8e6 Technologies

8e6® Enterprise Reporter

USER GUIDE

Administrator Console

Model: ER 4.0

Release 4.1.20 • Manual Version 1.01

8E6 ENTERPRISE REPORTER ADMINISTRATOR USER GUIDE

© 2008 8e6 Technologies
All rights reserved.
828 W. Taft Ave., Orange, CA 92865, USA

Version 1.01, published January 2008 for software release 4.1.20

Printed in the United States of America

This document may not, in whole or in part, be copied, photocopied, reproduced, translated, or reduced to any electronic medium or machine readable form without prior written consent from 8e6 Technologies.

Every effort has been made to ensure the accuracy of this document. However, 8e6 Technologies makes no warranties with respect to this documentation and disclaims any implied warranties of merchantability and fitness for a particular purpose. 8e6 Technologies shall not be liable for any error or for incidental or consequential damages in connection with the furnishing, performance, or use of this manual or the examples herein. Due to future enhancements and modifications of this product, the information described in this documentation is subject to change without notice.

The latest version of this document can be obtained from http://www.8e6.com/docs/er4server.pdf.

Trademarks

Other product names mentioned in this manual may be trademarks or registered trademarks of their respective companies and are the sole property of their respective manufacturers.

Part# ER4-SUG_v1.01-0801

CONTENTS

ENTERPRISE REPORTER OVERVIEW 1

Operations 1

How to Use this User Guide 2
Organization 2
Conventions 3
Terminology 4

ADMINISTRATOR SECTION 8

Introduction 8

Components and Environment 10
Components 10
Hardware 10
Software 10
Environment 11
Workstation Requirements 11
Network Requirements 11

Chapter 1: Accessing the Server 12
Preliminary Network Settings 12
Procedures for Accessing the Server 12
Procedures for Logging On, Off the Server 13
Log On 13
Logging on the First Time 14
Specify the Server's function 15
Set up an Administrator Login ID 16
Log Off 17

Chapter 2: Configuring the ER Server 19
Administrator Console 19
Network Menu 20
Box Mode screen 21
Live Mode 21
Archive Mode 21
Change the Box Mode 22

Add/Edit/Delete Administrators screen 23
View a List of Administrators 24
Add an Administrator 24
Edit an Administrator's Login ID 24
Delete an Administrator 25
Locked-out Accounts and IPs screen 26
View Locked Accounts, IP addresses 27
Unlock Accounts, IP addresses 27
Network Settings screen 28
Set up/Edit IP Addresses 29
Routing Table screen 30
View a List of Routers 30
Add a Router 31
Delete a Router 31
Regional Setting screen 32
Specify the Time Zone 33
Specify the Language Set 33
Specify Network Time Protocol Servers 33
Update the Time on the Server 34
Network Diagnostics screen 35
Ping 36
Trace Route 37
SNMP screen 39
Enable SNMP 40
Set up Community Token for Public Access 40
Create, Build the Access Control List 40
Maintain the Access Control List 40
Server Menu 41
Backup screen 42
Backup and Recovery Procedures 42
Set up/Edit External Backup FTP Password 44
Execute a Manual Backup 44
Perform a Remote Backup 45
Perform a Restoration to the ER Server 46
Self Monitoring screen 47
View a List of Contact E-Mail Addresses 48
Set up and Activate Self-Monitoring 48
Remove Recipient from E-mail Notification List 48
Deactivate Self-Monitoring 48
SMTP Server Setting screen 49
Enter, Edit SMTP Server Settings 49

Verify SMTP Settings....50
Server Status screen....51
View the Status of the Server....52
Secure Access screen....53
Activate a Port to Access the Server....54
Terminate a Port Connection....55
Terminate All Port Connections....55
Software Update screen....56
View Installed Software Updates....57
Uninstall the Most Recently Applied Software Update....57
View Available Software Updates....57
Install a Software Update....58
Software Update Setting screen....61
Select the Transfer Protocol....61
Specify Proxy Settings....62
FTP: Specify Transfer Type....62
Save Settings....62
Shut Down screen....63
Server Action Selections....63
Perform a Server Action....64
NIC Mode screen....65
View the NIC Negotiation....66
Modify the NIC Mode Setting....66
Web Client Server Management screen....67
Restart the Web Client Server....68
Enable/Disable Web Client Server Access....68
Enable/Disable the Web Client Scheduler....68
Hardware Failure Detection screen....69
View the Status of the Hard Drives....69
Database Menu....71
User Name Identification screen....71
View the User Name Identification screen....74
Set up a Customized Label for Unidentified Machines....74
Configure the Server to Log User Activity....74
Deactivate User Name Identification....75
Username Display Setting screen....76
View the Current Username Display Setting....77
Modify the Username Display Setting....77
Page View Elapsed Time screen....79
Establish the Unit of Elapsed Time for Page Views....79
Elapsed Time Rules....80

Page Definition screen 81
View the Current Page Types 81
Remove a Page Type 82
Add a Page Type 82
Tools screen 83
View Diagnostic Reports 84
View Database Status Logs 84
Expiration screen 87
Expiration Screen Terminology 88
Expiration Rules 89
View Data Storage Statistics 90
Change Data Storage Settings 93
NAS Status screen 95
View NAS Status Information 96
Optional Features screen 96
Enable Search String Reporting 98
Enable Block Request Count 98
Enable Wall Clock Time 98
Enable Page and/or Object Count 99
Enable, Configure Password Security Option 100
User Group Import screen 102
Import User Groups 102

TECHNICAL SUPPORT / PRODUCT WARRANTIES 104

Technical Support 104
Hours 104
Contact Information 104
Domestic (United States) 104
International 104
E-Mail 104
Office Locations and Phone Numbers 105
8e6 Corporate Headquarters (USA) 105
8e6 Taiwan 105
Support Procedures 106

Product Warranties 107
Standard Warranty 107
Technical Support and Service 108
Extended Warranty (optional) 109
Extended Technical Support and Service 109

APPENDICES SECTION 110

Appendix A 110
Evaluation Mode 110
Administrator Console 110
Use the Server in the Evaluation Mode.....112
Expiration screen.....112
Change the Evaluation Mode.....113
Activation Page.....114

Appendix B 116
Disable Pop-up Blocking Software 116
Yahoo! Toolbar Pop-up Blocker 116
Add the Client to the White List 116
Google Toolbar Pop-up Blocker 118
Add the Client to the White List 118
AdwareSafe Pop-up Blocker 119
Disable Pop-up Blocking 119
Windows XP SP2 Pop-up Blocker 120
Set up Pop-up Blocking 120
Use the Internet Options dialog box.....120
Use the IE Toolbar 122
Set up the Information Bar.....123
Access the Client.....123

Appendix C 125
RAID Maintenance 125
Part 1: Hardware Components 125
Part 2: Server Interface 126
LED indicators in SL and HL units 126
Front control panels on H, SL, and HL units 128
Rear panels on H and HL units.....130
Part 3: Troubleshooting 131
Hard drive failure.....131
Step 1: Review the notification email.....131
Step 2: Verify the failed drive in the Admin console ...132
Step 3: Replace the failed hard drive.....133
Step 4: Rebuild the hard drive 134
Step 5: Contact Technical Support.....134
Power supply failure.....134
Step 1: Identify the failed power supply.....134

Step 2: Unplug the power cord 134
Step 3: Replace the failed power supply 135
Step 4: Contact Technical Support 135
Fan failure 136
Identify a fan failure 136

INDEX 137

ENTERPRISE REPORTER OVERVIEW

Though many companies have Internet filtering solutions to prevent employees from accessing inappropriate, non-work related Web sites, simply blocking these sites is not enough. Administrators want the ability to know who is accessing which site, the duration of each site visit, and the frequency of these visits. This data can help administrators identify abusers, develop policies, and target sites to be filtered, in order to maximize bandwidth utilization and productivity.

The Enterprise Reporter (ER) from 8e6 Technologies is designed to readily obtain this information, giving the user the ability to interrogate massive datasets through flexible drill-down technology, until the desired view is obtained. This "view" can then be memorized and saved to a user-defined report menu for repetitive, scheduled execution and distribution.

Operations

In simplified terms, the ER operates as follows: the ER Server accepts log files (text files containing Web access data) from a source device such as the 8e6 R3000 Enterprise Filter. 8e6's proprietary programs "normalize" the transferred data and insert them into a MySQL database. The ER Client reporting application accesses this database to generate a virtually unlimited number of queries and reports.

How to Use this User Guide

Organization

This User Guide is organized into the following sections:

- **Overview** - This section provides information on how to use this user guide to help you configure the ER Server.
- **Administrator Section** - Refer to this section for information on configuring and maintaining the ER Server via the Administrator console application.
- **Tech Support / Product Warranties Section** - This section contains information on technical support and product warranties.
- **Appendices Section** - Appendix A provides information on how to use the ER Server in the evaluation mode, and how to switch to the activated mode. Appendix B explains how to disable many types of pop-up blocking software. Appendix C includes information about RAID maintenance and troubleshooting on an ER “H”, “SL”, or “HL” server.
- **Index** - This section includes an index of topics and the first page numbers where they appear in this user guide.

Conventions

The following icons are used throughout this user guide:

***NOTE**: The "note" icon is followed by italicized text providing additional information about the current topic.*

***TIP**: The "tip" icon is followed by italicized text giving you hints on how to execute a task more efficiently.*

***WARNING**: The "warning" icon is followed by italicized text cautioning you about making entries in the application, executing certain processes or procedures, or the outcome of specified actions.*

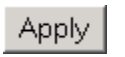
***IMPORTANT**: The "important" icon is followed by italicized text informing you about important information or procedures to follow to ensure maximum uptime on the ER Server.*

Terminology

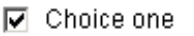
The following terms are used throughout this user guide. Sample images (not to scale) are included for each item.

- **alert box** - a message box that opens in response to an entry you made in a dialog box, window, or screen. This box often contains a button (usually labeled “OK”) for you to click in order to confirm or execute a command.

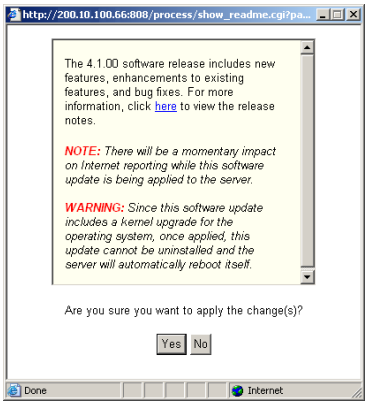
- **button** - an object in a dialog box, window, or screen that can be clicked with your mouse to execute a command.



- **checkbox** - a small square in a dialog box, window, or screen used for indicating whether or not you wish to select an option. This object allows you to toggle between two choices. By clicking in this box, a check mark or an “X” is placed, indicating that you selected the option. When this box is not checked, the option is not selected.



- **dialog box** - a box that opens in response to a command made in a window or screen, and requires your input. You must choose an option by clicking a button (such as “Yes” or “No”, or “Next” or “Cancel”) to execute your command. As dictated by this box, you also might need to make one or more entries or selections prior to clicking a button.

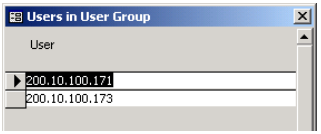


- **field** - an area in a dialog box, window, or screen that either accommodates your data entry, or displays pertinent information. A text box is a type of field.

- **frame** - a boxed-in area in a dialog box, window, or screen that includes a group of objects such as fields, text boxes, list boxes, buttons, radio buttons, and/or tables. Objects within a frame belong to a specific function or group. A frame often is labeled to indicate its function or purpose.

- **list box** - an area in a dialog box, window, or screen that accommodates and/or displays entries of items that can be added or removed.

- **pop-up box** or **pop-up window** - a box or window that opens after you click a button in a dialog box, window, or screen. This box or window may display information, or may require you to make one or more entries. Unlike a dialog box, you do not need to choose between options.



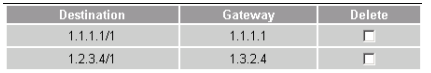
- **pull-down menu** - a field in a dialog box, window, or screen that contains a down arrow to the right. When you click the arrow, a menu of items displays from which you make a selection.

- **radio button** - a small, circular object in a dialog box, window, or screen used for selecting an option.

This object allows you to toggle between two choices. By clicking a radio button, a dot is placed in the circle, indicating that you selected the option. When the circle is empty, the option is not selected.

- **screen** - a main object of an application that displays across your monitor. A screen can contain windows, frames, fields, tables, text boxes, list boxes, buttons, and radio buttons.

- **table** - an area in a window or screen that contains items previously entered or selected.



Destination	Gateway	Delete
1.1.1.1/1	1.1.1.1	☐
1.2.3.4/1	1.3.2.4	☐

- **text box** - an area in a dialog box, window, or screen that accommodates your data entry. A text box is a type of field.

- **window** - displays on a screen, and can contain frames, fields, text boxes, list boxes, buttons, and radio buttons. Types of windows include ones from the system such as the Save As window, pop-up windows, or login windows.

ADMINISTRATOR SECTION

Introduction

The authorized administrator of the ER Server is responsible for integrating the Server into the existing network, and providing the Server a high speed connection to the designated logging device(s) and remote Client workstations. To attain this objective, the administrator performs the following tasks:

- executes Quick Start procedures defined in the ER Quick Start Guide booklet packaged with the ER Server
- provides a suitable environment for the Server, including:
  - high speed, File Transfer Protocol (FTP) link to the current logging device
  - power connection protected by an Uninterruptible Power Supply (UPS)
  - high speed access to the Server by authorized Client workstations
- adds new administrators
- sets up administrators for receiving automatic alerts
- updates the Server with software updates supplied by 8e6
- analyzes Server statistics
- utilizes diagnostics for monitoring the Server status to ensure optimum functioning of the Server
- establishes and implements backup and restoration procedures for the Server

Instructions on configuring and maintaining the ER Server are documented in this section.

***NOTES**: This user guide is accessible via the **Help** link beneath the banner in any screen in the Administrator console.*

*Information about the ER Client can be found in the ER Web Client User Guide that can be obtained from **http:// www.8e6.com/docs/er4_wclient.pdf**.*

Components and Environment

Components

Hardware

- High performance server
- One or more high-capacity hard drives
- Optional: One or more attached “NAS” storage devices (e.g. Ethernet connected SCSI connected “SAN”)

Software

- Linux OS
- Administrator Graphical User Interface (GUI) console utilized by an authorized administrator to configure and maintain the ER Server
- MySQL database
- 8e6 Technologies proprietary Client application employed by report users for generating “views” and reports

Environment

Workstation Requirements

- Windows 2000, NT 4.0, or XP operating system
- Internet Explorer (IE) Version 6.0 or later
- Pop-up blocking software, if installed, must be disabled
- Session cookies from the ER Server must be allowed in order for the Administrator console to function properly

***NOTE**: Information about disabling pop-up blocking software can be found in Appendix B: Disable Pop-up Blocking Software.*

Network Requirements

- High speed connection from the ER Server to the Web access logging device(s)
- High speed connection from the ER Server to the Client workstation(s)

Chapter 1: Accessing the Server

Preliminary Network Settings

To initially set up your ER Server, follow the instructions in the ER Quick Start Guide booklet packaged with your ER unit. This guide explains how to perform the initial configuration of the Server so that it can be accessed via an IP address on your network.

***NOTE**: If you do not have the ER Administrator Quick Start Guide, contact 8e6 Technologies immediately to have a copy sent to you.*

***WARNING**: In order to prevent data from being lost or corrupted while the Server is running, the Server should be connected to a UPS or other battery backup system.*

Procedures for Accessing the Server

***WARNING**: Once you turn on the Server, **DO NOT** interrupt the initial boot-up process. This process may take from five to 10 minutes per drive. If the process is interrupted, damage to key files may occur.*

When the Server is fully booted, any workstation on the network that can access the Server's IP address (set up during Quick Start procedures) will be able to communicate with the Server via the Internet.

1. Launch Internet Explorer (IE).
2. In the address line of the IE browser window, type in the Server's IP address appended by the following port number:
   - ":88" for an HTTP address
   - ":8843" for an HTTPS address

For example, if your IP address is 1.2.3.4, type in ***http://1.2.3.4:88*** or ***https://1.2.3.4:8843***.

3. Click **Go** to open the login screen of the Administrator console application (see Fig. 1:1-1).

Procedures for Logging On, Off the Server

Log On

Fig. 1:1-1 Login screen

1. In the login screen, type in the generic User Name ***admin***, and Password ***reporter***, if you have not yet set up your own user name and password. Otherwise, enter your personal **User Name** and **Password**.
2. Click **Login** to go to the main screen of the Administrator console.

***NOTE**: When logging on the Server for the first time, the ER Status pop-up box opens, and the main screen displays with a message, as shown in the example in Logging on the First Time. Follow the directions in this sub-section before proceeding. (Refer to Appendix A: Evaluation Mode for information on using the ER Server in the evaluation mode, or for changing the Server from this mode to the activated mode.)*

If you are logging on during a subsequent session, the main screen displays as in Fig. 1:2-1. If you have not set up your own user name and password, see Set up an Administrator Login ID.

Logging on the First Time

If you are logging on the Administrator console for the first time, the main screen displays with a message that asks you to specify the Server's function:

Fig. 1:1-2 Administrator console, main screen, first-time access

Specify the Server's function

1. Click the appropriate radio button to specify the function of the Server:
   - choose **Live** if you wish the Server to function in the "live" mode, receiving and processing real time data from the Web access logging device.
   - choose **Archive** if you wish the Server to function in the "archive" mode, solely as a receptacle for historical, archived files. In this mode, "old" files placed on the Server can be viewed using the Client reporting application.
2. Click **Apply** to confirm your selection. The mode you specify will immediately be in effect.

***TIP**: After choosing the function for the ER Server box on the main screen, if you have not previously set up your own user name and password, you should do so before entering any Server settings.*

Set up an Administrator Login ID

***NOTE**: If you have already set up your user name and password, you can skip this section.*

1. At the Network pull-down menu, choose **Administrators** to display the Add/Edit/Delete Administrators screen where you will set up your user name and password:

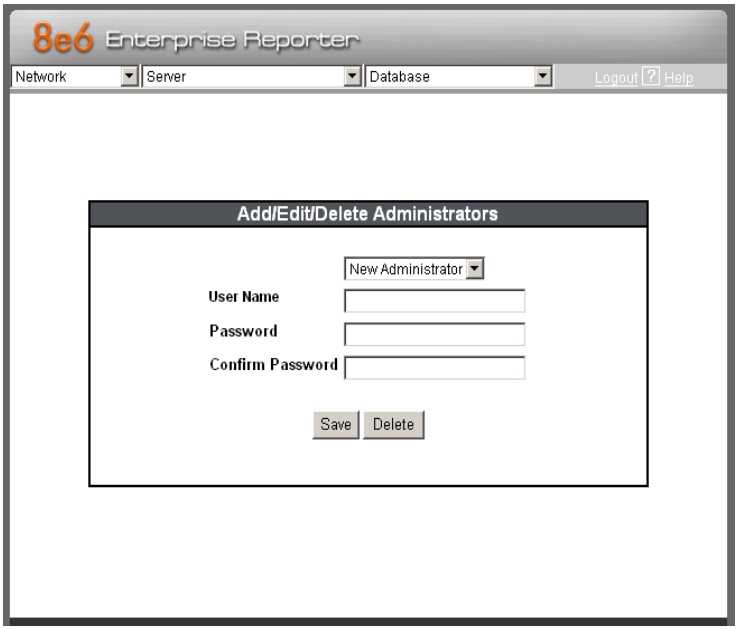


Fig. 1:1-3 Add/Edit/Delete Administrators screen

2. Select **New Administrators** from the pull-down menu.
3. In the **User Name** field, enter up to 20 characters—this may include upper- and/or lowercase alphanumeric characters, and special characters.
4. In the **Password** field, enter eight to 20 characters—including at least one alpha character, one numeric character, and one special character. The password is case sensitive.

5. In the **Confirm Password** field, re-enter the password in the exact format used at the Password field.
6. Click the **Save** button.

Log Off

To log off the Administrator console, click the **Logout** link beneath the banner in any screen to display the log out screen:

Fig. 1:1-4 Logout screen

Click the “X” in the upper right corner of the browser window to close the window. Exiting the Administrator console will log you off the Server, but will not turn off the Server.

***WARNING**: If you need to turn off the Server, follow the shut down procedures outlined in the Shut Down screen sub-section under the Server Menu section in Chapter 2. Failure to properly shut down the Server can result in data being lost or corrupted.*

Chapter 2: Configuring the ER Server

Administrator Console

After logging on the Server, the main screen of the Administrator console displays in your Web browser:

Fig. 1:2-1 Administrator console, main screen

The Administrator console is used for configuring and maintaining the ER Server. Settings made in the Administrator console affect the Client reporting application. On the main screen of the Administrator console, there are three menus: Network, Server, and Database. Each menu contains options from which you make selections to access screens used for configuring your Server.

***NOTE**: The mode of the Server displays on the main screen. More information about the "live" and "archive" Server box modes can be found in the Box Mode sub-section under the Network Menu section in this chapter.*

***TIP**: When making a complete configuration of the Server, 8e6 Technologies recommends you navigate from left to right (Network to Server to Database) in choosing your menu options.*

Network Menu

The Network pull-down menu includes options for setting up and maintaining components to be used on the Server's network. These options are: Box Mode, Administrators, Lockouts, Network Setting, Routing Table, Regional Setting, Diagnostics, and SNMP.

Fig. 1:2-2 Network menu, main screen

Box Mode screen

The Box Mode screen displays by default when you first log on the Server, or when the Box Mode option is selected from the Network menu. (See Figs. 1:2-1 and 1:2-2.) The box mode indicates whether the Server box is functioning in the "live" mode, or in the "archive" mode. When the box mode displays on the screen, you can view the current mode set for the Server, and can change this setting, if necessary.

