

## **About**

Text Log Monitor provides Systems Administrators the ability to monitor, filter, alert, archive, schedule web and email reports, and tail critical operating system and application logs.

### ***Delimited and Non-Delimited***

Supports both delimited and non-delimited text log files. Delimited files follow a specific format enabling programmatic parsing over multiple lines, for example, syslog files. Delimited files are read line by line until the next entry delimiter is reached. Once reached, all lines are concatenated together to form an entry. Non-delimited files do not follow any specific format making programmatic parsing impossible. Non-delimited log files are read and filtered line by line.

### ***Directory Monitor***

Many applications create log files using a random or a date driven naming mechanism. Text Log Monitor enables you to monitor files within a directory that match user defined file name masks such as \*.txt and \*.log. When a new file is detected, Text Log Monitor automatically starts monitoring the file contents.

### ***Advanced Filtering***

Text Log Monitor's powerful filtering searches through text logs allowing you to pin point critical entries using simple or complex regular expression driven filters.

### ***Compliance***

Sarbanes-Oxley may require your organization archive critical text log files for future reference and accountability. Text Log Monitor will archive your logs in their entirety or as a sub-set to a central SQL Server or MySQL database as well as to CSV, HTML, TXT, or XML files.

### ***Alerts, Notifications, and Actions***

Trigger actions such as fully customizable email, export to file, message box, sound, write to database, write to event log, forward to syslog, system tray message, or SMS notification.

### ***Automatic Report Generation***

Create scheduled web and email reports that contain specific entries, for example, receive a daily email that contains critical application information contained within its service log.

### ***User Interface***

The Text Log Monitor user interface enables users to view, search, filter and tail large text files replacing popular command-line text file parsing tools.

### ***Key Features***

- Monitor text log files and fire various alerts.
- Archive specific log entries to either a file server , SQL Server or MySQL.
- View large text files quickly while only using minimal resources.
- Specify complex filters & search criteria using regular expressions.
- Export filtered logs to user defined SQL Server or MySQL tables or to one of the following file formats: CSV, HTML, TEXT, and XML.
- Forward filtered text logs to your Syslog server.
- Raise custom detailed and PDA friendly email alerts.
- Supports SMTP authentication.
- Single installation monitors entire network.

- No installation requirements on managed computers.

## *Architecture*

TLM consists of three major components:

**User Interface:** The user interface is used to configure the logs to monitor, configure the reports to generate, and view, tail, search, and filter log files.

**Windows Service:** The service monitors files and generates scheduled reports. When changes are made to a file being monitored, the changes are parsed, all assigned filters are executed, actions completed, and alerts fired.

**Tray Icon:** The tray icon is responsible for firing user interface dependent alerts (message box, sound, system tray popup, etc.) including application status.

**For more information, see:**

[How to Monitor Files](#)

# How to Monitor Files

---

## *File Monitoring*

File monitoring is the most basic form of monitoring. User's select a file that already exists and configure the monitor, specify filters and assign actions. For more information see [File Monitor Wizard](#).

## *Directory Monitoring*

Directory monitoring enables users to monitor all files that match a search criteria for example \*.log. When an application creates a new file that matches the file name search criteria, Text Log Monitor discovers the file within one minute and then starts monitoring the file. Directory monitoring is most commonly used to monitor files that contain date information within the file name itself. For example syslog\_2008\_01\_31.log. For more information see [Directory Monitor Wizard](#).

## *Read Methods*

Whether monitoring files or directories, users have the option to monitor each file in real-time or at specific intervals called scheduled reports.

## **Real-Time Monitoring**

Use real-time monitoring when you must be notified as soon as an entry is written to a file. Users have the option of reading the file with 3 different methods.

**Beginning of File** – When selected, the first time the monitor starts, Text Log Monitor reads, filters, fires alerts for the entire file, and lastly, waits for new entries. When the service is restarted or the computer is rebooted, the monitor picks up where it left off.

**End of File** – When selected, the first time the monitor starts, Text Log Monitor moves to the end of the file (ignoring current entries) and waits for new entries. When the service is restarted or the computer is rebooted, the monitor picks up where it left off.

**Read All** – When selected, the first time the monitor starts, Text Log Monitor does not read the file. When the operating system notifies Text Log Monitor the file has been updated, Text Log Monitor reads, filters, fires alerts for the entire file. When the service is restarted or the computer is rebooted, Text Log Monitor does not read the file. There is an exception to this rule, however. When monitoring a directory rather than a single file, newly created files are read in their entirety.

## **Scheduled Reports**

Use scheduled reports when you want to receive notification of specific events at a predetermined interval. For example, every Monday at 8:00 AM. Users have the option of reading the file with 3 different methods.

**Beginning of File** – When selected, the first time the report is run, Text Log Monitor reads, filters, fires alerts for the entire file. Each successive report picks up where it left off reading only entries written since the previous report.

**End of File** – When selected, the first time the report is run, Text Log Monitor saves off the length of the file and then exits. Each successive report picks up where it left off reading only entries written since the previous report.

**Read All** – When selected, Text Log Monitor reads the entire file, filters each entry, and lastly fires alerts every time the report is run.

**For more information, see:**

[File Monitor Wizard](#)

[Directory Monitor Wizard](#)

[Selecting Files and Directories to Monitor](#)



# System Architecture

---



Server



Desktop



Laptop

Monitors files on local or remote computers



Text Log Monitor

Stores entries in either a file system or SQL Server



File Server



SQL Server

Fires alerts through mail server



Mail Server

Exports filter results to web server



Web Server

Exports filter results to sysloger



Syslog Server

# System Requirements

---

## **Supported Operating Systems**

Windows Server 2008, Vista, Server 2003, XP, 2000 Server, or 2000

## **Memory**

512 MBs of available memory, 2 GBs suggested for large networks.

## **.Net Framework 2.0**

The installation detects if .Net Framework 2.0 is already installed. If not, the framework is automatically downloaded from Microsoft and then installed.

