M86 Appliance Watchdog

USER GUIDE

Software Version: 3.0.00
Document Version: 06.01.10

M86 APPLIANCE WATCHDOG USER GUIDE

828 W. Taft Ave., Orange, CA 92865, USA

Version 1.02, published June 2010 for software release 3.0.00

Printed in the United States of America

Every effort has been made to ensure the accuracy of this document. However, M86 Security makes no warranties with respect to this documentation and disclaims any implied warranties of merchantability and fitness for a particular purpose. M86 Security 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.m86security.com/support/Watchdog/documentation.asp

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# AW-UG_v1.02-1006

CONTENTS

APPLIANCE WATCHDOG OVERVIEW

M86 Appliance Watchdog provides monitoring services for the M86 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 M86 Appliance Watchdog User Guide addresses the administrator designated to configure the M86 Appliance Watchdog and monitor M86 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 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.*

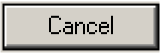
***TIP**: The “tip” icon is followed by italicized text giving you hints on how to execute a task more efficiently.*

***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.*

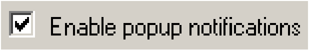
Terminology

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

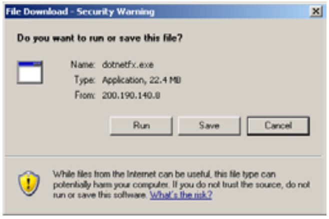
- **button** - an object in a dialog box, window, or screen that can be clicked with your mouse to execute a command.



- **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.


☑ Enable popup notifications

- **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.

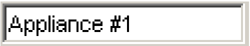

File Download - Security Warning

Do you want to run or save this file?

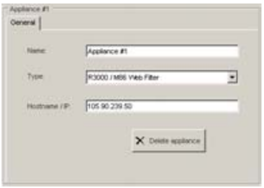
Name: dotnetfx.exe
Type: Application, 22.4 MB
From: 200.190.140.0

While files from the Internet can be useful, this file type can potentially harm your computer. If you do not trust the source, do not run or save this software. What's the risk?

- **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.


Appliance #1

- **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.



Appliance #1

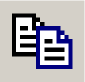
General

Name: Appliance #1

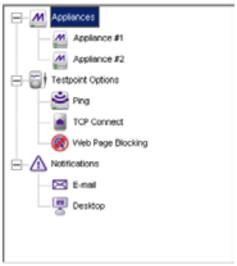
Type: R3000 / M86 Web Filter

Hostname / IP: 105.90.239.50

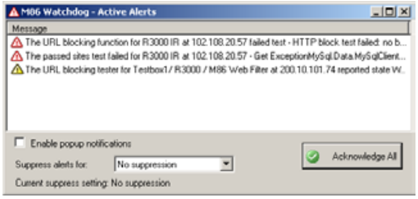
- **icon** - a small image in a dialog box, window, or screen that can be clicked. This object can be a button or an executable file.



- **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.



M86 Watchdog - Active Alerts

Message

The URL blocking function for R3000 IR at 102.108.20.57 failed test - HTTP block test failed: no b...

The passed sites test failed for R3000 IR at 102.108.20.57 - Get ExceptionMySql.Data.MySqlClient...

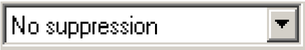
The URL blocking tester for Testbox1 / R3000 / M86 Web Filter at 200.10.101.74 reported state W...

☐ Enable popup notifications

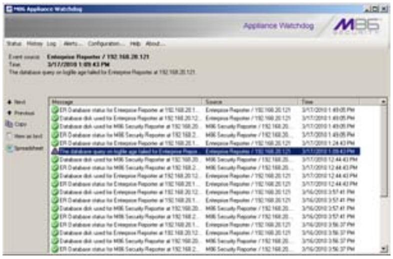
Suppress alerts for: No suppression

Current suppress setting: No suppression

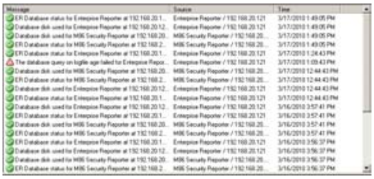
- **pull-down menu** - a field in a dialog box, window, or screen that contains a down-arrow to the right. When you click the arrow, a menu of items displays from which you make a selection.


No suppression

- **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.

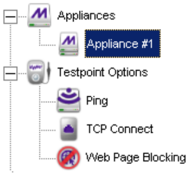


- **table** - a section of a screen containing a list of records populated by the application.

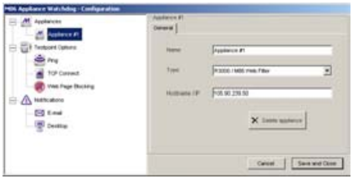


- **text box** - an area in a dialog box, window, or screen that accommodates your data entry. A text box is a type of field. (See “field”.)

- **tree** - a tree displays in the navigation 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.



Name: Appliance #1

Type: R3000 / M86 Web Filter

Hostname / IP: 105.90.239.50

ADMINISTRATOR SECTION

Introduction

The authorized administrator of the M86 Appliance Watchdog is responsible for setting up the application and adding M86 appliances to be monitored. To attain this objective, the administrator performs the following tasks:

- installs and configures the M86 Appliance Watchdog on a designated workstation
- adds M86 appliances to be monitored by the M86 Appliance Watchdog
- analyzes logs generated by the application
- establishes alert notifications for network problems affecting M86 appliances

Environment Requirements

Workstation Requirements

Minimum system requirements for the administrator include the following:

- 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

This software version of the Appliance Watchdog has been tested for compatibility with the following Windows Operating Systems:

- Windows XP 32-bit
- Windows Vista 32-bit
- Windows 7 32-bit

Network Requirements

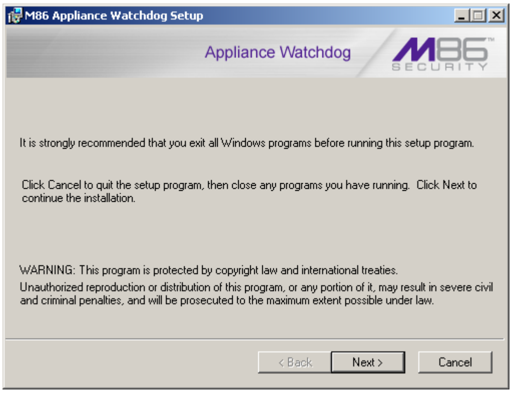
- High speed connection from the M86 Appliance Watchdog application to M86 appliances set up to be monitored

Chapter 1: Watchdog Installation

Install the Appliance Watchdog

1. Go to **http://www.m86security.com/support/Watchdog/upgrade.asp**.

2. Click the link for the Appliance Watchdog application .msi file to launch the M86 Appliance Watchdog Setup wizard:



It is strongly recommended that you exit all Windows programs before running this setup program.

