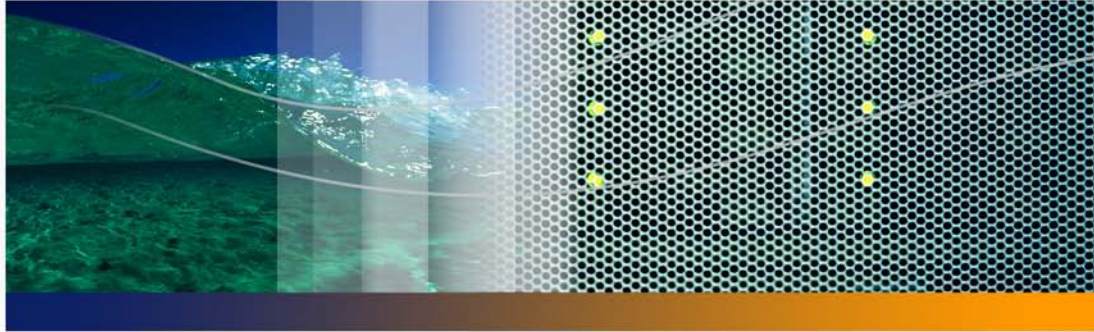


Peregrine Systems, Inc.

# Enterprise Discovery™ 2.0



## Network Data Analysis



Copyright © 2005 Peregrine Systems, Inc.

PLEASE READ THE FOLLOWING MESSAGE CAREFULLY BEFORE INSTALLING AND USING THIS PRODUCT. THIS PRODUCT IS COPYRIGHTED PROPRIETARY MATERIAL OF PEREGRINE SYSTEMS, INC. ("PEREGRINE"). YOU ACKNOWLEDGE AND AGREE THAT YOUR USE OF THIS PRODUCT IS SUBJECT TO THE SOFTWARE LICENSE AGREEMENT BETWEEN YOU AND PEREGRINE. BY INSTALLING OR USING THIS PRODUCT, YOU INDICATE ACCEPTANCE OF AND AGREE TO BE BOUND BY THE TERMS AND CONDITIONS OF THE SOFTWARE LICENSE AGREEMENT BETWEEN YOU AND PEREGRINE. ANY INSTALLATION, USE, REPRODUCTION OR MODIFICATION OF THIS PRODUCT IN VIOLATION OF THE TERMS OF THE SOFTWARE LICENSE AGREEMENT BETWEEN YOU AND PEREGRINE IS EXPRESSLY PROHIBITED.

Information contained in this document is proprietary to Peregrine Systems, Incorporated, and may be used or disclosed only with written permission from Peregrine Systems, Inc. This book, or any part thereof, may not be reproduced without the prior written permission of Peregrine Systems, Inc. This document refers to numerous products by their trade names. In most, if not all, cases these designations are claimed as Trademarks or Registered Trademarks by their respective companies.

Peregrine Systems, Enterprise Discovery, AssetCenter and ServiceCenter are trademarks or registered trademarks of Peregrine Systems, Inc. or its affiliates.

This document and the related software described in this manual are supplied under license or nondisclosure agreement and may be used or copied only in accordance with the terms of the agreement.

The information in this document is subject to change without notice and does not represent a commitment on the part of Peregrine Systems, Inc. Contact Peregrine Systems, Inc., Customer Support to verify the date of the latest version of this document. The names of companies and individuals used in the sample database and in examples in the manuals are fictitious and are intended to illustrate the use of the software. Any resemblance to actual companies or individuals, whether past or present, is purely coincidental. If you need technical support for this product, or would like to request documentation for a product for which you are licensed, contact Peregrine Systems, Inc. Customer Support by email at [support@peregrine.com](mailto:support@peregrine.com). If you have comments or suggestions about this documentation, please contact Peregrine Systems, Inc. Technical Publications by email at [doc\\_comments@peregrine.com](mailto:doc_comments@peregrine.com). This edition applies to version 2.0 of the licensed program.

For more copyright information, see the Copyright chapter of the Enterprise Discovery Reference Guide.

Peregrine Systems, Inc.  
3611 Valley Centre Drive San Diego, CA 92130  
858.481.5000  
Fax 858.481.1751  
[www.peregrine.com](http://www.peregrine.com)



# Contents

Chapter 1	Introduction . . . . .	7
Chapter 2	Finding your Network Devices . . . . .	9
	Finding devices . . . . .	9
	Easy Find . . . . .	11
	Advanced Find. . . . .	12
	Aggregate Find . . . . .	13
Chapter 3	Health Panel and Alarms Viewer . . . . .	15
	See a network overview with the Health Panel . . . . .	16
	Customizing the Alarm List . . . . .	17
	Using the Aggregate Health Panel . . . . .	18
	Using the Alarms Viewer . . . . .	19
	Using the Aggregate Alarms Viewer . . . . .	20
	Saving data to a text file . . . . .	21
Chapter 4	Events Browser . . . . .	23
	Opening the Events Browser . . . . .	24

	Network Events . . . . .	24
	Toolbar . . . . .	26
	The Aggregate Events Browser . . . . .	28
Chapter 5	Understanding the Device Manager . . . . .	29
	Toolbar . . . . .	30
	Configuration . . . . .	32
	Reports . . . . .	38
	Diagnosis . . . . .	39
	Diagnostic Information. . . . .	39
	Agent Deployment Log . . . . .	43
	Scanner Deployment Log . . . . .	43
	IP Ping. . . . .	44
	Traceroute. . . . .	44
	SNMP Ping. . . . .	45
	Agent Ping . . . . .	46
	DNS Query. . . . .	46
	Ports . . . . .	47
	Events. . . . .	47
	View Scan Data . . . . .	47
	Web. . . . .	48
	Telnet. . . . .	48
	Update Model <i>[Administrator or IT Manager]</i> . . . . .	49
	Device Visibility <i>[Administrator or IT Manager]</i> . . . . .	50

	Properties . . . . .	51
	Refresh . . . . .	51
	Print. . . . .	51
	Close . . . . .	51
Chapter 6	Understanding the Port Manager . . . . .	53
	Toolbar . . . . .	54
	Configuration . . . . .	55
	Reports . . . . .	57
	Diagnosis . . . . .	58
	Events. . . . .	59
	Purge Port. . . . .	60
	Port Properties. . . . .	60
	Refresh . . . . .	62
	Print. . . . .	62
	Close . . . . .	62
	Port number. . . . .	63
Chapter 7	Exporting Data into Data Access Applications . . . . .	65
	Step 1: Set up Enterprise Discovery to export data. . . . .	66
	Step 2: Install the MySQL ODBC driver. . . . .	66
	Step 3: Select MYSQL as the data source (create an ODBC alias) . . . . .	67
	Step 4: Create a new database in Microsoft Access 2000 . . . . .	70
	Step 5: Link in the Enterprise Discovery tables. . . . .	71
	Step 6: Create a basic assets and recognition query . . . . .	74

	Step 7: Create a basic license query . . . . .	78
Chapter 8	Deleting Data . . . . .	81
	Deleting data . . . . .	81
Chapter 9	Reports . . . . .	83
	Executive/Summary Network Reports . . . . .	83
	Scanned Machine Reports . . . . .	84
	Scanned Machine Summaries . . . . .	84
	Application Reports . . . . .	87
	Index . . . . .	89



# 1 | Introduction

CHAPTER

Welcome to the *Network Data Analysis Guide*.

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 devices
- Understanding the Health Panel and Alarms Viewer
- Understanding the Events Browser
- Exporting Data
- Deleting data from the Enterprise Discovery database
- Understanding the Device Manager
- Understanding the Port Manager







# 2 Finding your Network Devices

## CHAPTER

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. For more information, see [Aggregate Find on page 13](#).

---

## Finding devices

To use the Find tool:

- 1 Open the Find tool:
  - a On the Home page click **Find**.

OR

  - b From the Health Panel, Alarms Viewer, or Events Browser, click **Tools > Find** (or Ctrl-F).
- 2 By default, you can use the **Easy Find** feature (go to [Step 5](#)). 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 device data you want to search on (for example, “asset tag”).

- 4 In the second pull-down list, select a match mode (for example, "containing").

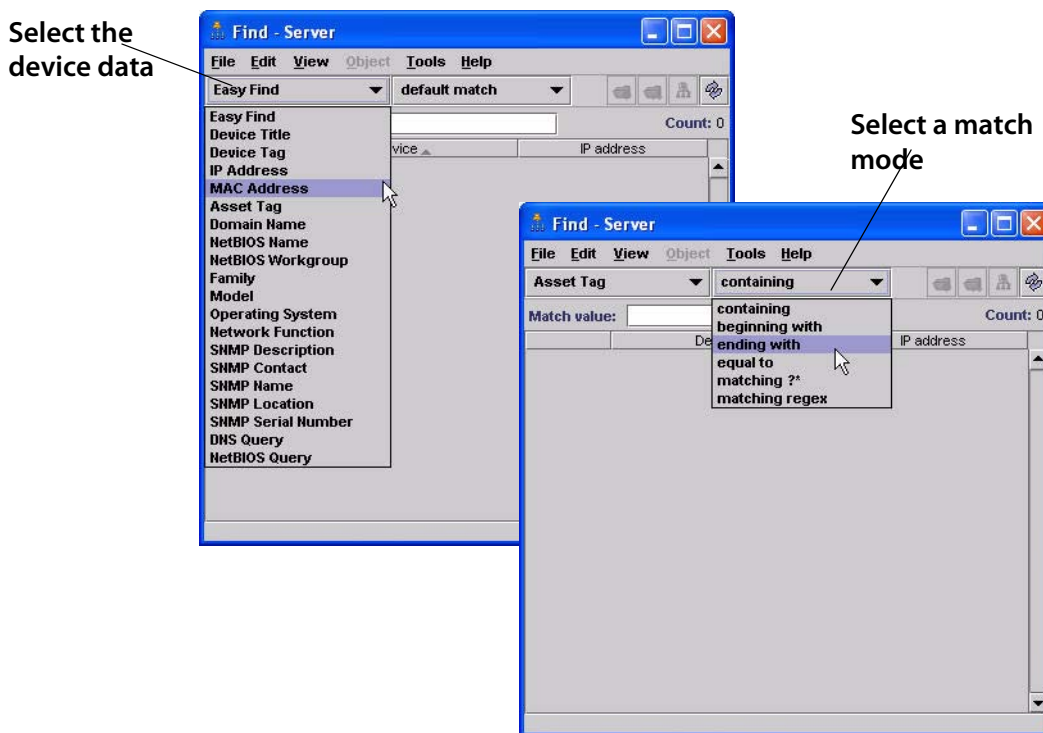
**Note:** There are different match modes available for different types of device data.

