TIBCO LogLogic®

Security Event Manager (SEM)

Reference Guide

Software Release: 3.6.0

March 2013

Two-Second Advantage®

TIBCO®

Important Information

Contents

Chapter 5 - Configuration Menu 107

List of Figures

List of Tables

Preface

The Reference Guide contains information essential to the user when implementing and monitoring alerts and events with the Web Console.

Audience

This guide is intended for:

- Security Analysts who are responsible for network security.
- Security Network Administrators who are responsible for installing and maintaining network security software.

Related Documentation

Table 1 Related Documentation

Documentation	Content
Administration Guide	This guide explains how to configure the various functions of the Security Event Manager in an advanced manner.
Concepts Guide	This guide gives an overview of: ▪ Regulatory Compliance through its three underlying domains: regulation, standards and technical reporting. ▪ TIBCO LogLogic®'s Taxonomy. ▪ How logs are converted into user-oriented messages. ▪ Correlation in TIBCO LogLogic®. ▪ Encryption of logs in TIBCO LogLogic®.
Log Collector Installation Guide	This guide explains how to install and configure the Log Collector software on both Windows and Linux/ Unix O.S.
SMP Installation Guide	This guide explains how to install and configure the Security Management Platform.
User Guide	This User Guide explains how to use and configure the various functions and modules provided in the Web Console application.

Technical Support Information

TIBCO LogLogic® is committed to the success of our customers and to ensuring our products improve customers' ability to maintain secure, reliable networks. Although TIBCO LogLogic® products are easy to use and maintain, occasional assistance might be necessary.

TIBCO LogLogic® provides timely and comprehensive customer support and technical assistance from highly knowledgeable, experienced engineers who can help you maximize the performance of your TIBCO LogLogic® Compliance Suites.

To reach TIBCO LogLogic® Customer Support:

Telephone: Toll Free—1-800-957-LOGS

Local—1-408-834-7480

EMEA— +44 1480 479391

Email: ll-support@tibco.com

You can also visit the **TIBCO LogLogic®** Support website at:
https://support.tibco.com/esupport/loglogic.htm

When contacting the support, be prepared to provide the following information:

- Your name, email address, phone number, and fax number
- Your company name and company address
- Your machine type and release version
- A description of the problem and the content of pertinent error messages (if any)

Documentation Support Information

The TIBCO LogLogic® documentation includes Portable Document Format (PDF) files. To read the PDF documentation, you need a PDF file viewer such as Adobe Acrobat Reader. You can download the Adobe Acrobat Reader at http://www.adobe.com.

Contact Information

Your feedback on the TIBCO LogLogic® documentation is important to us. If you have questions or comments, send email to DocComments@loglogic.com. In your email message, please indicate the software name and version you are using, as well as the title and document release date of your documentation. Your comments will be reviewed and addressed by the TIBCO LogLogic® Technical Publications team.

Conventions

The TIBCO LogLogic® documentation uses the following conventions to distinguish text and information that might require special attention.

Caution: Highlights important situations that could potentially damage data or cause system failure.

IMPORTANT! Highlights key considerations to keep in mind.

Note: Provides additional information that is useful but not always essential or highlights guidelines and helpful hints.

This guide also uses the following typographic conventions to highlight code and command line elements:

- `Monospace` is used for programming elements (such as code fragments, objects, methods, parameters, and HTML tags) and system elements (such as file names, directories, paths, and URLs).
- **`Monospace bold`** is used to distinguish system prompts or screen output from user responses, as in this example:

```
username: system
```

```
home directory: home\app
```

- *`Monospace italic`* is used for placeholders, which are general names that you replace with names specific to your site, as in this example:

```
LogLogic_home_directory\upgrade\
```

- Straight brackets signal options in command line syntax.

```
ls [-AabCcdFfgiLlmnopqRrstux1] [-X attr] [path ...]
```

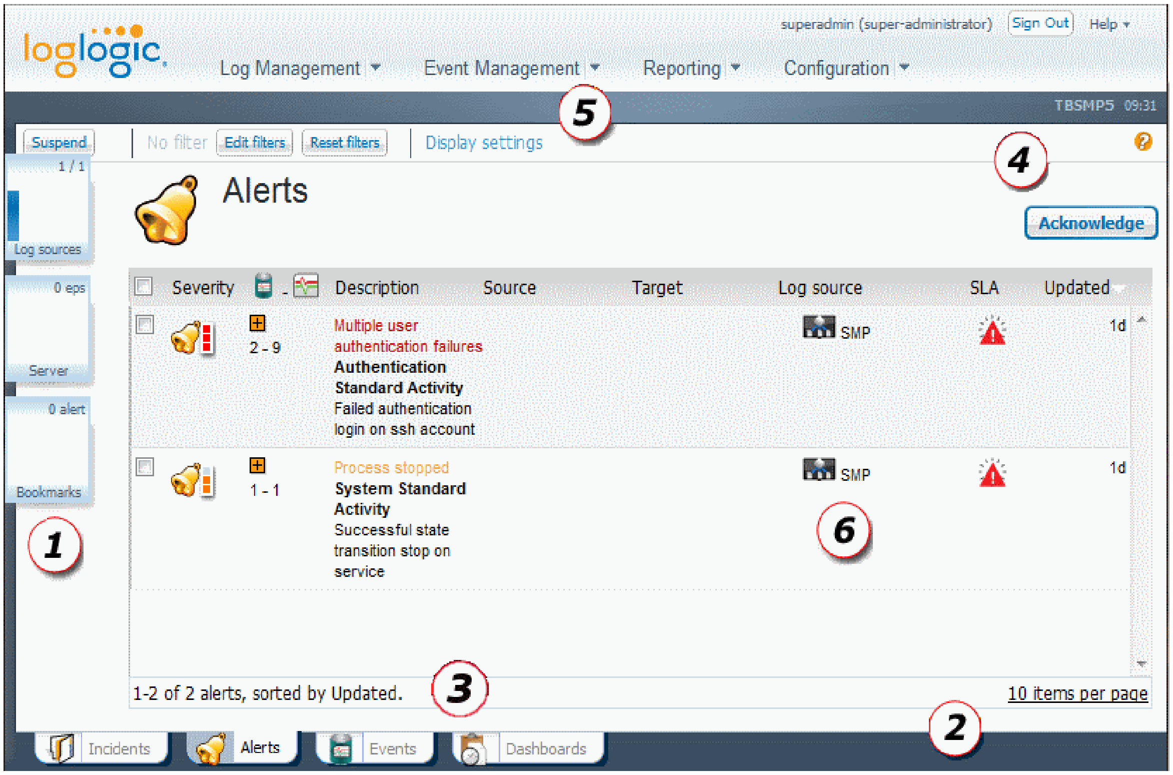
Chapter 1 - Workspace Overview

The Security Event Manager workspace or “monitoring screen” is the main screen typically used by security analysts or displayed on a large screen in a Security Operations Centre. You access the screen as soon as you log in. You can monitor data by incidents, alerts and events.

The workspace consists of the following main components:

- Sticky Pane (1)
- Tabs (2)
- Status Bar (3)
- Menu Bar and Acknowledge Button (4)
- Action Bar and Session Information (5)
- Filters and Tabs (5)
- Contents (6)

Figure 1 Main Screen



☐	Severity		Description	Source	Target	Log source	SLA	Updated
☐		2 - 9	Multiple user authentication failures **Authentication Standard Activity** Failed authentication login on ssh account			SMP		1d
☐		1 - 1	Process stopped **System Standard Activity** Successful state transition stop on service			SMP		1d

Sticky Pane

The sticky pane is located in the left-hand side of the screen. It is composed of thumbnails that give you a general overview of the current server activity.

Figure 2 Sticky Pane

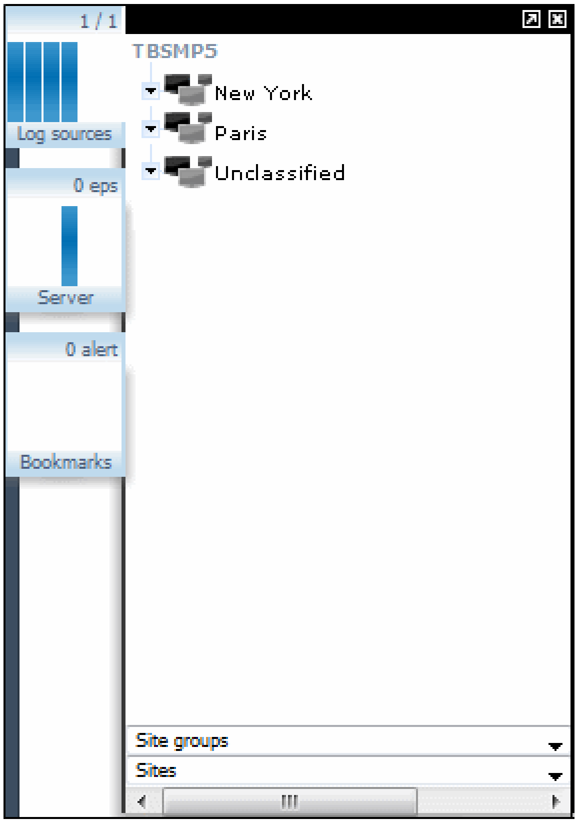
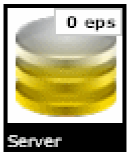
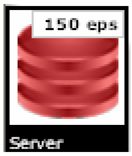


Table 2 Sticky Pane Thumbnails

Thumbnail	**Description**
Log Sources	Displays the percentage of currently connected log sources along with bar charts showing the connected log sources tendency in the last hour. A bar chart is equal to 10 mn.
Server	Displays the EPS flow and the elementary events that are coming to the SMP. Two indicators are sometimes displayed: If the database is almost full (80%):  If the database is full: 
Bookmarks	Displays the number of alerts waiting to be displayed in the last hour, along with bar charts showing the tendency of alerts waiting to be displayed. A bar chart is equal to 10 mn.

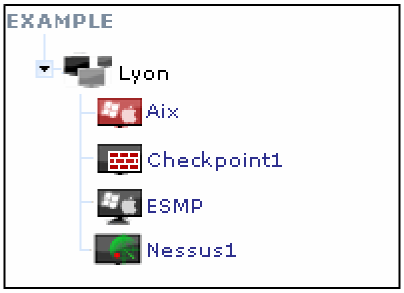
If you click on the thumbnails, you can display the following modules:

- "Log Sources List"
- "SMP Monitoring"
- "Summary Zone"

Note: To close a pane, click on the black cross at the top right-hand side of the sticky pane.
To disconnect a pane from the main interface, click on the black arrow at the top right-hand side of the sticky pane.

Log Sources List

The connection status of each supported product is shown in a hierarchical structure, grouped by site name.



Here is the list and description of the log source icons. Their display depends from the selected **Type** when editing a Log Source.

Table 3 Log Source Icons

Icons	Description
✚	Antivirus/spyware/spam
	Authentication server
$	Business application
	Centralized management
	Database services
	Directory services
DNS	Domain Name System (DNS)
	File server
	Honeypot
	▪ Database IDS ▪ Host IDS ▪ Network IDS

Table 3 Log Source Icons

Icons	Description
	Log management
✉	Messaging services
	Network device
	Operating System
PROXY	Proxy
	Remote desktop
	Unified Threat Management
	Virtualization
	Vulnerability Scanner
WEB	Web server
	Unknown
	The Log Source has not been sending heartbeat for at least 2 minutes. However, it does not mean that the Log Collector was disconnected. A connected Log Collector whose Log Source is displayed with a red cross can mean that a Log Collector is blocked or that a software crash happens. **Note:** A virtual Log Source cannot send heartbeat so it will not appear with a red cross.

The drop-down lists allow you to organize the hierarchical view of the log sources shown above. Log sources can be grouped by either:

- Top drop-down list: Sites, Organizational Unit (OU) or Site Groups

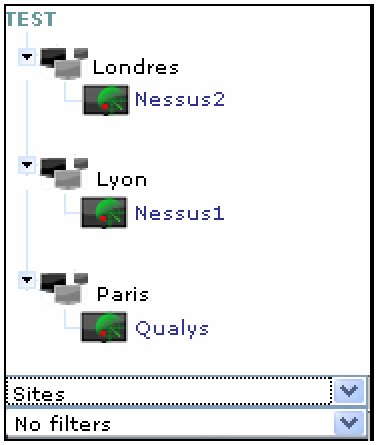
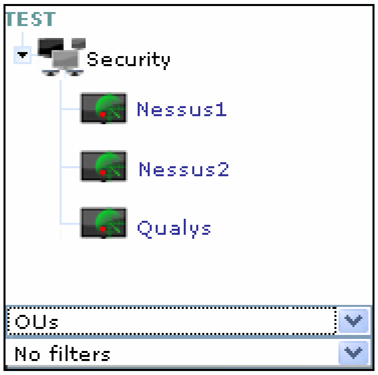
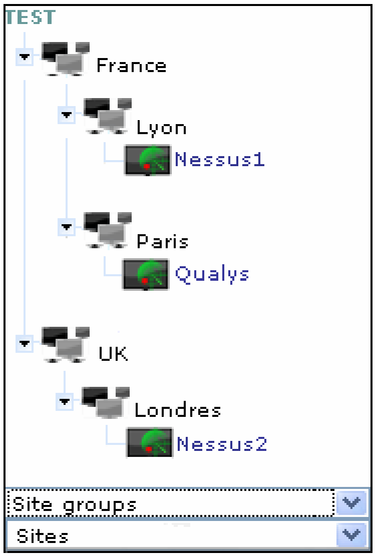
or

- Bottom drop-down list: Log source type, Organisational Unit or Site.

Examples of log source organization using the drop-down lists

For example, if you had these log source types:

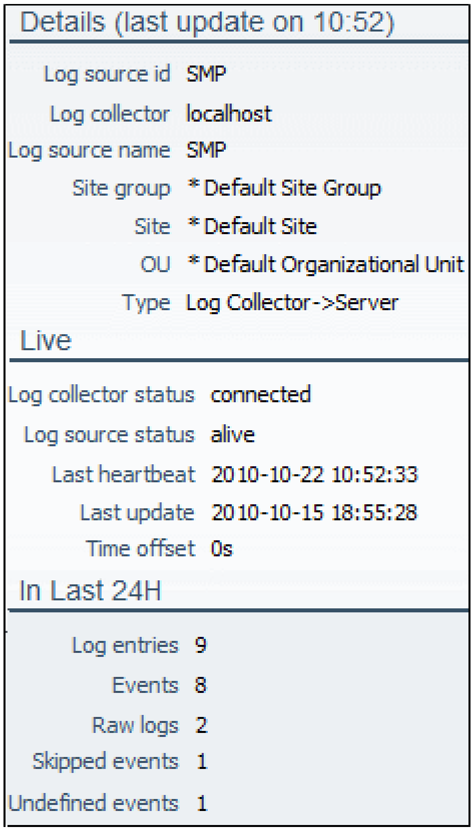
- Nessus1
  Site Group: France, **Site**: Lyon, **OU**: Security, **Log Source type**: scanner
- Nessus2
  Site Group: UK, **Site**: London, **OU**: Security, **Log Source type**: scanner
- Qualys
  Site Group: France, **Site**: Paris, **OU**: Security, **Log Source type**: scanner

Cases	Example
1st case: If you had selected Site in the first drop-down list and No Filters in the second list, you would see.	 TEST Londres Nessus2 Lyon Nessus1 Paris Qualys Sites No filters
2nd case: If you had selected **OUs** in the first drop-down list and **No Filters** in the second list, you would see.	 TEST Security Nessus1 Nessus2 Qualys OUs No filters
3rd case: If you had selected **Site Groups** in the first drop-down list and **Sites** in the second list, you would see.	 TEST France Lyon Nessus1 Paris Qualys UK Londres Nessus2 Site groups Sites

Log Source Information

When you click on a log source's name, the following screen is displayed:

Figure 3 Details screen



Details (last update on 10:52)

Log source id SMP
Log collector localhost
Log source name SMP
Site group * Default Site Group
Site * Default Site
OU * Default Organizational Unit
Type Log Collector->Server

Live

Log collector status connected
Log source status alive
Last heartbeat 2010-10-22 10:52:33
Last update 2010-10-15 18:55:28
Time offset 0s

In Last 24H

Log entries 9
Events 8
Raw logs 2
Skipped events 1
Undefined events 1

Note: If you clicked on a virtual log source's name (i.e. a log source from which events are emitted instead of the log source you configured), the screen varies a bit as explained in the table below.

Table 4 Log Source Information

Details	**Description**
Details (Last update on hh:mm)	
Log Source Id	Log Source name.
Log collector	Name of the Log Collector that communicates with the log source.
Log Source Name	Analyzer ID (same as log source name).
Site group	Group to which the log source site belongs.
Site	Site to which the log source belongs.
OU	Organisational Unit to which the log source belongs.
Type	Log source type.
Live	
Log Collector status	Indicates whether the Log Collector is connected.
Log Source status	Indicates whether the log source (or equipment) is currently sending heartbeat.
Last heart beat	Time and date when the last heartbeat was sent by the log source.
Last update	Time and date when the Log Collector has been updated.
Time offset	Offset between the SMP and the Log Collector.

Table 4 Log Source Information

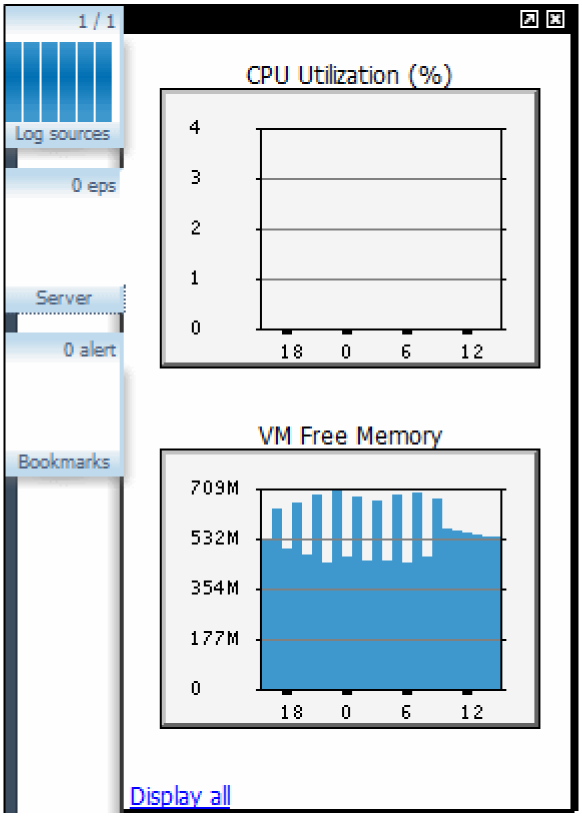
Details	Description
[Virtual Log Source only] Logs collected via log source	Name of the log source through which events collected by the virtual log source pass.
In Last 24H	
Log entries	How many log entries were received by the Log Collector in the last 24 hours.
Events	How many events were sent by the Log Collector in the last 24 hours.
Raw logs	How many raw logs were sent by the Log Collector in the last 24 hours.
Events skipped in last 24H	How many events were skipped by the Log Collector in the last 24 hours.
Undefined events in last 24H	How many events were not recognized by the Log Collector in the last 24 hours.

SMP Monitoring

The SMP Monitoring screen allows you to monitor the activities of the SMP server.

You can access it by clicking on the **Display more figure for the system** link.

Figure 4 Live Explorer link



By default, the **Live Explorer** tab is displayed. For more information, refer to the SMP Monitoring section.

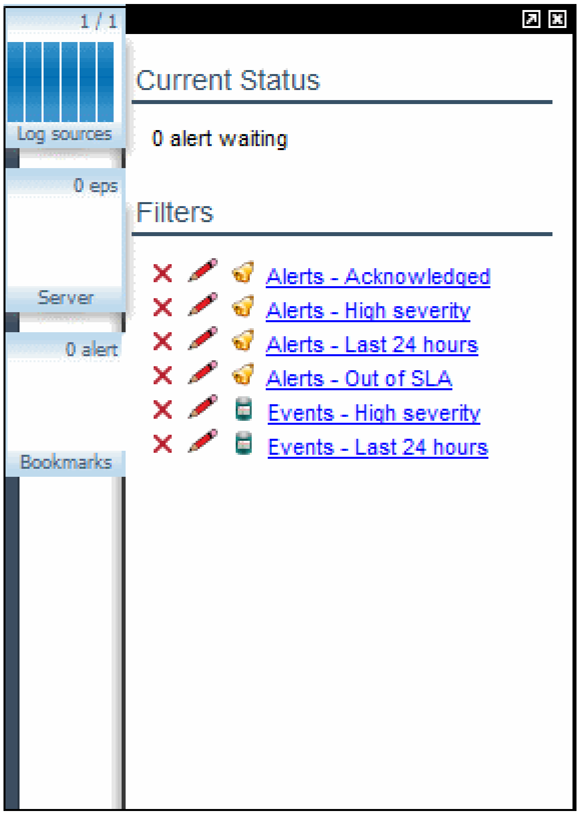
Summary Zone

The Summary Zone displays a summary for the alert activities in the last five hours, along with bar charts indicating the number of alerts generated in the last hour. Hover the mouse pointer over the bar chart to see the actual figure as well as the percentage comparing that hour to the previous 24.

The Summary Zone is used to get an immediate picture of trends in alert activity - whether alerts are currently increasing or decreasing.

It contains a list of default filters as well as the list of filters you have saved. Refer to the Use of Filters section in the User Guide.

Figure 5 List of filters



Current Status

0 alert waiting

Filters

- Alerts - Acknowledged
- Alerts - High severity
- Alerts - Last 24 hours
- Alerts - Out of SLA
- Events - High severity
- Events - Last 24 hours

Description

Table 5 Default Filters

Name	Description
Alerts - Acknowledged	Displays acknowledged alerts only.
Alerts - High severity	Displays alerts with a high severity only.
Alerts - Last 24 hours	Displays alerts generated in the last 24 hours only.
Alerts - Out of SLA	Displays alerts that should have been acknowledged within SLA limits.
Events - High severity	Displays events with a high severity only.
Events - Last 24 hours	Displays events generated in the last 24 hours only.

Tabs

At the bottom of the display, the status tabs allow you to switch rapidly from one view to the other, for example from the Alerts view to the Events view. To do so, you just have to click on the required tab.

Refer the Use of Tabs section in the ***User Guide*** to know how to manage tabs.

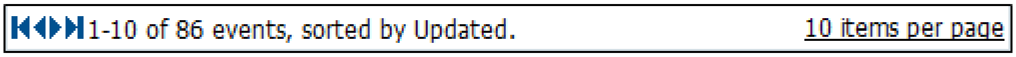
Table 6 Tabs

Menu	**Description**
Incidents	Allows you to view and manage incidents. See the *"**Incidents**"* sub-section in the user Guide for further information.
Alerts	Allows you to view and manage alerts. See the *"**Alerts**"* sub-section in the user Guide for further information.
Events	Allows you to view and manage events. See the *"**Events**"* sub-section in the user Guide for further information.
Dashboards	To produce graphical dashboards, reports and exports. See the *"**Security Dashboards**"* sub-section in the user Guide for further information.

Status Bar

The status allows you to browse through events, alerts and incidents. For example, to view older or newer alerts on the display, use the forward and back browsing buttons.

Figure 6 Status Bar



1-10 of 86 events, sorted by Updated.

The four buttons (from left to right) enable you to:

- view the newest alerts page
- view the previous alerts page
- view the next alerts page
- view the last alerts page

It also indicates the type of sorting order you defined. The status bar also allows you display a given number of elements in the list.

Menu Bar and Acknowledge Button

Menu Bar

Other components of the Web Console are available from the menu bar at the top-right of the display.

Table 7 Menu Bar

Menu	Description
Log Management	This menu allows you to access the internal log source and archives management.
Event Management	This menu allows you to access the main monitoring screens, create incidents or alerts and create aggregation and correlation policies.
Reporting	This menu allows you to access the reporting interface and Live and Batch reporting policies.
Configuration	This menu allows you to access configuration options such as configuring user accounts or backups.
Help	This menu allows you to access the standard help information: the online help, the About screen (containing a brief list of credits, information about system properties and connected users), our Support Center, the TIBCO LogLogic® website. You can also send an instant message to all connected users.
🏃▶	This icon allows you to log out from the application.

Acknowledge Button

The **Acknowledge button** allows you to activate - once the alert is selected - the **Acknowledge** screen where you will be able to acknowledge or attach an alert to an incident. This button is not available in the **Events** view.

Action Bar and Session Information

Action Bar

In the action bar, various elements are available.

Figure 7 Action Bar

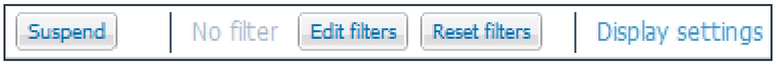


Table 8 Action Bar

Button	Description
Suspend button	Allows you to stop the automatic refresh of the display. However, this does not stop the alert or event generation.
Text displayed near the **Suspend** button (**No filter** in the above example)	Indicates whether a filter is applied to the current view or not. See section "Filters and Tabs" below.
Edit filters button	Allows you to create a filter and activate it. See the following section for more information.

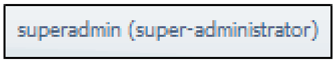
Table 8 Action Bar

Button	Description
Reset filters button	Allows you to remove the filter applied and display the list by default.
Display settings button	Displays the **Display Settings** pane where you define the alert’s display format, either: - date format: hour and day, hour only or elapsed time - type of date: detection, creation, last update or SLA expiration. This action is also possible by right clicking on the far right black header. See chapter "View Alerts" for more information.

Session Information

Four main types of information are displayed:

- The current logged-in user.
- The user right (in brackets).
- The name of the instance.
- The hour of the server.

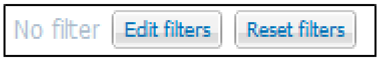


Click the user name if you want to edit the user properties and to change the password (refer to the "Add/Edit Users" for section in the User Guide.

Filters and Tabs

Events, alerts and incidents can be filtered. This tool allows you to display only the events, alerts or incidents you want to monitor. By doing so, you will gain time, performance and readability.

Detailed filters can be created via the menu bar.



This chapter aims at providing basic background information and common use of filters and tabs in the Web Console. You will thus find information about the:

- Filters and Tabs
- Tabs

Use of Filters

The use of filters will be explained through simple examples.

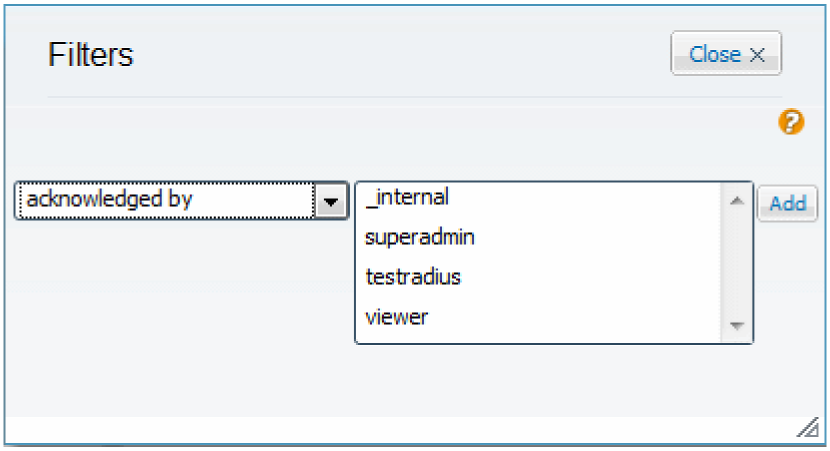
Creating a Filter

Let us suppose you want to display only the alerts that have been acknowledged by the user with the super-administrator account. To do so:

1. Click on the **Edit** button.

The **Filters** screen is displayed.

Figure 8 Filters



2. Click on the **Select a Field** drop-down list and select **Acknowledged by**. A list of users is displayed.

3. Select the **superadmin** user in the list and click on the **Add** button.

4. Close the screen. The filter is automatically displayed.

5. Repeat the operation to add as many other filters as you need.

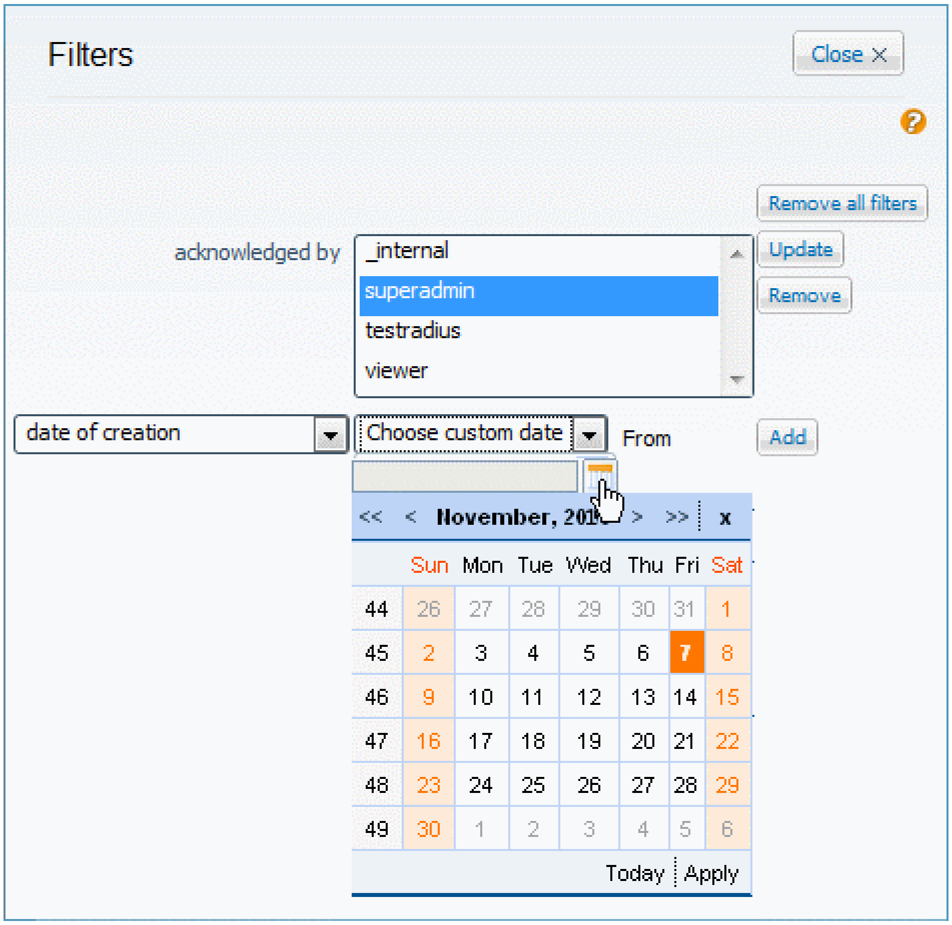
In the **Filters** menu bar, you can see that “1 filter” is displayed meaning it has been created.

However, the filter has not been saved, which means that the filter is only available for the current view and will not be active if you close the application.

Saving the view will allow you to display the filtered view each time you connect to the Web Console.

You can add as many filters as you want at the same time and then create a group composed of several combined filters.

Figure 9 Two filters are being applied



Examples of Filters Configuration

Dates

1. Set the type of date (e.g. Date of Creation or Detection)

2. Either choose a date specifier from the **Choose Custom Date** drop-down list or enter the date and time range which will be used to selectively restrict the display of alerts:

- The drop-down list provides pre-defined date ranges such as “yesterday”. Common selections are provided in the drop-down list:

– Last 24 hours

– Last 7 days

– Last 30 days

– Yesterday

– Last week

– Last month

– Current month

- The calendar icon provides a graphical method for date entry where you just have to select the date and time (hh:mm format) and validate by clicking **Apply**.

Note: You can also specify day / month / year figures. If required, the time must be specified numerically. If the time is not specified, the entire 24 hour period of the specified date will be used.

---

3. Specify dates and times (hh:mm:yy) for the **From** and **To** fields and click on the cross to activate the filter.

Name

The classification of events is set by the default rule-set. Alerts, however, have their classification set by correlation rules and scenarios. See Correlation Policy for more information on this subject.

The classification filter allows you to select alerts and events which have a given text string in the classification name.

1. Select a text string filter by choosing:

- **Equals**: to specify the exact contents of the field.
- **Begins**: to specify the beginning of the field contents.
- **Ends**: to specify the end of the field contents.
- **Contains**: the field must have this value in it.
- **Regex**: use a MySQL regular expression to specify the contents. Refer to the "MySQL Regular Expressions" section to get the list of the regular expressions.

In order to properly match the alerts, you must understand the difference between the **Equals** and the **Contains** options. The **Equals** option will search for an exact match with the string entered in the field. If there is more than one word entered, the search will be performed using an **OR** logic and a match will be attempted for each word separately. However, if the words are enclosed in quotes, an exact match for the full string of characters will be attempted.

The **Contains** option will also search for each word entered in the field, but it suffices that one word is found in the classification text for the condition to be valid. Analogously, if the string is enclosed in quotes, the full string must be found to be contained in the matching text. See the table with the matching examples below.

Example 1 - Classification text: **root login**

Table 9 Matching Examples - root login

Option	Matching Value	Result
equals	root login	**No match.** The comparisons made are: ***root*** = ***root login***?No. ***login*** = ***root login***?No. The match is attempted by comparing each word in the field separately with the classification text.
equals	“root login”	**Match.** The comparison made is: ***root login*** = ***root login***?Yes. The comparison is made using the full character string, without breaking it up in separate words.
contains	root login	**Match.** The comparison made is: Does ***root login*** contain ***root***?Yes.

Table 9 Matching Examples - root login

Option	Matching Value	Result
contains	"root login"	**Match.** The comparison made is: Does ***root login*** contain ***root login***?Yes.
contains	login root	**Match.** The comparison made is: Does ***root login*** contain ***login***?Yes.
contains	"login root"	**No match.** The comparison made is: Does ***root login*** contain ***login root***?No.

Example 2- Classification text: **SSH remote root login**

Table 10 Matching Examples - SSH remote root login

Option	Matching Value	Result
equals	root login	**No match.** The comparisons made are: ***root*** = ***SSH remote root login***?No. ***login*** = ***SSH remote root login***?No. The match is attempted by comparing each word in the field separately with the classification text.
equals	"root login"	**No match.** The comparison made is: ***root login*** = ***SSH remote root login***?No. The comparison is made using the full character string, without breaking it up in separate words.
contains	root login	**Match.** The comparison made is: Does ***SSH remote root login*** contain ***root***?Yes.
contains	"root login"	**Match.** The comparison made is: Does ***SSH remote root login*** contain ***root login***?Yes.

Table 10 Matching Examples - SSH remote root login

Option	Matching Value	Result
contains	login root	**Match.** The comparison made is: Does ***SSH remote root login*** contain ***login***?Yes.
contains	"login root"	**No match.** The comparison made is: Does ***SSH remote root login*** contain ***login root***?No.

Note: There are other filters which apply to numbers:
* Equals: specifies the exact value in the field
* Greater: the events with a greater value than the contents of the field
* Lower: the events with a lower value than the contents of the field

Note: The filter can be inverted by ticking the **not** check-box.

1. Enter the matching text in the text box.

2. Click on the cross to activate the filter.

Source

You can create a filter based on the following attributes of the source of an event:

- Node Address
- Node Name
- UserId Name
- UserId Number
- Process
- Service Name
- Service Protocol
- Service Port
- Tool Command
- Tool Name
- Webservice URL
- Webservice CGI
- Webservice Arg

Note: Refer to the "Filters and Tabs" section of the Reference Guide for a detailed description of each attribute.

1. For each attribute, a filter method such as **equals** must be selected to specify how the text string is interpreted - e.g., an exact match. Note that the filter can be inverted by clicking the **Not** check-box.

