User Guide

Security Reporting Center

July 15, 2006

MARSHAL™

Contents

Chapter 5

Chapter 6

Chapter 7
Managing Proxy Report Content 125

Chapter 8
Managing User Access 139

Chapter 9

Managing Your Product Installation 149

Chapter 10

Managing Databases 158

Chapter 11

Using Reports 173

Chapter 12

Managing Data with Filters 189

About This Book and the Library

The User Guide provides conceptual information about the Security Reporting Center product (Security Reporting Center). This book defines terminology and various related concepts.

Intended Audience

This book provides information for firewall administrators and other individuals responsible for understanding Security Reporting Center concepts.

Other Information in the Library

The library provides the following information resources:

Evaluation Guide
Provides general information about the product and guides you through the trial and evaluation process.

Firewall Configuration Guide
Provides information about configuring your firewall to work with Marshal firewall security applications.

Help
Provides context-sensitive information and step-by-step guidance for common tasks, as well as definitions for each field on each window.

Conventions

The library uses consistent conventions to help you identify items throughout the documentation. The following table summarizes these conventions.

Convention	Use
Bold	• Window and menu items • Technical terms, when introduced
Italics	• Book and CD-ROM titles • Variable names and values • Emphasized words
`Fixed Font`	• File and folder names • Commands and code examples • Text you must type • Text (output) displayed in the command-line interface
Brackets, such as [*value*]	• Optional parameters of a command
Braces, such as {*value*}	• Required parameters of a command
Logical OR, such as *value1* | *value2*	• Exclusive parameters. Choose one parameter.

About Marshal

Marshal delivers a complete email and Web security solution to a variety of Internet risks. The Marshal solution provides comprehensive protection by acting as a gateway between an organization and the Internet. It allows organizations to restrict, block, copy, archive, and automatically manage the sending and receiving of messages.

Marshal Products

Marshal's Content Security solution, which includes MailMarshal SMTP, MailMarshal Exchange and WebMarshal, delivers a complete email and Web security solution to these risks by acting as a gateway between your organization and the Internet. The products sit behind your firewall but in front of your network systems to control outbound documents and their content. By providing anti-virus, anti-phishing and anti-spyware protection at the gateway, Marshal's Content Security solution offers you a strategic, flexible and scalable platform for policy-based filtering that protects your network, and as a result, your reputation.:

Contacting Marshal

Please contact us with your questions and comments. We look forward to hearing from you. For support around the world, please contact your local partner. For a complete list of our partners, please see our Web site. If you cannot contact your partner, please contact our Technical Support team.

Telephone:	+44 (0) 1256 848 080 (EMEA) +1 404 564-5800 (Americas) + 64 9 984 5700 (Asia-Pacific))
Sales Email:	info@marshal.com
Support:	www.marshal.com/support
Web Site:	www.marshal.com

Chapter 1

Introduction

This chapter provides an overview of Security Reporting Center's analytical and reporting capabilities. It describes how Security Reporting Center addresses common concerns in network security, tracking, and maintenance. Finally, it lists further resources for information about Security Reporting Center.

What is Security Reporting Center?

Security Reporting Center analyzes your firewall and proxy server logs and answers questions like the following:

- Who are the top Web surfers in the company, and what Web sites are they visiting?
- How many users inside the firewall are accessing Web sites with inappropriate content?
- How much network activity originates on each side of the firewall?
- Are we experiencing attempts to hack into our network? Where are they originating?
- Which departments or groups are using the largest amount of bandwidth?
- Which servers receive the most hits?
- How much bandwidth are we using, and how much does it cost? How much is consumed by each user, department, or protocol?

Security Reporting Center is a scalable, browser-based reporting framework that can be customized with add-on modules that provide specialized analysis and reporting tools. It can be deployed in a distributed environment using either Windows or Solaris computers, or a combination of both platforms. Thus it can be adapted to serve both relatively small operations and large enterprise networks such as managed service providers.

Security Reporting Center Modules

Security Reporting Center always includes two core modules: the Scheduler module, which configures and schedules reporting and analysis events, and the Administration module, which controls access rights to Security Reporting Center features for users and teams of users. Every Security Reporting Center installation also includes one or more add-on modules, which are specialized to perform analysis and reporting tasks for different types of data. Security Reporting Center currently offers the Firewall Reporting module and the Proxy Reporting module. You can install either or both depending on your reporting needs. The Firewall and Proxy Reporting modules can analyze log files generated by a variety of firewalls, proxy servers, and security devices. The *Firewall Configuration Guide* describes these devices and how to configure them for use with Security Reporting Center.

The Firewall Reporting module provides high-level reporting about the activity that crosses your firewall. It uses the data in your firewall, proxy server, or security device logs to report detailed statistics about the data sent and received by different users, teams and protocols, including assessments of bandwidth and how much it costs your business. It also lets you monitor security threats to your firewall, VPN usage, and server hits, offering you both short- and long-term pictures of network activity and security.

The Proxy Reporting module focuses on the Web traffic generated by users inside your firewall. Using the records in your firewall or proxy server log, the Proxy Reporting module provides detailed reports showing the sites internal users are visiting, the top surfers and departments in your company, the most popular sites visited, the times when Web surfing occurs most frequently, and many other important statistics about how employees use the World Wide Web.

Architecture

Security Reporting Center consists of the following core components, which can be installed on both Windows and Solaris platforms:

- One or more Database servers built on MySQL. Each Database server stores information about scheduling and configuration as well as report content.
- A User Interface server, which can be accessed from any computer with a Web browser.
- One or more Firewall Reporting agents. (One agent can be installed per computer.) Firewall Reporting agents do the work of log analysis and reporting to produce Firewall reports.
- One or more Proxy Reporting agents. (One agent can be installed per computer.) Proxy Reporting agents do the work of log analysis and reporting to produce Proxy reports.

The following components are optional. Choose whether to install them based on how you want Security Reporting Center to access your log files.

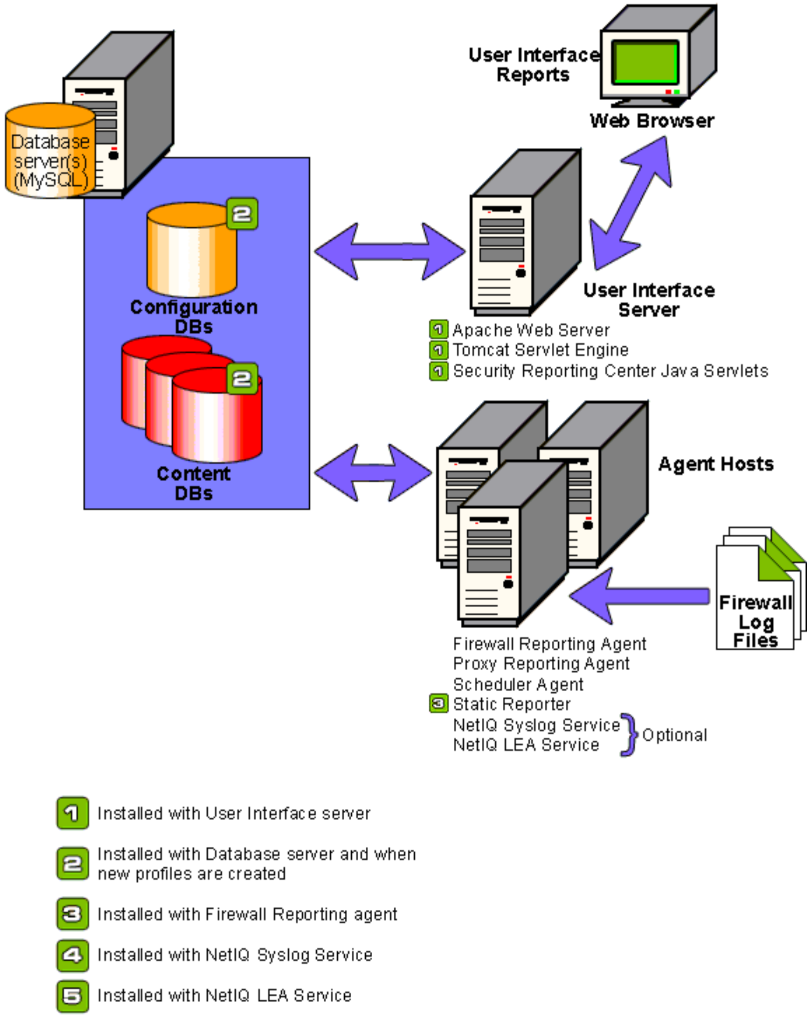
- The NetIQ LEA Service. Install this service if you use Check Point firewalls and want collect log information using OPSEC LEA.
- The NetIQ Syslog Service. Install this service if you want to collect log information using syslog.

For more information about these services, see "Installing Security Reporting Center" on page 7.

A Scheduler agent, which schedules events, communicates with the databases, and assigns tasks to the Reporting agent(s), is silently installed with each of these components.

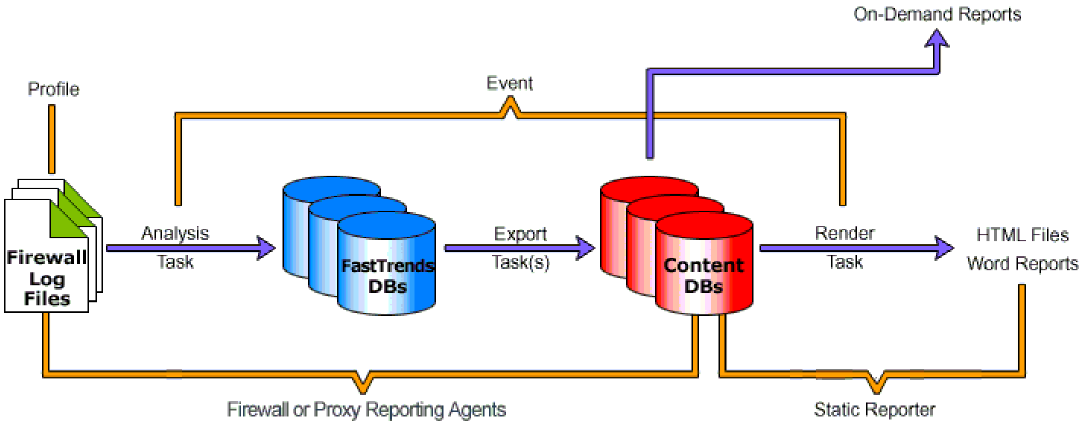
Deploying Security Reporting Center

The following diagram illustrates the Security Reporting Center architecture.


Database server(s) (MySQL)
2
Configuration DBs
2
Content DBs
User Interface Reports
Web Browser
User Interface Server
1 Apache Web Server
1 Tomcat Servlet Engine
1 Security Reporting Center Java Servlets
Agent Hosts
Firewall Log Files
Firewall Reporting Agent
Proxy Reporting Agent
Scheduler Agent
3 Static Reporter
NetIQ Syslog Service
NetIQ LEA Service
Optional
1 Installed with User Interface server
2 Installed with Database server and when new profiles are created
3 Installed with Firewall Reporting agent
4 Installed with NetIQ Syslog Service
5 Installed with NetIQ LEA Service

Report Generation

The following diagram illustrates how log files are analyzed and reports are generated:



Reporting Tasks

A Firewall or Proxy Reporting agent performs multiple *tasks*. During the first task, the analysis task, the Reporting agent analyzes the contents of one or more log files from a firewall, proxy server or security device, and stores the results in a FastTrends database. FastTrends is a patent-pending technology used to store compressed forms of log files to significantly speed subsequent analysis of the log files. For example, suppose Security Reporting Center analyzes the log file data for Monday. Because Monday's data resides in a FastTrends database, if a subsequent analysis calls for Monday's and Tuesday's data, only the data for Tuesday needs to be analyzed.

The second set of tasks, the export tasks, transfers the data to a report-ready Content database. Content databases store the data for quick rendering into reports.

A Scheduler agent is installed on each computer along with the Reporting agent. In a distributed installation, Scheduler agents take turns acting in the role of the Scheduler, which is responsible for scheduling the execution of event tasks. The Scheduler agent currently acting as the Scheduler polls the Scheduler database for pending events. When an event is ready to run, the Scheduler agent divides the event into the necessary tasks and allocates the tasks to a computer with an available Reporting agent. The Reporting agent executes the task(s). For more information about tasks, see “Reporting Tasks” on page 5.

Reports

Security Reporting Center produces two types of reports, on-demand reports and static reports. On-demand reports are generated from the Content database when a user requests a report from the user interface. Static reports are generated by a third type of task, the render task, which is carried out by the Static Reporter after the Reporting agent has completed its tasks. During the render task, the Static Reporter takes information from the Content database and generates either a custom on-demand report or a static report. Static report formats include HTML, Microsoft Word, Microsoft Excel, Adobe PDF, and comma-separated value (CSV) format.

Events and Profiles

Profiles and events are terms that describe how users configure Security Reporting Center to analyze log files. An *event* is an analysis and reporting job. The analysis, export, and render tasks are segments of an event. Event configuration determines the type of report to generate, the period of time covered in the report, and the *profile* the reports are based on.

The *profile* defines the location of the firewall log file(s) to be analyzed as well as how Security Reporting Center can access the log file information.

Deploying Agents

You can install only one Reporting agent of each type (Firewall Reporting or Proxy Reporting) on one computer. However, a Security Reporting Center installation can include many computers with agents installed.

Chapter 2

Installing Security Reporting Center

This chapter describes the hardware and software requirements for installing Security Reporting Center, the installable components, how to plan a distributed installation, the installation procedures for both Windows and Solaris computers, and how to launch the application.

System Requirements

The minimum and recommended requirements described in the following tables are estimates based on a minimum trial installation and a typical production environment. However, system requirements depend on the volume of logs you analyze and the number of computers in your Security Reporting Center installation. Contact your Marshal Sales representative for help determining what resources you need to run Security Reporting Center in your environment.

Windows Requirements

The following table shows the requirements for Windows computers.

Component	Minimum Requirements
Processor	Pentium III or higher **Recommended:** dual Pentium IV for typical installations
Disk Space	1GB free disk space. **Recommended:** SCSI.
RAM	512 MB **Recommended:** 1 GB for typical installations
Operating System	Microsoft Windows 2000, Windows XP, and Windows 2003 Server
Database Application	MySQL

Solaris Requirements

The following table shows the requirements for Solaris computers.

Component	Minimum Requirements
Processor	Single UltraSparc II **Recommended:** Dual UltraSparc III for typical installations
Disk Space	1 GB free disk space
RAM	512 MB **Recommended:** 1 GB for typical installations
Operating System	Sun Solaris 8 and 9
Database Application	MySQL

Browser Support

Security Reporting Center supports the following browsers on a Windows computer for accessing the java-based user interface as well as on-demand and static HTML reports: Microsoft Internet Explorer 5.*x* or higher, or Netscape 6.*x* or higher. Netscape 6.0 is not supported.

Reports rely on Java, which is installed with most browsers. However, Java support is not included by default when installing Netscape 6.1. If you use Netscape 6.1, make sure you also install Java.

Planning Your Installation

When planning an installation of Security Reporting Center, decide which components to install and whether to install components on more than one computer.

Installable Components

The following table shows an overview of Security Reporting Center installable components.

Component	Description
Database server	The database that stores report data and program configuration data.
User Interface server	The browser-based Security Reporting Center user interface, including online help.
Firewall Reporting agent	The log analysis software for Firewall reports.
Proxy Reporting agent	The log analysis software for Proxy reports.
NetIQ LEA Service	A service that retrieves log file records from a properly configured Check Point Management Server. For more information, see “Using Check Point LEA” on page 101.
NetIQ Syslog Service	A service that monitors and reproduces log file records sent by syslog-capable firewalls and proxy servers. For more information, see “Using the NetIQ Syslog Service” on page 99. **Note** To install the NetIQ Syslog Service on a Solaris computer, first disable the Solaris syslog daemon.

Distributed Installations

You can install each of these components on different computers. If your computational load will be light, or if you can allocate a powerful multi-processor computer with a large amount of memory and disk space, it may make sense to run all of them on the same computer. If you use a single computer, we recommend using a dual-processor computer.

In large installations with many firewalls, install multiple Reporting agents on your network to share the computational load among computers. Make sure that Reporting agent computers, which perform analysis tasks, have sufficient resources to handle the load. As you work with Security Reporting Center, you may choose to install more Reporting agents on your network.

Before you decide how to deploy an installation across multiple computers and/or platforms, review "Architecture" on page 3.

Warning
If you are installing different components of Security Reporting Center on different computers, install the Database server first and the User Interface server second before you install the other components. Otherwise, installation will fail.

Installation Procedures: Windows

The steps below describe a complete installation of all the Security Reporting Center components. If you do a partial installation, installing only some components on a particular computer, some steps will be skipped.

Note
This section gives instructions for installing Security Reporting Center on a Microsoft Windows 2000, Microsoft Windows XP, or Microsoft Windows 2003 Server computer. For information about installing on a Sun Solaris computer, see "Installation Procedures: Sun Solaris" on page 16.

To install one or more Security Reporting Center component(s) on a Windows computer:

1. Insert the CD-ROM in the CD-ROM drive.
2. Click **Install**.
3. Click **Next**.
4. Click **I accept the terms in the license agreement**.
5. Click **Next**.

Note
If you do not accept the terms of the license agreement, you cannot install Security Reporting Center.

6. In the Custom Setup Type dialog box, choose a Setup Type.

   – To install all the components of Security Reporting Center in the default directory on this computer, click **Complete**, then click **Next**.

   – To choose which components to install on this computer, or to choose an installation directory other than the default, click **Custom**, then click **Next**. The Custom Install dialog box is displayed. By default, all the components are installed. For more information about whether to install all components on one computer, see “Planning Your Installation” on page 9.

   Warning
   If you are installing different components of Security Reporting Center on different computers, install the Database server and the User Interface Server before you install the other components. Otherwise, installation will fail.

   If you do not want to install a component, click the icon next to it and select **Do not install this component**

7. When you finish choosing components, click **Next** to continue installing. The Database Server Parameters dialog box opens.

   This dialog box defines the location and access parameters for a database server. If you install multiple Database servers during a distributed installation, specify their parameters manually using the Log Analysis options in the Reporting module. This allows the other components of Security Reporting Center to contact the database. For more information, see “Configuring Program Services and User Rights” on page 14.

8. In the **Host Name** text box, type the host name of the computer where the MySQL database will be installed. This name should be identical for every installation in your Security Reporting Center environment. If it is entered incorrectly, you will not be able to connect to the databases.

9. In the **Port Number** text box, type the number of the port used to communicate with your database. The default port number is 3306.

10. In the **User Name** text box, type an administrator user name for your database. If you are installing the database component on this computer, then the user name you type in this dialog box also becomes the database administrator user name. This user name and its password are used internally to contact the database.

11. In the **Password** text box, type a password for the user name.

12. In the **Confirm Password** text box, re-type the password.

13. Click **Next** to continue. The UI Server Parameters dialog box is displayed. The information you type in this dialog box should be the same for every computer where Security Reporting Center is installed, regardless of which components you are installing.

14. In the **Host Name** text box, type the host name of the computer where the User Interface server for your installation will be installed.

15. In the **Port Number** text box, type the number of the port used to communicate with the user interface. The default port number is `9000`.

16. In the **Login Name** text box, type a login name for the Security Reporting Center administrator account. This login name and its password will be used to log in to the user interface the first time you open Security Reporting Center.

17. In the **Password** text box, type a password for the user name.

18. In the **Confirm Password** text box, re-type the password.

19. Click **Next** to continue. You are prompted to begin the installation.

20. Click **Install** to begin installing Security Reporting Center software. The installation may take several minutes.

21. Click **Finish** to exit the InstallShield Wizard.

Configuring Program Services and User Rights

If you have installed Security Reporting center on multiple computers, or if you plan to access log files or other resources through mapped (or network) drives, you must configure Security Reporting Center services to log on under an account with access rights to those drives. By default, product services log on under the system account. To access mapped drives, you should typically configure the services to log on under a user account. This involves two steps: selecting an account to use for each service, and giving that account the appropriate rights.

You should perform the steps described below if you plan to use a network drive to do any of the following:

- Retrieve log files
- Store the DNS cache
- Collect Check Point log files using OPSEC LEA
- Collect log files with the NetIQ Syslog Service
- Store FastTrends databases.
- Unzip log files.

To configure services:

1. Go to the Windows Control Panel and double-click **Administrative Tools**.
2. In the Administrative Tools window, double-click **Component Services**.
3. Select **Services (local)** in the left pane.
4. Right-click **NetIQ Scheduler Agent** in the right panel and select **Properties**.
5. Click the Log On tab.
6. Select **This Account** and click **Browse** to select an account from the list.
7. Type the password for the account, confirm it, and click **OK** to exit the dialog box.
8. Stop and restart the service.
9. If you want the NetIQ LEA Service or NetIQ Syslog Service to write to a mapped (or network) drive, repeat Steps **1-8** for those services.

To give the account necessary rights:

1. Go to the Windows Control Panel and double-click **Administrative Tools**.
2. Double-click **Local Security Policy**.
3. Under Security Settings in the left pane, expand **Local Policies**.
4. Double-click **User Rights Assignment**.
5. Double-click **Act as Part of the Operating System**, and make sure the account you specified earlier is in the list. Click **Add** to add the user account.
6. Repeat this step for Log on as a Service and Log on Locally.

Uninstalling Security Reporting Center: Windows

To uninstall Security Reporting Center:

1. Go to the Windows Control Panel and double-click **Add/Remove Programs**.
2. Select **Security Reporting Center** and click **Remove**.

Installation Procedures: Sun Solaris

Notes

Do not install Security Reporting Center as the root user.

To install Security Reporting Center, a user must have full rights to the installation directory.

To install the NetIQ Syslog Service on a Solaris computer, you must first disable the Solaris syslog daemon.

Solaris installations require you to execute an installation script. Because all the installed services for Security Reporting Center will run under the same user account you are using when you run the script, you should switch to the appropriate user account before you begin installation.

The steps below describe a complete installation of all the Security Reporting Center components. If you do a partial installation, installing only some components on a particular computer, the installation skips some steps. However, you may be prompted to provide access information for components not included in the current installation. For example, when you install the Database server, you provide access information for the User Interface server.

To install Security Reporting Center:

1. Make sure you are logged in to the user account you want Security Reporting Center to run under.
2. From the Security Reporting Center CD-ROM, move one of the two compressed TAR files (`frs-solaris.sparc.tar.gz` and `frs-solaris.sparc.tar.z`) to a local directory, uncompress it, and unTAR it. This creates a directory called `src-2.0`.
3. At a command prompt, type `install.src` to run the installation script.
4. If you want to install as the current user, press **Enter**.

5. If you want to install as a different user:

   a. Type `Ctrl-C` to cancel the installation script.

   b. Login or su to the appropriate user account.

   c. Re-execute the installation script.

6. Press **Enter** to view the license agreement.

7. Type `accept` to accept the license agreement. You are prompted to choose an installation directory for Security Reporting Center.

Note
To install Security Reporting Center, the installation user needs full rights to the installation directory.

8. ***If you want to use the default directory***, press **Enter**. The default directory is `/usr/local/NetIQ`.

9. ***If you want to use a different directory***, type the path to the directory and press **Enter**. You are prompted to confirm the directory.

   – Type `Y` if the directory is correct.

   – Type `n` if the directory is not correct and select a new directory.

10. Choose which components of Security Reporting Center to install.

    – If you want to install all the components on this computer, type `D`.

    – If you do not want to install all the components on this computer, type the number for each component you do not want to install, followed by the letter `D`. Press **Enter** only after you have specified all the components you want excluded from the installation.

11. Type a user name for the Database server. This user name has no relationship to the Unix username.

12. Type the host name of the computer where the Database server will run. The default computer is your local computer.

13. Type the name of the MySQL server socket. The default socket is `/tmp/mysql.sock`.

14. Type the port number for MySQL. The default port number is 3306.

15. The core components are installed, and the MySQL database starts and is populated with initial data. Press **Enter** to continue.

16. Type a user name for the User Interface server. (This user name has no relationship to the Unix username.)

17. Type a password for the User Interface server.

18. Type a port number for the User Interface server. The default port number is `9000`.

19. Press **Enter** to install the User Interface server.

20. Press **Enter** to install the Firewall Reporting agent.

21. Press **Enter** to install the Proxy Reporting agent.

22. Press **Enter** to install the NetIQ Check Point LEA service.

23. Press **Enter** to install the NetIQ Syslog Service.

24. Choose whether to copy the necessary scripts to `etc/init.d` in order to launch Security Reporting Center during startup.

    – Type `n` to continue without copying the scripts.

    – Type `Y` to copy the scripts. When prompted, type the root password.

25. Choose whether to start the User Interface server.

    – Type `Y` to start the User Interface server.

    – Type `n` to continue without copying the scripts.

26. ***If you did not start the User Interface server during installation***, start it manually. Go the `installation directory\common\bin` directory in the and execute `startallui.sh`.

27. The URL you need to access the Security Reporting Center Console is displayed.

Starting and Stopping Services

If you need to start or stop any Security Reporting Center components, execute the start and stop scripts installed with Security Reporting Center. The following table shows the scripts for starting and stopping each service.

Service	Script
User Interface Server	`installpath/common/bin/startallui.sh` `installpath/common/bin/stopallui.sh`

Database Server	`installpath/common/bin/mysql.server start`
	`installpath/common/bin/mysql.server stop`

Scheduler agent	`installpath/modules/agent/agent.sh –start`
	`installpath/modules/agent/agent.sh -stop`

NetIQ LEA Service	`installpath/modules/leaservice/wtlead –start`
	`installpath/modules/leaservice/wtlead -stop`

NetIQ Syslog Service	`installpath/modules/syslogservice/wtsyslogd –stop`
	`installpath/modules/syslogservice/wtsyslogd -start`

All Security Reporting Center services	`installpath/common/bin/stopallsrc.sh`

Uninstalling Security Reporting Center: Sun Solaris

To uninstall Security Reporting Center:

1. Become the install user used to run the installer, for example `src`.
2. Execute the following script:

   ```
   common/bin/stopallsrc.sh
   ```

3. Delete the directory where you installed Security Reporting Center.

Starting Security Reporting Center

To start the user interface, use the URL `http://hostname:9000`, where `hostname` is the name of the computer where the User Interface server is installed.

To log in to Security Reporting Center and launch the application:

1. Open a Web browser.
2. Go to `http://hostname:9000`.
3. In the text boxes provided, type the login name and password you specified during installation for logging in to the user interface.

   Note
   To log in to a domain other than the local domain, specify the domain name before the user name. Use the format `domain name/user name`.

4. To log in automatically when you open the program again, select the **Remember Me** check box.
5. Click **Log in**.

Adding a Serial Number

To begin using the program, add at least one trial code (to run the program in demo mode) or one serial number.

To add a trial code or serial number:

1. Type or paste a trial code or serial number into the text box at the bottom of the screen.

   – ***If you do not have a trial code and want to request one***, click **Trial Registration**.

   – ***If you want to purchase a license for a fully functioning version of Security Reporting Center***, click **Order Online**.

2. Click **Submit** to submit the code, or click **Cancel** to clear the text box.

3. To add more codes or serial numbers, click **Add Another** and repeat Steps **1** and **2**.

4. When you finish adding serial numbers, click **Done**. You can view the current serial numbers at any time by clicking **Administration > Licensing** in the left pane of Security Reporting Center.

To add another serial number after your initial installation:

1. Click **Administration > Licensing** in the left pane of Security Reporting Center.

2. Click **Add Trial Code or Serial Number**.

3. Type or paste a serial number into the Trial Code or Product Serial Number text box.

4. Click **Submit** to submit the code, or click **Cancel** to clear the text box.

5. To add more codes or serial numbers, click **Add Another** and repeat Steps **2** and **3**.

6. When you finish adding serial numbers, click **Done**. Security Reporting Center displays the current serial numbers.

Registration

If you have not yet registered, you are prompted to register your Security Reporting Center installation after you log in.

- Click **Register Now** to access the registration Web site.
- Click **Register Later** to continue using Security Reporting Center without registering. You will be prompted to register each time you log in until you have registered.

The User Interface

The Security Reporting Center user interface is a two-paned Web-based console. The left navigation pane shows a list of the currently available modules. It also shows a list of the available configuration areas for the currently selected module.

The current content you have selected is shown in the right-hand panel. To see a different panel, use the navigation buttons on the panel or choose another link from the left pane. If the panel contains a **Save**, **Next**, **Cancel**, or **Done** button, use one of these choices to move forward or backward in a sequence. Do not use the browser's **Back** button to move to the previous panel.

Open Tasks

If you exit a panel during a configuration task without saving or canceling, the panel is added to the list of Open Tasks in the left pane below the module list. Click any open task to return to the abandoned configuration panel.

Help

You can find Help in several ways.

- Click the **?** icon to get context-sensitive information about using the panel you are currently viewing. You can access context-sensitive Help from any panel except the introductory and main Options panels of each module.
- Click the **help** link in the Tools menu to view the Table of Contents for the Help.
- Use the Index and Search tabs within the Help to find topics.

The Tools Menu

The Tools menu is the menu of links at the top right of the Security Reporting Center console.

The following table shows the function of each link in the Tools menu.

Link	Function
logout	Click to log out of Security Reporting Center.
feedback	Click to send feedback about the product to Marshal.
about	Click to see the version number of the current module, the platform where it is installed, and the name of the user who is currently logged in. You can also access the Marshal Web site and the Customer Support Web site from this link.
support	Click to access the Marshal Customer Support Web site.
help	Click to access the Help for the current module

Licensing

The serial numbers you add can license tasks, firewall servers, or firewall profiles. To see your licensing status, view the Licensing panels. You can access these panels by selecting **Administration > Licensing** on the left pane of Security Reporting Center. Security Reporting Center can license tasks, firewalls, profiles, and support plans.

Licensed Tasks

The Licensed Tasks panel displays your licensed tasks by operating system. Tasks are the smaller units of work that make up one event. Each event that is run is decomposed into a number of tasks, which can be run simultaneously. All the tasks from one event run on the same computer. If more than one event runs at the same time, tasks can be distributed to different computers and run simultaneously provided enough tasks have been licensed.

You can also add more serial numbers or trial codes from this panel. See “Serial Numbers” on page 26 for more information.

For each operating system, the panel shows the operating mode and the number of licensed tasks.

Operating Modes

The operating mode describes the type of license you have purchased. Operating modes include:

Full

Gives you full access to Security Reporting Center functionality, as limited by your user rights. Definition

Trial

Gives you a limited-time trial version of Security Reporting Center with all features activated

Expired Trial

After your trial version has expired, lets you run reports that analyze sample data only. You must purchase Security Reporting Center to continue using it with full functionality.

Limited Demo

Lets you access the Security Reporting Center interface and view reports for existing profiles and events, but doesn't let you create new profiles or events.

