Release Number: 6.1.2

SecureLogix Syslog Alert Tool

User Guide

DOC-SAT-ETM612-2011-0801

About SecureLogix Corporation

SecureLogix Corporation enables secure, optimized, and efficiently managed enterprise voice networks. The company's ETM® (Enterprise Telephony Management) System hosts a suite of integrated telecom applications that protect critical network resources from telephony-based attack and abuse, and simplify voice network management.

SecureLogix® Solutions address real-world problems for real-world voice networks. The flexible ETM System scales to support any voice environment, no matter how large or small. Engineered with full hybrid voice technology, the ETM System supports multi-vendor networks containing any mix of converging VoIP and legacy voice systems.

SecureLogix Solutions are currently securing and managing over two million enterprise phone lines. The company's customers span nearly every industry vertical, from regional banks and hospitals, to the largest military installations and multi-national corporations.

For more information about SecureLogix Corporation and its products and services, visit our website at *http://www.securelogix.com.*

Corporate Headquarters:

SecureLogix Corporation

13750 San Pedro, Suite 820

San Antonio, Texas 78232

Telephone: 210-402-9669 (non-sales)

Fax: 210-402-6996

Email: *info@securelogix.com*

Website: *http://www.securelogix.com*

Sales:

Telephone: 1-800-817-4837 (North America)

Email: *sales@securelogix.com*

Customer Support:

Telephone: 1-877-SLC-4HELP

Email: *support@securelogix.com*

Web Page: *http://support.securelogix.com*

Training:

Telephone: 210-402-9669

Email: *training@securelogix.com*

Web Page: *http://training.securelogix.com*

Documentation:

Email: *docs@securelogix.com*

Web Page: *http://support.securelogix.com*

IMPORTANT NOTICE:

This manual, as well as the software and/or Products described in it, is furnished under license with SecureLogix Corporation ("SecureLogix") and may be used only in accordance with the terms of such license.

The content of this manual is subject to change without notice. SecureLogix assumes no responsibility or liability for any errors or inaccuracies that may be contained herein or to correct the same.

This product is protected by one or more of the following patents: US 6,249,575 B1, US 6,320,948 B1, US 6,687,353 B1, US 6,700,964 B1, US 6,718,024 B1, US 6,735,291 B1, US 6,760,420 B2, US 6,760,421 B2, US 6,879,671 B1, US 7,133,511 B2, US 7,231,027 B2, US 7,440,558 B2, CA 2,354,149, DE 1,415,459 B1, FR 1,415,459 B1, and GB 1,415,459 B1. U.S. Patents Pending.

ETM is used herein as shorthand notation to refer to the ETM® System.

This product includes:

Customer Support for Your ETM® System

1-877-SLC-4HELP
(1-877-752-4435)
support@securelogix.com
http://support.securelogix.com

SecureLogix Corporation offers telephone, email, and web-based support. For details on warranty information and support contracts, see our web site at

http://support.securelogix.com

Contents

Preface

About the SecureLogix Syslog Alert Tool Documentation

The documentation for the SecureLogix Syslog Alert Tool consists of a user guide in PDF format and online Help. The electronic PDF is available at the root of the SecureLogix Syslog Alert Tool software installation CD.

Tell Us What You Think

We welcome your suggestions or comments on the user guides and the online Help provided with your ETM System. Please send your documentation feedback to the following email address:

docs@securelogix.com

Additional Documentation on the Web

SecureLogix Corporation provides corrections and additional documentation for its products via the SecureLogix Knowledge Base online at the following web address:

http://support.securelogix.com

Conventions Used in This Guide

The following conventions are used in this guide:

- Functions that require two or more mouse clicks to open a dialog box or make a selection are written using the pipe symbol. For example:

  Click **View | Implied Rules**.

- Names of keys on the keyboard are uppercase. For example:

  Highlight the field and press DELETE.

- If two or more keys must be pressed at the same time, the PLUS SIGN (+) is used as follows:

  Press CTRL+ALT+DELETE.

- Bold text indicates GUI labels, menu items and options, literal file names, and paths. For example:

  Click **Edit**, and then click **Preferences**.

  C:\Program Files\SecureLogix\ETM\TWLicense.txt

- Keyboard input is indicated by monospaced font. For example:

  In the **Name** box, type: `My report tutorial`
- Italics indicate web addresses and names of publications.
- ETM System components and features are capitalized.

