

# HP Discovery and Dependency Mapping Inventory

for the Windows<sup>®</sup> operating system

Software Version: 9.30

---

## Network Data Analysis Guide

Manufacturing Part Number: None  
Document Release Date: February 2011  
Software Release Date: February 2011



## 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

© Copyright 1993-2011 Hewlett-Packard Development Company, L.P.

### 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 Oracle Corporation.

UNIX® is a registered trademark of The Open Group.

Intel® is a 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](http://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](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 | Introduction                                      | 9  |
| 2 | Finding Network Devices                           | 11 |
|   | How to Find Your Devices                          | 11 |
|   | Finding Devices                                   | 12 |
|   | Easy Find   | 14 |
|   | Basic Match                                       | 15 |
|   | Asset Match                                       | 16 |
|   | IP Address  | 19 |
|   | MAC Address                                       | 20 |
|   | DNS Query   | 21 |
|   | Advanced Find                                     | 21 |
| 3 | Using the Network Map                             | 23 |
|   | How Does the Map Work?                            | 24 |
|   | Status Bar  | 24 |
|   | What are the Icons on the Map?                    | 25 |
|   | Devices and Packages                              | 26 |
|   | Connector Devices                                 | 26 |
|   | Priority  | 27 |
|   | Package Icons Group other Icons Together          | 27 |
|   | Icon Appearance                                   | 28 |
|   | Customizing the Network Map View                  | 29 |
|   | Changing Map User Preferences                     | 29 |
|   | Changing the Map Background Image                 | 33 |
|   | Managing Your Background Image Library            | 34 |
|   | Packaging Your Network                            | 34 |
|   | How Packaging Works                               | 35 |
|   | How You Can Request the Creation of Packages      | 36 |
|   | How You Can Create Your Own Packages              | 37 |
|   | How You Can Unpack Your Packages                  | 38 |
|   | How to Create Locked Objects                      | 38 |
|   | How to Change the Automatic Packaging Preferences | 39 |
|   | Organizing Map Configuration Files                | 42 |
|   | What is a Map Configuration?                      | 42 |
|   | Prime Configuration                               | 43 |
|   | Saving Your Changes                               | 43 |
|   | Starting a Map Configuration                      | 43 |
|   | Saving a Map Configuration File                   | 43 |

|  |           |
|--|-----------|
| Saving the Prime Map Configuration . . . . .                                   | 44        |
| Opening a Saved Map Configuration File . . . . .                               | 45        |
| Managing Map Configuration Files . . . . .                                     | 45        |
| Saving a Map Window as a Graphic File . . . . .                                | 47        |
| <b>4 Using the Service Analyzer . . . . .</b>                                  | <b>49</b> |
| Choosing Your Path . . . . .   | 49        |
| Service Analyzer Window . . . . .  | 50        |
| User Interface . . . . .   | 50        |
| Path Diagram . . . . .   | 51        |
| Full-Path Graphs Tab . . . . .   | 51        |
| <b>5 Using the Health Panel . . . . .</b>                                      | <b>53</b> |
| Viewing Network Overview with Health Panel . . . . .                           | 53        |
| Customizing the Alarms List . . . . .  | 54        |
| Using the Aggregate Health Panel . . . . .                                     | 55        |
| Servers button . . . . .   | 55        |
| <b>6 Using the Alarms Viewer . . . . .</b>                                     | <b>57</b> |
| Using the Alarms Viewer . . . . .  | 58        |
| Using the Aggregate Alarms Viewer . . . . .                                    | 59        |
| Saving Data to a Text File . . . . .   | 59        |
| <b>7 Using the Events Browser . . . . .</b>                                    | <b>61</b> |
| Events Browser . . . . .   | 61        |
| Opening the Events Browser . . . . .   | 62        |
| Network Events . . . . .   | 62        |
| Access Events . . . . .  | 63        |
| Toolbar . . . . .  | 67        |
| Using the Aggregate Events Browser . . . . .                                   | 67        |
| <b>8 Using the Device Manager . . . . .</b>                                    | <b>69</b> |
| List of Device Manager Panels . . . . .  | 70        |
| Configuration . . . . .  | 72        |
| Reports . . . . .  | 79        |
| Diagnosis . . . . .  | 80        |
| Diagnostic Information . . . . .   | 81        |
| Agent Deployment Log . . . . .   | 87        |
| Scanner Deployment Log . . . . .   | 88        |
| Virtual Log . . . . .  | 88        |
| Mobile Discovery Log . . . . .   | 88        |
| IP Ping . . . . .  | 88        |
| Traceroute . . . . .   | 88        |
| SNMP Ping . . . . .  | 89        |
| Agent Ping . . . . .   | 90        |
| DNS Query . . . . .  | 90        |
| Special Note about Using the Diagnosis Tools with Aggregator Servers . . . . . | 91        |
| Ports . . . . .  | 91        |

|   |            |
|---|------------|
| View Scan Data . . . . .                                  | 92         |
| Web . . . . .   | 92         |
| Update Model (Administrator or IT Manager) . . . . .      | 93         |
| Special Note about the Query Device Panel . . . . .       | 97         |
| <b>9 Using the Port Manager . . . . .</b>                 | <b>99</b>  |
| List of Port Manager Panels . . . . .                     | 99         |
| Configuration . . . . .                                   | 101        |
| State . . . . .   | 103        |
| Reports . . . . .   | 103        |
| Diagnosis . . . . .                                       | 104        |
| Statistics . . . . .                                      | 107        |
| Purge Port . . . . .                                      | 109        |
| Create Connection (Administrator or IT Manager) . . . . . | 109        |
| Break Connection (Administrator or IT Manager) . . . . .  | 110        |
| Port Properties . . . . .                                 | 110        |
| <b>10 Using the Line Manager . . . . .</b>                | <b>113</b> |
| Single Line Manager . . . . .                             | 113        |
| List of Line Manager Panels . . . . .                     | 114        |
| About . . . . .   | 114        |
| Break Connection (Administrator or IT Manager) . . . . .  | 115        |
| Multiple Line Manager . . . . .                           | 115        |
| <b>11 Using the Attribute Manager . . . . .</b>           | <b>117</b> |
| List of Attribute Manager Panels . . . . .                | 117        |
| Configuration . . . . .                                   | 118        |
| Manage (Administrator or IT Manager) . . . . .            | 119        |
| Purge Attribute (Administrator or IT Manager) . . . . .   | 120        |
| <b>12 Using the MIB Browser . . . . .</b>                 | <b>121</b> |
| Opening the MIB Browser . . . . .                         | 121        |
| Parts of the MIB Browser . . . . .                        | 122        |
| Tree View . . . . .                                       | 124        |
| Pull-down List of Devices . . . . .                       | 124        |
| Find Function . . . . .                                   | 124        |
| Credentials Function . . . . .                            | 125        |
| Locate on Map . . . . .                                   | 125        |
| Get Next . . . . .  | 126        |
| Refresh . . . . .   | 126        |
| Folder Tab . . . . .                                      | 126        |
| Variable Tab . . . . .                                    | 127        |
| MIB Description . . . . .                                 | 128        |
| Read and Write Credentials . . . . .                      | 128        |
| Walking the MIB . . . . .                                 | 129        |
| Using Multiple MIB Browser Sessions . . . . .             | 130        |
| Watching an OID with MIB Radar . . . . .                  | 130        |

|  |            |
|--|------------|
| Saving MIB Data as a Text file .....                   | 131        |
| Save Table Data .....                                  | 131        |
| MIB Walk .....   | 131        |
| <b>13 Using the Scan Data Viewer .....</b>             | <b>133</b> |
| Opening the Scan Data Viewer .....                     | 133        |
| Parts of the Scan Data Viewer .....                    | 134        |
| Pull-down List of Devices .....                        | 134        |
| Find Function .....                                    | 134        |
| Locate on Map .....                                    | 134        |
| Refresh .....  | 134        |
| Using Multiple Scan Data Viewer Sessions .....         | 135        |
| Menu Commands .....                                    | 135        |
| Viewing Hardware and Configuration Data .....          | 135        |
| Hardware and Configuration Data Page Overview .....    | 135        |
| The Hardware and Configuration Tab Page Layout .....   | 136        |
| Viewing Software Application Data .....                | 137        |
| Software Application Tab .....                         | 137        |
| Information Shown in the Application Data Window ..... | 138        |
| Software Utilization .....                             | 140        |
| <b>14 Using the Reports .....</b>                      | <b>143</b> |
| Report Periods .....                                   | 144        |
| Recognition Options in Reports .....                   | 144        |
| Finding Information in a Report .....                  | 144        |
| Executive/Summary Network Reports .....                | 145        |
| Scanned Device Reports .....                           | 146        |
| Scanned Device Summaries .....                         | 146        |
| Software Inventory Reports .....                       | 149        |
| Recognized Applications .....                          | 149        |
| OS Reported Applications .....                         | 152        |
| Unrecognized Files .....                               | 153        |
| Virtualization Reports .....                           | 154        |
| Mobile Device Reports .....                            | 155        |
| WAN Reports .....                                      | 156        |
| LAN Reports .....                                      | 156        |
| Device Reports .....                                   | 156        |
| Remote Management Cards Reports .....                  | 157        |
| <b>Index .....</b>                                     | <b>159</b> |



---

# 1 Introduction

HP DDM Inventory™ collects a lot of different data from your network devices. This guide will help you understand how to read the data collected by DDM Inventory's discovery features.

For information on data collected by DDM Inventory scanners, refer to the *Scan Data Analysis Guide*.

This guide provides information on the following topics:

- [Finding Network Devices](#) on page 11
- [Using the Network Map](#) on page 23
- [Using the Service Analyzer](#) on page 49
- [Using the Health Panel](#) on page 53
- [Using the Alarms Viewer](#) on page 57
- [Using the Events Browser](#) on page 61
- [Using the Device Manager](#) on page 69
- [Using the Port Manager](#) on page 99
- [Using the Attribute Manager](#) on page 117
- [Using the MIB Browser](#) on page 121
- [Using the Scan Data Viewer](#) on page 133
- [Using the Reports](#) on page 143



## 2 Finding Network Devices

The Find command lets you locate and examine any device on the network. There are many ways to search for a particular device, based on its DNS name, IP address, MAC address, and so on.

There is also an Aggregate Find feature that will let you search for devices across all of your aggregated DDM Inventory servers. The Aggregate Find is almost identical to the regular Find, but the Aggregate Find has fewer search options. The Easy Find option is now available within Aggregate Find.

The following sections explain the Find command in detail:

- [How to Find Your Devices](#) on page 11
- [Finding Devices](#) on page 12
- [Easy Find](#) on page 14
- [Basic Match](#) on page 15
- [Asset Match](#) on page 16
- [IP Address](#) on page 19
- [MAC Address](#) on page 20
- [DNS Query](#) on page 21
- [Advanced Find](#) on page 21

### How to Find Your Devices

There are six Find modes.

**Table 1** Types of Find

| Name        | Why use it?   |
|-------------|---|
| Easy Find   | This option is a “catch-all” that should be good for most searches. Read more details about it in <a href="#">Easy Find</a> on page 14. |
| Basic Match | A Basic match allows you to perform a search based on various device attributes.  |
| Asset Match | An Asset match allows you to perform a search based on asset data collected.  |

**Table 1 Types of Find**

| Name        | Why use it?  |
|-------------|--|
| IP Address  | Find a device with a specific IP address.  |
| MAC Address | Find a device with a specific MAC address.   |
| DNS Query   | Do a DNS Query on a specific domain name.<br>Note: Not available with Aggregator Find. |


## Finding Devices

To use the Find tool:

- 1 Open the Find tool:

**Table 2 Opening Find**

| From   | Click                  |
|--|------------------------|
| Navigation Tree  | Find                   |
| Health Panel, Network Map, Alarms Viewer, Events Browser, MIB Browser, or Service Analyzer | <b>Tools &gt; Find</b> |

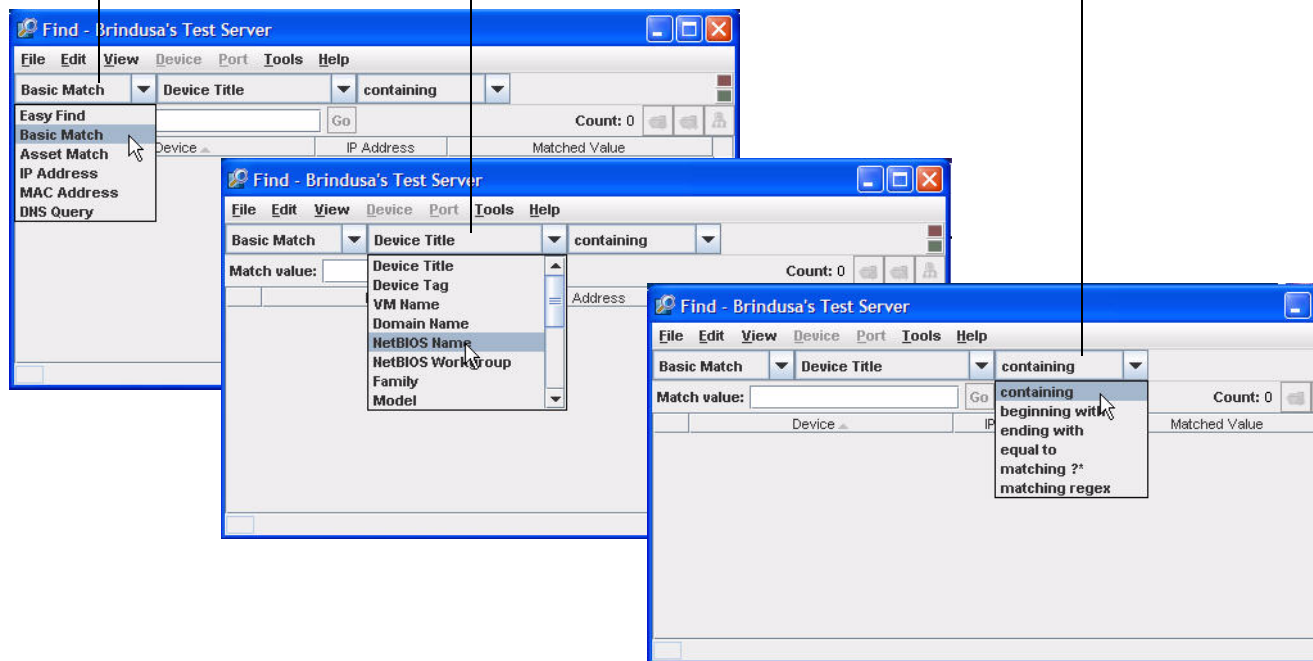
- 2 By default, you can use the **Easy Find** feature (go to [step 6](#)). If you want to do a more advanced find, continue with the next step in this procedure.
- 3 In the first pull-down list, select the Find mode you want to use to perform the search (for example, “Basic Match”).
- 4 In the second pull-down list, select the device data you want to search on (for example, “NetBIOS Name”).
- 5 In the third pull-down list, select a match mode (for example, “containing”). (For explanation of these match modes, see [Advanced Find](#) on page 21).
- 6 Enter a match value.
  -  When using Easy Find, enter the first letters of a title or the first numbers of an address to find multiple devices in the DDM Inventory database.
- 7 Press **Enter** or click **Go**.


DDM Inventory searches for the device. The results of the search appear in table format, and you can select the device you want to open. You can double-click (or right-click) to open a Device Manager or Port Manager.

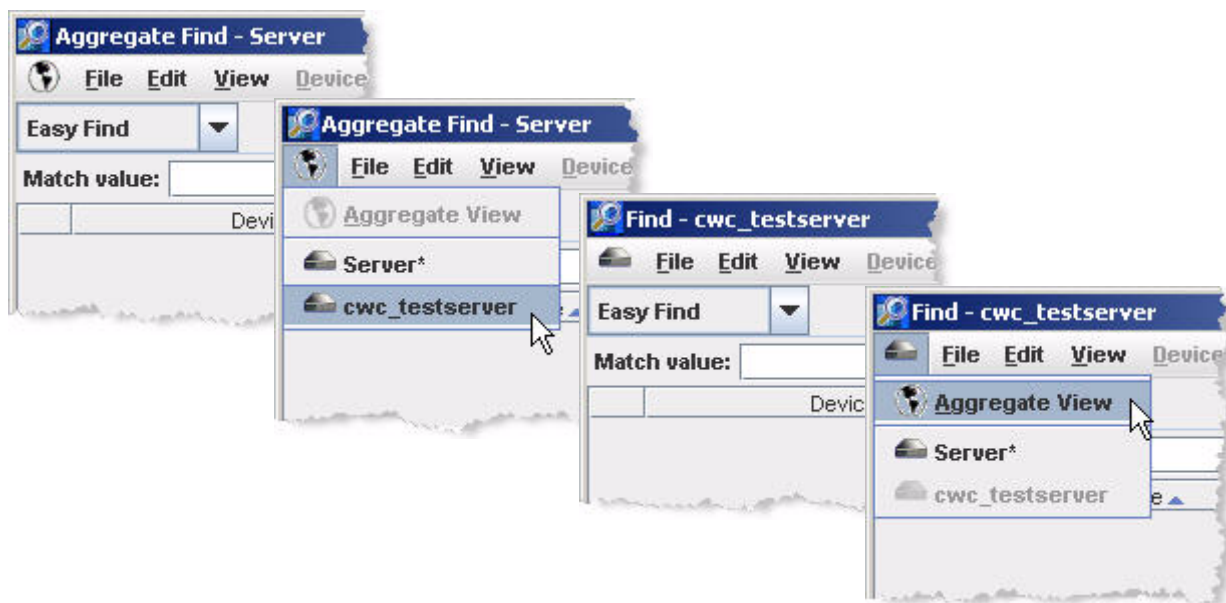
Select the Find mode


Select the device data

Select a match mode



The Aggregate Find window has a  (globe) icon to the left of the File menu on the main menu bar. When you click this icon, you can open the Find window for one of the remote servers associated with this Aggregator:



The Find window for an individual server has a  (server) icon instead of a globe icon. When you click the server icon, you can either return to the Aggregate Find window or open the Find window for any other remote server associated with this Aggregator.

## Easy Find

When you enter text into the Find box, DDM Inventory searches the network in the following order. If there is no result at one stage, DDM Inventory will try the next. For example, once an IP address has been found, DDM Inventory does not search domain names and device titles.

**Table 3 Internal Search Order for the Easy Find**

| Find Method          | Explanation   |
|----------------------|---|
| “localhost” or “nmc” | These are two shortcuts for finding the DDM Inventory server.   |
| MAC address          | DDM Inventory will try to search based on the known MAC address.<br>Note: To find a specific device, you can either enter its complete MAC address in <b>12:AB:34:CD:56:EF</b> , <b>12AB34CD56EF</b> , or <b>12AB34 CD56EF</b> format, or you can use wildcard characters. Refer to <a href="#">MAC Address</a> on page 20 for detailed instructions. |
| IPv4 or IPv6 address | DDM Inventory will try to search based on the known IP address (IPv4 or IPv6).<br>Note: To find a specific device, you can either enter its complete IPv4 or IPv6 address, or you can use wildcard characters. Refer to <a href="#">IP Address</a> on page 19 for detailed instructions.  |
| Device Title         | DDM Inventory will then search the network based on your device title preferences from <b>Administration &gt; System Configuration &gt; Display preferences &gt; Device title preference</b> . Only the selected titles are searched.   |
| Asset Tag            | Even if Asset Tag is not listed in your Device title preference, DDM Inventory will search for it next.   |
| NetBIOS Name         | Even if NetBIOS name is not listed in your Device title preference, DDM Inventory will search for it next.  |
| Domain Name          | DDM Inventory searches based on the DNS suffix as configured in your server DNS (done in Control Panel).  |

Easy Find now finds ports as well as devices. If you specify an IP or MAC address, and that address is associated with a port, you will see a value in the Port column of your Easy Find results.



The Find tool treats incomplete IP and MAC addresses differently than addresses that contain wildcard characters.

For example, if you enter “192.168.2”, you will not find all devices in the range 192.168.2.0–192.168.2.255. You will find only devices with “192.168.2” in the device title. If the device with IP address 198.168.2.55 gets its title from its domain name instead of its IP address, that device will not be found.

If, on the other hand, you specify “192.168.2.\*”, you will find all devices in the range 192.168.2.0–192.168.2.255 that DDM Inventory has thus far discovered in your network.



When you use Easy Find, it may take several seconds to get a response—especially on a large network.

## Basic Match

**Table 4 Basic Match**

| <b>Name</b>       | <b>Why use it?</b>   | <b>Examples</b>   |
|-------------------|--|---|
| Device Title      | Find a device when you know the name, but not necessarily the type of device.  | 172.22.5.5<br>anydevice.example.com   |
| Device Tag        | Find a device with a specific device tag. A device tag is a short descriptive string assigned to this type of device.<br><br>You can also enter a partial device tag to find several devices with similar numbers. | VMware or Microsoft   |
| VM Name           | Find a VMware virtual machine by its VM name.  | VM_WinXP  |
| Domain Name       | Find a device with a specific domain name.   | anydevice.example.com<br>hp.com   |
| NetBIOS Name      | Find a device with a specific NetBIOS name.  | NT4WORKQA<br>mymachine  |
| NetBIOS Workgroup | Find a device within a specific NetBIOS workgroup.   | QA_SAN_DIEGO<br>ACTIVE  |
| Family            | Find a device within a specific family.  | Cisco 2600 Series Modular Access Routers<br>WaveSwitch 1000 Series Workgroup Switch   |
| Model             | Find a device of a specific model.   | IBM xSeries 330 (867411X)<br>Cisco Intelligent Gigabit Ethernet Switch Module (IGESM) |
| Operating System  | Find a device with a specific operating system.  | Linux<br>HP-UX 11.0   |
| Network Function  | Find a device which serves a specific network function.  | router  |
| SNMP Description  | Find a device with a specific description in the SNMP MIB.   | Linux Virtual Gateway<br>3Com SuperStack II   |
| SNMP Contact      | Find a device with a specific contact in the SNMP MIB.   | Kevin<br>IT Manager   |
| SNMP Name         | Find a device with a specific name in the SNMP MIB.  | Demo Server<br>manager.example.com  |

**Table 4 Basic Match**

| Name                | Why use it?   | Examples              |
|---------------------|---|-----------------------|
| SNMP Location       | Find a device with a specific location in the SNMP MIB.   | server room<br>QA LAB |
| SNMP Serial Number  | Find a device with a specific serial number in the SNMP MIB.  | 12345ABCDE            |
| Mobile Phone Number | Find a mobile device with a specific phone number. This option is only available when mobile discovery is active. <sup>a</sup>  | 888-555-1212<br>613   |
| Mobile User Name    | Find a mobile device with a specific user name. This option is only available when mobile discovery is active and mobile user names are collected. <sup>a</sup><br>See <a href="#">Special Note About Mobile User Names</a> on page 16. | Smith<br>Wong, James  |

- a. See [Enabling and Disabling Mobile Discovery](#) and [Protecting Private Information for Mobile Devices](#) in the *Reference Guide* for more information.

### Special Note About Mobile User Names

In the DDM Inventory database, mobile user names are stored in two parts: the first name and the last name. To find mobile devices based on a Mobile User Name, you can specify either the first name, the last name, or both. Use a comma (,) to separate the names when you type them in the **Match value** box, as shown here:

| Search by                | Match value format                 | Example              |
|--------------------------|------------------------------------|----------------------|
| Last name                | <last name><br>or<br><last name> , | Wong<br>or<br>Wong , |
| First name               | , <first name>                     | , James              |
| Both first and last name | <last name> , <first name>         | Wong, James          |

Spaces between the names are ignored. The results of the Find operation are displayed in <last name> , <first name> format.

## Asset Match

An Asset match allows you to perform a search based on asset data collected. It includes details about users, departments, physical assets, equipment, and any other information that is useful to record.



There are three methods of collecting asset data: scanner, bulk import, or Web Asset Questionnaire (WAQ). One or multiple methods can be used for a device but the order of priority is as follows:

- Web Asset Questionnaire
- Bulk import
- Scanner

When you perform a Find query, the search query will look at all three levels in the priority order.

For example, a device may be picked based on the AssetTag collected by the scanner if the value matches and there is no AssetTag collected through either the WAQ or bulk import.

The resultant value is always the one collected by the method with the highest priority.

**Table 5 Asset Match**

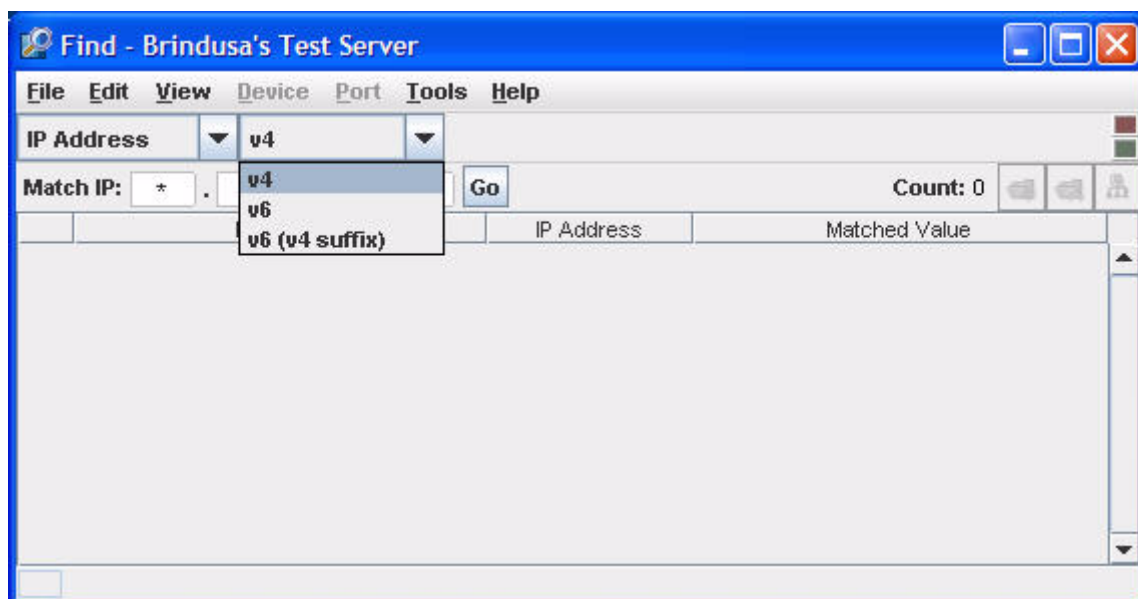
| <b>Name</b>   | <b>Why use it?</b>   | <b>Examples</b>         |
|---------------|--|-------------------------|
| Description   | Find a device from the Description line that contains a brief description of the asset.  | Development Machine     |
| Asset Tag     | Find a device with a specific asset tag. The Asset Tag field contains a unique identifier for the machine.<br>You can also enter a partial asset tag to find several devices with similar numbers. | EXAMPLE123456<br>123456 |
| Employee ID   | Find devices from a specific Employee ID as used in the organization.  | FINANCE3746             |
| Last Name     | Find devices with a specific last name of user   | SMITH                   |
| Full Name     | Find devices with a specific full name of user   | JOHN SMITH              |
| Job Title     | Find devices with a specific job title of user   | IT Manager              |
| Cost Center   | Find devices with a specific cost center description or code   |                         |
| Business Unit | Find devices with a specific name of business unit   |                         |
| Division      | Find devices with a specific division description or code  |                         |
| Department    | Find devices with a specific department description or code  | IT32                    |
| Section       | Find devices with a specific section description or code   |                         |

**Table 5 Asset Match**

| <b>Name</b>         | <b>Why use it?</b>   | <b>Examples</b>         |
|---------------------|--|-------------------------|
| Office Location     | Find devices with a specific location of office.   | UKRichmond              |
| Building            | Find devices from the building containing the machine  | RICHMOND                |
| Floor               | Find devices with a specific floor on which the machine is located   | first                   |
| Room                | Find devices with a specific description, name or number of the room containing the machine  | Room5                   |
| Bar Code            | Find a device with a specific bar code.  |                         |
| Telephone Extension | Find devices with a specific internal telephone extension  | 3256                    |
| Telephone Number    | Find devices with a specific full direct telephone number of user  | 020 8956 5569           |
| Cellphone Number    | Find devices with a specific cell/mobile phone number of user  | 07285692658             |
| Printer Description | Find devices with a specific description of a local printer attached to the machine, if any  | FinancePrinter          |
| Printer Asset Tag   | Find devices with a specific from the Asset tag of a local printer attached to the machine, if any   | FinancePrinter1234      |
| Machine Make        | Find devices with a specific Make or Manufacturer of the machine. This data is automatically collected on machines supporting SMBIOS   | HP                      |
| Machine Model       | Find devices from the Model of the machine. This data is automatically collected on machines supporting SMBIOS   |                         |
| Device Type         | Find devices from the Device type of the machine.  | Server, Notebook, Tower |
| User field 29       | User field 29 is the default label for a user defined field.<br>When the field is configured in the User Interface, the field is given a meaningful name.<br>The user defined fields will show in the Asset Match list only if a custom label is being used for a field. |                         |

# IP Address

The Find function enables you to search for devices using IPv4, IPv6, or IPv6 with the IPv4 suffix format:



**Table 6** IP Address

| Name       | Why use it?                               | Examples   |
|------------|---|--|
| IP Address | Find a device with a specific IP address. | 172.22.5.5<br>172.*.*.255<br>1080:0:0:0:8:800:200C:417A<br>1080::8:800:200C:417A<br>1080::8:800:200C:129.144.52.38 |

Depending on the IP format you choose, you specify the IP address as follows:

- IPv4 – 123.123.123.123
- IPv6 – 1234:ABCD:1234:ABCD:1234:ABCD:1234:ABCD
- IPv6:v4 suffix – 1234:ABCD:1234:ABCD:1234:ABCD:123.123.123.123

To find multiple devices, you can substitute an asterisk (\*) for an octet in an IPv4 address or a group of four hexadecimal digits in an IPv6 address. You can also copy/paste IP addresses in these fields. The following are valid search strings:

The first screenshot shows an 'IP Address' dropdown set to 'v4'. The 'Match IP' field contains '123 . 123 . \* . \*' and a 'Go' button.

The second screenshot shows an 'IP Address' dropdown set to 'v6'. The 'Match IP' field contains '\* : \* : \* : \* : 1234 : abcd : \* : \*' and a 'Go' button.

The third screenshot shows an 'IP Address' dropdown set to 'v6 (v4 suffix)'. The 'Match IP' field contains '\* : \* : \* : \* : \* : \* : \* : \* . \* . \* . \*' and a 'Go' button.

- ▶ All IPv6 notation formats specified by the RFC2373 standard are supported. The last example above is a format, where the last eight hexadecimal digits in the IPv6 address are represented as an IPv4 address.
- ▶ If you specify an IP address, and that address is associated with a port, you will see this port listed in your Find (or Easy Find) results.

## MAC Address

**Table 7 MAC Address**

| Name        | Why use it?   | Examples                             |
|-------------|---|--------------------------------------|
| MAC Address | Find a device with a specific MAC address.<br>Note: You can use asterisks (*) to find multiple devices. | 12:AB:34:CD:56:EF<br>12:*:34:*:56:EF |

You must specify the MAC address in the following format: 12:AB:34:CD:56:EF  
You can substitute a \* for a segment of a MAC address. The following, for example, are valid search strings:

The first screenshot shows a 'MAC Address' dropdown. The 'Match MAC' field contains '12 : \* : \* : \* : \* : \*' and a 'Go' button.

The second screenshot shows a 'MAC Address' dropdown. The 'Match MAC' field contains '12 : AB : \* : CD : 56 : EF' and a 'Go' button.

The third screenshot shows a 'MAC Address' dropdown. The 'Match MAC' field contains '\* : AB : \* : CD : \* : EF' and a 'Go' button.

You cannot omit leading zeros in a MAC address segment. For example, you cannot enter “5” instead of “05” for a segment.

- ▶ If you specify a MAC address, and that address is associated with a port, you will see this port listed in your Find (or Easy Find) results.

