# Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Introducing Eventia Reporter</strong></td>
<td>5</td>
</tr>
<tr>
<td>The Eventia Reporter Solution</td>
<td>5</td>
</tr>
<tr>
<td>Log Consolidation Process</td>
<td>6</td>
</tr>
<tr>
<td>DBsync</td>
<td>7</td>
</tr>
<tr>
<td>Basic Concepts and Terminology</td>
<td>7</td>
</tr>
<tr>
<td>Predefined Reports</td>
<td>7</td>
</tr>
<tr>
<td>Eventia Reporter Considerations</td>
<td>8</td>
</tr>
<tr>
<td>Eventia Reporter Backward Compatibility</td>
<td>8</td>
</tr>
<tr>
<td>Standalone vs. Distributed Deployment</td>
<td>9</td>
</tr>
<tr>
<td>Log Availability vs. Log Storage and Processing</td>
<td>9</td>
</tr>
<tr>
<td>Log Consolidation Phase Considerations</td>
<td>9</td>
</tr>
<tr>
<td>Report Generation Phase Considerations</td>
<td>10</td>
</tr>
<tr>
<td>Eventia Reporter Database Management</td>
<td>11</td>
</tr>
<tr>
<td>Tuning the Eventia Reporter Database</td>
<td>11</td>
</tr>
<tr>
<td><strong>Getting Started</strong></td>
<td>15</td>
</tr>
<tr>
<td>Starting Eventia Reporter</td>
<td>15</td>
</tr>
<tr>
<td>Provider-1</td>
<td>15</td>
</tr>
<tr>
<td>Licenses</td>
<td>15</td>
</tr>
<tr>
<td><strong>Using Eventia Reporter</strong></td>
<td>16</td>
</tr>
<tr>
<td>Quick Start</td>
<td>16</td>
</tr>
<tr>
<td>Generating a Report</td>
<td>16</td>
</tr>
<tr>
<td>Scheduling a Report</td>
<td>17</td>
</tr>
<tr>
<td>Customizing a Report</td>
<td>17</td>
</tr>
<tr>
<td>Viewing Report Generation Status</td>
<td>17</td>
</tr>
<tr>
<td>Starting and Stopping the Log Consolidator Engine</td>
<td>19</td>
</tr>
<tr>
<td>Configuring Consolidation Settings and Sessions</td>
<td>19</td>
</tr>
<tr>
<td>Exporting and Importing Database Tables</td>
<td>21</td>
</tr>
<tr>
<td>Configuring Database Maintenance Properties</td>
<td>22</td>
</tr>
<tr>
<td>Eventia Reporter Instructions</td>
<td>23</td>
</tr>
<tr>
<td>Required Security Policy Configuration</td>
<td>23</td>
</tr>
<tr>
<td>Express Reports Configuration</td>
<td>23</td>
</tr>
<tr>
<td>Report Output Location</td>
<td>24</td>
</tr>
<tr>
<td>Using Accounting Information in Reports</td>
<td>24</td>
</tr>
<tr>
<td>Additional Settings for Report Generation</td>
<td>25</td>
</tr>
<tr>
<td>Generating Reports using the Command Line</td>
<td>25</td>
</tr>
<tr>
<td>Reports based on Log Files not part of the Log File Sequence</td>
<td>25</td>
</tr>
<tr>
<td>Generating the Same Report using Different Settings</td>
<td>25</td>
</tr>
<tr>
<td>How to Recover the Eventia Reporter Database</td>
<td>25</td>
</tr>
<tr>
<td>How to Interpret Report Results whose Direction is &quot;Other&quot;</td>
<td>26</td>
</tr>
<tr>
<td>How to View Report Results without the Eventia Reporter Client</td>
<td>26</td>
</tr>
<tr>
<td>How to Upload Reports to a Web Server</td>
<td>26</td>
</tr>
<tr>
<td>Uploading Reports to an FTP Server</td>
<td>27</td>
</tr>
<tr>
<td>Distributing Reports with a Custom Report Distribution Script</td>
<td>27</td>
</tr>
<tr>
<td>Improving Performance</td>
<td>28</td>
</tr>
<tr>
<td>Dynamically Updating Reports</td>
<td>29</td>
</tr>
<tr>
<td>Creating a Report in a Single File</td>
<td>30</td>
</tr>
<tr>
<td>Consolidation Policy Configuration</td>
<td>30</td>
</tr>
<tr>
<td>Overview</td>
<td>30</td>
</tr>
<tr>
<td><strong>Troubleshooting</strong></td>
<td>32</td>
</tr>
<tr>
<td>Common Scenarios</td>
<td>32</td>
</tr>
<tr>
<td><strong>Out of the Box Consolidation Policy</strong></td>
<td>36</td>
</tr>
</tbody>
</table>
Predefined Consolidation Policy ................................................................. 36
Out of the Box Consolidation Rules .............................................................. 36
Predefined Reports .......................................................................................... 38
Anti-Virus & Anti-Malware Blade Reports ......................................................... 38
Content Inspection Reports ............................................................................. 38
Cross Blade Network Activity Reports ............................................................. 39
Cross Blade Security Reports .......................................................................... 40
Endpoint Security Blade Reports ..................................................................... 40
Event Management Reports ............................................................................ 41
Firewall Blade - Activity Reports ..................................................................... 41
Firewall Blade - Security Reports ..................................................................... 42
Firewall GX ...................................................................................................... 42
Firewall Network Activity ................................................................................. 43
InterSpect Reports ........................................................................................... 43
IPS Blade Reports ............................................................................................ 44
IPSEC VPN Blade Reports ................................................................................. 44
My Reports ....................................................................................................... 45
Network Security Reports ............................................................................... 45
Regulatory Compliance Reports ...................................................................... 46
SSL VPN Blade Reports ................................................................................... 47
System Information Reports ............................................................................. 48
Index .................................................................................................................. 49
Chapter 1

Introducing Eventia Reporter

In This Chapter

The Eventia Reporter Solution 5
Eventia Reporter Considerations 8
Eventia Reporter Database Management 11

The Eventia Reporter Solution

Check Point Eventia Reporter delivers a user-friendly solution for monitoring and auditing traffic. You can generate detailed or summarized reports in the format of your choice (list, vertical bar, pie chart etc.) for all events logged by Check Point Security Gateway, SecureClient and IPS.

Eventia Reporter implements a Consolidation Policy, which goes over your original, "raw" log file. It compresses similar events and writes the compressed list of events into a relational database (the Eventia Reporter Database). This database enables quick and efficient generation of a wide range of reports. The Eventia Reporter solution provides a balance between keeping the smallest report database possible and retaining the most vital information with the most flexibility.

A Consolidation Policy is similar to a Security Policy in terms of its structure and management. For example, both Rule Bases are defined through the SmartDashboard's Rules menu and use the same network objects. In addition, just as Security Rules determine whether to allow or deny the connections that match them, Consolidation Rules determine whether to store or ignore the logs that match them. The key difference is that a Consolidation Policy is based on logs, as opposed to connections, and has no bearing on security issues.

The Log Consolidation Solution diagram illustrates the Consolidation process, defined by the Consolidation Policy. After the Security Gateways send their logs to the Security Management server, the Log Consolidator Engine collects them, scans them, filters out fields defined as irrelevant, merges records defined as similar and saves them to the Eventia Reporter Database.

Figure 1-1  Log Consolidation Solution
The Eventia Reporter server can then extract the consolidated records matching a specific report definition from the Eventia Reporter Database and present them in a report layout.

**Figure 1-2**  Eventia Reporter Report Generation

Two types of reports can be created: Standard Reports and Express Reports. The Standard Reports are generated from information in log files through the Consolidation process to yield relevant analysis of activity. Express Reports are generated from SmartView Monitor History files and are produced much more quickly.

Eventia Reporter Standard Reports are supported by two Clients:
- SmartDashboard Log Consolidator — manages the Log Consolidation rules.
- Eventia Reporter Client — generates and manages reports.

The interaction between the Eventia Reporter client and Server components applies both to a distributed installation, where the Security Management server and Eventia Reporter’s Server components are installed on two different machines, and to a standalone installation, in which these Software Blades are installed on the same machine.

**Log Consolidation Process**

It is recommended to use the Log Consolidator’s predefined Consolidation Policy (the Out of the Box Policy), designed to filter out irrelevant logs and store the most commonly requested ones (such as blocked connection, alert or web activity logs). The Log Consolidator Engine scans the Consolidation Rules sequentially and processes each log according to the first Rule it matches.

Figure 1-3 illustrates how the Consolidation Policy processes logs: when a log matches a Consolidation Rule, it is either ignored or stored. If it is ignored, no record of this log is saved in the Eventia Reporter system, so its data is not available for report generation. If it is stored, it is either saved as is (so all log fields can later be represented in reports), or consolidated to the level specified by the Rule.

**Figure 1-3**  Event Consolidation Flow Chart

The consolidation is performed on two levels: the interval at which the log was created and the log fields whose original values should be retained. When several logs matching a specific Rule are recorded within a predefined interval, the values of their relevant fields are saved “as is”, while the values of their irrelevant fields are merged (for example, “consolidated”) together.

**How to interpret Computer names in DHCP enabled networks**

In DHCP address mapping is used. Assuming the DNS knows how to resolve dynamic addresses, the information you see in the report reflects the correct resolving results for the time the reported log events have been processed by the SmartDashboard Log Consolidator and inserted into the database.
Because of the dynamic nature of DHCP address distribution, there is no guarantee that consolidation of old log files will produce correct address name resolving.

When DHCP is in use, consolidating log files close to the time of their creation will improve address-resolving accuracy.

**DBsync**

DBsync enables Eventia Reporter to synchronize data stored in different parts of the network. In distributed information systems DBSync provides one-way synchronization of data between the Security Management servers object database and the Eventia Reporter machine, and supports configuration and administration of distributed systems.

With DBsync, initial synchronization is established between the Eventia Reporter machine and the Management machine (for example, Security Management server or MDS). If the initial synchronization is not complete the administrator will receive a warning informing him that the GUI will open in read-only mode. Once initial synchronization is complete Eventia Reporter will open in Read/Write mode.

As a result of DBsync, whenever an object is saved (that is, a new object is created or an existing object is changed) on a Management machine the object is automatically synchronized in the Eventia Machine.

**Note** - When working in Provider-1 mode you must select a customer(s) that will initiate a synchronization with the CMA of the selected customer (Tools > Customer Activation).

Synchronization can take time up to 30 minutes, although this is usually the time needed for a very large database.

### Basic Concepts and Terminology

- **Automatic Maintenance** - the process of automatically deleting and/or archiving older database records into a backup file.
- **Consolidation** - the process of reading logs, combining instances with the same key information to compress data and writing it to the database.
- **Consolidation Policy** - the rules to determine which logs the consolidator will accept and how to consolidate them. We recommend that you use the out-of-the-box policy without change.
- **Consolidation Session** - an instance of the consolidation process. There can be one active session for every log server.
- **Express Reports** - reports based on the SmartView Monitor counters and SmartView Monitor History files. These reports are not as flexible as standard reports but are generated quickly.
- **Log Sequence** - the series of log files as specified by `fw.logtrack`. When a log switch is performed, the log file is recorded in the sequence of files. The log consolidator can follow this sequence.
- **Report** - a high-level view of combined log information that provides meaning to users. Reports are comprised of sections.
- **Standard Reports** - reports based on consolidated logs.
- **$RTDIR** - the installation directory of the Eventia Reporter.

### Predefined Reports

The Eventia Reporter client offers a wide selection of predefined reports for both Standard and Express reporting, designed to cover the most common network queries from a variety of perspectives (see "Predefined Reports" on page 38).

### Eventia Reporter Standard Reports

The Log Consolidation process results in a database of the most useful, relevant records, known as the Eventia Reporter Database. The information is consolidated to an optimal level, balancing the need for data availability with the need for fast and efficient report generation.
Reports are generated based on a single database table, specified in the Reports view > Standard Reports > Input tab. By default, all consolidated records are saved to the CONNECTIONS table and all reports use it as their data source. However, each time you create a new consolidation session, you have the option of storing records in a different table.

Dividing the consolidated records between different tables allows you to set the Eventia Reporter client to use the table most relevant to your query, thereby improving the Eventia Reporter server's performance. In addition, dividing records between tables facilitates managing the Eventia Reporter Database: you can delete outdated tables, export tables you are not currently using to a location outside of the Eventia Reporter Database and import them back when you need them.

**Eventia Reporter Express Reports**

Express Reports are based on data collected by Check Point system counters and SmartView Monitor History files. Standard Reports, in contrast, are based on Log Consolidator logs. Because Express Reports present historical data, they cannot be filtered, but they can be generated at a faster rate.

Express Reports are supported by one Client, the Eventia Reporter. To configure your system to generate Express Reports, see Express Reports Configuration (on page 23).

The Express Report Architecture diagram illustrates the Eventia Reporter architecture for Express Network Reports:

![Express Report Architecture](image)

**Report Structure**

Each report consists of a collection of sub-topics known as sections, which cover various aspects of the report. For example, the User Activity report consists of sections such as User Activity by Date, Top Users and Top Services for User Related Traffic.

**Customizing Predefined Reports**

You can easily customize the report that is closest to your needs (by changing its date range, filters etc.) to provide the desired information. Changing the filters of a predefined report constitutes a change in the nature of the report and the report must therefore be saved in a different location or under a different name. You can save the customized report under a different name in the report subject dedicated to user-defined reports, My Reports.

**Eventia Reporter Considerations**

Eventia Reporter's default options have been designed to address the most common reporting needs. To maximize the product's benefits, it is recommended that you adapt it to your specific profile. This section describes the considerations you should take into account before starting to use Eventia Reporter.