***NOTE**: When accessing the Box Mode screen for the first time, the ER Status pop-up box opens to inform you that the ER unit is currently in the evaluation mode. To continue using the box in the evaluation mode, click the "X" in the upper right corner to close the pop-up box. (Refer to Appendix A: Evaluation Mode for information on using the Server in the evaluation mode, or for changing from this mode to the activated mode.)*

Live Mode

Once your Server is configured and the Server box is set in the "live" mode, it will receive and process real time data from the Web access logging device. The Client reporting application can then be used to capture data and create views.

Archive Mode

In the "archive" mode, the Server box solely functions as a receptacle in which historical, archived files are placed. In this mode, "old" files placed on the Server can be viewed using the Client reporting application.

Change the Box Mode

1. Click the **Change Mode** button to display the two box mode options on the screen:

Fig. 1:2-3 Change Box Mode

2. Click the radio button corresponding to **Live** or **Archive** to specify the mode in which the Server should function.
3. Click the **Apply** button to confirm your selection. The "new" mode will be in effect after the Server is restarted.

***NOTE**: After applying the box mode setting, you must restart the Server by selecting the **Restart Hardware** option on the Shut Down screen. (See the Shut Down sub-section under the Server menu section in this chapter.)*

Add/Edit/Delete Administrators screen

The Add/Edit/Delete Administrators screen displays when the Administrators option is selected from the Network menu. This screen is used for viewing, adding, editing, and deleting the login ID of personnel authorized to configure the Server. For security purposes, administrators should be the first users set up on the Server.

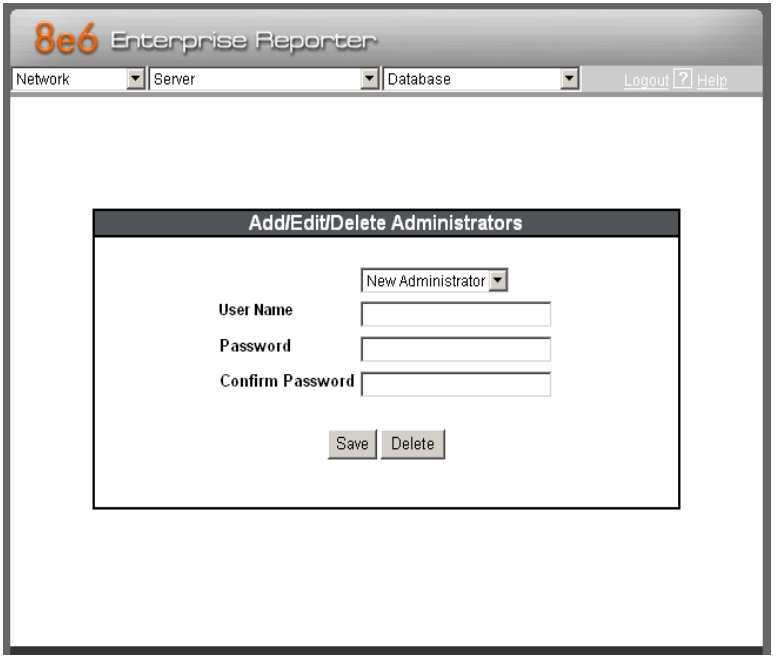


Fig. 1:2-4 Add/Edit/Delete Administrators screen

***TIP**: 8e6 recommends adding an alternate login ID prior to editing or deleting the default login ID. By doing so, if one login ID fails, you have another you can use.*

View a List of Administrators

To view a list of administrator user names, click the down arrow at the **New Administrator** field. If no administrator has yet been assigned to the Server, no selections display except for the default “admin” user name.

Add an Administrator

1. Select **New Administrator** from the pull-down menu.
2. In the **User Name** field, enter up to 20 characters—this may include upper- and/or lowercase alphanumeric characters, and special characters.
3. In the **Password** field, enter eight to 20 characters—including at least one alpha character, one numeric character, and one special character. The password is case sensitive.
4. In the **Confirm Password** field, re-enter the password in the exact format used in the Password field.
5. Click the **Save** button to add the administrator to the choices in the pull-down menu.

Edit an Administrator’s Login ID

1. Select the administrator’s user name from the pull-down menu.
2. Edit either of the following fields:
   - User Name
   - Password (if this field is edited, the Confirm Password field must be edited in tandem)
3. Click the **Save** button.

Delete an Administrator

1. Select the administrator's user name from the pull-down menu.
2. After the administrator's login ID information populates the fields, click the **Delete** button to remove the administrator's user name from the choices in the pull-down menu.

Locked-out Accounts and IPs screen

The Locked-out Accounts and IPs screen displays when the Lockouts option is selected from the Network menu. This screen is used for unlocking accounts or IP addresses of administrators and sub-administrators that are currently locked out of the Administrator console or Web Client.

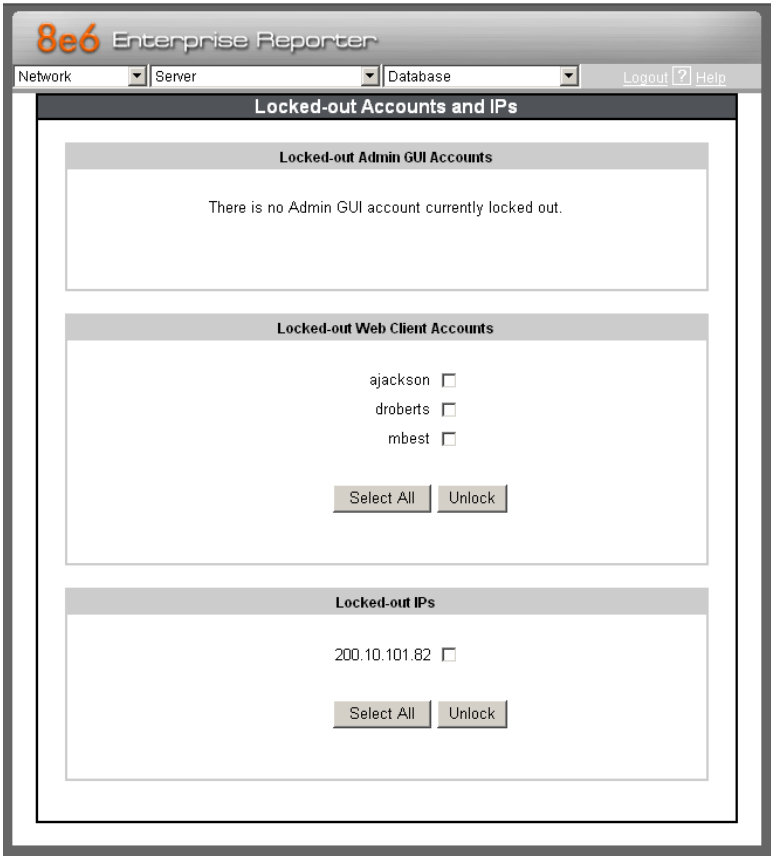


Fig. 1:2-5 Locked-out Accounts and IPs screen

***NOTE**: An account or IP address becomes locked if the Password Security Options feature is enabled in the Optional Features screen, and a user is unable to log into the Administrator console or Web Client due to a password expiration, or having met the specified number of failed password attempts within the designated timespan.*

View Locked Accounts, IP addresses

The frames in this screen display the following messages if there are no users currently locked out:

- **Locked-out Admin GUI Accounts** - There is no Admin GUI account currently locked out.
- **Locked-out Web Client Accounts** - There is no Web client account currently locked out.
- **Locked-out IPs** - There is no IP currently locked out.

If there are any locked accounts/IP addresses in a frame, each locked username/IP address displays on a separate line followed by a checkbox. The Select All and Unlock buttons display at the bottom of the frame.

Unlock Accounts, IP addresses

To unlock an account/IP address in a frame:

1. Click the checkbox corresponding to the username/IP address.

***TIP**: To unlock all accounts/IPs in a frame, click **Select All** to populate all checkboxes in the frame with check marks.*

2. Click **Unlock** to unlock the specified accounts/IPs, and to display the message screen showing one of the following pertinent messages for each unlocked account/IP:
   - Admin account: ‘xxx’ has been successfully unlocked.
   - Web client account: ‘xxx’ has been successfully unlocked.

- IP: ‘x.x.x.x’ has been successfully unlocked.

***NOTE**: In the text above, ‘xxx’ and ‘x.x.x.x’ represents the unlocked username/IP address.*

3. Click **OK** to return to the Locked-out Accounts and IPs screen that no longer shows the accounts/IPs that have been unlocked.

Network Settings screen

The Network Settings screen displays when the Network Setting option is selected from the Network menu. This screen is used for setting up IP addresses so the Server can communicate with your system.

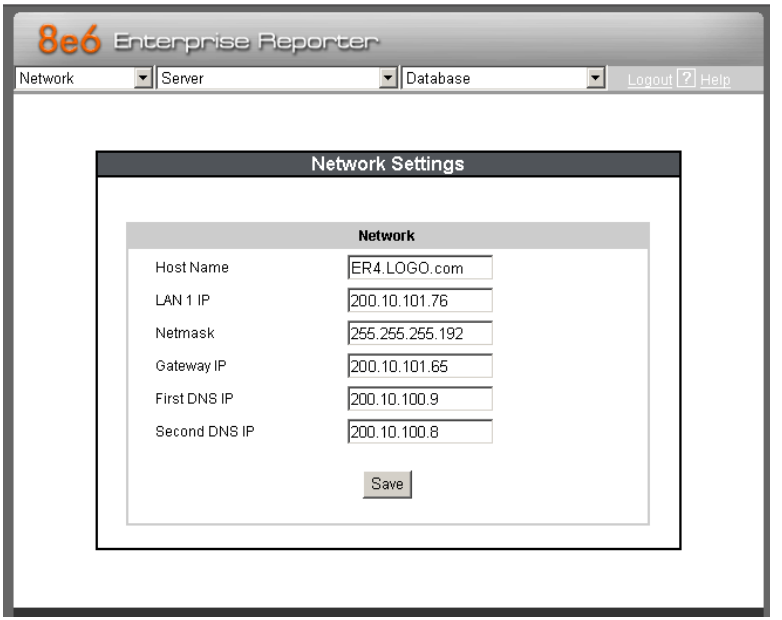


Fig. 1:2-6 Network Settings screen

Set up/Edit IP Addresses

***TIP**: In order for the Server to effectively communicate with your system, be sure all fields contain accurate information before saving your settings.*

1. Enter or edit an IP address in each appropriate field:
   - In the **Host Name** field, enter the address or URL that will be used for accessing the Administrator console. This entry should include the full, qualified domain name, and the "host" name for the box (i.e. reporter.myserver.com).
   - In the **LAN 1 IP** field, enter the IP address of the ER Server on your Local Area Network (LAN 1).
   - In the **Netmask** field, enter the netmask that will define the traffic designated for the LAN.
   - In the **Gateway IP** field, enter the IP address for the default router that will be the main gateway for the entire network segment.
   - In the **First DNS IP** field, enter the IP address of the primary Domain Name System (name server). The Server box will use this IP address to identify other IP addresses on the system, including its own IP address.
   - In the **Second DNS IP** field, enter the IP address of the fallback DNS.
2. Be sure each IP address is correct, and then click **Save**.

***NOTE**: After appropriate entries have been made in these fields and saved, you must restart the Server to activate the IPs. To restart the Server, select the **Restart Hardware** option on the Shut Down screen. (See the Shut Down sub-section under the Server menu section in this chapter.)*

Routing Table screen

The Routing Table screen displays when the Routing Table option is selected from the Network menu. This screen is used for viewing, building, and maintaining a list of routers—network destination and gateway IP addresses—the Server will use for communicating with other segments of the network. You will only need to set up a routing table if your local network is interconnected with another network.

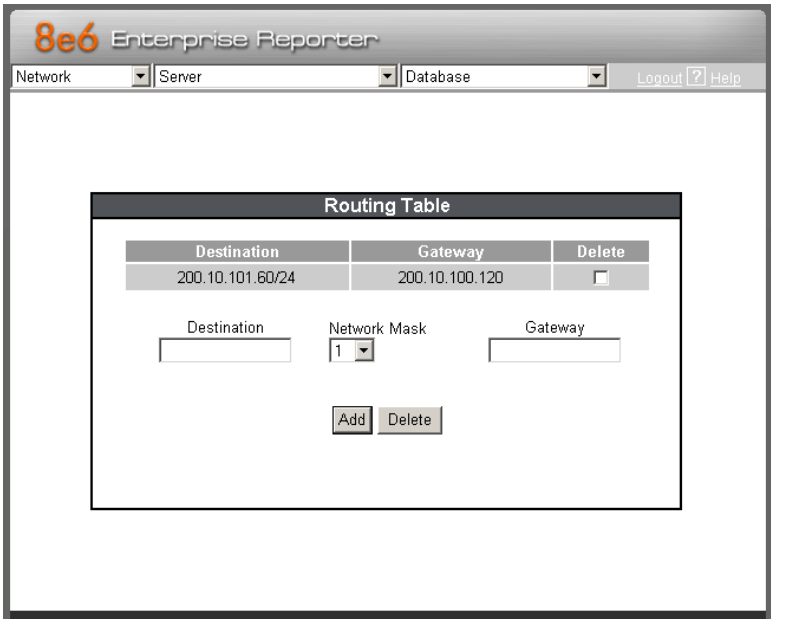


Fig. 1:2-7 Routing Table screen

View a List of Routers

Each router that was configured in the routing table displays as a separate row in the table. The IP address and subnet mask to receive data packets display in the Destination column, and the IP address of the portal that will transfer data packets to and from the Internet displays in the Gateway column.

Add a Router

1. In the **Destination** field, enter the IP address of the network to which data packets will be forwarded.
2. At the **Network Mask** pull-down menu, specify the number (1-32) of the subnet mask that will be used for grouping IP addresses on the same local network.
3. In the **Gateway** field, enter the IP address of the portal to which data packets will be transferred to and from the Internet.
4. Click the **Add** button to include your entry in the table. If you have another router to add, follow steps 1-4.
5. Click the **Back** button on the confirmation screen to return to the Routing Table screen.

Delete a Router

1. Click in the **Delete** checkbox of the row corresponding to the router you wish to remove from the routing table.
2. Click the **Delete** button.
3. Click the **Back** button on the confirmation screen to return to the Routing Table screen.

Regional Setting screen

The Regional Setting screen displays when the Regional Setting option is selected from the Network menu. This screen is used for specifying the time zone and network time to be used by the Server when generating reports via the Client application, and setting the language set type to be displayed in the Administrator console, if necessary.

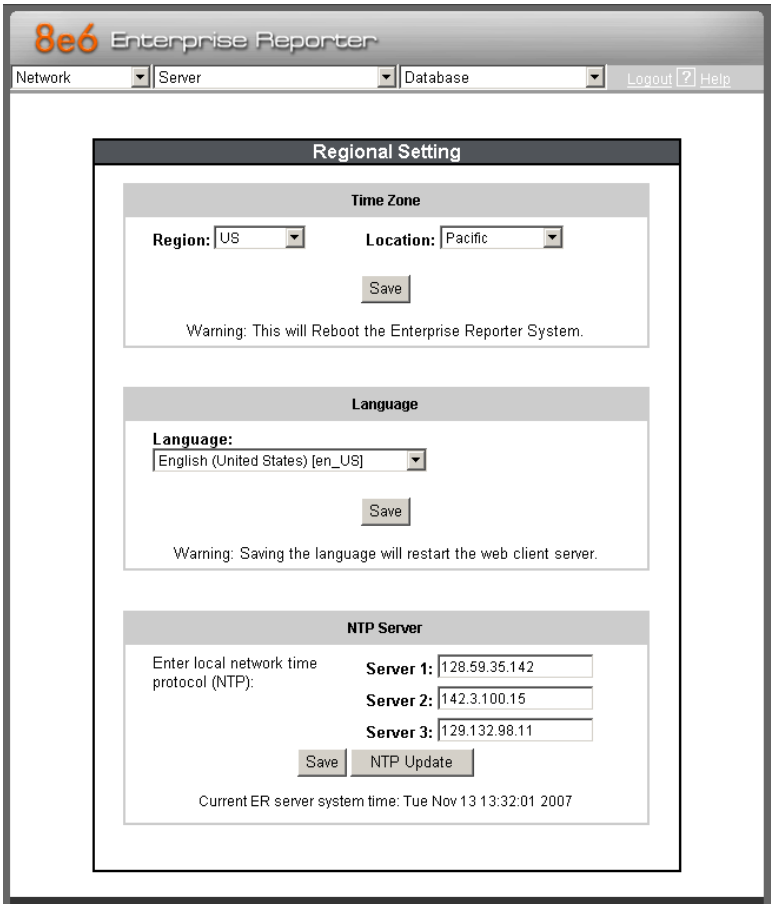


Fig. 1:2-8 Regional Setting screen

Specify the Time Zone

1. At the **Region** pull-down menu, select your country from the available choices.
2. At the **Location** pull-down menu, select the time zone for the specified region.
3. Click **Save** to apply your settings, and to restart the Web Client Server.

***WARNING**: The time zone set for the ER should be the same one set for each Web access logging device to be used by the ER. These "like" settings ensure consistency when tracking the logging times of all users on the network.*

Specify the Language Set

1. If necessary, select a language set from the **Language** pull-down menu to specify that you wish to display that text in the console.
2. Click **Save** to apply your settings, and to restart the Web Client Server.

Specify Network Time Protocol Servers

IP addresses of servers running Network Time Protocol (NTP) software are entered in the Server fields, and the Current ER server system time (day, date, HH:MM:SS time format, and year) displays below. NTP is a time synchronization system for computer clocks throughout the Internet. Your ER Server will use the actual time from clocks at the IP addresses you've specified.

For the Enter local network time protocol (NTP) server fields, by default, the following IP addresses display in these three fields: 128.59.35.142, 142.3.100.15, and 129.132.98.11. If you wish to use different NTP servers, follow these steps:

1. Enter or edit an IP address in each appropriate field:
   - In the **Server 1** field, enter the IP address of the primary NTP server to be used for clock settings on your Server.
   - In the **Server 2** field, enter the IP address of the secondary NTP server. The time from this server will be used by your Server if the IP address for the primary server fails to be accessed by your Server.
   - In the **Server 3** field, enter the IP address of the tertiary NTP server. The time from this server will be used by your Server if the IP addresses for the primary and secondary servers fail to be accessed by your Server.
2. Click the **Save** button to save your entries.

***NOTE**: When you click the Save button, the IP addresses you entered are saved, but the time on your Server will not be synchronized with the NTP servers until you click the NTP Update button.*

Update the Time on the Server

After you have saved the IP addresses of NTP servers you wish your Server to access, click the **NTP Update** button to synchronize the clock on your Server with the NTP server clocks.

Network Diagnostics screen

The Network Diagnostics screen displays when the Diagnostics option is selected from the Network menu. This screen is used to help you identify and resolve problems with your network configuration, using the ping and trace route utility tools.

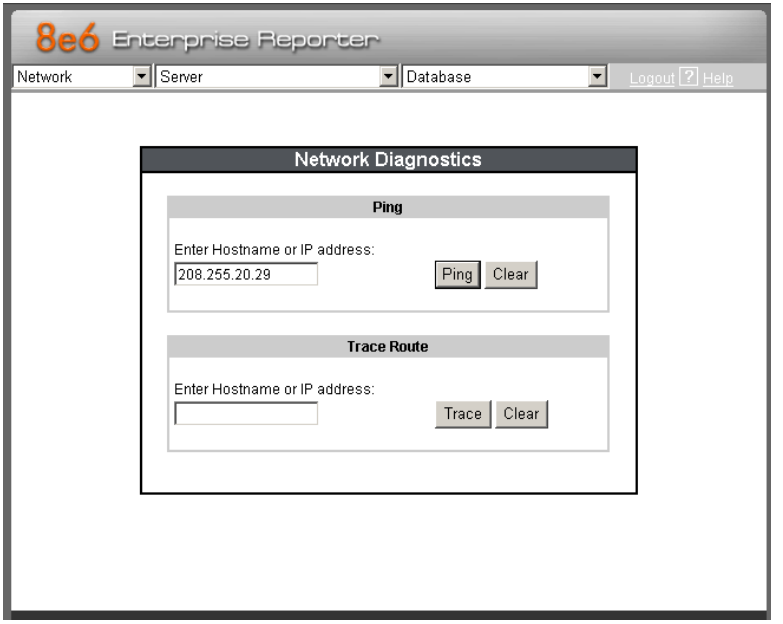


Fig. 1:2-9 Network Diagnostics screen, Ping entry

Ping

The ping utility is used for verifying whether the Server can communicate with a machine at a given IP address within the network, and the speed of the network connection.

1. In the Ping frame, enter the IP address or host name of the specific Internet address to be contacted (pinged).
2. Click the **Ping** button to display the results found by the Server, as shown on the sample screen:

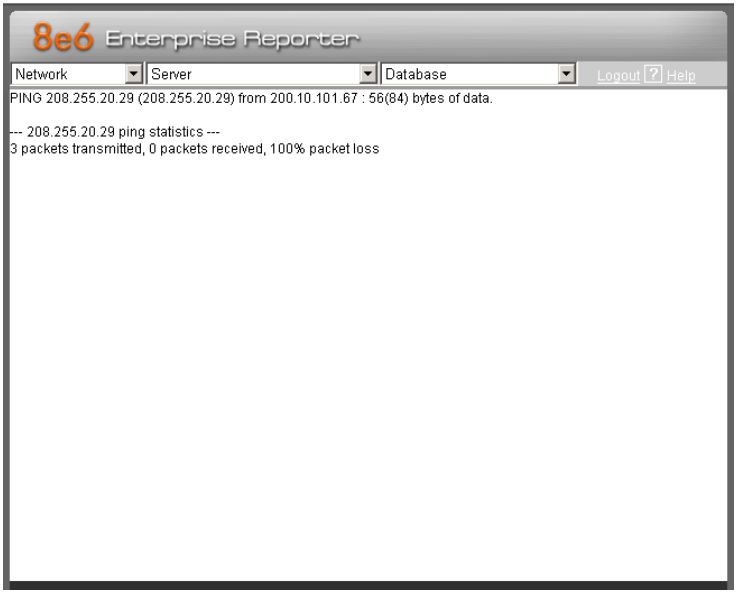


Fig. 1:2-10 Ping results

As indicated by the results for the sample entry, the Server at 206.255.20.29 was not able to communicate with the machine at the IP address 200.10.101.67. The statistics show that three (3) data packets were transmitted by the Server, but zero (0) packets were received by the designated machine, for a total of three (3) errors and a 100 percent packet loss.