## DNS Query

**Table 8 DNS Query**

| Name      | Why use it?  | Examples   |
|-----------|--|------------|
| DNS Query | Do a DNS Query on a specific domain name.<br>Note: Not available with Aggregator Find. | www.hp.com |

## Advanced Find

For the advanced find option, there are different match modes that will help your search. These modes are described in the following table.

- ▶ Searches are not case-sensitive.

**Table 9 Advanced Find**

| Match Modes    | Notes  |
|----------------|--|
| containing     | —  |
| beginning with | —  |
| ending with    | —  |
| equal to       | —  |
| matching ?*    | Wildcard characters: <ul style="list-style-type: none"><li>• “?” can represent any single character. For example, “gr?y” finds “gray” and “grey.”</li><li>• “*” can find multiple characters. For example, “E*t” finds “Ethernet.”</li></ul> |
| matching regex | Matching a regular expression.<br>Note: For some examples of regular expressions, see the Analysis Workbench chapter in the <i>Scan Data Analysis Guide</i> .  |



---

## 3 Using the Network Map

You can only use the Network Map if you have an DDM Inventory topology license.

The Network Map gives you a graphical view of your network, using icons and lines that represent the devices in your network and their connectivity.

There are many ways to change how you view the map. You can change the layout, and many look-and-feel features. You can even save different layouts (configuration files) in case you want to look at the network in different ways.

This chapter will start off by explaining what you first see on the map (icons, lines), and then get into details about how to change the map.

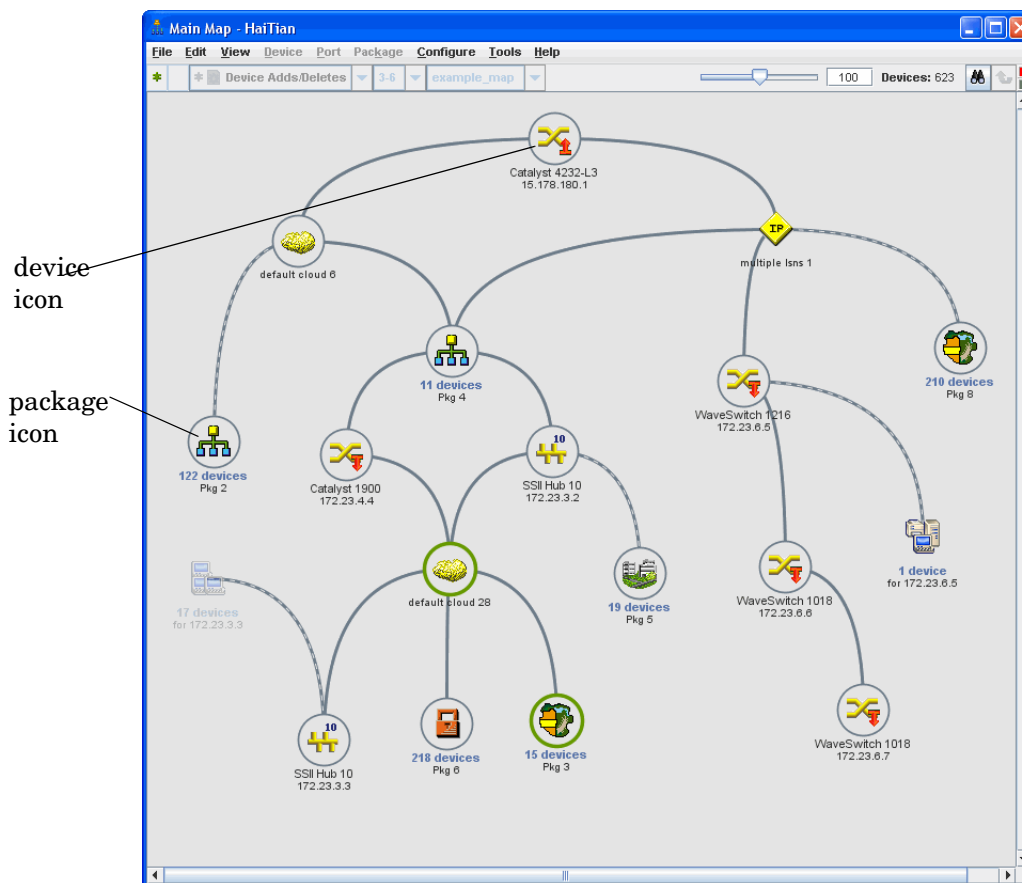


The map is generated automatically based on the data gathered through the discovery process. If the source data is reliable, the map will accurately represent your network. There may be cases where information is not available for certain devices or connections. In these cases, DDM Inventory will make its best “guess” about connectivity.

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

- [How Does the Map Work?](#) on page 24
- [What are the Icons on the Map?](#) on page 25
- [Customizing the Network Map View](#) on page 29
- [Changing the Map Background Image](#) on page 33
- [Managing Your Background Image Library](#) on page 34
- [Packaging Your Network](#) on page 34
- [Organizing Map Configuration Files](#) on page 42
- [Saving a Map Window as a Graphic File](#) on page 47

## How Does the Map Work?



To determine what the Map will display, select an alarm category on the Health Panel or Alarms Viewer, or click the alarm list on the map status bar. For more information, see [Status Bar](#) on page 24.

The colored ring around an icon indicates the device's status for the category you select. For example, if you select Device Adds/Deletes, any devices that were recently added will have green rings.

- To show rings, the objects must be within the priority range as selected on the map status bar, Health Panel, or Alarms Viewer. (Information about setting device priorities is in the *Configuration and Customization Guide*.)
- Devices and ports that do not have applicable attribute or report data will not have a ring (for example, connector devices).

### Status Bar

The Status Bar appears at the top of every map window. It displays information about the window contents, and allows you to change the window display.



The following graphic shows the Status Bar. The table below the graphic explains the features available on the Status Bar.



Some parts of the Status Bar duplicate information available on the Health Panel.



**Table 1    Toolbar Legend**

| Number | Name  |
|--------|---|
| 1      | package alarm state   |
| 2      | object alarm state (displayed when you mouse over an object on the map) |
| 3      | alarm type pull-down list   |
| 4      | priority range pull-down list   |
| 5      | map configuration file  |
| 6      | map scale slider  |
| 7      | map scale percentage in this window                                     |
| 8      | number of devices in this package                                       |
| 9      | Find a device   |
| 10     | go up one level   |
| 11     | connectivity (green = OK, red = no connection to server)                |

## What are the Icons on the Map?

The following sections describe the different icons you will encounter on the Network Map:



- [Devices and Packages](#) on page 26
- [Connector Devices](#) on page 26
- [Priority](#) on page 27
- [Package Icons Group other Icons Together](#) on page 27
- [Icon Appearance](#) on page 28

## Devices and Packages

DDM Inventory tries to develop a realistic view of your network, and that view is represented with icons (representing a device or a group of devices) and lines that connect the devices.

The icons on the map fall into categories:

**Table 2 Icon Categories**

| Icon Type     | Example   | Description  |
|---------------|---|--|
| Device Icons  |  An icon representing a Windows XP Pro workstation. It features the Windows XP logo and the text "Win XP Pro" and "win.example.com". | Device icons represent the physical equipment in your network.                   |
| Package Icons |  An icon representing a package of devices. It features a printer icon and the text "2 devices for 172.23.4.4".                      | A package is a collection of objects (objects means either devices or packages). |

DDM Inventory selects device icons based on the data collected from that device. For example, if DDM Inventory sees that a device is a Microsoft Windows 2000 workstation, that device will appear on the map with a “Win2000 Workstation” icon.



- ▶ DDM Inventory will usually select the correct device icon. If for some reason, the wrong icon has been selected, you can change it. See [Customizing the Network Map View](#) on page 29.

## Connector Devices

When DDM Inventory is unable to determine the exact physical, port-level connectivity between devices, it displays the connection with a connector device icon representing the logical subnet.

DDM Inventory creates two types of connector devices: clouds and diamonds.

**Table 3 Connector Devices**

| Icon Type | Example  | Description  |
|-----------|--|--|
| Cloud     |  A yellow, textured cloud icon representing a logical subnet.                       | Clouds represent one or more devices or MAC systems that provide connectivity in the network.  |
| Diamond   |  A yellow diamond icon with the letters "IP" inside, representing a logical subnet. | Diamonds do not represent actual network devices; they indicate connectivity. Sometimes, DDM Inventory knows that there is connectivity without being able to specify the devices. |

For more information on the real and connector devices, see the Reference Guide.

You can see a complete list of all the icons used in DDM Inventory in **Help > Classifications > Device Types/Package Types**.

## Priority


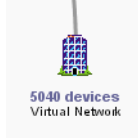
In DDM Inventory, devices can have priorities 1–6. Devices with priority 1 are the least important. The higher the number, the higher the priority and greater the importance.

By default, priorities 5 and 6 are reserved for the user. By default, priority 6 is reserved for those devices that should trigger event notification—see the Event Filters chapter in the *Configuration and Customization Guide*.

## Package Icons Group other Icons Together

DDM Inventory helps you organize and simplify your Network Map with packages. A package is a collection of objects (objects means either devices or packages) that is represented by an icon. You can double-click a package icon to open the package in its own window. There are two types of packages:

**Table 4 Packages**

| Package Type         | Description  | Example  |
|----------------------|--|--|
| Automatic Package    | These packages are automatically created by DDM Inventory. For more information on packaging, see <a href="#">Packaging Your Network</a> on page 34.                                     |   |
| Multi-object Package | These packages are created by the user, and can contain any devices you wish to place in them. For more information on packaging, see <a href="#">Packaging Your Network</a> on page 34. |  |

Any map window can contain packages. You can modify the contents of a package (selecting objects or groups of objects) exactly as you can in the Main Map.

As with other icons, you will sometimes see package icons with colored rings around them (when you select an alarm type). The color of the ring around the package depends on the color of rings around objects inside the package. The ring around the package icon will match the most severe alarm of the devices in the package.





For example, if there are Critical (red), Minor (gold) and Info (green) rings inside a package, the package will have a Critical (red) ring.

For more information on packaging, see [Packaging Your Network](#) on page 34.




## Icon Appearance

The following table shows a device icon in the possible states as it will appear on the Network Map.

**Table 5 Icon Appearance**

| Appearance  | What it means  |
|---|--|
|    | <p><b>Normal Icon</b></p> <p>This is how a device icon will appear when:</p> <ul style="list-style-type: none"> <li>no alarms are selected</li> <li>an alarm has been selected but that type of alarm does not apply to this device</li> <li>an alarm has been selected but this device is not in the priority range</li> </ul>  |
|    | <p><b>Colored Ring</b></p> <p>A thin gray ring will appear around a device when:</p> <ul style="list-style-type: none"> <li>this device is in the priority range</li> <li>this device is not alarmed</li> </ul> <p>A colored ring will appear around a device when:</p> <ul style="list-style-type: none"> <li>an alarm is selected that exists on this device</li> <li>this device is in the priority range</li> </ul>  |
|  | <p><b>Faded Icon</b></p> <p>If an object appears faded, that means DDM Inventory has not seen that device for more than 24 hours. DDM Inventory will eventually deactivate such a device from the Network Map and, eventually, DDM Inventory will purge the device and all its associated data.</p>  |
|  | <p><b>Locked Icons</b></p> <p>If you have manually packaged your map configuration, you will see many icons with a blue line beneath them, if you have selected the “Underline locked objects” option in <b>Edit &gt; User Preferences</b>. The blue line indicates that the device has been manually packaged by a user, meaning it has been put inside a package (<b>Package</b> command), promoted from a package (<b>Promote</b>), or has had its package removed (<b>Unpackage</b>).</p> <p>DDM Inventory does create some automatic packages. They are created during discovery and whenever you use the <b>Pack</b> or the <b>Unpack All</b> commands.</p> <p>For more information on packaging, see <a href="#">Packaging Your Network</a> on page 34.</p> |

**Table 5 Icon Appearance**

| Appearance  | What it means   |
|---|---|
|  | <b>Selected Icon</b><br>If you select an icon on the Network Map, it will appear dark.  |
|  | <b>Found Icon</b><br>This icon was located on the Network Map using the Locate feature.<br>Note: For packages, the large yellow circle indicated that you have just left this package, as you are navigating through the Network Map. Also note that the package tag is a different color after you have been inside the package. |
|  | <b>Deactivated or Hidden Icon</b><br>This device has been manually deactivated or hidden by an Admin account. It will disappear from the Network Map at the end of the next network poll cycle.   |

## Customizing the Network Map View

There are several ways you can change the look and feel of your Network Map. Your account-type determines the preferences and properties you are allowed to change.

All accounts can change preferences such as line style, background color, background image, and scale.

Administrator or IT Manager users have the option of changing Device Properties such as device icon, device title, and so on (from the Network Map, click **Device > Device Properties**). These properties will affect all accounts.

[Changing Map User Preferences](#) on page 29 explains several ways that you can use to change the look of your Network Map.

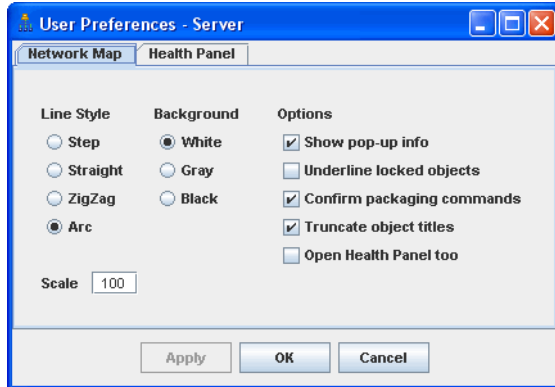
### Changing Map User Preferences

Topics in this section include:

- [Map Preferences](#) on page 30
- [Placing an Object at the Top of the Map Window](#) on page 31
- [Layout](#) on page 32
- [Promoting Objects](#) on page 32
- [Reverting Your Map Changes](#) on page 32

## Map Preferences

You can change the look of your Network Map in several ways. To open this dialog from the Network Map, click **Edit > User Preferences**.



**Table 6 Map Preferences**

| Preference                 | Description  |
|----------------------------|--|
| Line Style                 | This option lets you choose which style of line to draw to connect objects in a Network Map window. You can change this setting from the default (straight) whenever you wish.   |
| Background                 | This option lets you choose the background color for your map windows.   |
| Show pop-up info           | This option lets you choose whether an information box associated with an object or a line appears when you position the mouse pointer over an icon.   |
| Underline locked objects   | This option lets you choose if locked objects should be underlined in all map windows. Objects that are “locked” from a packaging status are shown with a blue line under the icon.<br><br>Typically, objects acquire locked status when they are packaged by a user. When an object is locked, DDM Inventory does not package or unpackage it automatically.                      |
| Confirm packaging commands | This option lets you choose if you will require confirmation when using packaging commands such as <b>Layout</b> , <b>Make Top of the Network</b> , <b>Unpackage</b> , <b>Pack</b> , <b>Unpack</b> , and <b>Unpack All</b> .<br><br>You receive a confirmation question that gives you time to reconsider what you are doing. You can turn confirmation messages off, if you wish. |

**Table 6 Map Preferences**

| Preference                         | Description   |
|------------------------------------|---|
| Truncate object titles             | This option lets you choose if you want to truncate object titles on your map. Sometimes, the object titles are very long, and DDM Inventory will automatically truncate them to save space on the map. If you would rather have the full object name appear on the map, you can change it.   |
| Scale                              | This option lets you choose the scale for all map windows.<br><br>Also, the scale slider appears on every map window. You can click this and change the scale to from as small as 1% up to 200%. You can also type in a number into the text box, and hit Enter on your keyboard to initiate the change.<br><br>You can also use the <b>Zoom In</b> and <b>Zoom Out</b> commands to change the scale of one map window at a time. |
| Open Health Panel with Network Map | This option lets you choose if the Health Panel will automatically be opened when you click open the <b>Network Map</b> .<br><br>Note: This setting does not affect the Aggregate Health Panel.   |

## Placing an Object at the Top of the Map Window

When you are organizing a map window, you can assign one object to appear at the top of the window. This object should be of special significance in relation to the other objects in the window.

DDM Inventory may not have been running long enough to show the right device at the top of the map, or you may know a top-of-network router or a core device would make more sense.



This preference will affect the current map configuration file.

To place an object at the top of the map window:

- 1 Select an icon.
- 2 Click **Configure > Top of Network**.  
A confirmation message appears.
- 3 Click **Top of Network**.

The window is redrawn with the selected icon at the top.

To reset the top object for the window to the default chosen by DDM Inventory:

- 1 Select the icon at the top of the map window.  
The **Top of Network** command should have a check mark with it, indicating that you have previously chosen this object to be at the top of the window.
- 2 Click **Configure > Top of Network**.

A confirmation message appears.

3 Click **Top of Network**.

The window is redrawn with the default icon at the top, as chosen by DDM Inventory.

## Layout

The **Layout** command reorganizes the layout of the active map window, then redraws the window. Use it to tidy a map with confusing layout and crisscrossing connections.

To clean up a map window:

- Click **Configure > Layout**.

This command will destroy any custom layout, but will not affect any of the packaging.

## Promoting Objects

The **Promote** command moves the selected objects to the window one level above the current window (in terms of hierarchy, not screen space).

To promote an object:

- Click **Configure > Promote**.

This command locks all selected objects (unless they are promoted into the Main Map).

▶ When the last object is promoted out of the package, the package is destroyed.

## Reverting Your Map Changes

If you are making changes to your map layout, and decide not to save your changes, you can **Revert** your map. This way, the autosave function will not save your changes.

▶ This feature works for changes to your map layout and packaging. Changes to the device properties (device tag, title, icon, or priority) or port properties cannot be reverted.

To revert your map to the version you last saved:

- 1 Click **File > Revert**.

A warning dialog appears.

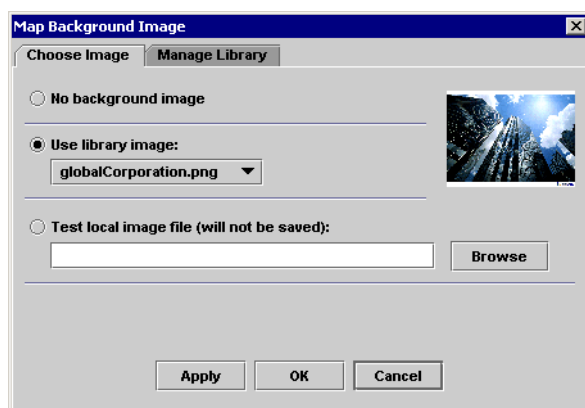
- 2 Click **OK**.



## Changing the Map Background Image

You can add images to your Network Map background (main map and packages).

There is a library of images you can select, all of which are available to all users. An Administrator or IT Manager account can add more pictures to the library (see [Managing Your Background Image Library](#) on page 34).



To test an image file from your computer:

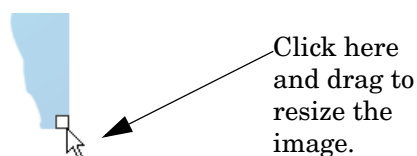
- 1 Click **Configure > Background Image**.  
The Map Background Image dialog appears.
- 2 Select **Test Local Image File** and browse to find the file you want.
- 3 Click **Apply**.

▶ This background will not be saved as part of your map configuration. Only files in the image library can be saved.

To select an image file from the library:

- 1 Click **Configure > Background Image**.  
The Map Background Image dialog appears.
- 2 Select an image from the image library pull-down list.
- 3 Click **Apply**.

The image will appear as the background of your map window. By default, the image will cover the entire map window. You can alter the size of the image by clicking and dragging the image from its bottom-right corner.



## Managing Your Background Image Library

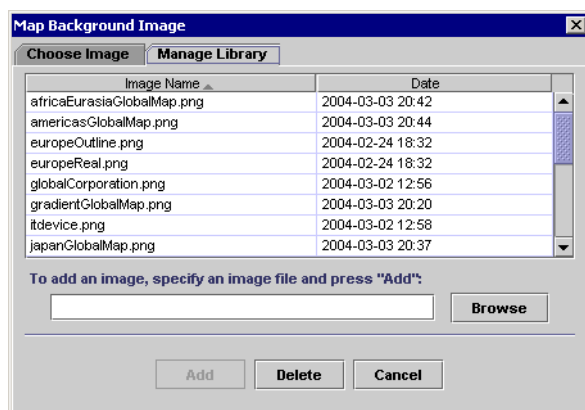
An Administrator or IT Manager account can add and delete images from the DDM Inventory image library. These images are available to every user, regardless of account type. .



If you add images that are larger than 250KB, you may notice the Network Map scrolling slowly



You will notice that the background images are dimmed slightly, so the image colors will not interfere with the map icons and lines. If you add your own images to the library, DDM Inventory will automatically dim the images, so you need not alter your graphic files before adding them to the library.



To add an image to the library:

- 1 Click **Configure > Background Image**.  
The Map Background Image dialog appears.
- 2 Select the Manage Library panel.
- 3 Click **Browse** and search for your image file.
- 4 Click **Add**.

To delete an image from the library:

- 1 Click **Configure > Background Image**.  
The Map Background Image dialog appears.
- 2 Select the Manage Library panel.
- 3 Select the file you want to delete.
- 4 Click **Delete**.

## Packaging Your Network

You can group objects into packages so that the map is more organized and easier to understand.

Regardless of your account type, you can package the network any way you want. You can also save different layouts and packages into map configuration files.

Topics in this section include:

- [How Packaging Works](#) on page 35
- [How You Can Request the Creation of Packages](#) on page 36
- [How You Can Create Your Own Packages](#) on page 37
- [How You Can Unpack Your Packages](#) on page 38
- [How to Create Locked Objects](#) on page 38
- [How to Change the Automatic Packaging Preferences](#) on page 39

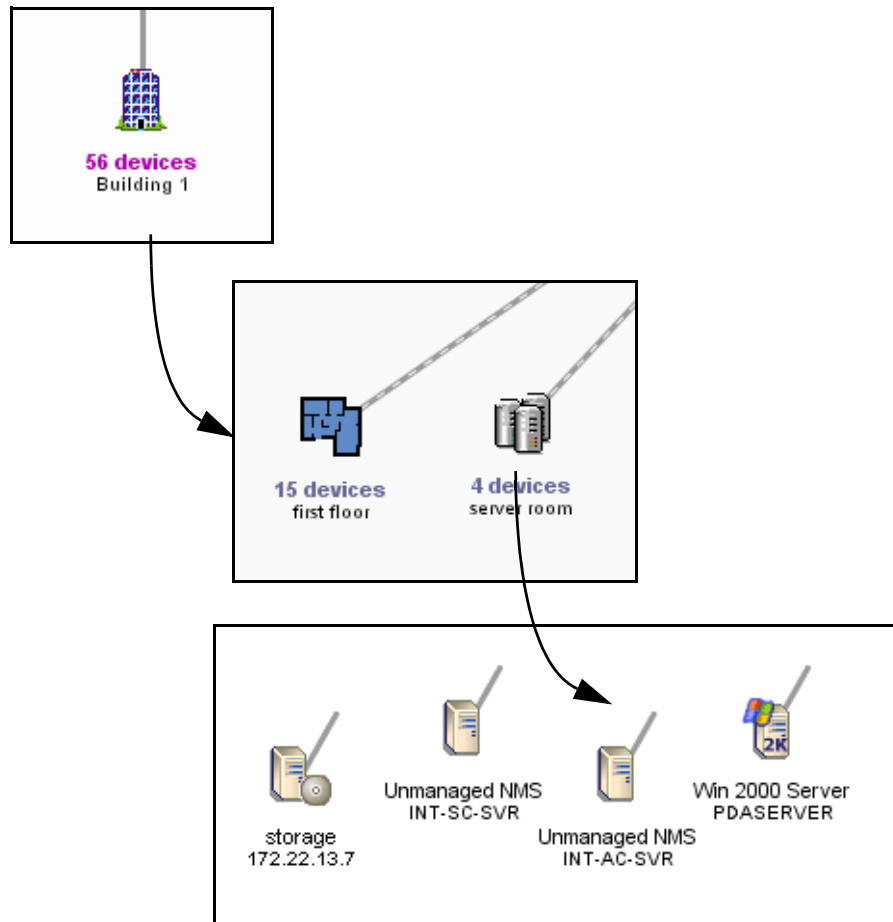
## How Packaging Works

By packaging devices, you can reduce the size of the Network Map. You can package your network differently in each map configuration file.

You can create packages to represent hierarchies, such as campuses, buildings, floors in buildings and so on. There are many package icons available to help you create the desired look and feel of the Network Map.

There are two types of packages: the type DDM Inventory creates automatically and the type you can create yourself.

One application of multi-object packaging is mapping the network at a physical location, such as a city. For example, in the figure below, the main map contains a package for Building 1. Drilling down one level, the Building 1 map contains packages for the first floor and the server room. Drilling down further, you reach the devices for the “server room” within the end node package.



## How You Can Request the Creation of Packages

DDM Inventory can create packages for you. This is a quick way to reduce the size of the Network Map. DDM Inventory will create a package for each port of the device at the top of the network. Each package will contain the devices connected to that port.

To have DDM Inventory create your multi-object packages:

- 1 Select a map window.
- 2 Click **Configure > Pack**.  
You are asked to confirm the action.
- 3 Click **Pack**.

The **Pack** command does not lock your objects on the Network Map.

The **Pack** command does not delete any existing packages. However, the **Pack** command will remove any other layout changes you have made.

If you wish, you can open each package and click **Pack** again to continue packaging your network.

Multi-object packages can be created by the user. DDM Inventory can create them with the **Pack** command, but if the packages are to be meaningful to you, it is best to create them yourself.

- ▶ Exception: While customizing your network, you may decide to use the **Unpack All** command. This command will destroy all the packages you have created. However, DDM Inventory will recreate all of the automatic packages.

## How You Can Create Your Own Packages

If you wish, you can create your own packages as well. Packages you create are called multi-object packages. How you package the Network Map will depend on how your network is connected, and on how you want to view the map. You are not changing the actual connectivity of any devices only how you view them on the map.

- ▶ Remember, you can create many different map configuration files, each with different packaging.

- ▶ You can add new devices to a package at any time by dragging the icons on the map, or between map windows. However, your layout may change when you drop new devices into a package:

- If the package has been laid out by the user: when adding new devices, DDM Inventory places them without moving any of the other icons.
- If the package is in “auto-layout” mode: when adding new devices, DDM Inventory places them and moves the other icons around as well.

Here are three quick procedures that will show you how to create your own packages.

To create a new package with objects in it:

- 1 Click an object icon, or select a group of objects.
- 2 Click **Configure > Create Package**.

To create a new package with objects in it:

- ▶ This method is handy for tidying up devices connected to a Logical View icon.

- 1 Right click an object that has dependent objects.
- 2 Select **Create Package**.

The object will absorb any dependent object that:

- is not packaged
- is not locked
- does not have another connection

To change the icon and title of your package:

- 1 With the package icon selected, click **Package > Package Properties**.
- 2 Select a custom package icon from the pull-down list.
- 3 Enter a custom title for the package.
- 4 Click **Apply** or **OK**.

## How You Can Unpack Your Packages

To move the contents of the active package up one level:

- From the package window, click **Configure > Promote All**.

This command causes the following:

- Only the current package window is destroyed. Packages within the current package are not destroyed.
- Unlocks all objects.
- Automatic packages that were within the window are repackaged.

➤ In the Main Map window, this command is replaced by **Unpack All**.

To unpack the entire Network Map, and destroy all packaging:

- From the Main Map window, click **Configure > Unpack All**.

This command causes the following:

- All packages are destroyed.
- Unlocks all objects.
- Automatic packages are repackaged.

➤ In a package window, this command is replaced by **Promote All**.

To empty one package:

- From any map window, with a package selected, click **Configure > Unpackage**.

This command causes the following:

- Causes the selected package to be unpackaged, which also deletes the package
- Locks all objects within the package (unless they are unpackaged into the main map).

➤ Available to single packages only.

## How to Create Locked Objects

If you have manually packaged your map, you will see many icons with a blue line beneath them, if you have selected the “Underline locked objects option in **Edit > User Preferences**. The blue line indicates that the device has been manually packaged, meaning it has been put inside a package (**Package** command), promoted from a package (**Promote**), or has had its package removed (**Unpackage**).



When you manually package or unpackage an icon, you lock it into position. For example, if you take a workstation icon from a package and place the icon on the Network Map, that workstation icon will be locked there.

DDM Inventory creates some automatic packages. Whenever you use the **Pack** or the **Unpack All** commands, DDM Inventory will recreate all automatic packages. To keep a device from being automatically packaged, you can lock the device by using the **Lock** command.

To use the **Lock** command:

- Click **Configure > Lock**.

➤ To see which objects have been locked, turn on **View locked objects**. An icon you have moved yourself—into a place DDM Inventory would not naturally have chosen—will have a blue line beneath it to indicate that it is locked.

## How to Change the Automatic Packaging Preferences

Automatic packaging is based on connectivity. There are a few basic scenarios:

- device with one connection to a single connectivity device (such as a router or switch)
- device with multiple connections to a single connectivity device
- devices connected to a cloud or phone, which has a single connection to a connectivity device (in this case, the cloud or phone is also packaged with the devices)

DDM Inventory automatically creates packages, based on the major connectivity devices in your network.

These packages appear on your map with the label “X devices for Y” where X is the number of devices (this number is constantly updated as devices are added to or removed from the package) and Y is the name of the connectivity device.

Connectivity devices will have other devices associated with them (for example, workstations). DDM Inventory automatically packages the devices associated with that connectivity device.

➤ DDM Inventory usually treats a telephone as an end-node, but it may see it as a connectivity device.

By default, whenever DDM Inventory detects two or more end nodes of any classes, it creates a package to contain those objects. If it detects 3 or more objects of the same class (for example, workstations) it will create class-specific packages. The default is 3, but you can change this threshold if you wish.

Also by default, whenever DDM Inventory detects 10 or more network devices, it will automatically package those devices.

The defaults work well with most networks. You can change them to package the network in a particular way.

➤ If you have an Administrator account, you can change whether or not each class of device is packaged.

There are seven automatic package types available:

- Workstations
- Servers

- Printers
- POS/ATM
- Controllers
- Unknown
- Network Devices
- End Nodes



The End Nodes package is a generic package type. If there are devices that do not fit the thresholds of another package type, those devices may fit into a generic End Node package. There are also three device icons native to this package type.

Automatic packaging settings do not affect your ability to create custom packages.

To create automatic packages of a particular type:

- 1 Click **Administration > System Configuration > Automatic packaging.**

| Contents                                       | Description     | Package | On/Off | Threshold |
|--|-----------------|---------|--------|-----------|
| Primary Selection:<br>                         | Workstations    |         | On     | 3         |
| Primary Selection:<br>                         | Servers         |         | On     | 3         |
| Primary Selection:<br>                         | Printers        |         | On     | 3         |
| Primary Selection:<br>                         | POS/ATM         |         | On     | 3         |
| Primary Selection:<br>                         | Controllers     |         | On     | 3         |
| Primary Selection:<br>                         | Unknown         |         | On     | 3         |
| Primary Selection:<br>                         | Network Devices |         | On     | 10        |
| Primary Selection:<br>Secondary Selection:<br> | End Nodes       |         | On     | 2         |

Submit    Restore Defaults

- 2 For the package types you want to create, turn the package type On.
- 3 Select a threshold for each type of package.
- 4 To prevent a class of devices from being packaged, turn it Off.
- 5 Click **Submit**.
- 6 To restore the default settings, click **Restore Default**.

[Examples](#) on page 41 provides specific packaging guidelines depending on your use case.



## Examples

If you don't usually monitor end nodes, you should package all types of end node into a single type of package:

- 1 Set these controls **Off**:
  - Workstations
  - Servers
  - Printers
  - POS/ATM
  - Controllers
  - Unknown
- 2 Set this control **On**:
  - End Nodes
- 3 Set the End Nodes threshold to **2**.