## **Domain administrator account credentials**

To access remote logs from the user interface, your login must have domain administrator rights. When scheduling the service to monitor and filter remote logs, the service must be run with domain administrator rights. The first time the application is run, you will be prompted to assign domain administrator rights to the service.

# Licensing

---

Corner Bowl Software offers 6 different licenses:

## Desktop

This license allows you to install the software on a single workstation and manage 20 local or remote text log files. Please note, this license can not be installed on a Windows Server operating systems, however; the software can still remotely manage Windows Server computers.

## Server

This license allows you to install the software on a single server or workstation and manage 50 local or remote text log files.

## Unlimited

This license allows you to install the software on a single server or workstation and manage an unlimited number of text log files.

## 5 Pack

Includes 5 Unlimited licenses enabling your organization to load balance, install Text Log Monitor on alternate networks or on various systems administrators' computers.

## Enterprise

Includes 20 Unlimited licenses and includes an additional year of support and updates for a total of 2 years of support and updates.

## Single Server

This license allows you to install the software on a single server or workstation and manage 50 local text log files only.

## *Support and Maintenance*

Your purchase of Text Log Monitor includes:

- Email and phone support for 1 year.
- Product updates for both maintenance builds and major releases for 1 year.
- In addition, annual maintenance contracts can be purchased for 50% the original list price.

## Registration

---

To register your software, visit <http://www.cornerbowl.com> and purchase a license. Once purchased, we will automatically email you a license key. After you receive your license key, select *Register* from the *Help* menu item. When prompted, specify the email address the license key was emailed to and the license key. Click *Submit*. Our software will transmit the email address, license key, and the active IP address's MAC address to our registration web service running on our web server. Once verified a digitally signed license file will be transmitted back to you. This file will automatically be saved to your program data directory. Licenses can be transferred to another computer upon request.

## **Update Service**

---

All of our software supports automatic updates. At startup, each of our user interfaces downloads an XML file from our web server. Using version information, our software determines if an update is necessary. License information may be transmitted to our registration web service, also running on web server, to determine upgrade eligibility. If eligible, our software will download the latest version from our web server.

Each license comes with access to updates and major releases for 1 year. After that, you can purchase a maintenance contract that provides you access to updates and major releases for 1 more year.

# About Corner Bowl Software

---

## *Who We Are*

Corner Bowl Software is a privately held company located in Park City, Utah, USA. We have been developing and selling software specifically for Information Technology professionals for over 7 years now. Our products are designed, developed, and continually updated in direct response to user feedback. All of our software tools are developed and supported in Park City.

## *Our Software*

Corner Bowl Software offers 4 distinct software tools that enable System Administrators to monitor and maintain their servers and workstations. We offer event log, text log, and syslog management applications as well as disk monitoring and server monitoring software tools. Our oldest and most popular applications are our event log management and disk monitoring applications (Network Event Viewer and SMART Disk Monitor). Both our text log and server monitoring tools (Text Log Monitor and Internet Server Monitor) are relatively new and quickly gaining traction. We welcome you to evaluate our software tools and very much appreciate feedback enabling us to update our applications to meet your demanding needs.

## *Development Cycles*

Corner Bowl Software prides itself on producing high quality usable software that utilizes the latest user interface components. We receive feature requests on a daily basis and in response have implemented a development system that enables us to quickly add, test, and release new features. Over the years, we have worked closely with System Administrators during Sarbanes Oxley compliance audits providing them with new features that enable them to more quickly respond to auditor requests.

## *How to Contact Us*

### **Our Address**

Corner Bowl Software  
PO Box 682876  
Park City, Utah 84068, USA

### **Support Inquiries**

Email: [support@cornerbowl.com](mailto:support@cornerbowl.com)  
Phone: 1-866-543-9470

### **Sales Inquiries**

Email: [sales@cornerbowl.com](mailto:sales@cornerbowl.com)  
Phone: 1-866-543-9470

## User Interface Components

---

The Text Log Monitor user interface is made up of several views that enable you to configure files to monitor, view file content, and service status messages.

### Network View

This window enables users to browse the network, configure files and directories for monitoring, and lists all files and directories being monitored.

### File Contents

File contents are displayed when you either double-click on a file in the Network window or when you open a file from the File menu. This window enables you to page through file contents, search for specific messages, apply filters, and lastly, export the view to a file or email.

### Output

This window displays application status messages.

### Service Output

The windows service writes status messages to a log file in the program data directory. This window tails the log file and displays each status message. This file is located in the following directory:

- *Windows XP/2000:* 'documents and settings\all users\application data\CornerBow\Text Log Monitor\Tlm.log'
- *Windows Vista:* '\programdata\CornerBow\Text Log Monitor\Tlm.log'

## Actions

Text Log Monitor fires actions when log entries pass filter criteria. The following actions are available:

<b>Database</b>	Writes each filtered log entry to a SQL Server or MySQL database table.
<b>Email</b>	Sends a simple notification message or a detailed message that contains the filtered log entries.
<b>Event Log Entry</b>	Writes the filtered log entries to a Windows event log.
<b>File</b>	Exports the filtered log entries to CSV, HTML, TXT, or XML.
<b>Message Box</b>	Displays a message box that optionally includes the filtered log entries.
<b>SMS (Clickatell)</b>	Sends a text message using Clickatell's web email-to-SMS online gateway service or any third party email-to-SMS gateway.
<b>Sound</b>	Plays a sound.
<b>Start Process</b>	Starts a background process.
<b>Syslog Message</b>	Forwards each filtered log entry to a syslog server.
<b>Tray Icon</b>	Updates the tray icon when log entries pass filter criteria.
<b>Tray Popup</b>	Displays a balloon window above the tray icon that optionally includes the filtered log entries.

