Important Information

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

Latest Documentation
The latest version of this document is at: http://supportcontent.checkpoint.com/documentation_download?ID=14681
For additional technical information, visit the Check Point Support Center (http://supportcenter.checkpoint.com).

Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>07 May 2012</td>
<td>Minor topic update</td>
</tr>
<tr>
<td>16 April 2012</td>
<td>First release of this document</td>
</tr>
</tbody>
</table>

Feedback
Check Point is engaged in a continuous effort to improve its documentation.
Please help us by sending your comments (mailto:cp_techpub_feedback@checkpoint.com?subject=Feedback on SmartLog R75.40 Administration Guide).
# Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Important Information</td>
<td>3</td>
</tr>
<tr>
<td>Introduction</td>
<td>5</td>
</tr>
<tr>
<td>SmartLog Overview</td>
<td>5</td>
</tr>
<tr>
<td>The SmartLog Index Server</td>
<td>5</td>
</tr>
<tr>
<td>The SmartLog Client</td>
<td>6</td>
</tr>
<tr>
<td>SmartLog User Interface</td>
<td>6</td>
</tr>
<tr>
<td><strong>Working with Queries</strong></td>
<td>7</td>
</tr>
<tr>
<td>Running Queries</td>
<td>7</td>
</tr>
<tr>
<td>Working with the Favorites List</td>
<td>7</td>
</tr>
<tr>
<td>Adding a Query to the Favorites List</td>
<td>8</td>
</tr>
<tr>
<td>Creating a New Folder</td>
<td>8</td>
</tr>
<tr>
<td>Deleting a Folder</td>
<td>8</td>
</tr>
<tr>
<td>Working with the Results Pane</td>
<td>8</td>
</tr>
<tr>
<td>Showing Query Results</td>
<td>9</td>
</tr>
<tr>
<td>Exporting Query Results</td>
<td>9</td>
</tr>
<tr>
<td>Creating Custom Queries</td>
<td>9</td>
</tr>
<tr>
<td>Selecting Query Fields</td>
<td>9</td>
</tr>
<tr>
<td>Selecting Criteria from Grid Columns</td>
<td>10</td>
</tr>
<tr>
<td>Manually Entering Query Criteria</td>
<td>10</td>
</tr>
<tr>
<td><strong>Query Syntax</strong></td>
<td>11</td>
</tr>
<tr>
<td>Query Language Overview</td>
<td>11</td>
</tr>
<tr>
<td>Criteria Values</td>
<td>11</td>
</tr>
<tr>
<td>IP Addresses</td>
<td>12</td>
</tr>
<tr>
<td>IP Address Ranges</td>
<td>12</td>
</tr>
<tr>
<td>Numeric Ranges</td>
<td>12</td>
</tr>
<tr>
<td>Wildcards</td>
<td>12</td>
</tr>
<tr>
<td>Using Wildcards with IP Addresses</td>
<td>13</td>
</tr>
<tr>
<td>Field Keywords</td>
<td>13</td>
</tr>
<tr>
<td>Boolean Operators</td>
<td>14</td>
</tr>
<tr>
<td>Date and Time Ranges</td>
<td>14</td>
</tr>
<tr>
<td>Preceding Time Period Queries</td>
<td>15</td>
</tr>
<tr>
<td>From-To Queries</td>
<td>15</td>
</tr>
</tbody>
</table>
Chapter 1

Introduction

SmartLog is Check Point's newest management product that lets administrators rapidly get critical information from the maze of log records generated by Check Point products.

In This Chapter

SmartLog Overview 5
The SmartLog Index Server 5
The SmartLog Client 6

SmartLog Overview

SmartLog reads and indexes logs generated by activity logged by Check Point and OPSEC log-generating product. It can also be used to give an indication of problems. Network administrators can use this log information for:

- Detecting and monitoring security-related events.
  For example, alerts, rejected connections or failed authentication attempts, might point to intrusion attempts.
- Collecting information about problematic issues.
  For example, a client is authorized to create a connection, but those attempts have failed. SmartLog can show that the Rule Base was incorrectly configured to block the client connection attempts.
- Statistical purposes such as analyzing network traffic patterns.
  For example, how many HTTP services were used during peak activity as opposed to Telnet services.