If your network contains many servers for which you are responsible, you should package servers separately, but allow all other end nodes to be placed in a single type of package:

- 1 Set these controls **Off**:
  - Workstations
  - Printers
  - POS/ATM
  - Controllers
  - Unknown
- 2 Set these controls **On**:
  - Servers
  - End Nodes
- 3 Set the Servers threshold to **1**.
- 4 Set the End Nodes threshold to **2**.

If you are responsible for the three most common types of end nodes (workstations, servers, and printers), you should package each type separately for easy locating and identifying.

- 1 Set these controls **Off**:
  - POS/ATM
  - Controllers
  - Unknown
- 2 Set these controls **On**, and set each threshold to **1**:
  - Workstations
  - Servers
  - Printers
  - End Nodes

# Organizing Map Configuration Files

DDM Inventory lets you save different map configuration files. Each of these map configurations contains your layout and packaging. You can save as many configurations as you want, so you can quickly change your view of the Network Map.



These configuration files are saved (by default) at this location:

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

If you backup your system data, these configuration files will be included. For more information on creating a backup, see the *Installation and Initial Setup Guide*.

For example, you may want to concentrate on one particular building or campus. So you create a map configuration that shows that campus, and all your important devices there. In another map configuration, you may want to see an overview of the entire network.

Topics in this chapter include:

- [What is a Map Configuration?](#) on page 42
- [Prime Configuration](#) on page 43
- [Saving Your Changes](#) on page 43
- [Starting a Map Configuration](#) on page 43
- [Saving a Map Configuration File](#) on page 43
- [Saving the Prime Map Configuration](#) on page 44
- [Opening a Saved Map Configuration File](#) on page 45
- [Managing Map Configuration Files](#) on page 45

## What is a Map Configuration?

DDM Inventory automatically opens a map configuration file at the start of each map session. The first time a new account starts a map session, this is always a copy of the Prime configuration. All other times, the map configuration file that DDM Inventory opens depends on the type of account you are using.

**Table 7 Default Map Configurations**

| Account type  | Subsequent default file   |
|---------------|---------------------------|
| Demo          | Copy of Prime             |
| IT Employee   | last opened or designated |
| IT Manager    | last opened or designated |
| Administrator | last opened or designated |

When you end a map session, DDM Inventory takes note of what map configuration file is in use. The next time you start a map session, DDM Inventory opens that file. There are two exceptions:

- You can designate a different configuration file to be opened next time.

- Demo accounts always start a map session with a configuration called “Copy of Prime”. This is so that each user of a Demo account can start fresh, unaffected by previous users. Demo accounts can open a saved configuration if they want to pick up where they left off.

## Prime Configuration

The Prime configuration is a special configuration not associated with a particular account. As the owner of an Administrator account or an IT Manager account, you control the Prime map configuration. The Prime configuration can serve as a basis or starting point; people can copy it and make their own configurations.

- ▶ If you have just installed and set up DDM Inventory, you will notice that the Prime configuration does not exist. First, an Administrator account or IT Manager account must save a Prime configuration with the **Save As Prime** command (in a Network Map window, click **File > Save As Prime**).

Any user can open a copy of the Prime configuration in the Network Map by clicking **File > Open Copy of Prime**.

## Saving Your Changes

Each account may save one or more named map configuration files. Each file contains information on the account’s Network Map, and priorities, layout, packaging, package icons and titles.

An account owner can use the different map configuration files for different purposes. For example, one configuration file could show the network geographically, and another configuration file could show the network by subnets.

An account may open a different configuration at any time. Once saved, this configuration becomes the “current” configuration and will be used for the next map session.

- ▶ Your current configuration is normally the one active when you exit the Network Map, but you can alter this with the **Manage Map Configurations** option.

Each account has the configuration files saved in a separate space. Therefore, each account may have a configuration named “test” without interfering with other accounts.

## Starting a Map Configuration

- ▶ A new configuration will be labeled “Untitled” until you save it, at which time you are able to name the file.

To start a new map configuration:

- Click **File > New**.

## Saving a Map Configuration File

Creating a specific configuration name enables you to see your configuration the next time you log in to the Network Map.

A configuration name must be 1–30 bytes long (the number of characters depends on language encoding). You can use the following characters:

- A through Z (upper case)
- a through z (lower case)
- 0 through 9 (numbers)
- underscore (\_)
- hyphen (-)

To save a map configuration:

- 1 Click **File > Save As**.
- 2 Enter the new configuration name.
- 3 Click **OK**.

Also see [Autosave](#).

## Autosave

DDM Inventory provides an autosave capability for recovery purposes by saving the “current” configuration to a recovery file. DDM Inventory will make an autosave file (within a time period ranging from 10 seconds to two minutes, depending on the changes made by the account). If a session ends abnormally, the recovery file will be used the next time you open a map.

When you next open a map, you will see the message “Restored configuration from autosave” to remind you that a recovery has occurred. In the event that DDM Inventory uses the recovery file, the user still has the opportunity to discard the unsaved changes and re-open the configuration that represents the state of the last explicit save.



Autosave will not overwrite your named configuration. When you respond “no” to the question “Do you want to save the changes?”, you are discarding the active changes and the autosave file. The autosave file is also discarded when you save a configuration.

## Saving the Prime Map Configuration

The Prime map configuration is the default configuration for all accounts. Any account can open the Prime map configuration, but only Administrator and IT Manager accounts can change it. IT Employee and Demo accounts must save their changes under a different file name.

To save the Prime map configuration:

- 1 Click **File > Save As Prime**.

A confirmation box appears, asking if you really want to save this configuration as the Prime configuration.

- 2 Click **Save As Prime**.

## Opening a Saved Map Configuration File

You can only open your own configuration files with this procedure. If you wish to use the configuration file of another account, you must first copy that file into your account.

- ▶ When you open a configuration file, all open package windows close. The Device Manager windows, Port Manager windows, Line Manager windows, Network Map, and Health Panel stay open.

To open a saved map configuration:

- 1 Click **File > Open**.
- 2 Select the file name of the configuration you wish to use.
- 3 Click **OK**.

## Managing Map Configuration Files

This section applies to all accounts, except for the demo account. The demo account cannot perform any administration functions. The other three types of accounts can perform the following tasks:

- copy map configuration files
- delete map configuration files
- rename map configuration files
- choose which map configuration file will be the one that opens first (Make current)

- ▶ Close your map before performing any of these procedures.

To reach the Administration menu, click the **Administration** button.

To copy a map configuration file:

- 1 Click **Administration > My map configurations > Manage map configurations**.
- 2 Select a configuration file from the first pull-down list.
- 3 Select **Copy**.
- 4 Click **Next**.
- 5 Enter a name for the new configuration file.
- 6 Click **Finish**.

To delete a map configuration file:

- 1 Click **Administration > My map configurations > Manage map configurations**.
- 2 Select a configuration file from the first pull-down list.
- 3 Select **Delete**.
- 4 Click **Next**.
- 5 Click **No** to delete the file.

To rename a configuration file:

- 1 Click **Administration > My map configurations > Manage map configurations**.
- 2 Select a configuration file from the first pull-down list.
- 3 Select **Rename**.
- 4 Click **Next**.
- 5 Enter a name for the new configuration file.
- 6 Click **Finish**.

To choose which map configuration that will open first:

The command, **Make Current**, makes a map file the first one you see when you open the Network Map.

- 1 Click **Administration > My map configurations > Manage map configurations**.
- 2 Select a configuration file from the first pull-down list.
- 3 Select **Make Current**.
- 4 Click **Next**.
- 5 Click **Yes** to make this your default map configuration.

Also see [Sharing Map Configuration Files with other Accounts](#).

## Sharing Map Configuration Files with other Accounts


You can make it possible for other accounts to make copies of your files, but you cannot actually send a file. The procedure is simple and quick. First, you make sure that your account has its permissions set correctly. Next, the user with whom you want to share the file requests it.

To permit others to share your map configuration files:

- 1 Click **Administration > My account administration > Modify properties**.
- 2 Click **Account Properties**.
- 3 Select “Yes” from the “Allow others to copy map configurations?” radio button. (If “Yes” has already been selected, your task is complete.)
- 4 Click **Modify Properties**.

You have just permitted *all* users to copy *all* your map configuration files.

What the other user must do:

 The other user must not have a map session open.

- 1 Click **Administration > My map configurations > Copy map configurations**.
- 2 Select an account name (of the person whose file they want to copy) and click **Next**.
- 3 Select a configuration file and click **Next**.
- 4 Enter a name for the configuration file.
- 5 Click **Finish**.

The other user now has a copy of one of your map configuration files.

## Saving a Map Window as a Graphic File

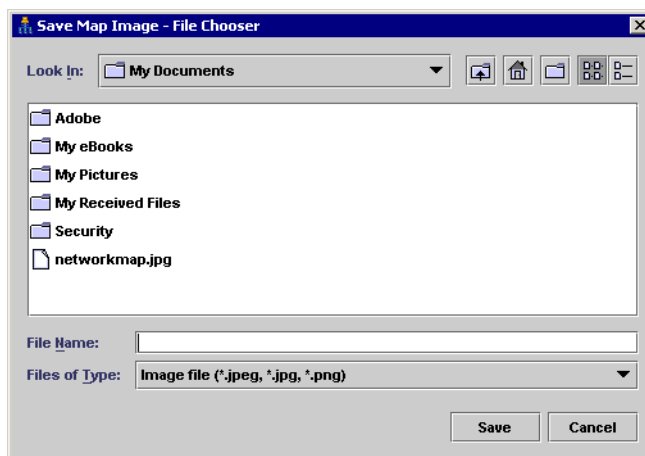
You can save any map window (the main map, or any package) as an image file (either jpg or png).

To save your map as an image file:

- 1 Click **File > Save Map Image**.

The File Chooser dialog appears.

- 2 Enter the name and location of the image file you want to save.
- 3 Select a file type.
- 4 Click **Save**.







## 4 Using the Service Analyzer

The DDM Inventory Service Analyzer allows you to analyze the network path between two devices. To get started with the Service Analyzer, you must identify the devices at the ends of the path you want to analyze.

Topics in this section include:

- [Choosing Your Path](#) on page 49
- [Service Analyzer Window](#) on page 50

### Choosing Your Path

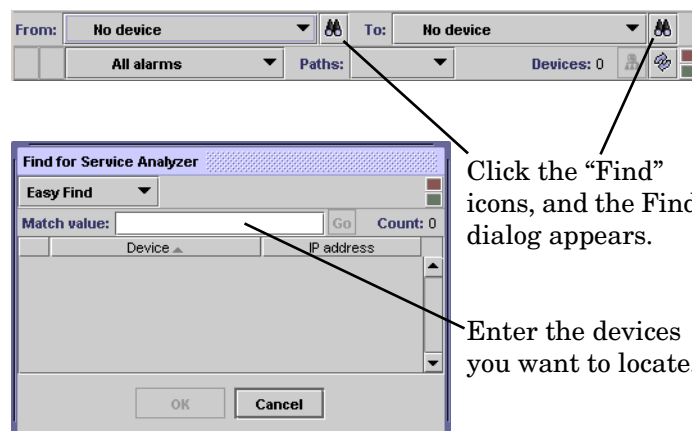
The toolbar contains two search boxes: **From** and **To**. Each box searches for a device based on its name, title, or address. This Find window works exactly the same way as the global Find feature. For more information, see [Finding Network Devices](#) on page 11.

To use the Service Analyzer:

- 1 From the DDM Inventory navigation tree, click **Service Analyzer**.



You can also open the Service Analyzer from the Device Manager. That device will be the first device in the Service Analyzer query.



- 2 Click the first **Find** icon.
- 3 In the **Match value** box, enter the IP address or the first few characters of the device identifier for the first device that you want to find, and press **Enter**.
- 4 Select a device from the Find dialog and click **OK**.

5 Repeat [step 2](#) to [step 4](#) for the second **Find** icon.



It is important to fill in the device on the left first. Changing the device on the left side will automatically clear the device on the right side.

## Service Analyzer Window

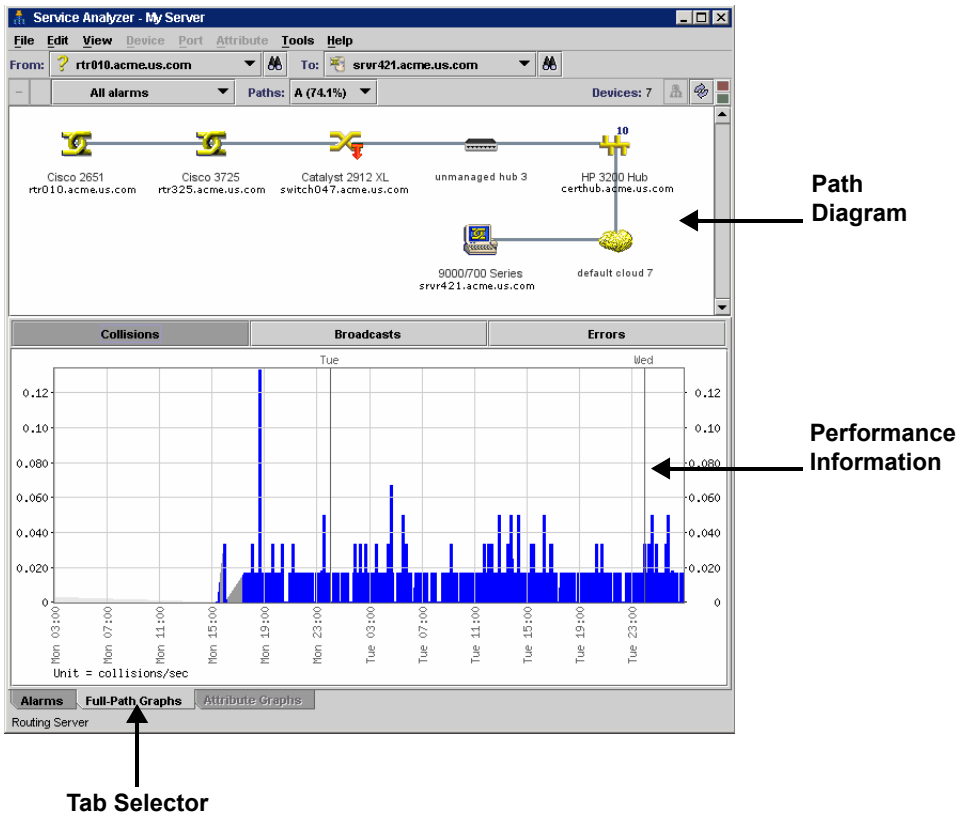
Topics in this section include:

- [User Interface](#) on page 50
- [Path Diagram](#) on page 51
- [Full-Path Graphs Tab](#) on page 51

### User Interface

After you provide valid endpoints for the path to be analyzed, the Service Analyzer displays a diagram of the path in the upper pane and a graphical representation of performance information for that path in the lower pane.

In the following example, the lower pane shows the rate of collisions observed over a 48-hour period. To see the number of broadcasts or errors that took place during this same 48 hours, you would click the Broadcasts button or the Errors button.



## Path Diagram

You will notice that the path diagram has a similar look to the Network Map. The path diagram presents only devices and lines. Packages are not shown. In the Paths drop-down list, multiple views are available to display the data for different paths between the two devices.



If there is only a single path, it will be the only choice. The percentage indicates how frequently a path was taken. If the sum of the percentages is less than 100, this indicates that a path was not available at some point during the preceding 48 hours.

## Full-Path Graphs Tab

The Full-Path Graphs tab shows a summary of the entire path for the following alarm categories:

**Table 1**    **Graphs**

| <b>Alarm Category</b> | <b>Notes</b>   |
|-----------------------|--|
| Collisions            | Collisions per seconds; for ports                    |
| Broadcasts            | Broadcasts in frames/sec.; for ports, bi-directional |
| Errors                | Errors in frames/sec.; for ports                     |

You can click any of the buttons to view the related alarm category. All graphs display traffic levels for the last 48 hours across the entire path.



# 5 Using the Health Panel

There are many ways to look at your device data with DDM Inventory. The Health Panel allows you to see your devices, and to determine the devices that currently have problems.

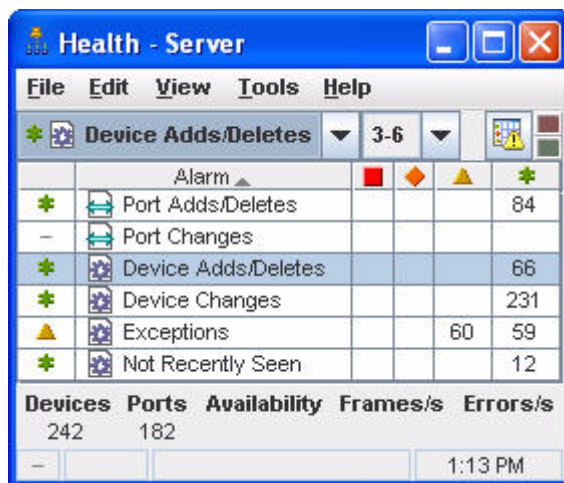
Typically, a user would start with the Health Panel, which lists all the alarms currently on your network. To see a list of devices with these alarms, double-click on an alarm category in the Health Panel, and the Alarm Viewer opens. The Alarms Viewer is described in [Using the Alarms Viewer](#).

Topics in this chapter include:

- [Viewing Network Overview with Health Panel](#) on page 53
- [Using the Aggregate Health Panel](#) on page 55

## Viewing Network Overview with Health Panel





The Health Panel enables you to set up, highlight, and examine conditions, alarms, and statistics that DDM Inventory has gathered about your devices. To change which Alarms are displayed, see [Customizing the Alarms List](#) on page 54.



The Health Panel is automatically updated with current device information.

There are icons on the Health Panel to distinguish device and port alarms. The Health Panel is divided into sections as indicated by these icons:

**Table 1 Alarm Indicators**

| Category               | Indicator  |
|------------------------|--|
| Port Attribute Alarm   |  |
| Device Attribute Alarm |  |
| Port Report Alarm      |  |
| Device Report Alarm    |  |

The Health Panel will show you how many devices have alarms. You can drill down with the Alarms Viewer to see exactly which devices have the alarms. For more information, see [Using the Alarms Viewer](#).

**Table 2 Health Panel footer**

| Statistic    | Explanation  |
|--------------|--|
| Devices      | The number of discovered devices in the network.   |
| Ports        | The number of discovered ports in your network   |
| Availability | This number represents the number of real devices with priority 3 (or higher) that are operational as a percentage of the total number of real devices with priority 3 (or higher).              |
| Frames       | This number represents the instantaneous number of frames per second seen on the entire network.   |
| Errors       | This number represents the instantaneous number of errors per second seen on the entire network. This includes the number of errors on both the “in” and the “out” ports of the network devices. |

## Customizing the Alarms List

The following sections describe how to customize the appearance of the Health Panel.

- [My User Alarms](#) on page 54
- [Hide Inactive Alarms](#) on page 55

### My User Alarms

You can change the appearance of the Health Panel so you see only the alarms in which you are interested.

To customize the alarms shown on the Health Panel:

- 1 From the Health Panel, click **Edit > User Preferences > Health Panel tab**.  
Here, you can create a list of the alarms you want to see on the Health Panel.
- 2 After you have created your list, click **Apply**.
- 3 Click **OK**.  
Next, you must select these changes in the View menu.
- 4 Click **View > My User Alarms Only**.

## Hide Inactive Alarms

You can hide the categories that currently have no alarms associated with them.

To hide the inactive alarm categories:

- Click **View > Hide Inactive Alarms**.

## Using the Aggregate Health Panel

The Aggregate Health Panel looks similar to the regular Health Panel; it has all the same buttons and statistics. However, the Aggregate Health Panel combines all the statistics from all the aggregated DDM Inventory servers in your network.

You can click on the report buttons to see complete lists of all alarms in the entire network. If you were looking at a regular Health Panel for one server, you would only see alarms for a portion of your network.



You can tell what Health Panel you are looking at by the report banner. If it is the Aggregate Health Panel, the banner says “Aggregate Health” rather than “Health Panel”. A “globe” symbol also shows that you are looking at an Aggregator.

The statistics listed in the Aggregate Health Panel are the same as those listed in the regular Health Panel.

To open the Aggregate server Health page, click the [Servers button](#).

## Servers button

Clicking the **servers** button at the bottom of the Health Panel takes you to the **Aggregate server Health** page. This page shows you a summary of the health status of all your remote DDM Inventory servers.

By clicking on any of the server hyperlinks on this page, you can see the **server Health** page for that DDM Inventory server.



The local DDM Inventory server is always at the top of the list with an asterisk (\*).





---

## 6 Using the Alarms Viewer

There are many ways to look at your device data with DDM Inventory. The section, [Using the Health Panel](#), tells you how this is done with the Health Panel. This section explains how to use the Alarms Viewer with the Health Panel.

Typically, a user would start with the Health Panel, which lists all the alarms currently on your network. To see a list of devices with these alarms, double-click on an alarm category in the Health Panel, and the Alarm Viewer opens.

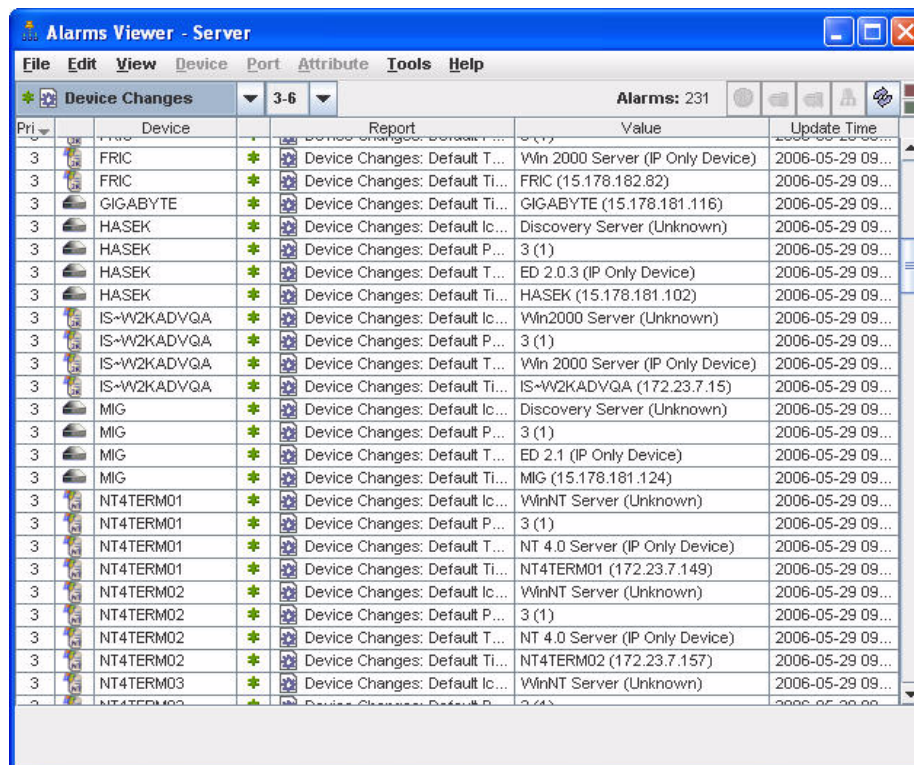
The Alarms Viewer shows all the devices on the network with current alarms. From the Alarms Viewer, you can open up the Device Manager, Port Manager, or Attribute Manager.

Topics in this chapter include:

- [Using the Alarms Viewer](#) on page 58
- [Using the Aggregate Alarms Viewer](#) on page 59
- [Saving Data to a Text File](#) on page 59

## Using the Alarms Viewer

The Alarms Viewer is an extension of the Health Panel and shows you exactly on which devices and ports the alarms have occurred. By double-clicking on a line in the Health Panel, you will open the Alarms Viewer. The Alarms Viewer works with the Health Panel to show you which devices on your network have Critical, Major, Minor, or Info alarms.



The screenshot shows the 'Alarms Viewer - Server' window. The title bar includes standard window controls and the text 'Alarms: 231'. The menu bar contains 'File', 'Edit', 'View', 'Device', 'Port', 'Attribute', 'Tools', and 'Help'. Below the menu bar, there are two pull-down menus: 'Device Changes' (set to '3-6') and 'Alarms: 231'. The main area is a table with the following columns: 'Pri', 'Device', 'Report', 'Value', and 'Update Time'. The table contains 23 rows of data, each representing an alarm event. The 'Device' column lists various network devices like FRIC, GIGABYTE, HASEK, IS-W2KADVQA, MIG, and NT4TERM01-03. The 'Report' column shows the type of alarm, such as 'Device Changes: Default T...'. The 'Value' column provides details like 'Win 2000 Server (IP Only Device)' or 'FRIC (15.178.182.82)'. The 'Update Time' column shows the date and time of the alarm, all from 2006-05-29.

| Pri | Device      | Report                        | Value                            | Update Time      |
|-----|-------------|-------------------------------|----------------------------------|------------------|
| 3   | FRIC        | Device Changes: Default T...  | Win 2000 Server (IP Only Device) | 2006-05-29 09... |
| 3   | FRIC        | Device Changes: Default Ti... | FRIC (15.178.182.82)             | 2006-05-29 09... |
| 3   | GIGABYTE    | Device Changes: Default Ti... | GIGABYTE (15.178.181.116)        | 2006-05-29 09... |
| 3   | HASEK       | Device Changes: Default Ic... | Discovery Server (Unknown)       | 2006-05-29 09... |
| 3   | HASEK       | Device Changes: Default P...  | 3 (1)                            | 2006-05-29 09... |
| 3   | HASEK       | Device Changes: Default T...  | ED 2.0.3 (IP Only Device)        | 2006-05-29 09... |
| 3   | HASEK       | Device Changes: Default Ti... | HASEK (15.178.181.102)           | 2006-05-29 09... |
| 3   | IS-W2KADVQA | Device Changes: Default Ic... | Win2000 Server (Unknown)         | 2006-05-29 09... |
| 3   | IS-W2KADVQA | Device Changes: Default P...  | 3 (1)                            | 2006-05-29 09... |
| 3   | IS-W2KADVQA | Device Changes: Default T...  | Win 2000 Server (IP Only Device) | 2006-05-29 09... |
| 3   | IS-W2KADVQA | Device Changes: Default Ti... | IS-W2KADVQA (172.23.7.15)        | 2006-05-29 09... |
| 3   | MIG         | Device Changes: Default Ic... | Discovery Server (Unknown)       | 2006-05-29 09... |
| 3   | MIG         | Device Changes: Default P...  | 3 (1)                            | 2006-05-29 09... |
| 3   | MIG         | Device Changes: Default T...  | ED 2.1 (IP Only Device)          | 2006-05-29 09... |
| 3   | MIG         | Device Changes: Default Ti... | MIG (15.178.181.124)             | 2006-05-29 09... |
| 3   | NT4TERM01   | Device Changes: Default Ic... | WinNT Server (Unknown)           | 2006-05-29 09... |
| 3   | NT4TERM01   | Device Changes: Default P...  | 3 (1)                            | 2006-05-29 09... |
| 3   | NT4TERM01   | Device Changes: Default T...  | NT 4.0 Server (IP Only Device)   | 2006-05-29 09... |
| 3   | NT4TERM01   | Device Changes: Default Ti... | NT4TERM01 (172.23.7.149)         | 2006-05-29 09... |
| 3   | NT4TERM02   | Device Changes: Default Ic... | WinNT Server (Unknown)           | 2006-05-29 09... |
| 3   | NT4TERM02   | Device Changes: Default P...  | 3 (1)                            | 2006-05-29 09... |
| 3   | NT4TERM02   | Device Changes: Default T...  | NT 4.0 Server (IP Only Device)   | 2006-05-29 09... |
| 3   | NT4TERM02   | Device Changes: Default Ti... | NT4TERM02 (172.23.7.157)         | 2006-05-29 09... |
| 3   | NT4TERM03   | Device Changes: Default Ic... | WinNT Server (Unknown)           | 2006-05-29 09... |
| 3   | NT4TERM03   | Device Changes: Default P...  | 3 (1)                            | 2006-05-29 09... |

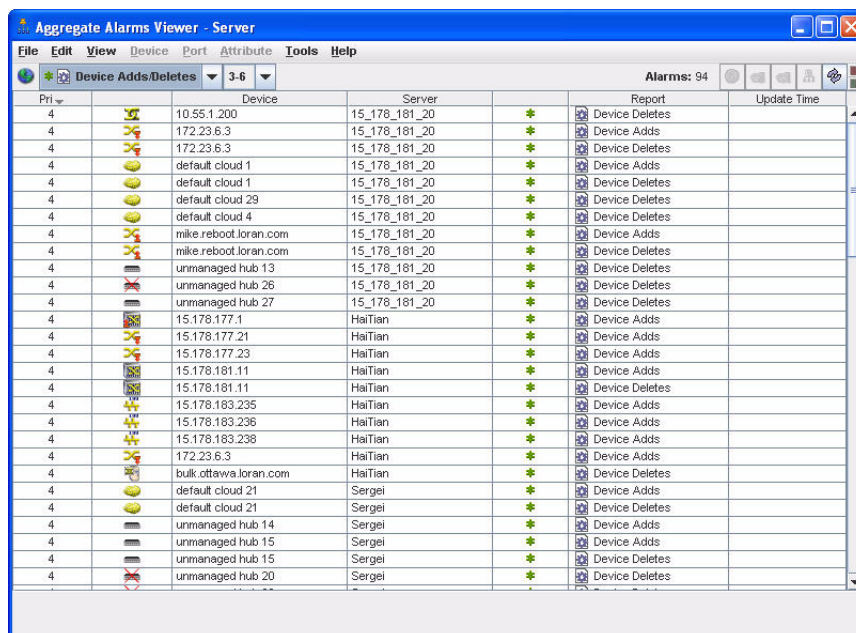
The status bar in the Alarms Viewer is similar to that on the Health Panel. You can change the displayed alarm type or priority with the pull-down lists on either window. Your selection will appear in the Health Panel and the Alarms Viewer.



The Alarms Viewer will show a maximum of 1000 alarms.

## Using the Aggregate Alarms Viewer

The Aggregate Alarms Viewer is almost identical to the regular Alarms Viewer. The major difference is that the **Server** column shows which server is the source of the alarm data.



| Pri | Device                | Server        | Report         | Update Time |
|-----|-----------------------|---------------|----------------|-------------|
| 4   | 10.55.1.200           | 15_178_181_20 | Device Deletes |             |
| 4   | 172.23.6.3            | 15_178_181_20 | Device Adds    |             |
| 4   | 172.23.6.3            | 15_178_181_20 | Device Deletes |             |
| 4   | default cloud 1       | 15_178_181_20 | Device Adds    |             |
| 4   | default cloud 1       | 15_178_181_20 | Device Deletes |             |
| 4   | default cloud 29      | 15_178_181_20 | Device Deletes |             |
| 4   | default cloud 4       | 15_178_181_20 | Device Deletes |             |
| 4   | mike.reboot.loran.com | 15_178_181_20 | Device Adds    |             |
| 4   | mike.reboot.loran.com | 15_178_181_20 | Device Deletes |             |
| 4   | unmanaged hub 13      | 15_178_181_20 | Device Deletes |             |
| 4   | unmanaged hub 26      | 15_178_181_20 | Device Deletes |             |
| 4   | unmanaged hub 27      | 15_178_181_20 | Device Deletes |             |
| 4   | 15.178.177.1          | HaiTian       | Device Adds    |             |
| 4   | 15.178.177.21         | HaiTian       | Device Adds    |             |
| 4   | 15.178.177.23         | HaiTian       | Device Adds    |             |
| 4   | 15.178.181.11         | HaiTian       | Device Adds    |             |
| 4   | 15.178.181.11         | HaiTian       | Device Deletes |             |
| 4   | 15.178.183.235        | HaiTian       | Device Adds    |             |
| 4   | 15.178.183.236        | HaiTian       | Device Adds    |             |
| 4   | 15.178.183.238        | HaiTian       | Device Adds    |             |
| 4   | 172.23.6.3            | HaiTian       | Device Adds    |             |
| 4   | bulk.ottawa.loran.com | HaiTian       | Device Deletes |             |
| 4   | default cloud 21      | Sergei        | Device Adds    |             |
| 4   | default cloud 21      | Sergei        | Device Deletes |             |
| 4   | unmanaged hub 14      | Sergei        | Device Adds    |             |
| 4   | unmanaged hub 15      | Sergei        | Device Adds    |             |
| 4   | unmanaged hub 15      | Sergei        | Device Deletes |             |
| 4   | unmanaged hub 20      | Sergei        | Device Deletes |             |

## Saving Data to a Text File

You can now use the **Save Table Data** feature to save selected info into a tab separated value (.tsv) file in the following DDM Inventory features:

- Health Panel
- MIB Browser
- Find
- Alarms Viewer
- Service Analyzer
- Events Browser

You can save the entire contents of a window, or you can **Ctrl-click** to select the data you want to save.

