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=22931
For additional technical information, visit the Check Point Support Center (http://supportcenter.checkpoint.com).
For more about this release, see the R76 home page (http://supportcontent.checkpoint.com/solutions?id=sk91140).

Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>10 February 2013</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 R76 Administration Guide).
# Contents

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Important Information</strong></td>
<td>3</td>
</tr>
<tr>
<td><strong>Introduction</strong></td>
<td>5</td>
</tr>
<tr>
<td>Activating the SmartLog Index Server</td>
<td>5</td>
</tr>
<tr>
<td>Activating SmartLog on Multi-Domain Security Management</td>
<td>5</td>
</tr>
<tr>
<td>SmartLog User Interface</td>
<td>6</td>
</tr>
<tr>
<td>Working with More than One Log Server</td>
<td>7</td>
</tr>
<tr>
<td>Minimum Disk Space</td>
<td>7</td>
</tr>
<tr>
<td><strong>Working with Queries</strong></td>
<td>9</td>
</tr>
<tr>
<td>Running Queries</td>
<td>9</td>
</tr>
<tr>
<td>Working with the Favorites List</td>
<td>9</td>
</tr>
<tr>
<td>Adding a Query to the Favorites List</td>
<td>10</td>
</tr>
<tr>
<td>Creating a New Folder</td>
<td>10</td>
</tr>
<tr>
<td>Deleting a Folder</td>
<td>10</td>
</tr>
<tr>
<td>Working with the Results Pane</td>
<td>10</td>
</tr>
<tr>
<td>Showing Query Results</td>
<td>11</td>
</tr>
<tr>
<td>Customizing the Results Pane</td>
<td>11</td>
</tr>
<tr>
<td>Exporting Query Results</td>
<td>11</td>
</tr>
<tr>
<td>Creating Custom Queries</td>
<td>12</td>
</tr>
<tr>
<td>Selecting Query Fields</td>
<td>12</td>
</tr>
<tr>
<td>Selecting Criteria from Grid Columns</td>
<td>12</td>
</tr>
<tr>
<td>Manually Entering Query Criteria</td>
<td>12</td>
</tr>
<tr>
<td><strong>Query Syntax</strong></td>
<td>13</td>
</tr>
<tr>
<td>Query Language Overview</td>
<td>13</td>
</tr>
<tr>
<td>Criteria Values</td>
<td>13</td>
</tr>
<tr>
<td>IP Addresses</td>
<td>14</td>
</tr>
<tr>
<td>IP Address Ranges</td>
<td>14</td>
</tr>
<tr>
<td>Numeric Ranges</td>
<td>14</td>
</tr>
<tr>
<td>Null Values</td>
<td>14</td>
</tr>
<tr>
<td>Wildcards</td>
<td>14</td>
</tr>
<tr>
<td>Using Wildcards with IP Addresses</td>
<td>15</td>
</tr>
<tr>
<td>Field Keywords</td>
<td>15</td>
</tr>
<tr>
<td>Boolean Operators</td>
<td>16</td>
</tr>
<tr>
<td>Date and Time Ranges</td>
<td>16</td>
</tr>
<tr>
<td>Preceding Time Period Queries</td>
<td>17</td>
</tr>
<tr>
<td>From-To Queries</td>
<td>17</td>
</tr>
<tr>
<td><strong>Index</strong></td>
<td>19</td>
</tr>
</tbody>
</table>
Chapter 1

Introduction

In This Chapter

- Activating the SmartLog Index Server 5
- Activating SmartLog on Multi-Domain Security Management 5
- SmartLog User Interface 6
- Working with More than One Log Server 7
- Minimum Disk Space 7

SmartLog reads and indexes logs generated by Check Point and OPSEC products. You can use this data to:

- Detect and monitor security-related events. For example: alerts, rejected connections, and failed authentication attempts can indicate intrusion attempts.
- Collect data on problematic issues. For example: a client is authorized to create a connection, but cannot connect. SmartLog shows that the Rule Base incorrectly blocks the client connection attempts.
- Analyze network traffic patterns. For example: find out how many HTTP services were used during peak activity.

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 log servers and indexes them for rapid data extraction. SmartLog includes a powerful query language that lets you create your own queries in minutes.

SmartLog is part of the R76 SmartConsole installation.

Activating the SmartLog Index Server

The SmartLog Index Server contains a central index to log entries and all SmartLog enabled management and log servers.

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 the Menu icon > Policy > Install Database.

Activating SmartLog on Multi-Domain Security Management

SmartLog in a Multi-Domain Security Management environment works on the Multi-Domain Server. This server is used to query results from the Domain Management Servers and Multi-Domain Log Servers.

SmartLog on the Multi-Domain Server is active by default. Each Domain Management Server and Multi-Domain Log Server can be activated separately.