**Eventia Reporter Backward Compatibility**

Eventia Reporter supports Security Management servers of the following versions:

- Eventia Reporter R60 with SmartCenter R60
- Eventia Reporter R60A with SmartCenter R60A
• Eventia Reporter R61 with SmartCenter R61
• Eventia Reporter R62 with SmartCenter R62
• Eventia Reporter R65 with SmartCenter R65
• Eventia Reporter R70 with SmartCenter R70

Standalone vs. Distributed Deployment

In a standalone deployment, all Eventia Reporter server components (the Log Consolidator Engine, the Eventia Reporter Database and the Eventia Reporter server) are installed on the Security Management server machine. In a distributed deployment, the Eventia Reporter server components and the Security Management server are installed on two different machines. They communicate through standard Check Point protocols such as LEA and CPMI.

The standalone deployment saves relegating a dedicated machine for the Eventia Reporter, but the distributed deployment significantly improves your system's performance.

Log Availability vs. Log Storage and Processing

Since all Eventia Reporter operations are performed on the logs you have saved, the extent to which you can benefit from this product depends on the quality of the available logs. Therefore, you must ensure your Security Policy is indeed tracking (logging) all events you may later wish to see in your reports.

In addition, you should consider how accurately your logs represent your network activity. If only some of your Rules are tracking events that match them, the events' proportion in your reports will be distorted. For example, if only the blocked connections Rule is generating logs, the reports will give you the false impression that 100% of the activity in your network consisted of blocked connections.

On the other hand, tracking multiple connections results in an inflated log file, which not only requires more storage space and additional management operations, but significantly slows down the Consolidation process.

Log Consolidation Phase Considerations

Record Availability vs. Database Size

Reports are a direct reflection of the records stored in the Eventia Reporter Database. To generate detailed, wide-ranging and accurate reports, the corresponding data must be available in the database.

However, effective database management requires keeping the database table size from growing too large. As the consolidated records accumulate in the database, the tables where they are saved may become quite large. The data gradually approaches the disk space limit, using more and more memory and slowing down the Eventia Reporter processes (especially the data retrieval for report generation). Refer to Automatically Maintaining the Size of the Database (on page 14) for additional information on how Eventia Reporter tackles database management.

Carefully consider which logs you wish to store, and to what extent you wish to consolidate them.

Saving Consolidated Records to One vs. Multiple Database Tables

A report is generated based on a single table. If you save all consolidated records to the same table, all the data is readily accessible and you are saved the trouble of moving records between tables and selecting the appropriate source table for each report you wish to generate.

Dividing the records between different tables reduces the report generation time and allows you to maintain a useful database size by exporting tables you are not currently using to an external location.

High Availability


In High Availability, the active Security Management server always has one or more standby Security Management servers that are ready to take over from the active Security Management server. These Security Management servers must all be of the same Operating System (for instance, all Windows NT), and
have to be of the same version. The existence of the standby Security Management server allows for crucial backups to be in place:

- for the Security Management server - the various databases in the corporate organization, such as the database of objects and users, policy information and ICA files are stored on both the Standby SCSs as well as the active Security Management server. These Security Management servers are synchronized so data is maintained and ready to be used. If the active Security Management server is down, a standby Security Management server needs to become Active in order to be able to edit and install (that is, enforce) the Security Policy.

- for the gateway - certain operations that are performed by the gateways via the active Security Management server, such as fetching a Security Policy, or retrieving a CRL from the Security Management server, can be performed on standby Security Management server.

In a High Availability deployment the first installed Security Management server is specified as the Primary Security Management server. This is a regular Security Management server used by the system administrator to manage the Security Policy. When any subsequent Security Management server is installed, these must be specified as Secondary Security Management servers. Once the Secondary Security Management server has been installed and manually synchronized, the distinctions between Primary versus Secondary is no longer significant. These servers are now referred to according to their role in the Management High Availability scenario as Active or Standby, where any Security Management server can function as the active Security Management server.

When changes are made to report definitions (including report schedules), consolidation sessions and their settings, automatic maintenance configuration and report configuration, the information is stored in the active Security Management server and will be synchronized to the secondary Security Management server when a user synchronizes the Security Management servers.

The report generation results are not synchronized between Security Management servers. For instance, when Eventia Reporter generates a report connected to Security Management server A, a record of its generation will be stored in Security Management server A. When Eventia Reporter generates a report connected to Security Management server B, a record of its generation will be stored in Security Management server B. The Activity Log in Security Management server A will not be visible in Security Management server B and vice versa. However, even though the Activity Log in the inactive Security Management server A is not visible, it is still possible to connect to the inactive Security Management server A in read-only mode to access the report generations that are not visible in Security Management server B.

Report Generation Phase Considerations

Adapting the Report's Detail Level to your Needs

When a report is very detailed, it may become difficult to sort out the most significant results and understand it. To achieve the optimal balance between getting the right level of detail in your reports, closely examine the report's date range, filters (source, destination, service etc.) and filter values, and adjust them to pinpoint details.

Generating Only Selected Sections

By default, specific sections are included in the report generation and sections that require a great deal of resources (that is, report generation time and the report's size) are not selected. However, you can generate any sections in the list provided by checking them in the Content tab associated with the selected report in the Reports > Definitions view.

Scheduling Reports

The Schedule feature allows you to set both delayed and periodic report generations.

If you wish to produce a detailed and lengthy report, you should consider postponing its generation and scheduling it so that it does not run at time of peak log creation activity since such a report generation might slow down your system.

In addition, it is useful to identify the reports you require on a regular basis (for example, a daily alerts report or a monthly user activity report) and schedule their periodic generations.
**Report Filters**

Reports are based on records of the most commonly required filters, such as Source and Destination. Specifying the appropriate filter settings is the key to extracting the information you are looking for.

For each filter you choose, specify the values, such as network objects or services, to be matched out of all values available for that filter. The available values are taken from the Security Management server and are refreshed on a regular basis. If you cannot see a value you have added through SmartDashboard in the available values list, refresh the list by selecting a different filter and then return to the previous one.

The Eventia Reporter client also allows you to include additional objects by manually adding them to the matched values list.

Filters and their values can be specified for all sections of a report using the Filter tab, or for individual sections by editing the section from the Content tab. Filters for individual section set in the Content tab will override conflicting filters set for all sections using the Filter tab.

**Report output (Email, FTP Upload, Web Upload, Custom)**

All report results are displayed on your screen and saved to the Eventia Reporter server.

By default, the report is saved in HTML output in an index.htm file; and in CSV (Comma Separated Values) format in a tables.csv file. The HTML file includes descriptions and graphs, but the CSV file contains only the report table units, without a table of contents, descriptions or graphs. The tables.csv is provided in order to conveniently import tables into applications like Excel.

**Table 1-1 Report Files and Formats**

<table>
<thead>
<tr>
<th>File Format</th>
<th>HTML</th>
<th>CSV</th>
</tr>
</thead>
<tbody>
<tr>
<td>File Name</td>
<td>index.htm</td>
<td>tables.csv</td>
</tr>
<tr>
<td>Includes</td>
<td>Table of contents, tables, descriptions, graphs.</td>
<td>Data only. Cell values separated by commas. Rows and tables separated by lines.</td>
</tr>
</tbody>
</table>

Before generating a report, determine whether you want it to be saved or sent to additional or different targets. For example, when you generate a user activity-related report, you may wish to make it available to all managers in your organization by sending them the output via email or by placing it on your intranet.

**Eventia Reporter Database Management**

All database management operations are performed through the Eventia Reporter Database Maintenance view.

**Tuning the Eventia Reporter Database**

To improve performance, adjust available RAM memory for MySQL usage (see UpdateMySQLConfig -R option for additional information). In addition, place the database data and log files on different hard drives (physical disks), if available. Moving the temporary directory to a different hard drive will improve the performance of report generation and will avoid the possible clash between the temporary database directory and the space intended for the data directory.

**Note** - In a Unix environment, the database configuration file can be found in $RTDIR/Database/conf/my.cnf, whereas on a Windows platform it can be found in %RTDIR%\Database\conf\my.ini.
Modifying Eventia Reporter Database Configuration

It is possible to change the Eventia Reporter Database settings by modifying the *my.cnf* file, located in the $RTDIR/Database/conf directory (in Windows, *my.ini*). This can be done by running the `UpdateMySQLConfig` application. Note that before running this application you must stop all Eventia Reporter services by running `evstop-reporter`.

Running the `UpdateMySQLConfig` application creates a backup of the database configuration file.

There are a number of factors that can improve performance of the Eventia Reporter's database. Most of these factors can be fine tuned by using the `UpdateMySQLConfig` utility.

- **RAM** - The database needs substantial amounts of RAM to buffer data up to 1200 MB. This can be set using `UpdateMySQLConfig -R`.

- **Temporary directories** - The database uses temporary disk space to perform intermediate operations (such as sorting and grouping during report generation and during the table import operation) and may require up to 50% of the current database size to generate large reports. After report generation the temporary directory is emptied.
  
  Generating a substantial report may fail to execute the required SQL query if there is not enough disk space for the temporary directory. The temporary directory can be moved to a new location using `UpdateMySQLConfig -T`.

- **Log files** - The database log files ensure that changes persist in the event of a system crash. Place these files on a device that is separate from the database's data files using the `UpdateMySQLConfig -L` option.

- **Database data files** - these files should be put on a large, fast disk. The database's data files can be placed on several disks. Use `UpdateMySQLConfig -A` to add a new file to the set of database files and use `UpdateMySQLConfig -M` to move an existing file to a new location. Do not place database files on a network drive since performance may suffer and in some instances the database will not work.

  The default database file is *ibdata1*. If this file needs to be moved to a new absolute directory (for example, *d:/Database/data*), verify that the directory exists and run:

  ```bash
  UpdateMySQLConfig -M -src=ibdata1 -dst="d:/Database/data/ibdata1"
  ```

  If you want to remove an absolute directory (for example, *d:/Database/data2* to *d:/Database/data*), verify that the directory exists and run the following:

  ```bash
  UpdateMySQLConfig -M -src="d:/Database/data/ibdata1" -dst="d:/Database/data2/ibdata1"
  ```

- **An alternative way to enlarge database capacity is to enlarge the maximum size of the default data file (*ibdata1*). Use the $RTDIR/Database/conf/my.cnf file (in Windows, *my.ini*) for the required configuration. In order to enlarge the maximum size of *ibdata1* edit the value `innodb_data_file_path` and change its maximum. For example, change

  ```ini
  innodb_data_file_path=ibdata1:10M:autoextend:max:40G
  ```

  to

  ```ini
  innodb_data_file_path=ibdata1:10M:autoextend:max:60G
  ```

  This will enable *ibdata1* to grow up to 60G.

  **Important** - You cannot lower the maximum size of the database. Doing so could result in database failure.

- **Default data directory** - this is the directory that contains the MySQL table definitions and data.

Changing the Database Data Directory

1. Run the command `cpstop`.

2. Move database files.
   
   The location of the database data files is specified in the *mysql* configuration file `my.ini` (Windows) or `my.cnf` (all other platforms).
   
   Open the *mysql* configuration file located in the directory $RTDIR/Database/conf/.

3. Locate the lines that begin as follows:

   ```ini
   datadir=
   innodb_data_file_path=
   ```

   The directories indicated by these entries are the directories and subdirectories that should be copied to the new location. The following example shows how these directories appear in the *mysql* configuration file.

   ```bash
   datadir="C:/Program Files/CheckPoint/EventiaReporter/R60/ReportingServer/Database/data"
   ```
innodb_log_group_home_dir="C:/Program Files/CheckPoint/EventiaReporter/R60/ReportingServer/Database/log"
innodb_data_file_path = ibdata1:10M:autoextend:max:40G

The entry `innodb_data_file_path`, records database files that were added or moved to absolute locations. Make sure that these recorded database files are copied to a new location so that they are not forgotten.

4. Modify the following fields in the `mysql` configuration file so that they match the new locations of the database data files: `datadir`, `innodb_data_file_path`.
   Make sure that the paths are written in Unix format, with forward (/) slashes between directories.

5. Run the command `cpstart`.

**UpdateMySQLConfig Syntax**

The `UpdateMySQLConfig` Options table contains the usage of the `UpdateMySQLConfig` application.

Syntax

```
UpdateMySQLConfig
[-A -f=string -s=number -auto[=true|=false] [ -m=number ] ]
[-R=number ]
[ -M -src=string -dst=string ]
[-T=string ]
[-L=string ]
[-h ]
```

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Sub-parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>-A</code></td>
<td><code>-f</code> - the name of the file to add.</td>
<td>add a new data file to the database.</td>
</tr>
<tr>
<td></td>
<td><code>-s</code> - the initial size of the file when it is created (format [0-9]+{KIMIG})</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>-auto</code> - specifies whether the database should grow the file on demand.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>-m</code> - the maximum size the file can grow (format [0-9]+{KIMIG}). If this option is not specified, the database will grow the file to the available size on the disk.</td>
<td></td>
</tr>
<tr>
<td><code>-R</code></td>
<td>Sets the level of database RAM usage.</td>
<td></td>
</tr>
<tr>
<td><code>-M</code></td>
<td><code>-src</code> - original file path</td>
<td>Moves a database file to a new location.</td>
</tr>
<tr>
<td></td>
<td><code>-dst</code> - destination file path</td>
<td></td>
</tr>
<tr>
<td><code>-T</code></td>
<td>Changes the path to MySQL temporary directory</td>
<td></td>
</tr>
<tr>
<td><code>-L</code></td>
<td>Changes the path to MySQL log directory and copies log files to the new location.</td>
<td></td>
</tr>
<tr>
<td><code>-h</code></td>
<td>Displays this help message.</td>
<td></td>
</tr>
</tbody>
</table>
Automatically Maintaining the Size of the Database

The Log Consolidator process continuously adds new records into the database as they are generated from the Security Gateway. Eventually, the space allocated for the database will fill up. Typically, users can manually archive or delete older, less pertinent records from the database to provide space for the newest records. Automatic Maintenance performs this process automatically. With Automatic Maintenance, the user selects a maintenance operation (whether it is deleting records or archiving them to an external file) and specifies high and low watermarks to trigger when Automatic Maintenance should occur.