2. Click on the cross to activate the filter.

Target

You can create a filter based on the following attributes of the target of an event. The elements are the same as the Source elements. See the "Source" sub-section for more information.

- File Name
- Node Address
- Node Name
- UserId Name
- UserId Number
- Process
- Service Name
- Service Protocol
- Service Port
- Tool Command
- Tool Name
- Webservice URL
- Webservice CGI: the program name in a URL
- Webservice Arg: the arguments to the program in a URL

Note: Refer to the "Filters and Tabs" section of the Reference Guide for a detailed description of each attribute.

---

1. For each attribute a filter method such as **equals** must be selected to specify how the text string is interpreted - e.g., an exact match. Note that the filter can be inverted by clicking the **Not** check-box.

2. Click on the cross to activate the filter.

Id

1. The **Id** field selects alerts by the unique number given to each alert. Each alert is given a unique number which can be used to select it - the alerts filter offers a choice of **equals**, **greater** or **lower**.

2. Click on the cross to activate the filter.

Log Source

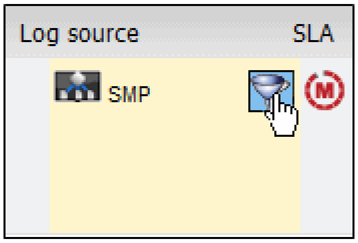
1. Specify the log source; use CTRL-click to select multiple log sources.

2. Click on the cross to activate the filter.

Quick Filters

Filters are used for viewing only a subset of events, alerts or incidents. Quick filters can be set by clicking on the mini filter displayed when dragging your cursor over the item to be filtered.

Example: To only show alerts with the SMP log source, click the quick-filter icon in the Log source column.

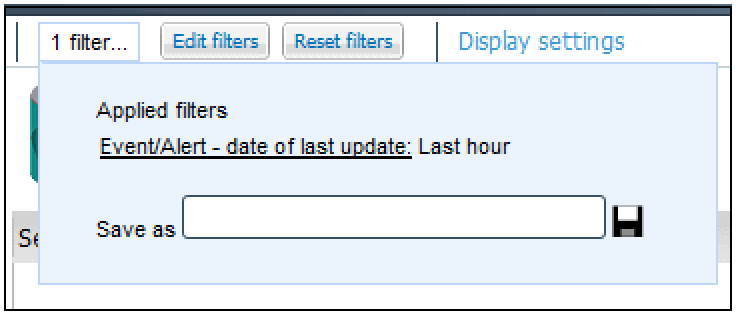


The view then only displays the filtered elements.

Saving a Group of Filters

1. Click on “1 filter”. The following panel is displayed:

Figure 10 Saving a filter



Applied filters

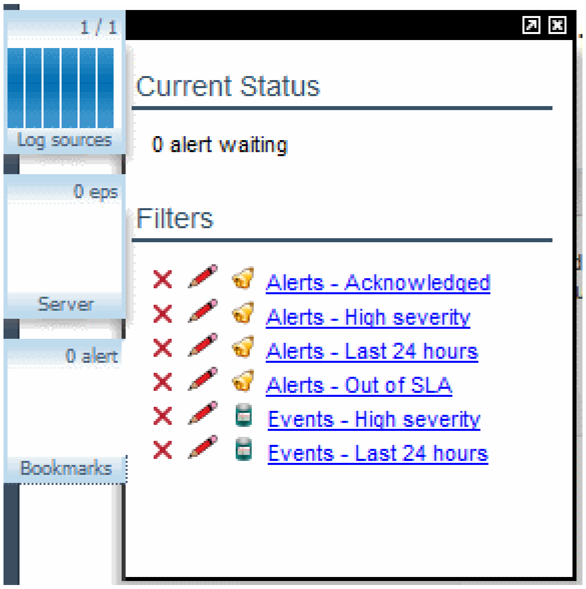
Event/Alert - date of last update: Last hour

Save as

2. Enter a name for the filter and click on the **Save** icon.

3. To see that your filter has correctly been saved, click on the **Bookmarks** thumbnail from the **Sticky Pane**.

Figure 11 The Filter is Saved



0 alert waiting

- Alerts - Acknowledged
- Alerts - High severity
- Alerts - Last 24 hours
- Alerts - Out of SLA
- Events - High severity
- Events - Last 24 hours

As you can see, your filter is available. If you click on it, the interface corresponding to the filtered information is displayed.

Removing a Filter

If you want to remove a filter, you have two possibilities. Either remove a filter from the current view or remove a filter from the list of saved filters.

Removing a Filter or all Filters from the Current View

To remove the filter currently applied, click on the **Reset** button.

The general interface automatically displays the list of alerts or events by default.

Removing a Filter from the List of Saved Filters

To remove the filter saved in the list of saved filters under the **Bookmarks** thumbnail, click on the red cross on the left side of the filter's name.

The general interface automatically displays the list of alerts or events by default.

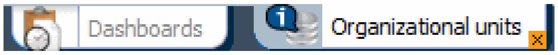
Note: Most criteria on this screen include filters to specify a selection of alerts. A filter comprises text entered in the dialog box and the rule in the drop-down list (equal, contains, begins with, matches a MySQL regular expression or is null). The filter can be negated by ticking the **Not** checkbox, in this case, alerts not matching the filter are displayed. More information on MySQL regular expressions is available in the Appendix in the "MySQL Regular Expressions" section.

Use of Tabs

Refer the *"Tabs"* section in the ***Reference Guide*** to get a description of the various tabs.

Closing a View

Each time you open a screen from a menu, the corresponding tab is displayed near default ones. You can close the newly added tab by clicking on the tab's cross.



Duplicating a View

You can duplicate the alert, event or incident tabs (i.e. a view) in order to compare between the current view and the view you saved. This is useful if you want to have a list of alerts with different filters applied.

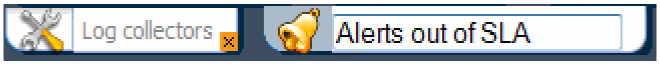
1. Right click on the tab.
2. Select **Duplicate**.

The copy of the tab has been added near the default tabs. Now, it is recommended to rename the tab to differentiate it from the original one.

Renaming a View

You can rename a duplicated tab or a tab that you have just activated via the interface menu.

1. Right click on the tab.
2. Select **Rename** and enter the name you want.



The modification is automatically applied.

Refreshing a View

1. Right click on the tab.
2. Select **Refresh**.

The view data is automatically refreshed. The latest events are displayed.

Caution: DO NOT use the **Refresh** and **Back** button of your web browser. Otherwise, it could generate an error.

Opening a View in a New Window

1. Right click on the tab.
2. Select **Open in a new window**.
   The view is then opened in another window and can be managed as a separate screen, independent from the other views of the interface. This is useful if you want to focus on only one view.
3. Click on the **Close** button to go back to the former view.

List of Filters Available

Filters are described in the table below.

Table 11 Filters List

Name	**Description**
Acknowledgment	
Acknowledged by	Filters the view according to the analyst(s) who acknowledged the alerts; use CTRL-click to select multiple analysts.
Acknowledgment category	Displays the alerts per categories. The category is set when the alert is acknowledged - either manually by the analyst or automatically. The category of alerts can be: ▪ Attack on 3rd Party ▪ Authorized Activity ▪ Authorized Security Testing ▪ Emergency changes ▪ TIBCO LogLogic® Event ▪ False Positive ▪ Known error ▪ Network Noise ▪ True Security Alert ▪ Unauthorized Activity ▪ Unknown
Acknowledgment comment	Displays alerts containing information in their comment. The comment is set when the alert is acknowledged - manually by the analyst or automatically as one of a rule's actions.

Table 11 Filters List

Name	**Description**
Acknowledgment status	Displays alerts according to their acknowledgement status (acknowledged or not).
SLA status	Displays alerts that were generated within SLA limits or not.
Asset Database	
Log Source asset name	Displays the alerts/events generated per asset name.
Log Source host group	Displays the alerts/events generated per host group.
Log Source OU name	Displays the alerts/events generated per Organization Unit.
Log Source site name	Displays the alerts/events generated per log source site (Paris, London...).
Target asset name	Displays the alert per target business asset.
Event/Alert	
Additional data	Displays the event/alert according to additional data. The additional data fields can include items such as rule-set name and logfile name, which can then be filtered. You must use the following format: "my addData meaning=my addData value". E.g. to find authentication alerts, enter "rulesetName=esmp_auth.rules" in the additional data filter.
Date of creation	Displays alerts or events created in a given time period.
Date of detection	Displays alerts or events detected in a given time period.
Date of last update	Displays alerts or events detected since the last update.
Ident	Displays alerts or events according to their Id.
Impact Description	Displays alerts or events that have been caught by a rule which includes an impact description.
Name	Displays alerts or events according to their description (or classification name).
Severity	Displays events/alerts according to the events' severity level. Click the severity levels you want to be displayed. Use CTRL+ click to select multiple levels. High, Info, Low, Medium.
Weight	Displays alerts/events that are composed of a specific number of elementary events.
Log Source	
Log Source name	Displays the alerts/events generated per log source name (IP address, title...).
TIBCO LogLogic® Taxonomy	
Access layer	Displays alerts or events according to the type of events collected (e.g. system malware).
Action	Displays alerts or events according to their main activity (e.g. Trojan).
Action detail	Specify the alert/event's activity in details.

Table 11 Filters List

Name	**Description**
Event Type	Specify the alert/event's event type. The type of event can be: - Attack - Configuration - Information - Malware - Suspicious - Use - Vulnerability
Result	Displays alerts or events according to their status. The status can be Accepted, Active etc.
Target	Displays alerts or events according to the target type the alert refers to (e.g. Account).
Target detail	Displays alerts or events according to the target details the alert refers to.
Source	
Node address	Displays alerts or events according to their node address (e.g. an IP address in dotted decimal format (1.2.3.4) or an email address).
Node name	Displays alerts or events according to their nodename, host name, etc., either DNS name (e.g. www.loglogic.com) or Netbios name (e.g. SERVER1).
Process name	Displays alerts or events according to the process name (e.g. sshd or IEXPLORE.EXE).
Service name	Displays alerts or events according to the name of the service (e.g. SSH).
Service port	Displays alerts or events according to the number of the TCP or UDP port used by the service.
Service protocol	Displays alerts or events according to the protocol being used (e.g. TCP or UDP).
Tool command	Displays alerts or events according to the tool command (e.g. nmap.exe).
Tool name	Displays alerts or events according to: Source: the tool name (e.g. nmap for a network port scanner). Target: the virus name (e.g. eicar).
User name	Displays alerts or events according to the user name (e.g. root or Administrator).
User number	Displays alerts or events according to the user identifier (e.g. 0).
Webservice arg	Displays alerts or events according to the arguments to the program in a URL. For webservers, the arguments passed to a CGI program can be filtered on.
Webservice CGI	Displays alerts or events according to the CGI program name if a CGI program name is included in the URL for webservers.
Webservice URL	Displays alerts or events according to the webservers URL.

Table 11 Filters List

Name	Description
Target (except File Name, all filters are similar to Event - Source)	
File name	Displays events or alerts according to the name of the file or directory (e.g. for alerts involving access failures).

Note: Most criteria on this screen include filters to specify a selection of alerts. A filter comprises text entered in the dialog box and the rule in the drop-down list (equal, contains, begins with, matches a MySQL regular expression or is null). The filter can be negated by ticking the Not checkbox, in this case, alerts not matching the filter are displayed. More information on MySQL regular expressions is available in the Appendix in the "MySQL Regular Expressions" section in the User Guide.

Contents

The main part of the display is used to display lists of incidents, alerts, events or reports in a tabular view and monitor the relevant information.

Chapter 2 - Log Management Menu

The Log Management menu includes the following menu items:

- The Wizard
- Log Collection: Log Sources
- Log Collection: Log Collectors
- Log Collection: Download Log Collector Installation File
- Log Collection: Supported Products
- Log Collection: Advanced: Confsets
- Log Collection: Advanced: Converters
- Log Collection: Advanced: Conversion Rulesets
- Archiving
- Raw Logs Forensic
- Log Collection Policies Menu
- Aggregation Policy

The Wizard

Use the wizard to add and configure a log source in an easy and friendly way.

You can access the wizard by clicking on **Log Management > Add a Log Source** menu entry.

The **Welcome page** is displayed. It lists important information about what you must gather before starting the wizard such as the:

- Log source type (e.g. CheckPoint, Squid...),
- Log source host IP or DNS address,
- Name of the SMP Log Collector that will collect the log,
- Connection parameters to the log source (e.g. installation folder, login, password, domain...).

Characteristics

Description

The characteristics of the wizard screens are described in the following table.

Table 12 The Wizard

Steps	Description
STEP 1. Log Source Settings	Step 1 allows you to define the log source. It can be either a firewall, a proxy, an IDS, a web application, an Operating System, a database... Each log source has a host that needs to be defined. It is essential for communication between the SMP and the log source. Afterwards, you will have to define the kind of events to be collected.
STEP 2. Log Collector Settings	Step 2 allows you to define the Log Collector. The aim of the Log Collector is to collect the events generated by the log source, and then to convert them into a standardized format. The Log Collector then securely transmits this data to the Security Management Platform for further processing. You must specify the host where the Log Collector is installed. You must also indicate the connection type of the Log Collector. Indeed, if the connection is lost for any reason, the SMP will be aware of the problem. In both cases, events are sent immediately by the Log Collector to the SMP.
STEP 3. Connection Settings	Step 3 allows you to enter the necessary connection parameters to allow the Log Collector to connect to the log source. Thanks to these parameters, the Log Collector will be able to retrieve the logs. Parameters can be a folder, a login or a password depending on the selected log source.
STEP 4. Summary	Step 4 gives you a summary of your configuration. Review the details to make sure you have correctly configured your log source and the Log Collector.
STEP 5. Configuration Completed	Step 5 indicates the status of the configuration and if you need to download the Log Collector installer, the Log Collector installation file or the documentation.

Log Collection: Log Sources

Use the log source screen to configure the list of log sources (**Log Management > Log Collection > Log Sources)**.

The log sources list page displays the device being monitored by the SMP. The characteristics of this screen are described in the following table.

Table 13 Log Source List Column

Column	Description
Log Source	The name of the device being monitored, typically the same as the hostname. Click the name to see more details.
Type	The function of the device being monitored. This determines the icon used to represent the device in the real-time monitoring screen, and helps to determine which vulnerabilities may be applicable.
Virtual	A log source is virtual if it is not related to a log source.
Host	The known information about the device, such as names, IP addresses, criticality ratings, existing vulnerabilities. This information is used in conjunction with the configuration settings when correlating and prioritizing alerts. Click the **hostname** to display host details.
Delete	Allows you to delete the log source.

Log Collection: Log Collectors

Use the **Log Collectors** screen to configure local and remote Log Collectors (**Log Management > Log Collection > Log Collectors**).

The characteristics of this screen are described in the following table.

Table 14 Log Collector Configuration Fields

Field	**Description**
Name	The Log Collector's name. Usually it is the hostname of the system where the Log Collector is installed.
Type	The initial connection can be from server-to-Log Collector or Log Collector-to-server. Once the connection has been established, the SSL over TCP connection is kept alive with periodic heartbeats. If the connection is lost for any reason, the SMP will be aware of the problem. In both cases, events are sent immediately by the Log Collector to the SMP. When SMPs are chained together, for example, for a dedicated reporting SMP, or when events are to be transferred to another SMP, the type can also be set to server -> server.
Host	The host where the Log Collector software is installed. Only required in Server->Log Collector Mode.
Nb	Displays how many virtual Log Collectors have been defined for this Log Collector.
Ignore	Displays the current "Ignore" status, that is, if the SMP is ignoring the Log Collector when the connection type is "server -> Log Collector". If the SMP is not ignoring the Log Collector, it will try to connect to the Log Collector using the IP address and TCP port (as described above). If the Log Collector is unavailable, the SMP will keep re-trying. If you do not want the SMP to keep re-trying (e.g., because you know the Log Collector will be unavailable for a significant time), click this checkbox to ignore the Log Collector. Possible values: True, False, N/A. Note that the ignored Log Collector is automatically stopped.
Updated	Displays the last update date and time. If a virtual Log Collector has not been defined for the Log Collector, the display will be similar to this: `2006-07-20 13.54.26 (1/2).` **(1/2)** indicates that the Log Collector configuration contains 2 log sources - although the Log Collector is not synchronized - and that 1 log source has not been defined yet. Three icons indicate whether the configuration of the Log Collector is up-to-date. There are 3 possible statuses: ✓ The configuration on the Log Collector is up-to-date compared to the configuration on the server. ✖ The configuration on the Log Collector is not up-to-date compared to the configuration on the server. ⌛ The configuration on the Log Collector is currently synchronizing with the configuration on the server (i.e., you will see this status displayed after having clicked the **Apply** button).
Connected	Indicates whether the Log Collector is connected or disconnected. If the status is disconnected, check that the Log Collector is correctly installed and that network connections are authorized between the Log Collector and the server. If the status is connected, this indicates that the communication between the Log Collector and the server is working. **Note:** To know whether events collection correctly work, you must look at the equipment view list.
Action: Refresh the list	To refresh the list of Log Collectors.

Table 14 Log Collector Configuration Fields

Field	**Description**
Button Ignore	To ignore the Log Collector when the connection type is "server -> Log Collector". See the description of the “Ignore” parameter above.
Button Apply	To manually apply the Log Collector’s configuration defined on the SMP. The configuration is then sent to the Log Collector.
Button Delete	Removes the Log Collector from the list of monitored Log Collectors (only administrator and super-administrator can perform this action).
Button Add	Adds a Log Collector from the list of monitored Log Collectors (only administrator and super-administrator can perform this action).

Log Collector Edition/Creation

Server-to-Log Collector Connection

The characteristics of this screen are described in the following table.

Table 15 Server-to-Log Collector Connection Fields

Field	**Description**
Log Collector Name	Each Log Collector must have a unique name. Typically this is the hostname where the Log Collector software is installed.
Host	Select one of the hosts that has been defined in the asset database. This host corresponds to the machine on which the Log Collector will be installed. If the host you want to use is not available in the list, it means that you must create it in the **Asset Database** as explained in chapter Host of the ***User Guide***.
Info used to connect to Log Collector	Used by server-> Log Collector connections to establish the connection to the Log Collector.
Port	Used by server-> Log Collector connections to establish the connection to the Log Collector.
Advanced Parameters	Tick this checkbox to set advanced parameters. These parameters are described below.
Max EPS	The maximum events per second that the Log Collector is allowed to send to the SMP. ***Default value = 1000.*** 150 specifies no limit. If the number of events per second to be sent reaches this limit, events are spooled on the Log Collector so that the events arriving at the SMP does not exceed this figure. When the events per second to be sent drops below this maximum, events will be sent from the spool. The Log Collector prioritizes alerts during this “throttling” such that high priority alerts will be sent in preference to lower priority ones.
Compress Event Stream	Use this to enable compression of the traffic between the Log Collector and the server.
Max line length	The maximum number of characters per line in a log file that will be read by the Log Collector. Log lines longer than this value will not be analysed, and a special alert will be generated. ***Default value = 100000.*** If you change this value and a log file contains lines with a length larger than the old or new value, the Log Collector will re-analyse the log file from the beginning. This could lead to duplicate events. So it would be safer to recreate the log file.
Max line repetition	How many times an alert will be repeated when you receive a line such as: "last message repeated 120 times". ***Default value = 1000.***
Spooler Configuration	

Table 15 Server-to-Log Collector Connection Fields

Field	**Description**
By default, options are already set in the spooler configuration section. The corresponding files are located in the following folders: - For the local Log Collector: `/home/exaprotect/spool/[Instance]/agent`. - For the remote Log Collector: [Log Collector_`directory]\spool\agent`.	
One spool per severity	When the connection to the SMP is lost, the Log Collector spools events to be sent to the SMP as files on the Log Collector. Tick this option to have one queue per alert severity. ***Default value = not checked.***
Spool event with info severity	Specify whether informational events are spooled or not. ***Default value = not checked.***
Num. files	Maximum number of files to write before pausing the collection of events (collection resumes when space is available in the files, no events are lost in the original log). ***Default value = 10.***
File size (MB)	How large each file can grow to before a new one is created. ***Default value = 10.***
Syslog Configuration	
Socket buffer size (ko)	How large the socket buffer must be if messages are received via syslog UDP. ***Default value = 128***
UDP max packet size (ko)	How large a packet must be if messages are received via syslog UDP. ***Default value = 8***

Caution: It is not recommended to modify the **spooler configuration**. However, if you really want to modify it, clean the spool directory first by deleting all the files before doing any change in the configuration.

Log Collector-to-Server Connection

Refer to the "Server-to-Log Collector Connection" sub-section for a description of the various parameters. The Log Collector-to-server connection type has one more parameter:

- The **Use alternate server IP name** parameter is required when the Log Collector cannot directly connect to the server, e.g., in a network containing an asymmetrical NAT definition. This parameter, which is either a name or an IP address, must be recognized on the network used by the Log Collector.

Server-to-Server Connection

Refer to the "Server-to-Log Collector Connection" sub-section to get a description of the various parameters. The server-to-server connection type has two other parameters described in the following table.

Description

The characteristics of this screen are described in the following table.

Table 16 Server-to-Server Connection

Field	Description
Remote instance name	Required when forwarding alerts to a remote SMP, since an SMP may have multiple instances.
Use alternate server IP/name	Required when the Log Collector cannot connect directly to the server, e.g., in a network containing an asymmetrical NAT definition. This parameter, which is either a name or an IP address, will be recognized on the network used by the Log Collector.

Collected Log Sources

Use the **Collected log sources** screen to assign a confset to a Log Collector (**Log Management > Log Collection >** Log Collector**s > click on a** Log Collector).

Description

The characteristics of this screen are described in the following table.

Table 17 Collected Log Sources Columns

Column	Description
Log Source	To change the configuration settings (confset) used by the Log Collector, click the supported product name.
Confset	Edit the confset properties. See sub-section "Log Collection: Advanced: Confsets".
Type	The log source type.
Last update	The last time the Log Collector software was updated.
Active	Indicates if the log source is collected or not.
Enable	To enable an Log Collector's log source that was previously disabled.
Disable	To disable temporarily an Log Collector's log source for further use.
Delete	To delete a Log Collector's log source from the list.
Add	To add a Log Collector's log source in the list.

Log Source Definition

Use this screen to add a new log source. The **Log Source Definition** screen is displayed when you click on **Add** in the list of collected log sources.

Description

The characteristics of this screen are described in the following table.

Table 18 Log Source Definition

Column	Description
Confset drop-down list	Confset name.
Log source name	Name of the log source.
Host	The host defines the Site and the Organizational Unit of the log source. If you choose **Same as** Log Collector, the Log Collector's host will be used for this log collector.
Type	Select the icon type that will be used to represent the log source in the GUI.
Active	Indicate whether the log source should be collected or not.

To know how to manage log collectors, refer to section "Log Collectors" in the User Guide.

Log Collection: Download Log Collector Installation File

The Log Collector Installation File pane is used to create the zip file which is required during the installation of a new Log Collector.

To display the Log Collector Installer pane, go to **Log Management > Log Collection > Download log collector Installation File**.

The zip file will contain a certificate file `*.ks` and a configuration file `*.xml` containing the parameters given on this page.

Log Collector Installation File

Use the Log Collector **Installation File** screen to download the Log Collector installation file.

Description

The characteristics of this screen are described in the following table.

Table 19 Log Collector Installation File

Field	**Description**
SMP server address	SMP Server Address. Alternatively you can enter the IP address of the SMP server.
Port	Port number (in this case 5555).
Type	Communication type.
Download button	Displays the File Download dialog box where you can save this file to the disk and transfer it to the machine where the Log Collector will be installed.
Log Collector Installers	To download SEM Log Collector installer, go to download.tibco.com or contact the support.

Log Collection: Supported Products

Use the **Supported Products** screen to display the devices currently monitored by the SMP (Log Management > Log Collection > Supported Products).

Characteristics

Description

The characteristics of this screen are described in the following table.

Table 20 Supported Products List Column

Column	**Description**
Name	The name of the device being monitored. Click the blue arrow to see more details.
Vendor	The vendor of the device.
Type	The function of the device being monitored. It can help you to determine which vulnerabilities may be applicable.
Supported via TIBCO LogLogic® Log Management Appliance	Indicates which product is handled by TIBCO LogLogic® Log Management Appliance, i.e. the collection is made via the TIBCO LogLogic® appliance and not directly from the supported product itself.
PDF icon	By clicking on this icon, you can download the configuration documentation related to this product.

Log Collection: Advanced: Confsets

The confset consists of a group of converters and properties allowing to define what must be collected, i.e. events and/or raw logs.

Note: Some converter parameters can be edited through the confsets. If you edit them this way, then your modifications will simply override those that were defined in the converter configuration (i.e. they will not change the configuration of options of the converter itself).

To access the Confsets pane, go to **Log Management > Log Collection > Advanced > Confsets.** The list of confsets shows the name, description, and which converters are included

Characteristics

The characteristics of this screen are described in the following table.

Table 21 Confset View Possible Actions

Action	Description
Edit	Click the name of the confset to edit it.
Copy	Copies the selected confset.
Delete	Deletes the selected confset.
Standard	An icon indicates whether a confset is standard.
Add	Click the **Add** button to add a new confset.
Refresh the list	This link enables the reloading of the list of confsets. This is useful if you have modified the confset manually in command line.

General Confset Properties

The characteristics of this screen are described in the following table.

Table 22 General Confset Properties Fields

Property	Description
Name	Every confset must have a unique name.
Description	A brief description of the purpose of the confset which is shown besides the name when the confset is included in Log Collector properties.
Collection Policy	Collection policies allow you to determine which events are sent from the Log Collector to the SMP. A collection policy file contains a list of rules which determine the actions to take, such as: ▪ nothing is sent ▪ only elementary events are sent: a small number or only the main ones or all those with a Taxonomy or all of them ▪ both are sent: all the elementary events with a Taxonomy + small number of raw logs or all the elementary events with a Taxonomy + raw logs or all the elementary events + all types of raw logs ▪ all types of elementary events + all types of raw logs are sent This can reduce the amount of events sent from the Log Collector to the SMP. You cannot choose if its filter name contains the string “copy”. ▪ If you try to do this, an error message will be displayed. If you want to use a copy, please change the filter name. ▪ By default, if an event is not handled by a collection policy, then this event will be automatically retrieved.
Detection of Log Source Inactivity	

Table 22 General Confset Properties Fields

Property	Description
Generate an event	Generates an event if no elementary event or raw log has been received for a certain amount of time from a connected log source. The generated event will have the following syntax: ***No event has been sent for xx minutes*** and no alert will be created from it.
Period of inactivity	Period of inactivity (in minutes) from which the event is generated.
Address Resolution on Log Collector	
Resolve DNS name	Ensure the alert includes IP addresses that match any hostnames mentioned in the event. **Note:** Enabling this option can significantly reduce the performance of the Log Collector.
Resolve IP	Ensure the alert includes hostnames that match any IP addresses mentioned in the event. **Note:** Enabling this option can significantly reduce the performance of the Log Collector.
Elements Recorded in the Event	
Log source chain	Indicates whether the information contained in the event must come from the original log source only or from both the original log source and log source relay.
Syslog source	Turn on this option when log entries are collected via a SysLog Concentrator, to ensure that they are correctly identified by their originating device and NOT the concentrator. This will create a "virtual" device using the host name from the syslog events.
Target node	Indicate if you want to add the log source host (name or address) if there is no target node.
Detection date	If the timezone of the machine on which the Log Collector is installed is not the same as the time server, an automatic reset of the events detection time can be applied by ticking this checkbox. The events will then match the time on the server. **Example:** ▪ The time system of the machine on which the Log Collector is installed is **9.15**. ▪ The time server is **9.30**. ▪ Then a time shift of **15** minutes will be applied to any collected events. E.g. a log has been generated at **7.30** and then the detection time will be **7.45**. The information about the initial detection date is not lost but available in the event additional data. Remember that this option must be used **only if** you did not properly configure and synchronize according to a NTP server the machine on which the Log Collector is installed as described in the Log Collector **Installation Guide**.

Adding Converters to the Confset

Use the Converters screen to add converters to the Confset.

The characteristics of this screen are described in the following table.

Table 23 Converters

Column or button	Description
Add button	Add a converter to a confset.
Converter	Name of the converter.
Delete	Remove the converter from the confset. This does not delete the converter altogether, it can still be used in other confsets.

Log Collection: Advanced: Converters

Use the Log Collection: Advanced: Converters screen to convert log entries into events

Caution: Standard converters (delivered by TIBCO LogLogic®) cannot be modified. To change the configuration of converters, copy and edit them as needed.
DO NOT use the Add button to add OPSEC, WELF and Multi-Line converters. You can only add them by using the Copy function.

To access the Converters pane, go to **Log Management** > **Log Collection** > **Advanced** > **Converters**.

The converter configuration page lists the available standard converters in a table as shown in the example below.

Characteristics

Description

The characteristics of this screen are described in the following table.

Table 24 Converter Configuration

Column	**Description**
Name	Converter name and a short comment describing the purpose of the converter.
Type	There are 9 types of converters: ▪ DB (databases), ▪ Logger (flat plain-text log file), ▪ TIBCO LogLogic® (sends syslog messages) ▪ LotusNotes ▪ OPSEC (CheckPoint protocol), ▪ WMI (Windows Management Instrumentation protocol), ▪ WELF (WebTrends Enhanced Logfile Format), ▪ RDEP, ▪ SCANNER, ▪ Multi-Line ▪ RSA.
Standard	Indicate if the converter is standard or user- defined.
Copy	Copy an existing converter (if a similar one is needed).
Delete	Delete a converter. Only possible if the converter is not in use in a confset and/ or if it is not a standard converter.

Types of Converters

To display the converter details that you copied, click on the name of the converter: the converter's name, description, and **type** are displayed.

Table 25 Types of Converter

Type	**Description**
Database Converter	A database converter is used when the source of events to be monitored is an SQL database.
Log Converter	A logger converter is used when the source of events to be monitored is a text File.
TIBCO LogLogic® Converter	A TIBCO LogLogic® converter is used when the source of events to be monitored is coming from the TIBCO LogLogic® Open Log Management Platform via the Syslog protocol.

Table 25 Types of Converter

Type	Description
Lotus Notes Converter	A Lotus Notes converter is used when the source of events to be monitored is a Lotus Domino database.
WMI Converter (Windows Management Instrumentation protocol)	A WMI converter is used when the events are to be collected via the WMI protocol, e.g., when collecting events from a Microsoft Windows server event log.
WELF Converter (WebTrends Enhanced Logfile Format)	A WELF converter is used when the source of events to be monitored is a text file in the WELF format.
OPSEC Converter (Checkpoint protocol)	An OPSEC converter is used when the events are to be collected via the OPSEC protocol, e.g., when collecting events from Firewall-1.
RDEP Converter	A RDEP converter is used when the events are to be collected via the RDEP protocol, e.g., when collecting events from CISCO secure IDS.
SCANNER Converter	A scanner converter is used to collect the results of vulnerability scans from scanners such as Nessus, Criston, and Qualys.
Multi-Line Converter	A multi-line converter is used when events span more than one line of a log file. Each of the constituent lines must have the same event identifier ID so that the lines can be treated as one event.
RSA Converter	A RSA converter is used to connect to the RSA ACE Log Database using RSA admin toolkit api.

Database Converter

Table 26 Database Converter Fields

Field	Description
Database address	IP address of the host database. [Can be overridden in Confset]
Database port	The network port to connect to the database. [Can be overridden in Confset]
Database instance name	The name of the database. [Can be overridden in Confset]
Database User	The name of the database user with the required credentials. [Can be overridden in Confset]
Database Password	The password for the database. [Can be overridden in Confset]
JDBC Option	Select the appropriate option for your database type. For more information refer to the documentation for the JDBC driver in use. [Can be overridden in Confset]
Polling Delay (s)	The time in seconds between SQL requests. [Can be overridden in Confset]
Date Format	Select the date format. See section Date Time Format Specification in the User Guide's ***Appendix*** for further information. [Can be overridden in Confset]
Time Zone	Select the time zone used by the log source. [Can be overridden in Confset]
Charset	Select the charset (UTF8, US-ASCII...).used by the log source. [Can be overridden in Confset] Note that modifying the charset leads to a file irrelevance.

Table 26 Database Converter Fields

Field	Description
Database	Select the database to use. If the desired database is not listed you will need to add the driver and to complete the `database.conf.xml`, in the directory `/home/exaprotect/conf/<clientname>/rulest/db/dbdriver.` Note that this file is automatically overwritten during an update
DB MAP File	Select a map file from the list. The map file must match your product and product version number.
New Query	Add SQL query to the list of queries that will be sent to the database to obtain the alerts.
Queries	A list of SQL queries.

Log Converter

Table 27 Log Converter Fields

Field	Description
Log format	Select a log format: ▪ plaintext: the log will be a text file. If you select this format, the Collection source parameter is set to **from file**. ▪ syslog (RFC 3164): the log will be a syslog file. If you select this format, you must define the collection source, either **from file** or **from network (syslog protocol RFC 3164)**.
Collection Source	Select the collection source i.e. **from file** or **from network (syslog protocol RFC 3164)**. [Can be overridden in Confset]
File Name (if Collection Source is "From File")	The full path and filename of the file you wish to convert. [Can be overridden in Confset] **Caution:** If you selected **From File** as collection source, you can enter a character chain such as: **c:\agent\agent.log.[id]-[date]** provided you checked **Using Index** and **Using Time Stamping** boxes. e.g. provided you enter a specific date format, you will get file names such as **agent.log.1.221107**, **agent.log.2.231107**...etc. [Can be overridden in Confset]
Using Index (if Collection Source is "From File")	If your file name includes an id such as `logFile-01.txt,logFile-02.txt` you must use these additional options: Nb. digit: the number of digits in the filename. A maximum of 9 digits is allowed. [Can be overridden in Confset] e.g. if the file name is **agent.log.[id]**, then you will get **agent.log.1**, then a**gent.log.2**...etc.

Table 27 Log Converter Fields

Field	Description
Using Time Stamping (if Collection Source is "From File")	If the file name is not constant because it includes information relative to date/time, you must define this parameter by: 1. Ticking the checkbox. The Date Format field will then appear. 2. Defining the field: ▪ Date format: lets you enter the date if your filename includes a date. See section Date Time Format Specification in the User Guide's ***Appendix*** for further information. [Can be overridden in Confset] e.g. if the file name is **agent.log.[date]**, then you will get **agent.log.221107**, then a**gent.log.231107**...etc.
Listening Port (if Collection Source is "from network (syslog protocol RFC 3164)"	Enter the port that the local Log Collector will use to retrieve the Syslog logs. The default value is 514. **Caution:** By default, you cannot use another port than the 514/UDP port. However, if you want to use another port, you must manually configure the firewall. [Can be overridden in Confset] **UDP:** To specify that the syslog logs should be collected via UDP protocol. This is the default configuration. [Can be overridden in Confset] When modifying the Log Collector status (such as updating or stopping it) or when the Log Collector is not running during the collection, events may be lost. Indeed, contrary to the TCP protocol, the **UDP** protocol avoids the overhead of checking whether every packet actually arrived, which may lead to data loss. **TCP:** To specify that the syslog logs should be collected via TCP protocol. [Can be overridden in Confset] If another Syslog log is running on the server where the Log Collector is installed, the Log Collector and syslog will not have the same port, IP and protocols. In that case, you must either stop the syslog (but it is not recommended on SMP) or make the Log Collector listen to 515/udp/0.0.0 for example.
Listening IP address (if Collection Source is "from network (syslog protocol RFC 3164)"	Enter the IP address of the machine interface on which you want to collect syslog log. The default value is 0.0.0.0 which means that data will be collected from all the machine interfaces. [Can be overridden in Confset]
Facility (if Collection Source is "from network (syslog protocol RFC 3164)"	To indicate the type of message that must be collected by selecting its corresponding facility number. By default, all the facilities are selected. Refer to the following URL for further information about the BSD syslog Protocol: http://www.ietf.org/rfc/rfc3164.txt. [Can be overridden in Confset]

Table 27 Log Converter Fields

Field	Description
Severity (if Collection Source is “from network (syslog protocol RFC 3164)”	To indicate which levels of severity will be reported, select one of the following levels: ▪ Emergency: system is unusable. ▪ Alert: action must be taken immediately. ▪ Critical: critical conditions. ▪ Error: error conditions. ▪ Warning: warning conditions. ▪ Notice: normal but significant condition. ▪ Informational: informational messages. ▪ Debug: debug-level messages. The default value is **Informational**. [Can be overridden in Confset]
Authorized IP addresses (regexp) (if Collection Source is “from network (syslog protocol RFC 3164)”	Enter a Java regular expression to indicate from which source machine the messages should be collected. Refer to the "Java Regular Expressions" section in the User Guide to get the list of regular expressions to be used. By default, messages are collected from all source machines. The default value is therefore `.*` . [Can be overridden in Confset]
Country Code	This code is the upper-case, two-letter code as defined by ISO-639. [Can be overridden in Confset]
Language Code	This code is the lower-case, two-letter code as defined by ISO-3166. [Can be overridden in Confset]
Date Format	See section Date Time Format Specification in the User Guide’s ***Appendix*** for further information. [Can be overridden in Confset]
Time Zone	Select the time zone used by the log source. [Can be overridden in Confset]
Rulesets	Select the appropriate rule-set to use with this converter.
Log Map Files	Select the appropriate MAP file.

