TIBCO LogLogic®

Security Event Manager (SEM)

User Guide

Software Release: 3.6.0

March 2013

Two-Second Advantage®

Important Information

SOME TIBCO SOFTWARE EMBEDS OR BUNDLES OTHER TIBCO SOFTWARE. USE OF SUCH EMBEDDED OR BUNDLED TIBCO SOFTWARE IS SOLELY TO ENABLE THE FUNCTIONALITY (OR PROVIDE LIMITED ADD-ON FUNCTIONALITY) OF THE LICENSED TIBCO SOFTWARE. THE EMBEDDED OR BUNDLED SOFTWARE IS NOT LICENSED TO BE USED OR ACCESSED BY ANY OTHER TIBCO SOFTWARE OR FOR ANY OTHER PURPOSE.

USE OF TIBCO SOFTWARE AND THIS DOCUMENT IS SUBJECT TO THE TERMS AND CONDITIONS OF A LICENSE AGREEMENT FOUND IN EITHER A SEPARATELY EXECUTED SOFTWARE LICENSE AGREEMENT, OR, IF THERE IS NO SUCH SEPARATE AGREEMENT, THE CLICKWRAP END USER LICENSE AGREEMENT WHICH IS DISPLAYED DURING DOWNLOAD OR INSTALLATION OF THE SOFTWARE (AND WHICH IS DUPLICATED IN THE LICENSE FILE) OR IF THERE IS NO SUCH SOFTWARE LICENSE AGREEMENT OR CLICKWRAP END USER LICENSE AGREEMENT, THE LICENSE(S) LOCATED IN THE “LICENSE” FILE(S) OF THE SOFTWARE. USE OF THIS DOCUMENT IS SUBJECT TO THOSE TERMS AND CONDITIONS, AND YOUR USE HEREOF SHALL CONSTITUTE ACCEPTANCE OF AND AN AGREEMENT TO BE BOUND BY THE SAME.

THIS SOFTWARE MAY BE AVAILABLE ON MULTIPLE OPERATING SYSTEMS. HOWEVER, NOT ALL OPERATING SYSTEM PLATFORMS FOR A SPECIFIC SOFTWARE VERSION ARE RELEASED AT THE SAME TIME. PLEASE SEE THE README.TXT FILE FOR THE AVAILABILITY OF THIS SOFTWARE VERSION ON A SPECIFIC OPERATING SYSTEM PLATFORM.

THIS DOCUMENT IS PROVIDED “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. THIS DOCUMENT COULD INCLUDE TECHNICAL INACCURACIES OR TYPOGRAPHICAL ERRORS. CHANGES ARE PERIODICALLY ADDED TO THE INFORMATION HEREIN; THESE CHANGES WILL BE INCORPORATED IN NEW EDITIONS OF THIS DOCUMENT. TIBCO SOFTWARE INC. MAY MAKE IMPROVEMENTS AND/OR CHANGES IN THE PRODUCT(S) AND/OR THE PROGRAM(S) DESCRIBED IN THIS DOCUMENT AT ANY TIME.

THE CONTENTS OF THIS DOCUMENT MAY BE MODIFIED AND/OR QUALIFIED, DIRECTLY OR INDIRECTLY, BY OTHER DOCUMENTATION WHICH ACCOMPANIES THIS SOFTWARE, INCLUDING BUT NOT LIMITED TO ANY RELEASE NOTES AND "READ ME" FILES.

Contents

Chapter 4 - Preparing the Asset DataBase

Chapter 5 - Managing Logs and Events

Chapter 6 - Monitoring...

Chapter 7 - Reporting

Chapter 8 - Configuring...

List of Figures

List of Tables

Preface

The Web Console is the graphical user interface to the Security Event Manager. It provides a real-time view of the current security alerts, color-coded to reflect severity and priority. Each alert can be explored through an intuitive drill-down to display its component events and all the collected and enriched information for these events, including the raw log entries.

This User Guide describes how to configure the main functions of the Web Console application.

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 Solution 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 on both Windows and Linux/ Unix O.S.
Reference Guide	This guide gives a description of the various modules provided in the Web Console application.
SMP Installation Guide	This guide explains how to install and configure the Security Management Platform.
SOC Implementation Guide	This guide explains how to implement a SOC project.

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:

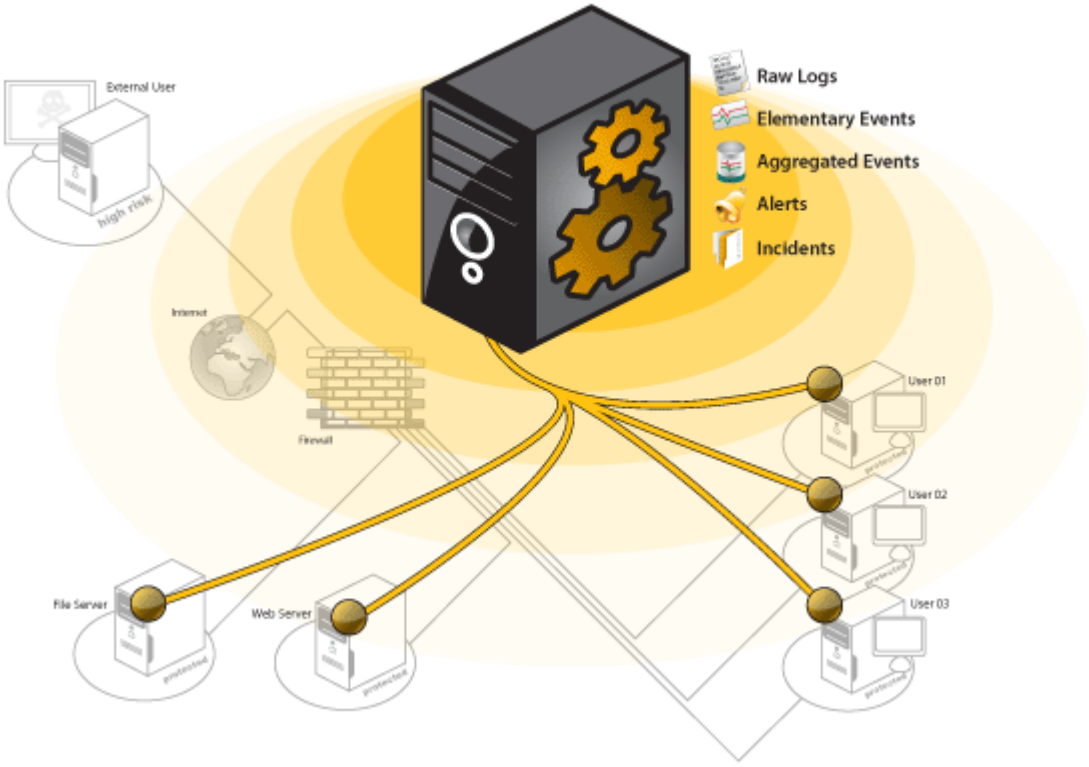
`LogLogic_home_directory``\upgrade\`

- Straight brackets signal options in command line syntax.

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

Chapter 1 - Overall Product Presentation

Security Event Manager (SEM) offers a data security monitoring system for organizations challenged by the complexity of modern IT infrastructures, and which face constant security threats, old and new.



As corporations' IT systems grow and become enormously complex, the challenges for collecting and analyzing security events multiply on various levels. Overseeing a gigantic number of events generated by critical applications and security systems soon becomes impractical without assistance. Event data for systems and applications are often stored in different locations and in a variety of formats. Event transfer protocols are often connection-less, unsecured, and prone to data loss.

The TIBCO LogLogic® SEM is designed to solve these security data collection issues by filtering out expected and authorized events, standardizing the collected data, and providing tools for security monitoring, analysis, response, and forensics. In the TIBCO LogLogic® SEM, Log Collectors collect event data from application and logs from supported products, treat the data and transmit it to the Security Management Platform (SMP). This allows the SMP to analyze and correlate a multitude of events, providing comprehensive, real-time end-to-end session tracking and monitoring. In addition, a comprehensive security record is created.

Among its key functions, the SEM:

- Provides an aggregated, easy-to-understand analysis of large volumes of data regarding security-related events.
- Aids administrators in quickly detecting the most urgent and top-priority threats or problems regarding the security of their system.

- Supplies administrators with a comprehensive, auditable approach to security event analysis, delivering management reports to meet the needs of stakeholders, security analysts, and regulatory bodies.

Understanding the SEM Model

TIBCO LogLogic®'s Security Event Manager is based on a three-tier model, comprising Log Collectors, Platform, and Console. This model can be extended with additional components to provide further resilience, distributed monitoring, optimal bandwidth usage, and layered security.

Log Collectors

The Log Collectors collect all relevant event data from the system, application and logs from supported products, converting them into a standardized format.

The Log Collectors then securely transmit this data to the Security Management Platform for further processing.

Security Management Platform

The Security Management Platform (SMP) is the heart of the Security Event Manager solutions, processing the myriad of security events collected from different systems in order to create a unified, real-time view of the organization's current security status. Administrators create their own rules of aggregation to tailor the system's monitoring functions according to their specific needs.

Following these rules, the Security Management Platform aggregates received event data, enriches the data with business-specific intelligence, and correlates the many events into a few, combined alerts. The SMP is also responsible for generating reports.

Web Console

The Web Console displays the processed events and alerts in a real-time security dashboard view. The Web Console provides a user-friendly Graphical User Interface (GUI) for the administration of the Security Event Manager Solutions, including configuration, managing backup schedules, and generating and scheduling reports.

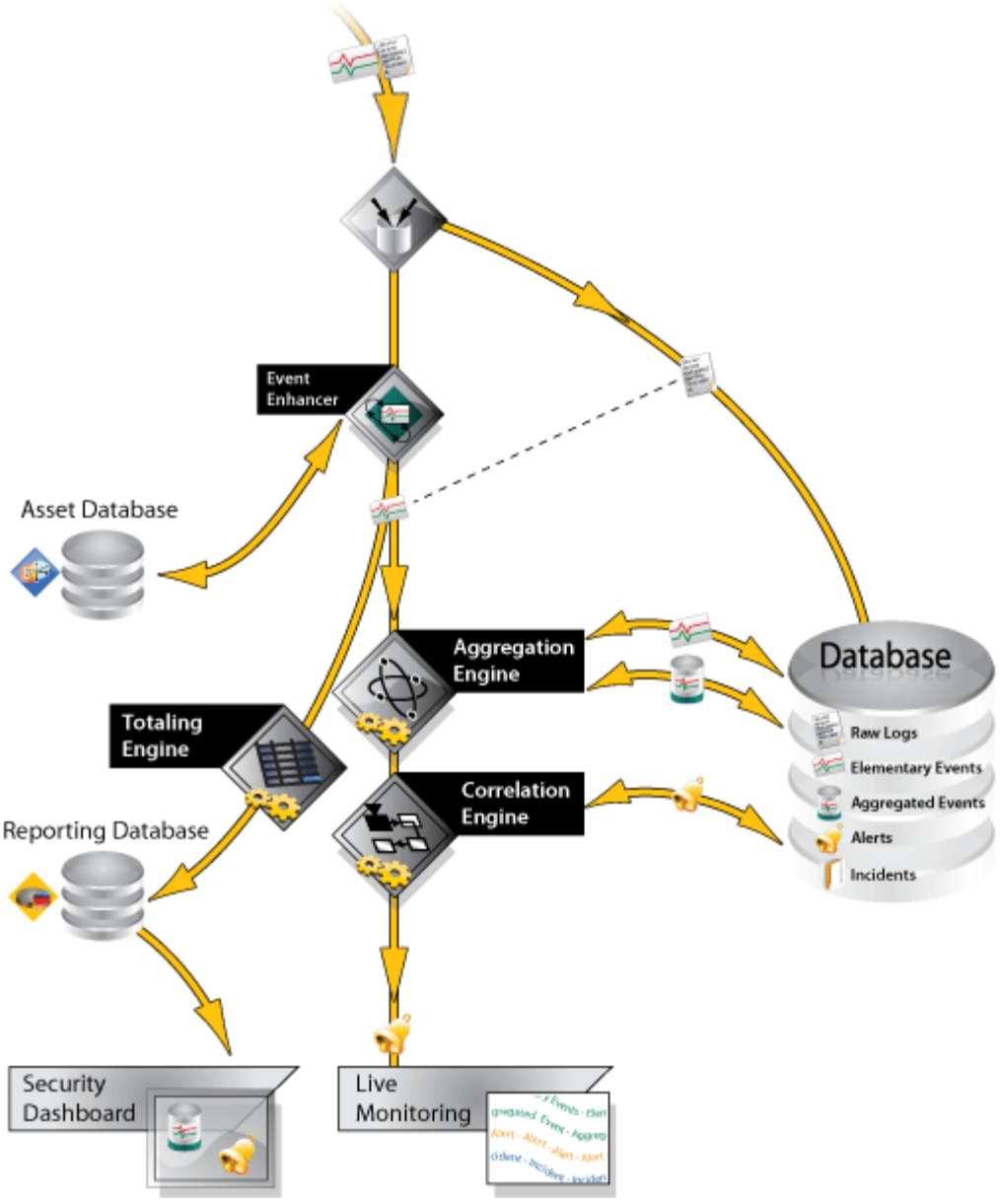
The multi-user console provides:

- Centralized configuration and management of TIBCO LogLogic® SMPs. The TIBCO LogLogic® Web Console provides a centralized configuration interface for monitoring and managing the Security Event Manager Solutions.
- Log management. The TIBCO LogLogic® SEM provides an archiving functionality. Records can be easily retrieved and analyzed when necessary.
- Reporting. The TIBCO LogLogic® SEM contains over 20 security dashboards (containing more than 150 standard reports). Additional reports can be created by the user (usually by amending a current report) and the database can be queried using SQL if required. Reports can be saved as PDF and automatically sent via email.
- Real-time alerting. The SEM includes a real-time display of alerts. The alerts are prioritized according to their criticality which in turn is based on the Confidentiality, Integrity and Availability (CIA) rating of HBOS' assets.
- User GuideForensic analysis. Forensic reports are easily generated using the forensics module.

A Three-Engine Architecture

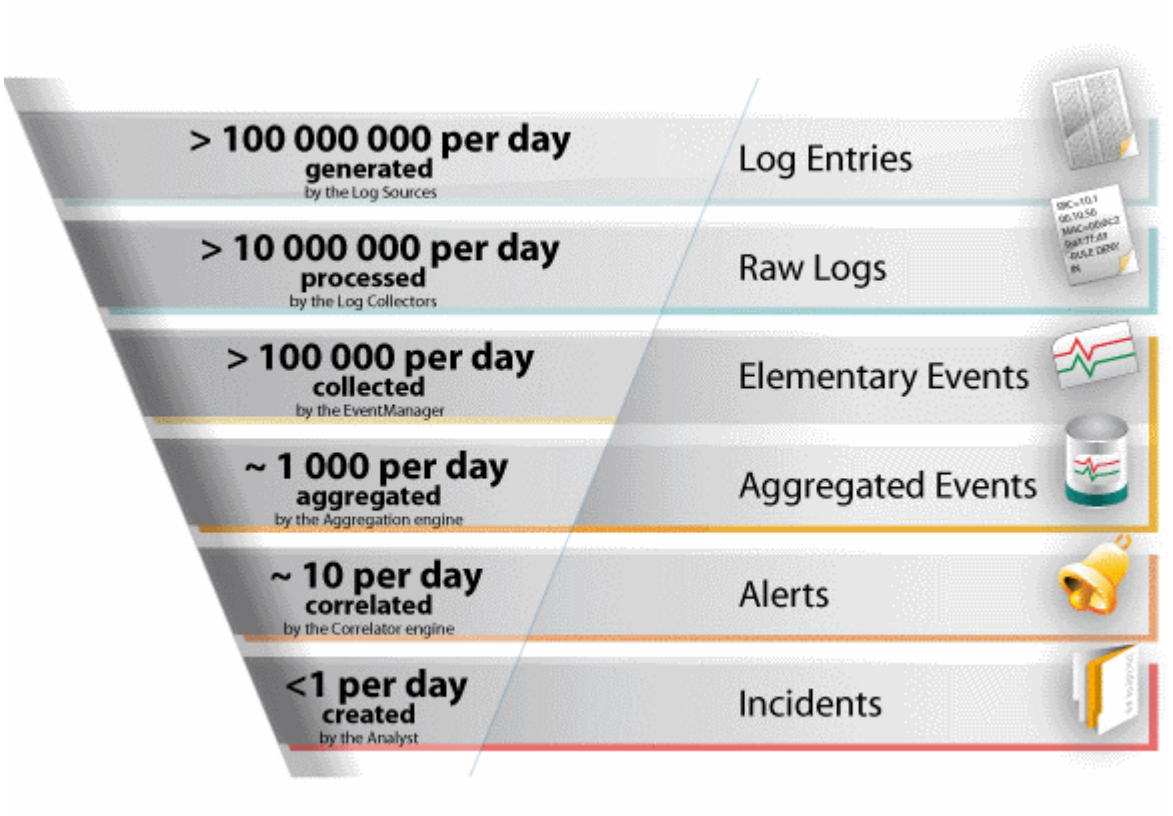
The SMP comprises three core engines to process the incoming events data: the aggregation, the totaling, and the correlation engines.

Figure 1 Three-engine Architecture



The raison-d'être of this three-engine architecture is to increase performance to optimal levels regarding the fundamental functions of the SMP: processing large volumes of incoming data, storing essential information, and displaying for the user only the security data that are most useful for analysis.

Figure 2 Incoming Data Processed by the SMP



The Sequence for Processing Security Events

The following section explains the fundamental sequence performed by the SEM for processing security events data.

Figure 3 SEM Sequence

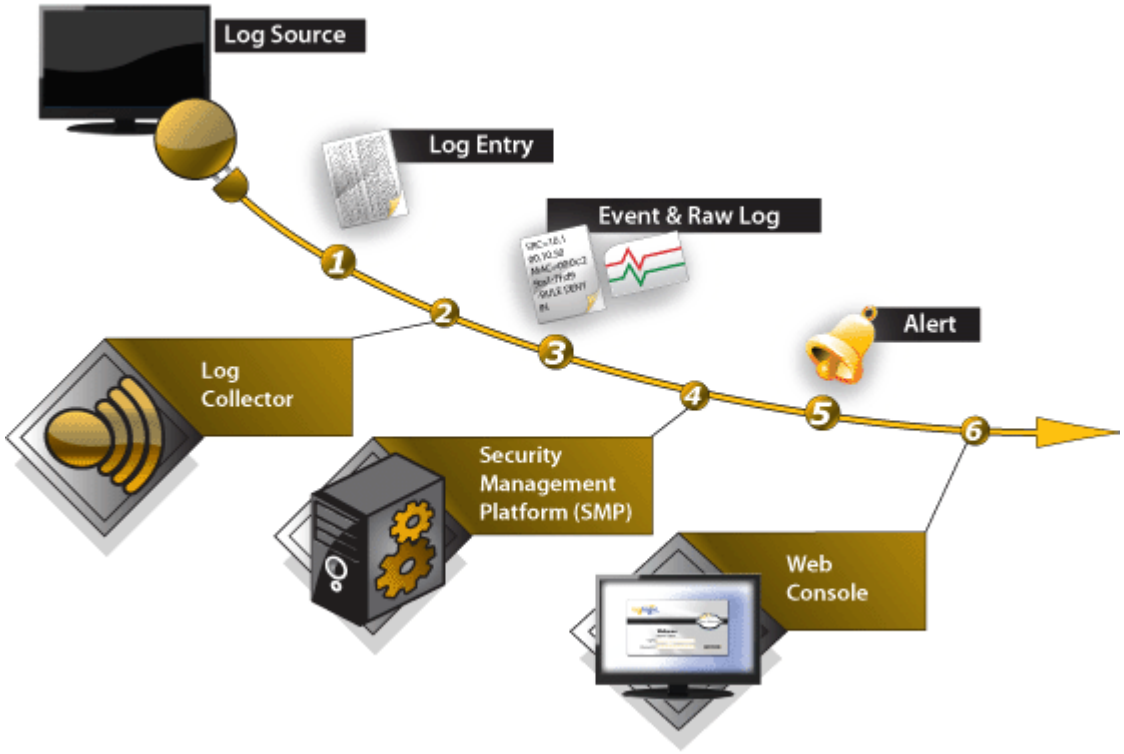


Table 2 Security Event Manager Sequence

1	**A Log Source Event Occurs** An activity ("log source event") occurs in an equipment unit. The "log source event" is registered in the product log which is not a part of the SEM. Depending on the product configuration, this log entry can be a text file, a database, or another proprietary format.
2	**Log Collector Analysis** According to pre-defined and custom rule-sets, the Log Collector will then analyze the product log entry and possibly forward it to the SMP. Whether the Log Collector discards the information or forwards it to the SMP depends upon how the Log Collector was previously configured.
3	**Log Collector Data Formatting** If the Log Collector has been configured to forward the information to the SMP, the Log Collector may format this data in two ways: a raw log text format (comprising the date, the log source name, and the original message), and a standardized IDMEF format, also called an "event" in SEM terminology. (This data standardization will enable the Security Management Platform to directly compare fields within events collected from different systems and services and execute any subsequent aggregation and correlation operations.) Data that is not selected to be forwarded to the SMP is discarded from the SEM. The main reason for the importance of the raw log is in view of required legal proof about an event generated by a supported product since a raw log entry is the most faithful format derived from the data produced by a log source. This is why the SEM can be configured to keep a record of the event generated by a supported product in the raw log format as well as producing a standardized version of it in the IDMEF database (an event).
4	**Forwarding Information to the SMP** The Log Collector will send either the event, or the raw log entry, or both. This information is then transmitted by SSL/TLS to the Security Management Platform. (In case of network failure or congestion, events are spooled in temporary files and transmitted later). The Log Collector has a spooling functionality, but it does not have a permanent storage function. This spooling mechanism will locally store events in case the link with the SMP goes down. Regarding storage of information, there are two possibilities: data of an event generated by a supported product in their original format can be stored in the equipment log, which is not part of the SEM. The Log Collector can also format and forward the data to the SMP which stores them in the SMP Normalized Event database. Additional backup operations/systems can provide long-term storage of information.
5	**Alert Generation** The three-engine ensemble of the SMP processes incoming events.
6	**Monitoring via the Web Console** Events and alerts are displayed in the Web Console to be monitored by the analyst.

The Three Engines

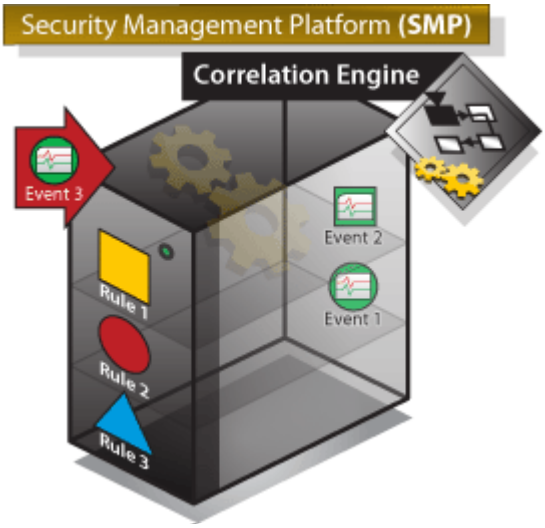
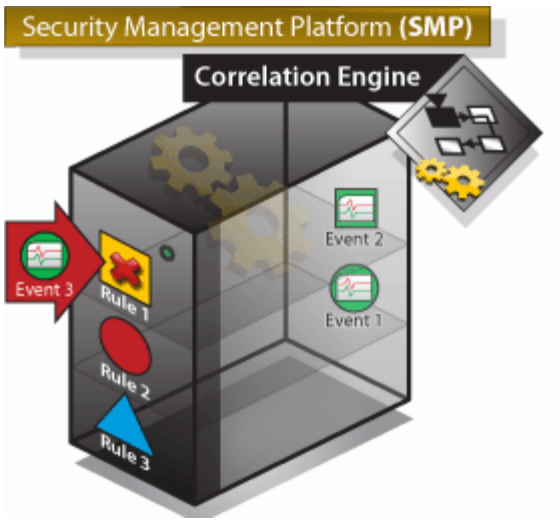
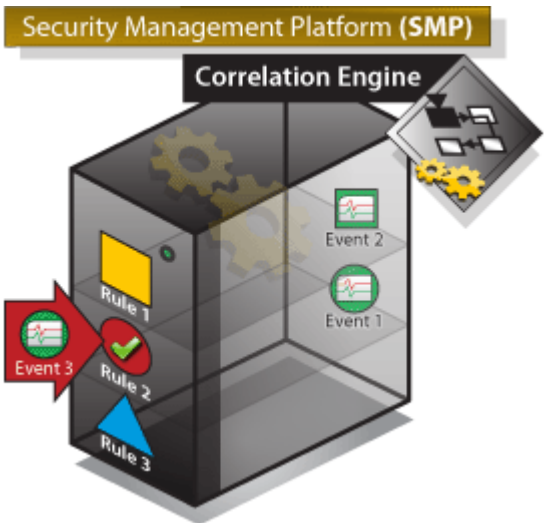
When the SMP receives an event (which has already been formatted in the IDMEF format by the Log Collector), it can extract information for statistics and reporting with the totaling engine and it can further process this information through the aggregation engine, compressing necessary information and discarding the remainder.

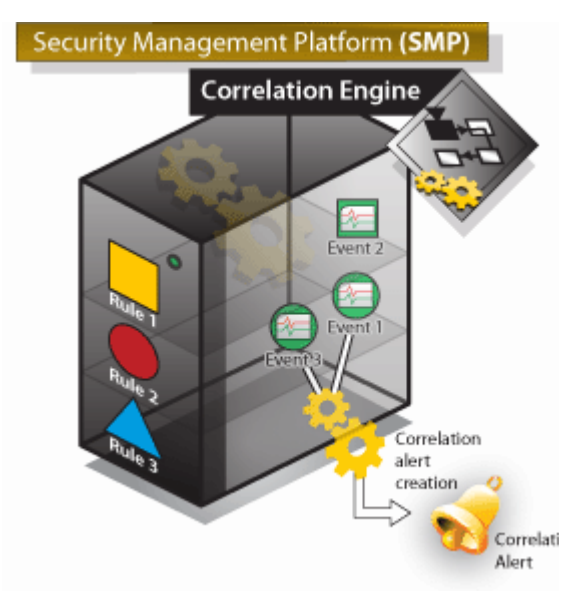
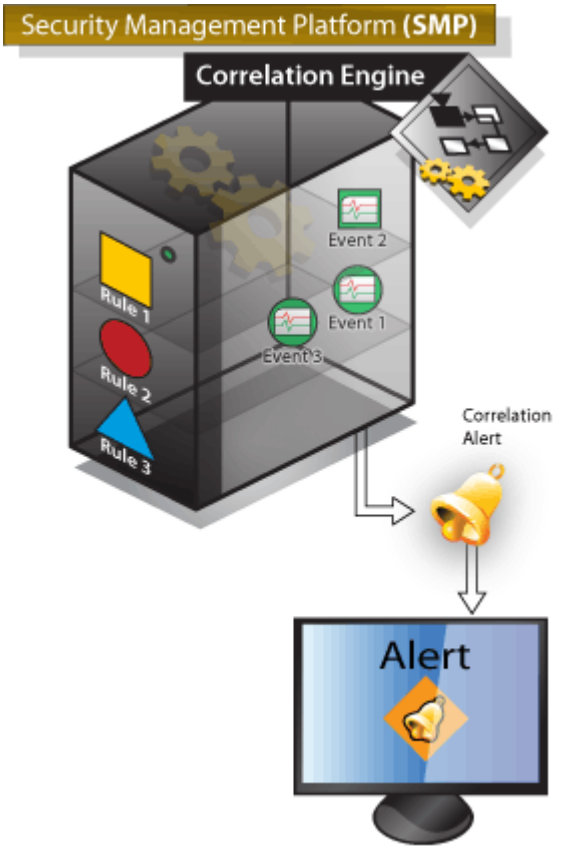
The totaling engine's main function is to count and sum up events, that is, it has a statistical function. The totaling engine also processes data according to default and user-specified rules. The totaling engine does not store all of the incoming information for incoming events, in fact, it discards most of the information and extracts only the necessary details to generate statistics (which are later also used for reporting).

The aggregation engine analyzes incoming data and combines together similar elementary events into one aggregated event. This process is also based on default or user-defined aggregation rules. In an optimal case, the aggregation process will considerably reduce the volume of the original incoming event data. This achieves two key objectives: a great gain concerning storage performance and the reduction of processing time consumed by the SMP engines.

The aggregation engine will then send the aggregated events to the correlation engine which will possibly correlate these events with other stored events to produce an alert or it may display this event as a sole component in an alert.

See a sequence of illustrations showing the correlation engine functioning logic below.

<table>
<tr>
<td> 
</td>
<td> 
</td>
</tr>
<tr>
<td>Inside the SMP correlation engine we find the SMP rules database. In our example, two events have already arrived at the engine and are pending.</td>
<td>A new event arrives.</td>
</tr>
<tr>
<td> 
</td>
<td> 
</td>
</tr>
<tr>
<td>The SMP correlation engine compares information with the conditions in Rule 1, looking for a match.
No match is found with Rule 1.</td>
<td>The SMP correlation engine proceeds to compare information with the conditions in Rule 2.
A match is found with Rule 2.</td>
</tr>
</table>

	
For the purpose of this example, Rule 2 tells the SMP to create a correlation alert and stop the comparisons if a match is found. As a consequence, a correlation alert is created.	The corresponding alert is displayed in the GUI.

As with the aggregation and the totaling engine, the correlation engine's procedure will depend on the rules and scenarios that have been previously configured by default or by the user. A brief description of the process of enriching the collected data and its subsequent correlation follows.

Enrichment of Collected Data

The enrichment process enables the TIBCO LogLogic® SEM to consider alerts in a business specific context. For example, specific alerts or events can be 'weighted' according to the criticality of the asset and the real threat posed. This dramatically reduces the number of false positives, whilst accurately representing the threat posed by current security violations.

TIBCO LogLogic®'s SEM uses an Asset Database populated from a variety of sources which include:

- Assets - from automated asset scanners or management tools or from an asset file. Each asset has a criticality (high, medium, low), a specific SLA (Service Level Agreement), and can be assigned to a group (e.g. servers, firewalls, mission critical, marketing department, SOX assets, HIPAA assets, accounting department, etc);
- Vulnerabilities - from active vulnerability assessment and management tools;
- Risk assessments;
- Security policies and processes;
- Incident response plans;

- Service Level Agreements (SLA's).

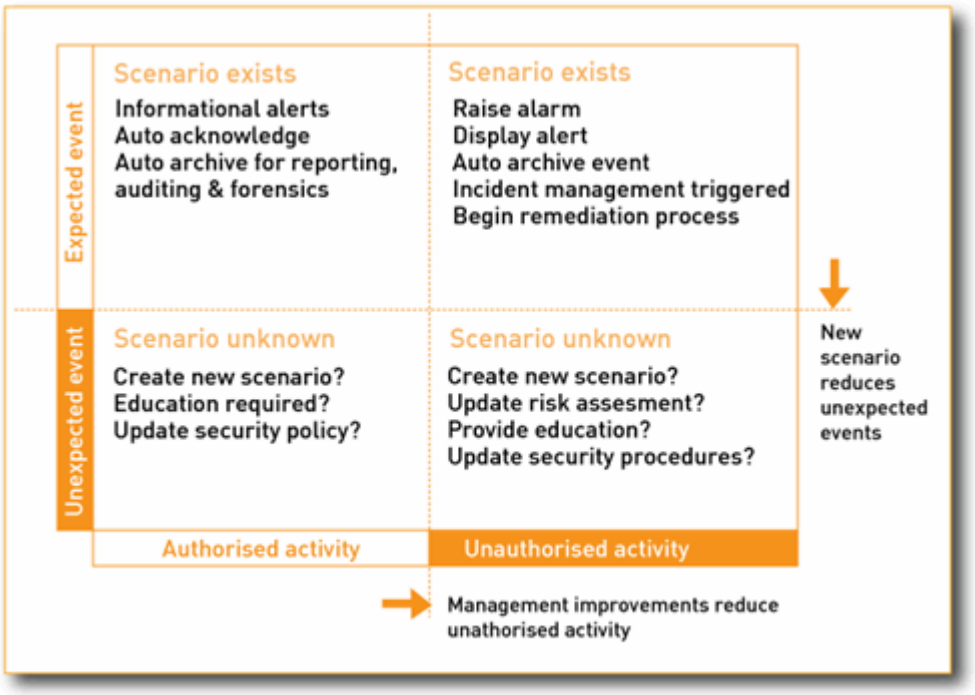
Correlation

By correlating events, deductions can be automated as to whether the events are authorized or not. For example, a firewall event reporting a connection to an email server in itself cannot be classified as unauthorized. An isolated event on the mail server regarding a user sending an email is also not of great interest. By correlating the two events we can determine that an authorized user has successfully accessed the mail server. If only a firewall event is recorded, and there is no corresponding email server access event, this can be investigated further to decide if it is part of an attack on the mail server.

Authorized, expected events can be archived, while unauthorized events can be alerted enabling the necessary remedial action to be taken. This may include adding additional scenarios to the SEM to include some of these events as new expected behavior.

As the process continues, more and more types of events become expected and actions can be pre-defined depending on whether they are authorized or not. The total number of types of unexpected events will decrease and this will improve the overall efficiency of analyses. This iterative process further reduces the event noise and increases the operational effectiveness and response times of the security team.

Figure 4 Processing Events



Examining a Real Example (*Brute Force Attack)*

Let us look at the sequence of events in a real example, a detection of a brute force attack on an SSH service. Our Log Collector has been configured to detect when a user tries to log on and whether they succeed or fail. Every time a user fails to log on, the Log Collector sends an event to the SMP signaling the login attempt failure. Since a brute force attack will consist of multiple attempts to log on to our machine, we have also specified this correlation condition in our "Aggregation and Correlation" rule-set definition. Thus, several similar events for login failure will be correlated into one brute force attack alert.

Step 1: A log is generated by a supported product

A user tries to connect from a source machine with the IP 192.168.10.12 to the 192.168.10.55/icare machine through SSH, but the connection fails. This activity will generate the following log entry in the file /var/log/messages (on the target machine):

```
Apr 13 14:45:17 icare sshd[25491]: Failed password for root from
192.168.10.12 port 4555 ssh2
```

The Log Collector installed on the target machine had been configured to monitor the file /var/log/messages with a conversion rule-set for the SSH server in order to detect whether a connection was successful or not. This rule-set contains the following rule to analyze and convert the log entry that was generated:

```
regex=([\w.-]+) sshd\[\d+\]:.* Failed (\S+) for root from
(?:::\w+:)?([\d\.]+) port (\d+)\s*(ssh2)?;
        regexId=3;
        categoryId=3_56.67_57.45;
        skip=false;
        classification.text=SSH Remote root login failed;
        assessment.impact.severity=medium;
        assessment.impact.completion=failed;
        assessment.impact.type=admin;
      assessment.impact.description=Someone tried to login as root
from $3:$4 using the $2 method;
        source.node.nameOrIp=$3;
        source.service.nameOrPort=$4;
        source.service.protocolNameOrNumber=tcp;
        target.node.nameOrIp=$1;
        target.service.nameOrPort=22;
        target.service.protocolNameOrNumber=tcp;
        target.user.userId.nameOrNumber=root;
        last;
```

Listed below are a few explanations for the parameters above:

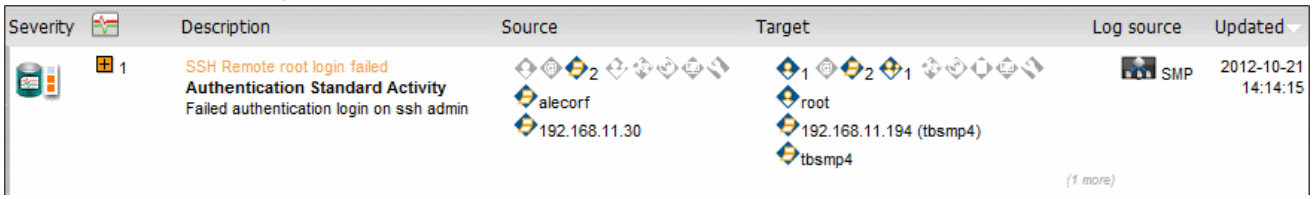
- The parameter "skip=false;" instructs the Log Collector to send the event to the SMP server.
- The parameter "classification.text=SSH Remote root login failed;" specifies the event's name.

Since there was a login failure, the Log Collector standardizes the log entry into its IDMEF format, and then transmits this information to the SMP.

Step 2: The SMP Receives Events and Creates an Alert

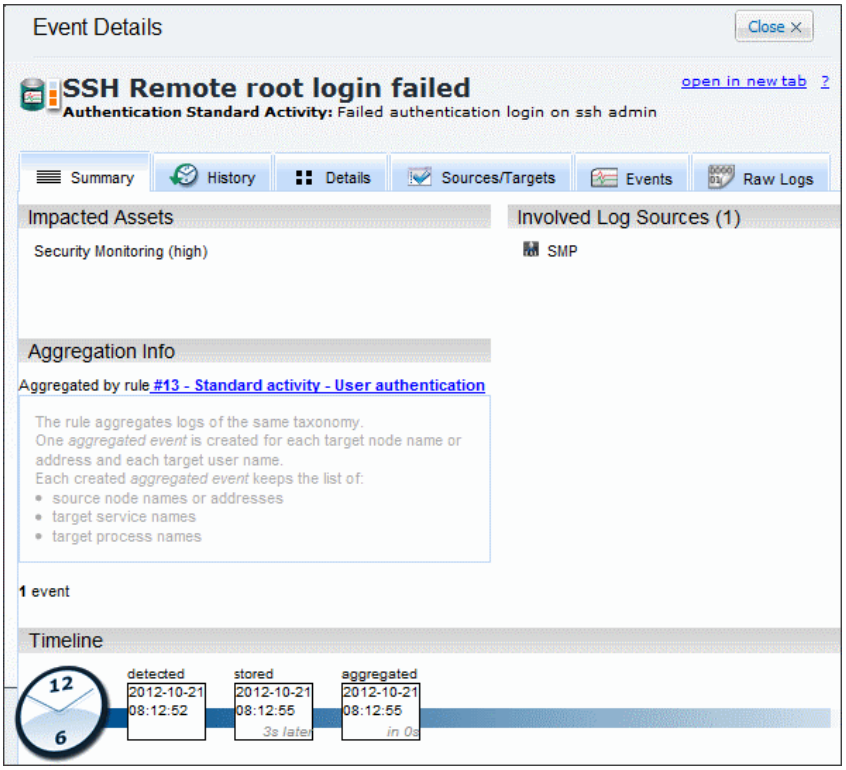
The SMP receives the event information sent by the Log Collector, which is displayed in the event monitoring screen.

Figure 5 The Events



If we click on the classification name (**SSH Remote root login failed**), we will see the details for this event.

Figure 6 Summary Tab



In our example, the same user then executes 3 subsequent attempts to connect to the SSH server, reaching a total of 4 attempted logins. This information is processed by the Log Collector and sent to the SMP. These events will now all be grouped together into an alert -- this time, a Service Brute Force Attack alert.

Step 3: Configuration of the Correlation Rule

Let us examine how we have configured our correlation rule. Our correlation condition is whether the authentication activity of the login has failed. We have also specified that the threshold is 4 alerts/events and the alert will be of medium severity. Therefore, if a user attempts to log on only twice and gives up, no alert will be created.

Figure 7 General Tab

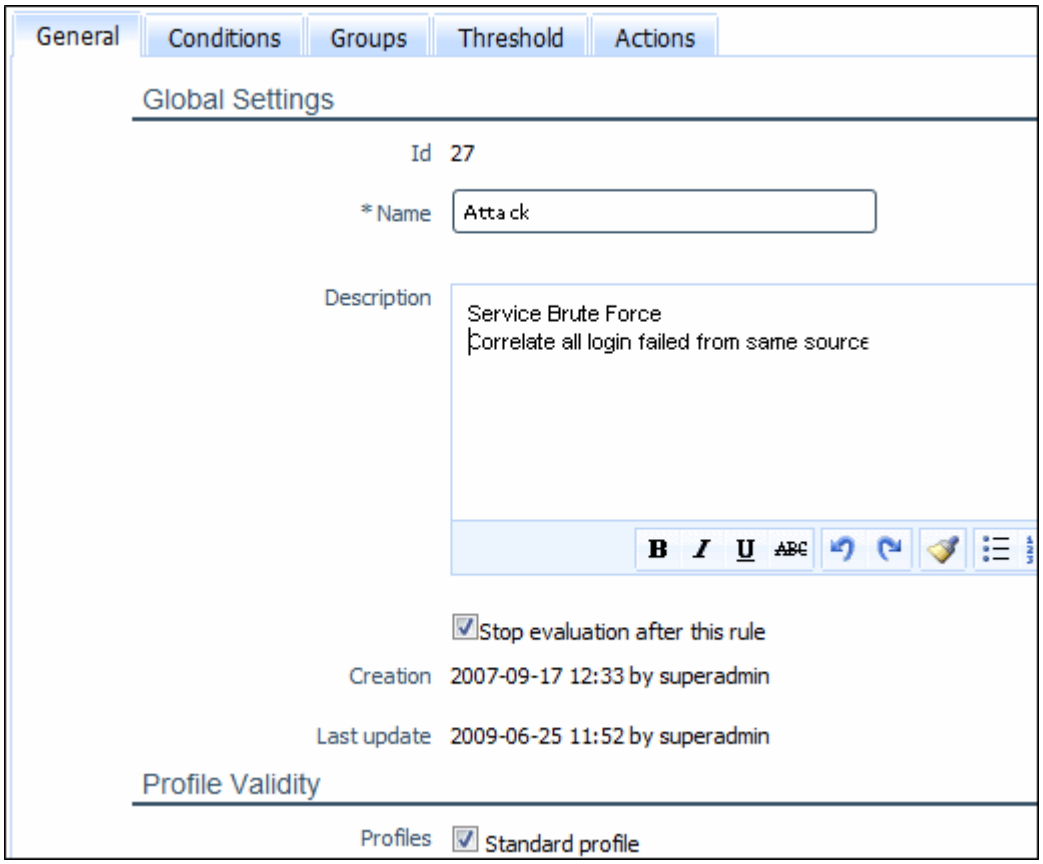
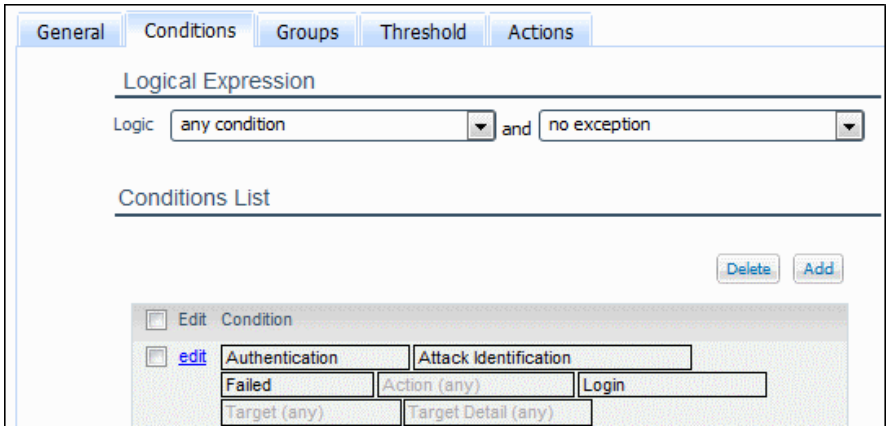
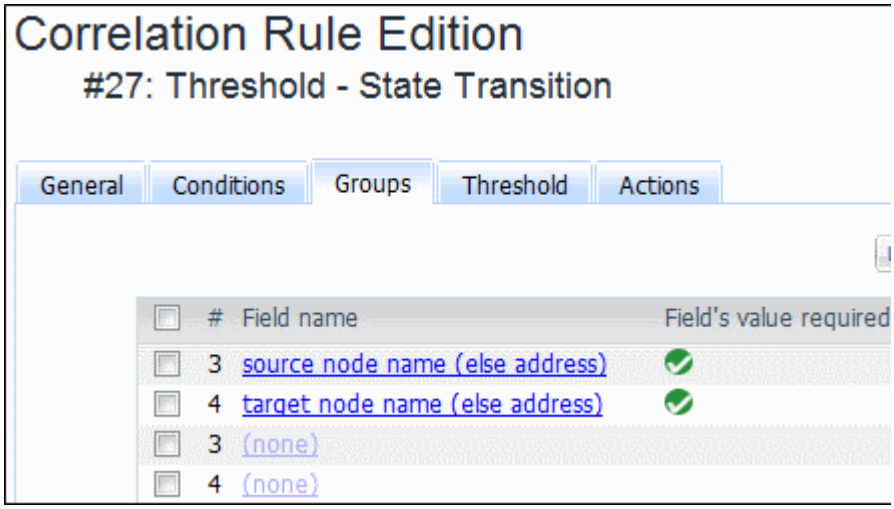


Figure 8 Filters Tab



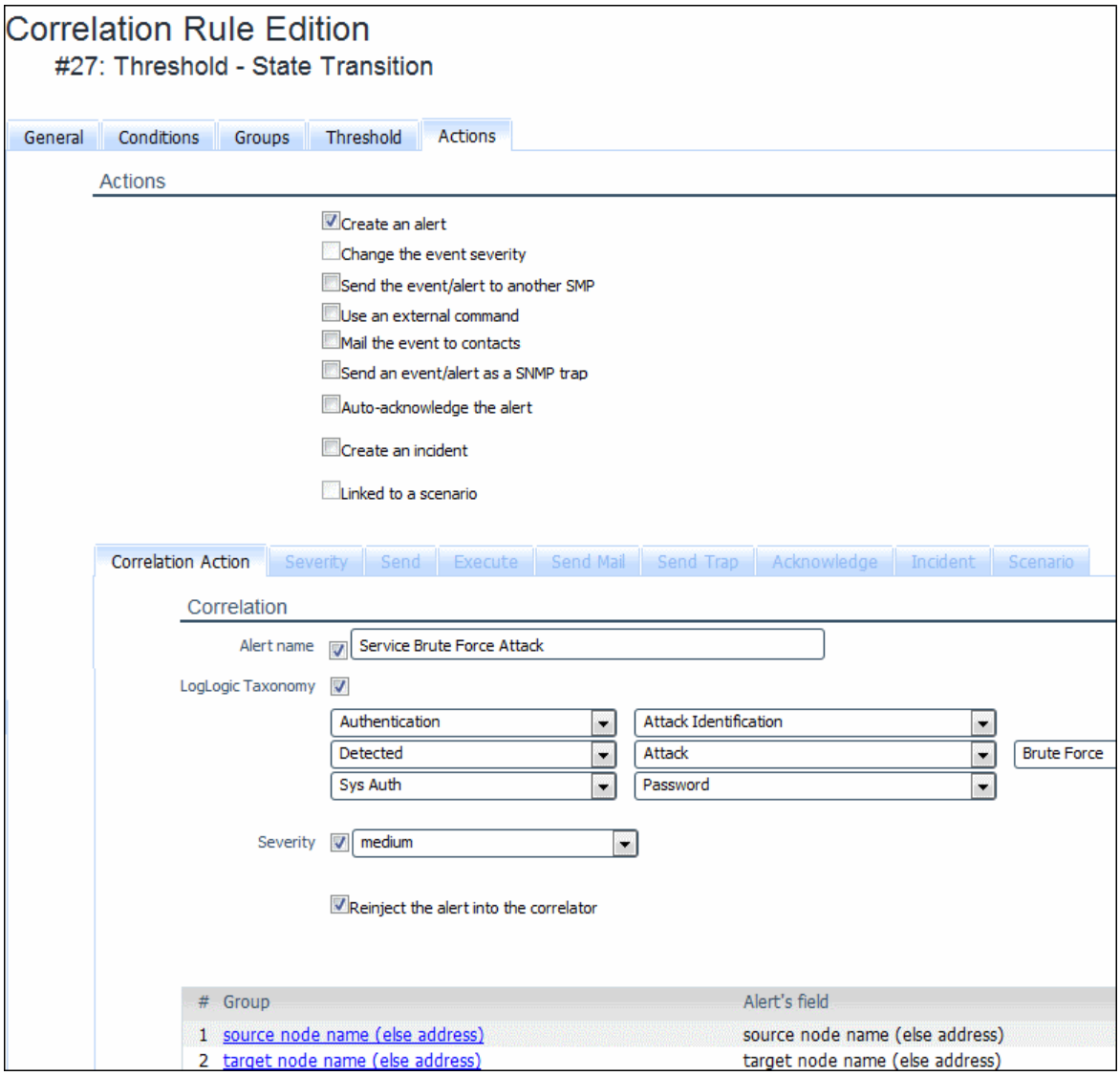
Notice that we have also specified in the Aggregators section the **Source Node Name Or Address** and the **Target Node Name Or Address** fields. This means that the SMP will verify if the events' source and target machines are the same. If they are not, this condition is not met and the login failure alert will not be incorporated into a brute force attack alert. In this case, if a user makes multiple login attempts to different machines, these login events will not be correlated into a brute force attack alert according to this rule-set.

Figure 9 Groups Tab



In the section displayed below, we have specified that, in case all our conditions are met, the SMP will create an alert (named "Service Brute Force Attack"):

Figure 10 Actions tab



Step 4: The SMP Creates an Alert

Four failed login attempts take place, consequently, the SMP produces an alert according to our rule configuration, and displays it on the Alert Monitoring screen.

If you click on **Service Brute Force Attack**, a screen pops up furnishing details for this alert such as **Alert Displayed** the number of aggregated events contained in this new alert. Please note that an alert can contain one or more alerts/events and/or one or more alerts.

Conclusion

Through this simple example, we have explained the sequence and logical mechanism for creating an alert according to predefined specifications and rules. In the end, we obtained the desired result - an alert containing 4 disparate events for failed login attempts.

This example shows the core logic of the SEM for correlating alerts. By using the SEM system, this key process of correlating multiple alerts into fewer important ones allows you to monitor huge volumes of events and still detect important hidden threats and other security problems.

Chapter 2 - Connecting to the Web Console

The Web Console Welcome screen allows the user to enter his login/password and launch the application after authentication.

This chapter contains information about:

- Requirements
- User Authentication
- About the Web Console Locked Access

Requirements

Five pre-requisites are necessary before connecting to the Web Console:

- Your workstation must have at least **1 GB RAM** installed.
- A web browser must be installed on your computer. It must be either **Microsoft Internet Explorer v.7.0** or higher or **Mozilla Firefox 13**. For the best Web Console performance, we suggest disabling Firebug if you use **Mozilla Firefox.**
- The Security Network Administrator must have done the initial configuration of the Web Console installed and accepted the server certificate.
- The user with the super-administrator or administrator account must have created your user account via the Web Console. For more information about adding a user or modifying a user account, refer to the Add/Edit Users section.

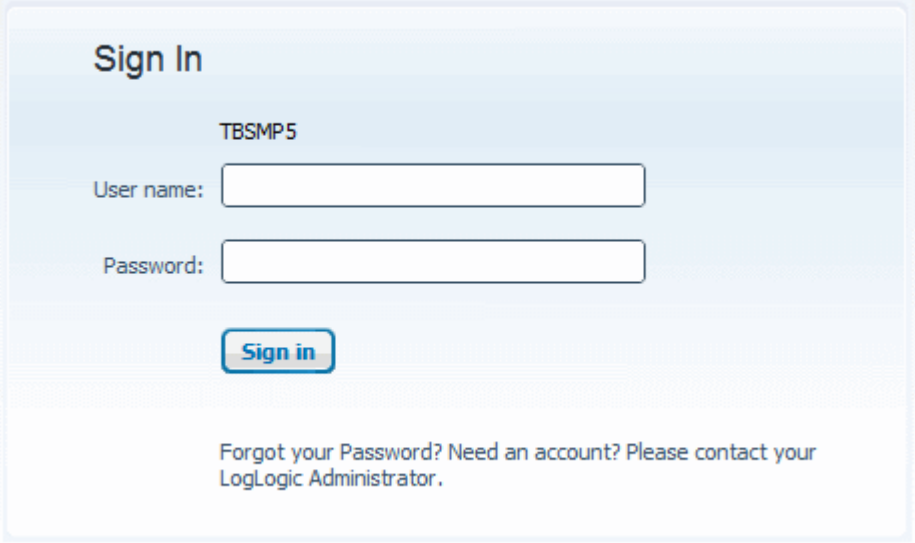
User Authentication

The procedure to authenticate is the same, whether you use a standard or a RADIUS external authentication server.

1. Connect to the Web Console. A warning message asking you to check the TIBCO LogLogic® certificate may appear. In that case, please contact your security network administrator.

The Web Console **Welcome screen** is displayed:

Figure 11 Web Console Welcome Screen



2. Enter your user name in the **Login** field (no more than 50 characters).

3. Enter your password in the **Password** field (no more than 25 characters). If you have forgotten your password, contact the super-administrator or administrator who will give you a new password.

4. Click on the **Log in** button. The monitoring screen is displayed.

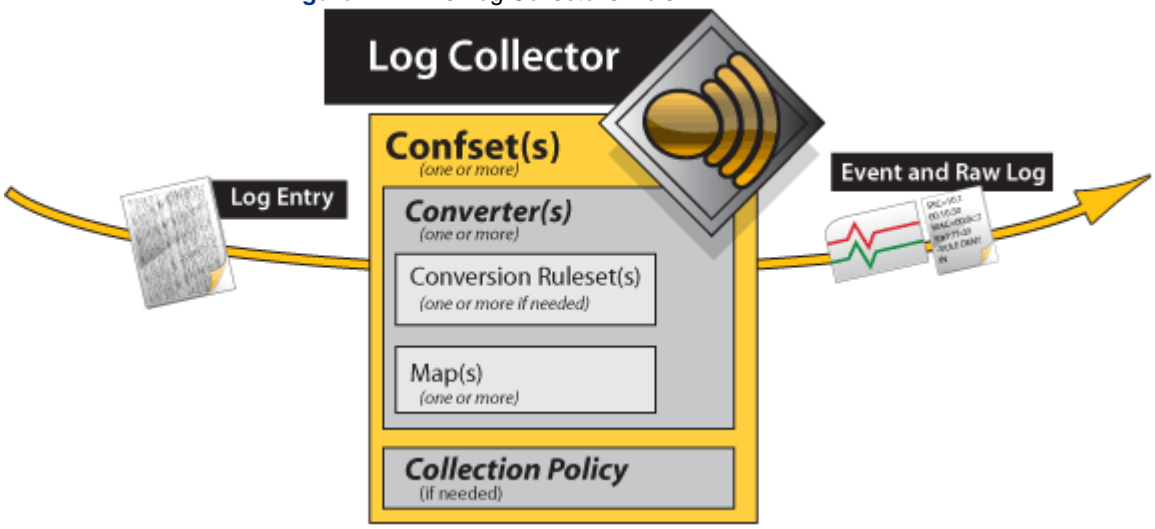
About the Web Console Locked Access

- If you enter a wrong login or password, you will get an error message.
- For security reasons, if you fail to login to the Web Console after three consecutive attempts using the wrong password, you will not be able to access the Web Console any longer.
- At the third attempt, the message **Account locked** will be displayed. In that case, you must contact the user with the super administrator or administrator account. He is the only one who can enable your user account as described in the Locking/Unlocking a User Account section.

Chapter 3 - Collecting Logs

The Log Management menu allows the user to deal with large volumes of device-generated log messages by defining relevant collection policies performed by an intelligent tool called the Log Collector.

