TIBCO LogLogic®

Security Event Manager (SEM)

Administration 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 document contains confidential information that is subject to U.S. and international copyright laws and treaties. No part of this document may be reproduced in any form without the written authorization of TIBCO Software Inc.

TIBCO, Two-Second Advantage and LogLogic are either registered trademarks or trademarks of TIBCO Software Inc. and/or subsidiaries of TIBCO Software Inc. in the United States and/or other countries.

All other product and company names and marks mentioned in this document are the property of their respective owners and are mentioned for identification purposes only.

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.

Copyright © 2002-2013 TIBCO Software Inc. ALL RIGHTS RESERVED.

TIBCO Software Inc. Confidential Information

Contents

List of Tables

List of Figures

Preface

This guide describes how to configure and manage advanced parameters.

You will learn how to:

- configure in an advanced way your SMP.
- managing Incidents via an External Server.
- automatically send an email when an incident is created.

Audience

This guide is intended for Security Network Administrators who are responsible for installing and maintaining network security software.

Related Documentation

Documentation	Content
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.
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 ...]
```

Requirements

Prior to using the various procedures described in this guide, please make sure to read and follow the hardware and software requirements listed in this chapter.

Hardware

You will need:

- an installed and configured Security Management Platform.
- either a monitor and keyboard for a local connection or a computer station for a remote connection.
- a PC with a web browser such as Microsoft Internet Explorer v.7.0 or higher, Mozilla Firefox 13.
- an Internet Protocol (IP) network connection between the above equipment units.

Limitations

Filesystem Check

In the event of a server reboot, the **Operating System** will check the filesystem. In this case, the time of the process differs according to the type of arrays.

- ODA 4 Tb: 15 minutes
- ADA 14 Tb: 1 hour

Chapter 1 - The SMPConfig Tool

Caution: Please read carefully the Requirements section before configuring the SMPConfig tool.

Opening the SMPConfig Main Menu

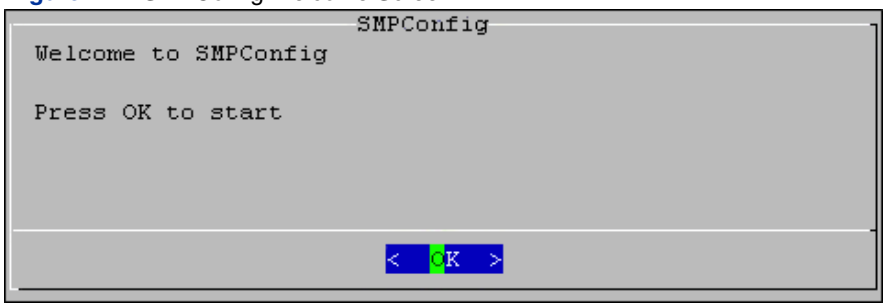
1. If you are using a remote connection to the server, open an SSH console on the SMP.

Note: 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.

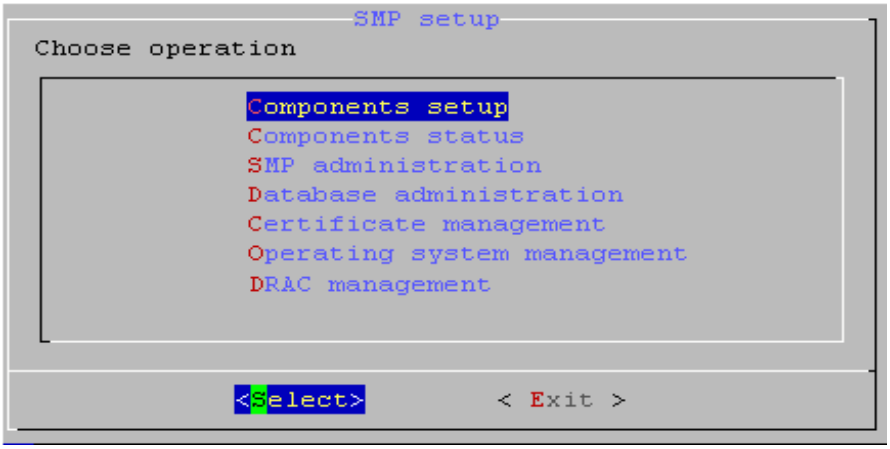
3. The **Welcome to SMPConfig** screen is displayed. To continue, press Enter.

Figure 1 SMPConfig Welcome Screen



4. The **SMP setup** main menu with several options is displayed.

Figure 2 The SMP setup menu



Note: The DRAC management menu entry is only displayed if a DRAC card is installed.

Navigating through the Menus

1. To enter a submenu, use the **Up** and **Down** arrows to highlight the desired submenu and then click **Return**.

2. Once you have entered a submenu, you may go back to a higher menu level by selecting **Back** and then clicking **Return**.

3. You may also use the **Right** and **Left** arrows to navigate and highlight another option on the same level (such as going from **Select** to **Exit -** bottom of the screen in Figure 2 "The SMP setup menu").

4. Depending on the software you are using to connect to the server, you will also have the option to use your mouse pointer to click on a menu label and select it.

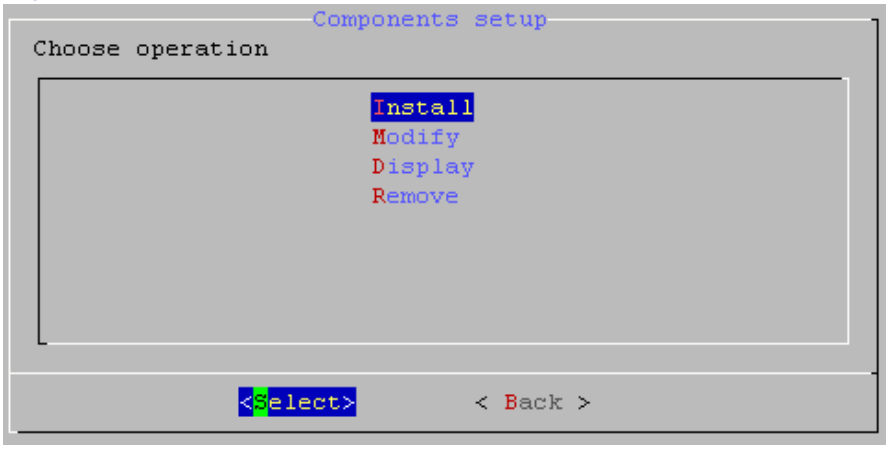
The Components Setup Menu

In this menu section you may execute various actions referring to one or more SMP instances.

Opening the Components Setup Menu

To open the Components Setup menu, go to the main menu and select Components Setup. (See "Opening the SMPConfig Main Menu" and "Navigating through the Menus").

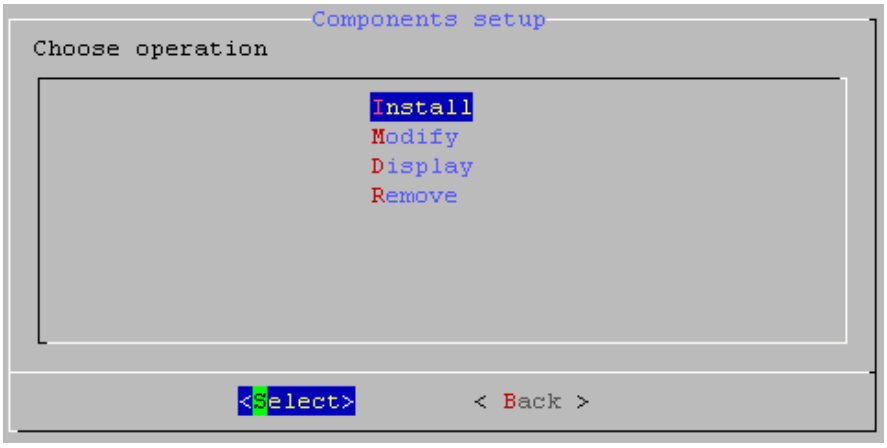
Figure 3 Components setup



Installing a New Instance

1. Use the **Up** and **Down** arrows to highlight **Install** and then click **Return.**

Figure 4 Components setup - install a new instance

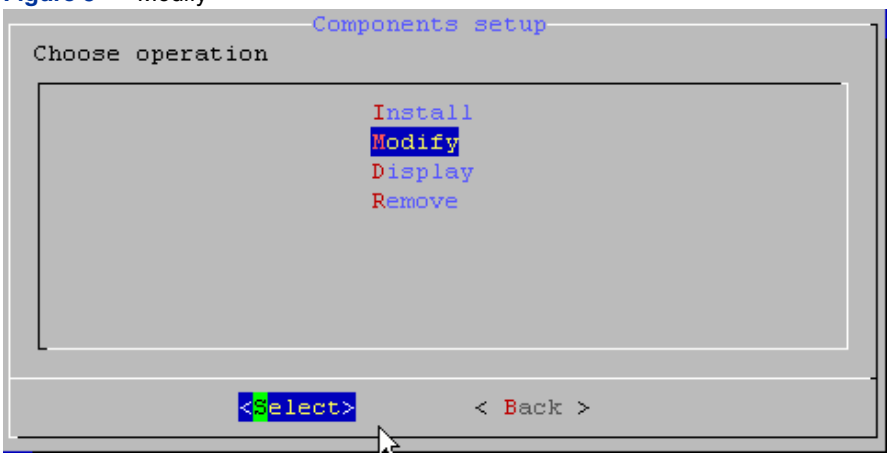


2. Use the **Up** and **Down** arrows to highlight the package to install and then click **Return.**
3. To install multiple instances, please contact our technical support for additional guidance.

Modifying an Instance

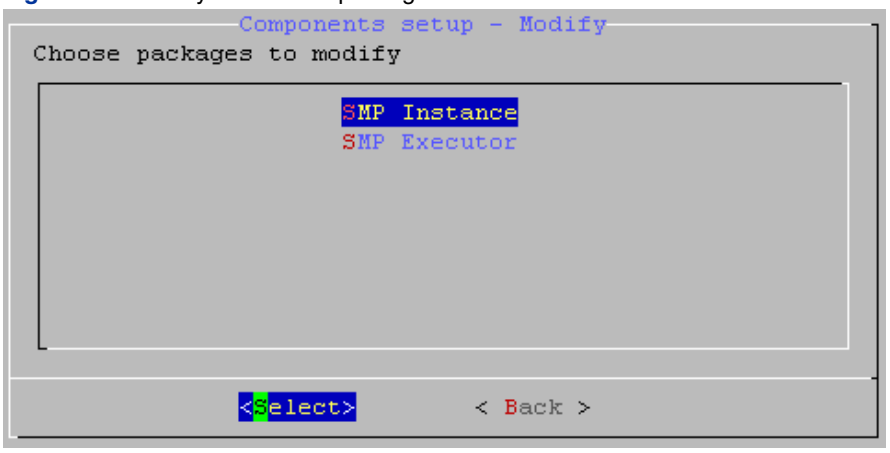
1. Use the **Up** and **Down** arrows to highlight **Modify** and then click **Return.**

Figure 5 Modify



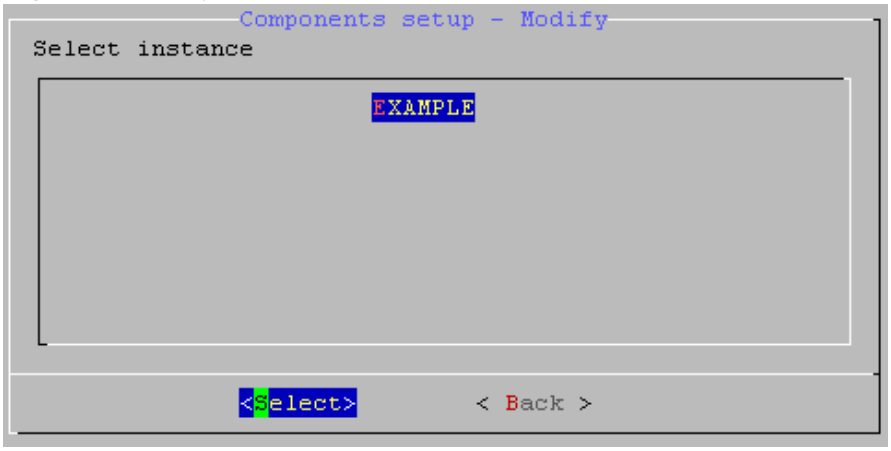
2. Use the **Up** and **Down** arrows to highlight the package to modify and then click **Return.**

Figure 6 Modify - select the packages



3. Use the **Up** and **Down** arrows to highlight the instance to modify and then click **Return**.

Figure 7 Modify - select the instance



4. The instance parameters menu appears.

Figure 8 Modify - select the parameter to modify

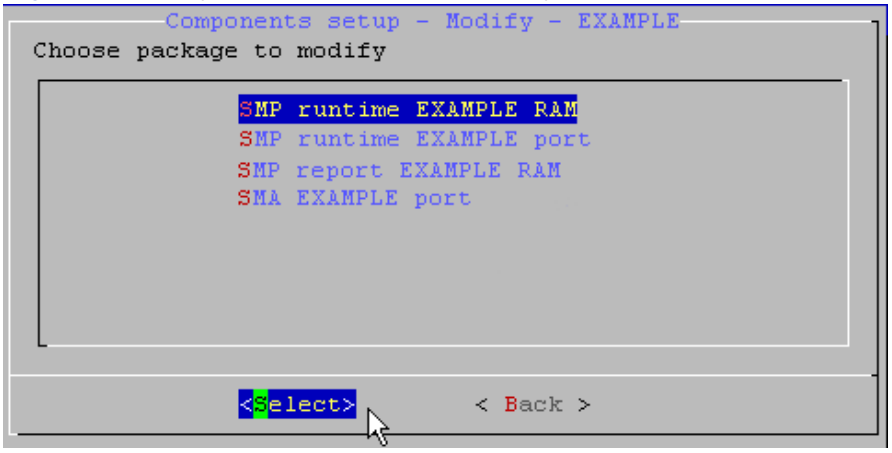


Table 1 The instance parameters

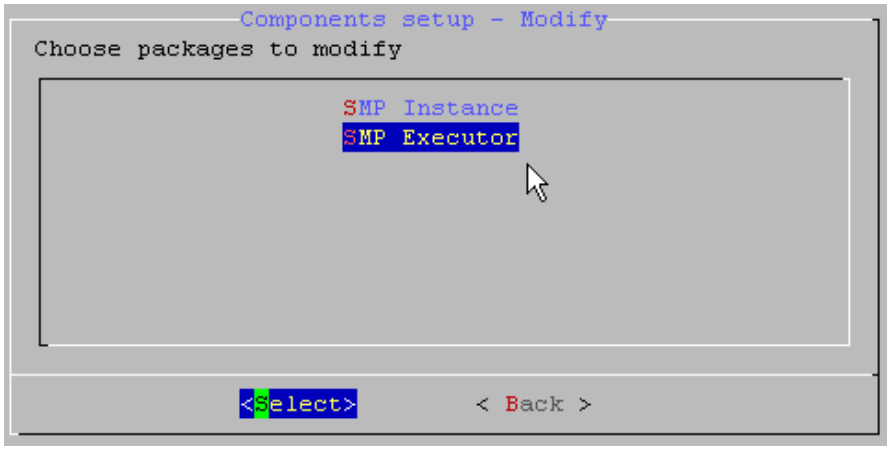
Parameters	Description
SMP Runtime RAM	Allows you to change the amount of RAM (Random Access Memory) allocated to the related instance. This parameter indicates how much memory will be used by the correlation engine and the display of alerts.
SMP Runtime port	Allows you to modify the port being used by the related instance. This port is used to make a HTTPS connection to the Web Console console. Default value: 10443.

Table 1 The instance parameters

Parameters	Description
SMP Report RAM	Allows you to change the amount of RAM (Random Access Memory) allocated to the reporting instance. This parameter indicates how much memory will be used by the reporting engine.
Log Collector port	Allows you to modify the port through which the Log Collectors connect to the instance in the Log Collector->server mode. Default value: 5555.

Use the **Up** and **Down** arrows to highlight the parameter to modify and then click **Return.** Enter the new values for the parameter and click **Return**.

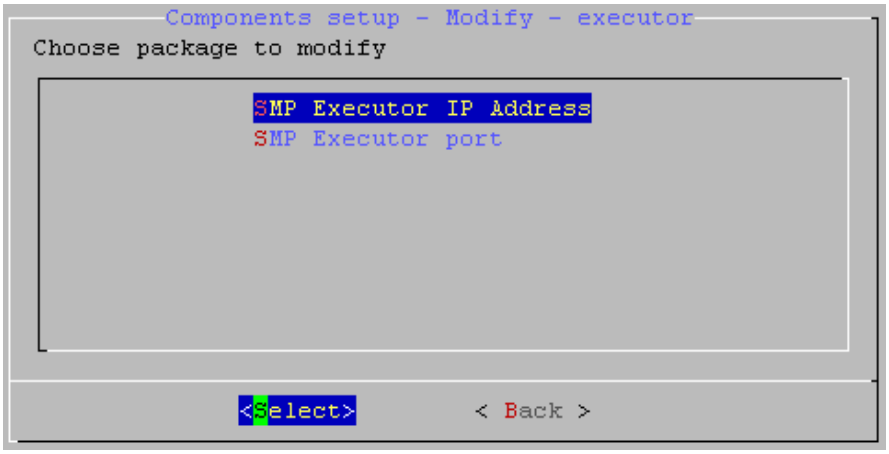
Figure 9 Components setup - SMP Executor



To Change the IP Address

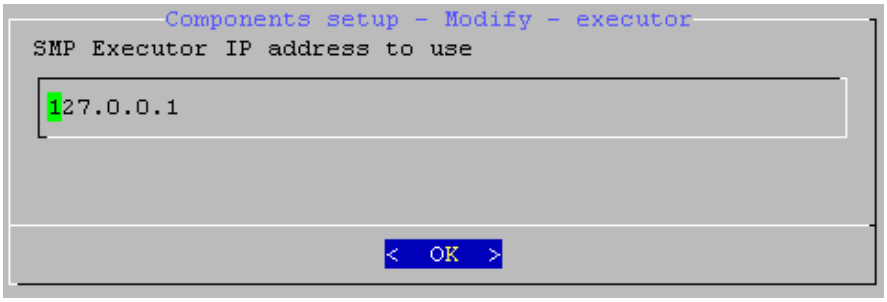
1. Go to **Main menu -> Components Setup ->Modify -> SMP Executor.**
2. Use the **Up** and **Down** arrows to highlight SMP **Executor IP address** and then click **Return.**

Figure 10 Components setup - SMP executor IP address



3. Enter the desired IP address and then click **Return.**

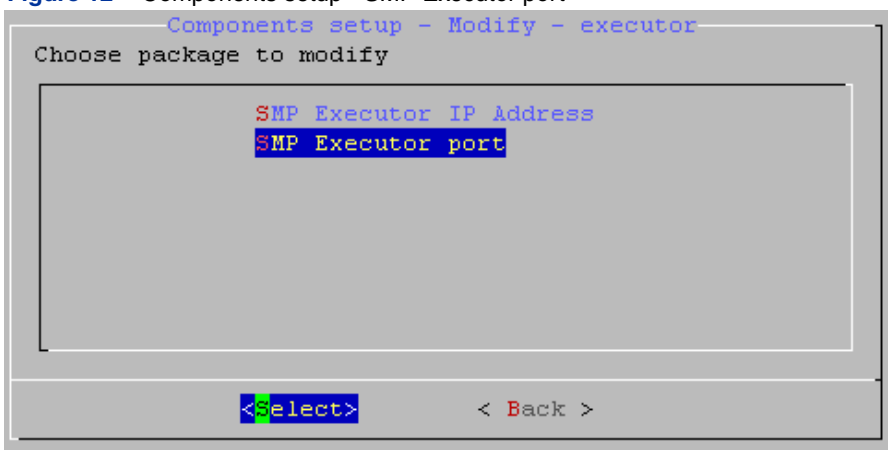
Figure 11 Components setup - Modifying the IP address



To Change the Port Number

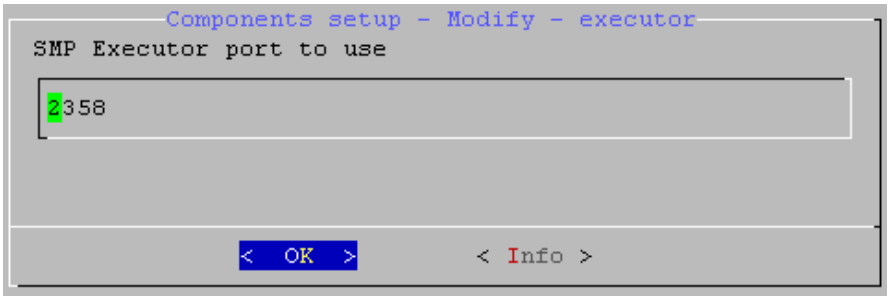
1. Go to **Main menu -> Components Setup ->Modify -> SMP Executor.**
2. Use the **Up** and **Down** arrows to highlight SMP **Executor IP address** and then click **Return.**

Figure 12 Components setup - SMP Executor port



3. Enter the desired port number and then click **Return.**

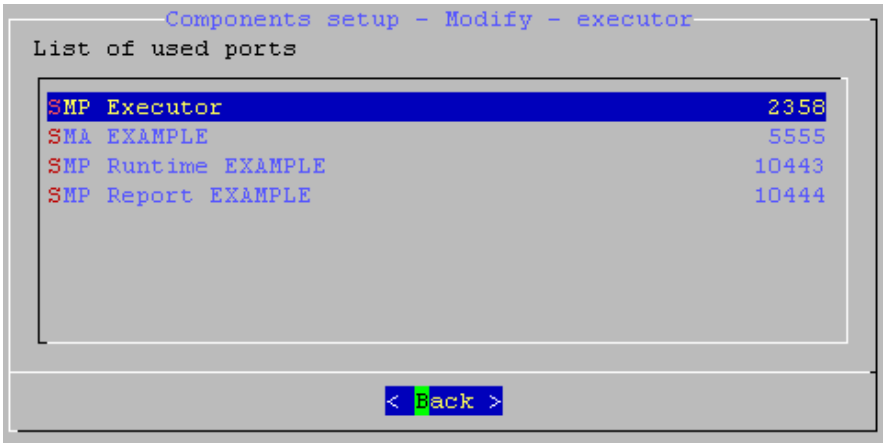
Figure 13 Components setup - modifying the port number



Displaying Information Regarding Ports and RAM

1. Use the **Up** and **Down** arrows to highlight the **SMP Executor Port** (see "To Change the Port Number") and then click **Return**.
2. Enter the Port number and then click **Return.**
3. To view the ports currently in use, click the **Up** and **Down** arrows to highlight **Info** and then click **Return.**

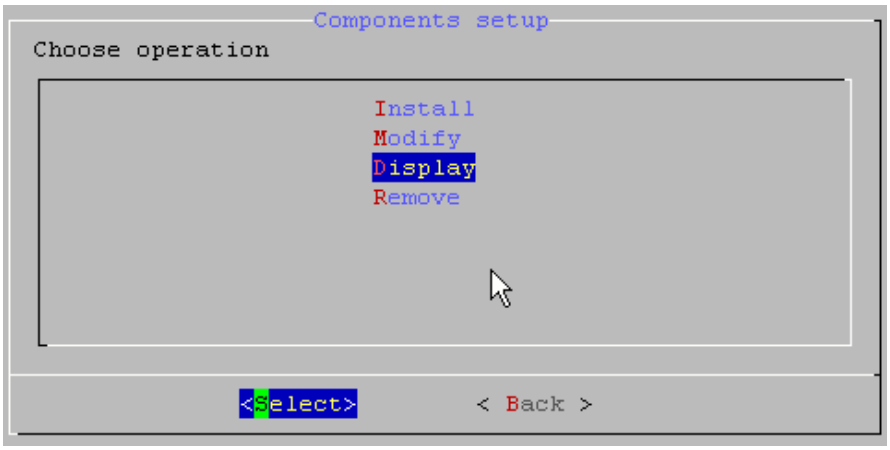
Figure 14 Components Setup - list of used ports



Displaying Information Regarding Ports and RAM Being Used

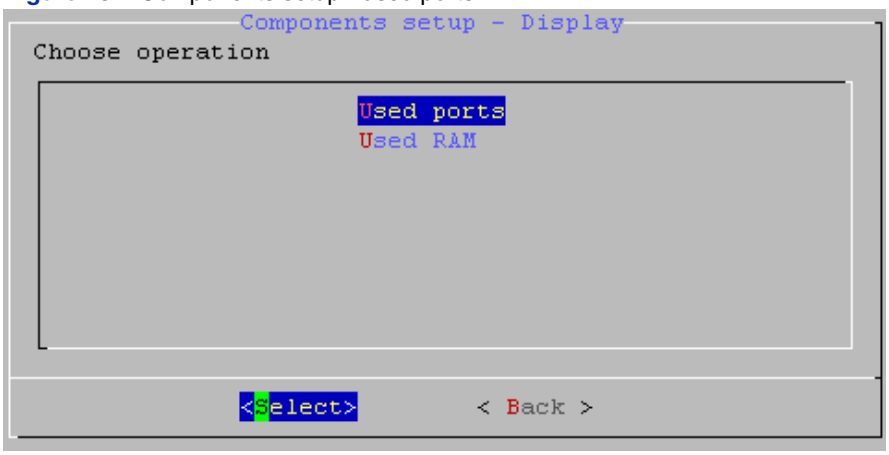
1. Go to **Main menu -> Components Setup ->Display.**

Figure 15 Components setup - Display submenu



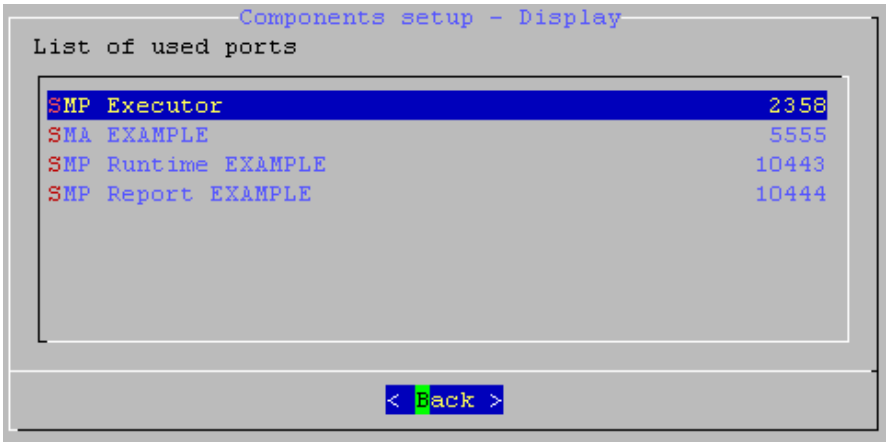
2. Use the **Up** and **Down** arrows to highlight **Used ports** and then click **Return.**

Figure 16 Components setup - used ports



3. A list of ports currently in use will be displayed. To return to the previous screen, click **Return.**

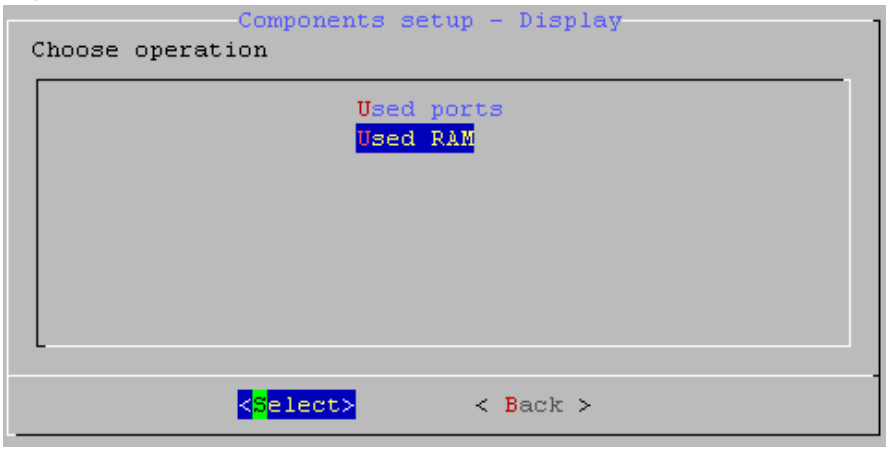
Figure 17 Components setup - displaying used ports



To View RAM Currently in Use

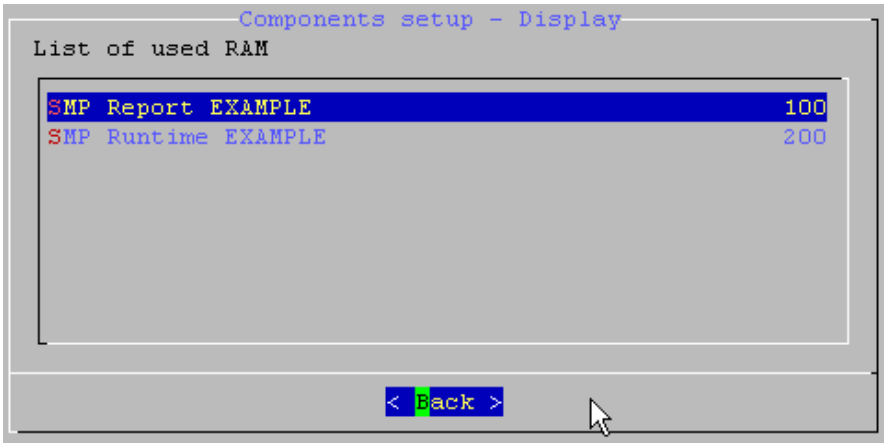
1. Go to **Main menu -> Components Setup ->Display**
2. Use the **Up** and **Down** arrows to highlight **Used RAM** and then click **Return**.

Figure 18 Components setup - used RAM



3. A list of RAM currently in use will be displayed. To return to the previous screen, click **Return.**

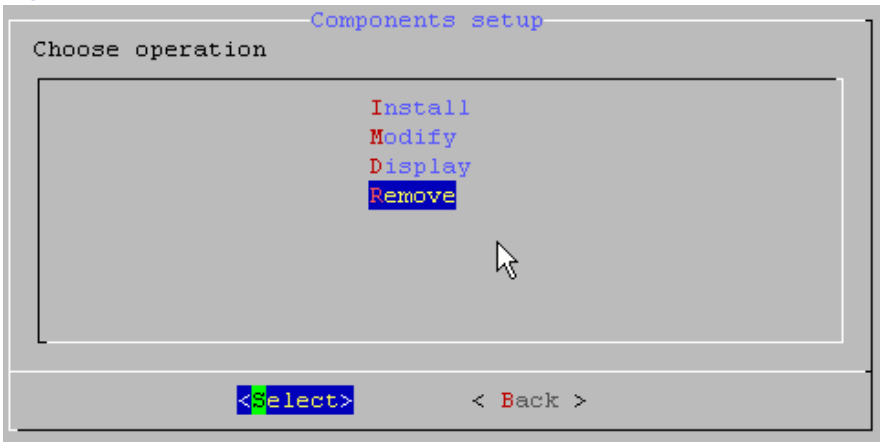
Figure 19 Components setup - list of used RAM



Removing an Instance

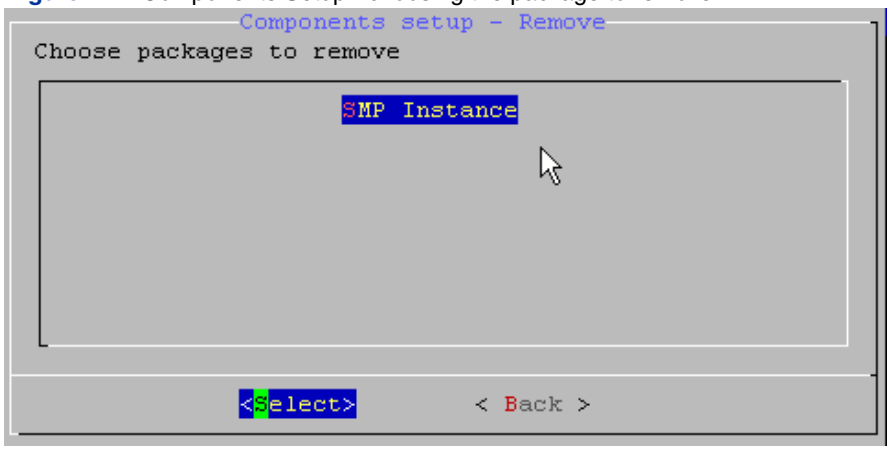
1. Go to **Main menu -> Components Setup ->Remove.**

Figure 20 Components Setup - Remove submenu



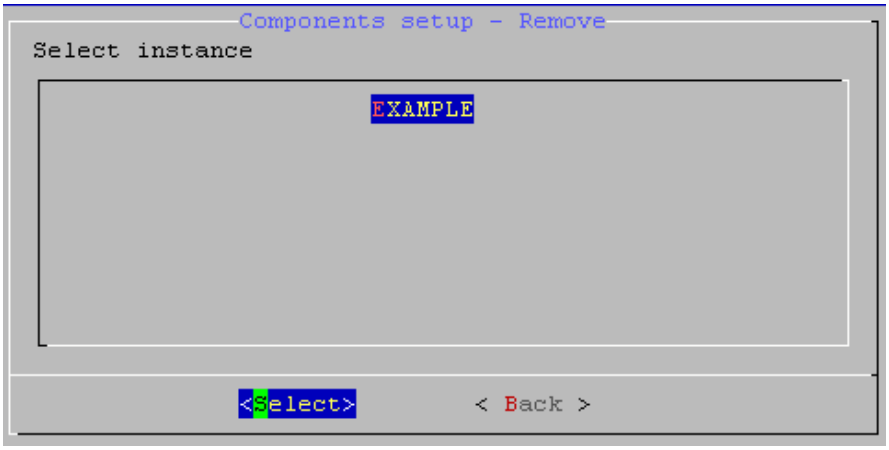
2. Use the **Up** and **Down** arrows to highlight the package to be removed and then click **Return.**

Figure 21 Components Setup - choosing the package to remove



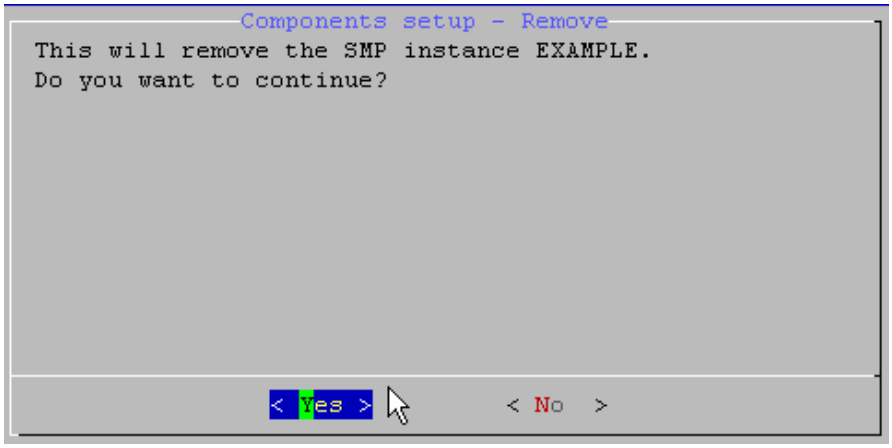
3. Use the **Up** and **Down** arrows to highlight the instance to be removed and then click **Return.**