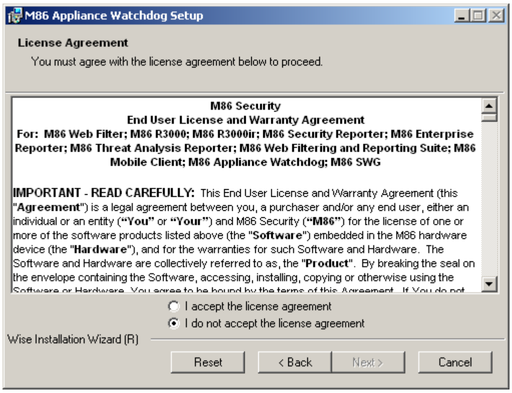
Click Cancel to quit the setup program, then close any programs you have running. Click Next to continue the installation.

WARNING: This program is protected by copyright law and international treaties.
Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under law.

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):



License Agreement

You must agree with the license agreement below to proceed.

M86 Security
End User License and Warranty Agreement
For: M86 Web Filter; M86 R3000; M86 R3000ir; M86 Security Reporter; M86 Enterprise Reporter; M86 Threat Analysis Reporter; M86 Web Filtering and Reporting Suite; M86 Mobile Client; M86 Appliance Watchdog; M86 SWG

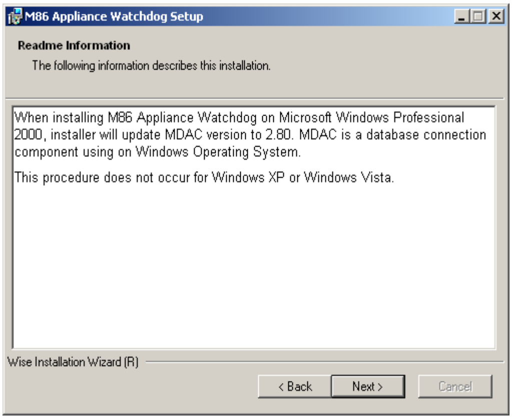
IMPORTANT - READ CAREFULLY: This End User License and Warranty Agreement (this "**Agreement**") is a legal agreement between you, a purchaser and/or any end user, either an individual or an entity (**"You"** or **"Your"**) and M86 Security (**"M86"**) for the license of one or more of the software products listed above (the "**Software**") embedded in the M86 hardware device (the "**Hardware**"), and for the warranties for such Software and Hardware. The Software and Hardware are collectively referred to as, the "**Product**". By breaking the seal on the envelope containing the Software, accessing, installing, copying or otherwise using the Software or Hardware. You agree to be bound by the terms of this Agreement. If You do not

○ I accept the license agreement
● I do not accept the license agreement

Fig. 1:1-2 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:



Readme Information

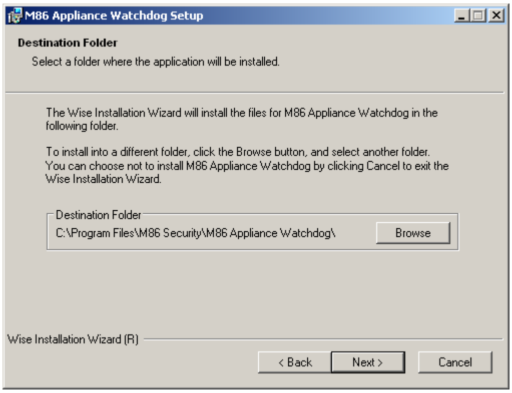
The following information describes this installation.

When installing M86 Appliance Watchdog on Microsoft Windows Professional 2000, installer will update MDAC version to 2.80. MDAC is a database connection component using on Windows Operating System.

This procedure does not occur for Windows XP or Windows Vista.

Fig. 1:1-3 Readme information

6. Click **Next** to specify the destination folder for installing Watchdog:



M86 Appliance Watchdog Setup

Destination Folder

Select a folder where the application will be installed.

The Wise Installation Wizard will install the files for M86 Appliance Watchdog in the following folder.

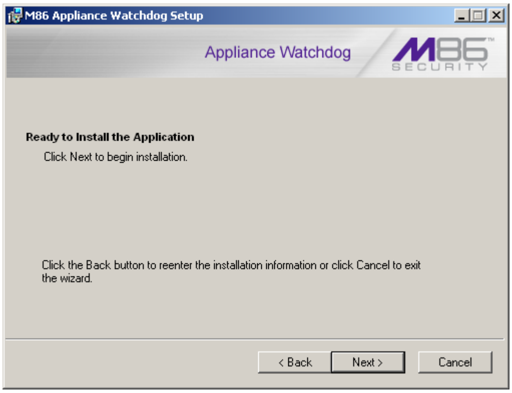
To install into a different folder, click the Browse button, and select another folder. You can choose not to install M86 Appliance Watchdog by clicking Cancel to exit the Wise Installation Wizard.

