QUANTUM

04 July 2024

LOGGING AND MONITORING

R80.40

Administration Guide

CHECK POINT™

Check Point Copyright Notice

© 2020 - 2024 Check Point Software Technologies Ltd.

All rights reserved. This product and related documentation are protected by copyright and distributed under licensing restricting their use, copying, distribution, and decompilation. No part of this product or related documentation may be reproduced in any form or by any means without prior written authorization of Check Point. While every precaution has been taken in the preparation of this book, Check Point assumes no responsibility for errors or omissions. This publication and features described herein are subject to change without notice.

RESTRICTED RIGHTS LEGEND:

Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 and FAR 52.227-19.

TRADEMARKS:

Refer to the Copyright page for a list of our trademarks.

Refer to the Third Party copyright notices for a list of relevant copyrights and third-party licenses.

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.



Certifications
For third party independent certification of Check Point products, see the Check Point Certifications page.



Check Point R80.40
For more about this release, see the R80.40 home page.



Latest Version of this Document in English
Open the latest version of this document in a Web browser.
Download the latest version of this document in PDF format.



Feedback
Check Point is engaged in a continuous effort to improve its documentation.
Please help us by sending your comments.

Revision History

Date	Description
08 April 2024	Updated *"Working with Syslog Servers" on page 91*
19 November 2023	Updated *"Log Exporter Advanced Configuration in CLI" on page 184*
14 November 2023	Updated *Log Actions*

Date	Description
08 August 2023	Updated *"Selecting Query Fields" on page 83*
25 July 2023	Updated *Gateway Status*
26 June 2023	Updated *"Log Exporter" on page 180*
21 February 2023	Updated Daily Logs Retention section in *"Understanding Logging" on page 18*
14 February 2023	Updated "reconf" command in *"Log Exporter Advanced Configuration in CLI" on page 184*
05 January 2023	Updated: ■ *"Tracking Options" on page 77*
19 December 2022	Updated: ■ *"Log Exporter Advanced Configuration in CLI" on page 184*
17 October 2022	Updated: ■ *"Log Exporter Basic Configuration in CLI" on page 182* ■ *"Log Exporter Advanced Configuration in CLI" on page 184*
24 July 2022	Updated: ■ *"Understanding Logging" on page 18*
14 June 2022	In the HTML version, added glossary terms in the text
26 April 2022	Added limitations to: ■ *"SmartView Web Application" on page 74* ■ *"Showing Query Results" on page 81*
05 January 2022	Added limitations to: ■ *"Understanding Logging" on page 18* ■ *"Monitoring Traffic or System Counters" on page 166* ■ *"Using the Logs View" on page 72* ■ *"Transition from LEA to Log Exporter" on page 221*
29 December 2021	Updated: ■ *"SmartView Web Application" on page 74*

Date	Description
11 May 2021	Updated: ■ *"Widgets" on page 57*
7 February 2021	Updated: ■ *"Showing Query Results" on page 81*
07 January 2021	Updated: ■ *"Monitoring VPN Tunnels" on page 162* ■ *"Widgets" on page 57*.
26 October 2020	Updated: ■ *"Adding a Logo to Reports" on page 56*
19 February 2020	Updated: ■ *"Query Language Overview" on page 86* - "Wildcards"
04 February 2020	Updated: ■ *"Working with Syslog Servers" on page 91*
13 January 2020	First release of this document

Table of Contents

Introduction to Logging and Monitoring ... *16*

Getting Started ... *17*

Logging and Monitoring Clients ... *17*

Understanding Logging ... *18*

Log Storage ... *20*

Daily Logs Retention ... *24*

Log Receive Rate ... *29*

Deploying Logging ... *29*

Enabling Logging on the Security Management Server ... *30*

Deploying a Dedicated Log Server ... *30*

Configuring the Security Gateways for Logging ... *30*

Enabling Log Indexing ... *31*

Disabling Log Indexing ... *31*

Deploying SmartEvent ... *32*

SmartEvent Licensing ... *32*

Enabling SmartEvent on the Security Management Server ... *32*

System Requirements ... *33*

Installing a Dedicated SmartEvent Server ... *33*

Configuring the SmartEvent Components in the First Time Configuration Wizard ... *33*

Connecting R80.40 SmartEvent to R80.40 Security Management Server ... *34*

Advanced Configuration for a dedicated SmartEvent Server that is also a Correlation Unit ... *34*

Connecting R80.40 SmartEvent to R77.X Security Management Server ... *35*

Connecting R80.40 SmartEvent to R80.40 Multi-Domain Server ... *36*

Connecting R80.40 SmartEvent to R77.X Multi-Domain Server ... *37*

Configuring SmartEvent to use a Non-Standard LEA Port ... *38*

Configuring SmartEvent to read External Logs ... *39*

Administrator Permission Profiles ... *39*

Configuring Permissions for Monitoring, Logging, Events, and Reports ... 40
Multi-Domain Security Management ... 40
SmartEvent Reports-Only Permission Profile ... 41
Importing Offline Log Files ... 41
Importing Log Files from SmartEvent Servers ... 42
Offline Work For Correlated Events ... 42
Importing Syslog Messages ... 44
Generating a Syslog Parser and Importing syslog Messages ... 44
Configuring SmartEvent to Read Imported Syslog Messages ... 44
Views and Reports ... 45
Enabling Views and Reports ... 45
Catalog of Views and Reports ... 45
Views ... 46
Reports ... 47
Automatic View and Report Updates ... 48
Opening a View or Report ... 48
Exporting Views and Reports ... 48
Generating a Network Activity Report ... 49
Sharing Reports ... 50
Exporting and Importing Templates ... 51
Scheduling a View or Report ... 52
Customizing a View or Report ... 53
View Settings ... 53
Report Settings ... 55
Configuring Email Settings for Views and Reports ... 55
Configuring Email Server Settings ... 55
Configuring Email Recipients ... 56
Adding a Logo to Reports ... 56
Widgets ... 57
Adding and Customizing Widgets ... 57

Copying Widgets and Views to other Locations ... 67
Filters ... 70
Filtering for Active Directory User Groups ... 71
Logging ... **72**
Sample Log Analysis ... 72
Using the Logs View ... 72
SmartView Web Application ... 74
Working with Logs ... 76
Choosing Rules to Track ... 76
Configuring Tracking in a Policy Rule ... 77
Tracking Options ... 77
Log Sessions ... 78
Viewing Rule Logs ... 79
Packet Capture ... 80
Searching the Logs ... 80
Running Queries ... 81
Showing Query Results ... 81
Customizing the Results Pane ... 82
Creating Custom Queries ... 83
Selecting Query Fields ... 83
Using the Action Filter ... 83
Selecting Criteria from Grid Columns ... 86
Manually Entering Query Criteria ... 86
Query Language Overview ... 86
Criteria Values ... 87
IP Addresses ... 87
NOT Values ... 88
Wildcards ... 88
Field Keywords ... 88
Boolean Operators ... 90

Log Server High Availability ... 91
Working with Syslog Servers ... 91
Introduction ... 91
Configuring Security Gateways ... 91
Log Count for CoreXL Firewall Instances ... 95
Event Analysis ... **97**
Event Analysis with SmartEvent ... 97
What is an Event? ... 97
How Are Logs Converted to Events? ... 97
The SmartEvent Architecture ... 97
SmartEvent Correlation Unit ... 99
SmartEvent Correlation Unit High Availability ... 99
Configuring SmartEvent Policy and Settings ... 99
Opening the SmartEvent GUI Client ... 99
Policy Tab ... 100
Save Event Policy ... 100
Revert Changes ... 100
Event Definitions and General Settings ... 101
Event Definition Parameters ... 101
Modifying Event Definitions ... 101
Event Threshold ... 102
Severity ... 102
Automatic Reactions ... 102
Creating a Mail Reaction ... 104
Creating an SNMP Trap Reaction ... 104
Creating a Block Source Reaction ... 105
Creating a Block Event Activity Reaction ... 105
Creating an External Script Automatic Reaction ... 105
Assigning an Automatic Reaction to an Event ... 107
Creating a Mail Reaction ... 107

Creating an SNMP Trap Reaction ... 108
Creating a Block Source Reaction ... 108
Creating a Block Event Activity Reaction ... 108
Creating an External Script Automatic Reaction ... 109
Assigning an Automatic Reaction to an Event ... 110
Working Hours ... 111
Exceptions ... 111
High Level Overview of Event Identification ... 112
Matching a Log Against Global Exclusions ... 112
Matching a Log Against Each Event Definition ... 112
Creating an Event Candidate ... 113
Matching a Log Against Event Exclusion ... 116
Event Generation ... 117
Creating a User-Defined Event ... 117
Creating a New Event Definition ... 117
Customizing a User-Defined Event ... 119
Eliminating False Positives ... 121
Services that Generate Events ... 121
Common Events by Service ... 121
System Administration ... 131
Adding Network and Host Objects ... 131
Monitoring Traffic and Connections ... 133
How SmartView Monitor Works ... 133
AMON Protocol Support ... 134
Defining Status Fetch Frequency ... 134
To Start Monitoring ... 135
SmartView Monitor Features ... 135
SmartView Monitor Use Cases ... 136
Immediate Actions ... 136
Monitoring and Handling Alerts ... 137

Viewing Alerts 137
System Alert Monitoring Mechanism 137
Monitoring Suspicious Activity Rules 138
The Need for Suspicious Activity Rules 138
Creating a Suspicious Activity Rule 138
Creating a Suspicious Activity Rule from Results 140
Managing Suspicious Activity Rules 140
sam_alert 141
Configuring Alerts and Thresholds in SmartView Monitor 141
System Alerts and Thresholds 141
Working with SNMP Monitoring Thresholds 143
Types of Alerts 143
Configuring SNMP Monitoring Thresholds 143
Configuration Procedures 145
Configure Global Alert Settings 145
Configure Alert Destinations 146
Configure Thresholds 146
Completing the Configuration 147
Monitoring SNMP Thresholds 147
Customizing Results 149
Editing a Custom View 149
Creating a Custom Gateway Status View 149
Creating a Custom Traffic View 150
Creating a Custom Counters View 151
Creating a Custom Tunnel View 152
Creating a Custom Users View 152
Custom View Example 153
Exporting a Custom View 154
Setting Your Default View 154
Refreshing Views 154

Monitoring Device Status ... 155
Device Status ... 155
Displaying Gateway Data ... 156
System Information ... 156
Firewall ... 157
Virtual Private Networks ... 157
QoS ... 159
ClusterXL ... 159
OPSEC ... 159
Check Point Security Management ... 159
SmartEvent Correlation Unit and the SmartEvent Server ... 160
Anti-Virus and URL Filtering ... 161
Multi-Domain Security Management ... 161
The cpstat Command ... 161
Starting and Stopping Cluster Members ... 162
Monitoring VPN Tunnels ... 162
VPN Tunnels Solution ... 162
VPN Tunnel View Updates ... 163
Running VPN Tunnel Views ... 163
Run a Down Tunnel View ... 164
Run a Permanent Tunnel View ... 164
Run a Tunnels on Community View ... 164
Run Tunnels on Gateway View ... 165
Monitoring Traffic or System Counters ... 166
Traffic or System Counters Solution ... 166
Traffic ... 166
Traffic Legend Output ... 167
System Counters ... 167
Select and Run a Traffic or System Counters View ... 168
Recording a Traffic or Counter View ... 168

Play the Results of a Recorded Traffic or Counter View ... 169
Pause or Stop the Results of a Recorded View that is Playing ... 169
Monitoring Users ... 169
Users Solution ... 170
Run a Users View ... 170
Run a User View for a Specified User ... 170
Run a User View for all Users or Mobile Access Users ... 171
Run a User View for a Specified Security Gateway ... 171
Cooperative Enforcement Solution ... 171
NAT Environments ... 172
Configuring Cooperative Enforcement ... 172
Non-Compliant Hosts by Gateway View ... 173
Third-Party Log Formats ... **174**
Importing Syslog Messages ... 174
Generating a Syslog Parser and Importing syslog Messages ... 174
Configuring SmartEvent to Read Imported Syslog Messages ... 174
Importing Windows Events ... **176**
How Windows Event Service Works ... 176
Administrator Support for WinEventToCPLog ... 176
Sending Windows Events to the Log Server ... 177
Creating an OPSEC Object for Windows Event Service ... 177
Configuring the Windows service ... 177
Establishing Trust ... 178
Configuring the Windows Audit Policy ... 178
Working with SNMP ... 179
Log Exporter ... **180**
Overview ... 180
How Log Exporter Works ... 181
Configuring Log Exporter in CLI ... 182
Log Exporter Basic Configuration in CLI ... 182

Log Exporter Advanced Configuration in CLI ... 184
Log Exporter TLS Configuration ... 204
Log Exporter Advanced Configuration Parameters ... 207
Log Exporter Instructions for Specific SIEM ... 217
Rsyslog ... 217
ArcSight ... 217
Splunk ... 219
QRadar ... 220
Transition from LEA to Log Exporter ... 221
Transition from CPLogToSyslog to Log Exporter ... 223
Log Exporter - Appendix ... 224
Special Log Fields ... 224
Syslog-NG Listener Configuration ... 224
Splunk Listener Configuration ... 225
ArcSight Listener Configuration ... 226
QRadar Log Event Extended Format (LEEF) Mapping ... 228
Command Line Reference ... 229
Appendix: Manual Syslog Parsing ... 230
Planning and Considerations ... 230
The Parsing Procedure ... 231
Manual Syslog Parsing ... 232
The Free Text Parsing Language ... 234
The Commands ... 234
Try ... 235
Group_try ... 236
Switch ... 237
Unconditional_try ... 238
Include ... 239
Add_field ... 239
Dictionary ... 245

The Parsing Procedure 246

Glossary ***247***

Introduction to Logging and Monitoring

From R80, logging, event management, reporting, and monitoring are more tightly integrated than ever before. Security data and trends easy to understand at a glance, with Widgets and chart templates that optimize visual display. Logs are now tightly integrated with the policy rules. To access logs associated with a specific rule, click that rule. Free-text search lets you enter specific search terms to retrieve results from millions of logs in seconds.

One-click exploration makes it easy to move from high-level overview to specific event details such as type of attack, timeline, application type and source. After you investigate an event, it is easy to act on it. Depends on the severity of the event, you can ignore it, act on it later, block it immediately, or toggle over to the rules associated with the event to refine your policy. Send reports to your manager or auditors that show only the content that is related to each stakeholder.

In this release, SmartReporter and SmartEvent functionality is integrated into SmartConsole.

With rich and customizable views and reports, R80 introduced a new experience for log and event monitoring.

The new views are available from two locations:

- **SmartConsole > Logs & Monitor**
- **SmartView Web Application**. Browse to: *https://<Server IP Address>/smartview/*

  Where *Server IP Address* is IP address of the Security Management Server or SmartEvent Server.

Getting Started

This section introduces the logging and monitoring clients, and explains how to install and configure logging and monitoring products.

Logging and Monitoring Clients

Monitor logs and events using customizable views and reports. Use these GUI clients:

GUI Client	Description
SmartConsole > Logs & Monitor	Analyze events that occur in your environment with customizable views and reports. The **Logs** view replaces the SmartView Tracker and SmartLog GUI clients.
SmartView Web Application	It has the same real-time event monitoring and analysis views as SmartConsole, with the convenience of not having to install a client. Browse to: `https://<Server IP>/smartview/`, where `<Server IP>` is IP address of the Security Management Server or SmartEvent Server.

These GUI clients are still supported:

GUI Client	Description
SmartEvent	■ For initial settings - configure the SmartEvent Correlation Unit, Log Server, Domains and Internal Network. ■ For the correlation policy (event definitions) ■ For Automatic Reactions
SmartView Monitor	■ To monitor tunnels ■ To monitor users ■ For suspicious activity rules ■ To monitor alerts - Thresholds configuration For more about monitoring, see *"Monitoring Traffic and Connections" on page 133*.

SmartView GUI Clients

Administrator access permissions can be limited by the GUI Clients list based on IP address, IP range, a network or a host name.This list is based on the GUI clients' access configuration as defined on the relevant Security Management Server or a Multi-Domain Server.

See the *R80.40 Security Management Administration Guide* > Chapter *Managing Administrator Accounts* > Section *Defining Trusted Clients*.

To open the SmartEvent GUI:

1. Open **SmartConsole** > **Logs & Monitor**.
2. Click (**+**) for a Catalog (new tab).
3. In the External Apps section, click **SmartEvent Settings & Policy**.

To open the SmartView Monitor GUI:

1. Open **SmartConsole** > **Logs & Monitor**.
2. Click (**+**) for a Catalog (new tab).
3. In the External Apps section, click **Tunnel & User Monitoring**.

Understanding Logging

Security Gateways / Cluster Members generate network logs, and the Management Server generates audit logs, which are a record of actions taken by administrators. The Security Policy that is installed on each Security Gateway / Cluster determines which rules generate logs.

Logs can be stored on a:

- Management Server that receives logs from the managed Security Gateways / Clusters. This is the default.
- Log Server on a dedicated machine. This is recommended for organizations that generate a lot of logs.
- Security Gateways / Cluster Members. This is called local logging.

Note - Logs can be automatically forwarded to the Security Management Server or Log Server, according to a schedule, or manually imported with the Remote File Management operation via CLI (with the "`fw fetchlogs`" command). The management servers and log servers can also forward logs to other servers.

To find out how much storage is necessary for logging, see the *R80.40 Release Notes*.

A Log Server handles log management activities:

- Automatically starts a new log file when the existing log file gets to the defined maximum size.
- Stores log files for export and import.
- Makes an index of the logs to enable faster responses to log queries.

Notes:

- SmartLog Indexing mode is not enabled by default after upgrade or new installation, on Smart-1 205, Smart-1 210, or Open Servers with less than 4 cores.
- To change SmartLog mode from Indexing to Non-Indexing on a Domain Management Server or Domain Log Server, edit the Domain Server object on the Domain level. There is no option to change the entire Multi-Domain Server or Multi-Domain Log Server to Non-Indexing mode.

An administrator can configure Backup Log Servers:

- If all Primary Log Servers are disconnected, the Security Gateway / Cluster starts to send logs only to the first configured Backup Log Server.
- If the first Backup Log Server is also disconnected, the Security Gateway / Cluster sends logs to the second configured Backup Log Server, and so on.

Log Storage

SmartEvent Server and Log Server use an optimization algorithm to manage disk space and other system resources. When the Logs and Events database becomes too large, the server automatically deletes the oldest logs and events based on the configured thresholds.

Procedure for a Management Server / SmartEvent Server / Log Server

1. Connect with SmartConsole to the Management Server.
2. From the left navigation panel, click **Gateways & Servers**.
3. Open the object of the Management Server / SmartEvent Server / Log Server.
4. From the left tree, go to **Logs** > **Storage**.

   Note - The **Logs** section appears only if you enabled the **Logging & Status** Software Blade on the **General Properties** page > **Management** tab.

5. In the **Disk Management** section, configure these settings:

Field	Description / Instructions
Measure free disk space in	Select **MBytes** or **Percentage**.
When disk space is below <number> Mbytes, issue alert <type>	Get an alert when the available disk space for logs and log index files is below this threshold. This value must be at least 5 MB greater than the value in the **When disk space is below <number> Mbytes, stop logging** field on the **Additional Logging Configuration** page.
When disk space is below <number> Mbytes, start deleting old files	Delete the oldest logs and log index files when the available disk space is below this threshold. The server examines the available space in the log partition every 1 minute. When the threshold is reached, the log disk maintenance occurs- deleting the **oldest day** of log and index data and repeating until reaching the available space above the configured threshold. This value must be at least 5 MB greater than the value in the **When disk space is below <number> Mbytes, issue alert <type>** field on this page.
Run the following script before deleting old files	Enter an absolute path to the shell script (path and the file name). This shell script must exist on the server.

6. In the **Daily Logs Retention Configuration** section, configure these settings:

   For more information, see *"Daily Logs Retention" on page 24*.

   First, select **Apply the following logs retention policy**.

Field	Description / Instructions
Keep indexed logs for no longer than <number> days	Occurs daily at midnight. Deleting oldest index files by **days**, keeping today + the configured number of index days (14 = 14 days + today).
Keep log files for an extra <number> days	Occurs daily at midnight. Deleting oldest log files by days, keeping today + the configured number of index days + extra log days (3664 = 14 [from index settings] + 3650 days + today). As 3664 is more than 10 years, effectively keeping all log files.

   Note - The maximum total value of both indexed logs and log files is 3664 days.

7. Click **OK**.
8. Publish the SmartConsole session.
9. Install the database (click **Menu** > **Install database** > select all server objects > click **Install**)

Procedure for a Security Gateway / Cluster

1. Connect with SmartConsole to the Management Server.
2. From the left navigation panel, click **Gateways & Servers**.
3. Open the object of the Security Gateway / Cluster.
4. From the left tree, go to **Logs** > **Storage**.
5. In the **Disk Management** section, configure these settings:

Field	Description / Instructions
Measure free disk space in	Select **MBytes** or **Percentage**.

Field	Description / Instructions
When disk space is below <number> Mbytes, issue alert <type>	Get an alert when the available disk space for logs and log index files is below this threshold. This value must be at least 5 MB greater than the value in the **When disk space is below <number> Mbytes, stop logging** field on the **Additional Logging Configuration** page.
When disk space is below <number> Mbytes, start deleting old files	Delete the oldest logs and log index files when the available disk space is below this threshold. The server examines the available space in the log partition every 1 minute. When the threshold is reached, the log disk maintenance occurs- deleting the **oldest day** of log and index data and repeating until reaching the available space above the configured threshold. This value must be at least 5 MB greater than the value in the **When disk space is below <number> Mbytes, issue alert <type>** field on this page.
Run the following script before deleting old files	Enter an absolute path to the shell script (path and the file name). This shell script must exist on the server.
Reserve <number> <units> for packet capturing	Some types of logs can also capture the packets that created the log event. Set the amount, in megabytes or percent, that you want to use for captured packets.

6. In the **Daily Logs Retention Configuration** section, configure these settings:

   For more information, see *"Daily Logs Retention" on page 24*.

   First, select **Apply the following logs retention policy**.

Field	Description / Instructions
Keep indexed logs for no longer than <number> days	Occurs daily at midnight. Deleting oldest index files by **days**, keeping today + the configured number of index days (14 = 14 days + today).

Field	Description / Instructions
Keep log files for an extra <number> days	Occurs daily at midnight. Deleting oldest log files by days, keeping today + the configured number of index days + extra log days (3664 = 14 [from index settings] + 3650 days + today). As 3664 is more than 10 years, effectively keeping all log files.

Note - The maximum total value of both indexed logs and log files is 3664 days.

7. Click **OK**.
8. Publish the SmartConsole session.
9. Install the Access Control policy on the Security Gateway / Cluster object.

Examples

For these examples, the administrator enables these thresholds:

- **When disk space is below [5000] Mbytes, start deleting old files**
- **Daily logs retention**
  - **Keep indexed logs for 14 days**
  - **Keep log files for an extra 6 days** (6 + 14 = *20* days of log files)

Example	Description
1	The server has 3000 MBytes of free disk space, and 5 days of logs and index files. The server deletes logs and index files, one day at a time, until there is 5000 Mbytes of free disk space.
2	The server has 10 GBytes of free disk space and 30 days of logs and index files. The server deletes all log files older than 20 days ago (6 + 14), each day at midnight. The server deletes all index files older than 14 days ago, each day at midnight.

Example	Description
3	A server produces 1GB of logs and 1GB of index files each day. The server now has 35 days of logs and 30 days of index files and only 2.5GB of free disk space left. The configured disk space threshold is 5GB, which means the server is now 2.5GB below the threshold. The index files threshold is 14 days. The log file threshold is 20 days. When the disk space threshold (5GB) is reached, disk space maintenance deletes logs and index data until there is again more than 5GB of free space. In this example: 1. Logs from day one are deleted first, as they are older. Three days of the oldest logs are deleted to clear 3GB of logs and leave 6GB of free space on the drive, 1GB above the threshold, leaving the server with 32 log days and 30 index days. 2. The server still has more than 14 days of index files - an extra 16 days (30 days of index files now) And more than 20 days of logs – an extra 12 days (32 days of log files now). At midnight, the extra log & index files are deleted until only the current day's log files plus the last 20 days remain. Index days are deleted until only the current day's index plus the last 14 days remain. The deletion of three days of logs left 5.5GB of free space. The deletion of 12 log file days + 16 index file days frees up a total of 28GB (12 + 16) of space. 33.5GB of space is now free. The daily logs retention occurs every day at midnight keeping the chosen number of days of log + index data. Most likely, this means it will never reach the log disk space threshold. But if the log disk space threshold is again reached, the log disk maintenance process repeats to make sure space never runs out.

Daily Logs Retention

In R80.40 and higher, daily logs retention refers to how long logs are stored before they are deleted. Configure this value to help you manage free disk space.

The Management Server does **not** delete **audit log files**, even in a case of emergency disk space maintenance, regardless of the configured log retention value. You cannot configure the daily retention for the Management Server audit logs.

The Management Server does **not** delete **audit indexes** as part of daily maintenance regardless of the value configured in SmartConsole. The Management Server deletes audit log indexes (not the log files) only in a disk space emergency. In a Multi-Domain environment, you can change this behavior only for the Global SmartEvent Server in the `log_maintenance_domain_conf.csv` file (see the corresponding section below).

Note - The server deletes old logs daily at midnight.

Important - The server can apply the **"Daily Logs Retention Configuration"** only when **"When disk space is below <number> Mbytes, start deleting old files"** is enabled. To control this behavior, see sk176803.

You can configure log retention policy on different servers:

Configuring daily logs retention for a Security Management Server / dedicated SmartEvent Server / dedicated Log Server

1. Connect with SmartConsole to the applicable server:
   - Security Management Server if managed Security Gateways send their logs to it
   - Security Management Server that manages the dedicated SmartEvent Server or dedicated Log Server
2. From the left navigation panel, click **Gateways & Servers**.
3. Open the object of the Management Server / dedicated SmartEvent Server / dedicated Log Server.
4. From the left tree, go to **Logs** > **Storage**.
5. In the section **Daily Logs Retention Configuration**:
   a. Select **Apply the following logs retention policy**.
   b. In the field **Keep indexed logs for no longer than <number> days**, configure the required number of days.
   c. In the field **Keep log files for an extra <number> days**, configure the required number of days.

      Notes:
      - When this value is 0, the servers keeps the indexed logs and the log files for the same number of days.
      - If you configure a value greater than 0, the server keeps the log files for the **additional** configured number of days (after the configured number of days for indexed logs).

   Note - The maximum total value of both indexed logs and log files is 3664 days.
6. Click **OK**.

7. Publish the SmartConsole session.
8. Install the database (click **Menu** > **Install database** > select all server objects > click **Install**).

Configuring daily logs retention in a Multi-Domain environment - for all Domain Management Servers / Domain Log Servers

Notes:

- Only Super User can configure these settings.
- This configuration applies to all Domain Management Servers and Domain Log Servers that are not configured explicitly (see the corresponding section).
- The daily index deletion on the Multi-Domain Server / Multi-Domain Log Server is enforced based on the greatest value configured between the Domain and the Multi-Domain Server levels.

1. Connect with SmartConsole to the applicable Multi-Domain Server / Multi-Domain Log Server to the **MDS** context.
2. From the left navigation panel, click **Multi-Domain** > **Domains**.
3. In the table, locate the column for this Multi-Domain Server / Multi-Domain Log Server.
4. Right-click the cell for this Multi-Domain Server / Multi-Domain Log Server and click **Edit**.

   The **Multi-Domain Server** window opens.
5. From the left tree, go to **Log Settings** > **General**.
6. In the section **Daily Logs Retention Configuration**:
   a. Select **Apply the following logs retention policy**.
   b. In the field **Keep indexed logs for no longer than <number> days**, configure the required number of days.
   c. In the field **Keep log files for an extra <number> days**, configure the required number of days.

      Notes:
      - When this value is 0, the servers keeps the logs and the indexed logs for the same number of days.
      - If you configure a value greater than 0, the server keeps the logs for the additional configured number of days.

   Note - The maximum total value of both indexed logs and log files is 3664 days.
7. Click **OK**.
8. Publish the SmartConsole session.

Configuring daily logs retention in a Multi-Domain environment - for a specific Domain Management Server / Domain Log Server

Notes:

- Only Super User can configure these settings.
- By default, all Domain Management Servers use the settings a Super User configured in the Multi-Domain Server / Multi-Domain Log Server object.
- The Multi-Domain Server / Multi-Domain Log Server deletes a log index only when no Domains use this log index.
  For example, if you configured one Domain to keep its log index for 5 days and another Domain to keep its log index for 30 days, then the server deletes the log index only after 30 days.

1. Connect with SmartConsole to the applicable Domain Management Server.
2. From the left navigation panel, click **Gateways & Servers**.
3. Open the object of the Domain Management Server / Domain Log Server.
4. From the left tree, go to **Logs** > **Storage**.
5. In the section **Daily Logs Retention Configuration**:
   a. Select **Override Multi-Domain Settings**.
   b. In the field **Keep indexed logs for no longer than <number> days**, configure the required number of days.
   c. In the field **Keep log files for an extra <number> days**, configure the required number of days.

      Notes:
      - When this value is 0, the servers keeps the logs and the indexed logs for the same number of days.
      - If you configure a value greater than 0, the server keeps the logs for the additional configured number of days.

   Note - The maximum total value of both indexed logs and log files is 3664 days.
6. Click **OK**.
7. Publish the SmartConsole session.
8. Install the database (click **Menu** > **Install database** > select all server objects > click **Install**)

Configuring daily logs retention in a Multi-Domain environment - for a Global SmartEvent Server

You must configure the required settings only in the corresponding configuration file:

Settings	Configuration File	Comment
General settings that apply to all Domain Management Servers that use this Global SmartEvent Server	`log_policy_extended.C`	See sk117317
Settings that apply to only to a specific Domain Management Server that uses this Global SmartEvent Server	`log_maintenance_domain_conf.csv`	See below

Note - If you do not configure settings explicitly, then the default values apply.

To configure settings for specific Domain Management Servers:

1. Connect to the command line on the Multi-Domain Server over SSH.
2. Log in to the Expert mode.
3. Back up the current file:

   ```
   cp -v $RTDIR/conf/log_maintenance_domain_conf.csv{,_
   ORIGINAL}
   ```

4. Get the contents of the current file:

   ```
   cat $RTDIR/conf/log_maintenance_domain_conf.csv
   ```

5. On your computer, copy the two lines from this file (from the SSH session) into a text editor or table editor (like Microsoft Excel, or LibreOffice Calc).
6. Save the file in the CSV format with this name:

   ```
   log_maintenance_domain_conf.csv
   ```

7. Configure the names of Domains and the required number of days to keep the logs.

   Best Practice - Add the row with the Domain name "`default`" and configure the default values. Each new Domain you create automatically uses these default values.

   Example for "Domain1" and "Domain2":

Domain_name	audit	files	firewallandvpn	other	other-smartlog	resources	smartevent
Domain 1	3650	20	15	15	14	14	30
Domain 2	3650	20	30	30	14	14	14
default	3650	30	14	14	14	14	14

Note - If you do not configure a Domain explicitly, then it takes the greatest values from each column. In the example, if there is a Domain called "Domain3", but you do not configure it explicitly in this file, then this Domain uses the values "`3650, 20, 30, 30, 14, 14, 14, 30`".

8. Copy the modified CSV file from your computer to the Multi-Domain Server to some directory (for example, `/var/log/`).
9. Go back to the SSH session on the Multi-Domain Server.
10. If you edited this CSV file on Windows OS, then convert the file from the DOS format to the UNIX format:

```
dos2unix /var/log/log_maintenance_domain_conf.csv
```

11. Replace the current file with the modified file:

```
cp -f -v /var/log/log_maintenance_domain_conf.csv
$RTDIR/conf/log_maintenance_domain_conf.csv
```

```
cat $RTDIR/conf/log_maintenance_domain_conf.csv
```

12. Restart Check Point services:

```
mdsstop ; mdsstart
```

Log Receive Rate

To learn how to monitor the Log Receive Rate on the Management Server / Log Server, see sk120341.

Deploying Logging

You can enable logging on the Security Management Server (enabled by default), or deploy a dedicated Log Server.

After you deploy the Log Server, you must configure the Security Gateways for logging.

You must execute the **Install Database** function on the remote Log Server when you:

- Enable or disable a logging related blade or function, including Log Indexing in a server object.
- Add a new Log Server to the system.
- Change a Security Gateway's Log Server.
- Change a Log Server's log settings or make any other Log Server object change.
- Change anything in the Global Properties that might affect the Log Server.

Enabling Logging on the Security Management Server

1. Open SmartConsole.
2. Edit the network object of the Security Management Server.
3. In the **General Properties** page, on the the **Management** tab, enable **Logging & Status**.
4. Click **OK**
5. Publish the SmartConsole session.

Deploying a Dedicated Log Server

To deploy a dedicated Log Server, you must install it, and then connect it to the Security Management Server.

For details, see the *R80.40 Installation and Upgrade Guide*.

Configuring the Security Gateways for Logging

To configure a Security Gateway for logging:

1. Open SmartConsole.
2. In the **Gateways & Servers** view, double-click the Security Gateway object.
3. From the navigation tree, click **Logs**.
4. Configure where to send logs:
   - To save logs to the Security Management Server - Select **Send gateway logs to server**.
   - To save logs to a dedicated Log Server - Select the Log Server from the list.
   - To save logs locally - Select **Save logs locally, on this server**.
5. Click **OK**.

6. Publish the SmartConsole session.
7. Install a policy on the Security Gateway.

Enabling Log Indexing

Log indexing on the Security Management Server or Log Server reduces the time it takes to run a query on the logs. Log indexing is enabled by default.

In a standalone deployment, log indexing is disabled by default. Enable log indexing only if the standalone server CPU has 4 or more cores.

To manually enable Log Indexing:

1. Open SmartConsole.
2. From the **Gateways & Servers** view, double-click the Security Management Server or Log Server object.

   The **General Properties** window opens.
3. In the **Management** tab, select **Logging & Status**.
4. From the navigation tree, click **Logs**.
5. Select **Enable Log Indexing**.
6. Click **OK**.
7. Publish the SmartConsole session.
8. From **Menu**, select **Install Database** > select all objects > click **Install**.

Disabling Log Indexing

To save disk storage space, a Log Server can be configured to work in non-index mode. If you disable log indexing, queries will take longer.

When log indexing is disabled, you must connect with SmartConsole to each Log Server separately to query its logs. When you connect to the Management Server you do not get a unified view of all logs, as in index mode. On each Log Server, the search is done on one log file at a time.

To disable Log Indexing:

1. Open SmartConsole.
2. From the **Gateways & Servers** view, double-click the Security Management Server or Log Server object.
3. From the navigation tree, click **Logs**.
4. Clear the **Enable Log Indexing** option.

5. Click **OK**.
6. Publish the SmartConsole session.
7. From **Menu**, select **Install Database** > select all objects > click **Install**.

To select a log file to search:

1. Open **Logs & Monitor > Logs** view.
2. Click the **Options** menu button to the right of the search bar.
3. Select **File > Open Log File**.

Deploying SmartEvent

SmartEvent Server is integrated with the Security Management Server architecture. It communicates with Log Servers to read and analyze logs. You can enable SmartEvent on the Security Management Server or deploy it as a dedicated server.

You can deploy R80.40 SmartEvent on a dedicated server and connect it to Security Management Servers or Multi-Domain Servers of version R77.X and higher. This lets you extend an R77.X environment with the new capabilities of R80.40 SmartEvent.

Only a Security Management Server can also work as a SmartEvent Server. In a Multi-Domain environment, you must install SmartEvent on a dedicated server.

You must execute the **Install Database** function on the remote SmartEvent Server when you:

- Enable or disable a SmartEvent Server blade, including Log Indexing in a server object.
- Add a new SmartEvent Server to the system.
- Change a SmartEvent Server log settings or make any other SmartEvent Server object change.
- Change anything in the Global Properties that might affect the SmartEvent Server.

SmartEvent Licensing

You can deploy SmartEvent in these ways:

- As part of the SmartEvent - A renewable one year license is included with the SmartEvent package.
- As a dedicated server - You can purchase a perpetual license for a SmartEvent Server.

Enabling SmartEvent on the Security Management Server

1. Open SmartConsole.
2. From the left navigation panel, click **Gateways & Servers**.

3. Open the Security Management Server object.
4. On the **Management** tab, enable these Software Blades:
   - **Logging & Status**
   - **SmartEvent Server**
   - **SmartEvent Correlation Unit**
5. Click **OK**.
6. Publish the SmartConsole session.

Note - For Security Gateways R77.30 and lower, you must activate the Firewall session for the network activity report. See *"Exporting Views and Reports" on page 48*.

System Requirements

To use SmartEvent, see the requirements in the *R80.40 Release Notes*.

Installing a Dedicated SmartEvent Server

For information on how to install a SmartEvent Server, see the *R80.40 Installation and Upgrade Guide*.

1. Download the installation ISO file.
2. Install the ISO on a Smart-1 appliance or an open server.

   Allocate partition size:
   - Root partition: at least 20 GB
   - Logs partition: more than allocated for Root and backup (set maximum possible) to let the server keep a long history.
3. When prompted, reboot.
4. Run the Gaia First Time Configuration Wizard.

Configuring the SmartEvent Components in the First Time Configuration Wizard

Configure the components of the dedicated server for SmartEvent on a Smart-1 appliance, or on an open server.

For information on how to install a SmartEvent Server, see the *R80.40 Installation and Upgrade Guide*.

Connecting R80.40 SmartEvent to R80.40 Security Management Server

This procedure explains how to configure a dedicated server for these components:

- SmartEvent Server and SmartEvent Correlation Unit

Note - For information on how to install a dedicated SmartEvent Server, see the *R80.40 Installation and Upgrade Guide*.

To connect R80.40 SmartEvent Server and SmartEvent Correlation Unit to R80.40 Security Management Server:

1. In SmartConsole, create a new **Check Point Host** object for the dedicated SmartEvent Server.
2. In the **Version** field, select R80.40.
3. Create a SIC trust with the dedicated SmartEvent Server.
4. On the **Management** tab, enable these Software Blades:
   - **Logging & Status**
   - **SmartEvent Server**
   - **SmartEvent Correlation Unit**
5. On a dedicated SmartEvent Server that is not a Log Server (recommended):

   In the **Logs** page, make sure that **Enable Log Indexing** is not selected.

   This ensures that Firewall connections (which are not relevant for views and reports) are not indexed.
6. Click **OK**.
7. Publish the SmartConsole session.
8. Click **Menu** > **Install Database** > select all objects > click **Install**.

Note - For Security Gateways R77.30 and lower: activate the Firewall session for the network activity report. See *"Exporting Views and Reports" on page 48*.

Advanced Configuration for a dedicated SmartEvent Server that is also a Correlation Unit

1. Open the SmartEvent GUI:
   a. In **SmartConsole** > **Logs & Monitor**, click **+** to open a catalog (new tab).
   b. Click **SmartEvent Settings & Policy**.
2. In **Policy tab** > **Correlation Units**, define a Correlation Unit object.

3. Select the production Log Servers and local Log Server on the SmartEvent Server to read logs from.
4. In **Policy tab** > **Internal Network**, define the internal Network.
5. Click **Save**.
6. Install the Event Policy on the Correlation Unit:

   SmartEvent menu > **Actions** > **Install Event Policy**.

Connecting R80.40 SmartEvent to R77.X Security Management Server

This procedure explains how to configure a dedicated server for these components:

- SmartEvent Server and SmartEvent Correlation Unit

To connect R80.40 SmartEvent Server and SmartEvent Correlation Unit to an R77.X Security Management Server:

1. Open an SSH connection to the SmartEvent Server.
2. Run this script:

   ```
   $RTDIR/scripts/SmartEvent_R80_change_dbsync_mode.sh
   ```

3. Wait until the script has finished running. This is when `cpstart` has finished and you have a prompt.
4. Run: `cpconfig`
5. Select `(2) Administrator` to configure the SmartEvent Server administrators.

   Note - Administrators that are configured in R77.X SmartConsole cannot manage the R80.40 SmartEvent Server.
6. Open the R77.X SmartDashboard.
7. In SmartDashboard, create a Check Point Host object for the SmartEvent Server R80.40.
8. Create an SIC trust between the Security Management Server and the new SmartEvent Server R80.40.
9. Define it with the highest version available and ignore the "**Warning**" message.
10. For a dedicated SmartEvent Correlation Unit that is not a SmartEvent Server: In the **Logs** page, click **Enable SmartLog**.
11. In the **Check Point Host** > **Management** tab, enable these Software Blades:

- **Logging & Status**
- **SmartEvent Server**
- **SmartEvent Correlation Unit**

12. Click **OK**.
13. Click **Menu** > **Policy** > **Install Database** > select all objects > click **Install**.
14. Wait until the server synchronizes and loads SmartEvent.

See also Advanced Configuration for a dedicated SmartEvent Server that is also a Correlation Unit in *"Connecting R80.40 SmartEvent to R80.40 Security Management Server" on page 34*.

Note - For Security Gateways R77.30 and lower: activate the Firewall session for the network activity report in *"Exporting Views and Reports" on page 48*.

Connecting R80.40 SmartEvent to R80.40 Multi-Domain Server

You can configure a dedicated R80.40 server for SmartEvent components, and connect them to one or more Domains in an R80.40 Multi-Domain Security Management environment.

This procedure explains how to configure a dedicated server for these SmartEvent components:

- SmartEvent Server and SmartEvent Correlation Unit

Notes:

- In R80 Multi-Domain Security Management environment, you can only define the SmartEvent Server and SmartEvent Correlation Unit at the global level and not the domain level.
- Configure SmartEvent to read logs from one domain or a number of domains.

To connect R80.40 SmartEvent Server and SmartEvent Correlation Unit to an R80.40 Multi-Domain Server:

1. Open SmartConsole.
2. Log in to the Global Domain:
   - In the SmartConsole login window, enter the Multi-Domain Server IP address or host name.
   - Select the Global Domain from the list (`Global`).
3. Create a Check Point Host object for **SmartEvent Server R80.40**.
4. In the **Check Point Host** > **Management**, select these Management Blades:

- **Logging & Status**
- **SmartEvent Server**
- **SmartEvent Correlation Unit**

5. Initialize SIC with the new SmartEvent Server R80.40 Server.
6. Click **OK**.
7. Publish the SmartConsole session.
8. Reassign the Global Policy for the Domains that use SmartEvent. For new Domains, create a new global assignment.
9. In each Domain Management Server, open SmartConsole.
10. Click **Menu** > **Policy** > **Install Database** > select all objects > click **Install**.
11. Wait until the server synchronizes and loads SmartEvent process.

See also Advanced Configuration for a dedicated SmartEvent Server that is also a Correlation Unit in *"Connecting R80.40 SmartEvent to R80.40 Security Management Server" on page 34*.

Note - For Security Gateways R77.30 and lower: activate the Firewall session for the network activity report in *"Exporting Views and Reports" on page 48*.

Connecting R80.40 SmartEvent to R77.X Multi-Domain Server

You can connect R80.40 SmartEvent components to one or more Domains in an R77.X Multi-Domain Security Management environment.

This procedure explains how to configure a dedicated server for these components:

- SmartEvent Server and SmartEvent Correlation Unit

Configure SmartEvent to read logs from one domain or a number of domains.

To connect R80.40 SmartEvent Server and SmartEvent Correlation Unit to an R77.X Multi-Domain Server:

1. Open an SSH connection to the SmartEvent Correlation Unit server.
2. Run this script:

   ```
   $RTDIR/scripts/SmartEvent_R80_change_dbsync_mode.sh
   ```

3. Wait until the script has finished running. This is when `cpstart` has finished and you have a prompt.
4. Open R77.X SmartDomain Manager.
5. Log in to the Global Domain:

6. Create a Check Point Host object for the dedicated server for SmartEvent Server R80.40.

   Define it with the highest version possible, and ignore the "**Warning**" message.

7. In the **Check Point Host** > **Management**, select these Management Blades:
   - **Logging & Status**
   - **SmartEvent Server**
   - **SmartEvent Correlation Unit**
8. Initialize SIC between the Multi-Domain Server and the SmartEvent Server R80.40.
9. In the **Logs** page, click **Enable Log Indexing**.
10. Click **OK**.
11. Publish the SmartConsole session.
12. Reassign the global Policy for the Domains that use SmartEvent. For new Domains, create a new global assignment.
13. In each Domain Management Server, open SmartDashboard.
14. Click **Menu** > **Policy** > **Install Database** > select all objects > click **Install**.
15. Wait until the server synchronizes and loads SmartEvent.
16. Click **Save**.
17. Install the Event Policy on the Correlation Unit:

    SmartEvent menu > **Actions** > **Install Event Policy**.