To activate SmartLog on the Multi-Domain Security Management:
1. Open the SmartDomain Manager > General Multi-Domain Server Contents.
2. Right-click the Domain Management Server and select Launch Application > SmartDashboard.
3. In the properties of the Domain Management Server object > Logs, select Enable SmartLog. Do this also for the Multi-Domain Log Servers objects.

4. Click OK and then Save.

5. In the SmartDomain Manager > General Multi-Domain Server Contents, double-click the Multi-Domain Server object.

6. Select Enable SmartLog.

7. Click OK.

8. Start the SmartLog console.

SmartLog can be used to access the Domain Management Servers or Multi-Domain Log Servers directly, or through the Multi-Domain Server.

When you connect through the Multi-Domain Server, on the left pane, SmartLog shows the Domain Management Servers and Multi-Domain Log Servers that you can select as query targets. The results are a collection of logs from the selected Domain Management Servers and Multi-Domain Log Servers (that match the query).

**SmartLog User Interface**

- **Favorites** - Shows list of predefined queries. Select a query in this list to run it.

- **Back/Forward** - Scroll backward and forward between recent queries.

- **Log pane toolbar** - 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.

- **Query Definition field** - 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.

- **Top Results pane** - Shows the top results of the most recent query.

- **Results pane** - Shows the log entries for the most recent query.
### Working with More than One Log Server

You can include log records from more than one log server in your SmartLog queries. The only restriction is that the log servers must all be managed by the same Security Management Server or Multi-Domain Server. When enabled, SmartLog automatically indexes logs on all applicable log servers. The Top Results pane is not available when working with more than one log server.

**To see logs from more than one log server:**
1. Select View > Log servers connection.
2. In the Log Servers Connection window, select Multiple Log Servers.
3. Click OK.
4. On the Log Servers pane, select the log servers to include in your queries. By default, all servers are selected.

If you have many log servers with large log files, it may take a long time to index the servers. Please be patient. The Top Results pane does not show.

**To see logs from only the connected log server:**
1. Select View > Log servers connection.
2. In the Log Servers Connection window, select Single Log Server.
3. Click OK.

The Top Results pane shows in the user interface.

### Minimum Disk Space

SmartLog creates and uses index files for fast access to log file contents. The index files are located by default at `$SMARTLOGDIR/data`.

To make sure that there is always sufficient disk space on the server, SmartLog deletes the oldest index entries when the available disk space is less than a specified minimum. The default minimum value is 10,240 MB.
To change the minimum available disk space value:

1. On the SmartLog index server command line, go to $SMARTLOGDIR.
2. Open smartlog_settings.txt in a text editor.
3. Add this line to the section:
   
   :min_disk_space (space), where space = the minimum available disk space in MB.
   
   The default value is 10240 MB, which is in effect when there is no :min_disk_space line in the smartlog_settings.txt file. A smaller number will let the index file contain more entries before it automatically deletes the oldest records.
Chapter 2

Working with Queries

In This Chapter

- Running Queries 9
- Working with the Favorites List 9
- Working with the Results Pane 10
- Creating Custom Queries 12

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.

Running Queries

You can run a SmartLog an existing query or create a custom query ("Creating Custom Queries" on page 12).

To run a query:
- Click Favorites and select a predefined or custom query.
  Or
- Click in the Query Definition field and select a recent query.

To create and run a query:
1. Click in the Query Definition field.
2. Enter or select query criteria.
   The query runs automatically. As you add more criteria, results are updated dynamically.

To manually refresh your query:

Click the Refresh icon.

To continuously refresh your query (Auto-Refresh):

Click Auto-Refresh icon. The icon is highlighted when you enable Auto-Refresh.

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

To stop refreshing your query:

Click Auto-Refresh icon. The icon is not highlighted when you deactivate Auto-Refresh.

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**

You can control how the data shows on in the results.

- Select **Grid View**. This shows log records in a detailed tabular view. You can select the fields that show and change the column order and width.
- Select **Table View**. This shows a short summary of basic log data. You cannot customize this view.
- Show resolved IP addresses and service names.
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.

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 number of results shows above the Results pane.

For example, on the first run of a query, you can see:

*Showing first 50 results (128 ms), out of over 150,000 results*

After you scroll down, you see:

*Showing first 100 results (128 ms), out of over 150,000 results*

**Customizing the Results Pane**

By default, SmartLog shows a predefined set of columns and information based on the selected blade in your query. This is known as the **Column Profile**. If no blade is specified, a column profile is assigned based on the blade that occurs most frequently in the query results.

The Column Profile defines which columns appear in the Results Pane and in which order. You can change the Column Profile as necessary for your environment. You can sort the results by the actual event date and time or by the time that the event index arrived to the SmartLog Server.

