TIBCO LogLogic®

Security Event Manager (SEM)

Log Collector Installation Guide

Software Release: 3.6.0

March 2013

Two-Second Advantage®

TIBCO®

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

List of Figures

Preface

About This Guide

This guide is intended as a step by step guide to the initial configuration of the TIBCO LogLogic® Security Event Manager Log Collector and its connection to the Security Management Platform (SMP) - the appliance delivered with the Security Event Manager.

There are four phases to the installation of the Log Collector:

- Phase 1 - Configuring a Log Collector.
- Phase 2 - Generating the Log Collector Installation and Installer Files.
- Phase 3 - Installing a Log Collector.
- Phase 4 - Checking the Log Collector Connection on the Web Console.

This guide will take you through these phases step by step.

At the end of the document, you will also find the procedure to uninstall the Log Collector.

Audience

This guide is intended for 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 SEM.
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®.
Reference Guide	This guide gives a description of the Web Console modules.
SMP Installation Guide	This guide explains how to install and configure the SMP.
User Guide	This guide explains how to use and configure the various functions and modules provided in the Web Console application.

Technical Support Information

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

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

To reach TIBCO LogLogic® Customer Support:

Telephone: Toll Free—1-800-957-LOGS

Local—1-408-834-7480

EMEA— +44 1480 479391

Email: ll-support@tibco.com

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

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

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

Documentation Support Information

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

Contact Information

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

Conventions

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

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

IMPORTANT! Highlights key considerations to keep in mind.

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

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

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

```
username: system
```

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

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

```
LogLogic_home_directory\upgrade\
```

- Straight brackets signal options in command line syntax.

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

Chapter 1 - Important Recommendation

The following section provides security recommendations that need to be followed to install the Log Collector in a secure manner that is consistent with Common Criteria Evaluation Assurance Level 2+ (EAL2+):

General Security Considerations

The administrator must ensure that:

- The machines on which TIBCO LogLogic® Security Event Manager Log Collectors are installed are fully secured. These machines should be located in a physically secure environment in which only a trusted personnel has access.
- Ensure that the default admin password to connect to the machine is changed. A good password has a combination of alphabetic and numeric characters and comprises at least eight characters in length. It should be known by a very restricted number of people.
- All operating systems and software installed on the machine must be correctly updated to avoid any security breach which could expose admin rights.
- A VPN between the two machines is installed if the machine with a TIBCO LogLogic® Security Event Manager Log Collector installed communicates with the Security Management Platform server via a public network.

Chapter 2 - Requirements

Supported Platforms

The machine where the TIBCO LogLogic® Security Event Manager Log Collector is installed and then runs must be safe and secured by a reliable administrator.

It must also be synchronized according to a NTP server (for a reliable time management).

The supported platforms on which you install the TIBCO LogLogic® Security Event Manager Log Collector are:

- AIX 7
- RedHat 5
- 64-bit RedHat 5
- Solaris 10
- Windows 2003/2003R2/Seven/2008
- 64-bit Windows 2003/2003R2/Seven/2008/2008R2

> **Caution:** At least 100 MB of disk space must be available on your machine to install the Log Collector.

Software

Prerequisites

Please ensure that:

- A web browser is installed on your computer. It must be either **Microsoft Internet Explorer v.7** or higher or **Mozilla Firefox 13**.
- A Security Management Platform (SMP) appliance is running before installing the Log Collector.
- You have administrator rights on the Web Console.

Contact your TIBCO LogLogic® representative for more details.

Chapter 3 - Installation Phases

There are two ways to pre-configure the TIBCO LogLogic® Security Event Manager Log Collector from the Web Console. You can either pre-configure it using an installation **wizard** or in an advanced manner using the **Log Collection Creation** screen.

Phase 1 - Configuring a Log Collector

Configuring a TIBCO LogLogic® Security Event Manager Log Collector via the Wizard

The wizard is a tool intended at adding and configuring a log source and a TIBCO LogLogic® Security Event Manager Log Collector in an easy and friendly way.

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

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

- configure the log source,
- configure the TIBCO LogLogic® Security Event Manager 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.

