

HP OpenView Enterprise Discovery

for the Windows[®] operating system

Software Version: 2.20

Network Data Analysis Guide

Manufacturing Part Number: None
Document Release Date: April 2007
Software Release Date: April 2007



Legal Notices

Warranty

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

The information contained herein is subject to change without notice.

Restricted Rights Legend

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

Copyright Notices

© Copyright 1993-2007 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 Sun Microsystems, Inc.

UNIX® is a registered trademark of The Open Group.

Support

You can visit the HP Software Support web site at:

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

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

- Search for knowledge documents of interest
- Submit and track support cases and enhancement requests
- Download software patches
- Manage support contracts
- Look up HP support contacts
- Review information about available services
- Enter into discussions with other software customers
- Research and register for software training

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

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

Contents

1	Introduction	9
2	Finding your Network Devices	11
	How to Find Your Devices	11
	Finding devices	12
	Easy Find	13
	Basic Match	15
	Asset Match	16
	IP Address	18
	MAC Address	19
	DNS Query	19
	Advanced Find	20
3	Using the Network Map	21
	How does the map work?	22
	Status Bar	22
	What are the icons on the map?	23
	Devices and Packages	23
	Connector Devices	24
	The priority	25
	Package icons group other icons together	25
	Icon Appearance	26
	Customizing Your View of the Network Map	27
	Changing Map User Preferences	28
	Changing the map background image	31
	Managing your background image library	32
	Packaging Your Network	32
	How packaging works	33
	You can request the creation of packages	34
	You can create your own packages	34
	You can also unpack your packages	35
	Locked objects	36
	Changing the automatic packaging preferences	36
	Organizing Map Configuration Files	39
	What is a Map Configuration?	40
	The Prime configuration	40
	Saving your changes	40
	Starting a map configuration	41
	Saving a map configuration file	41

Saving the Prime map configuration	42
Opening a saved map configuration file	43
Managing map configuration files	43
Saving a map window as a graphic file	45
4 Using the Service Analyzer	47
Choosing Your Path	47
The Service Analyzer Window	48
5 Using the Health Panel and Alarms Viewer	51
See a network overview with the Health Panel	51
Customizing the Alarm List	52
Using the Aggregate Health Panel	53
Servers button	53
Using the Alarms Viewer	54
Using the Aggregate Alarms Viewer	55
Saving data to a text file	55
6 Using the Events Browser	57
Opening the Events Browser	57
Network Events	58
Access Events	59
Toolbar	63
The Aggregate Events Browser	63
7 Using the Device Manager	65
List of Device Manager Panels	66
Configuration	68
Reports	73
Diagnosis	74
Diagnostic Information	74
Agent Deployment Log	80
Scanner Deployment Log	80
Virtualization Log	80
IP Ping	80
Traceroute	80
SNMP Ping	82
Agent Ping	82
DNS Query	82
Ports	83
View Scan Data	83
Web	84
Update Model (<i>Administrator or IT Manager</i>)	84
Special Note about the Query Network Panel	86
8 Using the Port Manager	89
List of Port Manager Panels	89
Configuration	91

State	93
Reports	93
Diagnosis	94
Statistics	97
Purge Port.	99
Create Connection (Administrator or IT Manager)	99
Break Connection (Administrator or IT Manager)	100
Port Properties	100
9 Using the Line Manager	103
Single Line Manager	103
List of Line Manager Panels	104
About.	104
Break Connection (<i>Administrator or IT Manager</i>)	105
Multiple Line Manager	105
10 Using the Attribute Manager	107
List of Attribute Manager Panels	107
Configuration	108
Manage (<i>Administrator or IT Manager</i>).	109
Purge Attribute (<i>Administrator or IT Manager</i>)	110
11 Using the MIB Browser	111
Opening the MIB Browser.	111
Parts of the MIB Browser	112
Tree View.	113
Pull-down list of Devices	113
Find Function	114
Credentials Function	114
Locate on Map.	114
Get Next	115
Refresh.	115
Folder Tab	115
Variable Tab	116
MIB Description	117
Read and Write Credentials	117
Walking the MIB	118
Using Multiple MIB Browser Sessions.	119
Watching an OID with MIB Radar	119
Saving MIB Data as a Text file	119
Save Table Data	120
MIB Walk	120
12 Using the Scan Data Viewer	121
Opening the Scan Data Viewer	121
Parts of the Scan Data Viewer	122
Pull-down list of Devices	122

Find Function	122
Locate on Map	122
Refresh.	122
Using Multiple Scan Data Viewer Sessions	122
Menu commands	123
Viewing Hardware and Configuration Data.	123
Hardware and Configuration Data Page Overview	123
The Hardware and Configuration Tab Page Layout	124
Viewing Software Application Data	125
Information shown in the Application data window.	126
Software Utilization.	127
13 Using the Reports	129
Report periods	130
Executive/Summary Network Reports	130
Scanned Device Reports	132
Scanned Device Summaries	132
Application Reports	133
Unrecognized Files	134
Microsoft Windows Vista Readiness Reports	135
WAN Reports	136
LAN Reports.	137
Device Reports	137
Index	139

1 Introduction

Welcome to the *Network Data Analysis Guide*.

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

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

This guide provides information on the following topics:

- [Finding your Network Devices](#) on page 11
- [Using the Network Map](#) on page 21
- [Using the Service Analyzer](#) on page 47
- [Using the Health Panel and Alarms Viewer](#) on page 51
- [Using the Events Browser](#) on page 57
- [Using the Device Manager](#) on page 65
- [Using the Port Manager](#) on page 89
- [Using the Attribute Manager](#) on page 107
- [Using the MIB Browser](#) on page 111
- [Using the Scan Data Viewer](#) on page 121
- [Using the Reports](#) on page 129

2 Finding your 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 Enterprise Discovery servers. The Aggregate Find is almost identical to the regular Find, but the Aggregate Find has fewer search options.

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 Easy Find on page 13. Note: Not available with Aggregator Find.
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.
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. 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	Tools > Find

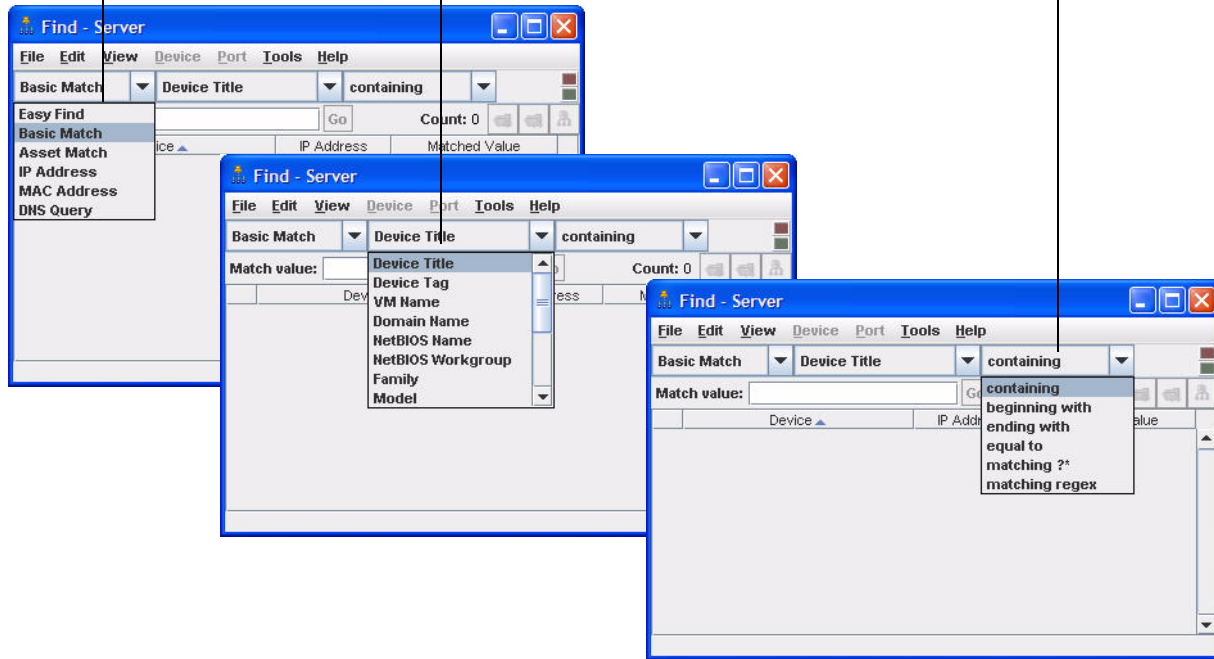
- 2 By default, you can use the **Easy Find** feature (go to [step 6](#)). If you want to do a more advanced find, continue with the next step in this procedure.
- 3 In the first pull-down list, select the Find mode you want to use to perform the search (for example, “Asset Match”).
- 4 In the second 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 20).
- 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 Enterprise Discovery database.
- 7 Press **Enter** or click **Go**.

Enterprise Discovery 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



Easy Find

When you enter text into the Find box, Enterprise Discovery searches the network in the following order.

- ▶ If there is no result at one stage, Enterprise Discovery will try the next.

Example: Once an IP address has been found, Enterprise Discovery 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 Enterprise Discovery server.
MAC address	Enterprise Discovery will try to search based on the known MAC address. Note: To find a specific device, you must enter its complete MAC address in one of these formats: 12:AB:34:CD:56:EF or 12AB34CD56EF .
IPv4 or IPv6 address	Enterprise Discovery will try to search based on the known IP address (IPv4 or IPv6). Note: To find a specific device, you must enter its complete IP address.
Domain Name	Enterprise Discovery searches based on the DNS suffix as configured in your server DNS (done in Control Panel).
Device Title	Enterprise Discovery will then search the network based on your device title preferences from Administration > System Configuration > Display preferences > Device title preference . Only the selected titles are searched.
Asset Tag	Even if Asset Tag is not listed in your Device title preference, Enterprise Discovery will search for it next.
NetBIOS Name	Even if NetBIOS name is not listed in your Device title preference, Enterprise Discovery will search for it next.



Multiple results are based only on the device title. Example: If you enter “192.168.2.”, you will not find all devices 192.168.2.0–192.168.2.255. You will only find devices with “192.168.2.” in the title. If the device with IP address 198.168.2.55 takes its title from its domain name, that device will not be found.



When using the Easy Find, it may take several seconds to get a response, especially on a large network.

Basic Match

Table 4 Basic Match

Name	Why use it?	Examples
Device Title	Find a device when you know the name, but not necessarily the type of device.	172.22.5.5 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. 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 hp.com
NetBIOS Name	Find a device with a specific NetBIOS name.	NT4WORKQA mymachine
NetBIOS Workgroup	Find a device within a specific NetBIOS workgroup.	QA_SAN_DIEGO ACTIVE
Family	Find a device within a specific family.	Cisco 2600 Series Modular Access Routers WaveSwitch 1000 Series Workgroup Switch
Model	Find a device of a specific model.	IBM xSeries 330 (867411X) Cisco Intelligent Gigabit Ethernet Switch Module (IGESM)
Operating System	Find a device with a specific operating system.	Linux 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 3Com SuperStack II
SNMP Contact	Find a device with a specific contact in the SNMP MIB.	Kevin IT Manager

Table 4 Basic Match

Name	Why use it?	Examples
SNMP Name	Find a device with a specific name in the SNMP MIB.	Demo Server manager.example.com
SNMP Location	Find a device with a specific location in the SNMP MIB.	server room QA LAB
SNMP Serial Number	Find a device with a specific serial number in the SNMP MIB.	12345ABCDE

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, 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

Name	Why use it?	Examples
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. You can also enter a partial asset tag to find several devices with similar numbers.	EXAMPLE123456 123456
Employee ID	Find devices from a specific Employee ID as used in the organization.	FINANCE3746

Table 5 Asset Match

Name	Why use it?	Examples
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	
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

Table 5 Asset Match

Name	Why use it?	Examples
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. When the field is configured in the User Interface, the field is given a meaningful name. The user defined fields will show in the Asset Match list only if a custom label is being used for a field.	