- 5 Enter a match value.

**Note:** 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.

- 6 Press Enter.

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.



## Easy Find

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

**Note:** 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.

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. <b>Note:</b> To find a specific device, you must enter its complete MAC address in one of these formats: <b>12:AB:34:CD:56:EF</b> or <b>12AB34CD56EF</b> .
IP address	Enterprise Discovery will try to search based on the known IP address. <b>Note:</b> 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 <b>Administration &gt; System preferences &gt; Display preferences &gt; Device title preference</b> . Only the selected titles are searched.
Asset Tag	Even if Asset Tag is not listed in your Device title preference, 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.

**Important:** 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.

## Advanced Find

**Note:** Searches are not case-sensitive.

Match Modes	Notes
containing	—
beginning with	—
ending with	—
equal to	—
matching ?*	<p>Wildcard characters:</p> <ul style="list-style-type: none"> <li>■ “?” can represent any single character. For example, “gr?y” finds “gray” and “grey.”</li> <li>■ “*” can find multiple characters. For example, “E*t” finds “Ethernet.”</li> </ul>
matching regex	Matching a regular expression.
matching address*	<p>This works only for IP address and MAC address searches. You must enter an entire IP or MAC address in these formats:</p> <ul style="list-style-type: none"> <li>■ IP - 123.123.123.123</li> <li>■ MAC - 12:AB:34:CD:56:EF</li> </ul> <p><b>Note:</b> 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</p> <p><b>Note:</b> For MAC addresses, you can compress the zeros in each segment. For example, you can enter “5” instead of “05” for a segment.</p> <p><b>Note:</b> If an IP or MAC address is associated with a port, you will see a port listed in your Find results.</p>
name prefix	—
name equal to	—

## Aggregate Find

The Aggregate Find is almost identical to the regular Find feature. The major difference is that there are fewer find options in the Aggregate Find.

	Regular Find	Aggregate Find
Easy Find	✓	—
Device Title	✓	✓
IP Address	✓	✓
MAC Address	✓	✓
Asset Tag	✓	✓
Domain Name	✓	✓
NetBIOS Name	✓	✓
NetBIOS Workgroup	✓	✓
Family	✓	✓
Model	✓	✓
Operating System	✓	✓
Network Function	✓	✓
SNMP Description	✓	✓
SNMP Contact	✓	✓
SNMP Name	✓	✓
SNMP Location	✓	✓
SNMP Serial Number	✓	✓
DNS Query	✓	—
NetBIOS Query	✓	—





# 3 Health Panel and Alarms Viewer

## CHAPTER

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 double click on an alarm and open up a Device Manager, and from there you can investigate a problem with that device.

Topics in this chapter include:

- See a network overview with the Health Panel on page 16
- Using the Aggregate Health Panel on page 18
- Using the Alarms Viewer on page 19
- Using the Aggregate Alarms Viewer on page 20
- Saving data to a text file on page 21

## 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.



**Note:** 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:

Category	Indicator
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.

**Note:** 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 20](#).



# 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**.

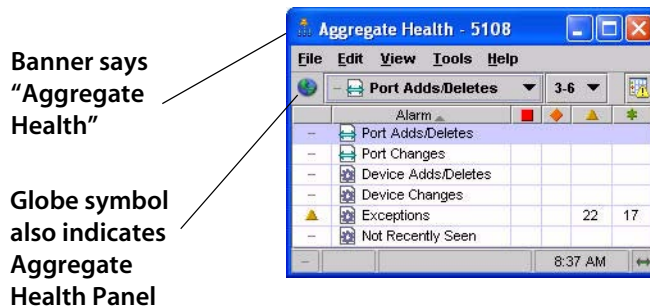
## Using the Aggregate Health Panel

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.

**Note:** 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.

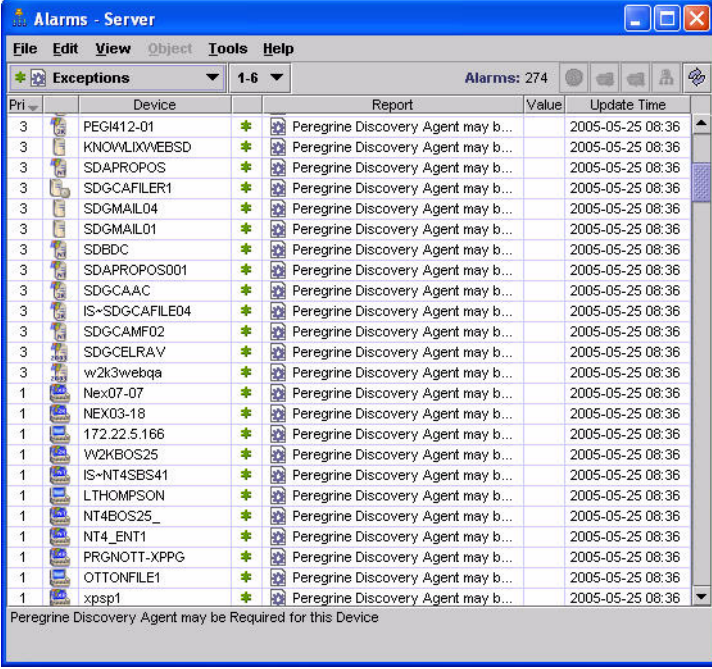
The statistics listed in the Aggregate Health Panel are the same as those listed in the regular Health Panel.



## 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 - Server' window with a menu bar (File, Edit, View, Object, Tools, Help) and a toolbar. The main area contains a table of alarms. The status bar at the bottom indicates 'Alarms: 274' and 'Peregrine Discovery Agent may be Required for this Device'.

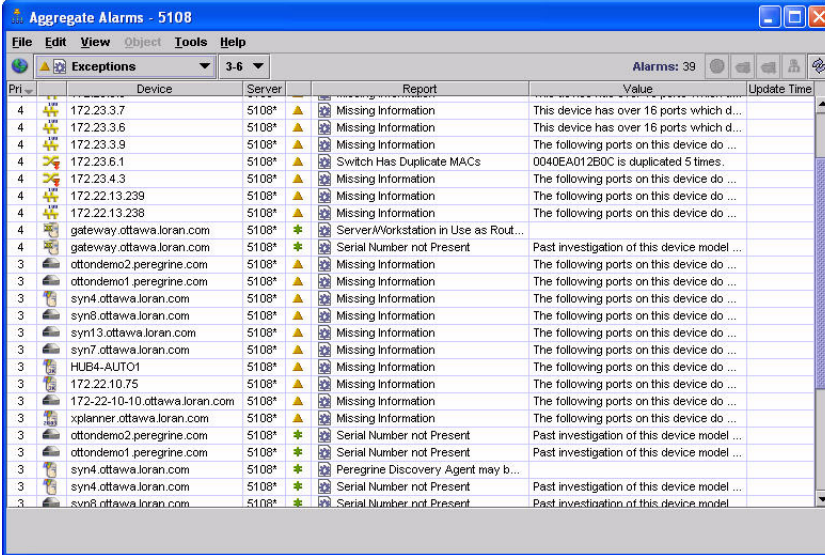
Pri	Device	Report	Value	Update Time
3	PEG412-01	Peregrine Discovery Agent may b...		2005-05-25 08:36
3	KNOWLIXWEBS	Peregrine Discovery Agent may b...		2005-05-25 08:36
3	SDAPROPOS	Peregrine Discovery Agent may b...		2005-05-25 08:36
3	SDGCASFILER1	Peregrine Discovery Agent may b...		2005-05-25 08:36
3	SDGMAL04	Peregrine Discovery Agent may b...		2005-05-25 08:36
3	SDGMAL01	Peregrine Discovery Agent may b...		2005-05-25 08:36
3	SDBDC	Peregrine Discovery Agent may b...		2005-05-25 08:36
3	SDAPROPOS001	Peregrine Discovery Agent may b...		2005-05-25 08:36
3	SDGCAAC	Peregrine Discovery Agent may b...		2005-05-25 08:36
3	IS~SDGCFILE04	Peregrine Discovery Agent may b...		2005-05-25 08:36
3	SDGCAMF02	Peregrine Discovery Agent may b...		2005-05-25 08:36
3	SDGCELRAV	Peregrine Discovery Agent may b...		2005-05-25 08:36
3	w2k3webqa	Peregrine Discovery Agent may b...		2005-05-25 08:36
1	Nex07-07	Peregrine Discovery Agent may b...		2005-05-25 08:36
1	NEX03-18	Peregrine Discovery Agent may b...		2005-05-25 08:36
1	172.22.5.166	Peregrine Discovery Agent may b...		2005-05-25 08:36
1	YW2KBOS25	Peregrine Discovery Agent may b...		2005-05-25 08:36
1	IS-NT4SBS41	Peregrine Discovery Agent may b...		2005-05-25 08:36
1	LTHOMPSON	Peregrine Discovery Agent may b...		2005-05-25 08:36
1	NT4BOS25_	Peregrine Discovery Agent may b...		2005-05-25 08:36
1	NT4_ENT1	Peregrine Discovery Agent may b...		2005-05-25 08:36
1	PRGNOTT-XPPG	Peregrine Discovery Agent may b...		2005-05-25 08:36
1	OTTONFILE1	Peregrine Discovery Agent may b...		2005-05-25 08:36
1	xpsp1	Peregrine Discovery Agent may b...		2005-05-25 08:36

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.

