13 March 2017

Logging and Monitoring

R80.10

Administration Guide

Early Availability

Classification: [Restricted]

Check Point
SOFTWARE TECHNOLOGIES LTD.

Important Information

Latest Software

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

Check Point R80.10

For more about this release, see the R80.10 home page http://supportcontent.checkpoint.com/solutions?id=sk111841.

More Information

Visit the Check Point Support Center http://supportcenter.checkpoint.com.

Latest Version of this Document

Download the latest version of this document http://supportcontent.checkpoint.com/documentation_download?ID=46535.

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

Feedback

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

Please help us by sending your comments mailto:cp_techpub_feedback@checkpoint.com?subject=Feedback on Logging and Monitoring R80.10 Administration Guide.

Searching in Multiple PDFs

To search for text in all the R80.10 PDF documents, download and extract the complete R80.10 documentation package http://supportcontent.checkpoint.com/documentation_download?ID=TBD.
Use **Shift-Control-F** in Adobe Reader or Foxit reader.

Revision History

Date	Description
13 March 2017	First release of this document

Contents

Terms

Administrator

A SmartConsole user with permissions to manage Check Point security products and the network environment.

Audit Log

A record of an action that is done by an Administrator. See also *Log* (on page 7).

Cluster

1. Two or more Security Gateways or servers synchronized for High Availability or Load Sharing.

2. In a virtualized environment - a set of ESX/i hosts used for High Availability or Load Sharing.

Cluster Member

A Security Gateway that is part of a cluster.

Configure

To select or to enter values that change how a product works.

Cooperative Enforcement

Integration of Endpoint Security server compliance to verify internal network connections.

Correlation Unit

A SmartEvent software component that analyzes logs and detects events.

Custom Report

A user defined report for a Check Point product, typically based on a predefined report.

Database

The Check Point database includes all objects, including network objects, users, services, servers, and protection profiles.

DLP

Data Loss Prevention. Detects and prevents the unauthorized transmission of confidential information.

Event

A 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

A procedure that extracts, aggregates, correlates and analyses events from the logs.

Event Policy

A set of rules that define the behavior of SmartEvent.

External Network

Computers and networks that are outside of the protected network.

Internal Network

Computers and resources protected by the Firewall and accessed by authenticated users.

IPS

Intrusion Prevention System. Check Point Software Blade that inspects and analyzes packets and data for numerous types of risks.

Log

A record of an action that is done by a Software Blade.

Log Server

Physical server that hosts Check Point product log files.

Management Server

A Security Management Server or Multi-Domain Server that manages one or more Security Gateways and security policies.

Network

1. A configuration of nodes and connecting branches. 2. A site of machines, services, and the links (physical, virtual, wireless, encrypted) that connect them.

Policy

A collection of rules that control network traffic and enforce organization guidelines for data protection and access to resources with packet inspection.

Predefined Report

A default report included in a Check Point product that you can run right out of the box.

Remote Access VPN

An encryption tunnel between a Security Gateway and remote access clients, such as Endpoint Security VPN, and communities.

Report

A summary of network activity and Security Policy enforcement that is generated by Check Point products such as SmartEvent.

Security Cluster

A cluster that has identical Check Point Security Gateway members for High Availability and Load Sharing.

Security Gateway

A computer or an appliance that inspects traffic and enforces Security Policies for connected network resources.

Security Management Server

The server that manages, creates, stores, and distributes the security policy to Security Gateways.

Security Policy

A collection of rules that control network traffic and enforce organization guidelines for data protection and access to resources with packet inspection.

SmartConsole

A Check Point GUI application used to manage security policies, monitor products and events, install updates, provision new devices and appliances, and manage a multi-domain environment.

SmartEvent Server

Physical server that hosts the events database.

Software Blade

A software blade is a security solution based on specific business needs.

Each blade is independent, modular and centrally managed. To extend security, additional blades can be quickly added.

System Counter

SmartView Monitor data or report on status, activity, and resource usage of Check Point products.

Traffic

The flow of data between network resources.

VPN

Virtual Private Network. A secure, encrypted connection between networks and remote clients on a public infrastructure, to give authenticated remote users and sites secured access to an organization's network and resources.

VPN Tunnel

An encrypted connection between two hosts using standard protocols (such as L2TP) to encrypt traffic going in and decrypt it coming out, creating an encapsulated network through which data can be safely shared as though on a physical private line.

Welcome

With 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 R80.10, SmartReporter and SmartEvent functionality is integrated into SmartConsole.

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

The new views are available from two locations:

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

Getting Started

In This Section:

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:

SmartConsole > Logs & Monitor	Analyze events that occur in your environment with customizable views and reports. The **Logs** view replaces the SmartView Tracker and SmartLog SmartConsole GUI clients.
SmartView Web Application	A SmartEvent 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:

SmartEvent	• For initial settings - configure the Correlation Unit, Log Servers, Domains and Internal Network. • To schedule Reports • To configure the SmartEvent Correlation Unit • 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 80).

To open the SmartEvent GUI client:

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

To open the SmartView Monitor GUI client:

1. Open SmartConsole > Logs & Monitor.
2. Click (+) for a Catalog (new tab).
3. Click **Tunnel & User Monitoring**.

Understanding Logging

Security Gateways generate logs, and the Security Management Server generates audit logs. The Security Policy that is installed on each Security Gateway determines which rules generate logs. Logs can be stored on a:

- Security Management Server that collects logs from the Security Gateways. This is the default.
- Log Server on a dedicated machine. This is recommended for organizations that generate a lot of logs.
- Security Gateway. This is called local logging.

To find out how much storage is necessary for logging, see sk87263 http://supportcontent.checkpoint.com/solutions?id=sk87263.

In a Multi-Domain Security Management environment, the Security Gateways send logs to the Domain Server or to dedicated Domain Log Servers. The Multi-Domain Server generates logs, and they can be stored on the Multi-Domain Server or on a dedicated Multi-Domain Log Server. To learn how to deploy logging in a Multi-Domain Security Management environment, see the *R80.10 Multi-Domain Security Management Administration Guide* http://supportcontent.checkpoint.com/documentation_download?ID=46532.

To decrease the load on the Security Management Server, you can install a dedicated Log Server and configure the gateways to send their logs to this Log Server. To see the logs from all the Log Servers, connect to the Security Management Server with SmartConsole, and go to the **Logs & Monitor** view **Logs** tab.

A Log Server handles log management activities:

- Automatically starts a new log file when the existing log file gets to the defined maximum size.
- Handles backup and restore for log files.
- Stores log files for export and import.
- Makes an index of the logs. Therefore, log queries work quickly.

Deploying Logging

You can enable logging on the Security Management Server, or deploy a dedicated Log Server. After you deploy the Log Server, you must configure the Security Gateways for logging

In This Section

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, enable **Logging & Status**.
4. In the SmartConsole main toolbar, click **Publish**.

Deploying a Dedicated Log Server

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

Installing a Dedicated Log Server

1. Download the R80.10 installation ISO file.
2. Install the ISO on the appliance or open server.
3. Reboot when prompted.
4. Connect to the WebUI of the Log Server:
   `https://<ServerIP>`
5. Run the **First Time Configuration Wizard**.
6. On the **Installation Type** page, select **Security Management**.
7. On the **Products** page:
   - On a Smart-1 appliance, select **Dedicated Server** and **SmartEvent**.
   - On an open server, select **Log Server/SmartEvent only**.

Connecting the Dedicated Log Server to the Security Management Server

You can connect the R80.10 Log Server to an R80.10 Security Management Server.

To connect the R80.10 Log Server to an R80.10 Security Management Server:

1. In SmartConsole, create a new Check Point host object for the Log Server.
2. Create an SIC trust with the Log Server.
3. Select **Version** R80.10.
4. In the **General Properties** page **Management** tab, enable **Logging & Status**.
5. Click **Publish**.
6. In the Menu, click **Install Database**.

Configuring the Security Gateways for Logging

Security Gateways can store their logs on:

- A Security Management Server that collects logs from the Security Gateways. This is the default.
- A Log Server on a dedicated machine. This is recommended for organizations that generate a lot of logs.
- The Security Gateway. This is called local logging. These files 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.

To configure a Security Gateway for logging:

1. Open SmartConsole.
2. In the **Gateways & Servers** view, double-click the gateway object.
   The **Check Point Gateway** window opens.
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 machine**.
5. Click **OK**.
6. Click **Publish**.
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 computer 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 Domain 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. Click **Publish**.
8. From **Menu**, select **Install Database**.

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. You must disable it on *all* management and Log Server objects in the environment. You are not allowed to have some Log Servers in index mode and other Log Servers in non-index mode.

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 in one log file at a time.

Note - You cannot enable SmartEvent or a SmartEvent Correlation Unit on a Log Server on which indexing is disabled, or on other server in the environment. SmartEvent and Correlation Units require indexing.

To disable Log Indexing:

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

   The **General Properties** window opens.
3. From the navigation tree, click **Logs**.
4. Clear the **Enable Log Indexing** option.
5. Click **OK**.
6. Click **Publish**.
7. From **Menu**, select **Install Database**.

To select a log file to search:

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

Deploying SmartEvent

SmartEvent Server is integrated with the Security Management Server architecture. It communicates with Security Management 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 R80.10 SmartEvent on a dedicated server and connect it to Security Management Servers or Multi Domain servers of version R77.xx (or earlier). This lets you extend an R77.xx environment with the new capabilities of R80.10 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.

Note - For R80.10, SmartReporter functionality (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, see Connecting SmartEvent Server to a Security Management Server ("Connecting the SmartEvent Components to a Security Management Server" on page 16).

in This Section:

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.

System Requirements

To use SmartEvent, see the requirements in the *R80.10 Release Notes* http://supportcontent.checkpoint.com/documentation_download?ID=TBD.

Enabling SmartEvent on the Security Management Server

1. Open SmartConsole
2. Open the Security Management Server network object.
3. On the **Management** tab, enable these Software Blades:
   - **Logging & Status**
   - **SmartEvent Server**
   - **SmartEvent Correlation Unit**
4. In the SmartConsole main toolbar, click **Publish**.
5. **Optional**: activate the firewall session for the network activity report ("Generating a Network Activity Report" on page 37).

   The **Network Activity** report gives information about Firewall connections. For example, top sources, destinations, and services. To create this report, the SmartEvent must make an index of the Firewall logs.

   To enable this report, on the SmartEvent GUI **Policy** tab, select and enable **Consolidated Sessions > Firewall Session**.

   Note: This configuration increases the number of events a day by five. This can have a performance effect.

Deploying a Dedicated SmartEvent Server

Installing a Dedicated SmartEvent Server

1. Download the installation ISO file.
2. Install the ISO on the open server or appliance.

   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.

Configuring the SmartEvent components in the First Time Configuration Wizard

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

To configure the SmartEvent components:

1. Connect to the SmartEvent Server WebUI:
   `https://`*<ServerIP>*
2. Run the **First Time Configuration Wizard**.

   To learn how to run the First Time Configuration Wizard, see the *R80.10 Installation and Upgrade Guide* http://downloads.checkpoint.com/dc/download.htm?ID=TBD.
3. On the **Installation Type** page, select **Security Management**.
4. On the **Products** page:
   - On a Smart-1 , select **Dedicated Server** and **SmartEvent**.
   - On an open server select **Log Server / SmartEvent only**
5. Install the R80.10 SmartConsole GUI client.

   R80.10 SmartConsole has the Logs & Monitor catalog of views, which includes the views in the SmartEvent GUI.

Connecting the SmartEvent Components to a Security Management Server

Connect the R80.10 SmartEvent components to a R80.10 Security Management Server or to a R77.xx Security Management Server.

To connect the R80.10 SmartEvent components to an R80.10 Security Management Server:

1. In SmartConsole, create a new Check Point host object for the SmartEvent Server.
2. Create an SIC trust with the SmartEvent Server.
3. Select **Version** R80.10.
4. On the **Management** tab, enable these Software Blades:
   - **Logging & Status**
   - **SmartEvent Server**
   - **SmartEvent Correlation Unit**

Note - A Correlation Unit can also be installed on a dedicated server ("Configuring Dedicated Correlation Units" on page 20).

5. In the Logs pane, make sure the **Enable Log Indexing** option is selected.
6. Click **OK**.
7. Click **Publish**.
8. Click **Install Database**.
9. **Advanced Configuration**:
   a) Open the SmartEvent GUI:
      (i) In **SmartConsole** > **Logs & Monitor**, click **+** to open a catalog (new tab).
      (ii) Click **SmartEvent Settings & Policy**.
   b) In **Policy tab** > **Correlation Units**, define a Correlation Unit object.
   c) Select the production Log Servers and local log server on the SmartEvent Server to read logs from.
   d) In **Policy tab** > **Internal Network**, define the internal Network.
   e) **Optional**: Enable the **Network Activity** report.
      The **Network Activity** report gives information about Firewall connections. For example, top sources, destinations, and services. To create this report, SmartEvent must make an index of the Firewall logs.
      To enable this report, on the SmartEvent GUI **Policy** tab, select and enable **Consolidated Sessions > Firewall Session**.
   f) Click **Save**.
   g) Install the Event Policy on the Correlation Unit: **SmartEvent** menu > **Actions** > **Install Event Policy**.

To connect the R80.10 SmartEvent components to an R77.xx Security Management Server:

1. Open an SSH connection to the SmartEvent Server.
2. Run this script:
   `$RTDIR/scripts/SmartEvent_R80_change_dbysync_mode.sh`
3. Run: `cpconfig`
4. Select `(2) Administrator` to configure the SmartEvent Server administrators.
   Note – Administrators that are configured in R77.xx SmartDashboard cannot manage the R80.10 SmartEvent Server.
5. In SmartConsole, create a new Check Point host object for the SmartEvent Server.
6. Open the R77.xx SmartDashboard.
7. Create an SIC trust with the SmartEvent Server.
8. Select the highest version available and ignore the **Warning** message.
9. On the **Management** tab, enable these Software Blades:
   - **Logging & Status**
   - **SmartEvent Server**
   - **SmartEvent Correlation Unit**

Note - A SmartEvent Correlation Unit can also be installed on a dedicated server ("Configuring Dedicated Correlation Units" on page 20).