IP Address

Table 6 IP Address

Name	Why use it?	Examples
IP Address	Find a device with a specific IP address. Note: You must enter a complete IP address. You can use asterisks (*) to find multiple devices.	172.22.5.5 172.*.*.255

This works only for IP address and MAC address searches. You must enter an entire IP or MAC address in these formats:

- IP - 123.123.123.123
- MAC - 12:AB:34:CD:56:EF

Note: You can substitute a * for an octet in an IP address octet or a segment of a MAC address. For example: “123.*.123.123” or 12:AB:*.CD:56:EF

Note: For MAC addresses, you can compress the zeros in each segment. For example, you can enter “5” instead of “05” for a segment.

Note: If an IP or MAC address is associated with a port, you will see a port listed in your Find results.

MAC Address

Table 7 MAC Address

Name	Why use it?	Examples
MAC Address	Find a device with a specific MAC address. Note: You must enter a complete MAC address. You can use asterisks (*) to find multiple devices.	12:AB:34:CD:56:EF 12:*.34:*.56:EF 12AB34CD56EF

This works only for IP address and MAC address searches. You must enter an entire IP or MAC address in these formats:

- IP - 123.123.123.123
- MAC - 12:AB:34:CD:56:EF

Note: You can substitute a * for an octet in an IP address octet or a segment of a MAC address. For example: “123.*.123.123” or 12:AB:*.CD:56:EF

Note: For MAC addresses, you can compress the zeros in each segment. For example, you can enter “5” instead of “05” for a segment.

Note: If an IP or MAC address is associated with a port, you will see a port listed in your Find results.

DNS Query

Table 8 DNS Query

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

Advanced Find

For each advanced find option described above, 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">• “?” can represent any single character. For example, “gr?y” finds “gray” and “grey.”• “*” can find multiple characters. For example, “E*t” finds “Ethernet.”
matching regex	Matching a regular expression. 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 Enterprise Discovery 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.

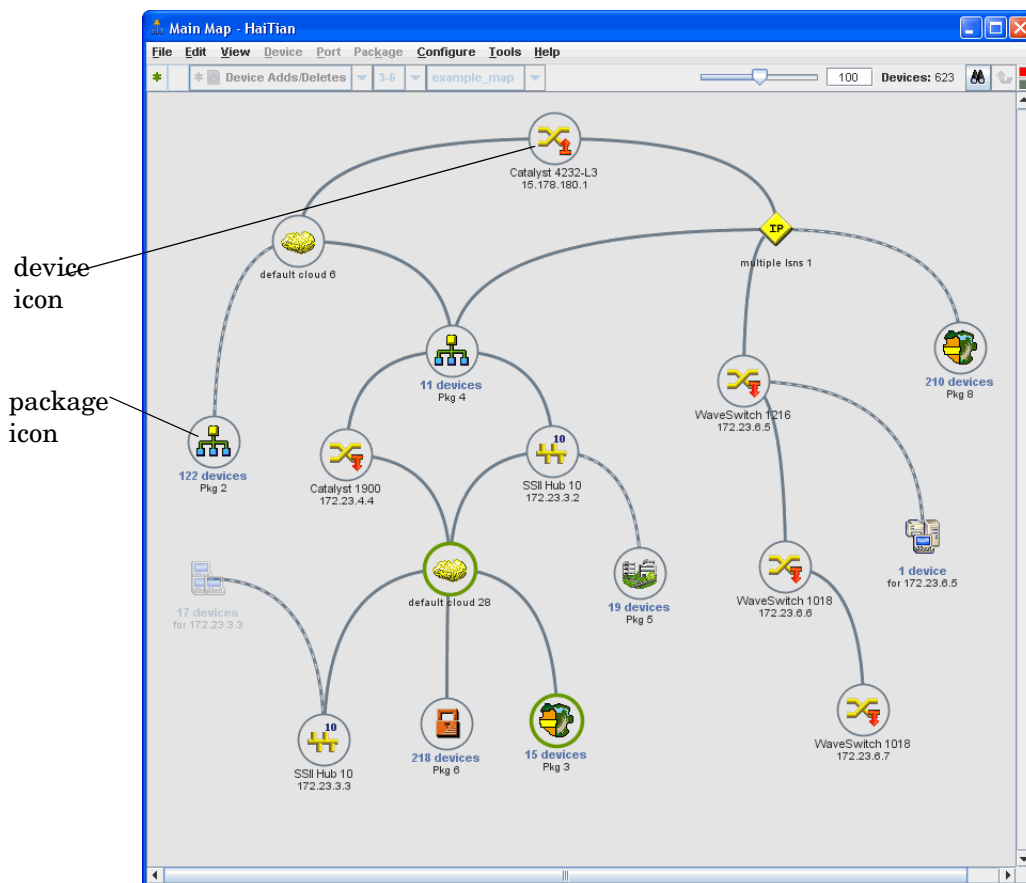


The map is generated automatically based on the data gathered through the discovery process. If the source data is reliable, the map will accurately represent your network. There may be cases where information is not available for certain devices or connections. In these cases, Enterprise Discovery will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

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

- [How does the map work?](#) on page 22
- [What are the icons on the map?](#) on page 23
- [Customizing Your View of the Network Map](#) on page 27
- [Changing the map background image](#) on page 31
- [Managing your background image library](#) on page 32
- [Packaging Your Network](#) on page 32
- [Organizing Map Configuration Files](#) on page 39
- [Saving a map window as a graphic file](#) on page 45

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.

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.

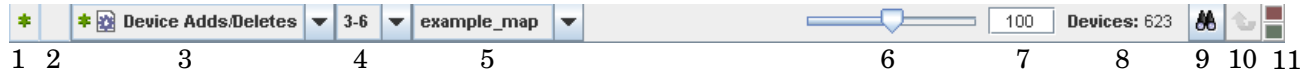


Table 1 Toolbar Legend

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?

Devices and Packages

Enterprise Discovery 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	 Win XP Pro win.example.com	Device icons represent the physical equipment in your network.
Package Icons	 2 devices for 172.23.4.4	A package is a collection of objects (objects means either devices or packages).

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





Enterprise Discovery will usually select the correct device icon. If for some reason, the wrong icon has been selected, you can change it. See [Customizing Your View of the Network Map](#) on page 27.

Connector Devices

When Enterprise Discovery 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.

Enterprise Discovery creates two types of connector devices: clouds and diamonds.

Table 3 Connector Devices

Icon Type	Example	Description
Cloud		Clouds represent one or more devices or MAC systems that provide connectivity in the network.
Diamond		Diamonds do not represent actual network devices; they indicate connectivity. Sometimes, Enterprise Discovery 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 Enterprise Discovery in **Help > Classifications > Device Types/Package Types**.

The priority



In Enterprise Discovery, 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

Enterprise Discovery 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 Enterprise Discovery. For more information on packaging, see Packaging Your Network on page 32.	
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 Packaging Your Network on page 32.	

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 32.

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>Normal Icon</p> <p>This is how a device icon will appear when:</p> <ul style="list-style-type: none"> • no alarms are selected • an alarm has been selected but that type of alarm does not apply to this device • an alarm has been selected but this device is not in the priority range
	<p>Colored Ring</p> <p>A thin gray ring will appear around a device when:</p> <ul style="list-style-type: none"> • this device is in the priority range • this device is not alarmed <p>A colored ring will appear around a device when:</p> <ul style="list-style-type: none"> • an alarm is selected that exists on this device • this device is in the priority range
	<p>Faded Icon</p> <p>If an object appears faded, that means Enterprise Discovery has not seen that device for more than 24 hours. Enterprise Discovery will eventually deactivate such a device from the Network Map and, eventually, Enterprise Discovery will purge the device and all its associated data.</p>
	<p>Locked Icons</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 Edit > User Preferences. The blue line indicates that the device has been manually packaged by a user, meaning it has been put inside a package (Package command), promoted from a package (Promote), or has had its package removed (Unpackage).</p> <p>Enterprise Discovery does create some automatic packages. They are created during discovery and whenever you use the Pack or the Unpack All commands.</p> <p>For more information on packaging, see Packaging Your Network on page 32.</p>

Table 5 Icon Appearance

Appearance	What it means
	<p>Selected Icon</p> <p>If you select an icon on the Network Map, it will appear dark.</p>
	<p>Found Icon</p> <p>This icon was located on the Network Map using the Locate feature.</p> <p>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.</p>
	<p>Deactivated or Hidden Icon</p> <p>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.</p>

Customizing Your View of the Network Map

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

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

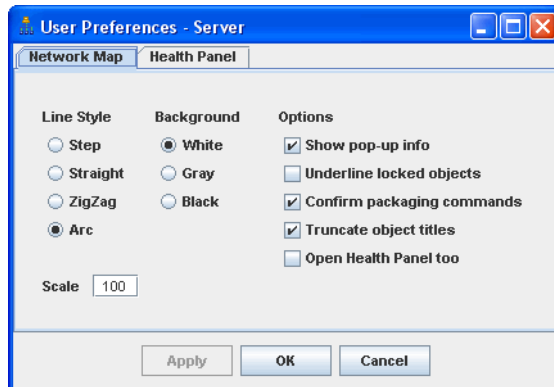


Table 6 Map Preferences

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. Typically, objects acquire locked status when they are packaged by a user. When an object is locked, Enterprise Discovery 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 Layout , Make Top of the Network , Unpackage , Pack , Unpack , and Unpack All . 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 Enterprise Discovery 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. 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. You can also use the Zoom In and Zoom Out 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 Network Map . 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.

Enterprise Discovery 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 Enterprise Discovery:

- 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 Enterprise Discovery.

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**.

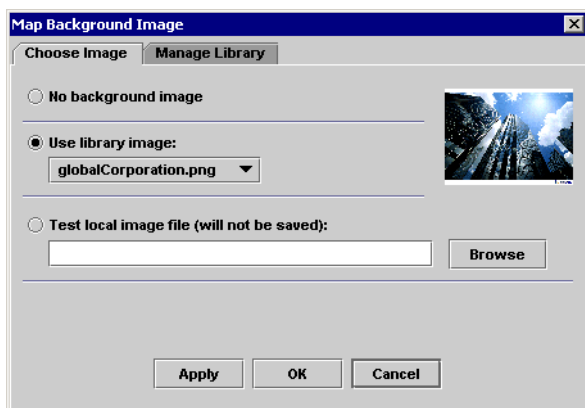
A warning dialog appears.

- 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 32).



To test an image file from your computer:

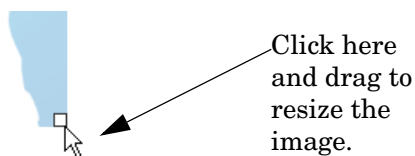
- 1 Click **Configure > Background Image**.
The Map Background Image dialog appears.
- 2 Select **Test Local Image File** and browse to find the file you want.
- 3 Click **Apply**.

▶ 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

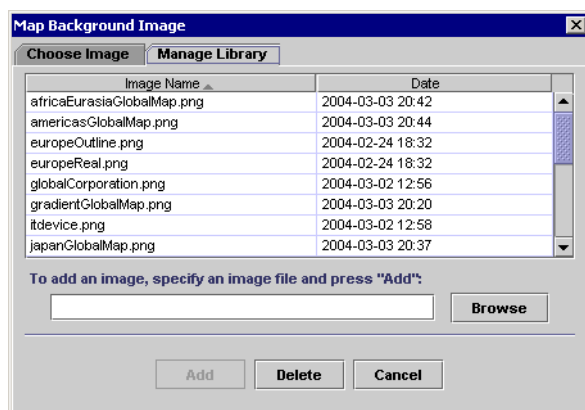
An Administrator or IT Manager account can add and delete images from the Enterprise Discovery image library. These images are available to every user, regardless of account type.



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, Enterprise Discovery 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.

