8e6 Technologies

8e6® Appliance Watchdog

USER
GUIDE

Models: ER, R3000, R3000IR, ProxyBlocker, TAR

Release 2.0.00 • Manual Version 1.01

8E6 APPLIANCE WATCHDOG ADMINISTRATOR USER GUIDE

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.

8E6 TECHNOLOGIES, APPLIANCE WATCHDOG ADMINISTRATOR USER GUIDE

CONTENTS

APPLIANCE WATCHDOG OVERVIEW

The 8e6 Appliance Watchdog provides monitoring services for the 8e6 Internet filtering and management appliances. This application runs on the network administrator's desktop, notifying him/her if problems occur with the network or equipment associated with content filtering.

About this User Guide

The 8e6 Appliance Watchdog User Guide addresses the administrator designated to configure the 8e6 Appliance Watchdog and monitor 8e6 appliances on the network.

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 8e6 Appliance Watchdog.

- **Administrator Section** - Refer to this section for information on configuring and maintaining the Appliance Watchdog via the Administrator console application.

- **Technical Support Section** - This section contains information on technical support coverage.

- **Index** - This section includes an index of topics and the first page numbers where they appear in this user guide.

How to Use 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.*

Terminology

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

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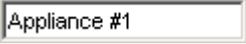
- **frame** - a boxed-in area in a dialog box, window, or screen that includes a group of objects such as fields, text boxes, list boxes, buttons, radio buttons, checkboxes, and/or tables. Objects within a frame belong to a specific function or group. A frame often is labeled to indicate its function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

- **icon** - a small image in a dialog box, window, or screen that can be clicked. This object can be a button or an executable file.

- **navigation panel** - the panel that displays at the left of a screen. This panel can contain links that can be clicked to open windows or dialog boxes at the right of the screen. One or more tree lists also can display in this panel. When an item in the tree list is double-clicked, the tree list opens to reveal items that can be selected.

- **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.

- **screen** - a main object of an application that displays across your monitor. A screen can contain panels, windows, frames, fields, tables, text boxes, icons, buttons, and checkboxes.
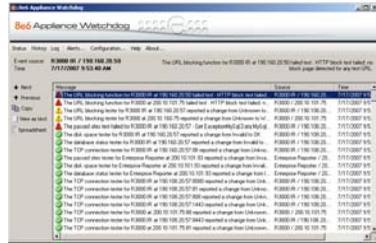
- **table** - a section of a screen containing a list of records populated by the application.

- **text box** - an area in a dialog box, window, or

screen that accommodates your data entry. A text box is a type of field. (See "field".)

- **tree** - a tree displays in the naviga-tion panel of a screen, and is comprised of a hierarchical list of items. An entity associated with a branch of the tree is preceded by a plus (+) sign when the branch is

collapsed. By double-clicking the item, a minus (-) sign replaces the plus sign, and any entity within that branch of the tree displays. An item in the tree is selected by clicking it.
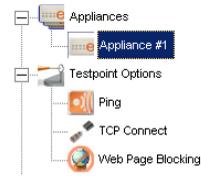
- **window** - a window
  displays on a screen,
  and can contain frames,
  fields, text boxes, list
  boxes, buttons, and
  checkboxes. Types of
  windows include pop-up windows, login windows, or
  ones from the system such as the Save As or Choose file
  windows.

ADMINISTRATOR SECTION

Introduction

The authorized administrator of the Appliance Watchdog is responsible for setting up the application and adding 8e6 appliances to be monitored. To attain this objective, the administrator performs the following tasks:

- installs and configures the Appliance Watchdog on a designated workstation

- adds 8e6 appliances to be monitored by the Appliance Watchdog

- analyzes logs generated by the application

- establishes alert notifications for network problems affecting 8e6 appliances

Environment Requirements

Workstation Requirements

Minimum system requirements for the administrator include the following:

- Windows XP 32-bit or 64-bit, Windows Server 2003 Enterprise x64, and Windows 2000 Professional

- 256 MB RAM minimum, 1 GB RAM recommended

- 100 MB hard drive space for running log files

- Microsoft .NET Framework 2.0 runtime application

- Microsoft Windows Installer 3.0

Network Requirements

- High speed connection from the Appliance Watchdog application to 8e6 appliances set up to be monitored

Chapter 1: Watchdog Installation

Install 8e6 Appliance Watchdog

1. Go to **http://www.8e6.com/software-updates/8e6-appliance-watchdog-updates**.

2. Click the link for the 8e6 Appliance Watchdog application .msi file to launch the 8e6 Appliance Watchdog Setup wizard:

Fig. 1:1-1 Pre-installation message

NOTE: *If prompted, install Microsoft .NET Framework 2.0. Note that Framework may require updating other Windows components—such as Microsoft Windows Installer 3.0—before installing the Appliance Watchdog.*

3. After closing any open Windows applications, click **Next** to display the End User License Agreement (EULA):
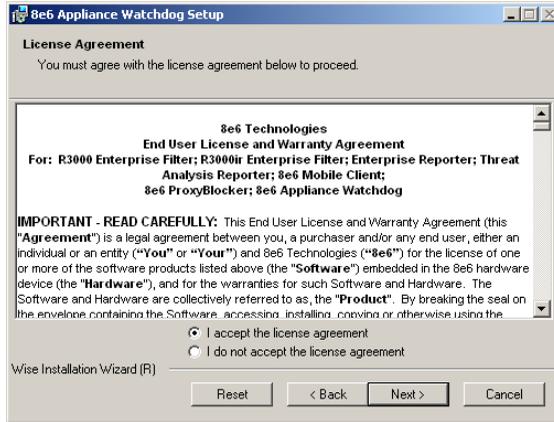
Fig. 1:1-2 8e6 Appliance Watchdog EULA

4. Read the EULA, and if you agree with its terms, click the radio button corresponding to "I accept the license agreement" to activate the Next button.