SecureLogix Syslog Alert Tool

About the Syslog Alert Tool

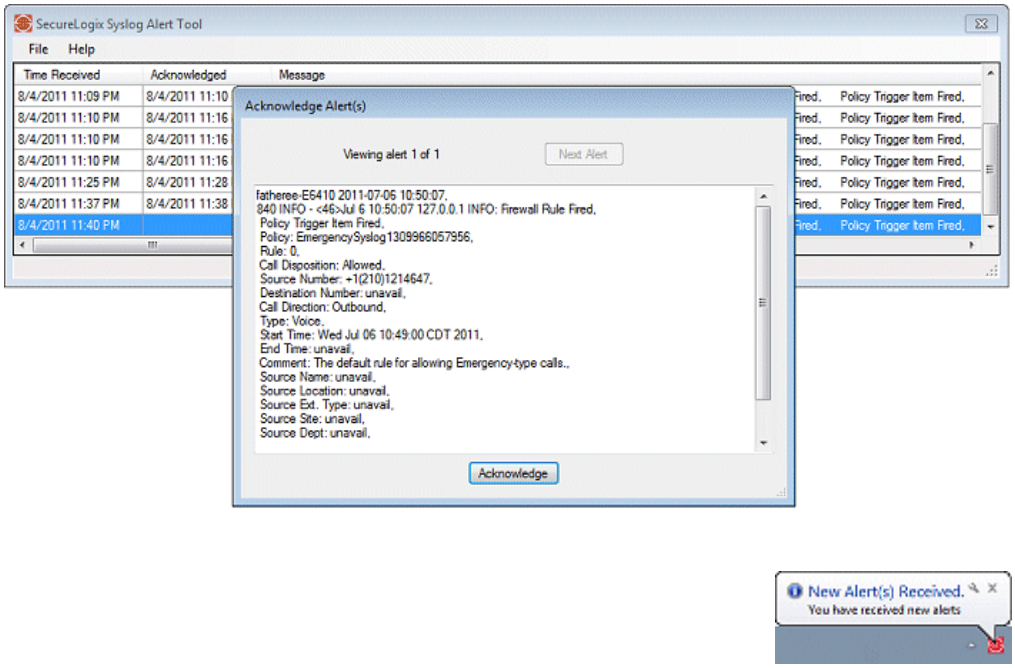
Visual and Audible Alert Notifications

The SecureLogix Syslog Alert Tool automatically notifies a workstation user when a system event and/or policy alert, such as a 911 call, is received from the ETM® Syslog Server.

When a user logs in to a workstation on which the Syslog Alert Tool is installed, the program automatically launches and runs continuously as a background process.

When a system event and/or policy alert, also referred to as a syslog alert, is received, all of the following actions occur:

- An audible tone sounds.
- The **SecureLogix Syslog Alert Tool** window and the **Acknowledge Alert(s)** window are both proximately displayed in front of all other currently running applications with detailed information about the syslog alert.
- The Syslog Alert Tool icon in the system tray displays a "New Alert(s) Received" message.
- The alert is written to an alert log text file.



The workstation user reviews alert details and acknowledges the alert(s) in the **Acknowledge Alert(s)** window. After acknowledging alerts, the **SecureLogix Syslog Alert Tool** window remains displayed in front of all other windows showing acknowledged alerts for the current user session.

If alerts are not acknowledged, any new alerts that occur are added to the **Acknowledge Alert(s)** and **SecureLogix Syslog Alert Tool** windows with the most recent alert highlighted.

After all alerts have been acknowledged, the **SecureLogix Syslog Alert Tool** window can be closed to the system tray. When a new alert is later received, the **Acknowledge Alert(s)** and **SecureLogix Syslog Alert Tool** windows are both again proximately displayed.

All syslog alerts received by the Syslog Alert Tool are added to a daily alert log text file allowing system administrator to view historical alert details.

Installation Instructions

Installation and Configuration Overview

This chapter explains how to install and configure the SecureLogix Syslog Alert Tool for use with the ETM® System.

The installation and configuration steps include:

- Software Installation
- Configuring the local computer to received syslog alerts from the ETM Server
- Configuring the ETM Server to send syslog alerts.

The ability to start, stop, and configure the Syslog Alert Tool is only available to users who are logged in as an administrator on the local computer. (Users without administrator rights are only able to acknowledge alerts and minimize the tool after all alerts are acknowledged.)

Software Installation

The SecureLogix Syslog Alert Tool is an optional ETM® component that is installed from a CD onto a workstation that is configured to receive syslog alerts from the ETM Syslog Server.

System Requirements

The SecureLogix Syslog Alert Tool system requirements are:

- Windows XP, Windows Vista, or Windows 7.
- Microsoft .NET Framework 4.
  (If not currently installed on the local computer, the installation CD will direct you to the Microsoft website for download.)

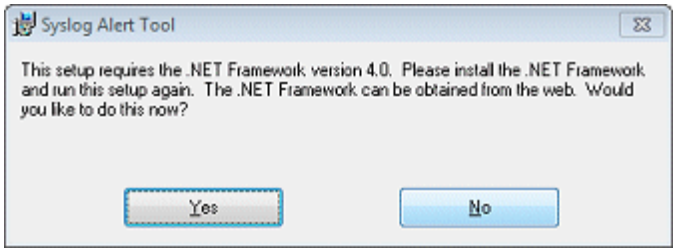
Software Installation

The software installation is typical for a Windows installation process.

To install the SecureLogix Syslog Alert Tool software

1. Insert the Syslog Alert Tool CD into the CD-ROM drive.
2. Navigate to the **Syslog Alert Tool** directory, and then double-click **Setup.exe**.

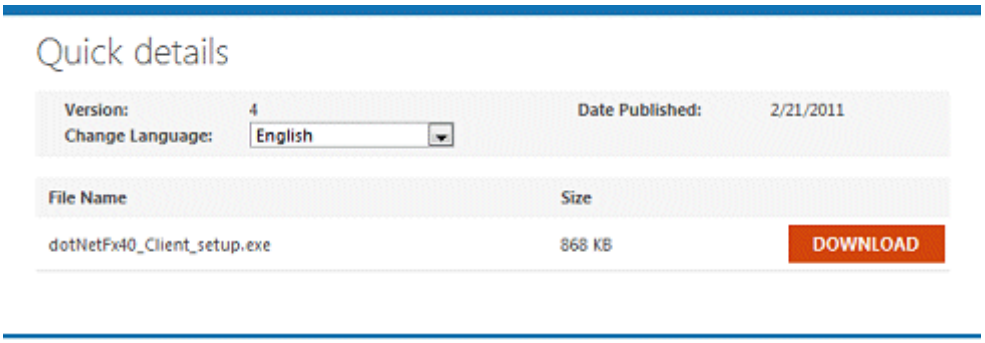
   If Microsoft .NET Framework 4 is **not** currently installed, the **Syslog Alert Tool** dialog box appears asking you install this program. (Otherwise, continue with step 3 below.)

   a. Click **Yes** to be directed to the Microsoft download center.