Figure 22 Components Setup - selecting the instance to be removed



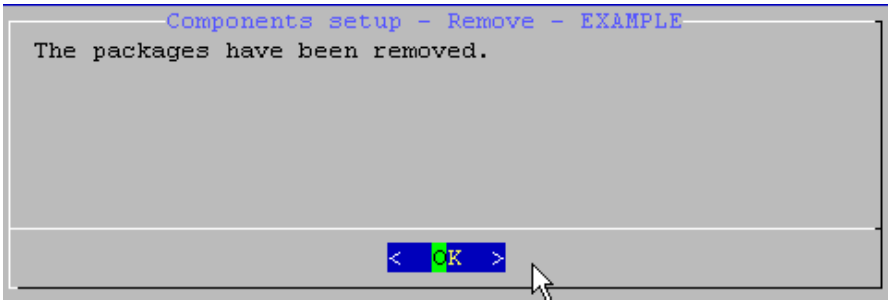
4. Please confirm the removal of the instance by selecting **Yes**.

Figure 23 Components Setup - confirming the removal



5. The system will display one or more messages that it is processing the removal of the instance. When it finalizes the process, it will display:

Figure 24 Components setup - remove finished



6. Click **Return** to continue.

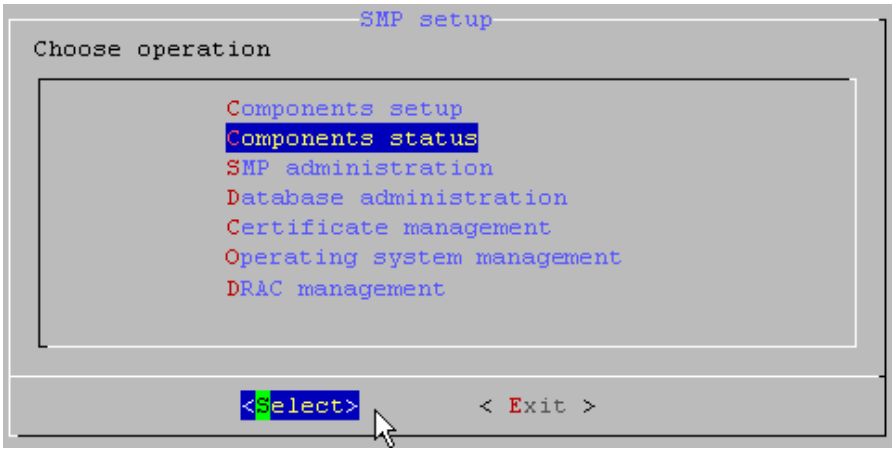
The Components Status Menu

In this menu section you may start or stop one or more components.

Starting or Stopping a Component

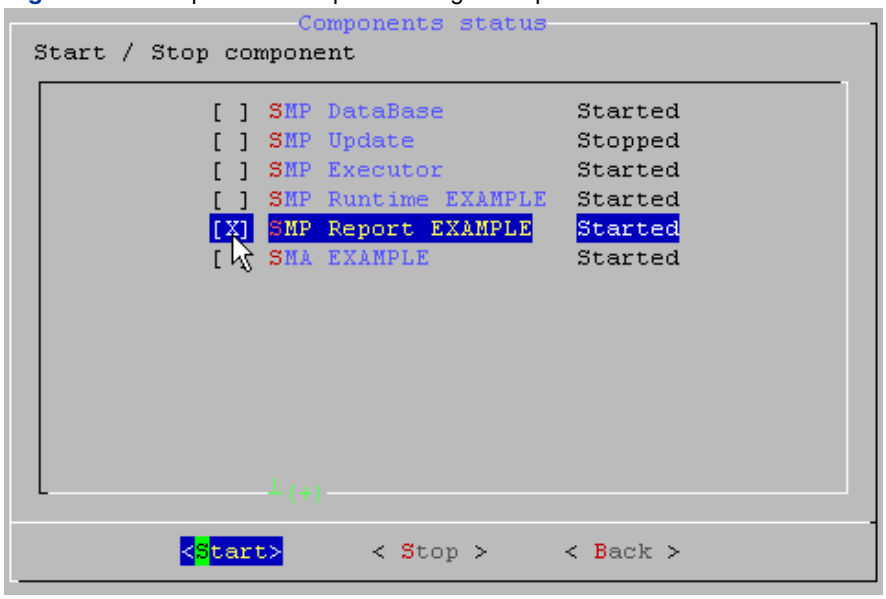
To open the **Components Status** menu, go to the main menu and select **Components Status**. (See "Opening the SMPConfig Main Menu" and "Navigating through the Menus").

Figure 25 Components status



1. A list of components is displayed.

Figure 26 Components Setup - choosing a component



2. Use your keyboard navigation arrows to highlight the desired choice, press the space bar to select the option, and then click **Return**. (To select a component, you may also click inside a set of empty brackets using your mouse pointer).

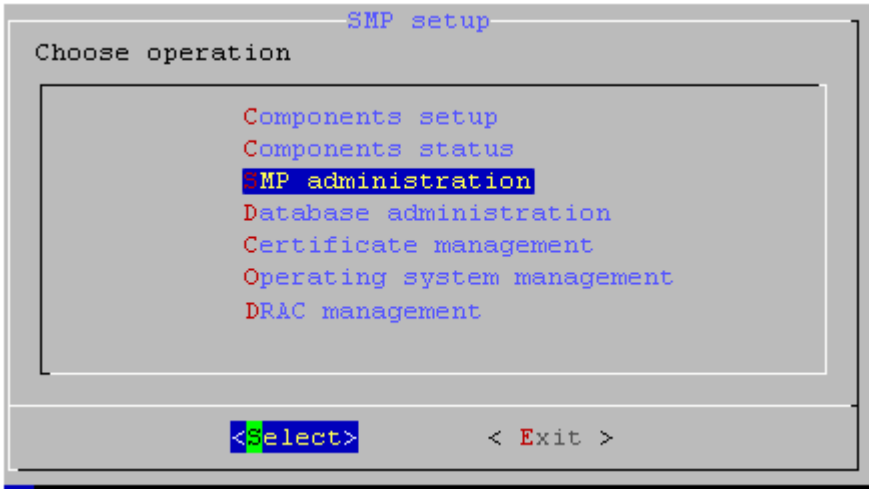
3. Navigate to highlight either the **Start** or the **Stop** options and then click **Return**.

4. Please wait while the system processes your request. You will see the updated list of components next. To return to previous menus, highlight **Back** and click **Return**.

The SMP Administration Menu

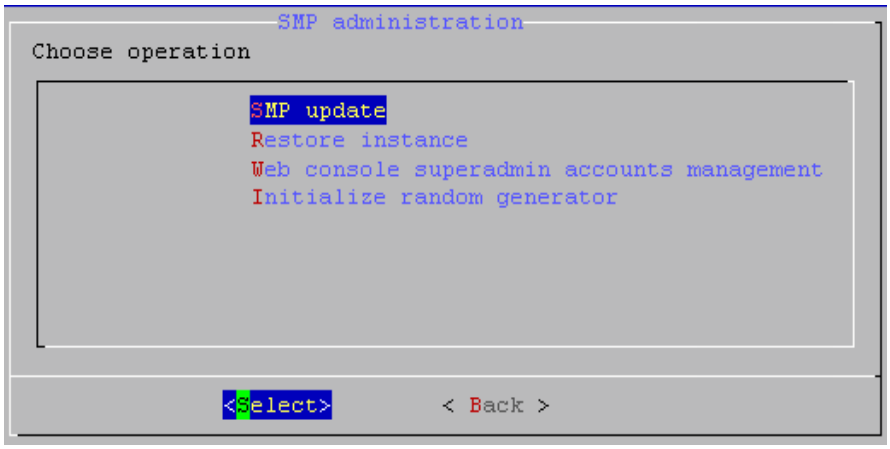
To open the SMP **Administration** menu, go to the main menu and select SMP **Administration**. (See "Opening the SMPConfig Main Menu" and "Navigating through the Menus").

Figure 27 SMP setup - SMP Administration



The SMP Administration submenu is displayed:

Figure 28 SMP Administration submenus



Restoring an Instance

The following operation consists in reinstalling an instance in the event of a server failure. The ZIP file allows the reintegration of the instance total configuration

Prerequisites

To restore an instance, you must have previously made a backup of the instance. Please refer to the User Guide to know how to make a backup of an instance

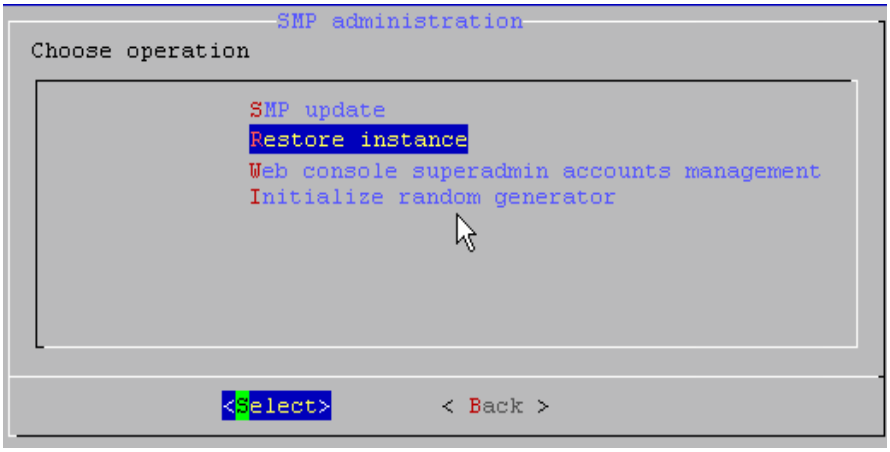
A backup can only be restored:

- 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.

> **Caution:** The backup restoration overwrites all data available in the database. Only the backup file configuration is restored, i.e. alerts, incidents, aggregated events are lost.

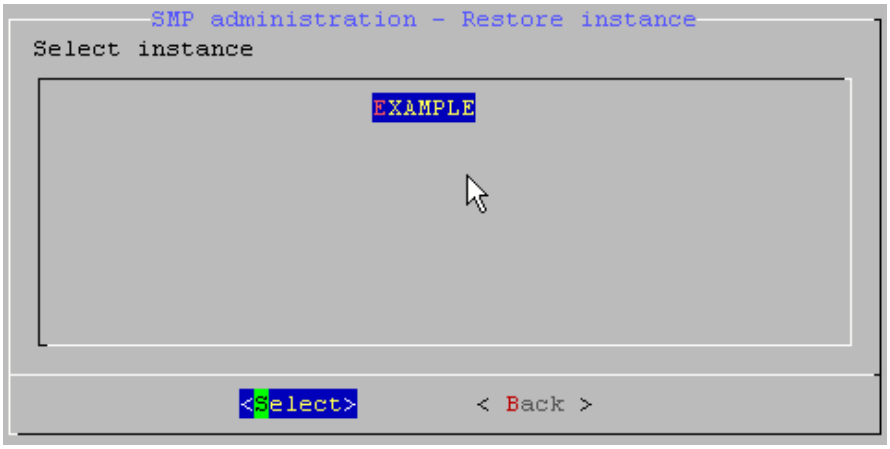
1. To restore an instance, go to **Main menu ->** SMP **Administration -> Restore Instance** and click **Return.**

Figure 29 Restore instance



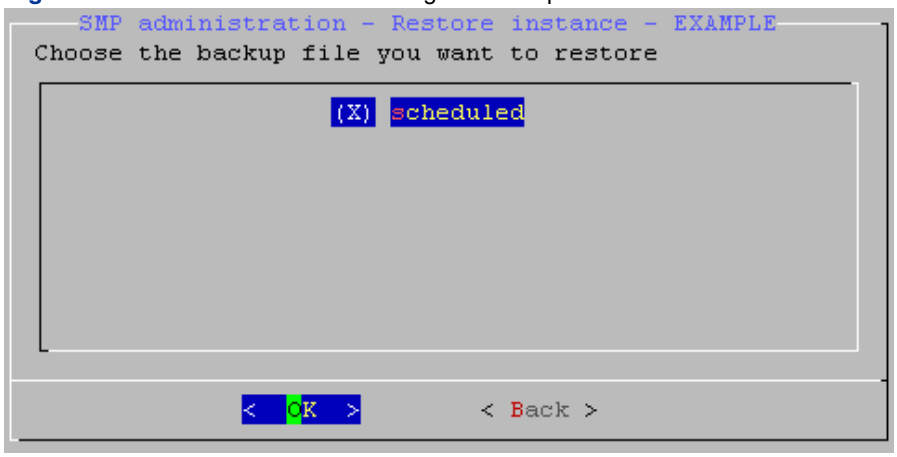
2. Use the **Up** and **Down** arrows to highlight the instance to be restored and then click **Return.**

Figure 30 Restore instance - selecting the instance



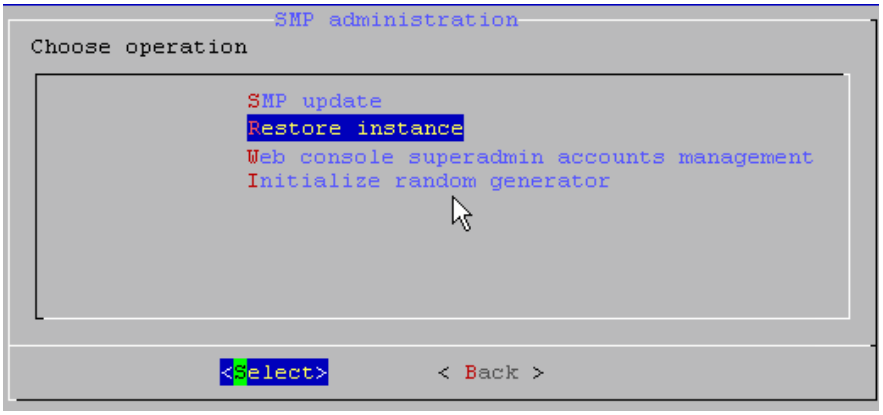
3. Use the **Up** and **Down** arrows to highlight the backup file to restore and then click **Return.**

Figure 31 Restore instance - selecting the backup file



4. Please confirm your selection by clicking **Return.**

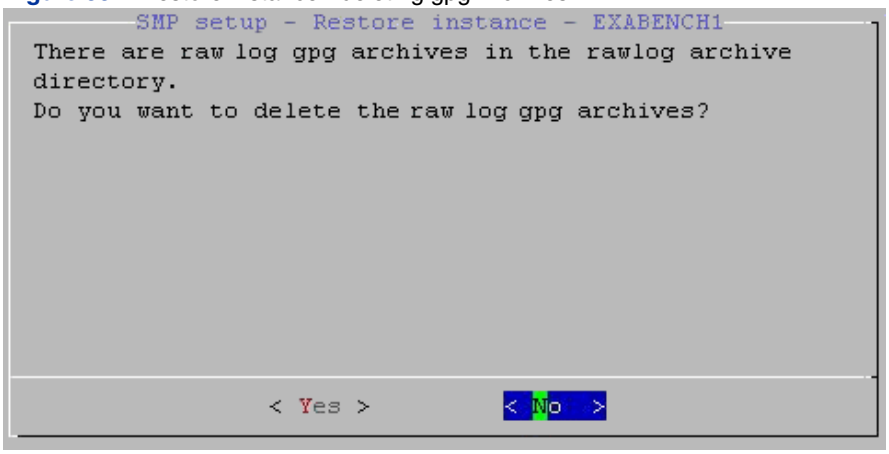
Figure 32 Restore instance



5. The system will display one or more messages regarding the progress of the operation**.**

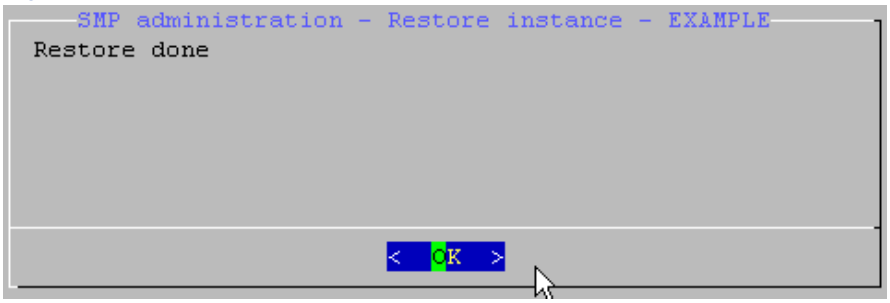
6. When the operation is finished, you will see the following message asking you if you want to delete the existing gpg raw logs in your database. Select **Yes** or **No**.

Figure 33 Restore instance - deleting gpg Archives



7. The restore is done.

Figure 34 Restore instance - operation finished



8. Click **Return** to return to the previous menu.

Account Management

This menu section allows you to execute certain operations to manage your Web Console account(s).

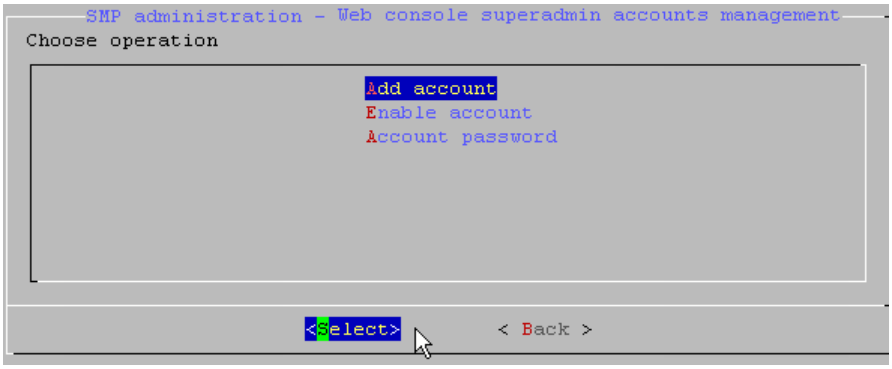
Note: The operations described in this section refer only to your superadmin account(s).

Adding a Web Console Account

1. To add a Web Console account, go to Main menu -> SMP Administration ->Web console superadmin accounts management-> Add account.

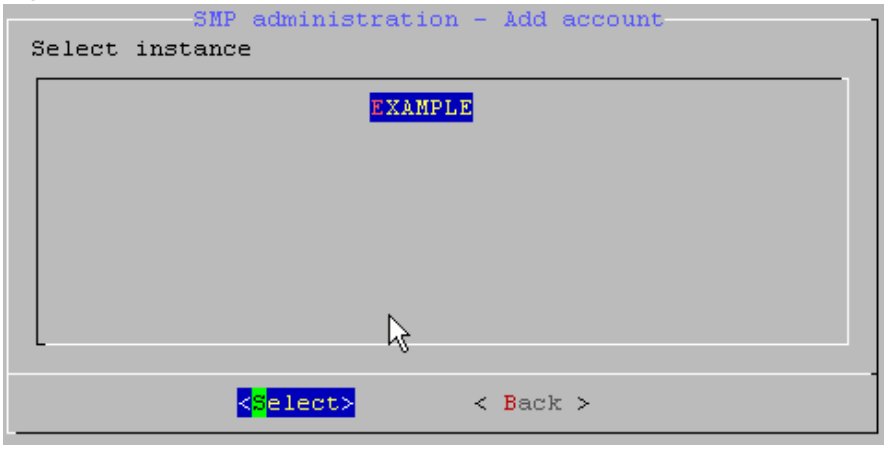
The following screen is displayed.

Figure 35 Add account



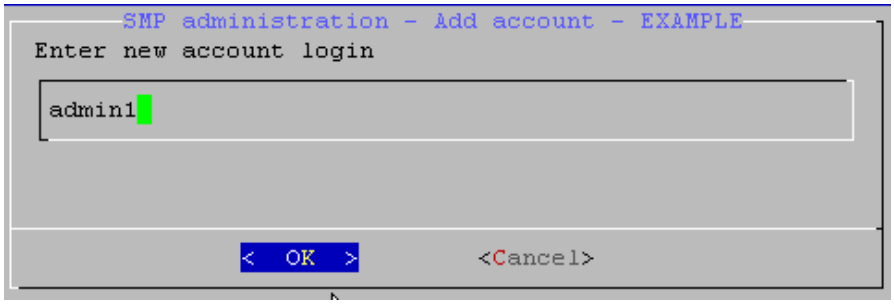
2. Use the Up and Down arrows to highlight the instance to add the account to and then click Return.

Figure 36 Add account - select the instance



3. Enter the new account login and then click **Return.**

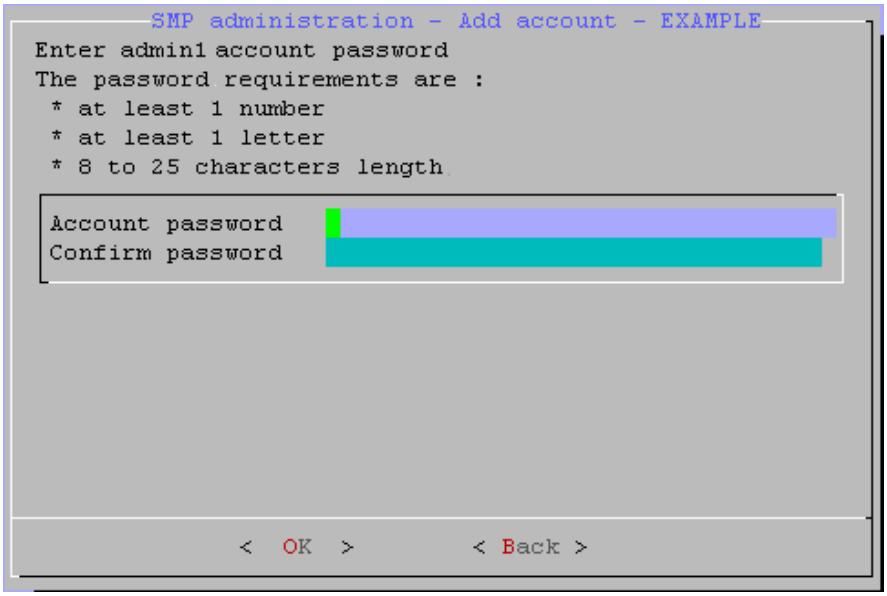
Figure 37 Add account - enter the new account login



4. Enter the new account password and press the **down arrow** key to go to the line below.

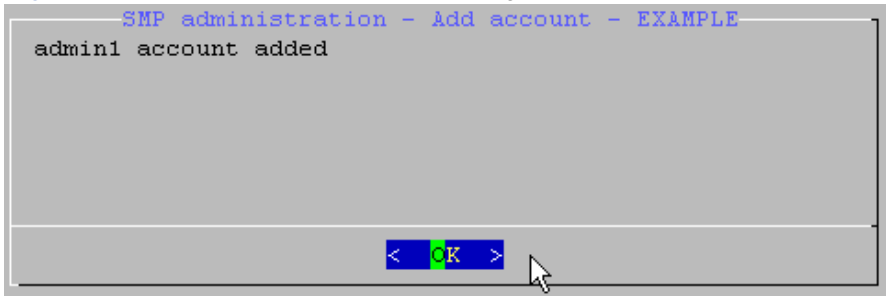
5. Confirm the account password then press the **Tabular key** and select **OK.**

Figure 38 Add account - enter the new account password



6. A confirmation message will be displayed. Click **Return** to return to the previous menu.

Figure 39 Add account - confirmation message

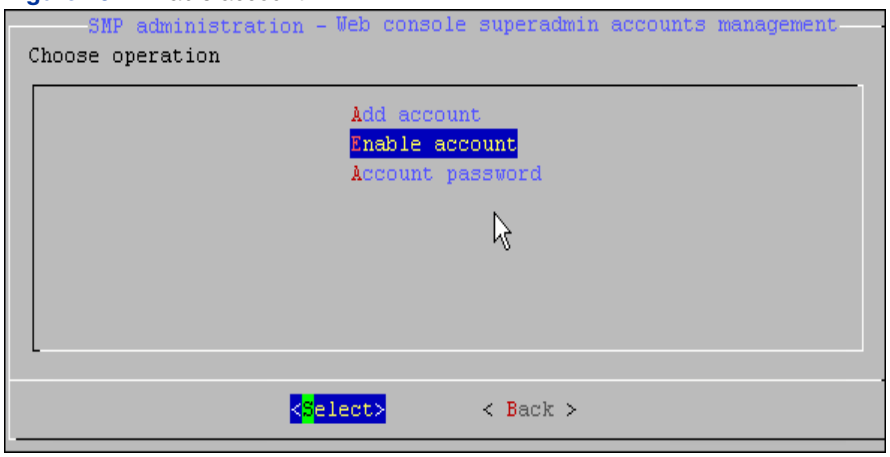


Caution: This procedure does not give access to the reporting interface. To access it, you must activate the user access from the Web Console via the User Account Edition window (Configuration > User Accounts).

Enabling a Web Console Account

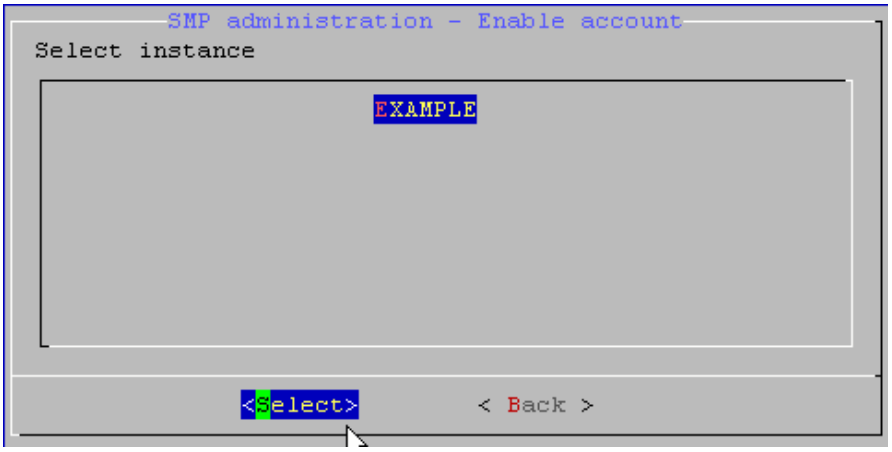
1. To enable an account, go to **Main menu ->** SMP **Administration ->Web Console superadmin accounts management-> Enable account.**

Figure 40 Enable account



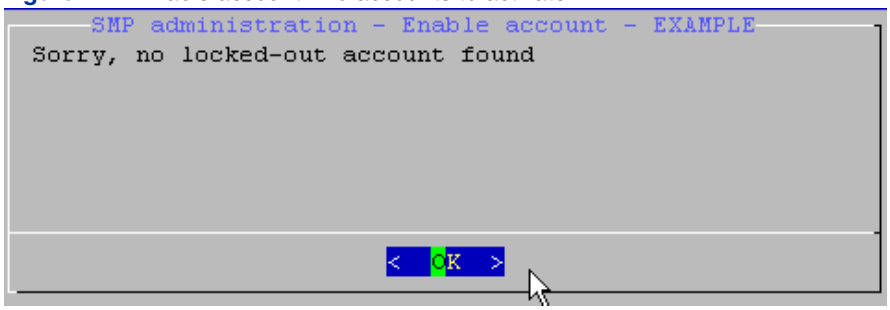
2. Use the **Up** and **Down** arrows to highlight the instance related to the account and then click **Return.**

Figure 41 Enable account - selecting the instance



3. If there are any accounts to be activated, they will be displayed. Click on the account to activate. Otherwise, if there are no accounts to activate, you will see the following message:

Figure 42 Enable account - no accounts to activate

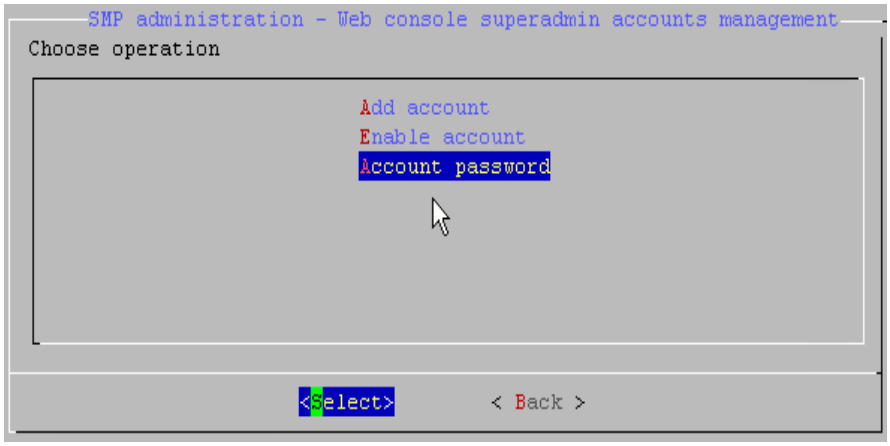


4. Click **Return** to return to the previous menu.

Changing the Account Password

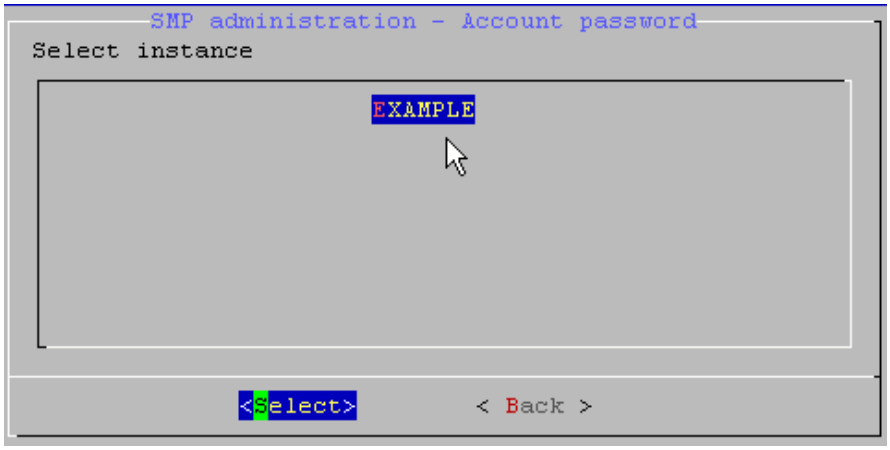
1. To change the password related to a Web Console account, go to **Main menu ->** SMP **Administration ->Web Console superadmin accounts management-> Account password.**

Figure 43 Account password



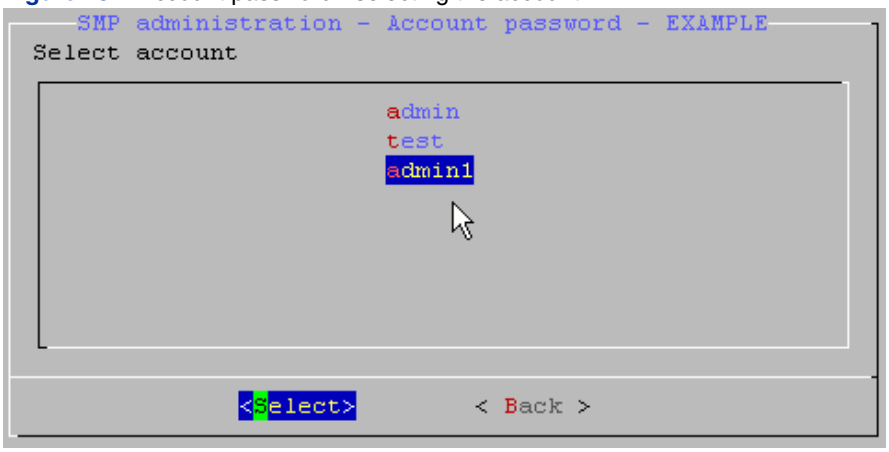
2. Use the **Up** and **Down** arrows to highlight the related instance and then click **Return.**

Figure 44 Account password - selecting the instance



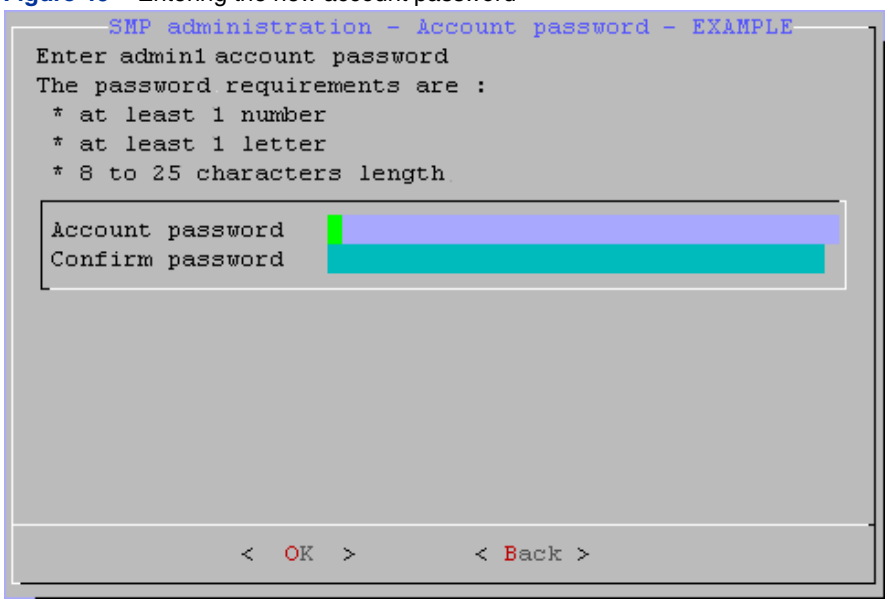
3. Select the related account and then click **Return.**

Figure 45 Account password - selecting the account



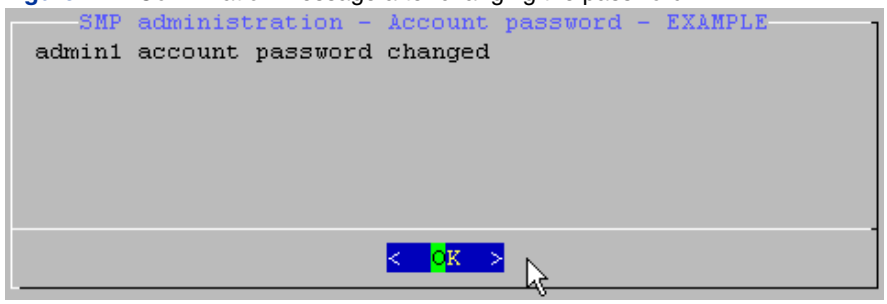
4. Enter the new account password and press the **down arrow** key to go to the line below.
5. Confirm the account password then press the **Tabular key** and select **OK.**

Figure 46 Entering the new account password



6. A confirmation message will be displayed. Press **Return** to return to the previous menu.

Figure 47 Confirmation message after changing the password



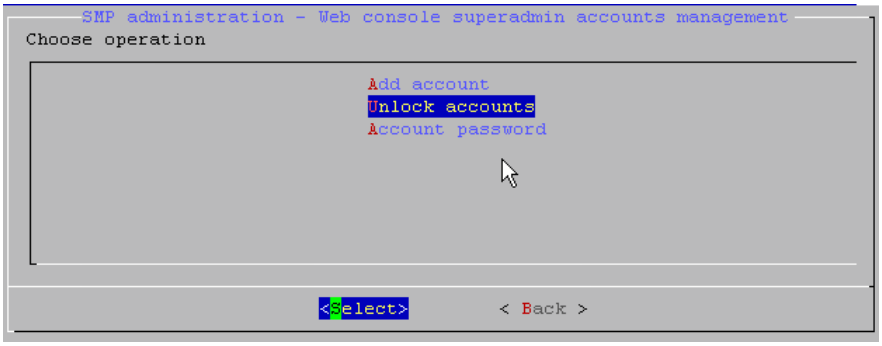
Unlocking the Superadmin Web Console Account

If a user with a **superadmin** account locked his account, e.g. s/he tried to connect to the Web Console with a wrong password, you must unlock it via the **SMPConfig**. The other accounts can be unlocked via the Web Console.

1. To unlock the superadmin account, go to **Main menu ->** SMP **Administration ->Web console superadmin accounts management-> Unlock accounts**

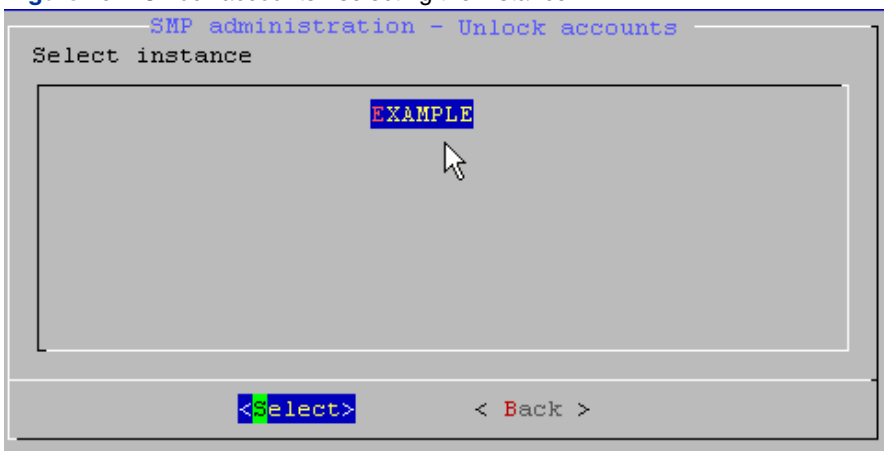
The following screen is displayed.

Figure 48 Unlock accounts



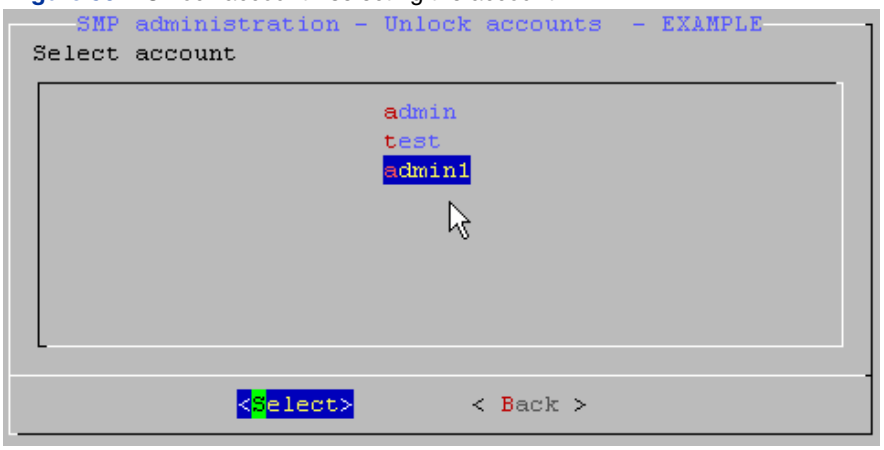
2. Use the **Up** and **Down** arrows to highlight the related instance and then click **Return.**

Figure 49 Unlock accounts - selecting the instance



3. Select the related account and then click **Return.**

Figure 50 Unlock account - selecting the account



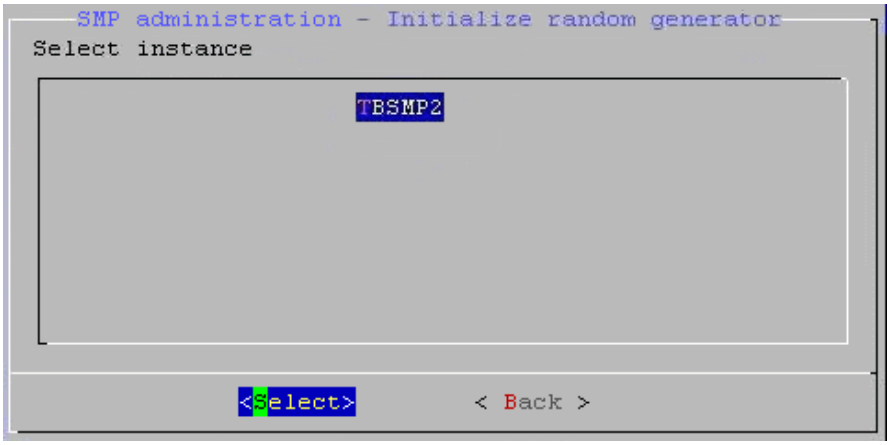
Initializing the Random Generator

The following procedure consists in entering a random character chain in order to generate cryptographically secure keys.

1. To enter a random character chain, go to **Main menu ->** SMP **Administration ->Initialize Random Generator.**

The **Select Instance** screen is displayed.

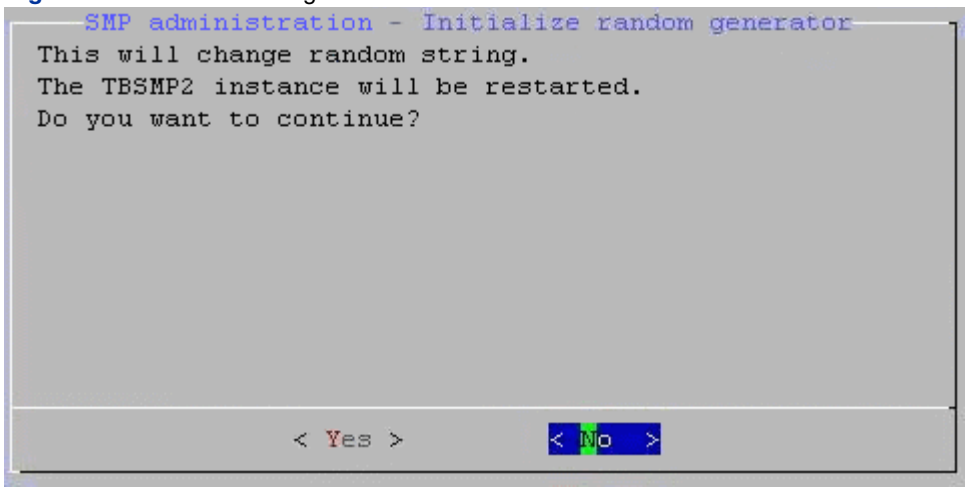
Figure 51 Select the Instance



2. Highlight the required instance name and choose **Select**.

The following message is displayed.

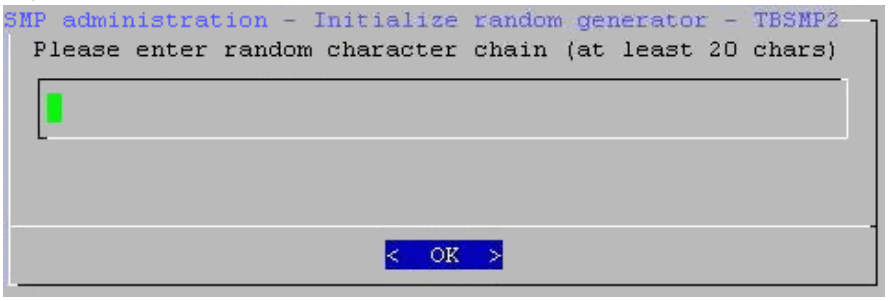
Figure 52 Confirm Message



3. Select **Yes** to accept and continue.

The screen where you must enter the random character chain is displayed.

Figure 53 Enter the Random Character Chain



4. Enter any characters in the field and select **OK**.

The instance restarts.

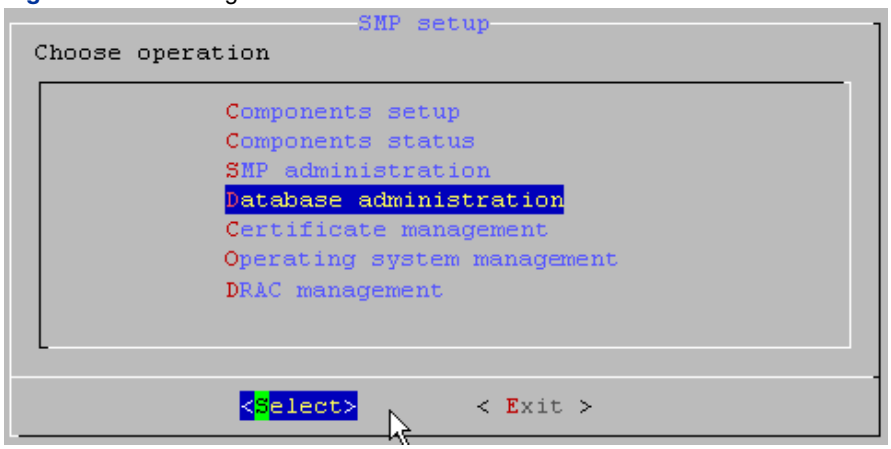
The Database Administration Menu

In this menu section you may execute various actions in order to manage the SMP database.

Opening the Database Administration Menu

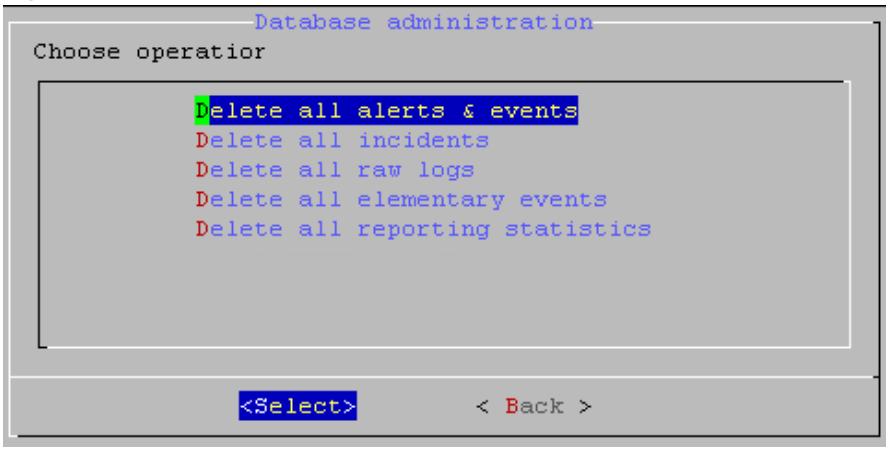