Figure 12 The Log Collector's Role



The Log Collector:

- collects all desired event data from the system, application and device event logs, giving the most comprehensive security record possible. This makes possible the correlation of events gathered from all relevant internal and external systems, providing real-time end-to-end session tracking and monitoring.
- can receive data directly as a Log Collectorless connection on systems where the deployment of the Log Collector is not possible or desired. For example, routers which do not allow Log Collector installation can instead send Syslog event data directly to the SMP.
- converts collected event data into a standardized IDMEF format according to pre-defined and custom rule-sets. This data standardization enables the SMP to directly compare fields within events collected from different systems and services.
- transmits converted events by SSL/TLS to the SMP for further processing. The encryption process first compresses the data for optimal bandwidth utilization. In case of network failure or congestion, spooled events are sorted and transmitted in priority order.
- can extract event information from multiple log formats and protocols, including: RDEP, WMI, Syslog, OPSEC, proprietary databases, flat-files and APIs.

Supported Collection Method per Log Collector Platform

Table 3 Supported collection types for each Log Collector platform - 32 bit

		Syslog	File	Database	Windows Event Logs*	Check Point	Scanners	Cisco IPS	RSA	Lotus Notes
Windows	2008 R2	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
	2008	✓	✓	✓	✓	✓	✓	✓	✓	✓
	7	✓	✓	✓	✓	✓	✓	✓	✓	✓
	2003 R2	✓	✓	✓	✓	✓	✓	✓	✓	✓
	2003	✓	✓	✓	✓	✓	✓	✓	✓	✓
RHEL***	5	✓	✓	✓	✓	✓ **	✓	✓	✗	✓
AIX	7	✓	✓	✓	✓	✗	✗	✓	✗	✓
Solaris	10	✓	✓	✓	✓	✗	✓	✓	✗	✓

Table 4 Supported collection types for each Log Collector platform - 64 bit

		Syslog	File	Database	Windows Event Logs*	Check Point	Scanners	Cisco IPS	RSA	Lotus Notes
Windows	2008 R2	✓	✓	✓	✓	✗	✓	✓	✗	✓
	2008	✓	✓	✓	✓	✗	✓	✓	✗	✓
	7	✓	✓	✓	✓	✗	✓	✓	✗	✓
	2003 R2	✓	✓	✓	✓	✗	✓	✓	✗	✓
	2003	✓	✓	✓	✓	✗	✓	✓	✗	✓
RHEL	5	✓	✓	✓	✓	✗	✓	✓	✗	✓
AIX	7	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Solaris	10	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A

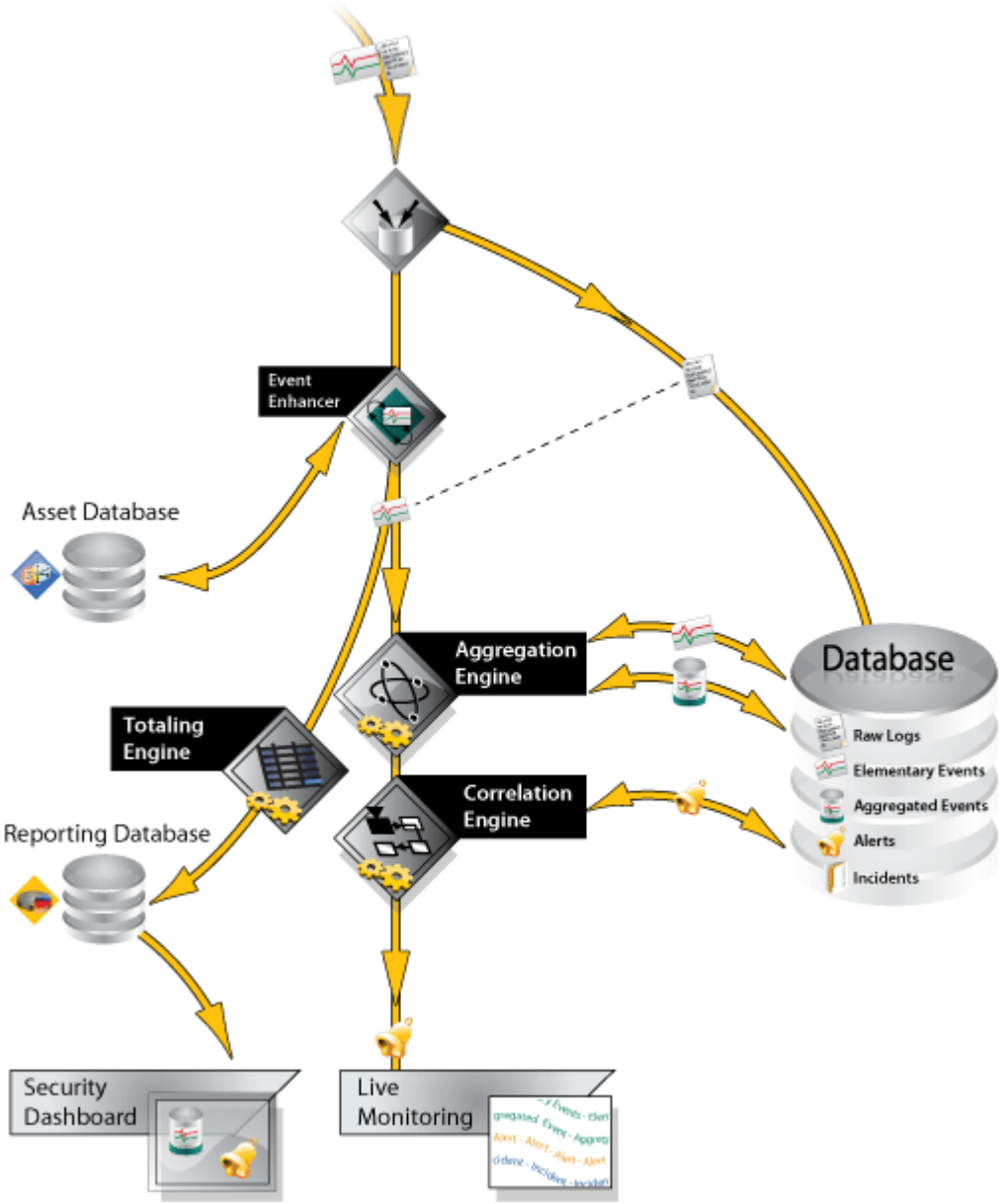
*** Supported Log Sources are: 2003, 2003 R2, 2008, XP, Vista**
**** You must install the 'compat-libstdc++' compatibility module to make it work properly.**
***** If 32-bit SE linux is enabled, log collection cannot start. You need to set SELINUX=permissive in /etc/selinux/config.**

Log Process

This part of the documentation allows you to have a schematic view of log processing from its process by the Log Collector to its display within the Web Console or reporting interface through the correlation and aggregation engines.

Schema

Figure 13 Log Process



Description

1. A Log Collector collects and processes logs obtained via syslog, database connection, through the direct reading of a file, etc. The process:

a. either ignores the log,

b. or sends raw log and/or event data in an IDMEF format via a safe channel.

For a more detailed diagram, please refer to The Log Collector.

2. Once the object has been received by the SMP, the server extracts the various components (raw log and/or elementary event).

a. If the object is a raw log: it is redirected towards the database dedicated to raw logs, then its process stops. For legal reasons, no action is performed on it, from reception to archiving process. You can view this via a search screen (forensic dedicated to raw logs).

b. If the object is an event: it is forwarded on to the Event Preparer.

3. The Event Preparer has only one function: enriching the event according to the information contained in the database regarding the DNS name or IP address.

a. If the event contains two kinds of information, then they will both be inserted into the database (if this is not already the case).

b. If the event contains no information of this kind, then it is ignored.

c. If the event contains one of these two kinds of information, this tool evaluates whether it can add another kind of information to it according to its database.

4. The main function of the Totaling Engine is for statistic analysis. It allows the counting of events. In other words, it means that each event coming from the Asset Database is sent to both the Aggregation Engine and the Totaling Engine.

The log contains evaluation rules to count different elementary events according to criteria predefined by the user.

The aim of this step is to calculate for example the number of alerts coming from various sources received by the firewall per day. It is then possible to draw up a precise report without generating calculations regarding aggregation, correlation, etc. It allows the processing of minor events with a high interest regarding the counting.

5. The Aggregation Engine's main aim is to produce fewer events and then take less amount of space on the disk. It behaves nearly in the same way as the Correlation Engine. Rules evaluate events in order to generate actions. Usually, when there is an action, the engine is separating one event from another. Here are the possibilities:

a. To be able to ignore an event (skip).

b. To fuse this event (or not) with other ones according to specific criteria (definition of common fields, grouped fields, deleted fields). This is the only way to proceed with continuous treatment of an aggregated event.

By default, it is also possible to store a elementary event in a dedicated database. This is especially useful for event storage and searching. For a more detailed diagram, please refer to section The Aggregation Process.

6. Once events have been processed by the Aggregation Engine, they are not only sent to the Correlation Engine but also stored in a dedicated database (aggregated events).

The data contained in this database are available from within the Web Console. The aggregated events details are based upon the elementary events database.

7. The aim of this step is to correlate various aggregated events and/or alerts. This will give you a more general view of the different actions to perform (creation of an alert most often).

Alerts are created and stored in a dedicated database allowing report edition, visualization (main view of the console) and forensic search.

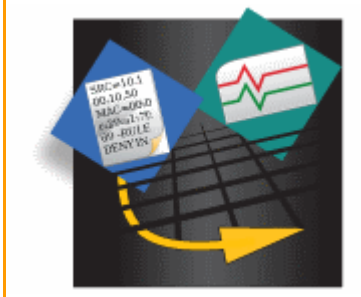
For a more detailed diagram, please refer to section The Correlation Process.

Adding a Log Source Automatically: Wizard

The wizard is a tool intended at adding and configuring a log source in an easy and friendly way.

The log source is the element which generates security events or logs that will be collected by the Log Collector e.g. a firewall, a proxy, an IDS, a web application, an Operating System, a database...

Here is a description of the log collection by the Log Collector.

	The Log Collector selects a log among the list of logs pending to be processed.
	The Log Collector: extracts the necessary data to create an elementary event in IDMEF format. transforms it to create a raw log.
	Both raw logs and elementary events enter a filter where a Collection Policy will be applied. Several options are possible: 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
	The element (either the elementary event or raw log or both) is sent to the SMP via a safe channel (SSL).

The wizard is composed of three main screens where you must:

- configure the log source,
- configure the Log Collector,
- define the connection type.

Opening the Wizard

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...).

You must click **Configure a Product** to start the wizard.

> **Note:** If you work with an LMI (LX/ST/MX) server, then click on **Configure a Forwarder** and follow the procedure described in the **UCM User Guide.**

Step 1 - Configuring the Log Source

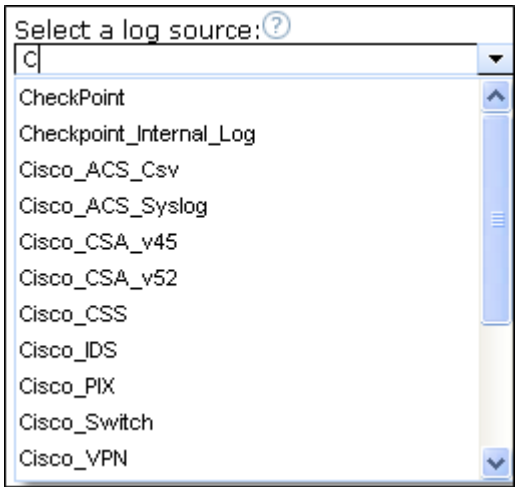
Selecting a Log Source

To select the log source:

- Either click in the combo box and select the name of the relevant log source in the list.
- Or type in the first letter of the log source name and all the names starting with this letter will be displayed. Then select the relevant log source.

Example:

Figure 14 Log Sources Starting with C



Selecting a Log Source Host

Each log source has a host that needs to be defined. It is essential for communication between the SMP and the log source. You have two possibilities. Either selecting an already existing host or creating a new one.

If you select an existing host:

1. Click on the drop-down list arrow. The list of existing hosts is displayed. Once the host selected, a new field is displayed.

2. Enter the necessary addresses so that the Log Collector can communicate with the log source and click on the + button to add them.

Note: All existing hosts are available in the Host list except the SMP host. Indeed, no application must be installed on this host.

If you create a new host:

1. Enter the new host name in the field.

Three new fields are displayed.

2. Enter the necessary addresses so that the Log Collector can communicate with the log source and click on the + button to add it.

3. Select the operating system on which the log source is installed.

4. Indicate the host site. Either select a host site in the list or create a site by entering its name in the field (e.g. Lyon).

5. If you have created a new host site, you must then also indicate its corresponding time zone (e.g. If Lyon is the site, the time zone is Europe/Paris).

6. Customize the log source name by entering a name of your choice.

7. Select a **Collection Policy**. If you decide to follow a policy of collecting events, then select the kind of events to be collected in the drop-down list.

Remember that an event is a representation of an entry in a system' s log referring to an actual “device event”. The list contains all the collection policies available. Please refer to "Log Collection Policy" section.

By default, the wizard uses the:

exa_6_StandardRawLog_AllElemEvent policy

except for the TIBCO LogLogic® log source for which the **exa_2_NoRawLog_StandardElemEvent** policy is used.

8. Once all the information entered, click **Next**.

Step 2 - Configuring the Log Collector

The aim of the Log Collector is to collect the events generated by the log source, and convert them into a standardized format. The Log Collector then securely transmits this data to the Security Management Platform for further processing.

Selecting a Remote or Local Log Collector

If you want the events to be collected by a Log Collector installed on the SMP:

1. Select the **Local** Log Collector radio button.

2. Click the **Next** button to go to the next step.

If you want the events to be collected by a Log Collector that is NOT installed on the SMP but on a remote machine or on the log source host:

1. Select the **Remote** Log Collector radio button.

Three fields about the Log Collector's log configuration are now displayed as described below.

Selecting a Log Collector Host

First case: you are selecting an existing Log Collector host in the list

- If the Log Collector's host is the same as the log source host, then all the fields below are shaded. It means that all data is exactly the same.
- If you select an existing host but different from the log source host, you must enter the addresses to communicate with the host. Follow the procedure as in Step 1 - "Selecting a Log Source Host".

Second case: you are creating a new Log Collector host

1. Enter the name of the host in the field.
2. Follow the procedure described in Step 1 - "Selecting a Log Source Host".

Selecting a Log Collector Communication Type

When you create a new Log Collector host, 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 immediately sent by the Log Collector to the SMP.

- If you want the SMP to detect the unavailability of the Log Collector more readily, choose **server->**Log Collector type.
- If there is a firewall between the two which prevents from connections to the Log Collector, e.g., when relaying alerts, you may have to use Log Collector**->server.**

Once you have defined the communication type, enter a name to describe the Log Collector. Then click **Next** to go to the next step.

> **Note:** The Log Collector's name must neither contains \ / : * ? " < > | characters nor a blank space.

Step 3 - Defining the Log Collector Connection

Step 3 allows you to enter the necessary connection parameters to allow the Log Collector to connect to the log source and retrieve logs.

Five cases are possible **according to the selection** made in **step 1**.

FILE log source selected in Step1

It means that the source of events to be monitored is a text file in the WELF format, a log or a multi-line.

If the Log Collector's host is the same as the log source host:

1. Enter the pathname of each file in which the logs will be collected.
2. Click **Next**.

If the Log Collector's host is different from the log source host:

1. Select the protocol through which syslog logs will be collected: **TCP** or **UDP**.
2. Enter the corresponding port (514).

3. Select the **severity** of the log to be collected in the drop-down list.

4. Select the **type** (or "facility") of the log to be collected by clicking on it. It is automatically moved to the selection list.

    a. If you want to select the whole list of facilities, click **Copy All**.

    b. If you want to remove a facility from the selection list, select it and click **Remove All** and click **Next**.

DATABASE log source selected in Step1

It means that the source of events to be monitored is an SQL database.

1. Select the database name.
2. Enter a name and password for the Log Collector to connect to the database.
3. Indicate the port to which the Log Collector can connect and click **Next.**

OPSEC log source selected in Step1

The events will be collected via the OPSEC protocol, e.g. when collecting events from a firewall.

1. Select the relevant authentication mode i.e. ***clear, sslca clear*** or ***sslca***.
    - ***clear***: no authentication.
    - ***sslca***: protocol based on encrypted certificates. It is used for authentication, all data is also encrypted.
    - ***sslca clear***: protocol based on encrypted certificates. It is used for authentication, all data is not encrypted.
2. Select the OPSEC port and address.
3. If you have selected **sslca clear** or **sslca** authentication modes, you must indicate the:
    - SIC name client and server. Remember that the SIC or Secure Internal Communication is used for authentication between **CheckPoint** components.
    - **sslca** file location.
4. Click **Next.**

WMI log source selected in Step1

The events will be collected via WMI.

- If the host where the Log Collector is installed is the same as the log source host, no additional parameter is required.
- If the host where the Log Collector is installed is different from the log source host:

1. Enter the log source's IP address or name.
2. Enter the user login and password to connect to the machine.
3. Specify the domain and click **Next.**

RSA log source selected in Step1

You have already entered all the necessary data for log collection.

1. Click **Next**.

RDEP log source selected in Step1

It means that the events will be collected via the RDEP protocol, e.g. when collecting events from CISCO secure IDS.

1. Enter the address of the converter.
2. Enter a login and password for enabling communication.
3. Optionally, you can enter the port to which the Log Collector must connect.
4. Click **Next**.

SCANNER log source selected in Step1

It means that the events will be collected via a vulnerability scanner, e.g. when collecting events from Criston VM.

1. Enter the pathname to the directory where scanner reports in xml format will be available. E.g. /var/log/exaprotect/criston
2. Click **Next**.

Log Management log selected in Step 1

It means that the events will be collected via the TIBCO LogLogic® Open Log Management Platform.

1. Select the listening port and protocol.
2. Fill in the **Authorized IP address** field:
   a. If the selected host has no IP address defined in Step 1, enter an authorized IP address.
   b. If the selected host has one or several IP addresses defined in Step 1, the IP addresses are automatically displayed.
3. Click **Next**.

LOTUS DOMINO NOTES log source selected in Step1

It means that the events will be collected via the Lotus Domino mail routing server.

1. Select the Lotus Domino Notes server address.
2. Enter the access control information you configured during the installation of your Lotus Domino server.
3. Click **Next**.

Step 4 - Summary

Step 4 sums up all the parameters entered from the beginning of the wizard.

If you do not agree with the summary, then you can click on **Previous** to go back to the previous screen and modify the necessary data.

If you agree with the information displayed, then click **Confirm.**

> **Note:** Once you have clicked on Confirm, you cannot go backward but only restart the wizard completely.

Step 5 - Installing the Log Collector

Once Step 4 is confirmed, the three following icons are displayed in Step 5.

Table 5 Wizard Download Icons

Icons	Description
	Download Log Collector Installation file. This file is necessary when installing the Log Collector (see above). Otherwise, the icon is not available.
	Download Documentation. This icon allows you to download the documentation related to the log source you have previously selected.

To download the Log Collector installer, go to download.tibco.com or contact the support.

Once you are finished with your configuration, you can immediately configure another log source by clicking on **Restart.**

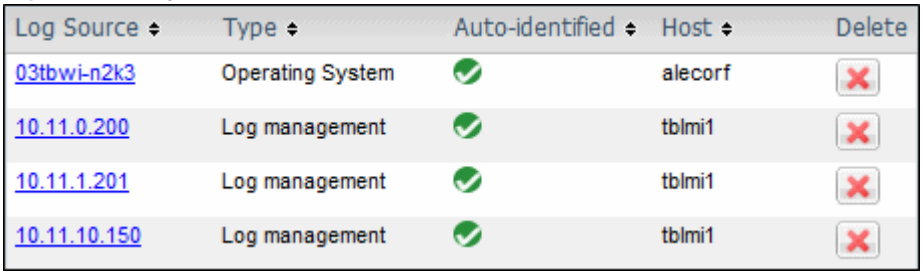
Adding a Log Source Manually: Log Collection

Log Sources

A log source is a product that generates log entries collected by a Log Collector.

To display the list of log sources, go to **Log Management > Log collection > Log sources**.

Figure 15 Log Sources



Viewing the log source characteristics

1. Click on the name of a log source. The **Description** screen is displayed. However, you cannot modify the log source in this screen, it is for information only.
2. Click on **Back** to go away from this screen.

If the log source is a network or database scanner (as indicated in the **Type** column), then the asset database is updated when reporting a scan:

- a new host corresponding to the target host is inserted
- vulnerabilities are automatically filled in the asset database

- when an alert generated by a scanner is acknowledged as **False Positive**, this vulnerability will automatically be transferred from the Vulnerability list to the False Positive list. Please refer to the Effective Vulnerabilities section for more information about vulnerabilities.

Deleting a Log Source

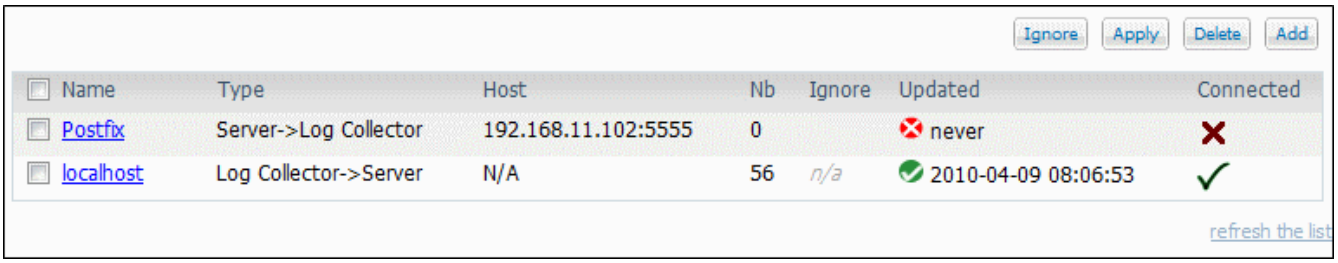
1. Click on the **Delete** icon.
2. Click **OK** in the pop-up window asking you to confirm the deletion.

> **Note:** If the log source is connected to a log collector, you will not be able to delete it. You will have to go to the **Log Collectors** screen.

Log Collectors

To display the **Log Collectors** pane, go to **Log Management > Log Collection > Log Collectors**.

Figure 16 Log Collectors Pane (Administrator or Super-Administrator View)



Creating a New Log Collector

> **Note:** Make sure you have created the host where your Log Collector will be installed. Otherwise, you will not be able to choose a host and then create your new Log Collector. Please refer to chapter Host to know how to add a new host.

To create a new Log Collector, perform the following steps:

1. Click on **Add**. The **Log Collector Creation** pane is displayed.
2. First choose the **type** of connection between server and Log Collector. If possible, use **server->**Log Collector as this will enable the SMP to detect the unavailability of the Log Collector more readily.
   a. You may have to use Log Collector**-> server,** for example, if there is a firewall between the two which prevents connections to the Log Collector, e.g., when relaying alerts.
   b. **Server->server** is used for connections between SMPs, e.g., when relaying alerts. When you add or edit a Log Collector, you can add or delete the associated log collector.
3. Then configure the connection type using the information provided below.

Server-to-Log Collector Connection

1. Select **Server-to-**Log Collector communication mode.

2. Enter a unique name. Typically this is the hostname where the Log Collector software is installed.

a. Allowed characters: A to Z, digits, underscore and dash.

b. Forbidden characters: space or any other characters.

3. 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.

4. Enter the **Port** number to establish the connection to the Log Collector.

5. Tick the **Advanced parameters** checkbox to set advanced parameters.

6. Enter the maximum events per second that the Log Collector is allowed to send to the SMP.

7. Select the **Compress Event Stream** checkbox to enable compression of the traffic between the Log Collector and the server.

8. Enter 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.

9. Enter the number of times an alert will be repeated when you receive a line such as: "last message repeated 120 times".

10. Modify the information of the spooler in the **Spooler Configuration** section

> **Note:** 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.

11. Tick **One spool per severity** to have one queue per alert severity.

12. Tick **Spool event with info severity** to specify whether informational events are spooled or not.

13. Enter the maximum number of files to write before pausing the collection of events in the **Num. Files**.

14. Enter a number corresponding to how large each file can grow to before a new one is created in the **File size (MB)** field.

15. If messages are received via Syslog UDP, define how large the socket buffer must (default size is 128) in the **Socket Buffer Size (Ko)**.

16. If messages are received via Syslog UDP, define a packet must be (default size is 8) in the **UDP Max Packet Size**.

Log Collector-to-Server Connection

1. Refer to the "Server-to-Log Collector Connection" procedure. for a description of the various parameters.

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

Server-to-Server Connection

1. Refer to the "Server-to-Log Collector Connection" sub-section to get a description of the various parameters.

2. Enter a name in the **Remote instance name** to forward alerts to a remote SMP, since an SMP may have multiple instances.

3. Enter a name or IP address in the **Use alternate server IP/name.** This parameter is required when the Log Collector cannot connect directly to the server, e.g., in a network containing an asymmetrical NAT definition.

Editing a Log Collector

1. To edit a Log Collector, click on its name in the **Log Collectors** list. You can then view the collected log sources. Collected log sources are used to assign a confset to a Log Collector.

2. Click on the log source name if you want to change the configuration settings (confset) used by the Log Collector.

Adding a Log Source

1. To add a new log source, click on **Add** in the list of collected log sources.

2. Select the **Confset** from the drop-down list.

If you select a default confset (e.g. `exa_Postfix`), then the newly created confset's name will be displayed in the following format:
`LogSourceName_exa_ConfsetName`.

E.g. If the log source is called `localhost` and the selected confset is `exa_Postfix`, then the confset will be called `localhost_exa_Postfix`.

3. Enter the name of the log source using alphanumeric characters, hyphen [-] and underscores [_]. The first character must be alphanumeric. Once entered, you cannot change the name of an Analyzer ID.

4. Select the log source's 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.

5. Use the **Type** pull-down menu to select the icon type that will be used to represent the log source in the GUI.

6. Check the **Active** box to indicate whether the log source should be collected or not.

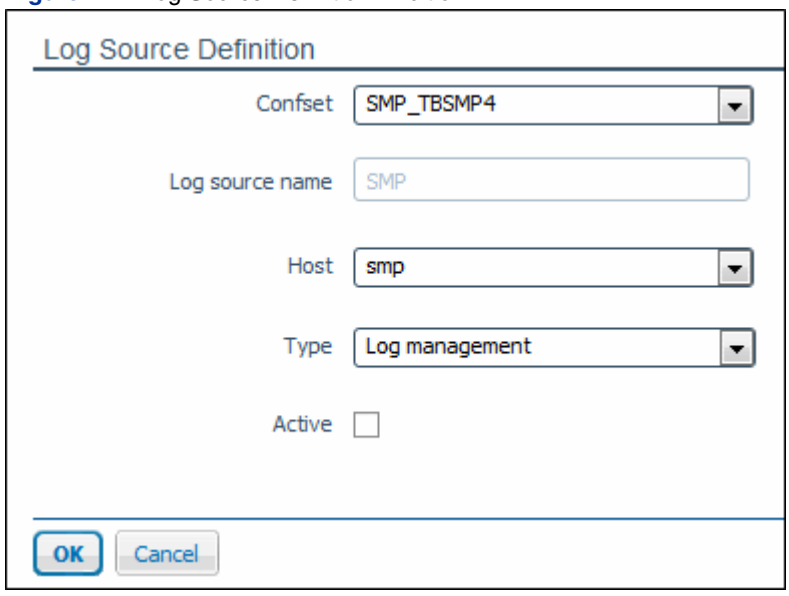
7. Click **OK** to save your changes, or click **Cancel** to return to the previous screen without saving your changes.

Editing a Log Source

To edit the individual log sources, click on the corresponding Log Collector name. The log sources on this Log Collector are displayed, along with the confset being used.

1. To change which configuration settings (confset) is used by the log source, click the **log source's name**.

Figure 17 Log Source Definition - Edition



a. Select the confset from the **Confset** drop-down list.

b. The **log source's name** is displayed for your reference - you can change the other settings for the selected supported product.

c. As defined in the asset database, the **host** is used to add business intelligence to the correlation performed with the specified confset. If no corresponding entry exists in the asset database, select **default host**.

d. The **Type** drop-down list allows you to select the icon that will be used to represent the supported product in the GUI and also to remove non-applicable GUI options relating to this supported product.

e. Check the **Active** box to indicate that the log source is collected or not.

2. Click the **Confset** name. This is a shortcut to the confset edit screen (see "Advanced Log Collection: Confset") where you can specify which converters are included in the confset.

Enabling/Disabling a Log Source

These action buttons allow you to enable or disable a Log Collector's log source that was previously enabled/disabled. Disabling a Log Collector's log source is useful if you need to do something else and then avoiding wasting machine performance.

1. Click on a log source checkbox.

2. Click on **Disable** or **Enable**.

Deleting a Log Source

1. Click on a log source checkbox.

2. Click on **Delete**.

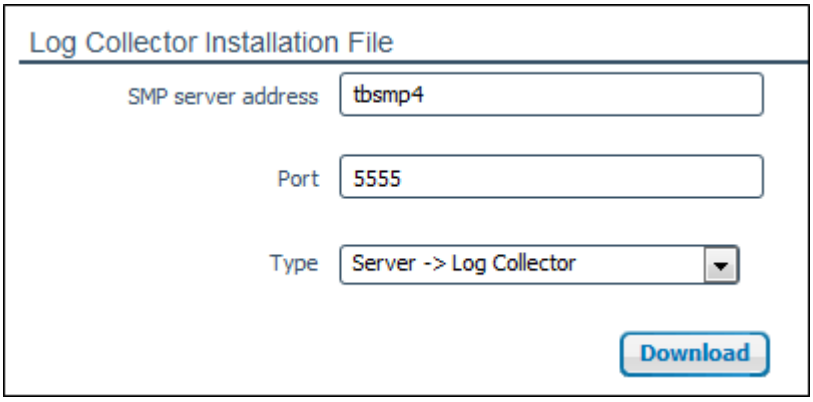
Download the Log Collector Installation File

The Log Collector Installer 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**.

Downloading Log Collector Installation File

Figure 18 Log Collector Installation File



1. Enter the SMP Server Address. Alternatively you can enter the IP address of the SMP server.

2. Enter the Port number (in this case 5555).

3. Choose a communication type from the drop-down list, either:

- Server > Log Collector
- Log Collector > Server
- Server > Server

4. When you have finished entering the Log Collector Configuration information, click **Download**. This displays the **File Download** dialog box.

5. Click **Save** to save this file to the disk and transfer it to the machine where the Log Collector will be installed. This file is necessary to finalize the configuration of the Log Collector. The installation of the Log Collector will prompt for the file location.

6. Download SEM Log Collector installer at download.tibco.com or contact the support.

Get the List of Supported Products

The **Supported Products** list page displays the devices being monitored by the SMP. This page is for information purpose only.

To display the Supported Products pane, go to **Log Management > Log Collection > Supported Products.**

Figure 19 Supported Products

Name	Vendor	Type	Supported via LogLogic Log Management Appliance	"Working with" guide
Activescout	ForeScout	Intrusion Detection System (IDS) / Intrusion Prevention System (IPS)		
Activpack v4	ActivIdentity	Authentication server		
Activpack v6.3	ActivIdentity	Authentication server		
Activpack v6.5	ActivIdentity	Authentication server		
Aix	IBM	Operating System	✓	
Alteon Web Switch	Nortel	Network device		
Apache	Apache	Web server	✓	

- Click on the **PDF** icon to download the configuration documentation related to this product.

Advanced Log Collection: Confset

The confset is a group of configuration settings. The confset consists of a group of converters and properties, such as what to collect - events and/or raw logs.

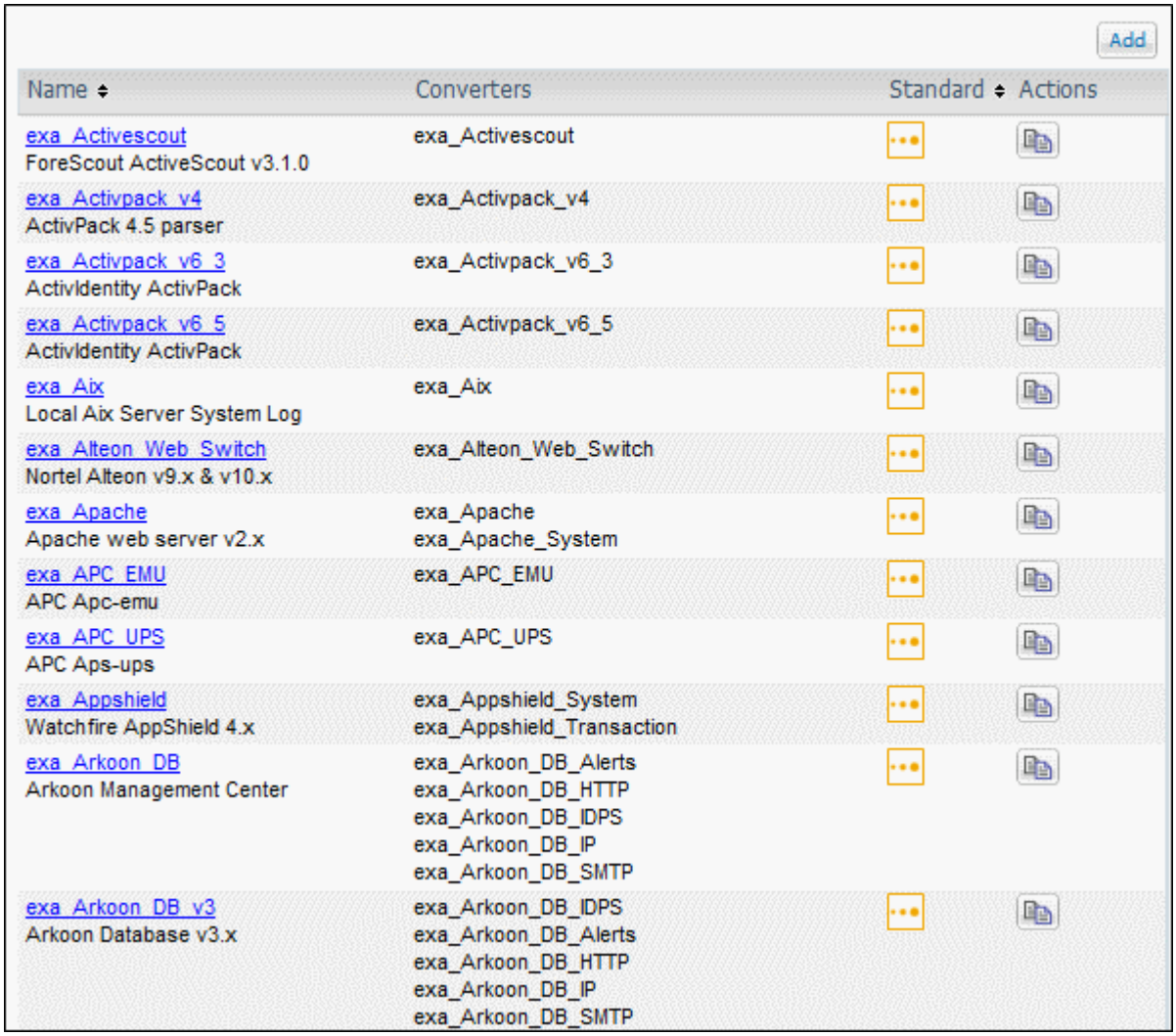
There are several pre-configured confsets supplied, but you can also create your own. The pre-configured or standard confsets cannot be modified.

> **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).

Create/Edit a confset

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

Figure 20 Confset View

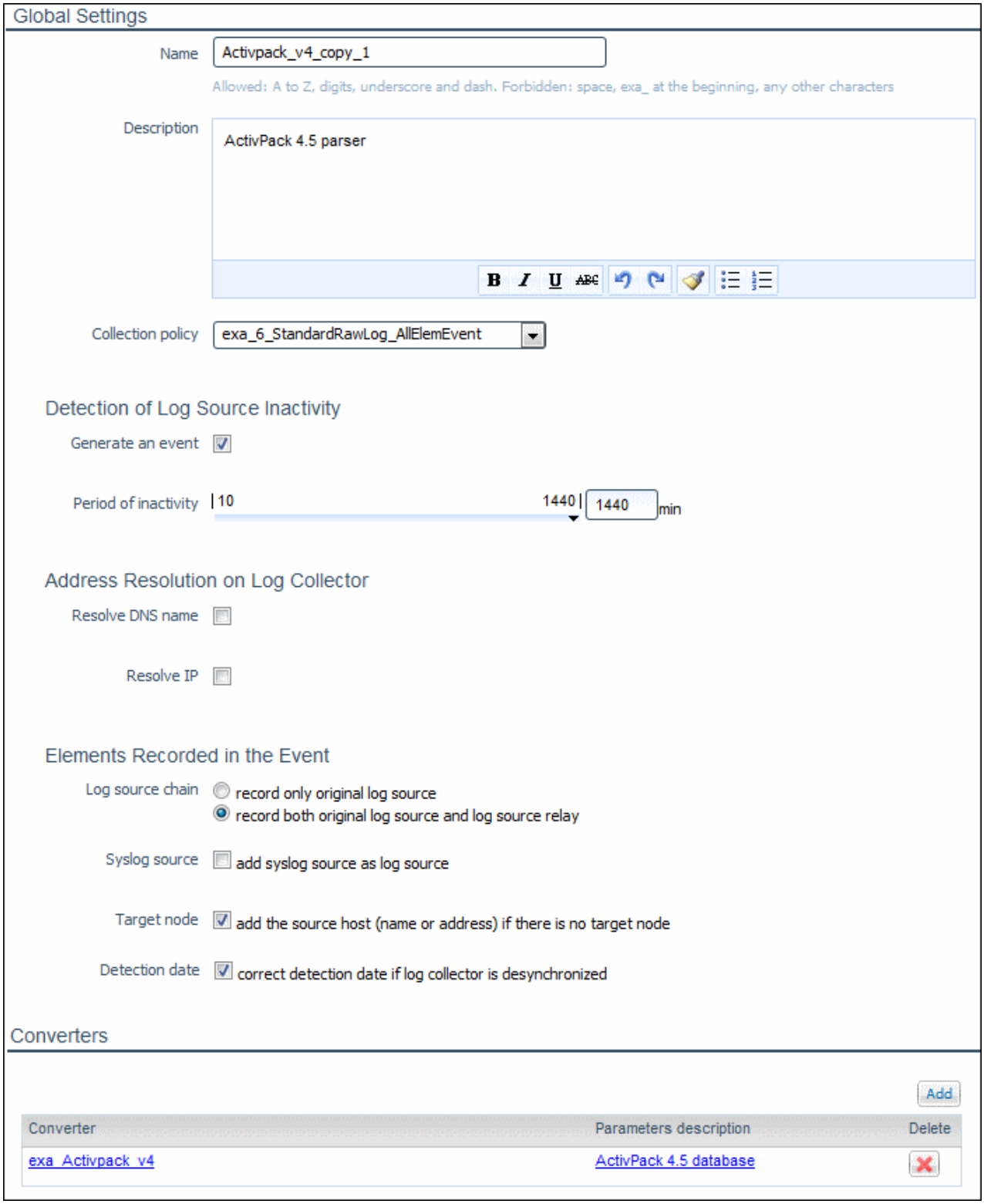


To create a confset, you have two possibilities:

- either add a new blank confset by clicking on the **Add** button
- or click on the **Copy** button and then on the name of the confset copy to work on a working copy of a default confset as default confsets cannot be modified.

The following screen is displayed.

Figure 21 Confset Creation



The procedure is the same for both methods:

1. Enter a unique name and description of the confset:
    a. Allowed characters: A to Z, digits, underscore and dash.
    b. Forbidden characters: space, the string **exa_** at the beginning, any other characters.

2. Select a collection policy to determine which events are sent from the Log Collector to the SMP. You cannot choose it if its filter name contains the string "copy".

> **Note:** By default, if an event is NOT handled by a collection policy, this event will be automatically retrieved. It also concerns raw logs and events NOT skipped by rulesets. Indeed, the **skip** option in the ruleset file has priority over a collection policy.

Detection of Log Source Inactivity

1. Select the **Generate an event** checkbox if you want an event to be generated 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.

2. Define the period of inactivity (in minutes) from which the event is generated by moving the arrow right or left.

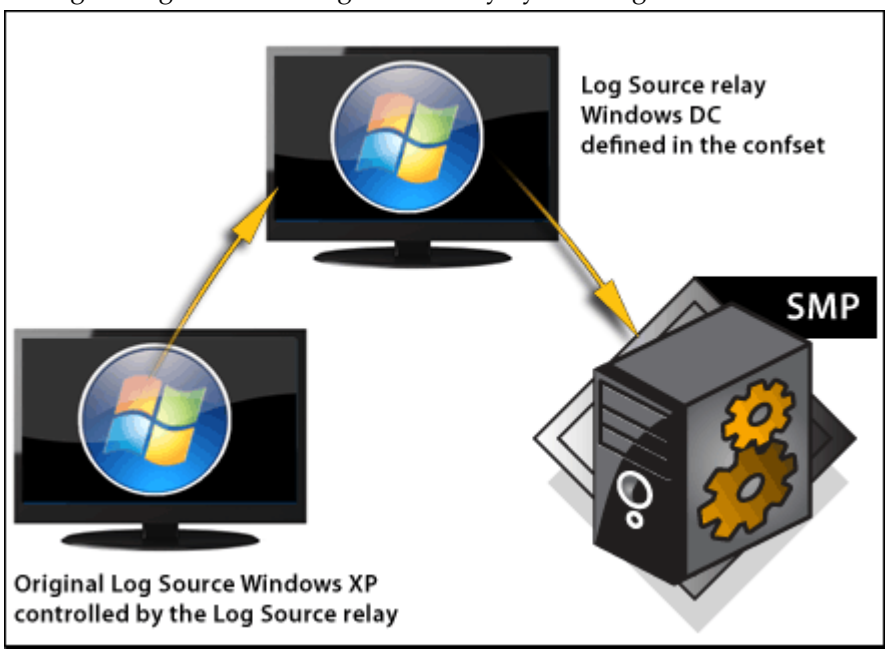
Address Resolution on Log Collector

1. Select the Resolve DNS name checkbox to ensure the event includes IP addresses that match any hostnames mentioned in the event. Enabling this option can significantly reduce the performance of the Log Collector.

2. Select the Resolve IP checkbox to ensure the event includes hostnames that match any IP addresses mentioned in the event. Enabling this option can significantly reduce the performance of the Log Collector.

Elements Recorded in the Event

1. In the event of a specific log source installation (see schema below), indicate 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 by selecting the relevant radio buttons.



2. Select the **add syslog source as log source** 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" log source using the hostname from the syslog events.

3. Indicate if you want to **add the log source host (name or address) if there is no target node** by selecting the relevant checkbox.

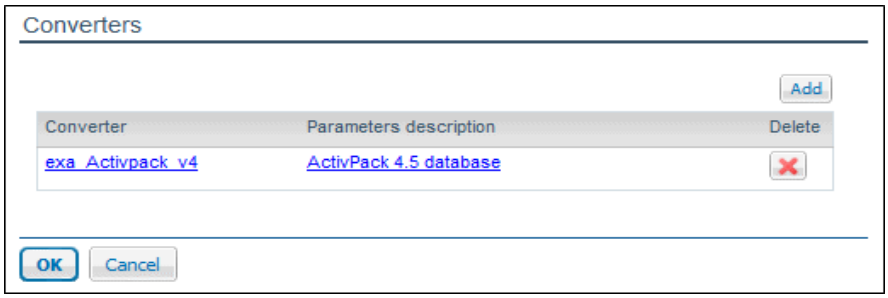
4. Select **Detection date** if the timezone of the machine on which the Log Collector is installed is not the same as the time server. An automatic reset of the events detection time can be applied by ticking this checkbox. The events will then match the time on the server.

> **Note:** 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

Now you must add a converter to the confset.

Figure 22 Adding a New Converter



1. Click **Add**.

2. Select the converters that will belong to this confset. Use the corresponding **Delete** button to remove the converter from the confset. This does not delete the converter altogether, it can still be used in other confsets.

3. Click **OK** to save changes and return to the previous screen, or click **Cancel** to ignore changes and return to the previous screen.

Example: Creating a Confset with Several Converters

You may want to create only one confset consisting of several converters. For example, this is useful if you want to limit the tree structure display to the main data in the **Alert Monitoring** screen.

Let us suppose you want to create a Confset called ***Linux_squid*** containing a ***Linux*** converter and a ***Squid*** converter.

- Go to **Log Management > Log Collection > Advanced > Confsets**.

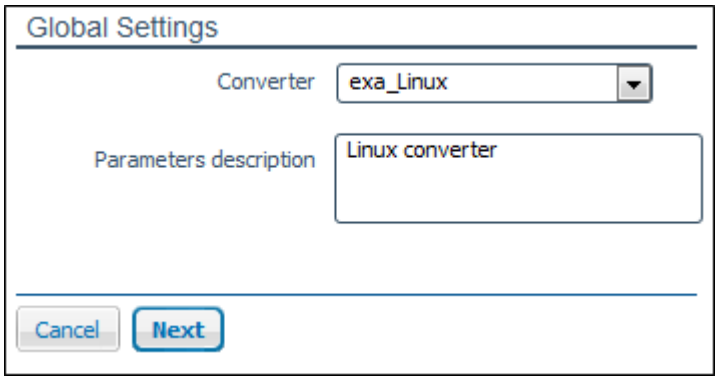
The list of available confsets is displayed.

1. Click on the **Add** button.

2. Enter the relevant parameters.

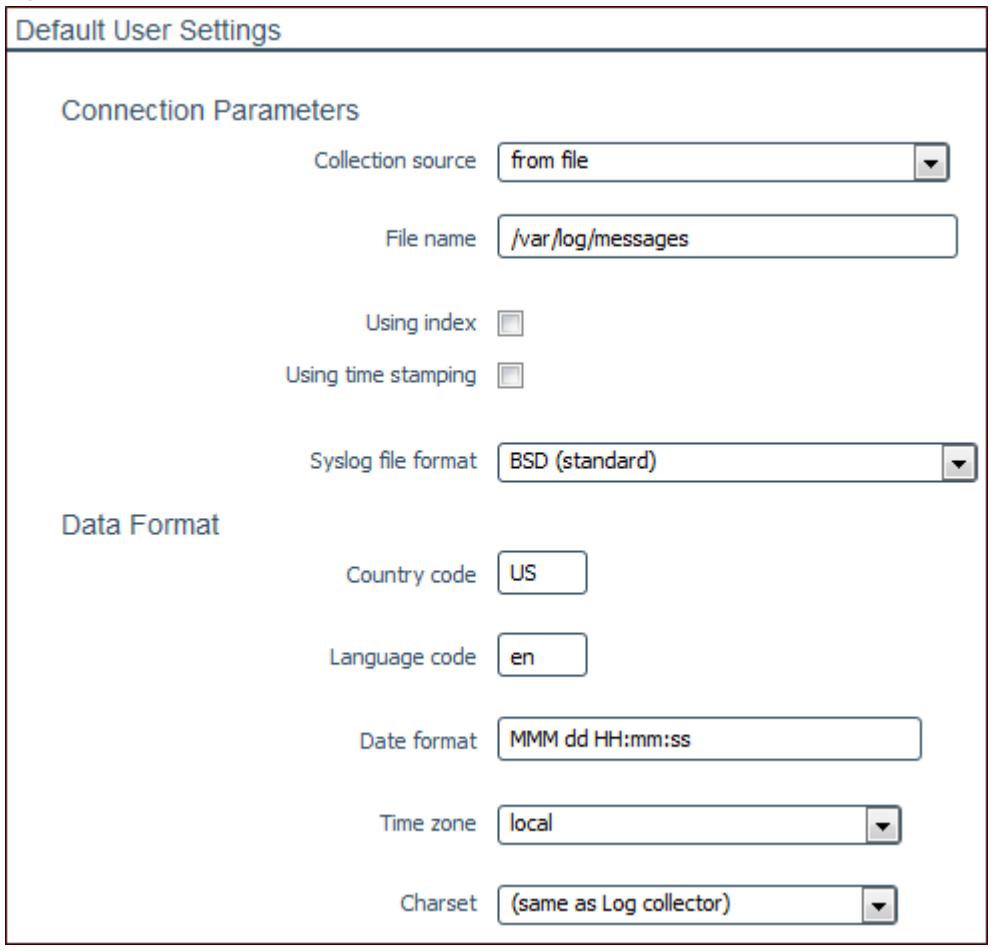
3. Click on the **Add** button to add the first converter. The following screen is displayed.

Figure 23 Converter



4. Select **Linux** in the drop-down list, enter a descriptive name and click **Next**. The following screen is displayed.

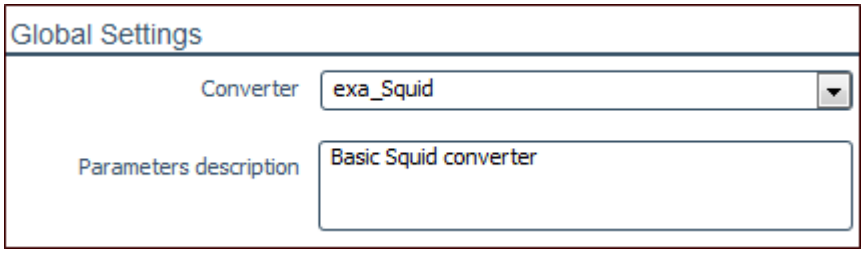
Figure 24 Confset Specific Properties for Converter Linux



5. Enter the relevant parameters and click **OK**.

6. Click the **Add** button to add the second converter and select **Squid** in the drop-down list.

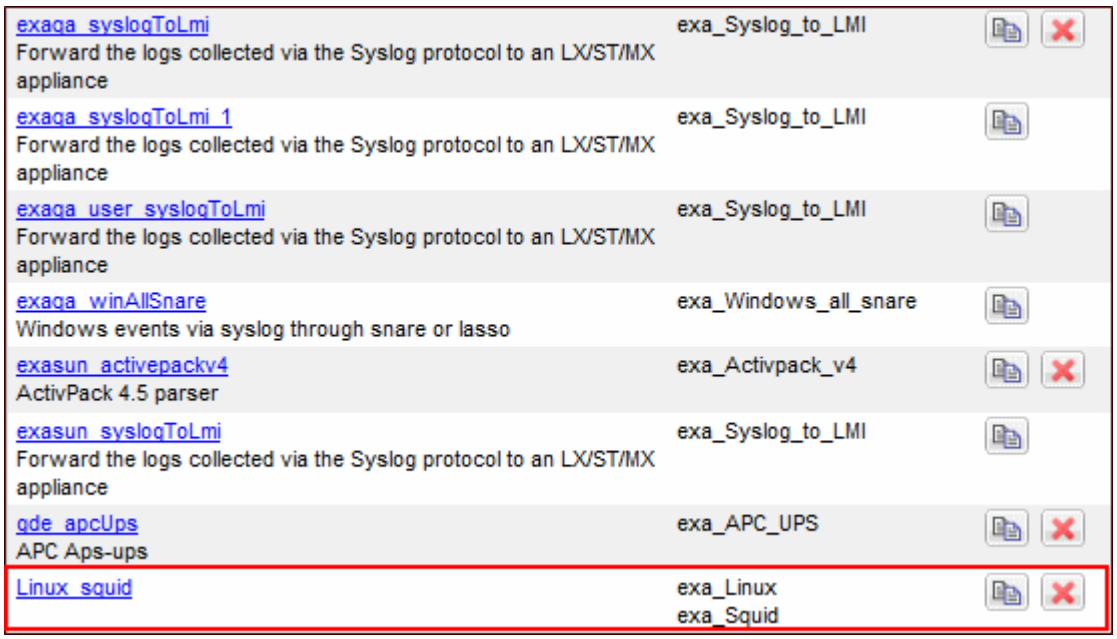
Figure 25 Converter



7. Repeat the same procedure for a third converter and so on until you have inserted all the converters you need.
Note that if you want to add several converters of the same type with different functions (for example Squid_Acces, Squid-Cache...), you have to enter each converter one by one.

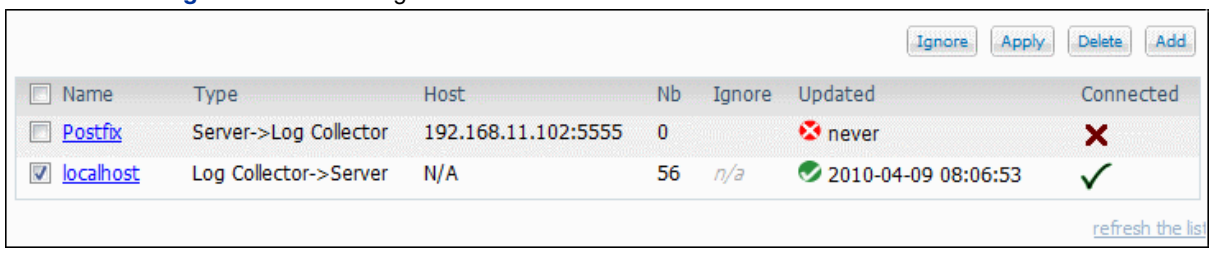
If you click on the **Confset** menu entry again, you can see that your new confset is now displayed.

Figure 26 List of Confsets



8. Go to **Log Management > Log Collection > Log Collectors**.

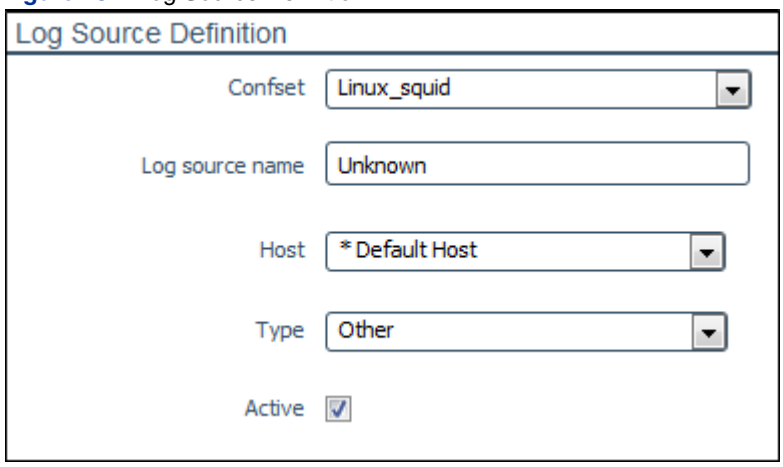
Figure 27 List of Log Collectors



9. Select the desired Log Collector and click on its name.

10. In the Collected Log Sources section, click on the **Add** button. The **Log Source Definition** pane is displayed.

Figure 28 Log Source Definition



11. Select the confset you created in the drop-down list.

12. Enter the **Log source name**, select the host and its type (UNIX).

13. Click on the **OK** buttons until you go back to the list of log collectors.

14. Select the corresponding Log Collector checkbox and click on the **Apply** button.

Your confset with multiple converters is created.

Advanced Log Collection: Converter

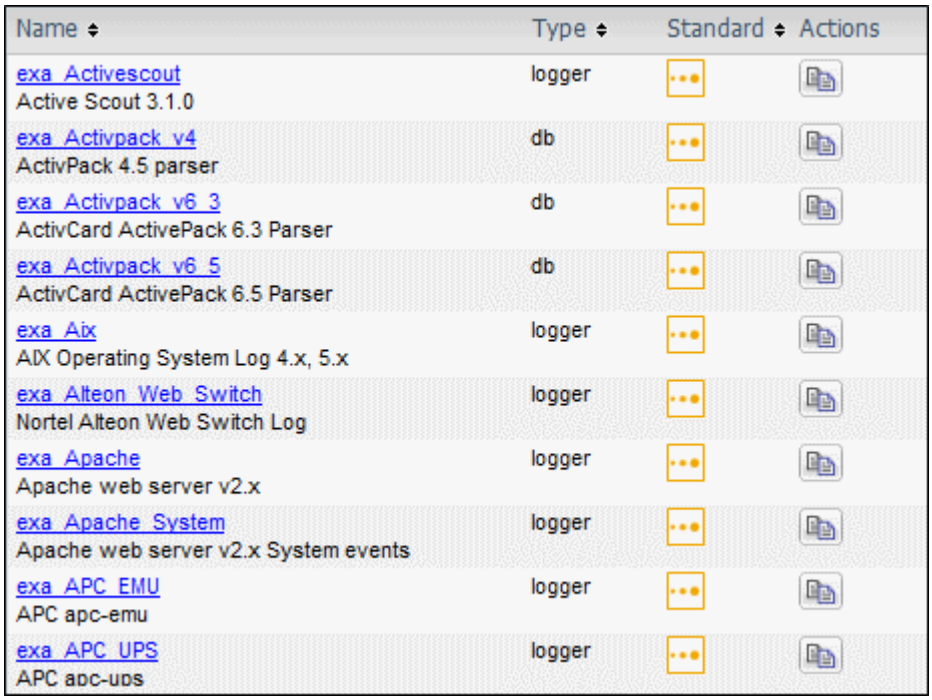
A converter is a set of rules used to convert a log entry into an event. It contains information about the connection between the Log Collector and the log source which allows collecting logs.

