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 NGSE and R80**

For more about the NGSE release, and to download the latest hotfixes, see sk98767 http://supportcontent.checkpoint.com/solutions?id=sk98767.

SmartEvent R80 replaces NGSE. We recommend that you install R80. You can manage an R80 SmartEvent Server with an R77.x Security Management Server. See sk110894 http://supportcontent.checkpoint.com/solutions?id=sk110894.

**Latest Version of this Document**

Download the latest version of this document http://supportcontent.checkpoint.com/documentation_download?ID=40644.

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 SmartEvent NGSE Release Notes and Getting Started Guide.

**Revision History**

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>13 April 2016</td>
<td>SmartEvent R80 replaces NGSE. We recommend that you install R80. You can manage an R80 SmartEvent Server with an R77.x Security Management Server. See sk110894 (&quot;SmartEvent R80&quot; on page 6).</td>
</tr>
<tr>
<td>13 October 2015</td>
<td>Changes to installation procedures.</td>
</tr>
<tr>
<td>10 September 2015</td>
<td>Added installation instructions for appliances with Gaia R77.30 (or higher), R75.47, and SmartEvent NGSE (on page 7). Updated the instructions for enabling the Network Activity report:</td>
</tr>
<tr>
<td></td>
<td>• Connecting SmartEvent NGSE to a Security Management Server (on page 9).</td>
</tr>
<tr>
<td></td>
<td>• Connecting SmartEvent NGSE to the Multi-Domain Server (on page 10).</td>
</tr>
<tr>
<td></td>
<td>Corrected a file path (&quot;Importing Offline Log Files&quot; on page 12)</td>
</tr>
<tr>
<td>Date</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>30 June 2015</td>
<td>Added procedure for importing logs that are older than 90 days (&quot;Importing Offline Log Files&quot; on page 12).</td>
</tr>
<tr>
<td>1 June 2015</td>
<td>Updated Importing Offline Log Files (on page 12)</td>
</tr>
<tr>
<td>19 April 2015</td>
<td>Updated the prerequisites for Installation (on page 7)</td>
</tr>
<tr>
<td>23 March 2015</td>
<td>Added Troubleshooting (on page 25)</td>
</tr>
<tr>
<td>16 March 2015</td>
<td>First release of this document</td>
</tr>
</tbody>
</table>
Contents

Important Information ................................................................................................... 3
Introduction to SmartEvent NGSE .............................................................................. 6
SmartEvent R80 ........................................................................................................ 6
What’s New in NGSE ................................................................................................. 6
System Requirements ............................................................................................... 7
Installation .................................................................................................................... 7
Connecting SmartEvent NGSE to a Security Management Server ......................... 9
Connecting SmartEvent NGSE to the Multi-Domain Server .................................... 10
Configuring Dedicated Correlation Units ................................................................. 11
Upgrading a Public EA Server to GA ....................................................................... 11
Importing Offline Log Files ..................................................................................... 12
Configuring Disk Space Management .................................................................... 13
Changing the Default LEA Port ............................................................................... 13
Smart Search .............................................................................................................. 15
Query Language Overview ....................................................................................... 16
Criteria Values ........................................................................................................ 16
IP Addresses ............................................................................................................. 17
NOT Values .............................................................................................................. 17
Wildcards ................................................................................................................ 17
Using Wildcards with IP Addresses ....................................................................... 17
Field Keywords ....................................................................................................... 18
Boolean Operators .................................................................................................. 19
Next Generation Reporting ....................................................................................... 19
Importing and Exporting Reports .......................................................................... 20
Automatic Report Updates ..................................................................................... 20
Adding a Logo to Reports ....................................................................................... 20
Defining Custom Reports ......................................................................................... 21
Defining the Report Outline and Filters .................................................................. 21
Defining Views ....................................................................................................... 21
Defining Widgets ................................................................................................... 22
Increasing the Maximum Rows Per Table ............................................................. 23
Filtering Reports by User Groups .......................................................................... 24
Known Limitations .................................................................................................. 25
Troubleshooting ...................................................................................................... 25
Introduction to SmartEvent NGSE

Next Generation SmartEvent shows real-time network activity in customized views and reports. Customized views let you monitor activities that are most important to you. Personalized reports let you quickly inform key stakeholders about security activities related to their work. Next Generation SmartEvent empowers you with quick data and easy priorities for incident response.

