SmartEvent Intro

R76

Administration Guide

8 September 2013

Classification: [Protected]
Important Information

Latest Software

We recommend that you install the most recent software release to stay up-to-date with the latest functional improvements, stability fixes, security enhancements and protection against new and evolving attacks.

Latest Documentation

The latest version of this document is at:
(http://supportcontent.checkpoint.com/documentation_download?ID=22922)

To learn more, visit the Check Point Support Center (http://supportcenter.checkpoint.com).

For more about this release, see the R76 home page

Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>08 September 2013</td>
<td>General Updates</td>
</tr>
<tr>
<td>10 February 2013</td>
<td>First release of this document</td>
</tr>
</tbody>
</table>

Feedback

Check Point is engaged in a continuous effort to improve its documentation.

Please help us by sending your comments
(mailto:cp_techpub_feedback@checkpoint.com?subject=Feedback on SmartEvent Intro R76 Administration Guide).
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Important Information</td>
<td>3</td>
</tr>
<tr>
<td><strong>Introduction to SmartEvent Intro</strong></td>
<td>6</td>
</tr>
<tr>
<td>Basic Concepts and Terminology</td>
<td>6</td>
</tr>
<tr>
<td>SmartEvent Sizing Guide</td>
<td>6</td>
</tr>
<tr>
<td><strong>Initial Configuration</strong></td>
<td>7</td>
</tr>
<tr>
<td>Check Point Licenses</td>
<td>7</td>
</tr>
<tr>
<td>Initial Configuration of the SmartEvent Client</td>
<td>7</td>
</tr>
<tr>
<td>Enabling Connectivity with Multi-Domain Security Management</td>
<td>8</td>
</tr>
<tr>
<td>Installing the Network Objects in the SmartEvent Database</td>
<td>8</td>
</tr>
<tr>
<td>Configuring SmartEvent to work with Multi-Domain Security Management</td>
<td>8</td>
</tr>
<tr>
<td><strong>Working with Queries</strong></td>
<td>9</td>
</tr>
<tr>
<td>Event Queries</td>
<td>9</td>
</tr>
<tr>
<td>Predefined Queries</td>
<td>9</td>
</tr>
<tr>
<td>Custom Queries</td>
<td>9</td>
</tr>
<tr>
<td>Event Query Results</td>
<td>12</td>
</tr>
<tr>
<td>Event Log</td>
<td>12</td>
</tr>
<tr>
<td>Event Statistics Pane</td>
<td>16</td>
</tr>
<tr>
<td>Event Details</td>
<td>16</td>
</tr>
<tr>
<td>Event Data Analysis</td>
<td>17</td>
</tr>
<tr>
<td>Overview Tab</td>
<td>17</td>
</tr>
<tr>
<td>Timeline Tab</td>
<td>19</td>
</tr>
<tr>
<td>Charts Tab</td>
<td>20</td>
</tr>
<tr>
<td>Maps Tab</td>
<td>23</td>
</tr>
<tr>
<td>Reports Tab</td>
<td>24</td>
</tr>
<tr>
<td>Administrator Permission Profiles - Events and Reports</td>
<td>24</td>
</tr>
<tr>
<td>Multi-Domain Security Management</td>
<td>25</td>
</tr>
<tr>
<td><strong>Reports</strong></td>
<td>26</td>
</tr>
<tr>
<td>Reports Tab</td>
<td>26</td>
</tr>
<tr>
<td>Predefined Reports</td>
<td>26</td>
</tr>
<tr>
<td>Custom Reports</td>
<td>27</td>
</tr>
<tr>
<td>Configuring Reports</td>
<td>27</td>
</tr>
<tr>
<td>Defining the Time Frame</td>
<td>27</td>
</tr>
<tr>
<td>Report Filters</td>
<td>28</td>
</tr>
<tr>
<td>Automatic Report Scheduling</td>
<td>28</td>
</tr>
<tr>
<td>Configuring Email Settings</td>
<td>29</td>
</tr>
<tr>
<td>Generating Reports</td>
<td>30</td>
</tr>
<tr>
<td><strong>Investigating Events</strong></td>
<td>31</td>
</tr>
<tr>
<td>Tracking Event Resolution using Tickets</td>
<td>31</td>
</tr>
<tr>
<td>Editing IPS Protection Details</td>
<td>31</td>
</tr>
<tr>
<td>Displaying Original Event Log Information</td>
<td>31</td>
</tr>
<tr>
<td>Using Custom Commands</td>
<td>32</td>
</tr>
<tr>
<td><strong>System Administration and Modifying Event Policy</strong></td>
<td>33</td>
</tr>
<tr>
<td>Adding Exclusions</td>
<td>33</td>
</tr>
<tr>
<td>Modifying the System General Settings</td>
<td>34</td>
</tr>
<tr>
<td>Adding Network and Host Objects</td>
<td>34</td>
</tr>
<tr>
<td>Defining Correlation Units and Log Servers</td>
<td>35</td>
</tr>
<tr>
<td>Defining the Internal Network</td>
<td>35</td>
</tr>
<tr>
<td>Offline Log Files</td>
<td>35</td>
</tr>
<tr>
<td>Configuring Custom Commands</td>
<td>36</td>
</tr>
<tr>
<td>Creating an External Script</td>
<td>37</td>
</tr>
</tbody>
</table>
Managing the Event Database .................................................................37
Backup and Restore of the Database ....................................................37
Administrator Permissions Profile - Policy ..........................................38
Multi-Domain Security Management .....................................................38
Index .....................................................................................................39
Chapter 1

Introduction to SmartEvent Intro

In This Chapter

Basic Concepts and Terminology 6
SmartEvent Sizing Guide 6

SmartEvent Intro lets you use SmartEvent features with one Security Gateway Software Blade. SmartEvent Intro has these modes:

- IPS mode - shows events from the IPS blade
- DLP mode - shows events from the DLP blade
- Application Control mode - shows events from the Application Control blade

The mode is determined by the Software Blades activated and the licenses installed on the management server. If more than one of the possible SmartEvent Intro blades are installed and licensed, select which mode to use from the properties of the Management object > SmartEvent Intro.

Important -

- You cannot monitor more than one of the possible software blades: IPS, DLP, or Application Control. To monitor more than one blade, you must purchase the full SmartEvent Suite.
- A Security Management Server can host only one SmartEvent Intro server.

Basic Concepts and Terminology

- Event Policy - the rules and behavior of SmartEvent
- Event - activity that is perceived as a threat and is classified as such by the Event Policy
- Log Server - receives log messages from the gateway
- SmartEvent Correlation - component that analyzes logs on Log servers and detects events
- Event Database - stores all detected events
- SmartEvent Server - houses the Event Database, receives events from Correlation Units, and reacts to events as they occur
- SmartEvent Client - Graphic User Interface where the Event Policy is configured and events are displayed
- Management Server - Security Management Server or, in a Multi-Domain Security Management environment, Domain Management Server

SmartEvent Sizing Guide

The SmartEvent Sizing Guide helps you find the recommended SmartEvent appliance suitable to your environment scale. See the Sizing Guide in sk87263 (http://supportcontent.checkpoint.com/solutions?id=sk87263).
Chapter 2

Initial Configuration

In This Chapter

<table>
<thead>
<tr>
<th>Check Point Licenses</th>
<th>7</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initial Configuration of the SmartEvent Client</td>
<td>7</td>
</tr>
<tr>
<td>Enabling Connectivity with Multi-Domain Security Management</td>
<td>8</td>
</tr>
</tbody>
</table>

SmartEvent and SmartReporter components require secure internal communication (SIC) with the Management server, either a Security Management Server or a Domain Management Server (see "Enabling Connectivity with Multi-Domain Security Management" on page 8).

Once connectivity is established, install SmartEvent and SmartReporter and perform the initial configuration.

Check Point Licenses

Check Point software is activated with a License Key. You can obtain this License Key by registering the Certificate Key that appears on the back of the software media pack, in the Check Point User Center.

The Certificate Key is used in order to receive a License Key for products that you are evaluating.

In order to purchase the required Check Point products, contact your reseller.

Check Point software that has not yet been purchased will work for a period of 15 days. You are required to go through the User Center in order to register this software.