Destination Folder
C:\Program Files\M86 Security\M86 Appliance Watchdog\

Fig. 1:1-4 Destination Folder selection

***TIP**: To select a folder for installing Watchdog other than the default M86 Appliance 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:



M86 Appliance Watchdog Setup

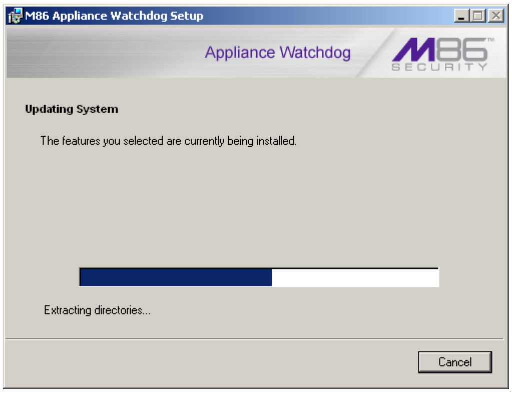
Ready to Install the Application

Click Next to begin installation.

Click the Back button to reenter the installation information or click Cancel to exit the wizard.

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

8. Click **Next** to begin installing M86 Appliance Watchdog on your machine:



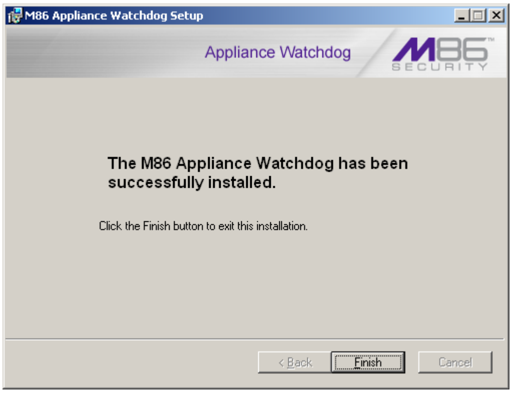
Updating System

The features you selected are currently being installed.

Extracting directories...

Fig. 1:1-6 Appliance Watchdog installation

When the Appliance Watchdog installation setup process has successfully finished, completion information displays:



The M86 Appliance Watchdog has been successfully installed.

Click the Finish button to exit this installation.

Fig. 1:1-7 Installation complete

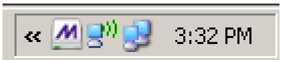
9. Click **Finish** to close the installation setup window and to open the Appliance Watchdog console (see Fig. 1:2-1). The configuration setup for the Appliance Watchdog can be completed now or at a later point in time.

Chapter 2: Access the Admin Console

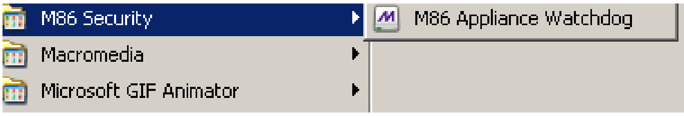
Launch the Application

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

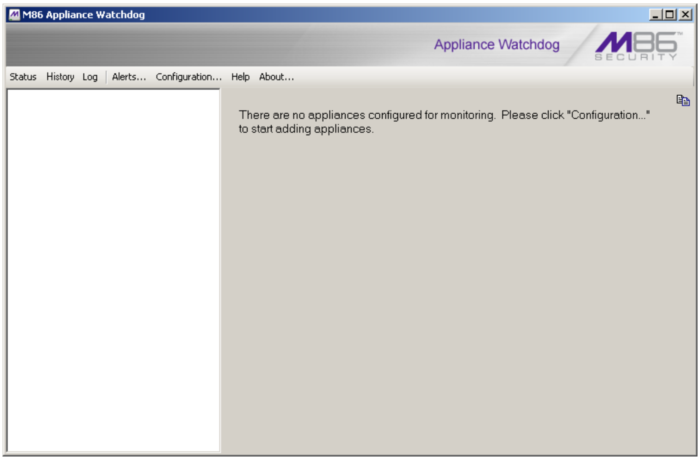
- **system tray icon -** double-click the purple “M” icon in your system tray (the icon to the left in the image below):



- **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 choose **M86 Security > M86 Appliance Watchdog**:



Clicking the Watchdog system tray icon or selecting the M86 Appliance Watchdog menu item launches the M86 Appliance Watchdog Administrator console—the latter selection also loads the Watchdog icon in your system tray:



There are no appliances configured for monitoring. Please click "Configuration..." to start adding appliances.

Fig. 1:2-1 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 opens a browser window containing online help, with a link to access the latest M86 Appliance Watchdog Administrator User Guide.
- **About** - Clicking this menu item opens a pop-up box containing the following information about this application: Product version number, M86 Web site link, M86 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 M86 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 - 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.

TIP*: The Administrator console can be re-accessed—and the system tray icon reloaded—by going to the Start menu and selecting M86 Appliance Watchdog from the M86 Security menu.*

Chapter 3: Watchdog Configuration

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

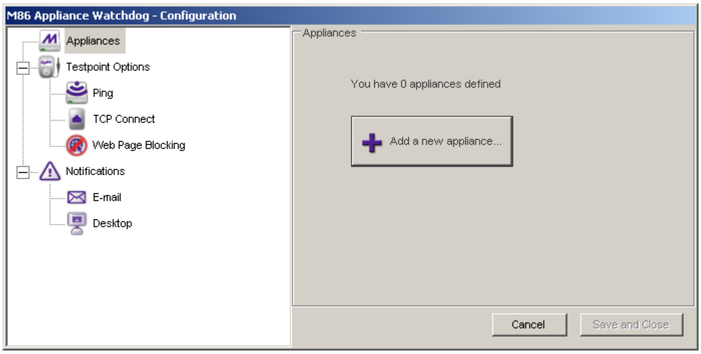
***NOTE**: See the Warnings page in this chapter for special settings to make in your M86 applications to allow Watchdog to monitor your appliances.*

Configuration window

The Configuration window is used for setting up M86 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:



You have 0 appliances defined

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

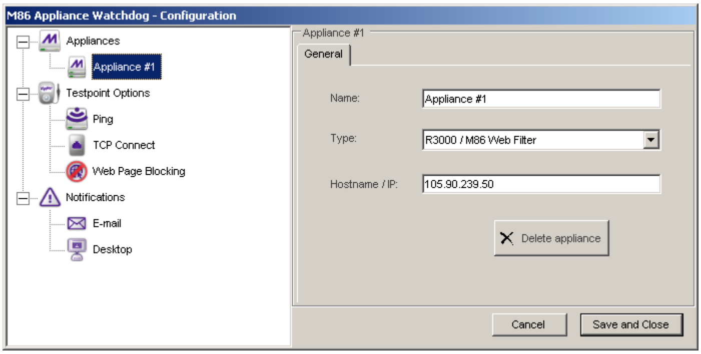
The Appliances branch of the tree lets you set up and maintain appliances to be monitored by Watchdog.