Next Generation SmartEvent delivers large data threat detection in seconds. You can move from a high level view to detailed forensic analysis in one click. With the free-text search and suggestions, you can quickly run data analysis and identify critical security events from the clutter. You can collect, process, and search billions of logs in seconds.

This guide contains documentation for the new features and functionality in SmartEvent NGSE. To learn more about SmartEvent and its existing feature set, see R77 SmartEvent Administration Guide.

SmartEvent R80

SmartEvent R80 replaces NGSE. We recommend that you install R80. You can manage an R80 SmartEvent Server with an R77.x Security Management Server. See sk110894 http://supportcontent.checkpoint.com/solutions?id=sk110894.

What's New in NGSE

The NGSE version of SmartEvent allows you to enjoy the new capabilities SmartEvent before the release of R80. SmartEvent NGSE servers can be upgraded to R80 after it is released.

Enhanced Speed and Scale

- Get results for filtering, searching and report-generating in seconds
- Analyze hundreds of millions of logs per day

Smart Search

- Free-text search on all logs and events, with auto-suggest and favorites

Next Generation Reporting

- Fully customizable graphical reports that you create with a rich and interactive GUI
- New predefined reports with a modern look and feel that answer most common security requirements
- Automatic report updates from the cloud and export/import report functionality
System Requirements

For the system requirements, see the sizing guide on the SmartEvent NGSE home page sk98767

Installation

Prerequisites:

- Dedicated server for SmartEvent NGSE that is connected to a management server.
- You must do a clean installation. But you can do an upgrade from the NGSE Public Early Availability (EA).
- If you have an old SmartEvent NGSE client installed on your computer, uninstall it before you install the new SmartEvent NGSE client.
- Connection to management server (Security Management Server or Multi-Domain Server) version R75.40 or higher.

To install SmartEvent NGSE on Smart-1 205, 210, 225, 3050, and 3150 appliances:

For appliances that have these predefined images:

- Gaia R77.30 (or higher)
- Gaia R75.47
- Gaia SmartEvent-NGSE

Follow these instructions:

1. Select the default SmartEvent-NGSE image on the appliance.
2. Follow the instructions in the First Time Configuration Wizard to configure a dedicated SmartEvent Server.
   Make sure that the /var/log partition is the largest partition.

For appliances that have these predefined images:

- Gaia R77.10 or Gaia R77.20
- Gaia R75.47
- SecurePlatform R75.47
- Gaia SmartEvent-NGSE

The default NGSE image on the appliance is an old version. Follow these instructions to update the NGSE image on the appliance to the latest version:

1. Select the default SmartEvent-NGSE image on the appliance.
   Follow the instructions in the First Time Configuration Wizard to configure a dedicated SmartEvent Server.
   Make sure that the /var/log partition is the largest partition.
2. Install the SmartEvent NGSE appliance package:
   a) Download:
      Check_Point_Hotfix_NGSE_Smart-1_2xx_3xxx.tgz
Installation

b) Copy this file to the SmartEvent server and extract the installation file:
   # gtar xzvf Check_Point_Hotfix_NGSE_Smart-1_2xx_3xxx.tgz

c) Run:
   # ./ReportingServer_HOTFIX_GULLI_HF_RAPHAEL_002_990008157_1

d) Follow the instructions on the screen.

3. Install the SmartEvent NGSE General Availability (GA) package:
   a) Download:
      Check_Point_Hotfix_NGSE.tgz
   b) Copy this file to the SmartEvent server and extract the installation file:
      # gtar xzvf Check_Point_Hotfix_NGSE.tgz
   c) Run:
      # ./ReportingServer_HOTFIX_GULLI_HF_RAPHAEL_004_901001057_1
   d) Follow the instructions on the screen.