A converter can be of different types, either:

- Database
- Log
- Lotus Notes
- TIBCO LogLogic®
- Multiline
- OPSEC
- RDEP
- RSA
- Scanner
- Welf
- WMI

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

Figure 29 Converter Configuration Pane



To create a converter, you have two possibilities:

- either add a new blank converter by clicking on the **Add** button.
- or click on the **Copy** button and then on the name of the converter copy to work on a working copy of a default converter as default converters cannot be modified.

> **Caution:** You cannot add OPSEC, WELF and MULTILINE converters but only copy and edit them.

Then the procedure is the same for both methods.

1. Enter a unique name and description of the converter:
   - Allowed characters: A to Z, digits, underscore and dash.
   - Forbidden characters: space, the string **exa_** at the beginning, any other characters.
2. Select the type of the converter.

> **Caution:** If you try to edit a converter manually, i.e. edit in command line, once you have finished, you will have to do one of the following actions BEFORE editing the convertor again in the GUI, either:
> - restart the runtime
> or
> - refresh the list of converters by clicking on the Refresh link.
> Otherwise, the manual changes will not be taken into account.

Configure a Database Converter

1. Enter the various information for the database such as the:

- IP address of the host database.
- network port to connect to the database.
- name of the database.
- name of the database user with the required credentials.
- password for the database.
- appropriate option for your database type. For more information refer to the documentation of the JDBC driver in use.

> **Note:** You do not have to enter an address or port for the ODBC database converter type. An SQLServer database converter needs a JDBC option.

- time in seconds between SQL requests.

2. Enter the various information for the data format such as the:

- date format. See section Date Time Format Specification in the ***Appendix*** for further information.
- time zone used by the log source.

3. 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.

4. Select a map file from the list. The map file must match your product and product version number.
Note that if you want to modify the map file, you must do it manually via the SMP.

5. Add an SQL query to the list of queries that will be sent to the database to obtain the alerts.

Configure a Log Converter

1. 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)**.

2. Select a collection source. See description below.

If from file is selected:

1. Enter the full path and filename of the file you wish to convert. You can enter a character chain such as: c:\agent\agent.log.[id]-[date] provided you checked Using Index and Using Time Stamping boxes.

2. Select the relevant checkboxes:

- **Using index**: if you want to add an id number to the converter. If the file name includes an id such as `logFile-01.txt,logFile-02.txt` you must use these additional options. e.g. if the file name is **agent.log.[id]**, then you will get **agent.log.1**, then **agent.log.2**...etc. A maximum of 9 digits is allowed.
- **Using time stamping**: if you need to avoid the problem of a non constant file name which includes information relative to date/time. if the file name is **agent.log.[date]**, then you will get **agent.log.221107**, then a**gent.log.231107**...etc.

3. Enter the various information for the data format such as the:

- country code with upper-case and two-letter code as defined by ISO-639, e.g. US.
- language code with lower-case, two-letter code as defined by ISO-3166, e.g. en.
- date format. See section Date Time Format Specification in the ***Appendix*** for further information.
- time zone used by the log source.
- charset (UTF8, US-ASCII...). Note that modifying the charset leads to a file irrelevance.

4. Select the appropriate rule-set to use with this converter in the Rulesets list.

5. Select the appropriate MAP file.

If from network (syslog protocol RFC 3164) is selected:

1. Select the protocol to be used:

- **UDP**: specify that the syslog logs should be collected via UDP protocol. This is the default configuration.
  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**: specify that the syslog logs should be collected via TCP protocol.
  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.

2. Enter the port that the local Log Collector will use to retrieve the Syslog logs. 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.

3. Enter the IP address of the machine interface on which you want to collect syslog log in the **Listening IP address**. The default value is 0.0.0.0 which means that data will be collected from all the machine interfaces.

4. Select the type of message that must be collected by clicking on its corresponding **facility**.

5. Indicate which levels of **severity** will be reported by selecting one of the various 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

6. Enter a Java regular expression to indicate from which source machine the messages should be collected in the **Authorized IP addresses (regexp)** field. Refer to the "Java Regular Expressions" section in the **Appendix** to get the list of regular expressions to be used.

7. Enter the various information for the data format such as the:
   - country code with upper-case and two-letter code as defined by ISO-639, e.g. US.
   - language code with lower-case, two-letter code as defined by ISO-3166, e.g. en.
   - date format. See section Date Time Format Specification in the ***Appendix*** for further information.
   - time zone used by the log source.

8. Select the appropriate rule-set to use with this converter in the Rulesets list.

9. Select the appropriate MAP file.

Configure a WELF Converter

1. 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)**.

2. Select a collection source. See description below.

If from file is selected:

1. Enter the full path and filename of the file you wish to convert.

2. Select the relevant checkboxes:
   - **Using index**: if you want to add an id number to the converter. If the file name includes an id such as `logFile-01.txt,logFile-02.txt` you must use these additional options. e.g. if the file name is **agent.log.[id]**, then you will get **agent.log.1**, then a**gent.log.2**...etc. A maximum of 9 digits is allowed.
   - **Using time stamping**: if you need to avoid the problem of a non constant file name which includes information relative to date/time. if the file name is **agent.log.[date]**, then you will get **agent.log.221107**, then a**gent.log.231107**...etc.

3. Enter the various information for the data format such as the:

- separator used between fields.
- separator used between field name and value.
- empty field value as some products use a default value instead of being empty, e.g., n/a.
- header regex to parse the beginning of the line which is not WELF formatted.
- country code with upper-case and two-letter code as defined by ISO-639, e.g. US.
- language code with lower-case, two-letter code as defined by ISO-3166, e.g. en.
- date format. See section Date Time Format Specification in the ***Appendix*** for further information.
- time zone used by the log source.
- charset (UTF8, US-ASCII...). Note that modifying the charset leads to a file irrelevance.

4. Select the appropriate rule-set to use with this converter in the Rulesets list. Note that if you want to modify the map file, you must do it manually via the SMP.

5. Select the appropriate MAP file.

If from network (syslog protocol RFC 3164) is selected:

1. Select the protocol to be used:

- **UDP**: specify that the syslog logs should be collected via UDP protocol. This is the default configuration.
  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**: specify that the syslog logs should be collected via TCP protocol.
  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.

2. Enter the port that the local Log Collector will use to retrieve the Syslog logs. 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.

3. Enter the IP address of the machine interface on which you want to collect syslog log in the **Listening IP address**. The default value is 0.0.0.0 which means that data will be collected from all the machine interfaces.

4. Select the type of message that must be collected by clicking on its corresponding **facility**.

5. Indicate which levels of **severity** will be reported by selecting one of the various 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

6. Enter a Java regular expression to indicate from which source machine the messages should be collected in the **Authorized IP addresses (regexp)** field. Refer to the "Java Regular Expressions" section in the **Appendix** to get the list of regular expressions to be used.

7. Enter the various information for the data format such as the:

- separator used between fields.
- separator used between field name and value.
- empty field value as some products use a default value instead of being empty, e.g., n/a.
- header regex to parse the beginning of the line which is not WELF formatted.
- country code with upper-case and two-letter code as defined by ISO-639, e.g. US.
- language code with lower-case, two-letter code as defined by ISO-3166, e.g. en.
- date format. See section Date Time Format Specification in the ***Appendix*** for further information.
- time zone used by the log source.

8. Select the appropriate rule-set to use with this converter in the Rulesets list. Note that if you want to modify the map file, you must do it manually via the SMP.

9. Select the appropriate MAP file.

Configure a WMI Converter

1. Enter the address of the Windows host from which to obtain events.

2. Enter the administrator account login and password.
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.

3. Enter the Windows domain name, or if there is no domain name, the hostname (not address).

4. Indicate the delay in seconds between WMI requests.

5. Select the time zone used by the Windows log source.
If the log source has a **Windows 2008 or Vista Operating System**, then you MUST select **GMT** in the list, no matter the log source's location.

6. Select the set of user preference information related to the user's language, environment and/or cultural conventions.

Caution: 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) because Windows events are stored in English US language in that specific case.

7. Check the **Store Description** box to obtain the description of the Windows event.

8. Select whether you want to include or exclude the MS Windows journals. See the WMI Journal option.

9. 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.

10. Select the appropriate map file to use with this converter.

Configure a TIBCO LogLogic® Converter

1. Select the protocol to be used:

- **UDP**: specify that the syslog logs should be collected via UDP protocol. This is the default configuration.
  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**: specify that the syslog logs should be collected via TCP protocol.
  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.

2. Enter the port that the local Log Collector will use to retrieve the Syslog logs. 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.

3. Enter the IP address of the machine interface on which you want to collect syslog log in the **Listening IP address**. The default value is 0.0.0.0 which means that data will be collected from all the machine interfaces.

4. Enter a Java regular expression to indicate from which source machine the messages should be collected in the **Authorized IP addresses (regexp)** field. Refer to the Java Regular Expressions section in the Appendix to get the list of regular expressions to be used.

5. Select the time zone of the log source.

6. Click on the link below the screen to display the list of supported products by the TIBCO LogLogic® converter.

Note: Unlike the other syslog converters, it is not possible to select a collection source as it is always *from network*.

Configure a Lotus Notes Converter

1. Enter the Domino server address and port.

2. Enter the login and password configured to access the Domino server.

3. Enter the various information for the data format such as the:

   - separator used between fields.
   - separator used between field name and value.
   - empty field value as some products use a default value instead of being empty, e.g., n/a.
   - header regex to parse the beginning of the line which is not WELF formatted.
   - country code with upper-case and two-letter code as defined by ISO-639, e.g. US.
   - language code with lower-case, two-letter code as defined by ISO-3166, e.g. en.
   - date format. See section Date Time Format Specification in the ***Appendix*** for further information.
   - time zone used by the log source.

4. Select the appropriate **Welf map file** to use with this converter.

5. Click on the **Upload Notes jar** files, then select the two relevant jar files that you need to make Lotus Domino work.

6. Click **OK**.

Configure an OPSEC Converter

1. Enter the **config file** content:

   ```
   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
   ```

2. Enter the **p12 certificate** file 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.

3. Select the **time zone** used by the Checkpoint host.

4. Select the appropriate **opsec map file** to use with this converter.

Configure an RDEP Converter

1. Enter the IP address or name of the CISCO RDEP server from which you wish to obtain events.

2. Enter the network port required to connect to the CISCO REDEP server.

3. Enter the CISCO server account name with which to authenticate.

4. Enter the password of the CISCO server account.

5. Select the time zone used by the log source.

6. Select the appropriate map file.

Configure a SCANNER Converter

1. Enter the directory where the XML output will be stored.

2. Enter 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).

3. Enter the port used for the connection.

4. Enter the Login required for authenticating on the Qualys server.

5. Enter the Password required for authenticating on the Qualys server.

6. Enter the Interval between each connection made with the Qualys server to check if new scan reports must be analyzed in the **Period (min)** field.

7. Enter the HTTP proxy parameters, such as the:

- IP address required to connect to the proxy server.
- Port required to connect to the proxy server.
- User name required to connect to the proxy server.
- Password required to connect to the proxy server.

8. Enter the time zone used by the log source.

9. Enter 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.

10. Enter the appropriate map file to use with this configuration.

Configure a Multi-Line Converter

1. 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)**.

2. Select a collection source. See description below.

If from file is selected:

1. Enter the full path and filename of the file you wish to convert.

2. Select the relevant checkboxes:

- **Using index**: if you want to add an id number to the converter. If the file name includes an id such as logFile-01.txt,logFile-02.txt you must use these additional options. e.g. if the file name is **agent.log.[id]**, then you will get **agent.log.1**, then **agent.log.2**...etc (refer to Figure 68: "Log converter"). A maximum of 9 digits is allowed.
- **Using time stamping**: if you need to avoid the problem of a non constant file name which includes information relative to date/time. if the file name is **agent.log.[date]**, then you will get **agent.log.221107**, then **agent.log.231107**...etc (refer to Figure 68: "Log converter").

3. Enter the various information for the data format such as the:

- country code with upper-case and two-letter code as defined by ISO-639, e.g. US.
- language code with lower-case, two-letter code as defined by ISO-3166, e.g. en.
- date format. See section Date Time Format Specification in the ***Appendix*** for further information.
- time zone used by the log source.
- charset (UTF8, US-ASCII...). Note that modifying the charset leads to a file irrelevance.

4. Click the **Advanced Parameters** and enter:

- the maximum number of lines from partially completed events, that are held in memory, while waiting for the remaining expected lines.
- the maximum amount of time the partially completed events will be held in memory.

5. Select the product that produces the log files (e.g., Postfix) in the **Type** drop-down list.

If from network (syslog protocol RFC 3164) is selected:

1. Select the protocol to be used:

- **UDP**: specify that the syslog logs should be collected via UDP protocol. This is the default configuration.
  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**: specify that the syslog logs should be collected via TCP protocol.
  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.

2. Enter the port that the local Log Collector will use to retrieve the Syslog logs. 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.

3. Enter the IP address of the machine interface on which you want to collect syslog log in the **Listening IP address**. The default value is 0.0.0.0 which means that data will be collected from all the machine interfaces.

4. Select the type of message that must be collected by clicking on its corresponding **facility**.

5. Indicate which levels of **severity** will be reported by selecting one of the various 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

6. Enter a Java regular expression to indicate from which source machine the messages should be collected in the **Authorized IP addresses (regexp)** field. Refer to the "Java Regular Expressions" section in the **Appendix** to get the list of regular expressions to be used.

7. Enter the various information for the data format such as the:

- country code with upper-case and two-letter code as defined by ISO-639, e.g. US.
- language code with lower-case, two-letter code as defined by ISO-3166, e.g. en.
- date format. See section Date Time Format Specification in the ***Appendix*** for further information.
- time zone used by the log source.

8. Click the **Advanced Parameters** and enter:

- the maximum number of lines from partially completed events, that are held in memory, while waiting for the remaining expected lines.
- the maximum amount of time the partially completed events will be held in memory.

9. Select the product that produces the log files (e.g., Postfix) in the **Type** drop-down list.

> **Note:** The multiline converter uses lots of memory to store the data extracted from each line. Therefore, it is recommended to increase the default memory size (more than 200 Mbytes at least).

Configure an RSA Converter

1. Enter 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).

2. Enter the various information for the data format such as the:

- country code with upper-case and two-letter code as defined by ISO-639, e.g. US.
- language code with lower-case, two-letter code as defined by ISO-3166, e.g. en.
- date format. See section Date Time Format Specification in the ***Appendix*** for further information.
- time zone used by the log source.
- charset (UTF8, US-ASCII...). Note that modifying the charset leads to a file irrelevance.

3. Select the appropriate rule-set to use with this converter.

4. Select the appropriate MAP file.

Conversion Rulesets

A conversion rule-set is a file in which rules are set to allow the automatic conversion of log entries into events. Rules are used by log and RSA converters. Several standard rulesets are provided. However, they are not editable, you must copy them to modify the content.

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

Figure 30 Conversion Rule-Set

Creating a customizable rule

1. Click on the **Add** button.
2. Enter a unique name and description of the ruleset:
   - Allowed characters: A to Z, digits, underscore and dash.
   - Forbidden characters: space, the string **exa_** at the beginning, any other characters.
3. Click on the **OK** button.

The rule file is created and displayed in the list. You can also modify it by clicking on its name or delete it.

Note: The skip option in the rule-set file has priority over a collection policy.

Chapter 4 - Preparing the 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.

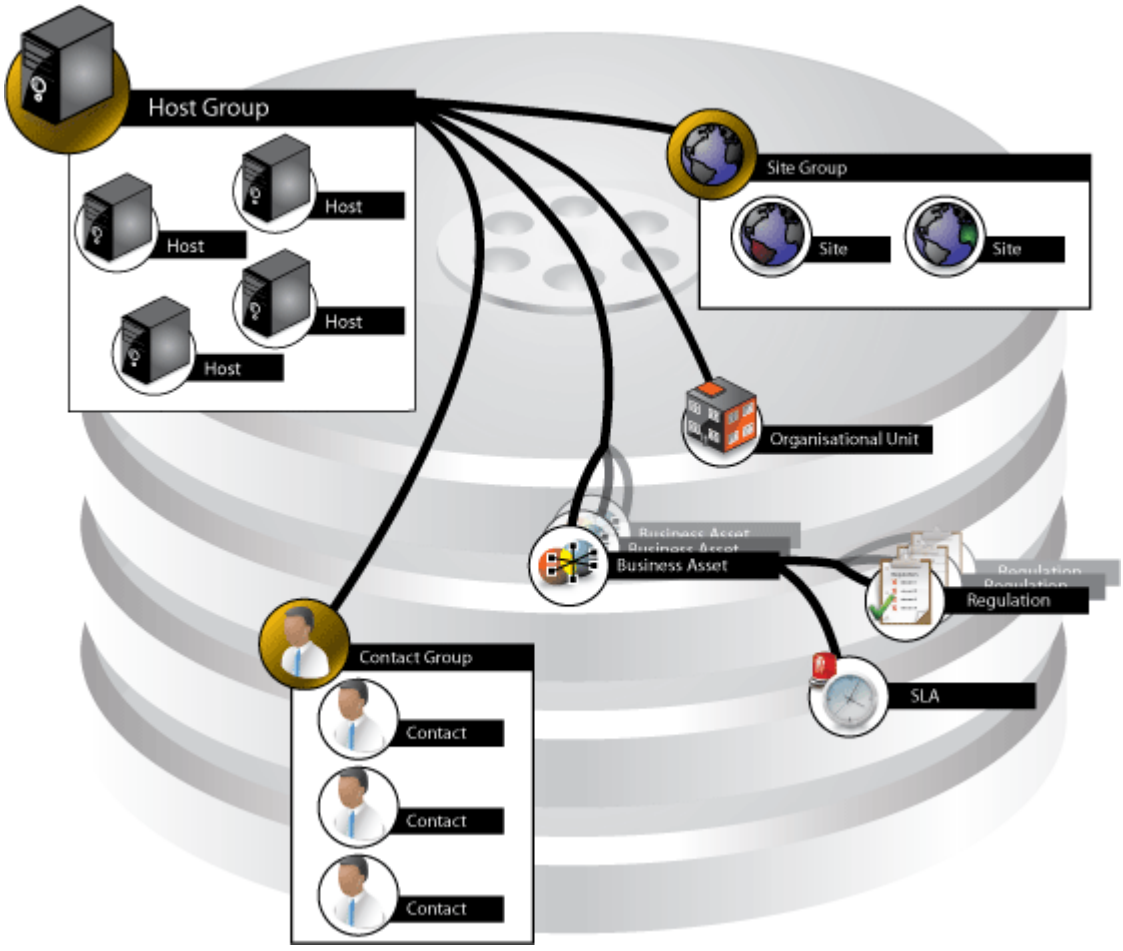
This chapter gives a description of the Asset Database and explains how to enter information about your:

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

> **Note:** Each time the asset database is updated, the engines (Configuration > SMP Monitoring > Engine Management tab) must be synchronized for the modification to be taken into account.

Description

The asset database can be represented as follows:



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

Table 6 Description of the Asset Database

Icon	Description	Example
	A **host group** is the only entity linked to all the other entities in the asset database. It is a kind of cluster composed of hosts with same functions. Host groups support business assets. The default host group is either filled by auto-discovery scanners or automatically filled with a new default host.	Internet Firewalls, Administration Stations, Security Management Servers, Configuration Management Servers, Financial Servers…
	A **host** is contained in a host group. A host is a single hardware system. Multiple addresses, nodes, or applications can be assigned to a single host. The default host is used during the installation of a new Log Collector.	Server...
	The host group is located in a **site** that usually corresponds to a country or a town. One or several contacts work in a site.	Paris, New York...

Table 6 Description of the Asset Database

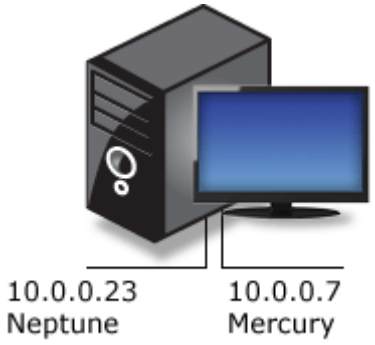
Icon	Description	Example
	The host group is part of an **organizational unit**. An organizational unit is composed of host groups coming from the same organization branch.	Accountancy
	The host group belongs to **business assets**. A business asset is a corporate service supported by components (host groups). Business assets may have to comply with specific regulations. Detailed views of alerts and events show impacted business assets.	E-business Web Site, Electronic Mails, WAN Access…
	**Contact groups** are allocated to host groups to define ownerships and responsibilities.	Sales, Network administrators…
	Contacts are grouped into **contact groups**. Ownership is then defined through contact groups.	Administrator, analyst…
	The **Service Level Agreement (SLA)** is an 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 business asset, the current security level and the work hours of the security analyst.	High, Low or Standard
	A **regulation** can be applied on a specific business asset in order to gain a maximum level of security in your business IT infrastructure.	SOX, PCI-DSS...

Host

The host entry is used to provide further information that will be useful for enriching events.

For example, if a unique host is connected via two network interfaces with different names and IP addresses, events coming from these addresses will be treated separately.

Figure 31 Example of a unique host with two hostnames

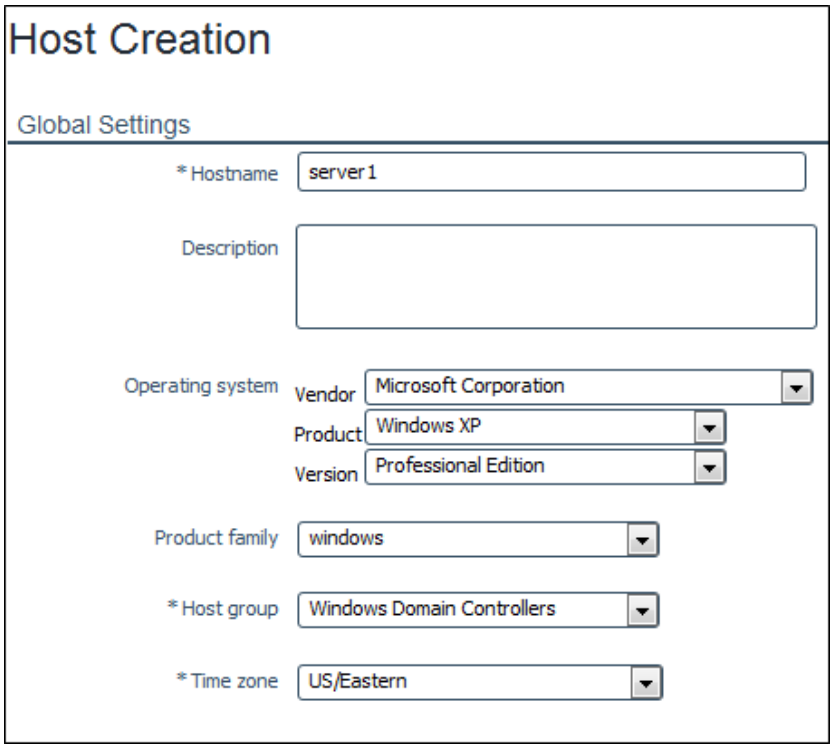


However, if you specified in the asset database that there is one unique host which is connected to two network interfaces with different host names and IP addresses, events will be treated altogether.

Adding a New Host

1. Click **Add** to add a new host.

Figure 32 Adding a New Host



2. Enter a name and description. Each host in the asset database must have a unique name.

The hostname must be a set of alphanumerical characters in lower case, beginning with a letter. Authorized characters are a-z, 0-9.

3. Select the **vendor**, **product**, and **version** of the operating system so that the SMP can report vulnerabilities that may affect the host. Note that you must either select **all** the OS information or **none of them**.

4. In the **Product family** drop-down list, select the type of operating system, such as Windows or UNIX, which can be used to select hosts when producing reports.

5. Select a host group in the **Host Group** drop-down list.
Each host MUST belong to a host group. By default, the host automatically belongs to the Default Host Group.

6. Select the **time zone** where the host is located.

7. Click **OK** to save the host with just these attributes and to return to the list of hosts.

8. In the list of hosts, click on the entry you have just created. New fields are added in the screen.

9. Enter the host address(es) - including IP4 and IP6 addresses - in the **Addresses** pane then click **Add**. This enables events attributed to IP addresses to be correlated when a host has multiple addresses.

10. Enter the host name(s) in the **Nodes** pane then click **Add**. 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.

11. In the **Applications** pane, select the Vendor, Product and Version details of applications installed on the host then click **Add**. This information is used to report possible vulnerabilities the host may have.

12. Click **OK** to save your changes and return to the previous screen.

Editing a Host

1. Click the name of the host to edit it.

2. Follow the instructions provided in sub-section Adding a New Host to configure the host.

> **Note:** The default host cannot be edited.

Host Group

For ease of management, groups of hosts can be created. A host can only belong to one host group.

Adding a New Host Group

1. Click **Add** to add a new host group.

2. Enter a **name** and **description**. Each host group must have a unique name.

3. Select the site in which the hosts are located from the **Site** drop-down list. The site is created on the sites screen (see sub-section Adding a New Site).

4. Select the organizational unit in which the hosts are located from the **Organizational Unit** drop-down list (see sub-section Organizational Units (OU)).

5. In the **Hosts** pane, click on the host you want to add to the host group.

- If you want to select all the hosts, click on **Copy all**.
- If you want to remove one of the hosts from the **Selected hosts** list, click on its name.
- If you want to remove all the hosts from the **Selected hosts** list, click on **Remove all**.

6. In the **Contact Groups** pane, click on the contact group you want to add to the hosts. 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. The procedure is the same as for the **Hosts** pane.

7. In the **Business Assets** pane, click on the business asset to apply to the new host group. Business Assets specify which SLAs and Criticality apply to the alerts relating to the hosts.

8. Click either **OK** to save the changes and return to the previous screen, or **Cancel** to return to the previous screen without saving your changes.

> **Note:** The default host group cannot be deleted.

Editing a Host Group

1. Click the name of the host group to edit it.

2. Follow the instructions provided in sub-section Adding a New Host Group to configure the host group.

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.

For example, you could separate critical servers from test servers, by allocating the former to a business asset called “Critical servers,” and the latter to a business asset named “Test servers”.

Adding a Business Asset

1. Click **Add** to add a new business asset.

2. Enter a **name** and a **description** for the new business asset.

3. Select the criticality level and specific **SLA** from the drop down lists.

4. Select the host group that belongs to this business asset by clicking on the host group name. The host group displayed in the **Selected host groups** list will be taken into account.

- If you want to select all the host groups, click on **Copy all**.
- If you want to remove one of the host group from the **Selected host groups** list, click on its name.
- If you want to remove all the host groups from the **Selected host groups** list, click on **Remove all**.

5. Select the regulation to apply to the business asset. The procedure is the same as for selecting host groups.

- If you want to select all the regulations, click on **Copy all**.
- If you want to remove one of the regulation from the **Selected Regulations** list, click on its name.
- If you want to remove all the regulations from the **Selected Regulations** list, click on **Remove all**.

6. Click **OK** to save the new business asset group or **Cancel** to close without making any changes.

Editing a Business Asset

1. Click the name of the business asset to edit it.

2. Follow the instructions provided in "Adding a Business Asset" to configure the business asset.

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 emails. They are used to define the area 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”.

Adding a New Site

1. To display the **Sites** screen, go to **Configuration > Asset Database > Sites**.

2. To add a new site, click **Add.**

3. Enter a **name** (e.g. London, Paris, Lyon, Cambridge) and **description**.

4. From the **Site Group** drop-down list, select which Site Group this site belongs to.

5. Select the **time zone** corresponding to the site location

6. In the **Host Groups** pane, click on the host group that must be present in the site. See section Adding a New Host Group for further information about host groups.

- If you want to select all the host groups, click on **Copy all**.
- If you want to remove one of the host group from the **Selected host groups** list, click on its name.
- If you want to remove all the host groups from the **Selected host groups** list, click on **Remove all**.

7. In the **Contacts** pane, click on the contact that should be notified when alerts have notification actions, such as sending an email. See section Contacts for further information about contacts. Note that you cannot select the contact group.

8. Click **OK** to save the changes and return to the list of sites or click **Cancel** to ignore changes and return to the previous screen.

Note: The default site cannot be deleted.

Editing a Site

1. Click the name of the site to edit it.

2. Follow the instructions provided in sub-section Adding a New Site to configure the site.

Site Groups

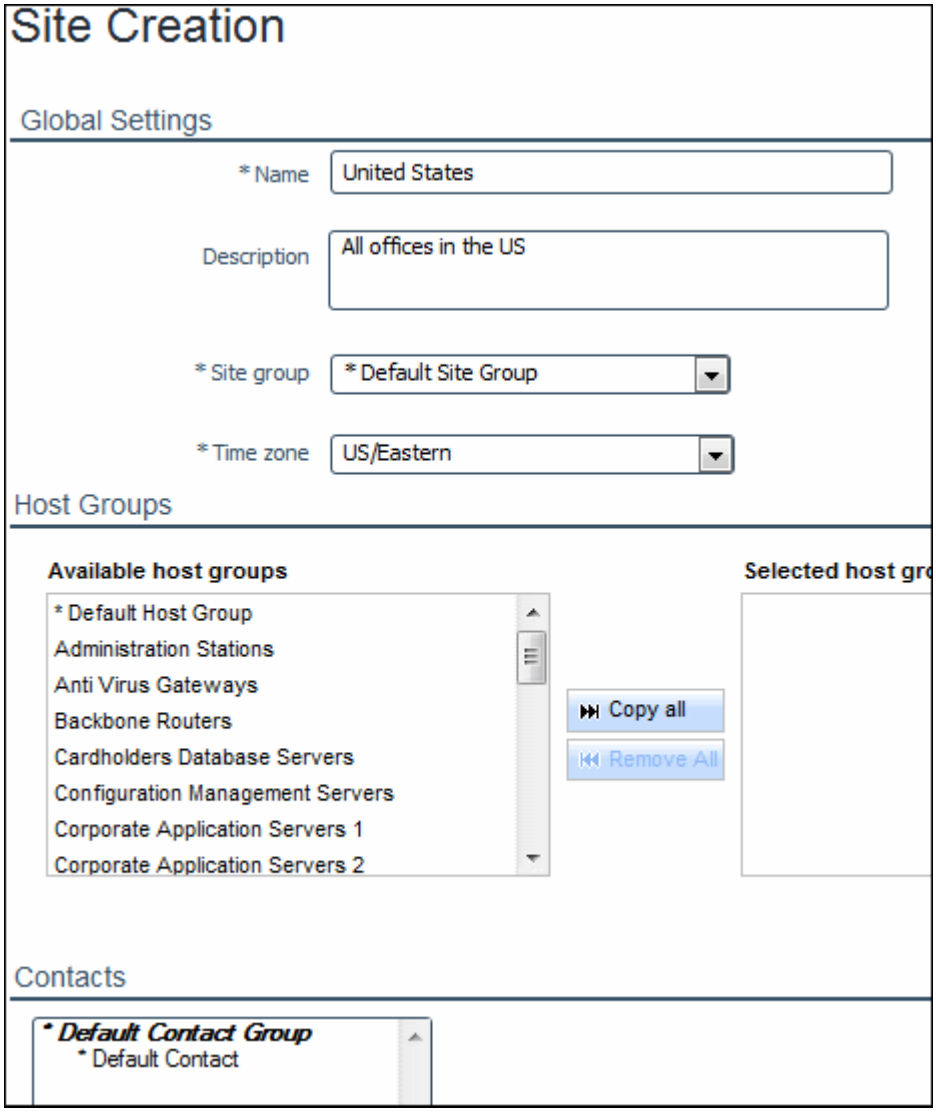
A **Site Group** contains several sites. For example, the site group “France” contains the sites Lyon and Paris, and the site group “United Kingdom” contains the sites “Cambridge” and “London”. This allows you to better organize your log source.

Adding a New Site Group

1. Go to **Configuration > Asset Database > Site Groups** to display the **Site Groups** screen.

2. To add a new site, click **Add**.

Figure 33 Add a New Site Group



3. Enter a **name** (e.g. France, United Kingdom) and **description**.

4. In the **Sites** pane, click on the site you want to add to the group.

- If you want to select all the sites, click on **Copy all**.
- If you want to remove one of the site from the **Selected sites** list, click on its name.
- If you want to remove all the sites from the **Selected sites** list, click on **Remove all**.

5. Click **OK** to save the changes and return to the list of site groups, or click **Cancel** to ignore changes and return to the previous screen.

Note: The default site group cannot be deleted.

Editing a Site Group

1. Click the name of the site group to edit it.

2. Follow the instructions provided in sub-section Adding a New Site Group to configure the site group.

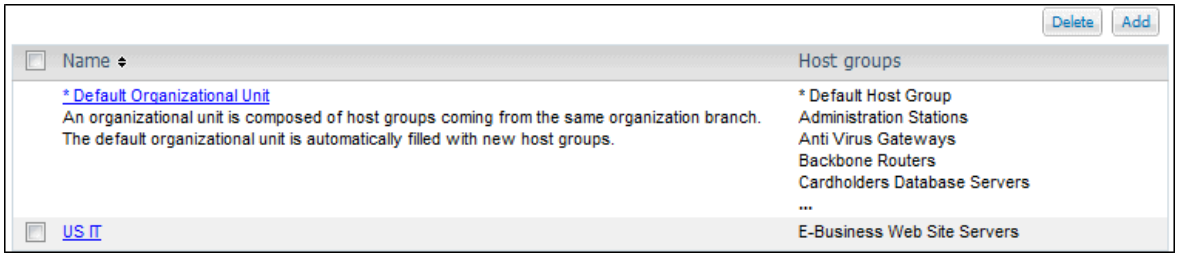
Organizational Units (OU)

Host groups can be grouped according to the **Organizational Unit** (OU) they belong to. Typically this is based on responsibility e.g. all host groups that the UK IT department are responsible for would be assigned to the OU "UK IT". The OU is used in reports such as number of alerts (by priority) for each OU.

Adding an Organizational Unit

1. To display the OU list, go to **Configuration > Asset Database > Organizational units**.

Figure 34 List of Organizational Units



2. Click **Add** to add an OU.

3. Enter a **name** and **description**. Each OU must have a unique name. The OU can be renamed.

4. Click on the host group you want to add to the OU.

- If you want to select all the host groups, click on **Copy all**.
- If you want to remove one of the host group from the **Selected host groups** list, click on its name.
- If you want to remove all the host groups from the **Selected host groups** list, click on **Remove all**.

5. Click **OK** to save the changes and return to the list of OUs.

Note: The default OU cannot be deleted.

Editing an Organizational Unit

1. Click the name of the Organizational Unit to edit it.

2. Follow the instructions provided in sub-section Organizational Units (OU) to configure the Organizational Unit.

Contacts

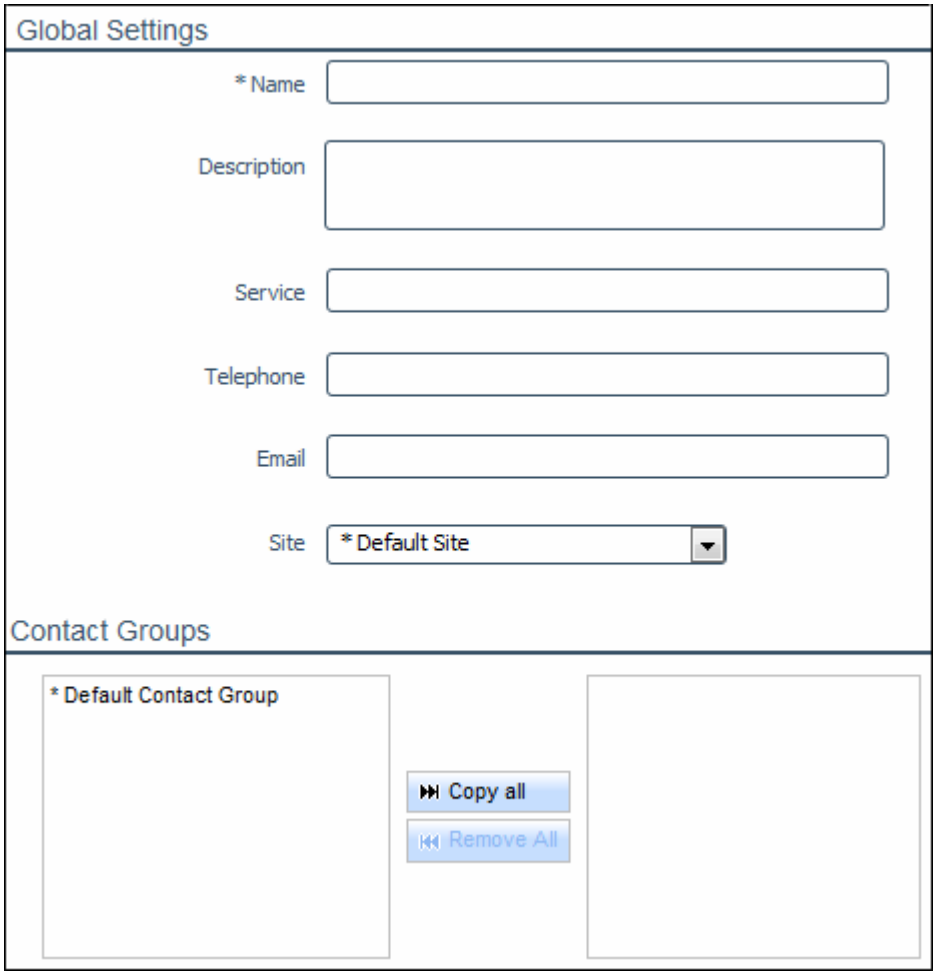
For each contact, the notification methods are detailed - e.g. the email address and phone number can be specified. Contacts are then notified when alerts occur.

Adding a New Contact

1. To add a contact, go to **Configuration > Asset Database > Contacts**.

2. Click **Add**.

Figure 35 Contact Creation



3. Enter the **name** and **description** of the contact. Every contact must have a unique name.

4. Enter the **service** name and the **telephone** number of the contact. The contact telephone number is for reference purposes only.

5. Enter the contact's **e-mail** address. This address will be used to receive a message following an alert generation.

6. Select the **site** the contact is based at from the drop-down list.

7. Select the **contact groups** to which this contact must belong to by clicking on the contact group name in the **Available contact groups** list. Contact groups are used to specify destinations for messages such as emails. This action is mandatory.

8. Click **OK** to save changes and return to the list of contacts.

Editing a Contact

1. Click the name of the contact to edit it.

2. Follow the instructions provided in sub-section Adding a New Contact to configure the contact.

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.

A contact group can be assigned to multiple host groups, and a host group can have multiple contact groups providing a flexible setup for who gets notified when events occur on hosts.

> **Note:** The default contact group cannot be deleted.

Adding a New Contact Group

1. To add a contact group, go to **Configuration > Asset Database > Contact Groups** and click **Add**.

2. Enter a **name** and **description**. Every contact group must have a unique name.

3. In the **Host Groups** pane, select the host groups that must be contacted if required by an alert action. To do so, click on the required host group's name.

- If you want to select all the host groups, click on **Copy all**.
- If you want to remove one of the host group from the **Selected host groups** list, click on its name.
- If you want to remove all the host groups from the **Selected host groups** list, click on **Remove all**.

4. In the **Contacts** pane, select the contacts who must belong to this group.

- If you want to select all the contacts, click on **Copy all**.
- If you want to remove one of the contacts from the **Selected Contacts** list, click on its name. If you remove a contact from the list, then the contact will be automatically transferred to the **Default Contact** group.
- If you want to remove all the contacts from the **Selected Contacts** list, click on **Remove all**.

5. Click **OK** to save the changes and return to the list of contact groups.

Editing a Contact Group

1. Click the name of the contact group to edit it.

2. Follow the instructions provided in sub-section Adding a New Contact Group to configure the contact group.

> **Note:** If you delete a contact group, the contacts included in this group will be automatically transferred to the **Default Contact** group.

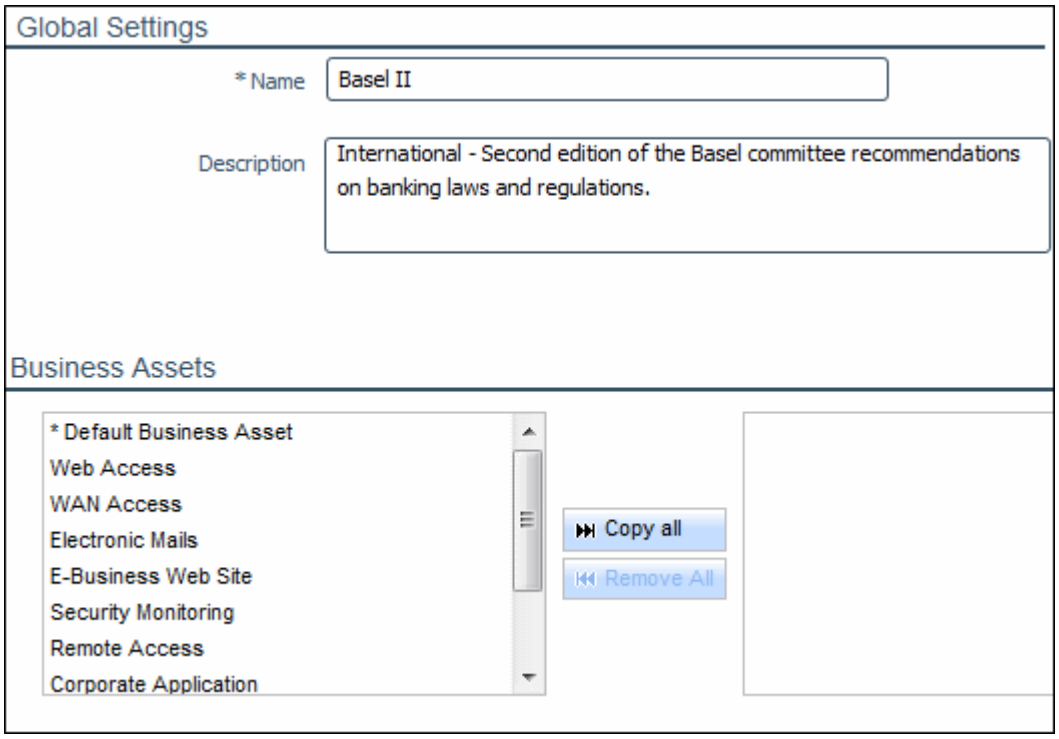
Regulations

Adding an Asset Regulation

1. To add an asset regulation, go to **Configuration > Asset Database > Asset Regulations**.

2. Click **Add**.

Figure 36 Asset Regulations



3. Enter a **name** and **description** for the regulation.

4. In the **Business Assets** pane, select the assets that must be compliant with the regulation. To do so, click on the required asset's name.

- If you want to select all the assets, click on **Copy all**.
- If you want to remove one of the asset from the **Selected assets** list, click on its name.
- If you want to remove all the assets from the **Selected assets** list, click on **Remove all**.

Editing an Asset regulation

1. Click the name of the asset regulation to edit it.

2. Follow the instructions provided in sub-section Adding an Asset Regulation to configure the asset regulation.

Service Level Agreements

The Service Level Agreement screen is used to configure the response times required for alerts' acknowledgement. The following levels of severity must be defined:

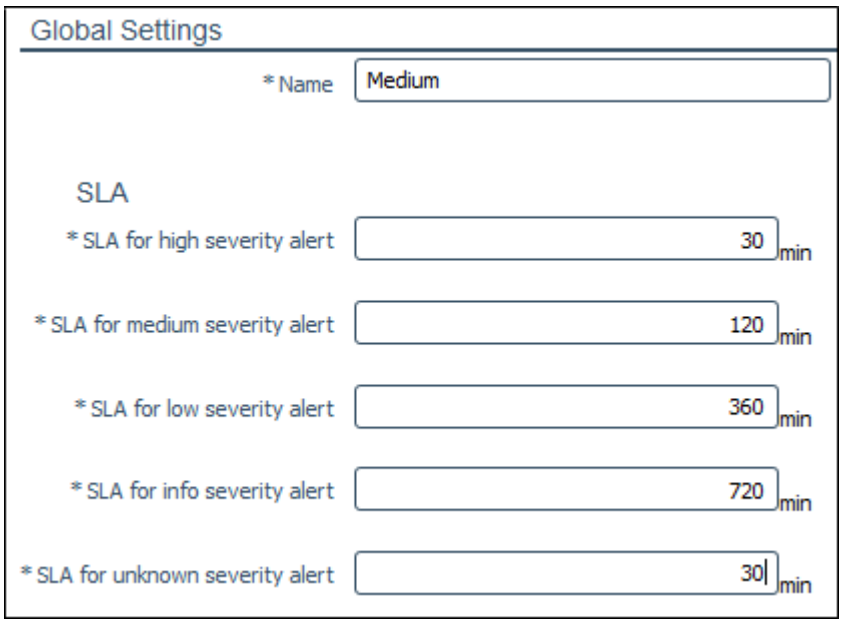
- High
- Medium
- Low
- Informational
- Unknown (only for alerts)

Different SLAs can be created to meet the requirements for assets, and they can be linked to configuration profiles. For example, mission critical servers could be assigned a SLA with very short response times, while test servers could have long response times or even none at all.

Adding a New SLA

1. Click **Add** to add a new SLA.

Figure 37 Add a New SLA



2. Enter a unique **name** for this SLA grouping required response times.
3. For each severity level, enter the allowed timeframe (in minutes) for a response.
4. Click **OK** to save the SLA or **Cancel** to close without making any changes.

Editing an SLA

1. Click the name of the desired SLA to edit it.
2. Follow the instructions provided in sub-section Adding a New SLA to configure the SLA.

Effective Vulnerabilities

Navigating through the list

- As the list may extend to several pages, use the First Page, Back a page, Forward a page, and Last page icons. 1-3/3 1

Selecting the number of rows per page to display

- Click on the number of vulnerabilities being displayed (1-3/3 in the above example).

Marking Vulnerabilities as False Positives

If some of the vulnerabilities should not be included, they can be marked as false positives.

1. Tick the relevant checkboxes

2. Click **False Positive**.

When an alert generated by a scanner is acknowledged as **False Positive**, this vulnerability will automatically be transferred from the **Vulnerability** list to the **False Positive** list.

False Positive Vulnerabilities

Navigating through the list

- As the list may extend to several pages, use the First Page, Back a page, Forward a page, and Last page icons. 

Selecting the number of rows per page to display

- Click on the number of vulnerabilities being displayed (1-3/3 in the above example).

Marking Vulnerabilities as True Vulnerabilities

If some of the vulnerabilities should not be listed as false positives, they can be marked as true vulnerabilities.

1. Tick the relevant checkboxes.

2. Click **True vulnerability**.

Chapter 5 - Managing Logs and Events

Managing logs and events implies working with a large amount of logs composed - hopefully - of meaningful information.

The user must consider this aspect by implementing policies that will allow clarity and consistency in his security information management.

These policies are the following:

- Log Collection Policy, which allows you to determine which events at the Log Collector are sent to the SMP.
- Aggregation Policy, which regroups similar events in order to diminish the total number of events to be processed by the SMP.
- Correlation Policy, which is the process of using a pre-defined correlation rule to combine one or more different events into an alert.

Log Collection Policy

What is a Collection Policy?

Collection policies allow you to determine which events at the Log Collector are sent to the SMP. Filtering is carried out at the Log Collector, to avoid wasting bandwidth from the Log Collector to the SMP.

> **Caution:** Standard collection policies (delivered by TIBCO LogLogic®) cannot be modified. To change the configuration of collection policies, copy and edit them as needed.

A collection policy file contains a list of **rules** which determine the actions to take, such as:

- send elementary events only:
  - a small number of them
  - only the main ones
  - all those with a Taxonomy
  - all of them
- send both raw logs and Elementary Events:
  - all the elementary events with a Taxonomy + a small number of raw logs
  - all the elementary events with a Taxonomy + raw logs
  - all the elementary events + all types of raw logs
- send everything:
  - all types of elementary events
  - all types of raw logs
- send nothing to the SMP.

This can reduce the amount of events sent from the Log Collector to the SMP.

Each rule within a collection policy file is made up of a list of **conditions**, each of which has an associated **action**.

Collection policies can be configured from **Log Management > Log Collection policies**.

Edit a Copy of an Existing Collection Policy

1. Select one of the collection policy's name, e.g. *_2_NoRawLog_StandardElemEvent* and click on the **Copy** button.

2. Click on the copy of the policy to open the **Collection Policy Edition** screen.

This screen allows you to manage the list of **rules** that make up the particular collection policy file. Each rule is made up of **conditions**, where each condition determines the action to take.

3. Rename the collection policy:

- Allowed characters: A to Z, digits, underscore and dash.
- Forbidden characters: space, the string **exa_** at the beginning, any other characters.

4. To determine the action to take for a particular rule, or multiple rules, click the desired rules' checkbox(es), and then click **Set Action**. Select the desired action from the **New Action** drop-down list, then click **OK**.

> **Caution:** If you choose the action **Skip Event**, please be aware that the event will not be sent to the server. It will be lost.

5. You can change the sequential order of the rules by selecting a rule, and then clicking **Move**. The rule order is important since they are evaluated in ascending order. When a rule is matched, the associated action is executed, and the other rules are ignored.

Edit or Create a Rule Condition

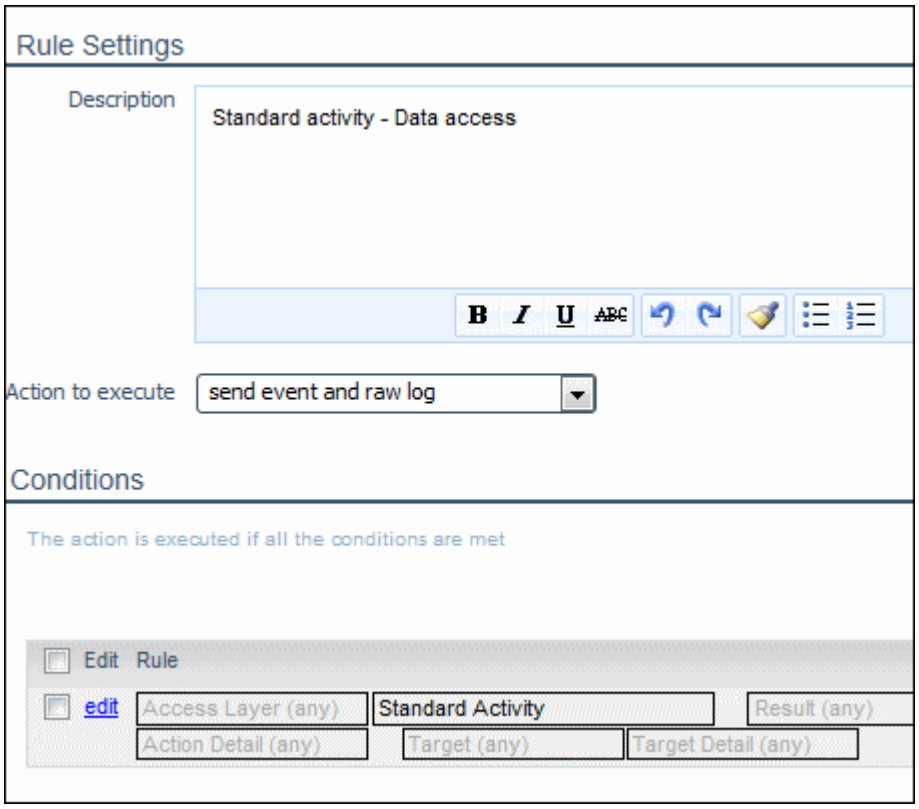
Rules contain associated conditions; a rule is only matched when all of its associated conditions are met.

> **Caution:** Using multiple rule conditions with a REGEXP matching type can increase the Log Collectors CPU usage and decrease the Log Collector's performance.

Editing a Rule Condition

1. In the **Collection Policy** screen you have selected, click on the **edit** link corresponding to the relevant rule. This displays the following screen.

Figure 38 Editing a Rule Condition



2. In the **Conditions** pane, click on the edit link to edit an existing condition. It displays the Conditions screen:

3. Using the drop-down lists, select the category that the event must match, then click **OK**. See the section on Correlation rules for an explanation of the drop-down lists in this section.

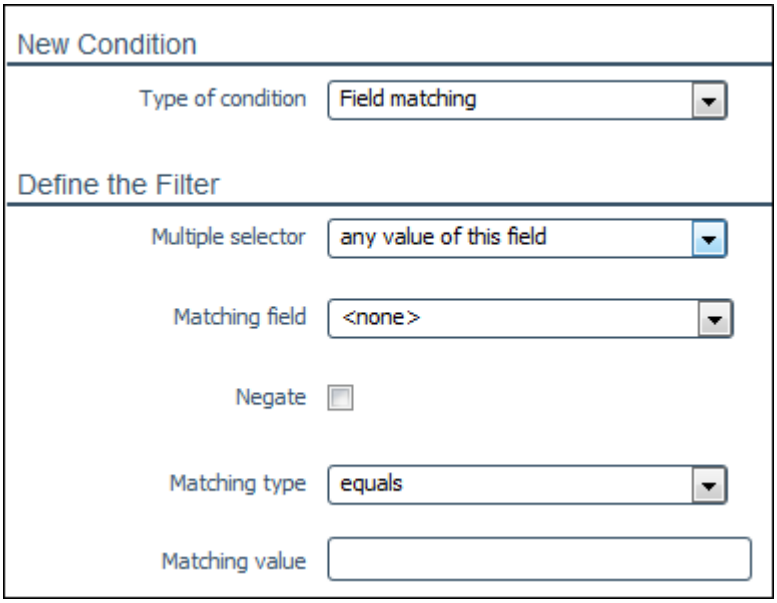
Creating a new condition

1. Click on **Add** to display the **Add a New Condition** screen.

2. From the **Type of Condition** drop-down list, select either **Field Matching** or TIBCO LogLogic® Taxonomy.

- Selecting **Field Matching** displays the **Define the Filter** pane.
- Selecting TIBCO LogLogic® Taxonomy displays the **Define the** TIBCO LogLogic® Taxonomy pane.

Figure 39 Filter Applied Pane



Define the Filter pane

1. Select a 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**.

2. Select which field in the event is to be checked in the **Matching field** drop-down list. 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.

3. Set **Negate** to reverse the logic - e.g., to look for events which is not authentication.

4. Specify which type of test is to be performed in the **Matching Type** field.

5. In the **Matching Value** field, specify the value to be tested. The field is not case sensitive. 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".

6. Click **OK**. The condition is created and it will be displayed in the **Collection Policy** rule list.

Define the TIBCO LogLogic® Taxonomy

- Select the TIBCO LogLogic® Taxonomy fields that must be matched.

Aggregation Policy

What is Aggregation?

The overall objective of the aggregation engine is to regroup similar events in order to diminish the total number of events to be processed by the SMP, thereby increasing the overall performance of the system.

For example: Several events that have the same source and the same target IP address would be aggregated in one event.