See also Advanced Configuration for a dedicated SmartEvent Server that is also a Correlation Unit in *"Connecting R80.40 SmartEvent to R80.40 Security Management Server" on page 34*.

Note - For Security Gateways R77.30 and lower: activate the Firewall session for the network activity report. See *"Exporting Views and Reports" on page 48*.

Configuring SmartEvent to use a Non-Standard LEA Port

You can get logs from and send logs to a third-party Log Server. The Check Point Log Server and the third party Log Server use the LEA (Log Export API) protocol to read logs. By default, the Check Point Log Server uses port 18184 for this connection. If you configure the Log Server to use a different LEA port, you must manually configure the new port on the SmartEvent Server and on the SmartEvent Correlation Unit.

Note - This procedure is not relevant if you use *"Log Exporter" on page 180*

To change the default LEA port:

1. Open `$INDEXERDIR/log_indexer_custom_settings.conf` in a text editor.
2. Add this line to the file:

   `:lea_port (<new_port_number>)`
3. Save the changes in the file and exit the editor.
4. In the SmartEvent client, configure the new port on the Correlation Unit.
5. In **Policy tab** > **Correlation Units**, configure the Correlation Unit to read logs from the local Log Server (on the SmartEvent Server).
6. **Configure the new port on the SmartEvent Server**
   a. In **Policy tab** > **Network Objects**, double-click the SmartEvent Server object.
   b. Change the **LEA port No** parameter to `<new_port_number>`.
7. Install the Event Policy on the Correlation Unit: **Actions** > **Install Event Policy**
8. **On the SmartEvent Server**
   a. Run: `cpstop`
   b. Open `$FWDIR/conf/fwopsec.conf` in a text editor.
   c. Change these parameters:

      ```
      lea_server auth_port <new_port_number>
      lea_server port 0
      ```
   d. Save the changes in the file and exit the editor.
   e. Run: `cpstart`

Configuring SmartEvent to read External Logs

To configure SmartEvent to read logs from an *externally-managed Log Server* or an *external Security Management Server*, see sk35288.

An *externally managed Log Server* is managed by a different Security Management Server than the one that manages the SmartEvent Server. An *external Security Management Server* is not the one that manages the SmartEvent Server.

Administrator Permission Profiles

You can give an administrator permissions for:

- Monitoring and Logging
- Events and Reports

To define an administrator with these permissions:

1. Define an administrator or an administrator group.
2. Define a Permission Profile with the required permissions in SmartConsole (**Manage & Settings** > **Permission Profiles**).
3. Assign that profile to the administrator or to the administrator group.

Configuring Permissions for Monitoring, Logging, Events, and Reports

In the **Profile** object, select the features and the Read or Write administrator permissions for them.

Monitoring and Logging Features

These are *some* of the available features:

- **Monitoring**
- **Management Logs**
- **Track Logs**
- **Application and URL Filtering Logs**

Events and Reports Features

These are the permissions for SmartEvent:

- **SmartEvent**
  - **Events** - views in SmartConsole > **Logs & Monitor**
  - **Policy -SmartEvent Policy and Settings** on SmartEvent GUI.
  - **Reports** - in SmartConsole > **Logs & Monitor**
- **SmartEvent Application & URL Filtering reports only**

Multi-Domain Security Management

In a Multi-Domain Security Management, each Event and Report is related to a Domain. Administrators can see events for Domains according to their permissions.

A Multi-Domain Security Management Policy administrator can be:

- Locally defined administrator on the SmartEvent Server.
- Multi-Domain Server Super User defined on the Multi-Domain Server.

- An administrator with permissions on all Domains. Select the Domains in SmartEvent, in **Policy** > **General Settings** > **Objects** > **Domains**. This type of administrator can install a Policy, and can see events from multiple Domains.

SmartEvent Reports-Only Permission Profile

You can define a special permission profile for administrators that only see and generate SmartEvent reports. With this permission profile, Administrators can open SmartConsole, but in the **Logs & Monitor** view can see only **Reports**. They cannot access other security information in SmartEvent. You can configure this permissions profile to apply to the Application & URL Filtering blade only, or apply to all blades.

To create a SmartEvent report-only permissions profile:

1. In SmartConsole, click **Manage & Settings** > **Permissions Profiles**.
2. In the **Permission Profiles** page, select a permission profile, or click the **New** button and create a permission profile.
3. Select **Customized**.
4. On the **Events and Reports** page, select **SmartEvent Reports**.
5. Clear all other options.
6. On the **Access Control**, **Threat Prevention**, and **Others** pages, clear all options.
7. On the **Monitoring and Logging** page, select all features, with **Write** permissions.
8. Click **OK**.

   The profile shows in the **Permission Profiles** page.
9. Assign the SmartEvent Reports Only permissions profile to administrators.
10. Publish the SmartConsole session.
11. Install the policy.

Importing Offline Log Files

The administrator can examine logs from a previously generated log file. This makes it possible to review security threats and pattern anomalies that occurred in the past, before SmartEvent was installed. You can investigate threats such as unauthorized scans targeting vulnerable hosts, unauthorized legions, denial of service attacks, network anomalies, and other host-based activity.

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

Importing Log Files from SmartEvent Servers

By default, you can import offline logs from the last 1 day. To import more days of logs, change the log indexing settings.

To change log indexing settings:

Note - Do this to make it possible to import logs that are older than 1 day before the SmartEvent Server was installed.

1. Run: `# evstop`
2. Run: `$INDEXERDIR/log_indexer -days_to_index <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 decrease the performance effect while you index the offline logs, import only the necessary number of days of logs.
3. In the **Logs** > **Storage** page of the SmartEvent Server, Make sure that **Delete Index files older than** is not selected, or is selected with an equal or larger number of days than configured in `days_to_index`.
4. Run: `# evstart`

To allow the SmartEvent Server to index offline log files:

1. Copy the log files and related pointer files `<log file name>.log*` to `$FWDIR/log`. Copy the files to the Log Server that sends logs to the SmartEvent Server.
2. Optional: Do an Offline Work for Correlated Events procedure for each log file. This procedure is done to run the log files through the Correlation Unit for correlation analysis according to the Event Policy (defined in SmartEvent GUI client).

   To run SmartEvent offline jobs for multiple log files, see: sk98894.

Offline Work For Correlated Events

To detect suspicious logging activity (suspicious according to the Event Policy on the **SmartEvent GUI** > **Policy** tab), run the offline log file through the Correlation Unit.

The settings to generate of Offline logs are in: **SmartEvent GUI client** > **Policy tab** > **General Settings** > **Initial Settings** > **Offline Jobs**, connected to the Security Management Servers or Multi-Domain Server.

The settings are:

- **Add** - Configure an Offline Log File procedure.
  - **Name** - Lets you recognize the specified Offline Line log file for future processing.
  - **Comment** - A description of the Offline Job.
  - **Offline Job Parameters:**

    SmartEvent Correlation Unit: The machine that reads and processes the Offline Logs.

    Log Server: The machine that contains the Offline Log files. SmartEvent makes a query to this Log Server to find out which log files are available.

    Log File - A list of available log files found on the selected Log Server. These log files are processed by the SmartEvent Correlation Unit. In this window, select the log file from which to retrieve historical information.
- **Edit** - Change the parameters of an Offline Log File procedure.
- **Remove** - Delete an Offline Log File procedure. After you start an Offline Log File procedure you cannot remove it.
- **Start** - Run the Offline Log File procedure.
- **Stop** - Stop the Offline Log Files procedure. It does not delete the full procedure, but stops the procedure at the specified point.

Importing Syslog Messages

Many third-party devices use the *syslog* format for logging. The Log Server reformats the raw data to the Check Point log format to process third-party *syslog* messages.

The Log Server uses a syslog parser to convert syslog messages to the Check Point log format.

To import syslog messages, define your own syslog parser and install it on the Log Server.

SmartEvent can take the reformatted logs and convert them into security events.

Generating a Syslog Parser and Importing syslog Messages

To import syslog messages from products and vendors that are not supported out-of-the-box, see sk55020. This shows you how to:

1. Import some sample syslog messages to the Log Parsing Editor.
2. Define the mapping between syslog fields and the Check Point log fields.
3. Install the syslog parser on the Log Server.

After you imported the syslog messages to the Log Server, you can see them in SmartConsole, in the **Logs & Monitor** > **Logs** tab.

Note - Make sure that Access Control rules allow ELA traffic between the Syslog computer and the Log Server.

Configuring SmartEvent to Read Imported Syslog Messages

After you imported the syslog messages to the Log Server, you can forward them to SmartEvent Server (and other OPSEC LEA clients), as other Check Point logs. SmartEvent converts the syslog messages into security events.

To configure the SmartEvent Server to read logs from this Log Server:

1. Configure SmartEvent to read logs from the Log Server.
2. In SmartEvent or in the SmartConsole event views, make a query to filter by the **Product Name** field. This field uniquely identifies the events that are created from the syslog messages.

Views and Reports

You can create rich and customizable views and reports for log and event monitoring. The views present queries in a graphical way which can be used for analytical and presentation purposes.

Use these GUIs:

- **SmartConsole** > **Logs & Monitor**
- **SmartView Web Application** - for generating and editing views in a browser: `https://<Server IP Address>/smartview/`

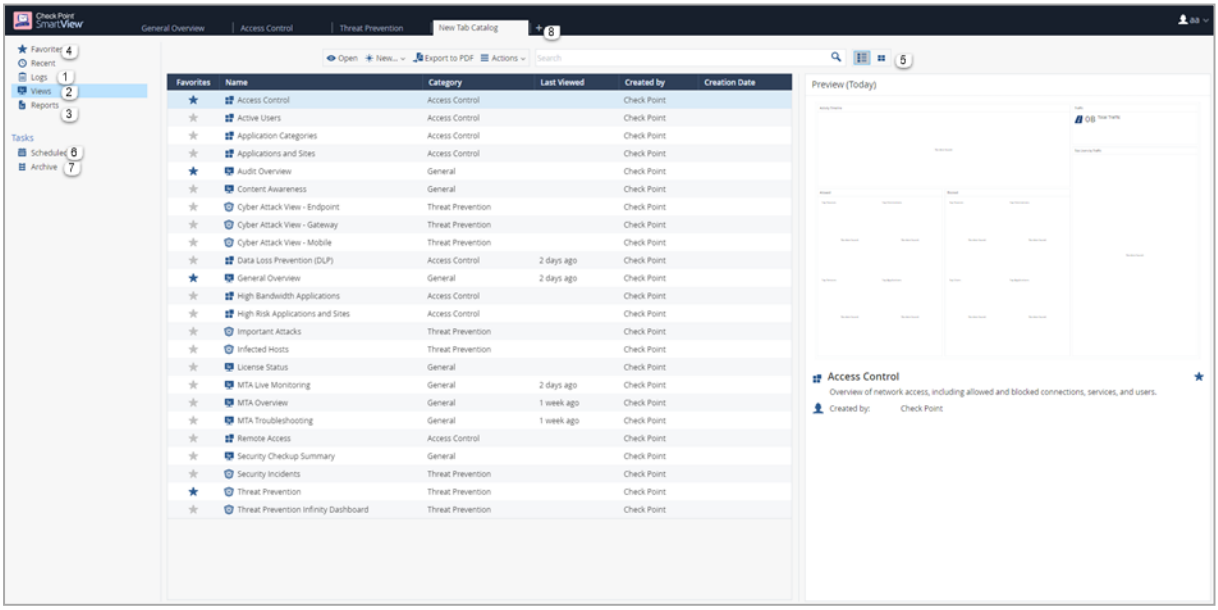
  Where `<Server IP Address>` is IP address of the Security Management Server or SmartEvent Server.

Enabling Views and Reports

To enable SmartEvent views and reports, you must install and configure a SmartEvent Server.See *"Deploying SmartEvent" on page 32*.

Catalog of Views and Reports

In the **Logs & Monitor** view, click the **(+)** tab to open a catalog of all views and reports, predefined and customized. Click a view or report to open it. You can create a new view or report, or export them to PDF. To see other actions, open the **Actions** menu.

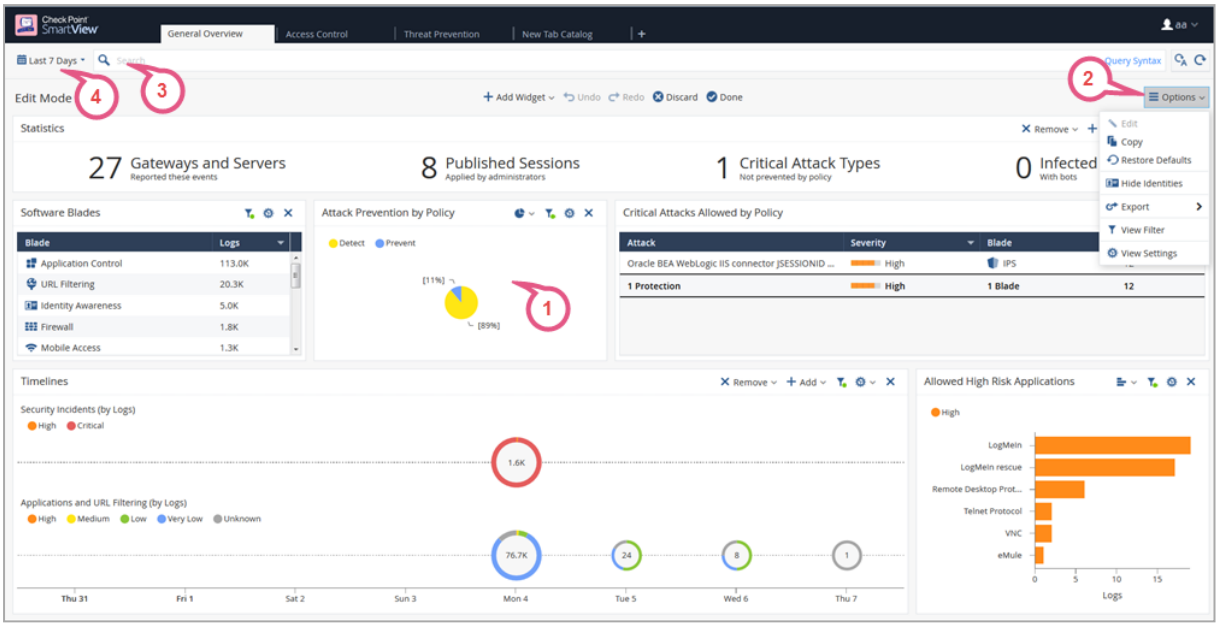


Item	Description
1	**Open Log View** - See and search through the logs from all Log Servers. In SmartConsole only, you can also search the logs from a specific Log Server. **Open Audit Logs View** - See and search records of actions done by SmartConsole administrators. These views come from the Log Servers. All other Views/Reports (except the Compliance View) come from the SmartEvent Server.
2	**Views** -The list of predefined and customized views. A view is an interactive dashboard made up of widgets. The view tells administrators and other stakeholders about security and network events. Each widget is the output of a query. Widgets can show the information as a chart, table, or some other format. To find out more about the events, double-click a widget to drill down to a more specific view or raw log files. **Compliance View** -Optimize your security settings and ensure compliance with regulatory requirements.
3	**Reports** -The list of predefined and customized reports. A report consists of multiple views. There are several predefined reports, and you can create new reports. A report gives more details because it consists of multiple views. Reports can be customized, filtered, generated and scheduled. You cannot drill down into a report.
4	**Favorites** - Use this view to collect the views and reports you use the most. **Recent** - Shows the most recently opened report or view.
5	**Switch to Table View** or **Thumbnails View** -The Table view is the default for **Views** and **Reports**. The Thumbnails view is the default for the **Favorites** , **Recent**, and **Logs**.
6	**Scheduled Tasks** - See and edit scheduled tasks.
7	**Archive** - Download the exported views and reports.
8	**Catalog (New Tab)** - Open a Catalog (new tab) and select Log View, Audit View, Views, or Reports. In the Logs & Monitor view, click the (**+**) tab to open a catalog of all views and reports, predefined and customized. To open a view, double-click the view or select the applicable view and click **Open** from the action bar.

Views

Views shows an interactive dashboard made up of widgets. Each widget is the output of a query. A **Widget** pane can show information in different formats, for example, a chart or a table.

SmartView and SmartEvent come with several predefined views. You can create new views that match your needs, or you can customize an existing view.



Item	Description
1	**Widget** - The output of a query. A Widget can show information in different formats, for example, a chart or a table. To find out more about the events, you can double-click most widgets to drill down to a more specific view or raw log files.
2	**Options** - Customize the view, restore defaults, Hide Identities, export.
3	**Query search bar** - Define custom queries using the GUI tools, or manually entering query criteria. Shows the query definition for the most recent query. Click **Query Syntax** to open the online Help for more information.
4	**Time Period** - Specify the time periods for the view.

Reports

A report consists of multiple views and a cover page. There are several predefined reports, and you can create new reports. A report gives more details than a view. Reports can be customized, filtered, generated and scheduled. You cannot drill down into a report.

Note - For Security Gateways R77.30 and lower, the ability to generate reports on Firewall and VPN activity is integrated into SmartConsole. To enable this functionality, activate the Firewall session event on the SmartEvent **Policy** tab. Select and enable **Consolidated Sessions** > **Firewall Session**. For more information, see *"Connecting R80.40 SmartEvent to R80.40 Security Management Server" on page 34*.

Automatic View and Report Updates

SmartEvent automatically downloads new predefined views and reports, and downloads updates to existing predefined ones. To allow this, make sure the management server has internet connectivity to the *Check Point Support Center*.

Opening a View or Report

Use the predefined graphical views and reports for the most frequently seen security issues. You can also customize the views and reports.

To open a view or report:

1. In SmartConsole, open the **Logs & Monitor** view.
2. Click the **+** icon to open a new catalog.
3. Click **Views** or **Reports**.
4. Select a view or a report, and click **Open**. You can also double click to open it.
5. Define the required timeframe, and filter in the search bar.
6. Click **Enter**.

Exporting Views and Reports

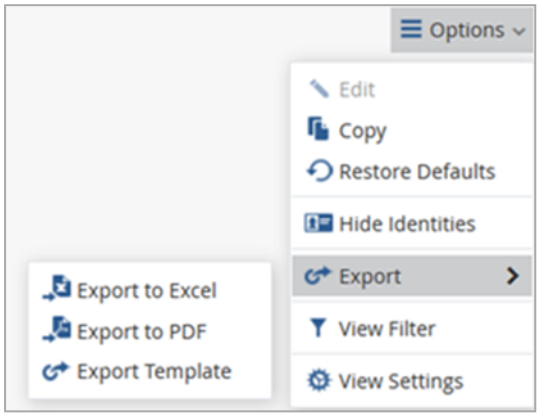
The **Export to PDF** and **Export to Excel** options save the current view or report as a PDF or Excel file, based on the defined filters and time frame. **Note** - When you export to Excel, only tables are exported.

To export a view or report to PDF or Excel:

1. In SmartConsole, open the **Logs & Monitor** view.
2. Click the **+** tab to open a new tab.
3. Click **Views** or **Reports**.
4. Select a view or report.
5. Click **Export to PDF**.Optionally:

- Configure the **Period and filter**.
- To automatically send by email to specified recipients each time the view or report runs, configure the **Send by email** settings.See *"Configuring Email Settings for Views and Reports" on page 55*.

Alternatively, click **Open** and from inside the view or report click **Options** > **Export to PDF** or **Export to Excel**.



To see your exported views and reports:

1. Add a new tab. Click **+**.
2. Go to **Tasks** > **Archive**.

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. Indexing is on by default in R80 and higher, in all environments except for Standalone.

To enable the Network Activity Report for Security Gateways R80.10 and higher:

In SmartConsole, in the Access Control Policy rule, add **per Session** to the **Track** settings. See *"Tracking Options" on page 77*.

To enable the Network Activity Report for Security Gateways R77.30 and lower:

1. In SmartConsole, open the **Logs & Monitor** view.
2. Click the (**+**) to open a new tab.
3. In the **External Apps** section, click **SmartEvent Settings & Policy** link.
4. In the SmartEvent GUI client > **Policy** tab, select and expand **Consolidated Sessions**.
5. Select **Firewall Session**.

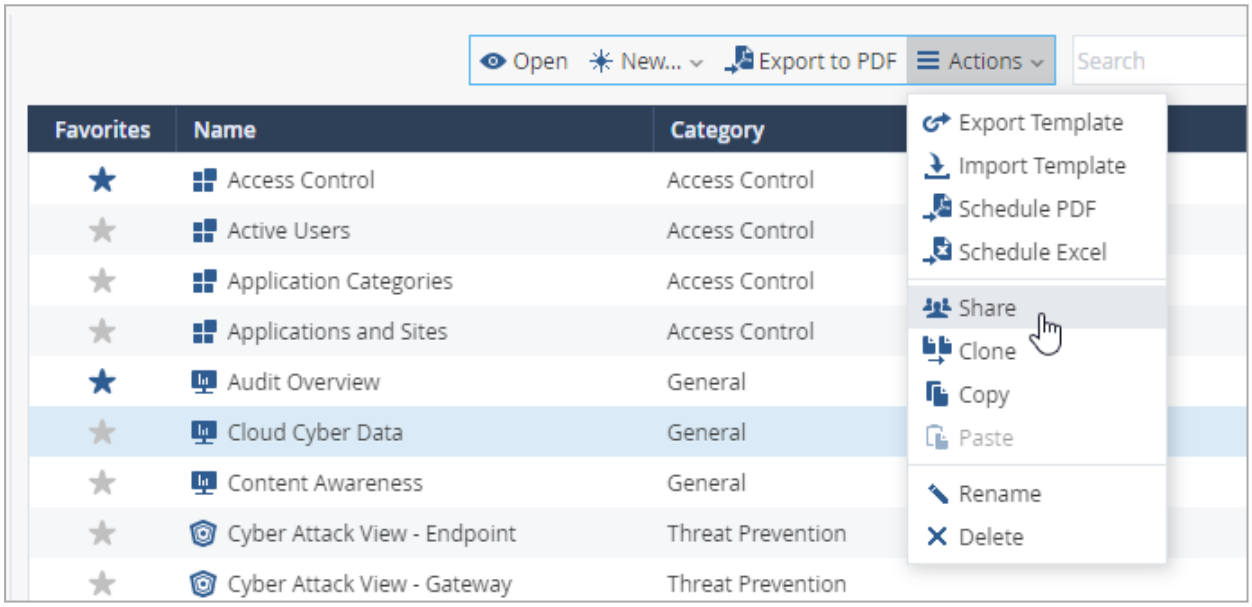
Note - This configuration increases the number of events per day by about five times. To avoid a performance impact, make sure the hardware can handle the load.

Sharing Reports

You can share a report you created with your team, without export or import. If a regular admin shares a view or report, it is shared with all the admins on the domain. A super admin for the Multi-Domain Server can share with all users under all domains.

To share a report:

1. In SmartConsole, open **Logs & Monitor** and click **+** to open a new tab.
2. Click **Reports** and select a report.
3. Click **Actions** and select **Share**.



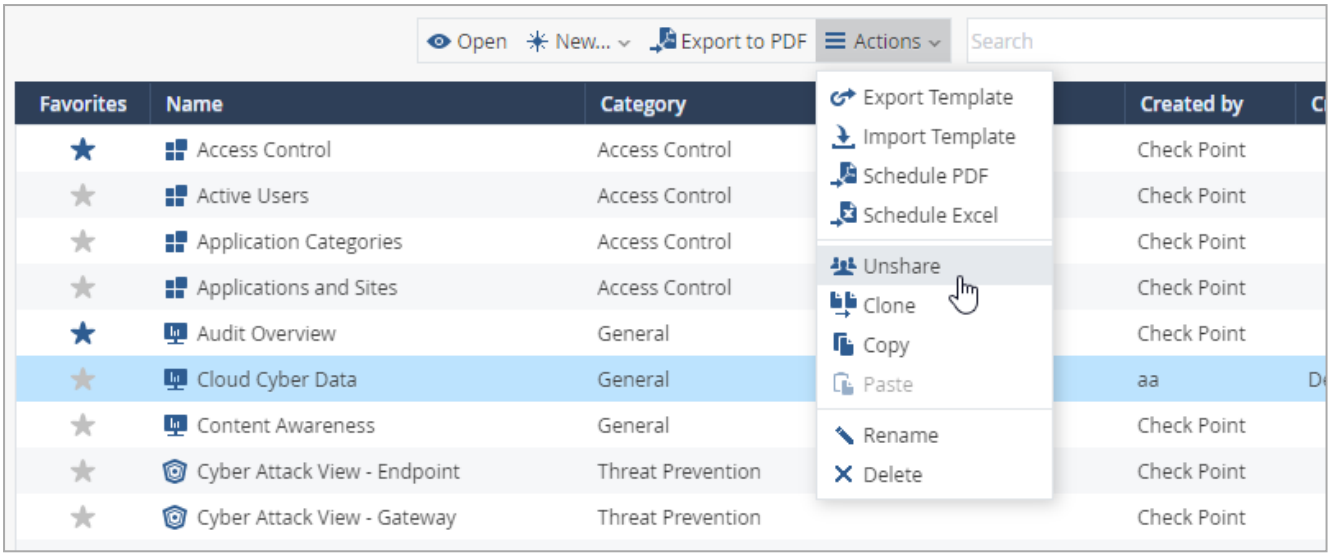
4. Click **Yes** to approve sharing the report.

   The report is now marked as shared.

The report owner can undo the action and unshare the report.

To unshare the report:

Click **Actions** and select **Unshare**.



Note - A Super User can take ownership of reports or views created by other administrators via the **take ownership** feature.

Permissions when an owner shares a view/report:

	Visible on Catalog	Can Edit	Can clone	Can Delete
Owner	+	+	+	+
Super User	+	-	+	-

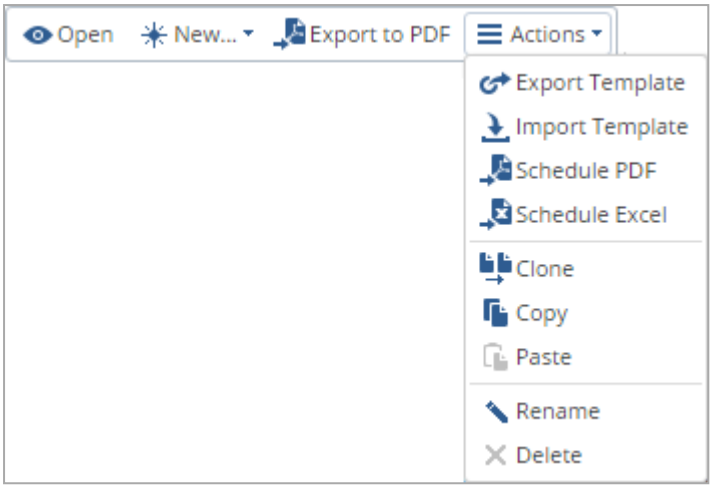
Exporting and Importing Templates

You can export the view or report layout and widget definitions to a file. This is called a *template.* You can import the template from another server or from another administrator.

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

To download exported templates, click the link in the notification message. To view historical reports, views, and templates, go to **Tasks** > **Archive**.

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



Scheduling a View or Report

To schedule a view or report, you need to define and edit it in SmartConsole.

To schedule a report:

1. In SmartConsole, open the **Logs & Monitor** view.
2. Click the **+** tab to open a new tab.
3. Click **Views** or **Reports**.
4. Select a view or a report.
5. Select **Actions** > **Schedule PDF** or **Schedule Excel**.

   The **Schedule** page of the **Export** settings window opens.
6. Define the **recurrence pattern**.
7. Define the **Period and Filter**.
8. **Optional**: Configure email settings to get the scheduled view or report automatically. Click **Send by email**.

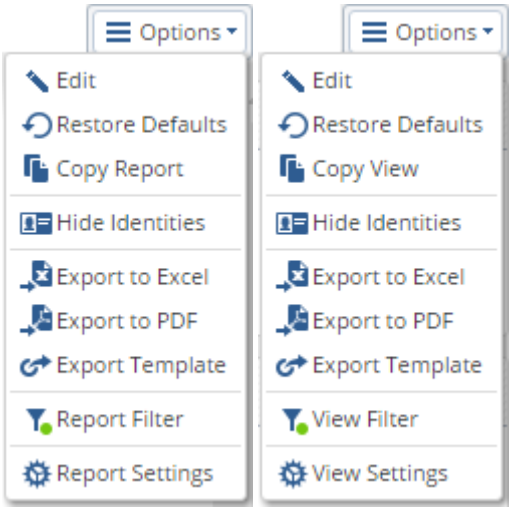
To edit your scheduled views and reports:

1. In SmartConsole, open the **Logs & Monitor** view.
2. Click the **+** tab to open a new tab.
3. Select **Tasks** > **Scheduled**.

Customizing a View or Report

To customize a view or report:

1. Select a view or a report and click **Open**.
2. Click **Options** > **Edit**.



3. In a report, you can edit the report or the current view in the report.
   - To add or remove, click the relevant icon in the edit toolbar (becomes available when in edit mode):

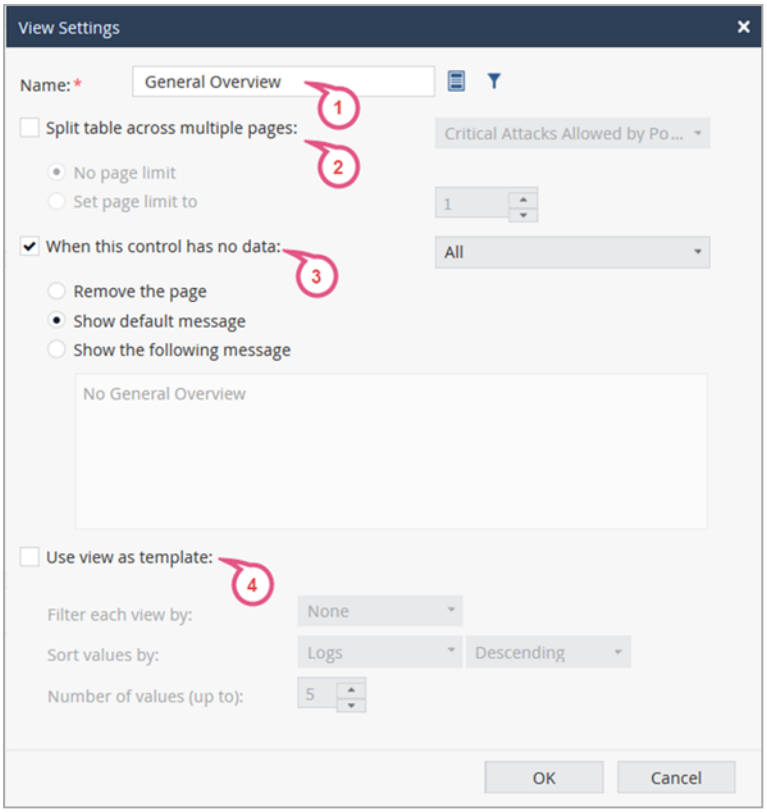
     

   - To add a widget or arrange the *"Widgets" on page 57* in the view, use Drag & Drop or expand..
   - Define filters. (see *"Widgets" on page 57*).

Note - If you change the timeframe, the data changes according to the start and stop times. The timeframe and search bar are not saved with the view or report definition. Define them as needed when generating the view or report. See *"Opening a View or Report" on page 48*.

View Settings

Views can be configured according to these options:



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 all the results for the selected table query, spread across as many pages as required.
3. Select what you want to display when this control has no data:
   - Remove the page
   - Show a default or custom message.
4. Select to use the view as a template and add filter and sort criteria.

   Use the view as a basis for generating duplicate views with more granularity.

Use Case:

The **Active Users** predefined view shows all active users. You want to see a more granular view per user:

1. Open the **Active Users** view and click **Options** > **View settings**.

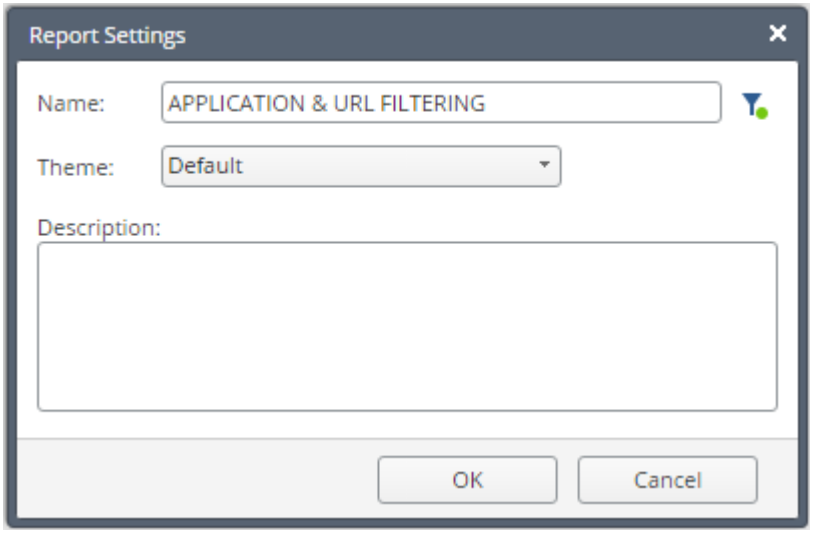
   The **View Settings** window opens.
2. Select **Use View as template**.
3. For **Filter each view by**, select **User**.

4. Select **Number of values**. For example, 5.
5. Click **OK**.
6. Go to **Options** > **Export** > **Export to PDF**.
7. The view is exported. Wait until a message shows the view was successfully exported.
8. Click **Download**.

   The report shows all widgets in the view filtered according to each user.

Report Settings

Reports can be configured according to these options:



Configuring Email Settings for Views and Reports

You can automatically send views and reports by email to specified recipients each time the view or report runs.

Configuring Email Server Settings

Mail server settings in SmartConsole and SmartView are shared for all email interactions. For each SmartConsole administrator, configure them one time.

To configure email server settings:

1. Select a view or a report in the catalog.
2. Click **Export to PDF**, or **Actions** > **Schedule PDF** or **Actions > Schedule Excel**.
3. Click **Send by email**.
4. In the **Email Server** section, click **Edit**.

Note - In SmartView, you can edit the mail server on the user preferences menu.

5. Configure the email server options:
   - **Sender email address**. This shows on all report emails.
   - **Outgoing mail server (SMTP)**
   - **Port** - The default port is 25.
   - **Use authentication** (Optional) - if required by the email server, configure a **Username** and **Password**.
   - **Connection encryption** (Optional) - if required by the email server, choose **SSL** or **TLS**.
6. Click **OK**.

Configuring Email Recipients

Define the email recipients every time you run the view or report, or one time for scheduled reports.

To configure email recipients:

1. Select a view or a report from the catalog.
2. Click **Export to PDF**, or **Actions** > **Schedule PDF** or **Actions > Schedule Excel**.
3. Click **Send by email**.
4. In the **Email recipients** section, click **+** to enter an email address. You can add multiple addresses.
5. Click **OK**.

Adding a Logo to Reports

You can configure reports to show your company logo on report cover pages instead of the Check Point logo.

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** - This applies when there is local SmartEvent on the Management Server. Otherwise, you must add the logo image to every machine the users connect to or the logo only displays when conected to the SmartEvent IP.

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

Widgets

You can customize the widgets to optimize the visual display. To customize widgets, switch to edit mode. Click **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**.

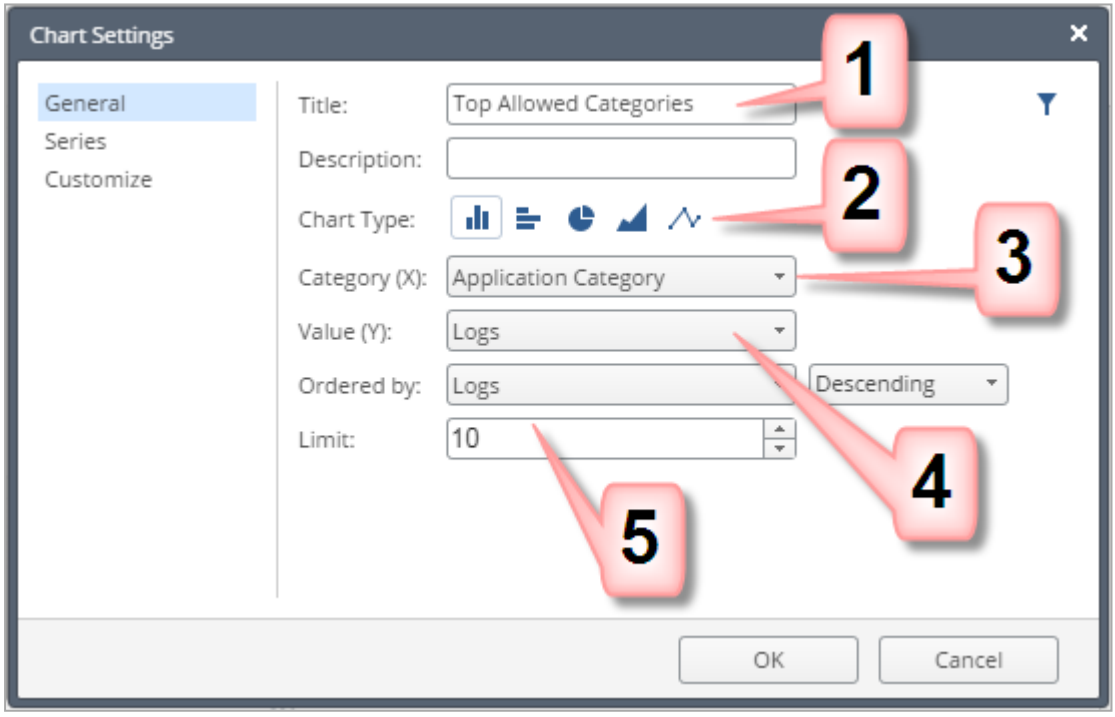
  Note - **Restore Defaults** option is only available after you modify a predefined view.

Adding and Customizing Widgets

To add a Widget:

1. Double-click a view or report to open it.
2. Click **Options** > **Edit**.
3. Click **Add Widget** and select the widget type.

   Chart Settings:



   a. Enter a title.

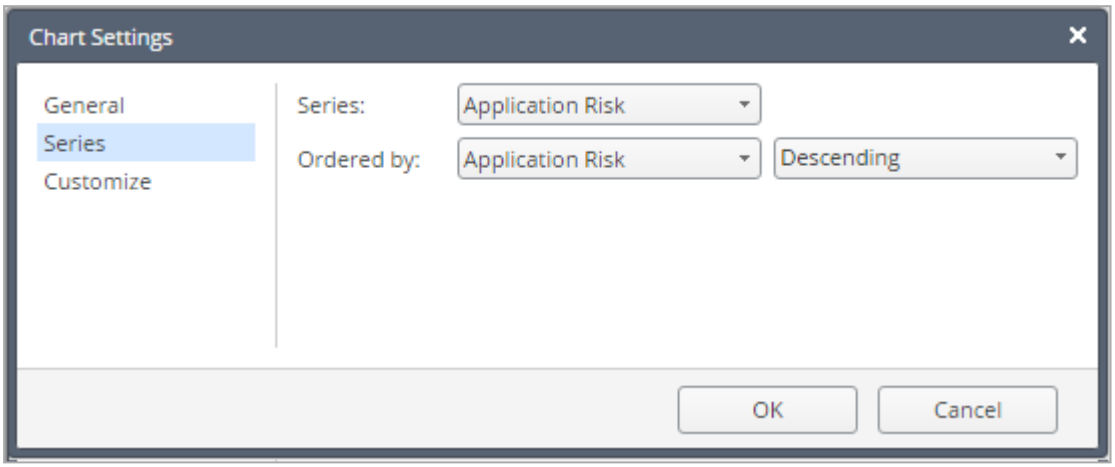
   b. Select a chart type: vertical bar, horizontal bar, pie, area or line.

c. Select a data category for the X axis.

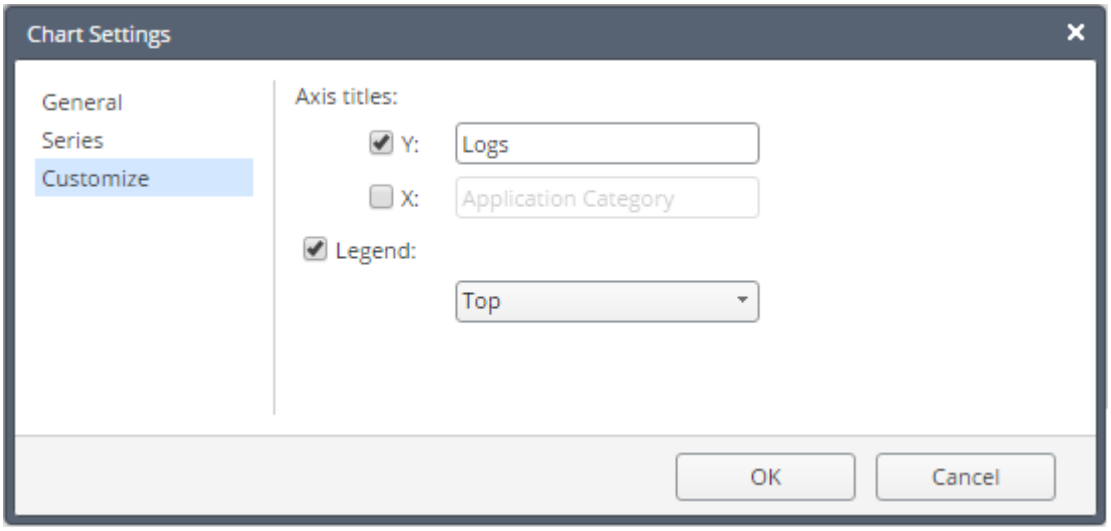
d. Define how the Top Values are calculated (by number of logs, or by traffic).

e. Set a limit for how many top values to show.

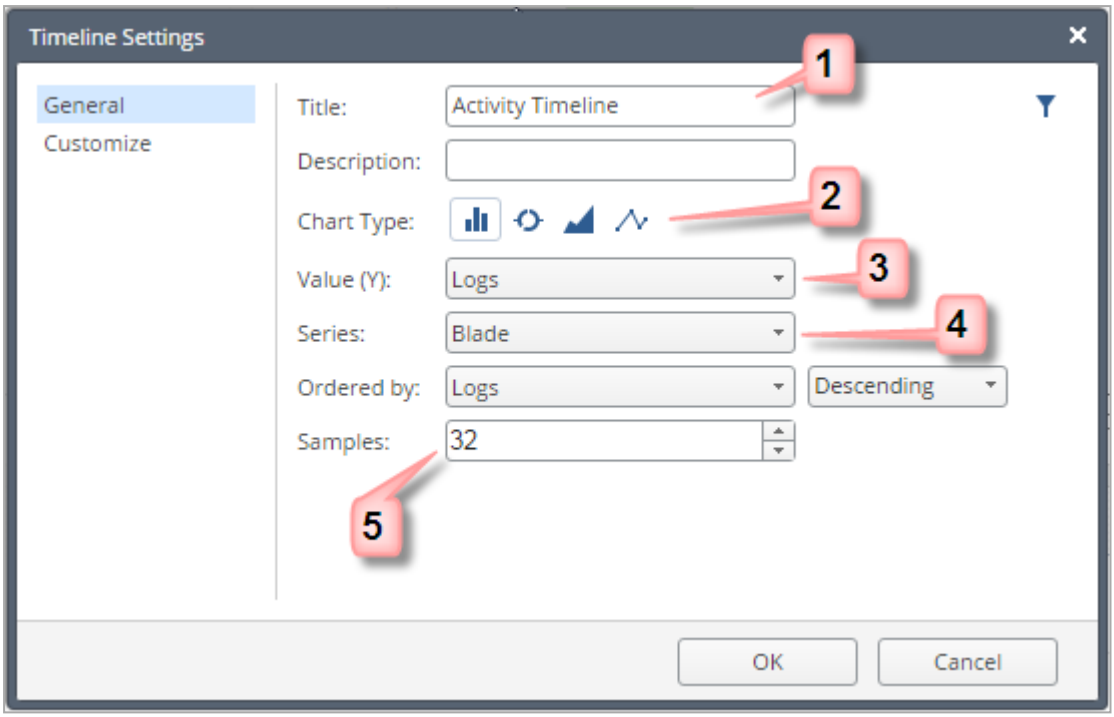
f. Optional: click **Series** - split the results into colored groups with different values for the series.



g. Optional: click **Customize** and define axis titles and legend position.



Timeline Settngs:



a. Enter a title.

b. Select a timeline graphical presentation: vertical bar, doughnut, area or line.