The High Watermark value represents the percentage of space that can occupy the database and/or the age of database records (that is, how many days old the records are). When the database occupies too much space or the records are older than the specified age, then the conditions are right to trigger an Automatic Maintenance operation. The High Watermark values are checked once a day and if the percentage of space or the age of the database records is higher than the assigned values, the Automatic Maintenance operation is triggered.

The Automatic Maintenance operation will delete records from the database until it reaches the Low Watermark. For example, if you specify that the High Watermark is 80% and the Low Watermark is 70% then the operation will begin to delete the oldest records when the occupied space is over 80%.

Typically, it is recommended that 80% would be the High Watermark to avoid reaching 100% capacity in certain cases.

In addition, it is possible to specify which database tables will participate in Automatic Maintenance. Since some of the tables are created for special purposes (for example, a table created from an external log file), Automatic Maintenance should not be performed on them.

When deletion of records occurs during automatic maintenance, you may see that the database size grows at first. This is normal behavior since the database needs to keep duplicate information in case of a server crash. The database will recover the disk space allocated for logs for about an hour after the maintenance operation is complete.

Backing Up the Eventia Reporter Database

The Eventia Reporter Database system consists of a set of files that can be copied, compressed or backed up like any other file. Backup files require the same disk space as the original files. It is highly recommended to save backup copies of the Eventia Reporter Database files, which can later be used to recover from an unexpected database corruption. Proceed as follows:

1. Stop the Eventia Reporter services by running: `evstop -reporter`.
2. From the Eventia Reporter Database directories, copy the entire `data` directory tree (as specified by the `datadir` parameter in the `my.cnf` or `my.ini` file) to the backup location. You may compress them to save disk space. Copy any database and log files that may have been moved to a different location using the `UpdateMySQLConfig` utility.
3. Restart the Eventia Reporter services and run `rmdstart`. 
Chapter 2

Getting Started

In This Chapter

- Starting Eventia Reporter
- Licenses

Starting Eventia Reporter

To start Eventia Reporter, perform one of the following actions:

1. Select Start > All Programs > Check Point SmartConsole > Eventia Reporter.
2. Double-click the Eventia Reporter desktop icon.
3. From SmartDashboard, select Window > Eventia Reporter, or press Ctrl+Shift+R.

Eventia Reporter starts in the Reports view.

Provider-1

When working with Provider-1, select Tools > Customer Activation and select the customers that you wish to work with.

Licenses

Licenses are installed on the Eventia Reporter server on a per gateway basis.

When the license is installed on a per gateway basis the user must select which gateways for which reports are generated. With Provider-1, select the customers instead of the gateways.

If you have three gateways and you buy three licenses you do not have to select the gateways because the system knows that you only have three. If you have 4 gateways and three licenses you have to choose the gateways to which each license belongs.

Up to 5 UTM Edge devices are considered a single gateway. Beyond 5 each UTM Edge gateway is counted as an individual gateway.

The Eventia Reporter server will now search for the Eventia Reporter license on the Eventia Reporter machine and if the license is not found it will search for the previous license on the Management Server.
Quick Start

This section is a step-by-step guide that covers the basic Eventia Reporter operations.

Generating a Report

The following procedure demonstrates how to create a basic report based on a predefined template. Proceed as follows:

1. In the Reports view, select Definitions.
3. Access the Period tab to determine the period over which the report will be generated and the information that should be used to generate the report.
   - Report Period - In this area select one of the following options:
     - Relative Time Frame includes the time period relative to the report generation. This time period defines a proportional interval (for example, Last Week or This Quarter).
     - Specific Dates includes the exact time period for which the report will be generated.
4. Access the Input tab to determine the gateways for which you would like to generate a report. If more than one gateway is selected as your source, you can generate information per gateway, or create a summary for all the selected gateways.
   - Select Check Point Security Gateways - In this area select the Security Gateways that will participate in report generation:
     - Select all gateways selects all the Security Gateways that are run by the Security Management server.
     - Select specific gateways enables you to select specific Security Gateways that are run by the Security Management server, from the tree provided.
     - Add enables you to add a gateway to the existing tree.
   - Show Result - In this area select one of the following options:
     - Per gateway instructs the Eventia Reporter to create a report that details information for each of the selected gateways.
     - Summary of all gateways instructs the Eventia Reporter to create a report that summarizes the information associated with all of the selected gateways.
     - Generation Input - In this area select the database table that contains the information for the report you are generating. By default the CONNECTIONS table is the primary database table.
     - Sample Mode provides the information for a demo mode. This option is used when you want to see an example of the report you are creating.
     - Other Database Tables enables you to access the information on which you would like your report to be based.
5. Click the Generate Report button to create the Blocked Connections report.
6. Click **Yes** to display the results.
   A new window appears containing the results of the report generation. Scroll down this window to view the specific report output.

### Scheduling a Report

The following procedure allows you to coordinate the creation of a report ahead of time. Proceed as follows:

1. In the **Reports** view, select **Definitions**.
2. In the **Standard** tab, select **Firewall Blade - > Security > Blocked Connections**.
3. On the **Schedule** tab, click the **Add** button to create a new schedule or the **Edit** button to revise an existing schedule.
   - **Frequency** - In this area select how often you would like the report to be generated.
   - **Generate On** - With this option select the date on which Eventia Reporter should begin to generate the report.
   - **Schedule time** - With this option select the time at which Eventia Reporter should begin to generate the report.
   - **Schedule activation period** - This section is available once you decide the report should be generated more than once. In this area select the date on which Eventia Reporter should begin to generate the report and the date on which Eventia Reporter should stop generating the report (if at all).

### Customizing a Report

When you generate a report, you generate the selected component using its default properties, or adjust these properties to better address your current requirements. This section describes the most important properties you should examine before generating a report.

In this section you will learn how to customize a new report. For example purposes, you will learn how to create a Security report about Blocked Connections.

1. In the **Reports** view, select **Definitions**.
2. In the **Standard** tab select **Firewall Blade - Security > Blocked Connections**.
3. Select the **Content** tab to see the sections (that is, sub-topics) associated with this report.
4. Review the **Blocked Connections** sections by double-clicking a specific section. The window that appears contains information about the selected section.
   To remove a section from the **Blocked Connections** report, clear the checkbox next to the specific section's name in the **Content** tab.
5. Select **Blocked Connections** and configure the report using the tabs available.
6. Access the **Filter** tab to isolate the report data by limiting the records in the database by specific filters. For each filter you select, you can specify the values, such as network objects and services, to be matched out of all values available for that filter.
7. Click the **Generate Report** button to create the **Blocked Connections** report.
   This process may take several seconds to several hours, depending on the amount of data that is currently in the database.
8. Click **Yes** to display the results.
   A new window appears containing the results of the report generation. Scroll down this window to view the specific reports output.

### Viewing Report Generation Status

In this section you will learn how to follow the progress of report generation using the **Reports** and **Management** views.

#### To View Report Generation Schedules

- In the **Reports** view, select **Schedules**.
  The **Schedules** view lists all the generation schedules of all the reports in your system, as defined in the **Schedule** tab of each report's properties. In this view, you can see a list of all the delayed reports and
periodic generation schedules. In addition, you can see the time, frequency and activation period of each scheduled report generation.

To improve performance, schedule report generation when there is less traffic and fewer logs are being generated, so the log consolidator is consuming fewer resources.

To View Reports and Status

- In the Reports view, select Results.

  The Results page lists reports that are either already generated, being generated, distributed or are pending. This view allows you to follow the report generation progress. In addition, once the generation is complete, it is recorded on the Activity Log page.

  The Results list contains the following information:
  - Name indicates the name of the report.
  - Action indicates the type of operation.
  - Status indicates the current status of the operation. For instance, if a specific report generation is waiting to be generated the status will be Pending.
  - Start Time indicates the time at which the operation began.
  - End Time indicates the time at which the operation ended and the time that a current report generation is expected to complete.

To View Server Activities

- In the Management view, select Activity Queue.

  The Activity Queue page lists reports and general activities that are either being generated, distributed or are pending. This view allows you to follow the report generation progress. Once the generation is complete, it is recorded in the Activity Log page.

  The Activity Queue list contains the following information:
  - Order indicates the order in which the reports will be generated. All operations are performed one at a time. The order column displays the order of the operations.
  - The order of pending operations can be changed.
  - Action specifies the operation that will be performed. That is, whether they are report generations or database maintenance operations.
  - Status indicates the current status of the operation. For instance, if a specific report generation is waiting to be generated the status will be Pending.
  - Start Time indicates the time at which the operation began.
  - Last Updated indicates the last time the status and the estimated completion time were updated.
  - Estimated End Time indicates the time at which the operation is expected to complete. This value is determined by analyzing the current operation and comparing the time it took to complete similar operations in the past.

To Stop a Specific Report Generation Process

1. In the Management view, select Activity Queue.
2. Select the report generation (that is, a specific line in the list) that you would like to stop.

To View the Status of Previously Generated Reports

1. In the Reports view, select Results.
   The Results View lists the status, start and end times of previously generated reports.
2. Double click a record to display the report results.

To Obtain Additional Information about the Status of a Previously Generated Report

1. In the Reports view, select Results.
2. Select the generated report (that is, a specific line in the list) that you are interested in.
3. Click the **Info** button in the toolbar.
   The **Action More Information** window appears. This window includes detailed information about the status in the **Results** view. For example, if the status of a generated report is **Failed**, this window will tell you why it failed.

The reporting server can store a limited amount of Report-Generation status records. In order to modify the amount of information stored, go to the **Tools > Options** window, and select the **Activity Log** page. Modify the amount in **Activity Log size**.

When the quantity of the status reports passes the limit, the oldest status record is deleted. You can decide whether you would like the associated generated Report to be deleted as well by changing the **Report output delete method** setting.

## Starting and Stopping the Log Consolidator Engine

### Starting the Log Consolidation Engine

If the Log Consolidation Engine is not running, you can start the Engine according to the Consolidation Policy that was last installed.

1. To start the Log Consolidation Engine, go to the **Management** section of the toolbar and select the **Consolidation** button.
2. Select the **Consolidation** session and click **Restart**.

### Stopping the Log Consolidation Engine

1. To stop the Log Consolidation Engine, go to the **Management** section of the toolbar and select the **Consolidation** button.
2. Select the **Consolidation** session and click **Stop**.
   The **Stop Engine** window is displayed.
3. Choose one of the following:
   - **Shutdown** — This option stops the Log Consolidation Engine in an order way. All data that has been consolidated up to this point is stored in the Database. Shutdown may take several minutes to an hour.
   - **Terminate** — This option stops the Log Consolidation Engine immediately. Data that has been consolidated but not yet stored in the Database is not saved.

## Configuring Consolidation Settings and Sessions

### To Create a Consolidation Session

When creating a Consolidation session you are determining the log server that should be used to extract information and the database table in which the consolidated information should be stored.

By default if there is a single log server connected to your Security Management server, a Consolidation session will already be created to read the latest logs that are added to the log sequence.

1. In the **Management** view, select **Consolidation**.
2. Select the **Sessions** tab.
3. Click the **Create New** button to create a new session. The **New Consolidation Session - Select Log Server** window opens.
4. Select the log server from which logs will be collected and will be used to generate reports. In Provider-1, you must select a customer before choosing the log server.
5. Click **Next**. The **New Consolidation Session - Select Log Files and database for consolidation session** window appears.
6. Choose whether to use the default source logs and default database tables, or select specific source logs and specific database tables for consolidation.
   If you select **Select default log files and database** click **Finish** to complete the process. This option indicates that the source of the reports will be preselected logs and all the information will be stored in the default database table named CONNECTIONS. The preselected logs are the sequence of log files that are generated by Check Point Software Blades. The preselected logs session will begin at the beginning of last file in the sequence or at the point the previous consolidation session was stopped.
If you select Customize continue with the next step. This option indicates that you will select the source logs and their target table in the next window.

7. Click Next. The New Consolidation Session - Log File window appears.
8. Select the source logs and the database table in which the information should be stored.
   - From the Read Log Files list, select the source of the information on which your reports are founded.
     - From the beginning of the sequence - the Consolidation session begins from the beginning of the first file in the log sequence.
     - Newly created from the end of the sequence - the Consolidation session begins from the end of last file in the log sequence.
     - Continuing the sequence from the last stopped position - the Consolidation session will begin from the point at which the previous Consolidation session stopped.
     - In the sequence starting from a specific log file - the Consolidation session begins from the beginning of a specific log file in the log sequence. Select the external log file from the list provided.
     
     Note - In the case of each of the above four options the Consolidation session will run continuously.

   - From a specific log file outside the sequence - the Consolidation session will consolidate external log files that are not in the log sequence. When Consolidation session reaches the end of the external log file, it will be stopped.
     If the specific external log file was previously processed the following two options are activated. Select the external log file from the list provided and select one of the following two options:
     - Beginning of file - the session will begin at the beginning of the selected log file.
     - Last stop - the session will continue from the point at which the previous Consolidation session stopped.

   - In the Database Table area select the table in which log file information should be stored.
     - Click the Policy Rules button to select the Consolidation policy rule that is defined in the SmartDashboard Log Consolidator view.
     - It is recommended that the Out of the Box policy be used. This option is for advanced users only, and by default the Policy Rules button should not be used.

9. Click Finish.
   The new session is added to the Consolidation Sessions list in the Sessions tab. The session will begin automatically.

**To View Detailed Information about a Specific Session**

1. In the Management view select Consolidation.
2. Select the Sessions tab.
3. In the Consolidation Sessions list select whose detail you would like to review.
4. Click the More Info... button.
   The Consolidated Session More Information window appears.

**To Configure Consolidation Settings**

When configuring the global session settings you are specifying the values according to the logs that are collected. Once the required log values are set, the Log Consolidator Engine collects them, scans them, filters out fields defined as irrelevant, merges records defined as similar and saves them to the Eventia Reporter database.