To save data to a text file:

- 1 Select the table items you want to save. To select the entire table, click **Edit > Select Table**.
- 2 Click **File > Save Table Data**.

A Save Table Data dialog appears.

To save data to the clipboard:

- 1 Select the table items you want to save. To select the entire table, click **Edit > Select Table**.
- 2 Click **Edit > Copy**.  
Your selected items have been copied to the clipboard. For example, you can paste it into a file or an e-mail.
- 3 Select a file name and location for the text files.
- 4 Click **Save**.

# 7 Using the Events Browser

DDM Inventory logs network and access events. The Events Browser can display up to 1,000 events at a time.

An event occurs when:

- A device or port is physically added, deleted, or moved.
- A device or port property is changed by a user (through the Device or Port Properties dialog) or by the system itself.

An access event occurs when:

- Users access (or attempt to access) or logout of the DDM Inventory server.
- An admin or IT manager user writes to a device MIB, updates a device model, changes a device's visibility, or changes device properties.



Only admin accounts can view access events.

For example, DDM Inventory can log an event if it discovers a device has been added to the network. It may also log an event when a line breaks or if there are too many delays on a line. The Events Browser shows you a list of events that occurred on lines and devices in your network during a specified period.

The Health Panel and Network Map give you information about the current state of your network. The Events Browser gives you historical information. The Health Panel and Network Map can tell you what's wrong now. The Events Browser shows you problems that only patterns over time can reveal.



The Events Browser shows events for the past 45 days or up to a maximum of 500,000 events (whichever is less).

Topics in this section include:

- [Events Browser](#) on page 61
- [Using the Aggregate Events Browser](#) on page 67

## Events Browser

Topics in this section include:

- [Opening the Events Browser](#) on page 62
- [Network Events](#) on page 62
- [Access Events](#) on page 63
- [Toolbar](#) on page 67

## Opening the Events Browser

To open the Events Browser:

- On the navigation tree, click the Events Browser link.

OR

- From the Health Panel or Alarms Viewer, click **Tools > Events Browser**.

OR

- From a Device Manager or Port Manager, click the **Events** button.

## Network Events

All users can see the network events on the Events Browser. The next figure shows an example of what you will see if you selected All Events from the events pull-down list. If you select one type of event from the list, the display will change, and you will see only that event and columns relating to that event-type.

| Event Time       | Pri | Device            | Port | Attribute                        | Value                            |
|------------------|-----|-------------------|------|----------------------------------|----------------------------------|
| 2006-05-29 12:00 | 3   | example_45_server |      | Device Changes: User Title       | example_45_server (<default>)    |
| 2006-05-29 12:00 | 3   | server2_example   |      | Device Changes: User Title       | server2_example (<default>)      |
| 2006-05-29 11:59 | 3   | server_ED         |      | Device Changes: User Title       | server_ED (<default>)            |
| 2006-05-29 11:37 | 3   | example_45_server |      | Device Changes: Default Title    | motleycrue (MOTLEYCRUE)          |
| 2006-05-29 11:37 | 3   | example_45_server |      | Device Changes: Default Tag      | Win 2003 Server (VMware)         |
| 2006-05-29 11:37 | 3   | example_45_server |      | Device Changes: Default Priority | 3 (1)                            |
| 2006-05-29 11:37 | 3   | example_45_server |      | Device Changes: Default Icon     | Win2003 Server (Workstation)     |
| 2006-05-29 11:37 | 3   | example_45_server | 0.0  | Port Adds: Port 0.0              |                                  |
| 2006-05-29 11:34 | 3   | server2_example   |      | Device Changes: Default Title    | skidrow (15.178.180.235)         |
| 2006-05-29 11:34 | 3   | server2_example   |      | Device Changes: Default Tag      | Win 2003 Server (VMware)         |
| 2006-05-29 11:34 | 3   | server2_example   |      | Device Changes: Default Priority | 3 (1)                            |
| 2006-05-29 11:34 | 3   | server2_example   |      | Device Changes: Default Icon     | Win2003 Server (Workstation)     |
| 2006-05-29 11:34 | 3   | server2_example   | 0.0  | Port Adds: Port 0.0              |                                  |
| 2006-05-29 11:31 | 3   | server_ED         |      | Device Changes: Default Title    | ironmaiden (15.178.180.233)      |
| 2006-05-29 11:31 | 3   | server_ED         |      | Device Changes: Default Tag      | Win 2003 Server (VMware)         |
| 2006-05-29 11:31 | 3   | server_ED         |      | Device Changes: Default Priority | 3 (1)                            |
| 2006-05-29 11:31 | 3   | server_ED         |      | Device Changes: Default Icon     | Win2003 Server (Workstation)     |
| 2006-05-29 11:31 | 3   | server_ED         | 0.0  | Port Adds: Port 0.0              |                                  |
| 2006-05-29 11:23 | 3   | W2K3ent-02        |      | Device Changes: Default Title    | W2K3ent-02 (W2K3ENT-02)          |
| 2006-05-29 11:23 | 3   | W2K3ent-02        |      | Device Changes: Default Tag      | Win 2003 Server (IP Only Device) |

Each row in the Events Browser window contains the following information:

**Table 1 Events Browser columns**

| Data            | Explanation                       |
|-----------------|-----------------------------------|
| Event Time      | The time the event was generated. |
| Device Priority | —                                 |
| Device type     | Small device icon                 |
| Device          | Device title <sup>a</sup>         |

**Table 1 Events Browser columns**

| <b>Data</b>        | <b>Explanation</b>  |
|--------------------|---|
| Port               | Port number (will not appear if a device alarm is selected) |
| Alarm type         | Alarm type icon   |
| Attribute          | Name of the alarm   |
| Value <sup>b</sup> | Numerical value, if any, associated with this alarm.        |

- a. If no device title can be determined, the Events Browser title column is blank. This depends on the Device Title Preferences as set in **Administration > System Configuration > Display preferences**.
- b. There will not be a Value column for Line and Device Breaks.

“Broadcast In” and “Broadcast out” alarms are not logged, due to the potentially very high number of events. “Source of Broadcast” alarms are logged.

## Access Events

Only admin accounts can view access events on the Events Browser. You can select any of the these event types to view:

- Server Access
- SNMP Write by MIB OID
- SNMP Write by Attribute
- Port Adds/Deletes
- Port Changes
- Device Adds/Deletes
- Device Changes
- Update Model

You will notice that the Port and Device events are listed in the Network Events panel as well as the admin-only Access Events panel. The same events are listed in both panels, but under Access Events, you can see more details about where these changes originated: the source IP address and account name.

Similar to the network events list, the columns will change depending on the type of event you choose to display.

Server Access events show the following data:

**Table 2 Server Access Events**

| <b>Data</b> | <b>Explanation</b>           |
|-------------|------------------------------|
| Event time  | the time of the access event |

**Table 2 Server Access Events**

| <b>Data</b>   | <b>Explanation</b>  |
|---------------|---|
| Account name  | the user accessing DDM Inventory  |
| From IP       | the IP address from which the user accessed DDM Inventory   |
| Access status | whether or not the user was able to access DDM Inventory: <ul style="list-style-type: none"> <li>• Connect – the user has connected to DDM Inventory, and disconnected without attempting to login.</li> <li>• Login OK – the user has successfully logged in to DDM Inventory.</li> <li>• Login fail – the user has attempted to login, and did not have the correct password.</li> <li>• Logout – the user has logged out of DDM Inventory.<sup>a</sup></li> <li>• Login disabled – the user has tried to login with a failed password too many times (limit has been set in <b>Administration &gt; System Configuration &gt; Appliance passwords</b>)</li> <li>• Login no permission – this account has been denied permission to access DDM Inventory.</li> </ul> |

a. Logout for HTTP and HTTP proxy has a timeout of 5 minutes from your last HTTP request.

SNMP Write events show the following data:

**Table 3 SNMP Write Events**

| <b>Data</b>            | <b>Explanation</b>   |
|------------------------|--|
| Event time             | the time of the access event   |
| Account name           | the user accessing DDM Inventory   |
| From IP                | the IP address from which the user accessed the device   |
| To IP                  | the device that had its MIB changed  |
| MIB OID                | the MIB OID changed by the user (for “Write by MIB OID” only)  |
| Attribute              | either Administrative Status or Bridge Aging Interval, these being the only attributes a user can change through the MIB (for “Write by Attribute” only)   |
| Write Community String | the community string used to access the MIB  |
| Value                  | the new “changed” value of the OID   |
| Access Status          | whether or not the user was able to write to the MIB: <ul style="list-style-type: none"> <li>• Write OK</li> <li>• Fail (any of the following messages may appear): invalid response, too big, no such name, bad value, read only, gen err, no access, wrong type, wrong length, wrong encoding, wrong value, no creation, inconsistent value, resource unavailable, commit failed, undo failed, authorization error, not writable.</li> </ul> |



Device and Port Add/Delete events show the following data:

**Table 4 Add/Delete Events**

| <b>Data</b>  | <b>Explanation</b>                                     |
|--------------|--|
| Event Time   | the time of the access event                           |
| Account name | the user accessing DDM Inventory                       |
| From IP      | the IP address from which the user accessed the device |
| Priority     | the priority of the device                             |
| Icon         | the current icon representing this device              |
| Device       | the current device title                               |
| Port         | The port number (only appears for Port event)          |
| Attribute    | Add or Delete  |

Device and Port Change events show the following data:

**Table 5 Change Events**

| <b>Data</b>  | <b>Explanation</b>                                     |
|--------------|--|
| Event Time   | the time of the access event                           |
| Account name | the user accessing DDM Inventory                       |
| From IP      | the IP address from which the user accessed the device |
| Priority     | the priority of the device                             |
| Icon         | the current icon representing this device              |
| Device       | the current device title                               |
| Port         | The port number (only appears for Port event)          |
| Attribute    | The type of change (device title, etc.)                |
| Value        | The changed value                                      |

Update Model events show the following data:

**Table 6 Update Model Events**

| <b>Data</b>  | <b>Explanation</b>                                     |
|--------------|--|
| Event Time   | the time of the access event                           |
| Account Name | the user accessing DDM Inventory                       |
| From IP      | the IP address from which the user accessed the device |
| Priority     | the priority of the device                             |

**Table 6 Update Model Events**

| Data           | Explanation   |
|----------------|---|
| Icon           | the current icon representing this device                       |
| Device         | the current device title  |
| Access Command | The command issued by the user (Update Model, Enrich XML, etc.) |

To view access events on the Events Browser:

- Click **View > Show Access Events**.

The screenshot shows the 'Events Browser - Server' window. The menu bar includes File, Edit, View, Device, Port, Attribute, Tools, and Help. The 'Server Access' dropdown is selected. The 'now' filter is active, and the 'Limit' is set to 20. The 'Events: 20' indicator is visible. The main table displays the following data:

| Event Time       | Account Name | From IP      | Access Point | Access Status |
|------------------|--------------|--------------|--------------|---------------|
| 2006-05-29 12:30 | admin        | 16.117.57.30 | HTTP         | Login OK      |
| 2006-05-29 12:05 | admin        | 16.117.57.30 | HTTP         | Logout        |
| 2006-05-29 11:33 | admin        | 16.117.57.18 | HTTP         | Logout        |
| 2006-05-29 11:09 | admin        | 16.117.57.18 | HTTP         | Login OK      |
| 2006-05-29 11:06 | admin        | 16.117.57.18 | HTTP         | Logout        |
| 2006-05-29 11:01 | admin        | 16.117.57.28 | HTTP         | Logout        |
| 2006-05-29 10:57 | admin        | 16.117.57.30 | HTTP         | Login OK      |
| 2006-05-29 10:55 | admin        | 16.117.57.28 | HTTP         | Login OK      |
| 2006-05-29 10:55 | admin        | 16.117.57.18 | HTTP         | Login OK      |
| 2006-05-29 10:31 | admin        | 16.117.57.28 | HTTP         | Logout        |
| 2006-05-29 10:23 | admin        | 16.117.57.18 | HTTP         | Logout        |
| 2006-05-29 10:21 | admin        | 16.117.57.30 | HTTP         | Logout        |
| 2006-05-29 10:14 | admin        | 16.117.57.30 | HTTP         | Login OK      |
| 2006-05-29 10:07 | admin        | 16.117.57.18 | HTTP         | Login OK      |
| 2006-05-29 10:01 | admin        | 16.117.57.18 | HTTP         | Logout        |
| 2006-05-29 09:55 | admin        | 16.117.57.18 | HTTP         | Login OK      |
| 2006-05-29 09:53 | admin        | 16.117.57.18 | HTTP         | Logout        |
| 2006-05-29 09:53 | admin        | 16.117.57.28 | HTTP         | Login OK      |
| 2006-05-29 09:47 | admin        | 16.117.57.28 | HTTP         | Logout        |
| 2006-05-29 09:44 | admin        | 16.117.57.18 | HTTP         | Login OK      |

## Toolbar

The following diagram of the Events Browser toolbar shows all the methods of changing the event list. You can use the different buttons and text boxes to view the events in which you are most interested.



**Table 7 Toolbar Legend**

| Number | Feature                          |
|--------|----------------------------------|
| 1      | Event Category Pull-down list    |
| 2      | Priority                         |
| 3      | Recent device list               |
| 4      | Find a device                    |
| 5      | Older                            |
| 6      | Events Time Frame                |
| 7      | Newer                            |
| 8      | Maximum number of events to find |
| 9      | Show Additional Info             |
| 10     | Open Device Manager              |
| 11     | Open Port Manager                |
| 12     | Locate on Network Map            |
| 13     | Refresh                          |
| 14     | Connectivity Indicator           |

## Using the Aggregate Events Browser

The Aggregate Events Browser is almost identical to the regular Events Browser. The major difference is that the “Server” column shows which server is the source of the event data.

By default, the Aggregator updates events hourly. Due to the time lag, events may not be completely up to date.

If aggregation is turned on, but no Aggregators have been set up, the aggregate Events Browser will look very much like the regular Events Browser, except for the time delay.



## 8 Using the Device Manager








The Device Manager provides you with detailed information about a device, in several panels. Through its series of panels, you can see the current alarms on the device, as well as historical statistics. You can also interact with the device directly through the Device Manager, by pinging the device, opening a telnet session, or by forcing DDM Inventory to update the device model.










To open the Device Manager:





| <b>From</b>  | <b>Open by...</b>  |
|--|--|
| Health Panel, Alarms Viewer, Events Browser, Network Map, Service Analyzer, Scan Data Viewer | Click <b>Tools &gt; Find</b> (Ctrl - F). Enter a device address or title, then click <b>Find</b> .   |
| Alarms Viewer, Events Browser, Virtual Servers window  | Double-click on a table row, or right-click on the device icon, title, or IP address.  |
| Find   | Enter a device address, title, or any other criterion available in the Find tool then click <b>Find</b> .                                      |
| Reports, Status, Manager panels  | Click a hyperlinked device title   |
| Network Map, Service Analyzer  | Double-click a device icon. Right-click a device icon, and select Open Device. Click a device icon, and click <b>Object &gt; Open Device</b> . |

## List of Device Manager Panels

This is a complete list of panels available in the Device Manager. If you are reading this document online, click the hyperlinks in this table to read more information on these panels. Some panels are only available with certain license combinations.

| Icon  | Name             | Description  |
|---|------------------|--|
|    | Configuration    | This panel identifies a device and presents an overview of the device's identity and status.<br>For more information, see <a href="#">Configuration</a> on page 72.  |
|    | Reports          | This panel displays current values for report and summary historical data. Displays alarm signals even when the device priority is less than the minimum priority for a configuration (unlike in map windows).<br>For more information, see <a href="#">Reports</a> on page 79.  |
|    | Diagnosis        | This panel displays information about the current state of the device that can be helpful in diagnosing problems.<br>For more information, see <a href="#">Diagnosis</a> on page 80.   |
|    | Ports            | This panel lists ports for this device and summarizes the information available for them. By default, it displays 24 ports at a time. You can change this value directly in the panel or in <b>Administration &gt; Account administration &gt; Account properties</b> .<br>For more information, see <a href="#">Ports</a> on page 91.   |
|  | Events           | This button opens the Events Browser with this device in context.<br>For more information, see <a href="#">Using the Events Browser</a> on page 61.  |
|  | Locate           | This button highlights in a map window the location of the device.<br>If a map session was not open already, one will open now. Within the map window, the device you are locating has a yellow circle around it.<br>If the window containing the device was already open, that window becomes the front-most window, and the window scrolls so that the highlighted icon can be seen. |
|  | Service Analyzer | This button opens the Service Analyzer query with the current device already selected as Device 1, to allow the user to view the state of the path between this device and any other device on the Network Map. This functionality exists only if you have the Topology and Alarms licenses.   |

| Icon  | Name   | Description  |
|---|--|--|
|    | Manage   | This button launches an element manager of your choice.<br>The URL or application must be defined in <b>Administration &gt; System Configuration &gt; Element management</b> . If not, this button is dimmed.<br>Note: for Aggregator—Definitions for Element management are supplied from the Aggregator server, not the remote server. |
|    | Browse MIB   | This button opens the MIB Browser to allow the user to view the device's SNMP MIB.<br>The MIB Browser also allows an expert user with an Administrator or IT Manager account to manipulate the device on a more detailed level.  |
|    | View Scan Data                                     | This button opens one of the DDM Inventory Viewers to show device information collected by DDM Inventory scanners.<br>For more information, see <a href="#">View Scan Data</a> on page 92.   |
|    | Web  | This button attempts to open a web browser window for the device.<br>For more information, see <a href="#">Web</a> on page 92.<br>Note: The device must have an IP address. If not, this button is dimmed.   |
|  | Telnet   | This button attempts to open a Telnet session. Many network devices provide Telnet as a means to set up and configure the device.<br>Note: The device must have an IP address. If not, this button is dimmed.<br>Note: The device must support Telnet sessions. (DDM Inventory does not check before attempting a connection.)           |
|  | Update Model<br>(Administrator or IT Manager)      | This panel provides several actions you can take to update the device information in the DDM Inventory database. At the top of the panel, there is a drop-down list that you can use to select the action that you want to perform.<br>For more information, see <a href="#">Update Model (Administrator or IT Manager)</a> on page 93.  |
|  | Device Visibility<br>(Administrator or IT Manager) | This panel gives you options to activate, deactivate, hide, or purge devices.<br>For information on how to activate, deactivate, hide, or purge devices, refer to the <i>Configuration and Customization Guide</i> .   |
|  | Properties   | This button allows you to change the icon, title, and priority of a device in your network.<br>For instructions on how to use this feature, refer to the <i>Configuration and Customization Guide</i> .  |
|  | Asset<br>Questionnaire                             | This button opens up an Asset Questionnaire for this device.<br>For more information on how to create and use this feature, refer to the <i>Installation and Initial Configuration Guide</i> .   |

| Icon  | Name    | Description   |
|---|---------|---|
|  | Refresh | This button refreshes the contents of the panel.<br>When used with IP Ping and SNMP Ping panels, uses the last entered value instead of prompting you for a value.<br>Note: Does not re-read the data in the panel from the network. Re-reads the data only from the DDM Inventory database.<br>Note: Does not affect Properties or Locate panels, or any of the interactive session windows (Browse MIB, Web, Telnet). |
|  | Print   | This button prints the contents of the panel.   |
|  | Close   | This button closes the window and exits the Device Manager.   |
|  | Help    | This button opens a window that display context-sensitive help about the Device Manager.  |

## Configuration

This panel identifies a device and presents an overview of the device's identity and status.



This panel is blank if the device is not in the DDM Inventory database.

At the top of this panel, the device icon appears. Next to the icon, you can see if the device is SNMP-managed, unmanaged, or a virtual device. If an asterisk appears next to this description, it means that the IP address of the device has been cleaned from the DDM Inventory database because it was a duplicate of a more recently discovered device. To understand how devices with dynamically assigned IP addresses are managed, see the "Adding, Removing, and Replacing Devices" chapter in the *Configuration and Customization Guide*. When the device description appears with an asterisk, it is a link to the exception that is generated by this condition.

The remainder of this panel is divided into the following principal sections:

- Identity table (real devices only)
- Virtual Devices (host devices only)
- Virtual Devices Management Software (VMware VirtualCenter servers only)
- Asset Data table
- SNMP Configuration
- VMware Credentials (VMware hosts only)
- Mobile Discovery Credentials (mobile device servers only)
- Device structure (Serial number and description, disk, CPU, memory)
- Address table (real devices only)
- Virtual LANs



## Identity Table

As shown in [Table 1](#) on page 73, the information in the Identity table can come from these sources: the DDM Inventory Rulebase, the SNMP MIB of the object, and the data included in a scan file.

The Rulebase determines the device's operating system, application, device family, and model.

Some of the information collected from the SNMP MIB has been set by the device manufacturer; other information can be customized.

More elements of identity appear for the DDM Inventory server than for any other device.



All these elements are optional.

**Table 1 Identity Table**

| <b>Data</b>                                   | <b>Example</b>                              | <b>Creator</b>            | <b>Administrator or IT Manager</b> |
|---|---|---------------------------|------------------------------------|
| Package <sup>a</sup>                          | Main Map                                    | DDM Inventory/<br>account | —                                  |
| UNSPSC  | Computer Servers                            | Rulebase                  | —                                  |
| Family  | Cisco 2600 Series<br>Modular Access Routers | Rulebase                  | —                                  |
| Family current<br>manufacturer                | Cisco Systems Inc                           | Rulebase                  | —                                  |
| Model <sup>b</sup>                            | Cisco 2621XM Modular<br>Access router       | Rulebase                  | —                                  |
| Model current<br>manufacturer                 | Cisco Systems Inc                           | Rulebase                  | —                                  |
| Model historical<br>manufacturer <sup>c</sup> | Cisco Systems Inc                           | Rulebase                  | —                                  |
| Operating system                              | Cisco IOS Version 12.2<br>(8) T5            | Rulebase                  | —                                  |
| Operating system<br>current manufacturer      | Cisco Systems Inc                           | Rulebase                  | —                                  |
| Operating system<br>historical manufacturer   | Cisco Systems Inc                           | Rulebase                  | —                                  |
| Network Function                              | —   | Rulebase                  | —                                  |
| Network Function<br>current manufacturer      | —   | Rulebase                  | —                                  |
| Network Function<br>historical manufacturer   | —   | Rulebase                  | —                                  |
| Operating system                              | Linux                                       | DDM Inventory             | —                                  |
| Service pack                                  | —   | DDM Inventory             | —                                  |

**Table 1 Identity Table**

| <b>Data</b>                         | <b>Example</b>                          | <b>Creator</b>         | <b>Administrator or IT Manager</b> |
|-------------------------------------|---|------------------------|------------------------------------|
| NetBIOS name (network) <sup>d</sup> | DUPONT                                  | device owner           | —                                  |
| NetBIOS workgroup                   | MARKETING                               | device owner           | —                                  |
| Rulebase extra info                 | —                                       | DDM Inventory Rulebase | —                                  |
| Device-specific title               | —                                       | scripts                | —                                  |
| System OID                          | .1.3.6.1.4.1.295.5.1.1.2                | manufacturer           | —                                  |
| System OID manufacturer             | PlainTree Systems Inc                   | Rulebase               | —                                  |
| System description <sup>b</sup>     | Ethernet Switch                         | manufacturer           | —                                  |
| System contact                      | test@example.com                        | device owner           | set <sup>e</sup> link              |
| System name <sup>b</sup>            | ws1216-2                                | device owner           | set <sup>e</sup> . link            |
| System location                     | Server Room                             | device owner           | set <sup>e</sup> . link            |
| Managing VirtualCenter              | vmwar_host1/<br>15.178.180.105          | DDM Inventory          | —                                  |
| Asset tag                           | 78LL996                                 | Scanner                | —                                  |
| BIOS asset tag                      | —                                       | Scanner                | —                                  |
| BIOS product name                   | eserver xSeries 330<br>-[867441X]-      | Scanner                | —                                  |
| BIOS product manufacturer           | IBM                                     | Scanner                | —                                  |
| BIOS serial number                  | 78LL996                                 | Scanner                | —                                  |
| BIOS chassis                        | —                                       | Scanner                | —                                  |
| CPU                                 | Pentium III 1133 MHz<br>(Genuine Intel) | Scanner                | —                                  |
| Computer name (scan) <sup>f</sup>   | DUPONT                                  | device owner           | —                                  |
| Memory (MB)                         | 1024                                    | Scanner                | —                                  |
| Windows/NIS domain                  | MARKETING                               | Scanner                | —                                  |
| VM type                             | VMware                                  | DDM Inventory          | —                                  |
| VM name                             | VM-Vista64-Business                     | DDM Inventory          | —                                  |
| VM operating system                 | Microsoft Windows<br>Vista (64-bit)     | DDM Inventory          | —                                  |
| VM status                           | powered on                              | DDM Inventory          | —                                  |

**Table 1 Identity Table**

| <b>Data</b>                             | <b>Example</b>  | <b>Creator</b>       | <b>Administrator or IT Manager</b> |
|---|---|----------------------|------------------------------------|
| VM host                                 | myvmhost.mybiz.com / 208.77.188.166                   | DDM Inventory        | —                                  |
| VM UUID                                 | 50 3b c7 ba c9 fe<br>45 95-c2 15 3f de<br>23 f5 da 52 | DDM Inventory        | —                                  |
| VM Path                                 | [storage1]<br>VM-NoOS-3a/<br>VM-NoOS-3a.vmx           | DDM Inventory        | —                                  |
| Mobile phone number                     | (613) 123-4567  | Mobile device server | —                                  |
| Mobile carrier company                  | Cingular  | Mobile device server | —                                  |
| Mobile carrier network                  | CDMA  | Mobile device server | —                                  |
| Mobile status                           | Assigned  | Mobile device server | —                                  |
| Mobile user last name <sup>g</sup>      | Doe   | Mobile device server | —                                  |
| Mobile user first name <sup>h</sup>     | Jane  | Mobile device server | —                                  |
| Mobile user e-mail address <sup>g</sup> | jane_doe@hotmail.com                                  | Mobile device server | —                                  |
| Mobile device server                    | myserver.mycarrier.com / 208.77.188.166               | DDM Inventory        | —                                  |

- a. This is optional if you have not opened a map configuration since this object was discovered. The Network Map feature is available only if you have the Topology license.
- b. Appears with an asterisk next to it if the information about this device was gathered indirectly through Cisco Discovery Protocol (CDP) cache information from other network devices. When the data name appears with an asterisk, it is a link to the exception that is generated by this condition.
- c. Appears only when different from the current manufacturer.
- d. NetBIOS data is blank unless the device has an IP address or if the network card is disabled.
- e. A shortcut to the MIB Browser.
- f. On Windows workstations, frequently the same as the system name.
- g. NetBIOS data is blank unless the device has an IP address or if the network card is disabled.
- h. Only appears when this information is collected. Refer to “Protecting Private Information for Mobile Devices” in the *Reference Guide*.

## About the Package Data

The package row displays the position of a device within the packaging of the Network Map. Click on a hyperlink to open a corresponding map window.

If you have a map open, this row reflects the packaging of your current configuration. If you open the Device Manager and then make packaging changes that affect the device, click the **Refresh** button to have this row updated.

If you do not have a map open, this row reflects the packaging of the configuration you were using in your previous map session.

If you have never had a map open, this row does not appear.

If the device has been added to the network since the last time you saved your configuration, this row does not appear.

## Virtual Devices

The Virtual Devices table appears only when the device is a VM host. The table has two parts: information about the host itself, and information about the virtual devices that are associated with this host.

For the host, the following items are displayed:

- **Server:** Type of virtualization software running on the virtual device
- **Version:** Version of the virtualization software running on the virtual device
- **Platform:** Operating system running on the virtual device
- **Model:** Model of the virtual device server machine
- **UUID:** Universal Unique Identifier of the virtual device server

For each virtual device associated with this host, the following items are displayed:

- **Device:** Logical machine name and IP address of the virtual device
- **VM Name:** Name assigned to the virtual device
- **VM OS:** Operating system running on the virtual device
- **VM Status:** Current status of the virtual device
- **Update Time:** Time that DDM Inventory last collected information about this virtual device

## Virtual Devices Management Software

The Virtual Devices Management Software table appears only when the device is a VirtualCenter server. The table has two parts: information about the VirtualCenter server itself, and information about the VMware host that are managed by the VirtualCenter server.

For VirtualCenter, the following items are displayed:

- **Server:** Type of the virtualization software running on the VirtualCenter server
- **Version:** Version of the virtualization software running on the VirtualCenter server
- **Platform:** Operating system running on the VirtualCenter server
- **Model:** Model of the VirtualCenter server

For each VMware host managed by the VirtualCenter server, the following items are displayed:

- Device: Logical machine name and/or IP address of the VMware host
- Server: Type of the virtualization software running on the VMware host
- Version: Version of the virtualization software running on the VMware host
- Platform: Operating system running on the virtual device
- Model: Model of the VMware host machine
- Update Time: Time that DDM Inventory last collected information about VMware host

## Asset Data

This table displays the data entered in the Asset Questionnaire or collected from the scanner.

## SNMP Configuration

These are the community strings (for devices with SNMPv1/v2) and users (for devices with SNMPv3). The entire list is displayed in the Diagnostics panel. It will be blank if there are no strings or users configured in DDM Inventory.

An Admin or IT Manager user will also see a read and a write community string (for devices with SNMPv1/v2) or user (for devices with SNMPv3) for a device. These values are taken from the list of community strings and users; however:

- Strings and users from the list appear here only if they are valid.
- Only a single valid string/user appears here even if the list has multiple valid strings/users for this device.
- The read string/user that appears here is the string/user that DDM Inventory is currently using to poll the device.

## Deployment Credentials

This table shows you the deployment credentials (Admin and IT Manager only) that were most recently used to successfully communicate with this device. It shows you the values of the following settings:

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

## VMware Credentials

This table displays the preferred VMware credentials, including the user name and a password hint, for VMware hosts in this device group. This table is present only for VMware host devices. The information in the table is populated after the VMware discovery process is completed for this host. This information is only visible to Admin and IT Manager type accounts.

For additional information about how DDM Inventory works with VMware and other virtualization methods, refer to Chapter 4, “Virtualization in DDM Inventory” in the *Reference Guide*.

## Mobile Discovery Credentials

This table is present only for mobile device servers. The table displays the preferred log-on credentials, including the user name and a password hint, for this mobile device server. The information in the table is populated after the mobile discovery process is completed for this server. This information is only visible to Admin and IT Manager type accounts.

Mobile discovery credentials are specified in the Mobile configuration profile associated with the device group that contains this mobile device server. The profile can contain multiple sets of log-on credentials.

For more information about mobile device discovery, refer to “Mobile Devices in DDM Inventory” in the *Reference Guide*.

## Device Structure

This table provides information on the serial number of the chassis and modules in a device. You will see the following information about each module:

- Type (backplane, container, misc, other, powerSupply, stack, chassis, fan, module, port, sensor, CD, disk, cpu, ram, vram, tray, toner, unknown)
- If the following information is present in the MIB, it is also displayed: hardware, firmware, software, serial number, mount point, capacity, description

## Address

This table provides information about the IP addresses and/or MAC addresses of a device’s ports. The information comes from the Network Explorer or from scan file data.