**Note:** 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 a window titled "Aggregate Alarms - 5108". The window contains a table with the following columns: Pri, Device, Server, Report, Value, and Update Time. The table lists various alarms, including missing information and serial number not present, across different devices and servers.

Pri	Device	Server	Report	Value	Update Time
4	172.23.3.7	5108*	Missing Information	This device has over 16 ports which d...	
4	172.23.3.6	5108*	Missing Information	This device has over 16 ports which d...	
4	172.23.3.9	5108*	Missing Information	The following ports on this device do ...	
4	172.23.6.1	5108*	Switch Has Duplicate MACs	004DEA012B0C is duplicated 5 times.	
4	172.23.4.3	5108*	Missing Information	The following ports on this device do ...	
4	172.22.13.239	5108*	Missing Information	The following ports on this device do ...	
4	172.22.13.238	5108*	Missing Information	The following ports on this device do ...	
4	gateway.ottawa.loran.com	5108*	Server/Workstation in Use as Rout...		
4	gateway.ottawa.loran.com	5108*	Serial Number not Present	Past investigation of this device model ...	
3	ottondemo2.peregrine.com	5108*	Missing Information	The following ports on this device do ...	
3	ottondemo1.peregrine.com	5108*	Missing Information	The following ports on this device do ...	
3	syn4.ottawa.loran.com	5108*	Missing Information	The following ports on this device do ...	
3	syn8.ottawa.loran.com	5108*	Missing Information	The following ports on this device do ...	
3	syn13.ottawa.loran.com	5108*	Missing Information	The following ports on this device do ...	
3	syn7.ottawa.loran.com	5108*	Missing Information	The following ports on this device do ...	
3	HUB4-AUT01	5108*	Missing Information	The following ports on this device do ...	
3	172.22.10.75	5108*	Missing Information	The following ports on this device do ...	
3	172.22-10-10.ottawa.loran.com	5108*	Missing Information	The following ports on this device do ...	
3	xplanner.ottawa.loran.com	5108*	Missing Information	The following ports on this device do ...	
3	ottondemo2.peregrine.com	5108*	Serial Number not Present	Past investigation of this device model ...	
3	ottondemo1.peregrine.com	5108*	Serial Number not Present	Past investigation of this device model ...	
3	syn4.ottawa.loran.com	5108*	Peregrine Discovery Agent may b...		
3	syn4.ottawa.loran.com	5108*	Serial Number not Present	Past investigation of this device model ...	
3	syn8.ottawa.loran.com	5108*	Serial Number not Present	Past investigation of this device model ...	

## 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
- Find
- Alarms Viewer
- 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**.





# 4 Events Browser

## CHAPTER

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 or deleted
- 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

**Note:** 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. The Events Browser shows you a list of events that occurred on devices in your network during a specified period.

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

**Important:** 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 Home page, click the Events Browser link.

OR

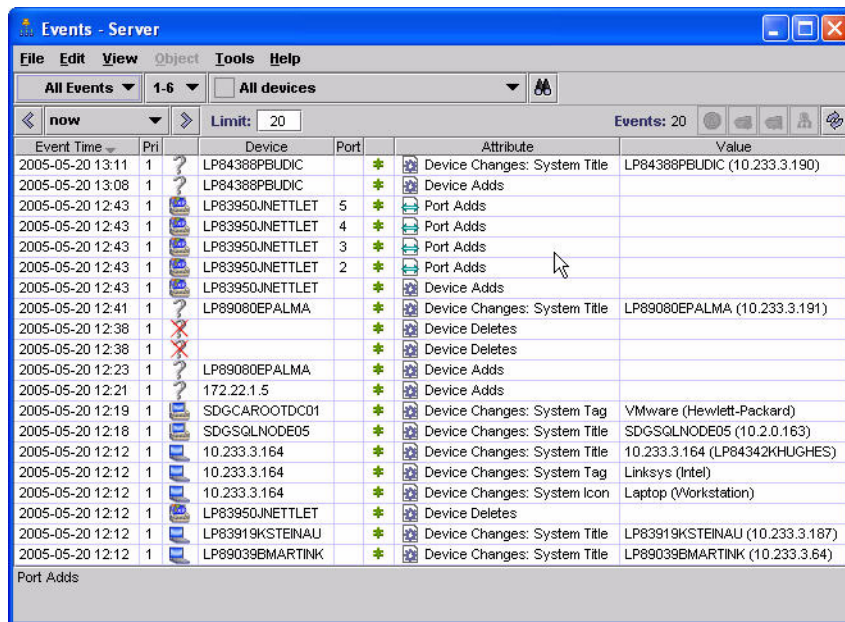
- From the Health Panel or Alarms Viewer, click **Tools > Events Browser**.

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
2005-05-20 13:11	1	LP84388PBUDIC		Device Changes: System Title	LP84388PBUDIC (10.233.3.190)
2005-05-20 13:08	1	LP84388PBUDIC		Device Adds	
2005-05-20 12:43	1	LP83950JNETTLET	5	Port Adds	
2005-05-20 12:43	1	LP83950JNETTLET	4	Port Adds	
2005-05-20 12:43	1	LP83950JNETTLET	3	Port Adds	
2005-05-20 12:43	1	LP83950JNETTLET	2	Port Adds	
2005-05-20 12:43	1	LP83950JNETTLET		Device Adds	
2005-05-20 12:41	1	LP89080EPALMA		Device Changes: System Title	LP89080EPALMA (10.233.3.191)
2005-05-20 12:38	1			Device Deletes	
2005-05-20 12:38	1			Device Deletes	
2005-05-20 12:23	1	LP89080EPALMA		Device Adds	
2005-05-20 12:21	1	172.22.1.5		Device Adds	
2005-05-20 12:19	1	SDGCAROOTDC01		Device Changes: System Tag	VMware (Hewlett-Packard)
2005-05-20 12:18	1	SDGSQLNODE05		Device Changes: System Title	SDGSQLNODE05 (10.2.0.163)
2005-05-20 12:12	1	10.233.3.164		Device Changes: System Title	10.233.3.164 (LP84342KHUGHES)
2005-05-20 12:12	1	10.233.3.164		Device Changes: System Tag	Linksys (Intel)
2005-05-20 12:12	1	10.233.3.164		Device Changes: System Icon	Laptop (Workstation)
2005-05-20 12:12	1	LP83950JNETTLET		Device Deletes	
2005-05-20 12:12	1	LP83919KSTEINAU		Device Changes: System Title	LP83919KSTEINAU (10.233.3.187)
2005-05-20 12:12	1	LP89039BMARTINK		Device Changes: System Title	LP89039BMARTINK (10.233.3.64)
Port Adds					



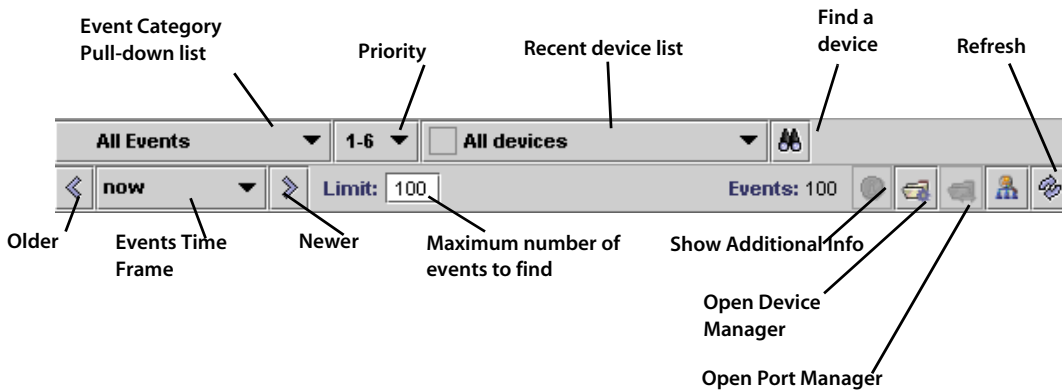
Each row in the Events Browser window contains the following columns.

<b>Data</b>	<b>Explanation</b>
Time	The time the event was generated.
Device Priority	—
Device type	small device icon
Device	device title <sup>a</sup>
Port	port number
State	alarm icon
Attribute	For more information on the attributes, see the <i>Reference Guide</i> .
Value	For more information on the values, see the <i>Reference Guide</i> .

<sup>a</sup> 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 preferences > Display preferences**.

## 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.



### Event Category Pull-down List

Selects the category of events for display so that you can focus on a specific event type.

### Priority

Selects the priority of devices that you want to see.

### Recent Device list

This is a list of recently seen devices. You can toggle between these devices to see the events on each device.

A device will appear on this list by being selected on Find, the Alarms Viewer or the Events Browser.