Notes:

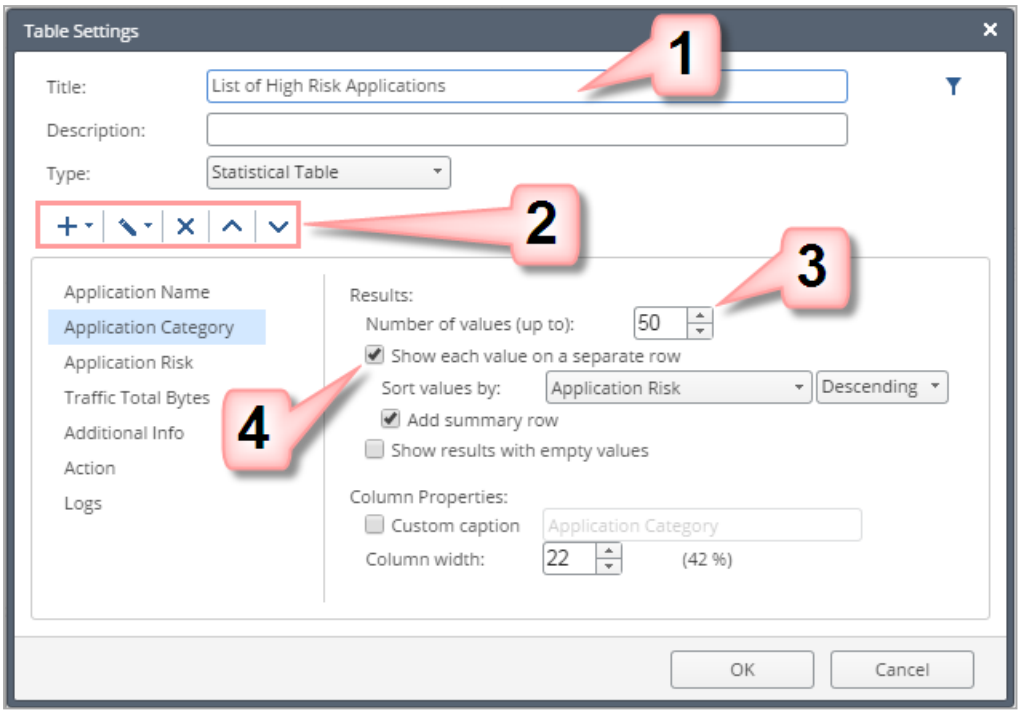
- In R80.40 GA, the last field is called **Samples** and accepts integer values.
- In R80.40 with R80.40 Jumbo Hotfix Accumulator, the field is called **Resolution** and it is a drop-down list with predefined values.

c. Select the data to count.

d. Advanced - split the results into colored groups, with different values for the **Series**.

e. Define the time-granularity. Enter the number of bars or doughnuts to show.

Table Settings:



a. Enter a title.

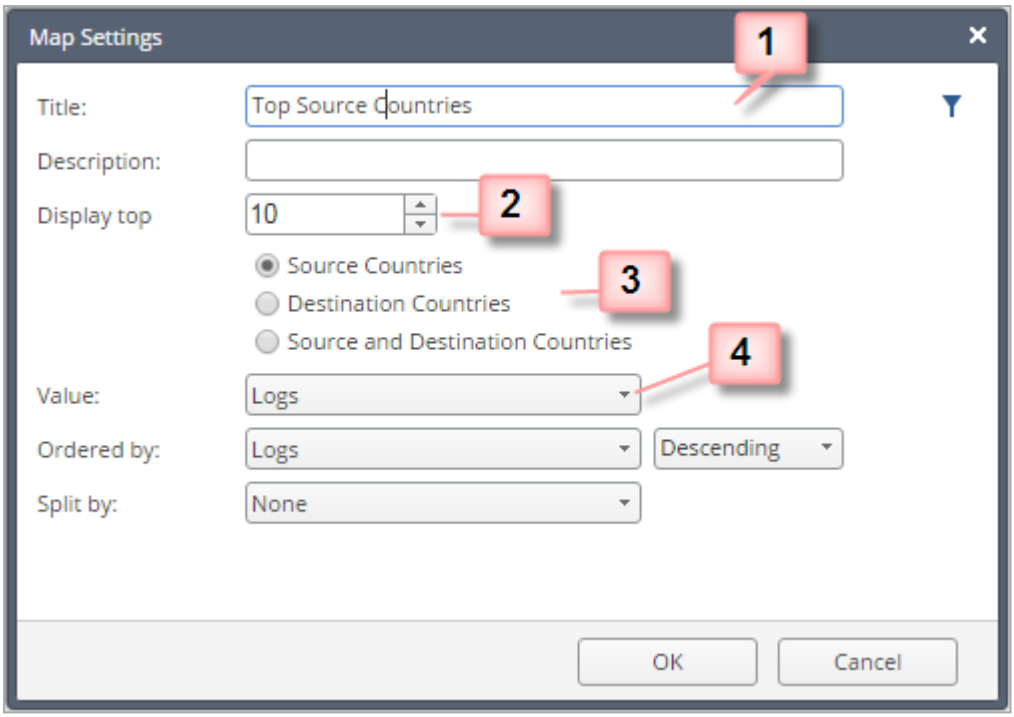
b. Manage columns: add, edit, remove, and change the order.

c. Select a column on the left and define its settings:

   - Enter the number of top values to show.
   - Select how values are sorted.

d. Select this option to group results with the same value in one row.

Map Settings:



a. Enter a title.

b. Enter the number of Top Countries to mark.

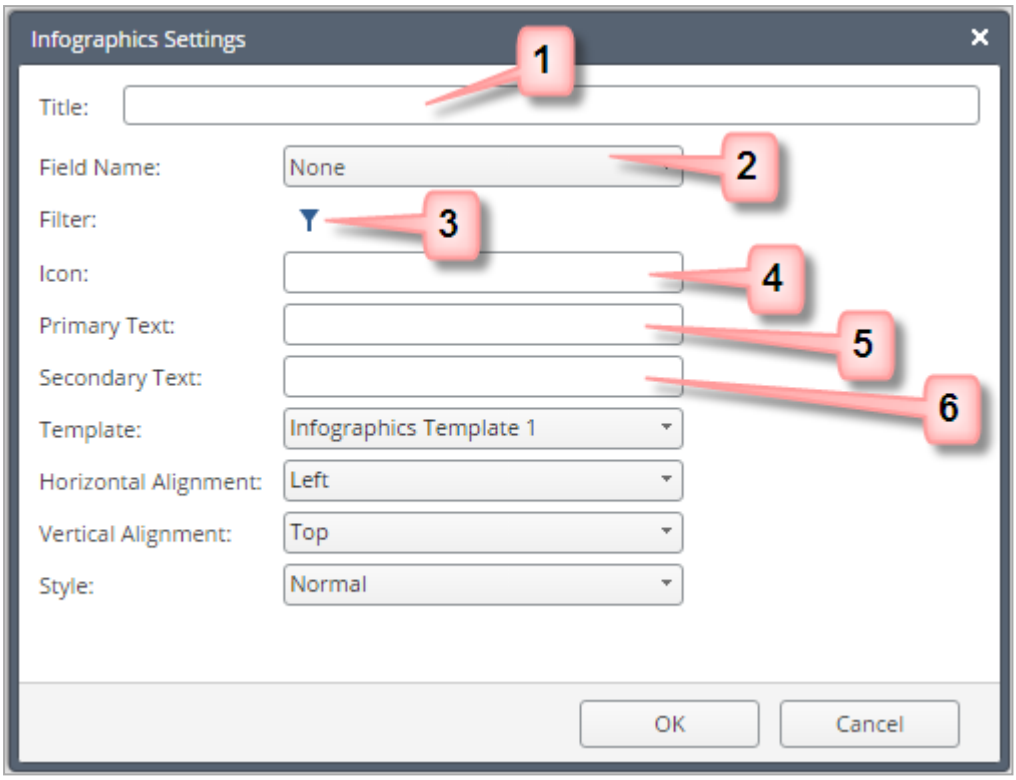
c. Select to mark Top Source Countries, Top Destination Countries, or both.

d. Define how to find the Top Countries (for example, by number of logs or by traffic).

The infographic widget shows large meaningful values. For example:



Infographic Settings:



a. Enter a title

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

c. Define filter criteria.

   This critieria is in addition to the inherited filters for the report and view layers.

   For more, see Filters in *"Widgets" on page 57*.

d. 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.

Icon	Used for
apps	
attacks	
hosts	
gateway	
traffic	
usercheck	
users	
new	Audit Logs
add	Audit Logs
remove	Audit logs
modify	Audit logs
install-policy	
publish	
ips	
anti-bot	
anti-virus	
threat-emulation	

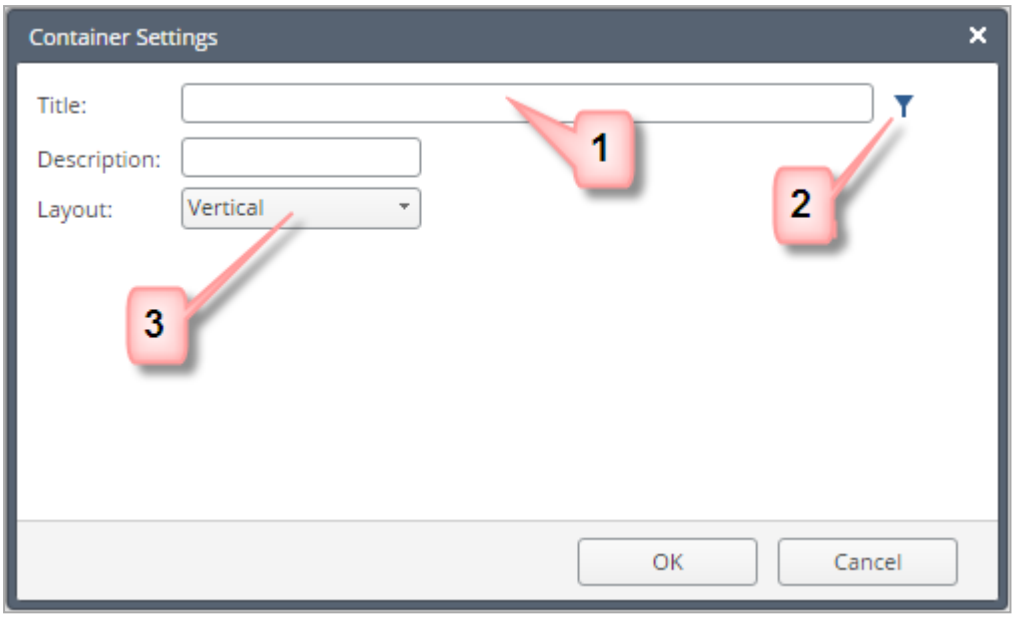
e. Enter primary text that describes the value counted.

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

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.

Container Settings:

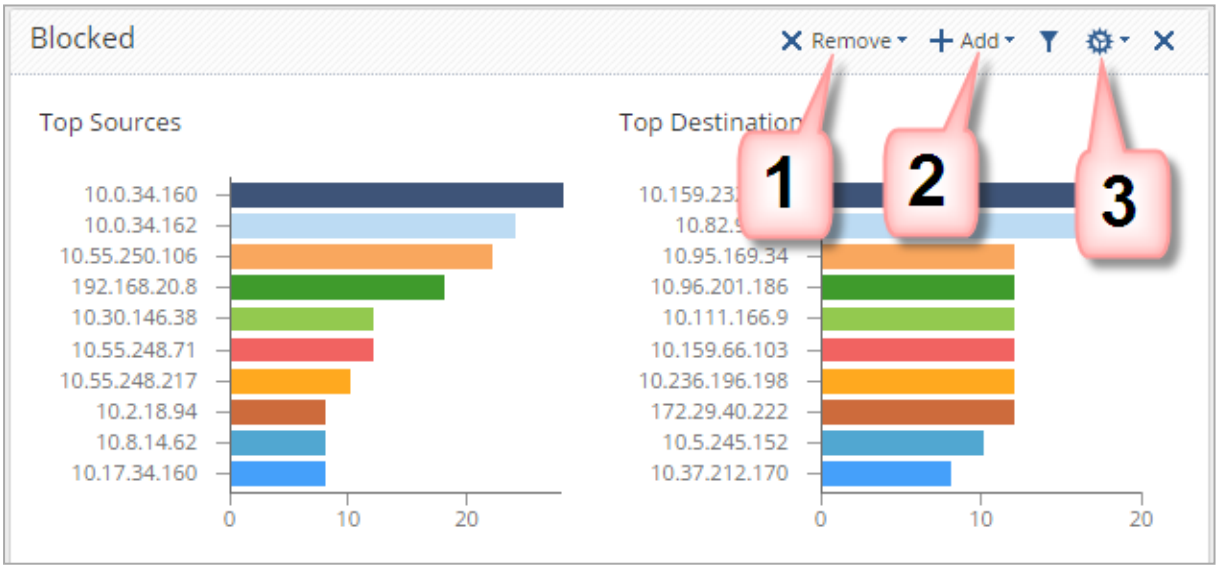


a. Enter a title.

b. Optional: filter at the container level. The filter applies to all internal widgets.

c. Select the widget order inside the container: Horizontal, Vertical, Grid or Tabs.

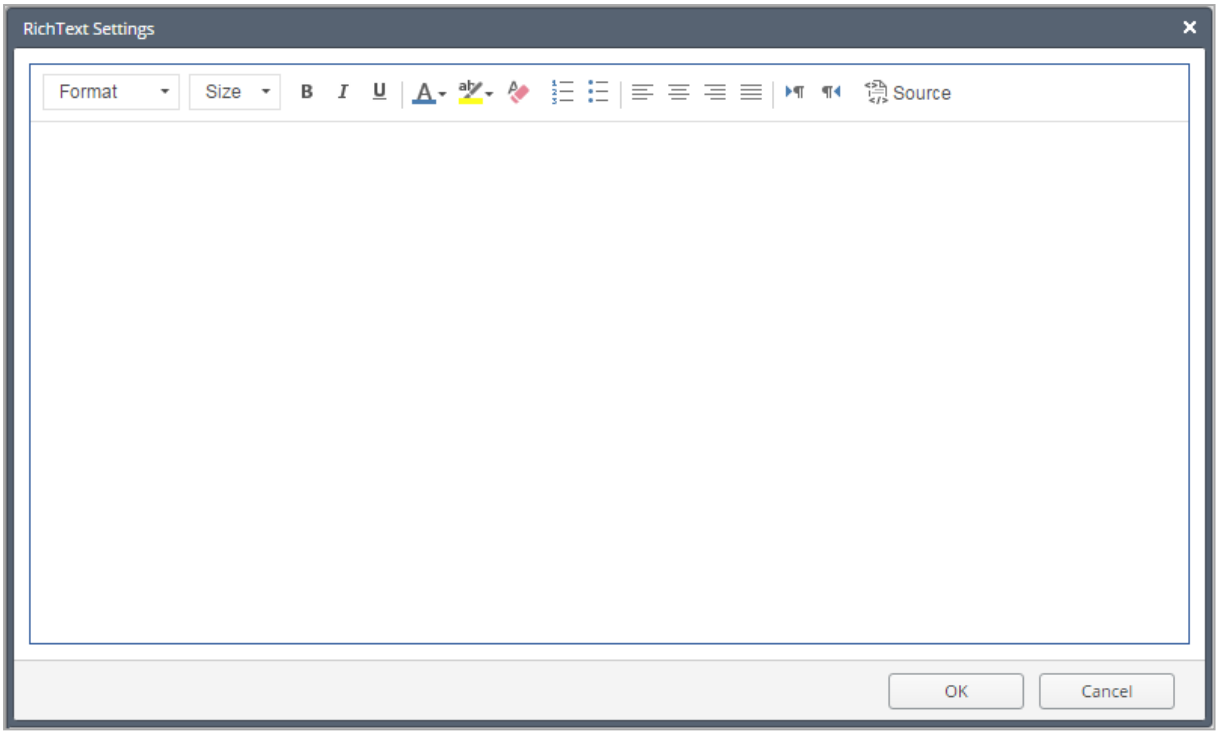
After the container is added to the view, you can configure it further.



a. Remove the widget from the container.

b. Add a new widget.

c. Edit the settings for the container, or edit one of the widgets in the list.

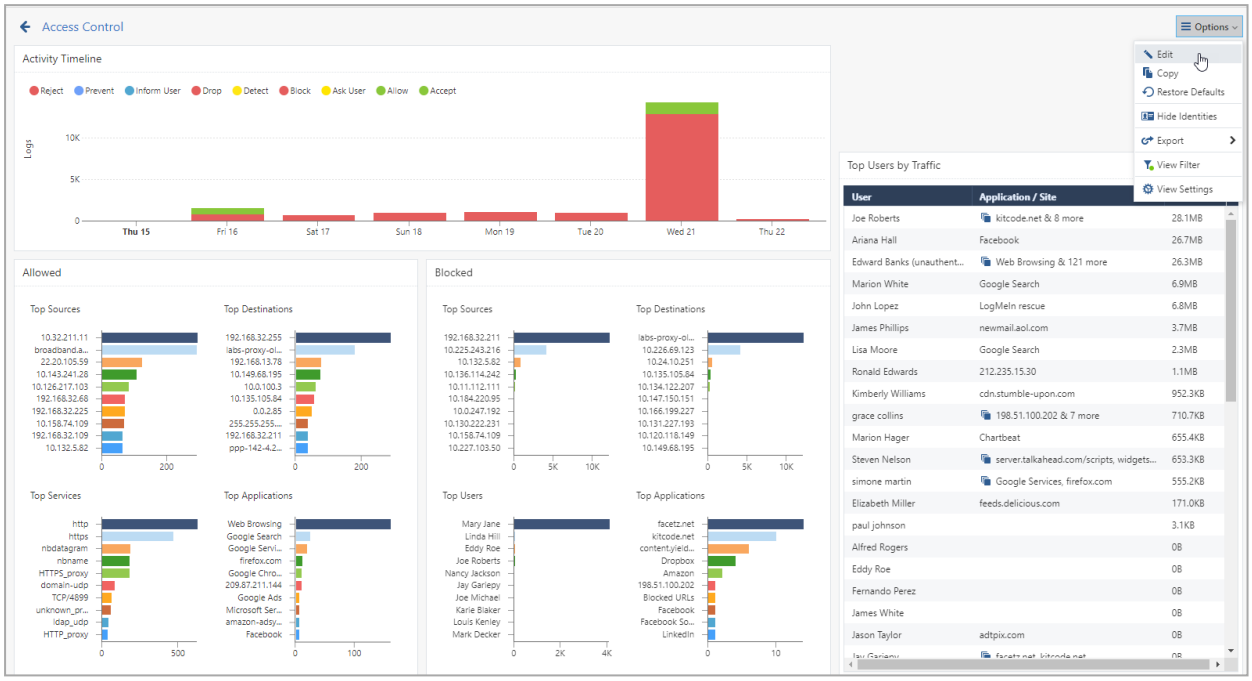


Use this window to add textual explanations to the View text box.

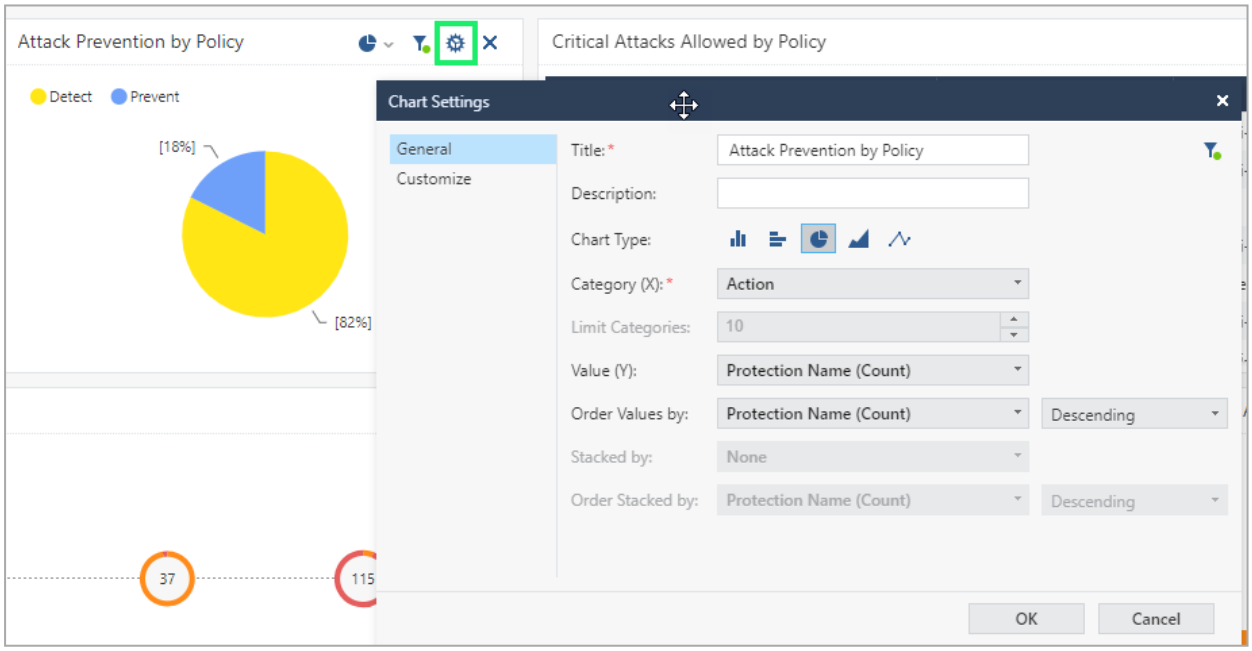
4. Click **OK**.
5. Select filters for the widget in addition to the inherited filters from the report and view layers. See Filters in *"Widgets" on page 57*.
6. Configure settings for the widget.

To customize a widget:

1. In the view where the widget is located, click **Options** > **Edit**.

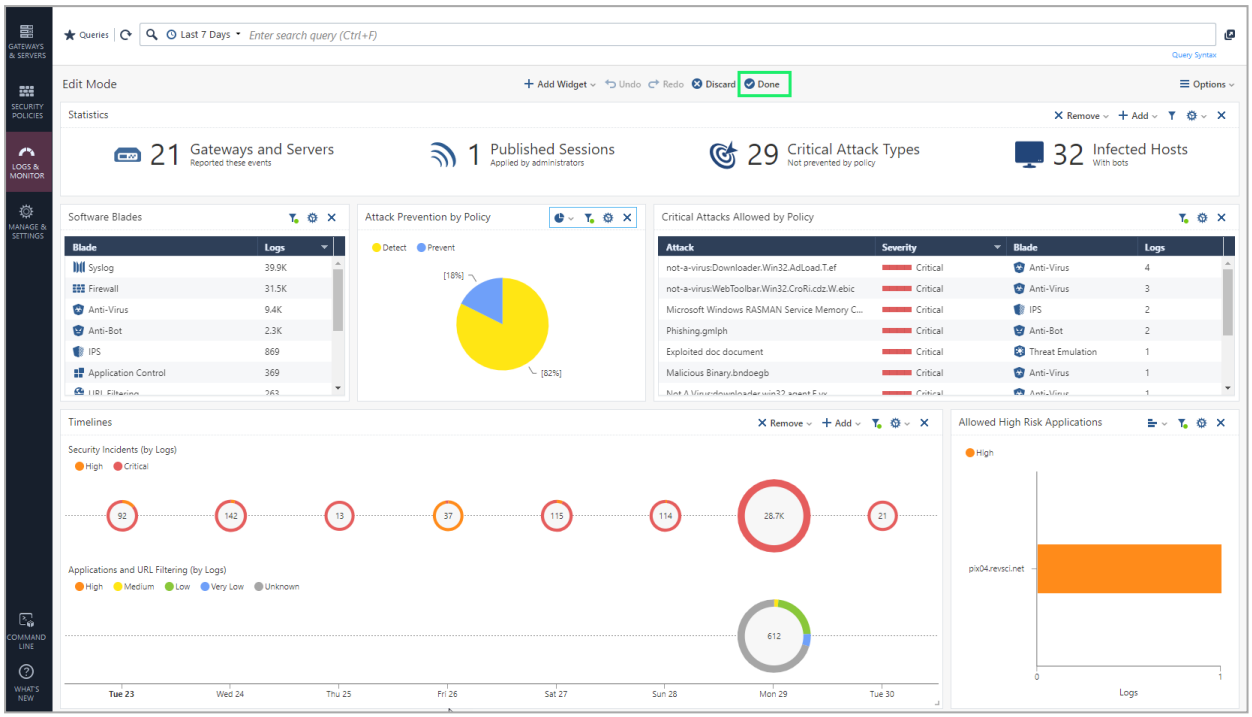


2. Go to the required widget and click the wheel icon to edit the image properties:.



3. Edit the required properties.

4. Click **Done**.

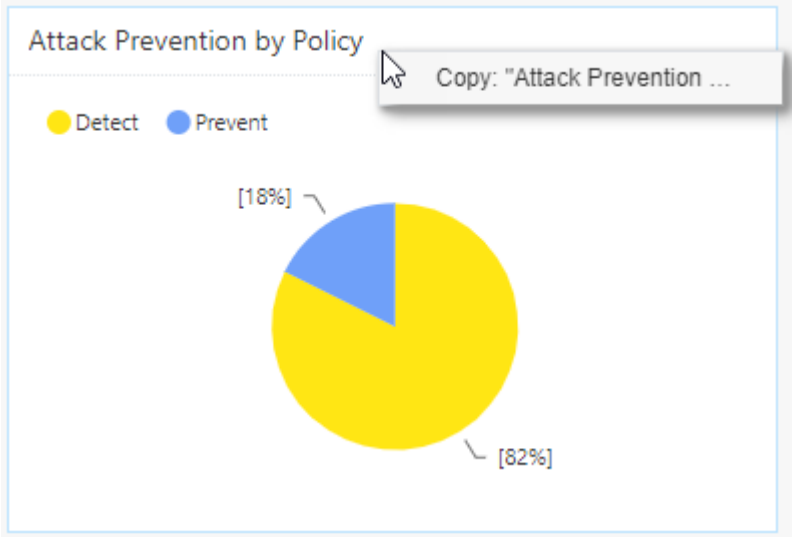


Copying Widgets and Views to other Locations

You can copy a widget used in one view or report and paste it in another view or report.

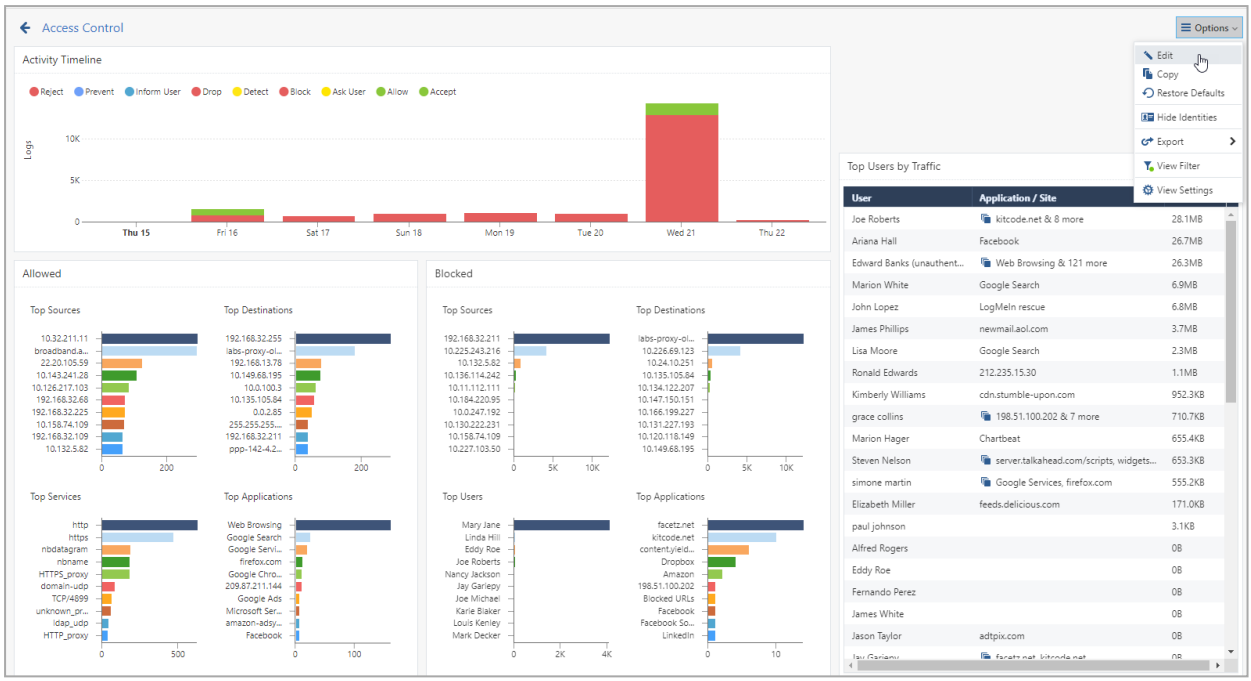
To copy a widget to another location:

1. Right-click the required widget.
2. The copy option shows with the name of the widget:



3. Select **Copy: [widget name]**.
4. Go to the view or report in which you want to paste the widget.

5. Go to **Options** and select **Edit**:



6. Right-click an empty space in the view or report.

   From the **Paste** drop-down menu, select the widget you want to paste:



7. Click **Done**.

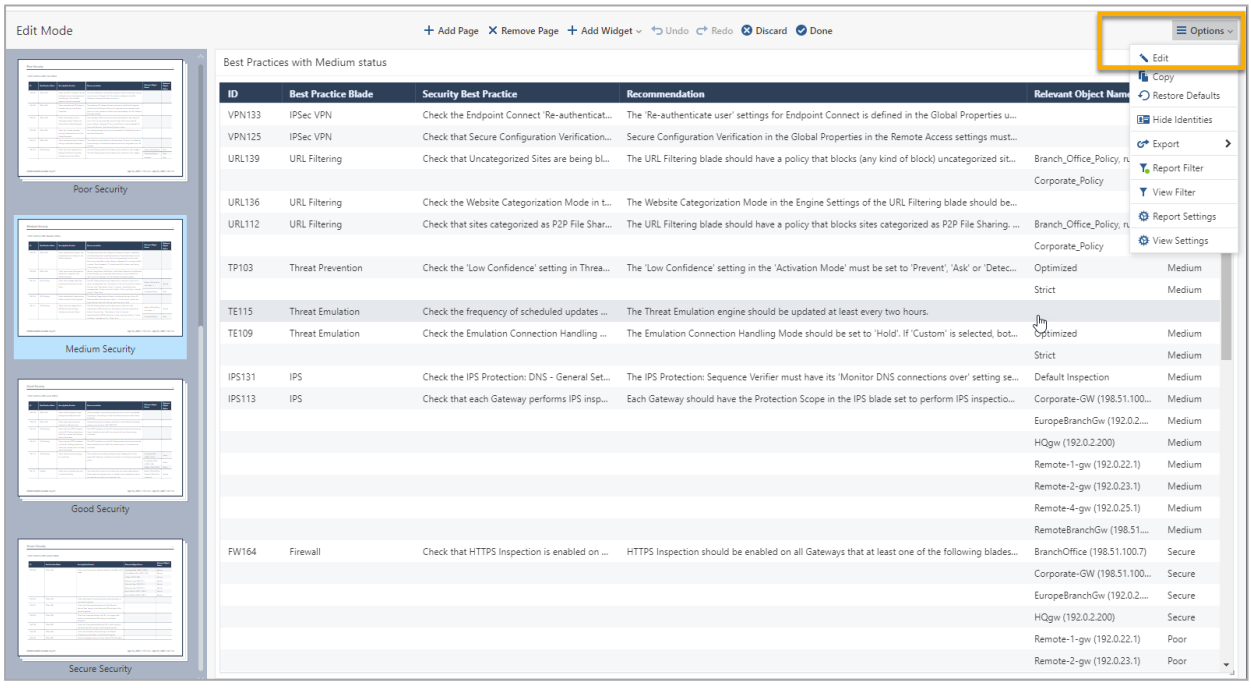
Note - When you copy a widget to another view or report, the copied widget does not include the filter of the original view or report, only the filter defined for the copied widget.

To copy a view to another report:

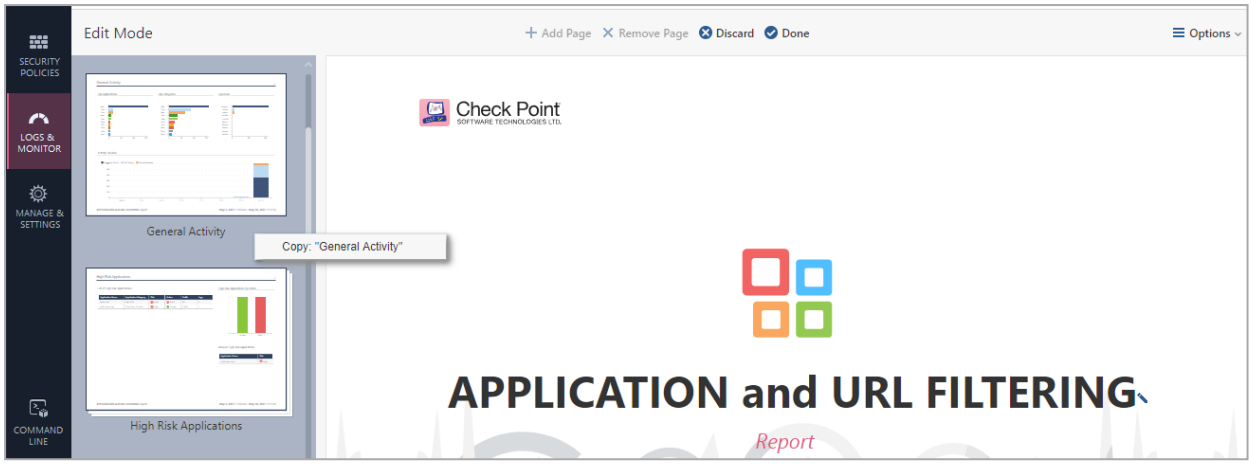
1. Right-click the required view.
2. The copy option shows with the name of the view:



3. Select **Copy: [view name]**
4. Go to the report in which you want to past the view.
5. Go to **Options** and select **Edit**:



6. Right-click an empty space in the report.
7. From the **Paste** drop-down menu, select the view you want to paste:

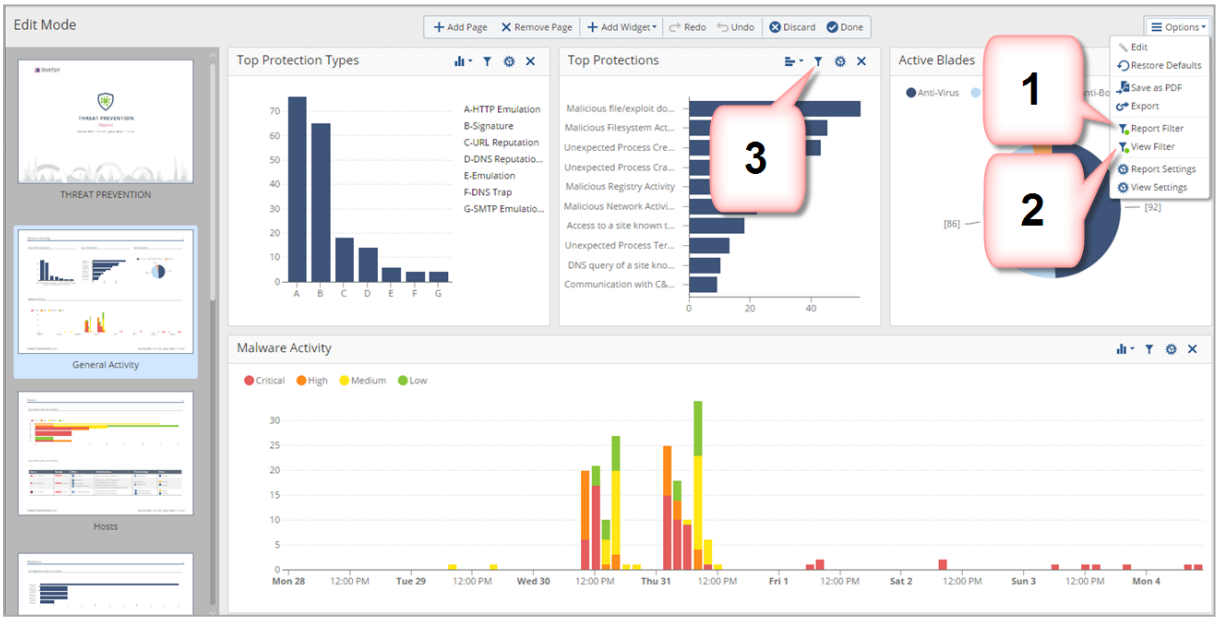


8. Click **Done**.

Note - When you copy a view to another report, the copied view does not include the filter of the original report, only the filter of the copied view.

Filters

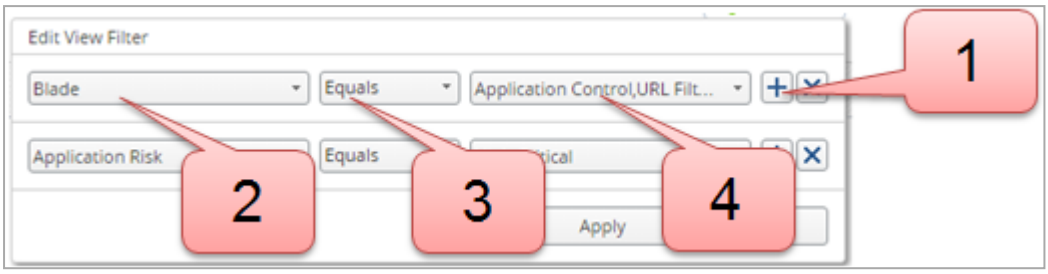
The search bar is used to apply on-demand filters, but you can also save filters with the view / report definition.



There are different layers of filters:

1. Filters to apply to the full report.
2. Filters to apply to a view (specified page in a report) and all widgets that this page includes.
3. Filters to apply to the selected widget.

To edit the 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.

Filtering for Active Directory User Groups

You can filter logs, reports, and views for one or more Active Directory groups.

1. In your Access Control Policy, create an Access Role that includes all the Active Directory groups you want to have in the query.
2. Install the Access Control Policy on the Security Gateways.
3. Look at the Identity Awareness login logs, and copy the names of the relevant groups. They usually have the prefix "**ad_**".
4. Add a filter for the field **User Group** and type or paste the name of the group that you want to include in the filter. For multiple groups, use a comma-separated list.

Logging

SmartConsole lets you transform log data into security intelligence. Search results are fast and immediately show the log records you need. The Security Gateways send logs to the Log Servers on the Security Management Server or on a dedicated server. Logs show on the SmartConsole **Logs & Monitor Logs** tab. You can:

- Quickly search through logs with simple Google-like searches.
- Select from many predefined search queries to find the applicable logs.
- Create your own queries using a powerful query language.
- Monitor logs from administrator activity and connections in real-time.

For more information, see *"Working with Logs" on page 76*.

Sample Log Analysis

This is a sample procedure that shows how to do an analysis of a log of a dropped connection.

To show a log of a dropped connection:

1. Log into SmartConsole.
2. Connect to the IP address of the Security Management Server, not to a Log Server.
3. In the **Security Policies** > **Access Control** > **Policy** view, select a rule with the **Drop** action.
4. In the bottom pane, click **Logs**.

   This shows the logs for connections that were dropped by the specific rule.
5. Double-click a log.

   The **Log Details** window opens.

Using the Logs View

In SmartConsole:

1. Go to **Logs and Monitoring** > **View**.
2. Click **New**, and select **New View**.
3. In the **New View** window, enter:

- **Name**
- **Category** - For example, select **Access Control**
- **Description** (optional)

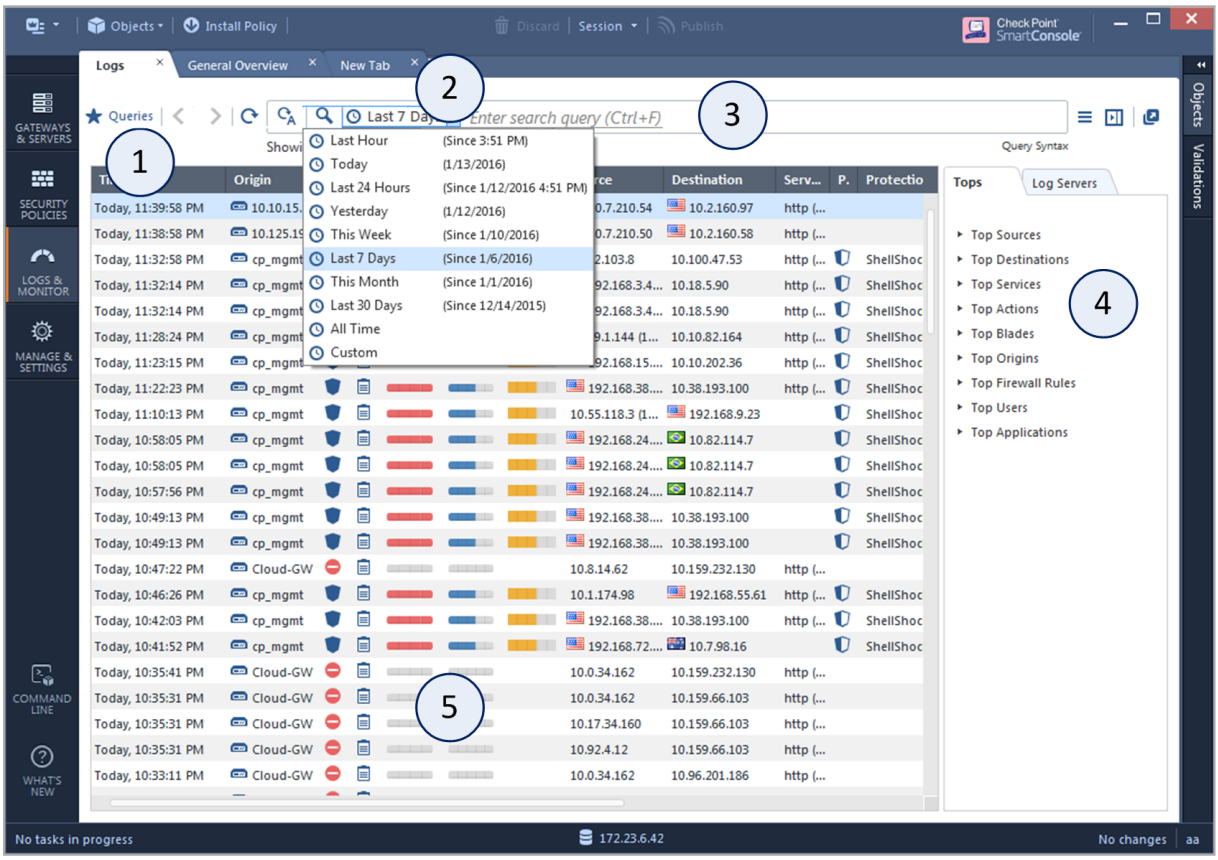
4. In the new window that opens, create a query. Click **Options** > **View Filter** and select blade and app control.
5. Click **Add Widget** to customize how you see the data that comes back from the query.

   Start with a **Timeline** of all events.

   In **Table**, you can create a table that contains multiple fields such as user, application name, and the amount of traffic. There are more widgets you can use: map, infographic, rich text, chart, and container (for multiple widgets).

   After you save the dashboard (done), you can schedule and get an automatic email at multiple intervals.

This is an example of the **Logs** view.



Item	Description
1	**Queries** - Predefined and favorite search queries.
2	**Time Period** - Search with predefined custom time periods.

Item	Description
3	**Query search bar** - Define custom queries in this field. You can use the GUI tools or manually enter query criteria. Shows the query definition for the most recent query.
4	**Log statistics pane** - Shows top results of the most recent query.
5	**Results pane** - Shows log entries for the most recent query.

Note - On a Security Management Server with the "Enable Log Indexing" option not selected, and a dedicated Log Server with "Enable Log Indexing" option selected: When you connect with SmartConsole to the Security Management Server, the **Logs** view shows the logs of individual log files. It is not possible to get a unified view of all the logs.

SmartView Web Application

Use Case - You are the system administrator at a small company and are concerned that some employees spend too much time looking at Facebook. You want a way to monitor the employee application use.

The SmartView Web Application is one of the SmartEvent clients that you can use to analyze events that occur in your environment. Use the SmartView Web Application to see an overview of the security information for your environment. It has the same real-time event monitoring and analysis views as SmartConsole. The convenience is that you do not have to install a client.

Note - SmartView graphics do not display properly in Internet Explorer. Accessing SmartEvent Server from the web (SmartView) is supported only from Google Chrome and Mozilla Firefox.