This table has hyperlinks for all the ports with addresses. If a port does not have an address, it does not appear in the list. To open a Port Manager, click a port hyperlink. Each table row contains either:

- A MAC address, an OUI abbreviation (if known), and a manufacturer (if known)
- An IP address, a netmask (if known), and a domain name (if known)

A special port of “Device” is used:

- For the IP or MAC address that DDM Inventory identifies as the primary IP or MAC address for the device
- When DDM Inventory does not know which port an IP or MAC address is associated with

| Data                     | Notes                                       |
|--------------------------|---|
| Port index               | port number and description                 |
| MAC/IP address           | —   |
| OUI/Netmask              | netmask in octet notation                   |
| Manufacturer/Domain name | usually hyperlinked to an external web site |

The address table is particularly useful:

- When the device is
  - a router
  - a device with multiple IP addresses and domain name aliases (such as a web server)
- When you want to know a device's domain name (and domain name is not included in the list of **Device Title Preferences**)

## VLANs

VLANs are software-defined broadcast domains, created by your System Administrator at the switch. If your device has any VLANs configured, you will see them in the Device Manager.

VLAN example:

Virtual LANs:

| VLAN ID | Description        |
|---------|--------------------|
| 1       | default            |
| 100     | ComputerRoom       |
| 200     | VLAN0200           |
| 1002    | fddi-default       |
| 1003    | token-ring-default |
| 1004    | fddinet-default    |
| 1005    | trnet-default      |

## Reports

This panel displays current values for report and summary historical data. Displays alarm signals even when the device priority is less than the minimum priority for a configuration (unlike in map windows).

This 'report' data is historical information. You can use the data on this panel in conjunction with the State panel to look for problem trends in your device. For example, you can see an alarm in the State panel for the device CPU, you can check the 'reports panel' to see if there was a problem yesterday, or over the past week or month.

This panel is not available if the object is not in the DDM Inventory database.

## State

Displays 'report' data like adds, deletes, and changes. Also displays notifications if any of these are in an alarm state (info, minor, major, critical).

If there are any exceptions for the device, they are noted in this table. For a list of exceptions in your network devices, see the Health Panel and Alarms Viewer. For a complete listing of DDM Inventory exceptions, see **Help > Classifications > Exceptions**.

| Data        | Notes   |
|-------------|---|
| Report name | Exceptions, Device Adds, Device Deletes, Device Moves <sup>a</sup> , Device Changes, Not Recently Seen              |
| State       | OK, Info, Minor, Major, Critical  |
| Value       | For exceptions: <ul style="list-style-type: none"> <li>• description</li> <li>• effect</li> <li>• action</li> </ul> |

a) Device moves are only reported if the Topology license is installed.








Exceptions cannot always be reported for a device.





## Diagnosis

This panel displays information about the current state of the device that can be helpful in diagnosing problems.

You can access the following diagnostic tools from this panel:

| Icon  | Name                   | Description   |
|---|------------------------|---|
|  | Agent Deployment Log   | This button displays information logged during the agent deployment process.<br>For more information, see <a href="#">page 87</a> .                                   |
|  | Scanner Deployment Log | This button displays information logged during the scanner deployment process.<br>For more information, see <a href="#">page 88</a> .                                 |
|  | Virtual Log            | This button displays information logged during the VMware discovery process running on the host.<br>For more information, see <a href="#">page 88</a> .               |
|  | Mobile Discovery Log   | This button displays information logged during the mobile discovery process running on a mobile device server.<br>For more information, see <a href="#">page 88</a> . |
|  | IP Ping                | This button allows you to ping the device to see if it responds, and how quickly.<br>For more information, see <a href="#">page 88</a> .                              |



|   |            |   |
|---|------------|---|
|  | Traceroute | This button displays the path that data takes to get from the DDM Inventory server to the selected device.<br>For more information, see <a href="#">page 88</a> .                       |
|  | SNMP Ping  | This button allows you to query the device for basic SNMP information and displays this information.<br>For more information, see <a href="#">page 89</a> .                             |
|  | Agent Ping | This button allows you to make a connection to the agent running on the device.<br>For more information, see <a href="#">page 90</a> .  |
|  | DNS Query  | This button allows you to send a host query to the domain name server and displays a table that highlights configuration errors.<br>For more information, see <a href="#">page 90</a> . |

## Diagnostic Information

Beneath the heading, this panel is divided into these main sections:

- Main Diagnosis
- Configuration Profiles
- Discovery Configuration
- SNMP Configuration
- Asset Data
- Property Assignment

### Main Diagnosis

The information in the main table describes the data flow for this device, including when the device was first and most recently seen by various parts of DDM Inventory. It also shows the current value of numerous parameters.

[Table 2](#) summarizes the information displayed in the main diagnosis table:

**Table 2 Main Diagnosis**

| Data                                       | Output   | Notes                         |
|--|--|-------------------------------|
| First discovered                           | elapsed time <sup>a</sup> / absolute date & time | Reset if database is cleared. |
| Create time on mobile device server        | elapsed time / absolute date & time              | For mobile devices only       |
| Last profiled time on mobile device server | elapsed time / absolute date & time              | For mobile devices only       |
| Scanner model last updated <sup>b</sup>    | elapsed time / absolute date & time              | —                             |

**Table 2 Main Diagnosis**

| <b>Data</b>   | <b>Output</b>  | <b>Notes</b>  |
|---|--|---|
| Added to map  | elapsed time / absolute date & time                  | Resets if the device is deactivated, but then returns to the map.   |
| Last replied to ICMP                                    | elapsed time / absolute date & time                  | In ping or poll by DDM Inventory  |
| Last changed  | elapsed time / absolute date & time                  | The last time a connection to this device changed   |
| Device last modeled as a managed device <sup>b</sup>    | elapsed time / absolute date & time                  | The last time the model changed; determines whether or not the model has been updated for this device                         |
| Device last modeled as an unmanaged device <sup>b</sup> | elapsed time / absolute date & time                  | The last time a device was pinged for discovery; should be “n/a” or a time before “Model last updated”                        |
| Device last modeled as a mobile device <sup>b</sup>     | elapsed time / absolute date & time                  | The last time the model for this mobile device changed; determines whether or not the model has been updated for this device  |
| Last deactivated or hidden                              | elapsed time / absolute date & time                  | The last time a device was deactivated  |
| Mean break diagnosis time                               | minutes for alarms                                   | Mean break diagnosis time is approximate. Diagnosing a break may take longer, if communication with the device is unreliable. |
| Agent version   | version number (example, 9.30)                       | —   |
| Agent operating system                                  | name of operating system                             | —   |
| Agent port number                                       | port number (example, 2738 or 7738)                  | —   |
| Scanner version   | version number (example, 7.60.8200)                  | —   |
| Scanner configuration                                   | name of scanner configuration applied to this device | —   |
| Scan file location                                      | location of scan file on your DDM Inventory server   | —   |

**Table 2 Main Diagnosis**

| <b>Data</b>                      | <b>Output</b>   | <b>Notes</b>   |
|----------------------------------|---|--|
| Scan debug file                  | name of scanner log file; click the file name to display its contents, or click [Export] to write the contents to a text file | Appears only after the scanner runs on this device; the content of this file depends on the log level specified for the scanner (see “Command Line Parameters and Switches” in the “Scanners” chapter of the <i>Reference Guide</i> for additional information). |
| Scan type                        | the type of scan performed on the device  | —  |
| ARP tables seen                  | elapsed time / absolute date & time   | The last time the ARP tables were seen, to the nearest 30 minutes.   |
| Port ARP tables seen             | elapsed time / absolute date & time   | The last time the ARP tables were seen by this device, to the nearest 30 minutes.  |
| Port Bridge tables seen          | elapsed time / absolute date & time   | The last time the Bridge tables were seen by this device, to the nearest 30 minutes.   |
| Port Source address capture seen | elapsed time / absolute date & time   | The last time the Source address capture was seen by this device, to the nearest 30 minutes.   |
| Port Radio link seen             | elapsed time / absolute date & time   | The last time a Radio link was seen by this device, to the nearest 30 minutes.   |
| Port Bus link seen               | elapsed time / absolute date & time   | The last time a Bus link was seen by this device, to the nearest 30 minutes.   |
| Port carrier link seen           | elapsed time / absolute date & time   | The last time a carrier link was seen by this device, to the nearest 30 minutes.   |
| Port link training seen          | elapsed time / absolute date & time   | The last time link training was seen by this device, to the nearest 30 minutes.  |
| Port detailed link training seen | elapsed time / absolute date & time   | The last time detailed link training was seen by this device, to the nearest 30 minutes.   |
| Device modeler interval          | time (in days, hours, minutes, seconds)   | If custom, is shown here.  |

**Table 2 Main Diagnosis**

| Data                                   | Output       | Notes   |
|--|--------------|---|
| Mean device modeler update run time    | elapsed time | The mean length of time it takes to update the model for this device the previous 4 times |
| Recent device modeler update run times | elapsed time | The length of time it took to update the model for this device the previous 4 times       |
| Rulebase ID                            | —            | An internal number  |

- a. Elapsed time is reported in at least two of the following units: weeks, days, hours, minutes, and seconds. As elapsed time increases, the finer units of measure are not reported.
- b. The time gets updated when the model gets updated.

## Configuration Profiles and Device Groups

Configuration profiles are sets of attributes that define how a device is managed. There are several different types of configuration profiles, and you can associate one profile of each type with each device group.

**Table 3 Types of Configuration Profiles**

| Profile Type                 | Description  |
|------------------------------|--|
| Discovery profile            | Specifies how DDM Inventory finds devices to manage.   |
| SNMP profile                 | Specifies 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 also contain SNMP credentials.   |
| Network profile              | Specifies additional information that can be gathered from devices as well instructions as to how to use this information.   |
| Agent profile <sup>a</sup>   | Specifies high level agent deployment preferences and agent communication preferences.   |
| Scanner profile <sup>a</sup> | Specifies when devices should be scanned, how they should be scanned, and how the data should be returned to DDM Inventory.  |
| Virtualization profile       | Specifies how often and when to discover virtual devices such as VMware virtual machines. VMware credentials are also specified in Virtualization profiles.  |
| Mobile profile               | Specifies 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 log-on credentials for mobile device servers. |

- a. This profile only appears in the table when the Automated Inventory license is installed. See “License Options” in the *Installation and Initial Setup Guide* for more information about DDM Inventory licenses.

The DDM Inventory licensing model controls which of the above configuration profiles are available in your installation. For example, you will not be able to create agent and scanner configuration profiles if your license does not support these features.

DDM Inventory provides multiple preconfigured configuration profiles that support common management behaviors. These groups are denoted by < > symbols when they are displayed in a list. You cannot modify these preconfigured profiles.

For each type of configuration profile, there is one <default> profile. The <default> profiles ensure that all devices have a minimum set of management properties defined.

The Configuration Profiles table on the Diagnosis Panel shows you two things:

- It lists the configuration profiles associated with the highest priority device group to which this device belongs.
- For each profile type, it shows the highest priority device group to which this device belongs.



To optimize performance, DDM Inventory consolidates adjacent or parent-child IP ranges that share the same Basic Discovery and SNMP profiles. For this reason, the device group names that appear in this table for these two profiles may not match the highest priority device group listed on the Assign Priorities tab of the Administration > Discovery Configuration > Device Groups page.

## Discovery Configuration

This table shows the discovery parameters that have been set up for the device group to which this device belongs and what the values of these parameters are. These parameters are established using configuration profiles.

The Discovery Configuration table displays the default settings, and will display any overrides that have been performed through external means such as Web Services.

Discovery configuration parameters include:

- Basic discovery parameters
  - Allow the group to manage devices
  - Actively ping devices
  - Allow ICMP and SNMP
  - Allow IP addresses
- Network parameters
  - 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 parameters
  - Allow agent communication
  - Limit bandwidth for data transfers
  - Collect utilization data
  - AUM agent migration

- Allow agent upgrade
- Agent automatic upgrade schedule
- Agent deployment
- Deployment credentials
- Allow agentless scanner execution
- Remove scan data
- Allow new public key
- Allow modified public key
- Anonymization
- Scanner parameters
  - Deploy/upgrade scanners using this schedule
  - Run the scanner using this schedule
  - Download the scan file using this schedule
  - Automatically workflow interval
  - Allow scanners to be upgraded
  - Run pre-scan and post-scan scripts
  - Win32 scanner
  - HP-UX (HPPA) scanner
  - HP-UX (ia64) scanner
  - Linux scanner
  - AIX scanner
  - Solaris (SPARC) scanner
  - Solaris (x86) scanner
  - Mac OS X (PPC) scanner
  - Mac OS X (x86) scanner
- Virtualization parameters
  - VMware discovery interval
  - Discover VMware using this schedule
  - VMware credentials
  - Inventory VMware hosts
- Mobile parameters
  - Mobile discovery interval
  - Mobile inventory interval
  - Discover mobile devices using this schedule
  - Mobile port number
  - Use HTTPS to connect to mobile server

- Mobile credentials

➤ The Agent and Scanner parameters only appear in the table when the Automated Inventory license is installed. See “License Options” in the Installation and Initial Setup Guide for more information about DDM Inventory licenses.

## SNMP Configuration

These are the community strings (for devices with SNMPv1/v2) and users (for devices with SNMPv3) that will be tried for this device. This will be blank if there are no strings or users configured in DDM Inventory.

➤ Only Admin and IT Manager accounts can see the community strings and users.

## Asset Data

This table displays the data entered in the Asset Questionnaire.

## Property Assignment

The Property Assignment table helps you to determine the rules DDM Inventory has used to assign the title, icon, and priority to the device.

The Property Assignment table displays the Default settings, and will display any overrides that have been performed through External means such as Web Services, or by an Admin user through the Device Properties feature.

| Parameter | Notes  |
|-----------|--|
| Title     | The device title (default, external, and user-assigned)    |
| Icon      | The device icon (default, external, and user-assigned)     |
| Priority  | The device priority (default, external, and user-assigned) |
| Tag       | The device tag (default, external, and user-assigned)      |

If no value has been assigned, an asterisk (\*) appears in this table, indicating that the value for the property comes from the previous row of the table.

## Agent Deployment Log

The agent deployment log shows you all the operations performed during the deployment process, including any errors that may occur. This is very useful for troubleshooting.

➤ This button is only available if the Automated Inventory license is present. An exception is the DDM Inventory server itself, where this button is always available regardless of license.

## Scanner Deployment Log

The scanner deployment log shows you all the operations performed during the deployment process, including any errors that may occur. This is very useful for troubleshooting.



This button is only available if the Automated Inventory license is present. An exception is the DDM Inventory server itself, where this button is always available regardless of license.

## Virtual Log

The virtual log shows you raw discovery information for the VMware physical host and its hosted VMs for VMware on ESX server 3.0 or later. The information logged includes attempts to open a session with the host, attempts to login using different credentials, and, if successful, all the information that you can obtain about the host itself and the VMs it hosts. This information can be useful for debugging purposes.

## Mobile Discovery Log

The mobile discovery log shows you raw discovery information for a particular mobile device server. The information logged includes attempts to open a session with the mobile device server and attempts to run discovery and inventory commands using different logon credentials until a successful set of credentials is found. If and when DDM Inventory is successful in logging on to the mobile device server, the log will contain all the discovery and inventory information about the mobile devices that the mobile device server hosts. This information can be useful for debugging.

## IP Ping

Pings the device to see if it responds, and how quickly. The IP address pinged is the address identified by DDM Inventory as the primary IP.

### Limits

- 1–20 pings
- The device must have an IP address. If not, this button is dimmed.

### Default

5 pings

## Traceroute

Displays the path that data takes to get from the DDM Inventory server to the selected device by listing the gateway devices associated with each hop of the journey. The device identifier is often the host name, where available, but can also be the IP address. Each device title is hyperlinked to a Device Manager.

Traceroute also displays the amount of time each hop took. This time is the round trip in milliseconds. Traceroute includes two retry hops for each try, so the times for all three hops are shown.



Traceroute helps you to understand where on the network problems are occurring. It is often used after [IP Ping](#) has been used to confirm the existence of a device.

▶ The path displayed by traceroute is at OSI layer 3 and may not match the connectivity on the Network Map or in the Service Analyzer, which map at layer 2.

#### When to use it

- If you suspect that you are losing packets due to a large hop count.

In a TCP/IP network, where data are transmitted in packets, the header for a packet tracks the hop count. If the hop count grows too large, the packet is discarded.

- If you are trying to determine the point along the path where traffic is slowing down or getting lost altogether.
- If you are trying to determine the precise path taken—not so much to solve a problem as for general information.

▶ The device must have an IP address. If not, this button is dimmed.

Results of an asterisk for the device and for all three times (i.e. the result \* \* \*) indicates that data is not available for that hop of the journey, and usually indicates a trouble spot along the path. The following table explains codes you may see when you attempt a Traceroute.

| Character | Meaning  |
|-----------|--|
| *         | no response within a 3-second timeout interval |
| !         | ttl <= 1 <sup>a</sup>                          |
| !H        | host is unreachable                            |
| !N        | network is unreachable                         |
| !P        | protocol is unreachable                        |
| !S        | source route failed                            |
| !F        | fragmentation needed                           |
| !X        | communication is prohibited administratively   |
| !V        | a host precedence violation has occurred       |
| !C        | precedence cutoff is in effect                 |

- a. Time to Live (ttl) specifies how many more hops a packet can travel before being discarded or returned. The ttl value is supposed to start at 1 and increase by 1 until the host is reached.

## SNMP Ping

Queries the device for basic SNMP information and displays this information, and supports SNMPv1/v2 and SNMPv3. The IP address pinged is the address identified by DDM Inventory as the primary IP.

### Limits

The device must have an IP address. If not, this button is dimmed.

### Default

- Demo, IT Employee, IT Manager: “public”
- Administrator: The read community string or user for the device as defined on the SNMP tab in **Administration > Discovery Configuration > Configuration Profiles**.

## Agent Ping



This button is only available if the Inventory license is present. An exception is the DDM Inventory server itself, where this button is always available regardless of license.

Makes a connection to the agent running on the device to see if:

- the port number you have is correct (you can set this in **Administration > System Configuration > Agent communication**)
- the agent is installed and running on the device
- the security keys are correct

### Limits

The device must be in the DDM Inventory database.

## DNS Query

Sends a host query to the domain name server and displays a table that highlights configuration errors. A highlighted line indicates that the next line in the progression is missing.

The highlighted configuration errors are:

- a pointer (PTR) without an IP address (A or AAAA)
- duplicate pointer (PTR) records for the same IP address (A or AAAA)
- a mail exchanger (MX) directed to a canonical name (CNAME)
- a canonical name (CNAME) directed to anything that doesn't exist

Highlighted information also includes an explanation in the “Exceptions” column. You will see one of the following explanations:

- Duplicate
- Target does not exist
- n/a

If no information in the table is highlighted, DDM Inventory did not detect any problems with the DNS configuration of the device.

## Limits

If the device does not have an IP address, the button is dimmed.



If DDM Inventory displays the message “Non-existent domain”, it means that the device has not been assigned a domain name.



## Special Note about Using the Diagnosis Tools with Aggregator Servers

When you are accessing an Aggregator server, you can use the diagnosis tools—including Traceroute, IP Ping, SNMP Ping, Agent Ping, and DNS Query—in two different ways. The following example uses Traceroute, but the same principle applies to all the diagnosis tools.

To trace the route from the Aggregator server to a particular device:

- 1 Find a device using either the Aggregate Find tool or the Find tool associated with one of the aggregated servers.
- 2 In the Find tool results, right click that device, and select **Diagnosis > Traceroute**.

To trace the route from an *aggregated* server to a particular device:

- 1 From the left navigation menu, select one of the servers that is being aggregated.
- 2 Open the Device Manager for a device that has been discovered by this server.
- 3 In the Device Manager, click the **Diagnosis**  button.
- 4 In the Diagnosis panel, click the **Traceroute**  button.

For more information about Aggregator servers, refer to the “How It Works” chapter in the *Reference Guide*.

## Ports

This panel lists ports for this device and summarizes the information available for them. By default, it displays 24 ports at a time. You can change this value directly in the panel or in **Administration > Account administration > Account properties**).

There are also **Previous** and **Next** buttons and an All button that shows all ports in a single panel.



Ports do not always support all the attributes listed on the Device Manager Ports panel. If an attribute is not supported, the table column will be blank.

You can create different views for this panel, so you can concentrate on the data most important to you. See **Administration > System Configuration > Device Manager ports display preferences**. Read the inline help for definitions of all the preference properties.

The Configuration panel and Ports panel are the most commonly used ways of starting the Port Manager.

## View Scan Data

- ▶ For the customers with previous versions, this button is only available if the Inventory license is present. An exception is the DDM Inventory server itself, where this button is always available regardless of license.

This button opens one of the DDM Inventory Viewers to show device information collected by DDM Inventory scanners.

There are two different Viewers in DDM Inventory. The Win32 based Viewer is available with the DDM Inventory client, and the Java based Scan Data Viewer is available through the web user interface. You can select your preferred Viewer under **Administration > Account Administration > Account Properties**.

When you click this button, your preferred Viewer will appear.

You can see a complete list of hardware and software installed on the device, plus usage data, depending on how you have configured your Scanners with the Scanner Generator (see the *Configuration and Customization Guide*).

### Limits

If there is no scan data, the View Scan data button is dimmed.

- ▶ The DDM Inventory server always has scan data, as long as you have installed the Agent on the server. For more information, see the *Installation and Initial Setup Guide*.

## Web

This button attempts to open a web browser window for the device.

Only use this feature if the device supports web-based management or other web services.

### Limits

- The device must have an IP address. If not, this button is dimmed.
- The device must support HTTP sessions. (DDM Inventory does not check before attempting a connection.)

## Update Model (Administrator or IT Manager)

This panel provides several actions you can take to update the device information in the DDM Inventory database. At the top of the panel, there is a drop-down list that you can use to select the action that you want to perform.

The following table describes these actions.



These actions are also available on the Device menu and the right-click shortcut menu in any applet window (such as the Find or Network Map windows).

| Action               | Explanation   |
|----------------------|---|
| Query Device         | <p>Puts the device at the top of the device modeler's queue, and runs through all the steps as required.</p> <p>DDM Inventory tries all valid community strings or users for this device, in the order specified in the SNMP configuration profile assigned to this device group. It does not begin with the currently active community string/user; it begins with the first string/user in the list.</p> <hr/> <p>For individual mobile devices, this action initiates a mobile inventory operation. DDM Inventory determines which mobile device server manages this mobile device and issues an inventory command to that server. The mobile device server returns detailed information about this particular mobile device, such as the telephone number, manufacturer, model, operating system, subscriber name, and so on.</p> <p>Refer to "Mobile Devices in DDM Inventory" in the <i>Reference Guide</i> for more information.</p> |
| Run Mobile Discovery | <p>This action is only available for mobile device servers. Regardless of the schedule you have defined in the Mobile configuration profile, DDM Inventory immediately tries to connect to this mobile device server. If it successfully connects, it retrieves a list of the mobile devices managed by this server.</p> <p>This option is disabled, and mobile discovery will not run, if the mobile discovery frequency is disabled.</p> <p>If you select this action and do not see the results you expect, be sure to click the <a href="#">Mobile Discovery Log</a> button on the Diagnosis panel toolbar.</p> <p>Refer to "Mobile Devices in DDM Inventory" in the <i>Reference Guide</i> for more information.</p>   |

| Action               | Explanation   |
|----------------------|---|
| Run VMware Discovery | <p>Forces the immediate update (regardless of the user defined schedule) of the network model for the VMware physical host device and its hosted VMs in the DDM Inventory database.</p> <p>This action is disabled, and VMware discovery will not run, if either of the following conditions is true:</p> <ul style="list-style-type: none"> <li>• The virtualization discovery frequency is disabled.</li> <li>• The node does not have a valid IP address.</li> </ul> <p>If you select this action and do not see the results you expect, be sure to click the <a href="#">Virtual Log</a> button on the Diagnosis panel toolbar.</p> <p>Refer to “<a href="#">Virtualization in DDM Inventory</a>” in the <i>Reference Guide</i> for more information.</p> |
| Deploy Agent         | <p>Sends the Agent to the device.</p> <p>This action is not available if the <b>Automatic agent deployment active</b> option is turned off.</p>   |
| Upgrade Agent        | <p>Upgrades the Agent on the device.</p> <p>This action is only available when an Agent has been deployed to this device.</p> <p>If you select this action, you can specify the level of detail to output to the agent log file when the agent is upgraded.<sup>a</sup></p> <p>You can view the Agent information, the scanning workflow status, and the Scanner execution results on the page.</p>   |
| Upgrade Scanner      | <p>Transfers the relevant scanner executable and configuration files to the device, execute the scanners, and finally transfers the resulting scan file to the DDM Inventory server.</p> <p>This action is only available when an Agent has been deployed to this device.</p> <p>If you select this action, you can specify the level of detail to output to the scanner log file when the scanner is upgraded.<sup>a</sup></p>   |
| Run Scanner          | <p>Requests an immediate DDM Inventory scan of this device.</p> <p>This action is only available when an Agent has been deployed to this device.</p> <p>If you select this action, you can specify the level of detail to output to the scanner log file when the scanner is running.<sup>a</sup></p> <p>You can view the Agent information, the scanning workflow status, and the Scanner execution results on the page.</p>   |

| Action                | Explanation  |
|-----------------------|--|
| Retrieve Scan File    | <p>Transfers the result of the latest scan from the device to the DDM Inventory server.</p> <p>This action is only available when an Agent has been deployed to this device.</p> <p>If you select this action, you can specify the level of detail to output to the scanner log file when the scan file is retrieved.<sup>a</sup></p> <p>You can view the Agent information, the scanning workflow status, and the Scanner execution results on the page.</p>  |
| Uninstall Agent       | <p>Removes the Agent from the device. To verify that it has been uninstalled, try to do an Agent Ping on the Diagnosis panel.</p> <p>This action is only available when an Agent has been deployed to this device.</p> <p>After the Agent is uninstalled, the Agent-related actions will disappear from the drop-down list in the Update Model panel.</p>  |
| Run Agentless Scanner | <p>Requests an immediate agentless scan of this device. A secure connection is created, the appropriate scanner executable is transferred to the device, the scanner is executed, the scan data is retrieved, and the scanner executable is removed.</p> <p>If Secure Shell (SSH) is used to create the secure connection, the following message may appear:</p> <p><b>The SSH public key for this device does not match the key stored in the DDM Inventory database. Before you can run an agentless scanner on this device, you must reset the public key.</b></p> <p>If this happens, you can click the <b>Reset</b> button to reset the key that is stored in the database. The next time you perform an agentless scan on this device, the modified key on the device will be accepted and stored.</p> <p>If you have added new SSH public key credentials since running a scan, you can check the <b>Reset the SSH public key</b> check box above the <b>Update</b> button to reset the preferred credentials used by DDM Inventory server when making a secure connection.</p> <p>These actions are available if the <b>Allow agentless scanner execution</b> option in the Agent configuration profile associated with this device is selected.</p> <p>You can view the Agent information, the scanning workflow status, and the Scanner execution results on the page.</p> <p>Refer to <a href="#">“Two Types of Scanning: Agent-Based and Agentless”</a> in the <i>Installation &amp; Initial Setup Guide</i> for additional information.</p> |
| Enrich XML            | <p>Requests immediate enrichment of the scan file associated with this device.</p>   |
| Run Rulebase          | <p>Allows you to only re-check the DDM Inventory rulebase for this device.</p>   |

- a. In the **Detailed scanner logging** field at the bottom of the page, select **Off, Debug, or Trace**. Refer to the documentation for the `-log` scanner command line option in the “[Command Line Parameters and Switches](#)” section in the “[Scanners](#)” chapter of the *Reference Guide* for detailed descriptions of the various log levels.

If DDM Inventory is not able to perform a particular action at a given point in time, that action does not appear in the Update Model drop-down menu. Here, for example, are the actions available under various circumstances:

- Before a device is discovered, the Update Model menu contains the following actions:
  - Query Device
  - Deploy Agent
- After a device has been discovered, but before DDM Inventory has been able to communicate with the Agent, the Update Model menu contains the following actions:
  - Query Device
  - Deploy Agent
  - Run Agentless Scanner
  - Run Rulebase
- After DDM Inventory has been able to communicate with the Agent on a device, the Update Model menu contains the following actions:
  - Query Device
  - Deploy Agent
  - Upgrade Agent
  - Upgrade Scanner
  - Run Scanner
  - Retrieve Scan File
  - Uninstall Agent
  - Run Agentless Scanner
  - Run Rulebase
- After a scan file has been retrieved and processed by the XML Enricher, the Update Model menu contains the following actions:
  - Query Device
  - Deploy Agent
  - Upgrade Agent
  - Upgrade Scanner
  - Run Scanner
  - Retrieve Scan File
  - Uninstall Agent
  - Run Agentless Scanner
  - Enrich XML
  - Run Rulebase



- If the device belongs to a device group that has a Mobile configuration profile with a non-zero mobile discovery interval, the Update Model menu contains the following actions prior to the deployment of an agent on that device:
  - Query Device
  - Run Mobile Discovery
  - Deploy Agent
  - Run Agentless Scanner
  - Run Rulebase



The Update Model panel enables you to update the device model for a single device. To update device models for multiple devices, use **Administration > Data Management > Update device models**. See [Updating Device Models for Multiple Devices](#) in the *Reference Guide* for more information.

## Special Note about the Query Device Panel

On the Query Device panel, you will see a list of alarms associated with this device. The following is a list of all possible options that you can see. If you are performing an Update Model action on a new device, there may be a delay of as much as 1–2 hours before the device appears on the Network Map.

| State       | Message  |
|-------------|--|
| major alarm | IP address is not in scope                           |
| major alarm | no read community strings/users have been specified  |
| minor alarm | no write community strings/users have been specified |
| minor alarm | IP address is not in scope for resource management   |
| info        | current discovery process                            |
| info        | list of read community strings/users to be tried     |
| info        | list of write community strings/users to be tried    |
| info        | update interval                                      |
| info        | mean time to update model                            |

### When to use it

- When you've made physical changes to a device—for example, when you've changed cards in a router.
- When you've made changes to a device's community strings/users.

### Limits

The device must have an IP address. If not, this button is dimmed.

## Related

To determine when these commands have been run (either manually or automatically by DDM Inventory) see the [Diagnosis](#) panel. It lists all the relevant information.

## 9 Using the Port Manager

To select a different port for the same device, use the port list box.

Provides you with detailed information about a device's ports, in one of several panels.

Administrator or IT Manager: Also enables you to change the way DDM Inventory perceives a connection.



The Port Manager enables you to change only DDM Inventory's perception of a connection. The Port Manager does not change the physical connection.

To open the Port Manager:









| From  | Open by...                  |
|---|-----------------------------|
| Device Manager (State or Port panel), Reports | Click a port hyperlink.     |
| Network Map                                   | Right-click a line.         |
| Events Browser, Alarms Viewer                 | Double-click a port number. |







### List of Port Manager Panels

This is a complete list of panels available in the Port Manager. Click the hyperlinks in this table to read more information on these entries.