***TIP**: If the machine cannot be contacted, be sure the ping feature on that machine is turned on.*

***NOTE**: To ping another IP address, click the Back button in your browser window, then click the Clear button in the Ping frame, and follow the procedures documented in this sub-section.*

Trace Route

If the ping utility was not able to help you diagnose the problem with your network configuration, you should use the trace route utility. This diagnostic tool records each “hop” (trip from one router to another) the data packet made, identifying the IP addresses of gateway computers where the packet stopped en route to its final destination, and the length of time of each hop.

***NOTE**: The trace route utility can be used after your routing table has been set up. To set up a routing table, see the Routing Table screen sub-section under the Network menu in this chapter.*

1. In the Trace Route frame, enter the IP address or host name of the specific Internet address to be validated.
2. Click the **Trace** button to display the results found by the Server, as shown on the sample screen:

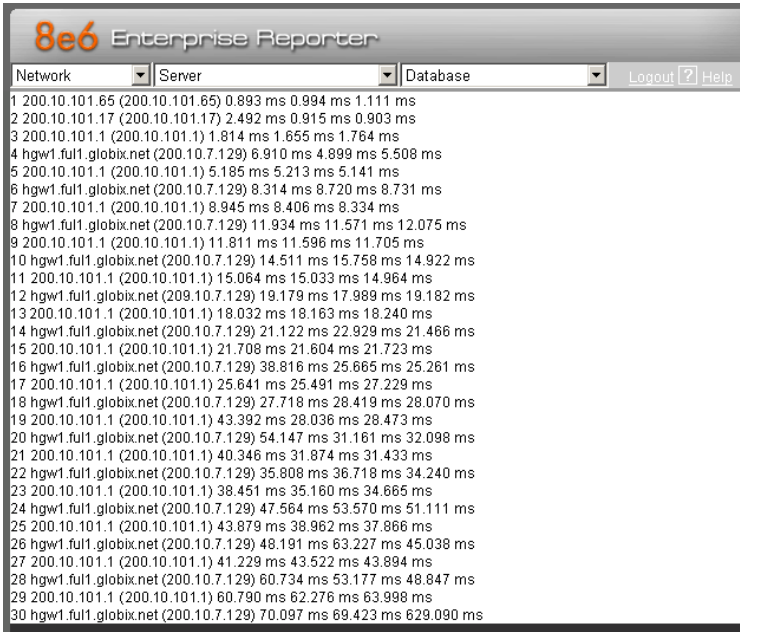


Fig. 1:2-11 Trace Route results

As indicated by the results for the sample entry, the packet made 30 hops. For each line in the report, the hop number displays, followed by the IP address or host name; the IP address in parentheses; and the maximum, minimum, and average response time in milliseconds.

***TIP**: To "trace" another IP address, click the Back button in your browser window, then click the Clear button in the Trace Route frame, and follow the procedures documented in this subsection.*

SNMP screen

The SNMP screen displays when the SNMP option is selected from the Network menu. This feature lets the global administrator use a third party Simple Network Management Protocol (SNMP) product for monitoring and managing the working status of the ER's Internet reporting on a network.

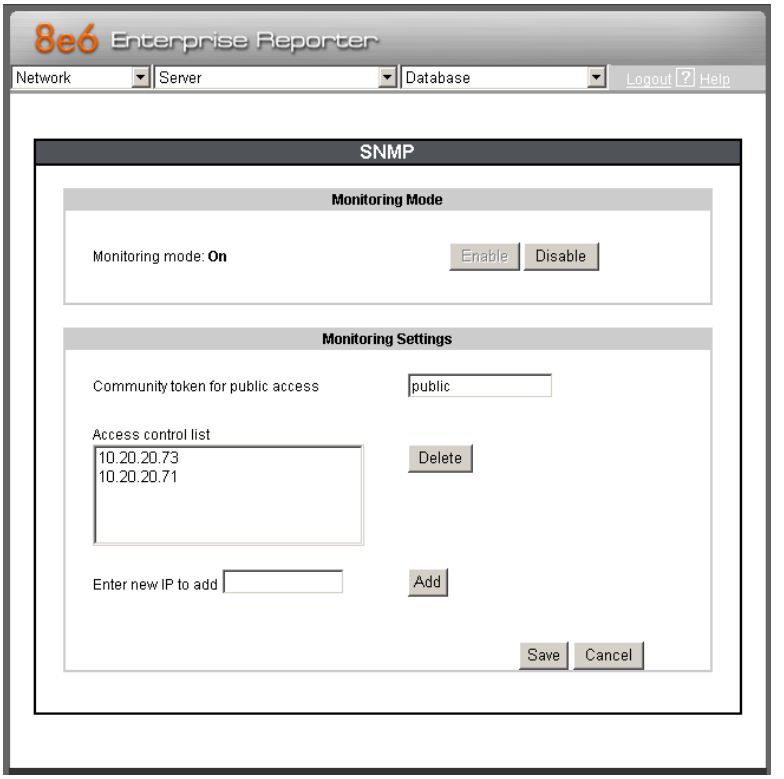


Fig. 1:2-12 SNMP screen

The following aspects of the ER are monitored by SNMP: data traffic sent/received by a NIC, CPU load average at a given time interval, amount of free disk space for each disk partition, time elapse since the box was last rebooted, and the amount of memory currently in usage.

Enable SNMP

The **Monitoring mode** is “Off” by default. To enable SNMP, click **Enable** in the Monitoring Mode frame. As a result, all elements in this window become activated.

Set up Community Token for Public Access

Enter the password to be used as the **Community token for public access**. This is the password that the management console would use when requesting access.

Create, Build the Access Control List

1. In the **Enter new IP to add** field, enter the IP address of an interface from/to which the SNMP should receive/send data.
2. Click **Add** to include the entry in the Access control list box.

   Repeat steps 1 and 2 for each IP address to be included in the list.
3. After all entries are made, click **Save**.

Maintain the Access Control List

1. To remove one or more IP addresses from the list, select each IP address from the Access control list, using the **Ctrl** key for multiple selections.
2. Click **Delete**.
3. Click **Save**.

Server Menu

The Server pull-down menu includes options for setting up processes for maintaining the Server. These options are: Backup, Self-Monitoring, SMTP Server Setting, Server Status, Secure Access, Software Update, Software Update Setting, Shut Down, NIC Mode, Web Client Server Management, and Hardware Failure Detection.

***NOTE**: The Software Update Setting option is only available if the R3000 unit is set up in the Stand Alone mode. See the Synchronization sub-section in the R3000 User Guide for more information about setup modes.*

Fig. 1:2-13 Server menu, main screen

Backup screen

The Backup screen displays when the Backup option is selected from the Server menu. This screen is used for setting up the password for the remote server's FTP account, for executing an immediate backup on the ER Server, and for performing a restoration to the database from the previous backup run.

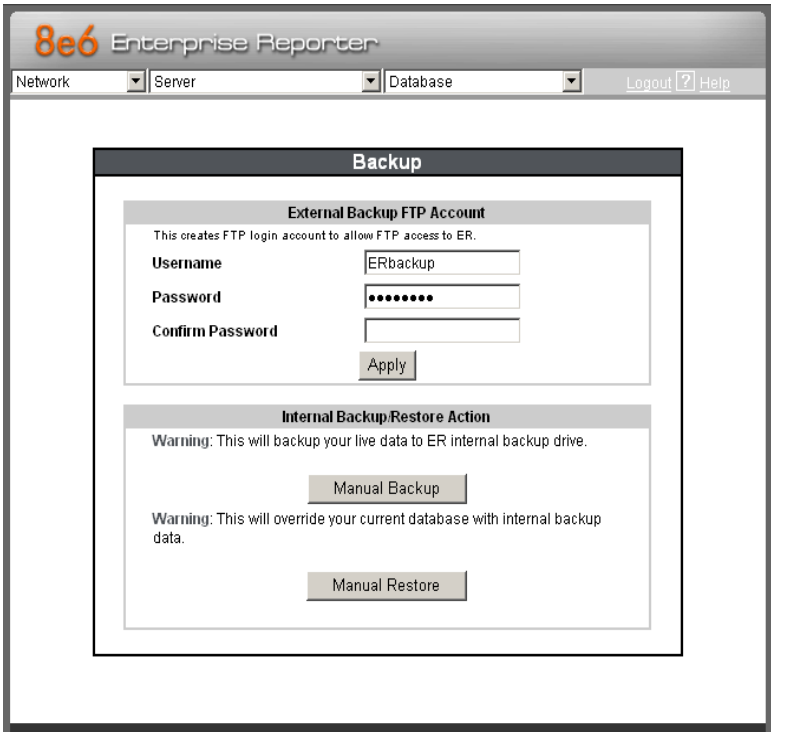


Fig. 1:2-14 Backup screen

Backup and Recovery Procedures

***IMPORTANT**: 8e6 recommends establishing backup and recovery procedures when you first begin using the ER Server. Please follow the advice in this section to ensure your ER Server is properly maintained in the event that data is lost and back up procedures need to be performed to recover data.*

Although automatic backups to a local ER hard drive are scheduled nightly by default, it is important that the ER administrator implements a backup policy to ensure data integrity and continuity in the event of any possible failure scenario. This policy should include frequent, remote backups, such that raw logs and ER database files are available for restoration without relying on the ER's hard drives.

In general, recovery plans involve (i) restoring the most recent backup of the database, and (ii) restoring raw logs to fill in the gap between the most recent backup of the database, and the current date and time.

Some scenarios and action plans to consider include the following:

- **The ER database becomes corrupted** - Correct the root problem. Restore the database from the most recent ER backup, and reprocess raw logs up to the current date and time.
- **The data drive fails** - Replace the data drive. Restore the database from the ER backup drive, and reprocess raw logs up to the current date and time.
- **The backup drive fails** - Replace the backup drive, and perform a manual backup.
- **Both data and backup drives are damaged** - Restore the database from the most recent remote backup, and reprocess raw logs up to the current date and time.

As you can see, it is critical that raw logs are available to bridge the gap between the last database backup and the present time, and more frequent backups (local and remote) result in less "catch-up" time required for reprocessing raw logs.

Set up/Edit External Backup FTP Password

In order to back up the ER Server's database to a remote server, an FTP account must be established for the remote server.

***NOTE**: In the External Backup FTP Account frame, the login name that will be used to access the remote server displays in the Username field. This field cannot be edited.*

1. In the **Password** field, enter up to eight characters for the password. The entry in this field is alphanumeric and case sensitive.
2. In the **Confirm Password** field, re-enter the password in the exact format used in the Password field.
3. Click the **Apply** button to save your entries. The updated Account ID will be activated after two minutes.

Execute a Manual Backup

In addition to performing on demand backups in preparation for a disaster recovery, you may wish to execute a manual backup under the following circumstances:

- **Power outage** - If there is a power outage at your facility and your system uses a backup battery, you might want to back up data before the battery fails.
- **Rolling blackout** - If your facility is subjected to rolling blackouts, and a blackout is scheduled during the time of your daily backup, you should back up your data before the blackout period, when the ER Server will be down.
- **Expiration about to occur** - If a data expiration is about to occur, you might want to back up your data before losing the oldest data on the ER Server, prior to the daily backup process.

***WARNING**: If corrupted data is detected on the ER Server, do not backup your data, as you may back up and eventually restore a corrupted database.*

When performing a manual backup, the ER's database is immediately saved to the internal backup drive. From the remote server, the backup database can be retrieved via FTP, and then stored off site.

***TIP**: 8e6 recommends executing an on demand backup during the lightest period of system usage, so the Server will perform at maximum capacity.*

1. Click the **Manual Backup** button in the Internal Backup/ Restore Action frame to specify that you wish to back up live data to the ER Server's internal backup drive.
2. On the Confirm Backup/Restore screen, click the **Yes** button to back up the database tables and indexes.

***WARNING**: 8e6 recommends that you do not perform other functions on the ER Server until the backup is complete. The time it will take to complete the backup depends on the size of all tables being saved.*

Perform a Remote Backup

After executing the manual backup, a remote backup can be performed on your remote server.

***NOTE**: Before beginning this FTP process, be sure you have enough space on the remote server for storing backup data. The required space can be upwards of 200 gigabytes.*

1. Log in to your FTP account.
2. Use FTP to download the ER Server's backup database to the remote server. When you are in the /backup/database/ directory, be sure to get all the *.data files to include in your backup. You can then go to the archive directory to get all the raw logs to include in your backup.
3. Store this backup data in a safe place off the remote server. If this backup database needs to be restored, it can be uploaded to the ER Server via FTP. (See Perform a Restoration to the Server.)

Perform a Restoration to the ER Server

There are two parts in performing a restoration of data to your ER Server. Part one requires data to be loaded on the remote server and then FTPed to the ER Server. Part two requires the FTPed data to be restored on the ER Server.

***NOTE**: Before restoring backup data to the ER Server, be sure you have enough space on the ER Server. Data that is restored to the ER Server will automatically include indexes.*

Perform these steps on the remote server:

1. Load the backup data on your remote server.
2. Log in to your FTP account.
3. FTP the backup data to the ER Server's internal backup drive.

On the ER Server's Backup screen:

1. Click the **Manual Restore** button in the Internal Backup/ Restore Action frame to specify that you wish to over-write data on the live ER Server with data from the previous, internal backup run.
2. On the Confirm Backup/Restore screen, click the **Yes** button to restore database tables and indexes to the ER Server.

***NOTE**: The amount of time it will take to restore data to the ER Server depends on the combined size of all database tables being restored. 8e6 recommends that you do not perform other functions on the ER Server until the restoration is complete.*

Self Monitoring screen

The Self Monitoring screen displays when the Self-Monitoring option is selected from the Server menu. This screen is used for setting up and maintaining e-mail addresses of contacts who will receive automated notifications if problems occur with the network. Possible alerts include situations in which a daemon stops running, software fails to run, corrupted files are detected, or a power outage occurs.

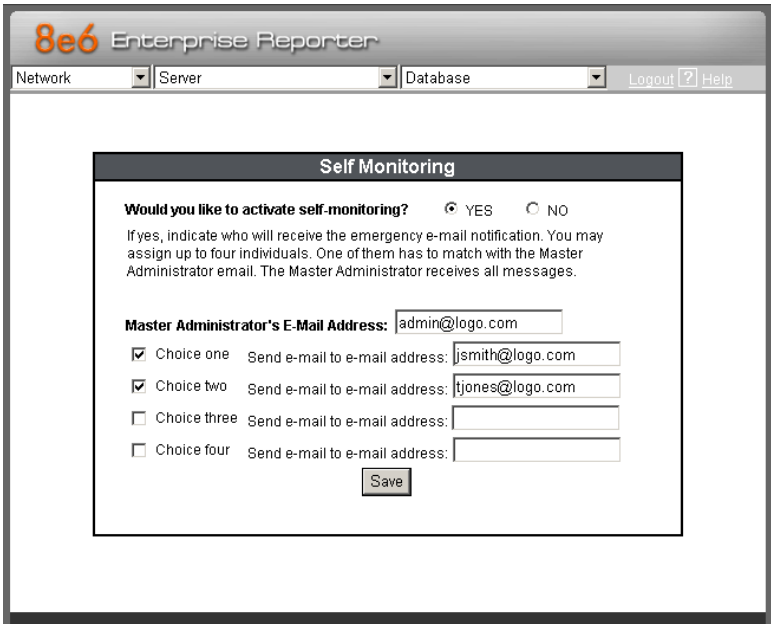


Fig. 1:2-15 Self Monitoring screen

As the administrator of the Server, you have the option to either activate or deactivate this feature. When the self-monitoring feature is activated, an automated e-mail message is dispatched to designated recipients if the Server identifies a failed process during its hourly check for new data.

View a List of Contact E-Mail Addresses

If this feature is currently activated, the e-mail address of the Master Administrator displays on this screen, along with any other contacts set up as Choice one - four.

Set up and Activate Self-Monitoring

1. Click the radio button corresponding to **YES**.
2. Enter the **Master Administrator's E-Mail Address**.
3. In the **Send e-mail to e-mail address** fields, enter at least one e-mail address of a person authorized to receive automated notifications. This can be the same address entered in the previous field. Entries in the three remaining fields are optional.
4. If e-mail addresses were entered in any of the four optional e-mail address fields, click in the **Choice one** - **Choice four** checkboxes corresponding to the e-mail address(es).
5. Click the **Save** button to activate self-monitoring.

Remove Recipient from E-mail Notification List

1. To stop sending emergency notifications to an e-mail address set up in the list, remove the check mark from the checkbox corresponding to the appropriate e-mail address.
2. Click the **Save** button to remove the recipient's name from the e-mail list. The Master Administrator and any remaining e-mail addresses in the list will continue receiving notifications.

Deactivate Self-Monitoring

1. Click the radio button corresponding to **NO**.
2. Click the **Save** button to deactivate self-monitoring.

SMTP Server Setting screen

The SMTP Server Setting screen is used for entering settings for the Simple Mail Transfer Protocol that will be used for sending email alert messages to specified administrators.

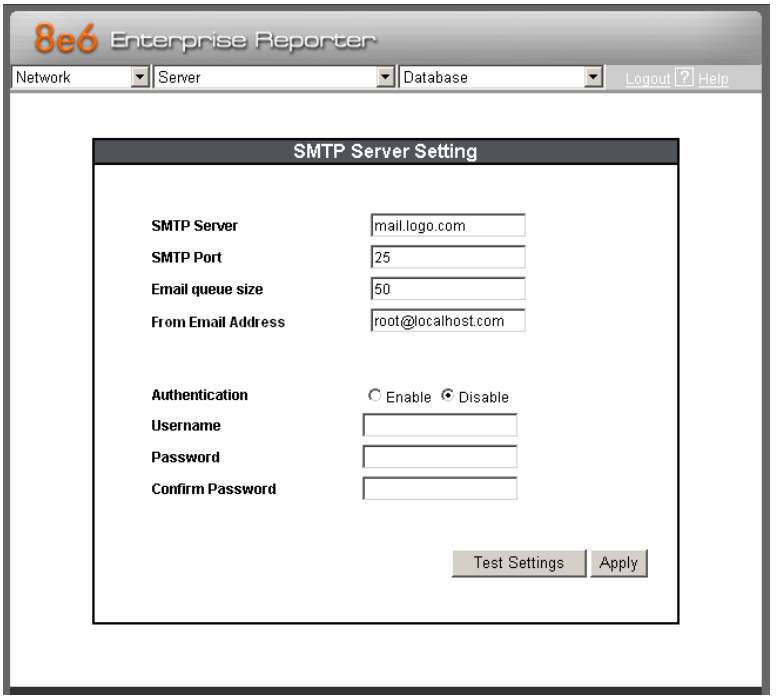


Fig. 1:2-16 SMTP Server Setting screen

Enter, Edit SMTP Server Settings

1. Enter the **SMTP Server** name, for example: **mail.logo.com**.
2. By default, the **SMTP Port** number used for sending email is *25*. This should be changed if the sending mail connection fails.

3. By default, the **Email queue size** is *50*. This can be changed to specify the maximum number of requests that can be placed into the queue awaiting an available outbound connection.
4. In the **From Email Address** field, enter the email address of the server that will be sending alert email messages to designated administrators.
5. By default, **Authentication** is disabled. Click “Enable” if a username and password are required for logging into the SMTP server. This action activates the fields below.

   Make the following entries:

   a. Enter the **Username**.

   b. Enter the **Password** and make the same entry in the **Confirm Password** field.
6. Click **Apply** to apply your settings.

Verify SMTP Settings

To verify that email messages can be sent to a specified address:

1. Click **Test Settings** to open the pop-up box:

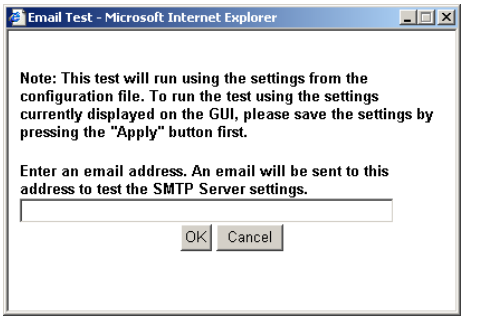


Fig. 1:2-17 SMTP Email Test box

2. Enter the email address in the pop-up box.

3. Click **OK** to close the pop-up box and to process your request. If all SMTP settings are accepted, the test email should be received at the specified address.

Server Status screen

The Server Status screen displays when the Server Status option is selected from the Server menu. This screen, which automatically refreshes itself every 10 seconds, displays the statuses of processes currently running on the Server, and provides information on the amount of space and memory used by each process.