### *Database*

When entries match filter criteria, Text Log Monitor can write the entries of interest to a SQL Server or MySQL database table.

*NOTE:* First, you must configure the database connection via the Tools | Options dialog. For more information see [Options](#).

Once configured, specify the name of the table to write the entries. If the table does not already exist, it will be automatically created. Entries from different logs can be written to the same table. The table is self-contained meaning it does not contain any foreign keys to other tables.

The following replacement tags are supported for table name:

- <HOST>
- <FILENAME>
- <FILTER>

### *Email*

When entries pass filter criteria, Text Log Monitor can email a simple notification message or a detailed message. Notification messages are designed to be seen on PDAs, phones, or as a reminder to look at the logs. Detailed messages contain each entry that passed the filter criteria. The subject and simple message support replacement tags listed at the bottom of this page.

### **Template**

Text Log Monitor uses a template file to create the detailed email content. For more information see [Mail and HTML Templates](#).

### *Event Log Entry*

When entries pass filter criteria, Text Log Monitor can write the entries of interest to a Windows Event Log.

Specify an already existing Event Log or the name of a new log to create. Specify the source to associate the entries with. Please note the source must be unique across all logs. The message supports the replacement tags listed at the bottom of this page.

## ***File***

When entries pass filter criteria, Text Log Monitor can write the entries of interest to various file types.

You must specify the file type, filename (excluding the extension), and if exporting to HTML, the template.

The following file types are supported:

- CSV
- HTML
- TEXT
- XML

The following replacement tags are supported for the file path and name:

- <HOST>
- <FILENAME>
- <FILTER>

## **Template**

Text Log Monitor uses a template file to create the HTML content. For more information see [Mail and HTML Templates](#).

## ***Message Box***

When entries pass filter criteria, Text Log Monitor can display a message box. The message box can optionally include all entries or can simply be a notification message reminding the logged on user to review the logs. The message supports the replacement tags listed at the bottom of this page.

## ***SMS (Clickatell)***

When entries pass filter criteria, Text Log Monitor can send a message to the Clickatell online SMS gateway. The message can optionally include all entries or can simply be a notification message reminding the logged on user to review the logs. The message supports the replacement tags listed at the bottom of this page.

## ***Sound***

When entries match filter criteria, Text Log Monitor can notify the logged on user to review the logs by playing a sound.

## ***Start Process***

When entries match filter criteria, Text Log Monitor can start a background process. Please note, user interface processes can not be started unless the Text Log Monitor Service is configured to interact with the desktop.

## ***Syslog***

When entries match filter criteria, Text Log Monitor can forward the entries of interest to your syslog server.

Specify syslog facility and syslog server to forward log entries. For more information on syslog see: RFC 3164 available at <http://www.faqs.org/rfcs/rfc3164.html>

## ***Tray Popup***

When entries pass filter criteria, Text Log Monitor can display a tray popup message. The popup can include all entries or can simply be a notification message reminding the logged on user to review the logs. . The message supports the replacement tags listed at the bottom of this page.

## ***Replacement Tags***

Text Log Monitor supports several replacement tags for message content. These tags are:

- <DATE>
- <ENTRIES>
- <ENTRY\_COUNT>
- <FILENAME>
- <FILTER>
- <HOST>
- <TIME>

**For more information, see:**

[Mail and HTML Templates](#)

[Options](#)

<http://www.faqs.org/rfcs/rfc3164.html>

## **Backing Up and Restoring the Configuration**

---

Text Log Monitor stores all configuration settings in the Windows Registry. To backup Text Log Monitor's configuration select *Export Configuration* from the Tools menu item. The registry is iterated and saved to an XML file. This file can be imported by the current system or another at any time by selecting Import Configuration from the Tools menu item. Please note the Windows's service credentials are not saved by Text Log Monitor.

## Copying Entries to the Clipboard

---

To copy a log entry to the clipboard, select the entry and press Ctrl-C, or Copy from the Edit menu, or select the toolbar button.



The log entry contents are copied to the system clipboard in string format. Once in the system clipboard, you can paste the contents to an email message or ASCII editor by pressing Ctrl-V or selecting Paste from the target application's Edit menu.