Number of Licensed Tasks

The number of licensed tasks is the number of simultaneous tasks that Security Reporting Center can run on a given operating system. One task license allows only one task at a time for a given operating system, regardless of whether tasks are run on the same computer or on different computers.

Tasks may be licensed for Windows, for Solaris, or for All OS. By default, if you do not add serial numbers to add more tasks, installing Security Reporting Center licenses one task for the operating system where you installed the Firewall Reporting agent. If you purchase a task license for All OS, you can use it to run tasks on any operating system.

Before it runs, each event is decomposed into a number of tasks. Some tasks can run simultaneously on the same computer. All the tasks from one event must run on the same computer. If more than one event runs at the same time, tasks can be distributed to different computers and can run simultaneously provided enough tasks have been licensed.

Licensed Firewalls

The Licensed Firewalls panel displays the number of firewalls or proxy servers for which you have purchased Security Reporting Center licenses. When you create a profile, Security Reporting Center records the name of the firewall or device and adds it to the list of licensed firewalls. If you delete all the profiles associated with a firewall, the firewall name is deleted from the database, and you can add a new firewall to the license.

You can also add more serial numbers or trial codes from this panel. See “Serial Numbers” on page 26 for more information.

If you attempt to generate a report for a profile with an unlicensed firewall, Security Reporting Center displays an error message.

Licensed Profiles

The Licensed Profiles panel displays the number of profiles for which you have purchased Security Reporting Center licenses. When you create a profile, Security Reporting Center makes a note of it and adds it to the list of licensed profiles. When you delete a profile, the profile is deleted from the list, and you can add a new profile to the license.

You can also add more serial numbers or trial codes from this panel. See "Serial Numbers" on page 26 for more information.

Serial Numbers

The Serial Numbers panel lets you view the list of serial numbers that have been entered for your Security Reporting Center installation. Adding one or more serial numbers allows you to operate Security Reporting Center using a certain number of servers, firewalls, tasks, and/or profiles. To add more servers, firewalls, tasks or profiles, you must add more serial numbers. Marshal serial numbers can be obtained from a Marshal sales representative. To contact a sales representative, send email to sales@marshal.com.

To refresh the Serial Number List, click **Refresh Licensing Info**.

Support Plans

The Support Plans panel displays information about the subscriptions currently in effect for your Security Reporting Center installation. Support plans determine the time period during which you can receive free upgrades. You can also add more serial numbers or trial codes from this panel.

Chapter 3
Getting Started

This chapter explains the main functions of the four modules included in your product installation. Using the sample profiles provided with your installation, it also walks you through the basic configuration steps you use to generate useful reports. For detailed information about creating profiles and events, see "Basic Configuration" on page 41.

The Express Interface

The Express interface provides quick configuration and report access designed for new users of Security Reporting Center and for users who primarily use Security Reporting Center to view reports. The Express interface provides the following features:

- A consolidated, automatically updated view of all pending reports
- Automatic report launching
- The ability to quickly create and launch new reporting profiles

To switch to Express interface mode from Expanded interface mode, click **Express Interface** on the left pane of Security Reporting Center. To begin configuring a new report in Express interface mode, click **New Profile**.

Creating Reports in Express Mode

The Express interface lets you create reports quickly with the minimum configuration. In Express mode, reporting profiles require the following information:

1. Whether you want to create a Firewall or Proxy report. For more information, see “Profile Type Panel” on page 43.
2. A brief name or description to identify the profile. For more information, see “General Panel” on page 44.
3. The type of log file you want Security Reporting Center to analyze. For more information, see “Log File Type” on page 44.
4. The location of the log file. For more information, see “Log File Location” on page 45.
5. Information about addresses of computers behind your firewall. Security Reporting Center uses this information to determine the direction of traffic flow in your network. For more information, see “Addresses Behind Firewall” on page 51.

The Expanded Interface

The Expanded interface includes all Security Reporting Center configuration features. If you used Security Reporting Center in earlier versions, you should already be familiar with the Expanded interface. The Expanded interface provides full functionality for advanced users and administrators.

To move from Express interface mode to Expanded interface mode, click **Expanded Interface** on the left pane of Security Reporting Center.

Security Reporting Center Modules

The Security Reporting Center Expanded interface includes four modules:

- The Firewall Reporting Module. For more information, see “The Firewall Reporting Module” on page 29.
- The Proxy Reporting Module For more information, see “The Proxy Reporting Module” on page 31.
- The Scheduler Module. For more information, see “The Scheduler Module” on page 34.
- The Administration Module. For more information, see “The Administration Module” on page 35.

The Firewall Reporting Module

Use the Firewall Reporting module to create profiles for the logs used to generate firewall reports. Firewall reports emphasize security, traffic across the firewall, and bandwidth. Use the options in this module to fine-tune the way Security Reporting Center analyzes the data in your firewall logs and the content and style of your reports.

Each profile is a set of instructions that determines what log data Security Reporting Center collects, where to access the data, and how to analyze and present it in reports. For instance, a profile identifies the locations of your firewall log files, determines how to resolve IP addresses, and tells the Firewall Reporting module who can access reports. Profiles also allow you to choose filters that can narrow down your data to the information you need most, which can save time and resources.

Firewall Reporting Module Options

To access the Firewall Reporting module options, open the Firewall Reporting module and click **Options**.

The Firewall Reporting module includes the following options for configuring data collection and reporting.

Options Grouping	**Functions**
Log Analysis	Lets you fine-tune the handling of log files during analysis. For more information, see “Setting a Default UnZip Location” on page 112, “Managing Protocols” on page 117, “Managing Protocol Families” on page 118, and “Default Operating System” on page 153.
Firewall Reporting	Lets you manage report content. For more information, see “Managing Protocols” on page 117, “Limiting Content Database Table Size” on page 169, and “Work Hours” on page 116.
Global Filters	Lets you create filters to include and exclude data from analysis and reporting. Global filters are available when configuring any profile. For more information, see “Managing Data with Filters” on page 189.
FastTrends Database Management	Lets you manage the locations of FastTrends databases and delete them to save space. For more information, see “Delete Database Information” on page 161, “FastTrends Database Maintenance Event” on page 163, and “FastTrends Location” on page 160.
Content Database Management	Lets you manage the locations of Content databases and decide whether and when to delete them. For more information, see “Content Database Maintenance Event” on page 166 and “Content Database Locations” on page 167.
Report Styles*	Lets you design visual styles that can be applied to reports by selecting colors, fonts, and images. For more information, see “Understanding Report Styles” on page 182.
Department Management*	Lets you group IP addresses into departments for more effective filtering and reporting. For more information, see “Department Management” on page 115.

Syslog*	Sets the log file rotation frequency for log records sent to the NetIQ Syslog Service, and allows binding to a single IP address. For more information, see “Syslog Settings” on page 99.
Log File Path Macros*	Lets you create custom macros for specifying the path to your log files. For more information, see “Log Path Macros” on page 95.
Check Point LEA Connections*	Lets you create connections between a Check Point Management Server and the NetIQ LEA Service. For more information, see “Creating LEA Connections” on page 102.
Check Point LEA Performance*	Lets you fine-tune connections between a Check Point Management Server and the NetIQ LEA Service. For more information, see “Check Point LEA Performance Options” on page 107.
Cisco PIX Interfaces*	Lets you define custom interfaces logged by Cisco PIX firewalls so Security Reporting Center can parse them. For more information, see “Cisco PIX Interfaces” on page 122.
Currency*	Lets you manage the list of currencies used to calculate bandwidth cost. For more information, see “Currency Types” on page 121.
DNS*	Lets you fine-tune internal and external DNS handling. For more information, see “Optimizing DNS” on page 108.

Note

Options marked with an asterisk (*) are shared between the Firewall and Proxy modules. Changes made to a setting in one module affect the setting in the other module as well

The Proxy Reporting Module

The Proxy Reporting module is primarily used to create profiles for the logs used to generate proxy reports. Proxy reports focus on the Web-surfing habits of users inside the firewall, providing detailed information about how often users surf and which Web sites they visit. Use the options in this module to fine-tune the way Security Reporting Center analyzes the data in your proxy server logs and the content and style of your reports.

Each profile is a set of instructions that determines what log data to collect, where to access the data, and how to analyze it and present it in reports. For instance, a profile identifies the locations of your firewall log files, determines how to resolve IP addresses, and tells the Proxy module who can access reports. Profiles also allow you to choose filters that can narrow down your data to the information you need most, which can save time and resources.

Proxy Reporting Module Options

The Proxy Reporting module includes the following options for configuring data collection and reporting.

Options Grouping	Functions
Log Analysis	Lets you fine-tune the handling of log files during analysis. For more information, see “Setting a Default UnZip Location” on page 112, “Managing Protocols” on page 117, “Managing Protocol Families” on page 118, and “Default Operating System” on page 153.
Proxy Reporting	Lets you manage report content. For more information, see “Protocols and Protocol Families” on page 117, “Limiting Content Database Table Size” on page 169, and “Work Hours” on page 116.
URL Categorization	Lets you decide how to use URL categories in reporting Web activity. For more information, see “URL Categorization” on page 130.
Global Filters	Lets you create filters to include and exclude data from analysis and reporting. Global filters are available when configuring any profile. For more information, see “Managing Data with Filters” on page 189.
FastTrends Database Management	Lets you manage the locations of FastTrends databases and delete them to save space. For more information, see “Deleting FastTrends Databases” on page 161, “FastTrends Database Maintenance Event” on page 163, and “FastTrends Location” on page 160.
Content Database Management	Lets you manage the locations of Content databases and decide whether and when to delete them. For more information, see “Content Database Maintenance Event” on page 166 and “Content Database Locations” on page 167.
Report Styles*	Lets you design visual styles that can be applied to reports by selecting colors, fonts, and images. For more information, see “Understanding Report Styles” on page 182.
Department Management*	Lets you group IP addresses into departments for more effective filtering and reporting. For more information, see “Department Management” on page 115.

Syslog*	Sets the log file rotation frequency for log records sent to the NetIQ Syslog Service, and allows binding to a single IP address.
Check Point LEA Connections*	Lets you create connections between a Check Point Management Server and the NetIQ LEA Service. For more information, see “Creating LEA Connections” on page 102.
Check Point LEA Performance*	Lets you fine-tune connections between a Check Point Management Server and the NetIQ LEA Service. For more information, see “Check Point LEA Performance Options” on page 107.
Cisco PIX Interfaces*	Lets you define custom interfaces logged by Cisco PIX firewalls so Security Reporting Center can parse them. For more information, see “Cisco PIX Interfaces” on page 122.
Log File Path Macros*	Lets you create custom macros for specifying the path to your log files. For more information, see “Log Path Macros” on page 95.
Currency*	Lets you manage the list of currencies used to calculate bandwidth cost. For more information, see “Currency Types” on page 121.
DNS*	Lets you fine-tune internal and external DNS handling. For more information, see “Optimizing DNS” on page 108.

Note
Options marked with asterisks are shared between the Firewall and Proxy modules. Changes made to a setting in one module affect the setting in the other module as well.

The Scheduler Module

The Scheduler module lets you create and monitor scheduled events. An event is an action scheduled by a Scheduler agent and performed by a Reporting agent. In Security Reporting Center, the Scheduler creates events that perform data analysis and report generation.

When you create an event, you control the following settings:

- When and how often the event runs;
- What range of log file data to analyze;

- What, if any, programs should run before and after the event runs;
- What profile settings the event uses.

An event is always associated with a particular profile. This means that the settings in that profile determine the source and scope of the data used to carry out the event.

Scheduler Module Options

The Scheduler also includes a number of panels used to manage events and Scheduler agent computers. The following table shows the functions of these panels.

Panel	Functions
Event Queue	Tracks events and tasks that are currently running and waiting to run.
Event Status	Shows status messages for each scheduled event and task.
Agents	Shows system statistics and status messages for each computer where Security Reporting Center is installed.
Options	Sets default event characteristics, Scheduler polling frequency, and status message duration.

The Administration Module

The Administration module controls access rights for users and teams and displays licensing information for your product installation. Using the Users and Teams panels in the Administration module, you can create lists of users and give them differing sets of access rights to profiles and events. You can also create and manage teams of users, who can be assigned differing rights within the team. Users and teams created in the Administration module can be given access to specific profiles using either of the Reporting modules.

Administration Module Options and Licensing

The Administration module also includes panels that provide information about the software you have licensed and installed. The following table shows the functions of the Options and Licensing panels.

Panel	Functions
Licensing	Shows what event tasks you are licensed to perform and which operating systems you are licensed to run tasks on, the number of firewalls you are licensed to monitor, and the serial numbers for the current installation. Lets you add new serial numbers.
Options	Shows what Security Reporting Center software components are installed on each computer, and the version of each software component. Controls global authentication options and the default time zone. Lets you select proxy server settings for downloading URL categorization databases.

How to Create a Report

This section outlines how to use Security Reporting Center to analyze log files and generate reports using the Expanded interface. The Expanded interface includes the full range of configuration options. To create reports quickly with minimum configuration, see “Creating Reports in Express Mode” on page 28.

To initiate log file analysis and reporting:

1. Make sure that your firewall can generate logs that are accessible by Security Reporting Center or a syslog server. See the *Firewall Configuration Guide* or the Reporting module Help for instructions on configuring your firewall.

2. Create a profile. Use the Firewall Reporting module or the Proxy Reporting module to configure profiles.

3. Create an associated event. Use the Scheduler module to configure events.

To see how events and profiles work together, practice generating reports using a sample profile and a sample event included with your installation.

4. Run the event. Events analyze the data in your logs and export report-ready data to a Content database where it can be accessed on demand.

To enable a disabled profile:

1. Click the **Edit** icon next to the profile, or click the name of the profile.
2. On the General tab, clear the **Disable this profile** check box.
3. To see the saved settings in the sample profile, click the profile name. When you add a new profile, you see all the panels in the Add Profile wizard in sequence. When you edit a profile, you see all the configuration panels in a tabbed view.
4. Click the Log Files tab to see the log file format and location. The sample profiles use log files installed on the computer where you installed the Reporting agent.

Sample Event Settings

You can view the two preconfigured sample events using the Scheduler module. Click **Scheduler > Scheduled Events** on the left pane to see the list of scheduled events. Because each one is associated with one of the sample profiles, the sample events installed with Security Reporting Center are called Event for Sample Firewall Profile and Event for Sample Proxy Profile. If the sample events have been deleted, see “Creating an Event” on page 73 for detailed information about creating a new event.

As you can see from the Profile column in the List of Scheduled Events, this event is associated with the Sample Firewall Profile. This means that whenever this event is run, it uses the settings configured in that profile.

The event may be grayed out. A grayed-out event has been disabled, and cannot run.

To enable a disabled event:

- Click the **Edit** icon next to the event, or click the name of the event.
- On the General tab, clear the **Disable this event from running** check box.

Running the Event

To run the event immediately, click the associated **Run Event Now** icon. A Scheduler agent divides the event into tasks, and it runs as soon as these tasks can be allocated to a computer with an available Reporting agent.

To track the progress of the event, click **Event Queue** on the left pane. The event queue shows which event tasks are currently running and which tasks are waiting to run.

To see the status messages generated by an event as it runs, click **Event Status**.

Viewing Reports

You can view reports after an event has finished running. A green check-mark icon next to an event shows that it has completed.

To view reports on demand:

Click the **View On-demand reports for this profile** icon next to a sample event. All the on-demand reports for the profile associated with this event (not just the on-demand reports for this event) can be accessed from this interface.

When you have data from multiple events that use the same profile, the report interface becomes a report center for all these events. For more information about using multiple on-demand reports for a single profile, see "Using Reports" on page 173.

Icon Definitions

The following table shows the toolbar icons used to manage profiles, events, and other Security Reporting Center objects.

Icon	Name	Function
✎	Edit	Lets you change the settings of an existing object such as a profile, event, or user.
⧉	Copy	Lets you make a copy of the settings of an existing object such as a profile, event, or user so you can modify them to create a new object.
✗	Delete	Lets you delete an object.
📊	View Reports for This Profile	Lets you view all the reports associated with a Firewall or Proxy Reporting profile.
→	Run Now	Adds an event to the event queue so that log analysis will take place.
📂	View Event Detail	Shows detailed run status information for an event.
🌐	Make Local	Makes a global filter into a local filter that can be accessed only from inside the current profile.

Chapter 4
Basic Configuration

This chapter discusses in detail how to create profiles using the Reporting modules, and how to create and run events using the Scheduler module. It contains a thorough description of the user interfaces for both these tasks.

Creating a Profile

You can create a profile very quickly using the Add Profile wizard. The Add Profile wizard takes you through the entire series of panels controlling profile features. Some of these features require configuration for every profile. Some are optional.

If you change a profile after you have initially created and saved it, you may need to delete the FastTrends and Content databases before continuing to run events. For more information, see “Delete Database Information” on page 161 .

The following table shows a list of the profile configuration panels and their functions. When you copy or edit a profile, these panels appear in a tabbed view rather than in sequence.

Panel	Task	Required?
Module (Express Mode)	Choose whether to create a Firewall or Proxy reporting profile	yes
General	Name the profile and enable or disable reporting for it	yes
Log File Type	Specify the firewall type, whether the firewall resides on one computer or several, and whether to retrieve logs using the NetIQ Syslog Service.	yes
Log File Location	Specify where the logs reside.	
Addresses Behind Firewall(s)	Identify computers behind the firewall, so reports can show the direction of traffic	yes
DNS Lookup	Decide how to handle IP address resolution and where to store the DNS cache	no
Categories (Proxy profiles only)	Choose whether to track Web content using URL categorization databases, and whether to apply category mapping schemes created in the URL Categorization options	no
Filters	Attach filters to limit data collection and reporting	no
Bandwidth Cost	Assign a monetary value per KB to track bandwidth cost	no
User Access	Identify users who have access to the profile	no
Team Access	Identify teams who have access to the profile	no
Report Header	Specify a title, description, image(s) and/or associated URL(s) for your report output	no
Report Style Access	Specify which visual styles can be applied to reports for this profile.	no
Report URL	Specify a custom URL to request on-demand reports	no

FastTrends Directory*	Specify the FastTrends database location for this profile	no
Content Database*	Specify the Content database location for this profile	no
UnZip Directory*	Specify the location where log files in compressed format will be extracted for this profile	no
OS Binding*	Specify the operating system(s) on which events using this profile can run	no
Host Binding*	Specify a limited group of computers where events using this profile can run	no
FTP Directory*	Specify the temporary storage directory for log files downloaded using FTP	no
Content Database Table Size*	Specify the number of entries per table to export to the Content database	no

Note
Items marked with an asterisk appear in the profile configuration panels only when profile-specific configuration is enabled in the corresponding panel in the Firewall or Proxy options.

To start creating a profile:

Go to the Profiles panel in either Reporting module (or in the Express interface) and click **New Profile** to open the Add Profile wizard.

Profile Type Panel

The Profile Type panel lets users in Express mode choose whether to create a Firewall Reporting profile or a Proxy Reporting profile. Firewall reports focus on security, bandwidth usage, and the type of traffic surrounding your firewall. Proxy reports focus on Web and FTP use by users on your network.

To select a profile type, click **Firewall Reporting** or **Proxy Reporting**.

General Panel

The General profile panel lets you assign a name. You can also use it to disable the profile if you do not want Security Reporting Center to analyze or report on the log file data specified in the profile.

- To specify the profile name, type a name for the profile in the **Description** text box.
- To prevent any scheduled events based on this profile from running, select the **Disable this profile** check box. No new reports can be generated for this profile while it is disabled.

Log File Type

The Log File Type panel lets you specify the following information:

- The brand and model of your firewall or proxy server
- Whether your firewall resides on more than one computer
- How Security Reporting Center should access the log files.

The information you supply in this panel determines the information requested in the Log File Location panel.

Note
Before you set up a profile, make sure your firewall is configured to generate logs that are accessible by Security Reporting Center or a syslog server. For more information about configuring your firewall to work with Security Reporting Center, see the *Firewall Configuration Guide*.

To specify the log file type and collection method

1. In the Log File Format list, select a firewall type such as **Cisco PIX firewall** or a log format such as **WELF** or **squid**. If you are not sure of the firewall type, contact your system administrator. Depending on your Log File Format selection, some options may be grayed out.
2. ***If your firewall is installed on more than one computer***, select the **Multiple Servers** check box.

   If your Security Reporting Center installation includes multiple computers, we recommend storing log files in a shared network location. Storing logs in a shared location makes the logs available to all the computers assigned to analyze them.
3. ***If you want the NetIQ Syslog Service to collect the log files***, select the **Use Syslog** check box. The NetIQ Syslog Service collects log records from firewalls and writes them to a log file in a location you select. For more information about whether your firewall can send log records to the NetIQ Syslog Service, see the *Firewall Configuration Guide*.

Log File Location

The Log File Location panel specifies where Security Reporting Center can find your log files. Unless you plan to use the NetIQ Syslog Service or the NetIQ LEA Service to collect your logs, you should store them in a location where all Security Reporting Center components have access to them.

This panel asks for different information depending on the settings in the Log File Type panel.

- ***If you selected a Check Point firewall using OPSEC LEA***, see “Check Point with OPSEC LEA” on page 46.
- ***If you selected*** **Use the NetIQ Syslog Service to collect firewall logs**, see “NetIQ Syslog Service” on page 46.
- ***If you selected any other firewall or log type***, see “All Other Log Types” on page 46.

Check Point with OPSEC LEA

If you selected a Check Point firewall with OPSEC LEA, select a Check Point LEA connection from the list. For more information about Check Point OPSEC LEA and Check Point LEA connections, see "Using Check Point LEA" on page 101.

NetIQ Syslog Service

To specify log collection settings for the NetIQ Syslog Service:

1. In the **Firewall IP Address** text box, type the IP address of the firewall.
2. In the **Log File Destination** text box, type the full path to the location where you want the NetIQ Syslog Service to save the log file. If your Security Reporting Center installation includes multiple computers, we recommend storing log files in a shared network location. Storing logs in a shared location makes the logs available to all the computers assigned to analyze them.

All Other Log Types

To specify any other log type:

1. In the **Log File Path** text box, type the path to the log files you want to analyze, listing each file path on a separate line, or click the folder icon to create a file list by browsing.

   If you browse to a file, Security Reporting Center adds a prefix to your log file path to indicate file location. The prefix `file:///` means indicates that the file is located on the local computer. The prefix `file://` means that it is located on a remote computer. If you type a path in the text box, you do not need to type this prefix.

   Note
   On a Solaris computer, log file paths are case-sensitive.

   For examples of log file paths, including how to use wildcards and date macros, see "Log File Path Examples" on page 48.

2. ***If you are accessing log files using FTP:***

a. Select absolute or relative FTP paths.

b. If your FTP server requires a login, supply the user name and password required to access it in the **Login Name** and **Password** text boxes. Click **Use Anonymous Login** to populate the **Login Name** and **Password** text boxes with the user name `Anonymous` and the password `user@marshal.com`.

Log Files: Multiple computers

If your firewall experiences high volumes of traffic, it may need multiple servers, also known as a cluster server, to handle the volume. And because each server generates its own log file, you need to analyze these log files collectively to achieve a complete view of the activity around your firewall.

If you indicated that your firewall is part of a cluster in the General panel, you can use the Log Files panel to specify the brand and model of your firewall, to build a list of the servers in the cluster on which your firewall resides, and to specify the location of the firewall log files. A message at the bottom of the panel tells you how many firewall servers are covered by your current Security Reporting Center license.

Note
You must define at least one server.

To add a server to the list:

1. Select the brand and model of your firewall server from the Log File Format list.
2. Click **New Server** and complete the information in the New Cluster Server panel.

To edit, copy, or delete servers in a cluster:

- To edit a server, click the **Edit** icon next to the server you want to edit. The Edit Cluster Server panel opens.
- To add a server based on existing server settings, click the **Copy** icon in the same line of the server list as the server you want to edit.
- To delete a server from the list, click the **Delete** icon next to the server in the list.

To exit the panel:

- ***If you are editing an existing profile***, click **Save** to save your changes, or Cancel to abandon your selections and return to the profiles list.
- ***If you are creating a new profile***, click **Next** to continue to the next panel, or **Cancel** to abandon your selections and return to the profiles list.

Log File Path Examples

The first table gives examples for paths using various types and numbers of log files. The other tables describe the available date macros and give examples for how they can be used to specify log files.

Path Examples

For these files:	This path	Does this:
Standard log files	`c:\winnt\system32\logfiles \logfile.20020214`	Specifies the file location of the log file
	`ftp://ftp.domain.com/logs /ex20020214.log`	Retrieves the log file `ex20020214.log`, located in the `logs` directory from the FTP server `domain.com`.
Compressed log files	`c:\winnt\system32\logs \logfile.20020214.zip`	Specifies the zipped log `logfile.20020214.zip`, located in the `\winnt\system32\logs\ directory` on drive c
	`ftp://ftp.isp.com/log /ex20020214.gz`	Specifies the compressed log `ex20020214.gz`, located in the log directory on the `isp.com` FTP server.
Multiple log files (using wildcards)	`c:\logfiles\logfile.*`	Specifies all log files in the `c:\winnt\system32\logfiles` directory that begin with `logfile`.
	`c:\winnt\system32\log* \logfile.*`	Specifies all log files beginning with `logfile` in any directory.

Date Macros

You can use the following date macros to return specific log files that are named by date.

This macro:	Specifies:
`%dd%`	Day
`%mm%`	2-digit month

`%Mon%`
Note
This variable is case-sensitive:
`%Mon%` returns `Jan`
`mon` returns `jan`
`MON` returns `JAN`
	Abbreviated month

`%yy%`	2-digit year
`%yyyy%`	4-digit year
`%Date-X%`	Subtracts X days from the current system date.

The following date macro examples use 02/24/2000 as the current system date.

This macro:	Specifies this path:
`c:\winnt\system32\logfiles \logfile.%yyyy%%mm%%dd%`	`c:\winnt\system32\logfiles\logfile.20020224`
`c:\winnt\system32\logfiles \logfile.%yyyy%%mm%*`	`c:\winnt\system32\logfiles\logfile.200002*`
`c:\winnt\system32\logfiles\logfile.%Date-5%%yyyy%%mm%%dd%.log`	`c:\winnt\system32\logfiles\logfile.20000219`
`c:\winnt\system32\logfiles\access-%Mon%/%dd%/%yyyy%.log`	`c:\winnt\system32\logfiles\access-Feb/24/2000.log`

Addresses Behind Firewall

Use the Addresses Behind Firewall panel to specify domain names or IP addresses for computers that reside behind your firewall. Security Reporting center reports use this information to identify the origin and direction of firewall activity.

Typically, addresses behind the firewall are the computers your employees use. By identifying addresses that reside behind your firewall, you allow Security Reporting Center to tell whether traffic originates inside or outside the firewall, and thus track incoming and outgoing activity in your reports. For example, Security Reporting Center can report which internal addresses had the highest level of activity, how much outgoing email activity occurred during the reporting period, and how many firewall rules were triggered by external addresses.

The following table shows examples of how to specify address ranges.

Specify an individual IP address	`192.168.10.10`
Specify a range of IP addresses:	`192.168.10.0/24`
Use wildcards to specify multiple IP addresses:	`192.168.*`
Specify a domain name:	`*.marshal.com`

By default, any addresses encountered in the log files that are not in the list of addresses behind firewalls are assumed to be external addresses.

To add a domain or IP address range:

1. In the text box above the **Add to List** button, type the domain name, IP address, or IP address range for the computers you want to identify as located behind the firewall. You may use wildcards or CIDR notation to designate multiple IP addresses.

   Note
   If you are using a Gauntlet firewall for Windows NT, specify both the domain name and the IP address found in the firewall log file. This ensures more accurate reporting. For example, if the log file contains the record `host=hostx4.zzz.com/99.99.3.40`, add two separate entries: `hostx4.zzz.com` and `99.99.3.40`.

2. Click **Add to List** to add the text box entry.

3. Repeat to add more domains, addresses, or address ranges.

To remove a domain or IP address range:

1. In the list box, select the domain, IP address, or IP address range that you want to delete. Press `Ctrl` to select multiple items.

2. Click **Remove from List**.

To clear the list of domain names, IP addresses, and IP address ranges:

1. Click **Select All** to select the entire list.
2. Click **Remove from List**.

To unselect all domains, IP addresses, and IP address ranges:

Click **De-select All**. Any items you previously selected are now unselected.

To exit the panel:

- ***If you are editing an existing profile***, click **Save** to save your changes, or Cancel to abandon your selections and return to the profiles list.
- ***If you are creating a new profile***, click **Next** to continue to the next panel, or **Cancel** to abandon your selections and return to the profiles list.

DNS Lookup

The DNS Lookup panel lets you select a DNS lookup mode and, if necessary, specify the location of the DNS cache. DNS lookups translate numeric IP addresses into domain names, and are used to resolve the addresses provided in the Addresses Behind Firewall panel.

If you choose Resolve mode, Security Reporting Center creates a DNS cache. You can store the cache in the default location or specify a different cache location for the current profile. To configure DNS handling in more detail, you can use the Internal and External DNS Options in each Reporting module. For more information, see “Optimizing DNS” on page 108.

To specify DNS lookup information:

1. Select a resolution mode from the Domain Name/IP Resolution Mode list.

   – Select **Quick mode** for the fastest performance. Quick mode uses the domain name or IP address from the log file, and is the fastest mode for creating reports.

     DNS lookups are performed more efficiently by the firewall server itself as the log is created, rather than by Security Reporting Center. If your firewall resolves IP addresses, disable DNS Lookup by selecting Quick mode.

   – Select **Resolve mode** if your Web server does not resolve IP addresses, and if processing speed is not a concern. In Resolve mode, Security Reporting Center performs a DNS lookup for each unresolved IP address.

     Note
     Using Resolve mode can slow down reporting significantly. However, once a numeric address has been looked up, its text equivalent is stored in a cache to expedite subsequent reports. By default, a separate cache is maintained for each profile.

2. ***If you selected Resolve mode***, specify the location of the DNS cache. The DNS cache stores lookup information only for addresses behind the firewall. DNS lookups for addresses outside the firewall are stored in memory.

3. ***If you want to choose where to store the DNS cache***, select the **Store DNS cache in custom location** check box. Type the path to the new location in the text box.

4. ***If you want to store the DNS cache in the default locatio***n, clear the check box.

5. Do one of the following:

   – ***If you are editing an existing profile***, click **Save** to save your changes, or **Cancel** to abandon your selections and return to the profiles list.

   – ***If you are creating a new profile***, click **Next** to continue to the next panel, or **Cancel** to abandon your selections and return to the profiles list.

Filters

The Filters panel lets you attach Include and Exclude filters to the profile. Filters help you limit the data collected and displayed in reports to focus on the information that is most important to you. Any filter can be added to a profile as an Include filter or an Exclude filter. When you add a filter as an Include filter, Security Reporting Center analyzes all the data described in the filter and includes it in reports. When you add the same filter as an Exclude filter, Security Reporting Center excludes the data described in the filter from analysis and does not include it in reports.

