



perfecting the art of network security

SECUREWATCH™ RELEASE NOTES

Software Version: SecureWatch Version 2.22

Part Number: 990-0146-00

Date: June 2002

Top Layer Networks, Inc.
2400 Computer Drive
Westboro, MA 01581

Top Layer Networks™, Inc. reserves the right to revise this documentation and to make changes in content from time to time without obligation on the part of Top Layer to provide notification of such revision or change. Top Layer provides this documentation without warranty, term, or condition of any kind, either implied or expressed, including, but not limited to, the implied warranties, terms or conditions of merchantability, satisfactory quality, and fitness for a particular purpose. Top Layer may make improvements or changes in the product(s) and/or the program(s) described in this documentation at any time.

If there is any software on removable media described in this documentation, it is furnished under a license agreement included with the product as a separate document, in the printed documentation, or on the removable media. If you are unable to locate a copy, please contact Top Layer.

If you are a United States government agency, this documentation and the software described herein are provided to you subject to the following:

All technical data and computer software are commercial in nature and developed solely at private expense. Software is delivered as "Commercial Computer software" as defined in DFARS 252.227-7014 (June 1995) or as a "commercial item" as defined in FAR 2.101(a) and as such is provided with only such rights as are provided in Top Layer's standard commercial license for the software. Technical data is provided with limited rights only as provided in DFAR 252.227-7015 (November 1995) or FAR 52.227-14 (June 1987), whichever is applicable. You agree not to remove or deface any portion of any legend provided on any licensed program or documentation contained in, or delivered to you in conjunction with, this document.

Adaptive Security, AppBalancing, AppSafe, AppWizard, Attack Mitigator, DCFD, Flow Mirror, IDS Balancer, perfecting the art of network security, Queue Manager, Relay Engine, Secure Balance, Secure Edge Controller, Secure QoS, SecureWatch, Top Layer, and Top Layer Networks are trademarks of Top Layer.

AppSwitch, TopFire, TopFlow, TopPath, and TopView are registered trademarks of Top Layer. Unless otherwise indicated, Top Layer trademarks are registered in the U.S. Patent and Trademark Office.

All other company and product names may be trademarks of the respective companies with which they are associated.

No part of this documentation may be reproduced in any form or by any means or used to make any derivative work (such as translation, transformation, or adaptation) without written permission from Top Layer.



perfecting the art of network security

CONTENTS

ABOUT THIS DOCUMENT

Related Documentation	6
Documentation Description	7
Customer Support	8
Customer Support Phone Number	8
Product Returns	8

RELEASE NOTE INFORMATION

Overview	9
Changes and Enhancements	10
Known Problems	14
Product Versions	15
Installation and Setup	16
Technical Tips	18

CONFIGURE CHECK POINT ELA NG

Integrate the SecureWatch Product with Check Point ELA NG	19
(Optional) Install the Check Point Strong Security DLL	20
Configure ELA Authentication Type	20
Authentication Configuration Steps	21
Verify SecureWatch Output with the ELA Agent	24



perfecting the art of network security

ABOUT THIS DOCUMENT

This document is intended for use by the person who needs information on known problems, bug fixes, technical tips, installation, and support information for the Top Layer SecureWatch™ data gathering and analysis software.



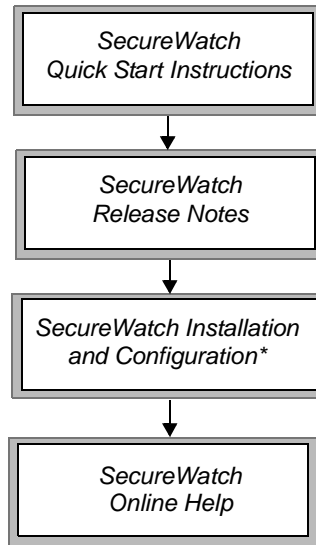
This document contains information that pertains to the Top Layer AppSafe™ and AppSwitch™ system units. Throughout this document, a Top Layer AppSafe or AppSwitch system unit is referred to as a Top Layer system unit or a system unit.



The information contained in this section is correct at the time of publication.

**Related
Documentation**

The following diagram and table present the SecureWatch technical documentation set.