4. After the installation completes, run:
   # cpstart

5. Download and install Check_Point_SmartConsole_NGSE.exe on your SmartEvent GUI client computer.
   **Note**: Do not download the SmartConsole clients from the Gaia Web UI.

To install SmartEvent NGSE on Open Server platforms and other Smart-1 models:

1. Download: Check_Point_NGSE.iso

   Make sure that the /var/log partition is the largest partition.

3. After the First Time Configuration Wizard completes, run:
   # cpstart

4. Download and install Check_Point_SmartConsole_NGSE.exe on your SmartConsole client computer.
Connecting SmartEvent NGSE to a Security Management Server

To configure SmartEvent NGSE to connect to a Security Management Server:

1. Connect SmartEvent NGSE to your Security Management Server.
   a) In SmartDashboard, create a new R77 Check Point host object.
   b) Establish SIC trust with the SmartEvent NGSE server.
   c) On the Management tab, enable:
      - Logging & Status blade
      - SmartEvent blade
      - SmartEvent Correlation Unit
      
      **Note:** SmartEvent NGSE supports a connection to a management server earlier than R77. In this case, define the SmartEvent host with the latest possible version.

2. Install the database on your production Log Servers:
   
   **SmartDashboard Menu > Policy > Install Database**
   
   This action lets the Log Server identify the SmartEvent NGSE server and send logs to it.
   
   **Important:** Do **not** install the database on the SmartEvent NGSE server, because the database is automatically synchronized with the Management Server. However, if the Management Server version is R77 or R77.x with no add-ons, it is safe to install the database.

3. Go to **SmartEvent Policy tab > Correlation Units** and double-click a Correlation Unit object.

4. Select the production Log Servers and the local Log Server (on the SmartEvent server).

5. **Optional:**
   
   The **Network Activity** report gives information about Firewall connections. For example, top sources, destinations, and services. To create this report, SmartEvent must make an index of the Firewall logs.
   
   To enable this report, on the SmartEvent **Policy** tab, select and enable **Consolidated Sessions > Firewall Session**
   
   **Note:** This configuration increases the number of events per day by about 5 times. This may have a performance impact. To make sure the hardware can handle the load, see the sizing guide on the SmartEvent NGSE home page
   

6. Install the SmartEvent Policy on the Correlation Unit:
   
   **SmartEvent menu > Actions > Install Event Policy**
   
   **Note:** For more details about connecting SmartEvent to a Security Management Server, see the **R77 SmartEvent Administration Guide**
   
Connecting SmartEvent NGSE to the Multi-Domain Server

You can connect SmartEvent NGSE to one or more Domains in a Multi-Domain Security Management environment. To connect to one Domain, use the procedure for connecting to a Security Management Server ("Connecting SmartEvent NGSE to a Security Management Server" on page 9).

To connect SmartEvent NGSE to more than one Domain:

1. Connect the SmartEvent NGSE to the Multi-Domain Server:
   a) In the Global SmartDashboard, create a new R77 SmartEvent network object.
   b) Establish SIC trust.
   c) On the Management tab, enable:
      - Logging & Status blade
      - SmartEvent blade
      - SmartEvent Correlation Unit

   **Note:** SmartEvent NGSE supports a connection to a management server earlier than R77. In this case, define the SmartEvent host with the latest possible version.

2. In SmartDomain Manager, assign the Global Policy to all Domains that use SmartEvent NGSE.

3. For each Domain that uses SmartEvent NGSE, install the database on the production Log Servers.
   a) Connect to the Domain SmartDashboard.
   b) Select **Menu > Policy > Install Database.**
      This lets the Log Server identify the SmartEvent NGSE server and send logs to it.

   **Important:** Do not install the database on the SmartEvent NGSE server, because the database is automatically synchronized with the Management Server. However, if the Management Server version is R77 or R77.x with no add-ons, it is safe to install the database.