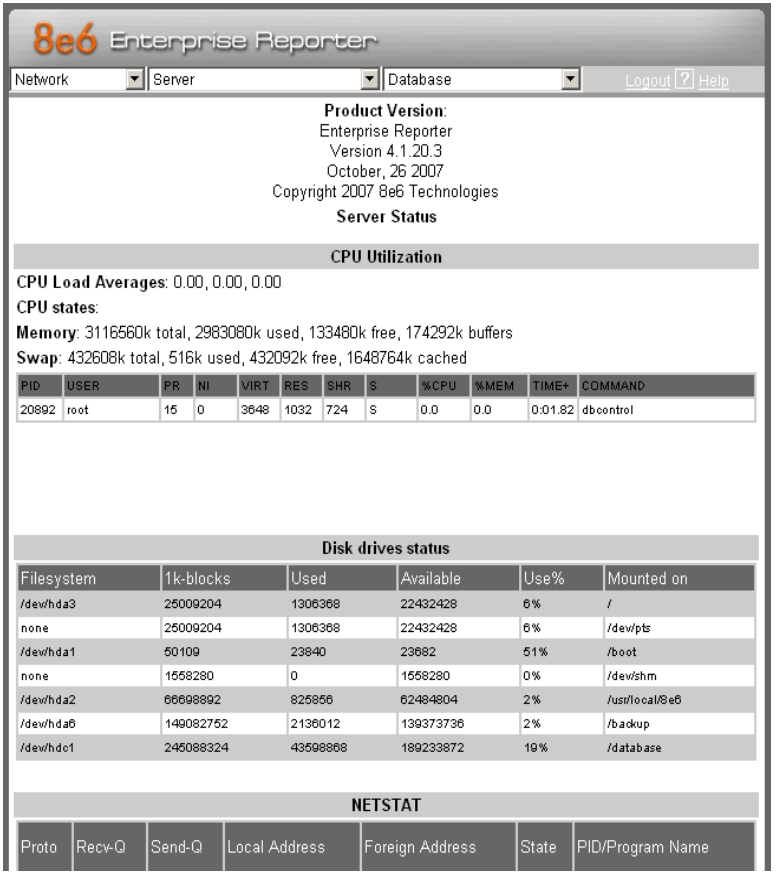


Fig. 1:2-18 Server Status screen

View the Status of the Server

The Product Version number of the software displays at the top of the screen, along with the date that software version was implemented. Status information displays in the following sections of this screen:

- CPU Utilization - includes CPU process data and information on the status of the top command
- Disk drives status - provides data on the status of each drive of the operating system
- NETSTAT - displays the status of a local IP address

Secure Access screen

The Secure Access screen displays when the Secure Access option is selected from the Server menu. This screen is primarily used by 8e6 technical support representatives to perform maintenance on your Server, if your system is behind a firewall that denies access to your Server.

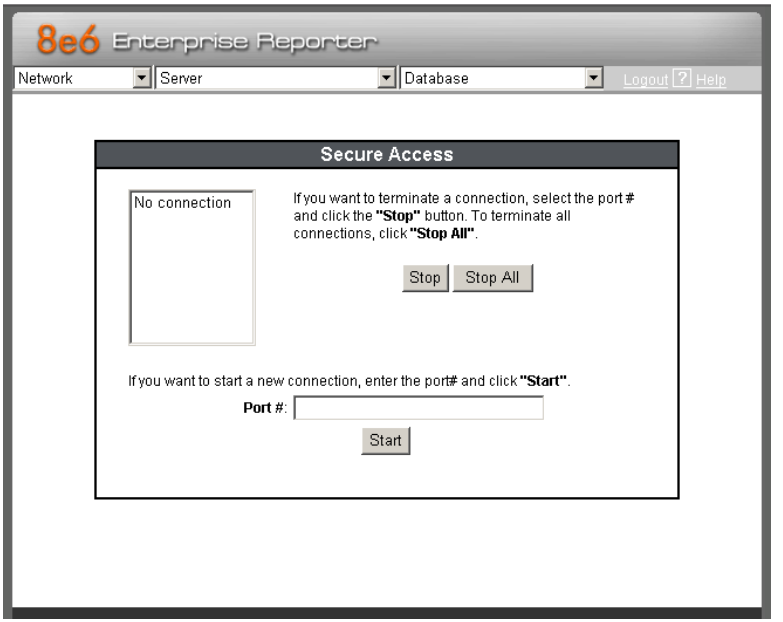


Fig. 1:2-19 Secure Access screen

Activate a Port to Access the Server

1. After the administrator at the customer's site authorizes you to use a designated port to access their Server, enter that number at the **Port #** field.
2. Click the **Start** button to activate the port. This action enters the port number in the list box above, replacing the text: "No connection".

Fig. 1:2-20 Port entries

Terminate a Port Connection

1. After maintenance has been performed on the customer's Server, select the active port number from the list box by clicking on it.
2. Click the **Stop** button to terminate the port connection. This action removes the port number from the list box.

Terminate All Port Connections

If more than one port is currently active on the customer's Server and you need to terminate all port connections, click the **Stop All** button. This action removes all port numbers from the list box.

Software Update screen

The Software Update screen displays when the Software Update option is selected from the Server menu. This screen is used for updating the Server with software updates supplied by 8e6, and for viewing a list of software updates that are available and/or previously installed on the Server.

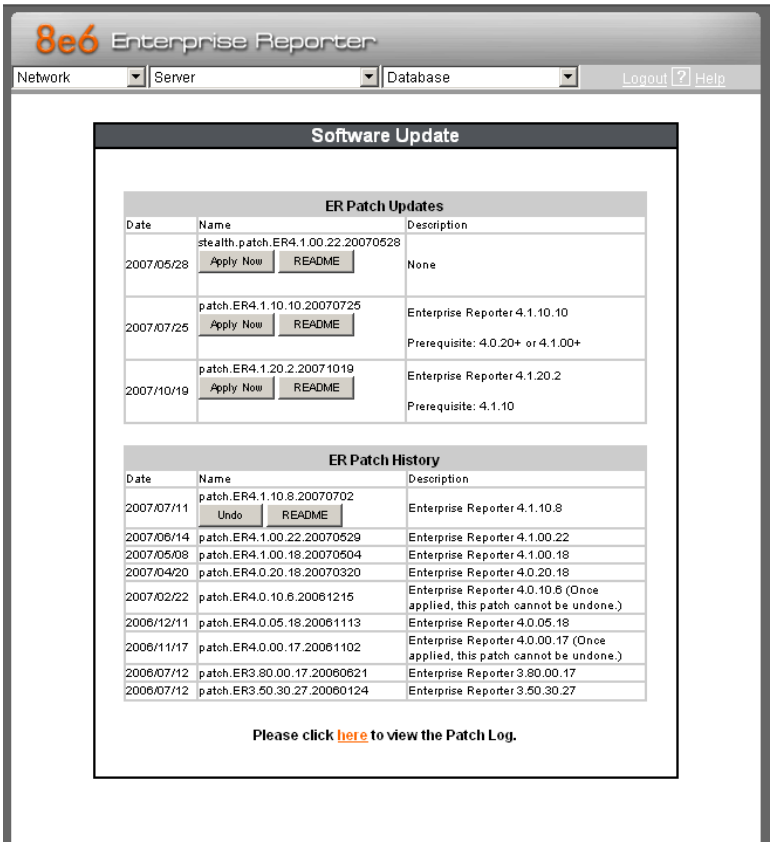


Fig. 1:2-21 Software Update screen

View Installed Software Updates

Any software update previously installed on the Server displays in the ER Patch History frame. For each installed software update, the Date installed (YYYY/MM/DD), and software update Name and Description display.

Uninstall the Most Recently Applied Software Update

In the ER Patch History frame, the most recently applied software update can be unapplied by clicking **Undo**. This action removes the software update from the Server.

View Available Software Updates

Any software update available for installing on the ER Server displays in the ER Patch Updates frame. The following information is included for each software update: Date the software update was made available (YYYY/MM/DD), software update Name, and Description (software version number, and Prerequisite software version for installing the software update). The Apply Now and README buttons display beneath the software update name. (See Install a Software Update for information about these buttons.)

Install a Software Update

***WARNING**: Before installing a software update, you must shut off the Server's software by selecting the **Shutdown Software** option on the Shut Down screen. (See the Shut Down sub-section under the Server menu section in this chapter.) All software updates must be installed in numerical order on your Server.*

***NOTES**: Be sure to terminate all reports that are currently running or are scheduled to run before applying a software update, and that port 8084 is open on your network.*

In the ER Patch Updates frame, two buttons are available: README and Apply Now.

README:

1. Click **README** to open a pop-up box containing information about the software release:

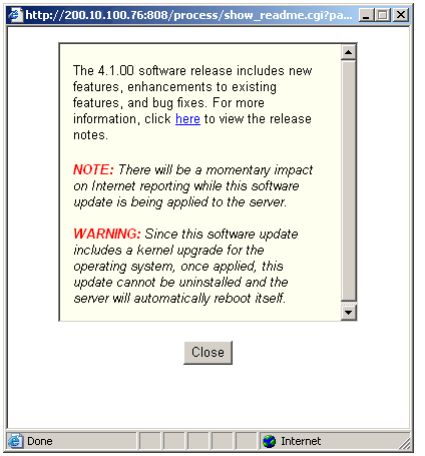


Fig. 1:2-22 Software update box

2. After reading the contents of the software release, click **Close** to close the pop-up box.

Apply Now:

1. Click **Apply Now** to open a dialog box containing information about the software release:

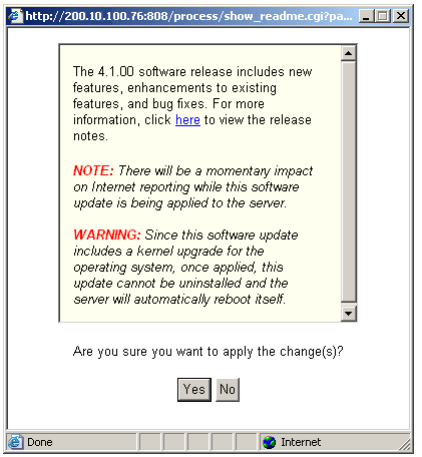


Fig. 1:2-23 Software update dialog box

2. Click **Yes** to open the EULA dialog box:

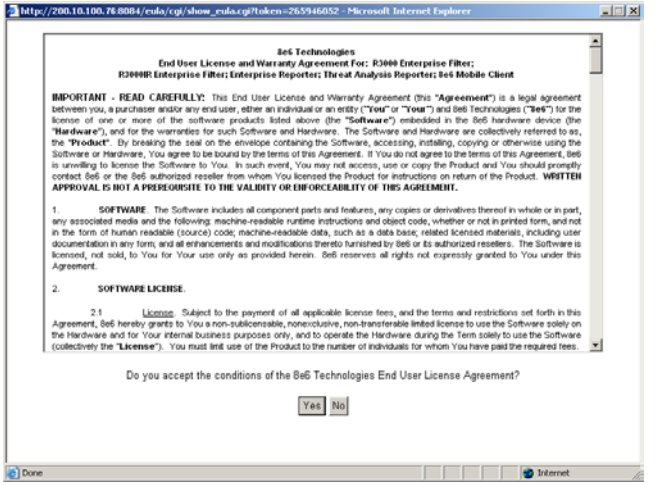


Fig. 1:2-24 EULA dialog box

3. After reading the contents of the End User License Agreement, click **Yes** if you agree to its terms. This action closes the EULA dialog box and begins the software update application process.

4. To determine whether the software update has been successfully applied, click the hyperlink (“here”) beneath the ER Patch History frame in the Software Update screen to open the Patch Log window:

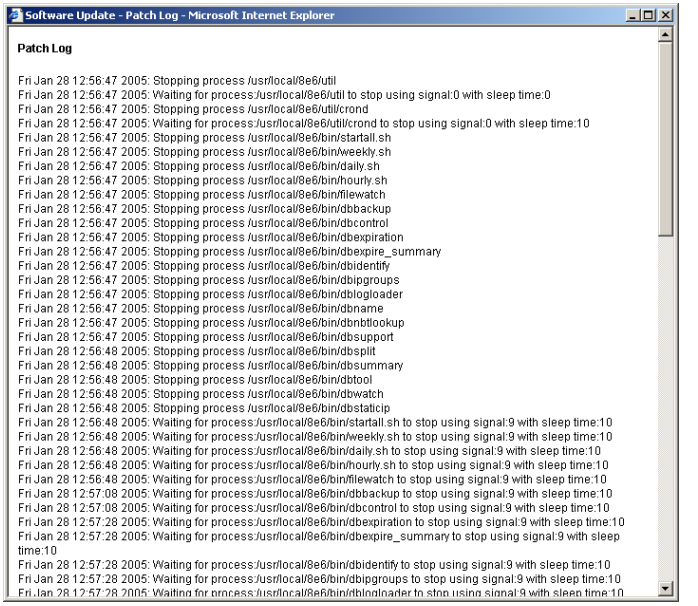


Fig. 1:2-25 Patch Log window

5. After viewing the contents of this window, click **Close** to close this window.

6. After the software update has been successfully applied, refresh the Software Update screen by selecting Software Update from the Server pull-down menu. The software update details should display in the ER Patch History frame.

***NOTE**: After installing the software update, if a message displays that informs you to reboot the Server, you should select the **Restart Software** option on the Shut Down screen.*

Software Update Setting screen

The Software Update Setting screen displays when the Software Update Setting option is selected from the Server menu. This screen is used for configuring the ER Server to receive software updates.

***NOTE**: This screen is only available if the R3000 unit is set up in the Stand Alone mode. See the Synchronization sub-section in the R3000 User Guide for more information about setup modes.*

Fig. 1:2-26 Software Update Setting screen

Select the Transfer Protocol

In the Transfer Protocol frame, choose either the “HTTPS” or “FTP” transfer protocol.

Specify Proxy Settings

1. In the Proxy Setting frame, by default “Disable” is selected. Click “Enable” if the server is in a proxy server environment.
2. In the **Proxy Server** field, enter the host name of the proxy server.
3. In the **Proxy Port** field, enter the port number of the proxy server.
4. In the **Username** field, enter the username for the proxy account.
5. Enter the same password in the **Password** and **Confirm Password** fields.

FTP: Specify Transfer Type

If using FTP, in the Transfer Type frame, by default “Active” is selected, indicating that transfers will be initiated by the server. Click “Passive” if transfers will be made via unrestricted outgoing network connections.

Save Settings

Click **Save** to save your settings.

Shut Down screen

The Shut Down screen displays when the Shut Down option is selected from the Server menu. This screen is used to restart or shut down the Server's software or hardware.

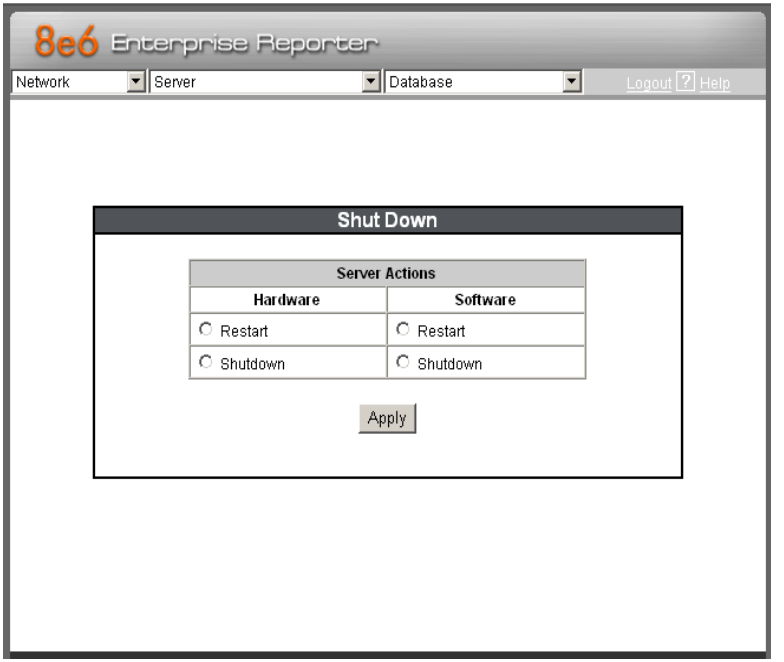


Fig. 1:2-27 Shut Down screen

Server Action Selections

- **Restart the Server's Hardware** - The Restart Hardware option should be selected if the Server box needs to be rebooted—for example, when applying certain hardware configurations. You will need to use this option if the box mode has been changed or after an IP address has been entered in the Network Settings screen. During the Hardware Restart process, files normally FTPed to the Server are routed to a problem directory in the logging device.

When the Server is running again, these files are FTPed to the Server.

- **Shut Down the Server's Hardware** - The Shutdown Hardware option should only be selected if the Server's hardware must be completely shut down—for example, if the Server box will be physically relocated. When this option is selected, the Server box shuts off, and files normally FTPed to the Server will be routed to a problem directory in the logging device. When the Server is rebooted, these files will be FTPed to the Server.
- **Restart the Server's Software** - The Restart Software option should be selected if daemons fail to run and/or the database needs to be started again. When this option is selected, the MySQL database is rebooted.
- **Shut Down the Server's Software** - The Shutdown Software option should be selected if a software update needs to be installed on the Server. When the Shutdown Software option is selected, the MySQL database shuts off and no files are FTPed to the Server.

Perform a Server Action

1. Click the radio button corresponding to the Server Action you wish to execute.
2. Click the **Apply** button to display the warning screen.
3. To proceed with your selection, click the **Restart** or **Shut-down** button on the warning screen. To change your selection, click the **Back** button of the browser window to return to the Shut Down screen.

***NOTE**: When the Restart Software or Hardware option is selected, the Server will take five to 10 minutes to reboot. After this time, you can go to another screen or log off.*

NIC Mode screen

The NIC Mode screen displays when the NIC Mode option is selected from the Server menu. This screen lets you specify the speed for the ER's Network Interface Card settings so that the ER can communicate with the network switch or hub.

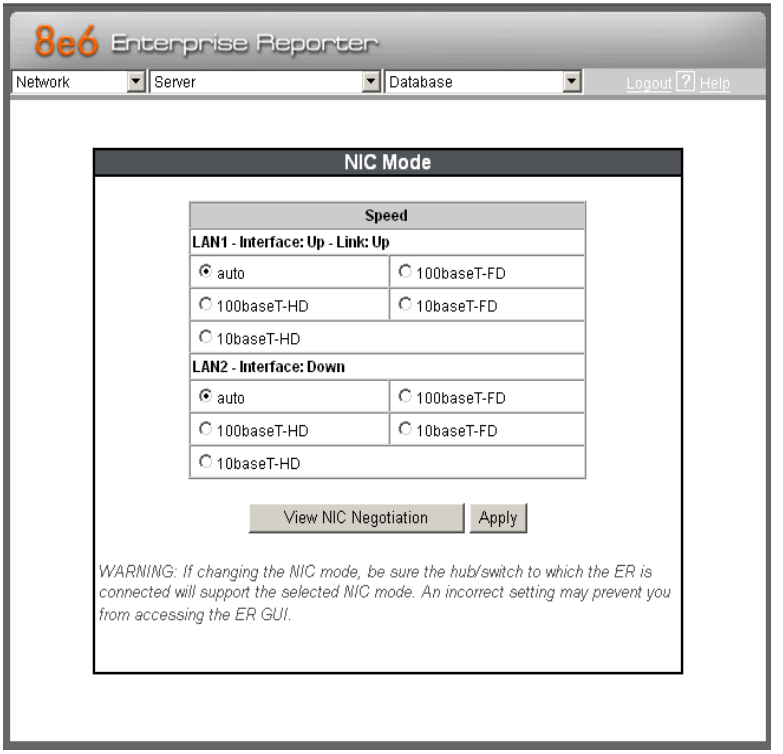


Fig. 1:2-28 NIC Mode screen

By default the NIC mode for LAN1 and LAN2 is set to "Auto". The auto-negotiation setting indicates that both connected devices will negotiate the fastest possible commonly shared speed.

***NOTE**: The options available in this window depend on the hardware components installed for the ER unit.*

View the NIC Negotiation

To verify or correct the negotiation for a NIC, click **View NIC Negotiation** to open a window containing results from the mii-tool and the ethtool about the status of the NIC mode(s):

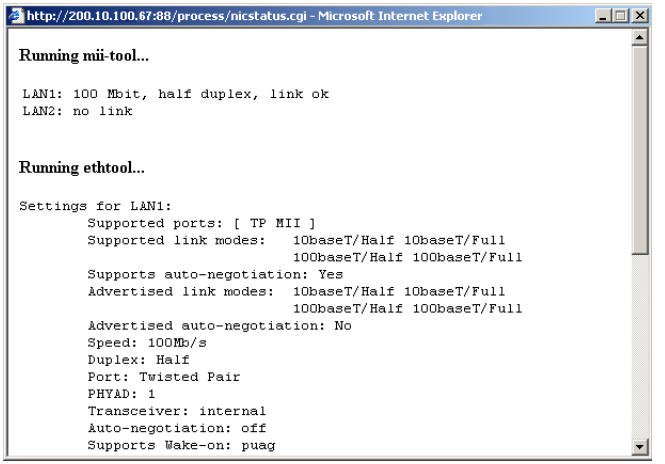


Fig. 1:2-29 NIC Negotiation window

Mii-tool checks or sets the status of a network interface's Media Independent Interface (MII) unit. Ethtool is a diagnostic and tuning tool that examines and tunes the NIC.

Modify the NIC Mode Setting

***WARNING**: If changing the NIC mode, be sure the hub/switch to which the ER is connected will support the selected NIC mode. An incorrect setting may prevent you from accessing the ER console.*

To modify the NIC setting, in the LAN1 or LAN2 frame:

1. Click the radio button for the available option you wish to select: 10baseT-Full Duplex, 10baseT-Half Duplex, 100baseT- Full Duplex, 100baseT-Half Duplex, or 1000baseT-Full Duplex, if available on your ER Server.
2. Click **Apply** to activate the new NIC mode setting.