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

Step 1 - Configuring the Log Source

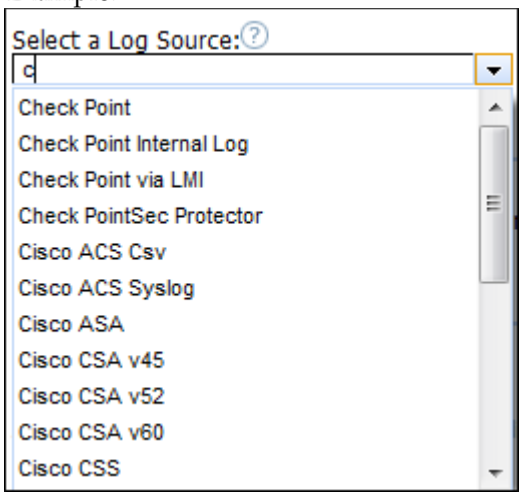
Selecting a Log Source

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:



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. The list of existing hosts is displayed. Once the host selected, a new field is displayed.

2. Enter the necessary addresses so that the TIBCO LogLogic® Security Event Manager Log Collector can communicate with the log source and click on the + button to add them.

> **Caution:** 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 TIBCO LogLogic® Security Event Manager 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. By default, the wizard uses the **Standard Policy**.

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

Step 2 - Configuring the Log Collector

The aim of the TIBCO LogLogic® Security Event Manager Log Collector is to collect logs from any devices and is able to forward them to both a SEM appliance using the existing mechanism and an LMI appliance using a TCP Syslog connection (no parsing in this case). The forwarding to LMI mechanism is available for some supported collection methods: Syslog, Windows WMI, File, SDEE.

Configuring the Log Collector

If you want the events to be collected by the TIBCO LogLogic® Security Event Manager 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 the 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 TIBCO LogLogic® Security Event Manager Log Collector 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 TIBCO LogLogic® Security Event Manager 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 TIBCO LogLogic® Security Event Manager Log Collector Communication Type

When you create a new TIBCO LogLogic® Security Event Manager 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 TIBCO LogLogic® Security Event Manager 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 TIBCO LogLogic® Security Event Manager 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 TIBCO LogLogic® Security Event Manager Log Collector to connect to the log source and retrieve the logs.

Eight cases are possible.

First case: you have selected a FILE log source in Step 1

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 TIBCO LogLogic® Security Event Manager 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 TIBCO LogLogic® Security Event Manager 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.

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

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

Second case: you have selected a DATABASE log source in Step 1

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 TIBCO LogLogic® Security Event Manager Log Collector to connect to the database.
3. Indicate the port to which the TIBCO LogLogic® Security Event Manager Log Collector can connect and click **Next**

Third case: you have selected an OPSEC log source in Step 1

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.**

Fourth case: you have selected a WMI log source in Step 1

The events will be collected via WMI.

- If the host where the TIBCO LogLogic® Security Event Manager Log Collector is installed is the same as the log source host, no additional parameter is required.
- If the host where the TIBCO LogLogic® Security Event Manager 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.**

Fifth case: you have selected a RSA log source in Step 1

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

1. Click **Next**.

Sixth case: you have selected a RDEP log source in Step 1

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 to enable communication.
3. Optionally, you can enter the port to which the Log Collector must connect.
4. Click **Next**.

Seventh case: you have selected a SCANNER log source in Step 1

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.
2. Click **Next**.

Eighth case: you have selected a LOTUS DOMINO NOTES log source in Step 1

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

1. Select the Lotus Domino 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 on **Confirm**.

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

Step 5 - Installing the TIBCO LogLogic® Security Event Manager Log Collector

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

Table 2 Wizard Download Icons

Icons	Description
	Download TIBCO LogLogic® Security Event Manager Log Collector Installation file. This file is necessary when installing the TIBCO LogLogic® Security Event Manager 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 TIBCO LogLogic® Security Event Manager 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.**