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:



Name: Appliance #1

Type: R3000 / M86 Web Filter

Hostname / IP: 105.90.239.50

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 / M86 Web Filter, R3000 IR, R3000 Mobile, ProxyBlocker, Enterprise Reporter, Threat Analysis Reporter, M86 Security Reporter, M86 Web Filtering and Reporting Suite.

***TIP**: If using the failover detection feature on an R3000, M86 Web Filter, M86 Web Filtering and Reporting Suite server, 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.*

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.

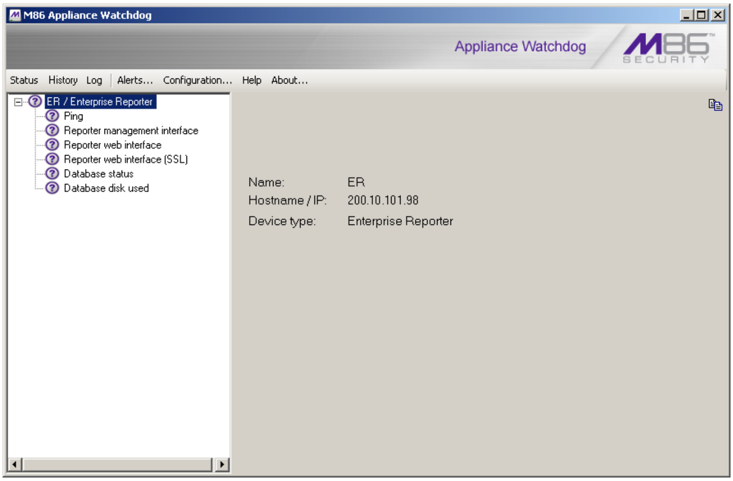
5. To add another appliance:

   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**: M86 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 save your entries, close the Configuration window, and to restart the service. The refreshed Status screen of the Administrator console shows information about the appliance(s) you just added:



Name: ER
Hostname / IP: 200.10.101.98
Device type: Enterprise Reporter

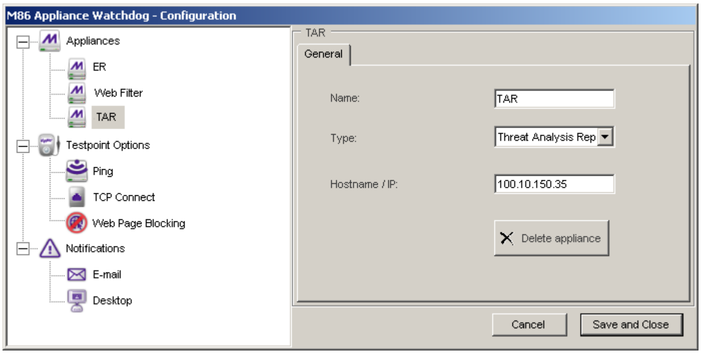
Fig. 1:3-3 Console with one appliance added

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.

Delete appliances

***TIP**: When deleting appliances, M86 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:



Name: TAR

Type: Threat Analysis Rep

Hostname / IP: 100.10.150.35

Fig. 1:3-4 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 remove the configuration for the appliance(s) from Watchdog, close the Configuration window, and to restart the service. The refreshed Status screen of the Administrator console displays your modifications (see Fig. 1:3-3).

WARNINGS

⚠ ***R3000, Web Filter, WFR, and ProxyBlocker** - In order for Watchdog to monitor filtering on the R3000, Web Filter, or Web Filtering and Reporting Suite (WFR), 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, Web Filter, and WFR, 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, Security Reporter** - If Watchdog is monitoring a Threat Analysis Reporter or Security Reporter, the workstation running Watchdog should be excluded from monitoring, otherwise you would be locked out from any Web access.*

⚠ ***Erroneous failure status messages** - 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 user interface will display a failure status, whereas the appliance(s) may be functioning well.*

⚠ ***ER version prior to 6.0, CER, R3000IR prior to 4.0** - For an ER appliance running a software version prior to 6.0, any Consolidated ER (CER), or R3000IR running software prior to R3000 4.0, the testpoint statuses for “ER Database status” and “Database disk used” will display as “Failed”, and the latter test-point will include the message: “Unable to connect to database.”*

⚠ ***Threat Analysis Reporter software version prior to 2.1** - If monitoring a Threat Analysis Reporter appliance running a software version prior to 2.1, the testpoint status for “TAR Database status” will display as “Failed” and will include the message: “Unable to connect to database.”*

Testpoint Options

Testpoints are a series of checkpoints used for systematically monitoring each M86 appliance added to the Appliances branch of the tree. Each type of appliance has its own list of testpoints Watchdog uses to determine if that appliance 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

M86 Appliance	Accessibility Ping	Admin Interface	Block Page / Authentication Service (port 81)	URL Filtering
R3000 / M86 Web Filter	Yes	Yes: Ports 88 & 1443	Yes	Yes
R3000IR	Yes	Yes: Ports 88, 808, 1443, 8080 & 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
M86 Security Reporter	Yes	Yes: Ports 808, 8080, 8443 & 8843	No	No
M86 Web Filtering and Reporting Suite	Yes	Yes: Ports 88, 808, 1443, 8080, 8443 & 8843	Yes	Yes