The Filters panel also lets you create local filters. Only users with access to the profile can see a profile's local filters. For more information about creating local and global filter, see "Managing Data with Filters" on page 189.

This panel lets you view and manage the list of Global and Local filters associated with the current profile. You can use this list to:

- Add or remove filters from this profile, convert a global filter to a local filter, and view settings for global filters.
- Create, edit, delete, and view settings for local filters.
- Specify whether a filter is an Include or an Exclude filter.

Filters allow you to tailor the data analyzed for reports. Filters are sets of criteria that identify a given set of data: For instance, a filter may specify all the records that mention a particular authenticated user name.

When you add a filter to a profile you can choose to apply it as either an Include or Exclude filter. If a filter is added to a profile as an Include filter, all the log data matching the criteria in the filter is included in log analysis and thus in reports for the profile. Adding the same filter as an Exclude filter ensures that none of the log data matching the criteria in the filter will be analyzed for reports based on the profile. For example, if you add the global filter Inbound Traffic Only as an Include filter, all log file data for traffic coming from outside the firewall is analyzed for reports using this profile. If you add an Inbound Traffic filter as an Exclude filter, all incoming traffic is excluded from analysis. You may combine Include and Exclude filters for highly specific and complex filtering statements. For more information, see "Using Multiple Filters" on page 194.

Filters may also be added as either global or local filters. A global filter can be selected for any profile within the installation, while a Local filter is only visible within a single profile. Global filters are created, edited, and deleted using the Filter options in each Reporting module. Local filters are created, edited, and deleted using the Filters panel in the profile settings.

To add a Global filter to a profile:

1. Click **Add Global Filter**. The Add Global Filter to Profile panel opens.
2. Select a filter in the left-hand list. Press `Ctrl` to select multiple filters.
3. Click **Select** to move it to the right-hand list.
4. Click **Done** to save your changes. You are returned to the Filters panel, and the filters you selected appear in the filter list.
5. Under Type, select:
   - **Include** to create an Include filter.
   - **Exclude** to create an Exclude filter.

To convert a Global filter into a Local filter:

Click the **Make Local** icon next to an entry in the list.

To create a Local filter and add it to the current profile:

1. Click **Create Local Filter**. The General filter panel opens.
2. Click **Save** to save your changes.
3. The **Type** radio button shows whether the filter is an Include or Exclude filter. By default, the filter is added to your profile as an Include filter. If you want to add it as an Exclude filter, click **Exclude**.

To manage Local filters:

- To edit a filter, click the **Edit** icon next to an entry in the list and edit the information in the General filter panel.
- To delete a filter from the profile, click the **Delete** icon next to an entry in the list.

- To create a filter based on an existing filter, click the **Copy** icon next to an entry in the list and edit the settings in the General filter panel.
- To view settings for a filter, click the **View** icon next to an entry in the list.

To exit the panel:

- ***If you are editing an existing profile***, click **Save** to save your changes, or **Cancel** to abandon your selections and return to the profiles list.
- ***If you are creating a new profile***, click **Next** to continue to the next panel, or **Cancel** to abandon your selections and return to the profiles list.

Bandwidth Cost

The Bandwidth Cost panel lets you assign a cost, or tariff, per KB of bandwidth transferred, so you can track the cost of incoming and outgoing traffic. You can also specify the currency used in reports. The list of currencies you can select is maintained in the Currency options. For more information about modifying the Currency list, see "Currency Types" on page 121.

Security Reporting Center calculates bandwidth cost by multiplying the per-KB cost you supply by the number of KB transferred. Bandwidth calculations include all firewall events that log a value for KB transferred. In general, firewalls log a value for all events associated with a protocol.

Cost accounting for network activity is addressed in the Bandwidth report chapter, a specialized grouping of report pages. Bandwidth reports show the number of events, percent of total events, KB transferred, and cost for each of the top user addresses, outgoing protocols, and incoming protocols. Because different firewalls report different information, reports may not include all this information. See the *Firewall Configuration Guide* or the Help for your firewall to find out what information your firewall logs about protocols.

To report cost accounting, use the graphs and tables for Top Clients by Kilobytes, Outgoing Protocol Usage, and Incoming Protocol Usage. You can customize these reports by using filters to include or exclude specific users and specific protocols.

To specify bandwidth cost:

1. In the Currency list, specify the currency symbol that will appear in reports of bandwidth cost.

2. In the **Cost** text box, type the cost per KB of bandwidth. You can use up to five decimal places.

   Note
   Although Security Reporting Center uses five decimal places to calculate bandwidth cost, reports show bandwidth cost with only two decimal places.

3. Do one of the following:

   – ***If you are editing an existing profile***, click **Save** to save your changes or **Cancel** to abandon your selections and return to the profiles list.

   – ***If you are creating a new profile***, click **Next** to continue to the next panel or **Cancel** to abandon your selections and return to the profiles list.

User Access

The User Access panel lets you specify which users can access the current profile as well as their level of access rights to the profile. For more information about user rights, see “User Rights and Team Rights” on page 139.

In Security Reporting Center, a user is an individual who has access rights within the application. Users are added from the Administration module's User Rights panel. Within the User Access panel, access rights can be assigned at three levels: Report User, Power User, and Admin.

The following table summarizes these access rights.

User Rights	View Reports*	Schedule Events*	Edit Profiles*
Report Users	X		
Power Users	X	X	X
System Admins	X	X	X

*Only applies to profiles to which the user has access.

Note
User rights are additive. A user can obtain access to a profile by being assigned profile-specific rights, rights within a team, or general user rights. For instance, a System Admin has access rights to all profiles regardless of access rights granted within the profile.

To add a user:

1. Click **Add**. The Add User Access to Profile panel opens.
2. Select or de-select users by clicking an item in the list and clicking **Select** or **De-select**.
3. Click **Done** to save your changes, or click **Cancel** to abandon them. You are returned to the User Access panel.

To assign user access rights:

1. Select a user from the list. A list of options is shown in the lower portion of the panel.
2. Select one of the following levels of access rights for this user:
   - **Report User**. The user can only view reports for the profile.
   - **Power User**. The user can view reports for the profile, edit the profile settings, and schedule events for the profile.
   - **Admin**. The user can view reports for the profile, edit profile settings, schedule events for the profile, and delete the profile.

Note
User rights are additive. A user can obtain access to a profile by being assigned profile-specific rights, rights within a team, or general user rights. For instance, a System Admin has access rights to all profiles regardless of access rights granted within the profile.

To remove a user:

1. Select a user from the list.
2. Click **Remove**.

To exit the panel:

- ***If you are editing an existing profile***, click **Save** to save your changes, or **Cancel** to abandon your selections and return to the profiles list.
- ***If you are creating a new profile***, click **Next** to continue to the next panel, or **Cancel** to abandon your selections and return to the profiles list.

Team Access

The Team Access panel lets you specify which teams have access to the current profile.

A team is a logical grouping of users created in the main Teams panel of the Administration module. For example, a team called Human Resources Team might consist of various Human Resources employees who need to access reports about employee Web surfing as well as a team administrator who creates profiles, schedules events, and manages team membership and member rights.

Each individual team member's rights to the profile are defined by the user's rights within the team. Team rights are configured in the Team Members panel when configuring a team.

To add a team:

1. Click **Add**. The Add Team Access to Profile panel opens.
2. Select a team from the left list and click **Select** to add the user to that team, or select a team from the right list and click **De-select** to remove that user from the selected team.

3. Click **Done** to save your changes, or click **Cancel** to abandon them. You are returned to the Team Access panel.

To remove a team:

1. Select a team from the list.
2. Click **Remove**.

To exit the panel:

- ***If you are editing an existing profile***, click **Save** to save your changes, or Cancel to abandon your selections and return to the profiles list.
- ***If you are creating a new profile,*** click **Next** to continue to the next panel, or Cancel to abandon your selections and return to the profiles list.

Report Header

The Report Header panel lets you specify the title and descriptive text displayed in the header of the reports for a specific profile. This title and description appear at the top left of a report in HTML format, and on the cover page of a report in Microsoft Word, Microsoft Excel, Adobe PDF , or CSV format.

To specify report headers:

1. In the **Report Title** text box, type the name you want to appear in the report header of HTML-based reports or on the cover page of static document reports. By default, the Report Title is the same as the profile description specified in the General panel.
2. In the **Report Description** text box, type a description for the report. The description is displayed below the title in reports.

3. Do one of the following:

   – ***If you are editing an existing profile***, click **Save** to save your changes, or **Cancel** to abandon your selections and return to the profiles list.

   – ***If you are creating a new profile***, click **Next** to continue to the next panel, or **Cancel** to abandon your selections and return to the profiles list.

Report Style Access

Report styles let you customize the look and feel of reports by creating style sheets that control the color scheme and the images. Users can select different styles while using on-demand reports.

Use the Report Style Access panel to control user access to any proprietary styles you have created. For example, Managed Service Providers may design multiple report styles with logos that brand reports for individual customers. The Report Style Access panel allows you to create an available list of styles linked to the profile. Users who view on-demand reports based on the profile can select only the styles in the list. Static report styles are selected within the report event and cannot be changed while viewing a report.

To specify the report styles available when viewing reports for this profile:

1. ***If you want to make all report styles available***, select **Make all report styles available for reports based on this profile.**

2. ***If you want to specify a limited list of available styles***, select **Make only selected report styles available for reports based on this profile** and move styles from the Configured Report Styles list to the Selected Report Styles list using the **Select** and **De-Select** buttons.

3. Do one of the following:

   – ***If you are editing an existing profile***, click **Save** to save your changes, or **Cancel** to abandon your selections and return to the profiles list.

   – ***If you are creating a new profile***, click **Next** to continue to the next panel, or **Cancel** to abandon your selections and return to the profiles list.

Report URL

The Report URL panel lets you customize the URL used to request on-demand reports for each profile. Unless you specify otherwise, on-demand reports by default are sent to a URL address created using the `%PROFILE%` macro. This macro creates a unique filename based on the profile name. The optional Report URL setting lets you modify the default URL used to view the on-demand report for each profile.

To customize the URL that generates On-Demand reports for immediate viewing, type some text in the text box. The Firewall Reporting module creates a unique profile name to be used in URL requests, using the Report URL ID as the final term in the URL. By default, the Report URL ID is the name of the profile. If you want to use another name, type it in the **Report URL ID** text box.

For example, if you type the company name `netiq` in the **Report URL ID** text box, on-demand reports are accessible at:

```
http://UIHostName/src/bin/FWReport/netiq
```

where `UIHostName` is the name of the computer where the User Interface server is installed.

Note
Because the string you provide becomes part of a URL request, use only lower-case letters without punctuation or spaces.

To exit the panel:

- ***If you are editing an existing profile***, click **Save** to save your changes, or **Cancel** to abandon your selections and return to the profiles list.
- ***If you are creating a new profile***, click **Next** to continue to the next panel, or **Cancel** to abandon your selections and return to the profiles list.

FastTrends Directory

FastTrends is a technology that efficiently stores analyzed log file data, making subsequent analyses of the same data much faster. For example, when you generate a report on Monday, the analyzed data for Monday is stored in a FastTrends database. If you run a report using the same profile for Monday and Tuesday, only the data for Tuesday needs to be analyzed.

As you run events, data is continuously stored in the FastTrends database unless you choose to delete is through FastTrends database maintenance. This process of storing analysis results occurs in the background and does not interfere with system performance. Each profile uses a separate FastTrends database.

The FastTrends Directory panel lets you specify the location of the FastTrends database for the current profile. If you do not specify a location, the database is created in the system-wide default location specified in the Log Analysis Options of the current module. You may want to specify a different location if you have space constraints. However, when choosing an alternate location for the FastTrends database, keep in mind that in a distributed installation, all computers with agents installed must be able to access the FastTrends database.

Note
This panel is displayed only when you select the **Allow per-profile settings** check box in the FastTrends Location panel of the module's Log Analysis Options. For more information, see “FastTrends Location” on page 160.

To specify the FastTrends database location:

1. In the **Database Directory** text box, type the path to the FastTrends database.
2. Do one of the following:
   - ***If you are editing an existing profile***, click **Save** to save your changes, or **Cancel** to abandon your selections and return to the profiles list.
   - ***If you are creating a new profile***, click **Next** to continue to the next panel, or **Cancel** to abandon your selections and return to the profiles list.

Content Database

The Content Database panel lets you specify whether to use the default Content database for the current profile or whether to select a different Content database. A Content database is the database from which reports are generated. After firewall log file data has been analyzed and stored in compressed form in the FastTrends database, report-ready content is exported from the FastTrends database to the Content database, where it can be quickly accessed and rendered into reports. Content databases are configured in the Content Database Locations panel.

Note

The Content Database panel is displayed only when per-profile configuration has been enabled in the corresponding Options panel. See "Content Database Locations" on page 167 for more information.

To specify the Content database to use for the current profile:

1. Select one of the following options:

   – If you want to use the default Content database, select **Use the default Content database**.

   – If you want to select a different Content database, select **Use the following Content database location** and select a Content database location from the list.

2. Do one of the following:

   – ***If you are editing an existing profile***, click **Save** to save your changes, or **Cancel** to abandon your selections and return to the profiles list.

   – ***If you are creating a new profile***, click **Next** to continue to the next panel, or **Cancel** to abandon your selections and return to the profiles list.

UnZip Directory

When a profile specifies compressed log files, for example `.zip` or `.gz` files, the Reporting agent requires a directory in which to temporarily store the uncompressed files. The UnZip Directory panel lets you specify that temporary directory location: either the default directory defined in the UnZip Location options panel, or a profile-specific directory that you define in this panel.

Note
This panel is visible only when you select the **Allow per-profile settings** check box on the UnZip Location panel of the module's Log Analysis Options. For more information, see "Setting a Default UnZip Location" on page 112.

To select a directory for unzipping files in compressed format:

1. Select one of the following two options:

   – Select **Use the global UnZip directory** if you want to use the default unzip directory that is specified in the UnZip Location panel of Log Analysis Options. The location of the global unzip directory is shown in the field below. When you include the `%PROFILE%` macro as part of the path, a separate sub-directory is created for each profile.

   – Select **Use the profile-specific UnZip directory** and type the path to the location in the text box if you want to specify a different unzip location for this profile. Paths beginning with `./` are relative to the `installation root/modules/firewall` directory, where `installation root` is the directory where the Firewall Reporting module is installed.

2. Do one of the following:

   – ***If you are editing an existing profile***, click **Save** to save your changes, or **Cancel** to abandon your selections and return to the profiles list.

   – ***If you are creating a new profile***, click **Next** to continue to the next panel, or **Cancel** to abandon your selections and return to the profiles list.

OS Binding

Security Reporting Center can be installed in an environment that includes both Windows and Solaris computers. The OS Binding panel lets you specify the operating system of the computers where Firewall Reporting agents can run events for this profile.

Note
This panel is displayed only when you select the **Allow per-profile settings** check box in the OS Binding Default panel of the module's Log Analysis Options. For more information, see “Default Operating System” on page 153.

To select the operating system on which all the events associated with this profile will run:

1. Select one of the following options:

   – Select **All Operating Systems** if you want events to run on the first available agent computer, regardless of operating system.

   – Select **Windows** if you want events to run only on agent computers with a Microsoft Windows operating system.

   – Select **Solaris** if you want events to run only on agent computers with a Sun Solaris operating system.

2. Do one of the following:

   – ***If you are editing an existing profile***, click **Save** to save your changes, or **Cance**l to abandon your selections and return to the profiles list.

   – ***If you are creating a new profile***, click **Next** to continue to the next panel, or **Cancel** to abandon your selections and return to the profiles list.

Host Binding

The Host Binding panel lets you specify a limited group of computers where events for this profile will run. Specifying host groups can be useful for allocating system resources. For example, you may want to assign profiles for large log files to run events only on computers with the resources to handle them efficiently. Host groups are created in the Host Groups panel in the Scheduler module options.

Note:
This panel is displayed only if you have selected the **Allow per-profile settings** check box in the Host Binding Default panel of the module's Log Analysis Options. For more information, see “Host Binding Default” on page 155.

To select the group of hosts on which all the events associated with this profile will run:

1. Choose one of the following options:
   - ***If you want events to run on the default host group***, which is shown grayed out below the selection, select **Use the default host group**.
   - ***If you want events to run only on the computers in another host group***, select **Use the following profile-specific host group** and choose a host group from the list.
2. Do one of the following:
   - ***If you are editing an existing profile***, click **Save** to save your changes, or **Cancel** to abandon your selections and return to the profiles list.
   - ***If you are creating a new profile***, click **Next** to continue to the next panel, or **Cancel** to abandon your selections and return to the profiles list.

FTP Directory

When you configure Security Reporting Center to download log files from an FTP server, it uses a temporary directory to store these files before they are analyzed and stored in the FastTrends database. The FTP Directory panel lets you choose whether to use the default FTP download location defined in the FTP Location panel of the Log Analysis options, or whether to specify a different location for this profile.

Note:
This panel is displayed only if you have selected the **Allow per-profile settings** check box in the FTP Location panel of the module's Log Analysis options.

To specify the FTP location:

1. Do one of the following:

   – Select **Use the global FTP directory** if you want to use the default temporary storage location that you specified in the FTP Location panel of the module's Log Analysis Options.

   – Select **Use the profile-specific FTP directory** if you want to override the default FTP location and specify a custom location to use with this profile.

2. Do one of the following:

   – ***If you are editing an existing profile***, click **Save** to save your changes, or click **Cancel** to abandon your selections and return to the profiles list.

   – ***If you are creating a new profile***, click **Next** to continue to the next panel, or click **Cancel** to abandon your selections and return to the profiles list.

Content Database Table Size

When exporting report-ready content to the Content database, you may want to save disk space by limiting the number of records that are exported to and stored in the Content database tables. The Content database table size specifies the maximum number of records per table that can be exported to the Content database.

Note

This panel is displayed only when you have selected the **Allow per-profile settings** check box in the Content Database Table Size Default panel of the Firewall Reporting options. For more information, see “Limiting Content Database Table Size” on page 169.

To set the Content database table size:

1. Do one of the following:
   - Select **Use the global Content database table size** to use the default Trim Count setting specified in the Default Trim Count panel of the Log Analysis options.
   - Select **Use the following profile-specific Content database table size** and type a value to specify the maximum number of records exported to each table during events for this profile only.
2. Do one of the following:
   - ***If you are editing an existing profile***, click **Save** to save your changes, or **Cancel** to abandon your selections and return to the profiles list.
   - ***If you are creating a new profile***, click **Next** to continue to the next panel, or **Cancel** to abandon your selections and return to the profiles list.

Categories

URL categorization is a method of tracking the content of Web and FTP sites your users access through the proxy server. Security Reporting Center can track URLs your users request against content categories defined by the categories defined within Security Reporting Center. Core categories include potentially sensitive content, for sexually explicit material or sites containing hate speech. General categories include inoffensive but potentially distracting sites focusing on topics such as news, astrology, or music. These categories are configured using the URL Categorization options in this module. For more information, see “URL Categorization” on page 130.

Category mappings let you associate and combine existing categories to produce reports for particular situations. For example, you may want to create reports that show whether activity is work-related. To make such a report more effective, you could map categories such as Gambling or Chat to the Non-Work-Related category. You may choose not to count certain other General categories (News, for example) as Non-Work Related.

To enable or disable URL categorization:

- To enable URL categorization and include categorization data in reports, select the **Enable categorization of Web activity** check box.
- To disable URL categorization and exclude categorization data from reports, clear the **Enable categorization of Web activity** check box.

To select a category mapping for use in reports for this profile:

1. Select the **Enable categorization of Web activity** check box. If this check box is not selected, the category mapping controls are grayed out.
2. Select a category mapping from the list.
3. To continue, do one of the following:
   - ***If you are editing an existing profile***, click **Save** to save your changes, or click **Cancel** to abandon your selections and return to the profiles list.
   - ***If you are creating a new profile***, click **Next** to continue to the next panel, or click **Cancel** to abandon your selections and return to the profiles list.

Creating a Default Event

When you finish creating a new profile, Security Reporting Center prompts you to auto-create and launch a default event. During a default events Security Reporting Center analyzes your log files and creates on-demand HTML-format reports using basic preconfigured event settings. If you want to create analysis events, reports with a custom time range or static reports in non-HTML report formats, do not create a default event; instead, create an event manually using the Scheduler module.

Default events use the default report range and report interval settings specified in the Scheduler module options and the default language and style settings selected in the Administration module options. For more information about these default settings, see "Default Report Range" on page 120, "Default Report Intervals" on page 119, and "Default Report Language and Styles" on page 121.

To choose whether to create a default event:

- To create and launch the default event, click **Create Default Event**.
- To save the profile without creating a default event, click **Don't Create Event**.

Editing Existing Profiles

If you change the parameters of an existing profile after initially saving it, keep in mind that you may need to delete the FastTrends and Content Databases for the profile. Because reports reflect all the data collected for a particular profile, reports for a profile that has been changed without deleting the existing databases may show confusing or unreliable data. For example, if you change the log file path and continue to use the same databases, reports reflect data from both log files.

When you change any of the following parameters and then attempt to save the revised profile, you are prompted to delete the FastTrends database and the Content database associated with the profile. You should delete both the databases.

If you delete only one of the two databases, either when prompted or using the database maintenance options, reports will still be generated using the old data in the remaining database.

When you change any of the following configuration options, you are prompted to delete databases:

- The log file path
- Whether to use the NetIQ Syslog Service
- Whether to use Check Point LEA

- The addresses located behind the firewall
- The DNS lookup method
- The associated filters

Creating an Event

During an event, the settings in a profile are used to analyze and report on your log file data. You can create an event very quickly using the Add Report Event wizard in the Scheduler module. The Add Report Event wizard takes you through the entire series of panels controlling event features. Some of these features require configuration for every event. Some are optional.

The following table shows the event configuration panels and their functions. When you copy or edit an event, these panels appear in a tabbed view rather than in sequence.

Panel	Task	Required?
General	Name the event, and enable it or disable it from running	Yes
Profile	Select the profile this event uses.	Yes
Schedule	Decide when the event runs.	Yes
Report Range	Choose the report range for this event.	Yes
Report Parameters and Destination	If you used a Custom report range, specify a label for a custom on-demand Report and/or destination(s) for static HTML and static Word, Excel, PDF, and CSV reports.	Yes
Pre-Processing	Specify a program to run before the event runs.	No
Post-Processing	Specify a program to run after the event runs.	No

To view the current list of events

Click **Scheduler > Scheduled Events** on the left pane of Security Reporting Center. The List of Scheduled Events is displayed.

To begin creating an event:

Click **New Event**.

Event Type

The Event Type panel lets you choose whether to create a Report event or an Analysis event. Most users use Report events, which are designed to make report data available immediately. Use Analysis events when you want to accumulate data over time without creating a report.

Report Events

Report events complete the standard sequence of steps required to create a report. When you run a Report event, Security Reporting Center analyzes your data and stores it in an interim FastTrends database, then exports the data in report-ready form to a Content database. The Content database provides the content for reports, which you can access them on demand or create on a schedule. You can configure Security Reporting Center to create scheduled reports in HTML, Microsoft Word, Microsoft Excel, Adobe PDF, or CSV format. For more information about choosing a report format, see “Report Parameters and Destination” on page 84.

Analysis Events

Analysis events analyze your data and store it in an interim FastTrends database, but do not create report-ready content. Analysis events are useful for accumulating large amounts of data over time. By analyzing data and letting it accumulate in a FastTrends database before you export it to a Content database, you can save processing time for large cumulative logs. For example, running an Analysis event allows you to accumulate data daily for a week. You can then export a week’s worth of data by running a Report event based on the same profile.

General

The event General panel lets you give a name to your new event or rename an existing event. It also lets you disable and enable events so you can easily control whether they run as scheduled.

To specify an event name:

1. In the **Description** text box, type a name for the event.

2. To enable or disable the event, do one of the following:

   – Select the **Disable this event** check box to prevent this event from running.

   – Clear the **Disable this event** check box if you want to let this event run according to its schedule.

3. Do one of the following:

   – ***If you are editing an existing event***, click **Save** to save your changes, or click **Cancel** to abandon your selections and return to the events list.

   – ***If you are creating a new event***, click **Next** to continue to the next panel, or click **Cancel** to abandon your selections and return to the events list.

Module

The event Module panel lets you choose whether to report on a profile from the Firewall Reporting module or the Proxy Reporting module. The module you select determines which profiles you can select in the Profile panel.

To specify the module:

1. Click **Firewall Reporting** or **Proxy Reporting**.

2. Do one of the following:

   - ***If you are editing an existing event***, click **Save** to save your changes, or click **Cancel** to abandon your selections and return to the events list.
   - ***If you are creating a new event***, click **Next** to continue to the next panel, or click **Cancel** to abandon your selections and return to the events list.

Profile

The Profile panel lets you select the profile associated with a scheduled event. When the event runs, it uses the log file location, filters, and other settings in the profile you select here to decide which data to analyze and other reporting settings.

To select a profile:

1. In the list, select the profile you want to use with this event. Every event must be associated with a profile. The profile determines the location, type and presentation of firewall log data to be used in reports.
2. Do one of the following:

   - ***If you are editing an existing event***, click **Save** to save your changes, or click **Cancel** to abandon your selections and return to the events list.
   - ***If you are creating a new event***, click **Next** to continue to the next panel, or click **Cancel** to abandon your selections and return to the events list.

Schedule

The Schedule panel lets you set a daily, weekly, or monthly schedule that determines when and how frequently the event will run. You can also specify a time, date, and time interval, choose a specific time for a single occurrence, or schedule the event to run repeatedly at a certain interval.

Multiple schedules can apply to a single event. For example, you may want to schedule an event to run at the same time Monday through Friday in order to track weekday activity on the firewall. By creating a second schedule to run one hour before a monthly meeting on security, you could arrange to supply the latest data exactly when you need it. You can create and manage multiple schedules using the Advanced mode of schedule creation.

To create a single schedule:

1. In the Run Event list, select a schedule type (**Daily**, **Weekly**, **Monthly**, **Once**, or **Repeated**) depending on how often you want the event to run.
2. Follow the directions below for creating that type of schedule.

To create multiple schedules:

1. Click the **Advanced Mode** hyperlink. The current list of schedules is shown.
2. To start adding a schedule, click **Add Entry**.
3. In the Run Event list, select a schedule type (**Daily**, **Weekly**, **Monthly**, **Once**, or **Repeated**) depending on how often you want the event to run.
4. Follow the directions below for creating that type of schedule.
5. When the schedule is correct, click **Apply Changes**. Your new schedule is added to the list.

To edit the list of schedules in Advanced mode:

- To edit an existing schedule, click the **Edit** icon and edit the schedule settings. Click **Apply Changes** to save your changes and return to the list.
- To delete a schedule, click the **Delete** icon.

To create a daily schedule:

1. In the Run Event list, select **Daily**.
2. In the **Start Time** text box, type the time when you want the event to run. Use format `hh:mm`. For example, for 5:15 p.m, type `17:15`.

3. In the **Start Date** text box, type the date when you want the event to run. Use the format `mm/dd/yyyy`. For example, for June 20, 2002, type `06/20/2002`.

4. Under **Run Daily**, choose one of the following options:

   – Click **Every [blank] days** and type a number in the text box to choose a custom interval in days. For instance, type `2` to run the event every other day.

   – Click **Weekdays** to run the event every day, Monday through Friday.

   – Click **Every day** to run the event every day, Monday, through Sunday.

5. Do one of the following:

   – ***If you are editing an existing event***, click **Save** to save your changes, or click **Cancel** to abandon your selections and return to the events list.

   – ***If you are creating a new event***, click **Next** to continue to the next panel, or click **Cancel** to abandon your selections and return to the events list.

To create a weekly schedule:

1. In the Run Event list, select **Weekly**.

2. In the **Start Time** text box, type the time when you want the event to run. Use the format `hh:mm`. For example, for 5:15 PM, type `17:15`.

3. In the **Start Date** text box, type the date when you want the event to run. Use the format `mm/dd/yyyy`. For example, for June 20, 2002, type `06/20/2002`.

4. From the **Run Weekly** check boxes, select the day(s) of the week on which you want the event to run weekly.

5. Do one of the following:

   – ***If you are editing an existing event***, click **Save** to save your changes, or click **Cancel** to abandon your selections and return to the events list.

   – ***If you are creating a new event***, click **Next** to continue to the next panel, or click **Cancel** to abandon your selections and return to the events list.

To create a monthly schedule:

1. In the Run Event list, select Monthly.
2. In the **Start Time** text box, type the time when you want the event to run. Use the format `hh:mm`. For example, for 5:15 PM, type `17:15`.
3. In the **Start Date** text box, type the date when you want the event to run. Use the format `mm/dd/yyyy`. For example, for June 20, 2002, type `06/20/2002`.
4. Under **Run Monthly**, choose one of the following options:
   - Click **Day [blank] of the month** and type a date in the text box to choose a date when the event will run.
   - Click the **[ordinal] [weekday]** of the month to run the event on the first, second, third, or fourth occurrence in the month of a given weekday. The default is the First Sunday of each month.
   - Select one or more check boxes to choose the months when you want to run the event.
5. Do one of the following:
   - ***If you are editing an existing event***, click **Save** to save your changes, or click **Cancel** to abandon your selections and return to the events list.
   - ***If you are creating a new event***, click **Next** to continue to the next panel, or click **Cancel** to abandon your selections and return to the events list.

To schedule an event to run once:

1. In the Run Event list, select **Once**.
2. In the **Start Time** text box, type the time when you want the event to run. Use the format hh:mm. For example, for 5:15 PM, type `17:15`.
3. In the **Start Date** text box, type the date when you want the event to run. Use the format `mm/dd/yyyy`. For example, for June 20, 2002, type `06/20/2002`.

4. Do one of the following:

   – ***If you are editing an existing event***, click **Save** to save your changes, or click **Cancel** to abandon your selections and return to the events list.

   – ***If you are creating a new event***, click **Next** to continue to the next panel, or click **Cancel** to abandon your selections and return to the events list.

To schedule an event to run repeatedly at a specified interval:

1. In the Run Event list, select Repeatedly.
2. In the **Start Time** text box, type the time when you want the event to run. The format is `hh:mm`. For example, for 5:15 PM, type `17:15`.
3. In the **Start Date** text box, type the date when you want the event to run. The format is `mm/dd/yyyy`. For example, type June 20, 2002 as `06/20/2002`.
4. Under Repeated Event, do the following:

   a. Type a number in the text box to determine what number of units apart the event will run.

   b. Select a time unit from the list to determine whether the event will happen minutes, hours, days, or weeks apart.
5. Do one of the following:

   – ***If you are editing an existing event***, click **Save** to save your changes, or click **Cancel** to abandon your selections and return to the events list.

   – ***If you are creating a new event***, click **Next** to continue to the next panel, or click **Cancel** to abandon your selections and return to the events list.