4. Go to the SmartEvent **Policy tab > Domains** and select the Domains to read logs from.

5. Go to **SmartEvent Policy tab > Correlation Units** and double-click a Correlation Unit object.

6. Select the production Log Servers and the local Log Server (on the SmartEvent server).

7. Optional:
   The **Network Activity** report gives information about Firewall connections. For example, top sources, destinations, and services. To create this report, SmartEvent must make an index of the Firewall logs.
   To enable this report, on the SmartEvent **Policy tab**, select and enable **Consolidated Sessions > Firewall Session**

   **Note:** This configuration increases the number of events per day by about 5 times. This may have a performance impact. To make sure the hardware can handle the load, see the sizing guide on the SmartEvent NGSE home page

8. Install the SmartEvent Policy on the Correlation Unit:
   **SmartEvent menu > Actions > Install Event Policy**
Configuring Dedicated Correlation Units

You can install a SmartEvent NGSE Correlation Unit on a dedicated server.

**Note:** Configuration of dedicated Correlation Units are only supported for management versions R77.x

To configure a dedicated Correlation Unit:

1. In SmartDashboard (Global SmartDashboard for Multi-Domain Security Management), create a new R77 Correlation Unit network object.
   a) Establish SIC trust.
   b) Enable the Logging & Status Blade.
   c) Enable the Correlation Unit.
2. If you are using a Multi-Domain Security Management deployment, assign the Global Policy to all Domains that use SmartEvent NGSE.
3. Install the database on your production Log Servers and the Correlation Unit:
   - **SmartDashboard Menu > Policy > Install Database**
     This action lets the log server identify the Correlation Unit and send logs to it.
     **Important:** Do not install database on the SmartEvent NGSE server.
4. Go to the SmartEvent Policy tab > Correlation Units, double-click the new Correlation Unit object.
5. Select the production Log Servers and the local Log Server for the Correlation Unit.
6. Install the Event Policy on the Correlation Unit:
   - **SmartEvent Menu > Actions > Install Event Policy**

Upgrading a Public EA Server to GA

You can easily upgrade a SmartEvent NGSE Public Early Availability (EA) server to this General Availability (GA) release. The upgrade procedure saves all log data and settings.

To upgrade a Public EA Server to GA:

1. Run:
   ```
   # cpstop
   ```
2. Download: `Check_Point_Hotfix_NGSE.tgz`
3. Copy this file to the SmartEvent server and extract the installation file:
   ```
   # gtar xzvf Check_Point_Hotfix_NGSE.tgz
   ```
4. Run:
   ```
   # ./ReportingServer_HOTFIX_GULLI_HF_RAPHAEL_004_901001057_1
   ```
   Follow the instructions on the screen.
5. After the installation completes, run:
   ```
   # cpstart
   ```
6. Uninstall the existing NGSE SmartConsole.
7. Download and install Check_Point_SmartConsole_NGSE.exe on your SmartEvent GUI client computer.

Importing Offline Log Files

You can add events to the SmartEvent NGSE server by importing offline log files. By default, you can import the 14 most recent days of offline logs. To import more days of logs, you must first change the log indexing settings.

To change log indexing settings:

**Note** - Do this to make it possible to import logs that are older than the last 14 days.

1. Run: `# evstop`
2. Edit the log settings file `smartlog_settings.txt`
   a) Make a backup. Run this command:
      ```
      cp $RTDIR/smartlog/smartlog_settings.txt
      $RTDIR/smartlog/smartlog_settings.txt_orig
      ```
   b) Edit `$RTDIR/smartlog/smartlog_settings.txt` in a text editor and delete these lines:
      ```
      :time_restriction_for_fetch_all (<existing_data>)
      :time_restriction_for_fetch_all_disp (<existing_data>)
      ```
3. Edit the log settings file `smartlog_settings.conf`
   a) Make a backup. Run this command:
      ```
      cp $RTDIR/smartlog/conf/smartlog_settings.conf
      $RTDIR/smartlog/conf/smartlog_settings.conf_orig
      ```
   b) Edit `$RTDIR/smartlog/conf/smartlog_settings.conf` and change the number of days of log entries to import:
      ```
      :num_days_restriction_for_fetch_all_integrated (<days>)
      ```
      `<days>` is the last number of days of logs to be indexed by the SmartEvent server. For example, to import and index logs from the last 30 days of logs, give a value of 30.
      **Note** - To reduce the performance impact while indexing the offline logs, we recommend that you import only the number of days of logs that you need.
4. The default database maintenance setting is to delete events older than 90 days. This releases disk space for new events. To import logs that are older than 90 days, change this setting. Note that storing more days of events increases the size of the event database.
   a) Make a backup of the database maintenance setting file `maintenanceConfig.xml`. Run this command:
      ```
      cp $RTDIR/conf/maintenanceConfig.xml
      $RTDIR/conf/maintenanceConfig.xml_orig
      ```
   b) Edit the file `$RTDIR/conf/maintenanceConfig.xml` and change the number of days of events to keep. In this section, change `day="90"` to the required number of days, in two places:
      ```
      <category name="other">
      ```
5. Run: `# evstart`

To import offline log files to the SmartEvent NGSE server:

1. Copy the log files and related pointer files (`.log`, `.logptr`, `.logaccount_ptr`, `.loginitial_ptr`) to `$FWDIR/log` on the SmartEvent Server.

### Configuring Disk Space Management

The NGSE Correlation Unit creates Events as logs on the local Log Server. The SmartEvent Server indexes these logs.

We recommend that you configure the **Disk Space Management** parameters to delete old log entries when the available disk space is 45% or less.

⚠️ **Important** - This procedure applies to the raw log files. It has no effect on the events database, which uses an internal disk space management policy.

To configure Disk Space Management:

1. In SmartDashboard, double-click the SmartEvent host object.
2. Go to **Logs > Storage**.
3. Set the **Measure free disk space** parameter to **Percentage**.
4. Set the **When disk space is below - start deleting old log files** parameter to 45%.

### Changing the Default LEA Port

The SmartEvent server and Correlation Unit connect to the Log Server and use the LEA protocol to read logs. By default, the Log Server uses port 18184 for this connection. If you configured the Log Server to use a different LEA port, you must manually configure the new port on the SmartEvent server and on the Correlation Unit.

Before changing the default LEA port on the NGSE server, make sure that the new LEA port that is configured on the Log Server is in authenticated mode. On the Log Server, open the file `$FWDIR/conf/fwopsec.conf`, and make sure it has this line:

```
lea_server auth_port <new_port_number>
```

If the line does not exist, contact Check Point Support.
To change the default LEA port on the NGSE server:

1. On the SmartEvent NGSE server, open
   
   \$RTDIR/smartlog/conf/smartlog_settings.conf
   
   in a text editor.

2. Add this line anywhere in the file:
   
   lea_port (<new_port_number>)

3. In the SmartEvent client, go to Policy tab > Correlation Units:
   
   Make sure that you configure the Correlation Unit to read logs from the local Log Server (on the SmartEvent NGSE server).

4. Go to Policy tab > Network Objects:
   
   a) Double-click the SmartEvent object
   b) Change the LEA port No. parameter to <new_port_number>.

5. Install the Event Policy on the Correlation Unit:
   
   Actions > Install Event Policy

6. On the SmartEvent NGSE server, run: > cpstop

7. Open \$FWDIR/conf/fwopsec.conf in a text editor and change these parameters:
   
   lea_server auth_port <new_port_number>

8. On the SmartEvent NGSE server, run: > cpstart
Overviews:
The Overview tab shows top events for all types. If you manage a specific area of protection, you can go directly to the data of that area.

Click the tab for events filtered by Software Blade:

- Application and URL Filtering
- Threat Prevention (IPS, Anti-Bot, Anti-Virus, and Threat Emulation)
- DLP

Drill down forensics:
Double-click a result in a pane (such as an IP address or a user name). The other Overview panes are filtered based on your selection. The search bar shows the filter applied to the events. For example, if you click one of the Top Sources, the search bar shows: src: "<ip_address>".