What sets SmartLog apart from other log utilities is its power, ease of use and speed. The SmartLog Index Server gets log files from many different log servers and indexes them for rapid data extraction. SmartLog includes a powerful, but easy to use, query language that lets administrators create their own queries in minutes.

SmartLog is part of the SmartConsole suite of utilities and is automatically installed with no additional configuration necessary. Administrators simple enable it on their management or log server.

The SmartLog Index Server

The SmartLog Index Server contains a central index to log entries an all SmartLog enabled management and log servers. When you install SmartConsole, the SmartLog Index Server is installed automatically.

You must enable SmartLog for all Security Management Servers and log servers that are to be used with SmartLog.

To enable SmartLog Index Server:
1. In SmartDashboard, open the applicable Security Management Server or log server.
2. Select Logs.
3. Select the Enable SmartLog option.
4. Select Policy > Install Database.
The SmartLog Client

The SmartLog client gives you the tools necessary to quickly show relevant logs in one, easy to use window.

To run the SmartLog client:
1. Click Start.
2. Select All Programs > Check Point SmartLog R75.40.
3. Log in to the SmartLog client.

SmartLog User Interface

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><strong>Top Results pane</strong> - Shows the top results of the most recent query.</td>
</tr>
<tr>
<td>2</td>
<td><strong>Favorites Icon</strong> - Shows list of predefined queries. Select a query in this list to run it.</td>
</tr>
<tr>
<td>3</td>
<td><strong>Back/Forward Icons</strong> - Scroll backward and forward between recent queries.</td>
</tr>
<tr>
<td>4</td>
<td><strong>Results pane</strong> - Shows the log entries for the most recent query.</td>
</tr>
<tr>
<td>5</td>
<td><strong>Query Definition field</strong> - Shows the query definition for the most recent query. You also define custom queries in this field using the GUI tools or manually entering query criteria.</td>
</tr>
<tr>
<td>6</td>
<td><strong>Log pane toolbar</strong> - Lets you select the grid or table view for the Log pane. You can also show IP addresses and ports as numbers or their resolved names.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Resolve</strong> - Resolves IP addresses and services to their names, if possible.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Grid view</strong> - Detailed tabular view. You can select the fields to show and change the order and width of the columns.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Table view</strong> - Summary view that shows basic information. This view is suitable for small windows, but cannot be customized.</td>
</tr>
<tr>
<td>7</td>
<td><strong>Log Details pane</strong> - Shows the detailed contents of the most recently selected log record.</td>
</tr>
</tbody>
</table>
Chapter 2

Working with Queries

SmartLog lets you quickly and easily create log queries. The query results show in the Results pane. SmartLog comes with many predefined queries that are ready to run right out of the box. You can create your own custom queries and save them for future use.

In This Chapter

Running Queries 7
Working with the Favorites List 7
Working with the Results Pane 8
Creating Custom Queries 9

Running Queries

There are three basic ways to run a SmartLog query:

- Select a predefined or custom query from the Favorites list.
- Create a query in the Query Definition field. As you enter or select criteria, the query runs automatically. As you add more criteria, the query automatically runs again showing the new results.
- Select a recent query from the Query Definition field. When you place the cursor or type in the Query Definition field SmartLog

To select and run a query from the Favorites list:

1. Click the Favorites icon.
2. Select a query from the Favorites tree.

The query results show in the Results pane. You can change the query criteria and run the query again by clicking Refresh.

To run a query from the Query Definition field:

1. Click the Clear icon to remove existing query definitions.
2. Start to enter query criteria in the Query Definition field.
   As you manually enter criteria, a list shows recent queries that match the text that you are typing. You can select a query from this list or continue typing.

Working with the Favorites List

The Favorites list lets you work with predefined and saved custom queries. The predefined queries are organized into folders by Software Blade. You can add new queries to existing folder or create new folders hold them.