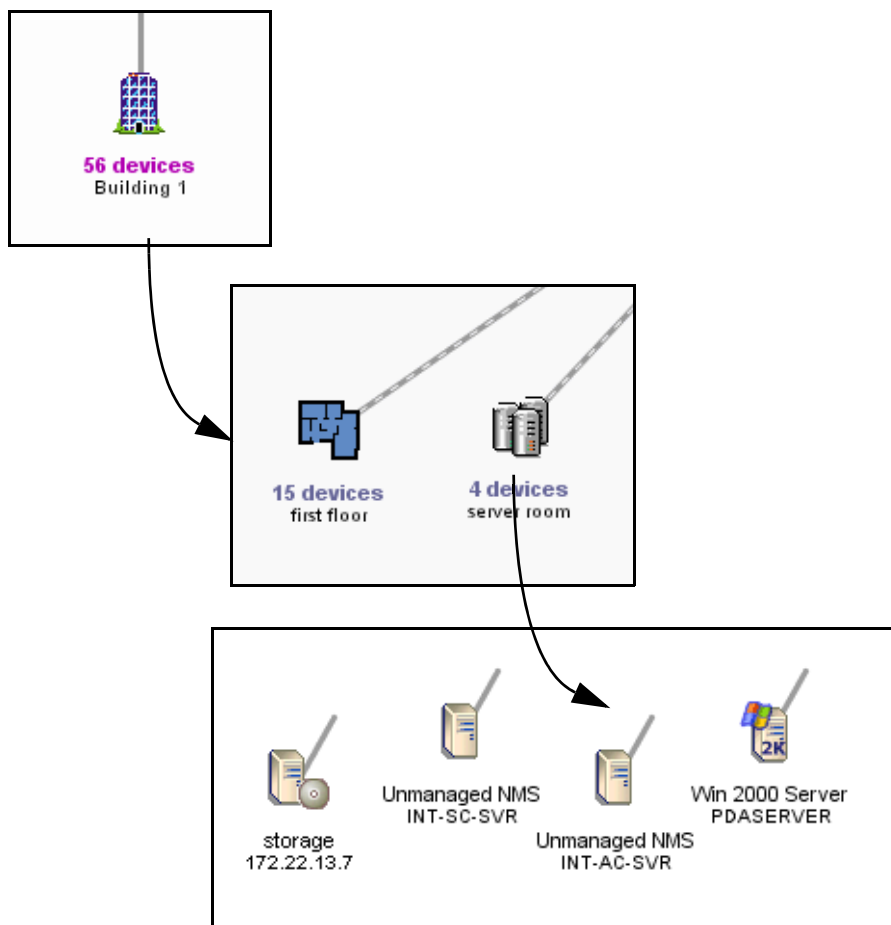
How packaging works

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 Enterprise Discovery 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.



You can request the creation of packages

Enterprise Discovery can create packages for you. This is a quick way to reduce the size of the Network Map. Enterprise Discovery 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 Enterprise Discovery create your multi-object packages for you:

- 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. Enterprise Discovery 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, Enterprise Discovery will recreate all of the automatic packages.

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, Enterprise Discovery places them without moving any of the other icons.
- If the package is in "auto-layout" mode: when adding new devices, Enterprise Discovery 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**.

You can also 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.

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.

Enterprise Discovery creates some automatic packages. Whenever you use the **Pack** or the **Unpack All** commands, Enterprise Discovery 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 Enterprise Discovery would not naturally have chosen—will have a blue line beneath it to indicate that it is locked.

Changing 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)

Enterprise Discovery 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). Enterprise Discovery automatically packages the devices associated with that connectivity device.

- ▶ Enterprise Discovery usually treats a telephone as an end-node, but it may see it as a connectivity device.

By default, whenever Enterprise Discovery 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 Enterprise Discovery 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:



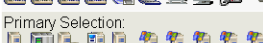



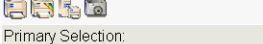

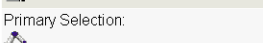

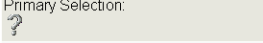



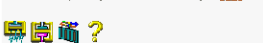

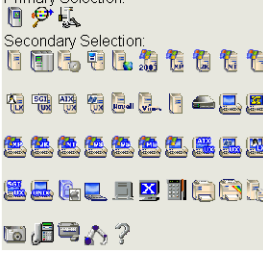
- Workstations
- Servers
- Printers
- POS/ATM
- Controllers
- Unknown
- Network Devices
- End Nodes

- ▶ 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: 	Workstations		On	3
Primary Selection: 	Servers		On	3
Primary Selection: 	Printers		On	3
Primary Selection: 	POS/ATM		On	3
Primary Selection: 	Controllers		On	3
Primary Selection: 	Unknown		On	3
Primary Selection: 	Network Devices		On	10
Primary Selection: 	End Nodes		On	2
Secondary Selection: 				

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.**

To restore the default settings, click **Restore Default.**

A few 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

Enterprise Discovery 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\Peregrine\Enterprise Discovery\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.

What is a Map Configuration?

Enterprise Discovery 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 Enterprise Discovery 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, Enterprise Discovery takes note of what map configuration file is in use. The next time you start a map session, Enterprise Discovery 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.

The 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 Enterprise Discovery, 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**.

Autosave

Enterprise Discovery provides an autosave capability for recovery purposes by saving the “current” configuration to a recovery file. Enterprise Discovery 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 Enterprise Discovery 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 is for any accounts, except demo. The demo account cannot perform any administration functions. The other three types of accounts can:

- 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.

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

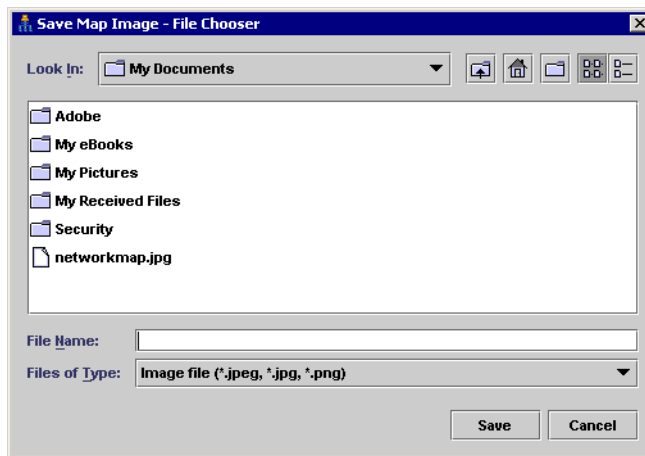
You can save any map window (the main map, or any package) as an image file (either jpg or png).

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 Enterprise Discovery 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.

Choosing Your Path

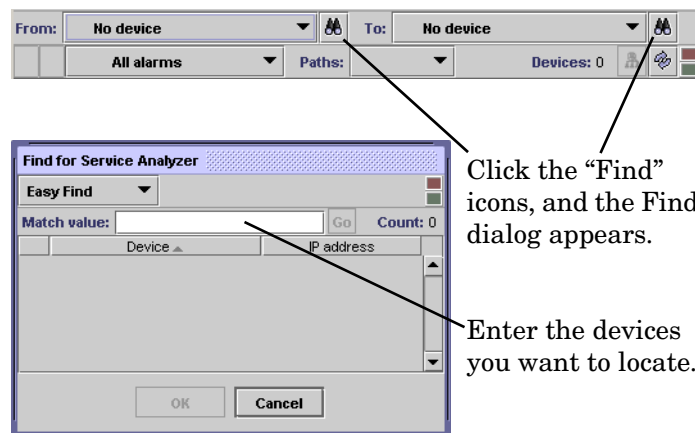
The toolbar contains two search boxes: **From** and **To**. Each box searches for a device based on its name, title, or address. This Find window works exactly the same way as the global Find feature. For more information, see [Finding your Network Devices](#) on page 11.

To use the Service Analyzer:

- 1 From the Enterprise Discovery 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.

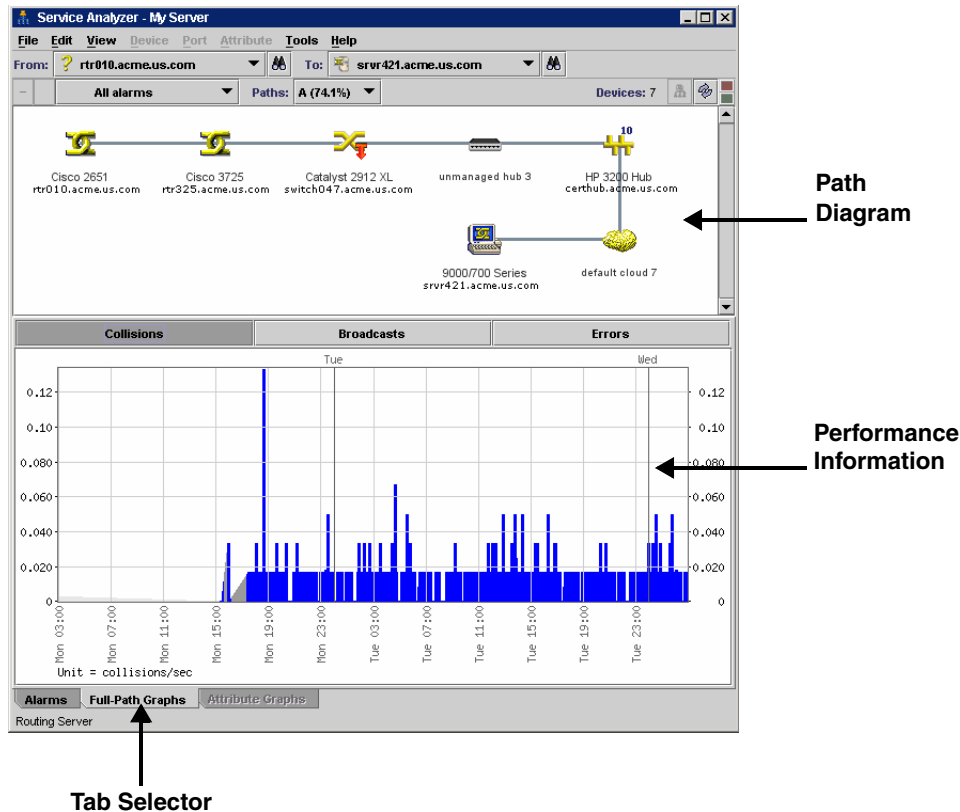


It is important to fill in the device on the left first. Changing the device on the left side will automatically clear the device on the right side.

The Service Analyzer Window

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**

Alarm Category	Notes
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.

Alarms Tab

This tab is not available in Enterprise Discovery version 2.20.

Attribute Graphs Tab

This tab is not available in Enterprise Discovery version 2.20.

5 Using the Health Panel and Alarms Viewer

There are many ways to look at your device data with Enterprise Discovery. The Health Panel and the Alarms Viewer allow 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.

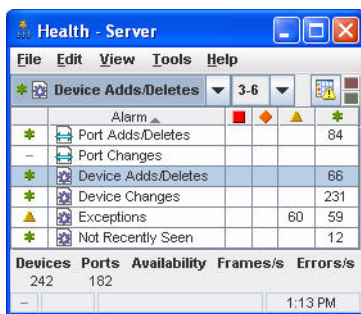
The Alarms Viewer shows all the devices on the network with current alarms. From the Alarms Viewer, you can open up a Device Manager, Port Manager, or Attribute Manager.

Topics in this chapter include:

- [See a network overview with the Health Panel](#) on page 51
- [Using the Aggregate Health Panel](#) on page 53
- [Using the Alarms Viewer](#) on page 54
- [Using the Aggregate Alarms Viewer](#) on page 55
- [Saving data to a text file](#) on page 55

See a network overview with the Health Panel





The Health Panel enables you to set up, highlight, and examine conditions, alarms, and statistics that Enterprise Discovery has gathered about your devices.



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.



The Aggregate Health Panel works the same way as the normal Health Panel, but it shows information for all the Enterprise Discovery servers in your network. For more information, see [Using the Aggregate Alarms Viewer](#) on page 55.

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 Alarm List

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 Enterprise Discovery 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're 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.

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 Enterprise Discovery servers.