Quickly search the database of logs and events:
Use Search Suggestions and Recent Searches. Click in the search bar to see the search suggestions and your recent searches. The search is fast, and gets results from the entire events database.

For example, to see only critical events from 192.168.2.15:
1. Click in the Search bar, and select Severity in the Suggestions list.
2. In the list of valid values that shows, click Critical.
3. Click in the Search bar, and select Source in the Suggestions list.
4. If the IP address you want is not in the list, enter it in the search bar.
   The data in all the panes is updated to match your search.

Free Text Search Query using the SmartLog Syntax:
For more sophisticated searching, you can do AND/OR searches with the Query Syntax.

Filter for quick standard results:
Click Filters to select a standard filter option. For example, in Application and URL Filtering, you can filter to see only events of Application Control or only events of URL Filtering. You can filter for Action, to see events for Blocked or Allowed traffic.
Query Language Overview

SmartEvent NGSE 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 NGSE query language.

When you use the SmartEvent NGSE GUI to create a query, the applicable criteria show in the Query Definition field.

The basic query syntax is:

\[\text{[<Field>:]} \ <\text{filter\_criterion}>\]

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

\[\text{[<Field>:]} \ <\text{filter\_criterion}> \ \text{AND|OR|NOT} \ [\text{<Field>:}] \ <\text{Filter\_Criterion}> \ \ldots\]

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 NGSE 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 NGSE queries to find events for which the field has no value.

Syntax
NOT <field>

Example
NOT src:10.0.4.10

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 NGSE only shows log records that match the criteria in the specified field. If you do not use field names, SmartEvent NGSE 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>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 the 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.

Next Generation Reporting

You can use predefined graphical report templates for the most frequently seen security issues. Try these before you create a customized report.

To generate a predefined report:

1. Open the **Reports** tab.
2. Choose a **Default Report** for a Software Blade.
3. Click **Generate**
4. In the **Generate a Report** window, choose a time period.
5. Click **Generate**.

Your reports are saved in the **Report History**.

To schedule a predefined or custom report for generation and email:

1. In the tree, click **Settings**.
2. Configure your email server and the email addresses of the people who should get the report.
3. In the SmartEvent menu, click **File > Save**.
4. Select a report.
5. Click **Schedule** (top of the workspace).
6. In the window that opens, configure when the report is to be automatically generated.
   You can configure multiple dates and times. For example, you can generate a report daily and monthly.
7. In Email Settings, click **Send By Email**.

**Importing and Exporting Reports**

The **Export** option exports the view layout and widget definitions to a file. You can import the file to another server, or by another administrator, when you use the **Import** option in the Catalog (new tab).

To export a report:
1. On the SmartEvent **Reports** tab, right-click a report on the navigation tree and select **Export**.
2. Enter the report file name and path.

To import a report:
1. Copy the report file to your SmartEvent GUI client computer.
2. On the SmartEvent **Reports** tab, right-click a report on the navigation tree and select **Import**.
3. Select the report file to import.
   The report is automatically imported to the correct section of the tree.

**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.
Defining Custom Reports

You can define all aspects for a new report type.

**To define custom reports for your organization:**

1. In the Reports tab, select a predefined or custom report.
2. Click Edit.
3. In the Save Report window, enter a name for this report.
4. Change the properties of the report as shown below.
5. Click Save.

Defining the Report Outline and Filters

When you edit a report, the workspace shows Views on the left. A view is a section of the report, which typically shows on one page. If the view includes a table, it can show on more than one page.

The View pane on the left has management controls:

- To add a view, click Add - adds a view.
- To remove a view, click Remove.
- To change the sequence of views, click the arrows.
- To set a filter for data included in this report:
  a) Click the Edit Report Filter icon.
  b) Select a field, a comparability operator, and a value.
  c) Click the +.

You can add as many filters as necessary. A filter on this level is for the full report. This filter is inherited by each view (section of data) and each widget (data representation). If no data is found for a new widget, change the filters.