* Available as a PDF file accessible from the online help

Documentation Description

The following table provides a description of the SecureWatch documentation:

Name of Document	Description
<i>SecureWatch Quick Start Instructions</i>	Provides instructions for installing the SecureWatch software and its license key.
<i>SecureWatch Release Notes</i>	Information on new features, known problems, bug fixes, documentation updates, technical tips, installation tips, and Top Layer Support access.
<i>SecureWatch Installation and Configuration</i>	Software installation steps and configuration information for: <ul style="list-style-type: none"> • SecWatch Windows service • Program security features • SecureWatch application • TopFlow Protocol on the system unit • Control and Monitoring functions • PerfMon monitors and the Check Point™ ELA Proxy
<i>SecureWatch Online Help</i>	Online information for the windows of the Web Management Interface, plus conceptual and troubleshooting information. Online help is accessible from individual windows and, as a more inclusive tool, from the Help buttons on the various Web Management Interface navigation trees.

Customer Support

Top Layer offers online technical resources through its World Wide Web site. Use the following URL:

For	URL
Product Information	http://www.TopLayer.com
Customer Support	http://www.TopLayer.com/support

To report a problem, enter a WISE support incident from the Top Layer World Wide Web site.

**Customer Support
Phone Number**

If you are unable to obtain assistance from Top Layer’s online technical resources at the above URLs or from your network supplier, Top Layer offers technical telephone support services. When you contact Customer Support for assistance, have the following information ready:

- Top Layer system unit name, model number, and serial number
- List of system hardware and software, including revision levels
- Details about recent configuration changes, if applicable

To contact Top Layer Customer Support, use the following phone number:

+1-508-870-1300 and Press 1 for support

Product Returns

Before you send a product directly to Top Layer for repair, you must first obtain a Return Material Authorization (RMA) number. Any product sent to Top Layer without an RMA cannot be accepted. Use the following return information to obtain the RMA and ship your product:

Support Phone Number for RMA	Product Return Address
+1-508-870-1300 and Press 1 for support	USA Top Layer Networks, Inc. 2400 Computer Drive Westboro, MA 01581



perfecting the art of network security

RELEASE NOTE INFORMATION

Overview

Please read this document in its entirety. It contains important information about:

- Oracle database support
- Enhancements to database profiles enabling better control of the type of information collected and the data's intended use
- Support for Top Layer system unit-initiated connections
- Audit trail for SecureWatch application configuration changes
- Improved Event Log Viewer operation
- SSL support for the Web-based administrative interface
- Extensive query interface "Analysis Package" for viewing data collected from system units
- Improved administrative interface
- Comprehensive user group access management
- Support for system unit Syslog output
- New tags for Syslog format definitions
- Description of new online help documentation suite
- Problem fixes
- Documentation covering the differences between AppSafe and AppSwitch system unit attack mitigation descriptions and the actual messages the units send to the SecureWatch system
- Support for the Check Point™ VPN-1/FireWall-1® Next Generation (NG) ELA (Version 5.0)
- Support for SSL or Encrypted SSL with Check Point ELA

Please visit Top Layer Network, Inc.'s Web site for support and information about Top Layer products at <http://www.TopLayer.com>. Top Layer frequently updates this site with FAQ sheets, detailed upgrade and configuration hints, and other useful product information.

Changes and Enhancements

This version of the SecureWatch software provides the following additions and enhancements:

- **Support for the Check Point VPN-1/FireWall-1 Next Generation (NG) ELA (Version 5.0)** — The addendum "Configure Check Point ELA NG" on page 19 describes how you configure authentication for the SecureWatch product and the Check Point ELA Server.

Note: The following table lists the location of related Check Point ELA configuration information:

Check Point ELA Proxy	Refer to
Version 4.1	"Appendix B, Configure Check Point ELA Proxy" in the <i>SecureWatch Installation and Configuration</i> guide
Version 5.0 (NG)	"Configure Check Point ELA NG" on page 19

- **Support for SSL or Encrypted SSL with Check Point ELA** — To use SSL or Encrypted SSL with the Check Point ELA, Versions 4.1 or 5.0 (NG) you must install the Check Point strong security DLL on the SecureWatch collector. The DLL which supports SSL and Encrypted SSL is named `opsec.dll`, which is the same name as the standard (non-secure) DLL.

Note: Contact Top Layer Customer Support for information about how you can obtain the DLL.