Report Range

The Report Range panel lets you determine whether a Report event will create custom or on-demand reports, what portion of the log file data specified in the profile will be analyzed and included in reports, and what report intervals are available in your on-demand reports.

Note
This panel is only available when creating and editing Report events. Analysis events use the Analysis Range panel. For more information, see "Analysis Range" on page 83.

By default, Security Reporting Center generates On-Demand Calendar reports, which are dynamically updatable and can be accessed directly from the Security Reporting Center User Interface.

If you choose **On-Demand Calendar Report**, you can choose which pre-defined reoccurring report intervals (such as Daily, Weekly or Monthly) appear in your on-demand reports. You can also define a report start and end date to specify what dates are covered in the report. On-Demand Calendar reports allow you to select all of the intervals you specify here.

Choosing **Custom Report** lets you specify a discrete time range for your reports such as **Current Day** or **Previous Week**. Select a custom report if you want to create static reports in HTML, Microsoft Word, Microsoft Excel, Adobe PDF, or CSV format. For more information about creating these report types, see "Using Reports" on page 173.

To create a Custom Report range:

1. Click **Custom Report** to activate the Custom report range settings.
2. In the Range list, select a pre-defined range from the list. Select **Specific** to choose a specific range of dates. Choose another range to select a range of dates relative to when the event runs: for example, select **Previous Complete Week Starting Sunday** to generate report data for the first full week beginning with a Sunday before the event run time.
3. ***If you selected*** **Specific**:
   - In the **Report Start Date** text box, type the date from which you want log file data to be used for this event. Use the format `mm/dd/yyyy`. For example, for June 20, 2002, type `06/20/2002`.
   - In the **Report End Date** text box, type the date up to which you want data from log file to be used for this event. Use the format `mm/dd/yyyy`. For example, for June 20, 2002, type `06/20/2002`.
4. ***If you selected a report range other than*** **Specific**, continue to the next step.

5. ***If you are editing an existing event:***

   – Click **Save** to save your changes.

   – Click **Cancel** to abandon your selections and return to the List of Scheduled Events.

6. ***If you are in the new event wizard:***

   – Click **Next** to continue to the next panel.

   – Click **Cancel** to abandon your selections and return to the List of Scheduled Events.

To create an On-Demand Calendar Report range:

1. Click **On-demand Calendar Report** to activate the on-demand report range settings.

2. Select one or more pre-defined ranges from the list.

3. In the **Report Start Date** text box, type the date from which you want log file data to be used for this event. Use the format `mm/dd/yyyy`. For example, for June 20, 2002, type `06/20/2002`.

4. In the **Report End Date** text box, type the date up to which you want data from log file to be used for this event. Use the format `mm/dd/yyyy`. For example, for June 20, 2002, type `06/20/2002`.

5. ***If you are editing an existing event:***

   – Click **Save** to save your changes.

   – Click **Cancel** to abandon your selections and return to the List of Scheduled Events.

6. ***If you are in the new event wizard:***

   – Click **Next** to continue to the next panel.

   – Click **Cancel** to abandon your selections and return to the List of Scheduled Events.

Analysis Range

Use the Analysis Range panel to determine what portion of your log data Security Reporting Center will analyze during an Analysis event. Analysis events do not create report-ready data.

Note
This panel is only available when creating and editing Analysis events. Report events use the ReportRange panel. For more information, see "Report Range" on page 80.

To run an event that will make data available for reports, run a Report event and use the Report Range panel to specify this information.

To create a Custom Report range:

1. In the **Report Start Date** text box, type the date from which you want log file data to be used for this event. Use the format `mm/dd/yyyy`. For example, for June 20, 2002, type `06/20/2002`.
2. In the **Report End Date** text box, type the date up to which you want data from log file to be used for this event. Use the format `mm/dd/yyyy`. For example, for June 20, 2002, type `06/20/2002`.
3. ***If you are editing an existing event:***
   - Click **Save** to save your changes.
   - Click **Cancel** to abandon your selections and return to the List of Scheduled Events.
4. ***If you are in the new event wizard:***
   - Click **Next** to continue to the next panel.
   - Click **Cancel** to abandon your selections and return to the List of Scheduled Events.

Report Parameters and Destination

Use the Report Parameters and Destination panel to choose directories, email addresses and/or report language and content for reports with Custom report ranges.

If you select an On-Demand Calendar report range or this event in the Report Range panel, the Report Parameters and Destination panel does not show any configuration options.

If you select a Custom report range in the Report Range panel, the Report Parameters and Destination panel lets you configure Custom On-Demand reports or static reports in HTML, Microsoft Word, Microsoft Excel, Adobe PDF, or comma-separated value (CSV) format. Select the report type you want to configure to enable the corresponding configuration panel.

Custom On-Demand Report

The Custom On-Demand panel allows you to specify a label for your Custom On-Demand report in the On-Demand Reporter interface used to view reports. While Custom On-Demand reports appear in the On-Demand Reporter, they cover a specific time range and cannot be clicked to show different time distributions. For example, you cannot click a custom on-demand report showing the last 30 days to show only the last seven days.

The Custom On-Demand panel is available only when you select a Custom report range in the Report Range panel.

To enable access to Custom date range reports using the On-Demand Reporter:

1. In the **Custom Report Label** text box, type the name you want to see in the list of Custom Date Reports in an on-demand report. A truncated version of this name is added to the date range menu for this scheduled event.

2. Do one of the following:

3. ***If you are editing an existing event:***

   – Click **Save** to save your changes.

   – Click **Cancel** to abandon your selections and return to the List of Scheduled Events.

4. ***If you are in the new event wizard:***

   – Click **Next** to continue to the next panel.

   – Click **Cancel** to abandon your selections and return to the List of Scheduled Events.

Static HTML Report

Static HTML reports are available when you select a Custom Report date range in the Report Range panel. These reports are generated once, and all the associated images and files that constitute each HTML-based report are then saved to a user-defined location. To open the report, navigate to this location and open the file.

The Static HTML panel is available only when you select a Custom report range in the Report Range panel.

We recommend that you save the report to a relative path on a networked drive to enable easier access to the reports, especially when multiple users require access. If you type an absolute path such as `c:\Firewall_Reports\default.html`, the files and images will actually be stored on the `c:\Firewall_Reports` drive of the server that renders the reports. You must then connect to that server and navigate to the report to view it.

To create a Static HTML report:

1. ***If you want to save the report to a specified directory***, select the **Save this report to a directory** check box and, in the text box provided, type the pathname of a `.htm` file in the folder where you want the report to be generated. If you specify a filename that does not already exist, Security Reporting Center creates the file when the event runs.

2. ***If you want to send the report as a `.zip` file attached to an email message***, select the **Email this report** check box and, in the text box provided, type the email address where you want Security Reporting Center to send the report.

3. ***If you want to send the report as a `.zip` file using FTP***, select the **FTP this report** check box and, in the text box, type the path to the location where you want Security reporting Center to send the report.

4. In the Report Language list, choose the language you want to use within the body of the report.

5. In the Report Template list, select the pre-defined report chapter you want to generate during the scheduled event. Chapters are specialized subsets of reports focusing on topics such as security and bandwidth. If you want to see all the report data, select **Complete Report**.

6. ***If you are editing an existing event:***

   – Click **Save** to save your changes.

   – Click **Cancel** to abandon your selections and return to the List of Scheduled Events.

7. ***If you are in the new event wizard:***

   – Click **Next** to continue to the next panel.

   – Click **Cancel** to abandon your selections and return to the List of Scheduled Events.

Static Word, Excel, PDF, and CSV Reports

Static reports in Microsoft Word, Microsoft Excel, Adobe PDF, and CSV format are available when you select a Custom date range in the Report Range panel. These reports are generated once, and are then saved to a user-defined report location and/or emailed to a specified address. To open the report, open the file named `default.wtw`. To convert the `.wtw` file to another document format, you must have the NetIQ Document Utility installed. Click the NetIQ Document Utility link in this panel to download it. Once you have installed the Document Utility, opening a `.wtw` file automatically converts it to the new format and opens it in a host application such as Microsoft Word.

The settings for creating static Word, Excel, PDF, and CSV reports are only available when you select a Custom report range in the Report Range panel.

We recommend that you save the `.wtw` file to a relative path on a networked drive to enable easier access to the reports, especially when multiple users require access. If you type an absolute path such as `c:\Firewall_Reports`, the files and images will actually be stored on the `c:\Firewall_Reports` drive of the server that renders the reports. You must then connect to that server and navigate to the report to view it.

To create a static report in Microsoft Word, Microsoft Excel, Adobe PDF, or CSV format:

1. ***If you want to save the report to a specified directory***, select the **Save this report to a directory** check box and, in the text box, type the pathname of a `.wtw` file in the folder where you want the report to be generated. If you specify a filename that does not already exist, Security Reporting Center creates the file when the event runs.
2. ***If you want to send the report as a `.zip` file attached to an email message***, select the **Email this report** check box and, in the text box provided, type the email address where you want Security Reporting Center to send the report.
3. ***If you want to send the report as a `.zip` file using FTP***, select the **FTP this report** check box and, in the text box, type the path to the location where you want Security Reporting Center to send the report.
4. In the Report Language list, choose the language you want to use within the body of the report.

5. In the Report Template list, select the pre-defined report chapter you want to generate during the scheduled event. Chapters are specialized subsets of reports focusing on topics such as security and bandwidth. If you want to see all the report data, select **Complete Report**.

6. ***If you are editing an existing event:***

   - Click **Save** to save your changes.
   - Click **Cancel** to abandon your selections and return to the List of Scheduled Events.

7. ***If you are in the new event wizard:***

   - Click **Next** to continue to the next panel.
   - Click **Cancel** to abandon your selections and return to the List of Scheduled Events.

Pre-Processing and Post-Processing

The Pre-Processing and Post-Processing panels let you specify an application to run before or after the log file has been analyzed. For example, you may want to set up a pre-processing event that runs a script to download a log file from a remote server using FTP. Once you have performed an analysis, you may want to run a post-processing event that emails a notification.

Note
In pre- and post-processing events, use only applications and scripts not already included in the Security Reporting Center user interface. For example, running a perl script to download logs files is supported, but having a Scheduled Event start the popular FTP client, `WS_FTP`, for the purpose of downloading your log files is not supported.

To specify a pre-processing event:

1. Select the **Enable Pre-Processing** check box.

2. In the **Application** text box, type the path to an executable for the application you want to run prior to log file analysis. For example, type `c:\perl\perl.exe`.

3. In the **Working Directory** text box, type the working directory to be used by the application. For example, type `c:\scripts`.

4. In the **Command Arguments** text box, type the command to be used by the application. For example, type a typical perl command such as `< downloadfiles.pl`.

5. ***If you are editing an existing event:***

   – Click **Save** to save your changes.

   – Click **Cancel** to abandon your selections and return to the List of Scheduled Events.

6. ***If you are in the new event wizard:***

   – Click **Next** to continue to the next panel.

   – Click **Cancel** to abandon your selections and return to the List of Scheduled Events.

To specify a post-processing event:

1. Select the **Enable Post-Processing** check box.

2. In the **Application** text box, type the path to an executable for the application you want to run after log file analysis. For example, type `c:\perl\perl.exe`.

3. In the **Working Directory** text box, type the working directory to be used by the application. For example, type `c:\scripts`.

4. In the **Command Arguments** text box, type the command line to be used by the application. For example, type a typical perl command such as `< uploadfiles.pl`.

5. ***If you are editing an existing event:***

- Click **Save** to save your changes.
- Click **Cancel** to abandon your selections and return to the List of Scheduled Events.

*6. **If you are in the new event wizard:***

- Click **Next** to continue to the next panel.
- Click **Cancel** to abandon your selections and return to the List of Scheduled Events.

Running and Tracking Events

When you create an event, it runs on the schedule you specify in the Schedule panel. However, you can also run the event on demand by clicking the **Run Event Now** icon.

The Scheduler module also provides several methods of tracking events. You can see the position of a given event in the event queue, see which of the tasks associated with the event have already been completed, and view status messages for events and tasks.

Running an Event on Demand

To run an event on demand, go to the List of Scheduled Events and click the **Run Event Now** icon next to the event. The event runs as soon as it can be assigned to a Reporting agent.

Tracking Events

You can track event progress and status in detail by examining the Event Queue and Event Status panels.

The List of Scheduled Events shows an icon indicating the most recent status message for each event, as well as the time when it was logged. You can refresh the list while an event is running to see current status messages. Mouse over the icon to see a brief description of the message.

The Event Queue

To see which tasks have run and which are waiting to run, click **Scheduler > Event Queue** on the left pane of Security Reporting Center. For more information about events and tasks, see "Architecture" on page 3.

Tasks currently running and waiting to run are displayed. The Event Queue also shows the event each task belongs to, the type of task, the computer the task is assigned to, and the time it was created.

- To cancel an individual task, click the **Delete** icon next to the task. Click the **Delete** icon next to the event to cancel the entire event.
- To view status details for the event, click the **View Event Detail** icon at the top right of the panel.
- To see the most recent status messages for all your events, click **Event Status** on the left pane. By default, events are listed alphabetically by event name. Click **Next Run** to sort by the time when messages were logged. Click the arrow next to the current sorting term to reverse the sort order.

The Event Queue panel shows the following four columns of data.

Event	shows the name of the event
Next Run	shows when the event is next scheduled to be run
Last Update	shows when the last message was logged
Last Message	shows the last status message, if any, logged for the event

Event Status Details

To see all the status messages for a given event, click the **View Event Detail** icon next to any event on the List of Scheduled Events or the Event Status panel. You see two lists of messages for the event. The first list shows status icons and messages logged for the event. The second list shows status icons and messages logged for each of the event sub-tasks.

Status Message Storage

By default, all status messages are stored for 3 days after they are logged. After 3 days, they are deleted. The Status Types panel lets you specify how long a particular type of status message should remain available after it is logged. After this specified period, the status message will be deleted.

The Status Types panel shows a list of status messages. For a description of each status icon, see “Status Icons” on page 93.

To change the length of time for which a type of status message remains in the database:

1. Type how long (in days) you want a given type of message to remain available once it has been logged. The default value for all messages is 3 days.
2. Click **Save** to save your changes, or click **Cancel** to abandon your changes and return to the main Options panel.

Status Icons

The following table shows the icons that accompany each status message and their definitions.

⏱	Real Time	A real-time status message was logged.
✖	Event Error	The Scheduler agent logged an error while the event was running.
❗	Event Critical	The Scheduler agent logged a critical error while the event was running.
▶	Event Starting	The event has started.
⏩	Event Progress	The event is running.
✓	Event Completion	The event has completed.
✖	Task Error	The Firewall agent logged an error while the task was running.
❗	Task Critical	The Firewall agent logged a critical error while the task was running.
▶	Task Starting	The task has started.
⏩	Task Progress	The task is running.
✓	Task Completion	The task has completed.

Chapter 5
Managing Log Files

To generate reports, first ensure that your log files are accessible. Different firewalls and devices handle log file information differently. For specific information about how to configure Security Reporting Center and your firewall, proxy server, or security device to work together, see the *Firewall Configuration Guide* or the Security Reporting Center Help.

Log Path Macros

In addition to supporting date macros that let you select groups of log files generated by date, Security Reporting Center lets you create macros you can use to designate paths to your log files.

Use the Log File Path Macros panel to specify the paths for each macro. Creating macros for log file paths is especially useful if you need to designate log file paths in a mixed installation. If you need to designate a log file path to a file server or network share so that it can be parsed by both Windows and Solaris agent computers, you can create a macro that uses two operating system-specific definitions so that the log file path is replaced with the appropriate path. For example, you could designate the macro `%WOPR%` to indicate the path to log files on a shared network drive called WOPR. If you specify a path containing the macro in the Log Files panel, Security Reporting Center can replace the macro in the file name with `file://wopr/logs/` on Windows computers, and with `/export/wopr/logs` on Solaris computers.

You can also use macros in your log file paths to conveniently maintain multiple profiles, even if you use only one operating system. If files are moved to a different location, for example, simply edit the macro definition rather than updating the path in each profile referencing files that use the same path.

Notes

- Log file macros apply to profiles in both Reporting modules.
- For examples of supported date macros, see "Log File Path Examples" on page 48.
- Log file macros apply to profiles in both Reporting modules.

To manage log file path macros:

- To add a log file path macro, click **Add New Macro** and provide the required information in the Edit Log File Path Macros panel.
- To edit a log file path macro, click the **Edit** icon next to an entry in the list and edit the information in the Edit Log File Path Macros panel.
- To delete a log file path macro, click the **Delete** icon next to an entry in the list.
- To continue, do one of the following:
  - Click **Save** to save your settings and return to the main Options panel.
  - Click **Cancel** to abandon your settings and return to the main Options panel.

Using FTP

Each Reporting module lets you decide how to use FTP for file downloads using the Log Analysis options. You can maximize efficiency by choosing the way Security Reporting Center handles FTP downloads, where downloaded log files are stored, and how long they remain in the FTP cache.

FTP Handling

Using the FTP settings, you can specify how Security Reporting Center handles FTP downloads when retrieving firewall log files using FTP.

To specify FTP settings:

1. Open a Reporting module and select **Options > Log Analysis > FTP**.
2. In the **FTP Timeout** text box, type the number of seconds that must elapse before a connection attempt is considered to have failed.
3. In the **FTP Retries** text box, type the number of times that a connection should be retried before the connection attempt is considered a failure.
4. Choose the FTP connection type:
   - Select **Use passive FTP** if you want FTP connections to be initiated from inside your firewall.
   - Select **Use active FTP** if you want to allow FTP connections to be initiated from outside your firewall.
5. Choose whether to use absolute or relative paths:
   - Select **Use absolute paths** if you want the specified path for the FTP server to be interpreted as an absolute path.
   - Select **Use relative paths** if you want the specified path for the FTP server to be interpreted relative to the login directory.

6. Specify a cache limit setting:

   - ***If you want to delete cached files that have not been used for a specific period of time***, select the **Delete Cached files not accessed in the last x days** check box. In the text box, type the number of days after which Security Reporting Center should delete cached files.
   - ***If you prefer to trim the cache after it has reached a certain size***, select the **On Reporting agent startup, trim the cache to x megabytes** text box. In the text box, type the maximum size the cache can reach before older records must be deleted.

FTP Location

When Security Reporting Center downloads log files from an FTP server, it stores them in a temporary directory before analyzing them and storing the data in a FastTrends database. The FTP Location panel lets you define the default storage location, which will be used for all profiles unless you enable per-profile configuration. If you enable per-profile configuration, the FTP Directory panel is available when adding or editing a profile, allowing you to specify a custom location.

To specify the temporary FTP storage location settings:

1. In the **Default FTP Location** text box, type the location in which you want to temporarily store log files downloaded from an FTP server.
2. ***If you want to allow System Admins to specify a custom location for log file storage on a profile-by-profile basis***, select the **Allow per-profile settings** check box .

Using the NetIQ Syslog Service

While some firewalls, proxy servers, and security devices can easily export log files in a readable format, others typically do not write log information to a readable file. In these cases, you may need to rely on a syslog server to capture and collect log information. The Reporting modules use the NetIQ Syslog Service to collect log file data. The NetIQ Syslog Service can be installed on any computer. It does not need to be installed on the same computer as other Security Reporting Center components.

Note
To install the NetIQ Syslog Service on a Solaris computer, first disable the Solaris syslog daemon.

Syslog Settings

The Syslog Settings panel lets you specify how often to rotate syslog-generated log files and the IP address where the NetIQ Syslog Service should receive data.

When you create a profile, you can choose the NetIQ Syslog Service to collect your log files. Using the Log Files panel of the Add Profile wizard, you specify the IP address where your log information is sent and the file where the NetIQ Syslog Service will write log data. The NetIQ Syslog Service collects log records by matching the UDP header to your profile, then writes them to the specified folder in the form of dated log files. A new log file is generated each day at 12:00 AM

By default, the NetIQ Syslog Service stores all syslog data in the same file in the directory you specified on the Log Files panel. If you want it to begin creating a new file every so often, you can choose to rotate the logs daily or monthly. For example, if your firewall generates a large amount of data, you may want to reduce the size of log files rather than storing all the data in a single large file. Using log file rotation also means that data is automatically grouped by date.

By default, any IP address on the computer where the NetIQ Syslog Service is installed can receive syslog data. However, if you have multiple NIC cards installed on that computer, you may want to ensure that data is sent only to a single IP address.

Note
Program services must be able to access your log files. For more information about configuring services to log on to the network with appropriate user rights, see "Configuring Program Services and User Rights" on page 14.

To define syslog settings:

1. Open a Reporting module and select **Options > Syslog**. The Syslog Settings panel opens.
2. Under Log File Rotation, do one of the following:
   - Select **Do not rotate log files** if you want the NetIQ Syslog Service to save all log file data in the same log file.
   - Select **Rotate log files daily** if you want the NetIQ Syslog Service to create a new log file for syslog data each day.
   - Select **Rotate log files monthly** if you want the NetIQ Syslog Service to create a new log file for syslog data once a month.
3. Under NetIQ Syslog Service IP Address, do one of the following:
   - If the computer where the NetIQ Syslog Service is installed has only one NIC installed, or if it has multiple NICs and you want all the IP addresses to be able to receive syslog data, select **Bind to all IP addresses**.
   - If the computer where the NetIQ Syslog Service is installed has multiple NICs, and you only want one IP address to be able to receive syslog data, select **Bind to a specific IP address** and type the IP address in the text box.
4. Click **Save** to save your changes and return to the main Options panel, or click **Cancel** to return to the Main Console without saving any of your changes.

   Note
   These shared settings apply to both the Firewall Reporting and Proxy Reporting modules. They can be set in either module.

Using Check Point LEA

Check Point VPN-1 and FireWall-1 log files are written to a local computer in binary form. Security Reporting Center supports two methods for accessing them.

- You can export log files to readable text files, which you can then make accessible to the Reporting module(s). For more information about using exported logs, see the *Firewall Configuration Guide*.
- Alternately, you can use OPSEC™ LEA to collect log records. The built-in NetIQ LEA Service connects directly to the Check Point Management Server and retrieves log files for local storage. The LEA service can be installed on any computer. It does not need to be installed on the same computer as other Security Reporting Center components.

To use Check Point OPSEC LEA to collect log files:

1. Configure your Check Point firewall to work with the NetIQ LEA Service. For detailed information about configuring the Check Point firewall for the LEA Service, see the *Firewall Configuration Guide*.
2. Create a connection using the Check Point LEA Connections options in any Reporting module. For more information, see “Creating LEA Connections” on page 102.
3. When you create a profile, select **Check Point FW-1/VPN-1 v4.*x* with OPSEC LEA** or **Check Point FW-1/VPN-1 vNG with OPSEC LEA** as the firewall type in the Log File Type panel of the Add Profile wizard. For more information about selecting a log type, see ”Log File Type” on page 44.

   Note
   Program services must be able to access your log files. For information about configuring services to log on to the network with appropriate user rights, see “Configuring Program Services and User Rights” on page 14.

4. Under LEA Connection Name, select the connection you created.
5. Complete and save the profile and run an event based on these profile settings.

Creating LEA Connections

To create a new LEA connection:

1. Open a Reporting module and select **Options > Check Point LEA Connections**. For more information about using the Check Point Lea Connections panel, see “Managing LEA Connections” on page 105.

2. Click **Add LEA Connection**. You are prompted to review the Check Point configuration instructions. Make sure you have collected the information you need to complete a connection and click **Continue**.

3. On the General panel, provide a name for the connection and select the firewall version you are using and the connection type you want to create. For more information about the fields in the general panel, see “LEA Connection General” on page 103.

4. On the Location panel, specify the location of the Check Point Management server, where you want to store the Check Point log files, and the port used to communicate with the Management Server. For more information about the fields in the Location panel, see “LEA Connection Location” on page 104.

5. On the Type-Specific panel, provide information about the firewall connection settings. For more information about the fields in the Type-Specific panel, see “LEA Connection Type-Specific” on page 105 and review the instructions for configuring your firewall type in the *Firewall Configuration Guide*.

6. Save the connection. The NetIQ LEA Service attempts to connect to the Check Point Management Server. The Check Point LEA Connections panel shows the current status of each connection. For more information about LEA status, see “Managing LEA Connections” on page 105.

LEA Connection General

The General panel of the LEA Connection wizard lets you specify the name for your connection as well as the type of firewall you are using and the type of LEA connection you want to create. The settings you choose here determine the information Security Reporting Center uses to create a connection between the NetIQ LEA Service and the Check Point Management Server. You can also choose to create a user-defined connection. To create a user-defined connection, you must select Check Point VPN-1/FireWall-1 vNG with a user-defined connection type and then configure the connection manually using the settings in the `lea.conf` file.

To specify connection settings:

1. Open a Reporting module and click **Options > Check Point LEA** Connections.
2. Select a connection in the list and click the **Edit** icon.
3. Click the General tab.
4. In the **Name** text box, type a name to identify this LEA connection when you select it on the Log Files panel. For example, depending on the number and type of firewalls in your configuration, you might use the host name or IP address of the Check Point Management Server, the version of the firewall (4.1 or NG, for example), or a connection type such as sslca or Unauthenticated.
5. Select the type of Check Point firewall you want to report on and the type of OPSEC LEA connection you want to configure. For information about Check Point connection types, see the *Firewall Configuration Guide*.
6. ***If you selected Check Point NG***, select **sslca**, **clear**, or **user-defined** from the list.

Warning:
Select **user-defined** only if you want to create a custom connection type by manually configuring the `lea.conf` configuration file, and only if you do not want to use any other connection type in the list. After they are created, user-defined connections cannot be edited using the Security Reporting Center user interface.

7. To enable or disable a connection, clear or select the **Disable this connection** check box. When a connection is disabled, the NetIQ LEA Service cannot collect Check Point firewall data.

LEA Connection Location

The Location panel of the LEA Connection wizard lets you specify the connection settings the NetIQ LEA Service uses to connect to the Check Point Management server as well as the location where the LEA Service will store log files.

Note
If you specify a UNC path to a location that requires authentication, make sure that both the NetIQ LEA Service and the NetIQ Tomcat Service are logged on as a user with permission to access the location. For more information about program service permissions, see "Configuring Program Services and User Rights" on page 14.

To specify location and port settings for the LEA connection:

1. Open a Reporting module and click **Options > Check Point LEA Connections**.
2. Select a connection in the list and click the **Edit** icon.
3. Click the Location tab.
4. In the **Directory** text box, browse or type a path to the directory where you want the NetIQ LEA Service to store the Check Point firewall logs it collects. The path must be unique, because you cannot store logs for more than one LEA connection in the same directory.
5. In the **Host IP** text box, type the IP address of the computer where the Check Point Management Server is installed.
6. In the **Port** text box, type the port number the NetIQ LEA Service should use to communicate with the Check Point firewall. The default port is 18184.

LEA Connection Type-Specific

The Type-Specific panel of the LEA Connection wizard lets you specify connection settings for the specific connection type selected in the General panel. To complete this panel, you need to use information about your Check Point firewall configuration. The required information varies according to the type of firewall and connection you create. For more information about the settings required in this panel, see the *Firewall Configuration Guide* or the Check Point firewall Help.

To provide type-specific information for the LEA connection:

1. Open a Reporting module and click **Options > Check Point LEA Connections**.
2. Select a connection in the list and click the **Edit** icon.
3. Click the Type-Specific tab.
4. In the **LEA SIC Name** text box, type the DN number for the OPSEC application you created in the Check Point Policy Editor. The DN number can be found under **Secure Internal Communication** in the OPSEC Application Properties dialog box. For more information, see the *Firewall Configuration Guide*.
5. In the **Management Server SIC Name** text box, type the DN number for the Check Point Management Server network object. The DN number can be found under **Secure Internal Communication** in the Object Properties dialog box. For more information, see the *Firewall Configuration Guide*.
6. In the **Certificate File Name** text box, type the name of the certificate file created using the `opsec_pull_cert` tool. The default name for the certificate file is `opsec.p12`. For more information, see the *Firewall Configuration Guide*.

Managing LEA Connections

The Check Point LEA Connections panel lists all currently configured connections between a Check Point firewall and the NetIQ LEA Service. A Check Point LEA Connection is required for the NetIQ LEA Service to collect Check Point log data. Use this panel to create, edit, and delete LEA connections. When you create a profile that uses Check Point with OPSEC LEA, you select one of the LEA connections in the list to collect the log data.

Before you add or edit connections, make sure you have configured your Check Point firewall to communicate with the NetIQ LEA Service. You need information about your Check Point configuration to create a LEA connection. For instructions on configuring Check Point firewalls, see the *Firewall Configuration Guide*.

For more information about Check Point OPSEC LEA, see “Using Check Point LEA.”

To manage Check Point connections:

1. Open a Reporting module and select **Options > Check Point LEA Connections**.

   – To add a LEA connection, click **Add LEA Connection** and provide the required information in the New LEA Connection wizard.

   – To edit a LEA connection, click the **Edit** icon next to an entry in the list and edit the information in the three tabs on the Edit LEA Connection panel.

   > **Note**
   > You cannot edit either a user-defined connection or a legacy connection that was created during an upgrade from an earlier version. For both these types of connections, the **Edit** icon is grayed out.

   – To delete a LEA connection, click the **Delete** icon next to an entry in the list.

   – To view the current status of a LEA connection, look at the status icon next to Last Status. The following table shows how to interpret each status. For more information about errors, see the error logs in the `modules\leaservice\log` directory.

Uninitialized	Connection information has been saved, but the connection has not yet been established.
Successful	The LEA service connected successfully and collected data with no errors.
Connection Error	An error was generated before, during or after connecting.
Critical Error	The LEA service itself generated an error, causing a connection failure.

Check Point LEA Performance Options

You can use the Check Point LEA Performance options settings to customize Check Point LEA connection handling in the following ways:

- Set the level of debugging written to the LEA service log file
- Set how long the LEA service pauses before downloading Check Point NG records
- Set the time elapsed before the LEA service initiates a new session
- Set how often the LEA service checks for profile changes
- Set whether the LEA service logs the Check Point firewall as a text name or an IP address

For more information about setting up LEA connections, see the *Firewall Configuration Guide*.

To customize LEA handling:

1. Open a Reporting module and click **Options > Check Point LEA Performance**.
2. In the **Debug Level** text box, type a value between 1 and 5 to determine the level of debug logging. The default value is 1.
3. In the **Download Time Lag** text box, type the number of seconds the LEA service should wait before downloading a Check Point NG log record. By default, the NetIQ LEA Service downloads log records for Check Point vNG firewalls only after they have aged for 3000 seconds (50 minutes). For example, the LEA Service does not download a record time-stamped 2:30 until 3:20. Because Check Point does not log bandwidth statistics for an individual connection until it closes, this time lag ensures that a connection has closed and bandwidth data is available. Specify a higher value to create a longer lag time and increase the likelihood of collecting bandwidth statistics. The minimum value is 30 seconds. The maximum value is 86400 seconds.