### Find Device

By clicking the "Find" button, you can find a single device and see only the events on that device.

## Refresh

Refreshes the events shown.

## Older

Updates the window with earlier events, relative to currently displayed events.

### Limits

45 days ago (or 500,000 events, whichever is less)

## Events Time Frame

This pull-down list lets you select older events from a particular time.

### Limits

Now | 1 hour ago | 2 hours ago | 4 hours ago | 8 hours ago | 16 hours ago | 1 day ago | 2 days ago | 4 days ago | 1 week ago | 2 weeks ago | 4 weeks ago

### Default

Now

## Newer

Updates the window with later events, relative to currently displayed events.

### Limits

current time

## Limit

Set the maximum number of events per window.

### Limits

1–1000

### Default

25

## Events

Shows the number of events listed in the window.

## Open Device Manager

Clicking this button will open the Device Manager for the selected device.

## Open Port Manager

Clicking this button will open the Port Manager for the selected port.

---

# 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.



# 5 Understanding the Device Manager

## CHAPTER

The Device Manager provides you with detailed information about a device, in several panels.

To open the Device Manager:


From	Open by...
Health Panel, Alarms Viewer, Events Browser	Click Tools > Find (Ctrl - F). Enter a device address or title, then click <b>Find</b> .
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 <b>Find</b> .
Reports, Status, Manager panels	Click a hyperlinked device title

## Toolbar

This table shows the availability of buttons in the Device Manager toolbar.

**Important:** Many of the panels in the Device Manager feature data in table form. Not all tables will look the same for all devices, because the tables will only show data that is available for that device.

Icon	Button name	No IP address	Not in database	Unknown	Demo or IT Employee user
	Configuration	✓	✓	✓	✓
	Reports	✓	—	✓	✓
	Diagnosis	✓	✓	✓	✓
Buttons on the Diagnosis Panel					
	Diagnostic Information	✓	—	✓	✓
	Agent Deployment Log	✓	—	—	✓
	Scanner Deployment Log	✓	—	—	✓
	IP Ping	—	✓	✓	✓
	Traceroute	—	✓	✓	✓
	SNMP Ping	—	✓	✓	✓
	Agent Ping	—	—	✓	✓
	DNS Query	—	✓	✓	✓
	Ports	✓	—	✓	✓

Icon	Button name	No IP address	Not in database	Unknown	Demo or IT Employee user
	Events	✓	—	✓	✓
	View Scan Data	✓	—	—	✓
	Web	—	✓	✓	✓
	Telnet	—	✓	✓	✓
	Update Model [Administrator or IT Manager]	—	✓	✓	—
	Device Visibility [Administrator or IT Manager]	✓	—	—	—
	Properties	✓	✓	✓	✓
	Refresh	✓	✓	✓	✓
	Print	✓	✓	✓	✓
	Close	✓	✓	✓	✓

# Configuration

Identifies a device and presents an overview of the device's identity and status.

**Note:** This panel is blank if the device is not in the Enterprise Discovery database.

This panel is divided into the following principal sections:

- Heading
- Identity table (real devices only)
- Device structure (Serial number and description, disk, CPU, memory)
- Address table (real devices only)

## Heading

The heading also appears in the State, Reports, and Diagnosis panels (when available).

Element	Notes	Type
Icon	for a complete list, see <b>Help &gt; Classifications &gt; Device Types/Package Types</b>	all
Descriptive prefix	for example, "SNMP-managed device"	
Device type	for a complete list, see <b>Help &gt; Device Types</b>	all
Device tag	see the <i>Configuration and Customization Guide</i> .	real
No. of ports	the number Enterprise Discovery uses for the port may not match the physical port	all
Object title	first title available; see <i>Terms and Concepts</i> in the <i>Reference Guide</i> .	all
Address	IP address; does not appear if identical to object title	real title
Priority	see <i>Terms and Concepts</i> in the <i>Reference Guide</i> .	all



## Identity

The information in this 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. It determines as many of these as are available.

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.

**Note:** All these elements are optional.

Data	Example	Creator	Administrator or IT Manager
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 <sup>a</sup>	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	—

Data	Example	Creator	Administrator or IT Manager
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	—
System OID manufacturer	PlainTree Systems Inc	Rulebase	—
System description	Ethernet Switch	manufacturer	—
System contact	test@example.com	device owner	set link
System name	ws1216-2	device owner	set link
System location	Server Room	device owner	set link
Read community string	public	device owner	view
Write community string	n/a	device owner	view
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) <sup>b, c</sup>	DUPONT	device owner	—
Last name	DUPONT	Scanner	—
First name	MARIE	Scanner	—

Data	Example	Creator	Administrator or IT Manager
Memory (MB)	1024	Scanner	—
Windows/NIS domain	MARKETING	Scanner	—

a Appears only when different from the current manufacturer.

b On Windows workstations, frequently the same as the system name.

c NetBIOS data is blank unless the device has an IP address.

## Community Strings

An Admin or IT Manager user will also see a read and a write community string for a device. These values are taken from the list of community strings; however:

- strings from the list appear here only if they are valid.
- only a single valid string appears here even if the list has multiple valid strings for this device.
- the read string that appears here is the string that Enterprise Discovery is currently using to poll the device.

## 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, tray, toner, unknown)
- Name
- Hardware
- Firmware
- Software
- SerialNumber

- Mount Point Capacity
- Description

Device Structure example:

Type	Name	Hardware	Firmware	Software	SerialNumber	Description
[-]	Switch System (Cisco Systems WS-C6509 9 slot switch)	3.0		7.6(3)	TSC07190058	WS-C6509
[-]	slot 1 (WS-C6509 9 slot switch chassis slot)					
[-]	1 (1000BaseX Supervisor 2 port WS-X6K-S2U-MSFC2 Rev. 4.2)	4.2	7.1(1)	7.6(3)	SAL0717CDW8	WS-X6K-S2U-MSFC2
	env temp (Module Intake Temp Sensor)					
	env temp (Module Exhaust Temp Sensor)					
	env temp (Module Device 1 Temp Sensor)					
	env temp (Module Device 2 Temp Sensor)					
[-]	L3 Switching Engine II Container					
[-]	L3 sub-module (L3 Switching Engine II)	3.3			SAL0718CERH	WS-F6K-PFC2
	env temp (L3 SE Intake Temp Sensor)					
	env temp (L3 SE Exhaust Temp Sensor)					
	env temp (L3 SE device1 Temp Sensor)					
	env temp (L3 SE device2 Temp Sensor)					
?	CPU of supervisor					
[-]	Container of Router Switch Feature Card					
[-]	15 (Router Switch feature Card)	2.5	12.1(19) E1	12.1(19) E1	SAL0718CE1U	WS-F6K-MSFC2
	env temp (RSFC Intake Temp Sensor)					
	env temp (RSFC Temp Sensor)					
	env temp (RSFC device1 Temp Sensor)					
	env temp (RSFC device2 Temp Sensor)					
[-]	slot 2 (WS-C6509 9 slot switch chassis slot)					
[-]	Container of Power Supply Group					
[-]	Container of Power Supply					
	2500 watt AC supply	1.0			ART070800DC	WS-CAC-2500W
	Fan Sensor (Power Supply Fan Sensor)					
[-]	Container of Power Supply					

## 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

Displays current values for report (Adds, Deletes, Changes) and summary historical data.

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 Changes
State	OK, Info, Minor, Major, Critical
Value	For exceptions: <ul style="list-style-type: none"><li>■ description</li><li>■ effect</li><li>■ action</li></ul>

**Note:** Exceptions cannot always be reported for a device.

---

## Diagnosis

Displays information about the current state of the device that can be helpful in diagnosing problems. Has buttons that give you access to diagnostic tools. Opens with a configuration panel.

### Diagnostic Information

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

- Main Diagnosis
- Network Configuration
- Property Assignment

#### Main Diagnosis

The main table indicates the data flow for this device—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 <sup>a</sup> / absolute date & time	Reset if database is cleared.
Scanner model last updated	elapsed time / absolute date & time	—
Last replied to ICMP	elapsed time / absolute date & time	in ping by Enterprise Discovery
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, 2.0.0)	—
Agent operating system	name of operating system	—
Agent port number	port number (example, 2738)	—
Scanner version	version number (example, 2.0.0.3809)	—
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.



Data	Output	Notes
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.
Device modeler interval	either "Default as set in Network Configuration" or time (in days, hours, minutes, seconds)	If custom, is shown here.
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.

## Network Configuration

The Network Configuration table shows what parameters have been set up for the range in which the device resides and what their values are. It shows the Network Properties (**Administration > Network Configuration**).

Network Properties include:

**Note:** Network Properties may be set to On or Off.

- Allow devices
- Actively ping
- NetBIOS query
- Resource manage
- Force ARP table read
- Accumulate IP addresses
- Allow IP addresses
- Allow ICMP and SNMP

- Device Modeler interval
- Community read and Community write (These are the strings that will be tried for this device. This will be blank if there are no strings configured in Enterprise Discovery.)

**Note:** Only Admin and IT Manager accounts can see the community strings.

- Bandwidth
- Frequency
- Win32 platform
- HP/UX platform
- Linux platform
- AIX platform
- Solaris platform
- Scanner upgrade
- Scanner upgrade schedule
- Scanner run schedule
- Scan file download schedule
- Agent upgrade
- Agent upgrade schedule
- Agent action
- Listener uninstall
- Collect usage data

## 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.

Parameter	Notes
Default title	—
Custom title	takes precedence over default
Actual title	the title as it appears for your account
Default icon	—

Parameter	Notes
Custom icon	the icon assigned by an Administrator or IT Manager account in <b>Object &gt; Device Properties</b> .
Actual icon	the icon as it appears for your account
Default priority	—
Custom priority	for information only; never affects active configuration; useful if you receive e-mail or a page from Enterprise Discovery
Actual priority	the priority as it appears for your account
Default tag	—
Custom tag	the tag assigned by an Administrator or IT Manager account in <b>Object &gt; Device Properties</b>
Actual tag	the tag as it appears for your account

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.