1. Activate the Certificate Key shown on the back of the media pack via Check Point User Center (http://usercenter.checkpoint.com).
   The Certificate Key activation process consists of:
   - Adding the Certificate Key
   - Activating the products
   - Choosing the type of license
   - Entering the software details
   Once this process is complete, a License Key is created and made available to you.

2. Once you have a new License Key, you can start the installation and configuration process. During this process, you will be required to:
   - Read the End Users License Agreement and if you accept it, select Yes.
   - Import the license that you obtained from the User Center for the product that you are installing. Licenses are imported via the Check Point Configuration Tool.
   The License Keys tie the product license to the IP address of the SmartEvent server. This means that:
   - Only one IP address is needed for all licenses.
   - All licenses are installed on the SmartEvent server.

Initial Configuration of the SmartEvent Client

The final stage of getting started with SmartEvent is the initial configuration of the SmartEvent clients. The SmartEvent client is part of the Check Point SmartConsole.

- Define the Internal Network
- Install the Event Policy

Events will begin to appear in the SmartEvent client.
Enabling Connectivity with Multi-Domain Security Management

In a Multi-Domain Security Management environment, the SmartEvent server can be configured to analyze the log information for any or all of the Domain Management Servers on the Multi-Domain Server. In order to do this, the SmartEvent server database must contain all of the network objects from each of the Domain Management Servers and then be configured to gather logs from the selected log servers.

Installing the Network Objects in the SmartEvent Database

1. From the SmartDomain Manager, open the Global SmartDashboard.
2. In the Global SmartDashboard, create a Host object for the SmartEvent server.
3. Configure the object as a SmartEvent server and Log server.
4. Save the Global Policy.
5. Close the Global SmartDashboard.
6. In the Multi-Domain Security Management client, assign the Global Policy to the Domains with which you will use SmartEvent.

Configuring SmartEvent to work with Multi-Domain Security Management

1. In the SmartEvent client, select Policy > General Settings > Objects > Domains and add all of the Domains you will be working.
   Objects will be synchronized from the Domain Management Servers – this may take some time.
2. Select Policy > General Settings > Objects > Network Objects, and add networks and hosts that are not defined in the Domain Management Servers.
3. Select Policy > General Settings > Initial Settings > Internal Network, and add the networks and hosts that are part of the Internal Network.
4. Select Policy > General Settings > Initial Settings > Correlation Units, click Add and select the SmartEvent Correlation Unit and its Log servers. For traffic logs, select the relevant Domain Log Server or Multi-Domain Log Server. For audit logs, select the relevant Domain Management Server.
5. Install the Event Policy.
Chapter 3

Working with Queries

In This Chapter

- Event Queries 9
- Event Query Results 12
- Event Data Analysis 17
- Administrator Permission Profiles - Events and Reports 24

SmartEvent uses filtered event views, called queries, to identify and show relevant events. Event window information, timelines, graphs and reports are based on queries that identify potentially dangerous events and event patterns. You use this information to adjust your Security Policies and protection settings in response to detected threats.

Event Queries

SmartEvent uses filtered event views, called queries, to define the events to view. Located in the Queries Tree, these queries filter and organize event data for display in the Events, Charts and Maps tabs. Queries are defined by filter properties and charts properties. Filter properties allow you to define what type of events to display and how they should be organized. Charts properties allow you to define how the filtered event data should be displayed in chart form.

Predefined Queries

SmartEvent provides a thorough set of predefined queries, which are appropriate for many scenarios. Queries are organized by combinations of event properties, for example:

- **IPS**, which includes queries of IPS events
- **Direction**, such as **Incoming**, **Internal**, and **Outgoing**
  - Direction is determined by the Internal Network (see "Defining the Internal Network" on page 35) settings.
- **IP**, either the **Source** or **Destination** IP address
- **Ticketing**, such as ticket **State** or **Owner**
- **Severity**, such as **Critical**, **High**, and **Medium**

Custom Queries

SmartEvent gives you the flexibility to define custom queries that show the most relevant events and trends. Once you have defined custom queries, you can organize them into folders so that they are easy to find and use.

You can use your queries to:

- Show an overview of events with specified characteristics in the **Events** tab
- Generate reports to analyze specified events and trends in the **Reports** tab
- Show event counts and severity trends in the **Timelines** tab
- Show event data in easy to read charts in the **Charts** tab
- Show events by source or destination country in the **Maps** tab
Creating Custom Queries
You can create a custom query from scratch in the Custom folder or based on an existing query.

To create a custom query based on the default query:
1. In the Selector tree, right-click on the Custom folder.
2. Select New.
3. Enter a name the custom query.

To create a custom query based on an existing query:
1. Right-click an existing query and select Save As.
2. Enter a name for the new query.
3. Click Save.

Customizing Query Filters
You can work with queries in the Events, Timelines, Charts and Maps windows. See the Reports ("Reports Tab" on page 26) section to learn about procedures for working with report queries.

To change query filter properties:
1. In the tree, right-click the query.
2. Select Properties > Events Query Properties from the options menu.
3. In the Query Properties window, do one or more of these tasks:
   - Use the Add and Remove buttons to select criteria fields to include in your query.
     Selected criteria show in the In Use list. Criteria not selected show in the Ignored list. You can enter text in the Search Fields box to highlight matching text strings in criteria fields.
   - Click the Filter column to define filter criteria. Select or enter criteria values in the window that opens.
     The window type and data entry procedures are different for each criterion type. The default value is Any.
   - Optional: Clear the Show option to prevent a criterion column from showing in the Event pane.
     In this case, the criterion filter applies to the query, but the column does not show. By default, the Show option is selected for all criteria.

   Note - If you clear the Show option for a criterion that does not have a filter applied, that criterion automatically moves to the Ignored list. This action is the same as using the Remove button.

   - Optional: Select a field in the In Use list and click Group.
     This shows events with the same field value under a collapsible summary line. This option works best when you select only one criteria field.
   - Use the Up and Down buttons to change the criteria column sequence in the Event Log.
4. Optionally define these additional query settings:
   - To require users to enter or select a filter value at run time, select the When running the query prompt for option. Select a filter criterion from the list.
     When enabled, the query shows a Filter window and the user must select or enter the filter value. This makes the query more dynamic, enabling the user to specify values each time the query is run.
   - Auto refresh query every 60 seconds - The query automatically updates the Event Log at 60 second intervals. This option is cleared by default.
   - Run query on OK - The query automatically updates the Event Log after you complete the definition and click OK. This option is selected by default.
   - Use existing value from the toolbar - Shows only the number of events as defined in the Show up to # toolbar field. This option is selected by default.
   - Return maximum of X events per query - Shows only the number of events defined it this field. SmartEvent ignores the value in the Show up to # toolbar field.
To clear filter values from a query:
1. In the tree, right-click the query.
2. Select Properties > Events Query Properties from the options menu.
3. In the In Use list, right-click the value in the Filter column.
4. Select Clear Filter. This step changes the filter to the value Any.

Customizing Query Charts

To change the way your custom query will display as a chart:
1. Right-click the new query and select Properties > Events Query Properties. The Events Query Properties window appears.
2. Add fields to the column on the right side of the window to make them available in the Split-By menu on the chart. Selecting a field from the Split-By menu displays the event data divided according to the selected event characteristic.
3. In Show top, select the number of top values to show from the chosen Split-By field.
4. Select to display the query by default as a Pie chart or on a Time axis. If you want to display on a Time axis using a pre-defined Time Resolution, choose the Time Resolution you want.

Organizing Queries in Folders

You can create custom folders to organize your custom queries, as well as subfolders nested within folders.

To create a custom folder:
1. Right-click on Custom (or any other custom folder you have created previously) and select New Folder.
2. Name the folder.

When you create a new query, you can save it to this new folder by selecting it before selecting Save in the Save to Tree window.
Event Query Results

The **Events** tab is the heart of SmartEvent.

These are the components of the Events tab:

1. Query Tree
2. Event Statistics Pane
3. Event Log
4. Log entry detail pane
5. Event Preview Pane

The **Events** tab is an **Event Log** that shows events generated by a query. In addition, the Events tab contains the **Query Tree**, the **Event Preview Pane** and the **Event Statistics Pane**.

Double-click a query in the **Query Tree** to run that query. The results show in the **Event Log**. The top Events, Destinations, Sources and Users of the query results are displayed in the **Event Statistics Pane**, either as a chart or in a tallied list. The details of the selected event are displayed in the **Event Preview Pane**.