You can do these actions with the Favorites list:

- Add new custom queries
- Add new query folders
- Delete queries

In this version, you cannot move a query from one folder to a different folder.
Adding a Query to the Favorites List

To add a folder to the Favorites list:
1. From the Favorites menu, select Add to Favorites.
2. In the Add to Favorites window, enter a name for the new query.
   The query criteria show in the Query field.
3. Select a folder from the list or click Create a New Folder.
4. Click Add.

Creating a New Folder

You can use folders to help you organize custom queries into logical groups. Folders can be created inside of other folders.

You can also do this procedure while adding a new query to the favorites list.

To create a new folder:
1. From the Favorites menu, select Add to Favorites.
2. In the Add to Favorites window, click the Folder list.
3. Select Create a New Folder from the list.
4. In the Create a Folder window, enter a name for the new folder.
5. Select a folder to contain the new folder.
6. Click Add.

Deleting a Folder

You can delete folders that are no longer necessary.

Important: When you delete a folder, you also delete any queries included in that folder. We recommend that you carefully look at folder contents before deleting it. In this release, you cannot move a query from one folder to a different one.

To delete a folder:
1. From the Favorites menu, select Organize Favorites.
2. In the Organize Favorites folder, select the folder to be deleted.
3. Click Delete.
4. Click Close.

Working with the Results Pane

SmartLog query results show in the Results pane. You can do these actions to control how the information shows on in the pane:

- Select a view mode:
  - The Grid View shows log records in a detailed tabular view. You can select the fields that show and can change the column order and width.
  - The Table View shows a short summary of basic log data. You cannot customize this view.

- Optionally show resolved IP addresses and service names. Use the Resolve icon to toggle this option.

- Scroll down to increase the quantity of query results that show.

- Export query results to a CSV file.
Showing Query Results

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

You must scroll down to show more results. As you scroll down, SmartLog extracts more records from the SmartLog Index Server and adds them to the results set. The actual number of results in the result set shows below the Query Definition pane.

Exporting Query Results

SmartLog lets you export queries to a comma separated value (CSV) file. You can then use Microsoft Excel or other database programs to further analyze the data information print reports.

SmartLog only exports the query result included in the result set. You must scroll down to add more records to the result set. The actual number of results in the result set shows below the Query Definition pane.

To export query results:
1. Create or run a query in SmartLog.
2. Scroll down in the Results pane until a sufficient quantity of records show.
3. From the File menu, select Export > Excel CSV.
4. Enter the file name and path and then click Save.

Creating Custom Queries

Queries can include one or more criteria. You can create custom queries using one or a combination of these basic procedures:

- Right-click columns in the grid view and select Add Filter.
- Click in the Query Definition field and select fields and filter criteria for those fields.
- Manually type filter criteria in the Query Definition field.

A good way to create a new custom query is to run an existing query and then use one of these procedures to change it. You can save the new query in the Favorites list.

When you create complex queries, SmartLog 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 Definition field.

To select field criteria from the Query Definition field:
1. If you are starting a new query, click the Clear icon to remove existing query definitions.
2. Put the cursor in the Query Definition Field.
3. Select a criterion from the drop-down list or enter the criteria in the Query Definition field.

The query runs automatically. You can continue to enter more criteria using this or other procedures.
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 Definition field and the query runs automatically.

You can continue to enter more criteria using this or other procedures.

Manually Entering Query Criteria

You can always type query criteria directly in the Query Definition field. You can manually create a new query or make changes to an existing query that shows in the Query Definition field.

As you type, SmartLog helps you by showing recently used query criteria or even complete queries. To use these suggestions, simply select them from the drop down list. If you make a syntax error in a query, SmartLog shows a helpful error message that identifies the error and suggests a solution.
Chapter 3

Query Syntax

In This Chapter

Query Language Overview 11
Criteria Values 11
Wildcards 12
Field Keywords 13
Boolean Operators 14
Date and Time Ranges 14

Query Language Overview

SmartLog includes a powerful query language that lets you show only selected records from the log files, according to your criteria. You can create complex queries by using Boolean operators, wildcards, fields, and ranges. This section is a detailed reference to the SmartLog query language.

