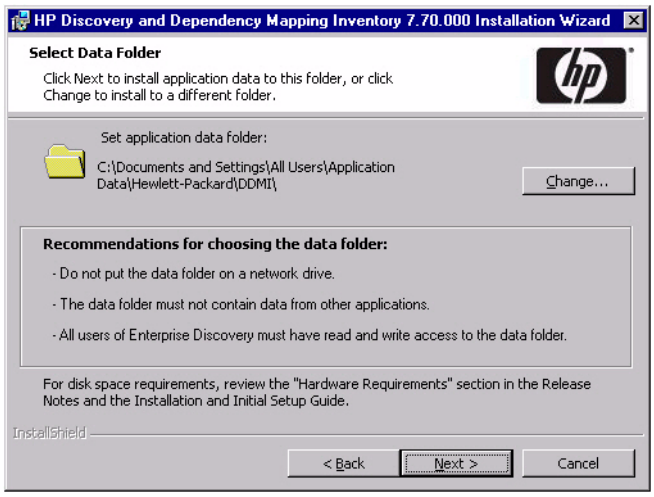
The Setup Type screen appears.



6 Select the **Client** setup type.

7 Click **Next**.

The Select Data Folder screen appears:



The default Data folder for Windows 2003 Server installations is as follows:

`C:\Documents and Settings\All Users\Application Data\Hewlett-Packard\DDMI`

For Windows 2008 Server installations, the default Data folder is:

`C:\ProgramData\Hewlett-Packard\DDMI`

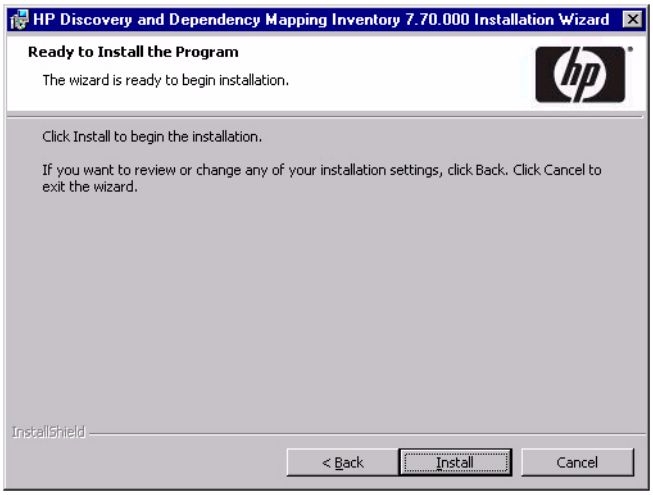
The location of the Data folder is represented by *<DataDir>* in this document.

The default Data folder may not be writable for users who are not Administrators. Check the NTFS permissions to make sure that the data folder location is writable for all users who will use the client installation.

8 If you do not want to use the default data folder, click **Change** and follow the on-screen instructions to specify a different folder.

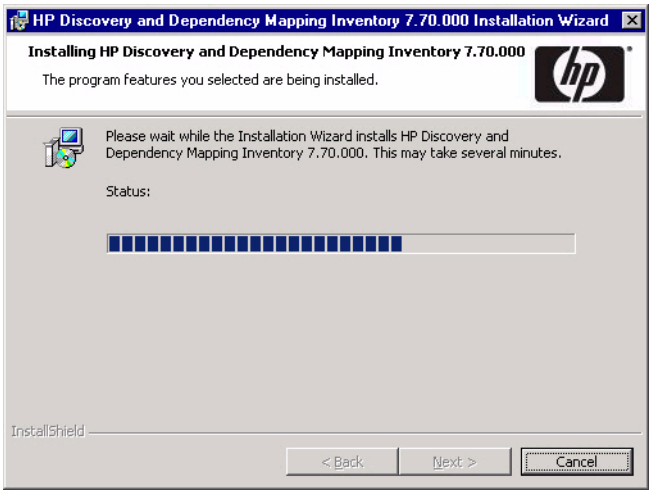
9 Click **Next**.

The Ready to Install the Program screen appears:

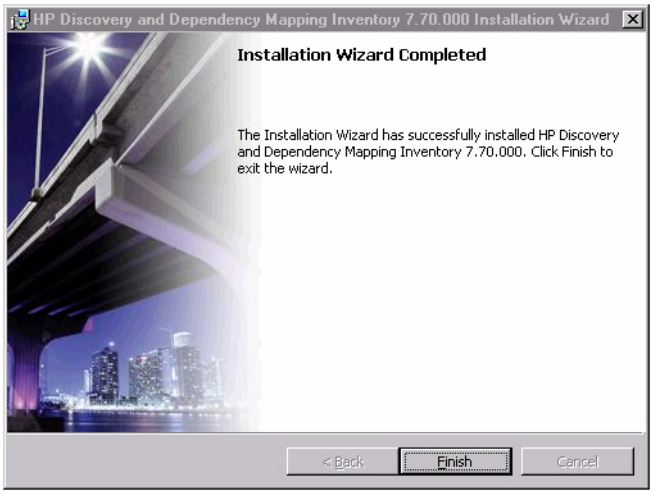


10 Click **Install** to begin the installation.

A progress indicator appears:



After the installation is complete, the following screen appears.



11 Click **Finish**.

The installation of DDM Inventory client components is complete.

What Next?

To	Go to
Learn how to access the different components	Chapter 7, Getting Started with DDM Inventory
Set up the server	Chapter 8, Configuring Your DDM Inventory Server

6 Disk Space Considerations

In this chapter, you will find information about what conditions contribute to the disk space requirements for both the DDM Inventory server and the managed devices on your network where inventory scanning occurs.

Disk Space for the DDM Inventory Server

For information about DDM Inventory server disk space requirements, refer to the *DDM Inventory Version 7.70 Release Notes*.

To conserve disk space on your DDM Inventory server, you can do the following:

Action	**Explanation**
Reduce the time that your server keeps data that will be sent to the Aggregator.	Click **Administration > System Configuration > Aggregate configuration**. Reduce the amount of time the server keeps its Aggregator data.
Do not back up your scan files	Configure DDM Inventory 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.
Turn off delta scanning	You can turn this off in the Scanner Generator. For more information, see the *Configuration and Customization Guide*.
Delete orphaned scan files	Click **Administration > System Configuration > Scan file management**. This option is enabled by default.
Turn off **Installed Applications (WMI)** in the scanner	This option is specified in the Scanner Generator. It is turned off by default. For more information, see the *Configuration and Customization Guide*.

Disk Space for Managed Devices

Disk space requirements can vary greatly for the managed devices in your network. The amount of disk space required on each device depends on the type of scanning that is performed, the size of the scanner, and the size of the managed device itself. Typical requirements are illustrated in the following table:

Scenario	Agent/ Scanner Size	Typical Inventory Data Size	Typical Utilization Size (Max for 1 year)	Typical Total Size without Utilization	Typical Total Size with Utilization
Desktop/ Workstation, targeted scan	< 7MB	250K - 3MB	5 - 10MB	< 10MB	< 20MB
Desktop/ Workstation, classic scan	< 7MB	1 - 10MB	5 - 10MB	< 20MB	< 30MB
Server, targeted scan	< 7MB	1 - 20MB	10 - 30MB	< 30MB	< 60MB
Server, classic scan	< 7MB	2 - 150MB	10 - 30MB	< 160MB	< 200MB

Although these are typical values, actual values may vary depending on selected collection options and the size of the managed computer. For example, if information on all files is collected and stored, as opposed to the default configuration where only information on executable files is collected, disk space requirements will be larger.

The sizes shown in the Disk Space Requirements table do not apply to devices with the HP-UX Itanium (ia64) operating system. On devices with this operating system, agent/ scanner file size is typically 12MB.

What Next?

To	Go to
Learn how to access the different components	Chapter 7, Getting Started with DDM Inventory
Set up the server	Chapter 8, Configuring Your DDM Inventory Server

7 Getting Started with DDM Inventory

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

Introduction

Depending on your installation, there are different ways to access the various DDM Inventory 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
  - Autopass
  - SAI Editor
  - System Panel
  - Viewer
- Web Interface Components (available through your web browser)
  - Health Panel
  - Alarms Viewer
  - Network Map
  - Service Analyzer
  - Events Browser
  - MIB Browser
  - Scan Data Viewer
  - Scanner Generator
  - Express Teaching
  - 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 DDM Inventory, your browser must have the following:

- Java (Sun) JRE version enabled for applets
- JavaScript enabled
- Pop-up windows enabled

You must also have the following:

- The IP address or domain name of the DDM Inventory server (if you are accessing the server through the intranet)
- A valid DDM Inventory account name and password

DDM Inventory is shipped with four pre-defined accounts.

Table 5 Default Accounts

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

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

To access the DDM Inventory web components:

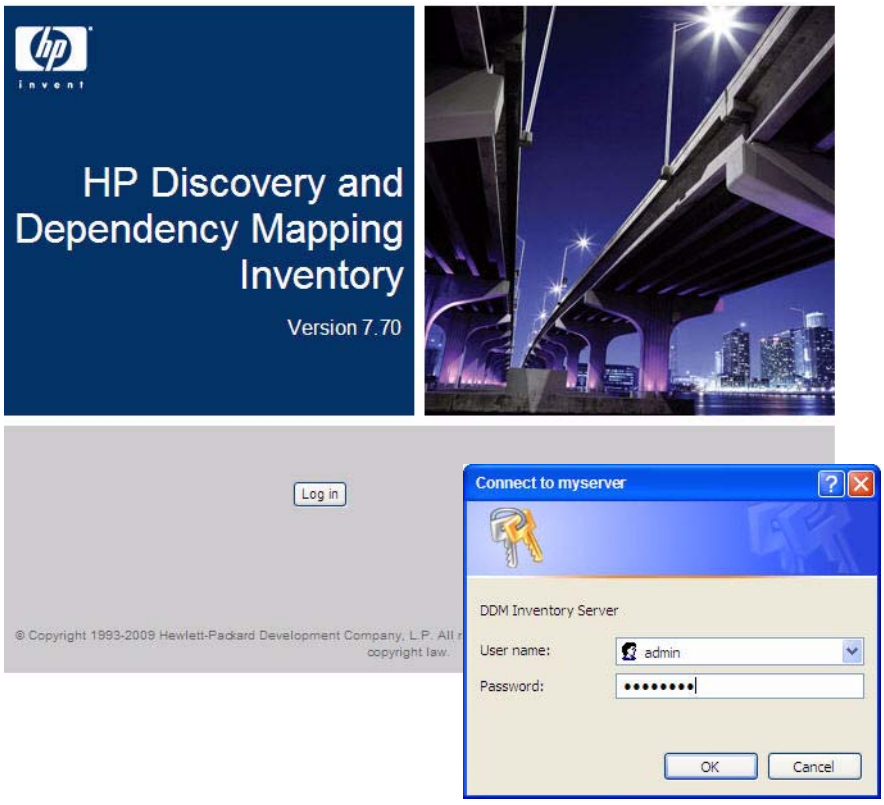
1 Launch your web browser.

2 In the URL area of your browser, enter the IP address or host name of your DDM Inventory server. If you are working on the server itself, you can specify `localhost` in the URL.

At this point, a message pertaining to the SSL certificate may appear. The content and format of this message will vary depending on the browser you are using and your specific browser settings.

You can choose either to proceed and accept the certificate for the duration of the current session only, or you can import the certificate (or accept it permanently, depending on your browser) in order to prevent this message from appearing in the future.

When the connection is made, the DDM Inventory splash screen and Login window appear.



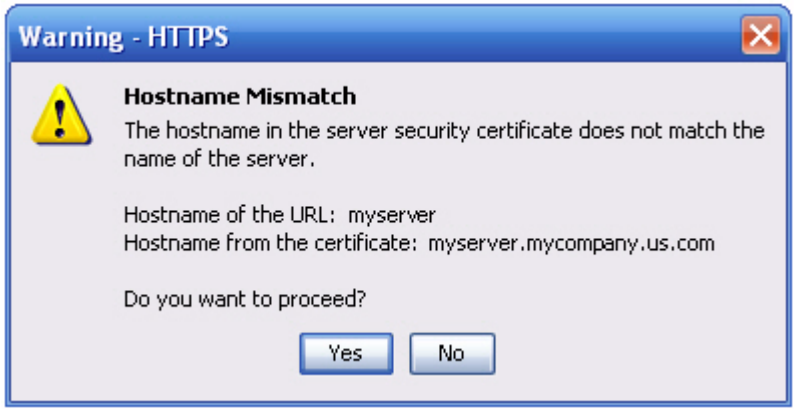
3 Enter the default account name (“admin”) and password (“password”).

Account names are all lowercase. Passwords are case-sensitive. For example, “PASSWORD” and “password” are two different passwords.

Once the account name and password are accepted, the DDM Inventory Home page appears.

- After the Home page appears, your browser may display another security message. If this happens, allow DDM Inventory to proceed. If you want to prevent this message from appearing in the future, select the option to always trust content from this publisher.

- If the URL that you specified when you started the DDM Inventory web UI was different than the DNS name that you specified during the installation (see page 27), a message like this will appear:



  This happens, for example, if you specify the IP address of the DDM Inventory server in the URL—or if you specify the fully-qualified host name in one place and the simple name in the other. Again, the exact content and format of the message depends on your browser.

  If such a message appears, allow DDM Inventory to proceed.

  If you want to prevent this message from appearing in the future, be sure to specify the host name of the DDM Inventory server in the URL using the same format that you used during the installation.

4 Change the password for the “admin” account. For detailed instructions, refer to Change the Default Admin Password on page 167.

Troubleshooting When Logging In for the First Time

The following scenarios represent common problems that can be easily resolved.

Why can't I connect to DDM Inventory?

If you are unable to access DDM Inventory using your web browser, check the following:

- Is the URL correct?
- Is there a firewall in place that is blocking port 80 or 443 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 DDM Inventory server fails to respond, contact your Customer Support representative for further assistance.

The Login did not appear.

- Click the DDM Inventory splash screen.

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

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

I can connect to the DDM Inventory 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 DDM Inventory server are on opposite sides of your corporate firewall. You should see a dialog box that explains that DDM Inventory 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 DDM Inventory 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 DDM Inventory 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.

* If you can log into the DDM Inventory server, you can use the System Panel to troubleshoot problems with ports or services. See Using the System Panel on page 37.

Understanding the Home Page

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

Discovery Status	
Devices Discovered	449
Percentage of Device License	4%
Ports Discovered	1,263
Percentage of Port Capacity	0%
Devices Inventoried	1
Percentage of Device Inventory License	0%
Devices with Agents	1
Recent Device Add Events	8
Recent Device Delete Events	23
Recent Device Change Events	6

Click blue numbers and words for more detailed information

Discovery Server Configuration	[help]
Discovery Configuration Ranges	6

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

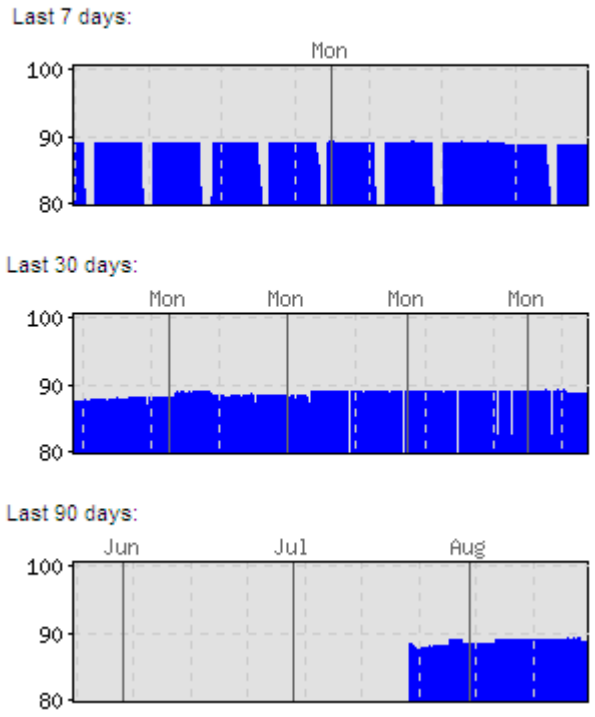
Exceptions	[show] [help]
No Real Connections	1
Duplicate Management IP	6
Unmanaged NCD	7
Reverse DNS Lookups Point To Multiple DNS Addresses	6
Managed Devices With No Ports	35
Switch Has Duplicate MACs	5
Unmanaged NCD with CDP	5
Missing Information	134

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

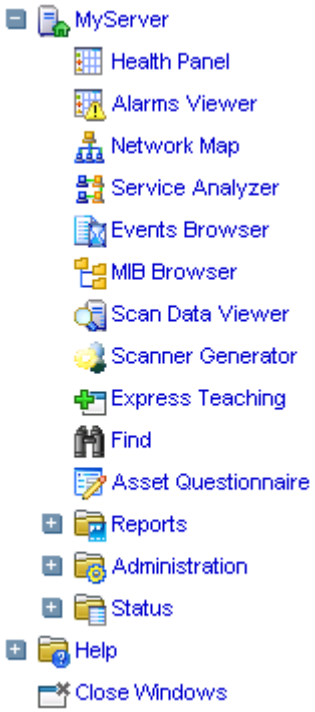
The following information is displayed in the main (center) portion of the Home page:

Table Name	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 DDM Inventory software.
Exceptions	This table displays the most important Exceptions seen in your network. For a complete list of Exceptions, check the Alarms Viewer.