To open the **Database Administration** menu, go to the main menu and select **Database Administration**. (See "Opening the SMPConfig Main Menu" and "Navigating through the Menus").

Figure 54 Selecting the Database Administration menu



The **Database Administration** submenu is displayed.

Figure 55 The Database Administration submenu

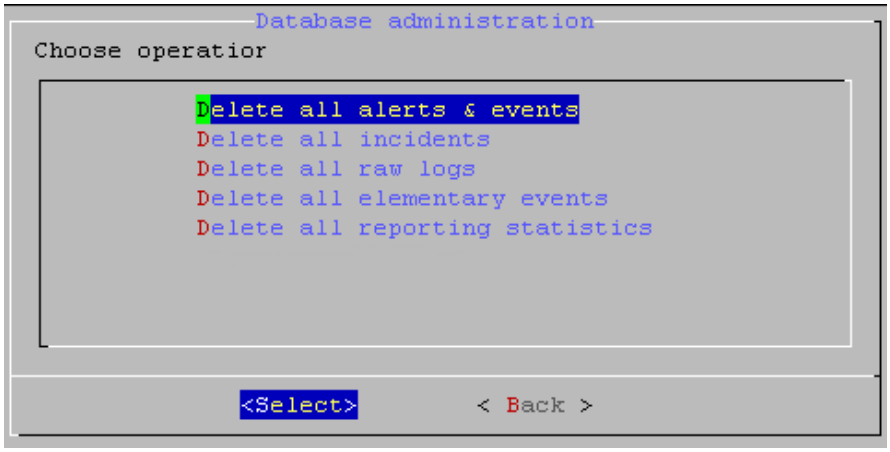


Deleting All Alerts and Events

Note: The related instance will be unavailable while this action is executed.

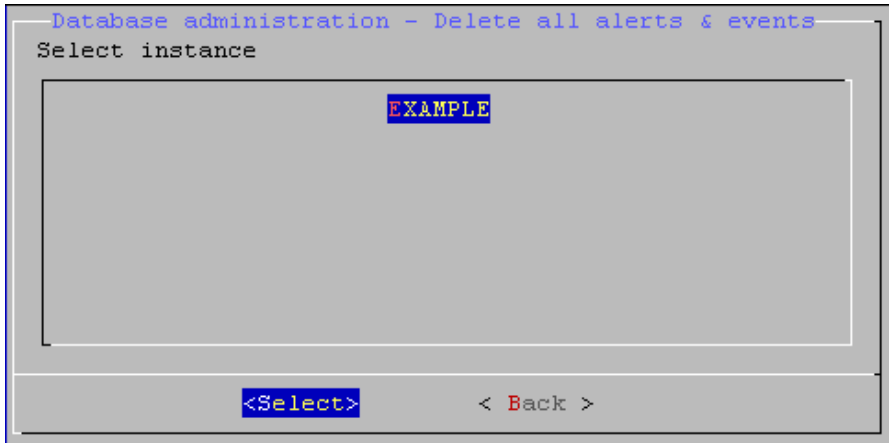
1. Use the **Up** and **Down** arrows to highlight **Delete all alerts & events** and then click **Return**.

Figure 56 Database Administration - Choosing “Delete all alerts & events”



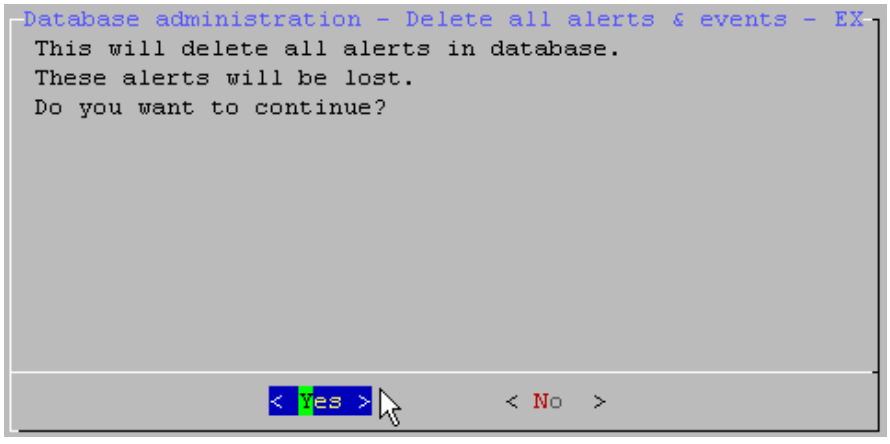
2. Use the **Up** and **Down** arrows to highlight the related instance and then click **Return.**

Figure 57 Database Administration - Selecting the related instance



3. A deletion confirmation message is displayed. Choose **Yes** or **No** and then click **Return.**

Figure 58 Database Administration - Confirming the deletion of alerts

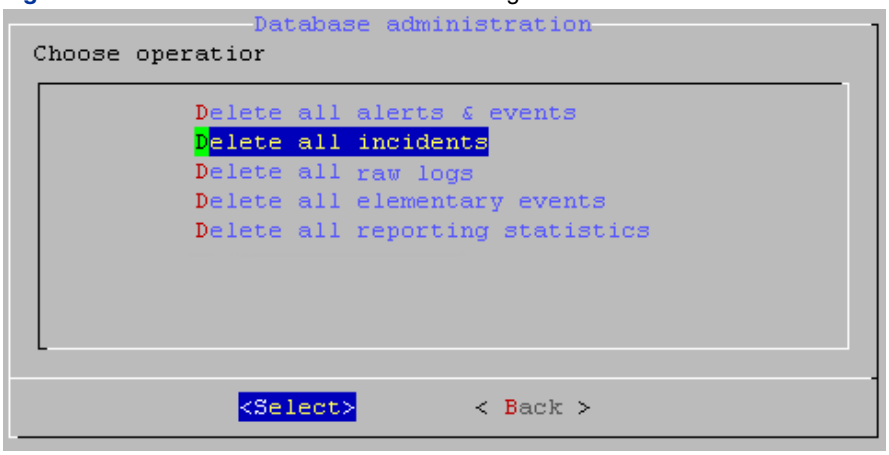


Caution: Approximately 500 to 1000 alerts/events are deleted per second, depending on the type of alerts. Therefore, an average of one million events will be deleted per hour.

Deleting All Incidents

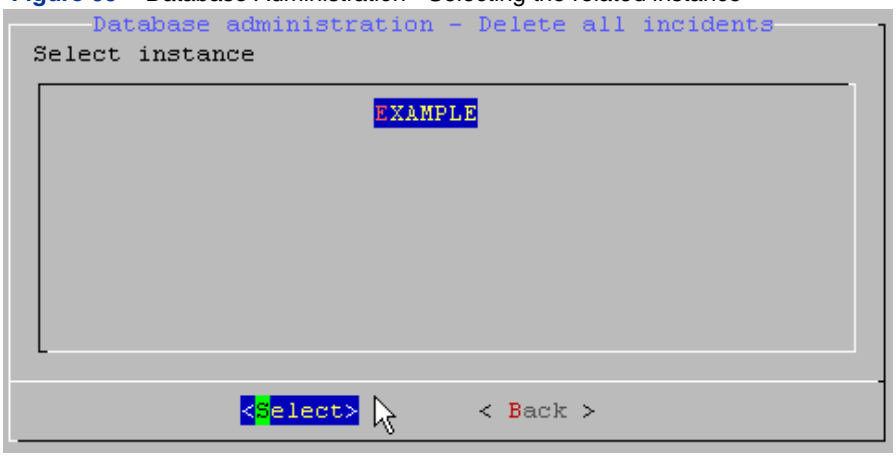
1. Use the **Up** and **Down** arrows to highlight **Delete all incidents** and then click **Return**.

Figure 59 Database Administration - Choosing “Delete all incidents”



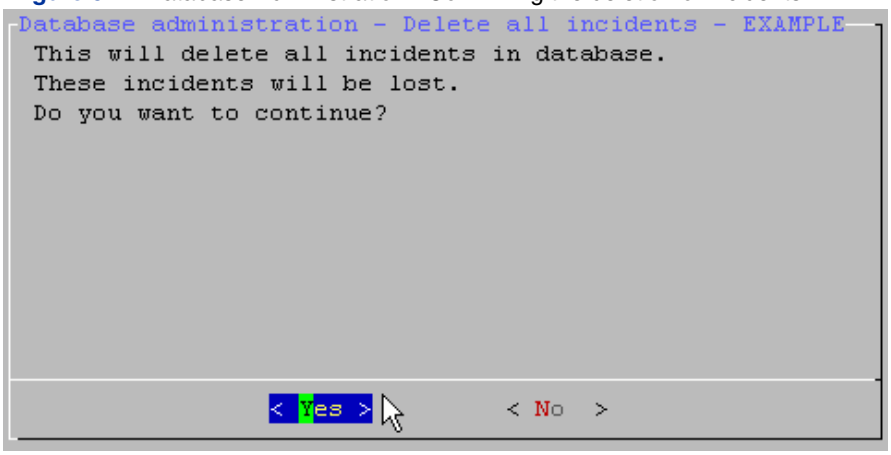
2. Use the **Up** and **Down** arrows to highlight the related instance and then click **Return.**

Figure 60 Database Administration - Selecting the related instance



3. A deletion confirmation message is displayed. Choose **Yes** or **No** and then click **Return.**

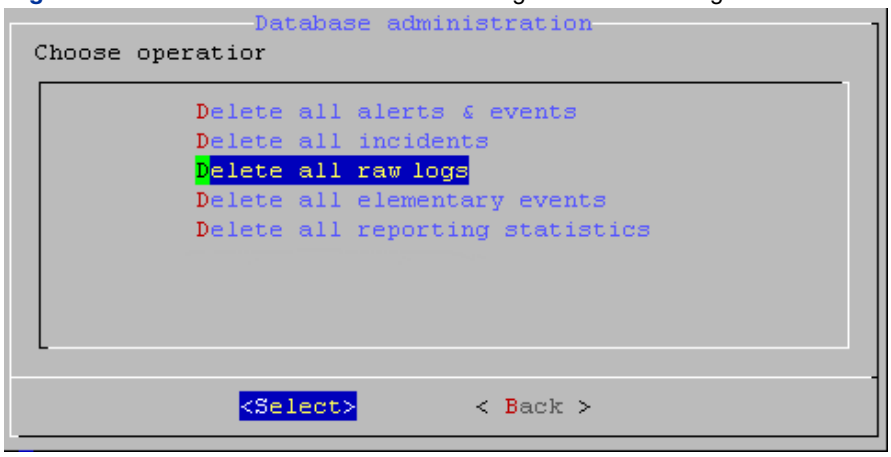
Figure 61 Database Administration - Confirming the deletion of incidents



Deleting All Raw Logs

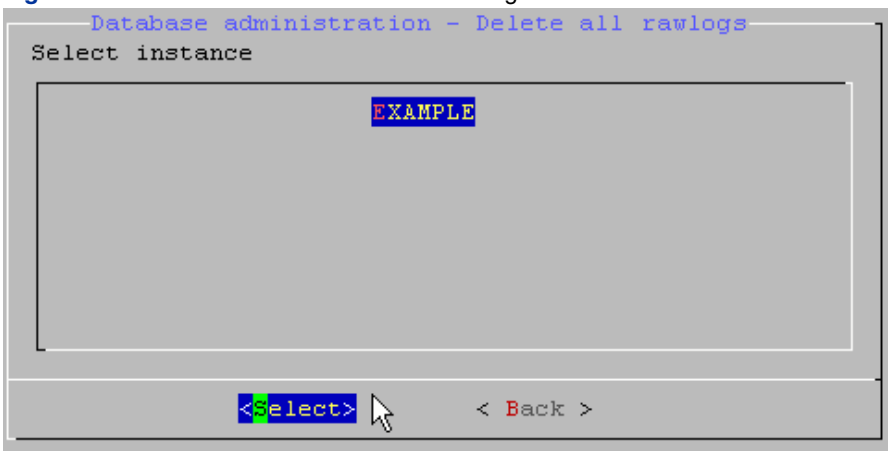
1. Use the **Up** and **Down** arrows to highlight **Delete all raw logs** and then click **Return**.

Figure 62 Database Administration - Choosing “Delete all raw logs”



2. Use the **Up** and **Down** arrows to highlight the related instance and then click **Return.**

Figure 63 Database Administration - Selecting the related instance



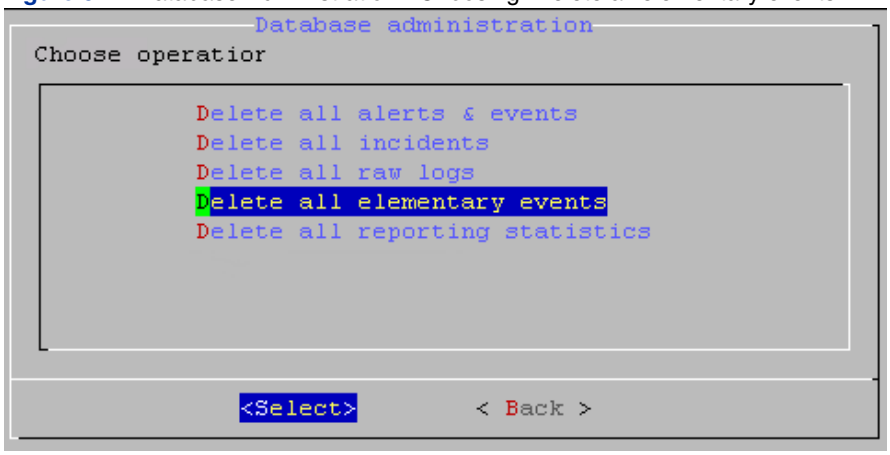
3. A deletion confirmation message is displayed. Choose **Yes** or **No** and then click **Return.**

Note: When deleting all raw logs, current processes will be stopped (runtime and report) and then automatically restarted.

Deleting All Elementary Events

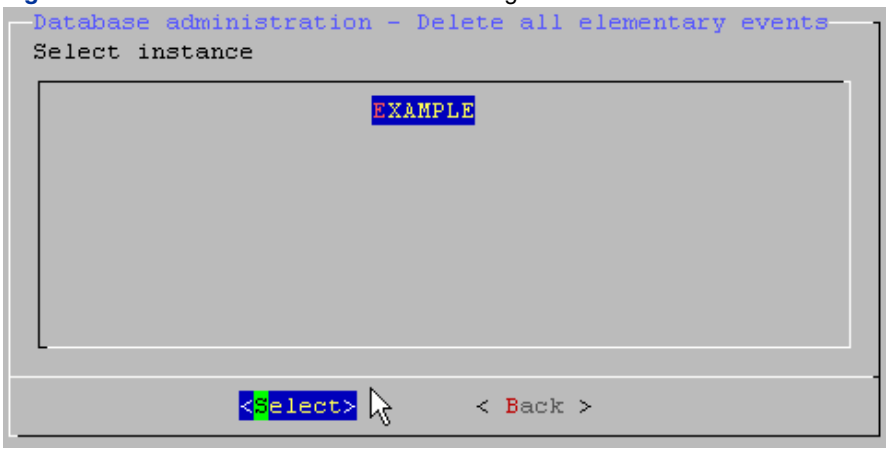
1. Use the **Up** and **Down** arrows to highlight **Delete all elementary events** and then click **Return**.

Figure 64 Database Administration - Choosing “Delete all elementary events”



2. Use the **Up** and **Down** arrows to highlight the related instance and then click **Return.**

Figure 65 Database Administration - Selecting the related instance

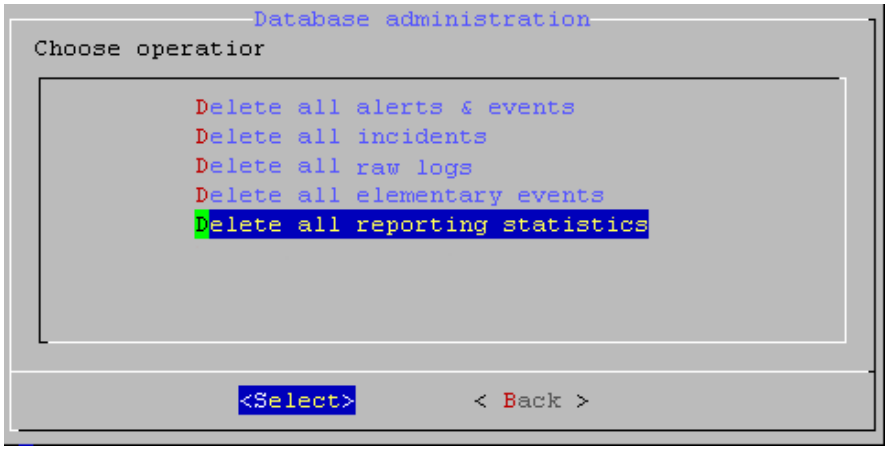


3. A deletion confirmation message is displayed. Choose **Yes** or **No** and then click **Return.**

Deleting All Reporting Statistics

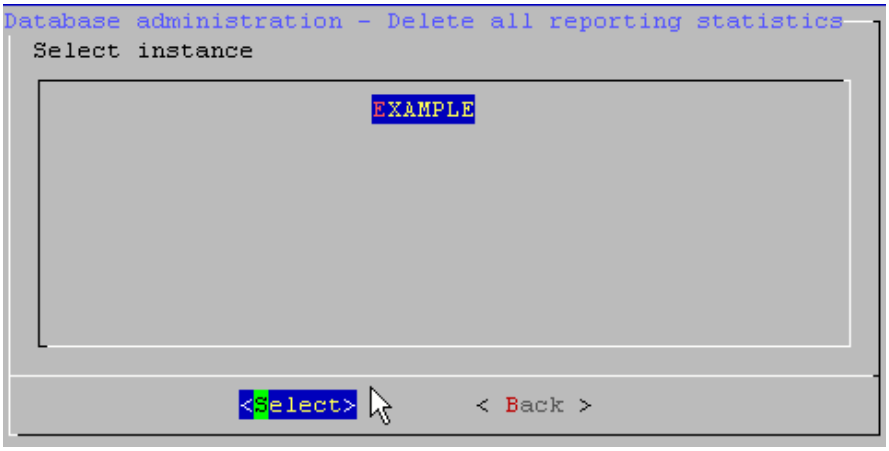
1. Use the **Up** and **Down** arrows to highlight **Delete all reporting statistics** and then click **Return**.

Figure 66 Database Administration - Choosing “Delete all reporting statistics”



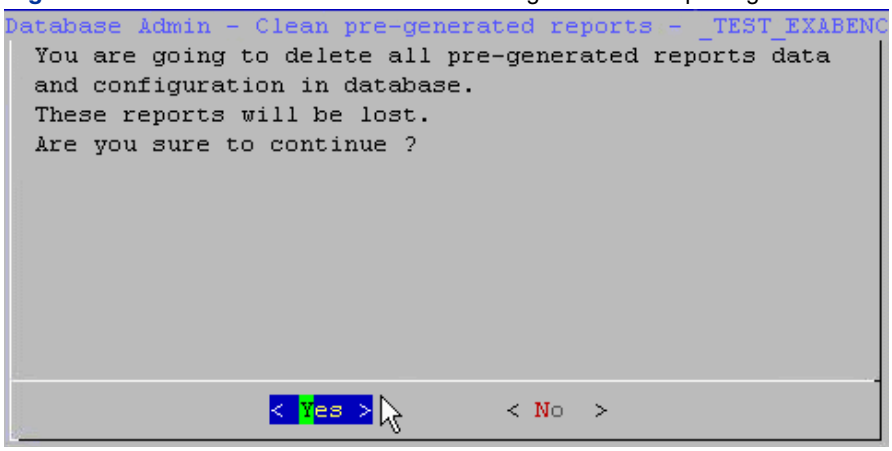
2. Use the **Up** and **Down** arrows to highlight the related instance and then click **Return.**

Figure 67 Database Administration - Selecting the related instance



3. A deletion confirmation message is displayed. Choose **Yes** or **No** and then click **Return.**

Figure 68 Database Administration - Confirming deletion of reporting statistics data



Managing the Web Console Certificate

A certificate is needed for the user to access the Web Console with confidence.

The objective is to include the Web Console certificate that will be generated in the company's Public Key Infrastructure (PKI).

By default, the certificate which allows access to the Web Console is a self-signed certificate.

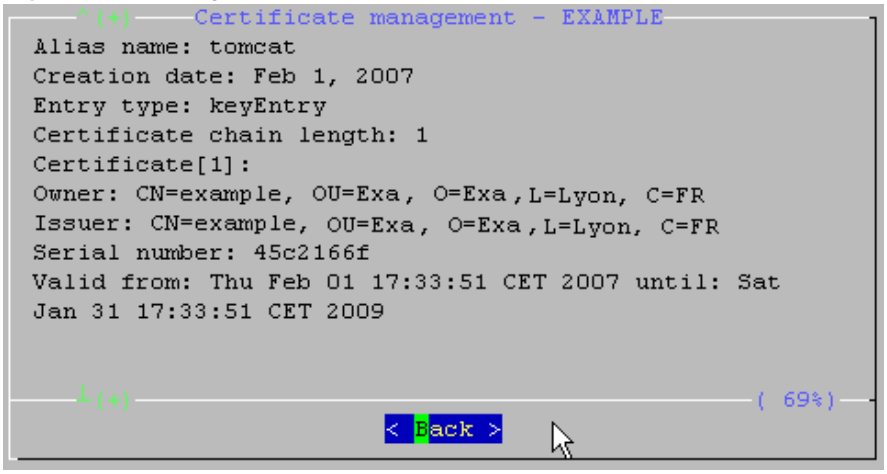
In order for other sources to trust your self-signed certificate, the latter should be certified by a Certificate Authority (CA). Examples of Certificate Authorities are Verisign, Entrust, Thawte Consulting, and BelSign. A Certificate Authority will verify the subject's identity, (usually in an off-line, manual process) and will sign the subject's public self-signed certificate, if successful.

Next, you will need to sign the certificate, and then import the certificate reply through the « Import certificate reply » menu option.

Prerequisites

Check that the certificate is correct by displaying the certificate information via **Certificate Management > Display Certificate**.

Figure 69 Viewing the certificate information



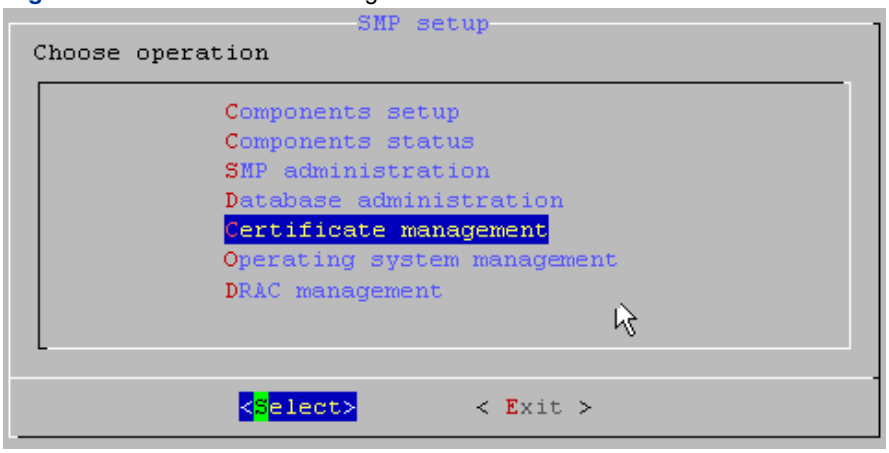
Note: If the number of lines containing the certificate information exceeds the screen size, you may scroll the screen using the **Up** and **Down** arrows. The percentage value of how much text is being displayed will be shown on the bottom right corner of the screen (in blue text).

If the certificate is not correct, you must create it again.

Creating a New Certificate

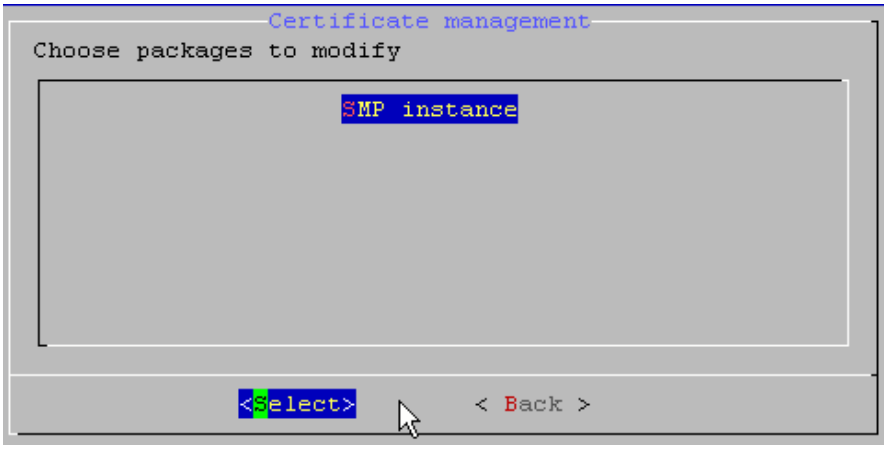
1. Go to the main menu and select **Certificate Management**. (See "Opening the SMPConfig Main Menu" and "Navigating through the Menus").

Figure 70 The Certificate Management menu



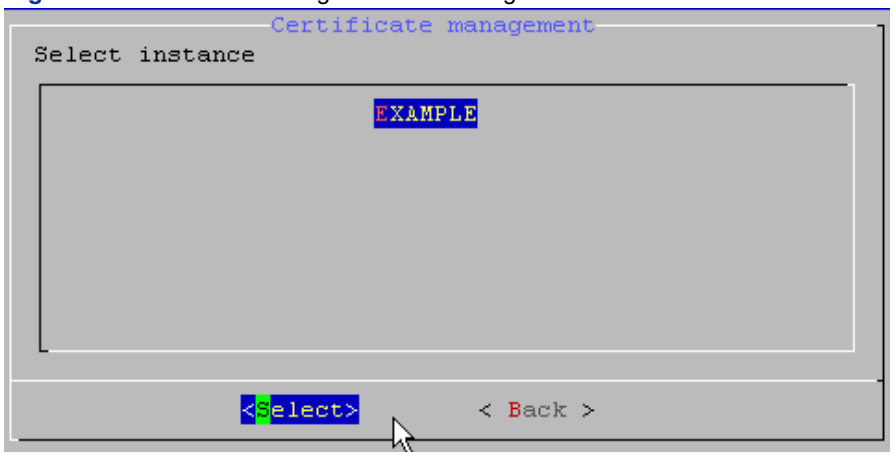
2. Use the **Up** and **Down** arrows to highlight the package to modify and then click **Return.**

Figure 71 Certificate Management - Choosing the package to modify



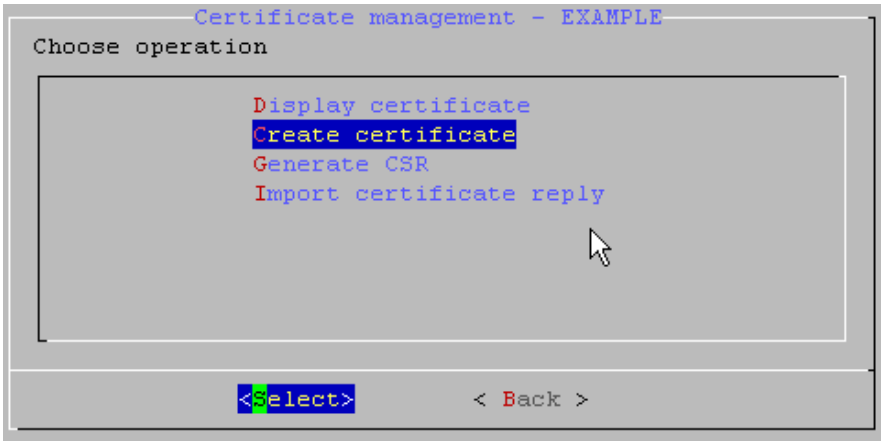
3. Use the **Up** and **Down** arrows to highlight the related instance and then click **Return.**

Figure 72 Certificate Management - Selecting the related instance



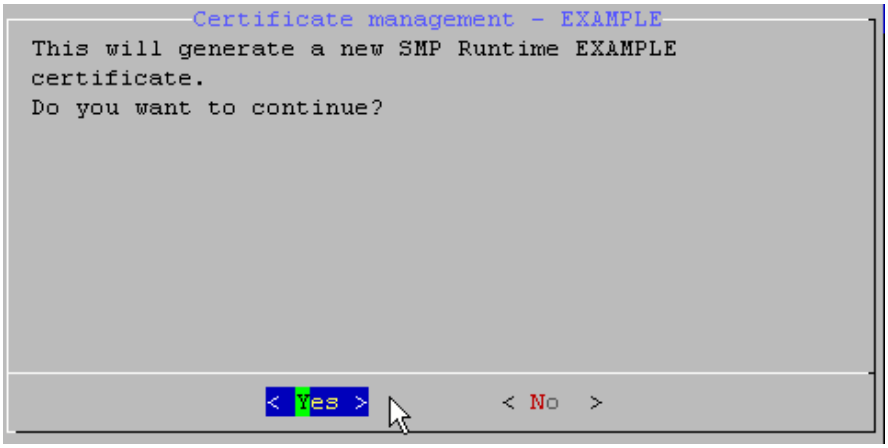
4. Use the **Up** and **Down** arrows to highlight **Create certificate** and then click **Return**.

Figure 73 Choosing “Create certificate”



5. A confirmation message will be displayed. Choose **Yes** or **No** and then click **Return**.

Figure 74 Creating a certificate - confirmation message



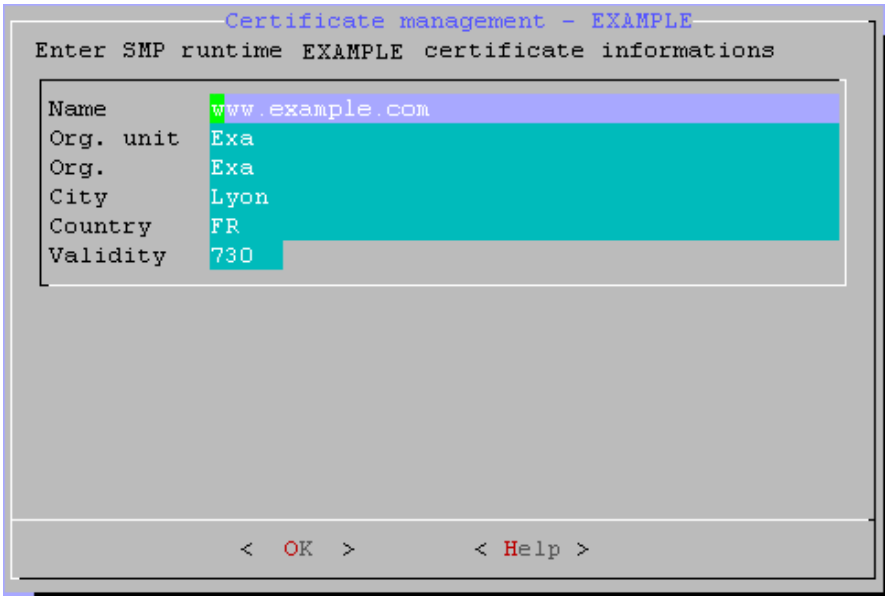
6. Next, the SMP services will be stopped by the system.

7. Enter the new certificate's information such as:

- server (FQDN) name
- the organization's name
- the organization unit
- the city
- the country code (only 2 letters. E.g. FR)
- The validity period in days

Then click **Return.**

Figure 75 Certificate Management



The SMP services will be restarted.

8. After finishing creating the certificate, the system will automatically display the Certificate Management submenu. To view your new certificate, click on **Display certificate** (See Figure 69 "Viewing the certificate information").

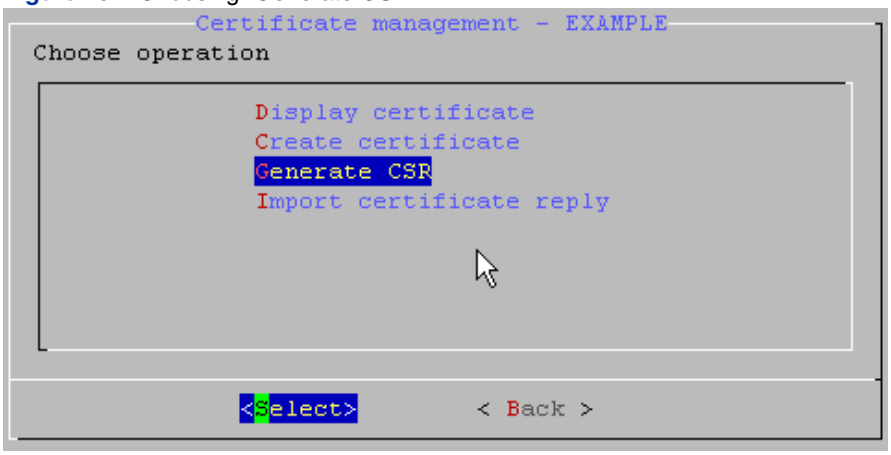
Including the Certificate in the PKI

You must include the certificate in the company's PKI. Indeed, to have a certificate signed by a Certification Authority (CA), you will need to first request it with a CSR (Certificate Signing Request).

Generating a CSR

1. Go to the **Certificate Management** submenu.
2. Select your instance and click **Return**.
3. Use the **Up** and **Down** arrows to highlight **Generate CSR** and then click **Return**.

Figure 76 Choosing "Generate CSR"



4. A confirmation message will be displayed showing the directory path to the folder where the new CSR was saved to.
5. Click **OK** to return to the **Certificate Management** submenu.

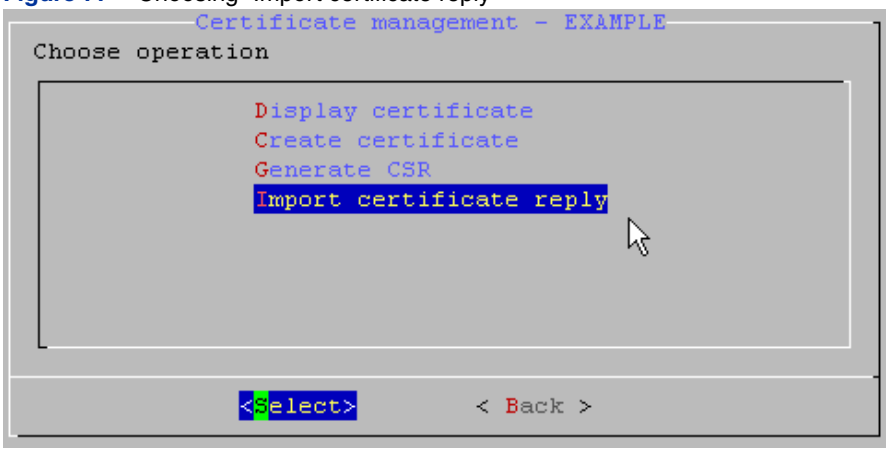
Once generated, the **CSR** is sent to the **Certificate Authority** so that a signed certificate reply can be generated in ***.der** format.

A `tomcat.csr` file is generated in `var/lib/exaprotect/tmp/`

Importing a Certificate Reply

1. Go to the **Certificate Management** submenu.
2. Use the **Up** and **Down** arrows to highlight **Import certificate reply** and then click **Return.**

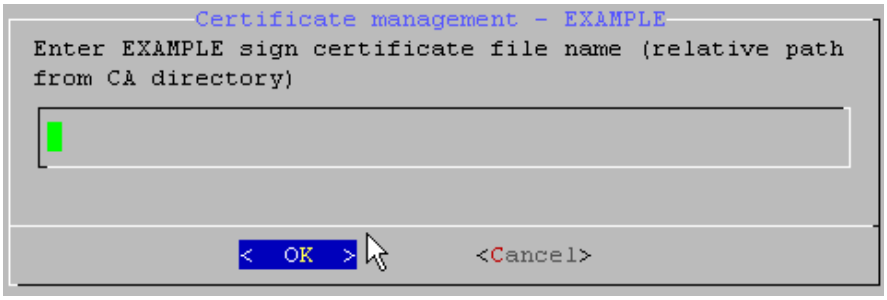
Figure 77 Choosing "Import certificate reply"



3. Put the ***.der** reply certificate in `/home/exaprotect/tmp/ca`.

4. Enter the filename. Only the filename is required, do not enter the directory path, e.g. `tomcat.der`

Figure 78 Importing a certificate reply - entering the filename



5. After entering the filename, press **Enter.**

6. The SMP services will be restarted.

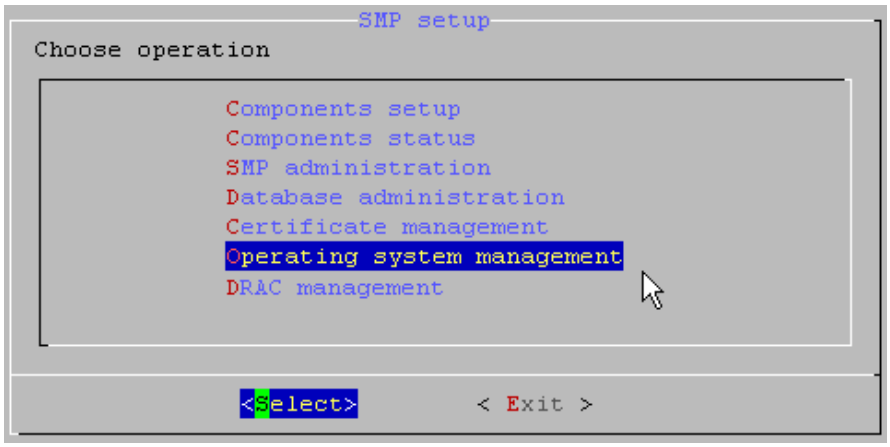
The Operating System Management Menu

In this menu section you may configure several operating system parameters.

Opening the Operating System Management Menu

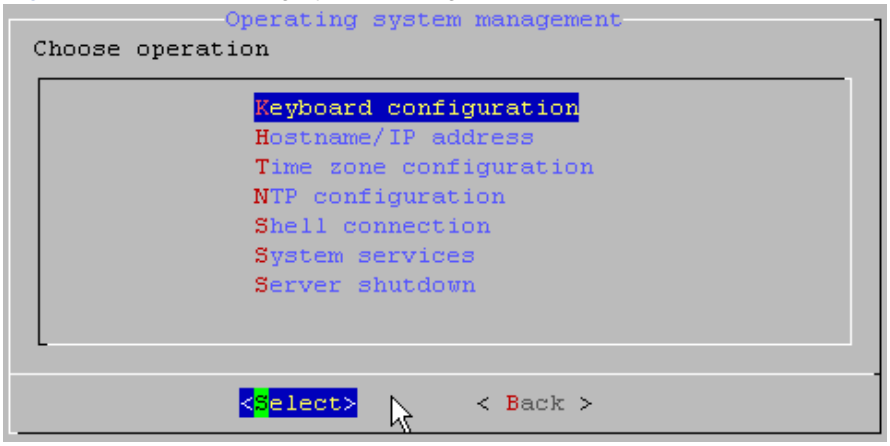
To open the **Operating System Management** menu, go to the main menu and select **Operating System Management**. (See "Opening the SMPConfig Main Menu" and "Navigating through the Menus").

Figure 79 The Operating System Management menu