10. In the **Logs** page, make sure **Enable SmartLog** is selected.
11. Click **OK**.
12. Click **File** > **Policies** > **Install Database**.
13. **Advanced Configuration**:
    a) Open the R80.10 SmartConsole to the IP address of the SmartEvent Server:
       (i) In **SmartConsole** > **Logs & Monitor**, click **+** to open a catalog (new tab).
       (ii) Click **SmartEvent Settings & Policy**.
    b) In **Policy tab** > **Correlation Units**, define a SmartEvent Correlation Unit object.
    c) Select the production Log Servers and local Log Server on the SmartEvent Server that will send logs to the SmartEvent Correlation Unit.
    d) In **Policy tab** > **Internal Network**, define the internal Network.
    e) **Optional**: Enable the **Network Activity** report.

       The **Network Activity** report gives information about Firewall connections. For example, top sources, destinations, and services. To create this report, SmartEvent must make an index of the Firewall logs.

       To enable this report, on the SmartEvent GUI **Policy** tab, select and enable **Consolidated Sessions > Firewall Session**.

       Note: This configuration increases the number of events a day by five. This can have a performance effect.
    f) Click **Save**.
    g) Install the Event Policy on the SmartEvent Correlation Unit: **SmartEvent** menu > **Actions** > **Install Event Policy**.

Connecting SmartEvent Components to a Multi-Domain Server

You can connect R80.10 SmartEvent Server to one or more Domains in an R80.10 Multi-Domain Security Management environment. Or, you can connect to an R77.xx Multi-Domain Security Management.

Notes:

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

To connect R80.10 SmartEvent to an R80.10 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 R80**.

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 R80.10 Server.
6. Click **OK**.
7. Click **Publish**.
8. Reassign the global Policy for the Domains that use SmartEvent. For new Domains, create a new global assignment.
9. In each Domain Server, open SmartConsole.
10. Click **Menu** > **Install Database** , on each Domain Server and Domain Log Servers.
11. Wait until the server synchronizes and loads SmartEvent process.
12. **Advanced Configuration**:
    a) Open SmartConsole and connect to the SmartEvent Server.
    b) Launch the SmartEvent GUI client:
       (i) In the **Logs & Monitor** view, click on **+** to open a catalog (new tab).
       (ii) Click the **SmartEvent Settings & Policy** link.

       Note - The primary GUI application is the R80.10 SmartConsole. With R80.10, some configurations can be done only in the SmartEvent GUI client.
    c) If SmartEvent is connected to a Multi-Domain Server, in **Policy** tab > **Domains**, define the required domains to connect to.
    d) In **Policy tab** > **Correlation Units**, define a SmartEvent Correlation Unit object.
    e) Select the production Log Servers and local Log Server on the SmartEvent Server to read logs from.
    f) In **Policy tab** > **Internal Network**, define the internal Network.
    g) **Optional**: Enable the **Network Activity** report.

       The **Network Activity** report gives information about Firewall connections. For example, top sources, destinations, and services. To create this report, SmartEvent must make an index of the Firewall logs.

       To enable this report, on the SmartEvent GUI **Policy** tab, select and enable **Consolidated Sessions > Firewall Session**.

       Note: This configuration increases the number of events a day by five. This can have a performance effect.
    h) Click **Save**.
    i) Install the Event Policy on the Correlation Unit: **SmartEvent** menu > **Actions** > **Install Event Policy**.

To connect R80.10 SmartEvent to an R77.xx Multi-Domain Server:

1. Open an SSM connection to the SmartEvent server.
2. Run this script: `$RTDIR/scripts/SmartEvent_R80_change_dbsync_mode.sh`
3. Open R77.xx SmartDashboard.

4. Log in to the global Domain:
5. Create a Check Point Host object for **SmartEvent R80**. define it with the highest version possible, and ignore the **Warning** message.
6. In the **Check Point Host** > **Management**, select these Management Blades:
   - **Logging & Status**
   - **SmartEvent Server**
   - **SmartEvent Correlation Unit**
7. Initialize SIC with the new R80.10 SmartEvent Server.
8. In the **Logs** page, click **Enable SmartLog**.
9. Click **OK**.
10. Click **Save**.
11. Reassign the global Policy for the Domains that use SmartEvent. For new Domains, create a new global assignment.
12. **Advanced Configuration**:
    a) Open R80.10 SmartConsole
    b) Launch the SmartEvent GUI client.
       (i) In the **Logs & Monitor** view, click on **+** to open a catalog (new tab).
       (ii) Click the **SmartEvent Settings & Policy** link.
       Note - The primary GUI application is the R80.10 SmartConsole. With R80.10, some configurations can be done only in the SmartEvent GUI client.
    c) If SmartEvent is connected to a Multi-Domain Server, in **Policy** tab > **Domains**, define the required domains to connect to.
    d) In **Policy tab** > **Correlation Units**, define a Correlation Unit object.
    e) Select the production Log Servers and local log server on the SmartEvent Server to read logs from.
    f) In **Policy tab** > **Internal Network**, define the internal Network.
    g) **Optional**: Enable the **Network Activity** report.
       The **Network Activity** report gives information about Firewall connections. For example, top sources, destinations, and services. To create this report, SmartEvent must make an index of the Firewall logs.
       To enable this report, on the SmartEvent GUI **Policy** tab, select and enable **Consolidated Sessions > Firewall Session**.
       Note: This configuration increases the number of events a day by five. This can have a performance effect.
    h) Click **Save**.
    i) Install the Event Policy on the Correlation Unit: **SmartEvent** menu > **Actions** > **Install Event Policy**.

Configuring Dedicated Correlation Units

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

Note: Configuration of dedicated Correlation Units are only supported for management versions R77 and higher.

To configure a dedicated Correlation Unit:

1. In SmartConsole (or in the Global SmartConsole for Multi-Domain Security Management), create a new Correlation Unit network object.
2. Create an SIC trust with the dedicated Correlation Unit.
3. On the **Management** tab, enable these Software Blades:
   - Logging & Status
   - SmartEvent Correlation Unit
4. If you use a Multi-Domain Security Management deployment, assign the Global Policy to all Domains that use SmartEvent.
5. Open the SmartConsole of each domain.
6. Install Database on the Log Servers and on the R80.10 Correlation Unit.

   If installation fails on the Correlation Unit, ignore the message and continue with these steps:
7. Open the SmartEvent GUI.

   a) In **SmartConsole** > **Logs & Monitor**, click **+** to open a catalog (new tab).

   b) Click **SmartEvent Settings & Policy**.
8. In the **SmartEvent Policy tab** > **Correlation Units**, double-click the new Correlation Unit object.

   The window shows a list of all objects defined as Correlation units.
9. Select which Correlation Unit to enable and which Log Servers they read logs from.
10. Select:
    - All Log Servers to read logs from
    - The Log Server with the dedicated Correlation Unit
    - The Log Server on SmartEvent R80.10
11. Click **Save**.
12. Install the Event Policy on the Correlation Unit: **SmartEvent menu** > **Actions** > **Install Event Policy**

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.

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. In the SmartEvent client, configure the new port on the Correlation Unit.
4. In **Policy tab** > **Correlation Units**, configure the Correlation Unit to read logs from the local Log Server (on the SmartEvent Server).

5. 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*>.
6. Install the Event Policy on the Correlation Unit: **Actions** > **Install Event Policy**
7. 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) 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 http://supportcontent.checkpoint.com/solutions?id=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.

Creating an Administrator

To Create an Administrator

1. In SmartConsole, open **Manage & Settings**.
2. Click **Administrators.**
3. Click **New Administrator**.
   The **New Administrator** window opens.
4. Enter a name for the administrator.
5. Select an **Authentication** method.

6. In the **Permission Profiles** area, select a permission profile, or click **New** and create a permission profile.
7. In a new profile, in the **Overview** tab, configure **Permissions**. If you select **Customized**, you can select these options for the features:
   - **Not selected** - The administrator cannot see the feature.

     Note - If you cannot clear a resource selection, the administrator access to it is mandatory, and you cannot make it invisible
   - **Selected** - The administrator can see the feature.
   - **Read** - The administrator can see the feature but cannot change it.
   - **Write** - The administrator can see and change the feature.

   Some resources do not have the **Read** or **Write** option. You can only select (for full permissions) or clear (for no permissions) these resources.
8. Optional: In the **Expiration** area, define an expiration date for the administrator account.
9. Optional: In the left of the window:
   a) Click **Additional**.
   b) Enter the personal information (email, phone number) for the administrator.
10. Click **OK**.

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 the SmartEvent GUI:

- **SmartEvent**
  - **Events** - The **Events** tab
  - **Policy** - Events correlation on the **Policy** tab
  - **Reports** - **Reports** tab
- **SmartEvent Application & URL Filtering reports only**

Multi-Domain Security Management

In 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.

Locally Managing the Administrator

If you do not want to centrally manage administrators, and you use the local administrator defined for the SmartEvent Server, run this CLI command on the SmartEvent Server:

```
cpprod_util CPPROD_SetValue FW1 REMOTE_LOGIN 4 1 1
```

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 the SmartEvent client, but only see the **Reports** tab. 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. For **SmartEvent Reports** option, select **All Blades**.
7. On the **Access Control**, **Threat Prevention**, and **Others** pages, clear all options.
8. On the **Monitoring and Logging** page, select all features, with **Write** permissions.
9. Click **OK**.

   The profile shows in the **Permission Profiles** page.
10. Assign the SmartEvent Reports Only permissions profile to administrators ("Creating an Administrator" on page 22).
11. Publish the changes.
12. 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 time period in the past and focus on deploying resources on threats that have been active for a period of time but may have been missed (for

example, new events which may have been dynamically updated can now be processed over the previous period).

Offline Work For Correlated Events

To detect suspicious logging activity (that is, 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 Server or Multi-Domain Server.

The settings are:

- **Add** - Configure an Offline Log File procedure.
  - **Name** acts as a label that enables you to recognize the specified Offline Line log file for future processing. For example, you can create a query according to the Offline Job name. This name is used in Event tab queries to search events that were generated by this job.
  - **Comment** contains a description of the Offline Job for edification.
  - **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 contains a list of available log files found on the selected Log Server. These log files will be 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. The results of this procedure show in the **Events** tab. These results are accessible by the **By Job Name** query or filter.
- **Stop** - Stop the Offline Log Files procedure. It does not delete the full procedure, but stops the procedure at the specified selected point. The information collected up until the procedure steps shows in the **Events** tab.

Importing Log Files from SmartEvent Servers

To import offline log files, add events to the SmartEvent Server. By default, you can import the 14 most recent days of offline logs. 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 the last 14 days before the SmartEvent Server was installed.

1. Run: `# evstop`
2. Edit the log settings file `log_indexer_custom_settings.conf`

   a) Make a backup. Run this command:

   ```
   cp $INDEXERDIR/log_indexer_custom_settings.conf
   $INDEXERDIR/log_indexer_custom_settings.conf_orig
   ```

b) Edit `$INDEXERDIR/log_indexer_custom_settings.conf` in a text editor.

c) Delete these lines:

```
:time_restriction_for_fetch_all (<existing_data>)
:time_restriction_for_fetch_all_disp (<existing_data>)
```

d) Add this line:

```
:num_days_restriction_for_fetch_all_integrated (<days>)
```

<days> is the last number of days of logs to be indexed by the SmartEvent Server. For example, to import and index logs from the last 30 days of logs, give a value of 30.

Note - To decrease the performance effect while you index the offline logs, import only the necessary number of days of logs.

3. Run: `# evstart`
4. In the SmartEvent Server object properties, in the **Logs** > **Storage** page, configure **Disk Space Management**.

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 (on page 25) 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 http://supportcontent.checkpoint.com/solutions?id=sk98894.

Views and Reports

In This Section:

You can create rich and customizable views and reports for log and event monitoring, that inform key stakeholders about security activities.

The views are available from two locations:

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

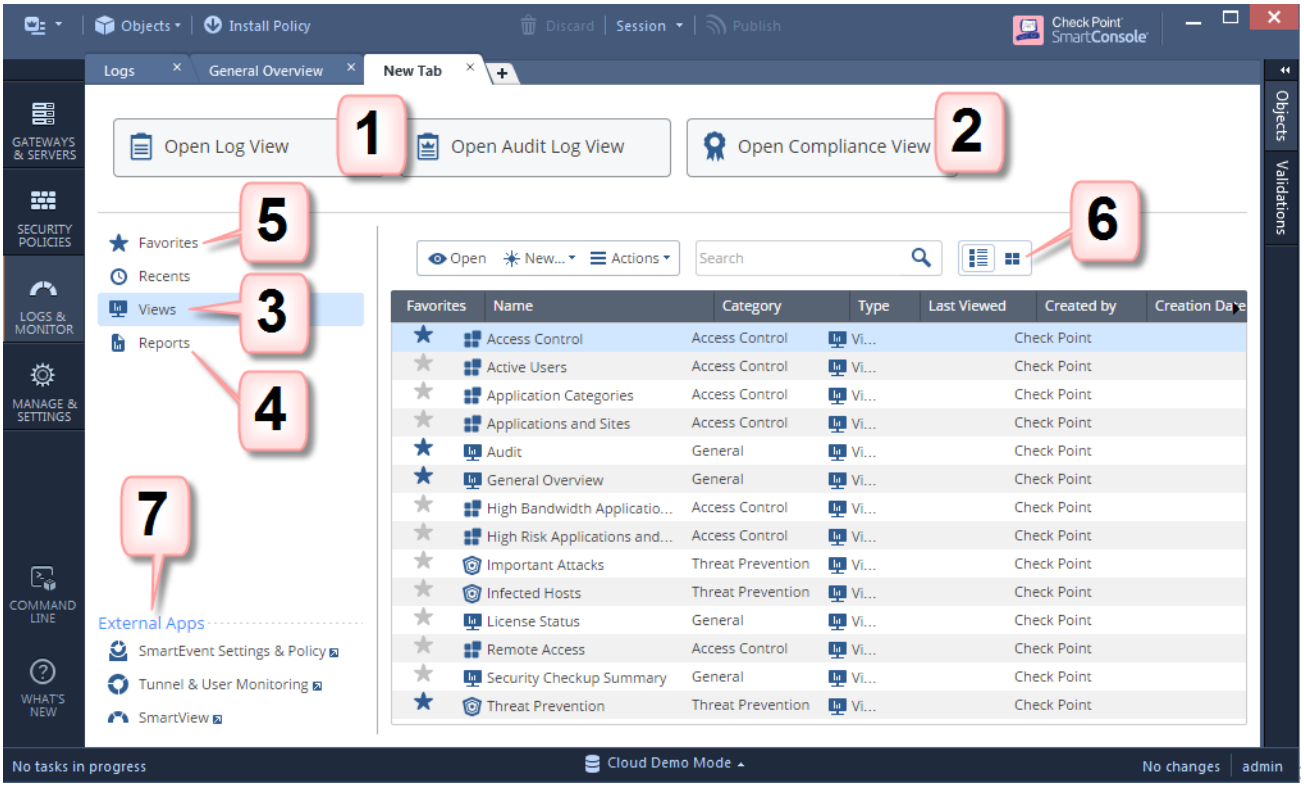
For a quick overview of Views and Reports in R80.10, see the online tutorial https://sc1.checkpoint.com/documents/R80/CP_SmartEvent_R80_Views_and_Reports_Tutorial_web/EN/html_frameset.htm.