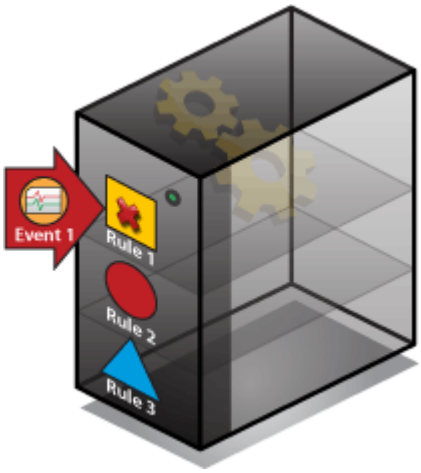
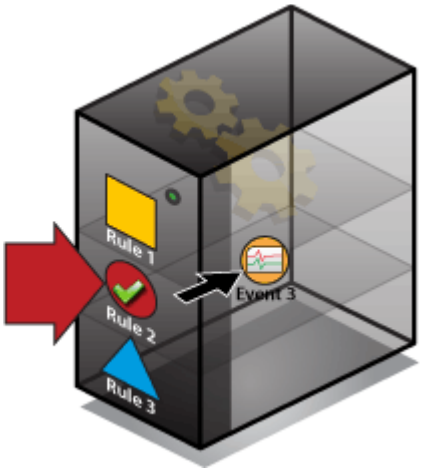
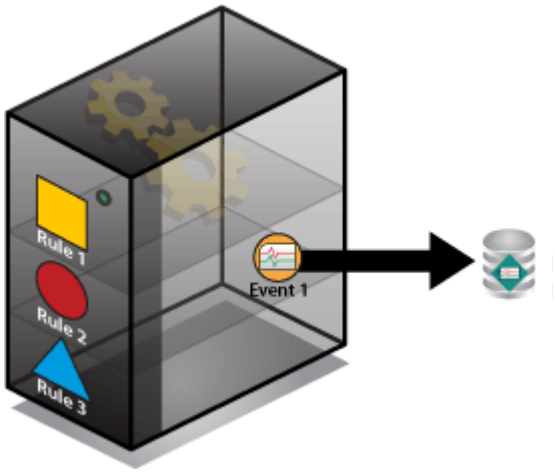
What are Rules used for?

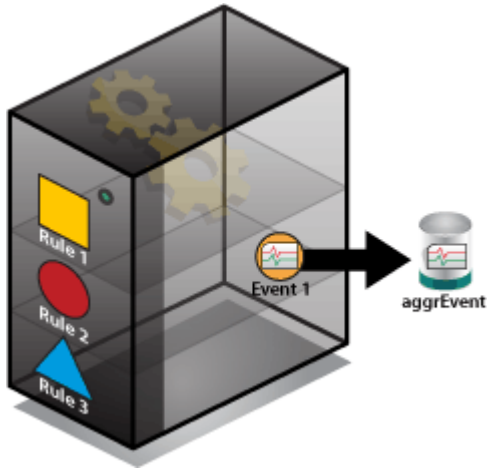
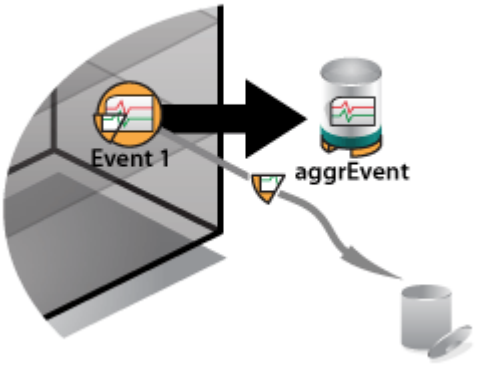
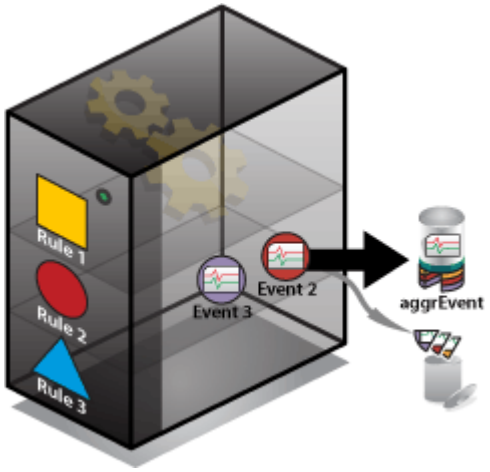
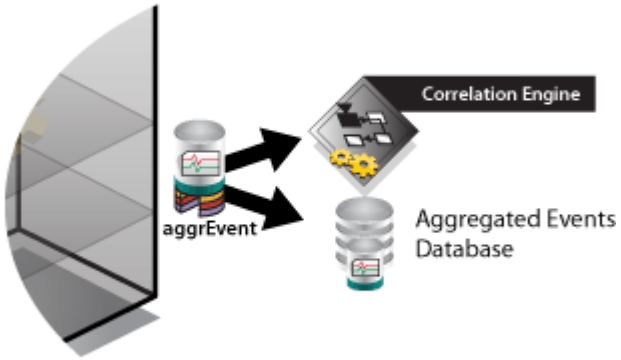
Rules control how events are aggregated, and they allow you to build up consistent policies to provide a high level information system security overview.

The aggregation rules are grouped into eight main categories:

- Information status
- Standard activity
- Configuration activity
- Vulnerability status
- Suspicious activity identification
- Malware identification
- Attack identification
- Undefined TIBCO LogLogic® Taxonomy
- Implied rule

The aggregation process can be represented as follows:

	
Event 1 is about to enter the aggregation engine. To match an aggregation rule, an elementary event must meet several conditions.	Event 1 does not match Rule 1 conditions.
	
Event 1 matches Rule 2 conditions and is stored in the waiting queue.	Event 1 is copied in the Elementary Events database according to the user's rule configuration.

	
Once Event 1 has been processed by the Aggregation engine, an aggregated event “a” is created.	A part of Event 1 has been removed during the Aggregation process. Only the relevant data is kept in the Aggregated Event.
	
As other events arrive in the Aggregated Engine, they are stored in the waiting queue and added to the Aggregated Event “a”, provided they meet the same rules’ conditions.	When the Aggregated event “a” is updated, it is stored in the database and sent to the Correlation engine.

Example

The Aggregation Engine must treat three elementary events (one after the other).

- The top of the cylinder in green represents the common elements.
- The two other cylinders, of various colors, represent the different information between the three events. These are two specific fields of an event.

In our example, it could correspond to:

	Event 1	Event 2	Event 3
Classification	Packet denied	Packet denied	Packet denied
IP source	10.0.0.1	10.0.0.2	10.0.0.3
Port Source	80	80	80
IP target	192.168.10.45	83.25.54.46	100.0.0.1
Port target	514	514	514

An aggregated event which contains 3 elementary events is generated.

It is composed of elements that each event shares in common. In our example, it refers to classification, source and target ports.

The gathered information corresponds to the source IP and the lost piece of information corresponds to the target IP.

The result should be the following:

Aggregated Event = 3	
Classification	Packet denied
IP Source	10.0.0.1 or 10.0.0.2 or 10.0.0.3
Port Source	80
Port Target	514

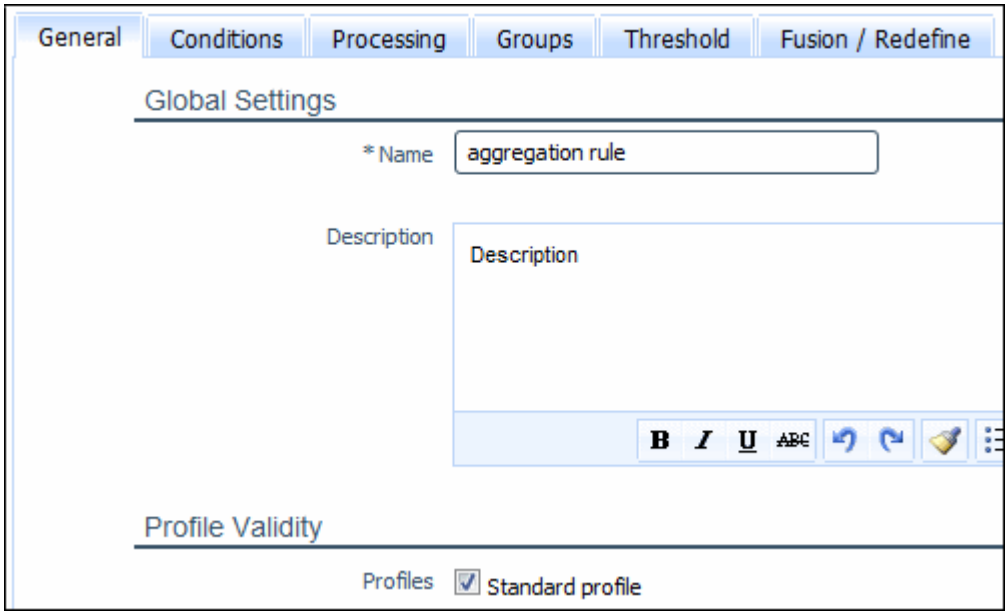
Create an Aggregation Rule

Aggregation rules control how events are aggregated, and allow you to build up complex scenarios to deal with events and alerts.

A business-oriented correlation allows the system to estimate the impact of an event on the information system and adjust priorities according to specific criteria. Moreover, a correct asset database configuration associated with a correlation rule can make the difference when monitoring events.

1. Go to **Log Management > Aggregation Policy.** and click on the **Add** button in the **Aggregation Policy** screen. The following screen is displayed.

Figure 40 Aggregation Rule General tab



General tab: enter general information

1. Select the **General** tab.
2. Enter the name and description of the aggregation rule.
3. Select in which security profiles this rule is active. See sub-section Configuration Profiles and Security Levels for further information.
4. Click **OK**.

Conditions: define the conditions and exceptions of the rule

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.

1. Select the **Conditions** tab.

Table 7 Aggregation rule - Logical Expression

Field	Description
Logical Expression	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.

2. Add the relevant conditions and/or exceptions by clicking **Add**. The **Add a new Condition/Exception** screen is displayed.

3. Select the type of condition/exception you want to use: either **Field Matching** or TIBCO LogLogic® Taxonomy.

- **Field Matching**: Specify the field contents in the event, e.g., Target hostname is "server1". Then several fields are displayed as described in the table below.
- TIBCO LogLogic® Taxonomy: Specify how the alert has been categorized, e.g., the action is ***malware*** and the target is a ***database***.

Table 8 Correlation & Aggregation - Add New Condition Fields

Field	Description
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". **Note:** The field is not case-sensitive.

4. Click **OK**.

Processing tab: define the action to perform when the event is matched

- Select the **Processing** tab.

Figure 41 Processing tab

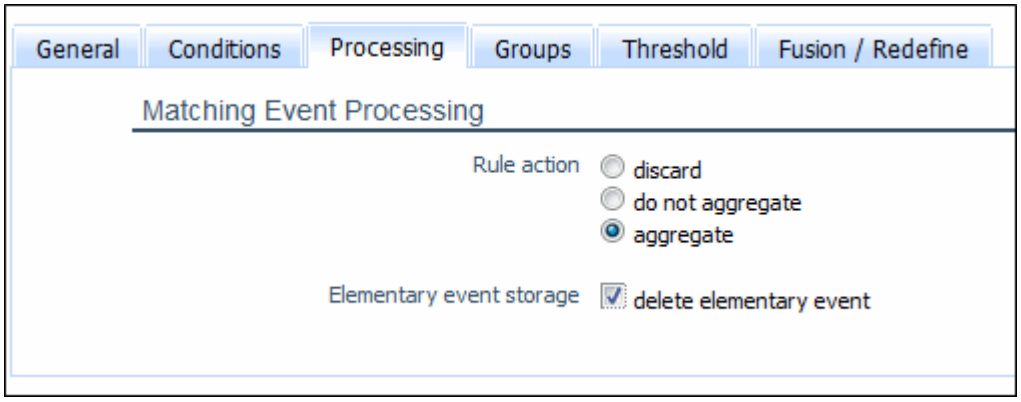


Table 9 Aggregation - Processing Tab

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: define the grouping process

- Select the **Groups** tab.

This type of rules enables the system to detect a set of successive events which occurred on a server. These rules are only used for scenarios.

For example, ***Corr. - Login Success*** detects that a user logged successfully on the server.

Associated with the rule called ***Corr. - Login Failed,*** the scenario ***Suspected bruteforce*** can be triggered.

To define how data will be grouped.

1. Click on the **(none)** entry. The **Group Field** pane is displayed.

2. Select 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.

3. Select the **Field's value Required** checkbox if only events with a defined field's value must be grouped.

4. Click **OK**.

5. In the **Groups** tab, indicate the processing order of rules by checking the relevant rule and clicking on **Move Up** or **Move Down**.

Define the Threshold for the Grouping Process

- Select the **Threshold** tab.

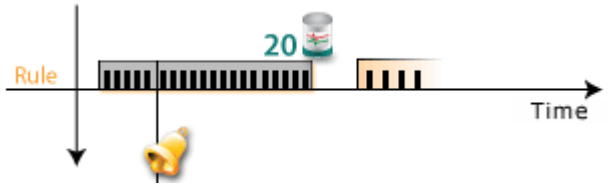
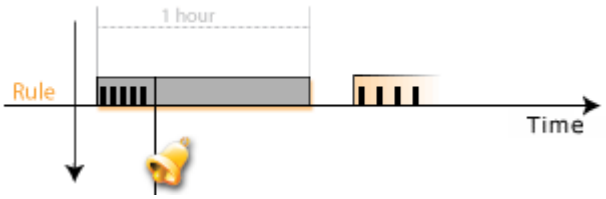
The threshold tab allows you to specify under which conditions a rule would be triggered, that is, to combine events into a single event.

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.

> **Note:** You can also use default threshold rules available. For example *Threshold - User authentication* detects that one or several users tried to - successfully or not - connect on a service ten times in a row on a short period of time.

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

Table 10 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: 

Redefine the characteristics of an event

- Select the **Fusion/Redefine** tab.

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

Table 11 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.

Correlation Policy

What is Correlation?

Correlation is the process of using a pre-defined ***correlation rule*** to combine one or more different events into an alert.

For example:

Alert 1: A "Suspicious" event followed by an "Attack" event is correlated into a "Possible Malicious Activities."

Alert 2: Several failed logins followed by a successful login event is correlated into a "Possible Brute Force Alert".

What are Rules used for?

Rules control how events are correlated, and they allow you to build up consistent policies to provide a high level information system security overview.

What are Scenarios used for?

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.

Analogy with E-mail Inbox

Let us make an analogy with your E-mail inbox.

You receive a great number of e-mails during the course of one day, of different subject matters, which clutter your e-mail inbox, and you find it increasingly difficult to find important e-mails. So you decide to organize your e-mails by creating rules and folders. You decide that if you receive three more e-mails this morning, with a subject line of “sponsor meeting”, you will create a folder called “Sponsor Meeting” and move your e-mails to this folder.

In a similar way:

- You can think of the received e-mails as events and the folder you have created as a correlated alert.
- You have also specified a Threshold (how many e-mails have to arrive before you will create an alert) and you have also specified a Duration (the e-mails must be received this morning).
- You have also specified that only today’s e-mails will be moved to the folder, so the Aggregation timeout is set to 24hrs.

Later in the afternoon, another “Sponsor Meeting” e-mail arrives. It can still go into the “Sponsor Meeting” folder file, since you have specified that all of today’s e-mails with the subject line “Sponsor Meeting” are to go into the “Sponsor Meeting” folder.

The next day, you receive new “Sponsor Meeting” e-mails, but since you had specified that only e-mails from the previous 24 hours would go into the “Sponsors Meeting” folder, that folder is now closed (the Aggregation Timeout has been reached). Therefore, you create a new folder.

The diagram below summarizes the process.

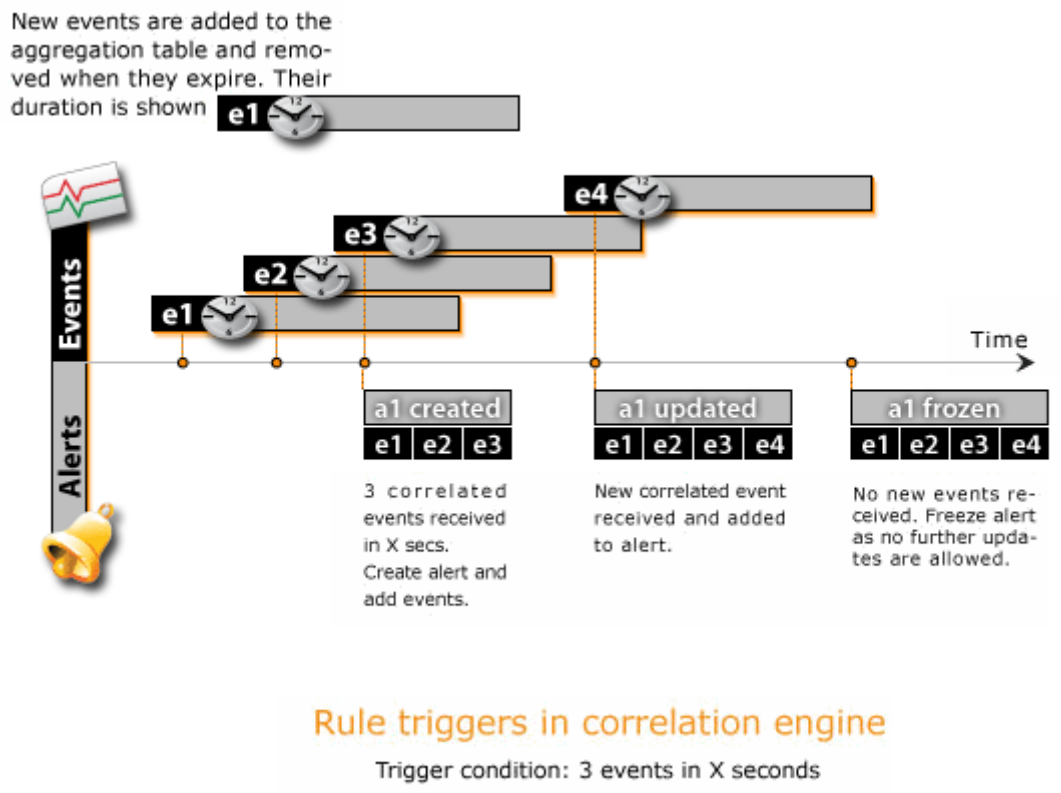
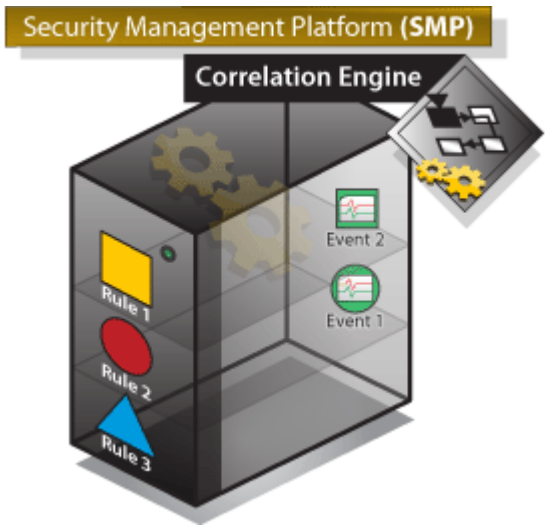


Table 12 Analogy between Correlation and Email Inbox

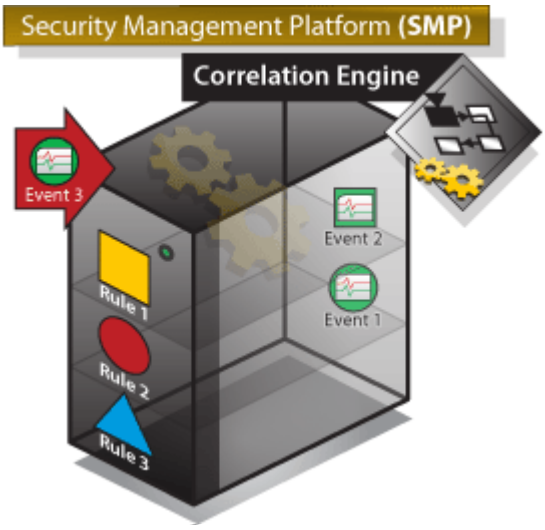
Email Inbox	Aggregator Properties
In order to better organize your inbox, you decide that if you receive 3 or more emails today with a subject line: "Sponsor Meeting," they will be moved to a folder called ***Meeting***	Decide how many alerts/ events have to occur (***Threshold***) within a given time (***Duration***) to trigger a correlated alert. Diagram: see step `a1:Created`
During the day, you receive more emails with this subject line, so you add them to the ***Meeting*** folder.	More events/ alerts are received with the specified time (***Duration***) so these are added to the already created alert. Diagram: see step `a1:updated`
This day reaches its end.	The maximum time for the alert to be open is reached (***Aggregation timeout***), so the original alert is frozen. Diagram: see step `a1:Frozen`
The next day, more "Sponsor Meeting" emails are received, but because you had specified that the "Sponsor Meeting" folder is only for emails from yesterday, you create a new folder.	A new event arrives after the ***Aggregation timeout***; a new alert is created.

The correlation process can be represented as follows:

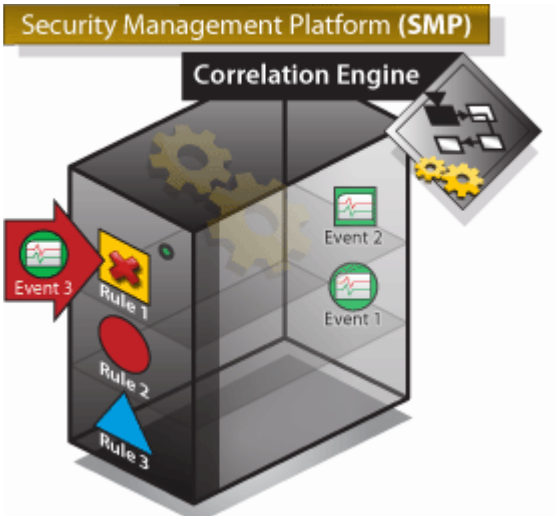
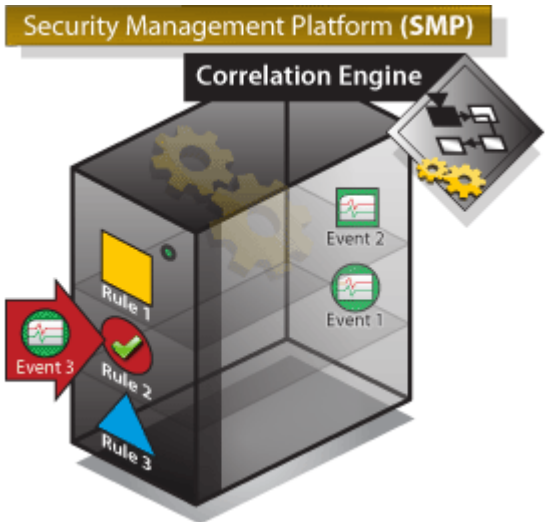
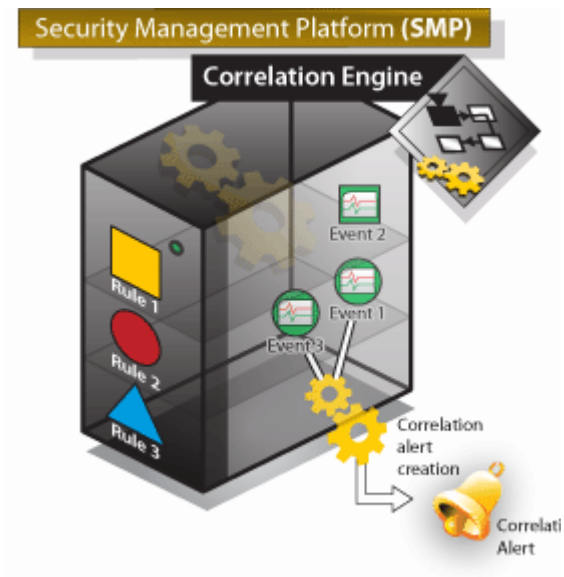
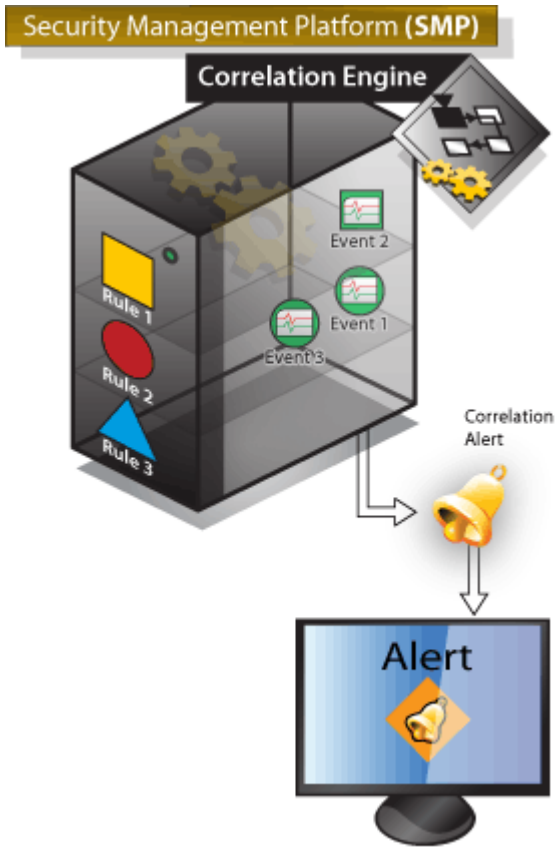
The Correlation Process



Inside the SMP correlation engine we find the SMP rules database. In our example, two events have already arrived at the engine and are pending.



A new event arrives.

	
The SMP correlation engine compares information with the conditions in Rule 1, looking for a match. No match is found with Rule 1.	The SMP correlation engine proceeds to compare information with the conditions in Rule 2. A match is found with Rule 2.
	
For the purpose of this example, Rule 2 tells the SMP to create a correlation alert and stop the comparisons if a match is found. As a consequence, a correlation alert is created.	The corresponding alert is displayed in the GUI.

Create a Correlation Rule

1. Click on the **Add** button. The **Correlation Rule Creation** screen is displayed.

General tab: enter general information

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

Table 13 Correlation rule - General Tab

Field	Description
[Edition] 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.
Rich text toolbar	Allows you to modify the description format.
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.
[Edition] Creation	The date and time that the rule was created and which user created it.
[Edition] 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 Configuration Profiles and Security Levels for further information.

Conditions tab: define the conditions and exceptions of the rule

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 14 Correlation rule - Logical Expression

Field	Description
Logical Expression	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.

1. Add the relevant conditions and/or exceptions by clicking **Add**. The **Add a new Condition/Exception** screen is displayed.

2. Select the type of condition/exception you want to use: either **Field Matching** or TIBCO LogLogic® Taxonomy.

- **Field Matching**: Specify the field contents in the event, e.g., Target hostname is "server1". Then several fields are displayed as described in the table below.
- TIBCO LogLogic® Taxonomy: Specify how the alert has been categorized, e.g., the action is ***malware*** and the target is a ***database***.

Table 15 Correlation rule - Add New Condition Fields

Field	Description
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". **Note:** The field is not case-sensitive.

3. Click **OK**.

Example with a Default Correlation Rule

Let us take the example of the default correlation rule entitled **ADB-Bypass-Windows Domain Controller**.

If you click on its name to edit it, you will obtain the following screen.

Figure 42 Conditions tab

The rule detects all the events whose target is a host.

The host is in a host group that does not contain the name Mail (e.g. Mail server) in its name. The event refers to a connection to a known mail port.

This rule prevents from the risk of a fraudulent mail server in the customer's asset database (not monitored by the site network administrator and by SEM) which sends/receives mails in the client network.

Then when you click on the **Actions** tab, you will see details of the rule.

The risk is described as a detected suspicious violation of a mail, which is described in the TIBCO LogLogic® Taxonomy.

As this is a known risk, the engine creates an alert called "Mail server bypass" with a medium priority to force the analyst to investigate the problem.

Limitations

A mismatch may occur when defining correlations policies' conditions and exceptions as in the following example:

Let us suppose:

- One Elementary Event (**EE1**) containing values **Administrator** and **User A**.
- One Elementary Event (**EE2**) containing values **Administrator** and **User B.**
- An Aggregation rule (**AR**) with a condition saying that value **Administrator** starts the aggregation process.
- A Correlation rule with an exception saying that value **User B** must not be taken into account and which creates a Correlation Alert.

Description

EE1 is matching **AR** for 100 seconds during which an Aggregated Event (**AE**) containing values **Administrator** and **User A** is created. Then a Correlation Alert (**CA**) is created.

At the same time, **EE2** also matches **AR** because of the value **Administrator**. **EE2** enters into **AE**.

EE2 then should not be taken into account in **CA** because of the exception ignoring value **User B**. However, in this case, **CA** will contain values **Administrator**, **User A** but also an aggregated event containing the value **User B** forbidden by the rule.

> **Note:** Should **EE2** be processed before **EE1**, the behavior would be the expected one.

Groups tab: define the grouping process

This type of rules enables the system to detect a set of successive events which occurred on a server. These rules are only used for scenarios.

For example, ***Corr. - Login Success*** detects that a user logged successfully on the server.

Associated with the rule called ***Corr. - Login Failed,*** the scenario ***Suspected bruteforce*** can be triggered.

To define how data will be grouped.

1. Click on the **(none)** entry. The **Group Field** pane is displayed.

2. Select 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.

3. Select the **Field's value Required** checkbox if only events with a defined field's value must be grouped.

4. Select a value in the **Grouping method** drop-down list. 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.

5. If you selected **distinct field values**, the **Minimum number of distinct values** field is displayed. Enter the minimum number of fields to add in the group to allow the creation of an alert.

6. Click **OK**.

7. In the **Groups** tab, indicate the processing order of rules by checking the relevant rule and clicking on **Move Up** or **Move Down**.

Threshold: define the threshold for the grouping process

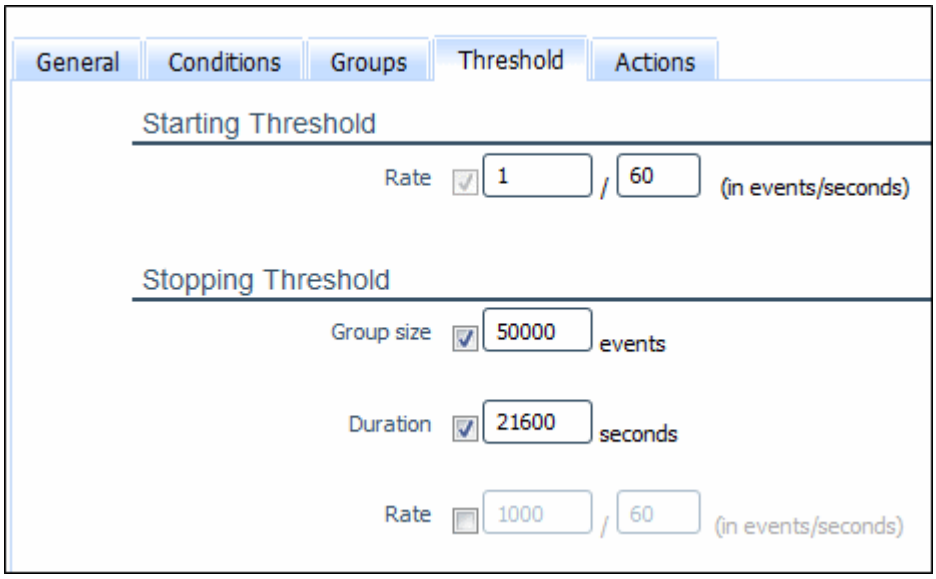
The threshold tab allows you to specify under which conditions a rule would be triggered, that is, to combine events into a single event.

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.

Note: You can also use default threshold rules available. For example *Threshold - User authentication* detects that one or several users tried to - successfully or not - connect on a service ten times in a row on a short period of time.

The threshold properties are the following.

Figure 43 Correlation rule Threshold tab



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

Table 16 Aggregation - Threshold Tab

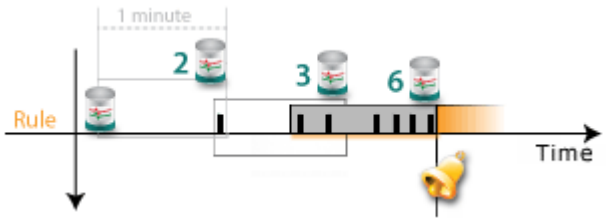
Property	To specify...
Starting Threshold	
Rate	The minimum number of events per defined interval (per second) needed to trigger a correlation process. Example with a rate set at 6/3600: 
Stopping Threshold	

Table 16 Aggregation - Threshold Tab

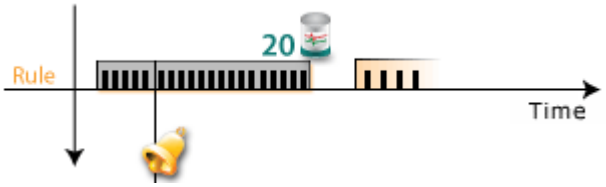
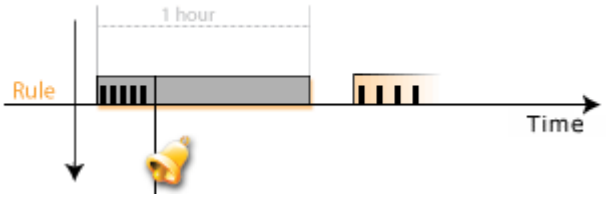
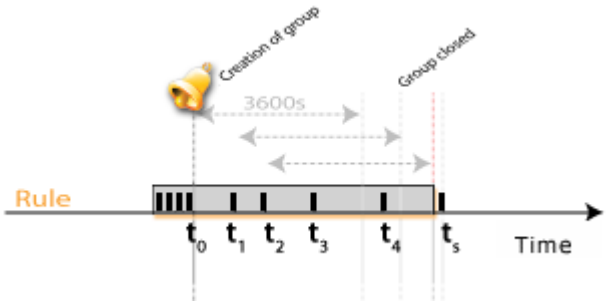
Property	To specify...
Starting Threshold	
Group size	The maximum number of events to group into a single event/alert. If matching events are received after the maximum threshold has been reached, then a new event is created. By default, the maximum number of events is set at 1000. Example with a group size set at 20: 

Table 16 Aggregation - Threshold Tab

Property	To specify...
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: 
Rate	The minimum number of events per defined interval (per second) under which to stop an aggregation or correlation process. Example with a rate set at 4/3600: ▪ t0 = time of creation of a group. ▪ t0 + 3600 = time before which at least 4 elementary events must have entered the group. ▪ t1, t2, t3, t4, t5 = elementary events entering the group. This group will be closed if it has not reached the minimum number of elements (4) in the time limit (3600s) to "stay alive".  **Note:** Usually, if the **Rate** checkbox is selected, the **Group size** and **Duration** checkboxes are not used.

Actions: define the correlation action

Table 17 Actions pane

Checkbox	Description
Create an alert	Creates an alert when the rule is triggered.
Change the event severity	Changes the event severity when the rule is triggered. Only available if the **Create an alert** checkbox is NOT selected.
Send the event/alert to another SMP	Sends an alert or event from one SMP to another one if you installed multiple SMPs.
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.
Mail the event to contacts	Defines the group of contacts to whom you will automatically send an E-mail regarding the event.
Send an event/alert as SNMP trap	Generates an SNMP (Simple Network Management Protocol) trap and sends it to a specified IP address or host name.
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.
Create an incident	Creates automatically an incident from the alert.
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.

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.

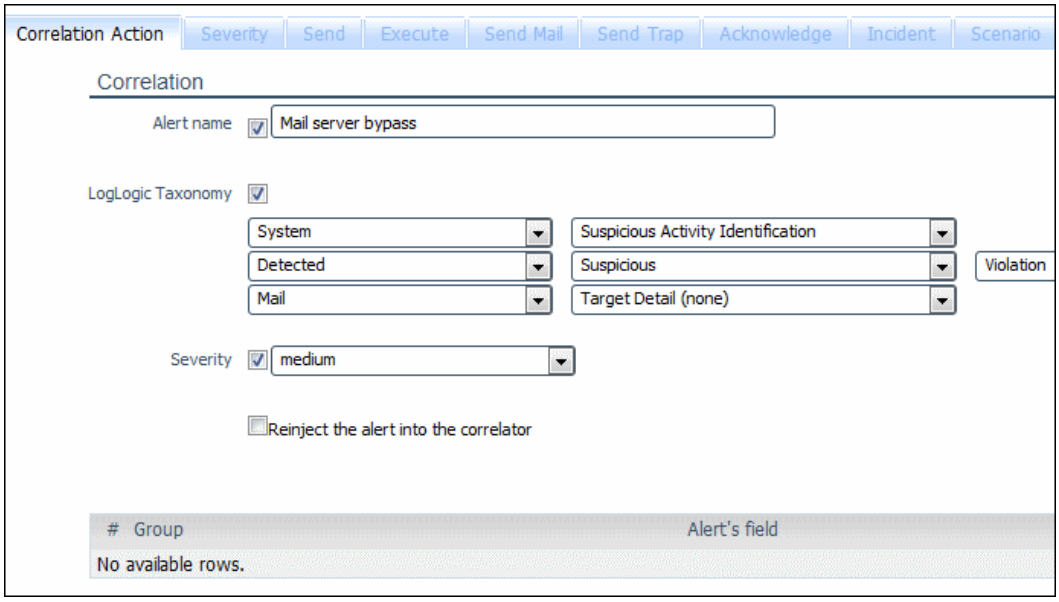
E.g. Let us suppose the expected action is **Use an external command**. When the rule is triggered, the script will be executed as many times as the number of aggregated events contained in the aggregate (e.g. threshold set to 10 events: when the rule is triggered, the script is executed 10 times).

Create an alert

To create an alert:

1. Enter the alert's name. The text string will be displayed on the alerts screen.

Figure 44 Correlation Action tab



2. Select the TIBCO LogLogic® Taxonomy or categories that can be used to match this new alert, with other rules that match by categories.

> **Note:** If you selected TIBCO LogLogic® Taxonomy **- (all fields)** in the **Groups** tab, the TIBCO LogLogic® Taxonomy checkbox is automatically selected.

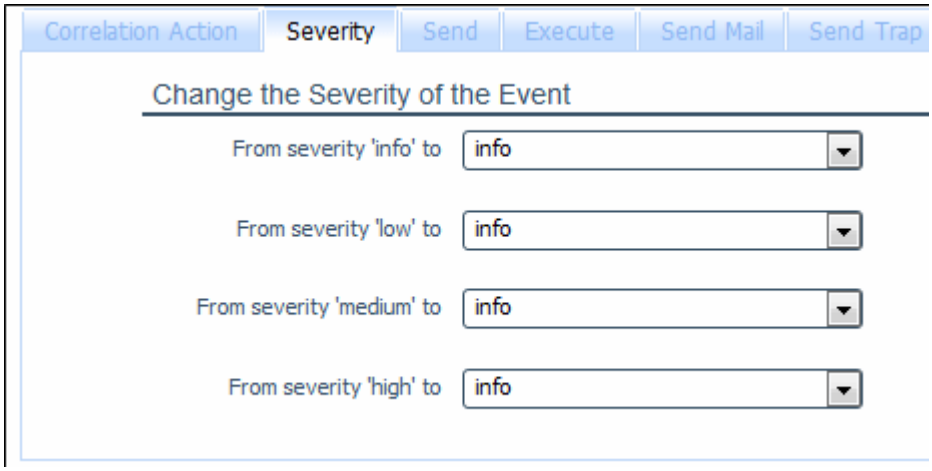
3. Select the severity of the new alert.

4. Indicate if the alert must be processed again by selecting the **Reinject the alert into the correlator** checkbox.

5. Specify the fields that will be available for correlation.

Change the event severity

Figure 45 Severity tab



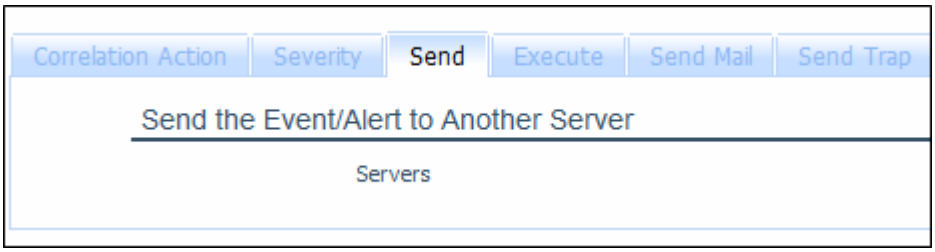
To change the new event severity:

- select the relevant severity in the drop-down lists.

Send the event/alert to another SMP

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.

Figure 46 Send tab

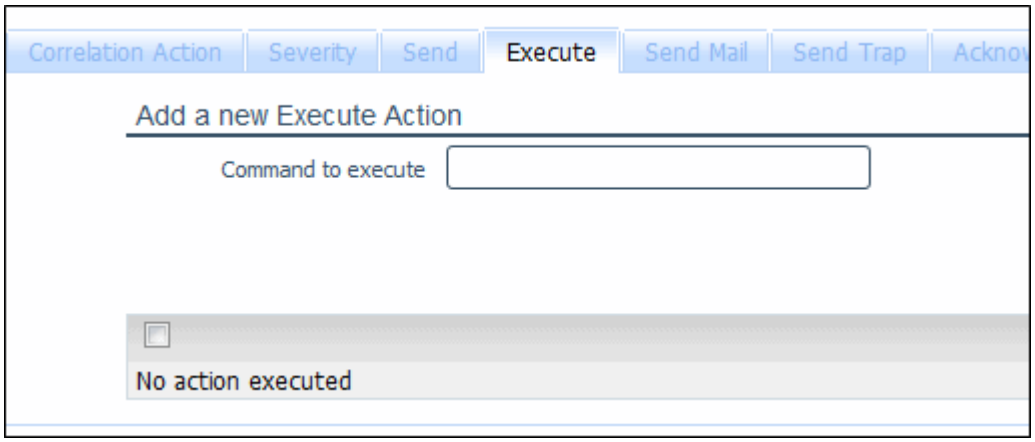


To do so:

- select the target server to which you want the alert/event to be sent.

Use an external command

Figure 47 Execute tab



To make this action efficient, please read carefully the following instructions:

In a shell:

- You must configure the user's permission to start the script.
Example: `[root@hostname script]# chmod +x ./command.pl`
- It is advised to specify the group and owner of the script as **exaprotect:exaprotect**.
Example: `[root@hostname script]# chown exaprotect:exaprotect ./command.pl`

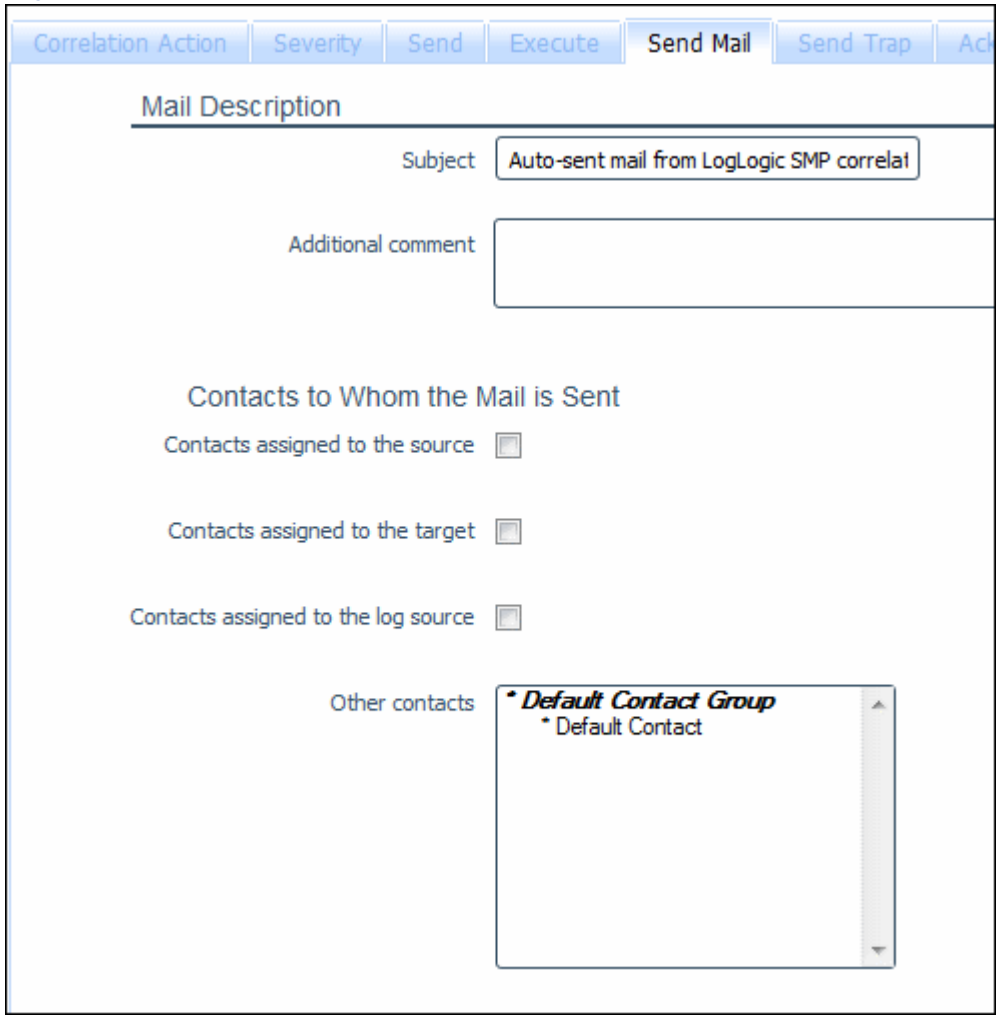
In the interface:

- The command to execute (or script) must be located under home/exaprotect/scripts/.
- You must enter the file name in the **Command to execute** field (for example `command.pl`).

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

Mail the event to contacts

Figure 48 Send Mail tab



To configure the e-mail:

1. Configure default *.properties files that contain all the mail sending process configuration data.

> **Caution:** Please 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).

2. Enter the e-mail subject and add a comment.

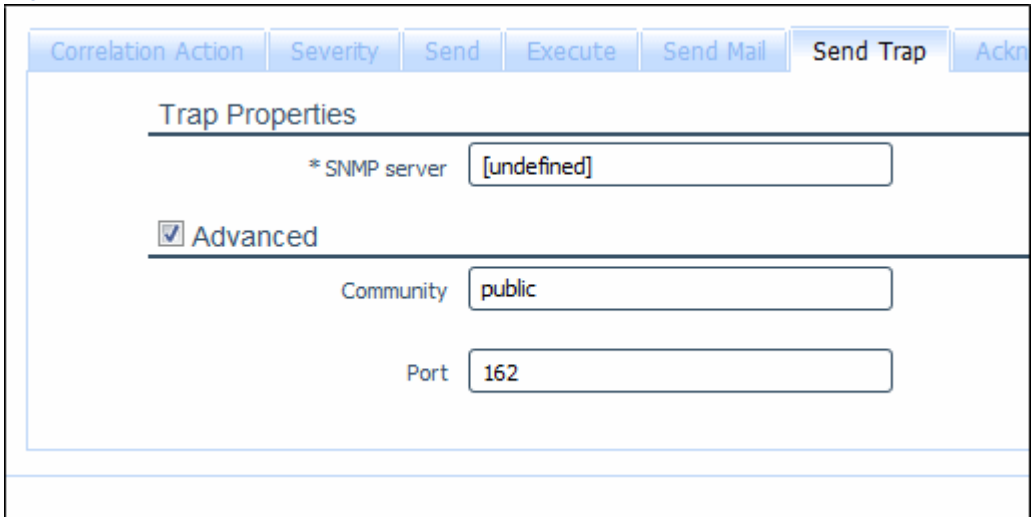
3. Select the type of contacts to whom you want to automatically send the E-mail: either contacts assigned to the source, to the target, to the log source or to other contacts. You can configure these contact groups under the **Asset Database > Contact Groups** screen.

The sent mail generally looks like the following example:

```
SSH Remote root login
**********************
Dates
 * Creation: 2007-05-07 16:26:30
 * Detection: 2007-05-07 16:26:29
 * Analyzer: 2007-05-07 16:26:30
**********************
Alert Info
 * Alert Ident: 410
 * Action Category: Authentication Activity
 * SubAction Category: Session
 * Target Object Category: SSH
 * Target Attribute Category: Admin
 * State Category: Success
 * Kind: normal
 * Computed Severity: medium
**********************
Analyzer #1
 * Analyzer ID: ESMP
 * Name: ESMP
 * Model: ExaLogConverter
 * Version: 1.0
 * Class: relay
 * Os Type: Linux
 * Os Version: 1.0
**********************
Assessment
 * Impact
  - Severity: medium
  - Type: admin
  - Completion: succeeded
  - Description: see below
---%<---%<---%<---%<---%<---%<---%<---%<---%<---%<---%<---%<---%<---%<---%<---%<
Root logged in from 192.168.10.21:1523 using the password method ---%<---%<---%<---%<---%<---
%<---%<---%<---%<---%<---%<---%<---%<---%<---%<---%<
**********************
Source #1
 * Node
  - Category: dns
  - Name: username
  - Address #1
   + Category: ipv4-addr
   + Address: <span style="white-space: nowrap;">192.168.10.21</span><br/><I style="white-
space: nowrap ;">( username.ept.<a HREF='Whois.jsp?TARGET=exaprotect.net'
TARGET=_blank>exaprotect.net</a>)</i>
 * Service
  - Port: 1523
  - Protocol: tcp
**********************
Target #1
 * Node
  - Category: dns
  - Name: localhost
 * User
  - UserId #1
   + Name: root
 * Service
  - Port: 22
  - Protocol: tcp
**********************
Additional Data
 * Log received from: /var/log/messages
 * rulesetName: ssh.rules
 * regexId: 1
          **********************
```

Send an event/alert as SNMP trap

Figure 49 Send Trap tab



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

1. Enter either the 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.
2. Enter the 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.
3. In the **Port** field, enter the port to which the **SNMP** server listens to.

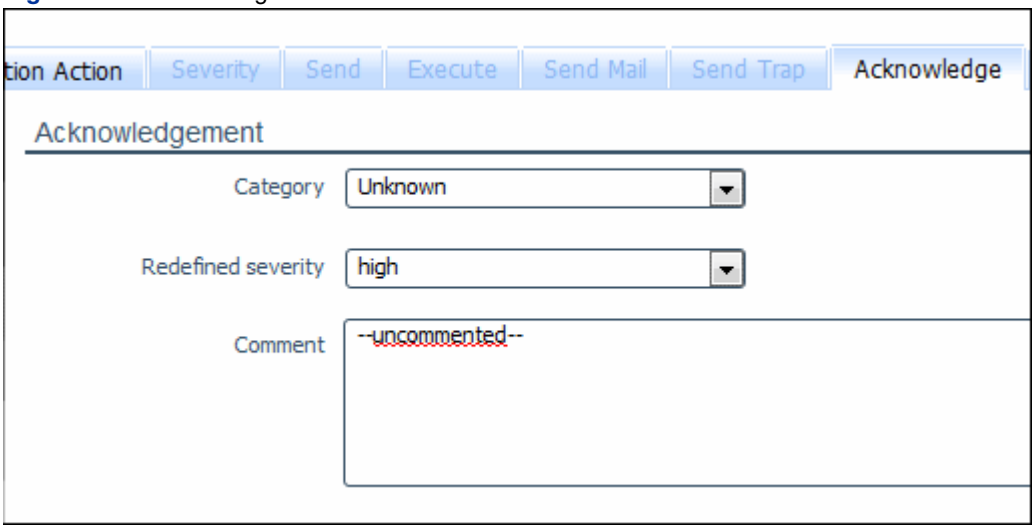
Here is an example of the syntax for a sent SNMP trap.

```
Dec  8 15:51:26 localhost snmptrapd[3684]: 192.168.10.221: Enterprise
Specific Trap (534) Uptime: 4:45:13.92, SNMPv2-MIB::sysDescr.0 = STRING:
id=594;alert=Root
login;severity=medium;target0_name=localhost;analyzer0_address0=192.168.1
1.110;analyzer0_name=esmp
```

It is not possible to configure content and syntax. However, this message allows you to know the alert's name, its criticality, the alert's target, etc.

Auto-acknowledge the alert

Figure 50 Acknowledge Tab



To acknowledge an alert automatically:

1. Select the type of alert in the Category drop-down list. This field is used by the reporting module to show what type of alerts are being generated.

2. Select the severity for the alert in the Redefined Severity drop-down list. This will lower the confidence rating in the analyzer.

3. Enter a comment regarding the alert and the auto-acknowledgement.

Create an incident

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 18 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.
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. You cannot select the contact group.
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. 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.

Table 18 Incident Tab

Field	Description
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.

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.

Please refer to the *SEM Concepts Guide - Appendix* to get the list of all the alert fields available.

Defining Scenarios

Scenarios are used to describe more complex situations requiring multiple actions that simple rules alone cannot manage to describe. A scenario is triggered when its rules are triggered. Scenario rules may be "required," "optional," or "exclusion." The scenario is triggered if the required rules are triggered, and the exclusion rules prevent the scenario from being triggered. Optional rules are useful for including extra evidence in the scenario.

- Click on a scenario entry to display the content.

General Tab

Table 19 Scenario - General Tab

Field	Description
Id	Every scenario is given a unique ID by the Security Management Platform
Name	Every scenario requires a unique name, specified by the administrator who creates it.
Description	Space for your comments.
Rich text toolbar	Allows you to modify the description format.
Creation	The date and time that the rule was created and by whom.

Table 19 Scenario - General Tab

Field	Description
Last Update	The date and time the rule was last updated and by whom.
Profiles	Select in which security profiles this rule is active. See sub-section Configuration Profiles and Security Levelsfor further information.

Selected Rules Tab

Table 20 Scenario - Selected Rules Tab

Field	Description
Required Rules	The matching rules must all be triggered in order for the scenario to be triggered. Click **Change** to select or deselect rules that must match.
Optional Rules	Optional rules are not required to trigger the scenario, but they can provide more information in the scenario alert.
Exception Rules	If at least one of the exception rules is triggered within the scenario threshold, the scenario is prevented from triggering for at least the threshold number of seconds.
Fields Matching Matrix	The matrix shows which information items relate to which rule(s).

Threshold Tab

1. Enter a value in the **Duration** field.

The duration is the time frame (in seconds) for considering an event or alert for aggregation or correlation. For example, you could specify that a rule would be triggered ten seconds after its creation.

By default, the duration is set at **3600**.

Actions Tab

The procedure is the same than the procedures in correlation rules. Please refer to section Actions: define the correlation action.

Chapter 6 - Monitoring...

In Security Event Manager, the user can monitor the activity of events, alerts or incidents. He can also get useful information about the SMP mechanism in the event of a performance problem or failure.

This chapter contains information on how to monitor:

- Raw Logs
- Events
- Alerts
- Incidents
- Database
- SMP Performances

Raw Logs

The Logs Forensic module is useful to display a list of raw logs collected in a given time period. This function also enables the user to search for raw logs using a variety of criteria such as date, log sources or contents.

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

The **Forensic Parameters** screen is displayed.

Search for Raw Logs

1. In the **Creation Date** section, using the drop-down lists and fields, indicate the time period during which the raw logs were generated. If you click on the button, a calendar is displayed allowing you to directly select the desired date.

Entering the **Creation Date is compulsory**.

2. If you also want to filter the raw log search according to log source type, select the respective log source in the **Log Sources** section.
To make the log source's selection easier, you can pre-filter the log source list by Organization Unit (OU), asset, site and/or type. To do so, simply select filters from the drop-down lists. The list of available log sources is automatically updated on the left-hand pane.

3. Then, you must decide whether you want to choose one, several or none of them. The selected log sources will be displayed on the right-hand pane.

- If you want to select all the log sources, click on the button.
- If you want to select one or several log sources, select the log sources and click on the button.
- If you eventually decide to remove one or several log sources listed on the right-hand pane, select them and click on the button.
- If you want to remove all the log sources listed on the right-hand pane, select them and click on the button.

4. If you want to filter the raw log display according to content, enter a keyword with a double-quote at the beginning and at the end of the string in the blank field.

5. Select the text string operation (either ***Equals***, ***Begins with***, ***Contains***, ***Matches/Regex*** or ***None/null***.)