To use the default Column Profile assignments, right-click a column heading and select **Columns Profile > Automatic Profile Selection**. This option is enabled by default.

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 Columns Profile**.
2. In the **Show Fields** window, select a Column Profile to change.
3. Select fields to add from the **Available Fields** column and click **Add**.
4. Select fields to remove from the **Selected Fields** column and click **Remove**.
5. Select a field in the **Selected Fields** and then click **Move Up** or **Move Down** to change its position in the Results Pane.
6. Double-click the Width column to change the default column width for the selected field.

**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, remove query definitions: click Clear.
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.

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 13
- Criteria Values 13
- Wildcards 14
- Field Keywords 15
- Boolean Operators 16
- Date and Time Ranges 16

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 \([\text{<Field>:}] \ <\text{Filter Criterion}>\).

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

\([\text{<Field>:}] \ <\text{Filter Criterion}> \ \text{AND|OR|NOT} \ [\text{<Field>:}] \ <\text{Filter Criterion}> \ ...\)

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
- 192.0.2.1
- 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 SmartLog queries are counted as one word. You can enter IPv4 address using dotted decimal or CIDR notation. IPv6 addresses are typically entered using CIDR notation.
You can also use the ‘*’ wildcard character with IPv6 addresses.
Examples:
- 20.20.20.1  
- 10.0.0.0/24  
- 2001:0db8::61:1/32  
- 2001:0db8::*

**IP Address Ranges**
You can use IPv4 and IPv6 address ranges in free text queries or with the source and destination fields. 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:
- 192.0.2.0-192.0.2.255  
- 2001:0db8::64:1-2001:0db8::64:199

**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

**Null Values**
You can use null (empty) values with field keywords (on page 15) in SmartLog queries with one of these syntax options:
- `<field> ""`  
- `<field> []`
You can also use the Boolean NOT operator to return fields that are not null:
- NOT `<field> ""`  
- NOT `<field> []`

Null value queries only work with fields contained in the field keywords (on page 15) table.

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

- The `?` (question mark) matches one character.
- 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*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:**

- `192.0.2.*` shows all records for 192.0.2.0 to 192.0.2.255 inclusive
- `192.0.*` shows all records for 192.0.0.0 to 192.0.255.255 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:192.0.2.1`
- `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.
- `192.0.2.133 10.19.136.101` - Includes log entries that match the two IP addresses. The AND operator is presumed.
- `192.0.2.133 OR 10.19.136.101` - Includes log entries that match one of the IP addresses.
- `(blade:Firewall or blade:IPS or blade:VPN) AND NOT action:drop` - Includes all log entries from the Firewall, IPS or VPN blades that are not dropped. The criteria in the parentheses are applied before the AND NOT criterion.
- `Source:(192.0.2.1 OR 192.0.2.2) AND destination:17.168.8.2` - Includes log entries from the two source IP addresses if the destination IP address is 17.168.8.2. This example also shows how you can use Boolean operators with field criteria.

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:

\texttt{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**

- \texttt{last 12 hours} - Shows logs generated during the last 12 hours.
- \texttt{past 10 week} - Shows logs generated during the last 10 weeks. Using the singular is permitted.
- \texttt{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 \texttt{last} or \texttt{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:

\texttt{last\|past\ [<number>]\ <period\ of\ time>}

**Examples**

- \texttt{last 12 hours} - Shows logs generated during the last 12 hours before the most recent time.
- \texttt{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.
- \texttt{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 \texttt{<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**

\texttt{dd/mmm/yyyy hh:mm:ss[-dd/mmm/yyyy hh:mm:ss]}

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

A
Activating SmartLog on Multi-Domain Security Management • 5
Activating the SmartLog Index Server • 5
Adding a Query to the Favorites List • 10

B
Boolean Operators • 16

C
Creating a New Folder • 10
Creating Custom Queries • 12
Criteria Values • 13
Customizing the Results Pane • 11

D
Date and Time Ranges • 16
Deleting a Folder • 10

E
Exporting Query Results • 11

F
Field Keywords • 15
From-To Queries • 17

I
Important Information • 3
Introduction • 5
IP Address Ranges • 14
IP Addresses • 14

M
Manually Entering Query Criteria • 12
Minimum Disk Space • 7

N
Null Values • 14
Numeric Ranges • 14

P
Preceding Time Period Queries • 17

Q
Query Language Overview • 13
Query Syntax • 13

R
Running Queries • 9

S
Selecting Criteria from Grid Columns • 12
Selecting Query Fields • 12
Showing Query Results • 11
SmartLog User Interface • 6

U
Using Wildcards with IP Addresses • 15

W
Wildcards • 14
Working with More than One Log Server • 7
Working with Queries • 9
Working with the Favorites List • 9
Working with the Results Pane • 10