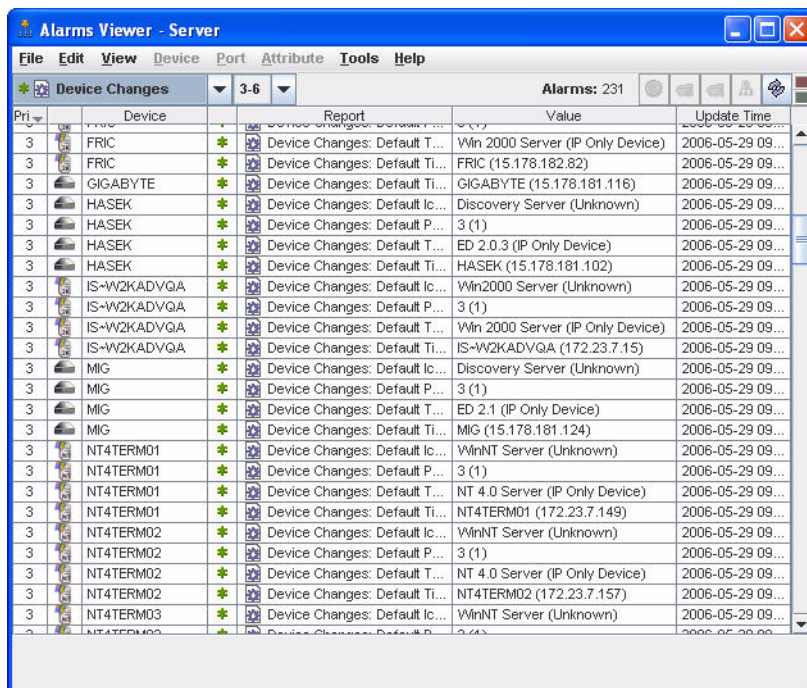
By clicking on any of the server hyperlinks on this page, you can see the **server Health** page for that Enterprise Discovery server.

- ▶ The local Enterprise Discovery server is always at the top of the list with an asterisk (*).

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' and '3-6'. 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. The 'Device' column lists various devices like FRIC, GIGABYTE, HASEK, IS-W2KADVGA, MIG, and NT4TERM01-03. The 'Report' column shows 'Device Changes: Default Ti...'. The 'Value' column shows details like 'Win 2000 Server (IP Only Device)', 'FRIC (15.178.182.82)', 'GIGABYTE (15.178.181.116)', 'Discovery Server (Unknown)', 'ED 2.0.3 (IP Only Device)', 'HASEK (15.178.181.102)', 'Win2000 Server (Unknown)', 'IS-W2KADVGA (172.23.7.15)', 'MIG (15.178.181.124)', 'WinNT Server (Unknown)', 'NT 4.0 Server (IP Only Device)', and 'NT4TERM01 (172.23.7.149)'. The 'Update Time' column shows dates like '2006-05-29 09...'. A status bar at the bottom of the window is empty.

Pri	Device	Report	Value	Update Time
3	FRIC	Device Changes: Default Ti...	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-W2KADVGA	Device Changes: Default Ic...	Win2000 Server (Unknown)	2006-05-29 09...
3	IS-W2KADVGA	Device Changes: Default P...	3 (1)	2006-05-29 09...
3	IS-W2KADVGA	Device Changes: Default T...	Win 2000 Server (IP Only Device)	2006-05-29 09...
3	IS-W2KADVGA	Device Changes: Default Ti...	IS-W2KADVGA (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...

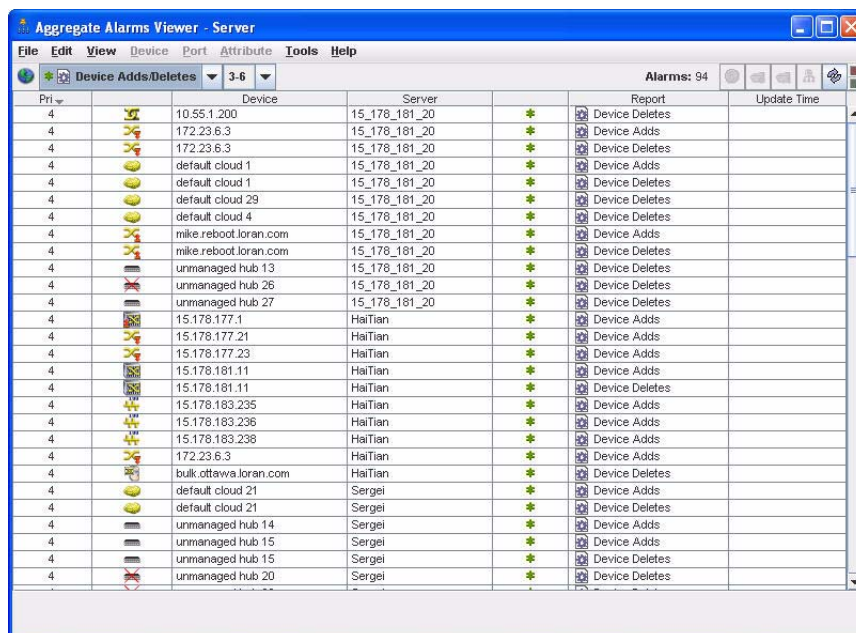
The status bar in the Alarms Viewer is similar to that on the Health Panel. You can change the displayed alarm type or priority with the pull-down lists on either window. Your selection will appear in the Health Panel and the Alarms Viewer.



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.



The screenshot shows the 'Aggregate Alarms Viewer - Server' window. The window title is 'Aggregate Alarms Viewer - Server'. The menu bar includes 'File', 'Edit', 'View', 'Device', 'Port', 'Attribute', 'Tools', and 'Help'. Below the menu bar, there is a toolbar with icons for 'Device Adds/Deletes' and a dropdown menu showing '3-6'. On the right side of the toolbar, it says 'Alarms: 94'. The main area is a table with the following columns: 'Pri', 'Device', 'Server', 'Report', and 'Update Time'. The table contains 24 rows of data, each representing an alarm event. The 'Report' column contains values like 'Device Deletes' and 'Device Adds'. The 'Update Time' column is currently empty.

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 Enterprise Discovery 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.

Saving 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.

Saving 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**.

6 Using the Events Browser

Enterprise Discovery 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 Enterprise Discovery 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, Enterprise Discovery 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).

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 ^a
Port	Port number (will not appear if a device alarm is selected)
Alarm type	Alarm type icon
Attribute	Name of the alarm
Value ^b	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

Data	Explanation
Event time	the time of the access event
Account name	the user accessing Enterprise Discovery

Table 2 Server Access Events

Data	Explanation
From IP	the IP address from which the user accessed Enterprise Discovery
Access point	the part of Enterprise Discovery accessed by the user: <ul style="list-style-type: none"> • MIB Browser – the user has accessed the MIB Browser. • Network Map – the user has accessed the Network Map. • HTTP – the user has successfully logged into Enterprise Discovery • Telnet Proxy – the first time this account has logged into a remote appliance through the aggregator. • HTTP Proxy – the first time this account has logged into a remote appliance through the aggregator. • MIB Browser Proxy – the first time this account has opened a MIB Browser session on a remote appliance through the aggregator. • Network Map Proxy – the first time this account has opened a Network Map session on a remote appliance through the aggregator.
Access status	whether or not the user was able to access Enterprise Discovery: <ul style="list-style-type: none"> • Connect – the user has connected to Enterprise Discovery, and disconnected without attempting to login. • Login OK – the user has successfully logged in to Enterprise Discovery. • Login fail – the user has attempted to login, and did not have the correct password. • Logout – the user has logged out of Enterprise Discovery.^a • Login disabled – the user has tried to login with a failed password too many times (limit has been set in Administration > System Configuration > Appliance passwords) • Login no permission – this account has been denied permission to access Enterprise Discovery.

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

Data	Explanation
Event time	the time of the access event
Account name	the user accessing Enterprise Discovery
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)

Table 3 SNMP Write Events

Data	Explanation
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"> • Write OK • 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.

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

Table 4 Add/Delete Events

Data	Explanation
Event Time	the time of the access event
Account name	the user accessing Enterprise Discovery
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

Data	Explanation
Event Time	the time of the access event
Account name	the user accessing Enterprise Discovery
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

Table 5 Change Events

Data	Explanation
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

Data	Explanation
Event Time	the time of the access event
Account Name	the user accessing Enterprise Discovery
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
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**.

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

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.

7 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 Enterprise Discovery to update the device model.









To open the Device Manager:









Table 1 Opening Device Manager




From	Open by...
Health Panel, Alarms Viewer, Events Browser, Network Map, Service Analyzer, Scan Viewer	Click Tools > Find (Ctrl - F). Enter a device address or title, then click Find .
Alarms Viewer, Events Browser	Double-click on a table row, or right-click on the device icon, title, or IP address.
Find	Enter a device address or title, then click Find .
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 Object > Open Device .

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. For more information, see page 68 .
	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). For more information, see page 73 .
	Diagnosis	This panel displays information about the current state of the device that can be helpful in diagnosing problems. For more information, see page 74 .
	Ports	This panel lists ports for this device and summarizes the information available for them. Displays 24 ports at a time (by default, you can change this in Administration > Account administration > Account properties). For more information, see page 83 .
	Events	This button opens the Events Browser with this device in context. For more information, see Using the Events Browser on page 57 .
	Locate	This button highlights in a map window the location of the device. 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. 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.
	Manage	This button launches an element manager of your choice. The URL or application must be defined in Administration > System Configuration > Element management . If not, this button is dimmed. Note: for Aggregator—Definitions for Element management are supplied from the Aggregator server, not the remote server.

Icon	Name	Description
	Browse MIB	This button opens the MIB Browser to allow the user to view the device's SNMP MIB. 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 Enterprise Discovery Viewers to show information about the device collected by Enterprise Discovery scanners. For more information, see page 83 .
	Web	This button attempts to open a web browser window for the device. For more information, see page 84 . 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. Note: The device must have an IP address. If not, this button is dimmed. Note: The device must support Telnet sessions. (Enterprise Discovery does not check before attempting a connection.)
	Update Model (Administrator or IT Manager)	This panel gives several options for updating the device information in the Discovery database. For more information, see page 84 .
	Device Visibility (Administrator or IT Manager)	This panel gives you options to activate, deactivate, hide, or purge devices on this panel. For information on how to activate, deactivate, hide, or purge devices, see the <i>Configuration and Customization Guide</i> .
	Properties	This button allows you to change the icon and name of a device in your network. For instructions on how to use this feature, see the <i>Configuration and Customization Guide</i> .
	Asset Questionnaire	This button opens up an Asset Questionnaire for this device. For more information on how to create and use this feature, see the <i>Installation and Initial Configuration Guide</i> .

Icon	Name	Description
	Refresh	This button refreshes the contents of the panel. When used with IP Ping and SNMP Ping panels, uses the last entered value instead of prompting you for a value. Note: Does not re-read the data in the panel from the network. Re-reads the data only from the Enterprise Discovery database. 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.

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 Enterprise Discovery database.

This panel is divided into the following principal sections:

- Identity table (real devices only)
- Virtual Devices (host devices only)
- Asset Data table
- SNMP Configuration
- VMware Credentials (VMware hosts only)
- Device structure (Serial number and description, disk, CPU, memory)
- Address table (real devices only)
- Virtual LANs

Identity table

As shown in [Table 2](#) on page 69, the information in the Identity table can come from these sources: the Enterprise Discovery 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 Enterprise Discovery server than for any other device.



All these elements are optional.