Defining Views

You can change an existing view, add a new View, or delete a view. Changes to views apply only to the custom report that you work on.

When you click a View thumbnail, the View opens in the main pane. You can see the widgets that this view includes. Each widget is contained in a panel, with management options.

- To add a widget to a view, click Add Widget.
- To remove a widget from the view, click the X on the widget panel.
- To move a widget in the view, drag the widget’s top panel bar.
- To resize a widget in the view, click and drag the lower-right corner.
  **Note** - You cannot resize or move a widget out of the page borders.
- To change the view title, click View Settings > Title and enter a heading for this report section.
- To set data filters that apply to all widgets in the view, click View Filter.
• Click **Show Inherited Filters**, to see the filters set on the full report.
• To show table layouts across more than one page:
  a) Click **View Settings**.
  b) Click **Split table across multiple pages**.
  c) Select **Show all table rows**.
     The table takes up as many pages as necessary to show the generated table.
     Alternatively, select **Limit selected table**, and enter the maximum number of pages.

### Defining Widgets

Widgets are a representation of the collected data. There can be different combinations of types, fields, operations, groups, filters, and settings for each widget. You can quickly create the graphical view of security in your organization that best meets your requirements.

The view must have sufficient space to contain the widget to add. If the space is not sufficient, an error message shows.

**To create a new widget:**
1. In a view, click **Add Widget**.
2. Enter a caption.
3. Select a type:
   • **Chart** - A graphical representation of data statistics.
   • **Timeline** - A chart with the time already deployed in best-effort layout as the X axis.
   • **Table** - A fitted table of columns and rows.
   • **Map** - A chart that shows events that occur in different parts of the world.
4. Click **Create**.
   The **Chart Settings**, **Timeline Settings**, or **Table Settings** window opens.
5. Click **OK** in this window.
   The data is generated on the fly.
6. To change the configuration of the widget, click **Settings** on the widget panel.

**To define a chart or timeline:**
1. In **General**, select the type of chart: area, horizontal bar, vertical bar, pie, or line.
2. Select a field for the **Category (X)**.
   In a timeline, this option is not available. The X axis is automatically the distributed dates or times, according to the number of **Samples** that you enter.
3. Select a field for the **Value (Y)**.
4. In **Category (X)**, define the X axis of a chart:
   • Enter a title.
   • Enter the number of categories to show (**Top 10** is default).
   • In **Ordered by**, select a field that shows the best grouping of data.
     **Important** - You can change the representation of the data. Therefore, make sure that you select a field that accurately shows the situation.
5. In **Value (Y)**, set the maximum value. For charts, you can set the **Function** to **Count** or **Sum**.

6. For three-dimensional data, select a field for **General > Series**.
   This color-codes the chart, to show how the third field is represented in the values of the category. For example, in a bar chart with **X = Application Name and Y = Sessions (Count)**, you add **Series = Application Risk**. Each bar can have multiple colors. The sections in-color show the number of sessions for which different countries were the source of used applications. If you add a series to a widget, make sure there is a **Legend** (shows by default), or the colors will not be useful.

7. To change the **Legend position**, select **Chart Settings > Display**.
   You can configure the statistics grouping of the series in the **Series** page.

**To define a table:**

1. Add fields, which become the table columns.

2. To select how statistics are grouped:
   a) Click **Group results by this column**.
   b) Select an option.

3. To select the aggregation of data:
   a) Click **Advanced > Aggregate values by**.
   b) Select an option.

4. To sort fields and show a summary row:
   a) Select a column.
   b) Click **Advanced**.
   c) Select the **Group results by this column** option.
   d) Select the column to sort from the **Sort by** list.
   e) Select the **Show Summary Row** option.

5. To change the column title:
   a) Select a column.
   b) Click **Advanced**.
   c) Select **Custom caption**.
   d) Enter a column name in the applicable field.

**Increasing the Maximum Rows Per Table**

By default, reports can show up to 2000 rows in a table. You can use this procedure to increase the maximum number of rows in a report table.