4. In the **Time Between Sessions** text box, type the time the LEA service should wait between LEA sessions for Check Point vNG firewalls. During each LEA session, the NetIQ LEA Service initiates a connection, downloads all available records, and then closes the connection. By default, the LEA service waits 300 seconds (5 minutes) before starting another session. Specify a smaller value to force more frequent downloads. The minimum value is 30 seconds. The maximum value is 300 seconds.
5. In the **Profile Changes Polling Interval** text box, type the number of seconds after which the LEA service should check the database for any profile changes that affect Check Point LEA.
6. Under **Firewall Name Logging**, select the **Log firewall IP addresses instead of firewall names** text box if you want the firewall name to be logged as an IP address. By default, the NetIQ LEA Service logs the text name of the Check Point firewall.

Optimizing DNS

If you choose to have the Reporting module(s) handle DNS lookups using Resolve mode (see “DNS Lookup” on page 53), you can fine-tune DNS handling for optimal performance. Security Reporting Center allows you to configure both internal and external DNS settings.

Internal DNS settings affect DNS lookups for IP addresses behind the firewall. For more information, see “Internal DNS Options” on page 109. External DNS settings affect DNS lookups for IP addresses outside the firewall. For more information, see “External DNS Options” on page 110.

Note
The shared DNS settings apply to both the Firewall Reporting and Proxy Reporting modules. They can be set in either module.

Internal DNS Options

The Internal DNS panel affects DNS lookups for addresses located behind the firewall for profiles that are using DNS Resolve mode. (See “DNS Lookup” on page 53 for information about choosing the DNS mode when creating a profile.) To choose settings that affect DNS lookups for addresses outside the firewall, see “External DNS Options” on page 110. When you choose internal DNS settings, keep in mind that internal lookups are processing-intensive. Also, internal DNS lookups attempt to resolve fewer addresses than external DNS lookups, because the number of addresses behind a firewall is limited to the number of people in the organization. Internal addresses rarely change significantly over time, and as a result, require infrequent updates.

To optimize internal DNS lookups when using Resolve mode:

1. In the **Threads** text box, type the maximum number of simultaneous processing tasks allowed when performing DNS lookups from the DNS queue.

   The default ratio between threads and queue size is 80 threads to 30,000 queue entries. For faster performance on higher-end systems, increase the ratio in increments of 1:100. In other words, increase the queue by 100 entries for each additional thread.

2. In the **Queue Size** text box, type the number of log entries that may be stored in more easily accessed memory. The default value is 30,000. Increasing the size of the queue can speed up processing, but uses more memory. This setting is used for both internal and external DNS lookups.

   See the note in Step **1** for information about optimizing the ratio between threads and queue size.

3. In the **Timeout** text box, type the number of seconds that must elapse before a given lookup is cancelled when performing DNS lookups. If a DNS lookup is unsuccessful in this period of time, that lookup is assumed to have failed.

Note
If most of your lookups exceed the timeout period before they are resolved, you may need to increase your timeout setting. However, if most addresses fail to be resolved within a reasonable timeout period, consider increasing the number of simultaneous threads in order to reduce the time it takes to process the queued IP addresses. This can avoid the bottleneck that results when your computer looks up a few addresses at once, most of these lookups fail to resolve, and your computer then attempts to look up the next addresses in the queue.

4. In the **Cache Expiration** text box, type the number of days that a domain name or IP address is retained in the cache and written to the system disk. After this period of time, Security Reporting Center discards the domain name or IP address from the cache and disk, and must perform a new lookup if the domain name or IP address occurs again.

External DNS Options

The External DNS settings affect DNS lookups for addresses located outside the firewall for profiles that use DNS Resolve mode. (See “DNS Lookup” on page 53 for information about choosing the DNS mode when creating a profile.) To choose settings that affect DNS lookups for addresses behind the firewall, see “Internal DNS Options” on page 109. Keep in mind that external DNS lookups are simpler than internal lookups, and that they store results in memory rather than in a local cache.

To choose external DNS settings:

1. Open a Reporting module and click **Options > Log Analysis**.
2. Click the External DNS Options tab.
3. In the **Memory Cache Size** text box, type the maximum number of domain names or IP addresses that can be stored in memory.

   The default value is `5000`.

4. In the **Lookup Retries** text box, type the number of times Security Reporting Center should retry a DNS lookup before assuming failure.

5. In the **Timeout** text box, type the number of seconds that must elapse before Security Reporting Center assumes a given lookup has failed.

6. Select the **Three-Byte Comparison** check box to match addresses only by the first three bytes. By default, Security Reporting Center uses four-byte comparison to resolve IP addresses. This means that all four bytes in the IP address are used to match the domain name. With four-byte comparison, addresses can be traced to the level of a specific computer name. Three-byte comparison results in faster DNS lookups, but provides a less accurate resolution.

   For example, a DNS server using three-byte comparison to resolve the IP address 60.88.212.164 uses only the first three bytes of the address, 60.88.212. The default four-byte comparison uses all four bytes of the IP address: 60.88.212.164. Choose three-byte comparison if you only need to determine the domain name, not the actual computer name.

Note
If you change this setting after an event has run, you may want to delete existing FastTrends and Content databases to ensure consistent data in future reports.

7. Specify which DNS servers Security Reporting Center uses to resolve IP addresses by editing the DNS Servers List:

   - To add a server to the list, type its IP address in the text box and click **Add to List**.
   - To delete one or more servers from the list, select them in the list and click **Remove from List**.
   - To select all the servers in the list, click **Select All**.
   - To de-select all the servers in the list, click **De-Select All**.

Note
If you leave this list empty, a default server looks up the values.

Setting a Default UnZip Location

Security Reporting Center lets you designate a temporary storage location where compressed log files can be uncompressed. The default UnZip location is configured in the UnZip Location panel in each Reporting module's Options. Unless you enable the default location to be overridden on a per-profile basis, data is stored in the default UnZip location.

When a profile is configured to use compressed log files such as `.zip` or `.gz` files, the Reporting agent requires a directory in which to temporarily store the uncompressed files. The UnZip Location panel lets you specify the temporary directory where compressed log file data can be unzipped. By default, all uncompressed data is stored in this directory, but you can also choose to use a separate UnZip directory for each profile. For more information, see "UnZip Directory" on page 66.

To select a directory for expanding compressed files:

1. In the **Unzip Directory Location** text box, type the path to the directory where you want to store uncompressed files. To maintain separate sub-directories for each profile, use the `%PROFILE%` macro. The `%PROFILE%` macro is automatically replaced by the profile name. Paths beginning with `./` are relative to the ***`installation root`***`/modules/`***`module name`*** directory, where ***`installation root`*** is the directory where Security Reporting Center is installed and ***`module name`*** is the name of the Reporting module.
2. ***If you want to be able to specify a different UnZip directory for each profile***, select the **Allow administrators to configure and override this default setting in each profile** check box. This allows users with full System Admin rights to override the default location of the unzip directory by changing the settings in the UnZip Directory panel when creating or editing a profile.

Re-Ordering Log File Records

If some log file records are out of chronological order, the Reporting agent can put them in the right order during analysis. However, log records that are significantly out of order may indicate a problem that will result in invalid report data. This typically happens when more than one firewall server reports results to the same log file. Re-ordering records also consumes memory, so that a log file with many disordered records may result in degraded performance.

To handle performance problems when records are out of order, the Reporting agent can discard records that are out of order. If a record's time stamp is out of sequence compared to the adjacent time stamps, the Reporting agent checks to see whether the time difference is more than a set number of seconds. If it is, the record is discarded. The time difference between the out-of-order record and the adjacent record(s) is set using the Out-of-Order Records panel in each Reporting module's Log Analysis options.

Note
If you change this setting after an event has run, you may want to delete existing FastTrends and Content databases to ensure consistent data in future reports.

To specify when to delete out-of-order records:

In the text box, type the number of seconds away from the adjacent record that a disordered record must be logged before it is discarded. The default setting is 30 seconds.

Chapter 6

Managing Report Criteria

This section describes some criteria used to categorize data in reports. For example, Security Reporting Center categorizes activity by department. You can define the IP addresses or ranges that make up a particular department to create reports that reflect the structure of your organization.

Departments are sub-groups within your organization identified by domain or IP address ranges. Departments are used in reports to organize information about activity around your firewall. For example, identifying departments might allow you to see differences between Web activity in Sales and Accounting. You can also use departments as an element in filters. For more information about filtering by department, see “Department Filter” on page 204.

Department Management

The Department Management panel lets you view a list of departments that have already been created. You may add, edit, or delete departments from this list

Departments are sub-groups within your organization that can be identified by IP address ranges. Departments are used in reports to organize information about activity around your firewall. For example, identifying departments might allow you to see differences between Web activity in Sales and Accounting. You can also use departments as an element in filters. See “Department Filter” on page 204 for more information about filtering by department.

Notes

- The shared Department Management settings apply to both the Firewall Reporting and Proxy Reporting modules. They can be set in either module.
- If you change Department settings after an event has run, you may want to delete existing FastTrends and Content databases to ensure consistent data in future reports.

To add, edit, or remove departments:

1. Do one of the following:
   - To create a new department, click **Add New Department** and supply the required information in the Add a New Department panel.
   - To edit a department, click the **Edit** icon next to a department in the list and supply the required information in the Add a New Department panel.
   - To delete a department from the list, click the **Delete** icon next to a department in the list.
2. Click **Done** to exit the panel.

Work Hours

You may want to generate reports that separate activity occurring during work hours from activity occurring during non-work hours. The Work Hours panel allows you to define the hours considered to be work hours for your organization.

Note

If you change this setting after an event has run, you may want to delete existing FastTrends and Content databases to ensure consistent data in future reports.

To define work hours:

1. Open a Reporting module and click **Options**.
2. Click **Firewall Reporting** or **Proxy Reporting**.

3. In the **Start** text box, type the time when work hours begin. Use the format `hh:mm` based on a 24-hour clock. For example, for 8:00 AM, type `08:00`.
4. In the **End** text box, type the time when work hours end. Use the format `hh:mm` based on a 24-hour clock. For example, for 5:30 PM, type `17:30`.

Protocols and Protocol Families

A protocol is a set of rules used to send data over the Internet, for example HTTP, FTP, and SMTP. Security Reporting Center reports on activity broken down by protocol and by groups of similar protocols called *protocol families*. Firewall reports show traffic on your network categorized by protocol family: for example, reports show all traffic logged as `pop3`, `smtp`, or `sendmail` as email traffic. Proxy reports use the protocol definitions to distinguish between Web and FTP traffic.

Managing Protocols

You can use the Protocols panel to manage protocols and protocol families. The Protocols panel shows the list of currently configured protocols and the protocol families they are assigned to. A protocol is a set of rules used to send data over the Internet: for instance, http: and SMTP are common protocols. Firewall Reporting module reports break down traffic in your network by protocol, and also by the protocol family associated with that protocol. Proxy Reporting module reports use the protocol definitions to distinguish between Web and FTP traffic.

Note
If you change the protocol settings after an event has run, you may want to delete existing FastTrends and Content databases to ensure consistent data in future reports.

To define a protocol, type the exact text or code as it appears in the log file, and associate it with the appropriate protocol family. For example, traffic logged as `ahttp` is associated with the protocol family `Web`. Protocol families are groups of similar protocols. For more information, see “Managing Protocol Families” on page 118.

To define a protocol:

1. **Open** a Reporting module and select **Options > Protocols**.
2. Click **Add Protocol**.
3. In the **Protocol appearing in log** text box, type the protocol exactly as it appears in the log file, for example `8080/tcp`.
4. Select the protocol family the protocol belongs to. For more information, see “Managing Protocol Families” on page 118.
5. Click **Done** to save the protocol or click **Cancel** to exit without saving the settings.

Managing Protocol Families

The Manage Protocol Families panel lets you add new protocol families and delete existing protocol families from the list of available types. Protocol families are typically associated with a protocol. Each protocol family represents a grouping of protocols. For instance, the protocol family "email" may include the protocols pop-3 and SMTP. You cannot delete a protocol family currently associated with an existing protocol.

You can also use protocol families as an element in a filter.

To add a protocol family:

1. Click **Add**. The **Protocol Family** text box is populated with a placeholder.
2. Edit the placeholder and click **Apply**. The new protocol family is saved to the list.

To remove a protocol family:

Select a protocol family in the list and click **Remove**. You are prompted to confirm the deletion.

Setting Report Defaults

To speed up event configuration, you can use default settings for your events. When you create a profile and save it, Security Reporting center prompts you to create an event. Default events use the default report range and report intervals settings you choose in the Scheduler Options panel. The same settings determine the default report range and the time intervals included when you create events using the Add Event wizard.

The default report range is always an On-Demand Calendar report range with recurring time intervals. To choose a Custom report range for an event, specify it in the Report Range panel of the event settings.

If you do not specify different default settings, the default event uses all the dates in the log file, and the following intervals are included in all reports:

- Daily
- Weekly (USA)
- Monthly
- Quarterly
- Yearly

Default Report Intervals

The Default Report Intervals panel lets you specify the default time intervals that will be used when creating events for On-Demand Calendar reports. For example, select the **Weekly** and **Quarterly** check boxes to make weekly and quarterly reports available. The intervals you set here apply to any new events you create, unless you specify different time intervals in the Report Range panel when creating or editing an event.

To specify the default report intervals:

1. On the left pane of Security Reporting Center, click **Scheduler > Options > Default settings for new events**. The Default Report Range tab is shown.

2. Click the Default Report Intervals tab to decide which intervals of time can be selected on your reports.

3. Select any of the intervals in the list to specify default report intervals. Select as many intervals as you want.

Default Report Range

The Default Report Range panel lets you specify the default date range settings used when creating events. These settings determine the default start and end dates for which log file data is analyzed. They can be overridden for any event by changing the settings in the Report Range panel as you create or edit the event.

These settings are used automatically when you create a default event after saving a new profile. They are also the default settings used for new events created in the Scheduler module.

To set the default report range:

1. For the Report Start Date, select one of the following options:

   - Use a wildcard (`*`) to include log file data from the beginning of the log file on. To include all data up to a certain date, use a wildcard for the Report Start date and choose a specific date or the current date for the Report Stop Date.

   - Use the current date to use the date when the event is created as the start of the log file date range included in reports.

   - Use the following value to choose a specific date after which to include log file data. Use the date format `dd/mm/yyyy`.

2. For the Report End Date, select one of the following options:

   - Use a wildcard (`*`) to include log file data up until the end of the log file. To include all data after a certain date, use a wildcard for the Report End date and choose a specific date or the current date for the Report Start Date.

   - Use the current date to use the date when the event is created as the end of the log file date range included in reports.

- Use the following value to choose a specific date after which log file data will not be included in reports. Use the date format `dd/mm/yyyy`.

Default Report Language and Styles

You can set a default report style and language for all Security Reporting Center reports. The default style and language determine the way new users see on-demand reports, as well as the default settings for creating all new reports. For example, if you want new report users to see reports in German, set the default language to **Deutsch**. Use the default style to choose the look and feel users encounter when they first view a report. Each user can later choose different language and style settings, which are persistent for that user.

To choose report defaults:

1. Open the Administration module and click **Options > Report Defaults**.
2. Select a default language from the list.
3. Select a report style from the list. The default style is **Marshal Default**.

Currency Types

Security Reporting Center is shipped with 33 preconfigured currencies and their corresponding symbols. When you configure Bandwidth Cost in each profile, you select a currency symbol to show the cost of bandwidth in reports.

Using the options in the Reporting modules, you can add currency types to the list.

Note
These shared settings apply to both the Firewall Reporting and Proxy Reporting modules. They can be set in either module.

Any user with System Admin rights can add currencies and edit or delete currencies added to Security Reporting Center. You cannot delete the preconfigured currencies included with Security Reporting Center.

To manage currencies:

1. Open a Reporting module and click **Options > Currency Types**.
   - To add a currency, click **Add Currency** and supply information in the Add Currency Types panel.
   - To edit a currency, click the **Edit** icon next to it and make changes in the Edit Currency Types panel.
   - To delete a currency, click the **Delete** icon next to it.
2. To exit the panel:
   - Click **Save** to save your changes and return to the main Options panel.
   - Click **Cancel** to abandon your changes and return to the main Options panel.

Cisco PIX Interfaces

The Cisco PIX Interfaces panel allows users of Cisco PIX v6.2 and later to specify custom firewall interfaces. When a PIX firewall is configured with more than one interface to a device or network, specifying custom interfaces can make Security Reporting Center reports more meaningful. For example, the firewall may use an interface to a VPN device as well as to the network, or it may connect to more than one network. When you define these interfaces in the Cisco PIX Interfaces panel, Security Reporting Center can parse the device names found in your log files and use them to report more effectively on the direction of traffic through the firewall.

Security Reporting Center automatically recognizes the following standard interface names:

- `inside`
- `outside`
- `laddr`
- `faddr`
- `gaddr`
- `dmz`

You do not need to define these interfaces.

Note
Interface names are case-sensitive.

For more information about configuring Cisco PIX firewalls, see the *Firewall Configuration Guide*.

To create or modify the list of interfaces:

Open a Reporting module and click **Options > Cisco PIX Interfaces**.

- To add an interface, click **Add New Interface**.
- To delete an interface, select its name in the list and click **Remove from list**.
- To select or de-select the entire list, click **Select All** or **De-Select All**.

Chapter 7
Managing Proxy Report Content

The Proxy Reporting module is preconfigured to generate reports that show many statistics about Web activity by users on your network, for example the number of file and page requests logged by the proxy server, the names and URLs of Web pages and sites, the duration of site visits, and the top-level domains accessed. One way to fine-tune report content is to use filters. For more information about filters, see “Managing Data with Filters” on page 189. However, you can also decide how Proxy reports will interpret specific information about Web activity. Settings that affect how the Proxy Reporting module counts and organizes your log file data include the File Types settings, the Domains settings, and the Visitor Sessions settings. See also “URL Categorization” on page 130.

How Proxy Reports Log Traffic

Although Firewall reports track a large variety of protocols in several protocol families, Proxy reports focus on only two protocol families: Web and FTP.

Security Reporting Center may identify a log record with the Web or FTP protocol family based on a scheme such as `https:` or `ftp:`, a port such as `80` or `20`, or a server daemon such as `httpd:` or `ftpd:`. For a complete list of protocols belonging to the Web and FTP protocol families, open a Reporting module and click **Options > Protocols** to view the Protocols panel.

If your proxy server logs protocols that are not included in the list on the Protocols panel, add them to the list as part of the Web or FTP protocol family. For more information about adding protocols, see "Protocols and Protocol Families" on page 117.

File Types

Security Reporting Center can analyze data accessed on the World Wide Web with varying degrees of granularity. The simplest measure of Web activity is hits, which include any kind of data requested from the Web server. A hit can be a request for a simple Web page. However, if the page contains images, dynamic HTML, or other content called dynamically using a script, accessing that page may generate a hit on the server for each item on the page. If each hit counts as a separate page view, your reports may show misleading data, depending on what data you wanted to consider.

You can configure Security Reporting Center to count requests for specific file types accessed on the Web as discrete file downloads and/or as Web page views. You can also set Security Reporting Center to distinguish between files that are created dynamically (in other words, automatically using a script), and those that the user accesses directly. In the settings for each file type, you choose whether to show it in your report counts, and under what conditions.

Note
The same group of options that controls how file types appear in reports also controls which domains are recognized for reporting purposes. For more information, see "Domains" on page 128.

In addition to hits and page views, Proxy reports log data about visits to Web sites. For more information about defining visits, see "Visitor Sessions" on page 129.

Download File Types

The Download File Types panel lets you specify the file types that will be counted as downloads in reports, and whether to count dynamically generated downloads of each type. For example, suppose you want to include actual user downloads of `.WAV` sound files in the Top Downloads report, but you don't want to include `.WAV` files that are dynamically downloaded when accessing a page. You can add `.WAV` to the list of Download File Types, but specify that `.WAV` files will only be included in reports when they are NOT generated by a script or dynamic Web page. Or, suppose you want Security Reporting Center to report on all downloaded `.EXE` files, regardless of whether they were dynamically generated. You can specify that all `.EXE` files should always be counted as downloads and included in reports accordingly.

Note
If you change these settings after an event has run, you may want to delete existing FastTrends and Content databases to ensure consistent data in future reports.

To manage the list of file types that will be counted as downloads in reports:

- To add a file type, click **Add File Type** and provide the required information in the File Type Details panel.
- To edit a file type, click the **Edit** icon next to an entry in the list and edit the information in the File Type Details panel.
- To delete a file type, click the **Delete** icon next to an entry in the list.
- To continue, click another Global Options tab, or do one of the following:
  - Click **Save** to save your settings and return to the Options panel.
  - Click **Cancel** to abandon your settings and return to the Options panel.

Page File Types

The Page File Types panel lets you determine which file types Security Reporting Center tracks in reports that count the number of Web pages viewed. You can also decide whether to report on files of a particular type based on whether they are generated by a script or dynamic Web page. The list of Page File Types determines which types of files are considered to be pages and under what conditions they are included in reports that specify pages. For example, suppose you want all `.EXE` files, including those generated by scripts, to be counted as pages for the purposes of reports. You can edit the definition of a `.EXE` file in the Page File Types list to ensure that every time a `.EXE` file is accessed, whether in a static or dynamic Web page, it counts as a page view.

Note
If you change these settings after an event has run, you may want to delete existing FastTrends and Content databases to ensure consistent data in future reports.

To manage the list of Page file types that will be tracked in reports:

Open the Proxy Reporting module and click **Options > Proxy Reporting**.

- To add a file type, click **Add File Type** and provide the required information in the File Type Details panel.
- To edit a file type, click the **Edit** icon next to an entry in the list and edit the information in the File Type Details panel.
- To delete a file type, click the **Delete** icon next to an entry in the list.

Domains

Proxy reports can show data about Web sites grouped by domain. For example, reports can show whether your users spend most of their time on government Web sites, which use the suffix `.gov`, or on commercial Web sites, which use the suffix `.com`. Some domain types use multiple domain suffixes. Security Reporting Center includes a number of preconfigured domain suffix groupings, including Government, Education, Commercial, and International.

The Domains panel lets you manage the list of top-level domains that will be used to show data grouped by domain in proxy reports. You can determine what domain types are tracked by adding your own domain types, editing the list of suffixes associated with a particular domain grouping, or deleting domain groupings from the list.

Note
If you change these settings after an event has run, you may want to delete existing FastTrends and Content databases to ensure consistent data in future reports.

To manage the list of top-level domains that will be tracked in reports:

- To add a domain, click **Add Domain** and provide the required information in the Domain Details panel.
- To edit a domain, click the **Edit** icon next to an entry in the list and edit the information in the Domain Details panel.
- To delete a domain, click the **Delete** icon next to an entry in the list.
- To continue, click another Global Options tab, or do one of the following:
  - Click **Save** to save your settings and return to the Global Options panel.
  - Click **Cancel** to abandon your settings and return to the Global Options panel.

Visitor Sessions

Proxy reports track each user's Web activity by counting hits, pages, and visits. A visit, also known as a visitor session, begins when a user requests a page or site and ends after a predetermined period of inactivity. The Visitor Sessions panel lets you choose the period of inactivity on the site or page after which Security Reporting Center counts the visit as complete.

Note
If you change this setting after an event has run, you may want to delete existing FastTrends and Content databases to ensure consistent data in future reports.

To set the interval of inactivity after which a visit to a page or site times out:

1. Open the Proxy Reporting module and click **Options > Proxy Reporting**.
2. Click **Visitor Sessions**.
3. Type an interval in minutes in the text box.

URL Categorization

For Proxy reporting, which focuses on the Web traffic generated by internal users, Security Reporting Center provides access to the URL categorization data from the user defined URL Categorization list. This list identifies Internet URLs that may expose the organization to legal liability, detract from employee productivity, and waste bandwidth. Security Reporting Center uses this information to track and report on the categories of Internet content accessed by users in your organization so you can ensure employees do not visit inappropriate Web sites

Note
If you change the URL Categorization settings after an event has run, you may want to delete existing FastTrends and Content databases to ensure consistent data in future reports.

Core Categories

Core Categories include URLs of Internet sites with the following types of content:

- Adult/Sexually Explicit
- Criminal Skills
- Drugs, Alcohol & Tobacco
- Gambling
- Hacking
- Hate Speech
- Violence
- Weapons

General Categories

General Categories include URLs for the following additional categories which, while they may not contain objectionable content, reduce employee productivity:

- Advertisements
- Arts & Entertainment
- Chat
- Computing & Internet
- Education
- Finance & Investment
- Food & Drink
- Games
- Glamour & Intimate Apparel
- Government & Politics
- Health & Medicine
- Hobbies & Recreation
- Hosting Sites
- Job Search & Career Development
- Kids Sites
- Lifestyle & Culture
- Motor Vehicles
- News
- Personals & Dating
- Photo Searches
- Real Estate
- Reference
- Religion
- Remote Proxies
- Search Engines
- Shopping
- Sports
- Streaming Media

- Travel
- Usenet News
- Web-based Email
- Sex Education

Enabling URL Categorization

URL Categorization is enabled individually for each profile. To enable or disable URL Categorization for a profile, use the Categories panel in the profile settings. By default, URL categorization is enabled for all profiles. For more information, see “Categories” on page 70.

Customizing URL Categorization

You can use URL categorization with no further configuration using the sample Categories database included with Security Reporting Center. The sample database is a fully functional database which you can update to the latest version at any time.

You can also customize URL categorization and URL categorization reports to meet your unique business needs. For example, Security Reporting Center lets you:

- Decide how URL categorization reports will categorize IP addresses and different file types
- Create a custom database that allows you to create new categories and assign URLs to them
- Use filters to include and exclude categories and category types from reports
- Map categories to other categories to design reports that focus only on targeted Web surfing issues.

The following table shows where you can find more information about using and customizing URL Categorization. For more information about detailed configuration, including field descriptions, see the Security Reporting Center Help.

To Perform This Task	See:
Enable and disable URL categorization for events associated with a profile	“Categories” on page 70
Create filters to include and exclude specific categories and category types from reports	“Core Category Filter” on page 214 “General Category Filter” on page 216 “Uncategorized Data Filter” on page 218
Decide whether to categorize IP addresses as well as URLs during log analysis	“Categorizing IP Addresses” on page 135
Decide whether to categorize files other than those defined as pages in the Page File Types panel.	“Categorizing Non-Page File Types” on page 135
Create and manage a custom database of URLs and assign them to categories.	“Custom Categorization Databases” on page 136
Create category mappings and mapping groups by assigning existing categories to category mapping groups such as Non-Work-Related.	“Category Mapping” on page 136
Add a category mapping group such as Non-Work-Related to a profile.	“Categories” on page 70

Categorizing IP Addresses

URL categorization tracks the content of pages and sites requested from your proxy server by matching them with content categories in a database. If you choose to categorize IP addresses as well as URLs, you may receive some misleading data, because a single IP address may host several Web sites, each of which contains different content. For example, the same IP address may host a news Web site and a gambling Web site. If you choose not to disable categorization of IP addresses, you should use your categorization reports with caution.

By default, the Proxy reporting module does not categorize IP addresses.

To enable and disable categorization of IP addresses:

1. Open the Proxy Reporting module and click **Options > URL Categorization**.
2. Click the General tab.
3. Select or clear the **Disable categorization by IP** address check box.

Categorizing Non-Page File Types

By default, Security Reporting Center categorizes only the file types defined as pages in the Page File Types panel. This improves performance by limiting the number of separate URLs Security Reporting Center checks against the database and thus the resources consumed by URL categorization. For example, if you have not defined `.GIF` as a page file type, and a user downloads a page with multiple images on it, Security Reporting Center only categorizes the page URL, not the URL for each individual image. If you choose to categorize file types other than page file types, be aware that performance may suffer.

For more information about how to define file types as pages, see “Page File Types” on page 128.

To enable and disable categorization of non-page file types:

1. Open the Proxy Reporting module and click **Options > URL Categorization**.
2. Click the General tab

3. Select or clear the **Only categorize Page File Types** check box.

Custom Categorization Databases

You can create your own categorization database using the Custom Database panel. You can add URLs to the database and categorize them using either the internal categories or categories you create. All custom categories are used to categorize URLs unless they a filter attached to the profile excludes them.

To create a Custom database:

1. Open the Proxy Reporting module and click **Options > URL Categorization**.
2. Click the Custom Database tab.
3. Create a list of URLs by associating each URL with a category and a category type.

For more information, including field descriptions, see the Help.

Category Mapping

Category mapping lets you manage custom groupings of categorization data for your reports by telling Security Reporting Center to report on groups of categories as if they belong to larger ones. When you assign a category mapping group to a profile, you can then focus reports to show data on issues that are important to you. For example, you may want to map a number of categories such as News or Astrology to a larger category called Non-Work Related. The groupings listed in the Category Mapping panel are category mapping groups, which are sets of such mappings.

Select a category mapping group in the Categories panel of the profile settings to create reports that reflect the mappings in the group rather than the many individual categories in your custom databases. Categories that do not belong to the mapping group associated with the profile show up in the report as usual.

Note
Category mapping groups specify groups of categories, and your reports reflect the group rather than the individual categories in the group. If you prefer to specify one or more individual categories or category mappings to include in or exclude from reports, create a Core or General Category filter and apply it to the profile.

For more information, including detailed field descriptions, see the Help for each panel.

Chapter 8

Managing User Access

Because Security Reporting Center can analyze a wide range of information about your enterprise network, it also provides a layered system of user permissions. System and Team Admins can assign varying levels of user access settings to provide useful information sharing while guarding confidential information.

User Rights and Team Rights

User and team rights control two kinds of permissions: permission to create and edit further users and teams, and permission to view, edit, and create reports for specific profiles. Permission to create and edit users and teams is granted in the Administration module User and Team settings. Permission to view or edit each individual profile is granted in the profile settings in the appropriate Reporting module.

Understanding User Rights

A user is an individual with access rights to items within Security Reporting Center. When users are created in the Administration module, they are granted a specific level of permissions to Security Reporting Center objects such as users, teams, and profiles.

Understanding Team Rights

A team is a logical grouping of users that can be assigned access to profiles. Unlike groups of users in some other applications, Security Reporting Center teams have different levels of access depending on each member's role within the team. For example, a team may include customers who have permission to see reports for a single profile, but it may also include a project manager with permission to modify profiles and create events. Team rights apply to users and objects specific to that team. The Teams setting for each profile then determines which teams have access to the profile.

A user with System Admin rights (granted in the user settings) or Team Admin rights (granted in the Team settings) can add members to each team and determine their level of team rights.

The following table briefly defines the rights of each level of team user.

Team User Rights	Add or Remove Members	Create, Edit, or Delete Profiles*	Schedule Events*	View Reports*
Team Admins	X	X	X	X
Team Power Users			X	X
Team Report Users				X

*Capability only applies to profiles to which the team has access.

Adding Users

To give users access to Security Reporting Center, create them with the Users panels in the Administration module. System Admins and Team Admins have the power to add Users to the global Users list. All team members are selected from this global list.