Deploying Views and Reports

To allow SmartEvent views and reports, you must install and configure a SmartEvent Server. For the details, see Deploying SmartEvent (on page 14).

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.



Item	Description
1	**Open Log View** - See and search through the logs from all Log Servers. You can also search the logs from a Log Server that you choose. **Open Audit Logs View** - See and search records of actions done by SmartConsole administrators. These views come from the Log Servers. Other views come from the SmartEvent Server.
2	**Compliance View -** Optimize your security settings and ensure compliance with regulatory requirements.
3	**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 graph, 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.
4	**Reports -** The list of predefined and customized reports. A report has multiple views, and applies to the time that the report is generated. It gives more details than a view. There are several predefined reports, and you can create new reports. Reports can be customized, filtered, generated and scheduled. You cannot drill down into a report. A report is divided onto pages.
5	**Favorites** - Use this view to collect the views and reports you use the most.

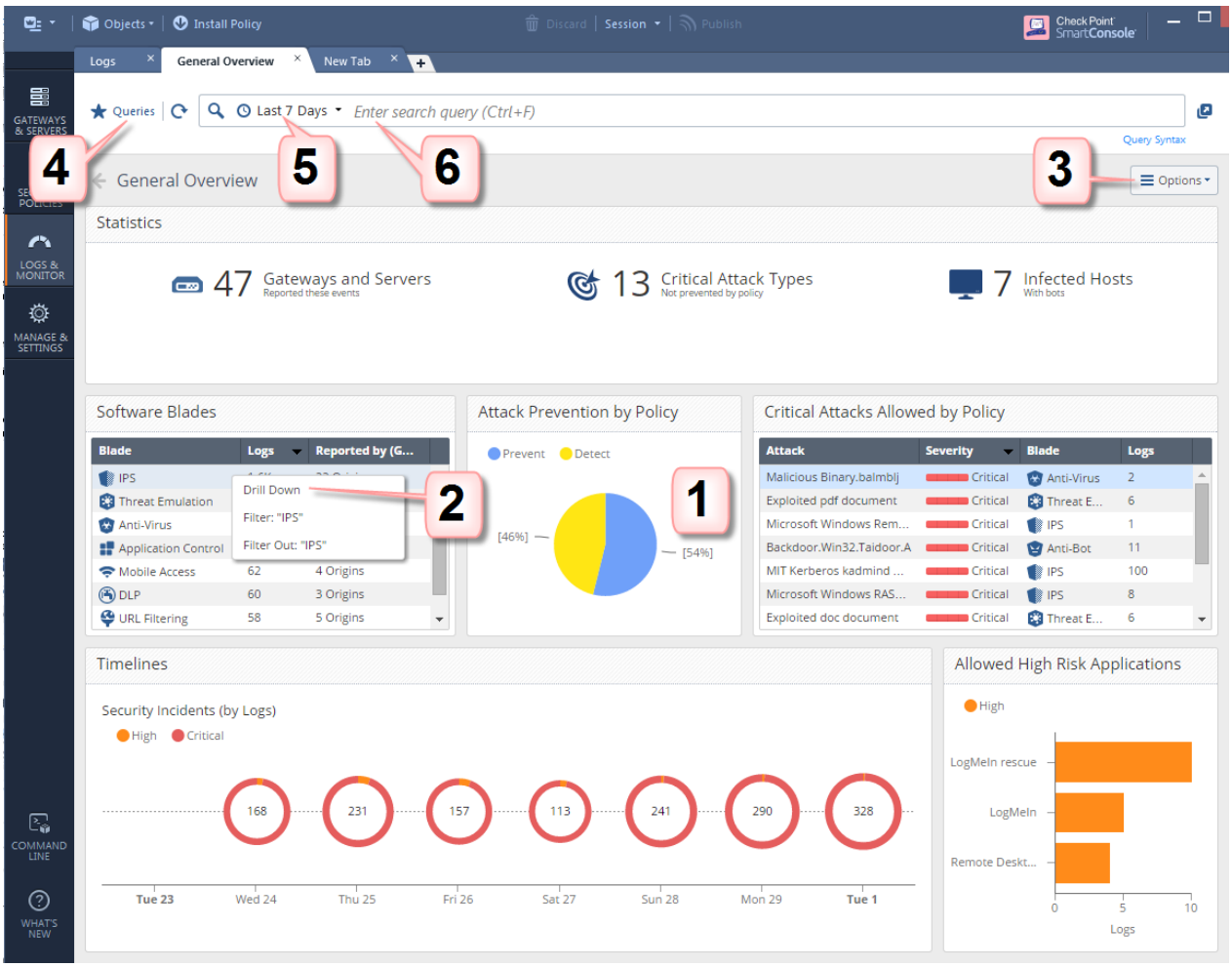
Item	Description
6	**Switch to Table View** or **Thumbnails View -** The Table view is the default for views and reports. The Thumbnails view is the default for the Favorites and Recents.
7	**External Apps** • **SmartEvent Settings & Policy** - The SmartEvent GUI client. Use it for initial setup and to define the SmartEvent Correlation Unit policy. The views in SmartConsole are a replacement for those in the SmartEvent GUI client. • **Open Tunnel and User Monitoring** - The SmartView Monitor GUI Client. The monitoring views in SmartConsole are a replacement for those in the SmartView Monitor GUI client, except for Tunnel and User Monitoring. • **SmartView Web Application** - A SmartEvent Web application that you can use to analyze events that occur in your environment. Use it to see an overview of the security information for your environment. It has the same real-time event monitoring and analysis views as SmartConsole, with the convenience of not having to install a client.

Views

Views tells administrators and other stakeholders about security and network events. A view is an interactive dashboard made up of widgets. Each widget is the output of a query. A Widget can show information in different formats, for example, a graph or a table.

SmartConsole comes with several predefined views. You can create new views that match your needs, or you can customize an existing view.

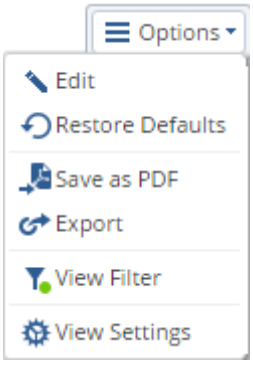
In the Logs & Monitor view, clicking the (+) tab opens a catalog of all views and reports, predefined and customized. Click a view to open it.



Item	Description
1	**Widget**- The output of a query. A Widget can show information in different formats, for example, a graph or a table.
2	**Drill Down** - To find out more about the events, double-click a widget to drill down to a more specific view or raw log files.
3	**Options** - Customize the view
4	**Queries** - Predefined and favorite search queries
5	**Time Period** - Specify the time periods for the view.
6	**Query search bar** - Define custom queries using the GUI tools, or manually entering query criteria. Shows the query definition for the most recent query.

Customization

Customize your views according to these options:

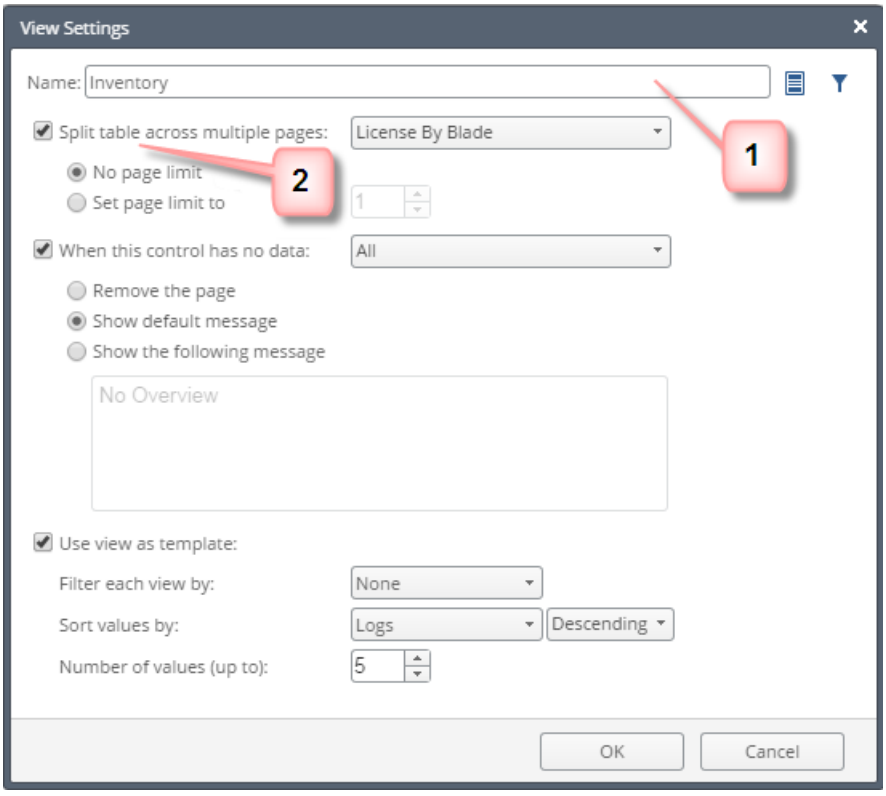


Click **Edit** to switch to view edit mode.

SmartConsole saves an administrator's customized views.

- To share a customized view with another administrator, use the Export and Import option ("Export and Import" on page 31).
- To customize a widget, see: Customizing Widgets ("Widgets" on page 39)

View Settings



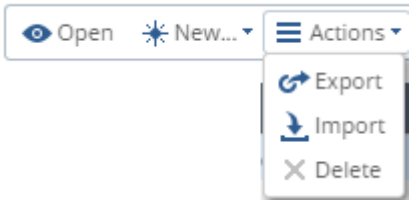
1. Enter a title.
2. To show more results, this option allows a table to spread across multiple pages when saved to PDF.

   The **No page limit** option shows more results by spreading them across a number of pages.

Export and Import

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

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



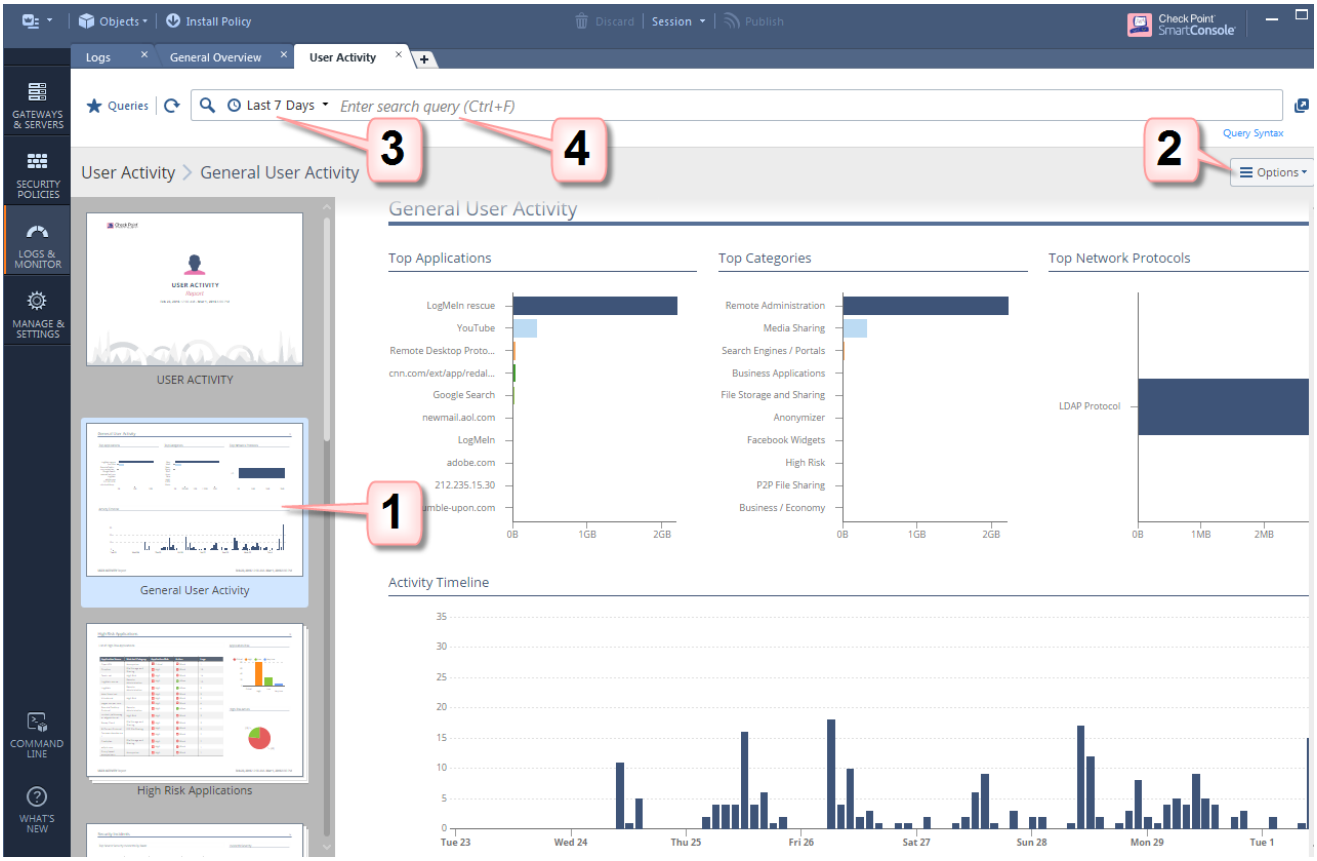
Save As PDF

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

Reports

A report has multiple views, and applies to the time that the report is generated. It gives more details than a view. There are several predefined reports, and you can create new reports. Reports can be customized, filtered, generated and scheduled. You cannot drill down into a report.

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

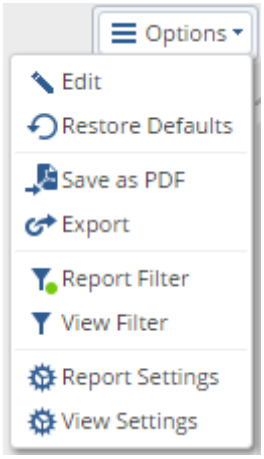


Item	Description
1	**Preview bar** - A report is divided onto pages, usually, one view on one page. Editing a report is done per page, in the same way as you edit a view.
2	**Options** - Customize, and generate a report.