TIBCO LogLogic® Converter

Table 28 TIBCO LogLogic® Converter Fields

Field	Description
Listening Port	This option allows you to specify that the syslog logs should be collected via TCP or UDP protocols. TCP is the default configuration. See Table Table 27 "Log Converter Fields" for more information about these protocols. Syslog is the protocol used for the communication between the TIBCO LogLogic® Platform and the Log Collector. **Note:** Port is 514 by default.
Listening IP address	The IP address of the Log Collector's host interface. The default value (0.0.0.0) means that logs are collected from all the Log Collector's host interface.

Table 28 TIBCO LogLogic® Converter Fields

Field	Description
Authorized IP addresses (regexp)	Enter a Java regular expression to indicate from which source machine the messages should be collected. Refer to the "Java Regular Expressions" section in the User Guide to get the list of regular expressions to be used. By default, messages are collected from all source machines. The default value is therefore `.*`. [Can be overridden in Confset]
Time zone	Select the time zone used by the log source. [Can be overridden in Confset]
Display the list of products that can be collected via TIBCO LogLogic® Platform	Gives the list of the products supported by the TIBCO LogLogic® appliance.

Lotus Notes Converter

Table 29 Lotus Notes Converter Fields

Field	Description
Server	The Lotus Domino server address.
Port	The Lotus Domino port address.
Login	The login configured to access the Domino server.
Password	The password configured to access the Domino server.
Field separator	The separator used between fields. [Can be overridden in Confset]
Value separator	The separator used between field name and value. [Can be overridden in Confset]
Empty field value	Some products use a default value instead of being empty, e.g., n/a. [Can be overridden in Confset]
Header regex	To parse the beginning of the line which is not WELF formatted. [Can be overridden in Confset]
Country code	The lower case, 2 letter code as defined by ISO-639. [Can be overridden in Confset]
Language code	The upper case, 2 letter code as defined by ISO3166. [Can be overridden in Confset]
Date format	See section Date Time Format Specification in the User Guide's ***Appendix*** for further information. [Can be overridden in Confset]
Time zone	Select the time zone used by the log source. [Can be overridden in Confset]
Type collector	Select if the Log Collector collects one or multiple events by doc.
Type converter	Select the sub-type of the converter: welf or log.
Welf map file	Select the appropriate map file.
Upload Notes jar files	To make the Lotus Domino converter work correctly, you must download two jar files.

WMI Converter

Table 30 WMI Converter Fields

Field	Description
Address	Address of the Windows host from which to obtain events. [Can be overridden in Confset]. Note that the user MUST HAVE at least a Local Administrator account. Otherwise, he will not have access to Event logs. However, there is no need to have Domain Administrator rights, Local Administrator account is enough.
User	The administrator account login. [Can be overridden in Confset]. Note that the user MUST HAVE at least a Local Administrator account. Otherwise, he will not have access to Event logs. However, there is no need to have Domain Administrator rights, Local Administrator account is enough.
Password	The password of the administrator login. [Can be overridden in Confset]
Domain	The Windows domain name, or if there is no domain name, the hostname (not address). [Can be overridden in Confset]
Polling Delay(s)	The delay in seconds between WMI requests. [Can be overridden in Confset]
Time Zone	The time zone used by the Windows host. [Can be overridden in Confset]
Locale	The set of user preference information related to the user's language, environment and/or cultural conventions. [Can be overridden in Confset] **Note:** For users with a Thai Windows OS only: make sure the **Time Zone** is set at ***local*** and the **Locale** is set at ***English (United States)*** as Windows events are stored in English US language in that specific case.
Store Description	Check this box to obtain the description of the Windows event. [Can be overridden in Confset]
Include or exclude Journal	Select whether you want to include or exclude the MS Windows journals. See the WMI Journal option. Example: To retrieve all the WMI journals, select Exclude and no WMI journal in the WMI Journal option. [Can be overridden in Confset]
WMI Journal	Define which WMI journals must be included or excluded (after having clicked either the Include or the Exclude radio buttons in the Include or Exclude Journal option). You can also enter another journal in the input field below and include it, likewise with available journals. [Can be overridden in Confset]
WMI Map File	Select the appropriate map file to use with this converter.

WELF Converter

Table 31 WELF Converter Fields

Field	Description
Log format	Select a log format: - plaintext: the log will be a text file. If you select this format, the Collection source parameter is set to **from file**. - syslog (RFC 3164): the log will be a syslog file. If you select this format, you must define the collection source, either **from file** or **from network (syslog protocol RFC 3164)**.
Collection Source	Select the collection source, i.e. “From file” or “From Syslog” source. [Can be overridden in Confset]
File Name (if Collection Source is “From File”)	The full path and filename of the file you wish to convert. [Can be overridden in Confset]
Using Index (if Collection Source is “From File”)	If your file name includes an ID such as `logFile-01.txt,logFile-02.txt,` you must use this additional option: Nb digit: the number of digits in the filename. A maximum of 9 digits is allowed. [Can be overridden in Confset]
Using Time Stamping (if Collection Source is “from network (syslog protocol RFC 3164)”	If the file name is not constant because it includes information relative to date/time, you must define this parameter by: 1. Ticking the checkbox. The Date Format field will then appear. 2. Defining the following field: - Date format: lets you enter the date, if your filename includes a date. See section Date Time Format Specification in the User Guide’s ***Appendix*** for further information. [Can be overridden in Confset]

Table 31 WELF Converter Fields

Field	Description
Listening Port (if Collection Source is "from network (syslog protocol RFC 3164)"	Enter the port that the local Log Collector will use to retrieve the Syslog logs. The default value is 514. **Note:** By default, you cannot use another port than the 514/UDP port. However, if you want to use another port, you must manually configure the firewall. [Can be overridden in Confset] **UDP:** To specify that the syslog logs should be collected via UDP protocol. This is the default configuration. [Can be overridden in Confset] When modifying the Log Collector status (such as updating or stopping it) or when the Log Collector is not running during the collection, events may be lost. Indeed, contrary to the TCP protocol, the **UDP** protocol avoids the overhead of checking whether every packet actually arrived, which may lead to data loss. **TCP:** To specify that the syslog logs should be collected via TCP protocol. [Can be overridden in Confset] If another Syslog log is running on the server where the Log Collector is installed, the Log Collector and syslog will not have the same port, IP and protocols. In that case, you must either stop the syslog (but it is not recommended on SMP) or make the Log Collector listen to 515/udp/0.0.0 for example.
Listening IP address (if Collection Source is "from network (syslog protocol RFC 3164)"	Enter the IP address of the machine interface on which you want to collect syslog log. The default value is 0.0.0.0 which means that data will be collected from all the machine interfaces. [Can be overridden in Confset]
Facility (if Collection Source is "from network (syslog protocol RFC 3164)"	To indicate the type of message that must be collected by selecting its corresponding facility number. By default, all the facilities are selected. Refer to the following URL for further information about the BSD syslog Protocol: http://www.ietf.org/rfc/rfc3164.txt [Can be overridden in Confset]
Severity (if Collection Source is "from network (syslog protocol RFC 3164)"	To indicate which levels of severity will be reported, select one of the following levels: ▪ Emergency: system is unusable. ▪ Alert: action must be taken immediately. ▪ Critical: critical conditions. ▪ Error: error conditions. ▪ Warning: warning conditions. ▪ Notice: normal but significant condition. ▪ Informational: informational messages. ▪ Debug: debug-level messages. The default value is **Informational**. [Can be overridden in Confset]

Table 31 WELF Converter Fields

Field	Description
Authorized IP addresses (regexp) (if Collection Source is “from network (syslog protocol RFC 3164)”	Enter a Java regular expression to indicate from which source machine the messages should be collected. Refer to the "Java Regular Expressions" section in the User Guide to get the list of regular expressions to be used. By default, messages are collected from all source machines. The default value is therefore `.*` . [Can be overridden in Confset]
Field separator	The separator used between fields. [Can be overridden in Confset]
Value separator	The separator used between field name and value. [Can be overridden in Confset]
Empty field value	Some products use a default value instead of being empty, e.g., `n/a`. [Can be overridden in Confset]
Header regex	To parse the beginning of the line which is not WELF formatted. [Can be overridden in Confset]
Country Code	The lower case, 2 letter code as defined by ISO-639. [Can be overridden in Confset]
Language Code	The upper case, 2 letter code as defined by ISO3166. [Can be overridden in Confset]
Date Format	See section Date Time Format Specification in the User Guide’s ***Appendix*** for further information. [Can be overridden in Confset]
Time Zone	Select the time zone used by the log source. [Can be overridden in Confset]
Charset	Select the charset (UTF8, US-ASCII...).used by the log source. [Can be overridden in Confset] Note that modifying the charset leads to a file irrelevance.
WELF Map File	Select the appropriate map file.

OPSEC Converter

Table 32 OPSEC Converter Fields

Field	Description

Config File	`lea_server_ip <firewall name or ip address>`
	`lea_server Port 18184`
	For example, if the CheckPoint IP address is 192.168.10.96, and the lea_server port is the default, the following would be displayed:
	`lea_server ip 192.168.10.96`
	`lea_server_port 18184`
	[Can be overridden in Confset]

Generated p12 certificate file	The certificate file used to authenticate the Log Collector to an OPSEC event source (generated on an OPSEC event source, e.g, FW-1 Manager.) This is not required for "clear" authentication, and only needed for secure mode. [Can be overridden in Confset]
Time Zone	Select the time zone used by the Checkpoint host. [Can be overridden in Confset]
OPSEC Map File	Select the appropriate map file to use with this converter.

Note: For information on how to configure an OPSEC converter with secure mode, please refer to the separate guide on OPSEC configuration entitled ***Working with CheckPoint***.

RDEP Converter

Note: The SMP cannot retrieve raw logs from RDEP converters for the moment.

Table 33 RDEP Converter Fields

Field	Description
Address	The IP address or name of the CISCO RDEP server from which you wish to obtain events. [Can be overridden in Confset]
Port	The network port required to connect to the CISCO REDEP server. [Can be overridden in Confset]
Login	The CISCO server account name with which to authenticate. [Can be overridden in Confset]
Password	The password of the CISCO server account. [Can be overridden in Confset]
Time zone	The time zone used by the log source. [Can be overridden in Confset]
RDEP Map File	Select the appropriate map file.

SCANNER Converter

Note: The SMP cannot retrieve raw logs from SCANNER converters for the moment.

Table 34 SCANNER Converter Fields

Field	Description
Directory to supervise	The directory where the XML output will be stored. [Can be overridden in Confset]
URL	Type in the URL required to connect to the Qualys server so as to retrieve the scanner report (the Log Collector must have access to internet to retrieve this report). [Can be overridden in Confset]
Port	Type in the port used for the connection. [Can be overridden in Confset]
Login	Type in the Login required for authenticating on the Qualys server. [Can be overridden in Confset]
Password	Type in the Password required for authenticating on the Qualys server. [Can be overridden in Confset]
Period (min.)	Interval between each connection made with the Qualys server to check if new scan reports must be analyzed. This interval is set in minutes. [Can be overridden in Confset]

Table 34 SCANNER Converter Fields

Field	Description
HTTP proxy IP	IP address required to connect to the proxy server. This parameter is optional. [Can be overridden in Confset]
HTTP proxy port	Port required to connect to the proxy server. This parameter is optional. [Can be overridden in Confset]
HTTP proxy username	User name required to connect to the proxy server. This parameter is optional. [Can be overridden in Confset]
HTTP proxy password	Password required to connect to the proxy server. This parameter is optional. [Can be overridden in Confset]
Time zone	Time zone used by the log source. [Can be overridden in Confset]
Type	The type of scanner that will generate the XML file. If you select Qualys as scanner type, several other options will have to be configured. [Can be overridden in Confset]
Scanner Map File	The appropriate map file to use with this configuration.

Multi-Line Converter

Table 35 Multi-Line Converter Fields

Field	Description
Log format	Select a log format: ▪ plaintext: the log will be a text file. If you select this format, the Collection source parameter is set to **from file**. ▪ syslog (RFC 3164): the log will be a syslog file. If you select this format, you must define the collection source, either **from file** or **from network (syslog protocol RFC 3164)**.
Collection Source	Select the collection source, i.e. “From file” or “From Syslog” source. [Can be overridden in Confset]
File Name (if Collection Source is “From File”)	The full path and filename of the file you wish to convert. [Can be overridden in Confset]
Using Index (if Collection Source is “From File”)	If your file name includes an ID such as `logFile-01.txt,logFile-02.txt,` you must use this additional option: Num. digit: the number of digits in the filename. A maximum of 9 digits is allowed. [Can be overridden in Confset]

Table 35 Multi-Line Converter Fields

Field	Description
Using Time Stamping (if Collection Source is "From File")	If the file name is not stable because it includes information relative to date/time, you must define this parameter by: 1. Ticking the checkbox. The **Date Format** field will then appear. 2. Defining the field: - Date format: lets you enter the date if your filename includes a date. See section Date Time Format Specification in the User Guide's ***Appendix*** for further information. [Can be overridden in Confset]
Listening Port (if Collection Source is "from network (syslog protocol RFC 3164)"	Enter the port that the local Log Collector will use to retrieve the Syslog logs. The default value is 514. **Note:** By default, you cannot use another port than the 514/UDP port. However, if you want to use another port, you must manually configure the firewall. [Can be overridden in Confset] **UDP:** To specify that the syslog logs should be collected via UDP protocol. This is the default configuration. [Can be overridden in Confset] When modifying the Log Collector status (such as updating or stopping it) or when the Log Collector is not running during the collection, events may be lost. Indeed, contrary to the TCP protocol, the **UDP** protocol avoids the overhead of checking whether every packet actually arrived, which may lead to data loss. **TCP:** To specify that the syslog logs should be collected via TCP protocol. [Can be overridden in Confset] If another Syslog log is running on the server where the Log Collector is installed, the Log Collector and syslog will not have the same port, IP and protocols. In that case, you must either stop the syslog (but it is not recommended on SMP) or make the Log Collector listen to 515/udp/0.0.0 for example.
Listening IP address (if Collection Source is "from network (syslog protocol RFC 3164)"	Enter the IP address of the machine interface on which you want to collect syslog log. The default value is 0.0.0.0 which means that data will be collected from all the machine interfaces. [Can be overridden in Confset]
Facility (if Collection Source is "from network (syslog protocol RFC 3164)"	To indicate the type of message that must be collected by selecting its corresponding facility number. By default, all the facilities are selected. Refer to the following URL for further information about the BSD syslog Protocol: http://www.ietf.org/rfc/rfc3164.txt [Can be overridden in Confset]

Table 35 Multi-Line Converter Fields

Field	Description
Severity (if Collection Source is "from network (syslog protocol RFC 3164)"	To indicate which levels of severity will be reported, select one of the following levels: The various levels are the following: ■ Emergency: system is unusable. ■ Alert: action must be taken immediately. ■ Critical: critical conditions. ■ Error: error conditions. ■ Warning: warning conditions. ■ Notice: normal but significant condition. ■ Informational: informational messages. ■ Debug: debug-level messages. The default value is **Informational**. [Can be overridden in Confset]
Authorized IP addresses (regexp) (if Collection Source is "from network (syslog protocol RFC 3164)"	Enter a Java regular expression to indicate from which source machine the messages should be collected. Refer to the "Java Regular Expressions" section in the User Guide to get the list of regular expressions to be used. By default, messages are collected from all source machines. The default value is therefore `.*` . [Can be overridden in Confset]
Country Code	This code is the lower-case, two-letter code as defined by ISO-639. [Can be overridden in Confset]
Language Code	This code is the upper-case, two-letter code as defined by ISO-3166. [Can be overridden in Confset]
Date Format	See section Date Time Format Specification in the User Guide's ***Appendix*** for further information. [Can be overridden in Confset]
Time Zone	Select the time zone used by the log source. [Can be overridden in Confset]
Charset	Select the charset (UTF8, US-ASCII...).used by the log source. [Can be overridden in Confset] Note that modifying the charset leads to a file irrelevance.
Advanced Parameters	Tick this checkbox to set further parameters. These parameters are described below.
Max hash size	The maximum number of lines from partially completed events, that are held in memory, while waiting for the remaining expected lines. [Can be overridden in Confset]
Max hash time (in min.)	The maximum amount of time the partially completed events will be held in memory. [Can be overridden in Confset]
Type	Choose the product that produces the log files (e.g., Postfix).

RSA Converter

Table 36 RSA Converter Fields

Field	**Description**
Polling delay(s)	Delay in seconds between two pollings of the log source by the Log Collector. You must enter a value between 30 and 86401 (that is to say 1 second added to 1 day). [Can be overridden in Confset]
Country code	This code is the lower-case, two-letter code as defined by ISO-639. [Can be overridden in Confset]
Language code	This code is the upper-case, two-letter code as defined by ISO-3166. [Can be overridden in Confset]
Date format	See section Date Time Format Specification in the User Guide's ***Appendix*** for further information. [Can be overridden in Confset]
Time zone	Select the time zone used by log source. [Can be overridden in Confset]
Rulesets	Select the appropriate rule-set to use with this converter.
Log map files	Select the appropriate MAP file.

Log Collection: Advanced: Conversion Rulesets

Use the Log Collection: Advanced: Conversion Rulesets screen to allow the automatic conversion of log entries into events.

To access the Conversion Rulesets screen, select Log Management > Log Collection > Advanced > Conversion Rulesets.

Characteristics

The characteristics of this screen are described in the following table.

Table 37 Description of Conversion Rule-Set Table Columns

Column	**Description**
Name	File Name (*.rule) and the log source name to which the rule applies.
Group	The group to which the log source belongs to (e.g., the Stonegate Firewall belongs to the Firewalls group).
Standard	Indicate if the conversion rule is standard or user defined.
Add	Creates a customizable rule.
Delete	Deletes a rule. Only possible if the rule is not a standard rule.

Archiving

This functionality allows the creation of archiving files for ***elementary events*** and ***raw logs.***

Raw Logs

Use the Raw Logs screen to download and delete raw log archives. To display the Raw Log list, go to **Log Management > Archiving > Archives**.

The **Raw Log Archive Files List** screen displays a list of archives containing raw logs.

Note: Each raw log file contains one day of data.

Description

The characteristics of this screen are described in the following table.

Table 38 Description of the Raw Log Archive File List columns

Column	Description
Name	The file name as used on the Security Management Platform, in the directory `/var/lib/loglogic/archive/INSTANCE_NAME/rawlogs/`.
Size	Indicates the size of the compressed file (the value is in MB).
On disk	Indicates if the file is on the local disk or not (True or False values).
⬇	Allows you to download the *.gpg file corresponding to the raw log.
Delete button	Deletes the selected file (checkbox selected).

Settings

Use the Settings screen to configure the raw log archive settings. To configure raw log archive options, you must go to **Log Management > Archiving > Settings**.

Description

The characteristics of this screen are described in the following table.

Table 39 Raw Log Archive Options Fields

Field	Description
Public Signing Key	This is the public key which allows checking if the archive has been signed by TIBCO LogLogic®.
Public encryption key	This is the public key provided by the user to encrypt the raw log archives (optional). **Note:** Raw Log Archive encryption is possible through the public key displayed in the interface (PGP, GPG, OpenPGP formats). Algorithms available for encryption are: 3DES, CAST5, BLOWFISH, AES, AES192, AES256, TWOFISH. It is recommended to use the AES algorithm.
Export script	A script to execute after the archive task completes successfully. Typically this is used to copy or move the archive file to an external storage location, e.g., tape or remote FTP server. **Note:** The SMP is executing external scripts with "exaprotect" user rights.
Num. retention days	Define the number of days during which you want the raw logs to be kept in the database. 7 is the value by default. However, you can enter a value between 2 and 1000. **Note:** In this case, 30 means a total of 30 consecutive days during which raw logs are kept in the database.

Note: The SMP is executing external scripts with TIBCO LogLogic® user rights.

Raw Logs Forensic

The Logs Forensic module is useful to display a list of raw logs collected in a given time period and search for raw logs using several criteria such as date, log sources or contents.

To access the Logs Forensic module, you must go to **Log Management > Logs Forensic** entry.

The characteristics of this screen are described in the following table.

Table 40 Forensic Parameters

Parameter	Description
Creation Date	Indicate the time period during which the raw logs were generated.
📅	Calendar allowing you to directly select the desired date.
Log Sources section	Filter the raw log search according to log source type.
⏭	Select all the log sources.
▶	Select one or several log sources.
◀	One or several log sources listed on the right-hand pane.
⏮	Remove all the log sources listed on the right-hand pane.
Raw Log content	Filter the raw log display according to content.

Private Encryption Key

Once you have configured the **Forensic Parameters** screen, the **Key Selection** screen is displayed.

This screen allows you to enter the private key content of the raw logs you are searching. This is possible only if the raw logs are not in database but they have been archived on your disk according to a previously configured retention period.

> **Note:** If you used a password (or passphrase) to generate encryption keys, searching encrypted gpg raw logs is not possible.

Raw Log List

Once all the steps have been performed, the **Raw Log List** is displayed.

This screen lists all the online raw logs available for the selected period.

It allows you to export this data in Excel and pdf format.

Log Collection Policies Menu

Use this menu to determine which events at the Log Collector are sent to the SMP. To access the Log Collection Policies screen, select Log Management > Log collection policies.

Characteristics

Description

The characteristics of this screen are described in the following table.

Table 41 Collection Policies View Possible Actions

Action	Description
Delete	Click to delete an existing collection policy. You cannot delete a filter which is already in use in a confset.
Copy	Click this button to copy an existing collection policy and edit it.
Add	Click this button to create a new collection policy.

To get the list of the corresponding collection policy rules, please see section List of Default Collection Rules in the ***Appendix***.

Choice of Collection Policies

The following table describes the various collection policies that can be used.

Table 42 Collection Policies

Name	Description
exa_0_NoRawLog_NoElemEvent	**Raw logs**: None The log collector does not send raw logs to the SMP. **Elementary events**: None The log collector does not send elementary events to the SMP. No elementary events will be used by the SMP for archiving, correlation and reporting. Use this Collection Policy to disable Log Collector forwarding.
exa_1_NoRawLog_LightElemEvent	**Raw logs**: None The log collector does not send raw logs to the SMP. **Elementary events**: Light The log collector sends to the SMP only minimum of elementary events to preserve performances.
exa_2_NoRawLog_StandardElemEvent	**Raw logs**: None The log collector does not send raw logs to the SMP. **Elementary events**: Standard The log collector sends to the SMP only important elementary events to preserve performances.
exa_3_NoRawLog_AllElemEvent	**Raw logs**: None The log collector does not send raw logs to the SMP. **Elementary events**: All The log collector sends to the SMP all elementary events with a defined Taxonomy.
exa_4_NoRawLog_FullElemEvent	**Raw logs**: None The log collector does not send raw logs to the SMP. **Elementary events**: Full The log collector sends to the SMP all elementary events, including elementary events with no defined Taxonomy.

Table 42 Collection Policies

Name	Description
exa_5_LightRawLog_AllElemEvent	**Raw logs**: Light The log collector sends the minimum raw logs required by main IT Security Standards for archiving. **Elementary events**: All The log collector sends to the SMP all elementary events with a defined Taxonomy.
exa_6_StandardRawLog_AllElemEvent	**Raw logs**: Standard The log collector only sends raw logs recommended by main IT Security Standards for archiving. **Elementary events**: All The log collector sends to the SMP all elementary events with a defined Taxonomy.
exa_7_FullRawLog_AllElemEvent	**Raw logs**: Full The log collector sends all original logs to the SMP for Log archiving. **Elementary events**: All The log collector sends to the SMP all elementary events with a defined Taxonomy.

Note: Raw logs are used for archiving only. Elementary events are used for correlation and reporting.

Collection Policy Edition

When copying on a collection policy's name, the **Log Collection Policy** edition screen is displayed.

The **Log Collection Policy** screen displays several fields described in the table below.

Table 43 Log Collection Policy Edition

Field	Description
Name	Name of the collection policy. It is highly recommended to rename the collection policy. The name of the collection policy must not start with the character _ or the string exa_.
Description	Description of the log collection policy.
Set Action	Determines the action to take for a particular rule, or multiple rules.
Move	Changes the sequential order of the rules.
Delete	Deletes the log collection policy.
Add	Adds a log collection policy.
Edit	Allows the edition of the rule.

Rule Edition

When editing a collection policy's rule, the **Rule Edition** edition screen is displayed.

The **Rule Edition** screen displays several fields described in the table below.

Table 44 Log Collection Policy's Rule Edition

Field	Description
Description	Description of the log collection policy's rule.
Action to execute	Selects which events and/or raw logs to be kept.

Table 44 Log Collection Policy's Rule Edition

Field	Description
Add	Adds a new condition to the rule.
Delete	Deletes a selected condition.

Edition of a Rule's Condition

When editing a collection policy's rule, the **Rule Edition** edition screen is displayed.

The **Rule's Condition Edition** screen displays several fields described in the table below.

Table 45 Log Collection Policy's Rule Edition

Field	Description
Edit a New Condition	
Type of Condition	Either TIBCO LogLogic® Taxonomy or Matching Fields.
Define the TIBCO LogLogic® Taxonomy	
TIBCO LogLogic® Taxonomy	Select the category that the event must match.
Define the Filter	
Multiple selector	- Select **any value of this field** when it suffices for only one element in the field to match the **Matching Value**. - Select **all values of this field** when all elements in the field must match the **Matching Value**.
Matching field	Select which field in the event is to be checked. If you select a TIBCO LogLogic® Taxonomy matching field, ONLY a **number (or ID)** found in the relevant ruleset file and corresponding to the Taxonomy field can be entered in the **Matching Value** field below. A text string will not be taken into account.
Negate	If set, the logic is reversed - e.g., to look for events which is not authentication.
Matching type	Specify which type of test is to be performed.
Matching value	Specify the value to be tested. The value MUST be a number if you previously selected a TIBCO LogLogic® Taxonomy **matching field.** - Additional data: you must specify the value with the following format: `“my  addData meaning=my addData value”.` For a test of authentication: `“rulesetName=esmp_auth.rules”` - DetectTime: the format is Tue May 13 11:50:06 CEST 2008. To search correlated alerts on a specific date: ".* May 13 .* 2008". **Note:** The field is not case sensitive.

Aggregation Policy

Use the Aggregation Policy screen to monitor the aggregation rules that must be applied on the events processed by the SMP.

The Aggregation screen is available from Event Management > Aggregation Policy. The list of standard aggregation policies is displayed

Description

The characteristics of this screen are described in the following tables.

Table 46 Aggregation Policy

Item	Description
Checkbox	Allows an action to be performed on the selected rule.
#	Position number of the rule.
Name	Name of the rule.
Processing	A list of the actions to be performed if the rule is triggered
Thresholds	The **threshold** is the number of times the rule must be matched for the action(s) to be performed. The **duration** is the maximum number of seconds between events that will trigger the rule.
Profiles	Whether the rule is active or inactive and which configuration profiles contain this rule. A configuration profile shown with a red cross does not contain the rule and a configuration profile shown with a yellow tick indicates the rule is used in said profile.

Edit an Aggregation Policy

When clicking on a rule's name, the rule edition window is displayed.

The **General** tab displays several fields described in the table below.

Table 47 Aggregation - General Tab

Field	Description
Id	Every rule is given a unique id by the Security Management Platform.
Name	Every rule requires a unique name, specified by the administrator who creates it.
Description	User description of the rule.
Creation	The date and time that the rule was created and which user created it.
Last Update	The date and time the rule was last updated and which user updated it.
Profiles	Select in which security profiles this rule is active. See sub-section Advanced Configuration of Security Levels and Configuration Profiles for further information.

Conditions tab

Multiple conditions can be required to trigger the rule, add as many as required. Exceptions are used to avoid triggering the rule when specified events occur. Specify exceptions in the same way as conditions.

Table 48 Logical Expression

Field	**Description**
Logic	Choose whether all conditions listed below are required to be matched or whether just one of them is enough. Select the logical expressions to make the conditions match. ▪ all conditions: means all conditions must be taken into account. ▪ any condition: means at least one condition must be taken into account. and ▪ no exception: means there is no exception to make the condition match. ▪ all exceptions: means all exceptions must be taken into account. ▪ any exception: means at least one exception must be taken into account.
Conditions List	List of conditions you added by clicking on the Add button. See description in Table 49 "Add New Condition/Exception".
Exceptions List	List of exceptions you added by clicking on the Add button. See description in Table 49 "Add New Condition/Exception".

Table 49 Add New Condition/Exception

Field	**Description**
Type of condition	Specify the type of conditions/exceptions: either specific fields or TIBCO LogLogic® Taxonomy.
Multiple selector	There are two options: “any value of this field” and “all values of this field.” Select “any value of this field” when it suffices for only one element in the field to match the Matching Value. Select “all values of this field” when all elements in the field must match the Matching Value.
Matching field	Select which field in the event is to be checked. If you select a TIBCO LogLogic® Taxonomy matching field, ONLY a number (or ID) found in the relevant ruleset file and corresponding to the Taxonomy field can be entered in the **Matching Value** field below. A text string will not be taken into account.
Negate	If set, the logic is reversed - e.g., to look for events which is not authentication.
Matching type	Specify which type of test is to be performed.
Matching Value	Specify the value to be tested. ▪ Additional data: you must specify the value with the following format: `“my addData meaning=my addData value”.` For a test of authentication: `“rulesetName=esmp_auth.rules”` ▪ DetectTime: the format is Tue May 13 11:50:06 CEST 2008. To search correlated alerts on a specific date: ".* May 13 .* 2008".
TIBCO LogLogic® Taxonomy	Select the necessary fields based on the TIBCO LogLogic® Taxonomy.

Processing tab

Define the action to perform when the event is matched.

Table 50 Aggregation - Processing Tab

Options	**Description**
Rule action	
discard	No aggregated event must be created
do not aggregate	Allows the creation of an aggregated event with only one event
aggregate	Aggregates matched events. This option activates the **Groups, Threshold** and **Fusion/ Redefine** tabs.
Elementary event storage	
delete elementary event	Check this option to delete the elementary event

Groups tab

To define how data will be grouped.

Table 51 Aggregation - Groups Tab

Field	**Description**
Field	Field to group. Click on **(none)** to add a field to group. See the description of this option in Table 52 "Group Field".
Required	Indicate if null values are considered.
Split multi-valued field	Indicate if multi-value fields must be split or not.
Move Down button	Indicate if the selected rule must be processed before the other ones.
Move Up button	Indicate if the selected rule must be processed after the other ones.
Delete button	Delete the selected rule.

Table 52 Group Field

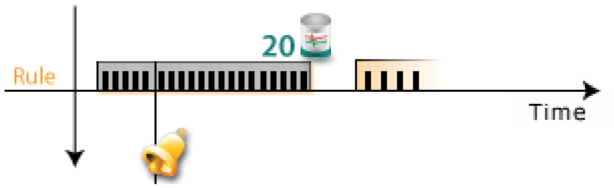
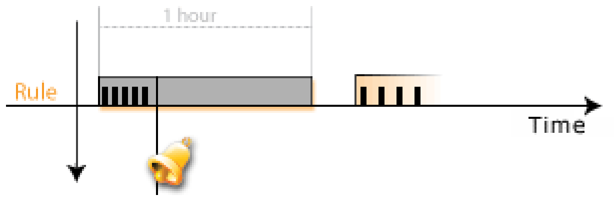
Field	**Description**
Field Name	Allows the selection of the name of the field on which the grouping is performed. Refer to the ***Default Content*** section in the Reference Guide to get the full list of grouping fields.
Field's Value Required	Select the **Field's value Required** checkbox if only events with a defined field's value must be grouped.

Threshold tab

The threshold tab allows you to specify under which conditions a rule should be triggered, that is, to combine events into a single event. For example, the number of events that have to occur within a specified time period could be set as a condition. If this condition was met, the events would be combined into a single event. This allows you to reduce the number of alerts displayed on the dashboard.

Note that when you select several checkboxes, it means that you define several possibilities to stop the aggregation process. They are not combined.

Table 53 Aggregation - Threshold Tab

Property	**To specify...**
Stopping Threshold	
Group size	The maximum number of events to group into a single event/alert. If matching events are received after the maximum threshold has been reached, then a new event is created. By default, the maximum number of events is set at 10000. Example with a group size set at 20: 
Duration	The time frame (in seconds) for considering an event or alert for aggregation or correlation in a specific event/alert. For example, you could specify that an event or alert would not accept any further events/alerts 10 seconds after its creation. By default, the duration is set at 3600. Example with a duration set at 3600: 

Fusion / Redefine tab

This tab allows you to modify the default characteristics of an event to aggregate.

Table 54 Aggregation - Fusion/Redefine Tab

Field or Option	**Description**
Redefine	
Event name	A default event's name can be modified by entering a new name in this field. All characteristics are fused no matter the event is overwritten or not.
TIBCO LogLogic® Taxonomy	Select the categories that can be used to match this new event, with other rules which match by categories.
Severity	A default event's severity can be modified by selecting another severity.
Fusion	
sources/targets	Indicate which target or source to melt with the default event.

Chapter 3 - Event Management Menu

The Event Management menu includes the following menu items:

- "Monitor..."
- "Advanced Configuration of Security Levels and Configuration Profiles"
- "Correlation Policy"

Monitor...

The TIBCO LogLogic® SEM includes an Event Management module with a real-time display of events, alerts and incidents. With this module you can configure the display of events, alerts and incidents according to their critical priority. Among the key functions available, you can:

- Apply user-defined filters to configure the display.
- Inspect further levels of data detail contained in each event, alert and incident.
- Search data using a variety of criteria.

Events

Use the Event screen to monitor elementary or aggregated events.

Table 55 List of events - column description

Information	Description
Severity	The events are displayed with an icon that corresponds to the severity level. The severity is based on the severity defined in the log.
📈	Allows you to display the elementary events associated to the incident.
Description	Below the title, a description of the event in the standardized TIBCO LogLogic® format is displayed.
Source	Display the sources involved in the generation of the event.
Target	Display the targets involved in the generation of the event.
Log Source	Display events in alphabetical order according to the Log source name.
Detected	Display events according to the time when the event has been detected by the Log Collector.

To view the list of events, either click on the Events tab or go to Event Management > Monitor > Events.

Event Details Tabs

To display the details of an event, click on the **Description** title.