To install the DLL, complete the following steps:

- 1 On the SecureWatch collector, move or rename the file **Program Files\SecWatch\opsec.dll**.
- 2 Copy the new DLL into the directory **Program Files\SecWatch**

- **Supported Database Agents** — The SecureWatch product has a reporting agent available for:
 - Oracle 7 or later
 - Microsoft SQL

Note: DATABASE SERVER AVAILABILITY — The SecureWatch reporting agents that support the Oracle Database Server and the Microsoft SQL Server products are not available in all markets. Contact your local Top Layer Sales Representative for availability information.

Note: DATABASE SERVER SUPPORT — You are solely responsible for the selection, sizing, configuration, tuning and maintenance of the database server connected to the SecureWatch server. Top Layer will not provide any support for these activities.

- **Data Collection and Usage Enhancements** — When you configure a database profile, you can:
 - Select the type of data that should be gathered: network traffic, security, system unit Syslog messages, or a combination of these items.
 - Select the usage allowed for the data being collected: collection, analysis only, or both. The *analysis only* setting enables you to treat a database as an archive to be referenced; using this setting, new data is not added.
- **System Unit Initiated Report Producers** — In addition to SecureWatch initiated report producers, you can now define connections to your SecureWatch application that are initiated directly by system units. You can configure the system units to try different SecureWatch collectors if a specific collector does not respond or stops responding. You can configure the system unit to use SSL encryption for the connections that it initiates.
- **Configuration Audit Trail** — The Web-based administrative interface includes a configuration log file that details all SecureWatch application configuration changes made from the interface.
- **Improved Event Log Viewer** — The Event Log Viewer includes better display controls including an End button that displays the entries at the end of the file.

- **SSL support for the SecureWatch Management Web Interface** — From the SecWatch service applet, you can set up SSL encrypted access to the SecureWatch Management Web Interface. The feature supports self-generated or your existing SSL certificates.
- **Analysis Module** — The Web-based interface includes an Analysis module that provides:
 - Sets of predefined database queries providing both table and graph displays
 - Search parameters used to refine certain queries
 - Histograms
 - Library of standard queries you can copy and modify
 - Personal and shared query libraries
 - Access to the tables of stored data in both translated and raw formats
 - Query creation windows with execute and save features
 - An Entity Relationship diagram helpful for creating your own queries
- **Improved Administrative Interface** — The SecureWatch Web-based administrative graphical user interface is enhanced as follows:
 - All tables can now be easily sorted by clicking the arrow icons at the top of each table column.
 - Enable and disable most objects directly from their summary windows.
 - Monitor and configuration tasks have separate navigation trees, accessed by buttons at the top of the SecureWatch window.
 - Standard and Advanced user settings enable standard users to be assigned simplified configuration windows.
 - Improved messages, visual feedback, and selection controls.
 - Database initialization, testing, and deletion directly from individual database profile windows.
- **Support for System Unit Syslog Output** — SecureWatch can accept Syslog input from a system unit that is capable of including its Syslog output with its other TopFlow protocol reports. The Syslog output will become available as Top Layer system units are developed that support this enhanced TopFlow protocol. This support enables better

report input control to reporting tools such as the Check Point's ELA client.

- **New Tags for Syslog Format Definitions** — New tags include:
 - SPN (Server Port Number)
 - CPN (Client Port Number)
 - ACT (Action: Accept, Drop, Reject; based on policy settings)
 - IPT (IP Protocol Type)
- **Web GUI Online Help Expanded** — In addition to context help for each window, you can access a complete help system including overview, configuration, and troubleshooting information. You can also access the *SecureWatch Installation and Configuration* guide as a PDF file directly from the management GUI's navigation trees.

Known Problems

The following are known problems:

- Syslog and ELA Agents Report Packets Dropped while System Unit is Running in Monitor Mode** — If you configure your Top Layer system unit for attack mitigation, and set the system unit to *Monitor* mode, the system unit reports attacks, but does not actually drop the offending packets. However, SecureWatch reports the packets as being dropped. There is no current work around for this incorrect reporting.
- Messages for Some Attack Filters Do Not Match Their Names** — Some of the AppSafe and AppSwitch system unit security filter names do not match the messages that the system units send to the SecureWatch product when there is a security violation, and for some types of attack, the system units do not send messages to the SecureWatch product. The following table lists those filters that the system units report under a different attack name or do not report at all (even though the system units **do** stop the named attacks):