Please refer to the list of MySQL regular expressions in the Appendix, "MySQL Regular Expressions" section.

6. Click on **Next**.

The **Private Encryption Key** screen is displayed.

Define the Private Encryption Key

First case

- If the raw logs are still in the database, click **Next**.

Second case

1. If the raw logs are not in the database but they have been archived on your disk according to a previously configured retention period, copy the private key content and paste it in the blank space.

2. Then click on **Next**.

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

Third case

- If the raw logs are not in the database and have not been archived on your disk, the list of files to upload is displayed.

When restoring an archive file, make sure there is enough space in the database. Otherwise, the table called “Exa_Rawlog” may crash and raw logs archived on a daily basis may be lost.

1. Import raw logs by clicking on the **Upload** button.

2. Click on **Add**.

3. Select the raw logs to import by clicking on the **Browse** button.

4. Select the *.gpg file you need.

5. Click **Apply**.

6. Go back to the **Private Encryption Key** screen.

7. Copy the private key content.

8. Paste it in the blank space and click on **Next**.

You must wait until the process is finished. The list of filtered raw logs is then displayed where no more than 10 000 raw logs can be displayed.

> **Note:** The column **Related Event** refers to the raw log’s related **Elementary event ID number** and not the aggregated event one. Therefore, you can not make a search on this **ID**, it is for information only.

Exporting the List of Raw Logs to Excel or PDF Formats

You can export the list of raw logs in Excel and PDF formats. To do so:

1. Click on the **Export** button that you want.
2. In the pop-up screen, select if you want to open the file directly or save it on your disk.
3. Click **OK**.

You obtain an Excel or PDF file with a table containing all the data available in the list of raw logs.

Events

An event (or log entry) is a fundamental element as it represents the original log entries generated by the Log Collector in the IDMEF standard format. It is based on the TIBCO LogLogic® Taxonomy.

The event's content gives unaltered detailed information after passing through the various TIBCO LogLogic® engines.

The event will be used for aggregation and correlation rules relevance and consistency analysis, for forensic search, etc.

There are two types of events:

- elementary events composed of one or several raw logs.
- aggregated events composed of one or several elementary events.

This section contains several procedures to:

- View Events
- Filter Events
- Edit Events

View Events

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

As you have just logged in, the following event is displayed.

The list of aggregated events - i.e. events composed of elementary events grouped according to their similarities - is by default displayed and sorted by “Detected”, that is sorted according to the time the event was detected by the Log Collector **during the last hour**. All the events previously detected are not displayed.

Click on the relevant black header to sort events according to their:

- Severity
- Description (in alphabetical order)
- Log Source (in alphabetical order)
- SLA
- Detected time (by default).

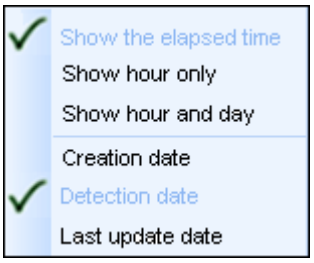
If you want to sort events according to time, you can customize the display by indicating the date format or another type of filter. To do so, either:

- Use the **Display Settings** pane:
  - Click on the **Display Settings** button in the action bar. The **Display Settings** pane is displayed.
  - Select the date format of the event. Several options are available as explained in Table 21 "Date format for event".
  - Select the number of events you want to display in the screen.
  - Select the way you want to refresh the list of events, either in real time or by ordering a time lag. It can be useful if you want to have a bit more time to analyze the events entries.

Note: All the modifications will be automatically saved as soon as you leave this screen and log off from the application.

- Use the right click menu.
  - Right click on the black header. A menu is displayed:

Figure 51 Event time menu



  - Select the date format of the event. Several options are available as explained in Table 21 "Date format for event".

Description

Table 21 Date format for event

Menu entry	Description
Show the elapsed time	Displays the time when the event was detected/created/last updated in days, minutes or hours for the last 7 days. E.g. 6d
Show hour only	Displays the time when the event was detected/created/last updated for the current day in the following format: hh:mm:ss. E.g. 16:28:07
Show hour and day	Displays the time when the event was detected/created/last updated for the current day in the following format: yy-mm-dd hh:mm:ss. E.g. 2008-10-17 16:28:07
Creation date	Displays the date when the event was created.
Detection date	Displays the date when the event was detected by the log source.
Last update date	Displays the date when the event was last updated.

Filter Events

Please refer to the Use of Filters section to configure and apply filters.

Sorting by Severity

To display events by severity (highest or lowest), click on **Severity**. Severity is based on the severity defined in the log.

Events are displayed with icons corresponding to their severity level. Refer to Table 57 "Event - Severity Levels and Corresponding Icons" in the **Reference Guide**.

Sorting by Description

To display events in alphabetical sorting order and according to the classification name they have been given in the aggregation policy, click on **Description** on the black header.

Below the title, a description of the event is displayed in the standardized TIBCO LogLogic® format.

Figure 52 Event description

The message is standardized in a way that allows you to understand that a user succeeded in entering his login.

Sorting by Log Source

To display events in alphabetical sorting order according to the Log source name, click on **Log Source** in the black header.

Sorting by Detected

To display events according to the time when events have been detected by the Log Collector, click on **Detected** in the black header.

Sorting by Event Weight

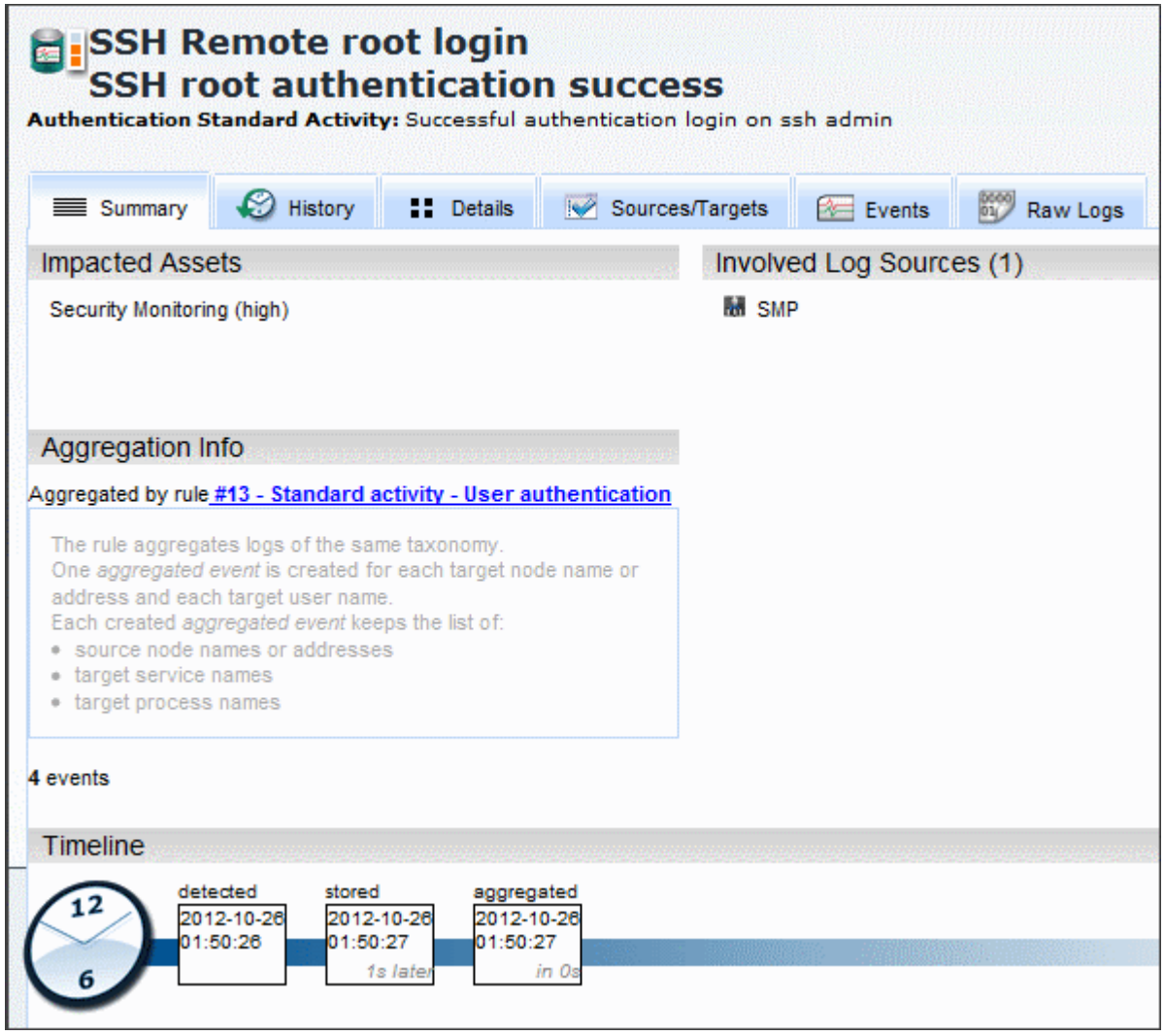
An aggregated event contains several elementary events that have a weight. The weight corresponds to the number of log entries sent and grouped into one elementary event.

Note that the number displayed (e.g. 1) does not correspond to the number of elementary events that composes the displayed aggregated event, but the ***weight*** of the events.

Edit Events

1. Click on the **Description** title to display the details of an event. If you click on an **aggregated event**, the following screen is displayed:

Figure 53 Event Details



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

Description

Table 22 Event Details

Tab	Description
Summary	To get general information about the event.
History	To get information about the event history per days such as 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.
Details	To get information about the alert linked to the event, the type, severity and description of the event...
Sources/Targets	To get information about an event that occurred on a source and/or target machine, by a source and/or target machine user, etc. These columns are for information purpose only. Several icons are used to represent target and source elements (refer to Table 58 "Event - Target and Source" in the Reference Guide to get each icon's description): ▪ Horizontally, all the source or target icons are displayed but only the highlighted icon indicates the type of selected source or target. ▪ Vertically, the icon and its description are displayed. 
Events [only displayed for an aggregated event]	To get information about the elementary events composing the events. Click on the hyperlink to display in a new tab the whole list of elementary events which compose the current aggregated event.
Raw Logs	To get information about the number of online raw logs, the first 5 raw logs online, the last 5 raw logs online and a link to the list of all raw logs online. When clicking on the link, all the online raw logs are displayed in a new tab.

Alerts

An alert contains one or several events enriched with information such as category, vulnerability and impact. Alerts are taken into account by analysts and can generate an incident if needed. Alerts are correlated according to pre-defined rules, which also specify which actions should be carried out when conditions are met.

A top-level alert can be managed in different ways. This section contains several procedures to:

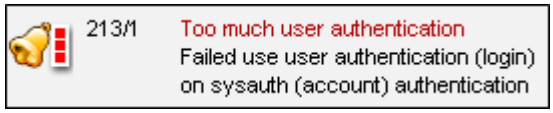
- View Alerts
- Filter Alerts
- Create Alerts
- Edit Alerts
- Acknowledge and Attach Alerts to an Incident

View Alerts

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

You may see the following alert depending on the correlation rule you configured.

Figure 54 Alert description



The list of not acknowledged alerts - composed of aggregated events - is by default displayed and sorted by “Created”, that is to say sorted according to the time the alert was created.

1. Click on the relevant black header to sort alerts according to their:

- Severity
- Number of elementary events that composed events
- Description (in alphabetical order)
- Log Source (in alphabetical order)
- SLA (Service Level Agreement)
- Created time (by default)

2. Clicking again on the active sort heading will alternate between sorting in ascending or descending order.

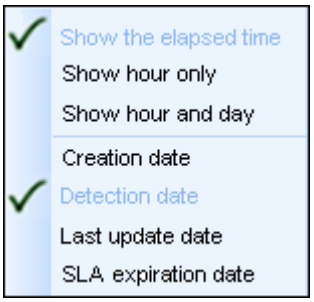
If you want to sort alerts according to time, you can customize the display by indicating the date format or another type of filter. To do so, either:

- Use the **Display Settings** pane:
  - Click on the **Display Settings** button in the action bar. The **Display Settings** pane is displayed.
  - Select the date format of the alert. Several options are available as explained in Table 23 "Date format for alert".
  - Select the number of alerts you want to display in the screen.
  - Select the way you want to refresh the list of alerts, either in real time or by ordering a time lag. It can be useful if you want to have a bit more time to analyze the alerts entries.

Note: All the modifications will be automatically saved as soon as you leave this screen and log off from the application.

- Use the right click menu:
  - right click on the black header. A menu is displayed:

Figure 55 Alert time menu



- Select the date format of the alert. Several options are available as explained in Table 23 "Date format for alert".

Description

Table 23 Date format for alert

Menu entry	Description
Show the elapsed time	Displays the time when the alert was detected/created/last updated in days, minutes or hours for the last 7 days. E.g. 6d
Show hour only	Displays the time when the alert was detected/created/last updated for the current day in the following format: hh:mm:ss. E.g. 16:28:07
Show hour and day	Displays the time when the alert was detected/created/last updated for the current day in the following format: yy-mm-dd hh:mm:ss. E.g. 2008-10-17 16:28:07
Creation date	Displays the date when the alert was created.
Detection date	Displays the date when the alert was detected by the log source.
Last update date	Displays the date when the alert was last updated.
SLA expiration date	Displays the date when the Service Level Agreement will or has expire(d).

Filter Alerts

Please refer to the Use of Filters section in this User Guide to configure and apply the filters.

Sorting by 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.

Table 24 Alert - Severity Levels

Icon	Severity Level
	High
	Medium

Table 24 Alert - Severity Levels

Icon	Severity Level
	Low
	Info
	Unknown

Sorting by Description

To display alerts in alphabetical order, click on **Description** on the black header.

Below the title, a description of the alert is displayed in the standardized TIBCO LogLogic® format.

Figure 56 Event description

The message is standardized in a way that allows you to understand that a user has tried to log in to the system and entered a wrong login or password several times.

Note that using the icon, you immediately know that this is a high-risk behavior.

Sorting by Log Source

To display alerts in alphabetical order according to the Log source name, click on **Log Source** in the black header.

Sorting by Created

To display alerts according to the time when the alert has been created from an event, click on **Created** in the black header.

Sorting by Alert number

The  icon in the black header corresponds to the alert's number.

Note that the number displayed (e.g. 1-6) does not correspond to the number of aggregated and elementary events that compose the displayed alert, but to the ***weight*** of the events.

Indeed, an alert contains aggregated events which contain several elementary events that have a weight. The weight corresponds to the number or log entries sent and grouped into one elementary event.

> **Note:** The number displayed near the alert may sometimes slightly differ from the number displayed near the aggregated events by the time the alert is refreshed.

Create Alerts

If a correlation rule did not work properly and generated an unexpected correlation alert, or if you consider that a specific type of alerts needs a human intervention, then it is advised to create custom alerts manually.

Step 1

1. You can create a new alert by selecting the **Event Management > Create Custom > Alert** menu item.

The **Create Custom Alert** screen opens and lets you configure the alert in 3 steps.

2. Type in a name in the **Alert name** field. The classification text is displayed on the alerts main display and it describes the alert, e.g. "Service stopped."

3. Specify the time when the alert is supposed to be detected. By default, the date is set to today's date.

4. The **Characterization** pane includes IDMEF attributes for the alert. Default values are provided and can be changed, e.g. to create a high-severity alert.

5. Set the TIBCO LogLogic® Taxonomy of the alert in the TIBCO LogLogic® Taxonomy pane by selecting each value in the drop-down lists.

6. Select the log source in the list of previously defined log sources. The log source is the source that generated the event that led to the alert, e.g. an "Intrusion Detection System" could be the log source that reports the event indicating an attack from a source workstation on a target server.

7. The **Advanced Parameters** pane enables you to add further IDMEF information. If advanced parameters are required, enter either the Reference or complementary data panes, and click **Add**.

8. Enter alerts' details 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 in the **Reference** pane.

9. Enter raw IDMEF parameters for which there is no specific GUI interface in the **Complementary Data** pane.

Step 2 - Sources

The second step is used to specify the alert source(s). For each source define its hostname.

Source Host(s)

1. Click **Add.** The **Add Host** pane is displayed.

2. Either select the hostname that has been previously defined in the asset database or simply enter the hostname by clicking on **Manually Referenced Host**. The host can have multiple nodes, e.g., if a host has multiple DNS names there can be one node for each name.

3. Click **Next**.

Source Address

1. In the **Add Host** screen now displayed, click **Add** to add each new IP address(es).

2. Define the IP address. The netmask and VLAN information are optional.

Note: If necessary, the IP address can be removed by ticking the selection box at the beginning of the line and clicking the delete button.

Source Port

The source port is defined next, either as an individual port or as a list (e.g. 138-139,445).

Source Interface

The actual network interface of the source device can be specified. This is useful when identifying which IP address has been spoofed on which interface.

Entry

1. Further sources can be entered, e.g. in the case of a Distributed Denial of Service attack where multiple sources have been used to overload a server. Otherwise, click **Next** to finish adding sources and move to the third step.

Step 3 - Targets

Entry of target hosts(s) is the same as entry of source hosts.

1. When you have added the target host information, click **Next**.

The results of the alert creation are displayed.

2. Click **OK** to close the screen.

The alert can then be seen on the main display.

Edit Alerts

1. Click on the **Description** title to display the details of an alert. The following screen is displayed:

1. Click on the **Summary** tab to get general information about the alert.

2. Click on the **History** tab to get information about the alert history per days such as 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.
- how many events this event contains.
- SLA details (respected or not).
- the rule used for the alert generation.

3. Click on the **Details** tab to get information about the alert linked to the event, the type, severity and description of the event...

4. Click on the **Sources/Targets** tab to get information about an event that occurred on a source and/or target machine, by a source and/or target machine user, etc. These columns are for information purpose only. Several icons are used to represent target and source elements (refer to Table 61 "Alert - Target and Source" in the Reference Guide to get each icon's description):

- Horizontally, all the source or target icons are displayed but only the highlighted icon indicates the type of selected source or target.
- Vertically, the icon and its description are displayed.

Figure 57 Example of target display

5. Click on the **Alerts/Events** tab to get information about the elementary events composing the event in the alert. Click on the hyperlink to display in a new tab the whole list of elementary events which compose the current aggregated event.

Acknowledge and Attach Alerts to an Incident

Acknowledging Alerts

Acknowledging an alert is a user-performed task indicating that the user is aware of the alert and shall cope with it.

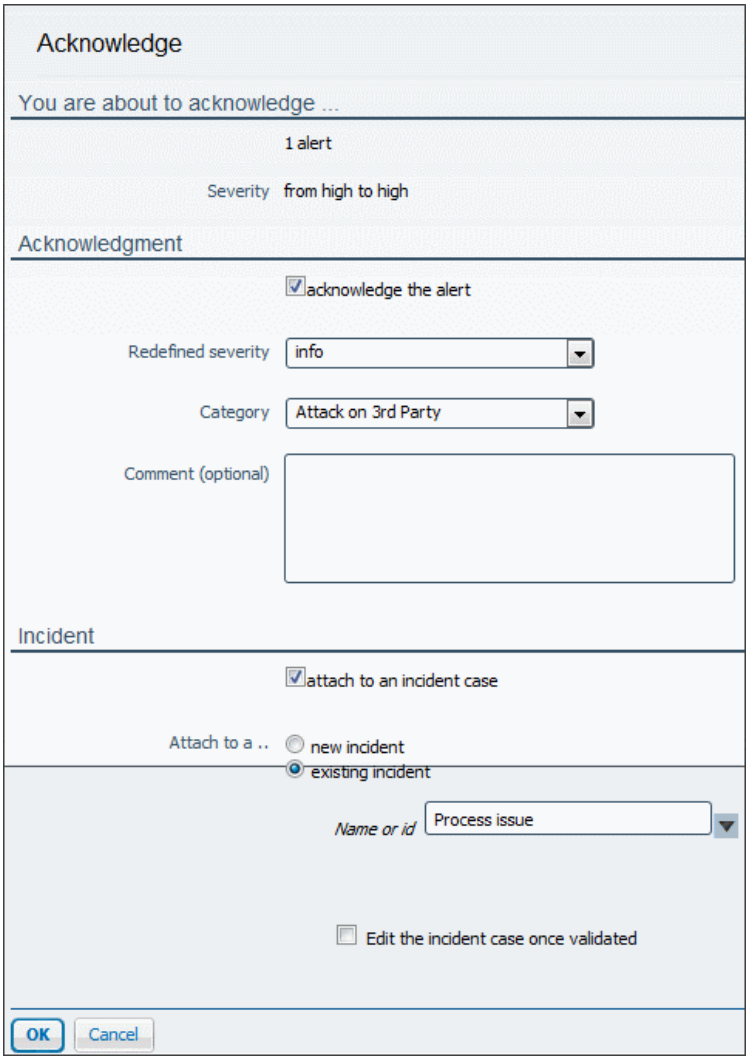
To acknowledge alerts:

1. First tick the box in the first column of the alert(s) you wish to acknowledge.

2. Once the alerts are selected, click on the **Acknowledge** button.

The **Acknowledge** screen is displayed:

Figure 58 Acknowledge



3. Select the **Acknowledge the alert** checkbox.
4. If necessary, redefine the severity level.

> **Note:** If you define the alert as “false positive,” the severity level will automatically be set to “info”.

5. Select the acknowledgement category from the drop-down list.
6. Optionally, add a comment.
7. Click **OK**.

The alert is no longer displayed in the list. If you want to display the acknowledged alerts, create a relevant filter. For more information, refer to sub-section Creating a Filter.

Attaching Alerts

To attach alerts to an incident:

1. Select the **Attach to an incident case** checkbox.
2. Click the relevant radio button to select the incident linked to the alert. It can be a new incident or an already existing incident.
3. If you selected **existing incident**, you can enter the incident name or ID.

4. Select **Edit the incident case once validated** to display the details of the incident you have just created. The incident detail will be immediately displayed once you have clicked on **OK**.

5. Click **OK**. The **Incident Edition** screen is automatically displayed for you to add detailed information.

6. Click on the **Incident** tab to view that a new incident is now available in the **Incident** list.

Note: If you decided to attach the alert to an existing incident, this incident will be updated.

Incidents

An incident can be managed in different ways. This section contains several procedures to:

- View Opened Incidents
- Filter Incidents
- Creating a New Incident from Alerts
- Create Incidents Manually
- Edit Incidents
- Close Incidents

View Opened Incidents

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

Here is an example of a display of an incident.

Figure 59 Incident description

By default, the **Incident** management system enables you to view and close opened incidents. You can also filter the display and get the list of closed incidents only.

1. Click on the relevant black header to sort events according to their:

- Severity
- Description (in alphabetical order)
- SLA (Service Level Agreement)
- Modified (by default)

2. Clicking again on the active sort heading will toggle between ascending or descending sorting order.

If you want to sort incidents according to time, you can customize the display by indicating the date format. To do so:

a. Use the **Display Settings** pane. Click on the **Display Settings** button in the action bar. The **Display Settings** pane is displayed.

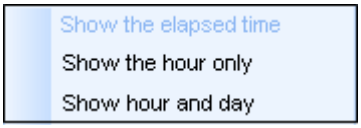
- Select the date format of the incident. Several options are available as explained in Table 25 "Date format for incident".
- Select the number of incidents you want to display in the screen.
- Select the way you want to refresh the list of incidents, either in real time or by ordering a time lag. It can be useful if you want to have a bit more time to analyze the incidents entries.

Note: All the modifications will be automatically saved as soon as you leave this screen and/or log off from the application.

b. Use the right click menu.

- Right click on the black header. A menu is displayed.

Figure 60 Incident time menu



- Select the date format of the incident. Several options are available as explained in Table 25 "Date format for incident".

Description

Table 25 Date format for incident

Menu entry	Description
Show the elapsed time	Displays the time when the incident was detected/created/last updated in days, minutes or hours for the last 7 days. E.g. 6d
Show hour only	Displays the time when the incident was detected/created/last updated for the current day in the following format: hh:mm:ss. E.g. 16:28:07
Show hour and day	Displays the time when the incident was detected/created/last updated for the current day in the following format: yy-mm-dd hh:mm:ss. E.g. 2008-10-17 16:28:07

Filter Incidents

Please refer to the Use of Filters section to configure and apply the filters.

Sorting by 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.

Table 26 Incident - Severity Levels and Corresponding Icons

Severity Level	Closed Incident	Opened Incident	Processed Incident	Reopened Incident
High				
Medium				
Low				
Info				
Unknown				

Note: Opened incidents have actions that need to be performed before being closed.

Sorting by Description

To display the incident in alphabetical order on the classification name, click on **Description** on the black header.

Below the title, a description of the incident in the standardized TIBCO LogLogic® format is displayed.

Figure 61 Incident description

Note that thanks to the icon, you immediately know that this is a medium incident.

Sorting by 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.

Other non-clickable columns

Five other columns - , **Impacted assets, Actions, React** and **Modified -** are also available. However, you cannot sort an incident according to this type of information. These columns are for information purpose only.

- The  column allows you to display the alerts attached to the incident.
- The **Impacted assets** column allows you to get the list of assets associated with targets and sorted by descending criticality order.
- The **Actions** column allows you to get the list of actions performed or not performed on an incident.
- The **React** column 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.
- The **Modified** column allows you to view the person who modified the incident and the time when it was modified.

Creating a New Incident from Alerts

To create an incident from one or more alerts:

1. Click on the **Alerts** tab.

2. Tick the box in front of the alert(s) you wish to create an incident from.

You can select as many alerts as you want.

3. Click on **Acknowledge** button**.** The **Acknowledge** screen is displayed.

4. Select **Attach to an incident case** in the **Incident** part of the screen.

5. Select the relevant radio button whether you want to attach the alert to a new incident or to an existing incident.

If you want to attach the alert to an existing incident, the relevant incident is selected.

An input field is also displayed for you to enter an incident ID if you remember the ID number instead of the incident title.

6. Select the **Edit the incident case once validated** checkbox to display the incident details immediately after its creation. You will be able to add information about the incident if necessary.

7. Click **OK** to validate the creation of the incident.

> **Note:** When creating an incident from alerts, the most critical existing SLA will be taken into account and applied to the current incident.

Create Incidents Manually

To create an incident from scratch, select the **Event Management > Create Custom > Incident** menu item.

General Tab

Fill in the following panes. Those marked with an asterisk (*) are required.

1. Enter a short description of the incident. This will be used in the incidents list along with an incident number. More details about the incident can be entered in the **Incident Description pane**.

2. Select whether the incident status is **opened** or **closed**. When creating an incident the status is set to **opened**.

3. In the **Contacts** list, select the user who will handle this incident. Use CTRL-click and SHIFT-click to select multiple contacts.

4. Enter the time and date the incident was detected and created in the **Detection Time** and **Start Time**.

- Dates are entered in the format `Year / Month / Day`.
- Times are entered in the format HH:mm.

  The date can either be directly entered in the **Time** fields in the YYYY/MM/DD format or selected in the calendar (opened by clicking on the calendar icon).

5. Select one or more log sources from the drop-down list. Typically the log source generates the alert. If multiple alerts from multiple log sources have been correlated, then multiple log sources can be selected from this list. Use CTRL-click and SHIFT-click to select multiple log sources.

6. You can indicate the timeframe within which the incident has to be closed. Click on **Change** and specify a SLA deadline or a specific time duration (in hours).

- If you select **by date**, you must enter a deadline (date and time).
- If you select **by time extension**, select a number of hours in the appropriate drop-down list.

  In the **Assessment** pane, you must define the impact the incident has had by displaying several attributes.

7. Select the incident severity level from the **Severity** drop-down list. The incident will be displayed with an icon corresponding to the severity level. Refer to "Edit Incidents" for more information on severities.

8. Modify the category by selecting if the incident is:

- a TIBCO LogLogic® event
- emergency changes
- a network noise
- an unauthorized activity
- a false positive
- a true security alert
- an attack on a third part
- an authorized activity
- unknown
- an authorized security testing
- a known error

9. In the **Completion** field, select either **failed** or **succeeded,** depending on whether the alert corresponds to a successful event or not.
Example: If the event refers to the deletion of a file, set completion to **succeeded**, if the file deletion was blocked by access controls, set completion to **failed**.

10. Select one of the following types of incidents from the **Type** drop-down list.

Table 27 Incident Types

Type	Description
admin	Administrative privileges were attempted or obtained
dos	A denial of service was attempted or completed
file	An action on a file was attempted or completed

Table 27 Incident Types

Type	Description
recon	A reconnaissance probe was attempted or completed
user	User privileges were attempted or obtained
other	Anything not in one of the above categories

11. In the **Confidence** field, select the value to represent the analyzer's best estimate of the analysis' validity. Approximate values are specified as high, medium or low. Numeric values are a percentage confidence level.

Properties Tab

1. The **Effects** pane is used to describe the impact the incident has had:

- **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**.

2. The **Time Impact** pane is used to describe the time impact the incident has had:

- Select the severity of this particular event: info, low, medium, high.
- Enter the time value during which the incident (e.g. a machine shutdown) lasts.
- Select the Metric (or type) to define the type of time it is: labor, shutdown or elapsed.
- Select the unit corresponding to the value entered: seconds, minutes, hours or days.

3. The **Monetary Impact** pane is used to describe the monetary impact the incident has had:

- Enter the value corresponding to the amount the incident will cost.
- Select the severity of this particular event: info, low, medium, high.
- Select the currency corresponding to the value entered: dollar, euro, pound.

4. Enter the necessary information to make a link with online vulnerability database in the **References** panel.

- Select the origin of the additional information from the drop-down list.

Table 28 Origin of Incidents

Origin	Description
unknown	Origin of the additional information is not known
vendor-specific	A vendor-specific name can be used to provide product-specific information
user-specific	A user-specific name can be used to provide installation-specific information
bugtraqid	The SecurityFocus ("Bugtraq") vulnerability database identifier (http://www.securityfocus.com/vdb)
cve	The Common Vulnerabilities and Exposures (CVE) name (http://cve.mitre.org/)
osvdb	The Open Source Vulnerability Database (http://www.osvdb.org)

- Type in the name of the reference as specified by the originator, e.g. an CVE identifier such as CVE-1999-1057.
- Type in the URL that points to the reference information.

Note: The URL will be automatically generated for bugtraqid, cve and osvdb.

- Click **Add** and repeat the procedure for each reference.

Sources tab

The **Sources** tab is used to select the incident source(s). Click **Add** for each source involved.

Two choices are available:

- Select the source if it already exists in the asset database.
- Create a new host in the asset database by clicking **Add.**

The following screen is then displayed.

1. In the **Host** pane, do the following:

- If the host is already in the asset database, click on the **Host referenced** radio button, select the host from the drop-down list and select the **Network Node** that identifies the hostname and naming convention to be used to identify this host. Typically this is the DNS nodename, but other naming systems such as NIS may be used, in that case select the node name and the type from the drop-down list.
- If the source host is not required to be in the asset database, click on the **Manually referenced host** radio button and enter its name.

2. Click **Next**. The following screen is displayed.

3. In the **Addresses** pane, click **Add** to enter details about the source host IP addresses:

- VLAN identifiers (optional).
- IP address.

If the host has IP address information defined in the asset database you can use the information displayed. If the address information for this incident needs to be specified, click on the first **Add** button and enter the IP address.

4. In the **Services** pane, click **Add** to specify the IP ports used by the source that can be added to the incident detail.

For each port, a number or list can be specified, as some protocols involve more than one port and the incident may involve more than one protocol (TCP, UDP or ICMP).

5. In the **Interface** pane, indicate the source network interface that may be of interest to the incident handler, especially if the IP address has been spoofed. Enter the interface name and whether spoofing has occurred in the **Interface** pane.

6. Once the source details are correct, click **Finish**.

> **Note:** If further sources are involved in the incident, they can be added by clicking **Add**. Once all sources have been entered, click **Next**. If the entry of a source was incorrect, it can be edited by clicking on the source name which is in blue, or deleted altogether by ticking the box at the beginning of the row and clicking **Delete**.

Targets tab

1. Entering target details is the same as entering the source details from step 1 to step 4. Please refer to the steps described in "Sources tab".

2. In the **Interface** pane, indicate the target network interface that may be of interest to the incident handler, especially if the IP address has been decoyed. Enter the interface name and whether decoy has occurred in the **Interface** pane.

3. Once the source details are correct, click **Finish**.

Attack Methods tab

The **Attack Methods** tab allows you to indicate if the incident involves any attacks (malicious or otherwise).

Table 29 Attack Methods

Attack Method	Description
Malicious code	
Activate	Activates the options available below.
Type	Select whether the malicious code is: ▪ Virus ▪ Trojan ▪ Worms ▪ Spyware
Name	Indicates the name of the malicious code.
Action mode	Indicates whether the malicious code execution mode is: ▪ coming from a macro ▪ appearing when starting the system ▪ resided in memory ▪ a self-changing virus ▪ self-encrypted ▪ hidden
Infected software	Indicates where the infection occurs.

Table 29 Attack Methods

Attack Method	Description
Effects	Indicates the effect it has on the infected software, such as: ▪ erase of data ▪ modification ▪ ciphering
Scan	
Activate	Indicates if an attack occurred via a port scan, e.g. by vulnerability scanner.
Intrusion	
Activate	Activates the fields to define the exploitation of a vulnerability
Password	The intrusion occurred through a password that was: ▪ cracked ▪ intercepted ▪ guessed
Access by trusted host	The intrusion occurred via a trusted host.
Backdoor	The intrusion occurred via a backdoor.
Social engineering	The intrusion is caused by a human factor (password orally given...)
Unusual process used	The intrusion is caused by something unusual.
Hack tool used	The intrusion is caused by a hack tool.
Denial of service	
Activate	Activates the fields to define the overloading of a service so it is unavailable to other users.
Packets saturation	Packets are saturated.
Malformed Packets	Packets are abnormally constructed.
Spoofed Address	The address has been spoofed.
Other	Other type of denial of service.
Other	
Activate	Activates the field to define the other type of attacks
Other	Allows you to enter the other type of attack not listed above.

Actions tab

The **Actions** tab allows you to specify which remedial actions are required for this incident. Later, as the incident is handled, the actions will be marked as done and the incident can be closed when all required actions have been performed.

1. Tick the box in the **Expected** column for each action that is required. If applicable, fill in further details in the corresponding check-boxes.

2. When the actions(s) have been **completed,** tick the corresponding box. This can be done during the creation of an incident or later when the incident is updated.

Table 30 Selection of Incident Remedial Actions

Checkbox	Description
Antivirus	Antivirus work is required. Select the box and select **acquired**, **updated** or **new** depending if the antivirus has to be installed, updated (e.g. with new versions or signatures) or purchased.
Changes of Policy	Changes to policy or procedures involve rewriting or updating documentation and not technical fixes.
System off-line	The affected host has to be shutdown or disconnected from the network temporarily.
Patching	Patching is required after an incident. Select the box and list the required patch(es) in the data column.
Scanner turned on	Vulnerability scanners must be configured to scan the affected hosts.
Security software installed	Security software must be installed. Select the box and, in the data column, indicate which software should be installed.
Useless services and applications stopped	The incident is due to an unnecessary service or application (e.g. a vulnerability in one of these was exploited), stopping or removing these can fix the problem.
Applications moved to another server	Moving the application(s) is required, e.g. moving it to a higher security-level server.
Space Disk or Memory increased	The incident is related to a lack of disk-space or memory.
Malicious code identified and erased	Virus, spyware, trojans, etc. may need to be analyzed by an anti-virus company before a disinfection method is available.
Password changed	Incidents due to weak or divulged passwords will require a password change.
Other	You need to add comments on other required actions. Select the box and enter your comments in the data column.
Impact	Enter your description if you want to describe the effects of these actions.

1. Click on **OK** to create the incident. A new incident has now been created in the list of **Incidents**.

Send the Incident to the Help Desk

If you have configured a help desk as explained in the ***Administration Guide***, a checkbox appears next to the **OK** and **Cancel** buttons.

- Click on the **Send the created incident to the help desk** to notify that a new incident has been created.

Edit Incidents

If necessary, you can edit an opened incident in order to modify the incident status, SLA, severity, and category. To do so:

1. Click on the incident title.

2. In the **Incident Details** screen, modify the data available for edition.

The procedure to modify an incident is the same as explained in section Create Incidents Manually. The only difference is the **History** tab where you can see the date and description of the selected incident.

3. Click **OK** for the modifications to be applied.

Close Incidents

Once an incident has had all required remediation actions performed, it can be closed by the analyst. Closed incidents are displayed separately from open incidents, but the process of selecting incidents with filters and refreshing the display is the same as above.

To close incidents:

1. First tick the box in the first column of the respective incident(s) you wish to close. Note that to select all incidents, you must click the box at the top of the first column.
2. Once the incidents are selected, click on **Close Incidents**.

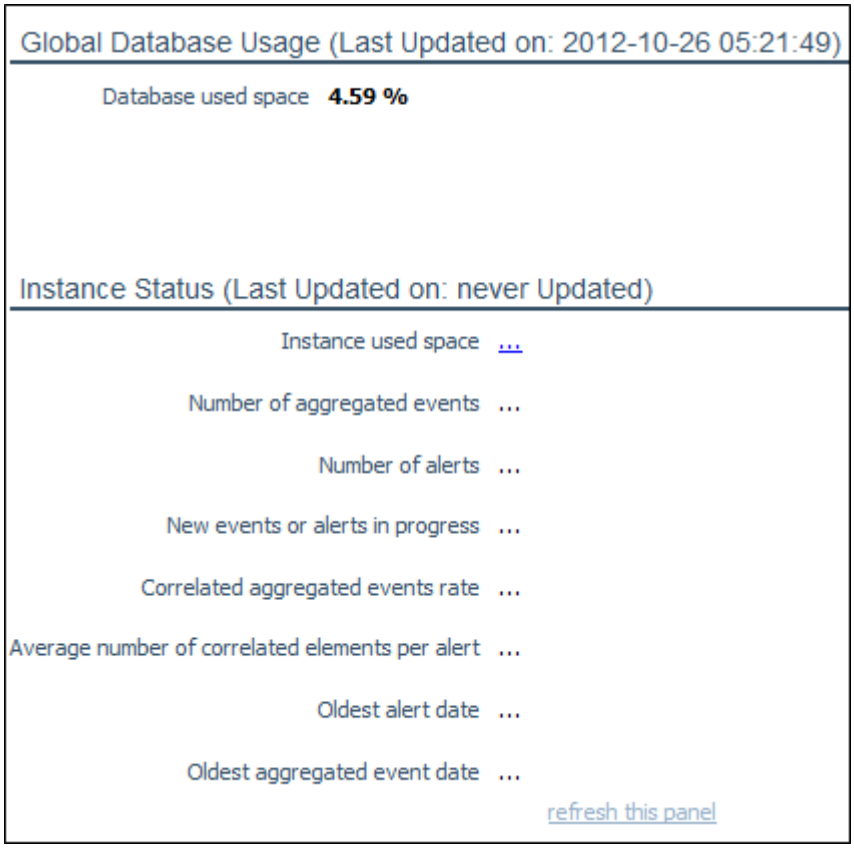
When closing an incident, the alerts contained in the incident are acknowledged according to the incident's category.

Database

The database configuration screen displays key statistics about the database.

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

Figure 62 Database Status



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

Please refer to "Database Statistics" in the ***Reference Guide*** for further information.

SMP Performances

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

Live Explorer Tool

The Live Explorer is a debugging tool which gives you information about the event treatment process. In other words, it gives a graphical representation of the TIBCO LogLogic® SMP mechanism.

This tool is helpful to check if there is:

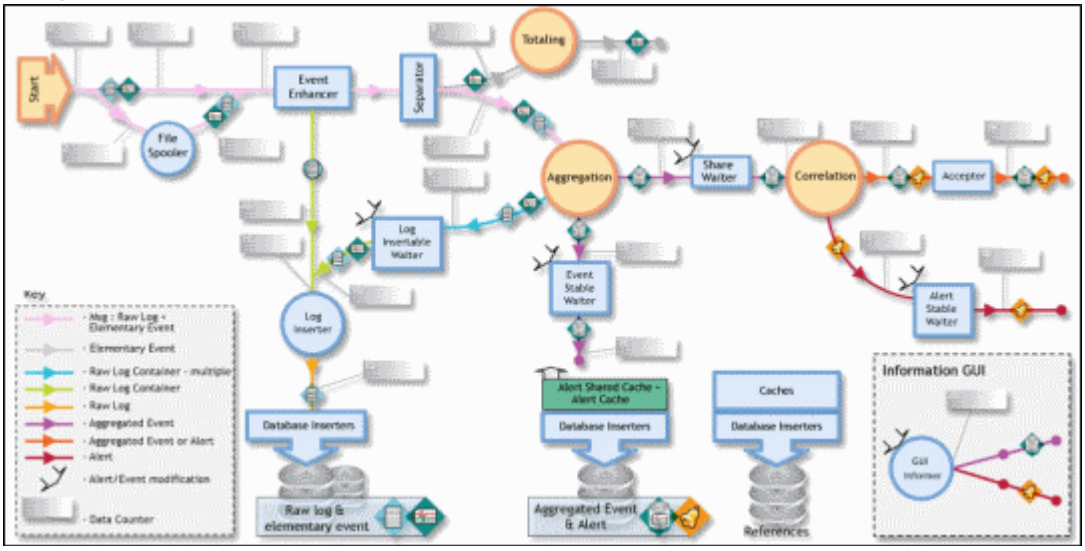
- A flood of events.
- A loss of events.
- A problem with an engine.

By default, the graph shows the average number of EPS for the last minute (**Average** radio button selected).

- If you want to display the total amount of events passing through the engine since the first restart of the SMP, select the **Total** radio button.
- If you want to display information in the last second, select the **last sec.** radio button.

The main objects contained in the SMP are represented as follows:

Figure 63 Live Explorer



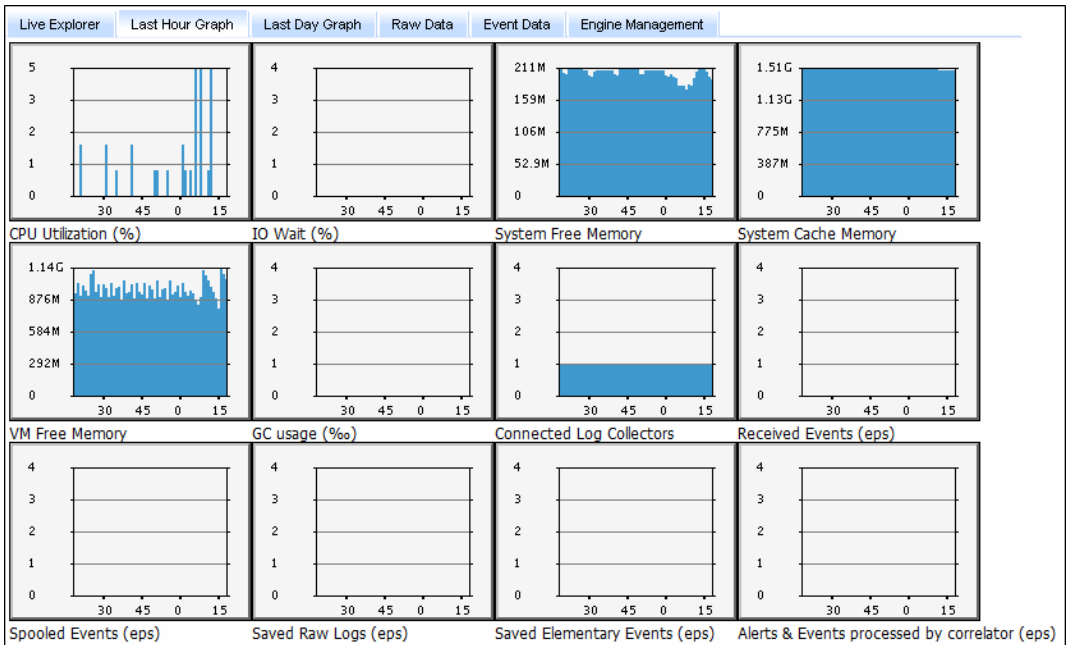
Refer to the ***Reference Guide*** - section Live Explorer Tab to get a description of the screen.

Consult the Other Graphs

Last Hour Graph

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

Figure 64 Live Explorer: Last Hour Graph Tab



Last Day Graph

The Last Day Graph graphically displays data for the current day. It is useful to make comparisons for longer periods of time. The last day graph is the same as the last hour graph except that it graphically displays the SMP server performance on a daily basis. This graph will be useful later to make a general comparison on a weekly basis for example.

Raw Data Graph

The Raw Data graph sums up all information in a text format. It gives precise information about the SMP server performance.

Event Data Graph

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

Engine Management Graph

The Engine Management graph displays the three main SMP engines.

For a detailed description of these tabs, refer to the ***Reference Guide*** - section SMP Monitoring.

Chapter 7 - Reporting

The Reporting menu allows the user to create relevant and intelligent security dashboards by giving a graphical representation of real-time security data movements within the network.

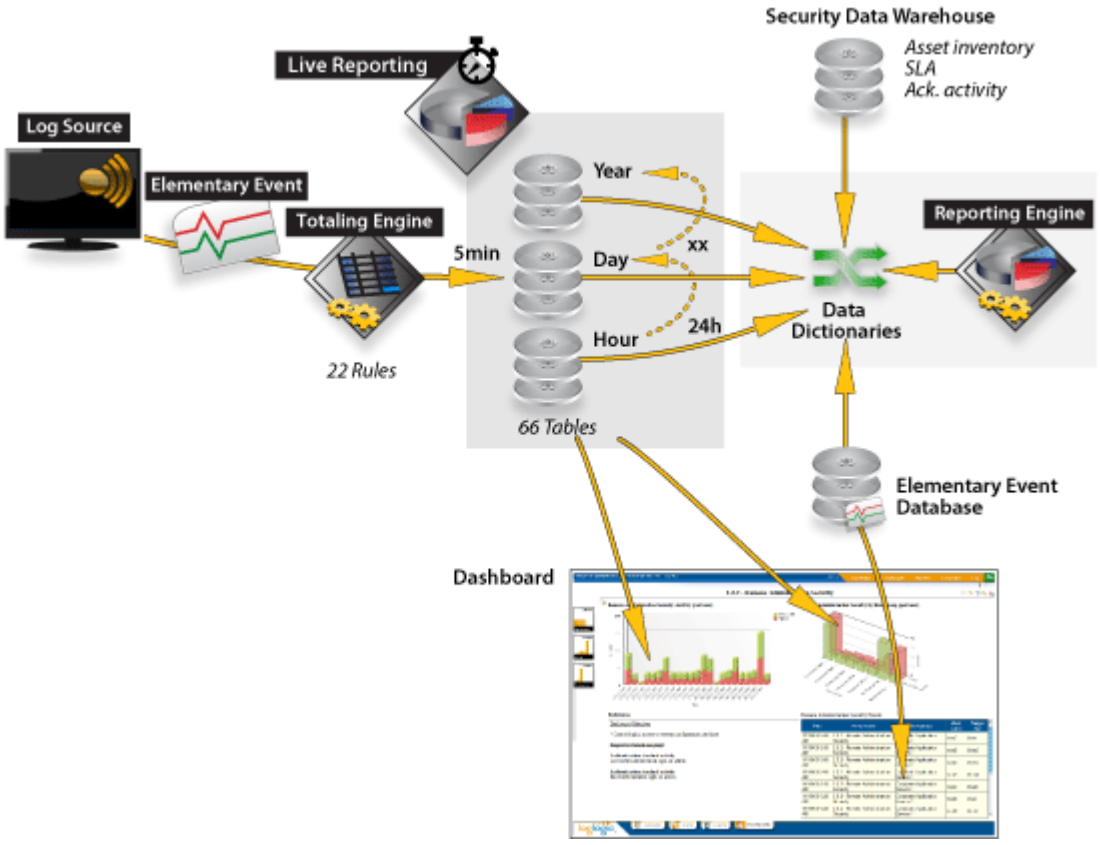
This chapter contains information about:

- Security Dashboards
- Security Dashboards: from Compliance to Technical Reporting
- Live Reporting Policy
- Batch Reporting Policy

They all form part of the **Reporting Engine** which allows the generation of reports.

The principle of the **Reporting Engine** can be represented as follows.

Figure 65 Reporting Engine principle



Security Dashboards

A dashboard is a set of reports. A report is a graphical representation of the number of alerts, incidents and/or vulnerabilities. You can display real-time reports, that is to say, reports based on raw logs.

This section shows you how to:

- Open the Security Dashboards Screens
- Use Default Dashboards

Open the Security Dashboards Screens

To access the **Reporting** module, you must go to **Reporting > Security Dashboards** in the menu bar or click on the **Dashboards** tab.

A table giving an overview of the content of the dashboard module is displayed:

Figure 66 Default Dashboard Display

	Content	Type		Time Scale			
		Dynamic	Static	Hour	Day	Month	Year
Home	Dashboards welcome page. It summarises the reporting content, accessible from the top left menu.						
1 - Access Control Security	User access, account management and remote access to systems.			●	●	●	●
2 - Operation Security	Basic IT operations: malware, viruses, e-mails, network, alerts, configuration management...	●		●	●	●	●
3 - Asset Security	Dedicated to the security of assets identified in the Asset Database: changes and backup activities, capacity management, vulnerabilities status and availability for each asset.	●		●	●	●	●
4 - Executive Reports	Combines all previous security dashboards in a single monthly report.		●		●	●	
5 - Regulatory Compliance	Reports specific for each of the main regulations (FSA, PCI-DSS, SOX). References for mapping to main regulations and standards (ISO 27002, CobiT 4.1, ...)		●		●	●	
6 - SANS Top 5	EventManager dashboards recommended by the SANS (SysAdmin, Audit, Network, Security) Institute in its "Top 5 Essential Log" document.	●		●	●	●	●
7 - PDF Reports	Executive Reports (part 4) and Regulatory Compliance Reports (part 5) . These reports are automatically generated in PDF format at the end of each month.		●		●	●	
Configuration	Access to reporting environment configuration.						

TIBCO LogLogic® dashboards and reports are contained in folders that can be divided into seven groups. These groups are:

Group 1

1 - Access Control Security

1.1 - Account Management

1.2 - User Access

1.3 - Remote Access

These reports are based upon standards.

Group 2

2 - Operation Security

2.1 - Malware Protection

2.2 - Data Exchange

2.3 - Operation Security Management

2.4 - Network Security

2.5 - Incident and Alert Management

2.6 - Log & Event Management

These reports are based upon standards.

Group 3

3 - Asset Security

3.1 - Asset Identification

3.2 - Change Management

3.3 - Backup Management

3.4 - Capacity Management

3.5 - Vulnerability Management

3.6 - Asset Availability

These reports are based upon standards.

Group 4

- Monthly Executive Report

The **Monthly Executive Report** combines all default security reports from Groups 1, 2 and 3 in a single static monthly report. It provides a monthly overview of the whole enterprise IT security status.

Group 5

5 - Regulatory Compliance

5.1 - Standards Mapping

5.2 - FSA

5.3 - PCI-DSS

5.4 - Sarbanes-Oxley

These reports are based upon regulations.

Group 6

6 - SANS Top 5

6.1 - Attempts to Gain Access Through Existing Accounts

6.2 - Failed File or Resource Access Attempts

6.3 - Unauthorized Changes to Users, Groups and Services

6.4 - Systems Most Vulnerable to Attack

6.5 - Suspicious or Unauthorized Network Traffic Patterns

These reports are based upon the TOP 5 established by the SANS Institute. To get the SANS official report about the TOP 5 essential log reports, refer to http://www.sans.org/resources/top5_logreports.pdf.

Group 7

7 - PDF Reports

7.1 - Executive

7.2 - FSA

7.3 - PCI-DSS

7.4 - Sarbanes-Oxley

7.5 - Other Reports

These folders contain dashboards that are automatically generated each month in pdf format. You have then constant access to a monthly system activity report that can be useful for an audit.

Use Default Dashboards

Displaying a Default Dashboard

1. Click on the  icon and deploy the tree structure until you display the relevant dashboard.

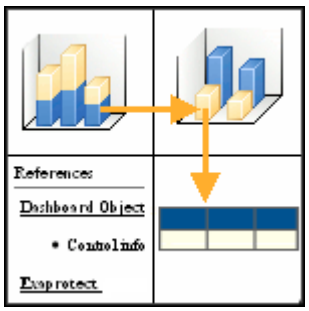
2. Click on the relevant dashboard's entry. The dashboard interface is divided into four main areas:

- The upper-left area displays a graph, e.g. System Access Activity per hour.
- The upper-right area displays a more precise graph, e.g. System Access Activity per host group per hour.
- The down-right area displays the events or logs that were used for the report generation.
- The down-left area entitled **Reference**s contains various information about the dashboard, such as a description, the related TIBCO LogLogic® Taxonomy used to generate the dashboard and the compliance with security standards.

Exploring dashboard data

The Drill-Down Approach

To explore dashboard data, the Drill Down approach is used. This approach can be represented as follows:

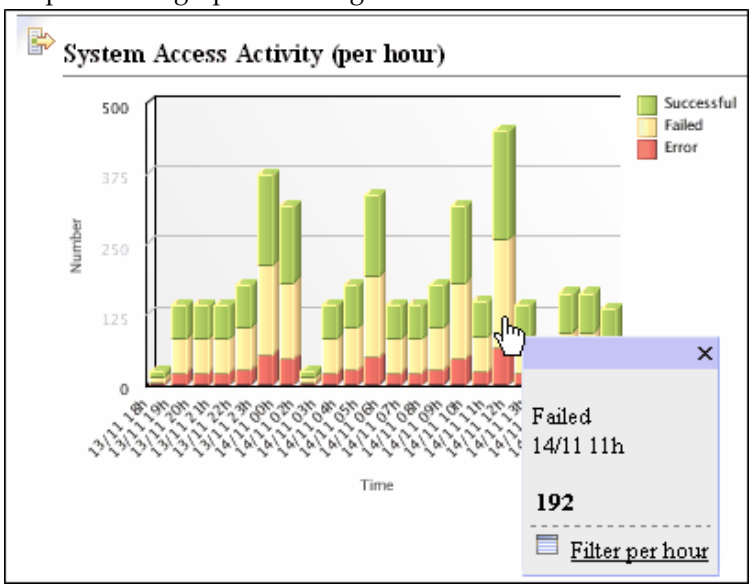


The orange arrows correspond to the dynamic links between the different reports.

Here is a real example.

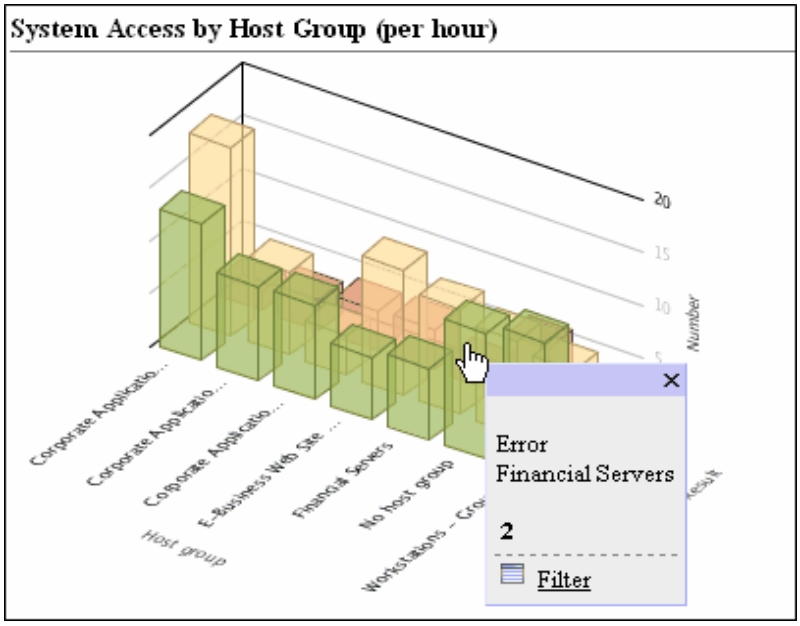
- If you click on the upper-left graph, a pop-up screen is displayed asking you to filter data.