***NOTE**: The status (Up or Down) of the Interface displays to the right of the LAN1 and LAN2 labels. For an Interface with an "Up" status, the Link status (Up or Down) displays to the right of the Interface status.*

Web Client Server Management screen

The Web Client Server Management screen displays when the Web Client Server Management option is selected from the Server menu. This screen is used for enabling specified Web Client Server features.

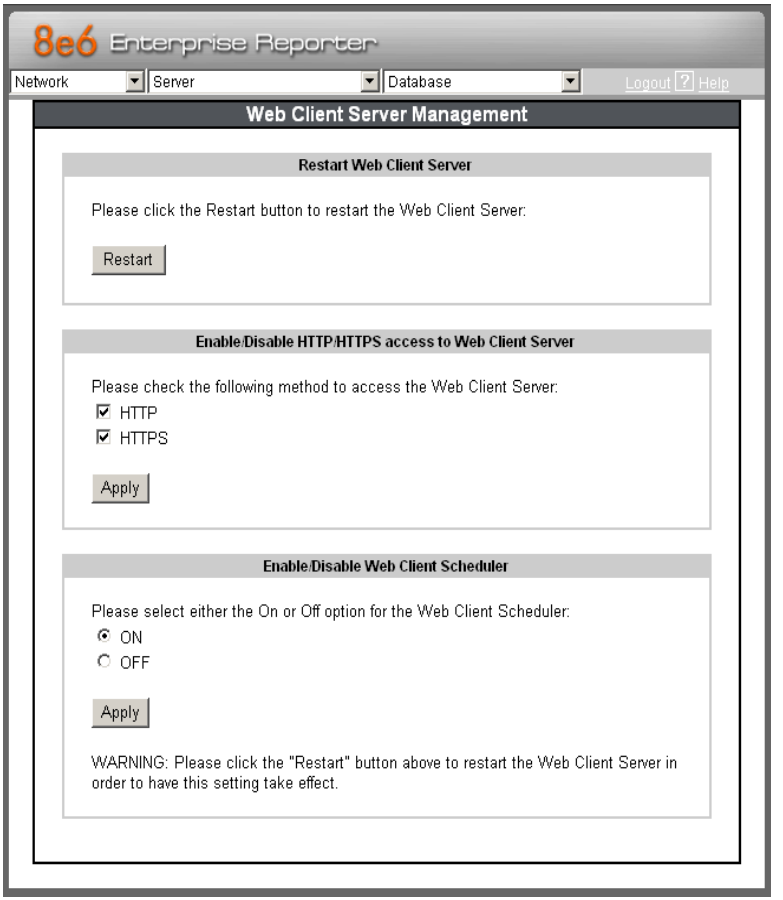


Fig. 1:2-30 Web Client Server Management screen

Restart the Web Client Server

In the Restart Web Client Server frame, click **Restart** to restart the Web Client server. As a result of this action, a screen displays with the following message: “The Web Client Server will restart in a few minutes.” Click **OK** to return to the Web Client Server Management screen.

Enable/Disable Web Client Server Access

1. In the Enable/Disable HTTP/HTTPS access to Web Client Server frame, click the checkbox(es) corresponding to the option(s) for logging into the Web Client:
   - “HTTP” - Choose this option to let users log into the Web Client using an HTTP IP address
   - “HTTPS” - Choose this option to let users log into the Web Client using an HTTPS IP address

***NOTE**: Remove the check mark to disable a selection.*

2. Click **Apply**.

Enable/Disable the Web Client Scheduler

1. In the Enable/Disable Web Client Schedule frame, click the appropriate radio button to specify whether or not to automatically run scheduled Web Client reports:
   - “ON” - Choose this option to let the Web Client automatically run scheduled reports.

***WARNING**: Do not select this option if using the Access Client to run scheduled reports; duplicate reports will be generated.*

   - “OFF” - Choose this option to use the Access Client for running scheduled reports, or if you do not want the Web Client to run scheduled reports.
2. Click **Apply**.
3. Click **Restart** to restart the Web Client Server.

Hardware Failure Detection screen

If using an ERH, HL, or SL unit, the Hardware Failure Detection screen displays when the Hardware Failure Detection option is selected from the Server menu. This screen is used for showing the status of each drive on the RAID server.

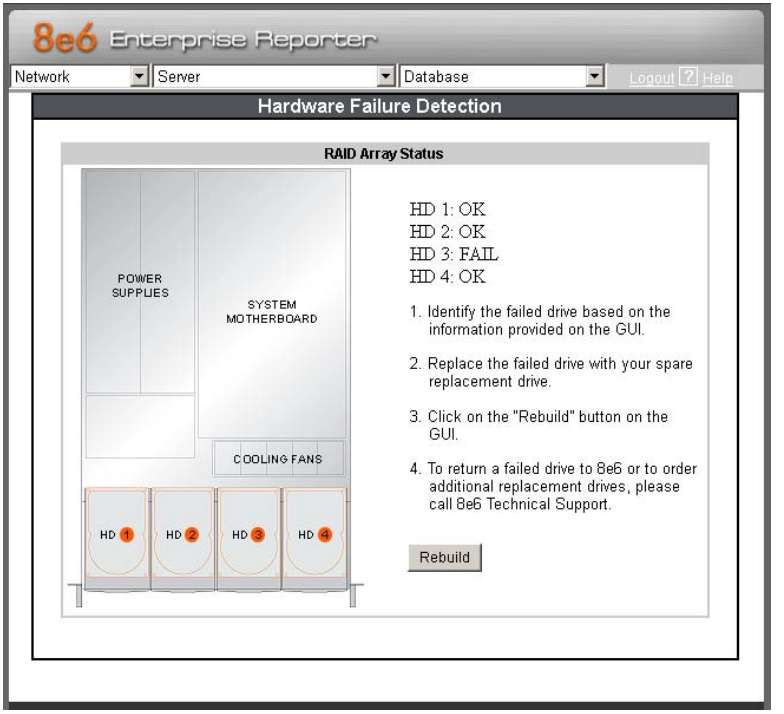


Fig. 1:2-31 Hardware Failure Detection screen

View the Status of the Hard Drives

The current RAID Array Status displays for the four hard drives (HD 1, HD 2, HD 3, HD 4). If all hard drives are functioning without failure, the text “OK” displays for each corresponding drive number listed at the right of the screen, and no other text displays.

If any of the hard drives has failed, the message “FAIL” displays for the corresponding drive number listed at the right of the screen, and instructions for replacing the hard drive display below:

1. Identify the failed drive based on the information provided on the GUI.
2. Replace the failed drive with your spare replacement drive.
3. Click on the “Rebuild” button on the GUI.
4. To return a failed drive to 8e6 or to order additional replacement drives, please call 8e6 Technical Support.

***NOTE**: For information on troubleshooting RAID, refer to Appendix C: RAID Maintenance.*

Database Menu

The Database pull-down menu includes options for configuring the database. These options are: IP.ID, Username Display Setting, Elapsed Time, Page Definition, Tools, Expiration, NAS Status, Optional Features, and User Group Import.

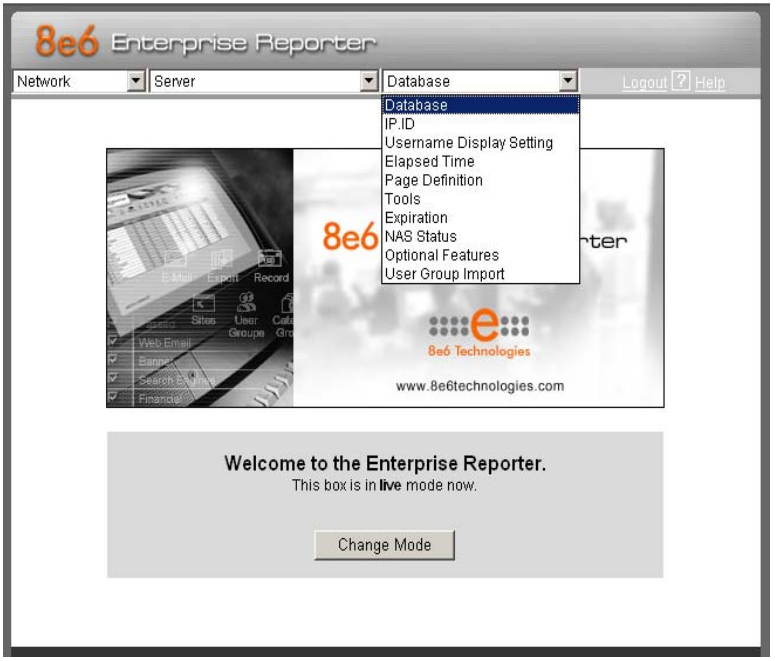


Fig. 1:2-32 Database menu, main screen

User Name Identification screen

The User Name Identification screen displays when the IP.ID option is selected from the Database menu. This screen is used for configuring the Server to identify users based on the IP addresses of their machines, their usernames, and/or their machine names. Information set up on this screen is used by the Client when logging a user's Internet activity.

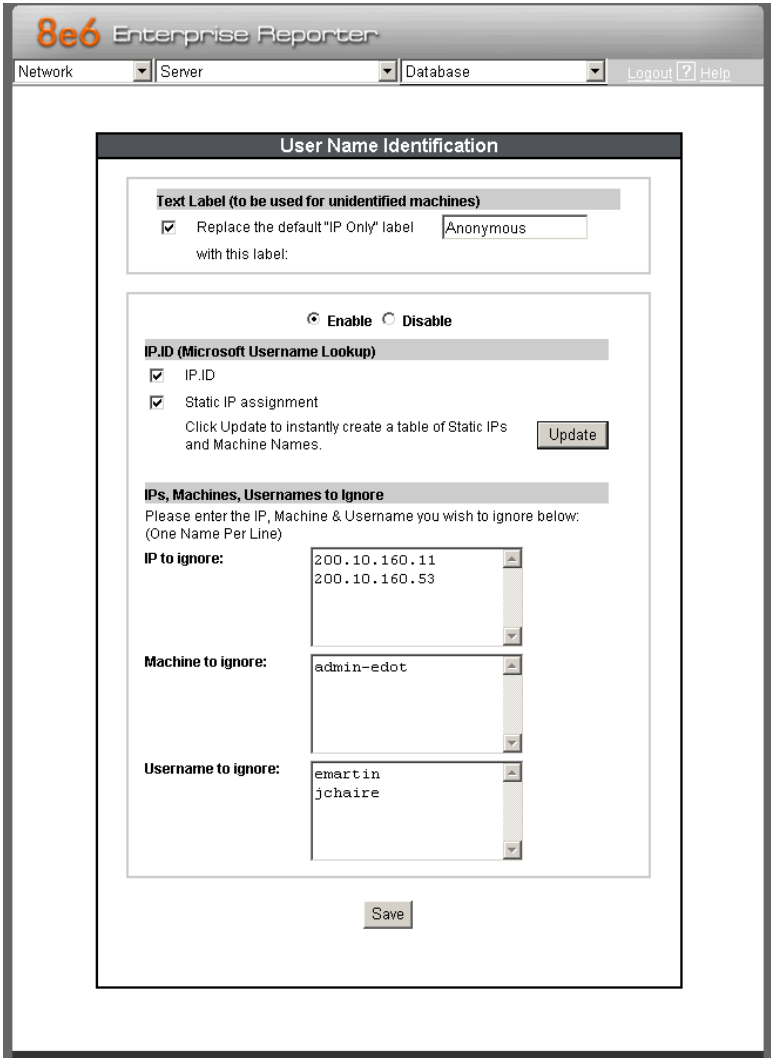


Fig. 1:2-33 User Name Identification screen with IP.ID activated

As the administrator of the Server, you have the option to either enable or disable this feature for logging users' activities by usernames, machine names, and/or IP addresses of machines.

WARNINGS

*The ER will generate NetBIOS requests outside the network if IP.ID is activated **and** if no segment settings have been specified in the configuration of the Web access logging device—causing it to log external traffic. To resolve this issue, the Web access logging device should be modified to log activity only within the network. If a firewall is used, it should be set up to prevent logging NetBIOS requests outside the network.*

***NOTE**: Depending on the type of Web access logging device you are using, there may not be a configuration parameter for segment settings.*

Be sure the time zone specified for the ER is the same for each Web access logging device the ER uses. Failure in executing this setup will cause inconsistencies when users' logging times are reported, especially if IP.ID is activated. If multiple Web access logging devices are used, be sure to identify the subnets assigned to each of these devices, as users cannot be tracked solely by IP address.

If using IP.ID, note that user login times are established for set periods of 15 minutes, and if more than one user logs onto the same machine during that time period, the activity on that machine will be identified with the first user who logged onto that machine. For example, the first user logs on a machine for three minutes and then logs off. The second user logs on the same machine for 11 minutes and then logs off. The first user logs back on that machine for 16 minutes. All 30 minutes are logged as the first user's activity.

View the User Name Identification screen

There are two frames on this screen: one used for customizing the label that displays in Client reports for unidentified machines, and the other used for specifying username identification (IP.ID) criteria. These frames will be populated if entries were previously made in them.

Set up a Customized Label for Unidentified Machines

The Text Label frame is used for creating a customized label to display in reports generated by the Client. This label will replace the default “IP Only” label that is used for identifying any machine that is not assigned to a specific user.

1. Click in the checkbox to indicate that you wish to create a customized text label for unidentified user machines.
2. In the **Replace the default “IP Only” label with this label** field, enter up to 14 characters of text for the label.
3. Click **Save** to save your entries.

Configure the Server to Log User Activity

1. In the IP.ID (Microsoft Username Lookup) section of the screen, click the radio button corresponding to **Enable**. This action opens an alert box informing you that if usernames are enabled, these usernames will overwrite those that are being imported from the shadow log.
2. Click **OK** to close the alert box, and to activate the IP.ID and Static IP assignment checkboxes.
3. Select one or both of the following options by clicking in the designated checkbox(es):
   - **IP.ID** - this option logs a user’s activity by username (login ID).

- **Static IP assignment** - this option logs a user's activity by the IP address of the machine used. When selecting this option, the Update button becomes activated.

  a. Click the **Update** button to automatically generate a table of static IP addresses and machine names. After this table is created, the message screen displays to confirm the successful execution of this task.

  b. Click the **Back** button to return to the User Name Identification screen.

4. In the IP/Machine/Username to ignore list boxes, enter all IP addresses, machine names, and/or usernames the Server should disregard when identifying users. Each entry should be made in a separate row.

5. After making all necessary entries on this screen, click the **Save** button.

***NOTE**: After saving your entries, the IP.ID frame becomes disabled. To make modifications in this frame, you must follow all steps in this sub-section.*

Deactivate User Name Identification

1. Click the radio button corresponding to **Disable**.

2. Click the **Save** button.

Username Display Setting screen

This Username Display Setting screen displays when the Username Display Setting option is selected from the Database menu. This screen is used for configuring the username format imported from raw logs and customizing the username format that displays in reports.

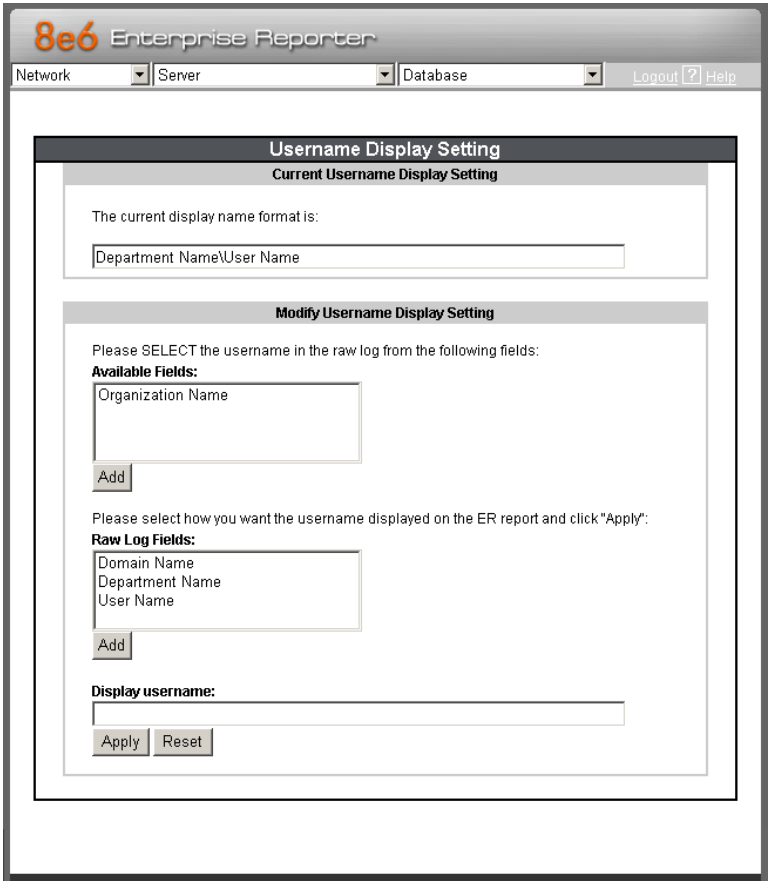


Fig. 1:2-34 Username Display Setting screen

View the Current Username Display Setting

In the Current Username Display Setting frame, the current username format displays—if previously entered in the Display username field and saved on this screen.

Modify the Username Display Setting

In the Modify Username Display Setting frame, make selections from list boxes and apply results for the new username format to be displayed in the report.

1. By default, the following choices display in the Available Fields list box: Domain Name, Organization Name, Department Name, User Name. Make a selection from this list for the first field displayed in your server console and raw logs that you wish to include in the username format in the report.
2. Click **Add** to include this selection in the Raw Log Fields list box below.

***NOTE**: Follow steps 1 and 2 for each consecutive field to be added to the Raw Log Fields list box.*

***TIP**: Click the Reset button on this screen at any time to revert to the default settings.*

***WARNING**: It is important to select the correct fields from this list, in the order in which they appear in your server console. For example, if the username format on the console is Domain Name\Department Name\User Name, and only User Name and Department Name are selected from the Available Fields list box—in that order—the report will display information in the wrong order. In this example, if the Domain Name is LOGO, the Department Name is Admin, and the User Name is JSmith, the report will show JSmith\Admin, instead of LOGO\Admin\JSmith.*

3. In the Raw Log Fields list box, select the first field to be displayed in the username format on the report.

4. Click **Add** to include your selection in the Display username field below.

***NOTE**: Follow steps 3 and 4 for each field to be added to the Display username field below. Each additional selection added to the display name is preceded by a backslash (\ ).*

5. Click **Apply** to save your entries and to display the new username format in the Current Username Display Setting frame.

***NOTE**: Changes made to username display settings in this screen will not be effective until the next day's reports are generated.*

Page View Elapsed Time screen

The Page View Elapsed Time screen displays when the Elapsed Time option is selected from the Database menu. This screen is used for establishing the value—amount of time—that will be used when tracking the length of a user's stay at a given Web site, and the number of times the user accesses that site.

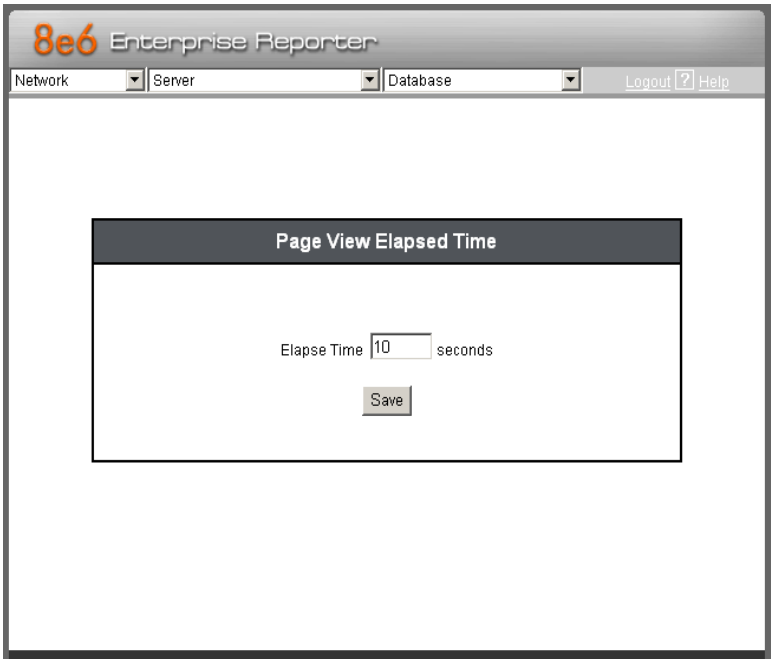


Fig. 1:2-35 Page View Elapsed Time screen

Establish the Unit of Elapsed Time for Page Views

1. In the **Elapse Time** field, enter the number of seconds that will be used as the value when tracking a user's visit to a Web site.
2. Click the **Save** button.

Elapsed Time Rules

Each time a user on the network accesses a Web site, this activity is logged as one or more visit(s) to that site. The amount of time a user spends on that site and the number of times he/she accesses that site is tracked according to the following rules:

- A user will be logged as having visited a Web site one time if the amount of time spent on any pages at that site is equivalent to the value entered at the Elapse Time field, or less than that value.

  For example, if the value entered at the Elapse Time field is 10 seconds, and if the user is at a site between one to 10 seconds—on the same page or on any other page within the same site—the user's activity will be tracked as one visit to that Web site.

- Each time the user exceeds the value entered at the Elapse Time field, the user will be tracked as having visited the site an additional time.

  For example, if the value entered at the Elapse Time field is 10 seconds and the user remains at a Web site for 12 seconds, two visits to that site will be logged for him/her.

- Each session at a Web site is tracked as one or more visit(s), depending on the duration of the session. A session is defined as a user's activity at a site that begins when the user accesses the site and ends when the user exits the site.

  For example, if the value entered at the Elapse Time field is 10 seconds and the user spends five seconds on a Web site, then exits, then returns to the same site for another 15 seconds, the user will have two sessions or three visits to that site logged for him/her (5 seconds = 1 visit, 15 seconds = 2 visits, for a total of 3 visits).