**Event Log**

The SmartEvent **Event Log** can display up to 30,000 events. The events displayed are the result of a query having been run on the Event Database. To run a different query, double-click on a query in the **Selector tree**. The **Event Log** will display the events that match the criteria of the query.

The **Event Log** is where detected events can be filtered, sorted, grouped, sent for review and exported to a file to allow you to understand your network security status. Event details, such as **Start** and **End Time**, **Event Name** and **Severity**, are displayed in a grid. In the **Status** bar at the bottom of the SmartEvent client window, **Number of records in view** displays a count of new events. **Refresh** retrieves the data from the database according the active query filter.

The details of an event provide important specifics about the event, including type of event, origin, service, and number of connections. You can access event details by double-clicking the event or by displaying the **Event Preview Pane**.
Queries are built with certain default settings that can be changed directly in the Events tab to provide more specific or more comprehensive results.

- The time frame Last... selection lets you choose the period of time for which events should be displayed.
- The Event number selection sets the number of events that should be displayed from the query (default is 5,000 events). Up to 30,000 events can be displayed and managed at one time.
- The Group By selection is particularly useful here to quickly divide the data by specific criteria and immediately show the number of events per grouping.

Filtering Events

After running a query, you can further filter the event data by right-clicking any column and defining the filter parameters. This will temporarily include the filter in the active query and run the query again against the database to return the matching values.

A green filter icon at the top of a column indicates that a filter is applied to that field. You can then choose to save the new set of filters as a custom query by selecting Save from the File menu. Running the query again will discard the filters that have not been saved.

To use filters with query results:
- To change the filter criteria, right-click on a column header and select Edit Filter.
- To remove events that have any specific field value, right-click on the value and select Filter out.
- To include only events that have a specific field value, right-click on the value and select Follow.
- To remove the extra conditions you have applied, right-click the filter and select Clear Filter.

Sorting and Searching Events

Running a query could return thousands of matching events. To help you organize the events that have already been returned by the query, you can sort them by clicking on any of the column headers.

You can also look for events which have specific values by entering values in the Search field. Searching for multiple values, using commas to separate the values, will return the events that contain all of the search values, although the values can be in any of the event fields. The search can be made case-sensitive or can look for data that is not displayed in columns.

Grouping Events

One of the most powerful ways to analyze event data is by grouping the data based on the specific columns using the Group By button on the toolbar. Here you can group the events by one or more columns and the Event Log shows the number of matching events in those groups, presented in descending order.

You can also specify the default grouping that a query should use by marking fields as Grouped in the Events Query Properties ("Customizing Query Filters" on page 10) window.

The top line of each group in the Event Log shows a summary of the events that it contains. If you hover over a field in the top line, you can see details of what data that field contains in all of the events in the group.

To group events by one or more fields, perform one of the following:
1. Click on Group By in the toolbar and select the field to use for grouping events.
2. Click on Group By in the toolbar and select More Fields. Then in the Group By window select one or more field to use for grouping events.
3. Right-click on the column in the Event Log you want to use for grouping events and select Group By This Column.
   
   Once you have already grouped by a column, you can add another column to use for grouping by right-clicking on the column in the Event Log you want to use for grouping events and select Add this Column to the Group.
To remove fields from the grouping, perform one of the following:
1. Click on **Ungroup** in the toolbar to remove all grouping.
2. Click on **Group By** in the toolbar and select **More Fields**. Then in the **Group By** window remove one or more field from grouping.
3. Right-click on the column in the Event Log you want to remove from the grouping and select **Remove Column from Group**.

**Sending an Event**

In some circumstances, event information can be used to show evidence of a security attack or vulnerability that needs to be resolved. For example, you may decide that another member of your security team should review an event as evidence of an attack. Also, reporting events to Check Point can help Check Point improve the IPS technology to detect new threats in an ever-changing security environment. From the Event Log, you can choose to send event details as an email using your default email client, or you can choose to send the event details to Check Point over a secure SSL connection.

**To send an event using email:**
1. Select the event in the Event Log.
2. Right-click on the event and select **Send event by Email**.
   A new email opens using your default email client and the event information is included in the body of the email.

**To report an event to Check Point:**
1. Select the event in the Event Log.
2. Right-click on the event, select **Report Event to Check Point** and choose whether you want to include just the Event Details or to also include the Packet Capture associated with the event.

Only the event information will be sent to Check Point over a secure SSL connection. The data is kept confidential and Check Point only uses the information to improve IPS.

**Exporting Events to a File**

The Event Log can contain thousands of events. You can export the events from the SmartEvent client into a text file to allow you to review or manipulate the data using external applications, such as a spreadsheet or text editor.

You can export events from the Overview tab, Events tab or Events window. When exported, the list of events will be saved exactly as it appears in the Event Log, including the visible columns and any sorting, filtering or grouping that is applied to the events.

**To export events to a comma-delimited (csv) file:**
1. In the Overview tab, Events tab or Events window, organize the events as you would like them to be saved.
   - Hide/show columns to display the information you want to save.
   - Apply sorting, filtering and grouping to produce a list of events in the format you want.
2. From the File menu, select **Export Events to csv File**.
3. Name the file, navigate to the location where you want the file saved and click **Save**.

**Examining Client Vulnerability**

To maintain a high level of security, organizations must install the latest security patches on network computers. Many of the security patches are designed to prevent threats from exploiting known vulnerabilities. If you are consistent with implementing software patches, your network computers will not be vulnerable to some of the attacks that are identified by SmartEvent. SmartEvent ClientInfo helps you determine whether an attack related to Microsoft software is likely to affect the target machine. If the target machine is patched, you can stop the events from being generated by choosing to exclude the target machine from the event definition or from the specific IPS protection.

SmartEvent ClientInfo connects to the computer whose IP address is listed in the event. After you enter credentials with administrator privileges on the target computer, SmartEvent ClientInfo reads the list of Microsoft patches installed on the computer as well as other information about the installed hardware and software. SmartEvent ClientInfo also retrieves the Microsoft Knowledge Base article related to the
vulnerability reported in the event and checks to see if the patches listed in the article are installed on the target computer. If SmartEvent ClientInfo finds that the matching patch is installed, it is likely that the attack will have no effect on the target computer and you can choose to create an exception so that IPS or SmartEvent stops recognizing the attack as a threat.

Once the computer information is loaded in SmartEvent ClientInfo, you can perform the following functions:

<table>
<thead>
<tr>
<th>Icon</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Save" /></td>
<td>Save the information in the active tab to a .csv file</td>
</tr>
<tr>
<td><img src="image" alt="Enter" /></td>
<td>Enter new credentials for accessing the computer information</td>
</tr>
<tr>
<td><img src="image" alt="Copy" /></td>
<td>Copy the contents of the selected cell</td>
</tr>
<tr>
<td><img src="image" alt="Run" /></td>
<td>Run Google.com search using the contents of the selected cell</td>
</tr>
<tr>
<td><img src="image" alt="Search" /></td>
<td>Filter the contents of the active tab for rows containing the search text</td>
</tr>
<tr>
<td><img src="image" alt="Filter" /></td>
<td>Filter the contents of the active tab for rows containing the KB number</td>
</tr>
<tr>
<td><img src="image" alt="Get Info" /></td>
<td>Connect to the specified IP address to gather the computer information</td>
</tr>
</tbody>
</table>

To make sure that a computer is not vulnerable to an attack:

1. In the **Events** tab, right-click on the event you want to investigate and select **SmartEvent ClientInfo**.
2. Enter user credentials that allow administrator privileges on the target computer or select **Use Windows Logon Account** to login with your current credentials. You can also save your credentials to avoid having to enter them again.

SmartEvent ClientInfo retrieves the software and hardware information from the target computer, as well as the details of the Knowledge Base article associated with the vulnerability identified in the event.

3. Check the result. SmartEvent ClientInfo returns one of the following results:
   - **Installed fix / Computer is not vulnerable** - In this instance, SmartEvent ClientInfo found that the patch recommended by Microsoft for protecting against the vulnerability is installed on the target computer.
     
     Based on this, you can decide to modify the associated IPS protection or event definitions to prevent these events from displaying in the future.
   