Table 2 Identity Table

Data	Example	Creator	Administrator or IT Manager
Package ^a	Main Map	Enterprise Discovery/ account	—
UNSPSC	Computer Servers	Rulebase	—
Family	Cisco 2600 Series Modular Access Routers	Rulebase	—
Family current manufacturer	Cisco Systems Inc	Rulebase	—
Model	Cisco 2621XM Modular Access router	Rulebase	—
Model current manufacturer	Cisco Systems Inc	Rulebase	—
Model historical manufacturer ^b	Cisco Systems Inc	Rulebase	—
Operating system	Cisco IOS Version 12.2 (8) T5	Rulebase	—
Operating system current manufacturer	Cisco Systems Inc	Rulebase	—
Operating system historical manufacturer	Cisco Systems Inc	Rulebase	—
Network Function	—	Rulebase	—
Network Function current manufacturer	—	Rulebase	—
Network Function historical manufacturer	—	Rulebase	—
Operating system	Linux	Enterprise Discovery	—
Service pack	—	Enterprise Discovery	—
NetBIOS name (network)	DUPONT	device owner	—
NetBIOS workgroup	MARKETING	device owner	—
rulebase extra info	—	Enterprise Discovery Rulebase	—
Device-specific title	—	scripts	—
System OID	.1.3.6.1.4.1.295.5.1.1.2	manufacturer	—

Table 2 Identity Table

Data	Example	Creator	Administrator or IT Manager
System OID manufacturer	PlainTree Systems Inc	Rulebase	—
System description	Ethernet Switch	manufacturer	—
System contact	test@example.com	device owner	set ^c link
System name	ws1216-2	device owner	set ^c link
System location	Server Room	device owner	set ^c link
Asset tag	78LL996	Scanner	—
BIOS asset tag	—	Scanner	—
BIOS product name	eserver xSeries 330 -[867441X]-	Scanner	—
BIOS product manufacturer	IBM	Scanner	—
BIOS serial number	78LL996	Scanner	—
BIOS chassis	—	Scanner	—
CPU	Pentium III 1133 MHz (Genuine Intel)	Scanner	—
NetBIOS name (scan) ^{d, e}	DUPONT	device owner	—
Memory (MB)	1024	Scanner	—
Windows/NIS domain	MARKETING	Scanner	—

- a. This is optional if you have not opened a map configuration since this object was discovered.
- b. Appears only when different from the current manufacturer.
- c. A shortcut to the MIB Browser.
- d. On Windows workstations, frequently the same as the system name.
- e. NetBIOS data is blank unless the device has an IP address.

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

This table lists the virtual devices that are associated with this host. For each device listed, the following items are shown.

- Device: Logical machine name and IP address of the virtual device
- VM Type: Virtual device type (VMware or Solaris zone)
- 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 Enterprise Discovery last collected information about this device

The Virtual Devices table only appears when the device is a host.

Asset Data

This table displays the data entered in the Asset Questionnaire.

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 Enterprise Discovery.

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 Enterprise Discovery is currently using to poll the device.

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.

For additional information about how Enterprise Discover works with VMware and other virtualization methods, see Chapter 4, “Virtualization in Enterprise Discovery” in the *HP OpenView Enterprise Discovery Reference Guide*.

Device Structure

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

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 Enterprise Discovery identifies as the primary IP or MAC address for the device
- when Enterprise Discovery 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 Enterprise Discovery 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 Enterprise Discovery exceptions, see **Help > Classifications > Exceptions**.

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

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. For more information, see page 80 .
	Scanner Deployment Log	This button displays information logged during the scanner deployment process. For more information, see page 80 .
	Virtualization Log	This button displays information logged during the VMware discovery process running on the host. For more information, see page 80 .
	IP Ping	This button allows you to ping the device to see if it responds, and how quickly. For more information, see page 80 .
	Traceroute	This button displays the path that data takes to get from the Enterprise Discovery server to the selected device. For more information, see page 80 .
	SNMP Ping	This button allows you to query the device for basic SNMP information and displays this information. For more information, see page 82 .
	Agent Ping	This button allows you to make a connection to the agent running on the device. For more information, see page 82 .
	DNS Query	This button allows you to send a host query to the domain name server and displays a table that highlights configuration errors. For more information, see page 82 .

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 Enterprise Discovery. It also shows the current value of numerous parameters.

Table 3 summarizes the information displayed in the main diagnosis table:

Table 3 Main Diagnosis

Data	Output	Notes
First discovered	elapsed time ^a / absolute date & time	Reset if database is cleared.
Scanner model last updated	elapsed time / absolute date & time	—
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 Enterprise Discovery
Last changed	elapsed time / absolute date & time	the last time a connection to this device changed
Device last modeled as a managed device	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	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”
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, 2.20)	—
Agent operating system	name of operating system	—
Agent port number	port number (example, 2738)	—
Scanner version	version number (example, 2.20.6150)	—

Table 3 Main Diagnosis

Data	Output	Notes
Scanner configuration	name of scanner configuration applied to this device	—
Scan file location	location of scan file on your Enterprise Discovery server	—
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 port, to the nearest 30 minutes.
Port Bridge tables seen	elapsed time / absolute date & time	the last time the Bridge tables were seen by this port, 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 port, to the nearest 30 minutes.
Port Radio link seen	elapsed time / absolute date & time	the last time a Radio link was seen by this port, to the nearest 30 minutes.
Port Bus link seen	elapsed time / absolute date & time	the last time a Bus link was seen by this port, to the nearest 30 minutes.
Port carrier link seen	elapsed time / absolute date & time	the last time a carrier link was seen by this port, to the nearest 30 minutes.
Port link training seen	elapsed time / absolute date & time	the last time link training was seen by this port, 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 port, to the nearest 30 minutes.
Device modeler interval	time (in days, hours, minutes, seconds)	If custom, is shown here.

Table 3 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.

Configuration Profiles and Device Groups

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

Table 4 Types of Configuration Profiles

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

The Enterprise Discovery 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.

Enterprise Discovery 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, Enterprise Discovery 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
 - Allow agent upgrade
 - Agent automatic upgrade schedule
 - Agent deployment
- 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
- Win32 scanner
- HP-UX scanner
- Linux scanner
- AIX scanner
- Solaris scanner
- MAC OS X scanner
- Virtualization parameters
 - VMware discovery interval
 - Discover VMware using this schedule
 - VMware credentials

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 Enterprise Discovery.



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 Enterprise Discovery 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 Inventory license is present. An exception is the Enterprise Discovery 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 Inventory license is present. An exception is the Enterprise Discovery server itself, where this button is always available regardless of license.

Virtualization Log

The virtualization 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.

IP Ping

Pings the device to see if it responds, and how quickly. The IP address pinged is the address identified by Enterprise Discovery 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 Enterprise Discovery 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 ^a
!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 Enterprise Discovery 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 Enterprise Discovery 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 Enterprise Discovery 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, Enterprise Discovery 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 Enterprise Discovery displays the message “Non-existent domain”, it means that the device has not been assigned a domain name.

Ports

This panel lists ports for this device and summarizes the information available for them. Displays 24 ports at a time (by default, you can change this 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



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

This button opens one of the Enterprise Discovery Viewers to show information about the device collected by Enterprise Discovery scanners.

There are two different Viewers in Enterprise Discovery. The Win32 Viewer is available with the Enterprise Discovery client, and the Java 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 Enterprise Discovery 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. (Enterprise Discovery does not check before attempting a connection.)

Update Model *(Administrator or IT Manager)*

This panel gives several options for updating the device information in the Discovery database.

At the top of the panel, there is a pull-down list so you can select the command you want to perform:

Command	Explanation
Query Network	Puts the device at the top of the device modeler's queue, and runs through all the steps as required. This command tries all valid community strings or users for this device, in the order specified in the SNMP configuration profile assigned to this device group. This command does not begin with the currently active community string/user, it begins with the first string/user in the list.
Run VMware Discovery	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 Enterprise Discovery database. This option is also available from any applet window from the right-click menu associated with a device. This option is disabled (discovery will not run) if the virtualization discovery frequency is disabled or set to 0, if the node does not have a valid IP address, or if the "Virtualization discovery active" option is disabled in Administration > System Configuration > Discovery Services .
Deploy Agent	Sends the Agent to the device.

Command	Explanation
Upgrade Agent	Upgrades the Agent on the device.
Upgrade Scanner	Transfers the relevant scanner executable and configuration files to the device, then execute the scanner and finally transfer the resulting scan file to the Enterprise Discovery server.
Run Scanner	Requests the immediate Enterprise Discovery scan of this device.
Retrieve Scan File	Transfers the result of the latest scan from the device to the Enterprise Discovery server.
Uninstall Agent	Removes the Agent from the device. To verify that it has been uninstalled, try to do an Agent Ping on the Diagnosis panel. Once the Agent is uninstalled, the Agent-related options will disappear from the Update Model panel's pull-down list.
Enrich XML	Requests immediate enrichment of the scan file associated with this device.
Run Rulebase	Allows you to only re-check the Enterprise Discovery rulebase for this device.

If Enterprise Discovery is not able to perform a particular option at a given point in time, that option does not appear in the Update Model drop-down menu in the Device Manager. Here, for example, are the options available under various circumstances:

- Before a device is discovered, the Update Model menu contains the following options:
 - Query Network
 - Deploy Agent
- After a device has been discovered, but before Enterprise Discovery has been able to communicate with the agent, the Update Model menu contains the following options:
 - Query Network
 - Deploy Agent
 - Run Rulebase
- After Enterprise Discovery has been able to communicate with the agent on a device, the Update Model menu contains the following options:
 - Query Network
 - Deploy Agent
 - Upgrade Agent
 - Upgrade Scanner
 - Run Scanner
 - Retrieve Scan File
 - Uninstall Agent
 - Run Rulebase

- After a scan file has been retrieved and processed by the XML Enricher, the Update Model menu contains the following options:
 - Query Network
 - Deploy Agent
 - Upgrade Agent
 - Upgrade Scanner
 - Run Scanner
 - Retrieve Scan File
 - Uninstall Agent
 - Enrich XML
 - Run Rulebase.

Special Note about the Query Network Panel

On the Query Network 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 doing an Update Model 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 Enterprise Discovery) see the [Diagnosis](#) panel. It lists all the relevant information.

8 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 Enterprise Discovery perceives a connection.



The Port Manager enables you to change only Enterprise Discovery'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. For more information, see page 91 .
	State	This panel displays current values for attributes. NOTE: This button is only available if the Topology license is present. For more information, see page 93 .
	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). For more information, see page 93 .
	Diagnosis	This panel displays information about the current state of the port that can be helpful in diagnosing problems with Enterprise Discovery. For more information, see page 94 .
	Statistics	This panel provides a second toolbar that you can use to view or export detailed historical statistics for the port. NOTE: This button is only available if the Topology license is present. For more information, see page 97 .
	Events	This button opens the Events Browser with this device and port in context. For more information, see Using the Events Browser on page 57 .
	Locate	This button highlights in a map window the location of the device. 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. 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. NOTE: 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 Enterprise Discovery. For more information, see page 99 .

Icon	Button name	Description
	Create Connection (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. For more information, see page 99 . NOTE: This button is only available if the Topology license is present.
	Break Connection (Administrator or IT Manager)	This panel lets you break an existing connection. For more information, see page 100 . NOTE: This button is only available if the Topology license is present.
	Port Properties	You can use the Properties dialog to change how Enterprise Discovery sees this port. For more information, see page 100 .
	Refresh	This button refreshes the contents of the panel. Does not re-read the data in the panel from the network. Re-reads the data only from the Enterprise Discovery 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. Note: The number Enterprise Discovery uses for the port may not match the physical port. 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 Enterprise Discovery 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 NOTE: 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/Enterprise Discovery Rulebase
Line alarm type	Ethernet 100 HD	from device MIB/Enterprise Discovery Rulebase
Interface rate	100 Mbits/sec.	from device MIB/Enterprise Discovery 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 Enterprise Discovery, 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 Enterprise Discovery 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 Enterprise Discovery 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 ^a , Device Adds, Device Deletes, Device Moves ^b , Device Changes, Not Recently Seen
State	OK, Info, Minor, Major, Critical
Value	For exceptions: description effect 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 Enterprise Discovery.

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 Enterprise Discovery—plus the current values for several parameters.

Data	Output	Notes
First discovered	elapsed time ^a / 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	—
Bridge tables seen	elapsed time / absolute date & time	—
Source address capture seen	elapsed time / absolute date & time	—

Data	Output	Notes
Radio link seen	elapsed time / absolute date & time	—
Bus link seen	elapsed time / absolute date & time	—
Carrier link seen	elapsed time / absolute date & time	—
Link training seen	elapsed time / absolute date & time	—
Detailed link training seen	elapsed time / absolute date & time	—
Connection method	bridge tables source address capture traffic link training logical subnet approximate; see “Terms and Concepts” in the <i>Reference Guide</i> . user-defined unknown	—
Previously connected to	none device (real or connector), hyperlinked to Device Manager 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.

Parameter	Notes
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.