Attack Filter Name	Actual Message
FTP restricted Port Filter	Ftp Port
FTP Bounce Filter	attack blocked, but no message sent
UDP Bomb Filter	attack blocked, but no message sent
IP Source Address Restrictions	attack blocked, but no message sent
IP Source Route Filter	IP Options Restriction Violation
IP Options Filter	IP Options Restriction Violation
Syn Flood Mitigation	Syn Flood
Boink	Overlaid Transport Header
Too Many Frags	attack blocked, but no message sent

Note: For a complete listing of filters and messages, see Configure Security Filters in Chapter 2 of the *SecureWatch Installation and Configuration* guide.

Product Versions

The SecureWatch product is available in different forms depending on the features you license. Also available are both a free version and an evaluation version. The following table describes the different software versions:

Version	Description
Standard	<p>Available to all Top Layer system unit owners. It has the following limitations:</p> <ul style="list-style-type: none"> • Limits the number of producers to four. Each producer accepts reports from one system unit. • Provides a limited set of reporting agents. • The user can convert this version to the Professional version by purchasing and installing a license key.
Evaluation	<p>Contains the following limitation:</p> <ul style="list-style-type: none"> • Enforces a 30 day evaluation period. <p>The user can convert this version to the Professional version by purchasing and installing a license key.</p>
Professional	<p>The type of license key you purchase determines:</p> <ul style="list-style-type: none"> • Agent types available • Installation IP addresses available <p>Note: The professional version allows an unlimited operational time period and unlimited number of producers that you can configure.</p> <p>You can upgrade a Professional license to include additional agents, as needed, by purchasing and installing a different license key.</p>
Product-specific Versions of the SecureWatch Software	<p>Some Top Layer hardware products may include a version of SecureWatch with features different from the combinations described above. You can upgrade these versions to SecureWatch Professional by buying a new license key.</p>

Installation and Setup

Use the following technical tips to help you during product installation and setup:

- **Restart SecureWatch Related Services** — When you install the SecureWatch product, you must restart any SecureWatch-related services, such as an ELA or database client, before you start the SecWatch service.
- **Administrative Identifier for the SecureWatch Producer** — The user ID you set between the AppSwitch or AppSafe system unit and the Producer in your SecureWatch application depends on the type of connection you are creating:
 - For a SecureWatch initiated producer, the ID must be *siteadmin*.
 - For a system unit initiated connection to a producer, the ID must be *monitor*.

However, for security purposes, you can, and should, change the user password for the login.

- **ELA Agent/ELA Proxy: Match Authentication Types** — Make sure to use the same authentication type for both the Check Point ELA Proxy and the SecureWatch ELA Agent (for example, Clear Text to Clear Text).

Clear text is the easiest authentication method to start with. Be sure SecureWatch is operating properly using Clear Text authentication before moving to the other, more secure and more complex authentication types. This version of the documentation provides complete instructions for configuring each form of authentication.

- **TCP Port Number 18187 for ELA Agent**—Make sure to use the same TCP port number for the ELA Proxy and the ELA Agent. The default TCP port number is 18187 and does not need to be changed.
- **Port 2885 Must be Available for SecureWatch Report Processing**—The SecureWatch product uses port 2885 for TopFlow Protocol Report TCP communication between the SecureWatch Producer and the AppSafe or AppSwitch system unit. When you deploy the SecureWatch product in a firewall environment, you must ensure that this port is available for SecureWatch report traffic.

- **Syslog Default UDP Port 514** — When you define a Syslog Agent, if you also define a Syslog host, the port you define for the host must match the port used by the Syslog daemon. The default port number is 514.
- **Not Necessary to Restart the SecWatch Service after Making SecureWatch Application Configuration Changes** — After reconfiguring parameters within the SecureWatch Management Web Interface, there is no need to restart the **SecWatch service**. Make your configuration changes, click the **Apply** button, and then start and stop or restart SecureWatch report processing from the Web interface.
- **Administrator Account Security** — Make sure that you change the password for the administrator using the provided SecureWatch service.
- **Autostarting the SecureWatch Data Collection Service** — Top Layer recommends that you do not enable the SecureWatch autostart feature on the Administrative Interface of the SecureWatch Professional product until you are certain that the configuration is properly configured and working. When the firewalls and the SecureWatch collectors are erroneously configured with different authentication modes, the Check Point ELA service on the SecureWatch collectors will stop and you will be unable to manage the collectors.