## 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.

## 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 on page 44](#) has been used to confirm the existence of a device.

### 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.

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

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

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

<sup>a</sup>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. 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 for the device as defined in **Administration > Network configuration > Community Property Groups**.

## Agent Ping

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

- 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.

**Important:** If Enterprise Discovery displays the message "Non-existent domain", it means that the device has not been assigned a domain name.

---

## Ports

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.

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

---

## Events

Opens the Events Browser with this device in context.

For detailed information, see [Events Browser on page 23](#).

---

## View Scan Data

**Important:** You must perform a client install of Enterprise Discovery to use the Viewer on your workstation.

Opens the Enterprise Discovery Viewer to show information about the device collected by Enterprise Discovery scanners.

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.

**Note:** 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

Attempts to open a web browser window for the device.

### When to use it

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.)

### Related

**Note:** for Aggregator—See also **Administration > Remote appliance administration > Remote appliance properties.**

---

## Telnet

Attempts to open a Telnet session. Many network devices provide Telnet as a means to set up and configure the device.

### Limits

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

### Related

**Note:** for Aggregator—See also **Administration > Remote appliance administration > Remote appliance properties.**



## Update Model *[Administrator or IT Manager]*

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 for this device, in the order specified in <b>Administration &gt; Network Configuration &gt; Community Property Groups</b> . This command does not begin with the currently active community string, it begins with the first string in the list of community strings.
Deploy Agent	Sends the Agent to the device.
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.

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.

State	Message
major alarm	IP address is not in scope
major alarm	no read community strings have been specified
minor alarm	no write community strings have been specified
minor alarm	IP address is not in scope for resource management
info	current discovery process
info	list of read community strings to be tried
info	list of write community strings 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.

### 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.

---

## Device Visibility *[Administrator or IT Manager]*

You can activate, deactivate, hide, or purge devices on this panel.

For information on how to activate, deactivate, hide, or purge devices, see the *Configuration and Customization Guide*.

---

## Properties

Allows you to change the icon and name of a device in your network.

For instructions on how to use this feature, see the *Configuration and Customization Guide*.

---

## Refresh

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.

### Limits

Does not re-read the data in the panel from the network. Re-reads the data only from the Enterprise Discovery database.

---

## Print

Prints the contents of the panel.

---

## Close

Closes the window and exits the Device Manager.





# 6 Understanding the Port Manager

## CHAPTER

To select a different port for the same device, use the port list box—see [Port number](#) on page 63.

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

### To open the Port Manager:

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










### Default panel

- *initial*: Configuration
- *subsequent*: from **Administration** > **Account administration** > **Account properties**

## Toolbar

This table shows the availability of buttons in the Port Manager toolbar.

**Important:** 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	IT Employee or Demo user	Admin or IT Manager user
	Configuration	✓	✓
	Reports	✓	✓
	Diagnosis	✓	✓
	Events	✓	✓
	Purge Port	—	✓
	Port Properties	—	✓
	<ul style="list-style-type: none"> <li>■ Interface Rate</li> <li>■ Interface Type</li> <li>■ Line Alarm Type</li> <li>■ Duplex Mode</li> </ul>		
	Refresh	✓	✓
	Print	✓	✓
	Close	✓	✓
	Port number	✓	✓

# Configuration

Identifies a port and presents an overview of the port's identity and properties.

This panel is divided into these main sections:

- Heading
- Identity table
- VLAN table

## Heading

The heading also appears in other panels.

Element	Notes	Type
Device Icon	for a complete list, see <b>Help &gt; Classifications &gt; Device Types/Package Types</b>	all
Device type	for a complete list, see <b>Help &gt; Classifications &gt; Device Types</b>	all
Device tag	see the <i>Configuration and Customization Guide</i>	real
No. of ports	the number Enterprise Discovery uses for the port may not match the physical ports	all
Object title	first title available; see <i>Terms and Concepts</i> in the <i>Reference Guide</i> .	all
Port no./ description	number of port / description of port	all
Device priority	see <i>Terms and Concepts</i> in the <i>Reference Guide</i> .	all

## Properties

Most information in this table comes from the Enterprise Discovery Rulebase.

Data	Example	Notes
Description	100Base-TX Port	from device manufacturer
Interface type	Ethernet CSMA/CD	from device MIB/Enterprise Discovery Rulebase

Data	Example	Notes
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

## 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.



---

## Reports

This panel shows details on all Add, Delete, or Change events associated with this port.

### Limits

This panel is not available if the object is not in the Enterprise Discovery database.

## Diagnosis

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 <sup>a</sup> / absolute date & time	resets if database is cleared
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
ARP tables seen	elapsed time / absolute date & time	—
Bridge tables seen	elapsed time / absolute date & time	—

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

## Property Assignment

The property assignment table helps you to determine how Enterprise Discovery sees the port.

Parameter	Notes
Default Interface Rate	as generated automatically by Enterprise Discovery
Custom Interface Rate	as set by the Administrator or IT Manager account
Actual Interface Rate	the interface rate as it appears for your account
Default Interface Type	as generated automatically by Enterprise Discovery
Custom Interface Type	as set by the Administrator or IT Manager account
Actual Interface Type	the interface type as it appears for your account
Default Line Alarm Type	as generated automatically by Enterprise Discovery
Custom Line Alarm Type	as set by the Administrator or IT Manager account
Actual Line Alarm Type	the line alarm type as it appears for your account
Default Duplex Mode	as generated automatically by Enterprise Discovery
Custom Duplex Mode	as set by the Administrator or IT Manager account
Actual Duplex Mode	the duplex mode as it appears for your account

## Events

Opens the Events Browser with this device and port in context.

For detailed information, see [Events Browser on page 23](#).

---

## Purge Port

Removes the port from the device's model as created by Enterprise Discovery.

**Warning:** This action cannot be undone.

**Important:** 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 events associated with the port from the event log.

### Related

- To purge a device, see the *Configuration and Customization Guide*.

---

## Port Properties

### 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.

### 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 62](#).

## 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

---

## Refresh

Refreshes the contents of the panel.

### Limits

Does not re-read the data in the panel from the network. Re-reads the data only from the Enterprise Discovery database.

---

## Print

Prints the contents of the panel.

---

## Close

Closes the window and exits the Port Manager.

---

## Port number

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).







# 7 Exporting Data into Data Access Applications

CHAPTER

This chapter contains a tutorial that walks you through a simple example of how to connect to the Enterprise Discovery database from Microsoft Access by means of ODBC; how to link in the tables and perform two basic queries.

Topics in this chapter include:

- Step 1: Set up Enterprise Discovery to export data on page 66
- Step 2: Install the MySQL ODBC driver on page 66
- Step 3: Select MYSQL as the data source (create an ODBC alias) on page 67
- Step 4: Create a new database in Microsoft Access 2000 on page 70
- Step 5: Link in the Enterprise Discovery tables on page 71
- Step 6: Create a basic assets and recognition query on page 74
- Step 7: Create a basic license query on page 78

---

## Step 1: Set up Enterprise Discovery to export data

To set up Enterprise Discovery to export data

- 1 Click **Administration > Account administration > Account Capabilities**.
- 2 Select the account that should have MySQL access.
- 3 Click **Modify Capabilities**.
- 4 Select **Yes** for MySQL ODBC access.
- 5 Click **Modify Capabilities**.

---

## Step 2: Install the MySQL ODBC driver

If your computer does not already have a MySQL driver, download the MySQL Connector/ODBC driver MSI or executable from the following URL and run the program:

<http://www.mysql.com/products/connector/odbc/>

In this example we have downloaded version 3.51 of the MySQL Connector/ODBC driver.

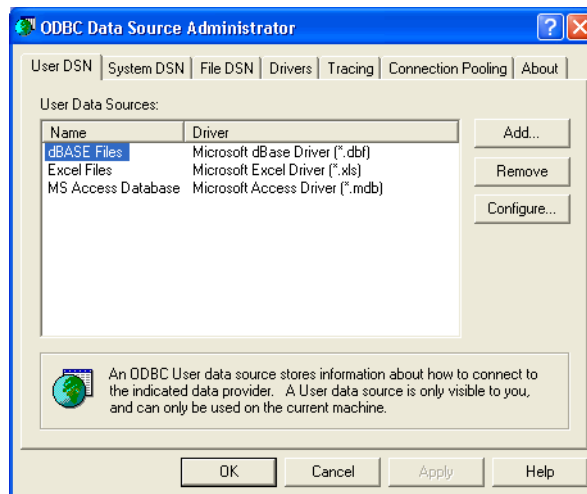
## Step 3: Select MYSQL as the data source (create an ODBC alias)

Before you can use the Enterprise Discovery data with Microsoft Access you need to create an ODBC alias for the database.