Configuring a Log Collector in Advanced Mode

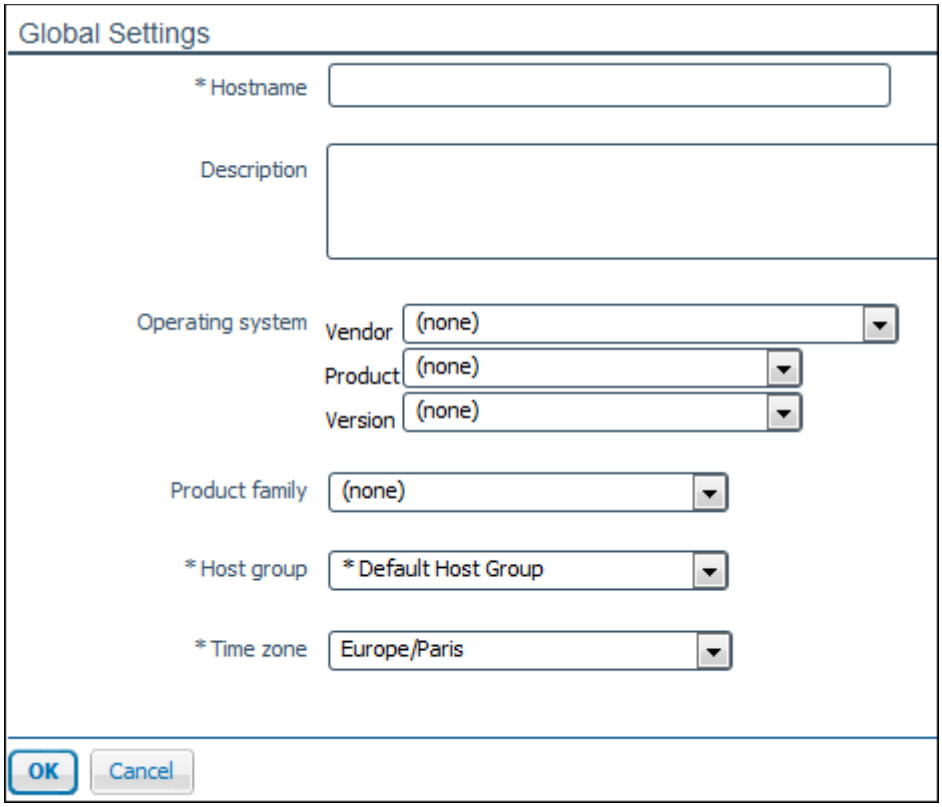
The SMP needs to be configured to collect log information from the TIBCO LogLogic® Security Event Manager Log Collector. In the following examples, a Log Collector will be installed to collect entries on a Solaris server.

Defining a New TIBCO LogLogic® Security Event Manager Log Collector

1. Open a Web Console and log in with an administrator account.

2. You must first define a host. To do so, select the host where the TIBCO LogLogic® Security Event Manager Log Collector is installed. If the host does not exist, click on **Configuration > Assets database > Hosts** to create a host.

Figure 1 Add a New Host - step 1



3. Enter a hostname in the **Hostname field** (e.g. exasun), select a **product family** (e.g. unix/linux), and a **host group** (e.g. Unix application servers) in the corresponding drop-down lists and click **OK.**

The host is displayed in the list of hosts.

4. Click on the name to modify the host configuration in the **Host Configuration** window.

5. If the type of connection is "server to log collector", enter the IP address and the hostname.

6. Once the host created, go to **Log Management > Log Collection > Log Collectors** and click **Add**.

The **Global Settings** window opens.

7. Ensure the type is **server -> log collector**. This is the preferred connection type. Use server -> log collector unless the server cannot connect to the TIBCO LogLogic® Security Event Manager Log Collector, e.g. due to an intermediate firewall.

8. Set the TIBCO LogLogic® Security Event Manager Log Collector name, e.g. exasun.

9. The default port number used by the Log Collector is 5555. If 5555 is unavailable on the host, choose another number higher than 1023. The same value must be equally set when installing the TIBCO LogLogic® Security Event Manager Log Collector and click **OK**.