You will see three Network Availability charts on the right side of the home page. These charts show you the percentage of your network devices that have been scanned on-time over the last seven days, thirty days, and ninety days:



You can use the links in the left navigation menu to access the features of the DDM Inventory web interface:



Accessing the Windows Components

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

To access the DDM Inventory Windows components:

1 Click **Start > All Programs > Hewlett-Packard > DDM Inventory 7.70**.

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

- Documentation
- Help
- Analysis Workbench
- Autopass
- SAI Editor
- System Panel
- Viewer

What Next?

To	Go to
Configure the server	Chapter 8, Configuring Your DDM Inventory Server

8 Configuring Your DDM Inventory Server

In this chapter, you will learn how to configure your DDM Inventory server.

Introduction

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

To configure your server, log in to the Web Interface as described in Getting Started with DDM Inventory on page 51, and then complete the following procedures:

- Enter the SMTP Server on page 63
- Enter a Server Name on page 63
- Enter the Administrator E-mail Address on page 63
- Enter the Server Host Name on page 64

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

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

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

Change

Enter the SMTP Server

An SMTP server handles standard Internet e-mail. DDM Inventory 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 DDM Inventory 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 DDM Inventory 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 DDM Inventory 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 DDM Inventory 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: DDM Inventory at Server
[mailto:email.address.not.configured@HP.Inventory]
```

To enter the DDM Inventory Administrator e-mail address:

- Enter the e-mail address of the DDM Inventory Administrator.

Enter the Server Host Name

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

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 10, Configuring the Discovery Process
Create SNMP profiles	Chapter 10, Configuring the Discovery Process
Create Agent profiles and Agent deployment accounts	Chapter 10, Configuring the Discovery Process and Chapter 11, Setting Up Agents and Scanners
Create Scanner profiles and Scanner schedules	Chapter 10, Configuring the Discovery Process and Chapter 11, Setting Up Agents and Scanners
Set up device groups, and assign your profiles to these groups	Chapter 10, Configuring the Discovery Process
Optional: Create custom scanners	"Scanner Generator" in the *Configuration and Customization Guide*
Optional: Enable multiple XML Enricher services	"XML Enricher" in the *Configuration and Customization Guide*

9 Discovery Quick Start Scenario

In this chapter, you will learn how to quickly set up DDM Inventory 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 10, Configuring the Discovery Process.

Introduction

DDM Inventory 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 DDM Inventory 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.

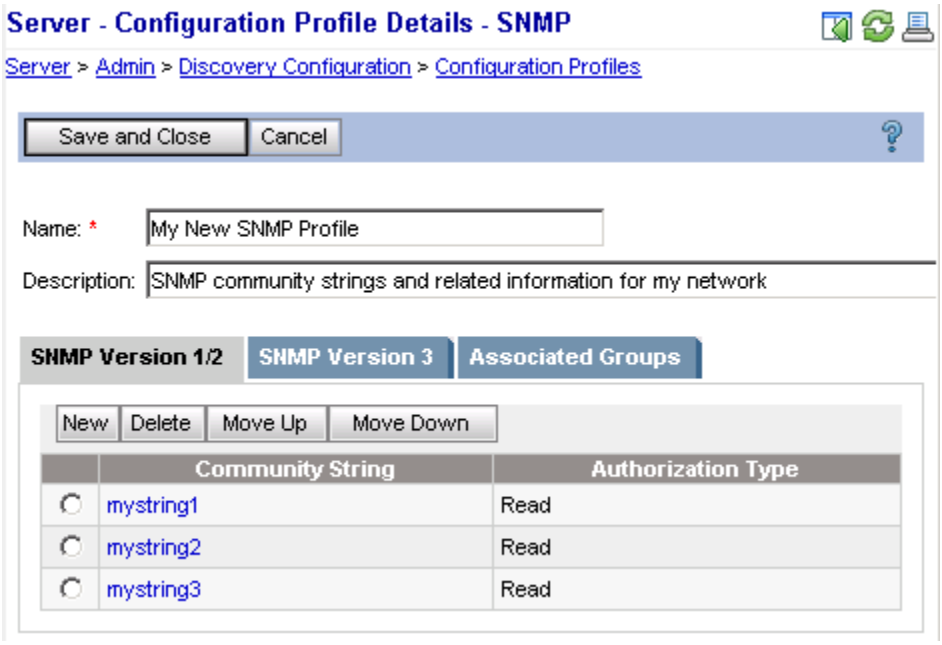
After you have a better idea of what your network contains, you can fine-tune your discovery configuration by setting up customized device groups and configuration profiles. This is covered in Chapter 10, Configuring the Discovery Process.

Set Up an SNMP Profile

If you provide the correct SNMP information, DDM Inventory 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 > 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. For example:



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 DDM Inventory 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 This	Take These Steps
Little about the contents of your network, and you're not sure where to begin	Run Router Discovery on page 67.
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 68. You can also Set Up an IP Range Device Group to Avoid on page 70 and Configure Discovery for DHCP Servers and Unmanaged Routers on page 71.

Run Router Discovery

You can use Router Discovery to automatically locate the SNMP-managed routers and subnets in your network. DDM Inventory will give you a list of routers that it finds, and you can use that list to define device groups.

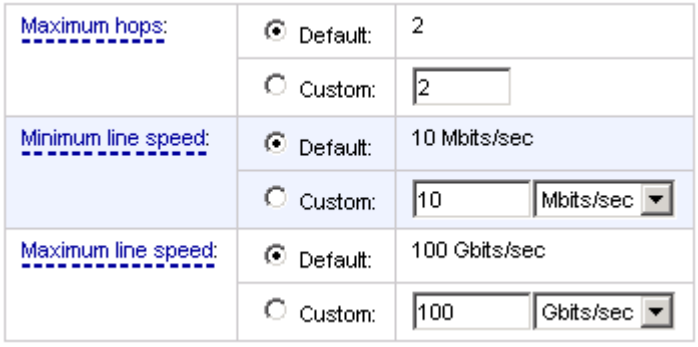
Router Discovery only runs when you initiate it. This is not a continuous process. Also, you must specify or create an SNMP profile that contains the correct SNMP access information—either community strings or user names and pass phrases. If you do not provide this information, Router Discovery will 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 68.

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 DDM Inventory 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 that 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**.

5 Click **Activate Changes** to add the new IP range device group to the database.

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 DDM Inventory 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:

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

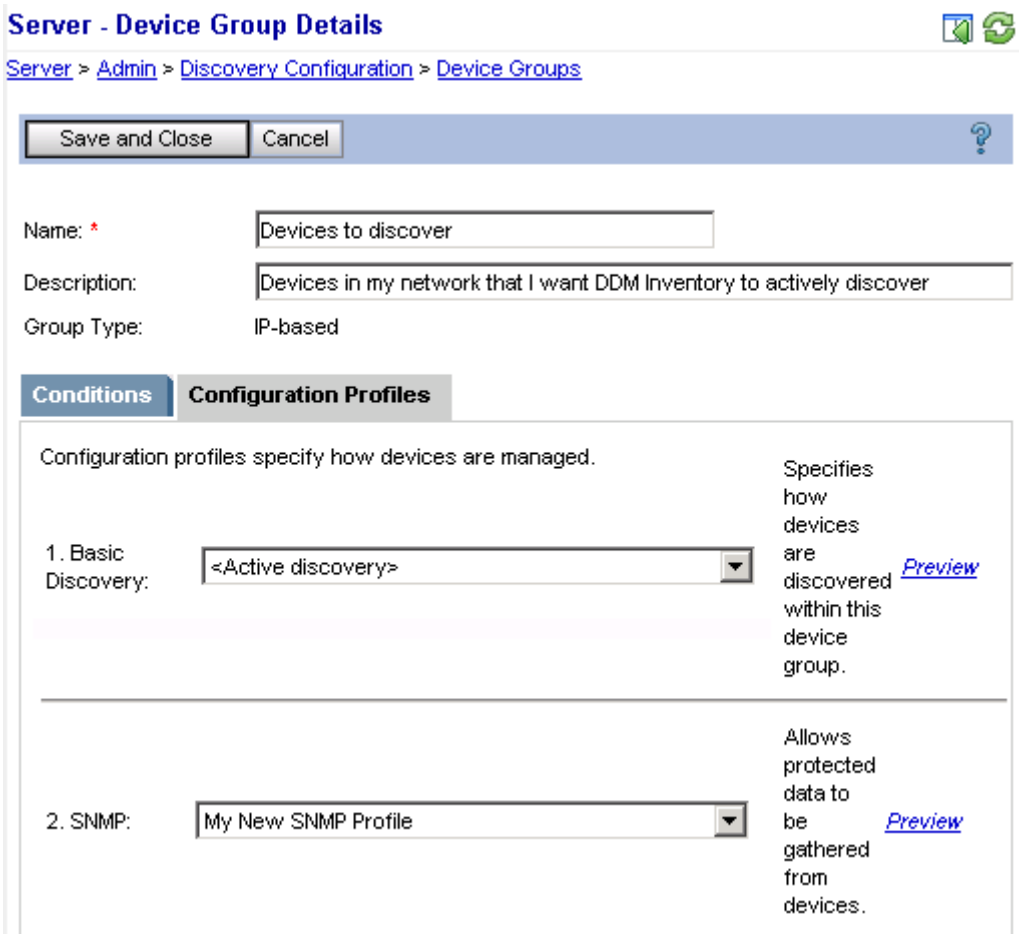
Create an IP Range Device Group

For each subnet in your network that you want DDM Inventory 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 101 for more information.
8. Click **Continue**.
9. Click the **Configuration Profiles** tab.
10. From the **Basic Discovery** profiles list, select <Active Discovery>.
11. From the **SNMP** profiles list, select the profile that you created on page 66. For example:



You can associate other configuration profiles with your device group, but this is not necessary to begin discovering your network devices.

12 Click **Save and Close**.

Repeat this procedure for each IP range device group that you want DDM Inventory to discover.

13 Activate your changes. See Activate Your Pending Changes on page 71 for details.

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 DDM Inventory to avoid, add a new IP range device group.

To avoid a range of IP addresses:

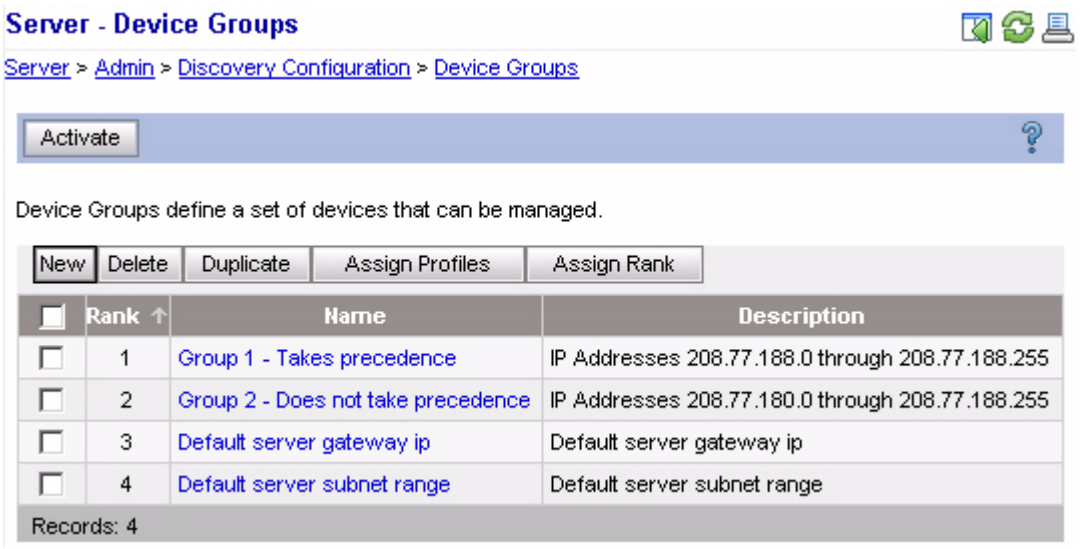
1 Create a new IP range device group for the IP range that you want to avoid. Follow steps 1–9 under Create an IP Range Device Group on page 68.

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

3 Click **Save and Close**.

4 On the **Administration** > **Discovery Configuration** > **Device Groups** page, be sure that your new device group takes precedence over any other device groups that are configured for active discovery and contain any of the same IP addresses.

As shown here, a device group with a lower device group Rank number takes precedence over any group with a higher number:



5 Repeat steps 1–4 for each IP range device group that you want DDM Inventory to avoid.

6 Activate your changes. See Activate Your Pending Changes on page 71 for details.

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 DDM Inventory 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 101 for more information.
3. For each DHCP server, add a Single IP condition.
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 profile.

   See Setting Up Discovery Configuration Profiles on page 95 for more information.
5. Click **Save and Close**.
6. Activate your changes. See Activate Your Pending Changes on page 71 for details.

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 a Single IP condition.
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 profile.
5. Click **Save and Close**.
6. Activate your changes. See Activate Your Pending Changes on page 71 for details.

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 > Activation**.

2 Review the information on each of the tabs on the Activation 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 114.

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 many community strings for security reasons and want to set up separate ranges for them. You can have DDM Inventory treat certain device groups—or individual devices, for that matter—differently than others.

DDM Inventory enables 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.

DDM Inventory actually works harder when it doesn't find devices than when it does, because it keeps trying. Once DDM Inventory 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 DDM Inventory 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 DDM Inventory to treat them.

To	Go to
Learn more about discovery configuration	Chapter 10, 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 DDM Inventory Aggregation

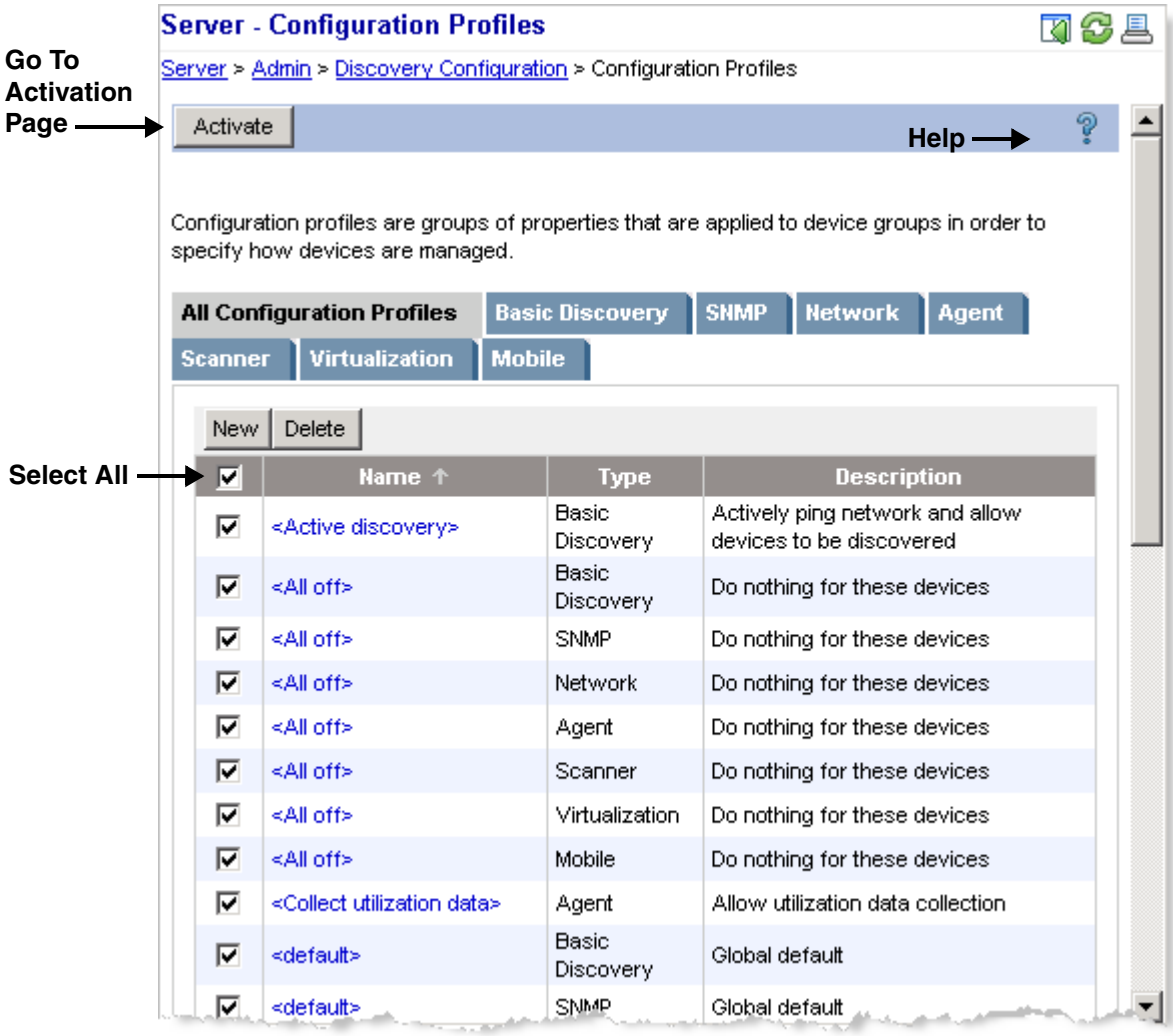
10 Configuring the Discovery Process

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

DDM Inventory supports both the IPv4 and IPv6 network layer protocols. All IP addresses, range, and subnet fields referenced in this chapter are shown in IPv4 format.

Notation and Navigation

In the DDM Inventory 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. You can also duplicate a system defined item to create a copy that you can modify.



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

DDM Inventory 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 DDM Inventory.
- **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 seven types of configuration profiles.

- Basic Discovery profiles specify how DDM Inventory finds devices to manage.
- SNMP profiles specify how DDM Inventory should access an SNMP-managed device in order to gather additional information, such as the type of device or its location. SNMP profiles contain SNMP community strings for SNMP Version 1/2, user names for SNMP Version 3, and related security settings.
- 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, communication preferences, and communication credentials.
- Scanner profiles specify when devices should be scanned, how they should be scanned, how the data should be returned to DDM Inventory, and whether or not to run pre-scan and post-scan scripts.
- Virtualization profiles specify when and how often DDM Inventory discovers virtual devices such as VMware virtual machines. They also specify VMware credentials and whether to gather detailed information of VMware hosts and virtual machines.
- Mobile profiles specify how DDM Inventory collects information about mobile devices in the network. This includes how often, when, and on which port mobile device servers are queried. Mobile profiles also include logon credentials for mobile device servers.

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.

Purpose of Configuration Profiles

Configuration profiles control the kind of information that DDM Inventory can obtain from your network devices. You can use profiles to determine where DDM Inventory will distribute Agents, run Scanners, and precisely how it will access your network devices. By setting up

different configuration profiles, you can instruct DDM Inventory 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 DDM Inventory 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 98 for descriptions of all system defined profiles.

Default Configuration Profiles

A collection of default configuration profiles are provided with your DDM Inventory 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 seven 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 DDM Inventory adds devices that it discovers within this device group to the database. If this option is **Off**, all the subsequent options in the Basic profile are disabled.

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, DDM Inventory 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.

SNMP Profiles

DDM Inventory 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, DDM Inventory 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 DDM Inventory 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.
Device modeler interval	2 days	2 days	Determines how frequently DDM Inventory updates the devices in the network.

Agent Profiles

Agent profiles tell DDM Inventory how to deploy Agents to devices in the network and how to collect information from the Agents. Agent profiles also tell DDM Inventory what login credentials to use when communicating with servers or workstations in the network.

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.

Agent Option	New Profile Default Value	<default> Profile Value	Description
Agent deployment actions	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.
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>	<default>	These are the same schedules used for Scanner distribution. You can create your own at **Administration > Discovery Configuration > Schedules**. This option is only meaningful if **Allow agent upgrade** is on.
Collect utilization data	Off	Off	Determines whether DDM Inventory collects software utilization data from the Agent. This option only appears when the Software Utilization license is installed. For the customers of previous versions who do not have this option enabled, contact your HP Account Representative for assistance.

Agent Option	New Profile Default Value	<default> Profile Value	Description
AUM agent migration *Note: Earlier versions of AUM were called Radia Usage Manager (RUM)* For more information about this migration process, refer to Appendix: Migrating Data from HP Client Automation Application Usage Manager on page 179	None	None	This option determines the specific action to take for this device group in the process of migrating data from HP Client Automation (HPCA) Application Usage Manager (AUM) to DDM Inventory. This option is only available when the **Collect utilization data** option is selected. If you select **Stop AUM agent and migrate data**, the following actions are taken: 1 The AUM agent is requested to stop collecting data. 2 The AUM usage data on each client system is converted to an XML format that DDM Inventory can read. 3 The data is then imported into the DDM Inventory database. The AUM agent is then left in suspended mode. This is useful in the event that an HPCA Configuration Server is controlling the presence of the AUM agent, as it will prevent cyclic reinstallation of the AUM agent. If you select **Uninstall AUM agent and clean up old data**, DDM Inventory will remove both the AUM agent and the pre-migration AUM usage data from each client system in this device group. This is useful when you have completed the necessary changes to the HPCA Configuration Server Database and can safely upgrade and uninstall the AUM agent.

Agent Option	New Profile Default Value	<default> Profile Value	Description
Anonymization	Off	Off	To ensure privacy, you can instruct DDM Inventory not to collect any or all of the following items when it collects software utilization data: • User names • Domain names • Device information • Usage data These options only appear when **Collect utilization data** is selected. In the Scan Data Viewer and software utilization reports, user names and domain names that are anonymized are listed as "Any User" and "Any Group" respectively. Anonymized usage data is reported as a random number of minutes. Selecting **Device information** disables all usage collection for the device
Allow agentless scanning	Off	Off	This option enables agentless inventory. This method of scanning does not install an Agent on the remote system. Instead, it creates a network connection to the remote system, copies a scanner executable to that system, runs the scanner, and transfers the resulting scan file (and log file, if pertinent). See Two Types of Scanning: Agent-Based and Agentless on page 119 for more information.

Agent Option	New Profile Default Value	<default> Profile Value	Description
Remove scan data	Off	Off	This option pertains only to agentless scanning. If enabled, this option instructs DDM Inventory to remove the files used to perform the scan from the remote system immediately after the results of the scan have been transferred to the server. If this option is not enabled, the files are removed the next time that the operating system automatically cleans up its temporary directories. Agentless scanning does not delete the following: • Files and subfolders generated by user scripts running during the pre-scan or post-scan process. • Subfolders uploaded by users during the pre-scan or post-scan process. Note that after the scan data files are deleted, delta scanning is no longer available. Even if the **Enable delta scan files** option is set in the scanner configuration, a full scan will be performed.
Accept new public client key	Off	Off	This option pertains only to agentless scanning on new UNIX/Linux/Mac OS X systems using SSH. If you select this option, DDM Inventory will accept the public SSH key of a newly discovered device with this profile and initiate an agentless scan. See How Is the Secure Connection Made for Agentless Scanning? on page 123 for more information.

Agent Option	New Profile Default Value	<default> Profile Value	Description
Accept changed public client key	Off	Off	This option pertains only to agentless scanning on UNIX/Linux/Mac OS X systems using SSH for which a public key is already known (systems that have already been scanned). If you select this option, DDM Inventory will accept a public SSH key that has been modified on a client system and, therefore, does not match the key that was previously used to scan that system. NOTE: Selecting this option creates a low-security environment. Select this option only under controlled conditions. See How Is the Secure Connection Made for Agentless Scanning? on page 123 for more information.
Limit bandwidth for data transfers	Off	Off	The maximum bandwidth that will be used when communicating with a single device when sending the Scanner executable file or retrieving the scan file. If you select this option, you must specify a value for the bandwidth limit that is greater than zero. If you do not select this option, DDM Inventory will use whatever bandwidth is available.
Communication credentials for Windows	None	None	This table lists the credentials that DDM Inventory will use to communicate with Windows clients that belong to device groups to which this profile is assigned. See Setting Up Deployment Credentials on page 104 for more information.
Communication credentials for SSH	None	None	This table lists the deployment credentials that DDM Inventory will use to communicate with UNIX/Linux/Mac OS X systems using SSH. These systems must belong to device groups to which this profile is assigned. See Setting Up Deployment Credentials on page 104 for more information.

Scanner Profiles

Scanners run on your network devices and send back scan files to the DDM Inventory server for processing and storage. After a scan file is delivered to the server, the XML Enricher processes the scan file, adding application data.

You also have the option of running pre-scan and post-scan scripts. This option enables you to customize and execute scripts on scanned devices as part of the DDM Inventory scanning process.

Scanner profiles determine if and how often Scanners run on devices in the network, how often the Scanners are upgraded, how often the Scanner data is sent back to the server to be processed, and whether or not to run pre-scan and post-scan scripts.

Before you set up your Scanner profiles, you should think about when you want the Scanners to run on your network. DDM Inventory gives you complete control over the scanning schedules. You can configure when you want DDM Inventory to perform the following actions:

- Scanner Upgrade
- Scanner Run
- Scan File Transfer

For example, you could set it up so that Scanners are upgraded on Monday, Scanners run on Tuesday, and the scan files are transferred to the server on Wednesday. To establish a schedule for your scanning activities, you must first create that schedule (or use an existing schedule) and then specify that schedule in your Scanner configuration profiles.

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 > Discovery Configuration > Schedules page.
Run the scanner using this schedule	<All the time>	<default>	When Scanners should be run on devices within this device group.
Transfer 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.
Run pre-scan and post-scan scripts	Off	Off	Determines if Scanners run pre-scan and post-scan scripts before and after scanning. For detailed information, refer to the “Pre-Scan and Post-Scan Scripts for Collecting Custom Hardware Data” section in the *Configuration and Customization Guide*.
Allow scanners to be upgraded	On	On	This must be set to for the Scanners to be automatically upgraded from the server.

Scanner Option	New Profile Default Value	<default> Profile Value	Description
Scanner configuration	Use one scanner configuration: <default>	Use one scanner configuration: <none>	You can specify a specific Scanner configuration for each supported operating system, or you can use one configuration for all operating systems. To create, modify, or delete a Scanner configuration, see Setting Up Scanner Configurations on page 111.

Virtualization Profiles

A virtualization profile enables you to specify three items: (1) VMware credentials, (2) Inventory VMware hosts, and (3) 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.
Inventory VMware hosts	On	On	Whether to gather detailed information of the VMware host and virtual machines.
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.

Mobile Profiles

A mobile profile enables you to specify four things:

- Mobile device server credentials
- Which port on the mobile device server (or servers) should be used to discover and inventory mobile devices
- How often and when mobile devices should be discovered
- How often detailed inventory information about each mobile device should be collected

Mobile Options	New Profile Default Value	<default> Profile Value	Description
Mobile discovery interval	None	None	How often the list of mobile devices is retrieved from the mobile device server (or servers).
Mobile inventory interval	None	None	How often detailed information about each mobile device is retrieved from the mobile device server (or servers).
Discover mobile devices using this schedule	<All the time>	<default>	When the discovery and inventory processes for mobile devices are initiated.
Mobile port number	7001 for HTTP connections 7002 for HTTPS connections	7001	Port on which the mobile device server (or servers) should be queried. NOTE: When configuring your mobile device server, do not use ports lower than 1024.
Use HTTPS to connect to mobile server	Selected	Selected	Protocol that DDM Inventory will use to communicate with your mobile device servers. If this communication will happen over a non-secure network, use HTTPS. If this option is not selected, HTTP is used.
Mobile credentials			User name, password, and password hint for the mobile device server (or servers).

DDM Inventory Server and Automatic Configuration

When you configure devices through profile attributes, it is important to understand that the DDM Inventory server device, itself, represents a special case. Regardless of the values that you assign to the configuration attributes in the profiles that are assigned to the device group containing the DDM Inventory server, some of these attributes will be reconfigured automatically.

When the HP DDMI Discovery Engine service starts, it loads configuration settings for every device. However, the DDM Inventory server is treated differently. The Discovery Engine changes many configuration settings affecting DDM Inventory server discovery—it creates a device group and profiles "on the fly" that are not saved in the database but are used to keep the configuration settings for the DDM Inventory server. The Discovery Engine creates the new settings by inheriting the settings from the profiles originally assigned to the group to which the DDM Inventory server belongs as an independent device. Some of these settings are kept, but many are modified.

Since the configuration settings are different and have been automatically adjusted by the Discovery Engine, the DDM Inventory server group and its profiles are referenced in the Device Manager as `<automatic configuration>`.

The best way to determine which DDM Inventory server settings were modified is to review the settings in the Device Manager in the Discovery Configuration table on the Diagnosis page. For additional information, refer to the "Using the Device Manager" chapter in the *Network Data Analysis Guide*.

If there is a profile for the group that contains the DDM Inventory server that exhibits all the settings necessary for DDM Inventory server configuration, the server may use this profile and not the `<automatic configuration>` one.

If the DDM Inventory server has multiple SNMP community strings, regardless of the SNMP profile assigned to its group, the DDM Inventory server will always select the first community string in the Windows SNMP credentials configuration.

As a specific example, say that the device group containing the DDM Inventory server has been configured with the following settings:

- No ping
- No scanning
- No resource polling
- No SNMP
- Only public community string

When the Discovery Engine starts, it will change the settings for the DDM Inventory server such that ICMP ping is turned on, scanning is turned on, resource polling is turned on, SNMP is turned on, and community strings are read from the registry and used for SNMP modeling.

Device Groups

Device groups determine what devices are discovered by DDM Inventory. Device groups are defined by IP addresses, device types, or both (see How Device Groups are Defined on page 88). Configuration profiles are assigned to device groups. These profiles specify how the devices in the group are managed by DDM Inventory.

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

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, DDM Inventory 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 200.12.*.*

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

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

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

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

There are two kinds of device groups: IP-only device groups and device type groups.

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.

You must exercise caution when using a wildcard in the class C range (a.b.*.d) of an IP address because it is possible to exceed the 2000 device range limitation. A wildcard in the class C range represents 256 ranges. If you use 8 wildcards in this position (8 x 256 = 2048), you will exceed the 2000 device range limitation.

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.

When you create a new device group or modify an existing one, you can enter IP addresses and ranges manually, or you can instruct DDM Inventory to read them from a text file. An IP address file must have one of the following two formats:

- Three column format—explicitly indicates the type of IP address data. In this case, the columns should be separated by tabs. For example:

```
Type            IP1             IP2
Single          208.77.188.166
Range           208.77.188.0    208.77.188.255
SubnetMask      208.77.188.0    255.255.255.0
SubnetMask      208.77.188.0    24
Wildcard        208.77.188.*
```

- One column format—type inferred from the format. Use a hyphen (-) to indicate a range and a slash (/) to indicate a subnet mask. For example:

```
IP
208.77.188.166
208.77.188.0-208.77.188.255
208.77.188.0/255.255.255.0
208.77.188.0/24
208.77.188.*
```

After DDM Inventory reads your file, it adds a new IP-only condition to the device group for each row in the file.

In the case of an existing device group, DDM Inventory will merge the imported and existing IP-only conditions together. It will not import an IP address or range that exactly duplicates an existing condition for this device group. It will, however, import IP ranges that overlap with existing ranges.

You must save your changes and activate them in the usual way to add the new conditions to the database. After you activate your changes, any overlapping IP ranges are consolidated in the DDM Inventory database.

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 DDM Inventory 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.

Device type groups cannot be used to filter devices.

Using Device Groups

A convenient way to use DDM Inventory 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

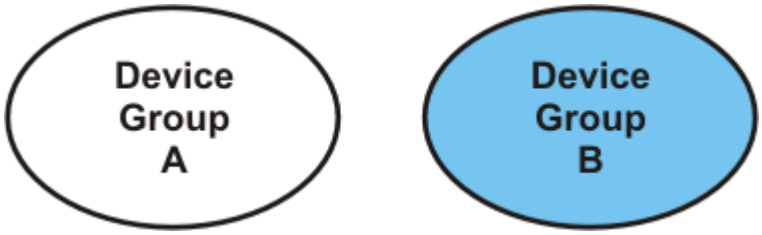
There are multiple ways to assign configuration profiles to device groups. When you initially create a device group, the system defined <default> profile is selected for each applicable configuration profile type.

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.

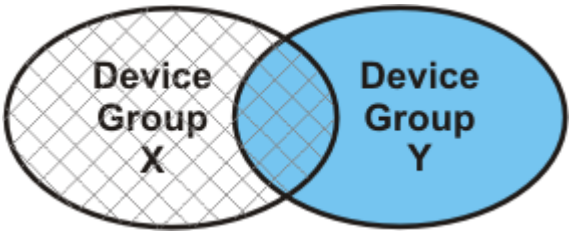
You can only assign Basic Discovery and SNMP configuration profiles to IP-only device groups. Device type device groups do not have Basic Discovery and SNMP profiles. A device within a device type group can only acquire these properties if this device also belongs to an IP-only group. Devices that do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

Potential Conflicts and Device Group Rank

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



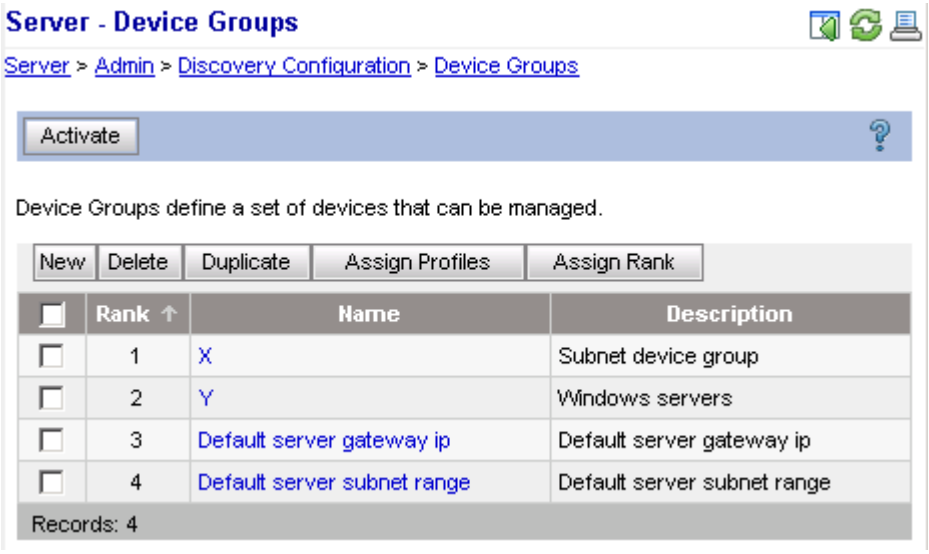
When two or more device groups intersect (contain a common device), the rank of the device groups determines which configuration profiles are applied. In the following example, device group X (cross-hatched area on the left) and device group Y (shaded area on the right) each have conditions that result in at least one device being part of both groups (cross-hatched and shaded area in the center).



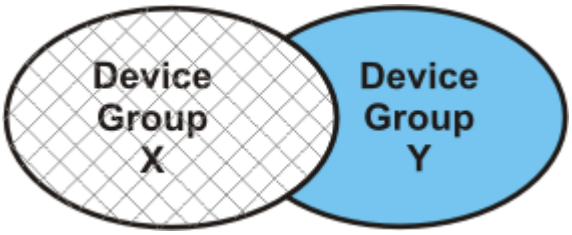
Say that device group X contains devices in a certain subnet, and device group Y contains devices of a particular type—say, Windows servers. In this case, any Windows servers whose IP addresses are in this subnet belong to both group X and group Y.

The problem with this is that DDM Inventory 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 DDM Inventory by ranking your device groups. In the following example, there are four device groups. The highest ranking group has rank "1," and the lowest ranking group has rank "4." In this case, group X outranks group Y and, therefore, takes precedence:



Because device group X takes precedence over device group Y, DDM Inventory 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.

Deployment Credentials

DDM Inventory uses deployment credentials to connect remotely to Windows client systems using the Windows Workstation Service and UNIX/Linux/Mac OS X client systems using Secure Shell (SSH). In both cases, deployment credentials can be used to perform agentless scans. For Windows client systems, deployment credentials can also be used to permanently install an Agent for agent-based scans. You can specify a collection of deployment credentials that are valid for devices in your network. You can then associate one or more sets of these credentials with an Agent configuration profile. DDM Inventory uses these credentials to establish a secure connection with devices that belong to device groups that have this Agent profile.

Deployment credentials include the following information:

Deployment Credential Fields	**New Profile Default Value**	**Description**
Label	None	The label is simply a descriptor that you assign to a particular set of deployment credentials. You can use the labels to manage and organize your collection of credentials. Each label must be unique.
Domain	None	For Windows systems, this is the Windows domain to which the user specified in the Login box belongs. This field is not used for UNIX/ Linux/Mac OS X systems.
Login	None	This is the login name for a user with Administrator privileges on Windows systems, or root privileges on UNIX/Linux/Mac OS X systems, to which these credentials pertain. NOTE: A root level user is the preferred and recommended approach. If this is not possible, be sure to specify a user with a sufficient access privileges. If this user's privileges are insufficient, the scanner may not be able to collect complete inventory information—for example, it will not be able to detect all hardware data or access all files required to perform a software inventory.
Password	None	This is the password for the user specified in the Login box.
Share	ADMIN$	For Windows systems, this is the name of the network share that DDM Inventory will use to copy the scanner executable to the remote machine. This field is not used for UNIX/Linux/ Mac OS X systems.

Deployment Credential Fields	New Profile Default Value	Description
Path	%SystemRoot%	For Windows systems, this is the path name of the folder on the remote machine where DDM Inventory will store the scan files while it performs an agentless inventory. You can specify an explicit path name, or you can specify an environment variable using the *%varname%* format. After the inventory is completed and the scan results are transferred to the DDM Inventory server, these files are removed from the remote machine. This field is not used for UNIX/Linux/Mac OS X systems.

Schedules

Schedules are used to distribute Agents and Scanners, define collection times for scan files, and specify the frequency of virtual and mobile device discovery. You can define your own schedules, or you can duplicate and modify copies of system-defined schedules. Both system and user-defined schedules can be associated with configuration profiles.

Scanner Configurations

Scanners are used to collect hardware and software inventory from the devices on your network. A Scanner consists of two files. One is the Scanner executable itself, and the other is the Scanner configuration file. When Scanners are run in Enterprise Mode, the server maintains a schedule dictating which computers should be scanned and when. In this mode, the Scanners read their configuration settings from a Scanner configuration file. The Scanner configuration can be customized to control how inventory is collected, what information is gathered, and the level of detail to be included.

There are previously defined Enterprise Mode Scanner configurations stored on the DDM Inventory server.

These include the following:

- System predefined Scanner configurations, which cannot be overwritten but can be saved on the server with a new file name
- User-defined configurations that have already been saved to the server

You can select one of these configurations, edit a stored configuration (if system defined, save it with a new name), or create a new one. You can then associate this Scanner configuration with a Scanner profile at the time that you setup the profile.

If you decide to edit an existing Scanner configuration or create a new one, the Scanner Generator is launched. Refer to the “Scanner Generator” chapter in the *Configuration and Customization Guide* for additional information.

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 DDM Inventory on a new server, for example, you can import your configuration data from an existing server.

For security reasons, passwords are not exported.

Activation

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

Pending Changes

DDM Inventory 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 indicates the total number of device groups, configuration profiles, deployment credentials, and schedules that will be affected. It also indicates 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 DDM Inventory 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 75.

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 115 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 gray arrow ( ) 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 76.

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 76.

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 76.

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 device groups 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.

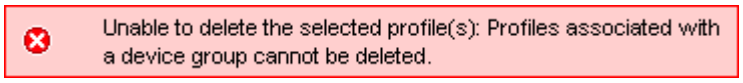
4 Click **Delete**.

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 DDM Inventory 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 76 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>	DDM Inventory does not actively look for devices, but will include them if it happens to find them. (For example, DDM Inventory may be able to gather the information from the ARP cache of a device.)
< 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 77 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. DDM Inventory will attempt to read the MIB of all devices in the device group using only "public."

Network Profiles

See Network Profiles on page 78 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 selected. For routers that do not have SNMP management enabled.
<DHCP Server>	This profile has **Force ARP table read** selected. 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 78 for information about Agent profile options.

Profile	Purpose
<Agentless scanning>	Use agentless scanning instead of deploying the Agent to network devices. See Two Types of Scanning: Agent-Based and Agentless on page 119 for more information.
<All off>	No Agent communication is allowed.

Profile	Purpose
<default>	Allows the Agent to be upgraded using the <default> system defined schedule.
<Deploy agent>, <Global>	Allows Agent communication, and allows the Agent to be upgraded using the <default> system defined schedule.
<Collect utilization data>	Allows the Agent to be upgraded using the <default> 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 83 for information about Scanner profile options.

Profile	Purpose
<All off>, <default>	Do nothing: Do not deploy, upgrade, transfer, or run Scanners, and do not upgrade the Agent.
<Global>	Upgrade or deploy the Scanners (and the Agent, if necessary) every 4 weeks.
<Hardware only>	Use the system defined <hwonly> Scanner configuration for all operating systems. Upgrade or deploy the Scanners (and the Agent, if necessary) every 4 weeks.
<Fast software>	Use the system defined <fastsw> Scanner configuration for all operating systems. Upgrade or deploy the Scanners (and the Agent, if necessary) every 4 weeks.

Virtualization Profiles

See Virtualization Profiles on page 85 for information about Virtualization profile options.

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

Mobile Profiles

See Mobile Profiles on page 86 for information about Mobile profile options.

Profile	Purpose
<All off>, <default>, <Global>	Do not discover mobile 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 88.

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 rank. Click any column header to change the sort parameter or toggle the sort order. The gray arrow ( ) 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.

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, Subnet, or File.
   b. For all IP types except File, type the IP information in the **IP Address** box (or boxes). Click the **Valid IP formats** link for additional tips about how to specify this.

      For the File type, browse to the tab-separated value (TSV) file containing your IP address information. Refer to How Device Groups are Defined on page 88 for information about the format of this file.

   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.

Refer to the **Select Conditions for a Device Group** online help topic for information about adding, modifying, or deleting conditions.

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 **Configuration Profiles** tab.

4 For each profile type that you want to assign, 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 Rank of a Device Group

You can change the rank of any device group relative to the other device groups. The device group with rank "1" is the highest ranking group; the device group with rank "2" is the next highest ranking group, and so on.

To change the relative rank of a device group:

1. Click **Administration > Discovery Configuration.**
2. Click **Device Groups**.
3. Click the **Assign Rank** tab.
4. Select the check box for the device group whose rank you want to change.
5. Click **Move Up** to increase its relative rank; 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.

Setting Up Deployment Credentials

Deployment credentials are used by the DDM Inventory server for Agent/Scanner communication with devices in your network. You can associate one or more sets of deployment credentials with an Agent configuration profile. DDM Inventory will use the credentials associated with this profile to communicate with devices that belong to device groups to which the profile is assigned. For additional information, see Deployment Credentials on page 92.

Create a New Set of Credentials

You can create as many sets of deployment credentials as you like. The order in which the credentials appear in the table on the Deployment Credentials page is not important. You can specify a priority order when you assign the credentials to Agent profiles.

To create a new set of deployment credentials:

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

2 Click **Deployment Credentials**.

3 Click **New**.

4 Click either the **Windows** tab (for Windows clients) or the **SSH** tab (for UNIX/Linux/Mac OS X computers).

5 Specify each of the remote login options:

- Label
- Domain (Windows only)
- Login
- Password
- Share (Windows only)
- Path (Windows only)

6 Click **Save and Close**.

Remember to activate your changes to have them take effect.

Modify an Existing Set of Credentials

When you modify a set of deployment credentials, the password is not displayed. You do not need to enter the password unless you want to change it. If you do enter a password, you must enter it both in the **Password** box and the **Password (Confirm)** box.

To modify an existing set of deployment credentials:

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

2 Click **Deployment Credentials**.

3 Click either the **Windows** tab (for Windows clients) or the **SSH** tab (for UNIX/Linux/Mac OS X computers).

4 Click the **Label** field of the set of credentials that you want to work with.

5 Modify any of the items that you want to change.

6 Click **Save and Close**.

Remember to activate your changes to have them take effect.

Associate a Set of Credentials with an Agent Profile

To instruct DDM Inventory to use deployment credentials to communicate with specific devices in your network, you can assign one or more sets of credentials to an Agent configuration profile and then assign this profile to the pertinent device group (or groups).

To associate deployment credentials with an Agent configuration profile:

1 Click **Administration > Discovery Configuration.**

2 Click **Configuration Profiles**.

3 Click the **Agent** tab.

4 In the list of Agent profiles, click the name of the profile that you want to modify.

5 Click the **Modify** button associated with one of the following tables:

— Communication credentials for Windows

— Communication credentials for SSH (UNIX/Linux/Mac OS X)

6 For each set of deployment credentials that you want to associate with this profile, follow these steps:

a In the **All Credentials** list, select one or more sets of credentials that you want to associate with this profile.

b Click the right arrow () to move these credentials into the **Current Credentials** list.

7 To change the priority order in which the credentials are attempted follow these steps:

a In the **Current Credentials** list, select a set of credentials.

b Choose one of the following actions:

– To move the credentials higher in the list, click the up arrow ().

– To move the credentials lower in the list, click the down arrow ().

– To move the credentials to the top of the list, click the top arrow ().

– To move the credentials to the bottom the list, click the bottom arrow ().

8 To remove credentials currently associated with this profile:

a In the **Current Credentials** list, select one or more sets of credentials.

b Click the left arrow button (). These credentials then move back into the **All Credentials** list.

9 When you are finished modifying the list of credentials, click **OK**.

10 When you are finished making changes to this profile, click **Save and Close**.

Remember to activate your changes to have them take effect.

Delete a Set of Credentials

You can delete any deployment credentials that are not associated with Agent configuration profiles. Be sure to carefully review the implications of your pending changes on the Activation page before permanently deleting a set of credentials, however. Since credentials can be assigned to multiple Agent profiles, there may be effects that you do not anticipate.

To delete a set of deployment credentials:

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

2 Click **Deployment Credentials**.

3 Select the box to the left of each set of credentials that you want to delete.

4 Click **Delete**.

Remember to activate your changes to have them take effect.

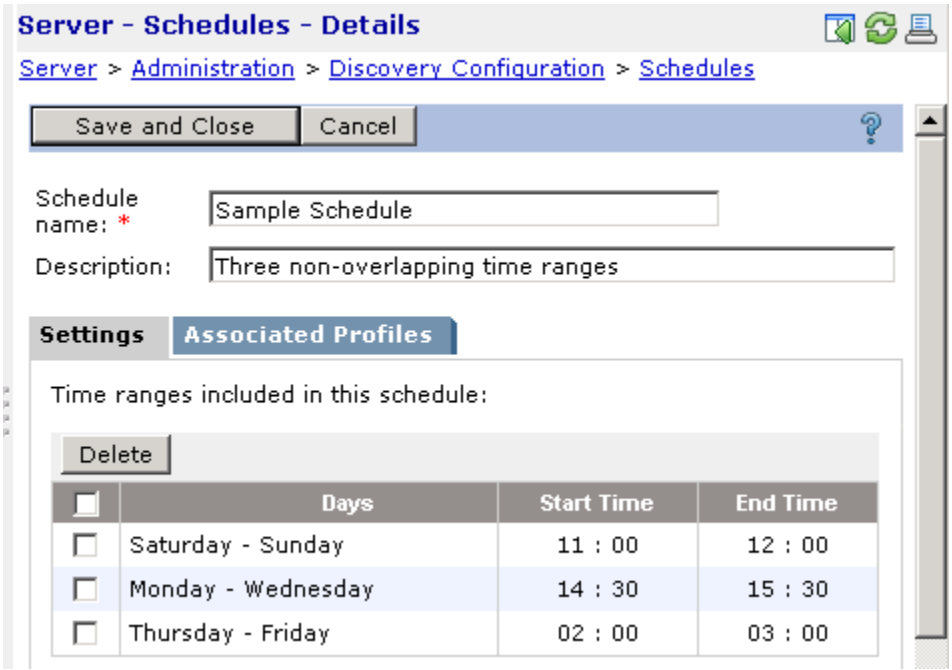
Setting Up Schedules

Schedules are used to distribute Agents and Scanners, define collection times for scan files, and specify the frequency of virtual and mobile device discovery. The following system-defined schedules are provided with DDM Inventory:

- <default>
- <All the time>
- <Weekends>
- <Work hours>
- <Not during work hours>

You can define your own schedules, or you can duplicate and modify copies of system-defined schedules. Both system and user-defined schedules can be associated with configuration profiles.

Schedules consist of one or more time ranges. In the following example, the schedule contains three time ranges:



Schedules can contain overlapping time ranges, but they cannot contain duplicate time ranges. If you attempt to specify a duplicate time range, you will get an error message. You can specify up to 16 time ranges for a particular schedule.

View the List of Existing Schedules

From the Discovery Configuration page, you can display the list of existing schedules. This list contains both system-defined and user-defined schedules.

To view the list of existing schedules:

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

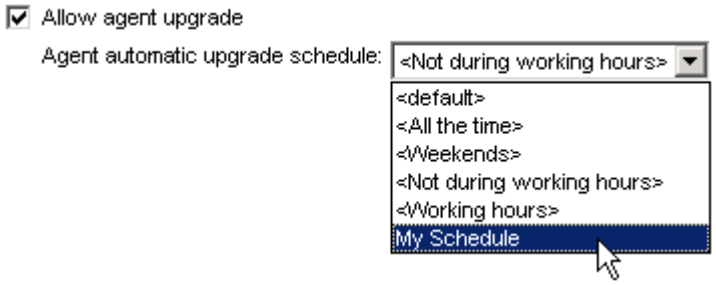
The Schedules page shows a comprehensive list of all available schedules, including both system-defined schedules and customized schedules that you have created. This list is initially sorted by schedule name. To view the details for a particular schedule, click the name of that schedule. Click any column header to change the sort parameter or toggle the sort order. The gray arrow indicates the sort order.

Associate Schedules with Configuration Profiles

The following types of configuration profiles include schedules:

- Agent profiles use schedules to specify when the agents should be automatically upgraded.
- Scanner profiles use them to specify when scanners should be deployed or upgraded, when scanners should be executed, and when scan files should be retrieved.
- Virtualization profiles use them to specify when virtual devices should be discovered.
- Mobile profiles use them to specify when mobile devices should be discovered.

When you create one of these types of configuration profiles, you can choose a schedule from a drop-down list, as shown here:



The drop-down list contains all schedules defined on the Administration > Discovery Configuration > Schedules page. In this example, five of the six schedules listed are system-defined schedules, as indicated by the <schedule name> notation. The last schedule, My Schedule, is a user-defined schedule.

Determine Configuration Profiles Associated with Each Schedule

After you create profiles and associate schedules with them, you can view a list of profiles that are associated with each schedule.

To view a list of profiles associated with each schedule:

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

Modify an Existing Schedule

You can modify any schedule that is not a system-defined schedule.

To modify a schedule:

1. Click **Administration** > **Discovery Configuration**.
2. Click **Schedules**.
3. In the list of schedules, click the name of the schedule that you want to modify.
4. For each new time range that you want to add, follow these steps:
   a. From the **From** list, select the day on which you want the time range to start.
   b. From the **Through** list, select the day on which you want the time range to end.
   c. In the **From** boxes for the time range, specify the time that you want the range to start. Use 24-hour time notation. For example, 8:00 AM would be 08:00, and 2:30 PM would be 14:30.
   d. In the **To** boxes for the time range, specify the time that you want the range to end.
   e. Click **Add**.
5. If you want to delete one or more existing time ranges, follow these steps:
   a. In the time ranges table, select the check box that corresponds to the time range (or ranges) that you want to delete.
   b. Click **Delete**.
6. If you want to modify an existing time range, you must first delete that range and then add a new one.
7. When you are finished making changes, click **Save and Close.**

Remember to activate your changes to have them take effect.

Define a New Schedule

You can add a new schedule at any time. You can then associate that schedule with configuration profiles that specify schedules (Agent, Scanner, Virtualization, and Mobile profiles).

To define a new schedule:

1. Click **Administration** > **Discovery Configuration**.
2. Click **Schedules**.
3. Click **New**.
4. In the **Schedule name** box, type a unique name for your schedule.
5. *Optional:* In the **Description** box, type additional information about this schedule.
6. For each time range that you want to add, follow these steps:
   a. From the **From** list, select the day on which you want the time range to start.
   b. From the **Through** list, select the day on which you want the time range to end.
   c. In the **From** boxes for the time range, specify the time that you want the range to start. Use 24-hour time notation. For example, 8:00 AM would be 08:00, and 2:30 PM would be 14:30.
   d. In the **To** boxes for the time range, specify the time that you want the range to end.

7 Click **Add**.

8 To save this schedule and return to the Schedules page, click **Save and Close**.

Remember to activate your changes to have them take effect.

Duplicate a Schedule

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

To duplicate a schedule:

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

2 Click **Schedules**.

3 Select the check box for the specific schedule that you want to duplicate. Note that only one schedule can be duplicated at a time.

4 Click **Duplicate**.

5 In the **Schedule Name** box, type a unique name for the new schedule.

6 *Optional:* In the **Description** box, type additional information about this duplicated schedule.

7 *Optional:* Add or modify any time ranges that you want to change. See Modify an Existing Schedule on page 108 for detailed instructions.

8 To save this schedule and return to the Schedules page, click **Save and Close**.

Remember to activate your changes to have them take effect.

Delete a Schedule

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

If a schedule is associated with a configuration profile, you cannot delete that schedule. You must first break the association by selecting a different schedule for that profile. You will then be able to delete the original schedule.

To delete a schedule:

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

2 Click **Schedules**.

3 In the list of schedules, select the check box for each schedule that you want to delete.

4 Click **Delete**.

5 Review the list of proposed deletions. If you selected any system-defined schedules in step 3, these schedules will not appear in the list.

If the list of schedules to be deleted matches what you want to delete, click **Continue**. One of the following two things happens next:

- If none of the schedules in the list are assigned to configuration profiles, you return to the main Schedules page.
- If one or more of the schedules is assigned to a profile, an error message appears. In this case, you must determine which schedule (or schedules) in your list is attached to a profile and assign a different schedule to that profile. Then, you can attempt the delete operation again.

Remember to activate your changes to have them take effect.

Setting Up Scanner Configurations

This section provides detailed instructions for creating, modifying, and deleting Scanner configurations that are stored on the DDM Inventory Server. For an overview of Scanner configurations, see Scanner Configurations on page 93.

Refer to the "Standard Configuration Page" section in the "Scanner Generator" chapter of the *Configuration and Customization Guide* for more information about stored Scanner configurations.

Create a Scanner Configuration

If you do not want to use the Scanner configurations already stored on the DDM Inventory server, you can create a new one.

To create a scanner configuration:

1. From the home page, click **Administration** > **Discovery Configuration**.
2. Click **Scanner Configurations**.
3. Click **New**. This launches the Scanner Generator.
4. Follow the steps in the Scanner Generator as described in the "Scanner Generator" chapter in the *Configuration and Customization Guide*. The new Scanner configuration is stored on the DDM Inventory server.

Edit a Scanner Configuration

You can edit an existing Scanner configuration already stored on the DDM Inventory server. If you want to edit a system predefined scanner configuration, the Scanner Generator interface will instruct you to save the configuration with a new name on the last page of the interface.

To edit a scanner configuration

1. From the home page, click **Administration** > **Discovery Configuration**.
2. Click **Scanner Configurations**.
3. Click the name link of the Scanner configuration that you want to modify. This launches the Scanner Generator in the context of the selected scanner configuration.

4 Follow the steps in the Scanner Generator as described in the “Scanner Generator” chapter in the *Configuration and Customization Guide*. The modified Scanner configuration is saved on the DDM Inventory server.

Delete a Scanner Configuration

If you want to preform some general cleanup of stored Scanner configurations, you can delete Scanner configurations stored on the DDM Inventory server. You cannot delete system predefined Scanner configurations

To delete a scanner configuration

1 From the home page, click **Administration** > **Discovery Configuration.**

2 Click **Scanner Configurations**.

3 Check the box next to the Scanner configurations that you want to delete.

4 Click **Delete**. The Delete window opens displaying the Scanner configurations that you have selected for deletion. If you have selected a system predefined Scanner configuration or a Scanner configuration that is already in use, it will not be displayed nor will it be deleted.

5 Click **Continue**. The valid selected Scanner configurations are removed from the DDM Inventory server.

Importing and Exporting Discovery Configuration Information

The import and export functions provide a convenient way to backup your configuration so that it can be restored on another server. The export function stores your configuration in a tab-separated value (TSV) file. The import function reads configuration information from a TSV file and stores it in the DDM Inventory database upon activation.

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

Export Your Configuration Information to a TSV File

You can export your discovery configuration information to a tab-separated value (TSV) file as a way of keeping an external record of your configuration information. This is useful, for example, if you are setting up a new DDM Inventory server and you want to use existing discovery configuration information from another server. It is also useful if you want to use configuration information from an earlier version of DDM Inventory.

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.

5 Save the file.

By default, the name of the TSV file is as follows:

`DiscoveryConfiguration_<serverName>_<year>_<month>_<day>.tsv`

For example: `DiscoveryConfiguration_MyServer_2008_01_01.tsv`

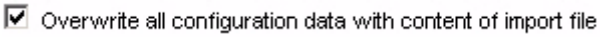
Depending on how your browser is configured, you may not have the opportunity to specify the name and location for this file. If your browser is set up to store all downloaded files in a single folder, for example, the TSV file will be stored there.

For security reasons, passwords used in VMware, mobile, and agent credentials are not exported. If you plan to import this configuration information at some point after you export it, you will need to replace the passwords in your Virtualization, Mobile, and Agent profiles after the import (or manually add them to the TSV file prior to the import).

Import Configuration Information from a TSV File

You can import discovery configuration from a TSV file. This is useful, for example, if you are setting up a new DDM Inventory server and you want to use existing configuration information from another server—or if you want to import data that you saved from an earlier version of DDM Inventory.

The following option ensures that the imported configuration data replaces all existing data:



When this option is selected, the existing configuration will be erased (except for any system-defined data). When it is not selected, the imported data is added to the existing configuration. In this case, there cannot be any name conflicts between the imported information and the existing information. This includes profile names, device group names, schedule names, agent credential names, and scan configuration names.

The **Overwrite** option is selected by default. It is best to leave it selected to ensure that the configuration you import is exactly the same as it is on the server where you exported it.

For security reasons, passwords for VMware, mobile, and agent credentials are not exported. After you import configuration information, you will need to replace the passwords in your Virtualization, Mobile, and Agent, profiles.

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**.

Remember to activate your changes to complete the import process.

Although there is no “undo” option available after the activation process is completed, you can review your changes prior to activating them. This enables you to understand the implications of the import. You can then revert your changes if you decide that you don't want to keep the imported configuration.

Activating Your Changes

For an overview of the activation process, see Activation on page 94.

Preview the Effect of Pending Changes

The Activation page enables you to review all the discovery 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 return to the Configuration Profiles, Device Groups, Schedules, or Deployment Credentials 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.

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 pages. Only changes that have been activated are reflected in these tables. Refer to Activating Your Changes on page 114 for more information.

Discovery Configuration Table

The information in the table is organized by device group. The groups are listed in rank 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 seven profile columns: Basic Discovery, SNMP, Network, Agent, Scanner, Virtualization, and Mobile. 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 seven tables on the Status > Current Settings > Discovery Configuration page show you the detailed settings for each configuration profile that has been established. Some of these profiles are provided with DDM Inventory, and others have been created by your administrator.

Basic Discovery Profiles

This table shows you the values of the following settings for each Basic Discovery profile:

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

SNMP Profiles

This table shows you the values of the following SNMP credentials for each SNMP profile:

- 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 shows you the values of the following settings for each Network 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 shows you the values of the following settings for each Agent profile listed:

- Allow agent communication
- Limit bandwidth for data transfers
- Collect utilization data
- AUM agent migration
- Allow agent upgrade
- Agent automatic upgrade schedule
- Agent deployment
- Allow agentless scanner execution
- Remove scan data
- Allow new key
- Allow modified public key
- Anonymization
- Deployment credentials

Scanner Profiles

This table shows you the values of the following settings for each Scanner profile listed:

- Deploy/upgrade scanners using this schedule
- Run the scanner using this schedule
- Transfer the scan file using this schedule
- Automatic workflow interval
- Allow scanners to be upgraded
- Run pre-scan and post-scan scripts
- Windows (x86) scanner
- HP-UX (HPPA) scanner
- HP-UX (ia64) scanner
- Linux (x86) scanner
- AIX (POWER) scanner
- Solaris (SPARC) scanner
- Solaris (x86) scanner
- Mac OS X (PPC) scanner
- Mac OS X (x86) scanner

Virtualization Profiles

This table shows you the values of the following settings for each Virtualization profile listed:

- VMware discovery interval
- Discover VMware using this schedule
- VMware host credentials
- Inventory VMware hosts

Mobile Profiles

This table shows you the values of the following settings for each Mobile profile listed:

- Mobile discovery interval
- Mobile inventory interval
- Discover mobile devices using this schedule
- Mobile port number
- Use HTTPS to connect to mobile server
- Mobile server credentials

Deployment Credentials Table

This table lists any deployment credentials that have been entered for remote communication with client devices. It shows you the values of the following settings for each set of credentials:

- Label
- Login
- Type (Windows or SSH)
- Domain
- Share
- Path

Schedules Table

This table lists all schedules that have been defined, including system-defined schedules. For each schedule listed, it shows you the value of the following settings:

- Name
- Description
- Time Range

11 Setting Up Agents and Scanners

In this chapter, you will learn how to set up either agent-based or agentless scanning. The following topics are covered:

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

Two Types of Scanning: Agent-Based and Agentless

You can choose between agent-based scanning and agentless scanning.

What is an Agent?

An Agent is a component that can be installed on each workstation or server in your network to automatically deploy and run scanners on these devices. The Agent is the component that communicates with your DDM Inventory server, allowing the server to run the scanner and retrieve the scan data. This scenario is called agent-based scanning.

You can configure DDM Inventory to automatically deploy the Agent on Windows devices as soon as they are discovered. For non-Windows platforms, you can create a custom deployment script to deploy the Agent. Once deployed, the Agent can be upgraded, if necessary, or uninstalled. The Agent configuration profile determines if and when the Agent is deployed, upgraded, or uninstalled. The Agent is responsible for encryption and bandwidth control.

When deployed, the software utilization plug-in is installed with the Agent.

What is Agentless Scanning?

Agentless scanning addresses the need for infrequent, small footprint, and one-off inventory.

Agentless scanning allows a device to be scanned without deploying an Agent to that device. In this case, DDM Inventory creates a secure connection to the client device, copies a scanner to the device, executes the scanner, and retrieves the scan data. All operations are encrypted and require knowledge of administrator credentials that are valid for the device or group of devices being scanned.

Which Method is Preferable?

That depends on your objective. Both methods of scanning use a secure and reliable connection between the DDM Inventory server and individual network devices. Both collect inventory information from the network devices.

Agentless scanning is particularly useful for one-time or infrequent scanning when you have no interest in software utilization data. For example, if you need to take inventory prior to or immediately after a site consolidation or move, agentless scanning would be appropriate.

The primary advantage of agentless scanning is that nothing needs to be installed on the device to be scanned prior to the scan—only a valid set of login credentials is required. Another advantage is that agentless scanning leaves almost no footprint on the scanned devices. Files created during a scan are saved in a temporary directory and are cleaned up later by the operating system. You can also instruct DDM Inventory to delete all traces of the scanning operation immediately after a scanner runs and the scan data is collected by the server.

If you want to collect software utilization data, you must either use agent-based scanning or install the software utilization plug-in using the Manual Deployment setup type (see the "Manual Deployment" section in the "Agent Communication Configuration" chapter of the *Configuration and Customization Guide*.).

Agent-based scanning is also the best method to use if you want to perform frequent, short scanning cycles on a large network. For example, if you want to track inventory and software utilization of a stable, large population of devices in order to track and tune the need for software licenses—and provide accurate IT information to support or other groups—agent-based scanning would be appropriate.

Agent-based scanning requires the Agent to be installed and keeps the local scan file and software utilization data (when enabled) on the managed computer. The added benefit of the local scan file, however, is to allow delta scanning to be performed. Instead of sending a full scan file to a server after every scan, the scanners can calculate the difference (or "delta") between the last full scan and the current one and transfer only that information. This reduces the amount of network bandwidth used when conducting subsequent inventories.

Agent Configuration Profiles

DDM Inventory comes with six system-defined Agent configuration profiles. You can also create your own profiles.

Agent profiles include communication credentials that the DDM Inventory server will use to either perform agentless scans or automatically deploy the Agent. There are two types of communication credentials:

- For Windows devices, communication credentials are used to either automatically deploy the Agent or perform agentless scanning.

- For UNIX, Linux, and Mac OS X devices, communication credentials are used to perform agentless scanning over a Secure Shell (SSH) connection.

In both cases, you must configure the communication credentials and then associate them with the pertinent Agent configuration profile (or profiles). For information about configuring and using communication credentials, see Setting Up Deployment Credentials on page 104.

You may also need to configure additional Agent Communication Settings. For more information, see the *Configuration and Customization Guide*.

Configuring Communication Credentials

When you set up communication credentials—also known as deployment credentials— it is equivalent to having DDM Inventory log in to your network computers as an Administrator (Windows) or a user with SSH login permissions (Mac OS X, Linux, or UNIX). Once DDM Inventory can access a computer, it can then perform an agentless scan (Windows, UNIX, Linux, or Mac OS X) or deploy the Agent to that computer (Windows only).

Windows Credentials

Windows communication credentials usually represent an administrator account. As multiple accounts can be used in the network, you can enter multiple account name/password combinations. 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.

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

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

This feature uses the standard Windows Workstation Service 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.

To configure Windows communication credentials:

1 Click **Administration > Discovery Configuration > Deployment Credentials**.

2 Click the **Windows** tab.

3 Click **New**.

4 Enter a **Label** for this set of communication credentials.

The label will appear in the list of communication credentials available for use in Agent configuration profiles. It can be anything you choose.