Note: If you click on an elementary event, the **Events** tab is not available.

Table 56 Event Details - Tabs

Tab	Description
Summary	This tab gives general information about the event. **Impacted Assets** It lists the target assets (defined in the Asset Database) on which the event has been detected. **Aggregation Info** It gives the number and type of aggregated events. A link displaying the edition pane of the rule which aggregated the event is available. **Involved Log Sources** It gives names and numbers of the log sources that received the event. **Timeline** It gives the time progress of the event: ▪ The time and date when the event has been detected by the log source. ▪ The time and date when the event has been stored in database. ▪ The time and date when the event has been correlated by the correlation engine.
History	This tab gives information about the event history per days. You know when: ▪ the first event has been detected. ▪ the last event has been detected. ▪ the alert got out of the correlation engine. ▪ the last event has been added. You can also know how many aggregated events the event contains.

Table 56 Event Details - Tabs

Tab	Description
Details	This tab gives the following information: **Impact assessment** It lists the type, severity and description of the event. TIBCO LogLogic® Taxonomy It gives the elements of construction for the TIBCO LogLogic® Taxonomy applied to the event. **References** It lists references such as where more information can be obtained, e.g. references to external web sites including product vendors, internal intranet pages, bug databases, and vulnerability databases. **Additional Data** It displays raw IDMEF parameters. **Alerts** It indicates the alerts (name and ID number) that contain the current aggregated event. **Open IDMEF event (XML document)** This link is only available if the event is an event standardized in the IDMEF format
Sources/Targets	This tab gives **Sources** and **Targets** details. **Source**: Address, Host, Interface, Process, Service, User and Web services. **Target**: Address, Host, Interface, Process, Service, User, Web services and File. See Table 58 "Event - Target and Source" for more details on the icons referring to sources and targets. **Note:** No more than 200 sources and/or targets can be displayed.
Events [only displayed for an aggregated event]	This tab gives a part of the list of the elementary events which compose the current aggregated event. Click on the hyperlink to display in a new tab the whole list of elementary events which compose the current aggregated event.
Raw Logs	This tab gives information about the number of online raw logs, i.e. the first 5 raw logs online, the last 5 raw logs online and a link to the list of all raw logs online. Click on the link to display all the online raw logs in a new tab. **Note:** an online raw log is a raw log that has been archived but not retrieved in the application.

Severity Levels

The following table displays the various severity levels and their corresponding icons.

Table 57 Event - Severity Levels and Corresponding Icons

Severity Level	Elementary Event	Aggregated Event
High	🟥	🟥
Medium	🟧	🟧
Low	🟩	🟩
Info	i	i
Unknown	?	?

Source/Targets Icons

The following table gives a description of the various icons that can be found in the Sources/ Targets tab.

Table 58 Event - Target and Source

Icon	Description
@	***Address*** E-mail address.
◆	***File*** [For Target only] If the object is a file or directory (e.g. for alerts involving access failures) its name can be used in the filter.
◆	***Host*** ▪ an IP address in dotted decimal format (1.2.3.4). ▪ a host name. ▪ an IP address in dotted decimal format with a country code. e.g. [fr] 192.53.21.23. ▪ a host name with a country code. e.g. [fr] hostname. If you are expecting a dns to be displayed, you must wait for a while then refresh the page manually.
◆	***Interface*** Network interface. e.g. eth0, eth1...etc
◆	***Process*** The process name (e.g. sshd or IEXPLORE.EXE).

Table 58 Event - Target and Source

Icon	Description
◆	*Service* ▪ Name of the service. ▪ Service protocol: the protocol being used (e.g. TCP or UDP). ▪ Service port: the number of the TCP or UDP port used by the service.
◆	*User* ▪ User name (e.g. root or Administrator). ▪ User identifier (e.g. 0).
◆	*Web services* ▪ Web service URL. ▪ Web service CGI program name included in the URL. ▪ Web service arguments passed to a CGI program.

Alerts

Use the **Alerts** screen to monitor alerts.

Table 59 List of alerts- column description

Information	Description
Severity	The alerts are displayed with an icon that corresponds to the severity level. The severity is based on the severity defined in the event or in correlation rules.
	Allows you to display the aggregated events associated to the alert. You can also display the elementary events included in the aggregated event.
Description	Below the title, a description of the alert in the standardized TIBCO LogLogic® format is displayed.
Source	Display the sources involved in the generation of the alert.
Target	Display the targets involved in the generation of the alert.
Log Source	Display alerts in alphabetical order according to the Log source name.
SLA (Service Level Agreement)	Indicates the maximum delay (in minutes) for an alert to be acknowledged. It takes into account the severity of the alert, the criticality on the impacted machine, the current security level and the working hours of the security analyst.
Detected	Display alerts according to the time when the alert has been created from an event.

To view the list of alerts, either click on the Alerts tab or go to **Event Management > Monitor > Alerts**.

Alert Details Tabs

To display the details of an alert, click on the **Description** title.

The following table describes the various tabs of the **Alert Details** screen.

Table 60 Alert Details - Tabs

Tab	Description
Summary	This tab gives general information about the event. **Impacted Assets** It lists the target assets (defined in the Asset Database) on which the alert has been detected. **Correlation Info** It gives the number and type of aggregated events used to generate the alert. A link displaying the edition pane of the rule which correlated the alert is available **Involved Log Sources** It gives numbers and names of the log sources that received the event on which the alert is based. **Acknowledgement** It gives information whether the alert has been acknowledged within the SLA time frame or not. **Timeline** It gives the time progress of the event on which the alert is based: ▪ The time and date when the event has been detected by the log source. ▪ The time and date when the event has been stored in database. ▪ The time and date when the alert has been acknowledged. ▪ The time and date when the event has been correlated by the correlation engine.
History	This tab gives information about the event history per days. You know when: ▪ the first event has been detected. ▪ the last event has been detected. ▪ the alert got out of the correlation engine. ▪ the last event has been added. You can also know: ▪ how many events this event contains. ▪ SLA details (respected or not). ▪ the rule used for the alert generation.

Table 60 Alert Details - Tabs

Tab	Description
Details	It lists references such as where more information can be obtained, e.g. references to external web sites including product vendors, internal intranet pages, bug databases, and vulnerability databases. **Name** Gives the name of the alert. TIBCO LogLogic® Taxonomy It gives the elements of construction for the TIBCO LogLogic® Taxonomy applied to the event. Impact Assessment It lists the type, severity and description of the alert. **Additional Data** It displays raw IDMEF parameters. **Incidents** It indicates the incident linked to the alert. **Alerts** It indicates the alerts (name and ID number) that contain the current aggregated event. **Open IDMEF event (XML document)** This link is only available if the event is an event standardized in the IDMEF format.
Sources/Targets	This tab gives **Sources** and **Targets** details. **Source** Address, Host, Interface, Process, Service, User and Web services. **Target** Address, Host, Interface, Process, Service, User, Webservice and File. See Table 61 "Alert - Target and Source" for more details on targets and sources.
Alerts/Events	This tab gives a part of the list of the alert/events which compose the current aggregated event. Click on the hyperlink to display the whole list of events which compose the current alert in a new tab.

Sources/Targets Icons

The following table gives a description of the various icons that can be found in the Sources/ Targets tab.

Table 61 Alert - Target and Source

Icon	Description
@	***Address*** E-mail address.
◆	***File*** [For Target only] If the object is a file or directory (e.g. for alerts involving access failures) its name can be used in the filter.
◆	***Host*** - an IP address in dotted decimal format (1.2.3.4). - a host name. - an IP address in dotted decimal format with a country code. (e.g. 192.53.21.23 [fr]). - a host name with a country code (e.g. hostname [fr]). **Note:** If you are expecting a dns to be displayed, you must wait for a while then refresh the page manually.
◆	***Interface*** Network interface. (e.g. eth0, eth1...etc).
◆	***Process*** The process name (e.g. sshd or IEXPLORE.EXE).
◆	***Service*** - Name of the service. - Service protocol: the protocol being used (e.g. TCP or UDP). - Service port: the number of the TCP or UDP port used by the service.
◆	***User*** - User name (e.g. root or Administrator). - User identifier (e.g. 0).
◆	***Webservice*** - Webservice URL. - Webservice CGI program name included in the URL. - Webservice arguments passed to a CGI program.

SLA Icons

The SLA time limit is represented by an icon in the list of alerts. The icon is different according to criticality or type of period.

For example,

The following table gives a description of the various icons that can be found regarding SLAs.

Table 62 Types of SLA

Day	Hour	Minute	Out of SLA	More than 6 days	Acknowledged within the SLA period	Acknowledged out of the SLA period
D or D	H	M	⚠	D+	✓	✓⚠

Incidents

Use the **Incidents** screen to monitor incidents.

To view the list of incidents, either click on the Incidents tab or go to **Event Management > Monitor > Incidents**.

Incidents Tabs

The following table describes the various tabs of the list of **Incidents**.

Table 63 List of incidents- column description

Information	Description
Severity	The incidents are displayed with an icon that corresponds to the severity level. The severity is based on the severity defined in the alert.
🔔	Allows you to display the alerts attached to the incident.
Description	Below the title, a description of the incident in the standardized TIBCO LogLogic® format is displayed.
Impacted assets	Allows you to get the list of assets associated with targets and sorted by descending criticality order.
Actions	Allows you to get the list of actions performed or not performed on an incident.
React	Allows you to display the expected actions to perform to avoid the attack. You just need to click on the red button to synchronize with the **Solsoft ChangeManager** application.
SLA (Service Level Agreement)	Indicates the maximum delay (in minutes) for an incident to be closed. It takes into account the severity of the incident, the criticality on the impacted machine, the current security level and the working hours of the security analyst.
Modified	Allows you to view the person who modified the incident and the time when it was modified.

Event Details Tabs

To display the details of an incident, click on the **Description** title.

General	This tab gives general information about the incident. **Incident title and description** Short description of the incident. This will be used in the incidents list along with an incident number. **Status** It says if the incident is open or closed. **Contacts** Users who will handle this incident. **Detection and Start time** Time and date when the incident was detected and created. **Log Sources** Log sources that generate the alert. **Current SLA** Timeframe within which the incident has to be closed **Severity** Indicates the severity level. **Category** Indicates the category of the event. **Confidence** Gives a percentage representing the analyzer's best estimate of the analysis' validity. **Completion** Indicates if the alert is successful or not. **Type** Indicate the type of incidents.

Table 64 Incident Details - Tabs

Tab	Description
Properties	**Confidentiality lost** Whether the incident includes a breach of confidentiality, e.g. a database has been accessed by an unauthorized user. **Integrity lost** Whether the incident has resulted in unauthorized changes, e.g. an unauthorized user has changed a database record. **Availability lost** If the incident has resulted in a service or asset not being available, set this field to Yes. **Severity** Severity of this particular event: info, low, medium, high. **Value** Time value during which the incident (e.g. a machine shutdown) lasts. **Metric** (or type) Defines the type of time it is: labor, shutdown or elapsed. **Units** seconds, minutes, hours or days. **Severity** Select the severity of this particular event: info, low, medium, high. **Value** Value corresponding to the amount the incident will cost. **Currency** Currency corresponding to the value entered: dollar, euro, pound. **References** It gives information to make a link with online vulnerability database.
Sources/Targets	This tab gives **Sources** and **Targets** details. **Source**: used to select the incident source(s). **Target**: used to select the incident target(s).
Attack Methods	Indicate if the incident involves any attacks (malicious or otherwise). See the section "Create Incidents Manually" in the User Guide for detailed information.
Actions	Allows you to specify which remedial actions are required for this incident.
History	Gives information about the previous actions performed on this incident.

Incident Severity Levels

The following table displays the various incident severity levels and their corresponding icons.

Table 65 Incident - Severity Levels and Corresponding Icons

Severity Level	Closed Incident	Opened Incident	Processed Incident	Reopened Incident
High	✓🟥	🟥	🟥	🟥
Medium	✓🟧	🟧	🟧	🟧
Low	✓🟩	🟩	🟩	🟩
Info	✓i	i	i	i
Unknown	✓?	?	?	?

Advanced Configuration of Security Levels and Configuration Profiles

Security Levels

Use the Security Levels screen to specify which configuration profiles are active and when they are active.

To access the **Security levels** screen, go to **Event Management > Advanced > Security Levels.**

Description

The characteristics of this screen are described in the following table

Table 66 Security Level

Parameter	Description
Activate	Activates the selected security level. Only one security level can be active.
Move	Moves a security level order the display.
Copy	Copies a security level. It is useful if you want to create a security level with the characteristics based on the standard one.
Delete	Deletes the selected security level.
Add	Adds a new security level.
#	Sorting order of the security level.
Name	Name of the security level.
Description	Description of the security level.
Active	Indicates with a green tick which security level is active.

Security Levels Edition

Once you have clicked on a security level, the following screen is displayed.

Description

The characteristics of this screen are described in the following table

Table 67 Security Level

Parameter	**Description**
Security Level	Description giving the purpose of the security level in the **Description** field.
Time Ranges	Allows the creation of a time range for each block of hours specifically related to the configuration profiles, e.g., a different time range for **office hours**, **night time,** and **weekend**.
Hours Diagram	The Hours Diagram shows when each profile is active. The key at the bottom of the table lists the profiles with their corresponding colors.

Configuration Profiles

Use the configuration profile screen to monitor configuration profiles, i.e. configure the configuration profiles to be used, lock, unlock and delete them if necessary.

To display the **Configuration Profiles** screen, go to **Event Management > Advanced > Configuration Profiles**.

Possible Actions

Table 68 Possible Actions

Action	**Description**
Lock/Unlock	To specify which Configuration Profile is to be used and to lock that setting so no automatic switching between profiles occurs, tick the desired profile and click **Lock**. If a configuration profile is locked in place, to return to automatic switching based on time of day, click **Unlock**.
Delete	To delete configuration profiles, select them by ticking the relevant checkboxes and then click **Delete**.
Copy	Select one configuration profile by ticking the relevant checkboxes and click **Copy** to add a new configuration profile with the same attributes.
Add	To add a new configuration profile.
Edit	Click the name of the configuration profile to edit it.

Configuration Profile Edition

Use the **Configuration Profile** screen to edit a selected profile.

Table 69 Configure Profile Edition Fields

Field	**Description**
Name	Specify a unique name for the profile, e.g., "Weekend profile".
Description	Enter a brief description, such as when the profile is to be applied.
SLA	Select the SLA that must be applied to the profile.
Rule names	Select the rules which should be active when this profile is active by clicking **Change**. The rules displayed in this pane are the following: ▪ Correlation rules and scenarios. ▪ Aggregation rule.

Correlation Policy

Use the Correlation Policy screen to monitor the correlation rules that must be applied on the events processed by the SMP.

To access the **Correlation Policy** screen, select E**vent Management > Correlation Policy**.

Description

The characteristics of this screen are described in the following tables.

Rules Tab

Table 70 Correlation Policy

Item	Description
Checkbox	Allows an action to be performed on the selected rule.
#	Position number of the rule.
Name	Name of the rule.
Start/Stop thresholds	The **threshold** is the number of times the rule must be matched for the action(s) to be performed. The **duration** is the maximum number of seconds between events that will trigger the rule.
Actions	A list of the actions to be performed if the rule is triggered.
Stop	If set, the event's processing stops after the triggering of the rule. Otherwise, the event is processed by subsequent rules. **Note:** This option becomes active only when the rule has matched the conditions/ exceptions and threshold.
Profiles	Whether the rule is active or inactive and which configuration profiles contain this rule. A configuration profile shown with a red cross does not contain the rule and a configuration profile shown with a yellow tick indicates the rule is used in said profile.

Note: Please refer to the "List of Correlation Rules" in the *Appendix* to get the list of the standard correlation rules.

Scenarios Tab

The list of scenarios is displayed under the **Scenarios** tab. The scenarios are processed in the order listed. The **Scenarios** list displays the following key information.

Table 71 Correlation - Correlation Action Tab

Field	Description
Checkbox	Allows an action to be performed on the selected scenario.
#	Position number of the scenario.
Name	Name of the scenario.

Table 71 Correlation - Correlation Action Tab

Field	Description
Rules	Rules that make up the scenario, can be: ▪ required. ▪ optional. ▪ excluding (if the rule is triggered, the scenario is not triggered).
Actions	A list of the actions to be performed if the scenario is triggered.
Profiles	Whether the rule is active or inactive and which configuration profiles contain this rule. A configuration profile shown with a red cross does not contain the rule and a configuration profile shown with a yellow tick indicates the rule is used in said profile.

Note: Please refer to the "List of Rules for Scenarios" in the *Appendix* to get the list of the standard incident rules.

When clicking on a correlation rule's name (**Rules** tab), the rule edition window is displayed.

General tab

The **General** tab displays several fields described in the table below.

Table 72 General Tab

Field	Description
Id	Every rule is given a unique id by the Security Management Platform.
Name	Every rule requires a unique name, specified by the administrator who creates it.
Description	User-entered description of the rule.
Stop evaluation after this rule	If ticked, and the event is matched by this rule, the event is not processed by subsequent rules. This is referred to as "cut" in the rule list.
Creation	The date and time that the rule was created and which user created it.
Last	The date and time the rule was last d and which user d it.
Profiles	Select in which security profiles this rule is active. See sub-section "Advanced Configuration of Security Levels and Configuration Profiles" for further information.

Conditions tab

Multiple conditions can be required to trigger the rule, add as many as required.

Exceptions are used to avoid triggering the rule when specified events occur. Specify exceptions in the same way as conditions.

Table 73 Logical Expression

Column	Description
Logic	Choose whether all conditions listed below are required to be matched or whether just one of them is enough. Select the logical expressions to make the conditions match. ▪ all conditions: means all conditions must be taken into account. ▪ any condition: means at least one condition must be taken into account. and ▪ no exception: means there is no exception to make the condition match. ▪ all exceptions: means all exceptions must be taken into account. ▪ any exception: means at least one exception must be taken into account.
Conditions List	List of conditions you added by clicking on the Add button. See description in Table 74 "Add a New Condition/Exception".
Exceptions List	List of exceptions you added by clicking on the Add button. See description in Table 74 "Add a New Condition/Exception".

Groups tab

To define how data will be grouped.

Table 74 Add a New Condition/Exception

Field	Description
Type of condition	Specify the type of conditions/exceptions: either specific fields or TIBCO LogLogic® Taxonomy.
Multiple selector	There are two options: “any value of this field” and “all values of this field.” Select “any value of this field” when it suffices for only one element in the field to match the **Matching Value**. Select “all values of this field” when all elements in the field must match the Matching Value.
Matching field	Select which field in the event is to be checked. If you select a TIBCO LogLogic® Taxonomy matching field, ONLY a number (or ID) found in the relevant ruleset file and corresponding to the Taxonomy field can be entered in the **Matching Value** field below. A text string will not be taken into account.
Negate	If set, the logic is reversed - e.g., to look for events which is not authentication.
Matching type	Specify which type of test is to be performed.
	Specify the value to be tested. ▪ Additional data: you must specify the value with the following format: `“my addData meaning=my addData value”`. For a test of authentication: `“rulesetName=esmp_auth.rules”` ▪ DetectTime: the format is Tue May 13 11:50:06 CEST 2008. To search correlated alerts on a specific date: ".* May 13 .* 2008".
TIBCO LogLogic® Taxonomy	Select the necessary fields based on the TIBCO LogLogic® Taxonomy.

Table 75 Groups Tab

Column	Description
Field	Field to group. Click on **(none)** to add a field to group. See the description of this option in Table 76 "Group Field".
Required	Indicate if null values are considered.
Split multi-valued field	Indicate if multi-value fields must be split or not.
Move Down button	Indicate if the selected rule must be processed before the other ones.
Move Up button	Indicate if the selected rule must be processed after the other ones.
Delete button	Delete the selected rule.

Table 76 Group Field

Field	Description
Field Name	Allows the selection of the name of the field on which the grouping is performed. Refer to the ***Default Content*** section in the Reference Guide to get the full list of grouping fields.
Field's Value Required	Select the **Field's value Required** checkbox if only events with a defined field's value must be grouped.
Grouping method	This information allows the creation of **one group** containing different elements from several incoming events. You can choose among the options described below: ▪ **same field values:** grouping is performed if at least one event field's value is the same as another one from a different event. ▪ **same split field values**: the principle of this grouping method is the same as that of the **same field values** option except that only the common value between several event's fields is kept as reference for the creation of a group. ▪ **distinct field values**: grouping is performed by adding all the different field's values from several events into only one group.
Minimum number of distinct values	If you selected **distinct field values**, this field is displayed. Enter the minimum number of fields to add in the group allowing the creation of an alert.

Threshold tab

The threshold tab allows you to specify under which conditions a rule would be triggered, that is, to combine events into a single event.

For example, the number of events that have to occur within a specified time period could be set as a condition. If this condition was met, the events would be combined into a single event. This allows you to reduce the number of alerts displayed on the dashboard.

The threshold properties are the following:

Note that when you select several checkboxes, it means that you define several possibilities to stop the aggregation process. They are not combined.

Table 77 Correlation - Threshold Tab

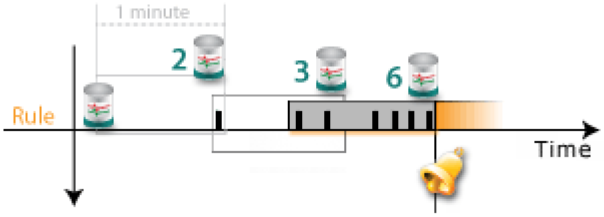
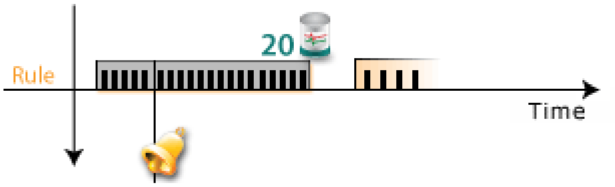
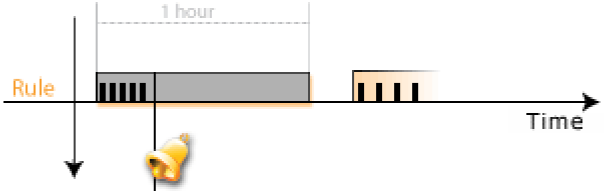
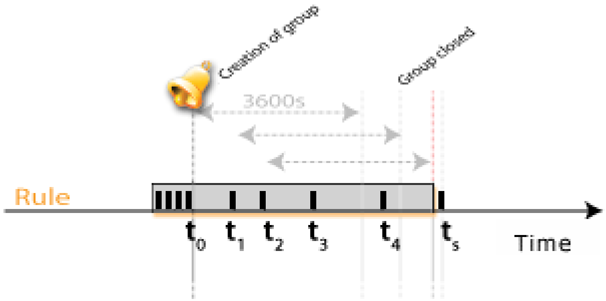
Property	To specify...
[correlation rule only] Starting Threshold	
Rate	The minimum number of events per defined interval (per second) needed to trigger a correlation process. Example with a rate set at 6/3600: 
Stopping Threshold	
Group size	The maximum number of events to group into a single event/alert. If matching events are received after the maximum threshold has been reached, then a new event is created. By default, the maximum number of events is set at 50000. Example with a group size set at 20: 

Table 77 Correlation - Threshold Tab

Property	To specify...
[correlation rule only] Starting Threshold	
Duration	The time frame (in seconds) for considering an event or alert for aggregation or correlation in a specific event/alert. For example, you could specify that an event or alert would not accept any further events/alerts 10 seconds after its creation. By default, the duration is set at 3600. Example with a duration set at 3600: 
[correlation rule only] Rate	The maximum number of events per defined interval (per second) needed to stop an aggregation or correlation process. Example with a group size set at 4/3600:  Creation of group Group closed 3600s Rule t0 t1 t2 t3 t4 t5 Time

Actions tab

You must select what to do if the rule is triggered.

Table 78 Actions

Checkbox	Description
Create an alert	Creates an alert when the rule is triggered. Activates the "Correlation Action tab".
Change the event severity	Changes the event severity when the rule is triggered. Only available if the **Create an alert** checkbox is NOT selected. Activates the "Severity tab".
Send the event/alert to another SMP	Sends an alert or event from one SMP to another one if you installed multiple SMPs. Activates the "Send tab".
Use an external command	Specifies the command to execute. The command will run in the context of the "TIBCO LogLogic®" account on the Security Management Platform. Activates the "Execute tab".
Mail the event to contacts	Defines the group of contacts to whom you will automatically send an E-mail regarding the event. Activates the "Send Mail tab".

Table 78 Actions

Checkbox	Description
Send an event/alert as a SNMP trap	Generates an SNMP (Simple Network Management Protocol) trap and sends it to a specified IP address or host name. Activates the "Send Trap tab".
Auto-acknowledge the alert	Acknowledges an alert that will not be listed on the “current alerts” display. Auto-acknowledged alerts are typically archived for future forensic work. Only available if the **Create an alert** checkbox is selected. Activates the "Acknowledge tab".
Create an incident	Creates automatically an incident from the alert. Activates the "Incident tab".
Linked to a scenario	If a rule is already allocated to a scenario, the **Linked to a scenario** checkbox is automatically selected and a pane with the name of the scenario is displayed. Activates the "Scenario tab".

General Behaviors

If you select the **Create an alert** checkbox along with another possible action, the action will be performed on the alert only once.E.g. Let us suppose the expected action is **Use an external command**. If a correlation alert is created, the script will be executed once (and only once) when the alert is created.

If you do NOT select the **Create an alert** checkbox but a possible action, then the action will apply on all the aggregated events each time conditions are matched.

E.g. Let us suppose the expected action is **Use an external command**. When the rule is triggered, the script will be executed as many times as the number of aggregated events contained in the aggregate (e.g. threshold set to 10 events: when the rule is triggered, the script is executed 10 times).

Correlation Action tab

Table 79 Correlation Action tab

Field	Description
Alert name	The text string that will be displayed on the alerts screen.
TIBCO LogLogic® Taxonomy	Select the categories that can be used to match this new alert, with other rules that match by categories. If you selected TIBCO LogLogic® Taxonomy **- (all fields)** in the **Groups** tab, the TIBCO LogLogic® Taxonomy checkbox is automatically selected.
Severity	Select the severity of the new alert.
Reinject the alert into the correlator	Indicate if the alert must be processed again.
Fields	Specify the fields that will be available for correlation.

Severity tab

Table 80 Severity tab

Field	Description
From severity 'info' to	Changes an event with a severity ‘info’ into an event with a new severity, either: - high - low - medium
From severity 'low' to	Changes an event with a severity ‘low’ into an event with a new severity, either: - high - info - medium
From severity 'medium' to	Changes an event with a severity ‘medium’ into an event with a new severity, either: - high - info - low
From severity 'high' to	Changes an event with a severity ‘high’ into an event with a new severity, either: - info - low - medium

Send tab

Table 81 Send tab

Field	Description
Servers	Select the target server. In the event of a multiple instances configuration when several SMPs are connected, you can automatically send an event/alert to another SMP. Please refer to the ***Administration Guide*** for more information about the communication between several SMP servers.

Execute tab

Table 82 Execute tab

Field	Description
Command to execute	The name of the file in which the command is executed (for example `comman`

Note: The SMP is executing external scripts with TIBCO LogLogic® user rights.

Send Mail tab

Caution: The default *.properties files that contain all the mail sending process configuration data must have been configured. Refer to the Administration Guide to learn how to precisely configure the sending of the mail (see Sending Mails as Soon as an Event Occurs section).

Table 83 Send Mail tab

Field	Description
Subject	Enter the e-mail subject.
Additional comment	Enter the e-mail comment.
Contacts assigned to the source	Select the contacts assigned to the source. You can configure these contact groups under the **Asset Database > Contact Groups** screen.
Contacts assigned to the target	Select the contacts assigned to the target. You can configure these contact groups under the **Asset Database > Contact Groups** screen.
Contacts assigned to the equipment	Select the contacts assigned to the equipment. You can configure these contact groups under the **Asset Database > Contact Groups** screen.
Other contacts	Select the contacts assigned to other contacts. You can configure these contact groups under the **Asset Database > Contact Groups** screen.

Send Trap tab

To generate an SNMP (Simple Network Management Protocol) trap and send it to a specified IP address or host name.

Table 84 Send Trap tab

Field	Description
* SNMP server	IP address in dotted decimal format or the host name of the system to which you want to send an SNMP trap when an associated event occurs.
Community	Community name used by the destination host in the **Community** field. By default, the value is set to “public”. It corresponds to the default installed account.
Port	Port to which the **SNMP** server listens to.

Acknowledge tab

To acknowledge an alert automatically.

Table 85 Acknowledge tab

Field	Description
Category	Type of alert. This field is used by the reporting module to show what type of alerts are being generated.
Redefined Severity	Severity for the alert. This will lower the confidence rating in the analyzer.
Comment	Comment regarding the alert and the auto-acknowledgement.

Incident tab

Caution: Make sure you only have a limited number of incidents. Otherwise, the correlator may be slow in processing the alerts.

The new alert can automatically create an incident with the following properties:

Table 86 Incident Tab

Field	Description
Incident title	The title is displayed in the list of incidents and is used to reference the incident.
Incident category	Select the incident’s category.

Table 86 Incident Tab

Field	Description
Incident description	Space for a description of the alert and why an incident was automatically created.
Incident contact	Select the previously defined contact to be marked as responsible for handling the incident.
Update incident every (alerts)	To send an update to the Incident Management System every X alerts (i.e., to avoid sending a modification each time the incident is updated). The default value is 1000. **Note:** If the value is set to 1, the correlator may be slow in processing the alerts: they will be processed one by one.
Add log source contacts	If selected, the contacts responsible for the log source device will also be marked as responsible for the incident.
Add source contacts	If selected, the contacts responsible for the source host of the alert will also be marked as responsible for the incident.
Add target contacts	If selected, the contacts responsible for the target host will also be marked as responsible for the incident.
Severity	Select the severity level of the incident; leave blank to use the severity level of the alert.
Switch source and target node	Tick this box if the event's source should be recorded as the incident's target and vice versa.
Switch source and target service	Tick this box if the event's source should be recorded as the incident's target and vice versa.
Assign fields	Select which fields are passed as details.
What if incident is closed?	Select the type of scenario that should be applied if the incident is closed when new alerts are received: ▪ create a new incident in which the alerts will be stored ▪ add new alerts to the same incident even if it is closed ▪ add new alerts in the re-opened incidents ▪ keep as it is and lose the alerts.

Scenario tab

If a rule is already allocated to a scenario, the **Linked to a scenario** checkbox is automatically selected and a pane with the name of the scenario is displayed, such as in the example below.

Chapter 4 - Reporting Menu

The **Reporting** menu is composed of three main modules:

- Security Dashboards
- Live Reporting Policy
- Batch Reporting Policy

Security Dashboards

Please refer to the Security Dashboards section in the User guide.

You will find the list of available predefined dashboards in the List of Predefined Dashboards section and the list of reports related to the predefined dashboards in the List of Reporting Tables section.

Characteristics

Icons

The dashboard interface is composed of several icons.

Table 87 Dashboard Icons

Icons	Description
⇨	Deploys the menu on the left-hand side.
⇦ ⇨	Browses dashboards of the same type but based upon different time measures (hour, day or month).
⟳	Refreshes the page display (or solely the report if the icon is in the **Description** box).
📄	Prints the dashboard (or solely the report, if the icon is in the **Description** box) in PDF format.
⇥	Displays the **Filter** screen.
✎	Customizes the report.
📊	Sends the report data in MS Excel.
▭	Displays the corresponding report configuration.
▢	Maximizes the report display.
❐	Restores the report display.

Note: The security dashboard is continuously displayed. The user cannot log out from the reporting interface unless the application is displayed on an another workstation or if the user session has expired.

Menu

The security dashboard interface contains a menu on the left-hand side that you can display by clicking on the icon.

This menu is the main entry to all the actions available.

Figure 12 Dashboard Menu

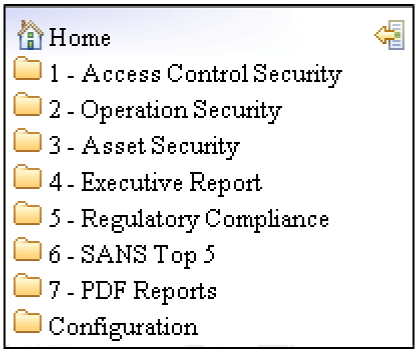


Table 88 Menu Entries

Entry	Description
1 - Access Control Security	Displays the list of predefined dashboards based upon reports about data access security.
2 - Operation Security	Displays the list of predefined dashboards based upon reports about operation security.
3 - Asset Security	Displays the list of predefined dashboards based upon reports about asset security.
4 - Executive Report	Displays a unique dashboard of several pages containing all the reports from groups 1, 2 and 3.
5 - Regulatory Compliance	Displays the list of predefined dashboards sorted out by regulatory compliance.
6 - SANS Top 5	Displays the list of predefined dashboards based upon the Top-5 vulnerabilities identified by the ***SANS Institute***.
7 - PDF Reports	Folders where standards and regulations reports are automatically generated in PDF format each month.
Configuration	Allows the access to the interface configuration: ▪ Administration: configuration of general preferences (display, user rights...etc). ▪ Control: creation of a task to monitor data. ▪ External Session: allows the creation of a web page which is not created with the help of the portal. It can be any source outside of the application like an existing intranet site, a web site, or any file readable with your web browser. ▪ Hidden: displays the list of reports. ▪ Report: creation and modification of reports. ▪ Strategy map: creation of strategy maps. ▪ Task: definition of starting tasks in batch mode. This is useful if you need to start a task at a precise moment that will automatically generate reports.

Notions

In this part of the documentation, you will find the following terms specific to the reporting engine.

Table 89 Terms Specific to Reports Engine

Terms	Definition
Dashboard	Overall picture of a set of consistent reports.
Report	Graphical representation of the alerts, incidents or vulnerabilities.
Workspace	A user will only have access to the sessions and reports defined in the workspace s/he belongs to.
Session	Directory allowing the classification of the different menu items. You can add as many sessions as you want to the existing default session groups

Report Queries

You access the query configuration screen via the main menu by clicking on **Configuration > Report > Data Dictionary**.

Icons

Table 90 Query Icons

Icon	Description
📄	Adds a new query.
⇥	Applies a filter to the query list.
⟳	Refreshes the display.
✖	Deletes the corresponding query.
📋	Copies the corresponding query. This is useful if you need to create a new query that is similar to an existing one.
⚬	Displays the report(s) linked to the request.
💾	Saves data.
💾	Saves data and returns to the list of queries.
✖	Returns to the list of queries without saving any data.
📝	Displays a box where you can enter your comment.
⇥	Refreshes the SQL filter.
?	Displays a help field below the SQL field.
▭	Displays a preview of the SQL query result.
SQL	Edits the field for the SQL syntax.

Live Reporting Policy

Overview

Use the Live Reporting Policy screen to group data and generate customized reports.

To open the **Live Reporting Policy** screen, go to **Reporting > Live Reporting Policy**.

The list of default live reporting policies is available in section

Description

The characteristics of this screen are described in the following table.

Table 91 Live Reporting Policy

Item	**Functionality**
Enable button	Enables selected tables.
Disable button	Disables selected tables.
Copy button	Creates a copy of the definition of the selected table.
Delete button	Deletes selected tables (definition and SQL table are deleted).
Add button	Adds a new definition for a table. (See instructions below).
Selection Box	Click a selection box to select a table. Clicking on the top most box will select all tables (even those that are not displayed on the current page).
Name	Name of the reporting table. You can click on the name to edit and check the table's content but you cannot modify it. To modify a table, you must first copy the table.
Active	Possible statuses: ▪ Yellow check mark: table is active. ▪ Red X: table is inactive.

Live Reporting Rule Edition/Creation

Once you have clicked on the **Add** button, a screen composed of four tabs is displayed. This screen allows you to precisely define the live reporting rule you want to generate reports in real time.