To regain the ability to manage the SecureWatch collectors, you must edit the Windows Registry to disable autostart. To change the registry, complete the following steps:

- 1 Open a command window and type **regedit**. The Registry Editor window displays.
 - 2 Open **HKEY_LOCAL_MACHINE\SOFTWARE\TopLayer\SecWatch\Default**. Right-click **autostart** and select **Modify**.
 - 3 Change the **Value data** text-box to **0**.
 - 4 Select **Registry --> Exit** to exit the Registry Editor.
- **Using SSL or Encrypted SSL with the Check Point ELA Proxy** — To use SSL or Encrypted SSL with the Check Point ELA Proxy, you must install the Check Point strong security DLL on the SecureWatch collector. The installation procedure is described in "(Optional) Install the Check Point Strong Security DLL" on page 20. Contact Top Layer Customer Service for more information about obtaining the proper DLL.

Technical Tips

General Operational Tips:

OPSEC ELA Proxy/ELA Agent Related Tips:

- **Throttle Default Value, Do Not Change Without Consulting Top Layer** — When you set up the ELA Agent, do not change the default value of Throttle unless you have consulted with Top Layer Professional Services. Sending too many reports to the ELA Proxy could overwhelm the Proxy. This is most likely to happen during a DDOS attack. The default value of Throttle protects the ELA Proxy from being overwhelmed.
- **Auto Reconnect to the ELA Proxy** — You can configure the SecureWatch program to attempt to reconnect to the ELA Proxy if the connection is lost.
- **OPSEC Version Information and Connection messages Available** — The Statistics Summary window now displays OPSEC version information if the ELA Agent is connected to the ELA Proxy. If the Agent is not connected to the ELA Proxy, a connection-related message displays.

Configure Check Point ELA NG

This addendum is a supplement to the SecureWatch Installation and Configuration guide and provides instructions for configuring the Version 5.0 Next Generation (NG) Check Point ELA for operation with the SecureWatch product.

NOTE: Appendix B, Configure Check Point ELA Proxy, of the *SecureWatch Installation and Configuration* guide provides instructions for configuring the Version 4.1 Check Point ELA Proxy for operation with the SecureWatch product.

Integrate the SecureWatch Product with Check Point ELA NG

There is no ELA proxy for Check Point ELA NG. The SecureWatch ELA Agent sends reports directly to the firewall which either connects to a management station or writes the files locally.

The steps to integrate the SecureWatch ELA Agent (Client), with Check Point™ VPN-1/FireWall-1® and the ELA Server include:

- Install VPN-1/FireWall-1 as described in the *Check Point Management Guide*. The VPN-1/FireWall-1 installation procedure installs the ELA Server.
- Enable ELA reporting in the SecureWatch Administrative Interface.
- Set up the form of authentication that the SecureWatch Agent uses when connecting to the ELA Server. The remainder of this addendum provides details for setting up authentication.

NOTES: The SecureWatch product uses TCP port 2885 for TopFlow Report Protocol communication between the SecureWatch Producer and the Top Layer system unit. It uses port 3885 for SSL communication. When you deploy the SecureWatch product in a firewall environment, you must ensure that this port (whichever one you use) is available for SecureWatch report traffic.

To use the Check Point ELA, you must also set up a local subnet address on the Top Layer system unit. Refer to the *SecureWatch Installation and Configuration* guide.

(Optional) Install the Check Point Strong Security DLL

To use SSL or Encrypted SSL with the Check Point ELA Server, you must install the Check Point strong security DLL on the SecureWatch collector. The DLL which supports SSL and Encrypted SSL is named `opsec.dll`, which is the same name as the standard (non-secure) DLL.

NOTE: Contact Top Layer Customer Support for information about how you can obtain the DLL.

To install the DLL, complete the following steps:

Step	Action
1	(Optional) On the SecureWatch collector, move or rename the file Program Files\SecWatch\opsec.dll .
2	Copy the new DLL into the directory Program Files\SecWatch

Configure ELA Authentication Type

You can establish one of four types of authentication to take place between the SecureWatch ELA Agent and the Check Point ELA Server:

- **Clear Text** — Authentication uses data that is not restricted or encrypted in any way.
- **Check Point Proprietary** — Authentication data uses Check Point's proprietary algorithm.
- **Secure Socket Layer (SSL)** — Uses a SSL certificate key to validate data transfer.
- **Encrypted SSL** — Uses a SSL certificate key to validate the data transfer and to decrypt the data. This is the most secure form of authentication and data transfer provided.