5. Click **Next** to review the Readme information for this software release:
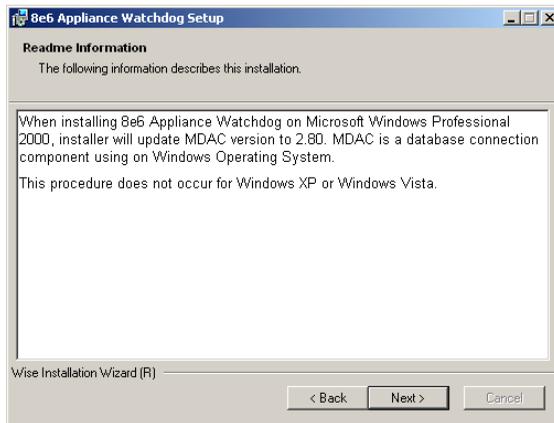
Fig. 1:1-3 Readme information

6. Click **Next** to specify the destination folder for installing Watchdog:
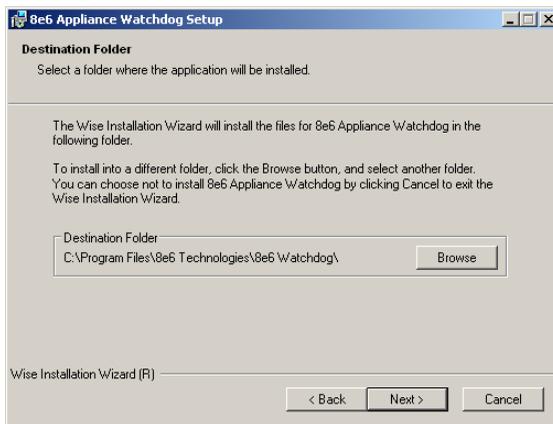
Fig. 1:1-4 Destination Folder selection

💡 *TIP: To select a folder for installing Watchdog other than the default 8e6 Watchdog folder, click Browse to open a pop-up window that lets you choose the destination folder.*

7. Click **Next** to confirm that you wish to proceed with the installation process:

Fig. 1:1-5 Ready to Install the Application

8. Click **Next** to begin installing 8e6 Appliance Watchdog on your machine:
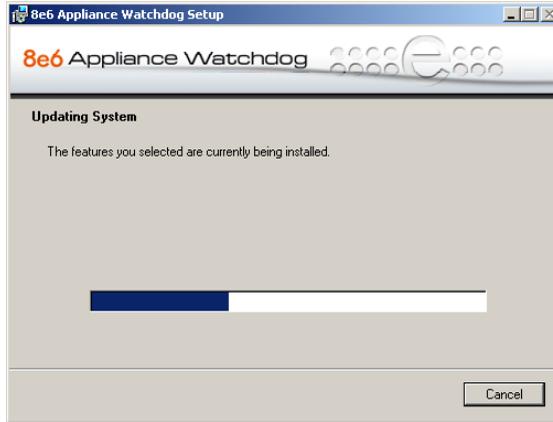
Fig. 1:1-6 8e6 Appliance Watchdog installation

When the 8e6 Appliance Watchdog installation setup process has successfully finished, completion informa-tion displays:

Fig. 1:1-7 Installation complete

9. Click **Finish** to close the installation setup window and to open the 8e6 Appliance Watchdog console (see Fig. 1:2-1). The configuration setup for the Appliance Watchdog can be completed now or at a later point in time.

Chapter 2: Access the Admin Console

Launch the Application

There are two ways to launch the application and access the Administrator console:

- **system tray icon** - double-click the orange "e" icon in your system tray (the icon to the left in the image below):

- **Start menu** - if the Watchdog icon is not currently loaded in your system tray, click **Start** in your taskbar, navigate to the Programs menu, and then select the menu item for **8e6 Watchdog > 8e6 Watchdog**:

Clicking the Watchdog system tray icon or selecting the 8e6 Watchdog menu item launches the 8e6 Appliance Watchdog Administrator console—the latter selection also loads the Watchdog icon in your system tray:

Fig. 1:2-1 8e6 Watchdog Appliance console, non-configured

The Administrator console is comprised of a navigation panel to the left, a window to the right, and the following menu items beneath the title banner:

• **Status** - Once Watchdog is configured and running, clicking this menu item displays a status view of all testpoint results.

• **History** - Once Watchdog is configured and running, clicking this menu item displays a history of testpoint state results.

• **Log** - Once Watchdog is configured and running, clicking this menu item displays activity logs.

• **Alerts** - Once Watchdog is configured and running, clicking this menu item opens a pop-up box containing currently active alerts and alert settings.

• **Configuration** - Clicking this menu item opens a window that lets you configure settings for Watchdog and specify criteria for selected options.

• **Help** - Clicking this menu item or pressing the **F1** key on your keyboard opens a browser window containing

online help, with a link to the latest 8e6 Appliance Watchdog Administrator User Guide in the PDF format.

• **About** - Clicking this menu item opens a pop-up box containing the following information about this application: Product version number, 8e6 Web site link, 8e6 Customer support email address link and phone number. Click **OK** to close this pop-up box.

TIP: The Administrator console can be moved by clicking in the title bar while dragging the console to another area of your desktop.

Use the System Tray icon menu

When right-clicking the system tray icon, a menu opens containing the following items:

• Alerts - Selecting this item opens the 8e6 Watchdog - Active Alerts pop-up window that displays information about recent alerts.

• Restore - Selecting this item launches the Administrator console if the console is not already open.

