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.

**Check Point R80**
For more about this release, see the R80 home page http://supportcontent.checkpoint.com/solutions?id=sk108623.

**Latest Version of this Document**
Download the latest version of this document http://supportcontent.checkpoint.com/documentation_download?ID=46507.
To learn more, visit the Check Point Support Center http://supportcenter.checkpoint.com.

**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 Views and Reports R80 Tutorial.

**Revision History**

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>18 September 2016</td>
<td>Updated numbering for Infographic (on page 25)</td>
</tr>
<tr>
<td>10 May 2016</td>
<td>Updated look and feel</td>
</tr>
<tr>
<td>13 January 2016</td>
<td>First release of this document</td>
</tr>
<tr>
<td>Section</td>
<td>Page</td>
</tr>
<tr>
<td>------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>Important Information</td>
<td>3</td>
</tr>
<tr>
<td>Introduction</td>
<td>5</td>
</tr>
<tr>
<td>Managing Views</td>
<td>7</td>
</tr>
<tr>
<td>Customization</td>
<td>7</td>
</tr>
<tr>
<td>View Settings</td>
<td>8</td>
</tr>
<tr>
<td>Export and Import</td>
<td>8</td>
</tr>
<tr>
<td>Save As PDF</td>
<td>8</td>
</tr>
<tr>
<td>Managing Reports</td>
<td>9</td>
</tr>
<tr>
<td>Customization</td>
<td>9</td>
</tr>
<tr>
<td>Customizing a Report</td>
<td>10</td>
</tr>
<tr>
<td>Automatic Report Updates</td>
<td>10</td>
</tr>
<tr>
<td>Adding a Logo to Reports</td>
<td>10</td>
</tr>
<tr>
<td>Export and Import</td>
<td>11</td>
</tr>
<tr>
<td>Generating a Report</td>
<td>11</td>
</tr>
<tr>
<td>Scheduling a Report</td>
<td>11</td>
</tr>
<tr>
<td>Generating a Network Activity Report</td>
<td>12</td>
</tr>
<tr>
<td>Search and Filters</td>
<td>14</td>
</tr>
<tr>
<td>Search Bar</td>
<td>14</td>
</tr>
<tr>
<td>Filters</td>
<td>15</td>
</tr>
<tr>
<td>Timeframe</td>
<td>16</td>
</tr>
<tr>
<td>Query Language Overview</td>
<td>16</td>
</tr>
<tr>
<td>Criteria Values</td>
<td>17</td>
</tr>
<tr>
<td>Wildcards</td>
<td>18</td>
</tr>
<tr>
<td>Field Keywords</td>
<td>18</td>
</tr>
<tr>
<td>Boolean Operators</td>
<td>19</td>
</tr>
<tr>
<td>Widgets</td>
<td>21</td>
</tr>
<tr>
<td>Adding and Customizing</td>
<td>21</td>
</tr>
<tr>
<td>Chart</td>
<td>23</td>
</tr>
<tr>
<td>Timeline</td>
<td>24</td>
</tr>
<tr>
<td>Table</td>
<td>24</td>
</tr>
<tr>
<td>Map</td>
<td>25</td>
</tr>
<tr>
<td>Infographic</td>
<td>25</td>
</tr>
<tr>
<td>Container</td>
<td>27</td>
</tr>
<tr>
<td>Rich Text</td>
<td>28</td>
</tr>
</tbody>
</table>
Introduction

Using rich and customizable views and reports, R80 introduces a new experience for log and event monitoring.

The new views are available from two locations:

- **SmartConsole > Logs & Monitor**
- **SmartView Web Application**. By browsing to: https://<Server IP>/smartview/
  
Where **Server IP** is IP address of the Security Management Server or SmartEvent server.

Catalog

In the Logs & Monitor view, clicking the (+) tab opens a catalog of all views and reports, predefined and customized. Click a view or report to open it.

1. **Opens Log View or Audit Logs View.**
   Use **Log View** to see and search through the logs from all Log Servers. You can also search the logs from a Log Server that you choose. You can also **Open Audit Logs View** to see records of actions done by SmartConsole administrators. Other views come from the SmartEvent Server.

2. **Views.**
   Shows a list of graphical widgets. Widgets represent predefined and customized views.
   Double-click a widget to drill down to a more specific view or raw log files. For more, see: Managing Views (on page 7).