   - **Unfound fix / Derived fixes exist** - In this instance, SmartEvent ClientInfo found that a patch is installed that is related to the Security Bulletin, but found that the main patch that is recommended by Microsoft for protecting against the vulnerability is not installed on the target computer. The installed fix may not cover all of the affected software.

     Click on the KB numbers specified to open the associated Knowledge Base articles. Review the recommended remediation steps, which may include installing a patch on the target computer.
   
   - **Missing Fix / Computer may be vulnerable** - In this instance, SmartEvent ClientInfo found that the patch recommended by Microsoft for protecting against the vulnerability is not installed on the target computer.

     Click on the KB number specified to open the associated Knowledge Base article. Review the recommended remediation steps, which may include installing a patch on the target computer.

   **Note** - If SmartEvent ClientInfo finds that the patch in the KB article is not installed on the remote computer, it may indicate one of the following:

   - The vulnerability does not affect or is not relevant to the target computer’s Operating System OR Service Pack version. If so, the computer is not vulnerable.
   
   - The article is relatively old and you may have installed Service Pack that includes the patch for the vulnerability. If so, you should check the installed Service Pack to see if it was released after KB article and may include the associated patch.
**Event Statistics Pane**

The Event Log is accompanied by charts displaying the Top Events, Top Sources, Top Destinations and Top Users for the active query. These statistics are automatically updated as filters are applied to the Event Log.

You can toggle between viewing the statistics as a chart or a list by clicking on the arrow in the top-right corner of each of the boxes and selecting Show Pie Chart.

You can filter in or out any value in the Event Statistics Pane to focus the query results on the data that is most important to you. Filtering in the Event Statistics Pane is also reflected in the Event Log, and clearing filters from the Event Statistics Pane clears all filters that have been applied to the query.

- To remove events that have any specific field value, right-click on the value and select Filter out.
- To include only events that have a specific field value, right-click on the value and select Follow.
- To remove the extra conditions you have applied, click on the Clear Filter icon.

**Event Details**

See the details of an event from the Preview Pane in the Events tab or by double-clicking on the event in the Event Log. The Event Details window has two tabs with different data:

- **Summary tab** - Shows a brief summary of the event in a user-friendly format.
- **Details tab** - Shows the full, technical details of the event.

These options are available from the Event Details window:

- **Copy** - Copies the event details to the Windows Clipboard.
- **Actions** - Actions that you can do that are related to this log. They include:
  - **Event Raw Logs** - Launches SmartView Tracker and displays the log entries upon which the event is based.
  - **Edit Ticket** - Lets you set the state of the event, assign an owner, and add a comment.
  - **Add Comment** - Lets you add a quick comment about the event without changing the state or owner.
  - **View History** - Lets you view the ticket activity on the event, including changes to the state, owner, or comments.
- **Blade Specific Menu** - For example, IPS or Application Control. This menu has different options depending on the Software Blade that is related to the event.
- **Previous** displays the event that appears before the current event in the Event Log.
- **Next** displays the event that appears after the current event in the Event Log.

**Summary Tab**

The Summary tab includes:

- The source of the activity. If Identity Awareness is enabled, this can be the user name.
- A brief description of the event.
- The action taken on the event.
- The time of the event.
- Other important data related to the event.

**Details Tab**

The Details tab includes:

- Details about the Software Blade and rule that caused the event.
- Ticketing information for the event - Use this to track activity related to the event.
- General Event Information - Includes the severity for the event and a unique ID.
- Traffic Information - Where the event originated, its destination, and the size of the data in bytes.
- Event Detection - How and when the event was detected and by which Security Gateway.
- More - Additional information related to the connections involved in the event and the source.

![Image of SmartEvent interface](image)

**Browse Time**

The **Browse Time** feature keeps track of the total time that users are connected to different sites and applications. R76 and later Security Gateways calculate the cumulative connection time for each session and periodically updates this value until the session is closed.

**Browse time is calculated as follows:**

- Total browse time is calculated for each site from the first HTTP request to the last HTTP response. Idle time of more than two minutes is not included in the browse time.
- The minimum calculated time is two minutes. Any connection of less than two minutes is rounded up to two minutes. However, browse time for each user does not include time spent at more than one site simultaneously. For example, if a user connects to google.com and facebook.com at the same time, only one site is included in the browse time calculation.

**Event Data Analysis**

SmartEvent includes a many different tools to let you analyze events that occur in your environment. You can get access to these tools using one of the tabs in the SmartEvent GUI.

**Overview Tab**

The SmartEvent **Overview** tab shows critical security status information for your environment. Its main focus is presenting a quick view of the recent events data using the Timeline View, Recent Critical Events, and Top tables and chart. These interactive sections report on the events based on the **Time Frame** setting to allow you to display event data from a specific latest period of time.
Double-click on data in any of the sections in the Overview tab to open the associated list of events so that you can continue investigating issues all the way down to the individual event level.

By default, the Overview tab includes these sections:

1. **Timeline View** - Timelines let you see specified recent events in a linear format. The number of events is shown inside a circle at each defined time interval. The circle itself is color coded to show the severity of the different events. You can add, modify or remove timelines from this view just as you would in the Timeline Tab (on page 19).

2. **Events Query** - This section shows events from a user-selected query. This is useful for examining important events that occurred during the specified Time Frame. To select a query to show in this pane:
   a) Click the cogwheel button in the pane.
   b) Select one of these options from the menu:
      - **Set Query** - Select a predefined query from Set Query window.
      - **Show Newly Detected Applications table** - Show applications seen for the first time during the specified Time Frame.

   You can search, sort, filter and group events using the same methods as in the Events tab ("Event Query Results" on page 12). Click the arrow to select a different query to show here.

3. **‘Top’ Panes** - The Top Application and Top Events panes show the most frequent occurrences during the specified Time Frame according to user-selected categories. You can show events according to traffic volume or the quantity of events. To show the top events:
   a) Click the cogwheel button in the pane.
   b) Select one of these criteria:
      - Sources
      - Users
      - Destinations
      - Malwares
      - Malware involved hosts
      - Malicious activities
      - Application / Site
      - Application Categories
c) Select a metric:
   - **Show Data by Event Count** - Quantity of events during the specified **Time Frame**
   - **Show Data by Traffic** - Traffic volume in MBs

4. **SmartEvent Status** - The Status section contains system information including:
   - **Status** - This indicator reports the current status of the Event Analysis system, including problems connectivity to Correlation Units and Log servers and when the allocated disk space is full. Click on the link for more information.
   - **Object Sync** - This indicator reports on the synchronization of objects between the management servers (either Security Management or Domain Management Server) and the SmartEvent server. Click on the link for more information.
   - **Config** - This indicator will appear if components are not configured, including Internal Network settings (see "Defining the Internal Network" on page 35) and Correlation Units. Click on the link for more information.
   - **Events received in the** - These statistics show the number of events received by the SmartEvent server in the last minute, hour and 24-hour period. This information gives a quick glance at the traffic load on the SmartEvent server. Unusual data in these fields may indicate connectivity problems between the components of the Event Analysis system.

### Timeline Tab

Timelines let you see specified recent events in a linear format. The number of events is shown inside a circle at each defined time interval. The circle itself is color coded to show the severity of the different events.

**Note** - Because timeline circles use colors to show event severity, timelines for queries without filters (such as a query by source IP address) are identical to those of the All Events query.

You can modify these timelines or add new timelines for predefined and custom queries. You can also rename timelines and move them up or down the in the window.
To add a new timeline:
1. Select Manage > Add Line.
2. In the Add Line window, do one of the following:
   a) **Use a Predefined Query**: Select an existing query and click OK.
   b) **Modify a Predefined Query**:
      i) Select an existing query and click Configure.
      ii) In the Events Query properties window, configure the query to filter for the events that you want to track and click OK.
      iii) Enter a name for the new custom query. You can choose to save the time frame for the query.
      iv) Click Save.
   c) **Create a new Custom Query**:
      i) Click New to create a custom query which you can use for the new timeline.
      ii) In the Events Query properties window, configure the query to filter for the events that you want to track and click OK.
      iii) In the Add Line window, enter a name for the custom query.
3. In the Add Line window, click OK.
You can now see the configured timelines and you can modify the Time Frame and Time Line Resolution to help you analyze the event data.

To modify an existing timeline:
1. Select a timeline and select Manage > Configure.
2. In the Events Query properties window, configure the query to filter for the events that you want to track.
3. Click OK.
The selected timeline now displays the event data based on the modified query.