For information about giving individual users access to a profile, see "User Access" on page 58.

To add a user to the system:

1. Open the Administration module and click **Users**.
2. Click **New User**.
3. On the General panel, specify login information for the user and determine what kind of authentication to use for the login. For more information including field descriptions, see “Users: General” on page 141.
4. On the Preferences panel, choose the time zone used to display event run times for this user. For more information including field descriptions, see “Users: Preferences” on page 142.
5. On the Teams panel, choose the teams this user belongs to. For more information including field descriptions, see “Users: Teams” on page 142.
6. On the User Rights panel, choose a level of user rights for the user. For more information including field descriptions, see “Users: User Rights” on page 143.
7. On the Summary panel, review and save the settings for this user.

Users: General

To add basic user information:

1. In the **Login Name** text box, type the name that the user will supply to log in to Security Reporting Console.
2. In the **User Description** text box, type the user’s actual name or other identifying information. For example, type `Jane Doe`.
3. Select an authentication type for the user.
   - Select **Use System Authentication for this user’s password** to require this user to log in using a system password such as a Windows domain password.
   - Select **Use Marshal Authentication for this user’s password** to require this user to log in using the password specified on this panel.

4. ***If you selected Marshal Authentication***, type the user's password in the **New Password** text box. Re-type the password in the **Type Again** text box to verify it.
5. Select the **Disable this account?** check box if you want to prevent the user from logging in to Security Reporting Center.

Users: Teams

The Teams panel lets you specify which teams the current user belongs to. For more information about teams, see

To add or remove a user from a team:

Select the teams to which this user will belong:

To add the user to a team:

1. Click **Add**. The Add User to Teams panel opens.
2. Select or de-select teams.
3. Click **Done** to save your changes, or click **Cancel** to abandon them. You are returned to the main Teams panel.

To add the user to more teams, repeat steps **a**-**c**.

To remove the user from a team:

Select a team name from the list.

Click **Remove**. The user is removed from the team.

Users: Preferences

The User Preferences panel lets you specify the user's default time zone. This time zone is used in the Schedule panel to show the times when scheduled events are set to run.

To specify the time zone preferences for a user:

- ***If you want to use the time zone specified as the system default***, select **Use the system default time zone**.
- ***If you want to specify a different time zone***:
  a. Select **Override the system default time zone**.

  b. Select a time zone from the list.

  Note
  All times are stored in the system as GMT (Greenwich Mean Time). A user in another time zone sees the time translated into the time zone specified in his or her user or team preferences.

To specify when an inactive session times out for this user:

- ***If you want to use the default session timeout interval***, as specified in the Administration options, select **Use the system default session timeout value**. .
- ***If you want to specify a different session timeout interval***:
  a. Select **Select this user's session timeout value**.

  b. Type an interval in minutes from 1 to 9999 in the text box. If the user remains inactive for this number of minutes while running the user interface or viewing on-demand reports, the user session is terminated.

Users: User Rights

The User Rights panel lets you specify access rights for the current user. User rights are granted in addition to the rights users and teams can be granted to specific profiles. The level of rights determines whether the user can view or modify system settings and features, whether the user can create and modify teams and users, and whether the user has access to profiles and events without being granted such rights on a profile-by-profile basis.

To select the level of rights assigned to this user:

- Select **System Admin** to let the user view all events, profiles, users and teams within the system. The System Admin can also view reports and schedule events for any profile.
- Select the **In addition, this user will be able to change all system options** check box to let a System Admin modify all options and profiles.
- Select **User** to let the user view reports and schedule events for profiles to which s/he has access.

Adding Teams

To add a new team, use the Teams panels on the Administration module. For information about giving individual teams access to a profile, see "Team Access" on page 60. After you create a team, you can add more members by editing the team or by editing an individual user's settings.

Users with either System Admin rights (granted in the User settings) or Team Admin rights (granted in the Team settings) have the power to add or edit users and teams. For more information, see "User Rights and Team Rights" on page 139.

To add a user to the system:

1. Open the Administration module and click **Teams**.
2. Click **New Team**.
3. On the General panel, specify a name for the team. For more information including field descriptions, see "Team: General" on page 145.
4. On the Preferences panel, choose the time zone used to display event run times for this user. For more information including field descriptions, see "Team: Preferences" on page 145.
5. On the Teams panel, choose the teams this user belongs to. For more information including field descriptions, see "Team Members" on page 142.

6. On the Team Rights panel, choose a level of user rights for the user. For more information including field descriptions, see “Users: User Rights” on page 143.
7. On the Summary panel, review and save the settings for this user.

Team: General

The team General panel lets you specify the name of a team.

To specify a team name:

In the **Team Name** text box, type an identifying name for the team.

Team: Preferences

The Team Preferences panel lets you specify the default time zone a particular team will use to schedule event run times and the period after which user sessions expire for members of this team.

To specify time zone preferences for a team, do one of the following:

- ***If you want to use the settings specified in User Defaults***, select **Use the system default time zone**. This time zone is used in the Schedule panel to show the times when scheduled events are set to run
- ***If you want to specify a different time zone for users in this team***:
  - **a.** Select **Override the system default time zone**.
  - **b.** Select a time zone from the list. .

Note
All times are stored in the system as GMT (Greenwich Mean Time). A user in another time zone sees the time translated into the time zone specified in his or her user or team preferences.

To specify when an inactive session times out for members of this team, do one of the following:

- ***If you want to use the default session timeout interval specified in the Administration options***, select **Use the system default session timeout value**. .
- ***If you want to specify a different session timeout interval***:
  - **a.** Select **Override the system default for users in this team**.
  - **b.** In the text box, type an interval in minutes from `1` to `9999`. If a user belonging to this team remains inactive for this number of minutes while running the user interface or viewing on-demand reports, the user's session ends.

Team Members

Use the Team Members panel to add users to or delete them from the current team and to assign rights to each user.

To add a user to the team:

1. Click **Add**. The Add Users to Team panel opens.
2. Select or de-select users.
3. Click **Done** to save your changes, or click **Cancel** to abandon them.
4. Repeat the previous steps for each user you want to add.

To remove a user from the team:

1. Select a user name from the list.
2. Click **Remove**. The user is removed from the team.

3. Repeat the previous steps for each user you want to remove.
4. View or change a user's access rights by selecting a user name from the list and selecting one of the following:
   - Team Admin
   - Team Power User
   - Team Report User

Understanding System Defaults for Users

You can choose whether to use system authentication (such as Windows domain authentication) for users logging into Security Reporting Center. If you are running Security Reporting Center on a Solaris system, you can also specify which forms of system authentication to enable.

User Defaults

When you create users and teams, you can choose a time zone for each team, or you can use the Security Reporting Center system default. You can set the system default time zone using the User options in the Options menu. You can also set a default timeout period for user sessions. Individual user or team settings, when they are specified, override the default settings.

If no other default time zone is specified, Security Reporting Center uses the time zone where the User Interface server is installed as the default.

The User Defaults panel lets you specify the system-wide default time zone used to view and schedule event run times. This time zone is used in the Scheduler panels to show the times when scheduled events are set to run. All times are stored in the system as GMT (Greenwich Mean Time). A user in another time zone sees the time translated into the time zone specified in his or her user or team preferences.

This panel also lets you set a system default timeout interval for user and team sessions. You can override these settings on a per-team or per-user basis using the Preferences panel when creating or editing users or teams.

To specify system-wide default settings:

1. Select the default time zone from the list.
2. Type an interval in minutes from 1 to 9999 (inclusive) in the text box to specify the system default session timeout interval. If a user remains inactive for this number of minutes while running the user interface or viewing on-demand reports, the user's session is terminated.

Chapter 9
Managing Your Product Installation

This section discusses how to configure and maintain components of your Security Reporting Center installation.

Enabling SSL

Web clients and Web servers often transmit sensitive information. Networks can protect this information by sending the data in an encrypted form and subsequently decrypting the data on the receiving side. The Secure Sockets Layer (SSL) protocol provides several features that enable secure transmission of Web traffic. These features include data encryption, server authentication, and message integrity.

SSL ensures secure communication from Web clients to Security Reporting Center. SSL is enabled by default for Windows installations. For Solaris installations, it is disabled by default.

To enable or disable SSL:

1. Open the Administration module and click **Options > SSL**.
2. Click **Enable SSL** or **Disable SSL**.
3. Restart the NetIQ Apache Service and the NetIQ Tomcat Service.

With SSL enabled, the URL for connecting to Security Reporting Center takes the format `https://hostname:9000/index.html`. With SSL disabled, the URL format is `http://hostname:9000/index.html`. When you enable or disable SSL, Security Reporting Center automatically updates any Windows shortcuts pointing to the old URL.

Scheduler Agents and Reporting Agents

Scheduler agents are responsible for making sure events happen. When you schedule an event using the Scheduler module, information about the event is logged in the database. A Scheduler agent acting as the Scheduler polls the database for pending events, then assigns tasks to other available agents. Other Scheduler agents learn about those tasks when they in turn poll the database for assigned tasks.

You can view information about each agent computer using the Agents panel in the Scheduler module. Click **Scheduler > Agents** on the left pane of Security Reporting Center.

The Agents Panel

The Agents panel provides system information about the Scheduler agent computers for your Security Reporting Center installation, tells you whether they are enabled to perform common agent functions, and links to panels allowing you to configure these functions. Computers are listed by name and IP address.

The Agents panel provides the following information:

- Information about agent functions (configured in the Agent Settings panel):
  - **Agent** shows whether the Scheduler agent on this computer has been enabled to poll the database for assigned tasks.
  - **Scheduler** shows whether the Scheduler agent has been enabled to poll the database for pending events, decompose them into tasks, and assign the tasks to computers.

  - **Logging** shows whether the Scheduler agent and the Firewall Reporting agent have been enabled to log status messages to files. If the Scheduler agent only is enabled, Logging displays `Event Only`. If the Firewall Reporting agent only is enabled, Logging displays `Agent Only`.

- Information about the host computer:
  - Host name and IP address
  - Total and free RAM
  - Total and free virtual memory
  - Free disk space and largest free disk space
  - Operating system type and version
  - Number of CPUs.

To view the list of status messages logged for a computer, click **View Status History** for that computer.

To enable and disable agent functions on a computer, click **Edit Agent Settings** for that computer.

Agent Settings

You can adjust how often the agent acting as the Scheduler polls the database for pending events as well as how often Scheduler agents poll the database for assigned tasks. You can also enable or disable polling and logging for specific agent computers. To review the functions carried out by the Scheduler agent and the Reporting agent(s), see "Architecture" on page 3.

The Agent Settings panel lets you enable and disable Scheduler and Reporting agent functions for the agents installed on a particular computer. By default, all functions are enabled. To disable an agent function on the current computer, clear the appropriate check box. To enable it, select the check box.

Use the following settings to determine the behavior of the Reporting agent and the Scheduler agent on the current host:

1. Select **Enable Agent** to allow the Scheduler agent on this computer to be assigned tasks. Clearing this check box disables the Scheduler agent so the Scheduler cannot assign it tasks. As a result, the Reporting agent installed on this computer cannot run tasks.

2. Type a value in the **Concurrent Tasks for Agent** text box to determine how many tasks the agent can run at one time. The default value is `2`. Keep in mind that running many tasks concurrently slows performance.

3. Select **Enable Scheduler** to allow this agent to take on the role of the Scheduler, which divides pending events into tasks and assigns them to available Scheduler agents. Clearing this check box disables the Scheduler function so the Scheduler agent cannot act as the Scheduler.

4. Select **Enable logging of status messages to a local file for the Scheduler agent running on this host** to enable status message logging for the Scheduler agent installed on this computer. This setting enables the status log generated in the *`installation directory`*`\modules\agent\log` folder.

   Note
   This setting does not affect logging for *`installation directory`*`\modules\agent\wtxd.err`.

5. Select **Enable logging of status messages to a local file for the Reporting agent(s) running on this host** to enable status message logging for the Reporting agent installed on this computer. This setting enables the status logs generated in the *`installation directory`*`\modules\firewall\log` folder and the *`installation directory`*`\modules\proxy\log` folder.

   Note
   To run multiple tasks, you need multiple task licenses. For more information about task licenses, see “Licensed Tasks” on page 24.

Stopping the Agent Service

When you disable an agent using the Agent Settings panel, its agent functions are disabled, but the agent continues to run as a service on the local computer. The NetIQ Scheduler Agent service can only be stopped permanently from the local computer.

When the NetIQ Scheduler Agent service stops communicating with the database (because the service is stopped, or because the computer is powered off), all agent functions stop. The Agents panel shows the following message:

```
The agent service on this host has stopped responding.
```

After the NetIQ Scheduler Agent service has been stopped for one hour, the computer is removed from the list on the Agents panel. When the service is restarted, the computer is displayed on the Agents panel again.

To adjust agent polling frequency:

1. Open the Scheduler module and click **Options > Global Agent Settings**.
2. Click the Agent Polling tab.
3. Set how frequently Scheduler agents poll the database for assigned tasks by typing the number of seconds in the text box. The default is every 10 seconds.
4. Set how frequently the agent acting as the Scheduler polls the database for pending report events by typing the number of seconds in the text box. The default polling interval is every 10 seconds.

Default Operating System

If your Security Reporting Center installation is installed in an environment that includes both Windows and Solaris computers, the OS Binding Default panel lets you choose the default operating system where events will run. It also lets you choose whether the operating system for events can be specified separately for each profile. If you choose to enable this per-profile option, an OS Binding panel is available when creating a new profile or when editing any existing profile's settings.

To choose the default operating system for firewall profiles:

1. Open a Reporting module and select **Options > Log Analysis**.
2. Click the OS Binding Default tab.
3. Select one of the following options to decide how event tasks will be assigned to agent computers by default. This setting applies to all events, unless you select the **Allow per-profile settings** check box on this panel.
   - **All Operating Systems** Select this option if you want events to run on the first available agent computer, regardless of operating system.
   - **Windows** Select this option if you want events to run only on agent computers with a Microsoft Windows operating system.
   - **Solaris** Select this option if you want events to run only on agent computers with a Sun Solaris operating system.
4. ***If you want to be able to override the default operating system setting on a per-profile basis using the OS Binding panel***, select the **Allow per-profile settings** check box. Clear the check box if you want the default setting to apply to all events.

Host Groups

In a distributed installation, you can choose to limit the set of computers where Scheduler agents can assign tasks by designating groups of computers called host groups. Create host groups using the Host Groups panels in the Scheduler module.

Use host groups to manage resources in a distributed installation. If you need to analyze firewall logs of different sizes, for example, you may want Security Reporting Center to process them using agent computers with enough resources to handle them efficiently. If you create a host group containing only the computers capable of analyzing large log files, you can assign profiles for large logs to this group.

You can select a host group as the default for all profiles or specify a host group on a per-profile basis. For more information about selecting a default host group for all profiles, see “Host Binding Default” on page 155. For more information about selecting a host group for an individual profile, see “Host Binding” on page 68.

By default, “all hosts” is the host group setting for all profiles.

Host Binding Default

The Host Binding Default panel sets a default group of computers where events run. This setting applies to all profiles, unless you choose to override the default setting on a per-profile basis. For information about configuring the host group setting for an individual profile, see “Host Binding” on page 68.

The Host Binding Default panel lets you choose the default group of computers where events will run. It also lets you choose whether the host group where events run can be specified separately for each profile. If you choose to enable this per-profile option, the Host Binding panel is available when you create a new profile or edit an existing profile's settings.

To create a host groups, use the Host Groups panel in the Scheduler options. Specifying host groups can be useful for allocating system resources. For example, you may want to assign profiles for large log files to run events only on hosts with the resources to handle them efficiently.

To choose the default host group for all profiles:

1. Open a Reporting module and select **Options > Log Analysis**
2. Click the Host Binding Default tab.
3. Select a host group from the list.
4. ***If you want to be able to override the default host binding setting on a per-profile basis using the Host Binding panel***, select the **Allow per-profile settings** check box. Clear the check box if you want the default setting to apply to all events.

5. Select another Options panel, or do one of the following:
   - Click **Save** to save your changes and return to the main Options panel.
   - Click **Cancel** to return to the main Options panel.

Email Settings

Security Reporting Center can automatically send static reports in HTML, Microsoft Word, Microsoft Excel, Adobe PDF, or CSV format to a specified address. For information about how to configure a static report to be sent as an email attachment, see "Report Parameters and Destination" on page 84.

The Email Settings panel lets you specify an email server as well as sender and reply addresses for sending static reports by email. You can also specify a subject line. The email subject line determines the name of the `.ZIP` file containing the report.

Note
Only Windows computers support MAPI mail. If your Security Reporting Center installation contains Solaris computers, use SMTP mail to email reports.

To send reports using SMTP mail:

1. Select **Use SMTP mail delivery**.
2. In the **SMTP Server** text box, type the host name or IP address of the SMTP server.
3. In the **From Address** text box, type the address you want to appear in the From field of the email message when the report is sent.
4. In the **Reply-to Address** text box, type the address you want to appear in the Reply-to field of the email message when the report is sent.
5. In the **Email Subject line** text box, type the subject line you want to appear when the report is sent. For example, type `Firewall Report`.

6. Click **Save** to save your changes, or click **Cancel** to abandon your changes and return to the main Options panel.

To send reports using MAPI mail:

1. Select Use MAPI mail delivery.
2. In the **Profile** text box, type the name of the MAPI profile that will be used to send mail.
3. In the **Password** text box, type the password associated with the profile.
4. In the **Email Subject line** text box, type the subject line you want to appear when the report is sent. For example, type `Firewall Report`.
5. Click **Save** to save your changes, or click **Cancel** to abandon your changes and return to the main Options panel.

Checking for Updates

The Check for Update panel lets you check for an updated version of Security Reporting Center. It also lets you disable reminders about updated versions that are shown when you log in to Security Reporting Center.

To register for an updated version and download it from the World Wide Web, click **Get Update**. The **Get Update** button is not displayed unless an updated version of Security Reporting Center is available.

By default, Security Reporting Center alerts you to new versions of the product each time you start the application unless you have already downloaded the updated version. You can disable the reminder in this panel. To disable reminders about updates, select the **Disable update notifications at startup** check box. Clear the check box to see reminders of updates.

Chapter 10
Managing Databases

This section describes how to maintain databases by limiting their size, and how to configure locations and settings when installing a distributed installation or changing an existing installation.

Database Consistency

When you change certain profile settings, for example the addresses behind the firewall and the filters applied to the profile, Security Reporting Center prompts you to delete the FastTrends and Content databases for the profile to avoid creating reports based on misleading data. You are also reminded to consider rebuilding databases whenever you change certain settings in the Options panels for each module. In this case, manually delete the databases using the FastTrends and Content Database Management options and re-run the events associated with the profile to create new databases.

Changing any of the following Options settings may result in invalid data if you do not rebuild the databases:

- Out-of-Order Records
- Work Hours
- Global Filters
- Department Management
- Protocols
- Domains
- Download File Types
- Page File Types
- Visitor Sessions

Managing FastTrends Databases

FastTrends is technology that efficiently stores analyzed log file data. Using FastTrends to store log data that has already been analyzed significantly improves performance when analyzing logs the second time. For example, when you generate a report on Monday, Monday's data is stored in the FastTrends database. If you run a report using the same profile for Monday and Tuesday, only the data for Tuesday needs to be analyzed. As you run events, the results are continuously stored in the FastTrends database. This process occurs in the background and does not interfere with the use of your system. Each profile uses a separate FastTrends database.

Security Reporting Center provides several methods for managing your FastTrends databases and limiting the disk space and memory they use.

- You can choose one default location for your FastTrends databases or specify a different location for each profile's FastTrends data. For more information, see "FastTrends Location" on page 160.
- You can mark specific FastTrends databases and date ranges for deletion using the FastTrends Database Maintenance options. For more information about marking records for deletion, see "Delete Database Information" on page 161.

- The daily FastTrends Database Maintenance event automatically deletes FastTrends databases for deleted profiles as well as any FastTrends records you have marked for deletion. You can set the event to run at a time you choose or run it automatically. For more information, see “FastTrends Database Maintenance Event” on page 163.
- You can limit the size of individual tables in FastTrends databases. For more information, see “Limiting FastTrends Memory Usage” on page 164.

FastTrends Location

The FastTrends Location panel lets you specify the default location of the FastTrends databases for each profile. This panel also allows you to determine whether the FastTrends default location can be changed for individual profiles. If you do not allow administrators to make changes to the FastTrends database location, the FastTrends panel will not appear in the profile configuration panels, and all profiles must use the same FastTrends location.

To specify where the FastTrends database will be stored:

1. In the **Database Directory** text box, type the path to the FastTrends database. Put a backslash at the beginning of the path to make it relative to the Security Reporting Center installation directory.
2. Use the `%PROFILE%` macro instead of a profile name if you want to maintain separate databases for each profile.
3. Select the **Allow Administrators to configure and override this default setting in each profile** check box to allow separate FastTrends database settings for each profile. Clear the check box if you want the same FastTrends directory to be used for all profiles.

Deleting FastTrends Databases

One way to manage database size is to delete FastTrends databases periodically. Use the Delete Database Information panel to mark records for deletion by flagging them in the database. The built-in FastTrends Database Maintenance event deletes all the flagged records daily for all profiles. In addition, each time you run an event the FastTrends Database Maintenance event runs before the analysis task begins. This deletes any flagged FastTrends records for the associated profile.

For instructions for marking records for deletion, see “Delete Database Information” on page 161. For more information about FastTrends databases, see “FastTrends Directory” on page 64.

Delete Database Information

When you use the Delete Database Information panel to mark FastTrends records for deletion, records are flagged in the database. Security Reporting Center deletes the flagged database records the next time the daily FastTrends Maintenance Event runs, or the next time an analysis task for the profile runs, whichever happens first. For information on how and when FastTrends records are deleted, see “FastTrends Database Maintenance Event” on page 163.

To delete information from FastTrends databases:

1. Open a Reporting module and click **Options** on the left pane.
2. Click **FastTrends Database Management**.
3. Click the FastTrends Maintenance tab.
4. In the Profiles list, select the profile associated with the database(s) that you want to delete.
5. Click **Manage Databases for Selected Profile(s)** to open the Delete Database Information panel showing the FastTrends databases for the selected profile.

6. Select the information to be marked for deletion, using one of the following methods.

   – To delete specific days from the FastTrends database for this profile, click **Delete individual days**.

   – To delete all the FastTrends database information for this profile, click **Delete all days**.

   – To delete all the days before a certain date, click **Delete all days before** and type a date in the text box using the format `dd/mm/yyyy`. For example, for June 20th, 2001 type `06/20/2001`.

   – To delete all the days after a certain date, click **Delete all days after** and type a date in the text box using the format `dd/mm/yyyy`. For example, for June 20th, 2001 type `06/20/2001`.

   – To delete all the days between two dates, click **Delete all days between** and type a date in each text box using the format `dd/mm/yyyy`. For example, for June 20th, 2001 type `06/20/2001`.

   – To cancel all the deletions you specified, click **Clear all deletions**.

7. Click **Done** to close the panel. If you did not specify any information for deletion, no information will be deleted.

8. Click another Options tab, or do one of the following:

   – Click **Save** to save your changes.

   – Click **Cancel** to return to the main Options panel.

For more information about the FastTrends Database Maintenance Event, see "FastTrends Database Maintenance Event" on page 163.

FastTrends Database Maintenance Event

The FastTrends Database Maintenance Event runs once per day. It deletes any FastTrends Maintenance records that you have marked for deletion, as well as any FastTrends databases generated by profiles that were subsequently deleted. The daily FastTrends Database Maintenance Event performs deletions for all profiles. The FastTrends Database Maintenance Event also runs before each event is run, deleting only marked FastTrends databases for the profile associated with that event.

The FastTrends Database Maintenance Event panel lets you determine when the FastTrends Database Maintenance event runs and whether it automatically deletes old data in FastTrends databases. To enable the FastTrends Database Maintenance Event to automatically delete outdated records, specify the deletion interval on this panel.

To configure the FastTrends Database Maintenance event:

1. Open a Reporting module and click **Options > FastTrends Database Management**.
2. Click the FastTrends DB Maintenance Event tab.
3. To enable automatic deletion, select the **Enable Auto-Delete feature** check box.
4. In the **Delete all log data time-stamped more than *x* days ago** text box, type the number of days after which FastTrends databases should be deleted. The age of the data is determined based on the time stamps in the original log file from which FastTrends is derived, not the age of the FastTrends database.
5. To specify the time when the daily FastTrends Database Maintenance Event runs, type the time when you want the event to run in the **Run at** text box. Use the format `hh:mm` and the 24-hour clock. For example, for 3:15 PM, type `15:15`.
6. If you want the event to be added to the event queue as soon as you save your changes to the panel, click **Queue Event Now**.

Limiting FastTrends Memory Usage

If you use Security Reporting Center to analyze large log files and you need to improve performance, one approach is to limit the size of the tables in the FastTrends database. The Memory Usage panel lets you choose individual tables and limit the number of unique elements per table, reducing the size of the data stored in FastTrends. The list shows the tables used by reports in this module, how much memory they use (in MB), and the maximum number of elements they contain. If performance is suffering, use this panel to set a new maximum number of unique elements for tables that are hogging resources. You can learn which tables are using the most memory by consulting the Analytical Statistics chapter in the report for each profile.

This setting controls memory usage in two ways. During the analysis task of an event, when data is transferred from the log file to a FastTrends database, this setting limits the number of elements that can be written to FastTrends for this table per day. During the export task, it trims the total number of elements accumulated per report interval (week, month, or year) for this table before FastTrends data is exported to the Content database. For example, if you specify 40 elements, each day of FastTrends data can store only 40 unique elements. If you are reporting on weekly intervals, the total number of elements accumulated in seven days of FastTrends data is then trimmed to the limit of 40 before export is completed.

To edit the maximum number of unique elements in a table:

1. Open a Reporting module and click **Options > Firewall or Proxy Reporting > Memory Usage.**
2. Click the **Edit** icon next to a table and use the Edit Memory Usage panel to choose limits for any tables that are using too much memory.
3. Click **Done** to return to the Memory usage panel.

FastTrends Database Location

FastTrends databases can reside on any computer, and unlike Content databases, they do not need to reside on the same computer as a Database server. If Security Reporting Center is installed in a distributed environment, you should locate the FastTrends databases on a file server, so that all Security Reporting Center agents can access the databases. Each FastTrends database is associated with a particular profile. However, events associated with a profile can run on different computers, so all the computers in the installation need access to the FastTrends database.

To select the default location of the FastTrends database, use the FastTrends Location panel in the FastTrends Database Management options.

For information about configuring the FastTrends database location for each profile, see "FastTrends Directory" on page 64.

Managing Content Databases

Security Reporting Center uses FastTrends databases to store compressed forms of log files. Using FastTrends to store log data that has already been analyzed significantly improves performance when analyzing logs the second time.

Security Reporting Center provides several methods for managing your Content databases and limiting the disk space and memory they use.

- The daily Content Database Maintenance event automatically deletes Content database records for deleted profiles as well as any data you have marked for deletion. You can set the event to run at a time you choose or run it automatically. For more information, see "Content Database Maintenance Event" on page 166.
- You can use a single Content database to store all your report-ready data, or you can use several Content databases on one or more computers. For more information about configuring and managing Content databases in multiple locations, see "Content Database Locations" on page 167.
- You can limit the size of tables that can be exported to the Content database. For more information, see "Limiting Content Database Table Size" on page 169.

Content Database Maintenance Event

You can limit the amount of data stored in the Content databases by setting the Content Database Maintenance Event to delete data older than a specified date. Specifying data for deletion flags it in the database. The specified data is deleted the next time the daily Content Database Maintenance event runs, or the next time an analysis task for the profile runs, whichever happens first.

The Content Database Maintenance panel lets you determine when the daily Content Database Maintenance event runs and whether it automatically deletes old report data. The Content Database Maintenance event is a built-in event that deletes flagged records daily for every profile. Data is marked for deletion when a profile is deleted or when certain settings are modified, causing report data in the Content database to become obsolete. Data is deleted the next time the daily Content Database Maintenance event runs, or the next time an analysis task for the profile runs, whichever happens first.

To enable automatic deletion of Content databases created before a certain date:

1. Select the **Enable Content database maintenance** check box.
2. In the **Delete all report data older than** text box, type the date after which data in Content databases should be deleted.

3. To specify the time when the daily Content Database Maintenance event runs:

4. In the **Run at** text box, type the time when you want the event to run. Use the format `hh:mm` and the 24-hour clock. For example, for 3:15 PM, type `15:15`.

5. ***If you want the event to be added to the event queue as soon as you save your changes to the panel***, click **Queue Event Now**.

Content Database Locations

If you have installed more than one Database server, you can configure multiple Content databases for your Security Reporting Center installation. Using more than one Content database can improve system performance when analyzing large amounts of data or running large numbers of simultaneous tasks.

A Content database is the database from which Security Reporting Center generates reports. After log file data has been analyzed and compressed for storage in the FastTrends database, report-ready content is exported from the FastTrends database to the Content database, where it can be quickly accessed and rendered into reports. Security Reporting Center Content databases use a built-in MySQL database.

The Content Database Locations panel displays the current list of Content database locations and lets you add, edit, and delete database locations. It also lets you specify which database location will be used by default for all Firewall profiles and whether all profiles must use this default location, or whether content database locations can be assigned on a profile-by-profile basis.

Use the Content Database Locations panel for the following operations:

- To add a Content database, click **Add Content Database Location**. In the Configure Content Database panel, supply definitions for a new Content database location. For detailed field descriptions, see “Content Database Configuration” on page 168.

- To edit the location settings for a database, click the **Edit** icon next to the location you want to edit. In the Configure Content Database panel, edit the definitions for the current Content database location. For detailed field descriptions, see “Content Database Configuration” on page 168.

- To delete a database location, click the **Delete** icon next to the location you want to delete.
- To mark a database location as the default location for new profiles, click **Default** next to the location.
- To allow per-profile Content database location settings, select the **Allow System Admins to configure and override this default setting in each profile** check box. When you enable this setting, the Content Database panel is available when you add or edit a profile. You can use the default Content database location or select a different Content database location for the profile.

Content Database Configuration

Content databases store report-ready information to allow efficient report generation. Security Reporting Center Content databases use a built-in MySQL database.

The Content Database Configuration panel lets you configure the connection parameters for a Content database. Each Content database location corresponds to the location of a Database server.

To configure a Content database location:

1. Open a Reporting module and click **Options > Content Database Management**.
2. Click the Content Database Locations tab.
3. Click **Add Content Database Location**. The Configure Content Database panel opens.
4. In the **Description** text box, type a short description that will be used to identify the location in the Content Database Locations panel.
5. In the **Content Database Server** text box, type the host name or IP address of the computer where the Database server for this Content database has been installed.
6. In the **Server Port** text box, type the port number the Database server is configured to listen on. This is the port number that was specified for the Database server during installation.