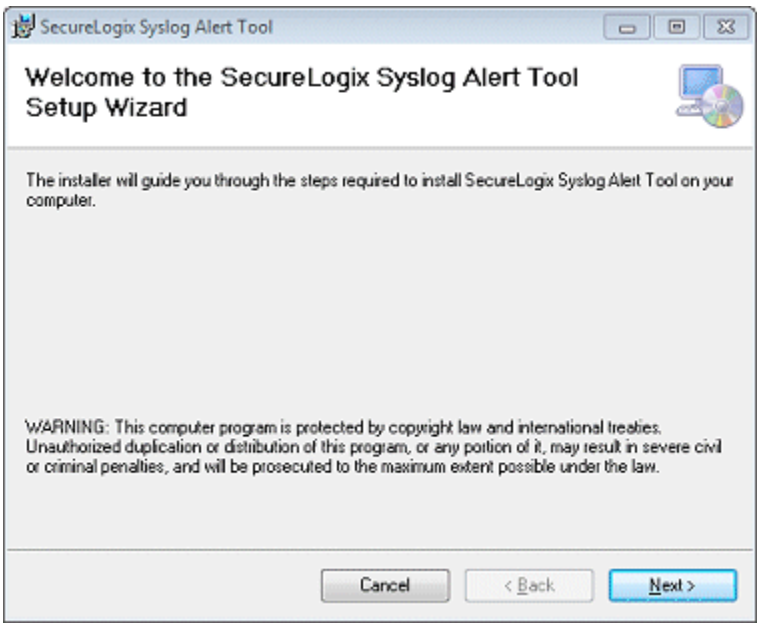
   b. On the webpage "Microsoft .NET Framework 4Client Profile (Web Installer)" review the System Requirements and Instructions, performing updates as necessary.

c. Click the **Download** button and follow the installation instructions.

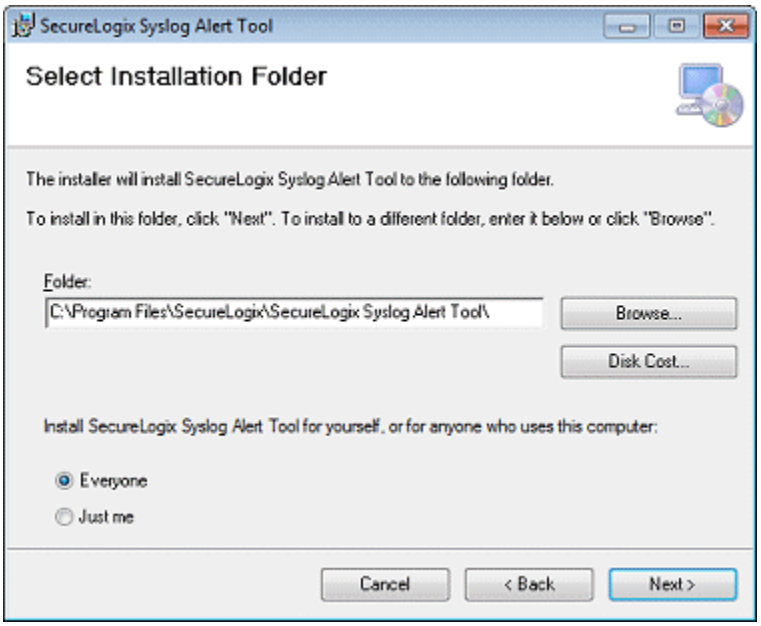


d. After the .NET Framework 4 installation is complete, navigate to the **Syslog Alert Tool** directory, and then double-click **Setup.exe**.