Please refer to the Add a New Definition for a Table section in the user Guide to know how to create a table.

General tab

The characteristics of this tab are described in the following table

Table 92 Live Reporting rule - General tab

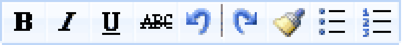
Item	**Description**
Id	Rule's unique identifier.
Name	Name of the rule.
Description	Description of the rule.
	Formatting bar to customize the description text.
Active	Defines if the rule is currently active or not.

Table 92 Live Reporting rule - General tab

Item	Description
Creation	Date of the rule's creation.
Last update	Date of the rule's last update.

Conditions tab

The characteristics of this tab are described in the following table.

Table 93 Live Reporting Rule - Conditions Tab

Item	Description
Logical Expression	Defines the condition and exceptions that should be met for the rule to be triggered. If you select all or any exceptions, the **Exceptions List** pane is displayed.
Add button (Conditions and Exceptions list)	Allows you to define the conditions and exceptions, either based on a specific field or on the TIBCO LogLogic® Taxonomy.
Delete button (Conditions and Exceptions list)	Allows the deletion of the selected condition and exception.
Checkbox	Allows the selection of the condition and exception to be deleted.

Groups tab

The characteristics of this tab are described in the following table.

Table 94 Live Reporting Rule - Groups Tab

Item	Description
Checkbox	Allows the selection of a field to be deleted, move down or up.
Field	Allows you to define the field to be aggregated into an event. Click on **(none)** to add a field to group. See the description of this option in Table 95 "Group Field".
Move Down button	Allows you to place a selected field down the other ones if you think the field should be grouped after the other ones.
Move Up button	Allows you to place a selected field over the other ones if you think the field should be grouped before the other ones.
Delete button	Allows you to delete the selected field.

Table 95 Group Field

Field	Description
Field Name	Allows the selection of the name of the field on which the grouping is performed. Refer to the ***Default Content*** section in the Reference Guide to get the full list of grouping fields.
Field's Value Required	Select the **Field's value Required** checkbox if only events with a defined field's value must be grouped.

Table Definition tab

The characteristics of this tab are described in the following table.

Table 96 Live Reporting Rule - Table Definition Tab

Item	Description
Time scales	Allows you to select the type of reports you want to monitor (**Hour, Day and Month** or **Day and Month** or **Month table** only).
Table name	Allows you to enter a customized name for the table. **Attention:** You cannot enter more than 35 characters.
Other generated tables	Gives example of the names of the other tables that will be generated based on the name entered in the **Table name** field.
Table structure	Indicates the structure of the table.

Batch Reporting Policy

Overview

Use the **Batch Reporting Policy** functionality to configure data groupings to later generate customized reports. The SMP **Batch Reporting Policy** functionality comprises several database tables and each table defines a certain configuration of data groupings.

To open the Batch Reporting Policy screen, go to Reporting > Batch Reporting Policy.

Description

The characteristics of this screen are described in the following table.

Table 97 Batch Reporting Policy

Item	Functionality
Create button	Creates one or more new SQL tables. Creating a table means that the SQL table will be created. However, it will not be filled with the latest alerts (see Generate below). The **Create** button will create a new SQL table in the database, whereas the **Add** button will simply add a new definition for a table. **Add** + **Create:** creates the definition and the SQL table. **Add** + **Generate:** creates the definition and the SQL table and then fills the table with the latest alerts.
Generate button	Generates selected tables. Generating a table means that the SQL table will be created and filled with the latest alerts.
Disable button	Disables selected tables. The selected tables won't be filled automatically every day/night.
Enable button	The selected tables will be filled automatically every day/night.
Add button	Adds a new definition for a table. The **Create** button will create a new SQL table in the database, whereas the **Add** button will simply add a new definition for a table. **Add** + **Create:** creates the definition and the SQL table. **Add** + **Generate:** creates the definition and the SQL table and then fills the table with the latest alerts.
Delete button	Deletes selected tables (definition and SQL table are deleted).
Copy button	Creates a copy of the definition of the selected table.
Selection Box	Click a selection box to select a table. Clicking on the top most box will select all tables (even those that are not displayed on the current page).
Name	Name of the reporting statistics table.
Latest Successful Generation	Indicates date and time of latest generation or if the table has never been generated.

Table 97 Batch Reporting Policy

Item	Functionality
Standard	Possible statuses: - 🔒: the table is part of the standard set of tables supplied by TIBCO LogLogic®. Standard tables supplied by TIBCO LogLogic® cannot be modified by the user. - **If the table cell is empty**: the table was defined by the user.
Active	Possible statuses: - Yellow check mark: table is active. - Red X: table is inactive.
Global Settings	
Daily Generation Time	All active tables are generated daily at this time automatically. The default setting is 2 a.m.
'Per hour' Data Retention (in days)	Data for tables that comprise hourly or daily information is not stored eternally. This parameter specifies the maximum number of days for retention of data for tables where data is grouped on an hourly basis. The default number is 200. Data that was generated in a time period further in the past is deleted.
'Per day' Data Retention (in days)	Data for tables that comprise hourly or daily information is not stored eternally. This parameter specifies the maximum number of days for retention of data for tables where data is grouped on a daily basis. The default number is 300. Data that was generated in a time period further in the past is deleted.
Maximum number of lines returned by an SQL query	In order to eliminate listing occurrences that are not important for analysis, insignificant results are discarded. The SMP orders the SQL SMP query results by their relevance according to their occurrence frequency (in decreasing order). The default number is 15000. The query returns results for alerts, incidents, vulnerability data, events, and raw logs.

Note: Data that is grouped on a monthly basis is not deleted.

Batch Reporting Rule Creation

There are 4 main sections in this screen:

- Global Settings (plus advanced parameters)
- The Operation Definition (with option for a customized operation definition)
- Data Fields Definition
- Additional Filter

Global Settings

Table 98 Batch Reporting Rule - Global Settings

Item	Description
Name	Name of the new table. Attention: You cannot enter more than 35 characters.
Advanced parameters	
Time scales (the frequency by which data is grouped in the table)	▪ Hour, Day, and Month tables (this will create 3 separate tables). ▪ Day and Month tables (this will create 2 separate tables). ▪ Month table only.
Target unit	▪ aggregated events. ▪ alerts. ▪ all alerts and aggregated events.
Time shift	From 0 to 9 days. For example, if you select 3 days, it means that you will take the TAT of the 4 last days (previous day + 3 days) into account in your report. It is useful for acknowledged alerts as you usually acknowledge alerts several days after their collection.
Operation definition	
Customized operation	To customize the operation definition. It opens the **Editing the Operation Definition** screen.
Delete	Once the operation selected, allows to delete it.
Add	Allows to add a new operation definition.
Customized Operation checkbox	Allows to edit, add, or delete a table operation definition. See table Batch Reporting Rule Creation.

The Operation Definition

Table 99 Batch Reporting Rule Creation

Reference data (source)	Description
Kind	This is the kind of the operation. The available types of operation are: ▪ Count. ▪ Average. ▪ Sum. ▪ Minimum. ▪ Maximum.
Field name*	Please see the database model for possible field names.

Data Fields Definition

If you click on the **Add** button, the following screen is displayed.

Table 100 Batch Reporting Rule - Data Fields Definition

Item	**Description**
Mode	- Normal: only a type of reference data needs to be selected. - Advanced: the type of table and the field's name must be filled in. The SQL string type must also be set. Note that if the field you would like to add is not found in normal mode, you can switch to advanced mode to make a specific reference to an existing table field in the SMP database.
Reference Data	
Table label	Reference Data name.
Field name	Field name.
Generated Column	
Column name	Generated column name.
Null values accepted	Select if null values are accepted. Fields marked with an asterisk are required.
SQL type	SQL type. Fields marked with an asterisk are required.

Additional Filter

Table 101 Batch Reporting Rule - Additional Filter

Item	**Description**
Activate filter checkbox	Makes the option below active.
Target table	Allows you to select the table where the filter will be applied to.
Definition	Allows you to enter the table definition in the SQL language format.

Chapter 5 - Configuration Menu

The Web Console **Configuration menu** includes the following menu items:

- Asset Database
- User Accounts
- External Servers
- Backup
- Database Statistics
- SMP Monitoring

Asset Database

The **Asset Database** is a module where you must enter the main information about your company. It it composed of interrelated objects that must be filled in with caution.

The **Asset Database** allows you to enter information about:

- Hosts
- Host Groups
- Business Assets
- Sites
- Site Groups
- Organizational Units (OU)
- Contacts
- Contact Groups
- Asset Regulations
- Service Level Agreements
- Effective Vulnerabilities
- False Positive Vulnerabilities

Hosts

To access the **Hosts** screen, select **Configuration** > **Asset Database** > **Hosts**.

Description

The characteristics of this screen are described in the following table.

Table 102 Host

Column	Description
Hostname	Each host must have a unique name, usually this is the same as the hostname of the actual system. Where systems have multiple hostnames, they can be described using “nodes”. When a new host is added, it will be created with 1 node of type DNS, with the same name as the hostname. This indicates that the host has the same DNS name as the hostname.
Host group	Shows which group the host belongs to. The host group contains similar machines located in the same site.
Log Collectors	Lists the Log Collectors that have been specified for this host. The Log Collector properties include which host the Log Collector is installed on. It is possible to have multiple installations of an Log Collector on the same host.
Log Sources	Lists the log sources. A log source describes which product the Log Collector is to monitor (and how).

Host Edition/Creation

This pane allows you to edit or create a host.

Description

The characteristics of this screen are described in the following table.

Table 103 Host Edition/Creation

Column	Description
Hostname	Name of the host. Each host in the asset database must have a unique name.
Description	Description of the host.
Operating system	Vendor, product, and version of the operating system so that the SMP can report vulnerabilities that may affect the host. You must either select **all** the OS information or **none of them**.
Product family	Type of the operating system, such as Windows or UNIX, which can be used to select hosts when producing reports.
Host group	Host group to which the host belongs. **Note:** By default, the host automatically belongs to the Default Host Group.
Time zone	Time zone where the host is located.
Addresses pane	Allows the user to enter host address(es) - including IP4 and IP6 addresses
Nodes pane	Allows the user to enter host name(s). A host may have multiple names, for example, if it has aliases such as server1.company.co.uk and it is also referred to as www.company.co.uk, or if it is running multiple naming systems such as a Windows server with a NetBIOS name of SERVER1 and a DNS name of server1.company.co.uk.
Applications pane	Allows the user to enter Vendor, Product and Version details of applications installed on the host. This information is used to report possible vulnerabilities the host may have.

Please refer to the Adding a New Host and Editing a Host sections in the user guide.

Note: The default host cannot be edited.

Host Groups

To access the host groups list, select **Configuration > Asset Database > Host Groups**.

Description

The characteristics of this screen are described in the following table.

Table 104 Host Groups

Parameter	Description
Checkbox	Once selected, allows you to delete a host group.
Name	Name and description of the host group.
Site	Site where the host group is located.
OU	OU from which the host group belongs to.
Hosts	Hosts contained in the host group.
Assets	Assets in the host group.
Contact Groups	Contacts linked with the host group.

Note: The default host group cannot be deleted.

Host Group Edition/Creation

This pane allows you to edit or create a host group.

Description

The characteristics of this screen are described in the following table.

Table 105 Host Group Edition/Creation

Column	Description
Name	Name of the host group. Each host group must have a unique name.
Description	Description of the host group.
Site	Site in which the hosts are located from the Site drop-down list. The site is created on the sites screen.
Organizational unit	Organizational unit in which the hosts are located from the Organizational Unit drop-down list.
Hosts	Host to add to the host group.
Contact Groups	Contact Groups to add to the host group. Actions such as send email use the contact groups as the recipients, so that only one alert action is required to trigger emails to appropriate contacts.
Business Assets	Business asset to apply to the new host group. Business Assets specify which SLAs and Criticality apply to the alerts relating to the hosts.

Please refer to the Adding a New Host Group and Editing a Host Group sections in the User Guide.

Business Assets

A business asset is a company item whose threats and vulnerabilities must be controlled, identified and calculated to evaluate risks. It is a group of hosts and host groups that can have the same SLA.

Please refer to the Adding a Business Asset and Editing a Business Asset sections in the User guide.

To access the Business Assets screen, select Configuration > Asset Database > Business Assets.

Description

The characteristics of this screen are described in the following table.

Table 106 Business Assets

Column	Description
Name	The Business Asset's name.
Criticality	Business Asset's significance level (critical, high, medium, low or lowest). It has an impact on the alert severity. For detailed information, see table Asset Criticality Impact on Alert Severity below.
Specific SLA	Displays the SLA which applies to hosts in this business asset. Choose a previously defined SLA, the default SLA, or choose **None** to have no SLA associated with this business asset (the SLA of the current configuration profile is used).
Host groups	Displays the host groups which are included in this business asset group.
Regulations	Displays the regulations to which business assets must be compliant with.

Business asset criticality has an impact on aggregated event severity. For example, if an event with “high” severity is sent to a Business asset server with a “lowest” level of criticality, then the event severity will automatically be changed to “medium” by the correlation engine.

Table 107 Asset Criticality Impact on Alert Severity

Business Asset Criticality	Aggregated Event Severity			
	Info	**Low**	**Medium**	**High**
Critical	Info	Medium	High	High
High	Info	Low	Medium	High
Medium	Info	Low	Medium	High
Low	Info	Low	Medium	High
Lowest	Info	Low	Low	Medium

Business Asset Edition/Creation

This pane allows you to edit or create a business asset.

Description

The characteristics of this screen are described in the following table.

Table 108 Business Asset Edition/Creation

Field	Description
Name	Name of the business asset.
Description	Description of the business asset.
Criticality	Business Asset's significance level (critical, high, medium, low or lowest). It has an impact on the alert severity. For detailed information, see table Asset Criticality Impact on Alert Severity.
Specific SLA	SLA which applies to hosts in this business asset. Choose a previously defined SLA, the default SLA, or choose **None** to have no SLA associated with this business asset (the SLA of the current configuration profile is used).
Host Groups pane	Host groups which are included in this business asset group.
Regulations pane	Regulations to which business assets must be compliant with.

Please refer to the Adding a Business Asset and Editing a Business Asset sections in the User Guide.

Sites

Sites are used to group hosts in reports (e.g. Lyon, Paris, or London, Cambridge), and to specify who is to be contacted when alerts have notification actions, such as e-mails. They are used to define the area of responsibility of one or more contacts.

Please refer to the Adding a New Site and Editing a Site sections in the User Guide

To access the site list, select **Configuration > Asset Database > Sites**.

The characteristics of this screen are described in the following table.

Table 109 Sites

Parameter	Description
Checkbox	Once selected, allows you to delete a site.

Table 109 Sites

Parameter	Description
Contacts	Contacts working on the site.
Host Groups	Host groups present on the site.

Note: The default site cannot be deleted.

Site Edition/Creation

This pane allows you to edit or create a site.

Description

The characteristics of this screen are described in the following table.

Table 110 Site Edition/Creation

Field	Description
Name	Site’s name (e.g. London, Paris, Lyon, Cambridge).
Description	Additional information about the site.
Site Group	Indicates which Site Group this site belongs to.
Time zone	Time zone corresponding to the site location.
Host Groups	Allows to define which host group must be present on the site.
Contacts	Allows you to define contacts that should be notified when alerts have notification actions, such as sending an email. Note that you cannot select the contact group.

Please refer to the Adding a New Site and Editing a Site sections in the User Guide.

Site Groups

A **Site Group** contains several sites. This allows you to better organize your log source.

Please refer to the Adding a New Site Group and Editing a Site Group sections in the User Guide.

To access the site group list, select **Configuration > Asset Database > Site Groups**.

Description

The characteristics of this screen are described in the following table.

Table 111 Site Groups

Parameter	Description
Checkbox	Once selected, allows you to delete a site group.
Name	Name of the site group.
Sites	Sites belonging to the group of sites.

Note: The default site group cannot be deleted.

Site Group Edition/Creation

This pane allows you to edit or create a site group.

Description

The characteristics of this screen are described in the following table.

Table 112 Site Group Edition/Creation

Field	Description
Name	Name of the site group.
Description	Description of the site.
Sites	List of the sites to be selected and included in the site group.

Please refer to the Adding a New Site Group and Editing a Site Group sections in the User Guide.

Organizational Units (OU)

Host groups can be grouped according to the **Organizational Unit** (OU) they belong to.

Please refer to the Adding an Organizational Unit and Editing an Organizational Unit sections in the User Guide.

To access the OU list, select **Configuration > Asset Database > Organizational Units**.

Description

The characteristics of this screen are described in the following table.

Table 113 Organizational Units

Parameter	Description
Checkbox	Once selected, allows you to delete an organizational unit.
Name	Name of the organizational unit.
Host groups	Host group belonging to the organizational unit.

Note: The default OU cannot be deleted.

Organizational Unit Edition/Creation

This pane allows you to edit or create an Organizational Unit.

Description

The characteristics of this screen are described in the following table.

Table 114 Organizational Unit Edition/Creation

Field	Description
Name	Name of the Organizational Unit.
Description	Description of the Organizational Unit.
Host Groups	List of the Host group belonging to the organizational unit.

Please refer to the Adding an Organizational Unit and Editing an Organizational Unit sections in the User Guide.

Contacts

For each contact, the notification methods are detailed - e.g. the email address and phone number can be specified. Contacts are then notified when alerts occur.

Please refer to the Adding a New Contact and Editing a Contact sections in the User Guide.

To access the list of contacts, select **Configuration > Asset Database > Contacts.**

Description

The characteristics of this screen are described in the following table.

Table 115 Contacts

Parameter	Description
Checkbox	Once selected, allows you to delete a contact.
Name	Name of the contact.
Site	Site where the contact is located.
Contact groups	Group to which the contact belongs.

Contact Edition/Creation

This pane allows you to edit or create a contact.

Description

The characteristics of this screen are described in the following table.

Table 116 Contact Edition/Creation

Field	Description
Name	Name of the contact.
Description	Description of the contact.
Service	Service name of the contact.
Telephone	Phone number of the contact. For information only.
Email	E-mail used to receive a message following an alert generation.
Site	Site where the contact is based.
Contact Groups	Groups to which the contact belongs used to specify destinations for messages such as e-mails. This action is mandatory.

Please refer to the Adding a New Contact and Editing a Contact sections in the User Guide.

Contact Groups

Create groups of contacts to control who is notified when the action attribute of an alert is set to send a message, such as an email.

Please refer to the Adding a New Contact Group and Editing a Contact Group sections in the User Guide.

To access the contact group list, select **Configuration > Asset Database > Contact Groups.**

Description

The characteristics of this screen are described in the following table.

Table 117 Contact Groups

Parameter	Description
Checkbox	Once selected, allows you to delete a contact group.
Name	Name of the contact group.
Host Groups	Host groups to which the contact belongs.
Contacts	Contacts belonging to the host group.It is highly recommended to allocate contacts to a contact group.

Note: The default contact group cannot be deleted.

Contact Group Edition/Creation

This pane allows you to edit or create a contact group.

Description

The characteristics of this screen are described in the following table.

Table 118 Contact Group Edition/Creation

Field	Description
Name	Name of the contact group.
Description	Description of the contact group.
Host Groups pane	Host groups that must be contacted if required by an alert action.
Contacts pane	Contacts who must belong to the selected group.

Please refer to the Adding a New Contact Group and Editing a Contact Group sections in the User Guide

Asset Regulations

Business assets can be compliant with specific regulations.

Please refer to the Adding an Asset Regulation and Editing an Asset regulation sections in the User Guide.

Description

The characteristics of this screen are described in the following table.

Table 119 Asset Regulation

Parameter	Description
Checkbox	Once selected, allows you to delete a contact group.
Name	Name of the regulation.
Assets	Assets to which the regulation is applied.

Asset Regulation Edition/Creation

This pane allows you to edit or create an asset regulation.

Description

The characteristics of this screen are described in the following table.

Table 120 Asset Regulation Edition/Creation

Field	**Description**
Name	Name of the asset regulation.
Description	Description of the asset regulation.
Business Assets pane	Assets that must be compliant with the regulation.

Please refer to the Adding an Asset Regulation and Editing an Asset regulation sections in the User Guide.

Service Level Agreements

The Service Level Agreement screen is used to configure the response times required for alerts' acknowledgement.

Please refer to the Adding a New SLA and Editing an SLA sections in the User Guide.

To access the SLAs screen, go to **Configuration > Asset Database > Service level agreements**.

Description

The characteristics of this screen are described in the following table.

Table 121 SLAs

Parameter	**Description**
Checkbox	Once selected, allows you to delete a contact group.
Name	Type of the SLA.
Configuration Profiles	Profile of user to which the SLA applies.
Assets	Assets linked with the SLA.

Service Level Agreements Edition/Creation

This pane allows you to edit or create a Service Level Agreement.

Description

The characteristics of this screen are described in the following table.

Table 122 SLA Edition/Creation

Field	Description
Name	Name of the SLA.
SLA pane	Allowed timeframe (in minutes) for a response based on the following severity: ▪ high ▪ medium ▪ low ▪ info ▪ unknown

Please refer to the Adding a New SLA and Editing an SLA sections in the User Guide.

Effective Vulnerabilities

The **Vulnerabilities** screen lists the vulnerabilities known by the SMP that may be exhibited by hosts.

Please refer to section Marking Vulnerabilities as False Positives section in the User Guide.

To display the list, go to **Configuration > Asset Database > Effective vulnerabilities**.

TIBCO LogLogic® uses a vulnerability database. This database contains the descriptions of product-related vulnerabilities (downloaded as a package) and vulnerabilities detected by the Log Collectors’ 'scanner' (such as Nessus, Qualys).

Description

The characteristics of this screen are described in the following table.

Table 123 Vulnerabilities

Column	Description
Vulnerability name	Click on the vulnerability name to edit it and to display vulnerability details.
CVE	The Common Vulnerability and Exposures list helps standardize reference to information about vulnerabilities and exposures. Click the CVE link to go to the entry on the CVE website.
Criticality	The criticality level according to the business asset related to the affected hosts, e.g. if the vulnerability exists on a host that belongs to the “Mission Critical” business asset, and this has a criticality of high, then that level is reported here.
Hosts nb	The number of hosts possibly affected by this vulnerability. Click the number to see a list of those hosts.

False Positive Vulnerabilities

The **False Positives** screen lists the vulnerabilities known by the SMP that have been identified as not being exhibited by hosts.

TIBCO LogLogic® uses a vulnerability database. This database contains the descriptions of product-related vulnerabilities (downloaded as a package) and vulnerabilities detected by the Log Collectors' 'scanner' (such as Nessus, Qualys).

Please refer to the Marking Vulnerabilities as True Vulnerabilities section in the User Guide.

Description

The characteristics of this screen are described in the following table.

Table 124 False Positive Vulnerabilities

Column	**Description**
Vulnerability name	Click on the vulnerability name to edit it and display vulnerability details.
CVE	The Common Vulnerability and Exposures list helps standardize reference to information about vulnerabilities and exposures. Click the CVE link to go to the entry on the CVE website.
Comment	Comments entered by the analyst when the vulnerability was identified as a false positive along with the analyst's username.
Hosts nb.	The number of hosts possibly affected by this vulnerability. Click the number to see a list of those hosts.

User Accounts

The list of users includes their name, whether they are locked out, user rights, the time of their last login, the preferred language used in the GUI, and what access they have to the reporting module.

To perform one of the following actions, first select the desired user by clicking the checkbox(es) on the left:

Table 125 User Accounts Buttons

Button	**Description**
Unlock	To enable a user account, that is, one that had been previously disabled.
Lock	To prevent a user logging on to the Web Console GUI, even with the correct password.
Delete	To delete one or more users.
Add	To add a new user.

To edit user properties, for example, to change their administrative rights, click on the username.

Add and Edit Users

Please refer to the "Add/Edit Users" section in the User Guide.

Description

The characteristics of this screen are described in the following table.

Table 126 User Account Creation

Item	Description
Name	User name. It must be a unique identifier. It must not contain more than 50 characters. It can be a name or an e-mail address
Authentication mode	▪ Local Password: this option must be selected if the user access the Web Console in the standard mode. ▪ Radius Password: this option must be selected if the user access the Web Console via the RADIUS server. If the user has not been configured as being a RADIUS user via the External Servers screen, this option is not available.
User password	Allows you to enter the TIBCO LogLogic® password you have just entered by entering it a second time.
Confirm password	Allows you to confirm the TIBCO LogLogic® password you have just entered by entering it a second time. The password must be at least 8 characters long, with at least one alphabetic and one numeric character. It must not contain more than 25 characters.
User rights	Right to be granted to the user. See section Add and Edit Users above. If you select Analyst or Viewer, the Monitoring Perimeter table is displayed.
Play sound for new alerts	Play a sound if a new alert is received when the list of alerts is set to pause.
Security dashboard access	Indicate if the user has access to security dashboards.
Workspace	Delimit the different reports available for different user roles. Each workspace contains a list of available reports.
Home page	Specify the initial page to be displayed to the user when starting the security dashboard module.

External Servers

LMI (LX/ST/MX) Server

This pane allows you to add **LMI** hosts.

Description

The characteristics of this screen are described in the following table.

Table 127 LMI (LX/ST/MX)

Field	Description
Host	Gives the LMI IP address
Syslog port	Gives the Syslog port
Delete	Allows you to delete a host
Add button	Allows you to add a new host

Incident Notification

Whenever an incident is created, updated or closed, an incident can be sent to a server in the IODEF format through the SOAP protocol.

To access the incident **Notification** screen, select **Configuration > External servers > Incident Notification** tab.

Description

The characteristics of this screen are described in the following table.

Table 128 Incident Notification

Item	Description
Notify on new, modified and closed incidents	Activates/deactivates the notification.
URL	Remote server configuration URL. This parameter is mandatory if you selected the **Incident Notification** checkbox. The format is: `http[s]://{incident_server_IP}:{port}/path`
Authentication	Available only if the URL is `https` (see above). **simple** indicates if a user login and password are needed to be authenticated. **certificate** indicates if a certificate is needed to be authenticated.
[**simple** is selected] User	User login to authenticate on the server.
[**simple** is selected] Password	Password to authenticate on the server.
[**certificate** is selected] Certificate	Allows the upload of the client certificate to authenticate on the server.
CA server certificate	Allows the upload of the CA server certificate to verify the validity of the server certificate provided during the connection.
CRL checkboxes	These checkboxes allow the validation of the certificate’s revocation.
Minimum duration between 2 update notifications	Time period at the end of which a notification is sent. The default time period is 60 seconds and the minimum is 30 seconds, i.e. each 30 seconds, you will receive a notification about your incidents.
Test the connectivity to the incident server link	Check if the server communicates correctly.
Synchronize the incidents link	This link is displayed once you have clicked on the **OK** button to save the configuration. This link applies the modification immediately.

Please refer to the Incident Notification section in the User Guide.

External Authentication

Security Event Manager can contact a RADIUS external server to authenticate users that try to log in.

To do so, you must allow the SEM solution to access your RADIUS authentication server. Only the **super-administrator** has the right to modify a RADIUS user account.

To access the **RADIUS Authentication Settings** screen, select **Configuration > External servers**.

Description

The characteristics of this screen are described in the following table.

Table 129 External Authentication

Item	Description
Address	RADIUS IP server address or hostname.
Shared Key	RADIUS shared secret key.

Table 129 External Authentication

Item	Description
Authentication port	RADIUS server authentication port.
Accounting port	RADIUS server accounting port.

Please refer to the External Authentication with RADIUS section in the User Guide.

Mail Configuration

To authorize the automatic sending of e-mail from the SMP, the **Mail Configuration** pane must be filled in.

To access the Mail Configuration screen, select **Configuration > External servers > Mail Configuration tab.**

Description

The characteristics of this screen are described in the following table.

Table 130 Mail Configuration Settings

Item	Description
Server name	IP address or DNS name of the sent mail server. This field is mandatory.
Server port	Port used by the SMTP server. This field is mandatory.
Max mail per minute	Maximum number of mails per minute you want to receive. This field is optional. This option is useful to filter the number of sent mails and then avoid overloading the server. The value must be between 1 and 50 inclusive.
Mail sender	Sender's address. It is recommended not to use the default value but to enter a customized value.

Please refer to the Mail Configuration section in the User Guide.

Backup

Backup Configuration

To display the **Backup Configuration** screen, go to **Configuration > Backup**.

Description

The following modules are available for inclusion in a backup:

- Configuration (log collectors, correlation rules...).
- Asset database.
- Reporting configuration.
- System configuration.
- SMP logs.

By default, SMP logs are also included in the backup, but these can be omitted by clearing the appropriate check boxes. It is also possible to backup other types of files and directories, by entering their full pathnames in the **User defined files** text box.

Note: If the total number of alerts and incidents in the database is exceedingly large, these modules will not be included by default in the backup. However, asset database, configuration, reports, and system configuration will always be included.

Please refer to section **Configuring the Backup Export Script** in the User Guide.

Database Statistics

The database configuration screen displays key statistics about the database.

To access the screen, select **Configuration > Database Monitoring**.

If the instance status information is out-of-date, click the **Refresh** button. This may take several seconds.

Characteristics

The characteristics of this screen are described in the following table.

Table 131 Global Database Usage Fields

Field	**Description**
Database used space	The percentage of the database space used for all instances on this SMP.
Instance used space	Shows what percentage of the database is used by the current instance.
Unitary events	Shows how many events are in the database.
Top level alerts	Shows how many top level alerts are being displayed.
New alerts in progress	Shows how many alerts/events are being correlated at the moment - e.g., if a scenario requires 3 alerts to trigger its own action, but only two alerts have been detected, these two alerts count towards this figure.
Correlated alerts rate	The ratio of alerts produced by the correlation engine compared to the number of events received, e.g., if four events were correlated into one alert, this figure would be 25%.
Alerts average number by correlation	Each set of alerts that have been correlated is averaged across the number of alerts. For example, if there were two correlations, one consisting of 10 alerts and one consisting of 6 alerts, this figure would be 8.
Oldest alert date	The date of the generation of the oldest alert in the database.
Oldest event date	The date of the generation of the oldest event in the database.

SMP Monitoring

The SMP Monitoring menu gives technical information about the SMP performances. This module is useful in the event of a performance problem or failure.

To display the SMP **Monitoring** screen, go to **Configuration** > SMP **Monitoring**.

Live Explorer Tab

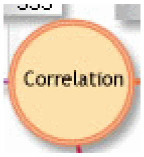
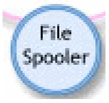
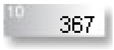
The **Live Explorer** tab graphically displays the events flow.

To display the SMP **Monitoring** screen, go to **Configuration > SMP Monitoring > Live Explorer**.

Description

The characteristics of this screen are described in the following table.

Table 132 Live Explorer

Type of Object	Description
	The orange object represents the various engines available in SEM: ▪ Totaling engine. ▪ Aggregation engine. ▪ Correlation engine. The **Start** orange object represents the Log Collector sending the event which is sent to the SMP.
	The blue object represents the **Additional modules**, i.e. the main steps of the process of events. ▪ File Spooler. ▪ Event enhancer. ▪ Event inserters into different databases.
	Number of EPS for each relevant event transformation.

Last Hour Graph Tab

The **Last Hour Graph** tab graphically displays data referring to the last hour. This is the most commonly used graph.

Description

The characteristics of this screen are described in the following table.

Table 133 Last Hour Graph Tab

Name	Description
CPU utilization	Displays the Central Processing Unit performance.
IO Wait	Displays the waiting time to connect to the disk. IO Wait should stay below 10% as an average. Anyhow, an IO wait exceeding 20% is unusual and may signify that the MySQL database queries are taking too much time and lessen performance.
System Free Memory	Displays the system's free memory.
System Cache Memory	Displays free memory in the core system. **Note:** It is important to analyze simultaneously the System Cache Memory and System Free Memory graphs. This analysis will furnish the total free memory space, the space available on the core system, and the total RAM available.
VM Free Memory	Displays the free space in the virtual Java machine. If it is near zero, it is recommended to increase the memory size.
GC usage (‰)	Displays the time spent by the JAVA Garbage Collector to clean up the memory by removing unused objects.
Connected Log Collectors	Displays the number of connected Log Collectors.
Received Events (eps)	Displays the number of events received per second.
Spooled Events (eps)	Displays the number of events stored in the buffer per second.
Saved Raw log (eps)	Displays the number of raw data units saved per second.

Table 133 Last Hour Graph Tab

Name	Description
Saved Elementary Events (eps)	Displays the number of elementary events saved per second.
Alerts & Events processed by correlator (eps)	Displays the number of events and correlation alerts saved per second.

Last Day Graph Tab

The **Last Day Graph** tab graphically displays data for the current day. The information is the same as for Last Hour Graph tab.

Raw Data Tab

The **Raw Data** tab displays raw data in text format. It must be linked with the Live Explorer graph.

Table 134 Raw Data tab

Name	Description
Java Virtual Machine	
Memory used	Used space available in the virtual Java machine. If it is near 100%, it is recommended to increase the memory size. It corresponds to the **VM Free memory** in the Graphical view.
reclaim unused memory	The garbage collecting process runs in the background and attempts to reclaim memory that is no more used by the application. Click this button to find more unused memory (just note that the process has an impact on the performance)
Event Entry Stream Counters	
ees:entry	Number of events that enter the process.
ees:unspooled	Number of events that pass without passing through the spooler.
ees:fileSpooler_in	Number of events that pass into the spooler.
ees:fileSpooler_out	Number of events that go out from spooler.
ees:eventPreparerIn	Number of events that pass through the database enhancer.
ees:accountingIn	Number of events that go into the database enhancer.
ees:accountingOut	Number of events that go out from the database enhancer. The number should be the same as the previous parameter.
ees:fusionIn	Number of events that go into the aggregation engine.
ees:shareableWaiterIn	Number of events that go out from the aggregation engine and go into the correlation engine.
ees:rawlogWaiterIn	Number of raw logs that are be stored in database.
ees:rawlogWaiterOut	Number of raw logs that go out from the database.
ees:rawlogInserterIn	Number of raw logs which go into the Log inserter.
ees:rawlogInserterOut	Number of raw logs which go out from the Log inserter.
ees:correlationIn	Number of aggregated events which enter the correlation engine.
ees:correlationOut	Number of aggregated events which go out from the correlation.
ees:fusionFlushedEvent	Number of aggregated events which go into the database.
ees:stableEventWaiterOut	Number of events that have exceeded the stopping threshold.
ees:correlationFlushedAlert	Number of pending alerts which have been correlated.

Table 134 Raw Data tab

Name	Description
ees:stableAlertWaiterOut	Number of alerts that have exceeded the stopping threshold.
ees:accepted	Number of elements which allow the display process to be started.
ees:guiInformerOut	Number of events which allow the display of information/
ees:guiInformerIn	N/A
ees:eventPreparerOutRawlog	Number of isolated raw logs to be processed.
ees:eventPreparerOutRawlog	Number of alerts - to be stored so that it can be sent in the correlation engine -, which go out from the event enhancer.
Log Counters	
rawlog:inserted	Number of inserted raw logs.
rawlog:nbLines	Number of lines of inserted raw logs.
elemEvent:inserted	Number of inserted Elementary Events.
elemEvent:nbLines	Number of lines in Elementary Events.
Receiver	
LOG_COLLECTOR-*name*:alerts	Number of events sent by the Log Collector to the server.
connections:msgReceived	Total of connection messages received.
connections:runningAtoS	Number of Log Collector > Server connections.
connections:runningCnx	Total of connections (Log Collector > Server and Server > Log Collector)
connections:runningStoA	Number of Server > Log Collector connections.
Processing Flows QLen = Queue Length; In = elements in the engines; Done = elements processed; Out = elements out of the engines */d = Delta difference between the element from the last second and the current one */s = Average of elements in minute	
Aggregation	Number of elements processed by the aggregation engine.
Correlation	Number of elements processed by the correlation engine.
LiveReporting	Number of elements processed by the Live Reporting engine.
QP-GUIInformer	Number of elements which potentially go to the GUI and waiting to be processed.
QP-LogInserter	Number of pending raw logs and events waiting to be processed.
QP-RT-CorrelatorQueue	Number of events which passed through the correlation engine.
QP-RT-CorrelatorStage-KB	Number of events processed by the correlation engine which have been enriched.
QP-alertInserters-x	Number of Aggregated Events and alerts waiting to be processed.
QP-eEventInserters-x	Number of Elementary Events waiting to be processed.
QP-rawlogInserters-x	Number of Raw Logs waiting to be processed.
Correlation Allocations	
Alert aggregates	Number of alerts that have been generated. These are correlated alerts.
Alerts in aggregates	Number of alerts contained in the aggregate.
Waiters Info	
WT-eventSharable:Waitings	Number of events which are waiting to be processed to the correlation engine.