**Charts Tab**

Charts display query results in a graphical format which you can configure to divide the events data based in any event characteristic. You can then drill down into any segment of the chart to display a list of those events in a new Events window.

Event queries can be shown with a **Time Axis** or as a **Pie Chart**. The query's chart properties define which type of chart will be shown by default but you can change the chart type to display at any time by selecting from the options in the upper-left corner.
- The **Time Axis** display shows the query results over time based on a configured **Time Resolution**. This method focuses attention on how the event data differs over time.

- The **Pie Chart** is the best way to show Top N data such as By Source (top sources), By Destination (top destinations), and By Service (top services). This method focuses attention on the number of events with specific properties.

**Event Data Options**

The following are settings that can be set from the Toolbar to change the event data that is displayed in the chart:
• **Time frame** - Select a specific time frame for which events are displayed. For example, you can choose to show only events during the last 24 hours, the last 30 days, or a custom time frame.

• **Time Resolution** - This field determines how events are grouped in charts and timelines. For example, when the time frame is set to one hour, all events that match the query filter properties and occurred within the period of one hour will be displayed together. The colors of the time wheel indicate the breakdown of events by category within the selected period of time.

• **Split By** - This field determines which dimension will be used to analyze the events. In the query Chart Properties, you can choose which dimensions to make available for displaying in the charts.

• **Show Top** - This field determines how many of dimensions results will be displayed in the chart. In the query Chart Properties, you can set the default number.

You can also set a particular chart to be displayed by default in the Charts tab by right-clicking on the query and selecting Run on Start.

**Manage Options**

The following are options that can be changed from the Toolbar to present the chart data in a more informative and appealing manner:

• **Fixed Scale** - By default, the scale of the number of events will change based on the results displayed in the chart. By selecting Fixed Scale, you can choose for the scale of the number of events to remain constant as you scroll through the chart.

• **Data Grid** - You can choose to show a data grid next to the chart. The data grid provides a table which shows a summary of all of the data points in the query. When you move the cursor over any part of the chart or grid, the associated data will be highlighted in the other area.

• **Copy to Clipboard** - Select the option to access the options for copying the event statistics to your computer Clipboard for external use. You can copy the image itself, or you can the copy raw event counts represented by the image that is currently displayed and then paste that data into another application.
  - **As a Bitmap** - To copy the image that is currently displayed.
  - **As Text (data only)** - To copy the raw event counts represented by the image that is currently displayed.

• **Print** - Select to print the image that is currently displayed.

• **3D/2D Display** - Select to choose if to display the chart as flat (2D) or with depth (3D).

• **Gallery** - Select to show the pie chart as a bar, doughnut, or pie chart.

The following are elements of the chart display that can be changed by right-clicking on the chart to customize the presentation of the chart:

• **Data Grid** - You can choose to show a data grid next to the chart. The data grid provides a table which shows a summary of all of the data points in the query. When you move the cursor over any part of the chart or grid, the associated data will be highlighted in the other area.

• **Legend Box** - You can choose to show or hide the Legend Box. The Legend Box is a key which indicates what the colors of the chart represent. Change the location and font of the Legend Box by right-clicking on it.

• **Background Color** - You can select a background color for the chart.

You can modify the display options for the data grid, legend box, axis labels or axis scales. Right-clicking any of the elements allows you to change the font, text color, display location and other graphical options.

**To view a chart:**

1. Run a query by double-clicking the query in the Query Tree. You can also open your chart in a new window by right-clicking the query and selecting Run in New Window. This allows you to keep multiple charts open at the same time.

2. Decide whether you want the chart to be based on time (Time Axis) or based on other event properties (Pie Chart).
   - When using Time Axis, choose a Chart Time Resolution to group the events by a specific time range.

3. The chart will display all events. You can choose to show only a number of the top query results by selecting a number from the Show Top menu.
Maps Tab

Source and Destination information are frequently critical when determining the potential threat of traffic. Some companies need to block traffic from certain countries based on security, political, or legal reasons whereas other companies may see identifying traffic by country of origin or destination simply as a way to limit the traffic passing through the network.

In the Maps tab, SmartEvent presents source and destination countries for the active query on an interactive world map. Countries are color-coded to indicate levels of event activity. You can define the number of countries to include in the top tier of countries (Top N) and in the second tier of countries (Next Top N) to change how countries are grouped in the map.

By double-clicking on a country, you can drill-down to see a detailed list of events for that country. By default the map shows the results of the All Events query; however, you can populate the map with information from any of the available queries by double-clicking on a query in the Query Tree. You can also choose to view continents individually in order to see countries more clearly.

Statistics information about the active query is displayed below the interactive map. The five countries with the highest number of events matching the query filter are shown with the number of events for each, as well as the total number of countries matching the query.

Interact with the map using the following actions:

- To see the number of events that correspond to a country, move the mouse over that country.
- To view query results for a country in an Events window, double-click on the country.
- To change between viewing the entire world map and viewing maps for individual continents, choose from the Map menu.
- Activity Level - In the bottom right corner of the map is the Activity Level key. Countries are colored according to four tiers:
  - Top - By default, the Top 3 countries are colored Red. Choose the number of countries to include in the top tier by changing this setting.
  - Next Top - By default, the Next Top 5 countries are colored Yellow. Choose the number of countries to include in the second tier by changing this setting.
• Others - All countries with events, but are not included in the Top or Next Top tiers, are colored Blue.
• No Activity - All countries without events are colored White.

Moving the mouse over a tier in the Activity Level key will highlight the Countries in that tier.
In addition, in the bottom left corner of the map is a summary of event statistics which includes the number of events for the top 5 countries and the total number of countries with events.

Reports Tab

Use the Reports tab to see, manage and generate reports that show a summary of events identified by SmartEvent. You can generate report for these supported blades:

• Application and URL Filtering events
• Data Loss Prevention events
• IPS events
• Anti-Bot and Anti-Virus events

• All - Tabular list of all events, including events not related to these supported blades
• Each supported blade has its own filter criteria and format that for presenting the information.

Administrator Permission Profiles - Events and Reports

SmartEvent enables you to provide an administrator with a Permission Profile for the SmartEvent database. A Permission Profile is a permission ID card that is assigned to administrators or administrator groups.

The administrator and his Permission Profile are verified during login. When an administrator logs into SmartEvent his user name and password are verified by the SmartEvent server. If the administrator is not defined on the SmartEvent server, the server will attempt the login process with the credentials that are defined on the Security Management Server or Multi-Domain Server connected with SIC to the SmartEvent server.

Note - If you do not want to centrally manage administrators, and you only use the local administrator defined for the SmartEvent server:

From the SmartEvent server command line, invoke:
cpprod_util CPPROD_SetValue FW1 REMOTE_LOGIN 4 1 1

The Permission Profile types for the SmartEvent Events tab are set in the SmartDashboard or SmartDomain Manager (SmartDashboard > Manage > Permissions Profiles > New / Edit).

The following are the three types of Permission Profiles:

• No Access indicates that the administrator cannot view the SmartEvent Events and Reports tabs.
• Read Only enables the administrator to view SmartEvent Events and Reports tabs.
• Read/Write enables the administrator to modify the SmartEvent Events and Reports tabs using the Change State option.

These permissions are available for Events and Reports:

• SmartReporter Policy - Configure Global Properties for SmartReporter.
• SmartReporter - Configure SmartReporter.
• SmartEvent Events Database - View and manage the Events tab of SmartEvent.
• SmartEvent Policy - View and manage the events correlation on the Policy tab of SmartEvent.
• SmartEvent Reports - Users only see the Reports tab.
  • All Blades - This setting applies to all blades.
  • Application and URL Filtering Blades - Applies only to the Application Control and URL Filtering blades.
Multi-Domain Security Management

When working with Multi-Domain Security Management, SmartEvent is Domain oriented. That is, each Event and Report is associated with a Domain.

The administrator can view Events and Reports about Domains to which he has permissions. Only locally defined administrators on the SmartEvent server or the Multi-Domain Server Super User can view all events including cross-Domain events.
# Chapter 4

## Reports

**In This Chapter**
- Reports Tab: 26
- Predefined Reports: 26
- Custom Reports: 27
- Configuring Reports: 27
- Generating Reports: 30

### Reports Tab

Use the **Reports** tab to see, manage and generate reports that show a summary of events identified by SmartEvent. You can generate reports for these supported blades:

- Application and URL Filtering events
- Data Loss Prevention events
- IPS events
- Anti-Bot and Anti-Virus events
- **All** - Tabular list of all events, including events not related to these supported blades

Each supported blade has its own filter criteria and format for presenting the information.