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

The basic query syntax is [Field]: Filter Criterion.
You can put together many criteria in one query by using Boolean operators:
[Field]: Filter Criterion AND|OR|NOT [Field]: Filter Criterion ...

Query keywords and filter criteria are not case sensitive.

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 apostrophes or quotation marks.

One character string examples:

- richard
- inbound
- 192.168.10.1
- mahler.ts.example.com
- dns_udp

Phrase examples:

- 'John Doe'
- 'log out'
- 'VPN-1 Embedded Connector'

Note - You cannot put numbers or IP addresses in quotation marks. For example, 'John 1234' is invalid.
**IP Addresses**

IPv4 and IPv6 addresses used in queries are one word. You can enter IPv4 address using dotted decimal or CIDR notation. IPv6 addresses are typically entered using CIDR notation.

Examples:
- 20.20.20.1
- 10.0.0.0/24
- 2010:10::0/64

**IP Address Ranges**

You can use IP address ranges in free text queries or with the source and destination fields. You enter the range criteria using this notation:

```
<starting IP address>-<ending IP address>
```

The query shows all IP addresses in the range, and includes the starting and ending addresses.

**Examples**

- 192.168.10.0-192.168.20.255

**Numeric Ranges**

You can use ranges for numeric values in free text and numeric field queries, such as the port fields.

**Syntax**

```
<Number>-<Number>
```

**Examples**

- 65000-66000
- port:80-660

**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 wild card character in query criteria.

**Wildcard syntax**

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

**Examples**

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

If your criteria value contains more than one word, you can use the wildcard in each word. For example, 'Jo* Na*' shows Joe Nameth, John Norris, Joshua Nathan, 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.

For Example:
- 192.168.10.* shows all records for 192.168.10.0 to 192.168.10.255 inclusive
- 192.168.* shows all records for 192.168.0.0 to 192.168.255.255 inclusive

Field Keywords

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

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

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Keyword Aliases</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>action</td>
<td></td>
<td>Action taken by a security rule</td>
</tr>
<tr>
<td>blade</td>
<td>product</td>
<td>Software Blade</td>
</tr>
<tr>
<td>destination</td>
<td>dst, dest, to</td>
<td>Traffic destination IP address, DNS name or Check Point network object name</td>
</tr>
<tr>
<td>ipproto</td>
<td>protocol</td>
<td>IP Protocol number</td>
</tr>
<tr>
<td>origin</td>
<td></td>
<td>Name of originating Security Gateway</td>
</tr>
<tr>
<td>port</td>
<td>dport, d_port, dst_port, destination_port</td>
<td>Destination TCP/UDP port</td>
</tr>
<tr>
<td>rule</td>
<td></td>
<td>Security rule that generated the log entry</td>
</tr>
<tr>
<td>service</td>
<td></td>
<td>Service that generated the log entry</td>
</tr>
<tr>
<td>source</td>
<td>src, from</td>
<td>Traffic source IP address, DNS name or Check Point network object name</td>
</tr>
<tr>
<td>source_port</td>
<td>sport, s_port, src_port</td>
<td>Source TCP/UDP port</td>
</tr>
<tr>
<td>user</td>
<td></td>
<td>User name</td>
</tr>
</tbody>
</table>

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

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

When using the Rule field as a criterion, you must specify rule number or rule UID together as one string. This is the syntax for this special case:

rule:<rule number or rule UID>/<policy name>

Examples:
- source:192.168.10.1
- rule:2/my_policy
- action:(drop or reject or block)

You can use the OR Boolean operator in parentheses to include multiple criteria values.
Notes:
- When using fields with multiple criteria values, you must explicitly write the Boolean operator. SmartLog does not automatically presume the `AND` operator if it is not specified.
- You must use parentheses when using multiple criteria with fields.

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 using multiple criteria without parentheses, the `OR` operator is applied before the `AND` operator.