To log in to SmartEvent using SmartView Web Application:

Browse to:

```
https://<IP Address of Management Server>/smartview/
```

or

```
https://<Host Name of Management Server>/smartview/
```

Notes:

- The `/smartview/` part of the URL is case sensitive.
- Login to SmartView Web Application is supported only using Check Point Password authentication configured in the administrator object in SmartConsole.

SmartView advantages:

- Available for non-admin users
- Export up to 1,000,000 logs
- Integrated top statistics and docked card
- Support for High Contrast theme

In SmartView:

SmartView opens by default in the **General Overview** tab. This shows the statistics, Software Blades, timelines, and more. Any open tabs from the previous session are retained.

Note - SmartView Web Application is available even without SmartEvent Software Blade, but the default page is different.

To open a new tab, click **+**.

The **Audit Logs** tab shows audit logs which are changes done in the management.

The **Logs** > **Logs View** tab shows blade activities.

In SmartView, you first filter for the application and then by user.

1. Click the **+** icon to open a new tab.
2. Click **Views** > **Access Control**.
3. Right-click the **User** column and drill down to see the user activity or create a filter for this user in your current view.

You can schedule for all activities for a user, but cannot set the system to trigger an alert at a certain threshold.

To select which columns are shown:

1. Right-click on a column heading and select **Profile editor**.

   The **Profile editor** window opens.
2. Select fields to add to or remove from the selected profile.
3. Click **OK**.

To set user display preferences:

1. Click the drop-down arrow next to your user name and select **User Preferences**.
2. For **Locale**, select the display language.
3. For **First day of the week**, select the day of the week for the weekly logs to start.

4. For **Theme**, select **Default** or **High Contrast**.

   In **High Contrast**, the view display is white text on a black background.

5. In **Default time frame**, set the default timeframe for all the SmartView Web Application functionalities.

   The default value is Last 24 hours.

   Note - The default time frames on the SmartView Web Application and SmartConsole are **not** synchronized.

6. For **Email server settings**, select **Edit** to enter the email server details.

7. Click **OK**.

Exporting Logs

Apply a filter to select the logs you want to export. Currently, you can only export logs to CSV.

To export logs:

1. In the **Logs** tab, click **Options** and select **Export** > **Export to CSV**.

   The **CSV Export** window opens.

2. Select the **Logs Amount**.

3. Select the **Exported Columns** - **All columns** or **Visible columns**.

4. Click **OK**.

5. A popup window appears when the export process starts.

   When you see a message that the exported completed successfully, click **Download**.

   All exported logs also appear in the archive tab.

Working with Logs

This section explains how to work with logs.

Choosing Rules to Track

Logs are useful if they show the traffic patterns you are interested in. Make sure your Security Policy tracks all necessary rules. When you track multiple rules, the log file is large and requires more disk space and management operations.

To balance these requirements, track rules that can help you improve your cyber security, help you understand of user behavior, and are useful in reports.

Configuring Tracking in a Policy Rule

To configure tracking in a rule:

1. Right-click in the **Track** column.
2. Select a tracking option.
3. Install the policy.

Tracking Options

Select these options in the **Track** column of a rule:

- **None** - Do not generate a log.
- **Log** -This is the default **Track** option. It shows all the information that the Security Gateway used to match the connection. At a minimum, this is the Source, Destination, Source Port, and Destination Port. If there is a match on a rule that specifies an application, a session log shows the application name (for example, Dropbox). If there is a match on a rule that specifies a Data Type, the session log shows information about the files, and the contents of the files.
- **Accounting** - Select this to update the log at 10 minutes intervals, to show how much data has passed in the connection: Upload bytes, Download bytes, and browse time.

Note - When upgrading from R77.X or from R80 versions to R80.40, there are changes to the behavior of the options in the **Track** column. To learn more see sk116580.

Advanced Track options

Detailed Log and **Extended Log** are only available if one or more of these Blades are enabled on the Layer: *Application & URL Filtering*, *Content Awareness*, or *Mobile Access*.

- **Detailed Log** -Equivalent to the *Log* option, but also shows the application that matched the connections, even if the rule does not specify an application. **Best Practice** - Use for a cleanup rule (Any/internet/Accept) of an Applications and URL Filtering Policy Layer that was upgraded from an R77 Application Control Rule Base.
- **Extended Log** -Equivalent to the *Detailed* option, but also shows a full list of URLs and files in the connection or the session. The URLs and files show in the lower pane of the **Logs** view.

Note - The **Detailed Log** and **Extended Log** options have a higher performance impact on the Security Gateway than the **Log** option, because they inspect the packets and connections more thoroughly.

Log Generation

- **per Connection** - Select this to show a different log for each connection in the session. This is the default for rules in a Layer with only *Firewall* enabled. These are basic Firewall logs.

  Important - SmartEvent does not index these logs.

- **per Session** - Select this to generate one log for all the connections in the same session (see *"Log Sessions" below*). This is the default for rules in a Layer with *Application & URL Filtering* or *Content Awareness* enabled. These are basic Application Control logs.

Alert:

For each alert option, you can define a script in **Menu** > **Global properties** > **Log and Alert** > **Alerts**.

- **None** - Do not generate an alert.
- **Alert** - Generate a log of type Alert and run a command, such as: Show a popup window, send an email alert or an SNMP trap alert, or run a user-defined script as defined in the **Global Properties**.
- **SNMP** - Generate a log of type Alert and send an SNMP alert to the SNMP GUI, as defined in the **Global Properties**.
- **Mail** - Generate a log of type Alert and send an email to the administrator, as defined in the **Global Properties**.
- **User Defined Alert** - Generate a log of type Alert and send one of three possible customized alerts. The alerts are defined by the scripts specified in the **Global Properties**.

Log Sessions

A session is a user's activity at a specified site or with a specified application. The session starts when a *user* connects to an *application* or to a *site*. The Security Gateway includes all the activity that the user does in the session in one session log (in contrast to the Security Gateway log, which shows top sources, destinations, and services).

To search for log sessions:

In the **Logs** tab of the **Logs & Monitor** view, enter:

```
type:Session
```

To see details of the log session:

In the **Logs** tab of the **Logs & Monitor** view, select a session log.

In the bottom pane of the **Logs** tab, click the tabs to see details of the session log:

- **Connections** - Shows all the connections in the session. These show if **Per connection** is selected in the **Track** option of the rule.
- **URLs** - Shows all the URLs in the session. These show if **Extended Log** is selected in the **Track** option of the rule.
- **Files** - Shows all the files uploaded or downloaded in the session. These show if **Extended Log** is selected in the **Track** option of the rule, or if a Data Type was matched on the connection.

To see the session log for a connection that is part of a session:

1. In the **Logs** tab of the **Logs & Monitor** view, double-click on the log record of a connection that is part of a session.
2. In the **Log Details**, click the session icon (in the top-right corner) to search for the session log in a new tab.

To configure the session timeout:

By default, after a session continues for three hours, the Security Gateway starts a new session log. You can change this in SmartConsole from the **Manage & Settings** view, in **Blades** > **Application & URL Filtering** > **Advanced Settings** > **General** > **Connection unification**.

Viewing Rule Logs

You can search for the logs that are generated by a specific rule, from the Security Policy or from the **Logs & Monitor** > **Logs** tab.

To see logs generated by a rule (from the Security Policy):

1. In SmartConsole, go to the **Security Policies** view.
2. In the **Access Control Policy** or **Threat Prevention Policy**, select a rule.
3. In the bottom pane, click one of these tabs to see:
   - **Logs** - By default, shows the logs for the *Current Rule*. You can filter them by **Source**, **Destination**, **Blade**, **Action**, **Service**, **Port**, **Source Port**, **Rule** (**Current rule** is the default), **Origin**, **User**, or **Other Fields**.
   - **History** (Access Control Policy only) - List of rule operations (Audit logs) related to the rule in chronological order, with the information about the rule type and the administrator that made the change.

To see logs generated by a rule (by Searching the Logs):

1. In SmartConsole, go to the **Security Policies** view.
2. In the **Access Control Policy** or **Threat Prevention Policy**, select a rule.
3. Right-click the rule number and select **Copy Rule UID**.
4. In the **Logs & Monitor** > **Logs** tab, search for the logs in one of these ways:
   - Paste the Rule UID into the query search bar and click **Enter**.
   - For faster results, use this syntax in the query search bar:

     `layer_uuid_rule_uuid:*_<UID>`

     For example, paste this into the query search bar and click **Enter**:

     `layer_uuid_rule_uuid:*_46f0ee3b-026d-45b0-b7f0-5d71f6d8eb10`

Packet Capture

You can capture network traffic. The content of the packet capture provides a greater insight into the traffic which generated the log. With this feature activated, the Security Gateway sends a packet capture file with the log to the Log Server. You can open the file, or save it to a file location to retrieve the information a later time.

For some blades, the packet capture option is activated by default in Threat Policy.

To deactivate packet capture (in Threat Policy only):

1. In SmartConsole, go to the **Security Policies** view > **Threat Prevention**.
2. In the **Track** column of the rule, right-click and clear **Packet Capture**.

To see a packet capture:

1. In SmartConsole, go to the **Logs & Monitor** view.
2. Open the log.
3. Click the link in the **Packet Capture** field.

   The **Packet Capture** opens in a program associated with the file type.
4. **Optional:** Click **Save** to save the packet capture data on your computer.

Searching the Logs

SmartConsole lets you quickly and easily search the logs with many predefined log queries.

To see the predefined queries:

1. Open SmartConsole > **Logs & Monitor** view.
2. Click **Queries**.

To create your own queries, see *"Creating Custom Queries" on page 83*.

Running Queries

To create and run a query:

1. In the query search bar, click *Enter Search Query (Ctrl+F)*.
2. Enter or select query criteria.

To manually refresh your query:

 Click **Refresh (F5)**.

To continuously refresh your query (Auto-Refresh):

 Click **Auto - Refresh (F6)**. The icon is highlighted when Auto-Refresh is enabled.

The query continues to update every five seconds while Auto-Refresh is enabled.

If the number of logs exceeds 100 in a five-second period, the logs are aggregated, and the summary view shows.

Showing Query Results

Query results can include tens of thousands of log records. To prevent performance degradation, SmartConsole only shows the first set of results in the **Results** pane. Typically, this is a set of 50 results.

Scroll down to show more results. As you scroll down, SmartConsole extracts more records from the log index on the Security Management Server or Log Server, and adds them to the results set. See the number of results above the **Results** pane.

For example, on the first run of a query, you can see the first 50 results out of over 150,000 results. When you scroll down, you can see the first 100 results out of over 150,000.

The **Tops** pane, on the right side of the **Results** pane, shows the top statistics such as top sources, top actions, etc.

Note - Top statistics are estimated according to the partial log results already shown on the screen. They are not calculated for the entire query timeframe.

Notes:

- Top statistics are estimated according to the partial log results already shown on the screen. They are not calculated for the entire query timeframe.
- A query that refers to these log fields is not resolved:
  - `Scan result`
  - `Destination DNS Hostname`

Customizing the Results Pane

By default, SmartConsole shows a predefined set of columns and information based on the selected blade in your query. This is known as the **Column Profile**. For example:

- The DLP column profile includes columns for: Blade, Type, DLP Incident UID, and severity.
- The Threat Prevention column profile includes columns for: Origin, Action, Severity, and Source User.

A column profile is assigned based on the blade that occurs most frequently in the query results. This is called **Automatic Profile Selection**, and is enabled by default.

The Column Profile defines which columns show in the **Results Pane** and in which sequence. You can change the Column Profile as necessary for your environment.

To use the default Column Profile assignments:

- Right-click a column heading and select **Columns Profile** > **Automatic Profile Selection**.

To manually assign Column Profile assignments by default:

- Right-click a column heading and select **Columns Profile** > **Manual Profile Selection**.

To manually assign a different Column Profile:

1. Right-click a column heading and select **Columns Profile**.
2. Select a Column Profile from the options menu.

To change a Column Profile:

1. Right-click a column heading and select **Columns Profile** > **Edit Profile**.
2. In the **Show Fields** window, select a Column Profile to change.
3. Select fields to add from the **Available Fields** column.
4. Click **Add**.
5. Select fields to remove from the **Selected Fields** column.
6. Click **Remove**.

7. Select a field in the **Selected Fields**.
8. Click **Move Up** or **Move Down** to change its position in the **Results** Pane.
9. Double-click the Width column to change the default column width for the selected field.

To change the column width:

1. Drag the right column border in the **Results** Pane.
2. Right-click and select **Save Profile**.

   Changes made to the column are saved for future sessions.

Creating Custom Queries

Queries can include one or more criteria. You can modify an existing predefined query or create a new one in the query box.

To modify a predefined query:

Click inside the query box to add search filters.

To save the new query in the Favorites list:

1. Click **Queries** > **Add to Favorites**.

   The **Add to Favorites** window opens.
2. Enter a name for the query.
3. Select or create a new folder to store the query
4. Click **Add**.

Selecting Query Fields

You can enter query criteria directly from the query search bar.

To select field criteria:

1. If you start a new query, click **Clear**  to remove query definitions.
2. Put the cursor in the query search bar.
3. Select a criterion from the drop-down list or enter the criteria in the query search bar.

Using the Action Filter

One of the search filters is **Action**. When you select the **Action** filter, a list shows with all the log actions available for searching. This table lists and explains these log actions:

Action	Description
Accept	The Security Gateway allowed traffic based on the Access ControlSecurity Policy.
Allow	The Security Gateway allowed traffic after Firewall or a VPN alert (for example: Protocol Violation) or DLP match on an exception to a rule.
Ask User	■ The user was prompted to decide if the Security Gateway must block or allow specific traffic, based on Access Control or Custom Threat PreventionSecurity Policies. Or ■ A DLP incident was captured and put in quarantine. The user was asked to decide what to do.
Block	The Security Gateway blocked traffic based on a URL Filtering or Application Control rule, after a user opted a UserCheck block Action.
Bypass	Threat Emulation, Threat Extraction or Anti-Virus did not inspect a file.
Decrypt	The Security Gateway decrypted a VPN packet to reveal its content and allow further inspection.
Detect	A Threat Prevention blade detected malicious traffic but did not block it because it worked in the Detect mode.
Do not send	User decided to drop transmission that was captured by DLP. An administrator with full permissions or with the View, Release or Discard DLP messages permission can also drop these transmissions. Email notification was sent to the user.
Drop	The Security Gateway blocked traffic based on the Access ControlSecurity Policy and did not notify the source.
Encrypt	The Security Gateway encrypted a VPN packet to secure its contents and prevent unauthorized access.
Extract	Threat Extraction extracted potentially malicious content from a file before the file entered the network.
Forgot Passcode	User tapped **Forgot Passcode** in the Capsule Workspace application.
HTTPS Bypass	The Security Gateway allowed network traffic to bypass HTTPS Inspection.
HTTPS Inspect	The Security Gateway inspected HTTPS traffic.

Action	Description
Inform User	■ The user was informed what the organization's policy was, based on the Access Control or Custom Threat PreventionSecurity Policies. Or ■ DLP transmission was detected and allowed, and the user was notified.
Inline	Traffic was sent for emulation before it was allowed to enter the internal network.
Inspect	Threat Emulation or Anti-Virus inspected a fie.
IP Changed	An association between a specific IP address and a user changed, because the IP address on the associated host changed (DHCP).
Key Install	The Security Gateway created encryption keys for VPN.
Open Shell	An administrator opened a command shell to a Gaia server.
Packet Tagging	The Security Gateway shared a packet tagging key with an Identity Agent.
Prevent	The Security Gateway blocked traffic based on the DLP or Threat Prevention policy.
Quarantine	The Security Gateway isolated an email that was identified as a potential security threat, until further investigation is made..
Reject	The Security Gateway rejected the packet and notified the source with the TCP [RST] packet.
Remote Wipe	The Security Gateway removed offline data cached on a user mobile device with Capsule Workspace Application.
Reset Passcode	User tapped **Reset Passcode** in the Capsule Workspace application.
Run Script	An administrator executed a script on a Gaia server from SmartConsole.
Send	User decided to continue transmission after DLP capture. An administrator with full permissions or with the View/Release/Discard DLP messages permission can also decide to continue transmission. Email notification is sent to the user.
System Backup	An administrator backed up the configuration of the GaiaOperating System of the Security Gateway.

Action	Description
System Restore	An administrator retrieved a backup file and restored configuration of the GaiaOperating System of the Security Gateway.
Update	The Security Gateway downloaded and installed the latest version or Hotfix.
VPN Routing	The Security Gateway directed the VPN traffic through the appropriate specific VPN tunnel or Security Gateway.

Selecting Criteria from Grid Columns

You can use the column headings in the **Grid** view to select query criteria. This option is not available in the **Table** view.

To select query criteria from grid columns:

1. In the **Results** pane, right-click on a column heading.
2. Select **Add Filter**.
3. Select or enter the filter criteria.
   The criteria show in the **Query search bar** and the query runs automatically.

To enter more criteria, use this procedure or other procedures.

Manually Entering Query Criteria

You can enter query criteria directly in the **Query search bar**. You can manually create a new query or make changes to an existing query that shows in the **Query search bar**.

As you enter text, the **Search** shows recently used query criteria or full queries. To use these search suggestions, select them from the drop-down list.

Query Language Overview

A powerful query language lets you show only selected records from the log files, according to your criteria. To create complex queries, use Boolean operators, wildcards, fields, and ranges. This section refers in detail to the query language.

When you use SmartConsole to create a query, the applicable criteria show in the **Query search bar**.

The basic query syntax is `[<Field>:] <Filter Criterion>`.

To put together many criteria in one query, use Boolean operators:

```
[<Field>:] <Filter Criterion> {AND|OR|NOT} [<Field>:] <Filter Criterion> ...
```

Most query keywords and filter criteria are not case sensitive, but there are some exceptions. For example, "`source:<X>`" is case sensitive ("`Source:<X>`" does not match). If your query results do not show the expected results, change the case of your query criteria, or try upper and lower case.

When you use queries with more than one criteria value, an AND is implied automatically, so there is no need to add it. Enter OR or other boolean operators if needed.

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 and IPv6 addresses used in log queries are counted as one word. Enter IPv4 address with dotted decimal notation and IPv6 addresses with colons.

Example:

- 192.0.2.1
- 2001:db8::f00:d

You can also use the *wildcard* '`*`' character and the *standard network suffix* to search for logs that match IP addresses within a range.

Examples:

- src:192.168.0.0/16 (shows all records for the source IP 192.168.0.0 to 192.168.255.255 inclusive)
- src:192.168.1.0/24 (shows all records for the source IP 192.168.1.0 to 192.168.1.255 inclusive)
- src:192.168.2.* shows all records for the source IP 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

NOT Values

You can use NOT *<field>* values with *Field Keywords* in log queries to find logs for which the value of the field is not the value in the query.

Syntax

```
NOT <field>: <value>
```

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. You can use more than the wildcard character.

Wildcard syntax:

- The **?** (question mark) matches one character.
- The ***** (asterisk) matches a character string.

Examples:

- Jo? shows Joe and Jon, but not Joseph.
- Jo* shows Jon, Joseph, and John Paul.

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.

Note – Using a single '`*`' creates a search for a non-empty value string. For example assetname:*

Field Keywords

You can use predefined field names as keywords in filter criteria. The query result only shows log records that match the criteria in the specified field. If you do not use field names, the query result shows records that match 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.

Keyword	Keyword Alias	Description
`severity`		Severity of the event
`app_risk`		Potential risk from the application, of the event
`protection`		Name of the protection
`protection_type`		Type of protection
`confidence_level`		Level of confidence that an event is malicious
`action`		Action taken by a security rule
`blade`	`product`	Software Blade
`destination`	`dst`	Traffic destination IP address, DNS name or Check Point network object name
`origin`	`orig`	Name of originating Security Gateway
`service`		Service that generated the log entry
`source`	`src`	Traffic source IP address, DNS name or Check Point network object name
`user`		User name

Syntax for a field name query:

`<field name>:<values>`

- ***<field name>*** - One of the predefined field names
- ***<values>*** - One or more filters

To search for rule number, use the **Rule** field name. For example:

```
rule:7.1
```

If you use the rule number as a filter, rules in all the Layers with that number are matched.

To search for a rule name, you must not use the **Rule** field. Use free text. For example:

```
"Block Credit Cards"
```

Best Practice - Do a free text search for the rule name. Make sure rule names are unique and not reused in different Layers.

Examples:

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

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

Important - When you use fields with multiple values, you must:

- Write the Boolean operator, for example **AND**.
- Use parentheses.

Boolean Operators

You can use the Boolean operators **AND** , **OR** , and **NOT** to create filters with many different criteria. You can put multiple Boolean expressions in parentheses.

If you enter more than one criteria without a Boolean operator, the **AND** operator is implied. When you use multiple criteria without parentheses, the **OR** operator is applied before the **AND** operator.

Examples:

- `blade:"application control" AND action:block`

  Shows log records from the Application and URL FilteringSoftware Blade where traffic was blocked.

- `192.168.2.133 10.19.136.101`

  Shows log entries that match the two IP addresses. The **AND** operator is presumed.

- `192.168.2.133 OR 10.19.136.101`

  Shows log entries that match one of the IP addresses.

- `(blade: Firewall OR blade: IPS OR blade:VPN) AND NOT action:drop`

  Shows 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`

  Shows 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.

Log Server High Availability

In SmartConsole, you can configure a Security Gateway, that when it fails to send its logs to one Log Server, it will send its logs to a secondary Log Server. To support this configuration, you can add Log Servers to a single SmartEvent Correlation Unit. In this way, the SmartEvent Correlation Unit gets an uninterrupted stream of logs from both servers and continues to correlate all logs.

Working with Syslog Servers

Introduction

Syslog (System Logging Protocol) is a standard protocol used to send system log or event messages to a specific server, the *syslog server*.

The syslog protocol is enabled on most network devices, such as routers and switches.

Syslog is used by many log analysis tools. If you want to use these tools, make sure Check Point logs are sent to from the Security Gateway to the syslog server in syslog format.

Check Point supports these syslog protocols: RFC 3164 (old) and RFC 5424 (new).

These features are **not** supported: IPv6 logs and Software Blade logs.

Configuring Security Gateways

By default, Security Gateway logs are sent to the Security Management Server.

You can configure Security Gateways to send logs directly to syslog servers.

Important - Syslog is not an encrypted protocol. Make sure the Security Gateway and the Log Proxy are located close to each other and that they communicate over a secure network.

Procedure

1. Define syslog server objects in SmartConsole.

   Instructions

   a. Connect with SmartConsole to the Management Server.

   b. From the left navigation panel, click **Gateways & Servers**.

c. Create the **Host** object that represents the Syslog server host.

i. In the Object Explorer, click **New** > **Host**.

ii. Configure these fields:

- **Name** - Enter a unique name.
- **IPv4 address** - Enter the correct IPv4 address of the syslog server.
- **IPv6 address** - Optional: Enter the correct IPv6 address of the syslog server. This requires the IPv6 Support be enabled on the Security Gateway / each Cluster Member.

iii. Click **OK**.

d. Create the **Syslog Server** object that represents the Syslog server:

i. In the Object Explorer, click **New** > **Server** > **More** > **Syslog**.

ii. Configure these fields:

- **Name** - Enter a unique name.
- **Host** - Select an existing host or click **New** to define a new computer or appliance.
- **Port** - Enter the correct port number on the syslog server (default = 514).
- **Version** - Select **BSD Protocol** or **Syslog Protocol**.

iii. Click **OK**.

e. Close the Object Explorer.

2. Select the configured syslog server objects in the Security Gateway / Cluster object.

Instructions

a. Double-click the Security Gateway object.

b. From the left tree, click **Logs**.

c. In the **Send logs and alerts to these log servers** table, click the green (**+**) button to select the **Syslog Server** object(s) you configured earlier.

Notes:

- You can configure a Security Gateway / Cluster Member to send logs to multiple syslog servers.

  All syslog servers selected in the Security Gateway / Cluster object must use the same protocol version: *BSD Protocol* or *Syslog Protocol*.

- You cannot configure a Syslog server as a backup server.

d. Click **OK**.

e. Install policy.

3. Configure the logging properties of the Security Gateways / each Cluster Member.

   The kernel parameter `fwsyslog_enable` optimizes logging performance in environments that require high log rates.

   Enable this kernel parameter only if explicitly instructed by Check Point Support.

   - `fwsyslog_enable=0`: Firewall logs are sent to the Syslog Server through the user space Syslog daemon (this is the default).
   - `fwsyslog_enable=1`: Firewall logs are sent to the Syslog Server directly from the Gaia OS kernel.

   Note - In a Cluster, you must configure each Cluster Member in the same way.

   To see the current state of the `fwsyslog_enable` parameter

   a. Connect to the command line on the Security Gateway / each Cluster Member.

   b. Log in to the Expert mode.

   c. Run:

   ```
   fw ctl get int fwsyslog_enable
   ```

   Output:

   - "`fwsyslog_enable = 0`" means that Firewall logs are sent to the Syslog Server through the user space Syslog daemon (this is the default).
   - "`fwsyslog_enable = 1`" means Firewall logs are sent to the Syslog Server directly from the Gaia OS kernel.

To set the state of the `fwsyslog_enable` parameter to (1) temporarily (does not survive reboot)

a. Connect to the command line on the Security Gateway / each Cluster Member.

b. Log in to the Expert mode.

c. Run:

```
fw ctl set int fwsyslog_enable 1
```

d. In SmartConsole, install policy on this Security Gateway / Cluster object.

To set the state of the `fwsyslog_enable` parameter to (1) permanently (survives reboot)

a. Connect to the command line on the Security Gateway / each Cluster Member.

b. Log in to the Expert mode.

c. Edit the `$FWDIR/boot/modules/fwkern.conf` file:

```
vi $FWDIR/boot/modules/fwkern.conf
```

d. Add this line:

```
fwsyslog_enable=1
```

e. Save the changes in the file and exit the editor.

f. Reboot the Security Gateway / each Cluster Member.

To set the state of the `fwsyslog_enable` parameter to (0) temporarily (does not survive reboot)

a. Connect to the command line on the Security Gateway / each Cluster Member.

b. Log in to the Expert mode.

c. Run:

```
fw ctl set int fwsyslog_enable 0
```

To set the state of the `fwsyslog_enable` parameter to (0) permanently (survives reboot)

a. Connect to the command line on the Security Gateway / each Cluster Member.

b. Log in to the Expert mode.

c. Edit the `$FWDIR/boot/modules/fwkern.conf` file:

```
vi $FWDIR/boot/modules/fwkern.conf
```

d. Do *one* of these actions:

- Set the value of the kernel parameter to 0:

  ```
  fwsyslog_enable=0
  ```

- Delete the entire line:

  ```
  fwsyslog_enable=1
  ```

e. Save the changes in the file and exit the editor.

f. Reboot the Security Gateway / each Cluster Member.

Log Count for CoreXL Firewall Instances

You can see the current number of syslog logs sent by CoreXL Firewall Instances on the Security Gateway / each Cluster Member.

To see log count for a CoreXL Firewall instance

1. Connect to the command line on the Security Gateway / each Cluster Member.
2. Log in to the Expert mode.
3. Run:

   ```
   fw -i <CoreXL Firewall Instance Number> ctl get fwsyslog_
   nlogs_counter
   ```

   Sample output:

   ```
   fwsyslog_nlogs_counter = 21
   ```

To see log count for all CoreXL Firewall instances

1. Make two command line connections to the Security Gateway / each Cluster Member.
2. In each command line connection, log in to the Expert mode.
3. In the first shell, run:

   ```
   fw ctl zdebug | grep logs
   ```

4. In the second shell, run:

   ```
   fw ctl set int fwsyslog_print_counter 1
   ```

5. In the first shell, see the counter for each CoreXL Firewall instance and the sum of all CoreXL Firewall instances.

Sample output:

```
;[cpu_2];[fw4_0];Number of logs sent from instance 0 is 43;
;[cpu_2];[fw4_0];Number of logs sent from instance 1 is 39;
;[cpu_2];[fw4_0];Number of logs sent from instance 2 is 50;
;[cpu_2];[fw4_0];Total logs sent from kernel (all instances)
= 132;
```

6. In the first shell, press CTRL+C to stop the debug.

For more on syslog, see: *"Appendix: Manual Syslog Parsing" on page 230*.

Event Analysis

This section deals with analyzing events.

Event Analysis with SmartEvent

The SmartEvent Software Blade is a unified security event management and analysis solution that delivers real-time, graphical threat management information. SmartConsole, SmartView Web Application, and the SmartEvent GUI client consolidate billions of logs and show them as prioritized security events so you can immediately respond to security incidents, and do the necessary actions to prevent more attacks. You can customize the views to monitor the events that are most important to you. You can move from a high level view to detailed forensic analysis in a few clicks. With the free-text search and suggestions, you can quickly run data analysis and identify critical security events.

What is an Event?

An *event* is a record of a security incident. It is based on one or more logs, and on rules that are defined in the Event Policy.

An example of an event that is based on one log: A High Severity Anti-Bot event. One Anti-Bot log with a Severity of High causes the event to be recorded.

An example of an event that is based on more than one log: A Certificate Sharing event. Two login logs with the same certificate and a different user cause the event to be recorded.

How Are Logs Converted to Events?

SmartEvent automatically defines logs that are not Firewall, VPN, or HTTPS Inspection logs, as events.

Events that are based on a suspicious pattern of one or more logs, are created by the SmartEvent Correlation Unit. These *correlated events* are defined in the SmartEvent client GUI, in the Policy tab.

Most logs are Firewall, VPN and HTTPS inspection logs. Therefore, SmartEvent does not define them as events by default to avoid a performance impact on the SmartEvent Server.

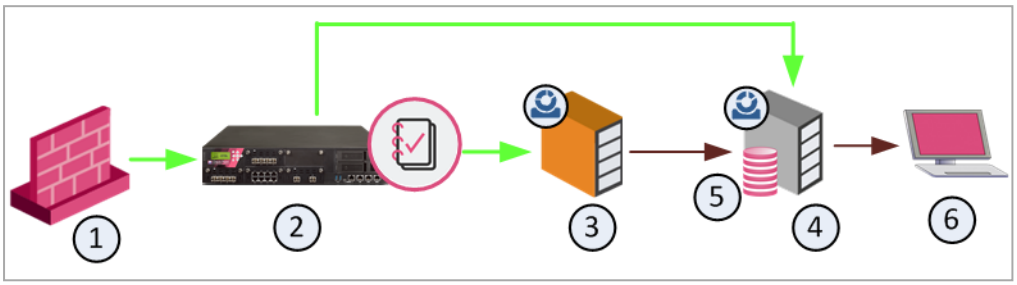
For logs from Security Gateways R77.X and lower: To create events for Firewall, in the SmartEvent Policy tab, enable **Consolidated Sessions > Firewall Session**.

The SmartEvent Architecture

SmartEvent has some components that work together to help track down security threats and make your network more secure.

This is how they work together. The numbers refer to the diagram:

- SmartEvent Correlation Unit (3) analyzes log entries on Log Servers (2) and stores the event in the same way the log server stores logs.
- SmartEvent Server (4) contains the Events Database (5).
- The SmartEvent and SmartConsole clients (6) manage the SmartEvent Server.



Item	Description	Purpose
	→	Log data flow
	→	Event data flow
1	Check Point Security Gateway	Sends logs to the Log Server.
2	Log Server	Stores logs.
3	SmartEvent Correlation Unit	Identifies events: Analyzes each log entry from a Log Server, and looks for patterns according to the installed *Event Policy*. The logs contain data from Check Point products and certain third-party devices. When a threat pattern is identified, the SmartEvent Correlation Unit forwards the *event* to the SmartEvent Server.
4	SmartEvent Server	The SmartEvent Server: ■ Indexes logs for SmartView ■ Defines the event policy ■ Manages correlation units
5	Events database	Stores events. Located on the SmartEvent Server.

Item	Description	Purpose
6	SmartEvent client	Shows the received events. Uses the clients to manage events (for example: to filter and close events), fine-tunes, and installs the Event Policy. The clients are: ■ SmartConsole ■ SmartView Web Application

The SmartEvent components can be installed on one computer (that is, a standalone deployment) or multiple computers and sites (a distributed deployment). To handle higher volumes of logging activity, we recommend a distributed deployment. Each SmartEvent Correlation Unit can analyze logs from more than one Log Server or Domain Log Server.

SmartEvent Correlation Unit

The SmartEvent Correlation Unit analyzes the log entries and identifies events from them. During analysis, the SmartEvent Correlation Unit:

- Marks log entries that are not stand-alone events, but can be part of a larger pattern to be identified later.
- Takes a log entry that meets one of the criteria set in the Events Policy, and generates an event.
- Takes a new log entry that is part of a group of items. Together, all these items make up a security event. The SmartEvent Correlation Unit adds it to an ongoing event.
- Discards log entries that do not meet event criteria.

SmartEvent Correlation Unit High Availability

Multiple correlation units can read logs from the same Log Servers. That way, the units provide redundancy if one of them fails. The events that the Correlation Units detect are duplicated in the SmartEvent database. But these events can be disambiguated if you filter them with the **Detected By field** in the Event Query definition. The **Detected By field** specifies which SmartEvent Correlation Unit detected the event.

Configuring SmartEvent Policy and Settings

This section discusses how to configure SmartEvent policy and settings.

Opening the SmartEvent GUI Client

Use the Policy tab of the SmartEvent GUI client to configure and customize the events that define the SmartEvent Policy.

To open the SmartEvent GUI client:

1. Open SmartConsole > **Logs & Monitor**.
2. Click (**+**) to open a Catalog (new tab).
3. Click **SmartEvent Settings & Policy**.

Policy Tab

Define the Event **Policy** in the Event **Policy** tab. Most configuration steps occur in the **Policy** tab. You define system components, such as SmartEvent Correlation Unit, lists of blocked IP addresses and other general settings.

The types of events that SmartEvent can detect are listed here, and sorted into a number of categories. To change each event, change the default thresholds and set Automated Responses. You can also disable events.

The **Policy** tab has these sections:

- **Selector Tree** - The navigation pane.
- **Detail pane** - The settings of each item in the **Selector Tree**.
- **Description pane** - A description of the selected item.

You can edit the event policy in one of these ways:

- Fine-tune the Event Policy.
- Change the existing Event Definition to see the events that interest you in *"Modifying Event Definitions" on the next page*.
- Create new Event Definitions to see the events that are not included in the existing definitions.

Save Event Policy

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

To enable changes made to the Event Policy:

1. Click **File** > **Save**.
2. Click **Actions** > **Install Event Policy**.

Revert Changes

You can undo changes to the **Event Policy**, if they were not saved.

To undo changes: click **File** > **Revert Changes**.

Event Definitions and General Settings

The **Selector tree** is divided into two branches: **Event Policy** and **General Settings**. The events detectable by SmartEvent are organized by category in the **Event Policy** branch. Select an event definition to show its configurable properties in the **Detail** pane, and a description of the event in the **Description** pane. Clear the property to remove this event type from the Event Policy the next time the Event Policy is installed.

The **General Settings** branch contains **Initial Settings**. For example: To define SmartEvent Correlation Unit, which is typically used for the initial configuration. Click a **General Settings** item to show its configurable properties in the Detail pane.

For details on specified attacks or events, refer to the **Event Definition Detail** pane.

Event Definition Parameters

When an event definition is selected, its configurable elements appear in the **Detail** pane, and a description of the event is displayed in the **Description** pane. These are the usual types of configurable elements:

- Thresholds, such as **Detect the event when more than x connections were detected over y seconds**
- **Severity**, such as **Critical**, **Medium**, **Informational**, etc.
- *"Automatic Reactions" on the next page* such as **Block Source** or run **External Script**
- *"Exceptions" on page 111*
- **Time Object**, such as to issue an event if the following occurs outside the following **Working Hours**

Not all of these elements appear for every Event Definition. After you install and run SmartEvent for a short time, you will discover which of these elements need to be fine-tuned per Event Definition.

For configuration information regarding most objects in **General Settings**, see *"System Administration" on page 131*.

Modifying Event Definitions

SmartEvent constantly takes data from your Log Servers, and searches for patterns in all the network chatter that enters your system.

Depending on the levels set in each Event Definition, the number of events detected can be high. But only a portion of those events can be meaningful. You can change the thresholds and other criteria of an event, to reduce the number of false alarms.

Event Threshold

The Event Threshold allows you to modify the limits that, when exceeded, indicate that an event occurred. Limits include the number of logs, and the timeframe in which they occurred:

Detect the event when more than *X* logs were detected over a period of *Y* seconds.

To decrease the number of false alarms based on a particular event, increase the number of logs and/or the timeframe for them to occur.

Severity

To modify the severity of an event, select a severity level from the drop-down list.

If the event is based on Threat Prevention logs, the event gets the severity from the protection type, not from the severity configured here.

To overwrite the severity:

1. Go to **SmartEvent** > **Policy**.
2. Select an event and right-click > **Select Properties**.

   The **Edit Event Definition** window opens.
3. In the **Event Format** tab, select **Determine event's display name and severity from event logs**.

Automatic Reactions

When detected, an event can activate an Automatic Reaction. The SmartEvent administrator can create and configure one Automatic Reaction, or many, according to the needs of the system.

For example: A Mail Reaction can be defined to tell the administrator of events to which it is applied. Multiple Automatic Mail Reactions can be created to tell a different responsible party for each type of event.

To create an automatic reaction:

1. Create an automatic reaction object in the Event definition, or from **General Settings** > **Objects** > **Automatic Reactions**.
2. Assign the Automatic Reaction to an event (or to an exception to the event).
3. To save the Event Policy, click **File** > **Save**
4. To install the Event Policy on the SmartEvent Correlation Unit, click **Actions** > **Install Event Policy**.

These are the types of Automatic Reactions:

- **Mail** - Tell an administrator by email that the event occurred. See *"Creating a Mail Reaction" on page 107*.
- **Block Source** - Instruct the Security Gateway to block the source IP address from which this event was detected for a configurable timeframe . Select a timeframe from one minute to more than three weeks. See *"Creating a Block Source Reaction" on page 108*.
- **Block Event activity** - Instruct the Security Gateway to block a distributed attack that emanates from multiple sources, or attacks multiple destinations for a configurable timeframe. Select a timeframe from one minute to more than three weeks). See *"Creating a Block Event Activity Reaction" on page 108*.
- **External Script** - Run a script that you provide. See *"Creating an External Script Automatic Reaction" on page 109* to write a script that can exploit SmartEvent data.
- **SNMP Trap** - Generate an SNMP Trap. See *"Creating an SNMP Trap Reaction" on page 108*.

  You can send event fields in the SNMP Trap message.

  The format for such an event field is `[seam_event_table_field]`.

  This list represents the possible **seam_event** table fields:

  AdditionalInfo varchar(1024)

  AutoReactionStatus varchar(1024)

  Category varchar(1024)

  DetectedBy integer

  DetectionTime integer

  Direction integer

  DueDate integer

  EndTime integer

  EventNumber integer

  FollowUp integer

  IsLast integer

  LastUpdateTime integer

  MaxNumOfConnections integer

  Name varchar(1024), NumOfAcceptedConnections integer

  NumOfRejectedConnections integer

  NumOfUpdates integer

ProductCategory varchar(1024)

ProductName varchar(1024)

Remarks varchar(1024)

RuleID varchar(48)

Severity integer

StartTime integer

State integer

TimeInterval integer

TotalNumOfConnections varchar(20)

User varchar(1024)

Uuid varchar(48)

aba_customer varchar(1024)

jobID varchar(48)

policyRuleID varchar(48)

Creating a Mail Reaction

1. Select **Add** > **Mail**.
2. Give the automatic reaction a significant name.
3. Fill out the **Mail Parameters of From**, **To** and **cc**.
4. To add multiple recipients, separate each email address with a semi-colon.

   Note - The **Subject** field has the default variables of *[EventNumber] - [Severity] - [Name].* These variables automatically adds to the mail subject the event number, severity and name of the event that triggered this reaction. These variables can be removed at your discretion.
5. Optional: Include your own standard text for each mail reaction.
6. Enter the domain name of the SMTP server.
7. Select **Save**.

Creating an SNMP Trap Reaction

1. Select **Add** > **SNMP Trap**.
2. Give the automatic reaction a significant name.
3. Fill out the **SNMP Trap parameters** of **Host**, **Message**, **OID** and **Community name**.

The command `send_snmp` uses values that are found in the file **chkpnnt.mib**, in the directory `$CPDIR/lib/snmp/`. An **OID** value used in the **SNMP Trap parameters** window must be defined in **chkpnnt.mib**, or in a file that refers it. If the **OID** field is left blank, the value is determined from **iso.org.dod.internet.private.enterprises.checkpoint.products.fw.fwEvent = 1.3.6.1.4.1.2620.1.1.11**.

When the automatic reaction occurs, the SNMP Trap is sent as a 256 byte `DisplayString` text. But, if the OID type is not text, the message is not sent.

4. Select **Save**.

Creating a Block Source Reaction

1. Select **Add** > **Block Source**.
2. Give the automatic reaction a significant name.
3. From the drop-down list, select the number of minutes to block this source.
4. Select **Save**.

Creating a Block Event Activity Reaction

1. Select **Add** > **Block Event Activity**.
2. Give the automatic reaction a significant name.
3. From the drop-down list, select the number of minutes to block this source.
4. Select **Save**.

Creating an External Script Automatic Reaction

To add an External Script:

1. Create the script.
2. Put the script on the SmartEvent Server
   a. In `$RTDIR/bin`, create the folder `ext_commands`:

      ```
      mkdir $RTDIR/bin/ext_commands
      ```

   b. Put the script in `$RTDIR/bin/ext_commands/` or in a folder under that location.

      The path and script name must not contain any spaces.

   c. Give the script executable permissions:

      ```
      chmod +x <script_filename>
      ```

3. In the SmartEvent GUI client **Policy** tab, in **Automatic Reactions**, Select **Add** > **External Script**.
4. In the **Add Automatic Reaction** window
   a. Give the automatic reaction object a significant Name.
   b. In Command line, enter the name of the script to run. Specify the name of the script that is in `$RTDIR/bin/ext_commands/` directory. Use the relative path if needed. Do not specify the full path of `$RTDIR/bin/ext_commands/`.
   c. Select **Save**.

Guidelines for creating the script

- Run the script manually and make sure it works as expected
- Make sure the script runs for no longer than 10 minutes, otherwise it will be terminated by the SmartEvent Server.
- Use the event fields in the script:

  To refer to the event in the script, define this environment variable:

  ```
  EVENT=$(cat)
  ```

  and use `$EVENT`

  Use line editor commands like `awk` or `sed` to parse the event and refer to specific fields. You can print the `$EVENT` one time to see its format.

  The format of the event content is a name-value set - a structured set of fields that have the form:

  ```
  (name: value ;* );
  ```

  where name is a string and value is either free text until a semicolon, or a nested name-value set.

  This is a sample event:

```
(Name: Check Pointadministrator credential guessing; RuleID:
{F182D6BC-A0AA-444a-9F31-C0C22ACA2114}; Uuid:
<42135c9c,00000000,2e1510ac,131c07b6>; NumOfUpdates: 0;
IsLast: 0;
StartTime: 16Feb2015 16:45:45; EndTime: Not Completed;
DetectionTime:
16Feb2015 16:45:48; LastUpdateTime: 0; TimeInterval: 600;
MaxNumOfConnections: 3; TotalNumOfConnections: 3; DetectedBy:
2886735150;
Origin: (IP: 192.0.2.4; repetitions: 3; countryname: United
States;
hostname: theHost) ; ProductName: SmartDashboard; User: XYZ;
Source:
(hostname: theHost; repetitions: 3; IP: 192.0.2.4;
countryname: United
States) ; Severity: Critical; EventNumber: EN00000184; State:
0;
NumOfRejectedConnections: 0; NumOfAcceptedConnections: 0) ;
```

If you need to add more fields to the event:

1. In the SmartEvent GUI client, in the **Policy** tab, right-click the event, and select **Properties** > **Event Format** tab
2. In the **Display** column, select the **Event fields** to have in the Event.
3. Install the Event Policy on the SmartEvent Correlation Unit.

Assigning an Automatic Reaction to an Event

You can add an Automatic Reaction for SmartEvent to run when this type of event is detected.

1. Select the icon **[...]**.
2. Select an Automatic Reaction that you created from the list, or select **Add new?**. For details on how to create each type of Automatic Reaction, see above section.
3. Configure the Automatic Reaction.
4. Select **Save**.
5. Click **OK**.

Creating a Mail Reaction

1. Select **Add** > **Mail**.
2. Give the automatic reaction a significant name.
3. Fill out the **Mail Parameters of From**, **To** and **cc**.

4. To add multiple recipients, separate each email address with a semi-colon.

   Note - the **Subject** field has the default variables of *[EventNumber] - [Severity] - [Name].* These variables automatically adds to the mail subject the event number, severity and name of the event that triggered this reaction. These variables can be removed at your discretion.