**Note:** Reports with very long tables can cause a heavy load on the SmartEvent NGSE server. We recommend that you do not use more than one column for "**Group By**" in long tables.

**To change the maximum rows per table:**

1. Run: `> evstop`
2. Open: `$RTDIR.smartview/conf/connections.xml` in a text editor.
3. Change the integer value in the `<groupByLimit>2000</groupByLimit>` parameter to the new value. This is a global setting that sets the maximum number of rows in all reports.

4. Run: `> evstart`

You can now change your report tables to show up to the new maximum number of rows.

### Filtering Reports by User Groups

You can filter based on User Groups.

To enable this feature, you must first do initial configuration steps.

**To configure SmartEvent for user group filtering:**

1. In SmartDashboard, define an Access Role object that includes User Groups to use for SmartEvent reports.
2. Install policies on the Security Gateways.

**To generate reports filtered by user groups:**

1. On the SmartEvent **Reports** tab, select a report.
2. Click **Generate**.
3. Select the **User Group** filter.
4. Select a one or more groups.
5. Click **Generate**.

The generated report is based on users mapped to the selected groups.

**To define a scheduled report filtered by user groups:**

1. Generate a report filtered by the specified User Group.
2. Copy the full User Group name from the generated report cover page. The User Group name typically starts with the prefix "ad_".
3. Define new custom report:
   a) Right-click on an existing report.
   b) Select **Save As**.
   c) Right-click the new report.
   d) Select **Edit**.
   e) Click the **Filter** icon.
   f) Define a User Group filter.
      The **Filter** icon is on the toolbar, above the report page selection area.
   g) Make sure that you accurately enter (or paste) the User Group name that you copied in step 2.
   h) Save the report.
4. Generate the new custom report.
5. Make sure that the filter works as expected.

**Note:** In the **Generate a Report** window, make sure that the User Group filter is defined as **Any**.
6. Click Schedule.
7. Configure the days and times that this custom report runs automatically.

## Known Limitations

For the list of known limitations, see the SmartEvent NGSE home page sk98767

## Troubleshooting

To collect debug information from a SmartEvent Server:

1. Collect debug log files of all processes, query history, and the status of the SmartEvent Server.
   Run:
   
   
   ```
   $RTDIR/bin/SmartEventCollectLogs --system_stats -d /var/log/
   ```

2. Send the output file `/var/log/AllSmartEvent.out.tgz` to Check Point Support.

### Advanced Troubleshooting

To get more detailed debug information, use the `SmartEventSetDebugLevel` command.

1. Collect detailed debug log files for one process or all processes. Run:
   ```
   SmartEventSetDebugLevel {cu|rfl|server|wd|smartview|solr|all} {trace|debug|info|warn|error|fatal|off}
   ```
   For example, run:
   ```
   SmartEventSetDebugLevel smartview debug
   ```

### Process Table

<table>
<thead>
<tr>
<th>Process</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cu</td>
<td>Correlation Unit process</td>
</tr>
<tr>
<td>rfl</td>
<td>RFL query manager process</td>
</tr>
<tr>
<td>server</td>
<td>SmartEvent Server process</td>
</tr>
<tr>
<td>wd</td>
<td>WatchDog process</td>
</tr>
<tr>
<td>smartview</td>
<td>Web application for report customization process</td>
</tr>
<tr>
<td>solr</td>
<td>Index database process</td>
</tr>
<tr>
<td>all</td>
<td>All processes</td>
</tr>
</tbody>
</table>

### Debug Level Table

<table>
<thead>
<tr>
<th>Debug Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>trace</td>
<td>The most verbose debug level</td>
</tr>
<tr>
<td>off</td>
<td>No debug logging</td>
</tr>
</tbody>
</table>

2. Reproduce the problem.
3. Collect all debug log files. Run:
   ```
   $RTDIR/bin/SmartEventCollectLogs --system_stats -d /var/log/
   ```
4. Send the output file `/var/log/AllSmartEvent.out.tgz` to Check Point Support.