1. In the Management view select Consolidation.
2. Select the Settings tab.
3. Click the Set button.
   The Consolidation Parameters Settings window appears.
4. In the Resolved names - Source drop down list select whether the IP addresses in the logs source field should be resolved to a name from the Security Management database only or from the Security Management database and from DNS.
5. In the **Resolved names - Destination** drop down list select whether the IP addresses in the logs destination field should be resolved to a name from the Security Management database only or from the Security Management database and from DNS.

6. In the **Maximum requests handled concurrent** field enter the number of threads that should handle DNS requests. Adding additional threads can improve DNS performance at the cost of additional memory overhead.

7. In the **Refresh cached items every** field enter how long it should take for a resolved IP address to expire and be removed from the cache. If set too high it may result in wrong data because DHCP may change the addresses (recommended value 24 hours).

8. In the **Commit consolidated records every** field specify when the consolidator should stop consolidating records and write the records out to the Eventia Reporter database. By default it writes the consolidated records into the database once an hour.

9. In the **Maximum consolidation memory pool** field specify how much memory is allocated for consolidated records. When the memory is exceeded the consolidator writes the records to the Eventia Reporter database.

   **Note** - The Consolidation Memory Pool is only used by the consolidation engine per consolidation session. The database service requires additional memory and is largely dependent on installation configuration and the server generator.

10. Click the **NAT translation: Source** check box to indicate that the consolidation data will include real IP addresses as set in Security Management objects, or translated IP addresses as set in the SmartDashboard NAT tab for those logs where NAT translation was used.

11. Click the **NAT translation: Destination** check box to indicate that the consolidation data will include real IP addresses as set in Security Management objects, or translated IP addresses as set in the SmartDashboard NAT tab for those logs where NAT translation was used.

12. Select **Save full URL in database** if you would like URL records to be stored in the Eventia Reporter Database.

   By default the Eventia Reporter does not store URL information in the database. As long as this checkbox is disabled, some sections in the "Web activity" will give empty results (and are disabled by default).

Using the command line you can control DNS implementation Time Out requests and the number of retries. These changes will only take affect after restarting the consolidation sessions.

- Use the following command to control the Time Out requests for DNS implementation:
  Timeout in milliseconds for one request (default is 5 seconds):
  ```
  cpprod_util CPPROD_SetValue "Reporting Module" DNSRequestTimeoutMSec 4
  <Parameter> 1
  The following is an example for 5 seconds (5000 milliseconds):
  ```
  ```
  cpprod_util CPPROD_SetValue "Reporting Module" DNSRequestTimeoutMSec 4 5000 1
  ```

- Use the following command to control the number of retries for DNS implementation:
  Number of retries (default is 2 retries):
  ```
  cpprod_util CPPROD_SetValue "Reporting Module" DNSRequestRetries 4
  <Parameter> 1
  The following is an example for 2 retries:
  ```
  ```
  cpprod_util CPPROD_SetValue "Reporting Module" DNSRequestRetries 4 2 1
  ```

**Exporting and Importing Database Tables**

**Exporting a Database Table**

1. In the **Management** view select **Database Maintenance**.
2. Select the **Tables** tab.
3. Click the **Export** button.
4. Select the table from which you are exporting the selected file in the **Table** drop down list provided.
5. In the **Directory Location** field enter the base directory where to export the table.

   When you export a table using `c:/export`, several files will be stored in `c:/export/<timestamp>` and all the files will be given the tables name (for example, `<tablename>.tbl <tablename>.con02`, etc.)

   For example, if you export the `security Logs` table, the resulting files will be `security Logs.tbl` and `security Logs.con02`
etc.). In order to backup the export results save the entire content of the directory in $c:/export/<timestamp>$.

6. Click the Send Request button to revoke the operation.

**Importing a Database Table**

1. In the Management view select Database Maintenance.
2. Select the Tables tab.
3. Click the Import button.
4. In the File Location field enter the full path of the exported .tbl file (for example, $c:/export/<timestamp>/<tablename>.tbl$). When this is done all the files in the same directory as the .tbl file are imported.
5. Using the Target options select the destination table in which to import the data.
6. Click the Send Request button to revoke the operation.

**Exporting a Database Table to a Remote Machine**

Exporting a table to a remote machine from a Windows platform requires the correct permissions to perform the action. In order to set the permissions, perform the following steps:

1. Open the Eventia Reporter Server service by going to the Window's Start Menu > Settings > Control Panel and select Administrative Tools > Services.
2. Double click the Eventia Reporter Server entry.
3. Select the Log On tab and set user permissions to an appropriate account that has access to the network drive.

**Configuring Database Maintenance Properties**

The Management view enables you to create, start and stop Consolidation sessions. In this view you can also view the Database Maintenance properties and modify them.

**To Configure Automatic Maintenance**

The Log Consolidator process continuously adds new records into the database as they are generated from the gateway. Eventually, the space allocated for the database will fill up. Automatic Maintenance automatically archives or deletes older, less pertinent records from the database to provide space for the newest records.

Before configuring Automatic Maintenance you should decide whether Automatic Maintenance should only be triggered by disk space or by disk space and record age. In addition, you should determine what the minimum and maximum disk space and age of records you want to store in the database. Since the operation is resource intensive, it should be performed during a period of low activity (for example, in the middle of the night).

Typically, 80% is the High Watermark, since Eventia Reporter requires the extra space to perform generation optimizations.

1. In the Management view select Database Maintenance.
2. Select the Tables tab.
3. In the Database Tables list, select the table whose data should be automatically archived or deleted.
4. Click the Maintenance button.
   - The Table Participating in Automatic Maintenance window appears.
5. Activate the Participating in Automatic Database Maintenance check box and click the Send Request button.
6. Click OK until the process is complete.

**To Modify the Database Maintenance Properties**

1. In the Management view select Database Maintenance.
2. Select the Maintenance tab.
3. Click the Set button to modify the Database Maintenance properties. The Database Automatic Maintenance Setting window appears.

4. With the Automatic Maintenance Action options determine whether to archive or delete old records from the database, when the database capacity exceeds the high-watermark.

5. In the Time of action field, set the time at which the Automatic Maintenance action will start. This should be performed when there is a low level of activity on the server.

6. In the Database capacity (% of the total database physical size) fields, set the high- and low-watermark (that is, the high- and low-end values of database capacity).
   - When the database capacity exceeds the high-watermark, Automatic Maintenance is performed and the oldest records in the database tables are removed so that the capacity is at the low-watermark.

7. In the Days records stored in database fields, indicate the age of records in the database. When a record gets to be more than a specific number of days old (for example, the High-end number), that record is removed from the database.

8. Click OK to set the new Automatic Maintenance properties.

To Manually Archive or Delete Older, Less Pertinent Records from the Database

1. In the Management view select Database Maintenance.
2. Select the Maintenance tab.
3. Click the Activate Now button.

   The Activate Now button begins the process of maintaining the database according to the settings in the Database Automatic Maintenance Setting window.

Eventia Reporter Instructions

This section provides information on advanced or specific configuration scenarios.

For Express Report configuration, see Express Reports Configuration (on page 23).

Required Security Policy Configuration

For a Security Rule to generate logs for connections that match it, the Rule's Track column should be set to any value other than None (for example, Log generates a standard log, while Account generates an accounting log).

Note that in order to obtain accounting information (the number of bytes transferred and the duration of the connection), the value of the Rule's Track column must be Account.

To utilize direction information ("incoming", "outgoing", "internal" or "other"), the organization's topology must be configured properly.

Express Reports Configuration

The following procedure sets the SmartView Monitor to collect complete system data in order to produce Eventia Reporter Express Reports. SmartView Monitor settings are enabled through the SmartDashboard. Proceed as follows:

1. In the SmartDashboard network objects branch, select a gateway of interest. Double click the gateway to open the Check Point Gateway properties window.
2. You will need to enable the SmartView Monitor to collect data for reporting purposes through SmartDashboard.
   - If you do not see SmartView Monitor in the selection to the left, enable it through the General Properties tab. Click General Properties, then in the Check Point Products scroll-down list, select SmartView Monitor. It will appear on the left.
   - Select SmartView Monitor, and in the SmartView Monitor tab, enable one or all of the following options to ensure that SmartView Monitor is collecting necessary data for reporting purposes:
     - Check Point System Counters
- Traffic Connections
- Traffic Throughput

Note - Selecting Traffic Connections and Traffic Throughput in the SmartView Monitor tab may affect the performance of the gateway.

3. To finish this procedure, in SmartDashboard select Policy > Install.

Report Output Location

Report results are saved in subdirectories of the Results subdirectory of the Eventia Reporter server as follows:

<Result Location>/<Report Name>/<Generation Data & Time>

For each report, a directory with the report's name (for example, <Report Name>) is created in <Result Location>, with a subdirectory named with the generation date and time <Generation Date & Time>. The report is generated into this <Generation Date & Time> subdirectory.

The result location can be modified by selecting Tools > Options and specifying the desired location in the Result Location field of the Options window's Generation page.

In addition to saving the result to the Eventia Reporter server, you can send it to any of the following:

- The Client's display (the default setting).
- Email recipients.
- An ftp or a web server. See Uploading Reports to an FTP Server (on page 27).
- Via a Custom Report Distribution script.

The Mail Information page of the Options window allows you to specify both the sender's Email address and the mail server to be used. It also allows you to specify the degree of message severity (Information, Warning or Error) that is to be sent to the administrator.

The Mail Information page of the Tools > Options window allows you to specify that an administrator receive warnings about errors. To enable this option, fill in the Administrator email address, and choose the severity factor for which an error message will be sent, by checking one or more of the severity levels in the Specify the severity of the administrator email notification section.

Using Accounting Information in Reports

Data Calculation Scheme

By default, report calculations are based on the number of events logged. If you have logged accounting data (done by setting the Security Rule’s Track column to Account), you can base the report calculations on the number of bytes transferred.

Sort Parameter

You may sort the results by one of two parameters: the number of bytes transferred and the number of events logged. Note that an event takes on different meanings, depending on its context. In most cases, the number of events refers to the number of connections. Access this through the Tools > Options menu.

The number of bytes transferred can be calculated only if the Security Rules' Track column is set to Account. The number of events logged can be calculated as long as the Track column is set to Log or Account.

If both types of information are available, they will both be displayed in the sort order you have specified. For example, a table listing the most active sources in your system can first specify the number of events each source generated and then note the number of bytes related to its activity.

Format

In several scenarios the user name appears in long format (for example, LDAP names). The manner in which the report shows the user name can be changed through the Tools menu > Options > Generation
By default, the Show abbreviated user name check box is selected, so that generated reports display only the user name part of the full name. To see the name with the full path, uncheck this box.

Additional Settings for Report Generation

The Options window allows you to specify additional settings including the name and the location of the logo to be displayed in the report header, as well as where to email reports, and report-sorting settings.

By default, the logo file is saved in the $RTDIR/bin directory.

Generating Reports using the Command Line

For your convenience, it is possible to generate reports both through the Eventia Reporter client and through the command line.

Generating reports using the command line GeneratorApp has the following limitations:

- No report status updates in the Management view's Activity Queue window and in the Results window.
- No distribution of the report result.

To generate reports through the command line, go to the $RTDIR/bin directory on the Eventia Reporter server and run the following command:

Usage: GeneratorApp [Directory/"""] {ReportID}

For example, to generate the Peer To Peer Activity report, whose ID is {60F6FCDA-0F66-43A6-B8E6-271247207F5B}, run the following command: GeneratorApp ./reports/test {60F6FCDA-0F66-43A6-B8E6-271247207F5B}

If the directory is empty (""), <Result location>/<Report Name>/<Generation Date & Time> would be used as the directory.

For a list of all Report IDs, see Predefined Reports (on page 38).

Reports based on Log Files not part of the Log File Sequence

To generate a report based on log files that are not part of the log file sequence (fw.log), you must first create a consolidation session to explicitly consolidate these log files.

To create a consolidation session refer to Configuring Consolidation Settings and Sessions (on page 19). When creating the consolidation session you should select From a specific log file outside the sequence in step 8.

So that data from the consolidation session based on an external log is not mixed with data from an internal sequence log we recommend that you use a new table for your external consolidation session.

When the consolidation session is complete generate reports based on log files that are not part of the log file sequence. To do this refer to Generating a Report (on page 16) and in step 3 select the table to which the external log file was consolidated.

Generating the Same Report using Different Settings

To schedule generations of the same report using different settings, modify the original report, save it under a different name (for example, Network_Activity_NYC, Network_Activity_Paris etc.) and specify the appropriate schedule for each modified report.

How to Recover the Eventia Reporter Database

To recover the Eventia Reporter database, proceed as follows:

1. Stop the Eventia Reporter by running evstop -reporter.
2. Replace the original Eventia Reporter database files with your backed up Eventia Reporter database files. The location of database files is defined by `datadir` and `innodb_data_file_path` entries in the `mysql` configuration file `my.ini` (Windows) or `my.cnf` (all other platforms).

3. Replace the database log files `ib_logfile[0-N]` under the log directory as specified by the `innodb_log_group_home_dir` parameter in the `my.ini` file with the backed up database log files.

4. Start the Eventia Reporter database service normally.

How to Interpret Report Results whose Direction is "Other"

To interpret direction data, the network's topology must be defined accurately. If the topology is not defined accurately, the traffic will be labeled with a direction of "Other."

How to View Report Results without the Eventia Reporter Client

You can make the report results available through an internet browser, by checking FTP Upload or Web Upload in the Output tab of the Report properties.

It is also possible to locate the report results on the Eventia Reporter server. To do this select Management > Activity Log and select More Information for the relevant historical generation status to view the full path of the location.

How to Upload Reports to a Web Server

In order to enable report uploads to a web server you must configure the report's output properties, and configure the web server to allow uploads.

**Configuring the Report Output tab**

1. Check the Web Upload checkbox.
2. Fill the server properties in the fields to the right of the checkbox list, including the web server's name or IP, the User Name and Password that Eventia Reporter uses to connect to the web server, and the Path of the directory in which the report results are saved.
3. Select how the new uploaded report is saved (that is, whether in a new directory or overriding the previous report).