7. In the **Logical Database Name** text box, type the database name. The logical database name must include the `%PROFILE%` macro.

8. In the **Database Username** text box, type the user name used to connect to the Database server. This is the user name specified during installation.

9. In the **Database Password** text box, type the password used to connect to the Database server. This is the password specified during installation.

10. Click **Test Connectivity** to see if your current settings allow you to connect to the database.

11. Select the **Create new Content database** check box to overwrite existing database settings. This check box is grayed out when you create a new database.

Limiting Content Database Table Size

To reduce the size of the tables in the Content database, Security Reporting Center can set the maximum number of rows of data per table exported from a FastTrends database to the Content database during the export task of an event. Unless you enable the default setting to be overridden on a per-profile basis, this maximum setting applies to all the profiles associated with the current module.

The Content Database Table Size Default panel lets you specify the default maximum table size for the Content database. It specifies the maximum number of records per table that can be exported to the Content database. When exporting report-ready content to the Content database, you may want to save disk space by limiting the number of records that are exported to and stored in the Content database tables. You can also use this panel to specify whether all profiles must use the default table size setting, or whether the setting can be assigned on a profile-by-profile basis.

For information about setting the Content database table size for an individual profile, see “Content Database Table Size” on page 69.

To set the maximum table size:

1. In the **Content Database Table Siz**e text box, type the maximum number of records per table that can be exported to the Content database.
2. ***If you want users with System Admin rights to be able to specify maximum table size on a profile-by-profile basis***, select the **Allow System Admins to configure and override this default setting in each profil**e check box. When you enable this setting, the Content Database Table Size panel is available in the New Profile wizard when you create or edit a profile. You can choose the default setting or select a different setting for the profile.

Changing MySQL Login Information

If you change the user name or password for your MySQL database after you first install Security Reporting Center, you need to replicate these changes across your installation so that your Security Reporting Center program components can log in to the database.

To change your database login information:

1. Use the MySQL command line or a third-party tool such as MySQL-Front to change the database user name and password.
2. Update the user name and password values in the following files:
   - `agent.conf` in the *`installation directory`*`\modules\agent` directory
   - `lea_service.ini` in the *`installation directory`*`\modules\leaservice` directory
   - `syslog_service.ini` in the *`installation directory`*`\modules\syslogservice` directory
3. Restart the NetIQ Scheduler Agent service, the NetIQ LEA Service, and the NetIQ Syslog Service to rewrite the files and encrypt the new values.
4. In the *`installation directory`*`\common\uiserver\WEB-INF` directory, open `web.xml`.

5. Update the following parameters with the new user name and password:

   `WtSchedJdbcUsername`

   `WtSchedJdbcPassword`

6. Change the value of `WtSchedJdbcEncrypted` from `true` to `false`.

7. Restart the Tomcat service to rewrite the file and encrypt the new values.

8. Open each of the Reporting modules and select **Options > Content Database Management**.

9. Use the Content Database Locations tab to edit the database user name and password for each affected database.

Chapter 11
Using Reports

This chapter gives an overview of how to access and use the three types of reports generated by Security Reporting Center. For more detailed help with reports, use the Help accessible from your on-demand reports.

On-Demand Reports

Security Reporting Center generates interactive HTML reports called on-demand reports. You access these reports through the Security Reporting Center user interface. When you click the **View Report** icon next to a profile name in the Scheduler module or in a Reporting module, you are accessing the on-demand report interface, which is a gateway to all the reports generated for that profile.

On-demand reports, as their name suggests, can be generated at any time and are fully interactive. This means that you can customize the report at any time by selecting the date and time-span covered by the report. It also means that when you re-generate the report after an event has run, you see new and updated information.

Configuring an On-Demand Report

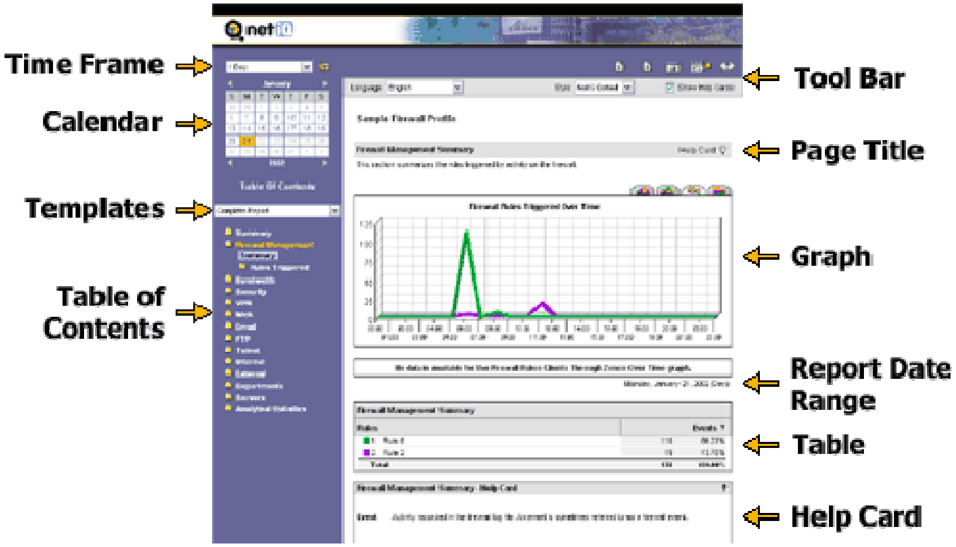
Report parameters such as date range and report intervals are configured in the Scheduler module as part of event configuration. If you want to change the default report range and intervals (for instance, if you want only daily report intervals to be used by default) you can change them in the Scheduler options under **Default settings for new events**.

Custom reports let you specify any single or recurring time interval rather than the set of recurring intervals available for all on-demand reports. Choose Custom in the Report Range panel to generate a custom on-demand report. To review how to configure reports, see “Report Range” on page 80 and “Report Parameters and Destination” on page 84.

Using the On-Demand Report Interface

The on-demand report interface is a report access gateway. When you click the **View On-Demand Report** icon in the list of profiles or the list of events, you can access all the on-demand reports generated for a profile. Multiple events can be configured to generate reports for the same profile. For example, one event may run daily to generate daily reports, while another runs once a month to generate monthly reports on the same profile.

The following diagram shows the layout of a report and its configuration areas.



Choosing Report Chapters

Click the folder links at the left of any report to access specialized report chapters. For example, the Bandwidth report chapter shows a collection of report pages on bandwidth costs.

Choosing a Time Interval

By default, each report shows data for a single day. Use the list to view the data for a different time interval. For instance, if you want to see data presorted by month, select **1 Month**. To see all possible data in the report, select the largest possible time interval. If you selected the **1 Month** interval, for example, and no critical events were logged during the currently selected month, the Critical Events report chapter shows no data. Selecting **1 year** captures all data in the year. You can drill down month by month to discover when critical events occurred.

To see a different interval (for example, a different week for a weekly report) use the report calendar. Unavailable intervals or dates indicate that there is no report data for that interval.

Choosing a Different Language

To see the report in a different language, choose a language from the list using the tool bar.

Converting On-Demand Reports to a new Format

You can convert on-demand reports to Microsoft Word, Microsoft Excel, Adobe PDF, or CSV format on the fly. These reports show the same information found in on-demand reports

To generate a different format for an on-demand report:

1. Click the **Export to MS Word, MS Excel, CSV or PDF** icon at the top of the report.
2. From the Report Content list, choose the contents of the report.
   - To create a report containing only the current page, select **Current page only**.
   - To create a report containing all reports for the profile, select **All chapters, sub-chapters and pages in the complete report**.
3. Select a format for the report.
4. Click **Generate Report**. You are prompted to download the latest version of the NetIQ Document Utility, which converts the `.wtw` file into the format you selected.

Static HTML Reports

Static HTML reports can be configured when you select a Custom Report date range in the Report Range panel. These reports are generated once, and all the associated images and files that constitute each HTML-based report are then saved to a user-defined location and/or sent as an email attachment. To open the report, navigate to this location and open the file.

Static HTML reports are configured in the Report Range panel when you create an event. If you clicked **Custom** in that panel and selected the **Static HTML** check box in the Report Destination panel, you can retrieve the report from the folder you specified in the Report Destination panel.

For detailed information about creating static HTML reports, see “Static HTML Report” on page 85.

Note
Save the report to a relative path on a networked drive to enable easier access to the reports, especially when multiple users require access. If you use an absolute path such as `c:\Firewall_Reports\default.html`, the files and images will actually be stored in the `c:\Firewall_Reports` directory on the server that renders the reports. You must then connect to that server and navigate to the report to view it.

Static Word, Excel, PDF, and CSV Reports

Static reports in the following formats are available when you select a Custom date range in the Report Range panel:

- Microsoft Word
- Microsoft Excel
- Adobe PDF
- Comma-separated value (CSV)

Security Reporting Center generates a static report once and then saves it to a user-defined report location or sends it as an email attachment. These static reports look similar to On-Demand reports that have been converted to a new format, but they are generated automatically for a custom range and in a custom location. The initial output for a static Word, Excel, PDF, or CSV report is a `.WTW` file. When a user with the document utility installed opens the .wtw file, the NetIQ Document Utility converts it to the correct format.

For more information about creating static reports, see “Static Word, Excel, PDF, and CSV Reports” on page 87.

Note
Save the `.WTW` file to a relative path on a networked drive to enable easier access to the reports, especially when multiple users require access. If you use an absolute path such as `c:\Firewall_Reports`, the files and images will actually be stored in `c:\Firewall_Reports` on the server that renders the reports. You must then connect to that server and navigate to the report to view it.

To access a static Word report:

1. If you have not already installed it, download the NetIQ Document Utility. When you configure or edit the destination for a static Word report, the Report Parameters and Destination panel contains a link for downloading this utility. To use the Document Utility, you need Microsoft Office 97 or later installed on a Windows operating system.

2. In the folder you specified in the Report Parameters and Destination panel, double-click the `.WTW` file containing your report. The NetIQ Document Utility converts the file to the appropriate format and opens it

Understanding Report Templates

You can choose the *chapters* for a report by applying a *template*. A chapter is a single page of report content. A template is a collection of chapters. For example, a Bandwidth template includes the following folders:

- General Statistics
- Summary
- Top Internal Addresses
- Protocols
- Outgoing Traffic
- Incoming Traffic

You can use templates to focus on a particular area of interest within the scope of a report. For example, you can create or select a template that contains reports related to an issue such as bandwidth or a particular protocol family such as Telnet. The chapters included in a template are drawn from the chapters within the larger report for the module. For example, templates for firewall reports can only contain chapters within the Complete Report template for the Firewall Reporting module. To create a template that includes chapters dealing with URL categorization, create the template in the Proxy Reporting module.

When using on-demand reports, you can select any available template on the fly. By default, Security Reporting Center displays the report with the template Complete Report when a new user accesses an on-demand report. When the same user launches the report again, the template setting persists and Security Reporting Center displays the report with the last template that the user applied.

For static reports, the template determines which chapters the report document includes. You can select the report template for a static report in the Report Parameters and Destination panel when creating an event.

Creating Report Templates

Security Reporting Center supports the creation of single-level templates. You can choose any number of chapters to group in a report template. However, you cannot create templates with sub-groupings.

To create a report template:

1. Open a Reporting module and click **Templates**.
2. Click **New Template.**
3. On the General panel, provide a name for the template. For more information, see "Template: General" on page 180.
4. On the Content panel, select the chapters to include in the template. For more information, see "Template: Content" on page 181.
5. On the Summary panel, review and save the settings for this template.

Template: General

Use the General panel to assign a descriptive name to a report template. A template tells Security Reporting Center what grouping of report chapters to include in a report, so that you can tailor any report to an audience or focus it on a particular business need or concern. You can change the report template for an on-demand report dynamically by selecting a new template from the menu. You can change the template used for a static Microsoft Word or HTML report by selecting a template on the Report Destination panel before you run an event.

By default, Security Reporting Center uses a template that includes all chapters and pages.

To specify a name for a template:

1. Open a Reporting module and click **Templates**.
2. Click the **Edit** icon next to a style and click the General tab.
3. In the **Template Name** text box, type a descriptive name for the template. This name identifies the template on the main Templates panel and in selection lists.

Template: Content

The Content panel lets you choose which report chapters are included in each template by editing a list.

A chapter is a single page of report content.

To specify the chapters for a template:

Edit the list of chapters by adding or deleting report chapters or moving them up and down in the list. In a completed report, chapters are displayed in the order you choose here.

- To add a new chapter, click the **New Chapter** icon.
- To delete a chapter, click it to select it and click the **Delete** icon.
- To move a chapter up or down in the list, click it to select it and click the Up or Down arrow.

Understanding Report Styles

Report styles let you design a look and feel for your reports by choosing unique colors, fonts, and images. A custom report design allows you to create special-purpose reports. For example, you may need to create reports with your company colors and logo so that report viewers outside the company can instantly recognize your company branding. If you plan to create reports for several customers, you can provide each one with a unique and recognizable style. Or you can use different and distinct styles to quickly differentiate confidential HR reports from security reports.

When you create a report style, you can specify colors using either hexadecimal notation or Security Reporting Center's color selector, which includes the full range of Web-safe colors. Security Reporting Center stores color and font information in a cascading style sheet, which can then be applied to any report. You can select any report style on the fly while viewing an on-demand report. To select a style for a static HTML report, use the Report Parameters and Destination panel when you create or edit an event. For more information, see "Report Parameters and Destination" on page 84.

Creating a Report Style

To create a report style:

1. Open a Reporting module and click **Options > Reporting Styles**.
2. On the General panel, provide a name for the style, decide where the `.css` file will be stored, and select banner images. For more information, see "Report Style: General" on page 183.
3. On the Base Text panel, select a font and color for the text used in report descriptions, tables, the calendar, and the Table of Contents. For more information, see "Report Style: Base Text" on page 184.
4. On the Heading Text panel, select a font and color for the text used in the report title, section titles, tables and column headings. For more information, see "Report Style: Heading Text" on page 185.

5. On the Page Background Color panel, select the background color for the main report page, which is shown in the right pane of each report. For more information, see "ToReport Style: Page Background Color" on page 185.

6. On the Bar Background Color panel, select the background color for the toolbar and navigation bar, which wraps around the left and top of each report page. For more information, see "Report Style: Bar Background Color" on page 186.

7. On the Primary Selection Color panel, select the color that will be used to highlight a first-level selection in the report. For more information, see "Report Style: Primary Selection Color" on page 186.

8. On the Secondary Selection Color panel, select the color that will be used to highlight a second-level selection in the report. For more information, see "Report Style: Secondary Selection Color" on page 187.

9. On the Summary panel, review the settings for the current report style.

Report Style: General

Use the General panel to assign a name to a group of report style settings, choose a file name for the cascading style sheet Security Reporting Center creates to save the settings, and choose a banner or other logo to identify the report style with recognizable visual elements such as a brand or company.

To specify a style name and banner images for a report style:

1. Open a Reporting module and click **Options > Reporting Styles**.

2. Click the **Edit** icon next to a style and click the General tab.

3. In the **Style Name** text box, type a descriptive name. This name identifies the style on the main Styles panel and in selection lists.

4. In the **Style Sheet File Name** text box, type a file name for the `.css` file Security Reporting Center creates to save the settings for this style. The file name must use a `.css` file extension. The file name is limited to 256 characters and cannot contain spaces.

5. In the **Banner Image File Name** text box, type the name of an image to be shown as a banner at the top of each report. We recommend using an image 810 pixels wide and 80 pixels high. If you use the `%WTIMAGEBASE%` macro in the file path, Security Reporting Center uses an image stored in the *`installation directory`*`/common/uiserver/images/report` directory. Alternately, type a URL to use a linked image on the Internet rather than a local file.

6. In the **Banner Image Alternate Text** text box, type the text you want to use as alternate text for the image. Alternate text functions as rollover text and replaces the image when it is not available.

7. ***If you want to see a sample report page with your current settings***, click **Preview**.

Report Style: Base Text

Use the Base Text panel to specify the color and font for non-heading text in each report. Base text includes all report text found outside the report headings, including report descriptions, tables, the calendar, and table of contents. To specify heading text, use the Heading Text panel.

To specify Base Text styles:

1. Open a Reporting module and click **Options > Reporting Styles**.

2. Click the **Edit** icon next to a style and click the Base text tab.

3. Select a text color by clicking it, or type a color value in the **Hexadecimal value** text box. We recommend using a dark color for the base text in your report. The default base text color used in Marshal reports is `#000000` (black).

4. Select a font from the list, or type one or more font names in the text box. If a remote user has different fonts from the one(s) you specify, Security Reporting Center substitutes the most similar font.

5. Select one or more check boxes to apply additional formatting to the text. By default, base text has no additional formatting.

6. ***If you want to see a sample report page with your current settings***, click **Preview**.

Report Style: Heading Text

Use the Heading Text panel to specify the color and font for the heading text in each report. Heading text is used in the report title, section title, and table and column headings. To specify non-heading text, use the Report Style: Base Text panel.

To specify Heading Text styles:

1. Open a Reporting module and click **Options > Reporting Styles**.
2. Click the **Edit** icon next to a style and click the Heading Text tab.
3. Select a text color by clicking it, or type a color value in the **Hexadecimal value** text box. We recommend using a dark color for the heading text in your report. The default base text color used in Marshal reports is `#000000` (black).
4. Select a font from the list, or type one or more font names in the text box. If a remote user has different fonts from the one(s) you specify, Security Reporting Center substitutes the most similar font.
5. Select one or more check boxes to apply additional formatting to the text. By default, heading text is bold.
6. ***If you want to see a sample report page with your current settings***, click **Preview**.

Report Style: Page Background Color

Use the Page Background Color panel to specify the color for the right pane of the report, which contains the graphs, tables, and other content. To specify the color for the navigation frame,

To specify the page background color:

1. Open a Reporting module and click **Options > Reporting Styles**.
2. Click the **Edit** icon next to a style and click the Page Background Color tab.
3. Select a background color by clicking it, or type a color value in the **Hexadecimal value** text box.

4. ***If you want to see a sample report page with your current settings***, click **Preview**.

Report Style: Bar Background Color

Use the Bar Background Color panel to specify the color for the background of bars in report graphs.

To specify the bar background color:

1. Open a Reporting module and click **Options > Reporting Styles**.
2. Click the **Edit** icon next to a style and click the Bar Background Color tab.
3. Select a background color by clicking it, or type a color value in the **Hexadecimal value** text box.
4. ***If you want to see a sample report page with your current settings***, click **Preview**.

Report Style: Primary Selection Color

Use the Primary Selection Color panel to specify the color for used to mark a selected report range or report grouping. To specify the color used to highlight a report page within a grouping, use the Secondary Selection Color panel.

To specify the primary selection color:

1. Open a Reporting module and click **Options > Reporting Styles**.
2. Click the **Edit** icon next to a style and click the Primary Selection Color tab.
3. Select a primary selection color by clicking it, or type a color value in the **Hexadecimal value** text box.
4. ***If you want to see a sample report page with your current settings***, click **Preview**.

Report Style: Secondary Selection Color

Use the Secondary Selection Color panel to specify the color used to highlight a report page within a grouping. To specify the color used to mark a selected report range or report grouping, use the Secondary Selection Color panel.

To specify the secondary selection color:

1. Open a Reporting module and click **Options > Reporting Styles**.
2. Click the **Edit** icon next to a style and click the Secondary Selection Color tab.
3. Select a secondary selection color by clicking it, or type a color value in the **Hexadecimal value** text box.
4. ***If you want to see a sample report page with your current settings***, click **Preview**.

Chapter 12
Managing Data with Filters

Security Reporting Center provides complex filtering capabilities that allow you to decide what data Security Reporting Center should analyze and present in reports. For instance, if you want to see reports on how much a particular campaign affected Web and email traffic in Sales and Marketing, you can create a filter that limits reports to those specific departments and protocols for the specific dates involved. You can even use filters to include or exclude activity linked to specific authenticated user names.

Global and Local Filters

In general, you create filters using the Global Filter Options in either of the Reporting modules. Filters you create using these options are called global filters because you can associate them with any profile. Global filters can be attached to a particular profile using the Filters panel when you create or edit the profile. For information about creating a global filter, see "Creating a Global Filter" on page 190.

You can also create filters that can only be used or viewed from within a single profile. These filters, which are called local filters, are not accessible from the Options panels, and can only be viewed by users who have access to the profile for which they were created. This can be useful if you want to filter information for purposes of confidentiality. For example, you may want to focus reports on very specific groups of users, departments, or Web sites. The steps for creating a local filter are similar to the steps for creating a global filter. To create a local filter while creating or editing a profile, use the instructions found in "Adding a Local Filter" on page 193 and continue with Steps **4**-**8**.

Creating a Global Filter

For a detailed description of the elements that can be used to construct a filter, and instructions on how to configure them, see "Filter Elements" on page 195.

To create a global filter:

1. Open a Reporting module and click **Profiles > Options**.
2. Click **Global Filters**. The main Filters panel is shown with the current list of available filters.
3. Click **Add** to create a new filter. The General panel is shown.
4. Type a descriptive name in the **Filter Title** text box (for example `Weekend email`).
5. Select a check box from the list to choose criteria for a filter type.
6. Provide information about your filter specifications in the right pane. For more information about configuring each filter type, use the Help or see the descriptions of filter elements in this chapter.
7. If you want to add more criteria to the filter, select more check boxes and continue choosing criteria. All the criteria you choose will be included in a single filter. To edit a filter type you have specified, click the link next to the checked box. To remove a specified criterion, click to clear the check box.
8. After you finish specifying filter criteria, click **Save**. Your filter name is added to the list in the Filters panel.

Keep in mind that the filter criteria you assemble in a single filter are additive: each criterion in the filter becomes part of a Boolean AND statement. This means that activity, in order to be included or excluded from the data reported for a profile, must meet all of the criteria you specify. For example, if you specify the authenticated user name jferrera, the date and time Saturday and Sunday and the Traffic Type email, only email activity generated by jferrera on Saturdays and Sundays is included or excluded for any profile using this filter. Whether the filter includes or excludes data depends on whether it is added to a particular profile as an Include or an Exclude filter.

For more information about each filter element, see “Filter Elements” on page 195.

Adding Filters to a Profile

This section describes how to associate filters with a profile to define what information Security Reporting Center analyzes to create reports for that profile.

Include and Exclude Filters

When you add a filter to a profile, you either include or exclude the data described in that filter for the purpose of any reports based on the profile. You can use any filter as either an Include filter or an Exclude filter. When you add a filter and designate it as an Include filter, the selection of data described in that filter is included in analysis and reporting, and any data that does not meet the criteria in the filter is excluded. If you add that same filter and designate it as an Exclude filter, the selection of data described in the filter is excluded from reports, and only data that does not meet the criteria in the filter will appear in reports.

Note
When you add both Include and Exclude filters to the same profile, the Include filters are read first.

The filters created in the Filter options for each reporting module are global. This means that they can be associated with any profile, and that any Security Reporting Center user who has access to filter settings can see them.

Local filters use all the same settings as global filters, but they are created within a profile and are bound to that profile. Only users who can access the profile can see its local filters.

For more information about the differences between global and local filters, see “Global and Local Filters” on page 189.

Adding a Global Filter

To add a global filter to a profile:

1. In a Reporting module, begin adding or editing a profile. If you are adding the profile for the first time, the Filters panel is part of the sequence of panels. If you are editing an existing profile, click the Filter tab to access the Filters panel.
2. Click **Add Global Filter**. The Add Global Filter to Profile panel opens, showing a list of all the filters configured using the Filters options in the current Reporting module.
3. To add filters, select one or more filters in the list on the left and click **Select** to move each one to the list on the right. To remove a filter from the selected list, select it in the right-hand list and click **De-select**.
4. When the list at the right shows the filters you want to add, click **Done** to save your settings and return to the Filters panel. Click **Cance**l to return to the Filters panel without saving your settings.
5. By default, each filter is added as an Include filter. To change an Include filter to an Exclude filter, click **Exclude** in the Type column.

Adding a Local Filter

To add a local filter:

1. In a Reporting module, begin adding or editing a profile. If you are adding the profile for the first time, the Filters panel is part of the sequence of panels. If you are editing an existing profile, click the Filter tab to access the Filters panel.
2. Click **Create Local Filter**. The New Filter panel opens. The steps you use to create a local filter are the same as the steps you use to create a global filter in the Options panels. To review these steps, see “Creating a Global Filter” on page 190.
3. By default, the filter is created as an Include filter. To change it to an Exclude filter, click **Exclude** in the Type column.

Making Global Filters Local

To convert a global filter into a local one, click the **Make Local** icon next to any global filter.

Using Multiple Filters

As described in “Creating a Global Filter” on page 190, individual filters function as if each separate element in the filter is a term in a Boolean AND statement. To be included or excluded by the filter (depending on whether it is an Include or Exclude filter), log activity must meet all the criteria described by the elements within that filter. When you add multiple filters, however, each separate filter functions as a term in a Boolean OR statement. That is, any activity which meets any one of the multiple filters is excluded or included.

In other words, if a profile contains several Include or Exclude filters—each having one or more elements—the report for that profile contains all activity that matches the criteria of all of the elements of any one of the filters. If a Log File Activity record matches Filter 1 OR matches Filter 2 (and so on, including all the filters added to the profile) then the data is included in (or excluded from) the report or view.

For example, the single filter described above specified the authenticated user name `jferrera`, the date and time `Saturday and Sunday` and the Traffic Type `email`. If these criteria were added as part of a single Include filter, only email activity generated by jferrera on Saturdays and Sundays would be included in reports. Weekend email generated by any other user would not be part of the activity analyzed and reported on, for example. If each of these criteria were added as a separate Include filter, however, any activity that met any of the three criteria would be used in both analysis and reporting. In this case not only would weekend email by other users be included in the reports, but so would all weekend activity, as well as all email activity by any user and all the traffic of any type generated by jferrera.

Using Both Include and Exclude Filters

If a profile contains Include filters and Exclude filters, data is included based on the Include filters and excluded based on the Exclude filters. The Include filters are read first.

To create a report including all weekend activity other than jferrera's email activity, create an Include filter with the element `date and time=Saturday and Sunday` and an Exclude filter with the elements `Authenticated username=jferrera` and `Protocol Family=email`.

Filter Elements

This section describes the elements you can use to create filters and gives instructions for configuring each element. Combine these elements to create complex filters.

See the following topics for information on each filter element:

- "Authenticated Username Filter" on page 196
- "Check Point Action Filter" on page 197
- "Firewall Status Code Filter" on page 198
- "Internal User Address Filter" on page 199
- "External User Address Filter" on page 199
- "Protocol Family Filter" on page 202
- "Traffic Direction Filter" on page 203
- "Date and Time Filter" on page 204
- "Department Filter" on page 204
- "Firewall Name Filter" on page 205
- "Firewall Rule Filter" on page 206
- "Site Filter" on page 206
- "User Address Filter" on page 207
- "Action Filter" on page 208

- “File Filter” on page 209
- “Proxy Cache Filter” on page 211
- “Core Category Filter” on page 214
- “General Category Filter” on page 216
- “Uncategorized Data Filter” on page 218

Authenticated Username Filter

This filter element lets you specify the activity of individual users by their authenticated username. The Authenticated User filter is useful if you have a secure site that requires visitors to log on with a user name and password. If your site does not require login with a user name and password, your log file will not contain authenticated user names.

To specify which authenticated users to filter:

1. In the **Authenticated Usernames** text box, type the user names. Use spaces to separate multiple entries. For example, type:

   ```
   Bob Mike John
   ```

   to filter any log entry that includes the text strings "Bob," "Mike," or "John."

   If the user name contains a space, surround the user name with quotation marks. For example, type:

   ```
   "Jane Smith"
   ```

   to filter any log entry that matches "Jane Smith."

2. Specify how this module will match user names.

   – Select **Include All Authenticated Users** to filter all authenticated users.

   – Select **Case Sensitive** to look for exact case matches (upper- or lowercase). Most servers do not require case-sensitive matches.

3. Do one of the following:

   - Select another filter element.
   - Click **Save** to save all the filter elements you selected and return to the list of filters.
   - Click **Cancel** to abandon all the filter elements you selected and return to the list of filters.

Check Point Action Filter

Use the Check Point Action filter element to specify which Check Point VPN-1/FireWall-1 firewall actions will be included in or excluded from the analysis and reporting for a profile. A Check Point action is a type of event noted in the firewall log record, for instance a response to a logon attempt or a data transfers. See your Check Point firewall documentation for more information.

Note
This filter element applies to Check Point VPN-1/FireWall-1 actions only. If you are using another firewall, use the Firewall Status Codes filter element instead.

To specify one or more Check Point Actions to filter:

1. Select a check box for each Check Point action you want to filter.
2. Do one of the following:

   - Select another filter element.
   - Click **Save** to save all the elements you selected and return to the list of filters.
   - Click **Cancel** to abandon all the filter elements you selected and return to the list of filters.

Firewall Status Code Filter

Use the Firewall Status Code filter element to specify one or more firewall status codes. Status codes are found in log records and describe specific types of events that occur on the firewall. For example, status codes could indicate a problem on the network or someone abusing public space. For more information about firewall status codes, see your firewall's documentation.

Note
Do not use this filter element if your log files are in Check Point VPN-1/FireWall-1 format. Instead, use the Check Point Actions filter element.

To specify which firewall status codes to filter:

1. In the **Firewall Status Codes** text box, type the status codes that you want to filter. Wildcards are not allowed. Specify a range of values by using a hyphen. For example, type:

   ```
   121 300-399 50-599
   ```

   Note
   You can find text files containing status codes for your firewall in the `\modules\firewall` directory of your Security Reporting Center installation. The file names follow the format ***`Firewallname`***`Messages.txt`, as in these examples:

   ```
   CiscoMessages.txt
   LucentMessages.txt
   RaptorMessages.txt
   ```

2. Do one of the following:

   - Select another filter element.
   - Click **Save** to save all the filter elements you selected and return to the list of filters.
   - Click **Cancel** to abandon all the filter elements you selected and return to the list of filters.

Internal User Address Filter

Use the Internal Address filter element to specify addresses behind your firewall. You can use this filter element to focus your reports on the activity of particular individuals, address ranges or domains.

You can specify the activity you want to filter by domain name, domain type, region, or country. For a table showing different ways to specify addresses, see "User Address Examples" on page 201.

To specify the internal user addresses to filter:

1. In the **Internal User Addresses** text box, type the user addresses that you want to specify. Use spaces to separate multiple entries. You may use asterisks (*) as wildcards to specify multiple addresses. For example, type `*.edu` to specify all addresses ending in .edu.

   To make sure that a user address is filtered regardless of how DNS lookups are handled, specify the address by both IP address and domain name. For example, specify both `domain.com` and `111.111.111.11`.

2. Do one of the following:

   – Select another filter element.

   – Click **Save** to save all the filter elements you selected and return to the list of filters.