• Exit GUI only - If the console is currently open, selecting this item closes the Administrator console and removes the Watchdog icon from the system tray. If the Administrator console is already closed, only the latter action will be performed.

• Exit and Stop Service - If the console is currently open, selecting this item closes the Administrator console, stops the service from running, and removes the Watchdog icon from the system tray. If the Administrator console is already closed, only the latter two actions will be performed.

TIP: The Administrator console can be re-accessed—and the system tray icon reloaded—by going to the Start menu and selecting 8e6 Watchdog from the menu.

Chapter 3: Watchdog Configuration

After installing the Appliance Watchdog, the first step is to configure the application using the Administrator console.

NOTE: *See the Warnings page in this chapter for special settings to make in your 8e6 applications to allow Watchdog to monitor your appliances.*

Configuration window

The Configuration window is used for setting up 8e6 appliances to be monitored by Watchdog, for specifying settings to check the status of these appliances, and to set up notifications to alert you to any network errors pertaining to these appliances.

Access the Configuration window

In the Administrator console, click the **Configuration** menu item to open the Configuration window:
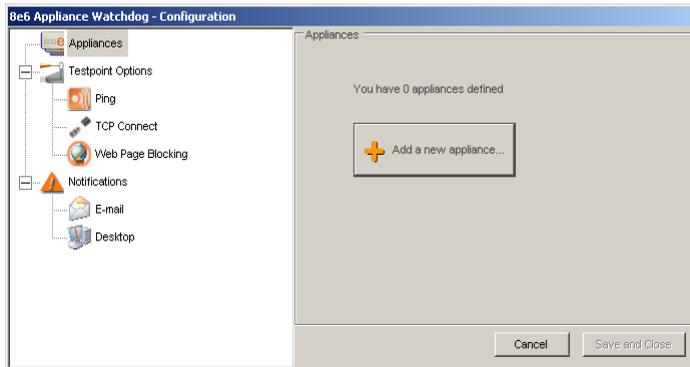
Fig. 1:3-1 Configuration window

The Configuration window is comprised of a tree in the left panel with three main branches—Appliances, Testpoint Options, Notifications—and a frame in the right panel, with

the Cancel button and Save and Close button below this frame.

TIPS: The Configuration window can be moved by clicking in the title bar while dragging the window to another area of your desktop.

To collapse any section of the tree, click the "-" (minus sign). To re-open the collapsed section, click the "+" (plus sign).

To return to the Watchdog Administrator console, click Cancel to close the Configuration window.

Appliances

The Appliances branch of the tree lets you set up and maintain appliances to be monitored by Watchdog.

Add an appliance to be monitored

💡 *TIP: In order to add one or more appliances to be monitored, the Configuration window must display the Appliances frame in the right panel. If this frame does not display, go to the left panel and click the Appliances branch header.*

Access and make entries in the General tab

1. In the Configuration window, click the **Add a new appliance** button in the Appliances frame (see Fig. 1:3-1) to display the Appliance #1 frame in the right panel, with its default General tab:
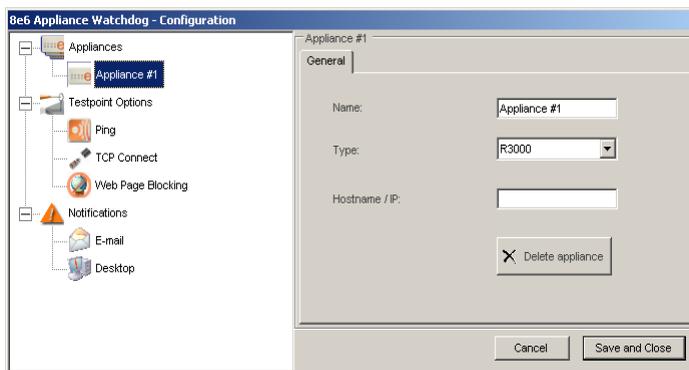
Fig. 1:3-2 Configuration window, add a new appliance

2. Type in the **Name** for the appliance.

3. Select the **Type** of appliance from the available selections in the pull-down menu: R3000, R3000 IR, R3000 Mobile, ProxyBlocker, Enterprise Reporter, Threat Analysis Reporter.

TIP: If using the failover detection feature on an R3000 or R3000IR appliance in a synchronization environment, Watchdog should be set up on separate workstations to monitor separate target servers. A separate Watchdog should also be set up on a separate workstation to monitor the source server.

NOTE: If the appliance you selected is an R3000IR or ER, the Database tab displays in addition to the General tab. See Database tab for information about viewing or making entries in this tab.

4. Type in the **Hostname / IP** address of the appliance. For example, enter *190.160.1.1* for an appliance at that designated IP address.

5. To add another appliance:

   a. Click the Appliances branch header to include the name of appliance you just added in the Appliances tree, and to display the Appliances frame in the right panel with the following message: "You have X appliances defined"—in which 'X' represents the number of appliances that currently display in the Appliances branch of the tree.

   b. Follow steps 1 to 4 for each appliance you add. For the last appliance you add, skip this step and go on to step 6.

TIP: 8e6 recommends not deleting or modifying fields in any newly-added appliance until all settings are saved and Watchdog is restarted.

6. After adding all appliances, click **Save and Close** to stop the service, close the Configuration window and the Administrator console, and to display the pop-up box with the following message: "The 8e6 Watchdog service is restarting..."

Fig. 1:3-3 Restart message box

When the service has restarted, the Administrator console re-opens and displays the Status screen, showing information about the appliance(s) you just added:

Fig. 1:3-4 Console with one appliance added

In the left panel of this screen, the tree displays the name(s) of the appliance(s) and types of testpoints for the appliance(s). In the right panel, the appliance Name, Hostname / IP address, and Device type display for the first appliance in the list, which is highlighted.