Page Definition screen

The Page Definition screen displays when the Page Definition option is selected from the Database menu. This screen is used for specifying the types of pages to be included in the detail report for Page searches.

Fig. 1:2-36 Page Definition screen

View the Current Page Types

The Current page types list box contains the extensions of page types to be included in the detail report.

Remove a Page Type

To remove a page type from the detail report:

1. Select the page extension from the Current page types list box.
2. Click **Remove**.
3. Click **Apply**.

Add a Page Type

To add a page type in the detail report:

1. Enter the **New Page Type** extension.
2. Click **Add** to include the extension in the Current page types list box.
3. Click **Apply**.

Tools screen

The Tools screen displays when the Tools option is selected from the Database menu. This screen is used for viewing reports and logs to help you troubleshoot problems with the Client application.

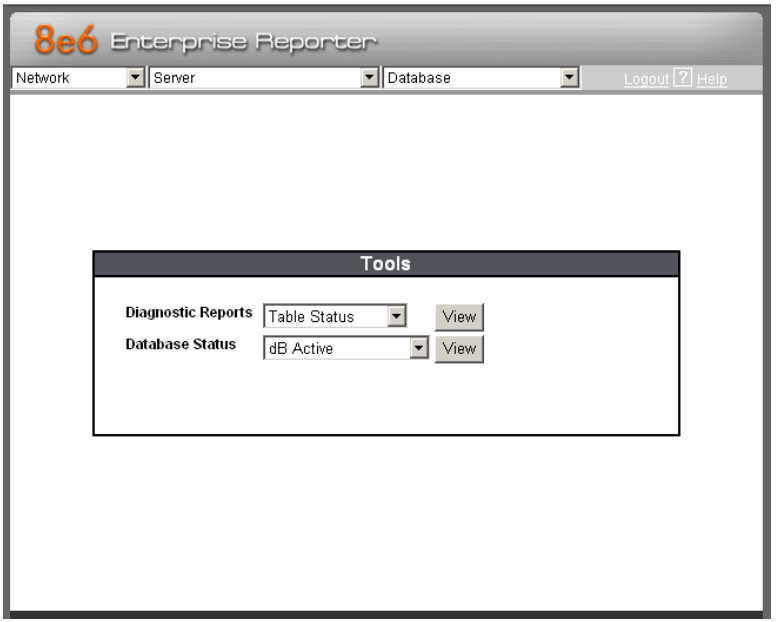


Fig. 1:2-37 Tools screen

The following options are available on this screen:

- View Diagnostic Reports
- View Database Status Logs

View Diagnostic Reports

1. Choose a report from the pull-down menu (Table Status, Process List, Full Process List, Tables, or Daily Summary).
2. Click the **View** button to view the selected diagnostic report in a pop-up window:
   - **Table Status** - This report contains a list of Client table names, and columns of statistics on each table, such as type, size, number of rows, and time created and updated.
   - **Process List** - This report shows a list of current SQL queries in the database, in an abbreviated format.
   - **Full Process List** - This report shows a list of current SQL queries in the database, in the full format that includes all columns of data.
   - **Tables** - This report contains a list of the names of tables currently in the database.
   - **Daily Summary** - This report shows the date range of summary tables currently in the database.
3. Click the “X” in the upper right corner of the pop-up window to close the window.

View Database Status Logs

1. Choose a database status log from the pull-down menu.
2. Click the **View** button to view the selected database status log in a pop-up window:
   - **db Active** - This log indicates when client tables were last updated with hits_objects and hits_pages.
   - **db Backup** - This log provides information about the MySQL backup/restore operation.
   - **db Control** - This log shows a list of actions performed by the ER process when processing log files.

- **db Expiration** - This log includes information about expiring data on the Server.
- **db Expire Summary** - This log provides a list of data expiration from summary tables.
- **db Identify** - This log provides information about the Server's action of obtaining user/machine names from name log files and populating the database with these names.
- **db Ipgroups** - This log lists individual and group IP records that were added to—and deleted from—the client group lookup table.
- **db Logloader** - This log provides information about log file parsing and the number of valid and invalid records that are processed.
- **db Nbtlookup** - This log provides a list of user/machine IP addresses from the NetBIOS lookup.
- **db Split** - This log contains information pertaining to the formation of the hits_objects/hits_pages tables.
- **db Staticip** - This log provides information about settings on the server for the static IP assignment option.
- **db Summary** - This log shows a summarization of activities from the dbsummary database tool.
- **db Support** - This log includes a list of temporary tables that were created for the formation of the hits tables.
- **db Tool** - This log shows information about system checks performed on disk usage, free memory, unprocessed files, and daemons.
- **db Traffic** - This log provides information about the daily traffic table.
- **File Watch Log** - This log shows a list of records that were imported from one machine to another.

- **Patch Log** - This log gives information about applied software updates.
- **MYSQL Log** - This log provides information pertaining to the MySQL server.
- **Error Entry - R2k** - This log displays a list of R2000 query errors.
- **Error Entry - R3k** - This log displays a list of R3000 query errors.

3. Click the “X” in the upper right corner of the pop-up window to close the window.

Expiration screen

The Expiration screen displays when the Expiration option is selected from the Database menu. This screen shows statistics on the amount of data currently stored on the Server box, and provides an estimated date when that data will expire. By reviewing the current database disk space utilization and the average number of daily hits on your Server, adjustments can be made to the number of weeks of live and archive data you wish to store in the future before that data expires.

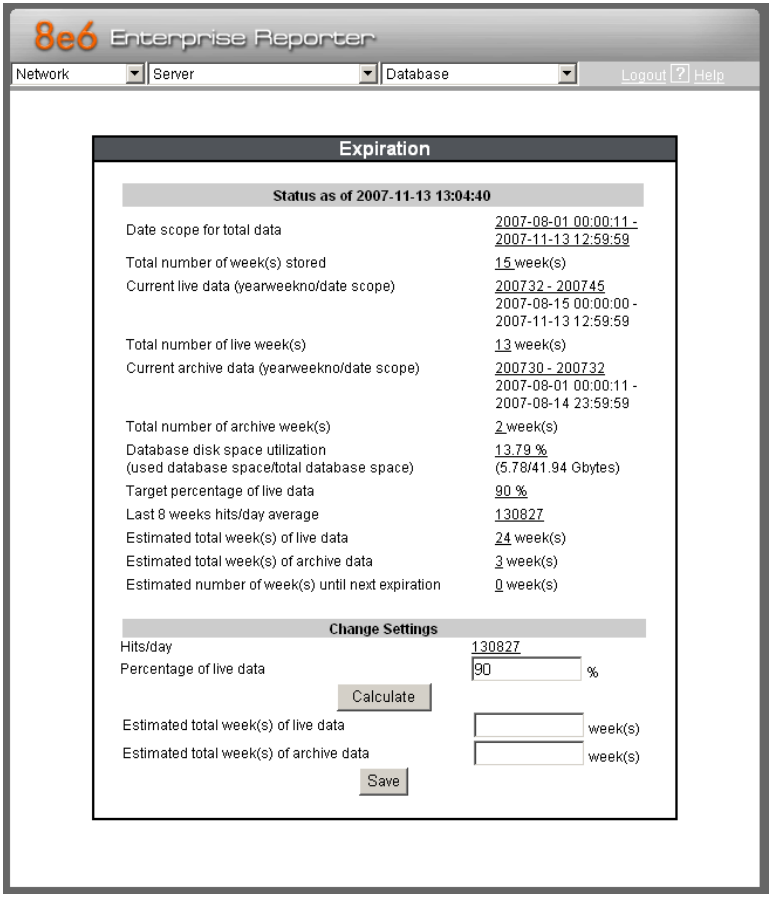


Fig. 1:2-38 Expiration screen

***NOTE**: Though the database is backed up automatically each day, under certain circumstances you may need to perform a manual backup to the internal backup drive, and then save this data off site. (See the Server Menu Backup screen section for information on establishing backup procedures, and backing up and restoring data on the ER Server.)*

Expiration Screen Terminology

The following terminology is used on the Expiration screen:

- **Live** - pertains to indexed data on the hard drive of the Server for the most recent weeks—the period designated as “live.” Indexed data includes pages and objects that were accessed by users on the Internet, as well as the indexes for these items.

  When setting up the Server to store data, 8e6 recommends that you allocate the highest percentage possible for live data storage, since reports run faster if indexes are available for pages and objects.

  If your Server is set up to store live data only (100 percent live data), you will be able to store less data than if you store both live and archive data, since indexes require additional storage space.

- **Archive** - pertains to non-indexed data on the hard drive of the Server for the oldest weeks—the period designated as “archive.” Non-indexed data might include pages and/or objects that were accessed by users on the Internet.

  Since archive data contain no indexes, they occupy less space on the Server than live data—which include indexes and pages/objects. However, reports generated for periods of time with archive data take longer to process since indexes are not included for that data.

- **Expire** - pertains to the action of dropping data from the Server when there is no room left on the hard drive for additional storage. When the hard drive reaches its maximum data storage capacity, indexes from the oldest week of data stored on the Server are dropped, or "expired" from the Server. Thereafter, when more space is needed on the Server, the oldest week of non-indexed data "expires."

Expiration Rules

The administrator of the Server specifies the number of weeks of data that will be stored on the Server, based on the storage capacity of the hard drive, and the number of hits on the Server. After inputting the percentage of live data to be stored, the Server translates that figure into the equivalent of weekly time periods for live and/or archive data storage.

When the Server reaches the maximum number of weeks allocated for live data storage, the oldest week of live data stored on the Server attains an archive data status. In attaining an archive data status, the index for that week of data is dropped from the database tables.

When the Server reaches its maximum number of weeks allocated for archive data storage, the oldest week of non-indexed data stored on the Server is automatically dropped (expired) from the database.

Once data expires, it cannot be recovered.

View Data Storage Statistics

In the Status section of this screen, the date and time of the last database expiration displays in the Status bar. The date displays in the YYYY-MM-DD format, and the time displays in military time (01-24 hours) using the HH:MM:SS time format.

The following data that displays is current as of the most recent database expiration run:

- **Data scope for total data** - the date and time range of all live and archive data currently stored on the Server. The date displays in the YYYY-MM-DD format, and the time displays in military time (01-24 hours) using the HH:MM:SS time format.
- **Total number of week(s) stored** - the number of weeks represented in the total data date scope.
- **Current live data (yearweekno/date scope)** - the range of dates and times of live data currently stored on the Server.

  The first line displays the range of year(s) and weeks in the YYYYWW format, where “Y” represents the year, and “W” represents the week number in that year (01-52).

  The second line displays the first date and time in the range of live data currently stored on the Server. The date displays in the YYYY-MM-DD format, and the time displays in military time (1-24 hours) using the HH:MM:SS time format.

  The third line displays the last date and time in the range of live data currently stored on the Server, using the same format as in the second line of data.
- **Total number of live week(s)** - the number of weeks represented in the live data date scope.

- **Current archive data (yearweekno/date scope)** - the range of dates and times of archive data currently stored on the Server.

  The first line displays the range of year(s) and weeks in the YYYYWW format, where "Y" represents the year, and "W" represents the week number in that year (01-52).

  The second line displays the first date and time in the range of archive data currently stored on the Server. The date displays in the YYYY-MM-DD format, and the time displays in military time (1-24 hours) using the HH:MM:SS time format.

  The third line displays the last date and time in the range of archive data currently stored on the Server, using the same format as in the second line of data.

- **Total number of archive week(s)** - the number of weeks represented in the archive data date scope.

- **Database disk space utilization** - the percentage of space currently being used on the hard drive for both live and archive data. If a high percentage displays, you may want to expire data in the near term (see Change Data Storage Settings).

- **(used database space/total database space)** - the amount of space in Gigabytes currently being used on the hard drive for both live and archive data, and the total amount of space in Gigabytes (Gbytes) on the hard drive allocated to database storage.

- **Target percentage of live data** - the percentage of live data to be stored on the Server. If this figure is 100, only live data will be stored. If this figure is less than 100, the remaining percentage to be stored will be archive data.

  The percentage that displays can be changed by entering and saving a different figure in the Percentage of live data field in the Change Settings section of this screen.

- **Last 8 weeks hits/day average** - the average number of hits on the Server per day, based on the last eight weeks of data stored on the Server.

The following data that displays is current as of the last changes made in the Change Settings section of the screen:

- **Estimated total week(s) of live data** - the number of weeks of live data the Server will store, based on your specifications. This number is affected by the hits/day on the Server, and the maximum number of weeks of data the Server is able to hold.

  The number of weeks of live data to be stored can be changed by making a new entry in the Percentage of live data field in the Change Settings section of this screen, and saving the result of your calculations that displays below in the Estimated total week(s) of live data field.

- **Estimated total week(s) of archive data** - the number of weeks of archive data the Server will store, based on your specifications. This number is affected by the hits/day on the Server, and the maximum number of weeks of data the Server is able to hold.

  The number of weeks of archive data to be stored can be changed by making a new entry in the Percentage of live data field in the Change Settings section of this screen, and saving the result of your calculations that displays below in the Estimated total week(s) of archive data field.

- **Estimated number of week(s) until next expiration** - the number of weeks from this week that data on the Server will expire.

Change Data Storage Settings

The Change Settings section of the screen is used for updating the amount of data that will be stored on the Server box in the future. By making an entry in this section of the screen, you dictate how data on the box will expire.

At the Hits/day field, the number of hits on the Server per day displays. This is the same figure that displays in the Last 8 weeks hits/day average field in the Status section above.

1. In the **Percentage of live data** field, enter a figure for the percentage of data you wish to be stored as live data on the box. If you want all data to be live data only, enter 100.
2. Click the **Calculate** button to display results in the following fields below: Estimated total week(s) of live data, and Estimated total week(s) of archive data.

   After viewing your results in these display fields, you can adjust the number of weeks that data will be saved on the Server, if necessary. To do so, follow steps 1 and 2 again.
3. Once you are satisfied with your results, click the **Save** button. As a result of your entries, the following occurs:
   - the figure saved in the Percentage of live data field displays in the Target percentage of live data field in the Status section
   - the figures displayed in the Estimated total week(s) of live/archive data fields display in the Estimated total week(s) of live/archive data fields in the Status section
   - the Estimated number of week(s) until next expiration field may display a new figure, based on the new settings you saved.

When the next database expiration runs, all other fields in the Status section will reflect the new calculations.

***TIP**: 8e6 recommends that you set up your Server to store more live data than archive data for the benefit of administrators and sub-administrators who generate reports via the Client application. Report processing times are slower when generating reports that include non-indexed data.*

If your Server is set up to store only live data, you will be able to store less data than if you store both live and archive data, since indexes require additional storage space.

***NOTE**: See Appendix A: Evaluation Mode for information about viewing the Expiration screen in the evaluation mode.*

NAS Status screen

The NAS Status screen displays when the NAS Status option is selected from the Database menu. This screen is used for verifying the status of the Network Attached Storage (NAS) device. The NAS is used for storing ER data that otherwise might be lost from the ER Server when reaching its maximum data storage capacity.

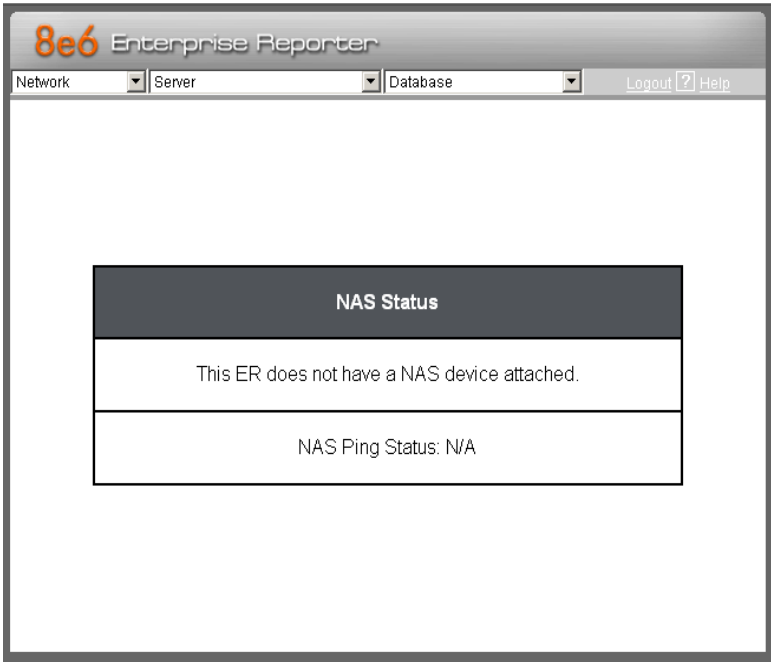


Fig. 1:2-39 NAS Status screen

View NAS Status Information

One of the following informational messages displays on this screen, depending on whether or not a NAS device is attached to the ER:

- This ER does not have a NAS device attached. NAS Ping Status: N/A
- This ER has a NAS device attached. NAS Ping Status: OK
- This ER has a NAS device attached. NAS Ping Status: FAILED

If the “FAILED” message displays, verify that the NAS is properly connected to the ER.

***NOTE**: Refer to the Quick Start Guides for the ER and NAS devices for setup information.*

Optional Features screen

The Optional Features screen displays when Optional Features is selected from the Database menu (see Fig. 1:2-40). This screen is used for specifying any of the following options to be available in the Web Client when generating specified types of reports: Search String Reporting, Block Request Count, Wall Clock Time, Object Count. This screen also is used for enabling and configuring the password security feature to be used for the Administrator console and/or Web Client.

***NOTE**: Optional features can be enabled or disabled at any time.*

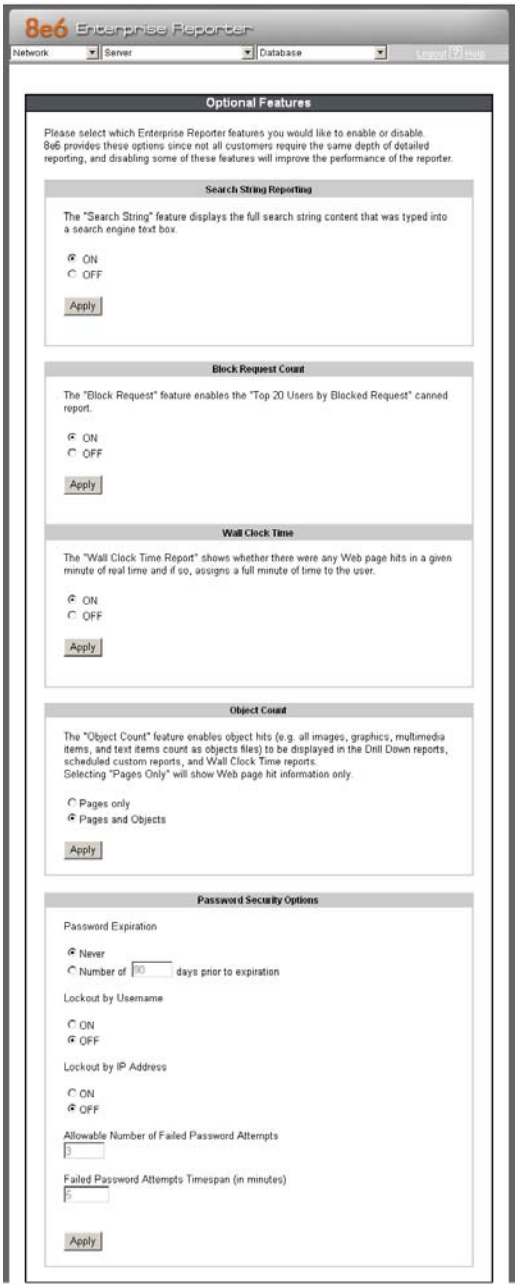


Fig. 1:2-40 Optional Features screen

Enable Search String Reporting

If Search String Reporting is enabled, detail drill down reports display the full search string content typed into a search engine text box for search sites such as Google, Yahoo!, MSN, AOL, Ask.com, YouTube.com, and MySpace.com.

1. Click the radio button corresponding to “ON” to let search string entries display in drill down reports.
2. Click **Apply** to apply your setting.

Enable Block Request Count

If Block Request Count is enabled, the Top 20 Users by Blocked Request canned report can be generated by the administrator.

1. Click the radio button corresponding to “ON” to make the Top 20 Users by Blocked Request canned report selection available in an administrator’s Canned Reports menu.
2. Click **Apply** to apply your setting.

***NOTE**: Since Canned Reports are processed each night, any changes made to settings today will not effective until the following day.*

Enable Wall Clock Time

If Wall Clock Time is enabled, Wall Clock Time Reports can be generated by the administrator. These reports use the Wall Clock Time algorithm to calculate the amount of time an end user spent accessing a given page or object—disregarding the number of seconds from each hit and counting each unique minute of Web time as one minute. Using this algorithm, an end user could never have more than 24 hours of Web time within a given 24-hour period.

1. Click the radio button corresponding to “ON” to make the Wall Clock Time Report selection available in an administrator’s Custom Reports menu.
2. Click **Apply** to apply your setting.

***NOTE**: Since Wall Clock Time reports are processed each night, any changes made to settings today will not effective until the following day.*

Enable Page and/or Object Count

In the Object Count frame, indicate whether drill down, Wall Clock Time, and scheduled custom reports will include Web page hits only, or both Web page and object hits. Objects include images, graphics, multimedia items, and text item object files.

***WARNING**: If “Pages only” is selected, **all** records of objects accessed by end users will be lost for the time period in which this option was enabled. Even if there were objects accessed by end users during that time period, zeroes (“0”) will display for object activity in generated reports.*

1. Select one of two radio buttons to specify the type of hits to be included in drill down, Wall Clock Time, and scheduled custom reports:
   - “Pages only” - Choose this option to include *only* Web page hits in reports.
   - “Pages and Objects” - Choose this option to include *both* Web page and object hits in reports.
2. Click **Apply** to apply your setting.