5 Enter the **Login**.

This is the login name for the user account on the remote Windows system that DDM Inventory will use to log in remotely and either deploy the agent or perform an agentless scan.

6 Enter the **Domain**.

This is the name of the Domain, Workgroup, or Active directory to which the user account specified in step 5 belongs.

7 Enter the **Password** (twice).

This is the password for the user account specified in step 5.

8 Enter the **Share** (if you want to change it from the default ADMIN$).

This is the name of the shared directory on the target system that is used for agent deployment. You must change the Path if you change the default Share.

9 Enter the **Path** (if you want to change it from the default %SystemRoot%).

This is the path to the default share on the target workstation.

10 Click **Save and Close**.

Remember to activate your changes to have them take effect.

SSH Credentials

SSH credentials are used to create a Secure Shell connection to UNIX, Linux, and Mac OS X devices for the purpose of agentless scanning. You can specify either a root account or any user account allowed to login using SSH. If you specify a non-root account, inventory information will be restricted to information accessible to the user account that you specify.

To configure SSH communication credentials:

1 Click **Administration > Discovery Configuration > Deployment Credentials**.

2 Click the **SSH** tab.

3 Click **New**.

4 Enter a **Label** for this set of communication credentials.

The label will appear in the list of communication credentials available for use in Agent configuration profiles. It can be anything you choose.

5 Enter the **Login**.

This is the login name for the user account on the remote system that DDM Inventory will use to create an SSH connection and perform an agentless scan.

6 Enter the **Password** (twice).

This is the password for the user account specified in step 5.

7 Click **Save and Close**.

Remember to activate your changes to have them take effect.

How Is the Secure Connection Made for Agentless Scanning?

For Windows client systems, DDM Inventory uses the remote management capabilities of the Windows operating system to create the secure connection. Data is encrypted in the same way that it is for agent-based scanning using 3DES / RSA 2048 encryption.

For UNIX, Linux, and Mac OS X client systems, Secure Shell version 2 (SSH-2) is used to create the connection.

For UNIX/Linux/Mac OS X clients using SSH, you can use the following Agent profile options to configure either an open testing environment or a more secure production environment:

Option	Effect
Allow new public client key	When this option is enabled, DDM Inventory does the following when it discovers a new UNIX/Linux/Mac OS X client device with this profile: • Accepts the SSH public key for the new UNIX/Linux/Mac OS X client • Initiates an agentless scan. If this option is disabled, a UNIX/Linux/Mac OS X client device with this profile is not automatically scanned upon discovery and cannot be scanned until this option is enabled. This option applies only to newly discovered devices. It does not affect devices that have already been agentlessly scanned.
Allow changed public client key	This option determines what DDM Inventory does if it determines that the public key has changed on a UNIX/Linux/Mac OS X client device since the previous scan. If the option is enabled and the SSH public key changes, DDM Inventory will accept the public key and perform agentless scans as instructed. If the option is disabled, DDM Inventory will not accept the SSH public key and will not perform agentless scans until the new key is validated. You can validate a new key by manually initiating an agentless scan. See Reset a Mismatched Key for more details. This option is useful if you want to perform agentless scans using SSH on devices that frequently change IP addresses—for example, devices that connect to your network through a virtual private network (VPN).

To create a “pass-through” security mode where any host is authenticated by default, even if the key is unknown or has changed, use the following settings:

- Enable **Allow new public client key**
- Enable **Allow changed public client key**

This is a low security mode that should only be used for testing in a highly controlled environment. It is not suitable for production except for devices that connect through a VPN.

To create a “one-time validation” security mode—where the key is accepted the first time and then memorized but subsequent connections are not allowed if the key changes—use these settings:

- Enable **Allow new public client key**
- Disable **Allow changed public client key**

Resolving Mismatched Keys for Agentless Scanning

If you are running in “one-time validation” mode, and the key changes on a client device, subsequent agentless scan operations will not be performed for this device. DDM Inventory flags a key mismatch in the database, and agentless scanning is not permitted for this device until you explicitly reset the key.

If DDM Inventory finds a mismatched key, it generates an exception report.

View Key Status

To view a list of devices that are configured to use agentless scanning, click **Status** > **Device Status** > **Agent status**. The SSH Public Key Status column shows you whether the key on each device matches the key stored in the DDM Inventory database for that device. There are four possible states:

Key Status	Meaning
Known	The SSH public key on this device matches the key stored in the database.
Unknown	Either no SSH public key for this device has been stored in the database, or the key has been reset.
Mismatch	The SSH public key on this device does not match the key stored in the DDM Inventory database for this device.
n/a	Agentless scanning is not enabled for this device.

This page also lists all devices that have Agents installed, whether or not these devices are configured to use agentless scanning.

Reset a Mismatched Key

If you determine that one or more keys do not match, you can reset them. There are two ways to reset a mismatched key:

- Using the Device Manager
- Using **Administration** > **Data Management** > **Reset SSH public keys**

Both methods are equally convenient when you want to reset the key for a single device. If you want to reset the keys for multiple devices, the second method is more efficient.

To reset a mismatched key using the Device Manager:

1 Open the Device Manager for a particular device.

2 Click the **Update Model** () button.

3 From the drop-down list, select **Run Agentless Scanner**. If there is a key mismatch, an error message will appear.

4 Click the **Reset** button.

5 From the drop-down list, select **Run Agentless Scanner** again.

Refer to "Using the Device Manager" in the *Network Data Analysis Guide* for more information about the Update Model function.

To reset one or more mismatched keys using **Reset SSH Public keys**:

1 In the navigation tree, select **Administration** > **Data Management** > **Reset SSH public keys**. All devices that have mismatched keys are listed.

2 Select the devices whose keys you want to reset, or select **All**.

3 Click **Confirm**.

After you reset the key for a device, the SSH Public Key Status for that device on the **Status** > **Device Status** > **Agent status** page is shown as Unknown. The next time that DDM Inventory attempts to run an agentless scan on the device, the modified key will be accepted and stored—provided that **Allow new public client key** is set in the Agent profile associated with this device.

Resetting SSH Public Key for Agentless Scanning

If you have changed the SSH public key after running a scan, you can reset the credentials to the new ones with one of the following methods:

- Using the Device Manager
- Using **Administration** > **Data Management** > **Update device models**

If you want to reset the keys for multiple devices, the second method is more efficient.

To reset public key for a single device using the Device Manager:

1 Open the Device Manager for a particular device.

2 Click the **Update Model** () button.

3 From the drop-down list, select **Run Agentless Scanner**.

4 Check the **Reset the SSH public key** check box.

5 Click **Update**.

Refer to "Using the Device Manager" in the *Network Data Analysis Guide* for more information about the Update Model function.

To reset public key for multiple devices

1. In the navigation tree, select **Administration** > **Data Management** > **Update device models**.The Update device models window opens.
2. Under **Action to Perform**, select **Reset SSH Public Key**.
3. Under **Device Selection**, select the option that covers the range of devices whose credentials you want to reset.
4. Click **Schedule**. The scheduling information for the update action is displayed.
5. Click **Submit**.

After you submit your request, you can select **Status** > **Device Status** to view the progress of the update actions.

Call Home Option

Overview

The Call Home option allows a device to call the DDM Inventory Server if no scan file has been retrieved from the device within a certain time period. By default, this option is enabled. It is recommended that you use the default setting for this option for networks that have VPN clients or very short DHCP lease time. Having this option enabled helps ensure that mobile devices will get scanned on a regular basis regardless of their intermittent connections to the network.

How Call Home Works

Who Can Initiate the Call

Call Home is initiated by the Agent on the remote device. The Agent calls the DDM Inventory Server if the Call Home option is enabled (enabled by default) and certain conditions have been met. See Call Home as the Only Discovery Source and Conditions for Contacting the Server.

How the Agent Knows which Server to Contact

The Agent knows its originating server by default and will call it if nothing else is configured. However, you can specify information about the DDM Inventory Server that is transmitted to the client device. This includes information about the primary and secondary custom servers and the originating server. See Specify List of Servers. It can either be the IP address or DNS name of the server. The Agent will call each server in the list, in the order specified until the Call Home communication succeeds. The originating server will only be called in case the two previous servers have not responded or configuration fields were not properly set. See Call Home as the Only Discovery Source.

Conditions for Contacting the Server

The Agent will call home if one of the following occurs:

- The Agent starts and the device has not been scanned. The Agent will trigger the Call Home notification within 1 and 11 minutes after startup while it is connected to the network.
- The DDM Inventory Server has not retrieved a scan file within a specific time interval. The time interval is set to the expected scan interval plus a delay of 20%. The delay will not be greater than 8 hours or less than 30 minutes.

Action After Call Home

After the Agent calls home, it expects that a valid scan cycle will take place within 8 hours. The Agent will call home again every 8 hours until the scan file is retrieved by the Server.

If the Call Home notification successfully reaches the DDM Inventory Server, the Server will decide if action needs to be taken. The determination is based on several factors including agent and scanner configuration settings. For example, if the Call Home notification is made from a device whose agent profile does not have **Allow agent communication** or **Allow agentless scanner execution** (depending on your scanning method) enabled, the DDM Inventory Server will not initiate scanning of the device. The Server can, however, start SNMP modeling of the address from which the Call Home notification was received if this address is not reported by any of the devices in DDM Inventory Server database.

So after the notification is received, it is possible for the DDM Inventory Server to drop the request, resume a scanning workflow, or start a new one depending on the configuration and other factors. Refer to the Configuring the Discovery Process chapter for more information on agent profiles.

If the DDM Inventory Server decides to start a new inventory cycle for that device and discovers that the scan file on the device is more recent than the one in the DDM Inventory database, it will retrieve the scan file before scheduling a scan. The DDM Inventory Server will inspect the local scan file *only if* you have enabled the scanner configuration option. See Enable Download of Current Scan File Option.

The download current scan file option is ignored if the Agents that you are using are older than the DDM Inventory version 7.60 Agent.

Typical Call Home Scenarios

In the scenarios described below, it is assumed that a 7.60 or later Agent (generated on the DDM Inventory Server) is installed on the managed device.

New Computer Connects to Network

1. A user connects a computer that has not been discovered by DDM Inventory.
2. The Agent installed on the computer sends a Call Home notification to the DDM Inventory Server.
3. The DDM Inventory Server receives the Call Home notification and determines that the device has not yet been discovered.
4. The DDM Inventory Server creates a new node for the device in its database with minimal information containing only the IP address of the device.
5. The DDM Inventory Server initiates the SNMP-modeling process on the device.

6 The DDM Inventory Server initiates the scanning process on the device.

> The SNMP-modeling and scanning processes run in parallel. It does not matter which process completes first.

7 After the modeling process completes, the DDM Inventory Server updates the device information in the database and may initiate other regular discovery processes on the device such as, VMware discovery, and others.

Laptop Frequently Connects to Network for Short Periods of Time

1 A user has a laptop connected to the network.

2 The DDM Inventory Server starts the scanning workflow execution on the laptop.

3 The laptop disconnects during workflow execution.

> This can be a VPN accidental disconnect or a planned disconnect by the mobile user.

4 The DDM Inventory Server determines that the laptop is no longer connected and saves the state of the scanning workflow.

5 The user reconnects to the network some time later.

6 The Agent determines that the network is up and sends a Call Home notification to the DDM Inventory Server.

7 The DDM Inventory Server receives the Call Home notification, identifies the device, and continues the workflow from the point where it was interrupted.

> The DDM Inventory Server determines the IP address of the device whose Agent sent the Call Home notification. It is very likely that the IP address of the device has changed. The DDM Inventory Server will use the new address to continue the interrupted workflow.

> If scanner execution was initiated on the laptop before the disconnect, the scanner will continue to execute and is likely to complete even though the device is disconnected. When the laptop reconnects again, the DDM Inventory Server will simply download the scan file for processing (if it is configured to do so - See Enable Download of Current Scan File Option).

> If the scan file download process was initiated but did not complete before the disconnect occurred, the DDM Inventory Server will attempt to resume the download the next time that the device re-connects. If it re-connects within the next seven days, the Server will resume the scan file download process from where if left off. If the re-connect occurs after more than 10 days, the entire workflow will be initiated from the very beginning.

8 After the scanning workflow completes and the scan file is retrieved, if the main IP address reported in the scan file differs from the one currently used in the DDM Inventory database, the DDM Inventory Server may start the SNMP-modeling process on the new IP address.

> This step occurs during the enrichment process, but it does not need to wait for the data to be imported into the Aggregate database. There may be a slight delay if there are many scan files in the incoming directory.

Laptop Seldom Connects to Network

1. A user connects a laptop to the network after a long delay, that is, longer than the Automatic Workflow Interval configured for the device in the scanner profile.
2. The Agent determines that the network is up and the scan file is stale and sends a Call Home notification to the DDM Inventory Server.
3. The DDM Inventory Server receives the Call Home notification, identifies the device, and starts the scanning workflow execution on the laptop.

   The DDM Inventory Server determines the IP address of the device whose Agent sent the Call Home notification. It is very likely that the IP address of the device has changed since the last time the device was connected to the network. The DDM Inventory Server will use the new address to run the scanning workflow.

   It is likely that the last scanning workflow on the device was interrupted and the DDM Inventory Server was not able to download the scan file created by the scanner running on the already disconnected laptop. In this case, if the **Download current scan file before running scanner** option is enabled, the DDM Inventory Server will download the recent scan file from the laptop and then continue the regular workflow execution. This ensures that the DDM Inventory Server is able to download the more recent can file from the remote device before the device disconnects.

   If the scan file download process was initiated but did not complete before the disconnect occurred, the DDM Inventory Server will attempt to resume the download the next time that the device re-connects. If it re-connects within the next seven days, the Server will resume the scan file download process from where if left off. If the re-connect occurs after more than 10 days, the entire workflow will be initiated from the very beginning.

4. After the scanning workflow completes and the scan file is retrieved, if the main IP address reported in the scan file differs from the one currently used in the DDM Inventory database, the DDM Inventory Server may start the SNMP-modeling process on the new IP address.

Call Home as the Only Discovery Source

In some network environments where ICMP is blocked by firewalls and there is no SNMP access to routers, switches, and computers, and no access to virtualization management software to do virtualization discovery, Call Home can be the only discovery source.

1. A user connects a laptop that has not been discovered by DDM Inventory.
2. The Agent sends a Call Home notification to the DDM Inventory Server.
3. The DDM Inventory Server receives the Call Home notification and determines that the device has not yet been discovered.
4. The DDM Inventory Server creates a new node for the device in it database with minimal information containing only the IP address of the device.

5 The DDM Inventory Server initiates the scanning workflow process on the device.

> The DDM Inventory Server will try to initiate the SNMP-modeling process on the device. The SNMP-modeling process will fail if there is no SNMP access to the device.

6 After the scanning workflow process completes and the scan file is retrieved, the DDM Inventory Server will continue to scan the device using the scanning frequency specified in the Automatic Workflow Interval setting configured in the scanner profile.

How to Configure Call Home

To use the Call Home option, you must:

- Enable Call Home Option (option is enabled by default)

In addition, you may want to optionally:

- Specify List of Servers
- Enable Download of Current Scan File Option

Enable Call Home Option

This option is enabled by default. If for some reason it has been disabled, perform the following procedure.

To enable the Call Home option

1 Go to **Administration** > **System Configuration** > **Discovery services**.

2 For the **Agent Call Home Active** option, select **Default**.

By default, this option is enabled. It is recommended that you use the default value for this option if you have devices that frequently connect to the network for short periods of time.

3 Click **Change** to activate your changes.

Specify List of Servers

To specify the list of servers to call home

1 Go to **Administration** > **System Configuration** > **Agent communication**.

2 Under Agent Call Home for the **Primary host name for agent Call Home** option, select **Custom**, and then specify the DDM Inventory Server name or IP address to be used by the Agent to call the DDM Inventory Server.