Each report contains a high-level summary of event patterns followed by detailed analyses and graphs. Each report has its own format and filter criteria.

You can generate reports that show events on a daily, weekly or monthly basis. Some blades can show events summarized by domain.

SmartEvent includes these output options for your generated reports:

- Show on the **Reports** tab
- Open in a Web browser
- Print
- Save as a PDF file
- Send as an email attachment to specified individuals

### Predefined Reports

SmartEvent includes many predefined reports that you can run right out of the box. This release includes predefined reports for daily, weekly, monthly and user-specified time frames (Shown as **Other** in the **Reports** tree).

You can identify predefined reports by the predefined report icon 📁 in the **Reports** tree. You cannot change the default time frame or filter parameters for predefined reports.
Custom Reports

You can define custom reports that show the information necessary to identify and handle security threats. Custom reports are based on existing predefined or custom reports.

You can identify custom reports in the Reports tree by the custom report icon 🎉.

To create a custom report:
1. Right-click an existing report in the Reports tree.
2. Select Save As from the options menu.
3. In the Save Report as window, enter a name for the new report.
4. Continue with the procedures in the Configuring Reports (on page 27) section.

You can also click a report definition and then save, rename or delete it.

Configuring Reports

You can configure predefined and custom reports in accordance with your requirements. Reports are based on queries using these criteria:

- **Period** - Defines the default time frame for a report (custom reports only)
- **Filter** - Defines the filter conditions for a report (custom reports only)
- **Schedule** - Defines when a report will run automatically (all report types)
- **Email** - Sends the report by email and defines the default email addresses to use (all report types)

To configure a report:
1. Select a report in the Reports tree and click Manage.
2. In the Configuration window, configure the report criteria using the procedures for the applicable blade or report type. The individual procedures show in the next sections.
3. Click OK.

Defining the Time Frame

You can define a default period of time (time frame) for each report. These defaults are used for reports that run automatically on a predefined schedule. When you manually generate a report, you define the time frame at run time.

There are five predefined time frames that you can use for all reports:

- **Today**
- **Yesterday** (default for predefined daily reports)
- **This week**
- **Last week** (default for predefined weekly and other reports)
- **This month**
- **Last Month** (default for predefined monthly reports)

**Specific Dates** - Select a start and end date

To define the time frame:
1. Select a report in the Reports tree.
2. Select Manage from the options menu.
3. On the Period page, do one of these steps:
   - Select a predefined time frame from the list.
   - Define a custom date or range of dates in the Specific Dates field.
**Report Filters**

You can use filters with reports to identify and summarize applicable events. Each report has one or more optional filters that you can use. You can define your own filters for custom reports but you cannot change filter definitions for predefined reports.

Each filter type has its own configuration window, from which you can select values from a list or manually enter values. See the online help for an explanation of the fields in each window type.

You can also add **Run-Time Filters**, where users enter filter criteria each time they run the report.

**To define a report filter:**
1. In the **Configuration** window, go to the **Filter** pane.

![Filter Settings](image)

2. In the **Filter Settings** pane, do one or more of these steps to work with the filter settings:
   - Click a **Filter** link in a row or select a row and click **Edit**.
   - In the **Filter** window that opens, enter or select one or more criteria.
     - The options and selection procedure is different for each type or criterion. See the online help for an explanation of the options.
     - To let the user enter or select criteria at run time, select the **Run-Time Filter** option.

3. Select the **Active** option to include the selected filter in this report.
   - Clear to exclude the selected filter.

4. Click **OK**.

**Special Considerations for User Groups**

Unlike most objects used in SmartEvent filters, **User Group** filters use objects that are defined in SmartDashboard. Before you can work with user group objects in filters, you must first define Access Roles for them. You can create SmartEvent reports for user groups that are not in your network, but these must also have defined Access Roles.

See the online help or **Creating Access Roles** section in the *R76 Firewall Administration Guide* for more information.

**Note:** You must enable Identity Awareness on your management server to use Access Roles.

**Automatic Report Scheduling**

You can configure a report to run automatically at specified times. A report can have more than one defined schedule.

**To configure an automatic report schedule:**
1. Go to the **Schedule Settings** window.
2. Select the **Active** option (cleared by default).
   - You must select this option to run reports automatically.
3. Select the report frequency from the list. The available options are:
   - **Once** - Run one time, at the specified time.
   - **Daily** - Run one time each day, at the specified time.
   - **Weekly** - Run one time each week, on the specified week day(s) and time.
   - **Monthly** - Run one time each month, on the specified date(s) and time.

4. Select or enter a run time for the report.

5. Select the **Start on** date.
   This is the date on which the report first runs.

6. Optional: Select the **Expiration date** option and then select the date on which the report runs for the last time.
   By default, this option is cleared.

7. Optional: Click **Add an additional schedule** to define more schedules for this report.

### Configuring Email Settings

You can configure SmartEvent to automatically send reports to specified, default recipients each time the report runs. You define these default recipients on the **Settings** page in the **Reports** tree. You can also send a report to different recipients at run-time, instead of the default recipients.

You must configure the **Outgoing SMTP mail server** and the **Sender Email Address** before you can send email.

**To configure email server settings:**
1. Go to the **Settings** branch in the **Reports** tree.
2. Enter the SMTP mail server URL in the applicable field.
3. Enter the sender email address in the applicable field.
   The sender email address shows on all report emails sent by SmartEvent.
4. Click **Test Connection** to make sure that the defined SMTP connection works correctly.
5. Enter the default recipient email addresses in the **To** and **Cc** fields.
   You can enter more than one email address in each field, separated by semicolons.

**To configure email settings for each defined report:**
1. Select a report in the **Reports** tree and click **Manage**.
2. Go to the **Email Settings** pane.
3. Select the **Send By Email** option (cleared by default).
   You must select this option to automatically send reports by email.
4. Select the **Custom** option.
5. Enter recipient email addresses in the **To** and **Cc** fields.
   You can enter many email addresses in each field, separated by a semicolon.
6. Select the **Report Format**:
   - **HTML**
   - **PDF**
   - **MHT** - MIME HTML archive format
Generating Reports

This section includes the procedure for manually generating reports.

**To generate a predefined or custom report:**

1. Select a report in the Reports tree.
2. Click **Generate**.
3. In the **Generate a Report** window, select or define a report time frame.

   **Note** - For your convenience, SmartEvent remembers the last time frame that you used during the current session. This is helpful when you generate several reports using the same time frame.

4. Click **Generate**.
   After a short time, the report shows in the Reports pane.

After you generate your report, you can use one or more of these output options:

- To print the report, click **Print**.
- To see the report in a Web browser, click **Open in Browser**.
- To save the report as a PDF, click **Save as PDF**. In the **Save As** window, enter the file name and path.
- To send an email with the report PDF attached:
  a) Click **Email**.
  b) In your email client, enter the recipient email addresses.
  c) Enter a subject.
  d) Click **Send**.
Chapter 5

Investigating Events

In This Chapter

- Tracking Event Resolution using Tickets
- Editing IPS Protection Details
- Displaying Original Event Log Information
- Using Custom Commands

Once you have arranged the events as you like in the Event Log, you can begin to investigate their details and evaluate whether they represent a threat.

Tracking Event Resolution using Tickets

Events can be categorized and assigned to administrators to track their path through the workflow of resolving threats. Once administrators review an event, they can assign it a status, such as Investigation in Progress, Resolved, or False Alarm; add comments that detail the actions that have been taken with respect to the event; and assign an administrator as the owner of the event. This process is called Ticketing.

After editing the ticket, administrators can use queries to track the actions taken to mitigate security threats and produce statistics based on those actions.

- To edit an Event Ticket, open the event and click Edit Ticket.
- To add a quick comment about the event without changing the state or owner, open the event and click Add Comment.
- To view the history of actions that have been taken on an event, open the event and click View History.

Editing IPS Protection Details

When reviewing events generated from the IPS blade, you may want to review the IPS protections and profiles to understand why an event was generated or attempt to change the way the traffic is handled by the IPS blade.