5. Optional: Include your own standard text for each mail reaction.
6. Enter the domain name of the SMTP server.
7. Select **Save**.

Creating an SNMP Trap Reaction

1. Select **Add** > **SNMP Trap**.
2. Give the automatic reaction a significant name.
3. Fill out the **SNMP Trap parameters** of **Host**, **Message**, **OID** and **Community name**.

   The command `send_snmp` uses values that are found in the file **chkpnnt.mib**, in the directory `$CPDIR/lib/snmp/`. An **OID** value used in the **SNMP Trap parameters** window must be defined in **chkpnnt.mib**, or in a file that refers it. If the **OID** field is left blank, the value is determined from **iso.org.dod.internet.private.enterprises.checkpoint.products.fw.fwEvent = 1.3.6.1.4.1.2620.1.1.11**.

   When the automatic reaction occurs, the SNMP Trap is sent as a 256 byte `DisplayString` text. But, if the OID type is not text, the message is not sent.

4. Select **Save**.

Creating a Block Source Reaction

1. Select **Add** > **Block Source**.
2. Give the automatic reaction a significant name.
3. From the drop-down list, select the number of minutes to block this source.
4. Select **Save**.

Creating a Block Event Activity Reaction

1. Select **Add** > **Block Event Activity**.
2. Give the automatic reaction a significant name.
3. From the drop-down list, select the number of minutes to block this source.
4. Select **Save**.

Creating an External Script Automatic Reaction

To add an External Script:

1. Create the script.
2. Put the script on the SmartEvent Server
   a. In `$RTDIR/bin`, create the folder `ext_commands`:

      ```
      mkdir $RTDIR/bin/ext_commands
      ```

   b. Put the script in `$RTDIR/bin/ext_commands/` or in a folder under that location.

      The path and script name must not contain any spaces.

   c. Give the script executable permissions:

      ```
      chmod +x $RTDIR/bin/ext_commands/<script_filename>
      ```

3. In the SmartEvent GUI client **Policy** tab, in **Automatic Reactions**, select **Add** > **External Script**.
4. In the **Add Automatic Reaction** window:
   a. Give the automatic reaction object a significant name.
   b. In Command line, enter the name of the script to run.

      Specify the name of the script that is in `$RTDIR/bin/ext_commands/` directory.

      Use the relative path if needed.

      Do not specify the full path of `$RTDIR/bin/ext_commands/`.

   c. Select **Save**.

Guidelines for creating the script

- Run the script manually and make sure it works as expected
- Make sure the script runs for no longer than 10 minutes, otherwise it will be terminated by the SmartEvent Server.
- Use the event fields in the script:

  To refer to the event in the script, define this environment variable:

  ```
  EVENT=$(cat)
  ```

  and use `$EVENT`

  Use line editor commands like `awk` or `sed` to parse the event and refer to specific fields. You can print the `$EVENT` one time to see its format.

The format of the event content is a name-value set - a structured set of fields that have the form:

```
(name: value ;* );
```

where name is a string and value is either free text until a semicolon, or a nested name-value set.

This is a sample event:

```
(Name: Check Point administrator credential guessing; RuleID:
{F182D6BC-A0AA-444a-9F31-C0C22ACA2114}; Uuid:
<42135c9c,00000000,2e1510ac,131c07b6>; NumOfUpdates: 0;
IsLast: 0;
StartTime: 16Feb2015 16:45:45; EndTime: Not Completed;
DetectionTime:
16Feb2015 16:45:48; LastUpdateTime: 0; TimeInterval: 600;
MaxNumOfConnections: 3; TotalNumOfConnections: 3; DetectedBy:
2886735150;
Origin: (IP: 192.0.2.4; repetitions: 3; countryname: United
States;
hostname: theHost) ; ProductName: SmartDashboard; User: XYZ;
Source:
(hostname: theHost; repetitions: 3; IP: 192.0.2.4;
countryname: United
States) ; Severity: Critical; EventNumber: EN00000184; State:
0;
NumOfRejectedConnections: 0; NumOfAcceptedConnections: 0) ;
```

If you need to add more fields to the event:

1. In the SmartEvent GUI client, in the **Policy** tab, right-click the event, and select **Properties** > **Event Format** tab.
2. In the **Display** column, select the **Event fields** to have in the Event.
3. Install the Event Policy on the SmartEvent Correlation Unit.

Assigning an Automatic Reaction to an Event

You can add an Automatic Reaction for SmartEvent to run when this type of event is detected.

1. Select the icon **[...]**.
2. Select an Automatic Reaction that you created from the list, or select **Add new?**. For details on how to create each type of Automatic Reaction, see above section.
3. Configure the Automatic Reaction.

4. Select **Save**.
5. Click **OK**.

Working Hours

Working Hours are used to detect unauthorized attempts to access protected systems and other forbidden operations after-hours. To set the **Regular Working Hours** for an event, select a **Time Object** that you have configured from the drop-down list.

To create a Time Object:

1. From the **Policy** tab, select **General Settings Objects** > **Time Objects**.
2. Click **Add**.
3. Enter a **Name** and **Description**.
4. Select the days and times that are considered **Regular Working Hours**.
5. Click **OK**.

To assign a Time Object to an event:

1. From the **Policy** tab, select an event that requires a **Time Object** (for example, **User Login at irregular hours** in the **Unauthorized Entry** event category).
2. Select the **Time Object** you created from the drop-down list.
3. Select **File** > **Save**.

Exceptions

Exceptions allow an event to be independently configured for the sources, destination, service and other parameters depending on the event type. For example, if the event **Port Scan from Internal Network** is set to detect an event when 30 port scans occur within 60 seconds, you can also define that two port scans detected from host *A* within 10 seconds of each other is also an event.

To add an exception:

1. Under **Apply the following exceptions**, click **Add**.
2. Select the **Source** and/or **Destination** of the object to apply different criteria for this event.

Note - If you do not see the host object listed, you may need to create it in SmartEvent.(see *"System Administration" on page 131*).

High Level Overview of Event Identification

Events are detected by the SmartEvent Correlation Unit. The SmartEvent Correlation Unit scans logs for criteria that match an Event Definition.

SmartEvent uses these procedures to identify these events:

- *"Matching a Log Against Global Exclusions" below*
- *"Matching a Log Against Each Event Definition" below*
- *"Creating an Event Candidate" on the next page*
- *"Matching a Log Against Event Exclusion" on page 116*
- *"Event Generation" on page 117*

Matching a Log Against Global Exclusions

When the SmartEvent Correlation Unit reads a log, it first checks if the log matches all defined **Global Exclusions**. Global Exclusions (defined on the **Policy** tab > **Event Policy** > **Global Exclusions**) direct SmartEvent to ignore logs that are not expected to contribute to an event.

If the log matches a Global Exclusion, it is discarded by the system. If not, the SmartEvent Correlation Unit starts to match it against each Event Definition.

Matching a Log Against Each Event Definition

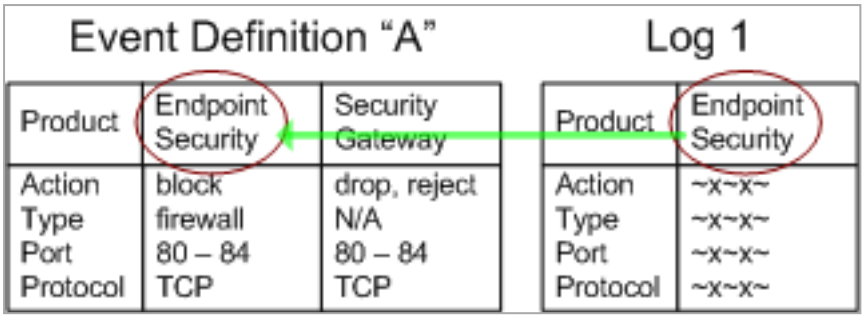
Each **Event Definition** contains a filter which is comprised of a number of criteria that must be found in all matching logs. The criteria are divided by product: The **Event Definition** can include a number of different products, but each product has its own criterion.

Event Definition “A”

Product	Endpoint Security	Security Gateway
Action	block	drop, reject
Type	firewall	N/A
Port	80 – 84	80 – 84
Protocol	TCP	TCP

To match the **Event Definition "A"**, a log from Endpoint Security must match the **Action**, **Event Type**, **Port**, and **Protocol** values listed in the Endpoint Security column. A log from a Security Gateway must match the values listed in its column.

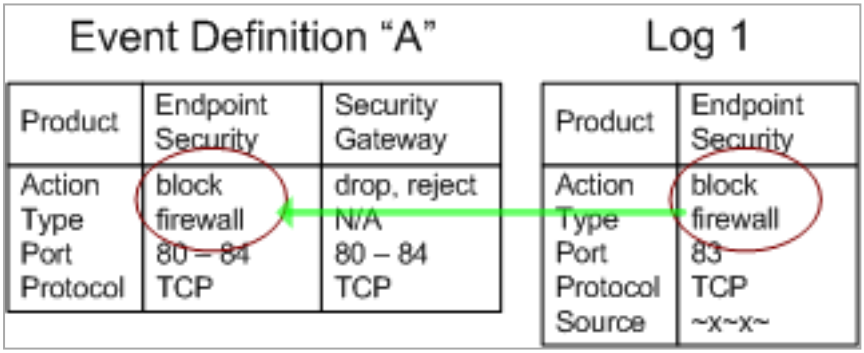
SmartEvent divides this procedure into two steps. The SmartEvent Correlation Unit first checks if the Product value in the log matches one of the permitted **Product** values of an **Event Definition**.



If Log 1 did not contain a permitted **Product** value, the SmartEvent Correlation Unit compares the log against **Event Definition "B"**, and so on. If the log fails to match against an **Event Definition**, it is discarded.

The SmartEvent Correlation Unit checks if the log contains the Product-specific criteria to match the **Event Definition**. For example: The product Endpoint Security generates logs that involve the Firewall, Spyware, Malicious Code Protection, and others. The log contains this information in the field **Event Type**. If an event is defined to match on Endpoint Security logs with the event type **Firewall**, an Endpoint Security log with Event Type "Spyware" fails against the Event Definition filter. Other criteria can be specified to the Product.

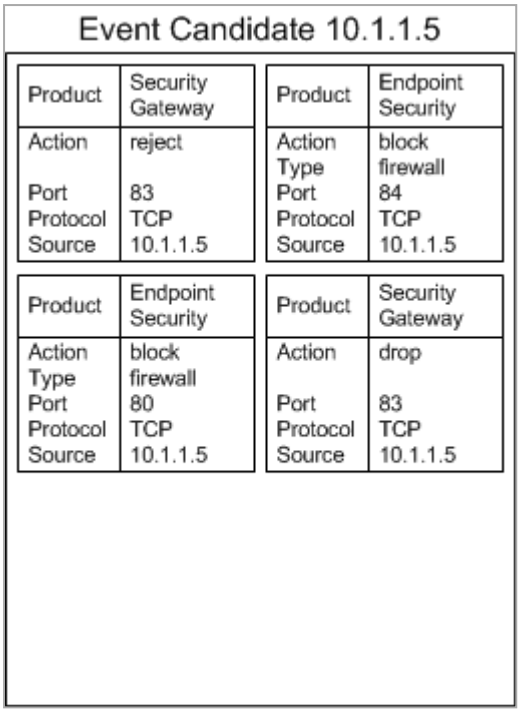
In our example, Log 1 matched **Event Definition "A"** with a permitted product value. The SmartEvent Correlation Unit examines if the log contains the necessary criteria for an Endpoint Security log to match.



If the criteria do not match, the SmartEvent Correlation Unit continues to compare the log criteria to other event definitions.

Creating an Event Candidate

When a log matches the criteria, it is added to an **Event Candidate**. Event candidates let SmartEvent track logs until an event threshold is crossed, at which point an event is generated.

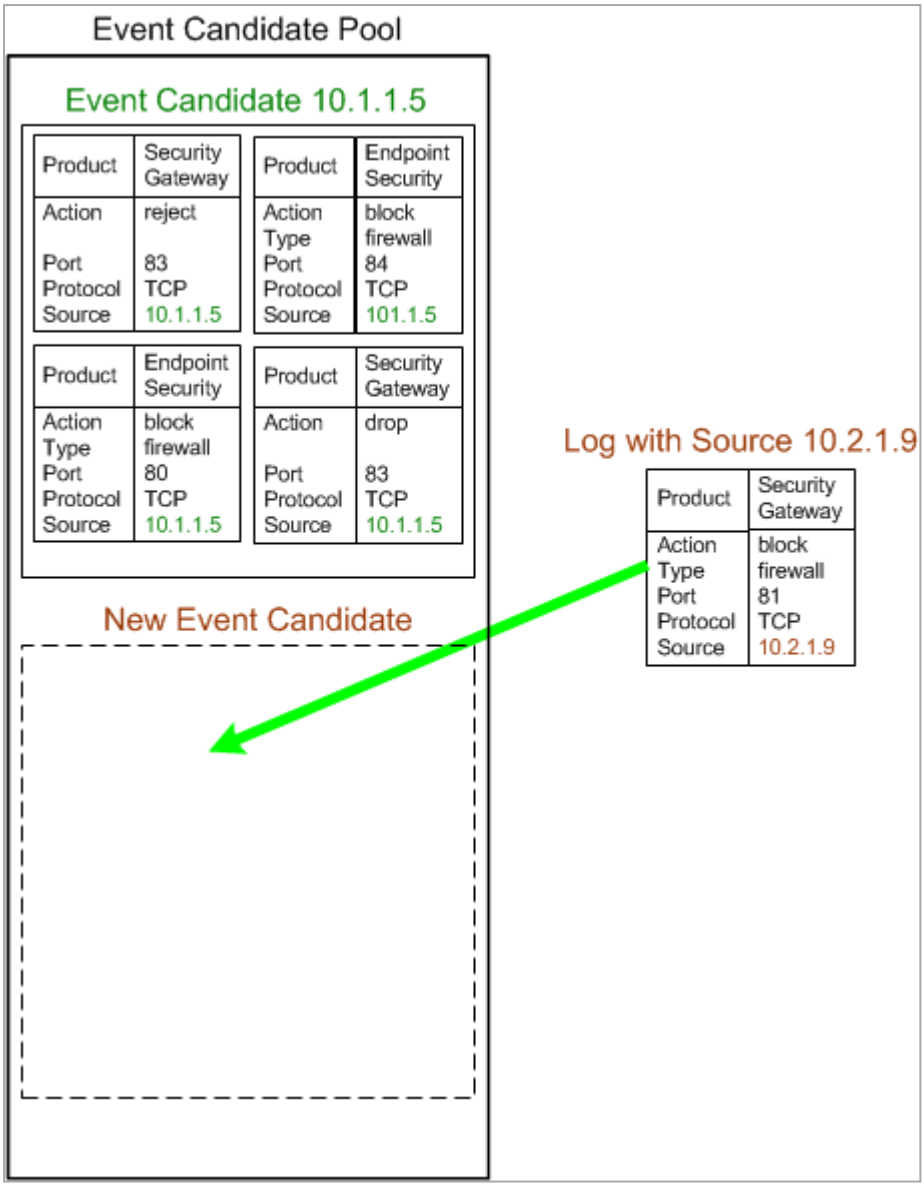


The logs can come from different log servers and be correlated in the same event.

The Event Candidate tracks logs until the criteria is matched (the criteria is the number of logs in a declared number of seconds).

Each **Event Definition** can have multiple event candidates, each of which keeps track of logs grouped by equivalent properties. In the figure above the logs that create the event candidate have a common source value. They are dropped, blocked or rejected by a Security Gateway. They are grouped together because the Event Definition is designed to detect this type of activity that originates from one source. Depending on the event declaration, if there is a grouping declaration on the source field, it will create a new event candidate.

When a log matches the event definition, but has properties different than those of the existing event candidates, a new event candidate is created. This event candidate is added to what can be thought of as the **Event Candidate Pool**.



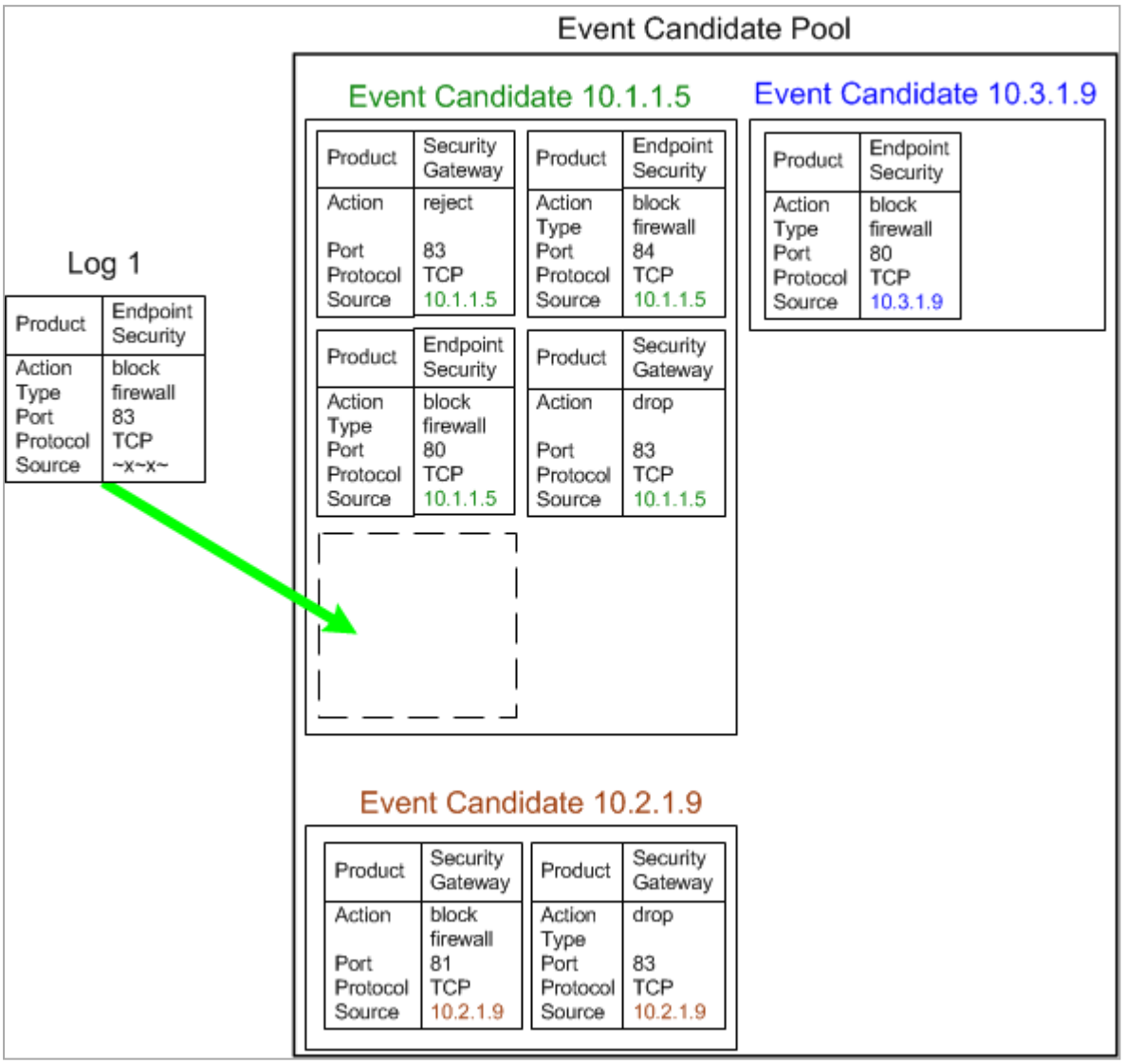
By default, SmartEvent creates a new event candidate for a log with a different source.

To customize the default behavior:

1. Go to **SmartEvent** > **Policy**.
2. Select an event and right-click > **Select Properties**.

   The **Edit Event Definition** window opens.
3. In the **Count logs** tab, click the options under **Select the fields by which distinct Event Candidates will be created**.
4. In the Event Definition Wizard window, select the log fields and click **OK**.

To illustrate more, an event defined detects a high rate of blocked connections. SmartEvent tracks the number of blocked connections for each Security Gateway, and the logs of the blocked traffic at each Security Gateway forms an event candidate. When the threshold of blocked connection logs from a Security Gateway is surpassed, that Security Gateway event candidate becomes an event. While this Event Definition creates one event candidate for each Security Gateway monitored, other Event Definitions can create many more.



The Event Candidate Pool is a dynamic environment, with new logs added and older logs discarded when they have exceeded an Event Definition time threshold.

Matching a Log Against Event Exclusion

Before SmartEvent generates logs for a specific event, it checks to see if this event candidate attributes are listed in the exclusions table or not. Event Exclusions are defined on the **Policy** tab > **Event Policy** > **Event Exclusions** according to the attributes selected.

If an attribute matches an Event Exclusion, it is discarded by the system (an event is not generated). If not, the SmartEvent Correlation Unit starts to match it against each Event Definition.

Event Generation

When a candidate becomes an event, the SmartEvent Correlation Unit forwards the event to the Event Database. But to discover an event does not mean that SmartEvent stops to track logs related to it. The SmartEvent Correlation Unit adds matching logs to the event as long as they continue to arrive during the event threshold. To keep the event *open* condenses what can appear as many instances of the same event to one, and provides accurate, up-to-date information as to the start and end time of the event.

Creating a User-Defined Event

To create New Event Definitions, right-click an existing Event Definition, or use the **Actions** menu:

Right Click	Actions Menu	Description
New	**New Custom Event**	Launches the Event Definition Wizard, which allows you to select how to base the event: on an existing Event Definition, or from scratch.
Save As	**Save Event As**	Creates an Event Definition based on the properties of the highlighted Event Definition. When you select **Save As**, the system prompts you to save the selected Event Definition with a new name for later editing. **Save As** can also be accessed from the **Properties** window.

All User Defined Events are saved at **Policy** tab > **Event Policy** > **User Defined Events**. When an Event Definition exists it can be modified through the **Properties** window, available by right-click and from the **Actions** menu.

Creating a New Event Definition

You can edit all events, not only user-defined events. If you change a predefined event,the result is saved as a new user defined event.

To create a new event definition:

1. From the **Actions** menu, select **New Custom Event**.

   The Event Definition Wizard opens.

2. **For Create an event**

   a. Select **that is based on an existing event**.

   b. Select an event that has equivalent properties to the event you want to create.

c. Click **Next**.

3. Name the **Event Definition**.
4. Enter a **Description**.
5. Select a **Severity** level.
6. Click **Next**.
7. Set which of these options generates the event:
   - **A single log** - Frequently depicts an event, such as a log from a virus scanner that reports that a virus has been found.
   - **Multiple logs** - Required if the event can only be identified as a result of a combination of multiple logs, such as a High Connection Rate.

   Click **Next**.
8. Examine the products that can cause this event.
9. Select **Next**.
10. Optional: Edit the product filters:
    - If you added a product you can edit the filters for each product (**Edit all product filters**), or those of new products you added (**Edit only newly selected product filters**).
    - If you did not add other products, edit the filters of existing products (**Yes**) or skip this step (**No, Leave the original files**).

    Click **Next**.
11. **Edit or add product filters for each log necessary in the Event Definition filter**
    a. Select the Log field from the available Log Field list.
    b. Click **Add** to edit the filter.
    c. Make sure that the filter matches on **All Conditions** or **Any Conditions**.
    d. Double-click the Log field and select the values to use in the filter.

    Click **Next**.
12. **When you defined the filters for each product, select values for these options to define how to process logs**

- **Detect the event when at least__ logs occurred over a period of __ seconds** contains the event thresholds that define the event. You can modify the event thresholds by altering the number of logs and/or the period of time that define the event.
- **Each event definition may have multiple Event Candidates existing simultaneously** allows you to set whether SmartEvent creates distinct Event Candidates based on a field (or set of fields) that you select below.

  Select the field(s) by which distinct Event Candidates will be created allows you to set the field (or set of fields) that are used to differentiate between Event Candidates.
- **Use unique values of the __ field when counting logs** directs SmartEvent to count unique values of the specified field when determining whether the Event Threshold has been surpassed. When this property is not selected, SmartEvent counts the total number of logs received.

13. Click **Finish**.

Customizing a User-Defined Event

Customizing a user-defined event:

1. From the **Policy** tab > **Event Policy** > **User Defined Events**, right-click a User-Defined Event and select **Properties**.
2. **In the tabs provided, make the necessary changes**
   - **Name** - Name the **Event Definition**, enter a **Description** and select a **Severity** level. The text you enter in the **Description** field shows in the Event Description area (below the event configurable properties).
   - **Filter - To edit a product filter**
     a. Select the product.
     b. Select the Log field from the available **Log Fields** list.
     c. If the necessary field does not show select **Show more fields...** to add a field to the **Log Fields** list.
     d. Click **Add** to edit the filter.
     e. Select if the filter matches on **All Conditions** or **Any Conditions**.

- **Count logs**

  This screen defines how SmartEvent counts logs related to this event.

  - **A Single log** - Frequently depicts an event, such as a log from a virus scanner that reports that a virus is found.
  - With this option you can set the fields that are used to group events into Event Candidates. Logs with matching values for these fields are added to the same event. For example: Multiple logs that report a virus detected on the same source with the same virus name are combined into the same event.
  - **Multiple logs** - Required for events that identify an activity level, such as a High Connection Rate.
  - When the event is triggered by multiple logs, set the behavior of Event Candidates:
  - **Detect the event when at least...** - Set the Event Threshold that, when exceeded, indicates that an event has occurred.
  - **Select the field(s) by which distinct event candidates will be created** - An event is generated by logs with the same values in the fields specified here. To define how logs are grouped into Event Candidates, select the related fields here.
  - **Use unique values of the ...** - Only logs with unique values for the fields specified here are counted in the event candidate. For example: A port scan event counts logs that include unique ports scanned. Also, the logs do not increment the log count for logs that contain ports already encountered in the event candidate.
  - **Advanced** - Define the keep=alive time for the event, and how often the SmartEvent Correlation Unit updates the SmartEvent Server with new logs for the created event.

- **Event Format**

  When an event is generated, information about the event is presented in the **Event Detail** pane.

  This screen lets you specify if the information will be added to the detailed pane and from which Log Field the information is taken.

  You can clear it in the **Display** column. The Event Field will not be populated.

- **GUI representation**

  All events can be configured. This screen lets you select the configuration parameters that show.

  - The **Threshold section** shows the number of logs that must matched to create the event. This is usually not shown for one log events and shown for multiple log events.
  - The **Exclude section** lets you specify the log fields that show when you add an event exclusion.
  - The **Exception section** lets you specify the log fields that show when you add an event exception.

3. Click **OK** to save your changes.

Eliminating False Positives

This section shows you how to reduce false positives.

Services that Generate Events

Some types of services are characterized by a high quantity of traffic that can be misidentified as events. These are examples of services and protocols that can potentially generate events:

- Software that does a routine scan of the network to make sure that everything runs correctly. Configuration of SmartEvent to exclude this source from a scan event eliminates a source of false positive events.
- High connection rate on a web server. Set SmartEvent to allow a higher connection rate for each minute on a busy web server, or to exclude this source from a scan event.

Common Events by Service

The information in this table provides a list of server types where high activity is frequently used. To change the Event Policy, adjust event thresholds and add Exclusions for servers and services . You can decrease more the quantity of false positives detected.

Common events by service

Server Type	Category	Event Name	Source	Dest	Service	Reason
SNMP	Scans	IP sweep from internal network	Any	Any	SNMP-read	Hosts that query other hosts

Server Type	Category	Event Name	Source	Dest	Service	Reason
DNS Servers	Scans	IP sweep from internal network	DNS servers	-	DNS	Inter-DNS servers updates
	Denial of Service (DoS)	High connection rate on internal host on service	Any	DNS servers	DNS	DNS requests and inter-DNS servers updates
	Anomalies	High connection rate from internal network	Any	Any	DNS	DNS requests and inter-DNS servers updates
	Anomalies	High connection rate from internal network on service	Any	Any	DNS	DNS requests and inter-DNS servers updates
	Anomalies	Abnormal activity on service	Any	Any	DNS	DNS requests and inter-DNS servers updates
NIS Servers	Scans	Port scan from internal network	NIS servers	Any	-	Multiple NIS queries

Server Type	Category	Event Name	Source	Dest	Service	Reason
	Denial of Service (DoS)	High connection rate on internal host on service	Any	NIS servers	NIS	NIS queries
	Anomalies	High connection rate from internal network	Any	Any	NIS	NIS queries
	Anomalies	High connection rate from internal network on service	Any	Any	NIS	NIS queries
	Anomalies	Abnormal activity on service	Any	Any	NIS	NIS queries
LDAP Servers	Denial of Service (DoS)	High connection rate on internal host on service	Any	LDAP servers	LDAP	LDAP requests
	Anomalies	High connection rate from internal network	Any	LDAP servers	LDAP	LDAP requests

Server Type	Category	Event Name	Source	Dest	Service	Reason
	Anomalies	High connection rate from internal network on service	Any	LDAP servers	LDAP	LDAP requests
	Anomalies	Abnormal activity on service	Any	LDAP servers	LDAP	LDAP requests
HTTP Proxy Servers - Hosts To Proxy Server	Denial of Service (DoS)	High connection rate on internal host on service	Any	Proxy servers	HTTP:8080	Hosts connections to Proxy servers
	Anomalies	High connection rate from internal network	Any	Proxy servers	HTTP:8080	Hosts connections to Proxy servers
	Anomalies	High connection rate from internal hosts on service	Any	Proxy servers	HTTP:8080	Hosts connections to Proxy servers
	Anomalies	Abnormal activity on service	Any	Proxy servers	HTTP:8080	Hosts connections to Proxy servers

Server Type	Category	Event Name	Source	Dest	Service	Reason
HTTP Proxy Servers - Out to the Web	Scans	IP sweep from internal network	Proxy servers	Any	HTTP/ HTTPS	Proxy servers connections out to various sites
	Denial of Service (DoS)	High connection rate on internal host on service	Proxy servers	Any	HTTP/ HTTPS	Proxy servers connections out to various sites
	Anomalies	High connection rate from internal network	Proxy servers	Any	HTTP/ HTTPS	Proxy servers connections out to various sites
		High connection rate from internal hosts on service	Proxy servers	Any	HTTP/ HTTPS	Proxy servers connections out to various sites
	Anomalies	Abnormal activity on service	Proxy servers	Any	HTTP/ HTTPS	Proxy servers connections out to various sites
UFP Servers	Denial of Service (DoS)	High connection rate on internal host on service	Any	UFP servers	Any/UFP by vendor	Firewall connections to UFP servers

Server Type	Category	Event Name	Source	Dest	Service	Reason
	Anomalies	High connection rate from internal network	Any	UFP servers	Any/UFP by vendor	Firewall connections to UFP servers
	Anomalies	High connection rate from internal hosts on service	Any	UFP servers	Any/UFP by vendor	Firewall connections to UFP servers
	Anomalies	Abnormal activity on service	Any	UFP servers	Any/UFP by vendor	Firewall connections to UFP servers
CVP Servers Request	Denial of Service (DoS)	High connection rate on internal host on service	Any	CVP servers	Any/CVP by vendor	Firewall connections to CVP servers
	Anomalies	High connection rate from internal network	Any	CVP servers	Any/CVP by vendor	Firewall connections to CVP servers
	Anomalies	High connection rate from internal hosts on service	Any	CVP servers	Any/CVP by vendor	Firewall connections to CVP servers

Server Type	Category	Event Name	Source	Dest	Service	Reason
	Anomalies	Abnormal activity on service	Any	CVP servers	Any/CVP by vendor	Firewall connections to CVP servers
CVP Servers Replies	Scans	Port scans from internal network	CVP servers	Any	-	Multiple CVP replies to same GW
	Scans	IP sweep from internal network	CVP servers	-	CVP	CVP replies to multiple GWs
	Denial of Service (DoS)	High connection rate on internal host on service	CVP servers	Any	Any/CVP by vendor	CVP replies
	Anomalies	High connection rate from internal network	CVP servers	Any	Any/CVP by vendor	CVP replies
	Anomalies	High connection rate from internal hosts on service	CVP servers	Any	Any/CVP by vendor	CVP replies
	Anomalies	Abnormal activity on service	CVP servers	Any	Any/CVP by vendor	CVP replies

Server Type	Category	Event Name	Source	Dest	Service	Reason
UA Server Request	Denial of Service (DoS)	High connection rate on internal host on service	Any	UA servers	uas-port (TCP:19191 TCP:19194)	Connections to UA servers
	Anomalies	High connection rate from internal network	Any	UA servers	(TCP:19191 TCP:19194)	Connections to UA servers
	Anomalies	High connection rate from internal hosts on service	Any	UA servers	uas-port (TCP:19191 TCP:19194)	Connections to UA servers
	Anomalies	Abnormal activity on service	Any	UA servers	uas-port (TCP:19191 TCP:19194)	Connections to UA servers
UA Servers Replies	Scans	Port scans from internal network	UA servers	Any	-	Multiple UA replies to the same computer
	Scans	IP sweep from internal network	UA servers	Any	uas-port (TCP:19191 TCP:19194)	Multiple UA replies to multiple computers
	Denial of Service (DoS)	High connection rate on internal host on service	UA servers	Any	uas-port (TCP:19191 TCP:19194)	UA replies

Server Type	Category	Event Name	Source	Dest	Service	Reason
	Anomalies	High connection rate from internal network	UA servers	Any	uas-port (TCP:19191 TCP:19194)	UA replies
	Anomalies	High connection rate from internal hosts on service	UA servers	Any	uas-port (TCP:19191 TCP:19194)	UA replies
	Anomalies	Abnormal activity on service	UA servers	Any	uas-port (TCP:19191TCP:19194)	UA replies
SMTP Servers	Scans	IP sweep from internal network	SMTP servers	-	SMTP	SMTP servers connections out to various SMTP servers
	Denial of Service (DoS)	High connection rate on internal host on service	SMTP servers	Any	SMTP	SMTP servers connections out to various SMTP servers
	Anomalies	High connection rate from internal network	SMTP servers	Any	SMTP	SMTP servers connections out to various SMTP servers

Server Type	Category	Event Name	Source	Dest	Service	Reason
	Anomalies	High connection rate from internal hosts on service	SMTP servers	Any	SMTP	SMTP servers connections out to various SMTP servers
	Anomalies	Abnormal activity on service	SMTP servers	Any	SMTP	SMTP servers connections out to various SMTP servers
Anti-Virus Definition Servers	Scans	IP sweep from internal network	AV_Defs servers	-	Any/AV by vendor	Anti-Virus definitions updates deployment
	Denial of Service (DoS)	High connection rate on internal host on service	AV_Defs servers	-	Any/AV by vendor	Anti-Virus definitions updates deployment
	Anomalies	High connection rate from internal network	AV_Defs servers	-	Any/AV by vendor	Anti-Virus definitions updates deployment
	Anomalies	High connection rate from internal hosts on service	AV_Defs servers	-	Any/AV by vendor	Anti-Virus definitions updates deployment

Server Type	Category	Event Name	Source	Dest	Service	Reason
	Anomalies	Abnormal activity on service	AV_Defs servers	-	Any/AV by vendor	Anti-Virus definitions updates deployment

System Administration

To maintain your SmartEvent system, you can do these tasks from the **General Settings** section of the **Policy** tab:

- Adding a SmartEvent Correlation Unit and Log Servers
- Create offline jobs analyze historical log files (see *"Importing Offline Log Files" on page 41*).
- Adding objects to the Internal Network
- Creating scripts to run as Automatic Reactions for certain events (see *"Creating an External Script Automatic Reaction" on page 109*)
- Creating objects for use in filters

Adding Network and Host Objects

Network Objects are the objects that are synchronized from the Management object database as well as user defined additional objects. These objects from the Management server are added to SmartEvent during the initial sync and updated at set intervals.

As a best practice, use SmartConsole to add new network or host objects to the Management server.

The customer cannot define the internal network until the initial sync is complete.

To add a host or network object to SmartEvent:

1. From the **Policy** tab, select **General Settings** > **Objects** > **Network Objects** > **Add** > **Host** or **Add Network**.
2. Give the device a significant name.
3. For a host, enter the **IP Address** or select **Get Address**.
4. For a network object, enter the **Network Address** and **Net Mask**.
5. Select **OK**.

Defining the Internal Network

To help SmartEvent conclude if events originated internally or externally, you must define the Internal Network. These are the options to calculate the traffic direction:

- Incoming - All the sources are external to the network and all destinations are internal.
- Outgoing - All sources are in the network and all destinations are external.
- Internal - Sources and destinations are all in the network.
- Other - A mixture of 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.

   We recommend you add all internal **Network** objects, and not **Host** objects.

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

Note - The customer cannot define the internal network until the initial sync is complete.

Monitoring Traffic and Connections

SmartView Monitor gives you a complete picture of network and security performance. Use it to respond quickly and efficiently to changes in Security Gateways, tunnels, remote users and traffic flow patterns or security activities.

SmartView Monitor is a high-performance network and security analysis system. This system helps you to establish work habits based on learned system resource patterns. Based on Check Point Security Management Architecture, SmartView Monitor provides a single, central interface, to monitor network activity and performance of Check Point Software Blades.

How SmartView Monitor Works

Data for the status of all Security Gateways in the system is collected by the Security Management Server and viewed in SmartView Monitor.

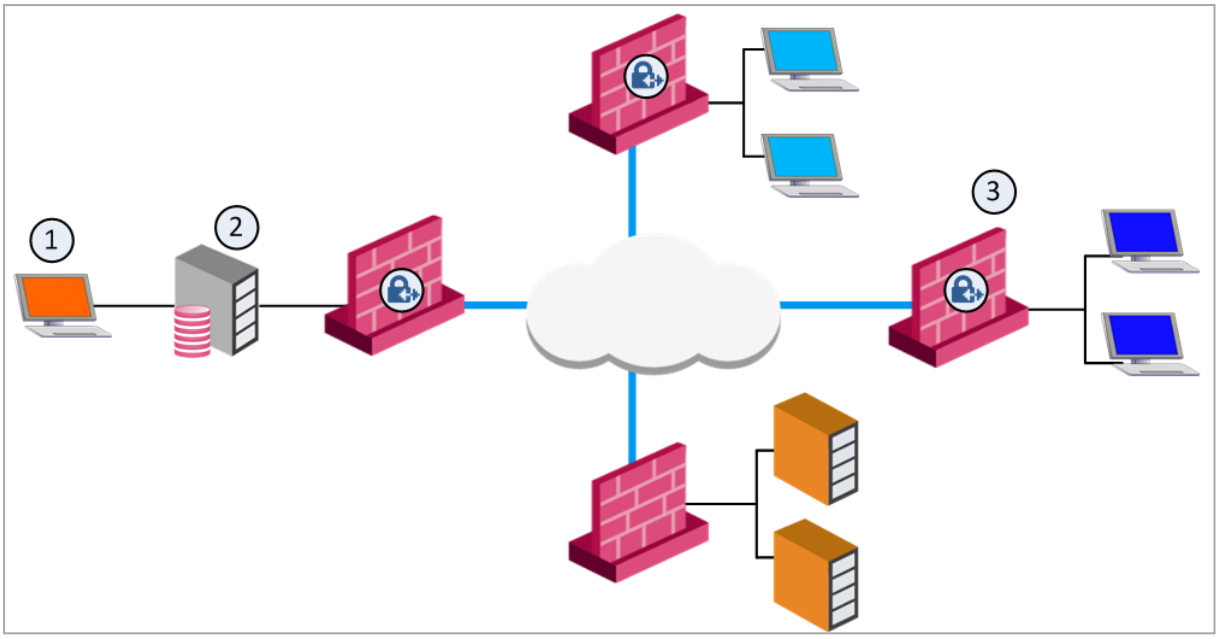
The data shows status for:

- Check Point Security Gateways
- OPSEC Gateways
- Check Point Software Blades

Gateway Status is the SmartView Monitor view, which shows all component status information.

A **Gateway Status** view shows a snapshot of all Software Blades, such as VPN and ClusterXL, and third party products (for example, OPSEC Gateways).

Gateway Status is similar in operation to the SNMP daemon that provides a mechanism to get data about Gateways in the system.



SIC is initialized between Security Gateways **(3)** (local and remote), and the Security Management Server **(2)**. The Security Management Server then gets status data from the Software Blades with the **AMON** (Application Monitoring)protocol. SmartView Monitor **(1)** gets the data from the Security Management Server.

AMON Protocol Support

The Security Management Server acts as an AMON client. It collects data about installed Software Blades. Each Security Gateway, or any other OPSEC Gateway, which runs an AMON server, acts as the AMON server itself. The Gateway requests status updates from other components, such as the Firewall kernel and network servers. Requests are fetched at a defined interval.

An alternate source for status collection can be any AMON client, such as an OPSEC partner, which uses the AMON protocol.

The AMON protocol is SIC- based. It can collect data only after SIC is initialized.

Defining Status Fetch Frequency

The Security Management Server collects status data from the Security Gateways on a defined interval. The default is 60 seconds.

To set the Status Fetching Interval:

1. Open SmartConsole.
2. Open **Global Properties** > **Log and Alert** > **Time Settings**.
3. Enter the number of seconds in **Status fetching interval**.

To Start Monitoring

To open the monitoring views in SmartConsole:

1. From the **Gateways & Servers** view, select a Security Gateway.
2. Click **Monitor**.

   The **Device and License information** window opens and shows:

   - Device Status
   - License Status
   - System Counters
   - Traffic

To open SmartView Monitor:

1. Open SmartConsole > **Logs & Monitor**.
2. Open the catalog (new tab).
3. Click **Tunnel & User Monitoring**.

Note - SmartView Monitor may fail to open if there are more than 15,000 objects configured in the management database on the Management Server.

SmartView Monitor Features

SmartView Monitor allows administrators to easily configure and monitor different aspects of network activities. You can see graphical from an integrated, intuitive interface.

Defined views include the most frequently used traffic, counter, tunnel, Security Gateway, and remote user information. For example, Check Point System Counters collect information on the status and activities of Check Point products (for example, VPN or NAT). With custom or defined views, administrators can drill-down the status of a specified Security Gateway and/or a segment of traffic. That way, administrators identify top bandwidth hosts that can influence network performance. If suspicious activity is detected, administrators can immediately apply a Firewall rule to the applicable Security Gateway to block that activity. These Firewall rules can be created dynamically through the graphical interface and be set to expire in a specified time period.

You can generate Real-time and historical graphical reports of monitored events. This provides a comprehensive view of Security Gateways, tunnels, remote users, network, security, and performance over time.

The monitoring views show real-time and historical graphical views of:

- Gateway status
- Remote users (SmartView Monitor only)
- System Counters
- VPN tunnel monitoring (SmartView Monitor only)
- Cooperative Enforcement, for Endpoint Security Servers
- Traffic

In SmartView Monitor, you can create customized monitoring view.

SmartView Monitor Use Cases

Use SmartView Monitor to:

- Create a Traffic view and report to identify the reasons for slow internet access. The view can be based on an inspection of: Specific Services, Firewall rules or Network Objects, that can be known to impede the flow of internet traffic. If the SmartView Monitor Traffic view indicates that users aggressively use such Services or Network Objects (for example, Peer to Peer application or HTTP), the cause of the slow internet access is determined. If aggressive use is not the cause, the network administrator have to look at other avenues. For instance, performance degradation can be the result of memory overload.
- Create a report to determine why employees who work away from the office cannot connect to the network. The view can be based on CPU Use %, to collect information about the status, activities hardware and software use of Check Point products in real-time. The SmartView Monitor Counter view can indicate that there are more failures than successes. Perhaps the company cannot accommodate the number of employees that try to log on at the same time?

Immediate Actions

If the status shows an issue, you can act on that network object.

For example:

- **Disconnect client** - Disconnect one or more of the connected SmartConsole clients.
- **Start/Stop cluster member** - You can see all Cluster Members of a Cluster in SmartView Monitor. You can start or stop a selected Cluster Member.
- **Suspicious Action Rules** - You can block suspicious network activity while you investigate the real risk or to quickly block an obvious intruder.

Monitoring and Handling Alerts

Alerts provide real-time information about possible security threats, and how to avoid, minimize, or recover from the damage. The administrator can define alerts to be sent for different Security Gateways and for certain policies or properties.

The Security Gateways send alerts to the Security Management Server. The Security Management Server forwards these alerts to SmartView Monitor. By default, an alert is sent as a pop-up message to the administrator desktop when a new alert arrives to SmartView Monitor.

You can set global alert parameters for all Security Gateways in the system, or specify an action to send an alert for a particular Security Gateway.

Alerts are sent when:

- Rules or attributes which are set to be tracked as alerts are matched by a passing connection.
- System events (also called System Alerts) are configured to cause an alert when different predefined thresholds are surpassed.