Testpoints Chart - Part 2

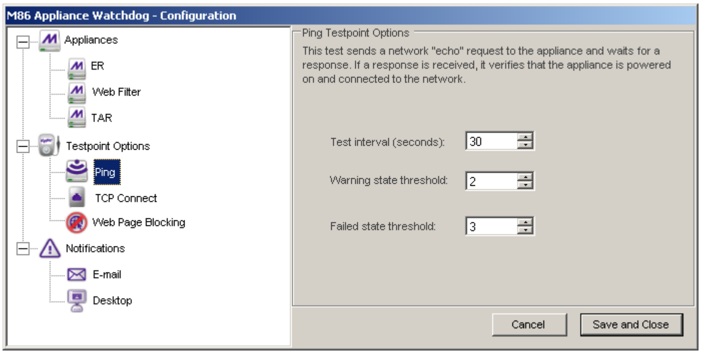
M86 Appliance	DB Engine / Reporting Service	M86 Client Service	Database Usage	CMC
R3000 / M86 Web Filter	No	No	No	Yes
R3000IR	Yes: Ports 3306, 8080 & 8443	No	Yes	Yes
R3000 Mobile	No	Yes: Port 443	No	No
ProxyBlocker	No	No	No	No
Enterprise Reporter	Yes: Ports 3306, 8080 & 8443	No	Yes	No
Threat Analysis Reporter	Yes: Port 3306	No	No	No
M86 Security Reporter	Yes: Ports 3306, 3307, 8080 & 8443	No	Yes	No
M86 Web Filtering and Reporting Suite	Yes: Ports 3306, 3307, 8080 & 8443	Yes: Port 443	Yes	Yes

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:



M86 Appliance Watchdog - Configuration

Ping Testpoint Options

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

Test interval (seconds): 30

Warning state threshold: 2

Failed state threshold: 3

Fig. 1:3-5 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.

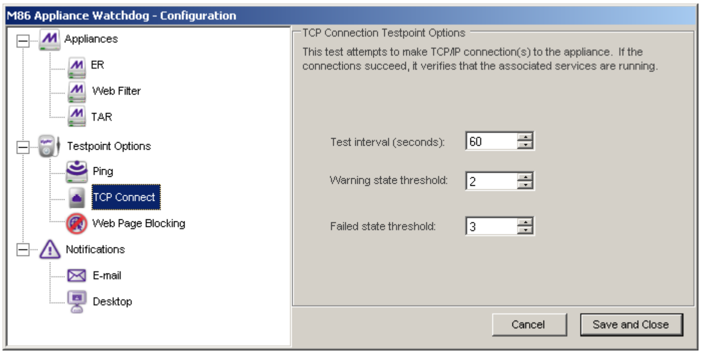
  Using these default settings, when Watchdog makes a third failed attempt to ping the appliance, the state of that appliance will be upgraded from a warning state to a failed state.

3. Click **Save and Close** to save your configuration, close the Configuration window, and to restart the service. The refreshed Status screen of the Administrator console displays your modifications.

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:



This test attempts to make TCP/IP connection(s) to the appliance. If the connections succeed, it verifies that the associated services are running.

Test interval (seconds): 60

Warning state threshold: 2

Failed state threshold: 3

Fig. 1:3-6 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.

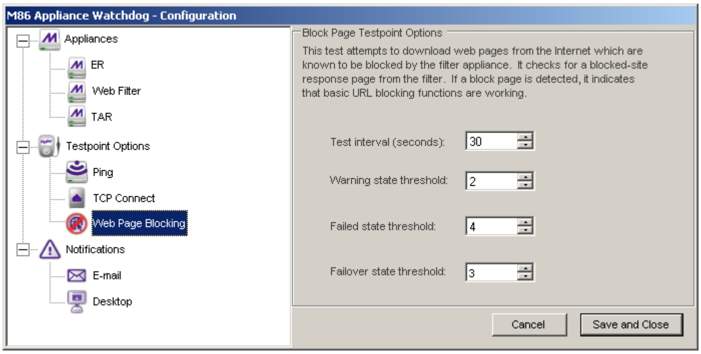
  Using these default settings, when Watchdog makes a third failed attempt to test the TCP connection to the appliance, the state of that appliance will be upgraded from a warning state to a failed state.

3. Click **Save and Close** to save your configuration, close the Configuration window, and to restart the service. The refreshed Status screen of the Administrator console displays your modifications.

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:



This test attempts to download web pages from the Internet which are known to be blocked by the filter appliance. It checks for a blocked-site response page from the filter. If a block page is detected, it indicates that basic URL blocking functions are working.

Test interval (seconds): 30

Warning state threshold: 2

Failed state threshold: 4

Failover state threshold: 3

Fig. 1:3-7 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 / M86 Web Filter, M86 Web Filtering and Reporting Suite, 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, close the Configuration window, and to restart the service. The refreshed Status screen of the Administrator console displays your modifications.

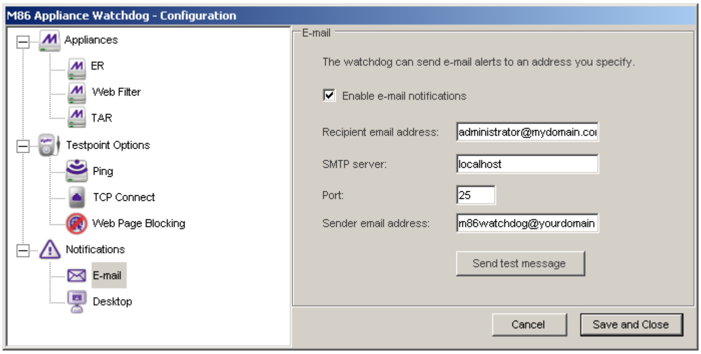
Notifications

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:



The watchdog can send e-mail alerts to an address you specify.

☑ Enable e-mail notifications

Recipient email address: administrator@mydomain.coı

SMTP server: localhost

Port: 25

Sender email address: m86watchdog@yourdomain

Fig. 1:3-8 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**.