Table 134 Raw Data tab

Name	Description
WT-logInsertable:Waiting	Number of raw logs which are waiting to be processed.
WT-eventStable:Waiting	Number of stable events which are waiting to be processed.
WT-alertStable:Waiting	Number of stable alerts which are waiting to be processed.

Event Data Tab

The **Event Data** tab displays events and alerts data in text format.

Table 135 Event Data tab

Name	Description
Total	Since last runtime
Last sec.	The second before the display (instantaneous value)
Average (last min., in eps)	Per second in the last minute
Alert Cache	
alerts:CacheSize	Current number of aggregated events and alerts stored in the cache.
alerts:CacheIn	Number of aggregated events and alerts written to the cache.
alerts:CacheOut	Number of aggregated events and alerts ejected from the cache.
alerts:CacheHit	Number of aggregated events and alerts that hit the cache.
alerts:CacheMiss	Number of alerts that did not go into the cache. If the number is high, it means that there is not enough memory.
Alert Shared Manager	
alertShared:created	Number of versioned alerts or events which are created.
alertShared:shareable	Number of versioned alerts or events which can be modified.
alertShared:versionAdded	Number of versioned alerts or events which have been modified.
alertShared:versionCommited	Number of queries sent to the database to apply the modification on versioned alerts or events.
alertShared:commitFailed	Number of commits of versioned alerts or events which are not sent.
alertShared:modified	Number of modified versioned alerts or events which are sent to the database.
alertShared:immutable	Number of versioned alerts or events that cannot be modified.
alertShared:deleted	Number of deleted versioned alerts or events.
alertShared:instable/immutable	Internal counter.
alertShared:stable/immutable	Internal counter.
alertShared:stable/not shared	Internal counter.
alertShared:stable/unknown	Internal counter.
alertShared:instable/unknown	Internal counter.
alertShared:stable/shared	Internal counter.
alertShared:instable/shared	Internal counter.
alertShared:inMemory	Number of versioned alerts or aggregated events which are not closed and kept in memory.
alertShared:lastId	Last ID number given to the event.
alertShared:immutableSize	N/A
alertShared:dbIdentToSharedIds	Internal counter.

Table 135 Event Data tab

Name	Description
Alert DB Facade	
Number of queries made in the database.	
JDBC Driver information	
Internal counter.	

Engine Management Tab

The **Engine Management** tab displays the list of the three main SMP engines.

Description

Table 136 Engine Management

Name	Description
Category	Type of engine.
Rules	Number of rules created per engine.
Scenarios	**[Correlation only]** Number of scenarios created.
Need sync	Indicates if an engine needs to be synchronized, e.g. if you did not synchronize the engine when creating a new correlation policy.
Restart all Engines	Synchronizes all the engine at the same time if some engines have not been synchronized. **Note:** Each time the asset database is updated, the engines must be synchronized for the modification to be taken into account.

Chapter 6 - Help Menu

The Web Console Help menu includes the following menu items:

- Table of Contents
- Support Center...
- LogLogic.com...
- Broadcast a Message
- About

Table of Contents

This item allows you to display the TIBCO LogLogic® **Online Help** table of contents.

You can also access the **Online Help** relevant pages by clicking on the **?** icon.

Support Center...

This item allows you to display the web portal of the TIBCO LogLogic® support at https://support.tibco.com/esupport/loglogic.htm

You can browse tickets or ask questions to the support via this site.

LogLogic.com...

This item allows you to display the TIBCO LogLogic® company website at http://www.loglogic.com/.

Broadcast a Message

This item allows you to display the **Broadcast a Message** screen where you can send a warning or an error message to all connected users on the interface. This is useful if for example you need to warn users about an activity that will affect users dispersed in various locations (e.g. maintenance that would need a server reboot).

1. Select the **Help > Broadcast a message** menu item.
2. Enter the message in the **Broadcast a Message** pop-up screen.
3. Click **OK** to send your message.

The message will automatically be displayed to all connected users.

About

This item allows you to display the **About** screen where you will find general information about the application.

Tabs	Description
About	Allows you to get information about all the software programs used to make the application work.
System	Allows you to know: ▪ The number of processors used to make the application work. ▪ The disk memory available on your computer. ▪ The size of logs on your machine. ▪ the system properties (Java properties, instance name, user timezone, user language...) ▪ The request attributes.
Users	Allows you to know the currently connected users and their connection time.

Chapter 7 - Default Content

This section contains information about the default content in Security Event Manager, such as:

- List of Aggregation Rules
- List of Correlation Rules
- List of Rules for Scenarios
- List of Default Collection Policies
- List of Default Collection Rules
- List of Predefined Dashboards
- List of Default Live Reporting Policies
- List of Default Batch Reporting Policies
- List of Reporting Tables
- List of Correlation/Aggregation/Live Reporting Grouping Fields

List of Aggregation Rules

The table below lists the default aggregation rules, grouped according to each main category.

Table 137 Aggregation Rules - Information status

Rule Name	Description
1 - Information status - Control	The rule aggregates logs of the same Taxonomy. One aggregated event is created for each target node name or address. Created aggregated events do not keep lists of attributes. In order to preserve the SMP storage capacity, elementary events related to “control” are not stored.
2 - Information status - Threshold	The rule aggregates logs of the same Taxonomy. One aggregated event is created for each target node name or address. Created aggregated events do not keep lists of attributes. In order to preserve the SMP storage capacity, elementary events related to “threshold” are not stored.

Table 138 Aggregation Rules - Standard activity

Rule Name	**Description**
3 - Standard activity - Backup Management	The rule aggregates logs of the same Taxonomy. One aggregated event is created for each target node name or address. Each created aggregated event keeps the list of target file(s) name(s).
4 - Standard activity - Communication Flow	The rule aggregates logs of the same Taxonomy. One aggregated event is created for each target node name or address. Each created aggregated event keeps the list of: ▪ source node names or addresses ▪ source or target service names In order to preserve the SMP storage capacity, elementary events related to "communication flow" are not stored.
5 - Standard activity - Control	The rule aggregates logs of the same Taxonomy. One aggregated event is created for each target node name or address. Created aggregated event do not keep lists of attributes.
6 - Standard activity - Data Access	The rule aggregates logs of the same Taxonomy. One aggregated event is created for each target node name or address. Each created aggregated event keeps the list of: ▪ source node names or addresses ▪ target service names ▪ target user names or ids ▪ target process names ▪ target file names
7 - Standard activity - Data Exchange	The rule aggregates logs of the same Taxonomy. One aggregated event is created for each target node name or address. Each created aggregated event keeps the list of: ▪ source node names or addresses ▪ target service names ▪ target user names or ids ▪ target process names ▪ target file names
8 - Standard activity - Gain	The rule aggregates logs of the same Taxonomy. One aggregated event is created for each target node name or address. Each created aggregated event keeps the list of: ▪ source node names or addresses ▪ target service names ▪ source or target user names or ids ▪ target process names

Table 138 Aggregation Rules - Standard activity

Rule Name	Description
9 - Standard activity - Process	The rule aggregates logs of the same Taxonomy. One aggregated event is created for each target node name or address. Each created aggregated event keeps the list of: ■ target services names ■ target user names or ids ■ target process names
10 - Standard activity - Service Availability	The rule aggregates logs of the same Taxonomy. One aggregated event is created for each target node name or address. Each created aggregated event keeps the list of: ■ target service names ■ target process names
11 - Standard activity - State Transition	The rule aggregates logs of the same Taxonomy. One aggregated event is created for each target node name or address. Each created aggregated event keeps the list of: ■ target service names ■ target process names
12 - Standard activity - User Authentication	The rule aggregates logs of the same Taxonomy. One aggregated event is created for each target node name or address and each target user name or ID. Each created aggregated event keeps the list of: ■ source node names or addresses ■ target service names ■ target process names

Table 139 Aggregation Rules - Configuration activity

Name	Description
13 - Configuration activity - Account (locking)	The rule aggregates logs of the same Taxonomy. One aggregated event is created for each target node name or address. Each created aggregated event keeps the list of: ■ source node names or addresses ■ target service names ■ source or target user names or ids ■ target process names
14 - Configuration activity - Management	The rule aggregates logs of the same Taxonomy. One aggregated event is created for each target node name or address. Each created aggregated event keeps the list of: ■ source node names or addresses ■ target service names ■ target user names or ids ■ target process names ■ target file names

Table 139 Aggregation Rules - Configuration activity

Name	Description
15 - Configuration activity - Repair	The rule aggregates logs of the same Taxonomy. One aggregated event is created for each target node name or address. Each created aggregated event keeps the list of: ▪ target user names or ids ▪ target process names ▪ target file names
16 - Configuration activity - Update	The rule aggregates logs of the same Taxonomy. One aggregated event is created for each target node name or address. Each created aggregated event keeps the list of: ▪ source node names or addresses ▪ target service names ▪ target user names or ids ▪ target process names ▪ target file names

Table 140 Aggregation Rules - Other

Name	Description
17 - Vulnerability status	The rule aggregates logs of the same Taxonomy. One aggregated event is created for each target node name or address. Each created aggregated event keeps the list of: ▪ source node names or addresses ▪ target service names ▪ target user names or ids ▪ target web service names ▪ target process names ▪ target tool names ▪ target file names
18 - Suspicious activity identification	The rule aggregates logs of the same Taxonomy. One aggregated event is created for each target node name or address and reference name/origin. The IDS events are correlated with the data contained in the vulnerability database. Each created aggregated event keeps the list of: ▪ source node names or addresses ▪ target service names ▪ target user names or ids ▪ target web service names ▪ target process names ▪ target tool names ▪ target file names

Table 140 Aggregation Rules - Other

Name	Description
19 - Malware identification	The rule aggregates logs of the same Taxonomy. One aggregated event is created for each target node name or address. Each created aggregated event keeps the list of: ▪ source node names or addresses ▪ target service names ▪ source or target user names or ids ▪ target web service names ▪ target process names ▪ target tool names ▪ target file names
20 - Attack identification	This rule aggregates logs of the same Taxonomy. One aggregated event is created for each target node name or address and reference name/origin. The IDS events are correlated with the data contained in the vulnerability database. Each created aggregated event keeps the list of: ▪ source node names or addresses ▪ target service names ▪ target user names or ids ▪ target web service names ▪ target process names ▪ target tool names ▪ target file names
21 - Undefined Taxonomy	This rule aggregates logs with an undefined Taxonomy. One aggregated event is created for each log source: ▪ it contains no elementary event as they do not contain categorized information. ▪ it contains raw logs with useful information for troubleshooting or to improve device support. Created aggregated events do not keep lists of attributes.
0 - Implied rule	When no aggregation rule has matched at all, the elementary event is matched by an implied rule. This rule aggregates logs of the same Taxonomy. ▪ One aggregated event is created for each target node name or address. ▪ Created aggregated events do not keep lists of attributes. The elementary events are not stored.

List of Correlation Rules

The set of correlation rules per group is listed below.

Table 141 Asset Database Rules

Name	Description	Alert's Name	Alert's Severity
1 - ADB - Misuse - Windows Domain Controller Output	The rule controls that hosts from the "Windows Domain Controllers" host group use only authorized services. Only the following services are allowed from a "Windows Domain Controllers" host: ▪ DNS (53 tcp/udp) ▪ Kerberos (88 tcp/udp) ▪ NTP (123 udp) ▪ LDAP (389 tcp/udp) ▪ Global Catalog LDAP (3268 tcp) ▪ AD Replication (53211 tcp) ▪ File Replication Service (53212 tcp) An alert is raised if any other service is used from a "Windows Domain Controllers" host.	Windows domain controller misused	🔔
2 - ADB - Misuse - Windows Domain Controller Input	The rule controls that hosts from the "Windows Domain Controllers" host group are only used for what they are designed for. Only the following services are allowed on a "Windows Domain Controllers" host: ▪ DNS (53 tcp/udp) ▪ Kerberos (88 tcp/udp) ▪ NTP (123 udp) ▪ LDAP (389 tcp/udp) ▪ Global Catalog LDAP (3268 tcp) ▪ AD Replication (53211 tcp) ▪ File Replication Service (53212 tcp) An alert is raised if any other service is used on "Windows Domain Controllers" hosts.	Windows domain controller misused	🔔
3 - ADB - Misuse - Mail Server Output	The rule controls that hosts from the "Mail Servers" host group use only authorized services. Only the following services are allowed from a "Mail Servers" host: ▪ SMTP (25 tcp) ▪ POP3 (110 tcp) ▪ IMAP (143 tcp) ▪ IMAPS (993 tcp) ▪ POP3S (995 tcp) An alert is raised if any other service is used from a "Mail Servers" hosts.	Mail Server Misused	🔔

Table 141 Asset Database Rules

Name	Description	Alert's Name	Alert's Severity
4 - ADB - Misuse - Mail Server Input	The rule controls that hosts from the "Mail Servers" host group are only used for what they are designed for. Only the following services are allowed on a "Mail Servers" host: - SMTP (25 tcp) - POP3 (110 tcp) - IMAP (143 tcp) - IMAPS (993 tcp) - POP3S (995 tcp) An alert is raised if any other service is used on "Mail Servers" hosts.	Mail Server Misused	🔔
5 - ADB - Misuse - Web Proxy Output	The rule controls that hosts from the "Web Proxies" host group use only authorized services. Only the following services are allowed from a "Web Proxies" host: - HTTP (80 tcp) - HTTPS (443 tcp) An alert is raised if any other service is used from a "Web Proxies" hosts.	Web Proxy Misused	🔔
6 - ADB - Misuse - Web Proxy Input	The rule controls that hosts from the "Web Proxies" host group are only used for what they are designed for. Only the following services are allowed on a "Web Proxies" host: - HTTP (80 tcp) - HTTPS (443 tcp) - SQUID (3128 tcp/udp) An alert is raised if any other service is used on a "Web Proxies" hosts.	Web Proxy Misused	🔔
7 - ADB - Misuse - Corporate Application Servers	The rule controls that hosts from the "Corporate Application Servers" host group are only used for what they are designed for. Only the following services are allowed on a "Corporate Application Servers" host: - HTTP (80 tcp) - HTTPS (443 tcp) An alert is raised: - if any other service is used on a "Corporate Application Servers" hosts - and if the host IP address corresponds to private address (RFC 1918)	Web Server Misused	🔔

Table 141 Asset Database Rules

Name	Description	Alert's Name	Alert's Severity
8 - ADB - Misuse - Instant Messaging	The rule controls that hosts from the "Mail Servers" host group (or any defined corporate instant messaging server) are only used for what they are designed for. Only the following services are allowed on a "Mail Servers" host: ▪ IRC (113 udp, 194 udp, 6660 to 6669 tcp) An alert is raised if any other service is used on a "Mail Servers" hosts.	Instant Messaging Misused	🔔
9 - ADB - Bypass - Windows Domain Controller	The rule controls that "Windows Domain Controllers" services are provided by well known servers, defined in the asset database. An alert is raised when a host not linked to the "Windows Domain Controllers" host group provides one of the following services: ▪ DNS (53 tcp/udp) ▪ Kerberos (88 tcp/udp) ▪ NTP (123 udp) ▪ LDAP (389 tcp/udp) ▪ Global Catalog LDAP (3268 tcp) ▪ AD Replication (53211 tcp) ▪ File Replication Service (53212 tcp)	DNS Assets Bypass	🔔
10 - ADB - Bypass - Mail Server	The rule controls that "Mail Servers" services are provided by well known servers, defined in the asset database. An alert is raised when a host not linked to the "Mail Servers" host group provides one of the following services: ▪ SMTP (25 tcp) ▪ POP3 (110 tcp) ▪ IMAP (143 tcp) ▪ IMAPS (993 tcp) ▪ POP3S (995 tcp)	Mail Server Bypass	🔔
11 - ADB - Bypass - Web Proxy	The rule controls that "Web Proxies" services are provided by well known servers, defined in the asset database. An alert is raised when a host not linked to the "Web Proxies" host group provides one of the following services: ▪ Web Proxy (8080 tcp) ▪ SQUID (3128 tcp/udp)	Web Proxy Bypass	🔔

Table 141 Asset Database Rules

Name	Description	Alert's Name	Alert's Severity
12 - ADB - Bypass - Corporate Application Servers	The rule controls that "Corporate Application Servers" services are provided by well known servers, defined in the asset database. An alert is raised when... ▪ a host is not linked to the "Corporate Application Servers" host group ▪ and the host IP address corresponds to RFC 1918 .... provides one of the following services: ▪ HTTP (80 tcp) ▪ HTTPS (443 tcp)	Web Server Bypass	🔔🟧
13 - ADB - Bypass - Instant Messaging	The rule controls that "Instant Messaging" services are provided by well known servers, defined in the asset database. An alert is raised when a host not linked to the "Mail Servers" host group (or any define instant messaging host group) provides one of the following services: ▪ IRC (113 udp) ▪ IRC (194 udp) ▪ IRC (6660 to 6669 tcp)	Instant Messaging Bypass	🔔🟧
14 - ADB - Cleartext Authentication Protocol	The rule controls that no cleartext authentication protocol is used on internal hosts. An alert is raised when a user authenticates himself on a host (linked to a defined host group) with one of the following protocols: ▪ Telnet (23 tcp) ▪ HTTP (80 tcp)	Unauthorized cleartext authentication protocol	🔔🟧
15 - ADB - Unauthorized Administration Stations	The rule controls that every IT administration task is performed from authorized "Administration Station". An alert is raised if a user authenticates himself ▪ on a defined host ▪ from a host not included in "Administration Station" host group ▪ with a protocol SSH or MS TSC	Unauthorized administration stations detected	🔔🟥
16 - ADB - Threat on Vulnerable Target	Detected attacks on target known to be vulnerable. A previous vulnerability scanner found vulnerability for the target and set the "target assessment" field to "vulnerable".	Known vulnerability exploited	🔔🟥

Table 142 Threshold Rules

Name	Description	Alert's Name	Alert's Severity
17 - Threshold - Information Threshold	The rule raises an alert when the same event occurs too many times and is considered as suspicious. Taxonomy: Information Status: Threshold Threshold: 3 events per minute	Threshold reached too many times	🟩
18 - Threshold - Information Control	The rule raises an alert when the same event occurs too many times and is considered as suspicious. Taxonomy: Information Status: Control Threshold: 10 events per minute	Multiple invalid information controls	🟩
19 - Threshold - Backup Management	The rule raises an alert when the same event occurs too many times and is considered as suspicious. Taxonomy: Standard Activity: Failed Backup Management Threshold: 3 events per minute	Multiple failed backup management activities	🟧
20 - Threshold - Communication Flows	The rule raises an alert when the same event occurs too many times and is considered as suspicious. Taxonomy: Standard Activity: Denied Communication Connect Threshold: 10 events per minute	Multiple connections denied	🟧
21 - Threshold - Control Use	The rule raises an alert when the same event occurs too many times and is considered as suspicious. Taxonomy: Standard Activity: Invalid Control Threshold: 10 events per minute	Multiple errors in controls use	🟩
22 - Threshold - Data Access	The rule raises an alert when the same event occurs too many times and is considered as suspicious. Taxonomy: Standard Activity: Failed Data Access Threshold: 10 events per minute	Multiple failed data access	🟥
23 - Threshold - Data Exchange	The rule raises an alert when the same event occurs too many times and is considered as suspicious. Taxonomy: Standard Activity: Error Data Exchange Threshold: 10 events per minute	Multiple errors in data exchanges	🟩
24 - Threshold - Gain Activities	The rule raises an alert when the same event occurs too many times and is considered as suspicious. Taxonomy: Standard Activity: Failed Gain Threshold: 5 events per minute	Multiple failed right gain attempts	🟥

Table 142 Threshold Rules

Name	Description	Alert's Name	Alert's Severity
25 - Threshold - Processing Activities	The rule raise an alert when the same event occurs too many times and is considered as suspicious. Taxonomy: Standard Activity: Error Process Threshold: 50 events per minute	Multiple processing errors	🟩
26 - Threshold - Service Availability	The rule raises an alert when the same event occurs too many times and is considered as suspicious. Taxonomy: Standard Activity: Service Availability Threshold: 1 event per minute	Service Availability Transition	🟧
27 - Threshold - State Transition	The rule raises an alert when the same event occurs too many times and is considered as suspicious. Taxonomy: Standard Activity: State Transition Threshold: 1 event per minute	Process stopped	🟩
28 - Threshold - User authentication	The rule raises an alert when the same event occurs too many times and is considered as suspicious. Taxonomy: Standard Activity: Failed Authentication Threshold: 5 events per minute	Multiple user authentication failures	🟥
29 - Threshold - Account Locking	The rule raises an alert when the same event occurs too many times and is considered as suspicious. Taxonomy: Configuration: Successful Account Lock/Unlock Threshold: 10 events per minute	Multiple accounts locked or unlocked	🟥
30 - Threshold - Configuration Repair Failed	The rule raises an alert when the same event occurs too many times and is considered as suspicious. Taxonomy: Configuration: Failed Repair Threshold: 1 event per minute	Configuration Repair Failure	🟧
31 - Threshold - Configuration Repair Success	The rule raises an alert when the same event occurs too many times and is considered as suspicious. Taxonomy: Configuration: Successful Repair Threshold: 10 events per minute	Multiple configuration repairs (possible virus outbreak)	🟧
32 - Threshold - Configuration Update	The rule raises an alert when the same event occurs too many times and is considered as suspicious. Taxonomy: Configuration: Error Update Threshold: 1 event per minute	Configuration Update Error	🟧

Table 142 Threshold Rules

Name	Description	Alert’s Name	Alert’s Severity
33 - Threshold - Configuration Management Failed	The rule raises an alert when the same event occurs too many times and is considered as suspicious. Taxonomy: Configuration: Failed Administration Add/Delete/Modify Threshold: 3 events per minute	Multiple failed configuration management activities	🔔🟥
34 - Threshold - Configuration Management Success	The rule raises an alert when the same event occurs too many times and is considered as suspicious. Taxonomy: Configuration: Successful Administration Delete/Modify Threshold: 10 events per minute	Multiple successful configuration management activities	🔔🟧
35 - Threshold - Vulnerability	The rule raises an alert when some vulnerabilities are detected on the same target node defined in the asset database. Taxonomy: Vulnerability Status Threshold: 1 event per minute	Vulnerability detected	🔔🟧
36 - Threshold - Suspicious	The rule raises an alert when some suspicious activities are detected on the same target node defined in the asset database. Taxonomy: Suspicious Activity Threshold: 1 event per minute	Suspicious activity detected	🔔🟧
37 - Threshold - Malware	The rule raises an alert when some malware are detected on the same target node defined in the asset database Taxonomy: Malware Threshold: 1 event per minute	Malware detected	🔔🟧
38 - Threshold - Attack	The rule raises an alert when some attacks are detected on the same target node defined in the asset database. Taxonomy: Attack Threshold: 1 event per minute	Attack detected	🔔🟥

Table 143 Correlation Rules for Scenario

Name	Description	Alert’s Name	Alert’s Severity
39 - Corr. - Attacks T(Node+Srv.)	The rule correlates all attacks detected on same target node or service. This rule is used in a default scenario named “Known Vulnerability Exploited on same Target Node or Service”.	Known Vulnerabilities Exploited	🔔🟥
40 - Corr. - Vulnerabilities	The rule correlates all vulnerabilities detected on same target node or service. This rule is used in a default scenario named “Known Vulnerability Exploited on same Target Node or Service”.	Known Vulnerabilities Exploited	🔔🟥

Table 143 Correlation Rules for Scenario

Name	Description	Alert's Name	Alert's Severity
41 - Corr. - Attacks ST(Node+Srv.)	The rule correlates all attacks detected on same: ▪ source node or service ▪ or target node or service This rule is used in a default scenario named "Malicious Service Node Activities".	Suspect service node activities	🔔
42 - Corr. - Suspicious	The rule correlates all suspicious activities detected on same: ▪ source node or service ▪ or target node or service This rule is used in a default scenario named "Malicious Service Node Activities".	Suspect service node activities	🔔
43 - Corr. - Attacks T(Node)	The rule correlates all attacks detected on same target node. This rule is used in a default scenario named "Successful Target Node Attacks".	Successful Node Attacks	🔔
44 - Corr. - Configuration Activity	The rule correlates all configuration activities detected on same target node. This rule is used in a default scenario named "Successful Target Node Attacks".	Successful Node Attacks	🔔
45 - Corr. - Brute Force Detected	The rule correlates all brute force attacks detected on same target node or target users account. This rule is used in a default scenario named "Successful Target Node bruteforce".	Successful target node bruteforce	🔔
46 - Corr. - Login Success	The rule correlates all successful login detected on same target node and target users account ("root", "administrator", "admin", "administrator" by default). This rule is used in default scenario named "Successful Target Node bruteforce".	Successful target node bruteforce	🔔
47 - Corr. - Backdoor Detected	The rule correlates all detected backdoor (attacks or vulnerabilities) on a target node or service. This rule is used in default scenario named "Known Target Node Backdoor Acceded".	Known Target Node Backdoor Accessed	🔔
48 - Corr. - Connection success	The rule correlates all successful connection on the same target node and service defined in the asset database. This rule is used in default scenario named "Known Target Node Backdoor Accessed".	Known target node backdoor acceded	🔔
49 - Corr. - DOS Activities	The rule correlates all detected denial of services on a same target node. This rule is used in default scenario named "Successful Node DOS".	Successful Node DOS	🔔
50 - Corr. - Service Loss	The rule correlates all services unavailability on a same target node. This rule is used in default scenario named "Successful Node DOS".	Successful Node DOS	🔔

Table 143 Correlation Rules for Scenario

Name	Description	Alert's Name	Alert's Severity
51 - Corr. - Denied Activity	The rule correlates all kinds of denied activities on a same source or target node defined in the asset database. This rule is used in default scenario named "Malicious Node Activity".	Malicious Node Activity	🔔🟥
52 - Corr. - Attack or Suspicious	The rule correlates all kinds of attacks or suspicious activities performed on the same source or target node. This rule is used in default scenario named "Malicious Node Activity".	Malicious Node Activity	🔔🟥
53 - Corr. - Privilege Mgt. (T+S)	The rule correlates all kinds of configuration changes performed from a account on a target node. This rule is used in default scenario named "Segregation of duties violation".	Segregation of duties violation	🔔🟥
54 - Corr. - Privilege Mgt. (S+T)	The rule correlates all kinds of configuration changes performed on an account on a target node. This rule is used in default scenario named "Segregation of duties violation".	Segregation of duties violation	🔔🟥
55 - Corr. - Login Failed	The rule correlates all failed logins performed on an account on a target node. This rule is used in default scenario named "Suspected bruteforce".	Suspected bruteforce	🔔🟥
56 - Corr. - User Account Sharing	This rule raises an alert when the same login is used several times on a host from different locations defined in the asset database. Taxonomy: Standard Activity: Authentication Login Grouping method: ▪ Same login value ▪ Same target node ▪ 2 or more distinct source nodes	User Account sharing detected	🔔🟧
57 - Corr. - User Account Usurpation	This rule raises an alert when differents logins are used on a host from the same location. Taxonomy: Standard Activity: Authentication Login. Grouping method: ▪ Same source node ▪ Same target node ▪ 3 or more distinct logins	User Account usurpation detected	🔔🟧
58 - Corr. - Distributed DOS	This rule raises an alert when multiple DOS are detected from different source nodes. Taxonomy: Attack Identification: Detected Attack DoS Grouping method: ▪ Same target node ▪ 10 or more distinct source nodes	Distributed DOS detected	🔔🟥

Table 143 Correlation Rules for Scenario

Name	Description	Alert’s Name	Alert’s Severity
59 - Corr. - Port Scan	This rule raises an alert when someone tries to connect to a computer on different ports. Taxonomy: Standard Activity: Communication Grouping method: ▪ Same source node ▪ Same target node ▪ 50 or more distinct target services	Port scan detected	🔔
60 - Corr. US - Access to a Country under Embargo	The rule controls any illegal activity with countries that are under a specific US policies and embargoes: (http://www.pmddtc.state.gov/embargoed_countries/index.html) Afghanistan China Congo, The Democratic Republic of the Cuba Cyprus Eritrea Haiti Iran, Islamic Republic of Iraq Korea, Democratic People’s Republic of Lebanon Liberia Libyan Arab Jamahiriya Sierra Leone Sudan Syrian Arab Republic Venezuela Vietnam Yemen An alert is raised if there is any outbound connection to one of these countries. Taxonomy: Standard Activity: Successful Communication Grouping method: Source Node Name Or Address Target Node Name Or Address	Access detected to a country under embargo and/or restricted by US State Dept of trade policies	🔔

List of Rules for Scenarios

Please find below the Rules to apply for a scenario.

Table 144 Rules for Scenario

Scenario Name	Description	Alert's Name	Alert's Severity
1 - Known Vulnerability Exploited on same Target Node or Service	The scenario raises an alert when a known vulnerability is exploited by an attack. The alert generated has a high severity level. This scenario is based on the two following alerts: ▪ Corr. - Attacks T(Node+Srv.) ▪ Corr. - Vulnerabilities	Known Vulnerabilities Exploited	🔔❗
2 - Malicious Service Node Activities	The scenario raises an alert when both suspicious activities and attacks occur from a source host. The alert generated has a high severity level. This scenario is based on the two following alerts: ▪ Corr. - Attacks ST(Node+Srv.) ▪ Corr. - Suspicious	Suspect service node activities	🔔❗
3 - Successful Target Node Attacks	The scenario raises an alert when successful configuration activities are detected after an attack. The alert generated has a high severity level. This scenario is based on the two following alerts: ▪ Corr. - Attacks T(Node) ▪ Corr. -Configuration Activity	Successful node attacks	🔔❗
4 - Successful Target Node Bruteforce	The scenario raises an alert when successful login is detected after a bruteforce. The alert generated has a high severity level. This scenario is based on the two following alerts: ▪ Corr. - Brute Force Detected ▪ Corr. - Login Success	Successfully Target Node Bruteforce	🔔❗
5 - Known Target Node Backdoor Accessed	The scenario raises an alert when a known backdoor is successfully accessed. The alert generated has a high severity level. This scenario is based on the two following alerts: ▪ Corr. - Backdoor Detected ▪ Corr. - Connection success	Known target node backdoor acceessed	🔔❗
6 - Successful Node DOS	The scenario raises an alert when a service is no more available after a deny of service attack. The alert generated has a high severity level. This scenario is based on the two following alerts: ▪ Corr. - DOS Activities ▪ Corr. - Service Loss	Successful node DOS	🔔❗
7 - Malicious Node Activity	The scenario raises an alert when activities are denied after attack or suspicious activities. The alert generated has a high severity level. This scenario is based on the two following alerts: ▪ Corr. - Attack or Suspicious ▪ Corr. - Denied Activity	Malicious node activity	🔔❗

Table 144 Rules for Scenario

Scenario Name	Description	Alert's Name	Alert's Severity
8 - Segregation of duties violation	The scenario raises an alert when a user modifies his own account. The alert generated has a high severity level. This scenario is based on the two following alerts: Corr. - Privilege Mgt. (S+T) Corr. - Privilege Mgt. (T+S)	Segregation of duties violation	🔔!
9 - Suspected bruteforce	The scenario raises an alert when a login success is detected after multiple login failed. The alert generated has a high severity level. This scenario is based on the two following alerts: Corr. - Login Failed Corr. - Login Success	Suspected bruteforce	🔔!

Collection Policies

List of Default Collection Policies

Table 145 Default Collection Policies

Name	Description
exa_0_NoRawLog_NoElemEvent	**Raw logs**: None The log collector does not send raw logs to the SMP. **Elementary events**: None The log collector does not send elementary events to the SMP. No elementary events will be used by the SMP for archiving, correlation and reporting. Use this Collection Policy to disable Log Collector forwarding.
exa_1_NoRawLog_LightElemEvent	**Raw logs**: None The log collector does not send raw logs to the SMP. **Elementary events**: Light The log collector sends to the SMP only minimum of elementary events to preserve performances.
exa_2_NoRawLog_StandardElemEvent	**Raw logs**: None The log collector does not send raw logs to the SMP. **Elementary events**: Standard The log collector sends to the SMP only important elementary events to preserve performances.
exa_3_NoRawLog_AllElemEvent	**Raw logs**: None The log collector does not send raw logs to the SMP. **Elementary events**: All The log collector sends to the SMP all elementary events with a defined Taxonomy.
exa_4_NoRawLog_FullElemEvent	**Raw logs**: None The log collector does not send raw logs to the SMP. **Elementary events**: Full The log collector sends to the SMP all elementary events, including elementary events with no defined Taxonomy.

Table 145 Default Collection Policies

Name	Description
exa_5_LightRawLog_AllElemEvent	**Raw logs**: Light The log collector sends the minimum raw logs required by main IT Security Standards for archiving. **Elementary events**: All The log collector sends to the SMP all elementary events with a defined Taxonomy.
exa_6_StandardRawLog_AllElemEvent	**Raw logs**: Standard The log collector only sends raw logs recommended by main IT Security Standards for archiving. **Elementary events**: All The log collector sends to the SMP all elementary events with a defined Taxonomy.
exa_7_FullRawLog_AllElemEvent	**Raw logs**: Full The log collector sends all original logs to the SMP for Log archiving. **Elementary events**: All The log collector sends to the SMP all elementary events with a defined Taxonomy.
exa_8_FullRawLog_FullElemEvent	**Raw logs**: Full The log collector sends all original logs to the SMP for Log archiving. **Elementary events**: Full The log collector sends to the SMP all elementary events, including elementary events with no defined Taxonomy.

Note: Raw logs are used for archiving only. Elementary events are used for correlation and reporting.

List of Default Collection Rules

Below is the detailed predefined collection policy. It lists what policy will be applied according to the collected event type and performed action.