3. The **SecureLogix Syslog Alert Tool Setup Wizard** appears.

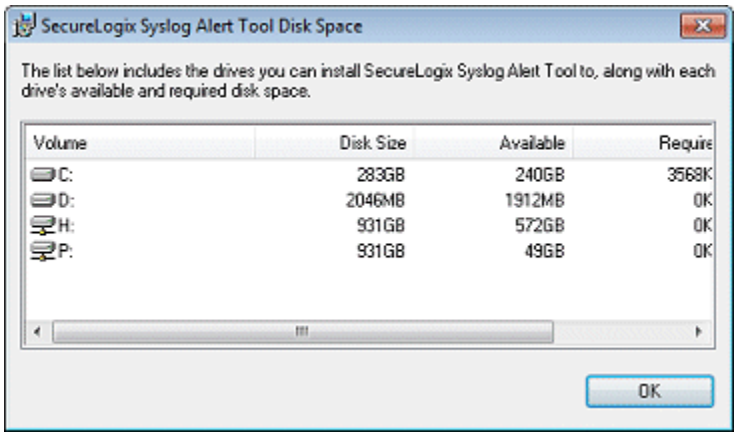


4. Click **Next**. The **Select Installation Folder** dialog box appears.



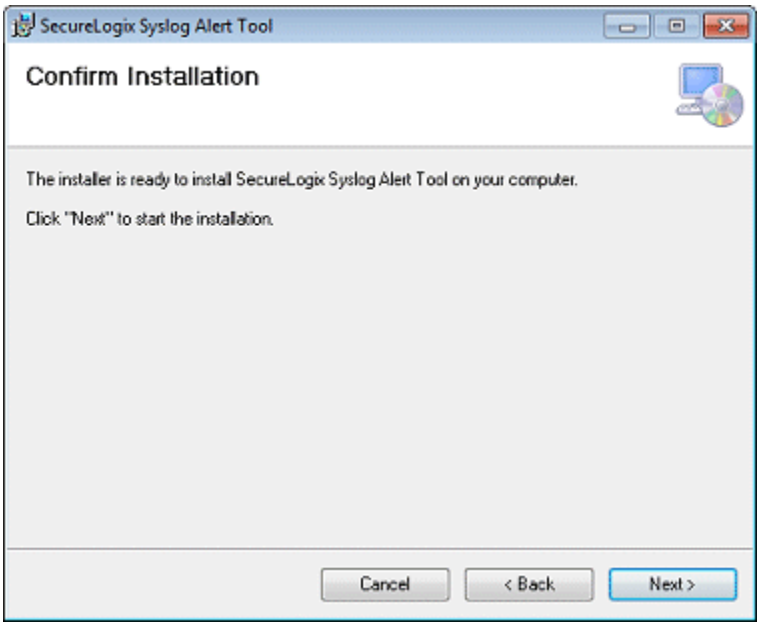
a. The **Folder** box displays the default installation path. To specify a different path, type it in the box or click **Browse** to select the path.

b. To verify available hard drive space, click **Disk Cost**. The **Syslog Alert Tool Disk Space** dialog displays the disk space available on each drive. Click **OK** to close the Disk Space window.

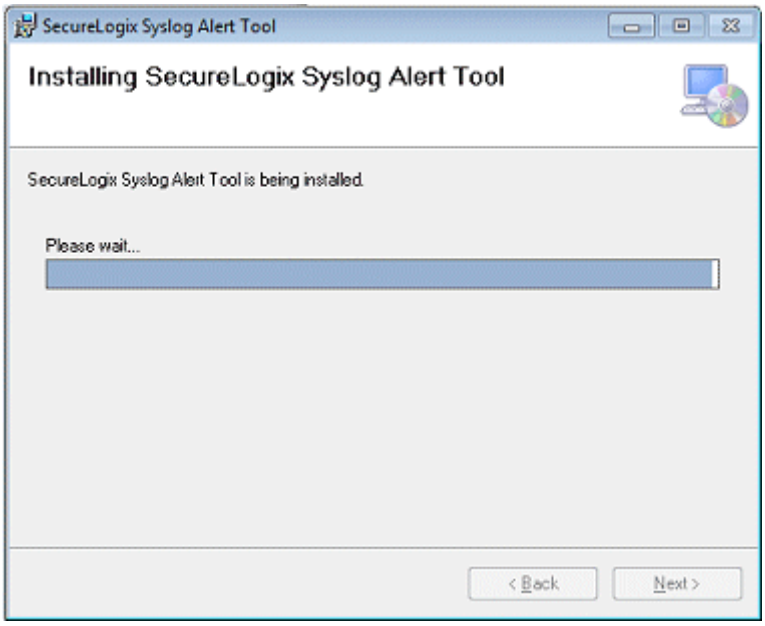


c. By default, the Syslog Alert Tool is only installed for the logged in user. To make the Syslog Alert Tool available to everyone who logs in to the computer, click **Everyone**.

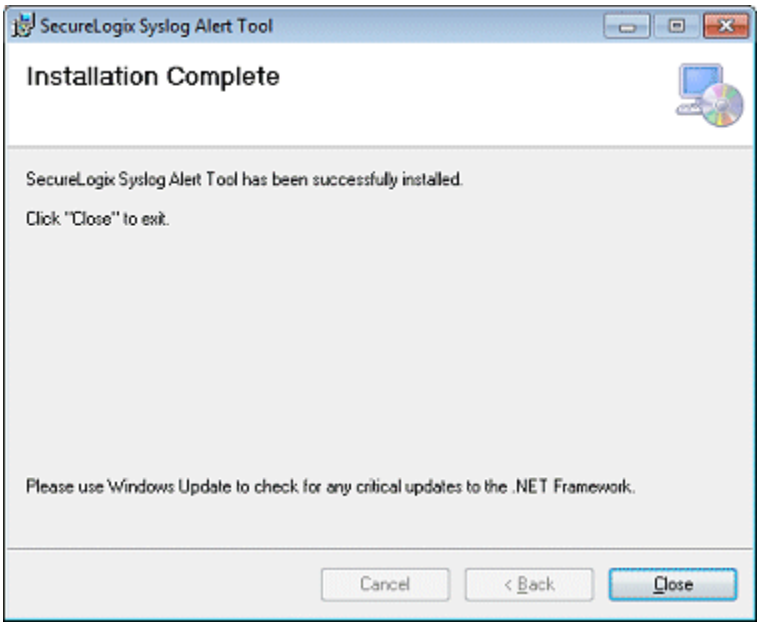
5. Click **Next**. The **Confirm Installation** dialog box appears.



6. Click **Next** to start the installation.



7. When the installation is complete, click **Close** to exit.



8. By default, the Syslog Alert Tool is configured to start automatically on system startup.

   To start the SecureLogix Syslog Alert Tool without restarting the computer, perform the following steps:

   - In Windows XP: Open the Control Panel, then select **Administrative Tools** | **Services**. Right-click **Syslog Alert Tool** and select **Start**.
   - In Windows 7: Open the Windows Task Manager and click the **Services** tab. Right-click **Syslog Alert Tool** and select **Start Service**. See "Windows 7 Hidden Icon" on page 16.

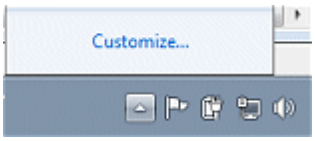
Windows 7 Hidden Icon

In Windows 7, the Syslog Alert Tool icon displays temporarily in the Notifications area and then it becomes a hidden icon. Perform the following steps so that the icon is always displayed.