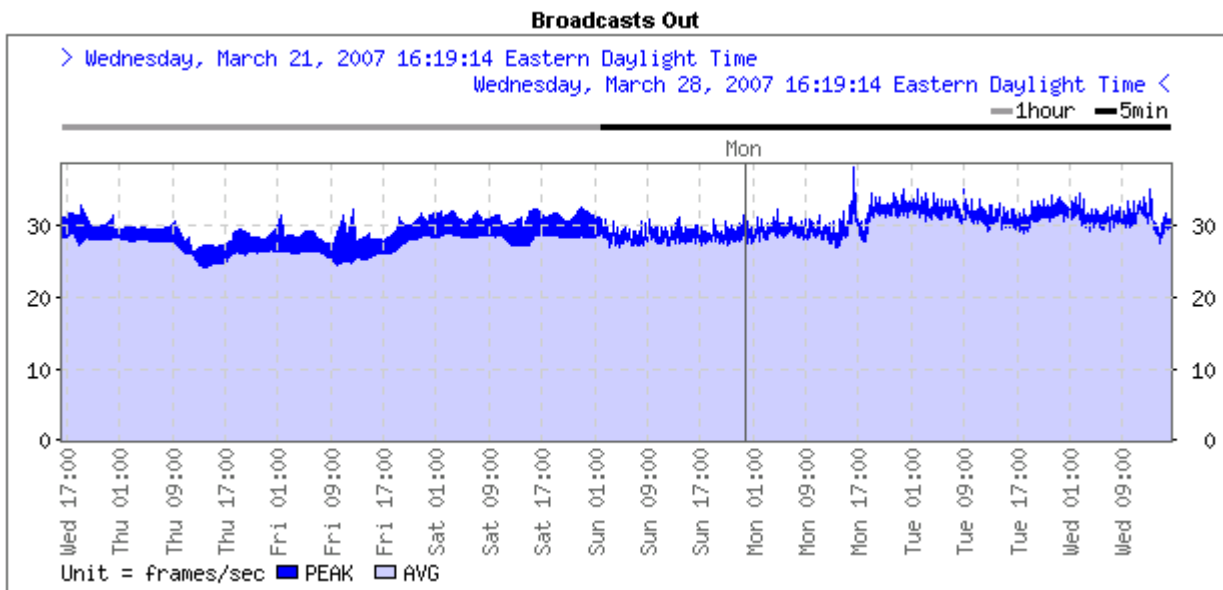
Inbound and outbound data is displayed for several statistics. Average values and peak values are available for some statistics. You can view the statistics in graph or table form, and you can export them to a Comma Separated Value (CSV) file.

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).

Enterprise Discovery 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 Enterprise Discovery.

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 Enterprise Discovery.



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 Enterprise Discovery'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 100.
- 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 Enterprise Discovery 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 Enterprise Discovery down or even make it impossible for Enterprise Discovery to correctly connect to your network. Never use forcing a connection as a quick fix.



Do not create a connection without consulting your Enterprise Discovery Customer Support representative. If you force a connection, Enterprise Discovery 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 Enterprise Discovery 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 Enterprise Discovery represents the connection on the Network Map.

When to use it

When Enterprise Discovery has made incorrect assumptions about connectivity.

Port Properties

You can use the Properties dialog to change how Enterprise Discovery 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 Enterprise Discovery 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 Enterprise Discovery does not recognize the type of interface for the line.
- When Enterprise Discovery has set the wrong interface type for the line.

Limits

Enterprise Discovery assigns a default duplex to each interface type.

Related

To change the duplex mode, see [Duplex Mode](#) on page 101.

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 Enterprise Discovery has set the wrong duplex. This changes how Enterprise Discovery interprets the duplex mode, not the setting on the actual port.

Limits

Full | Half

Effects

Duplex affects utilization statistics.

9 Using the Line Manager

Enterprise Discovery has two different Line Managers:

- [Single Line Manager](#) on page 103
- [Multiple Line Manager](#) on page 105

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:

From	Open by...
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.

Icon	Button name	
	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.
	Break Connection (Administrator or IT Manager)	This panel lets you break an existing connection.
	Refresh	This button refreshes the contents of the panel. Note: Does not re-read the data in the panel from the network. Re-reads the data only from the Enterprise Discovery database.
	Print	This button prints the contents of the panel.
	Close	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 94.

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 Enterprise Discovery has made incorrect assumptions about connectivity.

Related

See also the Port Manager [Break Connection \(Administrator or IT Manager\)](#) on page 100.

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.

The screenshot shows a software interface with a menu bar (File, Edit, View, Object, Tools, Help) and a status bar (CPU Utilization, 1-6, Lines: 5). Below the menu bar, there are two hub icons: "SSI Hub 500 hub 500" and "8 devices for hub 500". A table below shows connections between devices and ports. A context menu is open over the table, listing options: "Open Port", "Open Line", "Browse Port Events", and "Port Properties".

Device	Port	Device	Port
hub 500	1.24	172.23.0.17	3
hub 500	1.4	NT4_ENT1	
hub 500	1.3	NT4_ENT	
hub 500		hub 13	
hub 500		B	0.0

Connections →

Right-click to open a Line Manager or Port Manager →

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.

10 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 Enterprise Discovery 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
	Configuration	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. 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. 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.
	Manage (Administrator or IT Manager)	This panel lets you manage the attribute.

Icon	Button name	Description
	Purge Attribute (Administrator or IT Manager)	This panel lets you remove an attribute and its historical statistics from the Enterprise Discovery database.
	Refresh	This button refreshes the contents of the panel. Note: Does not re-read the data in the panel from the network. Re-reads the data only from the Enterprise Discovery 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 Help > Supported Device/Port Attributes	—
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 Enterprise Discovery 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 Enterprise Discovery 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 Enterprise Discovery 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—Enterprise Discovery 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.

11 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 Enterprise Discovery MIB Browser to read or write data to the device MIB.

Enterprise Discovery 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.

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.

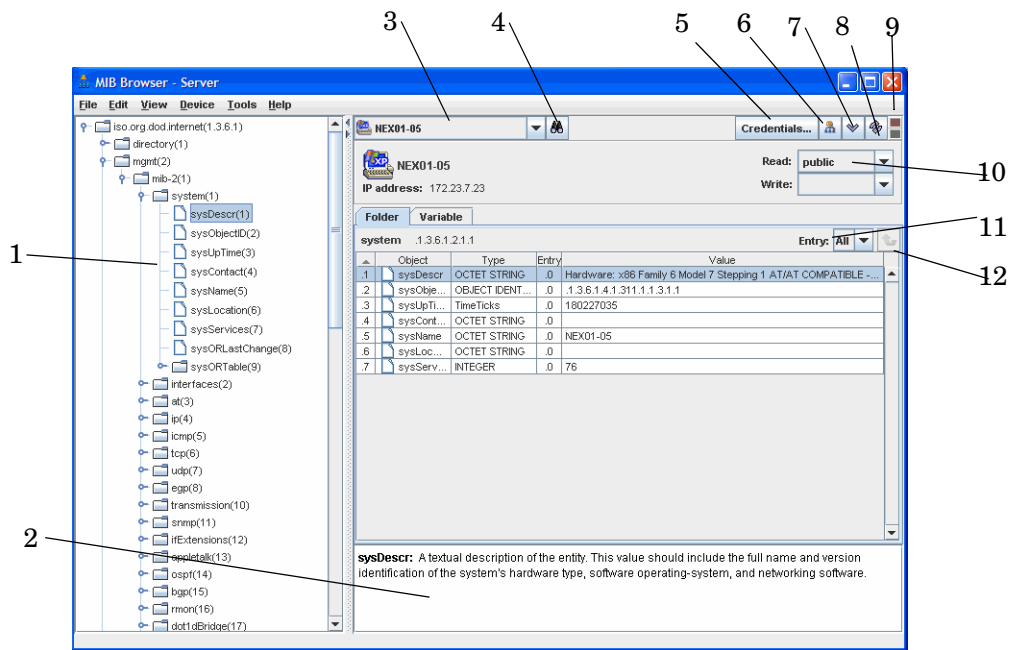
There are three ways to open a MIB Browser with a device in context:

- 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:

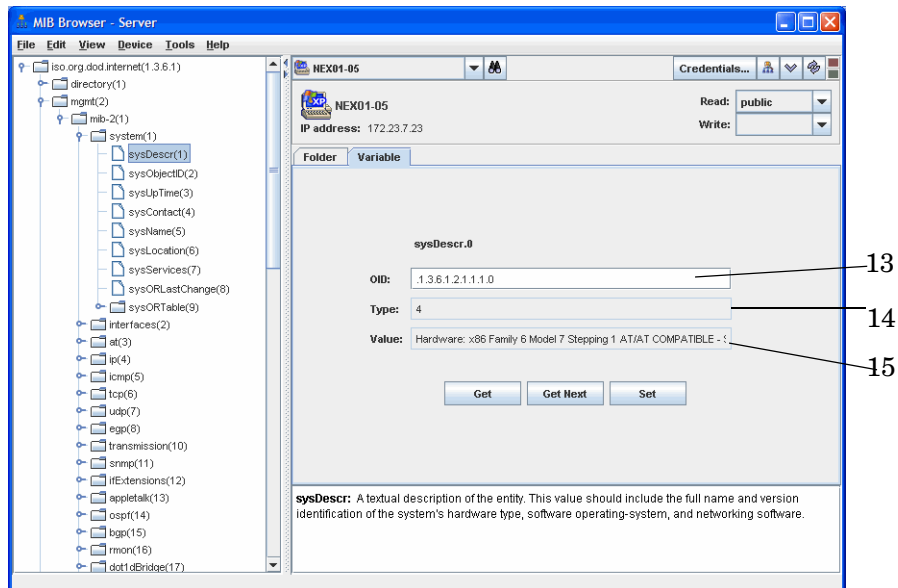


Table 1 MIB Browser legend

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

Tree View

The left hand side of a MIB Browser shows a tree view of all the MIBs for which Enterprise Discovery has definitions. These definitions are stored within the Enterprise Discovery 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 Enterprise Discovery 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 117.



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 Enterprise Discovery 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

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.

The image shows two screenshots of the MIB Browser GUI. The top screenshot shows the 'Folder' tab with the 'Entry' dropdown set to 'All'. The bottom screenshot shows the 'Variable' tab with the 'Entry' dropdown set to '.1'. Arrows point to these dropdown menus with labels 'Entry setting to "All"' and 'Entry setting to ".1"'.

Object	Type	Entry	Value
.1 ifIndex	INTEGER	.1	1
.1 ifIndex	INTEGER	.167772...	16777219
.1 ifIndex	INTEGER	.167772...	16777220
.1 ifIndex	INTEGER	.167772...	16777221
.2 ifDescr	OCTET STRING	.1	MS TCP Loopback interface
.2 ifDescr	OCTET STRING	.167772...	Intel 8255x-based Integrated Fast Et...
.2 ifDescr	OCTET STRING	.167772...	Intel 8255x-based Integrated Fast Et...
.2 ifDescr	OCTET STRING	.167772...	Intel 8255x-based Integrated Fast Et...
.3 ifType	INTEGER	.1	softwareLoopback
.3 ifType	INTEGER	.167772...	ethernetCsmacd
.3 ifType	INTEGER	.167772...	ethernetCsmacd
.3 ifType	INTEGER	.167772...	ethernetCsmacd
.4 ifMtu	INTEGER	.1	1500
.4 ifMtu	INTEGER	.167772...	1500
.4 ifMtu	INTEGER	.167772...	1500
.4 ifMtu	INTEGER	.167772...	1500
.5 ifSpeed	Gauge	.1	10000000
.5 ifSpeed	Gauge	.167772...	10000000

ifEntry(1): An entry containing management information applicable to a particular interface.

Move Up a Level

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

Variable Tab

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 Enterprise Discovery 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 Enterprise Discovery server that performs the SNMP **Set** and **Get**. A malicious user with the MIB Browser could leverage the Enterprise Discovery 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 114.

As Enterprise Discovery 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 Enterprise Discovery has determined is valid for that device.

However, if that device is not yet known to Enterprise Discovery, then Enterprise Discovery 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. Enterprise Discovery must have valid read credentials to discover a managed device, but valid write credentials are optional. Enterprise Discovery 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 Enterprise Discovery has not yet, or cannot, determine a valid one.