System Alerts are sent for predefined system events or for important situation updates. For example, if free disk space is less than 10%, or if a security policy is changed. System Alerts can also be defined for each product. For example, you can define other System Alerts for Check Point QoS.

Viewing Alerts

Alert commands are set in **SmartConsole** > **Global Properties** > **Log and Alert** > **Alerts** page. The Alerts in this window apply only to Security Gateways.

To see alerts:

1. Open SmartConsole > **Logs & Monitor** view > **External Apps**.
2. Click **Tunnel & User Monitoring**.

   SmartView Monitor opens.
3. Click the **Alerts** icon in the toolbar.

   The **Alerts** window opens. Use this window to monitor or delete alerts.

System Alert Monitoring Mechanism

The Check Point Security Management Server System Alert monitoring mechanism uses the defined System Alert thresholds. If a threshold is reached, it activates the defined action.

To activate System Alert monitoring:

Go to **Tools** > **Start System Alert Daemon**.

To stop the System Alert monitoring:

Go to **Tools** > **Stop System Alert Daemon**.

Monitoring Suspicious Activity Rules

Suspicious Activity Monitoring (SAM) is a utility integrated in SmartView Monitor. It blocks activities that you see in the SmartView Monitor results and that appear to be suspicious. For example, you can block a user who tries several times to gain unauthorized access to a network or internet resource.

A Security Gateway with SAM enabled has Firewall rules to block suspicious connections that are not restricted by the security policy. These rules are applied immediately (policy installation is not required).

The Need for Suspicious Activity Rules

Connections between enterprise and public networks are a security challenge as they leave the network and its applications open to attack. You must be able to inspect and identify all inbound and outbound network activity and decide if it is suspicious.

Creating a Suspicious Activity Rule

SAM rules use CPU resources. Therefore, set an expiration time so you can inspect traffic but not negatively affect performance.

If you confirm that an activity is risky, edit the Security Policy, educate users, or handle the risk.

You can block suspicious activity based on source, destination, or service.

To block an activity:

1. In the SmartView Monitor, click the **Suspicious Activity Rules icon** in the toolbar.

   The **Enforced Suspicious Activity Rules** window opens.

2. Click **Add**.

   The **Block Suspicious Activity** window opens.

3. In **Source** and in **Destination**, select **IP** or **Network**:

- To block all sources or destinations that match the other parameters, enter `Any`.
- To block one suspicious source or destination, enter an IP **Address** and **Network Mask**.

4. In **Service**:
   - To block all connections that fit the other parameters, enter `Any`.
   - To block one suspicious service or protocol, click the button and select a service from the window that opens.
5. In **Expiration**, set a time limit.
6. Click **Enforce**.

To create an activity rule based on TCP or UDP use:

1. In the **Block Suspicious Activity** window , click **Service**.

   The **Select Service** window opens.
2. Click **Custom Service**.
3. Select **TCP** or **UDP**.
4. Enter the port number.
5. Click **OK**.

To define SmartView Monitor actions on rule match:

1. In the **Block Suspicious Activity** window, click **Advanced**.

   The **Advanced** window opens.
2. In **Action**, select the Firewall action for SmartView Monitor to do on rule match:
   - **Notify** - Send a message about the activity, but do not block it.
   - **Drop** - Drop packets, but do not send a response. The connection will time out.
   - **Reject** - Send an RST packet to the source and close the connection.
3. In Track, select **No Log**, **Log** or **Alert**.
4. If the action is **Drop**: To close the connection immediately on rule match, select **Close connections**.
5. Click **OK**.

Creating a Suspicious Activity Rule from Results

If you monitor traffic, and see a suspicious result, you can create an SAM rule immediately from the results.

Note - You can only create a **Suspicious Activity** rule for **Traffic** views with data about the **Source** or **Destination** (Top Sources, Top P2P Users, and so on).

To create an SAM rule:

1. In SmartView Monitor open a Traffic view.

   The **Select Gateway / Interface** window opens.

2. Select an object.
3. Click **OK**.
4. In the Results, right-click the bar in the chart (or the row in the report), that represents the source, destination, or other traffic property to block.
5. Select **Block Source**.

   The **Block Suspicious Activity** window opens.

6. Create the rule.
7. Click **Enforce**.

For example:

Your corporate policy does not allow to share peer2peer file, and you see it in the **Traffic** > **Top P2P Users** results.

1. Right-click the result bar and select **Block Source**.

   The SAM rule is set up automatically with the user IP address and the **P2P_File_Sharing_Applications** service.

2. Click **Enforce**.
3. For the next hour, while this traffic is dropped and logged, contact the user.

Managing Suspicious Activity Rules

The **Enforced Suspicious Activity Rules** window shows the currently enforced rules. If you add a rule that conflicts with another rule, the conflicting rule remains hidden. For example, if you define a rule to drop http traffic, and a rule exists to reject http traffic, only the drop rule shows.

sam_alert

Description

For SAM v1, this utility executes Suspicious Activity Monitoring (SAM) actions according to the information received from the standard input.

For SAM v2, this utility executes Suspicious Activity Monitoring (SAM) actions with User Defined Alerts mechanism.

For more information, see the *R80.40 CLI Reference Guide* - Chapter *Security Management Server Commands* - Section *sam_alert*.

Configuring Alerts and Thresholds in SmartView Monitor

This section describes how to configure alerts and thresholds in SmartView Monitor.

System Alerts and Thresholds

You can set thresholds for selected Security Gateways. When a threshold is passed, a system alert is sent.

To set System Alert thresholds:

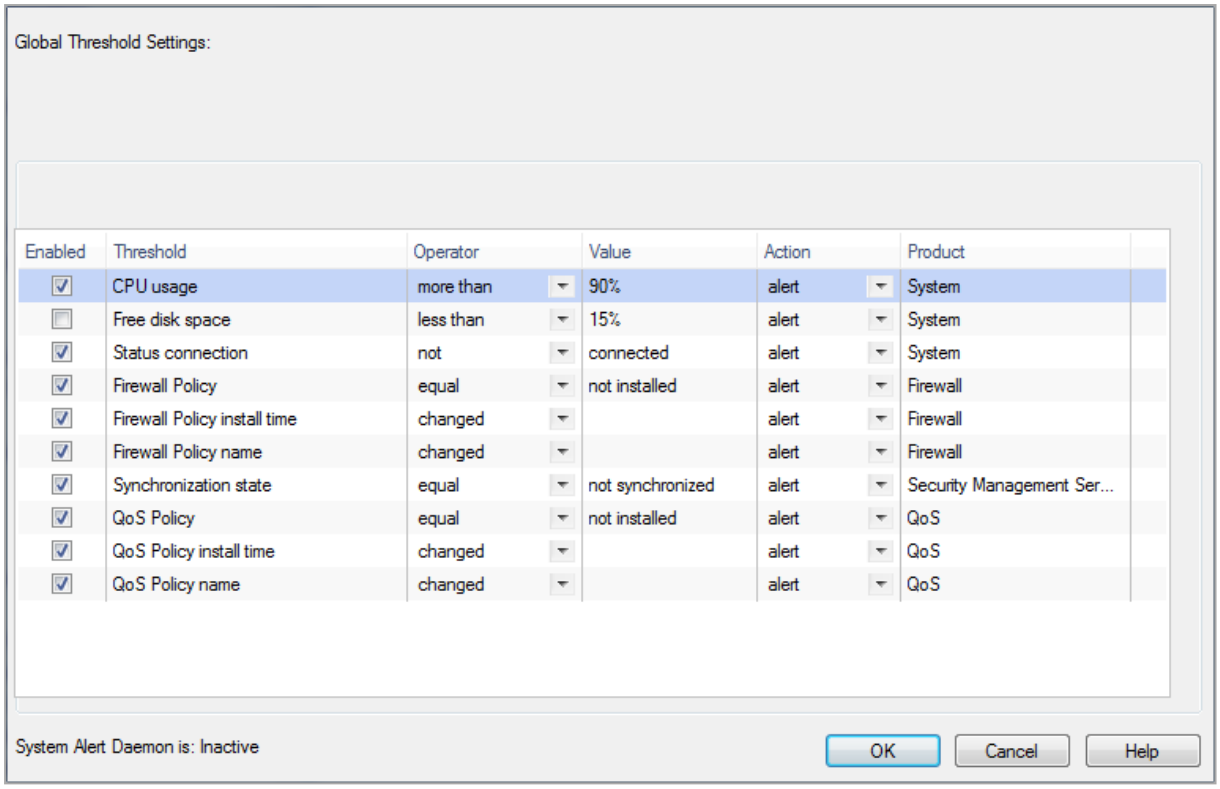
1. Open **Gateways Status** view.
2. Right-click a network object and select **Configure Thresholds**.

   The **Threshold Settings** window opens.
3. Set the thresholds for the selected object:
   - **Use global settings** - All objects get the same thresholds for system alerts.
   - **None** - The selected Security Gateway object does not have thresholds for system alerts.
   - **Custom** - Change the thresholds for the selected object to be different than the global settings.

To change Global Threshold settings:

1. In the **Threshold Settings** window, click **Edit Global Settings**.

   The **Global Threshold Settings** window opens.



2. Select thresholds.
3. In **Action**, select:
   - **none** - No alert.
   - **log** - Sends a log entry to the database.
   - **alert** - Opens a pop-up window to your desktop.
   - **mail** - Sends a mail alert to your Inbox.
   - **snmptrap** - Sends an SNMP alert.
   - **useralert** - Runs a script. Make sure a user-defined action is available (in SmartConsole, click Menu > **Global properties** > **Log and Alert** > **Alert Commands**).

To change custom threshold settings:

1. In the **Threshold Settings** window, select **Custom**.

   The global threshold settings show.
2. Select thresholds to enable for this Security Gateway or Cluster Member.
3. Set defining values.

Working with SNMP Monitoring Thresholds

You can configure a variety of different SNMP thresholds that generate SNMP traps, or alerts. You can use these thresholds to monitor many system components automatically without requesting information from each object or device. The categories of thresholds that you can configure include:

- Hardware
- High Availability
- Networking
- Resources
- Log Server Connectivity

Some categories apply only to some machines or deployments.

In each category there are many individual thresholds that you can set. For example, the hardware category includes alerts for the state of the RAID disk, the state of the temperature sensor, the state of the fan speed sensor, and others. For each individual threshold, you can configure:

- If it is enabled or disabled
- How frequently alerts are sent
- The severity of the alert
- The threshold point (if necessary)
- Where the alerts are sent to

You can also configure some settings globally, such as how often alerts are send and where they are sent to.

Types of Alerts

- *Active alerts* are sent when a threshold point is passed or the status of a monitored component is problematic.
- *Clear alerts* are sent when the problem is resolved and the component has returned to its normal value. Clear alerts look like active alerts but the severity is set to 0.

Configuring SNMP Monitoring Thresholds

Configure the SNMP monitoring thresholds in the command line of the Security Management Server. When you install the policy on the Security Gateways. the SNMP monitoring thresholds are applied globally to these Security Gateway.

Configuring SNMP thresholds on a Multi-Domain Server

In a Multi-Domain Security Management environment, you can configure thresholds on the Multi-Domain Server and on each individual Domain Management Server.

Thresholds that you configure on the Multi-Domain Server lkevel are for the Multi-Domain Server only.

Thresholds that you configure for a Domain Management Server are for that Domain Management Server and its managed Security Gateways. If a threshold applies to the Multi-Domain Server and the Security Gateways managed by the Domain Management Server, set it on the Multi-Domain Server and Domain Management Server. But in this situation you can only get alerts from the Multi-Domain Server if the threshold passed.

For example, because the Multi-Domain Server and Domain Management Server are on the same machine, if the CPU threshold is passed, it applies to both of them. But only the Multi-Domain Server generates alerts.

You can see the **Multi-Domain Security Management level** for each threshold with the "`threshold_config`" command.

- If the Multi-Domain Security Management level for a threshold is **Multi-Domain Server**:

  Alerts are generated for the Multi-Domain Server when the threshold point is passed.

- If the Multi-Domain Security Management level for a threshold is **Multi-Domain Server** and **Domain Management Server**:

  Alerts are generated for the Multi-Domain Server and Domain Management Servers separately when the threshold point is passed.

Configuring a SNMP thresholds on Security Gateways

You can configure SNMP thresholds locally on a Security Gateway with the same procedure that you do on a Security Management Server. But each time you install a policy on the Security Gateway, the local settings are erased and it reverts to the global SNMP threshold settings.

You can use the "`threshold_config`" command to save the configuration file and load it again later.

The configuration file that you can back up is: `$FWDIR/conf/thresholds.conf`

For more information about the "`threshold_config`" command, see the *R80.40 CLI Reference Guide*.

Configuration Procedures

There is one primary command to configure the thresholds in the command line - `threshold_config`. You must be in the Expert mode to run it. After you run the `threshold_config` command, follow the on-screen instructions to make selections and configure the global settings and each threshold.

When you run `threshold_config`, you get these options:

- **Show policy name** - Shows you the name configured for the threshold policy.
- **Set policy name** - Lets you set a name for the threshold policy.
- **Save policy** - Lets you save the policy.
- **Save policy to file** - Lets you export the policy to a file.
- **Load policy from file** - Lets you import a threshold policy from a file.
- **Configure global alert settings** - Lets you configure global settings for how frequently alerts are sent and how many alerts are sent.
- **Configure alert destinations** - Lets you configure a location or locations where the SNMP alerts are sent.
- **View thresholds overview** - Shows a list of all thresholds that you can set including: the category of the threshold, if it is active or disabled, the threshold point (if relevant), and a short description of what it monitors.
- **Configure thresholds** - Opens the list of threshold categories to let you select thresholds to configure.

Configure Global Alert Settings

If you select **Configure global alert settings**, you can configure global settings for how frequently alerts are sent and how many alerts are sent. You can configure these settings for each threshold. If a threshold does not have its own alert settings, it uses the global settings by default.

You can configure these options:

- **Enter Alert Repetitions** - How many alerts are sent when an active alert is triggered. If you enter 0, alerts are sent until the problem is fixed.
- **Enter Alert Repetitions Delay** - How long the system waits between it sends active alerts.
- **Enter Clear Alert Repetitions** - How many clear alerts are sent after a threshold returns to a regular value.
- **Enter Clear Alert Repetitions Delay** - How long the system waits between it sends clear alerts.

Configure Alert Destinations

If you select Configure Alert Destinations, you can add and remove destinations for where the alerts are sent. You can see a list of the configured destinations. A destination is usually an NMS (Network Management System) or a Check Point Log Server.

After you enter the details for a destination, the CLI asks if the destination applies to all thresholds.

- If you enter **yes**, alerts for all thresholds are sent to that destination, unless you remove the destination from an individual threshold.
- If you enter **no**, no alerts are sent to that destination by default. But for each individual threshold, you can configure the destinations and you can add destinations that were not applied to all thresholds.

For each threshold, you can choose to which of the alert destinations its alerts are sent. If you do not define alert destination settings for a threshold, it sends alerts to all of the destinations that you applied to all thresholds.

For each alert destination enter:

- **Name** - An identifying name.
- **IP** - The IP address of the destination.
- **Port** - Through which port it is accessed
- **Ver** - The version on SNMP that it uses
- **Other data** - Some versions of SNMP require more data. Enter the data that is supplied for that SNMP version.

Configure Thresholds

If you select Configure thresholds, you see a list of the categories of thresholds, including:

- Hardware
- High Availability
- Networking
- Resources
- Log Server Connectivity

Some categories apply only to some machines or deployments. For example, Hardware applies only to Check Point appliances and High Availability applies only to clusters or High Availability deployments.

Select a category to see the thresholds in it. Each threshold can have these options:

- **Enable/Disable Threshold** - If the threshold is enabled, the system sends alerts when there is a problem. If it is disabled it does not generate alerts.
- **Set Severity** - You can give each threshold a severity setting. The options are: Low, Medium, High, and Critical. The severity level shows in the alerts and in SmartView Monitor. It lets you know quickly how important the alert is.
- **Set Repetitions** - Set how frequently and how many alerts will be sent when the threshold is passed. If you do not configure this, it uses the global alert settings.
- **Set Threshold Point** - Enter the value that will cause active alerts when it is passed. Enter the number only, without a unit of measurement.
- **Configure Alert Destinations - See all of the configured alert destinations. By default, active alerts and clear alerts are sent to the destinations. You can change this for each destination. When you select the destination you see these options**
  - **Remove from destinations** - If you select this, alerts for this threshold are not sent to the selected destination.
  - **Add a destination** - If you configured a destination in the global alert destinations but did not apply it to all thresholds, you can add it to the threshold.
  - **Disable clear alerts** - Cleared alerts for this threshold are not sent to the selected destination. Active alerts are sent.

Completing the Configuration

1. On the Security Management Server, install the policy on all Security Gateways.
2. **For a local Security Gateway threshold policy or a Multi-Domain Server environment, use the `cpwd_admin` utility to restart the CPD process**
   a. Run: `cpwd_admin stop -name CPD -path "$CPDIR/bin/cpd_admin" -command "cpd_admin stop"`
   b. Run: `cpwd_admin start -name CPD -path "$CPDIR/bin/cpd" -command "cpd"`

Monitoring SNMP Thresholds

You can see an overview of the SNMP thresholds that you configure in SmartView Monitor.

To see an overview of the SNMP thresholds:

1. Open SmartView Monitor and select a Security Gateway.
2. In the summary of the Security Gateway data that open in the bottom pane, click **System Information**.
3. In the new pane that opens, click **Thresholds**.

In the pane that opens, you can see these details:

- **General Info - A summary of the SNMP Threshold policy.**
  - **Policy name** - The name that you set for the policy in the CLI.
  - **State** - If the policy is enabled or disabled.
  - **Thresholds** - How many thresholds are enabled.
  - **Active events** - How many thresholds are currently sending alerts.
  - **Generated Events** - How many **not active** thresholds became **active** since the policy was installed.
- **Active Events - Details for the thresholds that are currently sending alerts.**
  - **Name** - The name of the alert (given in the CLI).
  - **Category** - The category of the alert (given in the CLI), for example, Hardware or Resources.
  - **MIB object** - The name of the object as recorded in the MIB file.
  - **MIB object value** - The value of the object when the threshold became active, as recorded in the MIB file.
  - **State** - The status of the object: active or clearing (passed the threshold but returns to usual value).
  - **Severity** - The severity of that threshold, as you configured for it in the CLI.
  - **Activation time** - When was the alert first sent.
- **Alert Destinations - A list of the destinations, to which alerts are sent.**
  - **Name** - The name of the location.
  - **Type** - The type of location. For example, a Log Server or NMS.
  - **State** - If logs are sent from the Security Gateway or Security Management Server to the destination machine.
  - **Alert Count** - How many alerts were sent to the destination from when the policy started.

- **Errors - Shows thresholds that cannot be monitored.**

  For example, the Security Gateway cannot monitor RAID sensors on a machine that does not have RAID sensors. Therefore, it shows an error for the RAID Sensor Threshold.

  - **Threshold Name** - The name of the threshold with an error.
  - **Error** - A description of the error.
  - **Time of Error** - When the error first occurred.

Customizing Results

You can create Custom Views, to change the fields that show in the results.

Editing a Custom View

The changes you make to a view are not automatically saved. You can use this procedure to save a predefined view as a new Custom view.

To save a new view with changes:

1. Right-click the results of the view and select **Properties**.

   Note - For some of the views, this option is **View Properties** or **Query Properties**.
2. Add or remove fields and other options for the view.
3. Click **OK**.
4. For some of the views, select the Security Gateway.
5. In the Results toolbar, click the **Save View to Tree** button.
6. In the window that opens, enter a name for the new view.
7. Click **Save**.

Creating a Custom Gateway Status View

To create a custom Gateway status view:

1. In the **Tree**, right-click **Custom** and select **New Gateways View**.

   The **Gateway Properties** window opens.
2. In **Select available fields from**, select the source of the data.
3. In **Available fields**, double-click the data to add to SmartView Monitor.
4. Open the **Filter Gateways** tab to remove Security Gateways from the results of this view.

5. Click **OK**.
6. Right-click the new **Custom** view and select **Rename**.
7. Enter a name for the view.

Creating a Custom Traffic View

To creating a custom traffic view:

1. In the **Tree**, right-click **Custom** and select **New Traffic View**.

   The **Query Properties** window opens.
2. Select **History** or **Real Time**.
3. **If you select Real Time, select what you want to see**
   - **Interfaces**
   - **Services**
   - **IPs / Network Objects**
   - **QoS Rules**
   - **Security Rules**
   - **Connections**
   - **Tunnels**
   - **Virtual Links**
   - **Packet Size Distribution**
4. Select the **Target** Security Gateway.
   - If you often need results for on Security Gateway, select it in **Specific Gateway**.
   - If you have a small number of Security Gateways, you can create a custom view for each one.
   - If not, select **Prompt for Gateway before run**.
5. Open the next tabs.

   The tabs that show depend on the **Query Type** you selected.
   - If you select **History**, the next tab is **Traffic History**, where you select the **Time Frame** and type of report.

- If you select **Real Time**, the next tabs let you set services or objects to monitor, Security Gateways or specified IP addresses to monitor, update interval, result type, and chart settings.

6. Click **Save**.
7. Right-click the new **Custom** view and select **Rename**.
8. Enter a name for the view.

Creating a Custom Counters View

To create a custom counters view:

1. In the **Tree**, right-click **Custom** and select **New Counters View**.

   The **Query Properties** window opens.
2. Select **History** or **Real Time**.
3. Select the **Target** Security Gateway.
   - If results for one Security Gateway are frequently necessary, select it in **Specific Gateway**.
   - If you have a small number of Security Gateways, you can create a custom view for each one.
   - If not, select **Prompt for Gateway before run**.
4. Open the **Counters** tab.
5. Select a category and the counters to add.

   You can add counters from different categories to one view.
6. In the Query Type:
   - If the Query Type is **History**: Select the **Time Frame** and click **Save**.
   - **If the Query Type is Real Time:**
     a. Open the **Settings** tab.
     b. Set the update interval and chart type.
     c. Click **Save**.
7. Right-click the new **Custom** view and select **Rename**.
8. Enter a name for the view.

Creating a Custom Tunnel View

To create a custom tunnel view:

1. In the SmartView Monitor client, select **File** > **New** > **Tunnels View**.

   The **Query Properties** window shows.

2. Select **Prompt on** to generate a report about a specified Tunnel, Community or Gateway.

   Prompt on: When you run the view, you will be asked for the specified Tunnel, Community or Security Gateway, on which to base your view.

   Important - Do not select **Prompt on** if your view is not about one of these three.

3. Select **Show one record per tunnel** or **Show two records per tunnel**.

   Show two records per tunnel shows a more accurate status because the report provides the status for the tunnels in both directions.

4. In the **Show** column, select the filter to be related to this view
5. In the **Filter** column, click the corresponding **Any(*)** link.
6. Select the related objects to edit the selected filters.
7. Click the **Advanced** button.
8. Set a limit in the **Records limitation** window for the number of lines that show in the report.
9. Enter a record limitation.
10. Click **OK**.

    A **Tunnels** view shows in the **Custom** branch of the **Tree View**.

11. Enter the name of the new **Tunnel** view.
12. Click **Enter**.

Creating a Custom Users View

To create a custom users view:

1. In SmartView Monitor, select **File** > **New** > **Users View**.

   The **Query Properties** window shows.

2. Select **Prompt on** to generate a user report about a specified user or Gateway.

Prompt on: When you decide to run the view, you will be asked for the specified User DN or Security Gateway, on which to base your view.

Important - Do not select **Prompt on** if your view is not about one of these two.

3. In the **Show** column, select the filter to be related with this view.
4. In the **Filter** column, click the corresponding **Any(*)** link.
5. Select the related objects to edit the selected filters.
6. Click the **Advanced** button to set a limit (in the **Records limitation** window) to the number of lines that show in the report.
7. Enter a record limitation.
8. Click **OK**.

   A **Users** view shows in the **Custom** branch of the **Tree View**.
9. Enter a name for the new **Users** view.
10. Click **Enter**.

Custom View Example

For example purposes, we create a real-time **Traffic** view for **Services**.

To create a real-time traffic view:

1. Double-click the view to change and select the Security Gateway, for which you create the view.
2. Select the **View Properties** button on the view toolbar.

   The **Query Properties** window shows.
3. Select **Real-Time**.

   Real-Time provides information about currently monitored traffic or system counters.
4. Select **History** for information that was logged before.
5. Select the topic about which you want to create a **Real-Time** traffic view in the drop-down list provided. For example, for purposes select **Services**.

   Note - The remaining tabs in the **Query Properties** window change according to the type of view you create and the selection you made in the **Real-Time** drop-down list.
6. Select the **Target** of this **Custom Traffic** view.

   Target is the Security Gateway, for which you monitor traffic.
7. Click the **Monitor by Services** tab.

8. Select **Specific Services** and the **Services** for which you want to create a custom **Traffic** view.
9. Click the **Filter** tab.
10. Make the necessary selections.
11. Click the **Settings** tab.
12. Make the necessary selections.
13. Click **OK** when you are done with your selections.

    The **Select Gateway / Interface** window shows.
14. Select the Security Gateway or interface, for which you want to create or run this new view.
15. Click the **Save to Tree** button on the toolbar.
16. Enter a name for the new view.
17. Click **OK**.

    The new view is saved in the **Custom** branch.

Exporting a Custom View

You can back up a custom view before you install an upgrade. You can share a custom view with other SmartView Monitor GUI clients and other users.

To export a custom view:

1. Right-click the view and select **Export Properties**.
2. In the window that opens, enter a pathname for the export file.
3. Click **Save**.

   A file with an **svm_setting** extension is created.

Setting Your Default View

You can set which view to see when SmartView Monitor starts.

In the Tree, right-click the view and select **Run at Startup**.

Refreshing Views

Results are automatically refreshed every 60 seconds.

To refresh the view earlier, right-click the view name in the **Tree** and select **Run**.

To refresh data about an object in the current view, right-click the object in the results and select **Refresh**.

Monitoring Device Status

The Gateways & Servers view in SmartConsole contains 6 views of the status of the Security Management Server and all the devices it manages.

- **General** - Provides general information about all devices.
- **Health** - Provides information about the health or operational status of each device.
- **Traffic** - Provides information about the volume of network traffic which passes through a specific device
- **Access Control** - Provides information about the Access Control blades and Identity Awareness information for each device.
- **Threat Prevention** - Provides information about the Threat Prevention blades and policy for each device.
- **Management** - Provides information about the management blades for each device.
- **Licenses** - Provides information about the licenses of the device and Software Blades enabled on the device.

The **General** view is the default view. To change the view, go to the top-left corner of the **Gateways & Servers** view > **Columns**, and from the drop-down menu, select the required view.

Device Status

The status updates of a Security Gateway reflect the status of the Software Blades. For example, if statuses of all the **Software Blades** are **OK**, except for the SmartEvent blade, which has a **Problem** status, the overall status is **Problem**. You can see the statuses of the Security Gateways both in the Gateways & Servers view in SmartConsole and in SmartDashboard. To see the status updates of Security Gateways in SmartDashboard, in the **Logs & Monitor** view, go to **External Apps**, and click **Tunnel and User Monitoring**. This table summarizes the Security Gateway statuses:.

Status Icon	Description
OK	The Security Gateway and all its Software Blades work properly.
Attention	At least one Software Blade has a minor issue, but the Security Gateway works.
Problem	At least one Software Blade reported a malfunction, or an enabled Software Blade is not installed.

Status Icon	Description
Waiting	SmartView Monitor waits for the Security Management Server to send data from Security Gateways.
Disconnected	Cannot reach the Security Gateway.
Untrusted	Cannot make Secure Internal Communication between the Security Management Server and the Security Gateway.

Displaying Gateway Data

You can see detailed information about each Check Point Security Gateway or OPSEC Gateway.

To see data about a gateway:

1. In SmartConsole, go to the **Logs & Monitor** view.
2. At the bottom section of the view, go to **External Apps**, and select **Tunnel & User Monitoring**.

   The **Check Point SmartView Monitor** opens.
3. Go to **Gateway Status** > **Firewalls**.

   The **Firewalls** view displays general information about each Security Gateway.
4. For system information, click **System Information**.
5. For more information about a specific Software Blade, click the relevant Software Blade

System Information

- **OS Information** - The name, the version name/number, the build number, the service pack, and any additional information about the Operating System in use.
- **CPU** - The specific CPU parameters (for example, Idle, User, Kernel, and Total) for each CPU.
  Note - In the **Gateways Results** view the **Average CPU** indicates the average total CPU usage of all existing CPOS.
- **Memory** - The total amount of virtual memory, what percentage of this total is used. The total amount of real memory, what percentage of this total is used, and the amount of real memory available for use.

- **Disk** - Shows all the disk partitions and their specific details (for example, capacity, used, and free).
  Note - In the **Gateways Results** view the percentage/total of free space in the hard disk on which the Firewall is installed. For example, if there are two hard drives C and D and the Firewall is on C, the Disk Free percentage represents the free space in C and not D.

To view the status of Check Point applications on the local server or another appliance, the `cpstat` command. For more information, see the *R80.40 CLI Reference Guide* - Chapter *Security Gateway Commands* - Section *cpstat*.

Firewall

- **Policy information** - The name of the Security Policy installed on the Security Gateway, and the date and time that this policy was installed.
- **Packets** - The number of packets accepted, dropped and logged by the Security Gateway.
- **UFP Cache performance** - The hit ratio percentage and the total number of hits handled by the cache, the number of connections inspected by the UFP Server.
- **Hash Kernel Memory** (the memory status) and **System Kernel Memory** (the OS memory) - The total amount of memory allocated and used. The total amount of memory blocks used. The number of memory allocations, and those allocation operations which failed. The number of times that the memory allocation freed up, or failed to free up. The NAT Cache, including the total amount of hits and misses.

Virtual Private Networks

The Virtual Private Networks (VPN) is divided into these main statuses:

- **Current** represents the current number of active output.
- **High Watermark** represents the maximum number of current output
- **Accumulative data** represents the total number of the output.

This includes:

- **Active Tunnels** - All types of active VPN peers to which there is currently an open IPsec tunnel. This is useful to track the activity level of the VPN Security Gateway. High Watermark includes the maximum number of VPN peers for which there was an open IPsec tunnel since the Security Gateway was restarted.
- **Remote Access** - All types of Remote Access VPN users with which there is currently an open IPsec tunnel. This is useful to track the activity level and load patterns of VPN Security Gateways that serve as a remote access server. High Watermark includes the maximum number of Remote Access VPN users with which there was an open IPsec tunnel since the Security Gateway was restarted.

- **Tunnels Establishment Negotiation** - The current rate of successful Phase I IKE Negotiations (measured in Negotiations per second). This is useful to track the activity level and load patterns of a VPN Gateway that serve as a remote access server. High Watermark includes the highest rate of successful Phase I IKE Negotiations since the Policy was installed (measured in Negotiations per second). Accumulative data includes the total number of successful Phase I IKE negotiations since the Policy was installed.
- **Failed** - The current failure rate of Phase I IKE Negotiations can be used to troubleshoot (for instance, denial of service) or for a heavy load of VPN remote access connections. High Watermark includes the highest rate of failed Phase I IKE negotiations since the Policy was installed. Accumulative is the total number of failed Phase I IKE negotiations since the Policy was installed.
- **Concurrent** - The current number of concurrent IKE negotiations. This is useful to track the behavior of VPN connection initiation, especially in large deployments of remote access VPN scenarios. High Watermark includes the maximum number of concurrent IKE negotiations since the Policy was installed.
- **Encrypted and Decrypted throughput** - The current rate of encrypted or decrypted traffic (measured in Mbps). Encrypted or decrypted throughput is useful (in conjunction with encrypted or decrypted packet rate) to track VPN usage and VPN performance of the Security Gateway. High Watermark includes the maximum rate of encrypted or decrypted traffic (measured in Mbps) since the Security Gateway was restarted. Accumulative includes the total encrypted or decrypted traffic since the Security Gateway was restarted (measured in Mbps).
- **Encrypted and Decrypted packets** - The current rate of encrypted or decrypted packets (measured in packets per second). Encrypted or decrypted packet rate is useful (in conjunction with encrypted/decrypted throughput) to track VPN usage and VPN performance of the Security Gateway. High Watermark includes the maximum rate of encrypted or decrypted packets since the Security Gateway was restarted, and Accumulative, the total number of encrypted packets since the Security Gateway was restarted.
- **Encryption and Decryption errors** - The current rate at which errors are encountered by the Security Gateway (measured in errors per second). This is useful to troubleshoot VPN connectivity issues. High Watermark includes the maximum rate at which errors are encountered by the Security Gateway (measured in errors per second) since the Security Gateway was restarted, and the total number of errors encountered by the Security Gateway since the Security Gateway was restarted.
- **Hardware** - The name of the VPN Accelerator Vendor, and the status of the Accelerator. General errors such as the current rate at which VPN Accelerator general errors are encountered by the Security Gateway (measured in errors per second). The High Watermark includes the maximum rate at which VPN Accelerator general errors are encountered by the Security Gateway (measured in errors per second) since the Security Gateway was restarted. The total number of VPN Accelerator general errors encountered by the Security Gateway since it was restarted.

- **IP Compression** - Compressed/Decompressed packets statistics and errors.

QoS

- **Policy information** - The name of the QoS Policy and the date and time that it was installed.
- **Number of interfaces** - The number of interfaces on the Check Point QoS Security Gateway. Information about the interfaces applies to both inbound and outbound traffic. This includes the maximum and average amount of bytes that pass per second, and the total number of conversations, where conversations are active connections and connections that are anticipated as a result of prior inspection. Examples are data connections in FTP, and the "second half" of UDP connections.
- **Packet and Byte information** - The number of packets and bytes in Check Point QoS queues.

ClusterXL

- **Gateway working mode** - The Security Gateway works mode as a Cluster Member (Active or not), and its place in the priority sequence. Working modes are: ClusterXL, Load Sharing, Sync only. Running modes: Active, Standby, Ready, and Down.
- **Interfaces** - Interfaces recognized by the Security Gateway. The interface data includes the IP Address and status of the specified interface, if the connection that passes through the interface is verified, trusted or shared.
- **Problem Notes** - Descriptions of the problem notification device such as its status, priority and when the status was last verified.

OPSEC

- The version name or number, and build number of the Check Point OPSEC SDK and OPSEC product. The time it takes (in seconds) since the OPSEC Gateway is up and running.
- The OPSEC vendor can add fields to their OPSEC Application Gateway details.

Check Point Security Management

- The synchronization status indicates the status of the peer Security Management Servers in relation to that of the selected Security Management Server. View this status in the **Management High Availability Servers** window, if you are connected to the Active or Standby Security Management Server. The possible synchronization statuses are:
    - **Never been synchronized** - Immediately after the Secondary Security Management Server was installed, it did not undergo with the first manual synchronization. This synchronization brings it up to date with the Primary Management.

- **Synchronized** - The peer is synchronized correctly and has the same database information and installed Security Policy.
- **Collision** - The active Security Management Server and its peer have different installed policies and databases. The administrator must do manual synchronization and decide which of the Security Management Servers to overwrite.

- **Clients** - The number of connected clients on the Security Management Server, the name of the SmartConsole, the administrator that manages the SmartConsole, the name of the SmartConsole host, the name of the locked database, and the type of SmartConsole application.

SmartEvent Correlation Unit and the SmartEvent Server

SmartView Monitor reads statuses from the SmartEvent Correlation Unit and SmartEvent Server.

SmartEvent Correlation Unit status examples:

- Is the SmartEvent Correlation Unit active or inactive
- Is the SmartEvent Correlation Unit connected to the SmartEvent Server
- Is the SmartEvent Correlation Unit connected to the Log Server
- SmartEvent Correlation Unit and Log Server connection status
- Offline job status
- Lack of disk space status

SmartEvent Server status examples:

- Last handle event time
- Is the SmartEvent Server active or inactive
- A list of SmartEvent Correlation Unit the SmartEvent Server is connected to
- How many events arrived in a specified time period

Connect the SmartEvent Correlation Unit to the Log Server to read logs. Connect it to the SmartEvent Server to send events. If problems occur in the SmartEvent Correlation Unit connection to other components (for example, SIC problems) the problems are reported in the SmartEvent Correlation Unit status.

For the same reasons, the SmartEvent Server contains statuses that provide information about connections to all SmartEvent Correlation Unit.

Anti-Virus and URL Filtering

SmartView Monitor can now provide statuses and counters for Security Gateways with enabled Anti-Virus and URL Filtering.

The statuses are divided into these categories:

- Current Status
- Update Status (for example, when was the signature update last checked)

Anti-Virus statuses are associated with signature checks and URL Filtering statuses are associated with URLs and categories.

In addition, SmartView Monitor can now run Anti-Virus and URL Filtering counters.

For example:

- Top five attacks in the last hour
- Top 10 attacks since last reset
- Top 10 http attacks in the last hour
- HTTP attacks general info

Multi-Domain Security Management

SmartView Monitor can be used to monitor Multi-Domain Servers. This information can be viewed in the **Gateway Status** view. In this view you can see Multi-Domain Security Management counter information (for example, CPU or Overall Status).

The cpstat Command

Description

Displays the status and statistics information of Check Point applications.

Syntax

```
cpstat [-d] [-h <Host>] [-p <Port>] [-s <SICname>] [-f <Flavor>]
[-o <Polling Interval> [-c <Count>] [-e <Period>]] <Application
Flag>
```

Note - You can write the parameters in the syntax in any order.

For more information, see the *R80.40 CLI Reference Guide* - Chapter *Security Gateway Commands* - Section *cpstat*.

Starting and Stopping Cluster Members

To stop and start one member of a cluster from SmartView Monitor:

1. Open a **Gateway Status** view.
2. Right-click the cluster member and select **Cluster Member** > **Start Member** or **Stop Member**.

Monitoring VPN Tunnels

This section describes how to monitor VPN tunnels.

VPN Tunnels Solution

VPN Tunnels are secure links between gateways. These Tunnels ensure secure connections between gateways of an organization and remote access clients.

When Tunnels are created and put to use, you can keep track of their normal function, so that possible malfunctions and connectivity problems can be accessed and solved as soon as possible.

To ensure this security level, SmartView Monitor constantly monitor and analyze the status of an organization's Tunnels to recognize malfunctions and connectivity problems. With the use of **Tunnel** views, you can generate fully detailed reports that include information about the Tunnels that fulfill the specific **Tunnel** views conditions. With this information you can monitor Tunnel status, the Community with which a Tunnel is associated, the gateways, to which the Tunnel is connected, and so on.

These are the Tunnel types:

- A **Regular** tunnel refers to the ability to send encrypted data between two peers. The Regular tunnel is considered **up** if both peers have Phase 1 and Phase 2 keys.
- **Permanent** tunnels are constantly kept active. As a result, it is easier to recognize malfunctions and connectivity problems. With Permanent tunnels administrators can monitor the two sides of a VPN tunnel and identify problems without delay.

  Permanent tunnels are constantly monitored. Therefore, each VPN tunnel in the community can be set as a Permanent tunnel. A log, alert or user defined action can be issued when the VPN tunnel is down.

  The configuration of Permanent tunnels takes place on the community level and:

  - Can be specified for an entire community. This option sets every VPN tunnel in the community as permanent.

- Can be specified for a specific Security Gateway. Use this option to configure specific Security Gateways to have Permanent tunnels.
- Can be specified for a single VPN tunnel. This feature allows you to configure specific tunnels between specific Security Gateways as permanent.

This table shows the possible **Tunnel** states and their significance to a **Permanent** or **Regular** Tunnel.

State	Permanent Tunnel	Regular Tunnel
Up	The tunnel works and the data can flow with no problems.	IDE SA (Phase 1) and IPSEC SA (Phase 2) exist with a peer gateway.
Destroyed	The tunnel is destroyed.	The tunnel is destroyed.
Up Phase1	Irrelevant	Tunnel initialization is in process and Phase 1 is complete (that is, IKE SA exists with cookies), but there is no Phase 2.
Down	There is a tunnel failure. You cannot send and receive data to or from a remote peer.	Irrelevant.
Up Init	The tunnel is initialized.	Irrelevant.
Gateway not Responding	The Security Gateway is not responding.	The Security Gateway is not responding.

VPN Tunnel View Updates

If a Tunnel is deleted from SmartConsole, the **Tunnel Results View** shows the deleted Tunnel for an hour after it was deleted.

If a community is edited, the **Results View** shows removed tunnels for an hour after they were removed from the community.

Running VPN Tunnel Views

When a **Tunnel** view runs the results show in the SmartView Monitor client.

A **Tunnel** view can run:

- From an existing view
- When you create a new view
- When you change an existing view

A **Tunnels** view can be created and run for:

- Down Permanent Tunnels
- Permanent Tunnels
- Tunnels on Community
- Tunnels on a Security Gateway

Run a Down Tunnel View

Down Tunnel view results list all the **Tunnels** that are currently not active.

To run a down tunnel view:

1. In the SmartView Monitor, click the **Tunnels** branch in the **Tree View**.
2. In the **Tunnels** branch (Custom or Predefined), double-click the **Down Permanent Tunnel** view.

   A list of all the **Down Tunnels** associated with the selected view properties shows.

Run a Permanent Tunnel View

Permanent Tunnel view results list all of the existing **Permanent Tunnels** and their current status.

A **Permanent Tunnel** is a **Tunnel** that is constantly kept active.

To run a permanent tunnel view:

1. In the SmartView Monitor client, click the **Tunnels** branch in the **Tree View**.
2. In the **Tunnels** branch, double-click the **Custom Permanent Tunnel** view that you want to run.

   A list of the **Permanent Tunnels** related to the selected view properties shows.

Run a Tunnels on Community View

Tunnels on Community view results list all the **Tunnels** related to a selected Community.

To run a tunnels on community view:

1. In the SmartView Monitor client, click the **Tunnels** branch in the **Tree View**.
2. In the **Tunnels** branch (Custom or Predefined), double-click the **Tunnels on Community** view.

   A list of all Communities shows.
3. Select the Community whose **Tunnels** you want to monitor.
4. Click **OK**.

   A list of all the **Tunnels** related to the selected Community shows.

Run Tunnels on Gateway View

Tunnels on Gateways view results list all of the **Tunnels** related to a selected Security Gateway.

To run tunnels on Gateway view:

1. In the SmartView Monitor client, click the **Tunnels** branch in the **Tree View**.
2. In the **Tunnels** branch (**Custom** or **Predefined**), double-click the **Tunnels on Gateway** view.

   A list of the Security Gateways shows.
3. Select the Security Gateway, whose **Tunnels** and their status you want to see.
4. Click **OK**.

   A list of the **Tunnels** related to the selected Security Gateway shows.

Monitoring Traffic or System Counters

This sections describes how to monitor traffic or system counters.

Traffic or System Counters Solution

SmartView Monitor provides tools that enable you to monitor traffic related to specified network activities, and server, as well as the status of activities, hardware and software use of different Check Point products in real-time. With this knowledge you can:

- Block specified traffic.
- Control traffic flow on a Security Gateway.
- See how many tunnels are currently open, or the rate of new connections that pass through the VPN Gateway.

SmartView Monitor delivers a comprehensive solution to monitor and analyze network traffic and network usage. You can generate fully detailed or summarized graphs and charts for all connections intercepted and logged when you monitor traffic, and for numerous rates and figures when you count usage throughout the network.

Traffic

Traffic Monitoring provides in-depth details on network traffic and activity. As a network administrator you can generate traffic information to:

- Analyze network traffic pattern

  Network traffic patterns help administrators determine which services demand the most network resources.

- Audit and estimate costs of network us

  Monitoring traffic can provide information on how the use of network resources is divided among corporate users and departments. Reports that summarize customer use of services, bandwidth and time can provide a basis to estimate costs for each user or department.

- Identify the departments and users that generate the most traffic and the times of peak activity.
- Detect and monitor suspicious activity. Network administrators can produce graphs and charts that document blocked traffic, alerts, rejected connections, or failed authentication attempts to identify possible intrusion attempts.

A **Traffic** view can be created to monitor the **Traffic** types listed in the following table.

Traffic Type	Explanation
Services	Shows the current status view about Services used through the selected Security Gateway.
IPs/Network Objects	Shows the current status view about active IPs/Network Objects through the selected Security Gateway.
Security Rules	Shows the current status view about the most frequently used Access Control rules. The Name column in the legend states the rule number as previously configured in SmartConsole.
Interfaces	Shows the current status view about the Interfaces associated with the selected Security Gateway.
Connections	Shows the current status view about current connections initiated through the selected Security Gateway.
Tunnels	Shows the current status view about the Tunnels associated with the selected Security Gateway and their usage.
Virtual Link	Shows the current traffic status view between two Security Gateways (for example, Bandwidth, Bandwidth Loss, and Round Trip Time).
Packet Size Distribution	Shows the current status view about packets according to the size of the packets.
QoS	Shows the current traffic level for each QoS rule. **Note** - "Top QoS Rules" view in SmartView Monitor shows that almost all traffic matches the "No Match" rule when SecureXL is enabled on the Security Gateway. Refer to sk118720.