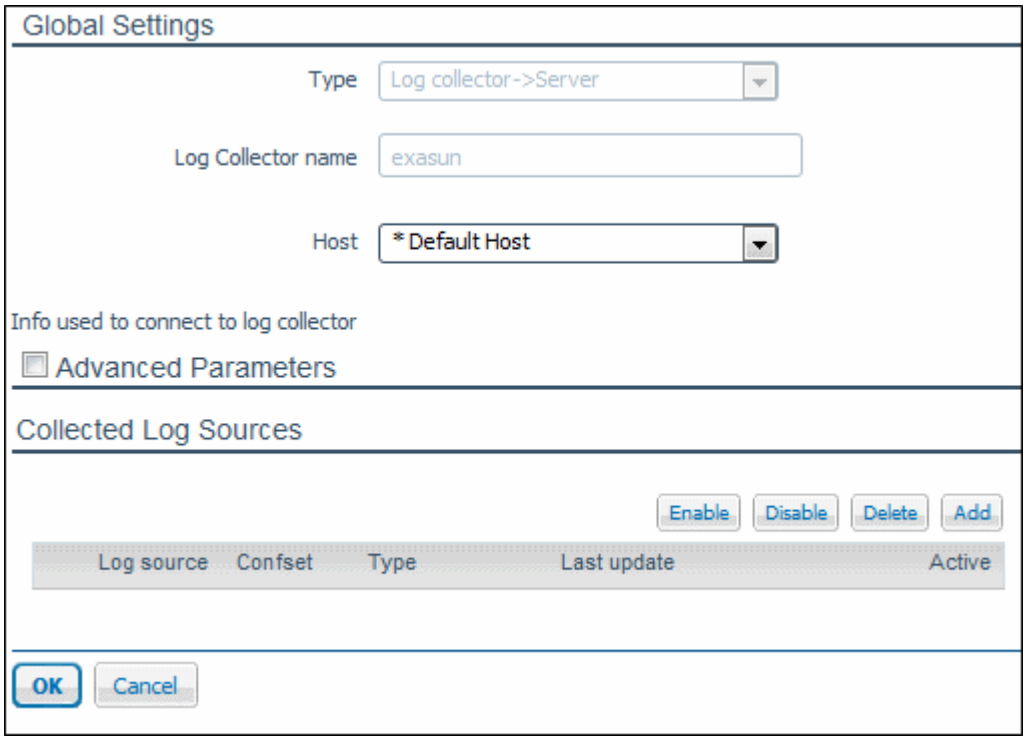
10. Enter a description of your recent action in the **History Validation** screen and click **OK**.

Configuring Log Collection

In addition to defining the new TIBCO LogLogic® Security Event Manager Log Collector, you will also need to specify the set of events to be collected. In this example, we will specify the collection of typical events of interest for a Solaris Server.

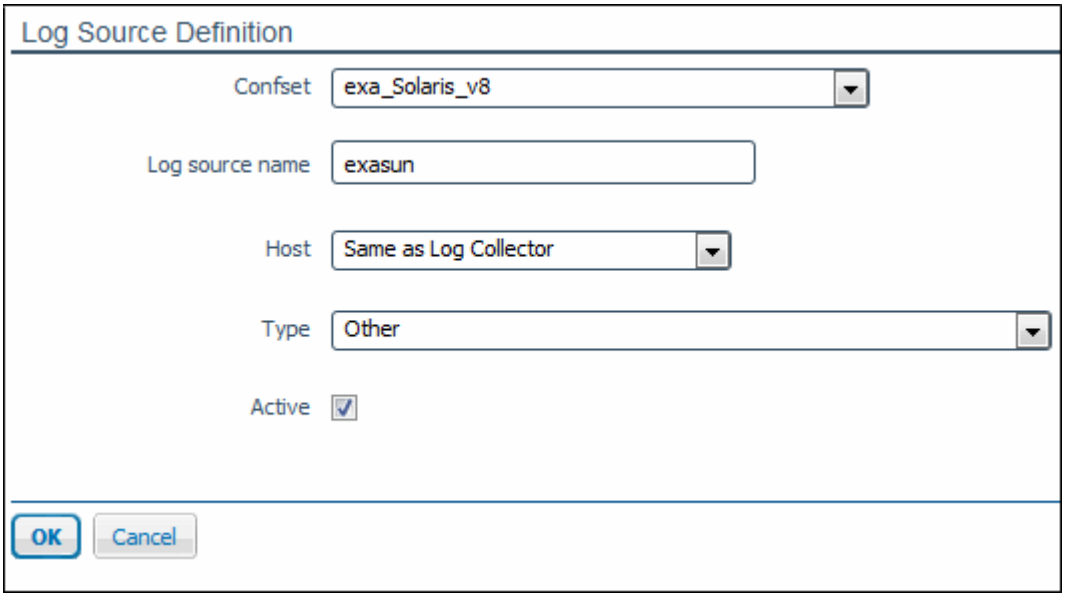
1. Click the Log Collector**'s name** of the newly added TIBCO LogLogic® Security Event Manager Log Collector (e.g. exasun) to edit it.