3 Under Agent Call Home for the **Secondary host name for agent Call Home** option, select **Custom**, and then specify a secondary DDM Inventory Server name or IP address to be used by the Agent to call the DDM Inventory Server. This acts as backup contact information, which can be useful if you plan to move the DDM Inventory Server or rename it in the near future.

4 Click **Change** to activate your changes.

Enable Download of Current Scan File Option

This option is disabled by default. Perform the following procedure to enable it.

To enable the download of current scan file option

1 Go to **Administration** > **System Configuration** > **Scanner Deployment**.

2 For the **Download current scan file before running scanner** option, select **Custom** and select **Yes**.

By default, this option is disabled. It is recommended that you enable this option if you have devices that infrequently connect to the network and for short periods of time. Enabling this option mitigates the risk involved if the workflow does not complete before the user disconnects. With short connects, the DDM Inventory Server may not have enough time to download the scan file that resulted from the scan. With this option enabled, the DDM Inventory Server will download the existing scan file on the remote computer and determine if it is more recent than the one in the DDM Inventory database. If it is, the Server will use the more recent scan file to update the information in its database.

Note that this option is ignored if the Agents that you are using are older than the DDM Inventory version 7.60 Agent.

See the “Configuring Scanner Settings“ chapter in the *Configuration and Customization Guide* for more information.

3 Click **Change** to activate your changes.

Disk Space Requirements on the Managed Device

Running scanners on your workstations requires a certain amount of available disk space on the workstation. Refer to Chapter 6, Disk Space Considerations in this guide.

Setting the Agent Port

You can configure the port that the DDM Inventory server uses to communicate with the Agent on network devices. The default port is 2738. If you believe there is a risk of port conflict, you can use port 7738 instead. This port is registered with the Internet Assigned Numbers Authority (IANA).

To Change the Default Agent Port:

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

2 Next to Agent Port, select **Custom**.

3 Select the port that you want to use.

4 Click **Change**.

This procedure is intended for when you are first installing DDM Inventory on your network. If you are upgrading—or you decide to change this port number after DDM Inventory has been running—you must first uninstall the Agent from your network devices.

For full details, see the online help file available at **Administration > System Configuration > Agent communication > Agent port**.

After you change the port setting in the Web UI, the agent media files for the current version of the product are regenerated. They are copied from the `RawMedia` directory to the `LiveAgent` directory with the port correctly configured in the files. Any other files in the `LiveAgents` directory (for example, from previous releases) are *not* updated with the correct port configuration.

For an agent port change to take affect, you must uninstall or upgrade the agent on the device after making the port change. Otherwise, DDM Inventory will continue to communicate with the device with the last successful agent port used on this device regardless if you have specified an agent port change after you have deployed the agent.

Enabling the Agent Port on Mac OS X

The built-in firewall on Mac systems running OS X may block communication between the DDM Inventory server and the Agent. If this happens, perform the following procedure on the Macs to ensure that the agent port is not blocked.

This procedure is not necessary for Mac OS X version 10.5. In this case, the operating system detects the fact that the Agent needs to open a specific port. It opens a dialog box asking whether the application should accept incoming connections on this port. If you choose to accept the incoming connections, the port is automatically configured.

To enable the Agent port on Mac OS X:

1. From the Apple menu, choose **System Preferences**.
2. From the View menu, choose **Sharing**.
3. Click the **Firewall** tab.
4. Click **New**.
5. From the Port Name menu, choose **Other**.
6. Type the agent port number in the appropriate field:
   - Mac OS X 10.3.9 or earlier, use the **Port Number, Range or Series** field.
   - In Mac OS X 10.4 or later, use the **TCP Port Numbers** field.
7. In the **Description** field type: `DDM Inventory agent port`.
8. Click **OK**.

Using A Different Tool to Deploy Scanners

This section applies only to agentless scanning.

If you use a software deployment tool—such as HP Client Automation—in your environment to distribute and install software applications on your network devices, you can use that tool to deploy DDM Inventory Scanners. This is an alternative to the built-in DDM Inventory Scanner deployment process and mechanism. In this case, you must tell DDM Inventory where the Scanner executable files are located on the client devices.

For UNIX devices, you can use the standard `$VAR` notation to include shell variables in the path to the scanner. For example: `$HOME\Scanners`

For Windows devices, you can use the standard `%VAR%` notation to include system environment variables or the following standard folders in the path to the scanner:

- `AppData`—Full path to the Roaming folder for the current user
- `ProgramFiles`—Full path to the predefined Program Files folder
- `CommonAppData`—Full path to application data for all users
- `CommonFiles`—Full path to the Common Files folder for the current user
- `LocalAppData`—Full path to the folder that contains local (nonroaming) applications
- `System`—Full path to the System folder for the current user
- `Temp`—Full path to the Temp folder
- `Windows`—Full path to the Windows folder

For example: `%AppData%\Scanners` or `%SystemRoot%\Scanners`

To specify the location of DDM Inventory Scanner executable files:

1. Click **Administration** > **System Configuration** > **Scanner deployment**.
2. Scroll down to the Location of Scanner Executable for Agentless Scanning section.
3. For each pertinent platform, follow these steps:
   a. Select the **Custom** box.
   b. Specify the directory or folder where the Scanner executable file resides on this platform.
4. Scroll to the bottom of the page.
5. Click **Change**.

If you name the Scanner executable files on the network devices something other than `scan` or `scan.exe`, you must also specify these file names in the Scanner File Name section of the **Scanner deployment** page.

If you want to prevent DDM Inventory from automatically upgrading the Scanner executable files when it performs the next agentless scan, be sure to clear the **Allow scanners to be upgraded** option in the pertinent Scanner configuration profiles.

If you want DDM Inventory to upgrade your Scanners, select the **Allow scanners to be upgraded** option in the profile (or profiles). If the Scanner location you have specified does not yet exist on a particular network device, DDM Inventory will create this directory before upgrading the Scanner—provided that the path is valid and the file system permissions allow the directory to be created.

Adding the DDM Inventory Agent to an OS Image

Getting an inventory as soon as a new device is available on the network is key for some organizations. The best way to do this is to enable Call Home and then include the DDM Inventory Agent in your corporate operating system image.

To include the Agent in an OS image package:

1. On the **Administration** > **System Configuration** > **Agent communication** page, make sure that the following options are set properly for your environment:
   - Agent port
   - Primary host name for agent Call Home
   - Secondary host name for agent Call Home
2. Wait at least five minutes for all configuration settings to fully propagate.
3. Take the appropriate Agent executable file from the `<DataDir>\LiveAgents` folder, and incorporate this file in your OS image package.

What Next?

To	Go to
Manually deploy agents (UNIX, Linux, Mac OS X, and Windows)	*Configuration and Customization Guide*
Set up DDM Inventory user accounts	Setting Up Accounts on page 141
Optional: Set up DDM Inventory aggregation	Setting up DDM Inventory Aggregation on page 147

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 configuration profile, device group, set of deployment credentials, or schedule, you are actually saving your changes in a working copy of the configuration database. To commit your changes to their permanent location in the DDM Inventory 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 94.

Reviewing Your Changes

DDM Inventory 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** > **Activation**

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 DDM Inventory 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, DDM Inventory 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 DDM Inventory license type.

The following issues are detected:

Issue	Resolution
No license available for software utilization.	Please check your license entitlement via HP Technical Support website or contact your HP Account Representative to find out how to obtain the DDMI Software Utilization license.
“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.
“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 DDM Inventory. 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 DDM Inventory.

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 rank 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 rank 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** > **Activation.**

2 Click **Revert Changes**.

Activating the Changes

To activate the pending changes:

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

2 Click **Activate Changes**.

Checking that DDM Inventory is Working as Expected

There are a couple of things you can do to make sure DDM Inventory 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 DDM Inventory 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 DDM Inventory 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 DDM Inventory. The following topics will be covered:

Introduction

Once you have set up the DDM Inventory server and configured DDM Inventory, 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 DDM Inventory has an account, and knows the limits of their account level.

There are Four Pre-Installed Accounts

DDM Inventory comes with four accounts pre-installed, one of each of the following types:

- Demo
- IT Employee
- IT Manager
- Administrator

The DDM Inventory 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 DDM Inventory at Once?

DDM Inventory 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 DDM Inventory 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 DDM Inventory, sets up more accounts
- Scanner—exclusively used to transfer scan files.
- Aggregator—exclusively used to configure the DDM Inventory 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 DDM Inventory 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 DDM Inventory 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 and 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. You can change the account type later if you like. See page 145 for more information.

➤ 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 DDM Inventory.

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.

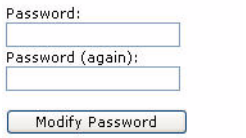
➤ A user password cannot be the same as the user name, a portion of the user name, or the inverse of the user name.

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 DDM Inventory 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 DDM Inventory Aggregation

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

Introduction

An **Aggregator** is a DDM Inventory server that collects and combines data from several DDM Inventory servers in your network. The health data from these **remote** servers is combined into one Aggregate Health Panel, so you can see the status of your entire network. An Aggregator also allows you to access other individual DDM Inventory servers without logging into them directly.

To facilitate communication between the Aggregator and the remote servers, you must create an **Aggregator Account** on the Aggregator and each remote server.

If you have purchased an Aggregator license, this chapter will show you how to set up and use the DDM Inventory Aggregator. To use the Aggregator, all of your DDM Inventory servers must be at least version 2.1 (DDM Inventory 2.0 does not support SSL, which is necessary for the servers to communicate).

Installing the Aggregator Server

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

An individual DDM Inventory 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 DDM Inventory server, as described in Server Installation on page 21.

Your Aggregator server must have considerably more disk space than a regular DDM Inventory server. You will require 6GB for the operating system and DDM Inventory 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 148.

Installing the Aggregator License

Only one DDM Inventory 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 30.

The Aggregator server will require more hardware resources (larger disk, more RAM) than a regular DDM Inventory server. See Server Installation on page 21 for details.

Installing the Remote DDM Inventory Servers

Remote servers should run the same version of DDM Inventory as the Aggregator server. Follow the instructions in Server Installation on page 21 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 148.

Sharing Security Keys Between All Your Servers

When you install DDM Inventory, 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 DDM Inventory servers, you will encounter major communication problems in your network, as the servers communicate with network devices and each other.

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 DDM Inventory server in your network as the “master” server. This will most often be the Aggregator server, but it can be any DDM Inventory server in your network. You will use the security keys from this server to copy to the other DDM Inventory 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 (`<DataDir>\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 DDM Inventory servers. This causes a Hostname mismatch error when accessing the other DDM Inventory 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 DDM Inventory 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 DDM Inventory server.
2. Copy the files from the floppy disk to the `Cert` directory (`<DataDir>\Cert`).
3. Either remove the floppy disk from the drive, or remove the USB key.
4. Restart your DDM Inventory server.

Configuring the Aggregator

For the Aggregator to work, you must prepare the Aggregator, and you must prepare each individual remote server. You must provide the following information to 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 to 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 152 for suggestions.

You must also perform discovery configuration for your Aggregator. For example, add device groups for your remote servers and router, associate Basic Discovery and SNMP profiles with these devices, and then be sure to **Activate** these changes. See Chapter 10, Configuring the Discovery Process for details.

On each individual DDM Inventory server that you will be aggregating, set up an Aggregator account that will allow the Aggregator to access the remote server's database. For more information about Aggregator accounts, refer to "Setting Up Accounts" in the *Configuration and Customization Guide*.

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 from the remote server.

   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 150.)
6. Select data transfer intervals:
   - Aggregate network inventory
   - Aggregate events
   - Aggregate workstation inventory
   - Aggregate mobile inventory

   Refer to the online help for information about these intervals.

   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 149).

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

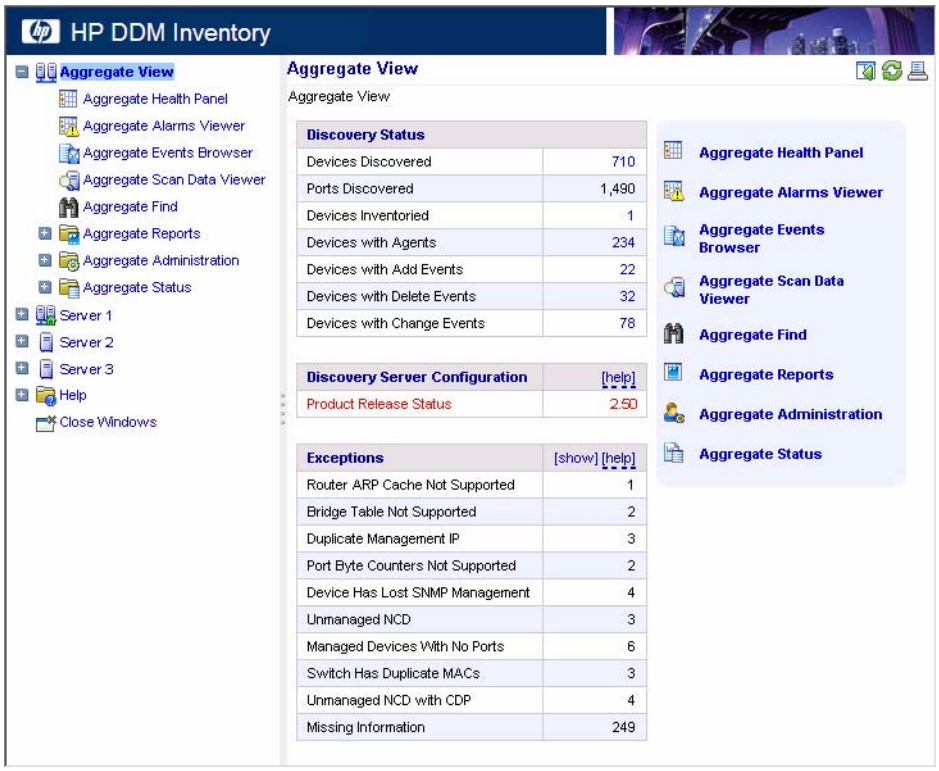
You can use the navigation frame on the left side of your window to look at the Aggregator, or any of your remote servers.

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 **Aggregate 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 149, 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
Configure your data backups	Chapter 15, Backing Up and Restoring Your Data

15 Backing Up and Restoring Your Data

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

Introduction

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

Table 6 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 32.

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 DDM Inventory server, and the current version of your DDM Inventory software.

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

The following data is not backed up by DDM Inventory:

- 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 DDM Inventory 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 DDM Inventory 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 DDM Inventory 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 DDM Inventory 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 DDM Inventory 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 DDM Inventory 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 synchronize 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 discovery 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 DDM Inventory Security Template on page 163.

DDM Inventory 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, DDM Inventory will automatically do a restore when you next restart your server.

To restore your backup data to the server:

1. In the <*DataDir*> folder, create an empty directory called `Restore` . See page 11 for the default <*DataDir*> location for your operating system.
2. Add your latest backup files to the `Restore` directory. You must include at least the following files:
   - `certs.zip`
   - `MySQL.zip`
   - `data.zip`

   You can also include the `scans.zip` file.
3. Restart your DDM Inventory server.

When you restart your server, DDM Inventory detects that a restoration has begun and displays the following information in a dialog box:

- A progress bar
- A brief description of the current operation
- The total elapsed time

During the restore process, you can interact with this dialog and place other windows over it. Should the dialog become lost, you can access it from the task bar. When the restore is completed, the progress bar will show 100% complete, and you will see a “success” or “failure” message. You can then close the dialog by clicking the X.

After the restore is completed, 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 DDM Inventory

In this chapter, you will learn how to uninstall DDM Inventory.

A complete uninstall may take 10-20 minutes.

Removing DDM Inventory Components

To remove DDM Inventory components installed on your system:

1. In **Control Panel** > **Add/Remove Programs** (for Windows Server 2003) or **Control Panel** > **Programs and Features** (for Windows Server 2008), select the HP Enterprise Discovery entry.
2. Click **Remove**. Follow the on-screen instructions.
3. *Optional:* You can also uninstall the DDM Inventory Agent if you want to. This is not necessary, however.

   When the DDM Inventory server starts up, it installs an Agent if and only if the server machine does not already have an Agent.
4. Remove the following folder:

   `<InstallDir>\Tomcat`

   In this case, `<InstallDir>` is the installation directory that you specified when you installed DDM Inventory. By default this is

   `C:\Program Files\Hewlett-Packard\DDMI\7.70`
5. *Optional:* View the DDM Inventory uninstall log file:

   `<InstallDir>\uninstall\uninst_ED.log`

   This file contains a list of all the files and folders that were removed during the uninstall.
6. Restart your server.

   You must restart your server before installing a new version of DDM Inventory.

17 Security Checklist

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

Introduction

Although your DDM Inventory 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 DDM Inventory server, all web UI pages are served via a secure HTTPS/SSL connection. When you install DDM Inventory, it generates default SSL keys and a certificate which are used to ensure secure communication with the server.

- The Scanners 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 as follows:

```
https://DDMIserver.yourcompany.com
```

- All HTTPS communication between the server and client (and for multiple aggregated servers) take place over port 443. Any attempts to port 80 will be redirected to 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 DDM Inventory client workstation.
- Purchase a commercial certificate from a recognized certificate authority (such as Verisign), and install it on the DDM Inventory server, replacing the default certificate.

Putting the Certificate on Your DDM Inventory Client

If you use the default certificate, or a new signed certificate, you must copy it to the DDM Inventory 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

The following instructions are for Windows XP client systems. Other versions of Windows may have different instructions.

To copy the files from the server to the client:

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 DDM Inventory 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.

To install the certificate through the web browser:

The first time you access the DDM Inventory 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 DDM Inventory 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 the following folder:

`C:\Program Files\Hewlett-Packard\DDMI\7.70\apache\bin`

If there are two `openssl` files with different extensions in this folder, choose the one with the extension `.CNF` and size 10K.

3 Follow the instructions available at this site:

http://httpd.apache.org/docs/2.2/ssl/ssl_faq.html#realcert

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

Table 7 Default Locations

File	Location
`server.crt`	*<DataDir>*`\Cert\ssl.crt`
`server.key`	*<DataDir>*`\Cert\ssl.key`

4 Finally, restart the HP DDMI Apache SSL Web Server service (**Start > Control Panel > Administrative Tools > Services**).

DDM Inventory Security Template

The DDM Inventory 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 > Hewlett-Packard > DDM Inventory 7.70 > Install Security Template**. After you make that selection, the security settings listed in Table 8 and Table 9 on page 164 are automatically applied to your system.

In the following tables, *<InstallDir>* represents the location of the DDM Inventory program files that you specified at install time, and *<DataDir>* represents the location of the data folder. See the Introduction on page 161 for more information.

Table 8 Folder Security for User Accounts

Folder	Security Measure
C:\Perl	Read-only access
<InstallDir>	Read-only access
<DataDir>\Autopass	No visibility
<DataDir>\Cert	No visibility
<DataDir>\Database	No visibility
<DataDir>\LiveAgents	No visibility
<DataDir>\PrePostScripting	No visibility
<DataDir>\Scans	Read-only access

In the following table, the abbreviation HKLM stands for HKEY_LOCAL_MACHINE.

Table 9 Registry Security for User Accounts

Registry Key	Security Measure
HKLM\SOFTWARE\Hewlett-Packard\ED	Read-only access
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\ovedDiscDB	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
HKLM\SYSTEM\CurrentControlSet\Services\ovedSysStatus	Read-only access
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 DDM Inventory Server Behind Your Company's Firewall

The DDM Inventory 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 with Windows Server 2003 SP1 or Windows Server 2008. If you are using Windows XP SP2 for a demo or trial installation, you should also enable the built-in firewall.

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

Change the Read Community String of the DDM Inventory Server

This is a documented community string, known to:

- Admin accounts at your site
- Existing and prospective DDM Inventory customers

Anyone who knows the default read community string ("public") will be able to access the SNMP MIB of your DDM Inventory 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 DDM Inventory customers

  Anyone who knows the default account names may be able to gain access to your DDM Inventory 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 167).

Anyone who knows the default password for the "admin" account may be able to gain top-level access to your DDM Inventory server.

There is information about accounts in Setting Up Accounts on page 141.

Change the Default Admin Password

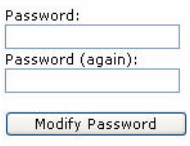
When you change the password for the admin account, you will have to log in again. (It is always necessary to log in again when you change the password for the account that you are using.)

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 DDM Inventory (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 DDM Inventory 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 DDM Inventory 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 DDM Inventory 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-7.70.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\Hewlett-Packard\DDMI\7.70\Install`

3. Restart your DDM Inventory server so it can recognize the update.

4. To view the knowledge package you have installed in the DDM Inventory user interface, click **Status > Current Settings > Installed components**.

DDM Inventory 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 `<DataDir>\logs\package-verify.log` file. 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`
- `BaseUnixOS.zsai`

By default DDM Inventory is configured to use only the Master and UNIX SAI files.

To ensure that any other SAI files are included in the enrichment process you will need to reconfigure the XML Enricher and restart the XML Enricher Service.

Refer to the section entitled “Configuring the XML Enricher Using the Web UI” 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

After you have installed your DDM Inventory server, you may want to set up an Asset Questionnaire to help you track details about your devices that would not normally be available to the product database. The Asset Questionnaire also enables you to input device level information that has higher priority than—and will thus override—automatically collected data.

The Asset Questionnaire enables you to associate a person's name, department, phone number, or other personal information that you want to associate with this device in the DDM Inventory 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 on your DDM Inventory server first, and then you can access the Asset Questionnaire from any workstation with a web browser.

This Asset Questionnaire data is saved in the DDM Inventory server database, and is also 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 DDM Inventory 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 > Asset Questionnaire.**

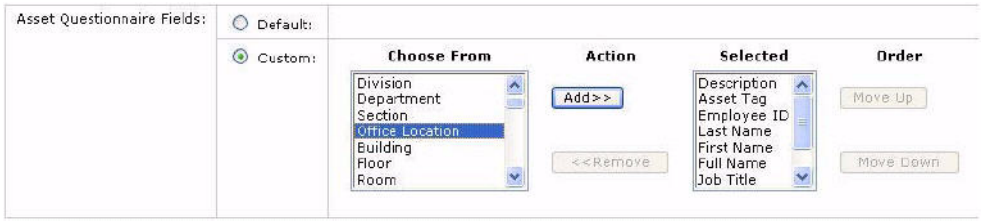
2 To create your own question fields, click **User-defined questions**.

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 > 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 > Asset Questionnaire > Question type.**

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

For example, if you want only a text string to be entered (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.

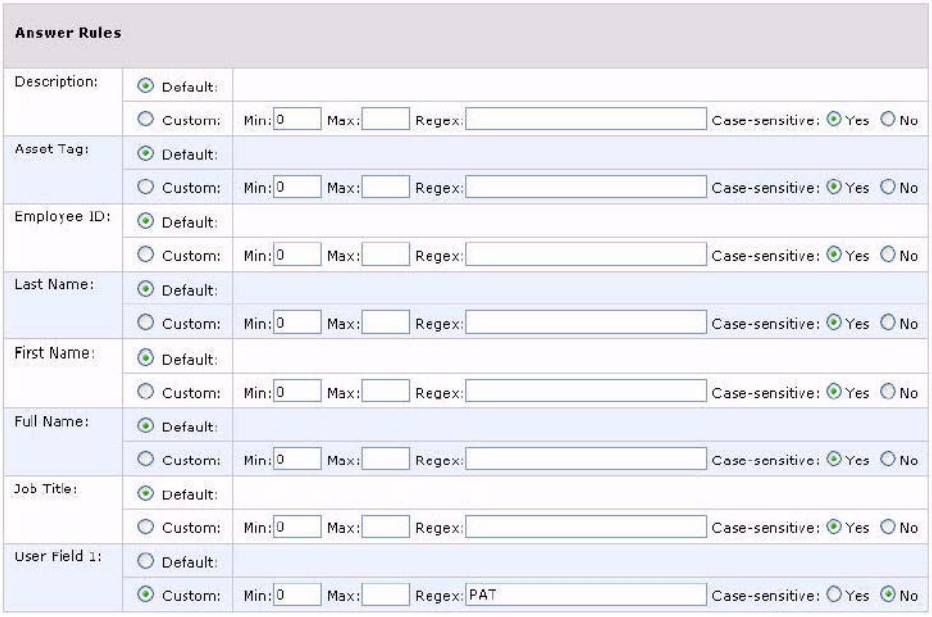
11 To configure which questions are required in the Asset Questionnaire, click **Administration > Asset Questionnaire > Required fields.**

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

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

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

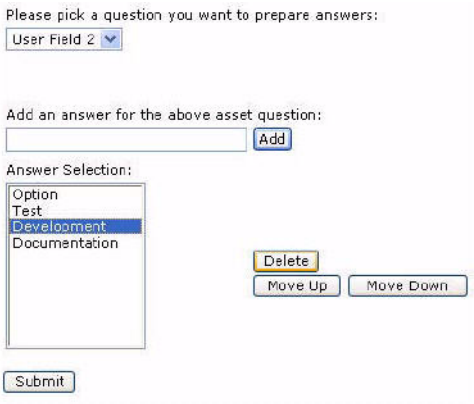
16 If you have configured any of your questions to have a List of possible answers, you should now configure the List. Click **Administration > Asset Questionnaire > Answer selection.**

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 175.

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 > Asset Questionnaire > Import answers.**
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 > Asset Questionnaire > Export answers.**

   A **File Download** dialog appears.
2. Click **Save**.
3. Save the file to your computer.

Using the Asset Questionnaire to Configure Asset Information

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 DDM Inventory 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 DDM Inventory.
2. Click **Asset Questionnaire**.
3. *Optional:* Enter the device title or IP address of the asset that you want to configure.

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 DDM Inventory 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 Included in an IP-only Device Group

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 DDM Inventory.

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 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.

Gathering Information for Support

With one click, you can save all your DDM Inventory server configuration information in an HTML file. You can then send this file to your support engineer. This information will enable your support engineer to more quickly troubleshoot your issue.

To save your server configuration to a file, click **Status** > **Current Settings** > **Server configuration for support**.

Using Windows Remote Desktop

On your DDM Inventory 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:

- The operating System installed on your server
- The version of DDM Inventory, including the build number (click **Status** > **Current Settings** > **License status**)
- The latest knowledge package that you have installed on the server
- Your customer number
- 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 in the following location:

  `<DataDir>\logs`

  Here, `<DataDir>` is the DDM Inventory data folder that you specified at install time (see page 11 for the default `<DataDir>` location for your operating system).

The first three items are included when you save your server configuration. See Gathering Information for Support on page 177.

A Appendix: Migrating Data from HP Client Automation Application Usage Manager

Hewlett Packard provides a streamlined path to enable you to switch from HP Client Automation (HPCA) Application Usage Manager (AUM) to DDM Inventory as your software usage collection and metering solution.

Prior to release 7.20, HP Client Automation was called HP Configuration Management (CM). The processes described in this appendix refer to HPCA, but they also pertain to CM version 5.11 or later.

This appendix is for HPCA or DDM Inventory system administrators who want to migrate their AUM agents and data from an HPCA environment to a DDM Inventory environment.

This migration path supports data migration from AUM agents as contained in the following products:

- HP Client Configuration Manager version 2.11
- HP Configuration Management version 5.11
- HP Client Automation versions 7.2x

You can retain up to one year of existing data on the migrated DDM Inventory systems. After the migration, existing usage data is available for HPCA Enterprise Management reports and analysis, and new usage data is collected and maintained by DDM Inventory.

To perform this migration:

- You should be familiar with HPCA components, such as the Configuration Server, the Configuration Server Database and Administrator tools, and the KB Server. For details, see the appropriate HPCA guides.
- You should also be familiar with DDM Inventory.
- You will need installation media for HPCA version 7.20 (or later—or CM version 5.11 or later) and DDM Inventory version 7.50 (or later).

Process Overview

Conceptually, the process of migrating the AUM data to DDM Inventory is straightforward. The AUM agent converts existing usage data (up to 12 months) into an XML format that DDM Inventory can read. DDM Inventory then reads the XML file and stores the usage data in its database. After the AUM data is migrated and stored, DDM Inventory begins collecting new usage data. The AUM agent can then be uninstalled.

Most of the migration process is automatic. There are, however, four manual tasks that you must perform to configure and initiate the process:

Task 1: Update your AUM agent to a migration-ready version.

Task 2: Instruct HPCA to stop managing the AUM agents.

Task 3: Install DDM Inventory, and set up an Agent configuration profile to support AUM migration.

Task 4: Remove the AUM policy in the HPCA Configuration Server Database.

Tasks 1, 2, and 4 pertain to the HPCA Configuration Server. Task 3 pertains to the DDM Inventory server. Each of these tasks will be explained in the next section.

For additional information about AUM or HPCA, refer to the HP Client Automation product documentation available online at **http://h20230.www2.hp.com/selfsolve/manuals**.

Configuring the Migration

You must perform the following four manual tasks, in the order shown, to configure and initiate the migration of your AUM data to DDM Inventory.

Task 1: Update your AUM agent to a migration-ready version.

Before you can perform the migration, you must manually update the HPCA Configuration Server Database (CSDB) with the HPCA AUM Agent installable resource from the installation media (HPCA version 7.2 or later or CM version 5.11 or later).

After you update the CSDB, the new AUM agent will be distributed automatically during the next HPCA Agent connect, according to the policy defined.

The AUM Agent is not included with the HPCA Agent import decks. You must import the instance and resource files from the installation media, and deploy them using the Application Usage Mgr Agent Install - Enterprise Collection service.

Task 2: Instruct HPCA to stop managing the AUM agents.

After the new AUM agent is deployed to all the pertinent machines in your network, you must make sure that HPCA will not attempt to further update or otherwise manage this agent on these devices. This requires a change in the usage policy. Use the HPCA Admin CSDB Editor to change the following settings:

- Switch the HPCA-AUM Agent Service to Optional Management Mode. (Set the `ZSVCMO` service attribute value to O for Optional).
- Set a date after which HPCA will no longer manage this service on target AUM agent devices. Use the first `ZSTOP` expression of the HPCA-AUM Agent Service to do this. For example, to no longer have HPCA manage the HPCA AUM agent as of March 17, 2008, enter this value in the first `ZSTOP001` expression on the HPCA-AUM Service:

  ```
  DATE('S') >= '20080317'
  ```

  `DATE('S')` is a built-in REXX function that returns the date in `YYYYMMDD` format.

For further information, refer to the *HPCA Configuration Server User's Guide* and the *HPCA Configuration Server Database Reference Guide*.

Task 3: Install DDM Inventory, and set up an Agent configuration profile to support AUM migration.

Install and set up the DDM Inventory server according to the instructions in this guide. Define one or more device groups that include the systems where data will be migrated. Create Basic Discovery, SNMP, and Agent configuration profiles as appropriate for your environment. Be sure to select the following options in your Agent configuration profile:

- Allow agent communication
- Collect utilization data
- Stop AUM agent and migrate data

For more information about these options, see Agent Profiles on page 78.

When DDM Inventory detects an HPCA AUM agent on a device with these options enabled, it performs the following actions:

1. Instructs the HPCA AUM agent to stop collecting data on this device.
2. Converts the HPCA AUM usage data to an XML format that DDM Inventory can read.
3. Imports the data into the DDM Inventory database.
4. Starts collecting software utilization data for this device.

The AUM agent is then left in suspended mode. This is useful in the event that an HPCA server is controlling the presence of the AUM agent, as it will prevent cyclic reinstallation of the AUM agent.

The following table summarizes some special cases that can arise:

Situation:	**Action taken:**
DDM Inventory detects an HPCA AUM agent, but that agent is running.	DDM Inventory waits for the AUM agent to finish before initiating the data migration. DDM Inventory will not begin to collect utilization data until a successful data migration has been completed.
DDM Inventory does not detect an HPCA AUM agent.	DDM Inventory applies the Agent configuration profile and ignores the AUM migration settings.
DDM Inventory detects an HPCA AUM agent, but it is an older version that does not support data migration.	The DDM Inventory Agent will attempt to migrate the AUM data. Because the AUM agent is too old and has no export capability, however, the migration will fail. DDM Inventory will report this failure in **Status** > **Device Status** > **Agent status**. After the AUM agent is upgraded, you must also upgrade the DDM Inventory Agent. There are two ways to do this. You can manually request an Agent Upgrade for a single device using the Update Model function in the Device Manager. This is practical if you have a small number of devices to upgrade. Refer to “Update Model (Administrator or IT Manager)” in the *HP DDM Inventory Network Data Analysis Guide* for detailed instructions. Alternatively, you can simply turn utilization data collection off and then on for the pertinent devices. If many devices have failed the migration due to outdated AUM agents, this approach is preferable. Refer to Agent Profiles on page 78 of this document for more information.

After you have verified that the data migration was successful, you can set the **Uninstall AUM agent and clean up old data** option in the Agent configuration profile. This removes both the AUM agent and the XML file used during the migration.

Task 4: Remove the AUM policy in the HPCA Configuration Server Database.

After the AUM data has been migrated to DDM Inventory, you must manually remove the service-entitlement policy for the HPCA-AUM Agent Service from any and all devices. Use the HPCA Admin CSDB Editor to remove this policy. This permanently unplugs the usage policy from the CSDB.

For further information, refer to the *HPCA Configuration Server User's Guide* and the *HPCA Administrator User's Guide*.

Determining the Status of the Migration

In the DDM Inventory navigation tree, select **Status** > **Device Status** > **Agent status** to view a list of your network devices and the current status of the DDM Inventory Agents installed on them. By default, only those devices that have Agents are listed.

The last column in the table shows you the status of the AUM data migration process. There are four possible states that the migration can be in:

- No AUM agent—an AUM agent is not present on this system.
- Succeeded—the AUM agent on this system was successfully upgraded, and the AUM data was imported into the DDM Inventory database.
- Failed—Either the AUM agent was not upgraded to version 5.11 (or later) and cannot be migrated, or an error occurred during the data export process.
- No data—DDM Inventory has not yet contacted the device and, therefore, has no information about whether or not the AUM agent is running.

If the AUM migration status is Failed, the error message will tell you specifically why the migration failed. The following are possible reasons that the migration could fail:

- Obsolete DDMI agent version
- Unable to open AUM Usage DB file
- Handle to AUM Usage DB File is NULL
- AUM internal error
- Unable to invoke AUM export utility
- Unable to write / create usage XML files or output path unavailable
- Cannot read exported AUM data or agent may not support DDM Inventory output format
- AUM agent uninstallation has failed

In the last case, the migration itself may have succeeded, but the post-migration clean-up failed. See Agent Profiles on page 78 for more information.

Viewing Your Migrated Data

You can view your migrated data, and any additional utilization data collected by DDM Inventory after the migration, in two ways:

- Using **Reports** > **Application Reports**
- Using the **Scan Data Viewer** for a particular device.

For information about using these tools, refer to the *HP DDM Inventory Network Data Analysis Guide*.

Index

D

E

F

H

I

K