**Configuring the Web Server**

Define the Report's Virtual Directory

1. You must define a virtual directory named `reports`, in the web server's root directory. All the Report files that are uploaded to the web server will be placed in this directory.
2. Grant this directory PUT command permission (also known as Write permission). It is not recommended that permission for anonymous http login be granted.

Create a Directory for each Report

For the Web upload, the Eventia Reporter uploads Report result files to the target directory. A target directory must exist at the time of the upload. The upload uses the `http:put` operation, and on most web servers, permission for this operation needs to be explicitly granted for the target directory.

There are 2 ways to ensure that target directories exist:

- Manual directory creation:
  
  On the web server, create a directory with the path `<report's directory root>/<optional path field>/<ReportName>` before generating the report. This operation needs to be performed only once.
  
  To avoid installing and configuring scripts create the directory manually. If you use this option, you must ensure that you select to Override Previous Report in the Report's Output tab.
If the Path field is left empty in the Report’s Output tab, create the folder `<report's directory root>/<ReportName>` on the web server.

- Automatic directory creation:
  
  a) Configure the `svr_webupload.pl` by running the `svr_webupload_config` utility:

  i) On the Eventia Reporter server, in the `$RTDIR/bin` directory, run the utility `svr_webupload_config` using the following command structure:

  ```
  svr_webupload_config [-i perl_int_loc] [-p rep_dir_root]
  ```

  Where `-i` specifies the Perl interpreter location and `-p` specifies the path for the reports virtual directory which you previously configured.
  
  An example of the command is:

  ```
  svr_webupload_config -i c:/perl/bin/perl.exe -p "c:/Inetpub/wwwroot/reports"
  ```

  ii) Copy the `svr_webupload.pl` file from the `$RTDIR/bin` directory from the Eventia Reporter computer to the `cgi-bin` directory on the web server.

  ![Note] - Both the `cgi-bin` directory and the script name can be changed in the Eventia Reporter Client via the `Tools > Options > Web Information > CGI Script Location` field.

  b) Grant the `svr_webupload.pl` script (on the web server only) execution permission. It is not recommended that permission be granted for anonymous http login.

### Uploading Reports to an FTP Server

In order to enable report uploads to an FTP server you must configure the Report’s output properties.

#### Configuring the FTP Upload

1. Enable the **FTP Upload** option.
2. Fill the server properties in the fields to the right of the option list, including the FTP server’s name or IP, the User Name and Password that Eventia Reporter uses to connect to the FTP server, and the Path of the directory in which the report results are saved.
3. Select how the new uploaded report is saved (that is, whether in a new directory or overriding the previous report).

The FTP upload does not require any configuration on the FTP server. The root directory for all report uploads is the FTP root directory the user specified in **User Name** field.

### Distributing Reports with a Custom Report Distribution Script

1. Place the script in the `$RTDIR/DistributionScripts` directory.
2. Make sure the name of the script matches the name given in the **Output** tab of the report definition. The script parameters are:
   - A path to the Report’s Result directory.
   - A string containing the Report name.

   In the **Customer Distribution** script the responsibility for distribution is placed on the user. The **Distribution Process** input is the directory that contains the report's output files. The script's exit code should be 0 upon success and none 0 upon failure.

   The **Customized Distribution** script will time-out after the number of seconds entered in the **Distribution** page of the Reporter’s options.
**To Set the Time-Out Value:**

1. Access the **Tools** menu and select **Options**.
2. Select the **Distribution** page.
3. Enter the number of seconds after which you would like the process to time-out.
4. Click **OK**.

For additional information, refer to Report output (Email, FTP Upload, Web Upload, Custom) (on page 11).

**Improving Performance**

For the most updated performance tuning information, see *Release Notes* for the Eventia Reporter at:

http://support.checkpoint.com (http://support.checkpoint.com)

**Performance Tips**

To maximize the performance of your Eventia Reporter server, follow the following guidelines.

**Hardware Recommendations**

- Use a computer that matches the minimum hardware requirements, as specified in the Release Notes at: http://support.checkpoint.com (http://support.checkpoint.com)
- Configure the network connection between the Eventia Reporter server and the Security Management, or the Log server, to the optimal speed.
- Use the fastest disk available with the highest RPM (Revolutions per Minute).
- Increase computer memory. It significantly improves performance (see Eventia Reporter Database Management (on page 11)).
- Increase the database and log disk size (for example, several gigabytes) to enable the Eventia Reporter to cache information for better report generation performance. If a report requires additional space for caching, it will be noted in the report's Generation Information section. The Generation Information section can be found in **Appendix A > View generation information** of the report result.

**Installation**

Use a distributed Security Management configuration, dedicating one computer to Consolidation and Report generation only.

**Log Consolidator**

Improve the Log Consolidator Engine’s performance by configuring the following settings:

1. Set the Consolidation Rules to ignore immaterial logs.
2. Change the consolidator settings:
   a) In Eventia Reporter select **Management > Consolidation > Settings**.
   b) Click the **Set** button.
   c) To improve DNS resolution performance, modify the following:
      - **Maximum requests handled concurrently** - Set to 50. This value controls the numbers of threads handling DNS requests.
      - **Refresh cached items every** - Set to 48 hours. This value determines how long it takes for a resolved IP address to expire and be removed from the cache setting. If set too high it may result in wrong data because DHCP may change the addresses.
   d) To turn off reverse DNS resolution, change **Object Database + DNS** to **Object Database** in the drop-down lists provided.
   e) To improve consolidation, modify the **maximum consolidation memory pool** to 256 MB according to the memory available on the Eventia Reporter server.
Note - The Consolidation Memory Pool is only used by the consolidation engine per consolidation session. The database service requires additional memory and is largely dependent on installation configuration and the server generator.

Report Section Generated

1. Do not choose unnecessary reporting elements. Deselect sections that are not relevant to your report. The Reporter Generator uses an internal cache for SQL query results therefore not every deselected section speeds up the report generation. In general, this will result in a smaller report and reduce generation time.

2. Table and Graph units that belong to the same section often use the same SQL, therefore deselecting only one of them may not decrease the generation time. It is recommended that you deselect (uncheck) an entire section.

3. If you deselect report sections, you should also deselect the matching category in the Summary section since it usually uses the same SQL query.

4. Every report contains a link to a file that contains details about the SQL queries that the Report Generator runs, how many queries are cached, and how long each query takes.
   To view this, scroll to Appendix A in the report result, and click View generation information at the bottom of Appendix A.

Report Filters

If you define different filters for different reporting units that share the same cached SQL, the SQL caching will no longer be viable and the report generation time will significantly increase. It is recommended that you define filters at the report level only.

Report Time Frame

When setting a user-defined time frame for the report, specify a time frame in whole days. When setting a report period, note that the following settings will slow down the report generation speed:

- Relative Time Frame for Last X hours
- Specific dates with Limit by Hour option
- Reports for short time periods are generated faster than reports for long time periods. A weekly report will be generated much faster than a monthly report.

Report Generation Scheduling

Schedule report generation when there is less traffic and fewer logs are being generated, so that the log consolidator will consume less resources. Schedule reports during the night and on the weekends.

Fine Tuning Eventia Reporter Database

Adjust the database cache size to match your Server’s available memory. Place the database data and log files on different hard drives (physical disks), if available. For additional information, refer to Modifying Eventia Reporter Database Configuration (on page 12).

Dynamically Updating Reports

To dynamically update reports an administrator must first obtain an update file that contains all the report changes. This file is provided by Check Point.

Once the is received and saved perform the following:

1. Access the Eventia Reporter File menu and select Import Reports....
   The Offline Update window appears.

2. Select Browse and chose the update file received from Check Point.

3. Click the View update info button.
   The file is opened in a browser.

4. Review all the changes and their descriptions.
5. Click **Update Now**. At this point the administrator will be asked to save the previous version before the changes are installed.

6. Click **Save As** and specify the location in which the previous version file should be saved (for example, My Reports > Old Blocked Connections).
   At this point the Eventia Reporter server is updated.

Once the process is complete the administrator will receive a file from Check Point informing him that the Predefined Reports have been updated.

**Creating a Report in a Single File**

When configuring a report you can select one of the following output formats:

- **HTML** contains multiple HTML files. If the output is an email, the email will contain a zip file with all of the report's components (for example, images, data, etc.).
- **MHT** contains multiple HTML files in one file. That is, all of the report's HTML files are compiled into one file. If the output is an email the email will contain two attachments. One attachment will open a screen version and the second attachment is a printer ready version. The report will appear as it does in the Eventia Reporter Sample tab.

**To create a report in one file:**

1. In Eventia Reporter select the **Predefined** report for which you would like to send a report in one file.
2. Select the **Output** tab.
3. In the **File Format** drop-down list select **MHT**.
   The file created has an .mht extension.

**Consolidation Policy Configuration**

**Overview**

The Out of the Box Consolidation Policy has been designed to address the most common Consolidation needs. However, in case you have specific Consolidation needs that are not covered by this Policy, the Consolidation Rules can be modified as needed.

**To modify the Consolidation settings, proceed as follows:**

1. Display the **SmartDashboard's Log Consolidator** View, by selecting **View > Products > Reporter Log Consolidator** from the menu.
2. Modify the Out of the Box Policy's Consolidation Rules as needed. Refer to Customizing Predefined Consolidation Rules (on page 31) for additional information.
3. Save the modified Policy under a different name (select **File > Save As** from the menu and specify the modified Policy's name).
4. In Eventia Reporter select **Management > Consolidation > Sessions** to create a new consolidation session.
5. Select the **Start New** button.
6. Select the relevant log server in which logs will be collected and will be used to generate reports and click Next.
7. Select **Customize** and click **Next** in order to select specific source logs and specific database tables for consolidation.
8. The **New Consolidation Session - Log File** window appears.
9. Select the source logs and the database table in which the information should be stored.
   - From the **Log File** list select the source of the information on which your reports are founded.
   - In the **Database Table** area select the table in which log file information should be stored.
   - Click the **Policy Rules** button to select the Consolidation policy rule that is defined in the SmartDashboard Log Consolidator view.
   - It is recommended that the Out of the Box policy be used.
10. Click Finish.
The new session is added to the **Consolidation Sessions** list in the **Sessions** tab.

**Specifying the Consolidation Rule's Store Options**

To specify whether logs matching a Consolidation Rule should be skipped or copied to the Eventia Reporter database, right click the **Rule's Action** column and choose **Ignore** or **Store** (respectively).

It is recommended to place **Ignore Rules** at the beginning of the Rule Bases, especially for services that are logged frequently but are not of interest for reports. **Ignore Rules** do not require Consolidation processes and, therefore, enable the Log Consolidator Engine to move quickly through the logs. The Log Consolidator Engine does not have to consolidate and store an event that matches an **Ignore Rule** and can quickly move to the next entry in the Log file.

The Rule order is also based on how frequently services are used. Rules regarding the most common services are defined before those addressing less common services. In this way, the Log Consolidator Engine does not have to scan a lengthy Rule Base in order to process most of your log data.

If you choose to store the logs, double click the **Action** cell to specify their storage format in the **Store Options** window. Choose one of the following:

- **As Is** — all log fields will be stored in the Eventia Reporter database and will be available for report generation. This is the default storage option.

- **Consolidated** — specify the interval at which logs matching this Rule are consolidated (for example, all logs generated within a 10 minute interval). Hourly intervals are measured.

By default, the Log Consolidator Engine loads the consolidated records to the Eventia Reporter database once an hour.

**Customizing Predefined Consolidation Rules**

This section provides instructions on modifying specific Out of the Box Rules to better address your specific consolidation requirements. For a detailed description of the Out of the Box Rules, see Out of the Box Consolidation Policy (on page 36).

If you wish to filter out all broadcast messages (both allowed and disallowed), proceed as follows:

1. In the Security Policy, define a group of objects with broadcast IP addresses.
2. In the Out of the Box Consolidation Policy, activate the broadcast Rule and add the broadcast group to its **Destination** column.
Chapter 4

Troubleshooting

In This Chapter

Common Scenarios

Common Scenarios

Eventia Reporter server is not running. Where can I get information to solve the problem?

To solve this problem perform one of the following:

- Run the `evstart -reporter` command to restart the Eventia Reporter server.
- Review the error information in the log file. The log file for the Eventia Reporter server can be found in `$RTDIR/log/SVRServer.log`. This file contains advanced log information about problems running the Eventia Reporter server.

Log Consolidator is not running. Where can I get information to solve the problem?

To solve this problem perform one of the following:

- Ensure that the consolidation session is defined in the Management > Consolidation window.
- If the session status indicates that logs are not being processed refer to the `$RTDIR/log_consolidator_engine/log/<Session_ID>/lc_rt.log` and check for errors. If there are errors restarting the session may solve the problem.
- If you defined logs outside the sequence, the consolidation process will stop when file processing is completed. In this case, you will receive the following message in the log file: "The engine has finished scanning the requested log files.”. The log file for the Log Consolidator can be found in `$RTDIR/log_consolidator_engine/log/<Session_ID>/lc_rt.log`. This file contains advanced log information about problems running the Log Consolidator.

I performed an upgrade from a previous version of Eventia Reporter. The Consolidation session status in the Eventia Reporter client is "Aborted" and the following error appears in `lc_rt.log`:

Error: failed to fetch `<TableName>_ID` inter_code table data
Table 'rt_database.<TableName>' doesn't exist

-Or-

Report generation failed and the following error appeared:
Failed to execute SQL query. Error: Table 'rt_database.<TableName>' doesn't exist. SQL: `SELECT <TableName>_CODE, <TableName>_NAME FROM <TableName>`.

What should I do?