Figure 2 Configuration



2. Click **Add**. The **Log Source Definition** window opens.

Figure 3 Log Source Definition window



3. Select the confset **Solaris_v8.** Please remember that the confset you are going to select is not a standard confset but a confset based on a standard confset.

4. Enter the hostname of the TIBCO LogLogic® Security Event Manager Log Collector (e.g. exasun) in the **Log source name** field.

5. Set host to **Same as** Log Collector.

6. Set the analyzer type to **Unix Host** and click **OK** then click **OK** to validate.

Figure 4 List of Event Collectors Updated

Name	Type	Host	Nb	Ignore	Updated	Connected
exasun	Log Collector->Server	N/A	1	n/a	never	✗
localhost	Log Collector->Server	N/A	1	n/a	2010-10-22 17:11:40	✓

Phase 2 - Generating the Log Collector Installation and Installer Files

An installation file is required during the installation of TIBCO LogLogic® Security Event Manager Log Collectors. This file describes how the communication between the TIBCO LogLogic® Security Event Manager Log Collector and the management platform will be performed. There are three types of connections:

- the TIBCO LogLogic® Security Event Manager Log Collector initiates a connection to the management platform;
- the management platform initiates a connection to the TIBCO LogLogic® Security Event Manager Log Collector (recommended);
- management platform to management platform.

> **Caution:** You must select the same type of connection as in the Global Settings window.

In all cases, events are sent from the TIBCO LogLogic® Security Event Manager Log Collector to the server as soon as they are detected. There is neither waiting nor polling. The connection type only determines the initial set-up of the connection; the network connection between TIBCO LogLogic® Security Event Manager Log Collector and SMP is always open. SSL is used and so an authentication certificate is required.

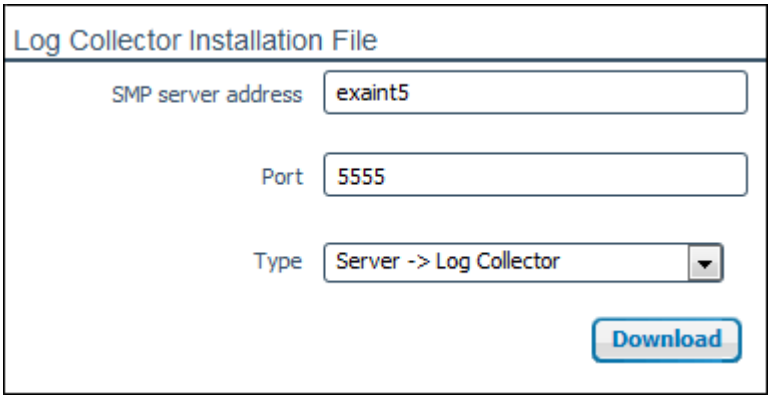
Other options such as the port number on the management platform are also included in the installation file.

This section describes the procedure that must be performed to generate the installation file.

1. Go to **Log Management > Log Collection > Download Log Collector Installation File**.

The TIBCO LogLogic® Security Event Manager Log Collector **Installation File** window opens.

Figure 5 Installation File window



2. Ensure the SMP address is correct. It is recommended to use a numeric IP address if the Log Collector is unavailable.
Please note that both the **port number** and the **connection type** must be the **same as** those

defined in the Log Collector configuration in **phase 1**.
The port number is usually 5555 but you can use another one if 5555 is not available. Ensure the connection type is the same as the one configured in phase 1.