NOTE: SSL or Encrypted SSL authentication types require an encryption-capable version of VPN-1/Firewall-1. Selecting "SSL" authentication means that SecureWatch authentication with Firewall-1 occurs using Secure Socket Layer (SSL). SSL is supported by VPN-1/FireWall-1 beginning with version 4.1 SP2. Selecting "Encrypted SSL" authentication within SecureWatch means that both authentication and data transfer are encrypted using a 3DES key. The Encrypted SSL connection is supported by VPN-1/FireWall-1 beginning with version 4.1.

You must set authentication in two places:

- Within the Check Point ELA configuration file (steps provided below).
- Within the SecureWatch administrative GUI when you configure the SecureWatch ELA Agent (refer to the online help for the ELA Agent window).

These two authentication type settings **must match**.

NOTE: Clear Text is the easiest form of authentication to set up. We recommend that you start with this form of authentication, confirm proper SecureWatch operation, then modify your configuration to the form of authentication you will use. To verify that the ELA Agent and ELA Server are working together properly, check for the **remote SDK version message** on the Statistics Summary window. Select the online help for the Statistics Summary window.

You do not need to stop the SecWatch service to make changes to the Check Point firewall service configuration file. Also, you do not need to stop the firewall service to make changes to the SecureWatch configuration.

Authentication Configuration Steps

NOTE: On the SecureWatch collector, the OPSECDIR system variable indicates where SecureWatch opsec keys and related programs reside. Encryption requires that the OPSECDIR variable is defined as the directory path where the opsec keys and related programs reside (**C:\Program Files\SecWatch**). To ensure that the OPSECDIR variable is defined and set to the correct value, log on to an administrator's account, right-click **My Computer**, select **Properties**, then click the **Advanced** button, and examine the **Environment** settings. Determine if the OPSECDIR variable is defined correctly. If the variable is not defined correctly, enter **OPSECDIR** in the **Variable** text-box, the directory path where the opsec keys and related programs reside in the **Value** text-box, then click the **Set** button.

Establish the authentication type used by the ELA by modifying the Check Point configuration file. On the server that is running the Check Point firewall service, perform the following steps:

Step	Action
1	Stop the firewall service, if it is running: On the taskbar of the machine running the firewall service: Click Start , select Run , and enter cpstop

Step	Action
------	--------

- 2 Open **Wordpad** and click **File --> Open**
- 3 For *Types of Files*, select **All Documents**
- 4 Double-click the **My Computer** icon and locate the **fwopsec.conf** file in either **Winnt\FW1\5.0\conf** or **Winnt\FW1\Ng\conf** depending on your configuration.
- 5 Click **Open**. The configuration file displays. Example file:

```
# sam_server auth_port 18183
# sam_server port 0
#
# lea_server auth_port 18184
# lea_server port 0
#
ela_server auth_port 18187
ela_server auth_type auth_opsec

# ela_server port 0
#
# cpmi_server auth_port 18190
#
# uaa_server auth_port 19191
# uaa_server port 0
```

- 6 Edit the lines indicating the authentication type to **match one of the four types** as follows:

Clear Text:

```
ela_server auth_port 0
ela_server port 18187
```

Check Point Proprietary:

```
ela_server auth_port 18187
ela_server auth_type auth_opsec
```

Secure Socket Layer (SSL):

```
ela_server auth_port 18187
ela_server auth_type ssl_clear_opsec
```

Encrypted SSL:

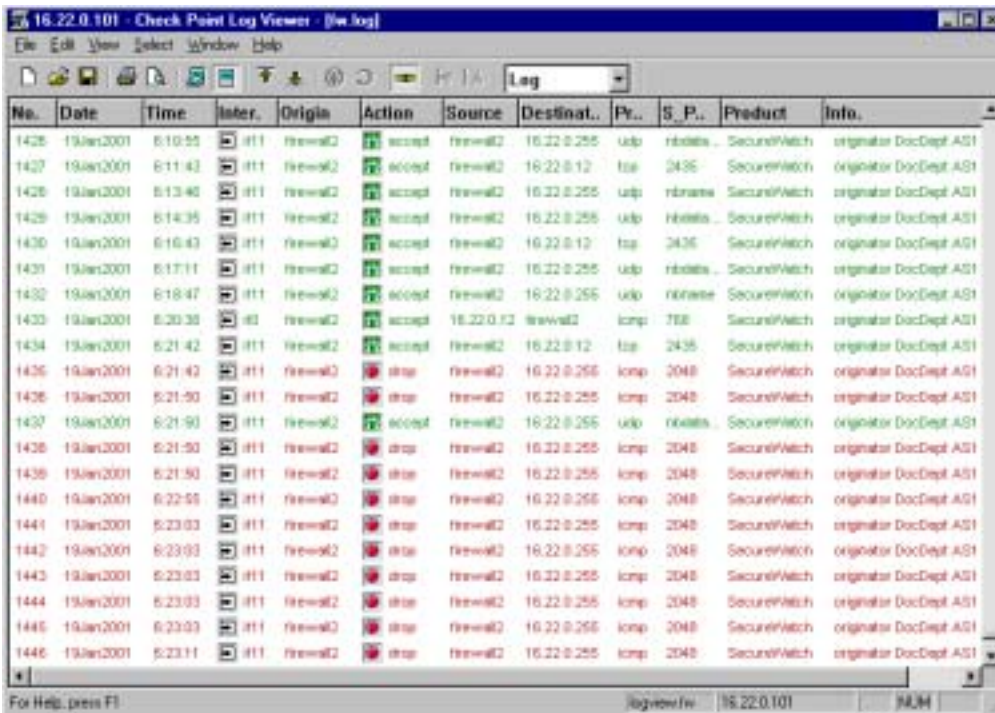
```
ela_server auth_port 18187
ela_server auth_type ssl_opsec
```

Step	Action
7	Click File --> Save to save the file with its .conf extension.
8	<p>For all authentication forms, except Clear Text, you must use the "<i>putkey</i>" program on the ELA Agent and the ELA Server to establish an encrypted user key.</p> <p>On the server that runs the Check Point firewall service, run one of the following commands:</p> <p>For Check Point Proprietary authentication: On the taskbar, click Start and select Run. Enter: <i>path</i>¹ fw putkey -opsec SecureWatchServerName Example: fw putkey -opsec Hobbs</p> <p>For Secure Socket Layer (SLL) and Encrypted SLL authentication: On the taskbar, click Start and select Run. Enter: <i>path</i> putkey -ssl SecureWatchServerName Example: fw putkey -ssl Hobbs</p>
9	<p>Restart the firewall service:</p> <p>On the taskbar, click Start, select Run, and enter cpstart</p>
10	<p>On the server that runs the SecWatch service run one of the following commands:</p> <p>For Check Point Proprietary authentication: On the taskbar, click Start and select Run. Enter: <i>path</i>² opsec_putkey ELAServerName Example: opsec_putkey Calvin</p> <p>For Secure Socket Layer (SLL) and Encrypted SSL authentication: On the taskbar, click Start and select Run. Enter: <i>path</i> opsec_putkey -ssl ELAServerName Example: opsec_putkey -ssl Calvin</p>
11	Configure the SecureWatch ELA Agent to the same authentication type that you set for the ELA Server. Refer to "Configure SecureWatch Report Processing and Global Settings" in the <i>SecureWatch Installation and Configuration</i> guide and to the online help for the ELA Agent window.

1. Where *path* is the path to the fw program in the bin directory of the Firewall-1 installation.
2. Where *path* is the path to the opsec_putkey program in the SecureWatch home directory.

Verify SecureWatch Output with the ELA Agent

To verify the SecureWatch output, examine the items in the viewer that SecureWatch is supplying reports to. In the following situation, a Smurf attack was launched (the person configuring the system unit had enabled the Smurf filter; refer to your Top Layer system unit documentation). The SecureWatch program sent the attack reports to the Check Point Log Viewer. The Check Point ELA Proxy is configured to show SecureWatch security-related reports in red. The **Product** column shows that SecureWatch generated the reports. The **Info** column shows the system unit that originated the security violation reports.