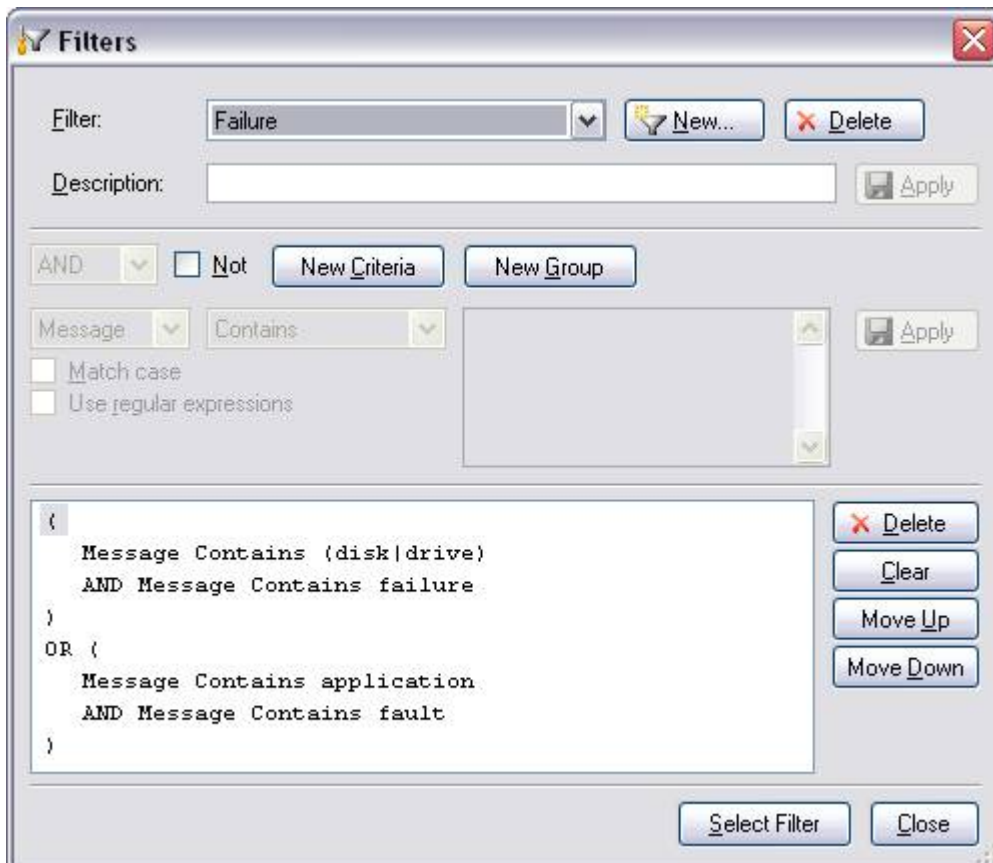
## Creating Filters

Logs can contain thousands of entries. In order to limit the entries viewed, users can create Filters. Filters have 2 purposes. First, filters enable users to search all entries in a log for specific entries. Second, filters enable users to remove entries deemed unimportant or not relevant at the time.

The Filters Dialog box enables you to create, modify, and delete filters. To open the Filters dialog box select Configure Filters from the Tools menu item.

### Filters Dialog Box

Filters are comprised of a series of very specific criteria that can be nested. Filters support AND, OR and NOT operands. Criteria can be nested by way of grouping criteria. Take the following filter as an example:



#### To add a new filter

Click the *Add* button and specify a name.

#### To remove an existing filter

Select the filter in the *Filter* drop-down list and click *Remove*.

#### To add criteria to a filter

Click *New Criteria*.

Specify the criteria.

Click *Apply*.

#### To group criteria in a filter

Select the position to append the group to, select AND, OR, NOT, and lastly click *New Group*.

**For more information, see:**

[Actions](#)

[Filters](#)

[How to Monitor Files](#)

# Directory Monitor Wizard

Directory monitoring enables users to monitor all files that match a search criteria for example \*.log. When an application creates a new file that matches the file name search criteria, Text Log Monitor discovers the file within one minute and then starts monitoring the file. Directory monitoring is most commonly used to monitor files that contain date information within the file name itself. For example syslog\_2008\_01\_31.log. For more information see [How to Monitor Files](#).

The Directory Monitor Wizard enables users to configure file name masks to monitor, apply filters, and assign actions.

## General

Use this tab to specify a user friendly name, logical group, and add or remove file name masks.

## File Masks

To monitor a file that contains date information use the following replacement strings:

Date/Time	Replacement String	Example
Year	yy or yyyy	Use yy to replace 08. Use yyyy to replace 2008.
Month	M or MM	Use M to replace 6. Use MM to replace 06.
Day	d or dd	Use d to replace 6. Use dd to replace 06.
Hour	h or hh	Use h to replace 6. Use hh to replace 06.
Minute	m or mm	Use m to replace 6. Use mm to replace 06.
Second	s or ss	Use s to replace 6. Use ss to replace 06.

To monitor the following file 'syslog\_2008\_01\_31.log' use the following mask: syslog\_<yyyy\_MM\_dd>.log.

## Entry Pattern

Use this tab to specify log entry delimiters.

Use the *Append lines to action* to specify the number of lines after a filtered entry to include in actions. For example, if a log file contains summary information at the end of the file, you can create a filter that specifies the summary header. Then specify the number of lines after the summary header to include in your action.

## Real Time

Use this tab to enable real-time monitoring and to specify the read method. When specifying an exclusion period you have the option to shutdown the monitor or suppress actions during the exclusion period. When shutting down the monitor the service will pick up where it left off once re-started. This means all entries written to the log during the exclusion period will be filtered and any corresponding actions fired. When suppressing actions the monitor continues to run, however; actions are suppressed. Once the exclusion period passes the service will only filter new entries.

For more information on real-time monitoring and the read method options see [How to Monitor Files](#).

## Real Time Actions

Use this tab to assign filters and actions for the real-time monitor.

## Frequency Detection

Frequency detection enables you to fire actions when an expected log entry fails fire within a specified frequency or fires more often than expected.

## ***Scheduled Report***

Use this tab to enable scheduled reports, schedule the frequency to run the report, and to specify the read method. For more information on scheduled reports and the read method options see [How to Monitor Files](#).

## ***Report Actions***

Use this tab to assign filters and actions for the report.

## ***Verify***

The Verify dialog enables you to review the configuration being set for the directory.

**For more information, see:**

[Actions](#)

[Creating Filters](#)

[File Monitor Wizard](#)

[How to Monitor Files](#)

[Selecting Files and Directories to Monitor](#)

## **Disabling Monitoring**

---

During maintenance periods you may find it necessary to disable monitoring. There are 2 different methods for disabling monitoring.

### **Stopping the Windows Service**

All monitoring is stopped when you stop the Text Log Monitor service. Select Stop from the Service menu item.