This updates the graph on the right.



- If you click on the upper-right graph, you can update the table below by displaying updated events.

Figure 67 Filter on the upper-right graph to update the table below



Note: This action is mandatory to display the table if you work on a hour-type dashboard with a list of events.

- The table containing the events reference is updated:

Figure 68 The table is updated

System Access TOP (per hour)

#	Target user	Result	Host group
80	User5	Failed	Corporate Application Servers 1
53	User4	Successful	Financial Servers
28	User4	Failed	No host group
28	User4	Successful	Corporate Application Servers 1
27	User	Error	No host group
27	User3	Successful	No host group
27	User4	Successful	Corporate Application Servers 2
26	User	Failed	E-Business Web Site Servers
26	User2	Successful	Corporate Application Servers 2
26	User3	Error	Workstations - Group 2

Caution: When clicking on a dynamic link, wait a little before clicking on another link as the refreshing process may take time.

Three Different Views and Scales

You can display the same type of dashboards based on a different time unit (hour, day or month).

Figure 69 The three different scales: Hour, Day and Month

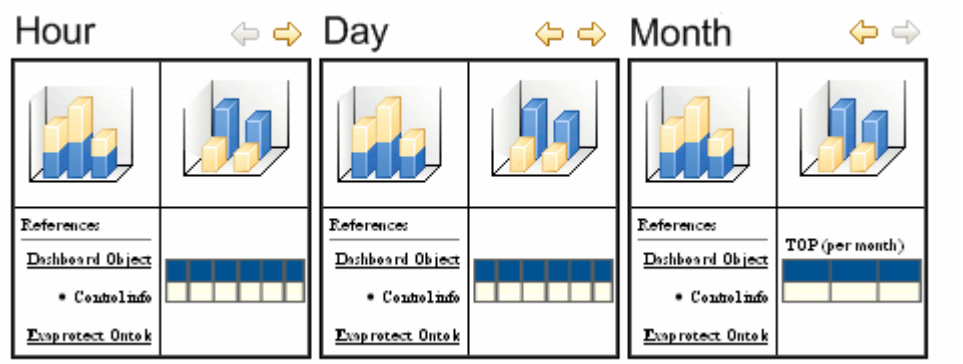
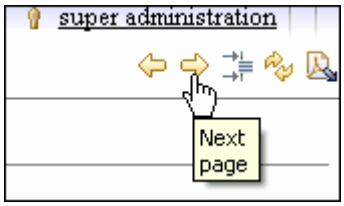


Table 31 The three different scales: Hour, Day and Month

Scale	Description
Hour	displays Elementary Events.
Day	displays Elementary Events and TOP 100 events.
Month	displays TOP 100 events.

To navigate between the different graphs, click on the upper right arrows to navigate between the dashboards.



Executive Compliance Dashboard

The **Executive Security Report** combines all default security dashboards in a single static monthly report. It provides a monthly overview of the whole enterprise IT security status. Security controls covered by EventManager are divided into three main parts:

1 - Access Control Security

This section provides information on user access, account management and remote access to systems.

2 - Operation Security

This section contains basic IT operation information: malware, viruses, emails, network, alerts, configuration management...

3 - Asset Security

This section is dedicated to the security of assets identified in the Asset Database: changes and backup activities, capacity management, vulnerabilities status and availability for each asset.

Location

To preview the dashboard, select **Home > Executive Report > Monthly Executive Report**.

The PDF file is located in:
`/var/lib/exaprotect/archives/<INSTANCE>/report/pdf/executive`

Note: The **Executive Security Report** is optimized for printing (A4 paper format).

Security Dashboards: from Compliance to Technical Reporting

This section gives an overview of the three main themes that will help you understand how to work with TIBCO LogLogic® reporting tool in terms of compliance.

Themes are:

- Regulations.
- Standards.
- Technical Reporting.

Overview

Regulations

In order to gain a maximum level of security in their business IT infrastructure, each company is entitled to follow and apply security laws and regulations, e.g. as SOX regulation underlines, a secured IT is mandatory to secure financial assets.

Main laws and regulations are:

- Basel II Accord.
- Federal Information Security Management Act of 2002 (FISMA).
- Financial Services Authority (FSA).
- Gramm-Leach-Bliley Act (GLBA).
- Health Insurance Portability and Accountability Act (HIPAA).
- Loi sur la Sécurité Financière - Financial Security Law of France (LSF).
- Markets in Financial Instruments Directive (MiFID).
- Payment Card Industry Data Security Standard (PCI-DSS).
- Sarbanes-Oxley Act of 2002 (SOX).

As laws and regulations are - in their vast majority - subdued to each countries' jurisdiction, the choice made by TIBCO LogLogic® is to work with their related ***standards.*** Indeed, standards can be easily applied, no matter the country.

Standards

Law and Regulation standards are composed of a list of measures, processes and best practices intended to help security managers in their security development process and daily use.

These detailed procedures can be easily followed.

Main supported standards are:

- ISO 27002:2005:
- Control Objectives for Information and related Technology (COBIT), e.g. adopted by public companies that are subject to the U.S. Sarbanes-Oxley Act of 2002.
- Payment Card Industry Data Security Standard (PCI-DSS) v1.2.

Technical Reporting

Companies are usually audited on a regular basis. Auditing information security covers topics from auditing the physical security of data centers to the auditing logical security of databases and highlights key components to look for and different methods for auditing these areas.

This particular appointment needs an important preparation as well as a structured information gathering.

TIBCO LogLogic® offers a comprehensive solution through its reporting module. Indeed, dashboards and reports take ***standards*** controls (organizational, technical...) as reference to construct business and security-oriented dashboards.

To evaluate and monitor each standard control, reports based on technical data collected by Security Event Manager are provided.

The TIBCO LogLogic® Solution

TIBCO LogLogic® innovative reporting tool can help you prepare audits and offer a clear and useful representation of your IT security environment through the management of:

- Regulations.
- Standards.

Managing Regulations

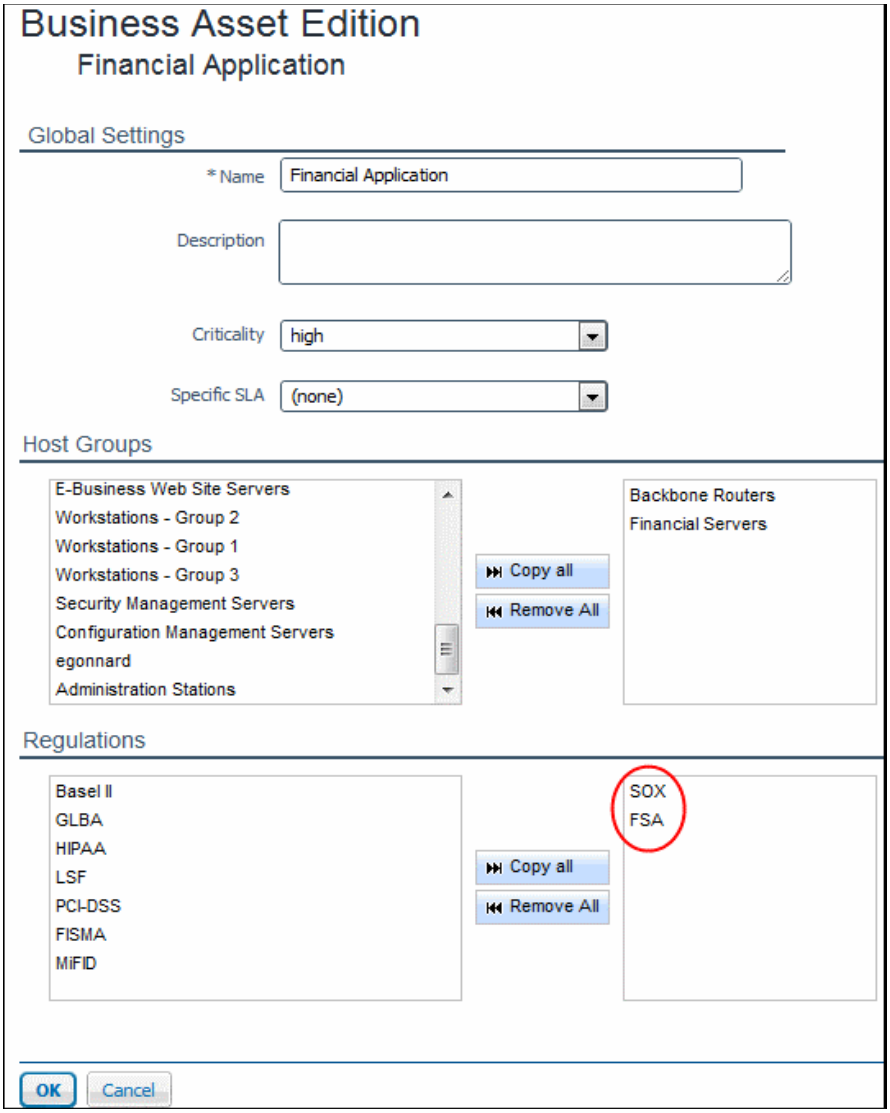
The Asset Database

To be able to manage regulations, the TIBCO LogLogic® asset database needs to be correctly filled. Indeed, the reporting tool will use the "regulation tag" from the asset database to create and filter the necessary data according to the regulations your company follows.

To do so:

1. Identify IT devices submitted to a regulation.
2. Tag related Business Assets with relevant regulation fields by defining it in **Configuration > Asset Database > Business Assets > click on a business asset**.

Figure 70 Regulations in business asset



3. Then, in each dashboard, you can filter the data to be displayed for a specific regulation.

Dashboard Filters for Regulations

When using TIBCO LogLogic® reports and dashboards, you will see that they are automatically based upon ***Standards*** and not regulations. However, if your business activity is submitted to one regulation and you want a dedicated reporting environment for this regulation, you just have to use the pre-defined compliance dashboards furnished by TIBCO LogLogic® as explained in the section Dashboards Based on Regulations.

Standards

The reporting module is by default based upon standards. This makes your dashboards' view easier to display and explain during an audit.

TIBCO LogLogic® Dashboards Framework

Seven groups of dashboards are available. Standards are combined into five main groups, each group containing the report suitable for a given standard.

A summary table of default TIBCO LogLogic® dashboards is available under the **Dashboards** tab by selecting **5 - Regulatory Compliance > Standards Mapping > Standards Mapping and Coverage >** TIBCO LogLogic® **Sec. Dashboards** tab.

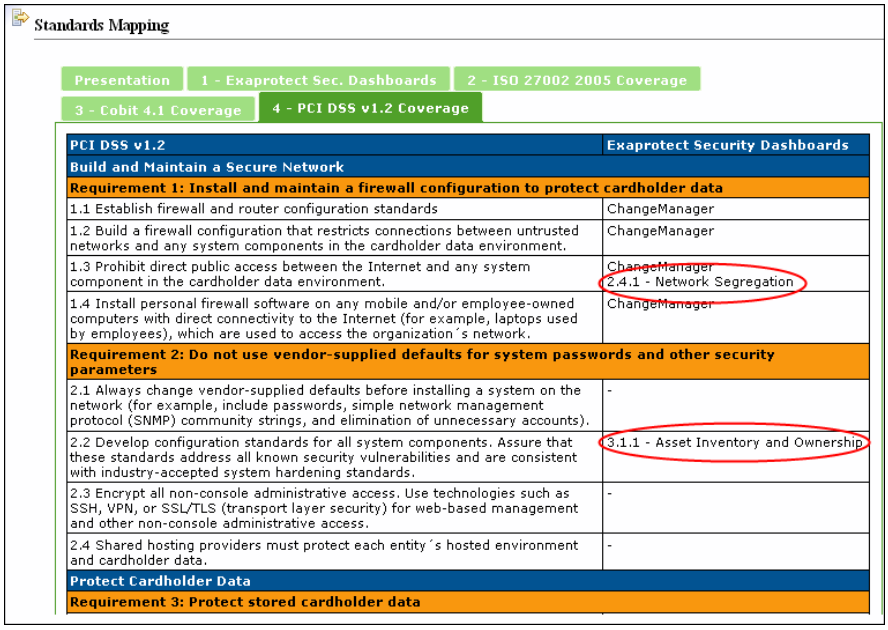
Refer to the ***Appendix*** to get the list of dashboards and their related reports.

Standards Mapping

Standards mapping has been performed in Security Event Manager to adapt a particular procedure taken from a standard to the relevant TIBCO LogLogic® security dashboards and reports.

A summary table of the main standards are available under the **Dashboards** tab by selecting **5 - Regulatory Compliance > Standards Mapping > Standards Mapping and Coverage > "name of the relevant standards" Coverage** tab.

Figure 71 Standards mapping



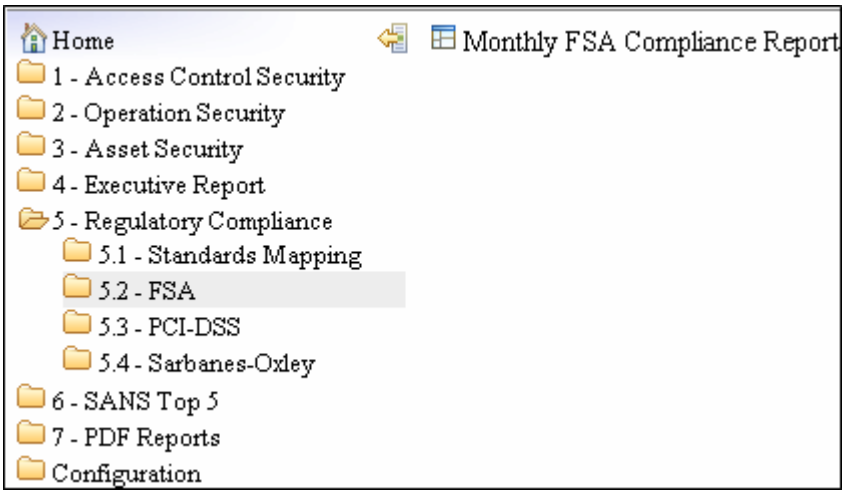
PCI DSS v1.2	Exaprotect Security Dashboards
Build and Maintain a Secure Network	
Requirement 1: Install and maintain a firewall configuration to protect cardholder data	
1.1 Establish firewall and router configuration standards	ChangeManager
1.2 Build a firewall configuration that restricts connections between untrusted networks and any system components in the cardholder data environment.	ChangeManager
1.3 Prohibit direct public access between the Internet and any system component in the cardholder data environment.	ChangeManager 2.4.1 - Network Segregation
1.4 Install personal firewall software on any mobile and/or employee-owned computers with direct connectivity to the Internet (for example, laptops used by employees), which are used to access the organization´s network.	ChangeManager
Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters	
2.1 Always change vendor-supplied defaults before installing a system on the network (for example, include passwords, simple network management protocol (SNMP) community strings, and elimination of unnecessary accounts).	-
2.2 Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards.	3.1.1 - Asset Inventory and Ownership
2.3 Encrypt all non-console administrative access. Use technologies such as SSH, VPN, or SSL/TLS (transport layer security) for web-based management and other non-console administrative access.	-
2.4 Shared hosting providers must protect each entity´s hosted environment and cardholder data.	-
Protect Cardholder Data	
Requirement 3: Protect stored cardholder data	

In the above example, you can see that each point of the PCI DSS v1.2 has been listed. For each main points, the relevant dashboard is indicated.

Note: When **ChangeManager** is indicated, it means that we suggest the use of the TIBCO LogLogic® **ChangeManager** solution to meet your demand in terms of compliance.

You can also use regulations and their associated dashboards and reports directly from the menu **Reporting > Security Dashboards > Home > 5 - Regulatory Compliance.**

Figure 72 Standards and associated dashboards



The process is the same for ISO 27002 2005 and Cobit 4.1 standards. In that way, you know exactly which dashboard you must use to be compliant with standards - and by extension regulations - followed by your company.

Dashboards Based on Regulations

Four dashboards based on specific regulations are automatically generated and exported in PDF on a monthly basis. These dashboards are:

- FSA-ComplianceReport-Month<nb>.pdf
- PCI-ComplianceReport-Month<nb>.pdf
- SOX-ComplianceReport-Month<nb>.pdf

The pdf exported files are accessible by selecting either:

- **Home > PDF Reports > "name of reports"**

or

- **Home > Regulatory Compliance > "name of reports"**. In this screen, you will be able to get a preview of the selected reports.

A maximum of 12 pdf files are generated per year, one for each month. Previous year's dashboards are overridden by newly generated ones.

Only day and month scales are available (no hour scales).

FSA Compliance Dashboard

The **FSA** dashboard includes existing reports with a filter on the **FSA** regulation. It is exported in format A4 Portrait and contains 56 pages:

- The first pages describe the FSA regulation.
- the rest of the document is composed of reports which:
    - describes the FSA section.
    - shows the evolution during the last month (in days)
    - shows a monthly activity in 3 dimensions (**X**: HostGroup or Asset, **Y**: TIBCO LogLogic® Taxonomy, **Z**: number)
    - shows 1 TOP for the month

To preview the dashboard, select **Home > Regulatory Compliance > FSA > Monthly FSA Compliance Report**.

The PDF file is located in:
`/var/lib/exaprotect/archives/<INSTANCE>/report/pdf/fsa`

> **Note:** The **FSA** dashboard is optimized for printing (A4 paper format).

PCI Compliance Dashboard

The **PCI-DSS** dashboard includes existing reports with a filter on the **PCI-DSS** regulation. It is exported in format A4 Portrait and contains 39 pages:

- The first pages describe the **PCI-DSS** regulation.
- The rest of the document is composed of reports which:
    - describes the **PCI-DSS** section.
    - shows the evolution during the last month (in days)
    - shows a monthly activity in 3 dimensions (**X**: HostGroup or Asset, **Y**: TIBCO LogLogic® Taxonomy, **Z**: number)
    - shows 1 TOP for the month

To preview the dashboard, select **Home > Regulatory Compliance > PCI-DSS > Monthly PCI-DSS Compliance Report**.

The PDF file is located in:
`/var/lib/exaprotect/archives/<INSTANCE>/report/pdf/pci-dss`

> **Note:** The **PCI** dashboard is optimized for printing (A4 paper format).

SOX Compliance Dashboard

The **Sarbanes-Oxley** dashboard includes existing reports with a filter on the **Sarbanes-Oxley** regulation. It is exported in format A4 Portrait and contains 62 pages:

- The first pages describe the **Sarbanes-Oxley** regulation.
- The rest of the document is composed of reports which:
    - describes the **Sarbanes-Oxley** section.
    - shows the evolution during the last month (in days)
    - shows a monthly activity in 3 dimensions (**X**: HostGroup or Asset, **Y**: TIBCO LogLogic® Taxonomy, **Z**: number)
    - shows 1 TOP for the month

To preview the dashboard, select **Home > Regulatory Compliance > Sarbanes-Oxley > Monthly SOX Compliance Report**.

The PDF file is located in:
`/var/lib/exaprotect/archives/<INSTANCE>/report/pdf/sox`

> **Note:** The **SOX** dashboard is optimized for printing (A4 paper format).

Dashboard Creation

This section shows you how to:

- Create a New Dashboard
- Plan Tasks in Batch Mode
- Customize the Reports User Interface
- Configure the Reporting System

Create a New Dashboard

Preparing a Report Query

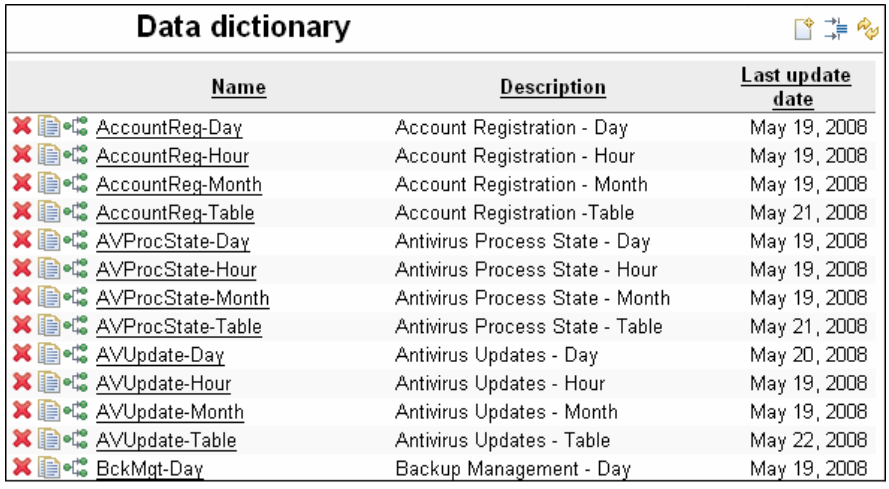
At first, it is important that you prepare a query for selecting the database fields for creating the report. With your query, you will be able to specify the data you want to display in the report's charts or graphs.

Overview of the Query Configuration Interface

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

A list of predefined queries is displayed.

Figure 73 List of queries



Note: You can click on the headers to order the list of queries by name, description, or the last update date.

The Predefined Queries

Usually, you will work either with the standard query called AssetId(the SMP database model) or with Reporting tables queries. These queries are already configured. Therefore, you should not edit them.

SMP *Query*

The SMP query - called SMP Req - is based on the complete TIBCO LogLogic® server data model.

Advantage: it offers the most complete source of queries, allowing you to get the complete set of data you would need for a report.

Drawback: it consumes a great deal of computing resources.

Reporting Tables Query

All the other queries are reporting tables queries. They are queries based on the main SMP model.

Advantage: they do not reduce performance as they are lighter to process.

Drawback: you may have to choose several short queries which could be cumbersome.

In addition, you can create your own query from scratch. This implies that you are well versed in MySQL language.

Creating a New Query

In the list of queries, click on the  icon on the right-hand side of the screen. The description tab is now active.

1. Enter a name and description.

2. Select the type of query you want to display in the **Type** drop-down.
If you select **SQL**, you will have to manually enter the SQL query.
If you select **Star**, you will get a logical view of the decisional database. In this way, when creating reports, the administrator will be shown functional items and not technical fields. Note that the star query is a logical view of an SQL structure. We recommend the use of the **Star** structure when you need to get a clearer view of the database.

3. In the **World** field, select the physical location of the SQL tables.
If you want to indicate the alert and events tables location, select **Events' World**.
If you want to indicate the reporting tables location, select **Reporting World**.

4. Enter the maximum number of lines stored in memory. Setting this parameter will help avoiding queries with an excessive load.

5. If you want to avoid the analysis each time you restart the query, select the **Use Prepared Statement** checkbox. This option is useful when there are many short queries, otherwise, this is not recommended.

6. If you want to display **Data Type** fields when modifying the tables under the star structure, select the **Show Data Type** checkbox.

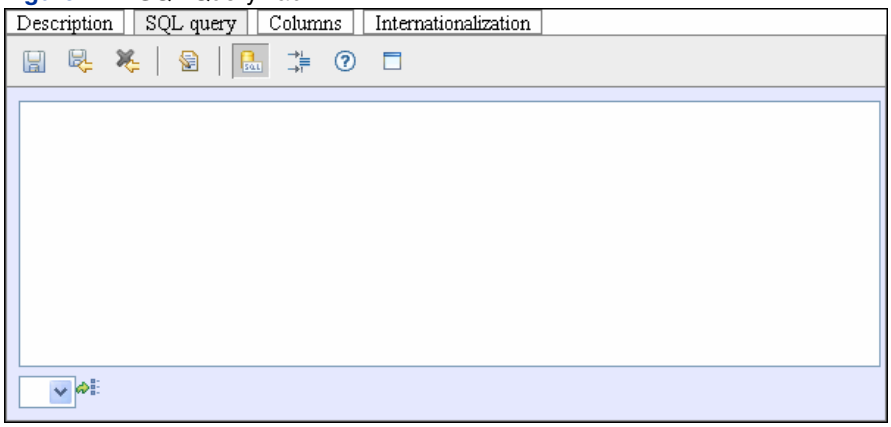
7. If you want to keep a version of your query, select the **Version** checkbox and enter a version number (**MM.mm.ccc** format, where **MM** represents the object's major version number, **mm** the minor version number and **ccc** the correction number). Each time the object is saved, the version number is incremented.

8. Click on the next tab.

Step 2-a: Entering the SQL Query

If you selected **SQL** in the **Type** drop-down list under the **Description** tab, the following screen is displayed:

Figure 74 SQL Query Tab



1. Enter the query in the field. Each variable parameter in the data dictionary must be replaced with a "?[i]", where “i” is the parameter number. Each parameter can be used more than once in your SQL function. If you do not attribute a number to the parameters and you type only "?", the system will automatically number them. You will be able to modify this choice.

2. Save your data.

3. Click on the **Columns** tab.

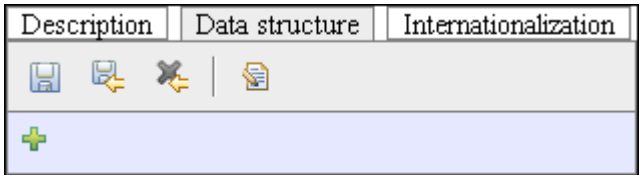
4. Define a name for each column. Do not hesitate to use the preview function located in the toolbar to test your data selection.

5. Save your data.

Step 2-b: Defining the Query Star Structure

If you selected **Star** in the **Type** drop-down list under the **Description** tab, the following screen is displayed:

Figure 75 Data Structure Tab



1. To add a new structure, click on the Add button.

A pop-up screen is displayed.

2. In the **Table Type Selection** screen, select the TABLE type.

3. Click on the right arrow to go to the next screen.

4. In the **Table Selection** screen, select the table that you need among the predefined tables. Exa_Alert is the most commonly used as it corresponds to the alerts in general. Otherwise, you can choose a more specific table. Note that it is always the star structure central table that is selected.

> **Caution:** To create consistent reports, you must associate the relevant table. To know which table to choose, please refer to the List of Reporting Tables section in the Appendix of the Reference Guide where you can find a list of all the tables and their related reports and dashboards.

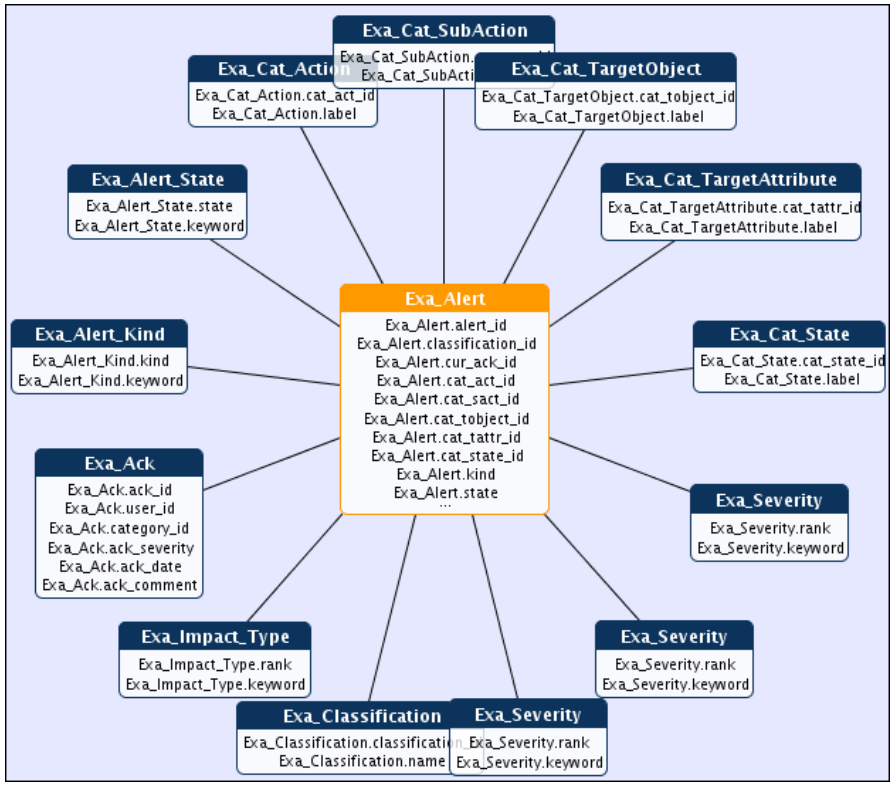
5. Click on the right arrow to go to the next screen.

6. In the **Depth** field, enter the number of links you want to display from the central view.

7. Select an option in the **Import fields** drop-down list: import all fields, all fields but keys, or no field at all by. This is based upon SQL foreign keys.

8. Click on the **Submit** button. The result looks like this:

Figure 76 Exa_Alert Table Star View



9. If you click on one of the field's title, the following menu is displayed:

Figure 77 Field Menu

Table 32 Field Menu Entries

Menu entry	Description
Modify	Allows the user to rename the table, choose the fields to display, rename them or change their types.
Erase	Removes the table from the logical view only. The physical table is not deleted.

Table 32 Field Menu Entries

Menu entry	Description
Wizard	Automatically detects the tables linked to the selected table up to the depth passed as a parameter.
Add a table	Allows you to manually link a table to the selected one. To do this, first choose the table to add. This function is useful if some tables are not initially detected.

10. Save your data.

Adding a Table

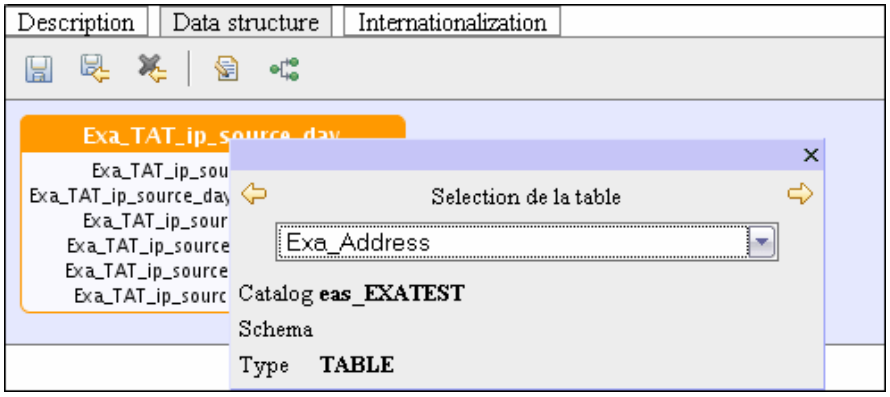
Adding a table and linking it with the main table is useful to get what is behind a field (or table ID) in informal language. To do so, you must make SQL joins between the selected table and the tables which contain the data. Let us suppose you want the IP source.

This field entitled **Exa_TAT_ip_source_day.source_address.id** is stored in the **Exa_Address** table.

1. Select the table to add and click on it.

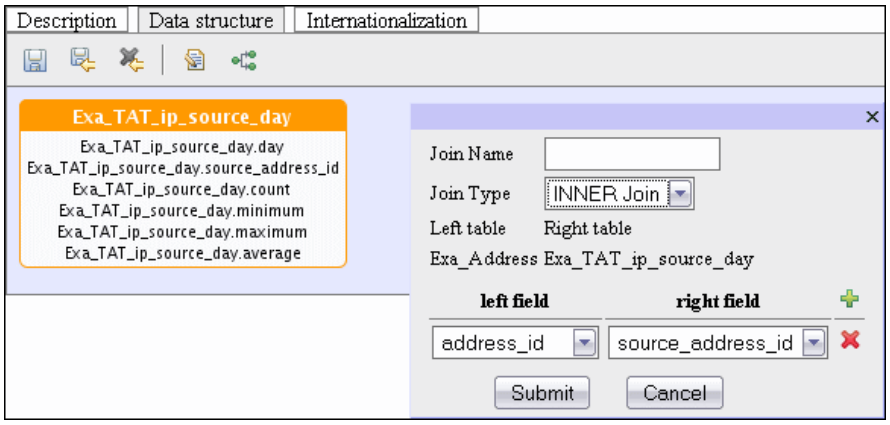
2. Click on the **Add a Table** menu entry. Then, the following pop-up screen is displayed:

Figure 78 Table Selection



3. Select the table which contains all the IP addresses in the drop-down list. A new screen is displayed:

Figure 79 Selecting Joins



4. Select the fields to be linked with one another in the **left field** and **right field** drop-down lists.

5. Select the **Join Type**.
Choose **INNER Join** if you do not want the NULL value to be inserted. In our example, it means that only the alerts with a known IP source address will be displayed.
Choose **LEFT Join** if you want to include NULL from the Reporting Statistics tables. In our example, it means that all alerts will be displayed, even those for which you do not know the IP source address.

6. Click on **Submit**.

Renaming the Field

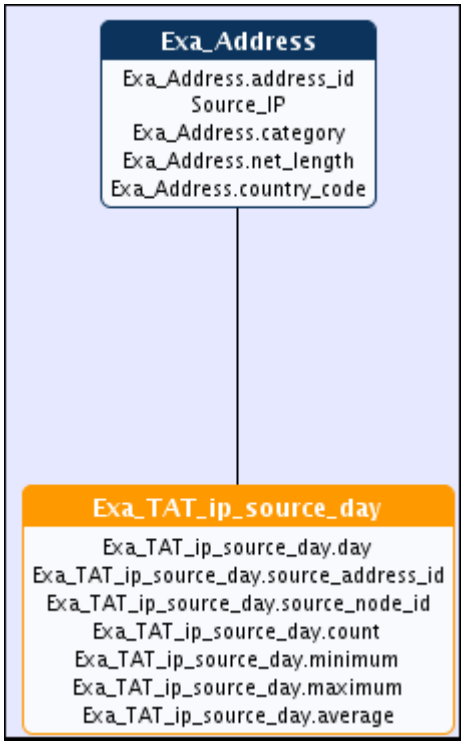
If you want to rename one of the field of the table (e.g. from **Exa_Address.address** to **SourceIP**):

1. Click on the table name to modify and click on the **Modify** menu entry.

2. Replace the name in the **Field name** and **Description** fields by the required name (e.g. **Source_IP** in our example).

3. Click on the button to save the modification. You should obtain the following display.

Figure 80 Name has been changed



Reducing the Display

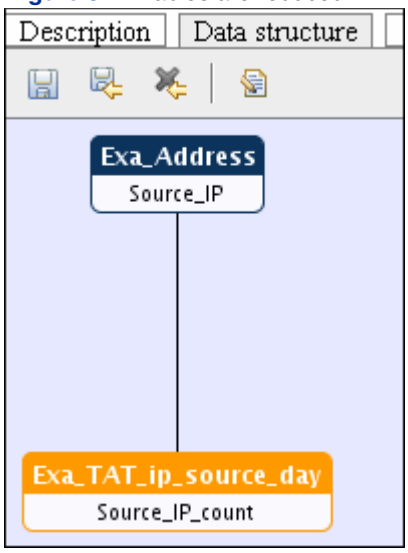
You can remove the fields from the table so that you obtain a reduced display.

1. Click on the table you want to reduce and select the **Modify** menu entry.

2. Deselect the unsuitable checkboxes.

3. Save the modification. You should obtain the following display.

Figure 81 Tables are reduced



4. Save your data. Your query is ready and you can now create your report.

Preparing a Report

You can access the report configuration screen via the main menu by clicking on **Home > Configuration > Report > Report**.

A list of predefined reports is displayed.

Figure 82 List of reports

Report

Name	Description	Last update date
AccountReg-Act-Day	Account Registration Activity (per day)	May 22, 2008
AccountReg-Act-Hour	Account Registration Activity (per hour)	May 22, 2008
AccountReg-Act-Month	Account Registration Activity (per month)	May 22, 2008
AccountReg-Event	Account Registration Events	May 22, 2008
AccountReg-Host-Day	Account Registration by Host Group (per day)	May 22, 2008
AccountReg-Host-Hour	Account Registration by Host Group (per hour)	May 22, 2008
AccountReg-Host-Month	Account Registration by Host Group (per month)	May 22, 2008
AVProcState-Act-Day	Antivirus Process States Activity (per day)	May 23, 2008
AVProcState-Act-Hour	Antivirus Process States Activity (per hour)	May 23, 2008
AVProcState-Act-Month	Antivirus Process States Activity (per month)	May 23, 2008
AVProcState-Event	Antivirus Process States Events	May 22, 2008
AVProcState-Host-Day	Antivirus Process States by Host Group (per day)	May 23, 2008

The report interface is the same as the query interface.

The Predefined Reports

Usually, you will work with standard reports as they are already predefined according to various needs.

You can have several representations for one report. This is to avoid displaying useless data that can lower performance.

Two "worlds" (**Menu > Configuration > Administration > World**) are necessary to display the various reports:

- Events world: allows you to use reports displaying events by seconds per week (and also days per month, hours per day, months per year).

- Reporting world: allows you to use reports displaying events by day in a month, by hour in a day or by month in a year.

The main difference between the reports below is that the report from the Events world has a high level of granularity, it contains more filters, and the time period is different from the other reports.

Creating a New report

> **Caution:** To create a report, you need a query. If you do not want to use any of the standard queries, make sure that you have already prepared a query that will correspond to the report you are going to create. For more information about query configuration, please refer to section Preparing a Report Query.

Step 1: Description Tab

In the list of reports, click on the  button on the right-hand side of the screen. The description tab is now active.

1. Enter a name and description. The description is very important since it is the information that will be displayed in the report list.

2. Select the query you have previously configured to apply to the report in the **Data Dictionary** drop-down list. New tabs are now displayed.
Note that you can also edit a query to modify it by clicking on the  button on the right-hand side of the drop-down list.

3. In the **Rows per Page** field, enter the number of rows to display. This is only used with tabular charts.

4. In the **Page Layout** drop-down list, select the page layout of the report (portrait, landscape, A3, A4, A5).

5. In the **Default Color List** drop-down list, select a color to be applied to the charts. The page layout and default color options are configurable. Please refer to the "Customizing Reports" section for more details.

6. If you want to display the filter when clicking on the document, then select the **Show Filter First** check box.

7. If you want to display a comment when hovering the mouse over the report's title in the dashboard, or if you want a comment to be displayed under the report, select the **Show Comment on Display** check box.

8. If you want to display an alert ranking stemmed from your report, select the **Show Ranking** checkbox. Fields are now activated below.

9. Enter the number of data to be displayed in the **Ranking** field.

10. Check the **Display other values** if you want to display an additional value. Enter a description for this value.

11. Define a version number.

12. Click on the **Field Selection** tab.

Step 2: Field Selection Tab

The items available to compose the report are displayed according to your query.

Their type is displayed above their group: **Metrics**  or **Attributes**  .

1. Tick the items you need for your report.

2. Click on the **Filter** tab.

Step 3: Filter Tab

This tab allows you to configure fields so that you can filter your report data and make rapid searches.

The generated fields for filtering are available when clicking on the  icon in the report.

A new screen is displayed.

1. If you want to have a filter comparing two items, select a value in the **Value list** drop-down list.
2. If you want to have a filter comparing an item and a constant value, enter a constant in the **Constant** field.
3. If you want to have a filter comparing an item and a user inputted value, select a prompt type.

In this last case, you have to enter a name and description for the filter's prompt. Choose the entry type and the default value.

Note that you must manually enter the operator after the text in the **Field Name** field: For example: “From date =”.

For each constant value or each user prompt's default value, you can also enter system values.

Table 33 List of System Values

[year]	Current year
[month]	Number for the current month
[weekofmonth]	Number for the week of the month
[weekofyear]	Number for week (relative to a one year period)
[dayofyear]	Number for day (relative to a one year period)
[dayofmonth]	Number for current day of the month
[dayofweek]	Number for current day of the week
[hour]	Current hour
[minute]	Current minute
[now]	System date
[firstdayinyear]	First day of the current year
[firstdayinmonth]	First day of the current month
[firstdayinweek]	First day of the current week
[null]	Null value

These system values can be incremented or decremented using the following syntax [xxx+nn] or [xxx-nn].

Examples:

[month-1] returns 7 if today is 17/08/2007.

[firstdayinmonth+14d] returns 15/08/2007 if today is 17/08/2007.

[firstdayinmonth+1m] returns 1/09/2007 if today is 17/08/2007.

[firstdayinmonth+1y] returns 1/08/2008 if today is 17/08/2007.

1. Click on the button to confirm your modifications.

2. Click on the **Design** tab.

Step 4: Design Tab

In this section, you can define the basic visual design of your report and the way you want to display data. To precisely configure the report display, please refer to the "Customizing Reports" section.

The **Design** screen is composed of:

- a toolbar
- a preview of the type of graph currently active in the left-hand side of the screen
- a table that represents the x-axis coordinates of your graph. A click on the column displays a menu allowing you to configure the table (or the graph) by editing, inserting, adding or deleting a column.

Select the type of table you want to use. To do so:

- click on the icon to select a standard display of the table (row/column mode).
- click on the icon to choose a cross table.
- click on the icon to choose an inverted table (or horizontal display of the table if a standard table is taken as reference).

Remember that the first column of the table corresponds to the x-coordinate and the second column corresponds to the y-coordinate regarding standard table only.

1. Click on the column in the zone indicated with dotted lines and select **Add column**. A panel is displayed which allows you to precisely define the look and use of your graph.

2. Enter a header caption in the respective field.

3. Select the field you want to have displayed in the current column.

4. Click on the button located near the **Header** field to define the style of the column header: color, background color, font, size, style (italic, bold...etc), weight, and alignment.

5. Click on the button located near the **Header Format** field to define the data format:

    - Number of significant digits: minimum number of digits to the left of the decimal point (e.g for 4 significant digits, the number 123 becomes 0123).
    - Number of decimals: number of digits after the decimal point.
    - Grouping separator: displays the digit grouping separator corresponding to the user's language (e.g in French: 1 284; in English: 1,284).
    - Prefix and suffix: currency, unit or any type of text situated before or after a number.

6. If you want column to appear in your graph, select **Visible**. The purpose of keeping the column invisible is to be able to use the column information for filtering or archiving without displaying it.

7. If you want to display a separation every time the value changes in a specific column, select **Break**.

8. If you want to avoid too many repetitive data and columns, select **Erase doublons**.

9. Select the aggregation type. Please note: if the field already has an aggregation, it will be used by default.

Remember that the **SUM** aggregation type will lead to the display of a report composed of similar alerts that will aggregated. If you select **COUNT**, the report will display all the alerts as unitary entities.

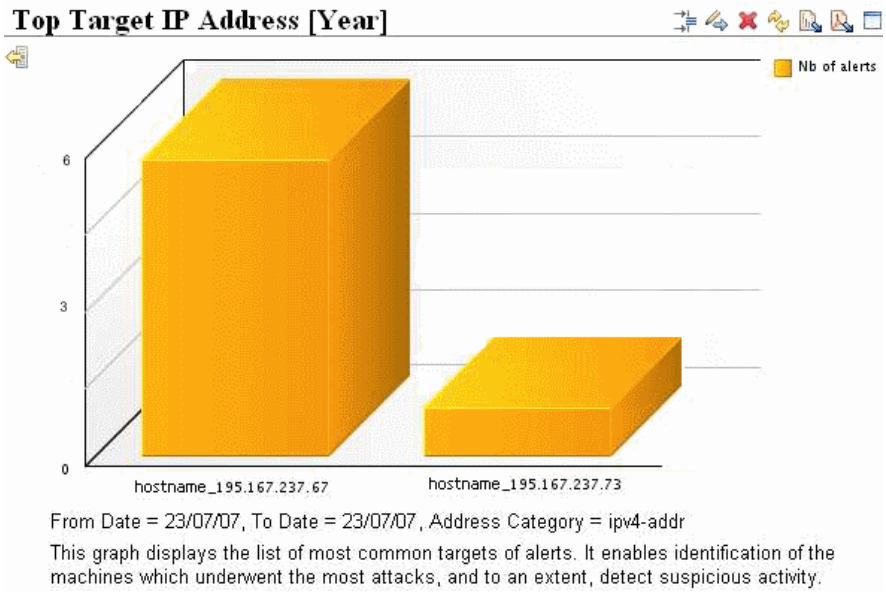
Example: let us suppose we want to display a report in which alerts with the same IP address and node are grouped for a given day in the month. The table contains the following values:

Table 34 Table Values

Hour	Address_id	Node_id	Domain_id	Count
2007-07-23 11:00:00	2	2	0	4
2007-07-23 00:00:00	2	2	0	1
2007-07-23 12:00:00	2	2	0	1
2007-07-23 14:00:00	3	2	0	1

If you selected **SUM**, the report should look like the following.

Figure 83 Alerts are grouped



The first block represents the three first lines of the table. They are aggregated as they have similar address_id, node_id and domain_id.

The second block corresponds to the last line of the table as address_id value is different from the other address_id lines.

1. Select a calculation type in the **Calculation** drop-down list. In each column or axis, you will see a "calculation" selection list that will fill the column with a calculation using values from other rows.

Examples:

- Cumul on break: same with reset at each break
- Global cumul: Value = Xn + Xn-1
- % / total on break: same with reset at each break
- Global % / total: Value = Xn / sum(X0 - Xmax)
- Variation on break: same with reset at each break
- Variation: Value = Xn - Xn-1
- % variation on break: same with reset at each break
- % variation: Value = (Xn - Xn-1)/Xn-1

You will now define the graphical representation of your chart or graph.

2. Click on the  icon.

A screen is displayed with all possible types of charts available (bar chart, line chart, pie chart...etc). The classical display is a data table.

As far as standard tables are concerned, remember that:

- Data in the first column define the x-coordinate values.
- Titles and colors of the others numerical rows are used to create the table input.
- Column data are used for the entry values.
- The ordinate axis is auto-defined or defined by the selected calculation.

3. Select the desired chart by clicking on it.

4. Save your data.

5. Preview your report by clicking on the  icon.

Your report is ready. However, you must allocate it to a session to be able to display it.

Step 5: Associating the Report to the Hidden Session

This step is very important as it will allow you to define the location from which reports will be displayed in your dashboards.

You access the list of sessions via the main menu by clicking on **Configuration > Administration > Workspace**.

1. Click on the user profile (here **superadmin**).

2. Click on the **Sessions** tab.

3. Click on the **Hidden** folder.

4. Click on the  icon to add your report. The **Sessions** screen is displayed.

5. Select the report's title in the list.

6. Click on the **OK** button. The report is added under the folder you deployed.

7. Define the report access status by selecting this option in the drop-down list. The different levels of access rights are the following:

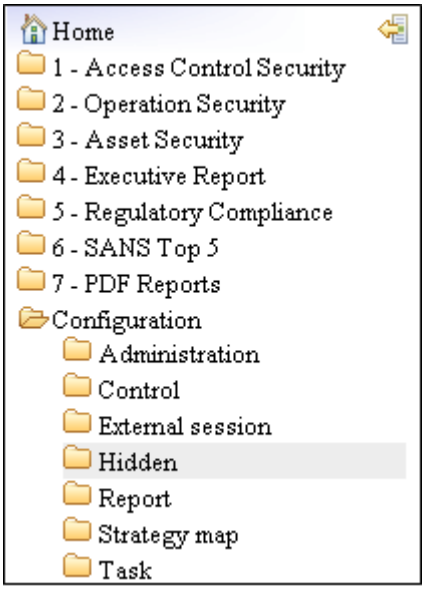
Table 35 Access Rights

Access right	Session	Dashboard	Report	Metrics
None	NA	NA	NA	NA
Read only	Open	View	View	View
Total	Open, create, and modify	View	Display and customize	Display and zoom

8. Save your modifications by clicking on the button.

Your report is now available in the Hidden folder's tree structure.

Figure 84 The report is located under the Hidden folder



To display your report, click on the report's name.

The last step consists in creating a dashboard containing the reports you want to display and monitor. You will be able to automatically display the dashboard when connecting to the report interface.

For more information about the report interface access configuration, please refer to "Accessing Security dashboards" section.

Inserting Reports in a Dashboard

You access the dashboard interface via the main menu by clicking on **Configuration** > **Report** > **Dashboard**.

Before creating a dashboard, make sure you have configured or created all the reports you want to display in the dashboard. For more information about creating reports, please refer to the "Preparing a Report" section.

Step 1: Description Tab

1. Click on the button to create a new dashboard.

2. Under the **Description** tab, enter a name and description.

3. In the **Refresh Delay** field, enter the time period after which there is an automatic refresh of the report blocks displayed in the dashboard.

4. Select the page layout in the drop-down list. This will be taken into account when printing the dashboard in PDF format.

5. Define the version number.

6. Click on the **Design** tab.

Step 2: Design Tab

The **Design** tab displays a page composed of one block that represents one report.

1. To add a block, that is, a report in your dashboard, click on the icon. You can add as many blocks as you want. In the following example, three reports have been added:
You will notice that the Block 1 on the left is yellow: it means that it is selected.

2. If you want to modify another block (or report), click on the respective block to activate it. The corresponding properties are now displayed below the blocks.

3. Select the report's display type in the **Bloc Properties** drop-down list.

4. Select the report you want to display instead of the block.

5. Enter the position and size of the selected report in the respective fields.

6. Select the **Auto-refresh** checkbox, if you want the block to be refreshed by frequency set by the corresponding parameter in the description tab. This function is particularly useful to monitor data undergoing rapid changes in your dashboard.

7. If you want to specify the display target block of a report resulting from a dynamic link, select the respective option in the drop-down list. If you keep the parameter empty, the navigation will stay in the block.

8. You can move the block using a "drag and drop" action. To do so:

- Make sure the correct block is selected.
- Click on the block title bar and drop it where you want to move it to.
- If you want to delete a selected block, just click on the icon in the toolbar.

9. If you want to add a dashboard template, click on the icon. A new template is displayed below the others. When exporting to a PDF format, the dashboard templates correspond to different pages in the generated PDF document.

10. Click on the **Filter** tab.

Step 3: Filter Tab

You can synchronize fields included in reports by creating dashboard filters. Dashboard filters will be displayed and will apply to the set of blocks.

1. Enter a name and description for the filter.

2. Select the block which will supply the default parameters. Note that the **Value list comes from** parameter is important when the corresponding field displays a list of values. The master report supplying the list must be defined.

3. If you want a filter to be applied to the dashboard, use the following options:

Table 36 The Filter Options

Options	Description
Use filter	This option has two functions: ▪ It MUST BE selected if the **Mandatory** option is selected (see below) so that the **Mandatory** option is fully available. ▪ If the **Use filter** checkbox is selected but the **Mandatory** option is not, a filter that can be deactivated can be applied in the dashboard interface.
Default value	Enter the desired value. The filter will be applied according to this value. This field is used with both the **Use filter** and **Mandatory** options.
Mandatory	The filter is automatically applied and cannot be deactivated in the dashboard. For this option to be fully available, you need to ensure that: • The **Use filter** option is selected. • The **Default value** field must be filled. Otherwise, the **Mandatory** option will not work.

If a filter is applied, the following icon will be displayed in the dashboard:  . If you click on this icon, you will see parameters for the filter, if the **Use filter** option is selected.

If the **Mandatory** option is selected, the check box will automatically be selected.

4. In the drop-down list, select the filter fields you want to display in the report.

Plan Tasks in Batch Mode

In the **Reporting** interface, you have the possibility to automatically generate tasks in batch mode. A task can consist in the generation of a report or dashboard in PDF format, or the creation of a strategic map.

The tasks automatically start according to the date and time you planned.

To access the **Task** section, go to **Configuration** > **Task** from the main menu.

Creating a Group of Tasks

The first thing to do before creating a task is to configure a group of tasks. It will allow you to sort the various tasks per folders and then gain in organization efficiency.

1. Click on the **Task Group** menu entry. The list of task groups is displayed.

2. Click on the  icon on the right-hand side of the screen. The **New Task Group** screen is displayed.

3. Enter a name and description in the corresponding fields.

4. If you want the group to always be displayed in the list of task groups, select the **Active** checkbox.

5. Save and close the screen by clicking on the  icon.

The new task group is now displayed in the list of task groups.

Creating a New Task

You can create and generate various types of tasks. You can create a task to:

- monitor data and control a query in order to be informed when fixed thresholds are reached. As soon as a threshold is reached, a control can be sent by message. You can configure one or more types of message (mails or SMS) to make the system send warnings.
- transfer data to automatically fill an empty database.
- generate documentations, that is to say reports or dashboards in PDF or XML formats.
- generate images from data.
- generate a strategic map or indicators.
- import and/or export data.
- execute a script.

To create a new task, you must display the task creation screen. To do so:

1. Click on the **Task** menu entry. The list of tasks is displayed.

2. Click on the  icon on the right-hand side of the screen. The **New Task** screen is displayed.

3. Enter a name and description for the task.

4. Select the type of task you want to generate in batch time.

5. Define the version number.

6. Indicate if you want to generate a **child** or **master task** by selecting the corresponding option.

If the task is defined as **child**, it will be executed according to the task it depends on, at the same frequency. For this reason there are different parameters for the definition of a task.

Each child task depends on a prior task and its execution is conditioned:

- execution if the prior task completed correctly or
- execution if there is a problem.

Thus, real execution scenarios can be determined.

As for **master** tasks, the task group parameter allows to group tasks into blocks and activate or deactivate all of them at the same time.

1. Select the group of task to which the task must belong.

2. To plan the tasks according to the start date, click on the  icon and select the date and time when the task must start. The start date is **mandatory**.

3. If you want to indicate an end date, click on the  icon and select the date and time when the task must start. The end date is not mandatory.

4. Enter the generation frequency, either in day, hour, minute, month or week.

According to the type of tasks you selected, different parameters must now be filled in.

Control: Creating a Task to Monitor Data

If you selected **Control** in the **Task Type** drop-down list, do the following:

Settings Tab

1. Click on the **Settings** tab.

2. Select the report you want to monitor.

3. If you want to receive an alert, either by mail or sms, as soon as an important event occurs, select the **Send Message** checkbox.

> **Caution:** Make sure you have configured the type of message you want to receive under **Administration > Message Type**.

4. If you want to see only lines which have a or a in the tabular display mode, select the **Remove Information Lines** checkbox.

Properties Tab

1. Click on the **Properties** tab.

2. Select the data column to monitor, either number of alerts, state or time in the **Field Name** drop-down list.

3. Click anywhere on the colored bar that graphically represents the operator and threshold combined. A pop-up screen is displayed listing the various type of operator bars you can choose.

For example, if you select the following bar:

It means that there are two thresholds used by the warning, so when the value reaches the first one, the warning becomes orange and when it reaches the second one, the warning becomes green.

4. Enter numerical threshold values in the **Threshold** field. You can enter up to 4 thresholds according to the chosen colored bar.

Message Tab

1. If you selected the **Send Message** checkbox under the **Settings** tab, the **Message** tab is displayed. It allows you to enter various parameters about the alerts you will receive. Click on the **Message** tab.

2. If you want only a group of predefined people to receive the message, select the **Users having access** checkbox.

3. If you want to add people in the list of users receiving the message, click on the icon and select the users that you want. To make it work, you must have defined users and their mail address under the **Administration** section.

4. Enter the message subject.

5. Activate the **Attachment** option if you want to attach to the email a PDF file corresponding to the report.

6. Enter the message body in the corresponding text zone.

7. If you want to insert fields in the text zone which will be automatically filled by the system when sending the message, select the relevant field in the drop-down list and click on the button to validate your selection.

8. You can define rules to activate the email launch by using the **Message Sending Policy** option. For example, if you want to receive a message when the state passes from warning to error, you must tick the box which is located on the right-hand side of the second line. Once created, you can follow the execution of these tasks using the task manager. The task manager allows you to display groups of tasks. For more information about the Task manager, please refer to the "Monitoring the Generation of Tasks in Batch Mode" section. In the case of SMS sending, note that you cannot enter more than 160 characters.

9. Save and close the screen by clicking on the icon.

Associating the Metric Task to a Workspace

Now, in order to display the metric in a tabular format in the reporting interface, you must associate the metric task to a workspace.

1. Select **Administration > Workspace** from the main menu.

2. Click on the desired profile.

3. Click on the **Controls** tab. The **Control Group** folder is displayed.

4. Click on the folder. A green cross is displayed.

5. Click on the green cross to add your control.

6. In the pop-up screen, select the control you want to display.

7. Click on the **OK** button.

8. To display your **Control** task, select **Control > Control Panel** under the main **Menu**.

Datamart: Creating a Task to Automatically Fill an Empty Database

If you selected **Datamart** in the **Task Type** drop-down list, do the following:

Execution Tab

1. Click on the **Execution** tab. This screen allows you to select the type of data source: database, XML file or CSV file. In any case, an XSL transformation file can also be added.