Item	Description
3	**Time Period** - Specify the time periods for the report.
4	**Query Search bar** - Define custom queries using the GUI tools, or manually entering query criteria. Shows the query definition for the most recent query.

Customization

Customize your reports according to these options:



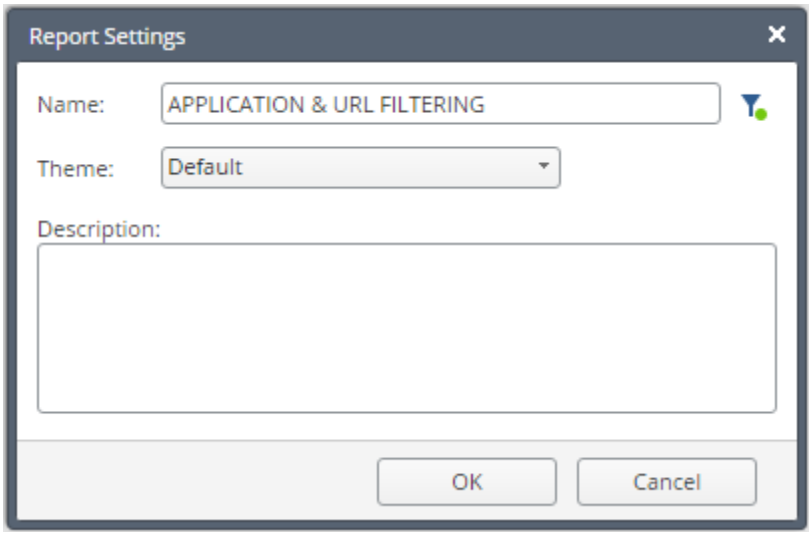
Click **Edit** to switch to the report edit mode.

To customize widgets, see: Customizing Widgets ("Widgets" on page 39)

SmartConsole saves an administrator's customized reports. To share customized reports with other administrators, use the **Export** and **Import** options.

Report Settings

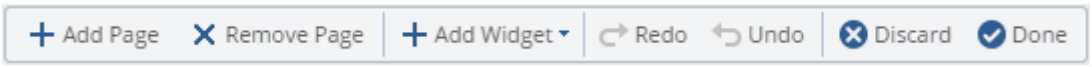
Reports can be configured according to these options:



Customizing a Report

1. Select a report from the Catalog (new tab).
2. Click Options > **Edit**.
3. Select the page to edit.

You can also add or remove pages by clicking one of these:



4. Customize the widgets ("Adding and Customizing" on page 39).
5. Add a widget, or arrange widgets in the view: Drag & Drop or expand.
6. Define filters.

Note -

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

See: Generating a Report (on page 35)

Filtering Reports by User Groups

You can filter based on User Groups.

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

To configure SmartEvent for user group filtering:

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

To generate reports filtered by user groups:

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

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

To define a scheduled report filtered by user groups:

1. Generate a report filtered by the specified User Group.
2. Copy the full User Group name from the generated report cover page.
   The User Group name typically starts with the prefix "**ad_**".
3. Define new custom report:
   a) Right-click on an existing report.
   b) Select **Save As**.
   c) Right-click the new report.
   d) Select **Edit**.
   e) Click the **Filter** icon.
   f) Define a User Group filter.

   The **Filter** icon is on the toolbar, above the report page selection area.

g) Make sure that you accurately enter (or paste) the User Group name that you copied in step 2.

h) Save the report.

4. Generate the new custom report.
5. Make sure that the filter works as expected.

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

Automatic Report Updates

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

Adding a Logo to Reports

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

To add a logo to your reports:

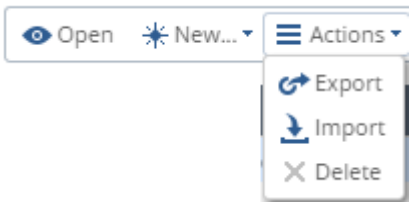
1. Save your logo image as a PNG file with the name `cover-company-logo.png`.
2. Copy the image to the `$RTDIR/smartview/conf` directory on the SmartEvent server.

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

Export and Import

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

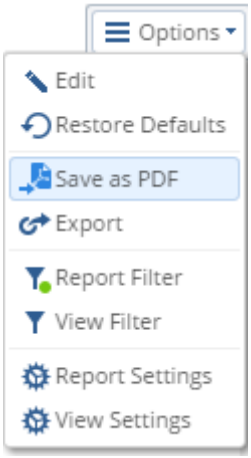
To import the file from another server, or from another administrator, use the **Import** option in the Catalog (new tab).



Generating a Report

1. Open the Catalog (new tab) and select a report.
2. Define the required timeframe and filter in the search bar.

3. Click **Options** > **Save As PDF**.



Generating a Predefined Report in the SmartEvent GUI Client

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

Generate a predefined report in the SmartEvent GUI if you want to schedule it.

To generate a predefined report:

1. Open **SmartConsole** > **Logs & Monitor**.
2. Click the **+** to open a Catalog (new tab).
3. Click the **SmartEvent Settings & Policy** link.
4. In the SmartEvent GUI, open the **Reports** tab.
5. Select a **Default Report** for a Software Blade.
6. Click **Generate**.
7. In the **Generate a Report** window, select a time period.
8. Click **Generate**.

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

Scheduling a Report

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

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

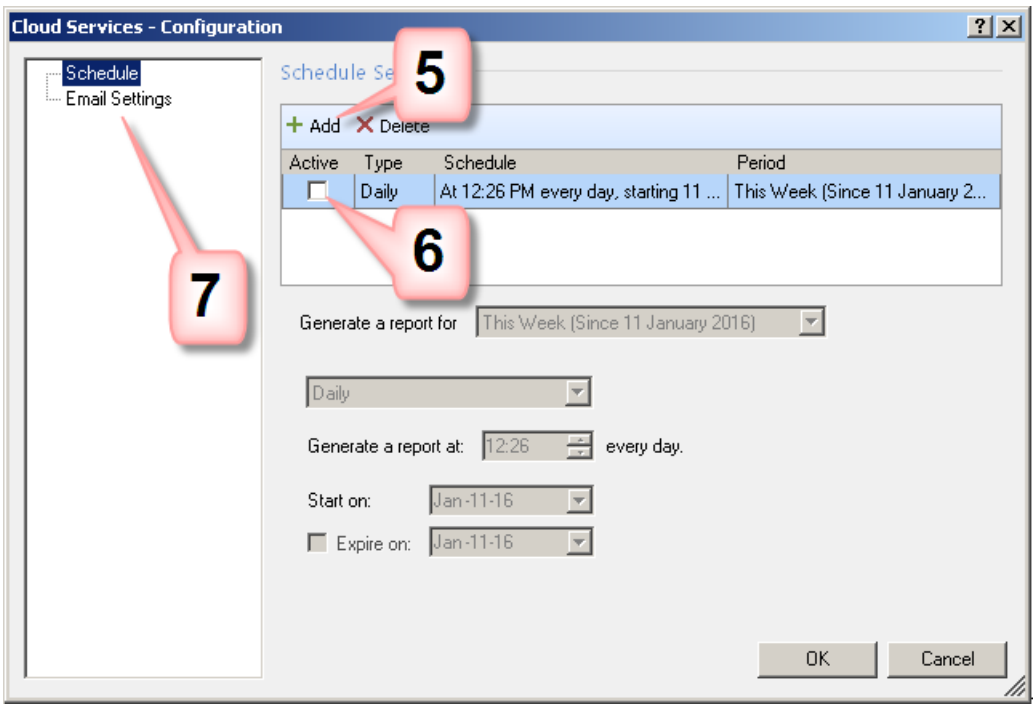
1. Open the **Report** tab
2. Select the report from the Report tree.
3. Click **Edit**.

To schedule a report:

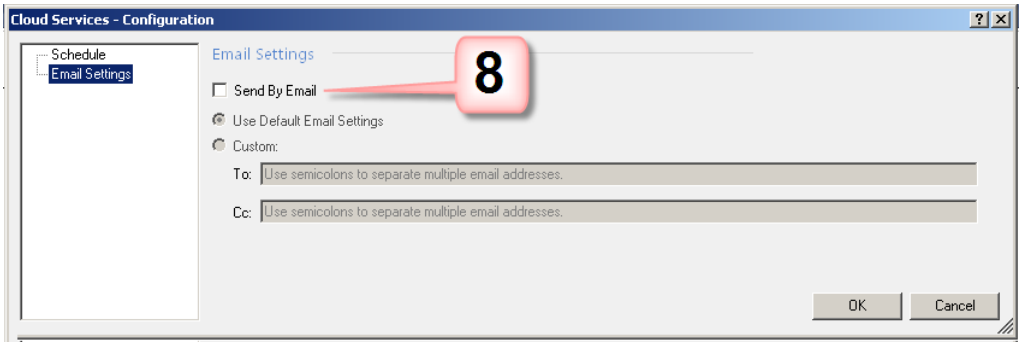
1. Open SmartConsole > Logs & Monitor.
2. Click the (+) to open a Catalog (new tab).
3. Click the **SmartEvent Settings & Policy** link.

4. In the SmartEvent GUI client, select **Schedule**.

The Schedule and Email settings configuration window opens.



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



Generating a Network Activity Report

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

To enable the Network Activity Report:

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

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

Configuring Email Settings for Reports

You can configure SmartEvent to automatically send reports by email to specified, default recipients each time the report runs. Use this procedure to define the default recipient addresses and the SMTP server connection.

To configure email server settings:

1. In SmartEvent, click **Settings** > **Reports**.
2. In the **Email Server s**ection, enter the SMTP mail server URL and sender email address in the applicable fields.

   The sender email address shows on all report emails sent by SmartEvent.
3. Click **Test Connection**, to make sure that the defined SMTP connection works correctly.
4. In the **Email Server** section, enter the default recipient email addresses in the **To** and **Cc** fields.

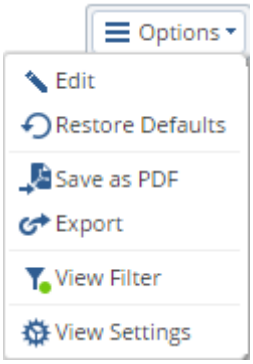
   You can enter more than one email address in each field, separated by semicolons.

Widgets

In This Section:

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

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



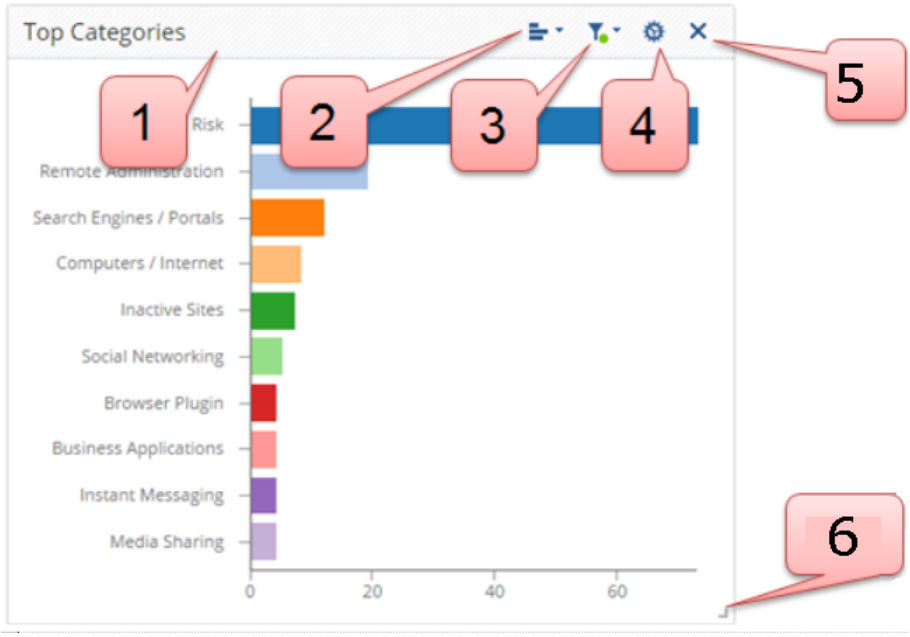
Adding and Customizing

To add a Widget:

1. Add a widget

2. Select a widget type:
   Chart
   Timeline
   Table
   Map
   Infographic
   Container
   Rich Text

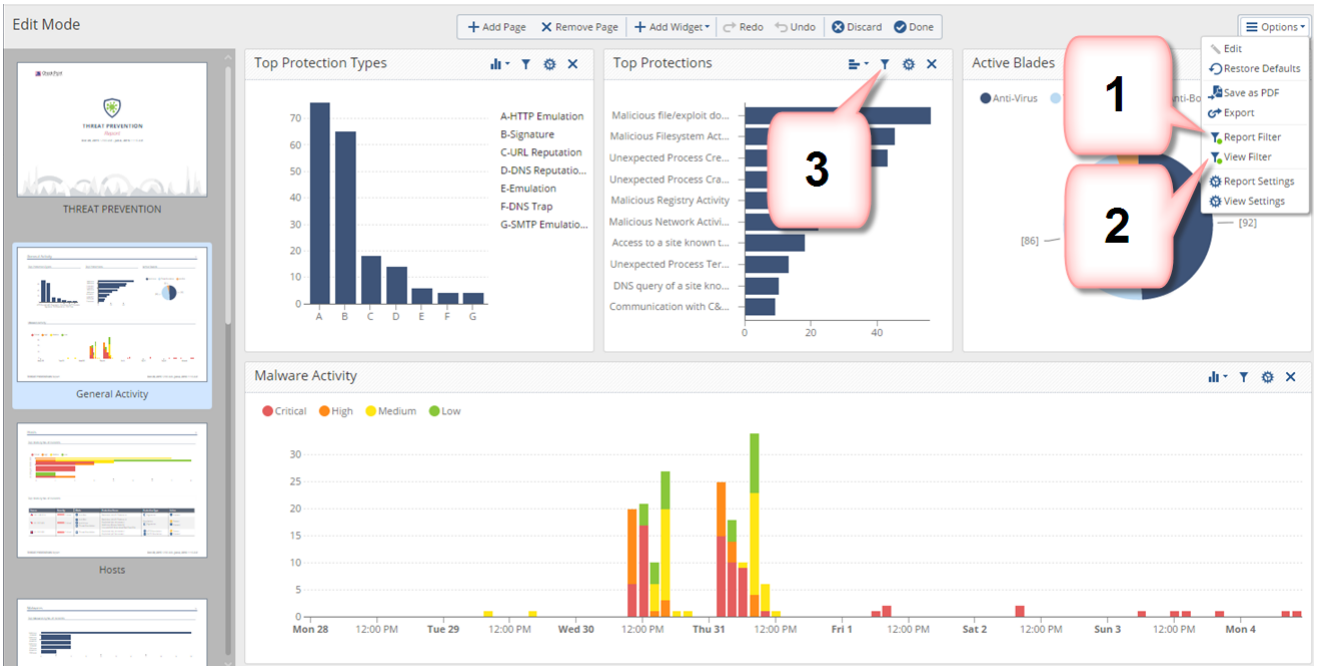
To customize a widget:



1. Drag and drop the widget within the view.
2. Select the graphic presentation that best fits the information you want to see.
3. Select filters for the widget in addition to the inherited filters from the report and view layers. (See: Filters (on page 40)).
4. Configure settings for the widget.
5. Delete a widget.
6. Resize widget.