Traffic Legend Output

The values that you see in the legend depend on the **Traffic** view that you run.

All units in the view results show in configurable Intervals.

System Counters

Monitoring System Counters provides in-depth details about Check PointSoftware Blade usage and activities. As a network administrator, you can generate system status information about:

- Resource usage for the variety of components associated with the Security Gateway. For example, the average use of real physical memory, the average percent of CPU time used by user applications, free disk space, and so on.
- Security Gateway performance statistics for a variety of Firewall components. For example, the average number of concurrent CVP sessions handled by the HTTP security server, the number of concurrent IKE negotiations, the number of new sessions handled by the SMTP security server, and so on.
- Detect and monitor suspicious activity. Network administrators can produce graphs and charts that document the number of alerts, rejected connections, or failed authentication attempts to identify possible intrusion attempts.

Select and Run a Traffic or System Counters View

When a **Traffic** or **System Counters** view runs, the results show in the SmartView Monitor client. A **Traffic** or **System Counter** view can run:

- From an existing view
- When you create a new view
- When you change an existing view

To run a Traffic or System Counters view:

1. In the SmartView Monitor client, select the **Traffic** or **System Counter** branch in the **Tree View**.
2. Double-click the **Traffic** or **System Counter** view that you want to run.

   A list of available Security Gateways shows.
3. Select the Security Gateway, for which you want to run the selected **Traffic** or **System Counter** view.
4. Click **OK**.

   The results of the selected view show in the SmartView Monitor client.

Recording a Traffic or Counter View

You can save a record of the **Traffic** or **System Counter** view results.

To record a traffic or counter view:

1. Run the **Traffic** or **System Counters** view.
2. Select the **Traffic** menu.
3. Select **Recording** > **Record**.

A **Save As** window shows.

4. Name the record.
5. Save it in the related directory.
6. Click **Save**.

   The word **Recording** shows below the **Traffic** or **Counter** toolbar. The appearance of this word signifies that the view currently running is recorded and saved.
7. To stop recording, open the **Traffic** menu and select **Recording** > **Stop**.

   A record of the view results is saved in the directory you selected in step 3 above.

Play the Results of a Recorded Traffic or Counter View

After you record a view, you can play it back. You can select **Play** or **Fast Play**, to see results change faster.

To play the results:

1. In the SmartView Monitor client, select **Traffic** > **Recording** > **Play**.

   The **Select Recorded File** window shows.
2. Access the directory in which the recorded file is kept and select the related record.
3. Click **Open**.

   The results of the selected recorded view start to run. The word **Playing** shows below the toolbar.

Pause or Stop the Results of a Recorded View that is Playing

- To pause the record select **Traffic** > **Recording** > **Pause**.
- Click **Recording** > **Play** to resume to play the **Traffic** or **Counter** view results recorded before.
- To stop the record select **Traffic** > **Recording** > **Stop**.

Monitoring Users

This section describes how to monitor users.

Users Solution

The User Monitor is an administrative feature. This feature lets you to keep track of Endpoint Security VPN users currently logged on to the specific Security Management Servers. The User Monitor provides you with a comprehensive set of filters which makes the view definition process user-friendly and highly efficient. It lets you to easily navigate through the obtained results.

With data on current open sessions, overlapping sessions, route traffic, connection time, and more, the User Monitor gives detailed information about connectivity experience of remote users. This SmartView Monitor feature lets you view real-time statistics about open remote access sessions.

If specific data are irrelevant for a given User, the column shows **N/A** for the User.

Run a Users View

When you run a **Users** view, the results show in the SmartView Monitor:

- From an existing view
- When you create a new view
- When you change an existing view

A **Users** view can be created and run for:

- One user
- All users
- A specific Security Gateway
- Mobile Access user

Run a User View for a Specified User

To run a user view for a specified user:

1. In SmartView Monitor > **Tree View**, click **Users**.
2. Click **Get User by Name**.

   The **User DN Filter** window opens.
3. Enter the specified User DN in the area provided.
4. Click **OK**.

   The view results show in the **Results View**.

Run a User View for all Users or Mobile Access Users

To run a user view for all users or Mobile Access users:

1. In SmartView Monitor > **Tree View**, click **Users**.
2. Click **All Users** or **Mobile Access Users**.

   The view results show in the **Results View**.

Run a User View for a Specified Security Gateway

To run a user view for a specified Security Gateway:

1. In SmartView Monitor > **Tree View**, click **Users**.
2. Click **Users by Gateway**.

   The **Select Gateway** window shows.
3. Select the Security Gateway, for which you want to run the view.
4. Click **OK**.

   The view results show in the **Results View**.

Cooperative Enforcement Solution

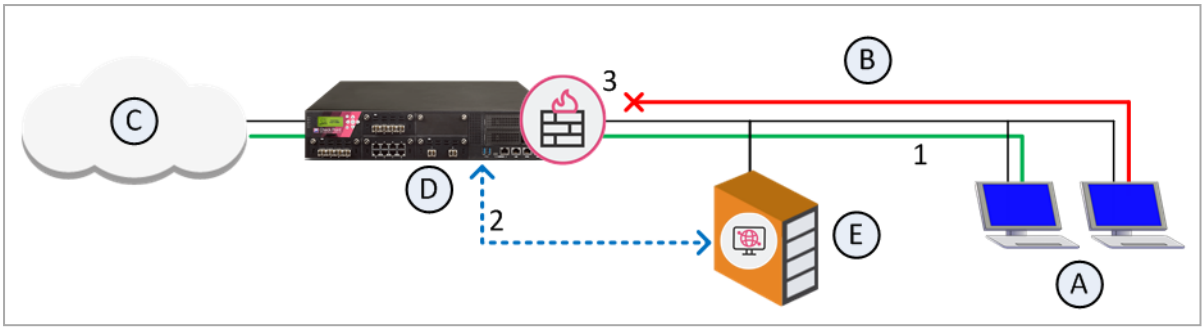
Cooperative Enforcement works with Check Point Point Endpoint Security Management Servers. This feature utilizes the Endpoint Security Management Server compliance function to make sure connections that come from different hosts across the internal network.

Endpoint Security Management Server is a centrally managed, multi-layered endpoint security solution that employs policy based security enforcement for internal and remote PCs. The Endpoint Security Management Server mitigates the risk of hackers, worms, spyware, and other security threats.

Features such as policy templates and application privilege controls enable administrators to easily develop, manage, and enforce Cooperative Enforcement.

With Cooperative Enforcement, a host that initiates a connection through a Security Gateway is tested for compliance. This increases the integrity of the network because it prevents hosts with malicious software components to access the network.

Cooperative Enforcement acts as a middle-man between hosts managed by an Endpoint Security Management Server and the Endpoint Security Management Server itself. It relies on the Endpoint Security Management Server compliance feature. It defines if a host is secure and can block connections that do not meet the defined prerequisites of software components.



—	Unauthorized
—	Authorized

1. The Endpoint Security client **(A)** in the internal network **(B)** opens a connection to the internet **(C)** through a Security Gateway **(D)**.
2. Cooperative Enforcement starts to work on the first server's reply to the client.
3. The Security Gateway sees the client's compliance in its tables and queries the Endpoint Security Management Server **(E)**.
4. When a reply is received, a connection from a compliant host to the internet is allowed.

   If the client is non-compliant and Cooperative Enforcement is not in Monitor-only mode, the connection is closed.

NAT Environments

Cooperative Enforcement is not supported by all the NAT configurations.

For Cooperative Enforcement to work in a NAT environment, the Security Gateway and the Endpoint Security Management Server must recognize the same IP address of a client. If NAT causes the IP address received by Security Gateway to be different than the IP address received by the Endpoint Security Management Server, Cooperative Enforcement will not work.

Configuring Cooperative Enforcement

To configure Cooperative Enforcement:

From the Security Gateway's **Cooperative Enforcement** page, click **Authorize clients using Endpoint Security Server** to enable Cooperative Enforcement.

- **Monitor Only** The Security Gateway requests authorization from the Endpoint Security Management Server, but connections are not dropped. Hosts can connect while the Security Gateway grants authorization. The Security Gateway generates logs for unauthorized hosts. You can add unauthorized hosts to the host's exception list or make those hosts compliant in other ways.

  If Monitor Only is not selected, Cooperative Enforcement works in **Enforcement mode**. The Endpoint Security Firewall blocks non-compliant host connections. For HTTP connections, the client is notified that its host is non-compliant. The user can change the computer to make compliant. For example, the user can upgrade the version of the Endpoint Security client.

- **Track unauthorized client status**. Set a log, or alert option for the hosts that would be dropped if not in Monitor Only mode.
- In the **Endpoint Security Server Selection** section, select which Endpoint Security Management Server is used:
  - To use this machine, select **Use Endpoint Security Server installed on this machine**.
  - To use another machine, select a server from **Select Endpoint Security Server**. Click **New** to create a new server.
- In the **Client Authorization**. section, define exceptions for client authorization.
  - **Check authorization of all clients** - Get authorization from all clients.
  - **Bypass authorization of the following clients** - Allow clients in the selected groups to always connect, without authorization inspection. All other clients are inspected.
  - **Check authorization only of the following clients** - Inspect authorization of clients from the selected groups. All other clients bypass authorization.

Non-Compliant Hosts by Gateway View

The **Non-Compliant Hosts by Gateway** view lets you to see Host IP addresses by Endpoint Security Management Server compliance:

- **Authorized** - Enables access to the internet. If a Security Gateway has **Authorized** status, it does not show in the **Non-Compliant Hosts by Gateway** view.
- **Unauthorized** - The Endpoint Security client is not compliant and the host is not authorized.
  - **Monitor Only mode** - The Endpoint Security client has access to the internet, authorized or not.
  - **Blocked mode** - Blocks access to the internet.
- **No Endpoint Security client** - The Security Gateway is not related to an Endpoint Security client.

Third-Party Log Formats

You can import these third-party log formats to a Check Point Log Server:

- Syslog messages.
- Windows Events.
- SNMP Traps.

The Log Server converts the third-party log messages to a Check Point log. The log is then available for further analysis by SmartEvent.

Importing Syslog Messages

Many third-party devices use the *syslog* format for logging. The Log Server reformats the raw data to the Check Point log format to process third-party *syslog* messages.

The Log Server uses a syslog parser to convert syslog messages to the Check Point log format.

To import syslog messages, define your own syslog parser and install it on the Log Server.

SmartEvent can take the reformatted logs and convert them into security events.

Generating a Syslog Parser and Importing syslog Messages

To import syslog messages from products and vendors that are not supported out-of-the-box, see sk55020. This shows you how to:

1. Import some sample syslog messages to the Log Parsing Editor.
2. Define the mapping between syslog fields and the Check Point log fields.
3. Install the syslog parser on the Log Server.

After you imported the syslog messages to the Log Server, you can see them in SmartConsole, in the **Logs & Monitor** > **Logs** tab.

Note - Make sure that Access Control rules allow ELA traffic between the Syslog computer and the Log Server.

Configuring SmartEvent to Read Imported Syslog Messages

After you imported the syslog messages to the Log Server, you can forward them to SmartEvent Server (and other OPSEC LEA clients), as other Check Point logs. SmartEvent converts the syslog messages into security events.

To configure the SmartEvent Server to read logs from this Log Server:

1. Configure SmartEvent to read logs from the Log Server.
2. In SmartEvent or in the SmartConsole event views, make a query to filter by the **Product Name** field. This field uniquely identifies the events that are created from the syslog messages.

Importing Windows Events

Check Point Windows Event Service is a Windows service application. It reads events from the Windows server and other configured Windows computers, converts them to Check Point logs, and places the data in the Check Point Log Server. The Log Server processes this data. The process can only be installed on a Windows computer, but it does not have to be the computer that runs Log Server. Therefore, Windows events can be processed even if the Log Server is installed on a different platform.

How Windows Event Service Works

To convert Windows events into Check Point logs:

1. Download the Windows Event Service agent `WinEventToCPLog` from the *Check Point Support Center*.
2. Install the service agent on a Windows server.

   An administrator user name and password are necessary. The administrator name is one of these:

   - A domain administrator responsible for the endpoint computer
   - A local administrator on the endpoint computer
3. Create SIC between the Windows server and the management.
4. Configure the Windows server to collect Windows events from required computers.

Administrator Support for WinEventToCPLog

`WinEventToCPLog` uses Microsoft APIs to read events from Windows operating system event files. To see these files, use the Windows Event Viewer.

`WinEventToCPLog` can read event files on the local machine, and can read log files from remote machines with the right privileges. This is useful when you make a central `WinEventToCPLog` server that forwards multiple Window hosts events to a Check Point Log Server.

To set the privileges, invoke the "`WinEventToCPLog -s`" to specify an administrator login and password.

These are the ways to access the files on a remote machine:

- To define a local administrator on the remote machine that their name matches the name registered with `WinEventToCPLog`.

- To define the administrator registered with `WinEventToCPLog` as an administrator in the domain. This administrator can access all of the machines in the domain.

Sending Windows Events to the Log Server

This section describes how to send Windows events to the Log Server. For advanced Windows event configuration, see sk98861.

Creating an OPSEC Object for Windows Event Service

In SmartConsole, create an OPSEC object for Windows Event Service.

To create an OPSEC object for windows event service:

1. From the Object Explore, click **New > Server > OPSEC Application > Application**.

   The **OPSEC Applications Properties** window shows.
2. Enter the name of the application that sends log files to the Log Server.
3. Click **New** to create a Host.
4. Enter an object name and the IP address of the machine that runs WinEventToCPLog.
5. Click **OK**.
6. Below **Client Entities**, select **ELA**.
7. Select **Communication**.
8. Enter an Activation Key, enter it again in the confirmation line, and keep a record of it for later use.
9. Click **Initialize**.

   The system must report the trust status as *Initialized but trust not established*.
10. Click **Close**.
11. Click **OK**.
12. Publish the SmartConsole session.

Note - Make sure that Access Control rules allow ELA traffic between the Windows computer and the Log Server.

Configuring the Windows service

On the Windows host, configure the Windows service to send logs to the Log Server.

To configure the Windows service:

1. Install the **WinEventToCPLog** package from the *Check Point Support Center*.
2. When the installation completes, restart the computer.
3. Open a command prompt window and go to this location:
   - On Windows 32-bit:

     ```
     C:\Program Files\CheckPoint\WinEventToCPLog\R65\bin\
     ```
   - On Windows 64-bit:

     ```
     C:\Program Files (x86)\CheckPoint\WinEventToCPLog\R65\bin\
     ```
4. Pull the certificate.

   Instructions

   a. Run:

   ```
   windowEventToCPLog -pull_cert
   ```

   b. Enter the IP address of the management server.

   c. Enter the name of the corresponding OPSEC Application object that you created in SmartConsole for the Windows events.

   d. Enter the Activation Key of the OPSEC object.
5. Restart the Check Point Windows Event Service.

Establishing Trust

Establish trust between the Security Management Server and the windows host.

To establish trust:

1. Edit the OPSEC Application that you created in SmartConsole for the Windows events.
2. Select **Communication**.
3. Make sure that the trust status is *Trust Established*.
4. Publish the SmartConsole session.

Configuring the Windows Audit Policy

On each machine that sends Windows Events, configure the Windows Audit Policy.

To configure the windows audit:

1. From the **Start** menu, click **Settings > Control Panel**.
2. Click **Administrative Tools > Local Security Policy >Local Policies >Audit Policy**.
3. Make sure that the **Security Setting** for the Policy **Audit Logon Events** is set to *Failure*. If not, double-click it and select *Failure*.
4. Open a command prompt window and go to this path:
   - On Windows 32 bit:

     ```
     C:\Program Files\CheckPoint\WinEventToCPLog\R65\bin\
     ```

   - On Windows 64 bit:

     ```
     C:\Program Files (x86)\CheckPoint\WinEventToCPLog\R65\bin\
     ```

5. Run these commands:

   windowEventToCPLog -l <*ipaddr*>, where **<ipaddr>** is the IP address of the Log Server that receives the Windows Events.

   windowEventToCPLog -a <*ipaddr*>, where **<ipaddr>** is the IP address of each machine that sends Windows Events.

   windowEventToCPLog -s, where you are prompted for an administrator name and the administrator password that to be registered with the **windowEventToCPLog** service.

   The administrator that runs the **windowEventToCPLog** service must have permissions to access and read logs from the IP addressed defined in this procedure. This is the IP address of the computer that sends Windows events.

6. When you configure **windowEventToCPLog** to read Windows events from a remote machine, log in as the administrator. This makes sure that the administrator can access remote computer events.
7. Use the Microsoft Event Viewer to read the events from the remote machine.

Working with SNMP

SNMP (Simple Network Management Protocol) is an internet standard protocol. SNMP is used to send and receive management data, protocol data units (PDUs), to network devices. SNMP-compliant devices, called agents, keep data about themselves in Management Information Bases (MIBs) and resend this data to the SNMP requesters.

For more information, see *R80.40 Gaia Administration Guide* > Chapter *System Management* > Section *SNMP*.

Log Exporter

Overview

Check Point Log Exporter is an easy and secure method to export Check Point logs over syslog in R80.20 and higher management. For information on deployment in R77.30 and R80.10 servers, see sk122323.

The Check Point App for Splunk uses the Log Exporter to seamlessly send logs from your Check Point Log Server / SmartEvent Server to your Splunk server. This enables you to collect and analyze millions of logs from all Check Point technologies and platforms. For more information, see the *App for Splunk User Guide.*

Log Exporter supports:

- **SIEM applications**: Splunk/Arcsight/RSA/LogRhythm/QRadar/McAfee/rsyslog/ng-syslog and any other SIEM application that can run a syslog agent.
- **Protocols**: Syslog over TCP or UDP.
- **Formats**: Syslog, CEF, LEEF, Generic.
- **Read-Mode**: Raw, Semi-Unified.
- **Security**: Mutual authentication TLS.
- **Types**: Security logs, Audit logs.
- **Export Links**: You can export links to the relevant log card in SmartView and the log attachment (such as Forensics\Threat Emulation report).
- **Filtering**:
  - Filter out (do not export) Security Gateway connection logs.
  - Select what to export based on field values.
  - For more information, including basic and advanced instructions for filtering, see sk122323.

How Log Exporter Works

Log Exporter is a multi-threaded daemon service which runs on a log server. Each log that is written on the log server is read by the Log Exporter daemon. It is then transformed into the applicable format and mapping and sent to the end target.

On Multi-Domain Server / Multi-Domain Log Server, if Log Exporter is deployed on several domains, each domain server has its own Log Exporter daemon service. If you export the logs to several targets, each target has its own Log Exporter daemon.

- **Extract** - Reads incoming logs from itself, the Log Server / SmartEvent Server of the Security Gateways.
- **Transform** - Changes the logs according to the configuration.
- **Export** - Sends the logs to the configured target server.

Configuring Log Exporter in CLI

This section describes the Expert mode CLI commands to configure the Log Exporter settings.

Log Exporter Basic Configuration in CLI

Common method for creating / modifying log exporters / targets.

To configure a new target for the exported logs:

1. Connect to the command line on the Management Server / Log Server.
2. Log in to the Expert mode.
3. Configure the Log Exporter settings:

```
cp_log_export add name <Name of Log Exporter Configuration>
[domain-server {mds | all}] target-server <HostName or IP
address of Target Server> target-port <Port on Target Server>
protocol {tcp | udp} format {cef | syslog} [--apply-now]
[<Other Optional Arguments>]
```

Parameters:

Parameter	Description
`name <Name of Log Exporter Configuration>`	Configures the name of the Log Exporter configuration. **Notes:** ■ Allowed characters are: Latin letters, digits ("0-9"), minus ("-"), underscore ("_"), and period ("."). ■ Must start with a letter. ■ The minimum length is two characters. ■ This command creates a new target directory with the specified unique name in the `$EXPORTERDIR/targets/` directory.

Parameter	Description
`domain-server {mds | all}`	On a Multi-Domain Server, specifies the applicable Domain Management Server context. On a Multi-Domain Log Server, specifies the applicable Domain Log Server context. This parameter is mandatory. ■ "`mds`" (in small letters) - Exports audit logs from only the main **MDS** level. ■ "`all`" (in small letters) - Exports audit logs from **all** Domains.
`target-server <HostName or IP address of Target Server>`	Configures the target server, to which Log Exporter sends the exported logs. You can enter an IP address or an FQDN.
`target-port <Port on Target Server>`	Configures the listening port on the target server, to which Log Exporter sends the exported logs.
`protocol {tcp | udp}`	Configures the Layer 4 protocol for Syslog traffic - TCP or UDP.
`format {...}`	Configures the format of exported logs: ■ `cef` - CEF ■ `syslog` - Syslog (default)
`--apply-now`	Optional. Automatically starts the new Log Exporter instance with the new settings. If you do not use this parameter, you must start the new Log Exporter instance manually with this command: `cp_log_export restart`
`<Other Optional Arguments>`	Optional. See *"Log Exporter Advanced Configuration in CLI" on page 184*.

Important - By default, Log Exporter sends the exported logs in clear text. To send the exported logs over an encrypted connection, see *"Log Exporter TLS Configuration" on page 204*.

Log Exporter Advanced Configuration in CLI

Advanced parameters for creating and modifying Log Exporter targets.

Usage

```
cp_log_export <command-name> [command-arguments]
```

To understand a specific command usage:

```
cp_log_export <command-name> help
```

Commands

Name	Description
`add`	Configures a new Check Point Log Exporter. `cp_log_export add name <Name> target-server <Target-Server> target-port <Target-Server-Port> protocol {udp | tcp} [Optional Arguments]`
`delete`	Removes an existing Log Exporter. `cp_log_export delete name <Name>`
`reconf`	Applies the Log Exporter configuration to all existing exporters. `cp_log_export reconf [name <Name>]`

`reexport`	Resets the current log position and exports all logs again based on the configuration.
	`cp_log_export reexport name <Name> --apply-now`
	`cp_log_export reexport name <Name> start-position <Position of Last Exported Log> --apply-now`
	`cp_log_export reexport name <Name> start-position <Position of Gap Start> end-position <Position of Gap End> --apply-now`

`restart`	Restarts a Log Exporter process. `cp_log_export restart name <Name>`
`set`	Updates an existing Log Exporter configuration. `cp_log_export set name <Name> [<Optional Arguments>]`
`show`	Shows the current Log Exporter configuration. `cp_log_export show [<Optional Arguments>]`
`start`	Starts an existing Log Exporter process. `cp_log_export start name <Name>`
`status`	Shows a Log Exporter overview status. `cp_log_export status [<Optional Arguments>]`

Name	Description
`stop`	Stops an existing Log Exporter process. `cp_log_export stop name <Name>`

Command Arguments

Name	Description	Required for "add" command	Required for "set" command	Required for "delete" command	Required for "reconf" command	Required for "restart", "show", "status", "start", "stop" command	Required for "reexport" command
`--apply-now`	Applies immediately any change that was done with the "`add`", "`set`", "`delete`", or "`reexport`" command.	Optional	Optional	**Mandatory**	N / A	N / A	**Mandatory**
`ca-cert <Path>`	Specifies the full path to the CA certificate file `*.pem`. **Important** - Applicable only when the value of the "`encrypted`" argument is "`true`".	Optional	Optional	N / A	N / A	N / A	N / A

Name	Description	Required for "add" command	Required for "set" command	Required for "delete" command	Required for "reconf" command	Required for "restart", "show", "status", "start", "stop" command	Required for "reexport" command
`client-cert <Path>`	Specifies the full path to the client certificate `*.p12`. **Important** - Applicable only when the value of the "`encrypted`" argument is "`true`".	Optional	Optional	N / A	N / A	N / A	N / A
`client-secret <Phrase>`	Specifies the challenge phrase used to create the client certificate `*.p12`. **Important** - Applicable only when the value of the "`encrypted`" argument is "`true`".	Optional	Optional	N / A	N / A	N / A	N / A

Name	Description	Required for "add" command	Required for "set" command	Required for "delete" command	Required for "reconf" command	Required for "restart", "show", "status", "start", "stop" command	Required for "reexport" command
`domain-server {mds | all}`	On a Multi-Domain Server, specifies the applicable Domain Management Server context. On a Multi-Domain Log Server, specifies the applicable Domain Log Server context. **Important:** ■ "`mds`" (in small letters) - Exports all logs from only the main **MDS** level. ■ "`all`" (in small letters) - Exports all logs from **all** Domains.	**Mandatory**	**Mandatory**	**Mandatory**	N / A	Optional	**Mandatory**

Name	Description	Required for "add" command	Required for "set" command	Required for "delete" command	Required for "reconf" command	Required for "restart", "show", "status", "start", "stop" command	Required for "reexport" command
`enabled {true | false}`	Specifies whether to allow the Log Exporter to start when you run the "`cpstart`" or "`mdsstart`" command. Default: `true`	Optional	Optional	N / A	N / A	N / A	N / A
`encrypted {true | false}`	Specifies whether to use TSL (SSL) encryption to send the logs. Default: `false`	Optional	Optional	N / A	N / A	N / A	N / A
`export-attachment-link {true | false}`	Specifies whether to add a field to the exported logs that represents a link to SmartView that shows the log card and automatically opens the attachment. Default: `false`	Optional	Optional	N / A	N / A	N / A	N / A

Name	Description	Required for "add" command	Required for "set" command	Required for "delete" command	Required for "reconf" command	Required for "restart", "show", "status", "start", "stop" command	Required for "reexport" command
`export-link {true | false}`	Specifies whether to add a field to the exported logs that represents a link to SmartView that shows the log card. Default: `false`	Optional	Optional	N / A	N / A	N / A	N / A

Name	Description	Required for "add" command	Required for "set" command	Required for "delete" command	Required for "reconf" command	Required for "restart", "show", "status", "start", "stop" command	Required for "reexport" command
`export-link-ip {true | false}`	Specifies whether to make the links to SmartView use a custom IP address (for example, for a Log Server behind NAT). **Important** - Applicable only when the value of the "`export-link`" argument is "`true`", or the value of the "`export-attachment-link`" argument is "`true`". Default: `false`	Optional	Optional	N / A	N / A	N / A	N / A

Name	Description	Required for "add" command	Required for "set" command	Required for "delete" command	Required for "reconf" command	Required for "restart", "show", "status", "start", "stop" command	Required for "reexport" command
`filter-action-in {"Action1","Action2",... | false}`	Specifies whether to export all logs that contain a specific value in the "**Action**" field. Each value must be surrounded by double quotes (""). Multiple values are supported and must be separated by a comma without spaces. To see all valid values: 1. In SmartConsole, go to the **Logs & Monitor** view and open the **Logs** tab. 2. In the top query field, enter **action:** and a letter. Examples of values:	Optional	Optional	N / A	N / A	N / A	N / A

Name	Description	Required for "add" command	Required for "set" command	Required for "delete" command	Required for "reconf" command	Required for "restart", "show", "status", "start", "stop" command	Required for "reexport" command
	■ **Accept** ■ **Block** ■ **Bypass** ■ **Detect** ■ **Drop** ■ **HTTPS Bypass** ■ **HTTPS Inspect** ■ **Prevent** ■ **Reject** **Important** - This parameter replaces any other filter configuration that was declared earlier on this field directly in the filtering XML file. Other field filters are not overwritten.						

Name	Description	Required for "add" command	Required for "set" command	Required for "delete" command	Required for "reconf" command	Required for "restart", "show", "status", "start", "stop" command	Required for "reexport" command
`filter-blade-in {"Blade1","Blade2",... | false}`	Specifies whether to export all logs that contain a specific value in the "**Blade**" field (the object name of the Software Blade that generated these logs). Each value must be surrounded by double quotes (""). Multiple values are supported and must be separated by a comma without spaces. To see all valid values: 1. In SmartConsole, go to the **Logs & Monitor** view and open the **Logs** tab.	Optional	Optional	N / A	N / A	N / A	N / A

Name	Description	Required for "add" command	Required for "set" command	Required for "delete" command	Required for "reconf" command	Required for "restart", "show", "status", "start", "stop" command	Required for "reexport" command
	2. In the top query field, enter **blade:** and a letter. Examples of values: ■ **Anti-Bot** ■ **Firewall** ■ **HTTPS Inspection** ■ **Identity Awareness** ■ **IPS** Valid Software Blade families: ■ **Access** ■ **TP** ■ **Endpoint** ■ **Mobile**						

Name	Description	Required for "add" command	Required for "set" command	Required for "delete" command	Required for "reconf" command	Required for "restart", "show", "status", "start", "stop" command	Required for "reexport" command
	Important - This parameter replaces any other filter configuration that was declared earlier on this field directly in the filtering XML file. Other field filters are not overwritten.						

Name	Description	Required for "add" command	Required for "set" command	Required for "delete" command	Required for "reconf" command	Required for "restart", "show", "status", "start", "stop" command	Required for "reexport" command
`filter-origin-in {"Origin1","Origin2",... | false}`	Specifies whether to export all logs that contain a specific value in the "**Origin**" field (the object name of the Security Gateway / Cluster Member that generated these logs). Each origin value must be surrounded by double quotes (""). Multiple values are supported and must be separated by a comma without spaces.	Optional	Optional	N / A	N / A	N / A	N / A

Name	Description	Required for "add" command	Required for "set" command	Required for "delete" command	Required for "reconf" command	Required for "restart", "show", "status", "start", "stop" command	Required for "reexport" command
	Important - This parameter replaces any other filter configuration that was declared earlier on this field directly in the filtering XML file. Other field filters are not overwritten.						
`format {cef | syslog}`	Specifies the format, in which the logs are exported. Default: `syslog`	Optional	Optional	N / A	N / A	N / A	N / A

Name	Description	Required for "add" command	Required for "set" command	Required for "delete" command	Required for "reconf" command	Required for "restart", "show", "status", "start", "stop" command	Required for "reexport" command
`name "<Name>"`	Specifies the unique name of the Log Exporter configuration.	**Mandatory**	**Mandatory**	**Mandatory**	Optional. By default, applies to all.	Optional. By default, applies to all.	**Mandatory**

Name	Description	Required for "add" command	Required for "set" command	Required for "delete" command	Required for "reconf" command	Required for "restart", "show", "status", "start", "stop" command	Required for "reexport" command
	Notes: ■ Allowed characters are: Latin letters, digits ("0-9"), minus ("-"), underscore ("_"), and period ("."). ■ Must start with a letter. ■ The minimum length is two characters. ■ The "add" command creates a new target directory with the specified unique name in the $EXPORTERDIR/targets/ directory.						

Name	Description	Required for "add" command	Required for "set" command	Required for "delete" command	Required for "reconf" command	Required for "restart", "show", "status", "start", "stop" command	Required for "reexport" command
`protocol {tcp | udp}`	Specifies the Layer 4 Transport protocol to use (TCP or UDP). There is no default value.	**Mandatory**	Optional	N / A	N / A	N / A	N / A

Name	Description	Required for "add" command	Required for "set" command	Required for "delete" command	Required for "reconf" command	Required for "restart", "show", "status", "start", "stop" command	Required for "reexport" command
`read-mode {raw | semi-unified}`	Specifies the mode, in which to read the log files. ■ `raw` - Specifies to export log records without any unification. ■ `semi-unified` - Specifies to export log records with step-by-step unification. That is, for each log record, export a record that unifies this record with all previously-encountered records with the same ID. Default: `raw`	Optional	Optional	N / A	N / A	N / A	N / A

Name	Description	Required for "add" command	Required for "set" command	Required for "delete" command	Required for "reconf" command	Required for "restart", "show", "status", "start", "stop" command	Required for "reexport" command
`target-port <Target-Server-Port>`	Specifies the listening port on the target server, to which you export the logs.	**Mandatory**	Optional	N / A	N / A	N / A	N / A
`target-server <Target-Server>`	Specifies the IP address or FQDN of the target server, to which you export the logs.	**Mandatory**	Optional	N / A	N / A	N / A	N / A

Log Exporter TLS Configuration

How to get a secured connection between the Log Exporter and the syslog server.

The only allowed authentication method via TLS is mutual authentication. For mutual authentication, Log Exporter needs these certificates:

- A **pem** Certificate Authority (CA) certificate
- A **p12** format client certificate

If you do not already have the required certificates, this procedure is an example of how to create the required certificates. There are also alternative procedures.

All commands need to run on the CA server.

Note - The CA server needs to be routable from the Log Exporter device.

To create a self signed CA:

Run this if you do not already have a trusted CA pem:

1. Generate the root CA key and do not pass to anyone:

   ```
   openssl genrsa -out RootCA.key 2048
   ```

2. Generate the root CA pem:

   ```
   openssl req -x509 -new -nodes -key RootCA.key -days 2048 -out
   RootCA.pem
   ```

3. Enter the **Distinguished Name (DN)** information for the certificate.
   - **Common Name(CN)** is the exact Fully Qualified Domain Name (FQDN) of the host that you use the certificate with.
   - All other fields are optional. If you purchase an SSL certificate from a certificate authority, these additional fields may be required.

An example of the prompt to provide information:

```
Country Name (2 letter code) [AU]:US

State or Province Name (full name) [Some-State]:New York

Locality Name (eg, city) []:MyCity

Organization Name (eg, company) [Internet Widgits Pty Ltd]:MyCompany

Organizational Unit Name (eg, section) []:MyDepartment

Common Name (e.g. server FQDN or YOUR name) []:www.company.com
```

```
Email Address []:
```

To create a client (log_exporter) .p12 certificate file:

1. Generate the client key and do not pass to anyone:

   ```
   openssl genrsa -out log_exporter.key 2048
   ```

2. Generate the client certificate sign request:

   ```
   openssl req -new -key log_exporter.key -out log_exporter.csr
   ```

3. Use the CA files to sign the certificate:

   ```
   openssl x509 -req -in log_exporter.csr -CA RootCA.pem -CAkey
   RootCA.key -CAcreateserial -out log_exporter.crt -days 2048 -
   sha256
   ```

4. Convert to p12 format:

   ```
   openssl pkcs12 -inkey log_exporter.key -in log_exporter.crt -
   export -out log_exporter.p12
   ```

Note - The challenge phrase used in this conversion is required in the `log_exporter` TLS configuration.

After you create the required certificates, update the security parameters on the Check Point exporting server:

To update the security parameters:

1. If running on Multi-Domain Server / Multi-Domain Log Server, switch to the required domain. Run:

   ```
   mdsenv <IP Address or Name of Domain Management Server>
   ```

2. Go to the deployment directory:

   ```
   cd $EXPORTERDIR/targets/<Deployment Name>
   ```

3. Create a directory for the certificates:

   ```
   mkdir certs
   ```

4. Copy `RootCA.pem` and `log_exporter.p12` to the certs directory

5. Give the `RootCA.pem` and `log_exporter.p12` execution privilege

   ```
   chmod +r RootCA.pem
   ```

   ```
   chmod +r log_exporter.p12
   ```

6. Update the `targetConfiguration.xml` file with the full path to the certificates and the challenge phrase used to create the .p12 certificate

To create a server (target) certificate:

1. Generate the server key and do not pass to anyone:

   ```
   openssl genrsa -out syslogServer.key 2048
   ```

2. Generate the server certificate sign request:

   ```
   openssl req -new -key syslogServer.key -out syslogServer.csr
   ```

3. Use the CA files to sign the certificate:

   ```
   openssl x509 -req -in syslogServer.csr -CA RootCA.pem -CAkey
   RootCA.key -CAcreateserial -out syslogServer.crt -days 2048 -
   sha256
   ```

Log Exporter Advanced Configuration Parameters

After deploying a new instance of Log Exporter, all configuration files for that deployment are located in this directory:

```
$EXPORTERDIR/targets/<Name of Log Exporter Configuration>/
```

Note - On a Multi-Domain Server / Multi-Domain Log Server, the value of the environment variable `EXPORTERDIR` changes automatically when you switch between Domain server contexts with the `mdsenv` command.

Important:

- You must restart the Log Exporter instance for the new settings to take effect. Run the "`cp_log_export restart`" command.
- For information on how to backup and restore your Log Exporter configuration, see sk127653.

You can configure specific parameters to control how Log Exporter exports the logs.

Target Server Configuration

The Log Exporter configuration for the target server is saved in this file:

```
$EXPORTERDIR/targets/<Name of Log Exporter Configuration>/targetConfiguration.xml
```

These are some of the configuration options:

Parameter	Description	Valid / Default Values
`<version></version>`	Current Log Exporter version - used for upgrades.	
`<is_enabled></is_enabled>`	Determines if the Log Exporter process is monitored by the watch dog.	true false

Destination Parameters

Parameter	Description	Valid / Default Values
`type`	Reserved for future use.	
`<ip></ip>`	The IP address of the target server that receives the logs.	Any IPv4 address or FQDN
`<port></port>`	The port on the target.	Any valid port number
`<protocol></protocol>`	The protocol used in the connection.	TCP or UDP

Security Parameters

These are discussed in more detail in *"Log Exporter TLS Configuration" on page 204*.

Parameter	Description	Valid / Default Values
`<security></security>`	Determines if the connection is sent in clear text or encrypted.	▪ `clear` - clear text (this is the default) ▪ `tls` - encrypted
`<pem_ca_file></pem_ca_file>`	The location of the root Certificate Authority certificate file in the PEM format.	
`<p12_certificate_file></p12_certificate_file>`	The location of the client key pair in the P12 format.	
`<client_certificate_challenge_phrase></client_certificate_challenge_phrase>`	The challenge phrase that was used to create the P12 certificate. The value is hashed when the Log Exporter is started or restarted.	

Source Parameters

Parameter	Description	Valid / Default Values
`<folder></folder>`	The path where the log files are located.	Default location is `$FWDIR/log/`
`<log_files></log_files>`	Determines which log records to export or how far back to read the log records from the `$FWDIR/log/fw.log` file.	■ *<Number>* - reads logs from the specific number (default=1) of days back (recommended) ■ *<Specific File Name>* - reads logs from the specified file ■ `on-line` ■ If no value is specified, uses '`on-line`'
`<log_types></log_types>`	Determines which logs to export.	■ `all` - Security and Audit (default) ■ `log` - Security only ■ `audit` - Audit only

Resolver Parameters

Parameter	Description	Valid / Default Values
`<mappingConfiguration></mappingConfiguration>`	Configures the XML file that contains the log field mapping scheme. If left empty, uses the default settings.	Default values are based on the format
`<exportAllFields>true</exportAllFields>`	When this field is set to '`true`', all log fields are sent regardless of whether they appear in the mapping scheme, except for specifically black-listed fields in the relevant log format mapping file (`<exported>false</exported>`). When this field is set to '`false`', only those fields which appear in the relevant log format mapping file are sent (with exported flag set to '`true`': `<exported>true</exported>`)	■ `true` ■ `false`

Format Parameters

Parameter	Description	Valid / Default Values
`<formatHeaderFile></formatHeaderFile>`	Configures the XML file that contains the log header format scheme. If left empty, uses the default settings.	Default values are based on the format

SmartView Link Parameters

Parameter	Description	Valid / Default Values
`export_log_link`	Adds a field to the exported log that represents a link to SmartView that shows the log card.	■ `true` ■ `false` (default)
`export_attachment_link`	Adds a field to the exported log that represents a link to SmartView that shows the log card and automatically opens the attachment.	■ `true` ■ `false` (default)
`export_link_ip`	Makes the above two links use a customized IP address (for example, for a NATed Log Server).	■ IPv4 address ■ empty (default)

Filter Parameters

This configuration allows Log Exporter instance to filter out the Security Gateway traffic logs for several Software Blades (**VPN-1 & Firewall-1**, **HTTPS Inspection**, and **Security Gateway/Management**).

Note:

- Security Gateway session logs are still exported (generated by tracking a Security Gateway rule per session).
- HTTPS Inspection logs, Security Gateway logs generated not from rules, and a few NAT update logs are still exported.

Parameter	Description	Valid / Default Values
`<filter filter_out_by_connection="false">`	Determines whether to filtered out the Access logs. When set to `true`, **VPN-1 & Firewall-1** logs are filtered out (**HTTPS Inspection** logs are still exported). **Note** - These are the only Software Blade filters currently supported.	■ `true` ■ `false`

Format Configuration

The Log Exporter format configuration is saved in these files:

```
$EXPORTERDIR/targets/<Name of Log Exporter
Configuration>/conf/*FormatDefinition.xml
```

Important - Do **not** edit the original `*FormatDefinition.xml` files. **Doing so causes a data loss after an upgrade**. Instead, create a copy of the file and modify the copied file, while leaving the original intact. After modifying the copied file, refer to it (using a full path) in the `<formatHeaderFile>` element in the applicable `targetConfiguration.xml` file.

Body

Parameter	Description	Syslog	Splunk	CEF	LEEF	Generic	LogRhythm	RSA
`<start_message_body></start_message_body>`	The character that precedes the log data payload.	`[`						
`<end_message_body></end_message_body>`	The character that follows the log data payload.	`]`						
`<message_separator></message_separator>`	The delimeter that separates logs.	`
(
=='\n')`	`
('\n')`	`
('\n')`	`
('\n')`	`('\n')`	`
('\n')`	`
('\n')`

Parameter	Description	Syslog	Splunk	CEF	LEEF	Generic	LogRhythm	RSA
<fields_separatator></fields_separatator>	The delimeter that separates log fields.	'; ' (semi colon, space)	| (pipe)	' ' (space)	(<TAB>)	' ' (space)	| (pipe)	' ' (space)
<field_value_separatator></field_value_separatator>	The assignment operator.	:	=	=	=	=	=	=
<value_encapsulation_start>"</value_encapsulation_start>	The value encapsulation operator (start).	"			"	"		
<value_encapsulation_start>"</value_encapsulation_start>	The value encapsulation operator (end).	"			"	"		

Parameter	Description	Syslog	Splunk	CEF	LEEF	Generic	LogRhythm	RSA
<escape_chars> <char> <orig></orig> <escaped></escaped> </char> </escape_chars>	To escape unwanted characters. The escape functionality replaces the string that is encapsulated by the orig tags with the string encapsulated by the escaped tags.	;\ --> \\ " --> \"
--> ' '] --> \]	| --> ; = --> \=
--> ' '	;\ --> \\ = --> \=
--> ' ' | --> \\|	= --> \=
--> ' '	\ --> \\ " --> '
--> ' '	| --> ; = --> \=
--> ' '	= --> \=
--> ' '

Header

Parameter	Description	Default values for sysl	Default values for CEF
<header_format></header_format>	The delimeter between the header values and the number of values. Every {} is replaced with one value.	' ' (space)	|

Notes:

- To add a constant string to the header, add the string to the `<header_format>` tag value.
- To add a new field to the header, add a new header format replacement string (for example: `{}`) to the `<header_format>` tag and add the applicable information in the `<headers>` tag.

Field Mapping Configuration

Every format has its own predefined fields configuration file that allow to change the name / value of the exported field, filter out irrelevant fields, and so on.

The Log Exporter format configuration is saved in these files:

```
$EXPORTERDIR/targets/<Name of Log Exporter Configuration>/conf/*FieldsMapping.xml
```

Important - Do **not** edit the original `*FieldsMapping.xml` files. **Doing so causes a data loss after an upgrade**. Instead, create a copy of the file and modify the copied file, while leaving the original intact. After modifying the copied file, refer to it (using a full path) in the `<formatHeaderFile>` element in the applicable `targetConfiguration.xml` file.

Parameter	Description	Valid / Default Values
`<table>`	Some fields appear in the tables based on the log format. This information can be found in the `.elg` log file - one entry for every new field. A field can appear in multiple tables. Each distinct instance is considered a new field.	
`<exported></exported>`	**Optional** You can use the exported true/false tag in the mapping configuration file to filter out specific fields. Alternatively, if the `exportAllFields` tag in the `targetConfiguration.xml` file is set to `false`, only those fields which are listed in the mapping file are exported.	■ `true` ■ `false`
`<origName></origName>`	The name of the field that is mapped to *<dstName>*	
`<dstName></dstName>`	The new mapping scheme name for the applicable field.	
`<required></required>`	**Optional** When set to `true`, only logs that contain this field are exported.	■ `true` ■ `false`

Log Exporter Instructions for Specific SIEM

This section shows how to configure SIEM applications to receive logs optimally.

Notes:

- When using Client Authentication, you must provide the absolute path to the client certificate.
- Make sure the "Common Name" is unique in every certificate.

Rsyslog

Procedure

By default, Rsyslog is not configured to use the RFC 5424 timestamp format.

Therefore, you should manually change the setting on the Rsyslog server for it to be compliant with the Log Exporter output format.