Many of the panels in the Port Manager feature data in table form. Not all tables will look the same for all ports, because the tables will only show data that is available for that port.

| Icon  | Button name   | Description  |
|---|---------------|--|
|    | Configuration | This panel identifies a port and presents an overview of the port's identity and properties.<br>For more information, see <a href="#">page 101</a> .   |
|    | State         | This panel displays current values for attributes.<br><b>NOTE:</b> This button is only available if the Topology license is present.<br>For more information, see <a href="#">page 103</a> .   |
|    | Reports       | This panel displays current values for report and summary historical data. Displays alarm signals even when the device priority is less than the minimum priority for a configuration (unlike in map windows).<br>For more information, see <a href="#">page 103</a> .   |
|    | Diagnosis     | This panel displays information about the current state of the port that can be helpful in diagnosing problems with DDM Inventory.<br>For more information, see <a href="#">page 104</a> .   |
|    | Statistics    | This panel provides a second toolbar that you can use to view or export detailed historical statistics for the port.<br><b>NOTE:</b> This button is only available if the Topology license is present.<br>For more information, see <a href="#">page 107</a> .   |
|  | Events        | This button opens the Events Browser with this device and port in context.<br>For more information, see <a href="#">Using the Events Browser on page 61</a> .  |
|  | Locate        | This button highlights in a map window the location of the device.<br>If a map session was not open already, one will open now. Within the map window, the device you are locating has a yellow circle around it.<br>If the window containing the device was already open, that window becomes the front-most window, and the window scrolls so that the highlighted icon can be seen.<br><b>NOTE:</b> This button is only available if the Topology license is present. |
|  | Purge Port    | This panel lets you remove the port from the device's model as created by DDM Inventory.<br>For more information, see <a href="#">page 109</a> .   |

| Icon   | Button name  | Description  |
|--|--|--|
|   | Create Connection<br>(Administrator or IT Manager) | This panel lets you force a new connection. You can create a connection to a real device or to a connector device.<br>For more information, see <a href="#">page 109</a> .<br><b>NOTE:</b> This button is only available if the Topology license is present.   |
|   | Break Connection<br>(Administrator or IT Manager)  | This panel lets you break an existing connection.<br>For more information, see <a href="#">page 110</a> .<br><b>NOTE:</b> This button is only available if the Topology license is present.  |
|   | Port Properties                                    | You can use the Properties dialog to change how DDM Inventory sees this port.<br>For more information, see <a href="#">page 110</a> .  |
|   | Refresh  | This button refreshes the contents of the panel.<br>Does not re-read the data in the panel from the network.<br>Re-reads the data only from the DDM Inventory database.  |
|   | Print  | This button prints the contents of the panel.  |
|  | Close  | This button closes the window and exits the Port Manager.  |
|  | Port number  | This pull-down list allows you to select from the valid port numbers for this device.<br>Note: The number DDM Inventory uses for the port may not match the physical port.<br>On your Cisco devices, the Cisco naming convention is displayed (for example, “Tu1” for Tunnel 1, or “Fa0/1” for Fast Ethernet 1). |

## Configuration

This panel identifies a port and presents an overview of the port’s identity and properties.

This panel is divided into these main sections:

- Connectivity table
- Identity table
- VLAN table

## Connectivity

Most information in this table comes from the DDM Inventory Rulebase.

| Data            | Example   | Notes  |
|-----------------|---|--|
| Connected to    | the selected port is connected to another device on this port | hyperlinked to Device Manager, Port Manager, and Line Manager<br><b>NOTE:</b> This column is only displayed when the Topology license is present |
| Description     | 100Base-TX Port   | from device manufacturer   |
| MTU             | 1500  | from device  |
| Interface type  | Ethernet CSMA/CD  | from device MIB/DDM Inventory Rulebase   |
| Line alarm type | Ethernet 100 HD   | from device MIB/DDM Inventory Rulebase   |
| Interface rate  | 100 Mbits/sec.  | from device MIB/DDM Inventory Rulebase   |
| Duplex          | Half  | Half   Full  |
| Autonegotiation | Auto negotiate  | -  |

## Identity

This table identifies the port and the manufacturer of the device:

- MAC address of the port
- OUI of the device/card (alphabetic abbreviation of the device manufacturer)
- Manufacturer of the device, hyperlinked to manufacturer's web site
- IP address of the port
- Netmask of the port
- Domain Name of the port

## VLAN Data

VLANs are software-defined broadcast domains, created by your System Administrator at the switch. By showing VLAN information in DDM Inventory, the Administrator can see how the devices in that virtual domain are configured.

## State

This panel displays current values for attributes.

### Limits

This panel is only available if the Topology license is present. This panel is not available if the object is not in the DDM Inventory database.

### Table

The table contains a list of supported device and port attributes in **Help > Classifications > Supported Device/Port Attributes**.

These values are collected from the network regularly and may change each time they are viewed. The values shown are the latest information available.

When data in a table has a gray background, the data shown is considered stale, because it was obtained before the beginning of your selected time period. To change the time before data is considered stale, see the section on Account Properties in the *Configuration and Customization Guide*.

## Reports

This panel displays current values for report and summary historical data. Displays alarm signals even when the device priority is less than the minimum priority for a configuration (unlike in map windows).

This 'report' data is historical information. You can use the data on this panel in conjunction with the State panel to look for problem trends in your device.

### Limits

This panel is not available if the object is not in the DDM Inventory database.

### State

Lists 'report' data like adds, deletes, moves, and changes, lets the user know if any of these are in an alarm state (info, minor, major, critical).

| Data        | Notes  |
|-------------|--|
| Report name | Exceptions <sup>a</sup> , Device Adds, Device Deletes, Device Moves <sup>b</sup> , Device Changes, Not Recently Seen |
| State       | OK, Info, Minor, Major, Critical   |
| Value       | For exceptions:<br>description<br>effect<br>action   |

- a. For a full list of possible exceptions, see **Help > Classifications > Exceptions**.
- b) Device moves are only reported when the Topology license is installed.

## Diagnosis

This panel displays information about the current state of the port that can be helpful in diagnosing problems with DDM Inventory.

This panel is divided into these main sections:

- Main table
- Property Assignment

### Main Table

The main table indicates the data flow for this port—when the device was first and most recently seen by various parts of DDM Inventory—plus the current values for several parameters.

| <b>Data</b>                | <b>Output</b>                                    | <b>Notes</b>  |
|----------------------------|--|---|
| First discovered           | elapsed time <sup>a</sup> / absolute date & time | resets if database is cleared   |
| Added to map               | elapsed time / absolute date & time              | resets if the device is deactivated/hidden, but returns to the map                            |
| Last moved                 | elapsed time / absolute date & time              | the last time a connection to this device changed   |
| Network model last updated | elapsed time / absolute date & time              | the last time the model changed; determines whether or not the model has been for this device |
| Scanner model last updated | elapsed time / absolute date & time              | —   |
| Last deactivated or hidden | elapsed time / absolute date & time              | the last time a device was deactivated or hidden  |
| Mean break diagnosis time  | time for alarms                                  | —   |
| ARP tables seen            | elapsed time / absolute date & time              | The last time the ARP tables were seen, to the nearest 30 minutes                             |
| Bridge tables seen         | elapsed time / absolute date & time              | The last time the Bridge tables were seen by this port, to the nearest 30 minutes             |



| <b>Data</b>                 | <b>Output</b>  | <b>Notes</b>   |
|-----------------------------|--|--|
| Source address capture seen | elapsed time / absolute date & time  | The last time the Source address capture was seen by this port, to the nearest 30 minutes. |
| Radio link seen             | elapsed time / absolute date & time  | The last time a Radio link was seen by this port, to the nearest 30 minutes.               |
| Bus link seen               | elapsed time / absolute date & time  | The last time a Bus link was seen by this port, to the nearest 30 minute.                  |
| Carrier link seen           | elapsed time / absolute date & time  | The last time a carrier link was seen by this port, to the nearest 30 minutes.             |
| Link training seen          | elapsed time / absolute date & time  | The last time link training was seen by this port, to the nearest 30 minutes.              |
| Detailed link training seen | elapsed time / absolute date & time  | The last time detailed link training was seen by this port, to the nearest 30 minutes.     |
| Connection method           | bridge tables<br>source address capture traffic<br>link training<br>logical subnet<br>approximate; see “Terms and Concepts” in the <i>Reference Guide</i> .<br>user-defined<br>unknown | —  |
| Previously connected to     | none<br>device (real or connector), hyperlinked to Device Manager<br>device and port, hyperlinked to the Device Manager and Port Manager   | if blank, the device is no longer in the database, or the connection has never changed     |

a. As elapsed time increases, the finer units of measure are not reported.

## Property Assignment

The Property Assignment table displays the Default settings, and will display any overrides that have been performed through External means such as Web Services, or by an Admin user through the Device Properties feature.

| <b>Parameter</b> | <b>Notes</b>   |
|------------------|--|
| Interface Rate   | The interface rate (default, external, and user-assigned)  |
| Interface Type   | The interface type (default, external, and user-assigned)  |
| Line Alarm Type  | The line alarm type (default, external, and user-assigned) |
| Duplex Mode      | The duplex mode (default, external, and user-assigned)     |

## Statistics

This panel provides a second toolbar that you can use to view or export detailed historical statistics for the port.

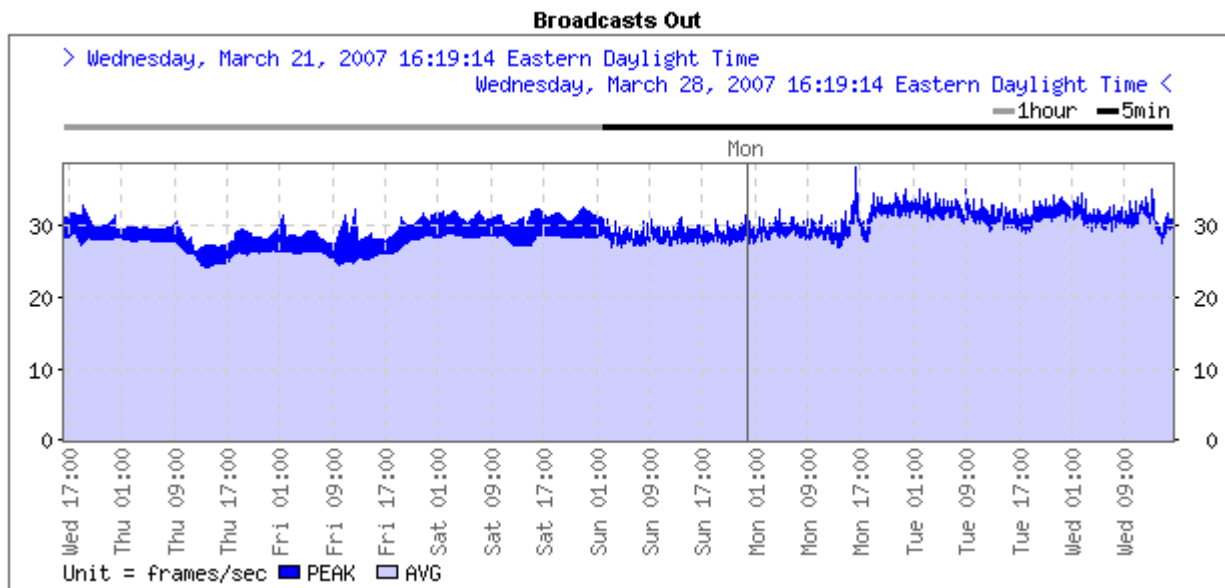
Inbound and outbound data is displayed for several statistics. Average values and peak values are available for some statistics. You can view the statistics in graph or table form, and you can export them to a Comma Separated Value (CSV) file.

Not all statistics are available for all ports. Only available statistics appear in the list. Statistics are a subset of Attributes (see Help > Classifications > Supported Device/Port Attributes).

DDM Inventory records current statistics every 5 minutes. After 2-3 days, the 5 minute samples are merged into 1 hour samples. After 33 days, the 1-hour samples are merged into daily samples.

### Graph

Depending on the time interval you select when you graph a statistic, the graph may contain data with different sampling granularity periods. If you display the last seven days, for example, the most recent 2-3 days will have 5-minute granularity, and the previous days will have 1-hour granularity.



Whenever a graph contains multiple sampling granularity periods, a horizontal bar that indicates the granularity of the data in each portion of the graph appears above the chart area. As shown here, the 1-hour averages produce a smoother graph than the 5-minute samples.

You can control the granularity of the data displayed by selecting different options in the granularity drop-down list. If you select Default, the least granular interval that applies to the time span of your graph will be used. In the graph above, the granularity selected was 5 minutes. If Default had been selected, 1-hour averages would have been displayed for the entire graph.

Gray portions of the graph indicate that data was not available for a period. Darker gray is used for unavailable data plotted in dark blue, lighter gray for unavailable data plotted in light blue. Also shown on the graph are horizontal lines representing alarm thresholds (depending on the option you have selected in the pull-down list).

You can change the graph by changing the selection in any of the pull-down lists. You can change the statistic, the interval, the maximum levels, and the granularity of data displayed.



Every account can have its own default settings for the statistic, interval, maximum levels, and granularity. See **Administration > Account administration > Account properties**.

### Table

The table shows a tabular view of the statistics.

### Export

Creates a Comma Separated Value (CSV) file of the data. Popular spreadsheets such as Microsoft Excel can import CSV files if you want to sort or graph the statistics in a way that is beyond the capabilities of DDM Inventory.

### Statistics

Available statistics depend on the device model.

### Interval

Past 2 hours | Past 4 hours | Past 6 hours | Past 12 hours | Past 24 hours | Past 48 hours | Past 7 days | Past 30 days | Past 90 days | Past 180 days | Past 365 days | Today | This week | This month | This quarter | This half | This year | Last week | Last month | Last quarter | Last half | Last year

### Maximum

These attributes show the maximum value of the vertical axis.

| Selection     | Description  |
|---------------|--|
| Data Max      | The vertical axis will show the maximum value of the data gathered.  |
| Attribute Max | Used for graphs such as Availability or Disk Space so that the vertical axis is scaled according to the maximum value of these Attributes. |



The y-axis maximum drop down list only applies when graphing data. It allows you to change the top most data point on the y-axis. Some of the options may have no effect on the display depending on the actual data. The highest data point is always shown, regardless of your selection.

### Granularity

Default granularity | 5-minute granularity | Hourly granularity | Daily granularity

## Purge Port

This panel lets you remove the port from the device's model as created by DDM Inventory.



This action cannot be undone.



You are *not* making a physical change to the port. If you purge a port but the port is still operational, the port will be rediscovered and will reappear.

### When to use it

When a port has been removed from the network and you wish to update DDM Inventory's representation of the device.

### Effects

- Deletes the statistical history associated with the port. This in turn affects the graphs and reports for this port.
- Deletes the events associated with the port from the event log.
- breaks the connection on the port

### Related

- To break a connection between ports, see [Break Connection \(Administrator or IT Manager\)](#) on page 110.
- To purge an attribute or a device, see the *Configuration and Customization Guide*.

## Create Connection (Administrator or IT Manager)



This panel is only available if the Topology license is present.

This panel lets you force a new connection. You can create a connection to a real device or to a connector device.

Create connection does not change the physical connection on the device; they change only how DDM Inventory represents the connection on the Network Map.



You can create a connector device by creating a connection to a nonexistent connector device.

Connections changes take effect at the end of the current sampling period.

### Effects



Do not create a connection to another real device except as a last resort. If you force a connection prematurely, you could slow DDM Inventory down or even make it impossible for DDM Inventory to correctly connect to your network. Never use forcing a connection as a quick fix.



Do not create a connection without consulting your DDM Inventory Customer Support representative. If you force a connection, DDM Inventory may not be able to correctly connect your network devices.



An exception: you may create connections to ports external to your network (for example, to your ISP) to ensure that the line break is reported.

Forcing a new connection first breaks any existing connection.

#### When to use it

When DDM Inventory has made incorrect assumptions about connectivity.

## Break Connection (Administrator or IT Manager)



This panel is only available if the Topology license is present.

This panel lets you break an existing connection.

Breaking a connection does not change the physical connection on the device; they change only how DDM Inventory represents the connection on the Network Map.

#### When to use it

When DDM Inventory has made incorrect assumptions about connectivity.

## Port Properties

You can use the Properties dialog to change how DDM Inventory sees this port.

### Interface Rate

Sets rate for a line interface.

#### When to use it

- When you want to set a custom line speed
- When DDM Inventory has set the wrong line speed.

#### Limits

0 bit/sec.–1 Tbit/sec.

#### Effects

Interface rate affects utilization statistics.

## Interface Type

Sets the media type used for the line.

### When to use it

- When DDM Inventory does not recognize the type of interface for the line.
- When DDM Inventory has set the wrong interface type for the line.

### Limits

DDM Inventory assigns a default duplex to each interface type.

### Related

To change the duplex mode, see [Duplex Mode](#) on page 111.

## Line Alarm Type

Sets the line alarm type for the connection. The line alarm type is normally associated with the interface type, but may be changed independently.

| Abbreviation | Expanded form                    |
|--------------|----------------------------------|
| ATM          | asynchronous transfer mode       |
| DSL          | digital subscriber line          |
| FD           | full duplex                      |
| FDDI         | fiber distributed data interface |
| HD           | half duplex                      |
| LAN          | local area network               |
| SPN          | switched packet network          |

### When to use it

When the default line alarm type associated with the interface is inappropriate.

## Duplex Mode

Sets the duplex to full or half. Full duplex allows for two-way communication over a line; half duplex permits only one-way communication.

### When to use it

When DDM Inventory has set the wrong duplex. This changes how DDM Inventory interprets the duplex mode, not the setting on the actual port.

### Limits

Full | Half

## Effects

Duplex affects utilization statistics.



---

# 10 Using the Line Manager

DDM Inventory has two different Line Managers:

- [Single Line Manager](#) on page 113
- [Multiple Line Manager](#) on page 115

## Single Line Manager

The single Line Manager provides you with detailed information about the two devices on either side of a connection.

The line can be between:






- the ports on two known devices
- a port on a known device and an unknown port on a device
- unknown ports on two devices

To open the Line Manager:

| <b>From</b>                  | <b>Open by...</b>                           |
|------------------------------|---|
| Network Map                  | Double-click a line, or right-click a line. |
| Service Analyzer             | Click a line.                               |
| Device Manager, Port Manager | Click a [line] hyperlink.                   |
| Report                       | Click a [line] hyperlink.                   |

## List of Line Manager Panels

This is a complete list of panels available in the Line Manager. Click the hyperlinks in this table to read more information on these entries.

| <b>Icon</b>   | <b>Button name</b>   |   |
|---|--|---|
|    | <a href="#">About</a>  | This panel shows two columns. In each column are a device and the relevant port for that device. If the Line Manager was opened by the Device Manager or Port Manager, the left column contains the device that was in context for the other Manager. |
|  | <a href="#">Break Connection (Administrator or IT Manager)</a> | This panel lets you break an existing connection.   |
|  | <a href="#">Refresh</a>  | This button refreshes the contents of the panel.<br>Note: Does not re-read the data in the panel from the network. Re-reads the data only from the DDM Inventory database.  |
|  | <a href="#">Print</a>  | This button prints the contents of the panel.   |
|  | <a href="#">Close</a>  | This button closes the window and exits the Line Manager.   |

### About

This panel shows two columns. In each column are a device and the relevant port for that device. If the Line Manager was opened by the Device Manager or Port Manager, the left column contains the device that was in context for the other Manager.

Underneath the heading is a single line that explains how the connection was made. This is identical to the “Connection method” row in the Port Manager panel for [Diagnosis](#) on page 104.

### Attribute name, unit, and value

Displays the current statistics for any attribute available.

These values are refreshed at the end of each poll cycle and may change each time they are viewed.

The metrics tables presented here is similar to the ones that would appear in the Device Manager and Port Manager’s State panel for each device port. The only difference here is the absence of the “update time column.”



It is important to understand that metrics for the two device ports will probably not match exactly. This is because the statistics for each device are not collected at the same time. Although there is rarely an exact match, the two sets of statistics should however be approximately equal, with in/out values reversed.

## Break Connection (Administrator or IT Manager)

This panel lets you break an existing connection.

### When to use it

When DDM Inventory has made incorrect assumptions about connectivity.

### Related

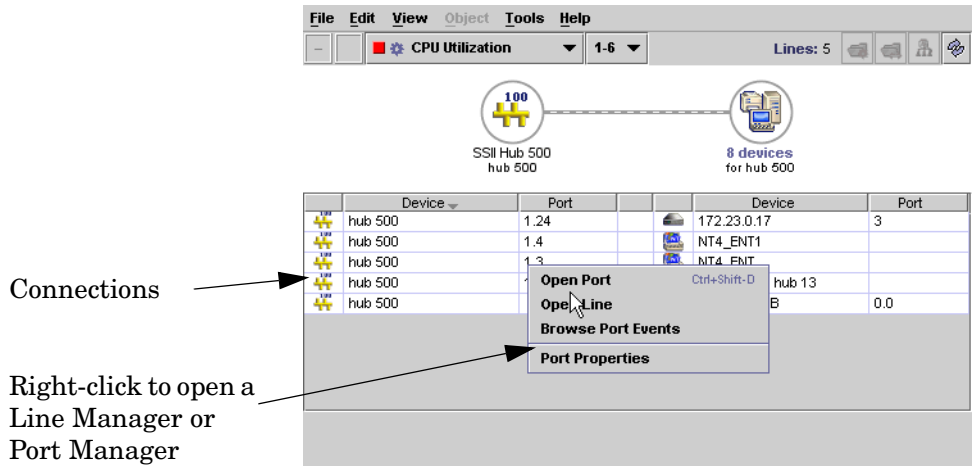
See also the Port Manager [Break Connection \(Administrator or IT Manager\)](#) on page 110.

## Multiple Line Manager

The multiline window opens when a line represents multiple connections between:

- two devices
- a device and a package

At the top of the multiline window is a graphic (looking like the Network Map), showing you the connected devices. Below the graphic is a table detailing all the connections.



By right-clicking on the port number, you can open a Port Manager or Single Line Manager. By right-clicking on a device name, you can open the Device Manager.

# 11 Using the Attribute Manager

The Attribute Manager provides you with detailed history of an attribute associated with a device or a port.



Connector devices cannot have attributes.




Administrator or IT Manager: Also enables you to change the state of an attribute, and to change the way DDM Inventory perceives an attribute.





To open the Attribute Manager:

| From                                       | Open by...                                     |
|--|--|
| Device Manager, Port Manager, Line Manager | Click an attribute hyperlink.                  |
| Events Browser, Alarms Viewer              | Right-click an attribute or event on the list. |

## List of Attribute Manager Panels

This is a complete list of panels available in the Attribute Manager. Click the hyperlinks in this table to read more information on these entries.

| Icon  | Button name  | Description  |
|---|--|--|
|  | <a href="#">Configuration</a>                        | This panel identifies an attribute and presents details of its most recently observed state.   |
|  | Locate   | This button highlights in a map window the location of the device.<br>If a map session was not open already, one will open now. Within the map window, the device you are locating has a yellow circle around it.<br>If the window containing the device was already open, that window becomes the front-most window, and the window scrolls so that the highlighted icon can be seen. |
|  | <a href="#">Manage (Administrator or IT Manager)</a> | This panel lets you manage the attribute.  |

| Icon  | Button name                                      | Description  |
|---|--|--|
|  | Purge Attribute<br>(Administrator or IT Manager) | This panel lets you remove an attribute and its historical statistics from the DDM Inventory database.   |
|  | Refresh  | This button refreshes the contents of the panel.<br>Note: Does not re-read the data in the panel from the network. Re-reads the data only from the DDM Inventory database. |
|  | Print  | This button prints the contents of the panel.  |
|  | Close  | This button closes the window and exits the Attribute Manager.   |

## Configuration

This panel identifies an attribute and presents details of its most recently observed state.

### Identity

| Element          | Notes  | Optional |
|------------------|--|----------|
| Name             | for a complete list, see <b>Help &gt; Supported Device/Port Attributes</b>   | —        |
| Description      | there can be multiples of an attribute (for example, disk, CPU, memory, toner)   | ✓        |
| Volume label     | —  | ✓        |
| Serial number    | —  | ✓        |
| Units            | varies according to the attribute, for example, time, percent, bytes/sec., frames/sec., milliseconds, days and hours, gigabytes. Not applicable for Breaks | ✓        |
| Minimum value    | —  | ✓        |
| Maximum value    | —  | ✓        |
| System threshold | available only for those attributes tracked on the Health Panel  | ✓        |

| Element               | Notes   | Optional |
|-----------------------|---|----------|
| Default threshold     | available only for those attributes tracked on the Health Panel | ✓        |
| State                 | available only for those attributes tracked on the Health Panel | ✓        |
| State Time            | available only for the Break attribute                          | ✓        |
| Value                 | —   | —        |
| Update time           | —   | —        |
| Forecast sample count | available only when using the Forecast feature                  | ✓        |
| Forecast first sample | available only when using the Forecast feature                  | ✓        |
| Forecast last sample  | available only when using the Forecast feature                  | ✓        |

For the Break attribute, there are two different times listed:

- The State Time represents the time when the attribute changed state (when the break occurred).
- The Update Time represents the most recent time DDM Inventory has seen the problem (i.e. the time of the last poll cycle where the problem was still present).



If a device had a partitioned disk, each partition will appear as a separate “Disk” attribute. You can open an Attribute Manager for each partition. Each partition will have a different disk serial number (assigned by the device OS).

## Manage (Administrator or IT Manager)

This panel lets you manage the attribute.

Examples: In the case of ports, Administrative Status can be turned on or off. In the case of the Bridge Aging Interval, the length of the interval can be changed.

### Limits

- Available only when DDM Inventory has a write community string for the attribute.
- Not all attributes can be managed.

## Purge Attribute (Administrator or IT Manager)

This panel lets you remove an attribute and its historical statistics from the DDM Inventory database.



This action cannot be undone.



You are *not* making a physical change. If you purge an attribute but the attribute is still present—that is, still associated with a device or port that is still present in your network—DDM Inventory will discover the attribute and the attribute will reappear.

### When to use it

- When an attribute is no longer associated with a device or port.
- When you no longer wish to retain or examine the history of an attribute.



## 12 Using the MIB Browser

The MIB Browser is a tool for the SNMP expert who knows what details to look for and how to look for them.

The MIB (Management Information Base) is a set of data that can be managed with SNMP. If you have the proper credentials for a device, you can use the DDM Inventory MIB Browser to read or write data to the device MIB.

DDM Inventory has a database of MIB definitions that the MIB Browser uses. The MIB Browser's private enterprises sub-tree contains placeholders for many of the vendors of network equipment who have non-standard or proprietary MIBs.



In order to work, the device must have an IP address, and it must support basic SNMP functionality.

The following sections describe how to use the MIB Browser, in detail:

- [Opening the MIB Browser](#) on page 121
- [Parts of the MIB Browser](#) on page 122
- [Read and Write Credentials](#) on page 128
- [Walking the MIB](#) on page 129
- [Using Multiple MIB Browser Sessions](#) on page 130
- [Watching an OID with MIB Radar](#) on page 130
- [Saving MIB Data as a Text file](#) on page 131

### Opening the MIB Browser

You can open a MIB Browser with or without a device in context. In other words, you can open a MIB Browser for a specific device, or you can open the MIB Browser and use its **Find** function to locate the device you want to see.

When you open a MIB Browser with a device in context, you will see the device icon, label and IP address in the right panel. It also shows the value of the “sysName” object from the MIB of that device.

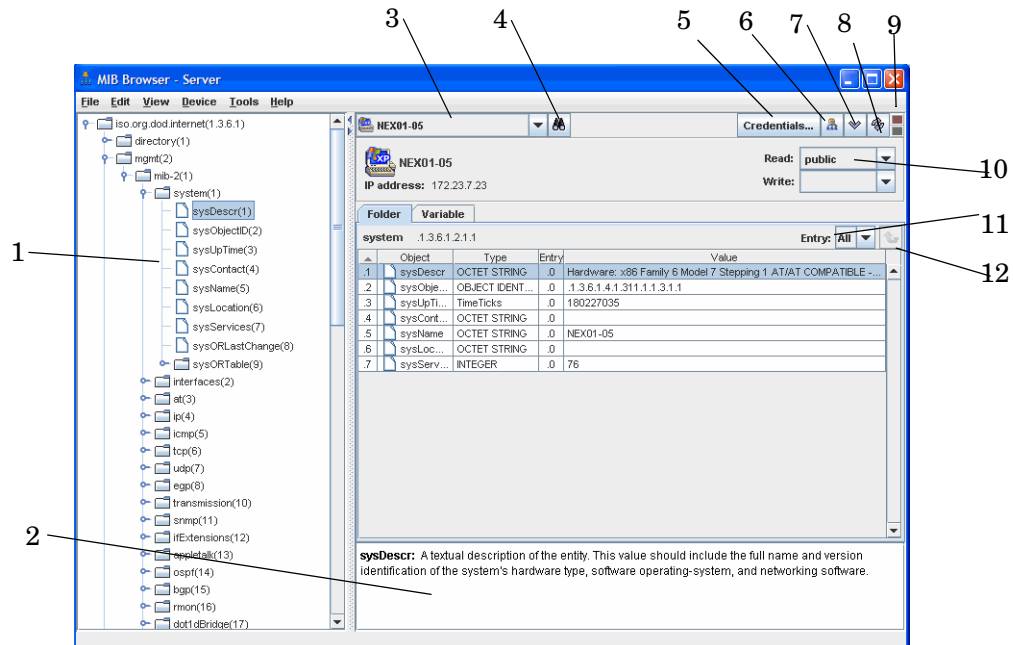
There are three ways to open a MIB Browser with a device in context:

- From the Device Manager, click the **Browse MIB** button.
- From the Device Manager's Configuration panel, click a **[set]** hyperlink. You must have Admin privileges.
- From any applet window (Network Map, Health Panel, and so on), click **Device > Browse MIB**.

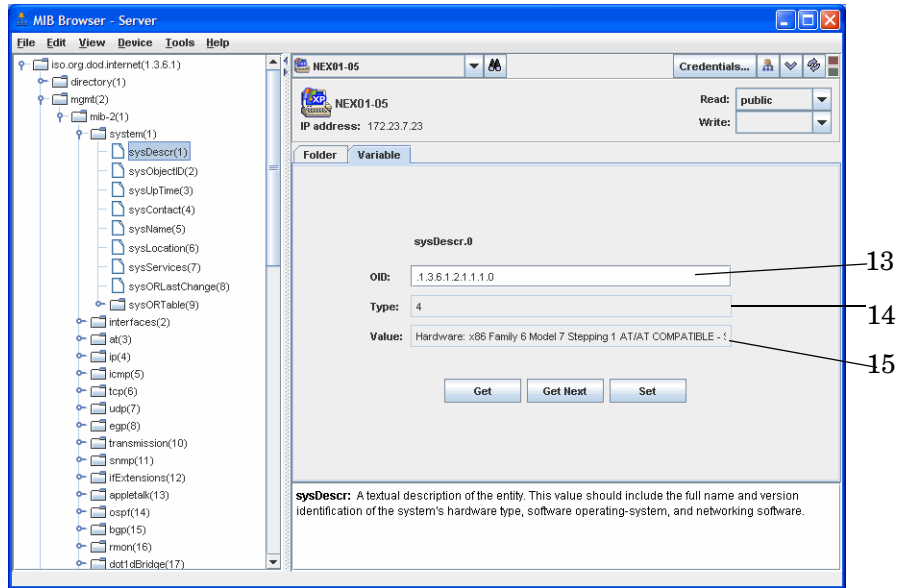
There are three ways to open a MIB Browser without a device in context:

- From the home page, click **MIB Browser**.
- From the MIB Browser, click **File > New MIB Browser**.
- From any applet window (Network Map, Health Panel, and so on), click **Tools > MIB Browser**.

## Parts of the MIB Browser



## MIB Browser example - Variable Panel:



**Table 1 MIB Browser legend**

| Number | Feature   |
|--------|---|
| 1      | MIB Tree View   |
| 2      | MIB OID Description   |
| 3      | Pull-down list of devices   |
| 4      | Find (to locate devices)  |
| 5      | Credentials (to view or add device credentials)                             |
| 6      | Locate on Map   |
| 7      | Get Next  |
| 8      | Refresh   |
| 9      | Colored lamps represent when the MIB Browser is connecting with the server. |
| 10     | SNMP Credentials (community string or user name)                            |
| 11     | Entry View  |
| 12     | Move up a Level   |
| 13     | OID number  |
| 14     | Type of OID   |
| 15     | Value of the OID  |

Topics in this section include:

- [Tree View](#) on page 124
- [Pull-down List of Devices](#) on page 124
- [Find Function](#) on page 124
- [Credentials Function](#) on page 125
- [Locate on Map](#) on page 125
- [Get Next](#) on page 126
- [Refresh](#) on page 126
- [Folder Tab](#) on page 126
- [Variable Tab](#) on page 127
- [MIB Description](#) on page 128

## Tree View

The left hand side of a MIB Browser shows a tree view of all the MIBs for which DDM Inventory has definitions. These definitions are stored within the DDM Inventory server, independent of any one device in your network. You can browse through the definition tree even without an SNMP device in context, by clicking on those tree nodes. Each node represents one SNMP object, and the hierarchy of nodes reflects the SNMP object hierarchy. The name, object ID, type and description of each SNMP object is displayed on the right hand side.