To display the Syslog Alert Tool icon

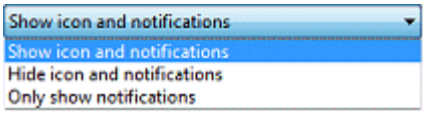
SecureLogix Syslog Alert Tool Icon

1. On the Windows 7 desktop, click the Notifications arrow. The Customize menu appears.



2. Click **Customize**.

3. Click the down arrow for the "Alert Tool Client" Behavior and select **Show icon and notifications**.



4. Click **OK**. The Syslog Alert Tool icon now displays in the Notifications area.

Configure the Local Computer to Receive ETM Syslog Alerts

To allow the Syslog Alert Tool to **receive** alerts, configure the local computer's **Windows Firewall** with the receiving Port number and the IP address of the ETM Server.

NOTE: Only the default ETM Syslog Port 514 is supported in this release. For future reference, see "Changing the Port Number in the Config File" on page 19.

Also see "Configuring the ETM Server to **Send** Syslog Alerts" on page 20.

Firewall Settings - Windows XP

To configure the IP address and Port in the Windows XP

1. Click **Start**, click **Run**, type **Firewall.cpl** in the Open box, and then click **OK.** The **Windows Firewall** window appears.
2. Click the **Exceptions** tab, and then click **Add Port**. The **Add a Port** dialog box appears.
3. In the **Name** box, type a descriptive name for this port such as "Syslog."

Default Receiving Port is UDP 514

4. In the **Port number** box, type: **514**
5. Select **UDP**.
6. Click the **Change scope** button. The **Change Scope** dialog box appears.
7. Select **Custom List**, and then type IP address of the ETM Server sending the syslog alerts.
8. Click **OK**.

Firewall Settings - Windows 7

To configure the IP address and Port in the Windows 7 Firewall

1. Click the Windows **Start** menu, type: **WF.msc** in the search box, and then press ENTER. The Windows Firewall with Advanced Security window appears.
2. In the left pane, click **Inbound Rules**.

3. In the right Actions pane, click **New Rule**. The New Inbound Rule Wizard window appears.
4. In the **Rule Type** dialog box, select **Custom**, and then click **Next**.
5. In the **Program** dialog box, select **This program path**.
6. Click the **Browse** button to navigate and select "<The Install Path> \SyslogAlertTool.exe". For a typical install, this is: "C:\Program Files\SecureLogix\Syslog Alert Tool\SyslogAlertTool.exe"
7. Click **Open**.
8. To the right of Services, click the **Customize** button. The **Customize Service Settings** dialog box appears.
9. Click **Apply to this Service**.
10. Scroll down and select **SecureLogix Syslog Alert Tool**, click **OK**, then click **Next**.
11. In the **Protocol and Ports** dialog box:
    a. Click the **Protocol type** down arrow and select **UDP**.
    b. Click the **Local port** down arrow and select **Specific Ports**.

Receiving Port is UDP 514

    c. In the **Local port** box, type the number of the receiving port: **514**
    d. Leave the **Remote port** set to **All Ports**.
    e. Click **Next**.
12. In the **Scope** dialog box:
    a. For the question *"Which local IP addresses does this rule apply to?"* select **Any IP address.**
    b. For the question *"Which remote IP addresses does this rule apply to?"* select **These IP addresses**.
    c. Click the **Add** button. The **IP Address** dialog box appears.
    d. Select **This IP address or subnet**, and then in the box, type the IP address of the ETM Server from which alerts will be received.
    e. Click **OK**.
13. In the **Scope** dialog box, click **Next**.
14. In the **Action** dialog box, click **Allow the connection**, then click **Next**.

15. In the **Profile** dialog box, in answer to the question "*When does this rule apply?*" select the profile for which the rule applies. (**Domain, Private,** and/or **Public**)
16. Click **Next**. The Name dialog box appears.
17. In the **Name** box, type a descriptive name for this rule, such as "Syslog Alerts."
18. Click **Finish**.

Changing the Port Number in the Config File

NOTE: For this software release, the receiving port number must be set to UDP 514.

The receiving port number is defined in the file: SyslogAlertTool.exe.config.

The following instructions to change the default port setting are provided for future reference only.

Currently supported Port is UDP 514

To change the receiving port number

1. Navigate to the file: SyslogAlertTool.exe.config

   For a typical installation, the file location is: C:\Program Files\SecureLogix\Syslog Alert Tool
2. Use a text editor to open the config file.
3. Edit the port value in the "appSettings" section.

```
<appSettings>
    <add key="ClientPath"
value="AlertToolClient.exe"/>
    <add key="ClientProcess"
value="AlertToolClient"/>
    <add key="Port" value="512"/>
</appSettings>
```

4. Save the SyslogAlertTool.exe.config file.

Additional Filter Settings in the Config File

The Syslog Alert Tool is configured to display the syslog alert that matches Firewall Policy Rule number zero (0) "Emergency Calls", i.e. 911 calls. This is accomplished by the use of a standard regular expression in the "Filter" section of the SyslogAlertTool.exe.config file.

```
<filter name="Emergency Calls" priority="10" regex="\s+Rule:\s+0,\s+"/>
```

As an advanced option, additional filters for syslog events (system events and/or rules) may be added. You can add as many filters as necessary for your monitoring preferences by adding filters inside the filters tag.

```
<filtersSection>
  <filters>
     <filter name="Emergency Calls" priority="10" regex="\s+Rule:\s+0,\s+"/>
  </filters>
</filtersSection>
```

Where:

- The filter name field needs to be unique.
- The priority field, while not currently used in this release, needs to be a positive integer.
- The regex field needs to be a valid standard regular expression.