Database tab

The Database tab displays if the appliance you added is an ER or R3000IR server:
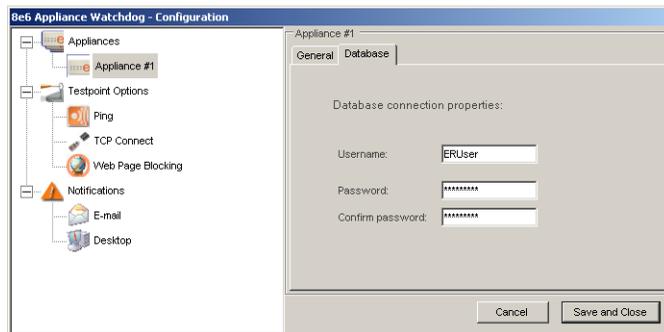
Fig. 1:3-5 Configuration window, Database tab

This tab is used for modifying the ER database password, if necessary. In most cases, the ER database password will not need to be edited. However, if this password has been changed from the default database password, you need to enter that same information in Watchdog in order for Watchdog to access the ER database. To do so:

1. Click the Database tab to display Database connection properities fields.

2. Enter the correct **Password**, and then enter it again in the **Confirm password** field.

3. After all entries are made in this window, click **Save and Close** to save your changes and to restart the service.

Delete appliances

TIP: When deleting appliances, 8e6 recommends that during this process no appliances are either added or modified.

1. From the Configuration window, click the appliance name in the Appliances branch of the tree to display information about that appliance in the right panel:
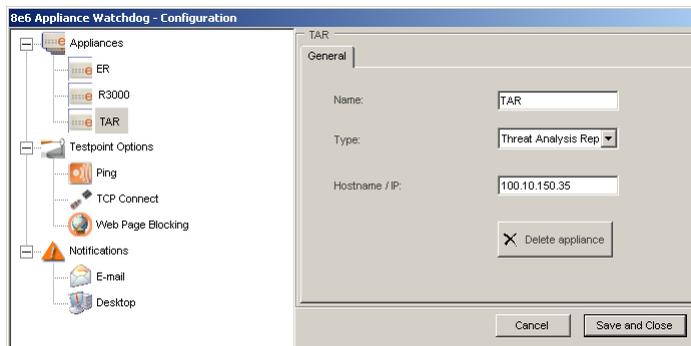
Fig. 1:3-6 Delete an appliance

2. Click **Delete appliance**, and then confirm this request in the subsequent dialog box to remove the appliance name from the Appliances branch of the tree.

3. If any other appliances need to be deleted from the Appliances tree, follow steps 1 and 2 for each appliance name to be removed.

4. After all appliances to be deleted have been removed from the tree, click **Save and Close** to stop the service, remove the configuration for the appliance(s) from Watchdog, and to display the restart service pop-up box (see Fig. 1:3-3).

When the service has restarted, the console re-opens, displaying the refreshed Status screen (see Fig. 1:3-4).

WARNINGS

R3000 and ProxyBlocker - *In order for Watchdog to monitor R3000 filtering, your filtering profile on the workstation with Watchdog installed must have GPORN blocked. To monitor filtering on the ProxyBlocker, PROXY or GPORN must be blocked in your filtering profile on the workstation with Watchdog installed.*

Testpoint URLs are included in shadow.log, which may cause confusion in reporting, as these URLs will increase the GPORN hit count for the R3000, and the GPORN or PROXY hit count for the ProxyBlocker.

The workstation running Watchdog should not have the X Strikes Blocking feature enabled, since this would lock you out from any Web access.

Threat Analysis Reporter - *If Watchdog is monitoring a Threat Analysis Reporter, the workstation running Watchdog should be excluded from monitoring, otherwise you would be locked out from any Web access.*

If there is a network connectivity problem between the workstation running Watchdog and the monitored appliance(s)—e.g. a cable is loose or unplugged—the Watchdog interface will display a failure status, whereas the appliance(s) may be functioning well.

Testpoint Options

Testpoints are a series of checkpoints used for systemati-
cally monitoring each 8e6 appliance added to the Appli-
ances branch of the tree. Each type of appliance has its own
list of testpoints Watchdog uses to determine if that appli-
ance is running successfully.

The following two charts list the different types of testpoints,
indicating which ones are performed on which appliance:

Testpoints Chart - Part 1

8e6 Appliance	Accessibility Ping	Admin Interface	Block Page / Authentication Service (port 81)	URL Filtering
R3000	Yes	Yes: Ports 88 & 1443	Yes	Yes
R3000IR	Yes	Yes: Ports 88 & 1443, 808 & 8843	Yes	Yes
R3000 Mobile	Yes	Yes: Ports 88 & 1443	No	No
ProxyBlocker	Yes	Yes: Ports 88 & 1443	Yes	Yes
Enterprise Reporter	Yes	Yes: Ports 88 & 8080 & 8843	No	No
Threat Analysis Reporter	Yes	Yes: Port 8080	No	No

Testpoints Chart - Part 2

8e6 Appliance	DB Engine / Reporting Service	8e6 Client Service	Database Usage	CMC
R3000	No	No	No	Yes
R3000IR	Yes: Ports 3306, 8080 & 8443	No	Yes	Yes
R3000 Mobile	No	Yes: Port 443	No	No
ProxyBlocker	No	No	No	No
Enterprise Reporter	Yes: Ports 3306, 8080 & 8443	No	Yes	No
Threat Analysis Reporter	Yes: Port 3306	No	No	No

The Testpoint Options branch of the tree consists of three sub-branches for configuring testpoints: Ping, TCP Connect, Web Page Blocking.