2. If you do not want to take contextualization into account, select the **Single Execution** checkbox.

3. If you want to take contextualization into account for all entities, select the **Multiple Execution on all Entities** option.

4. If you want to take contextualization into account for all entities with filters entities using the value of one of the personalized fields, select the **Multiple Execution on Entities Where** option.

5. If you selected this last option, then select a condition in the relevant field.

6. Select the source file type containing the data (either XML, CSV, Standard log file or a query).

7. If you want to apply an XSL style sheet to the file, select **XSL** in the **Transformation** drop-down list. Otherwise, if you do not want to apply a style sheet, select **None**.

8. Select the destination file format (either a table, an XML or CSV file).

Settings Tab

1. Click on the **Settings** tab.

2. Select the directory type in the corresponding drop-down list.

3. Enter the path to the file you want to take as reference.

4. If you want the file to be automatically deleted just after the transfer, select the **Delete after** checkbox.

5. If you previously decided to apply a style sheet to your file, you must indicate the directory and path name of the file. To do so, just repeat steps 10 and 11.

6. In the **Destination** part, select the world type you want to apply.

7. Enter the table you want to create or fill.

8. If you want to delete data, select the **Clear first** checkbox.

9. If you want to automatically create a table during the generation, select the **Create table if needed** checkbox.

10. Save and close the screen by clicking on the  icon.

Document Generation: Creating a Task to Generate Reports or Dashboards in PDF

If you selected **Document Generation** in the **Task Type** drop-down list, do the following:

Settings Tab

1. Click on the **Settings** tab.

2. If you do not want to take contextualization into account, select the **Single Execution** checkbox.

3. If you want to take contextualization into account for all entities, select the **Multiple Execution on all Entities** option.

4. If you want to take contextualization into account for all entities with filters entities using the value of one of the personalized fields, select the **Multiple Execution on Entities Where** option.

5. Select either the report or dashboard you want to generate in a PDF format by clicking on the radio button and selecting the respective report or dashboard.

6. In the **Destination** part, select the folder type and its pathname where the document will be generated.

7. Save and close the screen by clicking on the  icon.

Image Generation: Creating a Task to Generate an Image of a Report or Dashboard

If you selected **Image Generation** in the **Task Type** drop-down list, do the following:

Execution Tab

1. Click on the **Execution** tab.

2. If you do not want to take contextualization into account, select the **Single Execution** checkbox.

3. If you want to take contextualization into account for all entities, select the **Multiple Execution on all Entities** option.

4. If you want to take contextualization into account for all entities with filters entities using the value of one of the personalized fields, select the **Multiple Execution on Entities Where** option.

5. If you selected this last option, then select a condition in the relevant field.

6. Select the source file type containing the data (either XML, CSV, Standard log file or a query).

7. If you want to apply an XSL style sheet to the file, select **XSL** in the **Transformation** drop-down list. Otherwise, if you do not want apply a style sheet, select **None**.

8. Select the format of the target file (either PNG, GIF, SVG or JPG file).

Settings Tab

1. Click on the **Settings** tab.

2. Select the directory type in the corresponding drop-down list.

3. Enter the path to the file you want to take as reference.

4. If you want the file to be automatically deleted just after the transfer, select the **Delete after** checkbox.

5. If you previously decided to apply a style sheet to your file, you must indicate the directory and path name of the file. To do so, just repeat steps 10 and 11.

6. In the **Destination** part, select the folder type and its path name where the image will be generated.

7. Save and close the screen by clicking on the  icon.

Metric: Creating a Task to Create Strategic Map

If you selected **Metric** in the **Task Type** drop-down list, do the following:

Settings Tab

1. Click on the **Settings** tab.

2. Select the report to analyze to create the metric.

3. If you want to receive an alert, either by mail or sms, as soon as an important event occurs, select the **Send Message** checkbox.

> **Caution:** Make sure you have configured the type of message you want to receive under Administration > Message Type.

4. Select the strategic objective, in which the metric will be included, in the **Strategic Objective** drop-down list.

Properties Tab

1. Click on the **Properties** tab.

2. Select the reference report you want to receive as attached file.

3. Select the field name on which you will compute statistics in the **Field Name** drop-down list.

4. Select the world where you want to store metrics history.

5. Select the time period during which the map is stored. The duration must be equal to the Trend Calculation duration.

6. Select the calculation mode and calculation period. For example, you will be able to display the three first results of the query.

7. Select the color and format of the metric.

8. Select the trend calculation. It will be represented by a green, red or black arrow. The trend calculation duration must be lower than the storage duration.

9. Select the target value. It will be displayed in the graph. It is for information only.

10. Click anywhere on the colored bar that graphically represents the operator and threshold combined. A pop-up screen is displayed listing the various type of operator bars you can choose.
For example, if you select the following bar:  it means that there are two thresholds used by the warning, so when the value reaches the first one, the warning becomes orange and when it reaches the second one, the warning becomes green.

11. Enter numerical threshold values in the **Threshold** field. You can enter up to 4 thresholds according to the chosen colored bar.

12. If you selected the **Send Message** checkbox under the **Settings** tab, the **Message** tab is displayed. Please refer to the ***Control Option: Creating a Task to Monitor Data*** section where the Message tab is already described.

13. Save and close the screen by clicking on the  icon.

Associating the Metric Task to a Workspace

Now, in order to display the metric in a tabular format in the reporting interface, you must associate the metric task to a workspace.

1. Select **Administration > Workspace** from the main menu.

2. Click on the desired profile.

3. Click on the **Metrics** tab. The **Metric Group** folder is displayed.

4. Click on the folder. A green cross is displayed.

5. Click on the green cross to add your metric.

6. In the pop-up screen, select the metric you want to display.

7. Click on the **OK** button.

8. To display your **Metric** task, select **Strategy Map > Metric** under the main **Menu.**

Parameters Import/Export: Creating a Task to Import/Export Data

If you selected **Parameters Import** or **Parameters Export** in the **Task Type** drop-down list, do the following:

Execution Tab

1. Click on the **Execution** tab.

2. If you do not want to take contextualization into account, select the **Single Execution** checkbox.

3. If you want to take contextualization into account for all entities, select the **Multiple Execution on all Entities** option.

4. If you want to take contextualization into account for all entities with filters entities using the value of one of the personalized fields, select the **Multiple Execution on Entities Where** option.

5. If you selected this last option, then select a condition in the appropriate field.

6. If you want to apply an XSL stylesheet to the file, select **XSL** in the **Transformation** drop-down list. Otherwise, if you do not want to apply a stylesheet, select **None**.

Settings Tab

1. Click on the **Settings** tab.

2. If you previously decided to apply a stylesheet to your file, you must indicate the directory and pathname of the file. Select the directory type in the corresponding drop-down list.

3. Repeat step 8 in the **Destination** part to indicate where the file will be imported/exported.

4. Save and close the screen by clicking on the  icon.

Script: Creating a Task to Generate a Script

If you selected **Script** in the **Task Type** drop-down list, do the following:

Script Tab

1. Click on the **Script** tab.

2. If you do not want to take contextualization into account, select the **Single Execution** checkbox.

3. If you want to take contextualization into account for all entities, select the **Multiple Execution on all Entities** option.

4. If you want to take contextualization into account for all entities with filters entities using the value of one of the personalized fields, select the **Multiple Execution on Entities Where** option.

5. If you selected this last option, then select a condition in the relevant field.

6. Indicate the directory and pathname of the script to generate.

7. Select the desired **World**.

8. Select if you want to restart or stop the script execution when an error occurs.

9. Indicate when you want to display the **SQL query** that allows the automatic generation of the script: either when an error occurs, never or always.

Monitoring the Generation of Tasks in Batch Mode

To monitor the task generation process, you can display the **Task Manager** screen where all the current tasks are sorted in predefined folders.

The task manager gives an overall picture of the created scenarios' structure as well as the results of their execution.

To access the **Task Manager**, deploy the **Task** folder and click on **Task manager**.

Icons

In each task group folder you created, you can display the list of the enclosed tasks. At the beginning of each task, an icon is displayed. It is a visual help to indicate the type of files. Here is the list of the corresponding icons.

Table 37 Task Icons

Icon	Description
	Automatic control
	DataMart
	Script
	Metric
	Parameter settings import
	Parameter settings export
	Document generation
	Image generation

At the end of each task line, other icons are displayed indicating the task execution status:

Table 38 Task Execution Icons

Icon	Description
	No errors during the execution
	Errors occurred during the execution
	Failure
	Unknown status. Immediately displayed just after the first execution.
	The task is running

Using the Task Manager

When clicking on the task name, you display information about the task execution process.

The task manager has three buttons in its toolbar that allow you to control the generation process.

Table 39 Task Manager Icons

Icon	Description
	Starts the task manager
	Stops the task manager
	Refreshes the task manager screen

All of these functions are only available if the user has total access to the task manager. If the user is in "read only" mode, only the refresh function is available.

Customize the Reports User Interface

You can modify the visual aspect of your interface according to your preferences.

However, this customizing depends on the user rights defined in the SMP interface.

Remember that admin and super admin users can create, delete, and modify reports.

`Analyst` and `viewer` users can change views and filters, and modify reports.

Customizing Reports

You have the possibility to customize different aspects of a report: graph colors, page, and page layout (used for PDF export).

Color List

The color list option allows you to choose the color of the graph. Each color represents a type of data.

1. In the main Menu, click on **Configuration > Report > Color list**.
2. Either click on an existing color to modify it or click on the icon to add a new color.
3. Enter the new color name.
4. Define the colors by clicking on the icon near each field.
5. If you want transparency, select the corresponding radio button.
6. If you want to define a precise color, select the **Color** radio button.
7. Click on the left and right arrows to set the right color.
8. Give a name to your color in the blank field.
9. Click the **OK** button.
10. If you need to add another color, click on the icon. A new field is added at the end of the field list.

The colors will be used for the chart entries by creation order. In case the number of data entries are superior to the number of colors available in the color set, the application will start again at the beginning of the color set list.

Page

The page option allows you to configure the page format in the page layout.

1. In the main Menu, click on **Configuration > Report > Page**.
2. Either select an existing page format or click on the icon to add a new page format.
3. Enter a description for the page format.
4. Enter a size (width and height).
5. Select a unit for the size of your page

Page Layout

The page layout option allows you to configure the page format when exporting to PDF. The **export to PDF** function is available for each displayed report or dashboard. You can add, modify or delete the layout parameters used by this function. The layout is something you can use in the report definition and its customizing.

1. In the main Menu, click on **Configuration > Report > Page Layout**.
2. Either select an existing page layout or click on the icon to add a new page format.
3. Enter a description for the page layout.
4. Select the page size. The values of these fields correspond to the values defined in the **Page** screen.
5. Select the orientation of the page: **Portrait** or **Landscape**
6. If there is a section page break, click the respective checkbox.
7. Enter all the desired font sizes in the fields located under the **Unit** field.
8. Select the type of header and footer display.

Configuring the Interface Language

In each screen, you will find a tab called **Internationalization**. By clicking on it, you will be able to configure the text to display as well as a corresponding translation into a specific language.

1. Enter the report's title in the **Description** field.
2. In the **Comment** field, enter the comment to display when hovering the mouse over the report's title. The comment character limit is 255.
3. Enter the description you want in the respective fields.
4. Translate the texts in the opposite fields.
5. Save your data.

> **Caution:** It is not recommended to switch from English to French language via the User menu entry. Only English language is supported.

Configure the Reporting System

By default, the reporting system is already predefined by the TIBCO LogLogic® team.

However, you have the possibility to apply an advanced configuration to your reporting system. This is possible through the **Administration** menu.

Note that only the Super-Administrator and Administrator can apply modifications to the reporting system.

List of the Main Configuration Types Available

Table 40 Administration Menu Entries

Menu Entry	Description
Access Point	Allows you to configure the Reporting interface to have an access to reports via a mobile web browser on the extranet. This is only applicable if you use the Reporting interface on a standalone purpose.
"Entity"	Allows you to define groups of users. You can merge data for this group, with a view to calculate management metrics. By default, there is a defined entity allocated to all users.
"Message Type"	Allows you to create the type of warning message (sms or e-mail) to be received when generating tasks such as Metrics and Controls.
"Maintenance Period"	Allows you to forbid the access to the server for a certain period of time for maintenance purposes.
"Theme"	Allows you to configure the interface display as a whole. By default, there is a defined theme allocated to the whole interface.
"Folder"	Defines the location of the folder where your documents are stored (scripts, images, xml files...) and that you want to share with other report users. These folders are visible via the portal, and users will be able to navigate, download, or update files from these folders and in their sub-folders.
"User"	Allows the creation of users or personal logins with different profiles.
"System Preferences"	Allows you to define the system general information (default language, PDF tool...etc).
"Personalized Fields"	Allows you to add personalized fields for users, workspaces or entities. These values are used in queries to filter or calculate results.
"Style"	Allows you to define fonts and colors to apply to the various graphics.
Connected Users	Displays the list of all connected users. It allows you to monitor the activity on the reporting server. For each user connected you will have the date/time of the connection and the IP address.
Driver	Allows you to configure the type of drivers you want to use. You are not supposed to modify this TIBCO LogLogic® predefined option.
"Workspace"	Defines the access rights for all the system's objects and reports.
"World"	Only available for the Super Administrator. It allows you to define an access to a data source. You define its name, description, driver, URL and the schema (optional).
"Session"	Allows you to list each created item. There is one session per object type.
"Session Group"	Allows you to define the organization of your sessions.

Table 40 Administration Menu Entries

Menu Entry	Description
"XML Import / Export"	Allows you to import/export xml files containing general configuration data. It is useful to add or update specific reports. You can also export a report deletion. The result of this export is a zip file containing 2 XML files.
"Control Group"	Allows you to group control tasks together.

Description of the Main Configuration Types

Entity

To create a new entity or group of users (example: Paris Team) if no personalized field is defined:

1. Click on the **Entity** menu entry.
2. Click on the icon.
3. Enter a name and description.
4. Save by clicking on the icon.

You will now be able to choose the entity when creating a new user.

Message Type

To define the type of warning message you want to receive:

1. Click on the **Message Type** menu entry.
2. Click on the icon.
3. Enter a name and description.
4. Select the Message provider you want to use (either sms or e-mail). By default, four providers are included but you can obtain additional providers according to your sms gateway or your email server.
5. Click on the Properties tab.
   - **a.** If you selected SMS HTTP Clickatell under the **Description** tab:
     - Enter the API Product ID.
     - Enter the user name and password provided by Clickatell to access their service.
   - **b.** If you selected SMS HTTP SMStoB under the **Description** tab:
     - Enter the email address.
     - Enter the user password.
   - **c.** If you selected Email or Email Mobility under the **Description** tab:
     - Enter the Smtp Host's name.
     - Enter the recipient's address in the **From** Address field.
     - Enter a URL that will be displayed in the message content.
6. Save by clicking on the icon.

Maintenance Period

To configure a maintenance period:

1. Click on the **Maintenance Period** menu entry.
2. Click on the icon.
3. Enter a name and description.
4. Select the profile that has access to the maintenance period.
5. Define a **Start** and **End** date when the maintenance period must start and stop.
6. Select the **Active** checkbox to make the function available.
7. Enter the information and maintenance duration in the corresponding fields.
8. If you want to precisely configure the maintenance period, you can define the minute, hour, day of month, month, and the day of the week for the maintenance process.
9. Save by clicking on the icon.

Theme

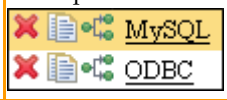
To create a theme:

1. Click on the **Theme** menu entry.
2. Click on the icon.
3. Enter a name and description.
4. Enter the name of the directory where your theme will be stored on the server.
5. Enter the name of the logo you want to display on the left-hand side of the screen. Make sure the logo is stored in `/home/exaprotect/conf/<instance_name>/report/pub/<theme_name>/img` directory.
6. Select the standard and navigation fonts.
7. Define the type of each font.
8. Define the color of the various elements composing the general interface:

Table 41 Description of the Element Color Modification

Element	Description
Main color	Changes the color of the menu and general screen main upper frame - where administration link is displayed.
Button color	Changes the color of all the buttons.
Button light color	Changes the color of the button's light border (usually used to texture the button).
Button dark color	Changes the color of the button's dark border (usually used to texture the button).
Toggled button color	Changes the color of the switch buttons when they are active or pushed in.
Table/group header background color	Changes the color of the table/list header background.
Active link color	Changes the link color when you hover the mouse over the link.
Title color	Changes the color of each page title.

Table 41 Description of the Element Color Modification

Element	Description
Footer color	Changes the color of the page footer.
Current navigation item background color	Changes the color of the graphical element that highlights the menu entry when it is active.
Odd row background color	Changes the color of odd rows in a list of elements. Example: 
Parameter filters background color	Changes the color of the dashboard's filter screen that you display by clicking on the button.
Popup screen title color	Changes the color of the pop-up screens upper bar.
Popup screen light color	Changes the color of the pop-up screens light border (usually used to texture the button).
Popup screen dark color	Changes the color of the pop-up screens dark border (usually used to texture the button).
Popup screen background color	Changes the background color of the pop-up screen that opens when clicking on a button.
Standard border color	Changes the color of the main interface border (but not the menu border).
Parameter toolbar background color	Changes the color of the tabs of each page.
Parameter background color	Changes the background color of the central configuration pages.
Dashboard active cell title - background color	Changes the color of the head of the dashboard screen that appears when hovering the mouse over it.
Message background color	Changes the frame color containing messages for the user (such as validation question).

9. Click on the button in front of the element you want to modify. The **Color Definition** screen is displayed.

10. Select the color you want to apply by clicking on the colored bars until you obtain the right color.

11. Click on **OK**.

12. Define the version number.

13. Save by clicking on the icon.

Folder

To define a folder to share with other users:

1. Click on the **Folder** menu entry.

2. Click on the icon.

3. Enter a name and description for the folder.

4. Indicate the network access path to the folder.

5. Indicate the folder's level.

6. Save by clicking on the  icon.

User

To define a new user:

1. Click on the **User** menu entry.
2. Click on the  icon.
3. Enter a name and description.
4. To make the user active, select the **Active** checkbox.
5. Enter the date when the user starts to be active in the **Start Date** field and when s/he stops to be active in the **End Date** field.
6. If you want the user to have access to the web portal, select the **Standard Access** checkbox.
7. If you want the user to receive alert messages (e-mail, SMS), select the **Messaging Access** checkbox.
8. If you want the user to have access to scorecards, select the **Scorecard Access** checkbox.
9. Select the **Mobile Access Point** (which you must have previously created under the **Access Point** menu entry).
10. If you want the user to access the portlets, select the **Portlet Access** checkbox. If not, deselect the checkbox.
11. If you want the user to be allowed to change his password, select the **Change Password** checkbox.
12. If you want the screen display to be automatically adjusted according to the screen size, select the **Auto Adjust Screen Size** checkbox.
13. If you want the screen size to be displayed according to the user profile needs, fill in the **Screen Width** and **Height** fields.
14. Select the workspace to combine with the user in the **Workspace** drop-down list.
15. Select the user group to which the user belongs in the **Entity** drop-down list.
16. Select the default user language in the **Language** drop-down list.
17. You have the possibility to define the dashboard to be displayed in the homepage by selecting it in the **Home** drop-down list.

    However, it is highly recommended that you define the default dashboard directly from the SMP server. Please refer to the Accessing Security dashboards section to know how to define it.
18. Select the default theme you want to use for the interface display in the **Theme** drop-down list. Please refer to the "Theme" section to know how to create a theme.
19. Select the default image format used by the user in the **Chart Type** drop-down list.
20. Select the default profile to be associated with the user.
21. If you want to enter additional information, click on the **Personalized Field** tab.
22. Enter a value in front of the field title.

> **Note:** The field title is only available if you have created personalized fields. Please refer to the "Personalized Fields" section to create them.

System Preferences

To configure system preferences:

1. Click on the **System Preferences** menu entry.

2. Select the system language (different from the user language) in the **Default Language** drop-down list. The Welcome page where you enter the login and password will be displayed in the selected language.

3. Indicate the maximum menu items' number of characters in the **Truncate the Menu to (Characters)** drop-down list. The value must be included between 10 and 50.

4. Select the PDF document export mode in the **PDF Generation Tool** drop-down list.

5. Enter the size of the object and the connection pool used in the respective fields.

6. If you want to display confirmation messages when doing an action, select the **Display Confirm Dialog** checkbox. It allows you to validate your choice a second time and offers a protection against manipulation errors .

7. If you want to firstly display the filter when configuring setting sessions, select the **Show Parameters Filter First** checkbox.

8. If you want to give users the possibility to choose their language, select **The User can Choose his Language**.

9. If you want to display filter criteria at the top of reports, select the **Report Filter on Top** checkbox.

10. If you want to give users the possibility to choose their theme, select the **The User can Choose his Theme** checkbox.

11. If you want to allow a direct link between reports, select the **Direct Dynamic Link** checkbox.

12. Save by clicking on the  icon.

The XML “export” and “import” functions allow you to generate a PDF document or SQL script containing the whole of the parameter settings.

Personalized Fields

To configure personalized fields:

1. Click on the **Personalized Fields** menu entry.

2. Click on the  icon.

3. Enter a name and description.

4. Select the desired parameters.

5. Select the data type you want to display.

6. Enter the default value you want to be displayed in the field.

7. Save by clicking on the  icon.

Style

To create a style to be applied to graphics:

1. Click on the **Style** menu entry.

2. Click on the  icon.

3. Enter a name and description.

4. Select the predefined default color set in the **Graphics Default Color Set** drop-down list. Please refer to the "Color List" section to know how to define the color set.

5. Define the style of header, body, comment, section, global breaks and calculations display. To do so, click on the  button in front of the elements you want to modify.

The **Style Definition** screen is displayed.

6. Enter the color and background color codes or click on the  button in the **Color** field. The colored square immediately displays the color you have just chosen.

7. Select the font, size, style, weight and alignment of the text in the corresponding fields.

8. Click on **OK**.

9. Define the reports' border type you want to display by selecting the respective checkboxes.

If you want to display reports' horizontal borders, select the **Display Horizontal Borders** checkbox.

If you want to display reports' vertical borders, select the **Display Vertical Borders** checkbox.

If you want to have different colors between each report's lines, select the **Switch Rows Background Colors** checkbox.

10. Indicate if you want to alternate the background colors for rows by selecting the corresponding checkbox.

11. Define the version number.

12. Save by clicking on the  icon.

Workspace

To create a workspace:

1. Click on the **Workspace** menu entry.

2. Enter a name and description.

3. Select the user profile you want to allow access to the workspace.

4. Define the version number.

5. Click on the **Sessions** tab. Please refer to the "Step 5: Associating the Report to the Hidden Session" section for more information on filling out the fields.

Controls and **Metrics** tabs work in the same way as the **Sessions** tab.

World

To create a world:

1. Click on the **World** menu entry.

2. Click on the  icon.

3. Enter a name and description.

4. Select the corresponding JDBC Driver that is already configured under the **Driver** tab.

5. Select the JDBC URL of the database containing your data.

6. Enter a user login and password. This login can be used by any user to have access to the corresponding world. If you want to use a login different from the one used by the portal user, select the **Use Another Connection** checkbox.

The advanced parameters located at the bottom of the screen contain default values that suit the majority of configuration. Only advanced users with solid database administration skills must modify those parameters.

Session

To create a session:

1. Click on the **Session** menu entry.
2. Click on the icon.
3. Enter a name and description.
4. Select the minimum user profile with which the user can access the current session.
5. Save by clicking on the icon.

Session Group

To create a session group:

1. Click on the **Session Group** menu entry.
2. Click on the icon.
3. Enter a name and description.
4. If you want the session group to be displayed in the main menu, select the **Active** checkbox.
5. If you want to define precisely the sorting order of the current session display, enter the level number in the **Sort Order** field.
6. Indicate in which folder the current session group will be included by selecting the folder in the **Parent Session Group** drop-down list.
7. Save by clicking on the icon.

XML Import / Export

To export a zip file containing interface configuration data xml files:

1. Click on the **XML Export** menu entry.
2. If you want to export your report configuration, click on the **XML Export** button. A pop-up screen is displayed asking you to save or open the file.
3. If you want to add/update data in the file you are going to export, click on the button. The **Add Objects** tab is displayed.
4. Select the data (or objects) you want to export by clicking on it in the **Objects** list. You can select several objects at the same time by pressing the **Ctrl** key while clicking on the objects.
5. Select the version of the object to export. You can choose either the exact version, the version higher than the one entered, lower than the one entered...etc.
6. Select the modification date of the object to export. You can choose either the exact date, the date higher than the one entered, lower than the one entered...etc.

7. Define if you want to export the objects that are dependent or not on the selected object by selecting the **Dependent Objects** checkbox.

8. Enter the dependency level in the respective field.

9. Click on the button to go to the next step. The **Result of Research** tab is displayed.

Result of Research Tab

1. Select the objects you want to export:
   - Either one by one, by clicking on the respective checkboxes;
   - Or select the whole list of objects by clicking on the checkbox located on top of all the others.
2. Click on the button to go to the next step. The **Objects to Export** tab is displayed.

Objects to Export Tab

1. The objects to export are listed. If the list is correct, click on the **XML Export** button.
2. A dialog box is displayed asking you to download the ZIP file containing the XML files.
3. If you want to delete data in the file you are going to export, click on the button. The **Delete Objects** tab is displayed.
4. Select the object you want to delete from the list in the **Objects** drop-down list.
5. Enter the exact name of the object.
6. Enter the version of the object you want to import.
7. Click on the button to go to the next step. The **Result of Research** tab is displayed.
8. Select the objects to delete.
9. Click on the **Export XML** button.

Note about the Save and Load buttons

The **Save** and **Load** buttons located at the bottom of the screen are useful if you need to do tasks during the xml export without losing your current export.

To save the list of objects you selected:

1. Under the **Objects to Export** tab, click on the **Save** button.
2. Navigate through the menu and perform needed actions.
3. Click on the **XML Export** menu entry to go back to the **XML Export** screen.
4. Click on the **Load** button.

To import an xml file containing interface configuration data:

1. Click on the **XML Import** menu entry.
2. Select the directory from where you want to import the xml file.
3. Enter the name of the xml file.

4. Click on the button to validate the import configuration. A list of the zip file contents is displayed.

   For each object, the name and description are displayed as well as the xml and database versions - if defined.

   Note that if the imported version is higher than the current version, then an update is automatically completed.

5. Click on the **Import** button.

Control Group

To create a control group:

1. Click on the **Control Group** menu entry.
2. Click on the icon.
3. Enter a name and description.

Sending Reports by E-mail Automatically

The reporting module allows you to automatically send generated reports by e-mail. To do so:

1. Configure the **Message type** screen as explained in section Message Type.
2. Select **Home > Configuration > Administration > User > Superadmin**.
3. Under the **Description** tab, select the **Messaging access** checkbox and save.
4. Select **Home > Configuration > Task > Task** and click on the icon to create a new task.
5. Create a new task as explained in section Creating a New Task.
6. Enter the relevant parameters as explained in section Control: Creating a Task to Monitor Data.

The report will now be automatically sent to the relevant users at a frequency you defined.

Live Reporting Policy

With the live reporting functionality, you will have precise control over the configuration of data groupings to immediately generate customized reports. The SMP live reporting functionality comprises several database tables and each table defines a certain configuration of data groupings.

Unlike Batch reporting policies, Live reporting policies are based on unitary event and are calculated in “real-time” before aggregation and correlation processes.

This section contains several procedures to:

- Open the Live Reporting Policy Screen
- Add a New Definition for a Table
- Copy an Existing Table
- Enable a Table
- Disable a Table
- Delete a Table

Open the Live Reporting Policy Screen

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

By default, standard policies are listed. They are not editable.

Figure 85 The Live Reporting Policy main screen.

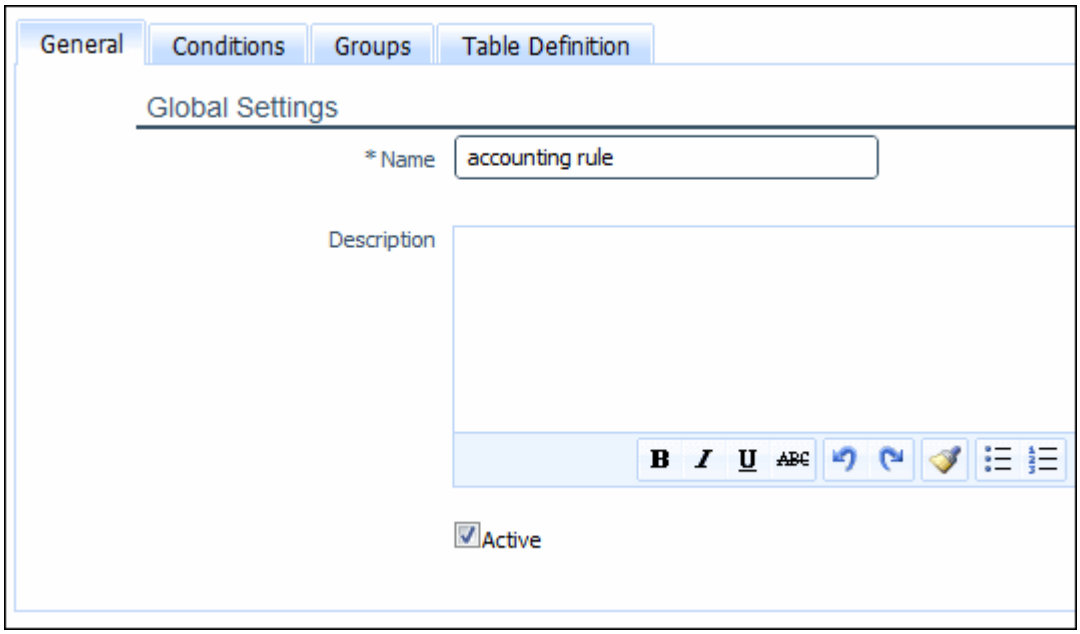
Add a New Definition for a Table

To add a new definition for a table:

1. Click on the **Add** button.

   The **Live Reporting Rule Creation** screen opens.

Figure 86 The “Live Reporting Rule Creation” screen



General tab

1. Enter a name and description for the table.

2. If you want to make the table immediately active, select the **Active** checkbox.

Conditions tab

1. 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.

2. Add the relevant conditions and/or exceptions by clicking **Add**. The **Add a new Condition/Exception** screen is displayed.

3. Select the type of condition/exception you want to use: either **Field Matching** or TIBCO LogLogic® Taxonomy.

- **Field Matching**: Specify the field contents in the event, e.g., Target hostname is "server1". Then several fields are displayed as described in the table below.
- TIBCO LogLogic® Taxonomy: Specify how the event has been categorized, e.g., the action is ***malware*** and the target is a ***database***.

Table 42 Add New Condition Fields

Field	Description
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 theTaxonomy 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". **Note:** The field is not case-sensitive.

4. Click **OK**.

Groups tab

To define how data will be grouped.

1. Click on the **(none)** entry. The **Group Field** pane is displayed.

2. Select 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.

3. Select the **Field's value Required** checkbox if only events with a defined field's value must be grouped.

4. Click **OK**.

5. In the **Groups** tab, indicate the processing order of rules by checking the relevant rule and clicking on **Move Up** or **Move Down**.

Table Definition tab

To specify the type of tables to be taken into account to build a dashboard in the **Reporting** interface.

1. Select the time scale you want to consider:
    - Hour, day and month tables.
    - Day and month tables.
    - Month table only.
2. Enter a name for your table. You cannot enter more than 35 characters as the whole table name cannot contain more than 64 characters.
3. Click **OK**.

Copy an Existing Table

To create a copy of an existing table:

1. Select desired table(s) by clicking on one or more selection boxes located in the first column on the left. Clicking on the top most box (located to the left of the **Name** column heading) will select all tables, even those that are not displayed on the current page.
2. Click the **Copy** button. A copy of each selected table is created and entitled **"table's name_copy"**. If you create another copy of the same table, the name will be **"table's name_copy_2"** and so on.
3. Click on the  icon to access the copy automatically set at the end of the list.
4. Click **OK** to validate the copy.
5. Enter a description in the **History** field then click **OK**.
6. Synchronize the engine to take the policy into account by clicking on the **synchronize** link.

Enable a Table

This means that the selected tables will be filled automatically.

To enable a table:

1. Select the table by clicking on the box next to the table's name.
2. Click on the **Enable** button.

The table will be enabled and the listing will be updated.

Disable a Table

This means that the selected tables will not be filled automatically.

To disable a table:

1. Select the table by clicking on the box next to the table's name.
2. Click on the **Disable** button.

The table will be disabled and the listing will be updated.

Delete a Table

To delete one or more tables:

1. Select desired table(s) by clicking on one or more selection boxes located in the first column on the left. Clicking on the top most box will select all tables (even those that are not displayed on the current page).

2. Click on the **Delete** button.

3. A confirmation message appears. Click **OK** to proceed with the deletion or click **CANCEL** to cancel the operation.

Batch Reporting Policy

The **Batch Reporting Policy** is based on the data mart concept. A data mart is a specialized version of a data warehouse. A data mart is predicated on defining certain groupings of data, which permit easy access to relevant information. Data marts contain snapshots of operational data which allow users to analyze past experiences.

With the **Batch Reporting Policy** functionality, you will have precise control over the configuration of data groupings to later generate customized reports. The **Batch Reporting Policy** functionality comprises several database tables and each table defines a certain configuration of data groupings.

Unlike Live Reporting policies, Batch reporting policies are based on alerts and aggregated events and are calculated once a day (by default at 3:00 am).

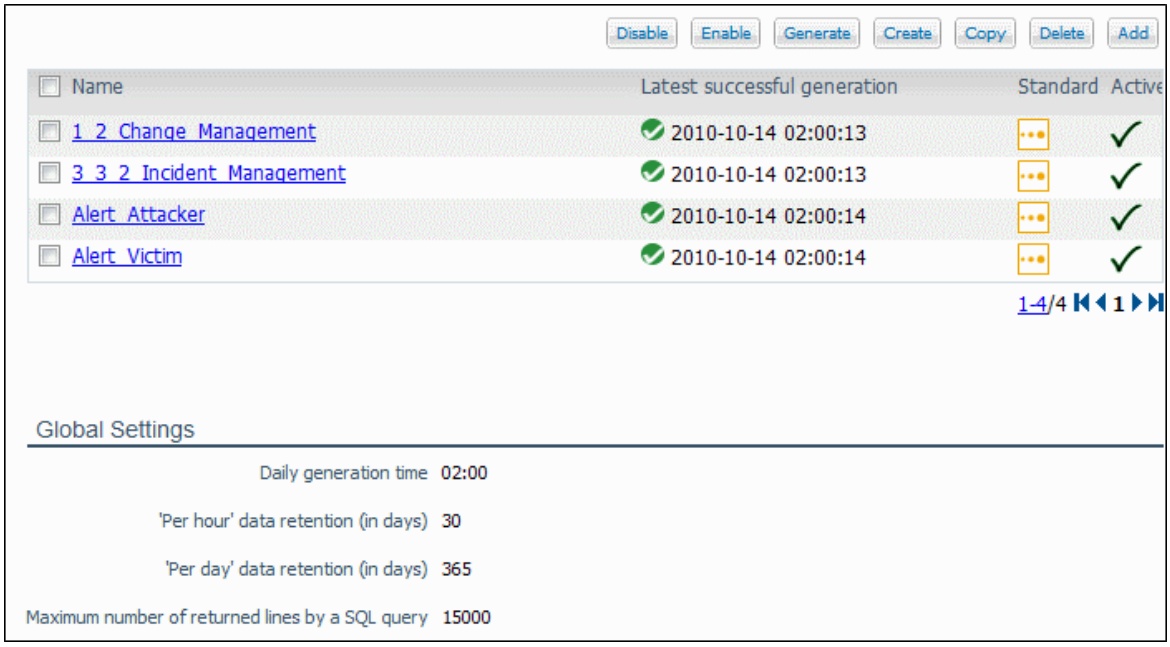
This section contains several procedures to:

- Open the Batch Reporting Policy Screen
- Add a New Definition for a Table
- Edit the Global Settings
- Create a Table
- Generate a Table
- Copy an Existing Table
- Enable a Table
- Disable a Table
- Delete a Table

Open the Batch Reporting Policy Screen

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

Figure 87 The Batch Reporting Policy main screen.

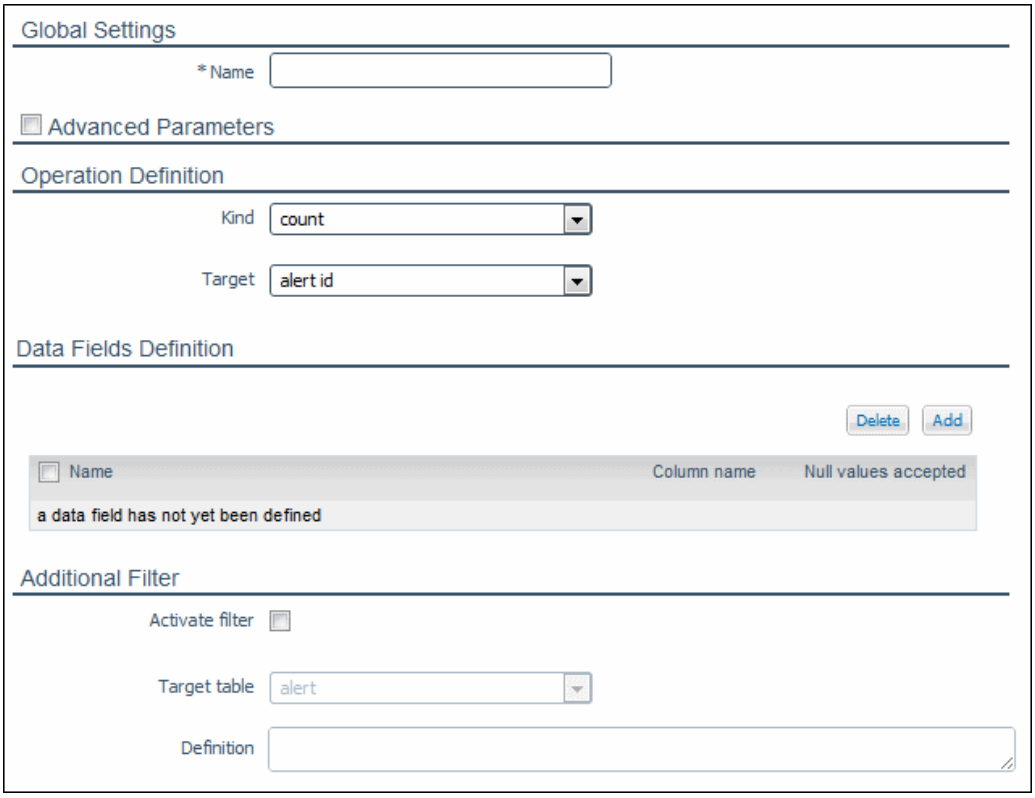


Add a New Definition for a Table

To add a new definition for a table:

1. Click on the **Add** button.
2. The **Batch Reporting Rule Creation** screen will open.

Figure 88 The "Batch Reporting Rule Creation" screen



Global Settings

1. In the **Global Settings** section, enter the name for the new table in the ***Name*** field (required).

When entering a table name, please remind that:

- The file name must contain only the following character types: a-z, A-Z, (accents) -, _, @ and it must not start with _, - or @
- The system will automatically add "Exa_TAT_Batch" to the beginning of the table name.
- You cannot enter more than 35 characters.

2. Check the **Advanced Parameters** box to enter optional information.

3. In the **Advanced Parameters** section, select the frequency by which data is grouped in the table in the **Time scales** drop-down list. You can choose between:

- Hour, Day, and Month tables (this will create 3 separate tables).
- Day and Month tables (this will create 2 separate tables).
- Month table only.

4. Select a target unit: aggregated events, alerts or all alerts and aggregated events.

5. Select a time shift number 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

If you need to further customize the operation for your table, select the relevant data in the **Operation Definition** pane.

1. Select the kind of the operation in the **Kind** drop-down list. The available types of operation are: Count, Average, Sum, Minimum, Maximum.

2. Select a field in the **Target** drop-down list. Please see the database model for possible field names.

Data Fields Definition

Editing a Data Field

This screen allows you to edit, add, or delete data field definitions.

1. Click on the data field definition you wish to edit.

The "**Editing the Data Field**" screen opens:

Figure 89 The Data Fields Edition Screen

Note: Fields marked with an asterisk are required.

2. Enter the generated column name and select if null values are accepted.

3. Click **Back** when finished.

Creating a New Data Field

1. In the **Data Field Definition** section, click on the **Add** button.
2. The **Create New Data Field** screen opens.

> **Note:** 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.

3. In **Normal mode**:
   - Select the ***Reference Data*** name from the listing.
   - Enter the ***Generated column name*** and select if null values are accepted. Fields marked with an asterisk are required.
4. In **Advanced mode**:
   - Select the ***Reference Data table label*** from the listing and enter the field name.
   - Enter the Generated column name and select if null values are accepted.
   - Enter the SQL type. Fields marked with an asterisk are required.
5. Click **OK** when finished or click **Cancel** to cancel the operation.

Deleting a Data Field

1. Click on the leftmost box related to the data field definition you wish to delete.
2. Click on the **Delete** button.
3. Confirm your deletion request by clicking on **OK**.

Additional Filter

In this section you will define additional filters for your report. To do so:

1. Select the **Activate Filter** checkbox to make the options below active.
2. Select the **Target Table** in the drop-down list, i.e. the table where the filter will be applied to.
3. Enter the table definition in the SQL language format.

Important notes about the SQL statement:

- The SQL statement should begin after the keyword **WHERE**.

  For example, if the full statement were:

  SELECT alert.create_date, count(alert.alert_id) FROM Exa_alert alert WHERE alert.display_severity=3 GROUP BY alert.create_date;

  You should enter in the ***Definition*** field:

  alert.display_severity=3

- The statement must have the following format: **<table_name>.<field_name>**.

  <table_name>: The table name must be the same as the one you previously selected in the **Target Table** drop-down list.

  <field_name>: The field name must be the same as the one displayed in the **Column Name** column.

- Pay special attention to the priority of **AND** and **OR** operators when there is more than one condition. If necessary, use parentheses to avoid incorrect logical combinations.

For example, you should enter something like: (analyzerid='myAnalyser1' AND evt_col_type_id=2) OR analyzerid='myAnalyzer2'

- The **GROUP BY** clause is not necessary.

1. Click the **Copy** button. A copy of each selected table is created and entitled "***table's name***_copy". If you create another copy of the same table, the name will be "***table's name***_copy_2" and so on.

> **Note:** You can change the name and other parameters of the created table by clicking on the name of the table. A screen with the configuration for the table will open. Please see Add a New Definition for a Table for details on how to configure all table parameters.

Edit the Global Settings

To edit the global settings:

1. Click on the **Edit** button below the **Global Settings** section. The **Global Settings** screen appears.

2. Click on the field you wish to change and enter the new value.

Table 43 Global Settings

Field	Description
Daily generation time	Indicate the time (in hour and minute) when reporting statistics generation is launched
'Per hour' data retention (in days)	Indicates the maximum number of days the lines in the Hour table are kept. e.g. if you enter 200, it means that lines generated more than 200 days ago will be removed from the table.
'Per day' data retention (in days)	Indicates the maximum number of days the lines in the Day table are kept. For example, if you enter 200, it means that lines generated more than 200 days ago will be removed from the table.
Maximum number of returned lines by a SQL query	Indicates the maximum number of lines available in the Hour table when generating reporting statistics in one time. **Note:** you must enter a value between 1 and 15000.

3. Click **OK** to implement changes or **CANCEL** to cancel the edits.

4. The **Global Settings** screen will close automatically. If you clicked on **OK**, the system will display a message confirming the changes.

Create a Table

Creating a table means that the SQL table will be created, but it will not be filled with the latest alerts. See also "Generate a Table".

You should have previously created a new definition for the table (see "Add a New Definition for a Table").

To create a table:

1. Select the table by clicking on the box next to the table's name.

2. Click on the **Create** button. A message is displayed indicating whether the operation was successful or not.

Generate a Table

Generating a table means that the SQL table will be created and filled with the latest alerts.

To generate a table:

1. Select the table by clicking on the box next to the table's name.

2. Click on the **Generate** button. The table will be generated and the listing will be updated.

Copy an Existing Table

To create a copy of an existing table:

- Select desired table(s) by clicking on one or more selection boxes located in the first column on the left. Clicking on the top most box (located to the left of the **Name** column heading) will select all tables, even those that are not displayed on the current page.

Enable a Table

This means that the selected tables will be filled automatically every day/night.

To enable a table:

1. Select the table by clicking on the box next to the table's name.

2. Click on the **Enable** button. The table will be enabled and the listing will be updated.

Disable a Table

This means that the selected tables will not be filled automatically every day/night.

To disable a table:

1. Select the table by clicking on the box next to the table's name.

2. Click on the **Disable** button.

The table will be disabled and the listing will be updated.

Delete a Table

To delete one or more tables:

1. Select desired table(s) by clicking on one or more selection boxes located in the first column on the left. Clicking on the top most box will select all tables (even those that are not displayed on the current page).

2. Click on the **Delete** button.

3. A confirmation message appears. Click **OK** to proceed with the deletion or click **CANCEL** to cancel the operation.

Tables Contents

All the tables are stored into the database **exa_<InstanceName>**.

The naming convention used in these tables is the following:

Table 44 Naming Convention

Type of Reports	Name
daily	**Exa_TAT_Batch_<TableName>_hour**
monthly	**Exa_TAT_Batch_<TableName>_day**
annual	**Exa_TAT_Batch_<TableName>_month**

The **<TableName>** is the name of the reporting table used in the field name when configuring the table.

Hour Tables

The hour tables contain the following fields:

Table 45 Hour Table Content

Table	Description
Hour	In yyyy-MM-dd hh:mm:ss date format
Count	The number of alerts or raw logs on a given hour
A list of fields selected during the configuration.	

Daily Tables

The daily tables contain the following fields:

Table 46 Daily Table Content

Table	Description
Day	In date format yyyy-MM-dd
Count	The number of alerts or raw logs on a given day.
Minimum	The lowest value of the **Count** column taken from the **Hour table** for an hour on a daily time period.
Maximum	The lowest value of the **Count** column taken from the **Hour table** for an hour on a daily time period.
Average	The average number of alerts generated for an hour on a daily time period.
A list of fields selected during the configuration.	

Monthly Tables

The monthly tables contain the following fields:

Table 47 Monthly Table Content

Table	Description
Month	In date format yyyy-MM-dd [dd] always corresponds to the first day of the month, which is [01].
Count	The number of alerts or raw logs on a given month.
Minimum	The lowest value of the **Count** column taken from the **Daily table** found for a day on a monthly time period.
Maximum	The higher value of the **Count** column taken from the **Daily table** found for a day on a monthly time period.
Average	The average number of alerts generated for a day on a monthly time period.
A list of fields selected during the configuration.	

Example of Tables

Table 48 select * from Exa_TAT_Top_Target_Address_hour

hour	address_id	node_id	domain_id	count
2007-07-17 13:00:00	2	2	0	10
2007-07-18 07:00:00	2	2	0	9
2007-07-19 12:00:00	2	2	0	4
2007-07-19 12:00:00	2	2	0	1
2007-07-19 15:00:00	2	2	0	2
2007-07-20 00:00:00	NULL	1	0	1
2007-07-21 00:00:00	2	2	0	1
2007-07-22 00:00:00	2	2	0	1
2007-07-22 02:00:00	2	2	0	1
2007-07-23 00:00:00	2	2	0	4
2007-07-23 11:00:00	2	2	0	1
2007-07-23 12:00:00	2	2	0	1
2007-07-23 14:00:00	2	2	0	1

Table 49 select * from Exa_TAT_Top_Target_Address_day

day	address_id	node_id	domain_id	count	min.	max.	avg.
2007-07-17	2	2	0	2	2	2	2
2007-07-18	2	2	0	9	9	9	9
2007-07-19	NULL	1	0	1	1	1	1
2007-07-19	2	2	0	11	1	10	6
2007-07-20	2	2	0	1	1	1	1
2007-07-21	2	2	0	1	1	1	1

Table 49 select * from Exa_TAT_Top_Target_Address_day

day	address_id	node_id	domain_id	count	min.	max.	avg.
2007-07-22	2	2	0	5	1	4	3
2007-07-23	2	2	0	7	1	4	2

Table 50 select * from Exa_TAT_Top_Target_Address_month

month	address_id	node_id	domain_id	count	min.	max.	avg.
2007-07-01	NULL	1	0	1	1	1	1
2007-07-01	2	2	0	36	1	11	5

Description

These tables give you a list of the alerts emitted either in the hour of a given day or in a day of a given month.

Let us take the example of alerts emitted on the 2007-07-23.

1. In **Table 48 - hour** column, there are four rows referring to the 2007-07-23.

2. For each of these four rows, take the number in the **Count** column and do a sum. You obtain: **4 + 1 + 1 + 1 = 7**.

3. 7 is the value that you have in **Table 49 - Count** column for the 2007-07-23 row.

4. It means that 7 alerts have been generated on the 2007-07-23 in a time range you previously defined.

5. Number 7 is decomposed into **Maximum, Minimum** and **Average** columns in order to list the maximum, minimum and average number of alerts in an hour for a given day.

6. In the **Minimum** column, at least 1 alert per hour is collected.

7. In the **Maximum** column, there is a maximum of 4 collected alerts per hour.

8. In the **Average** column, 2 alerts have been generated for this day. A calculation must be completed to know the average number of alerts per day:

- Take the numbers in the **Count** column of **Table 48** and do a sum: 4 + 1 + 1 + 1 = 7.
- Then, divide this number by the number of corresponding rows, that is to say 4.
- You obtain 7/4 = 1,75 in other words 2.

Building Reports Based on Reporting Tables

Building reports with reporting tables allows you to optimize the reports calculation time and then the display. It depends on the table type you use:

- For daily and weekly reports, use hourly reporting tables.
- For monthly reports, use daily reporting tables.
- For annual reports, use monthly reporting tables.

Please refer to section Reporting of this documentation to create your report based on reporting statistics.

Chapter 8 - Configuring...

To meet the user specific needs and to ensure the security of the information, basic information must be configured in SEM.

In this part of this document, you will learn how to configure:

- User Accounts
- External Servers
- Backup
- Raw Logs Archiving
- Configuration Profiles and Security Levels

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.

Add/Edit Users

General Information

1. Go to **Configuration > User Accounts >click on the Add button**.
2. Enter a unique identifier in the **Name** field (no more than 50 characters). It can be a name or an e-mail address.
3. Select the authentication mode. There are two possibilities:
    - If you use the standard authentication, select the **Local Password** radio button
    - If you use an external authentication method via **RADIUS**, select the **Radius Password** radio button.

Password RADIUS

Caution: When configuring a RADIUS user, it is recommended to create another local account.

In the event of a **RADIUS** server failure, the **superadmin** account may be lost and as a consequence, all the other user accounts will not be editable. Another solution is to create a new superadmin account via the SMPConfig tool (see the ***Administration Guide*** for more information).

The password you configured via **RADIUS** will be the one you must enter when connecting to the Web Console.

To authenticate via the RADIUS server, you must have configured the TIBCO LogLogic® connection options. See External Servers section for more information.

1. Enter the TIBCO LogLogic® user's authentication password (no more than 25 characters) in the **User Password** field and confirm it.

The password must be at least 8 characters long with at least one alphabetic and one numeric character.

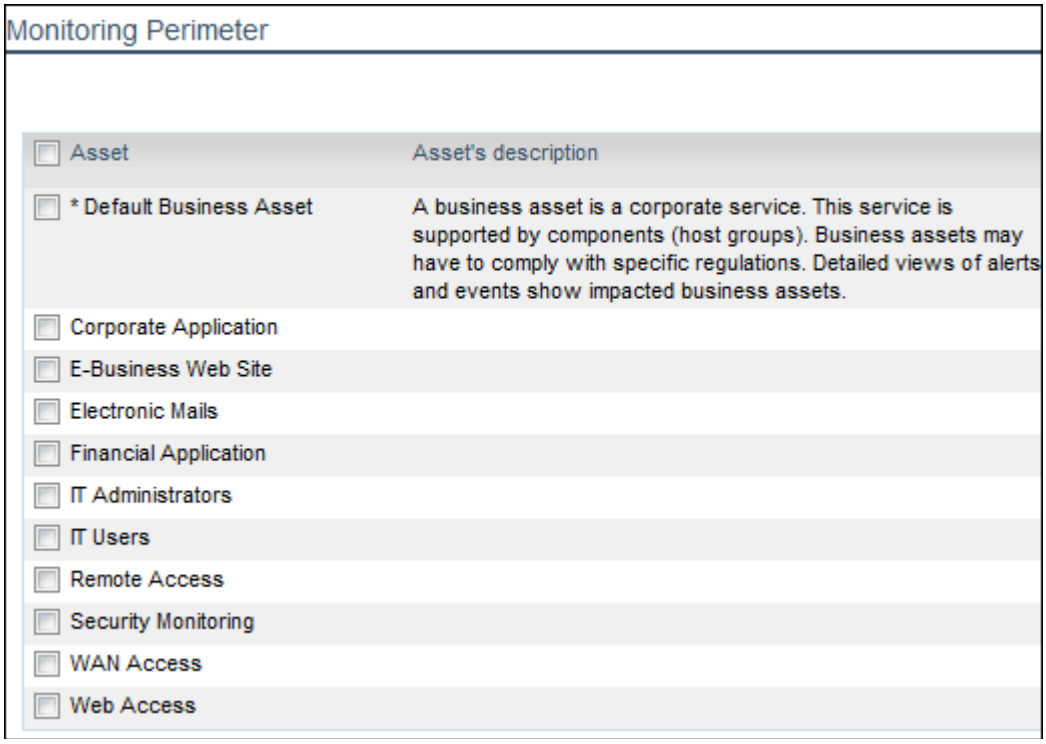
2. Select the right to be granted to the user in the **User rights** drop-down list.

Table 51 User Rights

User Rights	Description
Viewer	The user must have read-only access to the GUI and cannot acknowledge alerts, create alerts or incidents. He can modify his own password.
Analyst	The user must have all the rights of viewers and can acknowledge alerts, manage incidents, and manage the asset database.
Administrator	The user must have all the rights of analysts and can also make changes to the Security Event Manager configuration.
Super-Administrator	The user must have all the rights of administrators but also if he can delete alerts without prior backup, modify a RADIUS user account and make any change to the Security Event Manager.

Users cannot modify their own rights. If you select Analyst or Viewer, the **Monitoring Perimeter** table is displayed.

Figure 90 Monitoring Perimeter

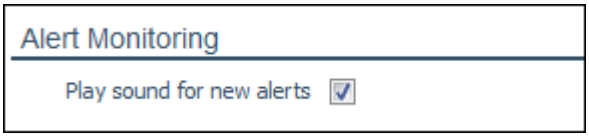


When creating or editing an **Analyst** or a **Viewer** user's profile, the administrator must select which **log source asset** the user is allowed to view events from, by ticking the checkbox(es) next to the list of assets.

Playing sound for new alerts

- Turn on the **Play sound for new alerts** tick box if you want to play a sound if a new alert is received when the list of alerts is set to pause, that is if you clicked on the **Suspend** button in the alert monitoring screen.