To set up MySQL as the data source

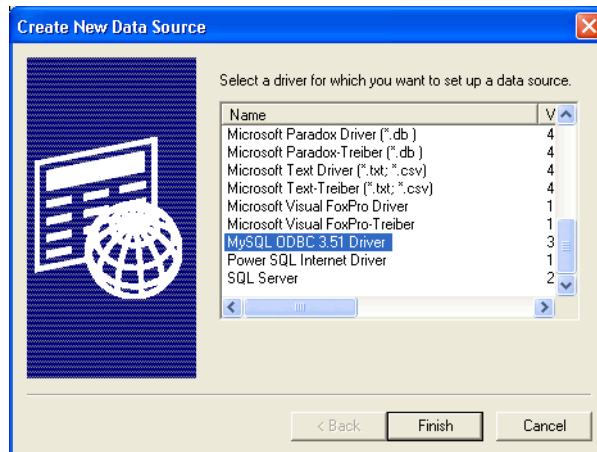
- 1 From the Windows **Control Panel**, select **Administrative Tools|Data Sources (ODBC)**.

The **ODBC Data Source Administrator** appears.



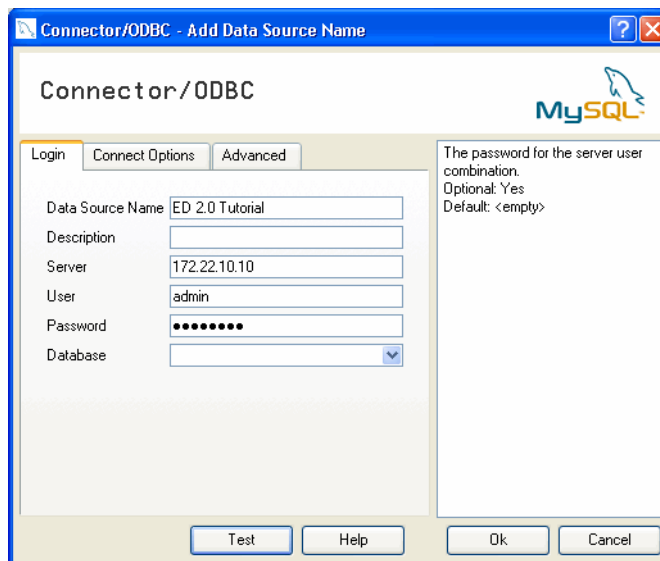
- In the **User DSN** tab, click **Add**.

The **Create New Data Source** dialog appears.



- In the list box select **MySQL ODBC**.
- Click **Finish**.

The **Connector/ODBC - Add Data Source Name** dialog appears.



- 5 Enter the following information:
  - The Windows Data Source Name (DSN). In the following example we have called it **ED 2.0 Tutorial**.
  - The name or IP address of the Enterprise Discovery server.
  - For the name of the user, enter the account name of anyone who has been set up with a user account
  - Enter the password for the above user.
  - In the **Database** name field, select the name of the database from the drop-down list.
- 6 Click on the **Connect Options** tab. For the number of the port, always enter **8108**.
- 7 Once you have entered these fields, click **OK**.

Now you are returned to the **UserDSN** tab in the **ODBC Data Source Administrator** dialog box.

- 8 Click **OK** to exit.

You are now ready to connect to the Enterprise Discovery database with applications such as MS Access by means of ODBC.

## Step 4: Create a new database in Microsoft Access 2000

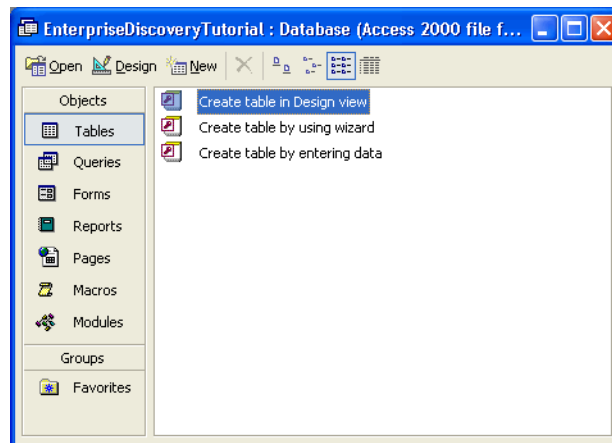
To create a new database

- 1 Start Microsoft Access.
- 2 Create a new blank database. Give it a name and save it.

The following screen is displayed. In this example, the database has been named **EnterpriseDiscoveryTutorial.mdb** and saved in the following directory

C:\Program Files\Peregrine\Enterprise Discovery\2.0.0\Common

The following dialog is displayed.

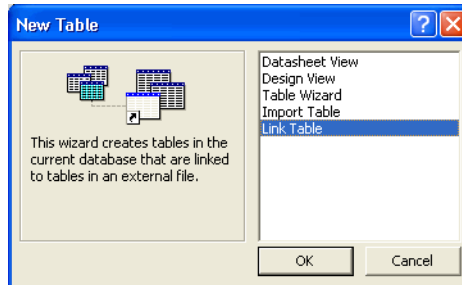


## Step 5: Link in the Enterprise Discovery tables

To link in the Enterprise Discovery tables

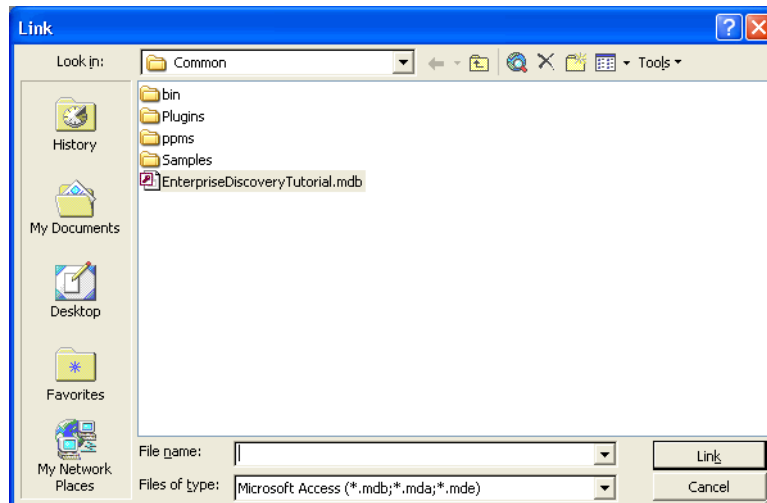
- 1 In the Objects menu, select **Tables** and click **New**.

The following dialog appears.



- 2 Select **Link Table** and click **OK**.

The following screen appears.

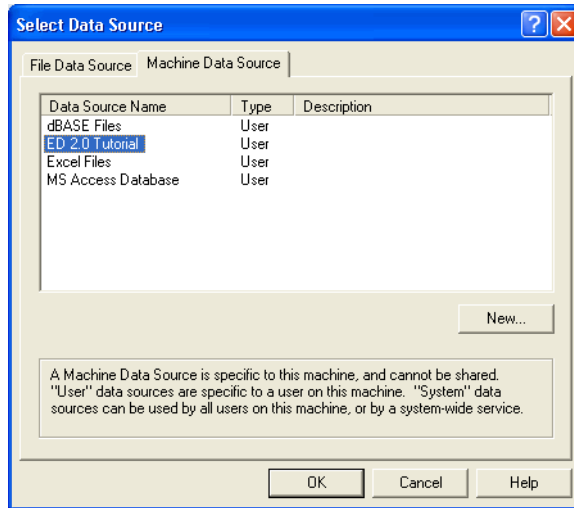


- 3 In the **Files of type** pull-down list, select **ODBC Databases**.

The following dialog appears.

**Note:** The **EnterpriseDiscoveryTutorial.mdb** file is not supplied with Enterprise Discovery, but is the file that you created in **Step 2** on page 70.

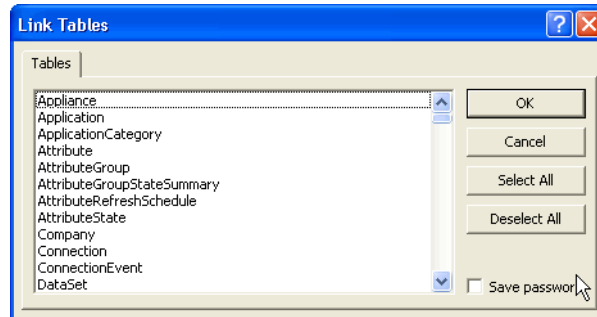
**4** Click the **Machine Data Source** tab.



**5** Select your entry (in this case **EnterpriseDiscoveryTutorial**) and click **OK**.

**Note:** Note, that this is the Tutorial data source name that you created on page 69.

The following **Link Tables** dialog is displayed.



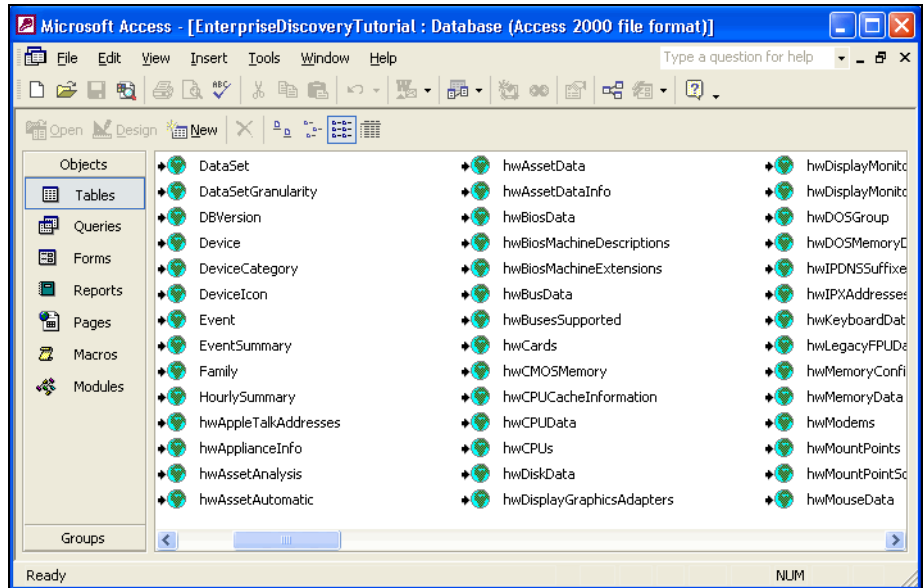


6 Click **Select All**.

All the entries are now highlighted.