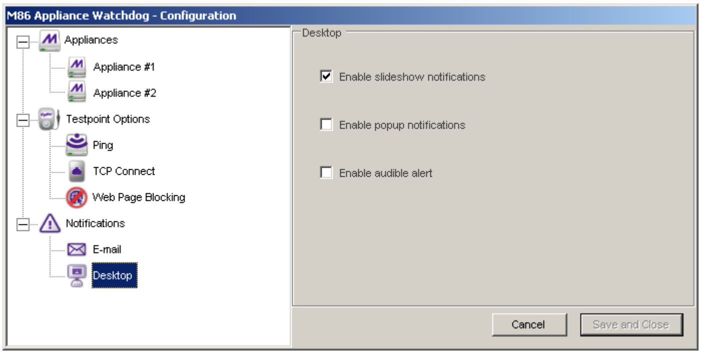
7. Click **Send test message** to verify your entries. If you receive a failure message, make any necessary modifications, and then perform this test again.

8. Once you have successfully configured email options, click **Save and Close** to save your configuration, close the Configuration window, and to restart the service. The refreshed Status screen of the Administrator console displays your modifications.

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:



Desktop

☑ Enable slideshow notifications

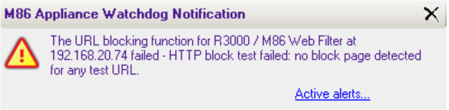
☐ Enable popup notifications

☐ Enable audible alert

Fig. 1:3-9 Desktop

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

- **Enable slideshow notifications** - By default, slideshow 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:



The URL blocking function for R3000 / M86 Web Filter at 192.168.20.74 failed - HTTP block test failed: no block page detected for any test URL.

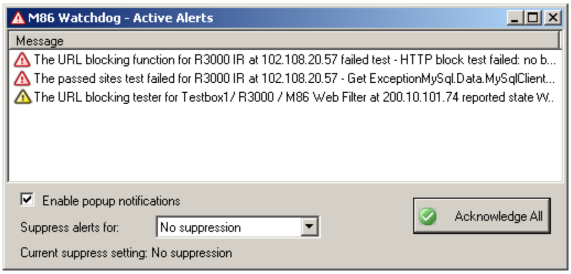
Fig. 1:3-10 Appliance Watchdog Notification

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:



The URL blocking function for R3000 IR at 102.108.20.57 failed test - HTTP block test failed: no b...
The passed sites test failed for R3000 IR at 102.108.20.57 - Get ExceptionMySql.Data.MySqlClient...
The URL blocking tester for Testbox1 / R3000 / M86 Web Filter at 200.10.101.74 reported state W...

☑ Enable popup notifications

Suppress alerts for: No suppression

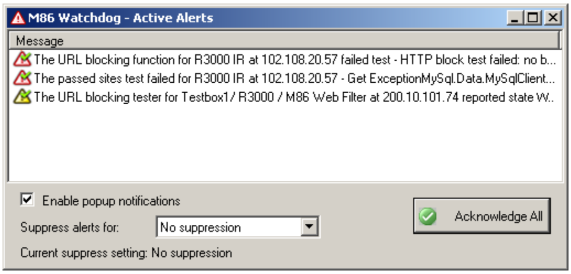
Current suppress setting: No suppression

Fig. 1:3-11 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 exclamation 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:


M86 Watchdog - Active Alerts

Message

The URL blocking function for R3000 IR at 102.108.20.57 failed test - HTTP block test failed: no b...

The passed sites test failed for R3000 IR at 102.108.20.57 - Get ExceptionMySql.Data.MySqlClient...

The URL blocking tester for Testbox1/ R3000 / M86 Web Filter at 200.10.101.74 reported state W..

☑ Enable popup notifications

Suppress alerts for: No suppression

Current suppress setting: No suppression

Fig. 1:3-12 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 a red circle containing a white ‘X’. 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 the red circle containing the white ‘X’.

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.*

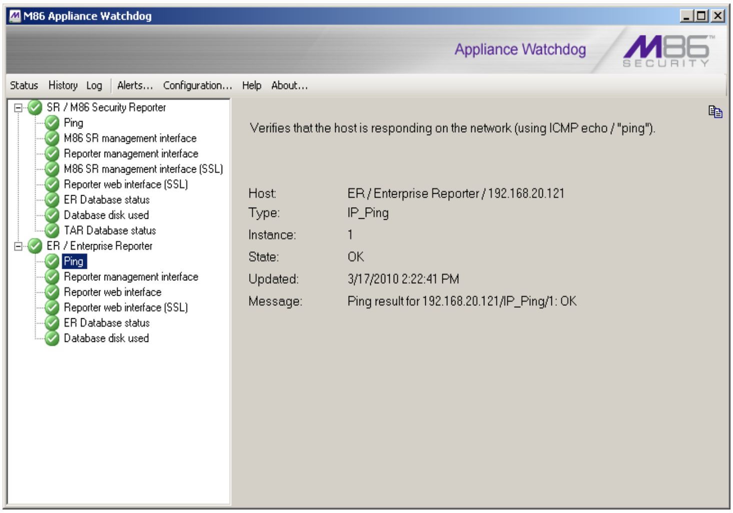
3. Once you have specified your alert notification option(s), click **Save and Close** to save your settings, close the Configuration window, and to restart the service. The refreshed Status screen of the Administrator console displays your modifications.

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 M86 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:



Verifies that the host is responding on the network (using ICMP echo / "ping").