- The device supports directed community strings, and Enterprise Discovery is not on the access list.

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

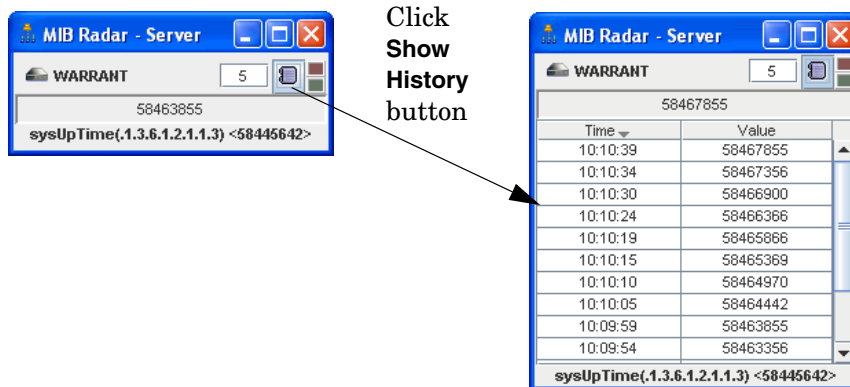
Using Multiple MIB Browser Sessions

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**.

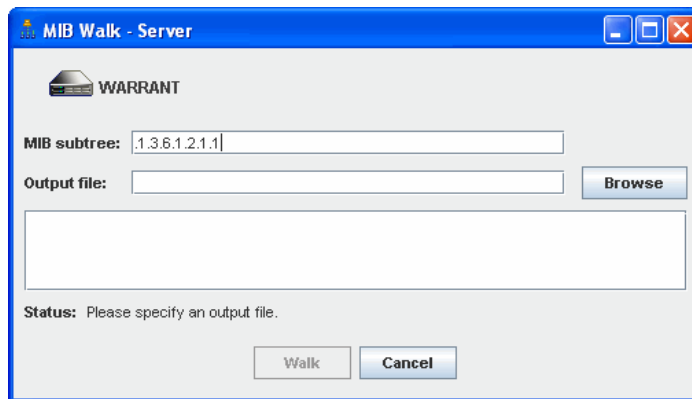
MIB Walk

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**.

12 Using the Scan Data Viewer

The Scan Data Viewer displays detailed information contained in the Discovery Database, data compiled from Enterprise Discovery'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 Enterprise Discovery client). They both show similar information, but the Scan Data Viewer is accessible through the web user interface.

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

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 Enterprise Discovery 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 Enterprise Discovery 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

Command	Description
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

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 Enterprise Discovery 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**.

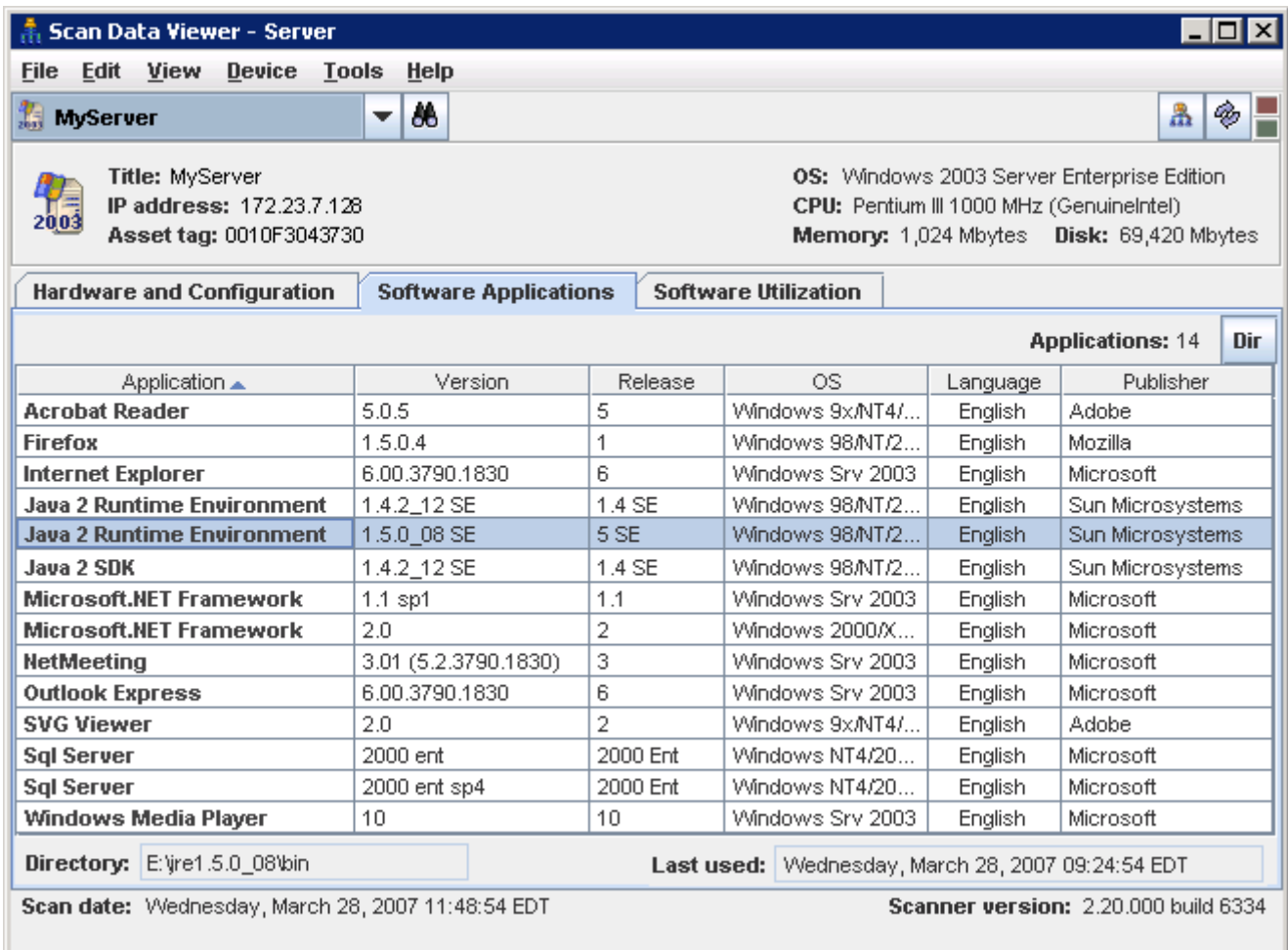
The  button will move you up one level in the Scan Data Viewer tree view.

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

Viewing Software Application Data

The Software Applications tab displays applications that have been recognized by the Software Applications Index.

All data shown is from the scan date shown at the bottom of the page.



The screenshot shows the 'Scan Data Viewer - Server' application window. The title bar indicates the server name is 'MyServer'. The menu bar includes File, Edit, View, Device, Tools, and Help. The main area displays system information for 'MyServer':

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

Below the system information are three tabs: 'Hardware and Configuration', 'Software Applications' (which is selected), and 'Software Utilization'. The 'Software Applications' tab shows a list of 14 applications with columns for Application, Version, Release, OS, Language, and Publisher. A 'Dir' button is visible next to the application count.

Application	Version	Release	OS	Language	Publisher
Acrobat Reader	5.0.5	5	Windows 9x/NT4/...	English	Adobe
Firefox	1.5.0.4	1	Windows 98/NT/2...	English	Mozilla
Internet Explorer	6.00.3790.1830	6	Windows Srv 2003	English	Microsoft
Java 2 Runtime Environment	1.4.2_12 SE	1.4 SE	Windows 98/NT/2...	English	Sun Microsystems
Java 2 Runtime Environment	1.5.0_08 SE	5 SE	Windows 98/NT/2...	English	Sun Microsystems
Java 2 SDK	1.4.2_12 SE	1.4 SE	Windows 98/NT/2...	English	Sun Microsystems
Microsoft.NET Framework	1.1 sp1	1.1	Windows Srv 2003	English	Microsoft
Microsoft.NET Framework	2.0	2	Windows 2000/X...	English	Microsoft
NetMeeting	3.01 (5.2.3790.1830)	3	Windows Srv 2003	English	Microsoft
Outlook Express	6.00.3790.1830	6	Windows Srv 2003	English	Microsoft
SVG Viewer	2.0	2	Windows 9x/NT4/...	English	Adobe
Sql Server	2000 ent	2000 Ent	Windows NT4/20...	English	Microsoft
Sql Server	2000 ent sp4	2000 Ent	Windows NT4/20...	English	Microsoft
Windows Media Player	10	10	Windows Srv 2003	English	Microsoft

At the bottom of the window, the 'Directory' is set to 'E:\jre1.5.0_08\bin' and the 'Last used' time is 'Wednesday, March 28, 2007 09:24:54 EDT'. The 'Scan date' is 'Wednesday, March 28, 2007 11:48:54 EDT' and the 'Scanner version' is '2.20.000 build 6334'.

Information shown in the Application data window

The following information is shown about each software application:

- **Application**
The name of the software application.
- **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)

The 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).

The screenshot shows the 'Scan Data Viewer - Server' application window. The title bar includes the application name and standard window controls. The menu bar contains 'File', 'Edit', 'View', 'Device', 'Tools', and 'Help'. Below the menu bar is a toolbar with a 'MyServer' dropdown menu and several icons. The main content area displays system information for 'MyServer':
Title: MyServer
IP address: 172.23.7.128
Asset tag: 0010F3043730
OS: Windows 2003 Server Enterprise Edition
CPU: Pentium III 1000 MHz (GenuineIntel)
Memory: 1,024 Mbytes
Disk: 69,420 Mbytes

Below the system information are three tabs: 'Hardware and Configuration', 'Software Applications', and 'Software Utilization'. The 'Software Utilization' tab is active. It features a 'User:' dropdown menu set to 'All Users' and an 'Applications:' label. A table displays utilization data for various applications:

Application	Version	Util	Used31	Used90	Used365	Avg Hrs	Peak Hrs	Hrs31	Hrs90	Hrs365
Acrobat Reader	5.0.5	6.03	0	0	22	10.36	15.97	0	0	227.83
Firefox	1.5.0.4	0.82	2	2	3	0.03	0.03	0.07	0.07	0.08
Internet Explorer	6.00.379...	18.63	2	2	68	10.84	24	0.07	0.07	737.32
Java 2 Runtime Environment	1.4.2_12 ...	10.68	0	0	39	12.08	22.05	0	0	471.13
Java 2 Runtime Environment	1.5.0_08 ...	21.1	20	20	77	13.28	24	256.75	256.75	1,022...
Microsoft.NET Framework	1.1 sp1	3.23	1	1	1	0.02	0.02	0.02	0.02	0.02
Microsoft.NET Framework	2.0	3.23	1	1	1	1.57	1.57	1.57	1.57	1.57
Outlook Express	6.00.379...	3.23	1	1	1	0.02	0.02	0.02	0.02	0.02
Sql Server	2000 ent	3.23	1	1	1	0.02	0.02	0.02	0.02	0.02
Sql Server	2000 ent ...	64.52	20	20	20	13.06	23.87	261.17	261.17	261.17

At the bottom of the window, the 'Scan date:' is 'Wednesday, March 28, 2007 11:48:54 EDT' and the 'Scanner version:' is '2.20.000 build 6334'.

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**
- **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.

13 Using the Reports

Enterprise Discovery provides numerous reports to help you analyze and understand what is contained in your network.

Enterprise Discovery reports comprise the following groups:

Table 1 Enterprise Discovery Reports

Report Category	Explanation
Executive/Summary Network Reports on page 130	These reports are intended as a general overview of what is in your network. You can see lists of all your network devices.
Scanned Device Reports on page 132	If you use Enterprise Discovery to scan devices in your network, these reports show data about the applications on those devices, data about which devices can be upgraded to Windows Vista, and data on any unrecognized files.
WAN Reports on page 136	These reports show information about your Frame Relay, Point to Point Serial, and other WAN connections in your network.
LAN Reports on page 137	These reports show information about your FDDI and Token Ring connections in your network.
Device Reports on page 137	These reports show inventory information.