### **Disabling Specific Real-Time Monitors**

You can disable specific monitors or a logical group of monitors by checking the monitors or logical groups via the Network view and selected Disable Real Time Monitoring from the Tools menu item. To re-enable the monitors, select Enable Real Time Monitoring from the Tools menu item.

## Display Pages

---

Logs can contain thousands of entries. Loading thousands of entries into the user interface is not only slow but CPU and memory intensive. For this reason, entries are viewed in pages. The first page contains up to 2000 entries while each corresponding read contains an additional 400 entries.

When a log is viewed, the log file is read in its entirety, however; the application does not load all the entries. Instead, the application determines the number of pages required to display the log given the size of the viewer.

To navigate between pages, use the toolbar buttons located directly above the entry list. Pages are displayed from the start to the end of the file. Clicking the *Next Page* button moves the view to the next page of log entries. Clicking the *Previous Page* button moves the view to the previous page of entries.



# File Monitor Wizard

File monitoring is the most basic form of monitoring. User's select a file that already exists and configure the monitor, specify filters and assign actions. For more information see [How to Monitor Files](#).

The file monitor wizard enables users to configure files to monitor, apply filters, and assign actions.

## *Files*

Use this tab to specify the files to monitor. If files were already selected before the wizard opened, this page displays all selected files otherwise use this page to add the files to monitor.

When configuring multiple files within the wizard, use the Files combo box (found at the top of the wizard on each page following the Files tab) to fine tune file configurations.

Please note when viewing and updating configurations for multiple files the following rules apply:

- Text fields and combo-boxes that have different configuration values are empty.
- Check boxes that have different configuration values display with a square rather than empty or with a check box.
- Setting a value in a control sets the value for all the selected logs.

## *General*

Use this tab to specify a user friendly name, logical group, and log entry delimiters.

Use the *Append lines to action* to specify the number of lines after a filtered entry to include in actions. For example, if a log file contains summary information at the end of the file, you can create a filter that specifies the summary header. Then specify the number of lines after the summary header to include in your action.

## *Real Time*

Use this tab to enable real-time monitoring and to specify the read method. When specifying an exclusion period you have the option to shutdown the monitor or suppress actions during the exclusion period. When shutting down the monitor the service will pick up where it left off once re-started. This means all entries written to the log during the exclusion period will be filtered and any corresponding actions fired. When suppressing actions the monitor continues to run, however; actions are suppressed. Once the exclusion period passes the service will only filter new entries.

For more information on real-time monitoring and the read method options see [How to Monitor Files](#).

## *Real Time Actions*

Use this tab to assign filters and actions for the real-time monitor.

### **Frequency Detection**

Frequency detection enables you to fire actions when an expected log entry fails fire within a specified frequency or fires more often than expected.

## *Scheduled Report*

Use this tab to enable scheduled reports and to specify the read method. For more information on scheduled reports and the read method options see [How to Monitor Files](#).

## *Report Actions*

Use this tab to assign filters and actions for the report.

## *Verify*

The Verify dialog enables you to review the configuration being set for each log.

**For more information, see:**

[Actions](#)

[Creating Filters](#)

[Directory Monitor Wizard](#)

[How to Monitor Files](#)

[Selecting Files and Directories to Monitor](#)

## Filters

---

Logs can contain thousands of entries. In order to limit the entries viewed, users can create Filters. Filters have 2 purposes. First, filters enable users to search all entries in a log for specific entries. Second, filters enable users to remove entries deemed unimportant or not relevant at the time. For information on creating filters, see [Creating Filters](#).

Filters are assigned to monitored files, however; users can also open a file within the user interface and apply the filter to the file. When monitoring, actions are fired on behalf of all entries that pass the assigned filter's criteria. For example, an email can be sent when a critical failure occurs. For more information see [Actions](#).

### **To assign a filter to the current view**

Select the appropriate filter from the toolbar's Filter combo-box. Once selected, the filter is automatically applied to the current file.

**For more information, see:**

[Actions](#)

[Creating Filters](#)

[How to Monitor Files](#)

## **Goto Line Number**

---

To jump to a line number, simply press Ctrl-G. Specify the line number. Text Log Monitor will find the line number in the file, display the page the line exists, and lastly highlight the line number.

# How to Monitor Files

---

## *File Monitoring*

File monitoring is the most basic form of monitoring. User's select a file that already exists and configure the monitor, specify filters and assign actions. For more information see [File Monitor Wizard](#).

## *Directory Monitoring*

Directory monitoring enables users to monitor all files that match a search criteria for example \*.log. When an application creates a new file that matches the file name search criteria, Text Log Monitor discovers the file within one minute and then starts monitoring the file. Directory monitoring is most commonly used to monitor files that contain date information within the file name itself. For example syslog\_2008\_01\_31.log. For more information see [Directory Monitor Wizard](#).

## *Read Methods*

Whether monitoring files or directories, users have the option to monitor each file in real-time or at specific intervals called scheduled reports.

## **Real-Time Monitoring**

Use real-time monitoring when you must be notified as soon as an entry is written to a file. Users have the option of reading the file with 3 different methods.

**Beginning of File** – When selected, the first time the monitor starts, Text Log Monitor reads, filters, fires alerts for the entire file, and lastly, waits for new entries. When the service is restarted or the computer is rebooted, the monitor picks up where it left off.

**End of File** – When selected, the first time the monitor starts, Text Log Monitor moves to the end of the file (ignoring current entries) and waits for new entries. When the service is restarted or the computer is rebooted, the monitor picks up where it left off.