The Operating System Management submenu is displayed.

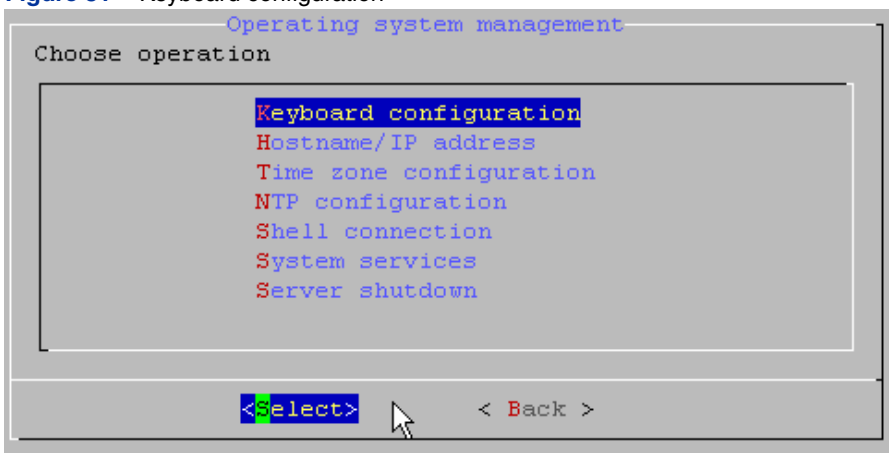
Figure 80 The Operating System Management submenu



Altering the Keyboard Configuration

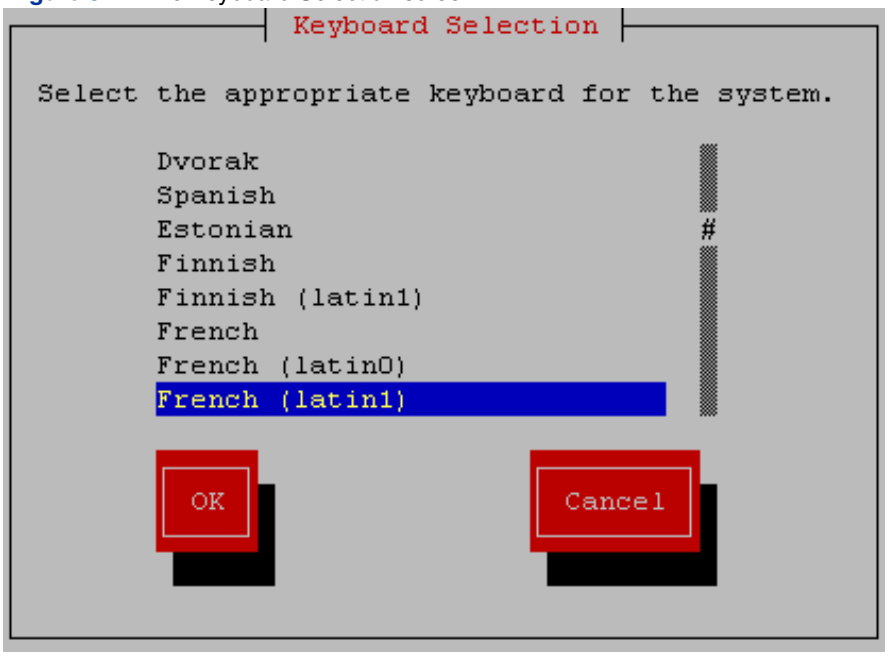
1. In the Operating System Management submenu, use the **Up** and **Down** arrows to highlight **Keyboard configuration** and then click **Return**.(See "Opening the Operating System Management Menu").

Figure 81 Keyboard configuration



2. Use the **Up** and **Down** arrows to highlight the desired language option. Use the **Right** and **Left** arrows to select **OK** and then click **Return.**

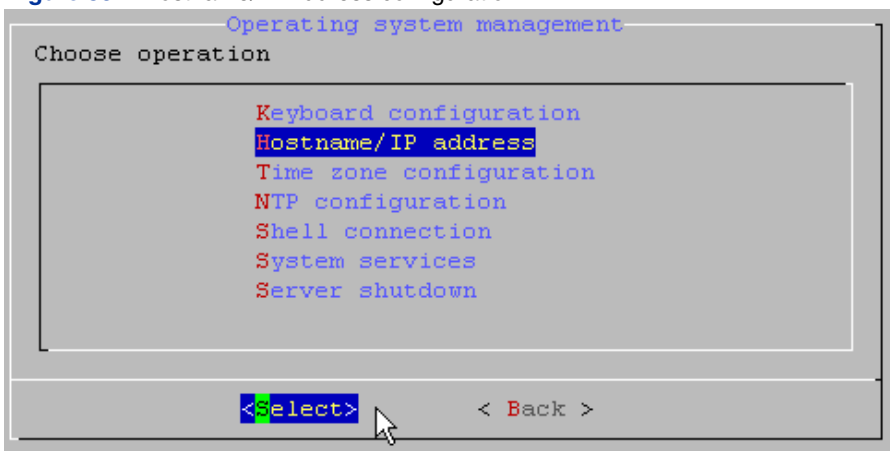
Figure 82 The Keyboard Selection screen



Altering the Hostname/IP Address

1. In the **Operating System Management** submenu, use the **Up** and **Down** arrows to highlight **Hostname/IP Address** and then click **Return** (See "Opening the Operating System Management Menu").

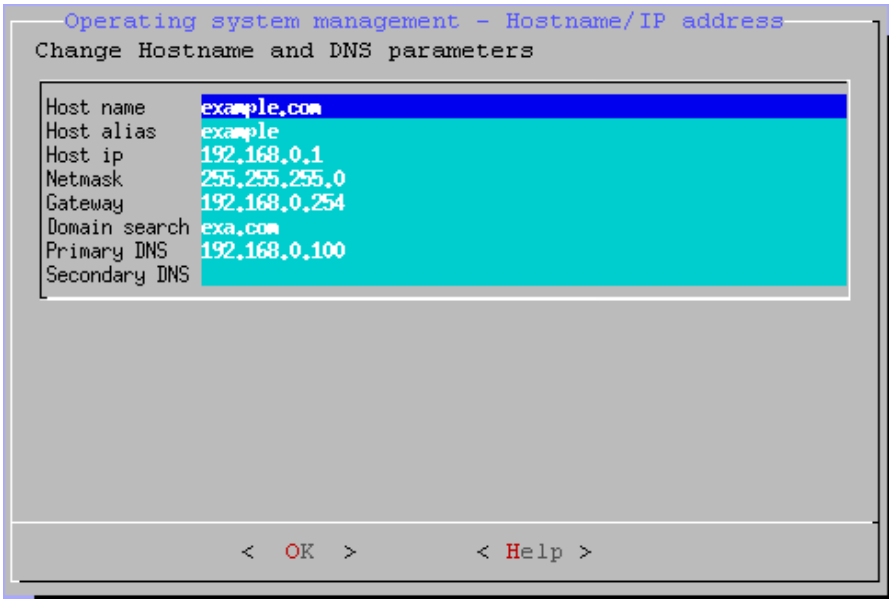
Figure 83 Hostname/IP Address configuration



2. Using the Down arrow key to navigate around the window, enter the **name**, **alias** and **IP configuration** for the host, **Netmask**, **Default gateway**, **Domain Search** and **Primary and Secondary nameserver** details for your SMP.

Note: For advice on the choice of an IP address for the appliance, contact your network administrator.

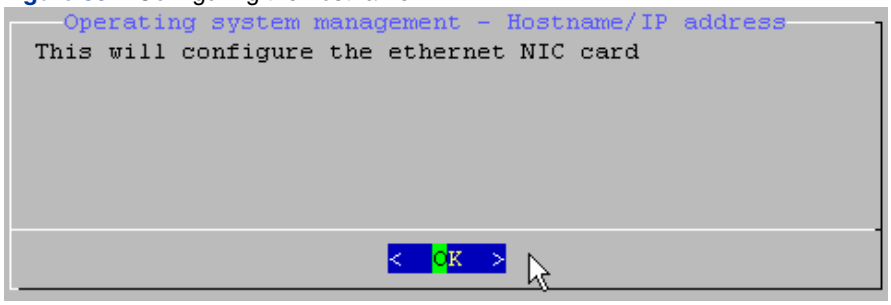
Figure 84 Entering the hostname



3. Press the Tab key until **OK** is highlighted, and then press Enter.

4. A confirmation message is displayed. press Enter.

Figure 85 Configuring the hostname



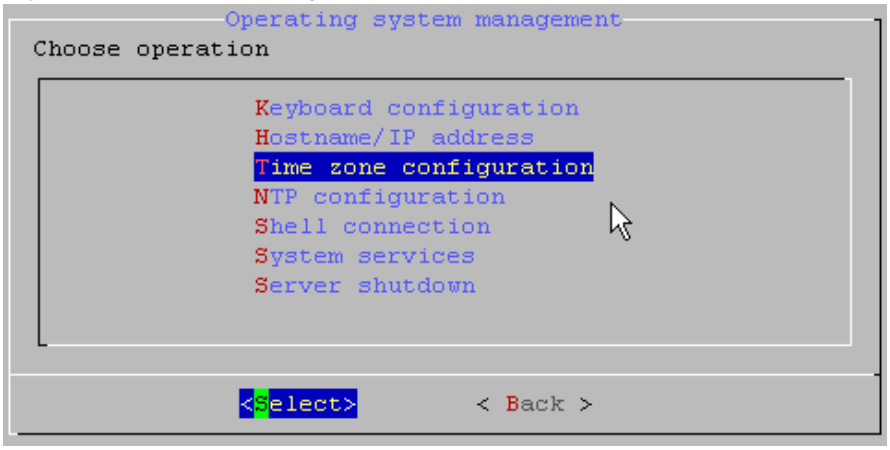
5. A message stating “Starting network services” will be momentarily displayed.

Note: If you are in Log Collector > Server communication mode, the local Log Collector will not work after the server’s hostname/IP address modification.

Time Zone Configuration

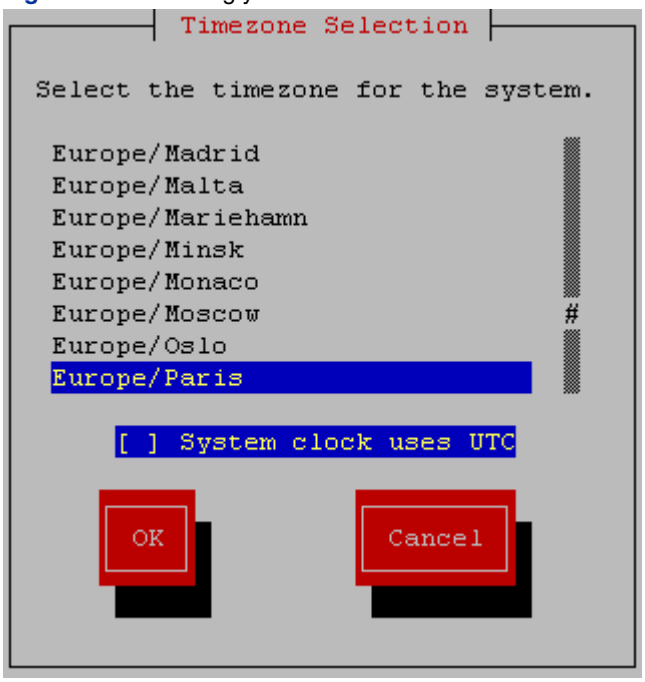
1. In the **Operating System Management** submenu, use the **Up** and **Down** arrows to highlight **Time Zone Configuration** and then click **Return.** (See "Opening the Operating System Management Menu").

Figure 86 Time zone configuration



2. Use the **Up** and **Down** arrows to select your time zone and then click **Return.**

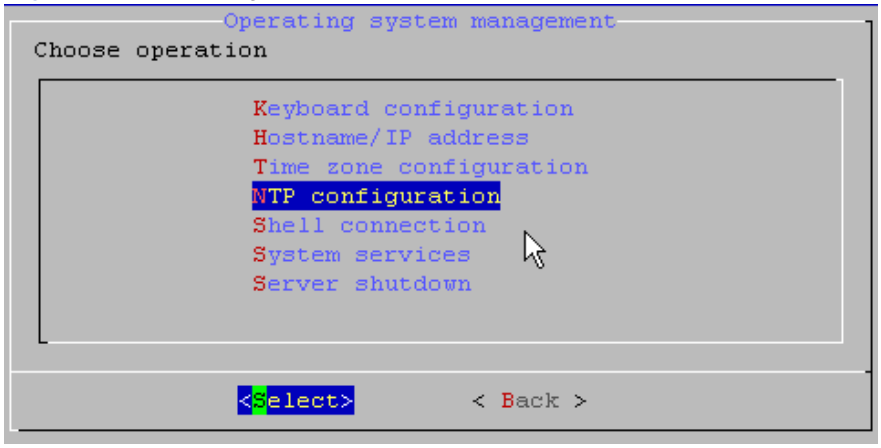
Figure 87 Selecting your time zone



NTP Configuration

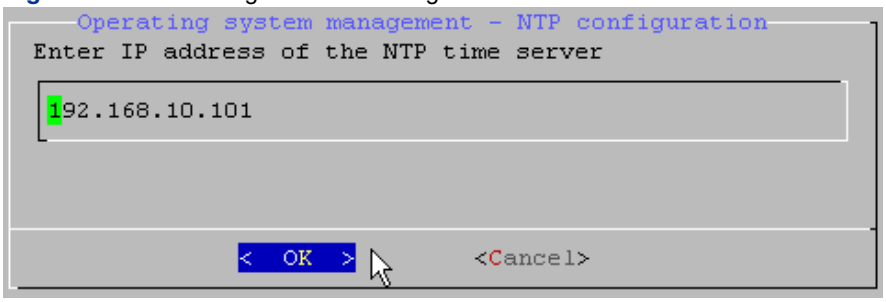
1. In the **Operating System Management** submenu, use the **Up** and **Down** arrows to highlight **NTP Configuration** and then click **Return** (See "Opening the Operating System Management Menu").

Figure 88 NTP configuration



2. Enter the IP address of your Network Time Protocol (NTP) Server, and then press Enter. Please contact your network administrator to obtain details regarding the NTP Server.

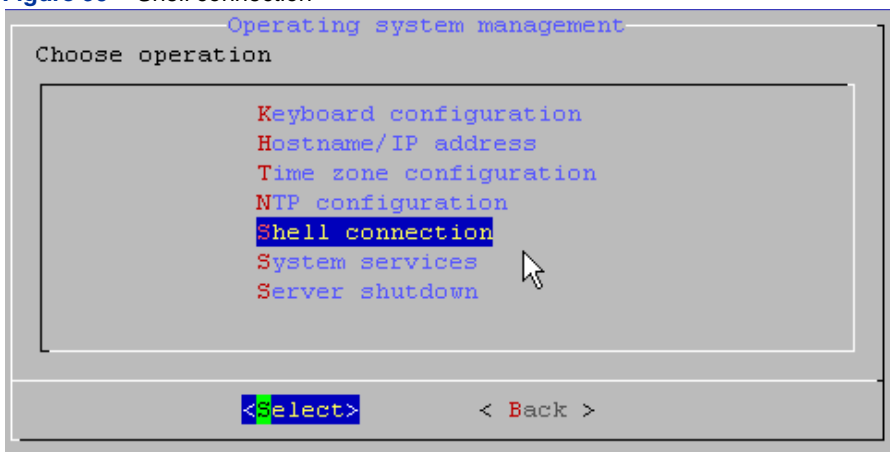
Figure 89 NTP configuration - entering the NTP time server IP address



Shell Connection

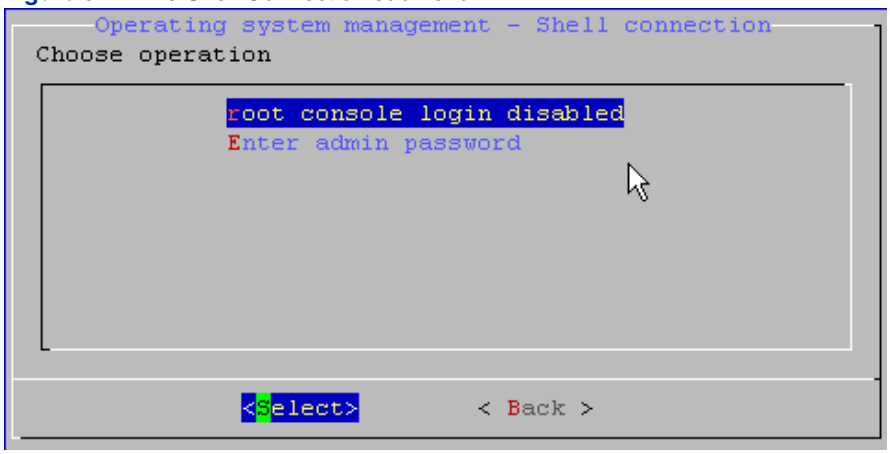
1. In the **Operating System Management** submenu, use the **Up** and **Down** arrows to highlight **Shell Connection** and then click **Return**. (See "Opening the Operating System Management Menu").

Figure 90 Shell connection



2. The **Shell Connection** submenu is displayed.

Figure 91 The Shell Connection submenu



Altering the State of the root console login

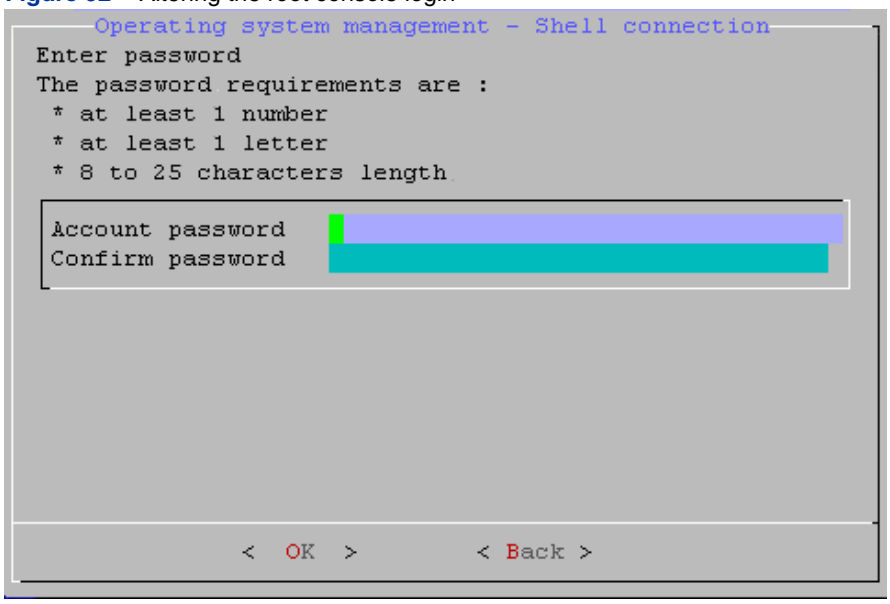
- This option enables or disables the local "root" system account connections on the SMP server.
- This operation authorizes only a local access to the server (through the console); it does not permit a remote access.
- Once you have enabled the "root" account, you will need to create a related password.

Note: Default state for this parameter: disabled.

ENABLING THE ROOT CONSOLE LOGIN

1. In the **Shell Connection** window, select **root console login disabled** and click **Return**.
2. Enter the new password, re-enter it and then click **Return**.

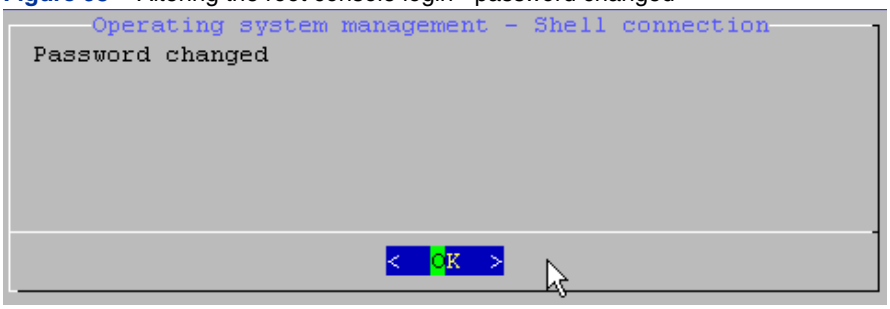
Figure 92 Altering the root console login



Note: You must enter a password at least 8 characters long with at least one number and one letter.

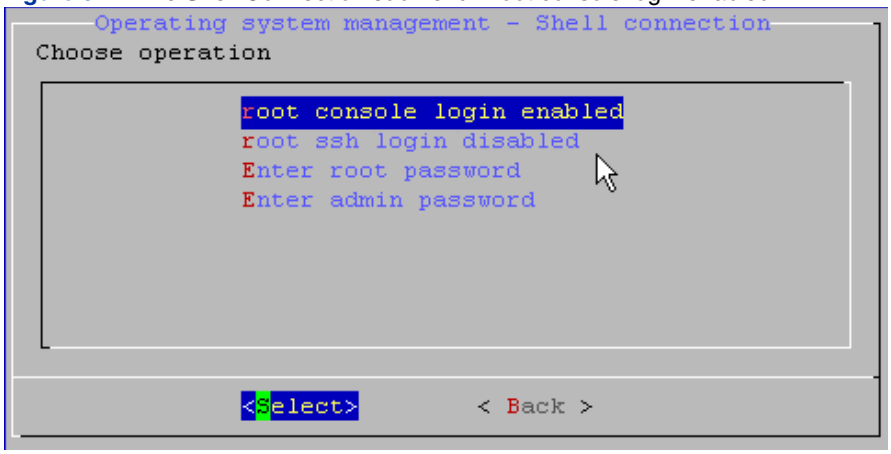
3. A confirmation message will be displayed. Click **Return** to continue.

Figure 93 Altering the root console login - password changed



The **root console login is enabled**.

Figure 94 The Shell Connection submenu - root console login enabled



DISABLING THE ROOT CONSOLE LOGIN

1. Select **root console login enabled.**

2. press Enter.

Altering the State of the root ssh login

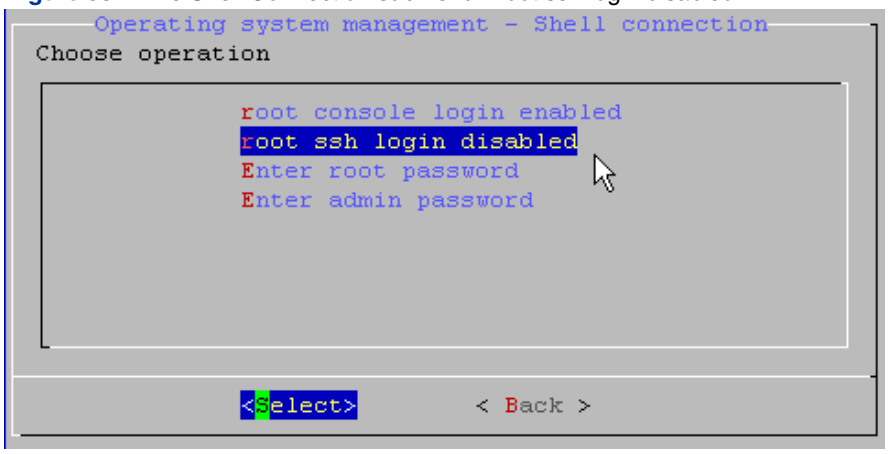
ENABLING THE ROOT SSH LOGIN

This option enables or disables the remote “root” system account connections (through SSH).

> **Note:** In order to activate this option, you will need to first authorize the local “root” connections. See "Altering the State of the root console login".
> Default state for this parameter: disabled.

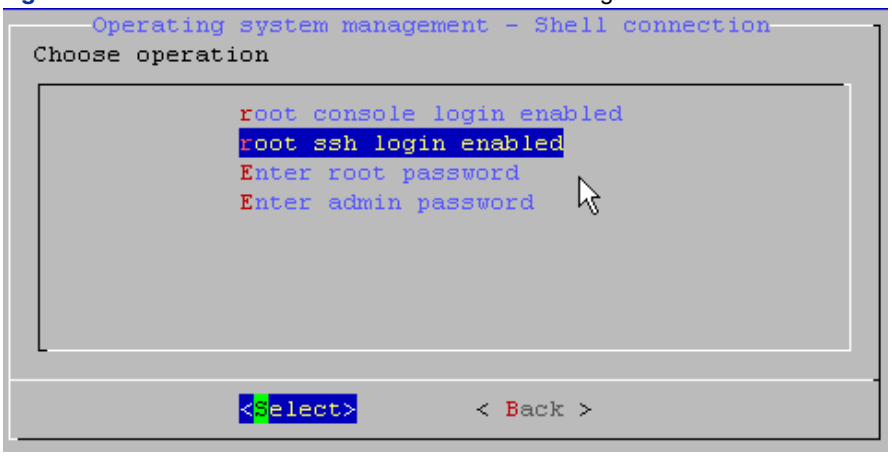
1. To alter the state of the root ssh login, use the **Up** and **Down** arrows to highlight **root ssh login disabled** and then click **Return**.

Figure 95 The Shell Connection submenu - root ssh login disabled



The root ssh login is now enabled

Figure 96 The Shell Connection submenu - root ssh login enabled



DISABLING THE ROOT SSH LOGIN

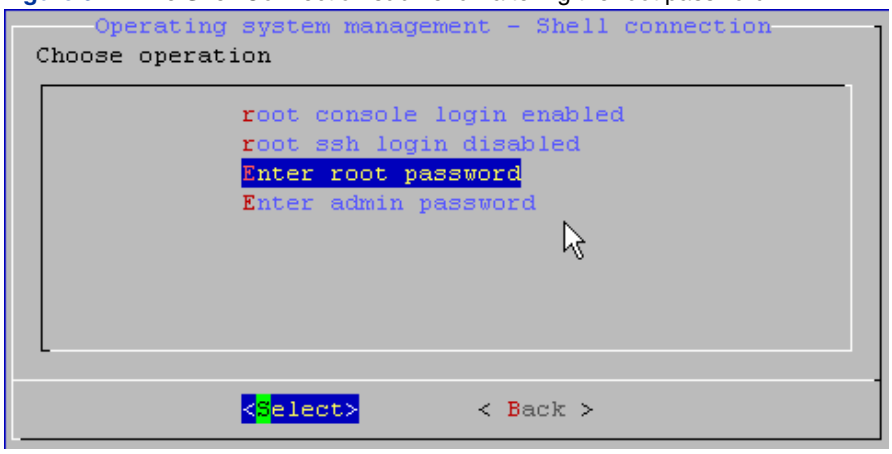
1. Select **root ssh login enabled.**
2. press Enter.

Entering the root Password

> **Note:** In order to enter the root password, you will need to first authorize the local “root” connections. See "Altering the State of the root console login".

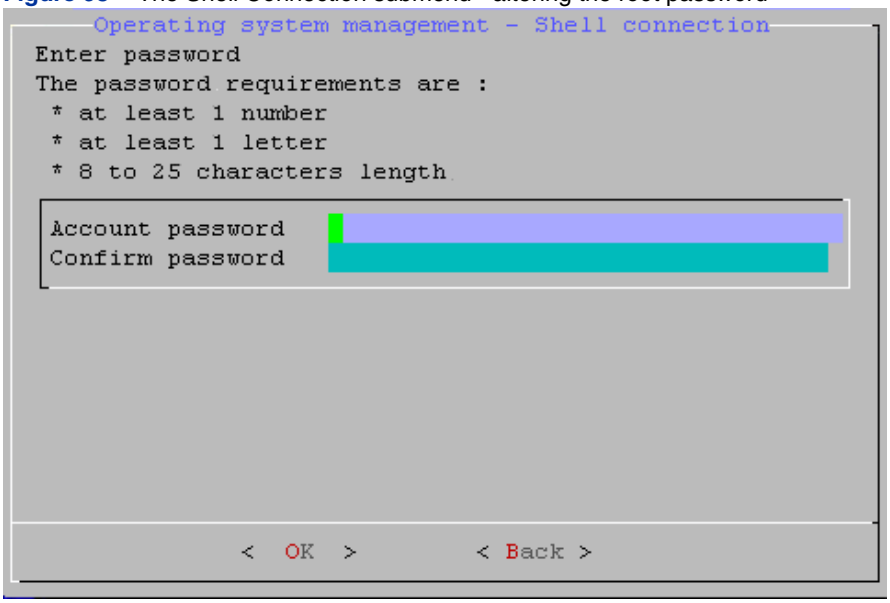
1. To change the root password, use the **Up** and **Down** arrows to highlight **Enter root password** and then click **Return**.

Figure 97 The Shell Connection submenu - altering the root password



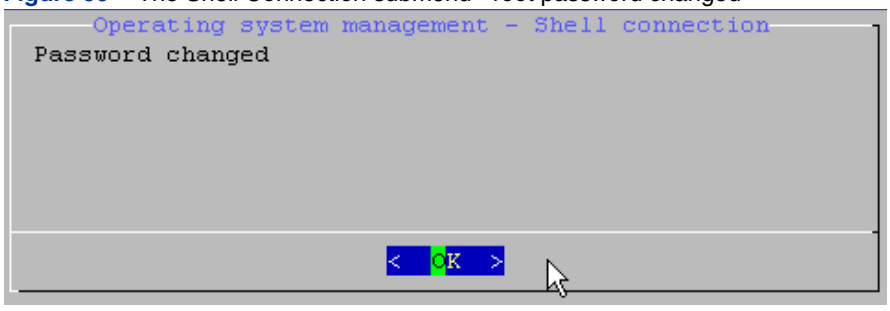
2. Enter the new password, re-enter it and then click **Return**.

Figure 98 The Shell Connection submenu - altering the root password



3. A confirmation message will be displayed. Click **Return** to continue.

Figure 99 The Shell Connection submenu - root password changed

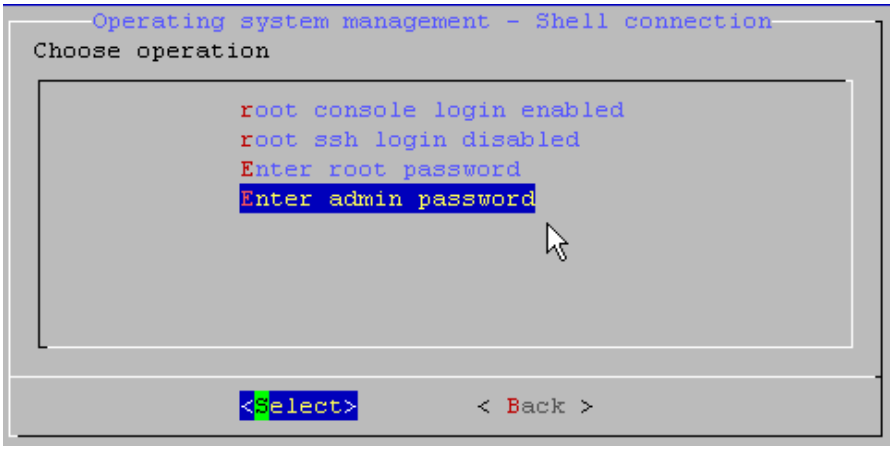


You must enter a password at least 8 characters long with at least one number and one letter.

Entering the admin Password

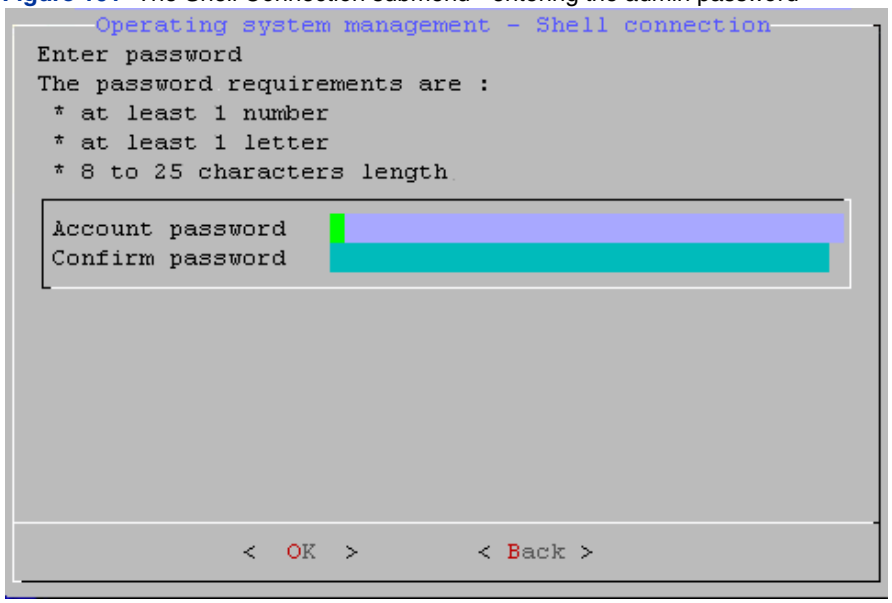
1. To change the `admin` password, use the **Up** and **Down** arrows to highlight **Enter admin password** and then click **Return**.

Figure 100 The Shell Connection submenu - altering the admin password



2. Enter the new password and then click **Return**.

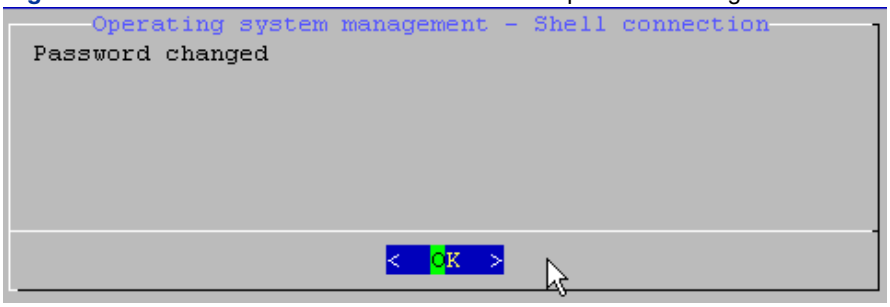
Figure 101 The Shell Connection submenu - entering the admin password



Note: It is advisable to enter a password at least 8 characters long, and to include at least one number and one letter.

3. A confirmation message is displayed. Click **Return** to continue.

Figure 102 The Shell Connection submenu - admin password changed



The System Services Submenu

In this menu section you may configure several server and firewall parameters.

Opening the System Services Management Submenu

To open the **System Services** submenu, go to **Main menu -> Operating System Management -> System Services**. (See "Opening the SMPConfig Main Menu" and "Navigating through the Menus").

Figure 103 The System Services submenu

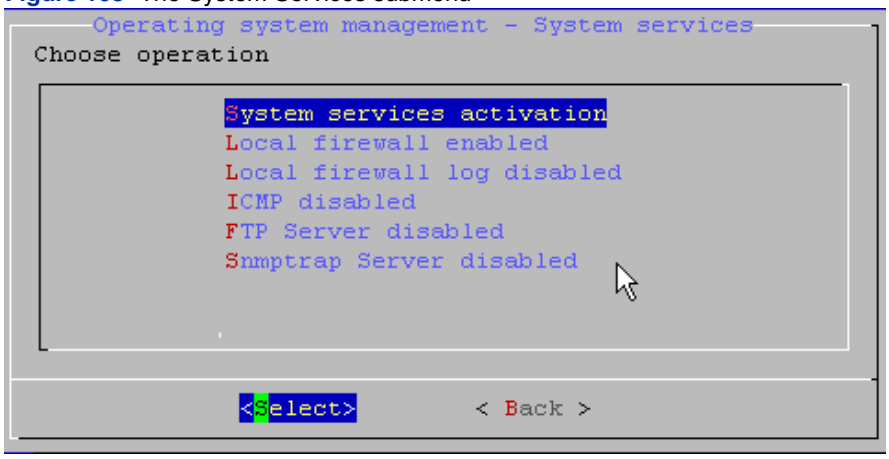


Table 2 The System Services menu options

System services activation	Allows you to manage the services that are launched when the SMP server is booted up. It is not recommended to change these parameters unless you have advanced expertise.
Local firewall enabled/disabled	Allows you to enable or disable the SMP server firewall. It is recommended that the firewall option be always enabled. Default state: firewall enabled.
Local firewall log enabled/ disabled	Enabled - allows the logging of the firewall activity information, which may be viewed in the Web Console console. By default, the Log Collector is configured to collect the firewall logs. Default state: disabled.

Table 2 The System Services menu options

ICMP enabled/disabled	Enabled - allows ICMP requests (“ping”) to the SMP server. Default state: disabled.
FTP Server enabled/disabled	Enabled - allows the FTP streams to the SMP server. This will also activate the VSFTP component in the server. Default state: disabled.
Snmptrap enabled/disabled	Enabled - allows the SNMP streams to the SMP server. This will also activate the SNMP component in the server. Default state: disabled.

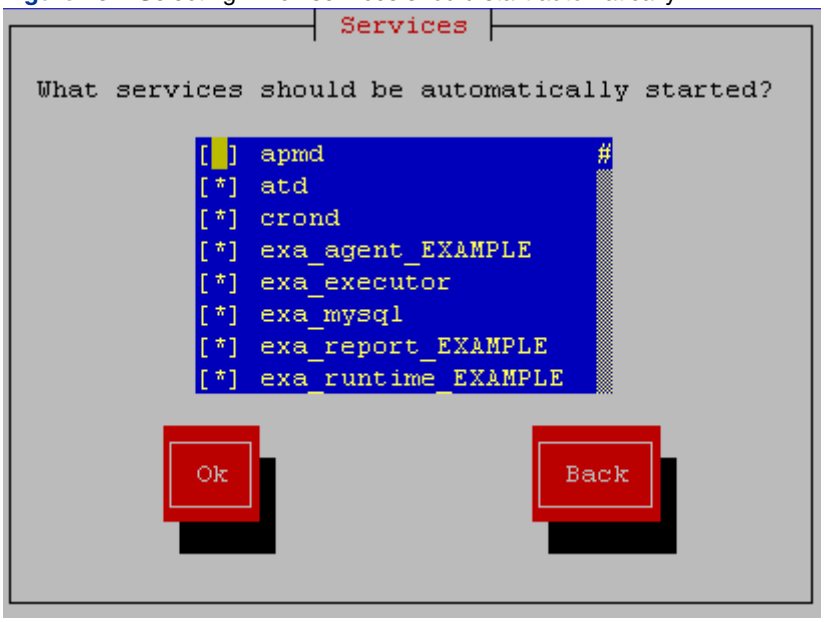
Selecting Which Services Should Start Automatically

1. To select which services should automatically start, go to **Main menu -> Operating System Management -> System Services-> System Services Activation**. (See "Opening the SMPConfig Main Menu" and "Navigating through the Menus").

2. Use the **Up, Down**, and **Tab** keys to navigate around the window. Use the **Space** key to select which services should start automatically. To view more information regarding a particular service, highlight the service and press **F1**.