Filters

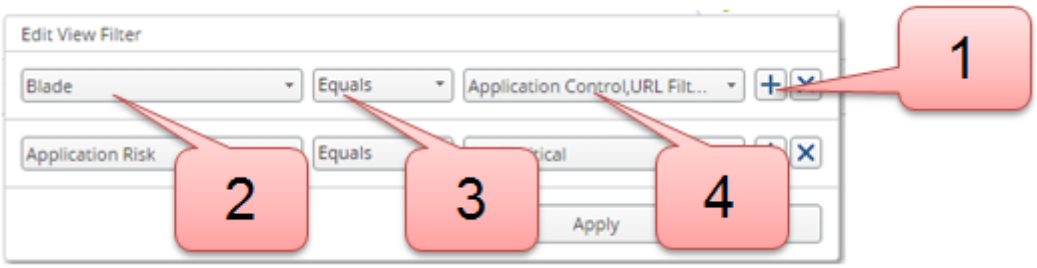
The search bar is used to apply on-demand filters, but you can also save filters with the view / report definition.



There are different layers of filters:

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

Edit View Filter



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

Logging

In This Section:

Log Analysis

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.

Sample Log Analysis

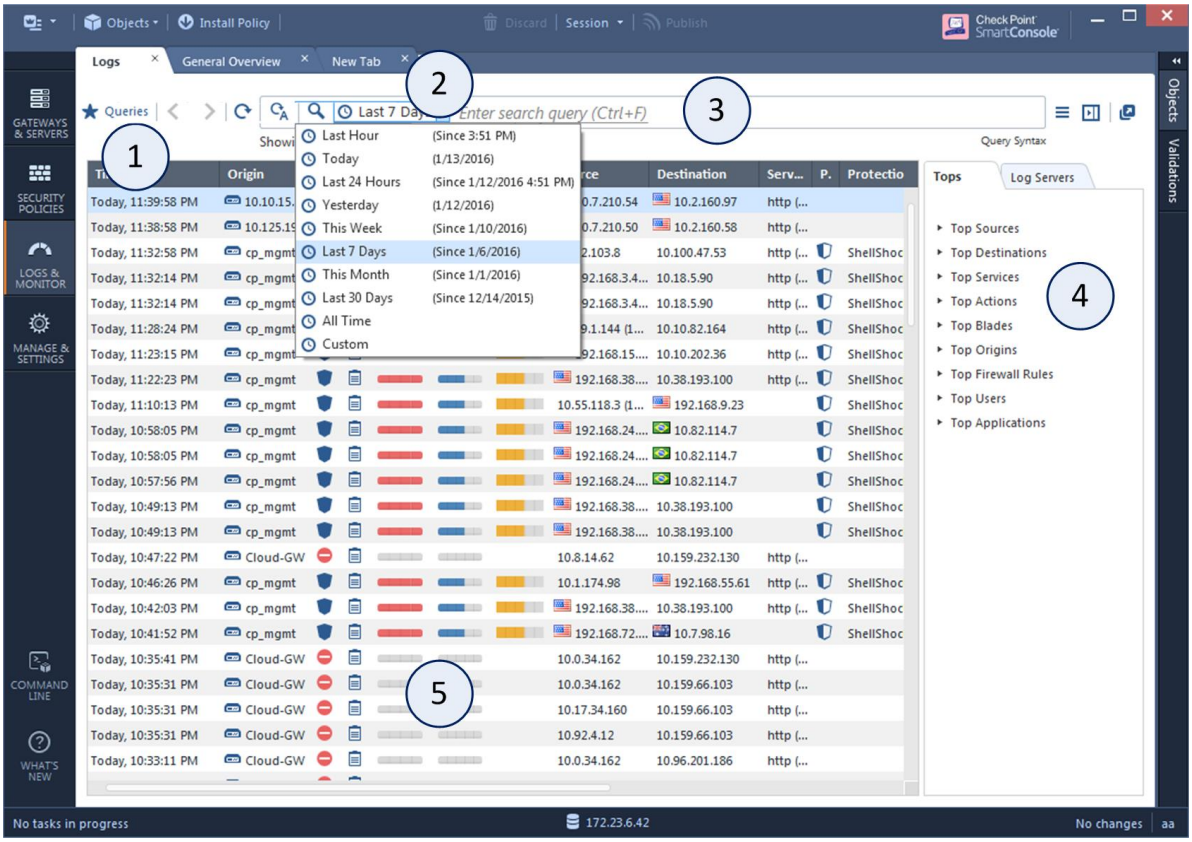
This is a sample procedure that shows how to do an analysis of a log of a dropped connection.

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 Access Control 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 Rule Base.
5. Double-click a log.
   The **Log Details** window opens.

Using the Log View

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



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

Working with Logs

In This Section:

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. But when you track multiple rules, the log file will be large, and will require 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.

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 minute intervals, to show how much data has passed in the connection: Upload bytes, Download bytes, and browse time.

Advanced Track options

Detailed Log and **Extended Log** are only available if one or more of these Blades are enabled on the Layer: *Applications & 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.

Granularity Level

- **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.
- **Per Session** - Select this to generate one log for all the connections in the same session. This is the default for rules in a Layer with *Applications and 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 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** - Send an SNMP alert to the SNMP GUI, or run the script defined in the **Global Properties**.
- **Mail** - Send an email to the administrator, or run the mail alert script defined in the **Global Properties**.
- **User Defined Alert** - Send one of three possible customized alerts. The alerts are defined by the scripts specified in the **Global Properties**.

Viewing Rule Logs

You can search for the logs that are generated by a specified 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:
   - **Summary** - Rule name, rule action, rule creation information, and the hit count. Add custom information about the rule.
   - **Details** (Access Control Policy only) - Details for each column. Select columns as necessary.
   - **Logs** - Log entries according to filter criteria - **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 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 press 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 press 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.

The packet capture option is activated by default.

To deactivate packet capture:

1. In SmartConsole, in the **Security Policies** view
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 Viewer Output** window opens.
4. Optional: Click **Save** to save the packet capture data as a text file.

Searching the Logs

SmartConsole lets you quickly and easily search the logs with many predefined log queries, and an easy to use language for custom queries ("Creating Custom Queries" on page 47).

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.
   The query runs automatically. When you add more criteria, results are updated dynamically.

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. To see all logs that have been aggregated in a specific time interval, click **View**.

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.

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.

If no blade is specified, 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.
10. To change the column width, drag the right column border in the **Results** Pane.
11. To save the column width, right-click and select **Save Profile**.

    The column is applicable to future sessions.

Creating Custom Queries

Queries can include one or more criteria. To create custom queries, use one or a combination of these basic procedures:

- Right-click columns in the grid view and select **Add Filter**.
- Click in the **Query search bar** and select the fields and filter criteria for those fields.
- Manually enter filter criteria in the **Query search bar**.

To create a new custom query, run an existing query, and use one of these procedures to change it. You can save the new query in the **Favorites** list.

When you create complex queries, the log search tool suggests, or automatically enters, an appropriate Boolean operator. This can be an implied AND operator, which does not explicitly show.

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.
   The query runs automatically.

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 type 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 type, the **Search** shows recently used query criteria or full queries. This helps you to search. To use these suggestions, select them from the drop-down list. If you make a syntax error in a query, the **Search** shows a helpful error message that identifies the error and suggests a solution.

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 the GUI 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, **Risk:High** is case sensitive (**Risk:high** 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, enter a Boolean operator.

Criteria Values

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

One word string examples:

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

Phrase examples

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

IP Addresses

IPv4 and IPv6 addresses used in log queries are counted as one word. Enter IPv4 address with dotted decimal notation and IPv6 addresses with colons. You can also use the '`*`' wildcard character with IP addresses.

Example:

- 192.0.2.1
- 2001:db8::f00:d

NOT Values

You can use NOT *<field>* values with field keywords (on page 50) 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. **The wildcard character cannot be the first character** in a query criterion. 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.

Using Wildcards with IP Addresses

The wildcard character is useful when used with IPv4 addresses. It is a best practice to put the wildcard character after an IP address delimiter.

Examples:

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

Field Keywords

You can use predefined field names 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
`risk`		Potential risk from 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

Keyword	Keyword Alias	Description
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>*|(*<value>**<operator>**<value>*)

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 & URL Filtering Software 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.

Event Analysis

In This Section:

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 two or more logs, are created by the SmartEvent Correlation Unit. These *correlated events* are defined in the SmartEvent client GUI, in the Policy tab.

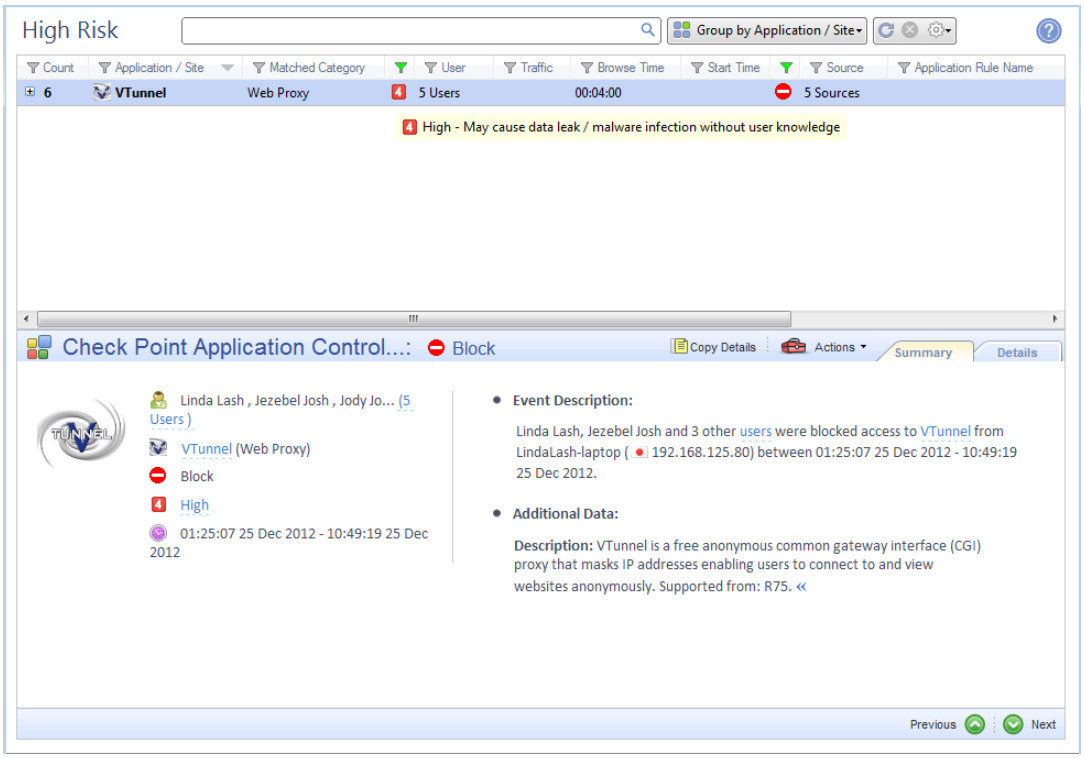
Most logs are Firewall, VPN and HTTPS inspection logs. Therefore, SmartEvent does not define them as events by default to avoid a performance impact on the SmartEvent Server. However, enabling consolidated events for Firewall saves disk space so and makes it possible to keep a longer event history. To create events for Firewall, in the SmartEvent Policy tab, enable **Consolidated Sessions > Firewall Session**.

Sample Application & URL Filtering Event Analysis

To show an Internet browsing event:

1. In the Logs & Monitor view of SmartConsole or the SmartView Web Application, open the **General Overview**.
2. In the Query search bar, select the time period. For example: **Past 24 Hours**
   The events of this time period show.
3. In **Timeline View**, click a circle below **High Risk Attacks**.

This is an example log of a High Risk event.



Information about the event:

- In the **User** column, five users tried to access the VTunnel web proxy.
- VTunnel is classified as a **High** security risk. It is a Web proxy site that lets users go to websites anonymously.
- The names of the five users that tried to go to the VTunnel website are shown.

The SmartEvent Solution

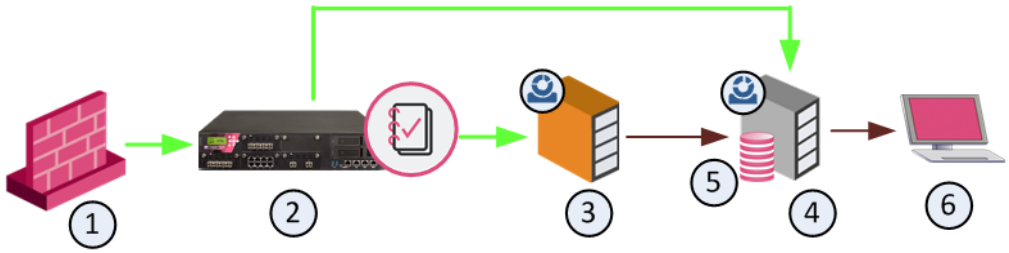
In This Section:

The Event Analysis 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).
- 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	Receives the items that are identified as events by the SmartEvent Correlation Unit. The SmartEvent Server does further analysis to determine the severity level of the event and what action to do. The event is stored in the system database.
5	Events database	Stores events. Located on the SmartEvent Server.
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 • SmartEvent GUI

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. You can install more than one SmartEvent

Correlation Unit. 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 does one of these actions:

- 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.