**Read All** – When selected, the first time the monitor starts, Text Log Monitor does not read the file. When the operating system notifies Text Log Monitor the file has been updated, Text Log Monitor reads, filters, fires alerts for the entire file. When the service is restarted or the computer is rebooted, Text Log Monitor does not read the file. There is an exception to this rule, however. When monitoring a directory rather than a single file, newly created files are read in their entirety.

## **Scheduled Reports**

Use scheduled reports when you want to receive notification of specific events at a predetermined interval. For example, every Monday at 8:00 AM. Users have the option of reading the file with 3 different methods.

**Beginning of File** – When selected, the first time the report is run, Text Log Monitor reads, filters, fires alerts for the entire file. Each successive report picks up where it left off reading only entries written since the previous report.

**End of File** – When selected, the first time the report is run, Text Log Monitor saves off the length of the file and then exits. Each successive report picks up where it left off reading only entries written since the previous report.

**Read All** – When selected, Text Log Monitor reads the entire file, filters each entry, and lastly fires alerts every time the report is run.

**For more information, see:**

[File Monitor Wizard](#)

[Directory Monitor Wizard](#)

[Selecting Files and Directories to Monitor](#)



## Logical Groups

---

To facilitate ease of configuration and navigation, the Network view supports logical grouping. By grouping file monitors into logical groups, you can easily select a group of file monitors and configure all file monitors in the group at the same time.

### **To create a Logical Group**

Select New Logical Group from the File menu. Once created, use drag and drop to move file and directory monitors from the Unassigned Logical Group to your new group.

### **To rename a Logical Group**

Highlight the logical group and press F2.

Enter the new name and press the enter key.

## **Mail and HTML Templates**

---

Text Log Monitor enables you to create your own email and HTML output templates.

The default template is stored under the installation directory in a sub-directory called HtmlTemplates. The templates are HTML files that must contain <ENTRY\_ODD> and <ENTRY\_EVEN> tags. Each file contains replacement tags denoted with {}. Please review the supplied template for your reference.

## **Mail Connection**

---

Mail Connection parameters are set via the Options dialog. To open the Options dialog, select Options from the Tools menu item. Once open, select the Mail Connection tab.

### **Server Information**

Specify the name of the SMTP server. For example: mail.yourserver.com. If your server runs on a port other than 25, for example 2000, use the following format: mail.yourserver.com:2000

### **Logon Information**

If your SMTP server requires authentication to send messages, specify your username and password.

### **Mail From Information**

Optionally, specify the name and from address to appear in outgoing mail.

### **Testing Account Settings**

When ever you change the mail server settings, it is a good idea to test the settings. To test the account settings, simply click the Test Account Settings button.

## Mapping Computers

The most common reason users map computers is to provide login credentials, however; computers online but undiscoverable can also be specified.

### To map a computer

Select Map Computer from the File menu or select the toolbar button.



From the map computer dialog, specify the hostname or IP address of the machine, the username, password, and domain or workgroup.

A screenshot of the 'Map Computer' dialog box. The title bar reads 'Map Computer'. The dialog has a blue header with a key icon. Below the header are four input fields: 'Computer:' (empty), 'Username:' (empty), 'Password:' (empty) with a 'Show' button to its right, and 'Domain:' (a dropdown menu showing 'CornerBowl'). At the bottom are 'OK' and 'Cancel' buttons.

### To modify login credentials

From the Network view, select the computer under the Mapped Computers tree node.

Select *Properties* from the File menu item or click the properties toolbar button.



Update the username and password as necessary.

A screenshot of the 'Mapped Computer Properties' dialog box. The title bar reads 'Mapped Computer Properties'. The dialog has a blue header with a key icon. Below the header are four input fields: 'Computer:' (filled with 'rm-mjanul-6606'), 'Username:' (filled with 'testuser'), 'Password:' (filled with '\*\*\*\*\*') with a 'Show' button to its right, and 'Domain:' (a dropdown menu showing 'CornerBowl'). At the bottom are 'OK' and 'Cancel' buttons.

### To remove a mapping

If you are no longer monitoring a computer that was previously mapped, or you no longer need to specify login credentials, you can remove the mapping. From the Network view, select the computer under the Mapped Computers tree node. Either click the Delete button, select *Delete* from the Edit menu item or click the delete toolbar button.

## Navigating the Network

---

Text Log Monitor enables you to navigate your network just as if you were in Windows Explorer. Network navigation is accessed via the Network view in the Navigation window.

While navigating your network, you have the ability to:

- Select a log to immediately view the contents.
- Configure monitoring and actions.
- Manually add computers that can not be discovered or require credentials other than the logged in user's credentials. For more information see [Mapping Computers](#).
- Delete manually added computers.
- Print log contents.

## Options

---

Use the options dialog to set configuration parameters.

To open the Options dialog, select Options from the Tools menu item.

The options dialog contains the following pages:

[Mail Connection](#)

[SQL Server](#)

[Syslog](#)

## Printing

---

Text Log Monitor enables you to print an entire log or the entries you have filtered. When you are viewing a log, what ever entries are displayed in the current view, including all pages not currently shown, are printed.

### **To print a log or specific entries**

Open the log and optionally select the filter to apply. Select Page Setup from the File menu. Use the Page Setup dialog to select the page orientation and margins. Once you have dismissed the Page Setup dialog, press Ctrl-P, or select Print from the File, or select the toolbar button.



## **Refresh**

---

Clicking Refresh from the View menu item refreshes the currently selected tree node in the Network View.

## Saving Filtered Results

---

Upon filtering a file within the user interface, you may want to export the results for another individual to review, archive purposes, or for future reference. Text Log Monitor can export files to CSV, HTML, XML, and TXT. The CSV export is optimized for Microsoft Excel.

### **To save filtered results to another file**

Select Save As from the File menu.