> **Note:** The installation file is in zip format.

3. Click on **Download**.

4. Save the file with a name such as DEMO.zip, where DEMO is the instance name of the management platform.

> **Caution:** Do not forget to delete the zip file once the Log Collector software is installed.

5. To download TIBCO LogLogic® Security Event Manager Log Collector installer, go to download.tibco.com or contact the support.

Phase 3 - Installing a Log Collector

Prerequisites

The installation of a TIBCO LogLogic® Security Event Manager Log Collector requires:

- the installation software,
- the installation file such as the one created in phase 1,
- administrator rights on the machine where the TIBCO LogLogic® Security Event Manager Log Collector is installed.

> **Note:** If your SMP server and your supported product are both located in a WAN environment, it is advisable to install the TIBCO LogLogic® Security Event Manager Log Collector near the supported product in a LAN environment. Therefore, the TIBCO LogLogic® Security Event Manager Log Collector can filter large flow of information, sort data and send the main part of the information from the supported product - through the TIBCO LogLogic® Security Event Manager Log Collector - to the SMP server. This is mainly applicable for Windows supported product.
> This procedure is useful to reduce the traffic in the WAN.

Installing a Log Collector on MS Windows

> **Caution:** Microsoft Visual C++ 2005 Redistributable SP1 will be automatically installed on your computer. This is a main component to make the Log Collector run so do not uninstall it while the TIBCO LogLogic® Security Event Manager Log Collector is running.

1. On the Windows Server, log in as **Local Administrator** (otherwise, you will not have access to Event logs). Note that there is no need to have Domain Administrator rights, a **Local Administrator** account level is enough to run the setup program.

2. Run the TIBCO LogLogic® Security Event Manager Log Collector setup program, read the introduction and click **Next**.

3. Scroll down through the license, then click the option to **accept the license** and click **Next**.

4. The default installation directory is usually appropriate, but it can be changed if required. Click **Next**.

5. Check the directory where to create shortcuts and click **Next.** The default directory for the product icons is usually appropriate, but it can be changed, e.g. if you want the icons to be available for only one user.

6. Click on **Choose…** to select the TIBCO LogLogic® Security Event Manager Log Collector installation file (e.g. DEMO.zip) and click **Next**.

7. If you did not pre-configure your TIBCO LogLogic® Security Event Manager Log Collector via the wizard and if the connection is Log Collector > Server, enter the TIBCO LogLogic® Security Event Manager Log Collector's name in the **What's the** Log Collector **Name** field:

> **Caution:** Make sure the name is exactly the same as the name you entered (name, character case) when pre-configuring your TIBCO LogLogic® Security Event Manager Log Collector in advanced mode (see "Configuring a Log Collector in Advanced Mode") and if the communication mode is Log Collector > server.

8. Check that the options are correct and click **Install**.

9. When the installation is complete, click **Done**.

If the installation has not been completed successfully, open the **LogCollector_install.log** to check error messages.

This file is by default located in ***C:\Program Files\LogLogic\LogCollector\logs***.

> **Caution:** For security reasons, the folder where installation files are located is by default restricted to a given type of users. Only the following users are allowed to access this folder: the **administrator group**, the **file owner** and the **system group**.

Installing a Log Collector on Linux/Unix

1. Connect to the machine as user **`root`**.

2. Launch the Log Collector executable file.

> **Note:** If you want to use a Linux graphical display, enter
> `<LogCollector_executableFile> -i gui.`

3. Read the introduction and press **Enter**.

4. Accept the license and press **Enter**.

5. The default installation directory is usually appropriate, but it can be changed if required. Press **Enter.**

6. The default directory for data storage is usually appropriate, but it can be changed. Press **Enter**.

7. Enter the path to the Log Collector Installation File defined in Phase 2, then press **Enter**.

8. If you did not pre-configure your Log Collector via the wizard or if the Log Collector connection is Log Collector **>** ***server***, enter the Log Collector's name.