The SmartEvent GUI

The SmartEvent GUI is one of the SmartEvent clients that you can use to analyze events that occur in your environment.

Overviews:

The **Overview** tab shows top events of all types. When you work with a protection type, you can go directly to the data for that area.

Click the tab for events filtered by Software Blade:

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

Drill down forensics:

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

Quickly search the database of logs and events:

Use **Search Suggestions** and **Recent Searches**. Click in the search bar to see the search suggestions and your recent searches. The search is fast, and the results are from the event database.

For example, to see only important events from 192.168.2.15:

1. Click the **Search** bar.
2. Select **Severity** in the **Suggestions** list.
3. In the list of valid values that shows, click **Critical**.
4. Click in the Search bar.
5. Select **Source** in the **Suggestions** list.
6. If the required IP address not in the list, enter it in the search bar.

The data in all the panes is updated to match your search.

Filter for standard results:

Click **Filters** to select a standard filter option. For example, in Application and URL Filtering, you can filter to see only events of **Application Control** or only events of **URL Filtering**. You can filter for **Action**, to see events for Blocked or Allowed traffic.

Free-text search using the log search syntax:

For more sophisticated searching, you can do AND/OR searches with the Query Syntax ("Query Language Overview" on page 48).

The SmartView Web Application

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.

To log in to SmartEvent using SmartView Web Application:

Browse to
`https://`*<Security Management Server IP Address>*`/smartview/`
or
`https://`*<Security Management Server host name>*`/smartview/`

Note - The URL is case sensitive.

Working with SmartEvent

In This Section:

Opening the SmartEvent GUI Client

To open the SmartEvent GUI client:

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

Configuring Event Definitions in the SmartEvent Policy Tab

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

After the SmartEvent client starts to show events, do these procedures:

- Fine-tune the Event Policy
- Change the existing Event Definition to see the events that interest you (see "Modifying Event Definitions" on page 57)
- Create new Event Definitions to see the events that are not included in the existing definitions (see "Creating Event Definitions (User Defined Events)" on page 63)

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**.

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.

To change Event Definitions:

1. Select a type of event from one of the **Event Policy** categories.
2. Adjust the Event Definitions. The elements that can be modified vary per event definition. Some event types include all; others have just one or two of these configurable elements.
3. To save the Event Policy, click **File** > **Save**.
4. From the **Actions** menu, click **Install Event Policy**.

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**, such as **Block Source** or run **External Script**
- Exceptions, such as **Apply the following exceptions**
- **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 77).

Event Threshold

The Event Threshold allows you to modify the limits that, when exceeded, indicates that an event has occurred. The limits typically are the number of connections, logs, or failures, and the period of time in which they occurred. It appears thus:

Detect the event when more than *x* **connections/logs/failures** (etc.) **were detected over a period of** *y* **seconds**.

To decreasing the number of false alarms based on a particular event, increase the number of connections, logs or failures and/or the period of time for them to occur.

Severity

An event severity affects in which queries (among those that filter for severity) this type of event will appear.

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

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 Create a Mail Reaction ("Creating a Mail Reaction" on page 60).
- **Block Source** - instruct the Security Gateway to block the source IP address from which this event was detected for a configurable period of time . Select a period of time from one minute to more than three weeks. See Create a Block Source Reaction ("Creating a Block Source Reaction" on page 61)
- **Block Event activity** - instruct the Security Gateway to block a distributed attack that emanates from multiple sources, or attacks multiple destinations for a configurable period of time. Select a period of time from one minute to more than three weeks). See Create a Block Event Activity Reaction ("Creating a Block Event Activity Reaction" on page 61).
- **External Script** - run a script that you provide. See Creating an External Script Automatic Reaction (on page 61) to write a script that can exploit SmartEvent data.
- **SNMP Trap** - generate an SNMP Trap. See Create an SNMP Trap Reaction ("Creating an SNMP Trap Reaction" on page 60).

  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)

These sections tell how to add an Automatic Reaction to an event:

Creating Automatic Reactions

You can create Automatic reaction from:

- The Policy tab: Select **General Settings**> **Object** > **Automatic Reactions**
- In an Event Definition: Select the icon **[...]** and click **Add New**.

The first step for each of the next procedures assumes that you are at one of the starting points above.

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. See the *Guidelines for creating the script* below.
2. Put the script on the SmartEvent Server:
   a) In `$RTDIR/bin`, create the folder `ext_commands`. Run:
   `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. Run:
   `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.

The following 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 refer to more fields, you can add them to the event:

a) In the SmartEvent GUI client, in the **Policy** tab, right click the event, and select **Properties > Event Format** tab

b) In the **Display** column, select the **Event fields** to have in the Event.

c) 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 section below.
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 or destinations that appear. For example, if the event **Port Scan from Internal Network** is set to detect an event when 30 port scans have occurred within 60 seconds, you can also define that two port scans detected from host *A* in 10 seconds of each other is also an event.

To manually add an exception, under the heading **Apply the following exceptions**, click **Add** and 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 "Adding Network and Host Objects" on page 77).

To modify or delete existing exceptions, select **Edit** or **Remove**, respectively.

Creating Event Definitions (User Defined Events)

To create a user-defined event you must have knowledge of the method by which SmartEvent identifies events. This section starts with a high level overview of how logs are analyzed to conclude if an event occurs or occurred.

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 (on page 63)
- Matching a Log Against Each Event Definition (on page 64)
- Creating an Event Candidate (on page 65)
- When a Candidate Becomes an Event (on page 67)

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

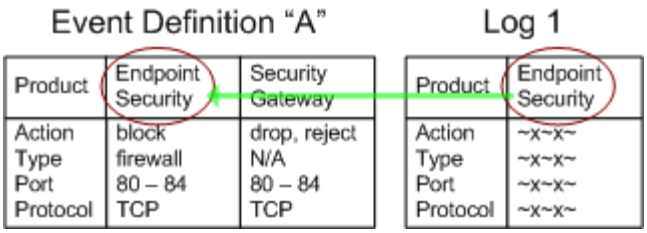
Each **Event Definition** contains a filter which is comprised of a number of criteria that must be found in all matching logs. The criteria are divided by product: The **Event Definition** can include a number of different products, but each product has its own criterion.

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.

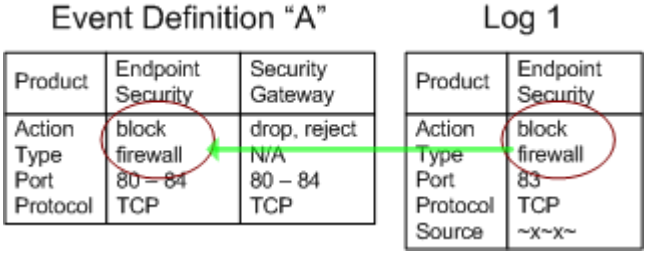
SmartEvent divides this procedure into two steps. The SmartEvent Correlation Unit first checks if the Product value in the log matches one of the permitted **Product** values of an **Event Definition**.



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.

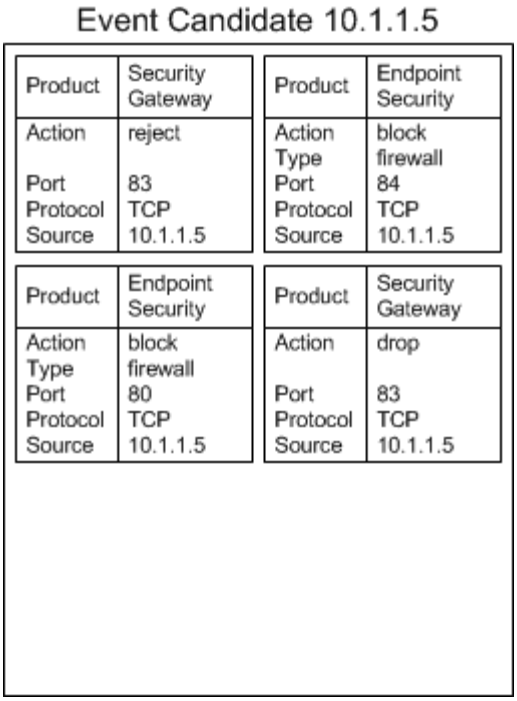
In our example, Log 1 matched **Event Definition "A"** with a permitted product value. The SmartEvent Correlation Unit examines if the log contains the necessary criteria for an Endpoint Security log to match.



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.

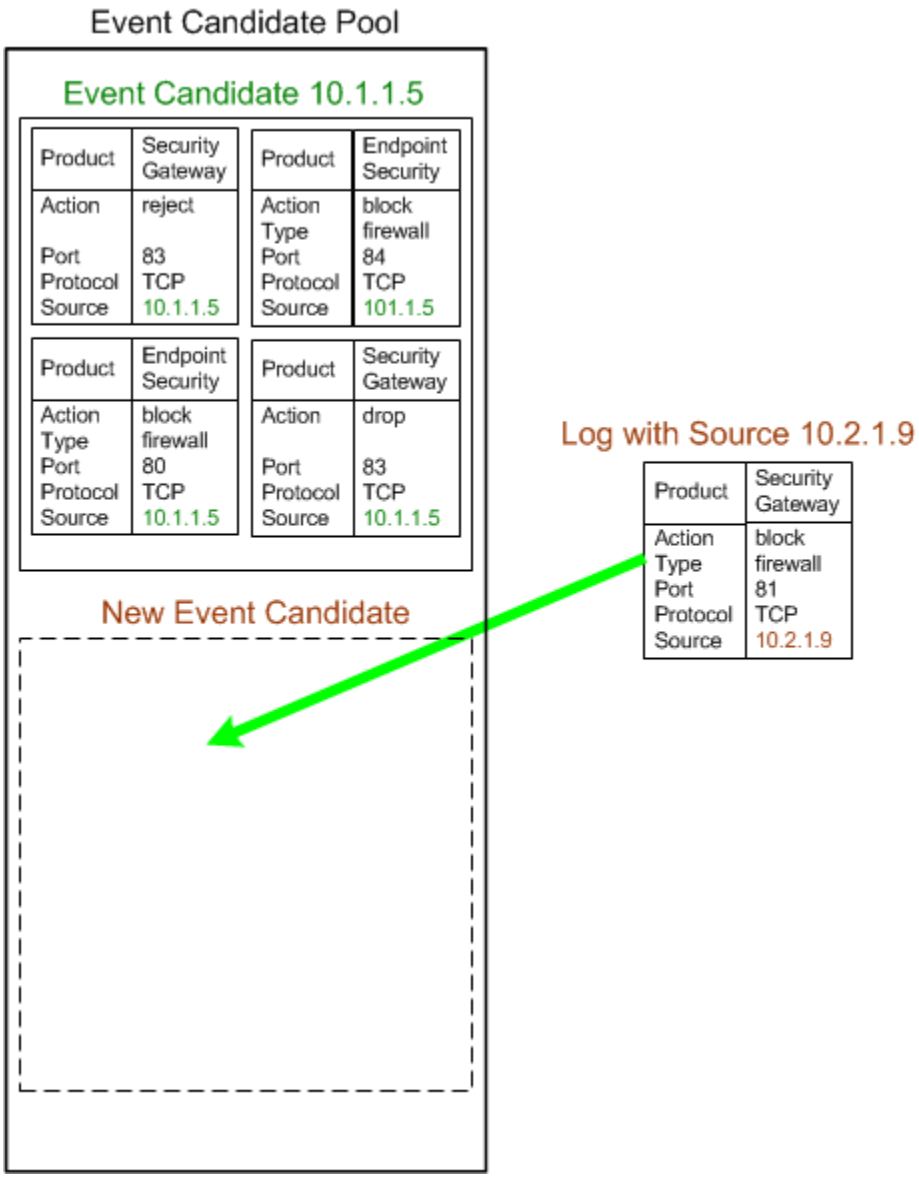


Notes -

- The **Event Candidate** can track logs from multiple products
- The logs must be from the same source
- The **Event Candidate** tracks logs before all of the criteria were matched

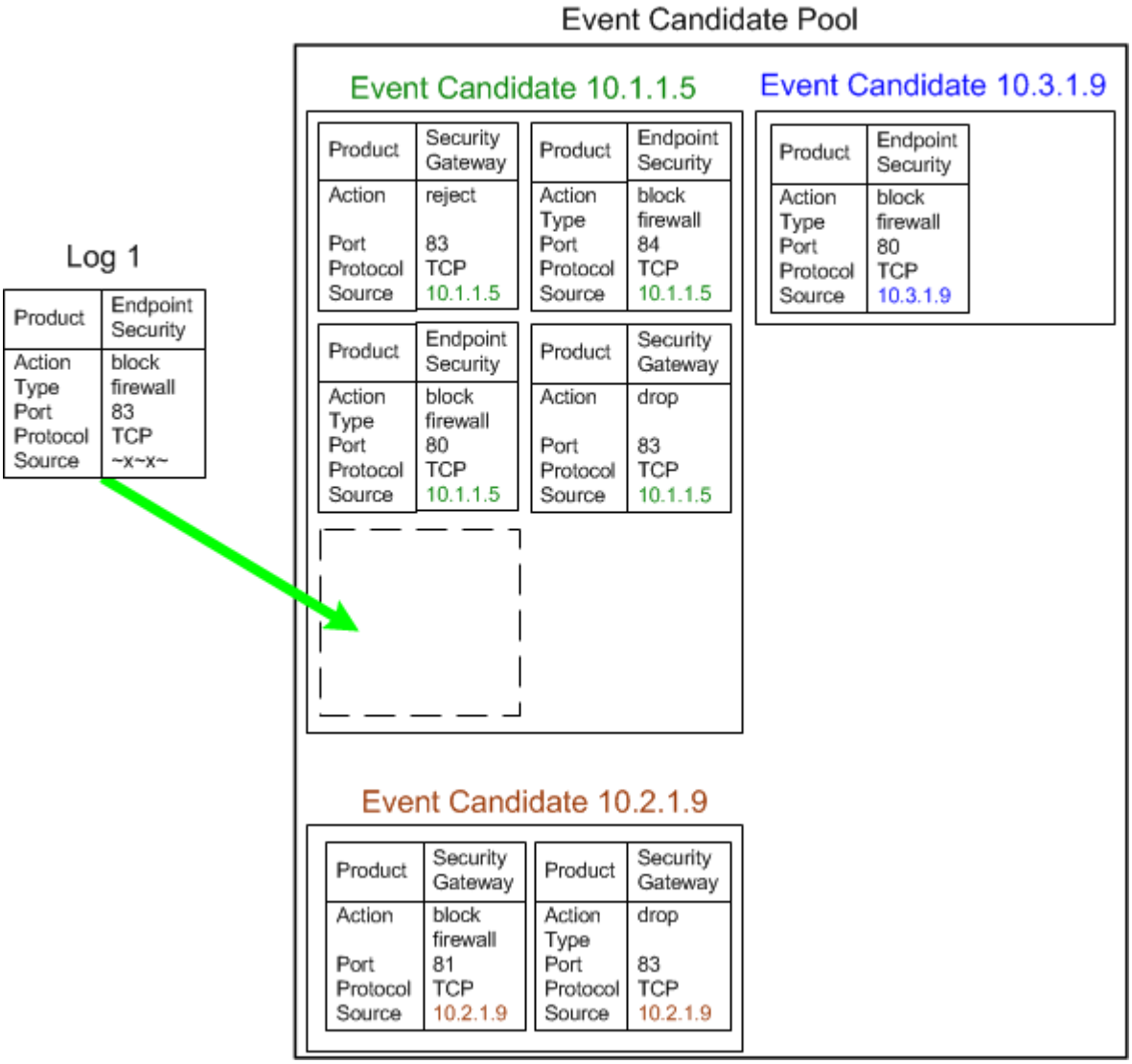
Each **Event Definition** can have multiple event candidates, each of which keeps track of logs grouped by equivalent properties. In the figure above the logs that create the event candidate have a common source value. They were dropped, blocked or rejected by a Firewall. They are grouped together because the Event Definition is designed to detect this type of activity, that originates from one source.