When there is an SNMP device in context (i.e. the device icon and IP address appear), clicking on a tree node will “Get” the value for that object from the device, if that object is supported. No one device supports all the objects in the MIB definition tree.

## Pull-down List of Devices

You can toggle between devices in the MIB Browser with this pull-down list. The pull-down list will display the 10 most recent devices that have been displayed in any applet window.

## Find Function

If you want to find a particular device to check its MIB, you can use the MIB Browser **Find** button. It works like the Find in the Network Map and other DDM Inventory features. Click the button, and a dialog appears. Enter the device name in the dialog and press **Enter**.

## Credentials Function

If you want to view or add credentials for a particular device, click **Credentials**. The Credentials dialog opens.

The screenshot shows the 'MIB Credentials' dialog box. It features a list on the left with 'private' and 'public' entries, where 'public' is highlighted. Below the list are 'Delete', 'Copy', and 'Create' buttons. The main area is split into two sections: 'SNMP V1/V2' and 'SNMP V3'. The 'SNMP V1/V2' section includes a 'Name' field containing 'public', a 'Mode' section with 'Read' checked and 'Write' unchecked, and a 'Community String' field containing 'public'. The 'SNMP V3' section includes a 'Mode' section with both 'Read' and 'Write' unchecked, a 'User Name' field, an 'Authentication Algorithm' section with 'None' selected (radio buttons for None, SHA, MD5), an 'Authentication Passphrase' field, an 'Encryption Algorithm' section with 'None' selected (radio buttons for None, DES, AES), and an 'Encryption Passphrase' field. An 'OK' button is located at the bottom center.

This dialog lists all the community strings and users the administrator has assigned to this device by way of an SNMP configuration profile. Click **Create** to create additional credentials for this device by specifying a community string or user name that you know is valid for that device. Click **Copy** if you want to duplicate and edit the credentials information for the currently highlighted credentials. The credentials you specify will apply for this one session and will not be added to the credentials that are associated with the SNMP configuration profile for this device. See [Read and Write Credentials](#) on page 128.



When creating credentials for an SNMPv3 device, you must follow certain rules for the various fields that make up the credentials for that device. Refer to the “Configuring the Discovery Process” chapter in the *Installation and Initial Setup Guide* for the rules governing user name, algorithms, and pass phrases.

## Locate on Map

The **Locate** button works like the Locate button in other DDM Inventory features. Click this button and you will see where this device is located on the Network Map.

## Get Next

The **Get Next** button will assist you in moving through the list of MIB objects.



For a given SNMP device, it is not possible to efficiently determine which MIB definitions it supports. It is only by “MIB walking” (using the **Get Next** button) a device that its supported objects can be determined. Thus the MIB Browser displays the same tree of MIB definitions for all devices, but not all of it is valid for any one device.

## Refresh

The **Refresh** button should be used after you change a community string, or after you change the device in context by using the device pull-down list.

## Folder Tab

This tab allows you to perform tasks that are described in the following sections:

- [Entry](#) on page 126
- [Move Up a Level](#) on page 127

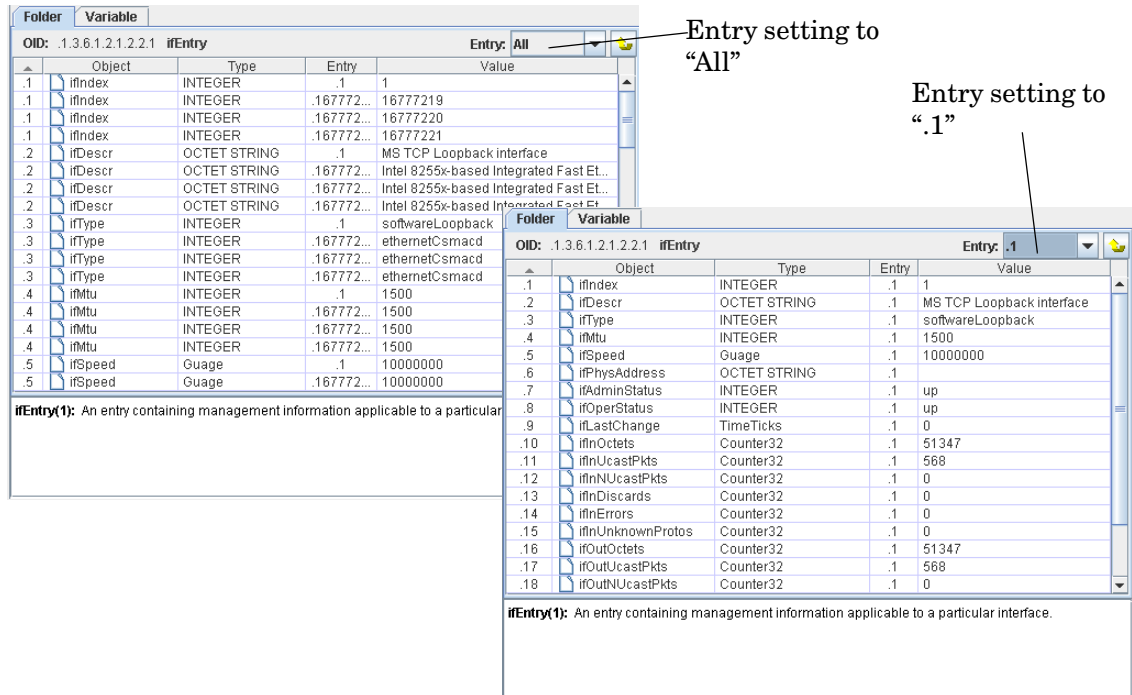
## Entry

Within an SNMP device, each supported object can have one or more entries, each of which has a value. For example, an object may define a column of a table, but each row of the column is a different value.

Each entry has an ID too, which defines how to index that entry within the object. The entry ID has the same syntax as an object ID. When a value is displayed, the “OID” field is actually the object ID followed by the entry ID. The “Name” field shows the name of the object followed by the entry ID.

Try thinking of it this way. The tree view on the left hand side shows objects and their hierarchy. The right hand side shows the values of instances of objects. As you press Get Next, you may see several successive instances of the same object.

The pull-down list will let you choose how the entries are displayed in the Folder Tab. By choosing All, you will see a list of all the entries, in numerical order. Also, you can select an entry number (for example, “.1”) and see only the object values for .1 entries.



## Move Up a Level

This button will move you up one level in the MIB tree view.

## Variable Tab

This tab allows you to perform tasks that are described in the following sections:

- [Read/Get](#) on page 127
- [Write](#) on page 127
- [Find OID](#) on page 128

## Read/Get

The Read area of the Variable tab displays the currently selected OID. If you want to update the view of that OID, click the **Get** button.

## Write

IT Manager and Administrator accounts can write to a device MIB.

Some devices may have a directed community string, which means they will only accept SNMP operations from specific devices. The network administrator may have created directed community strings that will allow only the DDM Inventory server access to the devices on your network.



Remember that although the MIB Browser GUI runs on a user's workstation, it is actually the DDM Inventory server that performs the SNMP **Set** and **Get**. A malicious user with the MIB Browser could leverage the DDM Inventory server to effectively bypass the protection of a directed community string. Thus it is a potential security breach to allow a user other than Administrator or IT Manager to do a **Set** with the MIB Browser.

To change a MIB entry:

- 1 In the MIB Browser **Folder** panel, select an OID.
- 2 Click the **Variable** panel.  
The **Variable** panel will show you the current definition for the OID.
- 3 Select the correct Write credentials.
- 4 In the **Write** section, enter a new definition for that OID.
- 5 Click **Set**.

## Find OID

When you select an OID in the tree view, the OID will also appear in the “Find OID” text box. Click the **Next** button to move through the MIB, like you would with the **Get Next** button at the top of the panel.

To go to a specific OID, you can change the OID in the “Find OID” text box, and click **Next**. The MIB Browser will go directly to that object entry.

## MIB Description

This area provides the standard description for each MIB object.

Sometimes, especially when first learning about MIBs, it is educational to view just the description of an object. Open a MIB Browser without a device in context, and you can see all the MIB descriptions available.

## Read and Write Credentials

Your ability to read or write MIB data depends on your account type.

Demo and IT Employee accounts can only read MIB data. They can do this with the “public” read community string for SNMPv2 devices. IT Employee accounts have the ability to enter temporary credentials for SMNMPv3 devices. There is no default SNMPv3 credentials for the Demo account.

IT Manager and Administrator accounts have full read/write access, as long as you have the correct credentials.



The MIB Browser Read Write pull-down lists display the network community strings and users you created on the SNMP tab in **Administration > Discovery Configuration > Configuration Profiles**. This procedure is described in the *Installation and Initial Setup Guide*.

The MIB Browser requests the complete list of credentials, as supplied on the SNMP tab on the **Configuration Profiles** page, and takes from that list all strings and users that apply to the device in context. For example, if the **Configuration Profiles** page lists the following strings for the network being explored:

- public (r), for 0.0.0.0-255.255.255.255
- private (w), for 192.168.0.0-192.168.9.255
- su\_only (r/w), for 192.168.0.0-192.168.0.255
- OnTheHalves (r/w), for 192.168.1.0-192.168.1.255

then the device 192.168.1.32 will show the following strings:

- public (r)
- private (w)
- OnTheHalves (r/w)

The string “su\_only (r/w)” will not appear in this window since the device's IP address (192.168.1.32) is outside the range of the string (192.168.0.0-192.168.0.255).



Community strings are case-sensitive. “Public” and “public” are two different strings.

If necessary, you can enter new credentials for the device by clicking **Credentials** in the MIB Browser as described in [Credentials Function](#) on page 125.

As DDM Inventory discovers the managed devices in your network, it uses the read credentials that you have configured to read the MIBs of those devices. The MIB Browser automatically uses the read credentials that DDM Inventory has determined is valid for that device.

However, if that device is not yet known to DDM Inventory, then DDM Inventory does not know the valid read credentials for that device, and you need to create new credentials by clicking **Credentials**.

The situation is a bit different for write credentials. DDM Inventory must have valid read credentials to discover a managed device, but valid write credentials are optional. DDM Inventory tries to determine valid write credentials for each managed device from the list of credentials in its SNMP configuration profile. If it finds one, the MIB Browser uses it, but otherwise the MIB Browser has no current write credentials.



If at any time you change the credentials that you are using to view the MIB, click the **Refresh** button.

## Walking the MIB

The Get Next button requests the value of the next SNMP object instance supported by this device. You may have noticed that as you push Get Next, the tree is expanded as necessary to keep the current object highlighted. Sometimes the next object a device supports is not the next item in the MIB tree because no one device supports all the objects in the MIB definition tree; some parts of the MIB tree are not relevant for any given device. These irrelevant sections of the MIB tree get skipped.

If there is no data available for a MIB object, the Value column will appear gray. If the community string does not allow you access to the MIB, you will see “no response.”

If there is a “no response” message, the SNMP device did not respond to a Get, Get Next, or Set request. There are a few reasons for this error:

- The device does not have an SNMP agent; in other words the device is not managed.
- The device has an SNMP agent, but it did not respond to the request within a certain amount of time. Some devices drop management requests when they are too busy handling their network traffic.
- The community string being used by the MIB Browser is incorrect. Perhaps someone recently changed the device's community string and DDM Inventory has not yet, or cannot, determine a valid one.
- The device supports directed community strings, and DDM Inventory is not on the access list.

Unfortunately, the SNMP protocol does not distinguish amongst these conditions.

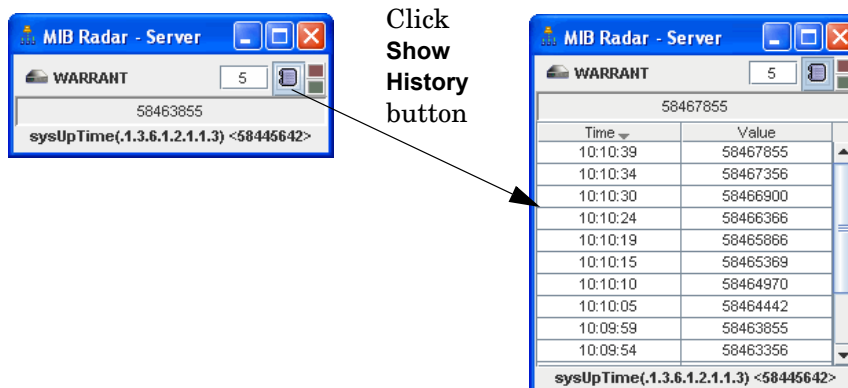
## Using Multiple MIB Browser Sessions

You can have more than one MIB Browser window open at any time. Also, you can toggle between several devices in the “found device” pull-down list at the top-left of the MIB Browser window.

To open a new MIB Browser session from your current MIB Browser window, click **File > New MIB Browser**.

## Watching an OID with MIB Radar

You can use the MIB Radar feature to watch a particular MIB object in a separate small window on your screen. If you want to monitor one counter in the MIB (for example, sysUpTime), you can select that OID and then click **File > Open Radar**. The radar window will appear, which looks like this:



By default, the data refreshes every 30 seconds.

You can change the refresh rate by entering a number (5 or higher) in the text box. Also, you can view the history of the OID by clicking on the **Show History** button.

## Saving MIB Data as a Text file

There are two ways you can save MIB Browser data to a text file:

- [Save Table Data](#)
- [MIB Walk](#)

### Save Table Data

You can use the **Save Table Data** feature to save selected info into a tab-separated-value (.tsv) file. This feature can also be found in the Health Panel, MIB Browser, Alarms Viewer, Service Analyzer, and Events Browser.

You can save the entire contents of a MIB Browser table, or you can Ctrl-click to select the OIDs you want to save.

Saving data to a text file

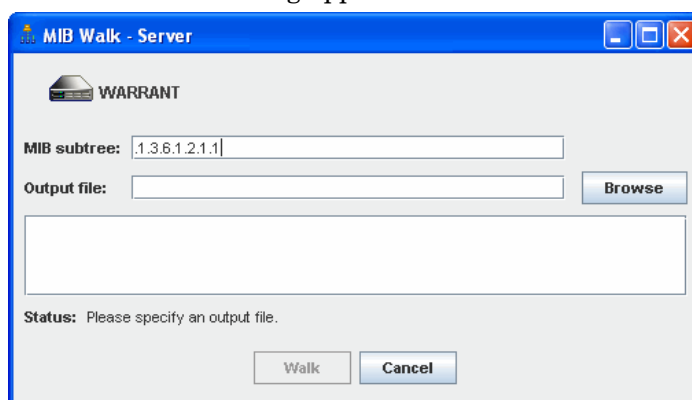
- 1 Select the MIB OIDs you want to save.
- 2 Click **File > Save Table Data**.  
A Save Table Data dialog appears.
- 3 Select a file name and location for the text files.
- 4 Click **Save**.

### MIB Walk

You can use the **MIB Walk** feature to save a sub-tree from the MIB Browser as a text (.txt) file.

Saving a MIB Walk:

- 1 Click **File > Open Walk**.  
The MIB Walk dialog appears.



- 2 Enter an OID that represents the start of the sub-tree you want to save.

- 3 Click **Browse** to select a name and location for your output file.
- 4 Click **Walk**.

# 13 Using the Scan Data Viewer

The Scan Data Viewer displays detailed information contained in the Discovery Database, data compiled from DDM Inventory's discovery and scanning processes. This provides a convenient way of displaying software, hardware and asset information collected for an individual device.

In summary, the Scan Data Viewer displays:

- Detailed and summarized hardware configuration information.
- Asset information.
- Details of all software scanned.
- Software Utilization data (if you have a Utilization license).



The Scan Data Viewer is similar to the Viewer (part of the DDM Inventory client). They both show similar information, but the Scan Data Viewer is accessible through the web user interface.

Topics in this section include:

- [Opening the Scan Data Viewer](#) on page 133
- [Parts of the Scan Data Viewer](#) on page 134
- [Viewing Hardware and Configuration Data](#) on page 135
- [Viewing Software Application Data](#) on page 137
- [Software Utilization](#) on page 140

## Opening the Scan Data Viewer

You can open a Scan Data Viewer with or without a device in context. In other words, you can open a Scan Data Viewer for a specific device, or you can open the Scan Data Viewer and use its **Find** function to locate the device you want to see.

There are three ways to open a Scan Data Viewer with a device in context:

- From the main navigation tree, click on **Devices with Scan files**. From the Device Manager, click the **View Scan Data** button.
- From any applet window (Network Map, Health Panel, and so on), click **Device > View Scan Data**.

There are three ways to open a Scan Data Viewer without a device in context:

- From the main navigation tree, click **Scan Data Viewer**.
- From the Scan Data Viewer, click **File > New Scan Data Viewer**.

- From any applet window (Network Map, Health Panel, and so on), click **Tools > Scan Data Viewer**.

When you open a Scan Data Viewer with a device in context, you will see the device icon, title, IP address, and asset tag in the top panel. It also shows the following values:

- OS
- CPU
- Memory
- Disk

## Parts of the Scan Data Viewer

Topics in this section include:

- [Pull-down List of Devices](#) on page 134
- [Find Function](#) on page 134
- [Locate on Map](#) on page 134
- [Refresh](#) on page 134
- [Using Multiple Scan Data Viewer Sessions](#) on page 135
- [Menu Commands](#) on page 135

### Pull-down List of Devices

You can toggle between devices in the Scan Data Viewer with this pull-down list. This list records the 10 devices that have been most recently used in any applet window.

### Find Function

If you want to find a particular device to load its scan file, you can use the Scan Data Viewer **Find** button. It works like the Find in the Network Map and other DDM Inventory features. Click the button, and a dialog appears. Enter the device name in the dialog and press **Enter**.

Any devices that have been found, but for which there is no scan data in the database, will be grayed out and cannot be opened.

### Locate on Map

The **Locate** button works like the Locate button in other DDM Inventory features. Click this button and you will see where this device is located on the Network Map.

### Refresh

The **Refresh** button launches a new request to the database to fetch the information again. A refresh will be done automatically when the device changes. It is not necessary to do it manually.

## Using Multiple Scan Data Viewer Sessions

You can have more than one Scan Data Viewer window open at any time. Also, you can toggle between several devices in the “found device” pull-down list at the top-left of the Scan Data Viewer window.

To open a new Scan Data Viewer session from your current Scan Data Viewer window, click **File > New Scan Data Viewer**.

## Menu Commands

**Table 1 Menu commands in the Scan Data Viewer**

| <b>Command</b>               | <b>Description</b>   |
|------------------------------|--|
| Print command in File menu   | This command will print the table currently displayed.           |
| Save Table Data in File menu | This command will output tab-separated data to a file.           |
| Copy in Edit menu            | This command will copy the selected table rows to the clipboard. |

## Viewing Hardware and Configuration Data

Topics in this section include:

- [Hardware and Configuration Data Page Overview](#) on page 135
- [The Hardware and Configuration Tab Page Layout](#) on page 136

### Hardware and Configuration Data Page Overview

The Hardware and Configuration tab displays:

- User and asset information collected using the asset questionnaire during the inventory.
- High level hardware information scanned during the inventory.

#### Further Information

- For a detailed list of all the hardware items scanned, see **Help > Data Collected by the Scanners**.

## The Hardware and Configuration Tab Page Layout

**Scan Data Viewer - Server**

File Edit View Device Tools Help

MyServer

**Title:** MyServer **OS:** Windows 2003 Server Enterprise Edition  
**IP address:** 172.23.7.128 **CPU:** Pentium III 1000 MHz (GenuineIntel)  
**Asset tag:** 0010F3043730 **Memory:** 1,024 Mbytes **Disk:** 69,420 Mbytes

Hardware and Configuration Software Applications Software Utilization

Asset Data  
 CPU Data  
 i CPUs  
 CPU Type  
 Intel CPU Brand  
 CPU Description  
 Actual CPU Speed (MHz)  
 Rated CPU Speed (MHz)  
 Model CPU Speed (MHz)  
 CPU Vendor  
 CPU Model  
 CPU Family  
 CPU Stepping  
 CPU Special  
 i CPU Cache Information  
 Intel CPU Features  
 Intel Extended CPU Feature...  
 CPU Serial Number  
 CPU Board  
 CPU Port Id  
 CPU Mask  
 CPU Overdrive  
 CPU Dual  
 CPU Active

| i | Item Name                    | Item Value                          |
|---|------------------------------|-------------------------------------|
| 0 | CPU Type                     | Pentium III                         |
| 0 | Intel CPU Brand              | Intel Pentium III                   |
| 0 | CPU Description              |                                     |
| 0 | Actual CPU Speed (MHz)       | 996                                 |
| 0 | Rated CPU Speed (MHz)        | 1000                                |
| 0 | Model CPU Speed (MHz)        |                                     |
| 0 | CPU Vendor                   | GenuineIntel                        |
| 0 | CPU Model                    | 8                                   |
| 0 | CPU Family                   | 6                                   |
| 0 | CPU Stepping                 | 10                                  |
| 0 | CPU Special                  |                                     |
| 0 | Intel CPU Features           | MMX,SSIMD                           |
| 0 | Intel Extended CPU Featur... |                                     |
| 0 | CPU Serial Number            |                                     |
| 0 | CPU Board                    |                                     |
| 0 | CPU Port Id                  |                                     |
| 0 | CPU Mask                     |                                     |
| 0 | CPU Overdrive                |                                     |
| 0 | CPU Dual                     |                                     |
| 0 | CPU Active                   |                                     |
| 0 | CPU Speed (MHz)              | 1000                                |
| 0 | CPU                          | Pentium III 1000 MHz (GenuineIntel) |

**CPUs:** This contains information about all CPUs in the machine; each field is repeated for every CPU the machine contains.

Scan date: Wednesday, March 28, 2007 11:48:54 EDT Scanner version: 2.20.000 build 6334

The left hand side of a Scan Data Viewer shows a tree view of all the Hardware and Asset data items for which DDM Inventory has definitions. All data shown is from the scan date shown at the bottom of the page.

You can browse through the hardware definition tree even without a device in context, by clicking on those tree nodes. Each node usually represents one hardware object. Those nodes with a red “i” indicate multiple values for that node, which often represent multiple hardware objects. The Item Number, Name and Value of the scanned data item is displayed on the right hand side.





Asset data is displayed in the first folder under Hardware data. The asset data to be collected is configured in the Web Asset Questionnaire, or in old scan files.

The information includes details about users, departments, physical assets, equipment, and any other information that is useful to record.

A description of the scanned data item can be found in the bottom pane.

A detailed list of all the hardware items scanned and their descriptions can be found at **Help > Data Collected by the Scanners**.

The  button will move you up one level in the Scan Data Viewer tree view.

The  indicator tells you whether there is connectivity between this device and the DDM Inventory server (green = OK; red = no connectivity to the server).

## Viewing Software Application Data

Topics in this section include:

- [Software Application Tab](#) on page 137
- [Information Shown in the Application Data Window](#) on page 138

### Software Application Tab

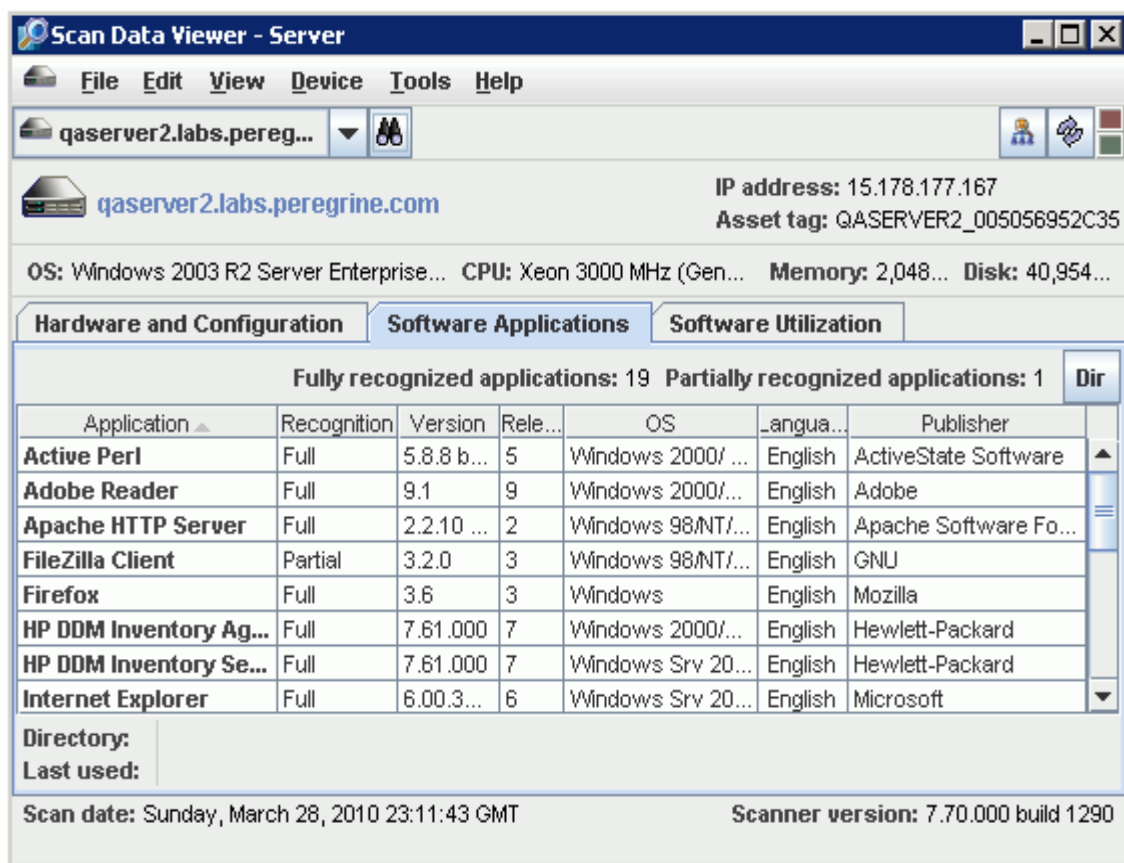
When the application recognition is enabled, a Software Application tab is available in the Scan Data Viewer workspace. This tab shows a summary of identified applications on the selected machine.

There are three options for the application recognition: No recognition, Installed applications, and Software application index (SAI). By default, Scan Data Viewer uses the SAI to perform application recognition. In this case, the Software Applications tab displays applications that have been fully or partially recognized by the SAI.



To configure the application recognition, go to **Server > Administration > System Configuration > Scan processing > Application Recognition**.

You can see the scan date at the bottom of the page.



## Information Shown in the Application Data Window

The following information is shown about each software application:

- **Application**  
The name of the software application.
- **Recognition**  
For the SAI recognition, this column displays `Full` for the fully recognized applications or `Partial` for the partially recognized applications.  
For the Installed applications recognition, this column displays `Installed Applications`.
- **Version**  
The application version
- **Release**  
The application release
- **OS**  
The operating system the application was running on.
- **Language**

The name of the language of the application.

- **Publisher**

The name of the software publisher (for example, Microsoft, IBM).

Two fields at the bottom of the page show the following information for an application:

- **Directory**

The directory on the scanned machine where the application was installed.

- **Last Used**

The last time the file was accessed - (yyyy/mm/dd) (hrs:mins)

See [Dir Button](#) for more information.

## Dir Button

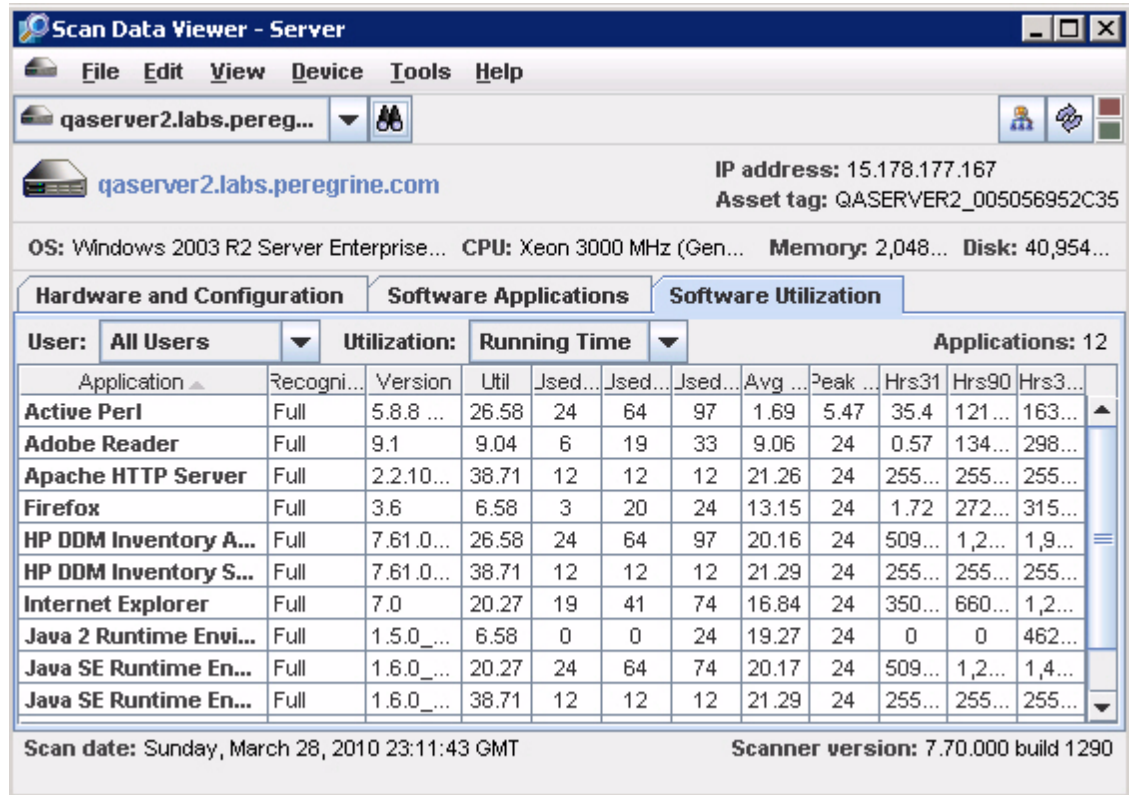
If this button is clicked the view presented will change to display the following columns:

- Application
- Version
- Directory
- Last used

Click the **Dir** button again to toggle back to the original view.

# Software Utilization

The Viewer shows per-user application utilization data (select a particular user from the User pull-down list). It also shows utilization time in terms of the total running time of an application or the focus time of an application when it is running in the foreground (select the time from the Utilization pull-down list).



This information is only available if the software utilization agent plug-in was running on the computer which was scanned.



Refer to the *Scan Data Analysis Guide* for more information on the Viewer and software utilization.

To view application utilization data:

Select the user you want to see data for from the drop-down list. The following information is shown for how users utilized a particular application.

- **Application**
- **Recognition**
- **Version**
- **Utilization**

The number of days that the application was used (as a percentage) over a period of time. The period is calculated automatically depending on how long the application was used for. As a rough guideline the time periods are as follows:

- Application used for more than 3 months - utilization is calculated over the year.

If the earliest application usage recorded is more than 3 months old, but less than 1 year (i.e. there was a record that the application was used more than 3 months ago, but less than a year ago), an annual figure will be used (number of days used in the last year / 365)

- Application used for less than 3 months but more than 1 month - utilization is calculated over a quarterly period.

If the earliest usage recorded is less than 3 months, but greater than 1 month, a quarterly figure is used (number of days used in the last quarter / 90).

- Application used for less than one month - utilization is calculated monthly

A monthly figure is used here (number of days used in the last month / 31)

- **Used31**

The number of days the application was used in the last month.

- **Used90**

The number of days the application was used in the last quarter.