Specify the file name and type. Lastly, click Save.

**For more information, see:**

[Filters](#)

## Searching Logs

Logs can contain thousands of entries. Text Log Monitor allows you to search for specific log entries. For information on filtering logs see [Filters](#).

### Find Dialog Box

The Find dialog box allows you to search for entries within the current view or page. You can access the Find dialog box by choosing Find on the Edit menu, or by pressing Ctrl-F, or by selecting the toolbar button.



The Find dialog box searches through the view from the insertion point down or from the insertion point up, depending on which search direction you choose.

The Find dialog box provides many search parameters to help you improve the accuracy of your search.

#### Message

Enter the text for which you intend to search. This field optionally supports regular expressions.

#### Match case

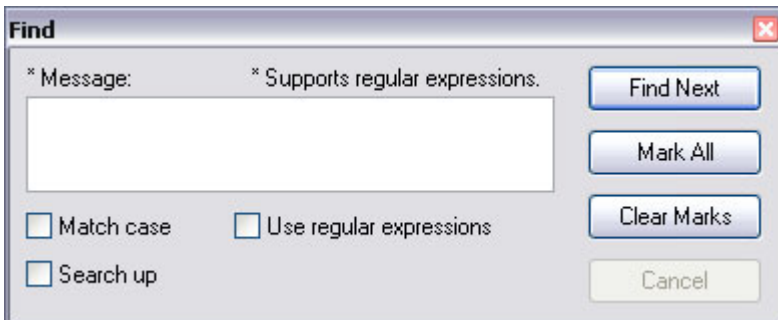
When selected, the search operation looks only for occurrences that match the uppercase and lowercase characters you enter in the Message box.

#### Search Up

When selected, the view is searched from the current row to the top.

#### Use regular expressions

When specified, regular expression rules apply.



For more information, see:

[Filters](#)

# Selecting Files and Directories to Monitor

---

## How to Select Files

### To configure a log for the first time

Select New File Monitor Wizard from the File menu. You must navigate your network from within the File Monitor Wizard.

or

From the Network view, select the file(s) of interest.

To configure multiple files at the same time, check each file of interest.

Please note, if you do not select any files, you must navigate your network from within the File Monitor Wizard.

Select File Monitor Wizard from the File menu.

Follow the instructions in the wizard. For more information on the wizard, see [File Monitor Wizard](#).

### To change a log's configuration

From the Network view, select the files(s) of interest.

To configure multiple files at the same time, check each computer of interest.

Select File Monitor Wizard from the File menu.

Follow the instructions in the wizard. For more information on the wizard, see [File Monitor Wizard](#).

### To remove a configured log

From the Network view, select the files(s) of interest.

To remove multiple configurations at the same time, check each file of interest.

Select Delete from the Edit menu.

## How to Select Directories

### To configure a directory for the first time

From the Network view, select the directory of interest.

Select Directory Monitor Wizard from the File menu. For more information on the wizard, see [Directory Monitor Wizard](#).

### To change a directory's configuration

From the Monitored Files tree node within the Network view, select the directory of interest.

Select Directory Monitor Wizard from the File menu. For more information on the wizard, see [Directory Monitor Wizard](#).

### To remove a configured directory

From the Monitored Files tree node within the Network view, select the directory of interest.

Select Delete from the Edit menu.

### For more information, see:

[Directory Monitor Wizard](#)

[File Monitor Wizard](#)

[How to Monitor Files](#)



## SQL Server

---

Text Log Monitor enables you to write entries that pass filter criteria to user defined tables. The first step in this process is to configure your SQL Server connection.

### **Setting the SQL Server Connection Parameters**

The SQL Server connection information is set from within the Options dialog. To open the Options dialog, select Options from the Tools menu item. Once open, select the SQL Server tab.

From the SQL Server tab of the Options dialog, specify the host, database, username and password to connect. The user must have rights to create new tables. Once input, click the *Test Connection* button.

### **Setting the SQL Server Connection and Command Timeouts**

It may become necessary to increase the connection and/or command timeouts. Use the connection timeout and command timeout controls to increase the timeouts.

### **SQL Server Filter Actions**

When entries match filter criteria, Text Log Monitor can write entries to a SQL Server database table. For more information, see [Configuration Wizard](#).

## Syslog

---

Text Log Monitor uses Syslog in 2 ways. First, you can configure a monitor to forward log entries to a syslog server. Second, the Text Log Monitor Windows Service optionally logs status messages to a syslog server.

Use the [Actions Manager](#) to create an action that forwards monitored log entries to your syslog server.

Use the Options dialog to configure the Text Log Monitor Windows Service to enable or disable syslog messaging as well as assign the host and facility to log to.

### Configuring the Text Log Monitor Windows Service to Syslog

Select *Options* from the *Tools* menu item.

*Enabled*

Check to forward service messages to your syslog server.

*Host*

Specify the host name of your syslog server. For example: yoursyslogserver.

*Facility*

Specify the syslog facility. The default value is Local1.

**Note:** If you change any settings, you must restart the service for the changes to take effect.

**For more information, see:**

[Actions](#)

RFC 3164 available at <http://www.faqs.org/rfcs/rfc3164.html>

## Tray Icon

---

Icons in the lower right corner of Windows Taskbar are called Tray Icons. Tray Icons display application status. The Text Log Monitor tray icon has two states:



### **Service Running**

This is the normal state and indicates the service is running properly.



### **Service Stopped**

This state indicates the Text Log Monitor service is not running. Either use the Windows Service Control Manager or Text Log Monitor to turn the Text Log Monitor service on. Once running, the icon will change to the Service Running state.

### **To temporarily turn the tray icon off**

Select *Close Tray Icon* from the *Service* menu.