7 Click **OK**.

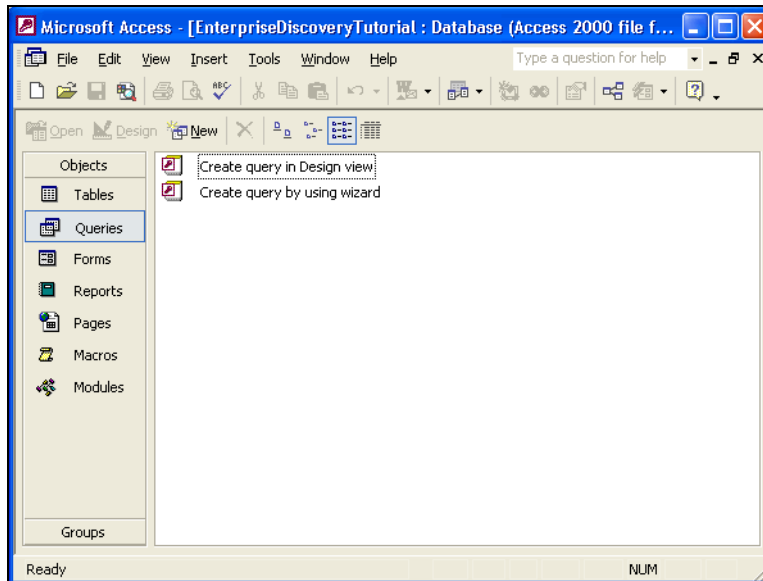
You are returned to the **Tables** Tab which shows the newly linked Enterprise Discovery tables.



## Step 6: Create a basic assets and recognition query

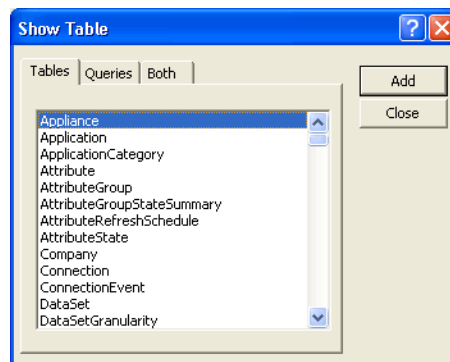
To create a basic assets and recognition query

- 1 From the **Objects** list, select **Queries**.



- 2 Double click **Create query in Design view**.

The **Show Table** dialog appears.



3 In the **Tables** tab page, from the list, select:

- hwAssetData
- Device
- hwCPUData
- hwRecognitionInfo
- hwSystemData

4 With the table selected, click Close.

The table appears.

5 Save the query. (In this example we have called it **Assets and Recognition**.)

## 6 Enter the query field parameters as shown below:

Microsoft Access - [Assets and Recognition : Select Query]

File Edit View Insert Query Tools Window Help

Type a question for help

hwAssetData

- Device\_ID
- hwAssetDescriptor
- hwAssetTag
- hwAssetEmployeeI
- hwAssetUserLastN

Device

- Device\_ID
- Device\_Discovered
- Device\_ManagedCe
- Device\_PREFERREDIP
- Device\_PREFERREDIP

hwCPUData

- Device\_ID
- hwCPUCount
- hwPhysicalCPUCount

hwRecognitionInfo

- Device\_ID
- hwFilesTotal
- hwFilesProcessed
- hwFilesRecognised
- hwFilesUnrecognised

hwSystemD...

- Device\_ID
- hwScanCmdLir
- hwCreationMe
- hwScannerDes
- hwScanDate
- hwScannerVer
- hwScannerVer
- hwScannerBuil

hwSystemData\_1

- Device\_ID
- hwScanCmdLine
- hwCreationMethod
- hwScannerDescription
- hwScanDate
- hwScannerVersionMajor
- hwScannerVersionMinor
- hwScannerBuild

Field:	Device_ID	hwAssetTag	hwAssetDescription	hwScanDate	hwCPUCount	hwFilesRecognised
Table:	hwAssetData	hwAssetData	hwAssetData	hwSystemData	hwCPUData	hwRecognitionInfo
Sort:						
Show:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Criteria:						
or:						

Ready NUM

## 7 Run the Query. From the **Query** pull-down menu, select **Run**.

A query is generated, showing asset and recognition data from the inventory scans in the Inventory Database.

Microsoft Access - [Query1 : Select Query]

Type a question for help

Device_ID	hwAssetTag	hwAssetDescription	hwScanDate	hwCPUCount	hwFilesRecognise
56	0010F3043879	0010F3043879 - Pentium III, 700MHz, 128Mb	i/2005 23:40:28	1	0
58	Windows_2000_Profession	Windows_2000_Professional_7895 - Pentium III, 700MHz, 128Mb	i/2005 23:39:48	1	0
59	0010F30437F6	0010F30437F6 - Pentium III, 700MHz, 128Mb	i/2005 22:02:20	1	0
60	78Y0099	78Y0099 - Pentium III, 1133MHz, 1280Mb	i/2005 00:29:51	1	0
61	0010F30437CE_Nex01-16	0010F30437CE_Nex01-16 - Pentium III, 700MHz, 128Mb	i/2005 22:38:10	1	0
62	0010F304372D	0010F304372D - Pentium III, 700MHz, 128Mb	i/2005 23:38:56	1	0
66	6118FCM4A100	() - Pentium III, 866MHz, 512Mb	i/2005 14:57:20	1	2105
67	0010F3043874	0010F3043874 - Pentium III, 700MHz, 128Mb	i/2005 23:40:58	1	0
68	0010F304385C	0010F304385C - Pentium III, 700MHz, 128Mb	i/2005 23:42:23	1	0
69	_0010F304389D	_0010F304389D - Pentium III, 700MHz, 128Mb	i/2005 23:37:08	1	0
70	0010F304B044	0010F304B044 - Pentium III, 1200MHz, 128Mb	i/2005 04:58:01	1	0
72	0010F304388C	0010F304388C - Pentium III, 700MHz, 128Mb	i/2005 02:00:46	1	0
73	0010F3043757	0010F3043757 - Pentium III, 700MHz, 128Mb	i/2005 23:10:56	1	0
74	0010F3043780_Nex10-04	0010F3043780_Nex10-04 - Pentium III, 700MHz, 128Mb	i/2005 17:41:36	1	0
75	0010F304B030	0010F304B030 - Pentium III, 1200MHz, 128Mb	i/2005 23:18:18	1	0
76	KCMC1FW	KCMC1FW - Pentium 4, 3000MHz, 1536Mb	i/2005 08:51:03	2	0
77	6107FCM4A173	6107FCM4A173 - Pentium III, 866MHz, 256Mb	i/2005 17:13:55	1	0
165	0010F30437E1	0010F30437E1 - Pentium III, 700MHz, 128Mb	i/2005 04:27:33	1	0
172	0010F30437ED	0010F30437ED - Pentium III, 700MHz, 128Mb	i/2005 23:32:37	1	0
176	0010F30438C8	0010F30438C8 - Pentium III, 700MHz, 128Mb	i/2005 02:04:33	1	0
179	NEX03-01	NEX03-01 - Pentium III, 700MHz, 128Mb	i/2005 10:19:04	1	0
182	0010F3043778	0010F3043778 - Pentium III, 700MHz, 128Mb	i/2005 23:38:44	1	0

Record: 60

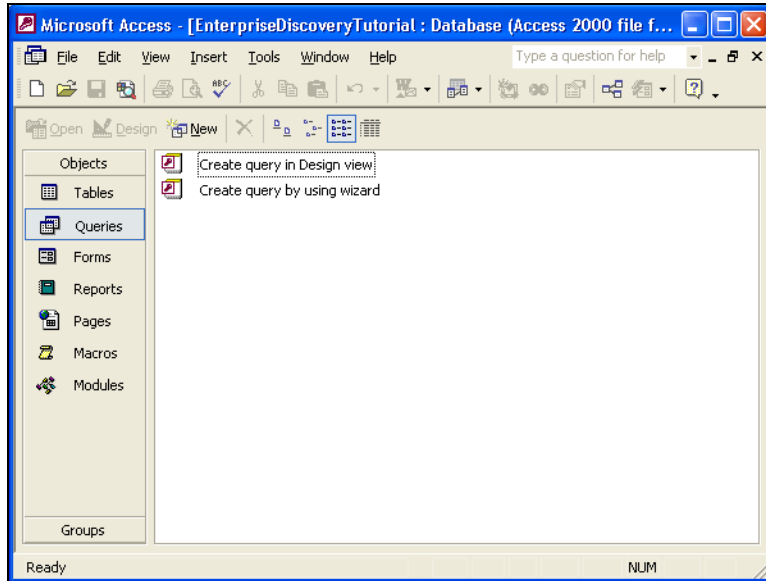
Datasheet View

NUM

## Step 7: Create a basic license query

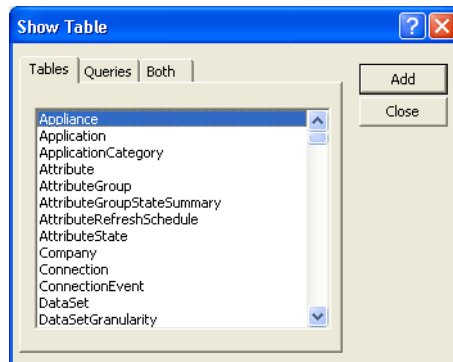
To create a basic license query

- 1 From the **Objects** list, select **Queries**.