Ping

The Ping testpoint sends a network "echo" request to the appliance and waits for a response. If a response is received, the test verifies that the appliance is powered on and connected to the network.

1. Click Ping in the Testpoint Options branch of the tree to display the Ping Testpoint Options frame in the right panel:
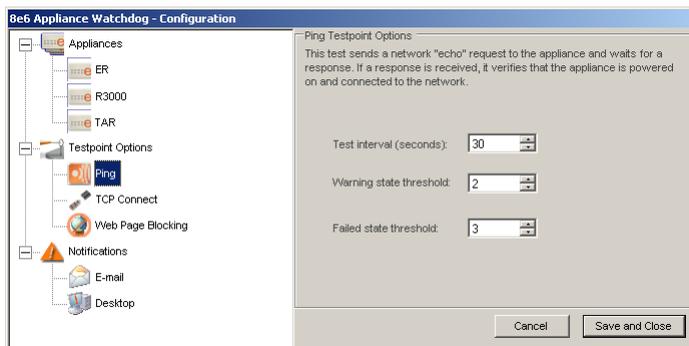
Fig. 1:3-7 Ping Testpoint Options

2. Configure any of the following options by making a numerical selection for that designated field:

   • **Test interval (seconds)** - The number of seconds Watchdog will use in the interval between pings to the appliance. The default is *30* seconds, and the minimum number of seconds that can be selected is *10*.

   • **Warning state threshold** - The number of consecutive tests an appliance can fail before Watchdog issues that appliance a warning state. The default is *2* tests.

   Using these default settings, Watchdog will issue a warning state for the failed appliance after one minute (one failed test in 30 seconds, plus another failed test in the next 30 seconds equals 60 seconds, or one minute).

- **Failed state threshold** - The number of consecutive tests an appliance can fail before Watchdog issues that appliance a failed state. The default is *3* tests.

  Using these default settings, when Watchdog makes a third failed attempt to ping the appliance, the state of that appliance will be upgraded from a warning state to a failed state.

3. Click **Save and Close** to save your configuration and close both the Configuration window and Administrator console, restart the service, and then re-open the console showing the Status screen.

TCP Connect

The TCP Connect testpoint checks for a TCP/IP connection to the appliance. If a response is received, the test verifies that the appliance can receive TCP traffic on the network.

1. Click TCP Connect in the Testpoint Options branch of the tree to display the TCP Connection Testpoint Options frame in the right panel:
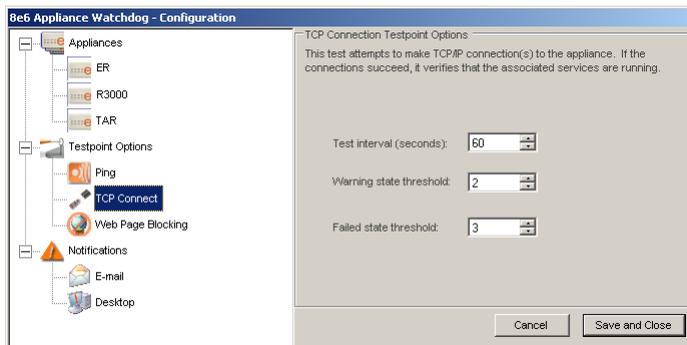
Fig. 1:3-8 TCP Connect

2. Configure any of the following options by making a numerical selection for that designated field:

- **Test interval (seconds)** - The number of seconds Watchdog will use in the interval between attempting to test the TCP connection to the appliance. The default is *60* seconds, and the minimum number of seconds that can be selected is *10*.

- **Warning state threshold** - The number of consecutive tests an appliance can fail before Watchdog issues that appliance a warning state. The default is *2* tests.

  Using these default settings, Watchdog will issue a warning state for the failed appliance every two minutes (one failed test in 60 seconds, plus another failed test in the next 60 seconds equals 120 seconds, or two minutes).

- **Failed state threshold** - The number of consecutive tests an appliance can fail before Watchdog issues that appliance a failed state. The default is *3* tests.

  Using these default settings, when Watchdog makes a third failed attempt to test the TCP connection to the appliance, the state of that appliance will be upgraded from a warning state to a failed state.

3. Click **Save and Close** to save your configuration and close both the Configuration window and Administrator console, restart the service, and then re-open the console showing the Status screen.

Web Page Blocking

The Web Page Blocking testpoint attempts to download Web pages from the Internet that are known to be blocked by the filtering appliance. It checks to see if a blocked page would display if a request is made for a site set up to be blocked by the filter. If a block page is detected, this indicates that basic URL blocking functions are working.

1. Click Web Page Blocking in the Testpoint Options branch of the tree to display the Block Page Testpoint Options frame in the right panel:
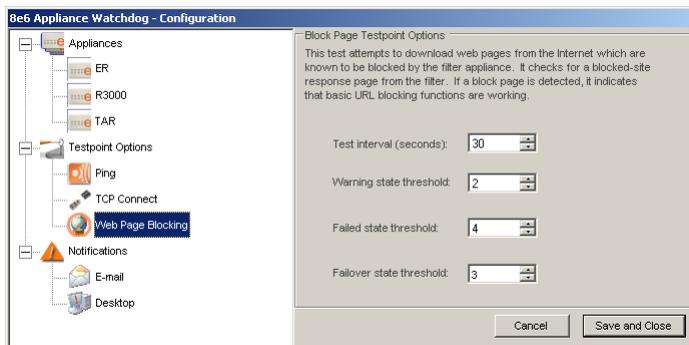
Fig. 1:3-9 Web Page Blocking

2. Configure any of the following options by making a numerical selection for that designated field:

   • **Test interval (seconds)** - The number of seconds Watchdog will use in the interval between attempting to test the block page response in the appliance. The default is *30* seconds, and the minimum number of seconds that can be selected is *10*.