For detailed information and instruction, see the topic "Regular Expressions" in the ETM System Technical Reference. **Tip:** Naming policies to include text indicating type or including meaningful text in the comment of a rule can assist in writing a regex. Additionally, contact Customer Support for assistance with modifying a regex.

To add filters to receive additional alerts

1. Navigate to the file: SyslogAlertTool.exe.config

   For a typical installation, the file location is: C:\Program Files\SecureLogix\Syslog Alert Tool
2. Use a text editor to open the config file.
3. Locate the "Filters Section".
4. Add a new filter line(s) after "Emergency Calls."
5. Save the SyslogAlertTool.exe.config file.

Configuring the ETM Server to Send Syslog Alerts

The ETM System supports system event and Policy alerting via Syslog. You can specify one or more ETM Syslog servers to receive alerts generated in response to specific system events or firing of Policy rules. Generated alerts are sent to all configured ETM Syslog servers. The ETM Server must be configured to receive Syslog alerts before the Syslog Alert Tool can receive and display the alerts.

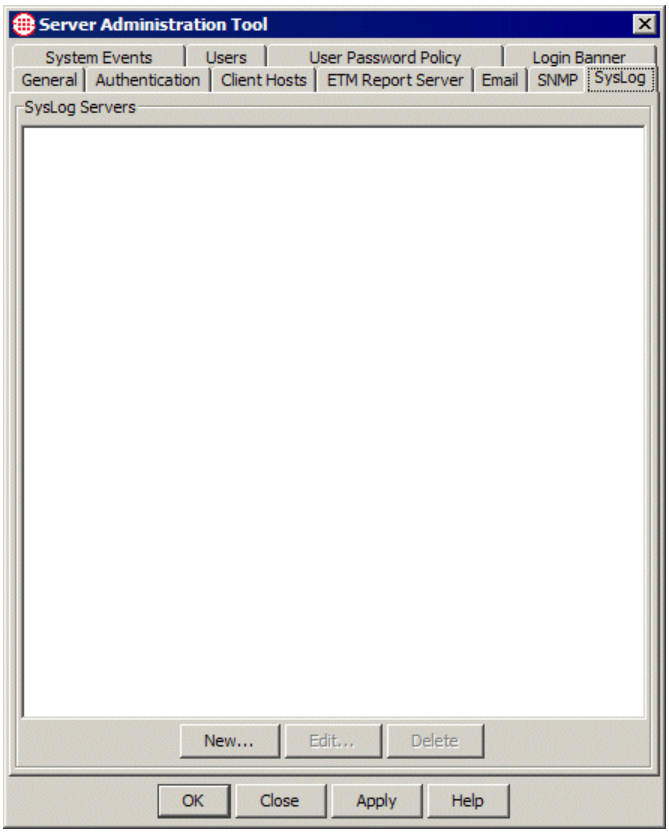
Also see "Configure the Local Computer to Receive ETM Syslog Alerts" on page 17.

Specifying Syslog Servers

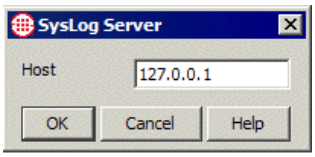
Configure the ETM Server to send system events and policy alerts to the Syslog Server.

To specify a Syslog server

1. On the ETM System Console, highlight the desired Management Server in the tree.
2. On the main menu, click **Servers | Server Management**. The **Server Administration Tool** appears.



3. Click the **Syslog** tab.
4. Click **New**. The **Syslog Server** dialog box appears.



5. In the **Host** box, type the IP address of the Syslog server. (Remember that only the default Syslog port (514) is supported in this release.)
6. Click **OK**. The Syslog server appears in the Syslog servers list.
7. Repeat for additional servers as needed. When you are done, click **OK** to save the changes and close the dialog box, or **Apply** to save the changes and leave the dialog box open.

Setting Email Alerts

The ETM Server manages system events and policy alerts. You can configure the ETM System to send an email notification to the appropriate personnel by assigning one or more Tracks to cause follow-up actions.

See “Setting Track Actions for System Events” in the *ETM® System Administration and Maintenance Guide.*

See "Tracks" in the *ETM® System User Guide* for instructions for defining email tracks.

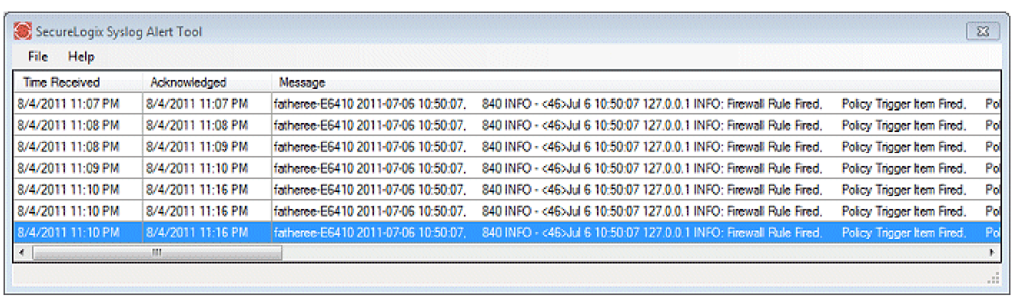
Monitoring Alerts

Overview

When a user logs in to a workstation on which the Syslog Alert Tool is installed, the tool automatically launches and the Syslog Alert Tool icon is displayed in the system tray. The Syslog Alert Tool runs continuously as a background process, listening for syslog alerts, until the user logs out.