To solve this problem perform the following:

- Check the `SmartViewReporterInstallation.log` file located in `c:\Program Files\CheckPoint\CPInstLog\` on Windows or in `/opt/CPInstLog/` on any other platform. If the `SmartViewReporterInstallation.log` file includes the following error(s) perform the following 4 steps:

  Error: Error in process '/opt/CPrt-FLO/svr/bin/evr_upgrade_db /opt/CPrt-FLO/svr'. Error code is 2
  Info: Error in database upgrade. For Database upgrade run /opt/CPrt-FLO/svr/bin/evr_upgrade_db after evstop -reporter.
1. Run the `evstop -reporter` command.

2. Ensure that the database process is not running. The database process name is `mysql-d-nt.exe` for Windows or `mysqld` for all other platforms.

3. On a Windows platform run `%RTDIR%\bin\evr_upgrade_db.bat`. On any other platform run `$RTDIR/bin/evr_upgrade_db`.

4. Start Eventia Reporter by running the `evstart -reporter` command.

**Eventia Reporter has been installed and the Standard Reports are empty. What should I do?**

**To solve this problem perform one of the following:**

- Make sure that the database contains data for the dates for which you would like to generate the report. To do this select `Management > Database Maintenance`. Each row in the Database table shows the number of rows in the table, as well as the date range of all the table's entries.
- Verify that the specific report is generated from the same table that was filled by the consolidation session.
  a) Select `Management > Consolidation > Sessions` and note the database table from which the information is collected.
  b) Select the report definition's `Input` tab and verify that the same database table is selected in the `Other Database Tables` drop-down list.
  Make sure that the date range for the report is defined correctly. This can be verified by selecting the report definition's `Period` tab and confirming the `From` and `To` values.
- The data may have been eliminated by report filters. Verify that unnecessary filters (for example, a filter that eliminates information on all relevant IP addresses) have not been set. Open the `Filter` tab associated with the specific report to verify the filters being used.
- Open the `Input` tab associated with the specific report and verify that the correct gateways have been selected.
- Verify that the consolidation engine policy is defined to store the relevant records. See Report Generation Phase Considerations (on page 10) for additional information.
- The Standard Reports maybe empty due to a consolidation delay. The firewall may have sent the logs before consolidation was complete. This usually occurs in daily reports.

**When configuring an Express Report I do not see a particular gateway in the Input tab.**

A gateway in the Express Report `Input` tab will not appear if SmartView Monitor is not enabled on the gateway. In order to see the gateway in the `Input` tab, enable the gateway object in SmartDashboard and install the policy on the gateway. Similarly, VPN needs to be selected for VPN reports.

**After performing a Distributed installation the Eventia Reporter server is not communicating with the management and I cannot login to Eventia Reporter. What should I do?**

**To solve this problem perform one of the following:**

- The Reporter object is not completely defined in the Security Management server. In
  SmartDashboard, establish SIC with Eventia Reporter, select the Eventia Reporter checkbox for the host object representing the Eventia Reporter server and perform `Install Database` on all relevant log servers.
- Check the connectivity between the Security Management server and the Eventia Server. Once this is verified, check that the Eventia Reporter object in SmartDashboard is configured with the correct IP in the `General Properties > IP address` field. In addition, verify that there is connectivity between the client and the server on the `CP_reporting` service (port 18205).

**When one of the following reports is run no data is received. What should I do?**

*FTP Activity, SMTP Activity, Web Activity and User Activity*

For each FTP Activity, SMTP Activity and Web Activity report, create the associated resource and add a rule in the Security Policy whose service column uses this resource. For more information see the *IPS Administration Guide* for using resources in the rule base.

FTP Activity uses an FTP resource, SMTP Activity uses an SMTP resource and Web Activity uses a URI resource.

*User Activity*
You may not receive data for a User Activity report because your logs do not contain User information. Open one of the relevant logs in SmartView Tracker™ and check whether the User field is empty for a relevant log entry.

If fields are empty, consult the IPS Administration Guide for more information on User field logging options.

**In my rule base reports I see an asterisk after the rule number. What does this mean?**

Security Gateways add the rule’s unique ID to each log to track the rule even though it may have changed its location in the policy and has a different index.

When the rule’s ID is defined, the report displays the index to the rule at the time of report generation. However, when the rule’s unique ID is not available in a log, the Reporter uses the rule’s index. Since the rule index can change, the index may not accurately reflect the rule. The asterisk warns the user that the rule number may not be exact.

**Standard report generation failed with the following error:**

"Failed to write to result file, please check that there is enough disk space in the result directory for this report”.

**To solve this problem perform one of the following:**

- This error occurs when Eventia Reporter cannot write report files. In this case, verify that there is a Write Permission in the results directory. The Results Directory can be found in Tools > Options > Generation > Results Location.

- Verify that there is enough disk space for the generated reports. If there is not enough disk space, then free space for the results or change the reports output directory to a new location (that is, on another disk).

**Standard report generation failed with the following error:**

"Report generation optimization caused a failure of the report generation, could not populate temporary table. Error: Got error 28 from table handler'.

In this situation, there is not enough disk space in the temporary database directory. To solve this problem, change the location of the temporary database directory. Refer to Modifying Eventia Reporter Database Configuration (on page 12) for additional information.

**When trying to define a new consolidation session the following error appears:** "Failed to get the log files list from server/database”.

- OR -

After successfully defining a consolidation session the log file in the log consolidator contains the following error "The Engine cannot read the log file from the Log Server, and will automatically try to reconnect every several minutes”.

- OR -

The session status in the Eventia Reporter Consolidation window is "Trying to reconnect”.

**To solve this problem perform one of the following:**

- Verify that there is connectivity between the Eventia Reporter machine and the log server. Communication between the two occurs on FW1_lea service (port 18184).

- If you are working with an external log server that is not installed on the Security Management server, perform SmartDashboard > Policy > Install Database... and select the appropriate object from the list provided.

- If you are working with Provider-1 verify that the CMA is assigned a global policy and that its database was installed.

**The Logs read per second value in the More Info page is too low.**

This value indicates the average log processing speed since the session began. However, this number is not accurate at the time the consolidation session starts processing logs. Wait at least 15 minutes and if this value does not rise try to disable the DNS and run the consolidation session again. If disabling the DNS improves performance, you can enable only internal address resolution, based on the gateway topology. In order to do this, access Eventia Reporter and enable DNS resolution in Consolidation > Settings. Run the following command in order to only enable internal address resolution:

```bash
cpprod_util CPPROD_SetValue "Reporting Module" "dns_internal_only" 1 true 1
```

If you want to enable the resolution of all addresses run the same command with a false flag:

```bash
cpprod_util CPPROD_SetValue "Reporting Module" "dns_internal_only" 1 false 1
```

Maintenance was completed with the following warning: "Automatic maintenance cannot remove enough records to reach the low-end threshold since participating tables do not have enough old records to remove".
• Ensure that all the relevant tables an **Auto. Maintenance** flag On (in **Database Maintenance > Tables > Database Tables list**). For example, if a table was imported from a file, it will not participate in maintenance.

• Verify whether you need to enlarge the database capacity.

**Maintenance failed with a Table** \texttt{CONXX_<Table-Name> is full error. For example, ’Table ’CON02_CONNECTIONS’ is full”}.

• Enlarge the database capacity. Refer to **Modifying Eventia Reporter Database Configuration** (on page 12) for additional information.

  \begin{itemize}
  \item Note - In order to avoid this error in the future, it is recommended that you change the database capacity High End to not more than 75%.
  \end{itemize}

• Maybe the database can not reach its maximum capacity because there is not enough free disk space. In this case, free disk space.

**A scheduled report does not appear in Eventia Reporter until the report is saved.**

After defining a schedule for the specific report, save the report. A report will appear only after it is saved.

**The status of a consolidation session is ”Trying to reconnect”.** In addition, in the \texttt{lc_rt.log} file the following error appears: ”Database space check failed. There may not be enough disk space or it may have failed to obtain database capacity information”.

**To solve this perform the following:**

1. Check your free disk space. Not enough free disk space can cause this error.
2. Run **Management > Database Maintenance > Maintenance > Activate now** in order to free database space.
Chapter 5

Out of the Box Consolidation Policy

Predefined Consolidation Policy

The predefined, Out of the Box Consolidation Policy consists of 13 Consolidation Rules. Each Rule addresses a certain type of log (for example, alerts, blocked or broadcast logs) and specifies whether to ignore it or store it.

If a log is to be stored, the Rule specifies its Store Properties:

- **As Is** — all log fields are stored in the Eventia Reporter database and will be available for report generation without consolidation. This is the default storage option when a new rule is created.
- **Consolidated** — specify the following consolidation parameters:
  - **Consolidation Interval** — the interval at which logs matching this Rule are consolidated (for example, all logs generated within a 10 minute interval). Hourly intervals are measured.

Out of the Box Consolidation Rules

The following table describes the function of each Rule and specifies its Store Properties.

<table>
<thead>
<tr>
<th>Rule No.</th>
<th>Description</th>
<th>Cons. Interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Consolidate and store alert logs.</td>
<td>1 hour</td>
</tr>
<tr>
<td>2</td>
<td>Consolidate and store blocked (rejected or dropped) connection logs</td>
<td>1 hour</td>
</tr>
<tr>
<td>3</td>
<td>Consolidate and store approved HTTP connections logs</td>
<td>1 hour</td>
</tr>
<tr>
<td>4</td>
<td>Consolidate all SMTP logs.</td>
<td>1 hour</td>
</tr>
<tr>
<td>5</td>
<td>Consolidate and store approved FTP logs</td>
<td>1 hour</td>
</tr>
<tr>
<td>6</td>
<td>Store all message logs.</td>
<td>none</td>
</tr>
<tr>
<td>7</td>
<td>By default, this Rule is inactive. If activated after adding the relevant groups it filters out all broadcast message logs.</td>
<td>none</td>
</tr>
<tr>
<td>8</td>
<td>Ignore both approved and blocked bootp (Bootstrap Protocol, used to boot diskless systems) packet logs.</td>
<td>none</td>
</tr>
<tr>
<td>9</td>
<td>Ignore both approved and blocked nbdatagram logs.</td>
<td>none</td>
</tr>
<tr>
<td>Rule No.</td>
<td>Description</td>
<td>Cons. Interval</td>
</tr>
<tr>
<td>---------</td>
<td>-----------------------------------------------------------------------------</td>
<td>----------------</td>
</tr>
<tr>
<td>10</td>
<td>Ignore both approved and blocked DNS logs</td>
<td>none</td>
</tr>
<tr>
<td>11</td>
<td>Consolidate and store approved POP-3 logs</td>
<td>1 hour</td>
</tr>
<tr>
<td>12</td>
<td>Consolidate and store NTP logs. NTP is a time protocol that provides access</td>
<td>1 hour</td>
</tr>
<tr>
<td></td>
<td>over the Internet to systems with precise clocks.</td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>Consolidate and store connections that do not match any of the previous</td>
<td>1 hour</td>
</tr>
<tr>
<td></td>
<td>Rules</td>
<td></td>
</tr>
</tbody>
</table>
Appendix A

Predefined Reports

This appendix describes the predefined reports available under each subject and specifies the report ID required for command line generation.

In This Appendix

- Anti-Virus & Anti-Malware Blade Reports
- Content Inspection Reports
- Cross Blade Network Activity Reports
- Cross Blade Security Reports
- Endpoint Security Blade Reports
- Event Management Reports
- Firewall Blade - Activity Reports
- Firewall Blade - Security Reports
- Firewall GX
- Firewall Network Activity
- InterSpect Reports
- IPS Blade Reports
- IPSEC VPN Blade Reports
- My Reports
- Network Security Reports
- Regulatory Compliance Reports
- SSL VPN Blade Reports
- System Information Reports

Anti-Virus & Anti-Malware Blade Reports

Standard Reports

- **Scanned File Types** — This report presents statistics about file types. It includes the distribution of file types by source, destination, date and time. This report can be used to determine which file types are most common and the top sources and destinations of these file types.
  
  Report ID — {316AF9AF-1A4E-4D7B-BB35-2B3238FD874D}

- **Viruses** — This report presents statistics about detected viruses. It includes the distribution of viruses by source, destination, date and time. This report can be used to determine which viruses are most common and the top sources and destinations of the viruses.
  
  Report ID — {A4AF4087-2120-454F-849F-641B6F2A1E5A}

Content Inspection Reports

Standard Reports

- **URL Filtering** — IMPORTANT: Information in this report is sensitive and must only be provided to users on a need-to-know basis.

  This report analyzes URL filtering activity by user, category, source and more. Specific sections include:

  - The top categories of web sites visited
• Top web sites visited
• Breakdown of blocked lists to URLs
• Categories of web sites visited by date and day of week

Express Reports

• **Anti-Spam Activity** — This report provides an overview of Anti-Spam activity. It includes data regarding:
  • Spam emails that were identified and handled
  • Spam emails categorized by date
  • Spam emails categorized by hour of the day

Report ID — {B5994073-C220-4CA7-9532-BD453304E67E}

• **Anti-Virus** — This report provides an overview of the items scanned by the Anti Virus (AV) and handled by the Security Gateway. It provides data about items that were accepted or blocked, projected by gateways, method of enforcement (infection, file type or configured limits) and dates.

Report ID — {85396AED-6554-4DB9-BBE3-28285E328424}

• **URL Filtering Activity** — This report provides an overview of Web (URL) filtering handled by the Security Gateways. It provides data about URLs that were accepted or blocked, projected by gateways, method of enforcement (categorization or custom lists) and dates.

Report ID — {3243E4CB-DA54-A08-A9D3-72EEC6C3200E}

Cross Blade Network Activity Reports

Standard Reports

• **Approved Traffic** — This report presents data about traffic that was accepted. This report can be used to see network activity to determine effective usage of your resources. Specific sections include information regarding:
  • overall traffic characteristics as well as a breakdown by hour and by date
  • the top network users
  • top services used
  • top sources and top destinations of network traffic

Report ID — {0C20043C-B8C1-4A20-9CD8-C2FAE589E877}

• **List of all Approved Traffic** — This report presents the details of all connections. It can be used for specific security or network behavior inspection. Use this report to collect specific data by filtering only the data you wish to view. This report can generate large amounts of data; select filters and time frames judiciously to create a useful result.