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**.



Note - SmartEvent creates a new event candidate for a log with a different source.

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

When a Candidate Becomes an Event

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

To create a User Defined Event based on an existing event:

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**.

To edit 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).
    - **Filte**r - To edit a product filter:
      (i) Select the product.
      (ii) Select the Log field from the available **Log Fields** list.
      (iii) If the necessary field does not show select **Show more fields...** to add a field to the **Log Fields** list.
      (iv) Click **Add** to edit the filter.
      (v) 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
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
	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

Server Type	Category	Event Name	Source	Dest	Service	Reason
	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
	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

Server Type	Category	Event Name	Source	Dest	Service	Reason
	Anomalies	Abnormal activity on service	Any	Proxy servers	HTTP:8080	Hosts connections to Proxy servers
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
	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

Server Type	Category	Event Name	Source	Dest	Service	Reason
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
	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
	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:19191 TCP:19194)	UA replies

Server Type	Category	Event Name	Source	Dest	Service	Reason
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
	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 (see "Configuring Dedicated Correlation Units" on page 20)
- Create offline jobs analyze historical log files ("Importing Offline Log Files" on page 24)
- Adding objects to the Internal Network (see "Defining the Internal Network" on page 78)
- Creating scripts to run as Automatic Reactions for certain events ("Creating an External Script Automatic Reaction" on page 61)
- Creating objects for use in filters (see "Adding Network and Host Objects" on page 77)

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**.

Adding Network and Host Objects

Certain objects from the Management server are added during the initial sync with the SmartEvent server and updated at a set interval. But it is useful (or necessary) to add other Network or Host objects, for these reasons:

- If some devices or networks are not represented on the Management server, and are important to define your internal network.
- When you add sources or destinations to exclusions or exceptions in Event Definitions.
- When you select sources or destinations in a filter.

These screens are locked until initial sync is complete:

- Network Objects
- Internal Network

- SmartEvent Correlation Unit

You can make a device available to use in SmartEvent.

To make a device that is a host object available in SmartEvent:

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

To make a device that is a network object available in SmartEvent:

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

See Defining the Internal Network (on page 78) for information about how to add objects to the Internal Network definition.

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 inner
- Outgoing – all sources are in the network and all destinations external
- Internal – sources and destinations are all in the network
- Other – a mixture of and internal and external values makes the result indeterminate

To define the Internal Network:

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

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

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

These screens are locked until initial sync is complete:

- Network Objects
- Internal Network
- Correlation Units

SmartEvent in a Management High Availability Environment

The SmartEvent database keeps a synchronized copy of management objects locally on the SmartEvent Server. This process, dbsync, allows SmartEvent to work independently of different management versions and different management servers in a High Availability environment.

Management High Availability capability exists for Security Management Servers, and in a Multi-Domain Security Management environment, `dbsync` supports High Availability for the Multi-Domain Servers and the Domain Servers.

How it works

Dbsync initially connects to the management server with which SIC is established. It retrieves all the objects. After the initial synchronization it gets updates when an object is saved. Dbsync registers all the High Availability management machines and periodically tests the connectivity with the newest management server. If connectivity is lost, it attempts to connect to the other High Availability management servers until it finds an active one and connects to it.

If two management servers are active concurrently, dbsync stays connected to one management server. Dbsync does not get changes made on the other management server until a synchronization operation is done.

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.

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.

If the SmartEvent Server becomes unavailable, the correlation units keep the events until it can reconnect with the SmartEvent Server and forward the events.

Monitoring Traffic and Connections

In This Section:

SmartView Monitor gives you a complete picture of network and security performance. Use it to respond quickly and efficiently to changes in 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.

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, 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 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 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 scenarios

Examples of scenarios for which SmartView Monitor can help:

- If the Internet access of a company is slow, a Traffic view and report can be created. This makes sure what can clog up the company's gateway interface. 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.
- If employees that work away from the office cannot connect to the network a Counter view. A report can be created to determine what can prevent network connections. 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. Therefore, it is possible that the company cannot accommodate the mass number of employees that try to log on at once.

To Start the Monitoring Views

To open the monitoring views in SmartConsole:

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

To open SmartView Monitor:

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

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 Gateway 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.

Deploying Monitoring

To monitor a Gateway in the Logs & Monitor view of SmartConsole, or in SmartView Monitor:

- You need a Security Management Server and one or more Security Gateways.
- Enable the Monitoring blade on the Security Management Server and Security Gateways.

No other deployment steps are necessary.

Monitoring and Handling Alerts

Alerts provide real-time information about vulnerabilities to computing systems and how they can be eliminated.

Check Point alerts users to possible threats of the security of their systems. Check Point provides information about how to avoid, minimize, or recover from the damage.

The gateways sends alerts to the Security Management Server. The Security Management Server forwards these alerts to SmartView Monitor, which is actively connected to the Security Management Server.

The gateways sends alerts to get the administrator's attention to problematic gateways. The alerts show in SmartView Monitor. These alerts are sent:

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

The administrator can define alerts to be sent for different gateways. These alerts are sent in specified conditions. For example, if they have been defined for certain policies, or if they have been set for different properties. 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 send alerts for predefined system events. If predefined conditions are set, you can get an alert for important situation updates. These are called System Alerts. For example, if free disk space is less than 10%, or if a security policy has been changed. This is how System Alerts are characterized:

- Defined for each product: For instance, you can define System Alerts for Unified Package and other System Alerts for Check Point QoS.
- Global for each gateway: Set global alert parameters for all gateways in the system, or specify an action to take on alert on the level of each Check Point gateway.
- Shows through the same user-friendly window.

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. Click the **Alerts** icon in the toolbar.
   The **Alerts** window opens.

2. Set alert attributes and delete shown alerts.

System Alert Monitoring Mechanism

Check Point Security Management Server has a System Alert monitoring mechanism. It uses the System Alert thresholds you defined. If reached, it activates the defined action.

- To activate this mechanism: Select **Tools > Start System Alert Daemon**.
- To stop the System Alert monitoring mechanism: Select **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 (**Install Policy** not required).

The Need for Suspicious Activity Rules

Connections that provide access to employees and customers can be an open doorway to attack the network and its applications. Therefore, the connection of enterprise and public networks make a good information security challenge.

A modern business requires an easy access to information, but to keep this information secure and private.

The changing network environment demands to immediately react to a security problem, but without to change the network's Firewall Rule Base. For example, you want to instantly block a user. Inspect and identify all inbound and outbound network activity as suspicious when necessary. For instance, when network or system activity indicates that someone attempts to break in.

Creating a Suspicious Activity Rule

SAM rules take some CPU resources. Therefore, set an expiration that gives you time to investigate, but does not influence performance. Best practice is to keep only the necessary SAM rules. 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 toolbar, click the **Suspicious Activity Rules** button.
   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 your examining time limit.
6. Click **Enforce**.

You can create a Suspicious Activity rule based on TCP or UDP use.

To create an activity rule:

1. In the **Block Suspicious Activity** window > **Service**, click the button.
   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 and click **OK**.
3. 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.
4. Select **Block Source**.
   The **Block Suspicious Activity** window opens.
5. Create the rule.

6. 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.

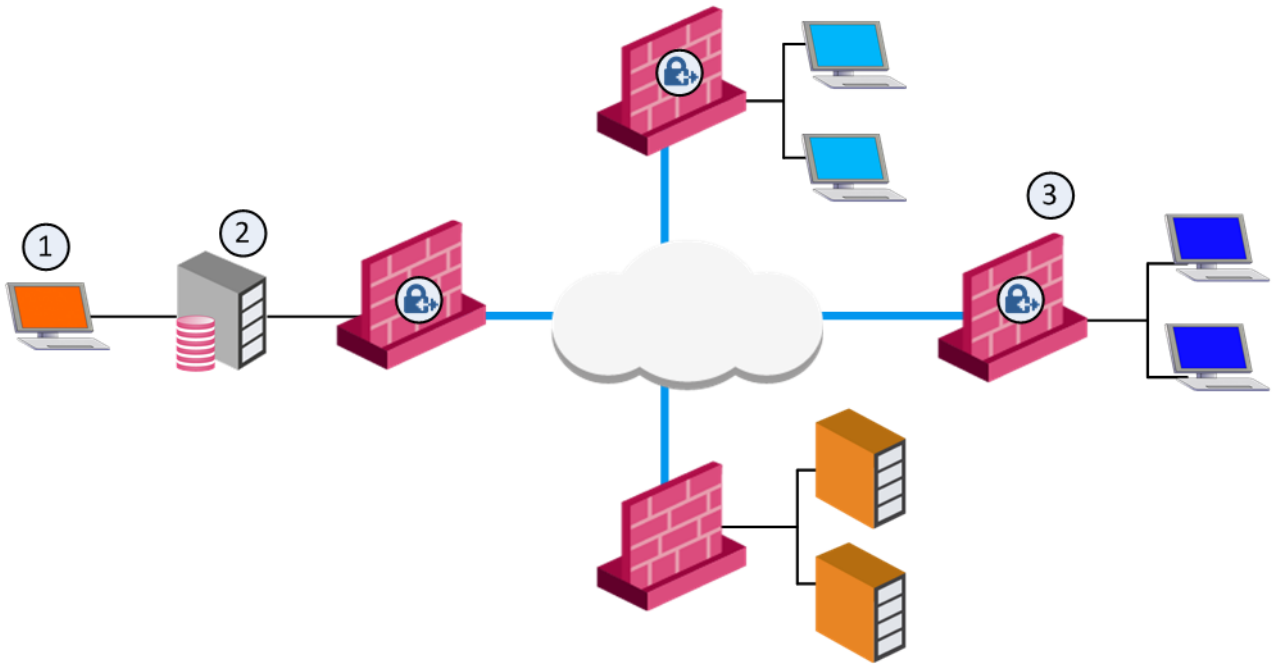
How SmartView Monitor Works

Data for the status of all 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-partner 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

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**.

Configuring SmartView Monitor

System Alerts and Thresholds

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

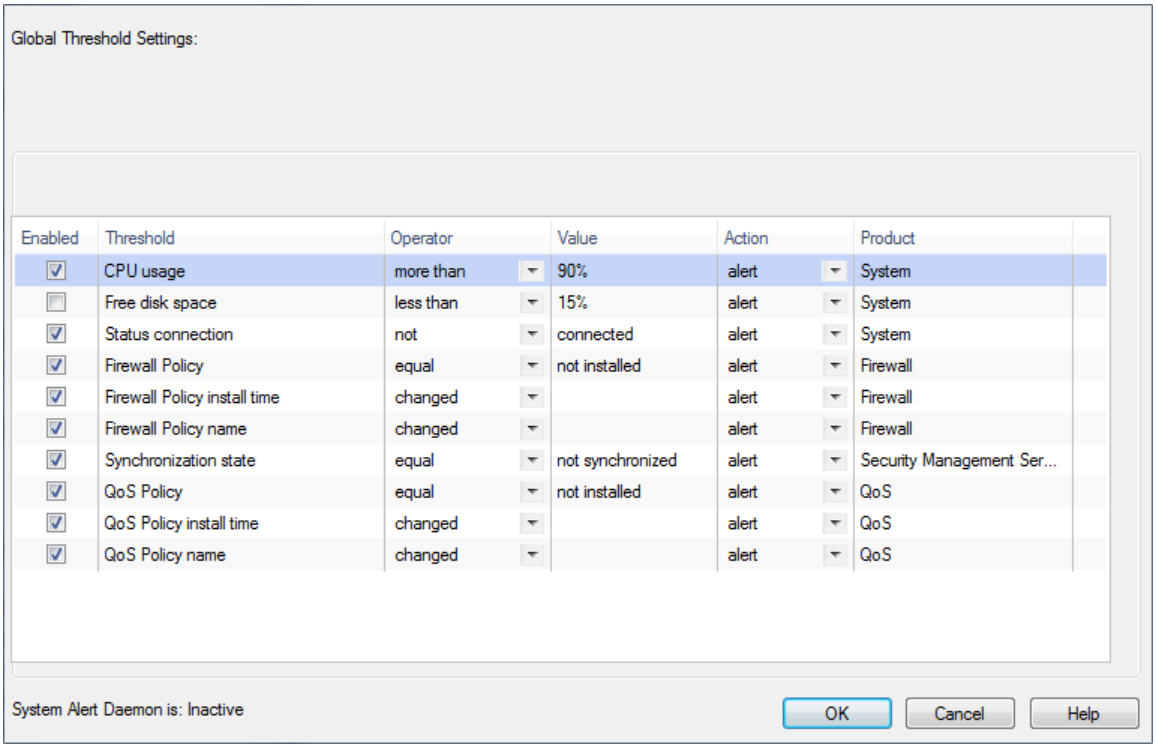
To set System Alert thresholds:

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 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. Go to **SmartConsole > 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 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

- Domain Log Server Connectivity

Some categories apply only to some machines or deployments.

 **Note** - SNMP monitoring thresholds are supported from R75.20, R71.30, and higher.

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

Configure the SNMP monitoring thresholds in the command line of the Security Management Server. When you install the policy on the gateways the SNMP monitoring thresholds are applied globally to all gateways.