When the SecureLogix Syslog Alert Tool receives an alert from the ETM Syslog Server, two (2) windows are displayed:

- The **Acknowledge Alert(s)** window enables the user to review alert details and then acknowledge the alert event.
- The **SecureLogix Syslog Alert Tool** window displays a list of acknowledged and unacknowledged alert(s) that have occurred during the current user session. The following information is displayed:
    - **Time Received** – date and time the syslog message was received from the ETM Syslog Server.
    - **Acknowledged** – date and time the workstation user clicked the **Acknowledge** button in the **Acknowledge Alert(s)** window.
    - **Message** – details about the syslog alert(s).

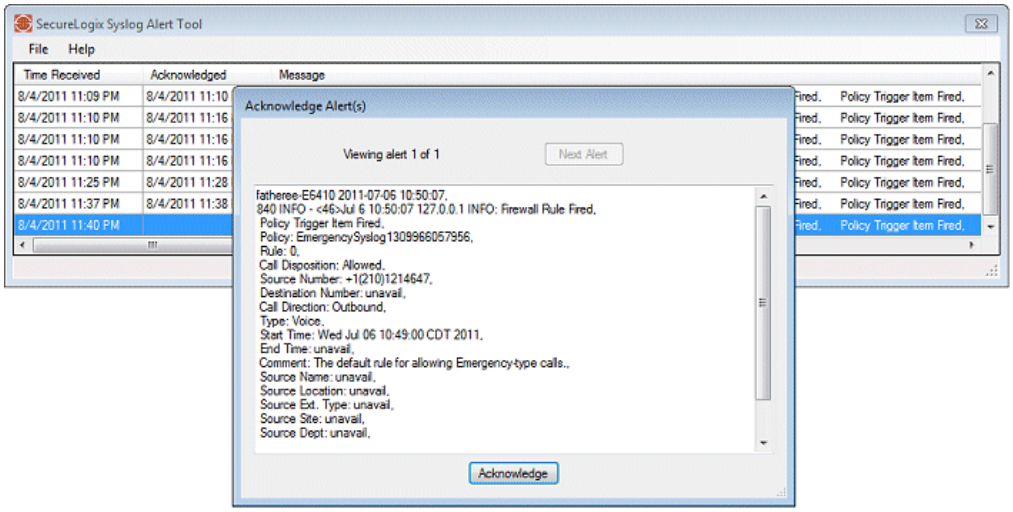


All syslog messages received that display the **Acknowledge Alert(s)** and the **SecureLogix Syslog Alert Tool** windows are also logged to a text file viewable to the system administrator. See “Syslog Alert Log Files” on page 28.

Monitoring Alerts

To monitor alerts with the SecureLogixSyslog Alert Tool

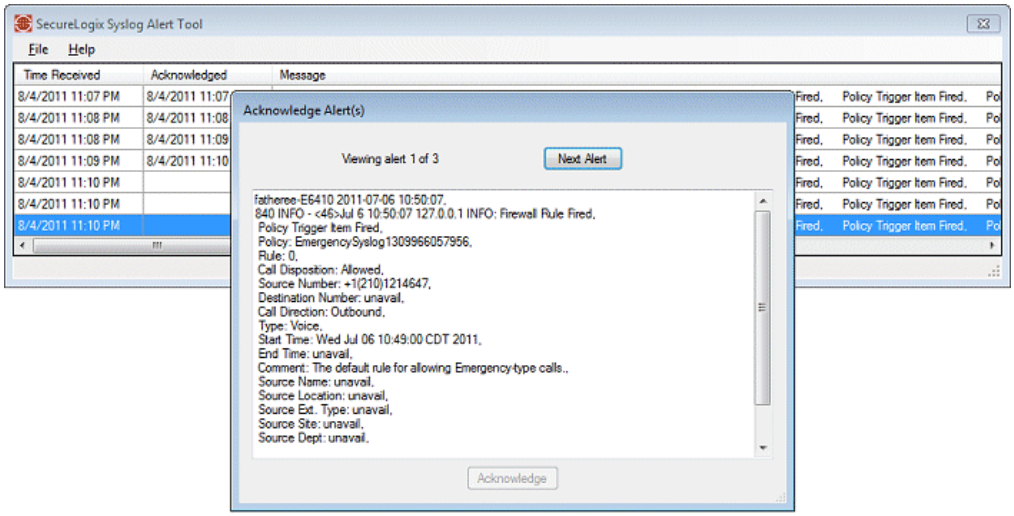
1. Log in to the workstation on which the SecureLogix Syslog Alert Tool is installed. The Syslog Alert Tool automatically launches, as indicated by the  icon in the system tray, and is waiting for syslog alerts. (See “Windows 7 Hidden Icon” on page 16.)
2. When a new alert is received, both the **SecureLogix Syslog Alert Tool** window and the **Acknowledge Alert(s)** window automatically appear. The most current alert is highlighted in the **SecureLogix Syslog Alert Tool** window.



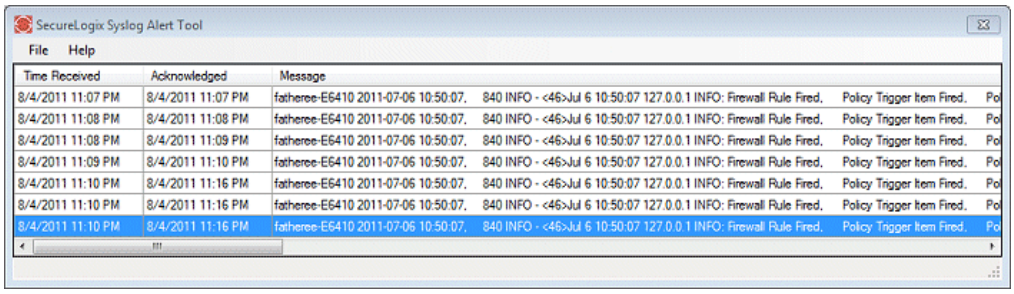
Acknowledging Alerts

To acknowledge alerts

1. When an alert is received, review the alert information in the **Acknowledge Alert(s)** window.
2. After completing actions in accordance with your company policy regarding alerts, click the **Acknowledge** button to close the Acknowledge Alert(s) window.
   - If more than 1 (one) alert has occurred, click the **Next** button in the **Acknowledge Alert(s)** window to view each alerts. When all alerts have been viewed, the **Acknowledge** button becomes available to click and close the window.