Report ID — {D7CD8E72-6978-48DB-897A-365ED6B42482}

• **User Activity** — This report presents the user's activity as it was logged by the gateway. It includes information about network activity that users performed through the gateway.

Report ID — {D7CD8E72-6978-48DB-897A-365ED6B42482}

• **Web Traffic** — This report presents data about the web traffic through Security Gateways and Connectra. Specific sections include:
  • Total web traffic load
  • Top sites visited
  • Top web users
  • Distribution of web traffic by direction
  • Web Traffic by hour and by date

Filtering data by user can refine the results about individual activity.

Report ID — {89A57E29-5F58-4E6E-B377-40702631A3A0}
Cross Blade Security Reports

Standard Reports

- **Blocked Traffic** — This report presents data regarding events that were blocked. It can be used to determine:
  - The volume of events that were blocked
  - The top sources of blocked events, their destinations and services
  Report ID — {C6F9ED20-E130-40BC-B67C-C37E3BFDD31D}

- **Login Activity** — This report presents login activity associated with Endpoint Security VPN, SSL Network Extender and Connectra.
  Report ID — {BCE31986-4FD9-4E67-8F1A-69D28E2F9A7F}

- **Login Failures** — This report presents all login failures that were reported by the Security Gateway and/or Connectra.
  Report ID — {18912ED2-E6E6-448D-9F5A-FD357AC4AE42}

Endpoint Security Blade Reports

Standard Reports

- **Anti-Malware** — This report shows Malware detected on endpoint computers by the Anti-Malware feature. Use this report to identify Malware and the users affected by Malware. You can extend the data to include all results, instead of just the top, by increasing the number of results in the Table Properties for each Table.
  Report ID — {8D555251-0525-4FE4-BDF2-84087B97E024}

- **Blocked Programs** — This report shows programs blocked on endpoint computers by your security policies. Use this report to see what programs are being used that are malicious or violate corporate policy and to identify the users that initiate these programs. You can extend the data to include all results, instead of just the top, by increasing the number of results in the Table Properties for each Table.
  Report ID — {65E33008-1764-44B0-A5B3-B0449034D3ED}

- **Compliance** — This report shows compliance events at the endpoint detected by the compliance enforcement rules. Use this report to see which endpoints and users are out of compliance with your security policies and to identify frequently violated enforcement rules. You can extend the data to include all results, instead of just the top, by increasing the number of results in the Table Properties for each Table. This report shows compliance events at the endpoint detected by the compliance enforcement rules.
  Report ID — {DCC0DC4D-D8CC-4654-A5EA-4288A24137FB}

- **Endpoint Errors** — This report shows errors detected with the Endpoint Security client. It identifies errors such as the inability to upload logs, download a policy, or errors in the policy file. Use this report to identify endpoints to investigate for errors or endpoints that may not have the latest policies. You can extend the data to include all results, instead of just the top, by increasing the number of results in the Table Properties for each Table.
  Report ID — {2C9BA414-30CA-4C24-B9F0-870B4D3FF7D4}

- **Firewall Events** — This report shows firewall events that occurred on endpoint computers. Use this report to monitor traffic, check the effectiveness of firewall rules, locate abnormally behaving endpoints, and identify suspicious sources and destinations. You can extend the data to include all results, instead of just the top, by increasing the number of results in the Table Properties for each Table.
  Report ID — {99DB6667-F1BC-43AD-B75A-7A7489148ABB}

- **Summary** — This report presents a summary of security activity on endpoint computers. Use this report to see trends in the security of endpoints and the effectiveness of the security policies.
  Report ID — {EBBD4849-5482-47AD-A1DF-005D012E646F}
Event Management Reports

- **Analyzer Events** — This report presents the events detected by Eventia Analyzer. It includes the distribution of events by severity, date and time, source, destination, service and product. This report can be used to determine which Eventia Analyzer events are most common and discover various event trends such as the top sources and destinations of the events.
  
  **Report ID** — \{CB08FAF2-2EF1-4FA2-8D46-5BF7857C348\}

- **List of all Events** — This report presents the events detected by Eventia Analyzer in a format similar to the Eventia Analyzer client. This report is commonly used in conjunction with filters to present customized event lists.
  
  **Report ID** — \{630DBB0B-459A-4650-8957-16BB8EC24EE1\}

Firewall Blade - Activity Reports

**Standard Reports**

- **FTP Activity** — This report presents data about FTP traffic through the gateway. It can be used to determine:
  - Total FTP traffic
  - FTP traffic by hour and by date
  - Top uploaded/downloaded files
  - Top uploaded/downloaded file types
  
  **Report ID** — \{7B12F482-5DF0-11D6-A343-0002B3321334\}

- **List of all Connections** - this report presents the details of all connections. It can be used for specific security or network behavior inspection. Use this report to collect specific data by filtering only the data you wish to view.
  
  **Note** - this report can generate large amounts of data. Select filters and time frames judiciously to create a useful result.

  **Report ID** — \{9CBEE3F3-DA22-46A8-B13B-3BF4D5E1D2EA\}

- **Network Activity** — This report presents data about traffic accepted by the Security Gateway. This report can be used to view network activity in order to determine effective usage of resources.
  
  Specific sections include information regarding:
  - overall traffic characteristics as well as a breakdown by hour and by date
  - the top network users
  - top services used
  - top sources and top destinations of network traffic
  
  **Report ID** — \{0A4E3BB9-55C0-11D6-A342-0002B3321334\}

- **POP3/IMAP Activity** — this report presents data about POP3/IMAP traffic through the gateway. It includes data about total POP3/IMAP traffic load and distribution of traffic by direction.

  **Report ID** — \{70D7A36F-B3E1-45B7-BDC9-165E35653538\}

- **SMTP Activity** — this report presents data about SMTP mail traffic through the gateway. It can be used to determine total mail traffic load as well as top mail senders and top mail recipients.

  **Report ID** — \{7B12F483-5DF0-11D6-A343-0002B3321334\}

- **User Activity** - this report presents the user's activity as it was logged by the gateway. It includes information about network activity that users performed through the gateway.

  **Report ID** — \{D7CB8E72-6978-48DB-897A-365ED6B42482\}

- **Web Activity** — this report presents data about the web traffic through the gateway.
  
  Specific sections include:
  - The total web traffic load
  - Top sites visited
  - Top web users
  - Distribution of web traffic by direction.
• Web Traffic by hour and by date
  Filtering data by user can refine the results about individual activity.
  Report ID — {7B12F481-5DF0-11D6-A343-0002B3321334}

Firewall Blade - Security Reports

Standard Reports

• Alerts — This report presents the alerts issued by the gateway. It includes the entire list of alerts issued, as well as the distribution of alerts by source, destination, and service.
  Report ID — {475AD894-2AC0-11D6-A330-0002B3321334}

• Blocked Connections — This report presents data regarding connections that the blocked by the gateway.
  It can be used to determine:
  - the volume of connections that were blocked
  - the top sources of blocked connections, their destinations and services
  Report ID — {475AD891-2AC0-11D6-A330-0002B3321334}

• Gateway Traffic — This report provides an overview of the network activity that the Security Gateway handled. It includes distribution of traffic by Firewall action and data about traffic that was originated from or destined to the gateway itself.
  Report ID — {0A4E3BC7-55C0-11D6-A342-0002B3321334}

• Policy Installations — This report presents policy installation data for a specific gateway. It includes data regarding the number of policy install and uninstall procedures. The report is designed to produce results for a single gateway. Using this report for multiple gateways may produce misleading results.
  Report ID — {475AD88F-2AC0-11D6-A330-0002B3321334}

• Rule Base Analysis — This report presents an analysis of gateway rule base for a specific gateway.
  The report can be used to determine which rules are used the most, which rules are used infrequently and which rules are never used. It can also be used to determine which rules are matched by service, source, and destination.
  Rules are presented by their location in the policy at the time of report generation, while their usage data is gathered by their unique ID where possible. If no unique ID data is available, the rules are marked with an asterisk.
  Report ID — {475AD88E-2AC0-11D6-A330-0002B3321334}

Firewall GX

Standard Reports

• GTP Accepted Signaling Activity — This report provides information regarding successful GTP tunnel management signaling activity and GTP path management signaling activity.
  Report ID — {84E06513-8CEF-47A9-9997-6B1E8CE771F4}

• GTP Activity Summary — This report provides an overview on the GTP activity as it was logged by all Firewall-1 GX gateways.
  Report ID — {7779B347-1023-4378-A7BC-F734C732DFB5}

• GTP Dropped/Rejected Signaling Activity — This report provides information regarding dropped or rejected GTP tunnel management signaling activity and GTP path management signaling activity.
  Report ID — {955137EF-1612-4387-8BA9-1F1296FA9A13}

• GTP exchanges not accepted by peer GSN — This report provides information regarding GTP exchanges that were not accepted by the system due to a response cause different than "request accepted" and GTP signaling requests that where not answered within 40 seconds.
  Report ID — {35AAF5B3-5EB5-436C-B47D-940F5FE740BD}
- **GTP Security alerts** — This report provides information regarding GTP signaling messages or GTP data packets that where dropped due to not meeting the necessary security requirements.
  Report ID — {B8A8B3F-49A8-4C20-AF12-D427317D99EA}

### Firewall Network Activity

#### Express Reports

- **FTP Activity** — This report provides an overview about FTP security server activity. It includes data about:
  - Accepted and rejected FTP sessions
  - Average concurrent FTP sessions
  - FTP sessions over time
  Report ID — {C0D0C34B-F35D-4482-9CF8-631B7ACEEE57}

- **Network Activity** — This report provides an overview of the network activity that Security Gateway handled. It includes data about top traffic sources, top destinations and top services in terms of bytes/sec or concurrent connections, as well as the top rules by date.
  Report ID — {DB3CBF73-DC1C-4E0C-8D04-8000EA64FF5F}

- **Selected Services Activity** — This report provides an overview about selected services:
  - FTP
  - HTTP
  - HTTPS
  - SMTP
  - TELNET
  - POP3/IMAP
  It includes data about traffic bytes, byte rate and the number of concurrent connections for these services.
  Report ID — {3D7854AB-6118-437F-87A3-71BD392E7DF3}

- **SMTP Activity** — This report provides an overview of the SMTP security server activity. It includes data about the number of SMTP emails handled and the number of SMTP connections.
  Report ID — {9BE87F3D-AADC-425D-B59E-E4B221564FAD}

### InterSpect Reports

#### Standard Reports

- **List of Added Dynamic Rules** — This report provides detailed information about the dynamic rules added to the system. This report can be filtered to reduce the size of its output.
  Report ID — {9CD89E76-EFE1-458B-91B4-A9043DDBCB777}

- **Quarantined Machines** — This report provides an overview about the hosts that were quarantined.
  Report ID — {809E625A-FB21-4EAD-8CB4-7AA3769F9790}

#### Express Reports

- **InterSpect Activity** — This report provides an overview of the network activity that InterSpect handled. It includes data about total traffic connections and total numbers of accepted and denied packets.
  Report ID — {2CFA72AF-47D1-4374-B542-9FE7181813F6}

- **InterSpect Network Activity** — This report provides an overview of the network activity that InterSpect handled. It includes data about traffic sources, destinations and services.
  Report ID — {B483F96A-E911-4F45-940C-A3F5E0AAD2FA}

- **InterSpect System Information** — This report provides data about the system's CPU, memory and free disk space.
  Report ID — {2320E7D8-3047-4D88-99E4-437A8AC0C063}
IPS Blade Reports

Standard Reports

- **IPS Attacks** — This report presents the security attacks detected by IPS. It includes the distribution of attacks by source, destination, date and time. This report can be used to determine which IPS attacks are most common and the top sources and destinations of the attacks.
  Report ID — {F76CEB9F-6718-4875-8273-54A0F420BC13}

- **IPS Detailed Attacks** — This report presents detailed security attacks detected by IPS (for example, Kazaa and eMule will appear instead of simply Peer to Peer). It includes the distribution of attacks by source, destination, date and time. This report can be used to determine which IPS attacks are most common and the top sources and destinations of the attacks.
  Report ID — {082444B7-1739-4CCA-87DF-A0A67C863067}

IPSEC VPN Blade Reports

Standard Reports

- **Encrypted Network Activity** — This report presents data about network traffic that the gateway encrypted. It includes data about total encrypted traffic load, distribution of encrypted traffic by services and by traffic direction.
  Report ID — {0A4E3BC6-55C0-11d6-A342-0002B3321334}

- **Endpoint Security VPN Users Activity** — This report presents Endpoint Security VPN activity as it was logged by the alerts uploaded from the desktops. It includes sections on:
  - Policy server logins
  - Top users by login duration
  - Top Servers by login
  The report also shows Policy Server activity information.
  Report ID — {E387C01B-0373-406a-84BC-DAF15A3E5759}

- **VPN Community** — This report provides data about VPN community activity. The report can also be used for any set of multiple gateways and provides data about:
  - Security Gateway encrypted traffic
  - VPN tunnel creation and its distribution throughout the day.
  Report ID — {BD534B0B-C4CA-41c4-A996-76D3317FF2D2}

- **VPN Tunnel for Specific Gateway** — This report provides data about specific gateway connections. The report shows the level of activity between a gateway and its peers, VPN traffic distribution and VPN tunnel creation. The report is designed to produce results for a single gateway. Using this report for multiple gateways may produce misleading results. To obtain data regarding multiple gateways use the 'VPN Community' report.
  Report ID — {E74B0FA9-7617-11D6-A351-0002B3321334}

Express Reports

- **VPN Activity** — This report provides an overview of the traffic handled by Security Gateways. It includes data about traffic encrypted and decrypted by the Security Gateways.
  Report ID — {E276053F-19B2-429C-9FB2-21BA0DE5B6B2}

- **VPN Tunnels** — This report provides data on the process of tunnel creation by Security Gateways. It includes data on VPN and remote access tunnels, as well as on IKE negotiations.
  Report ID — {B640C862-DF0E-485E-A0B0-086E0D35EC76}
My Reports

Standard Reports

This category includes predefined reports as well as reports you have customized to better address your specific needs.