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 ^a	✓	—
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).

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
	Virtual Devices by Virtualization Type	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

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 of those devices which belong to the summary group clicked on.

- ▶ 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.

Application Reports

These reports display software application license and installation counts for all installed applications grouped by application, application version, and application publisher. These reports also display whether there is usage data being collected for each application.

The reports also provide links to detailed reports of those scanned devices where the individual applications are installed.

These reports are based on Application Recognition performed by the XML Enricher.

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.

License Counts by Application

This summary report displays all applications by publisher and application with counts of licenses required and installations for each application. This report also displays whether there is usage data being collected for each application.

Clicking in the Publisher column will display detailed version information about all of the publisher's applications. Clicking in the Application Name column will display the details of the different versions of that application.

Top Applications

This report lists those applications requiring the largest number of licenses, sorted by number of licenses. This report also displays whether there is usage data being collected for each application.

Clicking in the Publisher column will display detailed version information about all of the publisher's applications. Clicking in the Application Name column will display the details of the different versions of that application.

Publishers Summary

This summary report lists all publishers sorted by name together with their application licenses required and installed application counts.

Clicking on the publisher's name will display detail information for all of the publisher's applications.

Top Publishers

This report lists the publishers with the greatest number of installed applications that require licenses.

Clicking on the publisher's name will display detail information for all of the publisher's applications.

Unrecognized Files

The unrecognized file reports display the files on your scanned devices that were not recognized as belonging to a known application. You can view the file data by Scanner Type or you can drill down to view the directories and devices where these files are located.

Unrecognized File Reports

These reports display the unrecognized files found on your scanned devices grouped by Scanner Platform.

Devices with High Risk Files

These reports display the devices that have the greatest number of files considered to be high risk. These "high risk" files are the 100 files that are not recognized as belonging to any known software application that occur most often in the population of scanned devices.

These devices are likely to be those devices that it will be most effective to teach to lower the number of unrecognized files. If you click on the link "[Export Analysis Workbench Load Script]", it will create a load script which will load the scan files for the 10 devices with the greatest number of high risk files into Analysis Workbench to begin the process of teaching.

Clicking on the link "[View the 100 Highest Risk Files Present]" will display file details for the 100 files considered highest risk used to rate each device for teaching. Clicking on the number in the column "# of the 100 Highest Risk Files ..." will display those files on that device that are in the group of 100 highest risk files.

Microsoft Windows Vista Readiness Reports

These reports list scanned devices that could potentially be upgraded to the Windows Vista operating system. For each device in the list, the following six components are assessed:

Component	Minimum Requirement	Recommended Capability
CPU Speed	800 MHz	1 GHz
System Memory	512 MB	1 GB
Disk Space	Total:20 GB Free: 15 GB	Total: 40 GB Free: 15 GB
Graphics Display	Supports SVGA graphics	Support for DirectX 9 graphics with a WDDM driver, 128 MB of graphics memory (minimum), Pixel Shader 2.0 in hardware, and 32 bits per pixel
Audio Output	No sound card	Sound card present
Optical Drive	CD-ROM drive	DVD-ROM drive

Each component is assigned one of the following four levels of readiness:

- Recommended—This component meets or exceeds the level recommended by Microsoft for Vista.
- Minimum—This component meets the minimum requirement for Vista.
- Not Ready—This component does not meet the minimum requirement for Vista.
- Unknown—Enterprise Discovery does not have information about this component.

An overall Vista readiness level is also reported for each device. The overall readiness level is equal to the minimum readiness level detected among the six components.

There are three different types of Vista Readiness reports:

- Microsoft Windows Vista Readiness Summary—shows the percentage and number of scanned devices at each Vista readiness level for each component.
- Microsoft Windows Vista Readiness for Scanned Devices—lists the Vista readiness information for all scanned Windows devices. Devices are listed in alphabetical order by device name.
- Microsoft Windows Vista Readiness for Vista Devices—lists the Vista readiness information for scanned devices that already have the Microsoft Windows Vista operating system installed.

In all three reports, you can drill down to get more detailed information about the various components and their readiness levels:

Component	Drill-Down Information Available
CPU Speed	Rated speed and measured speed
System Memory	Total memory, additional memory required to meet minimum and recommended levels, free memory slots, memory hardware configuration
Disk space	Total disk space, free disk space, additional disk space required to meet minimum and recommended levels, additional free disk space recommended, boot disk volume letter, logical disk volumes
Graphics display	Type of graphics card, resolution, graphics memory, refresh rate
Audio output	Type of sound card
Optical drive	None

Both reports show the device name, current operating system, and most recent scan date for each device listed.



The requirements discussed in this section are based on the Microsoft Windows Vista recommended requirements for business or enterprise systems. See the following web site for additional information:

www.microsoft.com/windows/products/windowsvista/editions/systemrequirements.mspx

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

Index

A

About
 Line Manager panel, 104

Administration
 configuration files
 change default, 44
 copy, 43
 delete, 43
 rename, 43

advanced Find, 20

Agent Ping
 Device Manager button, 82

Aggregate Alarms Viewer, 55

Aggregate Events Browser, 63

Aggregate Health Panel, 53

alarms, 54

Alarms Viewer, 54

Alarm Type panel (Port Manager), 101

appliance access events, 62

approximate connection, 95

asset tag, 20

Attribute Manager, 107
 Configuration, 108
 Manage, 109

Automatic packaging
 preferences, 36

autosave, 41

B

blue line under icon, 26, 36

Break Connection panel
 Line Manager, 105
 Port Manager, 100

breaking a connection, 100

C

clearing the database, 75, 94

colored ring, 22, 26

comma separated value *see* CSV

community strings
 in MIB Browser, 117

Configuration
 Attribute Manager panel, 108
 Device Manager panel, 68
 Port Manager panel, 91

configuration files, 39

connection
 breaking single (conceptual), 100, 105
 forcing single new (conceptual), 99
 types of, 95

contact, system, 70

Create Connection panel (Port Manager), 99

creating a connection, 99

CSV, 97, 137

customize the Network Map, 27

D

data
 clearing, 75, 94

default map configuration, 40, 137

device
 model, 84
 not seen, 26
 title, 14

- Device Manager
 - Agent Ping, 82
 - Configuration, 68
 - Diagnosis, 74
 - DNS Query, 82
 - Export (Statistics), 98
 - Graph (Statistics), 97
 - IP Ping, 80
 - Ports, 83
 - reports, 73
 - Scan Data, 83
 - SNMP Ping, 82
 - Statistics, ?? to 98
 - Table (Statistics), 98
 - Traceroute, 80
 - Update Model, 84
 - Web, 84

Device Reports, 137

device title, 20

Diagnosis

- Device Manager panel, 74

- Port Manager panel, 94

disconnecting a port or line, 100, 105

DNS Query button (Device Manager), 82

domain name, 20

Duplex Mode panel (Port Manager), 101

E

Easy Find, 12

Entry, 115

Events Browser, 57

Executive/Summary Reports, 130

Export

- Device Manager Statistics button, 98

exporting data

- saving to text file, 55

F

faded icon, 26

family, 20

Find, 11

- advanced, 20

- MIB Browser, 114

- Scan Data Viewer, 122

Find OID, 117

Folder tab, 115

forcing a connection, 99

found objects, 27

G

Get, 116

Get Next, 115, 118

Graph

- Device Manager button, 97

gray background

- Manager data, 93

H

Hardware data

- viewing in viewer, 123

Health Panel, 22, 51

- aggregator, 53

- alarm list, 52

- hide inactive alarms, 53

Hide Inactive Alarms, 53

HTTP session, 83, 84

I

icons, 23

- appearance, 26

- blue line under icons, 26

- faded, 26

- found, 27

- locked, 26

- package, 25

- selected, 27

- with colored ring, 26

Interface Rate panel (Port Manager), 100

Interface Type panel (Port Manager), 101

IP address

- multiple, 72

IP Ping

- Device Manager button, 80

L

LAN Reports, 137

Layout, 30

line, multiple, 105

Line Manager, 103

- About, 104

- Break Connection, 105

link training, 95

Locate

- MIB Browser button, 114

- Scan Data Viewer button, 122

location, system, 70

Lock, 26, 36

locked objects, 26, 36

logical subnet, 95

M

Manage

Attribute Manager button, 109

map configuration, 39

change default, 44

copy, 43

default, 40

delete, 43

New, 41

open, 43

organizing, 43

Prime, saving, 42

rename, 43

saving, 40, 41

sharing with other accounts, 44

map scale, 22

MIB Browser, 111

Entry, 115

find a device, 114

Find OID, 117

Folder tab, 115

Get, 116

Get Next, 115, 118

locate, 114

MIB description, 117

MIB radar, 119

opening, 111

pull-down list of devices, 113

refresh, 115

set, 116

tree view, 113

Variable tab, 116

write, 116

model, 20

multi-object packages, 34

create manually, 34

multiple IP addresses, 72

multiple lines, 105

My User Alarms Only, 52

N

name, system, 70

negative statistics, 93

NetBIOS name, 20

NetBIOS workgroup, 20

network function, 20

Network Map

autosave, 41

colored ring, 26

customizing, 27

faded icon, 26

icons, 23

opening a configuration, 43

placing an object at top, 29

saving a map configuration, 41

starting a configuration, 41

Status Bar, 22

New MIB Browser

MIB Browser

New MIB Browser, 119

not seen device, 26

O

objects

placing at top of network, 29

Open Copy of Prime, 40

operating system, 20

P

Package, 34

packaging, 25, 33

map configuration files, 39

multi-object packages, 34

Pack command, 34

ping button (Device Manager), 80

Port Manager

Alarm Type, 101

Break Connection, 100

Configuration, 91

Create Connection, 99

Diagnosis, 94

Duplex Mode, 101

Interface Rate, 100

Interface Type, 101

Purge Port, 99

Reports, 93

State, 93

Ports panel (Device Manager), 83

Preferences

automatic packaging, 36

Prime map configuration, 40

saving, 42

- priority
 - device
 - range, 25
 - reserved, 25
- Progress Bar, 22
- Promote, 30
- properties
 - object
 - priority, 25
- Purge Port (Port Manager), 99
- R**
- Radar, 119
- Reports, 129, 135
 - business
 - device, 137
 - executive/summary, 130
 - LAN, 137
 - WAN, 136
 - Windows Vista Readiness, 135
 - periods, 130
- Reports (Device Manager), 73
- Reports (Port Manager), 93
- ring, colored, 26
- S**
- sampling period, 99
- Save, 40
- Save as Prime, 40
- Save Table Data, 55
- Scan Data
 - Device Manager button, 83
- Scan Data Viewer, 121
 - find a device, 122
 - locate, 122
 - New Scan Data Viewer, 122
 - pull-down list of devices, 122
 - refresh, 122
- selected objects, 27
- Service Analyzer, 47
- Set, 116
- SNMP contact, 20
- SNMP description, 20
- SNMP location, 20
- SNMP name, 20
- SNMP Ping
 - Device Manager button, 82

- SNMP serial number, 20
- SNMP write by Attribute, 62
- SNMP write by MIB OID, 62
- Software Utilization, 127
- source address capture, 95
- speed, line
 - see Interface Rate
- spreadsheets, exporting to. *See* CSV
- stale data, 93
- Starting
 - Viewer, 121
- State panel
 - Port Manager, 93
- Statistics
 - Device Manager panel, ?? to 98
- Status Bar, 22
- system contact, 70
- system location, 70
- system name, 70

T

- Table
 - Device Manager button, 98
- table-based connection, 95
- text file, saving data to, 55
- title
 - device, 14
- top of network, 29
- Traceroute
 - Device Manager button, 80
- traffic-based connection, 95

U

- Unlock, 26, 36
- Unpack, 35
- Unpackage, 35
- Unpack All, 35
- Update Model button (Device Manager), 84
- Utilization, 127

V

- Variable Tab, 116
- virtual device
 - creating, 99

Vista
 readiness
 reports, 135
VLAN, 72

W

WAN Reports, 136
Web
 Device Manager button, 84
Windows Vista Readiness, 135
Write, 116