3. When finished making your changes, press the Tab key until **OK** is highlighted, and then press Enter.

Figure 104 Selecting which services should start automatically

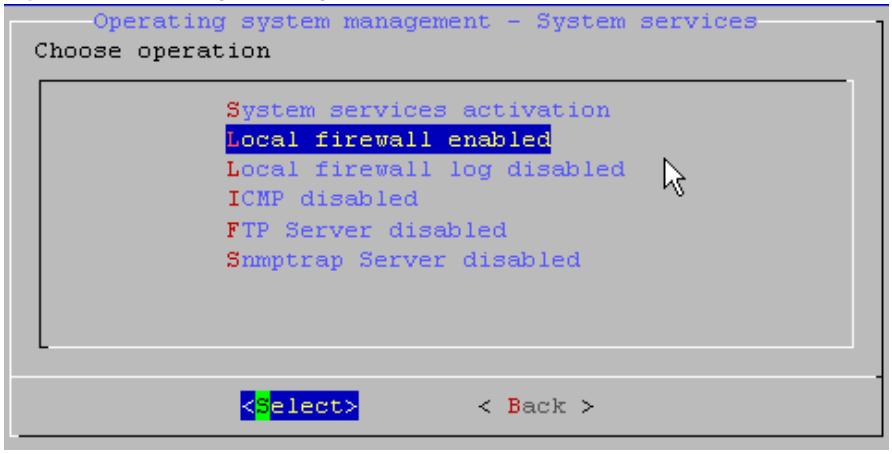


Enabling/Disabling the Local Firewall

1. To enable/disable the local firewall, go to **Main menu -> Operating System Management -> System Services -> Local Firewall Enabled/Disabled**. (See "Opening the SMPConfig Main Menu" and "Navigating through the Menus").

2. To toggle between Enabled or Disabled, press Enter.

Figure 105 Enabling/disabling the local firewall

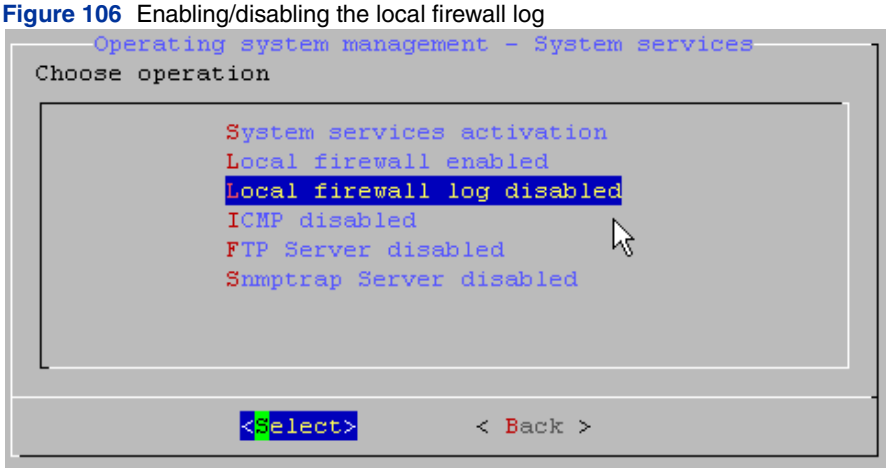


Enabling/Disabling the Local Firewall Log

1. To enable/disable the local firewall log, go to **Main menu -> Operating System Management -> System Services -> Local Firewall Log Enabled/Disabled**. (See "Opening the SMPConfig Main Menu" and "Navigating through the Menus").

2. To toggle between Enabled or Disabled, press Enter.

Figure 106 Enabling/disabling the local firewall log

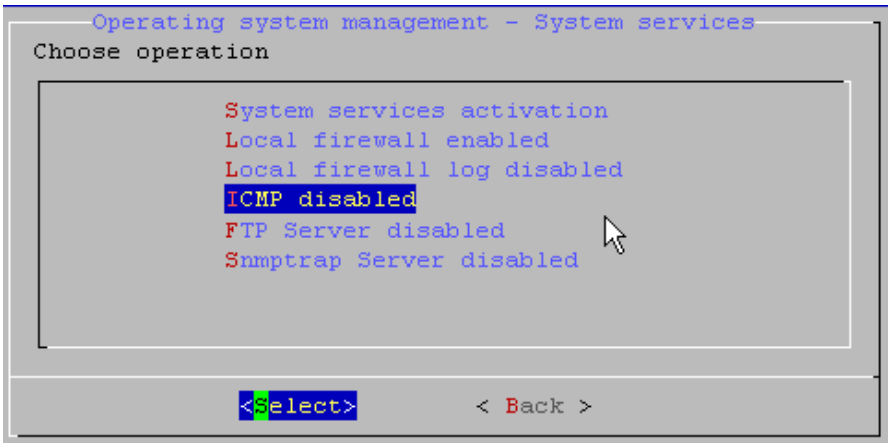


Enabling/Disabling the ICMP

1. To enable/disable the ICMP, go to **Main menu -> Operating System Management -> System Services -> ICMP Enabled/Disabled**. (See "Opening the SMPConfig Main Menu" and "Navigating through the Menus").

2. To toggle between Enabled or Disabled, press Enter.

Figure 107 Enabling/disabling the ICMP

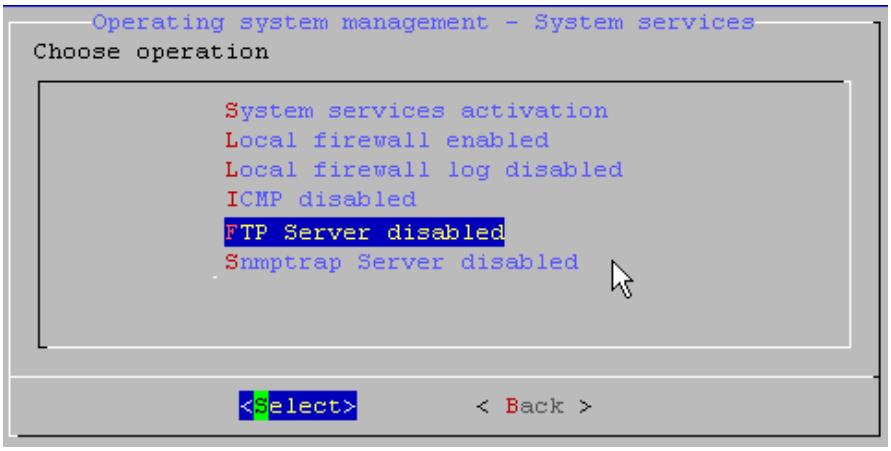


Enabling/Disabling the FTP Server

1. To enable/disable the FTP Server, go to **Main menu -> Operating System Management -> System Services -> FTP Server Enabled/Disabled**. (See "Opening the SMPConfig Main Menu" and "Navigating through the Menus").

2. To toggle between Enabled or Disabled, press Enter.

Figure 108 Enabling/disabling the FTP Server

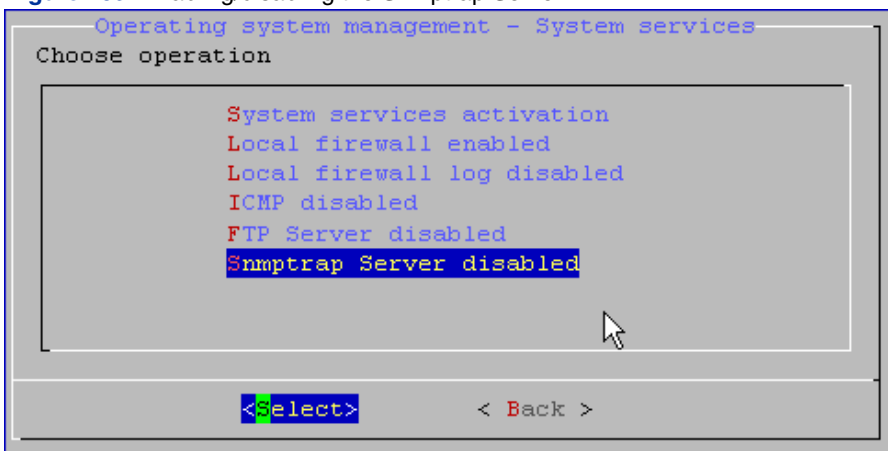


Enabling/Disabling the Snmptrap Server

1. To enable/disable the Snmptrap Server, go to **Main menu -> Operating System Management -> System Services -> Snmptrap Server Enabled/Disabled**. (See "Opening the SMPConfig Main Menu" and "Navigating through the Menus").

2. To toggle between Enabled or Disabled, press Enter.

Figure 109 Enabling/disabling the Snmptrap Server



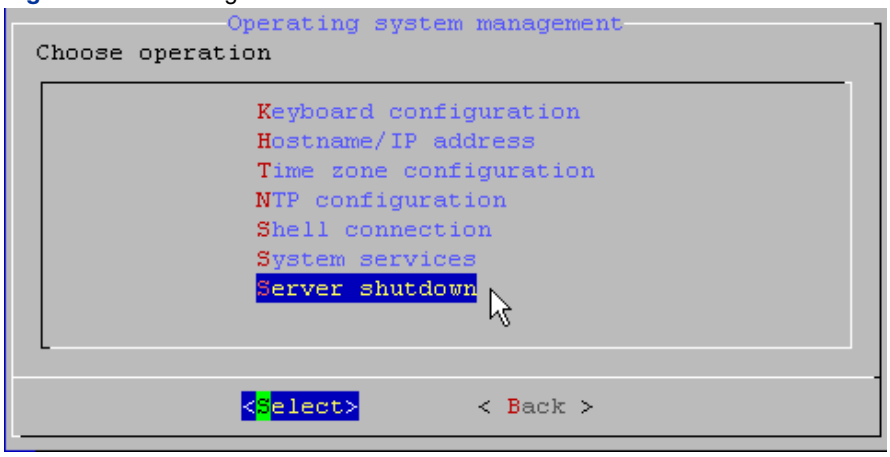
The Server Shutdown Submenu

In this menu section you may reboot or shut down the server.

Opening the Server Shutdown Submenu

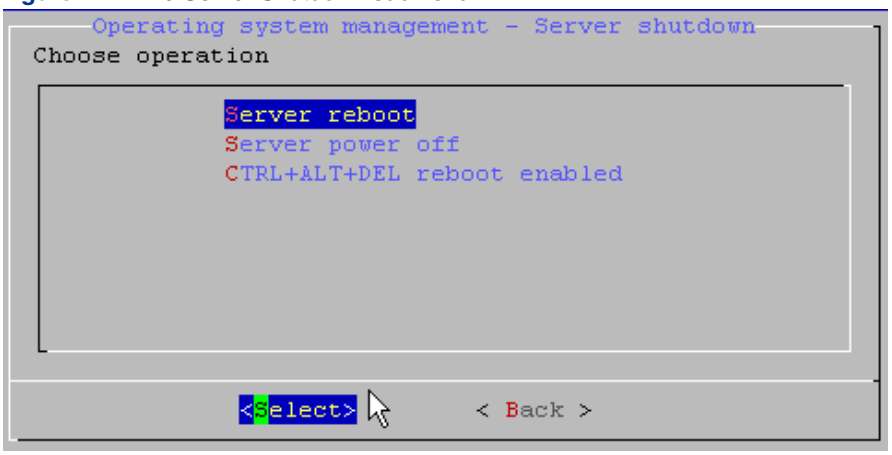
To open the **Server Shutdown** submenu, go to **Main menu -> Operating System Management -> Server Shutdown**. (See "Opening the SMPConfig Main Menu" and "Navigating through the Menus").

Figure 110 Selecting “Server Shutdown”



The Server Shutdown submenu is displayed.

Figure 111 The Server Shutdown submenu

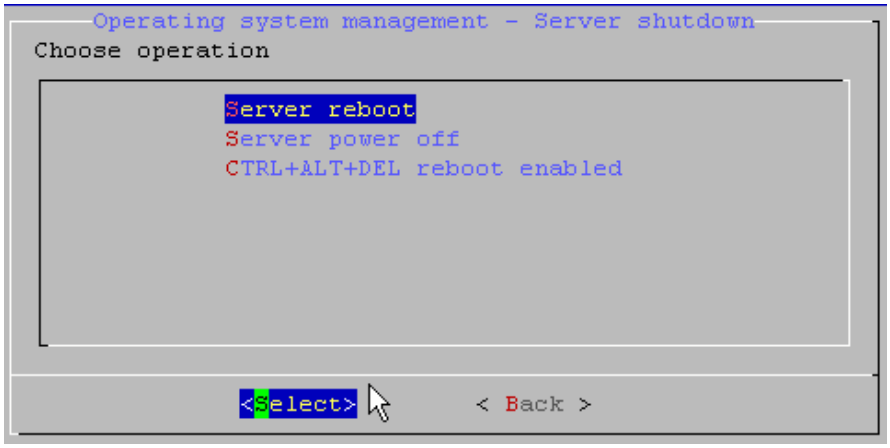


Rebooting the Server

1. To reboot the server, go to **Main menu -> Operating System Management -> Server Shutdown**. (See "Opening the SMPConfig Main Menu" and "Navigating through the Menus").

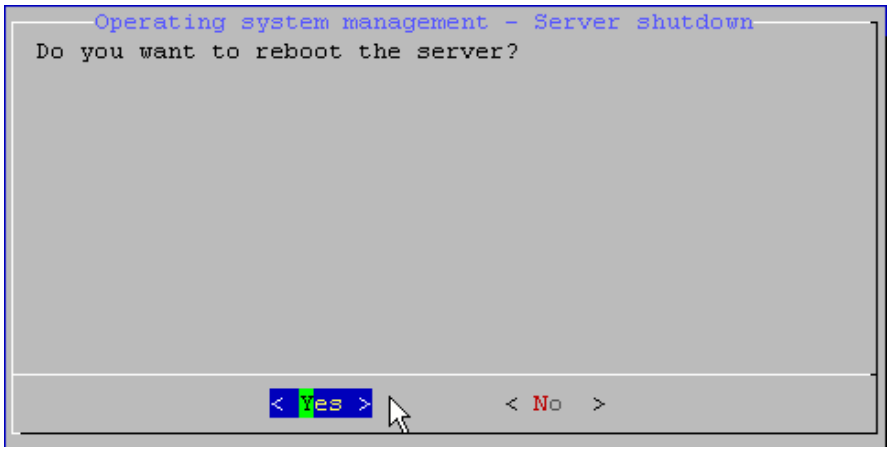
2. Use the **Up** and **Down** until **Server reboot** is highlighted, and then press Enter.

Figure 112 Rebooting the server



3. Confirm your request by selecting **Yes** and pressing **Return**.

Figure 113 Confirming the rebooting request



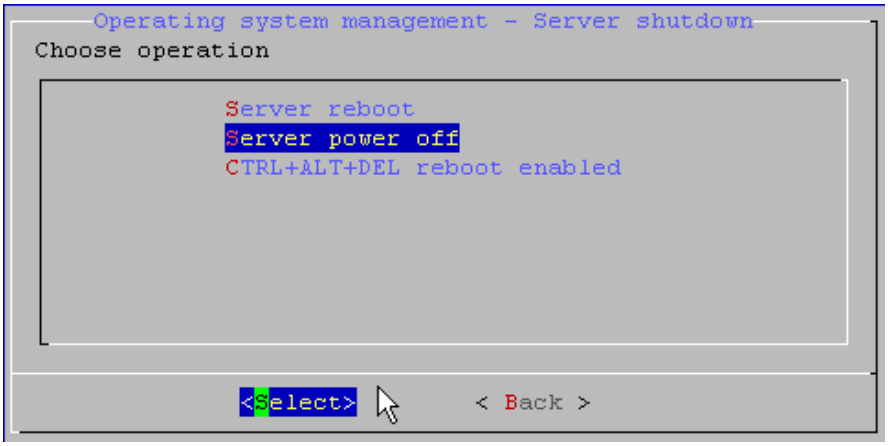
4. The console window will close automatically and the server will be rebooted. This may take a few minutes. Once the server is rebooted you will be able to open the SMPConfig Main Menu again in an SSH console.

Powering Off the Server

1. To power off the server, go to **Main menu -> Operating System Management -> Server Power off**. (See "Opening the SMPConfig Main Menu" and "Navigating through the Menus").

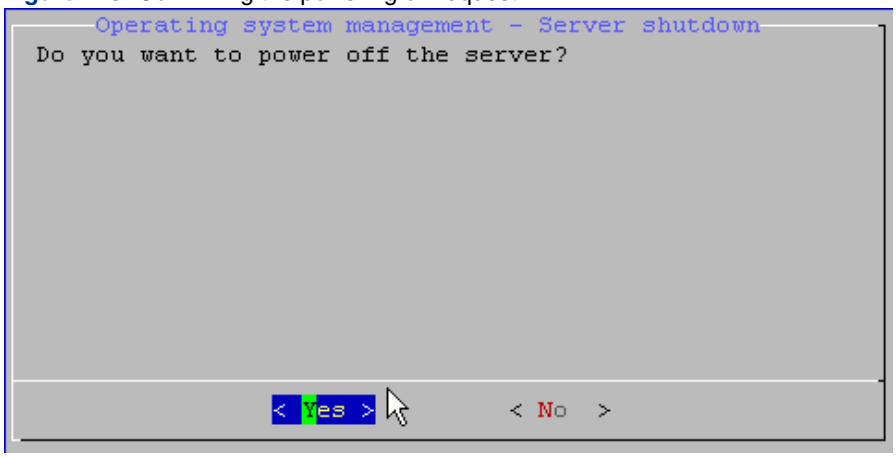
2. Use the **Up** and **Down** until **Server power off** is highlighted, and then press Enter.

Figure 114 Powering off the server



3. Confirm your request by selecting **Yes** and pressing **Return**.

Figure 115 Confirming the powering off request



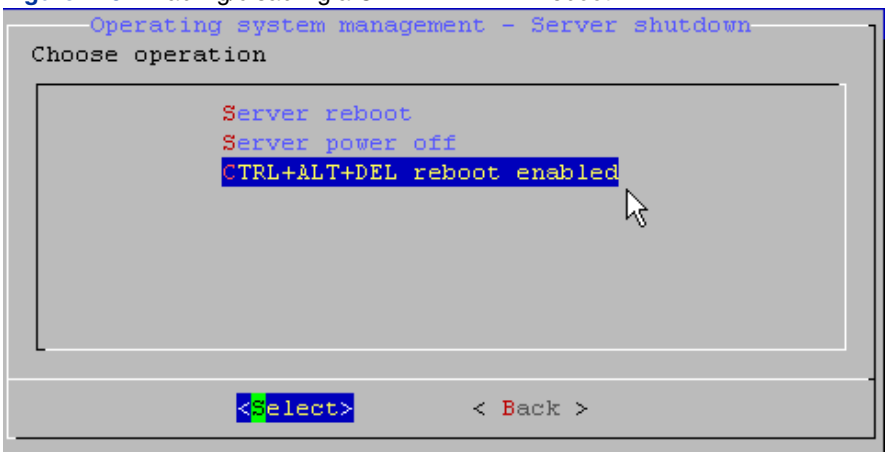
4. The console window will close automatically and the server will be powered off.

Enabling/Disabling a CTRL+ALT+ DEL Reboot

1. To enable/disable rebooting through CTRL+ALT+DEL, go to **Main menu -> Operating System Management -> CTRL+ALT+DEL Reboot Enabled/Disabled**. (See "Opening the SMPConfig Main Menu" and "Navigating through the Menus").

2. To toggle between **Enabled** or **Disabled**, press Enter.

Figure 116 Enabling/disabling a CTRL+ALT+DEL reboot



The DRAC Management Menu

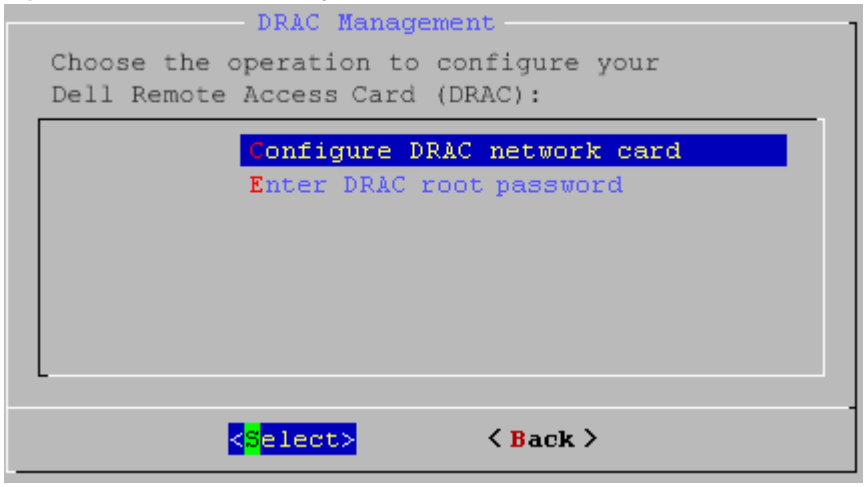
DRAC, an interface card from Dell Inc, provides out-of-band management facilities. The controller has its own processor, memory, battery, network connection, and access to the system bus. Key features include power management, virtual media access and remote console capabilities, all available through a supported web browser. This gives system administrators the ability to configure a machine as if they were sitting at the local console or terminal.

Note: Make sure that the DRAC firmware is compatible with the version of your RedHat Operating System.

Opening the DRAC Management Menu

To open the **DRAC management** menu, go to the main menu and select **DRAC management**. (See "Opening the SMPConfig Main Menu" and "Navigating through the Menus").

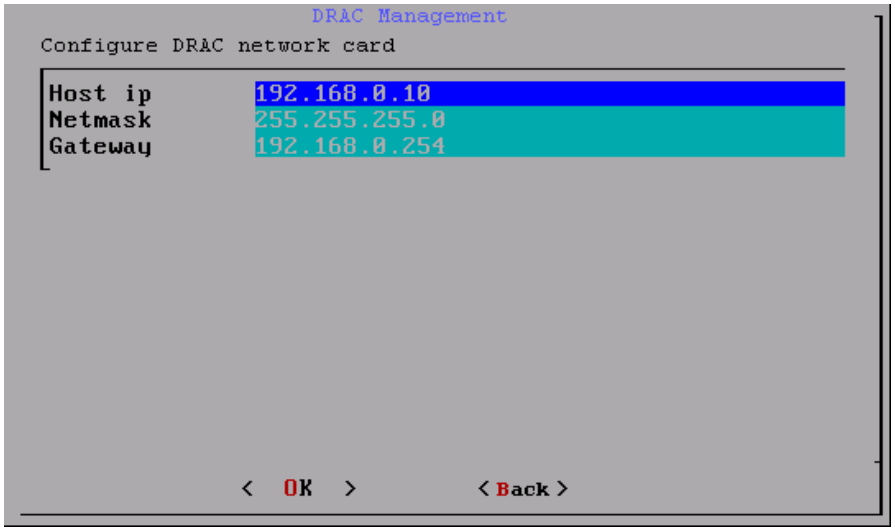
Figure 117 The DRAC management menu



Configuring the DRAC Network Configuration

1. Select **Configure DRAC network card** and press **Enter**. The following screen is displayed.

Figure 118 DRAC Configuration - Change IP

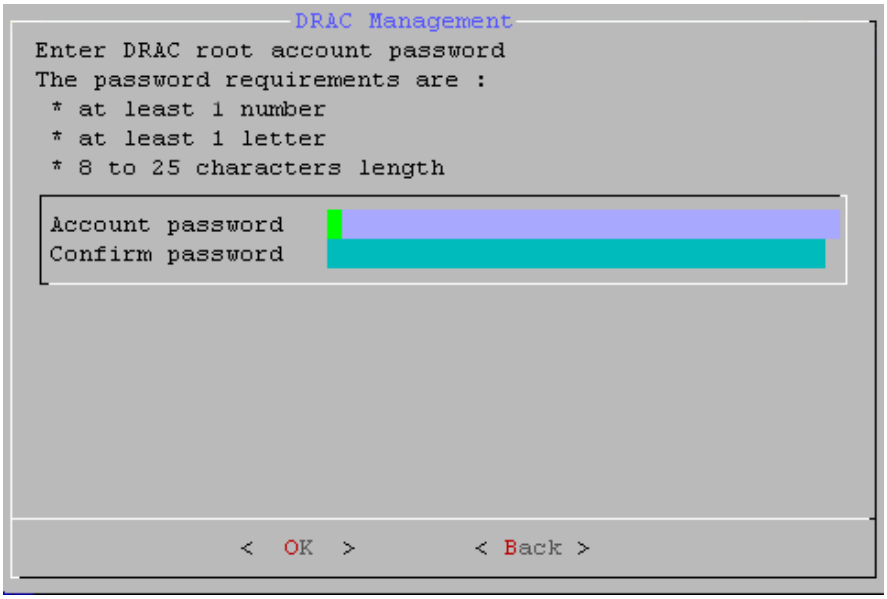


2. Enter **Host IP**, **netmask** and **gateway** addresses and select **OK**.

Entering the DRAC Root Password

1. Select **Enter DRAC root password** and press **Enter**. The following screen is displayed.

Figure 119 DRAC Administration - Root account



2. Enter the **DRAC root account password** and select **OK**.

Chapter 2 - Multi-Instance Installation

Why Installing Several Instances?

By default, when installing a SMP server, only one instance is available. However, you may need to add a new instance to:

- Manage different customers on the same appliance. In other terms, it means one instance = one customer.
- Isolate data such as Log Collector, rules... to guarantee a high security level.
- Perform tests and keep an instance 'at hand' while configuring the production instance.

Principles

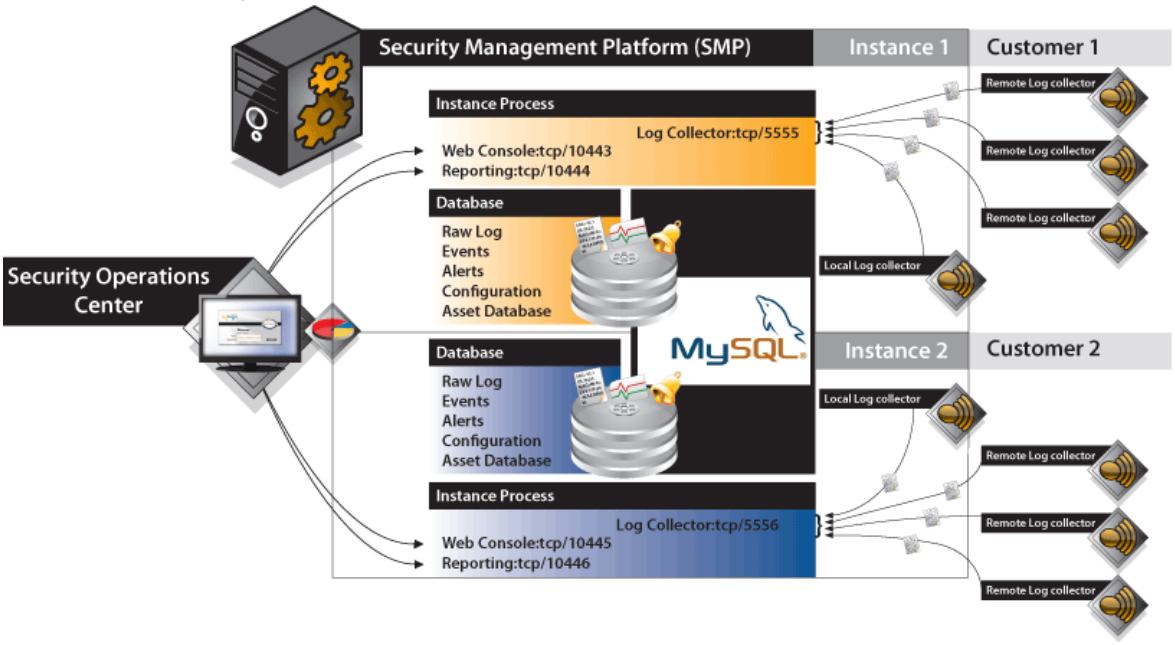
When installing a new instance, the configuration is by default very similar to the default one.

Remind that:

- One instance is supported if installed on Appliance 1065, 3065 and EVA,
- Two instances are supported if installed on Appliance 4065.

Here is the graphical representation of a multi-instance installation.

Figure 120 Multi-instance installation principle



The Log Collector

By default a local Log Collector is installed on the SMP to manage logs coming from external sources. However, for performance issues, it is not recommended to use it because it will use too much CPU performance.

On the other hand, you can use a remote Log Collector installed on a dedicated machine to save performance on the SMP. This remote Log Collector sends logs through Log Collector listening ports.

Database

The SMP server is based upon one MySQL Database Management System which manages data, i.e. each client has a single and dedicated database instance which allows data protection and isolation.

TCP Ports

Each instance has its own dedicated services and corresponding TCP ports:

- SMP port for Log Collector connection: 5555 is the default port for the first instance. Then during the installation, you will be suggested other ports such as 5556, 5557...
- SMP port for Web Console connection: 10443 is the default port for the first instance. Then during the installation, you will be suggested other ports such as 10445, 10447...
- SMP port for Reporting module connection: 10444 is the default port for the first instance. Then during the installation, you will be suggested other ports such as 10446, 10448...

> **Note:** You must authorize corresponding traffic or corporate internal firewall.

Performances

Each time you install an instance, even if it is not used, RAM and resources will be used. So it is recommended to correctly distribute the RAM between the various instances.

Only one MySQL server will be used for all the instances. This will lower performances.

> **Note:** To monitor EPS flow and performance of each instance, you must use the **SMP Monitoring** window which is available from the Web Console menu bar by clicking on **Configuration > SMP Monitoring**. Please refer to the Security Event Manager *User Guide* for more information.

Instance Naming

You must add a network alias per instance in your network configuration to avoid a conflict certificate with your web browsers. You can configure it in the `etc` file (`/etc/hosts`).

In the following examples, the aliases are in bold italic.

Table 3 Example of etc file with only one instance