3. **Reports.**
   Shows a list of predefined and customized reports. Report consists of multiple views. Reports can be customized, filtered, generated and scheduled. For more, see: Managing Reports (on page 9).

Use the **Favorites** view to collect the views and reports you use the most.

Connecting with SmartConsole to the Security Management Server lets you see all views and reports generated by SmartEvent, although SmartEvent can also reside on a separate server. Queries are forwarded to the SmartEvent Server, and the results shown in SmartConsole.
Note - In R80, the SmartEvent GUI client is still supported. Use it for initial setup and to define the SmartEvent Correlation Unit policy.

To open the SmartEvent GUI client:
1. Open SmartConsole > Logs & Monitor.
2. Click (+) for a new Catalog tab.
3. Click **SmartEvent Settings & Policy**.
Managing Views

In This Section:

- Customization .................................................................................................................7
- Export and Import ...........................................................................................................8
- Save As PDF ....................................................................................................................8

Views

A view is made up of graphical widgets. Double-click a widget to drill down to a more specific view or raw log file.

Customization

Customize your views according to these options:

Click Edit to switch to view edit mode.

SmartConsole saves an administrator’s customized views.

- To share a customized view with another administrator, use the Export and Import option ("Export and Import" on page 8).
- To customize a widget, see: Customizing Widgets ("Widgets" on page 21)
View Settings

1. Enter a title.
2. To show more results, this option allows a table to spread across multiple pages when saved to PDF.
   The **No page limit** option shows more results by spreading them across a number of pages.

Export and Import

To export the view layout and widget definitions to a file, use the *Export* option

To import the file from another server, or from another administrator, use the *Import* option in the Catalog (new tab).

Save As PDF

The Save as PDF option saves the current view as a PDF file, based on the defined filters and time frame.
Managing Reports

In This Section:

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customization</td>
<td>9</td>
</tr>
<tr>
<td>Automatic Report Updates</td>
<td>10</td>
</tr>
<tr>
<td>Adding a Logo to Reports</td>
<td>10</td>
</tr>
<tr>
<td>Export and Import</td>
<td>11</td>
</tr>
<tr>
<td>Generating a Report</td>
<td>11</td>
</tr>
<tr>
<td>Scheduling a Report</td>
<td>11</td>
</tr>
<tr>
<td>Generating a Network Activity Report</td>
<td>12</td>
</tr>
</tbody>
</table>

A report has multiple views. Report can be customized, filtered, generated and scheduled.

Customization

Customize your reports according to these options:

Click **Edit** to switch to the report edit mode.

To customize widgets, see: Customizing Widgets ("Widgets" on page 21)

SmartConsole saves an administrator’s customized reports. To share customized reports with other administrators, use the **Export** and **Import** options ("Export and Import" on page 11).
Report Settings

Reports can be configured according to these options:

![Report Settings](image)

**Customizing a Report**

1. Select a report from the Catalog (new tab).
2. Click Options > **Edit**.
3. Select the page to edit.
   
   You can also add or remove pages by clicking one of these:

   ![Page Editing Options](image)

5. Add a widget, or arrange widgets in the view: Drag & Drop or expand.
6. Define filters ("Search and Filters" on page 14).

**Note** -

- Use the timeframe to see how the report will look.
- The timeframe and search bar are not saved with the report definition. Define them as needed when generating the report (**Save as PDF**).

See: Generating a Report (on page 11)

Automatic Report Updates

SmartEvent automatically downloads new predefined reports and updates to existing predefined reports. To use this feature, the SmartEvent client computer must be connected to the Internet.

Adding a Logo to Reports

You can configure reports to show your company logo on report cover pages. The Check Point logo shows on report cover pages.

To add a logo to your reports:

1. Save your logo image as a PNG file with the name `cover-company-logo.png`. 
2. Copy the image to the $RTDIR/smartview/conf directory on the SmartEvent server.

Note: The best image dimensions are 152 pixels wide by 94 pixels high.

Export and Import

The Export option exports the view layout and widget definitions to a file. The file can be imported to another server, or imported by another administrator, using the Import option in the Catalog (new tab).

Generating a Report

1. Open the Catalog (new tab) and select a report.
2. Define the required timeframe and filter in the search bar ("Search and Filters" on page 14).
3. Click Options > Save As PDF.

Scheduling a Report

To schedule a report you need to define and edit it in the SmartEvent GUI client.