   • **Warning state threshold** - The number of consecutive tests an appliance can fail before Watchdog issues that appliance a warning state. The default is *2* tests.

Using these default settings, Watchdog will issue a warning state for the failed appliance after one minute (one failed test in 30 seconds, plus another failed test in the next 30 seconds equals 60 seconds, or one minute).

- **Failed state threshold** - The number of consecutive tests an appliance can fail before Watchdog issues a failed state for that appliance. The default is *4* tests.

  Using these default settings, when Watchdog makes a fourth failed attempt to test the block page response in the appliance, the state of that appliance will be upgraded from a warning state to a failed state.

- **Failover state threshold** - The number of consecutive tests a target R3000 or R3000IR appliance—set up to use the failover detection feature—can fail before Watchdog issues a failover state for that target appliance. The default is *3* tests.

  Using these default settings, when Watchdog makes a third failed attempt to test the block page response in the appliance, the state of that appliance will be upgraded from a warning state to a failed state.

3. Click **Save and Close** to save your configuration and close both the Configuration window and Administrator console, restart the service, and then re-open the console showing the Status screen.

Notifications

The Notifications branch of the tree consists of E-mail and Desktop options for configuring the method in which you wish to be alerted to errors detected by Watchdog.

E-mail

Using the E-mail notification option, Watchdog will send the specified email address alerts for warning and failed states detected on an appliance.

1. Click E-mail in the Notifications branch of the tree to display the E-mail frame in the right panel:
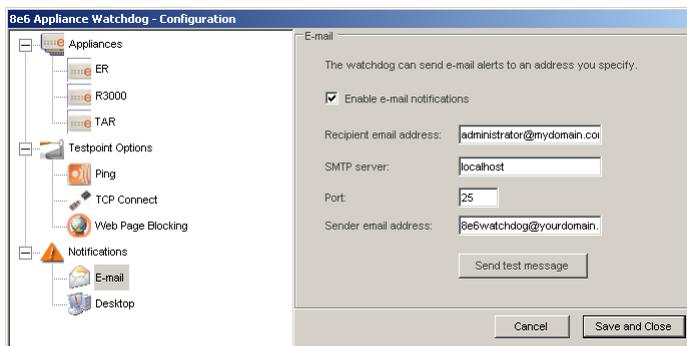
Fig. 1:3-10 E-mail

2. By default, the email alert option is disabled and all objects in this frame displayed greyed-out. Click the "Enable email notifications" checkbox to activate all objects in this frame and to enable the email alert option.

3. Type in the **Recipient email address** for the intended administrator to receive email alerts.

4. Enter the **SMTP server** name, for example: *mail.logo.com*.

5. By default, the **Port** number used for sending email is *25*. This should be changed if the sending mail connection fails.

6. Type in Watchdog's **Sender email address**.

7. Click **Send test message** to verify your entries. If you receive a failure message, make any necessary modifications, and then perform this test again.

8. Once you have successfully configured email options, click **Save and Close** to save your configuration and close both the Configuration window and Administrator console, restart the service, and then re-open the console showing the Status screen.

Desktop

Using the Desktop notification option, Watchdog will send alerts to your desktop for any warning and failed states detected on an appliance.

1. Click Desktop in the Notifications branch of the tree to display the Desktop frame in the right panel:
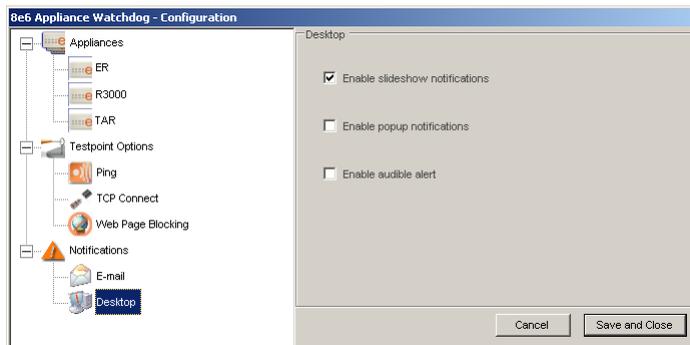
Fig. 1:3-11 Desktop

2. Any of the following desktop alert options can be enabled or disabled:

- **Enable slideshow notifications** - By default, slide-show notifications are selected. With this option enabled, when an alert is triggered, an orange pop-up window containing the alert message briefly displays in the lower right corner of your browser window and then dissolves:

Fig. 1:3-12 8e6 Appliance Watchdog Notification

Click the **Active alerts** link in the lower right corner of this window to open the Active Alerts pop-up box (see Fig. 1:3-13) where the entire alert can be viewed and acknowledged.

NOTE: The alert is acknowledged by clicking Acknowledge All in the Active Alerts pop-up box.

TIPS: The slideshow window remains open by hovering over—or clicking in—the window, and can be closed by clicking the "X" in the upper right corner.

- **Enable popup notifications** - Choose this option to select the Active Alerts pop-up box notification feature. With this option enabled, when an alert is triggered, the Active Alerts pop-up box opens:

Fig. 1:3-13 Active Alerts

The Message window in the middle of this pop-up box displays a list of warning and failed state alerts, each preceded by a triangular-shaped icon (yellow for "warning" and red for "failed") containing an exclaimation point.

TIP: The "Enable popup notifications" checkbox in this pop-up box performs the same function as in the Configuration window, and can be enabled or disabled using either tool. By enabling/disabling this feature using one tool, the feature is automatically enabled/disabled in the other tool.