- **Used 365**

The number of days the application was used in the last year.

- **Avg Hrs**

The daily average in hours over the period configured.

- **Peak Hrs**

The highest daily number in hours over the period configured.

- **Hrs31**

The number of hours the application was used in the last month.

- **Hrs90**

The number of hours the application was used in the last quarter.

- **Hrs365**

The number of hours the application was used in the last year.



# 14 Using the Reports

DDM Inventory provides numerous reports to help you analyze and understand what is contained in your network. DDM Inventory reports comprise the following groups:

**Table 1 DDM Inventory Reports**

| <b>Report Category</b>  | <b>Explanation</b>   |
|---|--|
| <a href="#">Executive/Summary Network Reports</a> on page 145 | These reports are intended as a general overview of what is in your network. You can see lists of all your network devices.  |
| <a href="#">Scanned Device Reports</a> on page 146            | If you use DDM Inventory to scan devices in your network, these reports provide hardware, operating system, application, and license information for scanned devices. Both summary and detailed reports are available. A special report indicating which devices can be upgraded to Windows Vista is also included in this category.   |
| <a href="#">Software Inventory Reports</a> on page 149        | These reports show information about the software applications installed on your scanned devices. This includes applications recognized by the DDM Inventory Software Application Library as well as unrecognized files. A special group of reports in this category enables you to examine unrecognized applications that are not yet in the Application Library. Another group shows you which applications and features were reported by the operating systems on your scanned devices. |
| <a href="#">Virtualization Reports</a> on page 154            | These reports provide information about Solaris global zones and the zones that they host, VMware hosts and their associated VMs, and VirtualCenter management servers and the VM hosts they manage.   |
| <a href="#">Mobile Device Reports</a> on page 155             | These reports show you summarized or detailed information about mobile devices in your network.  |
| <a href="#">WAN Reports</a> on page 156                       | These reports show information about your Frame Relay, Point to Point Serial, and other WAN connections in your network.   |
| <a href="#">LAN Reports</a> on page 156                       | These reports show information about your FDDI and Token Ring connections in your network.   |
| <a href="#">Device Reports</a> on page 156                    | These reports show inventory information.  |
| <a href="#">Remote Management Cards Reports</a> on page 157   | These reports provide information about remote management cards discovered by DDM Inventory.   |

## Report Periods

There are two types of report, summary and detail. Both report types have a different group of reporting periods.

**Table 2 Report Periods**

| Period      | Contents   | Generated                      | Summary | Detail |
|-------------|--|--------------------------------|---------|--------|
| Today       | data for today and yesterday   | each hour <sup>a</sup>         | ✓       | —      |
| Yesterday   | data for the previous 24 hours   | each day after midnight        | —       | ✓      |
| Last 7 Days | data for the previous 7 days, starting yesterday (not including today)           | each day after midnight        | ✓       | ✓      |
| Last Week   | data for the previous week (weeks begin each Monday)                             | each Monday                    | ✓       | ✓      |
| This Month  | data for the days in the current month, starting yesterday (not including today) | each day after midnight        | ✓       | —      |
| Last Month  | data for the previous calendar month   | on the first day of each month | ✓       | ✓      |

a. For a restricted period: 0600–2000 (6 AM–8 PM).

## Recognition Options in Reports

Some reports contain **[Full]**, **[Partial]**, and **[Both]** navigation links. You can select one of the links to change the recognition mode in a report:

- Full - Default mode. Shows only fully recognized applications.
- Partial - Shows only partially recognized applications. For these applications, only a partial match is found in the library, indicating that a different version of the application might be installed. The version shown is the closest one found in the Software Application Index (SAI).
- Both - Shows both fully and partially recognized applications. Refer to the **Recognition** column to differentiate between the partially and fully recognized applications.

## Finding Information in a Report

Most reports contain a Find tool that you can use to locate a particular string in a report. You specify a search string and several options to direct the search. If the search string is found, the text is highlighted and the following message is displayed:

Text found at row <n>



If the text is not found, the following message is displayed:

Text not found.

To use the Find tool in a report:

- 1 In the text box to the immediate right of the **Find** button, type the string that you want to find.
- 2 From the first drop-down menu, specify the search method. The choices are as follows:
  - contained in
  - at start of
  - at end of
  - equal to
  - match ?\*
- 3 From the second drop-down menu, specify the column that you want to search.

In some reports, you can specify **Row Number** here. In this case, the search string is a row number in the report. The row that you specify will become the first row displayed. If the row number that you specify is beyond the end of the report, the display will not change.
- 4 Specify the direction of the search by selecting either **Up** or **Down**.
- 5 *Optional:* Select **Match case** if you want to match the case specified in your search string.
- 6 *Optional:* To display only those items in the table that do NOT match your search string, select **Invert Match**.
- 7 Click **Find**.

The first match for your string and search criteria is highlighted. If you click **Find** again, the next match is highlighted.

## Executive/Summary Network Reports

Executive Summary reports are about the network as a whole. Here is one example of how you might use them—just to see what’s in your network.

To view the Executive/Summary Network Inventory Reports

- Click **Reports > Network Documentation > Device Inventory Summary**
- Or click **Reports > Network Documentation > Device Inventory**

You may have very little idea of what is actually in your network beyond the core network devices:

- There may be several people responsible for the network.
- Someone or several people may be adding equipment without informing you.
- You may be new to the job and the last person didn’t keep complete records or records you can understand.
- Some or all of the network management may have been delegated to someone outside your organization.
- You may be outside the organization whose network you must manage.

The Device Inventory Summary report tells you what is in your network, and the Device Inventory report tells you about the devices in your network in greater detail.

The following Reports are available:

| Folder                | Report                          | Type             |
|-----------------------|---------------------------------|------------------|
| Network Documentation | Network Classification          | pie graph, table |
|                       | Network Devices by Function     | pie graph, table |
|                       | End Nodes by Function           | pie graph, table |
|                       | Device Inventory Summary        | table            |
|                       | Device Inventory by Category    | table            |
|                       | Device Inventory by UNSPSC      | pie graph, table |
|                       | Device Inventory by Virtual LAN | table            |
|                       | Port Inventory by Virtual LAN   | table            |
|                       | Device Inventory                | list             |
|                       | Frame Relay PVC Inventory       | table            |
|                       | Possible Modems Report          | list             |
|                       | Under Utilized Equipment        | table            |

## Scanned Device Reports

If you use DDM Inventory to scan devices in your network, these reports provide the hardware, operating system, software application, and license information for scanned devices. Both summary and detailed reports are available. A special report indicating which devices can be upgraded to Windows Vista is also included in this category.

### Scanned Device Summaries

These reports display summary counts of the scanned devices grouped by different device properties. For example, devices at the top level may be grouped by their company division, in turn by their office location within that division, and finally by the department to which they belong.

The summary reports provide drill-down to details about the devices that belong to each summary group.



If collection of the relevant Asset Data fields is not enabled, the data will be categorized as N/A, making the reports less useful).

## Summary Report by Division, Location, Department

This report lists summary counts for all scanned devices by Division, Location, and Department.

Clicking on a summary count for a Division, Location, or Department will display a report of devices belonging to those categories summarized and sorted by any lower level categories. For example, clicking on a location count will display all devices at that location and division sorted by department.

Clicking on the Total Scanned Devices count at the bottom of the report will display a report of all scanned devices sorted by division, location, and department.

## Summary Report by Location, Division, Department

This report lists summary counts for all scanned devices by Location, Division, and Department.

Clicking on a summary count for a Location, Division, or Department will display a report of devices belonging to those categories summarized and sorted by any lower level categories. For example, clicking on a division count will display all devices at that division and location sorted by department.

Clicking on the Total Scanned Devices count at the bottom of the report will display a report of all scanned devices sorted by location, division, and department.

## Summary Report by Department, Location

This report lists summary counts for all scanned devices by Department and Location.

Clicking on a summary count for a Department or Location will display a report of devices belonging to those categories summarized and sorted by any lower level categories. For example, clicking on a department count will display all devices at that department sorted by location.

Clicking on the Total Scanned Devices count at the bottom of the report will display a report of all scanned devices sorted by department and location.

## Summary Report by Location, Building, Floor

This report lists summary counts for all scanned devices by Location, Building, and Floor.

Clicking on a summary count for a Location, Building, or Floor will display a report of devices belonging to those categories summarized and sorted by any lower level categories. For example, clicking on a building count will display all devices at that building and location sorted by floor.

Clicking on the Total Scanned Devices count at the bottom of the report will display a report of all scanned devices sorted by location, building, and floor.

## Summary Report by Location, Cost Center

This report lists summary counts for all scanned devices by Location and Cost Center.

Clicking on a summary count for a Location or Cost Center will display a report of devices belonging to those categories summarized and sorted by any lower level categories. For example, clicking on a location count will display all devices for that location sorted by cost center.

Clicking on the Total Scanned Devices count at the bottom of the report will display a report of all scanned devices sorted by location and cost center.

### Summary Report by Cost Center, Location

This report lists summary counts for all scanned devices by Cost Center and Location.

Clicking on a summary count for a Cost Center or Location will display a report of devices belonging to those categories summarized and sorted by any lower level categories. For example, clicking on a cost center count will display all devices for that cost center sorted by location.

Clicking on the Total Scanned Devices count at the bottom of the report will display a report of all scanned devices sorted by cost center and location.

### Summary Report by Operating System Category

This report lists summary counts for all scanned devices by Operating System Category.

Clicking on a summary count for an Operating System category will display a detailed report of devices belonging to that Operating System category.

Clicking on the Total Scanned Devices count at the bottom of the report will display a report of all scanned devices sorted by Operating System category.

### Summary Report by Hardware Chassis Type

This report lists summary counts for all scanned devices by hardware chassis type.

Clicking on a summary count for a chassis type will display a detailed report of devices belonging to that chassis type.

Clicking on the Total Scanned Devices count at the bottom of the report will display a report of all scanned devices sorted by hardware chassis type.

### Inventory of Scanned Devices (All Columns)

This detailed report displays hardware, operating system, software application, and license information available for each scanned device.

If you click the name of a device, the Device Manager opens.

If you click a value in any other column, more detailed information pertaining to that parameter is displayed.

### Inventory of Scanned Devices (Hardware Columns)

This detailed report displays information about the hardware features of each scanned device.

If you click the name of a device, the Device Manager opens.

If you click a value in any other column, more detailed information pertaining to that parameter is displayed.

### Inventory of Scanned Devices (Application Columns)

This detailed report displays information about the software applications found on each scanned device.

If you click the name of a device, the Device Manager opens.

If you click a value in any other column, more detailed information pertaining to that parameter is displayed.

## Software Inventory Reports

These reports display software application license and installation counts for all installed applications, including both recognized and unrecognized applications. The Application Utilization reports display utilization data, if collected, for each application.

These reports also provide links to detailed reports about the scanned devices where the individual applications are installed.

Most of these reports are based on the Application Recognition process performed by the XML Enricher. The information in the OS Reported Applications reports, however, comes from the operating systems on the scanned devices.

To ensure that the data presented is sufficiently accurate, make sure that

- Application Recognition is enabled in the XML Enricher.
- The Software Application Library used is up to date.

The Application Utilization reports are only available when the Software Utilization license is present.

## Recognized Applications

The first group of software inventory reports pertains to applications that are included in the Software Application Library and recognized by the XML Enricher.

### Licenses by Application

This summary report displays all recognized applications with the number of licenses required and installed for each application.

Click an application name to view more detailed information about that application.

### Licenses by Publisher

This summary report lists all software publishers sorted by name together with their application licenses required and installed application counts.

Clicking the publisher's name will display detailed information for all of the publisher's applications.

## Application Utilization Reports

These reports provide two types of software application utilization information:

- **Running** time indicates how long an application has been running.
- **Focus** time indicates how long an application has been running in the foreground—in other words, time when the application is in focus.

The Application Utilization reports also provide information about both running time and focus time at three levels of detail: summary, detailed, and drill-down information. The following tables show you how to access each type of report.

**Table 3 Summary Utilization Reports**

| <b>Name</b>                        | <b>Description</b>   | <b>Access From</b> | <b>Drill Down To</b>               |
|------------------------------------|--|--------------------|------------------------------------|
| Running Utilization By Application | How long each application was running over the last 31 days, 90 days, and 365 days                   | Navigation tree    | Application, version, or publisher |
| Focus Utilization By Application   | How long each application was running in the foreground over the last 31 days, 90 days, and 365 days | Navigation tree    | Application, version, or publisher |

**Table 4 Detail Utilization Reports**

| <b>Name</b>                               | <b>Description</b>   | <b>Access From</b>   | <b>Drill Down To</b> |
|---|--|--|----------------------|
| Running Utilization Details Last 31 Days  | How long each application was running over the last 31 days                        | Navigation tree or <b>[Last 31 Days]</b> link in other running utilization detail reports  | Device               |
| Running Utilization Details Last 90 Days  | How long each application was running over the last 90 days                        | Navigation tree or <b>[Last 90 Days]</b> link in other running utilization detail reports  | Device               |
| Running Utilization Details Last 365 Days | How long each application was running over the last 365 days                       | Navigation tree or <b>[Last 365 Days]</b> link in other running utilization detail reports | Device               |
| Running Utilization Details All Periods   | How long each application was running over the last 31 days, 90 days, and 365 days | Navigation tree or <b>[All Periods]</b> link in other running utilization detail reports   | Device               |
| Focus Utilization Details Last 31 Days    | How long each application was running in the foreground over the last 31 days      | Navigation tree or <b>[Last 31 Days]</b> link in other focus utilization detail reports    | Device               |

**Table 4 Detail Utilization Reports**

| <b>Name</b>                             | <b>Description</b>   | <b>Access From</b>   | <b>Drill Down To</b> |
|---|--|--|----------------------|
| Focus Utilization Details Last 90 Days  | How long each application was running in the foreground over the last 90 days                        | Navigation tree or <b>[Last 90 Days]</b> link in other focus utilization detail reports  | Device               |
| Focus Utilization Details Last 365 Days | How long each application was running in the foreground over the last 365 days                       | Navigation tree or <b>[Last 365 Days]</b> link in other focus utilization detail reports | Device               |
| Focus Utilization Details All Periods   | How long each application was running in the foreground over the last 31 days, 90 days, and 365 days | Navigation tree or <b>[All Periods]</b> link in other focus utilization detail reports   | Device               |

**Table 5 Utilization Drill-Down Reports**

| <b>Name</b>                      | <b>Description</b>   | <b>Access From</b>                                | <b>Drill Down To</b> |
|----------------------------------|--|---|----------------------|
| Device – Running                 | Running utilization information for all recognized applications on a single device         | Running utilization detail reports                | None                 |
| Device – Focus                   | Focus utilization information for all recognized applications on a single device           | Focus utilization detail reports                  | None                 |
| Application or Version – Running | Running utilization information by device for a specific application (or version)          | Running Utilization By Application summary report | Device               |
| Application or Version – Focus   | Focus utilization information by device for a specific application (or version)            | Focus Utilization By Application summary report   | Device               |
| Publisher – Running              | Running utilization information by device for all applications from a particular publisher | Running Utilization By Application summary report | Device               |
| Publisher – Focus                | Focus utilization information by device for all applications from a particular publisher   | Focus Utilization By Application summary report   | Device               |

## OS Reported Applications

The OS Reported Applications reports provide information about software applications and features that were reported by the operating system on each scanned device. These applications may or may not be included in the Software Application Library.

### OS Registered Applications – Application Summary

This report provides information about applications detected on your scanned devices that were known to the operating system.

- For Windows platforms, this is the list of installed software as reported in Control Panel > Add or Remove Programs (Programs and Features on Windows Vista and Windows Server 2008).
- For UNIX platforms, this is the list of installed software packages registered with the system's package manager.

This report is similar to the [OS Registered Applications – Publisher Summary with Drill Down](#) report, but it is organized differently. It does not offer drill-down to more detailed information.

### OS Registered Applications – Publisher Summary with Drill Down

This report provides information about applications detected on your scanned devices that were known to the operating system.

- For Windows platforms, this is the list of installed software as reported in Control Panel > Add or Remove Programs (Programs and Features on Windows Vista and Windows Server 2008).
- For UNIX platforms, this is the list of installed software packages registered with the system's package manager.

The report is organized by publisher. To view a list of applications from a particular software publisher, click that publisher's name. You can then drill down to a specific application and a specific device (asset) where that application was found.

### WMI Software Features – Application Summary

This report provides information about software features that were installed using the Microsoft installer (MSI). This information comes from the Windows Management Instrumentation (WMI) MSI provider. For Windows Server 2003, this is an optional component that is not installed by default.

This report is similar to the [WMI Software Features – Publisher Summary with Drill Down](#) report, but it is organized differently. It contains additional information about each software feature, but it does not offer drill-down to more detailed information.

### WMI Software Features – Publisher Summary with Drill Down

This report also provides information about software features that were installed using the Microsoft installer (MSI). This information comes from the Windows Management Instrumentation (WMI) MSI provider. For Windows Server 2003, this is an optional component that is not installed by default.



The report is organized by publisher. To view a list of applications and features from a particular software publisher, click that publisher's name. You can then drill down to a specific feature and a specific device (asset) where that feature was found.

## Publishers with Unidentified Applications

This report provides summary information about unrecognized files found on the scanned devices in your environment. These files are associated with software applications that are not currently included in the DDM Inventory Software Application Library.

The number of unidentified applications (and versions) found on your scanned devices for each recognized software publisher is shown. To view more detailed information about unidentified applications from a particular publisher, click the name of that publisher.

## Unrecognized Files

The unrecognized file reports display the files on your scanned devices that were not recognized as belonging to a known application.



This report is not populated unless the “Import file data” option is enabled on the **Administration > System Configuration > Scan processing** page.

Unrecognized files represent software applications that are not currently included in the DDM Inventory Software Application Library. You can add them to the library by using the Express Teaching process, the Analysis Workbench, or the SAI Editor. For more information, refer to “Application Teaching” in the *Scan Data Analysis Guide*.

## Unrecognized File Reports

These reports display the unrecognized files found on your scanned devices. Three types of reports are available:

- Unrecognized Files Summary by Scanner Platform
- Unrecognized Files with Drill Down to Directories and Devices
- Unrecognized Microsoft Windows Files with Publisher Information

From each of these reports, you can drill down to more detailed information about the individual files that were found.

### Alternate Views of Unrecognized Windows File Data

When you drill down to the Windows (x86) platform from the Unrecognized Files Summary by Scanner Platform report, you can view the detailed reports in various ways:

**Show Application Data** – shows Publisher, Application, and Version information, as well as Utilization Data, for each unrecognized file

**Show File Data** – shows File Size, File Version, and File Signature information, as well as Utilization Data, for each unrecognized file

**Show Exe Files** – shows only Windows executable files with the `.exe` file name extension

**Show All Files** – removes any filter such that all unrecognized files are listed

**Show OS Installed Applications** – shows only those applications that were installed and properly registered with the operating system

**Show Windows File Data** – turns off the Show OS Installed Applications filter or the Show WMI Software Features filter

**Show WMI Software Features** – shows information about software features for applications installed using the Microsoft installer (MSI). This information comes from the Windows Management Instrumentation (WMI) MSI provider.

If the Software Utilization license is not present, the Utilization Data columns in these detailed reports will contain zeros.

## Devices with High Risk Files

These reports display information about devices that contain the greatest number of files that are considered to be high risk. There are two types of reports in this group:

- Devices with High Risk Files Based on Frequency
- Devices with High Risk Files Based on Usage

In each case, the population of high risk files is slightly different. The first report considers the 100 unrecognized files that occur on the largest number of scanned devices. The second report considers the 100 unrecognized files with the greatest utilization (this report only contains meaningful data when the Software Utilization license is present).

The devices listed in these reports are likely to be those devices that it will be most effective to teach to reduce the total number of unrecognized files. If you click the **Export Analysis Workbench Load Script** link, a load script is created that loads the scan files for the 10 devices with the greatest number of high risk files into Analysis Workbench to begin the process of teaching.

If you click the **View the 100 Highest Risk Files** link, a list of the 100 highest risk files found on the scanned devices is displayed. If you click the value in the “# of the 100 Highest Risk Files...” column, the high risk files present on a particular device are listed.

## Virtualization Reports

The virtualization reports allow you to see information about virtual devices. The virtualization reports include reports on Solaris Zones, VMware Virtual Machines, and VMware VirtualCenter.

The Solaris Zones report provides information about the Solaris global zones and the zones that they host.

The VMware Virtual Machines report provides information about the VMware hosts and their associated Virtual Machines (VMs).

The VMware VirtualCenter report provides information about VirtualCenter management servers and the VM hosts they manage.

# Mobile Device Reports

You can create the following reports about mobile devices in your network:

| Report Name                                | Description  |
|--|--|
| Summary By Vendor, Model, Firmware Version | Device counts by vendor, model, and firmware version with drill down to device details |
| Summary By Mobile Carrier                  | Device counts by mobile carrier with drill down to device details                      |
| Locked Mobile Devices                      | Locked and/or wiped mobile device details  |

Here is an example of a Summary by Mobile Carrier report:

Report data generated: Sunday, July 29, 2007 22:50:23 Eastern Daylight Time [\[Refresh Data\]](#)

| Carrier                     | # Devices                            |
|-----------------------------|--------------------------------------|
| China Mobile                | 482 <a href="#">[Export]</a>         |
| Cingular                    | 181 <a href="#">[Export]</a>         |
| mBlox                       | 1 <a href="#">[Export]</a>           |
| T-Mobile                    | 162 <a href="#">[Export]</a>         |
| VZW/Sprint                  | 178 <a href="#">[Export]</a>         |
| [Unknown Carrier]           | 1 <a href="#">[Export]</a>           |
| <b>Total Mobile Devices</b> | <b>1005</b> <a href="#">[Export]</a> |

From any summary report, you can drill down to more detailed information about individual mobile devices:

- To view a detailed list of devices that share a particular vendor, model, firmware version, or mobile carrier, click the pertinent device count in the summary report.
- To export a detailed list of devices that share a particular vendor, model, firmware version, or mobile carrier, click the **[Export]** link for that parameter in the summary report.
- To view a detailed list of all mobile devices in your network, click the Total Mobile Devices count in the summary report.
- To open the Device Manager for a particular device, click the device title (far left column) in the detailed list.

The information contained in the detailed mobile device reports depends on the settings you have specified for mobile device discovery and inventory. Refer to “Mobile Devices in DDM Inventory” in the *Reference Guide* for more information about these settings.

## WAN Reports

Frame Relay reports, as an example, can tell you if you are getting the service you are paying for. Note, for instance, the Data Delivery Ratio Report, one of the detailed reports. The Data Delivery Ratio Report tells you which Permanent Virtual Circuits (PVCs) are dropping data and is a good guide to whether or not you are getting the Frame Relay service you are paying for and whether you could do with less.

To view a [Data Delivery Ratio Report](#):

- Click **Reports > WAN Reports > Frame Relay Service > Data Delivery Ratio**

There are two report structures for WAN Reports:

- Frame Relay folder
- all other folders

---

### Frame Relay Detail Reports

---

Inventory

---

Connected DLCI Inventory

---

### Other Detail Reports

---

Inventory

---

## LAN Reports

You can get inventory reports for your LAN backbone, FDDI, or Token Ring.

## Device Reports

Device reports give you inventory information and information about availability, throughput and utilization, broken down by category of device. They can also give you such information as what servers are using the most memory for a given time.



The Inventory report exported to a CSV file reflects the default map configuration for the current account.

All other reports reflect the Prime map configuration and its packaging.

Device Inventory reports are available for the following groupings of devices:

- Servers
- Routers
- Input and Output Devices
- Web Servers

## Remote Management Cards Reports

The Remote Management Cards reports show information about remote management cards discovered by DDM Inventory and the information about the devices which are installed with remote management cards.

To view the Remote Management Cards Reports, perform the following step:

- Click **Server > Reports > Remote Management Cards Reports > Remote Management Cards**

The Remote Management Cards report includes the following two types of reports:

- Devices with Remote Management Cards report
- Remote Management Card Summary report

The Devices with Remote Management Cards report shows the list of devices which are installed with remote management cards. Click a device link in the **Device** column to view the detailed information about the device in the **Device Manager** window (See [Using the Device Manager](#) on page 69).

The Remote Management Card Summary report shows the list of discovered remote management cards. The **Count** column displays the number of cards of each type. When you click a number in the **Count** column, you are led to the next report that shows the devices with that type of remote management card.



# Index

## A

- About
  - Line Manager panel, 114
- Administration
  - configuration files
    - change default, 46
    - copy, 45
    - delete, 45
    - rename, 46
- advanced Find, 21
- Agent Ping
  - Device Manager button, 90
- Aggregate Alarms Viewer, 59
- Aggregate Events Browser, 67
- Aggregate Health Panel, 55
- alarms, 58
- Alarms Viewer, 58
- Alarm Type panel (Port Manager), 111
- appliance access events, 66
- approximate connection, 105
- asset tag, 21
- Attribute Manager, 117
  - Configuration, 118
  - Manage, 119
- Automatic packaging
  - preferences, 39
- autosave, 44

## B

- blue line under icon, 28, 38
- Break Connection panel
  - Line Manager, 115
  - Port Manager, 110
- breaking a connection, 110

## C

- clearing the database, 81, 104
- colored ring, 24, 28

- comma separated value *see* CSV
- community strings
  - in MIB Browser, 128
- Configuration
  - Attribute Manager panel, 118
  - Device Manager panel, 72
  - Port Manager panel, 101
- configuration files, 42
- connection
  - breaking single (conceptual), 110, 115
  - forcing single new (conceptual), 109
  - types of, 105
- contact, system, 74
- Create Connection panel (Port Manager), 109
- creating a connection, 109
- CSV, 107, 156

## D

- data
  - clearing, 81, 104
- default map configuration, 42, 156
- device
  - model, 93
  - not seen, 28
- Device Manager
  - Agent Ping, 90
  - Configuration, 72
  - Diagnosis, 80
  - DNS Query, 90
  - Export (Statistics), 108
  - Graph (Statistics), 107
  - IP Ping, 88
  - Ports, 91
  - reports, 79
  - Scan Data, 92
  - SNMP Ping, 89
  - Statistics, 107 to 108
  - Table (Statistics), 108
  - Traceroute, 88
  - Update Model, 93
  - Web, 92
- Device Reports, 156, 157

- device title, 21
- Diagnosis
  - Device Manager panel, 80
  - Port Manager panel, 104
- disconnecting a port or line, 110, 115
- DNS Query button (Device Manager), 90
- domain name, 21
- Duplex Mode panel (Port Manager), 111

## E

- Easy Find, 12
- Entry, 126
- Events Browser, 61
- Executive/Summary Reports, 145
- Export
  - Device Manager Statistics button, 108
- exporting data
  - saving to text file, 59

## F

- faded icon, 28
- family, 21
- Find, 11
  - advanced, 21
  - MIB Browser, 124
  - Scan Data Viewer, 134
- Find OID, 128
- Folder tab, 126
- forcing a connection, 109
- found objects, 29

## G

- Get, 127
- Get Next, 126, 129
- Graph
  - Device Manager button, 107
- gray background
  - Manager data, 103

## H

- Hardware data
  - viewing in viewer, 135
- Health Panel, 24, 53
  - aggregator, 55
  - alarm list, 54
  - hide inactive alarms, 55

- Hide Inactive Alarms, 55
- HTTP session, 92

## I

- icons, 25
  - appearance, 28
  - blue line under icons, 28
  - faded, 28
  - found, 29
  - locked, 28
  - package, 27
  - selected, 29
  - with colored ring, 28
- Interface Rate panel (Port Manager), 110
- Interface Type panel (Port Manager), 111
- IP address
  - multiple, 79
- IP Ping
  - Device Manager button, 88

## L

- LAN Reports, 156
- Layout, 32
- line, multiple, 115
- Line Manager, 113
  - About, 114
  - Break Connection, 115
- link training, 105
- Locate
  - MIB Browser button, 125
  - Scan Data Viewer button, 134
- location, system, 74
- Lock, 28, 38
- locked objects, 28, 38
- logical subnet, 105

## M

- Manage
  - Attribute Manager button, 119



- map configuration, 42
  - change default, 46
  - copy, 45
  - default, 42
  - delete, 45
  - New, 43
  - open, 45
  - organizing, 45
  - Prime, saving, 44
  - rename, 46
  - saving, 43
  - sharing with other accounts, 46

- map scale, 24

- MIB Browser, 121

- Entry, 126
- find a device, 124
- Find OID, 128
- Folder tab, 126
- Get, 127
- Get Next, 126, 129
- locate, 125
- MIB description, 128
- MIB radar, 130
- opening, 121
- pull-down list of devices, 124
- refresh, 126
- set, 128
- tree view, 124
- Variable tab, 127
- write, 127

- model, 21

- multi-object packages, 36, 37
  - create manually, 37

- multiple IP addresses, 79

- multiple lines, 115

- My User Alarms Only, 54

## N

- name, system, 74

- negative statistics, 103

- NetBIOS name, 21

- NetBIOS workgroup, 21

- network function, 21

- Network Map

- autosave, 44
- colored ring, 28
- faded icon, 28
- icons, 25
- opening a configuration, 45
- placing an object at top, 31
- saving a map configuration, 43
- starting a configuration, 43
- Status Bar, 24

- New MIB Browser

- MIB Browser
  - New MIB Browser, 130

- not seen device, 28

## O

- objects

- placing at top of network, 31

- Open Copy of Prime, 43

- operating system, 21

## P

- Package, 37

- packaging, 27, 35

- map configuration files, 42
- multi-object packages, 37

- Pack command, 36

- ping button (Device Manager), 88

- Port Manager

- Alarm Type, 111
- Break Connection, 110
- Configuration, 101
- Create Connection, 109
- Diagnosis, 104
- Duplex Mode, 111
- Interface Rate, 110
- Interface Type, 111
- Purge Port, 109
- Reports, 103
- State, 103

- Ports panel (Device Manager), 91

- Preferences

- automatic packaging, 39

- Prime map configuration, 43

- saving, 44

- priority

- device
  - range, 27
  - reserved, 27

- Progress Bar, 24

- Promote, 32
- properties
  - object
  - priority, 27
- Purge Port (Port Manager), 109

## R

- Radar, 130
- Reports, 143
  - business
    - device, 156, 157
    - executive/summary, 145
    - LAN, 156
    - WAN, 156
  - find information, 144
  - periods, 144
- Reports (Device Manager), 79
- Reports (Port Manager), 103
- ring, colored, 28

## S

- sampling period, 109
- Save, 43
- Save as Prime, 43
- Save Table Data, 59
- Scan Data
  - Device Manager button, 92
- Scan Data Viewer, 133
  - find a device, 134
  - locate, 134
  - New Scan Data Viewer, 135
  - pull-down list of devices, 134
  - refresh, 134
- selected objects, 29
- Service Analyzer, 49
- Set, 128
- SNMP contact, 21
- SNMP description, 21
- SNMP location, 21
- SNMP name, 21
- SNMP Ping
  - Device Manager button, 89
- SNMP serial number, 21
- SNMP write by Attribute, 66
- SNMP write by MIB OID, 66
- Software Utilization, 140

- source address capture, 105
- speed, line
  - see Interface Rate
- spreadsheets, exporting to. *See* CSV
- stale data, 103
- Starting
  - Viewer, 133
- State panel
  - Port Manager, 103
- Statistics
  - Device Manager panel, 107 to 108
- Status Bar, 24
- system contact, 74
- system location, 74
- system name, 74

## T

- Table
  - Device Manager button, 108
- table-based connection, 105
- text file, saving data to, 59
- top of network, 31
- Traceroute
  - Device Manager button, 88
- traffic-based connection, 105

## U

- Unlock, 28, 38
- Unpack, 38
- Unpackage, 38
- Unpack All, 38
- Update Model button (Device Manager), 93
- Utilization, 140

## V

- Variable Tab, 127
- virtual device
  - creating, 109
- VLAN, 79

## W

- WAN Reports, 156
- Web
  - Device Manager button, 92
- Write, 127