Note - Reports in the SmartEvent GUI client are different from reports in SmartConsole or the SmartView Web Application. To customize a report before scheduling, edit the report in the SmartEvent GUI client:

1. Open the Report tab
2. Select the report from the Report tree.
3. Click Edit.

To schedule a report:

1. Open SmartConsole > Logs & Monitor.
Managing Reports

2. Click the (+) to open a Catalog (new tab).
3. Click the **SmartEvent Settings & Policy** link.
4. In the SmartEvent GUI client, select **Schedule**.

The Schedule and Email settings configuration window opens.

5. Click **Add**, and select a schedule.
6. Select **Active** for the schedules you want to activate.
7. **Optional**: Click **Email Settings**.
8. Select **Send By Email**, and configure email settings to get the schedule report automatically.

---

**Generating a Network Activity Report**

The **Network Activity** report shows important firewall connections. For example, top sources, destinations, and services. To create this report, SmartEvent must first index the firewall logs.

**To enable the Network Activity Report:**

1. Open SmartConsole > Logs & Monitor.
2. Click the (+) to open a Catalog (new tab).
3. Click the **SmartEvent Settings & Policy** link.
4. In the SmartEvent GUI client > **Policy** tab, select and expand **Consolidated Sessions**.

5. Select **Firewall Session**.
   
   **Note** - this configuration increases the number of events per day by about five times. To avoid a performance impact, make sure the hardware can handle the load.

   To configure SmartEvent on a dedicated server, see the SmartEvent sizing guide
Search and Filters

In This Section:

- Search Bar .................................................................................................................... 14
- Filters ............................................................................................................................ 15
- Timeframe ..................................................................................................................... 16
- Query Language Overview ............................................................................................ 16

This section covers the search bar and filters in Views and Reports.

Search Bar

The search bar lets you:

- Search for a string value in all fields.
- Search in one field, for example all logs that have a specified IP in the Source.

The search applies to all widgets in the view / report.

You can automatically enter query text into the search bar by right clicking a value in the widget and selecting Filter or Filter Out.
In the Log View, click the **Favorites** button to open the predefined queries.

For more on queries, see: Query Language Overview [on page 16]

### Filters

The search bar is used to apply on-demand filters, but you can also save filters with the view / report definition.
There are different layers of filters:
1. Filters to apply to the full report.
2. Filters to apply to a view, or a specified page in a report and all widgets that this page includes.
3. Filters to apply to the selected widget.

**Edit View Filter**

1. Click the + (plus) button to add a filter.
   To delete a filter, click the X button.
2. Select a field.
   To enable free text search, select Custom Filter.
3. Select a comparison method.
4. Select or enter the value.
   You can define multiple values, separated by a comma.

**Timeframe**

Select one of these time frames:

You can also define a time range.

**Query Language Overview**

SmartEvent includes a powerful query language that lets you show only selected records from the log files, according to your criteria. You can create complex queries with Boolean operators, wildcards, fields, and ranges. This section is a detailed reference to the SmartEvent query language.
When you use the SmartEvent GUI to create a query, the applicable criteria show in the **Query Definition** field.

The basic query syntax is:

```
[<Field>:] <filter_criterion>
```

You can put together many criteria in one query with Boolean operators:

```
[<Field>:] <filter_criterion> AND|OR|NOT [Field:] <Filter_Criterion> ...
```

Query keywords and filter criteria are not case sensitive.

Most query keywords and filter criteria are not case sensitive, but there are some exceptions. For example, **Risk:High** is case sensitive (**Risk:high** will not match). If your query results do not show the expected results, change the case of your query criteria or try both upper and lower case.

**Note:** When you use queries with more than one criteria value, you must explicitly enter a Boolean operator.

### Criteria Values

Criteria values are written as one or more text strings. You can enter one text string, such as a word, IP address or URL, without delimiters. Phrases or text strings that contain more than one word must be surrounded by quotation marks.

**One word string examples:**

- John
- inbound
- 192.168.2.1
- mahler.ts.example.com
- dns_udp

**Phrase examples**

- "John Doe"
- "Log Out"
- "VPN-1 Embedded Connector"

### IP Addresses

IPv4 addresses used in SmartEvent queries are counted as one word. You can enter IPv4 address using dotted decimal notation. You can also use the `*` wildcard character with IPv4 addresses.

**Example:**

- 20.20.20.1

### NOT Values

You can use NOT `<field>` values with field keywords in SmartEvent queries to find events for which the field has no value.