3. After acknowledging alert(s), the **SecureLogix Syslog Alert Tool** window remains displayed so that you can review all acknowledged alerts received so far for the current user session. Drag the scroll bar at the bottom of the window to view **Message** details.



Drag the scroll bar to view **Message** details.

LOCK the workstation instead of logging off

NOTE: Alerts listed in the **SecureLogix Syslog Alert Tool** window are cleared when you log out and end the user session; however, they are retained if you **Lock** your computer. See "Locking a Workstation to Retain Alert List" on page 27.

Closing the Syslog Alert Tool Window

After all alerts have been acknowledged, the **SecureLogix Syslog Alert Tool** window is designed to remain displayed in front of all other programs with the most current alert highlighted; however, this window can be closed to the system tray. Closing the window does not stop the program; the tool continues to run as a background process and when a new alert is received both the **SecureLogix Syslog Alert Tool** window and **Acknowledge Alert(s)** window will again be displayed.

To close the SecureLogix Syslog Alert Tool window

- Click the **X** button, or
- Click **File | Close**.

Displaying Acknowledged Alerts

If the **SecureLogix Syslog Alert Tool** window has been closed, you can re-open the window to view acknowledged alerts for the current user session that have not been cleared. See “Clearing Acknowledged Alerts” on page 26. Contact your System Administrator if you need access to cleared alerts and alerts for previous days. (See "Syslog Alert Log Files” on page 28.

To display previously acknowledged alerts that have not been cleared

1. Right click the **Syslog Alert Tool** icon in the system tray.
2. Select **Show Syslog Alerts Tool**. The **SecureLogix Syslog Alert Tool** window appears showing all alerts previously acknowledged for the current user session.

Clearing Acknowledged Alerts

You can clear all acknowledged alerts from the **SecureLogix Syslog Alert Tool** window at any time so that the only alerts displayed will be unacknowledged alerts. Clearing alerts only removes the alert listings from the window; all alerts are written to an alert log file.

NOTE: Only users with system administrator privileges can view cleared alerts. See “Syslog Alert Log Files” on page 28.

To clear acknowledged alerts

1. In the **SecureLogix Syslog Alert Tool** window, click **File | Clear Acknowledged Alerts**.
2. Click **OK**. All previously acknowledged alerts are permanently removed from the window.

Locking a Workstation to Retain Alert List

When a workstation user logs out and ends the user session, alerts are automatically cleared from the **SecureLogix Syslog Alert Tool** window. (Alerts *are* separately written to a syslog alert log file. See "Syslog Alert Log Files" on page 28.)

If you want to retain the list of alerts when you need to secure your workstation, use the computer's **Lock** feature.

To Lock a Windows XP computer

1. Press **Ctrl+Alt+Del** to display **Windows Security**.
2. Click the **Lock Workstation** button. The workstation is secured.

To Lock a Window 7 computer

1. Click the Windows **Start** menu.
2. Click the right arrow located to the right of "Shut down" to display the shutdown menu.
3. Select **Lock**. The workstation is secured.

Syslog Alert Log Files

Overview

In addition to visual and audible notification of syslog alerts received from the ETM System, the SecureLogix Syslog Alert Tool saves syslog alert information to the **alertsLog.txt** file.

A new alertsLog.txt file is generated for each 24-hour period. At midnight, the filename is appended with the date (alertsLog.txtYYYYMMDD), and a new alertsLog.txt file is created for the current day.

Log files are retained indefinitely unless manually purged.

Accessing Alert Log Files

Only users with access to the Syslog Alert Tool directory have access to the saved log files.

To view the current day's alert log files

Today's Alert Log File

1. Navigate to the Syslog Alert Tool directory. For example, C:\Program Files\SecureLogix\Syslog Alert Tool
2. Using a text editor, open the file: **alertsLog.txt**

To view a previous day's alert log files

Previous Day's Alert Log File

1. Navigate to the Syslog Alert Tool directory. For example, C:\Program Files\SecureLogix\Syslog Alert Tool
2. Locate the date for which you want to view the log files. For example, alert log files for August 1, 2011 will be saved to the log file: alertsLog.txt20110801
3. Using a text editor, open the file of interest.

Glossary

ETM Server - The background processing engine that controls all access to and aspects of the ETM System. You log in to the ETM Server via the ETM System Console. The Server receives data from the Appliances, pushes configuration and Policies to them, generates Track messages, and controls access to the system.

Syslog Server – An ETM Syslog server receives alerts generated in response to specific system events or firing of Policy rules. Generated alerts are sent from the ETM Server to all configured ETM Syslog Servers.

Syslog Alert Tool – A SecureLogix software program that provides visual and audible alerts for system events and policy alerts received from an ETM Syslog Server. The software resides on a user's workstation and automatically starts when the user logs in.

Syslog Alerts – The ETM Server sends system events and policy alerts, such as 911 calls, to the ETM Syslog Server. When the SecureLogix Syslog Alert Tool is installed and running, it receives and displays the events and alerts from the ETM Syslog Server and are referred to as Syslog Alerts.

Index