After reviewing all alert messages, click **Acknowledge All** to place green check marks across all icons:

Fig. 1:3-14 Active Alerts acknowledged

By default, "No suppression" is defined for alert notifications. To **Suppress alerts for** a specified period, make a selection from the following choices: 10 Minutes, 30 Minutes, 60 Minutes, 2 Hours, 4 Hours, 24 Hours, Indefinitely. This selection changes the text displayed below to indicate when the suppression period will end, and the Watchdog system tray icon displays with an 'X' across the icon. During the suppression period, alerts continue to display in the Message window but the administrator is not notified. After a defined suppression period has ended, the Watchdog system tray icon no longer displays with an 'X' across the icon.

NOTE: *If Watchdog is stopped and restarted during the suppression period, the suppression action will be terminated and the suppression setting will be reset to "No suppression".*

> Click the "X" in the upper right corner of the pop-up box to close it.

- **Enable audible alert** - Choose this option to receive an alert notification by a continuous, audible beep on your machine.

  To review alert messages and to stop your machine from beeping, do one of the following to access the Active Alerts pop-up box: Click the **Alerts** menu item in the Administrator console, or right-click the Watchdog system tray icon and select Alerts in the pop-up menu.

NOTE: *Your machine continues beeping as long as the alert remains unacknowledged. The alert is acknowledged by clicking Acknowledge All in the Active Alerts pop-up box.*

3. Once you have specified your alert notification option(s), click **Save and Close** to save your settings and close both the Configuration window and Administrator console, restart the service, and then re-open the console showing the Status screen.

Chapter 4: Analyze Data in Console

This chapter explains how to use the Status, History, and Log screens to analyze data that displays in the Administrator console. Once you have reviewed this criteria, you will be able to better monitor the health of the 8e6 appliances on your network and collectively manage these units.

Status screen

The Status screen is accessible by clicking the **Status** menu item in the Administrator console:
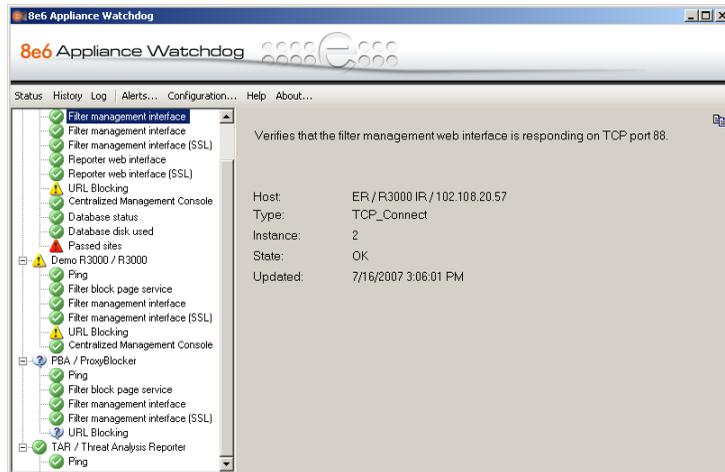
Fig. 1:4-1 Status screen

This screen includes a tree of appliances in the left panel, with a list of testpoint states for each appliance. Each item in the tree is preceded by an icon showing its current state: OK (green circle with white checkmark), Unknown (white balloon with question mark), Warning (yellow triangle with exclaimation point), Failed (red triangle with exclaimation point).

Click an item in the tree to display details about its status in the right panel.

To copy the contents displayed in the right panel, click the copy ![copy icon] icon located in the upper right corner of the panel. These contents can then be pasted into another application.

History screen

The History screen is accessible by clicking the **History** menu item in the Administrator console:
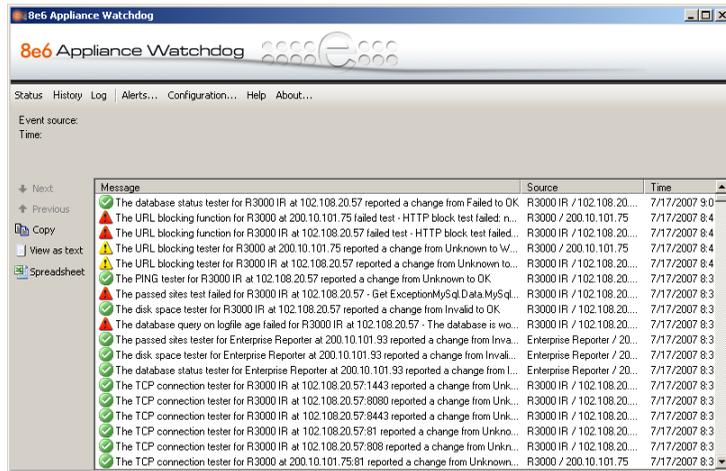
Fig. 1:4-2 History screen

This screen includes a window that contains up to 1000 records showing recent appliance testpoint results, with the newest testpoint result at the top of the list. For each record, the following columns of information display: testpoint Message (preceded by a status icon—OK, warning, failed); Source (appliance type / IP address); Time (MM/DD/YYYY HH:MM:SS AM/PM format).

NOTE: *The number of days is unlimited for the maximum 1000 records that can display.*

TIPS: A column can be expanded by placing your cursor over the section where the column ends—so that the cursor changes into a verticle bar with horizontal arrows on either side of it—left clicking, and then moving your mouse to the right.

The contents of the message window are refreshed by closing the Administrator console and reopening it.