Host: ER / Enterprise Reporter / 192.168.20.121
Type: IP_Ping
Instance: 1
State: OK
Updated: 3/17/2010 2:22:41 PM
Message: Ping result for 192.168.20.121/IP_Ping/1: OK

Fig. 1:4-1 Status screen

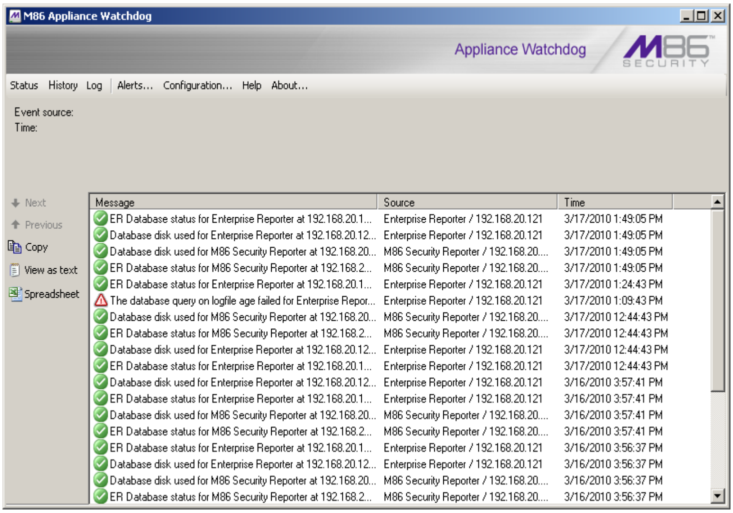
This screen includes a tree of appliances in the left panel, with a list of testpoint states for each appliance. Each item in the tree is preceded by an icon showing its current state: OK (green circle with white checkmark), Unknown/Invalid (purple circle with a question mark), Warning (yellow triangle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



Event source:
Time:

Message	Source	Time
✓ ER Database status for Enterprise Reporter at 192.168.20.1...	Enterprise Reporter / 192.168.20.121	3/17/2010 1:49:05 PM
✓ Database disk used for Enterprise Reporter at 192.168.20.12...	Enterprise Reporter / 192.168.20.121	3/17/2010 1:49:05 PM
✓ Database disk used for M86 Security Reporter at 192.168.20...	M86 Security Reporter / 192.168.20....	3/17/2010 1:49:05 PM
✓ ER Database status for M86 Security Reporter at 192.168.2...	M86 Security Reporter / 192.168.20....	3/17/2010 1:49:05 PM
✓ ER Database status for Enterprise Reporter at 192.168.20.1...	Enterprise Reporter / 192.168.20.121	3/17/2010 1:24:43 PM
⚠ The database query on logfile age failed for Enterprise Repor...	Enterprise Reporter / 192.168.20.121	3/17/2010 1:09:43 PM
✓ Database disk used for M86 Security Reporter at 192.168.20...	M86 Security Reporter / 192.168.20....	3/17/2010 12:44:43 PM
✓ ER Database status for M86 Security Reporter at 192.168.2...	M86 Security Reporter / 192.168.20....	3/17/2010 12:44:43 PM
✓ Database disk used for Enterprise Reporter at 192.168.20.12...	Enterprise Reporter / 192.168.20.121	3/17/2010 12:44:43 PM
✓ ER Database status for Enterprise Reporter at 192.168.20.1...	Enterprise Reporter / 192.168.20.121	3/17/2010 12:44:43 PM
✓ Database disk used for Enterprise Reporter at 192.168.20.12...	Enterprise Reporter / 192.168.20.121	3/16/2010 3:57:41 PM
✓ ER Database status for Enterprise Reporter at 192.168.20.1...	Enterprise Reporter / 192.168.20.121	3/16/2010 3:57:41 PM
✓ Database disk used for M86 Security Reporter at 192.168.20...	M86 Security Reporter / 192.168.20....	3/16/2010 3:57:41 PM
✓ ER Database status for M86 Security Reporter at 192.168.2...	M86 Security Reporter / 192.168.20....	3/16/2010 3:57:41 PM
✓ ER Database status for Enterprise Reporter at 192.168.20.1...	Enterprise Reporter / 192.168.20.121	3/16/2010 3:56:37 PM
✓ Database disk used for Enterprise Reporter at 192.168.20.12...	Enterprise Reporter / 192.168.20.121	3/16/2010 3:56:37 PM
✓ Database disk used for M86 Security Reporter at 192.168.20...	M86 Security Reporter / 192.168.20....	3/16/2010 3:56:37 PM
✓ ER Database status for M86 Security Reporter at 192.168.2...	M86 Security Reporter / 192.168.20....	3/16/2010 3:56:37 PM

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, unknown/invalid, warning, failed); Source (appliance type / IP address); Time (MM/DD/YYYY HH:MM:SS AM/PM format).

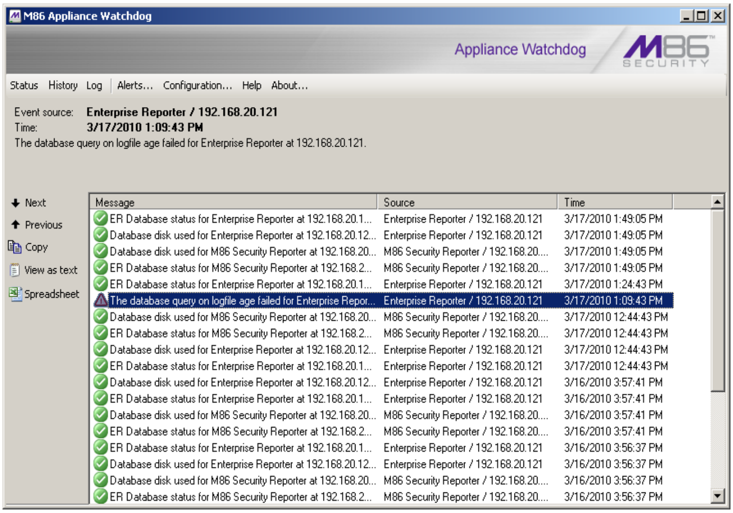
***NOTE**: The number of days is unlimited for the maximum 1000 records that can display.*

***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.



Event source: **Enterprise Reporter / 192.168.20.121**
Time: **3/17/2010 1:09:43 PM**
The database query on logfile age failed for Enterprise Reporter at 192.168.20.121.