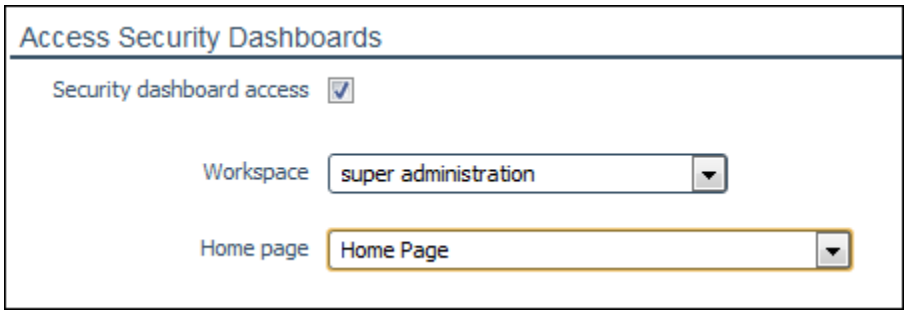
Figure 91 User Creation - Alerts Monitoring



Accessing Security dashboards

1. If the user is to have access to the reporting module, click the **Security dashboard access** checkbox.

Figure 92 Access Security Dashboards



If not, you can leave the **Workspace** and **Home page** fields blank.

2. Select the **workspace** which corresponds to the user type, i.e. Super-administrator, Administrator, Manager or Analyst. Workspaces delimit the different reports available for different user roles. Each workspace contains a list of available reports.

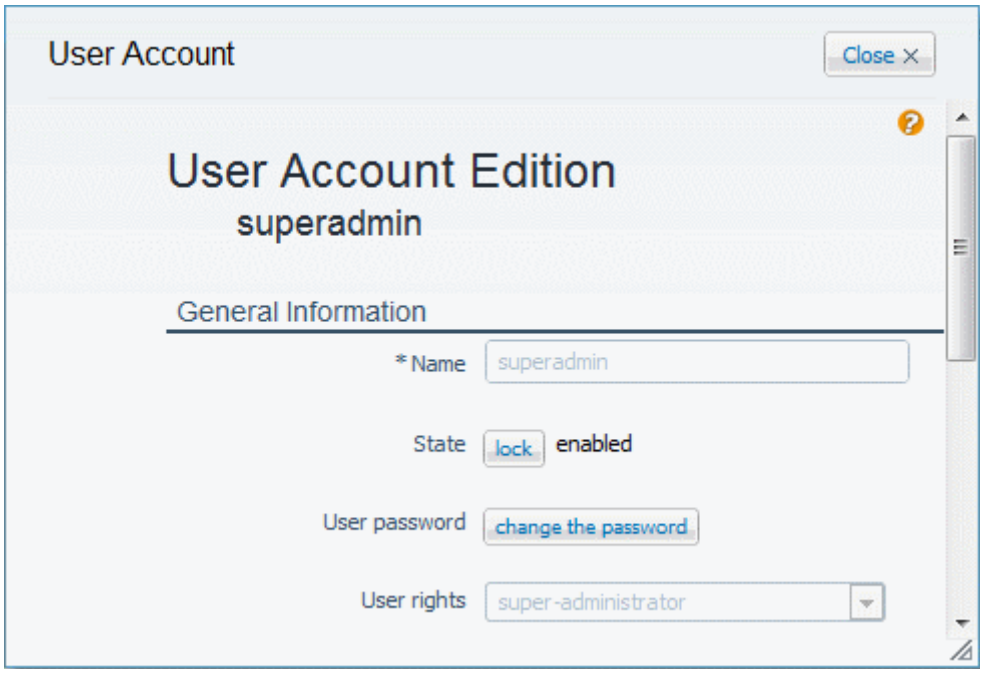
3. Specify the initial page to be displayed to the user when starting the security dashboard module.

4. Click **OK** to save the changes and return to the previous screen, or click **Cancel** to return to the previous screen without saving changes.

Changing the Password

1. Click on the link corresponding to the user account you want to edit. The screen for editing accounts opens.

Figure 93 Editing the User Account



2. Click **Change the password**. The **Changing Password** screen opens to let you change the password.

3. Set the new password (no more than 25 characters).

- If you use the standard TIBCO LogLogic® authentication, select the **Local Password** radio button and enter the **user password** and confirm it. The password must be at least 8 characters long, with at least one alphabetic and one numeric character.
  If you are the owner of this user account, enter your previous Password and then type in the new one.
- If you use an external authentication method via **RADIUS**, just select the **Radius Password** radio button. The password you configured via **RADIUS** will be the one you must enter when connecting to the Web Console.

To authenticate via the RADIUS server, you must have configured the TIBCO LogLogic® connection options. See External Servers section for more information.

Note: If you edit your own user account, you will be asked to enter your current password and then your new password and its confirmation.

4. Re-enter it in the **Confirm Password** field and click **OK** to validate.

Locking/Unlocking a User Account

For security reasons, only users with the administrator or super- administrator account have the right to lock or unlock a user account.

If a user fails to login after three successive attempts - e.g. by using the wrong password or login - he will not have access to the Web Console any longer.

In that case, the user must notify the user with the administrator or super-administrator account to unlock the account. To do so, he must:

1. Tick the check box in front of the relevant user name in the list of users

2. Click on the **Unlock** button. The user can now connect again to the Web Console with the same login and password he initially configured.

External Servers

LMI (LX/ST/MX) Server

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

1. Click on the **Add** button.

2. Enter the host address and the port and click **OK**.

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.

1. Go to **Configuration > External servers > Incident Notification tab**. The **Incident Notification** screen is displayed.

2. Select the **Notify on new, modified and closed incidents** checkbox to activate or deactivate the notification process.

3. Enter the remote server configuration URL. If you selected the **Incident Notification** checkbox, this parameter is mandatory. The format is: `http[s]://{incident_server_IP}:{port}/path`.

4. If you entered an **https** URL in the previous field, the **Authentication** field is available. Then, two options are possible:

- Select **simple** if you only want to use a user login and password to be authenticated.
- Select **certificate** if you want to use a certificate to be authenticated.

5. Enter the various connection information:

- either the login and password if **simple** has been previously selected.
- or upload the client certificate if **certificate** has been previously selected.

6. Upload the CA server certificate to verify the validity of the server certificate provided during the connection.

7. Select one of the relevant checkboxes to validate the certificate's revocation.

8. Define the minimum time period between two notifications by dragging the arrow on the horizontal slider. E.g. if you define 60 seconds as a period of time, then each 60 seconds, you will receive a notification about your incidents. You can also enter a value in the field box on the right.

9. Click on the **Test the connectivity to the incident server** link to check if the server communicates correctly. If it is not OK, it means that the server is not correctly configured to communicate with EventManager.

10. Click on the **Synchronize the incidents** link to apply the modification. If an error occurred, you must check the following settings:

- the SOAP server is currently working.
- the spool has not been completely emptied.
- there is a problem on the SOAP server itself.

External Authentication with RADIUS

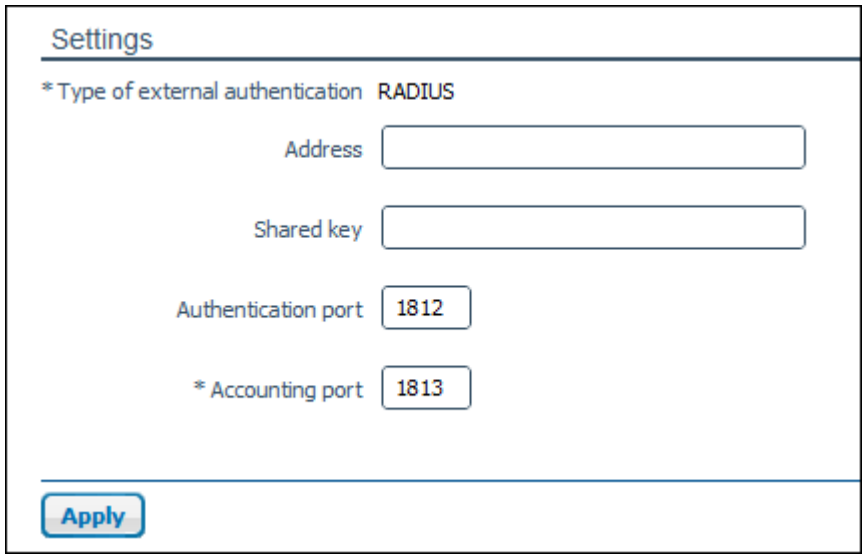
Security Event Manager can contact a RADIUS external server to authenticate users that try to log in.

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.

1. Go to **Configuration > External servers > External Authentication tab**.

The **Radius Authentication Configuration** screen is displayed.

Figure 94 Radius Authentication Settings



2. Complete the four fields with the following information:

- RADIUS IP server address or hostname.
- RADIUS shared secret key.
- RADIUS server authentication port.
- RADIUS server accounting port.

3. Click **Apply**.

You can now configure the users that must authenticate externally via the **User Rights** screen as explained in "Add/Edit Users".

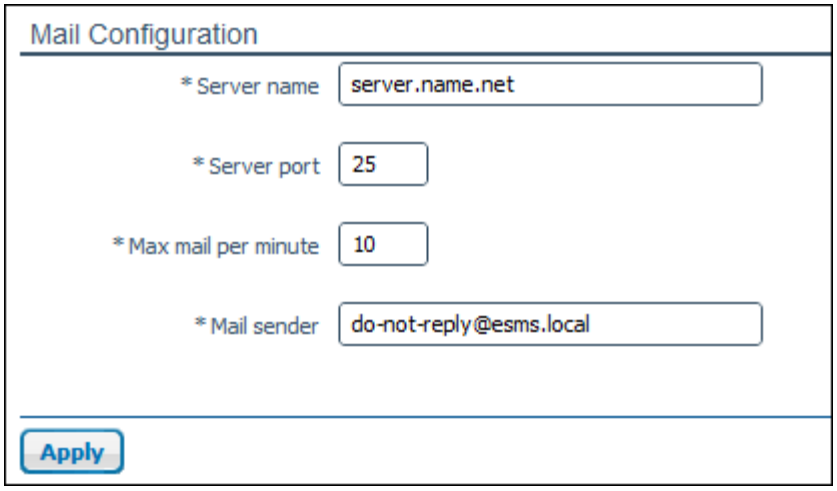
Mail Configuration

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

1. Go to **Configuration > External servers > Mail Configuration tab**.

The **Mail Configuration** screen is displayed.

Figure 95 Mail Configuration tab



2. Complete the four mandatory fields with the following information:

- IP address or DNS name of the sent mail server.
- Port used by the SMTP server.
- 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.
- Sender's address. It is recommended not to use the default value but to enter a customized value.

3. Once the modification applied, you must restart the instance by entering the following command:

```
/etc/init.d/exa_runtime_INSTANCE restart
```

Note: A manual procedure is also possible, for more information, refer to the Administration Guide - chapter SMP Configuration.

Backup

Recommendations

- The backup function is version-dependent, i.e. you cannot perform the backup of an older version to a new version SMP. If you need to restore a backup of an older version SMP, you will need to set up a server for this purpose and execute your restore operation on this special server.

- Reconstructing your main server through a restore operation should only be done in case of a system crash or where there was another event that resulted in the destruction or loss of the current system and its configuration data.
- The SMP server must not be considered as an archiving server.

Overview

The TIBCO LogLogic® SMP Backup functionality enables you to schedule automatic backups of the configuration information stored on the TIBCO LogLogic® SMP server.

The backup file is a ZIP file that contains all of the configuration details of a particular instance - so that in the event of hardware or software application failure, this information can be quickly restored and you will not need to recreate it manually. Since in the event of hardware or software application failure, disks and files on the server can become unusable, you must have a regular practice of backing up and archiving your data.

The Backup functionality allows you to schedule automatic backups of the ***Instance***, that is to say, the configuration information held on the SMP server (Log Collector configuration, correlation rules, report configuration, etc.).

Importance of the Backup Export Command

The backup files are generated on the SMP server. This is why you should use the **Backup export command** option, as it allows the automatic transfer of backup files to another machine once the backup has been completed. (See "Export a Daily Backup").

Export a Daily Backup

You can export the daily backup zip file to a remote machine, by using the **Backup export command** to specify a script to run upon successful completion of the backup.

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

The folder location of the script is:

```
/home/exaprotect/scripts/export
```

Below is an example script:

Table 52 Script scp.sh

```
#!/bin/sh

if [ $# -ne 5 ]; then
   echo "Usage : $0 host user dest
   instance file"
   echo ""
   exit
fi


host=$1
user=$2
destfile=$3
instance=$4
sourcefile=$5


if [! -f /var/lib/exaprotect/archives/$instance/
backups/$sourcefile]
; then
   echo "File : $sourcefile does not
   exist!"
   exit 1
fi


echo "/var/lib/exaprotect/archives/
$instance/backups/$sourcefile
   --> ${host}:${destfile}"
scp $sourcefile
${user}@${host}:${destfile}
```

Caution: host=$1 corresponds to the host target hostname.
user=$2 corresponds to the username for ssh connection.
destfile=$3 corresponds to the destination directory on remote host.
instance=$4 corresponds to the SEM instance name.
sourcefile=$5 corresponds to the source file to send.

Configuring the Backup Export Script

1. In the **Backup Export Command** text box, enter the full file name of the script. For example, you could enter the following command:

```
scp.sh 10.0.0.1 root /root/backup/ INSTANCE
```

Table 53 Description of the Example

Script Elements	Description
`scp.sh`	Script name
`10.0.0.1`	Host
root	User
`/root/backup/`	Destination folder
`INSTANCE`	Instance name

Within the script you can name utilities such as TFTP, SFTP, SCP, etc. The backup file is generated in `/home/exaprotect/scripts/.`

Caution: a generated backup name will be automatically added at the end of the arguments of the script, so there is no need to enter it.

2. In the **Add a new File to the Backup** field, enter the path of any additional file located on the appliance that you need, e.g. /etc/passwd.

Restore a Backup

The backup operation consists in reinstalling an instance in the event of a server failure. This file allows the reintegration on a server of the instance's total configuration.

The restoration overwrites all data that is in the database.

A backup can only be restored:

- If the server has the same version as the original server where the backup was generated
- If the instance has the same name as the instance where the backup was first generated

For more information, please refer to the A**dministration Guide -** SMP **advanced configuration** section.

Follow the same procedure as described in section "4th Step: Update the Server via the SMPConfig Tool".

Raw Logs Archiving

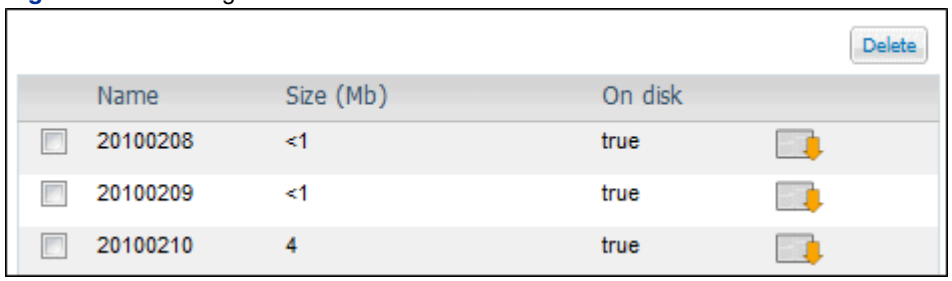
This functionality allows the creation of archiving files for **elementary events** and **raw logs.**

Archive Raw Logs and Elementary Events

The main reason for the importance of the raw log is in view of required legal proof about an event generated by a supported product. A raw log entry is the most faithful format derived from the data produced by a log source. This is why the SEM can be configured to keep a record of the event generated by a supported product in the raw log format.

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.

Figure 96 Raw Log Archive Files List Screen



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

Downloading Archives

To download the archive of raw log events:

1. Click on . A dialog box is displayed allowing you to indicate how to open the file.
2. Select the appropriate option and click **OK**.

If the archive file is encrypted, you will need the GPG private key to decrypt the archives (see section "Configure Archive Settings" for further information).

Deleting Archives

To delete archives:

1. Select the files by ticking the checkboxes.
2. Click **Delete**.

Configure Archive Settings

When the confset is configured to collect raw logs (i.e. full copies of the original events), use the **Raw Log Archiving** page to manage the "raw log" entries in the database. See Advanced Log Collection: Confset for more information.

The raw logs and the elementary events will be copied from the database to an archive file once a day. They are then deleted from the database to release space for new events. The archives will be in tgz format.

A raw log archive is signed and sometimes encrypted. During raw log archiving process, an alert maybe generated due to an encryption or signing error. If you encounter this kind of problem, please contact your TIBCO LogLogic® integration partner.

Note: The SMP cannot retrieve raw logs from RDEP and SCANNER converters.

To configure raw log archive option:

1. Make sure that the **export** folder (in **/home/exaprotect/scripts/**) contains the export scripts for raw log and elementary event archives and backup (user scripts).

2. Go to **Log Management > Archiving > Settings.** The **Archiving Settings** screen is displayed.

3. In the **Elementary Event Archive Settings** screen, select the script.

4. In the **args** field, enter the arguments connected with the selected script. In our example, the cp.sh arguments are **Destination**, **Instance** and **File.** You could obtain something like the following example.

If you want to enter several arguments in the same field, you must leave a space between each argument.

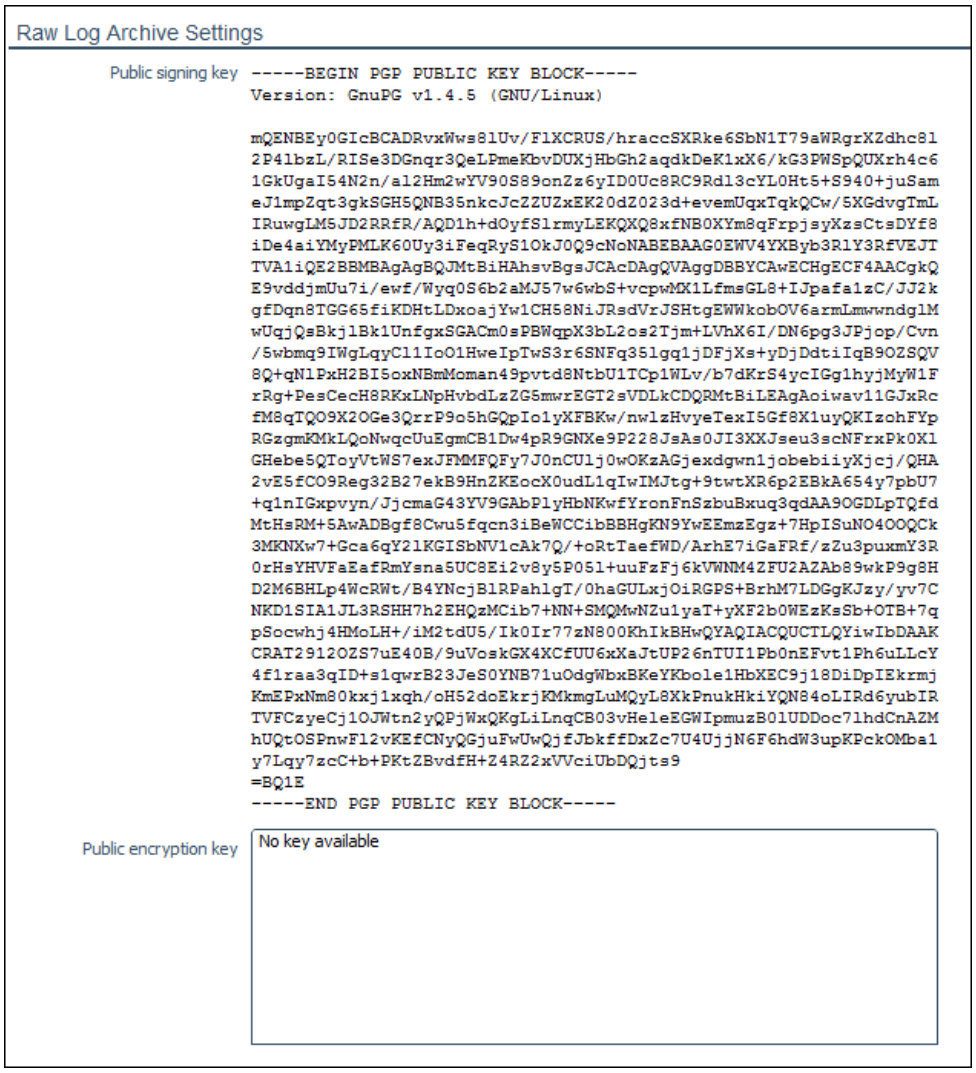
You can check if the export has correctly been completed by looking in `/var/lib/exaprotect/logs/smp_executor.log`.

5. Enter the number of days during which the data will be archived.

6. Click **Apply**.

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

Figure 97 Raw Log Archive Settings



7. In the Raw Log Archive Settings pane, enter the public and/or private key in the corresponding blank space. For more information about the procedure to generate the keys, refer to Generating a Public and Private GPG Keys on Windows and Linux.

8. Enter a script that must be executed after the archive task completes successfully in the **arg** field. Typically this is used to copy or move the archive file to an external storage location, e.g., tape or remote FTP server.

9. Enter 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. In this case, 30 means a total of 30 consecutive days during which raw logs are kept in the database.

Generating a Public and Private GPG Keys on Windows and Linux

You can generate either a gpg key for **Windows** or for **Linux**.

1. Download the GnuPG at the following address:
http://www.gnupg.org/download/index.en.html

2. Open a MSDOS prompt (**Windows**) or a shell (**Linux**).

3. Enter the following command line:

- C:\Program Files\GNU\GnuPG>gpg.exe --gen-key. (**Windows**)

Or

- `gpg --gen-key` (**Linux**)

You are asked several questions.

1. Select the kind of key you need: DSA and ElGamal (default) or DSA (sign only) or RSA (sign only) and validate by **Return.**

2. Enter the key size and validate by **Return**. The key size must be from 768 to 2048 bit inclusive. However, it is recommended to use a 2048 bit key. Also note that the key must NOT be protected by a password as it will not be taken into account.

3. Indicate the key validity (e.g. **2y** which means two years; **0y** which means **unlimited**). The key validity must be defined according to your security policy of raw log archiving.

4. Validate by **Return**.

5. Confirm it by entering **y** or **n** and validate by **Return**.

6. Indicate the user's identity according to the advice given in the prompt or shell, enter the e-mail and validate by **Return**.

7. Confirm your choice again and validate by **Return**.

8. Optionally, enter a passphrase.

9. Validate by **Return**.

Exporting a Public and Private GPG Keys on Windows and Linux

To export a public key:

1. In GnuPG, enter:

- `C:\Program Files\GNU\GnuPG>gpg.exe --export -a ExaProtect` (**Windows**)

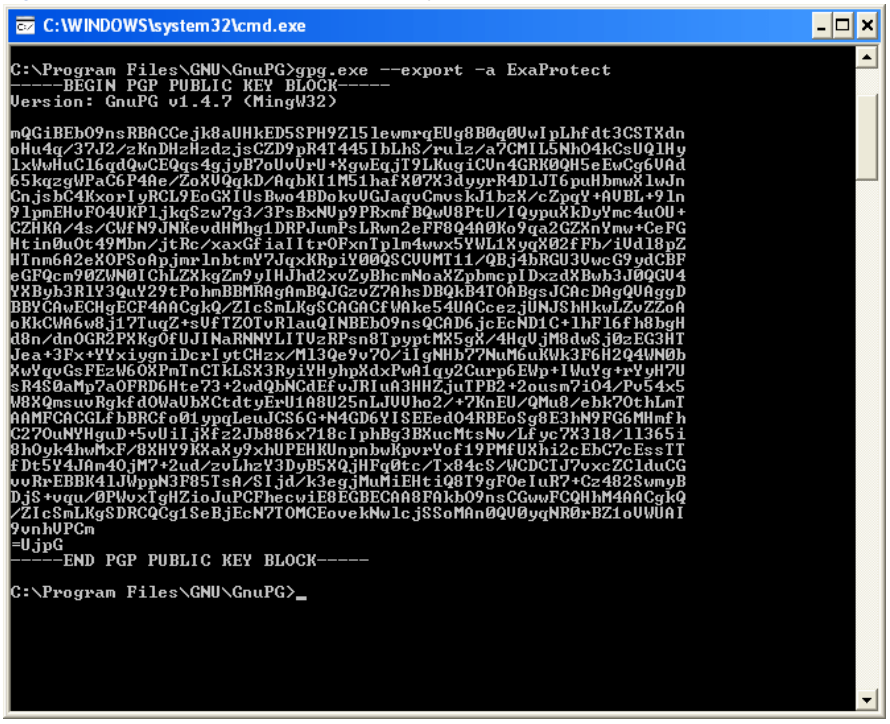
Or

- `gpg --export -a ExaProtect` (**Linux**)

Note that entering TIBCO LogLogic® allows you to differentiate between this key and the other keys available on this machine.

You obtain the following key in Windows:

Figure 98 Example of a Generated Key



1. Copy the key by selecting the whole text in the prompt from the sentence `----- BEGIN PGP PUBLIC KEY BLOCK-----` to the sentence `----- END PGP PUBLIC KEY BLOCK-----`.

2. Paste it in the **Public Encryption Key** part of the **Raw Log Archive Configuration** screen.

To export a private key:

1. If the private key is protected by a passphrase, remove the passphrase before exporting the key. To do so:

- Add the private key in the keyring if necessary.

```
gpg --allow-secret-key-import --import private.key
```

- Edit the key:

```
gpg --edit-key "UserName" passwd
```

- Then you will be asked to enter the former passphrase and the new one
- Enter **quit** and **y** to save.

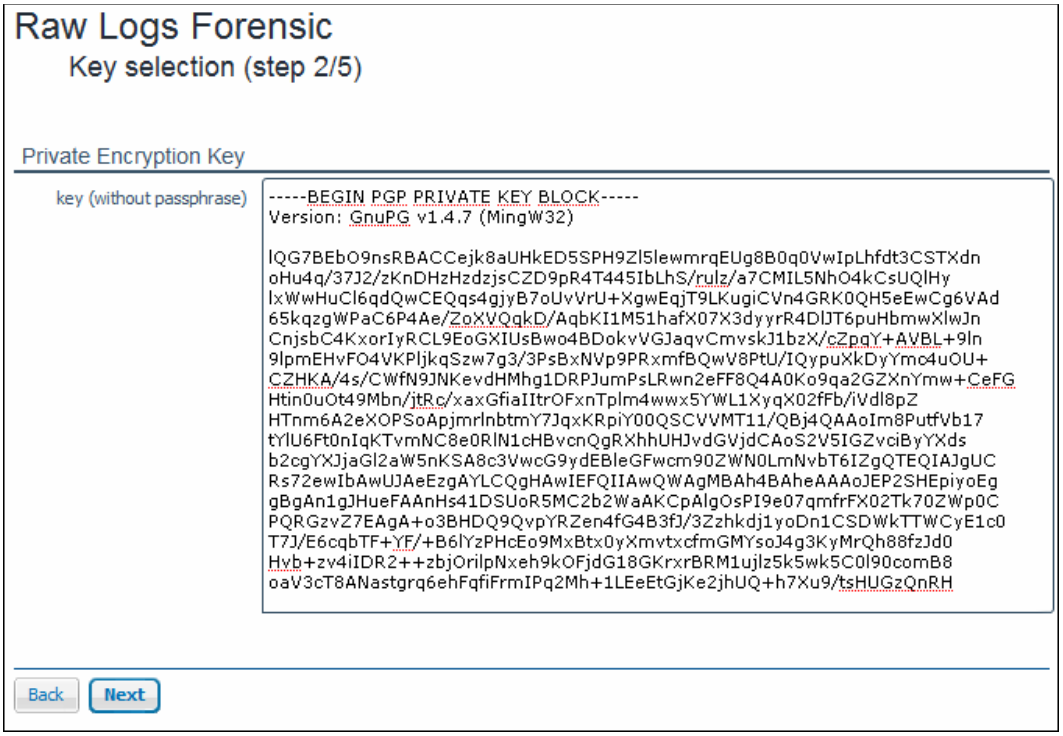
2. In GnuPG, enter:

- `C:\Program Files\GNU\GnuPG>gpg.exe --export-secret-key -a ExaProtect`

3. Copy the key by selecting the whole text in the prompt from the sentence `----- BEGIN PGP PRIVATE KEY BLOCK-----` to the sentence `----- END PGP PRIVATE KEY BLOCK-----`.

4. Paste it in the **Private Encryption Key** screen (**Log Management > Logs Forensic > step 2/5**) as in the example below:

Figure 99 Example of an exported private key



Raw Log Export script

Here is an example of an export script creation:

Table 54 Raw Log Export Script

```
[root@exabench1 rawlog]# pwd
/home/exaprotect/scripts/rawlog
[root@exabench1 rawlog]# vi ./cp.sh
[root@exabench1 rawlog]# chown exaprotect:exaprotect
./cp.sh
[root@exabench1 rawlog]# chmod +x ./cp.sh
```

The line starting with:

- `[# pwd]` indicates the folder location where you must store the scripts. This will allow you to select the export script from the drop-down list in the **Raw Log Archive Configuration** screen.
- `[# vi]` edits and creates the export script.
- `[# chown]` allows you to change group and owner parameters into `exaprotect:exaprotect`.
- `[# chmod +x]` changes file access permissions by giving access rights to execute the script.

Configuration Profiles and Security Levels

How Do Configuration Profiles Work?

A configuration profile is a group of rules and scenarios along with a Service Level Agreement set. A Security level specifies the time ranges during which one (and only one) configuration profile will be active.

We can make an analogy from public terror alert levels to the SMP's framework for security levels. Government officials may code each terror alert level with a color ranging from the slightest to the most critical level of alert (usually green to red).

For example:

- a green level of alert can mean that there is a low risk of terrorist attacks.
- Yellow would mean an elevated condition with significant risk of terrorist attacks.
- Red signifies severe risk of terrorist attacks.

For each of these levels, authorities will take different actions to address specific terrorist threats. For example, in a green low-risk scenario, authorities may assess public facilities for vulnerabilities and take measures to reduce them, whereas if the level jumps to red, the action taken will be to close public facilities.

In an analogous manner, the SMP allows you to create and configure multiple security levels according to your needs. By default, there is one **basic** security level which applies the **default configuration** profile for all hours, every day.

Within one security level there can be multiple profiles in use, e.g., a normal security level can be created which switches between several configuration profiles as shown in the following table.

Table 55 Various Configuration Profiles

Day	Times	Profile
Monday - Friday	09:00 - 17:30	Office Hours
Monday - Friday	18:00 - 23:30	Weekday non-office
Monday - Friday	00:00 - 08:30	Weekday non-office
Saturday - Sunday	00:00 - 23:30	Weekend

Note: The granularity is 30 minutes, so for example 23:30 means from 23:30 up to and including 23:59:59.

View and Edit Security Levels

Viewing Security Levels

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

Figure 100 Profile Configuration for Security Level

In the **Security Levels** screen you can:

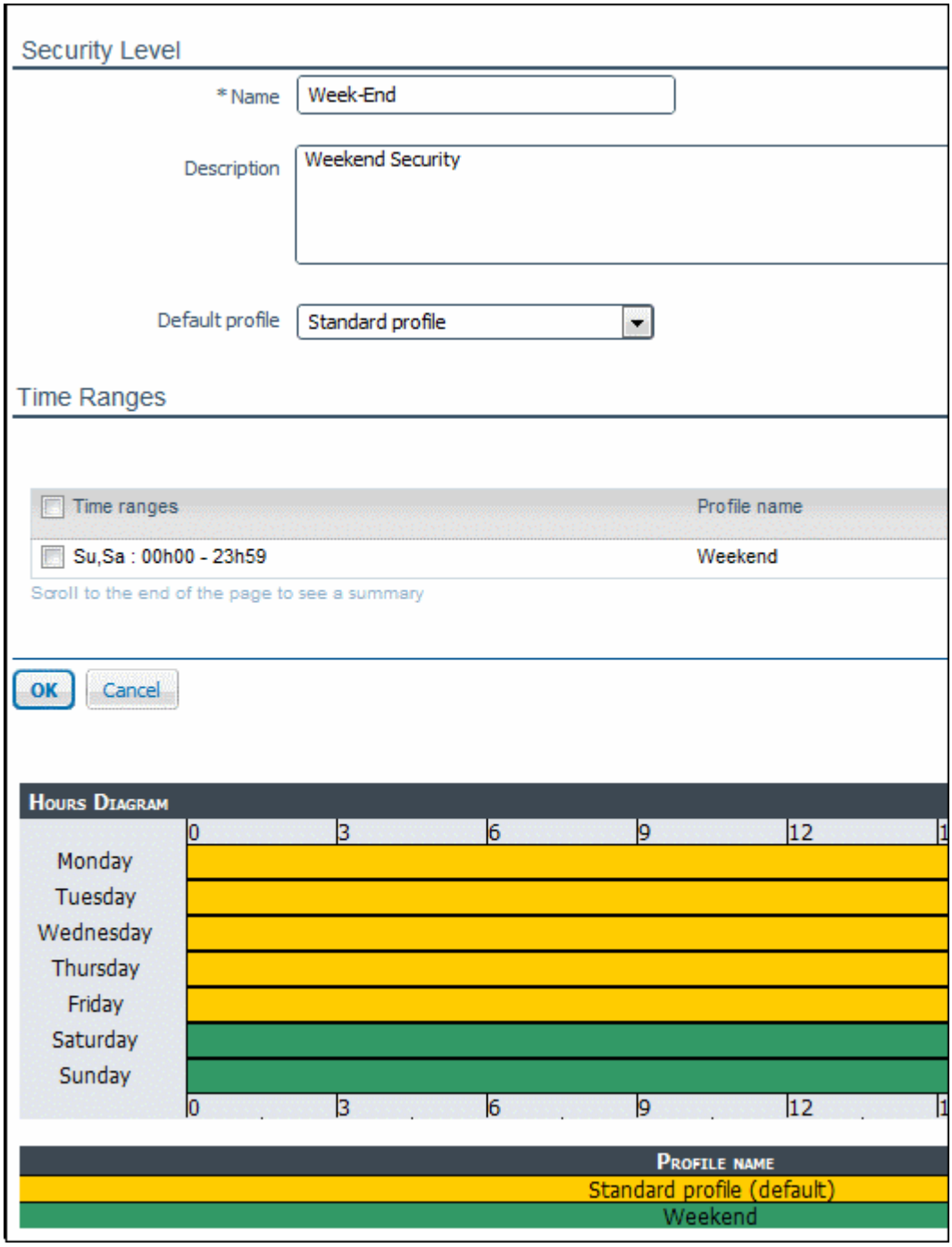
- Activate a security level
- Delete security level(s)
- Copy a security level - when you need to create a security level similar to a pre-existing one, you will create a copy to have a new security level with the same previous attributes, which can then be edited
- Move security levels to order them according to your preference
- Add a new security level

Editing Security Levels

To edit a security level:

1. Click the name of the security level in the list and perform the following procedures to edit the various sections.

Figure 101 Edit Security Level



2. Type in a unique name for the security level in the **Name** field.

3. Add a brief description giving the purpose of the security level in the **Description** field.

4. Create a time range for each block of hours specifically related to the configuration profiles, e.g., create a different time range for **office hours**, **night time,** and **weekend**.

5. Click **Add** to add a new time range.

6. Specify the following attributes:

- **Days**: Use CTRL-click to select multiple days (e.g., Saturday and Sunday for the weekend)
- **From**: Choose the initial hour and minute (00 or 30) of the time range (e.g., 00 to start at midnight 00:00)
- **To:** Choose the end hour and minute (00 or 30) of the time range (e.g., 10 to end at 09:59:59)
- **Profile:** Choose the configuration profile to be applied automatically during these hours and specify which profile is to be active outside the specified time ranges. See View and Edit Configuration Profiles for more details.

7. Click **OK** to save changes and return to the previous screen. Click **Cancel** to return to the previous screen without saving changes.

8. Check the **Hours Diagram** to see when each profile is active. The key at the bottom of the table lists the profiles with their corresponding colors.

View and Edit Configuration Profiles

Viewing Configuration Profiles

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

Figure 102 Configuration Profiles

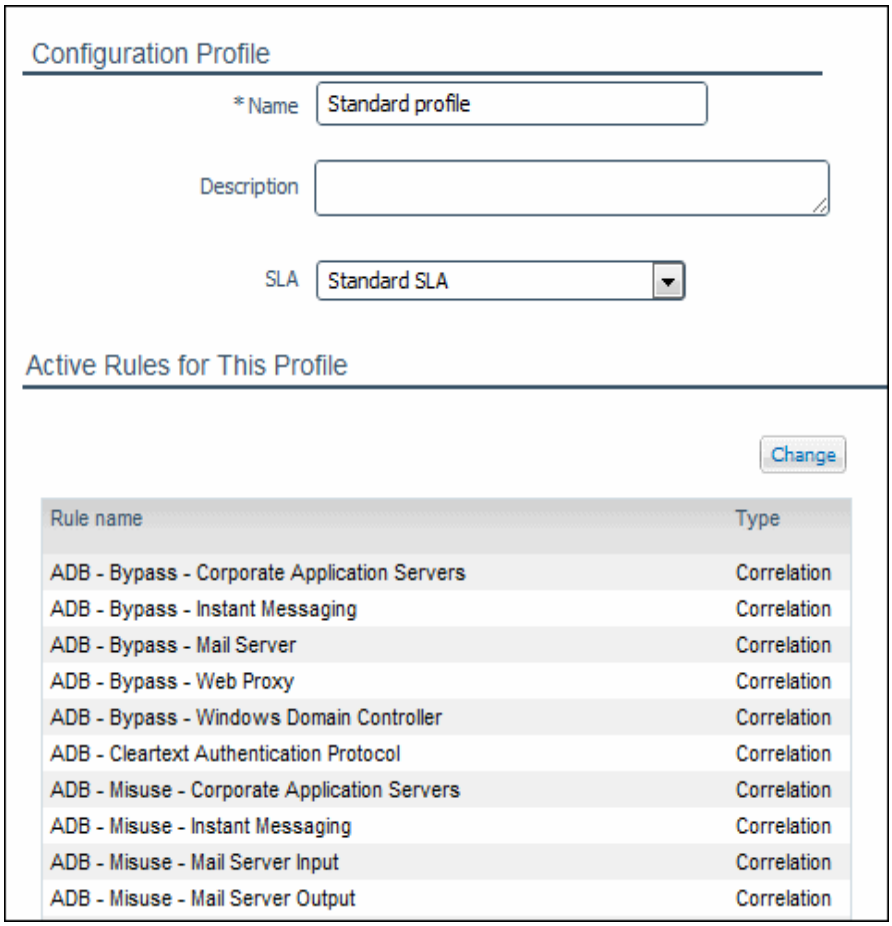
In the above figure, the **Standard Profile** is the active one.

Editing Profiles

1. Click the **Profile** that you want to edit in the **Name** column of the **Configuration Profile** screen.

A **Configuration Profile** screen opens to let you edit the selected profile.

Figure 103 Configuration Profile Edition



2. Enter a **name** and **description** in the corresponding fields.

3. Select the **SLA** that must be applied to the profile.

4. 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.

5. Click **OK** to save changes and return to the list of profiles, or click **Cancel** to ignore changes and return to the list of profiles.

Chapter 9 - Updating the SMP Server

For an optimal use of TIBCO LogLogic® Security Event Manager, it is recommended to update your SEM server, i.e. the appliance as well as the standard content, which is regularly enhanced to best meet your requirements. The updated standard content is detailed in the SEM Release Notes, section “Standard Content”.

The objective of this chapter is to learn how to apply a patch on a standard server.

In order to migrate from a version to another one, you must apply all the intermediary versions or patches of Security Event Manager.

Examples:

To go from v3.3.1 to v3.5.2, you must apply v3.3.2, v3.4, v3.5, v3.5.1 and v3.5.2.

List of all SEM versions:

- SEM v3.0
- SEM v3.1
- SEM v3.2
- SEM v3.3
- SEM v3.3.1
- SEM v3.3.2
- SEM v3.4
- SEM v3.5
- SEM v3.5.1
- SEM v3.5.2

For more information, please contact our technical support at ll-support@tibco.com.

Caution: As an administrator, you should be aware that your current TIBCO LogLogic® version is fully functional, but it may be altered as fixes are implemented following bug discoveries. Therefore, it is highly important that you carefully read the email notifications concerning SMP updates and download the available patches on the TIBCO LogLogic® website.

Updating the SMP Server

1st step: Downloading the *.rpm Files for Update

To connect to the update site:

1. Go to https://download.tibco.com/tibco/
2. Enter your credentials to access the website.
3. Click on the files you want to download and save the files on your disk.

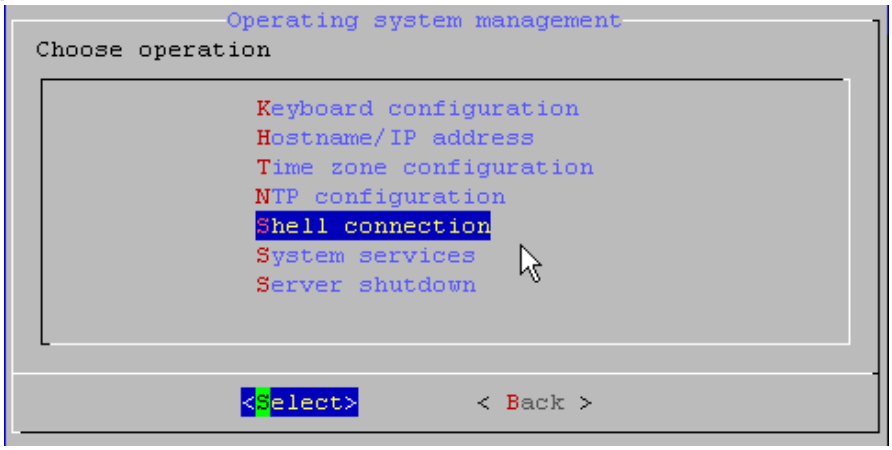
4. Check the downloaded TIBCO LogLogic® packages integrity with the provided digest.

2nd step: Activating the “Root” Connection on SMP Server

Now that the *.rpm files have been downloaded, you must prepare their installation on the server. To do so, you must first activate the “root” connection on the SMP server.

1. Open an SSH console.
2. With either a remote or local connection, identify yourself as `admin`.
3. In the **Operating System Management** submenu, use the **Up** and **Down** arrows to highlight **Shell Connection** and then click **Return**.

Figure 104 Shell connection



For more information about the admin connection, please refer to the ***Administration Guide*** (see SMP Advanced Configuration section). Please note:

- This option enables or disables the local “root” system account connections on the SMP server.
- This operation authorizes only a local access to the server (through the console); it does not permit a remote access.
- Once you have enabled the “root” account, you will need to create a related password.

4. Exit the SSH console.

Caution: To correctly follow the procedure, make sure the “root” and “root ssh” connections are enabled.

3rd step: Copying the *.rpm Files to the Server

There are two ways to copy the files you have just saved on your disk to the server:

- Copying and pasting the files with WinSCP, for example.
- Transferring files using a USB key.

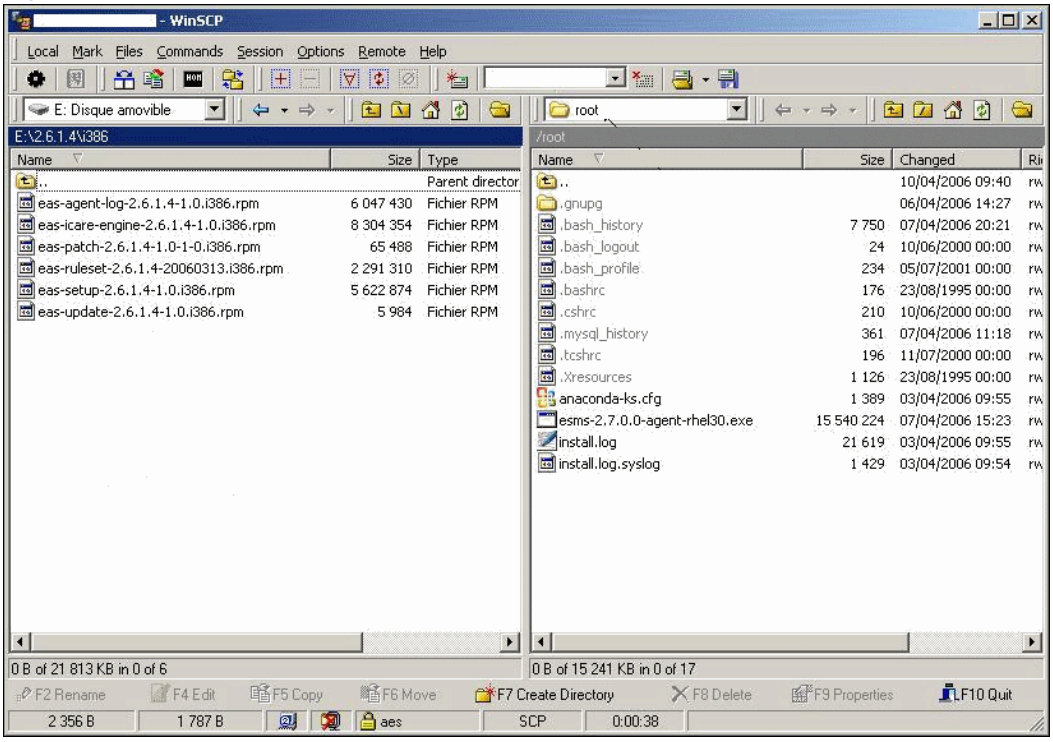
Copying the *.rpm Files via the Network Using the SCP Function

We will describe the way to copy the *.rpm files using the WinSCP software (downloadable at http://winscp.net) as a reference. Please note you must work on a Windows machine to use it.

Make sure you have enough free space on your file system before copying the *.rpm files. Otherwise, you will get an error message.

1. Activate the “root” and “root ssh” connections on the server.
2. Open WinSCP on the machine where the *.rpm files have been downloaded.
3. Connect as “root” user to access the SMP server in WinSCP.
4. Copy the files. Make sure the /tmp folder is displayed in the corresponding field.

Figure 105 WinSCP Interface



5. Open a shell as “root” user.
6. Enter the following command to apply the update:
`yum --nogpgcheck --disablerepo=* localinstall *.rpm`
7. Enter the following command to delete the *.rpm files:
`rm -f /tmp/*.rpm`
8. Restart the machine to take the modification into account.

Caution: Do not forget to deactivate the “root” connection at the end of the procedure.

Transferring the *.rpm Files from a USB Key to the Server

Caution: Make sure your USB key is compatible with the operating system.

1. Plug the USB key on the SMP server.
2. Open a shell as “root” user.
3. Enter the following command to mount the USB key:
`mount /mnt/flash.`
This command can vary according to the RedHat version you use.

4. Enter the following command to copy the files from the USB key to the tmp folder:
`yum --nogpgcheck --disablerepo=* localinstall /mnt/flash/*.rpm`

5. Unmount the USB key.

6. Unplug the USB key.

> **Caution:** Do not forget to deactivate the “root” connection at the end of the procedure.

4th Step: Update the Server via the SMPConfig Tool

Once the pre-installation of the update in the Web Console has been done, the process must be completed in the **SMPConfig**:

1. If you are using a remote connection to the server, open an SSH console on the SMP. You should use port TCP/22.

2. Log in as admin or login as root and type the “su - admin” command with either a remote or local connection.

   The **Welcome to SMPConfig** screen is displayed.

3. Select **Continue Update** and press **Enter**. The update is launched.

If no error occurred, a message saying the installation is successful is displayed.

Otherwise, a message is displayed advising you to see the log file located in:
`/usr/local/exaprotect-setup/logs/install.log`

5th Step: Update the Log Collectors

1. Log into the GUI.

2. Go to **Log Management > Log Collectors.**

3. Select all the Log Collectors and click **Apply**.

Appendix A - Appendix

- Java Regular Expressions
- MySQL Regular Expressions
- Date Time Format Specification

Java Regular Expressions

Construct	Matches
Characters	
x	The character x
\\	The backslash character
\0n	The character with octal value 0n (0 <= n <= 7)
\0nn	The character with octal value 0nn (0 <= n <= 7)
\0mnn	The character with octal value 0mnn (0 <= m <= 3, 0 <= n <= 7)
\xhh	The character with hexadecimal value 0xhh
\uhhhh	The character with hexadecimal value 0xhhhh
\t	The tab character ('\u0009')
\n	The newline (line feed) character ('\u000A')
\r	The carriage-return character ('\u000D')
\f	The form-feed character ('\u000C')
\a	The alert (bell) character ('\u0007')
\e	The escape character ('\u001B')
\cx	The control character corresponding to x
Character classes	
[abc]	a, b, or c (simple class)
[^abc]	Any character except a, b, or c (negation)
[a-zA-Z]	a through z or A through Z, inclusive (range)
[a-d[m-p]]	a through d, or m through p: [a-dm-p] (union)
[a-z&&[def]]	d, e, or f (intersection)
[a-z&&[^bc]]	a through z, except for b and c: [ad-z] (subtraction)
[a-z&&[^m-p]]	a through z, and not m through p: [a-lq-z] (subtraction)
Predefined character classes	
.	Any character (may or may not match line terminators)
\d	A digit: [0-9]
\D	A non-digit: [^0-9]
\s	A whitespace character: [\t\n\x0B\f\r]
\S	A non-whitespace character: [^\s]

Construct	Matches
\w	A word character: [a-zA-Z_0-9]
\W	A non-word character: [^\w]
POSIX character classes (US-ASCII only)	
\p{Lower}	A lower-case alphabetic character: [a-z]
\p{Upper}	An upper-case alphabetic character:[A-Z]
\p{ASCII}	All ASCII:[\x00-\x7F]
\p{Alpha}	An alphabetic character: [\p{Lower}\p{Upper}]
\p{Digit}	A decimal digit: [0-9]
\p{Alnum}	An alphanumeric character: [\p{Alpha}\p{Digit}]
\p{Punct}	Punctuation: One of !"#$%&'()*+,-./:;<=>?@[\]^_`{|}~
\p{Graph}	A visible character: [\p{Alnum}\p{Punct}]
\p{Print}	A printable character: [\p{Graph}]
\p{Blank}	A space or a tab: [\t]
\p{Cntrl}	A control character: [\x00-\x1F\x7F]
\p{XDigit}	A hexadecimal digit: [0-9a-fA-F]
\p{Space}	A whitespace character: [\t\n\x0B\f\r]
Classes for Unicode blocks and categories	
\p{InGreek}	A character in the Greek block (simple block)
\p{Lu}	An uppercase letter (simple category)
\p{Sc}	A currency symbol
\P{InGreek}	Any character except one in the Greek block (negation)
[\p{L}&&[^\p{Lu}]]	Any letter except an uppercase letter (subtraction)
Boundary matchers	
^	The beginning of a line
$	The end of a line
\b	A word boundary
\B	A non-word boundary
\A	The beginning of the input
\G	The end of the previous match
\Z	The end of the input except for the final terminator, if any
\z	The end of the input
Greedy quantifiers	
X?	X, once or not at all
X*	X, zero or more times
X+	X, one or more times
X{n}	X, exactly n times
X{n,}	X, at least n times
X{n,m}	X, at least n but not more than m times
Reluctant quantifiers	
X??	X, once or not at all
X*?	X, zero or more times
X+?	X, one or more times

Construct	Matches
X{n}?	X, exactly n times
X{n,}?	X, at least n times
X{n,m}?	X, at least n but not more than m times
Possessive quantifiers	
X?+	X, once or not at all
X*+	X, zero or more times
X++	X, one or more times
X{n}+	X, exactly n times
X{n,}+	X, at least n times
X{n,m}+	X, at least n but not more than m times
Logical operators	
XY	X followed by Y
X|Y	Either X or Y
(X)	X, as a capturing group
Back references	
\n	Whatever the nth capturing group matched
Quotation	
\	Nothing, but quotes the subsequent character
\Q	Nothing, but quotes all characters until \E
\E	Nothing, but ends a quote started by \Q
Special constructs (non-capturing)	
(?:X)	X, as a non-capturing group
(?idmsux-idmsux)	Nothing, but turns match flags on - off
(?idmsux-idmsux:X)	X, as a non-capturing group with the given flags on - off
(?=X)	X, via zero-width positive look ahead
(?!X)	X, via zero-width negative look ahead
(?<=X)	X, via zero-width positive look behind
(?<!X)	X, via zero-width negative look behind
(?>X)	X, as an independent, non-capturing group

MySQL Regular Expressions

Construct	Matches
Characters	
x	The character x
[:characters:]	Within a bracket expression (written using [and]), matches the sequence of characters of that collating element. Characters is either a single character or a character name like newline.
Character classes	
[abc]	a, b, or c (simple class)

Construct	Matches
[^abc]	Any character except a, b, or c (negation)
[a-zA-Z]	a through z or A through Z, inclusive (range)
Predefined character classes	
.	Any character (may or may not match line terminators)
[:character_class:]	Within a bracket expression (written using [and]), [:character_class:] represents a character class that matches all characters belonging to that class. ▪ alnum: Alphanumeric characters ▪ alpha:Alphabetic characters ▪ blank: Whitespace characters ▪ cntrl: Control characters ▪ digit: Digit characters ▪ graph: Graphic characters ▪ lower: Lowercase alphabetic characters ▪ print: Graphic or space characters ▪ punct: Punctuation characters ▪ space: Space, tab, newline, and carriage return ▪ upper: Uppercase alphabetic characters ▪ xdigit: Hexadecimal digit characters Example: [:alnum:]
Boundary matchers	
^	The beginning of a line
$	The end of a line
[[:<:]], [[:>:]]	These markers stand for word boundaries. They match the beginning and end of words, respectively. A word is a sequence of word characters that is not preceded by or followed by word characters. A word character is an alphanumeric character in the alnum class or an underscore (_).
Greedy quantifiers	
X?	Match either zero or one X character
X*	X, zero or more times
X+	X, one or more times
X{n}	X, exactly n times
X{n,}	X, at least n times
X{n,m}	X, at least n but not more than m times
Logical operators	
X | Y	Either X or Y

To use a literal instance of a special character in a regular expression, precede it by two backslash (\) characters. The MySQL parser interprets one of the backslashes, and the regular expression library interprets the other. For example, to match the string 1+2 that contains the special + character, only the last of the following regular expressions is the correct one:

```
mysql> SELECT '1+2' REGEXP '1+2'; -> 0

mysql> SELECT '1+2' REGEXP '1\+2'; -> 0
```

```
mysql> SELECT '1+2' REGEXP '1\\+2'; -> 1
```

Date Time Format Specification

Table 56 Date Converter

Letter	Date or Time Component	Example
y	Year	2008; 08
M	Month in year	July; Jul: 08
w	Week in year	27
W	Week in month	2
D	Day in year	189
d	Day in month	10
F	Day of week in month	2
E	Day in week	Tuesday, Tue
a	Am/pm marker	PM
H	Hour in day (0-23)	0
k	Hour in day (1-24)	24
K	Hour in am/pm (0-11)	0
h	Hour in am/pm (1-12)	12
m	Minute in hour	30
s	Second in minute	55
S	Millisecond	978
z	Time Zone (General)	Pacific Standard Time; PST; GMT-08:00
Z	Time Zone (RFC 822 time zone)	-0800

The default date format is: **`MMM dd HH:mm:ss`**

For formatting, the number of pattern letters is the minimum number of digits, and shorter numbers are zero-padded to this amount. For parsing, the number of pattern letters is ignored unless it is needed to separate two adjacent fields.

The following examples show how date and time patterns are interpreted in the U.S. locale. The given date and time are 2001-07-04 12:08:56 local time in the U.S. Pacific Time time zone.

Table 57 Date and Time Pattern

Date and Time Pattern	Result
"yyyy.MM.dd G 'at' HH:mm:ss z"	2001.07.04 AD at 12:08:56 PDT
"EEE, MMM d, ''yy"	Wed, Jul 4, '01
"h:mm a"	12:08 PM
"hh 'o''clock' a, zzzz"	12 o'clock PM, Pacific Daylight Time
"K:mm a, z"	0:08 PM, PDT
"yyyyy.MMMMM.dd GGG hh:mm aaa"	02001.July.04 AD 12:08 PM
"EEE, d MMM yyyy HH:mm:ss Z"	Wed, 4 Jul 2001 12:08:56 -0700
"yyMMddHHmmssZ"	010704120856-0700

SEM Glossary

Table 58 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 TIBCO LogLogic® 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 58 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.
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)
IODEF	Incident Object Description and Exchange Format.
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 58 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

E

F

G

H

I

L

M

O

P

Q

R

S

T

U

V

W