   – Click **Cancel** to abandon all the filter elements you selected and return to the list of filters.

External User Address Filter

Use this filter element to specify user addresses outside your firewall.

You can specify the activity you want to filter by domain name, domain type, region, or country. For example, you can create a filter that includes activity from a questionable IP address if you think someone is trying to attack your firewall. For a table showing different ways to specify addresses, see "User Address Examples" on page 201.

To specify external addresses to filter:

1. In the **External User Addresses** text box, type the user addresses that you want to specify. Use spaces to separate multiple entries. You may use asterisks (*) as wildcards. For example:

   ```
   *.edu *.com *.net*.uk
   ```

   To make sure that a user address is filtered regardless of how DNS lookups are handled, specify both the IP address and the domain name. For example:

   ```
   domain.com 111.111.111.11
   ```

2. Do one of the following:

   - Select another filter element.
   - Click **Save** to save all the elements you selected and return to the list of filters.

User Address Examples

The following table shows how to specify user address ranges using several different types of notation.

This Address	Specifies:
`204.245.240.*`	All IP addresses between 204.245.240.0 and 204.245.240.255, inclusive.
`192.168.0.50-100 or 192.168.0.50-192.168.0.100`	All IP addresses between 192.168.0.50 and 192.168.0.100, inclusive.
`111.92.76.0/26 (CIDR notation)`	All subnet addresses between 111.92.76.0 and 111.92.76.63, inclusive.
`204.245.240.64/26 (CIDR notation)`	All addresses of this classless subnet: 204.245.240.64 – 204.245.240.127.
`*.Marshal.com`	Only those addresses including a subdomain to the left of this domain (such as www.Marshal.com or ftp.Marshal.com). Excludes all addresses without a subdomain.
`* Marshal.com`	Any address including the specified domain, with or without a subdomain, such as www.Marshal.com, ftp.Marshal.com, or Marshal.com.
`*.edu *.com *.net`	All addresses that use one of the following domain types: edu, com, or net.
`www.*`	Only those addresses including www as a subdomain.

Protocol Family Filter

The Protocol Family filter element lets you specify the type of network traffic (for instance email traffic). You can add protocol families using the Manage Protocol Families panel, accessed from the Protocols tab in the Log Analysis Options. Protocol families are groups of protocols defined using the Protocols panel in the Log Analysis options. For more information, see “Managing Protocol Families” on page 118.

To specify the protocol family to filter:

1. Use the Protocol Family list to select one of the currently defined protocol families.
2. Do one of the following:
   - Select another filter element.
   - Click **Save** to save all the elements you’ve selected and return to the list of filters.
   - Click **Cancel** to abandon all the filter elements you’ve selected and return to the list of filters.

Traffic Direction Filter

The Traffic Direction filter element lets you specify the direction of network traffic. For example, a filter specifying outbound traffic can be used to include or exclude traffic going from your site to addresses outside your firewall.

To specify a traffic direction to filter:

1. Select the direction of traffic.
   - **Inbound traffic** specifies traffic coming from outside your firewall.
   - **Outbound traffic** specifies traffic going from inside your firewall to addresses outside the firewall.
   - **Both inbound and outbound traffic** specifies both types of traffic.
2. Do one of the following:
   - Select another filter element.
   - Click **Save** to save all the filter elements you selected and return to the list of filters.
   - Click **Cancel** to abandon all the filter elements you selected and return to the list of filters.

Date and Time Filter

The Date and Time filter element lets you select days of the week and a time of day or range of times.

To specify the date and time to filter:

1. Select one or more **Day of Week** check boxes to specify one or more days.
2. Specify the hour or range of hours during which you want activity to be filtered:
   - Select **All** to filter activity during the entire 24-hour period.
   - Select **Specified hours** to filter activity only during a specified period. Use the Start time and End time lists to specify the beginning and ending time of the period. Select **8:00** and **17:00**, for example, to include or exclude activity between 8:00 AM and 5:00 PM
3. Do one of the following:
   - Select another filter element.
   - Click **Save** to save all the elements you selected and return to the list of filters.
   - Click **Cancel** to abandon all the filter elements you selected and return to the list of filters.

Department Filter

The Department filter element lets you specify a department by selecting a currently defined departments for the list. You can create departments using the Department Definitions Options in any Reporting module. See “Department Management” on page 115 for more information about adding and editing departments.

To select a department to filter:

1. In the Department list, select a department.
2. Do one of the following:
   - Select another filter element.
   - Click **Save** to save all the elements you've selected and return to the list of filters.
   - Click **Cancel** to abandon all the filter elements you've selected and return to the list of filters.

Firewall Name Filter

The Firewall Name filter element lets you specify one or more firewalls. If your firewall log file includes events for more than one firewall, you can use this element to look at the activity for a single firewall.

To specify the firewalls to filter:

1. In the **Firewall Name** text box, type a name for each firewall exactly as it is recorded in the log file. Use commas to separate firewall names.
2. Do one of the following:
   - Select another filter element.
   - Click **Save** to save all the elements you've selected and return to the list of filters.
   - Click **Cancel** to abandon all the filter elements you've selected and return to the list of filters.

Firewall Rule Filter

The Firewall Rule filter element lets you specify which firewall rules to filter. Firewall rules determine what activity can take place inside and across the firewall. Most firewall rules are identified by numbers.

To specify the firewall rules to include in or exclude from analysis and reporting:

1. In the **Rules** text box, type the number of the firewall rules. Use commas or spaces to separate rule numbers.
2. Do one of the following:
   - Select another filter element.
   - Click **Save** to save all the elements you've selected and return to the list of filters.
   - Click **Cancel** to abandon all the filter elements you've selected and return to the list of filters.

Site Filter

Use the Site filter element to include or exclude one more Web sites or domain types from reporting. For example, you might want to filter all sites using a particular domain or country extension.

A typical use for the Site filter is to report on activity for your intranet. To report on intranet traffic only, create an Include filter and specify the URL for your intranet (for example `www.intranet.company.com`). The resulting report shows only hits to the site specified.

To specify which sites to filter:

1. Type the URL(s) you want to filter in the text box. To specify multiple URLs, use wildcards. For example, to specify all sites from educational domains, type:

   ```
   *.edu
   ```

   To specify several individual URLs, separate them with a vertical bar. For example, type:

   ```
   www.first.com|www.second.com
   ```

2. Select another filter element, or do one of the following:

   - Click **Save** to save all the filter elements you've selected and return to the list of filters.
   - Click **Cancel** to abandon all the filter elements you've selected and return to the list of filters.

User Address Filter

Use the User Address filter element to specify addresses behind your firewall. You can use this filter element to focus your reports on the activity of particular individuals, address ranges or domains.

You can specify the activity you want to filter by domain name, domain type, region, or country. For more information about how to specify user addresses, see "User Address Examples" on page 201.

To specify the user addresses to filter:

1. In the **User Addresses** text box, type the user addresses that you want to specify.

   Use spaces to separate multiple entries. You may use asterisks (*) as wildcards, for example `*.edu *.com *.net *.uk`.

   To make sure that a user address is filtered regardless of how DNS lookups are handled, specify the address by both IP address and domain name. For example, type:

   ```
   domain.com 111.111.111.11.
   ```

2. Select another filter element or do one of the following:

   – Click **Save** to save all the filter elements you selected and return to the list of filters.

   – Click **Cancel** to abandon all the filter elements you selected and return to the list of filters.

Action Filter

The Action filter element lets you specify Web or FTP activity that triggers an action on the firewall performing an action in response because the URL accessed belongs to the Core or General categories. For example, the firewall may be configured to block activity that matches the URLs in the Core Categories database. For more information about Core and General categories, see “URL Categorization” on page 130. To use this filter element, specify one or more action codes.

To specify the action(s) to filter:

1. In the **Actions** text box, type each action as it is recorded in the log file. Put quotes around values containing spaces or commas. Use commas to separate actions. The typical actions are `BLOCK` (for activity that is blocked by the proxy server) and `PASS` (for activity that the proxy server allows the user to download).

2. Select another filter element or do one of the following:

   – Click **Save** to save all the elements you've selected and return to the list of filters.

   – Click **Cancel** to abandon all the filter elements you've selected and return to the list of filters.

File Filter

Use the File filter element to include or exclude requests for certain files or file types from reporting. For example, you may want to include or exclude all requests for `.htm` files, or you may want to include or exclude requests for one or more particular `.htm` files.

To specify which files or file types to filter:

1. Type one or more file names or file extensions in the **Files** text box, or use the list box to select a single type of file. Use spaces to separate multiple entries. If you type a value that contains spaces, enclose the value in quotation marks. You may use asterisks (`*`) as wildcards.

2. ***If you want requests to Web pages that do not include a filename with a `.html` or `.htm` extension to be considered as HTML files for the purposes of the filter***, select the **Also include requests without filenames** check box.

   For example, most visitors to a Web site type a URL in the format `www.mydomain.com`. The proxy server logs the hit without a specified filename, but returns the file as `http://www.mydomain.com/default.htm`. When the check box is selected, Security Reporting Center counts the request for `www.mydomain.com` as a request for a `.htm` file and includes or excludes it in reports according to whether the filter is applied as an Include or Exclude filter. See the table for examples of how to specify file names.

3. ***If you want to treat file names as case-sensitive***, select the **File names are case-sensitive** check box. Most proxy servers do not require case-sensitive matches. If your proxy server does not require case-sensitive matches, do not select the check box.

4. Select another filter element, or do one of the following:

   – Click **Save** to save all the filter elements you've selected and return to the list of filters.

   – Click **Cancel** to abandon all the filter elements you've selected and return to the list of filters.

The following table shows examples of how to specify file names.

`help.htm`	Filters the file `help.htm`.
`*.gif *.bmp`	Filters bitmap (`.bmp`) and `.gif` files.
`help*.html`	Filters all html files whose names begin with `help`.
`help*.*`	Filters all files whose names begin with `help`, regardless of file type.

`marketing.htm`
`“marketing help.htm”`
`“marketing leads.htm”`
	Filters the files `marketing.htm`, `marketing help.htm`, and `marketing leads.htm`.

Proxy Cache Filter

The Proxy Cache filter element lets you filter activity that matches the proxy codes you specify.

To specify the proxy cache codes to include or exclude:

1. Select a single code from the list, or type one or more codes into the text box, separated by spaces. You cannot select multiple codes using the list box. For more information about proxy cache codes, see the table.
2. To continue, select another filter element or do one of the following:
   - Click **Save** to save all the filter elements you selected and return to the list of filters.
   - Click **Cancel** to abandon all the filter elements you’ve selected and return to the list of filters.

The following table shows proxy cache codes and their definitions.

Code type	Description
All Proxy Status Values	Includes or excludes records that have a proxy status value.
From the Internet (Summary)	Includes or excludes records with a status value indicating that the file requested was downloaded from the Internet.
From the Cache (Summary)	Includes or excludes records with a status value indicating that the file requested was downloaded either from the local proxy server's cache or from an upstream proxy server's cache.
Cache Unknown	Includes or excludes records with a status value indicating that the cache is not known.
From the Internet, then cached (new)	Includes or excludes records with a status value indicating that the file requested was downloaded from the Internet and then placed into the proxy server's cache for possible future use. This status value also indicates that the file was not present in the cache before downloading it.
From the Internet, then cached (updated file)	Includes or excludes records that have a status value indicating that the file requested was downloaded from the Internet and then placed into the proxy server's cache for possible future use. This status value also indicates that an older version of the file was in the cache before downloading it, and was updated by the newer version.
From the cache, verified by remote server	Includes or excludes records that have a status value indicating that the file requested was already present in the cache, and the proxy server contacted the remote server to verify that it was the newest version of the file.

From the cache, without verification	Includes or excludes records that have a status value indicating that the file requested was already present in the cache and the proxy server did not contact the remote server to verify that it was the newest version of the file.
Resource not cacheable	Includes or excludes records that have a status value indicating that the file requested was downloaded from the Internet and was not added to the proxy server's cache
Cache write aborted.	Includes or excludes records that have a status value indicating that the file requested was downloaded from the Internet, and while the file was being added to the cache, something happened that caused the proxy server to cancel writing the file
From the cache, no details	Includes or excludes records that have a status value indicating that the file requested was already in the cache. No other details were given.
Returned from array member cache	Includes or excludes records that have a status value indicating that the file requested was present in a proxy array member cache.
Returned from upstream cache.	Includes or excludes records that have a status value indicating that the file requested was present in a proxy server's cache upstream from the proxy server reported on
From the Internet, no details	Includes or excludes records that have a status value indicating that the file requested was downloaded from the Internet. No other details were given.
Successful connection	Includes or excludes records that have a status value indicating that the client initiated a successful connection with the proxy server.

Connection rejected by proxy server	Includes or excludes records that have a status value indicating that the client attempted to initiate a connection and was rejected by the proxy server.
Normal connection termination	Includes or excludes records that have a status value indicating that the proxy server terminated a connection normally.
Abortive connection termination	Includes or excludes records that have a status value indicating that the proxy server terminated the connection abnormally.

Core Category Filter

The Core Category filter element lets you include or exclude sites and pages on the Internet belonging to the Core categories. URLs are categorized according to the content they contain by any user-defined Core categories created in the Security Reporting Center Custom Database panel. Core categories track pages and sites with content of potential legal sensitivity, for example sexually explicit or drug-related material. To filter General categories, which include sites with content that, while not controversial in itself, may detract from employee productivity, for example news and entertainment sites, use the General Category filter element.

You can also use this panel to filter Core category mappings. For example, if you have one or more categories mapped to a Core category called Illegal Activity, you can use a filter to include or exclude activity mapped to that category. To create category mappings, see “Category Mapping” on page 136. For more information about URL Categorization, see “URL Categorization” on page 130.

Note
Category mappings are components of the category mapping groups listed in the Category Mapping panel. Mapping groups cannot be filtered.

To include or exclude all Core categories and mappings:

1. Click **Filter all Core categories and category mappings.**

2. Do one of the following:

   - Select another filter element.
   - Click **Save** to save all the filter elements you've selected and return to the list of filters.
   - Click **Cancel** to abandon all the filter elements you've selected and return to the list of filters.

To include or exclude only certain categories or mappings:

1. Click **Filter specific Core categories and category mappings**.
2. Under **Core Categories**, create a list of the Core categories you want to filter by moving categories from the Available Categories list to the Selected Categories list.

   - To move a category to the Selected Categories list, select it in the Available Categories list and click **Select**.
   - To remove a category from the Selected Categories list, select it in the Selected Categories list and click **De-select**.
3. Under **Category Mappings**, create a list of the category mappings you want to filter by moving mappings from the Available Mappings list to the Selected Mappings list.

   - To move a category to the Selected Mappings list, select it in the Available Mappings list and click **Select**.
   - To remove a category from the Selected Mappings list, select it in the Selected Mappings list and click **De-select**.
4. Do one of the following:

   - Select another filter element.
   - Click **Save** to save all the filter elements you've selected and return to the list of filters.
   - Click **Cancel** to abandon all the filter elements you've selected and return to the list of filters.

General Category Filter

The General Category filter element lets you include or exclude sites and pages on the Internet belonging to General categories. URLs are categorized according to the content they contain by any user-defined General categories created in the Security Reporting Center Custom Database panel. General categories track pages and sites with content that, while not controversial in itself, may detract from employee productivity, for example news and entertainment sites. To filter sites and pages with content of potential legal sensitivity, for example sexually explicit or drug-related material, use the Core Category filter element.

You can also use this panel to filter General category mappings. For example, if you have one or more categories mapped to a General category called Non-Work Related, you can use a filter to include or exclude activity mapped to that category. To create category mappings, see “Category Mapping” on page 136. For more information about URL Categorization, see “URL Categorization” on page 130.

Note
Category mappings are components of the category mapping groups listed in the Category Mapping panel. Mapping groups cannot be filtered.

To include or exclude all General categories and mappings:

1. Click **Filter all General categories and category mappings**.
2. Do one of the following:
   - Select another filter element.
   - Click **Save** to save all the filter elements you’ve selected and return to the list of filters.
   - Click **Cancel** to abandon all the filter elements you’ve selected and return to the list of filters.

To include or exclude specific General categories or mappings:

1. Click **Filter specific General categories and category mappings**.
2. Under **General Categories**, create a list of the General categories you want to filter by moving categories from the Available Categories list to the Selected Categories list.
   - To move a category to the Selected Categories list, select it in the Available Categories list and click **Select**.
   - To remove a category from the Selected Categories list, select it in the Selected Categories list and click **De-select**.
3. Under **Category Mappings**, create a list of the category mappings you want to filter by moving mappings from the Available Mappings list to the Selected Mappings list.
   - To move a category to the Selected Mappings list, select it in the Available Mappings list and click **Select**.
   - To remove a category from the Selected Mappings list, select it in the Selected Mappings list and click **De-select**.
4. Do one of the following:
   - Select another filter element.
   - Click **Save** to save all the filter elements you've selected and return to the list of filters.
   - Click **Cancel** to abandon all the filter elements you've selected and return to the list of filters.

Uncategorized Data Filter

The Uncategorized Data filter element lets you include or exclude uncategorized Web activity data from your reports. For example, if you only want reports about most-accessed sites to include sites that belong to the Core or General categories, you can exclude uncategorized URLs from analysis. By default, all uncategorized data is included in reports.

To filter uncategorized data:

1. Select the **Uncategorized Data** check box in the left pane of the Filters panel.
2. Select another filter element or do one of the following:
   - Click **Save** to save all the filter elements you've selected and return to the list of filters.
   - Click **Cancel** to abandon all the filter elements you've selected and return to the list of filters.

Managing Global Filters

The Global Filters panel allows you to manage the list of available Global filters by creating, deleting, or editing filters. You can also copy and modify an existing filter. The list of filters shown in this panel is the same list of filters you can draw from when creating a profile.

Note
If you edit global filters that are assigned to one or more profiles after an event has run, you may want to delete existing FastTrends and Content databases for those profiles to ensure consistent data in future reports.

To manage filters, do any of the following:

- To add a filter, click **Add Filter**. The General filter panel opens and you can begin creating a filter.
- To edit a filter, click the **Edit** icon next to an entry in the list and edit the information in the General filter panel.

- To delete a filter, click the **Delete** icon next to an entry in the list.
- To create a filter based on an existing filter, click the **Copy** icon next to an entry in the list and edit the settings in the General filter panel.

When you have finished managing filters, click **Done** to save your changes.

Appendix A
XML Interface

Security Reporting Center allows you to configure most database objects and settings using XML. XML support lets you bypass the user interface and pass data directly to the database using the command line. Typically, data is exported from the Security Reporting Center database in the form of an XML document, modified locally, and passed back to the database using the command line. You can also add and delete Security Reporting Center objects this way.

Using the command line to update database settings has clear advantages when updates need to be made on a large scale. For example, if you need to change one setting in a large number of profiles, you can make a global text change in a number of XML documents and quickly update all the profiles at once. Making the same change in the user interface would require you to open each profile, modify it, and save it separately. XML support also allows you to export all the settings for each module and re-import them after migration.

How it Works

Information about most objects and settings can be passed to the database using the command line. Objects, for example users, teams, events, and profiles, can be added, deleted, and modified. Settings, for example internal DNS handling and agent polling, can be modified but not added or deleted. XML support allows you to export and update information about objects and settings by exporting and importing an XML document describing the object or the group of settings.

Note
For certain objects, such as database locations, at least one object must be configured at all times.

When you install the Security Reporting Center User Interface server, a set of batch files is installed in the `Program Files\NetIQ\Common\XML` directory. These batch files simplify the command-line syntax used to update the Security Reporting Center database using XML documents. Without these batch files, communicating with the database requires you to call java.exe and specify the class path, the JDBC URL, and the database user name and password before specifying any additional arguments.

If you first call the batch file, you can bypass most of these parameters and use a very small number of arguments. Each module uses a separate batch file, which is called when configuring objects and settings for that module. The batch files for the respective modules are named FirewallXML, ProxyXML, AdminXML, and SchedXML.

Note
To view the database changes in the user interface, stop and then restart the NetIQ-Tomcat service.

Valid Arguments

Security Reporting Center recognizes the parameters shown in the following table.

Parameter	Definition
`-o`	The operation you want to perform. The value can be `export,` `update`, `add`, `delete`, or `listing`. This parameter is required.
`export`	outputs information about one or more entities to one ore more XML files.
`add`	adds a newly created entity to the database.
`update`	passes the information in an XML document to the database.
`delete`	permanently removes information about the entity from the database.
`listing`	outputs a list of all the entities of a given type to a specified file.
`-e`	The entity, which is the object you want to export, add, or modify. Some typical entities are profiles, events, and users, agent polling and log analysis options.
`-n`	The unique name of a specific entity, for example the name of a user or a profile. If you are updating a specific entity, this is the ID number generated by the database. To work with all the files in a directory, use -a instead of specifying -n.
`-d`	Specifies the directory where multiple exported files will be stored, or the directory from which files will be updated.
`-a`	Specifies that all entities of the given type should be added or exported. Use with -d to identify the destination or source directory.
`-l`	Lists all the objects that can be modified in the current module.

-h	Calls help text, including a list of available arguments.
-q	Runs XML commands in quiet mode. In quiet mode, no confirmation message is shown when an operation completes. Errors are always shown.
-c	Omits most of the explanatory comments from an XML document. Used only when exporting XML documents.

What Entities Can You Modify?

Each module has a different set of entities that can be modified. To find out what they are, use the -l parameter. For example, type the following at a command prompt to get a list of the Firewall module's entities:

```
adminxml -l
```

The following list is returned:

```
content_database_location
content_database_management
currency_types
departments
firewall_reporting_options
global_filter
log_analysis_options
log_path_macros
profile
syslog_settings
```

Use any of these entities with the `-e` parameter to export or update objects. For more information, see "Exporting and Updating Objects" on page 225.

Exporting and Updating Objects

Typically, XML is used to update all of one type of object, for example all the configured events or all the configured users. For information about exporting and updating individual objects where there is more than one of a particular object, see "Working with Single Objects" on page 240.

The simplest way to export all of a particular kind of entity is to use the `-a` argument. The `-a` argument signifies that the operation should be performed on all of the entities of that type.

For example, to export data about all users to the directory `c:\temp\xml\users`, go to the directory where your XML batch files are installed (by default, in `\Program Files\NetIQ\common\xml`) and type the following:

```
adminxml -o export -e user -a -d c:\temp\xml\users
```

Here the operation is `export`, the entity is `user`, and `-a` indicates that information for all users should be exported. The database exports each user's information as a separate XML file and supplies a filename for each one based on its database ID number.

After you modify the XML documents containing information about an object or setting, you can pass the changes to the database using the update operation. To import the changed information in the user files exported in the previous operating, use the following command:

```
adminxml -o update -e user -a -d c:\temp\xml\users
```

Adding Objects

To add an object, you should first export an object of that type, modify it, and save the XML file under a new name. Then use the add operation to add the entity, specifying the new file name as a source.

For example, to create a new event:

1. Export the data for all events to `c:\temp\xml\events` by typing:

   ```
   schedxml -o export -e event -a -d c:\temp\xml\events
   ```

2. Open one of the XML files for an existing event in `c:\temp\xml\events` and save it under a new filename such as `newevent.xml`. Modify it to use the settings you want to use for the new event.

3. Add the event by typing:

   ```
   schedxml -o add -e event c:\temp\xml\events\newevent.xml
   ```

Working with Single Objects

To export and/or update the information for a single entity, use the `-n` parameter to specify its unique ID number. The ID number is shown at the top of XML document. For example, the following line identifies a firewall profile:

```
<Profile ID="6" Cartridge_Key="firewall" Version="2.0">
```

The ID for this profile is `6`.

You can learn the IDs of all the objects of a type and correlate them to a name by using the listing operation, which creates an XML file containing a list of the objects of any given type. For example, suppose you want to know the ID of the profile for your Check Point firewall. Type the following at a command prompt:

```
firewallxml -o listing -e profile -a c:\temp\xml\profilelist.xml
```

Assuming in this case that your profiles are named after individual firewalls, the following text is returned:

```
<?xml version="1.0" encoding="UTF-8"?>
<profile_listing>
  <Element ID="7">Check Point Profile</Element>
  <Element ID="6">SonicWALL Profile</Element>
  <Element ID="2">Symantec Profile</Element>
</profile_listing>
```

The ID for the Check Point firewall in this case is `7`.

Use the `-n` parameter to specify the ID number when performing an operation that requires specifying a single object. For example, to export the profile to the file `c:\temp\xml\profiles\checkpoint.xml`, type:

```
firewallxml -o export -e profile -n 7 -d
c:\temp\xml\profiles\checkpoint.xml
```

Specifying Files and Directories

You can specify either a file or a directory where the database should export to or update from. By default, directories and files you specify are relative to the root directory. Not all objects and settings support both directories and files.

To export a profile to the directory c:\temp\xml\profiles, type:

```
firewallxml -o export -e profile -n 7 -d c:\temp\xml\profiles
```

The database provides a file name for the XML file.

To export the profile to a file with the name of your choice in the same location, type:

```
firewallxml -o export -e profile -n 6
c:\temp\xml\profiles\filename.xml.
```

The Structure of the XML Documents

Each XML document describes a simple object such as a user, a global filter, or an agent, or else a group of settings (such as the Log Analysis options found in each Reporting module). For example, the XML document associated with a user contains tags for each of the following settings:

- login name
- user name
- password
- password type
- enabled or disabled
- time zone
- session timeout
- team membership
- level of user rights

XML documents can also describe groups of settings not associated with a specific object. In this case, the settings are grouped as they are in the Security Reporting Center user interface. For example, `event_options.xml` describes all the options contained in the Options panels for events.

The following document shows the `syslog_settings` object in the Firewall Reporting module:

```
<?xml version="1.0" encoding="UTF-8"?>
<Syslog_Settings Cartridge_Key="firewall" Version="2.0">
  <!-- This lets you set the frequency with which log files created 
by the NetIQ Syslog Service are rotated. In a case where the NetIQ 
Syslog Service is installed on a computer with multiple NICs, it can 
also be used to specify the IP address where the NetIQ Syslog Service 
will receive data. These Syslog settings are shared by both Firewall 
and Proxy. -->
  <!-- Select one of the following options to set the frequency of 
log file rotation for Syslog Service to collect log data. -->
  <!-- Possible values for Log_File_Rotation:
       1 - Rotate log files daily
       2 - Rotate log files monthly
       3 - Do not rotate log files -->
  <Log_File_Rotation>3</Log_File_Rotation>
  <!-- Select one of the following options to set the IP address 
where the NetIQ Syslog Service will receive data. If the computer 
where the NetIQ Syslog Service is installed has only one IP address, 
set Bind_To_All_IP_Addresses to true. -->
  <!-- Note: If Bind_To_All_IP_Addresses is set to 'true',  the value 
of Bind_To_IP_Address will be ignored. -->
  <Bind_To_All_IP_Addresses>true</Bind_To_All_IP_Addresses>
  <Bind_To_IP_Address/>
</Syslog_Settings>
```

The long descriptive comments explain the meaning of each of the syslog settings and the possible values for each setting. To export the XML file without these descriptive comments, use the `-c` parameter.

Escaped Characters

A handful of characters represent special values in XML and require escaped characters. The following table shows these characters and an alternate way to represent them in an XML document.

Character	Escaped Character
`<`	`&lt;`
`>`	`&gt;`
`&`	`&amp;`
`'`	`&apos;`
`"`	`&quot;`

Glossary

addresses behind the firewall. A designated group of IP or network addresses that reside inside the firewall, used to differentiate incoming from outgoing traffic.

Administration module. The core module of the Security Reporting Center that controls user and team access, licensing and default time zone settings.

analysis task. The first of three stages of an event. During an analysis task, log file data is gathered and transferred to a FastTrends database.

Configuration database. The database to which product configuration data is written.

Content database. The database where report data is stored, and from which reports are generated. Report data is transferred to the Content database during the export task.

Content Database maintenance event. A built-in event that deletes records in a Content database that have been logged for deletion.

custom report range. A user-defined time interval for which reports are generated.

Database server. The installable component containing the Scheduler database, the Content database, and the Configuration database

department. A designated group of IP or network addresses that defines a department or other subgroup found on the network.

event. An action taken by Security Reporting Center to analyze log files. Events can be scheduled or run on demand. During an event, data from a log file is selected and transferred to an interim FastTrends database. The data is then exported to a report-ready Content database, from which reports can be rendered on demand.

export task. The second stage of an event. During the export task, data is exported from the FastTrends database to the Content database.

FastTrends database. A database to which data is transferred from the log file during an analysis task. The FastTrends database stores log file data in a compressed form.

Filter. A set of criteria used to include or exclude data from reports. Filters are created and attached using either of the Reporting modules.

FastTrends Database maintenance event. A built-in event that deletes records in a FastTrends database that have been logged for deletion.

Firewall Reporting module. An optional analysis module that works with the core modules of the Security Reporting Center to analyze and report on traffic and security on the firewall.

NetIQ LEA Service. The NetIQ service that retrieves log file records from a properly configured Check Point Management Server.

NetIQ Syslog Service. The built-in syslog service installed with Security Reporting Center. Certain firewalls do not generate accessible log files. The NetIQ Syslog Service collects log records and writes them to a specified location.

on-demand report. A dynamically generated report that can be accessed at any time by clicking the View Report icon.

On-Demand report range. A recurring range of time for which on-demand reports are generated, such as every day, week, or month.

On-Demand Reporter. The interactive HTML interface used to access reports. Each instance of the On-Demand Reporter can show all the reports generated for a single profile.

profile. A set of user-defined criteria that determine how firewall log file information will be collected.

Proxy Reporting module. An optional analysis module that works with the core modules of Security Reporting Center to analyze and report on Web and FTP activity generated by users inside the firewall.

Reporting agent. The component of Security Reporting Center that analyzes log files.

Scheduler agent. A software component silently installed with the major components of the Security Reporting Center. (See the installation chapters for more information.) Scheduler agents divide events into tasks and distribute the tasks to Reporting agents.

Scheduler database. The database component to which information about event scheduling is written.

Scheduler module. The core module of Security Reporting Center that controls the timing of events and the content of reports. It also displays information about the progress of scheduled events and their component tasks.

Task. A discrete segment of an event that can be assigned to a Reporting agent. A Security Reporting Center event is made up of an analysis task and an export task.

Content database table size. The number of rows of data per table that can be exported from the FastTrends database to a Content database.

User Interface server. The installable component that runs the Security Reporting Center user interface.

NetIQ Document Utility. A utility used to convert a report into a non-HTML format such as Microsoft Word, PDF, or CSV.

Security Reporting Center. A scalable, browser-based reporting framework that can be customized to track security violations and internal and external user activity on firewalls and proxy servers. Security Reporting Center includes the Firewall Reporting and Proxy Reporting modules, which provide specialized analysis and reporting tools.

URL Categorization. A feature in the Proxy Reporting module that identifies the content of Internet sites accessed by internal users by matching them against one or more categorization databases.

Index