**Syntax**

```
NOT <field>
```
Wildcards

You can use the standard wildcard characters (*) and ?) in queries to match variable characters or strings in log records. The wildcard character cannot be the first character in a query criterion. You can use more than wildcard character in query criteria.

Wildcard syntax

- The ? (question mark) matches one character in a string.
- The * (asterisk) matches zero or more characters in a string.

Examples:

- Jo* shows Jo, John, Jon, Joseph, Joshua, and so on.
- Jo? shows Joe and Jon, but not Joseph.

If your criteria value contains more than one word, you can use the wildcard in each word. For example, ‘Jo* N*’ shows Joe North, John Natt, Joshua Named, and so on.

Using Wildcards with IP Addresses

The * wildcard character can represent digits in IPv4 addresses. You can only use the wildcard character for one or more full octets in the address. It must be preceded by the dot character. For example, 192.168.* is legal, but 192.168.2* is not.

Examples:

- 192.168.2.* shows all records for 192.168.2.0 to 192.168.2.255 inclusive
- 192.168.* shows all records for 192.168.0.0 to 192.168.255.255 inclusive

Field Keywords

You can use predefined field names, followed by a colon, as keywords in filter criteria. SmartEvent only shows log records that match the criteria in the specified field. If you do not use field names, SmartEvent shows records that contain the criteria in all fields.

This table shows the predefined field keywords. Some fields also support keyword aliases that you can type as alternatives to the primary keyword.

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Keyword Aliases</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>severity</td>
<td></td>
<td>Severity of the event</td>
</tr>
<tr>
<td>risk</td>
<td></td>
<td>Potential risk from the event</td>
</tr>
<tr>
<td>protection</td>
<td></td>
<td>Name of the protection</td>
</tr>
<tr>
<td>protection_type</td>
<td></td>
<td>Type of protection</td>
</tr>
<tr>
<td><strong>Keyword</strong></td>
<td><strong>Keyword Aliases</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>------------</td>
<td>--------------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>confidence</td>
<td></td>
<td>Level of confidence that an event is malicious</td>
</tr>
<tr>
<td>action</td>
<td></td>
<td>Action taken by a security rule</td>
</tr>
<tr>
<td>blade</td>
<td>product</td>
<td>Software Blade</td>
</tr>
<tr>
<td>destination</td>
<td>dst</td>
<td>Traffic destination IP address, DNS name or Check Point network object name</td>
</tr>
<tr>
<td>origin</td>
<td></td>
<td>Name of originating Security Gateway</td>
</tr>
<tr>
<td>service</td>
<td></td>
<td>Service that generated the log entry</td>
</tr>
<tr>
<td>source</td>
<td>src</td>
<td>Traffic source IP address, DNS name or Check Point network object name</td>
</tr>
<tr>
<td>user</td>
<td></td>
<td>User name</td>
</tr>
</tbody>
</table>

The syntax for a field name query is: `<field_name>:<values>`

- `<field_name>` - One of the predefined field names
- `<values>` - One or more filter criteria

**Examples:**

- `source:192.168.2.1`
- `action:(Reject OR Block)`

You can use the OR Boolean operator in parentheses to include multiple criteria values.

**Boolean Operators**

You can use Boolean operators in queries. The available Boolean operators are:

- AND
- OR
- NOT

**Notes:**

- When you work with queries that have multiple criteria values, you must explicitly write the Boolean operator.
- You must use parentheses when using multiple criteria.

**Examples:**

- `blade:"application control" AND action:block` - Shows log records from the Application Control and URL Filtering Software Blade where traffic was blocked.
- `192.168.2.133 10.19.136.101` - Includes log entries that match the two IP addresses. The **AND** operator is presumed.
• **192.168.2.133 OR 10.19.136.101** - Includes log entries that match one of the IP addresses.

• **(blade:Firewall OR blade:IPS OR blade:VPN) AND NOT action:drop** - Includes all log entries from the Firewall, IPS or VPN blades that are not dropped. The criteria in the parentheses are applied before the **AND NOT** criterion.

• **Source:(192.168.2.1 OR 192.168.2.2) AND destination:17.168.8.2** - Includes log entries from the two source IP addresses if the destination IP address is **17.168.8.2**. This example also shows how you can use Boolean operators with field criteria.
Widgets

In This Section:

Adding and Customizing........................................................................................................21
Chart........................................................................................................................................23
Timeline....................................................................................................................................24
Table.........................................................................................................................................24
Map..........................................................................................................................................25
Infographic.............................................................................................................................25
Container...............................................................................................................................26
Rich Text...............................................................................................................................28

To customize widgets, switch to edit mode. Click on Options > Edit.