The IPS menu presents actions that are specific to IPS events. These actions include:

- **Go to Protection** which opens the SmartDashboard to the IPS protection which triggered the event.
- **Go to Advisory** which opens the Check Point Advisory article which provides background information about the IPS protection.
- **Protection description** which opens a detailed description of the IPS protection.

Displaying Original Event Log Information

To see log entries for an event, right-click the event and select Additional Information > View Event Raw Logs. SmartView Tracker displays the log entries that comprise the event.

**Note** - If the log data for a certain event exceeds 100Kb, the data is discarded.
Using Custom Commands

The SmartEvent client provides a convenient way to run common command line executables that can assist you in investigating events. By right-clicking on cells in the Event Log that refer to an IP address, the default list of commands appears in the context-sensitive menu.

The following commands are available by default: ping, whois, nslookup and Telnet. They appear by design only on cells that refer to IP addresses, because the IP address of the active cell is used as the destination of the command when run.

For example, if you right-click a cell containing an IP address and select the default ping command, a window opens and three ICMP packets are sent to that address. This behavior is configurable, and other commands can be added as well. To add your own custom commands, see Configuring Custom Commands (on page 36).
Chapter 6

System Administration and Modifying Event Policy

In This Chapter

- Adding Exclusions 33
- Modifying the System General Settings 34
- Managing the Event Database 37
- Administrator Permissions Profile - Policy 38

The following tasks help you maintain your SmartEvent system properly:

- Creating objects for use in filters (see "Adding Network and Host Objects" on page 34)
- Adding objects to the Internal Network (see "Defining the Internal Network" on page 35)
- Creating or modifying custom commands that can be run from the SmartEvent client (see "Configuring Custom Commands" on page 36)
- Creating scripts to run as Automatic Reactions for certain events (see "Creating an External Script" on page 37)
- Modify the database settings to fit your disk space and requirements (see "Managing the Event Database" on page 37)

These tasks can be performed from the Policy tab. The Policy tab is hidden by default.

To show the Policy tab: from the View menu, select Policy Tab.

Modifications to the Event Policy do not take effect until saved on the SmartEvent server and installed to the Correlation Units.

To enable changes made to the Event Policy, proceed as follows:

1. Select File > Save.
2. Select Actions > Install Event Policy.

Changes made to the Event Policy can be undone if the changes have not been saved first. To undo changes made to the policy, select File > Revert Changes.

Adding Exclusions

Exclusions remove log entries from query results according to defined criteria (query properties). For example, if source 10.10.10.1 is defined as exclusion for an event, all events with source 10.10.10.1 do not show in the query result. Global Exclusions work in the same way, except they apply to all events.

You can add exclusions in one of these ways:

- Manually using this window
- By accepting Learning Mode recommendations
- By right-clicking an event and selecting Exclude from event definition.

To manually add an exclusion:

1. Click Add.
2. In the Exclusion window, select the Source and/or destination Server object you want to exclude from the query results.
3. Configure any other filter criteria that are available for the specified event.
4. Optionally, click *Apply and delete existing events* to remove the excluded events from the existing query results.
   If you do not see the host object listed, you may need to create it in SmartEvent (see "Adding Network and Host Objects" on page 34).

You can change or delete existing exclusions by selecting *Edit* or *Remove*, respectively.

**Modifying the System General Settings**

The following tasks help you maintain your SmartEvent system:

- Creating objects for use in filters, as described in Adding Network and Host Objects (on page 34).
- Adding additional IPS Event Correlation Units and Log servers, as detailed in Defining Correlation Units and Log servers (on page 35)
- Adding objects to the Internal Network, as described in Defining the Internal Network (on page 35)
- Creating or modifying custom commands that can be run from the SmartEvent client, as explained in Configuring Custom Commands (on page 36)
- Creating scripts to run as Automatic Reactions for certain events, as detailed in Creating an External Script (on page 37).

These tasks can be performed from the Policy tab. The Policy tab is hidden by default, but can be revealed by selecting *Policy Tab* from the *View* menu.

**Adding Network and Host Objects**

Certain objects from the Management server are added during the initial sync with the SmartEvent server and updated at a set interval. However, it may be necessary or useful to add other Network or Host objects, for the following reasons:

- If you have devices or networks not represented on the Management server that are important for the purpose of defining your internal network
- When adding sources or destinations to exclusions or exceptions in Event Definitions
- When selecting sources or destinations in a filter

The following screens are locked until initial sync is complete:

- Network Objects
- Internal Network
- Correlation Units

To make these devices available for use in SmartEvent, proceed as follows:

For a *Host* object:
1. From the *Policy* tab, select *General Settings > Objects > Network Objects > Add > Host*.
2. Give the device a significant *Name*.
3. Enter its *IP Address* or select *Get Address*.
4. Select *OK*.

For a *Network* object:
1. From the *Policy* tab, select *General Settings > Objects > Network Objects > Add > Network*.
2. Give the network a significant *Name*.
3. Enter the *Network Address* and *Net Mask*.
4. Select *OK*.

See Defining the Internal Network (on page 35) for information on adding objects to the Internal Network definition.
Defining Correlation Units and Log Servers

The SmartEvent system works with correlation units that compile event information from log servers. Additional Correlation Units and their corresponding Log servers should be configured during the initial system setup.

To define Correlation Units or Log servers in SmartEvent:

1. From the Policy tab, select General Settings > Initial Settings > Correlation Units.
2. Select Add.
3. Select the […] symbol and select a Correlation Unit from the pop-up window.
4. Select OK.
5. Select Add and select a Log server available to the Correlation Unit from the pop-up window.
6. Select Save.
7. From the Actions menu, select Install Event Policy.

Note - The following screens are locked until sync is complete:
- Network Objects
- Internal Network
- Correlation Units

To define Correlation Units in SmartEvent Intro:
- In a Security Management Server environment: correlation is defined automatically.
- In a Multi-Domain Security Management environment: do the previous procedure on the Multi-Domain Server.

Defining the Internal Network

To help SmartEvent determine whether events have originated internally or externally, the Internal Network must be defined. The direction is calculated as follows:

1. Incoming – all the sources are outside the network and all destinations are inside
2. Outgoing – all sources are inside the network and all destinations are outside
3. Internal – sources and destinations are all inside the network
4. Other – a mixture of and internal and external values makes the result indeterminate

To define the Internal Network:

1. From the Policy tab, select General Settings > Initial Settings > Internal Network.
2. Add internal objects.

Note - It is recommended to add all internal Network objects, and not Host objects

Certain network objects are copied from the Management server to the SmartEvent server during the initial sync and updated afterwards periodically.

The following screens are locked until initial sync is complete:
- Network Objects
- Internal Network
- Correlation Units

Offline Log Files

SmartEvent enables an administrator to view existing logs from a previously generated log file. This feature is designed to enable an administrator to review security threats and pattern anomalies that appeared in the past. As a result, an administrator can investigate threats (for example, unauthorized scans targeting vulnerable hosts, unauthorized logins, denial of service attacks, network anomalies, and other host-based activity) before SmartEvent was installed.

In the same respect, an administrator can review logs from a specific time period in the past and focus on deploying resources on threats that have been active for a period of time but may have been missed (for
example, new events which may have been dynamically updated can now be processed over the previous period).

The generation of Offline logs are set in the **SmartEvent > Policy tab > General Settings > Initial Settings > Offline Jobs**, connected to the Security Management Server or Multi-Domain Server with the following options:

- **Add** enables you to configure an Offline Log File process.
  - **Name** acts as a label that enables you to recognize the specific Offline Line log file for future processing. For example, you can create a query according to the Offline Job name. This name is used in Event tab queries to search events that have been generated by this job.
  - **Comment** contains a description of the Offline Job for edification.
  - **Offline Job Parameters:**
    - **Correlation Unit** the machine that reads and processes the Offline Logs.
    - **Log Server** the machine that contains the Offline Log files. SmartEvent will query this log server to see which log files are available.
    - **Log File** contains a list of available of log files found on the selected Log server to be processed by the correlation unit. In this window you select the log file from which you would like to retrieve historical information.
  - **Edit** enables you to modify the parameters of an Offline Log File process.
  - **Remove** enables you to delete an Offline Log File process.
    - Once you **Start** an Offline Log File process you cannot remove it.
  - **Start** runs the Offline Log File process.
    - The results of this process appear in the **Events** tab and are accessible by the **By Job Name** query or filter.
  - **Stop** ends the Offline Log Files process.
    - **Stop** does not delete the entire process, it only stops the process at the specific point at which it is selected. The information collected up until the process is stopped will appear in the **Events** tab.