**NOTE:** Message box, tray popup messages, and sound actions will no longer occur.

### **To temporarily turn the tray icon on**

Select *Start Tray Icon* from the *Service* menu.

### **To permanently disable or re-enable the tray icon**

Select *Options* from the *Tools* menu item.

Select the *Tray Icon* tab.

Check the option to disable or un-check to re-enable.

## Change Service Login

---

Text Log Monitor uses a service to monitor files. This service is called Text Log Monitor. In order for the Text Log Monitor service to access network resources, it must run with domain administrator rights.

### To change the service login credentials

Select *Change Service Login* from the *Service* menu item.

Specify a domain administrator username and password. Lastly, specify the domain. When you are finished, click *Next*. The service configuration will be modified with these rights and the service restarted.

**For more information, see:**

[Security](#)

## Starting and Stopping the Windows Service

---

To configure Text Log Monitor to monitor files automatically, the service must be running. To aid in troubleshooting, the service can be started in verbose (debug) mode. In this mode, extra messages are logged.

### To Start the Service

Select *Start* from the *Service* menu item.

If you are unable to start the service because of a login failure, you must reset the login credentials. For more information see [Change Service Login](#).

### To Start the Service in Verbose Mode

Select *Start (Verbose)* from the *Service* menu item.

### To Stop the Service

Select *Stop* from the *Service* menu item.

**For more information, see:**

[Change Service Login](#)

[Windows Service Log File](#)

## Windows Service Log File

The Text Log Monitor Service logs all significant activity to a log file called 'tlm.log'. This information is invaluable when trouble shooting the service. This file is located in the installation directory. The default location is:

- *Window XP/2000*: 'documents and settings\all users\application data\CornerBow\Text Log Monitor\tlm.log'
- *Windows Vista*: '\programdata\CornerBow\Text Log Monitor\tlm.log'

### To View the Log File

Select *View Log* from the *Service* menu or select the toolbar button.



The entries are sorted from oldest to latest. The log file can also be viewed in any text editor.

### To Clear the Log File

The service automatically truncates the log file to a little less than 1 MB every hour on the hour. The service will log an error when attempting to truncate the log file when the user interface is open. To manually clear or delete the entire log file, the service must be stopped and the user interface closed. Once the service is stopped and the user interface is closed, manually delete the log file. After the file has been deleted, re-start the service. For more information on starting and stopping the service see [Starting and Stopping the Windows Service](#).

**For more information, see:**

[Starting and Stopping the Windows Service](#)

## Troubleshooting

---

The most common error reported by the operating system is:

- Access Denied

As you might have guessed, there are many causes for these errors. If reading files from another computer on the network, make sure that the account you are logged in as and the account the service is running under both have administrative privileges. For more information see [Change Service Login](#). If a networked file requires credentials other than the domain administrator credentials, you must map the computer to specify the credentials. For more information see [Mapping Computers](#).

**For more information, see:**

[Change Service Login](#)

[Mapping Computers](#)

## Security

---

To access files from the user interface your login account must have read rights to access the file. If your account does not have these rights, you can map a computer and specify appropriate login credentials. For more information see [Mapping Computers](#).

When scheduling the service to monitor logs and the logs reside on a computer that has been mapped, the Text Log Monitor service must be run with domain administrator rights. When the password assigned to the account the service is running under changes you must update the service to use the latest password. For more information see [Change Service Login](#).

**For more information, see:**

[Change Service Login](#)

[Mapping Computers](#)

[Troubleshooting](#)

## Windows Service Log File

The Text Log Monitor Service logs all significant activity to a log file called 'tlm.log'. This information is invaluable when trouble shooting the service. This file is located in the installation directory. The default location is:

- *Window XP/2000*: 'documents and settings\all users\application data\CornerBow\Text Log Monitor\tlm.log'
- *Windows Vista*: '\programdata\CornerBow\Text Log Monitor\tlm.log'

### To View the Log File

Select *View Log* from the *Service* menu or select the toolbar button.



The entries are sorted from oldest to latest. The log file can also be viewed in any text editor.

### To Clear the Log File

The service automatically truncates the log file to a little less than 1 MB every hour on the hour. The service will log an error when attempting to truncate the log file when the user interface is open. To manually clear or delete the entire log file, the service must be stopped and the user interface closed. Once the service is stopped and the user interface is closed, manually delete the log file. After the file has been deleted, re-start the service. For more information on starting and stopping the service see [Starting and Stopping the Windows Service](#).

**For more information, see:**

[Starting and Stopping the Windows Service](#)

## Technical Support

---

If you have any problems with Text Log Monitor you can contact our tech support by emailing us at:

[support@cornerbowl.com](mailto:support@cornerbowl.com)

Please make sure you tell us as much information as you can about the problem you are experiencing, including any error or warning messages that may have been displayed.

Please include the following information with all support requests:

- The version you are running. This information can be obtained from the About box.
- The 'tlm.log' file. This file is located in the installation directory. The default location is:
  - *Window XP/2000*: '\documents and settings\all users\application data\CornerBowl\Text Log Monitor\trlm.log'
  - *Windows Vista*: '\programdata\CornerBowl\Text Log Monitor\trlm.log'
- The operating system version.
- If applicable, your license key.
- Description of your problem. Please provide as much information as possible so we can reproduce the problem if necessary.

We'll try to help you as fast as possible, usually in one or two business days.

If you have any comments or suggestions for the next releases, please feel free to post them to us.

## Contact Information

Website: [www.cornerbowl.com](http://www.cornerbowl.com)

Email: [support@cornerbowl.com](mailto:support@cornerbowl.com)

Phone: 1-(866)-543-9470 (TOLL FREE)