• To save changes, click Done.
• To cancel changes, click on Discard.
• To restore the predefined view to the default values, click Options > Restore Defaults.

Adding and Customizing

To add a Widget:

1. Add a widget
2. Select a widget type:
   Chart (on page 23)
   Timeline (on page 24)
   Table (on page 24)
   Map (on page 25)
   Infographic (on page 25)
   Container (on page 26)
   Rich Text (on page 28)

To customize a widget:

1. Drag and drop the widget within the view.
2. Select the graphic presentation that best fits the information you want to see.
3. Select filters for the widget in addition to the inherited filters from the report and view layers. (See: Filters (on page 15)).
4. Configure settings for the widget.
5. Delete a widget.
6. Resize widget.
Chart

1. Enter a title.
2. Select a chart type: vertical bar, horizontal bar, pie, area or line.
3. Select a data category for the X axis.
4. Define how the Top Values are calculated (by number of logs, or by traffic).
5. Set a limit for how many top values to show.
6. Optional: click Series - split the results into colored groups with different values for the series.

7. Optional: click Customize and define axis titles and legend position.
Timeline

1. Enter a title.
2. Select a timeline graphical presentation: vertical bar, doughnut, area or line.
3. Select the data to count.
4. Advanced - split the results into colored groups, with different values for the Series.
5. Define the time-granularity. Enter the number of bars or doughnuts to show.

Table

1. Enter a title.
2. Manage columns: add, edit, remove, and change the order.
3. Select a column on the left and define its settings:
   - Enter the number of top values to show.
   - Select how values are sorted.
4. Select this option to group results with the same value in one row.

Map

1. Enter a title.
2. Enter the number of Top Countries to mark.
3. Select to mark Top Source Countries, Top Destination Countries, or both.
4. Define how to find the Top Countries (for example, by number of logs or by traffic).

Infographic

The infographic widget shows large meaningful values. For example:

Configure an infographic using these settings:
1. Enter a title

2. Select a field to count. Selecting **None** means all the logs that match the filter criteria are counted.

3. Define filter criteria.
   This criteria is in addition to the inherited filters for the report and view layers.
   For more, see Filters (on page 15).

4. Optional: Enter an icon name in the field.
   Select a name from the list below. Pay attention to upper and lower case letters and the use of hyphens.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Used for</th>
</tr>
</thead>
<tbody>
<tr>
<td>apps</td>
<td></td>
</tr>
<tr>
<td>attacks</td>
<td></td>
</tr>
<tr>
<td>hosts</td>
<td></td>
</tr>
<tr>
<td>Gateway</td>
<td></td>
</tr>
<tr>
<td>traffic</td>
<td></td>
</tr>
<tr>
<td>usercheck</td>
<td></td>
</tr>
<tr>
<td>users</td>
<td></td>
</tr>
<tr>
<td>new</td>
<td>Audit Logs</td>
</tr>
<tr>
<td>add</td>
<td>Audit Logs</td>
</tr>
<tr>
<td>remove</td>
<td>Audit logs</td>
</tr>
<tr>
<td>modify</td>
<td>Audit logs</td>
</tr>
<tr>
<td>install-policy</td>
<td></td>
</tr>
<tr>
<td>publish</td>
<td></td>
</tr>
<tr>
<td>ips</td>
<td></td>
</tr>
<tr>
<td>anti-bot</td>
<td></td>
</tr>
<tr>
<td>anti-virus</td>
<td></td>
</tr>
<tr>
<td>threat-emulation</td>
<td></td>
</tr>
</tbody>
</table>

5. Enter primary text that describes the value counted.

6. Optional: For secondary text, enter a more detailed description.
Container

Use a container to unify multiple widgets into one frame. Add a container, then add, edit, or remove the widgets inside it.

**Note** - The container widget cannot be added to a container.

1. Enter a title.
2. Optional: filter at the container level. The filter applies to all internal widgets.
3. Select the widget order inside the container: Horizontal, Vertical, Grid or Tabs.

After the container is added to the view, you can configure it further.

1. Remove the widget from the container.
2. Add a new widget.
3. Edit the settings for the container, or edit one of the widgets in the list.
Rich Text

Use this window to add textual explanations to the View text box.