With the SmartEvent **Events Tab** you can add offline jobs to query events generated by offline jobs. To do this perform the following:

1. Select the **Events** Tab.
2. Go to **Predefined > By Job Name**.
3. Double-click **By Job Name**.
   - Every job that appears in this window is an offline job except for **All online jobs**.
4. Select the job you want the **By Job Name** to query.
5. Click **OK**.

### Configuring Custom Commands

To add (or edit) custom commands:

1. Select **Actions > Configure Custom Commands**.
2. To add a command, select **Add**. (To edit an existing command, highlight the command and select **Edit**.)
3. Enter the text to appear in the right-click context menu.
4. Enter the command to run, and any arguments.
5. Configure the command to run in an SmartEvent window or a in separate Windows command window.
6. Select whether the command should appear in the context menu only when right-clicking in cells with IP address data.
7. Select **OK**.
Creating an External Script

An external script can be written to receive an Event Definition via standard input. The format of the event content is a name-value set – a structured set of fields that have the form:

\[(name: value ;\star)\]

where name is a string and value is either free text until a semicolon, or a nested name-value set. The script will be reported as successful if it completes within 10 minutes and its exit status is zero.

The following is a sample event as it is received by an external script:

\{(Name: Check Point administrator credential guessing; RuleID: {F182D6BC-A0AA-444a-9F31-C0C22ACA2114}; Uuid: <42135c9c,00000000,2e1510ac,131c07b6>; NumOfUpdates: 0; IsLast: 0; StartTime: 16Feb2005 16:45:45; EndTime: Not Completed; DetectionTime: 16Feb2005 16:45:48; LastUpdateTime: 0; TimeInterval: 600; MaxNumOfConnections: 3; TotalNumOfConnections: 3; DetectedBy: 2886735150; Origin: (IP: 1.2.3.4; repetitions: 3; countryname: United States; hostname: theHost) ; ProductName: SmartDashboard; User: XYZ; Source: (hostname: theHost; repetitions: 3; IP: 1.2.3.4; countryname: United States) ; Severity: Critical; EventNumber: EN00000184; State: 0; NumOfRejectedConnections: 0; NumOfAcceptedConnections: 0) ;

To add an External Script, proceed as follows:

1. From the Policy tab, select General Settings > Initial Settings > Automatic Reactions > Add > External Script.
2. Give the script a name.
3. In the field Action, enter the name of the file containing the script. The script must be placed in the directory $RTDIR/bin/ext_commands, and must have execute privileges.

Managing the Event Database

SmartEvent uses an optimization algorithm to manage disk space and other system resources. When the SmartEvent database becomes too large, the oldest events are automatically deleted to save space. In addition, events that are more than one year old are also automatically deleted.

For instructions to change maximum period and maximum database size to save past events in SmartEvent database see sk69706 (http://supportcontent.checkpoint.com/solutions?id=sk69706)

Backup and Restore of the Database

The evs_backup utility backs up the SmartEvent configuration files and places them in a compressed tar file. In addition, it backs up data files based upon the options selected. The files can be restored using the evs_backup_extractor script. Enclosed are two script versions, one for Windows that has a .bat suffix and one for Solaris, Linux and SecurePlatform that does not have a suffix but should have the executable permissions set.

Usage:

```
```

Additional options are:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EvaDb</td>
<td>Copy the SmartEvent events database</td>
</tr>
<tr>
<td>EvrDb</td>
<td>Copy the SmartReporter consolidation database</td>
</tr>
<tr>
<td>Results</td>
<td>Copy the SmartReporter results</td>
</tr>
<tr>
<td>Logs</td>
<td>Copy the SmartEvent error logs</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>-------------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>LogoAndScripts</td>
<td>Copy the logo file and the distribution script</td>
</tr>
<tr>
<td>export</td>
<td>Runs a evr_addon_export, for a different file name use -filename</td>
</tr>
<tr>
<td>All</td>
<td>Select all options</td>
</tr>
</tbody>
</table>

**Administrator Permissions Profile - Policy**

SmartEvent lets you to assign a Profile to an administrator for the SmartEvent database. When an administrator logs into SmartEvent his user name and password are verified by the SmartEvent server. If the administrator is not defined on the SmartEvent server, the server will attempt the login process with the credentials that are defined on the Security Management Server or Multi-Domain Server connected with SIC to the SmartEvent server.

The Permission Profile types for the SmartEvent **Events** tab are set in the SmartDashboard or SmartDomain Manager (SmartDashboard > Manage > Permissions Profiles > New / Edit) connected to the Security Management Server or Multi-Domain Server with this option:

The following are the four types of Permission Profiles:

- **None** indicates that the administrator cannot view the SmartEvent **Policy** tab.
- **Read Only** enables the administrator to view SmartEvent **Policy** tab.
- **Read/Write** enables the administrator to perform Install Policy and modify the SmartEvent **Policy** tab. With Read/Write permissions the administrator can also configure one or both of the following from within the **Events** tab:
  - **Exclude from Event Definition**
  - **Add Exception to Event Definition**
- **Customized** allows user-defined access to the selected Check Point products and select permissions per application

**Multi-Domain Security Management**

When using Multi-Domain Security Management, SmartEvent works with specified Domains. In the Policy tab, administrator can see events, exceptions and exclusions for Domains according to administrator permissions.

A Multi-Domain Security Management Policy administrator can be one of the following:

- Locally defined administrator on the SmartEvent Server
- Multi-Domain Server Super User defined on the Multi-Domain Server.
- An administrator with permissions to all Domains selected in SmartEvent (Policy > General Settings > Objects > Domains). Unlike the two above, this type of administrator can install a Policy and can view events that are cross-Domain (an event created from logs that come from multiple Domains).
Index

A
Adding Exclusions • 33
Adding Network and Host Objects • 34
Administrator Permission Profiles - Events and Reports • 24
Administrator Permissions Profile - Policy • 38
Automatic Report Scheduling • 28

B
Backup and Restore of the Database • 37
Basic Concepts and Terminology • 6
Browse Time • 17

C
Charts Tab • 20
Check Point Licenses • 7
Configuring Custom Commands • 36
Configuring Email Settings • 29
Configuring Reports • 27
Configuring SmartEvent to work with Multi-Domain Security Management • 8
Creating an External Script • 37
Creating Custom Queries • 10
Custom Queries • 9
Custom Reports • 27
Customizing Query Charts • 11
Customizing Query Filters • 10

D
Defining Correlation Units and Log Servers • 35
Defining the Internal Network • 35
Defining the Time Frame • 27
Details Tab • 16
Displaying Original Event Log Information • 31

E
Editing IPS Protection Details • 31
Enabling Connectivity with Multi-Domain Security Management • 8
Event Data Analysis • 17
Event Details • 16
Event Log • 12
Event Queries • 9
Event Query Results • 12
Event Statistics Pane • 16
Examining Client Vulnerability • 14
Exporting Events to a File • 14

F
Filtering Events • 13

G
Generating Reports • 30
Grouping Events • 13

I
Important Information • 3

M
Managing the Event Database • 37
Maps Tab • 23
Modifying the System General Settings • 34
Multi-Domain Security Management • 25, 38

O
Offline Log Files • 35
Organizing Queries in Folders • 11
Overview Tab • 17

P
Predefined Queries • 9
Predefined Reports • 26

R
Report Filters • 28
Reports • 26
Reports Tab • 24, 26

S
Sending an Event • 14
SmartEvent Sizing Guide • 6
Sorting and Searching Events • 13
Special Considerations for User Groups • 28
Summary Tab • 16
System Administration and Modifying Event Policy • 33

T
Timeline Tab • 19
Tracking Event Resolution using Tickets • 31

U
Using Custom Commands • 32

W
Working with Queries • 9

Initial Configuration • 7
Initial Configuration of the SmartEvent Client • 7
Installing the Network Objects in the SmartEvent Database • 8
Introduction to SmartEvent Intro • 6
Investigating Events • 31