The following reports present the events detected by Event Analysis blades. They include the distribution of events by severity, date and time, source, destination, service and product. These reports can be used to determine which Analyzer events are most common and to discover various event trends, such as the top sources and destinations of the events.

- **Daily Customer Detailed Events (Provider-1 Deployment)**
  Report ID — (7395F2D0-03A0-412E-8C04-ECF44E32681C)

- **Daily Detailed Events**
  Report ID — (9974A621-1470-4964-9180-14F62FB2DAD1)

- **Hourly Customer Detailed Events (Provider-1 Deployment)**
  Report ID — (28A841C5-5043-47A3-92C4-7CF2F7F3D054)

- **Hourly Detailed Events**
  Report ID — (A0F8AF8B-DAED-4844-B6CE-76C2B7F2FDA6)

- **Monthly Customer Detailed Events (Provider-1 Deployment)**
  Report ID — (26E5139C-1D2E-458E-AE98-92EE2635FF33)

- **Monthly Detailed Events**
  Report ID — (3C3D7646-9FF8-4B03-B69D-1B0B9712AC97)

- **Weekly Customer Detailed Events (Provider-1 Deployment)**
  Report ID — (38AE5F1A-6079-49BD-B37A-E5A8E799C109)

- **Weekly Detailed Events**
  Report ID — (4A1234B8-11EE-456D-BC37-F8A32E3CB9B6)

Network Security Reports

Express Reports

- **Firewall Activity** — This report provides an overview about the network activity that a gateway handled.
  It includes sections on:
  - Top gateways by concurrent connections
  - Top gateways by accepted and denied packets
  - Accepted and denied packets over time
  - Total activity by day of the week and by hour of the day.
  Report ID — (F9504B51-4E93-484E-BA9B-747632278B65)

- **Peer To Peer Activity** — This report provides information about Peer To Peer Activity. It includes data about traffic of services such as Kazaa, eMule, Gnutella, BitTorrent, Skype, ICQ and Yahoo! Messenger.
  Report ID — (60F6FCDA-0F66-43A6-B8E6-271247207F5B)

- **Port Scan Attacks** — This report provides an overview of Port Scan attacks detected by InterSpect.
  Report ID — (C93FF2C0-9F72-44C1-9734-38ED64FF96BD)

- **SYN Attacks** — This report provides an overview of SYN attacks detected by InterSpect.
  Report ID — (F0EFADA3-C79B-4E06-958A-E0365194CC83)
Regulatory Compliance Reports

Important - Information in these reports is sensitive and must only be provided to users on a need-to-know basis.

Compliance Reporting and Disclaimer:

The Regulatory Compliance reports provide “Compliance Source Information” for use in regulations and standards reporting requirements. Check Point is not providing legal and/or compliance advice and makes no warranties, express or implied, that this information meets compliance regulations. Always consult your legal advisors for compliance regulations and requirements which may be applicable to you.

The following reports meet ISO 17799, COBIT, PCI-DSS, SOX and HIPAA compliance Source requirements.

Standard Reports

- **Alert Risks** — This report presents the alerts issued by Firewall. It includes the entire list of alerts issued and the distribution of alerts by source, destination and service.
  Report ID — {F036E9AD-90F5-4EC5-BE5E-5C26FDCEBC2F}

- **Attacks** — It includes the distribution of attacks by source, destination, date and time. This report can be used to determine which IPS attacks are most common and the top sources and destinations of these attacks.
  Report ID — {FDEBC97B-B148-4F56-BC66-FB8439760C8D}

- **Blocked Connections** — This report presents data regarding connections that the Security Gateway blocked. It can be used to determine:
  - The volume of connections that were blocked
  - The top sources of blocked connections, their destinations and services
  Report ID — {81FC797B-8862-4CF1-BBD7-BEA504F31C15}

- **Blocked Programs Endpoint** — This report shows programs that were blocked on endpoint computers by your security policies. You can use this report to see what programs are being used that are malicious or violate corporate policy, and to identify the users that initiate these programs. You can extend the data to include all results, instead of just the top, by increasing the number of results in the Table Properties for each Table.
  Report ID — {95E1B452-E154-4421-8C9C-2B90CCE73DC}

- **Endpoint Security Compliance** — This report shows compliance events at the endpoint computer that were detected by the compliance enforcement rules. You can use this report to see which endpoint computers and users are out of compliance with your security policies and to identify frequently violated enforcement rules. You can extend the data to include all results, instead of just the top, by increasing the number of results in the Table Properties for each Table.
  Report ID — {A2C90031-B4AD-4643-B2CC-F699489388FB}

- **Failed Logins** — This report presents all login failures that were reported by Security Gateway and/or Connectra.
  Report ID — {BA92DEC2-D7C6-4CEE-B828-12FBE5B0E964}

- **GTP Firewall Security Alerts** — This report provides information regarding GTP signaling messages or GTP data packets that were dropped because they did not meet the necessary security requirements.
  Report ID — {8CC905F9-59F5-473C-AA86-42BB8763B7FD}

- **List of Added Dynamic Rules** — This report provides detailed information about the dynamic rules added to the system. This report can be filtered to reduce the size of its output.
  Report ID — {6CA37FB0-B322-44AC-9CCC-4EB80EF0CE2A}

- **MailSafe Endpoint** — This report shows email extensions that were quarantined on endpoint computers using the MailSafe feature. You can use this report to identify the use of attachments that could be malicious or may violate policy. You can extend the data to include all results, instead of just the top, by increasing the number of results in the Table Properties for each Table.
  Report ID — {0CB2D174-7B5B-47BD-B781-81C117E07344}

- **Policy Installations** — This report presents policy installation data for a specific gateway. It includes data regarding the number of policy install and uninstall procedures. The report is designed to produce
results for a single gateway. If you use this report for multiple gateways, it may produce misleading results.

Report ID — {E11B11B8-2311-4179-B58C-9F7C4498EA45}

- **Quarantined Hosts** — This report provides an overview about the host addresses that were quarantined.
  Report ID — {44C03345-4FE0-4AE2-A820-7C84FA9713EA}

- **Risk Summary** — This report presents data regarding connections that Firewall blocked. It can be used to determine:
  - The volume of connections that were blocked.
  - The top sources of blocked connections, their destinations and services.
  Report ID — {93803268-840C-476D-A859-1BF3D73EBBCD}

- **Spyware Endpoint** — This report shows spyware that is detected on endpoint computers by the Anti-Spyware feature. You should use this report to identify spyware programs and the users affected by spyware. You can extend the data to include all results, instead of just the top, by increasing the number of results in the Table Properties for each Table.
  Report ID — {BE003478-3AD7-46BD-A805-7E9584AB19D9}

- **Successful Logins** — This report presents login activity associated with Endpoint Security VPN, SSL Network Extender and Connectra.
  Report ID — {3968DFE8-403E-4A7A-9636-9B46188C2654}

- **Viruses** — This report presents statistics about detected viruses. It includes the distribution of viruses by source, destination, date and time. This report can be used to determine which viruses the are most common and the top sources and destinations of the viruses.
  Report ID — {DA589319-3268-4A4B-8569-11F45B397947}

**Express Reports**

- **Application Layer** — The report provides information about Application Layer defenses. It contains a summary of all the traffic that was classified as Application Layer attacks. Such attacks attempt to target the web application layer such as the database layer, server side scripts and various components used in the application. The attacks are divided into several categories: cross site scripting, command injection, SQL injection etc.
  Report ID — {865417E0-048A-404B-8E9F-777EB4F85D45}

- **Firewall Memory Information** — This report provides data about memory allocations that the Firewall made. It includes data about various types of memory allocations used by the Firewall.
  Report ID — {7762B74C-329D-49C2-A7AD-2466AFE7A0CC}

- **System Information** — This report provides data about the Security Gateways' system status, including data about CPU, memory and disk space. This report can be used to see the load on the Security Gateway over time.
  Report ID — {ABF9BF25-DBC0-46F0-A2D5-3C0C5086DDB6}

**SSL VPN Blade Reports**

**Standard Reports**

- **Connectra Events** — This report provides general data about Connectra events. This report offers a general impression of Connectra activity and can be filtered more specifically.
  Report ID — {C877E51F-3D84-42D9-BE31-2A6D53C4AC84}

- **Connectra File Shares Activity** — This report provides data about the file share activity through Connectra.
  Report ID — {D29B7BB1-9D18-4A60-8F97-57D883AFFE39}
System Information Reports

Express Reports

- **System Information** — This report provides data about gateway system status, including data about CPU, memory and disk space. This report can be used to see the load on gateway over time.
  
  Report ID — {26450EBC-37B4-4465-A9E0-F3FFA61917E6}

- **Security Gateway Memory** — This report provides data about memory allocations that the Security Gateways made. It includes data about various types of memory allocations used by Security Gateways.

  Report ID — {F896C74F-72F0-47A8-A54D-0974B518E9CD}
# Index

## A
- Adapting the Report's Detail Level to your Needs • 10
- Additional Settings for Report Generation • 25
- Anti-Virus & Anti-Malware Blade Reports • 38
- Automatically Maintaining the Size of the Database • 14

## B
- Backing Up the Eventia Reporter Database • 14
- Basic Concepts and Terminology • 7

## C
- Common Scenarios • 32
- Configuring Consolidation Settings and Sessions • 19
- Configuring Database Maintenance Properties • 22
- Configuring the FTP Upload • 27
- Configuring the Report Output tab • 26
- Configuring the Web Server • 26
- Consolidation Policy Configuration • 30
- Content Inspection Reports • 38
- Creating a Report in a Single File • 30
- Cross Blade Network Activity Reports • 39
- Cross Blade Security Reports • 40
- Customizing a Report • 17
- Customizing Predefined Consolidation Rules • 31
- Customizing Predefined Reports • 8

## D
- Data Calculation Scheme • 24
- DBsync • 7
- Distributing Reports with a Custom Report Distribution Script • 27
- Dynamically Updating Reports • 29

## E
- Endpoint Security Blade Reports • 40
- Event Management Reports • 41
- Eventia Reporter Backward Compatibility • 8
- Eventia Reporter Considerations • 8
- Eventia Reporter Database Management • 11
- Eventia Reporter Express Reports • 8
- Eventia Reporter Instructions • 23
- Eventia Reporter Standard Reports • 7
- Exporting a Database Table • 21
- Exporting a Database Table to a Remote Machine • 22
- Exporting and Importing Database Tables • 21
- Express Reports Configuration • 23

## F
- Firewall Blade - Activity Reports • 41
- Firewall Blade - Security Reports • 42
- Firewall GX • 42
- Firewall Network Activity • 43

## Format • 24

## G
- Generating a Report • 16
- Generating Only Selected Sections • 10
- Generating Reports using the Command Line • 25
- Generating the Same Report using Different Settings • 25
- Getting Started • 15

## H
- Hardware Recommendations • 28
- High Availability • 9
- How to interpret Computer names in DHCP enabled networks • 6
- How to Interpret Report Results whose Direction is • 26
- How to Recover the Eventia Reporter Database • 25
- How to Upload Reports to a Web Server • 26
- How to View Report Results without the Eventia Reporter Client • 26

## I
- Importing a Database Table • 22
- Improving Performance • 28
- Installation • 28
- InterSpect Reports • 43
- Introducing Eventia Reporter • 5
- IPS Blade Reports • 44
- IPSEC VPN Blade Reports • 44

## L
- Licenses • 15
- Log Availability vs. Log Storage and Processing • 9
- Log Consolidation Phase Considerations • 9
- Log Consolidation Process • 6
- Log Consolidator • 28

## M
- Modifying Eventia Reporter Database Configuration • 12
- My Reports • 45

## N
- Network Security Reports • 45

## O
- Out of the Box Consolidation Policy • 36
- Out of the Box Consolidation Rules • 36
- Overview • 30

## P
- Performance Tips • 28
- Predefined Consolidation Policy • 36
- Predefined Reports • 7, 38
- Provider-1 • 15

## Q
- Quick Start • 16
R
Record Availability vs. Database Size • 9
Regulatory Compliance Reports • 46
Report Filters • 11
Report Generation Phase Considerations • 10
Report Generation Scheduling • 29
Report output (Email, FTP Upload, Web Upload, Custom) • 11
Report Output Location • 24
Report Section Generated • 29
Report Structure • 8
Reports based on Log Files not part of the Log File Sequence • 25
Required Security Policy Configuration • 23

S
Saving Consolidated Records to One vs. Multiple Database Tables • 9
Scheduling a Report • 17
Scheduling Reports • 10
Sort Parameter • 24
Specifying the Consolidation Rule's Store Options • 31
SSL VPN Blade Reports • 47
Standalone vs. Distributed Deployment • 9
Starting and Stopping the Log Consolidator Engine • 19
Starting Eventia Reporter • 15
Starting the Log Consolidation Engine • 19
Stopping the Log Consolidation Engine • 19
System Information Reports • 48

T
The Eventia Reporter Solution • 5
To Configure Automatic Maintenance • 22
To Configure Consolidation Settings • 20
To Create a Consolidation Session • 19
To Manually Archive or Delete Older, Less Pertinent Records from the Database • 23
To Modify the Database Maintenance Properties • 22
To Obtain Additional Information about the Status of a Previously Generated Report • 18
To Set the Time-Out Value: • 27
To Stop a Specific Report Generation Process • 18
To View Detailed Information about a Specific Session • 20
To View Report Generation Schedules • 17
To View Reports and Status • 18
To View Server Activities • 18
To View the Status of Previously Generated Reports • 18
Troubleshooting • 32
Tuning the Eventia Reporter Database • 11

U
UpdateMySQLConfig Syntax • 13
Uploading Reports to an FTP Server • 27
Using Accounting Information in Reports • 24
Using Eventia Reporter • 16

V
Viewing Report Generation Status • 17