The following actions can be performed in this screen:

• View details for a testpoint result - Click a testpoint result in the list to highlight it and to display the following testpoint result information beneath the menu items at the top of the screen: Event source (appliance type / IP address); Time (MM/DD/YYYY HH:MM:SS AM/PM format); and message.
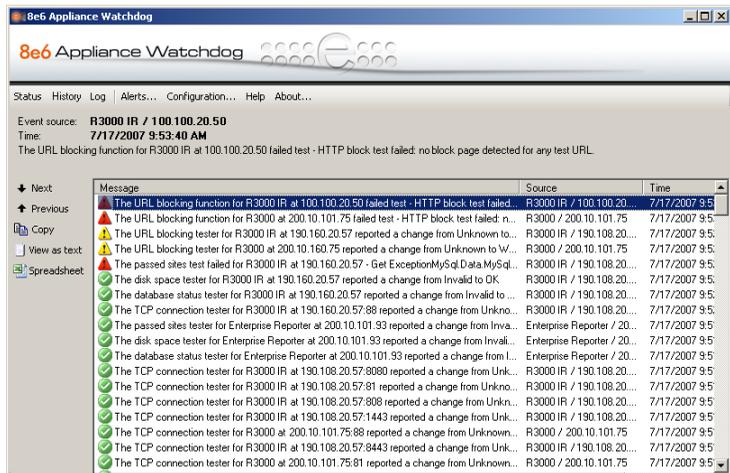
Fig. 1:4-3 History screen, testpoint result selected

The action of selecting a testpoint result also activates the Next and Previous buttons to the left of the Message window.

• View the next testpoint result - Click ![Next] to select and highlight the next testpoint result in the window.
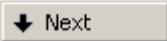
- View the previous testpoint result - Click ⬆ Previous to select and highlight the previous testpoint result in the window.

- Copy testpoint result contents - Click 📋 Copy to copy the current testpoint result messages to the Windows clipboard, so that this information can be pasted in a blank, open file.
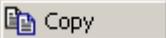
💡 *TIPS: To copy a selection of testpoint results and not the entire file, click the first record to select it from the list, and then click and hold Ctrl while selecting the next record, and so forth. To select a block of records, select the first record from the list, and then click and hold Shift while selecting the last record to be included in the block of records. The copied records can then be pasted in a blank, open file.*

- View testpoint result contents in a text file format - Click 📄 View as text to open a text file containing the current testpoint result messages.

- View testpoint result contents in a spreadsheet format - Click 📊 Spreadsheet to open a spreadsheet containing the current testpoint result messages.

Log screen

The Log screen is accessible by clicking the **Log** menu item in the Administrator console:
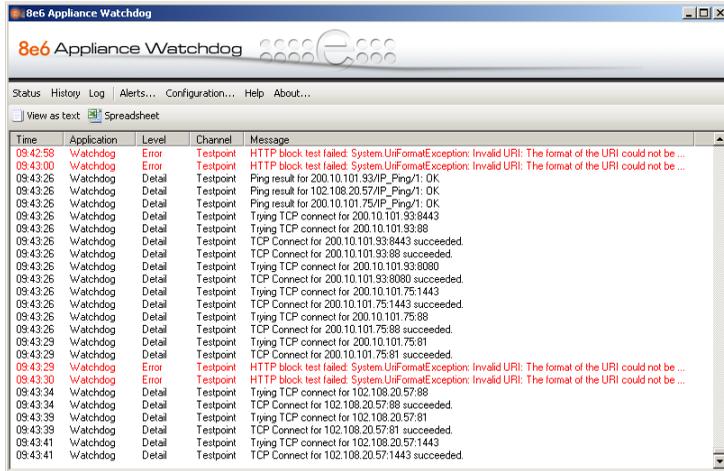
Fig. 1:4-4 Log screen

This screen displays a running list of up to 5000 records for the current day, showing the following columns of criteria: Time (HH:MM:SS format); Application (User, Watchdog); Level (App, Detail, Error, Module); Channel (Database, General, Testpoint); and Message.

Codes shown in the Level column indicate the following:

- App: Application start/initialization message

- Detail: Successful testpoint results

- Error: Testpoint failure and any exceptions caught

- Module: Version check results on DB schema

NOTE: The latest record displays at the bottom of the list, and error records display in red text.

TIP: To stop the log from automatically scrolling, right-click in the log to open the option box with the "Auto refresh" checkbox populated. Click the checkbox to remove the checkmark and to stop the log from scrolling. To re-enable auto-scrolling, right-click in the log again, and then click "Auto refresh".

The following actions can be performed in this screen, via the buttons above the log window:

- View the log contents in a text file format - Click

   to open a text file containing the current log file contents.

- View the log contents in a spreadsheet format - Click

   to open a spreadsheet containing the current log file contents.

TECHNICAL SUPPORT SECTION

Tech Support Coverage

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.

INDEX

A

About *15*
Access the Configuration window *16*
Acknowledge All *34*
Active alerts link *33*
Active Alerts pop-up box *33*
Add a new appliance *18*
Add appliances to be monitored *18*
Alerts *14*, *15*

B

button, terminology *3*

C

checkbox, terminology *3*
Configuration *14*
Conventions *2*

D

Delete an appliance *22*
Desktop notification *32*
dialog box, terminology *3*

E

E-mail notification option *31*
Enable audible alert *35*
End User License Agreement *9*
environment requirements *8*
Exit and Stop Service *15*
Exit GUI only *15*

F

failover detection *19*, *30*

slideshow notifications *33*
Status *14*
Status screen *36*
Suppress alerts *34*
system requirements *8*
system tray icon *13*, *15*

T

table, terminology *5*
TCP Connect *27*
Technical Support section *42*
Testpoint Options *24*
Testpoints Chart *24*
text box, terminology *5*
tree, terminology *5*

W

Warnings *23*
Web Page Blocking *29*
window, terminology *6*
workstation requirements *8*