Table 146 Default Collection Rules

Name	Conditions		Actions	
	Event type	Action	Send Raw Log	Send Elementary Events
COLLECTION POLICY: _0_NoRawLog _NoElemEvent				
1 - Any event	(any) for all Taxonomy fields			
COLLECTION POLICY: _1_NoRawLog _LightElemEvent				
1 - Standard activity - Data access	Standard Activity	Data Access		X
2 - Standard activity - Data access	Standard Activity	Authentication		X
3 - Configuration activity - Administration	Configuration Activity	Administration		X
4 - Undefined Taxonomy	(none) for all Taxonomy fields			
5 - Any other event	(any) for all Taxonomy fields			
COLLECTION POLICY: _2_NoRawLog _StandardElemEvent				
1 - Data access use	Standard Activity	Data Access		X
2 - Gain use	Standard Activity	Gain		X
3 - Processing use	Standard Activity	Process		X
4 - Service availability use	Standard Activity	Service Availability		X

Table 146 Default Collection Rules

Name	**Conditions**		**Actions**	
	Event type	**Action**	**Send Raw Log**	**Send Elementary Events**
5 - State transition use	Standard Activity	State Transition		X
6 - User authentication use	Standard Activity	Authentication		X
7 - Account locking configuration	Configuration Activity	Account Administration		X
8 - Configuration management	Configuration Activity	Account Administration		X
9 - Attacks	Attack Identification	(any)		X
10 - Undefined	(none) for all Taxonomy fields			
11 - Any other event	(any) for all Taxonomy fields			
COLLECTION POLICY: _3_NoRawLog _AllElemEvent				
1 - Undefined Taxonomy	(none) for all Taxonomy fields			
2 - Any other event	(any) for all Taxonomy fields			X
COLLECTION POLICY: _4_NoRawLog _FullElemEvent				
1 - Undefined Taxonomy	(none) for all Taxonomy fields			X
2 - Any other event	(any) for all Taxonomy fields			X
COLLECTION POLICY: _5_LightRawLog _AllElemEvent				
1 - Standard activity - Data access	Standard Activity	Data Access	X	X
2 - Standard activity - User authentication	Standard Activity	Authentication	X	X
3 - Configuration activity - Administration	Configuration Activity	Administration	X	X
4 - Undefined Taxonomy	(none) for all Taxonomy fields			
5 - Any other event	(any) for all Taxonomy fields			X
COLLECTION POLICY: _6_StandardRawLog _AllElemEvent				
1 - Data access use	Standard Activity	Data Access	X	X
2 - Gain use	Standard Activity	Gain	X	X
3 - Processing use	Standard Activity	Process	X	X
4 - Service availability use	Standard Activity	Service Availability	X	X
5 - State transition use	Standard Activity	State Transition	X	X
6 - User authentication use	Standard Activity	Authentication	X	X
7 - Account locking configuration	Configuration Activity	Account	X	X
8 - Configuration management	Configuration Activity	Administration	X	X
9 - Attacks	Attack Identification	(any)	X	X
10 - Undefined Taxonomy	(none) for all field of Exa. Taxonomy			
11 - Any other event	(any) for all field of Exa. Taxonomy			X
COLLECTION POLICY: _7_FullRawLog _AllElemEvent				
Undefined Taxonomy	(none) for all Taxonomy field		X	
Any other event	(any) for all Taxonomy field		X	X

Table 146 Default Collection Rules

Name	Conditions		Actions	
	Event type	Action	Send Raw Log	Send Elementary Events
COLLECTION POLICY: _8_FullRawLog _FullElemEvent				
1 - Undefined Taxonomy	(none) for all Taxonomy field		X	X
2 - Any other event	(any) for all Taxonomy field		X	X

List of Predefined Dashboards

Table 147 List of Predefined Dashboards

Dashboards	2.4 - Network Security
1 - Access Control Security	
1.1 - Account Management	
1.1.1 - Account Registration	Remove or adjust access rights of all IT Systems users that leave or change function.
1.1.2 - Privilege Management	Restrict and control the allocation and use of privileges.
1.1.3 - Password Management	▪ Ensure that password management systems provide quality passwords. ▪ Ensure that passwords are regularly changed.
1.2 - User Access	
1.2.1 - System Access	▪ Prevent unauthorized access to IT Systems. ▪ Ensure authorized access to IT Systems.
1.2.2 - Data Access	Prevent unauthorized access to information held in application systems.
1.3 - Remote Access	
1.3.1 - Virtual Private Networks (VPNs)	▪ Prevent unauthorized remote access to IT Systems. ▪ Use secure authentication methods to control remote users' access.
1.3.2 - Remote Administration Security	Control logical access to system configuration interfaces.
2 - Operation Security	
2.1 - Malware Protection	
2.1.1 - Antivirus System States	Control software protection activity against malware.
2.1.2 - Antivirus Updates	Control the activity of software protection against malware.
2.1.3 - Malware Protection	Control malware activity detection on IT Systems.
2.1.4 - Malware Infection	Control if malware-infected files are correctly cleaned up.
2.2 - Data Exchange	
2.2.1 - E-Mails	Control information involved in electronic messages.
2.2.2 - Instant Messaging	Control information involved in instant messaging.
2.3 - Operation Security Management	
2.3.1 - Configuration Management	Log system administrators and operators activity.
2.3.2 - Log Protection	Protect logging devices and logs against tampering and unauthorized access.

Table 147 List of Predefined Dashboards

Dashboards	**2.4 - Network Security**
2.3.3 - Clock Synchronization	▪ Synchronize clocks of all relevant IT Systems within an organization or security domain with an agreed accurate time source. ▪ Control clock synchronization on systems to prevent problems in logs interpretation or authentication systems.
2.4 - Network Security	
2.4.1 - Network Segregation	▪ Control that the segregation policy defined between different networks is efficient. ▪ Ensure that groups of information services, users, and information systems are segregated on networks.
2.4.2 - Network Routing Control	Ensure that computer connections and information flows do not breach the access control policy.
2.5 - Incident and Alert Management	
2.5.1 Alert Activity	▪ Detect unauthorized IT processing activities. ▪ Monitor use of IT Systems. ▪ Log IT Systems faults.
2.5.2 Alert Management	▪ Review regularly the IT Systems' monitoring activity. ▪ Analyze and correct IT Systems' faults.
3 - Asset Security	
3.1 - Asset Identification	
3.1.1 - Asset Inventory and Ownership	▪ Achieve and maintain appropriate protection of organizational assets. ▪ Identify all assets and maintain an inventory. ▪ Identify for each asset the part of the organization that owns it.
3.2 - Change Management	
3.2.1 - Change Management	Control authorization levels of information processing facilities and systems.
3.3 - Backup Management	
3.3.1 - Backup Management	▪ Maintain the integrity and availability of information and information processing facilities. ▪ Take regular back-up copies of IT Systems.
3.4 - Capacity Management	
3.4.1 - Capacity Management	▪ Minimize the risk of IT Systems failures. ▪ Monitor and enhance resources' use. ▪ Anticipate future systems capacity requirements.
3.5 - Vulnerability Management	
3.5.1 - Vulnerability Management	▪ Reduce risks resulting from exploitation of published technical vulnerabilities. ▪ Evaluate organization's exposure to vulnerabilities. ▪ Take measures to address the vulnerabilities associated risk. ▪ Ensure compliance of systems with organizational security policies and standards.
3.6 - Asset Availability	
3.6.1 - Asset Availability	Implement and maintain appropriate level of information security and service delivery.

Table 147 List of Predefined Dashboards

Dashboards	**2.4 - Network Security**
4 - Executive Report	
Monthly Executive Report	Combines all default security dashboards in a single static monthly report. It provides a monthly overview of the whole enterprise IT security status.
5 - Regulatory Compliance	
5.1 - Standards Mapping	
Standards Mapping and Coverage	Shows for each main Standard IT all controls covered by TIBCO LogLogic® Security Dashboards.
5.2 - FSA	
Monthly FSA Compliance Report	Gives a global FSA compliant report on a monthly basis.
5.3 - PCI-DSS	
Monthly PCI-DSS Compliance Report	Gives a global PCI-DSS compliant report on a monthly basis.
5.4 - Sarbanes-Oxley	
Monthly SOX Compliance Report	Gives a global SOX compliant report on a monthly basis.
6 - SANS Top 5	
6.1 - Attempts to Gain Access Through Existing Accounts	
6.1.1 - SANS - System Access	▪ Prevent unauthorized access to IT Systems. ▪ Ensure authorized access to IT Systems.
6.2 - Failed File or Resource Access Attempts	
6.2.1 - SANS - Data Access	Prevent unauthorized access to information held in application systems.
6.3 - Unauthorized Changes to Users, Groups and Services	
6.3.1 - SANS - Account Registration	Remove or adjust access rights of all IT System users that leave or change function.
6.3.2 - SANS - Privilege Management	Restrict and control the allocation and use of privileges.
6.4 - Systems Most Vulnerable to Attack	
6.4.1 - SANS - Vulnerability Management	▪ Reduce risks resulting from exploitation of published technical vulnerabilities. ▪ Evaluate organization's exposure to vulnerabilities. ▪ Take measures to address the vulnerabilities associated risk. ▪ Ensure compliance of systems with organizational security policies and standards.
6.5 - Suspicious or Unauthorized Network Traffic Patterns	
6.5.1 - SANS - Network Routing Control	Ensure that computer connections and information flows do not breach the access control policy.
7 - PDF Reports	
7.1 - Executive	
Store Monthly Executive Report in PDF format	
7.2 - FSA	
StoreMonthly FSA Compliance Report in PDF format	
7.3 - PCI-DSS	
Store Monthly PCI-DSS Compliance Report in PDF format	
7.4 - Sarbanes-Oxley	

Table 147 List of Predefined Dashboards

Dashboards	**2.4 - Network Security**
Store Monthly SOX Compliance Report in PDF format	
7.5 - Other Reports	
Store other reports in PDF format	

List of Default Live Reporting Policies

Table 148 List of Default Live Reporting Policies

#	Name	Description
1	Backup Management	This rule generates a reporting table for backup management. **Condition**: the reporting table is based on elementary events with the following Taxonomy: ▪ Standard Activity: Error backup management ▪ Standard Activity: Failed backup management ▪ Standard Activity: Successful backup management **Group**: the reporting table contains one line for each values of the following fields: ▪ TIBCO LogLogic® Taxonomy - Result ▪ Target Asset Name
2	Capacity Management	This rule generates a reporting table for capacity management. **Condition**: the reporting table is based on elementary events with the following Taxonomy: ▪ Information Status: Threshold **Group**: the reporting table contains one line for each values of the following fields: ▪ TIBCO LogLogic® Taxonomy - Result ▪ Target Asset Name
3	Vulnerability Management	This rule generates a reporting table for vulnerability management. **Condition**: the reporting table is based on elementary events with the following Taxonomy: ▪ Authentication Vulnerability Status: Detected Vulnerability ▪ Rights Vulnerability Status: Detected Vulnerability ▪ System Vulnerability Status: Detected Vulnerability **Group**: the reporting table contains one line for each values of the following fields: ▪ TIBCO LogLogic® Taxonomy - Access Layer ▪ Target Asset Name

Table 148 List of Default Live Reporting Policies

#	Name	Description
4	Asset Availability	This rule generates a reporting table for business services availability. **Condition**: the reporting table is based on elementary events with the following Taxonomy: ▪ System Standard Activity: Error service availability up ▪ System Standard Activity: Successful service availability down **Group**: the reporting table contains one line for each values of the following fields: ▪ TIBCO LogLogic® Taxonomy - Result ▪ Target Asset Name
5	Account Registration	This rule generates a reporting table for account registration. **Condition**: the reporting table is based on elementary events with the following Taxonomy: ▪ Authentication Configuration Activity: Successful account ▪ Authentication Configuration Activity: Successful administration **Group**: the reporting table contains one line for each values of the following fields: ▪ TIBCO LogLogic® Taxonomy - Action detail ▪ Target Host Group Name ▪ Target User Name
6	Privilege Management	This rule generates a reporting table for privilege management. **Condition**: the reporting table is based on elementary events with the following Taxonomy: ▪ Rights Configuration Activity: Successful administration **Group**: the reporting table contains one line for each values of the following fields: ▪ TIBCO LogLogic® Taxonomy - Action detail ▪ Target Host Group Name ▪ Target User Name
7	Password Management	This rule generates a reporting table for password management. **Condition**: the reporting table is based on elementary events with the following Taxonomy: ▪ Authentication Configuration Activity: Administration modify on account password **Group**: the reporting table contains one line for each values of the following fields: ▪ TIBCO LogLogic® Taxonomy - Result ▪ Target Host Group Name ▪ Target User Name

Table 148 List of Default Live Reporting Policies

#	Name	Description
8	System Access	This rule generates a reporting table for system access. **Condition**: the reporting table is based on elementary events with the following Taxonomy: ▪ Authentication Standard Activity: Error authentication login ▪ Authentication Standard Activity: Failed authentication login ▪ Authentication Standard Activity: Successful authentication login **Group**: the reporting table contains one line for each values of the following fields: ▪ TIBCO LogLogic® Taxonomy - Result ▪ Target Host Group Name ▪ Target User Name
9	Data Access	This rule generates a reporting table for data access. **Condition**: the reporting table is based on elementary events with the following Taxonomy: ▪ Standard Activity: Error data access ▪ Standard Activity: Failed data access ▪ Standard Activity: Successful data access **Group**: the reporting table contains one line for each values of the following fields: ▪ TIBCO LogLogic® Taxonomy - Result ▪ Target Host Group Name
10	Virtual Private Network	This rule generates a reporting table for remote access security. **Condition**: the reporting table is based on elementary events with the following Taxonomy: ▪ Authentication Standard Activity: Failed authentication login on VPN account ▪ Authentication Standard Activity: Successful authentication login on VPN account ▪ System Standard Activity: Error communication connect on VPN tunnel ▪ System Standard Activity: Successful communication connect on VPN tunnel ▪ **Group**: the reporting table contains one line for each values of the following fields: ▪ TIBCO LogLogic® Taxonomy - Result ▪ TIBCO LogLogic® Taxonomy - Target Detail ▪ Target Host Group Name
11	Remote Administration Security	This rule generates a reporting table for remote administration security. **Condition**: the reporting table is based on elementary events with the following Taxonomy: ▪ Authentication Standard Activity: Failed authentication login on admin ▪ Authentication Standard Activity: Successful authentication login on admin **Group**: the reporting table contains one line for each values of the following fields: ▪ TIBCO LogLogic® Taxonomy - Result ▪ Target Host Group Name

Table 148 List of Default Live Reporting Policies

#	Name	Description
12	Network Segregation	This rule generates a reporting table for network segregation. **Condition**: the reporting table is based on elementary events with the following Taxonomy: - Attack Identification: Detected attack spoofing - Suspicious Activity Identification: Detected suspicious spoofing - Vulnerability Status: Detected vulnerability spoofing **Group**: the reporting table contains one line for each values of the following fields: - TIBCO LogLogic® Taxonomy - Event Type - Target Host Group Name
13	Network Servers	This rule generates a reporting table for network servers. **Condition**: the reporting table is based on elementary events with the following Taxonomy: - System Standard Activity: Denied communication - System Standard Activity: Successful communication **Group**: the reporting table contains one line for each values of the following fields: - TIBCO LogLogic® Taxonomy - Result - Target Host Group Name - Target Node Name (else Address) - Target Service Name (else Port)
14	Antivirus System State	This rule generates a reporting table for antivirus software process states. **Condition**: the reporting table is based on elementary events with the following Taxonomy: - System Standard Activity: Successful state transition on antivirus **Group**: the reporting table contains one line for each values of the following fields: - TIBCO LogLogic® Taxonomy - Action Detail - Target Host Group Name
15	Antivirus Updates	This rule generates a reporting table for antivirus upgrade activity. **Condition**: the reporting table is based on elementary events with the following Taxonomy: - System Configuration Activity: Error update on antivirus - System Configuration Activity: Successful update on antivirus **Group**: the reporting table contains one line for each values of the following fields: - TIBCO LogLogic® Taxonomy - Result - Target Host Group Name

Table 148 List of Default Live Reporting Policies

#	Name	Description
16	Malware Protection	This rule generates a reporting table for malware protection. **Condition**: the reporting table is based on elementary events with the following Taxonomy: ▪ System Malware Identification: Detected malware **Group**: the reporting table contains one line for each values of the following fields: ▪ TIBCO LogLogic® Taxonomy - Action Detail ▪ Source Node Address Country Code ▪ Target Host Group Name ▪ Target Tool Name
17	Malware Infection	This rule generates a reporting table for malware protection (virus cleaned). **Condition**: the reporting table is based on elementary events with the following Taxonomy: ▪ System Configuration Activity: Error repair on antivirus file ▪ System Configuration Activity: Successful repair on antivirus file **Group**: the reporting table contains one line for each values of the following fields: ▪ TIBCO LogLogic® Taxonomy - Result ▪ Target Host Group Name
18	EMails	This rule generates a reporting table for E-Mails. **Condition**: the reporting table is based on elementary events with the following Taxonomy: ▪ System Malware Identification: Detected malware spam on mail ▪ System Malware Identification: Detected malware virus on mail ▪ System Standard Activity: Successful data exchange on mail message **Group**: the reporting table contains one line for each values of the following fields: ▪ TIBCO LogLogic® Taxonomy - Result ▪ TIBCO LogLogic® Taxonomy - Action Detail
19	Instant Messaging	This rule generates a reporting table for instant messaging. **Condition**: the reporting table is based on elementary events with the following Taxonomy: ▪ Detected chat **Group**: the reporting table contains one line for each values of the following fields: ▪ Target User Name (else Number) ▪ Source Node Name (else Address)

Table 148 List of Default Live Reporting Policies

#	Name	Description
20	Configuration Management	This rule generates a reporting table for configuration management. **Condition**: the reporting table is based on elementary events with the following Taxonomy: ▪ System Configuration Activity: Error administration ▪ System Configuration Activity: Successful administration ▪ System Configuration Activity: Successful repair ▪ System Configuration Activity: Error repair ▪ System Configuration Activity: Successful update ▪ System Configuration Activity: Error update **Group**: the reporting table contains one line for each values of the following fields: ▪ TIBCO LogLogic® Taxonomy - Result ▪ TIBCO LogLogic® Taxonomy - Action Detail ▪ Target Host Group Name ▪ Source User Name (else Number)
21	Log Protection	This rule generates a reporting table for protection of log information. **Condition**: the reporting table is based on elementary events with the following Taxonomy: ▪ Configuration Activity: Successful action on log file ▪ Standard Activity: Successful action on log file ▪ System Attack Identification: Detected actionattack on log file ▪ System Malware Identification: Detected actionmalware on log file ▪ System Suspicious Activity Identification: Detected actionsuspicious on log file **Group**: the reporting table contains one line for each values of the following fields: ▪ TIBCO LogLogic® Taxonomy - Event Type ▪ Target Host Group Name
22	Clock Synchronization	This rule generates a reporting table for clock synchronization. **Condition**: the reporting table is based on elementary events with the following Taxonomy: ▪ System Configuration Activity: Any result on time target ▪ System Information Status: Any result on time target ▪ System Standard Activity: Any result on time target **Group**: the reporting table contains one line for each values of the following fields: ▪ TIBCO LogLogic® Taxonomy - Event Type ▪ Target Host Group Name
23	Event by Log Source and Severity	This rule generates a reporting table for collected elementary events. No condition **Group**: the reporting table contains one line for each values of the following fields: ▪ Severity ▪ Log Source Id

Table 148 List of Default Live Reporting Policies

#	Name	Description
24	Event by Log Source and Taxonomy	This rule generates a reporting table for elementary event's Taxonomy. No condition **Group**: the reporting table contains one line for each values of the following fields: - Severity - TIBCO LogLogic® Taxonomy - Access Layer - TIBCO LogLogic® Taxonomy - Event Type - TIBCO LogLogic® Taxonomy - Result - TIBCO LogLogic® Taxonomy - Action - TIBCO LogLogic® Taxonomy - Action Detail - TIBCO LogLogic® Taxonomy - Target - TIBCO LogLogic® Taxonomy - Target Detail
25	Network Clients	This rule generates a reporting table for network clients. **Condition**: the reporting table is based on elementary events with the following Taxonomy: - System Standard Activity: Denied communication - System Standard Activity: Successful communication **Group**: the reporting table contains one line for each values of the following fields: - TIBCO LogLogic® Taxonomy - Result - Source Host Group Name - Source Node Name (else Address) - Target Service Name (else Port)

List of Default Batch Reporting Policies

Table 149 List of Default Batch Reporting Policies

Name	Description
1_2_Change_Management	Controls authorization levels of information processing facilities and systems.
3_3_2_Incident_Management	Review regularly the IT Systems' monitoring activity. Analyze and correct IT Systems' faults.
Alert Attacker	Display the alerts from the Attacker's point of view, i.e. it gives information about the machine from which the attack came.
Alert Victim	Display the alerts from the Victim's point of view, i.e. it gives information about the machine which was impacted by the attack.

List of Reporting Tables

Table 150 List of Reporting Tables

Dashboards	Reports	Data Dictionary	Main Tables
1 - Access Control Security			
1.1 Account Management			

Table 150 List of Reporting Tables

Dashboards	Reports	Data Dictionary	Main Tables
1.1.1 - Account Registration	TOP Account Registration (per day)	AccountReg-Day	Exa_TAT_Live_2_1_1_Account_Registration_day
	TOP Account Registration (per month)	AccountReg-Month	Exa_TAT_Live_2_1_1_Account_Registration_month
	Account Registration Activity (per day)	AccountReg-Day	Exa_TAT_Live_2_1_1_Account_Registration_day
	Account Registration Activity (per hour)	AccountReg-Hour	Exa_TAT_Live_2_1_1_Account_Registration_hour
	Account Registration Activity (per month)	AccountReg-Month	Exa_TAT_Live_2_1_1_Account_Registration_month
	Account Registration by Host Group (per day)	AccountReg-Day	Exa_TAT_Live_2_1_1_Account_Registration_day
	Account Registration by Host Group (per hour)	AccountReg-Hour	Exa_TAT_Live_2_1_1_Account_Registration_hour
	Account Registration by Host Group (per month)	AccountReg-Month	Exa_TAT_Live_2_1_1_Account_Registration_month
	Account Registration Events	AccountReg-Table	Exa_Alert
1.1.2 - Privilege Management	TOP Privilege Management (per day)	PrivMgt-day	Exa_TAT_Live_2_1_2_Privilege_Management_day
	TOP Privilege Management (per month)	PrivMgt-Month	Exa_TAT_Live_2_1_2_Privilege_Management_month
	Privilege Management Activity (per day)	PrivMgt-day	Exa_TAT_Live_2_1_2_Privilege_Management_day
	Privilege Management Activity (per hour)	PrivMgt-Hour	Exa_TAT_Live_2_1_2_Privilege_Management_hour
	Privilege Management Activity (per month)	PrivMgt-Month	Exa_TAT_Live_2_1_2_Privilege_Management_month
	Privilege Management by Host Group (per day)	PrivMgt-day	Exa_TAT_Live_2_1_2_Privilege_Management_day
	Privilege Management by Host Group (per hour)	PrivMgt-Hour	Exa_TAT_Live_2_1_2_Privilege_Management_hour
	Privilege Management by Host Group (per month)	PrivMgt-Month	Exa_TAT_Live_2_1_2_Privilege_Management_month
	Privilege Management Events	PrivMgt-Table	Exa_Alert

Table 150 List of Reporting Tables

Dashboards	Reports	Data Dictionary	Main Tables
1.1.3 - Password Management	TOP Password Management (per day)	PassMgt-Day	Exa_TAT_Live_2_1_3_Password_Management_day
	TOP Password Management (per month)	PassMgt-Month	Exa_TAT_Live_2_1_3_Password_Management_month
	Password Management Activity (per day)	PassMgt-Day	Exa_TAT_Live_2_1_3_Password_Management_day
	Password Management Activity (per hour)	PassMgt-Hour	Exa_TAT_Live_2_1_3_Password_Management_hour
	Password Management Activity (per month)	PassMgt-Month	Exa_TAT_Live_2_1_3_Password_Management_month
	Password Management by Host Group (per day)	PassMgt-Day	Exa_TAT_Live_2_1_3_Password_Management_day
	Password Management by Host Group (per hour)	PassMgt-Hour	Exa_TAT_Live_2_1_3_Password_Management_hour
	Password Management by Host Group (per month)	PassMgt-Month	Exa_TAT_Live_2_1_3_Password_Management_month
	Password Management Events	PassMgt-Table	Exa_Alert
1.2 - User Access			
1.2.1 - System Access	TOP System Access (per hour)	SysAccess-Hour	Exa_TAT_Live_2_2_1_System_Access_hour
	TOP System Access (per day)	SysAccess-Hour	Exa_TAT_Live_2_2_1_System_Access_day
	TOP System Access (per month)	SysAccess-Hour	Exa_TAT_Live_2_2_1_System_Access_month
	System Access Activity (per day)	SysAccess-Day	Exa_TAT_Live_2_2_1_System_Access_day
	System Access Activity (per hour)	SysAccess-Hour	Exa_TAT_Live_2_2_1_System_Access_hour
	System Access Activity (per month)	SysAccess-Month	Exa_TAT_Live_2_2_1_System_Access_month
	System Access by Host Group (per day)	SysAccess-Day	Exa_TAT_Live_2_2_1_System_Access_day
	System Access by Host Group (per hour)	SysAccess-Hour	Exa_TAT_Live_2_2_1_System_Access_hour
	System Access by Host Group (per month)	SysAccess-Month	Exa_TAT_Live_2_2_1_System_Access_month

Table 150 List of Reporting Tables

Dashboards	**Reports**	**Data Dictionary**	**Main Tables**
1.2.2 - Data Access	TOP Data Access (per month)	DataAccess-Month	Exa_TAT_Live_2_2_2_Data_Access_month
	Data Access Activity (per day)	DataAccess-Day	Exa_TAT_Live_2_2_2_Data_Access_day
	Data Access Activity (per hour)	DataAccess-Hour	Exa_TAT_Live_2_2_2_Data_Access_hour
	Data Access Activity (per month)	DataAccess-Month	Exa_TAT_Live_2_2_2_Data_Access_month
	Data Access by Host Group (per day)	DataAccess-Day	Exa_TAT_Live_2_2_2_Data_Access_day
	Data Access by Host Group (per hour)	DataAccess-Hour	Exa_TAT_Live_2_2_2_Data_Access_hour
	Data Access by Host Group (per month)	DataAccess-Month	Exa_TAT_Live_2_2_2_Data_Access_month
	Data Access Events	DataAccess-Table	Exa_Alert
1.3 - Remote Access			
1.3.1 - Virtual Private Networks	TOP Remote Access Security (per month)	RmAccessSec-Month	Exa_TAT_Live_2_3_1_Remote_Security_Ctrl_month
	Remote Access Security Events	RmAccessSec-Table	Exa_Alert
	Remote Site to Site VPN (per day)	RmAccessSec-Day	Exa_TAT_Live_2_3_1_Remote_Security_Ctrl_day
	Remote Site to Site VPN (per hour)	RmAccessSec-Hour	Exa_TAT_Live_2_3_1_Remote_Security_Ctrl_hour
	Remote Site to Site VPN (per month)	RmAccessSec-Month	Exa_TAT_Live_2_3_1_Remote_Security_Ctrl_month
	Remote Users VPN (per day)	RmAccessSec-Day	Exa_TAT_Live_2_3_1_Remote_Security_Ctrl_day
	Remote Users VPN (per hour)	RmAccessSec-Hour	Exa_TAT_Live_2_3_1_Remote_Security_Ctrl_hour
	Remote Users VPN (per month)	RmAccessSec-Month	Exa_TAT_Live_2_3_1_Remote_Security_Ctrl_month
1.3.2 - Remote Administration Security	TOP Remote Administration Security (per month)	RmAdminSec-Month	Exa_TAT_Live_2_3_2_Remote_Admin_Sec_month
	Remote Administration Security Activity (per day)	RmAdminSec-Day	Exa_TAT_Live_2_3_2_Remote_Admin_Sec_day
	Remote Administration Security Activity (per hour)	RmAdminSec-Hour	Exa_TAT_Live_2_3_2_Remote_Admin_Sec_hour
	Remote Administration Security Activity (per month)	RmAdminSec-Month	Exa_TAT_Live_2_3_2_Remote_Admin_Sec_month
	Remote Administration Security by Host Group (per day)	RmAdminSec-Day	Exa_TAT_Live_2_3_2_Remote_Admin_Sec_day
	Remote Administration Security by Host Group (per hour)	RmAdminSec-Hour	Exa_TAT_Live_2_3_2_Remote_Admin_Sec_hour
	Remote Administration Security by Host Group (per month)	RmAdminSec-Month	Exa_TAT_Live_2_3_2_Remote_Admin_Sec_month
	Remote Administration Security Events	RmAdminSec-Table	Exa_Alert

Table 150 List of Reporting Tables

Dashboards	Reports	Data Dictionary	Main Tables
2 - Operation Security			
2.1 - Malware Protection			
2.1.1 - Antivirus System States	TOP Antivirus Process States (per month)	AVProcState-Month	Exa_TAT_Live_3_1_1_month
	Antivirus Process States by Host Group (per hour)	AVProcState-Hour	Exa_TAT_Live_3_1_1_hour
	Antivirus Process States Activity (per day)	AVProcState-Day	Exa_TAT_Live_3_1_1_day
	Antivirus Process States Activity (per hour)	AVProcState-Hour	Exa_TAT_Live_3_1_1_hour
	Antivirus Process States Activity (per month)	AVProcState-Month	Exa_TAT_Live_3_1_1_month
	Antivirus Process States by Host Group (per day)	AVProcState-Day	Exa_TAT_Live_3_1_1_day
	Antivirus Process States by Host Group (per month)	AVProcState-Month	Exa_TAT_Live_3_1_1_month
	Antivirus Process States Events	AVProcState-Table	Exa_Alert
2.1.2 - Antivirus Updates	TOP Antivirus updates (per month)	AVUpdate-Month	Exa_TAT_Live_3_1_1_Antivirus_Upgrade_Activity_month
	Antivirus updates Activity (per day)	AVUpdate-Day	Exa_TAT_Live_3_1_1_Antivirus_Upgrade_Activity_day
	Antivirus updates Activity (per hour)	AVUpdate-Hour	Exa_TAT_Live_3_1_1_Antivirus_Upgrade_Activity_hour
	Antivirus updates Activity (per month)	AVUpdate-Month	Exa_TAT_Live_3_1_1_Antivirus_Upgrade_Activity_month
	Antivirus updates by Host Group (per day)	AVUpdate-Day	Exa_TAT_Live_3_1_1_Antivirus_Upgrade_Activity_day
	Antivirus updates by Host Group (per hour)	AVUpdate-Hour	Exa_TAT_Live_3_1_1_Antivirus_Upgrade_Activity_hour
	Antivirus updates by Host Group (per month)	AVUpdate-Month	Exa_TAT_Live_3_1_1_Antivirus_Upgrade_Activity_month
	Antivirus updates Events	AVUpdate-Table	Exa_Alert

Table 150 List of Reporting Tables

Dashboards	Reports	Data Dictionary	Main Tables
2.1.3 - Malware Protection	TOP Malware Protection (per month)	MalProtMap-Month	Exa_TAT_Live_3_1_2_Malware_Protection_month
	TOP Malware Protection (per hour)	MalProtMap-Hour	Exa_TAT_Live_3_1_2_Malware_Protection_hour
	TOP Malware Protection (per day)	MalProtMap-Day	Exa_TAT_Live_3_1_2_Malware_Protection_day
	Malware Protection Map (per day)	MalProtMap-Day	Exa_TAT_Live_3_1_2_Malware_Protection_day
	Malware Protection Map (per hour)	MalProtMap-Hour	Exa_TAT_Live_3_1_2_Malware_Protection_hour
	Malware Protection Map (per month)	MalProtMap-Month	Exa_TAT_Live_3_1_2_Malware_Protection_month
	Malware Protection Source Map (per day)	MalProtMap-Day	Exa_TAT_Live_3_1_2_Malware_Protection_day
	Malware Protection Source Map (per hour)	MalProtMap-Hour	Exa_TAT_Live_3_1_2_Malware_Protection_hour
	Malware Protection Source Map (per month)	MalProtMap-Month	Exa_TAT_Live_3_1_2_Malware_Protection_month
2.1.4 - Malware Infection	TOP Malware Protection Infection (per month)	MalProtInf-Month	Exa_TAT_Live_3_1_2_Malware_Prot_Virus_Cln_month
	Malware Protection Infection Activity (per day)	MalProtInf-Day	Exa_TAT_Live_3_1_2_Malware_Prot_Virus_Cln_day
	Malware Protection Infection Activity (per hour)	MalProtInf-Hour	Exa_TAT_Live_3_1_2_Malware_Prot_Virus_Cln_hour
	Malware Protection Infection Activity (per month)	MalProtInf-Month	Exa_TAT_Live_3_1_2_Malware_Prot_Virus_Cln_month
	Malware Protection Infection by Host Group (per day)	MalProtInf-Day	Exa_TAT_Live_3_1_2_Malware_Prot_Virus_Cln_day
	Malware Protection Infection by Host Group (per hour)	MalProtInf-Hour	Exa_TAT_Live_3_1_2_Malware_Prot_Virus_Cln_hour
	Malware Protection Infection by Host Group (per month)	MalProtInf-Month	Exa_TAT_Live_3_1_2_Malware_Prot_Virus_Cln_month
	Malware Protection Infection Events	MalProtInf-Table	Exa_Alert
2.2 - Data Exchange			
2.2.1 - E-Mails	TOP Emails (per month)	Emails-Month	Exa_TAT_Live_3_2_1_EMails_month
	Emails Activity (per day)	Emails-Day	Exa_TAT_Live_3_2_1_EMails_day
	Emails Activity (per hour)	Emails-Hour	Exa_TAT_Live_3_2_1_EMails_hour
	Emails Activity (per month)	Emails-Month	Exa_TAT_Live_3_2_1_EMails_month
	Emails Events	Emails-Table	Exa_Alert
	Malicious Emails (per day)	Emails-Day	Exa_TAT_Live_3_2_1_EMails_day
	Malicious Emails (per hour)	Emails-Hour	Exa_TAT_Live_3_2_1_EMails_hour
	Malicious Emails (per month)	Emails-Month	Exa_TAT_Live_3_2_1_EMails_month

Table 150 List of Reporting Tables

Dashboards	Reports	Data Dictionary	Main Tables
2.2.2 - Instant Messaging	TOP Instant Messaging (per month)	InstantMsg-Month	Exa_TAT_Live_3_2_2_Instant_Messaging_month
	Instant Messaging Activity (per day)	InstantMsg-Day	Exa_TAT_Live_3_2_2_Instant_Messaging_day
	Instant Messaging Activity (per hour)	InstantMsg-Hour	Exa_TAT_Live_3_2_2_Instant_Messaging_hour
	Instant Messaging Activity (per month)	InstantMsg-Month	Exa_TAT_Live_3_2_2_Instant_Messaging_month
	Instant Messaging Events	InstantMsg-Table	Exa_Alert
	Instant messaging TOP	InstantMsg-Hour	Exa_TAT_Live_3_2_2_Instant_Messaging_hour
2.3 - Operation Security Management			
2.3.1 - Configuration management	TOP Configuration Management (per day)	ConfMgt-Day	Exa_TAT_Live_3_4_1_day
	TOP Configuration Management (per month)	ConfMgt-Month	Exa_TAT_Live_3_4_1_month
	Configuration Management Activity (per day)	ConfMgt-Day	Exa_TAT_Live_3_4_1_day
	Configuration Management Activity (per hour)	ConfMgt-Hour	Exa_TAT_Live_3_4_1_hour
	Configuration Management Activity (per month)	ConfMgt-Month	Exa_TAT_Live_3_4_1_month
	Configuration Management by Host Group (per day)	ConfMgt-Day	Exa_TAT_Live_3_4_1_day
	Configuration Management by Host Group (per month)	ConfMgt-Month	Exa_TAT_Live_3_4_1_month
	Configuration Management by Hostgroup (per hour)	ConfMgt-Hour	Exa_TAT_Live_3_4_1_hour
	Configuration Management Events	ConfMgt-Table	Exa_Alert
2.3.2 - Clock Synchronization	TOP Clock Synchronization (per month)	ClockSync-Month	Exa_TAT_Live_3_4_3_Clock_Synchronization_month
	Clock Synchronization Activity (per hour)	ClockSync-Hour	Exa_TAT_Live_3_4_3_Clock_Synchronization_hour
	Clock Synchronization Activity (per day)	ClockSync-Day	Exa_TAT_Live_3_4_3_Clock_Synchronization_day
	Clock Synchronization Activity (per month)	ClockSync-Month	Exa_TAT_Live_3_4_3_Clock_Synchronization_month
	Clock Synchronization by Host Group (per hour)	ClockSync-Hour	Exa_TAT_Live_3_4_3_Clock_Synchronization_hour
	Clock Synchronization by Host Group (per day)	ClockSync-Day	Exa_TAT_Live_3_4_3_Clock_Synchronization_day
	Clock Synchronization by Host Group (per month)	ClockSync-Month	Exa_TAT_Live_3_4_3_Clock_Synchronization_month
	Clock Synchronization Events	ClockSync-Table	Exa_Alert
2.4 - Network Security			