Examples:
- `blade:"application control" AND action:block` - Shows log records from the Application and URL Filtering Software Blade where traffic was blocked.
- `192.168.19.133 OR 10.19.136.101` - Includes log entries the match one of the IP addresses.
- `(blade:Firewall or blade:IPS or blade:VPN) AND NOT action:drop` - Includes all log entries from the Firewall, IPS or VPN blades that are not dropped. The criteria in the parentheses are applied before the `AND NOT` criterion.
- `Source:(172.168.1.1 OR 172.168.1.2) AND destination:17.168.8.2` - Includes log entries from the two source IP addresses if the destination IP address is 17.168.8.2. This example also shows how you can use Boolean operators with field criteria.

Notes:
- Boolean operators are not case sensitive.

Date and Time Ranges

You can define a query that shows logs generated during the preceding period of time using the `last` or `past` keywords. The applicable periods of time are:
- minute
- hour
- day
- week
- month
- year

The syntax for this criterion is:
`last|past [number] period of time`

You can specify the period of time in the singular or the plural. If you do not enter a number, the value is presumed to be the most recent period.

Examples
- `last 12 hours` - Shows logs generated during the last 12 hours.
- `past 10 week` - Shows logs generated during the last 10 weeks. Using the singular is permitted.
- `last year` - Shows logs generated
**Preceding Time Period Queries**

You can define a query that shows logs generated during the preceding period of time using the **last** or **past** keyword.

Preceding period of time queries show log records based on the time that you run the query. For example, if your criterion is 'last 2 weeks' at 3:15 PM, SmartLog shows all logs starting from 3:15 on the 14th day before today. A log generated at 1:15 PM on the 14th day does not show, but one generated at 6:50 does show.

The valid periods of time are:

- minute
- hour
- day
- week
- month
- year

The syntax is:

```plaintext
last|past [<number>] <period of time>
```

**Examples**

- last 12 hours - Shows logs generated during the last 12 hours before the most recent time.
- past 10 week - Shows logs generated during the last 10 weeks before the most recent date and time. This example shows that you can use the singular or plural interchangeably.
- last year - Shows logs generated during the last 365 days starting from the most recent date and time. This example shows that the number one is assumed if no number value is entered.

**Notes:**

- You can specify the period of time in the singular or the plural.
- If you do not enter a `<number>` value, the number one is assumed.

**From-To Queries**

You can define queries that show log records between a starting date and time and an ending date and time. SmartLog shows records between and including the specified dates.

**Syntax**

```plaintext
dd/mmm/yyyy hh:mm:ss[-dd/mmm/yyyy hh:mm:ss]
```

- **dd** - Day of the month. The leading 0 is optional.
- **mmm** - Three character mnemonic for the month. This value is case insensitive.
- **yyyy** - Year (four digits are required).
- **hh** - Hour in 24 hour time notation. The leading 0 is optional.
- **mm** - Minutes. The leading 0 is optional.
- **ss** - Seconds. The leading 0 is optional.

**Syntax Notes**

- You can use the **yesterday** and **today** keywords as alternatives to the date parameter. You can use these with or without time values.
- The 'to' value is optional. If not specified, SmartLog shows all values on the specified 'from' value.
- The time value is optional. If no time is specified, SmartLog shows all records from 00:00 to 23:59 on the specified date.
- If you specify a time value, you must specify the hours and minutes. You can ignore the second values.
- The day and year values are optional. If you do not specify these values the most recent day and/or year is assumed.
- You can ignore the date value. Today is assumed.
- You must always specify the month value.
- You cannot use wildcards with dates and times.

Examples
- 1/mar/2012-5/mar/2012 - Shows all logs on and between these dates.
- 5/mar/2012 - Shows all logs for 5 March only.
- yesterday-today - Shows all logs from 00:00 yesterday to 23:59 today.
- 5/mar/2012 07:00-08:59 - Shows all logs from 7:00 on 5 March to 8:59 today. This example illustrates the fact that you can ignore the date value. Today is assumed.