Enable, Configure Password Security Option

In the Password Security Options frame, passwords for accessing the Administrator console or Web Client can be set to expire after a specified number of days, and/or lock out the user from accessing the Administrator console and Web Client after a specified number of failed password entry attempts within a defined interval of time.

1. Enable any of the following options:

   - At the **Password Expiration** field, click the radio button corresponding to either password expiration option:
     - **Never** - Choose this option if passwords will be set to never expire.
     - **Number of 'x' days prior to expiration** - Choose this option if password will be set to expire after 'x' number of days (in which 'x' represents the number of days the password will be valid).

***NOTES**: The maximum number of days that can be entered is 365.*

If a user's password has expired, when he/she enters his/her User Name and Password in the login screen and clicks Login, he/she will be prompted to re-enter his/her User Name and enter a new password in the Password and Confirm Password fields.

   - At the **Lockout by Username** field, click the radio button corresponding to either of the following options:
     - **ON** - Choose this option to lock out the user by username if the incorrect password is entered—for the number of times specified in the Allowable Number of Failed Password Attempts field—within the interval defined in the Failed Password Attempts Timespan (in minutes) field.

- **OFF** - Choose this option if the user will not be locked out by username after entering the incorrect password.

- At the **Lockout by IP Address** field, click the radio button corresponding to either of the following options:
  - **ON** - Choose this option to lock out the user by IP address if the incorrect password is entered—for the number of times specified in the Allowable Number of Failed Password Attempts field—within the interval defined in the Failed Password Attempts Timespan (in minutes) field.
  - **OFF** - Choose this option if the user will not be locked out by IP address after entering the incorrect password.
- **Allowable Number of Failed Password Attempts** - With the Lockout by Username and/or Lockout by IP Address option(s) enabled, enter the number of times a user can enter an incorrect password during the interval defined in the Failed Password Attempts Timespan (in minutes) field before being locked out of the ER application.

***NOTE**: The maximum number of failed attempts that can be entered is 10.*

- **Failed Password Attempts Timespan (in minutes)** - With the Lockout by Username and/or Lockout by IP Address option(s) enabled, enter the number of minutes that defines the interval in which a user can enter an incorrect password—as specified in the Allowable Number of Failed Password Attempts field—before being locked out of the ER application.

***NOTE**: The maximum number of minutes that can be entered is 1440.*

2. Click **Apply** to apply your settings.

User Group Import screen

The User Group Import screen displays when the User Group Import option is selected from the Database menu. This screen is used for specifying R3000 servers to send LDAP user group membership information to this ER Server.

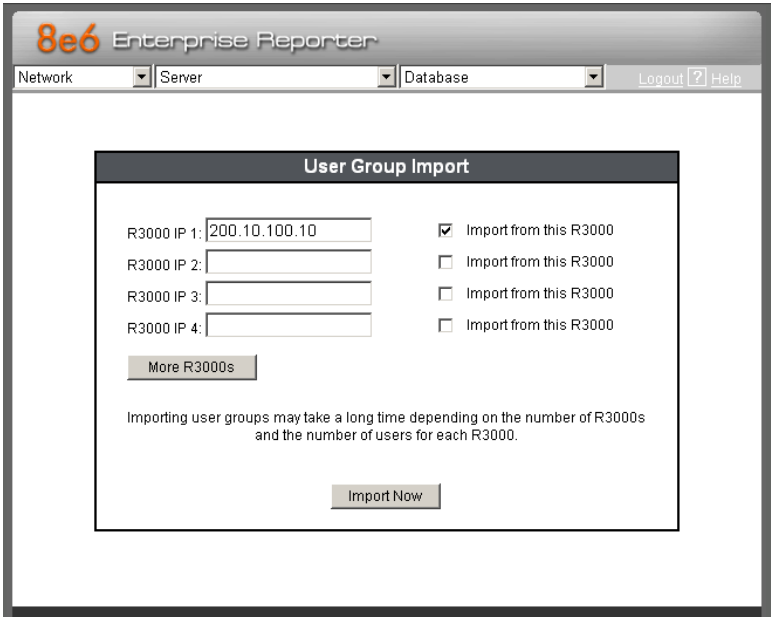


Fig. 1:2-41 User Group Import screen

Import User Groups

***NOTE**: R3000 IP fields are populated by default if one or more R3000 servers are connected to this ER server.*

1. Specify the **R3000 IP** address of each R3000 to send LDAP user group membership data to this ER.
2. Click the checkbox corresponding to “Import from this R3000”.

***NOTE**: If additional R3000 servers need to be specified, click **More R3000s** to display the next four sets of entry fields.*

3. After specifying all R3000 servers, click **Import Now** to begin the data importation process.
4. When the importation process has successfully been completed, a confirmation page displays the following message: “The importing process finished.” Click **OK** to return to the User Group Import screen.

***NOTE**: User groups will be imported in the exact format defined on the R3000.*

TECHNICAL SUPPORT / PRODUCT WARRANTIES

Technical Support

For technical support, visit 8e6 Technologies's Technical Support Web page at **http://www.8e6.com/support.html**, or contact us by phone, by e-mail, or in writing.

Hours

Regular office hours are from Monday through Friday, 8 a.m. to 5 p.m. PST.

After hours support is available for emergency issues only. Requests for assistance are routed to a senior-level technician through our forwarding service.

Contact Information

Domestic (United States)

1. Call **1-888-786-7999**
2. Select *option 3*

International

1. Call **+1-714-282-6111**
2. Select *option 3*

E-Mail

For non-emergency assistance, e-mail us at **support@8e6.com**

Office Locations and Phone Numbers

8e6 Corporate Headquarters (USA)

828 West Taft Avenue
Orange, CA 92865-4232
USA

Local	:	714.282.6111
Fax	:	714.282.6116
Domestic US	:	1.888.786.7999
International	:	+1.714.282.6111

8e6 Taiwan

7 Fl., No. 1, Sec. 2, Ren-Ai Rd.
Taipei 10055
Taiwan, R.O.C.

Taipei Local	:	2397-0300
Fax	:	2397-0306
Domestic Taiwan	:	02-2397-0300
International	:	886-2-2397-0300

Support Procedures

When you contact our technical support department:

- You will be greeted by a technical professional who will request the details of the problem and attempt to resolve the issue directly.
- If your issue needs to be escalated, you will be given a ticket number for reference, and a senior-level technician will contact you to resolve the issue.
- If your issue requires immediate attention, such as your network traffic being affected or all blocked sites being passed, you will be contacted by a senior-level technician within one hour.
- Your trouble ticket will not be closed until your permission is confirmed.

Product Warranties

Standard Warranty

8e6 Technologies warrants the medium on which the 8e6 product is provided to be free from defects in material and workmanship under normal use for period of one year (the "Warranty Period") from the date of delivery. This standard Warranty Period applies to both new and refurbished equipment for a period of one year from the delivery date. 8e6 Technologies' entire liability and customer's exclusive remedy if the medium is defective shall be the replacement of the hardware equipment or software provided by 8e6 Technologies.

8e6 Technologies warrants that the 8e6 product(s) do(es) not infringe on any third party copyrights or patents. This warranty shall not apply to the extent that infringement is based on any misuse or modification of the hardware equipment or software provided. This warranty does not apply if the infringement is based in whole or in part on the customer's modification of the hardware equipment or software.

8e6 Technologies specifically disclaims all express warranties except those made herein and all implied warranties; including without limitation, the implied warranties of merchantability and fitness for a particular purpose. Without limitation, 8e6 Technologies specifically disclaims any warranty related to the performance(s) of the 8e6 product(s). Warranty service will be performed during 8e6 Technologies' regular business hours at 8e6 Technologies' facility.

Technical Support and Service

8e6 Technologies will provide initial installation support and technical support for up to 90 days following installation. 8e6 Technologies provides after-hour emergency support to 8e6 server customers. An after hours technician can be reached by voice line.

Technical support information:

Online: http://www.8e6.com/support.html

Toll Free: 888-786-7999, *press 3*

Telephone: 1+714-282-6111, *press 3*

E-mail: support@8e6.com

Have the following information ready before calling technical support:

Product Description: _____

Purchase Date: _____

Extended warranty purchased: _____

Plan # _____

Reseller or Distributor contact: _____

Customer contact: _____

Extended Warranty (optional)

The extended warranty applies to hardware and software of the product(s) except any misuse or modification of the product(s), or product(s) located outside of the United States. The extended warranty does not include new product upgrades. Hardware parts will be furnished as necessary to maintain the proper operational condition of the product(s). If parts are discontinued from production during the Warranty Period, immediate replacement product(s) or hardware parts will be available for exchange with defective parts from 8e6 Technologies' local reseller or distributor.

Extended Technical Support and Service

Extended technical support is available to customers under a Technical Support Agreement. Contact 8e6 Technologies during normal business hours, 8 a.m. to 5 p.m. PST, at (888) 786-7999, or if outside the United States, call 1+(714) 282-6111.

APPENDICES SECTION

Appendix A

Evaluation Mode

By default, the ER Server and Client are set to the evaluation mode. This appendix explains how to use the ER Server in the evaluation mode, and how to activate the ER Server to function in the activated mode.

Administrator Console

After logging on the Server, the ER Status pop-up box opens to inform you that the ER unit is currently in the evaluation mode:

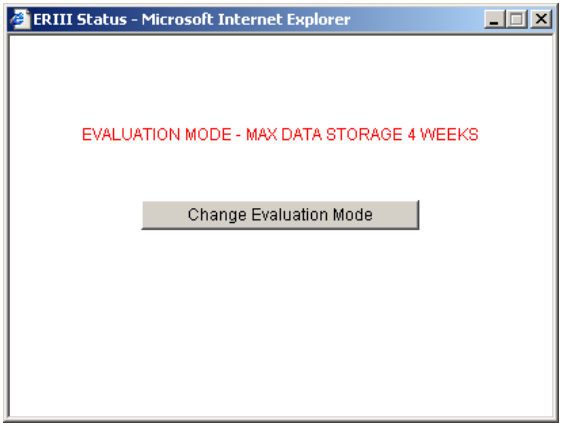


Fig. A-1 ER Status pop-up box

The Server will store data for the period specified in the pop-up box: “EVALUATION MODE - MAX DATA STORAGE ‘X’ WEEKS”—in which ‘X’ represents the maximum number of weeks in the ER’s data storage scope.

You have the option to either use the ER unit in the evaluation mode, or change the evaluation mode in one of two ways—by extending the evaluation period, or by activating the unit so that it can be used in the activated mode.

***NOTE**: The message: "EVALUATION MODE - MAX DATA STORAGE 'X' WEEKS" also displays at the top of the Expiration screen in the Administrator console. Refer to the Expiration screen sub-section in Chapter 2 of the Administrator Section for more information about data storage and expiration.*

Use the Server in the Evaluation Mode

To use the unit in the evaluation mode, click the "X" in the upper right corner of the ER Status pop-up box to close it.

Expiration screen

In the evaluation mode, the Expiration screen can only be used for viewing data storage statistics, and not for modifying data storage capacity criteria.

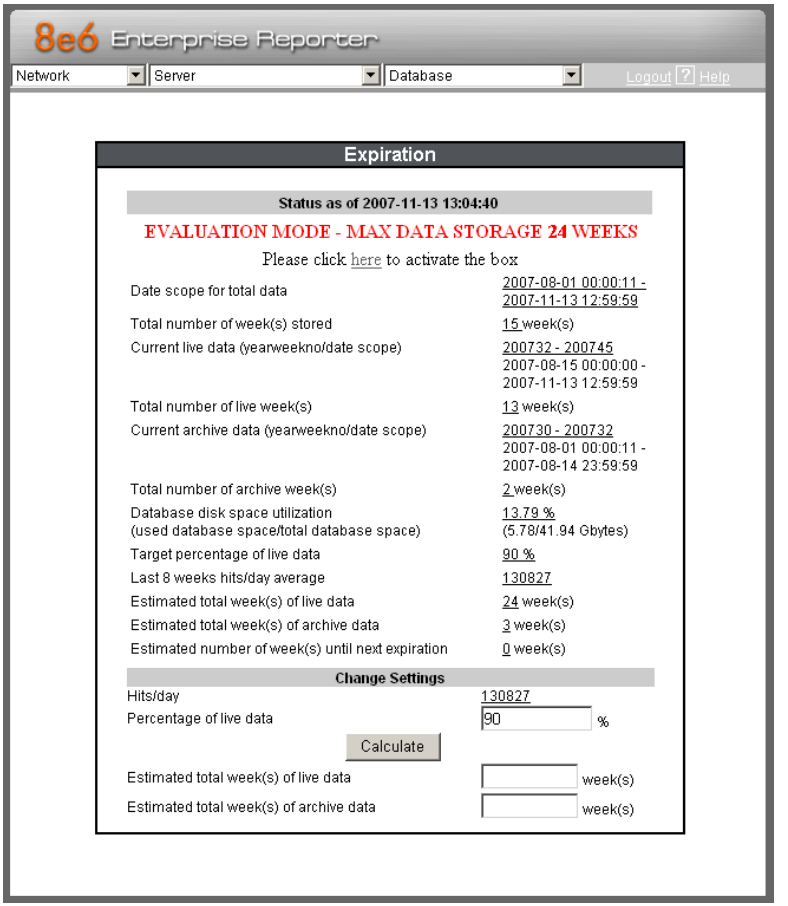


Fig. A-2 Expiration screen

When the Server is in the evaluation mode, the following message displays at the top of the screen: “Evaluation Mode – Max Data Storage ‘X’ Weeks” (in which ‘X’ represents the maximum number of weeks in the ER’s data storage scope).

Since the evaluation period is set for a fixed time period, you cannot make adjustments to the amount of data that will be stored on the Server. Thus, the **Save** button is not included at the bottom of the screen.

Change the Evaluation Mode

After the designated evaluation period has expired, you may extend your evaluation period, or activate the unit and use it in the activated mode. There are two ways to change the evaluation mode from the Administrator console:

- in the ER Status pop-up box (see Fig. A-1), click **Change Evaluation Mode**
- in the Evaluation screen, click the link (“here”) in the message at the top of the screen: “Please click here to activate the box”.

By clicking the button or link, the Activation Page pop-up box opens:

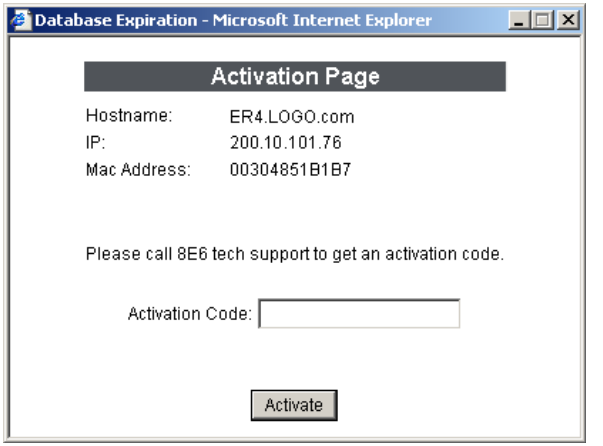


Fig. A-3 Activation Page pop-up box

Activation Page

1. In the Activation Page pop-up box, the **Hostname** of the Server, **IP** address, and **Mac Address** (Media Access Control address) display.
2. Call 8e6 Technologies at either 714-282-6111 or 1-888-786-7999, and speak to a technical support representative about changing the evaluation mode.

   The technical support representative will ask you for the following information:

   a. Hostname, IP address, and Mac Address.

   b. How you wish to change the evaluation mode. You may select either option:

   - extend the evaluation mode for 2, 4, or 8 weeks, or
   - change the evaluation mode to the activated mode.

   After obtaining this information from you, the technical support representative will issue you an activation code.
3. Enter the activation code in the **Activation Code** field.

4. Click **Activate** to display the confirmation message in the Activation Page pop-up box:
   - If extending the evaluation period for the unit, the following message displays: “It is now in evaluation mode (‘X’ weeks)!” in which ‘X’ represents the number of weeks in the new evaluation period.
   - If activating the unit, the following message displays: “Your box has been activated!”
5. Click **CLOSE** to close the Activation Page pop-up box.

Appendix B

Disable Pop-up Blocking Software

A user with pop-up blocking software installed on his/her workstation will need to disable pop-up blocking in order to use the Client.

This appendix provides instructions on how to disable pop-up blocking software for the following products: Yahoo! Toolbar, Google Toolbar, AdwareSafe, and Windows XP Service Pack 2 (SP2).

Yahoo! Toolbar Pop-up Blocker

Add the Client to the White List

If the Client was previously blocked by the Yahoo! Toolbar, it can be moved from the black list and added to the white list so that it will always be allowed to pass. To do this:

1. Go to the Yahoo! Toolbar and click the pop-up icon to open the pop-up menu:

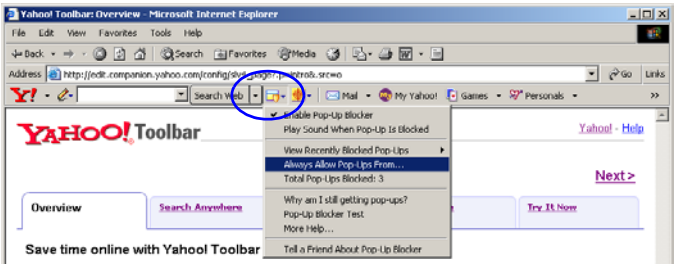


Fig. B-1 Select menu option Always Allow Pop-Ups From

2. Choose Always Allow Pop-Ups From to open the Yahoo! Pop-Up Blocker dialog box:

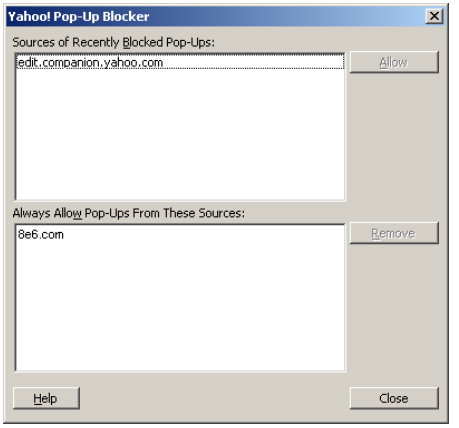


Fig. B-2 Allow pop-ups from source

3. Select the source from the Sources of Recently Blocked Pop-Ups list box to activate the Allow button.
4. Click **Allow** to move the selected source to the Always Allow Pop-Ups From These Sources list box.
5. Click **Close** to save your changes and to close the dialog box.

Google Toolbar Pop-up Blocker

Add the Client to the White List

To add the Client to the white list so that it will always be allowed to pass, go to the Google Toolbar and click the # blocked icon:

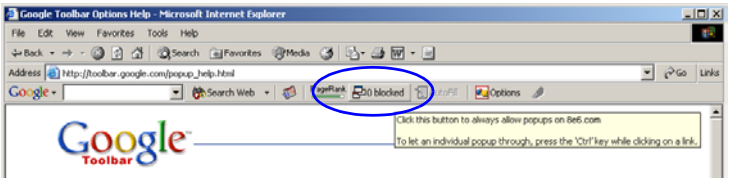


Fig. B-3 # blocked icon enabled

Clicking this icon toggles to the Site pop-ups allowed icon, adding the Client to your white list:

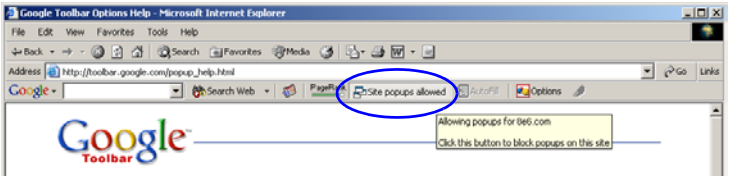


Fig. B-4 Site pop-ups allowed icon enabled

AdwareSafe Pop-up Blocker

Disable Pop-up Blocking

AdwareSafe's SearchSafe toolbar lets you toggle between enabling pop-up blocking (# popups blocked) and disabling pop-up blocking (Popup protection off) by clicking the pop-up icon.

1. In the IE browser, go to the SearchSafe toolbar and click the icon for # popups blocked to toggle to Popup protection off. This action turns off pop-up blocking.
2. After you are finished using the Client, go back to the SearchSafe toolbar and click the icon for Popup protection off to toggle back to # popups blocked. This action turns on pop-up blocking again.

Windows XP SP2 Pop-up Blocker

This sub-section provides information on setting up pop-up blocking and disabling pop-up blocking in Windows XP SP2.

Set up Pop-up Blocking

There are two ways to enable the pop-up blocking feature in the IE browser.

Use the Internet Options dialog box

1. From the IE browser, go to the toolbar and select **Tools > Internet Options** to open the Internet Options dialog box.
2. Click the Privacy tab:

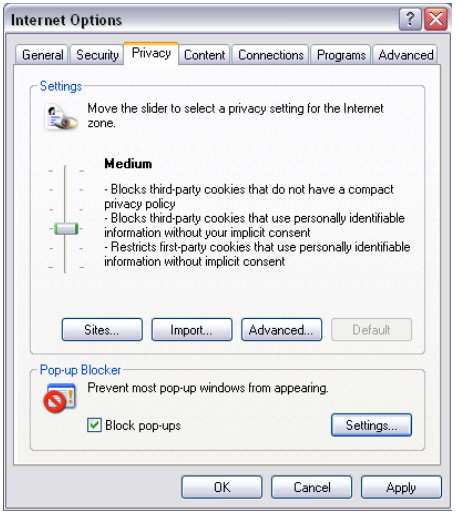


Fig. B-5 Enable pop-up blocking

3. In the Pop-up Blocker frame, check “Block pop-ups”.
4. Click **Apply** and then click **OK** to close the dialog box.

Use the IE Toolbar

In the IE browser, go to the toolbar and select **Tools > Pop-up Blocker > Turn On Pop-up Blocker**:

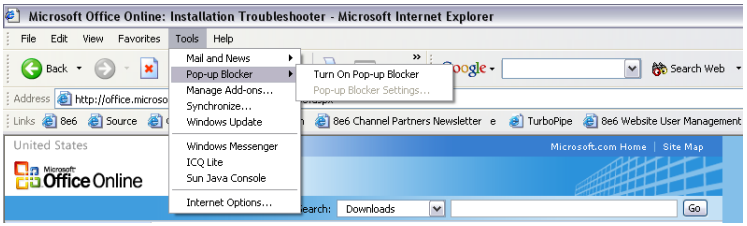


Fig. B-6 Toolbar setup

When you click Turn On Pop-up Blocker, this menu selection changes to Turn Off Pop-up Blocker and activates the Pop-up Blocker Settings menu item.