Table 150 List of Reporting Tables

Dashboards	Reports	Data Dictionary	Main Tables
2.4.1 - Network Segregation	TOP Network Segregation (per month)	NetSeg-Month	Exa_TAT_Live_2_3_3_Segregation_In_Network_month
	Network Segregation Activity (per day)	NetSeg-Day	Exa_TAT_Live_2_3_3_Segregation_In_Network_day
	Network Segregation Activity (per hour)	NetSeg-Hour	Exa_TAT_Live_2_3_3_Segregation_In_Network_hour
	Network Segregation Activity (per month)	NetSeg-Month	Exa_TAT_Live_2_3_3_Segregation_In_Network_month
	Network Segregation by Host Group (per day)	NetSeg-Day	Exa_TAT_Live_2_3_3_Segregation_In_Network_day
	Network Segregation by Host Group (per hour)	NetSeg-Hour	Exa_TAT_Live_2_3_3_Segregation_In_Network_hour
	Network Segregation by Host Group (per month)	NetSeg-Month	Exa_TAT_Live_2_3_3_Segregation_In_Network_month
	Network Segregation Events	NetSeg-Table	Exa_Alert
2.4.2 - Network Servers	TOP Servers (per day)	NetServers-TOP-Day	Exa_TAT_Live_2_3_4_Network_Routing_Ctrl_day
	TOP Servers (per hour)	NetServers-TOP-Hour	Exa_TAT_Live_2_3_4_Network_Routing_Ctrl_hour
	TOP Servers (per month)	NetServers-TOP-Month	Exa_TAT_Live_2_3_4_Network_Routing_Ctrl_month
	Network Connections (per day)	NetServers-Act-Day	Exa_TAT_Live_2_3_4_Network_Routing_Ctrl_day
	Network Connections (per hour)	NetServers-Act-Hour	Exa_TAT_Live_2_3_4_Network_Routing_Ctrl_hour
	Network Connections (per month)	NetServers-Act-Month	Exa_TAT_Live_2_3_4_Network_Routing_Ctrl_month
	Network Connections by Server Group (per day)	NetServers-Host-Day	Exa_TAT_Live_2_3_4_Network_Routing_Ctrl_day
	Network Connections by Server Group (per hour)	NetServers-Host-Hour	Exa_TAT_Live_2_3_4_Network_Routing_Ctrl_hour
	Network Connections by Server Group (per month)	NetServers-Host-Month	Exa_TAT_Live_2_3_4_Network_Routing_Ctrl_month

Table 150 List of Reporting Tables

Dashboards	Reports	Data Dictionary	Main Tables
2.4.3 - Network Clients	TOP Clients (per day)	NetClients-TOP-Day	Exa_TAT_Live_NetworkClient_day
	TOP Clients (per hour)	NetClients-TOP-Hour	Exa_TAT_Live_NetworkClient_hour
	TOP Clients (per month)	NetClients-TOP-Month	Exa_TAT_Live_NetworkClient_month
	Network Connections (per day)	NetClients-Act-Day	Exa_TAT_Live_NetworkClient_day
	Network Connections (per hour)	NetClients-Act-Hour	Exa_TAT_Live_NetworkClient_hour
	Network Connections (per month)	NetClients-Act-Month	Exa_TAT_Live_NetworkClient_month
	Network Connections by Client Group (per day)	NetClients-Host-Day	Exa_TAT_Live_NetworkClient_day
	Network Connections by Client Group (per hour)	NetClients-Host-Hour	Exa_TAT_Live_NetworkClient_hour
	Network Connections by Client Group (per month)	NetClients-Host-Month	Exa_TAT_Live_NetworkClient_month
2.5 - Incident and Alert Mgt.			
2.5.1 - Alerts & Victims	TOP Victims (per hour)	AlertsVict-TOP-Hour	Exa_TAT_Batch_Alert_Victim_hour
	TOP Victims (per day)	AlertsVict-TOP-Day	Exa_TAT_Batch_Alert_Victim_day
	TOP Victims (per month)	AlertsVict-TOP-Month	Exa_TAT_Batch_Alert_Victim_month
	Alerts by Severity (per hour)	AlertsVict-Act-Hour	Exa_TAT_Batch_Alert_Victim_hour
	Alerts by Severity (per day)	AlertsVict-Act-Day	Exa_TAT_Batch_Alert_Victim_day
	Alerts by Severity (per month)	AlertsVict-Act-Month	Exa_TAT_Batch_Alert_Victim_month
	Alerts by Victim Group (per hour)	AlertsVict-Host-Hour	Exa_TAT_Batch_Alert_Victim_hour
	Alerts by Victim Group (per day)	AlertsVict-Host-Day	Exa_TAT_Batch_Alert_Victim_day
	Alerts by Victim Group (per month)	AlertsVict-Host-Month	Exa_TAT_Batch_Alert_Victim_month

Table 150 List of Reporting Tables

Dashboards	Reports	Data Dictionary	Main Tables
2.5.2 - Alerts & Attackers	TOP Attackers (per hour)	AlertsAttack-TOP-Hour	Exa_TAT_Batch_Alert_Attacker_hour
	TOP Attackers (per day)	AlertsAttack-TOP-Day	Exa_TAT_Batch_Alert_Attacker_day
	TOP Attackers (per month)	AlertsAttack-TOP-Month	Exa_TAT_Batch_Alert_Attacker_month
	Alerts by Severity (per hour)	AlertsAttack-Act-Hour	Exa_TAT_Batch_Alert_Attackerhour
	Alerts by Severity (per day)	AlertsAttack-Act-Day	Exa_TAT_Batch_Alert_Attacker_day
	Alerts by Severity (per month)	AlertsAttack-Act-Month	Exa_TAT_Batch_Alert_Attacker_month
	Alerts by Attacker Group (per hour)	AlertsAttack-Host-Hour	Exa_TAT_Batch_Alert_Attacker_hour
	Alerts by Attacker Group (per day)	AlertsAttack-Host-Day	Exa_TAT_Batch_Alert_Attacker_day
	Alerts by Attacker Group (per month)	AlertsAttack-Host-Month	Exa_TAT_Batch_Alert_Attacker_month
2.5.3 - Alert Acknowledgment	TOP Analyst (per hour)	IncidentMgt-Event-Hour	Exa_TAT_Batch_3_3_2_Incident_Management_hour
	TOP Analyst (per day)	IncidentMgt-Event-Day	Exa_TAT_Batch_3_3_2_Incident_Management_day
	TOP Analyst (per month)	IncidentMgt-Event-Month	Exa_TAT_Batch_3_3_2_Incident_Management_month
	Alert's Acknowledgment Status (per hour)	IncidentMgt-Act-Hour	Exa_TAT_Batch_3_3_2_Incident_Management_hour
	Alert's Acknowledgment Status (per day)	IncidentMgt-Act-Day	Exa_TAT_Batch_3_3_2_Incident_Management_day
	Alert's Acknowledgment Status (per month)	IncidentMgt-Act-Month	Exa_TAT_Batch_3_3_2_Incident_Management_month
	Alert's Acknowledgement Status by Severity (per hour)	IncidentMgt-Host-Hour	Exa_TAT_Batch_3_3_2_Incident_Management_hour
	Alert's Acknowledgement Status by Severity (per day)	IncidentMgt-Host-Day	Exa_TAT_Batch_3_3_2_Incident_Management_day
	Alert's Acknowledgement Status by Severity (per month)	IncidentMgt-Host-Month	Exa_TAT_Batch_3_3_2_Incident_Management_month
2.6 - Log and Event Management			

Table 150 List of Reporting Tables

Dashboards	Reports	Data Dictionary	Main Tables
2.6.1 - Collected Elementary Events	TOP Log Sources (per day)	EEbySev&LS-TOP-Day	Exa_TAT_Live_EEbyLSandSev_day
	TOP Log Sources (per hour)	EEbySev&LS-TOP-Hour	Exa_TAT_Live_EEbyLSandSev_hour
	TOP Log Sources (per month)	EEbySev&LS-TOP-Month	Exa_TAT_Live_EEbyLSandSev_month
	Elementary Events Severity (per hour)	EEbySev-Hour	Exa_TAT_Live_EEbyLSandSev_hour
	Elementary Events Severity (per day)	EEbySev-Day	Exa_TAT_Live_EEbyLSandSev_day
	Elementary Events Severity (per month)	EEbySev-Month	Exa_TAT_Live_EEbyLSandSev_month
	Elementary Event Severity by Log Source Type (per hour)	EEbySev&LS-Hour	Exa_TAT_Live_EEbyLSandSev_hour
	Elementary Event Severity by Log Source Type (per month)	EEbySev&LS-Month	Exa_TAT_Live_EEbyLSandSev_month
	Elementary Event Severity by Log Source Type (per day)	EEbySev&LS-Day	Exa_TAT_Live_EEbyLSandSev_day
2.6.2 - Events Rates (EPS)	TOP Log Source Average EPS (per hour)	EPSAvgbyLS-TOP-Hour	Exa_TAT_Live_EC_msg_sent_hour
	TOP Log Source Average EPS (per day)	EPSAvgbyLS-TOP-Day	Exa_TAT_Live_EC_msg_sent_day
	TOP Log Source Average EPS (per month)	EPSAvgbyLS-TOP-Month	Exa_TAT_Live_EC_msg_sent_month
	Events Per Second (per hour)	EPS-Hour	Exa_TAT_Live_EC_msg_sent_hour
	Events Per Second (per day)	EPS-Day	Exa_TAT_Live_EC_msg_sent_day
	Events Per Second (per month)	EPS-Month	Exa_TAT_Live_EC_msg_sent_month
	Events Per Second by Log Source Type (per hour)	EPSbyProductType-Hour	Exa_TAT_Live_EC_msg_sent_hour
	Events Per Second by Log Source Type (per day)	EPSbyProductType-Day	Exa_TAT_Live_EC_msg_sent_day
	Events Per Second by Log Source Type (per month)	EPSbyProductType-Month	Exa_TAT_Live_EC_msg_sent_month

Table 150 List of Reporting Tables

Dashboards	Reports	Data Dictionary	Main Tables
2.6.3 - Elementary Event Taxonomy	TOP Event Taxonomy (per hour)	EEbyET&LS-TOP-Hour	Exa_TAT_Live_EEbyLSandTaxo_hour
	TOP Event Taxonomy (per day)	EEbyET&LS-TOP-Day	Exa_TAT_Live_EEbyLSandTaxo_day
	TOP Event Taxonomy (per month)	EEbyET&LS-TOP-Month	Exa_TAT_Live_EEbyLSandTaxo_month
	Elementary Events by Log Source Type (per hour)	EEbyET&ProductType-Hour	Exa_TAT_Live_EEbyLSandTaxo_hour
	Elementary Events by Log Source Type (per day)	EEbyET&ProductType-Day	Exa_TAT_Live_EEbyLSandTaxo_day
	Elementary Events by Log Source Type (per month)	EEbyET&ProductType-Month	Exa_TAT_Live_EEbyLSandTaxo_month
	Elementary Events "Event Type" (per hour)	EEbyEventType-Hour	Exa_TAT_Live_EEbyLSandTaxo_hour
	Elementary Events "Event Type" (per day)	EEbyEventType-Day	Exa_TAT_Live_EEbyLSandTaxo_day
	Elementary Events "Event Type" (per month)	EEbyEventType-Month	Exa_TAT_Live_EEbyLSandTaxo_month
2.6.4 - Log Protection	TOP Log Protection Information (per month)	LogProt-Month	Exa_TAT_Live_3_4_2_month
	Log Protection Information Activity (per day)	LogProt-Day	Exa_TAT_Live_3_4_2_day
	Log Protection Information Activity (per hour)	LogProt-Hour	Exa_TAT_Live_3_4_2_hour
	Log Protection Information Activity (per month)	LogProt-Month	Exa_TAT_Live_3_4_2_month
	Log Protection Information by Host Group (per day)	LogProt-Day	Exa_TAT_Live_3_4_2_day
	Log Protection Information by Host Group (per hour)	LogProt-Hour	Exa_TAT_Live_3_4_2_hour
	Log Protection Information by Host Group (per month)	LogProt-Month	Exa_TAT_Live_3_4_2_month
	Log Protection Information Events	LogProt-Table	Exa_Alert
3 - Assets Security			
3.1 - Asset Identification			
3.1 - Asset Inventory and Ownership			
3.2 - Change Management			

Table 150 List of Reporting Tables

Dashboards	Reports	Data Dictionary	Main Tables
3.2 - Change Management	TOP Change Management (per month)	ChangeMgt-Month	Exa_TAT_Batch_1_2_Change_Management_month
	Change Management Activity (per day)	ChangeMgt-Day	Exa_TAT_Batch_1_2_Change_Management_day
	Change Management Activity (per hour)	ChangeMgt-Hour	Exa_TAT_Batch_1_2_Change_Management_hour
	Change Management Activity (per month)	ChangeMgt-Month	Exa_TAT_Batch_1_2_Change_Management_month
	Change Management by Asset (per day)	ChangeMgt-Day	Exa_TAT_Batch_1_2_Change_Management_day
	Change Management by Asset (per hour)	ChangeMgt-Hour	Exa_TAT_Batch_1_2_Change_Management_hour
	Change Management by Asset (per month)	ChangeMgt-Month	Exa_TAT_Batch_1_2_Change_Management_month
	Change Management Event	ConfMgt-Table	Exa_Alert
3.3 - Backup Management			
3.3.1 - Backup Management	TOP Backup Management (per month)	BckMgt-Month	Exa_TAT_Live_1_3_Backup_Management_month
	Backup Management Activity (per day)	BckMgt-Day	Exa_TAT_Live_1_3_Backup_Management_day
	Backup Management Activity (per hour)	BckMgt-Hour	Exa_TAT_Live_1_3_Backup_Management_hour
	Backup Management Activity (per month)	BckMgt-Month	Exa_TAT_Live_1_3_Backup_Management_month
	Backup Management by Asset (per day)	BckMgt-Day	Exa_TAT_Live_1_3_Backup_Management_day
	Backup Management by Asset (per hour)	BckMgt-Hour	Exa_TAT_Live_1_3_Backup_Management_hour
	Backup Management by Asset (per month)	BckMgt-Month	Exa_TAT_Live_1_3_Backup_Management_month
	Backup Management Events	BckMgt-Table	Exa_Alert
3.4 - Capacity Management			

Table 150 List of Reporting Tables

Dashboards	Reports	Data Dictionary	Main Tables
3.4.1 - Capacity Management	TOP Capacity Management (per month)	BckMgt-Month	Exa_TAT_Live_1_3_Backup_Management_month
	Capacity Management Activity (per day)	CapMgt-Day	Exa_TAT_Live_1_4_Capacity_Management_day
	Capacity Management Activity (per hour)	CapMgt-Hour	Exa_TAT_Live_1_4_Capacity_Management_hour
	Capacity Management Activity (per month)	BckMgt-Month	Exa_TAT_Live_1_3_Backup_Management_month
	Capacity Management by Asset (per day)	CapMgt-Day	Exa_TAT_Live_1_4_Capacity_Management_day
	Capacity Management by Asset (per hour)	CapMgt-Hour	Exa_TAT_Live_1_4_Capacity_Management_hour
	Capacity Management by Asset (per month)	BckMgt-Month	Exa_TAT_Live_1_3_Backup_Management_month
	Capacity Management Events	CapMgt-Table	Exa_Alert
3.5 - Vulnerability Management			
3.5.1 - Vulnerability Management	TOP Vulnerability Management (per month)	VulMgt-Month	Exa_TAT_Live_1_5_Vulnerability_Management_month
	Vulnerability Management Activity (per day)	VulMgt-Day	Exa_TAT_Live_1_5_Vulnerability_Management_day
	Vulnerability Management Activity (per hour)	VulnMgt-Hour	Exa_TAT_Live_1_5_Vulnerability_Management_hour
	Vulnerability Management Activity (per month)	VulMgt-Month	Exa_TAT_Live_1_5_Vulnerability_Management_month
	Vulnerability Management by Asset (per day)	VulMgt-Day	Exa_TAT_Live_1_5_Vulnerability_Management_day
	Vulnerability Management by Asset (per hour)	VulnMgt-Hour	Exa_TAT_Live_1_5_Vulnerability_Management_hour
	Vulnerability Management by Asset (per month)	VulMgt-Month	Exa_TAT_Live_1_5_Vulnerability_Management_month
	Vulnerability Management Events	VulnMgt-Table	Exa_Alert
3.6 - Asset Availability			

Table 150 List of Reporting Tables

Dashboards	Reports	Data Dictionary	Main Tables
3.6.1 - Asset Availability	TOP Business Service Availability (per month)	BusSrvAv-Month	Exa_TAT_Live_1_6_month
	Business Service Availability (per day)	BusSrvAv-Day	Exa_TAT_Live_1_6_day
	Business Service Availability (per hour)	BusSrvAv-Hour	Exa_TAT_Live_1_6_hour
	Business Service Availability (per month)	BusSrvAv-Month	Exa_TAT_Live_1_6_month
	Business Service Availability by Asset (per day)	BusSrvAv-Day	Exa_TAT_Live_1_6_day
	Business Service Availability by Asset (per hour)	BusSrvAv-Hour	Exa_TAT_Live_1_6_hour
	Business Service Availability by Asset (per month)	BusSrvAv-Month	Exa_TAT_Live_1_6_month
	Business Service Availability Events	BusSrvAv-Table	Exa_Alert
4 - Executive Report			
4.1 - Monthly Executive Report			
Uses all the month and day reports, data dictionary and tables of the previous dashboards.			
5 - Regulatory Compliance			
5.1 - Standards Mapping			
Standards Mapping and Coverage			
5.2 - FSA			
Monthly FSA Compliance Report			
5.3 - PCI-DSS			
Monthly PCI-DSS Compliance Report			
5.4 - Sarbanes-Oxley			
Monthly SOX Compliance Report			
6 - SANS Top 5			
6.1 - Attempts to gain access through existing accounts			

Table 150 List of Reporting Tables

Dashboards	Reports	Data Dictionary	Main Tables
6.1.1 - SANS - System Access	System Access TOP (per hour)	SysAccess-Hour	Exa_TAT_Live_2_2_1_System_Access_hour
	System Access TOP (per day)	SysAccess-Dayr	Exa_TAT_Live_2_2_1_System_Access_day
	System Access TOP (permonth)	SysAccess-Month	Exa_TAT_Live_2_2_1_System_Access_month
	System Access Activity (per day)	SysAccess-Day	Exa_TAT_Live_2_2_1_System_Access_day
	System Access Activity (per hour)	SysAccess-Hour	Exa_TAT_Live_2_2_1_System_Access_hour
	System Access Activity (per month)	SysAccess-Month	Exa_TAT_Live_2_2_1_System_Access_month
	System Access by Host Group (per day)	SysAccess-Day	Exa_TAT_Live_2_2_1_System_Access_day
	System Access by Host Group (per hour)	SysAccess-Hour	Exa_TAT_Live_2_2_1_System_Access_hour
	System Access by Host Group (per month)	SysAccess-Month	Exa_TAT_Live_2_2_1_System_Access_month
	System Access Events	SysAccess-Table	Exa_Alert
6.2 - Failed file or resource access attempts			
6.2.1 - SANS - Data Access	TOP Data Access (per month)	DataAccess-Month	Exa_TAT_Live_2_2_2_Data_Access_month
	Data Access Activity (per day)	DataAccess-Day	Exa_TAT_Live_2_2_2_Data_Access_day
	Data Access Activity (per hour)	DataAccess-Hour	Exa_TAT_Live_2_2_2_Data_Access_hour
	Data Access Activity (per month)	DataAccess-Month	Exa_TAT_Live_2_2_2_Data_Access_month
	Data Access by Host Group (per day)	DataAccess-Day	Exa_TAT_Live_2_2_2_Data_Access_day
	Data Access by Host Group (per hour)	DataAccess-Hour	Exa_TAT_Live_2_2_2_Data_Access_hour
	Data Access by Host Group (per month)	DataAccess-Month	Exa_TAT_Live_2_2_2_Data_Access_month
	Data Access Events	DataAccess-Table	Exa_Alert
6.3 - Unauthorized changes to users, groups and services			

Table 150 List of Reporting Tables

Dashboards	Reports	Data Dictionary	Main Tables
6.3.1 - SANS - Account Registration	TOP Account Registration (per month)	AccountReg-Month	Exa_TAT_Live_2_1_1_Account_Registration_month
	TOP Account Registration (per day)	AccountReg-Day	Exa_TAT_Live_2_1_1_Account_Registration_day
	Account Registration Activity (per day)	AccountReg-Day	Exa_TAT_Live_2_1_1_Account_Registration_day
	Account Registration Activity (per hour)	AccountReg-Hour	Exa_TAT_Live_2_1_1_Account_Registration_hour
	Account Registration Activity (per month)	AccountReg-Month	Exa_TAT_Live_2_1_1_Account_Registration_month
	Account Registration by Host Group (per day)	AccountReg-Day	Exa_TAT_Live_2_1_1_Account_Registration_day
	Account Registration by Host Group (per hour)	AccountReg-Hour	Exa_TAT_Live_2_1_1_Account_Registration_hour
	Account Registration by Host Group (per month)	AccountReg-Month	Exa_TAT_Live_2_1_1_Account_Registration_month
	Account Registration Events	AccountReg-Table	Exa_Alert
6.3.2 - SANS - Privilege Management	TOP Privilege Management (per day)	PrivMgt-day	Exa_TAT_Live_2_1_2_Privilege_Management_day
	TOP Privilege Management (per month)	PrivMgt-Month	Exa_TAT_Live_2_1_2_Privilege_Management_month
	Privilege Management Activity (per day)	PrivMgt-day	Exa_TAT_Live_2_1_2_Privilege_Management_day
	Privilege Management Activity (per hour)	PrivMgt-Hour	Exa_TAT_Live_2_1_2_Privilege_Management_hour
	Privilege Management Activity (per month)	PrivMgt-Month	Exa_TAT_Live_2_1_2_Privilege_Management_month
	Privilege Management by Host Group (per day)	PrivMgt-day	Exa_TAT_Live_2_1_2_Privilege_Management_day
	Privilege Management by Host Group (per hour)	PrivMgt-Hour	Exa_TAT_Live_2_1_2_Privilege_Management_hour
	Privilege Management by Host Group (per month)	PrivMgt-Month	Exa_TAT_Live_2_1_2_Privilege_Management_month
	Privilege Management Events	PrivMgt-Table	Exa_Alert
6.4 - Systems most vulnerable to attacks			

Table 150 List of Reporting Tables

Dashboards	Reports	Data Dictionary	Main Tables
6.4.1 - SANS - Vulnerability Management	TOP Vulnerability Management (per month)	VulMgt-Month	Exa_TAT_Live_1_5_Vulnerability_Management_month
	Vulnerability Management Activity (per day)	VulMgt-Day	Exa_TAT_Live_1_5_Vulnerability_Management_day
	Vulnerability Management Activity (per hour)	VulnMgt-Hour	Exa_TAT_Live_1_5_Vulnerability_Management_hour
	Vulnerability Management Activity (per month)	VulMgt-Month	Exa_TAT_Live_1_5_Vulnerability_Management_month
	Vulnerability Management by Asset (per day)	VulMgt-Day	Exa_TAT_Live_1_5_Vulnerability_Management_day
	Vulnerability Management by Asset (per hour)	VulnMgt-Hour	Exa_TAT_Live_1_5_Vulnerability_Management_hour
	Vulnerability Management by Asset (per month)	VulMgt-Month	Exa_TAT_Live_1_5_Vulnerability_Management_month
	Vulnerability Management Events	VulnMgt-Table	Exa_Alert
6.5 - Suspicious or unauthorized network traffic patterns			
6.5.1 - SANS - Network Servers	TOP Servers (per hour)	NetServers-TOP-Hour	Exa_TAT_Live_2_3_4_Network_Routing_Ctrl_hour
	TOP Servers (per month)	NetServers-TOP-Month	Exa_TAT_Live_2_3_4_Network_Routing_Ctrl_month
	TOP Servers (per day)	NetServers-TOP-Day	Exa_TAT_Live_2_3_4_Network_Routing_Ctrl_day
	Network Connections (per hour)	NetServers-Act-Hour	Exa_TAT_Live_2_3_4_Network_Routing_Ctrl_hour
	Network Connections (per day)	NetServers-Act-Day	Exa_TAT_Live_2_3_4_Network_Routing_Ctrl_day
	Network Connections (per month)	NetServers-Act-Month	Exa_TAT_Live_2_3_4_Network_Routing_Ctrl_month
	Network Connections by Server Group (per hour)	NetServers-Host-Hour	Exa_TAT_Live_2_3_4_Network_Routing_Ctrl_hour
	Network Connections by Server Group (per day)	NetServers-Host-Day	Exa_TAT_Live_2_3_4_Network_Routing_Ctrl_day
	Network Connections by Server Group (per month)	NetServers-Host-Month	Exa_TAT_Live_2_3_4_Network_Routing_Ctrl_month

Table 150 List of Reporting Tables

Dashboards	Reports	Data Dictionary	Main Tables
6.5.2 - SANS - Network Clients	TOP Clients (per hour)	NetClients-TOP-Hour	Exa_TAT_Live_NetworkClient_hour
	TOP Clients (per day)	NetClients-TOP-Day	Exa_TAT_Live_NetworkClient_day
	TOP Clients (per month)	NetClients-TOP-Month	Exa_TAT_Live_NetworkClient_month
	Network Connections (per hour)	NetClients-Act-Hour	Exa_TAT_Live_NetworkClient_hour
	Network Connections (per day)	NetClients-Act-Day	Exa_TAT_Live_NetworkClient_day
	Network Connections (per month)	NetClients-Act-Month	Exa_TAT_Live_NetworkClientmonth
	Network Connections by Client Group (per hour)	NetClients-Host-Hour	Exa_TAT_Live_NetworkClient_hour
	Network Connections by Client Group (per day)	NetClients-Host-Day	Exa_TAT_Live_NetworkClient_day
	Network Connections by Client Group (per month)	NetClients-Host-Month	Exa_TAT_Live_NetworkClientmonth

List of Correlation/Aggregation/Live Reporting Grouping Fields

Table 151 Grouping Fields

Type	Name
Asset Database	
	Log Source Asset Name
	Log Source Host Group Name
	Log Source OU Name
	Log Source Site Name
	Source Asset Name
	Source Host Group Name
	Source Site Name
	Target Asset Name
	Target Host Group Name
	Target Site Name
Event	
	Additional Data
	Detect Time
	Duration
	Event Name
	Event Severity
	Impact Completion
	Impact Description
	Impact Type
	Reference Name

Table 151 Grouping Fields

	Reference Origin
	Reference URL
	Return Code
	Size
Log Sources	
	Log Source Id
	LogSource Name
TIBCO LogLogic® Taxonomy	
	(all fields)
	Access Layer
	Action
	Action Detail
	Event Type
	Result
	Target
	Target Detail
Source	
	Source Interface
	Source Spoofed
	Source Node Address
	Source Node Address (eMail)
	Source Node Address (IPv4)
	Source Node Address Category
	Source Node Address Country Code
	Source Node Category
	Source Node Location
	Source Node Name
	Source Node Name Or Address
	Source Process
	Source Process Name
	Source Process Path
	Source Process PID
	Source Service
	Source Service Name
	Source Service Name Or Port
	Source Service Port
	Source Service Protocol
	Source Tool Command
	Source Tool Name
	Source User Category
	Source User Name
	Source User Name Or Number
	Source User Number
	Source User Type

Table 151 Grouping Fields

	Source WebService Arg
	Source WebService CGI
	Source WebService HTTP Method
	Source WebService Url
Target	
	Target Assessment
	Target Decoy
	Target File
	Target File Name
	Target File Path and Name
	Target Interface
	Target Node Address
	Target Node Address (eMail)
	Target Node Address (IPv4)
	Target Node Address Category
	Target Node Address Country Code
	Target Node Category
	Target Node Location
	Target Node Name
	Target Node Name Or Address
	Target Process
	Target Process Name
	Target Process Path
	Target Process PID
	Target Service
	Target Service Name
	Target Service Name Or Port
	Target Service Port
	Target Service Protocol
	Target Tool Command
	Target Tool Name
	Target User Category
	Target User Name
	Target User Name Or Number
	Target User Number
	Target User Type
	Target WebService Arg
	Target WebService CGI
	Target WebService HTTP Method
	Target WebService Url

SEM Glossary

Table 152 Glossary

Term	Definition
Acknowledgement	The task of validating an alert displayed on the monitoring screen.
Administrator (User Rights)	See User Rights.
ADA	Archiving Disk Array.
Aggregation Engine	The process of using a pre-defined set of rules to group very similar events, reducing the total number that require further processing. For example: Several elementary events that have the same meaning (same TIBCO LogLogic® Taxonomy) and the same target address would be aggregated in one event.
Alert	An alert is composed of an event or a set of events that has/have an impact on confidentiality, integrity or availability of the information system. An alert is generated by the correlation engine according to predefined rules and scenarios.
Analyst (User Rights)	See User Rights.
Appliance	An equipment unit dedicated to be solely used as a software component of the SEM solution.
Backup	The TIBCO LogLogic® SMP Backup tool enables you to schedule automatic backups of the instance including database and configuration information held on the TIBCO LogLogic® SMP server. It is version-dependent. A backup file contains all of the backup configuration details - so that in the event of hardware or software application failure, this valuable information could be restored and would not need to be manually recreated.
Batch Reporting	Rules that allow the enrichment of the reporting database via alerts and aggregated events batch treatments.
Business Asset	Company items whose threats and vulnerabilities must be controlled, identified and calculated to evaluate risks.
Collection Policy	A collection policy allows you to determine which events will be selected to be forwarded to the SMP. Filtering is carried out by the Log Collector, to avoid wasting bandwidth from the Log Collector to the TIBCO LogLogic® SMP.
Configuration Profile	See Security Profile.
Confset	Definition of a set of converters, filters and parameters to collect the log entries of an equipment.
Converter	Set of rules for converting a log entry into an event.
Conversion Ruleset	File containing conversion rules.
Correlation Engine	The process of using a pre-defined set of rules and scenarios to combine one or more events into an alert.
Correlation Scenario	Scenarios are used to describe a situation matching the occurrence of a group of rules. Scenarios are used to describe complex situations requiring action which cannot be handled by the definition of a simple rule. For example, Rule A is used to detect when a process has stopped, Rule B is used to detect when a process has started. A scenario is created to detect that a process has been restarted (Rule A plus Rule B), that is, when both the stopped and the started rules match.
Criticality	Failure probabilities and severities referring to a certain asset, categorized as low, medium, or high.

Table 152 Glossary

Term	Definition
Event	An event is a standardized data object (IDMEF and TIBCO LogLogic® Taxonomy) representation of a log entry that has been generated by a log source. The events collected by the SMP is also called ‘elementary events’. On the SMP, these events are aggregated by the aggregation engine. Events generated by this engine is called ‘aggregated event’.
Heartbeat	A message sent by the Log Collector to the SMP to indicate the Log Collector is active.
IDMEF	Intrusion Detection Message Exchange Format. The IDMEF is a special data format used for sharing information of interest to intrusion detection and response systems, and to the management systems which may need to interact with them. Standard RFC 4765.
IODEF	Incident Object Description and Exchange Format.
Incident	Container of alerts of IODEF format, allowing to ensure the management of these alerts. It specifies their cause and the actions that must be triggered.
Instance	An instance consists of: ▪ the configuration of logs and devices to be monitored ▪ the collected events ▪ the rules and scenarios to apply to the collected events ▪ a console server (the Web Console)
Live Explorer screen	The Live Explorer screen allows you to monitor everything that happens on the SMP server.
Live Reporting	Rules used by the Totaling Engine to enrich the reporting database in real time.
Log Collector	The software Log Collector installed on a machine to collect information, format it, and forward it to the SMP.
Log Entry	A log entry is an individual message recording of an occurrence in an application, operating system or log source. For example, this could be a line in a text file describing a failed connection attempt, or a database record outlining a successful user log-in.
TIBCO LogLogic® Taxonomy	A TIBCO LogLogic® defined Taxonomy enabling to normalise events. A TIBCO LogLogic® Taxonomy is composed of seven fields that are themselves composed of three main groups: ▪ Result ▪ Objective, Event Type, Action, Action Detail ▪ Target, Target Detail
Log Source	Product that generates log entries collected by a Log Collector.
SEM	Security Event Manager. The SEM consists of a system where Log Collectors collect event data from application and device logs, then the data is treated and transmitted to the Security Management Platform (SMP). This allows the SMP to analyze and correlate a multitude of events, providing real-time monitoring. In addition, a comprehensive security record is created.
ODA	Online Disk Array.
Organization Unit (OU)	An Organization Unit (OU) is a collection of host groups. Typically this is based on overseeing responsibility, e.g., all host groups that the UK IT department are responsible for would be assigned to the "UK IT" OU. The OU is used in reports, such as a report listing the number of alerts (by priority) for each OU.
Raw Log	A record of individual activities of one or more equipment units, applications, operating systems or devices. The raw log provides an audit trail that can be used to diagnose problems or provide legal proof of said activity. It is a text-format representation of a log entry. A raw log is created by the Log Collector. A Raw Log Entry is an individual entry recorded in the raw log referring to a single device event.

Table 152 Glossary

Term	**Definition**
Rules	Engines need various configuring rules to manage events and then build up complex scenarios to deal with events and alerts. There are different types of rules: ▪ Collection rule ▪ Aggregation rule ▪ Correlation rule ▪ Live or Batch Reporting rules
Security Dashboard	Screen displaying a set of reports.
Security Profile	A security configuration profile is a group of rules and scenarios along with a Service Level Agreement set.
Site	Sites are used to group hosts in reports (e.g., Lyon, Paris, or London, Cambridge), and to specify who is to be contacted when alerts have notification actions, such as emails. Sites are therefore used to define the sphere of responsibility of one or more contacts. For example if London_Analysts are responsible for all the hosts in London, create a site called "London" and allocate the relevant hosts to the site "London".
Site Group	A Site Group contains several sites. (See Site).
SLA	Service Level Agreement. Indicator specifying the maximum delay (in minutes) for an alert to be acknowledged. It takes into account the severity of the alert, the criticality on the impacted machine, the current security level and the work hours of the security analyst.
SMP	Security Management Platform. The appliance which runs the SEM software. The SMP aggregates, enriches, and correlates received event data.
Super-Administrator (User Rights)	See User Rights.
Supported Product	A product supported by TIBCO LogLogic® SEM (Check Point Firewall-1, Windows 2003, ...).
Top Level Alert	Alert displayed on the main alert monitoring screen.
Totaling Engine	Engine which counts collected events according to Live reporting rules. It allows the enrichment of the Reporting Database used for security dashboards generation.
User Rights	There are four user rights available in the Security Event Manager: ▪ Viewer: Viewers have read-only access to the GUI and cannot acknowledge alerts. ▪ Analyst: Analysts have all the rights of viewers, plus they can acknowledge alerts and manage incidents. ▪ Administrator: Administrators have all the rights of analysts, plus they can make changes to the Security Event Manager Solutions configuration and configure the TIBCO LogLogic® policies (collection...). ▪ Super-Administrator: Super-Administrators have all the rights of administrators, plus they can manage all user accounts.
Viewer (User Rights)	See User Rights.
Web Console	The web-based graphical user interface (GUI) used for the administration of the SMP.

Index