Configuring in Multi-Domain Security Management

In a Multi-Domain Security Management environment, you can configure thresholds on the Multi-Domain Server and on each individual Domain Server. Thresholds that you configure on the Multi-Domain Server are for the Multi-Domain Server only. Thresholds that you configure for a Domain Server are for that Domain Server and its gateways. If a threshold applies to the Multi-Domain Server and the Domain Server gateways, set it on the Multi-Domain Server and Domain 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 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` utility.

- 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 Server**: Alerts are generated for the Multi-Domain Server and Domain Servers separately when the threshold point is passed.

Configuring a Local Gateway Policy

You can configure SNMP thresholds locally on a gateway with the same procedure that you do on a Security Management Server. But each time you install a policy on the gateway, the local settings are erased and it reverts to the global SNMP threshold settings.

You can use the `threshold_config` utility to save the configuration file and load it again later.

On SecurePlatform and Linux, the configuration file that you can back up is: `$FWDIR/conf/thresholds.conf`

On Windows, the configuration file that you can back up is: `%FWDIR%\conf\thresholds.conf`

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 `threshold_config`, 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 Domain 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
- Domain 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

You can complete threshold configuration and activate the settings.

To complete configuration and activate the settings:

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 Security Management 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 total 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 that alerts are sent to.
  - **Name** - The name of the location.
  - **Type** - The type of location. For example, a Domain Log Server or NMS.
  - **State** - If logs are sent from the 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 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 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** gateway.
   - If you often need results for on gateway, select it in **Specific Gateway**.
   - If you have a small number of 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, 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** gateway.
   - If results for one gateway are frequently necessary, select it in **Specific Gateway**.
   - If you have a small number of 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:**
     (i) Open the **Settings** tab.
     (ii) Set the update interval and chart type.
     (iii) 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 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 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 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 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 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 Gateway Status

Gateway Status

Status updates show for Security Gateways and Software Blades. The **Overall** status of a gateway is the most serious status of its Software Blades. For example, if all the **Software Blades** statuses are **OK** except for the SmartEvent blade, which has a **Problem** status, the **Overall** status is **Problem**.

Status Icon	Description
OK	The gateway and all its Software Blades work properly.
Attention	At least one Software Blade has a minor issue, but the gateway works.
Problem	At least one Software Blade reported a malfunction, or an enabled Software Blade is not installed.
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 gateway.

Displaying Gateway Data

Gateway Status data shows for each Check Point or OPSEC gateway.

To see data about a gateway, click the gateway in the **Gateway Results** view. Details about the gateway show in the **Gateway Details** pane.

System Data

- **Unified Package** - The version number.
- **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.

Firewall

- **Policy information** - The name of the Security Policy installed on the gateway, and the date and time that this policy was installed.
- **Packets** - The number of packets accepted, dropped and logged by the 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 gateway. High Watermark includes the maximum number of VPN peers for which there was an open IPsec tunnel since the 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 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 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 gateway. High Watermark includes the maximum rate of encrypted or decrypted traffic (measured in Mbps) since the gateway was restarted. Accumulative includes the total encrypted or decrypted traffic since the 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 gateway. High Watermark includes the maximum rate of encrypted or decrypted packets since the gateway was restarted, and Accumulative, the total number of encrypted packets since the gateway was restarted.
- **Encryption and Decryption errors** - The current rate at which errors are encountered by the 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 gateway (measured in errors per second) since the gateway was restarted, and the total number of errors encountered by the gateway since the 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 gateway (measured in errors per second). The High Watermark includes the maximum rate at which VPN Accelerator general errors are encountered by the gateway (measured in errors per second) since the gateway was restarted. The total number of VPN Accelerator general errors encountered by the 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 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 gateway working 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 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.
  - **Advanced -** The Security Management Server is more advanced and up-to-date than the standby server.
  - **Lagging -** The Security Management Server was synchronized correctly.
  - **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.

SmartConsole Server

The number of users that are currently connected.

Domain Log Server

Indicates the number of licensed users that are currently connected, and if the Security Management Server is active or not. The Domain Log Server includes elaborate details about the named connected client, the name of the administrator, managing the selected Domain Log Server, the host of the Domain Log Server, and the name of the database if it is locked. The Domain Log Server indicates the type of application that the Domain Log Server can track.

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 Domain Log Server
- SmartEvent Correlation Unit and Domain 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 or the Domain Log Server to let it read logs. Connect it to the SmartEvent Server to send events to it. 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 Correlation Units.

Anti-Virus and URL Filtering

SmartView Monitor can now provide statuses and counters for gateways with 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).

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 Tunnels

Tunnels Solution

VPN Tunnels are secure links between Security 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.

  Permanent tunnels can only be established between Check Point gateways. 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 gateway. Use this option to configure specific gateways to have Permanent tunnels.
  - Can be specified for a single VPN tunnel. This feature allows to configure specific tunnels between specific 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 gateway is not responding.	The gateway is not responding.

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 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 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 client, 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 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 gateways shows.
3. Select the gateway whose **Tunnels** and their status you want to see.
4. Click **OK**.
   A list of the **Tunnels** related to the selected gateway shows.

Monitoring Traffic or System Counters

Traffic or System Counters Solution

SmartView Monitor provides tools that enable you to know traffic related to specified network activities, server, and so on, and the status of activities, hardware and software use of different Check Point products in real-time. With this knowledge you can:

- Block specified traffic when a threat is imposed.
- Assume instant control of traffic flow on a gateway.
- Learn about how many tunnels are currently opened, 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 patterns

  Network traffic patterns help administrators determine which services demand the most network resources.
- Audit and estimate costs of network use

  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 gateway.
IPs/Network Objects	Shows the current status view about active IPs/Network Objects through the selected gateway.
Security Rules	Shows the current status view about the most frequently used Firewall rules. The Name column in the legend states the rule number as previously configured in SmartConsole.

Traffic Type	Explanation
Interfaces	Shows the current status view about the Interfaces associated with the selected gateway.
Connections	Shows the current status view about current connections initiated through the selected gateway.
Tunnels	Shows the current status view about the Tunnels associated with the selected gateway and their usage.
Virtual Link	Shows the current traffic status view between two 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.

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 Point Software 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 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.
- 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 gateways shows.
3. Select the 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

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 client:

- 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 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 Gateway

To run a user view for a specified Gateway:

1. In SmartView Monitor > **Tree View**, click **Users**.
2. Click **Users by Gateway**.
   The **Select Gateway** window shows.
3. Select the gateway for which you want to run the view.
4. Click **OK**.
   The view results show in the **Results View**.

Cooperative Enforcement Solution

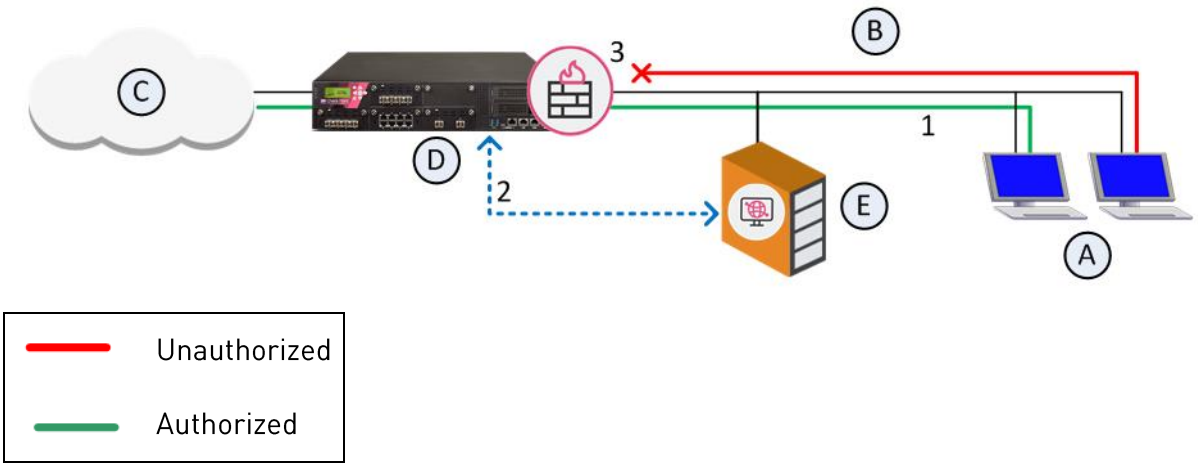
Cooperative Enforcement works with Check Point Endpoint Security Management Servers. This feature utilizes the Endpoint Security Management Server compliance function to make sure connections that come from different hosts across the internal network.

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 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.



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 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 gateway and the Endpoint Security Server must recognize the same IP address of a client. If NAT causes the IP address received by gateway to be different than the IP address received by the Endpoint Security Server, Cooperative Enforcement will not work.

Configuring Cooperative Enforcement

To configure Cooperative Enforcement:

From the gateway **Cooperative Enforcement** page, click **Authorize clients using Endpoint Security Server** to enable Cooperative Enforcement.

- **Monitor Only** - The firewall requests authorization from the Endpoint Security server, but connections are not dropped. Hosts can connect while the gateway grants authorization. The Firewall 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 server will be 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 IPs by Endpoint Security Management Server compliance:

- **Authorized** - Enables access to the Internet. If a gateway has Authorized status, it does not show in the Non-Compliant Hosts 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 gateway is not related to an Endpoint Security client.

Log and Index File Maintenance

In This Section:

Managing the Log and Event Database

SmartEvent 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 oldest events are automatically deleted to save space.

Minimum Disk Space

The Security Management Server or Log Server with log indexing enabled, creates and uses index files for fast access to log file content. Index files are located by default at `$RTDIR/log_indexes`.

To make sure that there is always sufficient disk space on the server, the server that stores the log index deletes the oldest index entries when the available disk space is less than a specified minimum. The default minimum value is 5000 MB, or 15% of the available disk space.

To change the minimum available disk space for Logs and indexes:

1. In SmartConsole, edit the Security Management Server or Log Server or SmartEvent network object.
2. Open **Logs > Storage**.
3. Select **When disk space is below <number> Mbytes, start deleting old log files**.
4. Change the disk space value.

   Note - In a Multi-Domain Security Management environment, the disk space for logs and indexes is controlled by the Multi-Domain Server, and applies to all Domain Servers. Configure the disk space on the Multi-Domain Server object.

Third-Party Log Formats

In This Section:

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 http://supportcontent.checkpoint.com/solutions?id=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 convert 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 (see "Configuring Dedicated Correlation Units" on page 20).
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 `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 shows how to send Windows events to the Log Server. For advanced Windows event configuration, see sk98861 (http://supportcontent.checkpoint.com/solutions?id=sk89961).

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. Click **Publish** to save the database.
    Note - Make sure that Access Control rules allow ELA traffic between the Windows computer and the Log Server.

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 Log Server.

To configure the Windows service:

1. Install the **WinEventToCPLog** package http://supportcenter.checkpoint.com/file_download?id=7200 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:
   `C:\Program Files\CheckPoint\WinEventToCPLog\R65\bin`
   On 64 bit computers the path starts with `C:\Program files (x86)`.
4. Run: `windowEventToCPLog -pull_cert`
   a) Enter the IP address of the management server.

b) Enter the name of the corresponding OPSEC Application object that you created in SmartConsole for the Windows events.

c) 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. Click **Publish** to save the database.

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, select: **Settings > Control Panel > Administrative Tools > Local Security Policy > Local Policies > Audit Policy**.
2. Make sure that the **Security Setting** for the Policy **Audit Logon Events** is set to *Failure*. If not, double-click it and select *Failure*.
3. Open a command prompt window and go to this path:
   `C:\Program Files\CheckPoint\WinEventToCPLog\R65\bin`.
   On 64 bit computers, the path starts with `C:\Program files (x86)`.
4. 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.
5. 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.
6. 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.

Network management applications use SNMP and the supported MIB to query a management agent. The Check Point SNMP implementation lets an SNMP manager monitor the system and modify selected objects only. You can define and change one read-only community string and one read-write community string. You can set, add, and delete trap receivers and enable or disable various traps. You can also enter the location and contact strings for the system.

Check Point platforms support SNMP v1, v2, and v3. An SNMP manager use `GetRequest`, `GetNextRequest`, `GetBulkRequest`, and a specified number of traps to monitor a device. The Check Point implementation supports `SetRequest` to change these attributes: `sysContact`, `sysLocation`, and `sysName`. You must configure read-write permissions for `set` operations to work.

SNMP Best Practices Guide

The *SNMP Best Practices Guide* http://supportcontent.checkpoint.com/documentation_download?id=31396 covers these topics:

- Recommendations about how to implement SNMP for Check Point Security Gateways and Security Management Servers
- Procedures that tell how to configure SNMP counters and traps for Check Point operating systems
- A list of commonly used OIDs for the Check Point MIB. These are some of the categories for the OIDs:
  - System - CPU, memory, hard disk
  - Appliance hardware monitoring
  - Network activity
  - Check Point Software Blades

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 ("Generating a Syslog Parser and Importing syslog Messages" on page 112). 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.

In This Appendix

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 ("The Free Text Parsing Language" on page 119) and the necessary parsing files and their location on the Log Server ("The Parsing Procedure" on page 118).
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 **$FWDIR\conf\syslog**. 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 dictionaries (see "Dictionary" on page 128) 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.

syslog_free_text_parser.C uses the **allDevices.C** file (which refers to two files: **UserDefined/UserDefinedSyslogDevices.C** and **CPdefined/CPdefinedSyslogDevices.C)**. The first (**UserDefined/UserDefinedSyslogDevices.C)** contains the names of the devices parsing files that the user defines. The second (**CPdefined/CPdefinedSyslogDevices.C)** contains devices parsing files that Check Point defines. **allDevices.C** 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 128).

   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
`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 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. In example 2, each message ID is attached with its corresponding `message` field which denotes its meaning.

Unconditional _try Command Sample 2

```
: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

Field Name to be Given	Column in Logs & Monitor > Logs
`product`	Product
`service`	Service (when resolved includes the port and protocol.)
`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 2004 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".
`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 it is **index**, field_index shows. If it is **const**, field_value shows.

  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 field_index denotes the bracket number whose pattern is taken into account.

Add_field Command Sample

```
: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)
                              )
                    )
          )
)
```

`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. See Dictionary (on page 128).

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
```

Dictionary Sample

The reference to a dictionary in the parsing file is shown in this table:

Dictionary Command Sample 2

```
  :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)
         )
  )
```