Message	Source	Time
✓ ER Database status for Enterprise Reporter at 192.168.20.1...	Enterprise Reporter / 192.168.20.121	3/17/2010 1:49:05 PM
✓ Database disk used for Enterprise Reporter at 192.168.20.12...	Enterprise Reporter / 192.168.20.121	3/17/2010 1:49:05 PM
✓ Database disk used for M86 Security Reporter at 192.168.20...	M86 Security Reporter / 192.168.20....	3/17/2010 1:49:05 PM
✓ ER Database status for M86 Security Reporter at 192.168.2...	M86 Security Reporter / 192.168.20....	3/17/2010 1:49:05 PM
✓ ER Database status for Enterprise Reporter at 192.168.20.1...	Enterprise Reporter / 192.168.20.121	3/17/2010 1:24:43 PM
⚠ The database query on logfile age failed for Enterprise Repor...	Enterprise Reporter / 192.168.20.121	3/17/2010 1:09:43 PM
✓ Database disk used for M86 Security Reporter at 192.168.20...	M86 Security Reporter / 192.168.20....	3/17/2010 12:44:43 PM
✓ ER Database status for M86 Security Reporter at 192.168.2...	M86 Security Reporter / 192.168.20....	3/17/2010 12:44:43 PM
✓ Database disk used for Enterprise Reporter at 192.168.20.12...	Enterprise Reporter / 192.168.20.121	3/17/2010 12:44:43 PM
✓ ER Database status for Enterprise Reporter at 192.168.20.1...	Enterprise Reporter / 192.168.20.121	3/17/2010 12:44:43 PM
✓ Database disk used for Enterprise Reporter at 192.168.20.12...	Enterprise Reporter / 192.168.20.121	3/16/2010 3:57:41 PM
✓ ER Database status for Enterprise Reporter at 192.168.20.1...	Enterprise Reporter / 192.168.20.121	3/16/2010 3:57:41 PM
✓ Database disk used for M86 Security Reporter at 192.168.20...	M86 Security Reporter / 192.168.20....	3/16/2010 3:57:41 PM
✓ ER Database status for M86 Security Reporter at 192.168.2...	M86 Security Reporter / 192.168.20....	3/16/2010 3:57:41 PM
✓ ER Database status for Enterprise Reporter at 192.168.20.1...	Enterprise Reporter / 192.168.20.121	3/16/2010 3:56:37 PM
✓ Database disk used for Enterprise Reporter at 192.168.20.12...	Enterprise Reporter / 192.168.20.121	3/16/2010 3:56:37 PM
✓ Database disk used for M86 Security Reporter at 192.168.20...	M86 Security Reporter / 192.168.20....	3/16/2010 3:56:37 PM
✓ ER Database status for M86 Security Reporter at 192.168.2...	M86 Security Reporter / 192.168.20....	3/16/2010 3:56:37 PM

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.

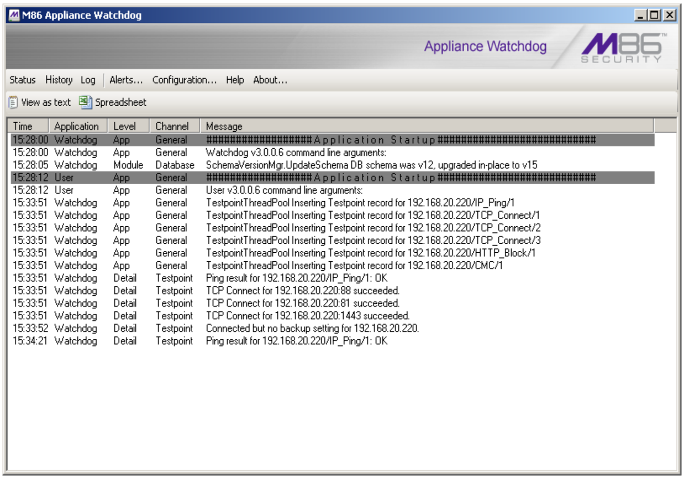
TIPS*: To copy a selection of testpoint results and not the entire file, click the first record to select it from the list, and then click and hold Ctrl while selecting the next record, and so forth. To select a block of records, select the first record from the list, and then click and hold Shift while 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:



Time	Application	Level	Channel	Message
15:28:00	Watchdog	App	General	##################Application Startup############################
15:28:00	Watchdog	App	General	Watchdog v3.0.0.6 command line arguments:
15:28:05	Watchdog	Module	Database	SchemaVersionMgr.UpdateSchema DB schema was v12, upgraded in-place to v15
15:28:12	User	App	General	##################Application Startup############################
15:28:12	User	App	General	User v3.0.0.6 command line arguments:
15:33:51	Watchdog	App	General	TestpointThreadPool Inserting Testpoint record for 192.168.20.220/IP_Ping/1
15:33:51	Watchdog	App	General	TestpointThreadPool Inserting Testpoint record for 192.168.20.220/TCP_Connect/1
15:33:51	Watchdog	App	General	TestpointThreadPool Inserting Testpoint record for 192.168.20.220/TCP_Connect/2
15:33:51	Watchdog	App	General	TestpointThreadPool Inserting Testpoint record for 192.168.20.220/TCP_Connect/3
15:33:51	Watchdog	App	General	TestpointThreadPool Inserting Testpoint record for 192.168.20.220/HTTP_Block/1
15:33:51	Watchdog	App	General	TestpointThreadPool Inserting Testpoint record for 192.168.20.220/CMC/1
15:33:51	Watchdog	Detail	Testpoint	Ping result for 192.168.20.220/IP_Ping/1: OK
15:33:51	Watchdog	Detail	Testpoint	TCP Connect for 192.168.20.220:88 succeeded.
15:33:51	Watchdog	Detail	Testpoint	TCP Connect for 192.168.20.220:81 succeeded.
15:33:51	Watchdog	Detail	Testpoint	TCP Connect for 192.168.20.220:1443 succeeded.
15:33:52	Watchdog	Detail	Testpoint	Connected but no backup setting for 192.168.20.220.
15:34:21	Watchdog	Detail	Testpoint	Ping result for 192.168.20.220/IP_Ping/1: OK

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 detected
- 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 View as text to open a text file containing the current log file contents.
- View the log contents in a spreadsheet format - Click Spreadsheet to open a spreadsheet containing the current log file contents.

TECHNICAL SUPPORT SECTION

Tech Support Coverage

For technical support, visit M86 Security's Technical Support Web page at **http://www.m86security.com/support** 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@m86security.com**

Office Locations and Phone Numbers

M86 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

M86 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