You can toggle between the On and Off settings to enable or disable pop-up blocking.

Add the Client to the White List

There are two ways to disable pop-up blocking for the Client and to add the Client to your white list.

Use the IE Toolbar

1. With pop-up blocking enabled, go to the toolbar and select **Tools > Pop-up Blocker > Pop-up Blocker Settings** to open the Pop-up Blocker Settings dialog box:

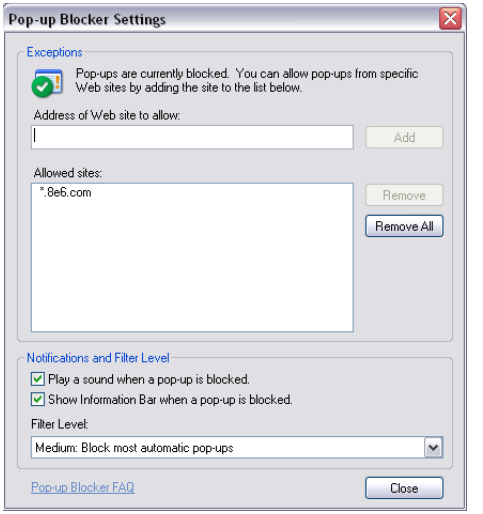


Fig. B-7 Pop-up Blocker Settings

2. Enter the **Address of Web site to allow**, and click **Add** to include this address in the Allowed sites list box. Click **Close** to close the dialog box. The Client has now been added to your white list.

Use the Information Bar

With pop-up blocking enabled, the Information Bar can be set up and used for viewing information about blocked pop-ups or allowing pop-ups from a specified site.

Set up the Information Bar

1. Go to the toolbar and select **Tools > Pop-up Blocker > Pop-up Blocker Settings** to open the Pop-up Blocker Settings dialog box (see Fig. B-7).
2. In the Notifications and Filter Level frame, click the checkbox for “Show Information Bar when a pop-up is blocked.”
3. Click **Close** to close the dialog box.

Access the Client

1. Click the Information Bar for settings options:

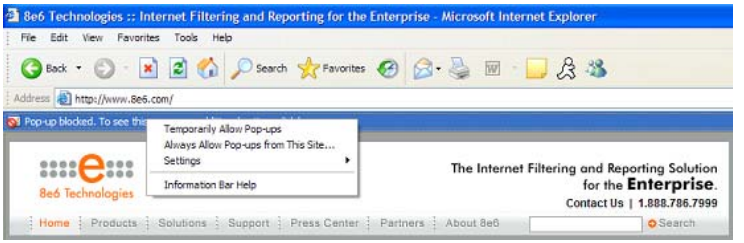


Fig. B-8 Information Bar menu options

2. Select Always Allow Pop-ups from This Site—this action opens the Allow pop-ups from this site? dialog box:

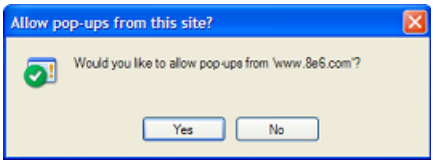


Fig. B-9 Allow pop-ups dialog box

3. Click **Yes** to add the Client to your white list and to close the dialog box.

***NOTE**: To view your white list, go to the Pop-up Blocker Settings dialog box (see Fig. B-7) and see the entries in the Allowed sites list box.*

Appendix C

RAID Maintenance

This appendix pertains to ER “H”, “SL”, and “HL” servers and is divided into three parts: Hardware Components, Server Interface, and Troubleshooting—in the event of a failure in one of the drives, power supplies, or fans.

***NOTE**: As part of the ongoing maintenance procedure for your RAID server, 8e6 recommends that you always have a spare drive and spare power supply on hand.*

Contact 8e6 Technical Support for replacement hard drives and power supplies.

Part 1: Hardware Components

The ER “H”, “SL”, and “HL” RAID server contains four hard drives, two power supplies, and five sets of dual cooling fans (10 in total). These components are depicted in the diagram below:

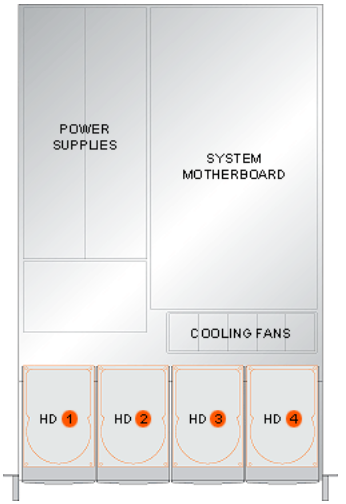
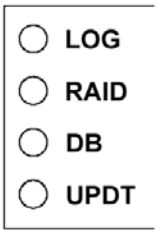


Fig. C-1 ER RAID Server components

Part 2: Server Interface

LED indicators in SL and HL units

On an “SL” and “HL” unit, the following LED indicators for software and hardware status monitoring display on the left side of the front panel:



- LOG = Log Download Status
- RAID = Hard Drive Status
- DB = Database Status
- UPDT = Software Update Status

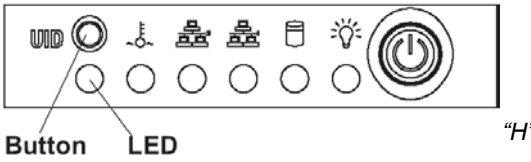
LED Indicator Chart

Below is a chart of LED indicators in the “SL” and “HL” unit:

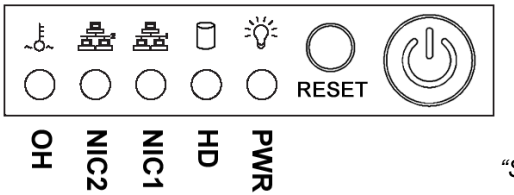
LED Indicator	Color	Condition	Description
LOG	Green	On	Downloading a log
	--	Off	No log download detected
RAID	Green	On	RAID mode enabled and running
	--	Off	RAID mode is inactive
	Red	On	Hard drive fault or failure
DB	Green	On	Database is active
	Red	On	Database in inactive
UPDT	Amber	On	Software update detected
	--	Off	No software update detected

Front control panels on H, SL, and HL units

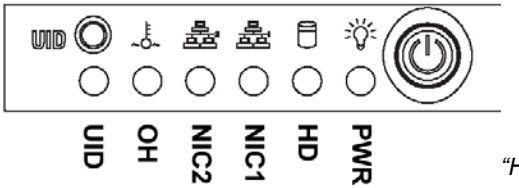
Control panel buttons, icons, and LED indicators display on the right side of the front panel. The buttons let you perform a function on the unit, while an LED indicator corresponding to an icon alerts you to the status of that feature on the unit.



"H" chassis front panel



"SL" chassis front panel



"HL" chassis front panel

The buttons and LED indicators for the depicted icons function as follows:

UID (button) – On an "H" or "HL" server, when the UID button is pressed, a steady blue LED displays on both the front and rear of the chassis (see also Rear of chassis). These indicators are used for easy location of the chassis in a large stack configuration. The LED remains on until the button is pressed a second time.

Overheat/Fan Fail (icon) – This LED is unlit unless the chassis is overheated. A flashing red LED indicates a fan failure. A steady red LED (on and not flashing) indicates an overheating condition, which may be caused by cables obstructing the airflow in the system or the ambient room temperature being too warm.

NIC2 (icon) – A flashing green LED indicates network activity on LAN2. The LED is a steady green with link connectivity, and unlit if there with no link connectivity.

NIC1 (icon) – A flashing green LED indicates network activity on LAN1. The LED is a steady green with link connectivity, and unlit if there with no link connectivity.

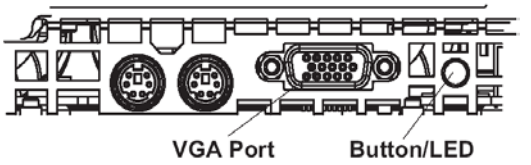
HDD (icon) – In addition to displaying in the control panel, this icon also displays on the front panel on each hard drive carrier. Hard drive activity is indicated by a green LED on an “H” or “HL” server, and by an amber LED on an “SL” server. An unlit LED on a drive carrier may indicate a hard drive failure. (See Hard drive failure in the Troubleshooting sub-section for information on detecting a hard drive failure and resolving this problem.)

Power (icon) – The LED is unlit when the server is turned off. A steady green LED indicates power is being supplied to the unit’s power supplies. (See also Rear of chassis.) (See Power supply failure in the Troubleshooting sub-section for information on detecting a power supply failure and resolving this problem.)

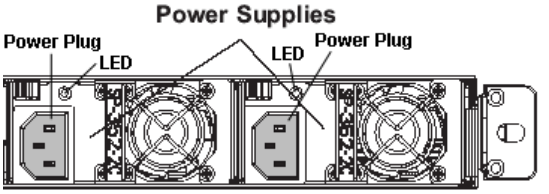
Power (button) – When the power button is pressed, the main power to the server is turned on. When the power button is pressed again, the main power to the server is removed but standby power is still supplied to the server.

Rear panels on H and HL units

UID (LED indicator) – On the rear of the “H” or “HL” chassis, to the left of the power supplies, a steady blue UID LED indicator displays when the UID button on the control panel is pressed. This LED remains lit until the UID button is pressed again.



Power Supplies (LED indicators) – The power supplies are located at the right on the rear of the chassis. An LED indicator is located above each of the power plugs. (See Power supply failure in the Troubleshooting sub-section for information on detecting a power supply failure and resolving this problem.)



Part 3: Troubleshooting

The text in this section explains how the server alerts the administrator to a failed component, and what to do in the event of a failure.

Hard drive failure

Step 1: Review the notification email

If a hard drive fails, a notification email is sent to the administrator of the server. This email identifies the failed hard drive by its number (HD 1, HD 2, HD 3, or HD 4). Upon receiving this alert, the administrator should verify the status of the drives by first going to the Hardware Failure Detection screen in the Administrator console.

***WARNING**: Do not attempt to remove any of the drives from the unit at this time. Verification of the failed drive should first be made in the Administrator console before proceeding, as data on the server will be lost in the event that the wrong drive is removed from the unit.*

Step 2: Verify the failed drive in the Admin console

The Hardware Failure Detection screen in the Administrator console is accessible via the **Server > Hardware Failure Detection** menu selection:

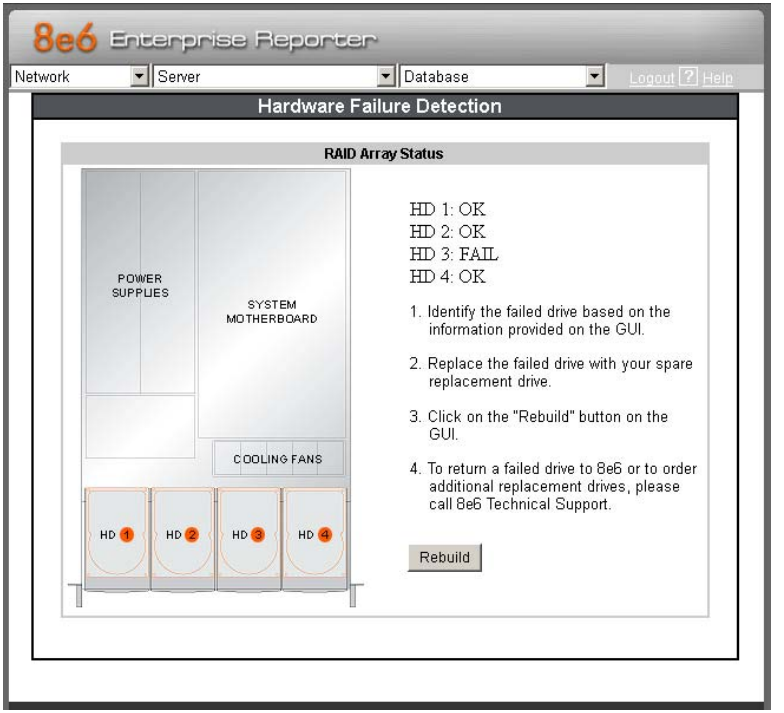


Fig. C-2 Hardware Failure Detection screen

The Hardware Failure Detection screen displays the current RAID Array Status for the four hard drives (HD 1, HD 2, HD 3, and HD 4) in text that appears at the right of the screen.

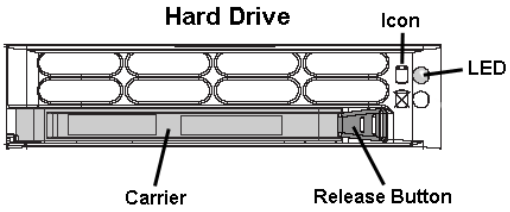
Normally, when all four hard drives are functioning without failure, the text “OK” displays for the corresponding hard drive number, and no other text displays in the screen.

However, if a hard drive has failed, the message “FAIL” displays for the corresponding hard drive number.

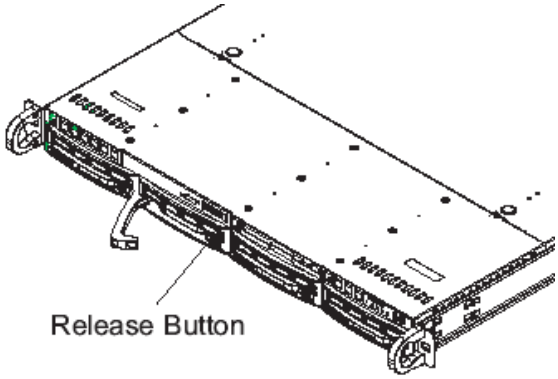
Before taking any action in this screen, proceed to Step 3.

Step 3: Replace the failed hard drive

After verifying the failed hard drive in the Administrator console, go to the server to replace the drive.



Press the red release button to release the handle on the carrier, and then extend the handle fully and pull the carrier out towards you. Replace the failed drive with your spare replacement drive.



***NOTE**: Contact Technical Support if you have any questions about replacing a failed hard drive.*

Step 4: Rebuild the hard drive

Once the failed hard drive has been replaced, return to the Hardware Failure Detection screen in the Administrator console, and click **Rebuild** to proceed with the rebuild process.

***WARNING**: When the RAID array reconstruction process begins, the message "Enterprise Reporter Functionality Suspended, Drive Rebuild in Process" displays and the hard drive becomes inaccessible.*

Step 5: Contact Technical Support

Contact Technical Support to order a new replacement hard drive and for instructions on returning your failed hard drive to 8e6.

Power supply failure

Step 1: Identify the failed power supply

The administrator of the server is alerted to a power supply failure on the chassis by an audible alarm and an amber power supply LED—or an unlit LED—on the front and rear of the chassis.

***NOTE**: A steady amber power supply LED also may indicate a disconnected or loose power supply cord. Verify that the power supply cord is plugged in completely before removing a power supply.*

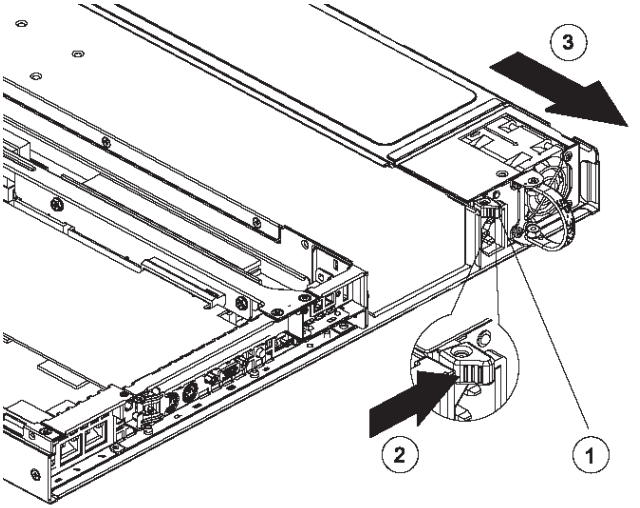
***WARNING**: Be sure the correct failed power supply has been identified. Removing the wrong power supply will cause the system to crash.*

Step 2: Unplug the power cord

To prevent electrical shock to yourself and damage to the unit, unplug the power cord from the failed power supply.

Step 3: Replace the failed power supply

Remove the failed power supply by locating the red release tab (1) and pushing it to the right (2), then lifting the curved metal handle and pulling the power supply module towards you (3).



Note that an audible alarm sounds and the LED is unlit when the power supply is disengaged. Replace the failed power supply with your spare replacement power supply. The alarm will turn off and the LED will be a steady green when the replacement power supply is securely locked in place.

Step 4: Contact Technical Support

Contact Technical Support to order a new replacement power supply and for instructions on returning your failed power supply to 8e6.

Fan failure

Identify a fan failure

A flashing red LED indicates a fan failure. If this displays on your unit, contact Technical Support for an RMA (Return Merchandise Authorization) number and for instructions on returning the unit to 8e6.

A steady red LED (on and not flashing) indicates an over-heating condition, which may be caused by cables obstructing the airflow in the system or the ambient room temperature being too warm. Check the routing of the cables and make sure all fans are present and operating normally. The LED will remain steady as long as the over-heating condition exists.

INDEX

A

Access Client *68*
add/edit/delete administrators *16*
Add/Edit/Delete Administrators screen *23*
administrator
    e-mail contact setup *47*
    log in to Server *16*
Administrator console *19*
alert box, terminology *4*
archive
    data setup on Server *87*
    terminology *88*

B

back up data
    internal on demand backup *44*
    to remote server *45*
backup
    procedures *42*
Backup screen *42*
Block Request Count *98*
Box Mode screen *21*
button, terminology *4*

C

checkbox, terminology *4*
Client *1*, *8*, *15*, *19*, *21*, *32*, *71*, *74*, *94*
    diagnostic reports *84*
    evaluation mode *110*
    troubleshoot problems *83*
    User Guide *9*
components *10*
Conventions *3*

D

data storage setup *87*
Database Menu *71*
database status logs *83*
Date Scope
    Expiration screen *87*
diagnostic reports *83*
Diagnostics *35*
dialog box, terminology *4*
disable pop-up blockers *116*

E

Elapsed Time *79*
expiration *89*
Expiration screen *87*
expire
    data from Server *87*
    passwords *100*
    terminology *89*

F

field, terminology *5*
File Transfer Protocol (FTP) *8*, *44*, *63*
frame, terminology *5*
FTP (File Transfer Protocol) *8*, *44*, *45*, *46*, *63*

G

generate
    static table of IP addresses, machine names *75*

H

hardware *10*
Hardware Failure Detection screen *69*
HL server *125*

I

install
Server patch *58*
Internet Explorer *11*, *119*
IP.ID *71*

L

LDAP *102*
LED indicators *126*
Linux OS *10*
list box, terminology *5*
live
data setup on Server *87*
terminology *88*
Locked-out Accounts and IPs screen *26*
lockout *100*
log
database status *84*
off the Server *17*
on the Server *13*

M

Manual Backup button *44*
Manual Restore button *46*
MySQL *1*, *10*, *64*

N

NAS Status screen *95*
Network Diagnostics screen *35*
Network Menu *20*
network requirements *11*
Network Settings screen *28*
Network Time Protocol (NTP) *33*
NIC Mode screen *65*
NTP (Network Time Protocol) *33*

O

Object Count *99*
Optional Features screen *96*

P

Page Count *99*
Page Definition screen *81*
Page View Elapsed Time screen *79*
password
    create for Administrator GUI *16*
    create for remote server's FTP account *44*
    security option *100*
patch
    Server *56*
    unapply *57*
Ping *36*
pop-up blocking, disable *116*
pop-up box/window, terminology *5*
Product Warranties section *107*
Proxy Setting *62*
pull-down menu, terminology *5*

Q

Quick Start Guide *8*, *12*, *96*

R

R3000 *1*, *41*, *61*, *102*
radio button, terminology *6*
RAID *69*, *125*
Regional Setting screen *32*
remote server backup *45*
reports
    diagnostic *84*
restart the Server *63*
restore data from backup *46*
Routing Table screen *30*
rules
    elapsed time *80*

expiration *89*

S

screen, terminology *6*
Search String Reporting *98*
Secure Access screen *53*
Self Monitoring screen *47*
Server
add, maintain routers *30*
download patch *56*
perform manual backup *44*
restart *63*
restore data from previous backup *46*
set time *32*
set up IP addresses *28*
shut down *63*
store data, change settings *87*
Server Menu *41*
Server Status screen *51*
Shut Down screen *63*
SL server *125*
SMTP Server Setting screen *49*
SNMP screen *39*
software *10*
Software Update screen *56*
Software Update Setting screen *61*

T

table, terminology *6*
technical support *53*
Technical Support section *104*
Terminology *4*
text box, terminology *6*
Tools screen *83*
Trace Route *37*

U

update
NTP server settings *33*

routing table *31*
Server software *56*
User Group Import screen *102*
User Name Identification screen *71*
Username Display Setting screen *76*

V

view
diagnostic reports *84*

W

Wall Clock Time *98*
Web Client Server Management screen *67*
window, terminology *7*
workstation requirements *11*