The screenshot shows the Check Point Log Viewer interface with a table of log entries. The table has columns: No., Date, Time, Inter., Origin, Action, Source, Destin., Pr., S. P., Product, and Info. The entries from 1425 to 1446 are highlighted in red, indicating security-related reports. The 'Product' column for these entries is 'SecureWatch' and the 'Info' column is 'originator DocDept AS1'. The 'Action' column shows 'accept' for entries 1425-1433 and 'drop' for entries 1434-1446. The 'Pr.' column shows 'udp' for entries 1425-1433 and 'icmp' for entries 1434-1446. The 'S. P.' column shows '2435' for entries 1425-1433 and '2048' for entries 1434-1446.

No.	Date	Time	Inter.	Origin	Action	Source	Destin.	Pr.	S. P.	Product	Info.
1425	19-Jan-2001	8:19:55	eth1	firewall2	accept	firewall2	16.22.0.255	udp	nbdata	SecureWatch	originator DocDept AS1
1427	19-Jan-2001	8:11:43	eth1	firewall2	accept	firewall2	16.22.0.12	tcp	2435	SecureWatch	originator DocDept AS1
1428	19-Jan-2001	8:13:40	eth1	firewall2	accept	firewall2	16.22.0.255	udp	nbname	SecureWatch	originator DocDept AS1
1429	19-Jan-2001	8:14:35	eth1	firewall2	accept	firewall2	16.22.0.255	udp	nbdata	SecureWatch	originator DocDept AS1
1430	19-Jan-2001	8:16:43	eth1	firewall2	accept	firewall2	16.22.0.12	tcp	2435	SecureWatch	originator DocDept AS1
1431	19-Jan-2001	8:17:11	eth1	firewall2	accept	firewall2	16.22.0.255	udp	nbdata	SecureWatch	originator DocDept AS1
1432	19-Jan-2001	8:18:47	eth1	firewall2	accept	firewall2	16.22.0.255	udp	nbname	SecureWatch	originator DocDept AS1
1433	19-Jan-2001	8:20:38	eth1	firewall2	accept	16.22.0.12	firewall2	icmp	788	SecureWatch	originator DocDept AS1
1434	19-Jan-2001	8:21:42	eth1	firewall2	accept	firewall2	16.22.0.12	tcp	2435	SecureWatch	originator DocDept AS1
1435	19-Jan-2001	8:21:43	eth1	firewall2	drop	firewall2	16.22.0.255	icmp	2048	SecureWatch	originator DocDept AS1
1436	19-Jan-2001	8:21:50	eth1	firewall2	drop	firewall2	16.22.0.255	icmp	2048	SecureWatch	originator DocDept AS1
1437	19-Jan-2001	8:21:50	eth1	firewall2	accept	firewall2	16.22.0.255	udp	nbdata	SecureWatch	originator DocDept AS1
1438	19-Jan-2001	8:21:50	eth1	firewall2	drop	firewall2	16.22.0.255	icmp	2048	SecureWatch	originator DocDept AS1
1439	19-Jan-2001	8:21:50	eth1	firewall2	drop	firewall2	16.22.0.255	icmp	2048	SecureWatch	originator DocDept AS1
1440	19-Jan-2001	8:22:55	eth1	firewall2	drop	firewall2	16.22.0.255	icmp	2048	SecureWatch	originator DocDept AS1
1441	19-Jan-2001	8:23:03	eth1	firewall2	drop	firewall2	16.22.0.255	icmp	2048	SecureWatch	originator DocDept AS1
1442	19-Jan-2001	8:23:03	eth1	firewall2	drop	firewall2	16.22.0.255	icmp	2048	SecureWatch	originator DocDept AS1
1443	19-Jan-2001	8:23:03	eth1	firewall2	drop	firewall2	16.22.0.255	icmp	2048	SecureWatch	originator DocDept AS1
1444	19-Jan-2001	8:23:03	eth1	firewall2	drop	firewall2	16.22.0.255	icmp	2048	SecureWatch	originator DocDept AS1
1445	19-Jan-2001	8:23:03	eth1	firewall2	drop	firewall2	16.22.0.255	icmp	2048	SecureWatch	originator DocDept AS1
1446	19-Jan-2001	8:23:11	eth1	firewall2	drop	firewall2	16.22.0.255	icmp	2048	SecureWatch	originator DocDept AS1

Figure 1: Check Point Log Viewer Verifies Security Reports Sent from the ELA Agent