1. Edit the `/etc/rsyslog.conf` file:

   ```
   vi /etc/rsyslog.conf
   ```

2. Comment out this line (add the # character in the beginning), if it is not commented out already:

   ```
   #"$ActionFileDefaultTemplate RSYSLOG_TraditionalFileFormat"
   ```

3. Add this line in the file:

   ```
   $ActionFileDefaultTemplate RSYSLOG_SyslogProtocol23Format
   ```

4. Save the changes in the file and exit the editor.

5. Restart the Rsyslog service:

   ```
   service rsyslog restart
   ```

ArcSight

Procedure

ArcSight recommends to name the server certificate file as "`syslog-ng`".

To name the certificate:

Convert the key to the P12 format:

```
openssl pkcs12 -inkey syslogServer.key -in syslogServer.crt -
export -out syslog-ng.p12 -name "syslogng-alias" -password
pass:changeit
```

To make sure the value of the environment variable ARCSIGHT_HOME is the connector install directory:

1. Run the certificates manager on the Linux KDE console:

   ```
   $ARCSIGHT_HOME/current/bin/arcsight agent keytoolgui
   ```

2. From the **File** menu, open the keystore:

   ```
   $ARCSIGHT_HOME/current/jre/lib/security/cacerts
   ```

   The password "`changeit`".

3. From the menu, select **Import Trusted Certificate**.
4. From the file dialog, select **Ca.pem** and save it.
5. Save the changes and close the certificate manager.

To edit the "agent.properties" file to enable mutual authentication:

1. Edit the file:

   ```
   vi $ARCSIGHT_HOME//current/user/agent/agent.properties
   ```

2. Change this value to true:

   ```
   syslogng.mutual.auth.enabled=true
   ```

3. Add these lines to the end:

   ```
   syslogng.tls.keystore.file=user/agent/syslog-ng.p12
   syslogng.tls.keystore.alias=syslogng-alias
   ```

4. Restart the connector service:

   ```
   /etc/init.d/arc_connector_name restart
   ```

Splunk

Procedure

1. Generate the server certificate file in the PEM format:

   ```
   cat syslogServer.crt syslogServer.key RootCA.pem >
   splunk.pem
   ```

2. Update the `inputs.conf` file on the Splunk server:

   a. Edit the file:

   ```
   vi /opt/splunk/etc/apps/<Name of the app, where the
   configuration is saved>/local/inputs.conf
   ```

   b. Configure these settings to use TLS:

   ```
   [SSL]
   serverCert = <Full path to CA PEM file>
   sslPassword = <Challenge Password>
   requireClientCert = true
   [tcp-ssl://<Port>]
   index = <Index>
   ```

   c. Save the changes in the file and exit the editor.

3. Update the `server.conf` file on the Splunk server:

   a. Edit the file:

   ```
   vi /opt/splunk/etc/system/local/server.conf
   ```

   b. Configure these settings:

   ```
   [sslConfig]
   sslRootCAPath = <Full path to CA PEM file>

   [SSL]
   cipherSuite = TLSv1+HIGH:TLSv1.2+HIGH:@STRENGTH
   ```

   c. Save the changes in the file and exit the editor.

4. Restart the Splunk service:

   ```
   /opt/splunk/bin/splunk restart
   ```

QRadar

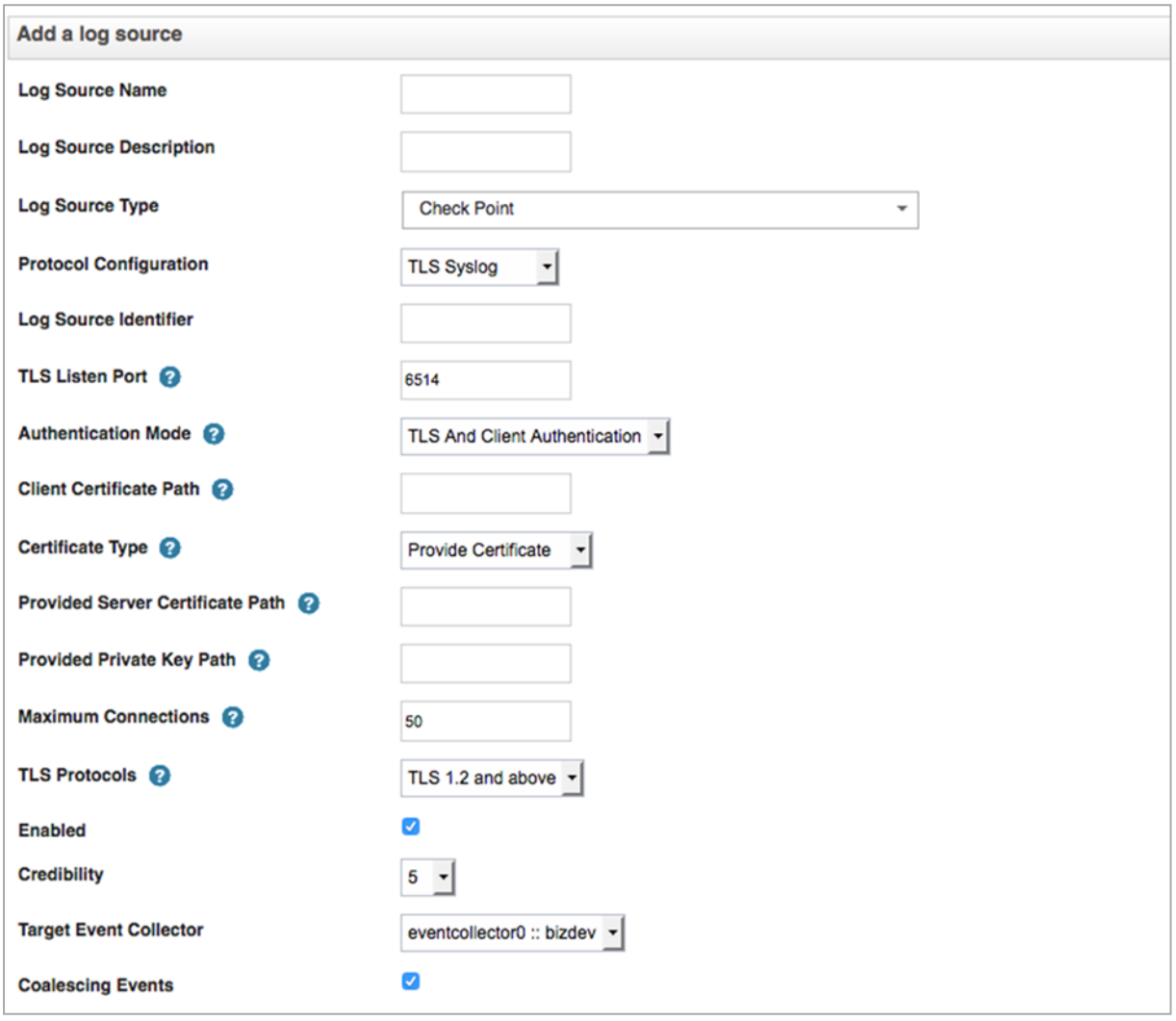
Procedure

1. In the **Authentication Mode** field, select **TLS And Client Authentication**.

   When you use **Client Authentication**, you must provide the absolute path to the client certificate.

2. Upload the Check Point certificate and private key to QRadar to the same directory.

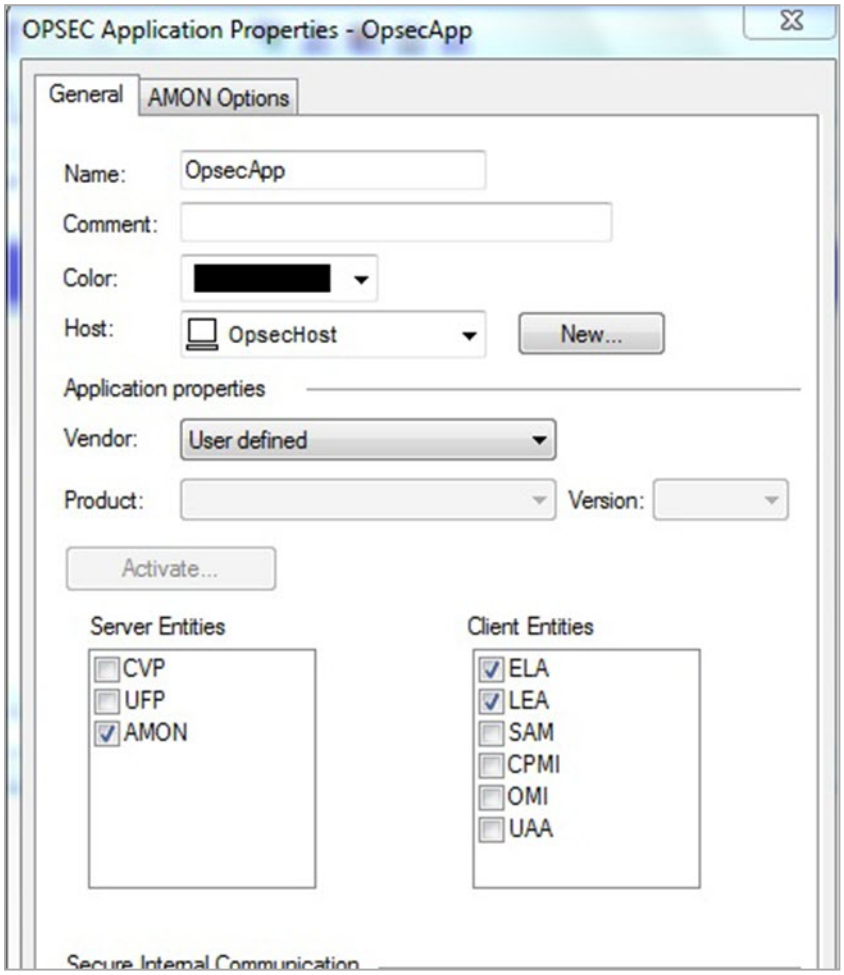
3. Enter the absolute path to the uploaded files in the **Provide Certificate** option.



Transition from LEA to Log Exporter

To move from the existing LEA connector to the new Log Exporter:

1. Delete the OPSEC application object from the GUI, if it is the only use for the OPSEC application. If not, remove the LEA client entity.



2. If this is the only OPSEC LEA client, configure $FWDIR/conf/fwopsec.conf to not allow LEA:

   Comment out these lines:

From	To
#	#
lea_server auth_port 18184	# lea_server auth_port 18184
lea_server port 0	# lea_server port 0

From	To
#	#

3. Install the Log Exporter according to the installation guide above.

Note - Reading logs through LEA, which were configured manually in the SmartLog custom settings file, is not available in R80.x.

Transition from CPLogToSyslog to Log Exporter

To move from the existing CPLogToSyslog to the new Log Exporter:

1. Use CPUSE to uninstall the CPLogToSyslog package. See section 4-C in sk92449.
2. Install the Log Exporter according to the installation guide above.

Log Exporter - Appendix

Special Log Fields

Field	Description
loguid	Log Unification ID. Some Check Point logs are updated over time. Updated logs have the same Log UID value. Check Point SmartLog client correlates those updates into a single unified log. When the update logs are sent to 3rd party servers, they arrive as distinct logs. Administrators can use the "`loguid`" field to correlate updated logs and get the full event chain. **Note** - Log Exporter's new semi-unified mode correlates all previous logs into one, so the latest log always shows the complete data. Examples of updated logs: ■ The total amount of bytes sent and received over time. ■ The severity field which is updated over time as more information becomes available.
hll_key	High Level Log Key. This concept was introduced in R80.10. Multiple connection logs can comprise one session with one shared HLL Key. For example, when you browse to a webpage, the Security Gateway may generate multiple connection logs which are related to the same session. Connection logs which are part of the same session share the same "`hll_key`" value.

Syslog-NG Listener Configuration

We recommend you use the syslog-protocol flag when you configure a source on a Syslog NG server.

For example:

```
source s_network { network(transport("tcp") port(514) flags
(syslog-protocol) ); };
```

Splunk Listener Configuration

We recommend that you add these time settings to your "`sourcetype`":

- `TIME_FORMAT = %s`
- `TIME_PREFIX = time=`
- `MAX_TIMESTAMP_LOOKAHEAD = 15`

ArcSight Listener Configuration

The Log Exporter solution does not work with the OPSEC LEA connector. Instead, you must install the ArcSight Syslog-NG connector.

ArcSight Common Event Format (CEF) Mapping

CEF is an extensible, text-based format that supports multiple device types by offering the most relevant information. Message syntax is reduced to work with ESM normalization. Specifically, CEF defines a syntax for log records comprised of a standard header and a variable extension, formatted as key-value pairs. The CEF format can be used with on-premises devices by implementing the ArcSight Syslog SmartConnector. CEF can also be used by cloud-based service providers by implementing the SmartConnector for ArcSight Common Event Format REST.

CEF Header Format

Item	Version	Device Vendor	Device Product	Device Version	Device Event Class ID	Name	Severity
Default	CEF:0	Check Point	Log Update	Check Point	Log	Log	0

Item	Version	Device Vendor	Device Product	Device Version	Device Event Class ID	Name	Severity
Values	-	-	Product Name (Blade)	-	■ Attack Name ■ Protection Type ■ Verdict ■ Matched Category ■ DLP Data Type ■ Application Category ■ Application Properties	■ Protection Name ■ Application Name ■ Message Info ■ Service ID ■ Service	■ Application Risk ■ Risk ■ Severity

QRadar Log Event Extended Format (LEEF) Mapping

The LEEF is a customized event format for IBM Security QRadar.

LEEF Header Format

Item	LEEF Version	Vendor	Product	Version	EventID
Default	LEEF:2.0	Check Point	Log Update	1.0	Check Point Log
Values	-	-	Product Name (Blade)	-	■ Protection Name ■ Application Name ■ Action

Note - The time format is not compliant with the official LEEF format.

As there is currently no Epoch time format, Log Exporter with LEEF format is only partially supported.

Command Line Reference

See the *R80.40 CLI Reference Guide*.

Appendix: Manual Syslog Parsing

Many third-party devices use the *syslog* format to log. The Log Server reformats the raw data to the Check Point log format to process third-party *syslog* messages. SmartEvent can take the reformatted logs and convert them into security events.

You can use the Log Parsing Editor to make a parsing file (see *"Importing Syslog Messages" on page 44*). As an alternative you can manually create a parsing file. This section shows you how to do that.

Warning - Manual modifications to out-of-the-box parsing files cannot be preserved automatically during an upgrade. Mark your modifications with comments so you can remember what changed.

Planning and Considerations

1. Learn the accurate structure of the logs the device generates with these guides.
   a. The vendor logging guide, or other documentation that specifies the logs the device can generate and their structure. Documentation is important to make sure that you found all possible logs. Usually it is sufficient to write the parsing file.
   b. Log samples, as many as possible. Use logs generated from the actual devices to be used with SmartEvent. Samples are important to examine the parsing file and to tune it accordingly.
2. Learn and know *"The Free Text Parsing Language" on page 234* and the necessary parsing files and their location on the Log Server (see *"The Parsing Procedure" on page 246*).
3. Compare existing parsing files of an equivalent product.
4. Select the fields to extract from the log. The fields to extract are different from one device to another. But devices of the same category usually have equivalent log fields. For example:

Device Type	Typical Log Fields
Firewall, router and other devices that send connection based logs	source IP address, destination IP address, source port, destination port, protocol, accept/reject indication
IDS / IPS, application Firewall and other devices that send attack logs	attack name/ID

The Parsing Procedure

The procedure occurs on the Log Server and starts with the syslog daemon. The syslog daemon that runs on the Log Server receives the syslogs and calls for their parsing. The parsing involves many parsing files, which contain the different parsing definitions and specifications, and can be found in the **$FWDIR/conf/syslog/** directory. In these files there are the device-specific parsing files, which define the actual parsing and extraction of fields, according to each device specific syslog format.

The parsing starts with the **syslog_free_text_parser.C** file. This file defines the different *"Dictionary" on page 245* terms and parses the syslog. The file extracts fields, which are common to all syslog messages (such as PRI, date and time), and the machine and application that generated the syslog.

The **syslog_free_text_parser.C** file uses the **allDevices.C** file (which refers to two files: **UserDefined/UserDefinedSyslogDevices.C** and **CPdefined/CPdefinedSyslogDevices.C)**.

- The first file (**UserDefined/UserDefinedSyslogDevices.C)** contains the names of the devices parsing files that the user defines.
- The second file (**CPdefined/CPdefinedSyslogDevices.C)** contains devices parsing files that Check Point defines.

The **allDevices.C** file goes over the device parsing files, and tries to match the incoming syslog with the syslog format parsed in that file.

After the parsing-file succeeds in the preliminary parsing of the syslog (that is, it matches the syslog format and is therefore the syslog origin), the remaining of the syslog is parsed in that file. If a match is not found, the file will continue to go over the Check Point device parsing files until it finds a match.

Manual Syslog Parsing

To parse a syslog file:

1. Create a new parsing file called **<device product name>.C**.
2. Put this file in the directory **$FWDIR/conf/syslog/UserDefined** on the Log Server.
3. On the Log Server, edit the file **$FWDIR/conf/syslog/UserDefined/UserDefinedSyslogDevices.C** to add a line that includes the new parsing file. For example:

```
: (
            :command (
                  :cmd_name (include)
                  :file_name ("snortPolicy.C")
            )
      )
```

4. **Optional:** If required.
   a. Create a new dictionary file called **<device product name>_dict.ini**. See *"Dictionary" on page 245*.
   b. Put it in the directory **$FWDIR/conf/syslog/UserDefined** on the Log Server.

      A dictionary translates values with the same meaning from logs from different devices into a common value. This common value is used in the Event Definitions.
   c. Edit the file **$FWDIR/conf/syslog/UserDefined/UserDefinedSyslogDictionaries.C** on the Log Server.
   d. Add a line to include the dictionary file. For example:

```
:filename ("snort_dict.ini")
```

5. To examine the parsing, send syslog samples to a Check Point Log Server.

To send syslog samples:

1. To configure the Log Server to accept syslogs, connect to the Security Management Server with SmartConsole.
2. In **Logs and Masters** > **Additional Logging Configuration**, enable the property **Accept Syslog messages**.
3. Edit the Log Server network object.

4. Run the commands `cpstop` & `cpstart`, or **fw kill fwd** & `fwd -n`.

   The **fwd** procedure on the Log Server restarts.

5. Send syslogs from the device itself, or from a syslog generator.

   For example: Kiwi Syslog Message Generator, available at `http://www.kiwisyslog.com/software_downloads.htm#sysloggen`.

Troubleshooting:

If SmartConsole does not show the logs as expected, there can be problems with the parsing files:

- If there is a syntax error in the parsing files, an error message shows. To read a specified error message, set the **TDERROR_ALL_FTPARSER** value to *5* before you run the procedure **fwd -n**.
- If the syslogs show in SmartConsole with '**Product syslog**', the log was not parsed properly, but as a general syslog.
- If the Product field contains another product (not the one you have just added) this means there is a problem with the other product parsing file. Report this to the Check Point SmartEvent team.
- If the product reports correctly in the log, look for all the fields you extracted. Some of them are in the **Information** section. Some fields can be seen only when you select **More Columns**.

The Free Text Parsing Language

The free text parsing language enables to parse an input string, extract information, and define log fields. These log fields which show as part of the Check Point log in the Log Server. They are used in the definition of events. Each parsing file contains a tree of commands. Each command examines or parses part of the input string (sometimes it adds fields to the log as a result), and decides if to continue to parse the string (according to the success/failure of its execution).

The Commands

Each command consists of these parts:

- `cmd_name` - the name of the command.
- `command arguments` - arguments that define the behavior of the command.
- `on_success` (optional) - the next command executed if the current command execution succeeds.
- `on_fail` (optional) - the next command executed if the current command execution fails.

Sample

```
:command (
   :cmd_name (try)
   :try_arguments
        .
        .
   :on_success (
       :command()
   )
   :on_fail (
       :command()
   )
)
```

Try

The `try` command matches a regular expression against the input string.

'Try' Command Parameters

Argument	Description
`parse_from`	`start_position` - run the regular expression from the start of the input string. `last_position` - run the regular expression from the last position of the previous successful command.
`regexp`	The regular expression to match.
`add_field`	One or more fields to add to the result (only if the regular expression is successful).

'Try' Command - Sample

```
:command (
     :cmd_name (try)
     :parse_from (start_position)
     :regexp ("([0-9]+\.[0-9]+\.[0-9]+\.[0-9]+)")
     :add_field (
       :type (index)
       :field_name (Src)
       :field_type (ipaddr)
       :field_index (1)
     )
)
```

In the above example, we try to match the regular expression "`([0-9]+\.[0-9]+\.[0-9]+\.[0-9]+)`" that looks at the entire log (`parse_from (start_position)`) - parse from the start of the log). If the regular expression is matched, we add a source field.

Group_try

The command `group_try` executes one or more commands in one of these modes:

- "`try_all`" tries all commands in the group, and ignores the return code of the commands.
- "`try_all_successively`" tries all the commands in the group, and ignores the return code of the commands.

  Each command tries to execute from the last position of the earlier successful command.
- "`try_until_success`" tries all the commands until one succeeds.
- "`try_until_fail`" tries all the commands until one fails.

The command "`group_try`" is commonly used when it parses a "free-text" piece of a log, which contains a number of fields we want to extract.

For example:

```
%PIX-6-605004: Login denied from 194.29.40.24/4813 to
outside:192.168.35.15/ssh for user 'root'
```

When you look at see this section of the log, you can use this structure:

'Group_try' Command - Sample 1

```
:command (
   :cmd_name (group_try)
   :mode (try_all_successively)
   :(
      # A "try" command for the source.
      :command ()
   )
   :(
      # A "try" command for the destination.
      :command ()
   )
   :(
      # A "try" command for the user.
      :command ()
   )
         .
         .
         .
)
```

In this example, the first try command in the "`group_try`" block (for the source) is executed.

If the source, destination and user are not in a specified sequence in the syslog, use the "`try_all`" mode instead of "`try_all_successively`".

'Group_try' Command - Sample 2

In this example, the regular expressions in the different commands try to match more specified logs.

At most, one command in the `group_try` block will be successful.

When it is found, it is not necessary to examine the others:

```
:command (
   :cmd_name (group_try)
   :mode (try_until_success)
   :(
      :command (
      .
      .
      .
        :regexp ("(\(|)(login|su)(\)|).* session (opened|closed) for user ([a-z,A-Z,0-9]*)")
      )
    )
   :(
      :command (
       .
       .
       .
        :regexp ("(\(|)su(\)|).* authentication failure; logname=([a-zA-Z0-9]*).* user=([a-zA-Z0-9]*)")
      )
    )
      .
      .
      .
)
```

Note - When you add a new device, the first "`try`" command in the parsing file must use the "`try_until_success`" parameter:

```
:cmd_name (group_try)
:mode (try_until_success)
: (
?
)
```

Switch

This command enables to compare the result of a specified field against a list of predefined constant values.

'Switch' Command Parameters

Parameter	Description
Parameter	Description
`field_name`	The field name whose value is checked.
`case`	One or more case attributes followed by the value with which to compare.
`default`	Execute only if no relevant case is available. The default value is optional.

'Switch' Command - Sample

```
:command (
   :cmd_name (switch)
   :field_name (msgID)
   :(
      :case (302005)
      :command ()
     )
   :(
      :case (302001)
      :case (302002)
      :command ()
     )
   :default (
      :command()
     )
)
```

Unconditional_try

This command is an "empty" command that allows you to add fields to the result without any conditions.

'Unconditional_try' Command - Sample 1

```
:command (
   :cmd_name (unconditional_try)
   :add_field (
      :type (const)
      :field_name (product)
      :field_type (string)
      :field_value ("Antivirus")
   )
)
```

A common usage of `unconditional_try` is with the **switch** command.

'Unconditional_try' Command - Sample 2

In this example, each message ID is attached with its corresponding "`message`" field which denotes its meaning.

```
:command (
   :cmd_name (switch)
   :field_name (msgID)
   (
   :case (106017)
   :command (
      :cmd_name (unconditional_try)
      :add_field (
      :type (const)
      :field_name (message)
      :field_type (string_id)
      :field_value ("LAND Attack")
      )
   )
   )
   :(
   :case (106020)
   :command (
      :cmd_name (unconditional_try)
      :add_field (
      :type (const)
      :field_name (message)
      :field_type (string_id)
      :field_value ("Teardrop Attack")
      )
   )
   )
   .
   .
   .
)
```

Include

This command enables the inclusion of a new parsing file.

`file_name`	The full path plus the file name of the file to be included.

'Include' Command - Sample

```
:command (
   :cmd_name (include)
   :file_name ("c:\freeTextParser\device\antivirusPolicy.C")
)
```

Add_field

Each "`add_field`" has some parameters:

- **Type** - The type of the "`add_field`" command. This parameter has these possible values:
  - **Index** - Part of the regular expression will be extracted as the field. The "`field_index`" value denotes which part will be extracted (see "`field_index`" bullet).
  - **Const** - Add a constant field whose value does not depend on information extracted from the regular expression. See `field_value` bullet.
- **field_name** - the name of the new field.

  There are some fields, which have corresponding columns in SmartConsole > **Logs & Monitor** > **Logs**.

  This table shows the names to give these fields to show in their **Logs & Monitor** > **Logs** column (and not in the Information field, where other added fields appear):

Field Name to be Given	Column in Logs & Monitor > Logs
`Src`	Source
`Dst`	Destination
`proto`	Protocol
`s_port`	Source Port
`product`	Product
`service`	Service (when resolved includes the port and protocol.)

Field Name to be Given	Column in Logs & Monitor > Logs
`Action`	Action
`ifname`	Interface
`User`	User

When you name the above fields accordingly, they are placed in their correct column in **Logs & Monitor** > **Logs**.

This enables them to participate in all filtering done on these columns. These fields automatically take part in existing event definitions with these field names.

- **field_type** - the type of the field in the log.

  This table shows the possible field types.

Field Type	Comment
`int`	
`uint`	
`string`	
`ipaddr`	For IP addresses used with the Src and Dst fields.
`pri`	Includes the facility and severity of a syslog.
`timestmp`	Includes the date and time of the syslog. Supports the format **'Oct 10 2019 15:05:00'**.
`time`	Supports the format **'15:05:00'**.
`string_id`	For a more efficient usage of strings. Used when there is a finite number of possible values for this field.
`action`	Supports these actions: drop, reject, accept, encrypt, decrypt, vpnroute, keyinst, authorize, deauthorize, authcrypt, and default.
`ifdir`	0 - inbound 1 - outbound
`ifname`	For an interface name (used with the "ifname" field).
`protocol`	The field name should be "proto".

Field Type	Comment
`port`	For "**service**", "**s_port**" or "**port**" fields.

The field type of the field names in this table must be as mentioned:

Field Name	Field Type
`Src`	**ipaddr**
`Dst`	**ipaddr**
`proto`	**protocol**
`s_port`	**port**
`service`	**port**
`Action`	**action**
`ifname`	**ifname**

- **field_index** or **field_value** - The parameter used depends on the value of the "`type`" field.
  - If the "`type`" field is **index**, the "`field_index`" shows.
  - If the "`type`" field is **const**, the "`field_value`" shows.

  The "`field_index`" denotes which part of the regular expression is extracted, according to the grouping of the patterns.

  To make this grouping, write a certain expression in brackets.

  In this expression, the number in the "`field_index`" denotes the bracket number whose pattern is taken into account.

'Add_field' Command - Sample 1

```
:command (
   :cmd_name (try)
   :parse_from (last_position)
   :regexp ("Failed password for ([a-zA-Z0-9]+) from ([0-9]+\.[0-9]+\.[0-9]+\.[0-9]+) port ([0-9]+)")
   :add_field (
      :type (index)
      :field_name (User)
      :field_type (string)
      :field_index (1)
     )
   :add_field (
      :type (index)
      :field_name (Src)
      :field_type (ipaddr)
      :field_index (2)
   )
   :add_field (
      :type (index)
      :field_name (port)
      :field_type (port)
      :field_index (3)
   )
)
```

The pattern for the User, "`[a-zA-Z0-9]+`", is located in the first pair of brackets. Therefore, the "`field_index`" is one.

The pattern for the Source address, "`[0-9]+\.[0-9]+\.[0-9]+\.[0-9]+`", is located in the second pair of brackets. Therefore, the index is two.

The pattern for the port is in the third pair of brackets.

In each parsed regular expression the maximum number of brackets must be up to nine.

To extract more than nine elements from the regular expression, break the expression into two pieces.

The first regular expression contains the first nine brackets.

The remaining of the regular expression is in the "`on_success`" command.

```
:command (
   :cmd_name (try)
   :parse_from (start_position)
   :regexp ("access-list (.*) (permitted|denied|est-allowed) ([a-zA-Z0-9_\([a-zA-Z0-9_\\.[0-9]+\.[0-9]+\.[0-9]+)\(([0-9]*)\)
-> "))
   :add_field (
      :type (index)
      :field_name (listID)
      :field_type (string)
      :field_index (1)
   )
   :add_field (
      :type (index)
      :field_name (action)
      :field_type (action)
      :field_index (2)
   )
   :add_field (
      :type (index)
      :field_name (proto)
      :field_type (protocol)
      :field_index (3)
   )
   :add_field (
      :type (index)
      :field_name (ifname)
      :field_type (ifname)
      :field_index (4)
   )
   :add_field (
      :type (index)
      :field_name (Src)
      :field_type (ipaddr)
      :field_index (5)
   )
   :on_success (
      :command (
         :cmd_name (try)
         :parse_from (last_position)
         :regexp ("([a-zA-Z0-9_\\.[0-9]+\.[0-9]+\.[0-9]+)\(([0-9]*)\) hit-cnt ([0-9]+) ")
         :add_field (
            :type (index)
            :field_name (destination_interface)
            :field_type (string)
            :field_index (1)
         )
      )
   )
)
```

'Add_field' Command - Sample 2

The "`field_value`" is the constant value to be added.

```
:command (
   :cmd_name (try)
   :parse_from (last_position)
   :regexp ("%PIX-([0-9])-([0-9]*)"))
   :add_field (
       :type (const)
       :field_name (product)
       :field_type (string_id)
       :field_value ("CISCO PIX")
   )
)
```

- **dict_name** is the name of the dictionary to use to convert the value. If the value is not found in the dictionary, the value is the result.

  The free text parser enables us to use dictionaries to convert values from the log. These conversions are used to translate values from logs from different devices, with the same meaning, into a common value, which is used in the event definitions.

  Each dictionary file is defined as an `.ini` file.

  In the `.ini` file the section name is the dictionary name and the values are the dictionary values (each dictionary can include one or more sections).

```
[dictionary_name]
Name1 = val1
Name2 = val2
[cisco_action]       [3com_action]
permitted = accept   Permit    = accept
denied = reject      Deny   = reject
```

'Add_field' Command - Sample 3

```
:command (
   :cmd_name (try)
   :parse_from (start_position)
   :regexp ("list (.*) (permitted|denied) (icmp) ([0-9]+\.[0-9]+\.[0-9]+\.[0-9]+) -> ([0-9]+\.[0-9]+\.[0-9]+\.[0-9]+).*
packet")
   :add_field (
         :type (index)
         :field_name (action)
         :field_type (action)
         :field_index (2)
         :dict_name (cisco_action)
    )
)
```

Dictionary

The free text parser enables us to use dictionaries to convert values from the log. These conversions are used to translate values from logs from different devices, with the same meaning, into a common value, which is used in the event definitions.

Each dictionary file is defined as an `.ini` file. In the `.ini` file the section name is the dictionary name and the values are the dictionary values (each dictionary can include one or more sections).

```
[dictionary_name]
Name1 = val1
Name2 = val2
[cisco_action]          [3com_action]
permitted = accept      Permit    = accept
denied = reject         Deny      = reject
```

Example

The reference to a dictionary in the parsing file is shown in this table:

```
:command (
      :cmd_name (try)
      :parse_from (start_position)
      :regexp ("list (.*) (permitted|denied) (icmp) ([0-9]+\.[0-
9]+\.[0-9]+\.[0-9]+) -> ([0-9]+\.[0-9]+\.[0-9]+\.[0-9]+).*
packet")
       :add_field (
                :type (index)
                :field_name (action)
                :field_type (action)
                :field_index (2)
                :dict_name (cisco_action)
       )
)
```

The Parsing Procedure

The procedure occurs on the Log Server and starts with the syslog daemon. The syslog daemon that runs on the Log Server receives the syslogs and calls for their parsing. The parsing involves many parsing files, which contain the different parsing definitions and specifications, and can be found in the **$FWDIR/conf/syslog/** directory. In these files there are the device-specific parsing files, which define the actual parsing and extraction of fields, according to each device specific syslog format.

The parsing starts with the **syslog_free_text_parser.C** file. This file defines the different *"Dictionary" on page 245* terms and parses the syslog. The file extracts fields, which are common to all syslog messages (such as PRI, date and time), and the machine and application that generated the syslog.

The **syslog_free_text_parser.C** file uses the **allDevices.C** file (which refers to two files: **UserDefined/UserDefinedSyslogDevices.C** and **CPdefined/CPdefinedSyslogDevices.C)**.

- The first file (**UserDefined/UserDefinedSyslogDevices.C)** contains the names of the devices parsing files that the user defines.
- The second file (**CPdefined/CPdefinedSyslogDevices.C)** contains devices parsing files that Check Point defines.

The **allDevices.C** file goes over the device parsing files, and tries to match the incoming syslog with the syslog format parsed in that file.

After the parsing-file succeeds in the preliminary parsing of the syslog (that is, it matches the syslog format and is therefore the syslog origin), the remaining of the syslog is parsed in that file. If a match is not found, the file will continue to go over the Check Point device parsing files until it finds a match.

Glossary

A

Anti-Bot
Check Point Software Blade on a Security Gateway that blocks botnet behavior and communication to Command and Control (C&C) centers. Acronyms: AB, ABOT.

Anti-Spam
Check Point Software Blade on a Security Gateway that provides comprehensive protection for email inspection. Synonym: Anti-Spam & Email Security. Acronyms: AS, ASPAM.

Anti-Virus
Check Point Software Blade on a Security Gateway that uses real-time virus signatures and anomaly-based protections from ThreatCloud to detect and block malware at the Security Gateway before users are affected. Acronym: AV.

Application Control
Check Point Software Blade on a Security Gateway that allows granular control over specific web-enabled applications by using deep packet inspection. Acronym: APPI.

Audit Log
Log that contains administrator actions on a Management Server (login and logout, creation or modification of an object, installation of a policy, and so on).

B

Bridge Mode
Security Gateway or Virtual System that works as a Layer 2 bridge device for easy deployment in an existing topology.

C

Cluster
Two or more Security Gateways that work together in a redundant configuration - High Availability, or Load Sharing.

Cluster Member
Security Gateway that is part of a cluster.

Compliance
Check Point Software Blade on a Management Server to view and apply the Security Best Practices to the managed Security Gateways. This Software Blade includes a library of Check Point-defined Security Best Practices to use as a baseline for good Security Gateway and Policy configuration.

Content Awareness
Check Point Software Blade on a Security Gateway that provides data visibility and enforcement. Acronym: CTNT.

Cooperative Enforcement
Integration of an on-premises Harmony Endpoint Security Server and Security Gateway.

CoreXL
Performance-enhancing technology for Security Gateways on multi-core processing platforms. Multiple Check Point Firewall instances are running in parallel on multiple CPU cores.

CoreXL Firewall Instance
On a Security Gateway with CoreXL enabled, the Firewall kernel is copied multiple times. Each replicated copy, or firewall instance, runs on one processing CPU core. These firewall instances handle traffic at the same time, and each firewall instance is a complete and independent firewall inspection kernel. Synonym: CoreXL FW Instance.

CoreXL SND
Secure Network Distributer. Part of CoreXL that is responsible for: Processing incoming traffic from the network interfaces; Securely accelerating authorized packets (if SecureXL is enabled); Distributing non-accelerated packets between Firewall kernel instances (SND maintains global dispatching table, which maps connections that were assigned to CoreXL Firewall instances). Traffic distribution between CoreXL Firewall instances is statically based on Source IP addresses, Destination IP addresses, and the IP 'Protocol' type. The CoreXL SND does not really "touch" packets. The decision to stick to a particular FWK daemon is done at the first packet of connection on a very high level, before anything else. Depending on the SecureXL settings, and in most of the cases, the SecureXL can be offloading decryption calculations. However, in some other cases, such as with Route-Based VPN, it is done by FWK daemon.

CPUSE
Check Point Upgrade Service Engine for Gaia Operating System. With CPUSE, you can automatically update Check Point products for the Gaia OS, and the Gaia OS itself.

Custom Report
User-defined report for a Check Point product, typically based on a predefined report.

D

DAIP Gateway
Dynamically Assigned IP (DAIP) Security Gateway is a Security Gateway, on which the IP address of the external interface is assigned dynamically by the ISP.

Data Loss Prevention
Check Point Software Blade on a Security Gateway that detects and prevents the unauthorized transmission of confidential information outside the organization. Acronym: DLP.

Data Type
Classification of data in a Check Point Security Policy for the Content Awareness Software Blade.

Distributed Deployment
Configuration in which the Check Point Security Gateway and the Security Management Server products are installed on different computers.

Dynamic Object
Special object type, whose IP address is not known in advance. The Security Gateway resolves the IP address of this object in real time.

E

Endpoint Policy Management
Check Point Software Blade on a Management Server to manage an on-premises Harmony Endpoint Security environment.

Event
Record of a security or network incident that is based on one or more logs, and on a customizable set of rules that are defined in the Event Policy.

Event Correlation
Procedure that extracts, aggregates, correlates, and analyzes events from the logs.

Event Policy
Set of rules that define the behavior of SmartEvent.

Expert Mode
The name of the elevated command line shell that gives full system root permissions in the Check Point Gaia operating system.

G

Gaia
Check Point security operating system that combines the strengths of both SecurePlatform and IPSO operating systems.

Gaia Clish
The name of the default command line shell in Check Point Gaia operating system. This is a restricted shell (role-based administration controls the number of commands available in the shell).

Gaia Portal
Web interface for the Check Point Gaia operating system.

H

Hotfix
Software package installed on top of the current software version to fix a wrong or undesired behavior, and to add a new behavior.

HTTPS Inspection
Feature on a Security Gateway that inspects traffic encrypted by the Secure Sockets Layer (SSL) protocol for malware or suspicious patterns. Synonym: SSL Inspection. Acronyms: HTTPSI, HTTPSi.

I

ICA
Internal Certificate Authority. A component on Check Point Management Server that issues certificates for authentication.

Identity Awareness
Check Point Software Blade on a Security Gateway that enforces network access and audits data based on network location, the identity of the user, and the identity of the computer. Acronym: IDA.

Identity Logging
Check Point Software Blade on a Management Server to view Identity Logs from the managed Security Gateways with enabled Identity Awareness Software Blade.

Internal Network
Computers and resources protected by the Firewall and accessed by authenticated users.

IPS
Check Point Software Blade on a Security Gateway that inspects and analyzes packets and data for numerous types of risks (Intrusion Prevention System).

IPsec VPN
Check Point Software Blade on a Security Gateway that provides a Site to Site VPN and Remote Access VPN access.

J

Jumbo Hotfix Accumulator
Collection of hotfixes combined into a single package. Acronyms: JHA, JHF, JHFA.

K

Kerberos
An authentication server for Microsoft Windows Active Directory Federation Services (ADFS).

L

Log Server
Dedicated Check Point server that runs Check Point software to store and process logs.

Logging & Status
Check Point Software Blade on a Management Server to view Security Logs from the managed Security Gateways.

M

Management Interface
(1) Interface on a Gaia Security Gateway or Cluster member, through which Management Server connects to the Security Gateway or Cluster member. (2) Interface on Gaia computer, through which users connect to Gaia Portal or CLI.

Management Server
Check Point Single-Domain Security Management Server or a Multi-Domain Security Management Server.

Manual NAT Rules
Manual configuration of NAT rules by the administrator of the Check Point Management Server.

Mobile Access
Check Point Software Blade on a Security Gateway that provides a Remote Access VPN access for managed and unmanaged clients. Acronym: MAB.

Multi-Domain Log Server
Dedicated Check Point server that runs Check Point software to store and process logs in a Multi-Domain Security Management environment. The Multi-Domain Log Server consists of Domain Log Servers that store and process logs from Security Gateways that are managed by the corresponding Domain Management Servers. Acronym: MDLS.

Multi-Domain Server
Dedicated Check Point server that runs Check Point software to host virtual Security Management Servers called Domain Management Servers. Synonym: Multi-Domain Security Management Server. Acronym: MDS.

N

Network Object
Logical object that represents different parts of corporate topology - computers, IP addresses, traffic protocols, and so on. Administrators use these objects in Security Policies.

Network Policy Management
Check Point Software Blade on a Management Server to manage an on-premises environment with an Access Control and Threat Prevention policies.

O

Open Server
Physical computer manufactured and distributed by a company, other than Check Point.

P

Predefined Report
Default report included in a Check Point product that you can run right out of the box.

Provisioning
Check Point Software Blade on a Management Server that manages large-scale deployments of Check Point Security Gateways using configuration profiles. Synonyms: SmartProvisioning, SmartLSM, Large-Scale Management, LSM.

Q

QoS
Check Point Software Blade on a Security Gateway that provides policy-based traffic bandwidth management to prioritize business-critical traffic and guarantee bandwidth and control latency.

R

Report
Summary of network activity and Security Policy enforcement that is generated by Check Point products, such as SmartEvent.

Rule
Set of traffic parameters and other conditions in a Rule Base (Security Policy) that cause specified actions to be taken for a communication session.

Rule Base
All rules configured in a given Security Policy. Synonym: Rulebase.

S

SecureXL
Check Point product on a Security Gateway that accelerates IPv4 and IPv6 traffic that passes through a Security Gateway.

Security Gateway
Dedicated Check Point server that runs Check Point software to inspect traffic and enforce Security Policies for connected network resources.

Security Management Server
Dedicated Check Point server that runs Check Point software to manage the objects and policies in a Check Point environment within a single management Domain. Synonym: Single-Domain Security Management Server.

Security Policy
Collection of rules that control network traffic and enforce organization guidelines for data protection and access to resources with packet inspection.

SIC
Secure Internal Communication. The Check Point proprietary mechanism with which Check Point computers that run Check Point software authenticate each other over SSL, for secure communication. This authentication is based on the certificates issued by the ICA on a Check Point Management Server.

SmartConsole
Check Point GUI application used to manage a Check Point environment - configure Security Policies, configure devices, monitor products and events, install updates, and so on.

SmartDashboard
Legacy Check Point GUI client used to create and manage the security settings in versions R77.30 and lower. In versions R80.X and higher is still used to configure specific legacy settings.

SmartEvent Correlation Unit
SmartEvent software component on a SmartEvent Server that analyzes logs and detects events.

SmartEvent Server
Dedicated Check Point server with the enabled SmartEvent Software Blade that hosts the events database.

SmartProvisioning
Check Point Software Blade on a Management Server (the actual name is "Provisioning") that manages large-scale deployments of Check Point Security Gateways using configuration profiles. Synonyms: Large-Scale Management, SmartLSM, LSM.

SmartUpdate
Legacy Check Point GUI client used to manage licenses and contracts in a Check Point environment.

Software Blade
Specific security solution (module): (1) On a Security Gateway, each Software Blade inspects specific characteristics of the traffic (2) On a Management Server, each Software Blade enables different management capabilities.

Standalone
Configuration in which the Security Gateway and the Security Management Server products are installed and configured on the same server.

System Counter
SmartView Monitor data or report on status, activity, and resource usage of Check Point products.

T

Threat Emulation
Check Point Software Blade on a Security Gateway that monitors the behavior of files in a sandbox to determine whether or not they are malicious. Acronym: TE.

Threat Extraction
Check Point Software Blade on a Security Gateway that removes malicious content from files. Acronym: TEX.

U

Updatable Object
Network object that represents an external service, such as Microsoft 365, AWS, Geo locations, and more.

URL Filtering
Check Point Software Blade on a Security Gateway that allows granular control over which web sites can be accessed by a given group of users, computers or networks. Acronym: URLF.

User Directory
Check Point Software Blade on a Management Server that integrates LDAP and other external user management servers with Check Point products and security solutions.

V

VSX
Virtual System Extension. Check Point virtual networking solution, hosted on a computer or cluster with virtual abstractions of Check Point Security Gateways and other network devices. These Virtual Devices provide the same functionality as their physical counterparts.

VSX Gateway
Physical server that hosts VSX virtual networks, including all Virtual Devices that provide the functionality of physical network devices. It holds at least one Virtual System, which is called VS0.

Z

Zero Phishing
Check Point Software Blade on a Security Gateway (R81.20 and higher) that provides real-time phishing prevention based on URLs. Acronym: ZPH.