```
# Do not remove the following line, or various programs

# that require network functionality will fail.

127.0.0.1       localhost.localdomain   localhost

::1     localhost6.localdomain6 localhost6

192.168.11.191  tbsmp1  tbsmp1
```

Table 4 Example of etc file with three instances

```
# Do not remove the following line, or various programs

# that require network functionality will fail.

127.0.0.1       localhost.localdomain   localhost

::1     localhost6.localdomain6 localhost6

192.168.11.191  tbsmp1  tbsmp1

192.168.11.191  tbsmp1_instance1  tbsmp1_instance2 tbsmp1_instance3
```

Installation Phases

Two installation modes are possible:

- Either you install the new instance in instance mode, which means you accept the TIBCO LogLogic® default configuration (port number, Log Collector port...)
- Or you install the new instance in advanced mode, which means that you must customize port numbers, the instance's name... This mode is useful if you know exactly the configuration of your machine.

To install a new instance, please follow the procedure below:

Starting the SMPConfig

1. Start a prompt window.

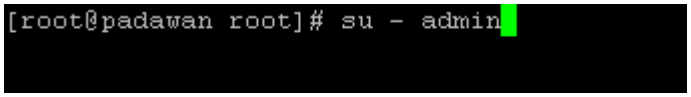
2. Edit the file:
`/usr/local/exaprotect-setup/config/install.cfg`.

3. Add `allow.mi=1` at the end of the file to allow the unlocking of the access to a new instance and save the file.

4. Connect to the SMPConfig:

- **Standard mode**: connect to the SMPConfig as admin by typing `su - admin`.

Figure 121 su - admin

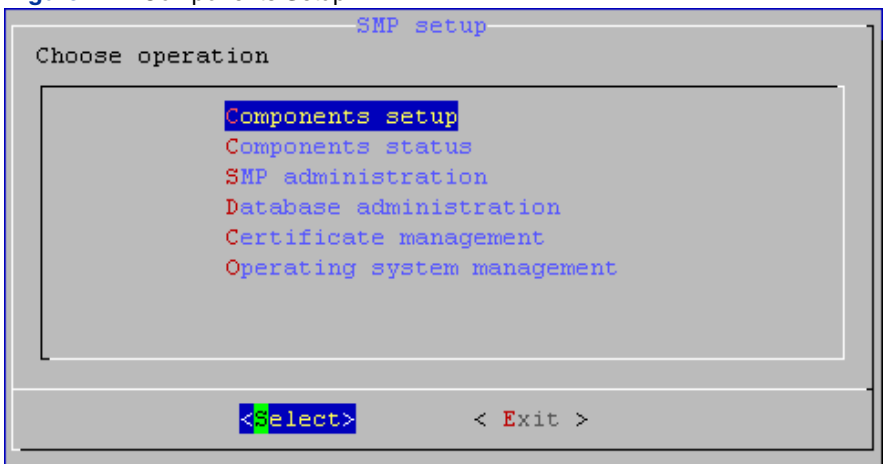


- **Advanced mode**: connect to the instance as **admin** by entering:
  `/usr/local/exaprotect-setup/scripts/setup.pl -a`

The **SMPConfig** window is displayed.

5. Select **Components Setup** and press Enter.

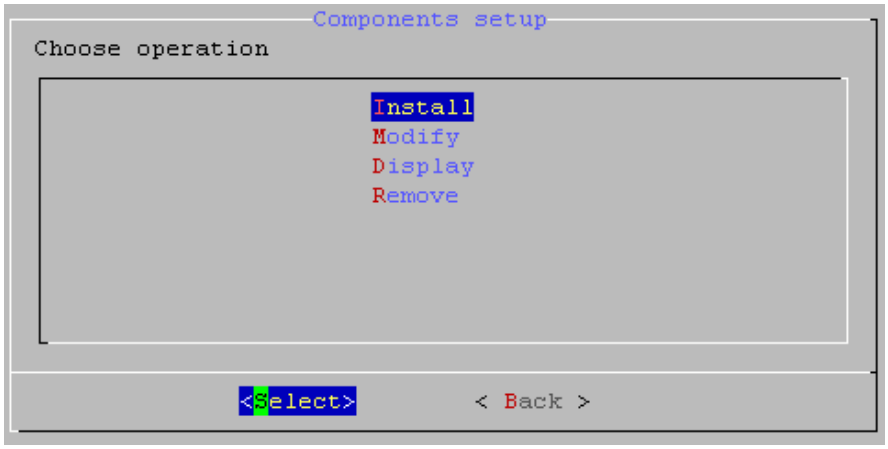
Figure 122 Components Setup



Installing the New Instance

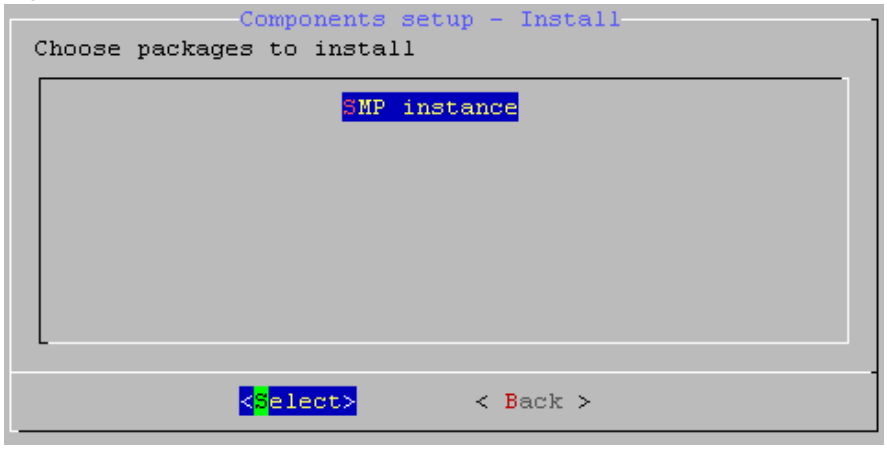
1. Select **Install** and press Enter.

Figure 123 Select install



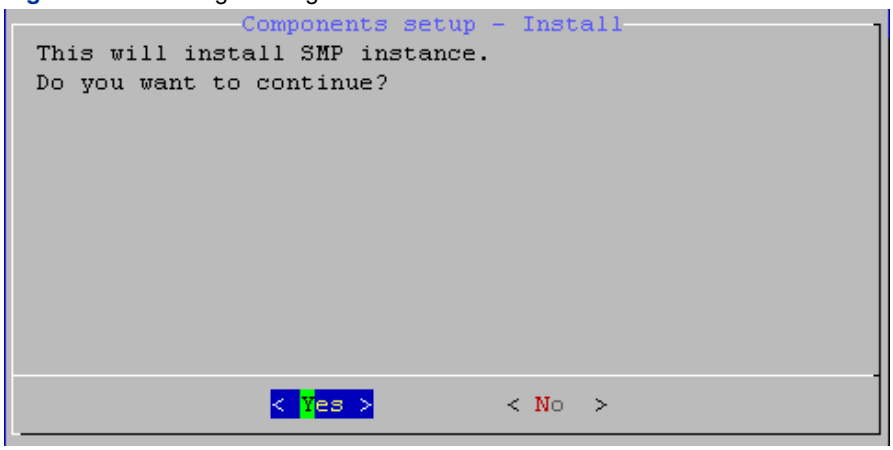
2. Select the instance upon which the new installation configuration and characteristics will be based. Then press Enter.

Figure 124 Select an instance



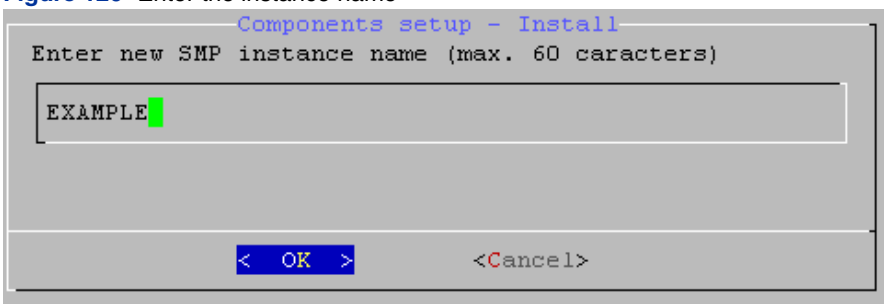
3. A warning message is displayed. press Enter to continue the installation process.

Figure 125 Warning message



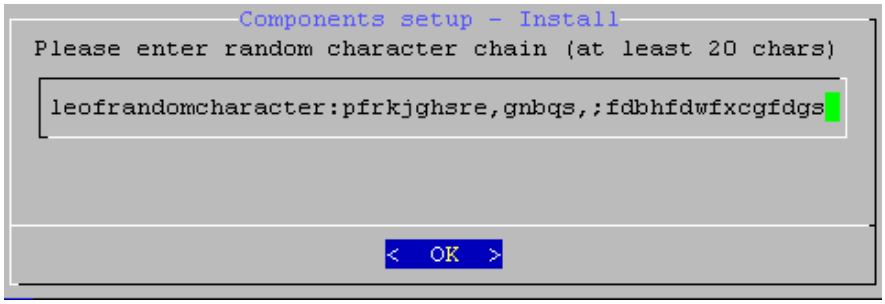
4. Enter the name of the instance you are going to install and press Enter.

Figure 126 Enter the instance name



5. Enter a random character chain to generate cryptographically secure keys and press **Enter**.

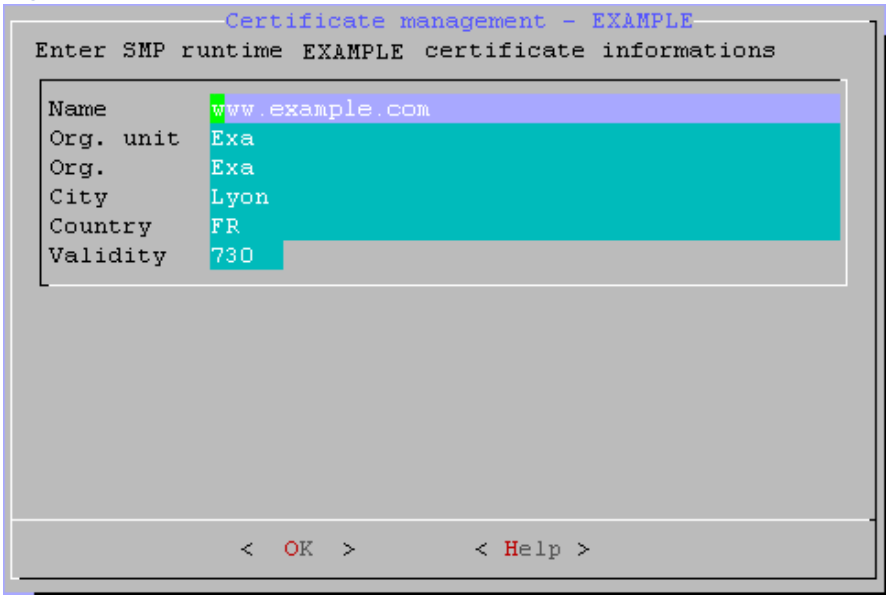
Figure 127 Enter a random character



6. The instance characteristics must be filled.

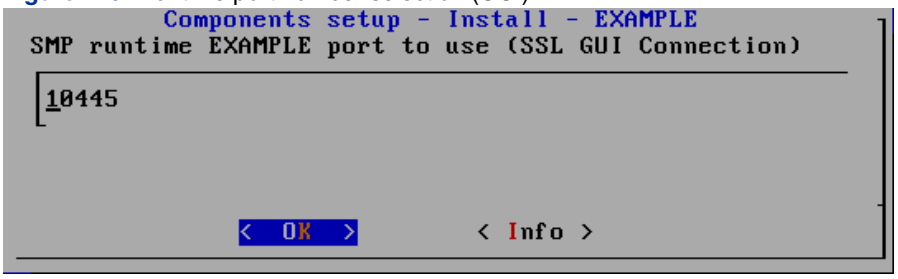
- **Standard mode**: the instance installation process starts (database, runtime, report, Log Collector, etc).
- **Advanced mode**: enter the various characteristics you want to apply to the new instance runtime, i.e. its name, the organization and organization unit associated, the city and the country where it is located, and its validity in days.

Figure 128 Various characteristics



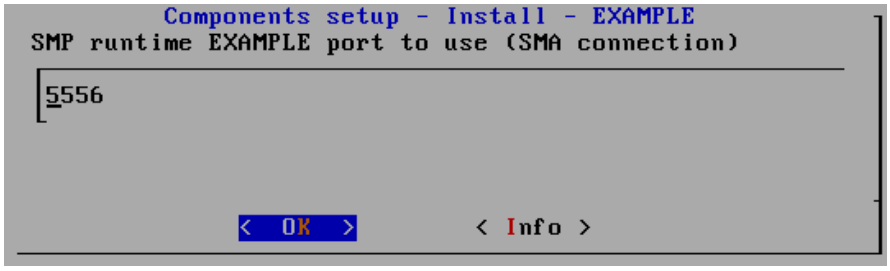
7. Enter the runtime port number to use to connect to the Web Console.

Figure 129 Runtime port number selection (GUI)



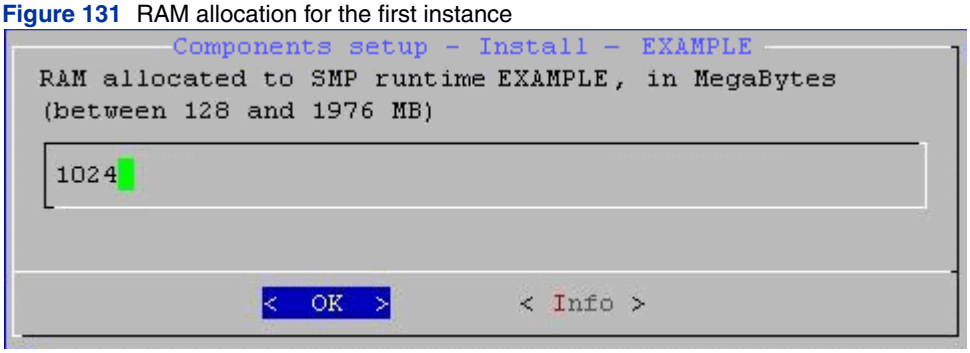
8. Enter the runtime port number to enable the Log Collector connection.

Figure 130 Runtime port number selection (Log Collector)



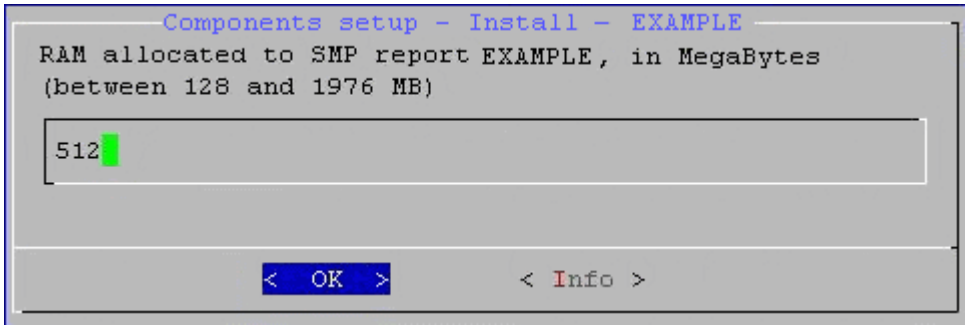
9. Enter the RAM necessary for the new instance runtime.

Figure 131 RAM allocation for the first instance



10. Enter the RAM necessary for the new instance report.

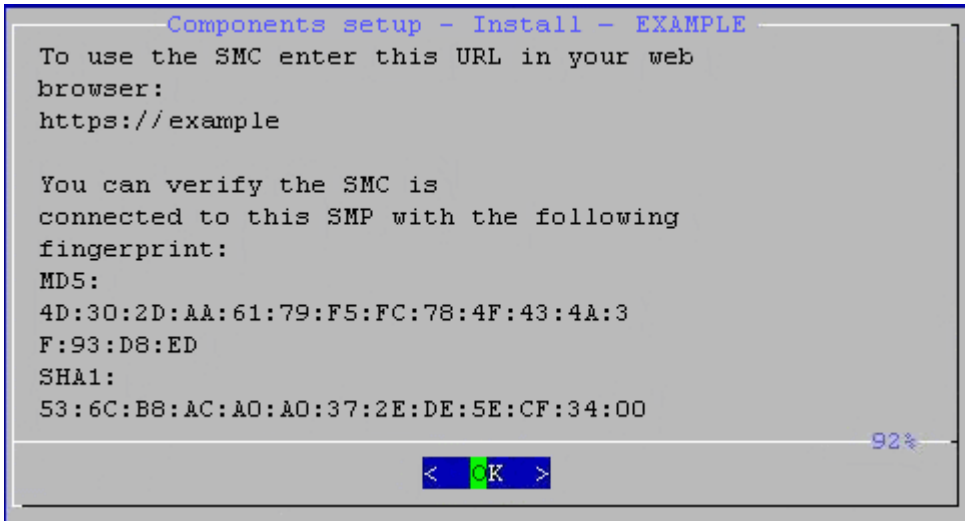
Figure 132 RAM allocation for the second instance



Note: If you want to check if all data has been correctly entered, go back to the **Installation** screen and select **Display > Ram** or **Ports**.
If you want to modify data, select **Modify** and choose the new instance.

11.A message is displayed indicating the URL to display the application. It also indicates the fingerprint codes you can use to check whether the Web Console is connected to the SMP.

Figure 133 Fingerprints



The installation process is finished. By default, the new instance is available at https://example:10445.

If you have modified the `etc` file as explained earlier in the ***Instance Naming*** section, you should obtain an URL such as, e.g.:

https://ip_serveur_instance1:10443/Exaprotect

https://ip_serveur_instance2:10445/Exaprotect

https://ip_serveur_instance3:10447/Exaprotect

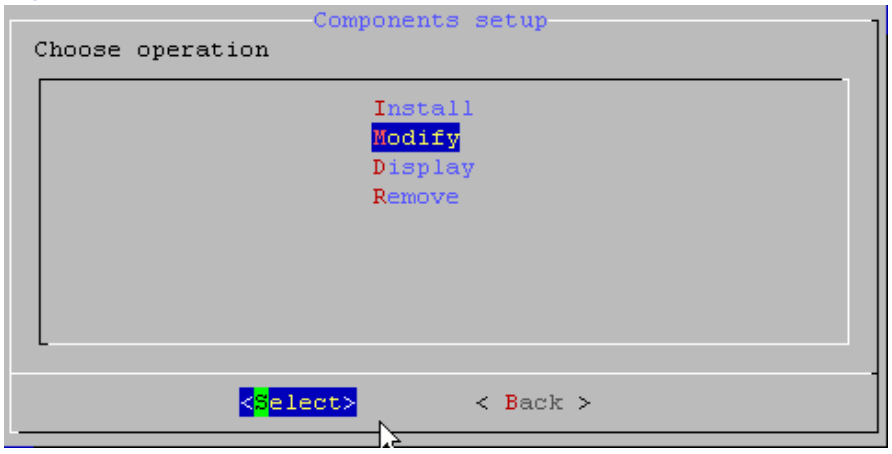
Modifying RAM

If you installed a new instance in standard mode, you will need to modify the configuration to share RAM between instances. To do so:

1. Re-open the SMPConfig prompt by following the procedure described in section **Starting the SMPConfig** until step **5**.

2. Select **Modify** and press Enter.

Figure 134 Select install

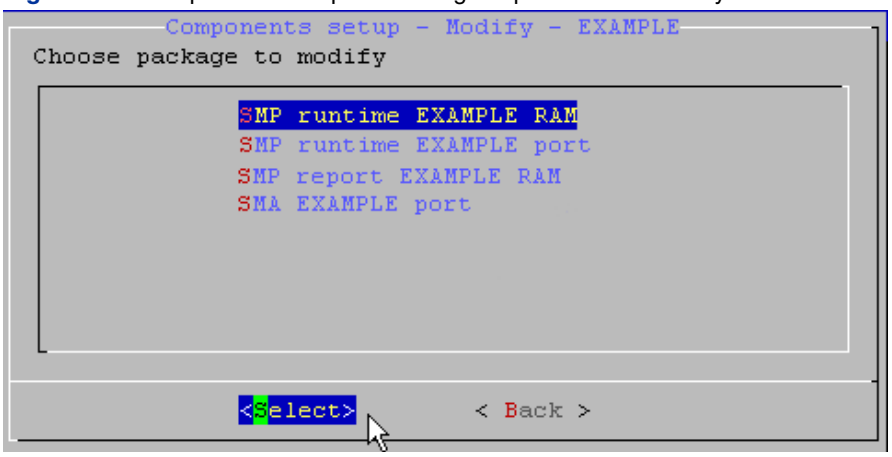


3. Use the **Up** and **Down** arrows to highlight the package to modify and then click **Return.**

4. Use the **Up** and **Down** arrows to highlight the instance to modify and then click **Return.**

5. The instance parameters menu appears.

Figure 135 Components Setup - Choosing the parameter to modify



6. Select SMP Report RAM to modify the RAM of the reporting engine.

7. Select SMP runtime RAM to modify the RAM used by the correlation engine and the display of alerts.

According to the appliance you have, we recommend you the following RAM configuration:

Appliance 4065

Only **2** instances supported.

Total RAM: 32768

If only one instance is installed:

- RAM for the instance runtime: 12 288
- RAM for the instance reporting: 4 096

If two instances are installed:

- RAM for each instance runtime: 6 144
- RAM for each instance reporting: 2 048

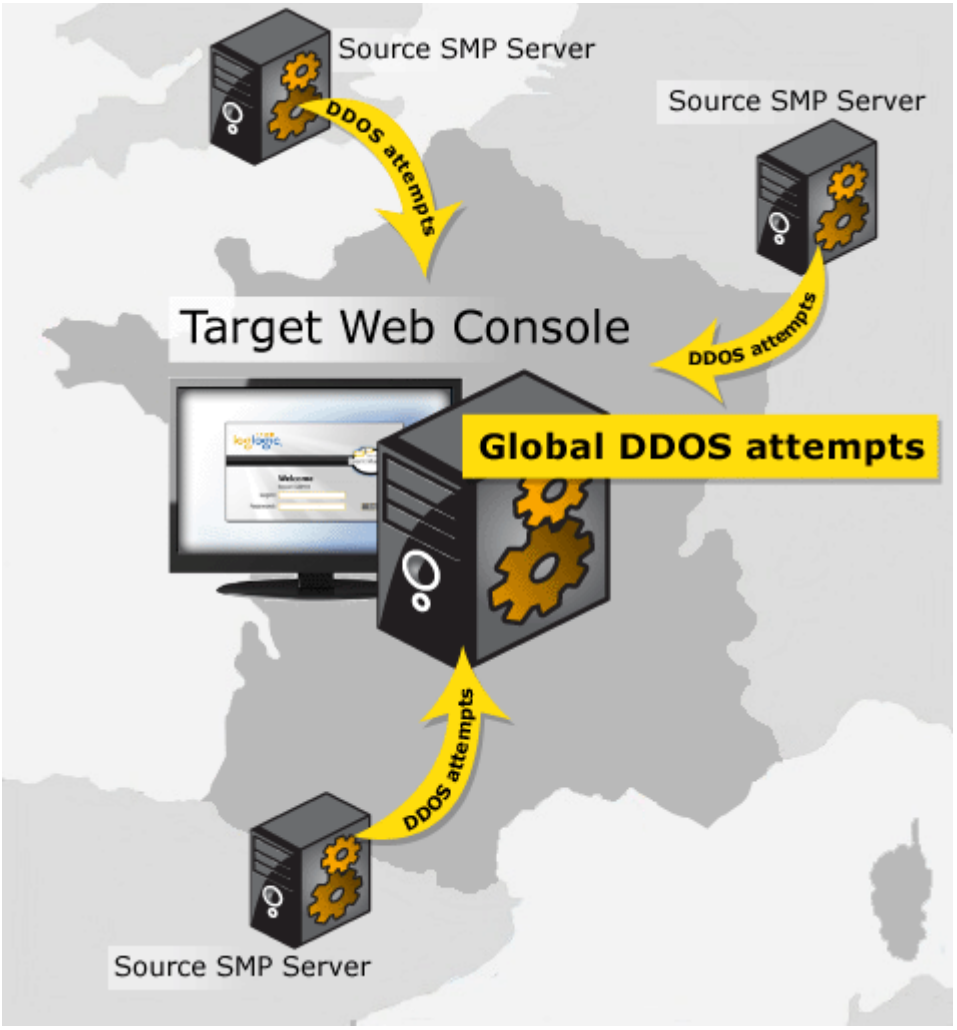
For more information about the instances to install on this appliance, please contact the support.

Chapter 3 - Communication between SMP Servers

If you need to centralize and diminish the alert's flow, you can install multiple SMPs consisting of several Source servers and one Target server. Only the relevant alerts or events generated from the source SMP will be displayed on the console of the target SMP.

The principle can be represented as follows:

Figure 136 Example of communication between SMP



Installing the Log Collector's File on the Target Server

You must generate a Log Collector's installation file (i.e. the SMP which receives alerts). To do so:

1. In the Web Console, go to **LogManager > Log Collection > Download Log Collector Installation File**.
2. Make sure the SMP **server address** and **Port** fields are correctly filled in.
3. Select the **server -> server** communication type.

4. Click **Download**.

5. Install the zip file as explained in the following section.

Preparing the Source Servers (i.e. the SMP sends alerts)

1. Unzip the file into the directory `home/exaprotect/conf/<InstanceName>/senders/` by executing the following commands:

```
unzip TBSMP2.zip -d /home/exaprotect/conf/<InstanceName>/senders
```

```
chown -R exaprotect:exaprotect /home/exaprotect/conf/<InstanceName>/senders
```

2. Restart the instance runtime:

/etc/init.d/exa_runtime_<InstanceName> restart

Adding a Log Collector on the Target Server

Now you must add a Log Collector with the **server -> server** communication type.

1. In the Web Console, go to **LogManager > Log Collection > Log Collectors**.

2. Click on **Add** to add a Log Collector.

3. Fill in the appropriate fields and make sure you selected the **server -> server** communication type in the **Type** field.

4. Click **OK**.

Editing Correlation Rules on the Source SMP

1. In the Web Console, go to **EventManager > Correlation Policy.**

2. Click on one of the proposed categories.

3. Click on the rule to activate.

4. Click on the **Actions** tab.

5. In the **Actions** section, check the **Send the event/alert to another SMP** box.

This type of architecture allows you to get a new security monitoring point of view (n+1) as you can go from one site-per-site monitoring to a global monitoring (on a national or international basis). The sending of alerts is then refined so that - for example - a global attack of an information system can be detected as quickly as possible.

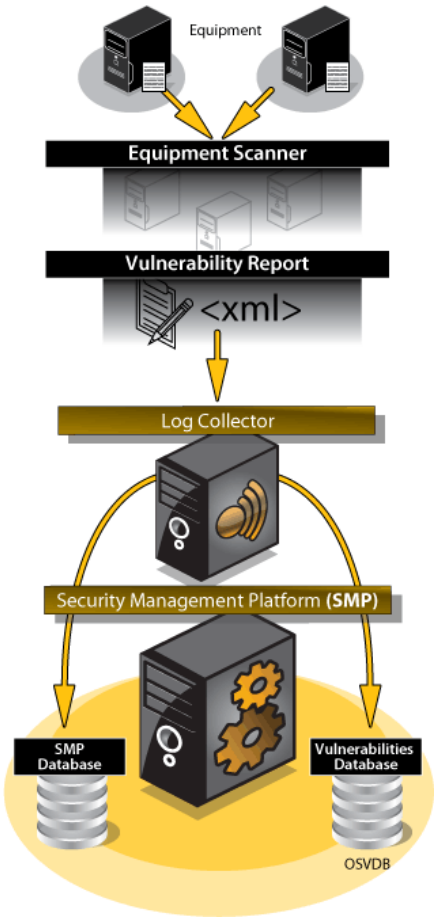
Notes:

- When you create a correlation rule, you can send the alert to the other SMP.
- Once an alert has been sent to the target server, it cannot be modified even if it has been modified on the source server.
- To send all alerts (including aggregated events) to another SMP, you need to create a rule with no specific conditions. This rule must be in first position in the correlation rules list.

Chapter 4 - Equipment Vulnerabilities

General Overview

Security Event Manager deals with equipment vulnerabilities by keeping a vulnerability database updated by information supplied by the Log Collector. The Log Collector's process information furnished by equipment scanners. The generated events are sent to the SMP and added in the vulnerability database. Security Event Manager also allows the user to monitor and manipulate this vulnerability information. Through the GUI, the user can view and categorize information detailing vulnerabilities for their equipment and they can also process the resulting alerts.



The Vulnerabilities Database

The Security Event Manager detects which vulnerabilities pertain to a client's equipment and this information is displayed in a vulnerabilities window. In addition, the user can categorize a known vulnerability as a false positive when this vulnerability has been corrected, for example, when a patch has been applied to a certain equipment unit/system, or if this vulnerability information is not applicable to the client's equipment configuration. The false-positive vulnerability will then be taken off the vulnerabilities list and it will be inserted into the False-Positive list. The vulnerabilities database is also updated with information gathered by Log Collector's which collect information from equipment scanners.

Vulnerability Events Produced by Log Collectors

An equipment scanner will periodically search a particular equipment unit for vulnerabilities and produce a report containing information concerning the vulnerabilities found on this equipment. Each time a new report is produced, the Log Collector will then compare this report with the previous one and possibly create events to call attention to changes or important vulnerabilities. These events will appear in the event monitoring window and they can be of 3 different types:

- Event for a newly detected vulnerability ("New flaw")
- Event for an existing vulnerability ("Active flaw")
- Event for a vulnerability that is no longer detected ("Fixed flaw")

> **Note:** At any given time, there are at most two report files stored in each scanner directory (the current scanner report and the previous one). Older scanner report files are automatically deleted.

Vulnerability Scanner Installation

Overview

Each vulnerability scanner needs to be configured to save its report to a specific user-defined folder. This folder specification is entered as a parameter into the Confset submenu. Defining this folder allows the Log Collector to compare each new scanner report to the previous one and create the necessary vulnerability events. Since each vulnerability scanner related to a particular equipment is different, please refer to the relevant equipment documentation for guidance on how to install and configure a particular vulnerability scanner, making sure that the configuration meets the requirements detailed below.

When configuring a vulnerability scanner, please observe the following:

- the exported file containing the scanner's report needs to be in XML;
- you will need to configure the scanner to periodically scan your equipment.

Defining the Vulnerability Scanner Directory

The instructions below show the steps for defining the directory where the vulnerability scanner reports will be saved to. In this example, we will define a directory for a Nessus scanner.

1. Go to **LogManager > Log Collection > Advanced > Confsets.**
2. Click on the **Copy** button in at the end of the **Nessus** row.
3. Click on the copy you have just created. The **General Confset Properties** screen is displayed.
4. In the Converter section, click on **Nessus** and enter the directory path.
5. Click **OK**.

Vulnerability Events

The following are descriptions of the information contained in vulnerability events.

A prefix is added to the event's classification name (IDMEF field: classification.text) to enable the identification of the 3 types of events. The prefixes are:

- New flaw: <original classification name>
- Active flaw: <original classification name>

- Fixed flaw: <original classification name>

Specific details regarding the vulnerability scanner are inserted in the IDMEF additionalData field :

Table 5 IDMEF additionalData field for Vulnerability

Meaning	Type	Data	Compulsory
Scanner_Name	string	Scanner name	X
Scanner_TestId	string	Test identifier	X
Scanner_TestName	string	Name of the test executed by the scanner	X
Scanner_ShortDescr	string	Short description of the vulnerability	
Scanner_VulnDescr	string	Description of the vulnerability and the risk	
Scanner_SolutionDescr	string	Recommendations	

The fields Scanner_Name and Scanner_TestId enable the identification of a test for a vulnerability scanner.

The descriptions Scanner_ShortDescr, Scanner_VulnDescr, and Scanner_SolutionDescr are general descriptions, they do not contain specific data concerning the impacted machine. On the other hand, the description contained in the IDMEF field assessment.impact.description is specific to the impacted machine. Events relating to vulnerabilities detected by the scanner are processed by the SMP to feed or to update the vulnerabilities database.

Event for a New Vulnerability (“New flaw”)

The new vulnerability information is stored in the database:

- The scanner name is added to the Exa_Scanner table if it does not exist.
- The vulnerability test is added to the Exa_Test table if it does not exist (name and code of the test).
- The descriptions related to the test are added to the Exa_Test_AddData table, if they do not exist
- The host is added to the knowledge database if it does not exist (insertion in tables Exa_Host, Exa_Address, Exa_Node). By default, the host identifier is the name of the machine. If it is not known, the identifier will be its IP address.
- The detection date of the vulnerability and the description concerning the impacted host are added to the Exa_Lnk_Host_Test table. The field success is positioned at 1 and the field false_positive at 0.

Event for an Existing Vulnerability (“Active flaw”)

Normally, only the vulnerability detection date and the specific impacted host description are updated in the database. This means that the database will contain the date referring to the most recent detection of the vulnerability by the scanner; previous detection dates are not stored.

Event for a Vulnerability that is No Longer Detected (“Fixed flaw”)

A vulnerability that is no longer detected by a scanner is considered by default as not being present on the machine. The field success of the Exa_Lnk_Host_Test table is positioned to 0. If the vulnerability is declared as false-positive, the fields false_positive and user_comment are re-initialized (respectively with 0 and NULL).

Another categorization is possible: the vulnerability is not taken into account any more. The fact that a vulnerability is no longer detected by a scanner does not necessarily entail that it is no longer present on the machine where it was first detected. In this case, the corresponding field in the Exa_Lnk_Host_Test table is simply deleted.

The parameter indicating the operation mode is in the configuration exa_kb.properties file:

```
vuln.notDetectedNotVuln=yes
```

Displaying the Details Pertaining to a Vulnerability

At best, the vulnerability details comprise the following information (vulnerabilities tested by scanners)

- the name of the vulnerability,
- documentation
- references

To view the details pertaining to a vulnerability:

1. Go to **Configuration > Asset Database > Effective vulnerabilities**
2. The list of vulnerabilities is displayed.
3. Click on the desired vulnerability name to view its details.

Table 6 Different Possible Categorizations for a Vulnerability

Access Required	Console/Physical Access Required Shell/Local Access Required Remote/Network Access Required Dialup/Modem Access Required Unknown Access Required
Types of Attacks	Authentication Attack Cryptographic Attack Denial of Service Attack Hijacking Attack Information Disclosure Attack Infrastructure Attack Input Manipulation Misconfiguration Problem Race Condition Other Attack Type Unknown Attack Type

Table 6 Different Possible Categorizations for a Vulnerability

Impact	Loss of Confidentiality Loss of Integrity Loss of Availability Unknown Loss
Exploit	Exploit Available Exploit Unavailable Exploit is Rumored Exploit Unknown

Displaying the Hosts Impacted by a Vulnerability

Several hosts can be impacted by a vulnerability. For each of these hosts, the GUI indicates the criticality (the highest criticality of the businesses assets for this host) and how the vulnerability was discovered. The name of the scanner, the test reference and the vulnerability detection date are specified.

Note: A vulnerability on a host can be declared a false positive.

To view the hosts impacted by a vulnerability:

1. Go to **Configuration > Asset Database > Effective Vulnerabilities**
2. Click on the number in the column **Hosts NB**.

Displaying Vulnerabilities Marked as False-positive

Vulnerabilities categorized as false-positive will appear in the False Positives list. The list will display the name of the vulnerability and the related machines. You may add a comment in the Comment field.

To view the vulnerabilities marked as false-positive:

1. Go to: **Configuration -> Asset database-> False Positive Vulnerabilities.**
2. The list of false-positive vulnerabilities is displayed.
3. Click on the desired vulnerability name to view its details.

Declaring a vulnerability for a host as false-positive modifies the following tables in the data base:

- update of the Exa_Lnk_Host_Test table (table indicating that a scanner found a vulnerability on a host)

- false_positive field set to 1
- user_date field set to the current date and hour
- user_id field set to the analyst's identifier
- user_comment field initialized with the analyst's comment - insertion in the Exa_Lnk_Not_Vuln_Host table (table indicating that a host product version is not vulnerable, as opposed to what is indicated in the vulnerability database)
- there are as many insertions in this table as there are vulnerable product versions used by the host for this vulnerability
- host_id, product_version_id, osvdb_id fields initialized with the host identifiers, the product version and the vulnerability concerned

- user_id field initialized with the analyst's identifier
- reason field initialized with the user's comment
- since_date field set to the current date and hour

Moving False-positive Vulnerabilities to the True Vulnerabilities List

Vulnerabilities categorized as false-positive will appear in the False-Positive list. To recategorize a vulnerability marked as false-positive as a true vulnerability:

1. Go to: **Configuration > Asset Database -> False Positive Vulnerabilities.**
2. The list of vulnerabilities marked as false-positive appears.
3. Tick the checkbox next to the desired vulnerability name.
4. Click the **True Vulnerability** button.

Acknowledging Vulnerability Scanner Alerts

An action is executed at the time that alerts coming from a vulnerability scanner are acknowledged. If the acknowledgement category is False Positive, the vulnerability is categorized as false-positive, otherwise the vulnerability is categorized as an “active flaw”. The Exa_Lnk_Host_Test table is updated as a consequence, as previously described.

Deleting Vulnerabilities that Have Been Previously Detected

This deletion function will erase the vulnerabilities which were detected before a certain date in the past (a number of N days). This function refers to vulnerabilities detected by a scanner. Only the entries in the Exa_Lnk_Host_Test table where the field **success** equals to 1 and where the **test_date** date is earlier than the current date minus N days are deleted. This operation is carried out at the same time as the daily backup. The parameters for this function are found in the user_backup.conf.xml configuration file. By default, vulnerabilities having been detected at a date earlier than 30 days are deleted.

<deleteOldVulnTests>true</deleteOldVulnTests>

<vulnTestsConservationPeriod>30</vulnTestsConservationPeriod>

Caution: if you modify any of these parameters, you will need to restart the application for the parameters to be taken into account by the application.

The target_assessment Field

The correlation engine also performs correlations with the vulnerabilities database. This allows alerts having an IDS origin (an analyzer of type Network IDS, Host IDS, or Database IDS) to have their respective attack information confirmed or not. The flaw discovered by an IDS is transmitted by a Log Collector to the SMP as an alert.

Alerts having an IDS origin usually contain information regarding the target (name, IP address) and references to the flaw being exploited (CVE, etc.). If the target is part of a host in the asset database and one of the flaw references is stored in the vulnerabilities database, it is possible to deduce if the host is vulnerable to the attack referred to in the IDS alert.

As a result of this correlation, the **target_assessement** field is set to one of three values:

- vulnerable

- not_vulnerable
- os_mismatched

By default, the severity level of an alert may be increased by a correlation rule which analyzes the type of attack information contained in the **target_assessement** field. See the following table for details concerning each of the three possible cases.

Table 7 target_assessment Field

Value	Action Description
vulnerable	In this case, the correlation rule will increase the severity of the alert by one level. See "The Vulnerability Rule"for more details.
not _vulnerable	In this case, the correlation rule perform an auto-acknowledgement of the alert and categorizes it as a false positive. See "The Vulnerability Rule"for more details.
os_mismatched	In the case where it is not known if the target is vulnerable to the attack, it is possible to verify if the vulnerability impacts the same operating system family as the host, when this vulnerability is referenced in the vulnerability database. If the vulnerability does not impact the same operating system family, this is clearly a false positive case. In an os_mismatch case, the correlation rule perform an auto-acknowledgement of the alert and categorizes it as a false positive. See "The Vulnerability Rule"for more details.

Note: The above is a description of the default configuration for the three rules. You may alter the prescribed actions in each of the correlation rules at any time as needed.

The Vulnerability Rule

To view details for the vulnerability rule entitled **ADB - Threat on Vulnerable Target** or to change parameters for a rule:

1. Go to **EventManager > Correlation Policy.**
2. Click on the desired rule name.
3. Change any of the configurable parameters.
4. Click **OK**.
5. Find:

PHP:

```
<tr bgcolor="#DDDDDD">
  <td class="cer_maintable_text"><b>Queue ID</b>
</td>
  <td class="cer_footer_text">##queue_id##</td>
  <td class="cer_maintable_text"><b>Queue Name</b>
</td>
  <td class="cer_footer_text">##queue_name##</td>
 </tr>
```

6. Following the text above, add:

PHP:

```
<tr bgcolor="#DDDDDD">
<td class="cer_maintable_text"><b>Ticket Priority</b>
</td>
<td class="cer_footer_text">##ticket_priority##</td>
</tr>
```

7.

Now open the file:

cerberus-gui/includes/cerberus-api/email_templates/cer_email_templates.class.php

8. Look for:

PHP:

```
$this->tokens[] = "##ticketid##"; // for compatibility with old autoreplies
```

9. Above this section, add:

PHP:

```
switch($ticket_data["ticket_priority"]){
case 0:
$priority = "Unassigned";
break;
case 5:
$priority = "None";
break;
case 25:
$priority = "Low";
break;
case 50:
$priority = "Medium";
break;
case 75:
$priority = "High";
break;
case 90:
$priority = "Critical";
break;
case 100:
$priority = "Emergency";
break;
}
```

10. Look for:

PHP:

```
$this->tokens[] = "##ticket_time_worked##";
```

11. Add the following code:

PHP:

```
$this->tokens[] = "##ticket_priority##";
```

12. Look for:

PHP:

```
$this->tokens_values[] =  cer_DateTimeFormat::secsAsEnglishString($ticket_da
ta["ticket_time_worked"]*60,true,4);
```

On the line below, add:

PHP:

```
$this->tokens_values[] = $priority;
```

How to Parse Email Content Sent to the Cerberus Application

> **Note:** The information provided below is for informational purposes or in case you encountered difficulty installing the compressed file.

The following code was extracted directly from the Cerberus editor.

1. In an editor, open the file:

/cerberus-gui/includes/elements/config_parser_rules_edit.php

2.

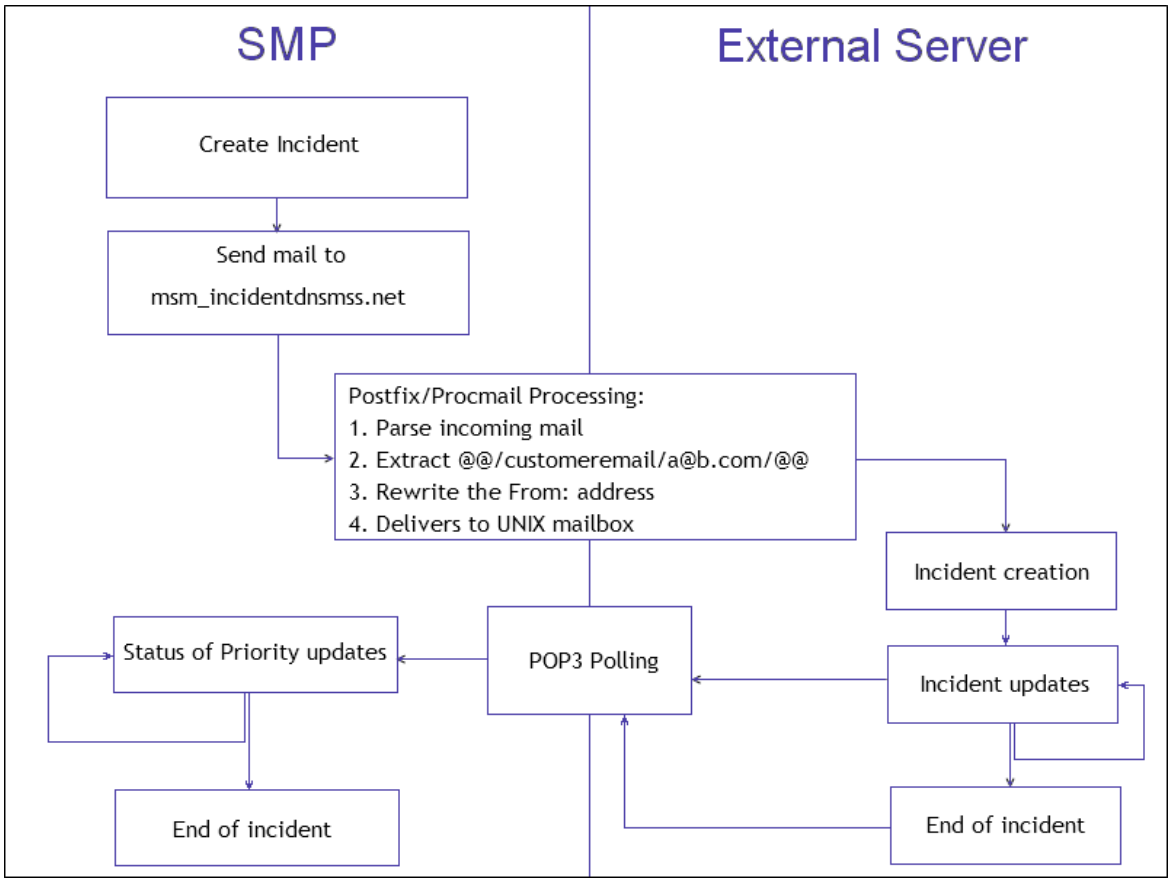
Chapter 5 - Managing Incidents via an External Server

Overview

The SMP allows you to manage incidents manually or automatically by using a correlation rule. It automatically sends an email when an incident is created. This is useful when you want to treat the incident with certain follow-up actions (e.g. through an external application).

This chapter covers the configuration of both the SMP and Serio application, enabling them to communicate by e-mail with each other.

Figure 137 Principles



Example

```
--[ SMP URL ]-----------------------------------------

SRV_ESMS:PORT_NUMBER/ExaProtect/incident/IncidentSummary.jsf?entered_id=712

--[ Summary ]-----------------------------------------

An incident “Last test for Serio” with severity “medium” was created by the user
“admin”

--[ Description ]-------------------------------------

This is the last email for testing Serio's

--[ Contacts ]----------------------------------------

admin - admin@company.com

usercompany - usercompany@ company.com

user1 - user1@corp.com

--[ SLA ]---------------------------------------------

No Sla

--[ Equipment ]---------------------------------------

EFO

--[ Alerts ]------------------------------------------

No 136174 : Correlation rule without classification name

No 136192 : Correlation rule without classification name

No 136179 : Correlation rule without classification name

--[ Source ]------------------------------------------

--[ Target ]------------------------------------------

--[ Expected Actions ]--------------------------------

System off-line

Security Software installed - Exaprotect

--[ Completed Actions ]-------------------------------

admin : Antivirus - updated

admin : Changes of Policy

--[ Attack Methods ]----------------------------------

Scan

Deny of service :

Malformed packets

@@/issuetype/MSM/@@

@@/problemarea/Msm/@@

@@/priority/P2/@@

@@/impact/P2 default/@@

@@/status/Active/@@

@@/item/admin/@@
```

@@/customerref/MSMID:712/@@

@@/customeremail/admin@company.com/@@

Serio Helpdesk

There are two kinds of e-mail messages:

- outgoing messages (They are sent by the SMP): they are necessary to create the incidents. The subject of the message is only a description of the content and is not mandatory.
- incoming messages (They are sent by the external server): they update the priority of the incident and status. If the new status is closed, the incident is closed. The subject must contain the incident ID and some words or numbers. The variables necessary to understand the messages are contained in the file: `exa_cerberus.properties`.

First part - Subject

Example

```
--[ SMP URL ]-----------------------------------------

SRV_ESMS:PORT_NUMBER/ExaProtect/incident/IncidentSummary.jsf?entered_id=712

--[ Summary ]-----------------------------------------

An incident “Last test for Serio” with severity “medium” was created by the user

“admin”

--[ Description ]-------------------------------------

This is the last email for testing Serio's

--[ Contacts ]----------------------------------------

admin - admin@company.com

usercompany - usercompany@ company.com

user1 - user1@corp.com

--[ SLA ]---------------------------------------------

No Sla

--[ Equipment ]---------------------------------------

EFO
```

--[Alerts]----------

No 136174 : Correlation rule without classification name

```
No 136192 : Correlation rule without classification name

No 136179 : Correlation rule without classification name

--[ Source ]------------------------------------------

--[ Target ]------------------------------------------

--[ Expected Actions ]--------------------------------

System off-line

Security Software installed - Exaprotect

--[ Completed Actions ]-------------------------------
```

```
admin : Antivirus - updated

admin : Changes of Policy

--[ Attack Methods ]-------------------------------------

Scan

Deny of service :

Malformed packets
```

Description

Entering a subject of a message is not compulsory. However, it is recommended to enter a topic for a better understanding.

Each time the message is modified (forwarded, replied…etc), the subject title evolves. You may obtain something like:

```
Subject: Re: [Cisco 12345] Microsoft:9874 MSMID:343 About your call
```

- Separating characters between `MSMID` and the incident ID such as # must be avoided. It can create a conflict with other systems. The whole string must not contain the 'space' character.
- the `MSMID:nnn` will be sent to SEM in the subject title line in all the replies sent by SERIO.

Second Part - Body

Example

@@/issuetype/MSM/@@

@@/problemarea/Msm/@@

@@/priority/P2/@@

@@/impact/P2 default/@@

@@/status/Active/@@

@@/item/admin/@@

@@/customerref/MSMID:712/@@

@@/customeremail/admin@company.com/@@

Description

@@/issuetype/MSM/@@

This is the type of issue raised by the incident. This information comes from the configuration file.

@@/problemarea/Msm/@@

This is the context of the problem, which generated an incident. This information comes from the configuration file.

@@/priority/P2/@@

This is the priority of the incident. This information comes from the configuration file.

@@/impact/P2 default/@@

This is the impact of the incident. This information comes from the configuration file.

@@/status/Active/@@

This is the status of the incident. This information comes from the configuration file.

@@/item/admin/@@

This is the login ID of the user who created/generated the incident. This information comes from the configuration file.

@@/customerref/MSMID:712/@@

This is the incident number. This information comes from the configuration file.

@@/customeremail/admin@company.com/@@

This is the customer e-mail address (selected when the incident is created). This information comes from the configuration file.

Incoming Message

Example

Regex : ".*\[(\w+)#(\w+)\].*\s(\d+)"

Subject : "Re: [cisco#12345] microsoft:9874 Regarding your call MSMID : 343"

External Queue : "cisco"

External ID : "12345"

Exaprotect ID : "343"

Regex : ".*\[(\w+)\s+(\w+)\].*MSMID:(\d+)\s*.*"

Subject : "Re: [cisco 12345] microsoft:9874 MSMID:343 Regarding your call"

External Queue : "cisco"

External ID : "12345"

Exaprotect ID : "343"

Description

When the option is activated, the SMP sends an e-mail to the ticketing tool to indicate that an incident occurred.

The ticketing tool must send an answer to the incident. In the answer, the incident ID must be displayed. This ID has been defined in the configuration file (regex file).

Example of an Answer from SERIO

```
external.to.esms.subject.regex=.*\\[(\\w+)\#(\\w+)].*\\s(\\d*)
```

If there is no answer from the ticketing tool, it means there is a technical problem. Then, the SMP sends another e-mail to the ticketing tool as if an incident has been opened. The subject is the initial subject.

Example of an Answer from the SMP if there is no answer from the ticketing tool

```
esms.to.external.subject.format=Incident SMS ID : {incidentID}
```

If there is an answer from the ticketing tool, then, when an update is performed on the incident, the subject of the incident is always sent.

Example of an Answer from the SMP if there is an answer from the ticketing tool

```
esms.to.external.subject.reply.format=Re: Incident
```

[{externalQueueName}\#{externalId}] SMS ID : {incidentID}

SOAP Server

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

The generated incident is available in XML format in the Incident summary. Any generated incident in Security Event Manager can be closed remotely with the help of a web request. There is no need to close it from the Web Console.

Pre-requisites

- The remote SOAP server must be reachable
- The server must be up and running
- Intermediate firewalls must be correctly configured

Requirements

The remote SOAP server is using:

- the definition of the methods provided in EventManager 3.3 release.
- the IODEF version provided in EventManager 3.3 release (RFC 5070).

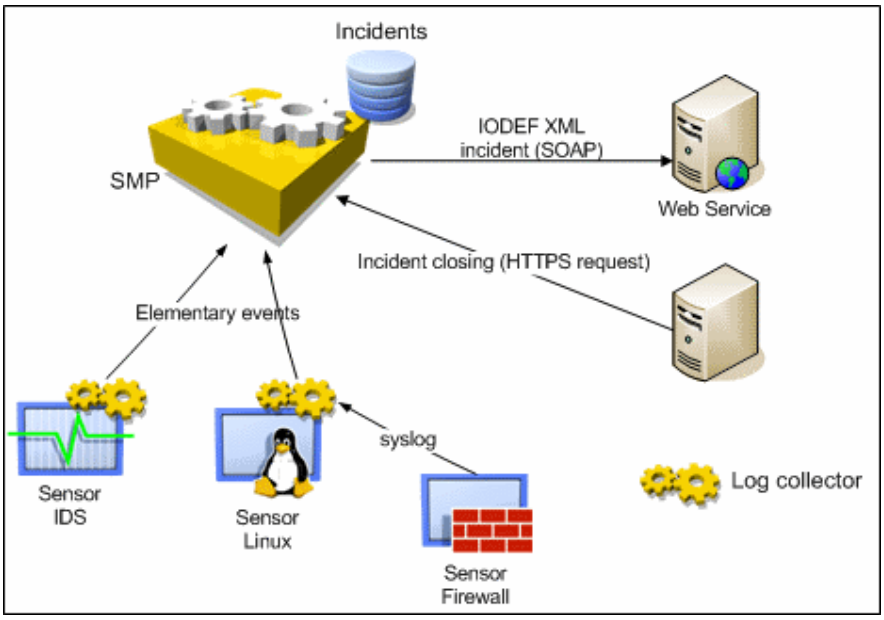
Limitations

Generating and sending “many” incidents in a short time period (especially when automatically sent from the correlation engine) can:

- decrease the overall performance of the system (less EPS processed).
- reduce the network available bandwidth (IODEF through XML being quite heavy).

Moreover, as the notifications rely on the TCP protocol, if the remote SOAP server is overloaded, it can prevent the SMP from sending the notifications in real time. Thus, the notifications must be spooled. This spool has a limited size, which may provoke the loss of notification information.

Figure 138 Overall Network Architecture



Sending Incidents to a SOAP Server

Configuring the SOAP Server

This screen aims at allowing the administrator:

- to activate/deactivate the feature (checkbox in the "Incident server" section).
- to enter the remote server configuration information, i.e. url and parameters.
- to test the connectivity with the remote SOAP server.
- to synchronize the SMP and the SOAP servers (sending of all pending open incidents).

To access this screen, go to **Configuration > External Servers**.

For more information on the Web Console configuration, refer to the User Guide - section Incident Notification.

> **Note:** The Generated IODEF XML incident screen allows the user to directly see the incident in XML format. To access this screen, go to Incident Monitoring > Incident Description > Get IODEF XML incident.

Defining the Incident Parameters from the Correlation Engine

The screen **Incident creation on correlation rule/scenario** allows the user to define the incident when this latter is raised from the correlation engine.

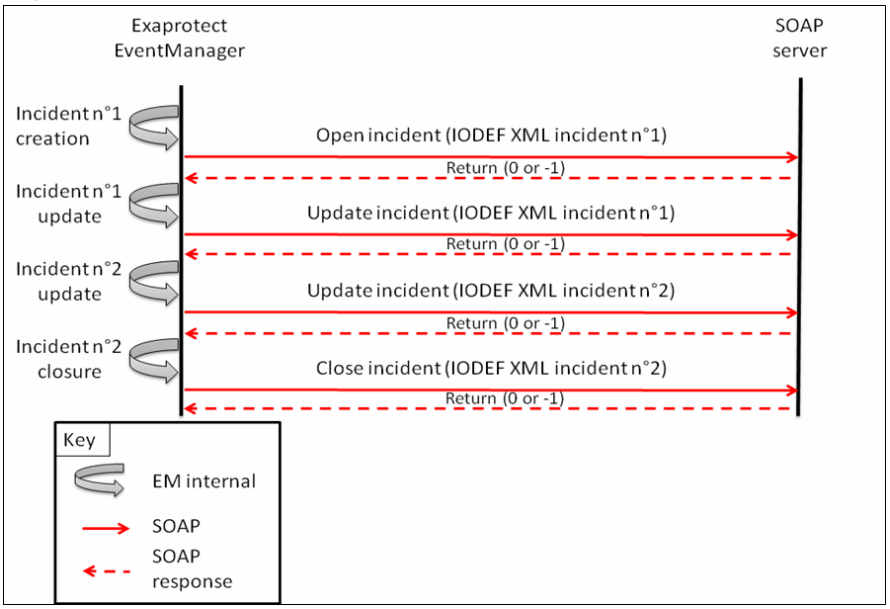
To access it:

1. go to **Event Management > Correlation Policy.**
2. click on a correlation rule/scenario.
3. click on the **Actions** tab and select **Create an incident.**
4. select the **Incident** tab**.**

Sending Incidents Remotely

Whenever an incident needs to be sent (because it has been created, updated or closed), the remote method is invoked.

Figure 139 SEM - SOAP server data flow



SOAP is a protocol that allows executing methods on a remote host (RPC).

The RPC methods that are used to exchange information with the SOAP server are defined in the **soapIncidentServer.wsdl** The exhaustive list of allowed methods to be executed is:

OpenIncidents(IODEF-Document)

This method sends one to several newly created incidents to the SOAP server.

The IODEF-Document contains one to several IODEF incidents as defined in the IODEF RFC (5070).

UpdateIncidents(IODEF-Document)

This method sends one to several updated incidents to the SOAP server.

The IODEF-Document contains one to several IODEF incidents as defined in the IODEF RFC (5070).

CloseIncidents(IODEF-Document)

This method sends one to several closed incidents to the SOAP server.

The IODEF-Document contains one to several IODEF incidents as defined in the IODEF RFC (5070).

SynchronizeIncidents(synchronization_ID, TotalNumberOfOpenedIncidents, RemainingIncidents, IODEF-Document)

This method sends one to several open incidents to the SOAP server. This allows the SOAP server to know all open incidents in SEM. The IODEF-Document contains one to several IODEF incidents as defined in the IODEF RFC (5070).

The parameters are:

- synchronization_ID: a random character string to identify the synchronization.
- the total number of opened incidents that will be sent.
- the number of remaining incidents to be sent during this synchronization (useful in case the messages are split in multiple IODEF-Documents).
- the IODEF-Document containing the incidents.

The response contains the synchronization_ID.

TestConnectivity()

This method checks that the remote server answers back, i.e. it is up and listening.

> **Note:** Those methods are defined in the soapIncidentServer.wsdl file.

In response to all those method, a “return” is sent back, indicating the outcome of the method.

The possible values of this return code are:

- 0 : OK
- -1 : NOK

Sending IODEF Incidents

Exchange Format

The incidents are exchanged in IODEF format described in XML language – compliant with the RFC 5070.

Exchange Protocol

The incidents that are opened, updated or closed in SEM are sent to the remote server using the SOAP (Simple Object Access Protocol) protocol over HTTP. Only non secure connections are available.

Incidents Format and Content

The information contained in the incidents remains the same except for the assessment impact type.

New possible values:

- admin
- dos
- file
- recon
- user
- other
- extortion
- info leak
- misconfiguration
- policy
- social engineering

- unknown

Inheritance Behavior

The incident automatically inherits from attributes of the underlying alerts or aggregated events.

Attributes are:

- Log sources
- Sources/targets
- Contacts

Manual Creation/Update of an Incident

The incident comes from the Acknowledgment of Alerts

The alerts' attributes are automatically added to the incident. These attributes can directly be modified by the user.

The incident comes from the correlation engine

In any case, the contacts of the incident are defined by the "Add log source contacts", "Add source contacts" and "Add target contacts" options.

The incident automatically inherits from the elements attributes at the input of the correlation engine (Aggregated Events or Alert) that matched the correlation rule/scenario. In most cases, this is an Aggregated Event. If an alert is "reinjected in the correlation engine" then, this is the alert (and not the underlying Aggregated events).

Each time a new aggregated event or alert matches the correlation rule/scenario, its attributes are added to the incident.

Each time a coming aggregated event, which matched the correlation rule) is updated, its attributes are added to the incident.

Auditable Logs

This type of logs allows storing action's description in logs.

admin.log

Activation/Deactivation of the feature

```
Incident soap sending feature enabled : server url {url}
Incident soap sending feature disabled
```

activity.log

Connection successful (first time messages are sent after a disconnection)

```
Connected to soap SOAP server : {url}
```

This message must be only written once

Connection error

```
Cannot connect to soap SOAP server : {url}
```

This message must be only written once

Remote SOAP method invocation error

```
Error {error_id} when invoking {method} on server {url}
```

This message must be only written once

Those 2 messages must be parsed by the local log collector

When the spool is full and some incidents need to be deleted from the spool

```
Incident spool is full - incident {n°}{status:created/updated/
deleted} is removed from the spool and will not be sent
```

Incident server returns an internal error (HTTP 5xx), the incident will not be sent again

```
Incident server returns an internal error {error_n°} – incident
{n°}{status:created/updated/deleted} will not be sent again
```

smp.log

Synchronization of the incidents

```
Incidents synchronization: update notifications sent to server
{url}
```

smp_errors.log

Sending of new/updated/closed incidents

(DEBUG MODE ONLY)

```
New incident #{n°} sent to SOAP server : {url} Updated incident
#{n°} sent to SOAP server : {url} Closed incident #{n°} sent to SOAP
server : {url}
```

Addition of new incidents parameters to be defined in the correlation rules/scenarios

All the following parameters can be statically (list, checkbox or text area) defined in the incident creation action of a correlation rule/scenario:

- Incident title
- Incident category
- Incident description
- Incident contact
- Update incident every (alerts)
- Add log source contacts
- Add source contacts
- Add target contacts
- Severity
- Switch source and target node
- Switch source and target service

The following parameters must be added to the list:

- Assessment- Impact-completion
- Success/failed

- Assessment- Impact-type
- Assessment-Confidence
- Integer value from 0 to 100 (steps of 10)

IODEF fields handling – IODEF incidents to be sent

Only one IODEF event data is contained in every incident.

Here is a mapping between the incident fields and the corresponding IODEF ones (that must be sent):

Field	IODEF field	Remark
	IODEf Document	
Incident ID	Incident ID + attribute name = “EventManager”	
Detect time	Detect time	
StartTime	StartTime	
Description	Description	
Contact	Contact	
Assessment Impact/ TimeImpact/ MonetaryImpact	Assessment Impact/ TimeImpact/ MonetaryImpact	
Confidence	Assessment Confidence	Only numeric values
Severity	Assessment Impact severity	Unknown and info severity are converted to low
Impact type	Assessment Impact type	SEE BELOW
Completion	Assessment Impact completion	
Source	Flow-System (category = source)	Node contains node names & addresses Service contains service ports Etc.
Target	Flow-System (category = target)	
Log source	Flow-System (category = sensor)	
Actions	Expectations	Everything put in “ext-value”
History	History	

Functions triggering

The incidents are sent to the SOAP server when each of the following operations occurs:

Table 8 Functions triggering - New/updated/closed incident sending

Action	From the GUI	From the correlation engine
Creation	X	X

Table 8 Functions triggering - New/updated/closed incident sending

Action	From the GUI	From the correlation engine
Closure	X	N/A
Update	X	X

The incident creation and closure notifications are sent as soon as they occur (asynchronous treatment): the incident is put in a queue pending to be processed.

In the case of an update, a minimum amount of time between two updates of the same incident must be defined in the configuration.

Reopen incident handling

If an incident is reopened, an open notification is sent.

The Incident ID used for this new open notification is the ID of the initial incident.

Update incident handling

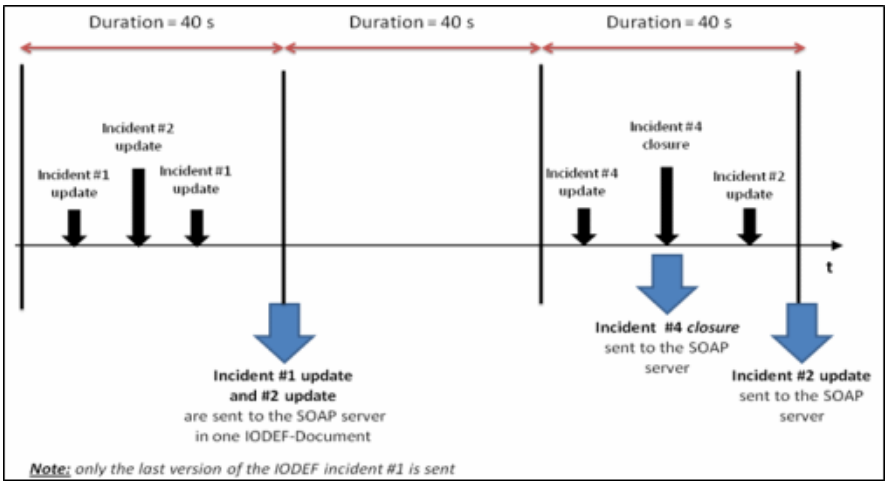
In order to avoid overloading the network and different involved modules, all the incidents updates will not be sent. The updates of all the incidents will be sent every X seconds where X is defined as below.

Description	Value
Minimum amount of time	30 sec
Maximum amount of time	3600 sec (1h)
Default amount of time	60 sec

Technically, every X seconds, the SMP will check all the incidents that were updated since the last update sending. Then, it will send all the updated incidents in an IODEF-Document. If the incident is closed before the update is sent:

- the closure notification is sent in real time
- the update notification IS NOT SENT

Figure 140 Incident updates example



Errors Handling

A spool mechanism will be implemented in case the incidents cannot be sent.

Spool

Table 9 Characteristics of the spools

Description	Default Value
Length (in incidents)	1000 (1) - if the spool is full, the oldest incidents are deleted from the spool
Content	The id of the incident AND the action (create/update/close)
Storage	In RAM (2)

Table 10 Characteristics of the retries

Description	Default Value
Time between 2 connection tries	60 seconds (1)

(1) These parameters can be defined in the **exa_incident.properties** file

(2) To avoid losing incident notifications if the runtime is stopped, a “synchronize” link will be available in the “Incident server” configuration page.

If the creation of an incident and the update of the same incident must be spooled, only the update is kept.

If the creation of an incident and the closure of the same incident must be spooled, the IODEF status of the opened incident can be “closed” (as the incident itself was closed before sending it).

Synchronize function

A “synchronize incidents” button is available in the Incident server configuration page. This button allows the complete synchronization between the SMP and the remote SOAP server: a **synchronize incidents** notification is sent to the remote SOAP server.

This notification contains:

- A synchronization ID (characters)
- The total number of open incidents (that will be sent)
- The number of incidents already sent during this synchronization
- The IODEF-Document containing all open incidents

Note that the incidents will be sent by **groups of 100 (defined in the properties file)**.

If the remote server sends a -1 return, the synchronization stops.

Thanks to it, both servers (EventManager and SOAP) know the open incident at a given time.

Methods execution errors

SOAP methods return code

The behavior depends on the return code:

Table 11 SOAP methods return code

Return code	Action
0	OK (incident sent)
-1	Spool

Caution: In the case of the incidents synchronization, a -1 return will stop the sending of incidents.

HTTP response

The behavior depends on the response:

Table 12 HTTP response

HTTP response Action	Action
2xx	OK (incident sent)
4xx (Client error - e.g. not found)	Spool
5xx (Server error)	Do not retry to send (to avoid crashing the server)

SOAP server unreachable / connection to SOAP server impossible

- In such a case, all the incidents are kept in the spool.

Configuration File

The configuration of the feature is stored in:

`/home/exaprotect/conf/{instance}/exa_incident.properties`

The following parameters will be described:

- feature enabled/disabled:
  `soap.use`
- the SOAP server URL:
  `soap.server.url`
- The duration between 2 update notifications:
  `soap.notification.period`
- The number of incidents kept in spool:
  `soap.spool.size.max`
- The time period (in seconds) between 2 sending retries (in case of error):
  `soap.error.retry.period`

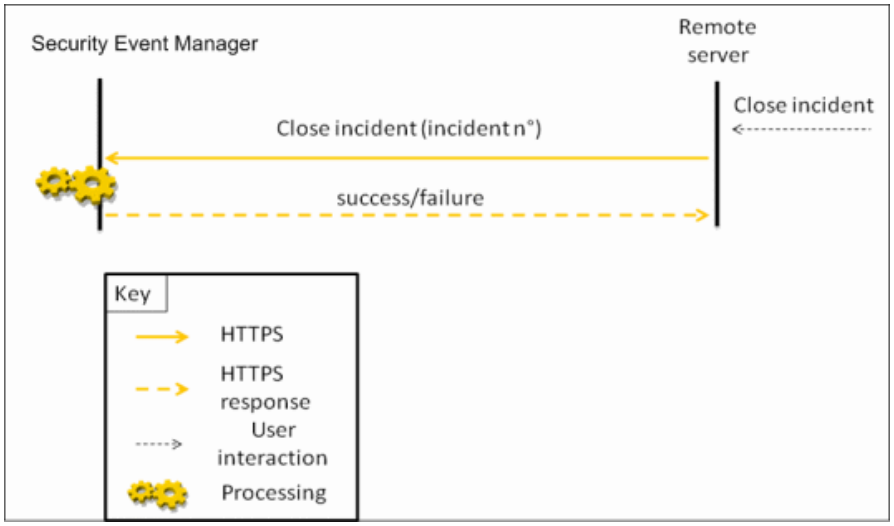
- The maximum number of incidents sent in an IODEF-document:
  `soap.document.incident.nb.max`

- The connection timeout (in seconds):
  `soap.connection.timeout`

Incident Closing

Once the request has been received, the incident is closed. A response is sent, which indicates the outcome is sent back to the remote server.

Figure 141 Incident closing from a remote host - data flow



Incident closing from a remote host

The incident closing request is performed through the HTTPS protocol.

Incident closing triggering

The incident can be closed from a remote host without using the Web Console. The following HTTPS request needs to be sent which specifies the incident id:

https://{SEM_hostname}:{SEM_port}/ExaProtect/incident/close?id={incidentID}

> **Note:** The user that performs the request needs to be authenticated.

Authentication methods

To perform the closure, the user MUST be authenticated with his credentials (admin rights at least) that can be provided:

- as parameters of the URL

```
?USER=test&PASS=my_password
```

- in the form (POST method)
- through the login screen before = session information stored in a cookie

Incident closing response

In response to the closure, the SMP sends back the HTTP responses containing:

- “OK” if the incident has closed successfully
- “ERROR : {description}” if the incident could not be closed

The possible values of description are:

- Incident ID not found
- Error while closing the incident

Direct Access to the List of Incidents

To rapidly display the list of filtered incidents only with the ID, you can use the following URL in your browser (replace the content between { } by the incident ID):

https://{SEM_IP}:{port}/ExaProtect/?IncidentFilter=incident.incident:="{id}"

Chapter 6 - Sending Mails as Soon as an Event Occurs

This part of the documentation describes how to define a correlation rule that will allow you to automatically receive a mail as soon as an event occurs.

You will learn how to:

- fill the configuration file.
- create a relevant correlation rule.

Filling the Configuration File

You must first configure a file that comprises all the necessary data for sending mails.

The file is called exa_mail.properties and is located at /home/exaprotect/conf/INSTANCE/.

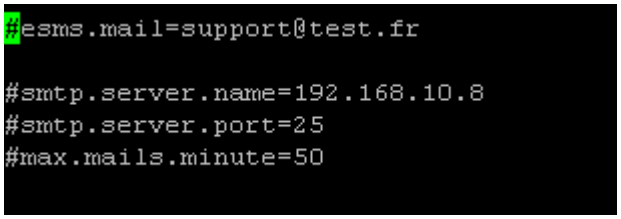
1. Activate the root account.

2. Connect either in SSH mode or Console mode.

3. Open the file.

The following screen is displayed:

Figure 142 Default File Configuration



4. Erase the # character in front of the fields that you want to customize. The # character indicates that the command line (for example: #smtp.server=25) is considered as a comment.

5. Enter the sender's address in the esms.mail field. This field is optional. It is recommended not to use the default value but to enter a customized value.

> **Note:** If the field is followed by a '#' character, it has a default value.

6. Enter the IP address or DNS name of the sent mail server in the smtp.server.name field. This field is mandatory.

7. Enter the port used by the SMTP server in the `smtp.server.port` field. This field is mandatory.

8. Enter the maximum number of mails per minute you want to receive in the `max.mails.minute` field. This field is optional. This option is useful to filter the number of sent mails and then avoid overloading the server.

Note that if the field is followed by a '#' character, the value must be set to 10.

Once the modification applied, you must restart the instance by entering the following command:

```
/etc/init.d/exa_runtime_INSTANCE restart
```

Caution: All fields must be filled in, even with an empty chain of characters.

Creating a Rule

Now you must create a correlation rule that will allow you to automatically receive a mail when an event is detected. Let us take the example of a mail sent when an event with a HIGH criticality is generated.

Prerequesites: contact information must be entered in the Asset database.

Caution: When you configure the contact in the Contact Details screen (Configuration > Asset Database > Contacts), make sure there is a consistency between the name and the recipient's mail. Indeed, the name will be displayed in the list of contacts when defining a rule.

To know how to define a rule, please refer to the User Guide.

Figure 143 Example of a Rule - General tab

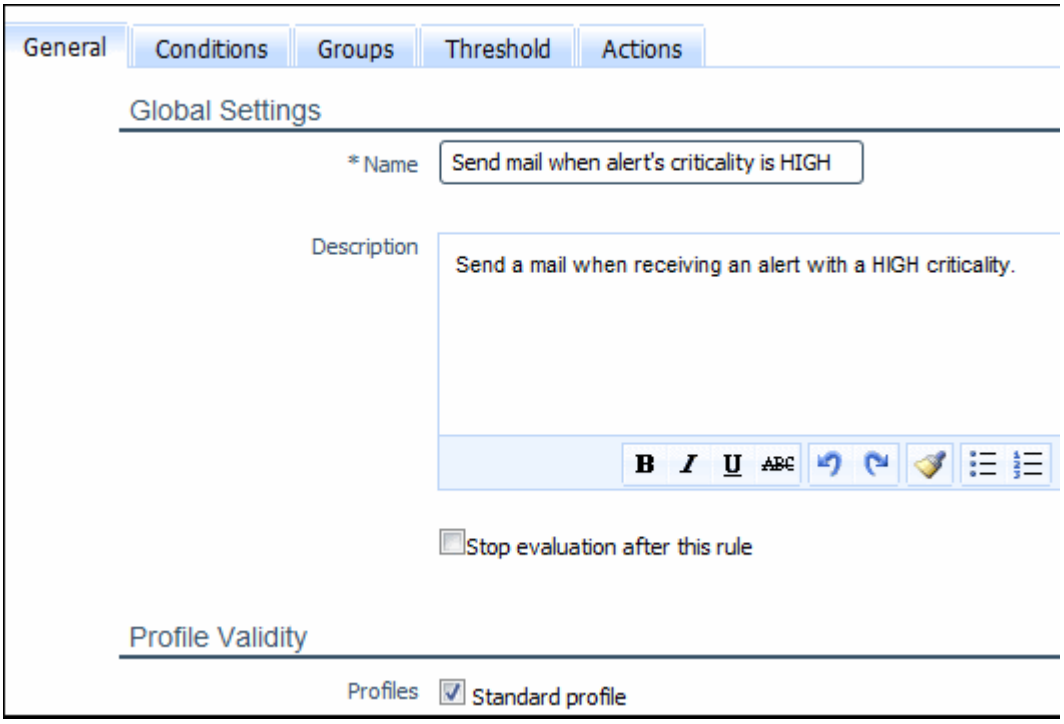
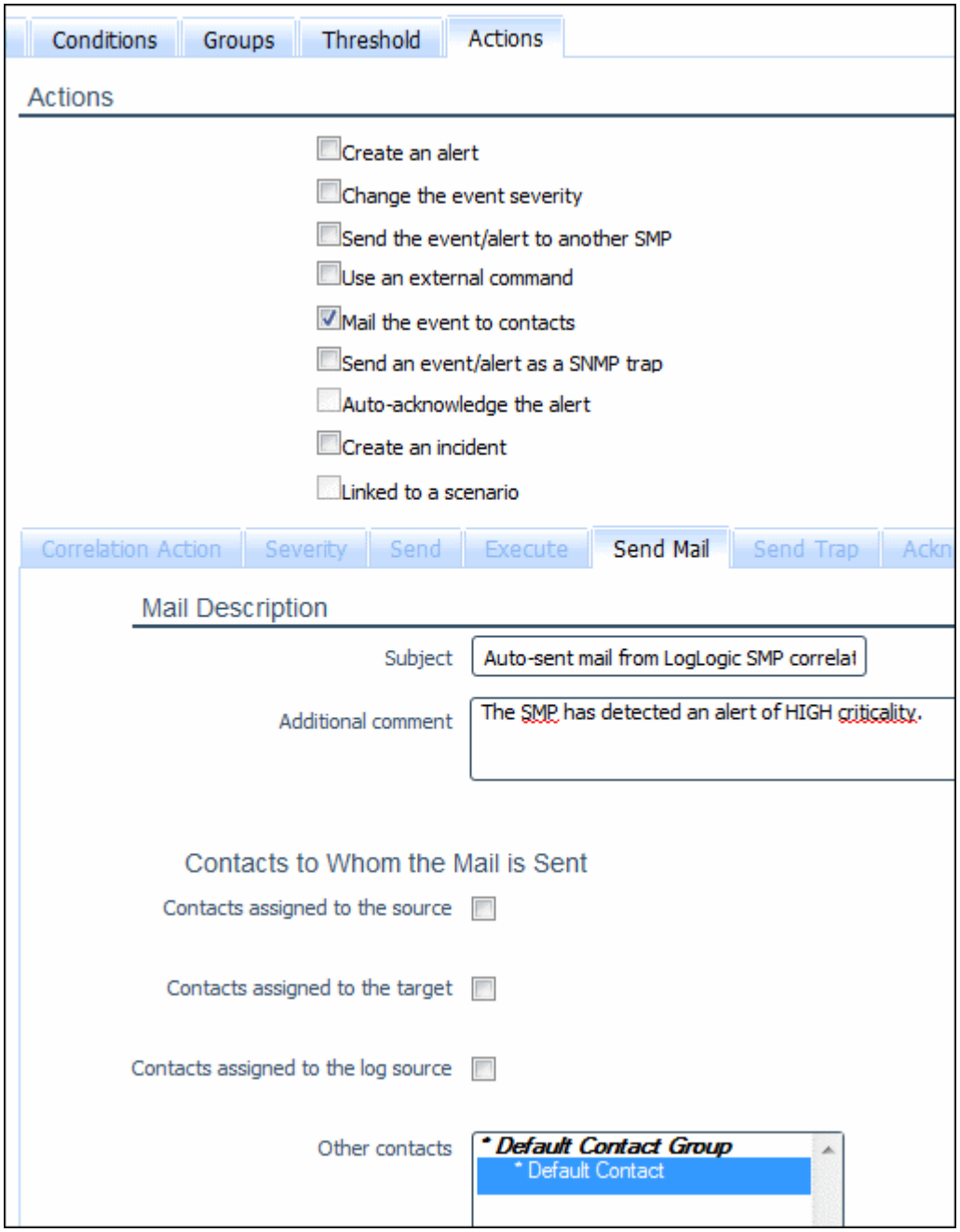


Figure 144 Example of a Rule - Actions tab



Please note that in this example:

- The threshold and the period allow you to determine when the mail will be sent. Only a mail will be sent, no other action will be performed.
- The sender is the person configured earlier in the exa_mail.properties file.
- The subject is an optional comment.

- The recipient can be either:
  - a contact assigned to the source: this option allows the automatic sending of the mail to the person who fulfills the following requirements:
  - His/Her mail address must be entered under Asset Database > Contacts.
  - S/he must belong to a contact group (Asset Database > Contact Groups).
  - The contact group must have a host (Asset Database > Hosts). The host must belong to a group of hosts and must be considered as source.
  - a contact assigned to the target: the mail will be sent to the person whose mail is associated with the target.
  - a contact assigned to the equipment.
  - other contacts: this field allows you to enter the recipients of the mail, no matter the target, source or equipment. Several persons can be selected at the same time.

In our example, only one person will receive the mail.

Example of a Sent Mail

Here is the example of a sent mail's content:

```
SSH Remote root login
************************
Dates
 * Creation: 2008-05-07 16:26:30
 * Detection: 2008-05-07 16:26:29
 * Analyzer: 2008-05-07 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
************************
```

Chapter 7 - Appendix

Understanding Scripts, Configuration and Log Files on an SMP Server

Introduction

This section presents an overview of the scripts, configuration and log files on the SMP server. The entries in this section are not an exhaustive list, but comprise the most important ones.

There are three main parts to this section:

- scripts
- log files
- configuration files

Lastly, you will find a subsection presenting the monitoring functionality.

> **Caution:** With regard to the configuration files, it is necessary to pay careful attention to their manipulation because the least change can imperil the stability of the server. If such actions are carried out without prior agreement from TIBCO LogLogic® or without having been requested by our technical support, they will entail the annulment of the maintenance contract. The same applies to changes applied to scripts.

Reminder:

The SMP server file architecture is listed in the table below.

Table 13 SMP Server File Architecture

/usr/local/exaprotect/	binary files
/home/exaprotect/	configuration files
/var/lib/exaprotect/	database, log files, archives

Scripts

There are several available scripts for debugging problems on the SMP server. In this section, you will find a description of each available script and its usage guidelines. These debugging scripts can also be launched in the background to avoid disrupting the SSH console connection.

> **Caution:** You should only execute any of the debugging scripts if you are certain they are appropriate for your needs. By using a script inappropriately, you could cause damage to the server and/or the system, having, as a consequence, the annulment of the maintenance contract. Therefore, read the script documentation carefully and use the scripts only as indicated.

If you have any questions, please contact our technical support **before** executing any of the scripts.

Scripts Folder

A part of the scripts is located in **/home/exaprotect/scripts/**

The table below lists the available sub-folders with their scripts and the scripts located in the <root> folder.

Table 14 Scripts folder

Folder	Script	Description
<in the root folder>	exa_iptables.sh	This script is used to configure the iptable's.
	send_mail.pl	This file allows you to configure the sending of an E-mail, after you have set the configuration parameters in the file /home/exaprotect/conf/INSTANCE/exa_mail.properties.
	send_trap_snmp.pl	Same as above, except that it refers to SNMP traps.
	service_mgnt.sh	This script allows you to launch the services from the GUI.
export		This folder will contain the export scripts for raw log and elementary event archives and backup (user scripts).
odt	manage_files.pl	Script for managing raw logs and elementary events. The actions are compress, encrypt, decrypt, move and remove.
	manage_gpg.sh	Script for managing gpg keys for raw logs.
	manage_rawlog.pl	Script for managing the archive of raw logs.
update	check_updatetunnel.sh	Script for checking the ssh channel between the update site and the SMP server.
	extract_privkey.sh	Script for installing the p12 certificate via the GUI.
	manage_pkg.pl	Script for managing the check of the updates and the SMP update server.

Other Folder

A part of the scripts is located in:
/usr/local/exaprotect-setup/scripts/others/

The table below lists the available sub-folders and their scripts and the scripts located in the <root> folder.

Table 15 Other folder

Folder	Script	Description
<in the root folder>	update_ruleset.pl	
	service_mgnt.sh	This script allows you to launch the services from the GUI.
	send_trap_snmp.pl	This script allows you to manage the sending of an SNMP trap.
	send_mail.pl	This file allows you to configure the sending of an E-mail, after you have set the configuration parameters in the file /home/exaprotect/conf/INSTANCE/exa_mail.properties.
	exa_iptables.sh	This script is used to configure the iptable's.
	criston_import.sh	
odt	manage_files.pl	Script for managing raw logs and elementary events.
	manage_gpg.sh	Script for managing keys for raw logs.
	manage_rawlog.pl	Script for managing the archive of raw logs.

Table 15 Other folder

Folder	Script	Description
update	check_updatetunnel.sh	Script for checking the ssh channel between the update site and the SMP server.
	extract_privkey.sh	Script for installing the p12 certificate via the GUI.
	manage_pkg.pl	Script for managing the check of the updates and the SMP update server.
launcher	"exa_dbmanager.sh"	Normally, you should not need to use this script, which allows you to manage data in the database. Instead, you should use the GUI menus to execute these database management actions.
	exa_do_backup.sh	Generates a backup of the configuration.
	exa_do_tat.sh	Executes a manual process for reporting table computation.
	exa_unzip.sh	Unzips or zips files.
recover	"ack_events.pl"	Process in a quick and complete manner all the events and alerts which are waiting to be processed or which are disrupting the functioning of the SMP server. See description below this table.
	"delete_events.pl"	This script will delete all alerts that have not been correctly deleted by an automatic process.
	dump_tat.pl	Allows the dumping of the reporting tables.
	init_report_conf.pl	DO NOT USE as you may lose all your reports.. Reinitialize the reports configuration.
	init_report_grant.pl	Gives the use the access rights to the reports.
	reinstall_agent.pl	Reinstall the local agent completely.
utils	"set_debug.sh"	Use this script to put the Log Collector, the reporting module or the server in debug mode.
	"set_slow_queries.sh"	Use this script to activate the real time storage of requests that take more than one second to be executed.
	"sql_analyze_table.pl"	Use this script to recalculate the database index. By default, this operation will be launched by MySQL at the time of a restart.
	"sql-fullprocesslist.pl"	Use this script to launch an analysis regarding the SQL requests that take more than one second to execute.
	"sql.sh"	Use this script to launch the MySQL command utility that allows you to execute database requests.

ack_events.pl

Description

This script will process in a quick and complete manner all the events and alerts which are waiting to be processed or which are disrupting the functioning of the SMP server.

In order to increase its efficiency, this script will automatically stop all the active TIBCO LogLogic® services on the server, except for the MySQL database management.

Usage

./ack_events.pl --client=<instance> <-i|-u|-t>

Table 16 ack_events.pl

Options	Description
h | help	show this message
d | debug	debug mode
c | client=<instance>	instance name
i | init	init correlator queue (no acknowledgment)
u | untreated	acknowledge all untreated events
t | treated	acknowledge all treated events

You will have to indicate the target instance name.

Table 17 Optional Parameters

Parameter	Explanation
init	This parameter will ensure all non-processed events will pass through the correlation engine as elementary events. It will not be possible to later correlate these same events. This option should only be used in the case of a less extensive correlation queue. Its value is displayed in the Correlation Queue Length Chart, found in the chart display screen, the last chart on the right, bottom row (Alert Monitoring -> Help -> Live Explorer -> Last Hour/Last Day). **Caution:** Be aware that if you have more than 100,000 events to be processed, the list containing the current alerts will be too extensive and the display will be limited to 100,000 events, which may cause performance to slow down.
untreated	This option will execute the same operation as above, except that it will, in addition, acknowledge the events that are treated. Use this option when the correlation queues contain a lot more than 100,000 events.
treated	This option will execute the second part of the preceding operation. This means that all events appearing on the console (in the current view) will be acknowledged. Running this script entails the execution of several phases contained in the script.

Note: A progress bar is not displayed, therefore, you will not be able to know how long a particular phase takes. The execution time depends on the number of alerts and whether it will be necessary to process several million events. The execution should take at least an hour, although usually longer.

You will see the following result after running the above script:

Table 18 Script "ack_events.pl"

```
[root@test others]# ./ack_events.pl -c TEST -i
Stopping SMP Runtime TEST
Launching requests. Please wait, this operation
can take several minutes.
Update untreated alerts (1/1)...
done
Requests finished
Starting SMP Runtime TEST
[root@test others]# ./ack_events.pl -c TEST -t
Stopping SMP Runtime TEST
Launching requests. Please wait, this operation
can take several minutes.
Create Acknowledgment (1/3)...
done
Create link records (2/3)...
done
Update treated alerts (3/3)...
done
Requests finished
Starting SMP Runtime TEST
[root@test others]# ./ack_events.pl -c TEST -u
Launching requests. Please wait, this operation
can take several minutes.
Create Acknowledgment (1/3)...
done
Create link records (2/3)...
done
Update untreated alerts (3/3)...
done
Requests finished
Starting SMP Runtime TEST
```

delete_events.pl

Description

This script will delete all alerts that have not been correctly deleted by an automatic process. Alerts which are dated past the maximum defined date for storing alerts in the database will be deleted after the defined retention period. You will use this script to delete alerts that were not automatically deleted, for example, alerts which were defectively built following the launch of an instance when a correlation process was being executed or if the server crashed.

It is not possible to delete such alerts using the traditional GUI method (“Schedule Backup and Archiving” in Backup Configuration).

You will need to use the script in the manner indicated below.

Table 19 delete_events.pl

```
[root@test others]# ./
delete_events.pl
Usage : ./delete_events.pl
--client=<instance>
<-count|--delete>
--h|help              : show this
message
--d|debug             : debug mode
--c|client=<instance> : instance
name
--count            : count events
to be deleted
--delete             : delete the
events
```

Usage

You will have to indicate the instance name.

Table 20 Optional Parameters

Parameter	Explanation
count	This parameter will count the alerts and events that may pose problems, by not having been deleted through the normal, automatic process.
delete	This parameter will launch the deletion of the above alerts.

You will see the following result after running the above script:

Table 21 Result

[root@test others]# ./delete_events.pl -c TEST -count Launching requests. Please wait, this operation can take several minutes. Count events without correlation alert in link table (1/2)... 0 events Count correlation alert with no state (2/2)... 0 events Requests finished [root@test others]# ./delete_events.pl -c TEST -delete Launching requests. Please wait, this operation can take several minutes. Stopping SMP Runtime TEST Delete events without correlation alert in link table (1/2)... done Delete correlation alert with no state (2/2)... done Starting SMP Runtime TEST Requests finished

exa_dbmanager.sh

Description

Normally, you should not need to use this script, which allows you to manage data in the database. Instead, you should use the GUI menus to execute these database management actions.

The logs for this script will be saved to:

`/var/lib/exaprotect/logs/smp_other.log`

Usage

Table 22 exa_dbmanager.sh

Usage
- delete all alerts: ExaDbManager -c <client> -a - delete alerts between 2 dates: ExaDbManager -c <client> -a -y 'YYYY-MM-DD HH:MM:SS' -z 'YYYY-MM-DD HH:MM:SS' - backup database (all alerts): ExaDbManager -c <client> -b <zip name> - backup database (only alerts between the 2 dates) : ExaDbManager -c <client> -b <zip name> -y 'YYYY-MM-DD HH:MM:SS' -z 'YYYY-MM-DD HH:MM:SS' - drop all tables: ExaDbManager -c <client> -o - restore all data (tables must be empty): ExaDbManager -c <client> -r <zip name >

The table below explains the various ways of using the ExaDbManager script.

Table 23 Available Options

Option	Description
Delete all alerts	This option makes it possible to remove all the alerts contained in the database. This option is usually valid. **Note:** this operation generally requires several hours or even days depending on the number of alerts contained in the database. It is thus necessary to launch its execution directly through the console or via a tool which allows you to put the request in the background, otherwise you will risk interrupting its execution in the event of the terminal being cut off. You will also find an option to execute this task in the administration menu.
Delete alerts between 2 dates	Same as above but allowing you to specify a date range.
Backup database (all alerts)	This option is obsolete and it will not work. Do not use it.
Backup database (only alerts between 2 dates)	Same as for the option above.
Drop all tables	Do not use this option unless absolutely necessary and only after being instructed to do so by our technical support.
Restore all data	You should not use this option.

send_trap_snmp.pl

This script allows you to manage the sending of an SNMP trap. For example, this script could be used to send an SNMP trap at the time of the creation of an incident. In this case, you would need to configure the following file:

```
/home/exaprotect/conf/INSTANCE/exa_incident.properties
```

set_debug.sh

Description

Use this script to put the Log Collector, the reporting module or the server in debug mode.

This script will save supplementary log files allowing you to better understand a particular activity on the server.

Usage

Table 24 set_debug.sh

Usage
[root@test others]# ./set_debug.sh Usage: ./set_debug.sh <on|off> <agent|runtime|report> <instance> ./set_debug.sh <on|off> <other|executor>

Table 25 Optional Parameters

Parameter	Description
On/Off	This option will set the server debug mode On or Off.
Agent | runtime | report	This option specifies which module will be put into debug mode.
Instance	Indicates the instance name.

You will see the following result after running the above script:

Table 26 Script Result

```
[root@test others]# ./set_debug.sh on agent TEST
Activate debug mode for agent TEST
Stopping SMA TEST: exa_agent_TEST.
Starting SMA TEST: exa_agent_TEST.
[root@test others]#
[root@test others]# ./set_debug.sh on runtime
TEST
Activate debug mode for runtime TEST
Stopping SMP Runtime TEST: exa_runtime_TEST.
Starting SMP Runtime TEST: exa_runtime_TEST.
[root@test others]#
[root@test others]# ./set_debug.sh off runtime
TEST
Deactivate debug mode for runtime TEST
Stopping SMP Runtime TEST: exa_runtime_TEST.
Starting SMP Runtime TEST: exa_runtime_TEST.
```

In the example above, this script will automatically stop the Log Collector, then modify the following file:

/home/exaprotect/agent_INSTANCENAME/conf/agent_log4j.properties

You must indicate the word “debug” (case-sensitive) in two distinct places.

This action will activate the debug mode. The debugging information will be saved to the file “sma_errors.log,” which is found at:

/var/lib/exaprotect/logs/INSTANCENAME/sma_errors.log

The contents of the file - when the debug mode is activated - is the following: the word “debug” appears on the first line (indicating that the debug mode should be activated), and on the last line (the debugging information is being redirected to the above log file and not to “smp.log”).

Table 27 File Contents

	log4j.rootLogger=debug, EXA_AGENT, EXA_AGENT_ERRORS log4j.appender.EXA_AGENT=org.apache.log4j.RollingFileAppender log4j.appender.EXA_AGENT.File=${eas.dir}/logs/sma.log log4j.appender.EXA_AGENT.layout=org.apache.log4j.PatternLayout log4j.appender.EXA_AGENT.layout.ConversionPattern=%d [%t] %-5p %m%n log4j.appender.EXA_AGENT.MaxFileSize=1MB log4j.appender.EXA_AGENT.MaxBackupIndex=10 log4j.appender.EXA_AGENT.Threshold=INFO log4j.appender.EXA_AGENT_ERRORS=org.apache.log4j.RollingFileAppender log4j.appender.EXA_AGENT_ERRORS.File=${eas.dir}/logs/sma_errors.log log4j.appender.EXA_AGENT_ERRORS.layout=org.apache.log4j.PatternLayout log4j.appender.EXA_AGENT_ERRORS.layout.ConversionPattern=%d [%t] %-5p %m%n log4j.appender.EXA_AGENT_ERRORS.MaxFileSize=1MB log4j.appender.EXA_AGENT_ERRORS.MaxBackupIndex=10 log4j.appender.EXA_AGENT_ERRORS.Threshold=DEBUG

set_slow_queries.sh

Description

Use this script to activate the real time storage of requests that take more than one second to be executed. These requests are saved in a file in order to be analyzed later.

This script either sets the real-time storage function On or Off.

This is the file:

/var/lib/exaprotect/logs/smp_mysql_slow_queries.log

Usage

Table 28 set_slow_queries.sh

Usage
[root@test others]# ./ set_slow_queries.sh Usage: ./set_slow_queries.sh <on|off>

You will see the following result after running the above script:

Table 29 Script Result

[root@exabench4 data]# /usr/local/ exaprotect-setup/scripts/others/ set_slow_queries.sh on Activate slow queries Stopping SMA TEST: exa_agent_TEST. Stopping SMP Runtime TEST: exa_runtime_TEST. Stopping SMP File Synchronization: exa_rsyncd. Stopping SMP Executor: exa_executor. Stopping SMP Update: exa_update was not running. Stopping SMP DataBase: Wait for mysqld to stop. exa_mysql. Starting SMP DataBase: Wait for mysqld to start exa_mysql. Starting SMP Update: FAILED. Starting SMP Executor: exa_executor. Starting SMP File Synchronization: exa_rsyncd. Starting SMP Runtime TEST: exa_runtime_TEST. Starting SMA TEST: exa_agent_TEST.

Below is an example of the file contents:

Table 30 File Contents

```
/usr/local/exaprotect/mysql/bin/mysqld,
Version: 5.0.22-pro-log. started with:

Tcp port: 3306  Unix socket: /var/lib/
exaprotect/mysql/mysql.sock

Time                 Id Command    Argument

# Time: 070301 15:21:07

# User@Host: exa_aaaaaaaaaaaa[exa_aaaaaaaaaaaa]
@ localhost [127.0.0.1]

# Query_time: 2  Lock_time: 0  Rows_sent: 210
Rows_examined: 210

use exa_TEST;

SHOW VARIABLES;

# User@Host: exa_bbbbbbbbbbbb[exa_bbbbbbbbbbbb]
@ localhost [127.0.0.1]

# Query_time: 3  Lock_time: 0  Rows_sent: 6
Rows_examined: 6

use exa_TEST;

SET timestamp=1172759211;

select count(*) /
(to_days(utc_timestamp())-to_days(min(ack_date
))) from Exa_Alert join Exa_Ack on
(cur_ack_id=ack_id);
```

sql_analyze_table.pl

Description

Use this script to recalculate the database index. By default, this operation will be launched by MySQL at the time of a restart.

This operation is automatically executed on all instances every night at 2:00 a.m.

Usage

Table 31 sql_analyze_table.pl

Usage

```
[root@test others]# ./sql_analyze_table.pl

Usage : ./sql_analyze_table.pl [ -h ] [-d <db>]
[ -a ]

-h              : show this message

-d <db>         : database name

-a              : all database defined
```

Note: The database name does not correspond to the instance name.

To obtain the database name, execute the following commands:

/usr/local/exaprotect-setup/scripts/others/sql.sh

Show databases;

You will then need to find the respective database name in the result. The name will start by "exa_" followed by the instance name.

You will see the following result after running the above script:

Table 32 Result

```
[root@test others]# /usr/local/
exaprotect-setup/scripts/others/
sql.sh
Welcome to the MySQL monitor.
Commands end with ; or \g.
Your MySQL connection id is 31 to
server version: 5.0.22-pro
Type 'help;' or '\h' for help.
Type '\c' to clear the buffer.

mysql> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| exa_TEST           |
| mysql              |
| prp_TEST           |
+--------------------+
4 rows in set (0.06 sec)
```

sql-fullprocesslist.pl

Description

Use this script to launch an analysis regarding the SQL requests that take more than one second to execute. This will allow you to discover why the GUI is taking time to post a result.

Caution: When requesting the display of information via the forensic tool or via a report, closing the window before the task's execution ends will not cancel the request. Therefore, if you launch a request, close the window, and then launch a second request, this will result in two requests being executed simultaneously by the system (the first plus the second).
You should note that MySQL can suffer overload if you request too many heavy operations for the database.

You can also monitor if a request to the database has executed correctly, such as when deleting alerts, a backup operation, etc.

Information will be displayed in the following format:

Table 33 Result

```
Id      Time     db                  Command     State
265        1     exa_TEST            Query       preparing
INSERT IGNORE INTO Exa_Alert_TmpArch (alert_id, level) SELECT alert_id,
'1' FROM Exa_Lnk_CorrAlerts WHERE correlation_alert_id IN (SELECT
alert_id FROM Exa_ALert_TmpArch WHERE level = 0) ON DUPLICATE KEY UPDATE
level = '1'
```

sql.sh

Description

Use this script to launch the MySQL command utility that allows you to execute database requests.

You should be careful about using this script because it can cause considerable damage if used incorrectly, in the event that you are not knowledgeable regarding the data model or SQL commands.

You should generally use the "exa_INSTANCENAME" database in order to execute operations referring to the alert database or pre-generated tables. It is not advisable for you to connect to the other databases.

A few usage examples are listed in the following table:

Table 34 Usage Examples

Usage	Description
show tables	This option will display all tables for the selected database.
show full processlist \G	This option will display all requests that are being executed.
show innodb status \G	This option will display information regarding the MySQL performance.
kill NumRequete	This option will interrupt the execution of the request where **NumRequete** is the request's number. The request's number can be obtained through the "show full processlist \G;" request.

Configuration Files

/home/exaprotect/conf/INSTANCE_NAME

The available files and directories are listed in the following two tables:

Table 35 /home/exaprotect/conf/INSTANCE_NAME

[root@test others]# ls /home/exaprotect/conf/INSTANCE_NAME/
agent
aggregation.rules.xml
batchReporting.tat.xml
confset
converter
correlation.properties
correlation.rules.xml
Eas_Receiver.ks
eventData.conf.xml
eventDataFiles.conf.xml
exa_backup.conf.xml
exa_cerberus.properties
exa_config.properties
exa_db.properties
exa_incident.properties
exa_instance.properties
exa_kb.properties
exa_mail.properties
exaprotect.asc
ExaProtect_log4j.properties
exaprotect.pub
exaprotect.sec
exa_reporting.properties
exa_security.properties
exa_SLA.properties
inserter.conf.xml.orig
liveReporting.tat.xml
rawData.conf.xml
rawDataFiles.conf.xml
receiver.conf.xml
replay.status.xml

Table 36 /home/exaprotect/conf/INSTANCENAME

report
ruleset
senders
skip
spooler.conf.xml
statRequest.conf.xml
tatComputedDates.data.txt
tatStatus.data.xml
tomcat.ks
users
users_backup.conf.xml

The folders are the following:

Table 37 Folders

Folder	Description
agent	This folder contains the server configuration file for the local Log Collector (communication port, Event Per Second limiter, size and number for the spool file, etc). It corresponds to the "advanced parameters" category for the localhost Log Collector.
confset	This folder contains the list for all the instance's confsets.
converter	This folder contains the list for all the instance's converters.
report	This folder contains report data referring to the instance: the configuration file (debug mode, etc), the folderswhere exported reports are saved to when a reporting task is executed, etc. The directories where PDF reports are exported are: /var/lib/exaprotect/archives/<INSTANCE_NAME>/report/pdf /var/lib/exaprotect/archives/<INSTANCE_NAME>/report/pdf/fsa /var/lib/exaprotect/archives/<INSTANCE_NAME>/report/pdf/pci-dss /var/lib/exaprotect/archives/<INSTANCE_NAME>/report/pdf/sox /var/lib/exaprotect/archives/<INSTANCE_NAME>/report/pdf/executive /var/lib/exaprotect/archives/<INSTANCE_NAME>/report/pdf/other

Table 37 Folders

Folder	Description
ruleset	This folder contains all of the instance's rulesets. The rulesets can be of different types: "db: connection to a database "kb: empty "log: connection to a log file (ruleset menu for the configuration menu) "opsec: connection to Checkpoint "rdep: empty "scanner: connection to scanner tools "welf: connection to a WELF-type file (field separated by a character, title and result separated by a character) "wmi: connection to Windows' Event Viewer.
senders	Within the framework of a server -> server configuration (an SMP server sending alerts to another server), this folder is used to store information related to this configuration. This configuration must be validated by TIBCO LogLogic® personnel before being installed.
skip	This folder contains all the instance's collection policy files.
users	This folder contains the list of users in the GUI.

There are also the following files:

- **aggregation.rules.xml**: file containing the aggregation rules and scenarios.
- **batchReporting.tat.xml**: file containing the Reporting Tables structure to be generated daily. From version 2.7.2.1 onward, there is a GUI menu option to execute the same task.
- **correlation.properties**: allows you to activate a debug mode referring to the correlation process (by default, this mode is not active). The debugging result will be saved to:

```
/var/lib/exaprotect/logs/INSTANCE/correlator.log
```

- **correlation.rules.xml**: this file contains the correlation rules and scenarios.
- **Eas_Receiver.ks**: file containing the "ks" certificate for the receiver so that it can connect to the SMP platform.
- **eventData.conf.xml**: this file contains the configuration for executing tasks for the events.
- **eventDataFiles.conf.xml**: this file contains the references for the events present on the machine (md5sum, size, etc).
- **exa_backup.conf.xml**: file containing information regarding the backup configuration and execution. Please note that this file is only a model allowing you to create the configuration file related to the instance:

```
user_backup.conf.xml
```

- **exa_cerberus.properties**: file containing connection parameters to be configured manually (and not through the GUI) in order to send the incidents created in the SEM to the Cerberus ticketing software.
- **exa_config.properties**: file containing the minimum and maximum time period from which an event must be generated if no event has been received from a connected log source.
- **exa_db.properties**: file containing information regarding the amount of data stored in the database. By default, when the database is 80% full, a message appears on the GUI. At 95%, alerts are no longer inserted in the database. After action is taken and the total used space in the database decreases below 90%, the insertion of alerts is resumed.

Table 38 exa_db.properties

Poll Delay (sec) : 2min when not in alarm, 1min else dbMonitor.slowRatePollDelay=120 dbMonitor.highRatePollDelay=60 dbMonitor.alarmStep=80 dbMonitor.restartStep=90 dbMonitor.stopStep=95

- **exa_incident.properties**: configures which script will be executed when creating, updating, or closing an incident (for example: sending an SNMP trap).
- **exa_instance.properties**: this file contains the instance's configuration, such as the GUI connection port, reporting, etc. These configurations can be accessed through the administration interface.
- **exa_kb.properties**: this file contains the matrix allowing the "business assets" to modify the criticality degree based on the initial severity level.

Table 39 exa_kb.properties

correlate.kb=yes # order for severity = info,low,medium,high correlate.criticalCriticity=info,medium,high,high correlate.highCriticity=info,low,medium,high correlate.mediumCriticity=info,low,medium,high correlate.lowCriticity=info,low,medium,high correlate.lowestCriticity=info,low,low,medium vuln.notDetectedNotVuln=yes

In this case, if we choose "critical" for the "business asset," the result for the alert severity level will be one of the following types:

- Info remains info
- Low becomes medium
- Medium becomes high
- High remains high

- **exa_mail.properties**: this file contains the necessary configuration to send an email through the platform when a rule is activated.
- **exaprotect.asc**: this file contains the TIBCO LogLogic® public key allowing the encryption of raw log files.
- **ExaProtect_log4j.properties**: this file contains the log files' redirection configuration for the files available on the server. You can also configure the debug mode through this file.

- **exaprotect.pub**: this file contains the public part of the key that allows the signing of the raw logs.
- **exaprotect.sec**: this file contains the private part of the key that allows the signing of the raw logs.
- **exa_reporting.properties**: this file contains the configuration for the time of execution for the Reporting Statistics file generation, and the number of retention days for these tables in the database. You can also use the GUI **Reporting Statistics Tables** menu option.
- **exa_security.properties**: configures the script to be executed when the current configuration profile changes (for example: a script to send an SNMP trap).
- **exa_SLA.properties**: this file allows you to configure the times when the SLA's are active. By default, the SLA's are active from 8:30 a.m. to 6:30 p.m. If an event occurs after 6:30 p.m., the expiration calculation for the SLA will start the following morning.

Table 40 exa_SLA.properties

workPeriod.monday.morning=08:30-18:30 workPeriod.tuesday.morning=08:30-18:30 workPeriod.wednesday.morning=08:30-18:30 workPeriod.thursday.morning=08:30-18:30 workPeriod.friday.morning=08:30-18:30

- **liveReporting.tat.xml**: this file allows you to define tables which contain an "on-the-fly" count of the number of events, raw logs, and ignored and unknown events per equipment unit.
- **rawData.conf.xml**: this file contains the configuration for executing tasks for the raw logs. You can execute these tasks through the GUI as well.
- **rawDataFiles.conf.xml**: this file contains the references for the raw log files present on the machine (md5sum, size, etc).
- **receiver.conf.xml**: this file contains information about the local Log Collector (port, certificate to be used, Events Per Second limiter)
- **replay.status.xml**: this file contains the status configuration for a replay action. In case the replay is stopped, you can find in this file the status of the replay execution at the time it was stopped.
- **rulesets.conf.xml**: this file contains the description of all the rulesets available. This file is automatically filled when adding a ruleset in the GUI.
- **spooler.conf.xml**: this file contains the server spooler parameters. This configuration can be changed via a configuration menu dedicated to each Log Collector. In our example, this is the local Log Collector configuration menu.
- **statRequest.conf.xml**: this file contains the requests for executing the statistics that are displayed in the alert monitoring window (bar chart, number of events per second, etc).
- **tatComputedDates.data.txt**: file listing the successful generation of Reporting Tables along with their respective time periods and execution date.

Figure 146 tatComputedDates.data.txt

```
2007-05-19 02:01:00 CEST|2007-05-18 00:00:00 CEST|2007-05-18 23:59:59 CEST
2007-05-19 02:03:02 CEST|2007-05-18 00:00:00 CEST|2007-05-18 23:59:59 CEST
```

- **tomcat.ks**: "ks" certificate for tomcat (access to the GUI).
- **user_backup.conf.xml**: this file contains the backup configuration. The corresponding GUI menu option is available from the Configuration menu.

/home/exaprotect/conf/

The table below lists the available files:

Table 41 /home/exaprotect/conf/

```
[root@test INSTANCE_NAME]# ls /home/exaprotect/conf/
ca.pem
client.key
client.p12
client.pem
exa_client_zip.properties
exa_dbmanager.properties
exa_do_backup.properties
exa_do_tat.properties
exa_executor.properties
exa_unzip.properties
exa_update.properties
executor_log4j.properties
executor.properties
feed
other_log4j.properties
INSTANCE_NAME
update_log4j.properties
update.properties
```

The directories are as follows:

- INSTANCE_NAME: Contains the files specifically related to the instance (described in this same chapter). Please note that the directory will have the same name as the respective instance. (INSTANCE_NAME is the name of the directory in this example where the instance's name is INSTANCE_NAME).
- Feed: Contains the configuration files or the messages relating to the mass injection of Log Collectors.

The scripts used to execute these actions are located in the following folder: `/usr/local/exaprotect/bin/feed`

The table below lists the files with respective descriptions:

- ca.pem: TIBCO LogLogic® certificate. DO NOT MODIFY.
- client.key: Customer certificate. DO NOT MODIFY.

- client.p12: Customer certificate. DO NOT MODIFY.
- client.pem: Customer certificate. DO NOT MODIFY.
- exa_client_zip.properties: Configuration for creating the installation file (.zip).
- exa_dbmanager.properties: Java configuration.
- exa_do_backup.properties: Configuration for generating a backup of the configuration (user, Log Collector, etc).
- exa_do_tat.properties: Configuration for manually executing batch reporting tables.
- exa_executor.properties: Configuration for the executor: launching commands via the GUI or relating to correlation.
- exa_unzip.properties: Configuration allowing the use of this program when installing a Log Collector for example (using the installation zip file).
- exa_update.properties: Java configuration of the update function.
- executor_log4j.properties: The configuration for the executor logs (debug, location, name of file…).
- executor.properties: The configuration for the executor
- other_log4j.properties: Configuration for "other" logs: manually launched commands which do not correspond to SMP services (debug, location, name of file…).
- update_log4j.properties: Allows you to manage the configuration of the update logs (debug, location, name of file…).
- update.properties: Allows you to store information relating to the machine update via the Web interface . This information is presented in the "configuration/package update" menu. (Note the connection with the files" ca.pem ", "client.pem" and" client.key.") It is necessary to have defined a p12 certificate in the GUI.

/home/exaprotect/etc/

The table below lists the available files:

Table 42 /home/exaprotect/etc/

```
[root@INSTANCE_NAME etc]# ls /home/exaprotect/
etc/
crontab  logrotate.d  ntp.conf  sysconfig
[root@INSTANCE_NAME etc]# ls logrotate.d/
smp  mgetty  postfix  psacct  rpm  snmpd  syslog
up2date  vsftpd.log
[root@INSTANCE_NAME etc]# ls sysconfig/
iptables
[root@INSTANCE_NAME etc]#
```

The directories are as follows:

logrotate.d: This directory contains all the files which allow you to set up rotations for files, such as for log files. To gain a better understanding about this operation, simply open one of the files present in this directory. The "logrotate" configuration file which manages these various files is found at:

/etc/logrotate.conf

sysconfig: This directory contains a file (iptables) storing all the deployed rules.

crontab: contains the crontab for the SMP server.

ntp.conf: contains the NTP server configuration for the server.

> **Caution:** For all these files, it is necessary to copy and paste them to the file of origin on the server (/etc/init.d/) as it is this field which is executed. These files are used only as reference by the GUI; they are then systematically copied.

Log Files

/var/lib/exaprotect/logs/

The table below lists the available files:

Table 43 Log Files

```
[root@INSTANCE_NAME etc]# ls /var/lib/exaprotect/logs/
smp_executor_errors.log
smp_executor.log
smp_executor.log.2007-05-18
smp_mysql.log
smp_other_errors.log
smp_other.log
smp_update_errors.log
INSTANCE_NAME
```

The directories are as follows:

INSTANCE_NAME: contains the log files for the INSTANCE_NAME instance

INSTANCE_NAME2: contains the log files for the INSTANCE_NAME2 instance

> **Note:** Please note that the directory will have the same name as the respective instance. ("INSTANCE_NAME" is the name of the directory in this example where the instance's name is INSTANCE_NAME).

The files are the following:

Table 44 Files

smp_executor_errors.log	Error log file for "smp_executor.log."
smp_executor.log	Log file corresponding to the launching of commands from the GUI or from the correlation process.
smp_monitor.log	Monitoring log file.

Table 44 Files

smp_mysql.log	MySQL database log file.
smp_other_errors.log	Error log file for “smp_other.log.”
smp_other.log	Log file concerning commands launched manually that do not correspond to SMP services.
smp_update_errors.log	Log files concerning updates executed through the GUI.

The files are replaced every day because of a particular configuration. That is why only 5 files are present online.

/var/lib/exaprotect/logs/INSTANCE_NAME/

The table below lists the available files:

Table 45 Files

admin.log	Platform administration logs (modification of user, rights, profile modification on rules...).
auth.log	Server authentication logs.
catalina.out	Apache server logs corresponding to standard runtime and reporting targets (enables to underline the Out of Memory).
correlator.log	Correlator debug logs.
sma_activity.log	Log activity of the local Log Collector.
sma_errors.log	Local Log Collector error logs (of a particular instance).
sma.log	Local Log Collector logs.
smp_errors.log	Server error logs (of a particular instance).
smp.log	Server logs.
smp_rawlog.log	The logs for the generation of raw log archives.
smp_report_errors.log	Reporting interface error logs.
smp_report.log	Reporting interface logs.
jdbc.log	Debug logs of the jdbc driver allowing the link between the GUI and the MySQL database.

The majority of the log files were conceived to be replaced by another without being deleted. There is a different configuration for each file and it is configurable for some of them.

/usr/local/exaprotect-setup/logs/

This folder contains all the logs relating to an update or installation.

The list of files is as follows:

Table 46 Log Files

install.files	This file contains the list of installed or modified files.
install.log	Log file.

Monitoring Resources

You can monitor all of the following:

- Binary files
- Configuration files
- Archives
- Log files

It is possible to monitor the SMP server concerning CPU use, memory, disk space…

Binary Files

The binary files are found in the following directory:

`/usr/local/exaprotect/monitoring/`

The list of files is as follows:

Table 47 Files

`monitor_analyzer.pl` `monitor_collector.pl` `monitor.pm` `monitor_sendlog.pl`

The Configuration Files

The configuration files are found in the following directory:

`/home/exaprotect/monitoring/`

The list of files is as follows:

Table 48 Configuration Files

monitor-analyser.properties	List of the fields that are monitored according to threshold values.
monitor-messages-en.properties	File in which are stored messages corresponding to the various alerts (in English).
monitor-messages-fr.properties	Same as above (in french).
monitor.properties	Monitoring configuration file allowing you to indicate the files to be used.

Table 48 Configuration Files

monitor-sender.properties	Configuration file about information sent by the monitoring window (sent via syslog, writing in a file, etc.)
monitor-sendlog.properties	Allows you to send logs by mail (cf crontab) periodically.

The Archive Files

The archive files are found in the following directory:

`/var/lib/exaprotect/monitoring/backup/`

The list of files is as follows:

Table 49 Archive Files

20070629152014-esmp_monitor-test.txt	Contains all the field values to be monitored
esmp_monitor-test.tar.gz	Contains all the monitoring values since the server installation

The Log File

The log file is found in the following file:

`/var/log/monitor.log`

The file is monitored by a specific converter in order to list the alerts in the SMP alert display.

Chapter 8 - List of Abbreviations

Here is the list of abbreviations used in this documentation.

They are sorted in alphabetical order.

A

ADA: Archiving Disk Array

C

CA: Certification Authority

CSR: Certificate Signing Request

D

DMZ: De Militarized Zone

DNS: Domain Name System

E

Eth: Ethernet

F

FQDN: Fully Qualified Domain Name

FTP: File Transfer Protocol

G

Gb/s: Gigabyte per Second

Gb: Gigabyte

GUI: Graphical User Interface

H

HTTP: HyperText Transfer Protocol

HTTPS: HyperText Transfer Protocol Secure

I

ICMP: Internet Control Message Protocol

IP: Internet Protocol

ISO: International Organization for Standardization

L

LAN: Local Area Network

M

MD5: Message-Digest algorithm 5

N

NTP: Network Time Protocol

P

PC: Personal Computer

R

RAID: Redundant Array of Independent Drives or Redundant Array of Inexpensive Drives

RAM: Random Access Memory

RH: RedHat

S

SAN: Storage Area Network

SEM: EventManager

SEM: Security Event Manager

SEV: LogManager

SLA: Service Level Agreement

SMP: Security Management Platform

SMTP: Simple Mail Transfer Protocol

SNMP: Simple Network Management Protocol

SSL: Secure Sockets Layer

SSH: Secure Shell

T

TCP: Transmission Control Protocol

TLS: Transport Layer Security

U

URL: Uniform Resource Locator

V

VIP: Virtual IP address

VPN: Virtual Private Network

VSFTP: Very Secure FTP

W

WAN: Wide Area Network

SEM Glossary

Table 50 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 50 Glossary

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

Table 50 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