9. Check that the options are correctly configured and press **Enter**.

10. An **Installation Complete** prompt appears. Press **Enter** to validate the installation.

If the installation has not been completed successfully, open the **LogCollector_install.log** to check error messages.

This file is located in **`/opt/LogLogic/LogCollector.`**

Caution: For security reasons, the folder where installation files are located is by default restricted to a given type of users. Only the following users are allowed to access this folder: the **root user** and the **file owner**.

Phase 4 - Checking the Log Collector Connection on the Web Console

Once the TIBCO LogLogic® Security Event Manager Log Collector is installed, the SMP connects to it and updates the Log Collector's configuration.

1. Connect to the Web Console and go to **Log Management** > **Log Collection** > **Log Collectors**.

Figure 6 Server-Log Collector Connection Status

If the status column does not display **Connected**, wait a few minutes for the connection to be established and eventually click **Refresh** if the status does not change.

If you want to ignore the new Log Collector in the **Server >** Log Collector mode, you can select the check box in the first column and then click **Ignore**.

2. If the **Status** column still displays **disconnected**, then:

- check the connection error messages in the Log Collector configuration window.
- check that there are no firewalls blocking connections between the SMP and the TIBCO LogLogic® Security Event Manager Log Collector, including host-based firewalls.

Note: It is recommended to reinstall the TIBCO LogLogic® Security Event Manager Log Collector should you suspect a problem with the Log Collector keys. The keys are used to ensure data exchange confidentiality and integrity between the Log Collector and the SMP.

Chapter 4 - Uninstallation Phases

Uninstalling a Log Collector on MS Windows

1. On the Windows Server, log in as **Local Administrator** (otherwise, you will not have access to Event logs). Note that there is no need to have Domain Administrator rights, a **Local Administrator** account level is enough to run the uninstallation program.

2. Choose one of the two following solutions to display the **Uninstall** window:

- **a.** Run the TIBCO LogLogic® Security Event Manager Log Collector uninstall program by selecting P**rograms> LogLogic > LogCollector> Uninstall TIBCO LogLogic(R) - SEM Log Collector**.
- **b.** Or Open the **Control Panel** by clicking on **Start > Programs > Control Panel> Add or Remove Programs.**
- **c.** Select **TIBCO LogLogic(R) - SEM Log Collector**.
- **d.** Click on the **Change/Remove** button.

3. Click on the **Uninstall** button. The automatic uninstallation is launched.

4. Click on the **Done** button to close the window.

Uninstalling a Log Collector on Linux/Unix

1. Connect to the machine as user `root`.

2. Enter the following command:

```
"/opt/LogLogic/LogCollector/Uninstall/Uninstall TIBCO LogLogic(R) -
SEM Log Collector"
```

3. Press Enter.

Appendix A - SEM Glossary

Table 3 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.

Table 3 Glossary

Term	Definition
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.
Event	An event is a standardized data object (IDMEF and TIBCO LogLogic® Taxonomy) representation of a log entry that has been generated by a log source. The events collected by the SMP is also called 'elementary events'. On the SMP, these events are aggregated by the aggregation engine. Events generated by this engine is called 'aggregated event'.
Heartbeat	A message sent by the Log Collector to the SMP to indicate the Log Collector is active.
IDMEF	Intrusion Detection Message Exchange Format. The IDMEF is a special data format used for sharing information of interest to intrusion detection and response systems, and to the management systems which may need to interact with them. Standard RFC 4765.
IODEF	Incident Object Description and Exchange Format.
Incident	Container of alerts of IODEF format, allowing to ensure the management of these alerts. It specifies their cause and the actions that must be triggered.
Instance	An instance consists of: the configuration of logs and devices to be monitored the collected events the rules and scenarios to apply to the collected events a console server (the Web Console)
Live Explorer screen	The Live Explorer screen allows you to monitor everything that happens on the SMP server.
Live Reporting	Rules used by the Totaling Engine to enrich the reporting database in real time.
Log Collector	The software Log Collector installed on a machine to collect information, format it, and forward it to the SMP.

Table 3 Glossary

Term	Definition
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.
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.

Table 3 Glossary

Term	Definition
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.