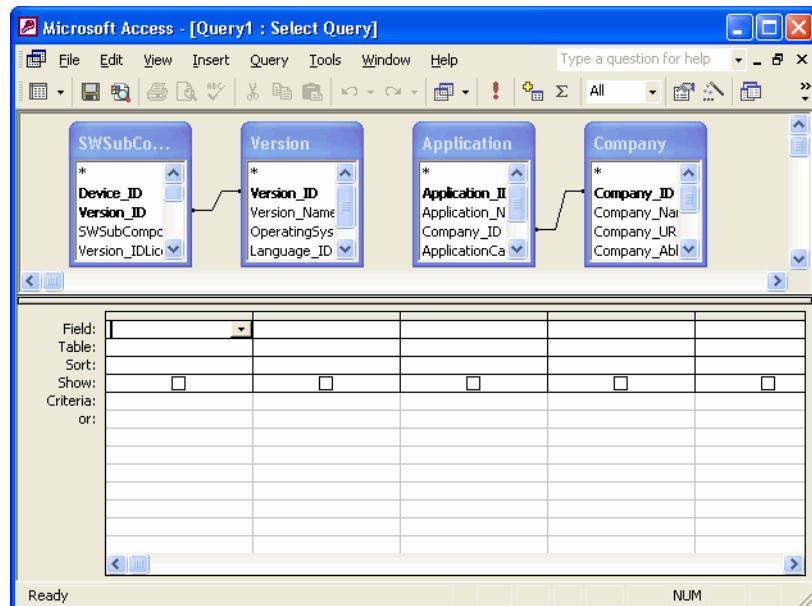
- 2 Double click **Create query in Design view**.

The **Show Table** dialog appears.



- 3 In the **Tables** tab page, select:
  - SWSubComponent
  - Version
  - Application
  - Company
- 4 With the table selected, click **Add**, then **Close**.

The table displayed is similar to this:



- 5 Click **File > Save As** and save the query

In this example, we have called it **Licenses**.

## 6 Enter the query field parameters as shown below:

The screenshot shows the 'Licenses : Select Query' dialog box. It contains four tables: SWSubComponent, Version, Application, and Company. SWSubComponent is linked to Version, and Application is linked to Company. Below the tables is a query grid with columns for Field, Table, Total, Sort, Show, and Criteria.

Field:	Company_Name	Application_Name	Version_Name	SWSubComponent_LicenceRequired	SWSubComponent_LicenceRequired
Table:	Company	Application	Version	SWSubComponent	SWSubComponent
Total:	Group By	Group By	Group By	Count	Group By
Sort:					
Show:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Criteria:					
or:					

## 7 Run the Query. From the **Query** pull down menu, select the **Run** option.

A query is generated, showing license data from the inventory scans in the Inventory Database.





# 8 Deleting Data

## CHAPTER

This section is for Administrator accounts only.

Do not perform these procedures unless you completely understand the consequences.

**Important:** If you are working on an Aggregator server, you can only delete the data native to the Aggregator. To delete the data associated with a remote server, you must delete the remote server. For more information, see the *Configuration and Customization Guide*.

---

## Deleting data

This procedure will delete all of your network and configuration data. Once you complete this operation, your server will appear as it did when you first installed Enterprise Discovery.

**Warning:** Deleting network data stored on your server is an extremely drastic action that cannot be undone. Consider making an external backup of your data first. See the *Installation and Initial Setup Guide*.

Performing this delete means that you will delete all of the following:

- **Network data:** the Enterprise Discovery database of your network devices are deleted, along with device statistics, and reports.
- **Account Information:** all accounts and passwords.
- **Configuration:** all configuration settings from the Administration menu.

- **Backup:** all backup files.
- **Scanners:** all scanners that you have created with the Scanner Generator.

After performing the data delete, your server will appear as it did when you first installed Enterprise Discovery.

### To delete Enterprise Discovery data:

- 1 Click **Administration > Data management > Delete data.**
- 2 Click **Delete Data.**

Send e-mail when data deletion done:  Yes  No

E-mail address:

Delete Data



# 9 Reports

## CHAPTER

Enterprise Discovery reports comprise the following groups:

- [Executive/Summary Network Reports on page 83](#)
- [Scanned Machine Reports on page 84](#)

---

## 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

- **Reports > Network Documentation > Device Inventory Summary**
- **Or 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 in more detail.

The following Reports are available:

Folder	Report	Type
Network Documentation	Network Classification	pie graph, table
	Network Devices by Function	pie graph, table
	End Nodes by Function	pie graph, table
	Device Inventory Summary	table
	Device Inventory by Category	list
	Device Inventory by UNSPSC	pie graph, table
	Device Inventory by Virtual LAN	table
	Port Inventory by Virtual Lan	table
	Device Inventory	list

## Scanned Machine Reports

### Scanned Machine Summaries

These reports display summary counts of the scanned machines grouped by different machine properties. For example, machines 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 machines which belong to the summary group clicked on.

**Note:** 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 machines by Division, Location, and Department.

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

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

## Summary Report By Location, Division, Department

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

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

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

## Summary Report By Department, Location

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

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

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

## Summary Report By Location, Building, Floor

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

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

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

## Summary Report By Location, Cost Center

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

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

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

## Summary Report By Cost Center, Location

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

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

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

## Summary Report By Operating System Category

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

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

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

## Summary Report By Hardware Chassis Type

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

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

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

## Application Reports

These reports display software application licence 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 machines 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.

## Licence Counts by Application

This summary report displays all applications by publisher and application with counts of licences 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 licences, sorted by number of licences. 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 licences 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 licences.

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





# Index

**PEREGRINE**

## A

- Access Query, Creating 74, 78
- advanced Find 12
- Agent Ping
  - Device Manager button 46
- Aggregate Alarms Viewer 20
- Aggregate Events Browser 28
- Aggregate Find 13
- Aggregate Health Panel 18
- Alarm Type panel (Port Manager) 61
- alarms 19
- Alarms Viewer 19
- asset tag 12

## C

- Cascade Database
  - Using With Microsoft Access 70
- Category
  - Events Browser list box 26
- clearing the database 40, 58
- Close
  - Device Manager 51
  - Port Manager 62
- Configuration
  - Device Manager panel 32
  - Port Manager panel 55
- contact, system 34
- Creating An Access query 74, 78

## D

- data
  - clearing 40, 58
- data access applications
  - ODBC 65
- deleting data 81
- device
  - icon 55
  - model 49
  - title 11
- Device Manager
  - Agent Ping 46
  - Configuration 32
  - Device Visibility 50
  - Diagnosis 39
  - DNS Query 46
  - Events 47
  - IP Ping 44
  - Ports 47
  - Properties 51
  - reports 38
  - Scan Data 47
  - SNMP Ping 45
  - Telnet 48
  - toolbar 30
  - Traceroute 44
  - Update Model 49
  - Web 48
- device title 12
- Device Visibility button (Device Manager) 50

## Diagnosis

- Device Manager panel 39
- Port Manager panel 58

DNS Query button (Device Manager) 46

domain name 12

Duplex Mode panel (Port Manager) 62

**E**

Easy Find 9

## Events

- Device Manager panel 47
- Port Manager panel 59

Events Browser 23–28

Category 26

Limit 27

Newer 27

Older 27

Executive/Summary Reports 83

exporting data

saving to text file 21

**F**

family 12

Find 9

advanced 12

**H**

Health Panel 16

aggregator 18

alarm list 17

hide inactive alarms 17

Hide Inactive Alarms 17

HTTP session 47, 48

**I**

Interface Rate panel (Port Manager) 60

Interface Type panel (Port Manager) 60

IP address

multiple 37

IP Ping

Device Manager button 44

**L**

Limit

Events Browser text box 27

Linking Cascade Tables 71

location, system 34

**M**

model 12

multiple IP addresses 37

My User Alarms Only 17

**N**

name, system 34

NetBIOS name 12

NetBIOS workgroup 12

network function 12

Newer button

Events Browser 27

**O**

object properties 51

Older button

Events Browser 27

operating system 12

**P**

ping button (Device Manager) 44

port index list box (Port Manager) 63

Port Manager

Alarm Type 61

Configuration 55

Diagnosis 58

Duplex Mode 62

Events 59

Interface Rate 60

Interface Type 60

port index 63

Purge Port 60

Reports 57

toolbar 54

Ports panel (Device Manager) 47

Print button

Device Manager 51

Port Manager 62

Properties

Device Manager button 51

properties

object 51

Purge Port (Port Manager) 60

## R

Refresh button

Device Manager 51

Events Browser 27

Port Manager 62

Reports 83–88

business

executive/summary 83

Reports (Device Manager) 38

Reports (Port Manager) 57

## S

Save Table Data 21

Scan Data

Device Manager button 47

SNMP contact 12

SNMP description 12

SNMP location 12

SNMP name 12

SNMP Ping

Device Manager button 45

SNMP serial number 12

speed, line

see Interface Rate

system contact 34

system location 34

system name 34

## T

Telnet

Device Manager button 48

text file, saving data to 21

ticket 12

title

device 11

toolbar

Device Manager 30

Port Manager 54

Traceroute

Device Manager button 44

## U

Update Model button (Device Manager) 49

## V

VLAN 37

## W

Web

Device Manager button 48





